UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)** **)**	**Docket No. RD13-_____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARD EOP-004-2 – EVENT REPORTING

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
Stacey Tyrewala
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
stacey.tyrewala@nerc.net

Counsel for the North American Electric Reliability Corporation

December 31, 2012

TABLE OF CONTENTS

I. Executive Summary…….. 3

II. Notices and Communications……... 6

III. Background ……. 6

a. Regulatory Framework
b. NERC Reliability Standards Development Procedure
c. History of Project 2009-01, Disturbance and Sabotage Reporting

IV. Justification for Approval of the Proposed Reliability Standard…….. 10

a. Basis and Purpose of Proposed Standard and Improvements in this Revision
b. Enforceability of the Proposed Reliability Standard

V. Summary of the Reliability Standard Development Proceedings…….. 19

a. Overview of the Standard Drafting Team
b. Standard Authorization Request Development
c. First Posting – Informal Comment Period
d. Second Posting – Informal Comment Period
e. Third Posting – Formal Comment Period and Initial Ballot and Non-Binding Poll
f. Fourth Posting – Formal Comment Period and Successive Ballot and Non-Binding Poll
g. Fifth Posting – Formal Comment Period and Successive Ballot and Non-Binding Poll
h. Sixth Posting – Recirculation Ballot and Non-Binding Poll
i. Board of Trustees Approval of EOP-004-2

VI. Conclusion……. 26

Exhibit A — Order No. 672 Criteria

Exhibit B — Proposed Reliability Standard EOP-004-2 Submitted for Approval

Exhibit C — Implementation Plan for Proposed Reliability Standard EOP-004-2 Submitted for Approval

Exhibit D — Consideration of Comments

Exhibit E — Analysis of how VRFs and VSLs Were Determined Using Commission Guidelines

Exhibit F — Record of Development of Proposed Reliability Standard

Exhibit G — Standard Drafting Team Roster for NERC Standards Development Project 2009-01

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)** **)**	**Docket No. RD13-____**

PETITION OF THE
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
FOR APPROVAL OF PROPOSED RELIABILITY STANDARD
EOP-004-2 – EVENT REPORTING

The North American Electric Reliability Corporation ("NERC")[1] hereby requests the Federal Energy Regulatory Commission ("FERC" or the "Commission") approve, in accordance with Section 215(d)(1) of the Federal Power Act ("FPA")[2] and Section 39.5 of the Commission's regulations, 18 C.F.R. § 39.5 (2012), the proposed Reliability Standard —EOP-004-2—Event Reporting, and find that the proposed Reliability Standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest. EOP-004-2 was approved by the NERC Board of Trustees on November 7, 2012.[3]

NERC is hereby requesting approval of the proposed Reliability Standard, the associated implementation plan, Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs"), and retirement of the currently effective Reliability Standard as detailed below. Specifically, NERC requests approval of the following:

- Approval of proposed Reliability Standard EOP-004-2 included in **Exhibit B**, effective the first day of the first calendar quarter that is six months following the effective date of a Final Rule in this docket;

---

[1] NERC has been certified by the Commission as the electric reliability organization ("ERO") in accordance with Section 215 of the Federal Power Act. The Commission certified NERC as the ERO in its order issued July 20, 2006 in Docket No. RR06-1-000. *North American Electric Reliability Corp.*, 116 FERC ¶ 61,062 (2006) ("ERO Certification Order").

[2] 16 U.S.C. § 824o (2012).

[3] Unless otherwise designated, all capitalized terms shall have the meaning set forth in the Glossary of Terms Used in NERC Reliability Standards, available here: http://www.nerc.com/files/Glossary_of_Terms.pdf.

- Retirement of the following standards at midnight of the day immediately prior to the effective date of EOP-004-2:[4]
    - EOP-004-1 – Disturbance Reporting
    - CIP-001-2a – Sabotage Reporting

- Approval of the implementation plan for the proposed EOP-004-2 Reliability Standard which is included in **Exhibit C**.

The proposed effective date for the standard is just and reasonable and appropriately balances the urgency in the need to implement the standards against the reasonableness of the time allowed for those who must comply to develop necessary procedures, software, facilities, staffing or other relevant capability. The proposed effective date will allow applicable entities adequate time to ensure compliance with the requirements in accordance with Order No. 672.[5] As required by Section 39.5 of the Commission's regulations, this petition presents the technical basis and purpose of the proposed Reliability Standard EOP-004-2 and a demonstration that the proposed Reliability Standard meets the criteria identified by the Commission in Order No. 672.

I. EXECUTIVE SUMMARY

The proposed Reliability Standard provides a comprehensive approach to reporting disturbances and events that have the potential to impact the reliability of the Bulk Electric System in accordance with several Commission directives. The principal goal of NERC is to promote the reliability of the Bulk-Power System in North America and this goal is directly supported by evaluating events, undertaking appropriate levels of analysis to determine the

---

[4] Note, Compliance Application Notice CAN-0016 CIP-001 R1: Sabotage Reporting Procedure will be deemed to have been retired on midnight of the day immediately prior to the effective date of EOP-004-2.

[5] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204 at P 333, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006) ("In considering whether a proposed Reliability Standard is just and reasonable, FERC will consider also the timetable for implementation of the new requirements, including how the proposal balances any urgency in the need to implement it against the reasonableness of the time allowed for those who must comply to develop the necessary procedures, software, facilities, staffing or other relevant capability.").

causes of the events, promptly assuring tracking of corrective actions to prevent recurrence, and providing lessons learned to the industry.

The proposed Reliability Standard requires Responsible Entities to have an Operating Plan for reporting applicable events to NERC and others (*e.g.*, Regional Entities, applicable Reliability Coordinators and law enforcement) within 24 hours of the event according to the procedure specified in their Operating Plan. This requires Responsible Entities to report events in a timely manner to allow governmental authorities and critical infrastructure members the opportunity to react in a meaningful manner to such information[6] which supports reliability principles and ultimately helps protect against future malicious physical attacks. The results-based approach of EOP-004-2 includes clear criteria for reporting, consistent reporting timelines, and encourages the development of an internal corporate culture of compliance that is focused on reliability and communication. The proposed Reliability Standard provides for timely event analysis and ensures that NERC can develop trends and prepare for a possible next event.

The requirements of the proposed Reliability Standard complement the efforts of the NERC Bulk-Power System Awareness group and event analysis programs, and the standard drafting team worked in coordination with the Event Analysis Working Group to develop a list of the events that are required to be reported for reliability purposes.[7] This list is incorporated into the proposed EOP-004-2 standard as Attachment 1. Attachment 2 (or alternatively Department of Energy ("DOE") Form OE-417) is the form to be used by Responsible Entities for reporting when the threshold for an event listed in Attachment 1 is met.

NERC's Bulk-Power System Awareness group seeks to provide timely, accurate and complete information regarding the current status of the Bulk-Power System and threats to its

---

[6] *See* Order No. 693 at P 470.

[7] *See e.g.*, Event Analysis Process Document – Version 1 at Appendix E, Categorization of Events, available at: http://www.nerc.com/page.php?cid=5|365.

reliable operation, enabling NERC and the industry to understand and learn from events and ultimately improve the reliability of the Bulk-Power System. The event analysis process also provides valuable input for training and education, reliability trend analysis efforts and reliability standards development, all of which support continued reliability improvement.

Proposed Reliability Standard EOP-004-2 is a result of merging EOP-004-1 and CIP-001-2a and represents a significant improvement in the identification and reporting of events. Successful event analysis depends on a collaborative approach in which registered entities, Regional Entities and NERC work together to achieve a common goal. NERC respectfully requests that the Commission approve the proposed Reliability Standard as just, reasonable, not unduly discriminatory or preferential and in the public interest.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[8]

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco*
Senior Vice President and General Counsel
Holly A. Hawkins*
Assistant General Counsel
Stacey Tyrewala*
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
stacey.tyrewala@nerc.net

[8] Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

III. BACKGROUND

a. Regulatory Framework

By enacting the Energy Policy Act of 2005,[9] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Nation's Bulk-Power System, and with the duty of certifying an ERO that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215 of the FPA states that all users, owners, and operators of the Bulk-Power System in the United States will be subject to Commission-approved Reliability Standards.[10]

Section 215(d)(5) of the FPA authorizes the Commission to order the ERO to submit a new or modified Reliability Standard. Pursuant to Section 215(d)(2) of the FPA and Section 39.5(c)(1) of the Commission's regulations, the Commission will give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard. In Order No. 693, the Commission noted that it would defer to the "technical expertise" of the ERO with respect to the content of a Reliability Standard and explained that, through the use of directives, it provides guidance but does not dictate an outcome. Rather, the Commission will consider an equivalent alternative approach provided that the ERO demonstrates that the alternative will address the Commission's underlying concern or goal as efficiently and effectively as the Commission's proposal, example, or directive.[11]

Section 39.5(a) of the Commission's regulations requires the ERO to file with the Commission for its approval each Reliability Standard that the ERO proposes to become mandatory and enforceable in the United States, and each modification to a Reliability Standard

---

[9] 16 U.S.C. § 824o (2012).

[10] *See* Section 215(b)(1)("All users, owners and operators of the bulk-power system shall comply with reliability standards that take effect under this section.").

[11] *See Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242 at PP 31, 186-187, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

that the ERO proposes to be made effective. The Commission has the regulatory responsibility to approve standards that protect the reliability of the Bulk-Power System and to ensure that such standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest.

b. NERC Reliability Standards Development Procedure

The proposed Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[12] NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual.[13] In its ERO Certification Order, the Commission found that NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards and thus satisfies certain of the criteria for approving Reliability Standards. The development process is open to any person or entity with a legitimate interest in the reliability of the Bulk-Power System. NERC considers the comments of all stakeholders, and a vote of stakeholders and the NERC Board of Trustees is required to approve a Reliability Standard before the Reliability Standard is submitted to the Commission for approval.

c. History of Project 2009-01, Disturbance and Sabotage Reporting

Project 2009-01—Disturbance and Sabotage Reporting, was initiated on April 2, 2009, by PJM Interconnection, L.L.C. as a request for revision to existing standards CIP-001-1,

---

[12] Order No. 672 at P 334 ("Further, in considering whether a proposed Reliability Standard meets the legal standard of review, we will entertain comments about whether the ERO implemented its Commission-approved Reliability Standard development process for the development of the particular proposed Reliability Standard in a proper manner, especially whether the process was open and fair. However, we caution that we will not be sympathetic to arguments by interested parties that choose, for whatever reason, not to participate in the ERO's Reliability Standard development process if it is conducted in good faith in accordance with the procedures approved by FERC.").

[13] The NERC Rules of Procedure are available here: http://www.nerc.com/page.php?cid=1%7C8%7C169. The current NERC Standard Processes Manual is available here: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf.

Sabotage Reporting, and EOP-004-1, Disturbance Reporting. The Standard Authorization Request was initiated to provide clarity on an appropriate threshold for reporting potential acts of sabotage as required by CIP-001-1, and to revise several requirements in currently effective EOP-004-1 that reference out-of-date Department of Energy forms and to eliminate "fill-in-the-blank" components.

The Disturbance and Sabotage Reporting drafting team was formed in late 2009. The drafting team developed EOP-004-2, Event Reporting, by combining the requirements of EOP-004-1 and CIP-001-2a into a single reporting standard using the results-based standard development approach.[14] The EOP-004-1 standard contains the requirements for reporting and analyzing disturbances while the CIP-001-2a standard addresses sabotage procedures and reporting. The drafting team used the NERC Security Guideline for the Electricity Sector: Threat and Incident Reporting as a resource.[15] In 2010, the drafting team developed a concept paper that identified the major concepts that the team proposed to be incorporated into the EOP-004-2 standard and posted the paper for comments. Additionally, the drafting team worked in coordination with the Events Analysis Working Group to develop a list of the events that would be required to be reported for reliability purposes and incorporated that list into Attachment 1 of the EOP-004-2 standard.

i. Issues With Respect to Defining the Term "Sabotage"

The drafting team considered the directive by the Commission in Order No. 693 to "further define the term [sabotage] and provide guidance on triggering events that would cause

[14] The results-based initiative is intended to focus the collective effort of NERC and industry participants on improving the clarity and quality of NERC Reliability Standards by developing performance, risk and competency-based requirements that accomplish a reliability objective through a defense-in-depth strategy, while eliminating documentation-driven requirements that do not benefit Bulk-Power System reliability.

[15] Available here: http://www.nerc.com/files/Incident-Reporting.pdf.

an entity to report an event."[16] However, there was concern among stakeholders that such a definition could be ambiguous or otherwise subject to interpretation.[17] The drafting team determined that it was almost impossible to determine if a particular act constituted sabotage without the intervention of law enforcement. There is an inherently subjective component to the determination of whether or not any particular event is caused by a malicious act and this determination may vary based on various factors, including the local jurisdiction, given that there is also a legal component to whether or not a particular act is considered to be deliberate or malicious. Further, the definition of the term "sabotage" would have to exclude events such as unintentional operator error, whereas an action by a third party with the same exact consequences or outcome might be considered "sabotage." The drafting team thus determined that attempting to define the term "sabotage" would result in further ambiguity with respect to the reporting of events. Instead, the drafting team developed a list of events included in Attachment 1 to provide guidance for reporting events. The drafting team determined that this method is an equally effective and efficient means of addressing the Commission directive in accordance with Order No. 693.[18]

IV. JUSTIFICATION FOR APPROVAL OF THE PROPOSED RELIABILITY STANDARD

a. Basis and Purpose of Reliability Standard and Improvements in this Revision

---

[16] Order No. 693 at P 461 (internal citation omitted).

[17] *See e.g.*, Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01) Reporting Concepts Paper at 3 ("One thing became clear in the [drafting team's] discussion concerning sabotage: everyone has a different definition."). *Available here*: http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html.

[18] Order No. 693 at P 31 ("we do expect the ERO to respond with an equivalent alternative and adequate support that fully explains how the alternative produces a result that is as effective as or more effective that the Commission's example or directive.").

As noted herein, EOP-004-2 merges CIP-001-2a, which addresses sabotage procedures and reporting, and EOP-004-1,[19] which addresses the reporting and analyzing of disturbances, into a single comprehensive Reliability Standard.[20] EOP-004 is part of the Emergency Preparedness and Operations ("EOP") body of Reliability Standards. The EOP group of Reliability Standards consists of eight Reliability Standards that address preparation for emergencies, necessary actions during emergencies and system restoration and reporting following disturbances.[21] CIP-001 is part of the Critical Infrastructure Protection body of standards.[22]

i. Proposed Reliability Standard, EOP-004-2

Proposed Reliability Standard EOP-004-2 requires reporting of events that impact or may impact the reliability of the Bulk Electric System, provides clear criteria for reporting, includes consistent reporting timelines, including a reporting hierarchy for reporting of disturbances, and

---

[19] The Commission approved EOP-004-1 in Order No. 693. *See* Order No. 693 at P 617.

[20] Requirement R2 of existing Reliability Standard EOP-004-1, which provides that each Reliability Coordinator, Balancing Authority, Transmission Operator, Generation Operator and Load-Serving Entity must promptly analyze Bulk Electric System disturbances on its system or facilities, is incorporated into Requirement R1 of the proposed EOP-004-2 Reliability Standard and is addressed by the NERC Bulk-Power System Awareness group and the NERC events analysis program. The Requirements of EOP-004-2 specify that certain types of events are to be reported, but do not include explicit provisions to analyze events. However, events reported under EOP-004-2 are incorporated into the real-time understanding of the grid that is maintained by the Bulk-Power System Awareness group. Further, such reports may trigger further scrutiny by the NERC event analysis program. If warranted, the events analysis program personnel may request that more data for certain events be provided by the reporting entity or other entities that may have experienced the event.

[21] EOP-001 is dedicated to Emergency Operations Planning. EOP-002 is dedicated to Capacity and Energy Emergencies. EOP-003 is dedicated to Load Shedding Plans. EOP-004 is dedicated to Event Reporting. EOP-005 is dedicated to System Restoration Plans and Blackstart Resources. EOP-006 is dedicated to System Restoration Coordination, [note there is no EOP-007]. EOP-008 is dedicated to Loss of Control Center Functionality and EOP-009 is dedicated to Documentation of Blackstart Generating Unit Test Results.

[22] The Commission approved CIP-001-1 in Order No. 693. *See* Order No. 693 at P 471. On April 21, 2010, NERC filed a petition for approval of an interpretation to Requirement R2 of CIP-001-1, which was approved in a letter order issued by the Commission on February 2, 2011. *North American Electric Reliability Corporation,* Letter order approving interpretation to CIP-001-1, Docket No. RD10-11-000, (February 2, 2011). On June 21, 2011, NERC submitted a Petition for Approval of Reliability Standards CIP-001-2a – Sabotage Reporting with a Regional Variance for Texas Reliability Entity, which was approved in a letter order issued by the Commission on August 2, 2011. *North American Electric Reliability Corporation,* Letter order approving Petition of the North American Electric Reliability Corporation for Approval of the Reliability Standard CIP-001-2a – Sabotage Reporting with a Regional Variance for Texas Reliability Entity, Docket No. RD11-6-000 (August 2, 2011).

provides clarity regarding who will receive the reported information. The proposed Reliability Standard consists of three Requirements. Requirement R1 mandates that Responsible Entities will have an event reporting Operating Plan for reporting specific types of events. Requirement R2 establishes a timeframe for reporting of events, and Requirement R3 states that Responsible Entities must validate the contact information contained in the Operating Plan each calendar year. The proposed Reliability Standard provides a comprehensive approach to disturbance and event reporting as explained in further detail below.

Proposed Requirements

R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

R2. Each Responsible Entity shall report events per their Operating Plan within 24 hours of recognition of meeting an event type threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

R3. Each Responsible Entity shall validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Requirement R1

Requirement R1 of proposed Reliability Standard EOP-004-2 requires Responsible Entities to have an event reporting Operating Plan that includes, but is not limited to the protocol(s) for reporting, and each organization identified to receive an event report, for event types specified in Attachment 1 of EOP-004-2. Attachment 1 of EOP-004-2, Reportable Events, lists: (i) events, (ii) the relevant entity with reporting responsibility and (iii) the threshold for reporting the event. In these situations, Responsible Entities are requirement to submit EOP-004-2 (or DOE Form OE-417) Attachment 2, pursuant to Requirements R1 and R2. The last

column of Attachment 1, "Threshold for Reporting" is a bright line that, if reached, triggers the obligation for the entity to report that they experienced the applicable event per Requirement 1.

The requirement to have an Operating Plan for reporting specific types of events provides the entity with a method to have its operating personnel recognize events that affect reliability and to be able to report them to appropriate parties; *e.g.*, Regional Entities, applicable Reliability Coordinators, and law enforcement and other jurisdictional agencies when so recognized. In addition, these event reports are an input to the NERC event analysis program. The results-based approach of EOP-004-2 encourages the development of a culture of compliance that is focused on reliability and communication.

It is generally accepted that as a good business practice, every Registered Entity that owns or operates elements or devices on the grid should have a formal or informal process, procedure, or steps it takes to gather information necessary to analyze events.[23] Requirement R1 mandates that the Responsible Entity establish documentation on how that procedure, process, or plan is organized. This documentation may be a single document or a combination of various documents that achieve the reliability objective.

The communication protocol(s) could include a process flowchart, identification of internal and external personnel or entities to be notified, or a list of personnel by name and their associated contact information. An existing procedure that meets the requirements of CIP-001-2a may be included in this Operating Plan along with other processes, procedures or plans to meet this requirement.[24]

---

[23] *See e.g*., PJM Manual 13, Emergency Operations, available at: http://www.pjm.com/~/media/documents/manuals/m13.ashx; *see also*, Midwest ISO Disturbance Reporting Procedure RTO-OP-023-r9.1, available at: https://www.midwestiso.org/Library/Repository/Procedure/RTO-OP-023-r9%201%20Disturbance%20Reporting%20Procedure.pdf.

[24] Proposed Reliability Standard EOP-004-2 incorporates existing Reliability Standard CIP-001-2a in its entirety. CIP-001-2a requires that each Reliability Coordinator, Balancing Authority, Transmission Operator, Generation Operator and Load-Serving Entity have procedures for recognizing and for making operating personnel

Requirement R2

Requirement R2 of proposed Reliability Standard EOP-004-2 requires Responsible Entities to report events within 24 hours of recognition of meeting an event type threshold for reporting, or, if an event occurs on a weekend, by the end of the next business day.[25] This incorporation of a deadline for reporting satisfies the Commission directive in Order No. 693 to "require an applicable entity to contact appropriate governmental authorities in the event of sabotage within a specified period of time."[26] Requirement R2 is based on "recognition" of meeting an event type threshold because basing the reporting of events on when the events actually occur would be impractical. In practice, an entity may not be immediately aware of destruction or damage to a remote piece of equipment.[27] Further, requiring Responsible Entities to constantly monitor all equipment and property for destruction or damage would be a waste of resources and would not serve the best interests of the reliability of the Bulk Electric System. For these reasons, the drafting team's incorporation of the term "recognition" is reasonable and is consistent with the Commission's support in Order No. 693 for defining the specified period of time for reporting an event based on when an event is discovered or suspected to be sabotage.[28]

---

aware of sabotage events (Requirement R1 of CIP-001-2a), and communicating information concerning sabotage events to appropriate "parties" in the Interconnection (Requirements R2 through R4 of CIP-001-2a). The requirements of CIP-001-2a are encompassed by Requirement R1 of EOP-004-2 and Attachment 1.

[25] Holidays are not specifically recognized in Requirement R2.

[26] Order No. 693 at P 471.

[27] *See e.g.*, *Comments of Xcel Energy Services, Inc.*, Docket No. RM06-16-000 (January 3, 2007) at p. 24 ("The triggering event for disclosure of an act of sabotage often will be unclear. That is, it is often not clear whether an event is the result of an act of sabotage, the result of negligent misconduct by an individual, or by equipment failure for other reasons. The Xcel Energy Operating Companies operate thousands of miles of bulk power transmission facilities, and many of these facilities are in remote locations. For this reason, it may require investigation to determine whether the triggering event was an act of sabotage, or the result of some other cause (such as weather or unintentional vehicle contact). This investigation will take time –especially if the event occurs at an unstaffed and/or remote station or facility.")(internal citation omitted).

[28] Order No. 693 at P 470 ("Thus, the Commission directs the ERO to modify CIP-001-1 to require an applicable entity to contact appropriate governmental authorities in the event of sabotage within a specified period of time, even if it is a preliminary report. The ERO, through its Reliability Standards development process, is directed to determine the proper reporting period. In doing so, the ERO should consider suggestions raised by

Each Responsible Entity must report and communicate events according to its Operating Plan based on the information in Attachment 1 of EOP-004-2. By implementing the event reporting Operating Plan, the Responsible Entity will assure that NERC has situational awareness so that NERC can develop trends and prepare for a possible next event, and mitigate the current event through the event analysis program.

Responsible Entities that have multiple registrations will only have to submit one report for any individual event.[29] For example, if an entity is registered as a Reliability Coordinator, Balancing Authority and Transmission Operator, the entity would only submit one report for a particular event rather submitting three reports as each individual registered entity. However, there may be several reports as a result of any individual event and this is appropriate as it will provide NERC with a better understanding of the depth and breadth of system conditions based on the given event.

Requirement R3 of existing Reliability Standard EOP-004-1, which requires each Reliability Coordinator, Balancing Authority, Transmission Operator, Generation Operator and Load-Serving Entity experiencing a reportable incident to provide a preliminary written report, has been incorporated into Requirement R2 of proposed Reliability Standard EOP-004-2.

Requirement R3

Requirement R3 of proposed Reliability Standard EOP-004-2 calls for the Responsible Entity to validate the contact information contained in the Operating Plan each calendar year. This requirement helps ensure that the event reporting Operating Plan is up to date and

---

commenters such as FirstEnergy and Xcel to define the specified period for reporting an incident beginning from when an event is discovered or suspected to be sabotage, and APPA's concerns regarding events at unstaffed or remote facilities, and triggering events occurring outside staffed hours at small entities.").

[29] *See* Guideline and Technical Basis for EOP-004-2, Multiple Reports for a Single Organization.

Responsible Entities will be able to effectively report events to NERC to assure situational awareness.

The incorporation of this annual validation in Requirement R3 satisfies the Commission directive in Order No. 693 to "incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."[30]

Attachment 1: Reportable Events

Attachment 1 of EOP-004-2, Reportable Events, lists (i) events, (ii) the relevant entity with reporting responsibility and (iii) the threshold for reporting the event. In these situations, entities are required to submit EOP-004-2 Attachment 2, pursuant to Requirements R1 and R2. The events addressed in Attachment 1 include, among others: damage or destruction of a Facility, transmission loss, generation loss and a BES Emergency[31] requiring public appeal for load reduction. Such events and the thresholds identified for reporting these events, are an equivalent alternative approach that ensures that Responsible Entities respond to events. Therefore, Attachment 1 addresses the Commission's underlying concern as efficiently and effectively as the Commission's directive to define the term "sabotage." Collectively, Requirement R1 and Attachment 1 require entities to properly identify and respond to events to minimize the adverse impact on the Bulk Electric System.[32]

In Attachment 1, the drafting team used the term "Facility" as defined in the Glossary of Terms Used in NERC Reliability Standards.[33] A Facility is defined as: "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a

---

[30] Order No. 693 at P 466.

[31] "BES Emergency" as used in EOP-004-2 is a defined term set forth in the Glossary of Terms Used in NERC Reliability Standards, available here: http://www.nerc.com/files/Glossary_of_Terms.pdf.

[32] This is responsive to the Commission directive at P471 of Order No. 693 requiring NERC to "specify baseline requirements regarding what issues should be addressed in the procedures for recognizing sabotage events and making personnel aware of such events").

[33] *Available here*: http://www.nerc.com/files/Glossary_of_Terms.pdf .

shunt compensator, transformer, etc.)" The drafting team does not intend the use of the term "Facility" to mean a substation or any other facility that one might consider in everyday discussions regarding the grid. This is intended to mean *only* a Facility as defined above. The use of the defined term provides greater clarity for entities regarding the specific types of events that are to be reported. Through the use of the term "Facility," all of the equipment within a substation that is critical to reliability is included.

Attachment 2: Event Reporting Form

Attachment 2 (or alternatively DOE Form OE-417) is the form to be used by Responsible Entities for reporting when the threshold for an event listed in Attachment 1 is met.

The DOE Office of Electricity Delivery and Energy Reliability uses Form OE-417, "Emergency Incident and Disturbance Report," to monitor major system incidents on electric power systems. Tracking disturbances that impact the integrated generating and transmission facilities is an important part of DOE's responsibilities, along with examining issues associated with insufficient capacity reserves. The form collects information on electric emergency incidents and disturbances for DOE's use in fulfilling its overall national security and other energy management responsibilities. The form is a mandatory filing whenever an electrical incident or disturbance is sufficiently large enough to cross the reporting thresholds. Reporting coverage for the Form OE-417 includes all 50 States, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, and the U.S. Trust Territories.

In an effort to minimize administrative burden, U.S. entities may use the DOE OE-417 form, rather than Attachment 2, to report under EOP-004.[34] Pursuant to the DOE's new online process, entities may record email addresses associated with their Operating Plan so that when the report is submitted to DOE, it will automatically be forwarded to the posted email addresses,

[34] Canadian entities are required to use Attachment 2 to report events.

thereby eliminating some administrative burden to forward the report to multiple organizations and agencies.[35] This approach is consistent with the Commission's suggestion in Order No. 693 for NERC to "consider consolidation of the sabotage reporting forms and the sabotage reporting channels with the appropriate governmental authorities to minimize the impact of these reporting requirements on all entities."[36]

b. Enforceability of the Proposed Reliability Standard, EOP-004-2

The proposed Reliability Standard contains measures that support each standard requirement by clearly identifying what is required and how the requirement will be enforced. These measures help provide clarity regarding how the requirements will be enforced, and ensure that the requirements will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party.[37] The VSLs also provide further guidance on how NERC will enforce the requirements of the standard.

i. Violation Risk Factors and Violation Severity Levels

There are three requirements in EOP-004-2. Requirement R1 was assigned a Lower VRF while Requirements R2 and R3 were assigned a Medium VRF. The VRFs and VSLs for the proposed standard comport with NERC and Commission guidelines related to their assignment. For a detailed review of the VRFs, the VSLs, and the analysis of how the VRFs and VSLs were determined using these guidelines, please see **Exhibit E**.

V. SUMMARY OF THE RELIABILITY STANDARD DEVELOPMENT PROCEEDINGS

---

35 *See* http://www.oe.netl.doe.gov/oe417.aspx.

36 Order No. 693 at P 471.

37 Order No. 672 at P 327 ("There should be a clear criterion or measure of whether an entity is in compliance with a proposed Reliability Standard. It should contain or be accompanied by an objective measure of compliance so that it can be enforced and so that enforcement can be applied in a consistent and non-preferential manner.").

The development record for proposed Reliability Standard EOP-004-2 is summarized below. **Exhibit D** contains the Consideration of Comments Reports created during the development of the Reliability Standards. **Exhibit F** contains the complete record of development for the standards.

a. Overview of the Drafting Team

When evaluating proposed Reliability Standard, the Commission is expected to give "due weight" to the technical expertise of the ERO.[38] The technical expertise of the ERO is derived from the drafting team. For this project, the drafting team consisted of four industry experts with a diversity of experience. A detailed set of biographical information for each of the team members is included along with the drafting team roster in **Exhibit G**. The development record for the proposed EOP-004-2 standard is summarized below.

b. Standard Authorization Request Development

The first draft of the Standard Authorization Request was posted for a 30-day public comment from April 22, 2009 to May 21, 2009. The drafting team received 40 sets of comments from 120 people from more than 60 companies representing 9 of the 10 industry segments. Most commenters agreed on the need for revisions to CIP-001-1 and EOP-004-1, but voiced concerns on issues including:

- The applicability of the final requirements;
- Whether or not the standards should be merged;
- The inclusion of vandalism and the thresholds for defining sabotage; and
- Onerous or duplicative reporting required by the current standards.

[38] Section 215(d)(2) of the Federal Power Act; 16 U.S.C. § 824o(d)(2) (2012).

The Disturbance and Sabotage Reporting drafting team was formed in late 2009. In 2010, the drafting team developed a concept paper that identified the major concepts that the team proposed to be incorporated into the EOP-004-2 standard and posted the paper for a 30-day public comment period from March 17, 2010 to April 16, 2010. NERC received 41 sets of comments from 95 different people from approximately 50 companies representing 8 of the 10 industry segments. Most commenters agreed that the guidance in the concept paper should be used as a foundation for revising the standards. In the concept paper, the drafting team proposed to consolidate disturbance and event reporting under a single standard in EOP-004.

c. The First Posting – Informal Comment Period

The first draft of EOP-004-2 was posted for a 30-day informal comment period from September 15, 2010 to October 15, 2010. A mapping document that showed the translation of CIP-001-1 and EOP-004-1 into EOP-004-2 was posted for guidance with the first draft. There were 60 sets of comments, with comments from more than 175 different people from approximately 100 companies representing 9 of the 10 industry segments. In response to comments, the drafting team made several changes to the draft standard including:

- Revised the purpose statement to address the concern that the drafting team went beyond the reliability intent of the standard by concentrating too much on event analysis;
- Added a proposed working definition for “impact events” to the NERC Glossary of Terms;
- Deleted all references to “situational awareness” and instead using the terms “industry awareness” where appropriate;
- Added Load Serving Entities as applicable entities;
- Deleted Requirement R1 and proposed revisions to the NERC Rules of Procedure to include a central system with responsibility for receiving and distributing impact event reports;
- Revised Requirement R2 to include Operating Plan, Operating Process and Operating Procedure;

- Removed Parts 2.5 through 2.9 of Requirement R2 and replaced with Requirement R1, Part 1.4 to require updates to the Impact Event Operating Plan within 90 days of any change to content;
- Rewrote Requirement R3 to eliminate the need to assess the probable cause of an impact event;
- Rewrote Requirement R4 by taking out prescriptive guidance;
- Removed Requirement 5, Parts 5.3 and 5.4 and removed Requirements R7 and R8;
- Removed several bright-line criteria from Attachment 1, modifying it to assign clear responsibility for reporting for each category of impact event, and clarifying the types of events included in Attachment 1; and
- Clarified that NERC will accept DOE OE-417 form in lieu of Attachment 2 if the responsible entity is required to submit an OE-417 form, and added a process for the reporting of a Cyber Security Incident.

d. The Second Posting – Informal Comment Period

The second draft of the standard was posted with the implementation plan for a public 30-day informal comment period from March 9, 2011 to April 8, 2011. The drafting team received 60 sets of comments from 188 different people from approximately 132 different companies representing all 10 industry segments. Several changes were made to the draft of the EOP-004-2 standard including:

- Deleted proposed definition of "Impact Event";
- Revised the reporting time to 24 hours from 1 hour for most events
- Rewrote Requirement R1 to specify that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1;
- Revised the wording in Requirement R2 and R3 to more closely track the actions that need to be taken for reporting events and communications involving the Operating Plan;
- Rewrote Requirement R4 to more closely match the rationale language on annually verifying the communication process in its Operating Plan to provide better guidance to responsible entities; and
- Added clarity on which entities report and to whom events should be reported to.

e. Third Posting – Formal Comment Period and Initial Ballot and Non-Binding Poll

The third draft of the standard was posted for a public 45-day formal comment period from October 28, 2011 to December 12, 2011, and included an initial ballot and non-binding poll from December 2, 2011 to December 12, 2011. A mapping document and the VRF/VSL justification document were provided to aid in the review. The initial ballot for the draft of EOP-004-2 received a quorum of 87.97% and a 36.21% approval. The non-binding poll received a quorum of 85.28% and a 45% approval. The drafting team received 76 sets of comments from 171 individuals from 140 different companies representing nine of the ten industry segments. As a result of the comments, the drafting team made changes to the draft standard including:

- Revised the purpose statement to remove ambiguous language "with the potential to impact reliability";
- Revised Requirement R1 for clarity and matched the language more closely to FERC Order No. 693, Paragraph 471, and eliminated Part 1.2 and reworded Part 1.3 (now 1.2);
- Removed Part1.4 and made Part 1.5 a new Requirement R4;
- Revised Requirement R4 and made it R3;
- Deleted Requirement R2 and merged with R3 to eliminate redundancy;
- Reformatted the table in Attachment 1 to separate one hour reporting requirements from 24-hour reporting requirements; and
- Revised the language and eliminated redundancy in types of events included in Attachment 1.

In response to comments on the third draft, the drafting team also addressed in depth the different processes and reasons for using either the DOE OE-417 form or EOP-004-2 Attachment 2 to report events, and why it was necessary for standard EOP-004-2 to retain Attachment 2 as a reporting option.

f. Fourth Posting – Formal Comment Period and Successive Ballot and Non-Binding Poll

The fourth draft of the EOP-004-2 standard was posted for a public formal comment period from April 25, 2012 to May 24, 2012 with a ten day successive ballot and non-binding poll held from May 15, 2012 to May 24, 2012. The mapping document, a "Consideration of Issues and Directives" document, a VRF/VSL justification document, and a proposed NERC Rules of Procedure Section 812 document were posted to assist in review. The successive ballot received a quorum of 84.43% and an approval of 46.18%. The non-binding poll results achieved a 79.95% quorum and a 52.67% supportive opinion. The drafting team received 87 sets of comments from 210 different people from approximately 135 different companies representing 9 of the 10 industry segments. Based on the comments received, NERC made the following changes to the draft standard:

- Removed the reporting of Cyber Security Incidents from EOP-004 and directed the team developing CIP-008-5 to retain this reporting;
- Removed Interchange Coordinator, Transmission Service Providers, Load-Serving Entity, Electric Reliability Organization and Regional Entity as Responsible Entities;
- Moved most of the "Background" Section language to the "Guidelines and Technical Basis" Section;
- Made minor language changes to the measures and the data retention section.
- Revised Attachment 2 to list events in the same order in which they appear in Attachment 1;
- Revised requirement R1 to include the Parts in the main body of the Requirement;
- Deleted Requirement R3 and R4 and established a new Requirement R3 to have the Registered Entity "validate" the contact information in the contact list(s) they may have for the events applicable to them;
- Updated Attachment 1 by assigning event titles and entity responsibilities.

In this iteration, the drafting team noted that NERC had initiated a new effort to forward event reports to applicable government authorities, so the proposed Section 812 of the NERC Rules of Procedure was no longer needed and was removed from the project. Due to suggestions received

during this comment period to improve the standard, the drafting team decided to post the standard for a second successive ballot period.[39]

g. Fifth Posting – Formal Comment Period and Successive Ballot and Non-Binding Poll

A fifth draft of the EOP-004-2 standard was posted for a 30-day public formal comment period from August 29, 2012 to September 27, 2012, with a second ten-day successive ballot and non-binding poll held during the last ten days of the comment period, from September 18, 2012 to September 27, 2012. The mapping document, the "Consideration of Issues and Directives" document, and the VRF/VSL justification document were posted to assist in review. The second successive ballot received a quorum of 78.54% and an approval of 63.40%, and the non-binding poll received a 72.59% quorum and a 63.05% supportive opinion. The drafting team received 56 sets of comments from 181 different people from 125 companies, representing 9 of the ten industry segments. In response to comments received, the drafting team made several changes:

- Added language to the Guidelines and Technical Basis section to clarify the applicability of Requirement R1 and R3 to Distribution Providers;
- Added language to the Guidelines and Technical Basis section to clarify that only one report per event is necessary for entities that are registered in several different categories of industry segments;
- Added clarifying language to Requirement R2 on 24-hour reporting; and
- Revised the VSL language for Requirement R1 to address the case in which the event reporting Operating Plan fails to include event types.

In response to the fifth round of comments, the drafting team explained that the investigation and analysis portions of the current mandatory and enforceable standards EOP-004-1 and CIP-001-2a will not be incorporated in EOP-004-2. Instead, the analysis provisions will be addressed in the NERC event analysis program upon regulatory approval of EOP-004-2.

---

[39] On July 30, 2012, the drafting team hosted a webinar in order to receive informal feedback and to explain proposed changes to the standard. The slides are available on the project page: http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting_RF.html.

h. Sixth Posting – Recirculation Ballot and Non-Binding Poll

Given that EOP-004-2 failed the second successive ballot with 63.4% support, on October 22, 2012, the drafting team conducted an industry webinar to explain several issues, including the applicability to Distribution Providers, duplicative reporting, the role of the Paragraph 81 project and the reporting burden of the standard.[40]

The sixth and final draft of the EOP-004-2 standard was posted for a recirculation ballot and non-binding poll from October 24, 2012 to November 5, 2012. The standard received a quorum of 85.14% and an approval of 71.39%. The non-binding poll resulted in a quorum of 78.93% and an approval of 71.04%.

i. Board of Trustees Approval of EOP-004-2

The final proposed EOP-004-2 standard was presented to the NERC Board of Trustees on November 7, 2012. NERC staff provided a summary of the proposed standard, as well as a summary of minority issues and associated drafting team responses. The NERC Board of Trustees approved the standard, and NERC staff recommended that it be filed with applicable regulatory authorities.

[40] Slides from the webinar are available here: http://www.nerc.com/docs/standards/dt/Disturbance_and_Sabotage_Reporting_Webinar_20121022_final.pdf.

VI. CONCLUSION

For the reasons set forth above, NERC respectfully requests that the Commission:

- approve the proposed EOP-004-2 Reliability Standard included in **Exhibit B,** effective as proposed herein;
- approve the implementation plan included in **Exhibit C**;
- approve the retirement of Reliability Standards, effective as proposed herein.

Respectfully submitted,

/s/ Stacey Tyrewala

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
Stacey Tyrewala
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
stacey.tyrewala@nerc.net

Counsel for the North American Electric Reliability Corporation

December 31, 2012

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 31st day of December, 2012.

/s/ Stacey Tyrewala
Stacey Tyrewala
Attorney for North American Electric Reliability Corporation

Exhibit A

Order No. 672 Criteria

EXHIBIT A

Order No. 672 Criteria

In Order No. 672,[1] the Commission identified a number of criteria it will use to analyze Reliability Standards proposed for approval to ensure they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. The discussion below identifies these factors and explains how the proposed Reliability Standard has met or exceeded the criteria:

1. Proposed Reliability Standards must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve that goal.[2]

The proposed standard achieves the specific reliability goal of ensuring that events that may impact the reliability of the Bulk Electric System are reported. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the Bulk Electric System. The

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

[2] Order No. 672 at P 321. The proposed Reliability Standard must address a reliability concern that falls within the requirements of section 215 of the FPA. That is, it must provide for the reliable operation of Bulk-Power System facilities. It may not extend beyond reliable operation of such facilities or apply to other facilities. Such facilities include all those necessary for operating an interconnected electric energy transmission network, or any portion of that network, including control systems. The proposed Reliability Standard may apply to any design of planned additions or modifications of such facilities that is necessary to provide for reliable operation. It may also apply to Cybersecurity protection.

Order No. 672 at P 324. The proposed Reliability Standard must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve this goal. Although any person may propose a topic for a Reliability Standard to the ERO, in the ERO's process, the specific proposed Reliability Standard should be developed initially by persons within the electric power industry and community with a high level of technical expertise and be based on sound technical and engineering criteria. It should be based on actual data and lessons learned from past operating incidents, where appropriate. The process for ERO approval of a proposed Reliability Standard should be fair and open to all interested persons.

inclusion of reporting to law enforcement enables and supports reliability principles such as protection of Bulk Electric System from malicious physical attack. The proposed Reliability Standard includes clear criteria for reporting and consistent reporting timelines.

2. Proposed Reliability Standards must be applicable only to users, owners and operators of the bulk power system, and must be clear and unambiguous as to what is required and who is required to comply.[3]

The proposed revisions to this Reliability Standard apply to the following Functional Entities: Reliability Coordinators; Balancing Authorities; Transmission Owners; Transmission Operators; Generator Owners; Generator Operators; and Distribution Providers. Section 4.1 of proposed Reliability Standard EOP-004-2 is clear and unambiguous as to who is required to comply, in accordance with Order No. 672. Further, Requirements R1 through R3 are clear and unambiguous as to what is required, in accordance with Order No. 672. Requirements R1 through R3 provide clear criteria for reporting and consistent reporting timelines and provide clarity around who will receive the information.

3. A proposed Reliability Standard must include clear and understandable consequences and a range of penalties (monetary and/or non-monetary) for a violation. [4]

The VRFs and VSLs for the proposed standard comport with NERC and Commission guidelines related to their assignment. The assignment of the severity level for each VSL is consistent with the corresponding Requirement and the VSLs should

---

[3] Order No. 672 at P 322. The proposed Reliability Standard may impose a requirement on any user, owner, or operator of such facilities, but not on others.

Order No. 672 at P 325. The proposed Reliability Standard should be clear and unambiguous regarding what is required and who is required to comply. Users, owners, and operators of the Bulk-Power System must know what they are required to do to maintain reliability.

[4] Order No. 672 at P 326. The possible consequences, including range of possible penalties, for violating a proposed Reliability Standard should be clear and understandable by those who must comply.

ensure uniformity and consistency in the determination of penalties. The VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations. For these reasons, the proposed Reliability Standard includes clear and understandable consequences in accordance with Order No. 672.

4. A proposed Reliability Standard must identify clear and objective criterion or measure for compliance, so that it can be enforced in a consistent and non-preferential manner. [5]

The proposed Reliability Standard contains measures that support each requirement by clearly identifying what is required and how the requirement will be enforced. These measures help provide clarity regarding how the requirements will be enforced, and ensure that the requirements will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party.

5. Proposed Reliability Standards should achieve a reliability goal effectively and efficiently — but do not necessarily have to reflect "best practices" without regard to implementation cost or historical regional infrastructure design.[6]

The proposed Reliability Standard achieves its reliability goals effectively and efficiently in accordance with Order No. 672. The proposed standard requires Functional Entities to report incidents and provide known information at the time of the report and also includes an illustrated example of a reporting process in an attached flowchart.

6. Proposed Reliability Standards cannot be "lowest common denominator,"

---

[5] Order No. 672 at P 327. There should be a clear criterion or measure of whether an entity is in compliance with a proposed Reliability Standard. It should contain or be accompanied by an objective measure of compliance so that it can be enforced and so that enforcement can be applied in a consistent and non-preferential manner.

[6] Order No. 672 at P 328. The proposed Reliability Standard does not necessarily have to reflect the optimal method, or "best practice," for achieving its reliability goal without regard to implementation cost or historical regional infrastructure design. It should however achieve its reliability goal effectively and efficiently.

***i.e.*, cannot reflect a compromise that does not adequately protect Bulk-Power System reliability. Proposed Reliability Standards can consider costs to implement for smaller entities, but not at consequences of less than excellence in operating system reliability.**[7]

The proposed Reliability Standard does not reflect a "lowest common denominator" approach. To the contrary, the proposed standard represents a significant improvement over the previous version as described herein. Specifically, Attachment 1 provides greater clarity of the types of events that are to be reported as compared to the previous version of the standard.

7. Proposed Reliability Standards must be designed to apply throughout North America to the maximum extent achievable with a single Reliability Standard while not favoring one geographic area or regional model. It should take into account regional variations in the organization and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.[8]

The proposed Reliability Standard, EOP-004-2, applies throughout North America and does not favor one geographic area or regional model.

---

[7] Order No. 672 at P 329. The proposed Reliability Standard must not simply reflect a compromise in the ERO's Reliability Standard development process based on the least effective North American practice — the so-called "lowest common denominator" — if such practice does not adequately protect Bulk-Power System reliability. Although FERC will give due weight to the technical expertise of the ERO, we will not hesitate to remand a proposed Reliability Standard if we are convinced it is not adequate to protect reliability.

Order No. 672 at P 330. A proposed Reliability Standard may take into account the size of the entity that must comply with the Reliability Standard and the cost to those entities of implementing the proposed Reliability Standard. However, the ERO should not propose a "lowest common denominator" Reliability Standard that would achieve less than excellence in operating system reliability solely to protect against reasonable expenses for supporting this vital national infrastructure. For example, a small owner or operator of the Bulk-Power System must bear the cost of complying with each Reliability Standard that applies to it.

[8] Order No. 672 at P 331. A proposed Reliability Standard should be designed to apply throughout the interconnected North American Bulk-Power System, to the maximum extent this is achievable with a single Reliability Standard. The proposed Reliability Standard should not be based on a single geographic or regional model but should take into account geographic variations in grid characteristics, terrain, weather, and other such factors; it should also take into account regional variations in the organizational and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.

8. Proposed Reliability Standards should cause no undue negative effect on competition or restriction of the grid beyond any restriction necessary for reliability.[9]

The proposed Reliability Standard does not restrict the available transmission capability or limit use of the Bulk-Power System in a preferential manner.

9. The implementation time for the proposed Reliability Standard is reasonable.[10]

The proposed effective dates for the standard are just and reasonable and appropriately balance the urgency in the need to implement the standards against the reasonableness of the time allowed for those who must comply to develop necessary procedures, software, facilities, staffing or other relevant capability.

The implementation plan proposes that EOP-004-2 become effective: (i) in those jurisdictions where regulatory approval is required, on the on the first day of the first calendar quarter that is six months after applicable regulatory approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities; and (ii) in those jurisdictions where no regulatory approval is required, on the first day of the first calendar quarter that is six months beyond the date the standard is approved by the Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

---

[9] Order No. 672 at P 332. As directed by section 215 of the FPA, FERC itself will give special attention to the effect of a proposed Reliability Standard on competition. The ERO should attempt to develop a proposed Reliability Standard that has no undue negative effect on competition. Among other possible considerations, a proposed Reliability Standard should not unreasonably restrict available transmission capability on the Bulk-Power System beyond any restriction necessary for reliability and should not limit use of the Bulk-Power System in an unduly preferential manner. It should not create an undue advantage for one competitor over another.

[10] Order No. 672 at P 333. In considering whether a proposed Reliability Standard is just and reasonable, FERC will consider also the timetable for implementation of the new requirements, including how the proposal balances any urgency in the need to implement it against the reasonableness of the time allowed for those who must comply to develop the necessary procedures, software, facilities, staffing or other relevant capability.

This will allow applicable entities adequate time to ensure compliance with the requirements. The proposed effective dates are explained in the proposed Implementation Plan, attached as **Exhibit C**.

10. The Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[11]

The proposed Reliability Standard was developed in accordance with NERC's Commission-approved, ANSI- accredited processes for developing and approving Reliability Standards. Section V, *Summary of the Reliability Standard Development Proceedings,* details the processes followed to develop the standard (for a more thorough review, please see the complete development history included as **Exhibit F**).

These processes included, among other things, multiple comment periods, pre-ballot review periods, and balloting periods. Additionally, all drafting team meetings were properly noticed and open to the public. The initial and recirculation ballots both achieved a quorum and exceeded the required ballot pool approval levels.

11. NERC must explain any balancing of vital public interests in the development of proposed Reliability Standards.[12]

NERC has identified no competing public interests regarding the request for approval of this proposed Reliability Standard. No comments were received that indicated the proposed standard conflicts with other vital public interests.

---

[11] Order No. 672 at P 334. Further, in considering whether a proposed Reliability Standard meets the legal standard of review, we will entertain comments about whether the ERO implemented its Commission-approved Reliability Standard development process for the development of the particular proposed Reliability Standard in a proper manner, especially whether the process was open and fair. However, we caution that we will not be sympathetic to arguments by interested parties that choose, for whatever reason, not to participate in the ERO's Reliability Standard development process if it is conducted in good faith in accordance with the procedures approved by FERC.

[12] Order No. 672 at P 335. Finally, we understand that at times development of a proposed Reliability Standard may require that a particular reliability goal must be balanced against other vital public interests, such as environmental, social and other goals. We expect the ERO to explain any such balancing in its application for approval of a proposed Reliability Standard.

12. Proposed Reliability Standards must consider any other appropriate factors.[13]

No other negative factors relevant to whether the proposed Reliability Standard is just and reasonable were identified.

[13] Order No. 672 at P 323. In considering whether a proposed Reliability Standard is just and reasonable, we will consider the following general factors, as well as other factors that are appropriate for the particular Reliability Standard proposed.

Exhibit B

Proposed Reliability Standard EOP-004-2 Submitted for Approval

A. Introduction

1. Title: Event Reporting

2. Number: EOP-004-2

3. Purpose: To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities.

4. Applicability:

4.1. Functional Entities: For the purpose of the Requirements and the EOP-004 Attachment 1 contained herein, the following functional entities will be collectively referred to as "Responsible Entity."

4.1.1. Reliability Coordinator

4.1.2. Balancing Authority

4.1.3. Transmission Owner

4.1.4. Transmission Operator

4.1.5. Generator Owner

4.1.6. Generator Operator

4.1.7. Distribution Provider

5. Effective Dates:

The first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities. In those jurisdictions where regulatory approval is not required, the standard shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

NERC established a SAR Team in 2009 to investigate and propose revisions to the CIP-001 and EOP-004 Reliability Standards. The team was asked to consider the following:

1. CIP-001 could be merged with EOP-004 to eliminate redundancies.
2. Acts of sabotage have to be reported to the DOE as part of EOP-004.
3. Specific references to the DOE form need to be eliminated.
4. EOP-004 had some 'fill-in-the-blank' components to eliminate.

The development included other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient Bulk Electric System reliability standards.

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009.

The DSR SDT developed a concept paper to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT had developed. The posting of the concept paper sought comments from stakeholders on the "road map" that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the DSR SDT. The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC issues database and FERC Order 693 Directives in order to determine a prudent course of action with respect to revision of these standards.

B. Requirements and Measures

R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Each Responsible Entity will have a dated event reporting Operating Plan that includes, but is not limited to the protocol(s) and each organization identified to receive an event report for event types specified in EOP-004-2 Attachment 1 and in accordance with the entity responsible for reporting.

R2. Each Responsible Entity shall report events per their Operating Plan within 24 hours of recognition of meeting an event type threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

M2. Each Responsible Entity will have as evidence of reporting an event, copy of the completed EOP-004-2 Attachment 2 form or a DOE-OE-417 form; and evidence of submittal (e.g., operator log or other operating documentation, voice recording, electronic mail message, or confirmation of facsimile) demonstrating the event report was submitted within 24 hours of recognition of meeting the threshold for reporting or by the

end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). (R2)

R3. Each Responsible Entity shall validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Each Responsible Entity will have dated records to show that it validated all contact information contained in the Operating Plan each calendar year. Such evidence may include, but are not limited to, dated voice recordings and operating logs or other communication documentation. (R3)

C. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

The Regional Entity shall serve as the Compliance Enforcement Authority (CEA) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2 Evidence Retention

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain the current Operating Plan plus each version issued since the last audit for Requirements R1, and Measure M1.
- Each Responsible Entity shall retain evidence of compliance since the last audit for Requirements R2, R3 and Measure M2, M3.

If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3 Compliance Monitoring and Enforcement Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4 Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Responsible Entity had an Operating Plan, but failed to include one applicable event type.	The Responsible Entity had an Operating Plan, but failed to include two applicable event types.	The Responsible Entity had an Operating Plan, but failed to include three applicable event types.	The Responsible Entity had an Operating Plan, but failed to include four or more applicable event types. OR The Responsible Entity failed to have an event reporting Operating Plan.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Assessment	Medium	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 24 hours but less than or equal to 36 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to one entity identified in its event reporting Operating Plan within 24 hours.	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 36 hours but less than or equal to 48 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to two entities identified in its event reporting Operating Plan within 24 hours.	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 48 hours but less than or equal to 60 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to three entities identified in its event reporting Operating Plan within 24 hours.	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 60 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to four or more entities identified in its event reporting Operating Plan within 24 hours. OR The Responsible Entity failed to submit a report for an event in EOP-004 Attachment 1.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Operations Planning	Medium	The Responsible Entity validated all contact information contained in the Operating Plan but was late by less than one calendar month. OR The Responsible Entity validated 75% but less than 100% of the contact information contained in the Operating Plan.	The Responsible Entity validated all contact information contained in the Operating Plan but was late by one calendar month or more but less than two calendar months. OR The Responsible Entity validated 50% and less than 75% of the contact information contained in the Operating Plan.	The Responsible Entity validated all contact information contained in the Operating Plan but was late by two calendar months or more but less than three calendar months. OR The Responsible Entity validated 25% and less than 50% of the contact information contained in the Operating Plan.	The Responsible Entity validated all contact information contained in the Operating Plan but was late by three calendar months or more. OR The Responsible Entity validated less than 25% of contact information contained in the Operating Plan.

D. Variances

None.

E. Interpretations

None.

F. References

Guideline and Technical Basis (attached)

EOP-004 - Attachment 1: Reportable Events

NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per Requirement R2 and provide as much information as is available at the time of the notification. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net, Facsimile 404-446-9770 or Voice: 404-446-9780.

Submit EOP-004 Attachment 2 (or DOE-OE-417) pursuant to Requirements R1 and R2.

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
Damage or destruction of a Facility	RC, BA, TOP	Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in actions to avoid a BES Emergency.
Damage or destruction of a Facility	BA, TO, TOP, GO, GOP, DP	Damage or destruction of its Facility that results from actual or suspected intentional human action.
Physical threats to a Facility	BA, TO, TOP, GO, GOP, DP	Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. OR Suspicious device or activity at a Facility. Do not report theft unless it degrades normal operation of a Facility.

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
Physical threats to a BES control center	RC, BA, TOP	Physical threat to its BES control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. OR Suspicious device or activity at a BES control center.
BES Emergency requiring public appeal for load reduction	Initiating entity is responsible for reporting	Public appeal for load reduction event.
BES Emergency requiring system-wide voltage reduction	Initiating entity is responsible for reporting	System wide voltage reduction of 3% or more.
BES Emergency requiring manual firm load shedding	Initiating entity is responsible for reporting	Manual firm load shedding ≥ 100 MW.
BES Emergency resulting in automatic firm load shedding	DP, TOP	Automatic firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS).
Voltage deviation on a Facility	TOP	Observed within its area a voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes.

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only)	RC	Operate outside the IROL for time greater than IROL T_V (all Interconnections) or Operate outside the SOL for more than 30 minutes for Major WECC Transfer Paths (WECC only).
Loss of firm load	BA, TOP, DP	Loss of firm load for ≥ 15 Minutes: ≥ 300 MW for entities with previous year's demand ≥ 3,000 OR ≥ 200 MW for all other entities
System separation (islanding)	RC, BA, TOP	Each separation resulting in an island ≥ 100 MW
Generation loss	BA, GOP	Total generation loss, within one minute, of : ≥ 2,000 MW for entities in the Eastern or Western Interconnection OR ≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection
Complete loss of off-site power to a nuclear generating plant (grid supply)	TO, TOP	Complete loss of off-site power affecting a nuclear generating station per the Nuclear Plant Interface Requirement

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
Transmission loss	TOP	Unexpected loss within its area, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing).
Unplanned BES control center evacuation	RC, BA, TOP	Unplanned evacuation from BES control center facility for 30 continuous minutes or more.
Complete loss of voice communication capability	RC, BA, TOP	Complete loss of voice communication capability affecting a BES control center for 30 continuous minutes or more.
Complete loss of monitoring capability	RC, BA, TOP	Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (i.e., State Estimator or Contingency Analysis) is rendered inoperable.

EOP-004 - Attachment 2: Event Reporting Form

EOP-004 Attachment 2: Event Reporting Form

Use this form to report events. The Electric Reliability Organization will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net , Facsimile 404-446-9770 or voice: 404-446-9780.

	Task	Comments
1.	Entity filing the report include: Company name: Name of contact person: Email address of contact person: Telephone Number: Submitted by (name):	
2.	Date and Time of recognized event. Date: (mm/dd/yyyy) Time: (hh:mm) Time/Zone:	
3.	Did the event originate in your system?	Yes ☐ No☐ Unknown ☐
4.	**Event Identification and Description:**	
	(Check applicable box) ☐ Damage or destruction of a Facility ☐ Physical Threat to a Facility ☐ Physical Threat to a control center ☐ BES Emergency: ☐ public appeal for load reduction ☐ system-wide voltage reduction ☐ manual firm load shedding ☐ automatic firm load shedding ☐ Voltage deviation on a Facility ☐ IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only) ☐ Loss of firm load ☐ System separation ☐ Generation loss ☐ Complete loss of off-site power to a nuclear generating plant (grid supply) ☐ Transmission loss ☐ unplanned control center evacuation ☐ Complete loss of voice communication capability ☐ Complete loss of monitoring capability	Written description (optional):

Guideline and Technical Basis

Distribution Provider Applicability Discussion

The DSR SDT has included Distribution Providers (DP) as an applicable entity under this standard. The team realizes that not all DPs will own BES Facilities and will not meet the "Threshold for Reporting" for any event listed in Attachment 1. These DPs will not have any reports to submit under Requirement R2. However, these DPs will be responsible for meeting Requirements R1 and R3. The DSR SDT does not intend for these entities to have a detailed Operating Plan to address events that are not applicable to them. In this instance, the DSR SDT intends for the DP to have a very simple Operating Plan that includes a statement that there are no applicable events in Attachment 1 (to meet R1) and that the DP will review the list of events in Attachment 1 each year (to meet R3). The team does not think this will be a burden on any entity as the development and annual validation of the Operating Plan should not take more that 30 minutes on an annual basis. If a DP discovers applicable events during the annual review, it is expected that the DP will develop a more detailed Operating Plan to comply with the requirements of the standard.

Multiple Reports for a Single Organization

For entities that have multiple registrations, the DSR SDT intends that these entities will only have to submit one report for any individual event. For example, if an entity is registered as a Reliability Coordinator, Balancing Authority and Transmission Operator, the entity would only submit one report for a particular event rather submitting three reports as each individual registered entity.

Summary of Key Concepts

The DSR SDT identified the following principles to assist them in developing the standard:

- Develop a single form to report disturbances and events that threaten the reliability of the Bulk Electric System
- Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements
- Establish clear criteria for reporting
- Establish consistent reporting timelines
- Provide clarity around who will receive the information and how it will be used

During the development of concepts, the DSR SDT considered the FERC directive to "further define sabotage". There was concern among stakeholders that a definition may be ambiguous and subject to interpretation. Consequently, the DSR SDT decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was sabotage or vandalism without the intervention of law enforcement. The DSR SDT felt that attempting to define sabotage would result in further ambiguity with respect to

reporting events. The term "sabotage" is no longer included in the standard. The events listed in EOP-004 Attachment 1 were developed to provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

The types of events that are required to be reported are contained within EOP-004 Attachment 1. The DSR SDT has coordinated with the NERC Events Analysis Working Group to develop the list of events that are to be reported under this standard. EOP-004 Attachment 1 pertains to those actions or events that have impacted the Bulk Electric System. These events were previously reported under EOP-004-1, CIP-001-1 or the Department of Energy form OE-417. EOP-004 Attachment 1 covers similar items that may have had an impact on the Bulk Electric System or has the potential to have an impact and should be reported.

The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in EOP-004 Attachment 1. Real-time communication is achieved is covered in other standards. The proposed standard deals exclusively with after-the-fact reporting.

Data Gathering

The requirements of EOP-004-1 require that entities "promptly analyze Bulk Electric System disturbances on its system or facilities" (Requirement R2). The requirements of EOP-004-2 specify that certain types of events are to be reported but do not include provisions to analyze events. Events reported under EOP-004-2 may trigger further scrutiny by the ERO Events Analysis Program. If warranted, the Events Analysis Program personnel may request that more data for certain events be provided by the reporting entity or other entities that may have experienced the event. Entities are encouraged to become familiar with the Events Analysis Program and the NERC Rules of Procedure to learn more about with the expectations of the program.

Law Enforcement Reporting

The reliability objective of EOP-004-2 is to improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of Bulk Electric System from malicious physical attack. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.

Stakeholders in the Reporting Process

- Industry

- NERC (ERO), Regional Entity
- FERC
- DOE
- NRC
- DHS – Federal
- Homeland Security- State
- State Regulators
- Local Law Enforcement
- State or Provincial Law Enforcement
- FBI
- Royal Canadian Mounted Police (RCMP)

The above stakeholders have an interest in the timely notification, communication and response to an incident at a Facility. The stakeholders have various levels of accountability and have a vested interest in the protection and response to ensure the reliability of the BES.

Present expectations of the industry under CIP-001-1a:

It has been the understanding by industry participants that an occurrence of sabotage has to be reported to the FBI. The FBI has the jurisdictional requirements to investigate acts of sabotage and terrorism. The CIP-001-1-1a standard requires a liaison relationship on behalf of the industry and the FBI or RCMP. These requirements, under the standard, of the industry have not been clear and have lead to misunderstandings and confusion in the industry as to how to demonstrate that the liaison is in place and effective. As an example of proof of compliance with Requirement R4, Responsible Entities have asked FBI Office personnel to provide, on FBI letterhead, confirmation of the existence of a working relationship to report acts of sabotage, the number of years the liaison relationship has been in existence, and the validity of the telephone numbers for the FBI.

Coordination of Local and State Law Enforcement Agencies with the FBI

The Joint Terrorism Task Force (JTTF) came into being with the first task force being established in 1980. JTTFs are small cells of highly trained, locally based, committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. The JTTF is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. Coordination and communications largely through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs. This information flow can be most beneficial to the industry in analytical intelligence, incident response and investigation. Historically, the most immediate response to an industry incident has been local and state law enforcement agencies to suspected vandalism and criminal damages at industry facilities. Relying upon the JTTF

coordination between local, state and FBI law enforcement would be beneficial to effective communications and the appropriate level of investigative response.

Coordination of Local and Provincial Law Enforcement Agencies with the RCMP

A similar law enforcement coordination hierarchy exists in Canada. Local and Provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. The Provincial law enforcement agency has a reporting relationship with the Royal Canadian Mounted Police (RCMP).

A Reporting Process Solution – EOP-004

A proposal discussed with the FBI, FERC Staff, NERC Standards Project Coordinator and the SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Reportable Events). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial or local level law enforcement agency. The state or provincial or local level law enforcement agency will coordinate with law enforcement with jurisdiction to investigate. If the state or provincial or local level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial or local level law enforcement agency will notify and coordinate with the FBI or the RCMP.

Example of Reporting Process including Law Enforcement

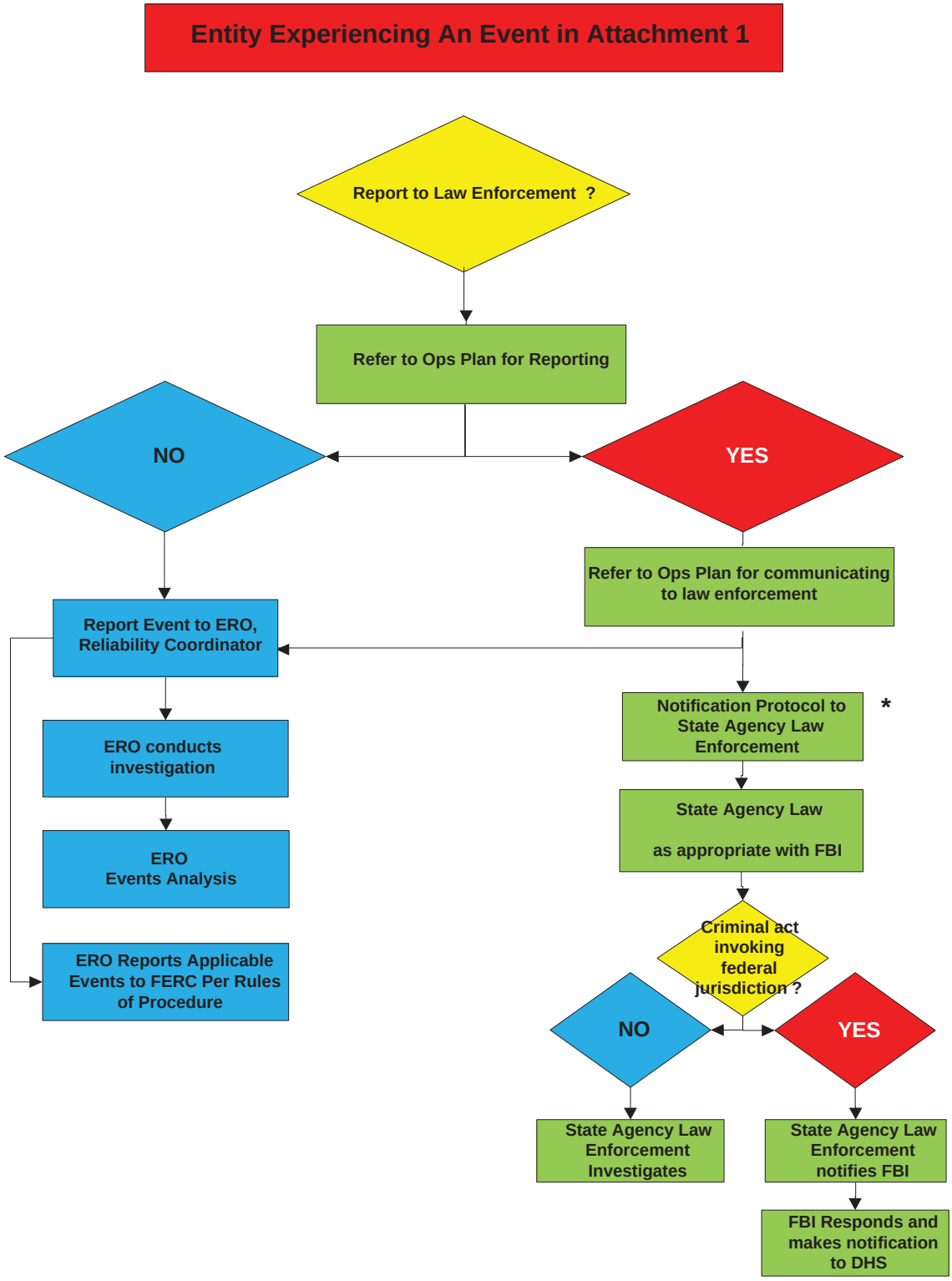

* Canadian entities will follow law enforcement protocols applicable in their jurisdictions

Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01) - Reporting Concepts

Introduction

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and has developed updated standards based on the SAR.

The standards listed under the SAR are:

- CIP-001 — Sabotage Reporting
- EOP-004 — Disturbance Reporting

The changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). These standards deal exclusively with after-the-fact reporting.

The DSR SDT has consolidated disturbance and sabotage event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts and Assumptions:

The Standard:

- Requires reporting of "events" that impact or may impact the reliability of the Bulk Electric System
- Provides clear criteria for reporting
- Includes consistent reporting timelines
- Identifies appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- Provides clarity around of who will receive the information

Discussion of Disturbance Reporting

Disturbance reporting requirements existed in the previous version of EOP-004. The current approved definition of Disturbance from the NERC Glossary of Terms is:

1. An unplanned event that produces an abnormal system condition.
2. Any perturbation to the electric system.

3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.

Disturbance reporting requirements and criteria were in the previous EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and developed the list of events that are to be reported under this standard (EOP-004 Attachment 1).

Discussion of Event Reporting

There are situations worthy of reporting because they have the potential to impact reliability.

Event reporting facilitates industry awareness, which allows potentially impacted parties to prepare for and possibly mitigate any associated reliability risk. It also provides the raw material, in the case of certain potential reliability threats, to see emerging patterns.

Examples of such events include:

- Bolts removed from transmission line structures
- Train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center)
- Destruction of Bulk Electric System equipment

What about sabotage?

One thing became clear in the DSR SDT's discussion concerning sabotage: everyone has a different definition. The current standard CIP-001 elicited the following response from FERC in FERC Order 693, paragraph 471 which states in part: *". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."*

Often, the underlying reason for an event is unknown or cannot be confirmed. The DSR SDT believes that by reporting material risks to the Bulk Electric System using the event categorization in this standard, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.

Certain types of events should be reported to NERC, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and/or Provincial or local law enforcement. Other types of events may have different reporting requirements. For example, an event that is related to copper theft may only need to be reported to the local law enforcement authorities.

Potential Uses of Reportable Information
Event analysis, correlation of data, and trend identification are a few potential uses for the information reported under this standard. The standard requires Functional entities to report the incidents and provide known information at the time of the report. Further data gathering necessary for event analysis is provided for under the Events Analysis Program and the NERC Rules of Procedure. Other entities (e.g. – NERC, Law Enforcement, etc) will be responsible for performing the analyses. The NERC Rules of Procedure (section 800) provide an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for reliability. Jurisdictional agencies (which may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE) have other duties and responsibilities.

Collection of Reportable Information or "One stop shopping"

The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT has updated the listing of reportable events in EOP-004 Attachment 1 based on discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences still exist.

The reporting required by this standard is intended to meet the uses and purposes of NERC. The DSR SDT recognizes that other requirements for reporting exist (e.g., DOE-417 reporting), which may duplicate or overlap the information required by NERC. To the extent that other reporting is required, the DSR SDT envisions that duplicate entry of information should not be necessary, and the submission of the alternate report will be acceptable to NERC so long as all information required by NERC is submitted. For example, if the NERC Report duplicates information from the DOE form, the DOE report may be sent to the NERC in lieu of entering that information on the NERC report.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:
The requirement to have an Operating Plan for reporting specific types of events provides the entity with a method to have its operating personnel recognize events that affect reliability and to be able to report them to appropriate parties; e.g., Regional Entities, applicable Reliability Coordinators, and law enforcement and other jurisdictional agencies when so recognized. In addition, these event reports are an input to the NERC Events Analysis Program. These other parties use this information to promote reliability, develop a culture of reliability excellence, provide industry collaboration and promote a learning organization.
Every Registered Entity that owns or operates elements or devices on the grid has a formal or informal process, procedure, or steps it takes to gather information regarding what happened when events occur. This requirement has the Responsible Entity establish documentation on

how that procedure, process, or plan is organized. This documentation may be a single document or a combination of various documents that achieve the reliability objective. The communication protocol(s) could include a process flowchart, identification of internal and external personnel or entities to be notified, or a list of personnel by name and their associated contact information. An existing procedure that meets the requirements of CIP-001-2a may be included in this Operating Plan along with other processes, procedures or plans to meet this requirement.

Rationale for R2:
Each Responsible Entity must report and communicate events according to its Operating Plan based on the information in EOP-004-2 Attachment 1. By implementing the event reporting Operating Plan the Responsible Entity will assure situational awareness to the Electric Reliability Organization so that they may develop trends and prepare for a possible next event and mitigate the current event. This will assure that the BES remains secure and stable by mitigation actions that the Responsible Entity has within its function. By communicating events per the Operating Plan, the Responsible Entity will assure that people/agencies are aware of the current situation and they may prepare to mitigate current and further events.

Rationale for R3:
Requirement 3 calls for the Responsible Entity to validate the contact information contained in the Operating Plan each calendar year. This requirement helps ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization. If an entity experiences an actual event, communication evidence from the event may be used to show compliance with the validation requirement for the specific contacts used for the event.

Rationale for EOP-004 Attachment 1:
The DSR SDT used the defined term “Facility” to add clarity for several events listed in Attachment 1. A Facility is defined as:

> “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)”

The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-2a Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2 Event Reporting; Retire CIP-001-2a Sabotage Reporting and Retired EOP-004-1 Disturbance Reporting.	Revision to entire standard (Project 2009-01)
2	November 7, 2012	Adopted by the NERC Board of Trustees	

Exhibit C

Implementation Plan for Proposed Reliability Standard EOP-004-2 Submitted for Approval

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2009-01 Disturbance and Sabotage Reporting

Implementation Plan for EOP-004-2 – Event Reporting

Approvals Required
EOP-004-2 – Event Reporting

Prerequisite Approvals
None

Revisions to Glossary Terms
None

Applicable Entities
Reliability Coordinator
Balancing Authority
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Distribution Provider

Conforming Changes to Other Standards
None

Effective Dates
In those jurisdictions where regulatory approval is required, this standard shall become effective on the first day of the first calendar quarter that is six months after applicable regulatory approval or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Retirements

EOP-004-1 – Disturbance Reporting and CIP-001-2a – Sabotage Reporting should be retired at midnight of the day immediately prior to the Effective Date of EOP-004-2 in the particular jurisdiction in which the new standard is becoming effective.

Exhibit D

Consideration of Comments

Project 2009-01
Disturbance and Sabotage Reporting

Related Files

Status:

Adopted by the Board of Trustees on November 6, 2012, pending regulatory approval.

Background:

This project will entail revision to the following existing standards:

- CIP-001-1 – Sabotage Reporting
- EOP-004-1 – Disturbance Reporting

Stakeholders have indicated that identifying potential acts of "sabotage" is difficult to do in real time, and additional clarity is needed to identify thresholds for reporting potential acts of sabotage in CIP-001-1. Stakeholders have also reported that EOP-004-1 has some requirements that reference out-of-date Department of Energy forms, making the requirements ambiguous. EOP-004-1 also has some 'fill-in-the-blank' components to eliminate.

The project will include addressing previously identified stakeholder concerns and FERC directives; will bring the standards into conformance with the latest approved version of the ERO Rules of Procedure; and may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

Draft	Action	Dates	Results	Consideration of Comments
Draft 6 **EOP-004-2** Clean | Redline to last posted Implementation Plan Clean **Supporting Materials:** Mapping	Recirculation Ballot and Non-binding poll Info>> Vote>>	10/24/12 - 11/05/12 (closed)	Summary>> Ballot Results>> Non-binding Poll Results>>	

Document Consideration of Issues and Directives VRF/VSL Justification CIP-001-2a EOP-004-1				
Draft 5 EOP-004-2 Clean | Redline to Last Posted Implementation Plan Clean | Redline to Last Posted **Supporting Materials:** Comment Form (Word) Mapping Document Consideration of Issues and Directives VRF/VSL Justification	Successive Ballot and Non-binding Poll Info>> Vote>>	09/18/12 - 09/27/12 (closed)	Updated Summary>> Ballot Results>> Non-binding Poll Results>>	
	Comment Period Info>> Submit Comments>>	08/29/12 - 09/27/12 (closed)	Comments Received>> Meeting Results>>	Consideration of Comments **(7)**

CIP-001-2a EOP-004-1				
Draft 4 **EOP-004-2** Clean | Redline to Last Posted **Supporting Materials:** Comment Form (Word) Implementation Plan Clean | Redline to Last Posted Mapping Document Consideration of Issues and Directives VRF/VSL Justification Proposed NERC RoP Section 812 CIP-001-2a CIP-008-3 EOP-004-1	Successive Ballot and Non-binding Poll Updated Info>> Info>> Vote>>	05/15/12-05/24/12 (closed)	Summary>> Ballot Results>> Non-binding Poll Results>>	
	Comment Period Info>> Submit Comments>>	04/25/12 - 05/24/12 (closed)	Comments Received>>	Consideration of Comments **(6)**
Draft 3 **EOP-004-2** Clean | Redline	Join Ballot Pools>>	10/28/11 - 11/28/11 (closed)		
	Formal Comment	10/28/11 -	Comments	

to Last Posted **Supporting Materials:** Comment Form (Word) Implementation Plan Clean | Redline to Last Posted Mapping Document VRF/VSL Justification CIP-001-1 EOP-004-1	Period Info>> Submit Comments>>	12/12/11 (closed)	Received>>	Consideration of Comments **(5)**
	Initial Ballot and Non-Binding Poll Updated Info>> Info>> Vote>>	12/02/11 - 12/12/11 (closed)	Summary>> Full Record>> Non-Binding Poll Results>>	
Draft 2 **EOP-004-2** clean | redline to last posted **Supporting Materials:** Comment Form (Word) Implementation Plan CIP-001-1 EOP-004-1	Info>> Formal Comment Period>>	03/09/11 - 04/08/11	Comments Received>>	Consideration of Comments **(4)**
Draft 1 **EOP-004-2**	Informal Comment	09/15/10 –	Comments Received>>	

EOP-004-2 **Supporting Materials:** Comment Form (Word) Mapping Document	Period Submit Comments>> Info>>	10/15/10		Consideration of Comments **(3)**
Concept Paper Supporting Disturbance and Sabotage Reporting Concept Paper **Supporting Materials:** Comment Form (Word) CIP-001-1 - Sabotage Reporting EOP-004-1 - Disturbance Reporting	Comment Period Submit Comments>> Info>>	03/17/10 - 04/16/10 (closed)	Comments Received >>	Consideration of Comments **(2)**
Nominations for Standard Drafting Team **Supporting Materials:** Nomination Form (Word)	Info>> Submit Nomination>>	09/16/09 - 09/30/09 (closed)		
Draft 2				

Disturbance and Sabotage Reporting SAR 2 Clean | Redline to Last Posting				
Nominations for SAR Drafting Team **Supporting Materials:** Nomination Form (Word)	Info>> Submit Nomination>>	04/29/09 - 05/13/09 (closed)		
Proposed SAR Draft SAR Version 1 **Supporting Materials:** Comment Form (Word)	Comment Period Info>> Submit Comments>>	04/22/09 - 05/21/09 (closed)	Comments Received>>	Consideration of Comments**(1)**

Consideration of Comments on Project 2009-01 — SAR for Disturbance and Sabotage Reporting

The Disturbance and Sabotage Reporting SAR Drafting Team (DSR SAR DT) thanks all commenters who submitted comments on the first draft SAR. The SAR was posted for a 30-day public comment period from April 22, 2009 through May 21, 2009. The stakeholders were asked to provide feedback on the documents through a special Electronic Comment Form. There were 40 sets of comments, including comments from more than 120 different people from over 60 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

The majority of stakeholders agree that there is a reliability related need to support modifying CIP-001-1 and EOP-004-1. Of those stakeholders providing comments, they predominantly agreed with the reliability-related reason for the SAR but offered the following concerns:

1) Concerns with applicability of the requirements: The SAR DT notes that applicability will be determined by the final requirements that are written for the standard.
2) Concerns on combining the standards: The SAR DT notes that the Purpose of the SAR indicates that the standards *may* be merged to eliminate redundancy and provide clarity. It will be up to the Standard Drafting team to make this determination through the Standard Development Process (with stakeholder input).
3) Concerns with the definition of sabotage and the inclusion of vandalism, thresholds for defining sabotage, etc.
4) Concerns on onerous or duplicative reporting: The Brief Description section of the SAR states "Specific references to the DOE form need to be eliminated". This should address its concerns.

The SAR DT does not feel that the SAR should be revised based on these comments. The SAR DT will forward these comments to the Standard Drafting Team for its consideration in the drafting of the standards.

The majority of stakeholders agree with the scope of the SAR. Several stakeholders offered suggestions for items to include in the SAR, however the SAR DT believes that these comments may be too prescriptive to include with the SAR. The team feels that inclusion of these types of comments would prevent the Standard Drafting Team from having the ability to develop standard(s) based on stakeholder consensus. The SAR DT will forward these comments to the Standard Drafting Team for its consideration. Some of the comments received include:

1) The inclusion of specific definitions in the SAR (operating personnel, sabotage events, obligations): The SAR DT believes that this would be too prescriptive and believe that this should be addressed by the Standard Drafting Team.
2) Consolidate documents covering reporting requirements: The SAR DT agrees and suggests that the Standard Drafting Team investigate a "one-stop-shopping" solution for the various reports required, including the DOE report.

Stakeholders did not identify any associated business practices for consideration under the SAR. One stakeholder identified a related standard that references multi-site sabotage. The team has included a reference to TOP-005, section 2.9 (Appendix 1) in the SAR under Related Standards. Two stakeholders suggested that Business Practices should not be considered in a standard. The SAR DT notes that standard development projects must not invalidate business practices that are already in place and aids in coordination with North American Energy Standards Board (NAESB).

Many stakeholders had comments regarding applicability of the two standards. Based on these comments, the SAR DT has added Transmission Owner, Generator Owner and Distribution Provider to the Applicability section of the SAR as *possible* entities in the standard(s) developed under this SAR as the Standard Drafting team may have a need to include them in the standard(s). The applicability of Load-Serving Entity or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements through the Standard Development Process. The three main comments were:

1) Regional Reliability Organization applicability: Several commenters do not feel the RRO should be in the standards. The DSR SAR DT concurs and notes that the SAR states that "EOP-004 has some 'fill-in-the-blank' components to eliminate". This will remove the RRO from applicability.
2) Load-Serving Entity/Distribution Provider: Several stakeholders do not feel that the standards should be applicable to LSEs, but should apply to Distribution Providers. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the standard as the Standard Drafting team may have a need to include them in the standard(s). The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements through the Standard Development Process.
3) Transmission Owner/Generator Owner: Several stakeholders have indicated a need to include the TO as an applicable entity. A couple of those would also include the GO. The SAR DT discussed the addition of the TO and GO. The team has a concern that there may be duplication of requirements between the TO/TOP and GO/GOP if the TO and GO are added to the SAR. That being said, the team added the TO and GO to the applicability of the SAR so that the Standard Drafting team may consider these entities for applicability. The applicability of requirements will ultimately be determined by the Standard Drafting Team as it develops the requirements through the Standard Development Process.

Stakeholders provided many good comments that should be considered in the development of the standards under this project. The SAR DT does not believe that these comments require any significant revisions to the SAR, but will forward these comments to the Standard Drafting Team for its consideration in drafting the standard(s). The comments include:

1) Consolidation of reports: The SAR DT agrees with this concept and will forward the comment to the Standard Drafting Team for its consideration.
2) Concerns about pre-determination of combining CIP-001 and EOP-004 into one standard: The SAR states: CIP-001 may be merged with EOP-004 to eliminate redundancies. The two standards may be left separate.

3) Reporting criteria in multiple tables: The team agrees that it would be easier if there were only one table. Part of this scope of this project is to eliminate redundancies and make general improvements to the standard. The team also agrees that the requirements developed should be clear in their reliability objective.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

1. Do you agree that there is a reliability-related reason to support modifying CIP-001-1 and EOP-004-1? If not, please explain in the comment area. 12

2. Do you agree with the scope of the proposed SAR? If not, please explain what should be added or deleted to the proposed scope. 20

3. Are you aware of any associated business practices that we should consider with this SAR? If yes, please explain in the comment area. 38

4. CIP-001-1 applies to the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, and the Load-serving Entity. EOP-004-1 applies to the same entities, plus the Regional Reliability Organization. Do you agree with the applicability of the existing CIP-001-1 and the existing EOP-004-1? If no, please identify what you believe should be modified. 43

5. If you have any other comments on the SAR or proposed modifications to CIP-001-1 and EOP-004-1 that you haven't provided in response to the previous questions, please provide them here. 51

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Jim Case	SERC OC Standards Review Group	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Al McMeekin	SCE&G	SERC	1, 3, 5
2.	Eugene Warnecke	Ameren	SERC	1, 3, 5
3.	Gary Hutson	SMEPA	SERC	1, 3, 5
4.	Melinda Montgomery	Entergy	SERC	1, 3
5.	Tom Sims	Southern	SERC	1, 3, 5
6.	Marc Butts	Southern	SERC	1, 3, 5
7.	Chris Bradley	BREC	SERC	1, 3, 5
8.	Tom Kanzlik	SCE&G	SERC	1, 3, 5
9.	Paul Turner	Ga Systems Operations Corp.	SERC	3
10.	Phil Creech	Progress Energy Carolinas	SERC	1, 3, 5
11.	Vicky Budreau	SCPSA	SERC	1, 3, 5, 9
12.	Renee Free	SCPSCA	SERC	9
13.	Mike Clements	TVA	SERC	1, 3, 5, 9
14.	Travis Sykes	TVA	SERC	1, 3, 5

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
15.	John Troha		SERC	RFC						10			
2.	Group	Harry Tom	Project 2007-02 Operating Personnel Comms Protocols SDT	X	X			X				X	X
	Additional Member		**Additional Organization**	**Region**						**Segment Selection**			
1.	Lloyd Snyder		GSOC	SERC						1			
2.	Tom Irvine		HydroOne	NPCC						1, 9			
3.	Alan Allgower		ERCOT	ERCOT						10			
4.	Harvie Beavers		Colmac Clarion/Piney Creek LP	RFC						5			
5.	Mark L. Bradley		ITC	MRO						1			
6.	Mike Brost		JEA	FRCC						1			
7.	William D Ellard		CAISO	WECC						10			
8.	Ronald Goins		MISO	MRO						10			
9.	Leanne Harrison		PJM	RFC						10			
10.	James McGovern		ISO-NE	NPCC						10			
11.	Wayne Mitchell		Entergy	SERC						1			
12.	John Stephens		City Utilities of Springfield	RFC						1			
13.	Fred Waites		Southern Company	SERC						1			
3.	Group	Kenneth D. Brown	PSEG Enterprise Group Inc Companies	X		X							
	Additional Member		**Additional Organization**	**Region**						**Segment Selection**			
1.	Clint Bogan		PSEG Fossil LLC	RFC						5			
2.	James Hebson		PSEG Energy Resources & Trade	RFC						6			
3.	Gary Grysko		PSEG Power Connecticut	NPCC						5			
4.	Dominic DiBari		PSEG Texas LLC	ERCOT						5			
4.	Group	Guy Zito	Northeast Power Coordinating Council										X
	Additional Member		**Additional Organization**	**Region**						**Segment Selection**			
1.	Ralph Rufrano		New York Power Authority	NPCC						5			
2.	Alan Adamson		New York State Reliability Council	NPCC						10			

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Greg Campoli		New York Independent System Operator	NPCC						2			
4.	Roger Champagne		Hydro-Quebec TransEnergie	NPCC						2			
5.	Kurtis Chong		Independent Electricity System Operator	NPCC						2			
6.	Sylvain Clermont		Hydro-Quebec TransEnergie	NPCC						1			
7.	Manuel Couto		National Grid	NPCC						1			
8.	Chris de Graffenried		Consolidated Edison Co. of New York, Inc.	NPCC						1			
9.	Brian Evans-Mongeon		Utility Services	NPCC						8			
10.	Mike Garton		Dominion Resources Services, inc.	NPCC						5			
11.	Mike Gildea		Constellation Energy	NPCC						6			
12.	Brian Gooder		Ontario Power Generation Incorporated	NPCC						5			
13.	Kathleen Goodman		ISO - New England	NPCC						2			
14.	David Kiguel		Hydro One Networks, Inc.	NPCC						1			
15.	Michael Lombardi		Northeast Utilities	NPCC						1			
16.	Randy MacDonald		New Brunswick System Operator	NPCC						2			
17.	Bruce Metruck		New York Power Authority	NPCC						6			
18.	Robert Pellegrini		The United Illuminating Company	NPCC						1			
19.	Michael Schiavone		National Grid	NPCC						1			
20.	Michael Sonnelitter		FPL Energy/NextEra Energy	NPCC						5			
21.	Peter Yost		Consolidated Edison Co. of New York, Inc.	NPCC						3			
22.	Lee Pedowicz		Northeast Power Coordinating Council	NPCC						10			
23.	Gerry Dunbar		Northeast Power Coordinating Council	NPCC						10			
5.	Group	Michael Gammon	Kansas City Power & Light	X		X		X	X				
	Additional Member		Additional Organization	Region						Segment Selection			
1.	Joe Doetzl		Kansas City Power & Light	SPP						1, 3, 5, 6			
2.	John Breckenridge		Kansas City Power & Light	SPP						1, 3, 5, 6			
6.	Group	Ben Li	IRC Standards Review Committee		X								
	Additional Member		Additional Organization	Region						Segment Selection			

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1. James Castle			NYISO	NPCC						2			
2. Charles Yeung			SPP	SPP						2			
3. Anita Lee			AESO	WECC						2			
4. Matt Goldberg			ISO-NE	NPCC						2			
5. Bill Phillips			MISO	MRO						2			
6. Steve Myers			ERCOT	ERCOT						2			
7. Lourdes Estrada-Salinero			CAISO	WECC						2			
7.	Group	Richard Kafka	Pepco Holdings, Inc. - Affiliates	X		X		X	X				
Additional Member			Additional Organization	Region						Segment Selection			
1. Kara Dundas			Conectiv Energy Supply, Inc.	RFC						5			
2. Tony Gabrielli			Conectiv Energy Supply, Inc.	RFC						5			
3. George Gacser			Potomac Electric Power Co.	RFC						1, 3, 5			
4. E. W. Stowe			Pepco Holdings, Inc	RFC						1, 3, 5			
5. Mark Godfrey			Pepco Holdings, Inc	RFC						1, 3			
8.	Group	Sam Ciccone	FirstEnergy	X		X	X	X	X				
Additional Member			Additional Organization	Region						Segment Selection			
1. Jim Eckels			FE	RFC						1			
2. John Martinez			FE	RFC						1			
3. John Reed			FE	RFC						1			
4. Dave Folk			FE	RFC						1, 3, 4, 5, 6			
5. Doug Hohlbaugh			FE	RFC						1, 3, 4, 5, 6			
6. Larry Hartley			FE	RFC						3			
9.	Group	Jalal Babik	Electric Market Policy	X		X		X	X				
Additional Member			Additional Organization	Region						Segment Selection			
1. Louis Slade				SERC						6			
2. Mike Garton				NPCC						5			

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
10.	Group	Denise Koehn	Bonneville Power Administration	X		X		X	X				

Additional Member	Additional Organization	Region	Segment Selection
1. Theodore Snodgrass	Dispatch	WECC	1

11.	Group	Michael Brytowski	MRO NERC Standards Review Subcommittee										X

Additional Member	Additional Organization	Region	Segment Selection
1. Carol Gerou	MRO	MRO	10
2. Neal Balu	WPS	MRO	3, 4, 5, 6
3. Pam Sordet	XCEL	MRO	1, 3, 5, 6
4. Joe DePoorter	MGE	MRO	3, 4, 5, 6
5. Ken Goldsmith	ALTW	MRO	4
6. Jim Haigh	WAPA	MRO	1, 6
7. Terry Harbour	MEC	MRO	1, 3, 5, 6
8. Joseph Knight	GRE	MRO	1, 3, 5, 6
9. Scott Nickels	RPU	MRO	3, 4, 5, 6
10. Dave Rudolph	BEPC	MRO	1, 3, 5, 6
11. Eric Ruskamp	LES	MRO	1, 3, 5, 6

12.	Individual	Stephen V. Fisher	Lands Energy Consulting										
13.	Individual	Brent Hebert	Calpine Corporation					X					
14.	Individual	Steve Toth	Covanta					X					
15.	Individual	Harvie Beavers	Colmac Clarion					X					
16.	Individual	Russell A. Noble	Cowlitz County PUD			X							
17.	Individual	Michael Puscas	United Illuminating	X		X							
18.	Individual	George Pettyjohn	Reliant Energy					X					

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
19.	Individual	Judith A. James	Texas Regional Entity										
20.	Individual	Edward C. Stein	self								X		
21.	Individual	Chris Scanlon	Exelon	X		X		X	X				
22.	Individual	Mike Davis	WECC										X
23.	Individual	Jimmy Hartmann	ERCOT ISO		X								
24.	Individual	Rick Terrill	Luminant Power					X					
25.	Individual	Rao Somayajula	ReliabilityFirst Corporation										X
26.	Individual	Tony Kroskey	Brazos Electric Power Cooperative, Inc.	X									
27.	Individual	Paul Golden	PacifiCorp	X		X		X	X				
28.	Individual	Terry Harbour	MidAmerican Energy	X									
29.	Individual	Darryl Curtis	Oncor Electric Delivery	X									
30.	Individual	Chris de Graffenried on behalf of Con Edison & O&R	Consolidated Edison Co. of New York, Inc.	X		X			X				
31.	Individual	Wayne Pourciau	Georgia System Operations Corp.			X							
32.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
33.	Individual	Kasia Mihalchuk	Manitoba Hydro	X		X		X	X				
34.	Individual	Jim Sorrels	AEP	X		X		X	X				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
35.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
36.	Individual	Howard Rulf	We Energies			X	X	X					
37.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
38.	Individual	Mike Sonnelitter	NextEra Energy Resources, LLC					X					
39.	Individual	D. Bryan Guy	Progress Energy	X		X		X					
40.	Individual	Kirit Shah	Ameren	X		X		X	X				

1. Do you agree that there is a reliability-related reason to support modifying CIP-001-1 and EOP-004-1? If not, please explain in the comment area.

Summary Consideration: The majority of stakeholders agree that there is a reliability related need to support modifying CIP-001-1 and EOP-004-1. Of those stakeholders providing comments, they predominantly agreed with the reliability-related reason for the SAR but offered the following concerns:

1) Applicability of the requirements: The SAR DT notes that applicability will be determined by the final requirements that are written for the standard.
2) Combining the standards: The SAR DT notes that the Purpose of the SAR indicates that the standards *may* be merged to eliminate redundancy and provide clarity. It will be up to the Standard Drafting team to make this determination through the Standard Development Process (with stakeholder input).
3) Definition of sabotage and the inclusion of vandalism, thresholds for defining sabotage, etc.
4) Onerous or duplicative reporting: The Brief Description section of the SAR states "Specific references to the DOE form need to be eliminated". This should address any concerns.

The SAR DT will forward these comments to the Standard Drafting Team for its consideration in the drafting of the standards.

Organization	Yes or No	Question 1 Comment
SERC OC Standards Review Group	No	The EOP-004-1 standard is an unnecessary duplication of existing DOE reporting requirements. This essentially exposes an entity to fines by NERC, enforced by FERC, for failure to comply with a DOE regulation, which seems improper to us. In addition, reporting requirements do not have an impact on the reliability of the BES
Response: The DSR SAR DT thanks you for your comment. The Brief Description section of the SAR states "Specific references to the DOE form need to be eliminated".		
MidAmerican Energy	No	MidAmerican Energy believes only EOP-004-1 is confusing and needs to modified or clarified. There is no need to combine the two standards. Standard EOP-004 could be clarified to eliminate references to sabotage which are already covered by CIP-001-1. Standard EOP-004 should be strictly limited to system events, not sabotage.
Response: The DSR SAR DT thanks you for your comment. The SAR DT notes that the Purpose of the SAR indicates that the standards *may* be merged to eliminate redundancy and provide clarity. It will be up to the Standard Drafting Team to make this determination through the Standard Development Process (with stakeholder input).		

Organization	Yes or No	Question 1 Comment
Bonneville Power Administration	No	Eliminating a single standard by consolidating two standards does not improve reliability. All of the defined actions are indeed being taken now.
Response: The DSR SAR DT thanks you for your comment. The SAR DT notes that the Purpose of the SAR indicates that the standards *may* be merged to eliminate redundancy and provide clarity. It will be up to the Standard Drafting team to make this determination through the Standard Development Process (with stakeholder input).		
Progress Energy	No	No. It is not clear that the issues listed in a revised standard will improve reliability. Revision based on redundancy is not sufficient reason for combination. Extensive documentation efforts have been made to comply with the current Standards. Unless combining these Standards provides compelling Reliability benefit, it is not worth the industry's resources to revise existing documentation and processes for the sake of eliminating redundancy. Redundancy issues were raised prior to the ERO adopting the initial Standard set into law. We have noted the other issues raised in the SAR, however, it is still unclear where the Reliability benefit of this SAR is evidenced.
Response: The DSR SAR DT thanks you for your comment. Industry consensus indicates that eliminating redundancy between standards is required to avoid potential double jeopardy issues with compliance to the standards. Furthermore, one of the FERC Order 693 directives for CIP-001 is: **Explore ways to reduce redundant reporting, including central coordination of sabotage reports and a uniform reporting format.**		
Kansas City Power & Light	Yes	Agree with the SAR that clarity would be helpful in establishing criteria regarding what constitutes sabotage reporting.
Response: The DSR SAR DT thanks you for your comment. One of the FERC Order 693 directives for CIP-001 is: **Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event.**		
Pepco Holdings, Inc. - Affiliates	Yes	PHI recommends merging these two standards into one.
Response: The DSR SAR DT thanks you for your comment. The SAR DT notes that the Purpose of the SAR indicates that the standards *may* be merged to eliminate redundancy and provide clarity. It will be up to the Standard Drafting team to make this determination through the Standard Development Process (with stakeholder input).		
Electric Market Policy	Yes	Comments: Agree with the statement that sabotage is hard to determine in real time by operations staffs. The determination of sabotage should be left up to law enforcement. They have the knowledge and peer contacts needed to adequately determine whether physical or cyber intrusions are merely malicious acts or coordinated efforts (sabotage).

Organization	Yes or No	Question 1 Comment
		The operators should only be required to report physical and cyber intrusions to law enforcement. All other reporting requirements should apply to law enforcement once a determination of sabotage has been made. If the recommendations above are not to be accepted, then we have the following comments: CIP-001-1 1) R1 states entities shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SAR notes that the industry objects to the multi-site requirement, most likely because the term is ambiguous. If this term remains in the standard, it needs to be clearly defined and responsibilities for obtaining (how do you get this information and from whom?) and distributing need to be included. 2) R1 audits have shown confusion over the requirement to make operating personnel aware of sabotage events. The term operating personnel needs to be defined. Are they the individuals responsible for operating the facility, coordinating with other entities (i.e., RC, BA, TOP, GOP, and LSE)? It has been suggested that notification is required to all personnel at a facility. Keep in mind the purpose of the standard is to ensure sabotage events are properly reported, not to address emergency response. 3) R1 The SAR (NERC Audit and Observation Team) notes that Registered Entities have processes and procedures in place, but not all personnel have been trained. There is no specific training requirement in the standard. 4) R2 & R3 I agree with the SAR that sabotage needs to be defined and these requirements should be more specific with respect to the information to be communicated. It seems to me that the standard should mirror the criteria contained in DOE OE-417. The emphasis should be placed on ensuring that the same information communicated to DOE is shared with the appropriate parties in the Interconnection. 5) R4 I agree with the SAR (NERC Audit and Observation Team) comments regarding the intention of this requirement. There is no language that directs contact with FBI or RCMP although that is what is implied by the Purpose statement. 6) VRF Comments I'm not sure what is intended by the statement Adequate procedures will insure it is unlikely to lead to bulk electric system instability, separation, or cascading failures? The purpose of the standard is that of communication. No operational decisions or actions are directed by this standard, nor does it require entities to address operational aspects resulting from sabotage. 7) The potential exists for overlapping sabotage reporting requirements at nuclear power plants due to multiple regulators (Nuclear Regulatory Commission (NRC) 10 CFR 73 and Federal Energy Regulatory Commission (FERC) NUC-001-1). Some entities may have revised existing NRC driven procedures to accommodate reporting requirements of both regulators. Because of the restrictions placed on NRC driven documents (i.e., procedures are classified as safeguards information), it can be difficult to demonstrate compliance to NERC and/or FERC without ensuring that the individuals are qualified for receipt of such information per 10 CFR 73. Additionally, multiple procedures may have the unintended consequence of delaying appropriate communication.EOP-004-1Consider removing Attachment 2 as the information is

Organization	Yes or No	Question 1 Comment
		duplicated in DOE Form OE-417. A simple reference to the form should suffice.
Response: The DSR SAR DT thanks you for your comment. The team notes that your comments relate directly to potential revisions of the standard requirements. The team will pass your comments along to the Standards Drafting Team for its consideration. For item 4, one of the FERC Order 693 directives for CIP-001 is: **Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event.**		
Lands Energy Consulting	Yes	I have worked with 5 Northwest public utilities on developing procedures related to CIP-001-1 and EOP-004-1. All 5 utilities operate electric systems in fairly remote locations and are embedded in a larger utility's Balancing Authority/Transmission Operator area. A. CIP-001-1 - Developing procedures to unambiguously identify acts of sabotage has been particularly challenging for these systems. In general, it's hard for them to determine whether the most prevalent forms of malicious and intentional system damage that they incur - copper theft and gun shot insulators/equipment - should qualify as acts of sabotage. Although none of the systems consider copper theft to be acts of sabotage, two of the systems consider gun shot insulators/equipment to be acts of sabotage. The other systems look for intent to disrupt electric system operations as a key component of their sabotage identification procedures. Additional guidance from NERC in the form of CIP-001-1 modifications or a companion guidelines document on sabotage identification would provide much needed guidance for these procedures. B. EOP-004-1 - This standard was clearly drafted with the larger electric systems in mind. I have one client that serves 3300 commercial/residential customers from 4-115/13 kV substation transformers and one large industrial customer (80% of its energy load) from a 230/13 kV substation. 75% of the client's load is served from three substations attached to a long, 115 kV transmission line operated by the Bonneville Power Administration. Whenever the line relays open on a permanent fault (which happens 2-3 times per year), the client loses over 50% of its customers (but no more than 10-15 MW during winter peak), thereby necessitating the preparation of a Disturbance Report. To allow utilities to concentrate on operating their systems, without fear of violating EOP-004-1 for failure to report trivial outages, I would remove LSEs from the obligation to report disturbances - leave the reporting to the BA/TOP for large outages in their footprint.
Response: The DSR SAR DT thanks you for your comment. **A. The team notes that your comments relate directly to potential revisions of the standard requirements. The team will pass your comments along to the Standards Drafting Team for its consideration.** **B. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the standard as the Standard Drafting team may have a need to include them in the standard(s). The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements through the Standard Development Process. The team**		

Organization	Yes or No	Question 1 Comment
will pass your comments along to the Standards Drafting Team for its consideration.		
Calpine Corporation	Yes	Communication of facility status or emergencies between merchant generators registered as GOP and the RC, BA, GOP, or LSE in which the facility resides should be coordinated for EOP -004 reporting. The reporting to NERC/DOE should come from the RC, BA, GOP, or LSE.
Response: The DSR SAR DT thanks you for your comment. The team concurs that reporting should be coordinated and will pass your comments along to the Standards Drafting Team for its consideration.		
Covanta	Yes	Yes - the key to Sabotage reporting requirements is identifying what the 'definition' is of an actual or potential 'Sabotage' event. Like any other standard, if FERC/NERC leave it up to 2000+ entities to establish their own definitions of 'Sabotage', you may likely get 2000+ answers. That is not a controlled and coordinated approach. I offer the following definition, "Sabotage - Deliberate or malicious destruction of property, obstruction of normal operations, or injury to personnel by outside agents." Examples of sabotage events could include, but are not limited to, suspicious packages left near site electrical generating or electrical transmission assets, identified destruction of generating assets, telephone/e mail received threats to destroy or interrupt electrical generating efforts, etc." These have passed multiple NERC regional audits and reviews to date.
Response: The DSR SAR DT thanks you for your comment. One of the FERC Order 693 directives for CIP-001 is: **Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event.** **The team will pass your comments along to the Standards Drafting Team for its consideration.**		
Cowlitz County PUD	Yes	The standards as written now create reporting on local customer quality of service outage events not related to BPS disturbances. Sabotage reporting has degenerated into reporting of mischievous vandalism and minor theft occurences. This creates compliance documentation overburden and waste of limited funds needed for true BPS reliability concerns, and also adds nuisance calls to the FBI and Homeland Security.
Response: The DSR SAR DT thanks you for your comment. One of the FERC Order 693 directives for CIP-001 is: **Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event.** **This should address the concern of sabotage vs. vandalism/theft reporting.**		
Reliant Energy	Yes	EOP-004-1 indicates that Generators should analyze disturbances on the bulk electrical system or their facilities. Generators do not have the capability of analyzing the bulk electrical system other than Frequency. Even so, generators can not unilaterally respond to what it thinks are disturbances. In the case of CAISO The Participating Generator

Organization	Yes or No	Question 1 Comment
		Agreement prevents me from making any unilateral moves save for the direst frequency emergencies. If the System operator or Reliability Coordinator informs the generator that there is a disturbance and that logs and readouts etc. are required then the generator should respond with all available information for the subject hours or time. Clearer responsibilities provide clearer results.
Response: The DSR SAR DT thanks you for your comment. While the team agrees that generators may not have the capability to analyze events, the team note that you concern is regarding applicability of requirements. The final wording of the requirements developed by the Standard Drafting Team will determine the applicability.		
Georgia System Operations Corp.	Yes	There is a need to eliminate burdensome reporting deadlines which interfere with the reliable operations or recovery of the BES. There is also a need to move requirements for reporting to NERC or Regional Entities (except for reporting of threats to physical or cyber security) from the Requirements section of Reliability Standards to elsewhere.
Response: The DSR SAR DT thanks you for your comment. Specific revisions to the requirements will be vetted during the standard development process.		
Illinois Municipal Electric Agency	Yes	Simplification of reporting requirements should facilitate reliability.
Response: The DSR SAR DT thanks you for your comment.		
Duke Energy	Yes	We agree that additional clarity is needed regarding sabotage and disturbance reporting. Requirements should be tightened up and triggering events/thresholds of materiality need to be better defined.
Response: The DSR SAR DT thanks you for your comment. One of the FERC Order 693 directives for this project is: Define “sabotage” and provide guidance on triggering events that would cause an entity to report an event.		
MRO NERC Standards Review Subcommittee	Yes	
Colmac Clarion	Yes	
United Illuminating	Yes	

Organization	Yes or No	Question 1 Comment
PSEG Enterprise Group Inc Companies	Yes	
Northeast Power Coordinating Council	Yes	
IRC Standards Review Committee	Yes	
FirstEnergy	Yes	
Texas Regional Entity	Yes	
Edward C. Stein	Yes	
Exelon	Yes	
WECC	Yes	
ERCOT ISO	Yes	
Luminant Power	Yes	
ReliabilityFirst Corporation	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	

Organization	Yes or No	Question 1 Comment
PacifiCorp	Yes	
Oncor Electric Delivery	Yes	
Consolidated Edison Co. of New York, Inc.	Yes	
Manitoba Hydro	Yes	
AEP	Yes	
We Energies	Yes	
Consumers Energy Company	Yes	
NextEra Energy Resources, LLC	Yes	
Ameren	Yes	

2. Do you agree with the scope of the proposed SAR? If not, please explain what should be added or deleted to the proposed scope.

Summary Consideration: The majority of stakeholders agree with the scope of the SAR. Several stakeholders offered suggestions for items to include in the SAR, however the SAR DT believes that these comments may be too prescriptive to include with the SAR. The team feels that inclusion of these types of comments would prevent the Standard Drafting Team from having the ability to develop standard(s) based on stakeholder consensus. The SAR DT will forward these comments to the Standard Drafting Team for its consideration. Some of the comments received include:

1 The inclusion of specific definitions in the SAR (operating personnel, sabotage events, obligations): The SAR DT believes that this would be too prescriptive and believe that this should be addressed by the Standard Drafting Team.

2 Consolidate documents covering reporting requirements: The SAR DT agrees and suggests that the Standard Drafting Team investigate a "one-stop-shopping" solution for the various reports required, including the DOE report.

Organization	Yes or No	Question 2 Comment
Project 2007-02 Operating Personnel Comms Protocols SDT	No	The Operating Personnel Communication Protocols standard drafting team respectfully requests that the Sabotage Reporting SAR Drafting Team incorporate the following into your proposed SAR: "Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have procedures for the communication of information concerning the Cyber and Physical emergency alerts in accordance with the conditions described in "Attachment 1 Security Emergency Alerts." The Operating Personnel Communications Protocols Project 2007-02 was initiated to ensure that real time system operators use standardized communication protocols during normal and emergency operations to improve situational awareness and shorten response time. The SDT developed a new COM-003-1 Standard that has yet to be posted and is dependent upon revising at least two other standards (CIP-001 and TOP Standard). COM-003 contains requirements that specify: 1. Use of three-part communication; 2. English language; 3. Common time zone; 4. NATO alpha-numeric alphabet; 5. Mutually agreed line identifiers; 6. The use of pre-defined system condition terminology such as those contained in the RCWG Alert Level Guide and EOP-002-2.

Organization	Yes or No	Question 2 Comment
		This request is based on recent NERC Standards Committee direction to our team to incorporate the Reliability Coordinator Working Group's (RCWG) Alert Level Guide into a Standard. The consensus of our team is that a TOP Standard is the most appropriate location for the Transmission Emergency Alert language from the Guide as the energy emergency alert language is currently described in EOP-002-2. The RCWG Guide proposes the se of pre-defined system condition descriptions for use during emergencies for reliability related formation. This guide was developed in response to a Blackout Report recommendation. Our team placed the Transmission Emergency Alert language into a TOP standard. Since the Sabotage Reporting SAR DT intends to modify CIP-001, we seek your consent to incorporate the cyber and physical security alert language to comply with the wishes of the Standards Committee. We believe that the CIP-001 Standard is the most appropriate location for this language for the following reasons: • The levels of emergency conditions related to the cyber and physical security of the electric system is directly related to Critical Infrastructure Protection. • The current version of CIP-001 already requires the timely reporting of actual and suspected security emergency conditions and the use of pre-defined terminology supports the efficient haring of such information. The OPCP SDT includes the following text for the record. It is a proposed draft revision of CIP-001. **A. Introduction** 1. Title: Security Incidents 2. Number: CIP-001-2 3. Purpose: To ensure the recognition, communication and response to cyber and physical security incidents suspected or determined to be caused by sabotage. 4. Applicability 4.1. Reliability Coordinators. 4.2. Balancing Authorities. 4.3. Transmission Operators. 4.4. Generator Operators. 4.5. Load Serving Entities. 5. Effective Date: The standard is effective the first day of the first calendar quarter after applicable regulatory approvals (or the standard otherwise becomes effective the first day of the first calendar quarter after NERC OT adoption in those jurisdictions where regulatory approval is not required).

Organization	Yes or No	Question 2 Comment
		B. Requirements R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of security threats on its facilities and multi site security threats affecting larger portions of the Interconnection. R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning the physical and cyber security status of their facilities in accordance with the conditions described in Attachment 1-CIP-001-1. R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with security threat or incident response guidelines, including personnel to contact, for reporting security threats and incidents. R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances. **C. Measures** M1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement 1 M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements 2 and 3. M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited o procedures, policies, a letter of understanding, communication records, or other equivalent evidence that will be used to confirm that it has established communications contacts with the applicable, local FBI or CMP officials to communicate sabotage events (Requirement 4). **D. Compliance** 1. Compliance Monitoring Process 1.1. Compliance Enforcement Authority Regional Entity 1.2. Compliance Monitoring Period and Reset One or more of the following methods will be used to verify compliance: - Compliance Audits

Organization	Yes or No	Question 2 Comment
		- Self-Certifications - Spot Checking - Compliance Violation Investigations - Self-Reporting - Complaints 1.3. Data Retention The Transmission Operator, Transmission Owner, Balancing Authority, Reliability Coordinator, Generator Operator and Distribution Provider shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation: o The Transmission Operator, Transmission Owner, Balancing Authority, Reliability Coordinator, Generator Operator and Distribution Provider shall retain its current, in force document and any documents in force since the last compliance audit. o If a Transmission Operator, Transmission Owner, Balancing Authority, Reliability Coordinator, Generator Operator or Distribution Provider is found non-compliant, it shall keep information related to the non-compliance until found compliant. o The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records. 1.4. Additional Compliance Information None. 2. Levels of Non-Compliance: 2.1. Level 1: There shall be a separate Level 1 non-compliance, for every one of the following requirements that is in violation: 2.1.1 Does not have procedures for the recognition of and for making its operating personnel aware of sabotage events (R1). 2.1.2 Does not have procedures or guidelines for the communication of information concerning sabotage events to appropriate parties in the Interconnection (R2). 2.1.3 Has not established communications contacts, as specified in R4. 2.2. Level 2: Not applicable.

Organization	Yes or No	Question 2 Comment
		2.3. Level 3: Has not provided its operating personnel with sabotage response procedures or guidelines (R3). 2.4. Level 4:.Not applicable. E. Regional Differences None. Version History Version Date Action Change Tracking 0 April 1, 2005 Effective Date New 0 August 8, 2005 Removed "Proposed" from Effective ate Errata 1 November 1, 2006 Adopted by Board of Trustees Amended 1 April 4, 2007 Regulatory approval — Effective Date New 2 March 2009 Added SEA attachment and updates to Effective Date and compliance sections. New **Attachment 1-CIP-001-2 Physical Security Emergency Alerts** General requirements 1. Initiation by Reliability Coordinator. A Physical Security Emergency Alert may be initiated only by a Reliability Coordinator at: a. The Reliability Coordinator's own decision, b. By request from a Transmission Operator, c. By request from a Balancing Authority, or d. By request from federal, state, or cal Law Enforcement Officials. 2. Situations for initiating alert. An Alert may be initiated for the following reasons: a. A physical threat affecting a control center, grid or generator asset has been identified, or b. A physical attack affecting a control center, grid or generator asset has occurred or is imminent. 3. Notification. A Reliability Coordinator who initiates a Physical Security Emergency Alert shall notify all Transmission Operators and Balancing Authorities in its Reliability Area. The Reliability Coordinator shall also notify other Reliability Coordinators of the situation via the Reliability Coordinator Information System (RCIS) using the "CIP" category. Additionally, conference calls between Reliability Coordinators shall be held as necessary to communicate system conditions. The Reliability Coordinator shall also notify all Transmission Operators and Balancing Authorities in its Reliability Area and other Reliability Coordinators hen the alert has changed levels or ended.

Organization	Yes or No	Question 2 Comment
		Physical Security Emergency Alert Levels To ensure that all Reliability Coordinators clearly understand potential and actual Physical Security Emergency Alerts, NERC as established three levels of Security Emergency Alerts. The Reliability Coordinators will use these terms hen explaining security alerts to each other. The Reliability Coordinator may declare whatever alert level is necessary, and need not proceed through the alerts sequentially. 1. Alert 1 – "Control Center / Bulk Electric system asset threat identified" Circumstances: A credible threat of physical attack on a Bulk Electric System asset has been communicated to the Reliability Coordinator. No physical attack has occurred at this point. Determining the credibility of any threat is a subjective process, but the following factors should be considered: a. The nature and specificity of the threat, b. The timing of the threat, c. Mode of threat communication, and d. The criticality of the threatened asset. During a Physical Security Emergency Alert Level 1, Reliability Coordinators, Transmission Operators and Balancing Authorities shall have the following responsibilities: i. Notification: The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area. ii. Updating Status during the Physical Security Emergency Alert The declaring Entity shall update the reliability Coordinator of any changes in the situation until the Alert Level 1 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 2. Alert 2 – "Verified Physical attack at a single site" circumstances: A Reliability Coordinator, Transmission Operator, or Balancing Authority has identified a physical attack upon a control center, generator asset, or other bulk electric system asset. During a Physical Security Emergency Alert Level 2, Reliability Coordinators, Transmission Operators and Balancing Authorities shall have the following responsibilities: i. Notification: The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area. ii. Updating Status during the Physical Security Emergency Alert The Declaring Entity shall update the Reliability Coordinator of the situation a minimum of once per hour until the Alert Level 2 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 3. Alert 3– "Verified Physical attack at multiple sites" Circumstances: Multiple attacks have been confirmed on control centers, generator assets or other bulk electric system assets. A Reliability Coordinator shall declare Physical Security

Organization	Yes or No	Question 2 Comment
		Emergency Alert 3 whenever: a. A Transmission Operator or Balancing Authority reports multiple physical attacks on bulk electric system assets, b. Multiple Transmission Operators or Balancing authorities report one or more physical attacks on their bulk electric system assets. i. Notification: The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area. ii. Updating Status during the Physical Security Emergency Alert The declaring Entity(ies) shall update the Reliability Coordinator of the situation a minimum of once per hour until the Alert Level 3 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 4. Alert 0 – "Termination of Alert Level" Circumstances: The threat which prompted the Physical Security Emergency Alert Level has diminished or has been removed. i. Notification The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall notify all other Reliability Coordinators via the RCIS, and it shall also notify all Transmission Operators and Balancing Authorities in its Reliability Area that the Alert Level has been terminated. Cyber Security Emergency Alerts Cyber Assets – Those programmable electronic devices and communication networks, including hardware, software, and data, associated with bulk electric system assets. Cyber Security Incident - Any malicious act or suspicious event that compromises, or attempts to compromise, the electronic or physical security perimeter of a critical cyber asset or disrupts or attempts to disrupt the operation of a critical cyber asset. Critical Cyber Asset – Those cyber assets essential to the reliable operation of critical assets. Electronic Security Perimeter – The logical border surrounding the network or group of sub-networks to which the critical cyber assets are connected, and for which access is controlled. Physical Security Perimeter – The physical border surrounding computer rooms, telecommunications rooms, operations centers and other locations in which critical cyber assets are housed and for which access is controlled. General Requirements 1. Initiation - A Cyber Security Emergency Alert shall be initiated by: a. The Reliability Coordinator's analysis, b. By request from any NERC functional Model entity that Com-003-0 is applicable to.

Organization	Yes or No	Question 2 Comment
		c. By request from federal, state, or local Law Enforcement Officials. 2. Situations for initiating alert. An Alert shall be initiated for the following reasons: a. A cyber threat affecting a control center or bulk electric system asset has been identified, or b. A cyber attack affecting a control center or bulk electric system has occurred or is imminent. 3. Notification. An entity who initiates a Cyber Security Emergency Alert shall make notification as per the NERC Functional model or as Regional / local instruction. The Reliability Coordinator shall notify FBI local office, Electricity Sector Information Sharing Analysis Center ESISAC) and Department of Homeland Security. The Reliability Coordinator shall also notify as necessary other Reliability Coordinators of the situation via the Reliability Coordinator Information System (RCIS) sing the "CIP" category. The Reliability Coordinator shall notify all Transmission Operators and Balancing Authorities in its Reliability Area and other Reliability Coordinators when the alert has changed levels or ended. Cyber Security Emergency Alert Levels To ensure that all applicable entities clearly understand potential and actual Cyber Security Emergency Alerts, three levels of Security Emergency Alerts shall be sed. The Reliability Coordinators will use these terms when communicating security alerts to each other. When declaring the applicable alert level it is important to note that the applicable level can be determined without sequentially proceeding through levels. As an example given circumstances an Alert Level 3 could be called without previously being in an Alert Level 1 or Level 2 state. 1. Alert 1 – "Verified Control Center / Bulk Electric System Cyber Asset threat identified or imminent" What is "verified" - unknown or unauthorized access to a cyber device, unknown or unauthorized change to a cyber device (i,e., config file, /S, firmware change. 'Verified' could mean the elimination of a false positive in your security monitoring system. 'Verified' could also be the differentiation between malicious and non-malicious (ie human error, not following policy, etc) intent. What is a "threat" - A threat can be perceived as any action or event that occurs where the monitoring authority was not previously made aware that that action would occur. With flimsy change control or access controls, field staff or technical staff performing troubleshooting or other maintenance may access or change devices without notifying the monitoring entity. The monitoring entity would have to treat this as a threat and take appropriate action to either isolate that device from the rest of the system, notify appropriate authority, dispatch a crew, etc. Examples of threats - Over and above the examples above, another threat example could be a notification from DHS or other security agency that they have reason to believe a hack, virus or other cyber terrorism activity could occur. Also, noticing a distinct change in network traffic which could imply someone has intercepted your data and can manipulate

Organization	Yes or No	Question 2 Comment
		before sending it from the control room to the device being controlled or manipulating the data coming from the device before a controller seeing it and forcing them to perform an incorrect control event in reaction to erroneous data. Circumstances: A credible threat of Cyber attack on a Control Center or Bulk Electric System asset has been communicated to the Reliability Coordinator. No cyber attack has occurred t this point. Determining the credibility of any threat is a subjective process, but the following factors should be considered: a. The nature and specificity of the threat, b. The timing of the threat, c. Mode of threat communication, and d. The criticality of the threatened asset. During a Cyber Security Emergency Alert Level 1, applicable entities shall have the following responsibilities: i. Notification An entity who initiates a Cyber Security Emergency Alert Level 1 shall make notification as per the NERC Functional model r as Regional / local instruction. The Reliability Coordinator shall post the declaration of the alert level long with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area. The Reliability Coordinator shall also notify as necessary the BI local office, Electricity Sector Information Sharing Analysis Center (ESISAC) and Department of Homeland Security. ii. Updating Status during the Cyber Security Emergency Alert The declaring Entity shall update those applicable entities of any changes in the situation until the Alert Level 1 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 2. Alert 2 – "Verified Cyber attack on a Control Center or Bulk Electric System asset" Circumstances: An applicable entity has identified a cyber attack upon a control center or bulk electric system asset. During a Cyber Security Emergency Alert Level 2, applicable entities shall have the following responsibilities: i. Notification An entity who initiates a Cyber Security Emergency Alert Level 2 shall make notification as per the NERC Functional model or as Regional / cal instruction. The Reliability Coordinator responsible shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area. The Reliability Coordinator shall also notify the FBI local office, Electricity Sector Information Sharing Analysis Center (ESISAC) and Department of Homeland Security. ii. Updating Status during the Cyber Security Emergency Alert The declaring Entity shall provide updates of the situation a minimum of once per hour until the Alert Level 2 is terminated. The Reliability Coordinator shall update the RCIS as changes occur.

Organization	Yes or No	Question 2 Comment
		3. Alert 3 – "Verified Cyber attack at one or more Control Center or Bulk Electric System cyber asset" Circumstances: An applicable entity has identified a cyber attack upon a control center or bulk electric system asset and shall declare a Cyber Security Emergency Alert 3 whenever: a. A Transmission Operator or Balancing Authority reports one or more cyber attacks on bulk electric system that render an asset(s) unavailable. i. Notification An entity who initiates a Cyber Security Emergency Alert Level 3 shall make notification as per the NERC Functional model or as Regional / local instruction. The Reliability Coordinator shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities its Reliability Area. The Reliability Coordinator shall also notify the FBI local office, Electricity Sector Information Sharing Analysis Center (ESISAC) and Department of Homeland Security. ii. Updating Status during the Cyber Security Emergency Alert The declaring Entity(ies) shall provide an update of the situation minimum of once per hour until the Alert Level 3 is terminated. The Reliability Coordinator shall update he RCIS as changes occur. 4. Alert 0 – "Termination of Alert Level" Circumstances: The threat which prompted the Cyber Security Emergency Alert Level has diminished or has been removed. i. Notification An entity who initiates a Cyber Security Emergency Alert shall make notification as per the NERC Functional model or as Regional / local instruction when situation has diminished or returned to normal. The Reliability Coordinator shall notify all other Reliability Coordinators via the RCIS, and it shall also notify all Transmission Operators and Balancing Authorities in its Reliability Area that the Alert Level has been terminated.
Response: The DSR SAR DT thanks you for your comment. The standards in this Project 2009-01 SAR are designed to specify reporting requirements for disturbance and sabotage events. The DSR SAR DT believes that the suggested additions go beyond the intended scope of the revisions to the standards, and do not feel that communications protocols belong in these reporting standards. The proposed revisions and Alert Levels are real-time requirements, and the team feels that these would be more appropriately addressed in an IRO or COM standard.		
Northeast Power Coordinating Council	No	The SAR needs to be more specific in defining its objectives. CIP-001Requirement R1 currently states: R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SDT needs to include the following objectives: 1. Develop clear definitions for the terms "operating personnel" and "sabotage events." The definition of "operating personnel," should be clarified and limited to staff at BES facilities. Operating personnel should report only those events

Organization	Yes or No	Question 2 Comment
		which meet a clear, recognizable threshold as reportable potential sabotage events. There should be a consistent continent-wide list of examples or typical reportable and non-reportable events to help guide operating personnel. The term "sabotage event" needs to be defined. Clarification is required regarding when the determination of a sabotage event is made, e.g., upon first observation (requiring operating personnel be educated in discerning sabotage events), or upon later investigation by trained security personnel and law enforcement individuals. The terms potential or suspected sabotage event for reporting purposes should be clarified or defined. 2. Define the obligations of Registered Entity operating personnel - who are required to be aware of such "sabotage events," e.g., who, what, where, when, why and how, and what they are to do in response to this awareness. The SDT should clarify the use of the term "aware" in the standard. "Aware" can be interpreted in accordance with its largely passive, dictionary-based meaning, where being "aware" simply means knowing about something, such as a sabotage event. Alternatively, the Reliability Standard meaning of "aware" could refer to more active wording, involving more than mere awareness, e.g., "alert and quick to respond," pointing to and requiring a specific affirmative response, i.e., reporting to the appropriate systems, governmental agencies, and regulatory bodies. EOP-004 - The SDT needs to work on the following areas. 1. NERC reporting needs to be clarified. For example, Attachment 1 paragraph 6c states: Introduction "The entity on whose system a reportable disturbance occurs shall notify NERC ... 6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in: c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance - The sense of Attachment 1 is internally inconsistent between the introduction ("occurs") and the required actions in 6c (could have resulted in a system disturbance). The initial intent appears to be only to report actual system disturbances. Yet, paragraph 6c adds the phrase "or could have resulted in" a potential system disturbance. This inconsistency should be clarified.
Response: The DSR SAR DT thanks you for your comment. **CIP-001: The inclusion of specific definitions in the SAR as you suggest (operating personnel, sabotage events, obligations) are too prescriptive and could prevent better definitions from being developed during the Standards Development stage of the project. The team will pass your comments along to the standard drafting team for its consideration.** **EOP-004: Your comment addresses specific revisions to the standard. The team will pass your comments along to the standard drafting team for its consideration.**		
Kansas City Power & Light	No	Agree with the scope of the SAR except for the applicable entities. See response to question #4.
Response: The DSR SAR DT thanks you for your comment. Please see response to Q4.		

Organization	Yes or No	Question 2 Comment
MRO NERC Standards Review Subcommittee	No	The MRO NSRS would like to keep the references to the DOE reporting form.
Response: The DSR SAR DT thanks you for your comment. The DSR SAR DT understands your comment to indicate that you would like to see a "one stop" reporting form for disturbances and sabotage events. The DSR SAR DT agrees with you and will pass this comment along to the standard drafting team for its consideration in developing the standard(s).		
Lands Energy Consulting	No	I would like to see the SAR expanded to cover the issues I mentioned in my prior comment. Otherwise, the scope of the SAR looks fine to me.
Response: The DSR SAR DT thanks you for your comment. Please see response to Q1 on other issues.		
Bonneville Power Administration	No	Leave as is, all requirements for reporting are now covered. A common definition of sabotage is already widely available.
Response: The DSR SAR DT thanks you for your comment. Most stakeholders desire more clarity around the definition of sabotage as well as examples of what is and is not sabotage as opposed to vandalism.		
Cowlitz County PUD	No	Added to the scope: For EOP-004 add a provision for a reporting flow rather than everything going to the RE and NERC. That is something going like the DP and TOP reports to the BA, the BA to the RE, and the RE to NERC. This would allow for multiple related reports to be combined into a single coherent report as the reporting goes up the chain. For CIP-001 consider reporting flow as above with local law enforcement notification. Let an upper entity in the reporting chain decide when to contact Federal Agencies such as the BA or the RC.
Response: The DSR SAR DT thanks you for your comment. The DSR SAR DT feels that your comments are "how" comments that should be addressed in standard drafting stage. The team will pass this comment along to the standard drafting team for its consideration.		
Reliant Energy	No	I think Generator operators should be excluded except to provide requested information from the System Operator or Reliability coordinator.
Response: The DSR SAR DT thanks you for your comment. Other commenters have questioned the ability of Generator Operators to have a wide area view and to be able to analyze disturbances on the system. The team agrees that generators may not have a wide area view and the capability to analyze system events. The final wording of the requirements (i.e. reporting vs. data provision) developed by the Standard Drafting Team will		

Organization	Yes or No	Question 2 Comment
determine the applicability to GOPs. The team will pass your comment on to the Standard Drafting Team for its consideration.		
ERCOT ISO	No	The scope should be modified to provide for a different treatment of reporting requirements that are administrative in nature, or that are after-the-fact (thus cannot impact reliability unless analysis and follow-up is not performed; even then, the impact would be at some future time). Reporting requirements which are of the nature to assist in identification of system concerns or which serve to prevent or mitigate on-going system problems (including, but not limited to, actual or attempted sabotage activity) should remain in standards, but should be separate and apart from the administrative reporting.
Response: The DSR SAR DT thanks you for your comment. The team concurs with the concepts on reporting as you suggest, however the team does not feel that this should be addressed in the SAR. The team suggests that this is more appropriately addressed in the standard drafting process, and the team will pass your comment along to the standard drafting team for its consideration in drafting the standard.		
MidAmerican Energy	No	See the responses to questions 1 and 5.
Response: The DSR SAR DT thanks you for your comment. Please see responses to Q1 and Q5.		
We Energies	No	Consider including the sabotage issues in IRO-014-1 R 1.1.1 footnote 1 and TOP-005-1 Attachment 1, 2.9.
Response: The DSR SAR DT thanks you for your comment. The team has added references to these two standards in the "Related Standards" section for the SAR.		
NextEra Energy Resources, LLC	No	The scope of the SAR should not include Generator Operators.
Response: The DSR SAR DT thanks you for your comment. Other commenters have questioned the ability of Generator Operators to have a wide area view and to be able to analyze disturbances on the system. The team agrees that generators may not have a wide area view and the capability to analyze system events. The final wording of the requirements (i.e. reporting vs. data provision) developed by the Standard Drafting Team will determine the applicability to GOPs. The team will pass your comment on to the Standards Drafting Team for its consideration.		
Progress Energy	No	No. If this SAR moves forward other standards may need to be considered. For example, in CIP-008, incident reporting for cyber incidents leads to filing of the OE-417 form.
Response: The DSR SAR DT thanks you for your comment. The SAR states "Specific references to the DOE form need to be eliminated." **This will remove the linkage that you identify between CIP-001 and CIP-008. There is also a directive from FERC Order 693 in the SAR that states:**		

Organization	Yes or No	Question 2 Comment
Consider FirstEnergy's suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality. **This allows the standard drafting team to delineate physical and cyber assets. The DSR SAR DT also notes that CIP-008 might be a good framework for drafting the standard requirements pertaining to sabotage and disturbance reporting of physical assets.**		
Ameren	No	There seems to be an open slate including the following language in the scope. The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards (see tables for each standard at the end of this SAR for more detailed information). The unnamed improvements should be limited to those requirements that relate only to Disturbance and Sabotage NOT a general wish list (or witch hunt).
Response: The DSR SAR DT thanks you for your comment. The passage that you mention is the intent of each SAR and is a stock statement that is included in almost every SAR. The SAR is limited to the standards listed in the SAR which is approved by the NERC SC to move to standards development.		
Consolidated Edison Co. of New York, Inc.	No	GENERAL CECONY and ORU support the general objectives of the SAR to merge existing standards CIP-001-1 Sabotage Reporting and EOP-004-1 Disturbance Reporting to improve clarity and remove redundancy. However, the SAR needs to be more specific in defining its objectives. CIP-001Requirement R1 currently states: R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SDT needs to include the following objectives: 1. Develop clear definitions for the terms operating personnel and sabotage events. The definition of operating personnel, should be clarified and limited to staff at BES facilities. Operating personnel should report only those events which meet a clear, recognizable threshold as reportable potential sabotage events. There should be a consistent continent-wide list of examples or typical reportable and non-reportable events to help guide operating personnel. The term sabotage event needs to be defined. Clarification is required regarding when the determination of a sabotage event is made, e.g., upon first observation (requiring operating personnel be educated in discerning sabotage events), or upon later investigation by trained security personnel and law enforcement individuals. The terms potential or suspected sabotage event for reporting purposes should be clarified or defined. 2. Define the obligations of Registered Entity operating personnel - who are required to be aware of such sabotage events, e.g., who, what, where, when, why and how, and what they are to do in response to this awareness. The SDT should clarify the use of the term aware in the standard. Aware can be interpreted in accordance with its largely passive, dictionary-

Organization	Yes or No	Question 2 Comment
		based meaning, where being aware simply means knowing about something, such as a sabotage event. Alternatively, the Reliability Standard meaning of aware could refer to more active wording, involving more than mere awareness, e.g., alert and quick to respond, pointing to and requiring a specific affirmative response, i.e., reporting to the appropriate systems, governmental agencies, and regulatory bodies. EOP-004 - The SDT needs to work on the following areas. 1. NERC reporting needs to be clarified. For example, Attachment 1 paragraph 6c states: Introduction The entity on whose system a reportable disturbance occurs shall notify NERC ... 6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in: ?c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance. The sense of Attachment 1 is internally inconsistent between the introduction (occurs) and the required actions in 6c (could have resulted in a system disturbance). The initial intent appears to be only to report actual system disturbances. Yet, paragraph 6c adds the phrase or could have resulted in a potential system disturbance. This inconsistency should be clarified.
Response: The DSR SAR DT thanks you for your comment. **CIP-001: The inclusion of specific definitions in the SAR as you suggest (operating personnel, sabotage events, obligations) are too prescriptive and could prevent better definitions from being developed during the standard drafting stage of the project. The team will pass your comments along to the standard drafting team for its consideration.** **EOP-004: Your comment addresses specific revisions to the standard. The team will pass your comments along to the standard drafting team for its consideration.**		
Georgia System Operations Corp.	No	The scope of the SAR should be to move all requirements to report to NERC or Regional Entities out of the Requirements section of all Reliability Standards to elsewhere. This does not include reporting, communicating, or coordinating between reliability entities. The NERC/Region reporting requirements could be consolidated in another document and referenced in the Supporting References section of the Reliability Standards. The deadlines for reporting should be changed to realistic timeframes that do not interfere with operating the BES or responding to incidents yet still allow NERC and the Regions to accomplish their missions.
Response: The DSR SAR DT thanks you for your comment. The team does not feel that this should be addressed explicitly in the SAR, but suggests that this is more appropriately addressed in the standard drafting stage for full industry vetting of the concepts. The team will pass your comment along to the standard drafting team for its consideration in developing the standard.		

Organization	Yes or No	Question 2 Comment
AEP	No	Sabotage is a term of intent that is often determined after the fact by the registered entity and/or law enforcement officials. In fact, it is often difficult to determine in real-time the intent of a suspicious event. We would suggest that suspicious events become reportable at the point that the event is determined to have had sabotage intent. The entities should have a methodology to collect evidence, to have the evidence analyzed, and to report those events that are determined to have had the intent of sabotage.
Response: The DSR SAR DT thanks you for your comment. The team concurs that it is difficult to determine sabotage in real-time. The teamdoes not feel that this should be addressed explicitly in the SAR and suggests that this is more appropriately addressed in the standard drafting stage for full industry vetting of the concepts. The team will pass your comment along to the standard drafting team for its consideration in developing the standard.		
Duke Energy	No	While we agree with the need for clarity in sabotage and disturbance reporting, we believe that the Standards Drafting Team should carefully consider whether there is a reliability-related need for each requirement. Some disturbance reporting requirements are triggered not just to assist in real-time reliability but also to identify lessons-learned opportunities. If disturbance and sabotage reporting continue to be reliability standards, we believe that all linkages to lessons-learned/improvements need to be stripped out. We have other forums to identify lessons-learned opportunities and to follow-up on those opportunities. Also, requirements to report possible non-compliances should be eliminated. We strongly support voluntary self-reporting, but not mandatory self-reporting.
Response: The DSR SAR DT thanks you for your comment. The team concurs that each requirement should be evaluated for its reliability need, and the team will pass your comment along to the standard drafting team for its consideration in the drafting stage of the standard.		
FirstEnergy	Yes	We agree with the scope but would also like to see the following considered: 1. References to the DOE reporting process in EOP-004 need to be revised. They currently refer to the old EIA form. 2. Besides "sabotage", it may be helpful to clearly define "vandalism". It is vaguely written in the standards. Also, the process of "public appeals" for the DOE reportable requirements needs to be more clearly defined. 3. Consolidate documents covering reporting requirements. There are currently several documents that require reporting (EOP-004, CIP-001, DOE oe-417, and NERC's Security Guideline for the Electricity Sector: Threat and Incident Reporting). NERC also has the "Bulk Power System Disturbance Classification Scale" that does not completely align with all the reporting requirements. Therefore we recommend keeping this as simple as possible by combining all the reporting requirements into one standard. It would be beneficial to not require operators to have to go to 4 different documents to determine what to report on.
Response: The DSR SAR DT thanks you for your comment.		

Organization	Yes or No	Question 2 Comment
The Brief Description of the SAR states: Specific references to the DOE form need to be eliminated. **The team will pass your comment along to the standard drafting team for its consideration.** **The team concurs that this should be considered in drafting the standards. The team will pass your comment along to the standard drafting team for its consideration.**		
Exelon	Yes	Consolidation of redundant requirements and clarifications of difficult to follow / interpret standards should be a high priority at NERC.
Response: The DSR SAR DT thanks you for your comment. One of the FERC directives for CIP-001 is: Explore ways to reduce redundant reporting, including central coordination of sabotage reports and a uniform reporting format.		
Electric Market Policy	Yes	
SERC OC Standards Review Group	Yes	
PSEG Enterprise Group Inc Companies	Yes	
IRC Standards Review Committee	Yes	
Pepco Holdings, Inc. - Affiliates	Yes	
Calpine Corporation	Yes	
Covanta	Yes	
Colmac Clarion	Yes	

Organization	Yes or No	Question 2 Comment
United Illuminating	Yes	
Texas Regional Entity	Yes	
Edward C. Stein	Yes	
WECC	Yes	
Luminant Power	Yes	
ReliabilityFirst Corporation	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	
PacifiCorp	Yes	
Oncor Electric Delivery	Yes	
Illinois Municipal Electric Agency	Yes	
Manitoba Hydro	Yes	
Consumers Energy Company	Yes	

3. Are you aware of any associated business practices that we should consider with this SAR? If yes, please explain in the comment area.

Summary Consideration: Stakeholders did not identify any associated business practices for consideration under the SAR. One stakeholder identified a related standard that references multi-site sabotage. The team has included a reference to TOP-005, section 2.9 (Appendix 1) in the SAR under Related Standards. Two stakeholders suggested that Business Practices should not be considered in a standard. The SAR DT notes that standard development projects must not invalidate business practices that are already in place. This question is required to be asked per the Standard Drafting Team Guidelines (page 8) and aids in coordination with North American Energy Standards Board. One stakeholder suggested a "one-stop-shopping" solution. The SAR DT agrees with this approach and will forward this comment to the Standard Drafting Team.

Organization	Yes or No	Question 3 Comment
MRO NERC Standards Review Subcommittee	Yes	
Luminant Power	Yes	The SAR drafting team should include in the SAR scope a review of the NRC sabotage and event reporting requirements to ensure there are no overlapping or conflicting requirements between NERC, FERC, and the NRC. The SAR scope should include a review of the CIP Cyber Security Standards and coordination with the CIP SDT to ensure that cyber sabotage reporting definitions are in concert, and ensure that cyber sabotage reporting requirements are not duplicated in multiple standards.
Response: The DSR SAR DT thanks you for your comment. The team notes that your comments relate directly to potential revisions of the standard itself. Part of this SAR is to eliminate redundancies as well. The team will pass your comments along to the Standards Drafting Team for its consideration. This project is designed to address physical asset reporting, not cyber assets. Therefore, cyber assets will not be included in this SAR.		
MidAmerican Energy	Yes	Attachment TOP-005, section 2.9 speaks of "Multi-site sabotage" with no definition. The ES-ISAC 2008 advisory is an associated standard or practice on sabotage. All references to sabotage should be eliminated or retired except for CIP-001.
Response: The DSR SAR DT thanks you for your comment. The team has included a reference to TOP-005, section 2.9 (Appendix 1) in the SAR under Related Standards. Project 2009-01 is designed to address physical asset reporting, not cyber asset sabotage and disturbance reporting. The standard drafting team will remove redundancies per the SAR.		

Organization	Yes or No	Question 3 Comment
Illinois Municipal Electric Agency	Yes	A one-stop reporting tool/site would facilitate efficient reporting and compliance; e.g., further development of the ES-ISAC/CIPIS to include all reportable categories and automatic notification of required parties. A single report form would be best.
Response: The DSR SAR DT thanks you for your comment. The team agrees with your suggestion and will pass this along to the Standard Drafting Team for its consideration in developing standards.		
AEP	Yes	The current reporting process necessitates multiple reports be sent to multiple parties, which is inefficient and may, inadvertently, result in alignment issues between the separate reports. We would recommend that a single report that combines NERC (CIPIS) and NERC ESISAC information be provided to NERC (CIPIS) that is systematically (programmatically) forwarded to all necessary entities. Further, updates to incidents would also go through NERC with the same electronic processing. Currently, we are not aware of a formal method to report incidents to the FBI, which should be also included in the distribution. The current reporting mechanism to the FBI JTTF is by telephone and the NERC platform described would provide more consistent reporting.
Response: The DSR SAR DT thanks you for your comment. The team agrees with your suggestion and will pass this along to the Standard Drafting Team for its consideration in developing standards. This project is designed to address physical asset reporting, not cyber assets.		
Progress Energy	Yes	Yes. If this SAR moves forward other practices such as those required by CIP-008 (cyber incident reporting via the OE-417 form) may need to be considered.
Response: The DSR SAR DT thanks you for your comment. The SAR states "Specific references to the DOE form need to be eliminated."**This will remove the linkage that you identify between CIP-001 and CIP-008. There is also a directive from FERC Order 693 in the SAR that states:** **Consider FirstEnergy's suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality.** **This allows the standard drafting team to delineate physical and cyber assets. The DSR SAR DT also notes that the general layout and sequencing of requirements in CIP-008 might be a good framework for drafting the standard requirements pertaining to sabotage and disturbance reporting of physical assets.**		
Exelon	No	We are not sure what this question means. Who's Associated Business practices, NERC, Applicable Entities in the Standard, our business practices?
Response: The DSR SAR DT thanks you for your comment. "Business practices" refers to any business practice of any stakeholder (e.g. North American Energy Standards Board business practices).		

Organization	Yes or No	Question 3 Comment
SERC OC Standards Review Group	No	Business practices should not be considered in a standard.
Response: The DSR SAR DT thanks you for your comment. Standard development projects must not invalidate business practices that are already in place. This question is required to be asked per the Standard Drafting Team Guidelines (page 8) and aids in coordination with North American Energy Standards Board.		
FirstEnergy	No	Although we are not aware of any NAESB business practices that need to be reviewed in conjunction with these proposed revisions, the SDT should consider reviewing current RTO procedures and practices that may require the need for variances in the revised standards.
Response: The DSR SAR DT thanks you for your comment. The Standard Drafting Team will review any procedures or practices that are identified for potential variances.		
Georgia System Operations Corp.	No	Business practices should not be part of a Reliability Standard. Neither should NERC/Region reporting requirements (except for reporting of threats to physical or cyber security). NERC may need to take some action in the case of threats but does not and cannot take any operational action for most of the reporting requirements that are presently in the Requirements section of the Reliability Standards.
Response: The DSR SAR DT thanks you for your comment. Standard development projects must not invalidate business practices that are already in place. This question is required to be asked per the Standard Drafting Team Guidelines (page 8) and aids in coordination with North American Energy Standards Board. The team disagrees with your assertion about reporting. Instances of sabotage are often not identified until after the fact, and these should be reported to alert other entities of the sabotage and for "lessons learned".		
PSEG Enterprise Group Inc Companies	No	
Northeast Power Coordinating Council	No	
Kansas City Power & Light	No	
IRC Standards Review Committee	No	

Organization	Yes or No	Question 3 Comment
Pepco Holdings, Inc. - Affiliates	No	
Electric Market Policy	No	
Bonneville Power Administration	No	
Lands Energy Consulting	No	
Covanta	No	
Colmac Clarion	No	
Cowlitz County PUD	No	
United Illuminating	No	
Reliant Energy	No	
Texas Regional Entity	No	
Edward C. Stein	No	
PacifiCorp	No	
WECC	No	
ERCOT ISO	No	
ReliabilityFirst Corporation	No	

Organization	Yes or No	Question 3 Comment
Brazos Electric Power Cooperative, Inc.	No	
Oncor Electric Delivery	No	
Consolidated Edison Co. of New York, Inc.	No	
Manitoba Hydro	No	
Duke Energy	No	
We Energies	No	
Consumers Energy Company	No	
NextEra Energy Resources, LLC	No	
Ameren	No	

4. CIP-001-1 applies to the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, and the Load-serving Entity. EOP-004-1 applies to the same entities, plus the Regional Reliability Organization. Do you agree with the applicability of the existing CIP-001-1 and the existing EOP-004-1? If no, please identify what you believe should be modified.

Summary Consideration: Many stakeholders had comments regarding applicability of the two standards. The three main concerns were:

1 Regional Reliability Organization applicability: Many commenters do not feel the RRO should be in the standards. The DSR SAR DT concurs and notes that the SAR states that "EOP-004 has some 'fill-in-the-blank' components to eliminate". This will remove the RRO from applicability.

2 Load-Serving Entity/Distribution Provider: Many stakeholders do not feel that the standards should be applicable to LSEs, but should apply to Distribution Providers. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team added DP to the applicability of the standard as the Standard Drafting team may have a need to include them in the standard(s). The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements through the Standard Development Process.

3 Transmission Owner/Generator Owner: Many stakeholders have indicated a need to include the TO as an applicable entity. A couple of those would also include the GO. The SAR DT discussed the addition of both the TO and GO. The team has a concern that there will be duplication of requirements between the TO/TOP and GO/GOP if the TO and GO are added to the SAR. That being said, the team added the TO and GO to the applicability of the SAR so that the Standard Drafting team may consider these entities for applicability. The applicability of requirements will ultimately be determined by the Standard Drafting Team as it develops the requirements through the Standard Development Process.

Organization	Yes or No	Question 4 Comment
SERC OC Standards Review Group	No	The EOP-004-1 standard should not apply to the RRO.
Response: The DSR SAR DT thanks you for your comment. The team concurs and notes that the SAR states: EOP-004 has some 'fill-in-the-blank' components to eliminate. This will remove the RRO from applicability.		
Kansas City Power &	No	Do not agree Load Serving Entities need to continue to be included for sabotage. According the NERC Functional Model,

Organization	Yes or No	Question 4 Comment
Light		an LSE provides for estimating customer load and provides for the acquisition of transmission and energy to meet customer load demand. An LSE has no real impact on maintaining the reliability of electric network short of their planning function. Unfortunately, an LSE needs to be included for disturbance reporting to the DOE under certain conditions for loss of customer load. This may be a reason to maintain a separation of CIP-001 and EOP-004 so as not to unnecessarily include an LSE when it is not needed.
Response: The DSR SAR DT thanks you for your comment. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team added DP to the applicability of the standard as the Standard Drafting team may have a need to include them in the standard(s). The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements through the standard drafting stage of the process. The team will pass your comment along to the Standard Drafting Team for its consideration.		
IRC Standards Review Committee	No	We agree with the applicability of CIP-001-1 but question the need to include the RRO in EOP-004-1. Requirement R1 of EOP-004-1 can be turned into an industry developed and approved procedural requirement with details included in an appendix; whereas R5 can be changed to a requirement for the responsible entities to act on recommendations and to self-report compliance. Tracking and reviewing status of recommendation do not need to be performed by the RRO, or any entity for that matter, if a self-reporting mechanism is developed.
Response: The DSR SAR DT thanks you for your comment. The team concurs and notes that the SAR states: EOP-004 has some 'fill-in-the-blank' components to eliminate. This will remove the RRO from applicability.		
Pepco Holdings, Inc. - Affiliates	No	As specified in Order 693, Regional Reliability Organizations are not to be assigned applicability. The revised standard(s) should contain the reporting form either directly or by reference and the RRO should be removed. The other EOP-004 requirements for RROs are now considered normal monitoring activities of the Regional Entities.
Response: The DSR SAR DT thanks you for your comment. The team concurs and notes that the SAR states: EOP-004 has some 'fill-in-the-blank' components to eliminate. This will remove the RRO from applicability.		
FirstEnergy	No	The Regional Reliability Organization should be removed from the applicability of EOP-004-1. Any report they receive would be from the other entities listed. For consistency, the entities should report to the appropriate law enforcement agency. A report to the Reliability Entity should also be made for that entities information only.
Response: The DSR SAR DT thanks you for your comment. The team concurs and notes that the SAR states: EOP-004 has some 'fill-in-the-blank' components to eliminate. This will remove the RRO from applicability.		
Electric Market Policy	No	Applicability should not apply to LSE unless they have physical assets. If they do not have such assets, they are unable to

Organization	Yes or No	Question 4 Comment
		determine how many customers are out, how much load was lost or the duration of an outage. We continue to question the need for the LSE entity in reliability standards. End use customer load is either connected to transmission or distribution facilities. So, the applicable planner has to plan for that load when designing its facilities or the load will not have reliable service. To the extent that energy and capacity for that load is supplied by an entity other than the TO or DP, the TO or DP should have interconnection requirements that compel the supplier to provide any and all data necessary to meet the requirements of reliability standards.
Response: The DSR SAR DT thanks you for your comment. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the standard as the Standard Drafting team may have a need to include them in the standard(s). The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting stage of the process. The team will pass your comment along to the Standard Drafting Team for its consideration.		
MRO NERC Standards Review Subcommittee	No	As FERC has directed, the RRO should be removed since they are not owners or operators of the BES.
Response: The DSR SAR DT thanks you for your comment. The team concurs and notes that the SAR states: EOP-004 has some 'fill-in-the-blank' components to eliminate. **This will remove the RRO from applicability.**		
Lands Energy Consulting	No	CIP-001-1 - Yes. In many cases, the staff of an LSE embedded in another entity's BA/TOP area is more likely to discover an act of sabotage directed toward a BA/TOP-owned facility that could affect the BES than the asset owner. This is because the LSE likely has more operating staff in the area. I have included a requirement in my clients' Sabotage Identification and Reporting Procedures that the client treat acts of sabotage to a third party's system discovered by client employees as though the act was directed toward client facilities. EOP-004-1 - As mentioned before, I would eliminate the LSE from the applicability list and leave the responsibility for disturbance reporting and response to the TOP/BA. However, I would retain a responsibility for the LSEs to cooperate (when requested) with any disturbance investigation.
Response: The DSR SAR DT thanks you for your comment. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the standard as the Standard Drafting team may have a need to include them in the standard(s). The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting stage of the process. The team will pass your comment along to the Standard Drafting Team for its consideration.		
Calpine Corporation	No	The reporting requirements of EOP - 004 are needed for the RC, BA, LSE and the GOP that operates or controls generation in a system as defined by NERC. (System - A combination of generation, transmission, and distribution components). A disturbance is described as an unplanned event that produces and abnormal system condition, any

Organization	Yes or No	Question 4 Comment
		perturbation to the electric system, and the unexpected change in ACE that is caused by the sudden failure of generation or interruption of load. The GOP operating/controlling generation within a system has the ability to analyze system conditions to determine if reporting is necessary. A NERC registered GOP that is a merchant generator within another company's system does not have the ability for a wide area view and cannot analyze system conditions beyond the interconnection point of the facility. Moreover, in most cases the reporting requirements outlined in the Interconnection Reliability Operating Limits and Preliminary Disturbance Report do not apply to the merchant generator that is not a generation only BA. The applicability of the standard does encompass the true merchant generation entities required to register as GOP. Similarly, the OE-417 table 1 reporting requirements generally do not apply to a true merchant generating entity that is required to register as a GOP.
Response: The DSR SAR DT thanks you for your comment. The team agrees that generators may not have a wide area view and the capability to analyze events. The final wording of the requirements developed by the Standard Drafting Team will determine the applicability. The team will pass your comment on to the Standards Drafting Team for its consideration. The SAR calls for the removal of references to the DOE form OE-417.		
Cowlitz County PUD	No	Replace LSE with DP, and the Regional Reliability Organization with the Regional Entity.
Response: The DSR SAR DT thanks you for your comment. The team has added DP to the applicability of the SAR. The SAR calls for removing the fill-in-the-blank standard elements which will remove the RRO.		
United Illuminating	No	Add Distribution Provider
Response: The DSR SAR DT thanks you for your comment. The team has added DP to the applicability of the SAR.		
Reliant Energy	No	EOOP-004-1 should exclude the generator operator from disturbance reporting except providing the system operator or reliability coordinator with appropriate unit operation information upon request. Acts of sabotage should be identified clearly and reported to the indicated authorities.
Response: The DSR SAR DT thanks you for your comment. Other commenters have questioned the ability of Generator Operators to have a wide area view and to be able to analyze disturbances on the system. The team agrees that generators may not have a wide area view and the capability to analyze system events. The final wording of the requirements (i.e. reporting vs. data provision) developed by the Standard Drafting Team will determine the applicability to GOPs. The team will pass your comment on to the Standards Drafting Team for its consideration.		
Texas Regional Entity	No	Add GO and TO to the list of applicability. The intent of CIP-001-1 when it was first written was to have the proper and most likely entities associated directly with operations to be the ones to begin the reporting process in the case of sabotage on the system. In the ERCOT Region and other regions in the US, the GOP may not be physically located at the site. The GOP is often removed from the minute-by-minute responsibilities of plant operations and, therefore, may be less

Organization	Yes or No	Question 4 Comment
		able to react to physical sabotage at the location/plant/facility in a timely manner. The concern is that, in the case of an actual sabotage event, the failure to report to the appropriate authorities in a timely manner may jeopardize the reliability of the BPS. Therefore, the Generator Owner (GO) should be added to the list of applicability for CIP-001-1, because it is the GO that is more likely to be on location at the generation site and thus aware of sabotage when it first occurs. This would disallow for any possible communication gap and put responsibility on all of the appropriate entities to report such an event. Additionally, and for the same reasons as adding the GO, the Transmission Owner (TO) should also be added to the list of applicability for reporting sabotage on its facilities.
Response: The DSR SAR DT thanks you for your comment. The SAR DT discussed the addition of the TO and GO. The team was concerned that there may be duplication of requirements between the TO/TOP and GO/GOP if the TO and GO are added to the SAR. That being said, the team added the TO and GO to the applicability of the SAR so that the Standard Drafting team may consider these entities for applicability. The applicability of requirements will ultimately be determined by the Standard Drafting Team as it develops the requirements through the standard drafting Process. The team will pass your comment along to the Standard Drafting Team for its consideration concerning applicability.		
NextEra Energy Resources, LLC	No	The scope of the proposed SAR should not include the Generator Operator.
Response: The DSR SAR DT thanks you for your comment. Other commenters have questioned the ability of Generator Operators to have a wide area view and to be able to analyze disturbances on the system. The team agrees that generators may not have a wide area view and the capability to analyze system events. The final wording of the requirements (i.e. reporting vs. data provision) developed by the Standard Drafting Team will determine the applicability to GOPs. The team will pass your comment on to the Standards Drafting Team for its consideration.		
Exelon	No	CIP-001, remove LSE's from the standard for the reasons identified in the FERC LSE order. Ad TO and DP. EOP-004, remove LSE's from the standard for the reasons identified in the FERC LSE order. Remove RRO's, they are not a user, owner, operator of the BES. Add DP or TO. Consider conditional applicability as in the UFLS standards, " the TO or DP who performs the functions specified in the standard..."
Response: The DSR SAR DT thanks you for your comment. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the SAR. The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting stage of the process. The SAR DT discussed the addition of the TO. The team is concerned that there may be duplication of requirements between the TO/TOP if the TO is added to the SAR. That being said, the team added the TO and GO to the applicability of the SAR so that the Standard Drafting team may consider these entities for applicability. The applicability of requirements will ultimately be determined by the Standard Drafting Team as it develops the requirements through the standard drafting Process. The SAR calls for elimination of fill in the blanks elements, which will remove the RRO from the standard. The team will pass your comment along to the Standard Drafting Team for its consideration concerning conditional applicability.		

Organization	Yes or No	Question 4 Comment
ERCOT ISO	No	The Regional Reliability Organization is not a registered Functional Entity in the NERC registry. The applicability must be revised to more appropriately assign the requirements to registered functional entities. Also, the industry needs to recognize that there are other resources than generation for which the operators need to be included. Perhaps a demand-side resource should have a resource operator. This particular SAR may not be the appropriate venue for this, but control of resources which can be used to mitigate sabotage events or disturbance events may need to be addressed.
Response: The DSR SAR DT thanks you for your comment. The SAR calls for elimination of fill-in-the-blank elements, which will remove the RRO from the standard. The applicability of requirements will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting stage of the process. The team will pass your comment along to the Standard Drafting Team for its consideration concerning conditional applicability. This SAR is for reporting rather than control actions as you mention.		
Brazos Electric Power Cooperative, Inc.	No	May need to consider adding Transmission Owner. I don't see a need for the RRO to be included as they are not owner/operators of grid facilities.
Response: The DSR SAR DT thanks you for your comment. The SAR DT discussed the addition of the TO. The team is concerned that there may be duplication of requirements between the TO/TOP if the TO is added to the SAR. That being said, the TO has been added to the applicability of the SAR so that the Standard Drafting team may consider these entities for applicability. The applicability of requirements will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting stage of the process. The SAR calls for elimination of fill in the blank elements, which will remove the RRO from the standard. The team will pass your comment along to the Standard Drafting Team for its consideration concerning conditional applicability.		
PacifiCorp	No	LSE's don't generally own/operate facilities/systems that would experience a logical or physical sabotage event.
Response: The DSR SAR DT thanks you for your comment. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the SAR. The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting stage of the process.		
MidAmerican Energy	No	MidAmerican Energy believes the requirement for the Regional Reliability Organization should be removed from EOP-004-1 since the RRO is a holdover from making the standards enforceable. It is no longer appropriate for the regions to be named as responsible entities within the standards.
Response: The DSR SAR DT thanks you for your comment. The SAR calls for elimination of fill-in-the-blank elements, which will remove the RRO from the standard.		

Organization	Yes or No	Question 4 Comment
Georgia System Operations Corp.	No	EOP-004 should be retired. CIP-001 should not apply to LSEs other than those that are retail marketers.
Response: The DSR SAR DT thanks you for your comment. The SAR calls for EOP-004 to be revised. The Standard Drafting Team may, with stakeholder approval, retire it. CIP-001: NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the SAR. The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting process.		
AEP	No	We would recommend that the Load Serving Entity (LSE) be removed from both standards, and that the Generator Owner and Transmission Owner be added to the resulting standard.
Response: The DSR SAR DT thanks you for your comment. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the SAR. The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting stage of the process. The SAR DT discussed the addition of the TO and GO. The team has a concern that there may be duplication of requirements between the TO/TOP and GO/GOP if the TO and GO are added to the SAR. That being said, the team added the TO and GO to the applicability of the SAR so that the Standard Drafting team may consider these entities for applicability. The applicability of requirements will ultimately be determined by the Standard Drafting Team as it develops the requirements through the standard drafting Process. The team will pass your comment along to the Standard Drafting Team for its consideration concerning applicability.		
Duke Energy	No	It's unclear to us that the RRO should continue to be an applicable entity.
Response: The DSR SAR DT thanks you for your comment. The team concurs and notes that the SAR states: EOP-004 has some 'fill-in-the-blank' components to eliminate. **This will remove the RRO from applicability.**		
Covanta	Yes	It would be a welcome enhancement to the end users to understand to communication link between all "appropriate parties" who shall be notified of potential or actual sabotage events.... which also needs to be defined.
Response: The DSR SAR DT thanks you for your comment. The team concurs, and will pass this comment on to the standard drafting team for its consideration.		
Edward C. Stein	Yes	
WECC	Yes	

Organization	Yes or No	Question 4 Comment
Luminant Power	Yes	
ReliabilityFirst Corporation	Yes	
Oncor Electric Delivery	Yes	
Consolidated Edison Co. of New York, Inc.	Yes	
Illinois Municipal Electric Agency	Yes	
Manitoba Hydro	Yes	
We Energies	Yes	
Consumers Energy Company	Yes	
PSEG Enterprise Group Inc Companies	Yes	
Northeast Power Coordinating Council	Yes	
Bonneville Power Administration	Yes	
Colmac Clarion	Yes	
Progress Energy	Yes	
Ameren	Yes	

5. If you have any other comments on the SAR or proposed modifications to CIP-001-1 and EOP-004-1 that you haven't provided in response to the previous questions, please provide them here.

Summary Consideration: Stakeholders provided many good comments that should be considered in the development of the standards under this project. The SAR DT does not believe that these require any revisions to the SAR and will forward these comments to the Standard Drafting Team for its consideration in developing the standard(s). These include:

1 Consolidation of reports: The SAR DT agrees with this concept and will forward the comment to the Standard Drafting Team for its consideration.

2 Concerns about pre-determination of combining CIP-001 and EOP-004 into one standard: The SAR states: CIP-001 *may* be merged with EOP-004 to eliminate redundancies. The two standards may be left separate.

3 Reporting criteria in multiple tables: The team agrees that it would be easier if there were only one table. Part of this SAR is to eliminate redundancies and make general improvements to the standard. The team also agrees that the requirements developed should be clear in their reliability objective.

Organization	Question 5 Comment
PSEG Enterprise Group Inc Companies	The PSEG Companies ask that the drafting team allow sufficient flexibility for sabotage recognition and reporting requirements such that nothing precludes utilizing a single corporate-wide program for both bulk electric system assets and other businesses. PSEG's Sabotage Recognition, Response and Reporting Program is directed to all business areas which are directed to follow the same internal protocol that also satisfies the NERC Standards requirements. For example, for gas assets, PSEG's gas distribution business follows the PSEG corporate-wide program for sabotage recognition and response. PSEG agrees that some modifications should be made to CIP-001 (ex. better define or give examples of sabotage) and EOP-004 to make them clearer? If they are merged, then Sabotage will not be in the title (or the primary focus) because several of the Disturbances that reporting is required for in EOP-004 have nothing to do with sabotage. EOP-004 has criteria listed in 4 places to determine when to send a report: o Criteria listed in EOP-004 Attachment 1 o Criteria listed in EOP-004 Attachment 2 o Criteria listed in top portion of Table 1-EOP-004 o Criteria listed in bottom potion of Table 1-EOP-004 Therefore, it would be much easier if there was one table of criteria for reference that addressed all of the reportable conditions and all of the applicable reports. If the 2 standards are merged as suggested in the SAR, any differences in the reporting obligation for actual or attempted sabotage and reporting of disturbances must be clear.

Organization	Question 5 Comment
Response: The DSR SAR DT thanks you for your comment. The team agrees that it would be easier if there were only one table. Part of this project is to eliminate redundancies and make general improvements to the standard. The team also agrees that the requirements developed should be clear in their reliability objective. The team will forward your comment to the standard drafting team for its consideration in the drafting of the standard.	
Kansas City Power & Light	If it is desirable to keep CIP-001 and EOP-004 separate, it is recommended the SDT consider adding a reference in CIP-001 to the DOE reporting form either by name or by internet link in the standard.
Response: The DSR SAR DT thanks you for your comment. The SAR SDT recommends eliminating all references to the DOE report, so there won't be a reference to it in CIP-001.	
IRC Standards Review Committee	We suggest that the revision not be conducted with a preconceived notion that the two standards must be combined since there are some differences between sabotage and emergency system conditions, and in the communication and reporting processes and channels. We suggest the SDT start off with a neutral position to focus on improving the standards, then assess the pros and cons of merging the two based on technical merit only.
Response: The DSR SAR DT thanks you for your comment. The SAR states: CIP-001 may be merged with EOP-004 to eliminate redundancies. The two standards may be left separate.	
Pepco Holdings, Inc. - Affiliates	Consider CIP-008-2 as potentially having overlaps with the proposed standard
Response: The DSR SAR DT thanks you for your comment. The SAR states "Specific references to the DOE form need to be eliminated." This will remove the linkage that you identify between CIP-001 and CIP-008. There is also a directive from FERC Order 693 in the SAR that states: **Consider FirstEnergy's suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality.** **This allows the standard drafting team to delineate physical and cyber assets. The DSR SAR DT also notes that CIP-008 might be a good framework for drafting the standard requirements pertaining to sabotage and disturbance reporting of physical assets.**	
FirstEnergy	1. Under Industry Need it states: "The existing requirements need to be revised to be more specific and there needs to be more clarity in what sabotage looks like." The use of the phrase "more specific" should be qualified by adding "while not being too prescriptive". As with other reliability standards, we do not want a standard that causes unwarranted and unnecessary additional work and costs to an entity to comply. 2. As pointed out by the NERC Audit and Observation Team in the "Issues to be considered" for CIP-001, clarification is needed regarding contacting the FBI. Prior audits dwelled heavily on FBI notification. For example, our policy states that Corporate Security notifies the FBI. In recent events it appears that local law enforcement handles day to day activities. The notification process for

Organization	Question 5 Comment
	contacting the FBI needs clarification along with specific instances in which to call them. Who should make the call to the FBI? It appears that a protocol needs to be developed to clarify what events require notifying the FBI. It could be as simple as after an incident a standard form is completed and forwarded to the FBI, letting them decide if follow up is needed. 3. We suggest aligning all reporting requirements for consistency. The items requiring reporting and the timelines to report are very inconsistent between NERC and the DOE. NERC's timelines are also not consistent with their own Security Guideline for the Electricity Sector: Threat and Incident Reporting.
Response: The DSR SAR DT thanks you for your comment. **The team concurs that the standards should provide the "what" without the "how". The standard drafting team will develop the standards using the NERC Standard Development Process that includes stakeholder consensus. The team does not feel it is necessary to add the "not too prescriptive" qualifier to the SAR.** **The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).** **The team concurs with your comment and notes that other commenters have suggested "one stop shopping" reporting for disturbances and sabotage. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).**	
Electric Market Policy	CIP-008-1 Incident Reporting and Response Planning include some requirements that require coordination with the requirements addressed in this project.
Response: The DSR SAR DT thanks you for your comment. The SAR states "Specific references to the DOE form need to be eliminated." This will remove the linkage that you identify between CIP-001 and CIP-008. There is also a directive from FERC Order 693 in the SAR that states: **Consider FirstEnergy's suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality.** **This allows the standard drafting team to delineate physical and cyber assets. The DSR SAR DT also notes that CIP-008 might be a good framework for drafting the standard requirements pertaining to sabotage and disturbance reporting of physical assets.**	
MRO NERC Standards Review Subcommittee	A. The SAR states that there may be impact on a related standard, COM-003-1 (page SAR-5). Is the SDT referring to Project 2007-02, Operating Personnel Communication Protocols? If so, this is a SAR too and should not be used as a reference. B. CIP-001-1 and EOP-004-1 should be combined into one EOP Standard. C. Within EOP-004-1 there is industry confusion on what form to submit in the event of an event. There should only be one form for the new combination Standard eliminating the need for reporting form attachments. It should be the DOE Form, OE-417. Although it is beyond the scope of this SAR, it would greatly benefit industry if there was a central location on the NERC website containing ALL reporting forms, including FERC, NERC, DOE, and ESIAC. This would enable the System Operators to efficiently locate the most current version of the appropriate form in order to report events.

Organization	Question 5 Comment
	D. The word Disturbance is primarily used in other Standards as in, Disturbance Control Standard or system separation due to a disturbance. Should the NERC definition be updated? Should the word "Sabotage" be defined by NERC? Additionally, we recommend that one definition of "Sabotage" be utilized industry-wide, instead of varying definitions by multiple groups like the DOE, ESIAC, etc.
Response: The DSR SAR DT thanks you for your comment. **A. It does reference project 2007-02, and it has been noted in the SAR.** **B. Will forward this comment to the standard drafting team for its consideration in developing the standard(s).** **C. The team concurs with your comment and notes that other commenters have suggested "one stop shopping" reporting for disturbances and sabotage. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).** **D. References to DOE are to be removed from the standards per the SAR. FERC Order 693 directives include definition of sabotage for CIP-001.**	
Lands Energy Consulting	One final comment on CIP-001-1. My clients received universally rude treatment from the FBI field offices when they attempted to establish the contacts required by the Standard. If the FBI doesn't see value in establishing these contacts, remove the requirement from the Standard. Making sure the LSE knows the FBI field office phone number is probably all the Standard should require.
Response: The DSR SAR DT thanks you for your comment. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).	
Colmac Clarion	Need single report for Sabotage so whatever is required results in notification of all parties (State Emergency Management, Homeland Security, FBI, Grid Reliability Chain of Command). Any and all of these can 'expand' knowledge later but all seem to require 'instant' notification.
Response: The DSR SAR DT thanks you for your comment. The team concur with your comment and notes that other commenters have suggested "one stop shopping" reporting for disturbances and sabotage. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).	
Cowlitz County PUD	Local Law enforcement agencies often are not friendly to Federal involvement with smaller problems they consider their "turf." Need to make sure the small stuff stays with them, however have a system of internal reporting that will catch coordinated sabotage efforts (multiple attacks on DPs and small BAs) at the RC or RE level who then can report to the Federal agencies. Currently EOP-004-1 requires small entities to report a "disturbance" if half of their firm customer load is lost. For some entities, this can be one small substation going down due to a bird. The "50% of total demand" requirement should be removed or improved to better define a true BPS disturbance.

Organization	Question 5 Comment
Response: The DSR SAR DT thanks you for your comment. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).	
Exelon	Exelon agrees this is a worthwhile project and that reliability will be enhanced and the compliance process will be simplified by clarifying terminology and reporting requirements in these standards. If nothing else, defining "Sabotage" so as to end interpretations of this term and the related requirements is necessary.
Response: The DSR SAR DT thanks you for your comment.	
ERCOT ISO	Due to the fact that both the CIP-001-1 and EOP-004-1 have similar reporting standards, initially combining the two sounds like a correct analysis. However, after further consideration and due to the critical nature of its intended function involving Security aspects, the CIP-001 should be intensely evaluated to determine if its intended purpose meets the threshold or criteria to stand alone. The existing standards for CIP-001-1 Sabotage Reporting may help prevent future mitigation actions caused by sabotage events. EOP-004-1 Disturbance Reporting is administrative in nature, thus the jeopardy of the Bulk Electric System reliability is impacted only if analysis is not performed or if corrective follow-up actions are not implemented. Combining EOP-004 Standard requirements under the umbrella of the CIP -001 Standard would create a high profile Disturbance Reporting Standard. The industry would be better served if information defining sabotage was provided as well as a technical reference document on recognizing sabotage that would also clarify or state any personnel training requirements. All aspects of the intended functions must be reviewed before merging the two standards. At a minimum, we must consider modification that provides improved understanding of the reporting standards and implications as they are currently written.
Response: The DSR SAR DT thanks you for your comment. The SAR states: CIP-001 *may* be merged with EOP-004 to eliminate redundancies. The two standards may be left separate. One of the FERC Order 693 directives for CIP-001 states: **Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event.** **The Standard Drafting Team will follow the NERC Standard Development Process in making revisions under this SAR, including a thorough review of the requirements of both standards. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).**	
MidAmerican Energy	Conflicting time frames exist from document updates. Reporting should be consolidated to one form and / or site to minimize conflicts, confusion, and errors. 1) Reporting requirements for the outage of 50,000 or more customers in EOP-004-1 requires a report to be made within one hour while the form OE-417 requires a report be made within six hours of the outage. The six hour reference on the updated OE-417 form is the correct reference. 2) Reporting for either CIP-001 or EOP-004 should center on the DOE Form OE-417. This would eliminate confusion and simplify reporting for system operators thereby directly enhancing reliability during system events. This would also eliminate much of the duplicate material and attachments in EOP-004. 3) Although it is beyond the scope of this SAR, the industry would benefit if there was a central location or link on the NERC website containing all

Organization	Question 5 Comment
	reporting forms, including FERC, NERC, DOE, and ESIAC. This would enable System Operators to more efficiently locate and report events.
Response: The DSR SAR DT thanks you for your comment. The team notes that other commenters have suggested "one stop shopping" reporting for disturbances and sabotage. The team concurs that timeframes for similar reports should be the same. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).	
Georgia System Operations Corp.	Entity reporting to NERC/Regions is needed by NERC and the Regions to accomplish their missions of overseeing the reliability of the BES and enforcing compliance with Reliability Standards. An entity not reporting as quickly as possible does not harm the integrity of the Interconnection. In fact, it increases the risk to the BES to be investigating details and filling out forms during a time when attention should be on correcting or mitigating an incident.
Response: The DSR SAR DT thanks you for your comment. The team agrees that non-reporting, in the administrative sense, may not harm the integrity of the Interconnection. The team suggests that the appropriate avenue for addressing this concern is through the development of Violation Risk Factors and Violation Severity Levels for each requirement. These compliance elements will be developed during the standard drafting stage of the development process.	
Illinois Municipal Electric Agency	IMEA recommends the following considerations: Simplification of reportable events and the reporting process should be the overriding objective. NERC's Security Guideline for the Electricity Sector: Threat and Incident Reporting (Version 2.0) should be updated to support this standards development initiative. At some point in the process, it may help if examples are given of events actually reported that did not need to be reported.
Response: The DSR SAR DT thanks you for your comment. The team notes that other commenters have suggested "one stop shopping" reporting for disturbances and sabotage. The team agrees that NERC's Security Guide should be in sync with the standards. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s). One of the FERC Order 693 directives for CIP-001 states: **Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event.** **Events that were reported, but didn't need to be, may be identified in "lessons learned".**	
WECC	No
Luminant Power	None
Oncor Electric Delivery	No Additional Comments

Organization	Question 5 Comment
NextEra Energy Resources, LLC	No comment.
Ameren	None

Consideration of Comments on Disturbance and Sabotage Reporting — Project 2009-01

The Disturbance and Sabotage Reporting Standard Drafting Team thanks all commenters who submitted comments on the proposed Concepts Paper for Disturbance and Sabotage Reporting. The document was posted for a 30-day public comment period from March 17, 2010 through April 16, 2010. Stakeholders were asked to provide feedback on the standards through a special Electronic Comment Form. There were 41 sets of comments, including comments from more than 95 different people from approximately 50 companies representing 8 of the 10 Industry Segments as shown in the table on the following pages.

The comments have been sorted and organized by question number in this report; the comments are shown in the original format on the following project web page:

http://www.nerc.com/filez/standards/Project2009-1_Disturbance_Sabotage_Reporting.html

Summary Consideration:

Use of "NERC Guideline: Threat and Incident Reporting"

Most stakeholders agree that existing guidance should be used as the foundation for disturbance reporting. Most commenters felt that the "NERC Guideline: Threat and Incident Reporting" document contains a lot of detailed information which greatly assists in determining reporting events and weaning out non important events. The most common desire was one, common form to be used for reporting and the OE-417 was considered to be a good starting point. Most respondents thought the form could be streamlined. The DSR SDT was urged to focus on applicable events and reporting timelines which are not clear now and to report items that are clearly essential to the reliability of the BES. There was some concern expressed about "over-reporting", out of fear of non-compliance rather than the over the reliability of the BES. There was also a clear desire to separate out vandalism & copper theft from reporting requirements.

Hierarchy for Reporting Disturbances

Most stakeholders (about 2/3) agree with the concept of developing a reporting hierarchy for disturbances. Stakeholders who disagreed believed that the RC should be one of many to receive information on impact events (DOE, RRO, etc.). Such a hierarchy would lead to reporting delays (leading to lack of situational awareness), be cumbersome and complicated and clouds responsibility for who is to report what to whom. Other negative comments believed that a hierarchy would distract the RC's focus from its primary responsibility. Those stakeholders who agreed commented that the RC should be the collection point for reports and information and take the responsibility to forward as required. This is from the concept that the RC has the "wider view" and can recognize patterns, and has the ability to "escalate" the reporting process. This would also minimize duplication of reports and information.

Single Form for All Agencies

Most stakeholders agreed with the concept of having one reporting form for all entities. Several commenters suggested that there is no need for a standard on reporting as they considered it administrative in nature. Most dissenters thought there should be a guideline, rather than an enforceable standard. There is widespread agreement that the one-size-fits-all approach would be very difficult to get agreement on, given the different countries and

agencies involved. Many stakeholders pointed out that consistency and simplification were drivers for one report form. Having multiple recipients, with different information requirements, seems to support an electronic format that would guide information only to those who need it. The concept of an electronic reporting tool will need to be further vetted and developed.

Supplements to NERC Form

Most stakeholders agreed with the concept of entities being able to use information from other sources such as the OE-417 form, to supplement the NERC report form. Some thought that duplicate reports were acceptable, as long as the information was not duplicated (if # of customers lost is required on form A, don't ask on forms B & C). Several stakeholders commented on the need for an electronic, one stop reporting tool. This would avoid duplication while ensuring that the information reported goes only to intended recipients. With an electronic, one stop reporting tool, reports can be updated/corrected instantly, without repeating previously submitted information. Some stakeholders cautioned that the OE-417 can change every three years and this should be taken into account when developing an electronic reporting tool. Again, such a reporting tool would need to be vetted and developed to meet reliability needs.

Impact Events

The majority of stakeholders agreed with the concept of "impact events." Some stakeholders felt that the introduction of impact events increased the risk that some items will go unreported. However, most felt that impact events would dramatically increase the number of reports being submitted, and it would be difficult to separate important information from background noise. Several respondents felt that the SDT ignored the FERC Directive, and did not define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event. Many respondents supplied the SDT with their own definition of "Sabotage". The DSR SDT believes that the concept of impact events and the specificity of what needs to be reported in the standard will be an equally efficient and effective means of address the FERC directive regarding sabotage. Some stakeholders felt that impact events add another layer of uncertainty to the reporting. Even with the switch from sabotage to impact events, several felt that "intent" was still key to determining reportability.

Regional Differences

Several commenters provided information on regional reporting. The SDT will consider whether these should be included in the continent-wide standard. These include:

1. NPCC maintains a document and reporting form (Document C-17 - Procedures for Monitoring and Reporting Critical Operating Tool Failures) that outlines the reporting requirements, responsibilities, and obligations of NPCC RCs in response to unforeseen critical operating tool failures.

2. For other events that do not meet the OE-417 and EOP-004 reporting criteria, ReliabilityFirst expects to receive notification of any events involving a sustained outage of multiple BES facilities (buses, lines, generators, and/or transformers, etc.) that are in close proximity (electrically) to one another and occur in a short time frame (such as a few minutes).

3. WECC sets its loss of load criteria for disturbance reporting at 200 MW rather than the 300 MW in the NERC reporting form.

4. SERC and RFC are developing additional requirements at this time. We suggest that reporting be based on impact to reliability, not on 'newsworthy'

events. We therefore do not agree with such regional efforts and would prefer a continent wide reporting requirements.

5. Some entities identified some in-force Regional Standards and other regional reporting requirements.

Project Scope

Some stakeholders suggested that the SDT has gone beyond its approved scope to "further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event." Further, there is no requirement to create a Reporting Standard to define sabotage. The SDT contends that the development of impact events and the reporting requirements for them will provide the clarity sought in the directive. Other stakeholders suggested that the SDT should seek to retire sanctionable requirements that require event reporting in favor of guidelines for reporting. Several commenters suggested that the introduction of impact events actually expands the reporting requirements. It should be noted that the list of impact events is expected to be explicit as to who is to report what to whom and within certain timelines.

Electronic Tool

Several stakeholders provided input as to what they believed an electronic reporting tool should contain:

1 If the decision is made to go to a single reporting form, it should be developed to cover any foreseeable event.

2 The SDT should work toward a single form, located in a central location, and submitted to one common entity (NERC)

3 Reports should be forwarded to the ES-ISAC, not NERC, as the infrastructure is already in place for efficient sharing with Federal agencies, with the regional entities and with neighboring asset owners. Reports should flow to all affected entities in parallel, rather than series (timing issues).

Commenters also suggested that the SDT should consider the impacts of the reporting requirements on the small and very small utilities.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Herbert Schrayshuen, at 609-452-8060 or at Herb.Schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

1. The details of reporting requirements and criteria are in the existing EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and will consider guidance found in the document "NERC Guideline: Threat and Incident Reporting" in the development of requirements. Do you agree with using the existing guidance as the foundation for disturbance reporting? Please explain your response (yes or no) in the comment area..... 12

2. The DSR SDT is considering developing a reporting hierarchy for disturbances that requires entities to submit information to the Reliability Coordinator and then for the Reliability Coordinator to submit the report. Do you agree with this hierarchy concept? Please explain your response (yes or no) in the comment area..... 24

3. The goal of the DSR SDT is to have one report form for all functional entities (US, Canada, Mexico) to submit to NERC. Do you agree with this change? Please explain your response (yes or no) in the comment area. 34

4. The goal of the DSR SDT is to eliminate the need to file duplicate reports. The standards will specify information required by NERC for reliability. To the extent that this information is also required for other reports (e.g. DOE OE-417), those reports will be allowed to supplement the NERC report in lieu of duplicating the entries in the NERC report. Do you agree with this concept? Please explain your response (yes or no) in the comment area. 42

5. In its discussion concerning sabotage, the DSR SDT has determined that the spectrum of all sabotage-type events is not well understood throughout the industry. In an effort to provide clarity and guidance, the DSR SDT developed the concept of an impact event. By developing impact events, it allows us to identify situations in the "gray area" where sabotage is not clearly defined. Other types of events may need to be reported for situational awareness and trend identification. Do you agree with this concept? Please explain your response (yes or no) in the comment area. 51

6. If you are aware of any regional reporting requirements beyond the scope of CIP-001, CIP-008 and EOP-004 please provide them here..... 61

7. If you have any other comments on the Concepts Paper that you haven't already provided in response to the previous questions, please provide them here..... 65

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	John Bee	Exelon	X		X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Dan Brotzman	ComEd	RFC	1
2.	Dave Weaver	PECO	RFC	1
3.	Ron Schloendorn	PECO	RFC	1
4.	John Garavaglia	ComEd	RFC	1
5.	Karl Perman	Exelon	NA - Not Applicable	NA
6.	Dave Belanger	Exelon Generation Co., LLC	RFC	5
7.	Alison MacKellar	Exelon Generation Co., LLC	RFC	5
8.	Tom Leeming	ComEd	RFC	1
9.	Tom Hunt	PECO	RFC	1

2.	Group	Guy Zito	Northeast Power Coordinating Council											X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	NA
2.	Michael Schiavone	National Grid	NPCC	1

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Roger Champagne		Hydro-Quebec TransEnergie	NPCC					2				
4.	Kurtis Chong		Independent Electricity System Operator	NPCC					2				
5.	Sylvain Clermont		Hydro-Quebec TransEnergie	NPCC					1				
6.	Chris de Graffenried		Consolidated Edison Co. of New York, Inc.	NPCC					1				
7.	Gerry Dunbar		Northeast Power Coordinating Council	NPCC					10				
8.	Ben Eng		New York Power Authority	NPCC					4				
9.	Brian Evans-Mongeon		Utility Services	NPCC					8				
10.	Mike Garton		Dominion Resources Services, Inc.	NPCC					5				
11.	Brian L. Gooder		Ontario Power Generation Incorporated	NPCC					5				
12.	Peter Yost		Consolidated Edison Co. of New York, Inc.	NPCC					3				
13.	David Kiguel		Hydro One Networks Inc.	NPCC					1				
14.	Michael R. Lombardi		Northeast Utilities	NPCC					1				
15.	Randy MacDonald		New Brunswick System Operator	NPCC					2				
16.	Bruce Metruck		New York Power Authority	NPCC					6				
17.	Lee Pedowicz		Northeast Power Coordinating Council	NPCC					10				
18.	Robert Pellegrini		The United Illuminating Company	NPCC					1				
19.	Saurabh Saksena		National Grid	NPCC					1				
20.	Kathleen Goodman		ISO - New England	NPCC					2				
21.	Greg Campoli		New York ISO	NPCC					2				
3.	Group	Wes Davis (SERC Staff) and Steve Corbin (Chair of SERC RCS)	SERC Reliability Coordinator Sub-committee (RCS)										X
	Additional Member		Additional Organization	Region					Segment Selection				
1.	Steve Corbin		Southeastern RC	SERC					NA				
2.	Joel Wise		TVA RC	SERC					NA				
3.	Don Reichenbach		VACAR South RC	SERC					NA				
4.	Don Shipley		ICTE RC	SERC					NA				
5.	Robert Rhodes		SPP RC	SERC					NA				
6.	Stan Williams		PJM RC	SERC									

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
7. Tim Aliff			Midwest ISO RC	SERC					NA				
4.	Group	Mike Garton	Electric Market Policy	X		X		X	X				
	Additional Member		Additional Organization	Region					Segment Selection				
1. Michael Gildea			Dominion Resources Services, Inc.	RFC					3				
2. Louis Slade			Dominion Resources Services, Inc.	SERC					6				
5.	Group	Carol Gerou	MRO's NERC Standards Review Subcommittee										X
	Additional Member		Additional Organization	Region					Segment Selection				
1.	Chuck Lawrence		American Transmission Company	MRO					1				
2.	Tom Webb		WPS Corporation	MRO					3, 4, 5, 6				
3.	Terry Bilke		Midwest ISO Inc.	MRO					2				
4.	Jodi Jenson		Western Area Power Administration	MRO					1, 6				
5.	Ken Goldsmith		Alliant Energy	MRO					4				
6.	Dave Rudolph		Basin Electric Power Cooperative	MRO					1, 3, 5, 6				
7.	Eric Ruskamp		Lincoln Electric System	MRO					1, 3, 5, 6				
8.	Joseph Knight		Great River Energy	MRO					1, 3, 5, 6				
9.	Scott Nickels		Rochester Public Utilties	MRO					4				
10.	Terry Harbour		MidAmerican Energy Company	MRO					1, 3, 5, 6				
6.	Group	Linda Perea	Western Electricity Coodinating Council										X
	Additional Member		Additional Organization	Region					Segment Selection				
1. Steve Rueckert			WECC	WECC					10				
7.	Group	Kenneth D. Brown	Public Service Enterprise Group Companies	X		X		X	X				
	Additional Member		Additional Organization	Region					Segment Selection				
1.	Ron Wharton		PSE&G	RFC					1, 3				
2.	Dave Murray		PSEG Power Connecticut	NPCC					5				
3.	Jim Hebson		PSEG Energy Resource & Trade	ERCOT					6				
4.	Jerzy Sluarz		PSEG Fossil	RFC					5				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
5.		Bruce Wertz	Odessa Ector Power Partners	ERCOT					5				
6.		Peter Dolan	PSEG Energy Resource & Trade	RFC					6				
8.	Group	Laura Zotter	ERCOT ISO		X								X
	Additional Member		**Additional Organization**	**Region**					**Segment Selection**				
1.	Steve Myers		ERCOT ISO	ERCOT					2, 10				
2.	Jimmy Hartmann		ERCOT ISO	ERCOT					2, 10				
3.	Christine Hasha		ERCOT ISO	ERCOT					2, 10				
9.	Group	Ben Li	ISO RTO Council Standards Review Committee		X								
	Additional Member		**Additional Organization**	**Region**					**Segment Selection**				
1.	Al Dicaprio		PJM	RFC					2				
2.	Jame Castle		NYISO	NPCC					2				
3.	Lourdes Estrada-Salinero		CAISO	WECC					2				
4.	Matt Goldberg		ISO-NE	NPCC					2				
5.	Steve Myers		ERCOT	ERCOT					2				
6.	Bill Phillips		MISO	RFC					2				
7.	Mark Thompson		AESO	WECC					2				
8.	Charles Yeung		SPP	SPP					2				
10.	Group	Denise Koehn	Bonneville Power Administration	X		X		X	X				
	Additional Member		**Additional Organization**	**Region**					**Segment Selection**				
1.	Tedd Snodgrass		BPA, Transmission Dispatch	WECC					1				
2.	Jim Burns		BPA, Transmission Technical Operations	WECC					1				
3.	Jeff Millennor		BPA, Security & Emergency Response	WECC					1, 3, 5, 6				
11.	Group	Jason L. Marshall	Midwest ISO Standards Collaborators		X								
	Additional Member		**Additional Organization**	**Region**					**Segment Selection**				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1. Bob Thomas			IMEA	SERC					4				
2. Jim Cyrulewski			JDRJC Associates, LLC	RFC					8				
3. Joe Knight			Great River Energy	MRO					1, 3, 5, 6				
4. Randi Woodward			Minnesota Power	MRO					1				
5. Kirit Shah			Ameren	SERC					1				
12.	Group	Sam Ciccone	FirstEnergy	X		X	X	X	X				
	Additional Member		Additional Organization	Region					Segment Selection				
1. Doug Hohlbaugh			FE	RFC					1, 3, 4, 5, 6				
2. Dave Folk			FE	RFC					1, 3, 4, 5, 6				
13.	Individual	Thomas Glock	Arizona Public Service Company	X		X		X					
14.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
15.	Individual	Brent Ingebrigtson	E.ON U.S. LLC	X		X		X	X				
16.	Individual	Steve Fisher	Lands Energy Consulting										
17.	Individual	David Kahly	Kootenai Electric Cooperative			X							
18.	Individual	Darryl Curtis	Oncor Electric Delivery Company LLC	X									
19.	Individual	Edward Bedder	Orange and Rockland Utilities, Inc.	X									
20.	Individual	Kasia Mihalchuk	Manitoba Hydro	X		X		X	X				
21.	Individual	Brian Bartos	Bandera Electric Cooperative, Inc.	X		X							
22.	Individual	John T. Walker	Portland General Electric	X									
23.	Individual	Gregory Miller	BGE	X									

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
24.	Individual	Dan Roethemeyer	Dynegy Inc.					X					
25.	Individual	Rick Terrill	Luminant					X					
26.	Individual	James Stanton	SPS Consulting Group Inc.								X		
27.	Individual	Andrew Gallo	Calpine Corp.					X					
28.	Individual	Steve Alexanderson	Central Lincoln			X							
29.	Individual	Brenda Frazer	Edison Mission Marketing & Trading					X					
30.	Individual	Martin Bauer	USBR					X					
31.	Individual	John Alberts	Wolverine Power Supply Cooperative, Inc.	X		X	X	X	X				
32.	Individual	Thad Ness	American Electric Power	X		X		X	X				
33.	Individual	James McCloskey	Central Hudson Gas & Electric	X		X							
34.	Individual	Deborah Schaneman	Platte River Power Authority	X		X		X					
35.	Individual	Howard Rulf	We Energies			X	X	X					
36.	Individual	Jianmei Chai	Consumers Energy Company			X	X						
37.	Individual	Amir Hammad	Constellation Power Source Generation					X					
38.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
39.	Individual	Kirit Shah	Ameren	X		X		X	X				
40.	Individual	Dan Rochester	Independent Electricity System Operator		X								

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
41.	Individual	Roger Champagne	Hydro-Québec TransEnergie (HQT)	X									

1. The details of reporting requirements and criteria are in the existing EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and will consider guidance found in the document "NERC Guideline: Threat and Incident Reporting" in the development of requirements. Do you agree with using the existing guidance as the foundation for disturbance reporting? Please explain your response (yes or no) in the comment area.

Summary Consideration: Most stakeholders agree that existing guidance should be used as the foundation for disturbance reporting. Most commenters felt that the "NERC Guideline: Threat and Incident Reporting" document contains a lot of detailed information which greatly assists in determining reporting events and weaning out non important events. The most common desire expressed was to have one common form for all reporting, and the OE-417 was suggested as a good starting point. Most respondents thought the form could be streamlined. The DSR SDT was urged to focus on applicable events and reporting timelines which are not clear now and to report items that are clearly essential to the reliability of the BES. There was some concern expressed about "over-reporting", out of fear of non-compliance rather reporting based on the reliability of the BES. There was also a clear desire to exclude vandalism & copper theft from reporting requirements.

Several specific suggestions were made to modify existing reporting requirements, and the drafting team will consider these when developing the proposed requirements.

Organization	Yes or No	Question 1 Comment
ERCOT ISO	Possible Yes	Parts of the Guideline are helpful, but the guideline goes beyond the scope of the requirements of the current standards, which could pose potential audit concerns. ERCOT ISO strongly feels this approach for reporting should be focused on physical events only and cyber event reporting should be contained within CIP-008 only. Continue to keep physical separate from cyber.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has not determined at this time what bright line will be used for the yet to be drafted Standard(s). The DSR SDT will take into consideration your comment on keeping cyber and physical events separate.		
Arizona Public Service Company	No Then Yes	APS supports standard revisions which streamline the reporting process for security incidents with a single form, which aligns both with EIA reporting and NERC Standards requirements, particularly those identified in the NERC Threat and Incident Reporting Guidelines. This would eliminate users issuing reports to multiple locations/government entities without a standard form or format. The DOE 417 form which is currently utilized

Organization	Yes or No	Question 1 Comment
		for reporting purposes is out-dated and does not account for the types of incidents as identified in the NERC Threat and Incident Reporting Guidelines. The guidelines state that an entity can report security incidents to the ESISAC , through CIPIS (Critical Infrastructure Protection Information System), and or RCIS (Reliability Coordinator Information Center). CIPIS refers an entity to the NICC and to the WECC. Additionally, APS proposes that the terms and timelines of reporting security incidents be clearly identified. Events are often detected quickly or immediately. Determining whether or not the event was sabotage and/or a reportable event; however, typically takes much longer. There is no time allowance for an entity to investigate the event to determine what actually occurred. Currently, DOE 417 provides that acts of sabotage should be reported within one hour of detection if the impact could affect the reliable operation of the bulk power system. This may affect the accuracy of the information being provided by an entity on it's initial reporting. Finally, provisions should be incorporated to address the privacy of information being submitted, including handling and storage.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has not determined at this time what bright line will be used for the yet to be drafted Standard(s) which should streamline the reporting process (what events and what timeline should be used). c		
SPS Consulting Group Inc.	No	At least not exclusively. The current standards and the guidance fail to consider that different registered entities will have different scopes of awareness for when disturbances may take place. We want to avoid the situation where a generator (for example) is cited for failure to report a disturbance of which they have way of knowing occurred.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT will take into consideration what Registered Entities are to be included within the yet to be written standard(s) based on the SAR and the facilities each type of Registered Entity is required to have.		
Bonneville Power Administration	No Then Yes	BPA likes the idea of consolidating information and eliminating duplication of reported information. In the report, don't include every detail possible found in the "Threat Guideline". TOP's are supposed to be operating the electrical system, not doing investigative work for copper theft incidents (see comment on #5).
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has not determined at this time what bright line will be used for the yet to be drafted Standard(s). We will consider your specific suggestion for not requiring reporting of incidents such as copper threat, when we develop the proposed requirements.		

Organization	Yes or No	Question 1 Comment
Lands Energy Consulting	No	My firm provides compliance consulting services to a number of smaller (50-700 MW peak load) LSE/DP registered entities. EOP-004 creates an obligation for LSEs to report "disturbances" that affect their systems. A few of the smaller of these systems receive service from Bonneville-owned transmission lines that serve only 4-6 substations. The NERC Form establishes loss of 50% of the LSE's retail customers as a reportable disturbances. One of my clients receives service from BPA at 5 substations. A single industrial customer with a substantially dedicated substation comprises 90% of the utility's MWH load. Were it not for this customer, the utility would have been well below the registration requirement for a DP/LSE. The balance of the load, about 15 MW of peak and 4000 retail customers, is served from 5 substations. Four of these substations serving 3000 customers are served from a long Bonneville 115 kV BES transmission line that runs through a heavily treed right of way. Every time this single line experiences a permanent outage (which will happen a few times a year), the utility loses less than 10 MW of load, but 75% of its retail customers. Under the disturbance reporting criteria, this outage would constitute a reportable disturbance for the utility. When the NERC disturbance reporting criteria were adopted, I doubt that anyone conceived that they would apply to cases like I just described. Reporting trivial events like I've just described constitutes a nuisance to the entity making the report and NERC/WECC for having to process the report. The outage has no earthly effect on the reliability of the BES and certainly doesn't warrant preparation of any kind of disturbance report.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT will take into consideration what Registered Entities are to be included within the yet to be written standard(s) based on the NERC Standards Committee approved SAR. The DSR SDT will review the Commissions concern that, an adversary might determine that a small LSE is the appropriate target when the adversary aims at a particular population or facility, as stated in FERC Order 693, paragraph 459. The intent of the proposed standard(s) is to address reporting needed for after-the-fact analyses of events as well as reporting necessary for situational awareness.		
SERC Reliability Coordinator Sub-committee (RCS)	No	Routine minor incidents such as copper theft and gun shots to insulators should not be reported. These types of minor events do not affect the reliability of the BPS. Existing reporting requirements are satisfactory. The focus of reporting should be on reliability related incidents and not incidents related to vandalism as such.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). Reporting threasholds will be determined during the next step of the Standards Development process. The DSR SDT agrees with your comments on vandalism but a balance must be further explored to meet industry and regulatory requirements specifically under FERC Order 693.		
Consumers Energy Company	No	The existing guidelines ignore the fact that there are currently three overlapping and inconsistent reporting requirements for disturbances of various types: CIP-001, EOP-004, and DOE OE-417. The reporting should be such that any single event type needs to be reported only once, and to only a single agency, for any

Organization	Yes or No	Question 1 Comment
		disturbance. First, CIP-001 events should be reported to the ES-ISAC under one specific requirement (or set of requirements) and removed from OE-417 and EOP-004, such that all interested agencies obtain their information from only that one source. Second, OE-417 events should be reportable ONLY to DOE, and, again, other agencies should obtain their information from only that one source. If NERC wishes to make such reporting mandatory and enforceable, the NERC requirements should indicate ONLY that such reporting should be made in accordance with OE-417. Finally, EOP-004 (or similar requirements) should require reporting to NERC ONLY in the case of events that don't fit under CIP-001 or OE-417 requirements. Alternatively, OE-417 should be submitted ONLY to NERC and they should disseminate the information.EOP-004 has several issues and inconsistencies: a. EOP-004 requires that the entity that submits form DOE-417 to provide copies to NERC. The DOE-417 form intermixes NERC entity definitions (e.g. BA, LSE, TO) with generic terms such as "Electric Utilities" and "Generating Entities". Is it the Generator Owner or Generator Operator that is required to submit the information? There should be one form or at least well defined definitions that apply to both forms. b. EOP-004-1 R3.1 requires submittal within 24 hours, however Table 1-EOP-004-0 which purports to summarize the standard appears to change this requirement to 1 hour for several disturbances. Additionally, it incorrectly summaries the reporting time for 50,000 customers, which is 6 hours in DOE-417 and summarized in Table 1-EOP-004-0 as 1-hour. An attachment to a standard should not be allowed to supersede the standard or create additional rules. c. EOP-004-1 R3.1 requires submittal within 24 hours, however Table 1-EOP-004-0 which purports to summarize the standard appears to change the standard. R3.1 clearly states that events are to be reported within 24 hours of identification, however Table 1-EOP-004-0 state that the events are to be reported on the basis of the start of the disturbance. An attachment to a standard should not be allowed to supersede the standard or create additional rules. d. EOP-004-1 R3.1 requires submittal within 24 hours, however Table 1-EOP-004-0 which purports to summarize the standard appears to change the standard. R3.1 clearly states that events are to be reported within 24 hours of identification, however Table 1-EOP-004-0 states that copies of DOE-417 are required to be submitted "simultaneously". It also states that schedules 1 and 2 are due within 24 hours of start of the event instead of 48 hours for per DOE-417 for schedule 2. An attachment to a standard should not be allowed to supersede the standard or create additional rules. e. The requirement of loss of customers should be scaled based on customers served. Loss of 50,000 customers to a utility that serves 100,000 customers is different than loss of 50,000 customers to a utility that serves 2,000,000 customers.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and		

Organization	Yes or No	Question 1 Comment
ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT agrees that present Reliability Standards can be complicated and lead to confusion when working on maintaining system reliability in the area of reporting per CIP-001-1 and EOP-004-1. We will consider the disagreements you've identified in existing reporting requirements when we develop the proposed requirements.		
Central Lincoln	No	The guidance document makes no distinction between entities that operate 24/7 dispatch and those that don't. The 1 hour and even the 24 hour reporting requirements in some cases will be impossible for entities without 24/7 dispatch to meet without changing business practices. These are the same entities that present little or no risk to the BES.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT will take into consideration what Registered Entities are to be included within the yet to be written standard(s) based on the SAR. The DSR SDT will establish the "requirements necessary for users, owners, and operators of the Bulk-Power-System" as stated in FERC Order 693, paragraph 617 and the difference in reporting of events on the BES, as stated in the Purpose statement of EOP-004-1. The intent of the proposed standard(s) is to address reporting needed for after-the-fact analyses of events as well as reporting necessary for situational awareness.		
MRO's NERC Standards Review Subcommittee	No Then Yes	We agree with using the present documentation but would like just one reporting form. We are concerned that the guidelines and reporting periods specified within the DOE OE-417 report conflict with the NERC Guidelines. For example. DOE OE-417 report requires "Suspected Physical or Cyber Impairment" to be reported within 6 hours. The NERC guidelines indicate "Suspected Activities" are to be reported within 1 hour. We recommend the SDT use the DOE OE-417 report as a guiding document, and then determine additional reporting requirements using guidance from the NERC Guideline. FERC Order 693 appears to indicate conflicts and confusion with NERC reporting requirements and DOE reporting requirements should be eliminated.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT is looking to streamline required reporting actions and remove any redundant reporting requirements if at all possible. The DOE Form OE-417 is currently mandatory under Public Law 93-275 for entities within the juristicion of the U.S Department of Energy. We will consider the disagreements you've identified in existing reporting requirements when we develop the proposed requirements.		
Luminant	No Then Yes	While the guidance is generally ok in the "NERC Guideline: Threat and Incidence Reporting", the reporting timelines include 1 hour, 2 hours, 4 hours, 6 hours, 8 hours, 24 hours, and 48 hours. Please simplify and reduce the variation in timelines. When it comes to Sabotage reporting, some time requirements start with detection, some start with determination of sabotage and some events do not specify the trigger for the reporting clock to start. Again, please provide clarity and consistency around the start of the timeline for

Organization	Yes or No	Question 1 Comment
		reporting. Generally, the reporting timing should start with the recognition or determination that a suspected or known sabotage event occurred.
Response: The DSR SDT thanks you for your comment. The DSR SDT is looking to streamline required reporting actions and remove any redundant reporting requirements if at all possible. The DSR SDT agrees that present Reliability Standards can be complicated and lead to confusion when working on maintaining system reliability in the area of reporting per CIP-001-1 and EOP-004-1. We will consider your specific suggestion for less variation in reporting timeframes, when we develop the proposed requirements.		
We Energies	No Then Yes	While the NERC Guideline includes readily discernible information (and we would like to see that format carried forward into any future documentation), utilize OE-417 as the foundation document in order to eliminate reporting redundancies. If supplemental references are necessary for the proposed resolution, list the document as an official attachment to the standard. Minimize the need to search in multiple locations for guideline information - some may not be aware supporting documentation exists without explicit reference within the standard.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT is looking to streamline required reporting actions and remove any redundant reporting requirements if at all possible. The DSR SDT agrees that present Reliability Standards can be complicated and lead to confusion when working on maintaining system reliabiltiy in the area of reporting per CIP-001-1 and EOP-004-1. The DOE Form OE-417 is currently mandatory under Public Law 93-275 for entities within the juristicion of the U.S Department of Energy. We will consider your recommendation regarding listing supplemental references within the body of the standard when we draft the proposed standard(s).		
American Electric Power	Yes	
Bandera Electric Cooperative, Inc.	Yes	
Calpine Corp.	Yes	
Duke Energy	Yes	
Edison Mission Marketing & Trading	Yes	

Organization	Yes or No	Question 1 Comment
Exelon	Yes	
Independent Electricity System Operator	Yes	
PacifiCorp	Yes	
Platte River Power Authority	Yes	
Central Hudson Gas & Electric	Yes	Central Hudson agrees with using the "NERC Guideline: Threat and Incident Reporting" in the development of requirements. Central Hudson has currently in place a NERC-DOE Threat and Incident Reporting Table developed from this NERC Guideline that allows for a quick-reference to all threat and incident reporting criteria (arranged by category)with a cross-reference to the specfic reporting form (NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report, DOE Form OE-417, or NERC ES-ISAC Threat and Incident Report Form). Central Hudson recommends maintaining the option of utilizing only 1 form, the DOE Form OE-417, for incidents that require reporting to the DOE and NERC to maintain the streamlined approach to this reporting process.
Response: The DSR SDT thanks you for your comment. The DSR SDT is looking to have a single reporting report form (per question 3) and streamline the reporting processes that may be developed within ~~a~~ yet to be written requirement(s).		
E.ON U.S. LLC	Yes	E.ON U.S. believe that the guidelines provide greater clarity for reporting forced outages caused by disturbances and sabotage but there remains issues that in need of further clarification. For example, there remains too much subjectivity on the reporting of forced outages when there is "identification of valuable lessons learned"
Response: The DSR SDT thanks you for your comment. The DSR SDT concurs that further clarification is required with the ambigious statement "identification of valuable lessons learned" contained in the guideline – use of this phrase does not meet the technical writing threshold required for inclusion in a NERC Standard. The DSR SDT's intent was to look at the posted NERC Guideline and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). Recommendation of changes to the "NERC Guideline: Threat and Incident Reporting" should be submitted to NERC via the Critical Infrastructure Protection Committee. I		
Public Service Enterprise Group Companies	Yes	EOP reportable disturbances are familiar concepts in the industry.

Organization	Yes or No	Question 1 Comment
Response: The DSR SDT thanks you for your comment and support.		
Orange and Rockland Utilities, Inc.	Yes	However, the SDT needs to maintain clear demarcation for the criteria for reporting events, and only those events that directly effect the reliability of the BES.
Response: The DSR SDT thanks you for your comment. The DSR SDT has been directed to review all disturbance type activities and submit to the industry a well thought out set of requirements that clearly define disturbance events and what information is required to enhance an entity'ssituational awareness. Clear demarcation for the criteria for reporting will be determined in the near future based on the approved SAR and industry feedback. The intent of the proposed standard(s) is to address reporting needed for after-the-fact analyses of events as well as reporting necessary for situational awareness.		
Wolverine Power Supply Cooperative, Inc.	Yes	I agree with referencing existing guidelines - However: My concern is that, until all reportable incidents are analyzed by the parties to which they are reported, their "impact" on the BES will not be quantified. Therefore, the tendency to want to "report all events so that their impact can be determined" or "report all events because the information can be utilized for informational purposes, regardless of impact on BES" might lead to expanded reporting requirements, some of which may have questionable value from a reliability standpoint.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if the DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has been directed to review all disturbance type activities and submit to the industry a well thought out set of requirements that clearly define reportable events and what information is required to enhance an entity's situational awareness. Clear demarcation for the criteria for reporting will be determined in the near future based on the approved SAR and industry feedback. The intent of the proposed standard(s) is to address reporting needed for after-the-fact analyses of events as well as reporting necessary for situational awareness.		
Hydro-Québec TransEnergie (HQT)	Yes	In considering guidance found in the document "NERC Guideline: Threat and Incident Reporting", the SDT should maintain focus on only those items that are absolutely necessary to maintain the reliability of the Bulk Electric System. In fact, the purpose of reporting per EOP-004 is that disturbances... need to be studied and understood to minimize the likelihood of similar events in the future.
Northeast Power Coordinating Council	Yes	In considering guidance found in the document "NERC Guideline: Threat and Incident Reporting", the SDT should maintain focus on only those items that are absolutely necessary to maintain the reliability of the Bulk Electric System. In fact, the purpose of reporting per EOP-004 is that disturbances... need to be studied and understood to minimize the likelihood of similar events in the future.
Response: The DSR SDT thanks you for your comment. The DSR SDT will establish the "requirements necessary for users, owners, and operators of		

Organization	Yes or No	Question 1 Comment
the Bulk-Power-System" as stated in FERC Order 693, paragraph 617 and the difference in reporting of events on the BES, as stated in the Purpose statement of EOP-004-1. The intent of the proposed standard(s) is to address reporting needed for after-the-fact analyses of events as well as reporting necessary for situational awareness.		
Western Electricity Coordinating Council	Yes	It is comprehensive; however, we must keep in mind that the OE-417 is required under Public Law 93-275 and needs to be attached if applicable in the US.
Response: The DSR SDT thanks you for your comment.		
Oncor Electric Delivery Company LLC	Yes	NERC Guideline: Threat and Incident Reporting" document should be used for guidance as it identifies best practices for reporting.
Response: The DSR SDT thanks you for your comment.		
Manitoba Hydro	Yes	The "Threat and Incident Reporting" document contains a lot of detailed information which greatly assists in determining reporting events and weaning out non important events. The document contains some examples and expected reporting time lines. Attachment 1-EOP-004, though considerably smaller and condensed it does contain some detail not mentioned in "Threat and Incident Reporting". Integrating the "Threat and Incident Reporting" into Attachment 1-EOP-004, though large in size, has lots of information and is easy to follow would be a large improvement to existing protocol OR SEE QUESTION 3 COMMENTS. Incidences we have experienced on our system, in past were difficult to delineate as reportable, who to report to and when. An improvement to this Standard is welcome.
Response: The DSR SDT thanks you for your comment. The DSR SDT is looking to streamline and remove any redundancies within the NERC Standard's requirements.		
Constellation Power Source Generation	Yes	The existing guidance is an excellent base on which to build changes to EOP-004 and CIP-001. However, the SDT must challenge each item in the different event categories and clarify or omit bullet points that are seemingly vague. For example, under System Disturbances, a forced outage report is needed when "a generation asset of 500 MW or above is on a forced outage for unknown reasons, or a forced outage of generation of 2,000 MW occurs..." Simply removing the 500 MW criteria would make this criterion less vague. There are other examples of this in the guideline.
Response: The DSR SDT thanks you for your comment. The DSR SDT is looking to streamline and remove any redundancies within the NERC Standard's requirements. It is the intent of the SDT to carefully review the different event categories and provide clarity where needed to remove ambiguity.		

Organization	Yes or No	Question 1 Comment
ISO RTO Council Standards Review Committee	Yes	The guidelines in EOP-004 and its attachments should be retained as the foundation for reporting disturbances. One would note that such EOP Disturbances are relatively well defined reliability impacts. Thus EOP-004 disturbances are based on HOW certain events impacted the BES. [Sabotage on the other hand requires an implication of WHY an event occurred.]The original EOP-004 represents a common sense approach to defining reliability events that may be useful to analyze on a regional basis. In the current environment, Regions are not sanctionable entities but they still are valuable sources to collect, analyze and trend the few disturbances that occur in each region. To make use of Regions, however, precludes the use of sanctionable NERC standards. EOP-004 as written does not meet the NERC requirements for standards but it does meet the Industry needs for a guideline for reporting events that deserve to be reviewed. The SDT should propose deleting EOP-004 and use it as a Disturbance Reporting Guideline.
Response: The DSR SDT thanks you for your comment. Regions are required to comply with requirements in NERC Reliability Standards – however Regions are not sanctioned the same way as users, owners and operators of the bulk power system – if a Region fails to comply with a NERC Reliability Standard, it can be fined for failure to comply under the ERO's Rules of Procedure.		
USBR	Yes	The reporting outlined in the proposed plan does not include a clear indication of how NERC will use the information they collect from the entities. Care needs to be taken in addressing the reporting requirements to not create a more confusing or onerous reporting process.
Response: The DSR SDT thanks you for your comment. It is anticipated that NERC will analyze events to assess trends and identify lessons learned for industry feedback and reliability improvement.		
FirstEnergy	Yes	This guideline appears to be a good starting point for developing consistency in reporting. However, we believe that after-the-fact event reporting is administrative in nature and seldom rises to the level of mandated reliability standard requirements. It is not clear what reporting would be made through this effort and how it differs from reporting made through the NERC Reliability Coordinator Information System (RCIS). With the initiative for more results-based standards being the goal of NERC, true after the fact reporting-type requirements should become administrative procedures and only be included in standards if they are truly required for preserving an Adequate Level of Reliability. If there are aspects that rise to be retained in a mandatory and enforceable reliability standard, we propose that those associated with sabotage be moved to CIP-001 and that EOP-004 be focused on operational disturbances that warrant wide-area knowledge. However, if the RCIS is the mechanism to convey real-time information and that is presently occurring outside of reliability standards, it is unclear what the delta improvement this project aims to achieve.
Response: The DSR SDT thanks you for your comment. As stated in FERC Order, 693, paragraph 611, "Complete and timely data is essential for analyzing system disturbances" and in paragraph 617, "the Commission directs the ERO to develop a modification to EOP-004-1 through the		

Organization	Yes or No	Question 1 Comment
Reliabiloity Standards development process that includes any requirements necessary for users, owners, and operators of the Bulk-Power-System to provide data that will assist NERC in the investigation of a blackout or disturbance". Some data is needed, therefore, for after-the-fact analyses. In addition, some data is needed much more quickly for situational awareness. The DSR SDT will analize and determine what constitues a reportable event and what information is required for situational awareness as opposed to after the fact analyses of events.		
Portland General Electric	Yes	This process is in place and utilities are familiar with it. This is a good place to start.
Response: The DSR SDT thanks you for your comment and support.		
Ameren	Yes	We agree that it makes sense to build upon existing documentation. However, we do not believe it is necessary to require event reporting to be in an enforceable standard. Rather the drafting team should consider developing a reporting guideline document and retiring the EOP-004 standard.
Response: The DSR SDT thanks you for your comment. As stated in FERC Order, 693, paragraph 611, "Complete and timely data is essential for analyzing system disturbances" and in paragraph 617, "the Commission directs the ERO to develop a modification to EOP-004-1 through the Reliabiloity Standards development process that includes any requirements necessary for users, owners, and operators of the Bulk-Power-System to provide data that will assist NERC in the investigation of a blackout or disturbance". Some data is needed, therefore, for after-the-fact analyses. In addition, some data is needed much more quickly for situational awareness. As envisioned, the requirements developed under this project will address both types of reporting requirements.		
Midwest ISO Standards Collaborators	Yes	We agree that it makes sense to build upon existing documentation. However, we do not believe it is necessary to require event reporting to be in an enforceable standard. Rather the drafting team should consider developing a reporting guideline document and retiring the EOP-004 standard. This is further supported by the fact that there is a role in the existing standard for the Regional Entities even though these requirements can't be enforced against the Regional Entities because they are not a user, owner or operator of the system.
Response: The DSR SDT thanks you for your comment. As stated in FERC Order, 693, paragraph 611, "Complete and timely data is essential for analyzing system disturbances" and in paragraph 617, "the Commission directs the ERO to develop a modification to EOP-004-1 through the Reliabiloity Standards development process that includes any requirements necessary for users, owners, and operators of the Bulk-Power-System to provide data that will assist NERC in the investigation of a blackout or disturbance". Some data is needed, therefore, for after-the-fact analyses. In addition, some data is needed much more quickly for situational awareness. As envisioned, the requirements developed under this project will address both types of reporting requirements.		
Dynegy Inc.	Yes	We agree with using the guidance; however, please consider revising the NERC Guideline: Threat and Incident Reporting document to (i) lengthen the reporting timelines related to attempted sabotage to allow for

Organization	Yes or No	Question 1 Comment
		additional time to deem the threat credible, (ii) expand the description of forced outage of generation greater than 2000 MW to include whether it is at the BA or GO level and if GO level, whether it is for one site or the combined GO's sites in a Region, and (iii) add a Responsible Party column to the Appendix A matrix.
Response: The DSR SDT thanks you for your comment. Recommendation of changes to the "NERC Guideline: Threat and Incident Reporting" should submitted to NERC via the Critical Infrastructure Protection Committee since that falls outside the scope of the SAR. **We will consider your specific suggestions for revisions to reporting requirements when we develop the proposed requirements.**		
BGE	Yes	We have no problem with NERC using the existing guidance as the foundation for disturbance reporting; however, since this project proposes to investigate incorporation of the Cyber Incident reporting aspects of CIP-008, we feel that if adopted, this concept should be added to the NERC Guideline document "Threat and Incident Reporting".
Response: The DSR SDT thanks you for your comment. Recommendation of changes to the "NERC Guideline: Threat and Incident Reporting" should submitted to NERC via the Critical Infrastructure Protection Committee since that falls outside the scope of the SAR.		
Electric Market Policy	Yes	Yes; however, in considering guidance found in the document "NERC Guideline: Threat and Incident Reporting" the SDT should maintain focus on only those items that are absolutely necessary to maintain the reliability of the Bulk Electric System. In fact, the purpose of reporting per EOP-004 is that disturbances... need to be studied and understood to minimize the likelihood of similar events in the future.
Response: The DSR SDT thanks you for your comment. The DSR SDT will establish the "requirements necessary for users, owners, and operators of the Bulk-Power-System" as stated in FERC Order 693, paragraph 617 and the difference in reporting of events on the BES, as stated in the Purpose statement of EOP-004-1. As envisioned, the requirements developed under this project will address reporting requirements that are used for after-the-fact analyses as well as reporting requirements that are associated with situational awareness.		

2. The DSR SDT is considering developing a reporting hierarchy for disturbances that requires entities to submit information to the Reliability Coordinator and then for the Reliability Coordinator to submit the report. Do you agree with this hierarchy concept? Please explain your response (yes or no) in the comment area.

Summary Consideration: Most stakeholders (about 2/3) agree with the concept of developing a reporting hierarchy for disturbances. Stakeholders who disagreed believed that the RC should be one of many to receive information on impact events (DOE, RRO, etc.). Such a hierarchy would lead to reporting delays (leading to lack of situational awareness), be cumbersome and complicated and clouds responsibility for who is to report what to whom. Other negative comments believed that a hierarchy would distract the RC's focus from its primary responsibility. Thos stakeholders who agreed commented that the RC should be the collection point for reports and information and take the responsibility to forward as required. This is from the concept that the RC has the "wider view" and can recognize patterns, and has the ability to "escalate" the reporting process. This would also minimize duplication of reports and information.

Organization	Yes or No	Question 2 Comment
BGE	No	As currently worded, BGE opposes the reporting hierarchy concept, since insufficient guidelines were proposed to prevent translation errors between the responsible entity (RE) and the RC. In addition to creating possible reporting errors, this also opens a risk that the RC could misrepresent the true intent of an RE's report contents if called upon to explain/justify a submitted report. Reporting delays are another concern with this proposal because the RE would basically be relinquishing control of the reporting process to the RC, while ultimately retaining the responsibility for ensuring the report gets submitted within the required timeframe. However, BGE recognizes that avoiding duplication and conflicting reports as well as encouraging communication are valuable. To make the reporting hierarchy concept acceptable to BGE, the DSR SDT must develop proper controls to ensure the RE has the ability to control or approve the information submitted and/or subsequently discussed with the respective authorities, and that it is done within the permissible timeframe to satisfy compliance requirements.
Response: The DSR SDT thanks you for your comment. If the reporting hierarchy concept is adopted, it will include controls to ensure timely reporting, clear accountability so that risk is not transferred, and a mechansim to ensure the Responsible Entity's reported information remains as submitted.		

Organization	Yes or No	Question 2 Comment
Consumers Energy Company	No	It would be inefficient for RC's to accumulate ALL disturbance data and submit it, and to bifurcate the reporting based on type of disturbance above and beyond OE-417 data (which should go ONLY to DOE) would make a standard very involved for an entity to comply with. We're discussing after-event data here, not data needed for current operations - and there's no reason to make it any more complicated than necessary.
Response: The DSR SDT thanks you for your comment. In order for a reporting hierarchy concept to be adopted, it will result in real effiency gains by eliminating duplication of reports. It will not be pursued if the result is a complicated or burdensome process for responsible entities.		
Exelon	No	Some of the DOE related reporting is driven by distribution events, i.e. outages greater then 50,000 customers, is it realistic to expect the RC, whose focus is on the transmission system to perform distribution related reporting?
Response: The DSR SDT thanks you for your comment. The DOE Reporting Form OE 417 is currently mandatory by Public Law and only applies to US entities and contains reporting thresholds that are not required by NERC. Our goal is to derive reporting thresholds that meet NERC's needs for information on bulk electric system disturbances and real-time events, not distribution level-only problems.		
USBR	No	The existing reporting methods collect reports of disturbances and analyze them by committees of the respective coordinating councils. The new process would introduce a duplicate layer and associated staffing. It would be better to ensure communication between the existing committees of the respective coordinating councils and the RC rather than creating a new layer of review tracking and analysis. While the layered reporting hierarchy discussed in the Disturbance Reporting section of the paper will eventually help with overall event awareness, the additional delays the hierarchical approach could result in a decrease in situational (timely) awareness. Having more comprehensive information as a result of the potential enhancements each layer adds to the chain of reporting may not be more valuable than timely and well disseminated information in an actual disturbance situation. We would suggest the SDT give careful consideration to this proposed direction. It may be appropriate to consider that expedited reporting of operational impacts would outweigh the benefit of administratively intensive reporting procedures. The events reported through the existing process have not yielded material feedback other than statistical analysis. Statistical analysis is not as sensitive to timely reporting. Operational impacts which may be the result of possible sabotage may be evident through assessment of widespread outage patterns or following event analysis. Comprehensive event analysis can take anywhere from 15 days to 90 days depending on the event.
Response: The DSR SDT thanks you for your comment. We agree that reporting timeliness must be weighed against the percieved benefits of a reporting hierarchy. If the reporting hierarchy concept is adopted, it should include controls to ensure timely reporting, clear accountability so that risk of a violation of the standard is not transferred, and a process to ensure the responsible entities' reported information remains as submitted. Also it must result in real effiency gains and support the reliability of the bulk electric system.		

Organization	Yes or No	Question 2 Comment
ISO RTO Council Standards Review Committee	No	The idea of a reporting hierarchy provides an easy to follow pro forma approach. But disturbance reports should not always follow a common reporting path. A disturbance on the transmission system for example need not be routed through an "if applicable" Balancing Authority. To mandate that a BA be in the path is inappropriate. To leave the applicability open is to create a subjective compliance problem for the impacted BA. Copper theft is another example that should not require reporting up through the RC. It is a local issue and the Transmission Owner should be able to report this directly to the appropriate parties. How would a DP, LSE or GO know if an event is an "impact event"? The posed impact events are a series of conditions for sabotage but not for EOP-type disturbances. The aforementioned entities have no requirement to monitor and analyze the BES, which then means every event would be an impact event for those entities (not an EOP disturbance but an impact event). Thus every theft of copper is an impact event mandating a Disturbance Report even though the SDT notes the RC only has to send it to the "local authorities". This seems to be a misuse of the RC resources; every train derailment is an impact event requiring a Disturbance report (is that a commercial train, regional rail line a local trolley car); every teenage prank would also generate an impact event mandating a disturbance report. The SDT defined impact events are not appropriate for use in defining disturbances. There is a big difference from creating a set of guidelines to follow as opposed to creating sanctionable standards
Response: The DSR SDT thanks you for your comment. Furthermore, impact events should not include copper theft or other conditions that pose no threat to the reliability of the BES. A train derailment is only an impact event if it threatens some element of the bulk electric system such as a transmission line corridor - the derailment in itself is not an impact event. See more on impact events under the responses to Question 3.		
Bonneville Power Administration	No	The RC is made aware of these type of incidents and goes right back to incorporating that in their awareness and to focusing on system reliability. If the RC is the recipient for further distribution of information of this type they will be forever going back for more information. Eliminate the middleman in whatever concept you propose, folks have plenty to do now. Let people make good judgments with the direct field people on the seriousness of the breach with their security personnel contacting the appropriate law enforcement agency. (Or are you looking to do a simple RE reports to the RC who marks various category items on a secure website Yes/No category item indicator that can be rolled up in ES-ISAC map board?)
Response: The DSR SDT thanks you for your comment. The Reliability Coordinator's suggested role in this is to allow them to incorporate the relevant data from responsible entities in their footprint for further analysis.		
Duke Energy	No	The RC should not be responsible for submitting the report to FERC, NERC or the RRO. The RC may not have the necessary first hand information concerning the facts of the event. Situation awareness can be maintained by including the RC in the distribution of any sabotage related reporting.

Organization	Yes or No	Question 2 Comment
SERC Reliability Coordinator Sub-committee (RCS)	No	The RC should not be responsible for submitting the report to FERC, NERC or the RRO. The RC may not have the necessary first hand information concerning the facts of the event. Situation awareness can be maintained by including the RC in the distribution of any sabotage related reporting.
Response: The DSR SDT thanks you for your comment. If the reporting hierarchy concept is adopted, it will include controls to ensure timely reporting, clear accountability so that risk of a violation of the standard is not transferred, and a process to ensure the responsible entities' reported information remains as submitted. Also it must result in real effiency gains and support the reliability of the bulk electric system.		
ERCOT ISO	No	There are some events that are truly local and should be handled by local entities and reported to local authorities (i.e. theft). If there is an impact or potential to have an impact to the BES or to the region, then hierarchical reporting would be appropriate.
Response: The DSR SDT thanks you for your comment. We agree - a clearly defined impact event criteria would do just as you suggest - leave local issues on the local level.		
Northeast Power Coordinating Council	No	This is not a standards issue, and NERC should not dictate the reporting structure. It should be left to the RCs and their members.
Response: The DSR SDT thanks you for your comment. In defining a disturbance reporting hierarchy we sought to realize efficencies. If the reporting hierarchy concept is adopted, it must result in real effiency gains and support the reliability of the bulk electric system. It will not be adopted if the result in a complicated or burdensome process for responsible entities.		
MRO's NERC Standards Review Subcommittee	No	We agree a coordinated reporting process is beneficial for the entity and the Reliability Coordinator (RC). However, a hierarchy would likely lengthen the reporting timeframe, or reduce the allotted time for each entity to provide notification to the RC in order to meet DOE or NERC timelines. Communication and coordination with the RC would likely provide more accurate and complete data submissions within a timely process and create shared accountability for the report being submitted.
Response: The DSR SDT thanks you for your comment. If the reporting hierarchy concept is adopted, it will include controls to ensure timely reporting, clear accountability so that risk of a violation of the standard is not transferred, and some mechansim to ensure the responsible entities's reported information remains as submitted.		

Organization	Yes or No	Question 2 Comment
Midwest ISO Standards Collaborators	No	We do not agree with developing a hierarchy for reporting for all disturbances and impacting events. For instance, copper theft is an example of an item that should be reported to the appropriate entities directly by the Transmission Owner. The RC does not need to be made aware of every copper theft unless it has a direct impact on reliability (affects rating, protection system, etc.) and the RC should not be burdened with expending resources for this reporting. A further example in which the hierarchy is not needed would be the case in which only one entity is impacted. If a significant event occurs on one TOP's system, then the TOP should be able to handle the reporting of all entities under its purview. If more than one TOP is involved, then it would be necessary to involve the RC in the reporting.
Response: The DSR SDT thanks you for your comment. The reporting hierarchy concept is meant to apply only to disturbance reporting. We agree that copper theft and other situations that do not pose a direct threat to reliability shouldn't be reported to NERC through this standard.		
FirstEnergy	No	While we appreciate the team's effort to serialize the reporting process, with the electronic communication methods available today, it seems that reporting can be accomplished simultaneously to multiple entities without shifting the burden of reporting to others along the communications path. This is particularly true if the reporting format is standardized to a one-size-fits-all report. Additionally, it would be a great burden to the Reliability Coordinator to review all events perceived by entities to be malicious sabotage events.
Response: The DSR SDT thanks you for your comment. The reporting hierarchy concept would only apply to disturbance reporting, not impact events. The Reliability Coordinator's suggested role in this to allow them to incorporate the relevent datea from responsible entities in their footprint for further analysis. We will consider your suggestion of simulataneous submissions as a means to effectively notify the necessary parties.		
Edison Mission Marketing & Trading	Yes	
PacifiCorp	Yes	
SPS Consulting Group Inc.	Yes	
Calpine Corp.	Yes	A Functional Entity such as a Generator Owner/Operator is not always aware that an event, such as a plant trip, is part of a wider system disturbance that rises to the level of a reportable event under EOP-004. A reporting hierarchy that allows a Generator to report the facts to its Transmission Operator and have that entity take a wider view to determine whether there is a disturbance should facilitate the reporting of actual disturbances. The SDT needs to ensure that some thought goes into the flow of information within the hierarchy and what triggers are needed to drive the reporting up the hierarchy.

Organization	Yes or No	Question 2 Comment
Response: The DSR SDT thanks you for your comment. A reporting hierarchy process must include clear triggers for reporting and provide an efficient, well-defined information flow.		
We Energies	Yes	A hierarchical approach in conjunction with a single, electronic form would provide consistent reporting timelines, provide clarity in the reporting process, and provide more accurate and meaningful data submissions while having shared accountability. Confusion in the current method could be alleviated while providing more consistency in the reporting of an "impact event".
Response: The DSR SDT thanks you for your comment.		
Arizona Public Service Company	Yes	All disturbance reporting should go through the RC.
Response: The DSR SDT thanks you for your comment.		
Constellation Power Source Generation	Yes	As stated in the concept paper, a hierarchy ensures proper communications, but it has the added benefit of reducing redundancy on the Registered Entities, so long as responsibilities and accountability are clearly established.
Response: The DSR SDT thanks you for your comment.		
Central Hudson Gas & Electric	Yes	Central Hudson agrees with this reporting hierarchy for disturbances given the "wider-view" of the Reliability Coordinator as opposed to an entity such as a Transmission Owner or Load-Serving Entity. While, based on past experience, the current process works if reports are filed to the DOE, RRO, and RC simultaneously via email for example. However, the RC is in a better position to identify multi-site incidents and escalate the reporting process if necessary.
Response: The DSR SDT thanks you for your comment.		
Wolverine Power Supply Cooperative, Inc.	Yes	From the perspective of a TOP, this seems to alleviate reporting burden and move it up line. I can understand the logic in wanting the reporting to flow through the RC for awareness purposes, but I can understand the RC's reluctance to bear the additional potential burden. Again, a focused effort to minimize the necessary reporting to 'true impact events" should be kept in mind, regardless of who has to report. Collecting reams of data and figuring out what impact it has later should not be the goal.

Organization	Yes or No	Question 2 Comment
Response: The DSR SDT thanks you for your comment. We agree that regardless of any reporting hierarchy, the goal is to report on disturbances and events with meaningful impact on the bulk electric system. See Question 3 responses for more information on how we view impact events.		
Electric Market Policy	Yes	Having the reporting flow through the Reliability Coordinator supports the reliability objective of assessing, monitoring, and maintaining a wide-area view of the reliability of the Bulk Electric System.
Hydro-Québec TransEnergie (HQT)	Yes	Having the reporting flow through the Reliability Coordinator supports the reliability objective of assessing, monitoring, and maintaining a wide-area view of the reliability of the Bulk Electric System. The reporting hierarchy should be to submit the information to the Reliability Coordinator, and to have the RC submit the report. This would eliminate the duplication of information.
Orange and Rockland Utilities, Inc.	Yes	Having the reporting flow through the Reliability Coordinator supports the reliability objective of assessing, monitoring, and maintaining a wide-area view of the reliability of the Bulk Electric System. The reporting hierarchy should be to submit the information to the Reliability Coordinator, and to have the RC submit the report. This would eliminate the duplication of information.
Response: The DSR SDT thanks you for your comment.		
Lands Energy Consulting	Yes	I would give the RC the authority to establish impact thresholds for reporting. Consistent with my earlier comment, I would set the materiality threshold for disturbance reporting purposes at LSEs (or a combination of LSEs in the case of BPA) serving at least 90,000 customers.
Response: The DSR SDT thanks you for your comment. Reporting thresholds in the standard will meet NERC requirements: Reliability Coordinator's may have different reporting criteria to meet Regional requirements, but they will not appear in this yet to be written Standard.		
Central Lincoln	Yes	In the west at least, this hierarchy should be extended to include BA's as indicated in the Concepts Paper. See: http://www.bpa.gov/corporate/business/reliability/Docs/2007/PNSC_RE_Data_Letter_2_070723.pdf for the RC's policy on which entities it chooses to communicate with.

Organization	Yes or No	Question 2 Comment
Response: The DSR SDT thanks you for your comment. The hierarchy concept includes BAs as appropriate in the reporting structure.		
Luminant	Yes	Luminant believes that one report should be filed with the Reliability Coordinator or one responsible entity, who then files the report with all applicable entities.
Response: The DSR SDT thanks you for your comment.		
Oncor Electric Delivery Company LLC	Yes	Oncor agrees that with this reporting hierarchy, in that dual reporting should be eliminated
Response: The DSR SDT thanks you for your comment.		
Portland General Electric	Yes	PGE is familiar with and works closely with WECC today so the hierarchial consideration makes sense.
Response: The DSR SDT thanks you for your comment.		
Platte River Power Authority	Yes	Situational awareness would be enhanced. All affected entities would be aware of the disturbance and relevant information. Also, the flow of information between entities would be enhanced and a more comprehensive report could be developed.
Response: The DSR SDT thanks you for your comment.		
Ameren	Yes	The hierarchy is appealing in the fact that the TOP/BA will be kept in the loop and receive critical information from the Generators, Distribution, LSE, etc. But there will be an inherent delay in reporting due to the fact that at every hand-off of information there will be questions for additional and/or clarified information, and there is always a possibility for the loss of information due to the transfer from one entity to the next. Further, this reporting through a hierarchy could also take away from the operators ability to respond to system events due to being tied to an information transfer ladder.
Response: The DSR SDT thanks you for your comment. If the reporting hierarchy concept is adopted, it will include controls to ensure timely reporting, clear accountability so that risk of a violation of the standard is not transferred, and some process to ensure the responsible entities' reported information remains as submitted. It must also ensure that it does not place any extra burden on operators that could create an additional risk to reliability.		

Organization	Yes or No	Question 2 Comment
E.ON U.S. LLC	Yes	The hierarchy will simplify reporting from the entity in that the RC is always notified and then the RC notifies other parties as required, (with the exception of OE-417, which still has to be filled out per law) E.ON U.S. recommends that the drafting team pay particular attention to the report process to make sure that duplicate reports are not being required. Currently information on forced outages is already communicated to the RC so formalizing a requirement to provide data to the RC may represent duplication to reports already provided.
Response: The DSR SDT thanks you for your comment. Avoiding duplication is a key goal of the drafting team.		
Public Service Enterprise Group Companies	Yes	The PSEG Companies believe that all entities with a reportable disturbance should report to the RC. The RC is best positioned to evaluate the impact of the event and forward the information to the appropriate entities. There should not be any intermediate entities to relay information to the RC as that can introduce delay and has the potential to introduce transcription errors. Sabotage events should be reported to the RC as well as to law enforcement. CIP-008 reporting is highly specialized and should be retained in the set of cyber security standards, not merged with CIP-001 and EOP-004.
Response: The DSR SDT thanks you for your comment. Detection of cyber events may be specialized but report of them is not. Threats to reliability must be reported no matter what the cause. The DSR SDT proposes using the thresholds found in CIP-008 - this standard would provide a one stop form to submit the information. Note that the current CIP-008 has a reporting requirement to the ES-ISAC only.		
Manitoba Hydro	Yes	The Reporting Concept states that the new hierarchy is, “Affected entity to TOP/ BA to RC. Then the RC will then submit to NERC and DOE (if required)”.This will enhance the existing requirement EOP-004-1 R4 which states that the RC shall assist the affected entity by providing representatives to assist in the investigation (this is also all reiterated in Attachment 1-EOP-004) .In an disturbance, the local resources would be tied up in the rectification of the problem. Analyzing and reporting the event (is it reportable, who to report to, what is the timeline) is distracting and time consuming. By leaving the final upper level steps of reporting to NERC/DOE by the RC would be efficient.
Response: The DSR SDT thanks you for your comment.		
Western Electricity Coordinating Council	Yes	There should be an established time sequence that allows the RC to review the entities material prior to forwarding to NERC. By channeling all reports through the RC situational awareness will be enhanced. Instead of "submit information", it should be clarified that entities submit complete written reports to RC in electronic format.
Response: The DSR SDT thanks you for your comment. If the reporting hierarchy concept is adopted, it will include controls to ensure timely reporting, clear accountability so that risk of a violation of the standard is not transferred, and a process to ensure the responsible entities’ reported information remains as submitted.		

Organization	Yes or No	Question 2 Comment
American Electric Power	Yes	This approach may work as long as there is a uniform process across all of the Reliability Coordinators. AEP owns and operates BES facilities under three separate RCs and having differing rules and processes would create confusion and additional burdens. There are some concerns about the time lag of reporting the information and this might not work well in all cases especially if the information and knowledge are at the local level. AEP recommends that the standard could have a default hierarchy, but this should not prohibit any entity from reporting directly.
Response: The DSR SDT thanks you for your comment. Our goal is uniform reporting criteria to meet specified requirements. We will consider the risks and benefits of allowing a default hierarchical reporting structure with the ability for responsible entities to report directly to NERC.		
Bandera Electric Cooperative, Inc.	Yes	This approach, while I suspect will not be universally agreed to, should provide some definitive guidance in reporting.
Response: The DSR SDT thanks you for your comment.		
Dynegy Inc.	Yes	This seems to be straightforward approach in that the RC is the best judge of threats to the overall system and could eliminate multiple reports of a single event.
Response: The DSR SDT thanks you for your comment.		
Independent Electricity System Operator	Yes	We do not agree with the need of such a hierarchy setup solely for the purpose of making reports to the need-to-know entities. All responsible entities (RC, BA, TOP, etc.) need to file a report. With the proposed set up noted under Q3, which we support, these reports should go directly to NERC. The RC should not be held responsible for forwarding other entities' reports to NERC, and in doing so subject itself to potential non-compliance.
Response: The DSR SDT thanks you for your comment. If the reporting hierarchy concept is adopted, it will include controls to ensure timely reporting, clear accountability so that risk of a violation of the standard is not transferred, and a process to ensure the responsible entities' reported information remains as submitted.		

3. The goal of the DSR SDT is to have one report form for all functional entities (US, Canada, Mexico) to submit to NERC. Do you agree with this change? Please explain your response (yes or no) in the comment area.

Summary Consideration: Most stakeholders agreed with the concept of having one reporting form for all entities.

Several commenters suggested that there is no need for a standard on reporting as they considered it administrative in nature. Most thought it should be a guideline, rather than an enforceable standard.

There is widespread agreement that the one-size-fits-all approach would be very difficult to get agreement on, given the different countries and agencies involved. Many stakeholders pointed out that consistency and simplification were drivers for one report form.

Having multiple recipients, with different information requirements, seem to support an electronic format that would guide information only to those who need it. The concept of an electronic reporting tool would need to be further vetted and developed.

Organization	Yes or No	Question 3 Comment
Bandera Electric Cooperative, Inc.		No preference in this area.
ISO RTO Council Standards Review Committee	No	The SRC supports NERC's initiative for Results Based Standards. The SRC understood RBS to mean the results were reliability based quantities not administrative quantities. There is no need for a NERC Reliability standard on reporting. The idea that all functional entities in each of the said countries will use one form would be a good idea if and only if all the countries and all of their agencies were willing to accept that form. The SRC does not believe that those agencies will be willing to cede what information they ask for to NERC; nor that NERC will be able to create a single form that all such agencies will accept.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements. The set of results-based standards is intended to provide a 'defense-in-depth' approach to protecting reliability of the bulk power system. While many reports are administrative and are only used to assess compliance with specific requirements, the reporting addressed in this project is focused on providing data needed to support		

Organization	Yes or No	Question 3 Comment
after-the-fact analyses of events, and reporting information needed to maintain situaitional awareness. As such, the SDT believes that these reporting requirements do need to be enforceable.		
FirstEnergy	No	While one consistent form for reporting may simplify reporting requirements, it would be very difficult to get all governmental agencies to agree to a one-size-fits all approach.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		
Public Service Enterprise Group Companies	No	While simplification and consistency is a laudable goal, it should not be applied to different governmental agencies (USA, Canada, Mexico) which may have different structures and processes. Moreover, results based standards should not include administrative matters such as reporting forms.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements. The set of results-based standards is intended to provide a 'defense-in-depth' approach to protecting reliability of the bulk power system. While many reports are administrative and are only used to assess compliance with specific requirements, the reporting addressed in this project is focused on providing data needed to support after-the-fact analyses of events, and reporting information needed to maintain situaitional awareness. As such, the SDT believes that these reporting requirements do need to be enforceable.		
American Electric Power	Yes	
Constellation Power Source Generation	Yes	
Exelon	Yes	
PacifiCorp	Yes	
Platte River Power Authority	Yes	

Organization	Yes or No	Question 3 Comment
Calpine Corp.	Yes	A single approach is desirable, particularly for those entities that find themselves in multiple regions or countries.
Response: The DSR SDT thanks you for your comment.		
We Energies	Yes	Agree in conjunction with proposed concept that DOE OE-417 will be allowed to supplement the NERC report in lieu of duplicating entries.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		
Consumers Energy Company	Yes	Agreed - to the extent that it's consistent with the concept that any specific type of data is submitted to ONLY one entity.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		
Arizona Public Service Company	Yes	APS supports the standardization of the form for consistency and format.
Response: The DSR SDT thanks you for your comment.		
Bonneville Power Administration	Yes	As long as we don't make one form that requires extraneous information for the sake of having agreement.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		

Organization	Yes or No	Question 3 Comment
Western Electricity Coordinating Council	Yes	Canadian and Mexican entities should be consulted on content of report form to assure their "buy in".
Response: The DSR SDT thanks you for your comment. It is DSR SDT's intent to discuss the need for information with appropriate jurisdictional agencies.		
Central Hudson Gas & Electric	Yes	Central Hudson agrees with this goal if the intent is to develop and implement an electronic version that would meet DOE requirements as well.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		
E.ON U.S. LLC	Yes	E.ON U.S. supports the proposal.
Response: The DSR SDT thanks you for your comment.		
MRO's NERC Standards Review Subcommittee	Yes	However, We believe the primary goal should focus on "each entity" being able to submit one report for all functional requirements. Entities in the US that are required to submit the DOE OE-417 form should not be required to submit an additional form developed for other entities (Canada & Mexico). One approach to satisfy this goal is for NERC to require all entities (US, Canada, & Mexico) to complete the DOE OE-417 form as their report.
Response: The DSR SDT thanks you for your comment.		
Wolverine Power Supply Cooperative, Inc.	Yes	I can't see how anyone would disagree with this concept - However - I question how practical it will be to implement, since various agencies would have to collaborate and coordinate to accomplish this task.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		

Organization	Yes or No	Question 3 Comment
Lands Energy Consulting	Yes	I think that the impact approach makes sense and that EOP-004 and CIP-001 are logically connected. Many entities of which I am aware link Sabotage Reporting Training to Disturbance Reporting obligation awareness already.
Response: The DSR SDT thanks you for your comment.		
Oncor Electric Delivery Company LLC	Yes	Oncor agrees that by using the same type reporting format, there should be consistency in regard to each functional entity's expectations.
Response: The DSR SDT thanks you for your comment.		
BGE	Yes	One form makes sense to us; less is better is the sense that it makes filing reports easier by not creating unnecessary complications.
Response: The DSR SDT thanks you for your comment.		
Ameren	Yes	One report would be great for this standard. While this standard needs simplification and automation, we strongly suggest developing a guideline for reporting rather than enforceable standards.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements. The set of results-based standards is intended to provide a 'defense-in-depth' approach to protecting reliability of the bulk power system. While many reports are administrative and are only used to assess compliance with specific requirements, the reporting addressed in this project is focused on providing data needed to support after-the-fact analyses of events, and reporting information needed to maintain situaitional awareness. As such, the SDT believes that these reporting requirements do need to be enforceable.		
Portland General Electric	Yes	PGE supports the efforts of the Standards Drafting Team on the SAR for Project 2009-01 to consolidate the disturbance and sabotage reporting processes as outlined in the concept paper.
Response: The DSR SDT thanks you for your comment.		
Dynegy Inc.	Yes	Please keep it short and simple.

Organization	Yes or No	Question 3 Comment
Response: The DSR SDT thanks you for your comment.		
ERCOT ISO	Yes	Standardization ensures consistency and relevance of the information received.
Response: The DSR SDT thanks you for your comment.		
USBR	Yes	The Bureau of Reclamation utilizes a form for tracking unexpected events. This form contains information which the agency considers important for its one reliability improvement program. The form is also used to meet NERC standard requirements for protection system operations analysis. This form contains most of information required by DOE. The SDT should consider requiring the submission of specific information rather than lock responses in one specific form. In this manner the agency would be avoid duplicate forms, one for NERC, the other for agency purposes.
Response: The DSR SDT thanks you for your comment.		
Central Lincoln	Yes	The existing reporting is needlessly complex. We appreciate the SDT's goal.
Response: The DSR SDT thanks you for your comment.		
SPS Consulting Group Inc.	Yes	There should have probably been one report all along.
Response: The DSR SDT thanks you for your comment.		
Duke Energy	Yes	There should only be one report for all functional entities to submit to NERC.
Response: The DSR SDT thanks you for your comment.		
SERC Reliability Coordinator Sub-committee (RCS)	Yes	There should only be one report for all functional entities.
Response: The DSR SDT thanks you for your comment.		
Manitoba Hydro	Yes	This is a promising idea, though there would be different requirements for the three countries, this could easily be rectified with "drop down menus". This electronic form could contain a lot of information without distracting clutter as you "tree" down the menu depending on the event that occurred. This could also contain electronic

Organization	Yes or No	Question 3 Comment
		references to information located in Attachment 1-EOP-004 and Threat and Incident Reporting.
Response: The DSR SDT thanks you for your comment. We will consider your specific suggestions when we develop the reporting requirements.		
Hydro-Québec TransEnergie (HQT)	Yes	We agree with the concept that there should be one report form for all functional entities (whether located in the US, Canada, Mexico) for use in reporting to NERC. This would provide for a consistent reporting format across the continent.
Response: The DSR SDT thanks you for your comment.		
Northeast Power Coordinating Council	Yes	We agree with the concept that there should be one report form for all functional entities (whether located in the US, Canada, Mexico) for use in reporting to NERC. This would provide for a consistent reporting format across the continent.
Response: The DSR SDT thanks you for your comment.		
Orange and Rockland Utilities, Inc.	Yes	We agree with the concept that there should be one report form for all functional entities (whether located in the US, Canada, Mexico) for use in reporting to NERC. This would provide for a consistent reporting format across the continent.
Response: The DSR SDT thanks you for your comment.		
Midwest ISO Standards Collaborators	Yes	We agree with the goal of having a single report form but believe there will be a significant challenge to get varying governmental agencies to agree on single report format.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		
Edison Mission Marketing & Trading	Yes	With the realization that having a common report form may be difficult to coordinate between differen agencies.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide		

Organization	Yes or No	Question 3 Comment
contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		
Independent Electricity System Operator	Yes	Yes, this will simplify the reporting effort. NERC may forward the reports to the other need-to-know entities.
Response: The DSR SDT thanks you for your comment.		
Electric Market Policy	Yes	Yes, we agree with the concept that there should be one report form for all functional entities (whether located in the US, Canada, Mexico) for use in reporting to NERC.
Response: The DSR SDT thanks you for your comment.		

4. The goal of the DSR SDT is to eliminate the need to file duplicate reports. The standards will specify information required by NERC for reliability. To the extent that this information is also required for other reports (e.g. DOE OE-417), those reports will be allowed to supplement the NERC report in lieu of duplicating the entries in the NERC report. Do you agree with this concept? Please explain your response (yes or no) in the comment area.

Summary Consideration: Most stakeholders agreed with the concept of entities being able to use information from other sources such as the OE-417 form, to supplement the NERC report form. Some thought that duplicate reports were acceptable, as long as the information was not duplicated (if # of customers lost is required on form A, don't ask on forms B & C). Several stakeholders commented on the need for an electronic, one stop reporting tool. This would avoid duplication while ensuring that the information reported goes only to intended recipients. With an electronic, one stop reporting tool, reports can be updated/corrected instantly, without repeating previously submitted information. Some stakeholders cautioned that the OE-417 can change every three years and this should be taken into account when developing an electronic reporting tool. Again, such a reporting tool would need to be vetted and developed to meet reliability needs.

Organization	Yes or No	Question 4 Comment
ERCOT ISO		ERCOT ISO agrees with the concept of eliminating the need to file duplicate reports, but as stated in the Concept Paper, the DOE form (OE-417) is required by law. Based on this, the elimination of EOP-004 (after the fact reporting) is essential, since the OE-417 is mandatory and all-inclusive.
Response: The DSR SDT thanks you for your comment. We agree that the OE-417 compiles a baseline set of information for disturbances, however, it does not function as an all-inclusive report of sabotage and cyber security incidents. The DSR SDT certainly seeks to gain effienciencies through the modification of EOP-004 and CIP-001, which may include the elimination of one or both. Further, the OE-417 is only mandatory for US entities.		
Midwest ISO Standards Collaborators	No	It certainly makes sense to eliminate duplication in reporting and to allow supplemental information to be submitted in other reports. However, it does not make sense to require reporting to other governmental agencies through NERC enforceable NERC standards. Those governmental agencies already have legal authority to compel reporting. Again, we support developing a guideline for reporting rather than enforceable standards. The guideline could certainly explain the various reporting requirements and supplemental reporting requirements mentioned in the question without causing the issues we have identified in our comments.
Response: The DSR SDT thanks you for your comment. The DSR SDT does not envision a NERC standard mandating submission of reports to DOE, which is mandatory under Public Law for US entities. If the DSR SDT is able to develop a one-stop-shopping electronic form, we plan to develop an		

Organization	Yes or No	Question 4 Comment
option to have the report submitted to NERC, DOE and FERC simultaneously. If an entity chooses to submit the report manually, they will then also be responsible for following DOE regulations and other mandatory requirements.		
Consumers Energy Company	No	NERC should either coordinate with DOE for a single reporting process or simply adopt the DOE's standard.
Response: The DSR SDT thanks you for your comment. The DSR SDT does not envision a NERC standard mandating submission of reports to DOE, which is mandatory under Public Law for US entities. If the DSR SDT is able to develop a one-stop-shopping electronic form, we plan to develop an option to have the report submitted to NERC, DOE and FERC simultaneously. If an entity chooses to submit the report manually, they will then also be responsible for following DOE regulations and other mandatory requirements. The DOE report does not collect all the information that NERC needs.		
E.ON U.S. LLC	No	Reliability standards are federal law enforced by fines that can reach up to $1,000,000 per day of violation. There is no reason to deliberately include ambiguity, i.e. "gray areas," in requirements such that registered entities are left unable to determine what it is they must do or refrain from doing to remain compliant. "Sabotage" for the purposes of these standards must be defined.
Response: The DSR SDT thanks you for your comment. The intent of the DSR SDT is to develop requirements for reporting that will be clear and unambiguous with respect to compliance issues. Sabotage will be included in the reporting for "impact events", but may not be called 'sabotage' as there are many different interpretations of "sabotage".		
ISO RTO Council Standards Review Committee	No	The concept of eliminating duplication is laudable, but the idea of writing a standard to mandate reporting that involves reporting to governmental areas does not make sense unless NERC will do all of the reporting for the Industry. A governmental agency is as likely as not to change the forms they require which would then mean two different reports (one for NERC and one for the given agency) or that the standard would have to be re-written every time there is a change.
Response: The DSR SDT thanks you for your comment. The DSR SDT does not envision a NERC standard mandating submission of reports to DOE, which is mandatory under Public Law for US entities. If the DSR SDT is able to develop a one-stop-shopping electronic form, we plan to develop an option to have the report submitted to NERC, DOE and FERC simultaneously. If an entity chooses to submit the report manually, they will then also be responsible for following DOE regulations and other mandatory requirements.		
Ameren	No	The DOE OE-417 report should not supplement the NERC report due to the fact that the majority of reportable events are defined in/come from the OE-417 report. The NERC reporting form should be based on the OE-417 report and then include additional reporting requirements defined by NERC. However, it does not make sense to require reporting to the governmental agencies through enforceable NERC standards. The governmental agencies already have legal authority to compel reporting.

Organization	Yes or No	Question 4 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT does not envision a NERC standard mandating submission of reports to DOE, which is mandatory under Public Law for US entities. If the DSR SDT is able to develop a one-stop-shopping electronic form, we plan to develop an option to have the report submitted to NERC, DOE and FERC simultaneously. If an entity chooses to submit the report manually, they will then also be responsible for following DOE regulations and other mandatory requirements.		
SERC Reliability Coordinator Sub-committee (RCS)	No	The requirement should be a single report that satisfies the need for all US governmental agencies as well as NERC and the RRO's.
Response: The DSR SDT thanks you for your comment. The intent of the DSR SDT is to develop standards to address the reliability needs for NERC and not governmental agency reporting criteria.		
Western Electricity Coordinating Council	No	This will work well for the USA entities to save us time in re-entering the same information. We believe that FERC and NERC and the Regions should have one common reporting form for North America. The OE-417 is not required by law outside of the United States. Canadian and Mexican entities may feel that US DOE has no jurisdiction in these countries, and therefore no right to required reporting as is stated on the OE-417.
Response: The DSR SDT thanks you for your comment. We agree that the OE-417 report is not required for Canadian or Mexican entities. The DSR SDT does not envision a NERC standard mandating submission of reports to DOE. If the DSR SDT is able to develop a one-stop-shopping electronic form, we plan to develop an option to have the report submitted (or not) to NERC, DOE and FERC simultaneously. If an entity chooses to submit the report manually, they will then also be responsible for following DOE regulations and other mandatory requirements.		
American Electric Power	Yes	
Edison Mission Marketing & Trading	Yes	
Exelon	Yes	
Orange and Rockland Utilities, Inc.	Yes	
PacifiCorp	Yes	
Platte River Power Authority	Yes	

Organization	Yes or No	Question 4 Comment
Arizona Public Service Company	Yes	APS supports eliminating the need to file duplicate reports. This standardized form should generate and send the DOE OE-417 report, totally eliminating duplicate work. Streamline the process.
Response: The DSR SDT thanks you for your comment.		
Central Hudson Gas & Electric	Yes	Central Hudson agrees with this concept and, as stated in a previous response, recommends that the ability of utilizing the DOE OE-417 to supplement the NERC report be maintained.
Response: The DSR SDT thanks you for your comment.		
Calpine Corp.	Yes	Clarification, simplicity and the removal of duplicate reporting is beneficial.
Response: The DSR SDT thanks you for your comment.		
Constellation Power Source Generation	Yes	Constellation agrees with the concept of eliminating the need to file duplicate reports. If the single NERC reporting form is both comprehensive and easy to use, then using a single report should not be an issue. It is essential that all elements of DOE OE-417, and any similar documents, be incorporated into this single report. Not incorporating all elements will result in gaps in reporting for all Registered Entities.
Response: The DSR SDT thanks you for your comment.		
SPS Consulting Group Inc.	Yes	Duplication is inefficient and casts the whole reporting mechanism in a questionable light.
Response: The DSR SDT thanks you for your comment.		
We Energies	Yes	However, also evaluate whether or not DOE OE-417 is sufficient in lieu of a NERC report. If additional information is required, duplicate format of DOE-OE-417 with additional NERC information listed at the end of the form.
Response: The DSR SDT thanks you for your comment.		
Wolverine Power Supply Cooperative, Inc.	Yes	I agree with the concept of minimizing duplication - See previous question 3 for concerns.
Response: The DSR SDT thanks you for your comment.		

Organization	Yes or No	Question 4 Comment
USBR	Yes	It should be clear what information is to be supplemented. The fewer times the information has to be handled the more efficient the process becomes. If the information exists on a required form, that legal form should be allowed. Also, if the form is already submitted, then reference to it should be sufficient rather than requiring resubmission of the form. That would require handling the information again. As explained in the previous answer, the SDT should recognize that responsible entities have already developed internal reporting processes which utilize forms for consistent responses. Those forms may contain more information than is needed by the new standard to be proposed. The entity should be allowed to submit the internal form or else duplication would be created, which may reduce the effectiveness of an entities reliability improvement program.
Response: The DSR SDT thanks you for your comment. The DSR SDT envisions a one-stop-shopping form that allows reports to be saved, revised and resubmitted at a later date without re-entry of data or information. However, as a caution the DSR SDT cannot guarantee the possibility to submit custom forms.		
Lands Energy Consulting	Yes	Less paperwork and fewer requirements to keep in mind during what may be once in a lifetime events are always good.
Response: The DSR SDT thanks you for your comment.		
Luminant	Yes	Luminant agrees with the concept of reducing reporting requirements, but asks the SDT to go even further. In the concept paper, the SDT discussed that information would not be duplicated on the NERC report and the DOE OE-417 report. The concept paper described a process where one report would simply supplement the other, but two reports would still be filed when required. Can the NERC SDT work with the DOE to develop one report to meet the needs of NERC and the DOE?
Response: The DSR SDT thanks you for your comment. We will consult with the DOE to see if it one report will meet the reporting needs for NERC and the DOE. NERC reliability needs will take precedence.		
Bonneville Power Administration	Yes	Minimizing the number of reports is a good thing. The concept of actually sharing information should be utilized as much as practical.
Response: The DSR SDT thanks you for your comment.		
Oncor Electric Delivery Company LLC	Yes	Oncor agrees that this effort should eliminate file duplication

Organization	Yes or No	Question 4 Comment
Response: The DSR SDT thanks you for your comment.		
Bandera Electric Cooperative, Inc.	Yes	One can only assume the number of reports required in this area will continue to increase in terms of scope and to which agency wants this data. The SDT is encouraged to attempt to find a reporting format and scope that does not needlessly duplicate or complicate overall reporting obligations.
Response: The DSR SDT thanks you for your comment. We will consult with the DOE and FERC to see if it one report will meet the reporting needs for NERC, FERC and the DOE. NERC reliability needs will take precedence.		
Portland General Electric	Yes	PGE supports reducing the duplication of reporting.
Response: The DSR SDT thanks you for your comment.		
Dynegy Inc.	Yes	Short and simple should be the goal.
Response: The DSR SDT thanks you for your comment.		
Duke Energy	Yes	Since the OE-417 is a DOE required report, it must be submitted. Including the OE-417 as part of the NERC electronic form will facilitate reporting to NERC.
Response: The DSR SDT thanks you for your comment. We will consult with the DOE to see if it one report will meet the reporting needs for NERC and the DOE. NERC reliability needs will take precedence.		
Central Lincoln	Yes	The existing reporting is needlessly complex. We appreciate the SDT's goal.
Response: The DSR SDT thanks you for your comment.		
Public Service Enterprise Group Companies	Yes	The PSEG Companies agree with the avoidance of duplicate reports. NERC report forms should not include anything in the DOE form, and NERC Regional report forms should not include anything in the DOE or NERC forms. Hence, a DOE report should not "supplement" a NERC form, but rather replace it unless the NERC form calls for other information for the same reportable incident, and likewise for the DOE - NERC - Regional form structure. DOE forms would be filed with DOE, NERC and the Regional Entity where the event originated. NERC forms would be filed with NERC and the region where the event originated and the Regional form filed only with the Region. In designing the NERC and Regional forms, the need to file multiple reports should be minimized, and in no event should any of the three (DOE, NERC, Region) forms contain

Organization	Yes or No	Question 4 Comment
		duplicative information requests.
Response: The DSR SDT thanks you for your comment. We will consider your comment in the development of the reporting structure / forms.		
Manitoba Hydro	Yes	This could be easily incorporated into the electronic form. You could be prompted for information required immediately, and notified for information that could be entered later. This form could contain all the enterable data that all agencies could require. If the form is live and on line, all entities could be notified (depending on the entries) of an going event immediately. Form could be web based similar to ARS program or even integrated into the ARS program.
Response: The DSR SDT thanks you for your comment. We will consider your comment in the development of the reporting structure / forms.		
FirstEnergy	Yes	We agree that the simplification and consistency of reporting will improve the reporting of this information. We support the drafting team's efforts in this area and hope that all regulatory agencies will as well. However, as we have mentioned in our other comments, the reporting requirements should not be in a reliability standard unless they are proven to be necessary to maintain an Adequate Level of Reliability of the BES. Reporting of these events should be required by NERC in arenas outside of the standards.
Response: The DSR SDT thanks you for your comment. The information provided in the reports is either used after the fact for analyses or used to maintain situational awareness, and is needed for reliability.		
MRO's NERC Standards Review Subcommittee	Yes	We agree with the concept to eliminate duplicate reports. However, we are concerned with the reference of the DOE OE-417 report being a “supplement” of the NERC report rather than “accepted” as the NERC report.
Response: The DSR SDT thanks you for your comment. Future NERC reliability reporting needs may not totally align with DOE report information. Therefore, the OE-417 report would not necessarily substitute for the NERC report. The DOE Reporting Form OE 417 is currently mandatory by Public for US entities.		
Hydro-Québec TransEnergie (HQT)	Yes	We agree with the objective of eliminating duplicate reporting. However, EOP-004 currently allows substitution of DOE OE-417 in place of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report. As suggested in the Concept Paper, entities meeting the criteria of OE-417 are still obligated to file a report with DOE. Given that and the fact that CIP-001 requires no actual reporting, it is not clear where duplication exists today. We agree with the recommendation to eliminate the need for filing duplicate reports such as the DOE form OE-417. There is no benefit with regard to CIP-001 in filing separate reports. Duplicate reports introduce the potential for incomplete information to be supplied to responsible parties.

Organization	Yes or No	Question 4 Comment
		Removing jurisdictional agencies from the Standard, and having NERC provide either query or situational awareness to those agencies being considered, might not be easy to achieve. There is an obligation under law to require entities to report to the DOE on the OE-417 form as amended or modified. This might drive the "omitted" agencies to have reporting laws enacted as well.
Northeast Power Coordinating Council	Yes	We agree with the objective of eliminating duplicate reporting. However, EOP-004 currently allows substitution of DOE OE-417 in place of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report. As suggested in the Concept Paper, entities meeting the criteria of OE-417 are still obligated to file a report with DOE. Given that and the fact that CIP-001 requires no actual reporting, it is not clear where duplication exists today. We agree with the recommendation to eliminate the need for filing duplicate reports such as the DOE form OE-417. There is no benefit with regard to CIP-001 in filing separate reports. Duplicate reports introduce the potential for incomplete information to be supplied to responsible parties. Removing jurisdictional agencies from the Standard, and having NERC provide either query or situational awareness to those agencies being considered, might not be easy to achieve. There is an obligation under law to require entities to report to the DOE on the OE-417 form as amended or modified. This might drive the "omitted" agencies to have reporting laws enacted as well.
Response: The DSR SDT thanks you for your comment. The DSR SDT has discussed the possibility of consolidating CIP-001 and EOP-004 to create a single reporting standard. FERC directives require modifications to the standards which also may impose additional reporting requirements (see paragraph 470 of Order 693). **We concur with your comments regarding the legal obligations to submit certain reports. The DSR SDT is attempting to consult with appropriate governmental aencies to address this.**		
BGE	Yes	We agree with this approach, as long as the latest version of the DOE OE-417 form is fully incorporated in the new single-reporting form, so that it maintains its credibility with the DOE.
Response: The DSR SDT thanks you for your comment. The intent is to maintain credibility with the DOE reporting requirements.		
Independent Electricity System Operator	Yes	We support this concept since it works well for those entities that are not required to file reports with the US agencies, e.g. the DOE.
Response: The DSR SDT thanks you for your comment.		
Electric Market Policy	Yes	Yes, we agree with the objective of eliminating duplicate reporting; however, EOP-004 currently allows

Organization	Yes or No	Question 4 Comment
		substitution of DOE OE-417 in place of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report. As suggested in the Concept Paper, entities meeting the criteria of OE-417 are still obligated to file a report with DOE. Given that and the fact that CIP-001 requires no actual reporting, it is not clear where duplication exists today.
Response: The DSR SDT thanks you for your comment. The DSR SDT has discussed the possibility of consolidating CIP-001 and EOP-004 to create a single reporting standard. FERC directives require modifications to the standards which also may impose additional reporting requirements (see paragraph 470 of Order 693).		

5. In its discussion concerning sabotage, the DSR SDT has determined that the spectrum of all sabotage-type events is not well understood throughout the industry. In an effort to provide clarity and guidance, the DSR SDT developed the concept of an impact event. By developing impact events, it allows us to identify situations in the "gray area" where sabotage is not clearly defined. Other types of events may need to be reported for situational awareness and trend identification. Do you agree with this concept? Please explain your response (yes or no) in the comment area.

Summary Consideration: The majority of stakeholders agreed with the concept of impact events. Some stakeholders felt that the introduction of impact events increased the risk that some items will go unreported. However, most felt that impact events would dramatically increase the number of reports being submitted, and it would be difficult to separate important information from background noise. Several respondents felt that the SDT ignored the FERC Directive, and did not define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event. Many respondents supplied the SDT with their own definition of "Sabotage". The DSR SDT believes that the concept of impact events and the specificity of what needs to be reported in the standard will be an equally efficient and effective means of addressing the FERC directive regarding sabotage. Some stakeholders felt that impact events add another layer of uncertainty to the reporting. Even with the switch from sabotage to impact events, several felt that "intent" was still key to determining reportability.

Organization	Yes or No	Question 5 Comment
ERCOT ISO		ERCOT ISO recognizes the risks associated with "gray areas" not being clarified. While "gray areas" pose compliance risk due to differing interpretations, a risk remains that some items will go unreported. A more prescriptive approach raises an even greater risk of events not being reported. People will not report events that are not specifically listed, and will not use judgment in determining the need for reporting.
Response: The DSR SDT thanks you for your comment. We agree that a more prescriptive approach could pose greater risks but we will attempt to clarify and define an approach to assist the industry and stakeholders for reporting impact events.		
Constellation Power Source Generation	No	Although defining an impact event would bring clarity to defining sabotage events, adding another situation would further complicate things. Furthermore, the examples of impact events used all fall under the Sabotage category in the Threat and Incident Reporting Guideline. Constellation Power Generation suggests the SDT further clarifies the items in the Sabotage category to ensure all grey area situations are included. Clarification is also needed in how a Cyber Security Incident (CIP-008) would map into the categories of Disturbance/Impact Events (CIP-001). To that point, Constellation Power Generation questions whether cyber related incidents should fall under the spectrum of sabotage type events, or remain separate and be incorporated in the CIP revisions. Having cyber related incidents separate from other sabotage events would

Organization	Yes or No	Question 5 Comment
		provide the clarity and guidance that the DSR SDT is striving to achieve.
Response: The DSR SDT thanks you for your comment. We are suggesting the term "Impact Event" be substituted to include all events that would impact the reliability of the BES. Events now included in reporting requirements that do not impact the reliability of the BES would be excluded from the reporting unless the DSR SDT clarifies why it should be included and under what specific instances or examples.		
Duke Energy	No	As FERC ordered in Order No. 693, the drafting team should further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event. Suggested definition: "Sabotage - the malicious destruction of, or damage to assets of the electric industry, with the intention of disrupting or adversely affecting the reliability of the electric grid for the purposes of weakening the critical infrastructure of our nation."
Response: The DSR SDT thanks you for your comment. The SDR SDT struggles with terms that deal with determing "intent" which may not be determined until after a lengthy investigation. We will continue to discuss for inclusion in a future draft of this project. The DSR SDT believes that the concept of impact events and the specificity of what needs to be reported in the standard will be an equally efficient and effective means of addressing the FERC directive regarding sabotage.		
Kootenai Electric Cooperative	No	Impact events seems to add another layer of uncertainty to the reporting. Define a transmission line. Our transmission lines have very little impact on the grid. It is possible for our lines to cause a local area outage on our transmission provider - but neither is of national security interest or even regional interest. There is no power flow going on across the lines other than local power delivery supply. It seems you run more risk of losing the important reports in the snow of reporting - similar to what we have to avoid on our SCADA systems for our operators to see the key information.
Response: The DSR SDT thanks you for your comment. The DSR SDT understands your concern and this was discussed a great deal. It is our belief that criteria of the "impact events" to be reported will be properly defined and discriminated from local events that have no impact on the reliability of the BES.		
SERC Reliability Coordinator Sub-committee (RCS)	No	Impact events that do not affect reliability should not be reported.
Response: The DSR SDT thanks you for your comment. The DSR SDT agrees but a balance must be further explored to meet industry and regulatory requirements specifically under FERC Order 693.		
Luminant	No	Luminant would prefer to report disturbances and sabotage events. The reporting of impact events could lead to unnecessary reporting. A definition of an "impact event" may be even more confusing than sabotage

Organization	Yes or No	Question 5 Comment
		events.
Response: The DSR SDT thanks you for your comment. The DSR SDT understands your concern and this was discussed a great deal. It is our belief that criteria of the "impact events" to be reported will be properly defined and discriminated from local events that have no impact on the reliability of the BES. We are suggesting the term "Impact Event" be substituted to include only events that would impact the reliability of the BES. Events now included in reporting requirements that do not impact reliabiltiy of the BES would be excluded from the reporting unless the DSR SDT clarifies why it should be included and under what specific instances or examples.		
Orange and Rockland Utilities, Inc.	No	Physical and cyber events must be investigated before a determination of sabotage or impact event can be made. Impact events should define or clarify the circumstances that would or could affect reliability. Reportable items should be based on impact to reliability, not on 'newsworthy' events or to gather information for trending. It is the law enforcement industry's responsibility to make a determination of "sabotage" or other. This determination cannot definitively be made by industry (operating) personnel. If NERC's definition is expanded for CIP-001 and/or EOP-004, responsibility and timing of reporting needs to addressed so that appropriate agencies conduct the investigation and assessment. Operating personnel need to remain focused on the primary responsibility of mitigating the effects.
Response: The DSR SDT thanks you for your comment. The SDR SDT struggles with terms that deal with determing "intent" which may not be determined until after a lengthy investigation. We will continue to discuss these ideas for inclusion in a future draft of this project. Timing of the reporting process will be further clarified based upon your comments and those in the industry that have voiced similar concerns.		
MRO's NERC Standards Review Subcommittee	No	Rather than attempting to define a new term (impact event), we suggest that the concept of impact event be replaced with further defining sabotage and providing guidance on trigger events (impact event) that would cause an entity to report.
Response: The DSR SDT thanks you for your comment. We will continue to discuss the FERC "Clarification of sabotage" directive and seek further guidance to meet this directive. The term sabotage has created conflict in its meaning among stakeholders as to when its determined and by whom and how long an investigation would take to make that call on the intent of the saboteur. The DSR SDT is reviewing what a reportable disturbance actually is and sabotage may be a sub component of a reportable disturbance event.		
Lands Energy Consulting	No	The level of complexity described will overwhelm the 20-200 employee utilities that have yet to see - and will never see - the kind of sabotage event that scares the Department of Homeland Security.
Response: The DSR SDT thanks you for your comment. The DSR SDT does not intend for the reporting of impact events to overwhelm smaller entities. If events do not affect the reliability of the BES, then it is our intent that they will be excluded from reporting requirements under our proposal. We will attempt to clarify and define an approach to assist the industry and stakeholders for reporting impact events. FERC cautioned the		

Organization	Yes or No	Question 5 Comment
industry that acts of sabotage may be "tested" on smaller entities and ultimately on larger entities.		
ISO RTO Council Standards Review Committee	No	The nature of the fact that "gray areas" exists preclude the idea of using a standard to report; particularly a standard for the vague topic of motivation such as sabotage events and the more defined disturbance events.
Response: The DSR SDT thanks you for your comment. We will attempt to clarify and define an approach to assist the industry and stakeholders for reporting impact events.		
Edison Mission Marketing & Trading	No	There are too many special circumstances to try and capture. I feel this would be best delivered as a guideline.
Response: The DSR SDT thanks you for your comment. We are suggesting the term "Impact Event" be substituted to include only events that would impact the reliability of the BES. Events now included in reporting requirements that do not impact reliability of the BES would be excluded from the reporting unless the DSR SDT clarifies why it should be included and under what specific instances or examples.		
Exelon	No	We agree with the direction to identify impact events examples that would trigger reporting and not be limited to sabotage reporting only. It is important to note that when an incident occurs, some level of investigation is required before a determination can be made as to the event is sabotage or not. The focus should be on reporting events when they occur and allow follow-up investigations to make the sabotage determination. That being said, care must be taken in the development of any list of impact events so that it doesn't become or is misinterpreted to be a definitive list. Therefore if it is not on the list, it is not reportable.
Response: The DSR SDT thanks you for your comment. We concur and plan to allow reports to be submitted, edited and re-submitted in the one-stop-shopping reporting tool. We are suggesting the term "Impact Event" be substituted for sabotage andinclude only events that would impact the reliability of the BES. Events now included in reporting requirements that do not impact reliability of the BES would be excluded from the reporting unless the DSR SDT clarifies why it should be included and under what specific instances or examples.		
Midwest ISO Standards Collaborators	No	We agree with the idea of identifying impact events but do not support the requirement for these to be always reported through the hierarchical structure identified in question 2. If an impact event only affects one entity, that entity should have the reporting requirement.
Response: The DSR SDT thanks you for your comment. The DSRSDT will continue to explore the benefits and weaknesses of the hierarchy reporting structure.		
Hydro-Québec TransEnergie (HQT)	No	We believe that physical and cyber events must be investigated before a determination of sabotage or impact event can be made. The purpose of the NERC Standards is to maintain the reliability of the BES. Therefore,

Organization	Yes or No	Question 5 Comment
		impact events should define or clarify the circumstances that would or could affect reliability. Reportable items should be based on impact to reliability, not on 'newsworthy' events or to gather information for trending. It is the law enforcement industry's responsibility to make a determination of "sabotage" or other. This determination cannot definitively be made by industry personnel, there is no expertise or time to investigate causes. It is the industry's job to mitigate effects. Examples would help provide for better guidance/direction. Industry examples would be welcomed to help reinforce developed internal processes for compliance.
Northeast Power Coordinating Council	No	We believe that physical and cyber events must be investigated before a determination of sabotage or impact event can be made. The purpose of the NERC Standards is to maintain the reliability of the BES. Therefore, impact events should define or clarify the circumstances that would or could affect reliability. Reportable items should be based on impact to reliability, not on 'newsworthy' events or to gather information for trending. It is the law enforcement industry's responsibility to make a determination of "sabotage" or other. This determination cannot definitively be made by industry personnel, there is no expertise or time to investigate causes. It is the industry's job to mitigate effects. Examples would help provide for better guidance/direction. Industry examples would be welcomed to help reinforce developed internal processes for compliance.
Response: The DSR SDT thanks you for your comment. The SDR SDT struggles with terms that deal with determing "intent" which may not be determined until after a lengthy investigation. We will continue to discuss issues with sabotage for inclusion in a future draft of this project. Timing of the reporting process will be further clarified based upon your comments and those in the industry that have voiced similar concerns.		
American Electric Power	Yes	
Calpine Corp.	Yes	
PacifiCorp	Yes	
Platte River Power Authority	Yes	
Central Lincoln	Yes	An act of vandalism may have impact. An act of sabotage may not be impactful alone, but may be part of a wider coordinated attack. Dictionary definitions speaking of "intent" are not helpful in this regard, since acts of vandalism and sabotage are both generally committed intentionally. Saboteurs, though, work for a higher cause. That cause may be political, social, environmental, etc. We ask that the SDT look beyond dictionary definitions in developing a definition of sabotage.

Organization	Yes or No	Question 5 Comment
Response: The DSR SDT thanks you for your comment. The SDR SDT struggles with terms that deal with determing "intent". The term sabotage has created conflict in its meaning among stakeholders as to when its determined and by whom and how long an investigation would take to make that call on the intent of the saboteur. We will strive to meet this challenge with the input on the right language from government agencies and industry experience expertise.		
Bonneville Power Administration	Yes	BPA agrees with providing an industry-wide definition and guideline. We do NOT agree with requiring reports for every instance of every activity. If your definition is good, you'll get what is needed and not much chaff.
Response: The DSR SDT thanks you for your comment.		
Central Hudson Gas & Electric	Yes	Central Hudson agrees with this concept, particularly if the reporting hierarchy through the RC is implemented in order to better identify trends.
Response: The DSR SDT thanks you for your comment. The DSRSDT will continue to explore the benefits and weaknesses of the hierarchy reporting structure.		
Wolverine Power Supply Cooperative, Inc.	Yes	I agree with the concept of focusing on impact instead of the type of event (sabotage, accident, vandalism, etc.)I hope that the reporting proposal that comes out of this project will clearly make a separation between true impact events that must be reported per the standards (enforceable), vs. "other" information that may be (electively - not enforceable) reported, per some set of guidelines.
Response: The DSR SDT thanks you for your comment. We agree reportable items should be based on impact to reliability and with other commenters that expressed a desire to avoid reporting on 'newsworthy' events but to gather meaningful information for trending. We are suggesting the term "Impact Event" be substituted for sabotage to include only events that would impact the reliability of the BES.		
Bandera Electric Cooperative, Inc.	Yes	In principle, I agree with this concept. Would like for the SDT to pursue this further and seek additional comments at that time.
Response: The DSR SDT thanks you for your comment. We will seek further comments on the concept and will prepare the beginnings of the first draft soon.		
Oncor Electric Delivery Company LLC	Yes	Oncor agrees that there are no broadly used guidance documents that detail how an event may be accurately defined.
Response: The DSR SDT thanks you for your comment. We agree that further industry guidance of a clear and understandable standard should be sought under the new Results Based approach. We will attempt to clarify and define an approach to assist the industry and stakeholders in reporting		

Organization	Yes or No	Question 5 Comment
impact events.		
Portland General Electric	Yes	PGE supports the DSR SDT's efforts to bring clarity and guidance to the spectrum of sabotage-type events.
Response: The DSR SDT thanks you for your comment.		
FirstEnergy	Yes	The concept paper makes good progress in this area and the drafting team is on the right track, and agree that better clarity needs to be developed surrounding sabotage events. However, some of the examples stated in the paper are too vague and do not address extenuating circumstances or reasons for the events. One example sighted in the paper is "Bolts removed from transmission line structures." This statement may be too broad. For instance, if the bolts are removed from the tower and the organization is not experiencing a labor dispute, it could be considered a sabotage event with wide area implications. However, if the organization is in the middle of a labor dispute, this would be vandalism and would most likely not be of a wide area concern. Also, the number and location of towers affected could be an important determination related to the risk the event imposes on the Bulk Electric System.
Response: The DSR SDT thanks you for your comment. We concur with your comments that the number and location of the towers affected may have a "local" vs "wide area" concern. However, under the "impact event" reporting that we are proposing, both scenarios above should be reported as impact events as long as it affects the BES.		
Public Service Enterprise Group Companies	Yes	The PSEG Companies agree with the concept, but reserve judgment on the descriptions of the impacts. There is clearly a need to better define what constitutes a sabotage incident versus common theft or vandalism. Moreover, where it may be impossible to determine if any given incident (e.g., several loose bolts on a transmission tower cross brace could be sabotage or could be human error in construction) falls within sabotage, a registered entity should not be second guessed in an audit if the registered entity determines not to report. Excessive unnecessary reporting can mask real incidents.
Response: The DSR SDT thanks you for your comment. The DSR SDT agrees with clearly defining a reportable impact versus common theft. Concern over reporting an incident and the audit process are within the discussions of the DSR SDT and will be fully explored to assist with the 1st Draft. The ability to identify trends could be very important compared to isolated incidents that do not impact the BES. Every effort to explore this balance of reporting will be taken into account.		
SPS Consulting Group Inc.	Yes	The term sabotage was always too narrow a concept for the standards. At times, questionable activities are not confirmed as sabotage events until well after the fact, forcing the registered entity to speculate on whether or not to report an activity that may not be a confirmed sabotage event at the time, and hence encounter another silly violation based on imprecise terminology.

Organization	Yes or No	Question 5 Comment
Response: The DSR SDT thanks you for your comment. We are suggesting the term "Impact Event" be substituted to include all events that would impact the reliability of the BES. Events now included in reporting requirements that do not impact reliability of the BES would be excluded from the reporting unless the DSR SDT clarifies why it should be included and under what specific instances or examples. Tightening the reporting criteria of impact events could possibly address the concern expressed by a "violation based on imprecise terminology."		
USBR	Yes	There should be a clear distinction between a cyber event and a cyber event that has a material impact on the reliability of the bulk electric system. Not all CIP-008 events will carry such a distinction. That being said, CIP 008 cannot be completely incorporated in this process. Denying access to a cyber asset is noteworthy under CIP008 but may not pose a threat to the reliability of the bulk electric system. Consider recognizing the impact on the bulk electric system when modifying definitions of adding the bulk electric system description to the definitions. This will help to clarify that disturbances, as discussed in this effort, are situations that produce an abnormal condition on the electric power system, not necessarily on ancillary or supporting systems, such as SCADA systems or the water-related systems at hydroelectric dams.
Response: The DSR SDT thanks you for your comment. We are suggesting in our discusssion to consolidate the location of reporting into one standard. The industry has demonstrated by comments that it favors streamlining the reporting process to achieve a "one stop shop" approach. We will continue to explore the possibilities to achieve the best results for all stakeholders. A discussion of advantages /disadvantages will continue to discover options and alternatives with input from all stakeholders.		
Western Electricity Coordinating Council	Yes	This will help eliminate regional differences in sabotage reporting. The definition should be broad enough so it covers new types of sabotage that may evolve. Event analysis facilitates situational awareness and if it requires further investigation regarding developing patterns and severity, it should be handled by law enforcement if need be.
Response: The DSR SDT thanks you for your comment. The DSR SDT will continue to explore the "Impact Event" definition to allow for new types of events. Event analysis is clearly a goal of reporting as is situational awareness and hopefully this project will enhance the understanding and clearly define obligations to all stakeholders.		
Manitoba Hydro	Yes	Though there are some specific events already included in this new definition, more could be added to dissolve specific "gray areas" and as new ones come up. Again these examples could be added into the electronic form and could contain a large data base which would be available depending on the event that occurred.
Response: The DSR SDT thanks you for your comment.		

Organization	Yes or No	Question 5 Comment
BGE	Yes	We agree that "the spectrum of all sabotage-type events is not well understood throughout the industry"; however, we feel that the proposed concept of an "Impact Event" falls short of clarifying what constitutes such events. We believe that "Impact Events" needs further clarification to eliminate "gray areas" and to provide more reporting consistency between entities.
Response: The DSR SDT thanks you for your comment. The DSR SDT will continue to clarify the impact events concept and eliminate "gray areas" while including language to give clarity to the reporting process.		
Dynegy Inc.	Yes	We agree with the concept but please provide specific examples. Also, please consider whether there are any penalties for misinterpreting an incident, who would determine if an event was a threat, and whether this could result in over reporting non-threats.
Response: The DSR SDT thanks you for your comment. The DSR SDT may include specific examples of impact events and types of reportables events in the 1st draft of the standard (or in supplemental guidance) to help illustrate reportable criteria.		
Consumers Energy Company	Yes	We agree with the concept, however, based on the information provided, it may be too vague to be of value. Terms such as "potential" and "significant" can be subjective and therefore provide little direction. We would like to see something more specific. Also, inclusion of the destruction of BES assets may be too inclusive and needs to be restricted to BES assets that will cause a specific level of impact on reliability.
Response: The DSR SDT thanks you for your comment. The SDR SDT struggles with terms that deal with determing "potential" and "significant". Specific examples of criteria is being explored and discussed. We will strive to meet this challenge with the input on the right language from government agencies and industry experience expertise. Your suggestion of restricting to BES assets that will cause a specific level of impact on reliability will be discussed with the DSR SDT.		
Independent Electricity System Operator	Yes	We agree with the general concept. However, we suggest that the classification of "events" to be compatible if not identical to those which need to be reported in real time as required in CIP-001, for otherwise it will create confusion and unnecessary, extra work. Also, this proposal appears to focus on the sabotage-type events only but the SAR deals with both sabotage and other disturbances (e.g. emergency type of events) reporting. A parallel type of "impact event" is needed for non-sabotage-type of events.
Response: The DSR SDT thanks you for your comment. The DSR SDT notes that impacts events include both sabotage and non-sabotage types of events and these events include CIP-001 events.		
Electric Market Policy	Yes	We believe that physical and cyber events must be investigated before a determination of sabotage or impact

Organization	Yes or No	Question 5 Comment
		event can be made.
Response: The DSR SDT thanks you for your comment. We agree that sabotage requires investigation. The term "impact event" was developed to allow immediate reporting of events based on impact to the BES rather than intent.		
We Energies	Yes	We would prefer to refer to all sabotage, vandalism, cyber attacks, and other criminal behavior as impact events. Focusing more on the event's impact on reliability and its ramifications on the systems seems to be more useful than to try to determine the intent of the perpetrator.
Response: The DSR SDT thanks you for your comment. The DSR SDT agrees with your assessment and will pursue the clarity and criteria examples to achieve reporting.		

6. If you are aware of any regional reporting requirements beyond the scope of CIP-001, CIP-008 and EOP-004 please provide them here.

Summary Consideration: Several commenters provided information on regional reporting. The SDT will consider whether these should be included in the continent-wide standard. These include:

1. NPCC maintains a document and reporting form (Document C-17 - Procedures for Monitoring and Reporting Critical Operating Tool Failures) that outlines the reporting requirements, responsibilities, and obligations of NPCC Reliability Coordinators in response to unforeseen critical operating tool failures.
2. For other events that do not meet the OE-417 and EOP-004 reporting criteria, ReliabilityFirst expects to receive notification of any events involving a sustained outage of multiple BES facilities (buses, lines, generators, and/or transformers, etc.) that are in close proximity (electrically) to one another and occur in a short time frame (such as a few minutes).
3. WECC sets its loss of load criteria for disturbance reporting at 200 MW rather than the 300 MW in the NERC reporting form.
4. SERC and RFC are developing additional requirements at this time.
5. We suggest that reporting be based on impact to reliability, not on 'newsworthy' events. We therefore do not agree with such regional efforts and would prefer a continent wide reporting requirements.
6. MISO RC (MISO OP-023) and RFC (PRC-002-RFC-01).

Organization	Question 6 Comment
Central Hudson Gas & Electric	Although not beyond the scope of these standards, NPCC maintains a document and reporting form (Document C-17 - Procedures for Monitoring and Reporting Critical Operating Tool Failures) that outlines the reporting requirements, responsibilities, and obligations of NPCC RCs in response to unforeseen critical operating tool failures.
Response: The DSR SDT thanks you for your comment. The DSR SDT will examine regional reporting criteria and requirements to determine whether it should be included in a continent wide standard.	
Exelon	At the 2010 RFC Spring Workshop the following disturbance reporting Criteria was rolled out: All events that are required to be reported by the OE-417 and EOP-004 criteria will use those published procedures. For other events that do not meet the OE-417 and EOP-004 reporting criteria, ReliabilityFirst expects to receive notification of any events involving a sustained outage of multiple BES facilities (buses, lines, generators, and/or transformers, etc.) that are in close proximity (electrically) to one another and occur in a short time frame (such as a few minutes).

Organization	Question 6 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT will examine regional reporting criteria and requirements to determine whether it should be included in a continent wide standard.	
Lands Energy Consulting	I believe WECC sets its loss of load criteria for disturbance reporting at 200 MW rather than the 300 MW in the NERC reporting form.
Response: The DSR SDT thanks you for your comment. The DSR SDT will consider regional criteria when developing reporting thresholds.	
Edison Mission Marketing & Trading	I don't know of any.
Orange and Rockland Utilities, Inc.	NERC's SDT effort requires a clear, consistent, and comprehensive continent-wide approach, thus mitigating any need for regional reporting requirements.
Response: The DSR SDT thanks you for your comment. The SDR SDT feels in many instances that region specific standards may be needed. However, the SDT will provide a clear reporting standard that can be consistently followed continent-wide.	
MRO's NERC Standards Review Subcommittee	No Comment.
Duke Energy	None
Bandera Electric Cooperative, Inc.	No.
Manitoba Hydro	No.CIP-001 contains references to NERC and the DOE.CIP-008 makes exclusions for facilities regulated by US Nuclear Regulatory Commission and Canadian Nuclear Safety Commission. It also contains references to ES ISAC (Electricity Sector Information Sharing and Analysis Center).EOP-004 contains reference to NERC and DOE. There is no reference to Homeland Security, FBI, etc or to Canadian equivalent references in any of these Standards. When NERC is notified of an event, it is likely other organizations will have to be notified. There should be some sort of consistency to cover all these Standards and all notifiable parties at a NERC Standards level.
Response: The DSR SDT thanks you for your comment. The DSR SDT absolutely understands your provided comment and have had detailed conversations surrounding "who" should be notified and "when". Most importantly, a level of consistency should exist when reporting disturbances and sabotage events negatively impacting the BES.	

Organization	Question 6 Comment
Oncor Electric Delivery Company LLC	Oncor is not aware of any regional reporting requirements beyond the scope of CIP-001, CIP-008 and EOP-004.
Response: The DSR SDT thanks you for your comment.	
Dynegy Inc.	Please consider MISO RTO-OP-023.
Response: The DSR SDT thanks you for your comment. The DSR SDT will examine regional reporting criteria and requirements to determine whether it should be included in a continent wide standard. Please provide a copy of the subject document.	
Electric Market Policy	SERC and RFC are developing additional requirements at this time. We suggest that reporting be based on impact to reliability, not on 'newsworthy' events. We therefore do not agree with such regional efforts and would prefer a continent wide reporting requirements.
Hydro-Québec TransEnergie (HQT)	
Northeast Power Coordinating Council	
Response: The DSR SDT thanks you for your comment. The DSR SDT will examine regional reporting criteria and requirements to determine whether it should be included in a continent wide standard.	
Public Service Enterprise Group Companies	The PSEG Companies believe that RFC is developing a regional disturbance reporting requirement for events not meeting the criteria of current DOE and NERC reports.
Response: The DSR SDT thanks you for your comment. The DSR SDT will examine regional reporting criteria and requirements to determine whether it should be included in a continent wide standard.	
Western Electricity Coordinating Council	There is a need to learn what reporting requirements are required by the Mexican and Canadian entities.
Response: The DSR SDT thanks you for your comment. The DSR SDT is comprised of international members and we are currently researching requirements that Mexico and Canada may have.	
SERC Reliability Coordinator Sub-committee (RCS)	We are not aware of any regional reporting requirements beyond the requirements of CIP-001, CIP-008 and EOP-004. However, the SERC RRO has shared a list of events of interest that it would like to be made aware of to maintain situation

Organization	Question 6 Comment
	awareness.
Response: The DSR SDT thanks you for your comment. The SDR SDT feels there will always be a need for the Regional Entities to be kept aware of certain "hot topic" issues. However, it is the SDT's intent to provide clear and concise reporting requirements for events impacting the BES.	
BGE	We are not aware of any regional requirements beyond the scope of CIP-001, CIP-008 and EOP-004.
Response: The DSR SDT thanks you for your comment.	
We Energies	What is meant by beyond the scope of the referenced standards? We Energies also has reporting obligations with the MISO RC (MISO OP-023), RFC (PRC-002-RFC-01), and the Wisconsin and Michigan Public Service Commissions.
Response: The DSR SDT thanks you for your comment. The DSR SDT will examine regional reporting criteria and requirements to determine whether it should be included in a continent wide standard. Please provide a copy of the subject reporting requirements for the SDT to review.	

7. If you have any other comments on the Concepts Paper that you haven't already provided in response to the previous questions, please provide them here.

Summary Consideration: Several stakeholders provided comments in this section. Some stakeholders suggested that the SDT has gone beyond its approved scope to "further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event." Further, there is no requirement to create a Reporting Standard to define sabotage. The SDT contends that the development of impact events and the reporting requirements for them will provide the clarity sought in the directive.

Other stakeholders suggested that the SDT should seek to retire sanctionable requirements that require event reporting in favor of guidelines for reporting.

Several commenters suggested that the introduction of impact events actually expands the reporting requirements. It should be noted that the list of impact events is expected to be explicit as to who is to report what to whom and within certain timelines.

Several stakeholders provided input as to what they believed an electronic reporting tool should contain:

1 If the decision is made to go to a single reporting form, it should be developed to cover any foreseeable event.

2 The SDT should work toward a single form, located in a central location, and submitted to one common entity (NERC)

3 Reports should be forwarded to the ES-ISAC, not NERC, as the infrastructure is already in place for efficient sharing with Federal agencies, with the regional entities and with neighboring asset owners. Reports should flow to all affected entities in parallel, rather than series (timing issues).

Commenters also suggested that the SDT should consider the impacts of the reporting requirements on the small, and very small utilities.

Organization	Question 7 Comment
BGE	1. If we move to a "one size fits all" single reporting form, it is important that the form be properly developed to cover any foreseeable event, which appears to be the intent of the DSR SDT, as outlined on page 4 of the concept document. Such an approach should also incorporate a single point of contact for reporting information, to avoid any confusion. 2. We would like clarification that any proposed CIP-008-related reporting requirement (including any linked reporting requirement between CIP-008 and CIP-001) is only applicable in situations where the incident/event involves a registered entity's Critical Cyber Asset.

Organization	Question 7 Comment
Response (Questions 3&6): The DSR SDT thanks you for your comment. The drafting team will explore clarification that any proposed CIP-008 related reporting requirement between CIP-008 and CIP-001 is only applicable where the incident/event involves a registered entity's CCA. Note that CIP-002 through CIP-009 are undergoing revision under project 2008-06 – Order 706 SDT. Note that the current CIP-008 has a reporting requirement to the ES-ISAC only.	
Electric Market Policy	a. NERC should focus efforts on developing specific event reporting criteria and not base the requirement on the definition of the term 'sabotage' but on the reporting criteria itself. b. The "opportunities for efficiency" discussed in the Concept Paper would be best achieved by focusing on those items that are necessary to maintain the reliability of the Bulk Electric System. If there are elements that need to be reported that, do not support this objective, than that reporting should not be required in reliability standards.
Hydro-Québec TransEnergie (HQT)	a. NERC should focus efforts on developing specific event reporting criteria and not base the requirement on the definition of the term 'sabotage', but on the reporting criteria itself. See comments above. b. The "opportunities for efficiency" discussed in the Concept Paper would be best achieved by focusing on those items that are necessary to maintain the reliability of the Bulk Electric System. If there are elements that need to be reported that do not support this objective, then that reporting should not be required in reliability standards. Consider making NERC the distributor of reports to other agencies. We recognize that the key is to simplify reporting to a single form, and to the extent possible, to one agency. "Front line" reliability personnel must have the "timely" knowledge to know when a situation warrants local, area, regional, or national involvement. Finally, the SDT should keep in mind the fact that Canadian stakeholders might have some difference in the way reports are made to Security Agencies.
Northeast Power Coordinating Council	a. NERC should focus efforts on developing specific event reporting criteria and not base the requirement on the definition of the term 'sabotage', but on the reporting criteria itself. See comments above b. The "opportunities for efficiency" discussed in the Concept Paper would be best achieved by focusing on those items that are absolutely necessary to maintain the reliability of the Bulk Electric System. If there are elements that need to be reported that do not support this objective, then that reporting should not be required in reliability standards. Consider making NERC the distributor of reports to other agencies. We recognize that the key is to simplify reporting to a single form, and to the extent possible, to one agency. "Front line" reliability personnel must have the "timely" knowledge to know when a situation warrants local, area, regional, or national involvement.
Response: The DSR SDT thanks you for your comment. The DSR SDT agrees to focus efforts to specific event reporting criteria. SDT believes that by reporting material risks to the Bulk Electrical System using the impact event categorization it will be easier to get the relevant information for mitigation, awareness, and tracking, not based on the requirement of defining "sabotage". The SDT believes that it is the submitter's responsibility to submit OE-417 forms to the DOE, as stated by Public Law for US entities. The DSR SDT does recognize that it may not be possible to eliminate	

Organization	Question 7 Comment
reporting to multiple jurisdictional agencies due to legislative or regulatory requirements.	
SPS Consulting Group Inc.	Again, please consider the unique scope of the entities to which these standards are to comply. Don't dump all the requirements on all the applicable entities and perpetuate the current practice of forcing them to parse the requirements into what is logical or illogical from their perspective. The drafting team should have the expertise to do this. Identify which requirements apply to which applicable entity.
Response: The DSR SDT thanks you for your comment. The DSR SDT will take into consideration what registered entities and thresholds are to be included in the revised standard(s) based on the SAR. The DSR SDT will establish the "requirements necessary for users, owners, and operators of the Bulk-Power-System" as stated in FERC Order 693 and the difference in reporting of events on the BES, as stated in the Purpose statement of EOP-004-1.	
ERCOT ISO	All references to CIP-008 should be removed and we reassert that physical and cyber reporting should be separate. There is documentation available from the CIPC that the drafting team considered CIP-001 related physical sabotage reporting and specified cyber incident reporting requirements in CIP-008.ERCOT ISO requests the DSR SDT to continue to improve its guidelines and to post those guidelines for all to use, but not to create sanctionable standards whose good intentions could result in unintended adverse consequences for the Industry. ERCOT ISO also suggests that all reporting forms and guidance should be located in a central, easily accessible location, eliminating confusion and simplify reporting for system operators thereby directly enhancing reliability during system events. The industry would benefit from a central location or link on the NERC website containing all reporting forms.
Response: The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if the DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has not determined at this time what bright line will be used for the yet to be drafted Standard(s). The DSR SDT will take into consideration your comment on keeping cyber and physical events separate. We are suggesting in our discussion to consolidate the location of reporting into one standard. The industry has demonstrated by its comments that it prefers that the reporting process be streamlined to achieve a "one stop shop" approach. We will continue to explore the possibilities to achieve the best results for all stakeholders. A discussion of advantages /disadvantages will continue to discover options and alternatives with input from all stakeholders.	
Western Electricity Coordinating Council	As stated previously, for "One stop shopping" we need "buy in" from the foreign nationals. The way to do this is to engage their opinions and respect their jurisdictional agencies as well.
Response (Question 6): The DSR SDT thanks you for your comment. The DSR SDT does recognize that it may not be possible to eliminate reporting to multiple jurisdictional agencies due to legislative or regulatory requirements. The SDT acknowledges that it is possible to consolidate various reports that ask repetitive questions and through this process can work with foreign nationals to receive their "buy in" for a one report form for all functional entities to submit to NERC.	

Organization	Question 7 Comment
MRO's NERC Standards Review Subcommittee	Confusion often arises in the industry between the CIP standards and other reliability standards based on CIP-001 naming convention. We would suggest the SDT retire CIP-001 and incorporate requirements within the EOP-004 standard or a new EOP-xxx standard to avoid confusion rising from CIP and other NERC Reliability Standards. Additionally, we assume the SDT has been created to specifically address FERC Order 693 directives to the ERO which appears to include the following items: 1. Applicability - "possible revisions to CIP-001-1 that address our concerns regarding the need for wider application of the Reliability Standard... the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate" (FERC, 2007, para. 460). 2. Definition of Sabotage - "we direct that the ERO further define the term and provide guidance on triggering events that would cause an entity to report an event... we believe the term sabotage is commonly understood and that common understanding should suffice in most instances... the ERO should consider FirstEnergy's suggestions to differentiate between cyber and physical sabotage and develop a threshold of materiality." (FERC, 2007, para. 461-462) 3. Periodic Review and Testing - "directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures." (FERC, 2007, para. 466) 4. Redundant Reporting - "now direct the ERO to address our underlying concern regarding mandatory reporting of a sabotage event... Regarding the potential for redundant reporting under CIP-001-1 and other government reporting standards, and the need for greater coordination... We direct the ERO to explore ways to address these concerns - including central coordination of sabotage reports and a uniform reporting format... with the appropriate governmental agencies that have levied the reporting requirements." (FERC, 2007, para. 468-469) 5. Specified Time - "the Commission directs the ERO to modify CIP-001-1 to require an applicable entity to contact appropriate governmental authorities in the event of sabotage within a specified period of time... the ERO should consider suggestions raised... to define the specified period for reporting an incident beginning from when an event is discovered or suspected to be sabotage" (FERC, 2007, para. 470). 6. Summary of CIP-001-1 - "the Commission directs the ERO to develop the following modifications... (1) further define sabotage and provide guidance as to the triggering events... (2) specify baseline requirements regarding... procedures for recognizing sabotage events... (3) incorporate a periodic review... and for the periodic testing... (4) require an applicable specified period of time. In addition... address our concerns regarding applicability to smaller entities... consolidation of the sabotage reporting forms and the sabotage reporting channels with the appropriate governmental authorities to minimize the impact of these reporting requirements on all entities." (FERC, 2007, para. 471) 7. Analyze Performance - "at a minimum, generator operators and LSEs should analyze the performance of their equipment and provide the data... The Commission directs the ERO to consider this concern in future revisions... that includes any Requirements necessary for users, owners and operators... to provide data that will assist NERC" (FERC,

Organization	Question 7 Comment
	2007, para. 613, 617). 8. Reporting Time Frames - "The Commission directs the ERO to change its Rules of Procedures to assure that the Commission also receives these reports within the same time frames as the DOE." (FERC, 2007, para. 618)
Response: The DSR SDT thanks you for your comment. The DSR SDT agrees with your comments to specifically address FERC Order 693 directives to the ERO and will determine a prudent course of action with respect to these standards and pursue the suggestion to retire CIP-001 and incorporate requirements within the EOP-004 standard to avoid confusion rising from CIP and other NERC Reliability Standards.	
Constellation Power Source Generation	Constellation Power Generation would like clarification that any proposed CIP-008-related reporting requirement (including any linked reporting requirement between CIP-008 and CIP-001) is only applicable in situations where the incident/event involves a registered entity's Critical Cyber Asset. In that vein, we want to emphasize the importance of the DSR SDT working with the CIP SDT on the cyber related events. If the DSR SDT is going to be adding clarity to cyber related events, then coordination with the CIP SDT is needed to ensure the same verbiage is being used. Furthermore, having any duplication of requirements will cause a double jeopardy scenario which would go against the SAR for the DSR SDT. As stated earlier, Constellation Power Generation also questions whether cyber related incidents should fall under the spectrum of sabotage type events, or remain separate and be incorporated in the CIP revisions.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has not determined at this time what bright line will be used for the yet to be drafted Standard(s). Note that CIP-002 through CIP-009 are undergoing revision under project 2008-06 – Order 706 SDT.	
We Energies	Give consideration to combining CIP-001 and EOP-004-1 through a common categorization. For example, "System Risk Reporting" could encompass both actual and potential events and would minimize the need to cross reference both standards, and provide one location for event and potential-event reporting. Much of the challenge in this project is in achieving a common understanding of the words sabotage and terrorism. There are nuances of meaning in the words that imply a relationship between the attacker and the victim, or a motive other than simple profit or mischief. This nuance of meaning requires the victim of the damage to discern a relationship or motive which may not be discoverable in the relatively brief time window during which the entity must report the event. In fact, they may never be known. Consequently, We Energies recommends elimination of the words sabotage and terrorism from these standards. We also recommend elimination of the word vandalism since it also implies an ability and duty to discern whether a particular act (barbed wire thrown over transformer bushings) was done out of pure mischief (vandalism) or with intent to destroy equipment for a political purpose (terrorism). And if the act was committed by a disgruntled employee, it becomes sabotage. No wonder there is confusion and indecision. Instead, We Energies recommends using the simple words "criminal damage". One need not be a prosecuting attorney or FBI Special Agent to know what this means. Simply ask, "Does is look like somebody damaged it (or hacked in) intentionally?" and, "Did we give consent?" and you're done. With

Organization	Question 7 Comment
	elimination of sabotage, terrorism and vandalism, and all of their baggage, comes the ability to integrate both CIP 001 and EOP 004. We now have criminal damage (or cyber attack) as just another event to be evaluated against certain pre-defined impact measures. No value judgments, no speculation. Another benefit of using these simple words and tests is that operating personnel, whether in the field or at the console, will not require special awareness training in discerning these nuances of meaning. They already have experience with the equipment or cyber systems and its normal performance. Operating personnel can readily assess whether an impact event is due to equipment failure, weather or animal contact vs. intentionally caused by a person. If it appears to be criminal damage, call the local police agency. Report the event and the impact. Cooperate with the investigation. Share your knowledge of the normal condition of the equipment or performance of the system. Share your experience with similar events. It will be important to highlight that the theft of all the grounding pigtails in a substation is different from the act of simply snipping each of them to leave the equipment electrically floating. The technical condition is the same, but this allows the police to make an inference with respect to motive, suspect profile, sophistication, etc. That's their job. They may ask us to speculate on the motive or skills of the attacker. That's okay. But at least we don't have to know or guess at it for the purpose of determining whether to report the event. No training required. With respect to notification to the FBI, We Energies recommends that the standard merely state that the owner of the damaged asset ensure the local office of the FBI is notified. The standard should permit documentation of either a direct phone call by the asset owner or obtaining an assurance from the local police that they will do so. There should be no need to prove earlier establishment of a relationship with the FBI. There should be no expectation that the entity have a signed letter from the FBI Special Agent in Charge acknowledging his agency's duty. This document means nothing. With respect to reporting within the industry, We Energies recommends that the only events to be reported "up the chain" are those that we choose to characterize as "impact events". That is, the events that meet some measurable threshold with respect to BES impact. We should describe these efficiently to avoid over-reporting of trivial events. It is apparent that we are already over-reporting since DHS HITRAC recently fed back to the industry that copper thieves attacked a substation in San Bernardino, CA taking some of the grounding conductors. The industry should have the option to report non-impact events that are unusual in some respect and which may have some mutual industry benefit in terms of prevention, awareness or recovery. Attack attempts with no impact, or observations of suspicious activity could fall into this optional category. These optional reports could be aggregated by the entity for the purpose of detecting patterns or trends, or be reported ad hoc. The ES-ISAC should be the recipient of the reports. It should be the single point of contact since it has the industry insight, engineering expertise and cross-sector relationships to analyze and return valuable intelligence to the industry. With the ES-ISAC as the recipient of the reports, efficient sharing with Federal agencies, with the regional entities and with neighboring asset owners could be automated and rapid. There is much benefit to be gained from this project, primarily in the area of creating clarity and uniformity. There is some risk that the reporting requirements will become onerous and prescriptive.
Response: The DSR SDT thanks you for your comment. The DSR SDT is proposing to consolidate disturbance and event reporting under a single standard. The DSR SDT believes that reporting material risks to the Bulk Electrical System by using the impact event categorization, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation by the elimination of the term "sabotage". The intent is to allow potentially impacted parties to prepare for and possibly mitigate the reliability risk. The NERC Rules of	

Organization	Question 7 Comment
Procedure (section 800) provides an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for reliability. The SDT is proposing that the new standard specify who has access to reported information and who should be notified about impact events, because agencies such as the DHS and FBI have other duties and responsibilities - an impact event that is related to copper theft may only need to be reported to the local law enforcement authorities. The goal of the DSR SDT is create clarity and uniformity by developing a single reporting form for all functional entities without regard to nationality (US, Canada, Mexico) to submit to NERC with guidance. Ideally, entities would complete a single form, which could then be distributed to jurisdictional agencies and functional entities as appropriate. The DSR SDT agrees with your assessment that there should be no expectation that the entity have a signed letter from the FBI Special Agent.	
Bandera Electric Cooperative, Inc.	I commend the SDT for working on this effort and wish them success.
Response: The DSR SDT thanks you for your comment.	
Public Service Enterprise Group Companies	If reporting does become the responsibility of the Reliability Coordinators, the RCIS should be made available view-only to registered entities with a notification when RC's have posted new entries. That will enhance the situational awareness of registered entities. The PSEG Companies disagree with inclusion of CIP-008 reporting requirements as part of the CIP-001 and EOP-004 initiative. CIP-008 reporting as part of the cyber security set of NERC standards is usually managed by specialized corporate organizations separate from those involved with the other NERC standards, and with highly specialized cyber skill sets. CIP-008 reporting requirements should remain where they are, and any perceived need for improvement addressed in the ongoing CIP Version 4 development process.
Response: The DSR SDT thanks you for your comment. The RCIS is a real-time communication and reporting tool and is outside the scope of the SDT. The goal of the DSR SDT is to develop a form to expedite report completion, sharing and storage. Ideally, entities would complete a single form, which could then be distributed to jurisdictional agencies and functional entities as appropriate. Functional entities may include the RC, TOP, and BA for situational awareness. The DSR SDT will take into consideration your comment with inclusion to CIP-008 reporting. However, the drafting team will explore clarification that any proposed CIP-008-related reporting requirement between CIP-008 and CIP-001 is only applicable where the incident/event involves a registered entity's CCA. Note that CIP-002 through CIP-009 are undergoing revision under project 2008-06 – Order 706 SDT.	
Independent Electricity System Operator	In the Background Section of the comment form, it is indicated that the SDT "...is NOT seeking input or guidance on the definition of physical or cyber sabotage, what type of disturbances should be reported, who should do reporting, or to whom or what organizations will be receiving the reports." Yet there are proposed definitions, with examples, in the concept paper. The SDT should make it absolutely clear that by supporting the general concept as described in the paper, the commenting entities are not endorsing the proposed definitions, nor the examples as elements to be included in the standard.

Organization	Question 7 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT will continue to clarify the impact events concept and eliminate "gray areas" while including language to give clarity to the reporting process. Standards developed under this project will be posted for comment on specific content.	
Luminant	Luminant disagrees with the direction of utilizing impact events, as this is an expansion in scope beyond the simplification of sabotage and disturbance reporting.
Response: The DSR SDT thanks you for your comment. We are suggesting the term "Impact Event" be substituted to include only events that would impact the reliability of the BES. The DSR SDT has reviewed the existing standards, the SAR; issues from the NERC database and FERC Order 693 Directives and determine this was a prudent course of action with respect to these standards to provide clear criteria for reporting.	
Dynegy Inc.	N/A
Manitoba Hydro	No
Edison Mission Marketing & Trading	No other comments.
SERC Reliability Coordinator Sub-committee (RCS)	None.
USBR	The concept of "threat" evaluation criteria is somewhat vague and a great care is needed to ensure it is clear enough that the most individuals would be able to analyze an event and end up at the same threat. Otherwise it would be almost impossible to ensure compliance with a requirement which cannot accurately describe criteria to be used to ensure that proper evaluation has occurred.
Response: The DSR SDT thanks you for your comment. We are suggesting the term "Impact Event" be substituted to include only events that would impact the reliability of the BES as opposed to requiring a threat evaluation. The DSR SDT intends to develop criteria that will assist entities in determining which events should be reported.	
Wolverine Power Supply Cooperative, Inc.	The concepts of removing duplication, consolidation, and focusing on "impact events" sound logical. I am concerned that the focus may drift to expanded reporting, not reduced reporting.
Response: The DSR SDT thanks you for your comment. The DST SDT discussed the reporting of "impact events" and will consider guidance found in the document, "NERC Guideline: Threat and Incident Reporting" which will include clear criteria to eliminate erroneous or expanded reporting.	

Organization	Question 7 Comment
ISO RTO Council Standards Review Committee	The FERC Order merely asked NERC to "further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event." There is no requirement to create a Reporting Standard and no mention of Disturbance events. There is a strong need to avoid heavy-handed use of NERC standards particularly for such post event reporting guidelines. The SRC would urge the DSR SDT to continue to improve its guidelines and to post those guidelines for all to use, but not to create sanctionable standards whose good intentions will inevitably result in many unintended adverse consequences for the Industry. Rather, the SDT should seek to retire sanctionable requirements that require event reporting in favor of guidelines for reporting.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if the DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has not determined at this time what bright line will be used for the yet to be drafted Standard(s). The DSR SDT will take into consideration your comment on keeping cyber and physical events separate. We are suggesting in our discussion to consolidate the location of reporting into one standard. The industry has demonstrated by its comments that the reporting process be streamlined to achieve a "one stop shop" approach. We will continue to explore the possibilities to achieve the best results for all stakeholders. A discussion of advantages /disadvantages will continue to discover options and alternatives with input from all stakeholders.	
Lands Energy Consulting	The lack of common sense that leads to a 15 MW loss of load resulting from a 115 kV line outage being categorized as a "reportable disturbance" really hurts the credibility of the entire NERC Compliance Program. The smaller utilities look at application of EOP-004 in particular to their operation and conclude that either the EO/RRO is: a. stupid; or b. Out to persecute the smaller utilities. In reality, EOP-004 was drafted for application to Southern California Edison, where loss of 50% of customers would be 2-3 million customers. Now that's really disturbing!
Response: The DSR SDT thanks you for your comment. The DSR SDT intends to develop criteria that will assist entities in determining which events should be reported. Acts of sabotage may be "tested" on smaller entities before the saboteurs move on the larger entities.	
Central Hudson Gas & Electric	The NERC Guideline: Threat and Incident Reporting Attachment A matrix is an extremely beneficial document that organizes reporting criteria. However, it identifies communications systems failure sub-category under the Equipment And/Or Systems Failure category as reportable with a reference to OE-417 - Schedule 1, Item 10. Item 10 on Schedule 1 addresses only failures due to attacks (not failures for other reasons).
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if the DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has not determined at this time what bright line will be used for the yet to be drafted Standard(s). Loss of communications would be considered an impact event. The reason for the loss of communications is irrelevant.	

Organization	Question 7 Comment
Duke Energy	We don't think CIP-001, EOP-004 and cyber incident reporting aspects of CIP-008 should all be combined into one standard, because of the significant differences between sabotage and disturbances. We have suggested that the drafting team further define sabotage, and we have included a suggested definition in our response to question #5 above. Sabotage is very specific due to the intent (for the purpose of weakening the critical infrastructure), and the potential impact to the BES. We believe that sabotage and cyber incident reporting should remain a part of the CIP Standards due to the emphasis placed on the criticality and vulnerability of the assets needed to support reliable operation of the BES. Cyber Security and Physical Security could be placed together in the same standard (remain in CIP) and other disturbances (i.e., accidental, natural) in a separate standard. "One stop shopping" for reporting is still possible as long as the OE-417 form is included as part of the NERC electronic form. And while we agree with the need for additional clarity in sabotage and disturbance reporting, we believe that the Standards Drafting Team should carefully consider whether there is a reliability-related need for each requirement. Some disturbance reporting requirements are triggered not just to assist in real-time reliability but also to identify lessons-learned opportunities. If disturbance and sabotage reporting continue to be reliability standards, we believe that all linkages to lessons-learned/improvements need to be stripped out. We have other forums to identify lessons-learned opportunities and to follow-up on those opportunities.
Response: The DSR SDT thanks you for your comment. The DSR SDT is still evaluating inclusion of CIP-008 reporting requirements with CIP-001 and EOP-004 requirements, Note that the current CIP-008 has a reporting requirement to the ES-ISAC only. The DSR SDT developed the more inclusive term "impact events" to eliminate using more confusing terms like sabotage (which is not likely to be determined until after a lengthy investigation). These standards may be combined to have all reporting requirements in a single standard, not because the items to be reported are necessarily related.	
FirstEnergy	We fully agree that sabotage events need to be more clearly defined and reporting requirements need to be better coordinated. But as we have stated in previous comments, the drafting team needs to determine if standard requirements need to be developed for this type of reporting or if this is better left to administrative requirements outside the standards arena. Also, while we appreciate the team's effort to simplify reporting requirements for entities, we are concerned with the serial communication offered by the concept paper. As an example, the team proposes to have LSE report the incident to the BA and/or TOP and then have the BA and/or TOP report it to the RC and the RC to report it to NERC and the NERC report to the regulatory agencies. While this simplifies it for each individual organization, this method introduces many opportunities for errors and miscommunications. Since this is after-the-fact reporting, it is difficult to defend this type of communication path when one consistent report could be sent simultaneously to all agencies at the same time from the originating location.
Response: The DSR SDT thanks you for your comment. The Reliability Coordinator's suggested role in this is to allow them to incorporate the relevant data from responsible entities in their footprint for further analysis. We will consider your suggestion of simultaneous submissions as a means to effectively notify the necessary parties. The SDT believes that it is the submitter's responsibility to submit OE-417 forms to the DOE. The DSR SDT does recognize that it may not be possible to eliminate reporting to multiple jurisdictional agencies due to legislative or regulatory	

Organization	Question 7 Comment
requirements.	
Ameren	While we are not opposed to the concept of identifying impact events, we are concerned that the drafting team may actually be expanding reporting requirements. We do not support expansion of reporting requirements unless a clear reliability or legal need is identified. Some of the impact events are almost never sabotage and do not warrant reporting for reliability needs and should not be included. For example, copper theft should not require reporting, in general, because it is almost never sabotage and rarely impacts reliability. If it does, impact reliability because, for example, the protection system is impacted and causes more significant potential contingencies, then reporting could be required. Why is a train derailment near a transmission right of way significant? It would only be significant if an investigation identified sabotage as the reason. Furthermore, what is considered near?
Midwest ISO Standards Collaborators	While we are not opposed to the concept of identifying impact events, we are concerned that the drafting team may actually be expanding reporting requirements. We do not support expansion of reporting requirements unless a clear reliability or legal need is identified. Some of the impact events are almost never sabotage and do not warrant reporting for reliability needs and should not be included. For example, copper theft should not require reporting, in general, because it is almost never sabotage and rarely impacts reliability. If it does impact reliability because, for example, the protection system is impacted and causes more significant potential contingencies, then reporting could be required. Why is a train derailment near a transmission right of way significant? It would only be significant if an investigation identified sabotage as the reason. Furthermore, what is considered near?
Response: The DSR SDT thanks you for your comment. It is not the intent of the DSR SDT to expand reporting requirements but rather to attempt to clarify and define an approach to assist the industry and stakeholders in reporting impact events. Furthermore, impact events should not include copper theft or other conditions that pose no threat to the reliability of the BES. A train derailment is only an impact event if it threatens some element of the power system such as a transmission line corridor - the derailment in itself is not an impact event.	
Exelon	You should consider providing clear and concise instructions as to the expectation on submitting forms, i.e. the DOE 417. There should be no guessing as to when and how reports should be submitted and who should receive them. Specific details on reporting criteria should be included.
Response : The DSR SDT thanks you for your comment. The DSR SDT intends to develop criteria for reporting impact events.	

Consideration of Comments on Disturbance and Sabotage Reporting — Project 2009-01

The Disturbance and Sabotage Reporting Drafting Team thanks all commenters who submitted comments on its preliminary draft of EOP-004-2 – Impact Event and Disturbance Assessment, Analysis, and Reporting. This standard was posted for a 30-day informal comment period from September 15, 2010 through October 15, 2010. Stakeholders were asked to provide feedback on the standard through a special Electronic Comment Form. There were 60 sets of comments, including comments from more than 175 different people from approximately 100 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

In this report, the comments have been sorted by question number so that it is easier to see where there is consensus. The comments are posted in their original format on the following project page:

http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Based on stakeholder comments, and also on the results of the observations made by the Quality Review team, the drafting team made the following significant changes to the standard following the posting period that ended on October 15, 2011.

Scope: A common thread through most of the comments was that the DSR SDT went beyond the reliability intent of the standard (reporting) and concentrated too much on the analysis of the event. The DSR SDT agrees with this response, and revised the purpose as follows:

> *Original Purpose:* Responsible Entities shall report impact events and their known causes to support situational awareness and the reliability of the Bulk Electric System (BES).
>
> *Revised Purpose:* To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of Impact Events and their causes, if known, by the Responsible Entities.

Definitions:

> **Impact Event:** The DSR SDT had proposed a working definition for "impact events" to support EOP-004 - Attachment 1 as follows:
>
> "An impact event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action."
>
> Many stakeholders indicated that the definition should be added to the NERC Glossary and the DSR SDT adopted this suggestion.
>
> The types of Impact Events that are required to be reported are contained within EOP-004 - Attachment 1. Only the events identified in EOP-004 – Attachment 1 are required to be reported under this Standard.
>
> **Sabotage:** FERC Order 693, paragraph 471 states in part: ". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide

guidance as to the triggering events that would cause an entity to report a sabotage event."

The DSR SDT made a conscious, deliberate decision to exclude a strict definition of sabotage from this standard and sought stakeholder feedback on this issue. Some suggested adopting the NRC definition of the term sabotage, and the DSR SDT did consider adopting the NRC definition shown below but determined that the definition is too narrowly focused.

Any deliberate act directed against a plant or transport in which an activity licensed pursuant to 10 CFR Part 73 of NRC's regulations is conducted or against a component of such a plant or transport that could directly or indirectly endanger the public health and safety by exposure to radiation.

Most respondents agreed that in order to be labeled as an act of sabotage, the intent of the perpetrators must be known. The team felt that it was almost impossible to determine if an act or event was that of sabotage or merely vandalism without the intervention of law enforcement after the fact. This would result in further ambiguity with respect to reporting events, and the timeline associated with the reporting requirements does not lend itself to the in-depth analysis required to identify a disturbance (or potential disturbance) as sabotage. The SDT felt that a likely consequence of having to meet this criterion, in the time allotted, would be an under-reporting of events. Accordingly, all references to sabotage have been deleted from the standard.

Instead, the SDT concentrated on providing clear guidance on the events that should trigger a report. The SDT believes that this more than adequately meets the reliability intent of the Commission as expressed in paragraph 471 of Order 693 in an equally efficient and effective manner.

Situational Awareness versus Industry Awareness: Some commenters correctly pointed out that "situational awareness" is a desirable by-product of an effective event reporting system, and not the driver of that system. Accordingly, all references to "situational awareness" have been deleted from the standard. The more generic "industry awareness" has been substituted where appropriate.

Applicability:

The DSR SDT had protracted discussions on the applicability of this standard to the LSE. Per the Functional Model, the LSE does not own assets and therefore should not be an applicable entity (no equipment that could experience a "disturbance"). However, the Registry Criteria contains language that could imply that the LSE does own assets, or is at least responsible for assets. In addition, the DSR SDT modified Attachment 1 to include reporting of damage or destruction of Critical Cyber Assets per CIP-002. The LSE, as well as the Interchange Authority and Transmission Service Provider are applicable entities under CIP-002 and should be included for Impact Events under EOP-004.

There were several comments that the asset owners (GO/TO) would be less likely than the asset operators (GOP/TOP) to be aware of an impact event. The DSR SDT recognizes that this may be true in some cases, but not all. In order to meet the reliability objectives of this requirement, the applicability for GO/TO will remain as per Attachment 1.

Requirement R1:

Based on stakeholder comments, Requirement R1, which assigned the ERO the responsibility for collecting and distributing impact event reports was deleted. There was strong support for a central system for receiving and distributing impact event reports (a/k/a one stop shopping). There was general agreement that NERC was the most likely, logical entity to perform that function. However several respondents expressed their concern that the ERO could not be compelled to do so by a requirement in a Reliability Standard (not a User, Owner or Operator of the BES). In their own comments, NERC did not oppose the concept, but suggested that the more appropriate place to assign this responsibility would be the NERC Rules of Procedure. The DSR SDT concurs. The DSR SDT has removed the requirement from the standard and is proposing to make revisions to the NERC Rules of Procedure as follows:

> 812. NERC will establish a system to collect impact event reports as established for this section, from any Registered Entities, pertaining to data requirements identified in Section 800 of this Procedure. Upon receipt of the submitted report, the system shall then forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, and regulatory agencies as necessary. These reports shall be forwarded to the Federal Energy Regulatory Commission for impact events that occur in the United States. The ERO shall solicit contact information from Registered Entities appropriate governmental, law enforcement and regulatory agencies for distributing reports.

Requirement R2 (now R1 in the revised standard):

There were objections to the use of the term "Operating Plan" to describe the procedure to identify and report the occurrence of a disturbance. The DSR SDT believes that the use of a defined term is appropriate and has revised Requirement R1 to include Operating Plan, Operating Process and Operating Procedure.

Many commenters felt that the requirements around updating the Operating Plan were too prescriptive, and impossible to comply with during the time frame allowed. The DSR SDT agrees, and Requirement R2, Parts 2.5 through 2.9 have been eliminated. They have been replaced with Requirement R1,Part 1.4 to require updating the Impact Event Operating Plan within 90 days of any change to content.

R1. Each Responsible Entity shall have an Impact Event Operating Plan that includes: *[Violation Risk: Factor Medium] [Time Horizon: Long-term Planning]*:

1.1. An Operating Process for identifying Impact Events listed in Attachment 1.

1.2. An Operating Procedure for gathering information for Attachment 2 regarding observed Impact Events listed in Attachment 1.

1.3. An Operating Process for communicating recognized Impact Events to the following:

1.3.1 Internal company personnel notification(s).

1.3.2. External organizations to notify to include but not limited to the Responsible Entities' Reliability Coordinator, NERC, Responsible Entities' Regional Entity, Law Enforcement, and Governmental or Provincial Agencies.

1.4. Provision(s) for updating the Impact Event Operating Plan within 90 days of any change to its content.

Other requirements reference the Operating Plan as appropriate. The requirements of EOP-004-2 fit precisely into the definition of Operating Plan:

> Operating Plan: A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan.

Requirement R3 (now R2 in the revised standard):

Requirement R3 has been re-written to exclude the requirement to "assess the initial probable cause". The only remaining reference to "cause" is in the Impact Event Reporting Form (Attachment 2). Here, there is no longer a requirement to assess the probable cause. The probable cause only needs to be identified, and only if it is known at the time of the submittal of the report.

> R2. Each Responsible Entity shall implement its Impact Event Operating Plan documented in Requirement R1 for Impact Events listed in Attachment 1 (Parts A and B). *[Violation Risk: Factor Medium] [Time Horizon: Real-time Operations and Same-day Operations]*

Requirement R4 (now R3 in the revised standard):

The DSR SDT did a full review based on comments that were received. R3 now is stream lined to read:

> R3. Each Responsible Entity shall conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 at least annually, with no more than 15 months between such tests. .

The testing of the Operating Process for communicating recognized Impact Events (as stated in R1) is the main component of this requirement. Several commenters provided input that too much "how" was previously within R3 and the DSR DST should only provide the "what". The DSR SDT did not provide any prescriptive guidance on how to accomplish the required testing within the rewrite. Testing of the entity's procedure (R1) could be by an actual exercise of the process (testing as stated in FERC Order 693 section 471), a formal review process or real time implementation of the procedure. The DSR SDT reviewed Order 693 and section 465 directs that processes are "verify that they achieve the desired result". This is the basis of R3, above.

Requirement R5 (now R4 in the revised standard):

The DSR SDT did a full review based on comments that were received. The major issues that

were provided by commenters involved the inclusion of Requirement R5, Part 5.3 and Part 5.4.

5.3 If the Operating Plan is revised (with the exception of contact information revisions), training shall be conducted within 30 days of the Operating Plan revisions.

5.4 For internal personnel added to the Operating Plan or those with revised responsibilities under the Operating Plan, training shall be conducted prior to assuming the responsibilities in the plan.

Upon detailed review the DSR SDT agrees with the majority of comments received regarding Requirement R5, Parts 5.3 and 5.4 and has removed Parts 5.3 and 5.4 completely from the Standard. Training is still the main theme of this requirement (now R4) as it pertains to the personnel required to implement the Impact Event Operating Plan (R1).

R4 now is stream lined to read:

> R4. Each Responsible Entity shall review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan at least annually with no more than 15 calendar months between review sessions

Requirement R6 (now R5 in the revised standard):

The DSR SDT did a full review based on comments that were received. Many comments received identified concerns on the reporting time lines within Attachment 1., Several commenters wanted the ability to report impact events to their responsible parties via the DOE Form OE-417. Upon discussions with the DOE and NERC, the DSR SDT has added the ability to use the DOE Form OE-417 when the same or similar items are required to be reported to NERC and the DOE. This will reduce the need to file multiple forms when the same or similar events must be reported to the DOE and NERC. The reliability intent of reporting impact events within prescribed guidelines, to provide industry awareness and to start any required analysis processes can be met without duplicate reporting R5 now is stream lined to read:

> R5. Each Responsible Entity shall report Impact Events in accordance with its Impact Event Operating Plan pursuant to Requirement R1 and Attachment 1 using the form in Attachment 2 or the DOE OE-417 reporting form.

Requirements R7 and R8:

The DSR SDT did a full review based on comments that were received. The DSR SDT has determined that R7 and R8 are not required to be within a NERC Standard since Section 800 of the Rules of Procedure already assigns this responsibility to NERC.

Attachment 1:

The DSR SDT did a full review based on comments that were received. The DSR SDT, the Events Analysis Working Group (EAWG), NERC Staff (to include NERC Senior VP and Chief Reliability Officer) had an open discussion involving this topic. The EAWG and the DSR SDT aligned Attachment 1 with the Event Analysis Program category 1 analysis responsibilities. This will assure that impact events in EOP-004-2 reporting requirements are the starting vehicle for any required Event Analysis within the NERC Event Analysis Program. The DSR SDT reviewed the "hierarchy" of reporting within Attachment 1. To reduce multiple entities reporting the same impact event, the DSR SDT has stated that the entity that performs the action or is directly

affected by an action will report per EOP-004-2. As an example, during a system emergency, the TOP or RC may request manual load shedding by a DP or TOP. The DP or TOP would have the responsibility to report the action that it took if it meets or exceeds the bright-line criteria established in Attachment 1. Upon reporting, the NERC Event Analysis Program would be made aware of the impact event and start the Event Analysis Process which is outside the scope of this Standard. Several bright-line criteria were removed from Attachment 1. These criteria (DC converter station, 5 generator outages, and frequency trigger limits) were removed after discussions with the EAWG and NERC staff, who concurred that these items should be removed from a reporting standard and analysis process.

Several respondents expressed concern that the reporting requirements were redundant. The general sentiment was that unclear responsibility to report a disturbance could trigger a flood of event reports. Attachment 1 has been modified to assign clear responsibility for reporting, for each category of Impact Event.

Some commenters indicated a concern that the list of events in Attachment 1 isn't as comprehensive as the existing standard since the existing standard includes bomb threats and observations of suspicious activities. Others commented that the impact event list should include deliberate acts against infrastructure. The DSR SDT believes that "observation of suspicious activity" and "bomb threats" are addressed in Attachment 1 Part B – "Risk to BES equipment from a non-environmental physical threat". The SDT has added the phrase, "and report of suspicious device near BES equipment" to note 3 of the "Attachment 1, Potential Reliability – Part B" for additional clarity.

Attachment 2:

The proposed Impact Event Report (Attachment 2) generated comments regarding the duplicative nature of the form when compared to the OE-417. The DSR SDT has added language to the proposed form to clarify that NERC will accept a DOE OE-417 form in lieu of Attachment 2 if the responsible entity is required to submit an OE-417 form.

In collaboration with the NERC Event Analysis Working Group (EAWG) the DSR SDT modified the attachment to eliminate confusion. This revised form will be Attachment 2 of the Standard and collects the only information required to be reported for EOP-004-2. Further information may be requested through the Events Analysis Process (NERC Rules of Procedure), but the collection of this information is outside of the scope of EOP-004.

The DSR SDT has also clarified what the form's purpose with the following addition to the form:

> "This form is to be used to report impact events to the ERO."

Other Standard Issues:

The DSR SDT proposed that combining EOP-004 and CIP-001 would not introduce a reliability gap between the existing standards and the proposed standard and the industry comments received confirms this.

Several entities expressed their concern with the fact that Attachment 1 contained most of the elements already called for in the OE-417. The DSR SDT agrees, and Attachment 1 part 1 has

been modified to even more closely mirror the Department of Energy's OE-417 Emergency Incident and Disturbance Report form. Additionally, the standard has been modified to allow for the use of the OE-417.

There was some concern expressed that there could be confusion between the reporting requirements in this standard, and those found in CIP-008. The DSR SDT agrees, and Attachment 1 Part B, has been modified to provide the process for the reporting of a Cyber Security Incident.

The DSR SDT also believes NERC's additional concern about what data is applicable is addressed by the revisions to Attachment 1, and the inclusion of the OE-417 as an acceptable interim vehicle.

Implementation Plan:

The DSR SDT asked stakeholders to provide feedback on the proposed effective date which provided entities at least a year following board approval of the standard. Most stakeholders supported the one year minimum, however based on the revisions made to the requirements, the drafting team is now proposing that this time period be shortened to between six months and nine months. The current CIP-001 plan is adequate for the new EOP-004 and training should be met in the proposed timeline. Note that the Implementation Plan was developed for the revised Requirements, which do not include an electronic "one-stop shopping" tool. The tool for 'one stop shopping' will be addressed in the proposed revisions to the NERC Rules of Procedure.

The industry commented on the need for e-mail addresses and fax numbers for back up purposes. These details were added to the standard and the implementation plan.

The proposed ballot in December was incorrect and has been deleted from the future development plan. The plan was updated with the correct project plan dates.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Herb Schrayshuen, at 609-452-8060 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

Index to Questions, Comments, and Responses

1. ***Do you agree with the purpose statement of the proposed standard? Please explain in the comment box below. …. ……19***
2. ***Do you agree with the applicable entities in the Applicability Section as well as assignment of applicable entities noted in Attachment 1? Please explain in the***

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

comment box below. …. ……35

3. *Do you agree with the requirement R1 and measure M1? Please explain in the comment box below. …. ……53*
4. *Do you agree with the requirement R2 and measure M2? Please explain in the comment box below. …. ……67*
5. *Do you agree with the requirement R3 and measure M3? Please explain in the comment box below. …. ……90*
6. *Do you agree with the requirement R4 and measure M4? Please explain in the comment box below. …. ……103*
7. *Do you agree with the requirement R5 and measure M5? Please explain in the comment box below. …. ……115*
8. *Do you agree with the requirement R6 and measure M6? Please explain in the comment box below …. ……132*
9. *Do you agree with the requirements for the ERO (R7-R8) or is this adequately covered in the Rules of Procedure (section 802)? Please explain in the comment box below. …. ……143*
10. *Do you agree with the impact event list in Attachment 1? Please explain in the comment box below and provide suggestions for additions to the list of impact events. ……155*
11. *Do you agree with the use of the Preliminary Impact Event Report (Attachment 2)? ……182*
12. *The DSR SDT has replaced the terms "disturbance" and "sabotage" with the term "impact events". Do you agree that the term "impact events" adequately replaces the terms "disturbance" and "sabotage" and addresses the FERC directive to "further define sabotage" in an equally efficient and effective manner? Please explain in the comment box below……192*
13. *The DSR SDT has combined EOP-004 and CIP-001 into one standard (please review the mapping document that shows the translation of requirements from the already approved versions of CIP-001 and EOP-004 to the proposed EOP-004), EOP-004-3 and retiring CIP-001. Do you agree that there is no reliability gap between the existing standards and the proposed standard?……201*
14. *Do you agree with the proposed effective dates? Please explain in the comment box below……207*

15. Do you have any other comments that you have not identified above?.....213

The Industry Segments are:

1 — Transmission Owners

2 — RTOs, ISOs

3 — Load-serving Entities

4 — Transmission-dependent Utilities

5 — Electric Generators

6 — Electricity Brokers, Aggregators, and Marketers

7 — Large Electricity End Users

8 — Small Electricity End Users

9 — Federal, State, Provincial Regulatory or other Government Entities

10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Gregory Campoli	New York Independent System Operator	NPCC	2
3.	Kurtis Chong	Independent Electricity System Operator	NPCC	2

Group/Individual	Commenter	Organization		Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
4.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC		1								
5.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC		1								
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC		10								
7.	Dean Ellis	Dynegy Generation	NPCC		5								
8.	Brian Evans-Mongeon	Utility Services	NPCC		8								
9.	Mike Garton	Dominion Resources Services, Inc.	NPCC		5								
10.	Brian L. Gooder	Ontario Power Generation Incorporated	NPCC		5								
11.	Kathleen Goodman	ISO - New England	NPCC		2								
12.	Chantel Haswell	FPL Group, Inc.	NPCC		5								
13.	David Kiguel	Hydro One Networks Inc.	NPCC		1								
14.	Michael R. Lombardi	Northeast Utilities	NPCC		1								
15.	Randy MacDonald	New Brunswick System Operator	NPCC		2								
16.	Bruce Metruck	New York Power Authority	NPCC		6								
17.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC		10								
18.	Robert Pellegrini	The United Illuminating Company	NPCC		1								
19.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC		1								
20.	Saurabh Saksena	National Grid	NPCC		1								
21.	Michael Schiavone	National Grid	NPCC		1								

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
22.		Peter Yost	Consolidated Edison Co. of New York, Inc. NPCC		3								
2.	Group	Jim Case, SERC OC Chair	SERC OC Standards Review Group	X		X							

Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Garton	Dominion Virginia Power	SERC	1, 3
2.	Jim Griffith	Southern	SERC	1, 3, 5
3.	Vicky Budreau	Santee Cooper	SERC	1, 3, 5, 9
4.	Gerry Beckerle	Ameren	SERC	1, 3
5.	Eugens Warnecke	Ameren	SERC	1, 3
6.	Scott McGough	Oglethorpe Power	SERC	5
7.	John Neagle	AEC I	SERC	1, 3, 5
8.	Joel Wise	TVA	SERC	1, 3, 5, 9
9.	Jennifer Weber	TVA	SERC	1, 3, 5, 9
10.	Robert Thomasson	BREC	SERC	1, 3, 5, 9
11.	Derek Bleyle	SCE&G	SERC	1, 3, 5
12.	Gene Delk	SCE&G	SERC	1, 3, 5
13.	Dave Plauck	Calpine	SERC	5

Group/Individual	Commenter	Organization			Registered Ballot Body Segment									
					1	2	3	4	5	6	7	8	9	10
14.	Tom Hanzlik	SCE&G	SERC	1, 3, 5										
15.	Randy Castello	Mississippi Power	SERC	1, 3, 5										
16.	Doug White	NCEMC	SERC	1, 3, 5, 9										
17.	Randy Haynes	Alcoa	SERC	1, 5										
18.	Joel Rogers	SMEPA	SERC	1, 3, 5, 9										
19.	Mike Bryson	PJM	SERC	2										
20.	Rick Meyers	EEI	SERC	1, 5										
21.	Tim Hattaway	PowerSouth	SERC	1, 3, 5, 9										
22.	Barry Warner	EKPC	SERC	1, 3, 5, 9										
23.	Jack Kerr	Dominion Virginia Power. P.	SERC	1, 3										
24.	Wes Davis	SERC Reliability Corp.	SERC	10										
25.	John Troha	SERC Reliability Corp.	SERC	10										
3.	Group	Brad Jones	Luminant Energy							X				
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1.	Kevin Phillips	Luminant Energy	ERCOT	6										
4.	Group	David Grubbs	City of Garland		X									
	Additional Member	**Additional Organization**	**Region**	**Segment**										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Selection										
1.		David Grubbs	ERCOT 1										
2.		Fred Sherman	ERCOT 1										
3.		Steve Zaragoza	ERCOT 1										
4.		Billy Lee	ERCOT 1										
5.		Heather Siemens	ERCOT 1										
6.		Ronnie Hoeinghaus	ERCOT 1										
7.		Matt Carter	ERCOT 1										
5.	Group	Terry L. Blackwell	Santee Cooper	X		X		X	X				
Additional Member		**Additional Organization**	**Region** / **Segment Selection**										
1.		S. T. Abrams	Santee Cooper SERC 1										
2.		Rene' Free	Santee Cooper SERC 1										
3.		Vicky Budreau	Santee Cooper SERC 1										
4.		Glenn Stephens	Santee Cooper SERC 1										
6.	Group	Steve Alexanderson	Pacific Northwest Small Public Power Utility Comment Group			X	X						

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

Additional Member	Additional Organization	Region	Segment Selection
1.	Russell Noble	Cowlitz County PUD No. 1	WECC 3, 4, 5
2.	Dave Proebstel	Clallam County PUD	WECC 3
3.	Ronald Sporseen	Blachly-Lane Electric Cooperative	WECC 3
4.	Ronald Sporseen	Central Electric Cooperative	WECC 3
5.	Ronald Sporseen	Clearwater Power Company	WECC 3
6.	Ronald Sporseen	Douglas Electric Cooperative	WECC 3
7.	Ronald Sporseen	Consumers Power	WECC 3
8.	Ronald Sporseen	Fall River Rural Electric Cooperative	WECC 3
9.	Ronald Sporseen	Northern Lights	WECC 3
10.	Ronald Sporseen	Lane Electric Cooperative	WECC 3
11.	Ronald Sporseen	Lincoln Electric Cooperative	WECC 3
12.	Ronald Sporseen	Raft River Rural Electric Cooperative	WECC 3
13.	Ronald Sporseen	Lost River Electric Cooperative	WECC 3
14.	Ronald Sporseen	Salmon River Electric Cooperative	WECC 3
15.	Ronald Sporseen	Umatilla Electric Cooperative	WECC 3

Group/Individual		Commenter	Organization		Registered Ballot Body Segment									
					1	2	3	4	5	6	7	8	9	10
16.		Ronald Sporseen	Coos-Curry Electric Cooperative	WECC		3								
17.		Ronald Sporseen	West Oregon Electric Cooperative	WECC		3								
18.		Ronald Sporseen	Pacific Northwest Generating Cooperative	WECC		5								
19.		Ronald Sporseen	Power Resources Cooperative	WECC		5								
7.	Group	Mallory Huggins	NERC Staff											

	Additional Member	Additional Organization	Region	Segment Selection
1.	Earl Shockley	NERC	NA - Not Applicable	NA
2.	Dave Nevius	NERC	NA - Not Applicable	NA
3.	Gerry Adamski	NERC	NA - Not Applicable	NA
4.	Roman Carter	NERC	NA - Not Applicable	NA

8.	Group	Carol Gerou	MRO's NERC Standards Review Subcommittee											X

Additional Member	Additional Organization	Region	Segment Selection
1.	Mahmood Safi	Omaha Public Utility District	MRO	1, 3, 5, 6
2.	Chuck Lawrence	American Transmission Company	MRO	1

Group/Individual	Commenter	Organization		Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Tom Webb	WPS Corporation	MRO	3, 4, 5, 6									
4.	Jodi Jenson	Western Area Power Administration	MRO	1, 6									
5.	Ken Goldsmith	Alliant Energy	MRO	4									
6.	Alice Murdock	Xcel Energy	MRO	1, 3, 5, 6									
7.	Dave Rudolph	Basin Electric Power Cooperative	MRO	1, 3, 5, 6									
8.	Eric Ruskamp	Lincoln Electric System	MRO	1, 3, 5, 6									
9.	Joseph Knight	Great River Energy	MRO	1, 3, 5, 6									
10.	Joe DePoorter	Madison Gas & Electric	MRO	3, 4, 5, 6									
11.	Scott Nickels	Rochester Public Utilties	MRO	4									
12.	Terry Harbour	MidAmerican Energy Company	MRO	1, 3, 5, 6									
9. Group	Sam Ciccone	FirstEnergy		X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Dave Folk	FE	RFC	
2.	Doug Hohlbaugh	FE	RFC	
3.	Andy Hunter	FE	RFC	
4.	Kevin Querry	FE	RFC	
5.	Brian Orians	FE	RFC	

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
6. John Martinez	FE	RFC										
7. John Reed	FE	RFC										
8. Marissa McLean	FE	RFC										
9. Phil Bowers	FE	RFC										
10. Group	Mike Garton	Electric Market Policy	X		X		X	X				

Additional Member	Additional Organization	Region	Segment Selection
1.	Michael Gildea	Dominion	NPCC 5
2.	Louis Slade	Dominion	SERC 6
3.	John Loftis	Dominion Virginia Power	SERC 1

11. Group	Denise Koehn	Bonneville Power Administration	X		X		X	X				

Additional Member	Additional Organization	Region	Segment Selection
1.	Jim Burns	BPA, Transmission, Technical Operations	WECC 1
2.	Russell Funk	BPA, Transmission, DCC Data System Hardware	WECC 1
3.	John Wylder	BPA, Transmission, CC HW Dsgn/Stds Montr & Admin	WECC 1

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
12.	Group	Kenneth D. Brown	PSEG Companies	X		X		X	X				

Additional Member	Additional Organization	Region	Segment Selection
1.	Ron Wharton	PSE&G System Ops	RFC	1, 3
2.	Jerzy Slusarz	PSEG Fossil	RFC	5, 6
3.	James Hebson	PSEG ER&T	ERCOT	5, 6
4.	Dominick Grasso	PSEG Power Connecticut	NPCC	5, 6

13.	Group	Steve Rueckert	WECC										X

Additional Member	Additional Organization	Region	Segment Selection	
1.	Tom Schneider	WECC	WECC	10
2.	John McGee	WECC	WECC	10

14.	Group	Richard Kafka	Pepco Holdings, Inc - Affiliates	X		X		X	X				

Additional Member	Additional Organization	Region	Segment Selection	
1.	Vic Davis	Delmarva Power & Light Co	RFC	1
2.	Dave Thorne	Potomac Electric Power Company	RFC	1

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
15.	Group	Howard Rulf	We Energies			X	X	X					

Additional Member	Additional Organization	Region	Segment Selection
1.	Tom Eells	We Energies RFC	3, 4, 5
2.	Fred Hessen	We Energies RFC	3, 4, 5
3.	Brian Heimsch	We Energies RFC	3, 4, 5

16.	Group	Annette M. Bannon	PPL Supply					X					

Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Heimbach	PPL Martins Creek, LLC RFC	5

17.	Group	J T Wood	Southern Company - Transmission	X		X							

Additional Member	Additional Organization	Region	Segment Selection
1.	Marc Butts	Southern Company Services SERC	1
2.	Andy Tillery	Southern Company Services SERC	1
3.	Jim Busbin	Southern Company Services SERC	1
4.	Phil Winston	Southern Company Services SERC	1

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
5.		Mike Sanders	Southern Company Services SERC 1										
6.		Bob Canada	Southern Company Services SERC 1										
7.		Boyd Nation	Southern Company Services SERC 1										
8.		Phil Whitmer	Georgia Power Company SERC 3										
9.		Randy Mayfield	Alabama Power Company SERC 3										
10.		Randy Castello	Mississippi Power Company SERC 3										
18.	Group	Jason L. Marshall	Midwest ISO Standards Collaborators		X								
Additional Member		**Additional Organization**	**Region** **Segment Selection**										
1.		Jim Cyrulewski	JDRJC Associates, LLC RFC 8										
2.		Kirit Shah	Ameren SERC 1										
3.		Robert A. Thomasson Sr.	Big Rivers SERC 1, 3										
19.	Group	Ben Li	IRC Standards Review Committee		X								
Additional Member		**Additional Organization**	**Region** **Segment Selection**										
1.		Bill Phillips	MISO MRO 2										
2.		Matt Goldberg	ISO-NE NPCC 2										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Charles Yeung	SPP	SPP 2										
4.	Mark Thompson	AESO	WECC 2										
5.	James Castle	NYISO	NPCC 2										
6.	Steve Myers	ERCOT	ERCOT 2										
7.	Greg Van Pelt	CAISO	WECC 2										
8.	Patrick Brown	PJM	RFC 2										
20.	Individual	Brian Pillittere	Tenaska					X					
21.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
22.	Individual	Jana Van Ness, Director Regulatory Compliance	Arizona Public Service Company	X		X		X	X				
23.	Individual	Brent Ingebrigtson	E.ON U.S. LLC	X		X		X	X				
24.	Individual	Brenda Lyn Truhe	PPL Electric Utilities	X									
25.	Individual	Greg Froehling	Green Country Energy					X					
26.	Individual	TransAlta Centralia Generation, LLC	TransAlta Corporation					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
27.	Individual	Doug Smeall	ATCO Electric Ltd.	X									
28.	Individual	Dan Roethemeyer	Dynegy Inc.					X					
29.	Individual	Kasia Mihalchuk	Manitoba Hydro	X		X		X	X				
30.	Individual	Philip Savage	PacifiCorp	X		X							
31.	Individual	Brian Reich	Idaho Power Company	X		X							
32.	Individual	Chris Hajovsky	RRI Energy, Inc.					X	X				
33.	Individual	Bill Keagle	BGE	X									
34.	Individual	John Brockhan	CenterPoint Energy	X									
35.	Individual	Joylyn Faust	Consumers Energy			X	X	X					
36.	Individual	Doug White	North Carolina Electric Coops			X	X	X					
37.	Individual	Lauri Jones	Pacific Gas and Electric Company	X		X		X					
38.	Individual	Laurie Williams	PNM Resources	X		X							
39.	Individual	Val Lehner	ATC	X									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
40.	Individual	Martin Bauer	US Bureau of Reclamation					X					
41.	Individual	Wayne Pourciau	Georgia System Operations Corporation			X	X						
42.	Individual	Rex Roehl	Indeck Energy Services					X					
43.	Individual	Jonathan Appelbaum	United Illuminating	X									
44.	Individual	Amir Y Hammad	Constellation Power Generation and Constellation Commodities Group					X	X				
45.	Individual	Carol Bowman	City of Austin dba Austin Energy	X									
46.	Individual	John Bee	Exelon	X		X		X					
47.	Individual	Kirit Shah	Ameren	X		X		X	X				
48.	Individual	Thad Ness	American Electric Power (AEP)	X		X		X	X				
49.	Individual	Joe Knight	Great River Energy	X		X		X	X				
50.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
51.	Individual	Nathan Lovett	Georgia Transmission Corporation	X									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
52.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X									
53.	Individual	Kathleen Goodman	ISO New England Inc.		X								
54.	Individual	Amanda Stevenson	E.ON Climate & Renewables					X					
55.	Individual	Christine Hasha	ERCOT ISO		X								
56.	Individual	Terry Harbour	MidAmerican Energy	X									
57.	Individual	Michael Gammon	Kansas City Power & Light	X		X		X	X				
58.	Individual	Ron Gunderson	Nebraska Public Power District	X		X		X					
59.	Individual	Dan Rochester	Independent Electricity System Operator		X								
60.	Individual	Catherine Koch	Puget Sound Energy	X									

1. Do you agree with the purpose statement of the proposed standard? Please explain in the comment box below.

Summary Consideration: Stakeholders who responded to this question were fairly evenly divided on acceptance of the original purpose statement with about half supporting the purpose and half suggesting revisions to the purpose. A common thread through most of the comments was that the DSR SDT went beyond the intent of the standard (reporting) and concentrated too much on the analysis of the event. Based on these comments, the SDT revised the purpose statement. The new purpose is:

> To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of Impact Events and their causes, if known, by the Responsible Entities.

Several commenters noted that the term, "impact event" is not a formally defined term. The DSR SDT has used a working definition for "impact events" to develop Attachment 1 as follows:

> An impact event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action.

Many stakeholders indicated that the definition should be added to the NERC Glossary and the DSR SDT adopted this suggestion.

The types of Impact Events that are required to be reported are contained within Attachment 1. Only these events are required to be reported under this Standard.

Some commenters correctly pointed out that "situational awareness" was a desirable by-product of an effective event reporting system, and not driver of that system. Accordingly, all references to "situational awareness" have been deleted from the standard. The more generic "industry awareness" has been substituted where appropriate.

Many commenters noted that the SDT did not define sabotage. FERC Order 693, paragraph 471 states in part: ". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event." The DSR SDT made a conscious, deliberate decision to exclude a strict definition of sabotage from this standard and sought

stakeholder feedback on this issue. Some suggested adopting the NRC definition of the term sabotage, and the DSR SDT did consider adopting the NRC definition shown below but determined that the definition is too narrowly focused.

> Any deliberate act directed against a plant or transport in which an activity licensed pursuant to 10 CFR Part 73 of NRC's regulations is conducted or against a component of such a plant or transport that could directly or indirectly endanger the public health and safety by exposure to radiation.

Most respondents agreed that in order to be labeled as an act of sabotage, the intent of the perpetrators must be known. The team felt that it was almost impossible to determine if an act or event was that of sabotage or merely vandalism without the intervention of law enforcement after the fact. This would result in further ambiguity with respect to reporting events, and the timeline associated with the reporting requirements does not lend itself to the in-depth analysis required to identify a disturbance (or potential disturbance) as sabotage. The SDT felt that a likely consequence of having to meet this criterion, in the time allotted, would be an under-reporting of events. Accordingly, all references to sabotage have been deleted from the standard.

Organization	Yes or No	Question 1 Comment
Ameren	No	The purpose talks about reporting impact events and their known causes. We have no problem with this generic intent, but the purpose says nothing about the very burdensome expectation of verbal updates to NERC and Regional Entities (Attachment 1, top of first page), Preliminary Impact Event Reports (Attachment 1, top of first page, are these Attachment 2?), "Actual" Impact Event Reports (Attachment 1 - Part A) and "Potential" Impact Event Reports (Attachment 1 - Part B). These multiple levels of reporting and events need to be greatly reduced.
American Electric Power (AEP)	No	It is unclear what the relationship between this project and the newly revamped NERC Event Analysis Process. We support moving towards one process opposed to separate obligations that may be in conflict.

Organization	Yes or No	Question 1 Comment
		In addition, AEP supports the concept of a central clearinghouse such as the RCIS that is shared by the industry. We support fewer punitive requirements and more prompting for using tools to make multiple entities aware of reliability related issues shortly after the fact.
CenterPoint Energy	No	CenterPoint Energy does not agree with the purpose statement of the proposed standard. The directive from the Commission in FERC Order 693 and restated in the Guideline and Technical Basis is "...the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: 1) further define sabotage and provide guidance as to the triggering events that would cause and entity to report a sabotage event." Instead the SDT has introduced another term, impact event, to address concerns regarding different definitions. The term, impact event and its proposed concept is too broad. Specifically the concept that an impact event "...has the potential to impact the reliability of the Bulk Electric System" leaves too much room for an entity and a regulatory body to have a difference of opinion as to whether an event should be reported. Required reporting should be limited to actual events. The reporting to follow could become overwhelming for the Responsible Entities, the ERO, and other various organization and agencies. Furthermore, situational awareness is a term that is associated with aspects of real-time. Given the analysis required before a report can be submitted, the report will not be real-time and will not sustain a purpose of supporting situational awareness. (See also comments on Q10 regarding the "Time to Submit Report".) A purpose that is more aligned with consolidation of the EOP-004 and CIP-001 standards would be as follows: Responsible Entities shall report disturbance events and acts of sabotage to support the reliability of the BES through industry awareness.
Consolidated Edison Co. of NY, Inc.	No	Comments: The purpose is not clear because it uses the term "impact events". This term should be a defined in the NERC glossary, and should not include words such as "potential".

Organization	Yes or No	Question 1 Comment
Duke Energy	No	The Purpose statement says that reporting under this standard supports situational awareness. However this is in conflict with Section 5. Background, where the DSR SDT makes clear that this standard includes no real-time operating notifications, and that this proposed standard deals exclusively with after-the-fact reporting. We also disagree with the stated concept of “impact event”. Including the phrase “or has the potential to impact” in the concept makes it impossibly broad for practical application and compliance.
Electric Market Policy	No	The term “impact events” does not draw a clear boundary around those events that are affected by this standard. Since this is not a defined term, nor is intended to be a defined term in the NERC glossary, this standard lacks clarity and is likely to produce significant conflict as an applicable entity attempts to establish procedures to assure compliance. It appears that situational awareness could not be improved with this standard since it is only dealing with events after-the-fact, not within the time frame to allow corrective action by the system operator. As conveyed in Dominion’s comments on NERC Reliability Standards Development Plan 2011 - 2013, Dominion does not see this draft standard as needing to be in the queue while other standards having more impact to bulk electric reliability remain incomplete or unfinished.
ERCOT ISO	No	ERCOT ISO believes that according to the timelines allotted in Attachment 1, it may not be possible for the entity to identify the “known cause” of an event. The requirements list identification of “initial probable cause”. This is more reasonable under the timelines noted in Attachment 1.
Exelon	No	The purpose states that Responsible Entities SHALL report impact events - this implies that ALL impact events need to be reported regardless of magnitude, suggest rewording to say "... shall report applicable impact events ..." to allow for evaluation of each impact for applicability in accordance with Attachment 1).

Organization	Yes or No	Question 1 Comment
FirstEnergy	No	Since this standard is after-the-fact reporting, the phrase "situational awareness" may not be appropriate since that phrase is attributed by a large part of the industry to real-time, minute-to-minute awareness of the system. We suggest the following rewording of the purpose statement: "To ensure Applicable Entities report impact events and their known causes to enhance and support the reliability of the Bulk Electric System (BES)".
Indeck Energy Services	No	Suggestion: "Functional Entities identified in Section 4 shall support situational awareness of impact events and their known causes."
Independent Electricity System Operator	No	(1) Our understanding of the proposed revision as conveyed in the SAR was to provide clarity and reduce redundancy on reporting the latest and even on-going events on the system that may be caused by system changes and/or sabotage. The intent is to ensure the proper authorities are informed of such events so that they may take appropriate and necessary actions to identify causes and/or mitigate or limit the extent of interruptions. We also supported a suggestion in the SAR to assess the merit of merging CIP-001 and EOP-004 to remove redundancy, although we suggested that this should not be a presumption when revising the standard(s).This posting appears to indicate that only EOP-004 will be revised at this time, and CIP-001 which deals with sabotage reporting will remain in effect. With this assumption, the proposed standard appears to contain a mixture of reporting two types of events of different time frame - the first type being those events that need to be reported soon or immediately after they occur (e.g. impact events that appear to be the result of a sabotage) with an aim to curb/contain these events by the appropriate authorities; the second type being the events that can be reported sometime well after the fact, e.g. system disturbances due to weather or switching or other known causes that are not of malicious nature. Combining the two types of requirement does not appear to be clearly conveyed in the SAR. We therefore suggest the SDT review the main purpose

Organization	Yes or No	Question 1 Comment
		and content in the proposed EOP-004 to ensure consistency with the SAR, and in relation to the purpose and requirements already contained in CIP-004.(2) With respect to disseminating reports and related information after the fact, we wonder if a data collection process, such as RoP 1900, can serve the purpose without having to create a standard or a requirement to achieve this.(3) Most of the requirements appear to be administrative in nature and they stipulate the how but not the what, which in our view does not conform with the Results-based standard concept and does not rise to the level of a reliability standard.(4) A number of requirements proposed in the draft standard are quite vague and cannot be measured. Details of this assessment is provided below.
IRC Standards Review Committee	No	The proposed requirements in the standard are not focused on the core industry concern that current requirements are unclear as to what types of events warrant entities to report. Per draft 2 of the SAR, "The existing requirements need to be revised to be more specific - and there needs to be more clarity in what sabotage looks like." Instead this proposed standard includes requirements that are more focused on "how" to report, rather than "what" to report. The SAR states that: "The development may include other improvements to the standards deemed appropriate by the drafting team, with consensus on the stakeholders (emphasis added), consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards." The SRC believes the scope of the SAR, and likewise the proposed standard, is inappropriate to the fundamental reliability purpose of what events need to be reported. The proposed administrative requirements are difficult to interpret, implement and measure, and do not clarify what type of sabotage information entities need to report. Although the use of procedures and an understanding by those personnel accountable seem helpful for ensuring reports are made, the fundamental purpose of clarifying what types of events should be reported and more importantly what types do not have to be reported, is lacking in the standard. Also, one of the first issues identified in the SAR for consideration by the drafting

Organization	Yes or No	Question 1 Comment
		team seems to be ignored, "Consider whether separate, less burdensome requirements for smaller entities may be appropriate." The requirements for entities to develop Operating Plans and to have training for those plans, further adds uncertainty and increases complexity of how entities, large and small, will have to comply with this standard.
ISO New England Inc.	No	The proposed requirements in the standard are not focused on the core industry concern that current requirements are unclear as to what types of events warrant entities to report. Per draft 2 of the SAR, "The existing requirements need to be revised to be more specific - and there needs to be more clarity in what sabotage looks like." Instead this proposed standard includes requirements that are more focused on "how" to report, rather than "what" to report. The draft 2 SAR has never been balloted for approval prior to standard drafting. In fact, the SAR states, "The development may include other improvements to the standards deemed appropriate by the drafting team, with consensus on the stakeholders (emphasis added), consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards." The scope of the SAR, and likewise the proposed standard, is inappropriate to the fundamental reliability purpose of what events need to be reported. The proposed administrative requirements are difficult to interpret, implement and measure, and do not clarify what type of sabotage information entities need to report. Although the use of procedures and an understanding by those personnel accountable seems helpful for ensuring reports are made, the fundamental purpose of clarifying what types of events should be reported and more importantly what types do not have to be reported, is lacking in the standard. Also, one of the first issues identified in the SAR for consideration by the drafting team seems to be ignored: "Consider whether separate, less burdensome requirements for smaller entities may be appropriate." The requirements for entities to develop Operating Plans and to have training for those plans, further adds uncertainty and increases complexity of how entities, large and small, will have to comply with this standard.The term "impact

Organization	Yes or No	Question 1 Comment
		events" does not draw a clear boundary around those events that are affected by this standard. Since this is not a defined term, nor is intended to be a defined term in the NERC Glossary, this standard lacks clarity and is likely to produce significant conflict as an applicable entity attempts to establish procedures to assure compliance. It appears that situational awareness could not be improved with this standard since it is only dealing with events after-the-fact, not within the time frame to allow corrective action by the system operator.This draft standard should not have this high a priority while other standards having a greater impact on Bulk Electric System reliability remain incomplete or unfinished.Regional reporting requirements should be in Regional Standards, and not be included in a NERC Standard.
Manitoba Hydro	No	Though new purpose greatly clarifies the proposed EOP-004-2 and using "situational awareness" is the key to this purpose, further clarification of specific items should be added to the purpose. "Responsible Entities shall report SIGNIFICANT events to support interconnection situational awareness on events that impact the integrity of the Bulk Electric System, such as islanding, generation, transmission and load losses, load shedding, operation errors, IROL/SOL violations, sustained voltage excursions, equipment and protection failures and on suspected or acts of sabotage."
Nebraska Public Power District	No	The background states there is no real-time reporting requirement in this standard, but the purpose states a purpose is for situational awareness. This implies real-time reporting. The purpose clearly identify the standard is for after the fact reporting to permit analysis of events, trend data, and identify lessons learned.
North Carolina Electric Coops	No	The term "impact event" is not a defined term in the NERC glossary and does not draw a clear boundary or give concise guidance to aid in event recognition.
Northeast Power Coordinating	No	The proposed requirements in the standard are not focused on the core industry concern that current

Organization	Yes or No	Question 1 Comment
Council		requirements are unclear as to what types of events warrant entities to report. Per draft 2 of the SAR, "The existing requirements need to be revised to be more specific - and there needs to be more clarity in what sabotage looks like." Instead this proposed standard includes requirements that are more focused on "how" to report, rather than "what" to report. The draft 2 SAR has never been balloted for approval prior to standard drafting. In fact, the SAR states, "The development may include other improvements to the standards deemed appropriate by the drafting team, with consensus on the stakeholders (emphasis added), consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards." The scope of the SAR, and likewise the proposed standard, is inappropriate to the fundamental reliability purpose of what events need to be reported. The proposed administrative requirements are difficult to interpret, implement and measure, and do not clarify what type of sabotage information entities need to report. Although the use of procedures and an understanding by those personnel accountable seems helpful for ensuring reports are made, the fundamental purpose of clarifying what types of events should be reported and more importantly what types do not have to be reported, is lacking in the standard. Also, one of the first issues identified in the SAR for consideration by the drafting team seems to be ignored: "Consider whether separate, less burdensome requirements for smaller entities may be appropriate." The requirements for entities to develop Operating Plans and to have training for those plans, further adds uncertainty and increases complexity of how entities, large and small, will have to comply with this standard.The term "impact events" does not draw a clear boundary around those events that are affected by this standard. Since this is not a defined term, nor is intended to be a defined term in the NERC Glossary, this standard lacks clarity and is likely to produce significant conflict as an applicable entity attempts to establish procedures to assure compliance. It appears that situational awareness could not be improved with this standard since it is only dealing with events after-the-fact, not within the time frame to allow corrective action by the system operator.This draft standard should not have this high a priority while other standards having a greater impact

Organization	Yes or No	Question 1 Comment
		on Bulk Electric System reliability remain incomplete or unfinished.Regional reporting requirements should be in Regional Standards, and not be included in a NERC Standard.
Pacific Gas and Electric Company	No	PG&E recognizes this is an after the fact report, however, the purpose statement should reflect the fact that this proposed standard is for after-the-fact reporting. If the future intent is for this report to replace current reporting criteria the purpose statement should be expanded to reflect the true intent of the Standard.
PNM Resources	No	PNM believes the purpose statement should reflect the fact that this proposed standard is for after-the-fact reporting. It is misleading and may have many thinking it is duplicative work.
PSEG Companies	No	The following sentence should be added. "This standard is not intended to be for real-time operations reporting."
RRI Energy, Inc.	No	The purpose does not need to mention "and the reliability of the Bulk Electric System." This is the Congressional mandate in FPA Section 215, and could be attached to every Standard, guide, notice and direction issued by FERC, NERC and Regional Entities. In addition, the purpose references "Responsible Entities." However, section 4 on "Applicability" references "Functional Entities." These terms should be consistent. Therefore, the purpose statement of the proposed standard should be corrected to read, "Functional Entities identified in Section 4 shall report impact events and their known causes to support situational awareness."CONSIDERATION: Is the phrase "shall report impact events and their known causes" really a purpose of the Proposed Standard, or is it instead merely a means to achieve the purpose of situational awareness? If the latter, the purpose statement can be further shortened to read, "Functional Entities identified in Section 4 shall support situational awareness of impact events and their known causes."

Organization	Yes or No	Question 1 Comment
Santee Cooper	No	Since this standard is written to report events after-the-fact and not for a System Operator to perform corrective action, we believe the words situational awareness should be removed from the purpose. Situational Awareness is typically used for real-time operations.Also, any events that require reporting should be clearly defined in Attachment 1 and leave no room for interpretation by an entity.
SERC OC Standards Review Group	No	The term “impact events” does not draw a clear boundary around those events that are affected by this standard. Since this is not a defined term, nor is intended to be a defined term in the NERC glossary, this standard lacks clarity and is likely to produce significant conflict as an applicable entity attempts to establish procedures to assure compliance. It appears that situational awareness could not be improved with this standard since it is only dealing with events after-the-fact, not within the time frame to allow corrective action by the system operator.
United Illuminating	No	UI suggests adding the phrase: and the ERO shall provide quarterly reports; Responsible Entities shall report impact events and their known causes, and the ERO shall provide quarterly reports, to support situational awareness and the reliability of the Bulk Electric System (BES).
US Bureau of Reclamation	No	The purpose is more closely related to the concept that "Responsible Entities shall document and analyze impact events and their known causes and disseminate the impact event documentation to support situational awareness". Not all impact events are to be reported. The analysis of the impact events is what is needed to achieve a lessons learned.
We Energies	No	Impact event needs to be clarified first, and DP references in Attachment 1 clarified. Distribution is not BES.
WECC	No	The purpose statement should reflect the fact that this proposed standard is for after-the-fact reporting. It is

Organization	Yes or No	Question 1 Comment
		misleading and may have many thinking it is duplicative work.
ATC	Yes	ATC agrees with the purpose statement. However, we do not agree with the implied definition of “impact events” as represented in Attachment 1. (See specific comments about what is included in Attachment 1 for the type of events that qualify as an “impact event”.)
Bonneville Power Administration	Yes	Known causes are difficult under 1 hour reporting requirements (Unusual events are even harder to narrow down in 24 hours and may take weeks.) The System Operators and RC’s handle situational awareness and reliability events, this is an extra wide view and learning for reporting only.
Dynegy Inc.	Yes	Statement is broad enough to cover both Standards.
Great River Energy	Yes	Thank you for the clarification of “known causes”, this will allow entities to report what they currently know when submitting an impact report.
MRO's NERC Standards Review Subcommittee	Yes	Thank you for the clarification of “known causes”, this will allow entities to report what they currently know when submitting an impact report.
Puget Sound Energy	Yes	However, further definition of "known causes" would be helpful as sometime the root cause analysis doesn't uncover the actual cause for sometime after the timeframes outlined in Attachment 1.
Arizona Public Service Company	Yes	
ATCO Electric Ltd.	Yes	

Organization	Yes or No	Question 1 Comment
BGE	Yes	
City of Austin dba Austin Energy	Yes	
City of Garland	Yes	
Constellation Power Generation and Constellation Commodities Group	Yes	
E.ON Climate & Renewables	Yes	
Georgia System Operations Corporation	Yes	
Green Country Energy	Yes	
Idaho Power Company	Yes	
Kansas City Power & Light	Yes	
Luminant Energy	Yes	
MidAmerican Energy	Yes	

Organization	Yes or No	Question 1 Comment
Midwest ISO Standards Collaborators	Yes	
NERC Staff	Yes	
Pacific Northwest Small Public Power Utility Comment Group	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	
Pepco Holdings, Inc - Affiliates	Yes	
PPL Electric Utilities	Yes	
PPL Supply	Yes	
Tenaska	Yes	
TransAlta Corporation	Yes	

2. Do you agree with the applicable entities in the Applicability Section as well as assignment of applicable entities noted in Attachment 1? Please explain in the comment box below.

Summary Consideration: There was no consensus amongst stakeholders who responded to this question regarding the acceptability of the proposed list of functional entities and the assignment of applicable entities in Attachment 1.

Several respondents replied with their concern that the reporting requirements were redundant. The general sentiment was that unclear responsibility to report a disturbance could trigger a flood of event reports. Attachment 1 has been modified to assign clear responsibility for reporting, for each category of Impact Event. There was some concern expressed that there could be confusion between the reporting requirements in this standard, and those found in CIP-008. The DSR SDT agrees, and Attachment 1 Part B, has been modified to provide the process for the reporting of a Cyber Security Incident.

The DSR SDT had protracted discussions on the applicability of this standard to the LSE. Per the Functional Model the LSE does not own assets and therefore should not be an applicable entity (no equipment that could experience a "disturbance"). However, the Registry Criteria contains language that could imply that the LSE does own assets, or is at least responsible for assets. In addition, the DSR SDT modified Attachment 1 to include reporting of damage or destruction of Critical Cyber Assets per CIP-002. The LSE, as well as the Interchange Authority and Transmission Service Provider are applicable entities under CIP-002 and should be included for Impact Events under EOP-004.

There were several comments that the asset owners (GO/TO) would be less likely than the asset operators (GOP/TOP) to be aware of an impact event. The DSR SDT recognizes that this may be true in some cases, but not all. In order to meet the reliability objectives of this requirement, the applicability for GO/TO will remain as per Attachment 1.

Organization	Yes or No	Question 2 Comment

Organization	Yes or No	Question 2 Comment
American Electric Power (AEP)	No	AEP does not agree with the addition of the Generator Owner to the standard. The Generator Owner does not have visibility to the real time operational status of a unit. As a result, the Generator Owner lacks the ability to recognize impact events and report them to the Regional Entity or NERC within the time frames specified in the standard. Reporting requirements for impact events should be the responsibility of the Generator Operator.
Arizona Public Service Company	No	AZPS recommends excluding 4.1.7 Distribution Providers, as Distribution Providers generally operate at levels below 100kV.
ATC	No	The Functional Entities identified in Attachment 1 do not align with the current CIP Standard obligations (e.g. Load Serving Entities are not included).
CenterPoint Energy	No	CenterPoint Energy does not agree with the addition of Transmission Owner and Distribution Provider to the Applicability section. Transmission Owner and Distribution provider are not currently applicable entities for either CIP-001 or EOP-004 and should not be included in the proposed combined standard. However, CenterPoint Energy does agree that LSE should be removed from the Applicability section. CenterPoint Energy appreciates the SDT's efforts in assigning entities to each event in Attachment 1. This is an improvement over the existing EOP-004 standard. It is clear, however, that with multiple entities responsible for reporting each event, there is no need to expand the Applicability Section to include Transmission Owner and Distribution Provider.
Consolidated Edison Co. of NY, Inc.	No	Comments: NERC's role as the Standard enforcement organization for the power industry will be in conflict if NERC is also identified as an applicable entity. What compliance organization will audit NERC's

Organization	Yes or No	Question 2 Comment
		performance? This is presently not clear.
Constellation Power Generation and Constellation Commodities Group	No	Constellation Power Generation and Constellation Commodities Group disagrees with the inclusion of Generator Owners. Since one of the goals in revising this standard is to streamline impact event reporting obligations, Generator Operators are the appropriate entity to manage event reporting as the entity most aware of events should they arise. At times, the information required to complete a report may warrant input from entities connected to generation, but the operator remains the best entity to fulfill the reporting obligation.
E.ON Climate & Renewables	No	1. Voltage deviation events are too vague for GOP. How does voltage deviations apply to GOP's or specifically renewables i.e., wind farms? 2. Define what an "entity" is. 3. Define what a "generating station" is. 4. Define what a "BES facility" is. 5. Define what a control center is. 6. Renewable energy/generators should be taken into consideration when crafting the events.
E.ON U.S. LLC	No	The proposed standard does not list the Load Serving Entity as an Applicable Entity, but the possible events that the standard addresses are within the scope of the LSE. Some functions of the LSE listed within the Functional Model are addressed in the proposed standard. Existing CIP-001-1a and EOP-004-1 are both applicable to the LSE.
Electric Market Policy	No	Having the ERO as an applicable entity is concerning as they are also the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. For example, establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC's open process. Attachment 1 is troublesome. The time frames listed are not consistent for similar events. For example, EEAs are either reported within one or 24 hours depending on the nuance. Having multiple entities

Organization	Yes or No	Question 2 Comment
		reporting the same event is troublesome, i.e., why does a RC have to report an EEA if the BA is going to report it? This will lead to conflicting reports for the same event. Attachment 1 seems to be consolidating time frames from other standards into one for reporting. However, we believe this subject is more complex than this table reveals and the table needs more clarification.Several of the events require filing a written formal report within one hour. For example, system separation certainly is going to require an “all hands on deck” response to the actual event. We note that the paragraph above the table in attachment 1 indicates that a verbal report would be allowed in certain circumstances, but this is the same issue with the formal report in that the system operators are concerned with the event and not the reporting requirements.There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
ERCOT ISO	No	ERCOT ISO recommends that the Electric Reliability Organization be removed from the standard. The Electric Reliability Organization should not be responsible for reliability functions and therefore should be excluded from reliability standards.
Exelon	No	Attachment 1, Part B, footnote 1. A GO is unlikely to know if a fuel supply problem would cause a reliability concern because one GO may not know the demand for an entire region. Attachment 1, Part B, footnote 1. What is the definition of an "emergency" related to problems with a fuel supply chain? What time threshold of projected need would constitute a 1 hour report?Attachment 1, Part A - Voltage Deviations - A GOP may not be able to make the determination of a +/- 10% voltage deviation for â‰¥ 15 minutes, this should be a TOP RC function only. Attachment 1, Part A - Generation Loss of â‰¥ 2, 000 MW for a GO/GOP does not provide a time threshold. If the 2, 000 MW is from a combination of units in a single location, what is the time threshold for the combined unit loss? Attachment 1, Part A - Damage or destruction of BES equipment o The

Organization	Yes or No	Question 2 Comment
		event criteria is ambiguous and does not provide clear guidance; specifically, the note needs to provide more explicit criteria related to parts (iii) and (iv) to remove the need for interpretation especially since this is a 1 hour reportable occurrence. In addition, determination of the aggregate impact of damage may not be immediately understood - does the 1 hour report time clock start on initiation of event or following confirmation of event? o The initiating event needs to explicitly state that it is a physical and not cyber. Events related to cyber sabotage are reported in accordance with CIP-008, "Cyber Security - Incident Reporting and Response Planning," and therefore any type of event that is cyber initiated should be removed from this Standard. o If the damage or destruction is related to a deliberate act, consideration should also be given to coordinating such reporting with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security event. Attachment 1, Part B - Loss of off-site power (grid supply) affecting a nuclear generating station - this event classification should be removed from EOP-004. The impact of loss of off-site power on a nuclear generation unit is dependent on the specific plant design and may not result in a loss of generation (i.e., unit trip); furthermore, if a loss of off-site power were to result in a unit trip, an Emergency Notification System (ENS) would be required to the Nuclear Regulatory Commission (NRC). The 1 hour notification in EOP-004 on a loss of off-site power (grid supply) to a nuclear generating station should be commensurate with other federal required notifications. Depending on the unit design, the notification to the NRC may be 1 hour, 8 hours or none at all. Consideration should be given to coordinating such reporting with existing required notifications to the NRC as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential transient on the unit. Attachment 1, Part B - Forced intrusion at a BES facility - Consideration should also be given to coordinating such reporting with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security event. Attachment 1, Part B - Risk to BES equipment from a non-environmental physical threat - this event leaves

Organization	Yes or No	Question 2 Comment
		the interpretation of what constitutes a "risk" with the reporting entity. Need more specific criteria for this event.Attachment 1, Part B - Detection of a cyber intrusion to critical cyber assets - Events related to cyber sabotage are reported in accordance with CIP-008, "Cyber Security - Incident Reporting and Response Planning," and therefore any type of event that is cyber initiated should be removed from this Standard.
FirstEnergy	No	We do not support the ERO as an applicable entity of a reliability standard because they are not a user, owner or operator of the bulk electric system. Any expectation of the ERO should be defined in the Rules of Procedure.
Georgia System Operations Corporation	No	This standard should not apply to distribution systems or Distribution Providers. It should apply only to the BES.
Georgia Transmission Corporation	No	These events generally are Operator Functions and should not apply to a TO.1. Energy Emergency requiring system-wide voltage reduction2. Loss of firm load greater than 15 min.3. Transmission loss (multiple BES transmission elements)4. Damage or destruction to BES equipment (thru operational error or equipment failure)5. Loss of off-site power affecting a nuclear generating station
Indeck Energy Services	No	---ERO should not be included in this or any other standard! FERC can decide whether NERC is doing a good job without having standards requirements to audit to. If NERC needs to be included in a standard, then it should a stand-alone one so that the RSAW for all of the other audits don't need to include those requirements. ---"Loss of off-site power (grid supply)" is important at control centers and other large generators. The SDT must use a well-defined standard such as potentially cause a Reportable Disturbance, to differentiate significant events from others. ---"Footnote 1. Report if problems with the fuel supply chain result in the projected need for emergency actions to manage reliability." is ambiguous. Everything in the

Organization	Yes or No	Question 2 Comment
		Standards program can "Affecting BES reliability". The SDT must use a well-defined standard such as potentially cause a Reportable Disturbance, to differentiate significant events from others. ---"Footnote 2. Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects the reliability of the BES)." is well intentioned but ambiguous. For example, if I know the motivation is to blow up the plant, then by this footnote, I don't have to report. The SDT must use a well-defined standard such as potentially cause a Reportable Disturbance, to differentiate significant events from others. ---All terms should be used from or added to the Glossary.
Independent Electricity System Operator	No	We do not agree with the inclusion of TO and GO. They are not operating entities and do not need to collect or provide information pertaining to impact events, which are the results and phenomena observe under operating conditions in the operation horizon, and such information collection and provision are the responsibility of the TOP and GOP.
IRC Standards Review Committee	No	Entities that have information about possible sabotage events should report these to NERC after the fact and the standard should simply reflect that. While we agree with the list of functional entities identified in the Applicability Section, we do not agree with their application in Attachment 1. As the functional entities are identified in Attachment 1, there is likely going to be duplicate reporting. Why should both the RC and BA submit a report for an EEA for example?
ISO New England Inc.	No	Having the ERO as an applicable entity raises the issue that they are also the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. For example, establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC's open process. NERC has also offered the opinion that since NERC is not a "user, owner, or

Organization	Yes or No	Question 2 Comment
		operator" Standards are not enforceable against the ERO. In Attachment 1 the time frames listed are not consistent for similar events. For example, EEAs are either reported within one or 24 hours depending on the nuance. Having multiple entities reporting the same event is troublesome, i.e., why does a RC have to report an EEA if the BA is going to report it? This will lead to unnecessary and possibly conflicting reports for the same event. Attachment 1 seems to be consolidating time frames from other standards into one for reporting. However, this subject is more complex than this table reveals, and the table needs more clarification.Entities that have information about possible sabotage events should report these to NERC after the fact, and the standard should simply reflect that. While we agree with the list of functional entities identified in the Applicability Section, we do not agree with their application in Attachment 1. As the functional entities are identified in Attachment 1, it is likely that there is going to be duplicate reporting. Several of the events require filing a written formal report within one hour. For example, system separation is going to require an "all hands on deck" response to the actual event. The paragraph above the table in Attachment 1 indicates that a verbal report would be allowed in certain circumstances, but this is the same issue with the formal report in that the system operators are concerned with the event and not the reporting requirements.There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements through NERC that cross federal agency jurisdictions.
Luminant Energy	No	Inclusion of both GO and GOP will result in duplicate reporting as both are responsible for reporting resource-related events such as Generation Loss, Fuel Supply Emergencies and Loss of Off-site power (grid supply). Recommend including only the GOP as it is critical that the GOP gather and communicate relevant information to the Reliability Coordinator.
Manitoba Hydro	No	Since this Standard is to support situational awareness, more entities should be included such as Load

Organization	Yes or No	Question 2 Comment
		Serving Entities (which was removed from EOP-004-1).
MidAmerican Energy	No	While we agree with the list of functional entities identified in the Applicability Section, we do not agree with their application in Attachment 1. As the functional entities are identified in Attachment 1, there is likely going to be duplicate reporting. Why should both the RC and BA submit a report for an energy emergency requiring public appeals?
Midwest ISO Standards Collaborators	No	While we agree with the list of functional entities identified in the Applicability Section, we do not agree with their application in Attachment 1. As the functional entities are identified in Attachment 1, there is likely going to be duplicate reporting. Why should both the RC and BA submit a report for an energy emergency requiring public appeals?
North Carolina Electric Coops	No	There is a conflict between the ERO being listed as an applicable entity and the fact that the ERO is the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that other applicable entities would be required to meet.Attachment 1 has inconsistent time frames listed for similar events. For example, EEA's are either reported within one or 24 hours depending on the nuance. Also, having more than one entity reporting an EEA can lead to conflicting information for the same event. Attachment 1 has the RC and the BA both reporting the same EEA event. Attachment 1 consolidates time frames from other standards for reporting purposes. There should either be a separate standard for "reporting" that encompasses reporting requirements for all standards or leave the time frames and reporting requirements in the original individual standards.Several of the events require filing a written formal report within one hour. For large events like cascading outages or system separation, "all hands on deck" attention will need to be given to the actual event. Although a verbal report would be allowed in certain circumstances, attention to the actual event should take precedence over formal reporting requirements.There is already a

Organization	Yes or No	Question 2 Comment
		DOE requirement to report certain events and no need to develop redundant reporting requirements in the NERC arena when this information is already available at the federal level at other agencies.
Northeast Power Coordinating Council	No	Having the ERO as an applicable entity raises the issue that they are also the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. For example, establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC's open process. NERC has also offered the opinion that since NERC is not a "user, owner, or operator" Standards are not enforceable against the ERO. In Attachment 1 the time frames listed are not consistent for similar events. For example, EEAs are either reported within one or 24 hours depending on the nuance. Having multiple entities reporting the same event is troublesome, i.e., why does a RC have to report an EEA if the BA is going to report it? This will lead to unnecessary and possibly conflicting reports for the same event. Attachment 1 seems to be consolidating time frames from other standards into one for reporting. However, this subject is more complex than this table reveals, and the table needs more clarification.Entities that have information about possible sabotage events should report these to NERC after the fact, and the standard should simply reflect that. While we agree with the list of functional entities identified in the Applicability Section, we do not agree with their application in Attachment 1. As the functional entities are identified in Attachment 1, it is likely that there is going to be duplicate reporting. Several of the events require filing a written formal report within one hour. For example, system separation is going to require an "all hands on deck" response to the actual event. The paragraph above the table in Attachment 1 indicates that a verbal report would be allowed in certain circumstances, but this is the same issue with the formal report in that the system operators are concerned with the event and not the reporting requirements.There is already a DOE requirement to report certain events. We see no need to develop redundant reporting

Organization	Yes or No	Question 2 Comment
		requirements through NERC that cross federal agency jurisdictions.
Pacific Gas and Electric Company	No	PG&E recognizes the ERO is in R1, however, it does not see where the ERO's applicability is applied in Attachment 1.
Pacific Northwest Small Public Power Utility Comment Group	No	See #15
PNM Resources	No	PNM OTS does not see where the ERO's applicability is applied in Attachment 1.
PPL Electric Utilities	No	While we agree with the applicable entities in the Applicability Section of the revised standard, we would like the SDT to reconsider the applicable entities identified on Attachment 1, specifically regarding duplication of reporting e.g. should TO and TOP report?
PPL Supply	No	While we agree with the list of functional entities identified in the Applicability Section, we do not agree with assignment of applicable entities noted in Attachment 1. As the functional entities are identified in Attachment 1, there will likely be duplicate reporting for many impact events. By applying reporting responsiblities to both the Gen Owner and Gen Operator, this will result in duplicate reporting for plants with multiple owners. It also increases the burden on the Gen Operator who is required to report the event to NERC and to other Gen Owners in a timely manner to allow other Gen Owners to meet the NERC reporting timeline. We suggest that the reporting requirements associated with generators be applied to the Gen Operator only.
RRI Energy, Inc.	No	Agree with the "Applicability" section functional categories.Agree with the Attachment 1 lists of "Entity with Reporting Responsibility," with the following exceptions:PART A"Damage or Destruction of BES Equipment" - This item has a footnote 1 listed, but nothing at the bottom of the page for a footnote. Assuming the footnote

Organization	Yes or No	Question 2 Comment
		reference is intended to reference the "Examples" at the bottom of the page, the following concerns exist:(i) "critical asset" - Is this term intended to reference a "Critical Asset" identified pursuant to the CIP-002 risk-based assessment methodology? If so, it should be capitalized. If not, who determines what constitutes a lower case "critical asset"? (ii) "Significantly affects the reliability margin of the system..." - If this is intended to be enforceable, several words need significant clarification and definition, such as "Significantly," "reliability margin," "system" (BES?), "potential," and "emergency action." The combined ambiguity of just two of those phrases would most likely result in a court holding this statement as so vague as to be unenforceable. The combined lack of clarity of all the highlighted words or phrases render this sentence meaningless.(iii) "Damaged or destroyed due to a non-environmental external cause" - "Non-environmental external cause" should be a defined term because, as is the case in item (ii) above, it is vague and subject to broad, random or arbitrary interpretation. Part B provides examples of "non-environmental physical threat" for "Risk to BES equipment." Those examples could be referenced here, or different examples included that are more applicable to the Event.The items highlighted in items (ii) and (iii) above are very similar to the unintended string of CIP-001 violations that Registered Entities experienced in 2007 and 2008 for failing to provide their own definition of "sabotage" under a sabotage reporting standard that failed to provide any guidance to the industry within the standard as to what constituted "sabotage." PART B"Detection of a cyber intrusion to critical cyber assets" - Capitalize "Critical Cyber Asset."
Santee Cooper	No	Standards cannot be applicable to an ERO because they are the compliance enforcement authority, and the ERO is not a user, owner, or operator of the BES. Since we are reporting events that may affect the BES, why does a DP need to be included as an applicable entity for this standard? If the DOE form is going to continue to be required by DOE, then NERC should accept this form. Entities do not have time to fill out duplicate forms within the time limits allowed for an event. This is burdensome on an entity. If NERC is going

Organization	Yes or No	Question 2 Comment
		to require a separate reporting of events from DOE, then NERC should look at these events closely to determine if any of the defined events should be eliminated or modified from the current DOE form. (For example: Is shedding 100 MW of firm load really a threat to the BES?)Why does Attachment 1 have multiple entities reporting the same event? An RC should not have to report an EEA if the BA is required to report it. This will lead to conflicting reports for the same event.Attachment 1 is just a consolidation of the time frame from other standards. It appears no review was done for consistency of time frames for similar events.
SERC OC Standards Review Group	No	We find it interesting that the ERO is listed as an applicable entity. The ERO can't be an applicable entity because they are the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. NERC seems to be attempting to evade FERC jurisdiction by having a standard that enables it to write new rules that don't pass through the normal standards development process with ultimate approval by FERC.Attachment 1 is troublesome. The time frames listed are not consistent for similar events. For example, EEAs are either reported within one or 24 hours depending on the nuance. Having multiple entities reporting the same event is troublesome, i.e., why does an RC have to report an EEA if the BA is going to report it? This will lead to conflicting reports for the same event. Attachment 1 seems to be consolidating time frames from other standards into one for reporting. However, we believe this subject is more complex than this table reveals and the table needs more clarification or it should be eliminated and leave the time frames in the other standards.Several of the events require filing a written formal report within one hour. For example, system separation certainly is going to require an "all hands on deck" response to the actual event. We note that the paragraph above the table in attachment 1 indicates that a verbal report would be allowed in certain circumstances, but this is the same issue with the formal report in that the system operators are concerned with the event and not the reporting requirements.There is already a DOE requirement to report

Organization	Yes or No	Question 2 Comment
		certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
Southern Company - Transmission	No	We find it interesting that the ERO is listed as an applicable entity. The ERO is responsible for multiple requirements in this standard that shapes the ultimate actual rules that the other applicable entities would be required to meet. Can the NERC/ERO be accountable for a feedback loop to the industry? Feedback is preferable but would NERC/ERO self-report a violation to the requirement?
We Energies	No	The need for a DP to be included needs to be clarified. The Purpose points to BES. A DP does not have BES equipment.
WECC	No	The ERO's applicability is not applied in Attachment 1.
Great River Energy	Yes	We believe that it is important for the ERO to provide valuable Lessons learned to our electrical industry, thus enhancing the reliability of the BES.
Kansas City Power & Light	Yes	Consideration should be given to the need for a preliminary impact event report to be filed by the Reliability Coordinator and the Registered Entity. If two reports should be filed, should they both contain the same information.
MRO's NERC Standards Review Subcommittee	Yes	The NSRS believes it is important for the ERO to provide valuable Lessons learned to our electrical industry, thus enhancing the reliability of the BES.
TransAlta Corporation	Yes	Electrical Reliability Organization (ERO) does not appear to be a defined term in the NERC Glossary of Terms on the NERC website. Last updated April 20, 2010.

Organization	Yes or No	Question 2 Comment
US Bureau of Reclamation	Yes	The question is focused on a limited area of Attachment A. There other problematic areas of Attachment 1 will be addressed in subsequent comments.
Ameren	Yes	
ATCO Electric Ltd.	Yes	
BGE	Yes	
Bonneville Power Administration	Yes	
City of Austin dba Austin Energy	Yes	
City of Garland	Yes	
Duke Energy	Yes	
Dynegy Inc.	Yes	
Green Country Energy	Yes	
Idaho Power Company	Yes	
Nebraska Public Power District	Yes	
NERC Staff	Yes	

Organization	Yes or No	Question 2 Comment
PacifiCorp	Yes	
PacifiCorp	Yes	
Pepco Holdings, Inc - Affiliates	Yes	
Puget Sound Energy	Yes	
Tenaska	Yes	
United Illuminating	Yes	

3. Do you agree with the requirement R1 and measure M1? Please explain in the comment box below.

Summary Consideration: There was no consensus amongst stakeholders who responded to this question. There was strong support for a central system for receiving and distributing impact event reports (a/k/a one stop shopping). There was general agreement that NERC was the most likely, logical entity to perform that function. However several respondents expressed their concern that the ERO could not be compelled to do so by a requirement in a Reliability Standard (not a User, Owner or Operator of the BES). In their own comments, NERC did not oppose the concept, but suggested that the more appropriate place to assign this responsibility would be the NERC Rules of Procedure. The DSR SDT concurs. The DSR SDT has removed the requirement from the standard and is proposing to make revisions to the NERC Rules of Procedure as follows:

> 812. NERC will establish a system to collect impact event reports as established for this section, from any Registered Entities, pertaining to data requirements identified in Section 800 of this Procedure. Upon receipt of the submitted report, the system shall then forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary. These reports shall be forwarded to the Federal Energy Regulatory Commission for impact events that occur in the United States. This can include state, federal, and provincial organizations. The ERO shall solicit contact information from Registered Entities appropriate governmental, law enforcement and regulatory agencies contact information for distributing reports.

The DSR SDT also believes NERC's additional concern about what data is applicable is addressed by the revisions to Attachment 1, and the inclusion of the OE-417 as an acceptable interim vehicle.

Organization	Yes or No	Question 3 Comment
WECC		R1 is appropriate for after-the-fact reporting. However, as proposed this standard eliminates all real-time notifications, including the CIP-001-1 R3 notice to appropriate parities in the Interconnection. New requirement R2.6 lists external parties to notify but it does not include the Reliability Coordinator. It is

Organization	Yes or No	Question 3 Comment
		important that the RC be notified of suspected sabotage. The RC's wide-area interconnection view and interaction with BAs may help recognize coordinated sabotage actions. Any "impact event" where sabotage is suspected as the root cause should require additional and real-time notifications.
ATC	No	ATC does not agree with R1 for three reasons:1. The ERO cannot be assigned obligations in NERC Standards. The requirements for the ERO should be addressed by a revision to Section 801 of the Rules of Procedure.2. This is a fill-in-the-blank requirement. The requirement, positioned as R1, does not allow for the obligations to be clearly defined. It refers to R6 which refers to R2 and Attachment 1. A clearer structure to the Standard would be to simply state that the Functional Entities have to meet the reporting obligations documented in Attachment 1 and delete the current R1.
BGE	No	R1 With the definition of "Impact Event", are we eliminating the term "Disturbance Reporting"? If we eliminate disturbance reporting, SDT should remove the reference from the Summary of Concepts and from the title, otherwise further definition on the distinction between the two terms is needed.R1. What is the "system" described here? What type of system is anticipated - electronic, programmatic or can it be better described by using "standard reporting form"?M1. Needs to seek evidence that the "system" was used for receiving reports, as well as distributing them.M1. Examples are more appropriately used in guidance documentation than in the standard. Rationale for R1 - Final statement regarding OE-417 needs to be removed. The ERO will establish the requirement in their "system" if the standard remains as is. The Requirement does not require the responsible entities to send OE-417 to DOE.
CenterPoint Energy	No	The ERO does not need to establish a "system for receiving reports" as the "system for receiving reports" is inherent given the requirements for reporting. The requirement also seems to add redundancy versus eliminating redundancy in the distribution of reports to applicable government, provincial or law enforcement

Organization	Yes or No	Question 3 Comment
		agencies on matters already reported by Responsible Entities. If an event is suspected to be an intentional criminal act, i.e. “sabotage”, the Responsible Entity would have contacted appropriate provincial or law enforcement agencies. The ERO is not in a position to add meaningful value to these reports as any information the ERO may provide is second hand. CenterPoint Energy recommends R1 and M1 be deleted.
City of Garland	No	Reason 1Most of this is duplication of existing processes - More “Big Government” and/or “Overhead” is not needed. There are already processes in place to notify “real time” 24 X 7 organizations that take action (RC, BA, TOP, DOE, FBI, Local Law Enforcement, etc) in response to an “impact event”. It is stated in your document on page five (5) “The proposed standard deals exclusively with after-the -fact reporting.” The combining of CIP 001 & EOP 004 should not expand on existing implemented reporting requirements nor should it result in NERC forming a 24 X 7 department to handle 1 hour (near real time) reporting requirements.Reason 2If this should go forward as drafted, NERC should not establish a “clearing house” for reporting requirements for Registered Entities without also taking legal responsibility for distributing those reports to required entities. It states in at least 2 places (Page 6 & Page 22) in the document that Responsible Entities are ultimately responsible for ensuring that OE-417 is received at the DOE. Thus, a Registered Entity could be penalized for violating this new standard if it did not file the reports with NERC or it could still be penalized (both criminal & civil) if they filed the reports with NERC but NERC (for whatever reason) did not follow through with ensuring the report was properly filed at the DOE.
Consolidated Edison Co. of NY, Inc.	No	See response to Question 2.
Duke Energy	No	The requirement again states the intent is to “enhance and support situational awareness”, which doesn’t sync with “after-the-fact reporting”. We question why NERC needs to create this report and system for

Organization	Yes or No	Question 3 Comment
		distributing impact event reports to various organizations and agencies for after-the-fact reporting, when we are still required to make real-time reports under other standards. For example, the Rational specifically recognizes that this standard won't release us from the DOE's OE-417 reporting requirement. We don't see that this provides value, unless NERC can find a way to eliminate redundancy in reporting.
Electric Market Policy	No	Having the ERO as an applicable entity is concerning as they are also the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. Establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC's open process. At this stage it is not clear how the ERO will develop or effectively maintain a list of "applicable government, provincial or law enforcement agencies" for distribution as defined in R1. The "rationale for R1" states that OE-417 could be included as part of the electronic form, but responsible entities will ultimately be responsible for ensuring that OE-417 reports are received at DOE. This requirement needs to be more definitive with respect to OE-417. It seems like the better approach would be for the entities to complete OE-417 form and this standard simply require a copy.
ERCOT ISO	No	Recommend that requirements for the Electric Reliability Organization be removed. However, if the requirements are retained, ERCOT ISO recommends the following wording change to be consistent with other standards. "R1. The ERO shall create, implement, and maintain a system for receiving and distributing impact event reports, received pursuant to Requirement R6, to applicable government, provincial or law enforcement agencies and Registered Entities to enhance and support situational awareness."
Exelon	No	This requirement should include explicit communications to the NRC (if applicable) of any reports including a nuclear generating unit as a jurisdictional agency to ensure notifications to other external agencies are

Organization	Yes or No	Question 3 Comment
		coordinated with the NRC. Depending on the event, a nuclear generator operator (NRC licensee) has specific regulatory requirements to notify the NRC for certain notifications to other governmental agencies in accordance with 10 CFR 50.72(b)(2)(xi). In general, the DSR SDT should include discussions with the NRC to ensure communications are coordinated or consider utilizing existing reporting requirements currently required by the NRC for each nuclear generator operator for consistency.
FirstEnergy	No	FirstEnergy proposes that requirement R1 and Measure M1 be deleted.A requirement assignment to the ERO is problematic and should not appear in a reliability standard. The team should keep in mind that all requirements will require VSL assignments that form the basis of sanctions. FE does not believe it is appropriate for the ERO to be exposed to a compliance violation investigation as the ERO is not a functional entity as envisioned by the Functional Model. If this "after-the-fact" reporting is truly needed for reliability then the standard must be written in a manner that does not obligate the ERO to reliability requirements. It would be acceptable and appropriate for a requirement to reference the "ERO Process" desired by R1, however, that process should be reflected in the Rules of Procedure and not a reliability standard.
Indeck Energy Services	No	This standard is an inappropriate place to define this requirement. NERC needs to be held accountable, but it should be independent of the standard. What if NERC fails to do it by the effective date of the standard, all Registered Entities will violate the standard until NERC is done. The effective date needs to be set based on NERC completing the system defined in R1.
Independent Electricity System Operator	No	R1 does not directly convey the need for reporting. The requirement could be written to require the responsible entities to report impact events to the ERO using a process to be described in the standard and according to a set of reporting criteria. Whether or not there is a “system” makes little difference if it complies with the requirement to provide the reports on time. In addition, an ERO established system which, without

Organization	Yes or No	Question 3 Comment
		being included in the standard and posted for public comment and eventually balloted, may not be acceptable to the entities that are responsible for reporting to the ERO. Further, a reliability standard should not need to bother with how the ERO disseminate this information to applicable government, provincial or law enforcement agencies. This is the obligation of the ERO and if required, can be included in the Rules of Procedure.
ISO New England Inc.	No	Having the ERO as an applicable entity raises a concern because they are also the Compliance Enforcement Authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. Establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC's open process. At this stage it is not clear how the ERO will develop or effectively maintain a list of "applicable government, provincial or law enforcement agencies" for distribution as defined in R1. The "rationale for R1" states that OE-417 could be included as part of the electronic form, but responsible entities will ultimately be responsible for ensuring that OE-417 reports are received at DOE. This requirement needs to be more definitive with respect to OE-417. The better approach would be for the entities to complete OE-417 form and this standard simply require a copy.
MidAmerican Energy	No	
NERC Staff	No	NERC staff is concerned about this requirement's applicability to the ERO. We feel that such a responsibility needs mentioning in the Rules of Procedure, the Compliance Monitoring and Enforcement Program (CMEP), or in a guideline document rather than in a standard requirement. Further, the requirement specifies "how" to manage the event data, not "what" should be monitored.

Organization	Yes or No	Question 3 Comment
North Carolina Electric Coops	No	The ERO cannot be subject to a requirement for which it is the compliance enforcement authority.
Northeast Power Coordinating Council	No	Having the ERO as an applicable entity raises a concern because they are also the Compliance Enforcement Authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. Establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC's open process. At this stage it is not clear how the ERO will develop or effectively maintain a list of "applicable government, provincial or law enforcement agencies" for distribution as defined in R1. The "rationale for R1" states that OE-417 could be included as part of the electronic form, but responsible entities will ultimately be responsible for ensuring that OE-417 reports are received at DOE. This requirement needs to be more definitive with respect to OE-417. The better approach would be for the entities to complete OE-417 form and this standard simply require a copy.
Puget Sound Energy	No	The language of R1 and M1 does not support the DSR SDT's goal of having a single form and system for reporting. The standard should specify the form and system rather than deferring that decision to the ERO. The language of R1 and M1 leaves the form and system to the ERO's discretion, which could lead to multiple forms and frequent revisions to them. This would lead to difficulties in tracking the reporting requirements. In addition, it is impossible to comment intelligently regarding the overall impact of the proposed standard and its requirements and measures without the reporting form and system being specified in the standard.
Santee Cooper	No	It cannot apply to the ERO.
SERC OC Standards Review	No	The ERO cannot be subject to a requirement for which it is the compliance enforcement authority. The

Organization	Yes or No	Question 3 Comment
Group		governance in this situation appears incomplete.
US Bureau of Reclamation	No	This standard should describe the ERO process of event documentation, analysis, and dissemination. Allowing the ERO to develop a event documentation, analysis, and dissemination process, which becomes a requirement on the Entities, must be derived through the Standards Development Process. The requirement, as it is currently worded, allows the ERO to develop standard requirements. If the intent is to only develop a means of collecting, which does not impose a requirement, the wording should state so. Otherwise, if the ERO wants to require that reports are posted to a specific location by the Entity, then it is a requirement and must go through the Standards Development Process. Secondly, there is already a single reporting form identified. It is not clear why the SDT could not accept that form as the reporting tool.
American Electric Power (AEP)	Yes	Overall we support the concepts; however, it is unclear if the ERO can be held accountable for compliance with NERC Requirements. If this requirement is removed there needs to be some mechanism for the ERO to establish a single clearinghouse.
City of Austin dba Austin Energy	Yes	Austin Energy would like to see OE-417 incorporated into the electronic form This will reduce the callout of EOP-004-2 and OE-417 forms in our checklists / documents and one form can be submitted to NERC and DOE.
E.ON Climate & Renewables	Yes	A generic ERCO approved electronic (form that can be submitted on-line) reporting form will help to add more clarity & consistency to the Impact event reporting process.
Georgia System Operations Corporation	Yes	Yes it would reduce duplication of effort and should ensure that the various entities and agencies all have consistent information. It should be simpler and quicker to file than what is needed to meet the current

Organization	Yes or No	Question 3 Comment
		standard.However, the system should allow for partial reporting and hierarchical reporting. Entities up the ladder in a reporting hierarchy may fill in additional info (usually from a wider scope of view) than what lower level entities are aware of. It would be better for information to go up a hierarchy than for bits and pieces to go to the ERO from many entities. Terminology may be different in each of the bits and pieces yet the same idea may be intended. The ERO may mistake multiple reports as being different events when they are all related to one event.The system should give an entity the ability to select the entities that should receive the impact event report.If hierarchical reporting is not enabled by the system, then entities should be allowed to work out a reporting hierarchy as a group and entities at lower levels should not be required to report over the NERC system. Some higher level entity would enter the information on the NERC system as coordinated by the entities within a group.
Idaho Power Company	Yes	the SDT must ensure that only a single form is required for compliance (such example OE-417)
IRC Standards Review Committee	Yes	Note that ERCOT does not sign on to this particular comment.
Kansas City Power & Light	Yes	Although we support situational awareness for the other registered entities, impact event reports should be distributed anonymously to communicate the information while protecting the registered entity.
Manitoba Hydro	Yes	Yes, keeping R1 generic and pointing to “government”, “Provincial”, “law” encompasses all entities in all major interconnections.
PacifiCorp	Yes	All efforts need to be made to include OE-417 reporting requirements to safeguard against duplicate reporting and / or delinquent reporting.One report for all events is more preferable than multiple reports for one event.

Organization	Yes or No	Question 3 Comment
RRI Energy, Inc.	Yes	While including the phrase "to enhance and support situational awareness" is a good use of the Results-Based Standards development tools and framework, the phrase is already included in the purpose statement. As such, it is unnecessary in Requirement 1. If it were to be included in Requirement 1, then it would also need to be included in each of the other Requirements 2 through 8. The "Purpose" statement captures this aptly.
Southern Company - Transmission	Yes	We do have one concern in that we are hopeful that NERC will develop a system that will allow a one stop shop of reporting.
Avmeren	Yes	
Arizona Public Service Company	Yes	
ATCO Electric Ltd.	Yes	
Bonneville Power Administration	Yes	
Constellation Power Generation and Constellation Commodities Group	Yes	
Dynegy Inc.	Yes	
Great River Energy	Yes	

Organization	Yes or No	Question 3 Comment
Green Country Energy	Yes	
Luminant Energy	Yes	
Midwest ISO Standards Collaborators	Yes	
MRO's NERC Standards Review Subcommittee	Yes	
Nebraska Public Power District	Yes	
Pacific Gas and Electric Company	Yes	
PacifiCorp	Yes	
Pepco Holdings, Inc - Affiliates	Yes	
PNM Resources	Yes	
PPL Electric Utilities	Yes	
PPL Supply	Yes	

Organization	Yes or No	Question 3 Comment
Tenaska	Yes	
TransAlta Corporation	Yes	
United Illuminating	Yes	
We Energies	Yes	

4. Do you agree with the requirement R2 and measure M2? Please explain in the comment box below.

Summary Consideration: Most stakeholders who responded to this question indicated disagreement with Requiremnet R2 and M2 as originally proposed. There were objections to the use of the term "Operating Plan" to describe the procedure to identify and report the occurrence of a disturbance. The DSR SDT concurs, and Operating plan has been replaced with the generic term "procedure" where appropriate believe that the use of a defined term is appropriate and has revised Requirement 1 to include Operating Plan, Operating Process and Operating Procedure.

R1. Each Responsible Entity shall have an Impact Event Operating Plan that includes [Violation Risk: Factor Medium] [Time Horizon: Long-term Planning]:

1.1. An Operating Process for identifying Impact Events listed in Attachment 1.

1.2. An Operating Procedure for gathering information for Attachment 2 regarding observed Impact Events listed in Attachment 1.

1.3. An Operating Process for communicating recognized Impact Events to the following:

1.3.1. Internal company personnel notification(s).

1.3.2. External organizations to notify to include but not limited to the Responsible Entities' Reliability Coordinator, NERC, Responsible Entities' Regional Entity, Law Enforcement, and Governmental or Provincial Agencies.

1.4. Provision(s) for updating the Impact Event Operating Plan within 90 days of any change to its content.

Other requirements reference the Operating Plan as appropriate. The requirements of EOP-004 fit precisely into the definition of Operating Plan:

Operating Plan: A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other

entities, etc., is an example of an Operating Plan.

Note R2 has been moved to R1 due to elimination of original R1. Many commenters felt that the requirements around updating the Operating Plan were too prescriptive, and impossible to comply with during the time frame allowed. The DSR SDT agrees, and Requirement R2 Parts 2.5 through 2.9 have been eliminated. They have been replaced with Requirement R1, Part 1.4 to update the Operating Plan within 90 days of any change to content.

Organization	Yes or No	Question 4 Comment
Bonneville Power Administration		As long as the 2.4 list is position based, not based on each individual that fills the position. (There is a concern of listing all 2.4 monitoring/reporting personnel in the company that cover the impact event, since there are different function groups and shift work. Documentation trails are difficult with personnel changes.) Because the CIP is being added, it requires an Operating Plan (instead of procedure) with 30 day revision timelines, so it increases the burden for electrical grid event reporting function. R2.9 language refers to R8 "annual" report; however R8 language is "quarterly" reporting of past year. It appears this standard is going to be in an update status 4 times per year, plus any event modifications plus personnel changes. This could be overly burdensome due to the expanding world of cyber security.
Ameren	No	While we agree with the intent to list certain minimum requirments for the Operating Plan, the draft list is too lengthy and prescriptive. This merely creates opportunites for failure to comply rather the real purpose of reporting data that can be used to meaningfully increase the reliability of the BES by identifying trends of events that may otherwise be ignored.
American Electric Power (AEP)	No	Component 2.2 "Method(s) of assessing cause(s) of impact events" is very vague. Furthermore, there are concerns whether these methods can be accomplished within one hour as might be required per Attachment

Organization	Yes or No	Question 4 Comment
		1, in addition to operating the system. Component 2.6 - need to add the statement "as appropriate for type of impact event" Components 2.7 through 2.9 - are good concepts to consider for future inclusion, but at this point in time these appear to be overreaching objectives. We recommend the SDT take smaller increments towards future progress at measure and reasonable pace. Furthermore, if Component 2.9 is retained it should only pertain to lessons learned on the reporting of impact events not all recommendations regarding remediation of the impact events themselves. Furthermore, the 30 day window to update the Operating Plans is aggressive considering the other priorities that may be present day to day.
ATC	No	The requirement should be rewritten to simply state that the Functional Entities has to meet the reporting obligations documented in Attachment 1. How the Functional Entity meets the obligations documented in Attachment 1 should be determined by the Functional Entity, not the requirement. The prescriptive nature of this requirement does not support the performance-based Standards that the industry and NERC are striving towards. In addition, requirement 2.9 creates an alternate method for NERC to develop Standards outside of the ANSI process. This requirement dictates that Functional Entities are required to incorporate lessons learned from NERC reports into their Plan, which is a requirement of this Standard.
BGE	No	R2.1 Creates the opportunity for differences in identifying impact events. BGE recommends additional clarity in the statement. Are we to use Attachment 1 as a "bright line" or can we use our Operating Plan to identify what an impact event is?R2.4 - 2.6 Does a standard need to specify both internal and external lists? 2.7 - is "component" defined anywhere? Is it a component of the BES or a component of the Operating Plan or a component of the three lists in 2.4 to 2.6?Rationale --- Parts 3.3 and 3.4?? Do you mean 2.3 and 2.4?Is the Operating Plan under scrutiny (mandatory and compensable) for all items in the last paragraph of the rationale?

Organization	Yes or No	Question 4 Comment
CenterPoint Energy	No	CenterPoint Energy does not agree with R2 and M2 as they are focused on process and procedure. Compliance with a reporting requirement should be based on a complete and accurate report submitted in a timely manner. The process an entity uses to accomplish that task is of no consequence. CenterPoint Energy recommends R2 and M2 be deleted.However, if the SDT feels it is necessary to include this process based requirement, CenterPoint Energy believes the SDT, in requiring an overly prescriptive Operating Plan, has expanded the requirement beyond the current CIP-001-1 and EOP-004-1 which only require "...procedures for the recognition of and for making operating personnel aware..." (CIP-001-1) and "...shall promptly analyze..." (EOP-004-1). Specifically, R2.2 is not found in the current Standards. "Methods for assessing causes(s) of impact events" would vary greatly depending upon the type and severity of the event. Responsible Entities would have a difficult time cataloging these various methods to any specific degree and if they are not specific then CenterPoint Energy questions their value in a documented method. R2.3 is not found in the current Standards and is an unnecessary requirement as the method of notification is irrelevant so long as the notification is made. R2.7, R2.8, and R2.9 are also unnecessary expansions beyond what is currently in CIP-001-1 and EOP-004-1. CIP-001-1 requires the Responsible Entity review its procedures annually and CenterPoint Energy believes this is sufficient. When taken in total, R2 requires seven (7) different processes, provisions, and methods. CenterPoint Energy recommends R2.2, R2.3, R2.7, R2.8 and R2.9 be deleted and believes this will not result in a reliability gap.
City of Garland	No	There are 4 "methods" and 2 "provision" required for this requirement - in other words, 6 "paperwork" items that auditors will audit and likely penalize entities for. On page 1, the statement is made "...proposed standard in accordance with Results-Based Criteria." Having to have 4 methods and 2 provisions to end with a report (all of which is paperwork) is not a "result based" standard. It is like being required to have a "plan to plan on planning on composing and filing a report". Events need to be analyzed, communicated, and reported and

Organization	Yes or No	Question 4 Comment
		should be audited as such (results based) - not audited on whether they have a book filled with methods and provisions.
Consolidated Edison Co. of NY, Inc.	No	Requirement R2 o Lead-in paragraph - Following the words “Attachment 1” add a period and the words “The Operating Plans shall” and then delete “that” and make “includes” singular. o R2.1, 2.2, 2.3, 2.7 - Replace the word “Method(s)” with the word “Procedure(s)”. o 2.6 - After the word “notify” add a period, then insert the words “For example, external organizations may include” and delete the words “to include but not limited to.” o 2.8 - After the words “Operating Plan based on” add the word “applicable”.Rational R2After the words “Every industry participant that owns or operates,” add the words “Bulk Electric System.” Then delete the words “on the grid.”
Constellation Power Generation and Constellation Commodities Group	No	Constellation Power Generation and Constellation Commodities Group has several issues with this requirement, but in general, this requirement is heavily prescriptive, administrative in nature, and is unclear whether it will positively impact BES reliability. As examples of administrative requirements that have no impact on reliability, please consider the following comments: oListing personnel in R2.4, - merely having a list of personnel does not add to the sufficiency of an Operating Plan, but it does create a burdensome obligation to maintain a list. As well, specifying “personnel” may limit plans from designating job titles or other designations that may more appropriately and consistently carry reporting responsibility in the Operating Plan. oR2.5 is unclear as to the intent of the requirement - what is threshold of notification? Is the list to be those that have a role in the event response or a list of all within the facility who may receive news notification of the event? Also, as explained above for 2.4, a list is not a beneficial to reliability, but is administratively burdensome. oWhat is the reasoning for the 30 day timeframe in R2.7 R2.8 and R2.9? The timeframe is not based on a specific necessity, and creates an unreasonable time frame for changing the Operating Plan, in

Organization	Yes or No	Question 4 Comment
		particular if lessons learned are either short turn adjustments or comprehensive programmatic changes what warrant more time to properly institute. In addition, coupled with other requirements (R4, R5, R8), the updating requirements of R2.7, R2.8 and R2.8 potentially create a continually updating Operating Plan which could create enough confusion to reduce the effectiveness of the Operating Plan. The updating and time frame requirements do not impact reliability, but again impose significant administrative burden and compliance exposure. oR2.9 is particularly problematic for its connection to R8. R8 requires NERC to create quarterly reports with lessons learned and R2.9 requires the registered entities to amend their Operating Plans? What if NERC doesn't write an annual or quarterly report? Are the registered entities out of compliance? The "summary of concepts" for this latest revision, as written by the SDT, includes the following items: oA single form to report disturbances and impact events that threaten the reliability of the bulk electric system oOther opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements oClear criteria for reporting oConsistent reporting timelines oClarity around of who will receive the information and how it will be usedMany of the sub-requirements in R2 do not address any of these items and do not serve to establish a high quality, enforceable and reliability focused standard. Constellation Power Generation therefore recommends that R2 be amended to read as follows:R2. Each Applicable Entity identified in Attachment 1 shall have an Operating Plan(s) for identifying, assessing and reporting impact events listed in Attachment 1 that includes the following components: 2.1. Method(s) for identifying impact events listed in Attachment 12.2. Method(s) for assessing cause(s) of impact events listed in Attachment 12.3. Method(s) for making internal and external notifications should an impact event listed in Attachment 1 occur. 2.4. Method(s) for updating the Operating Plan.2.5 Method(s) for making operation personnel aware of changes to the Operating Plan.
Consumers Energy	No	R 2.7, R 2.8 and R 2.9 are creating a requirement to have procedures to update procedures. Having updated

Organization	Yes or No	Question 4 Comment
		procedures should be the requirement, no more.
Duke Energy	No	Sections 2.4 and 2.5 should allow identification of responsible positions/job titles rather than specific people. Section 2.9 only allows 30 days for updates to our plan based upon lessons learned coming out of an annual report. 60-90 days would be more appropriate. Also, Section 2.9 says it's an annual report, while R8 only requires quarterly reports.
Dynegy Inc.	No	For 2.7, 2.8, 2.9, 30 days is to stringent. Some changes may not warrant changes until a cumulative amount of changes occur. Suggest making it no later than an annual review.
E.ON Climate & Renewables	No	Administrative burden to some of the components such as 2.5.
Electric Market Policy	No	This is an overly prescriptive requirement given the intent of this standard is after-the-fact reporting. The requirement to create an Operating Plan lacks continuity with the ERO Event Analysis Process that is currently slated to begin industry field testing on October 25, 2010. Suggest the SDT coordinate EOP-004-2 efforts with this process.R2.6 establishes an external organization list for Applicable Entity reporting, yet R1 suggests that external reporting will be accomplished via submittal of impact event reports. How will the two requirements be coordinated? What governmental agencies are appropriate and how will duplicative reporting be addressed (for example, DOE, Nuclear Regulatory Commission)? Also, in the "rationale for R2", please explain the reference to Parts 3.3 and 3.4.
ERCOT ISO	No	ERCOT ISO recommends the use of "Registered Entity" in place of "Applicable Entity". This would provide consistency with other requirements and Attachment 1. Recommend the following changes to the subrequirements. "2.6. List of external organizations to notify to include but not limited to NERC, Regional

Organization	Yes or No	Question 4 Comment
		Entity, relevant entities within the interconnection, Law Enforcement, and Governmental or Provincial Agencies.""2.7. Process for updating the Operating Plan within 30 days of any changes not of an administrative nature. This includes updates to reflect any lessons learned as a result of an exercise or actual event."Remove requirement 2.8 and move content to requirement 2.7."2.8. Process for updating the Operating Plan within 30 days of publication the NERC annual report of lessons learned."Add "2.9. Process to ensure updates are communicated to personnel responsible for under the Operating Plan within 30 days of the change being completed."
Exelon	No	R.2.4 and 2.5 - should not be required to have a list of internal personnel. If an entity has an Operating Plan that covers internal and external notifications that should be sufficient.R2.2.7, 2.8, 2.9 - R4 requires an annual drill. Updating the plan if required following an annual drill should be sufficientWhy does an entity need to develop a stand alone Operating Plan if there is an existing process to address identification, assessing and reporting certain events?30 day implementation for a component change or lesson learned does not seem reasonable or commensurate with the potential impact to the BES and should not be a required element of EOP-004.What is the communication protocol for lessons learned outside of the annual NERC report? What process will be followed and who will review, evaluate, and disseminate lessons learned that warrant updating the Operating Plan?
FirstEnergy	No	The term Operating Plan(s) is not the appropriate term for this standard. These should be called Reporting Plan(s). Operating Plans are usually designed to be applied during the operating timeframe. Parts 2.2 and 2.6 - We suggest changes to these two subparts as well as a new 2.2.1 and 2.6.1 as follows: 2.2. Method(s) for assessing the initial probable cause(s) of impact events(Add) 2.2.1. Method(s) for assessing the external organizations to be notified.2.6. List of external organizations to notify in accordance with Part 2.2.1. to

Organization	Yes or No	Question 4 Comment
		include but not limited to NERC, Regional Entity, and Governmental Agencies.(Add) 2.6.1. Method(s) for notifying Law Enforcement as determined by Part 2.2.1.Parts 2.4 and 2.6: This should be a list of job titles for ease of maintenance. An entity may choose to use someone in a job position that is a 24 by 7 operation with several personnel that cover that position over the 24 by 7 period. Listing each person by name should not be required as personnel change while the operating responsibility related to the job title can remain constant. We suggest changing the wording to "2.4. List of the job titles of internal company personnel responsible for making initial notification(s) in accordance with Parts 2.5.and 2.6.2.5. List of the job titles of internal company personnel to notify."Part 2.6 - We are under the impression that the phrase "include but not limited to" should not be used according to the NEW SDT guidelines. We suggest changing this to say "List of external organizations to notify that includes at a minimum, NERC, Regional Entity, and Governmental Agencies. (A provincial agency is a governmental agency)."Part 2.7. is overly burdensome. FE suggests the team revise to simply reflect annual updates that should consider component changes and updates from lessons learned. This also permits parts 2.8 and 2.9 to be deleted. FE proposes the following text for Requirement R2.7 "Annual review, not to exceed 15 months between reviews, and update as needed of the Reporting Plan that considers component changes and continuous improvement changes from lessons learned."Parts 2.8 and 2.9 - FE proposes to delete part 2.8 and 2.9. We do not see a need for these changes since the plan must be updated annually and will cover lessons learned.
Great River Energy	No	A. As detailed in R2, the Operating Plan shall contain provisions for “identifying, assessing, and reporting impact events”. R2.8, and R2.9 do not have a correlation to R2’s Operating Plan. Where, R2.7 states to update the Operating Plan when there is a component change. We believe that the components of this Operating Plan are only 1) indentifying impact events, 2) assessing impact events, and 3) reporting impact events. R2.8 and R2.9 are based on Lessons Learned (from internal and external sources) and do not fit in

Organization	Yes or No	Question 4 Comment
		the components of an entity's Operating Plan. R2.7 requires the Operating Plan to be updated. As written, every memo, simulations, blog, etc that contain the words "lessons learned" would be required to be in your Operating Plan. It is solely up to an entity to implement a "Lesson Learned" and not the place for this SDT to require an Operating Plan to contain Lessons Learned. Recommend that R2.8 and R2.9 be deleted for this requirement. If R2.8 and R2.9 are not removed, R5.3 will be in a constant state of change. B. In R2.8 & R2.9, It may be difficult to implement lessons learned within 30 days. We suggest that lessons learned should be incorporated within 12 calendar months if lessons learned are not deleted from the R2.8 & R2.9.
Green Country Energy	No	Highly administrative version of what could accomplish the same thing. A requirement that the applicable entitiy shall make appropriate notificatiions as required by attachment A and B events. I can see the need for review and lessons learned but that needs to be done at a higher level since many entities may be involved in an "event"
Idaho Power Company	No	The SDT needs to clarify Requirement 2.9 references an annual report issued persuant to requirement R8, however Requirement 8 references a quarterly report. These requirements should have the same time frames.
Indeck Energy Services	No	R2 needs to state that the Operating Plan needs to only those Attachment 1 events applicable to the Registered Entity. The Operating Plan should contain a list of these events so that the other Requirements can reference the Operating Plan and not Attachment 1 for the list of events. For example a GO/GOP <2,000 MW would not need to address this type of event and it wouldn't be listed in its Operating Plan. It would be unnecessarily cumbersome, to describe events which are not covered within the Operating Plan.
Independent Electricity System	No	R2 is not needed. An entity does not need to have an "operating plan" to identify and report on impact events;

Organization	Yes or No	Question 4 Comment
Operator		it needs only to report on the events listed in Attachment 1 in a form depicted in Attachment 2. How does the entity do this, and whether or not an operating plan is in place, or whether its staff is trained to provide the report should not need to be included in a reliability standard for so long as the responsible entity provides the report in the required form on time. If the responsible entity fails to report the listed events in the depicted format, it will be found non-compliant, and that's it - no more and no less. If the "operating plan" really means an established data collection and reporting procedure, then the requirement should be revised to more clearly convey the intent.
IRC Standards Review Committee	No	The SRC suggests that this is not, in fact, an Operating Plan. At most, it may be a reporting plan or reporting procedure. Most of these requirements are administrative and procedural in nature and, therefore, do not belong as requirements in a Reliability Standard. Perhaps they could be characterized as a best practice and have an associated set of Guidelines developed and posted on the subject.As proposed, the Operating Plan is not required to ensure bulk power reliability. As stated in the purpose of this standard, it does not cover any real-time operating notifications for the types of events covered by CIP-001, EOP-004. The Operating Plan requirements as proposed seem only to be suitable for real-time notifications. Since these incidents are meant to be reportable after-the-fact, familiarity with the reporting requirements and time frames is sufficient. Unlike the real-time operating notifications which have relatively short reporting time frames, there is sufficient time for personnel to make appropriate communications within their organizations to make timely after the fact reports under NERC Section 1600 authority. Would it be feasible for NERC to issue a standing requirement for timely after-the-fact reports under NERC Section 1600 authority?
ISO New England Inc.	No	This is an overly prescriptive requirement given that the intent of this standard is after-the-fact reporting. The requirement to create an Operating Plan is an unnecessary burden that offers no additional improvements to

Organization	Yes or No	Question 4 Comment
		the reliability of the Bulk Electric System, and this is not, in fact, an Operating Plan. At most, it may be a reporting plan. Most of these requirements are administrative and procedural in nature and, therefore, do not belong as requirements in a Reliability Standard. Perhaps they could be characterized as a best practice and have an associated set of Guidelines developed and posted on the subject.As proposed, the Operating Plan is not required to ensure Bulk Electric System reliability. As stated in the purpose of this standard, it does not cover any real-time operating notifications for the types of events covered by CIP-001, EOP-004. Since these incidents are meant to be reportable after-the-fact, familiarity with the reporting requirements and time frames is sufficient.Stating reporting requirements directly in the standard would produce a more uniform and effective result across the industry, contributing towards a more reliable Bulk Electric System.R2.6 establishes an external organization list for Applicable Entity reporting, yet R1 suggests that external reporting will be accomplished via submittal of impact event reports. How will the two requirements be coordinated? What governmental agencies are appropriate, and how will duplicative reporting be addressed (for example, DOE, Nuclear Regulatory Commission)? Also, in the "rationale for R2", please explain the reference to Parts 3.3 and 3.4.
Kansas City Power & Light	No	We agree with the rationale for R8 requiring NERC to analyze Impact Events that are reported through R6 and publish a report that includes lessons learned but disagree with R2.9 obligating an entity to update its Operating Plan based on applicable lessons learned from the report. Whether lessons learned are applicable to an entity is subjective. If an update based on lessons learned from an annual NERC report is required, the requirement should clearly state the necessity of the update is determined by the entity and the entity's Reliability Coordinator or NERC can not make that determination then find the entity in violation of the requirement. In addition, if an update based on lessons learned from a NERC report is required, NERC should publish the year-end report (R8) on approximately the same day annually (i.e. January 31) and allow

Organization	Yes or No	Question 4 Comment
		an entity at least 60 days to analyze the report and incorporate any changes it deems necessary in its Operating Plan. In addition, the language using quarterly and annual as a requirements between R2.9 and R8 is confusing.
MidAmerican Energy	No	R2 and R5 coupled with R8 will drive quarterly updates (in addition to drills, etc) and training to the literally hundreds to thousands of people per company for the proper internal operating personnel and management will actually hurt the development of a culture of compliance by overwhelming personnel with constant plan changes and training.The standards drafting team should remove all 30 day references or provide the technical basis of why revising plans and training to "changes and lessons learned" quarterly all within 30 days is the right use of reliability resources to improve the grid.The addition of the 30 day constraints and new vague criteria in Attachment one such as "damage to a BES element through and external cause" or "transmission loss of multiple BES elements which could mean two or more" is the opposite of clear standards writing or results based standards. We disagree with requiring an Operating Plan for identifying, assessing, and reporting impact events. This is an administrative requirement that has no clear reliability benefit. Furthermore, it is questionable that event reporting even meets the basic definition of an Operating Plan. Per the NERC glossary of terms, Operating Plans contain Operating Procedures or Operating Processes which encompass taking action real-time on the BES not reporting on it. As detailed in R2, the Operating Plan shall contain provisions for "identifying, assessing, and reporting impact events". R2.8, and R2.9 do not have a correlation to R2's Operating Plan. Where, R2.7 states to update the Operating Plan when there is a component change, the components of this Operating Plan are only 1) indentifying impact events, 2) assessing impact events, and 3) reporting impact events. R2.8 and R2.9 are based on Lessons Learned (from internal and external sources) and do not fit in the components of an entity's Operating Plan. R2.7 requires the Operating Plan to be updated. As written, every memo, simulations, blog, etc that contain the

Organization	Yes or No	Question 4 Comment
		words "lessons learned" would be required to be in your Operating Plan. It is solely up to an entity to implement a "Lesson Learned" and not the place for this SDT to require an Operating Plan to contain Lessons Learned. Recommend that R2.8 and R2.9 be deleted for this requirement. If R2.8 and R2.9 are not removed, R5.3 will be in a constant state of change. In R2.8 & R2.9, It may be difficult to implement lessons learned within 30 days. The NSRS recommends to incorporate lessons learned within 12 calendar months if lesson learned are not deleted from the R2.8 & R2.9.
Midwest ISO Standards Collaborators	No	We disagree with requiring an Operating Plan for identifying, assessing, and reporting impact events. This is an administrative requirement that has no clear reliability benefit. Furthermore, it is questionable that event reporting even meets the basic definition of an Operating Plan. Per the NERC glossary of terms, Operating Plans contain Operating Procedures or Operating Processes which encompass taking action real-time on the BES not reporting on it. What is an impact event? It appears that this undefined, ambiguous term was substituted for sabotage which is also undefined and ambiguous. One of the SARs stated goals was to "provide clarity on sabotage events". This does not provide clarity.
MRO's NERC Standards Review Subcommittee	No	A. As detailed in R2, the Operating Plan shall contain provisions for "identifying, assessing, and reporting impact events". R2.8, and R2.9 do not have a correlation to R2's Operating Plan. Where, R2.7 states to update the Operating Plan when there is a component change. The NSRS believes the components of this Operating Plan are only 1) indentifying impact events, 2) assessing impact events, and 3) reporting impact events. R2.8 and R2.9 are based on Lessons Learned (from internal and external sources) and do not fit in the components of an entity's Operating Plan. R2.7 requires the Operating Plan to be updated. As written, every memo, simulations, blog, etc that contain the words "lessons learned" would be required to be in your Operating Plan. It is solely up to an entity to implement a "Lesson Learned" and not the place for this SDT to

Organization	Yes or No	Question 4 Comment
		require an Operating Plan to contain Lessons Learned. Recommend that R2.8 and R2.9 be deleted for this requirement. If R2.8 and R2.9 are not removed, R5.3 will be in a constant state of change. B. In R2.8 & R2.9, It may be difficult to implement lessons learned within 30 days. The NSRS recommends to incorporate lessons learned within 12 calendar months if lesson learned are not deleted from the R2.8 & R2.9.
North Carolina Electric Coops	No	This requirement dictates details of documentation of after-the-fact reporting of events which cannot impact reliability of the BES and, as such, should not be a reliability standard. The cost and burden of becoming auditably compliant with this requirement can be extreme for small entities.
Northeast Power Coordinating Council	No	This is an overly prescriptive requirement given that the intent of this standard is after-the-fact reporting. The requirement to create an Operating Plan is an unnecessary burden that offers no additional improvements to the reliability of the Bulk Electric System, and this is not, in fact, an Operating Plan. At most, it may be a reporting plan. Most of these requirements are administrative and procedural in nature and, therefore, do not belong as requirements in a Reliability Standard. Perhaps they could be characterized as a best practice and have an associated set of Guidelines developed and posted on the subject.As proposed, the Operating Plan is not required to ensure Bulk Electric System reliability. As stated in the purpose of this standard, it does not cover any real-time operating notifications for the types of events covered by CIP-001, EOP-004. Since these incidents are meant to be reportable after-the-fact, familiarity with the reporting requirements and time frames is sufficient.Stating reporting requirements directly in the standard would produce a more uniform and effective result across the industry, contributing towards a more reliable Bulk Electric System.R2.6 establishes an external organization list for Applicable Entity reporting, yet R1 suggests that external reporting will be accomplished via submittal of impact event reports. How will the two requirements be coordinated? What governmental agencies are appropriate, and how will duplicative reporting be addressed (for example, DOE,

Organization	Yes or No	Question 4 Comment
		Nuclear Regulatory Commission)? Also, in the "rationale for R2", please explain the reference to Parts 3.3 and 3.4.
Pacific Gas and Electric Company	No	PG&E would like clarification on whether the 30 days, is calendar days or business days.
Pacific Northwest Small Public Power Utility Comment Group	No	See #15
Pepco Holdings, Inc - Affiliates	No	For R 2.7, 2.8 and 2.9, 30 days may be too short a time for large entities with multiple subsidiaries to do the necessary notice and coordination. PHI suggests 90 days.
PNM Resources	No	PNM would like clarification on whether the 30 days, is calendar days or business days.
PPL Electric Utilities	No	While we agree with documenting our process, we feel the use of the defined term Operating Plan is not required and possibly a misuse of the term. We would like to suggest using the term 'procedure'. Additionally, we would like the SDT to confirm/clarify whether Attachment 1 is a complete list of impact events. Also, please confirm that the Proposed R2.1 language 'Method(s) for identifying impact events' means identifying impact event occurrence as opposed to identifying list of impact events. i.e. does R2.1 mean recognize impact event occurrence?
PPL Supply	No	While we agree with concept addressed in R2, we don't agree with use of the defined term Operating Plan. Consider working the requirement as follows: "Each Applicable Entity identified in Attachment 1 shall have a documented process or program that includes the following components:..." Also, please consider changing 2.1 to be"Method(s) for recognizing the occurrence of impact events." The current wording could be

Organization	Yes or No	Question 4 Comment
		interpreted to mean, "create a list of the impact events."
Puget Sound Energy	No	While the concept of an operating plan is reasonable, the requirements for update in sections 2.7, 2.8 and 2.9 will lead to an immense amount of work for the entities subject to the standard. In addition, constant revisions to the operating plan makes it difficult to cement a habit through this procedure. The proposed update schedule does not strike the appropriate balance between the need to respond to lessons learned and the value of plan continuity.
RRI Energy, Inc.	No	1. R2 includes the phrase "for identifying, assessing and reporting," followed by R2.1 which states "identifying," R2.2 which states "assessing" and both R2.3 and R2.6 state "notify" or "making internal and external notifications" (i.e., reporting). The language is unnecessarily redundant. RECOMMENDATION: Reword R2 phrase "for identifying, assessing and reporting," to simply state, "for addressing."2. Rationale for R2 - The rationale section for R2 references in the third paragraph "Parts 3.3 and 3.4." Was this intended to reference R2.3 and R2.4?
Santee Cooper	No	The words “operating plan” should be removed from the requirement. This standard deals exclusively with after-the-fact reporting. This requirement is also overly prescriptive.
SERC OC Standards Review Group	No	This is an overly prescriptive requirement that dictates details of documentation and, as such, has no place in a reliability standard. NERC needs to trust the RCs to do their jobs; this standard and this requirement in particular seems to be attempting to codify the actions that an RC would take in response to an event. The cost and burden of becoming auditably compliant with this requirement is extreme and unrealistic, especially on small entities

Organization	Yes or No	Question 4 Comment
Southern Company - Transmission	No	The Operating Plan has a different connotation for different operations folks. We suggest that we call it an Impact Event Reporting Plan.
Tenaska	No	We have adequate compliance procedures already in place for the existing CIP-001-1 and EOP-004-1 Standards. The list of required “Operating Plan” components in the proposed R2 is too specific. Maintaining the “Operating Plan” described in R2 would increase the burden on Registered Entities to comply with the Standard and this type of "laundry list" Requirement would make it more difficult to prove compliance with EOP-004-2 during an audit.
United Illuminating	No	R2.9 requires provisions to update the Operating Plan based on the annual ERO report developed in R8. The ERO report does not appear to be providing lessons learned to be applied to the Operating Plan for impact event reporting, but more focsed on trends and threats to the BES. Also 30 days after the report is published by NERC is not enough time for the entity to read, and assess the report, and then to administratively update the Operating Plan. UI agrees that the Operating Plan should be reviewed annually and updated subsequent to the review within 30 days.
US Bureau of Reclamation	No	R2 does not reconcile with Attachment A or the sub paragraphs. As an example, the requirement 2.6 states "List of organizations to notify ...." All sub paragraphs use the term notify. Notify as used in Attachment A is when a report cannot be provided in the time frame listed in Attachment A. Therefore there is no requirement in this standard for the Operating Plan to have a provision for reporting.The subparagraph 2.8 indicates that the Entity must update it plan based on the lessons learned published by NERC. It would be appropriate to require a review and update of the plan based on the lessons learned.

Organization	Yes or No	Question 4 Comment
We Energies	No	R2.3, R2.4: “Part” is not a defined term or used in the NERC Standard Process Manual.R2: Attachments are not mentioned in the NERC Standard Process Manual. Is this a mandatory or informational part of the standard?R2.6 (and possibly R2.5): There does not seem to be discretion in notifications. Are all people or organizations on the notify lists always contacted for every impact event? Even Law Enforcement?R2.7: What is a “component? A Plan component? A BES component?R2.9: There is no annual NERC report issued pursuant to R8. R8 requires quarterly reporting.
WECC	No	Need clarification on whether the 30 days is calendar days or business days. As noted in the comment to question 3, any impact event where sabotage is suspected should be treated differently from those where sabotage is not suspected.
Arizona Public Service Company	Yes	AZPS agrees with R2, however, the use of the term "Operating Plan" is confusing. A more accurate term would be "Event Reporting Plan."
ATCO Electric Ltd.	Yes	
City of Austin dba Austin Energy	Yes	
Georgia System Operations Corporation	Yes	An entity-developed Operating Plan will allow the flexibility needed to address different entity relationships around the country, e.g., generating companies, cooperatives, munis, large IOUs, small IOUs, RTOs/ISOs, non-independent market area, and so on.However, all applicable entities should not be required to report directly to NERC or the region. The system should allow for partial reporting and hierarchical reporting. Entities within an area should be allowed to coordinate their plans to define reporting procedures within their area. They could have an entity at some wide scope top level that reports to NERC and the region the

Organization	Yes or No	Question 4 Comment
		information collected from multiple narrow scope lower levels within their wide area. If every small lower level entity directly reported to NERC and the Region, it could create situational confusion rather then situation awareness.
Manitoba Hydro	Yes	R2 - 2.1 to 2.9 detail what is expected of an Operating Plan for Impact Events.The attachment 1 details the event, the threshold parameters and time line. Though the threshold parameters in the attachment may be questioned, this greatly clarifies the expectations of reporting events. Further events should be added to this list:"Detection of suspected or actual or acts or threats of physical sabotage"
Luminant Energy	Yes	
Nebraska Public Power District	Yes	
NERC Staff	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	
TransAlta Corporation	Yes	

5. Do you agree with the requirement R3 and measure M3? Please explain in the comment box below.

Summary Consideration: There was no consensus amongst stakeholders who responded to this question. Requirement R3 has been re-written to exclude the requirement to "assess the initial probable cause". The only remaining reference to "cause" is in the Impact Event Reporting Form (Attachment 2). Here, there is no longer a requirement to assess the probable cause. The probable cause only needs to identified, and only if it is known at the time of the submittal of the report.

Organization	Yes or No	Question 5 Comment
Ameren	No	There are too many missing details on how this will be accomplished. As stated before, this Draft requires too much time be invested in verbal reports, "Preliminary" reports, "Final" reports and even "Confidential" reports (Attachment 2). If the goal is to report ASAP details on events which could impact BES reliability, all of these reports will need to be made at the worst possible time - when Operators are trying to collect data, analyze what they find and correct major problems on the system. And if the reports are wrong or not issued fast enough, the Operators will be keenly aware of potential fines and violations.
American Electric Power (AEP)	No	Not clear how this is different from R6 since it relies on the same timetable in Attachment 1.
ATC	No	ATC believes that this requirement should be deleted and that the SDT should coordinate its goal with the EAWG. We believe that the lessons learned process and identification of root cause is better covered under that process than through the NERC Mandatory Standards.
BGE	No	R3. Limits responsibility to Attachment 1 events only and mandates that an "initial probable cause" be identified. Are we at liberty to define "initial probable cause" and define time period for completion in the Operating Plan? BGE believes this could cause wide difference between Operating Plans and the standard

Organization	Yes or No	Question 5 Comment
		should be more prescriptive by relating to a time-table for the life of an impact event, including expected identification time, initial assessment time and analysis time leading to the reporting deadlines.BGE recommends not including examples of evidence in a measure but include it in a Guideline. Including in a measure will be translated as a requirement by an auditor.
CenterPoint Energy	No	CenterPoint Energy does not agree with R3 and M3 as written as the Company does not agree with the requirement to have an Operating Plan (see comments to Q4 above). However, if R2 and M2 were to be deleted, and R3 was revised to read; "Each Applicable Entity shall identify and assess initial probable cause of events listed in Attachment 1.", CenterPoint Energy could agree with this requirement.
City of Garland	No	Should be part of R2 or R6 - this is unnecessary duplication
Constellation Power Generation and Constellation Commodities Group	No	This requirement introduces double jeopardy for registered entities. If an entity does not include methods for identifying impact events and for assessing cause per R2.1 and R2.2 in their Operating Plan, they will be out of compliance with R2. Without the methods in R2 the registered entity is out of compliance with R3 as well for failing to identify and assess. Constellation Power Generation therefore recommends that R3 be amended to be incremental to R2 and read as follows: R3. Each Applicable Entity shall implement their Operating Plan(s) to identify and assess cause of impact events listed in Attachment 1.
Electric Market Policy	No	We think "impact event" needs to be defined in the NERC Glossary to provide the clarity the industry needs to build audit ready compliant procedures.
ERCOT ISO	No	ERCOT ISO recommends the use of "Registered Entity" in place of "Applicable Entity". This would provide consistency with other requirements and Attachment 1. The measure for this requirement notes the obligation

Organization	Yes or No	Question 5 Comment
		for “documentation”. This is not addressed in the requirement. The measure also notes “on its Facilities”. This clarification of scope should be addressed in the requirement. R3. Each Registered Entity shall identify, assess, and document initial probable cause of impact events on its Facilities listed in Attachment 1.
Exelon	No	: Agree that Each Applicable Entity shall identify and assess initial probable cause of impact events; disagree with aspects and time requirements in Attachment 1.
FirstEnergy	No	M3 - Power flow analysis would be used to assess the impact of the event on the BES, not to determine initial probable cause. It is more likely that DME would provide the data for the initial probable cause evaluation. We suggest rewording M3 as follows: "To the extent that an Applicable Entity has an impact event on its Facilities, the Applicable Entity shall provide documentation of its assessment or analysis. Such evidence could include, but is not limited to, operator logs, voice recordings, or disturbance monitoring equipment reports. (R3)"
Green Country Energy	No	Actually yes and no... An event may be caused, analyzed and corrected by one entity but most likely it will involve more. Low Voltage or frequency may not be caused by a generator but the generator will see the event and to have the generator assess the probable cause seems inappropriate. I can see reporting the event and duration and making notifications.
Indeck Energy Services	No	R3 should reference the events covered by the Operating Plan, as listed in it, rather than in Attachment 1. If the Plan is deficient, it is a violation of R2 and not every other Requirement that references the Plan.
Independent Electricity System Operator	No	We agree that the responsible entity needs to identify and assess initial probable cause of impact events but not in accordance with any operating plan in R2. Each operating entity (RC, BA, TOP) has an inherent responsibility to identify the cause of any system events to ensure it complies with a number of related

Organization	Yes or No	Question 5 Comment
		operational standards. R3, in fact, could be revised to require the Responsible Entity to include the probable cause of impact events in its report, rather than asking it to "identify and assess" since this is not measurable. Also, the ERO may be removed from the Applicability Section depending on the response to our comments under Q9.
IRC Standards Review Committee	No	Although it is useful for entities to make an initial assessment of a probable cause of an event, this requirement should stand alone and does not need to be tied to requirement R2, Operating Plan. Quite often, it takes quite some time for an actual cause to be determined. The determination process may require a root cause analysis of some complexity.Further, in the case of suspected or potential sabotage, the industry can only say it doesn't know, but it may be possible. It really is the law enforcement agencies who make the determination of whether sabotage is involved and the info may not be made available until an investigation is completed, if indeed it is ever made available.
ISO New England Inc.	No	We think "impact event" needs to be defined in the NERC Glossary to provide the clarity the industry needs to build auditable compliance procedures.Although it is useful for entities to make an initial assessment of a probable cause of an event, this requirement should stand alone and does not need to be tied to requirement R2, Operating Plan. Quite often, it takes a considerable amount of time for an actual cause to be determined. The determination process may require a complex root cause analysis.Further, in the case of suspected or potential sabotage, the industry can only say it doesn't know, but it may be possible. Law enforcement agencies make the determination of whether sabotage is involved, and the information may not be made available until an investigation is completed, if indeed it is ever made available.
Kansas City Power & Light	No	We believe R3 and M3 are unnecessary as a stand alone requirement and measure and propose combining this requirement and measure with R6 and M6. Identifying and assessing the initial probable cause of an

Organization	Yes or No	Question 5 Comment
		impact event is the obvious starting point in the reporting process and ultimate completion of the required report. Evidence to support the identification and assessment of the impact event and evidence to support the completion and submittal of the report are really one in the same.
Manitoba Hydro	No	Though each local entity should identify and assess initial probable cause of impact events as per their Operating Plan, the creation of this Operating Plan could be labor intensive and also guidelines for consistency within an RC region should be created.So “NO” is entered simply because a large time line would be needed to properly and efficiently implement R3 and R4.
MidAmerican Energy	No	
Midwest ISO Standards Collaborators	No	While we agree that it makes sense to report on the cause of an event, we disagree with the need for an Operating Plan as identified in R2.
North Carolina Electric Coops	No	The term “impact event” needs to be defined in the NERC Glossary to provide the clarity the industry needs to build auditably compliant procedures and give guidance on what is proper to report.
Northeast Power Coordinating Council	No	"Impact event” needs to be defined in the NERC Glossary to provide the clarity the industry needs to build auditable compliance procedures.Although it is useful for entities to make an initial assessment of a probable cause of an event, this requirement should stand alone and does not need to be tied to requirement R2, Operating Plan. Quite often, it takes a considerable amount of time for an actual cause to be determined. The determination process may require a complex root cause analysis.Further, in the case of suspected or potential sabotage, the industry can only say it doesn’t know, but it may be possible. Law enforcement agencies make the determination of whether sabotage is involved, and the information may not be made

Organization	Yes or No	Question 5 Comment
		available until an investigation is completed, if indeed it is ever made available.
Pacific Northwest Small Public Power Utility Comment Group	No	Comments: When applying R3 to row 11 of attachment 1, the comment group notes that applicable entities are expected to assess probable cause of BES equipment damage, including that which may be the result of criminal behavior. At best this would needlessly duplicate the efforts of law enforcement. A more likely result is that entity involvement would interfere with law enforcement and ultimately hinder prosecution of those responsible. Also See #15
PPL Electric Utilities	No	We believe the rationale for R3 is good and provides value. However, we feel the clarity was lost when the rationale was translated to the standards language. Please consider revising language to refocus on rationale of assess and report per Attachment 1 as opposed to identify. We suggest changing the word “identify” to “recognize” and add the Rationale statement to the requirement as follows: “Each Applicable Entity shall assess the causes of the reportable event and gather available information to the complete the report.”
PPL Supply	No	Please consider changing the word "identify" to "recognize" and adding the Rationale statement to the requirement as follows: "Each Applicable Entity shall assess the causes of the reportable event and gather available information to complete the report."
RRI Energy, Inc.	No	"Identify and assess" - Auditors are as much in need of clearly worded, unambiguous Reliability Standards are as Registered Entities. This phrase leaves much too wide a range of interpretations, almost guaranteeing regular and frequent disagreements during an audit between Registered Entity and Regional Entity auditor as to what constitutes "identify and assess" sufficient to meet the intent of this Requirement. Compounding this issue is the Rationale for R3 that states an Applicable Entity (which should probably read "applicable

Organization	Yes or No	Question 5 Comment
		Functional Entity") should "gather enough information to complete the report that is required to be filed." While Rationale statements are not technically part of the standard, this emphasizes the current wording of the requirement as subject to random and arbitrary interpretation by auditors and Registered Entities. RECOMMENDATION: Change "identify and assess" to "document," so that the Requirement now reads "Each Applicable Entity shall document initial probable cause of impact events..." including an option for "cause not determined".
Santee Cooper	No	Does the initial probable cause have to be reported within the timing associated in Attachment 1? Entities may not have enough information that soon to report the initial probable cause. This should be done with events analysis.
SERC OC Standards Review Group	No	We think “impact event” needs to be defined in the NERC Glossary to provide the clarity the industry needs to build auditably compliant procedures.
Tenaska	No	The probable cause of a reportable event is already required to be submitted on the OE-417 form. This Requirement is redundant.
TransAlta Corporation	No	Clarity required Does an entity have to report on the cause of every “applicable” impact event they witness even though the event did not originate at their plant, system or region and did not adversely affect them? Essentially this would require every entity that witnessed an “applicable” event to report on its cause. In most cases they will not know the cause if they did not create the event. Measure M3 should reference Attachment 1 to indicate the Time to Submit Report’.
We Energies	No	A DP may not have Facilities (a BES element). See NERC Glossary definition of Facility.

Organization	Yes or No	Question 5 Comment
Bonneville Power Administration	Yes	Known causes are difficult under 1 hour reporting requirements. (Unusual events are even harder to narrow down in 24 hours and may take weeks.)
Consolidated Edison Co. of NY, Inc.	Yes	We agree, however, the term “impact event” must be part of the NERC glossary.
Georgia System Operations Corporation	Yes	It directly supports the purpose of the standard.
Great River Energy	Yes	While we agree that it makes sense to report on the cause of an event, we disagree with the need for an Operating Plan as identified in R2
MRO's NERC Standards Review Subcommittee	Yes	The NSRS thanks the SDT for stating “initial probable cause” as this is in direct correlation to the Purpose which states “known causes”.
Puget Sound Energy	Yes	However, this requirement doesn't address the timing required for this analysis. This may be intentional and appreciated because at times the analysis can take months when the events are complex in nature.
US Bureau of Reclamation	Yes	This is provided that the report submitted in Attachment A does not include the probable cause. It is highly unlikely that a probable cause may be determined within the reporting timelines.
Arizona Public Service Company	Yes	
ATCO Electric Ltd.	Yes	

Organization	Yes or No	Question 5 Comment
City of Austin dba Austin Energy	Yes	
Duke Energy	Yes	
Dynegy Inc.	Yes	
Idaho Power Company	Yes	
Luminant Energy	Yes	
NERC Staff	Yes	
Pacific Gas and Electric Company	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	
Pepco Holdings, Inc - Affiliates	Yes	
PNM Resources	Yes	
Southern Company - Transmission	Yes	

Organization	Yes or No	Question 5 Comment
United Illuminating	Yes	
WECC	Yes	

6. Do you agree with the requirement R4 and measure M4? Please explain in the comment box below.

Summary Consideration: Note R4 has been moved to R3 due to rearranging of requirements. The DSR SDT did a full review based on comments that were received. R3 now is stream lined to read:

R3. Each Responsible Entity shall conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 at least annually, with no more than 15 months between such tests. The testing of the procedure (as stated in R1) is the main component of this requirement. Several commenters provided input that too much "how" was previously within R3 and the DSR DST should only provide the "what". The DSR SDT did not provide any prescriptive guidance on how to accomplish the required verification within the rewrite. Testing of the entity's Operating Process (R1) could be by an actual exercise of the process (testing as stated in FERC Order 693 section 471), a formal review process or real time implementation of the process. The DSR SDT reviewed Order 693 and section 465 directs that processes "verify that they achieve the desired result". This is the basis of R3, above.

Organization	Yes or No	Question 6 Comment
Ameren	No	Establishing a program with trigger actions expected to require reporting several times a year, combined with adequate initial, and on-going, training should preclude the need for mandatory drills as an added compliance burden.
ATC	No	We do not believe that a drill that exercises a written reporting obligation will add additional reliability to the BES.
BGE	No	M4. BGE recommends not including examples of evidence in a measure but include it in a Guideline. Including in a measure will be translated as a requirement by an auditor.Rationale for R4: If multiple

Organization	Yes or No	Question 6 Comment
		exercises are performed are all of them subject to the sub-R2 requirements and to audit/audit findings?
Bonneville Power Administration	No	There was no drill required for CIP-001 (a drill was in CIP-008, but the purpose did not list combining CIP-008). A drill is not needed for reporting Electrical Grid events, designate it as excluded in the intent of the requirement.
CenterPoint Energy	No	CenterPoint Energy does not agree with R4 and M4. See comments to Q4 above. In addition to the process vs. results based issue stated above, CenterPoint Energy believes conducting a drill to verify recognition, analysis, and reporting procedures is a waste of valuable resources and time.
City of Garland	No	Existing CIP 001 and EOP 004 are reporting standards - neither currently requires annual drills or exercises. Combining these two (2) should not entail expanding the requirements to include drills or exercises. There are existing drills / exercises that must be performed annually for compliance with CIP 008 & CIP 009 which require the same basic identifying, assessing, developing lessons learned, responding, and reporting skill sets. Requiring additional drills or exercises for this new combined standard will provide additional "business overhead" that results in basically nothing that is not obtained by the CIP 008 / 009 drills as far as securing or making the BES reliable. It does, however, result in additional audit risk at audit time.
Constellation Power Generation and Constellation Commodities Group	No	It is not clear how this requirement to conduct drills and exercises relates to the concepts spelled out by the SDT:oA single form to report disturbances and impact events that threaten the reliability of the bulk electric systemoOther opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirementsoClear criteria for reportingoConsistent reporting timelines oClarity around of who will receive the information and how it will be usedR4 does not address any of the above items and should therefore be removed from this standard.

Organization	Yes or No	Question 6 Comment
Consumers Energy	No	NERC should either standardize on a 12 month year or an annual year for reviews.
Dynegy Inc.	No	What is the basis for the drill being annual. This is to stringent. I suggest it be every 3 years.
Electric Market Policy	No	The need for a periodic drill has not been established and appears to be overly restrictive given the intent of the standard is reporting of impact events. Suggest this requirement be eliminated.
ERCOT ISO	No	ERCOT ISO believes that a drill or exercise of its Operating Plan is unnecessary. The intent of the drill can be addressed within the training requirements under R5.
Exelon	No	If drills remain as a component of the standard, an effort to consolidate updating an entities plan with a requirement to drill the plan should be made. . Each entity/utility should be able to dictate/determine if they need a drill for a particular event. Is this document implying a drill for every type of event?
FirstEnergy	No	FE suggests that this requirement be deleted. FE does not see a reliability need for conducting a drill on reporting. This is overly burdensome and should not be included within this reliability standard. Training on the plan and periodic reminder of reporting obligations should suffice.
Great River Energy	No	We disagree with the need to conduct a drill for reporting
Green Country Energy	No	Another training requirement with what benefit? We must train on all of our NERC requirements now anyway to insure compliance and that's not a requirement, thats implied and I think thats enough.
Indeck Energy Services	No	In M4, it is suggested that data from a real event would be evidence. R4 should be satisfied if the Operating

Organization	Yes or No	Question 6 Comment
		Plan is used for a real event within 15 months of the last drill or event.
Independent Electricity System Operator	No	Along the line of our comments on R2 for an operating plan (whose need we do not agree with), a drill, exercise, or Real-time implementation of the Operating Plan for reporting is also not necessary.
IRC Standards Review Committee	No	Similar to our comments on R2 for an Operating Plan, a drill, exercise, or Real-time implementation of its Operating Plan for reporting is unnecessary. Such things are really training practices. There are already existing standards requirements regarding training. There is no imminent threat to reliability that requires these events to be reported in a short time frame as may be required for real-time operating notifications.
ISO New England Inc.	No	The need for a periodic drill has not been established, and appears to be overly restrictive given the intent of the standard is the reporting of impact events. Suggest this requirement be eliminated. Similar to our comments on R2 for an Operating Plan, a drill, exercise, or Real-time implementation of its Operating Plan for reporting is unnecessary. Such things are training practices. There are already existing standards requirements regarding training. There is no imminent threat to reliability that requires these events to be reported in as short a time frame as may be required for real-time operating conditions notifications.
Kansas City Power & Light	No	We believe R4 and M4 are clearly unnecessary. Thoughtful preparation of an Operating Plan per R2 that specifically addresses personnel responsibilities and appropriate evidence gathering combined with the training requirement in R5 is sufficient.
Luminant Energy	No	We support the requirements outlined in R2 which create significant obligations to maintain and update the required Operating Plan. However, we believe annual drilling for a reporting process seems unnecessary, particularly given the response horizon of 24 hours for the majority of impact events. If drilling is required, the

Organization	Yes or No	Question 6 Comment
		standard should allow actual events to fulfill a drilling requirement as stated in the Rationale for R4 and within the text of M4.
Manitoba Hydro	No	Drills and exercise for implementation of the Operating Plan are important and critical, but as in question 5, or Requirement R3, careful and detailed creation of the Operating Plan are crucial to facilitate proper training, drills and exercises.So "NO" is entered simply because a large time line would be needed to properly and efficiently implement R4 and R3.
MidAmerican Energy	No	
Midwest ISO Standards Collaborators	No	We disagree with the need to conduct a drill for reporting.
North Carolina Electric Coops	No	Requiring a drill for "reporting" is unnecessary and burdensome. Reporting is covered in processes and procedures and during the normal training cycle. We recommend the elimination of this requirement.
Northeast Power Coordinating Council	No	The need for a periodic drill has not been established, and appears to be overly restrictive given the intent of the standard is the reporting of impact events. Suggest this requirement be eliminated. Similar to our comments on R2 for an Operating Plan, a drill, exercise, or Real-time implementation of its Operating Plan for reporting is unnecessary. Such things are training practices. There are already existing standards requirements regarding training. There is no imminent threat to reliability that requires these events to be reported in as short a time frame as may be required for real-time operating conditions notifications.
Pacific Gas and Electric	No	PG&E believes the addition of a drill constitutes additional training and should be added to R5. PG&E is

Organization	Yes or No	Question 6 Comment
Company		concerned as to who the target audience for this annual training would affect.
Pacific Northwest Small Public Power Utility Comment Group	No	See #15
PNM Resources	No	PNM feels the addition of a drill or exercise constitutes additional training and believes R4 should be added to R5. The WECC OTS also is interested as to what level does the annual training target, for instance, the field personnel. Will they have to complete the exercise/drill?
RRI Energy, Inc.	No	Every employee in a Registered Entity might potentially have exposure to an impact event, and therefore result in a list of thousands of employees subject to the EOP-004-2 Operating Plan. Does this mean, for example, an applicable Functional Entity with 3,000 employees, each capable of potentially observing an impact event, must include them in the drill, exercise, or Real-Time implementation? Such an expectation would require a hypothetical email notice to be sent to 3,000 employees, advising them "This is a test - You observe a suspicious vehicle driving around the fence of your power plant. Perform the next action you should take." The result in this hypothetical might be 3,000 phone calls and emails to the responsible employee in the applicable Functional Entity, each needing to be documented and retained for the audit period.As stated above in question 5, auditors need guidance as much as Registered Entities. Otherwise, it is observed that they will seek the most stringent approach they observe from the best of the best practices over the first year of implementation and apply that expectation as the base-case, under which all other approaches will be deemed violations.
Santee Cooper	No	There is no need to drill for administrative reporting! This requirement should be deleted.

Organization	Yes or No	Question 6 Comment
SERC OC Standards Review Group	No	We think this requirement is unclear - we think it requires a drill for “reporting”, which seems absurd! We recommend the elimination of this requirement.
Tenaska	No	This Requirement is too specific and places additional burdens on Registered Entities.
US Bureau of Reclamation	No	There is no rationale offered on why 15 months was selected. Without a defined basis the time period is arbitrary. It would be appropriate to let the Entity determine and document the time interval. That would allow the time frame to be sensitive to the complexity of the Operating Plan. Some entities aregeographically dispersed and a single Operating Plan may be difficult to test atone time or within 15 months.The allowance for real time events or actual use is a good move and maymake it easier to define a suitable time frame by the Entity.
WECC	No	The addition of a drill or exercise constitutes additional training and believes R4 should be added to R5. Clarification is needed as to what level does the annual training target, for instance, the field personnel. Will they have to complete the exercise/drill?
American Electric Power (AEP)	Yes	
Arizona Public Service Company	Yes	AZPS agrees with R4, however, the use of the term "Operating Plan" is confusing and leads one to believe an Operating Drill is necessary for a "reporting plan drill." A more accurate term to use would be "Event Reporting Plan."
Georgia System Operations Corporation	Yes	We agree with R4 with "... at least annually, with no more than 15 months ..." replaced with "... at least once per calendar year, with no more than 15 months ..." as in R5.

Organization	Yes or No	Question 6 Comment
MRO's NERC Standards Review Subcommittee	Yes	The NSRS agrees that to enhance reliability and situational awareness of the BES, the Operating Plan be exercised once per calendar year.
United Illuminating	Yes	Suggest R4 be improved to state that a Registered Entity is only required to conduct a drill or execute real-time implementation of the Operating Pan for one impact event listed in the attachment. In other words the Registered Entity is not required to drill on reporting each type of impact event on an annual basis.
ATCO Electric Ltd.	Yes	
City of Austin dba Austin Energy	Yes	
Consolidated Edison Co. of NY, Inc.	Yes	
Duke Energy	Yes	
Idaho Power Company	Yes	
NERC Staff	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	
Pepco Holdings, Inc - Affiliates	Yes	

Organization	Yes or No	Question 6 Comment
PPL Electric Utilities	Yes	
PPL Supply	Yes	
Puget Sound Energy	Yes	
Southern Company - Transmission	Yes	
TransAlta Corporation	Yes	
We Energies	Yes	

7. Do you agree with the requirement R5 and measure M5? Please explain in the comment box below.

Summary Consideration: Most stakeholders who responded to this question indicated disagreement with the originally proposed Requirement R5 and Measure M5. (Note R5 has been moved to R4 in the revised standard.) The DSR SDT did a full review based on comments that were received. The major issues that were provided by commenters was R5.3 and R5.4 and their contents. Upon detailed review the DSR SDT agrees with the majority of comments received with R5.3 and R5.4 and have removed them completely from the Standard. Training is still the main theme of this requirement as it pertains to the personnel in the procedure (R1). R4 now is stream lined to read:

> R4. Each Responsible Entity shall review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan at least annually with no more than 15 calendar months between review sessions

Organization	Yes or No	Question 7 Comment
Green Country Energy		Same as my comment for question 6
Arizona Public Service Company	No	AZPS believes the required training is too restrictive for minor changes/edits to the Event Reporting Plan.
ATC	No	ATC believes it is an inherent obligation of all Functional Entities to train their appropriate staff to meet all applicable NERC Standards. Including a training requirement in some, but not all, Standards implies that the other Standards do not necessitate training. Although this is an important Standard and one that should be included in a Functional Entities' training program, ATC does not believe that this Standard is more important than the other NERC Standards and, therefore, requires a separate training provision
ATCO Electric Ltd.	No	R5.3 requires an entity to conduct training within 30 days of a revision to the Operating Plan. For an entity

Organization	Yes or No	Question 7 Comment
		that covers a wide area, 30 days may not be sufficient to reach all employees.
BGE	No	Suggested revision to clarify R5:Each Applicable Entity shall provide training to all internal personnel identified in its Operating Plan on the Operating Plan annually. Training is only on Reporting, pursuant to R2, not on the Operating Plan?BGE does not believe the SDT needs to identify sub bullets on this requirement. R5.1 is not logical --- what does it mean?
CenterPoint Energy	No	CenterPoint Energy believes that R5 and M5 are not necessary and should be deleted. CenterPoint Energy supports an entity training its staff in any reporting responsibilities; however, such training should be the responsibility of each entity and such requirements do not belong in a NERC standard. In addition, CenterPoint Energy believes any necessary training requirements are covered in the PER Standards and therefore the addition of this requirement adds redundancy to the Standards.If a majority of the industry supports such a requirement, CenterPoint Energy cannot support R5 and M5 as written as we do not agree with the requirement to develop and maintain an Operating Plan (see comments to Q4 above). CenterPoint Energy offers the following alternate language: “Each Applicable Entity shall provide training concerning reporting requirements contained in this Standard to internal personnel involved in the recognition or analysis of events listed in Attachment 1.
City of Garland	No	This expands beyond the original CIP 001 and EOP 004 - neither explicitly requires training - combining does not mean expanding. In reality, what practical skill are you going to train on? People who perform the analysis on an event are going to have job specific training external to this standard and those same folks will maintain their skill set external to this standard. If it is going to be a results based criteria standard, then let the entities be responsible. Training on methods to fill out and file paper work does not make the BES more reliable. The vast majority of other standards do not have a training requirement section and yet, entities manage to be

Organization	Yes or No	Question 7 Comment
		compliant with those standards. Compared to all the other reliability standards and their requirements, are penalties for training on filling out paper work really making the BES more secure and reliable?
Consolidated Edison Co. of NY, Inc.	No	Requirement 5 - Training should be targeted only at those responsible for implementing the Operating Plan (OP), not all those mentioned in the OP.R5 - After the words “internal personnel” add the words “responsible for implementing.” The delete the words “identified in” and “for reporting pursuant to Requirement R2.”5.4 - Following the words “For internal personnel” add the words “responsible for implementing the Operation Plan.” Between the words “revised responsibilities” add the word “implementation.”M5 - After the words “between the people” add the words “responsible for implementing the Operating Plan”
Constellation Power Generation and Constellation Commodities Group	No	Constellation Power Generation questions how R5 relates to the SDT’s “summary of concepts”:oA single form to report disturbances and impact events that threaten the reliability of the bulk electric systemoOther opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirementsoClear criteria for reportingoConsistent reporting timelines oClarity around of who will receive the information and how it will be usedHowever, Constellation Power Generation believes that security awareness is an important aspect of personnel security and proposes an annual training similar to what was in the previous standards. Constellation Power Generation therefore recommends two requirement changes that would achieve security awareness without the burdensome administrative aspects. First, as stated earlier, a sub requirement in R2 should be added which reads as follows: R2.5 Method(s) for making operation personnel aware of changes to the Operating Plan.Second, this training requirement should be rewritten as follows: Each Applicable Entity shall provide training to all operation personnel at least annually.
Consumers Energy	No	Again, either 12 month year or annual year, NERC needs to standardize on one or the other. Training should apply only to those that must take action relevant the reliability of the BES. A plan would likely include

Organization	Yes or No	Question 7 Comment
		notification of senior officers, however they don't need to be included in drills and training if they have no active role.
Duke Energy	No	Strike the word "all" in the requirement. All personnel don't need to be trained - for example, the plan may contain references to some personnel as potential sources of the information that will then be reported. Also, Section 5.3 only allows 30 days for training, which may be impossible with rotating shift personnel and training schedules. 60 days is more appropriate.
Dynegy Inc.	No	The annual training seems excessive especially if their have been no changes. You have included one exception for contact information revisions; however, it should be expanded to include exceptions for minor/non-substantial changes. Also, make training requirements (after initial training)be required for substantive changes only.
E.ON Climate & Renewables	No	Redundant with R4.
Electric Market Policy	No	The need for a periodic training has not been established and appears to be overly restrictive given the intent of the standard is reporting of impact events. Suggest this requirement be eliminated.
Exelon	No	Exelon doesn't feel that the 30 day requirement is achievable and recommends an annual review. Training for all participants in a plan should not be required. Many organizations have dozens if not hundreds of procedures that a particular individual must use in the performance of various tasks and roles. Checking a box which states someone read a procedure does not add any value, it is an administrative burden with no contribution to reliability. It is Exelon's opinion that training requirements should be covered in the PER standards and that the audience to be trained should be identified. R5.4 requires internal personnel that

Organization	Yes or No	Question 7 Comment
		have responsibilities related to the Operating Plan cannot assume the responsibilities unless they have completed training. This requirement places an unnecessary burden on the registered entities to track and maintain a data base of all personnel trained and should not be a requirement for job function. A current procedure and/or operating plan that addresses each threshold for reporting should provide adequate assurance that the notifications will be made per an individual's core job responsibilities.
FirstEnergy	No	Requirement R5 and Part 5.1 - The wording in Part 5.1 is too prescriptive and shouldnot require training on the specific actions of personnel. Also, R5 should not require training for personnel that may only receive the report and are not required to do anything. Therefore we suggest rewording R5 and 5.1 as follows:"R5. Each Applicable Entity identified in Attachment 1 shall have a Reporting Plan(s) for identifying, assessing and reporting impact events listed in Attachment 1 that includes the following components:5.1 The training includes the personnel required to respond under the Reporting Plan."Part 5.3 - We suggest removing subpart 5.3. This requirement is overly burdensome and not necessary. We believe that the requirements for annual review and update of the plan as well as training sufficiently cover reviews of changes to the plan. Part 5.4 - The last phrase "training shall be conducted prior to assuming the responsibilities in the plan" should account for emergency situations when the entity does not have time to train the replacement before they are to assume a responsibility.
Great River Energy	No	We believe that this task should be incorporated into the Job Task Analysis for the System Operators and that this requirement should be deleted as being redundant.
Idaho Power Company	No	The 30 day Requirement is limited with real time operations. Most entities with real time operations utilize a 5 or 6 week rotating schedule to comply with PER-002. the NERC Continuing Education Program allows up to 60 days to comply, this allows the operating shifts to accomadate training within the operating schedule. The

Organization	Yes or No	Question 7 Comment
		requirement 5.3 should allow 60 days to complete the training.
Indeck Energy Services	No	It is wholly unreasonable to re-train everyone for each change to the Operating Plan. Suggestion: Clarify that upon changes to the Operating Plan, the Registered Entity may either require full training, or instead distribute a summary of the change to affected personnel only.
Independent Electricity System Operator	No	Along the line of our comments on R2 for an Operating Plan (whose need we do not agree with), any training on developing and providing the report is unnecessary. What matters is that the report is provided to the needed organizations or entities on time and in the required format according to established procedure. How this is accomplished goes outside of the purpose of reliability standard requirements.
IRC Standards Review Committee	No	We do not agree with the need for R5. We do not see the need for a standard requirement that stipulates training the personnel on reporting events. What matters is that the reports are provided to the needed organizations or entities on time and in the required format according to established procedure. Stipulating a training requirement to achieve this reporting is micro-managing and overly prescriptive.
ISO New England Inc.	No	The need for a periodic drill has not been established, and appears to be overly restrictive given that the intent of the standard is reporting of impact events. Suggest this requirement be eliminated. There are training standards in place that cover these requirements. We agree the relevant personnel should be “aware” of the reporting requirements. But there is not a need to have a training program with specific time frames for reporting impact events. Awareness of these reporting requirements can be achieved through whatever means are available for entities to employ to train on any of the NERC standards, and need not be dictated by requirements.

Organization	Yes or No	Question 7 Comment
Kansas City Power & Light	No	We agree with the need for the Operating plan and the provision of formal training to impacted personnel. We believe that the personnel references are too open-ended to be productive and measurable. This leaves all applicable entities open to subjectivity in assessment and may produce a large administrative burden to demonstrate compliance with no associated benefit to improved reliability.
Luminant Energy	No	Operating Plan revisions communicated through procedure updates and employee acknowledgements of the same are sufficient when coupled with a procedural training program that occurs according to a programmed schedule.
Manitoba Hydro	No	The comments in Question 6 and 7 encompass the training aspect of this requirement.
MidAmerican Energy	No	: R5.2. The NSRS agrees that to enhance reliability and situational awareness of the BES, the Operating Plan be trained once per calendar year.R5.3 As detailed in R2, the Operating Plan shall contain provisions for “identifying, assessing, and reporting impact events”. Where, R2.7 states to update the OperatingWe disagree with the need to provide formal training. We could agree with the need to communicate to System Operators and other pertinent personnel the criteria for reporting so that they know when system events need to be reported.
Midwest ISO Standards Collaborators	No	We disagree with the need to provide formal training. We could agree with the need to communicate to System Operators and other pertinent personnel the criteria for reporting so that they know when system events need to be reported.
MRO's NERC Standards Review Subcommittee	No	R5.2. The NSRS agrees that to enhance reliability and situational awareness of the BES, the Operating Plan be trained once per calendar year.R5.3 As detailed in R2, the Operating Plan shall contain provisions for

Organization	Yes or No	Question 7 Comment
		"identifying, assessing, and reporting impact events". Where, R2.7 states to update the Operating Plan when there is a component change. The NSRS believes the components of this Operating Plan are 1) indentifying impact events, 2) assessing impact events, and 3) reporting impact events. These components relate to training when the Operating Plan is revised per, R5.3, only. As written, every memo, simulations, blog, etc that contain the words "lessons learned" would be required to be in your Operating Plan and trained on every time one was issued or heard about internally or externally. Recommend that the Operating Plan be revised and training occurs when a change occurs to the entity's Operating Plan, consisting of 1) indentifying impact events, 2) assessing impact events, and 3) reporting impact events, only.
North Carolina Electric Coops	No	Requiring training to report of after-the-fact events does not improve the reliability of the BES. We recommend the elimination of this requirement.
Northeast Power Coordinating Council	No	The need for a periodic drill has not been established, and appears to be overly restrictive given that the intent of the standard is reporting of impact events. Suggest this requirement be eliminated. There are training standards in place that cover these requirements. The relevant personnel should be "aware" of the reporting requirements. But there is not a need to have a training program with specific time frames for reporting impact events. Awareness of these reporting requirements can be achieved through whatever means are available for entities to employ to train on any of the NERC standards, and need not be dictated by requirements.
Pacific Gas and Electric Company	No	PG&E believes 30 days is too restrictive due to real-time operations schedule requirements. The schedule is six weeks and individuals may be on either long change or vacation and therefore unable to complete the training within 30 days of the identification of the need. Suggest extending to 60 days to meet the training criteria which follows the NERC Continuing Education revised submittal date for the Individual Learning

Organization	Yes or No	Question 7 Comment
		Activities (ILA).
Pacific Northwest Small Public Power Utility Comment Group	No	See #15
PacifiCorp	No	Training required within 30 days of a revision to the Operating Plan is not feasible with 5 or 6 week shift rotations. A sixty day requirement would be more realistic.
Pepco Holdings, Inc - Affiliates	No	30 days may be too short a time for large entities with multiple subsidiaries to do the necessary notice and coordination. PHI suggests 90 days.
PNM Resources	No	PNM believes 30 days is too restrictive due to real-time operations schedule requirements. Most work schedules are either five or six weeks and individuals may be on either long change or vacation and therefore unable to complete the training within 30 days of the identification of the need. Based on the NERC Continuing Education revised submittal date for the Individual Learning Activities (ILA), PNM would recommend 60 days.Creating an Impact Event Report is duplicative and redundant and the WECC OTS feels this is not necessary.
PPL Electric Utilities	No	We agree with the need for training on one's process. However, we suggest changes to R5.3. Consider expanding the exception criteria to exempt non-substantive changes such as errata changes, minor editorial changes, contact information changes, etc. We also suggest saying '...,training shall be conducted, or notification of changes made, within 30 days of the procedure revisions.'
PPL Supply	No	We generally agree with R5 but recommend two changes to 5.3. Consider expanding the exception criteria to exempt non-substantive changes such as errata changes, minor editorial changes, contact information

Organization	Yes or No	Question 7 Comment
		changes, etc. Also, consider changing "training shall be conducted" to "training or communication/notification of changes shall be conducted."
Puget Sound Energy	No	The fact that proposed requirement R2 will require frequent updates to the operating plan means that the training required under this plan will occur quite frequently as well, leading to operator confusion. Even the comment allowing a review and “sign-off” will not completely mitigate this result.
RRI Energy, Inc.	No	1. This Requirement is structured to result in the same heavy-handed, zero-tolerance approach that has made CIP-004 one of the top three violated Reliability Standards. The failure in CIP-004 is that, for example, a seven-year background check or annual training program that is tardy by one day results in a violation. There is no margin of error, proviso, or cure scenario. Likewise, the proposed R5 in EOP-004-2 makes it a violation if someone takes their newly established training on the day after the end of 15 months. Systems configurations are often based on quarterly monitoring for individuals needing to take training. In addition, when dealing with potentially thousands of employees, it is inevitable that any one of hundreds of reasons might result in an employee not being included in the tracking system, and rolling past the 15th month. RECOMMENDATION: To avoid further burden to Regional Entity audit and enforcement personnel as has been the case in CIP-004, develop a cure process that allows the Registered Entity to correct the training or background check tardiness with prompt correction, fill out a notification report to submit to NERC, and proceed with protecting the reliable operation of the BES, rather than tying up Registered Entity and Regional Entity staffs with data requests, enforcement paperwork and administrative actions.2. The proposed R5.3 requires the entire applicable staff to redo the entire training within 30 days of a change to the Operating Plan. These Operating Plans will not be short documents, and formal training will not involve a 5 minute soundbite. However, for such a significant procedure as the Operating Plan, frequent changes and revisions are going to

Organization	Yes or No	Question 7 Comment
		be very common, especially given the likelihood of frequent clarifications, Compliance Action Notices ("CANs"), and lessons learned issued by NERC and Regional Entities over this very detailed set of new obligations. It is not unreasonable to expect a Registered Entity to make three or more revisions to their Operating Plan in a year, which would require training for thousands of employees three times a year, for what might amount to a single sentence revision. Furthermore, the obligation to retrain on the entire training program is not limited in this requirement to only those individuals impacted by the revision. Where a change or revision only impacts 3 possible employees, this standard would require a company with 1,500 employees subject to the Operating Plan to retake the entire training. RECOMMENDATION: Clarify that upon changes to the Operating Plan, the Registered Entity may either require full training, or instead distribute a summary of the change(s) via email to affected personnel only.
Santee Cooper	No	The concept of requiring training on reporting of after-the-fact events does not support or enhance bulk electric system reliability. We recommend the elimination of this requirement.
SERC OC Standards Review Group	No	While we support training on an annual basis for the operating plan, the concept of requiring training on reporting of after-the-fact events does not support or enhance bulk electric system reliability. We recommend the elimination of this requirement.
Southern Company - Transmission	No	We suggest that the time frame be changed to 60 or 90 days in 5.3. 5.4 needs to have a time frame associated with it; we suggest that it be 60 or 90 days.
Tenaska	No	This Requirement is too specific and places additional burdens on Registered Entities.
TransAlta Corporation	No	Measure M5 states applicable entities shall provide training material presented... This measure is unclear as

Organization	Yes or No	Question 7 Comment
		to whether the meaning is for internal personnel or to be provided to external entities upon request? Please clarify.
US Bureau of Reclamation	No	The measure is vague and redundant. The Entity is required to provide information to be used to "verify content". The information may be used to demonstrate compliance but who will verify the content is adequate and on what basis. Secondly, the measure requires training information be provided twice, once to demonstrate who participated and then to show who was trained. This is all unnecessary and could be remedied by simply stating that "evidence shall demonstrate that all individuals listed in the plan have received training on their role in the plan"
We Energies	No	Please clarify who is to be trained. As written, R5 requires any internal personnel identified in the plan, including CEO, Vice Presidents, etc., to be trained.
WECC	No	Thirty days is too restrictive due to real-time operations schedule requirements. Most work schedules are either five or six weeks and individuals may be on either long change or vacation and therefore unable to complete the training within 30 days of the identification of the need. Based on the NERC Continuing Education revised submittal date for the Individual Learning Activities (ILA), the requirement should be changed to require training to be conducted within 60 days.
Bonneville Power Administration	Yes	There was no training required for CIP-001 or in CIP-008. (The proposed EOP-008 purpose did not list incorporating CIP-008). Training was not really needed for reporting Electrical Grid events.
ERCOT ISO	Yes	ERCOT ISO believes the content of training can include an exercise or drill.

Organization	Yes or No	Question 7 Comment
United Illuminating	Yes	R5.3 coupled with the rationale provided is a sensible approach. It is important that the rational is not forgotten.
Ameren	Yes	
American Electric Power (AEP)	Yes	
City of Austin dba Austin Energy	Yes	
Georgia System Operations Corporation	Yes	
NERC Staff	Yes	
PacifiCorp	Yes	

8. Do you agree with the requirement R6 and measure M6? Please explain in the comment box below.

Summary Consideration: There was no consensus amongst stakeholders who responded to this question regarding agreement with the originally proposed Requirement R6 and Measure M6. (Note R6 been moved to R5 in the revised standard.) The DSR SDT did a full review based on comments that were received. Many comments indicated concerns with the reporting timelines within Attachment 1. (The DSR SDT has addressed those comments in response to Question 10).

Several commenters wanted the ability to report impact events to their responsible parties via the DOE Form OE-417. Following discussions with the DOE and NERC, the DSR SDT has added the ability to use of the DOE Form OE-417 when the same or similar items are required to be reported to NERC and the DOE. This will reduce the need to file multiple forms when like items must be reported to the DOE and NERC for the same impact event. The underlying fact is that impact events are to be reported within prescribed guidelines, thus providing industry awareness and starting of any analysis process. R5 now is stream lined to read:

> R5. Each Responsible Entity shall report Impact Events in accordance with the Impact Event Operating Plan pursuant to Requirement R1 and Attachment 1 using the form in Attachment 2 or the DOE OE-417 reporting form.

Organization	Yes or No	Question 8 Comment
American Electric Power (AEP)	No	It is not clear how this is different from R3 since it relies on the same timetable in Attachment 1.
CenterPoint Energy	No	CenterPoint Energy does not agree with R6 and M6 as written as we do not agree with the requirement to develop and maintain an Operating Plan (see comments to Q4 above) In addition CenterPoint Energy does not agree with the timelines required in Attachment 1 (see comments on Q10). CenterPoint Energy offers the following alternate language: “Each Applicable Entity shall report events outlined in Attachment 1 to applicable entities including but not limited to; NERC, and appropriate law enforcement agencies."

Organization	Yes or No	Question 8 Comment
City of Garland	No	1. The reporting requirements should not be expanded beyond CIP 001 and EOP 004-1. The goal for combining the two should be to make the process more efficient - not add on extra requirements for procedures on how to report, drills on reporting, training on reporting, etc. 2. The timelines requiring 1 hour reporting to the ERO are not needed and provide little realtime benefit to the BES. Real time or near real time reporting for "people on the ground" such as the RC, BA, TOP, FBI, Local Law Enforcement, DOE, etc. is necessary. They are in a position to take action in response to an event. On page 5, it states "The proposed standard deals exclusively with after-the-fact reporting. 1 Hour reporting requirements to the ERO in addition to existing reporting are not reasonable "after-the-fact" reporting requirements in the midst of an emergency. Also, there is not a 24X7 ERO center to report events to - why build and staff one when they already exists at the RC, BA, TOP, DOE, FBI, Local Law Enforcement, etc. - An ERO 24X7 center would be extra overhead that would provide no additional benefit in the first hour or hours of an emergency.
Consolidated Edison Co. of NY, Inc.	No	R2 requires applicable entities to have an Operating Plan which are company specific procedures and process required to be compliant with EOP-004. Therefore, R6 should be deleted since it is redundant with R2.
Electric Market Policy	No	Entities are already required by other agencies (e.g., DOE, NRC) to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
ERCOT ISO	No	ISO recommends the following changes to the language of the requirement.R6. Each Applicable Entity shall report impact events in accordance with Attachment 1.
Exelon	No	The time durations in the attachment are too short, it would be impossible to collect all the data necessary to report out on an impact event in the defined time to report.The SDT should evaluate each event for the most

Organization	Yes or No	Question 8 Comment
		appropriate entity responsible to ensure there is minimal confusion on who has the responsibility and eliminate duplication of reporting when feasible.
FirstEnergy	No	M6 - NERC's system should be capable of making this evidence available for the entities and provide a "return-receipt" of the reports that we send them. Also, M6 should be revised to state "Applicable Entities" as opposed to "Registered Entities".
Great River Energy	No	We believe the reporting time lines are too aggressive for some events. Reporting events within an hour is not reasonable as an entity may still be dealing the event. This will particularly difficult when support personnel are not present such as during nights, holidays and weekends.
Indeck Energy Services	No	---This is the first mention of the time lines in Attachment 1. If they are part of the standard, then they should be incorporated to the Operating Plan in R2 and then need not be mentioned again, only compliance with the plan. ---In M6, the last part, "evidence to support the type of impact event experienced; the date and time of the impact event ; as well as evidence of report submittal that includes date and time" is redundant. All of that should be in the report to NERC. If not, then it's not important to keep.
Independent Electricity System Operator	No	We agree with having a requirement to report impact events in accordance with the timelines outlined in Attachment 1, but not with the requirements indicated in R2.
IRC Standards Review Committee	No	There is not a need for an Operating Plan as proposed. This is not truly an Operating Plan. There are already other standards which create the requirements for an Operating Plan. This is an administrative reporting plan and any associated impact upon reliability is far beyond real-time operations.

Organization	Yes or No	Question 8 Comment
ISO New England Inc.	No	Entities are already required by other agencies (e.g., DOE, NRC) to report certain events. We see no need to develop redundant reporting requirements for NERC that cross other federal agency jurisdictions.There is no need for an Operating Plan as proposed. This is not truly an Operating Plan. There are already other standards which create the requirements for an Operating Plan. This is an administrative reporting plan and any associated impact upon reliability is far beyond real-time operations which is implied by the label "Operating Plan."
Kansas City Power & Light	No	We believe R3 and M3 are unnecessary as a stand alone requirement and measure and propose combining these requirements with R6 and M6. Identifying and assessing the initial probable cause of an impact event is the obvious starting point in the reporting process and ultimate completion of the required report. Evidence to support the identification and assessment of the impact event and evidence to support the completion and submittal of the report are really one in the same.
MidAmerican Energy	No	We believe the reporting time lines are too aggressive for some events. Reporting events within an hour is not reasonable as an entity may still be dealing the event. This will particularly difficult when support personnel are not present such as during nights, holidays and weekends.
Midwest ISO Standards Collaborators	No	We believe the reporting time lines are too aggressive for some events. Reporting events within an hour is not reasonable as an entity may still be dealing the event. This will particularly difficult when support personnel are not present such as during nights, holidays and weekends.
North Carolina Electric Coops	No	There is already a DOE requirement to report certain events. NERC should not be developing redundant reporting requirements when this information is already available at the federal level from other agencies.

Organization	Yes or No	Question 8 Comment
Northeast Power Coordinating Council	No	Entities are already required by other agencies (e.g., DOE, NRC) to report certain events. We see no need to develop redundant reporting requirements for NERC that cross other federal agency jurisdictions.There is no need for an Operating Plan as proposed. This is not truly an Operating Plan. There are already other standards which create the requirements for an Operating Plan. This is an administrative reporting plan and any associated impact upon reliability is far beyond real-time operations which is implied by the label “Operating Plan".
Pacific Gas and Electric Company	No	PG&E believes that if the standard is intended to be an after the fact report, we question the one and/or twenty-four hour reporting criteria and then the 30 day criteria?
Pacific Northwest Small Public Power Utility Comment Group	No	See #15
PNM Resources	No	PNM believes there seems to be redundancy in reporting based on the time frames in Attachment 1, i.e. OE-417 and other required reports. If this standard is intended to be an after the fact report, why is there one/twenty-four hour reporting criteria?
PPL Electric Utilities	No	We understand the rationale for this standard and support the project to combine EOP-004 and CIP-001 as well as the reporting requirement in CIP-008. We are concerned that it may be difficult to meet Attachment 1 Part B Potential Reliability Impact submittal times as the time to submit is 1 or 24 hour after occurrence. E.g. Risk to BES equipment, the example given is a major event and easy to conclude. Consider forced intrusion, risk to BES equipment (increased violence in remote area), or cyber intrusion - should Attachment 1 state ‘report within 24 hours after detection’?

Organization	Yes or No	Question 8 Comment
PPL Supply	No	It may be difficult to meet Attachment 1 Part B Potential Reliability Impact submittal times as the time to submit is 1 or 24 hours after occurrence. Consider changing the Time to Submit Report for Forced intrusion, Risk to BES equipment, and Detection of a cyber intrusion to be "report within 24 hours after detection".
RRI Energy, Inc.	No	RECOMMENDATION: Clarify that the reporting of impact events shall be to those entities identified in the Operation Plan section developed specifically in Section 2.6. Reference to Attachment 1 indicates reporting to "external" parties is the intent for R6.
Santee Cooper	No	If the DOE form is going to continue to be required by DOE, then NERC should accept this form. Entities do not have time to fill out duplicate forms within the time limits allowed for an event. This is burdensome on an entity
SERC OC Standards Review Group	No	There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
Southern Company - Transmission	No	The time to submit report column needs to be more flexible with time frames.
Tenaska	No	The reporting timelines are currently listed on the OE-417 form. This Requirement is redundant.
TransAlta Corporation	No	R6 should reference Attachment 2 to make it clear that this report form must be used.M6 seems to be requesting evidence that the Confidential Impact Event Report was submitted. TransAlta suggests the submission of the actual report is evidence the report was submitted.Records of this submission can be provided on request.Web Reports Project 2009-01 has indicated online reporting is the direction they are

Organization	Yes or No	Question 8 Comment
		going.If the impact report becomes an online Web report the entity submitting the report has no way of confirming the report ended up at the Compliance Enforcement Authority office after it is submitted. There needs to be some method that demonstrates the report was submitted and received.
We Energies	No	The proposed definition of “impact event” needs to be clarified.
WECC	No	There seems to be redundancy in reporting based on the time frames in Attachment 1, i.e. OE-417 and other required reports. If this standard is intended to be an after the fact report, why is there one/twenty-four hour reporting criteria?
Arizona Public Service Company	Yes	AZPS believes that Operating Plan should be replaced with "Event Reporting Plan."
ATC	Yes	ATC does agree that applicable entities report on events identified in Attachment 1 (See our comments about Attachment 1), but we do not agree that applicable entities should be required by this standard to have an Operational Plan. Please see our comments to question 4.
BGE	Yes	Comments for clarification:R6. Use of Capital letters in Operating Plan makes it unnecessary to state "created pursuant to Requirement 2
Bonneville Power Administration	Yes	The requirement needs to specify who (ERO) to report to. Attachment 1 doesn’t say to report to the ERO either. Clarify or remove the difference between the report submitted and evidence of the type of impact event required in the measurement.
Georgia System Operations Corporation	Yes	It directly supports the purpose of the standard.

Organization	Yes or No	Question 8 Comment
Green Country Energy	Yes	Now this is an excellent example of all that is needed for this requirement!
Manitoba Hydro	Yes	Attachment 1 details the impact events and the thresholds of which they should be reported.
Puget Sound Energy	Yes	It is assumed that for the purposes of M6, NERC and the regions would already have access to these reports.
Ameren	Yes	
ATCO Electric Ltd.	Yes	
City of Austin dba Austin Energy	Yes	
Constellation Power Generation and Constellation Commodities Group	Yes	
Duke Energy	Yes	
Dynegy Inc.	Yes	
Idaho Power Company	Yes	
Luminant Energy	Yes	
MRO's NERC Standards Review	Yes	

Organization	Yes or No	Question 8 Comment
Subcommittee		
NERC Staff	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	
Pepco Holdings, Inc - Affiliates	Yes	
United Illuminating	Yes	
US Bureau of Reclamation	Yes	

9. Do you agree with the requirements for the ERO (R7-R8) or is this adequately covered in the Rules of Procedure (section 802)? Please explain in the comment box below.

Summary Consideration: There was no consensus amongst the commenters who responded to this question. The DSR SDT did a full review based on comments that were received. The DSR SDT has determined that R7 and R8 are not required to be within a NERC Standard since Section 800 of the Rules of Procedure already assigns this responsibility to NERC. The DSR SDT, the Events Analysis Working Group (EAWG), NERC Staff (to include NERC Senior VP and Chief Reliability Officer) had an open discussion with this item being a major topic. The DSR SDT and EAWG are working in coordination with each other to provide NERC Staff with updated language for future inclusion into the Rules of Procedure. NERC Staff, the EAWG and the DSR SDT all supported this new initiative.

Organization	Yes or No	Question 9 Comment
Ameren	No	NERC's current heavy case load should justify reviewing the impact review table only once every 2 years.
ATC	No	ATC feels the ERO obligations should be covered in the Rules of Procedure.We do not agree with the requirements assigned to the ERO, but believe that they should be incorporated into the ERO's Rules of Procedure
BGE	No	R7. Make Impact Event Table all Capital Letters(it is a title). R8. Is the term "reportable impact events" new or is impact event intended to be capitalized? R8. Does a quarterly report of the year's reportable impact events include 12 months of "reportable impact events"? This is confusing. R8. In the Rationale for R8 Impact Events appears with Capital letters - why now? Shouldn't it appear with all Capital letters throughout the document as it is a defined term? R8. There are no previous requirements to report threats (R8.3) or

Organization	Yes or No	Question 9 Comment
		lessons learned (R8.5) or trends (R8.2) to an ERO. Is this information from reports to the ERO or from ERO research?
CenterPoint Energy	No	CenterPoint Energy does not believe this requirement is necessary; however, if the SDT insists on keeping this requirement then CenterPoint Energy believes it should remain as written. Any change to Attachment 1 should go through the Reliability Standards Development Procedure.
Consolidated Edison Co. of NY, Inc.	No	See response to Question 2Requirement 7Delete the words “and propose revisions to”Following the words (Attachment 1) add a period.Following that period add the words “The ERO shall revise the table”Requirement 8RECOMMEND DELETION OF R8 - CONFIDENTIALITY CONCERNS WILL MAKE ESTABLISHING A PUBLICATION REQUIRMENT EXTREMELY CHALLENGING.
Constellation Power Generation and Constellation Commodities Group	No	The impact event table (Attachment #1), as part of a standard, would have to be FERC approved every time it is edited. That would cause it to go through NERC’s Standard Development Process, and would cause a revision to the standard each time. This will also cause revisions to each and every registered entity’s Operating Plan. Overall, this requirement causes a large administrative burden on all entities, and does not improve reliability. As stated earlier, the “summary of concepts” for this latest revision, as written by the SDT, includes the following items:oA single form to report disturbances and impact events that threaten the reliability of the bulk electric systemoOther opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirementsoClear criteria for reportingoConsistent reporting timelines oClarity around of who will receive the information and how it will be usedRequirement 7 and 8 do not address any of these items. Furthermore, for R8, it is requiring NERC to send out quarterly reports, yet entities are supposed to amend their Operating Plans based on an annual NERC report. This requirement is confusing and is not consistent with earlier requirements. Constellation Power Generation

Organization	Yes or No	Question 9 Comment
		believes that these two requirements should be removed.
Electric Market Policy	No	Having the ERO as an applicable entity is concerning as they are also the compliance enforcement authority.
ERCOT ISO	No	Recommend that the Electric Reliability Organization be removed. The Electric Reliability Organization should not be responsible for reliability functions and therefore should be excluded from reliability standards.
FirstEnergy	No	FE disagrees with the ERO as an applicable entity within a reliability standard. See our responses to Questions 2 and 3 above. We do not believe the desired ERO process is adequately covered in section 802. Section 802 deals with assessments and not event reporting.
Georgia System Operations Corporation	No	It should not be necessary for the ERO to require itself to do these things. NERC's authority should be sufficient to do these things as part of its mission.With quarterly trending and analysis of threats, vulnerabilities, lessons learned, and recommended actions in R8, R7 (an annual review) should not be necessary. The quarterly activity could include proposing revisions to Attachment 1 if warranted.An alternative would be to perform annual trending and analysis of threats, vulnerabilities, lessons learned, recommended actions, and proposed revisions to Attachment 1 if warranted.Also, the Reliability Standards Development Procedure has been replaced with the Standard Processes Manual.
Indeck Energy Services	No	Reviewing Attachment 1 annually is unnecessary. Events don't change much and if they do, a SAR is needed to consider the changes. NERC should not be included in any standard!
Independent Electricity System Operator	No	We agree with the need to update the list as needed, but it does not have to be the ERO who takes on a reliability standard to do so. It can simply be an annual project in the standards development work plan to review Attachment 1 as part of a standard. The industry will then be provided an opportunity to weigh on the

Organization	Yes or No	Question 9 Comment
		changes. Also, we do not see the reliability results or benefits of R8. The ERO can issue the report quarterly but who are audiences? What reliability purpose does it serve if no further actions are pursued upon receiving the report? Can this be done as a standing item for the ERO at, say, the BoT meeting? Or, can this be a part of the quarterly communication from the ERO to the industry? To make this a reliability standard is an over-kill, and does not conform with the results-based standard concept.From our perspective, both R7 and R8 can be removed, and the ERO can be removed from the Applicability Section as well.
IRC Standards Review Committee	No	We do not support an annual time frame to update the events list. The list should be updated as needed through the Reliability Standards Development Process. Any changes to a standard must be made through the standards development process, and may not be done at the direction of the ERO without going through the process.
ISO New England Inc.	No	Having the ERO as an applicable entity raises concern as it is also the compliance enforcement authority. Requirement R7 is unnecessary as there are already requirements in place for three year reviews of all Standards. R8 contains requirements to release information that should be protected, such as identification of trends and threats against the Bulk Electric System. This may trigger more threats because it will be published to unwanted persons in the private sector.We do not support an annual time frame to update the events list. The list should be updated as needed through the Reliability Standards Development Process. Any changes to a standard must be made through the standards development process, and may not be done at the direction of the ERO without going through the process.
Kansas City Power & Light	No	We agree with the rationale for R8 requiring NERC to analyze Impact Events that are reported through R6 and publish a report that includes lessons learned but disagree with R2.9 obligating an entity to update its Operating Plan based on applicable lessons learned from the report. Whether lessons learned are applicable

Organization	Yes or No	Question 9 Comment
		to an entity is subjective. If an update based on lessons learned from an annual NERC report is required, the requirement should clearly state the necessity of the update is determined by the entity and the entity's Reliability Coordinator or NERC can not make that determination then find the entity in violation of the requirement. In addition, if an update based on lessons learned from a NERC report is required, NERC should publish the year-end report (R8) on approximately the same day annually (i.e. January 31) and allow an entity at least 60 days to analyze the report and incorporate any changes it deems necessary in its Operating Plan. Again, the language referencing annual and quarterly in these two requirements in confusing.
Manitoba Hydro	No	Rules of Procedure appear to have a different focus then R7 and R8.Briefing on Rules of Procedure 802Assess, review and report on:1.1 overall electric operation1.2 uncertainties and risks1.3 self assessment of supply and reliability1.4 projects on customer demand1.5 impact of evolving electric market practicesthat could affect the present and future of the BESBriefing on R7 and R8R7 - ERO shall review and propose revisions to Attachment 1R8- ERO shall publish quarterly reports on trends, threats, vulnerabilities, lessons learned and recommended actions.
Midwest ISO Standards Collaborators	No	We do not agree with the requirements and we do not believe it is adequately covered in section 802. First, section 802 deals with assessments not event reporting. Secondly, since attachment 1 is part of a standard, it should not be modified outside of the Reliability Standards Development process.
NERC Staff	No	NERC staff believes that requirements R7 and R8 are not needed because they are intrinsic expectations from its Rules of Procedure. Furthermore, these elements are necessary for analysis in support of the Reliability Metrics efforts NERC is leading under its Reliability Assessment and Performance Analysis

Organization	Yes or No	Question 9 Comment
		program.
North Carolina Electric Coops	No	The ERO cannot be subject to a requirement for which it is the compliance enforcement authority.
Northeast Power Coordinating Council	No	Having the ERO as an applicable entity raises concern as it is also the compliance enforcement authority. Requirement R7 is unnecessary as there are already requirements in place for three year reviews of all Standards. R8 contains requirements to release information that should be protected, such as identification of trends and threats against the Bulk Electric System. This may trigger more threats because it will be published to unwanted persons in the private sector.We do not support an annual time frame to update the events list. The list should be updated as needed through the Reliability Standards Development Process. Any changes to a standard must be made through the standards development process, and may not be done at the direction of the ERO without going through the process.
Puget Sound Energy	No	This is adequately covered by section 802 of the Rules of Procedure. There seems to be some conflict between R2.9 and R8 regarding timeframes and the specific elements required.
Santee Cooper	No	Standards cannot be applicable to an ERO because they are the compliance enforcement authority, and the ERO is not a user, owner, or operator of the BES.
SERC OC Standards Review Group	No	The ERO cannot be subject to a requirement for which it is the compliance enforcement authority. The governance in this situation appears incomplete.
United Illuminating	No	The rules of procedure adequately cover this.
US Bureau of Reclamation	No	Requirements 7 and 8 are covered in the Section 801.801. Objectives of the Reliability Assessment and

Organization	Yes or No	Question 9 Comment
		Performance Analysis Program. The objectives of the NERC reliability assessment and performance analysis program are to: (1) conduct, and report the results of, an independent assessment of the overall reliability and adequacy of the interconnected North American bulk power systems, both as existing and as planned; (2) analyze off-normal events on the bulk power system; (3) identify the root causes of events that may be precursors of potentially more serious events; (4) assess past reliability performance for lessons learned; (5) disseminate findings and lessons learned to the electric industry to improve reliability performance; and (6) develop reliability performance benchmarks. The final reliability assessment reports shall be approved by the board for publication to the electric industry and the general public.
Bonneville Power Administration	Yes	R2.9 language refers to R8 “annual” report; however R8 language is “quarterly” reporting. It appears this standard is going to be in an update status 4 times per year minimum, plus any event modifications plus personnel changes. Overly burdensome.
City of Garland	Yes	R7 - Yes as long as any changes to attachment 1 follow the “Reliability Standards Development Procedure. R8 - Yes as long as R8.6 is strictly “recommended actions.” They should not become “required actions” as this bypasses the standard development process.
Duke Energy	Yes	However, R8 only addresses quarterly reports, and R2 Section 2.9 states that there will be an annual report.
Green Country Energy	Yes	I realize this is another burden for the ERO but the information would be good to know what is going on outside the plant .
Luminant Energy	Yes	Continually refining the Impact Event table to better define which events should be reported would be extremely valuable. Section 802 does not adequately require such refinement, thus R7 and R8 are

Organization	Yes or No	Question 9 Comment
		appropriate inclusions to this standard.
MRO's NERC Standards Review Subcommittee	Yes	Should read “In accordance with Sections 401(2) and 405 of the Rules of Procedures, the ERO can be set as an applicable entity in a requirement or standard”. As stated in the text box.
RRI Energy, Inc.	Yes	We support the concept that Reliability Standard requirements and obligations that are subject to violations and penalties should all be contained in the four-corners of the Reliability Standard. If an obligation exists in the Rules of Procedures that creates a stand-alone responsibility that is subject to violation and penalty, it should be removed from the Rules of Procedure and inserted into the appropriate Reliability Standard.
ATCO Electric Ltd.	Yes	
City of Austin dba Austin Energy	Yes	
Dynegy Inc.	Yes	
Great River Energy	Yes	
Idaho Power Company	Yes	
MidAmerican Energy	Yes	
Pacific Gas and Electric Company	Yes	

Organization	Yes or No	Question 9 Comment
PacifiCorp	Yes	
PacifiCorp	Yes	
Pepco Holdings, Inc - Affiliates	Yes	
PNM Resources	Yes	
PPL Electric Utilities	Yes	
PPL Supply	Yes	
Southern Company - Transmission	Yes	
TransAlta Corporation	Yes	
We Energies	Yes	
WECC	Yes	

10. Do you agree with the impact event list in Attachment 1? Please explain in the comment box below and provide suggestions for additions to the list of impact events.

Summary Consideration: Most commenters who responded to this question disagreed with some aspect of Attachment 1 – most commenters provided specific suggestions for improvement. The DSR SDT did a full review based on comments that were received. The DSR SDT, the Events Analysis Working Group (EAWG), NERC Staff (to include NERC Senior VP and Chief Reliability Officer) had an open discussion with this item being a major topic. The EAWG and the DSR SDT aligned Attachment 1 with the Event Analysis Program category 1 analysis responsibilities. This will assure that impact events in EOP-004-2 reporting requirements are the starting vehicle for any required Event Analysis within the Event Analysis Program. The DSR SDT agrees that there are similar items in the DOE Form OE 417 and EOP-004-2. DOE, NERC and the DSR SDT are in initial talks to try and reduce duplicate reporting requirements. Until such time in the future that a new process is established between the DOE and NERC, the DSR SDT has revised the standard to indicate that the use of either the DOE Form OE 417 or Attachment 2 is an acceptable reporting form for applicable entities. The DSR SDT reviewed the "hierarchy" of reporting within Attachment 1. To reduce multiple entities reporting the same impact event, the DSR SDT has stated that the entity that performs the action or is directly affected by an action will report per EOP-004-2. As an example, during a system emergency, the TOP or RC may request manual load shedding by a DP or TOP. The DP or TOP would have the responsibility to report the action that they took if they meet or exceed the bright-line criteria established in Attachment 1. Upon reporting, NERC Event Analysis Program would be made aware of the impact event and start the EA Process which is outside the scope of this Standard.

Several bright-line criteria were removed from Attachment 1. These criteria (DC converter station, 5 generator outages, and frequency trigger limits) were removed after discussions with the EAWG and NERC staff, who concurred that these items should be removed from a reporting standard and analysis process.

Organization	Yes or No	Question 10 Comment

Organization	Yes or No	Question 10 Comment
WECC		For strictly after-the-fact reporting the list of Attachment 1 is appropriate. However, as noted in our earlier comments, actual or suspected sabotage events can have a potentially significant impact on reliability and should be treated differently, with additional real-time reporting requirements. It is important that such events be identified and recognized for reliability purposes and that notices include the RC.
Ameren	No	We have numerous comments about the Attachments. (1) What are the requirements for "verbal" reporting to NERC and Regional entities? (2) What are the requirements for a "Preliminary" Impact Event Report? (3) The Voltage Deviations Event is unclear (a) Are these consecutive minutes? (b) Where is the voltage measured? (generator terminals? Point of Interconnections? Anywhere?) (c) must each Entity report separately? (d) What is the +/- 10% measured against (Generator Voltage Schedule?) (4) For Generation loss events how is an "entity" defined? (a corporate parent? each registered entity? other?) (5) Are the "Examples" in the Attachment 1 - Part A really Examples, or mandatory situations? (6) Can you define "Damage"? (7) Can you define "external cause"? (8) Can you give examples of "non-environmental external causes"? (9) The footnote 1 reference for "Damage or destruction of BES equipment" doesn't match up with the a. and b. footnotes or the 1. footnote of Attachment A - Part B. (10) How is the Operator supposed to determine what Event affects the reliability of the BES fast enough to decide whether or not to report? (11) is the Loss of off-site power (grid supply) event to a nuclear plant already covered by NUC-001?(12) What are "critcal cyber assets" since CIP-002-4 will eliminate that term? (13) When is Attachment 2 supposed to be used? (14) What is meant by the word "Confidential" in the title of the Attachment 2 report? How would the SDT propose a GO/GOP handle the reporting for the following situation? A CTG unit is dispatched and the unit is started, synchronized and put on the bus. Immediately the Operator receives a high gas alarm from the GSU. The Operator quickly shuts the unit down and de-energizes the GSU. There are no relay targets and no obvious reason for the problem. After several weeks of analysis it's determined there was an internal fault in the GSU

Organization	Yes or No	Question 10 Comment
		and it must be replaced. How would the SDT recommend all the reporting requirments in this situation be addressed with the current draft?
American Electric Power (AEP)	No	Are the times listed for the initial probable reporting under R3 or the reporting under R6?Many of these items do not constitute emergency conditions. We view many of these as too onerous and would divert operating staff from monitoring and operating the BES. In addition, some terms (i.e. Frequency Trigger Limits) are not currently defined terms. Furthermore, there are existing requirements that have obligations for entities to provide this information to the RC. For example "Detection of a cyber intrusion to critical cyber assets" is already covered under CIP-008. This creates duplicate (and potentially competing) requirements.AEP also contends that some of the timelines are very aggressive and not consummate with perceived need for the information.Transmission loss of multiple BES transmission elements (simultaneous or common-mode event)within 24 hours after occurrence is overly aggressive and should provide more specific criteria.
Arizona Public Service Company	No	AZPS believes that the list in Attachment 1 would be complete, as long as the text box of examples is included. The examples demonstrate what is necessary.
ATC	No	ATC has several areas of concern regarding Attachment 1.1. The one hour requirement for reporting will take the Functional Entities' focus off of addressing the immediate reliability issues and instead force the FE to devote valuable resources to filling out forms which will potentially reduce reliability.2. Part A:a. Provide a definition of "system wide" for the Energy Emergency requiring system-wide voltage reduction.b. Add in the clarity that for Energy Emergency requiring firm load shed pertains to a single event, not cumulative events.c. Insert the word "continuous" for Voltage Deviations.d. Take off the TOP for IROL violations. (We believe that an IROL violation should be reported by the RC and not by the TOP based on the nature of the event. Requiring both the RC and TOP to report will only result in multiple reports for a single event. The RC is in

Organization	Yes or No	Question 10 Comment
		the best position to report on an IROL violation for its RC area.)e. Take off the TO, TOP and add the LSE for Loss of Firm Load. (As a transmission only company ATC does not have contracts with end load users. Because of this the Loss of Firm Load should be the reporting obligations of the entity closes to the end load users which is the BA, DP or LSE. Failure to modify this requirement will cause confusion as to which entity has to report Loss of Firm Load. f. Define a timeframe for Generation Loss g. Multiple should be changed to "4 or more" for Transmission Loss.(ATC is concerned that this would require reporting of events that have little or no industry wide benefits but would take up considerable Registered Entity resources.)h. Provide clarity to and tighten the definition of Damage or destruction of BES equipment. The way it is written now would require over-reporting of all damaged or destroyed equipment due to a non-environmental external cause (e.g. broken insulator).3. Part B:a. Take off the TO and TOP for Loss of off-site power. (The GOP has the responsibility to acquire off-site power and we believe it is the GOP's sole responsibility to report the Loss of off-site power. Failure to correct this would result in multiple reporting for the same event.)b. Take off RC for Risk to BES equipment. (The RC function does not own BES equipment and we believe it is impossible for them to report on risk to BES equipment if they are not the owner or operator of that equipment. This standard should be required of the entity that owns/operates BES equipment. c. Provide guidance to the phrase "reasonably determine" in footnote.d. Examples provided do not provide a clear obligation for an entity to follow. (Question: How close is the train to the substation? (Inches away from the substation fence, ten feet away from the substation fence or 500 feet away from the substation fence.) In addition, this standard is so open to interpretation that no entity can demonstrate compliance with the action. We believe that the only solution is to delete this reporting requirement. Overall:Multiple Functional Entities impacted by the same event are required to report. No lead entity is identified. This will result in multiple reports of the same event. ATC does not believe that this built-in duplicity enhances reliability?

Organization	Yes or No	Question 10 Comment
ATCO Electric Ltd.	No	Attachment 1: Part A - Transmission Loss: Only sustained outages should be reportable. Also the reporting threshold needs to be quantified for impact events, for example:a) Size of DC converter Station > 200 MW.b) Impact of loss of Multiples BES transmission elements in terms of significant load (> 200 MW for > 15 min).
BGE	No	TOP determines "system-wide" voltage reductions; why place this responsibility on a TO or DP? - Load Shedding is automatic load shedding; why 100MW? Does a DP need to provide a Report when directed by the RC, BA or TOP to shed load or reduce voltage? - No examples should be included in the standard! Need to define a "BES Transmission Element". - Table shows multiple entities in "Entity with Reporting Responsibility"; is it one or is it all entities report? - In an audit who determines "reasonably determined likely motivation" - Is it justified to expect to have "motivation" knowledge within one hour of an event? - Why are the Responsible Entities reporting Interruptible Demand tripped / lost?
Bonneville Power Administration	No	BPA suggests the following:Change loss of multiple BES to 3 or more. Loss of a double circuit configuration due to lightning doesn't need a report (it's a studied contingency). Add qualifier to damage/destruction of BES equipment, since a failed PCB or a system transformer normally doesn't have a MAJOR impact to the grid.Add qualifier to Loss of "ALL" off-site power affecting nuclear...The unplanned evacuation of control center is a busy time for the backup control center, yet this standard requires 1 hour reporting. Suggest changing to 24 hours.
CenterPoint Energy	No	CenterPoint Energy appreciates the efforts of the SDT in identifying the entity with reporting responsibility. This is an improvement to the event table. CenterPoint Energy is concerned with multiple entities being listed as having Reporting Responsibility. CenterPoint Energy recommends the SDT limit this to one entity having responsibility for reporting each event. This would not preclude that entity from coordinating with other entities

Organization	Yes or No	Question 10 Comment
		to gather data necessary to complete the report. In addition, CenterPoint Energy believes there are several events that should be removed from the list. “Transmission Loss” is covered by the TPL standards and does not need to be identified or reported under EOP-004. The loss of a DC converter station or multiple BES transmission elements may or may not disrupt the reliable operation of the BES, i.e. result in blackout, cascading outages, or voltage collapse. Likewise “Damage or destruction of BES equipment” in and of itself should not be the subject of reporting. If the damage or destruction results in true disruption to the reliable operation of the BES, that impact would be reported under one of the other identified events. “Voltage Deviations” is another unnecessary event. CenterPoint Energy believes a voltage event of the proposed magnitude will, more than likely, result in other events identified in Attachment 1 such as; IROL Violation or Generation Loss and would be reported under one of those triggers. Another concern is the threshold trigger of +/- 10% for 15 minutes or more. CenterPoint Energy is unclear as to the starting point to determine the deviation. In other words is the 10% deviation from nominal voltage, such as 138kV or 345kV, or the actual voltage at the time of the event? Additionally, must the deviation occur over a “wide area” or is such a deviation at one buss enough to trigger a report? Based upon these ambiguities and concerns CenterPoint Energy recommends “Voltage Deviations” be deleted from Attachment 1. The examples that follow on page 14 should also be deleted.
City of Garland	No	This report should follow exactly the OE-417 to avoid redundant, possible conflicting, and overall confusion in reporting.Note: The table has entries that are in conflict with the OE-417 and thus can cause confusion in filing multiple reports potentially causing an entity to violate Federal Law due to the confusion. By submiting the same information on different timelines, i.e. one hour reporting under OE-417 and 24 hours under this Standard, the reports may be significantly different causing confusion from differing reports of the same event.Although we prfer the events to match the OE-417 events exactly, if the SDT decides to include a

Organization	Yes or No	Question 10 Comment
		seperate events table we make the following suggestions: Energy Emergency requiring system-wide voltage reduction: should be reportable at 5% not 3% voltage reduction. The standard should clearly state this was applicable for BES energy emergency conditions only, not voltage reductions for other reasons.On voltage deviations: it should be clear that this applies to widespread effects on the BES not a single distribution feeder that has a low voltage.For the Frequency deviation: Did not see a definition for the FTL (frequency trigger limit)Generation loss: the reportable loss of generation should be significantly more than 500 MW. The number of units at the locaton is irrelevent. Ten units at 50 MW each is no more critical than a single 500 MW unit. Under this standard, if the plant with ten 50 MW units trips it is reportable but an 800 MW single unit is not reportable. The trip of the 800 MW unit has much more effect on the sytem reliability. Damage or destruction of BES equipment: Should be limited to specific equipment such as a 765 kV autotransformer not a 138 kV lightning arrestor. This needs to be eliminated or significantly limited as to the equipment type that is reportable.
Consolidated Edison Co. of NY, Inc.	No	It is absolutely essential that the work on EOP-004 and that on the NERC Event Analysis Process (EAP) be fully coordinated. We find that there are a number of inconsistencies between these two documents. The EAP and EOP-004 are not aligned. In order to operate and report effectively entities need consistent requirements.Attachment 1Frequency Deviations - The term “Frequency Trigger Limit (FTL)” is not defined. Only defined terms should be used, or the term should be defined. If the term is defined in another standard it should be moved to the Glossary of Terms for wider use.Loss of Firm load for 15 Minutes - The text under the rightmost column entitled, Time to Submit Report, appears to be incomplete in our copy.Transmission loss and Damage or destruction of BES equipment - At the end of the wording for both under the column entitled “Threshold for Reporting” add the words “that significantly affects the integrity of interconnected system operations.”Examples - Capitalize “Critical Asset” as this is a defined term.

Organization	Yes or No	Question 10 Comment
Constellation Power Generation and Constellation Commodities Group	No	Constellation Power Generation and Constellation Commodities Group questions why the generation loss line item includes generating facilities of 5 or more generators with an aggregate of 500 MW or greater? The number of units makes no difference for reporting, as is evident in the generation thresholds written before this inclusion. The examples of damaged or destroyed BES equipment are confusing, and do not clarify the reporting event. What if a GSU at a small plant (20 MW) were to fail? Is that reportable? Constellation Power Generation believes that equipment failures that are not suspicious do not need to be reported. Finally, Constellation Power Generation and Constellation Commodities Group believes that the "loss of offsite power affecting a nuclear generation station" should be removed for the following reasons:1)The purpose of this reliability standard is stated as being: "Responsible Entities shall report impact events and their known causes to support situational awareness and the reliability of the Bulk Electric System (BES). " While the "situational awareness" portion of the purpose could be interpreted as all-inclusive, the real element deals with BES reliability. Off-site power sources to nuclear units have nothing to do with BES reliability. Why should nuclear units be treated differently?2)The issue of concern for a loss of offsite power at a nuclear station is continued power supply (other than emergency diesels) to power equipment to cool the reactor core. A nuclear unit automatically shuts down when off-site power supply is lost. Availability of off-site power is a reactor safety concern (i.e., NRC regulatory concern and a one-hour report to the NRC) - not a reliability concern that FERC/NERC would have jurisdiction over.3)There is a nuclear-specific reliability standard (NUC-001) that contemplated off-site power availability. That standard contained no reporting requirements outside of those that may be already established in current procedures. Why try to impose one here?4)A loss of offsite power will result in an emergency declaration at the nuclear facility. Notifications will be made to federal (NRC), state, and local authorities. The control room crew is already overly-burdened with notifications - any additional call to NERC/Regional Reliability orgs will add insult-to-injury for no beneficial reason. If NERC is interested, they should obtain info from NRC.5)If all else fails and the item is to remain on the table, it needs

Organization	Yes or No	Question 10 Comment
		to be clarified as a “complete” loss of off-site power lasting greater than X minutes (i.e., would we have to report a complete momentary loss that was rectified in short order by an auto-reclose or quick operator action?).
Duke Energy	No	o General Comment - many timeframes in Attachment 1 are within one hour. This is inconsistent with the stated aim of the standard, which is after-the-fact reporting, as opposed to real-time operating notifications under RCIS and other standards (e.g. TOP). This standard should not be structured to require another layer of real-time reporting. o Voltage Deviation - Plus or minus 10% of what voltage? o Frequency Deviation - this is Interconnection-wide. Do you really want a report from every RC and BA in the Eastern Interconnection?? o Transmission Loss - “Multiple BES transmission elements” should be changed to “Three or more BES transmission elements”. Also, the time to submit the report should be based upon 24 hours after the occurrence is identified. o Damage or destruction of BES equipment - need clarity on the “Examples”. Is the intent to report an event that meets any one of the four “part a.” sub-bullets? i. - critical asset should be capitalized. Disagree with the phrase “has the potential to result” in section iii. - it should just say “results”. Section iv. is too wide open. It should instead say “Damaged or destroyed with malicious intent to disrupt or adversely affect the reliability of the electric grid.” o Unplanned Control Center evacuation - see our General Comment above. Clearly in this case the reporting individuals are evacuating and cannot report in one hour. 24 hours should be more than adequate for after-the-fact reporting. o Fuel Supply Emergency, Loss of off-site power, and Loss of all monitoring or voice communication capability - see our General Comment above. Time to report should be 24 hours after occurrence is identified. o Forced intrusion, Risk to BES equipment, Detection of a cyber intrusion to critical cyber assets - time to report should be 24 hours after occurrence is identified, and critical cyber assets should be capitalized.

Organization	Yes or No	Question 10 Comment
Dynegy Inc.	No	A 2000 MW loss needs to be more clearly defined by either the BA, ISO, RC, etc. for the applicable enity.Also, what is the distinction between the "damage or destruction of BES equipment" and the generation loss of >= 2000 MWs if it is a Critical Asset which is currently drafted as those greater than 1500 MW in current draft of CIP-002-4. This could lead to 2 events with different thresholds (i.e. 1500 MW and 2000 MWs). Possibly get rid of the 2000MW criteria and let the threshhold level be the same as the Critical Asset MW level. Or remove the Critical Asset threshhold in the footnote to Attachment 1.
E.ON Climate & Renewables	No	1. Voltage deviation events are too vague for GOP. How does voltage deviations apply to GOP's or specifically renewables i.e., wind farms? 2. Define what an "entity" is. 3. Define what a "generating station" is. 4. Define what a "BES facility" is.6. Define what a control center is.
Electric Market Policy	No	1) A particular Event could be applicable to multiple entities and Attachment 1 would require each applicable entity to report the event. This is duplicative and would appear to overburden the reporting system. 2) Loss of off-site power (grid supply) reporting for nuclear plants is duplicative of reporting done to satisfy NRC requirements. Given the activity at a nuclear plant during this event, this additional reporting is not desired. 3) Cyber intrusion remains an event that would need to be reported multiple times (e.g., this standard, OE-417, NRC requirements, etc.). 4) Since external reporting for other regulators (e.g., DOE, NRC, etc.) remains an obligation of the Applicable Entity, suggest that Attachment 1 only contain impact events as defined in the current version of EOP-004.
ERCOT ISO	No	ERCOT ISO requests the reporting timeframes be changed to reflect a 24 hour requirement for all events in Attachment 1. During an impact event, operating personnel are generally involved in event resolution and not available immediately to submit reports. ERCOT ISO requests that the "Detection of a cyber intrusion to a

Organization	Yes or No	Question 10 Comment
		critical cyber asset" be removed. There are established processes defined for incident response supporting CIP-008. By including this element in Attachment 1, the Operating requirement R2 would also require procedure documents for cyber security incident response. This would be redundant and would remove the responsibility away from the subject matter experts for cyber security incident response.
Exelon	No	The listed Impact Events is lacking specific physical security related events. .In general, all impact events need to be as explicit as possible in threshold criteria to eliminate any interpretation on the part of a reporting entity. Ambiguity in what constitutes an "impact event" and what the definition of "occurrence" is will ultimately lead to confusion and differing interpretations.
FirstEnergy	No	1. The table in Att. 1 and the requirements should alleviate the potential for duplicate reporting. For example, If the RC submits a report regarding a Voltage deviation in its footprint, the report should be submitted by the RC on behalf of the RC, TOP, and GOP, and not require the TOP and GOP to submit duplicate reports.2. Regarding the "Note" before the table - We agree that under certain conditions it is not possible to issue a written report in a given time period. However, the ERO and RE should also be required to confirm receipt of the verbal communication in writing to prove that the entity communicated the event as these verbal notifications may be done by an entity using an unrecorded line.3. Organizations with many registered entities should be permitted to submit one report to cover multiple entities under one parent company name. We suggest this be made clear in the Tables, the reporting form, and in the requirements.4. Voltage Deviations Event - We suggest the team provide more clarity with regard to the types and locations of voltage deviations that constitute an event.5. Examples of BES Equipment in Part A of "Actual Reliability Impact" Table - Is the phrase "critical asset" referring to the CIP defined term? If so, this should be capitalized.6. Under the "Time to Submit Report" column of the table, we suggest that all of the phrases end in "after identification of the

Organization	Yes or No	Question 10 Comment
		occurrence".7. Frequency Trigger Limit (FTL) for the Frequency Deviation event should be replaced with the values the FTL represent. The FTL is part of the BAAL Standards which have not been approved by the industry and are not in effect. It is possible that these terms are not used by those not participating in the field trial of the BAAL standards.
Great River Energy	No	Comments: Please provide a phone number and provision within the Note of EOP-004 - Attachment 1: Impact Events table for an entity to contact NERC if unable to contact NERC within the time described.Voltage Deviations - recommend adding the word “(continuous)” after sustained in Threshold column. This could be interpreted as an aggregate value over any length of time.Frequency deviations - recommend adding the word “(continuous)” after 15 minutes’ in Threshold column. This could be interpreted as an aggregate value over any length of time.CIP-008 R1.3 states the entity is to report Cyber Security Incidents to the ES_ISAC. Does the EOP-004 Attachment 2 fulfill this requirement?We request clarification on the Transmission Loss threshold events that constitute reporting. We also want clarification on what constitutes the loss of a DC Converter station and is there a time duration that constitutes the need for reporting or does each trip need to be reported? For example during a commutation spike the DC line could be lost for less than a minute. Does this loss require a report to be submitted? Is the SDT stating that each time a company loses their DC line, they are required to file a report even though it may not have an effect on the bulk system? What is the threshold for this loss?The SDT needs to clarify that duplicative reporting is not required and that only one entity needs to report. For instance, the first three categories regarding energy emergencies could be interpreted to require the BA and RC to both report. The reporting responsibilities in this table should be clarified based on who has primary reporting responsibility for the task per the NERC Functional Model and require only one report. For instance, since balancing load, generation and interchange is the primary function of a BA per the NERC Functional Model, only the BA should be required to provide this report.The

Organization	Yes or No	Question 10 Comment
		term Frequency Trigger Limit (FTL) is not currently defined in the NERC Glossary. The term FTL needs to be introduced at the beginning of the standard and defined as a new term.
Indeck Energy Services	No	Loss of off-site power is important to more than just nuclear plants--but which ones? Control centers or other large generators. But not small generators! Should there be a common element to Attachment 1, like the potential to cause a Reportable Disturbance, or maybe there need to be multiple criteria like that.
Independent Electricity System Operator	No	We do not support the 1 hour reporting time frames for Emergency Energy, System Separation, unplanned Control Center evacuation, Loss of off-site power, Loss of monitoring or voice communication. Energy emergency is broadcast on the RCIS which also goes to the ERO so its explicit reporting is not necessary (System Operations please verify). During other events listed above, the responsible entities will likely be concentrating its effort in returning the system to a stable and reliable state. Reporting to anyone not having direct actions to control, mitigate and contain the disturbances is secondary to restoring the system to t a reliable state. Since these are after the fact reports for awareness and/or analysis and not for real-time responses, these can be reported at a later time, up to 24 hours after the initial occurrence without any detriment to reliability, or at the very earliest: up to 1 hour after the system has returned to a reliable state, or after the backup control centre is fully functional, or after backup power is restored to the nuclear power plant, or after monitoring or voice communication is restored.
IRC Standards Review Committee	No	We do not agree with the requirement to report “detection of a cyber intrusion to critical cyber assets” as this creates a double jeopardy situation between CIP-008 and EOP-004-2 R2.6. We suggest that physical incident reporting be part of EOP-004 and cyber security reporting be part of CIP-008.
ISO New England Inc.	No	1) A particular Event could be applicable to multiple entities and Attachment 1 would require each applicable

Organization	Yes or No	Question 10 Comment
		entity to report the event. This is duplicative and would overburden the reporting system. 2) Loss of off-site power (grid supply) reporting for nuclear plants is duplicative of reporting done to satisfy NRC requirements. Given the activity at a nuclear plant during this event, this additional reporting is not desired. 3) Cyber intrusion remains an event that would need to be reported multiple times (e.g., this standard, OE-417, NRC requirements, etc.). 4) Since external reporting for other regulators (e.g., DOE, NRC, etc.) remains an obligation of the Applicable Entity, suggest that Attachment 1 only contain impact events as defined in the current version of EOP-004.What are the examples at the bottom of page 14 supposed to illustrate? Critical Asset should have the appropriate capitalization as being a defined term. Is Critical Asset what is intended to be used here? Should the "a" list be read as ANDs or Ors? Does "loss of all monitoring communications" mean "loss of all BES monitoring "communications"? Does "loss of all voice communications" mean "loss of all BES voice communications?"Are the blue boxes footnotes or examples?Does "forced intrusion" mean "physical intrusion" (which is different from "cyber intrusion")?Regarding "Risk to BES Equipment," request clarification of "non-environmental". Regarding the train derailment example, the mixture of BES equipment and facility is confusing. Request clarification for when the clock starts ticking.Regarding "Detection of a cyber intrusion to critical cyber assets", there is concern that this creates a double jeopardy situation between CIP-008 and EOP-004-2 R2.6. Suggest physical incident reporting be part of EOP-004 and cyber security reporting be part of CIP-008.
Kansas City Power & Light	No	We agree with the event descriptions listed in Attachment 1 and the review and revision of the impact table by the ERO is appropriately addressed in R7 but the time periods allowed to complete the new, longer preliminary report is insufficient. The correlation of this with the timing of the reporting quarterly and annually or pushing information for other entities' situational awareness does not allow the registered entity adequate time to thoughtfully consider the event and proposed root cause.

Organization	Yes or No	Question 10 Comment
Luminant Energy	No	The Impact Events Table might be easier to clarify if organized by Reporting Entity rather than Event Type as events vary substantially based on the affected BES component. For example, a GO or GOP cannot adequately determine if an event will significantly affect the reliability margin of the system or if an event results in an IROL. Examples specific to Reporting Entities would assist in more appropriate report submissions. Additionally, the footnote under examples of Damage or Destruction of BES Equipment, cites "A critical asset". This term must be clarified to indicate whether this refers to a Critical Asset as defined by CIP 002-1.Finally, the Fuel Supply Emergency item requires additional definitions as neither a GO nor a GOP can reasonably project if an individual fuel supply chain problem will result in the need for emergency actions by the RC or BA.
MidAmerican Energy	No	New vague criteria in Attachment one such as "damage to a BES element through and external cause" or "transmission loss of multiple BES elements which could mean two or more" is the opposite of clear standards writing or results based standards.
Midwest ISO Standards Collaborators	No	Several categories require duplicate reporting. For instance, the first three categories regarding energy emergencies could be interpreted to require the BA and RC to both report. The reporting responsibilities in this table should be clarified based on who has primary reporting responsibility for the task per the NERC Functional Model and require only one report. For instance, since balancing load, generation and interchange is the primary function of a BA per the NERC Functional Model, only the BA should be required to provide this report. As another option, perhaps the registered entity initiating the action should submit the report. If the BA did not take action and the RC had to direct the BA to take action, one could argue that perhaps the RC should submit the report then. However, if the BA takes action appropriately on their own, the BA should submit it. If the TOP reduces voltage for a capacity and energy emergency per a directive of the BA, then the

Organization	Yes or No	Question 10 Comment
		BA should report the event.
MRO's NERC Standards Review Subcommittee	No	Please provide a phone number and provision within the Note of EOP-004 - Attachment 1: Impact Events table for an entity to contact NERC if unable to contact NERC within the time described.Voltage Deviations - recommend adding the word “(continuous)” after sustained in Threshold column. This could be interpreted as an aggregate value over any length of time.Frequency deviations - recommend adding the word “(continuous)” after 15 minutes’ in Threshold column. This could be interpreted as an aggregate value over any length of time.CIP-008 R1.3 states the entity is to report Cyber Security Incidents to the ES_ISAC. Does the EOP-004 Attachment 2 fulfill this requirement?
Nebraska Public Power District	No	Since the reporting under this standard is for after the fact reporting, the minimum time to report should be the end of the next business day. The combination of the extremely short time periods to file a report and the amount of detail required in attachment 2 will lead to a reduction in the reliability of the BES. System Operators will be forced to take focus off their primary responsibility to respond to the event in order to complete the report within the required timeframe (within an hour for some events). During non-business hours the only personnel available to complete the reports will be those responsible for real-time operation of the BES. Since the background indicates this standard is only for after the fact reporting, the minimum required time to submit the report should be one business day to permit completion of the report without distracting from the real-time operation of the BES. Real-time reporting requirements are covered in other standards and should be to the Reliability Coordinator and from the Reliability Coordinator to NERC. For after the fact reporting, there is absolutely no reliability benefit for requiring reporting to be completed on such a short timeframe. This is especially true due to the amount of data required by Attachment 2.

Organization	Yes or No	Question 10 Comment
NERC Staff	No	The SDT should clarify its use of the term “critical asset” in the Examples section under Part A of the table. The term or versions of the term are used in different contexts in the NERC Reliability Standards. For instance, in CIP-002-1, Requirement 1, the Critical Asset Identification Method is used to identify its critical assets. In EOP-008-0, Requirement 1.3, the applicable entity is required to list its “critical facilities” in its contingency plan for the loss of control center functionality. The team should confirm what it is referring to in this proposed standard. To avoid confusion, the SDT may want to consider using a different term here or better clarify its meaning. Further, there exists the potential to have disparate reporting criteria in this proposed standard relative to the criteria being proposed by the Events Analysis Working Group as part of the Events Analysis Process document dated October 1, 2010. In particular, the following areas should be reconciled between the drafting team and the EAWG to ensure a consistent set of threshold criteria:Voltage Deviations --EOP-004-2: Greater than or equal to 15 minutes --EAWG Process: Greater than or equal to 5 minutesSystem Separation (Islanding) --EOP-004-2: Greater than or equal to 100 MW --EAWG Process: Greater than or equal to 1000 MWsSystem Separation (Islanding) --EOP-004-2: Does not address intentional islanding as in the case of Alberta, Florida, New Brunswick--EAWG Process: Addresses intentional islanding as in the case of Alberta, Florida, New BrunswickSPS/RAS --EOP-004-2: Does not expressly address proper SPS/RAS operations or failure, degradation, or misoperation of SPS/RAS --EAWG Process: Expressly addresses proper SPS/RAS operations or failure, degradation, or misoperation of SPS/RASTransmission Loss --EOP-004-2: Identifies Multiple BES transmission elements --EAWG Process: Provides specificity in Category 1a and 1b regarding transmission eventsDamage or destruction of BES equipment --EOP-004-2: Through operational error, equipment failure, or external cause but not linked to loss of load--EAWG Process: Identifies in Category 2h equipment failures linked to loss of firm system demandsForced intrusion--EOP-004-2: Addressed --EAWG Process: Not addressedRisk to BES equipment --EOP-004-2: Addressed --EAWG Process: Not addressedDetection of a cyber intrusion to critical cyber assets --EOP-004-2: Addressed --

Organization	Yes or No	Question 10 Comment
		EAWG Process: Not addressed
North Carolina Electric Coops	No	This list is too similar and redundant to the DOE requirements and does not provide any additional clarity on recognition of sabotage.
Northeast Power Coordinating Council	No	1) A particular Event could be applicable to multiple entities and Attachment 1 would require each applicable entity to report the event. This is duplicative and would overburden the reporting system. 2) Loss of off-site power (grid supply) reporting for nuclear plants is duplicative of reporting done to satisfy NRC requirements. Given the activity at a nuclear plant during this event, this additional reporting is not desired. 3) Cyber intrusion remains an event that would need to be reported multiple times (e.g., this standard, OE-417, NRC requirements, etc.). 4) Since external reporting for other regulators (e.g., DOE, NRC, etc.) remains an obligation of the Applicable Entity, suggest that Attachment 1 only contain impact events as defined in the current version of EOP-004.What are the examples at the bottom of page 14 supposed to illustrate? Critical Asset should have the appropriate capitalization as being a defined term. Is Critical Asset what is intended to be used here? Should the “a” list be read as ANDs or Ors? Does “loss of all monitoring communications” mean “loss of all BES monitoring “communications”? Does “loss of all voice communications” mean “loss of all BES voice communications?”Are the blue boxes footnotes or examples?Does “forced intrusion” mean “physical intrusion” (which is different from “cyber intrusion”)?Regarding “Risk to BES Equipment,” request clarification of “non-environmental”. Regarding the train derailment example, the mixture of BES equipment and facility is confusing. Request clarification for when the clock starts ticking.Regarding “Detection of a cyber intrusion to critical cyber assets”, there is concern that this creates a double jeopardy situation between CIP-008 and EOP-004-2 R2.6. Suggest physical incident reporting be part of EOP-004 and cyber security reporting be part of CIP-008.

Organization	Yes or No	Question 10 Comment
Pacific Northwest Small Public Power Utility Comment Group	No	Footnote 1 is missing from Part A, although it is referenced in column 1 row 11. Is this the Examples? The purpose of the Examples is unclear. Is it meant to limit the scope to those enumerated? This is not stated, but if not it should be removed since it adds confusion. What is meant by non-environmental? All external causes of damage or destruction come from the environment by definition. Please specify what is intended or remove the word.
PacifiCorp	No	Energy Emergency requiring firm load shedding - An SPS/RAS could operate shedding firm load but no Energy Emergency may exist. This requires clarification.Transmission Loss - Multiple BES transmission elements. Loss of two transmission lines in the same corridor due to a wildfire could qualify for this reporting. Once again clarification needed.
Pepco Holdings, Inc - Affiliates	No	Some items with one hour reporting (such as Unplanned Control Center evacuation) may be so disruptive to operations that one hour is too short. 4 hours suggested.
PPL Electric Utilities	No	While we think providing an impact event list is beneficial, we would like to see Attachment 1 revised and/or clarified. Refer to response to Question 2 considering duplicate reporting. Regarding impact event 'Damage or destruction of BES equipment' and considering the first example in the 'Examples' section, does 'example a. i.' mean if the BES equipment that is damaged is not identified as a critical asset per CIP-002 that no reporting is required? Clarify the Part A and Part B, specifically:Attachment 1 Part A is labeled 'Actual Reliability Impact'. Does this title mean that for all events listed that the 'threshold for reporting' is only met if the event occurs AND there is an actual reliability impact? As opposed to Part B where the threshold for reporting is met when the event occurs and there is a potential for reliability impact? This could be broad for event 'risk to BES equipment'. Providing as much clarity as possible on the 'threshold for reporting' is

Organization	Yes or No	Question 10 Comment
		beneficial to the industry and will help eliminate confusion with the existing CIP-001 standard regarding 'potential sabotage'.
PPL Supply	No	Attachment 1 Part A is labeled "Actual Reliability Impact". Does this title mean that for all events listed the "threshold for reporting" is only met if the event occurs AND there is an actual reliability impact? As opposed to Part B where the threshold for reporting is met when the event occurs and there is a potential for reliability impact? This could be broad for events like "Risk to BES equipment."
PSEG Companies	No	For many items, there are multiple entities listed with reporting obligations. For example, loss of off-site power to a nuclear plant lists RC, BA, TOP, TO, GO and GOP. This appears to result in the potential for the sending of 6 separate reports within the hour for the same event, which in wide area disturbances overload the recipients. The drafting team should consider revising the lists where possible to a single, or absolute minimum number, entity.Those items reportable OE-417 should be removed from Attachment 1. For example, voltage reduction, loss of load for greater than 15 minutes.The trigger for voltage reduction should be the time of issuance of the directive to reduce voltage in an emergency, not when "identified."
Puget Sound Energy	No	The proposed standard does not adequately ensure that the impact events subject to its requirements are limited to those listed in Attachment 1. In order to ensure that this is true, the term "impact event" should be a defined term and that definition should clearly limit impact events to those listed in Attachment 1.
Santee Cooper	No	The SDT should review the list of events closely to determine if the defined events actually impact the BES. (For example: Is shedding 100 MW of firm load really a threat to the BES?)
SERC OC Standards Review	No	Will all reporting requirements be removed from other standards to avoid duplication? And will all future

Organization	Yes or No	Question 10 Comment
Group		standard revisions include revisions to this standard to incorporate associated reporting requirements?There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
Southern Company - Transmission	No	The time to submit report column needs to be more flexible with time frames. The Entity with Reporting Responsibility column needs to be more descriptive in which there are multiple entitles with hierarchy reporting.
United Illuminating	No	UI agrees but the listing needs to be improved for clarity in certain instances. For example,EOP-004 Attachment 1 Part A - Example iii - uses the phrase “significantly affects the reliability margin of the system.” Significantly is an immeasurable concept and does not provide guidance to the Entity. The phrase “reliability margin” is not defined and is open to interpretation. Perhaps utilize “resource adequacy”, if that is all that intended, or use “adequate level of reliability”.
US Bureau of Reclamation	No	The Attachment is very vague and without modification creates a Pseudo definition of BES equipment in the example provided. The example now indicates that something is BES equipment if it is "Damaged or destroyed due to a non-environmental external cause". Perhaps the example should be reworded to "BES equipment whose operation effects or causes:" and then adjust each of the line items to clarify what was intended. Next, the Attachment A example redefines reportable levels for Risk to BES Equipment - From a non-environmental physical threat as "Report copper theft from BES equipment only if it degrades the ability of equipment to operate correctly". Who makes that determination? Not all events will be known within 24 hours. As example, Risk to BES Equipment - From a non-environmental physical threat may not be known until more thorough examination or investigation takes place. Also the reportable level appears to be defined by the Entity. While agree with that, we will end up with the same criticism from FERC when the level is set to

Organization	Yes or No	Question 10 Comment
		"high" in FERC's mind. The reporting times are unrealistic for complicated events. Notification is reasonable but not reporting. Many organizations's have internal processes the reports must be vetted through before they become public and subject to compliance scrutiny.
We Energies	No	I did not compare this standard to the OE-417 form. Please do not require operators to fill out a second form during an emergency within one hour.Energy Emergency requiring Public appeal...: "Public " is not a defined term.Energy Emergency requiring system-wide voltage...: DP does not control BES voltage.Energy Emergency requiring firm load shed...: TOP does not have load it would shed for an Energy Emergency.Frequency Deviations: Why is a BA reporting? This will be every BA in the Interconnection reporting the same Frequency Deviation.Frequency Deviations: Frequency Trigger Limit is not a defined term, and is not defined in this standard.Loss of Firm Load...: TO and TOP may coordinate or direct load shed, but they do not serve firm load.Damage or destruction of BES... There is no footnote 1 on this page. I assume it is the examples on the page. Are these "examples" of a larger set or are these all that is required? Critical Asset is a defined term.Forced Intrusion: "facility" or Facility? An RC and BA do not have Facilities.
Georgia System Operations Corporation	Yes	We support the concept of Impact Events and listing and describing them in a table. However, we have some concerns.Reporting of impact events should not be applicable to a DP.The timelines outlined in Attachment 1 should be targets to try to meet but it should not be a compliance violation of the reporting requirement if it is not met. Regarding the NOTE before the table, verbal reports and updates should be allowed for other than certain adverse conditions like severe weather as well as adverse conditions. The first priority for all entities should be addressing the effects of the impact event. It may not be possible to assess the damage or the cause of an impact event in the allotted time. All entities should make their best effort to quickly report under any circumstances what they know about the event even if it is not complete. They should be allowed to

Organization	Yes or No	Question 10 Comment
		report up through a hierarchy. The written report should not be issued until adequate information is available. Change "Preliminary Impact Event Report" to "Confidential Impact Event Report."Capitalization throughout this table is inconsistent. Sometimes an event is all capitalized. Sometimes not. It is not in synch with the NERC Glossary. All terms that remain capitalized in the next draft (other than when used as a title or heading) should be defined in the Glossary of Terms Used in NERC Reliability Standards. Examples of inconsistencies: Unplanned Control Center evacuation, Loss of off-site power, Voltage Deviations.-Energy Emergency requiring a public appeal or a system-wide voltage reduction: All The NERC Glossary defines Energy Emergency as a condition when a LSE has exhausted all other options and can no longer provide its customers' expected energy requirements. The events should not be described as an Energy Emergency requiring public appeal or system-wide voltage reductions. If public appeal and system-wide voltage reductions are still an option then all options have not been exhausted, the LSE can still provide its customers' energy requirements, and it is not an Energy Emergency. We suggest using "Energy Emergency Alert" rather than "Energy Emergency."-Energy Emergency requiring firm load shedding: load shedding via automatic UFLS or UVLS would not necessarily be due to an Energy Emergency. Other events could cause frequency or voltage to trigger a load shed. Most likely an entity would be seeing the Energy Emergency coming and would be using manual load shedding. -Forced intrusion and detection of cyber intrusion to critical cyber assets: CIP-008 is not referrenced for a forced intrusion. CIP-008 is referenced for a detection of cyber intrusion impact event. Aren't there reportable events per CIP-008 that involve physical intrusion that are not intrusions at a BES facility?-Risk to BES equipment: The threshold states that it is for a non-environmental threat but the examples given are environmental threats. Please clarify.
Manitoba Hydro	Yes	Though R7 indicated Attachment 1 will be reviewed and revised reguarily the immediate addition of:"Detection of suspected or actual or acts or threats of physical sabotage"should be added.

Organization	Yes or No	Question 10 Comment
City of Austin dba Austin Energy	Yes	
Green Country Energy	Yes	
Idaho Power Company	Yes	
Pacific Gas and Electric Company	Yes	
PacifiCorp	Yes	
PNM Resources	Yes	
RRI Energy, Inc.	Yes	
TransAlta Corporation	Yes	

11. Do you agree with the use of the Preliminary Impact Event Report (Attachment 2)? Please explain in the comment box below.

Summary Consideration: Most commenters who responded to this question disagreed with some aspect of the Preliminary Impact Event Report. The proposed Preliminary Impact Event Report (Attachment 2) generated comments regarding the duplicative nature of the form when compared to the OE-417. The DSR SDT has added language to the proposed form to clarify that NERC will accept a DOE OE-417 form in lieu of Attachment 2 if the responsible entity is required to submit an OE-417 form.

In collaboration with the NERC Event Analysis Working Group (EAWG) the DSR SDT proposes to modify the attachment to eliminate confusion. This revised form will be used as Attachment 2 of the Standard and is the only required information for EOP-004-2 reporting. Further information may be requested through Events Analysis Process (NERC Rules of Procedure), but this information is outside of the scope of EOP-004.

The DSR SDT has also clarified what the form is to be used for with the following language added:

"This form is to be used to report impact events to the ERO."

Organization	Yes or No	Question 11 Comment
City of Austin dba Austin Energy		Austin Energy would like to see OE-417 incorporated into the electronic form This will reduce the callout of EOP-004-2 and OE-417 forms in our checklists / documents and one form can be submitted to NERC and DOE.
Independent Electricity System Operator		TBD
Ameren	No	It is unclear when this should be used, or why.

Organization	Yes or No	Question 11 Comment
ATC	No	No. NERC does not have the authority to absolve the Functional Entities of the reporting obligations for the DOE Form OE-417. Therefore, there will be duplicate reporting requirements and the one hour timeframes required in Attachment 1 will take valuable resources away from mitigating the event to filling out duplicative paperwork. It is ATC's position that the OE-417 report be used as the main reporting template until NERC and the DOE can develop a single reporting template. Task #14 in the report should be modified to say, "Identify any known protection system misoperation(s)." If this report is to be filed within 24 hrs, there will not be enough time to assess all operations to determine any misoperation. As a case in point, it typically takes at least 24 hrs to receive final lightning data; therefore, not all data is available to make a determination.
ATCO Electric Ltd.	No	Attachment 2 Item 4 implies that an entity is required to analyse and report on an impact event that occurred outside its system. This is not practical as the entity will not have access to the necessary information.
BGE	No	There is considerable difference between this form and OE-417 necessitating that two forms be completed. BGE believes that the purpose of combining the standards was to reduce the number of reporting entities and number of reports to be generated by each entity. BGE believes this fails to accomplish this purpose.
City of Garland	No	The report filed should be the OE-417 ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT and should be filed only on OE-417 reportable incidents. If this report is implemented as drafted, companies with multiple registration numbers and functions should only have to file one report for all functions and registrations.
Consolidated Edison Co. of NY, Inc.	No	It is not clear why the DOE form cannot be used. NERC should make every effort to minimize paper work for entities responding to system events.
Constellation Power Generation and Constellation Commodities Group	No	It is unclear if an entity has to answer all the questions. In addition, "Preliminary" is not currently included in the report title.
Electric Market Policy	No	There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
ERCOT ISO	No	ERCOT ISO requests the use of a single report format to meet all requirements from NERC and DOE. There is no value added in requiring different reporting to different agencies.

Organization	Yes or No	Question 11 Comment
Exelon	No	Exelon agrees with the use of the report but feels that # 5 should consist of check boxes. #12, 13, and 14 will take more time then allotted by the reporting requirements to acquire, cannot be accomplished in an hour.Attachment 2 should have a provision for the reporting entity to enter (N/A) based on function (see below)Check box #8 A GO/GOP may not have the information to determine what the frequency was prior to or immediately after an impact event. This information should be the responsibility of a TOP or RC.Check box #9A GO/GOP may not have the information to determine what transmission facilities tripped and locked out. This information should be the responsibility of a TO, TOP or RC.Check box #10A GO/GOP may not have the information to determine the number of affected customers or the demand lost (MW-Minutes). This information should be the responsibility of a TO, TOP, or RC.
Great River Energy	No	NERC and the DOE need to coordinate and decide on which report they want to use and whichever report it is needs to include all information required by both entities. The way this standard is currently written there is the potential that two government entities may need to be reported to is a relatively short period of time. It is not clear what benefit providing the Compliance Registration ID number provides. Many of the registered entities employees that will likely have to submit the report, particularly given the one-hour reporting requirement for some impact events, will not be aware of this registration ID. However, they will know for what functions they are registered. We recommend removing the need to enter this compliance registration ID or extending the time frame for reporting to allow back office personnel to complete the form. For item two, please change “Time/Zone:” with “Time (include time zone)”. As written it is a little confusing.
Idaho Power Company	No	there should only be on report, utilized OE-417
Indeck Energy Services	No	The form needs to identify whether it is a preliminary or final report. An identifier should be created to tie the final to the preliminary one. Some fields, 1,2 3 5 & 6, are required for the preliminary report and should be labeled as such. With the 1 hour reporting deadline for some events, the details may not be known. 12 & 13 should be required for the final report. 13 should designate whether the cause is preliminary or final. 7-11 & 14 are optional, and the form should state this, and based on some types of events. It's confusing to have irrelevant blanks on the form.
IRC Standards Review Committee	No	Attachment 2 is not referenced in the standard requirements. Is it a part of the standard that an entity must use to file the impact event reports to a specific recipient. If so, this needs to be referenced in the standard.We question the need for using a fixed format for reports that vary from “shedding firm load” to “damaging equipment”. The nature of impact events varies from one event to another and hence a fixed format or pre-determined form may not be able to provide the appropriate template that is suitable for use for

Organization	Yes or No	Question 11 Comment
		all events. We urge the SDT to reconsider the use of Attachment 2 for reporting events, with due consideration to the actual intent of the standard (as pointed out in our comments under Q1).
ISO New England Inc.	No	There is already a DOE requirement to report certain events. There is no need to develop redundant reporting requirements to NERC that cross other federal agency jurisdictions.The heading on page 16 refers to EOP-002, but this is Standard EOP-004. If some questions do not require an answer all of the time, then the form should state that or provide a NA checkbox. While Attachment 1 details some cyber thresholds, Attachment 2 provides no means to report - which is acceptable if cyber incidents are handled by CIP-008 per the comment provided for Question 10.The Event Report Template in Appendix A is different from the most recent version, which is available at: http://www.nerc.com/docs/eawg/Event_Analysis_Process_WORKINGDRAFT_100110-Clean.pdf
Kansas City Power & Light	No	For easier classification and analysis of events for both external reporting to the ERO and internal reporting for the applicable entity, the form should include Event Type. The DSR SDT should code each event type and include the codes as part of Attachment 1.
Manitoba Hydro	No	Though a “Confidential Impact Event Report” is much needed the Attachment 2 needs refinement.Provide an explanation for each “task”.Isolate and simplify the “Who, When and What” section.Isolate the description of event.Remove items 7 to 10. Modify Attachment 1, add columns to indicate time of event, quantity, restore time, etc as required. The Attachment 1 can be attached to Attachment 2. This could simply and speed the reporting process.
MidAmerican Energy	No	
Midwest ISO Standards Collaborators	No	This form differs from the DOE reporting forms. We do not believe different reporting forms should be required. The DOE form should be sufficient for NERC reporting.It is not clear what benefit providing the Compliance Registration ID number provides. Many of the registered entities employees that will likely have to submit the report, particularly given the one-hour reporting requirement for some impact events, will not be aware of this registration ID. However, they will know for what functions they are registered. We recommend removing the need to enter this compliance registration ID or extending the time frame for reporting to allow back office personnel to complete the form. For item two, please change “Time/Zone:” with “Time (include time zone)”. As written it is a little confusing.

Organization	Yes or No	Question 11 Comment
MRO's NERC Standards Review Subcommittee	No	Number 4 of the reporting form does not take into consideration of potential impact events. Recommend that "Did the impact event originate in your system?" to "Did the impact event originate or affect your system?". This will provide clarity to entities.
Nebraska Public Power District	No	If the standard requires submission of the report within an hour (which is not appropriate), there must be an abbreviated form that can be quickly filled out by checking boxes and not require substantial narrative. The existing form has too much free form text that takes time to enter and with the short timeframe for reporting will distract the entities responsible for real-time reliabiltiy of the BES from that task by forcing them to complete after the fact reports. It is unrealistic to expect entities to staff personnel to complete the reporting 24 x 7 for unlikely events, so the task will fall to System Operators who should be focusing on operating the BES at the time of these events instead of providing after the fact reporting to entities that do not have responsibility for real-time operation of the BES. Real-time reporting to the RC and/or BA is covered under other standards and is necessary for the RC to have situational awareness, but is not covered under this standard. The registered entities may report to the proper law enforcement entities when the situation warrants, but again this form is not the appropriate way to handle that reporting requirement.
NERC Staff	No	Item 15: A one-line diagram should be attached to assist in the understanding and evaluation of the event.Two additional items are recommended:--Ongoing reliability impacts/system vulnerability - this would capture areas where one is not able to meet operating reserves or is in an overload condition, below voltage limits, etc. in real-time--Reliability impacts with next contingency - this would capture potential impacts as outlined above with the next contingency.
North Carolina Electric Coops	No	There is already a DOE requirement to report certain events. NERC should not be developing redundant reporting requirements when this information is already available at the federal level from other agencies.
Northeast Power Coordinating Council	No	There is already a DOE requirement to report certain events. There is no need to develop redundant reporting requirements to NERC that cross other federal agency jurisdictions.The heading on page 16 refers to EOP-002, but this is Standard EOP-004. If some questions do not require an answer all of the time, then the form should state that or provide a NA checkbox. While Attachment 1 details some cyber thresholds, Attachment 2 provides no means to report - which is acceptable if cyber incidents are handled by CIP-008 per the comment provided for Question 10.The Event Report Template in Appendix A is different from the most recent version, which is available at: http://www.nerc.com/docs/eawg/Event_Analysis_Process_WORKINGDRAFT_100110-Clean.pdf

Organization	Yes or No	Question 11 Comment
Pacific Gas and Electric Company	No	PG&E believes the report is duplicative to the OE-417 reporting criteria.
Pacific Northwest Small Public Power Utility Comment Group	No	We found no “Preliminary Impact Event Report” in the posted draft standard, so we assume the question is regarding the “Confidential Impact Report” (Attachment 2). It is unclear what role the form plays, since no requirement refers to it. If this is the form to report impact events per R6, then R6 should reference it. The comment group cautions that the use of the word “confidential” should be carefully considered, since many filled out forms that originally contained the word are now posted on the NERC website for all to see. If there are limits to the extent and/or duration of the confidentiality this should be clearly stated in the form, or the word should be avoided.Protection System misoperation reporting is already covered by PRC-004. Including it here is redundant, and doubly jeopardizes an entity for the same event.
PacifiCorp	No	As previously mentioned all effort should be made to ensure duplicate reporting is not required. OE-417 requirements should be covered by this one form.
Pepco Holdings, Inc - Affiliates	No	The list of events misses many items considered as suspicious or potential sabotage, such as suspicious observation of critical facilities.
PNM Resources	No	PNM believes the report is duplicative to the OE-417 reporting criteria.
PSEG Companies	No	The top of this form should have the following statement added: "This form is not required if OE-417 is required to be filed."
Puget Sound Energy	No	Attachment 2 is not referenced in the requirements of the proposed standard. As a result, it is not clear when its submission would be required.
Santee Cooper	No	If the DOE form is going to continue to be required by DOE, then NERC should accept this form. Entities do not have time to fill out duplicate forms within the time limits allowed for an event. This is burdensome on an entity.
SERC OC Standards Review Group	No	There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.

Organization	Yes or No	Question 11 Comment
TransAlta Corporation	No	We recommend the 'time to Submit Report' to start when the event is recognized verses when it occurred.
United Illuminating	No	The standard does not appear to require the use of Attachment 2. Placing the form within the Standard may require the use of the Standards Development Process to modify the form. UI suggests the form is maintained outside the Standard to allow it to be adjusted. UI would prefer NERC to establish an internet based reporting tool to convey the initial reports.
US Bureau of Reclamation	No	There is already a reporting form for disturbances. The SDT should reconcile this standard with all the other reporting that is being requested and not add more.
We Energies	No	The data required to assess an impact event thoroughly will often not be available or apparent. Immediate reporting should fall to the RE with assistance/information from the affected entities.There do not seem to be provisions for when it is impossible to take the time to fill out a form or when it is impossible to send a form.I did not compare this standard to the OE-417 form. Please do not require operators to fill out a second form during an emergency within one hour.
WECC	No	The report is duplicative to the OE-417 reporting criteria.
Bonneville Power Administration	Yes	Item 8: list Hz minimum on the second line prior to Hz max since that is the typical frequency excursion order.The Operating Plan is going to have to include the Compliance Registration ID number, since Operating Personnel don't carry that information around and it is not readily available.
Duke Energy	Yes	However, Attachment 2 is titled "Impact Event Reporting Form".
E.ON Climate & Renewables	Yes	Suggestions on the form: if an entity has not had time to fully determine the cause of an Impact Event such as for "Question # 4: Did the impact event originate in your system, yes or no?", perhaps more time is needed that 24 hours to determine the cause.
FirstEnergy	Yes	Although we agree with the report, it should be clear that organizations with many registered entities can submit one report to cover multiple entities under one parent company.
Georgia System Operations	Yes	We support having one form for reporting however every applicable entity should not be required to fill it out and send it to NERC. See previous comments about hierarchical reporting.The title of the report is

Organization	Yes or No	Question 11 Comment
Corporation		"Confidential Impact Event Report." Some suggested modifications: The form could have a blank added to enter the event "description" as described in the first column of Attachment 1. The first seven lines contain information that would most likely be filled out every time. The other lines except line 13 may or may not be applicable every time. It is required (R3) for an entity to access the initial probable cause of all impact events so line 13 will most likely be filled out every time. Please move the probable cause line up to line 7 or 8 (depending on if the event description line is added).
PPL Electric Utilities	Yes	For ease, timeliness, and accuracy of reporting an application with an easy to use interface would be preferred. If the reporting is done via an application, the ability to enter partial data, save and add additional info prior to submission would be helpful. Additionally, an application with drop downs to select from for impact event, NERC function, etc would be helpful. #1 - Is the 'Compliance Registration ID number' the same as the NCR number? If this is required, include as separate entry. #2 - is this the date of occurrence or detection?
Arizona Public Service Company	Yes	
Dynegy Inc.	Yes	
Green Country Energy	Yes	
Luminant Energy	Yes	
PacifiCorp	Yes	
PPL Supply	Yes	

Organization	Yes or No	Question 11 Comment
RRI Energy, Inc.	Yes	
Southern Company - Transmission	Yes	

12. The DSR SDT has replaced the terms "disturbance" and "sabotage" with the term "impact events". Do you agree that the term "impact events" adequately replaces the terms "disturbance" and "sabotage" and addresses the FERC directive to "further define sabotage" in an equally efficient and effective manner? Please explain in the comment box below.

Summary Consideration: There was no consensus amongst commenters who responded to this question. Several commenters expressed concern that the definition should be added to the glossary. The DSR SDT has proposed a definition for "Impact Events" to support Attachment 1 as follows:

> "An Impact Event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action."

The DSR SDT has proposed this definition for inclusion in the NERC Glossary for "Impact Event". The types of Impact Events that are required to be reported are contained within Attachment 1. Only these events are required to be reported under this Standard.

Several commenters expressed concern that the team did not define 'Sabotage' and FERC directed that the modifications to this standard include a definition of sabotage. The DSR SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was that of sabotage or merely vandalism without the intervention of law enforcement after the fact. This will result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The Impact Events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

Some commenters were concerned that some of the events that require reporting that were specifically listed in the previous version of the standard are not included in the revised standard. Attachment 1, Part A is to be used for those actions that have impacted the electric system and in particular the section "Damage or destruction to equipment" clearly defines that all equipment that intentional or non intentional human error be reported. Attachment 1, Part B covers the similar items but the action has not fully occurred but may cause a risk to the electric system and is required to be reported.

Organization	Yes or No	Question 12 Comment
Bonneville Power Administration		The definition of an impact event in EOP-004-2 seems clear, however the term "mis-operation" still may imply intent in the action of an individual. The SDT should consider further defining that term.
Independent Electricity System Operator		We do not have a view on what name is assigned to the reportable events for so long they are listed in Attachment 1. However, the heading of the Table contains the words “Actual Reliability Impact”, which does not accurately reflect the content inside the table and which may introduce confusion with the term “impact event”. We suggest to change them to “Reportable Impact Events”.As we read the Summary of Concept and Assumption, there appears to be a slightly different lists at the bottom of P. 21. With these events included, the meaning of “impact event” would seem to be too broad. Rather than calling those events listed in Attachment 1 “impact events”, why not simply call them “reportable events”?
CenterPoint Energy	No	CenterPoint Energy does not agree that the term “impact event” adequately replaces “disturbances” and “sabotage”. CenterPoint Energy suggests that just as the SDT has come to consensus on a concept for impact event, a definition could be derived for sabotage. “Potential”, as used in the SDT’s concept, is a vague term and indicates an occurrence that hasn’t happened. Required reporting should be limited to actual events. CenterPoint Energy offers the following definition of “sabotage”: “An actual or attempted act that intentionally disrupts the reliable operation of the BES or results in damage to, destruction or misuse of BES facilities that result in large scale customer outages (i.e. 300MW or more).”
City of Garland	No	1 In keeping with a Results Based Standard, the impact event should be a trigger for filing a report. At the time of the event, one may not know if the event was caused by sabotage. Sabotage that does not affect the BES should not be a reportable event. 2. To comply with the Commissioners request to define sabotage, Impact Event does not adequately replace “sabotage”. If someone reports sabotage, people universally have a concept that someone(s) have taken some type of action to purposely harm, disable, cripple, etc something. Impact Event does not convey that same concept. 3. If Sabotage is left as a “trigger,” it should not include minor acts of vandalism but only acts that impact reliability of the BES
Consolidated Edison Co. of NY, Inc.	No	The definition is open for interpretation beyond events identified in Attachment 1. In addition, all Standards are supposed to have Rationales. In the Draft Standard, the Rationales do not address the concept of Potential, and how it relates to an actual system event. Additional work needs to be done addressing the

Organization	Yes or No	Question 12 Comment
		meaning of “potential”.
Duke Energy	No	We disagree with the stated concept of “impact event”. Including the phrase “or has the potential to significantly impact” in the concept makes it impossibly broad for practical application and compliance. By not attempting to define “sabotage”, the standard creates a broad reporting requirement. “Disturbance” is already adequately defined. “Sabotage” should be defined as “the malicious destruction of, or damage to assets of the electric industry, with the intention of disrupting or adversely affecting the reliability of the electric grid for the purposes of weakening the critical infrastructure of our nation.”
Dynegy Inc.	No	The term is fine but FERC wants more specific examples. GO/GOP can't determine the effect on the BES.
E.ON Climate & Renewables	No	Acts of Sabotage is still not defined and if the registered entities are required to reports acts of sabotage, NERC still needs to define this further.
ERCOT ISO	No	
Exelon	No	Need to better define sabotage and provide examples, the term “impact events” create confusions as to what constitutes an event. The definition of impact event is vague and needs to be quantified or qualified with a term such as “significant”. Otherwise, almost any event could be deemed to be an impact event. Attachment 1 needs to clearly define that damage or destruction of BES equipment does not include cyber sabotage. Events related to cyber sabotage are reported in accordance with CIP-008, "Cyber Security - Incident Reporting and Response Planning," and therefore any type of event that is cyber initiated should be removed from this Standard. In general, all impact events need to be as explicit as possible in threshold criteria to eliminate any interpretation on the part of a reporting entity. Ambiguity in what constitutes an "impact event" and what the definition of "occurrence" is will ultimately lead to confusion and differing interpretations.
FirstEnergy	No	For the most part we support this definition of impact events. However, we have the following suggestions:1. We believe that it warrants an official NERC glossary definition. 2. The term "potential" in the definition should point to the specific events detailed in Attachment 1 Part B.3. Since the standard does not cover environmental events, the phrase "environmental conditions" in the definition is not an impact event in the context of this standard.

Organization	Yes or No	Question 12 Comment
Great River Energy	No	We believe the SAR scope regarding addressing sabotage has not been addressed at all. It appears that impact event essentially replaces sabotage. This standard needs to make it clear that sabotage, in some cases, cannot be identified until an investigation is performed by the appropriate policing agencies such as the FBI. Intent plays an important role in determining sabotage and only these agencies are equipped to make these assessments.
Green Country Energy	No	Yes and no ... Yes impact events is an adequate term however since it is restrained by the tables it may be helpful to define the term and scope of the term to be more inclusive of sabotage events.
Indeck Energy Services	No	Impact Events is OK. It needs to be balloted as a definition for the Glossary like Protection System.
IRC Standards Review Committee	No	This term and the FERC directive do not recognize limitations in what a registered entity can do to determine whether an act of sabotage has been committed. This term should recognize law enforcement's and other specialized agencies', including international agencies', role in defining acts of sabotage and not hold the registered entity wholly responsible to do so.
ISO New England Inc.	No	The use of the term "impact events" has simply replaced the terms "disturbance" and "sabotage", and has not further defined sabotage as directed by FERC. We do feel that "impact events" needs to be a defined term. While we agree with the SDT's new direction, the FERC directive has not been met. This term and the FERC directive do not recognize limitations in what a registered entity can do to determine whether an act of sabotage has been committed. This term should recognize law enforcement and other specialized agencies, including international agencies roles in defining acts of sabotage, and not hold the registered entity wholly responsible to do so.
Luminant Energy	No	The term "Impact Event" does not adequately replace the term "Sabotage" The Impact Events table seems to provide the definition of the term "Impact Event". This table does not include sufficient definition for actual sabotage events. Additionally, it does not include any provision for suspected sabotage events. Assuming the Damage or Destruction of BES Equipment event type is intended to cover actual sabotage, the Threshold for Reporting column should include specific levels of materiality that are specific to Functional Entity. For instance, a GO and GOP could have a MW level to define materiality as a GO or GOP cannot assess impact to an IROL or system reliability margin due to equipment damage. A threshold value consistent with "Generation Loss" in the proposed EOP-004 Attachment 1 would be appropriate.
Manitoba Hydro	No	The majority of the items listed in Attachment 1 are typically and historically operating events. Yes these are all "impact events". Sabotage, cyber and security are typically viewed as separate events. These events are

Organization	Yes or No	Question 12 Comment
		not part of “a typical day of BES operations”. These are outside event and though qualify as “impact events” should still be treated separately.
Midwest ISO Standards Collaborators	No	We believe the SAR scope regarding addressing sabotage has not been addressed at all. It appears that impact event essentially replaces sabotage. This standard needs to make it clear that sabotage, in some cases, cannot be identified until an investigation is performed by the appropriate policing agencies such as the FBI. Intent plays an important role in determining sabotage and only these agencies are equipped to make these assessments.
NERC Staff	No	NERC staff is concerned with the ambiguity of the term “impact event.” The definition of the term is not clear, in part because it includes using the words “impact” and “event” (and thus violates the frowned-up practice of using a word to define the word itself). NERC staff recommends the SDT consider using the term “Event.” The following definition (modified from the one used the INPO Human Performance Fundamentals Desk Reference, P. 11) would apply: Event: “An unwanted, undesirable change in the state of plants, systems or components that leads to undesirable consequences to the safe and reliable operation of the Bulk Electric System. ”Supporting statement following the definition: “An event is often driven by deficiencies in barriers and defenses, latent organizational weaknesses and conditions, errors in human performance and factors, and equipment design or maintenance issues.” Further, if this is intended for use in this standard, it should be presented as an addition to Glossary to avoid confusion with the use of the term event in other standards. Of course, this would require an analysis of how the term “Event” as defined herein would affect the other standards to which the term is used. In the end, this is the cleanest manner for the standards.
Northeast Power Coordinating Council	No	The use of the term “impact events” has simply replaced the terms “disturbance” and “sabotage”, and has not further defined sabotage as directed by FERC. We do feel that “impact events” needs to be a defined term.While we agree with the SDT’s new direction, the FERC directive has not been met.This term and the FERC directive do not recognize limitations in what a registered entity can do to determine whether an act of sabotage has been committed. This term should recognize law enforcement and other specialized agencies, including international agencies roles in defining acts of sabotage, and not hold the registered entity wholly responsible to do so.
Pacific Gas and Electric Company	No	PG&E believes Attachment 1 Part A or B do not clearing specify “sabotage” events, other than “forced entry” and the proposed definition of “impact event” does not meet FERC’s directive to “further define sabotage” nor does it take into consideration their request to address the applicability to smaller entities.
Pacific Northwest Small Public	No	The comment group fails to see how changing the words meet the directive. Sabotage implies an organized

Organization	Yes or No	Question 12 Comment
Power Utility Comment Group		intentional attack that may or may not result in an electrical disturbance. The distinction between sabotage and vandalism is important since sabotage on a small system may be the first wave of an attack on many entities. The proposed standard asks us to treat insulator damage caused by a frustrated hunter (an act of vandalism) the same as attack by an unfriendly foreign government (an act of sabotage). The comment group does not agree that these should be treated equally.
Pepco Holdings, Inc - Affiliates	No	The list of events misses many items considered as suspicious or potential sabotage, such as suspicious observation of critical facilities.
PNM Resources	No	PNM believes the proposed definition of “impact event” does not meet FERC’s directive to “further define sabotage” nor does it take into consideration their request to address the applicability to smaller entities. Attachment 1 Part A or B do not clearing specify “sabotage” events, other than “forced entry”.
Puget Sound Energy	No	With some of the tight timeframes for reporting, it is reasonable to focus on impact rather than motivation. Requiring further analysis of the event in order to assess the possibility that the event was caused by sabotage, however, may be necessary to address FERC’s concerns with respect to sabotage.
Santee Cooper	No	The term "impact events" needs to be more clearly defined.
US Bureau of Reclamation	No	The two are distinctly different. Disturbances are what happened, sabotage is why. We can easily tell what happened. Determining why it happened (e.g. sabotage) takes time.
We Energies	No	Impact Event could replace disturbance and sabotage but not in its present form. The proposed definition of impact event “An impact event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action.” Is too vague. The “potential to impact the reliability” is too broad and open to interpretation. It needs to be specific so entities know what is and is not an impact event and so an auditor clearly knows what it is. Define “impact event” as the items listed in Attachment 1.As you have done, focusing on an event’s impact on reliability is more important than determining an individuals intent (sabotage v.s. theft).
WECC	No	The proposed definition of “impact event” does not meet FERC’s directive to “further define sabotage” nor does it take into consideration their request to address the applicability to smaller entities. Attachment 1 Part A or B do not clearing specify “sabotage” events, other than “forced entry”. The purpose of CIP-001-1 and its requirements is to address the specific issue of possible sabotage of BES facilities. This is entirely different

Organization	Yes or No	Question 12 Comment
		than a “disturbance” or an “event” on the BES. The proposed definition for “impact events” is essentially any event that has either impacted the BES or has the potential to impact the BES, caused only by three specific things; equipment failure or misoperation, environmental conditions, or human action. Several of these “impact events could be a result of sabotage. Actual or potential sabotage clearly poses a risk to the reliability of the BES. It is important that the risks related to sabotage be reflected in either EOP or CIP
Ameren	Yes	However, the term Impact Event should be a new defined term. When the SDT determines this, it should use the term consistently on both pages 5 and 21 of the SDT document.
ATC	Yes	Yes, if ATC’s recommended changes are made to Attachment 1 and the Standard.
BGE	Yes	The defined term “impact events” should be capitalized throughout the document to identify it as a defined term. Additionally, BGE has noted in several comments that another term is used instead of “impact events”. These terms should be eliminated and use “impact events” instead.
Electric Market Policy	Yes	The use of the term “impact events’ has simply replaced the terms “disturbance” and “sabotage” and has not further defined sabotage as directed by FERC. We do feel that impact events needs to be a defined term.
Georgia System Operations Corporation	Yes	The new term is much more clear than those two terms. This will improve uncertainty and confusion regarding whether or not something should be reported.
Kansas City Power & Light	Yes	Should the word disturbance be removed from the title of EOP004-2 to avoid confusion and simply be called Impact Event and Assessment, Analysis and Reporting.
MRO's NERC Standards Review Subcommittee	Yes	As an industry we have looked at sabotage as a sub component of a disturbance. Sabotage is hard to measure since it is based on a perpetrator’s intent and thus very hard to determine.
Nebraska Public Power District	Yes	I agree there is a lot of interpretation and confusion as to what sabotage or a Cyber Incident is, so would welcome better clarity. Whether “impact events” can more effectively clarify, is yet to be seen. “it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.” “An impact event is any situation that has the potential to significantly impact the reliability of the Bulk Electric System. Such events may originate from malicious intent, accidental behavior, or natural occurrences.” I do know that Cyber Sabotage may take time or days to become aware so not sure

Organization	Yes or No	Question 12 Comment
		how that might expedite reporting and awareness.
PPL Electric Utilities	Yes	Refer to clarification requested in question 10 comments.
RRI Energy, Inc.	Yes	Agree. However, strongly encourage this to be made into a defined term in the Glossary of Terms.
SERC OC Standards Review Group	Yes	We do feel that this needs to be a defined term
United Illuminating	Yes	The term impact event can substitute for sabotage and disturbance. The use of Forced Intrusion is a bright line for reporting.
American Electric Power (AEP)	Yes	
Arizona Public Service Company	Yes	
ATCO Electric Ltd.	Yes	
City of Austin dba Austin Energy	Yes	
Constellation Power Generation and Constellation Commodities Group	Yes	
Idaho Power Company	Yes	

Organization	Yes or No	Question 12 Comment
MidAmerican Energy	Yes	
North Carolina Electric Coops	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	
PPL Supply	Yes	
Southern Company - Transmission	Yes	
TransAlta Corporation	Yes	

13. The DSR SDT has combined EOP-004 and CIP-001 into one standard (please review the mapping document that shows the translation of requirements from the already approved versions of CIP-001 and EOP-004 to the proposed EOP-004), EOP-004-3 and retiring CIP-001. Do you agree that there is no reliability gap between the existing standards and the proposed standard? Please explain in the comment box below.

Summary Consideration: While a majority of commenters who responded to this question support combining the two standards, some commenters suggested that in combining the standards, the team left some gaps in coverage with respect to the types of events that must be reported. The DSR SDT believes that combining EOP-004 and CIP-001 does not introduce a reliability gap between the existing standards and the proposed standard and the industry comments received confirms this. Some events that were specifically identified in the original standard (such as a bomb threat) are covered more generically in the revised standard. This modification encourages entities to focus on the 'types' of events that may be impactive rather than having a finite list that may omit an event that couldn't be anticipated when drafting the requirements.

The decision to eliminate the term sabotage from the standard and the retirement of CIP-001 should alleviate all concerns regarding the term sabotage and its definition. The DSR SDT believes that "observation of suspicious activity" and "bomb threat" is considered to be included in Part B – "Risk to BES equipment from a non-environmental physical threat". We have added "and report of suspicious device near BES equipment" to note 3 of the "Attachment 1, Potential Reliability – Part B".

Organization	Yes or No	Question 13 Comment
WECC		A potential gap may exist. Attacks on BES facilities, via either vandalism or sabotage, are very different events than impact events on the system. From a Compliance standpoint, a revised standard to address the FERC directive on sabotage should be developed as an EOP standard (that is grouped with 693 Standards) rather than as a CIP Standard (CIP-001-1).
Ameren	No	It appears that all requirements have been addressed from the existing standards. However, we believe there is a reliability gap that continues from the existing standards because sabotage is not defined any better than

Organization	Yes or No	Question 13 Comment
		in the existing standards.
Bonneville Power Administration	No	BPA supports the concept behind the revisions to EOP-004-2. Creating a single reporting methodology will improve the processes and lead to more consistency. BPA recommends that the Standards Drafting Team (SDT) coordinate any revisions in the reporting requirements with those found in CIP-008-3 to ensure that there are no conflicts. BPA asks the SDT to consider the impact of these changes on CIP-008-3 and work with the CIP SDT to ensure that the wording of the two requirements is similar and clear. Based on Attachment 1 part A of EOP-004-2, certain cyber security events, intrusions for example, would have to be reported under both EOP-004-2 and CIP-008-3. That puts a burden on a Registered Entity to take additional steps to coordinate reporting or face potential compliance risk for correctly reporting an event under one standard and failing to report it under the other standard. The mapping document had errors: a. CIP-001 R1 to EOP-004 R2.9 (annual vs quarterly). b. EOP-004-1 R2 was translated to R2 & R3 of version 2. c. EOP-004-1 R3 was translated to R6 of version 2 (which doesn't say to whom to report).
City of Garland	No	EOP-004-1 R2 did not get translated to EOP-004-2 R2 - table states it is mapped to R1
E.ON U.S. LLC	No	The Version History contained with EOP-004-2 indicates that CIP-001-1 and EOP-004-1 are "Merged", however, the actions do not reflect the retirement of CIP-001-1a and therefore, it is unclear if there will be remaining redundancies or potential gaps with the new version EOP-004-2 and CIP-001-1a.
Electric Market Policy	No	Per the mapping document, some of the existing requirements are awaiting a new reporting procedure being developed by NERC EAWG. For those requirements that were transferred over, the resulting standard seems overly complex and lacks clarity.
Exelon	No	Reporting form doesn't allow for investigations which result in no impact events found or identified.
Georgia Transmission Corporation	No	The only two events that apply to a TO are the ones related to CIP:1. Forced intrusion (report if motivation cannot be determined, i.e. to steal copper)2. Detection of a cyber intrusion to critical cyber assets (criteria of CIP-008)Everything in this standard applies to a TOP and therefore E-004-2 and CIP-001 should not be combined

Organization	Yes or No	Question 13 Comment
Great River Energy	No	It appears that all requirements have been addressed from the existing standards. However, we believe there is a reliability gap that continues from the existing standards because sabotage is not defined any better than in the existing standards.
Indeck Energy Services	No	Bomb threat has totally been lost.
Independent Electricity System Operator	No	We do not agree with the mapping. The proposed mapping attempts to merge the reporting in CIP-001-1 which has more of an on-going awareness nature to alert operating and government authorities of suspected sabotage to prompt investigation with a possible aim to identify the cause and develop remedies to curb the sabotage/events. The proposed EOP-004-2 appears to be more of a post-event reporting for need-to-know purpose only. This is not consistent with the purpose of the SAR.
ISO New England Inc.	No	Per the mapping document, some of the existing requirements are awaiting a new reporting procedure being developed by the NERC EAWG. For those requirements that were transferred over, the resulting standard seems overly complex and lacks clarity. EOP-004-3 should be EOP-004-2.
Luminant Energy	No	CIP-001-1 R3.1 includes instructions associated with the DOE OE-417 form. EOP-004-2 R2.6 should include the DOE as an example of an external organization requiring notification. Additionally, the Rationale for R1 discusses the possibility of one electronic form satisfying US entities with related disturbance reporting requirements but does not include any information about the likelihood of this outcome. Please elaborate on the process required to combine these reports.
Midwest ISO Standards Collaborators	No	It appears that all requirements have been addressed from the existing standards. However, we believe there is a reliability gap that continues from the existing standards because sabotage is not defined any better than in the existing standards.
North Carolina Electric Coops	No	
Northeast Power Coordinating Council	No	Per the mapping document, some of the existing requirements are awaiting a new reporting procedure being developed by the NERC EAWG. For those requirements that were transferred over, the resulting standard seems overly complex and lacks clarity. EOP-004-3 should be EOP-004-2.

Organization	Yes or No	Question 13 Comment
Pepco Holdings, Inc - Affiliates	No	The list of events misses many items considered as suspicious or potential sabotage, such as suspicious observation of critical facilities.
Santee Cooper	No	It is very difficult to assess this question with the standard as currently written.
SERC OC Standards Review Group	No	
US Bureau of Reclamation	No	The two could be combined with no reliability gap based on the concept rather than the proposed standard. As the standard is currently written, there is a reliability gap. Consider that after the fact reporting of a sabotage event (other than criminal acts which may have been witnessed) usually take some time to investigate and analyze.
ATC	Yes	ATC agrees with this effort and does not currently see a reliability gap
BGE	Yes	None.
CenterPoint Energy	Yes	CenterPoint Energy agrees that there is no reliability gap between the existing standards and the proposed standard. However, CenterPoint Energy believes that the SDT went too far in developing the proposed EOP-004-2 and added additional unnecessary requirements. If the comments made above to Q1 - Q12 were to be incorporated into the proposed Standard, CenterPoint Energy believes the product would be closer to a results based Standard with no reliability gap.
City of Austin dba Austin Energy	Yes	If we can used OE 417 for NERC and DOE we do not perceive a reliability gap.
Georgia System Operations Corporation	Yes	The new single standard will cover all necessary reporting requirements that are in the current two standards. They are being combined into EOP-004-2 not EOP-004-3.

Organization	Yes or No	Question 13 Comment
Green Country Energy	Yes	With the provision that definition and scope of "impact event" are developed and tables adjusted as needed to address FERCs concerns specifically ."(1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."
MRO's NERC Standards Review Subcommittee	Yes	Within the above question, the SDT is asking about EOP-004-2 not -3.
Nebraska Public Power District	Yes	Appears they only changed R1 for CIP-001 and moving R2-R4 directly over to EOP-004-2. R1 adds much more detail on our part for a company operating plan but would definitely help some of the present confusion.
RRI Energy, Inc.	Yes	Assume reference to EOP-004-3 in the question 13 was meant to reference version 2 (EOP-004-2).
American Electric Power (AEP)	Yes	
Arizona Public Service Company	Yes	
ATCO Electric Ltd.	Yes	
Consolidated Edison Co. of NY, Inc.	Yes	
Constellation Power Generation and Constellation Commodities Group	Yes	
Duke Energy	Yes	
Dynegy Inc.	Yes	
ERCOT ISO	Yes	
FirstEnergy	Yes	

Organization	Yes or No	Question 13 Comment
Idaho Power Company	Yes	
Kansas City Power & Light	Yes	
MidAmerican Energy	Yes	
NERC Staff	Yes	
Pacific Gas and Electric Company	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	
PNM Resources	Yes	
PPL Electric Utilities	Yes	
PPL Supply	Yes	
Puget Sound Energy	Yes	
Southern Company - Transmission	Yes	
TransAlta Corporation	Yes	
United Illuminating	Yes	
We Energies	Yes	

14. Do you agree with the proposed effective dates? Please explain in the comment box below.

Summary Consideration: While most stakeholders who responded to this question supported the 12 months originally proposed for entities to become compliant, the drafting team has revised this to 6 months. The DSR SDT feels that six months and not more than nine months is an adequate time frame. The current CIP-001 plan is adequate for the new EOP-004 and training should be met in the proposed timeline.

The Implementation Plan was developed for the revised Requirements, which do not include an electronic "one-stop shopping" tool. This topic is to be addressed in the proposed revisions to the NERC Rules of Procedure.

Organization	Yes or No	Question 14 Comment
Independent Electricity System Operator		We do not agree with the proposed standard. We therefore are unable to agree on any implementation plan.
City of Garland	No	Do not agree with this proposed draft - instead of combining 2 standards to gain efficiency, this expands the standard with unnecessary paperwork, drills, training, etc.
Constellation Power Generation and Constellation Commodities Group	No	Based on the drastic differences between the previous revisions to these standards, and this proposed revision, 24 months would be a more reasonable timeframe for an effective date.
IRC Standards Review Committee	No	If the training and Operation Plan requirements are adopted as proposed, this may not be sufficient time for some entities to comply, particularly those with limited number of staff but perform functions that have multiple event reporting requirements.
ISO New England Inc.	No	If the training and Operation Plan requirements are adopted as proposed, this may not allow sufficient time for some entities to comply, particularly those with limited number of staff, but perform functions that have multiple event reporting requirements.
Kansas City Power & Light	No	April 2011 is too soon for considerations applicable to the creation of an Operating Plan.

Organization	Yes or No	Question 14 Comment
Manitoba Hydro	No	Though CIP-001-1a already contained provisions for sabotage response guidelines, the new EOP-004-2 R2 (2.1 to 2.9) will require reexamination of existing policies to remain compliant. Upon the approval of Attachment 1, the existing disturbance guidelines will also have to be reexamined. With the addition of R3 (Identify and assess), R4 (Drills) and R5 (Training), will also require redevelopment of existing processes.
NERC Staff	No	In order to provide explicit dates, the language should be modified to state: "First calendar day of the first calendar quarter one year after the date of the order providing applicable regulatory authority approval for all requirements."
Northeast Power Coordinating Council	No	The effective dates in Canada need to be defined. The first bullet should be sufficient. If the training and Operation Plan requirements are adopted as proposed, this may not allow sufficient time for some entities to comply, particularly those with limited number of staff, but perform functions that have multiple event reporting requirements.
Puget Sound Energy	No	There are no effective dates listed in the proposed standard. The proposed effective date should allow at least one year for entities to implement the requirements of the standard. In addition, if requirement R1 remains, then the requirement to implement an operating plan should only be triggered by the ERO's finalization of the form and system for reporting impact events and should provide at least six months for the implementation of the operating plan.
Santee Cooper	No	With the proposed training and drill requirements in the current written standard, one year is not enough time.
United Illuminating	No	UI believes the implementation should be staged. For R1 and R2: First calendar day of the first calendar quarter one year after applicable regulatory authority approval for all. This provides sufficient time to draft a procedure Then time needs to be provided to provide training prior to implementation of R3 and R6. UI believes two calendar quarters should be provided to complete training; therefore R3and R6 is effective six calendar quarters following regulatory approval. Implementation for R4 should state that the initial calendar year begins on the date R2 is effective and entities have 12 months following that date to complete their first drill. R5 requires training once per calendar year. Implementation for R5 should state that the initial calendar year begins on the date R2 is effective and entities have 12 months following that date to complete their first drill.

Organization	Yes or No	Question 14 Comment
US Bureau of Reclamation	No	There is a 15 month training requirement. If the standard goes into effect in one year, most entities will not have had an opportunity to develop their new Operating Plans and train their staff. The effective date should recognize Operating Plans need to be revised and then training needs to be implemented. The most aggressive schedule is 18 months. Two years would be more appropriate. The implementation date could recognize the Operating Plan development as one phase and the training as the second.
ATC	Yes	Yes, if ATC's recommended changes are made to the Standard. However, if the changes are not supported then ATC recommends that the implantation time be changed to two years. Entities will need time to develop both the plan called for in this standard and to train the personnel identified in the plan.
BGE	Yes	None.
Exelon	Yes	Agree with the proposed implementation date. A 12 month implementation will provide adequate time to generate, implement and provide any necessary training by a registered entity.
Ameren	Yes	
Arizona Public Service Company	Yes	
ATCO Electric Ltd.	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Co. of NY, Inc.	Yes	
Duke Energy	Yes	
Dynegy Inc.	Yes	
E.ON Climate & Renewables	Yes	
Electric Market Policy	Yes	

Organization	Yes or No	Question 14 Comment
ERCOT ISO	Yes	
FirstEnergy	Yes	
Georgia System Operations Corporation	Yes	
Great River Energy	Yes	
Green Country Energy	Yes	
Idaho Power Company	Yes	
Indeck Energy Services	Yes	
Luminant Energy	Yes	
MidAmerican Energy	Yes	
Midwest ISO Standards Collaborators	Yes	
MRO's NERC Standards Review Subcommittee	Yes	
North Carolina Electric Coops	Yes	
Pacific Gas and Electric Company	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	

Organization	Yes or No	Question 14 Comment
Pepco Holdings, Inc - Affiliates	Yes	
PNM Resources	Yes	
PPL Electric Utilities	Yes	
PPL Supply	Yes	
RRI Energy, Inc.	Yes	
SERC OC Standards Review Group	Yes	
Southern Company - Transmission	Yes	
TransAlta Corporation	Yes	
We Energies	Yes	
WECC	Yes	

15. Do you have any other comments that you have not identified above?

Summary Consideration: The DSR SDT has met with the EAWG and has put in place a process to ensure the cooperation and coordination between the DSR SDT and the EAWG. The impact event list is comprehensive and addresses the needs of the EAWG and EOP-004.

There were concerns expressed that the impact event list should include deliberate acts against infrastructure. The impact list includes "Risk to BES equipment from a non-environmental physical threat" the DSR SDT feels that this is inclusive of deliberate acts against infrastructure.

During discussions around the use and definition of the term sabotage, the DSR SDT considered the NRC definition and decided to eliminate the use of the term sabotage from EOP-004 and replaced it with impact events. The DSR SDT has developed a definition for "Impact Events" to support Attachment 1 as follows:

> "An Impact Event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action."

The DSR SDT has proposed this definition for inclusion in the NERC Glossary for "Impact Event". The types of Impact Events that are required to be reported are contained within Attachment 1. Only these events are required to be reported under this Standard. The DSR SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was that of sabotage or merely vandalism without the intervention of law enforcement after the fact. This will result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The Impact Events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive. Attachment 1, Part A is to be used for those actions that have impacted the electric system and in particular the section "Damage or destruction to equipment" clearly defines that all equipment that intentional or non intentional human error be reported. Attachment 1, Part B

covers the similar items but the action has not fully occurred but may cause a risk to the electric system and is required to be reported.

The industry commented on the need for e-mail addresses and fax numbers for back up purposes. These details were added to the standard and will also be covered in the implementation plan.

The proposed ballot in December was incorrect and has been deleted from the future development plan. The plan was updated with the correct project plan dates.

Organization	Yes or No	Question 15 Comment
Indeck Energy Services		Good start on a unified event reporting standard!
IRC Standards Review Committee	No	The standards should be changed to define what a “disturbance” is for reporting in EOP-004. Also, sabotage reporting requirements in CIP-001 should be rescinded as EOP-004 already has such requirements.
PSEG Companies		
Arizona Public Service Company	No	
ATCO Electric Ltd.	No	
Duke Energy	No	
Electric Market Policy	No	
FirstEnergy	No	
Independent Electricity System Operator	No	
Luminant Energy	No	

Organization	Yes or No	Question 15 Comment
Manitoba Hydro	No	
PacifiCorp	No	
PPL Supply	No	
RRI Energy, Inc.	No	
United Illuminating	No	
Ameren	Yes	We are concerned with the Future Development Plan. It shows an initial ballot period starting in December. This standard has significant issues and will need another distinct comment period (and not the formal comment period in parallel with balloting) prior to balloting.
American Electric Power (AEP)	Yes	The standard needs to be modified to allow the ability for one entity to report on behalf of other entities. For example the loss of Generation over the threshold could be reported by the RC opposed to the GO individually, if mutually agreed upon before the fact.
ATC	Yes	ATC believes that it is not evident in this draft that the SDT has worked collaboratively with the Events Analysis working group to leverage their work. ATC believes that NERC must coordinate this project and the EAWG efforts. The EAWG is proposing to modify NERC Rules of Procedure but the SDT is suggesting requirement for the ERO be build within the standard. We believe that the Rules of Procedure is the proper course to take to for identifying NERC obligations, but what is clear is that NERC itself does not seem to have an overall plan for event reporting and analysis. Lastly, ATC would like to see the SDT expand the mapping document to include the work of the EAWG. The industry needs to be presented with a clear picture as to how all these things will work together along with their reporting obligations. The definition of an “impact event” needs to be revised. First, if these events are to include any equipment failure or mis-operation that impacts the BES, the standard is requiring more than is intended based upon the reading of the requirements. PRC-004 already covers the reporting of protection system mis-operations, and if reading this definition verbatim, it would lead one to conclude that those same mis-operations reported under PRC-004 shall also be reported under EOP-004. The definition should be revised to something like: “An impact event is a system disturbance affecting the Bulk Electric System beyond loss of a single element under normal operating conditions and does not include events normally reported under PRC-004. Such events may be caused by...”

Organization	Yes or No	Question 15 Comment
BGE	Yes	One item that is properly addressed is the removal of Load Serving Entity from the Applicable Functional Entities. There may be a need to provide some guidance to Functional Entities when there are separate Transmission Owners and Transmission Operators or Generation Owners and Generation Operators. If they are separate, there may be redundancy in reporting.From the documentation, it doesn't seem like the SDT are combining all reports into one form as we would like to see. In the rational for R1 section, it talks of getting both forms (NERC and OE-417) together in one document (however it sounds like the forms within the document are still separate), available electronically, which only seems like a step forward. However, it does not take away the confusing process for the operators of which part of the form would need to be filled, who should be set this form depending on what part is filled, if one part of the form is filled out do the other parts need to be filled, etc. If the forms cannot be consolidated, BGE would rather the forms be separate to reduce confusion.BGE believes all these reports should require one form with one set of recipients, period.This may mean that NERC needs to get DOE to modify their OE-417 form.
Bonneville Power Administration	Yes	The document retention times in EOP-004-3 should be spelled out more clearly. The Compliance summary does so (but needs some punctuation clarification regarding investigation), the SDT should consider making that part of the requirements or clarifying the wording in the requirements.
CenterPoint Energy	Yes	CenterPoint Energy appreciates the efforts of the SDT in removing outdated and unnecessary language from the existing EOP-004 standard. Additionally, CenterPoint Energy urges the SDT to also remove the proposed "how to" prescriptive requirements. CenterPoint Energy believes the SDT team's focus should be on drafting a results-based standard for reporting actual system disturbances and acts of sabotage that disrupt the reliable operation of the BES. The SDT should not delve into trying to identify a list of events that have a potential reliability impact.As stated in response to Q10, CenterPoint Energy strongly believes that cyber-related events should not be in the scope of this standard since they are already required to be identified and reported to appropriate entities under CIP-008. Excluding cyber events from this standard further supports the elimination of redundancies within the body of standards.
City of Garland	Yes	Do not agree with this proposed draft - instead of combining 2 standards to gain efficiency, this expands the standard with unnecessary paperwork, drills, training, etc.For reports required under this standard, companies with multiple registration numbers and functions should only have to file one report for all functions and registrations.
Consolidated Edison Co. of NY, Inc.	Yes	Overriding Comment and Concern: It is absolutely essential that the work on EOP-004 and that on the NERC Event Analysis Process (EAP) be fully coordinated. We find that there are a number of inconsistencies between these two documents. The EAP and EOP-004 are not aligned. In order to operate and report

Organization	Yes or No	Question 15 Comment
		effectively entities need consistent requirements.
Constellation Power Generation and Constellation Commodities Group	Yes	As stated earlier, the "summary of concepts" for this latest revision, as written by the SDT, includes the following items: o A single form to report disturbances and impact events that threaten the reliability of the bulk electric system o Other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements o Clear criteria for reporting o Consistent reporting timelines o Clarity around of who will receive the information and how it will be used. Each and every requirement should be mapped to one of these 5 items; otherwise, it should not be included in this standard. Summarizing all of the comments above, Constellation Power Generation proposes the following revision to EOP-004-2:1. Title: Impact Event and Disturbance Assessment, Analysis, and Reporting 2. Number: EOP-004-2 3. Purpose: Responsible Entities shall report impact events and their known causes to support situational awareness and the reliability of the Bulk Electric System (BES). 4. Applicability 4.1. Functional Entities:4.1.1. Reliability Coordinator 4.1.2. Balancing Authority 4.1.3. Transmission Operator 4.1.4. Generator Operator 4.1.5. Distribution Provider 4.1.6. Electric Reliability Organization. Requirements and Measures R1. The ERO shall establish, maintain and utilize a system for receiving and distributing impact event reports, received pursuant to Requirement R6, to applicable government, provincial or law enforcement agencies and Registered Entities to enhance and support situational awareness.R2. Each Applicable Entity identified in Attachment 1 shall have an Operating Plan(s) for identifying, assessing and reporting impact events listed in Attachment 1 that includes the following components: 2.1. Method(s) for identifying impact events listed in Attachment 2.2. Method(s) for assessing cause(s) of impact events listed in Attachment 12.3. Method(s) for making internal and external notifications should an impact event listed in Attachment 1 occur. 2.4. Method(s) for updating the Operating Plan.2.5 Method(s) for making operation personnel aware of changes to the Operating Plan.R3. Each Applicable Entity shall implement their Operating Plan(s) to identify and assess cause of impact events listed in Attachment 1.R4. Each Applicable Entity shall provide training to all operation personnel at least annually.R5. Each Applicable Entity shall report impact events in accordance with its Operating Plan created pursuant to Requirement 2 and the timelines outlined in Attachment 1.
Dynegy Inc.	Yes	This does not address the inability of a GO/GOP to determine effects on the BES. Surrounding BES knowledge is limited for a GO/GOP.
E.ON Climate & Renewables	Yes	Refrain from having redundant reporting forms if at all possible. This can create confusion and lead to unnecessary penalty amounts and violations for registered entities. Potential" impacts of an event on the BES need to be clearly defined in the standard.
E.ON U.S. LLC	Yes	The new standard should incorporate all other disturbance, sabotage, or "impact event" reporting standards, such as CIP-008-3. At the very least it should reference those other standards that have within their scope

Organization	Yes or No	Question 15 Comment
		same/similar events in order to ensure complete reporting and full compliance. Suggesting that one standard provides the single reporting procedure, when in actuality it does not, is counterproductive. The discussion of "impact event" clearly indicates the SDT's intent to include sabotage events in the proposed standard EOP-004-2.
ERCOT ISO	Yes	ERCOT ISO supports the comments provided by the SRC. However, if the standard is to be established, ERCOT ISO has offered the comments contained herein as improvements to the requirements proposed. The requirements listed do not take into consideration the hierarchical reporting necessary for events (i.e.: GO to GOP to BA). The current structure will lead to redundant and conflicting reporting from multiple entities. This will lead to confusion in the analysis of the event. Any system developed and used to report impact events must include notification to the other relevant entities (i.e.: Reliability Coordinator, Balancing Authority, Transmission Operator, and Generator Operator). The proposed standard should not rely on a centralized system that does not follow the established hierarchy of dissemination of information.
Exelon	Yes	The standard is lacking guidance for DOE Form OE-417 reporting as outlined in the current version of EOP-004 and doesn't contain any non-BES related reporting. What is the governing process for OE-417 reporting?. Need clarification if one entity can respond on behalf to all entities in one company. Need a provision for entities to provide one report for all entities. Radiological sabotage is a defined term within the NRC glossary of terms. It would seem that a deliberate act directed towards a plant would also constitute an "impact event." In general, the DSR SDT should include discussions with the NRC to ensure communications are coordinated or consider utilizing existing reporting requirements currently required by the NRC for each nuclear generator operator for consistency. The definition of sabotage is defined by NRC is as follows: Any deliberate act directed against a plant or transport in which an activity licensed pursuant to 10 CFR Part 73 of NRC's regulations is conducted or against a component of such a plant or transport that could directly or indirectly endanger the public health and safety by exposure to radiation.
Georgia System Operations Corporation	Yes	Light years better than the current CIP-001-1 and EOP-004-1! With some changes from this comment period, we should have a clearer set of realistic requirements which could likely pass the ballot. Thanks go out to the drafting team for bringing clarity to this topic. Capitalization throughout this document is inconsistent. It is not in synch with the NERC Glossary. All terms that remain capitalized in the next draft (other than when used as a title or heading) should be defined in the Glossary of Terms Used in NERC Reliability Standards. Examples of not in synch with the Glossary: Registered Entity, Responsible Entity, Law Enforcement. These are not defined in the Glossary. The requirements that apply to entities should not use the word "analysis." "Assessment" should be used. Analysis is a different process (an ERO process) and is being addressed by

Organization	Yes or No	Question 15 Comment
		another group within NERC (Dave Nevius). This EOP-004 drafting team and the NERC analysis group should closely coordinate such that there are no conflicts and the combined requirements/processes are realistic (mainly regarding timelines).
Great River Energy	Yes	We are concerned with the Future Development Plan. It shows an initial ballot period starting in December. This standard has significant issues and will need another distinct comment period (and not the formal comment period in parallel with balloting) prior to balloting. Please provide an e-mail address for the submittal of the report to NERC (and any other parties above a Regional Entity) within this Standard and a fax number as a backup to electronic submittal.
Green Country Energy	Yes	I think the drafting team has done a wonderful job of beginning the task of combining two related standards. I ask them to keep in mind the small generators, and others who do not have the wide view capability, that more than likely react to events that occur wih no knowledge of why they occured, and limited staff to address administrative standard requirements. Many times the KISS approach is the best approach.
Idaho Power Company	Yes	By including training requirements in each standard, creates confusion and compliance or failure to comply potentian. PER standards are in place for personel training, these standards should be utilized for adding requirements that require training for NERC Standards.
ISO New England Inc.	Yes	Request clarification on how RCIS is part of this Standard. The form should be filled out in two stages. First stage would be the immediately available information. The second stage would be the additional information such as one line diagrams. There is concern with burdening the reporting operator on filling out forms instead of operating the Bulk Electric System. Most of the draft requirements are written as administrative in nature, and this is not most effective. Changes need to be made to (or possibly elimination of) R1, R2, R3.The standards should be changed to define what a “disturbance” is for reporting in EOP-004. Sabotage reporting as per CIP-001 should be rescinded as EOP-004 already has such a requirement.
Kansas City Power & Light	Yes	The standard addressed a preliminary report it should also address the requirements of a final report.
MidAmerican Energy	Yes	This entire standard needs to be revised to consider a results based standard.
Midwest ISO Standards Collaborators	Yes	We are concerned with the Future Development Plan. It shows an initial ballot period starting in December. This standard has significant issues and will need another distinct comment period (and not the formal comment period in parallel with balloting) prior to balloting.

Organization	Yes or No	Question 15 Comment
MRO's NERC Standards Review Subcommittee	Yes	Please provide an e-mail address for the submittal of the report to NERC (and any other parties above a Regional Entity) within this Standard and a fax number as a backup to electronic submittal.EOP-004 Attachment 2: Impact Event Reporting Form (note in the proposed standards it states EOP-002) seems to be written for Actual Impact Events only. Perhaps another section could be added for "Potential" Impact Events.
NERC Staff	Yes	NERC staff commends the SDT on its work so far. Merging CIP-001 and EOP-004 is a significant improvement and eliminates some current redundancies for reporting events. NERC staff believes opportunities to improve the proposed standard still exist. In particular, the team should consider possible redundancies with the Reliability Coordinator Working Group (RCWG) reporting guidelines, the Electricity Sector - Information Sharing and Analysis Center (ES-ISAC) reporting requirements for sharing information across sectors, and the Events Analysis Working Group (EAWG) efforts to develop event reporting processes. Ideally, the SDT and the EAWG should work together to develop a single consistent set of reporting criteria that can be utilized in both the EAWG event reporting process and in the requirements of the EOP-004-2 Reliability Standard.
North Carolina Electric Coops	Yes	Keep in mind that redundancy in reporting requirements from the DOE does not improve or enhance bulk electric system reliability but rather creates more work for the reporting entity.
Northeast Power Coordinating Council	Yes	Request clarification on how RCIS is part of this Standard. The form should be filled out in two stages. First stage would be the immediately available information. The second stage would be the additional information such as one line diagrams. There is concern with burdening the reporting operator on filling out forms instead of operating the Bulk Electric System. Most of the draft requirements are written as administrative in nature, and this is not most effective. Changes need to be made to (or possibly elimination of) R1, R2, R3.The standards should be changed to define what a "disturbance" is for reporting in EOP-004. Sabotage reporting as per CIP-001 should be rescinded as EOP-004 already has such a requirement.
Pacific Gas and Electric Company	Yes	PG&E believes as the training requirements continue to expand, having one training standard that captures all the training required within the NERC standards will allow for better clarity for the training departments in providing and meeting all NERC Standard compliance issues.
Pacific Northwest Small Public Power Utility Comment Group	Yes	The proposed standard has a huge impact on small DPs. DPs that presently do not maintain 24/7 dispatch centers will need to begin doing so to meet the reporting deadlines such as 1 hour after an occurrence is identified (possibly identified by a third party) or 24 hour after an occurrence (regardless of when it was discovered by the DP). The planning, assessing, drilling, training, and reporting requirements (R2-R6), as well as documentation (M2-M6) by small entities will cause utility rates to rise, will reduce local level of service,

Organization	Yes or No	Question 15 Comment
		and will not represent a corresponding increase to the reliability of the BES.The SDT concept of clear criteria for reporting has not been met, since R2 effectively directs the applicable entities to develop their own criteria. The decision of which types of events will be reported to which external organizations has been left up to the applicable entity. The comment group notes that there is no coordination of effort required between the applicable entities and the RCs or TOs that issue reliability directives. Energy Emergencies requiring voltage reduction or load shedding are likely to be communicated to applicable entities via directives. The likely result of this lack of coordination is that entities will plan, drill, and train for an event, but when the directive comes it will not be the one planned, drilled, and trained for. Coordination between those sending and receiving directives would ensure the probable events and directed responses are the ones planned, drilled, and trained for.
PacifiCorp	Yes	This is yet another standard with training requirements not covered under any PER standards.Having different training requirements spread throughout the standards makes it increasingly difficult to ensure all training requirements are met.Developing a "Training Standard" that lists ALL required training would streamline the process and aid greatly in compliance monitoring.
Pepco Holdings, Inc - Affiliates	Yes	The EAWG is developing processes that will be enforced through the Rules of Procedure. It may be inappropriate to reference the EAWG process in the Mapping Document.
PNM Resources	Yes	PNM believes that having one training standard that captures all the training required within the NERC standards will allow for better clarity for the training departments in providing and meeting all NERC Standard compliance issues. This will become even more of an issue as training requirements continue to expand.
PPL Electric Utilities	Yes	Combining EOP-004, CIP-001 and CIP-008's reporting requirements reduces redundancy and will add clarity to the compliance activities.
Puget Sound Energy	Yes	The DSR SDT's concepts for implementing a new structure for reporting are appropriate. Proper implementation of those concepts is likely to result in a very much improved standard. However, the proposed standard falls well short of implementing the concepts and is not much of an improvement on the current standard.
Santee Cooper	Yes	We don't believe that entities should be subjected to duplicate reporting to existing DOE requirements. How does redundancy in reporting requirements improve or enhance bulk electric system reliability?
SERC OC Standards Review	Yes	We find it disturbing that NERC is headed down a path of codifying requirements that are redundant to

Organization	Yes or No	Question 15 Comment
Group		existing DOE requirements. How does redundancy in reporting requirements improve or enhance bulk electric system reliability? Disclaimer:" The comments expressed herein represent a consensus of the views of the above named members of the SERC OC Standards Review group only and should not be construed as the position of SERC Reliability Corporation, its board or its officers."
Southern Company - Transmission	Yes	The only concern that we have with the proposed standard is that it feels like it is creating dual, not quite redundant, reporting requirements for cyber intrusions in concert with CIP-008. Hopefully, there will not have to be a redundant reporting requirement if we continue to merge efforts with the CIP Drafting Team. Since we will no longer use the word SABOTAGE in the new EOP-004, we are hoping the industry and the CIP Drafting Team will give us the criteria they wish for us to use in order to report CIP-008 incidents. We will then achieve a "ONE STOP SHOP" reporting standard.
Tenaska	Yes	Since the proposed EOP-004-2 Standard does not eliminate the OE-417 reporting requirement, it does not streamline the existing CIP-001-1 and EOP-004-1 reporting requirements for GO/GOP's. The "laundry list" of components required in the Operating Plan described in R2 is too specific and would make it more difficult to prove compliance during an audit. We prefer that the existing CIP-001-1 and EOP-004-1 Standards remain unchanged.
TransAlta Corporation	Yes	A Confidential Impact Event Report form is included in attachment 2 but nowhere in the standard does it say to use this form. This form appears to be similar to the "Preliminary Disturbance Report" form used in EOP-004-1. Clarity is required.
US Bureau of Reclamation	Yes	The SDT should consider that in reality it would be more streamlined to require immediate notification of an event for situational awareness, and then give adequate time for analysis of the cause. Reports that have an arbitrary rush will be diseased with low quality information and not much value in the long run to the BES. The Attachment A should be constructed around notification of situational awareness. The reporting timeline should be constructed around the different levels severity. The more severe the event, usually the more complicated the event is to analyze. Simple events usually do not have a significant impact.
We Energies	Yes	Please be careful to capitalize defined terms. If the intent is to not use the defined term, use another word."Forced intrusion" (cutting a fence, breaking in a door) may not be discovered for quite some time after it occurs. Should it be reported as soon as discovered? Even if there was no impact event (disturbance)? "Destruction of a Bulk Electric System Component" seems pretty specific. However, if a transformer kicks off line due to criminal damage, yet is considered repairable, is the event reportable?

Organization	Yes or No	Question 15 Comment
WECC	Yes	Having one training standard that captures all the training required within the NERC standards will allow for better clarity for the training departments in providing and meeting all NERC Standard compliance issues. This will become even more of an issue as training requirements continue to expand.CIP-001-1 has surprisingly been one of the most violated standards during the initial period. However, most entities have now developed and demonstrated a decent compliance process. Unless a revised standard to address the FERC directive on sabotage is developed (as suggested in 13 above) this proposed standard appears to eliminate sabotage reporting as a reliability standard to the potential detriment of BES reliability.

Consideration of Comments on Disturbance & Sabotage Reporting — Project 2009-01

The Disturbance & Sabotage Reporting Drafting Team (DSR SDT) thanks all commenters who submitted comments on the Second Posting of EOP-004-2, Impact Event Reporting (Project 2009-01).
This standard was posted for a 30-day public comment period from March 9, 2011 through April 8, 2011. The stakeholders were asked to provide feedback on the standard through a special Electronic Comment Form. There were 60 sets of comments, including comments from 188 different people from approximately 132 companies representing 10 of the 10 Industry Segments as shown in the table on the following pages.

In this report, comments have been organized by question to make it easier to see where there is consensus. Comments may be reviewed in their original format on the project page:

http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

Summary Consideration: The DSR SDT received many comments regarding the proposed definition of "Impact Event," the requirements, and event reporting in Attachment 1. The main stakeholder concerns were addressed as follows:

- Many stakeholders disagreed with the need for the definition of "Impact Event" and felt that the definition was ambiguous and created confusion. The DSR SDT agrees and has deleted the proposed definition from the standard. The list of events in Attachment 1 is all-inclusive and no further attempts to define "Impact Event" are necessary.
- Many stakeholders raised concerns with the 1 hour reporting requirement for certain types of events. The commenters believed that the restoration of service or the return to a stable bulk power system state may be jeopardized by having to report certain events within one hour. The DSR SDT agreed and revised the reporting time to 24 hours for most events, with the exception of damage or destruction of BES equipment, forced intrusion or cyber related incidents.
- Many stakeholders suggested that the reporting of events after the fact only justified a VRF of "lower" for each requirement. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF, as this requirement deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all "lower" with the exception of Requirement R2 which is a requirement to analyze

[1] The appeals process is in the Standard Processes Manual:.

events. This standard relates only to reporting events. Analysis of reported events is addressed through the NERC Events Analysis Program. Proposed changes to the Electric Reliability Organization Events Analysis Process Field Trial documents that clarify the role of the Events Analysis program in analyzing reported events will be posted for stakeholder comment separately.

- The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events to the appropriate entities in accordance with the Operating Plan based on Attachment 1. Requirement R3 makes sure that an entity can communicate information about events. Some of these events are dealing with potential sabotage events, and part of the reason to communicate these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 are consistent with the existing approved VRFs for both EOP-004 and CIP-001.
- Several commenters wanted more clarity regarding which entities report and to whom they report. Many stakeholders were confused regarding law enforcement notifications and questioned whether certain types of events (IROL, Public Appeal, etc.) needed to be reported to law enforcement. The background section of the standard provides guidance with respect to reporting events to law enforcement. For clarity, the DSR SDT has added the following sentence to the first paragraph under the heading "Law Enforcement Reporting": "These are the types of events that should be reported to law enforcement." The entire paragraph is:
    - "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES."
- Some commenters also questioned whether or not the existing applicability would result in multiple reports being submitted by different entities for the same event. NERC staff has indicated that this is acceptable and that having multiple types of entities report the same event may provide different types of information about the event.

Commenters also had concerns about the applicability of the standard to Load Serving Entities who may not own physical assets as well as to the ERO and Regional Entity. The DSR SDT agrees that the Distribution Provider owns the assets per the Functional Model; however the LSE is an applicable entity under CIP-002. Events relating the CIP-002 assets are to be reported by the LSE. These are envisioned to be cyber assets. The DSR SDT also include the ERO or the RE as applicable entities based on the applicability of CIP-002

Some commenters identified issues with the footnotes in Attachment 1. These were revised as suggested. There were a few instances where the word "sabotage" remained in the standard or the flowchart. The DSR SDT has removed all instance of "sabotage" and replaced them with "event," and revised the flowchart to remove references to sabotage.

Several commenters were concerned that the DSR SDT and the NERC Events Analysis Working Group (EAWG) may not be in alignment. The DSR SDT is working in close coordination with the EAWG and will continue to develop the standard and will make the EAWG aware of the DSR SDT's efforts.

The issue of the FERC directives relating to this project was broached by several commenters. The DSR SDT envisions EOP-004-2 to be a continent-wide reporting standard. Any follow up investigation or analysis falls under the purview of the NERC Events Analysis Program under the NERC Rules of Procedure. This process is being revised by the EAWG. Discussions with FERC staff indicate that the current efforts of the DSR SDT and the EAWG are sufficient to address the intent of the directive.

After the drafting team completed its consideration of stakeholder comments, the standards and implementation plan were submitted for quality review. Based on feedback from the quality review, the drafting team has made two significant revisions to the standard. The first revision is to add a requirement for implementation of the Operating Plan listed in Requirement R1. There was only a requirement to report events, but no requirement specifically calling for updates to the Operating Plan or the annual review. This was accomplished by having two requirements. The first is Requirement R2 which specifies that an entity must implement the Operating Plan per Requirement R1, Parts 1.1, 1.2, 1.4 and 1.5:

> R2. Each Responsible Entity shall implement the parts of its Operating Plan that meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts 1.4 and 1.5 as specified.

The second Requirement is R3 which addresses Part 1.3:

> R3. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.

The second revision based on the quality review pertains to Requirement R4. The quality review suggested revising the requirement to more closely match the language in the Rationale box that the drafting team developed. This would provide better guidance for responsible entities as well as provide more clear direction to auditors. The revised requirement is:

> R4. Each Responsible Entity shall verify (through actual implementation for an event, or through a drill or exercise) the communication process in its Operating Plan, created pursuant to Requirement 1, Part 1.3, at least annually (once per calendar year), with no more than 15 calendar months between verification or actual implementation.

Index to Questions, Comments, and Responses

1. Do you agree with the revised Purpose Statement of EOP-004-2, Impact Event Reporting? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. ….....15
2. Do you agree with the proposed definition of Impact Event? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 23
3. Do you agree that the DSR SDT has provided and equally efficient and effective solution to the FERC Order 693 directive to "further define sabotage"? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 38
4. Do you agree with the proposed applicability of EOP-004-2 shown in Section 4 and Attachment 1 of the standard? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. ….. 46
5. Stakeholders suggested removing original Requirements 1, 7 and 8 from the standard and addressing the reliability concepts in the NERC Rules of Procedure. Do you agree with the removal of original requirements 1, 7 and 8 (which were assigned to the ERO) and the proposed language for the Rules of Procedure (Paragraph 812)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 64
6. Do you agree with the proposed revisions to Requirement 2 (now R1) including the use of defined terms Operating Plan, Operating Process and Operating Procedure? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 70
7. Do you agree with the proposed revisions to Requirement 3 (now R2)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 87
8. Do you agree with the proposed revisions to Requirement 4 (now R3)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 98
9. Do you agree with the proposed revisions to Requirement 5 (now R4)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 113
10. Do you agree with the proposed revisions to Requirement 6 (now R5) and the use of either Attachment 2 or the DOE-OE-417 form for reporting? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 123
11. Do you agree with the proposed revisions to Attachment 1? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 134
12. Do you agree with the proposed measures for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 159
13. Do you agree with the proposed Violation Risk Factors for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. ….**Error! Bookmark n**
14. Do you agree with the proposed Violation Severity Levels for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. ….**Error! Bookmark n**
15. Do you agree with the proposed Time Horizons for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 189
16. Do you agree with the proposed Implementation Plan for EOP-004-2? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 195
17. If you have any other comments you have not already provided in response to the questions above, please provide them here. …. 201

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	David Revill	Georgia Transmission Corporation & Oglethorpe Power Corporation			X	X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Miller	Georgia Transmission Corporation	SERC	1
2.	Greg Davis	Georgia Transmission Corporation	SERC	1
3.	Jason Snodgrass	Georgia Transmission Corporation	SERC	1
4.	Scott McGough	Oglethorpe Power Corporation	SERC	5

2.	Group	Guy Zito	Northeast Power Coordinating Council					X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Gregory Campoli	New York Independent System Operator	NPCC	2
3.	Kurtis Chong	Independent Electricity System Operator	NPCC	2
4.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
5.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
7.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1

Group/Individual		Commenter	Organization		Registered Ballot Body Segment									
					1	2	3	4	5	6	7	8	9	10
8.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5										
9.	Brian L. Gooder	Ontario Power Generation Incorporated	NPCC	5										
10.	Kathleen Goodman	ISO - New England	NPCC	2										
11.	David Kiguel	Hydro One Networks Inc.	NPCC	1										
12.	Michael R. Lombardi	Northeast Utilities	NPCC	1										
13.	Randy MacDonald	New Brunswick Power Transmission	NPCC	1										
14.	Bruce Metruck	New York Power Authority	NPCC	6										
15.	Chantel Haswell	FPL Group, Inc.	NPCC	5										
16.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10										
17.	Robert Pellegrini	The United Illuminating Company	NPCC	1										
18.	Saurabh Saksena	National Grid	NPCC	1										
19.	Michael Schiavone	National Grid	NPCC	1										
20.	Wayne Sipperly	New York Power Authority	NPCC	5										
21.	Donald Weaver	New Brunswick System Operator	NPCC	1										
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1										
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3										
3.	Group	Denise Koehn	Bonneville Power Administration				X	X	X	X				
	Additional Member	Additional Organization	Region	Segment Selection										
1.	Jim Burns	BPA, Transmission, Technical Operations	WECC	1										
4.	Group	Carol Gerou	Midwest Reliability Organization		X		X		X	X				
	Additional Member	Additional Organization	Region	Segment Selection										
1.	Mahmood Safi	Omaha Public Utility District	MRO	1, 3, 5, 6										
2.	Chuck Lawrence	American Transmission Company	MRO	1										
3.	Tom Webb	Wisconsin Public Service Corporation	MRO	3, 4, 5, 6										
4.	Jodi Jenson	Western Area Power Administration	MRO	1, 6										
5.	Ken Goldsmith	Alliant Energy	MRO	4										
6.	Alice Ireland	Xcel Energy	MRO	1, 3, 5, 6										
7.	Dave Rudolph	Basin Electric Power Cooperative	MRO	1, 3, 5, 6										

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
8. Eric Ruskamp	Lincoln Electric System	MRO 1, 3, 5, 6										
9. Joseph Knight	Great River Energy	MRO 1, 3, 5, 6										
10. Joe DePoorter	Madison Gas & Electric	MRO 3, 4, 5, 6										
11. Scott Nickels	Rochester Public Utilties	MRO 4										
12. Terry Harbour	MidAmerican Energy Company	MRO 1, 3, 5, 6										
13. Richard Burt	Minnkota Power Cooperative, Inc.	MRO 1, 3, 5, 6										
5. Group	Steve Rueckert	Western Electricity Coordinating Council					X					
Additional Member	Additional Organization	Region Segment Selection										
1. Don Pape	WECC	WECC 10										
2. Phil O'Donnell	WECC	WECC 10										
6. Group	Annette Bannon	PPL Supply	X		X		X	X				
Additional Member	Additional Organization	Region Segment Selection										
1.	Mark Heimbach	PPL Martins Creek, LLC RFC 5, 6										
7. Group	Steve Alexanderson	Pacific Northwest Small Public Power Utility Comment Group					X				X	
Additional Member	Additional Organization	Region Segment Selection										
1. Dave Proebstel	Clallam County PUD No.1	WECC 3										
2. Russell A. Noble	Cowlitz County PUD No. 1	WECC 3, 4, 5										
3. Ronald Sporseen	Blachly-Lane Electric Cooperative	WECC 3										
4. Ronald Sporseen	Central Electric Cooperative	WECC 3										
5. Ronald Sporseen	Clearwater Power Company	WECC 3										
6. Ronald Sporseen	Douglas Electric Cooperative	WECC 3										
7. Ronald Sporseen	Fall River Rural Electric Cooperative	WECC 3										
8. Ronald Sporseen	Northern Lights	WECC 3										
9. Ronald Sporseen	Lane Electric Cooperative	WECC 3										
10. Ronald Sporseen	Lincoln Electric Cooperative	WECC 3										
11. Ronald Sporseen	Raft River Rural Electric Cooperative	WECC 3										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
12.	Ronald Sporseen	Lost River Electric Cooperative	WECC 3										
13.	Ronald Sporseen	Salmon River Electric Cooperative	WECC 3										
14.	Ronald Sporseen	Umatilla Electric Cooperative	WECC 3										
15.	Ronald Sporseen	Coos-Curry Electric Cooperative	WECC 3										
16.	Ronald Sporseen	West Oregon Electric Cooperative	WECC 3										
17.	Ronald Sporseen	Pacific Northwest Generating Cooperative	WECC 3, 4, 8										
18.	Ronald Sporseen	Power Resources Cooperative	WECC 5										
19.	Ronald Sporseen	Consumers Power	WECC 1, 3										
20.	Steven J. Grega	Public Utility District #1 of Lewis County	WECC 5										
8.	Group	Patricia Hervochon	PSEG Companies	X				X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Jeffrey Mueller	PSE&G		3
2.	Kenneth Brown	PSE&G		1
3.	Peter Dolan	PSEG ER&T		6
4.	Eric Schmidt	PSEG ER&T		6
5.	Clint Bogan	PSEG Fossil		5
6.	Dominic Grasso	PSEG Fossil		5
7.	Kenneth Petroff	PSEG Nuclear		5
8.	Patricia Hervochon	PSEG NERC Compliance		NA

9.	Group	Louis Slade	Dominion			X	X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Lou Roeder	Electric Transmission	SERC	1, 3
2.	Mike Garton	Electric Market Policy	NPCC	5, 6
3.	Connie Lowe	Electric Market Policy	RFC	5, 6
4.	Jack Kerr	Electric Transmission	SERC	3, 1
5.	Len Sandberg	Electric Transmission	SERC	3, 1

10.	Group	David Thorne	Pepco Holdings Inc and Affiliates		X								

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1.	Mark Godfrey		RFC	1, 3									
11.	Group	Robert Rhodes	SPP Standards Review Group	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Allen	City Utilities of Springfield, MO	SPP	1, 4
2.	George Allan	Sunflower Electric Power Corporation	SPP	1
3.	Michelle Corley	CLECO	SPP	1, 3, 5, 6
4.	Robert Cox	Lea County Electric Cooperative	SPP	1, 3
5.	Kevin Emery	Carthage Water and Electric	SPP	3
6.	Denney Fales	Kansas City Power & Light	SPP	1, 3, 5, 6
7.	Louis Guidry	CLECO	SPP	1, 3, 5, 6
8.	Jonathan Hayes	SPP	SPP	2
9.	Philip Huff	Arkansas Electric Cooperative Corporation	SPP	3, 4, 5, 6
10.	Gregory McAuley	Oklamoma Gas & Electric	SPP	1, 3, 5
11.	Terri Pyle	Oklahoma Municipal Power Authority	SPP	4
12.	Sean Simpson	Board of Public Utilities, City of McPherson, KS	SPP	1, 3, 5
13.	Tay Sing	Oklahoma Municipal Power Authority	SPP	4
14.	Chad Wasinger	Sunflower Electric Power Corporation	SPP	1
15.	Mark Wurm	Board of Public Utilities, City of McPherson, KS	SPP	1, 3, 5
16.	Ron Gunderson	Nebraska Public Power District	MRO	1, 3, 5
17.	Bruce Schutte	Nebraska Public Power District	MRO	1, 3, 5
18.	Jeff Elting	Nebraska Public Power District	MRO	1, 3, 5

12.	Group	Marie Knox	Midwest ISO Standards Collaborators		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Bob Thomas	Illinois Municipal Electric Agency	RFC	4
2.	Jim Cyrulewski	JDRJC Associates, LLC	RFC	8
3.	Terry Harbour	MidAmerican	MRO	1
4.	Joe O'Brien	NIPSCO	RFC	6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
5. Robert Thomasson		Big Rivers Electric Corp.	SERC 1, 3										
13.	Group	Sam Ciccone	FirstEnergy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hohlbaugh	FE	RFC	1, 3, 4, 5, 6
2.	Bill Duge	FE	RFC	5
3.	John Reed	FE	RFC	1
4.	Jim Eckels	FE	RFC	1
5.	Kevin Querry	FE	RFC	5
6.	Ken Dresner	FE	RFC	5

14.	Group	Gerald Beckerle	SERC OC Standards Review Group					X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	David Trego	Fayetteville PWC	SERC	1, 3, 4, 9
2.	Melinda Montgomery	Entergy	SERC	1, 3
3.	Andy Burch	EEI	SERC	1, 5
4.	Eugene Warnecke	Ameren	SERC	1, 3
5.	Chuck Feagans	TVA	SERC	1, 3, 5, 9
6.	Larry Rodriquez	Entegra Power	SERC	5, 6
7.	Gary Hutson	SMEPA	SERC	1, 3, 5, 9
8.	Jennifer Weber	TVA	SERC	1, 3, 5, 9
9.	Doug White	NCEMC	SERC	1, 3, 5, 9
10.	Shaun Anders	CWLP	SERC	1, 3, 5, 9
11.	Jake Miller	Dynegy	SERC	5, 6
12.	Reggie Wallace	Fayette PWC	SERC	1, 3, 4, 9
13.	Dan Roethemeyer	Dynegy	SERC	5, 6
14.	Alvis Lanton	SIPC	SERC	1, 3, 5, 9
15.	Marc Butts	Southern	SERC	1, 3, 5
16.	Robert Thomasson	BREC	SERC	1, 3, 5, 9
17.	Srinivas kappagantula	PJM	SERC	2

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
18.	Barry Hardy	OMU	SERC 1, 3, 5, 9										
19.	Rene' Free	Santee Cooper	SERC 1, 3, 5, 9										
20.	Greg Matejka	CWLP	SERC 1, 3, 5, 9										
21.	John Troha	SERC Reliability Corp.	SERC 10										
15.	Individual	Srinivas Kappagantula	PJM Interconnection LLC	X									
16.	Individual	Cindy Martin	Southern Company				X						
17.	Individual	Cynthia Oder	SRP	X									
18.	Individual	Howard Rulf	We Energies	X				X		X			
19.	Individual	Brent Ingebrigtson	LG&E and KU Energy LLC	X									
20.	Individual	Silvia Parada Mitchell	Compliance & Responsiblity Organization			X							
21.	Individual	John Bee	Exelon	X		X		X	X				
22.	Individual	Jennifer Wright	SDG&E			X							
23.	Individual	Alan Gale	City of Tallahassee (TAL)	X									
24.	Individual	Mace Hunter	Lakeland Electric					X					
25.	Individual	Nathaniel Larson	New Harquahala Generating Co.	X		X		X	X				
26.	Individual	Brian Pillittere	Tenaska					X					
27.	Individual	MIchael Johnson	APX Power Markets			X	X						

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
28.	Individual	Jonathan Appelbaum	United Illuminating Co	X		X	X	X	X				
29.	Individual	Kevin Koloini	American Municipal Power					X					
30.	Individual	Daniel Duff	Liberty Electric Power LLC	X	X	X		X					
31.	Individual	Philip Huff	Arkansas Electric Cooperative Corporation	X									
32.	Individual	Joe Petaski	Manitoba Hydro	X									
33.	Individual	Mike Albosta	Sweeny Cogeneration LP			X	X	X					
34.	Individual	Thad Ness	American Electric Power					X					
35.	Individual	Andres Lopez	USACE			X	X	X	X				
36.	Individual	Nathaniel Larson	New Harquahala Generating Co.	X		X		X	X				
37.	Individual	Eric Salsbury	Consumers Energy					X					
38.	Individual	Michael Falvo	Independent Electricity System Operator	X		X		X	X				
39.	Individual	Kirit Shah	Ameren					X				X	
40.	Individual	Kathleen Goodman	ISO New England, Inc	X				X					
41.	Individual	Deborah Schaneman	Platte River Power Authority			X	X	X					
42.	Individual	Phil Porter	Calpine Corp		X								
43.	Individual	Bill Keagle	BGE	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
44.	Individual	Kenneth A Goldsmith	Alliant Energy		X								
45.	Individual	John Brockhan	CenterPoint Energy	X		X		X	X				
46.	Individual	Martin Kaufman	ExxonMobil Research and Engineering					X					
47.	Individual	Brenda Truhe	PPL Electric Utilities	X									
48.	Individual	Tim Soles	Occidental Power Marketing				X						
49.	Individual	Eric Ruskamp	Lincoln Electric System	X									
50.	Individual	Linda Jacobson	Farmington Electric Utility System	X				X		X			
51.	Individual	Andrew Z Pusztai	American Transmission Company	X									
52.	Individual	Michelle D'Antuono	Ingleside Cogeneration LP			X							
53.	Individual	Greg Rowland	Duke Energy	X		X		X					
54.	Individual	Amir Hammad	Constellation Power Generation			X							
55.	Individual	Scott Barfield-McGinnis	Georgia System Operations Corporation	X									
56.	Individual	Max Emrick	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power					X					
57.	Individual	Rex Roehl	Indeck Energy Services	X		X		X	X				
58.	Individual	Patricia Robertson	BC Hydro					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
59.	Individual	Tony Kroskey	Brazos Electric Power Cooperative			X	X						
60.	Individual	Jim Eckelkamp	Progress Energy	X									

1. **Do you agree with the revised Purpose Statement of EOP-004-2, Impact Event Reporting? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.**

Summary Consideration: The majority of stakeholders agree with the purpose statement. Some commenters had concerns with the use of the words "if known" and "industry awareness" and statements on requiring information from an analysis in the report which may not be known at the time of the report. Comments on this being an "after the fact" report and not real-time reporting have been addressed by a significant revision to the change in reporting times reflected in Attachment 1.

A number of commenters offered suggestions on the use of terms "situational awareness" versus "industry awareness." The DSR SDT used "industry awareness" to address concerns about real-time reporting (which this standard does not cover) and to avoid confusion with the NERC Situational Awareness organization.

The purpose statement was slightly revised to remove the defined term "Impact Event" and replace with the phrase "events with the potential to impact reliability". No other revisions were made.

> "To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of events with the potential to impact reliability and their causes, if known, by the Responsible Entities."

Organization	Yes or No	Question 1 Comment
Exelon	No	Although Exelon agrees that the proposed revision to the purpose statement of EOP-004-2 is better than the original draft; the DSR SDT should consider aligning the definition with the existing OE-417 terms. "Impact Events" are not clearly defined as reportable criteria in the DOE forms and may create confusion. Suggest rewording the purpose statement to simply "Incident Reporting" to align with existing terminology in OE-417 and removing the addition of a new term. A Purpose Statement is defined as "The reliability outcome achieved through compliance with the requirements of the standard." Propose that the purpose should be, "To require a review, assessment and report of events that could have an adverse material impact on the Bulk Electric System."
Response: The DSR DT thanks you for your comment. Form OE-417 report is a DOE report that is not specifically related to BES reliability and is not applicable outside of the United States. The standard only requires reporting of events. Analysis occurs through the NERC Events Analysis Program.		
SDG&E	No	SDG&E does not agree with the revised Purpose Statement because it does not reflect the standard's purpose of identifying reporting requirements for impact events. SDG&E recommends the following revised Purpose Statement: "To identify the reporting requirements for events considered to have an impact on the reliability of the Bulk

Organization	Yes or No	Question 1 Comment
		Electric System and to allow an awareness of these Impact Events to be understood by the industry in recognizing potential enhancements that may be made to the reliability of the BES."
Response: The DSR SDT thanks you for your comment. The DSR SDT believes that the existing purpose statement addresses most of your suggested rewording. The last phrase "recognizing potential enhancements that may be made to the reliability of the BES" is not in the scope of the standard or this project.		
Dominion	No	It is not evident how Impact Event reporting will "improve industry awareness" as suggested in the Purpose Statement. The transfer of Requirement R8 (ERO quarterly report) to the Rules of Procedure (paragraph 812) invalidates that claim within the context of this standard. Suggest removing this phrase from the Purpose Statement.
Response: The DSR DT thanks you for your comment. The ERO will issue reports for industry awareness purposes under the Rules of Procedure. If entities do not report events to the ERO, then these reports will not be issued.		
SPP Standards Review Group	No	We would suggest changing the purpose to read "To improve industry awareness and effectiveness in addressing risk to the BES by requiring the reporting of Impact Events and their causes, if known, by the Responsible Entities."
Response: The DSR DT thanks you for your comment. The DSR SDT contends that the phrase "addressing risk to the BES" applies to the analysis of events which is not covered under the standard.		
United Illuminating Co	No	UI agrees with the idea but believes the statement can be improved to remove ambiguities. For example: "if known" can be modifying the word causes, or the word Impact events. To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of identified Impact Events and if known their causes, if known, by the Responsible Entities.
Response: The DSR SDT thanks you for your comment. The words "if known" are intended to modify the word 'causes.' The DSR SDT has revised the existing wording (from the clean version of the standard) to: *To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of events with the potential to impact reliability and their causes, if known, by the Responsible Entities.*		

Organization	Yes or No	Question 1 Comment
Arkansas Electric Cooperative Corporation	No	The purpose statement reads "To improve industry awareness of the BES." We suggest the purpose should state "To improve industry awareness and effectiveness in addressing risks to the BES." We feel the remaining purpose statement is unnecessary.
Response: The DSR SDT thanks you for your comment. The DSR SDT contends that the phrase "addressing risk to the BES" applies to the analysis of events which is not covered under the standard.		
Manitoba Hydro	No	Situational Awareness was replaced by the generic "Industry awareness." Justification for this was that Situational Awareness was a byproduct of a successful event reporting system and not a driver. Using Industry awareness clouds the clarity of the purpose. If personal are properly trained and conscious of their responsibilities, then they are in fact situationally aware, and will therefore drive the reporting process on the detection an Impact Event. Industry awareness falsely labels this Standard as unique to the electrical industry when clearly many outside and international agencies will be notified and involved. Situational Awareness seems much more appropriate and encompassing. Other then that the Purpose is a large improvement from the original.
Response: The DSR SDT thanks you for your comment. The DSR SDT changed "situational awareness" to "industry awareness" to address concerns about real-time reporting (which this standard does not cover) and to avoid confusion with the NERC Situational Awareness organization.		
Ameren	No	The original Purpose wording was clear, concise and understandable.
Response: The DSR SDT thanks you for your comment. The original purpose statement was in the form of a requirement and not a purpose statement.		
ISO New England, Inc	No	The purposed states To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of Impact Events and their causes, if known, by the Responsible Entities. Awareness by who in the industry?
Response: The DSR SDT thanks you for your comment. The requirements of this standard require that events be reported after-the-fact. The NERC Events Analysis Program will take certain events reported under this standard and analyze them to provide information to the entire body of users, owners and operators of the BES.		
Calpine Corp	No	The purpose has moved significantly from the originally approved SAR. The purpose should focus on reporting requirements for reporting electrical disturbances to the Bulk Electric System that exceed specific thresholds. Sabotage/vandalism/theft are a subset of the reportable events that could have or do cause a Bulk Electric System Electrical Disturbance. The Standards content should focus on setting requirements to

Organization	Yes or No	Question 1 Comment
		report specific types of electrical disturbance events and providing guidance for performing that reporting. Alternative language: Purpose: To establish reporting requirements for events that either cause, or have the potential to cause, significant disturbances on the Bulk Electric System.
Response: The DSR SDT thanks you for your comment**.** The purpose covers the EOP-004 and CIP-001 standards which include disturbance and sabotage. The use of the word 'events' and the definition of the specific events to be reported (see Attachment 1) is a result of combining these two standards as well as the drafting team's efforts to address FERC Order 693 Directives. The proposed purpose statement does not adequately address these items.		
BGE	No	BGE believes that using the term Impact Events as currently defined is too vague. An alternative statement would be requiring the reporting of events listed in Attachment 1 and their causes, if known and making the definition change as noted in question 2.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated the defined term "Impact Events" and uses the generic term "events: in the purpose statement. *To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of events with the potential to impact reliability and their causes, if known, by the Responsible Entities.*		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	No	"To improve industry awareness and the reliability fo the Bulk Electric System by requiring the reporting of Impact Events and their causes, if known by the Responsible Entities." The revised purpose statement includes the phrase, if known. This seems like a huge loophole. They should change it to when discovered or when notified.
Response: The DSR SDT thanks you for your comment. The intent of "if known" was to make sure that events were reported regardless of whether the cause was known. It is important for entities to report events and to return the BES to a reliable operating state. Investigation of causes can occur at a later time.		
Indeck Energy Services	No	The reporting of events does not improve the reliability of the BES. If someone takes action based on the reporting, there might be an improvement. Because many of these events are not preventable, such as sabotage or weather, reporting them won't improve reliability. The original Purpose was satisfactory.
Response: The DSR SDT thanks you for your comment. The requirements of this standard require that events be reported after-the-fact. The NERC Events Analysis Program will take certain events reported under this standard and analyze them to provide information that will lead to improvements in BES reliability.		
Brazos Electric Power Cooperative	No	Instead of Impact Event could simply call it Event Information Reporting.

Organization	Yes or No	Question 1 Comment
Response: The DSR SDT thanks you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event."		
Compliance & Responsiblity Organization	No	See comments set forth in number 2.
Georgia Transmission Corporation & Oglethorpe Power Corporation	Yes	We find it unnecessary to state that the purpose of a Reliability Standard is to "improve the reliability of the Bulk Electric System."
Response: The DSR DT thanks you for your comment. The DSR SDT disagrees. This is an integral part of the purpose of reporting events.		
Midwest Reliability Organization	Yes	The addition of "industry awareness" adds to the scope of this Standard. Whereby an entity is required to inform the RC and others of actual and potential Impact Events.
Response: The DSR DT thanks you for your comment. The DSR SDT has streamlined Attachment 1 to ensure that the proper reporting is accomplished.		
American Municipal Power	Yes	The purpose is acceptable. I think it could be improved and simplified. There were not any questions on the title. Consider changing the title to Reportable Events. There were not any questions on the category. I suggest changing the category from Emergency Operations to Communications. Reporting events can trigger and be more than just Emergency Operations. I feel the reporting function performed by entities should be under the Communications category. Title: Reportable Events Purpose: To improve reliability by communicating timely information about an event or events.
Response: The DSR SDT thanks you for your comment. The DSR SDT revised the existing title of the standard to conform to the intended purpose of reporting events. The team discussed making this a COM standard during the initial DT discussions but decided to retain the existing EOP-004 standard category and number. This is not a real-time reporting standard but requires after the fact reporting.		
Ingleside Cogeneration LP	Yes	The addition of the modifier if known to reporting the cause of an Impact Event is appropriate. It often proves counter-productive to speculate as initial conjectures of the cause of an event are easy to come up with, but difficult to back out of later.
Response: The DSR SDT thanks you for your comment.		
Duke Energy	Yes	However, as we have noted previously, the DSR SDT statement that the proposed changes do not include any real-time operating notifications is inconsistent with requiring notification within one hour for thirteen of the

Organization	Yes or No	Question 1 Comment
		twenty listed Events in Attachment 1 Impact Event Table. Also, in the Background discussion, under Law Enforcement, the DSR SDT states that the objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting Impact Events. As we have previously commented, we are still required to make real-time reports under other standards. Requiring duplicate real-time reporting under EOP-004-2 is a waste of resources which could otherwise be used to improve reliability.
Response: The DSR SDT thanks you for your comment. We have made significant revisions to Attachment 1 and the reporting time requirements to address the real-time reporting concern.		
Constellation Power Generation	Yes	While CPG generally agrees with the purpose statement, we believe that the term Impact Events should be removed. Please see CPGs response to Question 2 discussing the term Impact Events.
Response: The DSR SDT thanks you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Please see responses to comments on question 2.		
Georgia System Operations Corporation	Yes	We agree with the purpose. However, we do not agree that the purpose will be achieved as this standard is currently drafted or that the standard is ready for balloting.
Response: The DSR SDT thanks you for your comment. We have made significant revisions to the body of the standard and Attachment 1.		
Northeast Power Coordinating Council	Yes	
Bonneville Power Administration	Yes	
Western Electricity Coordinating Council	Yes	
PPL Supply	Yes	
Pacific Northwest Small Public Power Utility Comment Group	Yes	
PSEG Companies	Yes	

Organization	Yes or No	Question 1 Comment
Pepco Holdings Inc and Affiliates	Yes	
Midwest ISO Standards Collaborators	Yes	
FirstEnergy	Yes	
SERC OC Standards Review Group	Yes	
PJM Interconnection LLC	Yes	
Southern Company	Yes	
SRP	Yes	
We Energies	Yes	
City of Tallahassee (TAL)	Yes	
Lakeland Electric	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
Liberty Electric Power LLC	Yes	
Sweeny Cogeneration LP	Yes	
American Electric Power	Yes	
USACE	Yes	

Organization	Yes or No	Question 1 Comment
New Harquahala Generating Co.	Yes	
Independent Electricity System Operator	Yes	
Platte River Power Authority	Yes	
Alliant Energy	Yes	
CenterPoint Energy	Yes	
ExxonMobil Research and Engineering	Yes	
PPL Electric Utilities	Yes	
Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
American Transmission Company	Yes	
BC Hydro	Yes	

2. Do you agree with the proposed definition of Impact Event? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: The majority of the commenters do not agree with the definition and thought the definition as overly broad, too subjective and confusing. Many commenters questioned whether there was a need for a definition of Impact Event at all. The DSR SDT discussed the comments and suggestions and decided to incorporate commenters' suggestion to delete the definition and rely on the Attachment 1 to stand on its own.

The DSR SDT has deleted the Impact Event definition.

Organization	Yes or No	Question 2 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation	No	We do not think that Impact Event should be defined using a recursive definition, i.e. that the word "impact" should be used in the definition of the term "Impact Event." Instead, we suggest using an enumerative definition in that the tables included in Attachment 1 are themselves used to define "Impact Event." If this definition is not acceptable, we suggest replacing the word "impact" in the definition with the word reduce, reduced, or potential to reduce the reliability of the BES.
Response: The DSR SDT thanks you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events for the given thresholds listed in Attachment 1.		
Northeast Power Coordinating Council	No	Is there a need for this definition? By itself the term is not specific on the types of events that are regarded as having an impact. The detailed listing of events that fall into a reportable event category, hence the basis for the Impact Event, is provided in Attachment A. The events that are to be reported can be called anything. Defining the term Impact Event does not serve the purpose of replacing the details in Attachment A, and such a term is not used anywhere else in the NERC Reliability Standards. For a complete definition of Impact Event, all the elements in Attachment A must be a part of it. Suggest consider not defining the term Impact Event, but rather use words to stipulate the need to have a plan, to implement the plan and to report to the appropriate entities those events listed in Attachment A.
Response: The DSR SDT thanks you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events for the given thresholds listed in Attachment 1.		

Organization	Yes or No	Question 2 Comment
Bonneville Power Administration	Yes	Agree, but note that this will add many more situations to reporting and it will require more staff time to accomplish this.
Response: The DSR SDT thanks you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events for the given thresholds listed in Attachment 1.		
Midwest Reliability Organization	No	The proposed definition is not supported by any of the established bright line criterias that are contained within attachment 1. This Results Based Standard should close any loop-holes that could be read into any section, especially the definition. According to rules of writing a definition, a definition should not contain part of the word that is being defined. Recommend the definition be enhanced to read: Impact Event: Any Contingency which has either effected or has the potential to effect the Stability of the BES as outlined per attachment 1. Within this enhanced recommendation, presently defined NERC terms are used (Contingency and Stability), thus supporting what is current used within our industry. There is also a quantifiable aspect of as outlined per attachment 1 that clearly defines Impact Events.
Response: The DSR SDT thanks you for your comment. The DSR SDT believes the definition is embodied in Attachment 1 criteria and needs no further clarification. We have deleted the proposed defined term "Impact Events" and will use the generic term "event."		
Western Electricity Coordinating Council	No	We question the need for a defined term. It appears that an Impact Event is any event identified in Attachment 1. The use of the defined term combined with the language of Requirement 2 to implement the Impact Event Operating Plan for Impact Events listed in Attachment 1 may be confusing. Is an Impact Event any event described by the proposed definition or is an Impact Event any event listed in Attachment 1?
Response: The DSR SDT thanks you for your comment. The DSR SDT agrees the definition could be confusing. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events for the given thresholds listed in Attachment 1.		
Dominion	Yes	Dominion agrees with the proposed definition of Impact Events, but notes the use of the phrase has the potential to impact is somewhat subjective. The concern being a Responsible Entity makes a judgment on an events potential impact that is viewed differently after-the-fact by an auditor.
Response: The DSR SDT thanks you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events for the given thresholds listed in Attachment 1.		
Pepco Holdings Inc and Affiliates	No	The two sentence definition will not be adequate to serve well over the course of time. People will have to read and understand the standard without benefit of the detailed information, explanations and interpretations

Organization	Yes or No	Question 2 Comment
		available during the standards development process. Without additional explanation as provided in the background and the guideline and technical basis sections, to support the definition, the standard will be subject to confusion and interpretations. Consider adding a lot of the information and explanation that is in those sections to the standard. Any event could be an impact event. However, only a subset is reportable. What is really being addressed are reportable events. More specifically after the fact reporting of unplanned events.
Response: Thank you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events for the given thresholds listed in Attachment 1.		
Midwest ISO Standards Collaborators	No	The definition of Impact Event is overly broad because of the use of potential to impact and the Such as list. Consider routine switching has the potential to result in a mis-operation. This means all routine switching is an impact event. The Such as list should be struck and potential language should be struck.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event."		
FirstEnergy	No	Although we agree with the definition of Impact Event, we believe that it should be clear that this term is specific to the events listed in Attachment 1 of the standard. Therefore, we suggest adding the phrase (as detailed in Attachment 1 of EOP-004-2) in the definition.
Response: Thank you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
SERC OC Standards Review Group	No	We believe the definition is too broad even considering Attachment 1, footnote1, which, for example, uses the term significantly and other ambiguous terms. Consideration should be given to limiting the definition to unplanned events.
Response: Thank you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event."		
PJM Interconnection LLC	No	The term "Impact Event" has been too broadly defined. According to the current definition, any event (including routine operations) can have the potential to impact the reliability of the Bulk Electric System and hence can be an Impact Event. The definition should only include unplanned events. Attachment 1 lists the events that are reportable. It seems that the definition of Impact Event refers to the events in Attachment 1 as opposed to defining Impact Event. As such, it is best that the SDT not define Impact Event but use words to the effect that requires an entity to have a plan and implement it for reporting unplanned events outlined in Attachment 1. If Impact Event were to be defined, we suggest the following definiton would be a better

Organization	Yes or No	Question 2 Comment
		option:"An Impact Event is any unplanned event listed in Attachment I that has either adversely impacted or has the potential to adversely impact the reliability of the Bulk Electric System."
Response: Thank you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event."		
SRP	No	Suggest that definition include reference to the fact that this is non-desired occurence, as the word 'impact' has neither a positivie nor negative implication. This is not a well formed definition as it contains circular refernces to 'impacted' and 'event' within the definition.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event."		
We Energies	No	From an on-line dictionary, an event is something that happens. Combined with the phrase has the potential to impact and the definition of Impact Event would include every routine operation performed by any entity. Taking a generator on or off line, switching a transmission line in or out, traffic driving past a substation, all have the potential to impact the BES. The Impact Event definition is overly broad and needs to be significantly narrowed.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event."		
Compliance & Responsiblity Organization	No	NextEra Energy Inc. (NextEra) appreciates the drafting team providing valuable ideas and a framework on how to improve and consolidate CIP-001 and EOP-004. However, NextEra also believes that the currently drafted EOP-004-2 needs to be revised and enhanced to more clearly explain the Responsible Entities' duties, the definition of sabotage and address FERC directives and concerns. For example, NextEra is not in favor using the term "Impact Event" which seems to add considerable confusion of what is or is not sabotage. In Order No. 693, FERC stated its interest in NERC revising CIP-001 to better define sabotage and requiring notification to the certain appropriate federal authorities, such as the Department of Homeland Security. FERC Order 693 at PP 461, 462, 467, 468, 471. NextEra has provided an approach that accomplishes FERC's objectives and remains within the framework of the drafting team, but also focuses the process of determining and reporting only those sabotage acts that could impact other BES systems. Today, there are too many events that are being reported as sabotage to all parties in the Interconnection, when in reality these acts have no material affect or potential impact to other BES systems other than the one that experienced it. For example, while the drafting team notes the issue of copper theft is a localized act, there are other localized acts of sabotage that are committed by an individual, and these acts pose little, if any, impact or threat to other BES systems other than the one experiencing the sabotage event. Reporting sabotage that

Organization	Yes or No	Question 2 Comment
		has no need to sent of everyone does not necessary add to the security or reliability of the BES. Related, there is a need to clarify some of the current industry confusion on who should (and has the capabilities to) be reporting to a boarder audience of entities. Hence, NextEra approach provides a clear definition of sabotage, as well as the process for determining and reporting sabotage. NextEra further believes that some of the requirements can be consolidated and more clearly stated, and NextEra has attempted to do that in the approach presented below. Lastly, NextEra comments on Attachment 1 are submitted in response to question 17. NextEra Approach Delete definition of Impact Event and its use in the requirements and in Attachment 1 Delete 13, 14, 15 and 19 in Attachment 1 Delete and replace R1 through R5 with the following: New Definition Attempted or Actual Sabotage: an intentional act that attempts to or does destroy or damage BES equipment or a Critical Cyber Asset for the purpose of disrupting the operations of BES equipment, Critical Cyber Asset or the BES, and has a potential to materially threaten or impact the reliability of one or more BES systems (i.e., is one act in a larger conspiracy to threaten the reliability of the Interconnection or other BES systems). R1. Each Responsible Entity shall document and implement a procedure (either individually or jointly with other Responsible Entities) to accomplish the reporting requirements, including the time frames, assigned to the Responsible Entity as set forth in Attachment 1 items 1 through 12, 16, 17 and 18 for reporting from the Responsible Entity to its Regional Entity and NERC, using the form in Attachment 2 or the DOE OE-417 reporting form. R2. Each Responsible Entity shall document and implement a procedure (either individually or jointly with other Responsible Entities) to report to its internal personnel with a need to know and its Reliability Coordinator an act of Attempted or Actual Sabotage, using the form in Attachment 2 or the DOE OE-417 reporting form, within one hour after a determination has been made that an act Attempted or Actual Sabotage has occurred. To make a determination that an act of Attempted or Actual Sabotage has occurred, the Responsible Entity shall document and implement a procedure that requires it, as soon as practicable after the discovering an act appearing to be Attempted or Actual Sabotage, to engage local law enforcement or the Federal Bureau of Investigation or Royal Canadian Mounted Police, as deemed appropriate, to assist the Registered Entity make such a determination. Upon receiving a report of Attempted or Actual Sabotage from a Responsible Entity, the Reliability Coordinator shall within one hour forward the report to other impacted Reliability Coordinators, Responsible Entities, Regional Entities, NERC, Department of Homeland Security, and the Federal Bureau of Investigation or the Royal Canadian Mounted Police. R3. Each Responsible Entity shall review (and conduct a test for sabotage only) of its documented procedure required in R1 and R2 with no more than 15 calendar months between tests for sabotage reporting. If, based on the review or test, the Responsible Entity determines there is a need to update its documented procedure, it shall update the procedures within 90 calendar days of the review or test.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comments and suggestions. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Other revisions were made to the standard based on comments received on specific requirements. The DSR SDT believes that these revisions clarify the requirements and has provided additional details in response to comments from questions Q3, Q6, Q7, Q8, Q11, Q12, Q13, Q14 and Q17. Please see the revised standard. In regards to sabotage, the DSR SDT believes that the reporting of events supports the reliability of the BES. Sabotage usually is determined after the event is investigated and sabotage may be one aspect of a single event. The intent is to report events (per Thresholds of Reporting in Attachment 1) that have an impact on BES reliability. The background section of the standard provides guidance with respect to reporting events to law enforcement. For clarity, the DSR SDT has added the following sentence to the first paragraph under the heading "Law Enforcement Reporting": "These are the types of events that should be reported to law enforcement." The entire paragraph is: "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES."		
Exelon	No	The definition of impact events should be reworded to align with OE-417 and to explicitly reference that only events identified in EOP-004 ? Attachment 1 are to be reported. Suggest the following:"An incident that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-opeation, environmental conditions, or human action as defined in EOP-004 Attachment 1." Propose the definition be changed to include material impact and read as follows; Any event which has either caused or has the potential to cause an adverse material impact to the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action?
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
City of Tallahassee (TAL)	No	While I agree with the overall concept, I am concerned with "or has the potential to impact." While the standard makes reference to Attachment 1 Parts A and B, the inclusion of the attachment is not in the definition. This leaves ambiguity in the definition that could enable second guessing by auditors. Proposed: "An impact event is any event that has either impacted or has the potential to impact (above the

Organization	Yes or No	Question 2 Comment
		thresholds described in EOP-004-2 Attachment 1) the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action."
Response: Thank you for your comments. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event."		
American Electric Power	No	The definition is too broad and vague. The text in the comment form has the following sentence Only the events identified in EOP-004 Attachment 1 are required to be reported under this Standard. The definition should contain that caveat or something similar.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
USACE	No	1) You cannot use the terms impact and event to define impact event. 2) The phrase "has the potential to impact" makes the definition too vague. Every action taken to modify the system or its components has the potential to impact the Bulk Electric System. 3) Recommend to change the definition to "Any occurrence which has adversely affected the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action."
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Consumers Energy	No	The definition of Impact Event seems very vague and nebulous. This definition should be modified to be clear and concise, such that entities clearly understand what is included within the definition.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Ameren	No	The documentation from the SDT included the reliability objective for EOP-004-2 which should be included in the definition of Impact Event. Our suggested alternate defintion for Impact Event: "An Impact Event is any event that has either caused, or has the likely potential to cause, an outage which could lead to Cascading. Such events will be identified as being caused by, to the best of the reporting entity's information: (1) equipment falure or equipment mis-operation, (2) environmental conditions, and/or (3) human actions."

Organization	Yes or No	Question 2 Comment
		This alternate wording includes the reliability objective and clarifies the three known, or likely, causes of the Impact Event.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
ISO New England, Inc	No	We question the need for this definition since by itself the term is not specific on the types of events that are regarded as having an impact. The detailed listing of events that fall into a reportable event category, hence the basis for the Impact Event, is provided in Attachment A. For that matter, these events that are to be reported can be called anything, or just simply be titled "Event to be Reported" without having to define them. Defining the term Impact Event does not serve the purpose of replacing the details in Attachment A, and such a term is not used anywhere else in the NERC reliability standards. In fact, for the term Impact Event to be fully defined, all the elements in Attachment A must become a part of it. We therefore suggest the SDT to consider not defining the term Impact Event, but rather use words to stipulate the need to have a plan, to implement the plan and to report to the appropriate entities those events listed in Attachment A. If the SDT still wishes to retain a definition despite our reservations noted above, we strongly suggest an improvement. The proposed definition of Impact Event is overly broad because of the use of "potential to impact" and the "Such as" list. Consider that routine switching has the potential to result in a mis-operation. In that regard most routine switching could be interpreted as an impact event. The "Such as" list should be struck and "potential" language should be struck. An alternative definition to consider: An Impact Event is any deliberate action designed to reduce BES reliability; unintended accident that could result in an Adverse Reliability Impact; or an unusual natural event that causes or could cause an Adverse Reliability Impact.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Calpine Corp	No	Adding a definition for Impact Event is unnecessary and does not provide useful clarification of the actual reporting requirement for events that either impact the Bulk Electric System or have the potential to impact the Bulk Electric System. The all-encompassing nature of the proposed definition seems to conflict with the finite listing of events that actually require reporting. Although FERC specifically requested additional clarification of the term sabotage to clarify reporting requirements, the Drafting Team is correct in noting that sabotage implies intent and that the intent of human acts is not always easily determined. The fact that intent is not always determinable within the reporting timeframe can be dealt with more simply by requiring (in attachment

Organization	Yes or No	Question 2 Comment
		1) that human intrusions that have not been identified within the reporting timeframe as theft or vandalism should be reported as potential sabotage pending further clarification. This approach negates the need for an additional definition that may cause confusion regarding which events are reportable and eliminates the potential for under-reporting based on the assumption that the cause might be theft or vandalism.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
BGE	No	Change the definition of "Impact Event", to add the following phase to the definition "Any event (listed in Attachment 1) which has either…." Also, the phrase "…or has the potential to impact the reliability…" is too vague and broad. Such broad statement is unhelpful in clarifying entities' compliance obligation and potentially creates conflicted reporting between entities. A clear statement of how the reliability is affected should be used, i.e., results in contingency emergency situation or IROL.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Alliant Energy	No	The proposed definition is not supported by any of the established bright line criteria that are contained within attachment 1. This Results Based Standard should close any loop-holes that could be read into any section, especially the definition. We recommend the definition be enhanced to read: Impact Event: Any Contingency which has either effected or has the potential to effect the Stability of the BES as outlined per attachment 1. Within this enhanced recommendation, presently defined NERC terms are used (Contingency and Stability), thus supporting what is current used within our industry. There is also a quantifiable aspect of as outlined per attachment 1 that clearly defines Impact Events. If the above definition is not adopted, we believe it should be rephrased to narrow the scope to those events that result from malicious intent or human negligence/error. We are concerned that by using phrases like unintentional or intentional human action in combination with damage or destruction basically means everything except copper theft becomes a reportable impact event (including planned actions we must perform to comply with CIP-007 R7).
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
CenterPoint Energy	No	CenterPoint Energy suggests that the phrase "…or has the potential to impact…" be deleted as it makes the definition vague and broad. Similar issues encountered in trying to define sabotage may resurface, such as

Organization	Yes or No	Question 2 Comment
		varying definitions or interpretations of "potential." If this standard is to support after-the-fact reporting, the focus should be on actual events, not potential situations or events. Effective and efficient prevention would come from analysis of actual events. Resources and reporting could become overwhelmed upon having to consider "potential." All references to "potential" should be removed from the standard, guidance, and attachments.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
ExxonMobil Research and Engineering	No	The use of the word potential is ominous.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Occidental Power Marketing	No	The SDT includes in the definition the "potential to impact the reliability of the BES." This seems vague, although Attachment 1 clarifies what actually has to be reported. An LSE may have limited or no knowledge of "potential to impact." The SDT may want to refine the definition, e.g., "to the extent the entities' knowledge could reasonably reveal the impact."
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Lincoln Electric System	No	As currently drafted, the proposed definition of Impact Event appears vague and provides entities minimal clarity in terms of distinguishing events of significance. Recommend the drafting team reference Attachment 1: Impact Events Tables within the definition to direct industry towards more specific criteria.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
American Transmission Company	No	ATC does not agree with the proposed definition and further disagrees whether a definition is needed at all. Proposed Definition: The definition, read outside of the proposed standard, does not provide Registered Entities with a clear meaning of the purpose of the definition. It is ATCs opinion that the SDT is using the term Impact Event as an introduction phrase to Attachment 1. ATC would be more comfortable if the

Organization	Yes or No	Question 2 Comment
		definition was dropped and the team would re-write the requirement to specifically point to Attachment 1. It is our opinion that this type of structure would achieve the goal of the team to get Registered Entities to report on events identified in Attachment 1.The other option is for the team to write into the definition that the events being discussed are limited to those identified in Attachment 1. Also the language currently being used in the definition includes potential and such as. These terms should be struck from the definition.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Ingleside Cogeneration LP	No	The SDT includes in the definition the potential to impact the reliabilty of the BES. This seems vague, although ultimately the events which meet the threshold of a reportable Impact Event are governed by the tables under Attachment 1. We believe that there should be close, if not perfect, synchronization between the EROs Event Analysis Process and Attachment 1 since they share the same ultimate goal as EOP-004-2 to improve industry awareness and BES reliability.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Duke Energy	No	The phrase "…or has the potential to impact…" makes this an impossibly broad definition, and demonstrating compliance will not be straightforward.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Constellation Power Generation	No	The currently proposed definition is vague and can be easily misinterpreted. Coining a term to define the events that the DSR SDT hopes to capture in EOP-004-2 is a difficult task, one that may not be necessary. Replacing the term Impact Events with events in Attachment 1, would eliminate the need to define such a term. In addition, the phrase or has the potential to impact the reliability is too vague and broad. Such broad statement is unhelpful in clarifying entities compliance obligation and potentially creates conflicted reporting between entities. The language in the reporting requirements should be limited to real impact events, while information sharing on near miss or deficiency incidents should be handled as good industry practices and not subject to onerous compliance obligations. The drafting team should also give careful consideration to the existing reporting and information sharing currently in place in the industry. When an event occurs, partners in the electric sector are notified as part of

Organization	Yes or No	Question 2 Comment
		existing requirements outside of NERC compliance.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Georgia System Operations Corporation	No	It is not clear for the purposes of complying with this standard what it means to impact reliability. Impact in what way. To what degree. Do not define this term. An alternative would be to define it as those events listed in Appendix 1.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Indeck Energy Services	No	It's not a definition. It needs some quantification, such as, a Reportable Disturbance (NERC glossary), a reportable event under DOE OE-417, sabotage or bomb threat. Defining it as having or potentially having an impact is no definition. What is an impact? It needs to be quantified or auditors will have license to define it any way that they want. It shouldn't be a NERC Glossary definition if its only use is in EOP-004. Within EOP-004, it can be defined as anything in Attachment 1.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Progress Energy	No	Progress Energy appreciates the Standard Drafting Teams work on this project. Any potential impact is too vague and impossible to measure. Progress is unsure of how the ERO or Regional Entity measure impact. Potential is very subjective.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Brazos Electric Power Cooperative	No	
Southern Company	Yes	There is concern that the proposed definition for Impact Event does not allow for prudent judgment and preliminary situational assessment by the entity to declare a Potential Impact Event (especially threats) as non-credible. The thresholds for reporting established in Attachment 1 ? Part A provide a somewhat definitive bright line with regard to those events identified in Part A, but for some of the events in Part B there should be allowance for an assessment by the entity to reasonably determine whether the event poses a credible threat

Organization	Yes or No	Question 2 Comment
		to the reliability of the BES. This is attempted in the footnote to the Forced Intrusion event in Attachment 1 ? Part B, but we think this allowance for entity assessment and prudent judgment needs to apply more pervasively, perhaps by including the term credible in the definition of Impact Event or at least by adding the term credible wherever the term physical threat is used.
Response: Thank you for your comments. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." The word "credible" could lead to many interpretations as well. Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
American Municipal Power	Yes	The definition of Impact Event is acceptable and an improvement. I feel it could be improved and simplified further. Consider changing Impact Event to a "reportable event."
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Liberty Electric Power LLC	Yes	I am interpreting the phrase "has the potential" to exclude events which had the potential, but did not impact the BES. An example would be a generation trip - if the trip had happened during a system emergency it could have affected the BES, but since it happened under normal conditions there is no reporting responsibility. Some assurance on this interpretation would be appreciated.
Response: The DSR SDT thanks you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Manitoba Hydro	Yes	"Disturbance" has a unique and traditional meaning in the electrical industry, basically meaning "a notable electrical event causing in imbalance of load and generation." Attempting to include the many scenarios can that can affect reliability blurred the current vision of "Disturbance" and the addition of "unusual occurrences" just added to the confusion. It never seemed appropriate to submit an unusual occurrence on a "Disturbance Report." "Impact Event" is very encompassing and then detailed specifically in Attachment 1.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Independent Electricity System Operator	Yes	We do not have any issue with the wording of the definition, but question the need for this definition since by itself the term is not specific on the types of events that are regarded as having an "impact." The detailed listing of events that fall into a reportable event category, hence the basis for the Impact Event, is provided in Attachment A. For that matter, these events that are to be reported can be called anything. Defining the term Impact Event does not serve the purpose of replacing the details in Attachment A, and such a term is not

Organization	Yes or No	Question 2 Comment
		used anywhere else in the NERC reliability standards. In fact, for the term Impact Event to be fully defined, all the elements in Attachment A must become a part of it. We therefore suggest the SDT to consider not defining the term Impact Event, but rather use words to stipulate the need to have a plan, to implement the plan and to report to the appropriate entities those events listed in Attachment A.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
PPL Electric Utilities	Yes	PPL EU agrees with the definition. We would like to point out that our interpretation of the definition excludes maintenance work. Our interpretation also concludes that maintenance work that does not go as planned or goes awry and impacts the reliability of the BES would be an impact event and reported as required per Attachment 1.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
SDG&E	Yes	
PPL Supply	Yes	
PSEG Companies	Yes	
SPP Standards Review Group	Yes	
Lakeland Electric	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
United Illuminating Co	Yes	
Arkansas Electric Cooperative	Yes	

Organization	Yes or No	Question 2 Comment
Corporation		
Sweeny Cogeneration LP	Yes	
New Harquahala Generating Co.	Yes	
Platte River Power Authority	Yes	
Farmington Electric Utility System	Yes	
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	
BC Hydro	Yes	
Response: Thank you for your response. Most commenters who responded to this question disagreed with the proposed definition and some suggested that the definition is not needed. In response, the drafting team has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		

3. Do you agree that the DSR SDT has provided an equally efficient and effective solution to the FERC Order 693 directive to "further define sabotage"? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: Most stakeholders agreed that the drafting team addressed the directive to further define sabotage. Commenters generally agreed that the DSR SDT approach in the currently proposed solution effectively addresses FERC Order 693 directive. The approach clarifies the triggering event for an entity to take action and, by deleting all references to "sabotage," in effect removes the very term that had no clear definition.

Organization	Yes or No	Question 3 Comment
Pepco Holdings Inc and Affiliates	No	See #2. With out the explanation contained in background information, over time those that have not been involved with this standard development will struggle with how to interpret the code words of non environmental and intentional human action.
Response: The DSR DT thanks you for your comment. This is a Results-based standard and the format includes all of the information, with the exception of the Rationale boxes, through the ballot and filing of the standard. The background section of the proposed standard will be retained with the standard for future reference.		
Midwest ISO Standards Collaborators	No	In general, we agree that the standard drafting team has provided an equally efficient and effective alternative, but we wonder if the SDT has not in essence already defined sabotage in their description for why they cant define sabotage. It seems that sabotage involves willful intent to destroy equipment. In general, intent would have to be determined by an investigation of law enforcement. This could be part of the definition. There might be some obvious acts that could be included without investigation such as detonation of a bomb. Is it possible for the SDT to use the DOE definition for sabotage? We encourage the SDT to provide a definition for sabotage.
Response: The DSR DT thanks you for your comment. The DSR SDT believes that the reporting of events supports the reliability of the BES. Sabotage usually is determined after the event is investigated and that sabotage may be one aspect of a single event. The intent is to report (per Thresholds of Reporting in Attachment 1) events that have an impact on BES reliability. The background section of the standard provides guidance with respect to reporting events to law enforcement. For clarity, the DSR SDT has added the following sentence to the first paragraph under the heading "Law Enforcement Reporting": "These are the types of events that should be reported to law enforcement." The entire paragraph is: o "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely		

Organization	Yes or No	Question 3 Comment
upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES."		
Compliance & Responsiblity Organization	No	See comments set forth in number 2.
Response: The DSR DT thanks you for your comment. Please see the DSR DT response above for question number 2.		
Sweeny Cogeneration LP	No	The threshold for reporting what could be sabotage still leaves the door open for second guessing after-the-fact. For example, if graffiti is sprayed on a BES asset, the entity is to assume that the event is not to be reported. However, intent to harm the BES may be discovered at a later point with ramifications to the entity who did not report it. A solution may be to strengthen footnote 3 to both reporting tables, which makes an allowance to report if you cannot reasonably determine likely motivation of sabotage. If acceptable methods to provide justifiable evidence that reporting was NOT required, then this loophole may be corrected.
Response: The DSR SDT thanks you for your comment. The DSR SDT believes that the reporting of events supports the reliability of the BES. Sabotage usually is determined after the event is investigated and that Sabotage may be one aspect of a single event. The intent is to report events (per Thresholds of Reporting in Attachment 1) that have an impact on BES reliability. Attachment 1 has been updated per comments received.		
USACE	No	The DSR SDT should have defined sabotage since it helps the SDT working on CIP standards further define its action. Sabotage can be defined as the deliberate act of destruction, disruption, or damage of assets to impact the reliability of the BES.
Response: The DSR SDT thanks you for your comment. The DSR SDT believes that the reporting of events supports the reliability of the BES. Sabotage usually is determined after the event is investigated and that Sabotage may be one aspect of a single event. The intent is to report events (in Attachment 1) that have an impact on BES reliability. Attachment 1 has been updated per comments received.		
Consumers Energy	No	EOP-004 does not appear to address a reliability need. Reporting after-the-fact information such as that described in Impact Events does not do anything to improve Bulk Electric System reliability. Therefore, we recommend that CIP-001 be updated to address sabotage events, and that NERC otherwise rely on the statutory reporting to the DOE that is represented by OE-417 for any after-the fact information. The remainder of our comments reflects detailed comments on the posted draft, presuming that our objection

Organization	Yes or No	Question 3 Comment
		represented above will be disregarded.
Response: The DSR SDT thanks you for your comment. Providing event reporting information will start the event analysis process done by the current NERC Event Analysis Program. EOP-004-2 is the reporting vehicle to the ERO that will support the analysis phase of any event.		
Ameren	No	The SDT did not further define sabotage as directed by FERC, but instead created a new term that does not address the order. The Term Impact Event has no clarity or quantitative qualities by which an entity can determine what should be reported. The use of the phrase "has the potential to impact reliability" has such a vague scope, an auditor can interpret to mean any "off-normal" condition, which makes this standard impossible to comply with. The SDT should use the DOE definition of sabotage as follows: Sabotage - Defined by Department of Energy (DOE) as: An actual or suspected physical or Cyber attack that could impact electric power system adequacy or reliability Vandalism that targets components of any security system on the Bulk Electric System Actual or suspected Cyber or communications attacks that could impact electric power system adequacy or vulnerability, including ancillary systems which support networks (e.g. batteries) Any other event which needs to be reported by the Balancing Authority (Transmission Operations) to the Department of Energy. Sabotage can be the work of a single saboteur, a disgruntled employee or a group of individuals.
Response: The DSR SDT thanks you for your comment. The DSR SDT believes that the reporting of events supports the reliability of the BES. Sabotage usually is determined after the event is investigated and that Sabotage may be one aspect of a single event. The intent is to report events (per Thresholds of Reporting in Attachment 1) that have an impact on BES reliability. Attachment 1 has been updated per comments received. EOP-004-2 sets the minimum reporting requirements for events.		
Calpine Corp	No	The additional definition for “Impact Event” is unnecessary and does not provide useful clarification regarding actual reporting requirements. Sabotage, whatever the exact definition used, implies intent to damage or disrupt. The committee correctly notes that determination of actual intent is not always readily available. However, adding a general expansive definition encompasses all events that might disrupt the Bulk Electric System does not add clarity to the types of events that require reporting - which are listed in detail in Attachment 1.The issue can be more simply addressed by replacing the item “Human Intrusion” on Attachment 1, as follows: Event: Sabotage (note 3) Entity with Reporting Responsibility: All affected Responsible Entities listed

Organization	Yes or No	Question 3 Comment
		in the Applicability Section of this Standard. Threshold for Reporting: Forced Intrusions at a BES facility that have not been determined within the reporting period to be theft or vandalism that does not affect the operability of BES equipment. Note 3 For purposes of reporting under Attachment 1, reportable sabotage includes all forced intrusions at BES facilities that have potential to cause, or cause, any of the disturbance events listed in Attachment 1 and have not been determined to be theft or vandalism that did not result in any event listed in Attachment 1. Responsible Entities are not required to report incidents of theft or vandalism that do not result in disturbance events. This approach also eliminates the need to reference copper theft as a particular type of theft that does not require reporting.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event.". Attachment 1 has been updated per comments received. The DSR SDT believes that the reporting of events supports the reliability of the BES. Sabotage usually is determined after the event is investigated and that Sabotage may be one aspect of a single event. The intent is to report events (per Thresholds of Reporting in Attachment 1) that have an impact on BES reliability. Footnotes have been updated per comments received.		
CenterPoint Energy	No	CenterPoint Energy would agree if the definition for Impact Event was changed as suggested in the response to Question 2.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event.". Attachment 1 has been updated per comments received. The DSR SDT believes that the reporting of events supports the reliability of the BES.		
Duke Energy	No	Sabotage is still identified on the flowchart. Timeframes for reporting on Attachment 1 should be made consistent with DOE OE-417 reporting. Also on Attachment 1, the Threshold for Reporting on a Forced Intrusion Event should be Affecting BES reliability instead of At a BES facility.
Response: The DSR SDT thanks you for your comment. The DSR SDT has updated the flowchart. The DOE Form OE-417 is reviewed biennially by the DOE and can be updated or changed without NERC's involvement. The DSR SDT has taken into consideration the possible use of Form OE-417 to report events to NERC and agrees that this will fulfill EOP-004-2's reporting requirements. The DSR SDT has removed sabotage from the flowchart and has replaced it with: "Criminal act under federal jurisdiction."		

Organization	Yes or No	Question 3 Comment
Indeck Energy Services	No	The SDT hasn't defined sabotage. Attachment 1 does not do justice to the concept of sabotage. Sabotage should be defined as any intentional damage to BES facilities the causes a Reportable Disturbance, reportable event under DOE OE-417 or involves a bomb or bomb threat.
Response: The DSR SDT thanks you for your comment. The DSR SDT believes that the reporting of events supports the reliability of the BES. The intent is to report events (per Thresholds of Reporting in Attachment 1) that have an impact on BES reliability. Sabotage usually is determined after the event is investigated and that Sabotage may be one aspect of a single event. The DOE Form OE-417 is reviewed biennially by the DOE and can be updated or changed without NERC's involvement. The DSR SDT has taken into consideration the possible use of Form OE-417 to report events to NERC and agrees that this will fulfill EOP-004-2's reporting requirements.		
Exelon	Yes	Exelon agrees with the DSR SDT in that the currently proposed solution effectively addresses the intent of FERC Order 693 directive to both clarify the triggering event for an entity to take action and by deleting all references to "sabotage" in effect removes the very term that had no clear definition.
Response: Thank you for your comment.		
Georgia Transmission Corporation & Oglethorpe Power Corporation	Yes	We agree with the approach taken by the SDT.
Northeast Power Coordinating Council	Yes	It is more important to report suspicious events than to determine if an event is caused by sabotage before it gets reported.
Midwest Reliability Organization	Yes	Sabotage is usually associated with a malicious attack. Entities have always lacked the clinical expertise to determine if an event was malicious or not. The Impact Event bright line criteria clearly states what the minimum reporting requirements are.
Manitoba Hydro	Yes	"Impact event", The DSR SDT reasoning for this. 'A sabotage event can only be typically determined by law enforcement after the fact" is very creative and concise!
Response: The DSR SDT thanks you for your comment.		

Organization	Yes or No	Question 3 Comment
Independent Electricity System Operator	Yes	We agree since it is more important to report suspicious events than to determine if an event is caused by sabotage before it gets reported.
Response: The DSR SDT thanks you for your comment.		
ISO New England, Inc	Yes	We agree since it is more important to report suspicious events than to determine if an event is caused by sabotage before it gets reported.
Ingleside Cogeneration LP	Yes	Sabotage cannot be confirmed until after the fact, so we support this initiative.
Bonneville Power Administration	Yes	
Western Electricity Coordinating Council	Yes	
PPL Supply	Yes	
PSEG Companies	Yes	
Dominion	Yes	
SPP Standards Review Group	Yes	
FirstEnergy	Yes	
SERC OC Standards Review Group	Yes	
PJM Interconnection LLC	Yes	
Southern Company	Yes	
SRP	Yes	

Organization	Yes or No	Question 3 Comment
We Energies	Yes	
SDG&E	Yes	
City of Tallahassee (TAL)	Yes	
Lakeland Electric	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
United Illuminating Co	Yes	
American Municipal Power	Yes	Well done.
Liberty Electric Power LLC	Yes	
Arkansas Electric Cooperative Corporation	Yes	
American Electric Power	Yes	
New Harquahala Generating Co.	Yes	
Platte River Power Authority	Yes	
BGE	Yes	No comments.
Alliant Energy	Yes	
ExxonMobil Research and Engineering	Yes	

Organization	Yes or No	Question 3 Comment
PPL Electric Utilities	Yes	
Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
American Transmission Company	Yes	
Constellation Power Generation	Yes	
Georgia System Operations Corporation	Yes	None.
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	
Brazos Electric Power Cooperative	Yes	
Response: The DSR SDT thanks you for your response. Several commenters proposed revisions to the definition, and after deliberation the SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event". Attachment 1 has been updated per comments received. The DSR SDT believes that the reporting of events supports the reliability of the BES.		

4. Do you agree with the proposed applicability of EOP-004-2 shown in Section 4 and Attachment 1 of the standard? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: The SDT believes that it has properly identified registered entities that may potentially have events and the appropriate types of events. A Registered Entity is only required to submit an events report for events listed in Attachment 1 if the registered entity was affected by the event. If an event occurs, only affected Registered Entities listed in Attachment 1 are required to submit a report on the event. The SDT believes that the industry will gain valuable information from having different perspectives of a single event. Differing viewpoints on the same event will provide for better clarity to all parties on the actual impact to the bulk electric system. The SDT would like to point out that reporting of events is from the time of identification not the time of the event. In response to the comments received, the SDT has made numerous enhancements to Attachment 1. **These revisions include:**

- **Added new column "Submit Attachment 2 or DOE OE-417 Report to:" which references Part 1.3 and provide the time required to submit the report.**
- **Combined Parts A and B into one table and reorganized it so that the events are listed in order of reporting times (either one hour or 24 hours)**
- **Removed references to "Impact Event" and replaced with the specific language for the event type in the "Entity with Reporting Responsibility". For example, replaced "Impact Event" with "automatic load shedding".**

The ERO and the RE were added as applicable entities to reflect CIP-002 applicability to this standard.

Organization	Yes or No	Question 4 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation	No	We do not believe that GO, TO, TSP, DP, or LSE should be included in the applicability of this standard. It is our opinion that the reporting requirements lie primarily with the applicable operator and should be limited as such. We recommend modifications as discussed in our response to question 6 to clearly define what types of events each Responsible Entity needs to prepare for. Currently, it seems that multiple entities are being required to report the same event for some events where only one entity should have a reporting responsibility. However, NERC should not decide which one entity should report a given event. The entities should have the flexibility to create a process which allows for coordination and communication at a local level and to work out with neighboring entities who might ultimately report events to the applicable

Organization	Yes or No	Question 4 Comment
		organizations.
Response: Thank you for your comments. The SDT disagrees that the operators are the only entities with obligations to report; owners and users may have very credible and valuable information relating to events. Such information may be extremely beneficial in developing lessons learned and analyzing events. Your suggestion to allow for local coordination and communication is a practical suggestion and the standard allows for it.		
Northeast Power Coordinating Council	No	Disagree with the following inclusion/exclusion of several entities: a. The applicable entities listed in Section 4 capture all the entities that are assigned a reporting responsibility in Attachment 1 of the standard. While some events in Attachment 1 have specific entities identified as responsible for reporting, certain events refer to the entities listed in specific standards (e.g. CIP-002) as the responsible entities for reporting. The latter results in IA, TSP and LSE (none of which being specifically identified as having a reporting responsibility) being included in the Applicability Section. NERC should be included in the Applicability Section as it is an applicable entity identified in CIP-002-3. b. If the above approach was not strictly followed, then suggest the SDT review the need to include IA, TSP and LSE since they generally do not own any Critical Assets and hence will likely not own any Critical Cyber Assets.
Response: The DSR SDT thanks you for your comment. The SDT believes it needs to follow the requirements of the standards as they currently apply. Since these entities are applicable to the underlying standards identified in Attachment 1, then they will be subject to reporting. If those standards are modified to remove the applicability to these functional registrations, then the appropriate SDT can modify the applicability of this standard. The SDT has reviewed the CIP-002-3 standard and has included the ERO and the RE in this standard.		
Pacific Northwest Small Public Power Utility Comment Group	No	We believe that facilities used in the local distribution of electric energy should be excluded from these requirements due the language of 16 U.S.C. ? 824o(a)(1) and 16 U.S.C. ? 824o(i)(1).
Response: The DSR SDT thanks you for your comment. The SDT constructed Attachment 1 based upon the existing requirements in the various reliability standards and established reporting obligations. The information about events and the analysis of those events will be useful to all owners, operators, and users of the bulk power system. The SDT has clarified the reporting requirement such that only those affected by the event are required to submit a report.		
PSEG Companies	No	The PSEG Companies believe the defining language, roles and responsibilities outlined in Attachment 1 are unclear and inconsistent. For example fuel supply emergency reporting footnote 2 “Report if problems with the fuel supply chain result in the projected need for emergency actions to manage reliability” attempts to clarify the condition for reporting but does not. Whose “emergency actions” are being referred to in the footnote? It is not clear if those actions would be related to the specific station or the overall Bulk Electric

Organization	Yes or No	Question 4 Comment
		System (BES). Can this be interpreted to imply a gas supply issue to one generating station as the result of pipeline maintenance, or local pressure issues would also requiring reporting? The PSEG Companies believe the definition of a fuel supply emergency needs to be more specific and less open to broad interpretation. In addition, the "Time to Submit Report" section of attachment 1 has a significant number of changes from the previous version. Accelerating the twenty four (24) hour to one (1) hour requirement for submitting the reports for several of the events takes resources away from managing the actual event. For the above comments failure to submit a report within 1 hour is a high or severe VSL for a fuel supply emergency. This approach seems inconsistent with ensuring the operation and reliability of the BES. One (1) hour reporting, in most cases, is not adequate time to compile the needed information, prepare report, ensure the accuracy, submit, and simultaneously manage the actual event. We recommend 24 hour reporting for: Damage or destruction to BES, Fuel Supply Emergency, Forced Intrusion, and Risk to BES equipment sections of Attachment 1.
Response: The DSR SDT thanks you for your comment. The SDT appreciates the observation on Fuel Supply Emergency and has adjusted Attachment 1 to address it. Reporting under the standard requires that the Registered Entity provide what information it has at the time of the report. The report may not provide the entire record or identification of the event. If the Registered Entity desires to submit an updated report, it may choose to do so; but there is no obligation to do so. The DSR SDT has significantly revised Attachment 1. We have removed the timing column and replaced it with more specific information regarding which form to submit and to whom the report is to be submitted. All events are now to be reported within 24 hours with the exception of Destruction of BES equipment, Damage or destruction of Critical Assets and Damage or destruction of Critical Cyber Asset events, Forced Intrusion, Risk to BES equipment and Detection of a reportable Cyber Security Incident. These events are to be reported within 1 hour. Notification of law enforcement (per Requirement R1, Part 1.3.2) is only required for these events. The background section of the standard provides guidance with respect to reporting events to law enforcement. For clarity, the DSR SDT has added the following sentence to the first paragraph under the heading "Law Enforcement Reporting": "These are the types of events that should be reported to law enforcement." The entire paragraph is: o "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES."		
Dominion	No	1) Several of the events require filing a written Impact Event report within one hour. System Separation, for example, is going to require an "all hands on deck" response to the actual event. We note that the paragraph above Attachment 1, Part A indicates that a verbal report would be allowed in certain circumstances, but this

Organization	Yes or No	Question 4 Comment
		is the same issue with the formal report in that the system operators are concerned with managing the event and not the reporting requirements. Another example would be the Loss of Off-site power to a nuclear generating plant. Suggest reconsideration of one hour reporting requirement for events requiring extensive operator actions to mitigate; 2) Several events seem to have the "Threshold for Reporting" contained in footnotes rather than in the table. For example, Damage or destruction of BES equipment - Footnote 1, Fuel supply emergency - Footnote 2, etc.) Suggest moving the actual threshold into the table; 3) If one hour reporting remains as indicated in Attachment 1; align/rename events similar to that of the 'criteria for filing' events listed in DOE OE-417 for consistency.
Response: Thank you for your comment. Reporting under the standard requires that the Registered Entity provide what information it has at the time of the report. The report may not provide the entire record or identification of the event. If the Registered Entity desires to submit an updated report, it may choose to do so; but there is no obligation to do so. Based upon comments received, the SDT has updated the time reporting requirements in Attachment 1. Most events are to be reported within 24 hours. The DSR SDT has retained a one-hour reporting requirement for those events the DSR SDT believes are the types of event that would be typically reported to law enforcement and are of a more urgent nature.		
SPP Standards Review Group	No	While the SDT has recognized the issue of applicability to GO/TO in its background information with the Unofficial Comment Form, we still do not feel comfortable with the GO/TO being listed as a responsible entity when in fact it may be days before they become aware of an event worthy of reporting. If the GOP/TOP makes the report, are the GO/TO still responsible for filing a report? If the GOP/TOP do not file the report, would the GO/TO then be non-compliant? This issue appears to put additional risk on the GO/TO over which they have no control. We need some mechanism to eliminate unnecessary risk while at the same time ensuring that we have coverage for the BES. Perhaps this could be done through delegation agreements between the entities involved or through allowances within the standard itself. For example, could the phrase "appropriate parties in the Interconnection" as currently contained in CIP-001-1, R2 be incorporated into the standard to basically replace GO/TO?
Response: The DSR SDT thanks you for your comment. The SDT believes that it has properly identified registered entities that may potentially have events and the appropriate types of events. A Registered Entity is only required to submit an events report for events listed in Attachment 1 if the registered entity was affected by the event. If an event occurs, only affected Registered Entities listed in Attachment 1 are required to submit a report on the event. Having reports from different entities for the same event may provide a more complete understanding of the event.		
FirstEnergy	No	1. Attachment 1, Part A - Energy Emergency requiring Public appeal for load reduction - In the current draft Standard, the applicability has been revised from an RC and BA to "initiating entity." We can't see where the GO/GOP would ever make this determination. Needs to be clarified.

Organization	Yes or No	Question 4 Comment
		2. Attachment 1, Part A - Energy Emergency requiring system-wide voltage reduction - In the current draft Standard, the applicability has been revised from an RC, TO, TOP, and DP to "initiating entity." We can't see where the GO/GOP would ever make this determination. Needs to be clarified. 3. Attachment 1, Part A - Voltage Deviations on BES facilities - A GOP may not be able to make the determination of a +/- 10% voltage deviation for ≥ 15 continuous minutes, this should be a TOP RC function only. 4. Attachment 1, Part A - Loss of offsite power (LOOP) classification should not apply to nuclear generators. The impact of a LOOP is dependent on the design of the specific nuclear unit and may not necessarily result in a unit trip. If a LOOP did result in a unit trip, the NRC requires notification by the nuclear GO/GOP via the Emergency Notification System (ENS), and time allowed for that notification (1 hour, 4 hours, 8 hour, or none at all) is, as mentioned above, dependent on the design of the plant. We believe it would be beneficial if consideration were given to coordinating reporting requirements for nuclear units with existing required notifications to the NRC to avoid duplication of effort. 5. Attachment 1 should align NERC Standard NUC-001 concerning the importance of ensuring nuclear plant safe operation and shutdown. If a transmission entity experiences an event that causes a loss of off-site power as defined in the nuclear generator's Nuclear Plant Interface Requirements, then the responsible transmission entity should report the event within 24 hours after occurrence. Also, for clarity "grid supply" should be replaced with "source" to ensure that notification occurs on a loss of one or multiple sources to a nuclear power plant. 6. Attachment 1, Part A - Damage or destruction of BES equipment. See Nuclear comments on question 17 below. 7. Attachment 1, Part B - Forced intrusion at a BES facility. See Nuclear comments on question 17 below. 8. Attachment 1, Part B - Risk to BES equipment from a non-environmental physical threat. What constitutes a "risk" to the reporting entity is still somewhat ambiguous, and although the DSR SDT has provided some examples, without more specific criteria for this event the affected entity will have difficulty in determining within 1 hour if a report is necessary. Also, see Nuclear comments on question 17 below.
Response: The DSR SDT thanks you for your comment. As a general note, the Applicability section of the standard includes each entity that will be responsible for reporting an event. Attachment 1 has a column "Entity with Reporting Responsibility" to indicate the appropriate entity that is required to report under this standard. For items 1-3 above, the GO or GOP will not be the likely deficient or initiating entity. This will most likely be the BA, TOP or the RC. For item 4, the LOOP event is to be reported by the TO and TOP, not the nuclear plant. For item 5, the TO and TOP are to report within 24 hours. The DSR discussed using "source", however this indicates a single source whereas "supply" encompasses all sources. For items 6, 7 and 8, please see response to Question 17 comments.		
SERC OC Standards Review Group	No	We agree that all of the entities listed should be responsible for reporting an event, provided they own BES assets, but guidance should be given for which entity in Attachment 1 actually files the report to avoid duplication for a single event.

Organization	Yes or No	Question 4 Comment
Response: The DSR SDT thanks you for your comment. The SDT believes that it has properly identified registered entities that may potentially have events and the appropriate types of events. A Registered Entity is only required to submit an events report for events listed in Attachment 1 if the registered entity was affected by the event. If an event occurs, only affected Registered Entities listed in Attachment 1 are required to submit a report on the event. Having reports from the different entities may provide valuable information on understanding the event.		
PJM Interconnection LLC	Yes	1. We agree that the entities listed should be responsible for ensuring events are reported, provided they own BES assets, but more guidance should be provided on which entity in Attachment 1 should actually file the report to avoid multiple entities reporting a single event. Current Attachment 1 results in significant duplicate reporting. 2. Although the applicable entities listed in Section 4 capture all entities that are assigned a reporting responsibility in Attachment 1, some events in Attachment 1 refer to entities applicable under a different standard (e.g CIP-002) as the responsible entities for reporting. This results in IA, TSP, and LSE (none of which, generally own Critical Assets and hence not likely own CCAs) as being responsible for reporting an event. We urge the SDT review the need to include IA, TSP, and LSE in applicable entities. Also, why is NERC an applicable entity in CIP-002-3 but not in this standard?
Response: Thank you for your comments. 1. The "Entity with Reporting Responsibility" column of Attachment 1 indicates who is responsible for submitting reports for each event type. It is expected that multiple reports will be received for the same event. Each entity experiencing the event may see something different. This reporting will allow for a more robust analysis process after the fact. 2. The IA. TSP and LSE are included as applicable entities for EOP-004 only because they are applicable under CIP-002. The only events that these entities are required to report are related to cyber assets. The ERO and the RE were added as applicable entities for consistency with CIP-002.		
SRP	No	The threshold for Reporting is broad, vague and repetitive. "Three or more BES Transmission Elements" is vague and could be interpreted as 3 breakers in a large system.
Response: The DSR SDT thanks you for your comment. Based upon comments received, the SDT has modified Attachment 1 accordingly.		
We Energies	No	Attachment 1: From the NERC Glossary, an Energy Emergency: A condition when a Load-Serving Entity has exhausted all other options and can no longer provide its customers' expected energy requirements. The first four events listed can only apply to an LSE. Loss of Firm Load for >15 Minutes: By the NERC Glossary definitions of DP and LSE, the LSE would seem to be more appropriate than the DP. With the proposed one-hour reporting requirement, the industry would be undertaking significant regulatory risk with respect to timely reporting. The requirement to report the crime-based events in the field within one

Organization	Yes or No	Question 4 Comment
		hour, as shown in Attachment 1 Part A or Part B will be difficult. We could even discover a theft in progress with the suspect trapped inside the substation fence and the police attempting to make a safe arrest. We need more reporting time, especially when they have not even resulted in an outage. The industry is keenly interested in understanding the benefit of taking on the risk. What analysis, insight, warnings or recommendations would the ES-ISAC provide to the reporting entity, the industry or to law enforcement agencies in the hours after such an incident is reported? Note too that DOE requires reporting of a physical attack within one hour only when it "causes a major interruption or major negative impact on critical infrastructure facilities or to operations." In lesser cases, the entity gets up to six hours if it "impacts electric power system reliability." DOE has said that it is not interested in copper theft unless it causes one of these events. If the SDT is working to ensure consistency of reporting requirements, please consider DOE requirements too. Meeting the reporting deadline will mean that available resources in the control center will be devoted to ensuring the report is filed on time instead of making the site safe and arranging for prompt repair. It may even mean that law enforcement won't be contacted until the forms are filed with the ES-ISAC. The exception contained in footnote #1 of Attachment 1 with respect to copper theft is not an exception at all. The majority of copper theft from substations is, in fact, such grounding connectors which may or may not render the protective relaying inoperative. You could end up receiving reports from all over the USA, Canada and Mexico, mostly on Monday mornings as weekend copper thefts are discovered. Attachment 1 Part A table also contains redundancies. One of the cells reads, "Damage or Destruction of Critical Asset." One cannot destroy something without damaging it first. Consequently, it is sufficient to simply say, "Damage to a Critical Asset." Apply to all cells with the same phrase.

Response: Thank you for your comments. Only Registered Entities affected by the event have to submit a report. Entities that were not affected by the event are under no obligation to submit a report. Registered Entities are to report what information they have at the submission timeline. The SDT recognizes that a final report may not be possible at the submission time. The reporting requirements are consistent with the current reporting requirements of the various authorities. The one hour reporting times are listed as "one hour within recognition of an event". This should be sufficient to allow the reporting entity time to submit the report after the event has been recognized. Based upon comments received from many stakeholders, the SDT has modified Attachment 1. The background section of the standard provides guidance with respect to reporting events to law enforcement. For clarity, the DSR SDT has added the following sentence to the first paragraph under the heading "Law Enforcement Reporting": "These are the types of events that should be reported to law enforcement." The entire paragraph is:

o "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES."

Organization	Yes or No	Question 4 Comment
Exelon	No	Remove LSE. As has been determined in previous filings, FERC has ruled that asset owning DP's must be registered as LSE's. The standard as proposed is applicable to DP's. This addresses any concern with a "reliability gap" for reporting events that could have an adverse material impact to the BES. See FERC Docket RC-07-4-003, -6-003, -7-003 paragraphs 24 and 25. "The Commission approves … revisions to the Registry Criteria to have registered distribution providers also register as the LSE for all load directly connected to their distribution facilities… The registration of the distribution provider as the LSE for all load directly connected to its distribution facilities is for the purpose of compliance with the Reliability Standards. As NERC explains, distribution providers have both the infrastructure and access to information to enable them to comply with the Reliability Standards that apply to LSEs… The Commission finds that, based on these facts, NERC acted reasonably in determining that the distribution provider is the most appropriate entity to register as the LSE for the load directly connected to its distribution facilities." Attachment 1, Part A – Energy Emergency requiring Public appeal for load reduction – In the current draft Standard, the applicability has been revised from an RC and BA to "initiating entity." As a GO/GOP, I cannot see any event where a GO/GOP would be the responsible "initiating entity" or have the ability to determine an "Energy Emergency." Suggest revising back to specific entities that would be likely responsible for this action (e.g., RC, BA, TOP). Attachment 1, Part A – Energy Emergency requiring system-wide voltage reduction – In the current draft Standard, the applicability has been revised from an RC, TO, TOP, and DP to "initiating entity." As a GO/GOP, I cannot see any event where a GO/GOP would be the responsible "initiating entity" or have the ability to determine an "Energy Emergency" related to system-wide voltage reduction. Suggest revising back to specific entities that would be likely responsible for this action. Attachment 1, Part A – Voltage Deviations on BES facilities - A GOP may not be able to make the determination of a +/- 10% voltage deviation for ≥ 15 continuous minutes, this should be a TOP RC function only. Attachment 1, Part A – Loss of off-site power (grid supply) affecting a nuclear generating station – this event applicability should be removed in its entirety for a Nuclear Plant Generator Operator. The impact of loss of off-site power on a nuclear generation unit is dependent on the specific plant design, if it is a partial loss of off-site power (per the plant specific NPIRs) and may not result in a loss of generation (i.e., unit trip). If a loss of off-site power were to result in a unit trip, an Emergency Notification System (ENS) would be required to the Nuclear Regulatory Commission (NRC). Depending on the unit design, the notification to the NRC may be 1 hour, 8 hours or none at all. Consideration should be given to coordinating such reporting with existing required notifications to the NRC as to not duplicate effort or add unnecessary burden on the part of a Nuclear Plant Generator Operator during a potential transient on the unit. In addition, if the loss of off-site power were to result in a unit trip, if the impact to the BES were ≥2,000 MW, then required notifications would be made in accordance with the threshold for reporting for Attachment 1, Part A – Generation Loss. However, to align with the importance of ensuring nuclear plant safe operation and shutdown as implemented in NERC Standard NUC-001, if a transmission entity experiences an event that causes an unplanned loss of off-site power (source) as defined in the applicable Nuclear Plant Interface Requirements, then the responsible

Organization	Yes or No	Question 4 Comment
		transmission entity should report the event within 24 hours after occurrence. In addition, replace the words "grid supply" to "source" to ensure that notification occurs on an unplanned loss of one or multiple sources to a nuclear power plant. Suggest rewording as follows (including replacing the words "grid supply" to "source" and adding in the word "unplanned" to eliminate unnecessary reporting of planned maintenance activities in the table below): Event Entity with Reporting Responsibility Threshold for Reporting Time to Submit Report Unplanned loss of off-site power to a Nuclear generating plant (source) as defined in the applicable Nuclear Plant Interface Requirements (NPIRs) Each transmission entity responsible for providing services related to NPIRs (e.g., RC, BA, TO, TOP, TO, GO, GOP) that experiences the event causing an unplanned loss of off-site power (source) Unplanned loss of off-site power (source) to a Nuclear Power Plant as defined in the applicable NPIRs. Within 24 hours after occurrence
Response: Thank you for your comments. The SDT constructed Attachment 1 based upon the existing requirements in the various reliability standards and established reporting obligations. The LSE is an applicable entity under CIP-002 and CIP-008. The types of events that you list are not applicable to a GO/GOP. The Applicability section of the standard lists each entity that is applicable for some portion of the standard. The information in Attachment 1 specifies which entity must report for which type of event. The loss of off-site power is only applicable to the TO and TOP and not the nuclear plant operator.		
SDG&E	No	SDG&E recommends that “Load Serving Entity,” “Transmission Service Provider,” and “Interchange Authority” be removed from the proposed applicability shown in Section 4. These entities do not own assets that could have an impact on the Bulk Electric System. Additionally, none of these entities is listed as an “Entity with Reporting Responsibility” in Attachment 1. Finally, “Transmission Service Provider” is covered by either “Transmission Owner” or “Balancing Authority,” which are entities also listed in the proposed Applicability section, and “Load Service Entity” and “Interchange Authority” are covered by “Balancing Authority.”
Response: Thank you for your comments. The SDT constructed Attachment 1 based upon the existing requirements in the various reliability standards and established reporting obligations. The LSE, TSP and IC are applicable entities under CIP-002 and CIP-008.		
United Illuminating Co	No	Will an entity be required to develop an Operating Process for every Impact Event in Attachment 1, or only those events that apply to its Registration. For example, does a DP require evidence of an Operating Process/Procedure for Voltage Deviations on a BES Facility? Some items in Attachment 1 state “Each RC, BA, TOP, DP that experiences the Impact Event” (such as Loss of Firm Load). DP’s may have arranged with TOP and RC to communicate the event to TOP who then will file the NERC report and OE-417. The requirements in the Standard would allow for this as long as the Operating Plan documents it. Attachment 1 though can be interpreted that this arrangement would not be allowed and each entity shall file its own and separate report. UI suggests that Attachment 1 be modified to allow for an Entities Operating Plan to rely on another Entity making the final communication to NERC. “Each RC, BA, TOP, DP that experiences the Impact Event, either individually or combined on a single filing”

Organization	Yes or No	Question 4 Comment
Response: The DSR SDT thanks you for your comment. The SDT believes that it is not necessary to develop a separate Operating Process for each event, unless the company requires it. The SDT feels that any Registered Entity affected by an event needs to submit a report. The SDT believes that the Registered Entity can utilize any resource it has available to complete the reporting obligations and does not believe that Attachment 1 inhibits any options from being used. Based upon comments received, the SDT has decided to remove the definition of Impact Event from the standard and leave as identified through Attachment 1.		
American Municipal Power	No	No, I do not agree. The DP and LSE functions should be removed.
Response: The DSR SDT thanks you for your comment. The SDT constructed Attachment based upon the existing requirements in the various reliability standards and established reporting obligations. This information will be useful to all owners, operators, and users of the bulk power system. The DP and LSE are applicable entities under CIP-002 and CIP-008.		
Sweeny Cogeneration LP	No	In Attachment 1, Generator Operators who experience a ± 10% sustained voltage deviation for ≥ 15 continuous must issue a report For externally driven events, the GOP will have little if any knowledge of the cause or remedies taken to address it. We believe the language presently in EOP-004-1 is satisfactory that any "action taken by a Generator Operator" that results in a voltage deviation has to be reported by the GOP.
Response: Thank you for your comment. Reporting of events is an obligation of affected Registered Entities. Registered Entities who do not experience an event do not have any reporting obligations.		
Independent Electricity System Operator	No	We disagree with the following inclusion/exclusion of several entities: a. We assess that the applicable entities listed in Section 4 capture all the entities that are assigned a reporting responsibility in Attachment 1 of the standard. While some events in Attachment 1 have specific entities identified as responsible for reporting, certain events refer to the entities listed in specific standards (e.g. CIP-002) as the responsible entities for reporting. The latter results in IA, TSP and LSE (none of which being specifically identified as having a reporting responsibility) being included in the Applicability Section. If our reasoning is correct, we question why NERC was dropped from the Applicability Section as it is an applicable entity identified in CIP-002-3. b. If the above approach was not strictly followed, then we'd suggest the SDT review the need to include IA, TSP and LSE since they generally do not own any Critical Assets and hence will likely not own any Critical Cyber Assets.
Response: The DSR SDT thanks you for your comment. The SDT believes it needs to follow the requirements of the standards as they currently apply. Since these entities are applicable to the underlying standards identified in Attachment 1, they will be subject to reporting. If those standards are modified to remove the applicability to these functional registrations, then the appropriate SDT can modify the applicability of this standard. The SDT has reviewed the CIP-002-3		

Organization	Yes or No	Question 4 Comment
standard and have added the ERO and the RE as applicable entities. If an IA, TSP or LSE does not own Critical Assets nor Critical Cyber Assets, then they will have nothing to report under this standard.		
Ameren	No	The 1 hour reporting requirement, as reference in Attachment 1 is inappropriate. In the event an "Impact Event" were to be discovered the Responsible Entity should focus on public and personnel safety. The reporting requirement should read "Within 1 hour or as soon as conditions are deemed to be safe." This statement would be applicable to "Damage or destruction of Critical Asset" The SDT should not put personnel in the position of choosing to either comply with NERC or address public or co-worker safety. The Time to Submit Report states "within 1 hour after occurrence is identified" This gives an auditor a wide area to question. If personnel report the occurrence 1 hour after identified, but 24 hours after it occurred, we are subject to the personal beliefs of the auditor that the event was not identified 24 hours ago, and reported 24 hours late. This will also be difficult to measure as the operator will have to document in the plant log the time the event was identified, while possibly dealing with Emergency Conditions. In the Note above the Actual Reliability Impact Table, the SDT identifies that under certain conditions, NERC / RRO staff may not be available for continuous 24 hour reporting. The SDT should consider the same stipulations apply to operating personnel and they should not be held to a higher standard that NERC / RRO.
Response: Thank you for your comment. The reporting timelines for most events have been changed from 1 hour to 24 hours. The events that retain the one hour requirement are those that are more closely related to sabotage type events. The DSR SDT chose the wording “upon identification of an event” to allow for cases where an event may not be recognized for some time due to an asset being in a remote location for example. It is expected that an auditor will follow what is written in the standard rather their personal preference. In the note above Attachment 1, it does not state that the ERO may not be available. This note is related to R3.3 of EOP_004-1 and provides for delayed reporting by an entity during storms or other such instances.		
ISO New England, Inc	No	We disagree with the following inclusion/exclusion of several entities: a. We acknowledge that the applicable entities listed in Section 4 capture all the entities that are assigned a reporting responsibility in Attachment 1 of the standard. While some events in Attachment 1 have specific entities identified as responsible for reporting, certain events refer to the entities listed in specific standards (e.g. CIP-002) as the responsible entities for reporting. The latter results in IA, TSP and LSE (none of which being specifically identified as having a reporting responsibility) being included in the Applicability Section. If our reasoning is correct, we question why NERC was dropped from the Applicability Section as it is an applicable entity identified in CIP-002-3. b. If the above approach was not strictly followed, then we’d suggest the SDT review the need to include IA, TSP and LSE since they generally do not own any Critical Assets and hence will likely not own any Critical Cyber Assets. c. There is still significant duplicate reporting included. For instance, why do both the RC and TOP to report

Organization	Yes or No	Question 4 Comment
		voltage deviations? As written, a voltage deviation on the BES would require both to report. The same would hold true for IROLs. Perhaps IROLs should only be reported by the RC to be consistent with the recently FERC approved Interconnection Reliability Operating Limit standards.
Response: The DSR SDT thanks you for your comment. (a) The SDT believes it needs to follow the requirements of the standards as they currently apply. Since these entities are applicable to the underlying standards identified in Attachment 1, then they will be subject to reporting. If those standards are modified to remove the applicability to these functional registrations, then the appropriate SDT can modify the applicability of this standard. The SDT has reviewed the CIP-002-3 standard and have added the ERO and the RE as applicable entities. (b) The IA, TSP and LSE are included in the Applicability only as it relates to CIP-002 events listed in the table. (c) The DSR SDT has removed the RC from "Voltage Deviations" and the TOP from the IROL to address the comment.		
Calpine Corp	No	Expanding the current applicability of CIP-001-1 and EOP-004-1 to the GO function is unnecessary and will result in numerous duplicate reports, self-certifications, spot checks, and audits reviews, with no benefit to the reliability of the Bulk Electric System. The GOP is the appropriate applicable entity for generation facilities.
Response: The DSR SDT thanks you for your comment. The SDT believes that it has properly identified registered entities that may potentially have events and the appropriate types of events. A Registered Entity is only required to submit an events report for events listed in Attachment 1 if the registered entity was affected by the event. If an event occurs, only affected Registered Entities listed in Attachment 1 are required to submit a report on the event. Having reports from the different entities may provide valuable information on understanding the event. The SDT would like to point out that reporting of events is from the time of identification not the time of the event.		
Occidental Power Marketing	No	Load Serving Entities that do not own or operate BES assets (or assets that support the BES) should not be included in the Applicability. The SDT includes LSEs based on CIP-002; however, if the LSE does not have any BES assets (or assets that support the BES), CIP-002 should also not be applicable because the LSE could not have any Critical Assets or Critical Cyber Assets. It is understood that the SDT is trying to comply with FERC Order 693, Sections 460 and 461; however, Section 461 also states: "Further, when addressing such applicability issues, the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate to address these concerns." A qualifier in the Applicability of EOP-004-2 that would include only LSEs that own, operate or control BES assets (or assets that support the BES) would seem appropriate and acceptable to FERC.
Response: The DSR SDT thanks you for your comment. The SDT believes it needs to follow the requirements of the standards as they currently apply. Since these entities are applicable to the underlying standards identified in Attachment 1, then they will be subject to reporting. The LSE is an applicable entity under CIP-002 and CIP-008. If those standards are modified to remove the applicability to these functional registrations, then the appropriate SDT can modify the applicability of this standard.		

Organization	Yes or No	Question 4 Comment
American Transmission Company	No	First, under Part A, the reporting requirement for three or more BES Transmission Elements will create confusion. The NERC definition for an Element is: "Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An element may be comprised of one or more components." This could be interpreted to be three potential transformers on a bus section; therefore, any bus section would require a report. It is suggested that this be reworded to indicate three or more BES transmission lines, bus sections, or transformers. Second, under Part A, the reporting requirement for "Damage or destruction of BES equipment" is too broad and needs to be modified. For example, an output contact on a relay could be damaged unintentionally during routine testing resulting in a reportable event. It is suggested that the list of BES equipment and full intent of this be further defined in the footnote. The intent needs to be clarified, such as "events that have an immediate and significant impact to the stability or reliability of the BES." Third, under Part A, the reporting requirement for "Damage or destruction of a Critical Cyber Asset" is too broad and needs to be modified. For example, an output contact on a relay could be damaged unintentionally during routine testing resulting in a reportable event.
Response: Thank you for your comments. (1) The event "Transmission Loss" has been modified to remove the word Element. This now refers to Facilities. 2. If damage to a contact on a relay poses a reliability threat, then it should be reported. There is a footnote for this the type of event that helps clarify what is expected to be reported. It states: 1 BES equipment that: i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii) Damaged or destroyed due to intentional or unintentional human action which removes the BES equipment from service. Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative). 3. This relates only to Critical Cyber Assets identified under CIP-002. If a relay contact is identified under CIP-002 as a Critical Cyber Asset, then its damage or destruction should be reported.		
Ingleside Cogeneration LP	No	Owners and operators of facilities whose total removal from the BES would not meet any reportable threshold under Attachment 1 should not have to create and maintain Operating documents. The same would be true of any LSE, TSP, or IA that does not oversee any Critical Cyber Assets as identified under CIP-002. A statement to that effect could be made in Section 4 of EOP-004-2.
Response: Thank you for your comments. Requirements under Standards can only be enforced against Registered Entities, not whether or not they own or operate certain types of assets. The SDT believes it needs to follow the requirements of the standards as they currently apply. Since these entities are applicable to the underlying standards identified in Attachment 1, then they will be subject to reporting. If those standards are modified to remove the applicability to these		

Organization	Yes or No	Question 4 Comment
functional registrations, then the appropriate SDT can modify the applicability of this standard.		
Duke Energy	No	Section 4 is fine, but on Attachment 1, Entity with Reporting Responsibility should just identify "Initiating entity" for every Event, as was done with the first three Events. That way you avoid errors in leaving an entity off, or including an entity incorrectly (as was done with the GOP on Voltage Deviations).
Response: Thank you for comment. The SDT considered your comment in the development of Attachment 1 decided against including the Initiating Entity designation as it was not appropriate in those cases. Based upon comments received, the SDT has modified Attachment 1 accordingly.		
Constellation Power Generation	No	As stated in comments to earlier versions of EOP-004-2, CPG disagrees with the inclusion of Generator Owners. Since one of the goals in revising this standard is to streamline impact event reporting obligations, Generator Operators are the appropriate entity to manage event reporting as the entity most aware of events should they arise. At times, the information required to complete a report may warrant input from entities connected to generation, but the generator operator remains the best entity to fulfill the reporting obligation.
Response: Thank you for your comment. The SDT has chosen not to distinguish between Registered Entities as far as reporting. Instead the SDT has included Registered Entities which are involved or potentially involved in the types of events. Registered Entities need to recognize that only entities that are affected by the event have the reporting obligation.		
Georgia System Operations Corporation	No	We do not agree that this standard assigns clear responsibility for reporting. It seems that multiple entities are being required to report the same event for some events. Only one entity should report. See comments later regarding Attachment 1. NERC should not decide which ONE entity should report. The entities should be allowed to decide this (and include it in the Impact Event Operating Plan) and to let NERC or the region know who will report (or give them a copy of the plan).
Response: Thank you for your comment. The SDT has chosen not to distinguish between Registered Entities as far as reporting. Instead the SDT has included Registered Entities which are involved or potentially involved in the types of events. Registered Entities need to recognize that only entities that are affected by the event have the reporting obligation.		
Indeck Energy Services	No	Voltage Deviations should not be reportable by GOP. That's why we have TOP's. Damage or destruction of BES equipment should be reportable only if it causes or could cause a Reportable Disturbance, reportable DOE OE-417 event or sabotage (as defined above). Otherwise, an auditor could require reporting of a relay failure caused by human error even though the relay was in test mode and no BES impact was experienced. This category could be dropped in favor of the next one, damage to Critical Asset. Fuel Supply Emergency needs a definition. For natural gas, various conditions could be referred to as

Organization	Yes or No	Question 4 Comment
		emergencies, but unless they actually affect generation, they should not need to be reported. Fuel Supply Emergencies that cause a Reportable Disturbance or reportable DOE OE-417 event should be reported. It is unclear why Forced Intrusion should be reportable under EOP-004. If it causes a problem, it will be reportable as another category and is one more unpreventable event. Forced Intrusion isn't, in many cases, as the exceptions try to define, an impact event at all, but could be a cause, which would be reported as the cause of an impact event. Risk to BES Equipment is not well defined. It should be expanded to Risk to BES Equipment from a non-environmental physical threat within a reasonable distance of the Equipment. A train derailment on the line past the plant would likely be known, whereas one that was 1/2 mile or more away with flammable materials might not be known about unless a public warning was made.
Response: The DSR SDT thanks you for your comment. Voltage Deviation reporting no longer applies to the GOP. There is a footnote on Damage or Destruction to BES equipment that addresses your comment. It states: [1]BES equipment that: i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii) Damaged or destroyed due to intentional or unintentional human action which removes the BES equipment from service. Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative). Fuel Supply Emergency has been removed from Attachment 1. Forced Intrusion is an event could be related to sabotage. Identification and reporting of such events may help identify trends. The footnote associated with Risk TO BES Equipment addresses your comment: Examples include a train derailment adjacent to BES equipment that either could have damaged the equipment directly or has the potential to damage the equipment (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center) and report of suspicious device near BES equipment.		
Brazos Electric Power Cooperative	No	Inclusion of LSE and DP is questionable.
Response: The DSR SDT thanks you for your comment. The SDT believes that it has properly identified registered entities that may potentially have events and the appropriate types of events. A Registered Entity is only required to submit an events report for events listed in Attachment 1 if the registered entity was affected by the event. The LSE and DP are applicable entities under CIP-002 and CIP-008. If an event occurs, only affected Registered Entities listed in Attachment 1 are required to submit a report on the event. Having reports from the different entities may provide valuable information on understanding the event. The SDT would like to point out that reporting of events is from the time of identification not the time of the event.		

Organization	Yes or No	Question 4 Comment
Manitoba Hydro	Yes	All registered entities are included. This means all field and office personal involved will create a 360 degree view of the BES, and fulfill "Situational awareness of the industry." In Attachment 1, the "Entity with Reporting Responsibility" entities vary. It might be clearer to leave all impact levels "Entity with Reporting Responsibility" as the RC, BA and TOP, as these are likely the only parties that will report as required. All other entities must report to the RC, BA and TOP.
Response: Thank you for your comment. The SDT had previously considered a hierarchal approach to report; however, this concept was rejected by the industry.		
American Electric Power	Yes	AEP agrees, but it further supports the notion that this standard should not apply to the IA, TSP, and LSE functions.
Response: The DSR SDT thanks you for your comment. The SDT constructed Attachment based upon the existing requirements in the various reliability standards and established reporting obligations. The LSE, TSP and IC are applicable entities under CIP-002 and CIP-008. The information about an event will be useful to all owners, operators, and users of the bulk power system.		
Southern Company	Yes	This will cause the duplication of reporting for some events. Reference EOP-004 Attachment 1: Impact Events Table; Event - Loss of Firm Load for ≥ 15 minutes (page 15 of standard) This requires the RC, BA, TOP, and DP to report. So if a storm front goes through our system and takes out 400MW of load in Alabama and Georgia the PCC would have to report as the RC, BA, and TOP. Alabama Power and Georgia Power would also have to report as DPs. The way it is now the PCC reports for any of these events.
Response: The DSR SDT thanks you for your comment. The SDT believes that it has properly identified registered entities that may potentially have events and the appropriate types of events. A Registered Entity is only required to submit an events report for events listed in Attachment 1 if the registered entity was affected by the event. If an event occurs, only affected Registered Entities listed in Attachment 1 are required to submit a report on the event. Having reports from the different entities for the same event may provide a more complete understanding of the event.		
Pepco Holdings Inc and Affiliates	Yes	More guidance is needed for which entity in Attachment 1 actually files the report to avoid duplicate filing.
Response: The DSR SDT thanks you for your comment. The SDT believes that it has properly identified registered entities that may potentially have events and the appropriate types of events. A Registered Entity is only required to submit an events report for events listed in Attachment 1 if the registered entity was affected by the event. If an event occurs, only affected Registered Entities listed in Attachment 1 are required to submit a report on the event. Having reports		

Organization	Yes or No	Question 4 Comment
from different entities for the same event may provide a more complete understanding of the event.		
Midwest ISO Standards Collaborators	Yes	
Bonneville Power Administration	Yes	
Midwest Reliability Organization	Yes	
Western Electricity Coordinating Council	Yes	
PPL Supply	Yes	
City of Tallahassee (TAL)	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
Liberty Electric Power LLC	Yes	
Arkansas Electric Cooperative Corporation	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Platte River Power Authority	Yes	
BGE	Yes	No comments.
Alliant Energy	Yes	

Organization	Yes or No	Question 4 Comment
ExxonMobil Research and Engineering	Yes	
PPL Electric Utilities	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	
Progress Energy	Yes	
Response: The DSR SDT thanks you for your comment. Several commenters provided suggestions that led to modifications of Attachment 1.		

5. Stakeholders suggested removing original Requirements 1, 7 and 8 from the standard and addressing the reliability concepts in the NERC Rules of Procedure. Do you agree with the removal of original requirements 1, 7 and 8 (which were assigned to the ERO) and the proposed language for the Rules of Procedure (Paragraph 812)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: Most commenters agreed with the removal of R1, R7 and R8. The SDT has provided suggested language to NERC for inclusion into the Rules of Procedure.

Organization	Yes or No	Question 5 Comment
Midwest ISO Standards Collaborators	No	We see no issue with imposing requirements on NERC. However, we are not opposed to making these changes in the Rules of Procedure either.
Response: Thank you for your comments. We are pursuing changes to the Rules of Procedure.		
SERC OC Standards Review Group	No	We agree that the ERO should not have requirements applicable to them, but disagree with changing or revising the Rules of Procedure (ROP) giving this reporting responsibility solely to NERC. This responsibility may be performed by NERC but other learning organizations should also be considered for performing this responsibility. In addition, the proposed wording of the revision to the ROP appears to place the responsibility of notifying the appropriate law enforcement with NERC rather than with the local responsible entity.
Response: Thank you for your comments. The responsibility for notifying law enforcement remains with the entity and has been clarified in Attachment 1.		
PJM Interconnection LLC	No	We agree that the standard should not have requirements applicable to the ERO, but disagree with revising the NERC Rules of Procedure (RoP) to include suggested Section 812. The reporting responsibility should not be solely given to NERC. Other learning organizations must also be considered for performing this responsibility. Additionally, the proposed wording of Section 812 appears to imply that NERC will notify the appropriate law enforcement agencies as opposed to the local responsible entity.
Response: Thank you for your comments. The responsibility for notifying law enforcement remains with the entity and has been clarified in Attachment 1.		
SDG&E	No	SDG&E agrees with removing original Requirements 1, 7, 8 from the standard. In addition, SDG&E recommends that the standard reference Section 812 of the Rules of Procedure.

Organization	Yes or No	Question 5 Comment
Response: Thank you for your comments.		
Duke Energy	No	Proposed language for Section 812 is very confusing. Is the NERC "system" really going to perform all notifications: "applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, and regulatory agencies as necessary?" Is it intended that the NERC "system" will relieve registered entities of the obligation to make these other reports? Is there an implementation plan to achieve that objective? It appears that this current version of EOP-004-2 has the potential for significantly creating redundant reporting. Will the NERC reports be protected from FOIA disclosure? How will FERC Order 630 be followed (CEII disclosure)?
Response: Thank you for your comments. The SDT expects any system would facilitate the reporting to organizations specified in the submitted report. Until such time that the system can be established, the Registered Entity will be obligated to make the notifications as specified in its Operating Plan(s). The SDT has proposed an amendment to the NERC Rules of Procedure to assist in the development of a single reporting process for all three obligations.		
ExxonMobil Research and Engineering	No	Abstain from commenting on this question.
Brazos Electric Power Cooperative	No	
Ingleside Cogeneration LP	Yes	Ingleside Cogeneration agrees that the NERC Rules of Procedure are the appropriate location for ERO assigned activities. However, we would like to get a solid commitment from NERC that the Events Analysis Process and the Reliability Assessment and Performance Analysis Group (RAPA) data analysis requirements for Protection System Misoperations is coordinated through a single process. Their unique data needs are understandable, but should not require the downstream entity to evaluate what is required by each sub-committee - and which reporting template to use.
Response: Thank you for your comments. Your comment addresses a concern that is beyond the scope of this project and cannot be addressed here. The SDT has communicated with the NERC Events Analysis Working Group and DOE in efforts to develop a single reporting process. The SDT will continue to work with those organizations to complete this task.		
Northeast Power Coordinating Council	Yes	Agree with the proposed removal, but have not assessed the proposed language for RoP para. 812 because unable to access it (not on the RoP page).
Response: Thank you for your comments.		

Organization	Yes or No	Question 5 Comment
Bonneville Power Administration	Yes	Ensure distribution of trends.
Response: Thank you for your comments.		
Midwest Reliability Organization	Yes	The ERO is not a user, owner or operator of the BES and the best place to contain their responsibilities, is in the Rules of Procedure.
Response: Thank you for your comments.		
Pepco Holdings Inc and Affiliates	Yes	Agree that NERC should not have requirements applicable to them.
Response: Thank you for your comments.		
American Municipal Power	Yes	A software solution may provide an easy expansion for reporting EOP-004, CIP-001, and additional standards.
Response: Thank you for your comments.		
Manitoba Hydro	Yes	Agree with R1, a central system for receiving and distributing reports. There is limited time and resources for control operators to follow up and ensure ALL required entities have received all information required in a timely manner. Agree with R7 and R8.
Response: Thank you for your comments.		
Sweeny Cogeneration LP	Yes	We agree that these requirements appropriately belong in the NERC Rules of Procedure. However, we are concerned with the multiple reporting requirements being driven by EOP-004-2, CIP-008-3, the ERO Events Analysis Team, the Reliability Assessment and Performance Analysis Group (RAPA). It is imperative that these efforts be consolidated into a single procedure using a single reporting template.
Response: Thank you for your comments. The DSR SDT agrees with the concept of the single reporting template and is working with other agencies to see if the single form would be achievable.		
Western Electricity Coordinating Council	Yes	

Organization	Yes or No	Question 5 Comment
PPL Supply	Yes	
Pacific Northwest Small Public Power Utility Comment Group	Yes	
PSEG Companies	Yes	
Dominion	Yes	
SPP Standards Review Group	Yes	
FirstEnergy	Yes	
Southern Company	Yes	
SRP	Yes	
We Energies	Yes	
Compliance & Responsiblity Organization	Yes	
Exelon	Yes	
City of Tallahassee (TAL)	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
United Illuminating Co	Yes	
Liberty Electric Power LLC	Yes	

Organization	Yes or No	Question 5 Comment
Arkansas Electric Cooperative Corporation	Yes	
American Electric Power	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Independent Electricity System Operator	Yes	
ISO New England, Inc	Yes	
Platte River Power Authority	Yes	
Calpine Corp	Yes	
BGE	Yes	No comments.
Alliant Energy	Yes	
CenterPoint Energy	Yes	
PPL Electric Utilities	Yes	
Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
American Transmission Company	Yes	

Organization	Yes or No	Question 5 Comment
Constellation Power Generation	Yes	
Georgia System Operations Corporation	Yes	None.
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	
Indeck Energy Services	Yes	
Progress Energy	Yes	

6. Do you agree with the proposed revisions to Requirement 2 (now R1) including the use of defined terms Operating Plan, Operating Process and Operating Procedure? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: Stakeholders were fairly evenly divided on this question. Overall, there appears to be a misconception on what is and isn't included in the Operating Plan(s). The SDT believes that current Sabotage Reporting substantially meets the requirements outlined in the standard, albeit there may be some needed alterations to accommodate the new standard. The updated subrequirement is a result of a FERC directive in Order No. 693. The DSR SDT removed references to Operating Process and Operating Procedure and revised the Requirement to:

R1. Each Responsible Entity shall have an Operating Plan that includes: [Violation Risk: Factor: Lower] [Time Horizon: Operations Planning]

1.1. A process for identifying events listed in Attachment 1.

1.2. A process for gathering information for Attachment 2 regarding events listed in Attachment 1.

1.3. A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate:

- Internal company personnel
- The Responsible Entity's Regional Entity
- Law enforcement
- Governmental or provincial agencies

1.4. Provision(s) for updating the Operating Plan within 90 calendar days of any change in assets, personnel, other circumstances that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to R3.

1.5. A Process for ensuring the responsible entity reviews the Operating Plan at least annually (once each calendar year) with no more than 15 months between reviews.

Organization	Yes or No	Question 6 Comment
Georgia Transmission Corporation & Oglethorpe Power	No	The terms "Operating Procedure, Operating Plan, and Operating Process," while included in the NERC glossary, are not consistently used throughout the body of NERC standards as they are used in R1 of EOP-

Organization	Yes or No	Question 6 Comment
Corporation		004-2. As such, we do not see a reliability benefit in using the defined terms over the more commonly used terms of simply "plans, processes, and procedures." In part 1.1 of R1, we think that the requirement should clearly indicate that a particular Responsible Entity's Impact Event Plan should only be required to include those particular Impact Events for which the Responsible Entity has the reporting obligation. Therefore, we suggest the following modification to R1: "1.1 An Operating Process for identifying Impact Events listed in Attachment 1 for those Impact Events where the Responsible Entity is identified as having the reporting responsibility." Additionally, in part 1.3 of R1, we believe the language to be vague and will introduce the need for further clarification either through an interpretation or the CAN process in part because the verb tenses of the sub-sub-requirements do not agree and it appears to require notification to all listed parties for every Impact Event instead of only those that make sense for a particular event. As such, we suggest adding a column to the tables in Attachment 1 that identifies precisely which organizations should be notified in the case of a particular Impact Event and modifying part 1.3.2 to read: "1.3.2 External organizations to notify as specified in Attachment 1." Currently, as written, the standard could be interpreted to require notification to law enforcement for an IROL violation, for instance. Furthermore, we are concerned that as written, the standard may require that the same event must be reported by multiple responsible entities. Our current process uses notification between Responsible Entities (i.e. from a TO to a TOP and then from the TOP to NERC) to allow for a centralized and coordinated notification to law enforcement, NERC, etc. We are concerned that the requirement as written does not appear to allow this flexibility and may require both the TO and TOP to report the same event in order to prove compliance with the Standard.
Response: Thank you for your comments. The SDT believes that in order for a term to become consistent with the body of the reliability standards, each SDT will have to incorporate the terms as the opportunity to revise each standard arises. The SDT envisions that each Registered Entity will develop Operating Plan(s) appropriate to meet its obligations as outlined in the standard. Part 1.3 has been revised to indicate that each report must be sent to the ERO and the Registered Entity's Reliability Coordinator and the remaining entities as appropriate. Law Enforcement would certainly not be interested in an IROL violation, but they would be interested in Forced Intrusion.		
Bonneville Power Administration	No	Not sure that a 90-day update is needed to be sent to CEF.
Response: Thank you for your comments. That is not required in the standard. The SDT believes that it is unnecessary to forward any update to any organization outside of the Registered Entity. Updates should be used to inform internal personnel of any Operating Plan changes.		

Organization	Yes or No	Question 6 Comment
Pacific Northwest Small Public Power Utility Comment Group	No	1.4 makes no sense. The operating plan update and the change to its content occur simultaneously. Perhaps the SDT meant to say "Provision(s) for updating the Impact Event Operating Plan within 90 days of identification of a needed change to its content. This would be consistent with the "lessons learned" language of the prior version.
Response: Thank you for your comment. The DSR SDT added additional detail to Part 1.4 to address the broader term "content."		
PSEG Companies	No	The PSEG Companies believe that sections 1.3 and 1.3.2 will require notification of law enforcement agencies for all Impact Events defined in Attachment 1. This is appropriate for some events if there has been destruction to BES equipment, for example, but not in certain operational events. It should not be necessary to notify law enforcement that a non sabotage event like an IROL violation, generation loss or voltage deviation has occurred.
Response: Thank you for your comments. The DSR SDT feels that the Registered Entity will establish Operating Plan(s) appropriate for its needs including the specification of how and when law enforcement agencies are contacted. Part 1.3 has been revised to indicate that each report must be sent to the ERO and the Registered Entity's Reliability Coordinator and the remaining entities as appropriate. Law Enforcement would certainly not be interested in an IROL violation, but they would be interested in Forced Intrusion. Attachment 1 language has been updated to say "The parties identified..." which should be included in the entity's Operating Plan(s).		
Dominion	No	The requirement for Responsible Entities to establish an Impact Event Operating Plan, Operating Process, and Operating Procedure seems overly cumbersome and prescriptive. The use of these NERC defined terms create additional compliance burden for little, if any, improvement to reliability. Suggest simplification by requiring the Responsible Entities to have a procedure to report Impact Events, to the appropriate parties, pursuant to EOP-004. In addition, we request clarification of R1.4. It seems circular to us in that it requires the plan to be updated within 90 days of when it changes. Is the intent that any necessary changes identified in the annual review required by R4 be incorporated in a revision to the plan within 90 days of the review? If so, R1.4 belongs under R4. If not, we do not understand the requirement. What starts the 90 day count down?
Response: Thank you for your comment. The language in Requirement R1, Part 1.4 was inserted in response to a directive in FERC Order 693. The SDT feels that the directive requires Registered Entities to update their Operating Plan(s) within 90 days of the time the entity identified the need for the change, such as a new telephone number, personnel staff name/title, or addition/deletion of person or organization. The DSR SDT has made changes to better clarify "content."		

Organization	Yes or No	Question 6 Comment
Pepco Holdings Inc and Affiliates	No	An Operating Plan, Operating Process or Operating Procedure implies something different than an after the fact reporting activity.
Response: Thank you for your comment. An Operating Plan is more than an after the fact reporting activity. The Operating Plan(s) incorporates the tasks or steps involved in the identification of events, establishing which internal personnel are to be involved in the communications and or reporting, and establishing the list of outside organizations to be contacted when an event happens.		
SPP Standards Review Group	No	We would suggest rewording Part 1.3.2 to read "External organizations to notify may include but are not limited to the Responsible Entity's Reliability Coordinator, NERC, Responsible Entity's Regional Entity, Law Enforcement and Governmental or Provincial Agencies." We would also suggest the following for Part 1.4: "Provision(s) for updating the Impact Event Operating Plan within 90 days of any known changes to its content." Would also suggest adding "as requested" at the end of M1.
Response: Thank you for your comments. (1) Requirement R1, Part 1.3 has been updated to "as appropriate" to address the parties to communicate event to. (2) The SDT agrees with your suggestions and has made similar word changes. 3) Agreed.		
Midwest ISO Standards Collaborators	No	We do not believe that the use of the Operating Process, Operating Procedure, and Operating Plan for a reporting requirement is consistent with their definitions and certainly not with the intent of the definitions. For instance, an Operating Process is intended to meet an operating goal. What operating goal does this requirement meet? An Operating Procedure includes tasks that must be completed by "specific operating positions." This reporting requirement could be met by back office personnel. We also believe that parts 1.3 and 1.3.2 under Requirement 1 will require notification of law enforcement agencies for all Impact Events defined in Attachment 1. While some should require notification to law enforcement such as when firm load is shed, others certainly would not. For instance, law enforcement does not need to know that an IROL violation, generation loss or voltage deviation occurred.
Response: Thank you for your comments. The Glossary Definition of Operating Plan is: A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan. The definition uses "goal" rather than "operating goal". The goal of the Operating Plan is to ensure that entities know how to identify the events listed in		

Organization	Yes or No	Question 6 Comment
Attachment 1 and report them to the appropriate parties. The SDT disagrees with your views on Operating Process, Operating Procedure, and Operating Plan. The SDT appropriately describes the task at hand. The SDT feels that the Operating Plan can identify when law enforcement agencies need to be notified without specification from the SDT. The Background section of the standard contains a heading for "Law Enforcement" and provides clarification regarding the types of events that should be reported to law enforcement.		
FirstEnergy	No	1. We believe that the use of stringent definitions for an entity's process requires too much of the "how" instead of the "what." As long as the entity has a process, procedure (or whatever they want to call it) that includes the necessary information detailed in sub-parts 1.1 through 1.4 then that should suffice. 2. In sub-part 1.3, we suggest adding the phrase "as applicable" to clarify that not every event will require a notification to, for example, law enforcement. 3. In sub-part 1.4, we suggest adding clarification that the 90-day framework is only required for substantive changes and that all other minor editorial changes can be updated within a year.
Response: Thank you for your comments. (1) The SDT agrees with your suggestion that the entity can best determine what is included in its Operating Plan. The SDT does not envision instructing an entity on what or how of the Operating Plan(s). (2) The SDT feels that the Operating Plan can identify when law enforcement agencies need to be notified without specification from the SDT. (3) The update requirement comes from a FERC directive in Order No. 693. The SDT has validated the intent of the directive and has included that intent in the requirement. The SDT feels that the directive requires Registered Entities to update their Operating Plan(s) within 90 days of the time the entity identified the need for the change, such as a new telephone number, personnel staff name/title, or addition/deletion of person or organization. The DSR SDT has made changes to better clarify "content."		
SERC OC Standards Review Group	No	This is a reporting requirement and should not be confused with Operating Plans that have specific operating actions and goals. Each entity should prepare its own event reporting guideline that address impact events, identification, information gathering, and communication without specifying a specific format such as Operating Plans, Operating Process and Operating Procedures.
Response: Thank you for your comment. The SDT agrees with your viewpoint and believes that your statement is consistent with the intent of the requirement.		
PJM Interconnection LLC	No	1. This is an "after-the-fact" reporting requirement and should not be confused with Operating Plans that have specific operating actions and goals. Each entity should prepare its own impact event operating guideline that addresses impact events, identification of impact events, information gathering, and communication without specifying a specific format such as Operating Plans, Operating Process, and Operating Procedures. In fact, all three documents mentioned can all be a single document. 2. 1.3.2 requires notification of law enforcement agencies for all events listed in Attachment 1. This is essentially not true. For example, firm load is shed requires notification to law enforcement but an IROL

Organization	Yes or No	Question 6 Comment
		violation, generation loss, or voltage deviation do not.
Response: Thank you for your comment. (1) The SDT disagrees with your viewpoint that this requirement specifies after-the-fact reporting. The reporting requirement is later in the standard. The SDT agrees with your viewpoint on the operating guideline you provide and believes that your statement is consistent with the intent of the requirement. (2) The SDT believes that the Registered Entity's Operating Plan(s) can establish when and how law enforcement agencies are notified.		
We Energies	No	R1.2: By its NERC Glossary definition, an Operating Procedure is too prescriptive for data collection. An Operating Procedure requires specific steps to be taken by specific people in a specific order. We would have to predict every event that could happen to have every step in proper order to collect the data. It will be impossible to comply with this requirement. R1.3: Change "Impact Event" to "Impact Event listed in Attachment 1."
Response: Thank you for your comment. The SDT has changed R1 to simply "Operating Plan. The term "Impact Event" has been removed from the standard and R1 and its Parts refer to Attachment 1 as appropriate.		
Compliance & Responsiblity Organization	No	See comments to 2. Also, although NextEra agrees that a documented procedure is appropriate, NextEra does not favor the current approach of pre-defined layers of processes and documentation that seem to overly complicate, and, possibly contradict, already established internal methods by which a company implements policies, procedures and processes. Thus, NextEra's options suggest using a more generic approach that allows entities more flexibility to establish documents and processes, and demonstrate compliance. Such a generic approach was used in NextEra's proposed options set forth in response to number 2.
Response: Thank you for your comments. The SDT believes that most entities already have plans to mostly satisfy the requirements of EOP-004. These would be the procedures that are required under existing CIP-001, R1 and R2.		
Exelon	No	R.1 Does an entity need to develop a standalone Operating Plan if there is an existing process to address identification, assessing and reporting certain events? Suggest rewording to state "Each Responsible Entity shall have an Impact Event Operating Plan or equivalent implementing process that includes:" Disagree these new terms are required. Commonly accepted descriptions of programs, processes and procedures exist in registrar entities that would suffice. For example, R1 could use "Impact Event evaluation

Organization	Yes or No	Question 6 Comment
		and reporting process" as a generic term to describe what is required. This would allow an entity to utilize any existing protocols or management guidelines and naming conventions in effect in their organization.
Response: Thank you for your comments. The SDT The SDT believes that most entities already have plans to mostly satisfy the requirements of EOP-004. These would be the procedures that are required under existing CIP-001, R1 and R2. The Registered Entity will need to examine its current processes to ensure that all aspects of the new requirements are addressed. Thank you for the suggested re-wording. The SDT revised "Impact Event Operating Plan" to just "Operating Plan", thus allowing the entity to implement the requirements as needed.		
Tenaska	No	We already have adequate procedures in place to address sabotage and other significant events, pursuant to the existing CIP-001-1 and EOP-004-1 Standards. The requirement to develop a new Impact Event Operating Plan would increase the administrative burden on Registered Entities to comply with the proposed Standard, without providing a foreseeable improvement in system reliability. The "laundry list" of required Impact Event Operating Plan components is too specific and would make it more difficult to prove compliance with EOP-004-2 during an audit. A revised version of the proposed R5 is the only Requirement that is necessary to achieve the stated purpose of Project 2009-01.
Response: Thank you for your comments. The SDT The SDT believes that most entities already have plans to mostly satisfy the requirements of EOP-004. These would be the procedures that are required under existing CIP-001, R1 and R2 and these should mostly meet the intent of EOP-004. The Registered Entity will need to examine its current processes to ensure that all aspects of the new requirements are addressed. The Parts of R1 are not prescriptive and only provide the minimum information that is required to be in the Operating Plan. The SDT has removed R2 and revised R5 (now R2) to eliminate any duplication.		
United Illuminating Co	No	Does R1.1 require an Operating Process for each Impact Event in attachment 1 or an Operating Process that in general applies to all Impact Events?
Response: Thank you for question. The SDT feels that the Registered Entity can have an Operating Plan that in general applies to all events.		
American Municipal Power	No	No, remove R1. R1 is not an acceptable requirement nor should this be an operation. Focusing on a plan and procedure is overly prescriptive and costly. The only requirement should be to have an entity submit a report. Let the entity decide how they want to implement the reporting.
Response: Thank you for your comment. The SDT agrees that the Registered Entity can decide on the how to implement the reporting; however, this requirement mandates that the Registered Entity document its process.		

Organization	Yes or No	Question 6 Comment
Arkansas Electric Cooperative Corporation	No	We appreciate the effort the team has taken in improving the requirements since the last posting. For 1.3, it appears to suggest the communication must always include communicating to internal personnel and ALL external organizations. We suggest removing the reference to 1.3.1 and 1.3.2 and move 1.3.1 and 1.3.2 to 1.4 and 1.5 respectively. For 1.3.2, modify to state "Internal company personnel notification(s) deemed necessary by the Responsible Entity." For 1.4, we feel the term "content" is too broad as used here. For example, if the FBI changes the contact info for the JTTF, the Responsible Entity may not find out until an incident or annual exercise. Or if the contact person for the state agency changes position without notifying us, it would require us to then change the plan within 90 days. We suggest an annual review of the plan is sufficient for the objective of this requirement.
Response: Thank you for your comments. The SDT has added language "as appropriate" to allow the entity to make its own determination who to contact. The term "content" has been removed and replaced with more detail. The requirement for updates requires changes within 90-days. The SDT believes that the timeline for updating can only be based upon the notification to the Registered Entity. The SDT believes that 90-days from the date the Registered Entity is notified or made aware of the change is a suitable time period to update the document.		
Manitoba Hydro	No	Plan, Process and Procedure are all too interchangeable with each other and have no value being used in "one paragraph" as they do not differentiate from one or other. The terms "identify", "gather" and "communicate" better describe "Process, plan or procedure" so simplify to:1.4. Identification of Impact Events as listed in Attachment 1.1.5. Gathering information for inclusion into Attachment 2 regarding observed Impact Events listed in Attachment 1.1.6. Communicate recognized Impact Events to the following:
Response: Thank you for your comments. The SDT has revised R1 to only include an Operating Plan. Part 1.2 has been revised to "A process for gathering information..."		
American Electric Power	No	Even best developed plans, processes and procedures do not always lend themselves to address the issues at hand. There needs to be flexibility to allow entities to first address the reliability concern and second report correspondingly. Currently, this requirement is overly prescriptive and places unnecessary emphasis on the means to an end and not the outcome. The outcome for this requirement is to report Impact Events.
Response: Thank you for your comments. While the SDT appreciates your views, it disagrees with your assessment. The outcome of this requirement is not to report events; the outcome is to ensure that the Registered Entity has Operating Plan(s) for the identification of events, establishing which internal personnel are involved, identification of outside agencies to be notified, and having a provision for updating the plan(s). Reporting of events is a requirement later in the standard.		

Organization	Yes or No	Question 6 Comment
Consumers Energy	No	Requirement R1, "Have a plan…" with all of the listed criteria, seems to present a serious compliance risk to applicable entities without a direct reliability benefit, as long as entities still indentify and report relevant events. Ad-hoc procedures, as discussed within the R1 "Rationale" have been acknowledged within the rationale to be working effectively, and should remain sufficient without having a documented and by inference, signed, approved, dated document with revision history (as is being demanded today by compliance auditors wherever a "documented plan" is specified within the requirements).
Response: Thank you for your comments. While the SDT appreciates your views, it disagrees with your assessment. The SDT believes that most entities already have plans to mostly satisfy the requirements of EOP-004. These would be the procedures that are required under existing CIP-001, R1 and R2. The measure calls for a current, dated, in force Operating Plan to be provided.		
ISO New England, Inc	No	We do not believe that the use of the Operating Process, Operating Procedure, and Operating Plan for a reporting requirement is consistent with their definitions nor with the intent of the definitions. For instance, an Operating Process is intended to meet an operating goal. What operating goal does this requirement meet? An Operating Procedure includes tasks that must be completed by "specific operating positions." This reporting requirement could be met by back office personnel. We suggest that R1.3.2 delete the list of entities to notify. The terms used to identify who to notify are not defined terms and can lead to subjective interpretations. As written, the requirement does not aid the Applicable entity or the Compliance enforcers in clearly including or excluding who to notify. We also believe that parts 1.3 and 1.3.2 under Requirement 1 will require notification of law enforcement agencies for all Impact Events defined in Attachment 1. While some should require notification to law enforcement such as when there has been destruction to BES equipment, others certainly would not. For instance, law enforcement does not need to know that an IROL violation, generation loss or voltage deviation occurred. We believe the reporting time lines are too aggressive for some events. Reporting events within an hour is not reasonable as an entity may still be dealing the event. This will be particularly difficult when support personnel are not present such as during nights, holidays and weekends. We further suggest that as explicit statement that "reliable operations must ALWAYS take precedence to reporting times" be included in the standard.
Response: Thank you for your comments. While the SDT appreciates your views, it disagrees with your assessment. (P1) The outcome of this requirement is not to report events; the outcome is to ensure that the Registered Entity has Operating Plan(s) for the identification of events, establishing which internal personnel are involved, identification of outside agencies to be notified, and having a provision for updating the plan(s). The		

Organization	Yes or No	Question 6 Comment
SDT feels that current Sabotage Reporting guides already provides much of the information needed in the new R1. (P2) We have revised Requirement R1, Part 1.3 to "A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate:" This should address your concern regarding law enforcement notification. (P3) We have revised most reporting times to 24 hours. Events of a "sabotage" type nature remain at one hour. (P4) While the DSR SDT sees the point you are trying to make, we do not believe that reporting the events in Attachment 1, under the times listed, is burdensome. At the least, this can be accomplished by back office personnel who are not involved in restoration or other reliability efforts.		
Calpine Corp	No	In the "Rationale for R1", the draft states: "Every industry participant that owns or operates elements or devices on the grid has formal or informal process, procedure, or steps it takes to gather information regarding what happened and why it happened when Impact Events occur. This requirement has the Registered Entity establish documentation on how that procedure, process, or plan is organized." Absent substantial evidence that the proposed requirement addresses an actual systemic problem with the "formal or informal process, procedure, or steps it takes" for internal and external evaluation and notification of items listed in Attachment 1, there is no obvious need for this additional paperwork burden, which in most cases will result in a written procedure that documents another existing written procedure or procedures, that will be maintained for the sole purpose of demonstrating compliance with the requirement. Failure to properly report events is currently sanctionable under CIP-001-1 and EOP-004-1 and will continue to be sanctionable under proposed EOP-004-2. Adding a requirement to implement an "Impact Event Operating Plan", "Operating Procedure", and "Operating Process" is unnecessary. However, if the requirement is maintained, the related Measure M1 should state in plain language exactly what elements are required for compliance. Statements such as "The Impact Event Operating Plan may include, but not be limited to, the following?" begs the question regarding what other elements are required to demonstrate compliance. As written, M1 requires that entities provide an "Impact Event Operating Plan", but does specify the required elements of the plan. In the absence of much more detailed instruction on exactly what elements must be included in the various documents, the proposed requirement will create confusion with both compliance and enforcement of the requirement. An example of each of the various required documents would be helpful. Any difficulty in developing such an example would be instructive of the probable compliance issues that would ensure from the necessarily varying approaches taken by disparate entities attempting to meet the requirement.
Response: The DSR SDT thanks you for your comment. Requirement R1 comes from existing CIP-001, R1. The SDT believes it has addressed these concerns by removing the terms "Operating Procedure" and "Operating Process" and has generically referred to them in the elements of the Operating Plan outlined in		

Organization	Yes or No	Question 6 Comment
Parts 1.1-1.5 of the requirement.		
BGE	No	This seems overly restrictive in its use. Requirement is now telling entities how to resolve situations, not giving them a requirement to resolve the situation.
Response: Thank you for your comments. The requirement is written so that an entity has an Operating Plan that contains certain items. The SDT does not specify in the standard how the entity meets these obligations nor does it specify the form nor format of these items.		

Organization	Yes or No	Question 6 Comment
ExxonMobil Research and Engineering	No	The requirement to notify State Law Enforcement deviates from existing government security requirements that Petrochemical Facilities (Cogenerators) are required to follow. Per the Maritime Transportation Security Act of 2002 (MTSA) and the Chemical Facility Anti-Terrorism Standard (CFATS), Petrochemical Facilities are required to report the security incidents identified in EOP-004 Revision 2 to the National Response Center which is staffed by the United States Coast Guard. The National Response Center coordinates incident reporting to both the Department of Homeland Security and Federal Bureau of Investigation. Requiring Petrochemical Facilities to report security incidences to State Law Enforcement agencies duplicates their reporting of incidences to the appropriate law enforcement agencies. EOP-004 Revision 2 should be modified to synergize with existing federal security regulations so that those facilities that are required to comply with the MTSA and CFATS are, by default, compliant with EOP-004 Revision 2 when they comply with these existing federal security regulations. It is unclear, from the documentation provided in this revision of EOP-004, which entities a Responsible Entity is required to notify when certain types of Impact Events occur. Previously, CIP-001 included a similarly vague instruction that required notifications to the 'appropriate parties in the interconnection' and the FBI/RCMP. The Standard Drafting Team should identify which NERC Functional Entities should be notified when each of the Impact Events identified in Attachment 1 occurs. Current revisions of CIP-001 Revision 1 or EOP-004 Revision 1 do not include corresponding requirements to update procedures within a certain time frame. It's difficult to foresee a situation where an Entity would initiate a change to its response plan without being required to update the formal response plan documentation per their management of change process. Additionally, failure to update the procedure would result in the entity deviating from the procedure any time an impact event occurred, which would automatically force a violation of EOP-004-2 R2 for failure to properly implement their Operating Process. Furthermore, the only changes occurring between review cycles should be revisions to the contact information for third parties. It is beyond an entity's power to require third parties to notify the entity when the third party changes their contact information, and, as such, this requirement burdens registered facilities with responsibility for compliance for items that are beyond their realm of control.

Response: Thank you for your comments. (P1) The SDT believes that the requirement does not mandate contact to State Law Enforcement agencies; but merely to include them if appropriate. While we have tried to coordinate with the US DOE, Federal security regulations are outside the scope of this project. (P2) We have revised Requirement R1, Part 1.3 to "A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate:" Each type of event should be assessed by the entity to determine whether or not law enforcement needs to be notified,

(P3)The subrequirement for updating comes from a FERC directive in Order No. 693. If the Registered Entity's Operating Plan(s) have a provision for updating, then the entity only needs to verify that the updating does not exceed 90 days from the date of being aware.

Organization	Yes or No	Question 6 Comment
Farmington Electric Utility System	No	consider rewording 1.4; the wording implies a change to content already occurred, so it would be updated concurrently ? consider, updating the plan within 90 days of discovery of content requiring a change?
Response: Thank you for your comment. The SDT agrees with your suggestion and has revised Requirement R1, Part 1.4 to: Provision(s) for updating the Operating Plan within 90 calendar days of any change in assets, personnel, other circumstances that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to R3.		
Constellation Power Generation	No	Per NERC's glossary of terms, an Operating Plan can include Operating Process documents and Operating Procedures. An Operating Process identifies general tasks while an Operating Procedure identifies specific tasks. CPG is unclear as to why R1.1 and R1.3 require the use of an Operating Process while R1.2 requires an Operating Procedure. CPG believes that R1.2 should be changed to require the use of an Operating Process instead of Operating Procedure. R1.2 is merely requiring an entity to fill out the necessary forms should an event occur, so requiring a clear and concise step by step procedure for filling out a form only adds a compliance burden to an entity instead of improving the reliability of the BES. CPG does agree with the DSR SDT that an entity should have a process in place mandating that the proper paperwork be completed in a timely manner should an event occur.
Response: Thank you for your comments. The SDT has modified Requirement R1, Part 1.1 and Part 1.3 to a "process" as part of the elements of the referenced "Operating Plan" in R1. The SDT has also changed "Operating Procedure" to a "process" in R1.2. This sub-requirement provides for establishing the list of internal personnel to be notified in the case of an event, not the reporting of the event.		
Georgia System Operations Corporation	No	-R1.3.2: "Law Enforcement", "Governmental Agencies", and "Provincial Agencies" are not proper nouns/names and are not defined in the NERC Glossary. They should not be capitalized. -R1.4: Keeping documents current and in force should be a matter of an entit
Response: Thank you for your comments. The SDT agrees with your suggestions on capitalization and has made the corrections. The update provision comes from a FERC directive in Order No. 693.		
Indeck Energy Services	No	The terms are not important and many plans or procedures already exist and restructuring them to match the

Organization	Yes or No	Question 6 Comment
		terms is wasteful. R1 is too prescriptive. R1 should state that a written document should show how the entity will comply with EOP-004. R1.2 is superfluous and should be deleted. The data must be gathered and the process will vary with the event. Trying to define the multitude of possibilities for the collection process is not productive and leaves open the possibility of missing something for an auditor to nit pick. R1.3 should just be a written communications plan/process/procedure for external notifications. R1.4 is redundant because it can't be changed within 90 days until the content has already been changed. R1.4 should be deleted. The Violation Risk Factor should be Low, if any, because this is historical reporting, with little or no reliability consequence.
Response: The SDT disagrees with your viewpoints associated with R1 because the requirement only specifies the elements required, now how to implement them. The SDT believes that many Registered Entities will be able to use their current Sabotage Reporting processes, with some slight modification to address the new sub-requirements. Requirement R1, Part 1.2: The requirement is written so that it is not prescriptive and allows the entity to identify the steps it will take to gather information for filing the report. The DSR SDT does not envision this as being a tome that contains specific data gathering protocol for each event type. Requirement R1, Part 1.3: Has been revised to: "1.3. A process for communicating recognized impact events listed in EOP-004 - Attachment 1 that includes to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and , but is not limited to the following as appropriate :" For Requirement R1, Part 1.4, the update provision comes from a FERC directive in Order No. 693. In addition, the SDT believes that the update is required within 90 days from the date of being notified of the change or update. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Midwest Reliability Organization	Yes	This is a NERC defined term and will assist entities in maintaining compliance with this (proposed) Standard.
Response: Thank you for your comment.		

Organization	Yes or No	Question 6 Comment
Western Electricity Coordinating Council	Yes	Are "Law Enforcement" considered a "Governmental Agency" (they are listed separately and both required) If not, is there any qualifiers on whether Law Enforcement or Governmental Agency refers to municipal, county, state or federal or any combination" Since the term "Provincial" is associated with "Governmental" it tends to indicate State level. As it is written now an auditor would require documentation of "some" Law Enforcement (other than company security) and an additional communication to at least "some" Agency which could be considered Governmental. Municipal or higher. Contact with City police or Sheriff and either city or county government rep would satisfy. Additional clarity would help from a compliance enforcement perspective.
Response: Thank you for your comments. The SDT expects that Registered Entities will identify the proper outside organizations needed for their organization. The SDT feels that law enforcement agencies include federal, state, provincial, or local law agencies and these are not the same as governmental or regulatory agencies. Please refer to the Background section of the standard for further clarification on law enforcement notifications.		
Alliant Energy	Yes	This is a NERC defined term and will assist entities in maintaining compliance with this (proposed) Standard. We believe the reference to Attachment 2 in R1.2 should be revised to the DOE Form and utilize only one reporting form, if at all possible.
Response: Thank you for your comments. The DSR SDT continues to work with the DOE to develop a single reporting form that is acceptable to both.		
Occidental Power Marketing	Yes	However, only LSEs with BES assets (or assets that support the BES) should be included in the Applicability section of the standard.
Response: Thank you for your comment. LSE applicability is related to their applicability under CIP-002 and CIP-008.		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	However, there needs to be some clarity on which government agencies (if not the FBI) are responsible for reporting these type of events.
Response: Thank you for your comments. Each Registered Entity should be aware of any reporting obligations it may have to various government agencies (federal, state/provincial, local). To the extent they exist, the notification needs to be included in the entity's Operating Plan(s).		
Northeast Power Coordinating	Yes	

Organization	Yes or No	Question 6 Comment
Council		
PPL Supply	Yes	
Southern Company	Yes	
SRP	Yes	
SDG&E	Yes	
City of Tallahassee (TAL)	Yes	
New Harquahala Generating Co.	Yes	
Liberty Electric Power LLC	Yes	
APX Power Markets	Yes	
Sweeny Cogeneration LP	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Independent Electricity System Operator	Yes	
Platte River Power Authority	Yes	
CenterPoint Energy	Yes	
PPL Electric Utilities	Yes	
Lincoln Electric System	Yes	

Organization	Yes or No	Question 6 Comment
American Transmission Company	Yes	
Ingleside Cogeneration LP	Yes	
Duke Energy	Yes	
Progress Energy	Yes	

7. Do you agree with the proposed revisions to Requirement 3 (now R2)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: The slight majority of commenters agreed with the language of Requirement R2. A significant minority opinion exists where commenters suggest revisiting R2 and R5 to eliminate potential redundancy and confusion. Similar comments were received pertaining to Requirement 5 (question 10 below). The DSR SDT has revised Attachment 1 to indicate that entities must submit Attachment 2 or the DOE OE-417 form. This information was contained in Requirement R5. The intent of the two requirements is to have entities make appropriate notifications and report impact events contained in Attachment 1. By eliminating R2 and revising R5 (now R2), the DSR SDT has maintained the intent of the requirements while eliminating potential confusion and redundancy. The revised requirements are shown below:

~~R2. Each Responsible Entity shall implement its Impact Event Operating Plan documented in Requirement R1 for Impact Events listed in Attachment 1 (Parts A and B). [Violation Risk: Factor Medium] [Time Horizon: Real-time Operations and Same-day Operations]~~

Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].

Organization	Yes or No	Question 7 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation	No	We are concerned with having a separate requirement to implement the Plan. Is this requirement necessary on its own? Should R1 instead require a Responsible Entity to "document and implement" an Impact Event Operating Plan? More specifically, if an Entity does not have an Impact Event, are they in violation of this requirement? If merging this requirement with R1 is not acceptable we suggest moving the language from the measure to the requirement as such: "To the extent that a Reponsible Entity has an Impact Event on its Facilities, Each Responsible Entity shall implement?" Additionally, R1 uses the phrase "recognized Impact Event" where as R2 simply uses the term "Impact Event." The phrase "recognized Impact Event" should be used consistently in R2 as well.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted requirement 2 and revised requirements 1 and 5 to address your concern. The DSR SDT believes that the requirement should remain separate to eliminate the possibility of double jeopardy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		

Organization	Yes or No	Question 7 Comment
Bonneville Power Administration	No	Minimize the number of requirements. Not sure what the new R2 intends that is different than having a valid plan (signed?). Why can't R1 have develop and implement? R5 is the reporting. Implement should be with R1 or R5 depending on the interpretation.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted requirement 2 and revised requirements 1 and 5 to address your concern. The DSR SDT believes that the requirement should remain separate to eliminate the possibility of double jeopardy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		
PSEG Companies	No	Fuel supply emergency, as discussed in response to question 4 above, is not a defined condition. This event should be removed.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Fuel Supply Emergency from Attachment 1. This item was removed in coordination with the NERC Events Analysis Working Group and the proposed Events Analysis Program.		
SERC OC Standards Review Group	No	We agree with the concept, but disagree with the use of the term “Operating Plan” as a defined term in line with our comments in question 6 above.
Response: The DSR SDT thanks you for your comment. Please see response to comments in Question 6 The DSR SDT has revised R1 to eliminate the use of Operating Process and Operating Procedure and have used more generic terms.		
PJM Interconnection LLC	No	We agree with the concept but disagree with the use of the term “Operating Plan” as a defined term in line with our comments in Question 6 above.

Organization	Yes or No	Question 7 Comment
Response: The DSR SDT thanks you for your comment. Please see response to comments in Question 6		
Compliance & Responsiblity Organization	No	See comments set forth in number 2.
Response: The DSR SDT thanks you for your comment. Please see response to question 2.		
Exelon	No	Agree that each Responsible Entity shall implement the [Impact] Events listed in Attachment 1 (Parts A and B); however, disagree with certain events, reporting responsibilities, threshold for reporting and time to submit reports as currently outlined in Attachment 1 (Parts A and B). Also suggest that R.2 be reworded to state for applicable [Impact] Events listed in Attachment 1 (Parts A and B). This requirement should only be applied to those events applicable to the registered entity.R2 is redundant to R1. No entity could claim to have met R1 if their plan / process was not operational and approved in the manner consistent with any other approved program, process, guideline etc. within their company.
Response: The DSR SDT thanks you for your comment. The DSR SDT has significantly revised Attachment 1. We have removed the timing column and replaced it with more specific information regarding which form to submit and to whom to submit the report. All events are now to be reported within 24 hours with the exception of Destruction of BES equipment, Damage or destruction of Critical Assets and Damage or destruction of Critical Cyber Asset events, Forced Intrusion, Risk to BES equipment and Detection of a reportable Cyber Security Incident. These events are to be reported within 1 hour. Notification of law enforcement per Part 1.3.2 is also required for these events only. The DSR SDT has also eliminated R2 and revised R5 for clarity and to eliminate potential redundancy. The DSR SDT believes that the requirement should remain separate to eliminate the possibility of double jeopardy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		
Tenaska	No	The proposed Impact Event Operating Plan should not be required.
Response: The DSR SDT thanks you for your comment.		

Organization	Yes or No	Question 7 Comment
The DSR SDT has revised R1 to only include development of an Operating Plan that includes the Parts of R1. This Operating Plan is required so that the entity's personnel will know what to do in the event of an event, how to report the event and to whom the report should be sent.		
American Municipal Power	No	No, remove R2. R2 is not an acceptable requirement nor should this be an operation. Focusing on a plan is overly prescriptive and costly. The only requirement should be to have an entity submit a report. Let the entity decide how they want to implement the reporting.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated R2 and revised R5 for clarity and to eliminate potential redundancy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		
American Electric Power	No	Requirement 5 and Requirement 2 are redundant. We recommend Requirement 2 be replaced with the language in Requirement 5. "Each Responsible Entity shall report Impact Events in accordance with the Impact Event Operating Plan pursuant to Requirement R1 and Attachment 1 using the form in Attachment 2 or the DOE OE-417."
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated R2 and revised R5 for clarity and to eliminate potential redundancy. The old Requirement R5 has been revised as the new Requirement R2, which reads: Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		
ISO New England, Inc	No	Fuel Supply Emergency is not a defined condition. We suggest that the SDT poll the ballot body regarding the reporting of Fuel Supply Emergencies. Fuel Supply is an economic consideration and the concept of Fuel Supply Emergency is subjective. A resource that uses coal or oil may vary its supplies based on economic considerations (the price of the fuel). For a conservative BA a fuel-on-demand supply line can be viewed as a fuel supply emergency whereas the resource owner sees the matter as good business. Moreover, the release of such reports to the public can have unintended consequences. Fuel disruptions caused by contract negotiations when reported to the public can result in non-union transportation employees being physically

Organization	Yes or No	Question 7 Comment
		harmed by fuel supply organizers thus resulting in the loss of non-contract fuel. Further, this information may aggravate the situation by causing the cost of fuel to be inflated by suppliers when demand is great. If this event is not deleted, then we would suggest that the definition be constrained to "declared" fuel supply emergencies. Suggest the deletion of category: Risk to BES equipment. Because of the broad definition of BES, the risk to BES equipment is overly broad and can be applied to any risk to any "part of" any BES asset. The footnote helps identify what the SDT was intending, however, the words themselves can result in overly broad findings by compliance enforcement people.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Fuel Supply Emergency from Attachment 1. This item was removed in coordination with the NERC Events Analysis Working Group and the proposed Events Analysis Program.		
Calpine Corp	No	Requirement R2 is unnecessary for the same reasons listed above in answer to question 6 regarding Requirement R1. A new Reliability Standard requirement is not needed to verify that internal notifications are made within Registered Entities or to ensure that Registered Entities notify local law enforcement of suspicious activity, sabotage, theft, or vandalism. Such notifications are made by any company, and this requirement does not clearly enhance the reliability of the Bulk Electric System. Requirement R5 provides sanction in the event that events listed in Attachment 1 are not made appropriately. However, if the requirement is maintained, the related Measure M2 should state in plain language exactly what elements are required for compliance. In the absence of much more detailed instruction on exactly what elements must be included in the various documents, the proposed requirement will create confusion with both compliance and enforcement of the requirement. A detailed example of example documentation would be helpful. Any difficulty in developing such an example would be instructive of the probable compliance issues that would ensure from the necessarily varying approaches that would be taken by disparate entities attempting to meet the requirement.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated R2 and revised R5 for clarity and to eliminate potential redundancy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		
CenterPoint Energy	No	CenterPoint Energy recommends deleting the current R2 as it is an inherent part of the current R5. For an entity to "report Impact Events in accordance with the Impact Event Operating Plan pursuant to R1" (see R5), the entity must "implement its Impact Operating Plan documented in Requirement 1?" (see R2). Including

Organization	Yes or No	Question 7 Comment
		both requirements is unnecessary and duplicative. Likewise, M2 should be deleted.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated R2 and revised R5 for clarity and to eliminate potential redundancy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		
ExxonMobil Research and Engineering	No	The notification requirement and documentation in Attachment 1 do not clearly identify which entities need to be notified for each type of event detailed in Attachment 1. While it makes sense to notify the Reliability Coordinator, NERC, Regional Entity, Law Enforcement and other Governmental Agencies for sabotage type events, it does not seem proper to notify Law Enforcement agencies of a system disturbance that is unrelated to improper human intervention. Furthermore, it is our belief that a time frame of 1 hour is a short window for making a verbal notification to third parties, and an impossibly short window for requiring the submittal of a completed form regardless of the simplicity. When a Petrochemical Facility experiences an impact event, the initial focus should emphasize safe control of the chemical process. For those cases where registered entities are required to submit a form within 1 hour, the Standard Drafting Team should alter the requirement to allow for verbal notification during the first few hours following the initiation of an Impact Event (i.e. allow the facility time to appropriately respond to and gain control of the situation prior to making a notification which may take several hours) and provide separate notifications windows for those parties that will need to respond to an Impact Event immediately and those entities that need to be informed that one occurred for the purposes of investigating the cause of and response to an Impact Event. For example, a GOP should immediately notify a TOP when it experiences a forced outage of generation capacity as soon as possible, but there is no immediate benefit to notify NERC when site personnel are responding to the event in order to gain control of of the situation and determine the extent of the problem. The existing standard's requirement to file an initial report to entities, such as NERC, within 24 hours seems reasonable provided that proper real time notifications are made and the Standard Drafting Team reinstates EOP-004 Revision 1's Requirement 3.3, which allows for the extension of the 24 hour window during adverse conditions, into the requirement section of EOP-004 [the current revision locates this extension in Attachment 1, which, according to input received from Regional Entities, means that the extension would not be enforceable].
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated R2 and revised R5 for clarity and to eliminate potential redundancy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment]. The DSR SDT has significantly revised Attachment 1. We have removed the timing column and replaced it with more specific information regarding which form to submit and to whom to submit the report. All events are now to be reported within 24 hours with the exception of Destruction of BES equipment, Damage or destruction of Critical Assets and Damage or destruction of Critical Cyber Asset events in Part A and Forced Intrusion, Risk to BES equipment and Detection of a reportable Cyber Security Incident in Part B. These events are to be reported within 1 hour. Notification of law enforcement per Part 1.3.2 is also required for		

Organization	Yes or No	Question 7 Comment
these events only.		
American Transmission Company	No	ATC does not agree with the proposed language in Requirement 3. ATC is concerned that, in order to demonstrate compliance, an entity will have to show that each step in the plan was followed which will likely leave entities facing the choice of choosing between different compliance violations. If the plan is not followed, but the report is made within the time given, then an entity is in violations of their plan. If the plan is followed, but the report does not get filed within the time allotted, then they face a possible violation of the time to report. ATC believes that the team should enforce the position that the report being filed in the time allotted is key, not that they necessarily follow and document that their plan was followed. Depending on the situation, the internal reporting will vary; however, based on the purpose of the Standard, the key is to get a report to NERC.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated R2 and revised R5 for clarity and to eliminate potential redundancy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		
Georgia System Operations Corporation	No	-We suggest moving the language from the measure to the requirement as such:"To the extent that a Reponsible Entity has an Impact Event on its Facilities, each Responsible Entity shall implement?"Additionally, R1 uses the phrase "recognized Impact Event"
Response: The DSR SDT thanks you for your comment. Requirement 2 has been deleted along with its associated Measure M2. R1 no longer references “recognized” events.		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	No	There are generally several events during the year. If the process is well documented, a drill or exercise is excessive. It should be sufficient to say “provide training.”
Response: The DSR SDT thanks you for your comment. This appears to be related to R3 in question 8. If an event occurs during the year, additional testing is not required.		
Indeck Energy Services	No	R2 is direct and to the point. The Violation Risk Factor should be Low, if any, because this is historical reporting, with little or no reliability consequence.

Organization	Yes or No	Question 7 Comment
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Midwest Reliability Organization	Yes	This clearly states that an entity's Operating Plan is to be used for reporting of Impact Events.
Response: The DSR SDT thanks you for your comment.		
Dominion	Yes	Dominion agrees subject to the comments provided in Question #6. In addition, Requirement R2 appears duplicative of Requirement R5.Suggest R2 be clarified relative to the intent.
Response: The DSR SDT thanks you for your comment. Please see responses to comments in Question 6. R2 was deleted and R5 was revised. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment]. The DSR SDT has revised R1 to eliminate the use of Operating Process and Operating Procedure and have used more generic terms.		
Manitoba Hydro	Yes	Removing "assess the initial probable cause" from the statement removes the ambiguity in the same way as replacing sabotage with impact level. Let the staff trained in this field determine probable cause after the fact.
Response: The DSR SDT thanks you for your comment.		
Occidental Power Marketing	Yes	However, only LSEs with BES assets (or assets that directly support the BES) should be included in the Applicability section of the standard.
Response: The DSR SDT thanks you for your comment. Attachment 1 specifies which types of events are required to be reported by each entity.		

Organization	Yes or No	Question 7 Comment
Constellation Power Generation	Yes	Although CPG agrees with the wording of Requirement 2, CPG has several comments and suggested changes regarding the Attachments, to which this requirement points. Please see those comments below.
Response: The DSR SDT thanks you for your comment. Please see responses below.		
Northeast Power Coordinating Council	Yes	
Western Electricity Coordinating Council	Yes	
Pacific Northwest Small Public Power Utility Comment Group	Yes	
Pepco Holdings Inc and Affiliates	Yes	
SPP Standards Review Group	Yes	
Midwest ISO Standards Collaborators	Yes	
FirstEnergy	Yes	
Southern Company	Yes	
SRP	Yes	
We Energies	Yes	
SDG&E	Yes	
City of Tallahassee (TAL)	Yes	
New Harquahala Generating Co.	Yes	

Organization	Yes or No	Question 7 Comment
APX Power Markets	Yes	
United Illuminating Co	Yes	
Liberty Electric Power LLC	Yes	
Arkansas Electric Cooperative Corporation	Yes	
Sweeny Cogeneration LP	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Independent Electricity System Operator	Yes	
Platte River Power Authority	Yes	
BGE	Yes	No comments.
Alliant Energy	Yes	
PPL Electric Utilities	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
Ingleside Cogeneration LP	Yes	
Duke Energy	Yes	

Organization	Yes or No	Question 7 Comment
Brazos Electric Power Cooperative	Yes	
Progress Energy	Yes	
Response: The DSR SDT thanks you for your comment. Based on stakeholder comments, Requirement R2 was deleted and R5 was revised. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		

8. Do you agree with the proposed revisions to Requirement 4 (now R3)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: There were several issues that commenters raised regarding removing the requirement. Below is a summary:

1) Review annual component CAN0010 states: Regardless of the registered entity's documented definition of annual, it will not supersede any requirement stated in the standard. The DSR SDT is defining "annual" within this Standard (and only for this Standard).

2) Remove R3-requirement – Several stakeholders believed the testing to be onerous. The language of the requirement was revised to indicate that only the communications portion of the Operating Plan is required to be tested. Each Responsible Entity shall conduct a test of the communication process in its Operating Plan, created pursuant to Requirement 1, Part 1.3, at least annually (once per calendar year), with no more than 15 calendar months between tests.

3) Unclear if actual events would qualify for a test in the requirement – The language in the measure was revised to add "Implementation of the communication process as documented in its Operating Plan for an actual event may be used as evidence to meet this requirement. "

4) VRF is too high on R3 – With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.

Organization	Yes or No	Question 8 Comment

Organization	Yes or No	Question 8 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation	No	With the current CAN on the definition of annual, we do not believe that the additional qualification that the test shall be conducted "with no more that 15 calendar months between tests" is necessary. If instead the team believes that, in order to support the reliability of the BES, tests should be performed at least every 15 months, then the requirement should be to perform a test at least every 15 calendar months and remove the annual component.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. Per the CAN, "Regardless of the registered entity's documented definition of annual, it will not supersede any requirement stated in the standard." The team believes the requirement is specifying what the team believes to be appropriate.		
Northeast Power Coordinating Council	No	The annual testing requirement is too frequent for a reporting, and not an operational process. The testing interval should be extended to five years.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. We feel that five years is too long of an interval between tests as contact information contained in the plan may change more often. A one year test is more likely to catch problems with the Operating Plan. If an entity has an event, then they do not need to test the plan during the annual cycle.		
Bonneville Power Administration	No	Too burdensome to go through EACH and ALL individual Impacts and report each one on a drill basis with outside entities. One or two scenarios may be OK.
Response: The DSR SDT thanks you for your comment. It is not intended to perform a test for each type of event listed in Attachment 1. The entity is free to choose any single event to test its operating plan. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The test under R3 Operating Plan is to test the communication aspect of your Operating Plan.		
Dominion	No	: The need to conduct a test of its Operating Process has not been established and is overly restrictive given that the purpose of the standard is to report Impact Events.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can		

Organization	Yes or No	Question 8 Comment
respond appropriately in the case of an actual event. The SDT thinks it is critical to test the Operating Plan to verify that employees know the appropriate actions to take and that there are no issues with the reporting procedures. Not testing the Operating Plan could result in employees being unprepared to communicate and report for an actual event.		
SPP Standards Review Group	No	The SDT included a formal review process in the discussion of R4 in the Background Information in the Unofficial Comment Form as one of three options for demonstrating compliance with the testing requirements of R4, yet M3 only contains two of those options ? a mock Impact Event exercise and a real-time implementation of its Operating Process. The third option, a formal review process, is missing from M3 and needs to be added. We would suggest the following for M3: ?In the absence of an actual Impact Event, the Responsible Entity shall provide evidence that it conducted a mock Impact Event and followed its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 or conducted a formal review of its Operating Process. The time period between tests, actual Impact Events or formal reviews shall be no more than 15 calendar months. Evidence may include, but is not limited to, operator logs, voice recordings or documentation.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The standard now has only three requirements. The requirement to test the communications process is important so that any issues or errors in the Operating Plan can be identified. The team feels that a formal review will not be able to identify any of these errors unless the communications process is tested.		
Midwest ISO Standards Collaborators	No	We appreciate the drafting team recognizes that actual implementation of the plan for a real event should qualify as a ?test?. However, we are concerned that review of this requirement in isolation of the background material and information provided by the drafting team may cause a compliance auditor to believe that a test cannot be met by actual implementation. Furthermore, we do not believe testing a reporting procedure is necessary. Periodic reminders to personnel responsible for implementing the procedure make sense but testing it does not add to reliability. If they don?t report an event, it will become obvious with all the tools (SAFNR project) the regulators have to observe system operations.
Response: The DSR SDT thanks you for your comment. We have added the following to the measure: "Implementation of the communication process as documented in its Operating Plan for an actual event may be used as evidence to meet this requirement."		
FirstEnergy	No	We believe that a separate requirement for testing the reporting process is unnecessary. The FERC directive that required periodic testing was directed at sabotage events per CIP-001. Since the proposed standard

Organization	Yes or No	Question 8 Comment
		moves the responsibility for classifying an event as sabotage from the entity to the applicable law enforcement authority, the need for a periodic drill is no longer necessary. We believe that Requirement R4 should suffice in ensuring that the individuals involved in the process are aware of their responsibilities.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The standard now has only three requirements. The requirement to test the communications process is important so that any issues or errors in the Operating Plan can be identified.		
SERC OC Standards Review Group	No	Annual testing of an ?after-the-fact? reporting procedure does not add to the reliability of the BES!
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The standard now has only three requirements. The requirement to test the communications process is important so that any issues or errors in the Operating Plan can be identified. This will allow for reporting to the appropriate entities in the case of an actual event.		
PJM Interconnection LLC	No	1. This is an ?after-the-fact? reporting requirement (administrative in nature). Annual testing of such a requirement does not add to the reliability of the BES. 2. R3 attempts to define ?Annual? for the Registered Entity to test its Operating Process. We believe R3 should follow the NERC definition of Annual as defined in the NERC Compliance Application Notice (CAN) ? CAN-0010 ? Definition of Annual as opposed to creating a new definition of Annual ? or ? refer to an entity?s defined use of the term annual.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The standard now has only three requirements. The requirement to test the communications process is important so that any issues or errors in the Operating Plan can be identified. This will allow for reporting to the appropriate entities in the case of an actual event. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. Per the CAN, “Regardless of the registered entity’s documented definition of annual, it will not supersede any		

Organization	Yes or No	Question 8 Comment
requirement stated in the standard." The team believes the requirement is specifying what the team believes to be appropriate.		
We Energies	No	A test of the Operating Process for communication would be placing telephone calls. This requirement would have virtually every entity in North America calling NERC, Regional Entities, FERC/Provincial Agency, Public Service Commission, FBI/RCMP, local Police, etc. annually. Every entity will probably be asking for a confirmation letter from each telephone call for proof of compliance. This is an unnecessary requirement. Delete it.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The standard now has only three requirements. The requirement to test the communications process is important so that any issues or errors in the Operating Plan can be identified. This will allow for reporting to the appropriate entities in the case of an actual event.		
Compliance & Responsiblity Organization	No	See comments set forth in number 2. Also, while NextEra understands the need to have a testing requirement for sabotage (Order 693 at P 446), it does not find it necessary to have a testing requirement for the other events. At this time in the process, additional requirements for the sake of having a requirement are likely to detract from reliability. Thus, NextEra requests that the testing requirement be limited to sabotage related events.
Response: The DSR SDT thanks you for your comment. Please see responses to Question 2 above. Each entity may choose an event type for which to perform the communications process test. It need not be performed for each and every event type listed in Attachment 1. The test must include all aspects of the communications process, including NERC and the RE. The measure for R3 was revised to make it explicit that evidence for compliance for R3 includes an actual event. M3. The Responsible Entity shall provide evidence that it conducted a test of the communication process as documented in its Operating Plan impact events created pursuant to Requirement R1, Part 1.3. Implementation of the communication process as documented in its Operating Plan for an actual impact event may be used as evidence to meet this requirement. The time period between an actual impact event or test shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or dated documentation of a test. (R3)		
Exelon	No	- Each entity should be able to determine if they need a drill for a particular event. Is this document implying that the annual drill covering all applicable [Impact] Events?

Organization	Yes or No	Question 8 Comment
		- A provision should be added to be able to take credit for an existing drill/exercise that could incorporate the required communications to meet the intent of R.3 to alleviate the burden on conducting a standalone annual drill. The DSR SDT needs to provide more guidance on the objectives and format of the drill expected (e.g., table top, simulator, mock drill). - A provision should be added to R.3 to allow for an actual event to be used as credit for the annual requirement. It would seem that the intent is as such based on the wording in M.3; however, it needs to be explicit in the Requirement. - Must a test include communicating to NERC or the Region?
Response: The DSR SDT thanks you for your comment. Each entity may choose an event type for which to perform the communications process test. It need not be performed for each and every event type listed in Attachment 1. The test must include all aspects of the communications process, including NERC and the RE. The measure for R3 was revised to make it explicit that evidence for compliance for R3 includes an actual event. M3. The Responsible Entity shall provide evidence that it conducted a test of the communication process as documented in its Operating Plan impact events created pursuant to Requirement R1, Part 1.3. Implementation of the communication process as documented in its Operating Plan for an actual impact event may be used as evidence to meet this requirement. The time period between an actual impact event or test shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or dated documentation of a test. (R3)		
City of Tallahassee (TAL)	No	Comments: The verbiage “at least annually, with no more than 15 months between such tests” is an attempt to define annually. If you want every 15 months say “at least every 15 months.” Otherwise just say annual and let the entities decide what that is, as is being done with other “annual” requirements. Additionally, while the Measure (M3) implies that an actual event would suffice it is not stated in the requirement, and the entire plan should be tested, not just a component. Proposed: Each Responsible Entity shall conduct a test of its Impact Event Operating Plan at least annually. A test of the Impact Event Operating Plan can range from a paper drill, to the response to an actual event.
Response: The DSR SDT thanks you for your comment. The language now reads: “annually (once per calendar year), with no more than 15 calendar months between tests”. This comports with the intent and with the recent CAN from NERC on the use of “Annual”. The intent of the requirement is to verify that an entity’s personnel can communicate with other entities when a real event occurs. It is expected that such a test will include all aspects of the communications process. The measure was revised to clarify that an actual event can be used in lieu of a test. R3 reads: “Each Responsible Entity shall conduct a test of the communication process as documented in its Operating Plan, created pursuant to Requirement 1, Part 1.3, impact events at least annually, (once per calendar year), with no more than 15 calendar months between tests.”		

Organization	Yes or No	Question 8 Comment
Tenaska	No	The proposed Impact Event Operating Plan should not be required, therefore any tests of the Operating Process should not be required.
Response: The DSR SDT thanks you for your comment. Stakeholder consensus indicates that the majority of stakeholders agree with the Operating Plan requirement.		
American Municipal Power	No	No, remove R3. R3 is not an acceptable requirement nor should this be an operation. Focusing on a test is overly prescriptive and costly. The only requirement should be to have an entity submit a report. Let the entity decide how they want to implement the reporting.
Response: The DSR SDT thanks you for your comment. The intent of the requirement is to verify that an entity's personnel can communicate with other entities when a real event occurs. It is expected that such a test will include all aspects of the communications process. The measure was revised to clarify that an actual event can be used in lieu of a test. This should not be a costly nor burdensome requirement.		
Liberty Electric Power LLC	No	It is not the proper role of the standards to dictate how an entity conducts training. Large utilities with backup control rooms and enough personnel can conduct routine drills without disturbing operations, but this is not always the case for small entities. Further, classroom training where emergency responses are discussed can be a better tool at times for assuring compliance with operating procedures. I would suggest R3 read "Each entity shall assure that personnel are aware of the requirements of EOP-004 and capable of responding as required."
Response: The DSR SDT thanks you for your comment. The DSR SDT agrees and has removed the training Requirement, R4.		
Sweeny Cogeneration LP	No	We do not see a reliability benefit in the planning and execution of tests or drills to ensure that regulatory reporting is performed in a timely fashion. It is sufficient that penalties can be assessed against entities that do not properly respond in accordance with EOP-004-2, leaving it to us to determine how to avoid them.
Response: The DSR SDT thanks you for your comment. The intent of the requirement is to verify that an entity's personnel can communicate with other entities when a real event occurs. It is expected that such a test will include all aspects of the communications process. The measure was revised to clarify that an actual event can be used in lieu of a test.		
American Electric Power	No	It is unclear if actual events would qualify for a test in the requirement; however, the associated measure and rationale appear to support this. We suggest the requirement be restated to allow for actual events to count for this requirement.

Organization	Yes or No	Question 8 Comment
Response: The DSR SDT thanks you for your comment. The intent of the requirement is to verify that an entity's personnel can communicate with other entities when a real event occurs. It is expected that such a test will include all aspects of the communications process. The measure was revised to clarify that an actual event can be used in lieu of a test.		
New Harquahala Generating Co.	No	M3. In the absence of an actual Impact Event, the Responsible Entity shall provide evidence that it conducted a mock Impact Event and followed its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The time period between actual and or mock Impact Events shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or documentation. (R3). The measure for R3 needs to make it clear that "exercise/drill/actual employment" can be a classroom exercise, utilizing scenarios for discussion. It should not be necessary to fully test the plan by making actual phone calls, notifications etc.
Response: The DSR SDT thanks you for your comment. The intent of the requirement is to verify that an entity's personnel can communicate with other entities when a real event occurs. It is expected that such a test will include all aspects of the communications process including making actual phone calls, etc. The measure was revised to clarify that an actual event can be used in lieu of a test. The purpose of the requirement is to ensure that the communications process works.		
ISO New England, Inc	No	We appreciate and agree with the drafting team recognizes that actual implementation of the plan for a real event should qualify as a "test." However, we are concerned that review of this requirement in isolation and without the benefit of the background material and information provided by the drafting team may cause a compliance auditor to believe that a test cannot be met by actual implementation. Furthermore, we do not believe testing a reporting procedure is necessary. Periodic reminders to personnel responsible for implementing the procedure make sense but testing it does not add to reliability. If they don't report an event, it will become obvious to compliance auditors. Recommend using language similar to CIP-009. "Each Responsible Entity shall conduct a an exercise of its operating process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 at least annually, with no more than 15 calendar months between exercises." An exercise can range from a paper drill, to a full operational exercise, to reporting of actual incident Also, we question the need to conduct a test annually. Since this is only a reporting Standard and, as such, has no direct impact on reliability, we suggest modifying the testing requirement to once every three years. CIP-009-3 **R.2** Exercises —The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident. **M2.** The Responsible Entity shall make available its records documenting required exercises as specified in

Organization	Yes or No	Question 8 Comment
		Requirement R2.
Response: The DSR SDT thanks you for your comment. The intent of the requirement is to verify that an entity's personnel can communicate with other entities when a real event occurs. It is expected that such a test will include all aspects of the communications process. The measure was revised to clarify that an actual event can be used in lieu of a test.		
Calpine Corp	No	Absent substantial evidence that the proposed requirement addresses an actual systemic problem with actual submittal of reports of electrical disturbances, Requirement R4 should be removed. Failure to properly report events is currently sanctionable under CIP-001-1 and EOP-004-1 and will continue to be sanctionable under proposed EOP-004-2. Entities are capable of implementing procedures appropriate to ensure compliance with the actual reporting requirements without the addition of this "test." Alternately, if this requirement for annual tests is retained, it should be supplemented with a detailed example of an acceptable test and acceptable documentation of the test to avoid future compliance and enforcement issues. Stating "evidence may include, but is not limited to..." provides broad and unnecessary opportunity for future compliance and enforcement issues. Any difficulty the committee might encounter in developing such a detailed example would be instructive of the probable compliance and issues that would ensure from implementation of the requirement.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The requirement is written so that it is not prescriptive and allows the entity flexibility in how it tests its communications process.		
BGE	No	Requirement 3 (formerly R4) should be removed altogether because it is covered by the new R4. The topic of Disturbance Reporting is covered several times each year during operator training classes and the operators are tested on the material. Actual issued Disturbance Reports throughout the year are also covered during training class.
Response: The DSR SDT thanks you for your comment. R4 was a training requirement which has been revised and incorporated into Requirement R1, Part 1.5. This now calls for an annual review of the Operating Plan rather than training. The intent of the review is to ensure that the plan is up to date.		
Georgia System Operations Corporation	No	-With the current CAN on the definition of annual, we do not believe that the additional qualification that the test shall be conducted "with no more that 15 calendar months between tests" is necessary. Although we understand the additional qualification

Organization	Yes or No	Question 8 Comment
Response: The DSR SDT thanks you for your comment. The CAN language defers to the standard drafting team for any qualifications on "annual." The DSR SDT prefers the existing language.		
Indeck Energy Services	No	For smaller entities, for which few of the Attachment 1 events apply (eg a 75 MW wind farm), a drill is overkill. Reviewing the procedure during training should be sufficient. The solution is to require a drill for any entity for which any of the Attachment 1 events would cause a Reportable Disturbance or reportable DOE OE-417 event and training review for any other entities. The Violation Risk Factor should be Low, if any, because this is historical reporting, with little or no reliability consequence.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. Any drill or exercise that meets the intent of the requirement is acceptable. **VRF:** With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
ExxonMobil Research and Engineering	No	The annual (15 month) time window for conducting annual performance tests appears to be reasonable. However, the required scope of the test is vague. The Standard Drafting Team should modify the testing requirement to include boundary criteria such as whether notifications to third parties and law enforcement are required or if the test is limited to internal notifications and response processes. Furthermore, the current measure associated with this requirement, EOP-004 Revision 2 Measure 3, implies, that if an Impact Event occurs, the registered entity can count the activation of its Impact Event Operating Plan as a test and extend the test window 15 months from the date of activation. The Standard Drafting Team should revise the requirement to clarify that the test window resets when a site initiates its Impact Event Operating Plan in response to a real Impact Event as requirement criteria should not be included in a measure.

Organization	Yes or No	Question 8 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. It is expected that such a test will include all aspects of the communications process. The measure was revised to clarify that an actual event can be used in lieu of a test.		
Occidental Power Marketing	No	We understand that this requirement is meant to comply with FERC Order 693, Section 466; however, there needs to be more specificity concerning what sort of "test" would be accepted for auditing purposes. Also, only LSEs with BES assets should be included in the Applicability section of the standard.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The requirement is written so that it is not prescriptive and allows the entity flexibility in how it tests its communications process.		
Lincoln Electric System	No	As currently drafted, requirement R3 states one must “conduct a test” whereas the associated Measure requests evidence that one “conducted a mock Impact Event.” The Rationale box lends to further confusion by referencing a “drill or exercise” as a process to verify one’s Operating Process. To avoid potential confusion between R3 and M3, as well as to maintain consistency with the Rationale box, recommend the drafting team replace the word “test” with “drill or exercise” within R3 and the associated Measure.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. It is not a common practice to include explanatory text in a requirement. The Results-based standards format allows the Rationale boxes to serve this role. The Rationale box includes language that indicates that an actual implementation of the plan counts as a test.		
Farmington Electric Utility System	No	The measure for R3 indicates an actual Impact Event would count as a test, consider aligning the requirement with the measure to clarify an Impact Event could be considered a test.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. It is not a common practice to include explanatory text in a requirement. The Results-based standards format allows the Rationale boxes to serve this role. The Rationale box includes language that indicates that an actual implementation of the plan counts as a test.		

Organization	Yes or No	Question 8 Comment
Ingleside Cogeneration LP	No	Since the reporting of event data to regulatory agencies does not support a front-line operations capability to mitigate or restore a BES impairment, regular simulations are not needed. Those notification items which test coordination between operating entities can be addressed in emergency operations exercises.
Response: The DSR SDT thanks you for your comment. We concur with your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event.		
Constellation Power Generation	No	As CPG stated in comments to earlier versions of EOP-004-2, this requirement adds a substantial compliance burden with little to no reliability improvement to the BES. Numerous entities in the NERC footprint have created fleet wide compliance programs for their facilities, instead of overseeing multiple stand alone compliance programs. This was done not just for the ease of administration, but it also greatly improves the reliability of the BES by ensuring consistency across multiple facilities. By requiring each responsible entity to test the Operating Process, those under a fleet wide compliance program will end up testing the same Operating Process numerous times. This would be inefficient, ineffective and unnecessarily costly. If the testing requirement remains, then the Responsible Entity should be able to take credit for testing of the Operating Process regardless of which entity in the fleet tested it. Alternatively, the drafting team should consider removing Requirement 3 (formerly R4) because in practice it is covered by the new R4. As discussed below R4 needs refinement, but the topic of Disturbance Reporting is covered during annual training.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. If the intent of this requirement is fulfilled by another exercise or drill conducted by the responsible entity, then that will meet the requirement.		
Duke Energy	Yes	We understand that the objective of this requirement is to test the Operating Process for communicating Impact Events; and that such test could be an actual exercise, a formal review, or a real-time implementation. But given that R1.4 requires updating the Operating Plan within 90 days of any changes, we believe the VRF for R3 should be LOW instead of MEDIUM.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a “lower” VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is		

Organization	Yes or No	Question 8 Comment
responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Progress Energy	Yes	Do all individuals who are assigned roles and responsibilities in the Impact Event Operating Plan have to be involved with the test each time? Since there are multiple different types of Impact Events, it seems likely that only a subset of those Impact Events would be tested during an annual test, and therefore only a subset of individuals with responsibilities in the Impact Event Operating Plan would participate. For example, one test may exercise the Operating Process for properly reporting damage to a power plant that is a Critical Asset, and personnel from the Distribution Provider would not be involved in that test. Would such a scenario meet the requirement for the annual test? If so, it seems that some aspects of the Plan may never actually be required to be tested. This is ok, since R4 requires an annual review with personnel with responsibilities in the Impact Event Operating Plan. It must be made clear what is required in the annual test.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The requirement is written so that it is not prescriptive and allows the entity flexibility in how it tests its communications process.		
Manitoba Hydro	Yes	This requirement appears to be written so as to leave how each entity tests this procedure is up to them and not how. The testing of this procedure could vary vastly from entity to entity, meaning there is no set protocol on this procedure. As long as this requirement remains open, it is fair.
Response: The DSR SDT thanks you for your comment.		
United Illuminating Co	Yes	: FERC did state in Order 693 that the reporting procedure requires testing. UI is concerned that the scope of the requirement is unspecified. Does the exercise require only one type of Impact Event to be exercised per period, or is an entity required to simulate each Impact Event and notification
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. If your communications process differs by event type, then all communications should be tested.		

Organization	Yes or No	Question 8 Comment
Southern Company	Yes	This will cause all of the entities listed in R1.3.2 to receive test communications from all of the applicable entities annually.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The standard now has only three requirements. The requirement to test the communications process is important so that any issues or errors in the Operating Plan can be identified. This will allow for reporting to the appropriate entities in the case of an actual event.		
SRP	Yes	
SDG&E	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
Arkansas Electric Cooperative Corporation	Yes	
Platte River Power Authority	Yes	
Alliant Energy	Yes	
CenterPoint Energy	Yes	
USACE	Yes	
Independent Electricity System Operator	Yes	
PPL Electric Utilities	Yes	
American Transmission Company	Yes	

Organization	Yes or No	Question 8 Comment
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	
Brazos Electric Power Cooperative	Yes	
Midwest Reliability Organization	Yes	
Western Electricity Coordinating Council	Yes	
Pacific Northwest Small Public Power Utility Comment Group	Yes	
PSEG Companies	Yes	
Pepco Holdings Inc and Affiliates	Yes	

9. Do you agree with the proposed revisions to Requirement 5 (now R4)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: A significant number of commenters indicated that there was confusion surrounding the use of the term "review" in Requirements R3 and R4. Similar comments suggested that the measure for Requirement R4 has a training connotation, which is inconsistent with the language in the requirement, which uses the term "review." The DSR SDT has eliminated Requirement R4 and added a part to Requirement 1, Part 1.5, to require a process for ensuring that the event Operating Plan is reviewed at least annually, with no more than 15 calendar months between review sessions. Eliminating R4 and adding Part 1.5 maintains the intent while eliminating potential confusion and redundancy.

Other commenters suggested revisions to the use of the term annual. The DSR SDT reviewed the NERC definition of Annual as defined in the NERC Compliance Application Notice (CAN) CAN-0010, which provides drafting teams latitude to define the term within a requirement as they intend it to be used.

Organization	Yes or No	Question 9 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation	No	We do not believe that the requirement should specify that the plan must be reviewed with those personnel who have responsibilities identified in that plan as there is no requirement in R1 that the plan must identify any specific personnel responsibilities. Additionally, we seek clarification on whether review in this instance means train as indicated in the measure.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated requirement R4 and added a Part under Requirement R1, to require a process for ensuring that the event Operating Plan is reviewed at least annually, with no more than 15 calendar months between review sessions. By adding this Part to Requirement R1, the SDT has eliminated confusion and redundancy around the use of the term "review" and the training connotation in the Measure.		
Dominion	No	The need to periodically review its Impact Event Operating Plan has not been established and is overly restrictive (annually) given that the purpose of the standard is to report Impact Events. Suggest removing this requirement
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated requirement R4 and added a Part under Requirement R1, to require a process for ensuring that the event Operating Plan is reviewed at least annually, with no more than 15 calendar months between review sessions. The DSR SDT		

Organization	Yes or No	Question 9 Comment
's intent is to ensure that there is no gap in the review of the Operating Plan even though the plan has provision(s) for updating the event Operating Plan within 90 days of any change to its content. By adding this Part to Requirement R1, the SDT has eliminated confusion and redundancy around the use of the term "review" and the training connotation in the Measure.		
SPP Standards Review Group	No	There is confusion surrounding the use of the term review in R3 and R4. In R3 and the suggested revision to M3 in Question 8, review is an analysis of the plan by a specific group tasked to determine if the plan requires updating or modifying to remain viable. Review in R4 has training connotations for all personnel who have responsibilities identified in the plan. Although we understand the use of review in R4 is new to this version of EOP-004-2, we believe it may be more appropriate to use training rather than review in R4. And further, we feel the training should be focused on those specific portions of the plan that apply to specific job functions.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated Requirement R4 and added a Part under Requirement R1, to require a process for ensuring that the event Operating Plan is reviewed at least annually, with no more than 15 calendar months between review sessions. By adding this Part to Requirement R1, the SDT has eliminated confusion and redundancy around the use of the term "review" and the training connotation in the Measure.		
FirstEnergy	No	We believe that Requirement 4 does not warrant a Medium risk factor. For example, a simple review of the process does not have the same impact on the Bulk Electric System as the implementation of the Operating Plan per R2. Therefore, we believe R4 is at best a Low risk to the BES.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated Requirement R4 and has re-evaluated the Violation Risk Factors for each requirement. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
We Energies	No	Include that this is for internal personnel as stated in the associated measure.

Organization	Yes or No	Question 9 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated Requirement R4 and the associated Measure.		
Compliance & Responsibility Organization	No	See comments set forth in number 2
Response: Thank you for your comments and suggestions. Please see responses to question 2.		
Exelon	No	Need more guidance on what personnel are expected to participate in the annual review. Training for all participants in a plan should not be required. Many organizations have dozens if not hundreds of procedures that a particular individual must use in the performance of various tasks and roles. Checking a box that states someone read a procedure does not add any value. This is an administrative burden with no contribution to reliability. If the intention is that internal personnel who have responsibilities related to the Operating Plan cannot assume the responsibilities unless they have completed training. This requirement places an unnecessary burden on the registered entities to track and maintain a database of all personnel trained and should not be a requirement for job function. A current procedure and/or operating plan that addresses each threshold for reporting should provide adequate assurance that the notifications will be made per an individual's core job responsibilities.
Response: Thank you for your comments. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The requirement is written so that it is not prescriptive and allows the entity flexibility in how it tests its communications process.		
City of Tallahassee (TAL)	No	The verbiage at least annually, with no more than 15 months between review sessions is an attempt to define annually. If you want every 15 months say at least every 15 months. Otherwise just say annual and let the entities decide what that is, as is being done with other annual requirements.
Response: Thank you for your comment. The DSR SDT took into consideration the CAN on the definition of 'Annual" and wrote the requirement to meet the intent of the team.		
Tenaska	No	The proposed Impact Event Operating Plan should not be required.
Response: The DSR SDT thanks you for your comment. The DSR SDT considers the proposed event Operating Plan a document that identifies the activities to achieve the purpose to improve industry awareness and the reliability of the Bulk Electric System. The DSR SDT has revised R1 to only include development of an Operating Plan that includes the sub-requirements of R1.		

Organization	Yes or No	Question 9 Comment
American Municipal Power	No	No, remove R4. R4 is not an acceptable requirement nor should this be an operation. Focusing on a plan and personnel tracking is overly prescriptive. The only requirement should be to have an entity submit a report. Let the entity decide how they want to implement the reporting.
Response: The DSR SDT thanks you for your comment. The DSR SDT has taken into consideration your comment, eliminated Requirement R4, and added Requirement R1, Part 1.5. The SDT agrees that the Registered Entity can decide on the how to implement the reporting; however, this requirement mandates that the Registered Entity document its process.		
Liberty Electric Power LLC	No	Again, the entity should determine the need for review of any procedure. Changing circumstances may dictate a shorter cycle, but no changes could dictate a longer review. I will note that spill prevention plans are required to be reviewed every five years, so I question the need for an 18-month review of the EOP plan.
Response: The DSR SDT thanks you for your comment. The review provisions are designed to ensure that contact information for internal and external organizations are correct and up to date.		
Arkansas Electric Cooperative Corporation	No	We appreciate the effort the team has taken in improving the requirements since the last posting. We request the team clarify if this also includes personnel observing and reporting the requirements or only those specifically listed in the plan. The measure seems to indicate it only includes those listed in the plan, but this is not clear in the requirement. If it includes those personnel involved in observing and notifying management, then this might include a significant portion of the organization. In either case, we feel the requirement should be modified as "review applicable portions of its Impact Event Operating Plan....
Response: The DSR SDT thanks you for your comment. The training provisions of the standard have been removed. The DSR SDT intent is to ensure that the Registered Entity has Operating Plan(s) for the identification of events, establishing which internal personnel are involved, identification of outside agencies to be notified, and having a provision for updating the plan(s). The SDT feels that current Sabotage Reporting guidelines already provide much of the information needed in the new R1.		
Calpine Corp	No	Failure to properly report events is currently sanctionable under CIP-001-1 and EOP-004-1 and will continue to be sanctionable under proposed EOP-004-2. Entities are capable of implementing procedures appropriate to ensure compliance with the actual reporting requirements without the addition a formal requirement to annually review their internal procedures with personnel. In the unlikely event that an entity cannot attain this level of operating competence without implementation of a new requirement, such Entities would be subject to enforcement under Requirement R5. Absent substantial evidence of systemic problems by Entities in contacting local law enforcement properly or failures to complete event reports to appropriate agencies when provided with clear guidance on the events to be reported, this requirement is unnecessary.

Organization	Yes or No	Question 9 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Requirement R2 and revised Requirements R1 and R5 to address your concern. Requirement R5 (now R2) reads: R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
ExxonMobil Research and Engineering	No	Its unclear whether R4 is a training requirement to train all individuals who may be required to implement its Impact Event Operating Plan on an annual basis or a requirement for an Entity to review the Impact Event Operating Plan with at least one person from each position that has a role in the Impact Event Operating Plan in order to complete a quality review of the Impact Event Operating Plan. The SDT should clarify the intent of the requirement. If the intent is that both of the aforementioned interpretations is expected to occur, the SDT should break R4 into two requirements so that an entity is not violation of Requirement R4 when the entity fails to comply with one of the two imbedded requirements (e.g. if the quality review is not performed but all individuals were trained).
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Requirement R4 and added a new Part 1.5 under R1 to address your concern. Part 1.5 calls for an annual review of the plan.		
Constellation Power Generation	No	The purpose of this requirement as currently worded is unclear. It seems to insinuate that a formal review of the Operating Plan takes place annually, and that any and all personnel identified in the plant are part of the review. If that is correct, than CPG believes this requirement is echoing Requirement 3. These two requirements can be incorporated into one. Furthermore, the Measure for R4 is too prescriptive, going so far as to specifically describe how this formal review should take place. It even states that the Responsible Entity needs to present documentation showing that the personnel in the plan were trained, yet there is no requirement for training. CPG would like the DSR SDT to revisit the purpose and intent of this requirement, alone and in concert with R3. If there are indeed similar then consolidate them into one requirement.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Requirement R4 and added a new Part 1.5 under R1 to address your concern. Part 1.5 calls for an annual review of the plan.		
Georgia System Operations Corporation	No	With the current CAN on the definition of annual, we do not believe that the additional qualification that the test shall be conducted "with no more that 15 calendar months between reviews" is necessary. Remove "with no more that 15 calendar months between reviews.
Response: The DSR SDT thanks you for your comment. The SDT has revised the term annual to align with the definition in the NERC Compliance Application		

Organization	Yes or No	Question 9 Comment
Notice (CAN) CAN-0010.		
SERC OC Standards Review Group	Yes	We agree with the concept, but disagree with the use of the term Operating Plan as a defined term in line with our comments in question 6 above.
Response: The DSR SDT thanks you for your comment. The DSR SDT believes that the use of a defined term "Operating Plan" to describe the procedure to identify and report the occurrence of a disturbance is appropriate and has revised Requirement R1 to remove the terms Operating Process and Operating Procedure to eliminate confusion.		
PJM Interconnection LLC	Yes	1. We agree with the concept but disagree with the use of the term Operating Plan as a defined term in line with our comments to Question 6 above. 2. R4 attempts to define Annual for the Registered Entity to review its Impact Operating Plan. We believe R4 should follow the NERC definition of Annual as defined in the NERC Compliance Application Notice (CAN) CAN-0010 Definition of Annual as opposed to creating a new definition of Annual or refer to an entities defined use of the term annual.
Response: The DSR SDT thanks you for your comment. Please see responses to question 6 above. The DSR SDT reviewed the NERC definition of Annual as defined in the NERC Compliance Application Notice (CAN) CAN-0010. The NERC CAN provides drafting teams latitude to define annual within a Requirement as they believe is appropriate in the context of a particular standard.		
United Illuminating Co	Yes	As written it is a training burden. Certain persons will have only one step in one operating procedure to perform. There is no necessity to review the entire Operating Plan with them. For example, Field Personnel need to know that if they see something not right to report it immediately. In this instance there is no benefit to review the Operating Procedure/Process for firm load shedding with them.
Response: The DSR SDT thanks you for your comment. The training requirement has been removed. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The DSR SDT has removed R4 to eliminate potential confusion and redundancy around the training connotation.		
Manitoba Hydro	Yes	Removing the extreme details within 30 days of revision and train before given responsibility and giving leeway to when this training is necessary, will allow training to be integrated into other existing training schedules. Inclusion of 5.3 and 5.4 would require unique set of time lines and additional resources to monitor and implement.
Response: The DSR SDT thanks you for your comment. The training provisions of the standard have been removed.		

Organization	Yes or No	Question 9 Comment
Occidental Power Marketing	Yes	However, only LSEs with BES assets (or assets that directly support the BES) should be included in the Applicability section of the standard.
Response: The DSR SDT thanks you for your comment. Attachment 1 specifies which types of events are required to be reported by each entity. LSE is included here due to CIP-002-3 applicability.		
Farmington Electric Utility System	Yes	A review of the Impact Event Operating Plan can be interrupted as an informal examination of the plan. The measure for R4 indicates evidence of a review, parties conducting the review AND when internal training occurred. It should be clarified in R4 training is expected as part of the review for personnel with responsibilities. This is an improvement from the previous 5.3 and 5.4, however, the team should consider adding back, and review/training shall be conducted prior to assuming the responsibility in the plan.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Requirement R4 and added a new Part 1.5 under R1 to address your concern. Part 1.5 calls for an annual review of the plan.		
Ingleside Cogeneration LP	Yes	Yearly refresher training on the reporting process is appropriate. Ingleside Cogeneration also agrees that a review with those individuals with assigned responsibilities under the Operating Plan is a better way to frame the requirement.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Requirement R4 and added a new Part 1.5 under R1 to address your concern. Part 1.5 calls for an annual review of the plan.		
Indeck Energy Services		R4 is redundant with R3 and should be deleted. The Violation Risk Factor should be Low, if any, because this is historical reporting, with little or no reliability consequence.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Requirement R4 and revised R3. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the		

Organization	Yes or No	Question 9 Comment
approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Northeast Power Coordinating Council	Yes	
Bonneville Power Administration	Yes	
Midwest Reliability Organization	Yes	
Western Electricity Coordinating Council	Yes	
Pacific Northwest Small Public Power Utility Comment Group	Yes	
PSEG Companies	Yes	
Pepco Holdings Inc and Affiliates	Yes	
Midwest ISO Standards Collaborators	Yes	
Southern Company	Yes	
SRP	Yes	
SDG&E	Yes	
New Harquahala Generating Co.	Yes	

Organization	Yes or No	Question 9 Comment
APX Power Markets	Yes	
Sweeny Cogeneration LP	Yes	
American Electric Power	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Independent Electricity System Operator	Yes	
ISO New England, Inc	Yes	
Platte River Power Authority	Yes	
BGE	Yes	No comments.
Alliant Energy	Yes	
CenterPoint Energy	Yes	
PPL Electric Utilities	Yes	
Lincoln Electric System	Yes	
American Transmission Company	Yes	
Duke Energy	Yes	
City of Tacoma, Department	Yes	

Organization	Yes or No	Question 9 Comment
of Public Utilities, Light Division, dba Tacoma Power		
Brazos Electric Power Cooperative	Yes	
Progress Energy	Yes	

10. Do you agree with the proposed revisions to Requirement 6 (now R5) and the use of either Attachment 2 or the DOE-OE-417 form for reporting? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: The slight majority of commenters suggested revisiting R2 and R5 to eliminate potential redundancy and confusion. The intent of the two requirements is to have entities utilize the DOE Form OE-417 to report events listed on Attachment 1. If the entity completes DOE Form OE-417 to report an event, it does not have to transcribe the same information onto Attachment 2 but may be required to submit the form to the DOE and NERC. By eliminating R2 and revising R5 (now R2), the DSR SDT has maintained the intent of the requirements.

R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.

Organization	Yes or No	Question 10 Comment
Northeast Power Coordinating Council	No	R5 stipulates the use of Attachment 2 or the DOE-417, which is the vehicle for reporting only. This is the how part, not the what. The vehicle for reporting can easily be included in ***R2 where an entity is required to implement (execute) the Operating Plan upon detection of an Impact Event***. Suggest combining R2 with R5.
Response: The DSR SDT thanks you for your comment. The DSR SDT has also eliminated R2 and revised R5 (now R2) for clarity and to eliminate potential redundancy. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
Dominion	No	Dominion does not agree because the Requirement is too restrictive giving the Responsible Entity the choice on reporting forms as either Attachment 2 or DOE OE-417. The use of Attachment 2 or DOE OE-417 may be appropriate when reporting to NERC, however, Requirement R 1.3.2 requires the Responsible Entities Impact Event Operating Plan to address notifications to non-NERC entities such as Law Enforcement or Governmental Agencies. It is likely that these organizations have specific reporting requirements or forms that will not line up the options prescribed in Requirement R5.Suggest revising Requirement R5 to not require the use of these two forms as the only options. If these 2 forms are used, suggest aligning the Event names in Attachment 1 to be similar to the criteria for filing event names in the DOE OE-417 to allow for consistency.

Organization	Yes or No	Question 10 Comment
		Also suggest aligning the time to submit for similar event names in each form.
Response: The DSR SDT thanks you for your comment. The DSR SDT has revised Attachment 1 to indicate that entities must submit Attachment 2 or the DOE OE-417 form. This information was contained in Requirement 5. The intent of the two requirements is to have entities make appropriate notifications and report events contained in Attachment 1. By eliminating R2 and revising R5 (now R2), the DSR SDT has maintained the intent of the requirements while eliminating potential confusion and redundancy. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1. The DSR SDT has enhanced Attachment 1 and clarified the intent of each event, threshold and reporting time limits. The DSR SDT removed the column, Time to Submit Report and replaced it with Submit Attachment 2 or DOE OE-417 Report.		
SPP Standards Review Group	No	We feel there is redundancy between R2 and R5. To eliminate this redundancy, we propose to take the phrase using the form in Attachment 2 or the DOE OE-417 reporting form and adding it at the end of R2. Then what is left of R5 could be deleted. The new R2 would read Each Responsible Entity shall implement its Impact Event Operating Plan documented in Requirement R1 for Impact Events listed in Attachment 1 (Parts A and B) using the form in Attachment 2 or the DOE OE-417 reporting form.?
Response: The DSR SDT has revised Attachment 1 to indicate that entities must submit Attachment 2 or the DOE OE-417 form. This information was contained in Requirement 5. The intent of the two requirements is to have entities make appropriate notifications and report events contained in Attachment 1. By eliminating R2 and revising R5 (now R2), the DSR SDT has maintained the intent of the requirements while eliminating potential confusion and redundancy. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
Midwest ISO Standards Collaborators	No	Requirement 2 and Requirement 5 appear to be very similar. Requirement 2 requires implementation of the Operating Plan, Operating Process and/or Operating Procedure in Requirement 1. The Operating Procedure requires gathering and reporting of information for the form in Attachment 2. What does Requirement 5 add that is not already covered in Requirement 2 except the ability to use the DOE OE-417 reporting form which
Response: The DSR SDT thanks you for your comment. The intent of the two requirements is to have entities utilize the DOE Form OE-417 to report events listed on Attachment 1. If the entity completes DOE Form OE-417 to report an event, they do not have to transcribe onto attachment 2 but may be required to submit it to the U.S. Department of Energy (DOE) and NERC. By eliminating R2 and revising R5 (now R2), the DSR SDT has maintained the intent of the requirements. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
FirstEnergy	No	We believe that Requirement 5 does not warrant a Medium risk factor. Not using a particular form is strictly

Organization	Yes or No	Question 10 Comment
		administrative in nature and the VRF should be Low.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
PJM Interconnection LLC	No	R5 seems redundant as R2 already requires an entity to report any Impact Events by executing/implementing its Impact Event Operating Plan. R5 merely stipulates the use of Attachment 2 or DOE-417, which an entity automatically would use for reporting purposes while implementing its Impact Event Operating Plan.
Response: The DSR SDT thanks you for your comment. The intent of the two requirements is to have entities utilize the DOE Form OE-417 to report events listed on Attachment 1. If the entity completes DOE Form OE-417 to report an event, they do not have to transcribe onto attachment 2 but may be required to submit it to the U.S. Department of Energy (DOE) and NERC. By eliminating R2 and revising R5 (now R2), the DSR SDT has maintained the intent of the requirements. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
Exelon	No	Agree that each Responsible Entity should be able to use either Attachment 2 or the DOE OE-417 form for reporting; however, a GO/GOP will not have the ability to respond to Attachment 2 Task numbers 8, 9, 10, 11, and 12. Suggest that the DSR SDT either evaluate a shortened form version, provide a note or provision for "N/A" based on registration, or revise form to be submitted by the most knowledgeable functional entity (e.g., TOP or RC).Need clear guidance as to which form is to be used for which Impact Event, we feel that one and only one form should be used to eliminate confusion. Attachment 2 has an asterisk on #s 7, 8, 9, 10 and 11 there is not reference corresponding to it.
Response: The DSR SDT thanks you for your comment. The DSR SDT has updated Attachment 2 to per comments received.		

Organization	Yes or No	Question 10 Comment
Tenaska	No	R5 should be changed to Each Responsible Entity shall report Impact Events listed in Attachment 1 using the form in Attachment 2 or the DOE OE-417 reporting form. This revised version of the proposed R5 is the only Requirement that is necessary to achieve the stated purpose of Project 2009-01. The proposed R1 through R4 should be deleted and R5 should be changed to R1.
Response: The DSR SDT thanks you for your comment. The SDT agrees the reporting is a fundamental aspect, but the operation plans are integral piece of the BES. The DSR SDT believes that the revisions created will provide clarity for the requirements. Please see the revised standard.		
American Municipal Power	No	R5 is not an acceptable requirement, but it can be improved. Each Responsible Entity shall report "Impact Events" to _____ (address specified in attachment 1, website, entity, email address, or fax, etc.) Focusing on a plan and procedure is overly prescriptive. The only requirement should be to have an entity submit a report. Let the entity decide how they want to implement the reporting.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated R2 and revised R5 (now R2) for clarity and to eliminate potential redundancy. The SDT agrees that the Registered Entity can decide on the how to implement the reporting; however, this requirement mandates that the Registered Entity document its process. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
Arkansas Electric Cooperative Corporation	No	We appreciate the effort the team has taken in improving the requirements since the last posting. For R5, we suggest including the reporting form as part of the plan in R1. Otherwise, a violation of R5 would also indicate a violation of R2.
Response: The DSR SDT thanks you for your comment. The DSR SDT has also eliminated R2 and revised R5 (now R2) for clarity and to eliminate potential redundancy. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
American Electric Power	No	This should be one-step covered by the implementation in requirement 2. We like the ability to use one form (i.e. NERC Attachment 2 or the DOE-417); however, we would prefer to have this information only be reported once.
Response: The DSR SDT thanks you for your comment. EOP-004-2 allows entities to utilize the DOE Form OE-417 to report events listed on Attachment 1. If the entity completes DOE Form OE-417 to report an event, they do not have to transcribe onto attachment 2 but may be required to submit it to the U.S. Department of Energy (DOE) and NERC.		

Organization	Yes or No	Question 10 Comment
Consumers Energy	No	We understand that DOE is migrating to an on-line reporting facility rather than the email-submitted OE-417. If they do so, Form OE-417will not be available for providing to NERC, and the reporting specified by EOP-004 will be duplicative of that for DOE. We recommend that NERC, RFC and the DOE work cooperatively to enable a single reporting system in which on-line reports are made available to all appropriate parties.
Response: The DSR SDT thanks you for your comment. The SDT agrees with the concept of the single reporting template and is working with other agencies to see if the single form would be achievable.		
Independent Electricity System Operator	No	R5 stipulates the use of Attachment 2 or the DOE-417, which is the vehicle for reporting only. This is the how part, not the what. The vehicle for reporting can easily be included in R2 where an entity is required to implement (execute) the Operating Plan upon detection of an Impact Event. We suggest the SDT combine R2 with R5.
Response: The DSR SDT thanks you for your comment. The DSR SDT has also eliminated R2 and revised R5 (now R2)for clarity and to eliminate potential redundancy. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
Ameren	No	The "Responsible Entity" should be limited to those functions with the most oversight such as the BA, RC, or TOP. Otherwise there will be multiple DOE OE-417 reports sent by multiple entities.
Response: Thank you for your comments. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received.		
ISO New England, Inc	No	R5 stipulates the use of Attachment 2 or the DOE-417, which is the vehicle for reporting only. This is the how part, not the what. The vehicle for reporting can easily be included in R2 where an entity is required to implement (execute) the Operating Plan upon detection of an Impact Event. We suggest the SDT combine R2 with R5.
Response: The DSR SDT thanks you for your comment. The DSR SDT has also eliminated R2 and revised R5 (now R2) for clarity and to eliminate potential redundancy.		
Calpine Corp	No	The use of DOE OE-417 is acceptable, but the language of Requirement R5 should be modified. The disturbance event form must be filled out correctly, irrespective of the requirements of an Entities Impact Event Operating Plan. Reference to that Plan does not add clarity to the requirement to report events. The

Organization	Yes or No	Question 10 Comment
		requirement should delete the reference to the Impact Event Operating Plan? and simply state: Each Responsible Entity shall report events listed in Attachment 1 using the provided form, or where also required to complete the current version of DOE OE-417, that form. Although one of the primary stated purposes of the original SAR was to simplify the reporting process by creating a single form, the fact that some entities are already required to report substantially identical information to DOE argues for retention of the use of the DOE form.
Response: The DSR SDT thanks you for your comment. DSR SDT has deleted requirement 2 and revised requirements R1 and R5 (now R2) to address your concern. The entire Attachment 1 has been updated to reflect the comments that were received.		
BGE	No	Language needs to be more specific on when to use Attachment 2 or DOE-OE-417.
Response: The DSR SDT thanks you for your comment. Attachment 2 should be the normal reporting vehicle unless the entity is required to submit an OE-417 to the DOE. This keeps the entity from having to file two distinctly different reports for the same event.		
Alliant Energy	No	We believe Attachment 2 should be deleted, and NERC should work with the DOE to have one form for all events, if possible. It makes the reporting procedure much simpler, only having to use one form.
Response The DSR SDT thanks you for your comment. EOP-004-2 allows entities to utilize the DOE Form OE-417 to report events listed on Attachment 1. If the entity completes DOE Form OE-417 to report an event, they do not have to transcribe onto attachment 2 but may be required to submit it to the U.S. Department of Energy (DOE) and NERC. The DSR SDT is currently working with the DOE to make revisions to Form OE-417 that would achieve the objective of your comment. We will continue to pursue this.		
ExxonMobil Research and Engineering	No	The notification requirement and documentation in Attachment 1 do not clearly identify which entities need to be notified for each type of event detailed in Attachment 1. While it makes sense to notify the Reliability Coordinator, NERC, Regional Entity, Law Enforcement and other Governmental Agencies for sabotage type events, it does not seem proper to notify Law Enforcement agencies of a system disturbance that is unrelated to improper human intervention. Furthermore, it is our belief that a time frame of 1 hour is a short window for making a verbal notification to third parties, and an impossibly short window for requiring the submittal of a completed form regardless of the simplicity. When a Petrochemical Facility experiences an impact event, the initial focus should emphasize safe control of the chemical process. For those cases where registered entities are required to submit a form within 1 hour, the Standard Drafting Team should alter the requirement to allow for verbal notification during the first few hours following the initiation of an Impact Event (i.e. allow the facility time to appropriately respond to and gain control of the situation prior to making a notification which may take several hours) and provide separate notifications windows for those parties that will need to respond to an Impact Event immediately and those entities that need to be informed that one occurred for the

Organization	Yes or No	Question 10 Comment
		purposes of investigating the cause of and response to an Impact Event. For example, a GOP should immediately notify a TOP when it experiences a forced outage of generation capacity as soon as possible, but there is no immediate benefit to notify NERC when site personnel are responding to the event in order to gain control of the situation and determine the extent of the problem. The existing standards requirement to file an initial report to entities, such as NERC, within 24 hours seems reasonable provided that proper real time notifications are made and the Standard Drafting Team reinstates EOP-004 Revision 1's Requirement 3.3, which allows for the extension of the 24 hour window during adverse conditions, into the requirement section of EOP-004 [the current revision locates this extension in Attachment 1, which, according to input received from Regional Entities, means that the extension would not be enforceable].
Response: The DSR SDT thanks you for your comment. The SDT envisions that each Registered Entity will develop Operating Plan(s) appropriate to meet its obligations as outlined in the standard. The SDT doesn't feel it necessary to prescribe to the Registered Entity any particular interpretation on how to achieve compliance, including who the information should be reported to. The entire Attachment 1 has been updated to reflect the comments that were received.		
American Transmission Company	No	Attachment 2, Task #14 in the report should be modified to read, Identify any known protection system misoperation(s). If this report is filed quickly, there is not enough time to assess all operations to determine any misoperation. As a case in point, it typically takes at least 24 hrs. to receive final lightning data; therefore, not all data is available to make a proper determination of a misoperation
Response: The DSR SDT thanks you for your comment. The entire Attachment 1 has been updated to reflect your comment.		
Constellation Power Generation	No	The requirements for filling out the DOE-OE-417 form are not necessarily the same as the requirements prescribed in Attachment 1. CPG suggests that the drafting team create a new requirement, spelling out when an entity is required to complete the DOE-OE-417 form.
Response: The DSR SDT thanks you for your comment. Any entity that is obligated to submit Form OE-417 may submit that completed form to NERC in lieu of Attachment 2.		
Georgia System Operations Corporation	No	R5: This standard should not require all Responsible Entities to report the same event. Entities should be allowed to report in a hierarchical manner. They should be allowed to coordinate impact event plans and include in their plans the entity that has the responsibility for reporting various events. Flexibility should be allowed to provide different reporting entities depending on the type of event. In R5, does each Responsible Entity shall report Impact Events in accordance with the Impact Event Operating Plan? Allow this hierarchical reporting and flexibility? An entity should be allowed to report to another operating entity by whatever reporting form or mechanism works and then the other entity reports to NERC using the required NERC or DOE form. Add "To the extent that a Responsible Entity had an Impact Event," at the beginning of R5 and

Organization	Yes or No	Question 10 Comment
		M5.
Response: The DSR SDT thanks you for your comment. Each entity is required to report their portion of the event, however they can coordinate. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, will be able to provide the ERO and others with a different views of what has happened. The DSR SDT understands that there may be multiple reports (for certain events) that are required by different government agencies. NERC will continue to streamline the reporting process as we move into the future. The DSR SDT has also eliminated R2 and revised R5 (now R2) for clarity and to eliminate potential redundancy.		
Indeck Energy Services	No	The Violation Risk Factor should be Low, if any, because this is historical reporting, with little or no reliability consequence.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Bonneville Power Administration	Yes	Reporting form OK. Note that the Frequency Maximum/Minimum Section should be clarified. A Gen Loss doesn't usually experience a high (maximum) frequency, just the low immediately following the event.
Response: The DSR SDT thanks you for your comment		
Midwest Reliability Organization	Yes	This will reduce any double reporting to the ERO and FERC.
PPL Supply	Yes	Reporting consistency and timelines may need to be reviewed for example: Fuel Supply Emergency - OE-417 requires reporting within 6 hours / Attachment 1 Part B requires reporting within 1 hour.
Response: The DSR SDT thanks you for your comment The DSR SDT has significantly revised Attachment 1 and deleted Fuel Supply Emergency from Attachment 1. This item was removed in coordination with the NERC Events Analysis Working Group and the proposed Events Analysis Program. All events are		

Organization	Yes or No	Question 10 Comment
now to be reported within 24 hours with the exception of Destruction of BES equipment, Damage or destruction of Critical Assets and Damage or destruction of Critical Cyber Asset events in Part A and Forced Intrusion, Risk to BES equipment and Detection of a reportable Cyber Security Incident in Part B.		
SERC OC Standards Review Group	Yes	We agree with the concept, but disagree with the use of the term Operating Plan as a defined term in line with our comments in question 6 above.
Response: The DSR SDT thanks you for your comment. The SDT agrees with your viewpoint and believes that your statement is consistent with the intent of the requirement. (refer to question 6)		
United Illuminating Co	Yes	Put it's before Impact Event Operating Plan.
Response: The DSR SDT thanks you for your comment. Please see the revised standard.		
Manitoba Hydro	Yes	The DOE-OE-417 appears more intuitive and descriptive (and on line ability), but having the either or option is fine.DOE-OE-417 Form is mentioned several time in this Standard, but no link to this document.
Response: The DSR SDT thanks you for your comment. Please see the revised standard.		
CenterPoint Energy	Yes	CenterPoint Energy agrees with the idea of streamlining the reporting process through the use of existing report forms. However, as noted in the response to Question 11, the Company has concerns about the DOE OE-417 Form, specifically the timeframes in which to submit reports. CenterPoint Energy will be making the same recommendation to extend reporting timeframes during the DOE OE-417 report revision process when the current form expires on 12/31/11. Any future changes to the DOE Form could also impact reporting for this requirement.
Response: The entire Attachment 1 has been updated to reflect the comments that were received. Footnotes in Attachment 1 have been updated to reflect the comments that the DSR SDT received. The DOE Form OE-417 is under review by the U.S. Department of Energy (DOE) and can be updated or changed without NERC's involvement. The DSR SDT has taken into consideration the use of OE-417 to report events to NERC and agrees that this will fulfill EOP-004-2's reporting requirements.		
PPL Electric Utilities	Yes	We would like to suggest the language be changed such that submission via a NERC system would be acceptable in addition to the use of the Attachment 2 Form or the DOE OE-417 form. The standard would then accommodate the proposed revision to NERC Rules of Procedure 812. NERC will establish a system to collect impact events reports??

Organization	Yes or No	Question 10 Comment
Response: The DSR SDT thanks you for your comment. The SDT expects any system would facilitate the reporting to organizations specified in the submitted report. Until such time that the system can be established, the Registered Entity will be obligated to make the notifications as specified in its Operating Plan(s). The DSR SDT is currently working with the U.S. Department of Energy (DOE) to make revisions to Form OE-417that would achieve the objective of your comment, and will continue to pursue this.		
Ingleside Cogeneration LP	Yes	Although our preference would be to have a single form, Ingleside Cogeneration realizes that is not likely in the near term. We would like to see that remain as a goal of the project team or the ERO.
Response: The DSR SDT thanks you for your comment. The DSR SDT is currently working with the DOE to make revisions to Form Form OE-417that would achieve the objective of your comment, and will continue to pursue this.		
Duke Energy	Yes	There is so much overlap between Attachment 2 and the DOE OE-417 that we believe the DOE OE-417 should be revised to include the additional items that must be reported to NERC, so that there is only one form to submit to NERC and DOE.
Response: The DSR SDT thanks you for your comment. The DSR SDT is currently working with the DOE to make revisions to Form OE-417 that would achieve the objective of your comment, and will continue to pursue this.		
Western Electricity Coordinating Council	Yes	
Pacific Northwest Small Public Power Utility Comment Group	Yes	
PSEG Companies	Yes	
Pepco Holdings Inc and Affiliates	Yes	
Southern Company	Yes	
SRP	Yes	
We Energies	Yes	

Organization	Yes or No	Question 10 Comment
Compliance & Responsibility Organization	Yes	
SDG&E	Yes	
City of Tallahassee (TAL)	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
Liberty Electric Power LLC	Yes	
Sweeny Cogeneration LP	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Platte River Power Authority	Yes	
Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	
Brazos Electric Power Cooperative	Yes	

11. Do you agree with the proposed revisions to Attachment 1? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: Most commenters expressed concerns with the reporting times listed in Attachment 1. Upon review of comments received concerning Attachment 1, the DSR SDT did a thorough review and updated the entire document, along with all Footnotes. The DSR SDT removed the column, Time to Submit Report and replaced it with Submit Attachment 2 or DOE OE-417 Report. There were many noted comments that a one hour reporting time frame does not coincide with an after the fact reporting Standard. The DSR SDT reviewed each time frame to report and has extended most of the time frames to 24 hours. There are a few events that have a one hour reporting requirement that was not changed because these are events that would generally be reported to law enforcement authorities and prompt reporting is in the interest of BES reliability. Duplicate reporting of events was minimized where possible. There are several events that will require reporting by multiple entities to achieve a complete enough picture to facilitate industry awareness.

Organization	Yes or No	Question 11 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation	No	As stated above in response to question 6, we believe that a column should be added to the tables to explicitly indicate what external organizations should receive the communications of a particular Impact Event type. Additionally we have concerns with the following table items: Threshold for reporting Transmission Loss: As stated, this will require the reporting of almost all transmission outages. This is particularly true taking into consideration the current work of the drafting team to define the Bulk Electric System. The loss of a single 115kV network line could meet the threshold for reporting as the definition of Element includes both the line itself and the circuit breakers. Instead, we recommend the following threshold "Three or more BES Transmission lines." This threshold has consistency with CIP-002-4 and draft PRC-002-2. This threshold also needs additional clarification as to the timeframe involved. Is the intent the reporting of the loss of 3 or more BES Transmission Elements anytime within a 24 hour period or must they be lost simultaneously? Also, we recommend that these three losses be the result of a related event to require reporting.Entity with Reporting Responsibility for Loss of Off-site power to a nuclear generating plant (grid supply): The reporting responsibility should clarify that this is only entities included in the Nuclear Plan Interface Requirements.
Response: The DSR DT thanks you for your comment. Upon review the DSR SDT has included a column to indicate the minimum parties who are required to receive the entity's notification. The Threshold for Reporting has been updated to reflect comments that have been received.		
Northeast Power Coordinating	No	As indicated under Question 4, we question the need to include IA, TSP and LSE in the responsible entities

Organization	Yes or No	Question 11 Comment
Council		for reporting.
Response: The DSR DT thanks you for your comment. The DSR SDT has established that CIP-002 and CIP-008 are applicable to an IA, TSP, and LSE. These entities will report a Cyber Security Incident per Attachment 2 (or OE-417) as the vehicle to inform the ERO, their Regional Entity and their Reliability Coordinator.		
Bonneville Power Administration	No	Generally OK, but there are too many events to report. The loss of 3 BES elements for a large geographic entity for a (5 county?) windstorm that has little impact to the system is not needed. 3 elements within the same minute could be acceptable and 6? elements still out within an hour ... or something to that affect could work.
Response: The DSR DT thanks you for your comment. Upon review the DSR SDT has included a column to indicate the minimum parties who are required to receive the entity's notification. The Threshold for Reporting has been updated to reflect comments that have been received.		
Midwest Reliability Organization	No	1) Section 9 of the Impact Reporting Form states: "List transmission facilities (lines, transformers, busses, etc.) tripped and locked out." But Part A of Attachment 1 states: "Three or more BES Transmission Elements." a. Should section 9 state: "List transmission facilities (lines, transformers, busses, etc.) tripped or locked out"? b. Should section 9 state: "List transmission elements (lines, transformers, busses, etc.) tripped or locked out"? This will align the reporting criteria with the actual reporting form.2) Section 13 of the Impact Reporting Form states: "Identify the initial probable cause or known root cause of the actual or potential Impact Event if know at the time of submittal of Part I of this report:." Recommend that "of Part I" be removed since there is no Part 2.3) Every Threshold in attachment 1 gives a clear measurable bright line, except: ?Transmission Loss?. As presently written ?Three or more BES Transmission Elements? could imply that a Report will be required to be submitted if a BES transmission substation is removed from service to perform maintenance. Or there could be three separate elements within a large substation that are out of service (and don?t effect each other) that will require a Report. Upon review of the TPL standards, there are normally planned items that our industry plans for. It is recommended that the Threshold for Reporting of Transmission Loss be enhanced to read: ?Two or more BES Transmission Elements that exceed TPL Category D operating criteria or its successor?. This threshold now is based on a actively enforced NERC Standard, and each RC and TOP are aware of what this bright line is.
Response: The DSR DT thanks you for your comment. Upon review the DSR SDT has included a column to indicate the minimum parties who are required to receive the entity's notification. The Threshold for Reporting has been updated to reflect comments that have been received. Attachment 2 has been updated to reflect the changes noted in your comments and changes per the received comments.		
PPL Supply	No	Recommendation: Add a column in Attachment 1 to acknowledge the events that require a OE-417 Report

Organization	Yes or No	Question 11 Comment
		and list the number under Schedule 1 that required Form OE-417Report. This would add accuracy and consistency among reporting entities.
Response: The DSR DT thanks you for your comment. The DOE Form OE-417 is under review by the DOE and can be updated or changed without NERC's involvement. The DSR SDT has taken into consideration the use of OE-417 to report events to NERC and agrees that this will fulfill EOP-004-2's reporting requirements.		
Pacific Northwest Small Public Power Utility Comment Group	No	The comment group is composed of smaller entities that do not all maintain 24/7 administrative support. While many of the 1 hour reporting thresholds do not affect us, some do. Others may come into play as standards are revised, such as the CIPs. We ask the SDT to consider the identification or verification that starts the clock on these may come at inopportune times for meeting a one hour deadline for these entities. Restoration may be delayed in an attempt to meet these time limits. Safety should always be the number one priority, and restoration and continuity of service second. We see reporting of these events much further down the list. We note that FERC order 693, paragraph 471 does not dictate a specific reporting time period and therefore we suggest timing requirements that promote situational awareness but allow smaller entities needed flexibility. FERC order 693, paragraph 470 directed the ERO to consider ?APPA?s concerns regarding events at unstaffed or remote facilities, and triggering events occurring outside staffed hours at small entities.? Our comment group does not believe the SDT has adequately responded to APPA?s concerns but rather took the 1 hour Homeland security requirement referenced in paragraph 470 verbatim. While a report within an hour might be ideal, it is not always practicable. We suggest: 1) as soon as possible after service has been restored to critical services within the service territory, or 2) By the COB the first business day after discovery. Our comment group realizes the difficulty in wording standards/requirements that lump small entities in with larger ones and we believe our suggestion achieves some balance. Expecting smaller entities to achieve timing requirements that can only be normally met under ideal conditions at large entities is not feasible or fair.
Response: The DSR DT thanks you for your comment. Upon review the DSR SDT has included a column to indicate the minimum parties who are required to receive the entity's notification. The Threshold for Reporting has been updated to reflect comments that have been received. EOP-004-2 requires an entity to "push" information to certain parties for industry awareness. Since this Standard is an after the fact reporting Standard, reporting times for a majority of event types reporting times for a majority of event types have been extended to allow the impacted entity to recover from the event and then report. The starting time to report is upon an entity's recognized the event, per Submit Report column of Attachment 1.		
PSEG Companies	No	For the reasons cited in response to question 4 above the language roles and responsibilities remain inconsistent and unclear. The Time to Report changes are unreasonable and there is significant duplicate reporting required.

Organization	Yes or No	Question 11 Comment
Response: The DSR DT thanks you for your comment. Upon review the DSR SDT has included a column to indicate the minimum parties who are required to receive the entity's notification. The Threshold for Reporting has been updated to reflect comments that have been received. EOP-004-2 requires an entity to "push" information to certain parties for industry awareness. Since this Standard is an after the fact reporting Standard, reporting times for a majority of event types have been extended to allow the impacted entity to recover from the event and then report.		
Dominion	No	1) A particular Event could be applicable to multiple entities and Attachment 1 would require each applicable entity to report the event. This is duplicative and would appear to overburden the reporting system. 2) Loss of off-site power (grid supply) reporting for nuclear plants is duplicative of reporting done to satisfy NRC requirements. Given the activity at a nuclear plant during this event, this additional reporting is not desired. 3) Cyber intrusion remains an event that would need to be reported multiple times (e.g., this standard, OE-417, NRC requirements, etc.). 4) Since external reporting for other regulators (e.g., DOE, NRC, etc.) remains an obligation of the Applicable Entity, suggest that Attachment 1 only contain impact events as defined in the current version of EOP-004.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the functional entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The DSR SDT understands that there may be multiple reports (for certain events) that are required by different governing agencies. NERC will continue to streamline the reporting process in the future.		
Pepco Holdings Inc and Affiliates	No	The entity responsible for reporting is not clear. Is the initiating entity the same as requesting entity or implementing entity? In the paper it indicates the DT intent is for the entity that performs the action or is directly affected will report.It seems that the proposal would result in a significant amount of duplicate reporting.
Response: The DSR DT thanks you for your comment. The DSR SDT believes it is clear that the reporting entity is the entity that experiences an event or initiates the event (per Threshold for Reporting in Attachment 1). The DSR SDT will ensure that the supporting guideline clearly states this. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view to what has happened.		
SPP Standards Review Group	No	Threshold for Reporting ? Some of the thresholds used to trigger event reporting seem arbitrary. For example, why were three BES Transmission Elements selected for the transmission loss trigger? What?s significant with three? There may be situations where one element can impact reliability more than other situations where three or more lines may be lost. The defining line should be impact to reliability, not a simple count of elements. Also, timing of the loss of these elements is important. If the three elements are lost over a 3-day span, does this trigger an event report? We would think not and would like to see that clarification in the

Organization	Yes or No	Question 11 Comment
		standard.Public appeals ? Some entities may utilize load reduction (Demand Response, interruptible loads, etc) in the normal course of daily operation in lieu of committing additional generation resources. Because this is not an Energy Emergency as defined in the NERC Glossary, would such an event trigger the filing of an Impact Event report under EOP-004-2? We would like clarification on this issue.Multiple entity reporting responsibility ? Several of the triggering events in Attachment 1 list multiple entity reporting responsibility. The SDT needs to clarify precisely who has the actual reporting responsibility for those events. For example, if a DP loses ? 300 MW (or ? 200 MW depending on size) of load who files the report? Is it the DP, TOP, BA or RC? Attachment 1 would lead us to believe all four are required to file reports. This redundancy is unnecessary and creates unneeded paperwork. Surely this redundancy is not the intent of the SDT.Reporting timeframe ? The timeframes for reporting these after-the-fact reports need to be thoroughly reviewed and, we believe, realigned. Which is more important to the reliability of the BES, operating and controlling the BES following an Impact Event or filing a report describing that event? Most operating desks are staffed by a single operator at nights and on weekends. Their focus should be on operating the system, not filing a report with NERC or DOE within one hour.There appears to be inconsistency in the reporting times among the triggering events. There doesn?t appear to be any logic regarding how the times were selected. Shouldn?t impact to the reliability of the BES be that basis? Why is a BA with 50 MW of load who makes a public appeal to customers for load reduction required to report within 1 hour while an IROL violation doesn?t need to be reported for 24 hours? Clearly the IROL violation has a greater impact on the reliability of the BES. Therefore, shouldn?t these types of reports be filed sooner than those events with less impact on BES reliability?Risk to BES equipment ? The Threshold for Reporting this event indicates that only those events associated with a non-environmental physical threat should be reported. The train derailment example in the footnote then conversely describes just such an environmental threat with flammable or toxic cargo. Which should it be? Additionally, how does one determine the applicability of a potential threat? Is this time dependent, is it threat dependent, how do we factor all this in?
Response: The DSR DT thanks you for your comment. The DSR SDT believes it is clear that the reporting entity is the entity that experiences an event or initiates the event (per Threshold for Reporting in Attachment 1). The DSR SDT will ensure that the supporting guideline clearly states this. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view to what has happened. The entire Attachment 1 has been updated to reflect the comments that were received.		
FirstEnergy	No	Nuclear facilities should be explicitly excluded from the events which have CIP standards as the threshold for reporting since they are exempt from the CIP standards.
Response: The DSR DT thanks you for your comment. The DSR SDT understands that nuclear facilities are exempt from CIP Standards but the Loss of Off Site Power to a nuclear generating plant is a Transmission Owner's and Transmission Operator's responsibility and needs to be reported to the ERO and their		

Organization	Yes or No	Question 11 Comment
Regional Entity for the follow up as described by the Event Analysis Program.		
SERC OC Standards Review Group	No	While we agree with the changes made, we do not believe the goal of eliminating duplicate reporting has been accomplished. In addition, the threshold for transmission loss does not adequately translate to previous ?loss of major system components? which had a threshold of ?significantly affects the integrity of interconnected system operations?.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received.		
PJM Interconnection LLC	No	There is still a significant amount of duplicate reporting involved in Attachment 1, which needs to be cleared. See comments to Question 4.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received.		
We Energies	No	It appears that the footnotes only apply one place in the table. Place the footnote in the table where it applies.Voltage Deviations on BES Facilities: 10% compared to what? Rated?Forced Intrusion: ?At a BES facility? facility or Facility?
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. The Footnotes have been reviewed and updated per comments received.		
LG&E and KU Energy LLC	No	In Attachment 1, the existing EOP-004-1 Attachment 1, point 6 includes an ?Or? for the entities (RC, TOP, GOP) for a, b and c. The way the SDT has pulled this apart, they have included the GOP as having an impact on the Voltage Deviations on BES Facilities. The TOP monitors the transmission system and directs GOPs when they need to change in order to protect the system reliability. This is not something the GOP is responsible for monitoring. The GOP is required to be at the TOP assigned voltage schedule and that actually falls under VAR-002 already. Please remove the GOP from the line of ?Voltage Deviations on BES Equipment.? The way EOP-004-1 Attachment 1 point 6 is currently written, the GOP is an ?or? and does fall into parts b or c, where part 6b is similar to the proposed line ?Damage or destruction of BES equipment? identified in the proposed EOP-004-2 Attachment 1. However, currently the GO/GOP reports ?Loss of Major System Components? on EOP-004-1 within 24 hours of determining damage to the equipment. The proposed ?One hour? is too tight of a window as the GO/GOP often do not know the extent of damage that

Organization	Yes or No	Question 11 Comment
		soon. Typically the OEM is called upon to come and do a thorough inspection and assess the extent of damage, of if there even is any damage; once the ?loss of major system components? is determined, then the 24 hour clock begins today.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received.		
Compliance & Responsiblity Organization	No	See comments set forth in number 2
Exelon	No	Attachment 1, Part A ? Energy Emergency requiring Public appeal for load reduction ? In the current draft Standard, the applicability has been revised from an RC and BA to "initiating entity." As a GO/GOP, I cannot see any event where a GO/GOP would be the responsible "initiating entity" or have the ability to determine an "Energy Emergency." Suggest revising back to specific entities that would be likely responsible for this action (e.g., RC, BA, TOP). Attachment 1, Part A ? Energy Emergency requiring system-wide voltage reduction ? In the current draft Standard, the applicability has been revised from an RC, TO, TOP, and DP to "initiating entity." As a GO/GOP, I cannot see any event where a GO/GOP would be the responsible "initiating entity" or have the ability to determine an "Energy Emergency" related to system-wide voltage reduction. Suggest revising back to specific entities that would be likely responsible for this action.Attachment 1, Part A ? Voltage Deviations on BES facilities - A GOP may not be able to make the determination of a +/- 10% voltage deviation for ? 15 continuous minutes, this should be a TOP RC function only. Attachment 1, Part A ? Generation Loss of ? 2, 000 MW for a GOP does not provide a time threshold. If the 2, 000 MW is from a combination of units in a single location, what is the time threshold for the combined unit loss? Suggest that a time threshold be added for clarity.Attachment 1, Part A ? Loss of off-site power (grid supply) affecting a nuclear generating station ? this event applicability should be removed in its entirety for a Nuclear Plant Generator Operator. The impact of loss of off-site power on a nuclear generation unit is dependent on the specific plant design, if it is a partial loss of off-site power (per the plant specific NPIRs) and may not result in a loss of generation (i.e., unit trip). If a loss of off-site power were to result in a unit trip, an Emergency Notification System (ENS) would be required to the Nuclear Regulatory Commission (NRC). Depending on the unit design, the notification to the NRC may be 1 hour, 8 hours or none at all. Consideration should be given to coordinating such reporting with existing required notifications to the NRC as to not duplicate effort or add unnecessary burden on the part of a Nuclear Plant Generator Operator during a potential transient on the unit. In addition, if the loss of off-site power were to result in a unit trip, if the impact to the BES were ?2,000 MW, then required notifications would be made in accordance with the threshold for reporting for Attachment 1, Part A ? Generation Loss. However, to align with the importance of ensuring nuclear plant safe operation and shutdown as implemented in NERC Standard NUC-001, if a transmission entity experiences an event

Organization	Yes or No	Question 11 Comment
		that causes an unplanned loss of off-site power (source) as defined in the applicable Nuclear Plant Interface Requirements, then the responsible transmission entity should report the event within 24 hours after occurrence. In addition, replace the words "grid supply" to "source" to ensure that notification occurs on an unplanned loss of one or multiple sources to a nuclear power plant. Suggest rewording as follows (including replacing the words "grid supply" to "source" and adding in the word "unplanned" to eliminate unnecessary reporting of planned maintenance activities in the table below):Event Entity with Reporting Responsibility Threshold for Reporting Time to Submit ReportUnplanned loss of off-site power to a Nuclear generating plant (source) as defined in the applicable Nuclear Plant Interface Requirements (NPIRs) Each transmission entity responsible for providing services related to NPIRs (e.g., RC, BA, TO, TOP, TO, GO, GOP) that experiences the event causing an unplanned loss of off-site power (source) Unplanned loss of off-site power (source) to a Nuclear Power Plant as defined in the applicable NPIRs. Within 24 hours after occurrenceAttachment 1, Part A ? Damage or destruction of BES equipment ? The event criteria is still ambiguous and does not provide clear guidance; specifically, the determination of the aggregate impact of damage may not be immediately understood ? it does not seem reasonable to expect that the 1 hour report time clock starts on identification of an occurrence. Suggest that the 1 hour report time clock begins following confirmation of event. ? The initiating event needs to explicitly state that it is a physical and not cyber. ? If the damage or destruction is related to a deliberate act, consideration should also be given to coordinating such reporting with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security event (see additional comments in response to item 17 below). Attachment 1, Part A ? Damage or destruction of Critical Cyber Asset The events that are associated with Critical Cyber Assets should be removed from this Standard. Critical Cyber Asset related events are better addressed in the reporting of Cyber Security Incidents which is already included in Attachment 1, Part B and the CIP standards currently require details about Critical Cyber Assets to be protected with access to that information restricted to only specifically authorized personnel.Attachment 1, Part A ? Damage or destruction of Critical Asset The events that are associated with Critical Assets should be removed from this Standard. Critical Assets are typically whole control centers, substations or generation plants and the damage or destruction of individual pieces of equipment at one of these locations will usually not have much impact to the BES. Any important impacts located at these sites are already addressed in the other existing [Impact] Event types or would be addressed in the Cyber Security Incident event which is already included in Attachment 1, Part B. The CIP standards also currently require that details about Critical Assets and Critical Cyber Assets must be protected with access to that information restricted to only specifically authorized personnel. The identification of Critical Asset is also only an interim step used to identify the Critical Cyber Assets that need to have cyber security protections and the NERC Project 2008-06 CSO706 Standards Drafting Team is currently expecting to eliminate the requirement to identify Critical Assets in the draft revisions they are currently working on. Attachment 1, Part B ? Forced intrusion at a BES facility ? Consideration should also be given to coordinating such reporting with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a

Organization	Yes or No	Question 11 Comment
		potential security event (see additional comments in response to item 17 below).Attachment 1, Part B ? Risk to BES equipment from a non-environmental physical threat ? this event leaves the interpretation of what constitutes a "risk" with the reporting entity. Although the DSR SDT has provided some examples, there needs to be more specific criteria for this event as this threshold still remains ambiguous and will lead to difficulty in determining within 1 hour if a report is necessary. Consideration should also be given to coordinating such reporting with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security event (see additional comments in response to item 17 below).Attachment 1, Part B ? Detection of a reportable Cyber Security IncidentAlthough the DSR SDT agreed that there may be confusion between reporting requirements in this draft and the current CIP-008, "Cyber Security ? Incident Reporting and Response Planning", Part B now requires a 1 hour report after occurrence. The DSR SDT should verify the timing and reporting required for these Cyber Security Incident events is coordinated with the NERC Project 2008-06 CSO706 Standards Drafting Team.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received. The DSR SDT has worked closely with NERC Staff, the Event Analysis Working Group, Project 2008-06 and the U.S. Department of Energy to ensure that EOP-004-2 captures what FERC has directed and will improve the reliability of the BES.		
SDG&E	No	For ?Detection of a reportable Cyber Security Incident,? Attachment 1 identifies the threshold for reporting as: ?that meets the criteria in CIP-008 (or its successor)?; however, CIP-008 has no specified criteria, so this is an unusable threshold. Additionally, SDG&E recommends that the timing of any follow-up and/or final reports required by the standard be listed in the Attachment 1 table.
Response: The DSR DT thanks you for your comment. CIP-008 states that an entity will report a Cyber Security Incident to the ES-ISAC. EOP-004-2, Attachment 2 is the vehicle to report a Cyber Security Incident. It is also required to be sent to their RC which will give them the industry awareness of a single event or is it a multiple event within their area.		
City of Tallahassee (TAL)	No	One hour should be expanded. While I realize the importance of getting information to NERC/ESISAC/whoever, most of the 1-hour requirements are tied to events that may not be resolved within one hour. This will result in stopping restoration efforts or monitoring to submit paperwork. Calling in additional assistance, while certainly a possibility, may not be feasible to accomplish in sufficient time to meet the one-hour deadline. If any of these events were to truly have a detrimental effect on the BES, the effects would have already been felt.Recommend all 1-hour reports be extended to 4-hours. This should also be placed on the list to modify Form OE-417report time lines.

Organization	Yes or No	Question 11 Comment
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received. The DOE Form OE-417 is not governed by NERC but the DSR SDT is proposing to allow an entity to use it to report an event in lieu of Attachment 2.		
Lakeland Electric	No	Event ? Transmission lossThreshold for Reporting ? Revise to ?Loss of three or more BES Transmission elements within a 15 minute period?. This change would capture a sequence of transmission element losses and remove the question if timing that will arise if other transmission elements trip, cascade, due to loss of the first element. There may also be a need for a footnote to clarify that a transmission element that is removed from service by a transmission operator to prevent uncontrolled cascading would be classified as a loss (something for the SDT to consider). Event ? Energy Emergency requiring Public appeal for load reductionThreshold for Reporting ? Add a footnote: Repeated public appeals for the same initiating Impact Event shall be reported as one Public Appeal Event. The initiation and release to the media of the Public appeal(s) should be the reportable event. Question: would an internal request to large industrial customers for voluntary load reductions be reportable under this Event?
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received. Demand responsive load is not covered within this proposed Standard unless it fulfills a Threshold of Reporting within Attachment 1. Footnotes have been update to reflect comments received.		
Arkansas Electric Cooperative Corporation	No	We appreciate the effort the team has taken in improving the requirements since the last posting. Event Forced Intrusion: The timeframe is very small given the possibly minimal risk to the BES. It often takes much longer than 1 hour after verification of intrusion to determine the intrusion was only for copper theft. We suggest a 24 hour time frame or tie the timeframe to the "verification of forced intrusion."
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received.		
Manitoba Hydro	No	Reporting for CCA's should be limited to damage associated with a detected cyber security incident.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. Damage or destruction of Critical Cyber Assets s is per CIP-002 and may not fall into the category of Cyber Security Response as outlined by an entity.		
Sweeny Cogeneration LP	No	In Attachment 1, Part A, Generator Operators who experience a ? 10% sustained voltage deviation for ? 15

Organization	Yes or No	Question 11 Comment
		continuous must issue a report For externally driven events, the GOP will have little if any knowledge of the cause or remedies taken to address it. We believe the language presently in EOP-004-1 is satisfactory that any ?action taken by a Generator Operator? that results in a voltage deviation has to be reported by the GOP.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received.		
American Electric Power	No	The time to submit a report for the inclusion of the damage or destruction of BES equipment, critical asset, or critical cyber asset is too aggressive. The critical cyber asset reporting is redundant with CIP-008. Furthermore, reporting equipment failures within an hour for Critical Assets is going to overwhelm operators that need to focus on the restoration efforts. Self-evident equipment failures at a Critical Asset (such as a tube leak at a generator which is a Critical Asset) should not be required to be reported. Maybe the wording should be stated as an ?abnormal occurrence? rather than ?equipment failure.?It would be helpful if there was a defining or a footnote that defines the nature and/or duration for loss of some equipment. For example, is a transmission loss for sustain or momentary outages?
Response: The DSR DT thanks you for your comment. The Implementation Plan for this project now includes a provision to retire the requirement in CIP-008 for reporting (Requirement 1, Part 1.3). The entire Attachment 1 has been updated to reflect the comments that were received.		
USACE	No	The "Potential Reliability Impact" table should be taken out. Refered to previous comment on our position on potentail impacts.
Response: The DSR DT thanks you for your comment. The DSR SDT believes that potential events are required to be reported to provide industry awareness.		
Consumers Energy	No	1. In reference to the Impact Event addressing ?Loss of Firm load for greater than or equal to 15 minutes?, this is likely to occur for most entities most frequently during storm events, where the loss of load builds slowly over time. In these cases, exceeding the threshold may not be apparent until a considerable time has lapsed, making the submittal time frame impossible to meet. Even more, it may be very difficult to determine if/when 300 MW load (for the larger utilities) has been lost during storm events, as the precise load represented by distribution system outages may not be determinable, since this load is necessarily dynamic. Suggest that the threshold be modified to ?Within 1 hour after detection of exceeding 15-minute threshold?. Additionally, these criteria are specifically storm related wide spread distribution system outages. These events do not pose a risk to the BES.2. Many of the Impact Events listed are likely to occur, if they occur, at widely-distributed system facilities, making reporting ?Within 1 hour after occurrence is identified? possibly impractical, particularly in order to provide any meaningful information. Please give consideration to clearly permitting some degree of investigation by the entity prior to triggering the ?time to submit?3. Referring to the

Organization	Yes or No	Question 11 Comment
		?Transmission Loss? Impact Event, please provide more specificity. Is this intended to address :- anytime that three or more BES Transmission Elements are out of service, - only when three or more BES Transmission Elements are concurrently out-of-service due to unscheduled events, - only when three or more BES Transmission Elements are simultaneously automatically forced out-of-service, or- only when three or more BES Transmission Elements are forced from service in some proximity to each other? It is not unusual, for a large transmission system, that this many elements may be concurrently forced out-of-service at widely-separated locations for independent reasons.4. Referring to the ?Fuel Supply Emergency? Impact Event, OE-417 requires 6-hour reporting, where the Impact Event Table requires 1-hour reporting. The reporting period for EOP-004-2 should be consistent with OE-417.5. For that matter, the SDT should carefully compare the Impact Event Table with OE-417. Where similar Impact Events are listed, consistent terminology should be used, and identical reporting periods specified. Where the Impact Event Table contains additional events, they should be clarified as being distinct from OE-417 to assist entities in implementation. Further, since OE-417 must be reviewed and updated every three years, EOP-004 should defer to the reporting time constraints within OE-417 wherever listed in order to assure that conflicting reporting requirements are not imposed.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed' Loss of Firm Load' as a reporting event, and believe the reporting requirement currently approved in EOP-004-1 should remain in EOP-004-2. The DSR SDT has removed the 'Fuel Supply Emergencies' event after considering comments the DSR SDT received on this event. The DOE Form OE-417 is reviewed biennially by the DOE and can be updated or changed without NERC's involvement. The DSR SDT has taken into consideration the use of Form O- 417 to report events to NERC and agrees that this will fulfill EOP-004-2's reporting requirements. The entire Attachment 1 has been updated to reflect the comments that were received.		
Independent Electricity System Operator	No	As indicated under Q4, we question the need to include IA, TSP and LSE in the responsible entities for reporting.
Response: The DSR DT thanks you for your comment. The DSR SDT has established that CIP-002-4 and CIP-008-3 are applicable to an IA, TSP, and LSE. These entities will report a Cyber Security Incident per Attachment 2 (or OE-417) as the vehicle to inform the ERO, their Regional Entity and their Reliability Coordinator.		
Ameren	No	See response to question 4.
Response: The DSR DT thanks you for your comment. Please see question 4 response.		
ISO New England, Inc	No	As indicated under Q4, we question the need to include IA, TSP and LSE in the responsible entities for reporting. There is still significant duplicate reporting included. For instance, why do both the RC and TOP to report voltage deviations? As written, a voltage deviation on the BES would require both to report. The same

Organization	Yes or No	Question 11 Comment
		would hold true for IROLs. Perhaps IROLs should only be reported by the RC to be consistent with the recently FERC approved Interconnection Reliability Operating Limit standards. Also, the CIP reporting requirements duplicate was is already contained in the CIP Standards, specifically CIP-008. Also, we are required to intentionally destroy Critical Cyber Assets when they are retired, why would we be required to report this?
Response: The DSR DT thanks you for your comment. The DSR SDT has established that CIP-002-3 and CIP-008-3 are applicable to an IA, TSP, and LSE. These entities will report a Cyber Security Incident per Attachment 2 (or OE-417) as the vehicle to inform the ERO, their Regional Entity and their Reliability Coordinator. If a Critical Cyber Asset (CCA) was to be retired, the entity would declassify it as a CCA and therefore it would not be required to be reported. The Implementation Plan for this project now includes a provision to retire the requirement in CIP-008 for reporting (Requirement 1, Part 1.3)		
Calpine Corp	No	1. Additional clarity on the nature of reportable ?Fuel Emergencies? is needed. Does loss of interruptible gas transportation require reporting? 2. Additional clarity on the threshold for ?damage or destruction of BES equipment? is needed. Footnote 1 on page 16 states, in part ?Significantly affects the reliability margin of the system (e.g. has the potential to result the need for emergency actions?. For generating facilities, does this statement refer specifically to the parallel requirement to report any loss of generation >= 2,000 in the Eastern or Western Connection or >= 1,000 in the ERCOT or Quebec Interconnection? If not, exactly what level of damage at a generating plant requires reporting? Use of imprecise terms such as ?significantly? sets the stage for future compliance and enforcement confusion.3. Additional clarity is required for ?Detection of reportable Cyber Security Incident." Is this item intended to apply only to Critical Cyber Assets, or is it an extension of the requirement to all applicable entities irrespective of their Critical Asset status? If it applies only to Critical Cyber Assets, does this reporting requirement create redundant reporting (as reporting is already required under CIP-008-4)? CIP-008-4 requires reporting only of events affecting Critical Cyber Assets. If a more expansive application is intended, what equipment or systems are to be included in the reporting requirement?
Response: The DSR DT thanks you for your comment. The event of Fuel Supply Emergencies has been removed per comments the DSR SDT received. The entire Attachment 1 has been updated to reflect the comments that were received. Footnotes in Attachment 1 have been updated to reflect the comments that the DSR SDT received. Damage to BES equipment's foot note has been enhanced to mean that the BES piece of equipment is required to be removed from service. CIP-008 states that an entity will report a Cyber Security Incident to the ES-ISAC. EOP-004-2, Attachment 2 is the vehicle to report a Cyber Security Incident.		
BGE	No	For the following Events (Damage or destruction of BES equipment, Damage of destruction of Critical Asset, and Damage or destruction of a Critical Cyber Asset), submitting a report within 1 hour after occurrence is identified is too short of a time frame. Generally, the initial time period is spent in recovering from the situation and restoring either electric service or restoring computer services to assure proper operations. To

Organization	Yes or No	Question 11 Comment
		distract from the restoration to normal activities to focus on a report would be detrimental to reliability. Notification of an event may perhaps be made by phone call within 1 hour but completing a report should be required no less than 6 or 12 hours. Determining a cause (especially external or intentional) could take longer than 1 hour to determine and complete a report.It is important to consider the imposition created by a compliance obligation and weigh it against the other demands before the operator at that time. A compliance obligation should avoid becoming a distraction from reliability related work. Under impact event type scenarios, in the first hour of the event, the primary concern should be coping with/resolving the event.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. Footnotes in Attachment 1 have been updated to reflect the comments that the DSR SDT received. Damage to BES equipment's foot note has been enhanced to mean that the BES piece of equipment is required to be removed from service.		
Alliant Energy	No	The item relating to Loss of Firm Load for > 15 minutes should be revised to 500 MW and 300 MW. For many companies, a storm moving across their system could cause more than 300 MW of firm load to be lost, but there is no impact on the BES, so why does the detailed reporting need to be done?The items relating to ?damage or destruction? need to be revised to not be so wide. As currently written, a plan by a company to raze a facility could be considered a violation and must be reported. We believe it needs to tightened to malicious intent or human negligence/error.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed Loss of Firm load and believe the reporting requirement presented approved in EOP-004-1 is substantial and should remain within EOP-004-2. If a Critical Cyber Asset (CCA) was to be retired, the entity would declassify it as a CCA and therefore it would not be required to be reported.		
CenterPoint Energy	No	(1) CenterPoint Energy believes that the ?Entity with Reporting Responsibility? for the first three events in Part A should be clarified. There could still be confusion regarding the ?initiating entity? for events where one entity directs another to take action. From the text on page 5 of the Unofficial Comment Form, it appears that the SDT intended for the ?initiating entity? to be the entity that takes action. To make this clear in Attachment 1, CenterPoint Energy recommends replacing ?initiating entity? with ?Each (insert applicable entities) that (insert action). For example, for ?Energy Emergency requiring a Public appeal? the Entity with Reporting Responsibility should be ?Each?that issues a public appeal for load reduction?. (2) Part A: The threshold for reporting ?System Separation? should not be fixed at greater than or equal to 100 MW for all entities, but rather should be scaled to previous year?s demand as in ?Loss of Firm load for greater than or equal to 15 minutes?, so that for entities with demand greater than or equal to 3000 MW, the island would be greater than or equal to 300MW. (3) Part A: The one hour reporting requirements are unreasonable and burdensome. The Background text indicates that ?proposed changes do not include any real-time operating notifications?? CenterPoint Energy believes all one hour reporting requirements could potentially divert resources away from

Organization	Yes or No	Question 11 Comment
		responding to the event. In many instances the event may still be developing within one hour. Likewise, the 24 hour reporting requirements are also burdensome. CenterPoint Energy recommends changing all reporting requirements to 48 hours. CenterPoint Energy acknowledges that the DOE OE-417 report requires certain one hour and 6 hour reporting. Those requirements should also be extended, and CenterPoint Energy will be making the same recommendation during the DOE OE-417 report revision process when the current form expires on 12/31/11.(4) Part B: CenterPoint Energy is very concerned with the ?events? listed under Attachment 1 ? Potential Reliability Impact ? Part B and believes Part B should be deleted. These arbitrary ?events? with ?potential reliability impact? and reporting times place unnecessary burden on entities to report ?situations? that would rarely impact the reliability of the BES. Entities should be aware of developing situations; however, this standard should not require reporting of such occurrences.(5) Part B: Of particular concern is the overly broad ?Risk to BES equipment? and the example provided in the footnote. CenterPoint Energy believes the SDT has already identified the events with the greatest risk to impact the BES in Part A. Also including ?potential reliability impact? situations in Part B inappropriately dilutes attention away from the truly important events. The industry, NERC and FERC should not lose sight of the forest for the trees.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. Footnotes in Attachment 1 have been updated to reflect the comments that the DSR SDT received. The DOE Form OE-417 is under review by the DOE and can be updated or changed without NERC's involvement. The DSR SDT has taken into consideration the use of OE-417 to report events to NERC and agrees that this will fulfill EOP-004-2's reporting requirements.		
ExxonMobil Research and Engineering	No	The notification requirement and documentation in Attachment 1 do not clearly identify which entities need to be notified for each type of event detailed in Attachment 1. While it makes sense to notify the Reliability Coordinator, NERC, Regional Entity, Law Enforcement and other Governmental Agencies for sabotage type events, it does not seem proper to notify Law Enforcement agencies of a system disturbance that is unrelated to improper human intervention. Furthermore, it is our belief that a time frame of 1 hour is a short window for making a verbal notification to third parties, and an impossibly short window for requiring the submittal of a completed form regardless of the simplicity. When a Petrochemical Facility experiences an impact event, the initial focus should emphasize safe control of the chemical process. For those cases where registered entities are required to submit a form within 1 hour, the Standard Drafting Team should alter the requirement to allow for verbal notification during the first few hours following the initiation of an Impact Event (i.e. allow the facility time to appropriately respond to and gain control of the situation prior to making a notification which may take several hours) and provide separate notifications windows for those parties that will need to respond to an Impact Event immediately and those entities that need to be informed that one occurred for the purposes of investigating the cause of and response to an Impact Event. For example, a GOP should immediately notify a TOP when it experiences a forced outage of generation capacity as soon as possible, but there is no immediate benefit to notify NERC when site personnel are responding to the event in order to gain control of of the situation and determine the extent of the problem. The existing standard?s

Organization	Yes or No	Question 11 Comment
		requirement to file an initial report to entities, such as NERC, within 24 hours seems reasonable provided that proper real time notifications are made and the Standard Drafting Team reinstates EOP-004 Revision 1's Requirement 3.3, which allows for the extension of the 24 hour window during adverse conditions, into the requirement section of EOP-004 [the current revision locates this extension in Attachment 1, which, according to input received from Regional Entities, means that the extension would not be enforceable].
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. Footnotes in Attachment 1 have been updated to reflect the comments that the DSR SDT received.		
PPL Electric Utilities	No	We very much appreciate the work performed by SDT and consideration of all the comments received. While we agree with the majority of the Attachment 1 changes, we suggest the SDT add further clarification to Attachment 1, Part A, Event 'Transmission Loss'. Does this mean permanent loss? Do two lines and a pole constitute a loss of three elements? E.g. Consider the loss of a 230 kV line with two tapped transformers. This does not have a significant effect on the BES, yet would it be reportable? We would prefer Attachment 1, Part A, ?Threshold Reporting? be clarified. E.g. ?Three or more "unrelated" pieces of equipment for a single event?.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. Footnotes in Attachment 1 have been updated to reflect the comments that the DSR SDT received.		
Lincoln Electric System	No	While LES supports the bright line criteria listed in Attachment 1 for reporting Impact Events, we have concerns regarding the reporting threshold for ?Transmission loss?. For Transmission loss of three or more Transmission Elements, LES supports the MRO NSRS? suggested wording of ?Two or more BES Transmission Elements that exceed TPL Category D operating criteria or its successor.?
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received.		
American Transmission Company	No	Energy Emergency requiring Public AppealATC believes that the phrase ?initiating entity? is unclear and could be interpreted in multiple ways. 1) the entity has the authority to call for public appeals, 2) the entity has the authority to declare an Energy Emergency, or 3) the entity determines and identifies the need for the Energy EmergencyTypically the BA?s call for public appeals, so does every BA that calls for the public appeal have to make a filing?The RC declares the need for an Energy Emergency, so are they the initiating entity? A TOP could also identify the need for public appeals and notify the RC about the request. In this case, is the TOP the initiating entity?Given the above examples, ATC believes that the SDT needs to clarify who is required to make the filing. Voltage Deviations on BES FacilitiesATC believes that this should be clarified because one may assume that a loss of a single bus in which voltage goes to zero for more than 15 minutes

Organization	Yes or No	Question 11 Comment
		is reportable. It is ATC understands that what the SDT means is a voltage dip, not an outage to a BES facility. However, given the brief description, ATC is not 100% sure whether there is a clear understanding of the standard?s intent.Energy Emergency resulting in automatic firm load shedding Please provide additional clarify.ATC believes that the SDT should not use the term ?Impact Event? when identifying the entity with reporting responsibility. The term ?Impact Event? is identified in the standard and points to Attachment 1 but now is being used outside of that context and requires entities to interpret what qualifies as an Impact Event.The above observation also applies to those other events that use the term ?Impact Event? to describe Reporting Responsibility.Footnote 1: ATC would like the phrase ?as determined by the equipment owner? added to the footnote. This simple phrase will allow entities to be sure that they are responsible for determining if the damage significantly affects the reliability margin of the system. Without this phrase, entities could be subject to non-compliance actions based on differences of opinions to the extent of the damage on the system. The other option the SDT has is to provide additional clarity on what qualifies as a significant affect.Time to Submit Report:ATC strongly disagrees with the 1 hour time to submit a report because it does not fit with the purpose of this standard. The purpose of this standard is to increase awareness, however, requiring a one-hour reporting window following the event provides little to no benefit. ATC believes that these events should have a 24 hour reporting window which allows for a reasonable amount of time to gather information and report the issue.If the SDT disagrees with this observation, ATC believes a complete explanation should be provided on why knowledge of an event within an hour is significantly better than having the knowledge of the event in a 24 hour time period. ATC strongly believes that NERC will gain as much or more knowledge of the event by giving entities time to understand the event and report.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received.		
Duke Energy	No	? Attachment 1 contains three reportable events (Damage or destruction of Critical Asset, Damage or destruction of a Critical Cyber Asset, and Detection of a reportable Cyber Security Incident) that overlap with CIP-008-3 Cyber Security Incident Reporting and Response Planning and could result in redundant or conflicting content between the two standards. We propose either of the following options:1. Remove the requirement for reporting these events from EOP-004-2 and add the timing and reporting requirements into CIP-008-3, R1.3. ?Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.? OR2. Replace the reporting requirement in CIP-008-3, R1.3. with a reference to report as required in EOP-004-2.? Also, as noted in our comment to Question #4 above, the Attachment 1 Section ?Entity with Reporting Responsibility? should just identify ?Initiating entity? for every Event, as was done with the first three Events. That way you avoid errors in leaving an entity off, or including an entity incorrectly (as was done with the GOP on Voltage Deviations). We note that LSE is listed in the standard as an Applicable entity, and should be included in Attachment 1.

Organization	Yes or No	Question 11 Comment
		Our suggestion would handle this oversight. We also note that CIP-001 does not include Distribution Provider in the list of applicable entities, but EOP-004-2 does include the DP.? We reiterate our comment to Question #1 above that the DSR SDT statement that the proposed changes do not include any real-time operating notifications is inconsistent with requiring notification within one hour for thirteen of the twenty listed Events in Attachment 1.? The last six events refer to the entity that experiences the potential Impact Event. We believe that the word ?potential? should be struck, as this creates an impossibly broad reporting requirement.? Footnote 1 should be revised to strike the phrase ?has the potential to? from the parenthetical, as this creates an impossibly broad reporting requirement.? The Impact Event ?Risk to BES equipment? should be revised to ?Risk to BES equipment that results in the need for emergency actions?. The accompanying footnote 4 should be revised to read as follows: Examples could include a train derailment adjacent to BES equipment (e.g. flammable or toxic cargo that would cause the evacuation of a BES facility control center), or a report of a suspicious device near BES equipment.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. CIP-008 states that an entity will report a Cyber Security Incident to the ES-ISAC. EOP-004-2, Attachment 2 is the vehicle to report a Cyber Security Incident. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The DSR SDT understands that there may be multiple reports (for certain events) that are required by different government agencies. NERC will continue to streamline the reporting process as we move into the future.		
Constellation Power Generation	No	CPG has the following concerns regarding Attachment 1: ?Real-Time - On page 5 of the proposed standard, the team noted that ?the proposed changes do not include any real-time operating notifications.? However, several events in Attachment 1 require that documentation be completed and submitted to the ERO within 1 hour. For generation sites that are unmanned, or only have 1 to 2 operators on site at all times, a 1 hour requirement is not only onerous but is essentially ?real time.??Response within 1 hour - It is important to consider the imposition created by a compliance obligation and weigh it against the other demands before the operator at that time. A compliance obligation should avoid becoming a distraction from reliability related work. Under impact event type scenarios, in the first hour of the event, the primary concern should be coping with/resolving the event. Other notification requirements exists based on required agency response relative to the concern at hand (e.g. public evacuations, fire assistance, etc.) Notification within an hour under EOP-004 does not appear to represent a relevant benefit to resolving the situation and the potential cost would be borne by reliability and recovery efforts. Anything performed within the first hour of the event must be to benefit the public or benefit the restoration of power.?Damage or destruction of BES equipment ? the reporting requirement of 1 hour is extremely onerous. A good example is the failure of a major piece of equipment at a remote combustion turbine generation site. Combustion turbine generation sites are not usually manned with many people. If a failure of a major piece of equipment were to occur, the few people on site need to complete communications to affected entities, communications to their management, as well as

Organization	Yes or No	Question 11 Comment
		emergency switching and ensuring that no other pieces of equipment are effected or harmed. There is little time to complete a form in 1 hour. This should be changed to 48 hours. The form is also inadequate for this type of event. o Using the example above of a failure of a major piece of equipment, CPG is not sure if it?s reportable per Attachment 1, which further proves that Attachment 1 is not clear. Per the footnote regarding damage to BES equipment, the failure would not be reportable, as it does not affect IROL, given the information at the plant it does not significantly affect the reliability margin of the system, and was not damaged or destroyed due to intentional or unintentional human action. However, it would be reportable per the table as the table states ?equipment failure? and ?external cause.? Clarification is needed.?Damage or destruction of Critical Asset ? This item should be removed or significantly refined. For generation assets, a critical asset is essentially the entire plant, so in many cases the information reported at this level would not be useful if the valuable details reside at the equipment level. If it is not removed, then see the notes above on the 1 hour requirement for the completion of the form. ?Fuel supply emergency ? 1 hour for reporting the document is unreasonable. See the earlier notes. ?Risk to BES equipment ? ?From a non-environmental physical threat? This item is too vague and subjective. A catch all category to capture a broad list of potential risks is problematic for entities to manage in their compliance programs and to audit. This should be removed.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received.		
Georgia System Operations Corporation	No	Energy Emergency requiring public appeal for load reduction:-The NERC Glossary defines ?Energy Emergency? as a ?condition when a Load-Serving Entity has exhausted all other options and can no longer provide its customers? expected energy requirements.? Per EOP-002, an Energy Emergency Alert may be initiated by the RC upon RC sole discretion, upon BA request, or upon LSE request.-Question: Is it intended that the LSE reports the event if the LSE requests an alert, the BA reports the event if the BA requests an alert, and the RC reports it if it is a RC sole discretion decision? What if an alert is not initiated? Is it an Energy Emergency? Is it an impact event? Who must initiate the public appeal? Since it must be reported within a certain time after the issuance of the public appeal, is it not an impact event until after the initiation of the public appeal (which should be after the initiation of the alert)? Shouldn?t the reporting of the impact event be done by the initiator of the public appeal? The event should probably be the public appeal and not the Energy Emergency.-?Public? should not be capitalized.-The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained.? Energy Emergency requiring system-wide voltage reduction: See Energy Emergency requiring public appeal for load reduction above regarding requesting Energy Emergency Alerts. If this event is to be reported within a certain time after ?the event?, at what time is the event marked? Or is it within a certain time after the initiation of the voltage reduction and, if so, shouldn?t the reporting of the impact event be done by the initiator of the voltage reduction? The event should probably be the system-wide voltage reduction and not the Energy Emergency. The reliability objective

Organization	Yes or No	Question 11 Comment
		of this standard is not achieved by NERC knowing of this within 1 hour and NERC does not need to know this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained.Energy Emergency requiring manual firm load shedding:-See Energy Emergency requiring public appeal for load reduction above regarding requesting Energy Emergency Alerts. If this event is to be reported within a certain time after ?the event?, at what time is the event marked? Or is it a certain time after the initiation of the shedding of load, if so, shouldn?t the reporting of the impact event be done by the initiator of the shedding of the load? If the RC directs a BA to shed load, then the BA directs a DP to do it, then the DP sheds the load, who is the initiator of the load shedding? The event should probably be the firm load shedding and not the Energy Emergency.-The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained.Energy Emergency resulting in automatic firm load shedding:Whenever load is automatically shed both the DP and the TOP ?experience? the event. So does the BA and the LSE. This event includes ?or? between ?DP? and ?TOP.? Is that intentional? Other events in the table do not include either an ?and? or an ?or.? The entities are separated only by commas. NERC should not require multiple entities to report the same event. See comment for R5 above. If a DP "experiences" an automatic load shedding doesn't the TOP also experience it? Both should not report the same event.-The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained.Voltage deviations on BES Facilities:-Should GOs/GOPs be required instead to report to BAs when this condition exists with the BA then reporting to NERC? The idea of a deviation "on BES Facilities" is not clear. On any one Facility? On all Facilities in an area? How wide of an area?-?Voltage Deviation? is not proper noun/name and is not defined in the NERC Glossary. It should not be capitalized.IROL violation: Multiple entities should not report the same event. Please define ?IROL Violation? or use lowercase. It is assumed that ?IROL Violation? means operation ?outside the IROL for a time greater than IROL TV.?Loss of firm load for ? 15 minutes:-Multiple entities should not report the same event. The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained. ?Firm Demand? is defined but not ?Firm load.?System separation (islanding):-Multiple entities should not report the same event. A DP separating from the transmission system should not be a reportable event for a DP in and of itself. If it leads to a sufficient loss of load, it is reportable as above.-The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained. The words ?separation? and ?islanding? should not be capitalized.Generation loss:-Should GOs/GOPs be required instead to report to BAs when their generation is lost with the BA then reporting to NERC when the total is ? 2,000 MW? A ?loss? of generation should be clarified. Is the discovery of damaged equipment in an offline plant which makes the plant unavailable for an extended period of time a ?loss? of generation?-It should be clarified if this event means the concurrent loss of the generation or losing the generation non-concurrently

Organization	Yes or No	Question 11 Comment
		but they are concurrently unavailable. What is the time window for losing the generation? Lost within seconds of each other? Minutes? Hours?Loss of off-site power to a nuclear generating plant (grid supply):-Multiple entities should not report the same event.-?Off? should be lowercase.Transmission loss:-RCs should not be required to report the loss of transmission elements to NERC. A ?loss? of a BES Transmission Element should be clarified.It should be clarified if this event means the concurrent loss of elements or the non-concurrent loss of the elements but they are concurrently unavailable. What is the time window for losing the elements? When elements are lost, it will be difficult to differentiate if they are BES Transmission Elements or not. Alarms don't immediately identify this. It could lead to gross over-reporting if no distinction is made by a TOP and the TOP reports all losses of 3 elements. It may still be over-reporting (from a reasonableness/practicality basis) even if the differentiation could be easily made and only BES Transmission Elements are reported. Threshold for reporting Transmission Loss: As stated, this will require the reporting of almost all transmission outages. This is particularly true taking into consideration the current work of the drafting team to define the Bulk Electric System. The loss of a single 115kV network line could meet the threshold for reporting as the definition of Element includes both the line itself and the circuit breakers. Instead, we recommend the following threshold "Three or more BES Transmission lines." This threshold has consistency with CIP-002-4 and draft PRC-002-2. This threshold also needs additional clarification as to the timeframe involved. Is the intent the reporting of the loss of 3 or more BES Transmission Elements anytime within a 24 hour period or must they be lost simultaneously? Also, we recommend that the three losses be the result of a related event to require reporting.Damage or destruction of BES equipment that i. affects an IROL; ii. significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); or iii. damaged or destroyed due to intentional or unintentional human action (Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly, e.g., removal of grounding straps rendering protective relaying inoperative.):-What is ?BES equipment?? Would an operator know which equipment is BES equipment and which is not or which BES equipment affects an IROL (if we had one) or which does not? It is a judgment call as to whether the effect was significant or not or if it has the potential or not. Multiple entities should not report the same event. Unplanned control center evacuation:-?Control Center? should be lowercase.-The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained.Fuel supply emergency:Multiple entities should not report the same event. Should GOs/GOPs be required instead to report to BAs when they have a fuel supply emergency with the BA then reporting to NERC if the situation is projected to require emergency action at the BA level?-The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained.Loss of all monitoring or voice communication capability (affecting a BES control center for ? 30 minutes):-Does this event mean that ALL capability at both the primary and backup control centers or just one?Forced intrusion at a BES facility (report if you cannot reasonably determine likely motivation, i.e., intrusion to steal copper or spray graffiti is not reportable unless it affects (affects ? not effects) the reliability

Organization	Yes or No	Question 11 Comment
		of the BES):-What is a ?BES facility?? It is not clear for the purposes of complying with this standard what it means to affect the reliability of the BES. Deferred for ECMS review and additional comments.Risk to BES equipment (examples include a train derailment adjacent to BES equipment that either could have damaged the equipment directly or has the potential to damage the equipment, e.g., flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center, and report of suspicious device near BES equipment.):-In the footnote, delete ?could have? from ??either could have damaged?? Something that could cause evacuation of a control center does not pose a risk to damaging BES equipment. The threshold is ?from a non-environmental physical threat? but the example (toxic cargo) IS an environmental threat.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. The DSR SDT reviewed the term 'Energy Emergency' and has removed it from Attachment 1.		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	No	The one hour reporting timeline is unrealistic for this event. In general it looks like other events requiring the 1 hour reporting timeline are for event that are ?initiated? by the system operator. (ie load shedding, public load reduction, EEP?). Loss of BES equipment is in general 24 hour reporting timeline. It should be, ?as soon as possible but within 24 hours."
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received.		
Indeck Energy Services	No	Comments were included in previous comments.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received.		
BC Hydro		For the change from 24hr to 1hr reporting for events, 1 hour goes extremely quickly in these types of events and it will be difficult to report anything meaningful. As the RC is kept informed during the event why is the report required within 1hr?
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. EOP-004-2 is an after the fact reporting Standard. The entity experiencing an event is required to inform their RC per other NERC Standards.		
Brazos Electric Power Cooperative	No	Question applicability to DP.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the		

Organization	Yes or No	Question 11 Comment
ERO and others with a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received.		
Progress Energy	No	Progress Energy appreciates the effort of the Standard Drafting Team, but we do have some issues with the content of Attachment 1. The loss of three Transmission Elements can occur with a single transmission line outage. Progress is concerned that the possible frequency of this type of reporting could be an extreme burden. Under the column ?Entity with Reporting Responsibility,? why do all related entities have to report the same event? (i.e. do the RC and the TOP in the RC footprint both have to report an event, or is it either/or? The word ?Each? implies separate reports. What is the Reliability-based need for both an RC and the BA/TOP/GO within the footprint to file the same report for the same event?) For vertically integrated companies it should be clear that only one report is required per Impact Event that will cover the reporting requirements for all registered entities within that company.The ?damage or destruction of BES equipment? footnote contains the language ?Significantly affects the reliability margin?.? The word significantly should not be used in a Standard because it is subjective. Reliability margin is also undefined. System Operators must be trained on how to comply with the Standard, and thus objective criteria must be developed for reporting. ?1 hour after occurrence? places a burden on System Operators for reporting when response to and information gathering dealing with the Impact Event may still be occurring. There is a note that states that the timing guidelines may not be met ?under certain conditions?? but then requires a call to both its Regional Entity and notification to NERC. The focus should be on the event response and this type of reporting should occur ?within an hour or as soon as practical.? It is unclear what the voltage deviations of +-10% based on (i.e. is that +-10% of nominal voltage? This may require new alarm set-points to be placed in service in Energy Management Systems in order for entities to able to prove in an audit that they reported all occurrences of voltage exceeding the 10% limit for 15 minutes or more. It has been stated by Regional Entity audit and enforcement personnel that attestations cannot be used to ?prove the positive.?)The word ?potential? should be removed from Attachment 1 and from the definition of Impact Event. An event is either an Impact Event or not. If an entity has to evacuate its control center facility temporarily for a small fire, or any other such minor occurrence, then it activates its EOP-008 compliant backup control center, and there is no impact to reliability, then why does there need to be a report generated?The ?Forced Intrusion? category is problematic. The footnote 3 states: ?Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects (sic) the reliability of the BES).? ?Reasonably determine likely motivation? makes this subjective. If someone breaks into a BES substation fence to steal copper, is interrupted and leaves, then entity personnel determine someone tried to break into the substation, but cannot determine why, then this table requires a report to be filed within an hour. It is unclear what the purpose of such a report would be. Progress agrees that multiple reports in a short time across multiple entities may indicate a larger issue.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. Footnotes		

Organization	Yes or No	Question 11 Comment
have been updated per comments received.		
Liberty Electric Power LLC	Yes	A qualified yes here - please clarify footnote 1 to the table. Are the listed qualifications "and" or "or" statements -IOW, if destruction of BES equipment through human error does not have the potential to result in the need for emergency actions, is it still reportable? If a 18-240 KV step-up transformer suffers minor damage because a conservator tank was valved out, is this reportable under this definition?
Response: The DSR DT thanks you for your comment. Footnotes have been update to reflect comments received. This proposed Standard is targeted at BES level Thresholds for Reporting as outlined in Attachment 1.		
Ingleside Cogeneration LP	Yes	We believe that there should be close, if not perfect, synchronization between the ERO?s Event Analysis Process and Attachment 1 since they share the same ultimate goal as EOP-004-2 to improve industry awareness and BES reliability.
Response: The DSR DT thanks you for your comment. EOP-004-2 is an after the fact reporting Standard and the reports submitted by entities complying with the standard may be used by the NERC Event Analysis Program to review reported events. The Event Analysis Program may change their categories of events at anytime, but revisions to an approved standard must follow the standards development process embodied in the NERC Standard Processes Manual. Despite the differences in process, the DSR SDT is working closely with the Event Analysis Working Group to ensure alignment between the standard and the program to the maximum extent possible.		
Occidental Power Marketing	Yes	There does not appear to be any reportable events for LSEs that do not own, operate, or control BES assets (or assets that directly support the BES) in Attachment 1. This would support removing such entities from the Applicability.
Response: The DSR DT thanks you for your comment. The DSR SDT understands that every LSE may not own or operate BES assets. If of the LSE does not own or operate BES assets, then EOP-004-2 would not be applicable to that LSE. Since CIP-002 and CIP-008 are applicable to LSEs they will be required to be applicable under EOP-004-2 for cyber incidents.		
Farmington Electric Utility System	Yes	
Platte River Power Authority	Yes	
New Harquahala Generating Co.	Yes	
Western Electricity Coordinating	Yes	

Organization	Yes or No	Question 11 Comment
Council		
Midwest ISO Standards Collaborators	Yes	
Southern Company	Yes	
SRP	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
American Municipal Power	Yes	

12. Do you agree with the proposed measures for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: The majority of commenters agree with the proposed measures. Since two requirements were removed, the DSR SDT did a complete review of the Requirements and associated Measure and assured that Measurements did not add to any Requirement. The Measures have been rewritten to reflect strict accuracy to each Requirement and provide a minimum measure required for an entity to be compliant.

Organization	Yes or No	Question 12 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation	No	Several of the measures appear to introduce items that are not required by the standard. For instance, R3 requires that a test of the communications process be performed, however Measure 3 indicates that a mock impact event be performed. Measure 4 indicates that personnel be listed in the plan and be trained on the plan, however there is no requirement to include people in the plan or to train them.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
Northeast Power Coordinating Council	No	Concerns with M5:a. As suggested in the response to Question 10 above, R5 should be combined with R2; b. If R5 to remain as is, then M5 goes beyond the requirement in R5 in that it asks for evidence to support the type of Impact Event experienced. Attachment 2 already requires the reporting entity to provide all the details pertaining to the Impact Event. It is not clear what kind of additional evidence is needed to ?support the type of Impact Event experienced?. Also, the date and time of the Impact Event is provided in the reporting form. Why the need to provide additional evidence on the date and time of the Impact Event?
Response: The DSR SDT thanks you for your comment. Requirement 2 has been deleted as requested by the industry. Requirement R5 (now R2) was revised along with the measure: R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment]. M2. Responsible Entities shall provide a record of the type of event experienced; a dated copy of the Attachment 2 form or OE-417 report; and dated and time-		

Organization	Yes or No	Question 12 Comment
stamped transmittal records to show that the event was reported.		
Pacific Northwest Small Public Power Utility Comment Group	No	It is unclear when reporting to the Compliance Enforcement Authority is required. Does the registered entity report initially, and then anytime a change to the plan is made, or a drill is performed. Or is the information only provided following a request of the Compliance Enforcement Authority, and if so what is the acceptable time limit to respond?
Response: The DSR SDT thanks you for your comment. The Measure is designed to inform applicable entities of the minimum acceptable evidence needed to prove compliance with a requirement. The reference to Compliance Enforcement Authority has been removed since it does not assist an entity in the minimum level of evidence needed per the requirement.		
Dominion	No	1) M1 is open ended. Suggest adding ?on request? to the end of the sentence as written; 2) M4 requires evidence of ?when internal personnel were trained; however, Requirement R4 does not require training.
Response: The DSR SDT thanks you for your comment. The Measure is designed to inform applicable entities of the minimum acceptable evidence needed to prove compliance with a requirement. The reference to Compliance Enforcement Authority has been removed since it does not assist an entity in the minimum level of evidence needed per the requirement.		
SPP Standards Review Group	No	The measures are written as if they are adding requirements to the standards. Using wording such as ?shall provide? gives this implication. We would suggest wording such as ?examples of acceptable evidence to demonstrate compliance may be??See Question 6 for comments regarding M1.See Question 8 for comments regarding M3.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
Midwest ISO Standards Collaborators	No	We disagree with Measurement 4. It implies that the review must be conducted in person. Why could other means such as a web training or a reminder memo not satisfy the requirement? Because Requirement 1 does not require submittal of the Operating Plan, Operating Process and/or the Operating Procedure, Measurement 1 should only require submittal to the Compliance Enforcement Authority upon its request.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement. Requirement 4 has been deleted.		
FirstEnergy	No	Measure M4 includes the phrase ?when internal personnel were trained on the responsibilities in the plan? implies the Requirement R4 requires training. R4 is only requiring the review of a document of the necessary

Organization	Yes or No	Question 12 Comment
		personnel and that the rest of the measure covers the needed evidence for R4. This phrase in the measure should be removed. We suggest the following for M4:M4. Responsible Entities shall provide the materials presented to verify content and the association between the people listed in the plan and those who participated in the review, documentation showing who was present.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement. Requirement 4 has been deleted.		
SERC OC Standards Review Group	No	The measures should be revised to match the general nature of the comments we have made on each requirement.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
PJM Interconnection LLC	No	1. We disagree with M4 as it seems to indicate that all training needs to be in person and precludes any form of Computer Based Training (CBT). 2. As indicated in 10, R5 is redundant as R2 already required an entity to report any Impact Events by executing/implementing its Impact Event Operating plan. If R5 is to remain as is, then M5 goes beyond the requirement by requiring the entity to produce evidence of compliance for the type of Impact Event experienced. It is not clear as to what additional evidence is needed to ?support the type of Impact Event experienced?.
The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
We Energies	No	M1 contains a redundancy: It currently reads, ?Each Responsible Entity shall provide the current in force Impact Event Operating Plan to the Compliance Enforcement Authority.? (?In force? is the same as ?current?.)M2: Change ?Impact Event? to ?Impact Event listed in Attachment 1?.M3: This is an additional requirement. R3 does not require a mock Impact Event. R3 requires a test of the communicating Operating Process. As stated above, R3 and M3 should be deleted.M4: This is written assuming classroom training. R4 does not require formal training much less classroom training. R4 requires that those (internal) personnel who have responsibilities in the plan review the Impact Event Operating Plan.M5: When we report, how do we show to an auditor that we reported ?using the plan?? Delete the reference to ?the plan?.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		

Organization	Yes or No	Question 12 Comment
Compliance & Responsiblity Organization	No	See comments set forth in number 2.
Exelon	No	? M1 - Suggest rewording to state "Each Responsible Entity shall provide the current revision of the Impact Event Operating Plan or equivalent implementing process"? M3 ? Need to provide more guidance on evidence of compliance to meet R.3 The DSR SDT needs to provide more guidance on the objectives and format of the drill expected (e.g., table top, simulator, mock drill) and what evidence will be required to illustrate compliance.? M5 - Suggest that the DSR SDT provide a note or provision to allow for the DOE OE-417 reporting form be submitted by the most knowledgeable functional entity (e.g., the TOP or RC) experiencing the event.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
City of Tallahassee (TAL)	No	M3 & M4 should be modified if comments above (#8 and #9) are incorporated.M4 - Providing the ?materials presented? is beyond the scope of compliance. This constitutes a review of the training program which is beyond the scope of the standard. Review of attendance sheets should be sufficient. The personnel will be listed in the Plan/Process/Procedure. Modify M4: Responsible Entities shall provide evidence of those who participated in the review, showing who was present and when internal personnel were trained on their responsibilities in the plan.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
Tenaska	No	The proposed R1 through R4 should be deleted and a revised version of R5 should become R1. The proposed measures for the new R1 should be revised accordingly.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
American Municipal Power	No	M1-M4 should be eliminated and M5 should be revised to incorporate a simplified R5. M5 - Date and time of submitted report
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		

Organization	Yes or No	Question 12 Comment
Liberty Electric Power LLC	No	Due to disagreement with R3 and R4.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
Arkansas Electric Cooperative Corporation	No	We applaud the drafting team's effort in crafting more meaningful measures. However, we have concerns with the measures reading like requirements in stating Responsible Entities "shall" do something. We suggest crafting the measures to provide acceptable, but not all exclusive, forms of evidence by stating something similar to "Acceptable forms of evidence may include??
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
New Harquahala Generating Co.	No	See R3 comments
Response: The DSR SDT thanks you for your comment. Please see R3 responses.		
Consumers Energy	No	We understand that DOE is migrating to an on-line reporting facility rather than the email-submitted OE-417. If they do so, Form OE-417will not be available for providing to NERC, and the reporting specified by EOP-004 will be duplicative of that for DOE. We recommend that NERC, RFC and the DOE work cooperatively to enable a single reporting system in which on-line reports are made available to all appropriate parties.
Response: The DSR SDT thanks you for your comment. The DSR SDT has been working with the U.S. Department of Energy (DOE) to streamline the reporting process. The DOE Form OE-417 will be accepted at NERC if you are reporting an event to the DOE.		
Independent Electricity System Operator	No	We do not have any issues with Measures M1, M2 and M4, but have a concern with M3 and a couple of concerns with M5:M3: This Measure contains a requirement for the Responsible Entities to conduct a mock Impact Event. We disagree to have this included in the Measure. R3 requires the Responsible Entity to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The Measure should adhere to this condition only. We suggest to change the wording to:The Responsible Entity shall provide evidence that it conducted a test of it its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The time period between actual and or mock Impact Events shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, documentation or a report on an actual Impact Event.M5: a. As

Organization	Yes or No	Question 12 Comment
		suggested above, R5 should be combined with R2;b. If R5 to remain as is, then M5 goes beyond the requirement in R5 in that it asks for evidence to support the type of Impact Event experienced. Attachment 2 already requires the reporting entity to provide all the details pertaining to the Impact Event. It is not clear what kind of additional evidence is needed to ?support the type of Impact Event experienced?. Also, the date and time of the Impact Event is provided in the reporting from. Why do we need to provide additional evidence on the date and time of the Impact Event?
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement. Requirement R5 (now R2) was revised along with the measure: R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment]. M2. Responsible Entities shall provide a record of the type of event experienced; a dated copy of the Attachment 2 form or OE-417 report; and dated and time-stamped transmittal records to show that the event was reported.		
ISO New England, Inc	No	We do not have any issues with Measures M1, M2 and M4, but have a comment on M3 and a couple of concerns with M5:M3: This Measure contains a requirement for the Responsible Entities to conduct a mock Impact Event. We disagree to have this included in the Measure. R3 requires the Responsible Entity to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The Measure should adhere to this condition only. We suggest to change the wording to:The Responsible Entity shall provide evidence that it conducted a test of it its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The time period between actual and or mock Impact Events shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, documentation or a report on an actual Impact Event.M5:a. As suggested above, R5 should be combined with R2;b. If R5 to remain as is, then M5 goes beyond the requirement in R5 in that it asks for evidence to support the type of Impact Event experienced. Attachment 2 already requires the reporting entity to provide all the details pertaining to the Impact Event. It is not clear what kind of additional evidence is needed to ?support the type of Impact Event experienced?. Also, the date and time of the Impact Event is provided in the reporting from. Why do we need to provide additional evidence on the date and time of the Impact Event?c. We disagree with Measurement 4. It implies that the review must be conducted in person. Why couldn?t other means such as web training or a reminder memo not satisfy the requirement?
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement. Requirement R5 (now R2) was revised along with the measure:		

Organization	Yes or No	Question 12 Comment
R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment]. M2. Responsible Entities shall provide a record of the type of event experienced; a dated copy of the Attachment 2 form or OE-417 report; and dated and time-stamped transmittal records to show that the event was reported.		
Calpine Corp	No	Requirements R1, R2, R3, and R4 are unnecessary, as discussed above. The measure for Requirement R5 should focus on the need to report accurately and promptly, not on a Responsible Entity?s ?Operating Plan?. If the Requirements are retained, the measures should state in much greater detail what actions and documentation are required for compliance.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement. Requirement R5 (now R2) was revised along with the measure: R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment]. M2. Responsible Entities shall provide a record of the type of event experienced; a dated copy of the Attachment 2 form or OE-417 report; and dated and time-stamped transmittal records to show that the event was reported.		
CenterPoint Energy	No	M1: CenterPoint Energy recommends that the phrase ?current in force? be updated to ?current? or ?currently effective?. Additionally, CenterPoint Energy suggests clarifying M1 by adding ?within 30 days upon request?, which would be consistent with language found in measures in other standards. The revised measure would read, ?Each Responsible Entity shall provide the currently effective Impact Event Operating Plan to the Compliance Enforcement Authority within 30 days upon request.? M2: If R2 is deleted (as recommended in response to Question 7), then M2 should be deleted.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement. R2 was deleted along with the measure M2.		
ExxonMobil Research and Engineering	No	Measure M3 introduces a psuedo-requirement by implying you are able to reset the testing clock if you implement our Impact Event Operating Plan in response to an Impact Event. This should be covered in Requirement R3. Measure M4 should refer to positions and evidence that people occupying those positions participated in the annual review of the Impact Event Operating Plan. Given the number of individuals involved in operations and the cycle of promotions and reassignments, it?s unreasonable to expect an entity

Organization	Yes or No	Question 12 Comment
		to identify specific individuals in their Impact Event Operating Plan. As the one hour time window is not long enough for entities to report all types of events when responding to the impact the Imact Event had on its facility, Measure M5 should be modified to include voice recordings and log book entries to capture verbal information reported to required parties.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
Constellation Power Generation	No	See CPG?s earlier comments regarding the Requirements and Measures.
Response: The DSR SDT thanks you for your comment. See response to comments on Requirements and Measures.		
Georgia System Operations Corporation	No	There are a lot of inconsistencies between the requirements and the measures. The measures add requirements that are not stated in the requirements. The measures need to be made consistent with the requirements and to not add to them. Also see comments on requirements earlier for language to move from the measures into the requirements.M2: Remove "on its Facilities." The word "its" leads to a lot of confusion regarding who reports what. Attachment 1 should make clear "what" needs to be reported. The entities' operating plan should make it clear as to who should report each "what." Furthermore, not all Impact Events are "on Facilities."M3: Replace "that it conducted a mock Impact Event" with "that it conducted a test of its Operating Process." Delete "The time period between actual and or mock Impact Events shall be nor more than 15 months."M4: The measure says that documentation showing when personnel were trained is required. R4 does not require training. The requirement and the measure should be made clear and consistent.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	No	M3 -The testing of the Plan by drill or mock impact event is unnecessary and burdensome.
Response: The DSR SDT thanks you for your comment. The Measure M3 has been revised as follows: M3. The Responsible Entity shall provide evidence that it conducted a test of the communication process in its Operating Plan events created pursuant to Requirement R1, Part 1.3. Implementation of the communication process as documented in its Operating Plan for an actual event may be used as evidence to meet this requirement. The time period between an actual event or test shall be no more than 15 months. Evidence may include, but is not limited to, operator logs,		

Organization	Yes or No	Question 12 Comment
voice recordings, or dated documentation of a test. (R3) The intent of R3 is to ensure that the communications process of the Operating Plan works when needed. The annual test is not burdensome and an actual event will take the place of the test.		
Farmington Electric Utility System	No	See comments in requirements for R3 and R4
Response: The DSR SDT thanks you for your comment. See response to comments on R3 and R4.		
Indeck Energy Services	No	M1 is OK. M2 should be about implementation, not about any particular events--M5 is about events. Implementation would include distribution and training. M3 should be modified to reflect a training review by entities that cannot cause a Reportable Disturbance or reportable DOE OE-417 event and for the others documentation of an actual event (which is not included in the present M3) or a drill or mock event. M4 is OK. M5 should only include the reports submitted and the date of submission. Further evidence of the event is redundant.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
Brazos Electric Power Cooperative	No	M2 and M5 appear to duplicate each other.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement. R2/M2 have been deleted and R5/M5 is now R2/M2.		
Progress Energy	No	M3 states that ?In the absence of an actual Impact Event, the Responsible Entity shall provide evidence that it conducted a mock Impact Event?? Does this mean that, if an entity experiences an Impact Event that is reportable, then the entity does not have to perform its annual test? If so, this should be made clear in the Requirement.
Response: The DSR SDT thanks you for your comment. That is the intent of the requirement. The Rationale box has been revised to express this intent. The measure now reads: The Responsible Entity shall provide evidence that it conducted a test of the communication process in its Operating Plan for events created pursuant to Requirement R1, Part 1.3. Implementation of the communication process as documented in its Operating Plan for an actual event may be used as evidence to meet this requirement. The time period between an actual event or test shall be no more than 15 months. Evidence may include, but is		

Organization	Yes or No	Question 12 Comment
not limited to, operator logs, voice recordings, or dated documentation of a test. (R3)		
Occidental Power Marketing	Yes	In general, the measures are okay. However, as mentioned above for R3, there needs to be more specificity as to what is acceptable as a "mock Impact Event" for auditing purposes--especially for small entities such as LSEs that do not own, operate, or control BES assets.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
SDG&E	Yes	
Lakeland Electric	Yes	
New Harquahala Generating Co.	Yes	
Bonneville Power Administration	Yes	
Midwest Reliability Organization	Yes	
PSEG Companies	Yes	
Pepco Holdings Inc and Affiliates	Yes	
Southern Company	Yes	
SRP	Yes	
APX Power Markets	Yes	
Manitoba Hydro	Yes	
Sweeny Cogeneration LP	Yes	
American Electric Power	Yes	

Organization	Yes or No	Question 12 Comment
USACE	Yes	
Ameren	Yes	
BGE		No position or comments.
Platte River Power Authority	Yes	
Alliant Energy	Yes	
PPL Electric Utilities	Yes	
Lincoln Electric System	Yes	
American Transmission Company	Yes	
Ingleside Cogeneration LP	Yes	
Duke Energy	Yes	

13. Do you agree with the proposed Violation Risk Factors for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: Many stakeholders suggested that the reporting of events after the fact only justified a VRF of Lower for each requirement. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.

Organization	Yes or No	Question 13 Comment
Northeast Power Coordinating Council	No	If R5 is to remain as is, then the VRF should be a Lower, not a Medium. R5 stipulates the form to be used. It is a vehicle to convey the needed information, and as such it is an administrative requirement. Failure to use the form provided in Attachment 2 or the DOE form does not lead to unreliability.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		

Organization	Yes or No	Question 13 Comment
Bonneville Power Administration	No	R2, R3 and R4 should be lower VRFs than R5 and R1.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
PSEG Companies	No	If Requirements 1-5 remain intact the Violation Risk Factor should be reduced to a Lower not a Medium since this is an administrative requirement and does not impact the reliability of the BES.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Dominion	No	All the VRFs are "Medium." Since the requirements deal with after-the-fact reporting and the administration of reporting plans, procedures, and processes; all VRFs should be "Lower."
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with		

Organization	Yes or No	Question 13 Comment
the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Pepco Holdings Inc and Affiliates	No	This standard involves after the fact reporting of events. Other standards deal with the real time notifications. How do the risk factors between the two line up? A VRF of Low would seem appropriate, since a violation would not affect the reliability of the BES.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
SPP Standards Review Group	No	These are reporting requirements and therefore do not deserve the "medium" VRF. We suggest making the VRFs for all requirements for EOP-004-2 "low."
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can		

Organization	Yes or No	Question 13 Comment
communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Midwest ISO Standards Collaborators	No	All violation risk factors should be Lower. All requirements are administrative in nature. While they are necessary because a certain amount of regulatory reporting will always be required, a violation will not in any direct or indirect way lead to reliability problem on the Bulk Electric System
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
FirstEnergy	No	1. We believe that Requirement 5 does not warrant a "Medium" risk factor. Not using a particular form is strictly administrative in nature and the VRF should be "Low." 2. We believe that Requirement 4 does not warrant a "Medium" risk factor. For example, a simple review of the process does not have the same impact on the Bulk Electric System as the implementation of the Operating Plan per R2. Therefore, we believe R4 is at best a "Low" risk to the BES.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these		

Organization	Yes or No	Question 13 Comment
events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
SERC OC Standards Review Group	No	How can an after-the-fact report require a VRF greater than low?
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
PJM Interconnection LLC	No	All VRFs should be lower as Requirements 1-5 are all administrative in nature. A violation of any of these requirements does not directly or indirectly affect the reliability of the BES.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
We Energies	No	All VRFs should be Lower. They are all administrative and will not affect BES Reliability.

Organization	Yes or No	Question 13 Comment
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
LG&E and KU Energy LLC		
Compliance & Responsiblity Organization	No	See comments set forth in number 2.
Response: The DSR SDT thanks you for your comment. See response to comments on Question 2.		
Exelon	No	R.4 should be a low risk factor, this is an administrative requirement with no contribution to reliability.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
City of Tallahassee (TAL)	No	R1 is administrative in nature (must have a document) and should be Lower.

Organization	Yes or No	Question 13 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT concurs and has assigned a "lower" VRF for Requirement R1.		
United Illuminating Co	No	R3 should be Low. It is a test of the communication Plan which is use of telephone and email.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
American Municipal Power	No	No, this is not acceptable. Eliminate R1-R4. Change R5 to Lower.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Liberty Electric Power LLC	No	See Q 12.
Response: The DSR SDT thanks you for your comment. Please see response to Question 12.		

Organization	Yes or No	Question 13 Comment
Manitoba Hydro	No	Reduce the Long Term Planning items to Lower VRF. The planning items will not have the same impact on the reliability of the system as real time operations.
Response: The DSR SDT thanks you for your comment. Each Requirement is in the Operations Assessment or Operations Planning time horizon. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Independent Electricity System Operator	No	If R5 were to remain as is, then the VRF should be a Lower, not a Medium since R5 stipulates the form to be used. It is a vehicle to convey the needed information, and as such it is an administrative requirement. Failure to use the form provided in Attachment 2 or the DOE form does not give rise to unreliability.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
ISO New England, Inc	No	If R5 is to remain as is, then the VRF should be a Lower, not a Medium since R5 stipulates the form to be

Organization	Yes or No	Question 13 Comment
		used. It is a vehicle to convey the needed information, and as such it is an administrative requirement. Failure to use the form provided in Attachment 2 or the DOE form has no impact on reliability. All violation risk factors should be Lower. All requirements are administrative in nature. While they are necessary because a certain amount of regulatory reporting will always be required, a violation will not in any direct or indirect affect reliability.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Calpine Corp	No	Requirements R1, R2, R3, and R4 are unnecessary, as discussed above. If retained, the violation risk factors should be low for those Requirements, as they all simply support the requirement to actually report correctly stated in Requirement R5.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
ExxonMobil Research and	No	VRFs, VSLs, and THs ideally should be based on the impact event type; alternatively a low VRF seems more

Organization	Yes or No	Question 13 Comment
Engineering		appropriate for this requirements of this standard.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Georgia System Operations Corporation	No	Failing to report to NERC any of many of the listed events does not present a reliability risk. The exception to this would be those threat events where the ES-ISAC needs to be notified. The object of the standard is to prevent or reduce the risk of Cascading. Reporting system situations to appropriate operating entities who can take some mitigating action (e.g., a LSE reporting to its BA or a BA reporting to its RC) and reporting threats to law enforcement officials could prevent or reduce the risk of Cascading but reporting to NERC (except for events where the ES-ISAC needs to know) is unlikely to do that. Reporting of most of the listed events to NERC does not meet the objective of this standard and should be removed from this standard. Such events should be reported to NERC through some other (than a Reliability Standard) requirement for reporting to NERC so that NERC can accomplish its mission of analyzing events. Analyzing events may lead to an understanding that could reduce the future risk of Cascading but analyzing events cannot be performed in time to reduce any impending risks.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for		

Organization	Yes or No	Question 13 Comment
EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Indeck Energy Services	No	If there are any, they should all be Low because this is reporting of historical events. There is no direct effect on BES reliability. Some effect could occur if someone reacts to the reports, but many are concerning unpreventable events.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	No	
Progress Energy	No	
BGE	Yes	No comments.
Platte River Power Authority	Yes	
Alliant Energy	Yes	
Midwest Reliability Organization	Yes	
Southern Company	Yes	
SRP	Yes	

Organization	Yes or No	Question 13 Comment
SDG&E	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
Arkansas Electric Cooperative Corporation	Yes	
Sweeny Cogeneration LP	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
American Transmission Company	Yes	
Ingleside Cogeneration LP	Yes	
Duke Energy	Yes	

14. Do you agree with the proposed Violation Severity Levels for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: Most commenters agreed with the VSLs. The DSR SDT has deleted R4 and R2, and R5 has become R2. The VSLs have been aligned with the revised requirements. The 'Severe' rating for excessively long reporting times has been retained as the DSR SDT believes that fairly reflects the definition of 'Severe' i.e., The performance or product measured does not substantively meet the intent of the requirement.

Organization	Yes or No	Question 14 Comment
Northeast Power Coordinating Council	No	No major issues with the proposed VSLs. However, because of the preceding comments, want to see the next revision of the draft.
Response: The DSR SDT thanks you for your comment.		
Bonneville Power Administration	No	For R5 VSL's: suggest moving the 1-2 hours down one level to Moderate and move the >2 hours down to High with a range of 2-8 hours. Leave the "Failed to Submit" in the Severe category.
Response: The DSR SDT thanks you for your comment. The DSR SDT has increased most reporting timeframes to 24 hours. Those that still require 1 hour reporting have been adjusted to better align with the 24 hour VSLs. Namely, taking twice as long to report is a 'Medium' VSL. The 'Severe' rating for excessively long reporting times has been retained as the DSR SDT believes that fairly reflects the definition of 'Severe' i.e., The performance or product measured does not substantively meet the intent of the requirement.		
Western Electricity Coordinating Council		Regarding the proposed VSLs for R3, since communication testing involves multiple parties it would be more appropriate to base severity level on the number of applicable parties which were not tested rather than how long after 15 months it took to do the test. The standard already builds in a 3 month leeway, In reality the way it is written almost guarantees a lower severity level.
Response: The DSR SDT thanks you for your comment. VSLs reflect the degree to which the requirements are met. The DSR SDT envisions that communication testing will include all parties referenced in the entity's operating plan. Failure to test any part of that communication process is a failure of that Part of the requirement.		
Pepco Holdings Inc and Affiliates	No	This standard involves after the fact reporting of events. Other standards deal with the real time notifications. How do the severity level between the two line up? See above VRF comments.

Organization	Yes or No	Question 14 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the VSLs appropriately align with the NERC Guidelines.		
SPP Standards Review Group	No	Requirement 4: We would suggest the following:Low ? The Responsible Entity reviewed its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 15 calendar months but less than 18 calendar months since the last review.Moderate - The Responsible Entity reviewed its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 18 calendar months but less than 21 calendar months since the last review.High - The Responsible Entity reviewed its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 21 calendar months but less than 24 calendar months since the last review.Severe - The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan within 24 calendar months since the last review.Requirement 5: With our suggested deletion of Requirement 5, we further suggest deleting the VSLs associated with Requirement 5.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R4 and R2, and R5 has become R2.		
SERC OC Standards Review Group	No	The VSLs should reflect the comments on the requirements above.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R4 and R2, and R5 has become R2. The VSLs have been aligned with the revised requirements.		
PJM Interconnection LLC	No	VSLs should reflect the comments on the VRFs above.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the VSLs appropriately align with the NERC Guidelines.		
We Energies	No	Change the VRFs as indicated above and the Time Horizons as indicated below.
Response: The DSR SDT thanks you for your comment. Please see responses to those comments.		
Compliance & Responsiblity Organization	No	See comments set forth in number 2.
Response: The DSR SDT thanks you for your comment. Please see responses Question 2.		

Organization	Yes or No	Question 14 Comment
Exelon	No	Suggest rewording the 1 hour reporting for High and Severe to state "communicate or submit" a report within ? depending on the severity of the event, an actual report may not be feasible. Similar to an NRC event report, a provision should be made for verbal notifications in lieu of an actual submitted report. An entity should not be penalized for failing to submit a written report within 1 hour if the communications were completed within the 1 hour time period meeting the intent of the Standard.
Response: The DSR SDT thanks you for your comment. Attachment 1 allows you to provide a verbal report under the conditions you contemplate.		
SDG&E	No	This Reliability Standard provides a list of reporting requirements that are applicable to registered entities, thus it is a paperwork exercise; therefore, SDG&E recommends that none of the requirements should exceed a ?Moderate? Violation Severity Level. Failure on the part of an applicable Registered Entity to provide an event report will have no immediate impact on the Bulk Electric System.
Response: The DSR SDT thanks you for your comment. VSLs describe how fully an entity meets the requirements and are not a measure of severity or impact. These items are captured in the VRFs.		
American Municipal Power		No, this is not acceptable. Eliminate R1-R4 and change R5. Severe: n/aHigh VSL: n/aMedium VSL: No report for a reportable eventLow VSL: Late report for a reportable event
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R4 and R2, and R5 has become R2. The VSLs have been aligned with the revised requirements.		
Liberty Electric Power LLC	No	See Q 12.
Response: The DSR SDT thanks you for your comment. Please see responses to Question 12.		
Consumers Energy	No	1. In reference to the Impact Event addressing ?Loss of Firm load for greater than or equal to 15 minutes?, this is likely to occur for most entities most frequently during storm events, where the loss of load builds slowly over time. In these cases, exceeding the threshold may not be apparent until a considerable time has lapsed, making the submittal time frame impossible to meet. Even more, it may be very difficult to determine if/when 300 MW load (for the larger utilities) has been lost during storm events, as the precise load represented by distribution system outages may not be determinable, since this load is necessarily dynamic. Suggest that the threshold be modified to ?Within 1 hour after detection of exceeding 15-minute threshold?. Additionally, these criteria are specifically storm related wide spread distribution system outages. These events do not pose a risk to the BES.2. Many of the Impact Events listed are likely to occur, if they occur, at widely-distributed system facilities, making reporting ?Within 1 hour after occurrence

Organization	Yes or No	Question 14 Comment
		is identified? possibly impractical, particularly in order to provide any meaningful information. Please give consideration to clearly permitting some degree of investigation by the entity prior to triggering the ?time to submit?.3. Referring to the ?Fuel Supply Emergency? Impact Event, OE-417 requires 6-hour reporting, where the Impact Event Table requires 1-hour reporting. The reporting period for EOP-004-2 should be consistent with OE-417.
Response: The DSR SDT thanks you for your comment. The DSR SDT has increased almost all reporting timeframe to 24 hours. Also, the fuel supply emergency has been removed from Attachment 1. Reporting period was chosen to meet NERC needs, you may have more restrictive periods for OE-417, but that is outside the jurisdiction of the DSR SDT.		
Calpine Corp	No	Requirements R1, R2, R3, and R4 are unnecessary, as discussed above. If retained, the violation risk factors should be low for those requirements, as they all simply support the requirement to actually report correctly stated in Requirement R5.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R4 and R2, and R5 has become R2. The VSLs have been aligned with the revised requirements.		
CenterPoint Energy	No	CenterPoint Energy believes that the Severe VSL for R5 (Reporting) in the current draft incorrectly equates 2X reporting with failure to submit a report. CenterPoint Energy believes the VSLs for R5 should all reflect a factor increase in time. For example, the lower VSL should be 1.5X the reporting time frame. The Moderate VSL should be 2x the reporting time frame. The High VSL should be 3x the reporting time frame. The Severe VSL should be failure to report.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R4 and R2, and R5 has become R2. The VSLs have been aligned with the revised requirements. The 'Severe' rating for excessively long reporting times has been retained as the DSR SDT believes that fairly reflects the definition of 'Severe' i.e., The performance or product measured does not substantively meet the intent of the requirement.		
ExxonMobil Research and Engineering	No	VRFs, VSLs, and THs ideally should be based on the impact event type; alternatively a low VRF seems more appropriate for the requirements of this standard.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the VSLs and time horizons appropriately align with the requirements and NERC Guidelines. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2)		

Organization	Yes or No	Question 14 Comment
and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Indeck Energy Services	No	There should be only Lower VSL's. This is reporting of historical events and there is no direct effect on BES reliability. How does missing 3 parts of R1 compare to tripping a 4,000 MW generating station because vegetation was not properly managed? Just because there are 4 levels, doesn't mean that all Standards need to use them all. If you step back, and think about causes of cascading outages, reporting events 1 hour or 24 hours later has no significance. There is no direct preventative causation either.
Response: The DSR SDT thanks you for your comment. VSLs describe how fully an entity meets the requirements and are not a measure of severity or impact to the BES. These items are captured in the VRFs.		
Progress Energy	No	Progress disagrees with the High and Severe VSLs listed for R5. If an entity experiences an Impact Event and fails to submit a report within an hour as required, it may be that there are multiple mitigating circumstances. It is not reasonable to require reporting within an hour since identifying a reportable event often takes longer than this time period.
Response: The DSR SDT thanks you for your comment. The DSR SDT has increased almost all reporting timeframe to 24 hours. Also, VSLs describe how fully an entity meets the requirements and are not a measure of severity or impact to the BES. These items are captured in the VRFs.		
Georgia System Operations Corporation	No	None.
Independent Electricity System Operator		We do not have any major issues with the proposed VSLs. However, in view of our comments on some of the Questions, above, we reserve our comments upon seeing a revised draft.
Response: The DSR SDT thanks you for your comment.		
ISO New England, Inc		We do not have any major issues with the proposed VSLs. However, in view of our comments on some of the Questions, above, we reserve our comments upon seeing a revised draft.

Organization	Yes or No	Question 14 Comment
Response: The DSR SDT thanks you for your comment.		
Midwest Reliability Organization	Yes	
Midwest ISO Standards Collaborators	Yes	
Southern Company	Yes	
SRP	Yes	
City of Tallahassee (TAL)	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
United Illuminating Co	Yes	
Arkansas Electric Cooperative Corporation	Yes	
Manitoba Hydro	Yes	
Sweeny Cogeneration LP	Yes	
American Electric Power	Yes	
New Harquahala Generating Co.	Yes	
Platte River Power Authority	Yes	

Organization	Yes or No	Question 14 Comment
BGE	Yes	No comments.
Alliant Energy	Yes	
Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
American Transmission Company	Yes	
Ingleside Cogeneration LP	Yes	
Duke Energy	Yes	
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	

15. Do you agree with the proposed Time Horizons for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: Many stakeholders suggested that the Time Horizons for this standard should be Operations Assessment or Operations Planning rather than Long Term Planning. The DSR SDT agrees. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Assessment, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 has been changed to Operations Planning.

Organization	Yes or No	Question 15 Comment
Northeast Power Coordinating Council	No	For the purpose of developing and updating an Impact Event Operating Plan, there should not be any requirements that fall into the Long-term planning horizon. As the name implies, the plan is used in the operating time frame. Consistent with other plans such as system restoration plans which need to be updated and tested annually, most of the Time Horizons in that standard (EOP-005-2) are either Operations Planning or Real-time Operations. Suggest the Time Horizon for R1, R3 and R4 be changed to Operations Planning.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Assessment, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 has been changed to Operations Planning.		
Bonneville Power Administration	No	Depends on the answer to #7. If implementation means a signed and valid Plan, then it should be with Long Term. If reporting the events, then it should be Real-Time/Same Day Operations.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted the separate requirement to 'implement the plan'. The reporting obligation is now R2 with a time horizon of Operations Assessment, which is defined as 'follow-up evaluations and reporting of real time operations'.		

SPP Standards Review Group	No	Based on our previous comments in response to Question 11, we feel that the Time Horizon for R2 should be lengthened. Assigning it a Real-time Operations and Same ?day Operations timeframe has too much of an impact on real-time operations. Pushing it back will allow support personnel to do the after-the-fact reporting and keep this burden off of the operators.
Response: The DSR SDT thanks you for your comment. The reporting obligation is now R2 with a time horizon of Operations Planning, which is defined as 'follow-up evaluations and reporting of real time operations'.		
Midwest ISO Standards Collaborators	No	R2 and R5 should be Operations Assessment since it deals with after the fact reporting. R3 should included Operations Assessment since an actual event could be used as the test.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Planning, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 have been changed to Operations Planning		
SERC OC Standards Review Group	No	R2 and R5 should be in the Operations Assessment time horizon.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Planning, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 have been changed to Operations Planning		
PJM Interconnection LLC	No	R2 and R5 should be in Operations Assessment Time Horizon as they deal with ?after-the-fact? reporting.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Planning, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 have been changed to Operations Planning		
We Energies	No	R2 and R5 should be Operations Assessment.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Planning, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 have been changed to Operations Planning		

Consumers Energy	No	1. In reference to the Impact Event addressing ?Loss of Firm load for greater than or equal to 15 minutes?, this is likely to occur for most entities most frequently during storm events, where the loss of load builds slowly over time. In these cases, exceeding the threshold may not be apparent until a considerable time has lapsed, making the submittal time frame impossible to meet. Even more, it may be very difficult to determine if/when 300 MW load (for the larger utilities) has been lost during storm events, as the precise load represented by distribution system outages may not be determinable, since this load is necessarily dynamic. Suggest that the threshold be modified to ?Within 1 hour after detection of exceeding 15-minute threshold?. Additionally, these criteria are specifically storm related wide spread distribution system outages. These events do not pose a risk to the BES.2. Many of the Impact Events listed are likely to occur, if they occur, at widely-distributed system facilities, making reporting ?Within 1 hour after occurrence is identified? possibly impractical, particularly in order to provide any meaningful information. Please give consideration to clearly permitting some degree of investigation by the entity prior to triggering the ?time to submit?.3. Referring to the ?Fuel Supply Emergency? Impact Event, OE-417 requires 6-hour reporting, where the Impact Event Table requires 1-hour reporting. The reporting period for EOP-004-2 should be consistent with OE-417.
Response: The DSR SDT thanks you for your comment. The DSR SDT has increased almost all reporting timeframe to 24 hours. Also, the fuel supply emergency has been removed from Attachment 1. Reporting period was chosen to meet NERC needs, you may have more restrictive periods for OE-417, but that is outside the jurisdiction of the DSR SDT.		
Independent Electricity System Operator	No	For the purpose of developing and updating an Impact Event Operating Plan, there should not be any requirements that fall into the Long-term planning horizon. As the name implies, the plan is used in the operating time frame. And consistent with other plans such as system restoration plan which needs to be updated and tested annually, most of the Time Horizons in that standard (EOP-005-2) are either Operations Planning or Real-time Operations. We suggest the Time Horizon for R1, R3 and R4 be changed to Operations Planning.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Planning, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 have been changed to Operations Planning		

ISO New England, Inc	No	For the purpose of developing and updating an Impact Event Operating Plan, there should not be any requirements that fall into the Long-term planning horizon. As the name implies, the plan is used in the operating time frame. And consistent with other plans such as system restoration plan which needs to be updated and tested annually, most of the Time Horizons in that standard (EOP-005-2) are either Operations Planning or Real-time Operations. We suggest the Time Horizon for R1, R3 and R4 be changed to Operations Planning. The Time Horizon for R2 and R5 should be changed to Operations Assessment since they both deal with after the fact reporting.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Planning, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 have been changed to Operations Planning		
ExxonMobil Research and Engineering	No	VRFs, VSLs, and THs ideally should be based on the impact event type; alternatively a low VRF seems more appropriate for this requirements of this standard.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001. The DSR SDT believe the VSLs and revised time horizons appropriately align.		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	No	Why shorten the normal process?
Response: The DSR SDT thanks you for your comment. The DSR SDT has revised most of the reporting timelines 24 hours.		

Indeck Energy Services	No	These requirements have no time horizon. There about history and not about the future.
Response: The DSR SDT thanks you for your comment. All NERC standards must have a time horizon associated with each requirement. Time horizons are used as a factor in determining size of a sanction.		
American Municipal Power	No	
USACE	No	
Pepco Holdings Inc and Affiliates	Yes	However, do they line up with the corresponding real time reporting procedures as mentioned above, #13 and #14?
Response: The DSR DT thanks you for your comment. Please see responses to comments #13 and #14. Since the time for reporting impact events is no more than 24 hours, the time horizon has been revised to Operations Planning.		
Midwest Reliability Organization	Yes	
PPL Supply	Yes	
Dominion	Yes	
FirstEnergy	Yes	
Southern Company	Yes	
SRP	Yes	
City of Tallahassee (TAL)	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
United Illuminating Co	Yes	

Liberty Electric Power LLC	Yes	
Arkansas Electric Cooperative Corporation	Yes	
Manitoba Hydro	Yes	
Sweeny Cogeneration LP	Yes	
New Harquahala Generating Co.	Yes	
Platte River Power Authority	Yes	
BGE		No position or comments.
Alliant Energy	Yes	
CenterPoint Energy	Yes	
PPL Electric Utilities	Yes	
Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
American Transmission Company	Yes	
Ingleside Cogeneration LP	Yes	
Duke Energy	Yes	

Georgia System Operations Corporation	Yes	None.

16. Do you agree with the proposed Implementation Plan for EOP-004-2? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: The majority of commenters agreed with the Implementation Plan. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with. Consequently the effective date remains as first calendar day of the third calendar quarter following the regulatory approval/BOT adoption as applicable.

Organization	Yes or No	Question 16 Comment
Pepco Holdings Inc and Affiliates	No	The proposed time line is too short. It is easy to revise procedures. However developing training and integrating the training into the schedule takes time. Shorter time frame takes away adequate time to integrate into the training plan and disrupts operator schedules. Since notifications already exist and after the fact reporting does not impact BES reliability, why the need to expedite? There are many other training activities that must be coordinated with this.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
FirstEnergy	No	We believe the previous proposal for a 12 month implementation was more appropriate and suggest the team revert back to that timeframe.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
Southern Company	No	The implementation time should be 12 months after approval regardless of the elapsed time taken to get the standard approved.

Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
Exelon	No	The DSR SDT reduced the implementation from one year to between six and nine months based on the revised standard requirements. Exelon disagrees with the proposed shortened implementation timeframe. The current revision to EOP-004 still requires an entity to generate, implement and provide any necessary training for the "Impact Event Operating Plan" by a registered entity. Commenters previously supported a one year minimum; but the requirements for implementation have not changed measurably - six to nine months is not adequate to implement as written.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
SDG&E	No	SDG&E recommends a 9 month minimum timeframe for implementation.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
United Illuminating Co	No	The SDT should be specific that on the effective date an Entity will have the Operating documented and approved. The SDT should be specific that the first simulation is required to occur 15 months following the effective date. The SDT should be specific that the first annual review shall occur with in 15 months after the effective date.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
American Electric Power	No	With the scope of applicable functions expanding, more time will be required to develop broader processes and training. This will need to be extended for 18 months to get the process implemented and everyone trained.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
CenterPoint Energy	No	CenterPoint Energy prefers the previously accepted timeline of 1 year.

Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
Georgia System Operations Corporation	No	There is nothing about the revisions that were made to the requirements that shortens the time needed by the industry to get prepared for this revision. The removal of requirements for NERC does not shorten the requirements for the industry. Eighteen months (or 12 months minimum) should be alloted to prepare for this revision.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
Brazos Electric Power Cooperative	No	A one year implementation is needed to develop and implement formal documents to meet requirements.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	No	The implementation Plan was to move up the timeline and we do not see why this needs to be pushed forward on a shortened timeline. It should remain at the one year implementation schedule especially if annual exercises are not removed from the standard requirements as this take some time to prepare.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
ExxonMobil Research and Engineering		Recommend 4th calendar quarter instead of 3rd.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
Consumers Energy	No	
Dominion	Yes	Dominion agrees with the Implementation Plan; however, notes that the title for EOP-004-2 is inconsistent with the actual proposed standard.

Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
Farmington Electric Utility System	Yes	Nine months would be preferred
Response: The DSR SDT thanks you for your comment. The majority of stakeholders agree with the proposed implementation plan and it will remain unchanged.		
Northeast Power Coordinating Council	Yes	
Bonneville Power Administration	Yes	
Midwest Reliability Organization	Yes	
PPL Supply	Yes	
SPP Standards Review Group	Yes	
Midwest ISO Standards Collaborators	Yes	
SERC OC Standards Review Group	Yes	
PJM Interconnection LLC	Yes	
SRP	Yes	
We Energies	Yes	
Compliance & Responsiblity Organization	Yes	
City of Tallahassee (TAL)	Yes	

Lakeland Electric	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
American Municipal Power	Yes	
Liberty Electric Power LLC	Yes	
Arkansas Electric Cooperative Corporation	Yes	
Manitoba Hydro	Yes	
Sweeny Cogeneration LP	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Independent Electricity System Operator	Yes	
ISO New England, Inc	Yes	
Platte River Power Authority	Yes	
BGE	Yes	No comments.
Alliant Energy	Yes	
PPL Electric Utilities	Yes	

Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
American Transmission Company	Yes	
Ingleside Cogeneration LP	Yes	
Duke Energy	Yes	
Indeck Energy Services	Yes	

17. If you have any other comments you have not already provided in response to the questions above, please provide them here.

Summary Consideration: The majority of comments received relate to Attachment 1 and the Flowchart in the background section. The DSR SDT has made conforming revisions to each based on the comments received. The Flowchart waqs updated to remove references to sabotage and replaced with "Criminal act invoking federal jurisdiction". In response to the comments received, the SDT has made numerous enhancements to Attachment 1. These revisions include:

- **Added new column "Submit Attachment 2 or DOE OE-417 Report to:" which references Part 1.3 and provide the time required to submit the report.**
- **Combined Parts A and B into one table and reorganized it so that the events are listed in order of reporting times (either one hour or 24 hours)**
- **Removed references to "Impact Event" and replaced with the specific language for the event type in the "Entity with Reporting Responsibility". For example, replaced "Impact Event" with "automatic load shedding".**

The ERO and the RE were added as applicable entities to reflect CIP-002 applicability to this standard.

Organization	Yes or No	Question 17 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation		In the discussion and related flowchart described as "A Reporting Process Solution - EOP-004," the discussion suggests that Industry should notify the state law enforcement agency and then allow the state agency to coordinate with local law enforcement. It has been our experience that we receive very good response from local law enforcement and they have existing processes to notify state or federal agencies as necessary. It appears the recommendation is to bypass the local law enforcement, but it is not clear that representatives from state or local law enforcement were included in this discussion (see proposal discussed with "FBI, FERC Staff, NERC Standards Project Coordinator and SDT Chair"). It would be helpful to see some additional clarification to understand why the state agency was chosen over local or federal agencies. Finally, we would like to express our gratitude to the DSR SDT for their hard work in making improvements to the NERC standards for event reporting.

Organization	Yes or No	Question 17 Comment
Response: The DSR DT thanks you for your comment. The Flowchart has been updated. The DSR SDT has reviewed all comments and believes it is the responsibility of the Reporting Entity to contact the appropriate law enforcement officials.		
Bonneville Power Administration		Work needed on Part A Damage or Destruction of BES equipment. The Note 1 is OK, but the Threshold doesn't match well. If a PCB is damaged by lightning or an earthquake, Note 1 (human action) doesn't require Reporting (proper interpretation), but the Threshold still requires "equipment damage."
Response: The DSR DT thanks you for your comment. Attachment 1 has been updated concerning Destruction of BES equipment and the associated footnote has been revised.		
Midwest Reliability Organization		On the Impact Reporting Form, number 7,8,9,10, and 11 have an astrict (*) but nothing describes what the astrict means. Recommend a foot note be added to state: * If applicable to the reported Impact Event.
Response: The DSR DT thanks you for your comment. Attachment 1, Part B has been updated to reflect these noted changes.		
Western Electricity Coordinating Council		Actual Reliability Impact Table comments: Note that per the NERC glossary "Energy Emergency" only is defined for an LSE. Energy Emergency is the precursor term in the first three lines. Thus logically an LSE is the only entity which would be initiating the event and responsible for reporting for first three items. We don't believe that is the intent.We suggest you consider just eliminating ?Energy Emergency? and going with:? Public appeal for load reduction? system-wide voltage reduction? manual firm load sheddingFor Loss of Off site power at Nuc Station is reporting really expected of each of the entities listed? (lots of reports) We suggest you consider just the Nuclear GOP and perhaps the associated TOP. Perhaps you could use the CIP approach as in the next two rows and say Applicable GOP and Transmission Entities under NUC-001-2Potential Reliability Impact Table Comments:For Fuel Supply Emergency, Forced Intrusion, Risk to BES Equipment, Cyber Security Incident where owner/operator are both listed (GO/GOP or TO/TOP) could consider perhaps reporting to be assigned to only one rather than both.
Response: The DSR DT thanks you for your comment. The DSR SDT has removed the use of "Energy Emergency" and has updated Loss of offsite power to a nuclear generating plant within Attachment 1. Fuel Supply emergency has been removed from Attachment 1 per comments received. The entire Attachment 1 has been updated per comments received.		
Pacific Northwest Small Public Power Utility Comment Group		All five requirements refer to Attachment 1 Part A either directly, or indirectly by referring to R1 plans. Attachment 1 Part A, though, only provides the thresholds required for reporting (R5). No thresholds are provided for planning (R1) or the requirements referencing the plan (R2-R4). Strictly interpreted, an entity would be required to plan for any amount of firm load loss exceeding 15 minutes (for example), implement the

Organization	Yes or No	Question 17 Comment
		plan for any amount and then report only those events that exceeded the applicable 200 or 300 MW level. An entity that had a peak load of less than 200 MW would still need to meet R1-R4 regarding load loss. We believe the SDT intended to use common thresholds for all the requirements. Suggest relabeling the Attachment 1 Part A column header from ?Threshold for Reporting? to ?Threshold.?We also fail to see how an entity?s size in MWh affects the threshold for reporting firm load loss.
Response: The DSR DT thanks you for your comment. The DSR SDT has revised each Requirement and Attachment 1. There are other events within Attachment 1 that a responsible entity will be required to report.		
Dominion		The following comments are provided on the Reporting Hierarchy for Impact Events EOP-004-2: 1) A reference to sabotage still exists in a ?decision block?; 2) The ?entry block? only specifies ?actual Impact Events? and does not address ?potential?; 3) Hierarchy is misspelled in the title.Attachment 2: Impact Event Reporting Form; in questions 7, 8, 9, 10, 11 what is the purpose of the *(asterisk) behind each Task that is named?
Response: The DSR DT thanks you for your comment. The Flowchart has been updated based on comments received. Attachment 2 has been updated to reflect comments received.		
Pepco Holdings Inc and Affiliates		IRO-000-1, Sec D1.5 and TOP-007, Sec D1.1 there are ?after the fact? reporting requirements for IROL violations. Since IROL violations are included in this standard, should those standards be modified?Should the standard include a specific statement that this standard deals only with after the fact and other standards deal with real time reporting?Since this standard deals with after the fact reporting, consideration should be given to extending the time to report as defined in Attachment 1. One hour does not seem to be reasonable.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed TOP-007 and note that the 72 hour issue is not defined within a Requirement. This issue has been forwarded to the "NERC Issues Data base." Attachment 1 has been updated to reflect this event to 24 hours per comments received.		
SPP Standards Review Group		In Attachment 2 just before the table, the statement is made that ?NERC will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report.? But the last sentence in the Guideline and Technical Basis white paper, it is stated that ? For example, if the NERC Report duplicates information from the DOE form, the DOE report may be included or attached to the NERC report, in lieu of entering that information on the NERC report.? These are in conflict with each other. Which is correct? We prefer the former over the latter.In Attachment 2 in Tasks 7-11 an asterisk appears in those tasks. To what does this asterisk refer?

Organization	Yes or No	Question 17 Comment
Response: The DSR DT thanks you for your comment. The DSR SDT's White Paper was the initial road map for the SDT to follow. The DSR SDT has proposed allowing entities to use the DOE Form OE-417 to report events listed within Attachment 1.		
Midwest ISO Standards Collaborators		We believe the reporting time lines are too aggressive for some events. Reporting events within an hour is not reasonable as an entity may still be dealing with the event. This will be particularly difficult when support personnel are not present such as during nights, holidays, and weekends.
Response: The DSR DT thanks you for your comment. Attachment 1 has been updated per comments received.		
FirstEnergy		FE offers the following additional comments and suggestions: 1. In the Background section of EOP-004-2, on page 6 under Stakeholders in the Reporting Process, we suggest adding ?Regional Entity? and ?Nuclear Regulatory Commission?. 2. The DSR SDT makes reference to comments that Exelon provided that suggested adopting the NRC definition of "sabotage." We feel the comment made by Exelon in their previous submittal was to ensure that the DSR SDT included the Nuclear Regulatory Commission (NRC) as a key Stakeholder in the Reporting Process and FE agrees with this suggestion. Nuclear generator operators already have specific regulatory requirements to notify the NRC for certain notifications to other governmental agencies in accordance with 10 CFR 50.72(b)(s)(xi). We ask that the DSR SDT contact the NRC about this project to ensure that existing communication and reporting that a licensee is required to perform in response to a radiological sabotage event (as defined by the NRC) or any incident that has impacted or has the potential to impact the BES does not create either duplicate reporting, conflicting reporting thresholds or confusion on the part of the nuclear generator operator. We believe this is a similar situation as what was recently resolved between NERC and the NRC concerning the applicability of CIPs 002 ? 009 for nuclear plants. Each nuclear generating site licensee must have an NRC approved Security Plan that outlines applicable notifications to the FBI. Depending on the severity of the security event, the nuclear licensee may initiate the Emergency Plan (E-Plan). We ask that the proposed "Reporting Hierarchy for Impact Event EOP-004-2," flow chart be coordinated with the NRC to ensure it does not conflict with existing expected NRC requirements and protocol associated with site specific Emergency and Security Plans.
Response: The DSR DT thanks you for your comment. 1. We have added these as requested. 2. The NRC was added to the list on page 6 as requested. The events in Attachment 1 that are applicable to nuclear plants are: Generation loss (>1,000 MW WECC, >2,000 MW Elsewhere); Destruction of BES Equipment; Damage or destruction of Critical Asset per CIP-002; Damage or destruction of a Critical Cyber Asset per CIP-002; Forced Intrusion; Risk to BES Equipment; and Detection of a Reportable Cyber Security incident. Two of these events are addressed in the situation that you mention above (CIP-002). The other events should be reported to both the NRC and ERO if they occur. These are considered to be sabotage type events.		

Organization	Yes or No	Question 17 Comment
SERC OC Standards Review Group		In Attachment 1, the reporting timeline should be no less than the end of the next business day for after-the-fact reporting of events. If reporting in a time frame less than this is required for reliability, the groups or organizations receiving the reports should be included in the functional model. The emphasis should be on giving the operators the time to respond to events and not to reporting requirements.?The comments expressed herein represent a consensus of the views of the above named members of the SERC OC Standards Review group only and should not be construed as the position of SERC Reliability Corporation, its board or its officers.?
Response: The DSR DT thanks you for your comment. Attachment 1 has been updated to reflect comments received. Many of the reporting time frames have been revised to 24 hours.		
PJM Interconnection LLC		In the Compliance Enforcement Authority Section on Page 11, the second bullet says ?If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement?. We are not sure what this exactly implies or means. Additional clarification is required.
Response: The DSR DT thanks you for your comment. The statement that PJM is referring to applies to Regional Entities that also have a functional model obligation.		
Southern Company		Need guidance for incorporating disturbance reporting that is in CIP-008.
Response: The DSR DT thanks you for your comment. EOP-004-2 is the reporting vehicle for CIP-008. CIP-008-4, Requirement 1, Part 1,3 will be retired upon approval of EOP-004-2.		
We Energies		Attachment 2: What do the asterisks refer to? I didn?t see a comment or description related to them.#7 & #10: What is ?tripped?? Automatic or manual or both.#13: This report has no Part 1.Flowchart: By the flowchart, the only time an OE-417 is filed is when I do not need to contact Law Enforcement. The Reporting Hierarchy flow chart should be modified. In the lower right corner it indicates that if sabotage is not confirmed, the state law enforcement agency investigates. Law enforcement agencies will not investigate an incident that is not a crime. Note too that state law enforcement agencies do not even investigate these kinds of events unless and until requested by local law enforcement. The local law enforcement agency always has initial jurisdiction until surrendered or seized by a superior agency?s authority. Evidence Retention is incomplete. From the NERC Standards Process Manual: ?Evidence Retention: Identification, for each requirement in the standard, of the entity that is responsible for retaining evidence to demonstrate compliance, and the duration for retention of that evidence.?

Organization	Yes or No	Question 17 Comment
Response: The DSR DT thanks you for your comment. Attachment 1 and Attachment 2 have been updated per comments received. The Flowchart has been updated per your comment.		
Compliance & Responsiblity Organization		Nuclear power plants (a need for a revised approach)With respect to sabotage, damage or destruction of BES equipment, damage or destruction of a Critical Asset, damage or destruction of a Critical Cyber Asset, forced intrusion, etc., nuclear plants already have a responsibility to report the events to the FBI and the Nuclear Regulatory Commission (NRC). Performing another report to NERC, with potentially different requirements, within 60 minutes of an event does not seem necessary or practical. It would also be difficult, during an event, to report to external organizations, including but not limited to the Responsible Entities? Reliability Coordinator, NERC, Responsible Entities? Regional Entity, Law Enforcement, and Governmental or Provincial Agencies when operations personnel are pre-occupied with an abnormal or emergency situation. Further, nuclear plants already have an obligation to report the loss of off site power to NRC. Similarly, now that cyber assets will be regulated by the NRC, these reporting requirements should not be applicable to a nuclear power plant. Thus, there is a need to exempt nuclear power plants from these requirements or provide more flexibility to such plants, given its pre-existing NRC reporting requirements.Attachment 1.There is no explanation for why a report must be submitted within one hour of a event. As stated with respect to nuclear, an entity should not be prioritizing between stabilizing the system and reporting. One approach that would help balance conflicting priorities is to start the time frame after ?all is clear.? Another approach could involve the use of target times, with an allowance for exceptions during emergencies or situations in which it is impracticable. Another alternative is to have two times: an earlier ?target reporting time? and second later ?mandatory reporting time.? Further, the current wording suggests that a generator owner or generator operator will be able to determine the impact or potential impact on the BES. This is not realistic, given that impacts to the BES are generally only understood at a transmission operator or reliability coordinator level. Thus, the concept of relying on generators to determine impacts on the BES needs to be eliminated.Also, as written, for a generator, Attachment 1 appears to require a report when a lighting arrestor fails at a Critical Asset. NextEra cannot see any justification for reporting such an event, and this is another reason why Attachment 1 needs more review and revision prior to the next draft of EOP-004-2. This one reason why NextEra has suggested a materiality test for reporting in a definition of Attempted or Actual Sabotage.
Response: The DSR DT thanks you for your comment. Attachment 1 has been updated per comments received. Any NRC requirements or comments fall outside the scope of this project.		
Exelon		The DSR SDT makes reference to comments that were previously provided that suggested adopting the NRC definition of "sabotage." Respectfully, this commenter believes the DSR SDT did not understand the intent of the original comment. The comment made by Exelon in the October 15, 2009 submittal was to ensure that the DSR SDT made an effort to include the Nuclear Regulatory Commission (NRC) as a key Stakeholder in

Organization	Yes or No	Question 17 Comment
		the Reporting Process and to consider utilizing existing reporting requirements currently required by the NRC for each nuclear generator operator.Depending on the event, a nuclear generator operator (NRC licensee) also has specific regulatory requirements to notify the NRC for certain notifications to other governmental agencies in accordance with 10 CFR 50.72, "Immediate notification requirements for operating nuclear power reactors," paragraph (b)(2)(xi).The one hour notification requirement for an intrusion event would also meet an emergency event classification at a nuclear power plant. If an operations crew is responsible for the one hour notification and if separate notifications must be completed within the Emergency Plan event response, then an evaluation in accordance with 10 CFR 50.54, "Conditions of licensees," paragraph (q), would need to be performed to ensure that this notification requirement would not impact the ability to implement the Emergency Plan.At a minimum the DSR SDT should communicate this project to the NRC to ensure that existing communication and reporting that a licensee is required to perform in response to a radiological sabotage event (as defined by the NRC) or any incident that has impacted or has the potential to impact the BES does not create either duplicate reporting, conflicting reporting thresholds or confusion on the part of the nuclear generator operator. Note that existing reporting/communication requirements are already established with the FBI, DHS, NORAD, FAA, State Police, LLEA and the NRC depending on the event. There are existing nuclear plant specific memorandums of understanding between the NRC and the FBI and each nuclear generating site licensee must have a NRC approved Security Plan that outlines applicable notifications to the FBI. Depending on the severity of the security event, the nuclear licensee may initiate the Emergency Plan. The proposed "Reporting Hierarchy for Impact Event EOP-004-2," needs to be communicated and coordinated with the NRC to ensure that the flow chart does not conflict with existing expected NRC requirements and protocol associated with site specific Emergency and Security Plans. Propose allowing for verbal reporting via telephone, for 1 hr. reporting with a follow up using the forms.With the revised standard EOP-004-2 it eliminates the #8; loss of electric service >= 50K, however, that requirement is still required for the DOE-OE-417 form. The question is do we still have to send it to NERC / Region if NERC/ Region does not specifically still have that as a requirement? Also, with that requirement, on the current EOP-004-1 it says that schedule 1 has to be filled out within 1 hour? This doe not coincide with DOE-OE-417 form. The bottom line, it looks like there is inconsistency as to what is reportable per EOP-004-2 and DOE-OE-417 form, some of the items are redundant, some are not, but better guidance is needs as to which form to use when. The SDT should have a Webaniar with the industry to create an understanding as to who is responsible to report what and at what time.
Response: The DSR DT thanks you for your comment. The NRC issues falls outside the scope of this project		
City of Tallahassee (TAL)		Attachment 2 (Impact Event Reporting Form) items 8, 9, 10, and 11 have an asterisk but no identification as to what the asterisks refer to.
Response: The DSR DT thanks you for your comment. The asterisk was addressed at the bottom of the second page of the form. Attachment 2 has been		

Organization	Yes or No	Question 17 Comment
updated to align with the types of events that are to be reported.		
APX Power Markets		The reporting of Impact Events needs to be clear spelled out and if moving some of that to State Agencies it needs to be consistent in all States at the same time and which State it should be reported to. We have a 24-hour Desk in one state that handles facilites in many other States. If there is an Impact Event that needs to be reported, where is that report sent to. The State the facility resides in or the State where our 24-hour Desk resides in.
Response: The DSR DT thanks you for your comment. Attachment 1 has been updated per comments received and a new column has been added to reflect who the impacted entity is required to report to.		
Arkansas Electric Cooperative Corporation		We appreciate the added context through the use of extended background information, rationale statements, and corresponding guideline and hope this context will remain in line with the Standards through the ballot and approval process. We have a few suggestions and questions related to this context. Our comments for this question relate to the contextual information. First of all, in the diagram on page 8, we suggest the appropriate question to ask is "Is event associated with potential criminal activity?" rather than "Report to Law Enforcement?? Also, it would be helpful to make clear the communication flow associated with the State Agency is the responsibility of the State Agency and not the Responsible Entity. This could be shown with a different colored background that calls this process out separately. In the rationale box for R3, it states "The DSR SDT intends?? We propose this should read similar to "The objective of this requirement is?? Overall, we suggest the SDT review the guidance document to make sure any changes made to the requirements are consistent with the guidance.
Response: The DSR DT thanks you for your comment. The flowchart has been updated per comments received. The Rationale box will be removed upon this Standard being Filled for approval.		
American Electric Power		We still do not agree that LSE, TSP and IA should be included in the applicability of this standard. Having processes to report to local or federal law enforcement agencies is ?legislating the obvious?. The focus on this standard should only be on Impact Event reporting to reliability entities.
Response: The DSR DT thanks you for your comment. Attachment 1 has been reviewed and updated. The LSE, TSP, and IA are required under the CIP Standards and Attachment 1 is based on reporting per the CIP requirements.		
Consumers Energy		1. We appreciate the aggregation of redundant standards on this subject, but have some concerns about the content of the aggregated standard as listed below and in reference to previous questions on this comment form.2. It is not clear whether an event that meets OE-417 reporting criteria but is not defined within EOP-

Organization	Yes or No	Question 17 Comment
		004-2 is an Impact Event; for example, ?loss of 50,000 or more customers for 1 hour or more? is required to be reported to DOE as a OE-417 type 11 event but it is not clear whether EOP-004-2 requires that such events be also reported to NERC. The ?Reporting Hierarchy? flow chart seems to suggest that any OE-417 must still be filed with NERC/RE. If the flow chart is not consistent with the intent of the Requirements, it must be clarified.3. NERC implies active involvement of law enforcement. This assumes that law enforcement has the resources to be involved in an Impact Event investigation and fulfill the standard reporting requirements. This is an unrealistic expectation as we have experienced first-hand, a lack of response by law enforcement agencies as their resources shrink due to economic issues. Additionally, NERC is asking that we place credence in law enforcement, on our behalf, to make a definitive decision about the reporting of events. Refer to page 6 of EOP-004-2 under ?Law Enforcement Reporting?: ??Entities rely upon law enforcement agencies to respond and investigate those Impact Events which have the potential of wider area affect?? In many cases, the internal security function must work with system operations personnel to thoroughly understand the system and the effects of certain events. It is unrealistic to think law enforcement would be in a position to make BES decisions within the timeframe given without having system operations experience. It is our experience that external agencies do not understand the integration / inter-connectivity, resiliency, or implications of our energy infrastructure.4. Within Michigan, a ?Michigan Fusion Center: Michigan Intelligence Operations Center (MIOC)? has been established. - Today, we share information such as substation issues and identity theft (not internal issues) to the MIOC. The MIOC is trending incidents on critical infrastructure assets and sectors around the state. The private sector is encouraged to report to the Fusion Center. If NERC is collecting this type of information for future studies and trending / analysis, they should coordinate with each state?s Fusion Center.
Response: The DSR DT thanks you for your comment**.** The DSR SDT has reviewed and updated the Requirements per the comments received. Attachment 1 has been updated and the team has an additional column to reflect where a report should be sent. EOP-004-2 does not define what “law enforcement”” is and that will be left up to each entity.		
Ameren		The following is a list of our greatest concerns. (1) We are concerned about the lack of definitions and use of critical non-capitalized terms. As an example, there is a reportable Impact Event if there is a +/- 10% Voltage Deviation for 15 minutes or more on BES Facilities. As a first example, why is the term Voltage Deviation capitalized when it is not in the NERC Glossary and not proposed to be added? Where is the deviation measured - at any BES metering device? What is the deviation to be reported - the nominal voltage? the high-side of the Voltage Schedule? the low-side of the Voltage Schedule? the generator terminals? when a unit is starting up? All of these are possible interpretations, but < 1% of them would ever result in a Cascading outage - which is the reliability objective of this Standard. A second example is a Generation loss. The threshold for reporting is 2,000 MW, or more, for the Eastern or Western Interconnection. Is this simultaneous loss of capacity over the entire Interconnection? Or, cumulative loss within 1 hour? Or, cumulative loss within 24 hours? How many individual GOPs have responsibility for > 2,000 MW? It seems

Organization	Yes or No	Question 17 Comment
		this would more effectively apply only to an RC and/or BA. The likelihood that one GOP would lose that much generation at once is probably remote. A third example would be the damage or destruction of BES equipment event. The term "equipment" was left lower case with a footnote explanation that includes "?due to intentional or unintentional human action?." This is likely to require the determination of intent by the human involved, which will almost certainly impossible to determine within the 1 hour reporting time. Also, what is the definition of the terms "damage" and "destruction"? Once again, if the reliability intent is to ONLY report Events that have a likely chance of leading to Cascading, this will greatly reduce the potentially enormous reporting burden. that could result without this type of clarification. (2) Without a very thorough understanding of the definitions of the terms requiring reporting, the 1 hour reporting constraint on most events will likely require that we frequently overreport events to minimize any chance of non-compliance. A webinar explaining expected reporting requirements would very useful and valuable. It is also unclear why so many Impact Events require such a short reporting time period. There will almost certainly be many times at 2:00 AM on a weekend when experts and the appropriate personnel will be available to quickly analyze an event and decide, within 1 hour, if a report is necessary. (3) Have all the new Impact Event reporting requirements been checked against reporting requirements from other Standards? For example, the Voltage Deviation Event would appear to potentially overlap/conflict with instructions from a TOP for VAR-002 compliance. Since VAR-002-2 is now in draft, has the SDT worked with that Team to determine if the requirements dovetail?
Response: The DSR DT thanks you for your comment**.** The DSR SDT has updated the Requirements within EOP-004-2 and both Attachments 1 and 2 per comments received. Many of the reporting time frames have been extended to 24 hours per comments received. Voltage deviation is no longer capitalized. All event types are not intended to be new defined terms for the NERC Glossary and have been revised to lower case words. The reporting of voltage deviations is no longer applicable to the GOP which obviates the need to coordinate with the VAR-002 standard drafting team.		
ISO New England, Inc		Under the ?Law Enforcement Reporting? it is stated ?The Standard is intended to reduce the risk of Cascading involving Impact Events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.? We question whether a reporting standard can ?reduce the risk of cascading? and wonder if the reference to the threat ?around them? refers to law enforcement? We would expect that the appropriate operating personnel are the only entities that would be able to mitigate the potential risk to the BES.As it currently stands there is a potential duplication between the reporting requirements under EOP-004-2 (i.e. Attachment 2 Form) and the ERO Event Analysis Process that is undergoing field test (i.e. Event Report Form). This will result in entities (potentially multiple) reporting same event under two separate processes using two very similar forms. Is this the intent or will information requirements be coordinated further prior to adoption in order to meet the declared objective that the impact event reporting under EOP-004 be ?the starting vehicle for any required Event Analysis within the NERC Event Analysis Program?

Organization	Yes or No	Question 17 Comment
Response: The DSR DT thanks you for your comment. The Background section was provided to assist entities in understanding the DSR SDT's process for updating CIP-001 and EOP-004, only.		
Calpine Corp		Focusing on reporting of actual disturbance events as listed in Attachment 1 based on potential or actual impact to the Bulk Electric System will provide maximum benefit to system reliability without adding needless levels of new documentation generated to demonstrate compliance. Absent significant evidence of systemic problems in the industry with past reporting attributable to causes other than a lack of clear guidance on the types events that require reporting, the proposed Standard should focus on the single issue of correct reporting, without attempting to micromanage how Entities internally manage such reporting.
Response: The DSR DT thanks you for your comment. The DSR SDT has updated the requirements andAttachments 1 and 2 per comments received.		
BGE		Please provide a Mapping Document which shows where the four CIP-001 requirements map to in the new EOP-004-2, and note if any of the CIP-001 requirements have been eliminated. A Mapping Document was provided during the first Comment Period, but not during the second Comment Period. A Mapping Document will be very helpful to companies in aligning standard owners in reviewing this proposal and in transitioning compliance programs when the revised standard is approved.
Response: The DSR DT thanks you for your comment. The DSR SDT has a current Mapping Document and it will be updated to reflect the changes that the DSR SDT has made to EOP-004-2. This Mapping document will be posted with the standard when it is posted for comment and ballot.		
CenterPoint Energy		CenterPoint Energy believes the flowchart found on page 8 identifying the reporting hierarchy for EOP-004 is helpful. CenterPoint Energy believes the DOE reporting items should also be included on the right side of the chart. Some of the issues with CIP-001 were a result of law enforcement?s preference and procedures for notification. Law enforcement?s preferences and procedures should be considered for this draft. (Reference: http://www.fbi.gov/contact-us/when)
• **Response:** The DSR DT thanks you for your comment. The DSR SDT has updated the flowchart and a current Mapping Document and it will be updated to reflect the changes that the DSR SDT has made to EOP-004-2. The background section of the standard provides guidance with respect to reporting events to law enforcement. For clarity, the DSR SDT has added the following sentence to the first paragraph under the heading "Law Enforcement Reporting": "These are the types of events that should be reported to law enforcement." The entire paragraph is: "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact		

Organization	Yes or No	Question 17 Comment
a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES."		
PPL Electric Utilities		We thank the SDT for addressing so many Industry concerns with the 2010 draft of EOP-004-2. We feel the current draft version of EOP-004-2 is a significant improvement over current EOP-004-1 and CIP-001-1 standard and the previous draft. Thank you for your time.
Response: Thank you for your comment.		
Occidental Power Marketing		Occidental Power Marketing appreciates the extensive work accomplished by the SDT and their responsiveness to comments. Also, the presentation of this draft with its extensive explanation of the SDT's considerations during development of the draft were very helpful in preparing our comments.
Response: Thank you for your comment.		
Constellation Power Generation		CPG has the following comments regarding Attachment 2:?Generally, this attachment is inadequate for all events. The real-life experience with the recent SW cold snap demonstrated that the questions inadequately capture what may be of greatest concern in the situation. ?Question 4 ? this question is vague. It should be removed. ?Question 7 ? the role of generation in an event may not always be related to a trip. As experienced with the recent SW cold snap, this question may inadequately capture information relevant to the situation at hand. The drafting team should reassess how best to gather information relevant to the event and useful for evaluation.?Question 8 ? generation is not required to monitor frequency during events, so this would not be answered. This question also assumes that frequency had been impacted, which is not always the case (i.e., the plant could not come online). ?The asterisk on some questions in Attachment 2 is not defined.
Response: The DSR DT thanks you for your comment. The DSR SDT has updated the requirements and Attachments 1 and 2 per comments received. Attachment 2 has been streamlined to match the types of events that are to be reported. The purpose of this standard is to have events reported. Once reported, the events are included in the NERC Events Analysis Program for possible further investigation. The asterisk has been removed from Attachment 2.		
Georgia System Operations Corporation		Attachment 2: Impact Event Reporting Form-Instructions for filling out this form are needed.-Line 7, Generation tripped off-line: What is the asterisk for after this task and after the many others following? This should only be reported by a BA. Does generation ?tripped off-line? mean the same as generation ?lost??-Line 9, List of transmission facilities (lines, transformers, buses, etc.) tripped and locked-out: Does this means the same as BES Transmission Elements lost?-Line 10: The column headings in white text on lighter blue

Organization	Yes or No	Question 17 Comment
		background at the top do not seem to apply from this line on.-Line 11, Restoration Time: Restoration of what? Initial/Final clock time? Transmission? What about transmission? Generation/Demand?-Line 13, Identify the initial probable cause or known root cause of the actual or potential Impact Event if known at time of submittal of Part I of this report: ?At the time of submittal of Part I of this report??? Where is Part II? Did you mean Part A? Is Part B to be submitted at a different time?Background-Page 5, last sentence which is continued on page 6: This standard does not recognize the various ?versions? of companies in the industry. The standard is made applicable to a long list of registered entity types. In many cases, many of these entities are wrapped into one company. A company may be responsible for ?everything? in a geographic area. It may be almost every registered entity type with no other registered entities within its geographic area. There should be no conflicts or need for coordination with others for this company. Everything would be coordinated internally within that one company before being reported to NERC and no one else would be reporting to NERC.However, sometimes one company is only a LSE. When an LSE-only is having a LSE impact event, the LSE should report to some higher operating entity like its BA and should not report to NERC. Reporting should be done in a hierarchical manner within appropriate operating entities and then reported to NERC at the RC (or BA) level or as agreed among entities in any coordinated impact event reporting plans. The RC, BA, TOP, and LSE should not all be held accountable for reporting the same event.This standard does not deal exclusively with after-the-fact reporting. Some events deal with the condition of the system (risk of possible future events) or condition of an entity?s ability to operate (supplying fuel, covering load, etc.) or with a threat to the BES.-Page 6, Summary of Concepts: A single form may have been an objective but it is obviously not a concept being implemented by the standard. There are two forms.-Page 6, Law Enforcement Reporting: The object of the standard may be to prevent or reduce the risk of Cascading. Reporting system situations to appropriate operating entities who can take some mitigating action (e.g., a LSE reporting to its BA or a BA reporting to its RC) and reporting threats to law enforcement officials could prevent or reduce the risk of Cascading but reporting to NERC is unlikely to a do that. Reporting of most of the listed events to NERC does not meet the objective of this standard and should be removed from this standard. Such events should be reported to NERC through some other (than a Reliability Standard) requirement for reporting to NERC so that NERC can accomplish its mission of analyzing events. Analyzing events may lead to an understanding that could reduce the future risk of Cascading but not any impending risks.-Page 6, Stakeholders: What is ?Homeland Security ? State?? We know what the Department of Homeland Security and the State Department are but this term is not clear. -Page 6, ?State Regulators?, ?Local Law Enforcement?, and State Law Enforcement?: These are not proper nouns/names and are not defined in the NERC Glossary. They should not be capitalized.-Pages 7 & 8, Law enforcement: Is each entity required to determine procedures for reporting to law enforcement and work it out with the state law enforcement agency? Do the state law enforcement agencies know this? Or is there a pre-determine procedure that is already worked out with the state law enforcement agency that entities are to follow?
• **Response:** The DSR DT thanks you for your comment. The DSR SDT has updated the requirements and Attachments 1 and 2 per comments received.		

Organization	Yes or No	Question 17 Comment
Attachment 2 has been streamlined to match the types of events that are to be reported. The purpose of this standard is to have events reported. Once reported, the events are included in the NERC Events Analysis Program for possible further investigation. The background section of the standard provides guidance with respect to reporting events to law enforcement. For clarity, the DSR SDT has added the following sentence to the first paragraph under the heading "Law Enforcement Reporting": "These are the types of events that should be reported to law enforcement." The entire paragraph is: "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES."		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power		We like the option to use the OE_417 as the reporting form for these events.
Response: The DSR DT thanks you for your comment. EOP-004-2 allows entities to utilize the DOE Form OE-417 to report events.		
Indeck Energy Services		This revision seriously missed the mark.
Response: The DSR DT thanks you for your comment. The DSR SDT has updated the requirements and Attachments 1 and 2 per comments received.		
Progress Energy		Progress thanks the Standard Drafting Team for their efforts on this project.The BES definition is still being revised under ?Project 2010-17: Proposed Definition of Bulk Electric System.? ?BES equipment? is mentioned several times in this Standard. A better definition of BES is important to the effectiveness of this Standard and integral to entities ability to comply with the Standard requirements. In Attachment 2, on the Impact Event Reporting form, item 10 is ?Demand Tripped? and the categories include ?FIRM? and ?INTERRUPTIBLE.? It is unclear why interruptible load is included on the reporting form.
Response: The DSR DT thanks you for your comment. The definition of BES will apply to this standard after it is approved by stakeholders, the NERC BOT and FERC. The DSR SDT has updated the requirements, Attachments 1 and 2 per comments received. Attachment 2 has been streamlined to match the types of events that are to be reported. The purpose of this standard is to have events reported. Once reported, the events are included in the NERC Events Analysis Program for possible further investigation. Firm and Interruptible load have been removed from the list of reportable events in Attachment 1.		

Consideration of Comments

Disturbance and Sabotage Reporting (Project 2009-01)

The Disturbance and Sabotage Reporting Drafting Team thanks all commenters who submitted comments on the second formal posting for Project 2009-01—Disturbance and Sabotage Reporting. The standard was posted for a 45-day public comment period from October 28, 2011 through December 12, 2011 and included an initial ballot during the last 10 days of the comment period. Stakeholders were asked to provide feedback on the standard and associated documents through a special electronic comment form. There were 76 sets of comments, including comments from approximately 171 different people from approximately 140 companies representing nine of the ten Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page:

http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President of Standards and Training, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

Summary Consideration

EOP-004-2 was posted for a 45-day formal comment period and initial ballot from October 28-December 12, 2011. The DSR SDT received comments from stakeholders to improve the readability and clarity of the requirements of the standard. The revisions that were made to the standard are summarized in the following paragraphs.

Purpose Statement

The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:

> "To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."

[1] The appeals process is in the Standard Processes Manual
http://www.nerc.com/files/Appendix_3A_Standard_Processes_Manual_Rev%201_20110825.pdf

Operating Plan

Based on stakeholder comments, Requirement R1 was revised for clarity. Part 1.1 was revised to replace the word "identifying" with "recognizing" and Part 1.2 was eliminated. This also aligns the language of the standard with FERC Order 693, Paragraph 471.

> "(2) specify baseline requirements regarding what issues should be addressed in the **procedures for recognizing** {emphasis added} sabotage events and making personnel aware of such events;"

Requirement R1, Part 1.3 (now Part 1.2) was revised by eliminating the phrase "as appropriate" and adding language indicating that the Responsible Entity is to define its process for reporting and with whom to report events. Part 1.2 now reads:

> "1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."

The SDT envisions that most entities will only need to slightly modify their existing CIP-001 Sabotage Reporting procedures to comply with the Operating Plan requirement in this proposed standard. As many of the features of both sabotage reporting procedures and the Operating Plan are substantially similar, the SDT feels that some information in the sabotage reporting procedures may need to updated and verified.

Operating Plan Review and Communications Testing

Requirement R1, Part 1.4 was removed and Requirement 1, Part, 1.5 was separated out as new Requirement 4. Requirement R4 was revised and is now R3. FERC Order 693, Paragraph 466 includes provisions for periodic review and update of the Operating Plan:

> "466. The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."

Requirement R3 requires an annual test of the communication portion of Requirement R1 while Requirement R4 requires an annual review of the Operating Plan.:

> "R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2."
>
> "R4. Each Responsible Entity shall conduct an annual review of the event reporting Operating Plan in Requirement R1."

The DSR SDT envisions that the annual test will include verification that communication information contained in the Operating Plan is correct. As an example, the annual update of the Operating Plan could include calling "others as defined in the Responsibility Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. Note that there is no requirement to test the reporting of events to the Electric Reliability Organization and the Responsible Entity's Reliability Coordinator.

Operating Plan Implementation

Most stakeholders indicated that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to:

> "R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."

Reporting Timelines

The DSR SDT received many comments regarding the various entries of Attachment 1. Many commenters questioned the reliability benefit of reporting events to the ERO within 1 hour. Most of the events with a one hour reporting requirement were revised to 24 hours based on stakeholder comments; those types of events are currently required to be reported within 24 hours in the existing mandatory and enforceable standards. The only remaining type of event that is to be reported within one hour is "A reportable Cyber Security Incident" as it is required by CIP-008 and FERC Order 706, Paragraph 673:

> "direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"

The table was reformatted to separate one hour reporting and 24 hour reporting. The last column of the table was also deleted and the information contained in the table was transferred to the sentence above each table. These sentences are:

> "One Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the event."

> "Twenty-four Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within twenty-four hour of recognition of the event."

Note that the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.

Cyber-Related Events

The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1. Stakeholders pointed out these events are adequately addressed through the CIP-008 and "Damage or Destruction of a Facility "reporting thresholds. CIP-008 addresses Cyber Security Incidents which are defined as:

> "Any malicious act or suspicious event that:
>
> - Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,
> - Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset."

A Critical Asset is defined as:

> "Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."

Since there is an existing event category for damage or destruction of Facilities, having a separate event for "Damage or Destruction of a Critical Asset" is unnecessary.

Damage or Destruction

The event for "Destruction of BES equipment" has been revised to "Damage or destruction of a Facility". The threshold for reporting information was expanded for clarity:

> "Damage or destruction of a Facility that: affects an IROL
> OR
> Results in the need for actions to avoid an Adverse Reliability Impact
> OR
> Results from intentional human action."

Facility Definition

The DSR SDT used the defined term "Facility" to add clarity for this event as well as other events in Attachment 1. A Facility is defined as:

> "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"

The DSR SDT did not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.

Physical Threats

Several stakeholders expressed concerns relating to the "Forced Intrusion" event. Their concerns related to ambiguous language in the footnote. The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "Any physical threat that could impact the operability of a Facility".

Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.

The footnote regarding this event type was expanded to provide additional guidance in:

> "Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also, report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."

Use of DOE OE-417

The DSR SDT received many comments requesting consistency with DOE OE-417 thresholds and timelines. These items, as well as, the Events Analysis Working Group's (EAWG) requirements were considered in creating Attachment 1, but differences remain for the following reasons:

- EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'
- OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America
- NERC has no control over the criteria in OE-417, which can change at any time
- Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary

In an effort to minimize administrative burden, US entities may use the OE-417 form rather than Attachment 2 to report under EOP-004. The SDT was informed by the DOE of its new online process coming later this year. In this process, entities may be able to record email addresses associated with their Operating Plan so that when the report is submitted to DOE, it will automatically be forwarded to the posted email addresses, thereby eliminating some administrative burden to forward the report to multiple organizations and agencies.

Miscellaneous

Other minor edits were made to Attachment 1. Several words were capitalized but not defined terms. The DSR SDT did not intend for these terms to be capitalized (defined terms) and these words were reverted to lower case. The event type "Loss of monitoring or all voice communication capability" was divided into two separate events as "Loss of monitoring capability" and "Loss of all voice communication capability".

Attachment 2 was updated to reflect the revisions to Attachment 1. The reference to "actual or potential events" was removed. Also, the event type of "other" and "fuel supply emergency" was removed as well.

It was noted that 'Transmission Facilities' is not a defined term in the NERC Glossary. Transmission and Facilities are separately defined terms. The combination of these two definitions are what the DSR SDT has based the applicability of "Transmission Facilities" in Attachment 1.

Index to Questions, Comments, and Responses

1. The DSR SDT has revised EOP-004-2 to remove the training requirement R4 based on stakeholder comments from the second formal posting. Do you agree this revision? If not, please explain in the comment area below..... 18
2. The DSR SDT includes two requirement regarding implementation of the Operating Plan specified in Requirement R1. The previous version of the standard had a requirement to implement the Operating plan as well as a requirement to report events. The two requirements R2 and R3 were written to delineate implementation of the Parts of R1. Do you agree with these revisions? If not, please explain in the comment area below..... 42

   R2. Each Responsible Entity shall implement the parts of its Operating Plan that meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts 1.4 and 1.5 as specified.

   R3. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.

3. The DSR SDT revised reporting times for many events listed in Attachment 1 from one hour to 24 hours. Do you agree with these revisions? If not, please explain in the comment area below..... .. 79
4. Do you have any other comment, not expressed in the questions above, for the DSR SDT?.....156

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Gerald Beckerle	SERC OC Standards Review Group	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Charlie Cook	TVA		5, 6, 1, 3
2.	Jake Miller	Dynegy	SERC	5
3.	Joel Wise	TVA	SERC	1, 3, 5, 6
4.	Tim Hattaway	PowerSouth	SERC	1, 5
5.	Robert Thomasson	BREC	SERC	1
6.	Shaun Anders	CWLP	SERC	1, 3
7.	Jim Case	Entergy	SERC	1, 3, 6
8.	Tim Lyons	OMU	SERC	3, 5
9.	Len Sandberg	Dominion Virginia Power	SERC	1, 3, 5, 6
10.	Brad Young	LGE-KU	SERC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
11. Larry Akens	TVA	SERC 1, 3, 5, 6										
12. Mike Hirst	Cogentrix	SERC 5										
13. Wayne Van Liere	LGE-KU	SERC 3										
14. Scott Brame	NCEMC	SERC 1, 3, 4, 5										
15. Steve Corbin	SERC Reliability Corp.	SERC 10										
16. John Johnson	SERC Reliability Corp.	SERC 10										
17. John Troha	SERC Reliability Corp.	SERC 10										
2. Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliaiblity Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Ben Wu	Orange and Rockland Utilities	NPCC	1
7.	Peter Yost	Consolidated Edison co. of New York, Inc.	NPCC	3
8.	Kathleen Goodman	ISO - New England	NPCC	2
9.	Chantel Haswell	FPL Group, Inc.	NPCC	5
10.	David Kiguel	Hydro One Networks Inc.	NPCC	1
11.	Michael R. Lombardi	Northeast Utilities	NPCC	1
12.	Randy Macdonald	New Brunswick Power Transmission	NPCC	9
13.	Bruce Metruck	New York Power Authority	NPCC	6
14.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
15.	Robert Pellegrini	The United Illuminating Company	NPCC	1
16.	Si-Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
17.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
18.	Saurabh Saksena	National Grid	NPCC	1
19.	Michael Schiavone	National Grid	NPCC	1
20.	Wayne Sipperly	New York Power Authority	NPCC	5
21.	Tina Teng	Independent Electricity System Operator	NPCC	2
22.	Donald Weaver	New Brunswick System Operator	NPCC	2

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Group	Steve Alexanderson	Pacific Northwest Small Public Power Utility Comment Group			X	X					X	

	Additional Member	Additional Organization	Region	Segment Selection
1.	Russell A. Noble	Cowlitz County PUD No. 1	WECC	3, 4, 5
2.	Ronald Sporseen	Blachly-Lane Electric Cooperative	WECC	3
3.	Ronald Sporseen	Central Electric Cooperative	WECC	3
4.	Ronald Sporseen	Consumers Power	WECC	1, 3
5.	Ronald Sporseen	Clearwater Power Company	WECC	3
6.	Ronald Sporseen	Douglas Electric Cooperative	WECC	3
7.	Ronald Sporseen	Fall River Rural Electric Cooperative	WECC	3
8.	Ronald Sporseen	Northern Lights	WECC	3
9.	Ronald Sporseen	Lane Electric Cooperative	WECC	3
10.	Ronald Sporseen	Lincoln Electric Cooperative	WECC	3
11.	Ronald Sporseen	Raft River Rural Electric Cooperative	WECC	3
12.	Ronald Sporseen	Lost River Electric Cooperative	WECC	3
13.	Ronald Sporseen	Salmon River Electric Cooperative	WECC	3
14.	Ronald Sporseen	Umatilla Electric Cooperative	WECC	3
15.	Ronald Sporseen	Coos-Curry Electric Cooperative	WECC	3
16.	Ronald Sporseen	West Oregon Electric Cooperative	WECC	3
17.	Ronald Sporseen	Pacific Northwest Generating Cooperative	WECC	3, 4, 8
18.	Ronald Sporseen	Power Resources Cooperative	WECC	5

4.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Allen	City Utilities of Springfield	SPP	1, 4
2.	Clem Cassmeyer	Western Farmer's Electric Cooperative	SPP	1, 3, 5
3.	Michelle Corley	Cleco Power	SPP	1, 3, 5
4.	Kevin Emery	Carthage Water and Electric Plant	SPP	NA
5.	Jonathan Hayes	Southwest Power Pool	SPP	2
6.	Philip Huff	Arkansas Electric Cooperative Corporation	SPP	3, 4, 5, 6
7.	Ashley Stringer	Oklahoma Municipal Power Authority	SPP	4

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

	Additional Member	Additional Organization	Region	Segment Selection
1.	Patricia Robertson	BC Hydro	WECC	1
2.	Rama Vinnakota	BC Hydro	WECC	2
3.	Pat Harrington	BC Hydro	WECC	3
4.	Clement Ma	BC Hydro	WECC	5
5.	Daniel O'Hearn	BC Hydro	WECC	6

6.	Group	Mary Jo Cooper	ZGlobal on behalf of City of Ukiah, Alameda Municipal Power, Salmen River Electric, City of Lodi			X							X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Elizabeth Kirkley	City of Lodi	WECC	3
2.	Colin Murphey	City of Ukiah	WECC	3
3.	Douglas Draeger	Alameda Municipal Power	WECC	3
4.	Ken Dizes	Salmen River Electric Coop	WECC	3

7.	Group	WILL SMITH	MRO NSRF										

	Additional Member	Additional Organization	Region	Segment Selection
1.	MAHMOOD SAFI	OPPD	MRO	1, 3, 5, 6
2.	CHUCK LAWRENCE	ATC	MRO	1
3.	TOM WEBB	WPS	MRO	3, 4, 5, 6
4.	JODI JENSON	WAPA	MRO	1, 6
5.	KEN GOLDSMITH	ALTW	MRO	4
6.	ALICE IRELAND	NSP (XCEL)	MRO	1, 3, 5, 6
7.	DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6
8.	ERIC RUSKAMP	LES	MRO	1, 3, 5, 6
9.	JOE DEPOORTER	MGE	MRO	3, 4, 5, 6
10.	SCOTT NICKELS	RPU	MRO	4
11.	TERRY HARBOUR	MEC	MRO	1, 3, 5, 6
12.	MARIE KNOX	MISO	MRO	2
13.	LEE KITTELSON	OTP	MRO	1, 3, 4, 5
14.	SCOTT BOS	MPW	MRO	1, 3, 5, 6
15.	TONY EDDLEMAN	NPPD	MRO	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
16. MIKE BRYTOWSKI	GRE	MRO	1, 3, 5, 6										
17. RICHARD BURT	MPC	MRO	1, 3, 5, 6										
8.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No Additional members listed.													
9.	Group	Jesus Sammy Alcaraz	Imperial Irrigation District	X		X	X	X	X				
Additional Member	Additional Organization	Region	Segment Selection										
1. Tino Zaragoza	IID	WECC	1										
2. Jesus Sammy Alcaraz	IID	WECC	3										
3. Diana Torres	IID	WECC	4										
4. Marcela Caballero	IID	WECC	5										
5. Cathy Bretz	IID	WECC	6										
10.	Group	Jean Nitz	ACES Power Marketing Standards Collaborators						X				
Additional Member	Additional Organization	Region	Segment Selection										
1. Chris Bradley	Big Rivers Electric Corporation	SERC	1										
2. Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5										
3. Susan Sosbe	Wabash Valley Power Association	RFC	3										
4. Scott Brame	North Carolina Electric Membership Corporation	RFC	5, 1, 3, 4										
5. Shari Heino	Brazos Electric Power Cooperative, Inc.	ERCOT	1										
6. Lindsay Shepard	Western Farmers Electric Cooperative	SPP	1, 5										
11.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				
Additional Member	Additional Organization	Region	Segment Selection										
1. Timothy Beyrle	City of New Smyrna Beach	FRCC	4										
2. Greg Woessner	KissimmeeUtility Authority	FRCC	3										
3. Jim Howard	Lakeland Electric	FRCC	3										
4. Lynne Mila	City of Clewiston	FRCC	3										
5. Joe Stonecipher	Beaches Energy Services	FRCC	1										
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4										
7. Randy Hahn	Ocala Utility Services	FRCC	3										
12.	Group	Terry L. Blackwell	Santee Cooper	X		X		X	X				
Additional Member	Additional Organization	Region	Segment Selection										

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
1. S. T. Abrams	Santee Cooper	SERC 1										
2. Wayne Ahl	Santee Cooper	SERC 1										
3. Rene Free	Santee Cooper	SERC 1										
13. Group	Joe Tarantino	Sacramento Municipal Utility District (SMUD)	X		X	X	X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Kevin Smith	BANC	WECC 1										
14. Group	Robert Rhodes	SPP Standards Review Group		X								
Additional Member	Additional Organization	Region Segment Selection										
1. John Allen	City Utilities of Springfield	SPP 1, 4										
2. Clem Cassmeyer	Western Farmer's Electric Cooperative	SPP 1, 3, 5										
3. Michelle Corley	Cleco Power	SPP 1, 3, 5										
4. Kevin Emery	Carthage Water and Electric Plant	SPP NA										
5. Jonathan Hayes	Southwest Power Pool	SPP 2										
6. Philip Huff	Arkansas Electric Cooperative Corporation	SPP 3, 4, 5, 6										
7. Ashley Stringer	Oklahoma Municipal Power Authority	SPP 4										
15. Group	Connie Lowe	Dominion	X		X		X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Louis Slade		RFC 3, 6										
2. Michael Crowley		SERC 1, 3										
3. Mike Garton		NPCC 5, 6										
4. Michael Gildea		MRO 5, 6										
16. Group	Sam Ciccone	FirstEnergy	X		X	X	X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Doug Hohlbaugh	FE	RFC 1, 3, 4, 5, 6										
2. Larry Raczkowski	FE	RFC 1, 3, 4, 5, 6										
3. Jim Eckels	FE	RFC 1										
4. John Reed	FE	RFC 1										
5. Ken Dresner	FE	RFC 5										
6. Bill Duge	FE	RFC 5										
7. Kevin Querry	FE	RFC 5										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
17.	Group	Annette M. Bannon	PPL Electric Utilities and PPL Supply Organizations`	X				X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Brenda Truhe	PPL Electric Utilities	RFC	1
2.	Annette Bannon	PPL Generation	RFC	5
3.	Annette Bannon	PPL Generation	WECC	5
4.	Mark Heimbach	PPL EnergyPlus	MRO	6
5.	Mark Heimbach	PPL EnergyPlus	NPCC	6
6.	Mark Heimbach	PPL EnergyPlus	RFC	6
7.	Mark Heimbach	PPL EnergyPlus	SERC	6
8.	Mark Heimbach	PPL EnergyPlus	SPP	6
9.	Mark Heimbach	PPL EnergyPlus	WECC	6

18.	Group	Tom McElhinney	Electric Compliance	X		X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Ted Hobson		FRCC	1
2.	John Babik		FRCC	5
3.	Garry Baker			3

19.	Group	Michael Gammon	Kansas City Power & Light	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Scott Harris	KCP&L	SPP	1, 3, 5, 6
2.	Monica Strain	KCP&L	SPP	1, 3, 5, 6
3.	Brett Holland	KCP&L	SPP	1, 3, 5, 6
4.	Jennifer Flandermeyer	KCP&L	SPP	1, 3, 5, 6

20.	Individual	Stewart Rake	Luminant Power					X					
21.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
22.	Individual	Janet Smith, Regulatory Affairs Supervisor	Arizona Public Service Company	X		X		X	X				
23.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
24.	Individual	Silvia Parada Mitchell	Compliance & Responsbility Office	X		X		X	X				
25.	Individual	Antonio Grayson	Southern Comnpany	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
26.	Individual	John Brockhan	CenterPoint Energy	X									
27.	Individual	Brenton Lopez	Salt River Project	X		X		X	X				
28.	Individual	Bo Jones	Westar Energy	X		X		X	X				
29.	Individual	Michael Johnson	APX Power Markets (NCR-11034)						X				
30.	Individual	David Proebstel	Clallam County PUD No.1			X							
31.	Individual	Michael Moltane	ITC	X									
32.	Individual	Tracy Richardson	Springfield Utility Board			X							
33.	Individual	Kasia Mihalchuk	Manitoba Hydro	X		X		X	X				
34.	Individual	Kevin Conway	Intellibind								X		
35.	Individual	Chris Higgins / Jim Burns / Ted Snodgrass / Jeff Millennor / Russell Funk	Bonneville Power Administration	X		X		X	X				
36.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				
37.	Individual	David Burke	Orange and Rockland Utilities, Inc.	X		X							
38.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
39.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
40.	Individual	Rodney Luck	Los Angeles Department of Water and Power	X		X		X	X				
41.	Individual	Daniel Duff	Liberty Electric Power					X					
42.	Individual	Lisa Rosintoski	Colorado Springs Utilities	X		X		X	X				
43.	Individual	Michael Falvo	Independent Electricity System Operator		X								
44.	Individual	John Bee on Behalf of Exelon	Exelon	X		X		X					
45.	Individual	John D. Martinsen	Public Utility District No. 1 of Snohomish County										
46.	Individual	RoLynda Shumpert	South Carolina Electric and Gas	X		X		X	X				
47.	Individual	Kathleen Goodman	ISO New England		X								

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
48.	Individual	Curtis Crews	Texas Reliability Entity										X
49.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
50.	Individual	Anthony Jablonski	ReliabilityFirst										X
51.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
52.	Individual	Dennis Sismaet	Seattle City Light	X		X	X	X	X				
53.	Individual	John Seelke	PSEG	X		X		X	X				
54.	Individual	Barry Lawson	NRECA										
55.	Individual	Terry Harbour	MidAmerican Energy	X		X		X					
56.	Individual	Thad Ness	American Electric Power	X		X		X	X				
57.	Individual	Guy Andrews	Georgia System Operations Corporation	X		X	X	X	X				
58.	Individual	Ed Davis	Entergy Services										
59.	Individual	Margaret McNaul	Thompson Coburn LLP on behalf of Miss. Delta Energy Agency										
60.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
61.	Individual	Kirit Shah	Ameren	X		X		X	X				
62.	Individual	Linda Jacobson-Quinn	FEUS			X							
63.	Individual	Tom Foreman	Lower Colorado River Authority	X		X		X	X				
64.	Individual	Richard Salgo	NV Energy										
65.	Individual	Nathan Mitchell	American Public Power Association			X							
66.	Individual	Angela Summer	Southwestern Power Administration	X									
67.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
68.	Individual	Tim Soles	Occidental Power Services, Inc. (OPSI)			X			X				
69.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
70.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
71.	Individual	James Sauceda	Energy Northwest - Columbia					X					
72.	Individual	Scott Berry	Indiana Municipal Power Agency				X						

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
73.	Individual	Maggy Powell	Constellation Energy on behalf of Baltimore Gas & Electric, Constellation Power Generation, Constellation Energy Commodities Group, Constellation Control and Dispatch, Constellation NewEnergy and Constellation Energy Nuclear Group.	X		X		X	X				
74.	Individual	Michael Brytowski	Great River Energy	X		X		X	X				
75.	Individual	Christine Hasha	Electric Reliability Council of Texas, Inc.		X								
76.	Individual	Darryl Curtis	Oncor Electric Delivery Company LLC	X									

1. The DSR SDT has revised EOP-004-2 to remove the training requirement R4 based on stakeholder comments from the second formal posting. Do you agree this revision? If not, please explain in the comment area below.

Summary Consideration: As a result of the industry comments, the SDT has further modified the standard as follows:

- Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom events are communicated.
- Combined relevant parts of Requirement R1, Parts 1.4, 1.5 and Requirement R4 into Requirement 1, Part 1.3.
- Deleted the requirement for drills or exercises
- Clarified that only Registered Entities conduct annual tests of the communication process outlined in Requirement 1, Part 1.2
- Changed the review of the Operating Plan to 'annually'

The DSR SDT envisions the testing under Requirement R1, Part 1.3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsibility Entity's Operating Plan" (see Part 1.2) to verify their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.

Despite some industry opposition, both the periodic review of the Operating Plan and the testing requirements were maintained to meet the intent of FERC Order 693, Paragraph 466:

"The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."

Organization	Yes or No	Question 1 Comment
Beaches Energy Services, City of	Negative	First, I wish to thank the SDT for their hard work and making significant progress in significant improvements in the standard. I commend the

Organization	Yes or No	Question 1 Comment
Green Cove Springs		direction that the SDT is taking. There are; however, a few unresolved issues that cause me to not support the standard at this time. 1. An issue of possible differences in interpretation between entities and compliance monitoring and enforcement is the phrase in 1.3 that states "the following as appropriate". Who has the authority to deem what is appropriate? The requirements should be clear that the Responsible Entity is the decision maker of who is appropriate, otherwise there is opportunity for conflict between entities and compliance. *Requirement R1,* Part *1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to communicate events to as stated in the entity's Operating Plan.* In addition, 1.4 is onerous and burdensome regarding the need to revise the plan within 90 days of "any" change, especially considering the ambiguity of "other circumstances". "Other circumstances" is open to interpretation and a potential source of conflict. *Requirement R1, Part 1.4 was removed from the standard.*
Response: Thank you for your comment. Please see response above.		
New Brunswick Power Transmission Corporation	Negative	It is NBPT's opinion that because this is a standard associated with reporting events after an occurrence, it is overly burdensome to require drills and exercises for verification purposes as described in R4. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications*

Organization	Yes or No	Question 1 Comment
		process in Part 1.2.
Response: Thank you for your comment. Please see response above.		
United Illuminating Co.	Negative	R4 is not clear what is expected. There is a difference between testing a process that consists of identify an event then select commuication contacts versus needing to test contacts for each event in Attachment 1 and drill each event and document each event drill. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement r3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* In R2 the phrase "as specified" should be replaced or completed, as specified by what. *The DSR SDT has deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read: "Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004*

Organization	Yes or No	Question 1 Comment
		Attachment1."
Response: Thank you for your comment. Please see response above.		
City of Farmington	Negative	R4 requires verification through a drill or exercise the communication process created as part of R1.3. Clarification of what a drill or exercise should be considered. In order to show compliance to R4 would the entity have to send a pseudo event report to Internal Personnel, the Regional Entity, NERC ES-ISAC, Law Enforcement, and Governmental or provincial agencies listed in R1.3 to verify the communications plan? It would not be a burden on the entity so much, however, I'm not sure the external parties want to be the recipient of approximately 2000 psuedo event reports annually. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.*
Response: Thank you for your comment. Please see response above.		
Hydro One Networks, Inc.	Negative	Referring to Requirement R4, the communication process can be verified without having to go through a drill or exercise. Any specific testing or

Organization	Yes or No	Question 1 Comment
		verification of the process is the responsibility of the Responsible Entity. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *Despite some industry opposition, both periodic review of the Operating Plan and the test requirements were maintained to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
Ameren Services	Negative	The current language in the parenthesis of R4 suggests that the training requirement was actually not removed, in that "a drill or exercise" constitutes training. As documented in the last sentence of the Summary of Key Concepts section, "The proposed standard deals exclusively with after-the-fact reporting." We feel that training, even if it is called drills or exercises is not necessary for an after-the-fact report. *Requirement R4 related to an annual test of the communication portion of*

Organization	Yes or No	Question 1 Comment
		Requirement R1 by a drill or exercise and this has been removed. This has been revised to: *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *Despite some industry opposition, both periodic review of the Operating Plan and the test requirements were maintained to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
Liberty Electric Power LLC	Negative	Voting no due to training not being an option to fill the "drill" requirement. The reason for R4 seems to be to assure personnel will respond to an event in accordance with the entity procedure. Entities meet their obligations for other regulatory requirements with training, and should be permitted to do so for R4. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including*

Organization	Yes or No	Question 1 Comment
		notification to the Electric Reliability Organization, of the communications process in Part 1.2. *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. This language does not preclude the verification of contact information taking place during a training event.*
Response: Thank you for your comment. Please see response above.		
ACES Power Marketing, Hoosier Energy Rural Electric Cooperative, Inc., Sunflower Electric Power Corporation, Great River Energy	Negative	We appreciate the efforts of the SDT in considering the comments of stakeholders from prior comment periods. We believe this draft is greatly improved over the previous version and we agree with the elimination of the term "sabotage" which is a difficult term to define. The determination of an act of sabotage should be left to the proper law enforcement authorities. However, we also realize that the proper authorities would be hard pressed to make these determinations without reporting from industry when there are threats to BES equipment or facilities. We understand and agree there should be verification of the information required for such reporting (contact information, process flow charts, etc). But we still believe improvements can be made to the draft standard. The use of the words "or through a drill or exercise" in Requirement R4 still implies that training is required if no actual event has occurred. When you conduct a fire "drill" you are training your employees on evacuation routes and who they need to report to. Not only are you verifying your process but you are training your employees as well. It is imperative that the information in the Event

Organization	Yes or No	Question 1 Comment
		Reporting process is correct but we don't agree that performing a drill on the process is necessary. We recommend modifying the requirement to focus on verifying the information needed for appropriate communications on an event. And we agree this should take place at least annually. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *This language does not preclude the verification of contact information taking place during a training event.*
Response: Thank you for your comment. Please see response above.		
Florida Municipal Power Agency	No	First, we wish to thank the SDT for their hard work and making significant progress in significant improvements in the standard. We commend the direction that the SDT is taking. There are; however, a few unresolved issues that cause us to not support the standard at this time. An issue of possible differences in interpretation between entities and compliance monitoring and enforcement is the phrase in 1.3 that states "the following as appropriate". Who has the authority to deem what is appropriate? The

Organization	Yes or No	Question 1 Comment
		requirements should be clear that the Responsible Entity is the decision maker of who is appropriate, otherwise there is opportunity for conflict between entities and compliance. *Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to communicate events to as stated in the entity's Operating Plan. Part 1.2 now reads: "A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."* In addition, 1.4 is onerous and burdensome regarding the need to revise the plan within 90 days of "any" change, especially considering the ambiguity of "other circumstances". "Other circumstances" is open to interpretation and a potential source of conflict. *Requirement R1, Part 1.4 was removed from the standard.*
Response: Thank you for your comment. Please see response above.		
Illinois Municipal Electric Agency	No	IMEA agrees with the removal of the training requirement, but also believes verification is not a necessary requirement for this standard; therefore, R4 is not necessary and should be removed. *Requirement R4 related to an annual test of the communication portion of Requirement 1. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including*

Organization	Yes or No	Question 1 Comment
		notification to the Electric Reliability Organization, of the communications process in Part 1.2. *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.*
Response: Thank you for your comment. Please see response above.		
Indiana Municipal Power Agency	No	IMPA does not believe that R4 is necessary. In addition, if a drill or exercise is used to verify the communication process, some of the parties listed in R1.3 may not want to participate in the drill or exercise every 15 months, such as law enforcement and governmental agencies. IMPA would propose a contacting these agencies every 15 months to verify their contact information only and updating their information in the plan as needed, without performing a drill or exercise. *This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *The testing requirement is included in the Standard to meet the intent of*

Organization	Yes or No	Question 1 Comment
		FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."
Response: Thank you for your comment. Please see response above.		
ISO New England	No	Please see further comments; we do not believe R4 is a necessary requirement in the standard and suggest it be deleted. *Requirement R4 related to an annual test of the communication portion of Requirement 1. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *The testing requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comment. Please see response above.		
Northeast Power Coordinating Council	No	Requirement R4 is unnecessary. Whether or not the process, plan, procedure, etc. is "verified" is of no consequence. EOP standards are intended to have entities prepare for likely events (restoration/evacuation), and to provide tools for similar unforeseen events (ice storms, tornadoes, earthquakes, etc.). They should not force a script when results are what matters. *Requirement R4 related to an annual test of the communication portion of Requirement 1. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *The testing requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 1 Comment
Southern Company	No	Southern agrees with removing the training requirement of R4 from the previous version of the standard. However, Southern suggests that drills and exercises are also training and R4 in this revised standard should be removed in its entirety *The "drill or exercise" language has been deleted. Requirement R4 related to an annual test of the communication portion of Requirement 1. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *The testing requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
Ameren	No	The current language in the parenthesis of R4 suggests that the training requirement was actually not removed, in that "a drill or exercise" constitutes training. As documented in the last sentence of the Summary of

Organization	Yes or No	Question 1 Comment
		Key Concepts section, "The proposed standard deals exclusively with after-the-fact reporting." We feel that training, even if it is called drills or exercises is not necessary for an after-the-fact report. *The "drill or exercise" language has been deleted. Requirement R4 related to an annual test of the communication portion of Requirement 1. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *The testing requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
Liberty Electric Power	No	Training should be left in the standard as an option, along with an actual event, drill or exercise, to demonstrate that operating personnel have knowledge of the procedure. *The "drill or exercise" language has been deleted. Requirement R4 related*

Organization	Yes or No	Question 1 Comment
		to an annual test of the communication portion of Requirement 1. This has been revised to: *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *This language does not preclude the verification of contact information taking place during a training event.*
Response: Thank you for your comment. Please see response above.		
SERC OC Standards Review Group	No	We agree with removing the training requirement of R4; however we believe that drills and exercises are also training and R4 should be removed in its entirety because drills and exercises on an after the fact process do not enhance reliability. *The "drill or exercise" language has been removed. Requirement R4 related to an annual test of the communication portion of Requirement 1 This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include*

Organization	Yes or No	Question 1 Comment
		verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. *The testing requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
ACES Power Marketing Standards Collaborators/Great River Energy	No	We understand and agree there should be verification of the information required for such reporting (contact information, process flow charts, etc). But we still believe improvements can be made to the draft standard, in particular to requirement R4. The use of the words "or through a drill or exercise" still implies that training is required if no actual event has occurred. When you conduct a fire "drill" you are training your employees on evacuation routes and who they need to report to. Not only are you verifying your process but you are training your employees as well. It is imperative that the information in the Event Reporting process is correct but we don't agree that performing a drill on the process is necessary. We recommend modifying the requirement to focus on verifying the information needed for appropriate communications on an event. And we agree this should take place at least annually. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. This has*

Organization	Yes or No	Question 1 Comment
		been revised to: *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *This language does not preclude the verification of contact information taking place during a training event.*
Response: Thank you for your comment. Please see response above.		
Ingleside Cogeneration LP	Yes	: Yes. Ingleside Cogeneration LP agrees that training on an incident reporting operations plan should be at the option of the entity. However, we recommend that a statement be included in the "Guideline and Technical Basis" section that encourages drills and exercises be coincident with those conducted for Emergency Operations. Since front-line operators must send out the initial alert that a reportable condition exists, such exercises may help determine how to manage their reporting obligations during the early stages of the troubleshooting process. This is especially true where a notification must be made within an hour of discovery - a very short time period. *The "drill or exercise" language has been removed. Requirement R4 related to an annual test of the communication portion of Requirement 1. This has*

Organization	Yes or No	Question 1 Comment
		been revised to: *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *This language does not preclude the verification of contact information taking place during a training event.*
Response: Thank you for your comment. Please see response above.		
American Public Power Association	Yes	APPA agrees that removal of the training requirement was an appropriate revision to limit the burden on small registered entities. However, APPA requests clarification from the SDT on the current draft of R4. If no event occurs during the calendar year, a drill or exercise of the Operating Plan communication process is required. APPA believes that if this drill or exercise is required, then it should be a table top verification of the internal communication process such as verification of phone numbers and stepping through a Registered Entity specific scenario. This should not be a full drill with requirements to contact outside entities such as law enforcement, NERC, the RC or other entities playing out a drill scenario. This full drill would be a major burden for small entities. *The "drill or exercise" language has been removed. Requirement R4 related to an annual test of the communication portion of Requirement 1. This has*

Organization	Yes or No	Question 1 Comment
		been revised to: *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.*
Response: Thank you for your comment. Please see response above.		
FirstEnergy	Yes	FirstEnergy supports this removal and thanks the drafting team.
Response: Thank you for your comment. Please see response above.		
Compliance & Responsbility Office	Yes	See comments in response to Question 4.
Response: Thank you for your comment. See response to Question 4.		
NV Energy	Yes	Thank you for responding to the stakeholder comments on this issue.
Response: Thank you for your comment.		
Constellation Energy on behalf of Baltimore Gas & Electric, Constellation Power Generation, Constellation Energy Commodities	Yes	Yes, we support removal of the training requirement.

Organization	Yes or No	Question 1 Comment
Group, Constellation Control and Dispatch, Constellation NewEnergy and Constellation Energy Nuclear Group.		
Response: Thank you for your comment.		
Pacific Northwest Small Public Power Utility Comment Group	Yes	
Southwest Power Pool Regional Entity	Yes	
BC Hydro	Yes	
ZGlobal on behalf of City of Ukiah, Alameda Municipal Power, Salmen River Electric, City of Lodi	Yes	
MRO NSRF	Yes	
Western Electricity Coordinating Council	Yes	
Imperial Irrigation District	Yes	
Santee Cooper	Yes	
Sacramento Municipal Utility District (SMUD)	Yes	

Organization	Yes or No	Question 1 Comment
SPP Standards Review Group	Yes	
Dominion	Yes	
PPL Electric Utilities and PPL Supply Organizations`	Yes	
Electric Compliance	Yes	
Kansas City Power & Light	Yes	
Luminant Power	Yes	
PacifiCorp	Yes	
Arizona Public Service Company	Yes	
CenterPoint Energy	Yes	
Salt River Project	Yes	
Westar Energy	Yes	
APX Power Markets (NCR-11034)	Yes	
Clallam County PUD No.1	Yes	
ITC	Yes	
Springfield Utility Board	Yes	

Organization	Yes or No	Question 1 Comment
Manitoba Hydro	Yes	
Intellibind	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Co. of NY, Inc.	Yes	
Orange and Rockland Utilities, Inc.	Yes	
Xcel Energy	Yes	
Duke Energy	Yes	
Colorado Springs Utilities	Yes	
Independent Electricity System Operator	Yes	
Exelon	Yes	
Public Utility District No. 1 of Snohomish County	Yes	
South Carolina Electric and Gas	Yes	
American Transmission Company, LLC	Yes	
Nebraska Public Power District	Yes	

Organization	Yes or No	Question 1 Comment
Seattle City Light	Yes	
PSEG	Yes	
MidAmerican Energy	Yes	
American Electric Power	Yes	
Georgia System Operations Corporation	Yes	
FEUS	Yes	
Lower Colorado River Authority	Yes	
Southwestern Power Administration	Yes	
Occidental Power Services, Inc. (OPSI)	Yes	
Northeast Utilities	Yes	
City of Austin dba Austin Energy	Yes	
Energy Northwest - Columbia	Yes	
Electric Reliability Council of Texas, Inc.	Yes	
Oncor Electric Delivery Company LLC	Yes	

Organization	Yes or No	Question 1 Comment
Progress Energy		
Los Angeles Department of Water and Power		
Texas Reliability Entity		
ReliabilityFirst		
NRECA		
Entergy Services		
Thompson Coburn LLP on behalf of Miss. Delta Energy Agency		

2. The DSR SDT includes two requirement regarding implementation of the Operating Plan specified in Requirement R1. The previous version of the standard had a requirement to implement the Operating plan as well as a requirement to report events. The two requirements R2 and R3 were written to delineate implementation of the Parts of R1. Do you agree with these revisions? If not, please explain in the comment area below.

R2. Each Responsible Entity shall implement the parts of its Operating Plan that meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts 1.4 and 1.5 as specified.

R3. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.

Summary Consideration: Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to:

"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."

Organization	Yes or No	Question 2 Comment
Ameren Services	Negative	(2) The new wording while well intentioned, effectively does not add clarity and leads to confusion. From our perspective, R1, which requires and Operating Plan, which is defined by the NERC glossary as: "A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan." *The DSR SDT thanks you for your comment. The SDT has made changes to the*

Organization	Yes or No	Question 2 Comment
		requirements highlighted in your comments. *FERC Order 693, Paragraph 466 includes provisions for periodic review and update of the Operating Plan: "466. The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."* (3) Is not a proper location for an after-the-fact reporting standard? In fact it could be argued that after-the-fact reports in and of themselves do not affect the reliability of the bulk electric system. *The DSR SDT does not agree with this comment. Reporting of an event will give the Electric Reliability Organization and your Reliability Coordinator the situational awareness of what has occurred on your part of the BES. Plus as described in your Operating Plan, you would have communicated the event as you saw fit. By broadcasting that an event has occurred you will increase the awareness of your company (as described in your Operating Plan) and increase the awareness of the Electric Reliability Organization and your Reliability Coordinator.* (4) But considering the proposed standard as written with the Operating Plan in requirement R1, and implementation of the Operating Plan in requirement R2 (except the actual reporting which is in R3) and then R3 which requires implementing the reporting section R1.3, it is not clear how these requirements can be kept separate in either implementation nor by the CEA. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2). The test and review requirement is*

Organization	Yes or No	Question 2 Comment
		included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures." (5) The second sentence in the second paragraph of "Rationale for R1" states:"The main issue is to make sure an entity can a) identify when an event has occurred and b) be able to gather enough information to complete the report." This is crucial for a Standard like this that is intended to mandate actions for events that are frequently totally unexpected and beyond normal planning criteria. This language needs to be added to Attachment 1 by the DSR SDT as explained in the rest of our comments. *The DSR SDT has updated the Rationale for Part 1.2 (previous Part 1.3) to read as: "Part 1.2 could include a process flowchart, identification of internal and external personnel or entities to be notified, or a list of personnel by name and their associated contact information." Whereas Part 1.2 now states:* *"1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."*
Response: Thank you for your comment. Please see response above.		
Old Dominion Electric Coop.	Negative	I disagree with two things in the presently drafted standard. First, I do not feel a separate requirement to implement the plan is necessary (R2), *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of*

Organization	Yes or No	Question 2 Comment
		Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read: *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* and I do not think that verification of the communications process should require a minimum of a drill or exercise. This is verified now under th current standard CIP-001 through verifice contact with the appropriate authorities and this should be enough to verify that the communications for the plan is in place. *The "drill or exercise" language has been removed. Requirement R4 related to an annual test of the communication portion of Requirement 1. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.*
Response: Thank you for your comment. Please see response above.		
ACES Power Marketing, Hoosier Energy Rural Electric Cooperative, Inc., Sunflower Electric Power Corporation,	Negative	Requirement R2 requires Responsible Entities to implement the various sub-requirements in R1. We believe it is unnecessary to state that an entity must implement their Operating Plan in a separate requirement. Having a separate requirement seems redundant. If the processes in the Operating Plan are not

Organization	Yes or No	Question 2 Comment
Great River Energy/ ACES Power Marketing Standards Collaborators/ Great River Energy		implemented, the entity is non-compliant with the standard. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* There doesn't need to be an extra requirement saying entities need to implement their Operating Plan. *The test and review requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
Hydro One Networks, Inc.	Negative	Requirement R2 seems to not be necessary. Who would have a plan and not implement it? This may also introduce double jeopardy issues should some entity not have a plan as required in R1. They would be unable to implement something they did not have so automatically non-compliant with R1 and R2. o Requirements R2 and R3 seem to be redundant. Isn't implementing the Operating Plan the same as reporting events in accordance with its Operating Plan? *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of*

Organization	Yes or No	Question 2 Comment
		Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read: *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* The standard mentions collecting information for Attachment 2, but the standard does not state what to do with Attachment 2. Is it merely a record for demonstrating compliance with R3? *The DSR SDT has updated Requirement R2 to read: "Each Responsible Entity must report and communicate events according to its Operating Plan based on the information in Attachment 1."* *The DSR SDT has also added the following statement to Attachment 1 for 1 hour reporting time frame and 24 hour reporting time frame, respectfully:* *"One Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the event"* *And* *"Twenty-four Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within twenty-four hour of recognition of the event."*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 2 Comment
Beaches Energy Services, City of Green Cove Springs	Negative	Requirements R2 and R3 are to implement the Operating Plan. Hence, R3 should be a bullet under R2 and not a separate requirement. In addition, for R2, the phrase "actual event" is ambiguous and should mean: "actual event that meets the criteria of Attachment 1" I suggest the following wording to R2 (which will result in eliminating R3) "Each Responsible Entity shall implement its Operating Plan: o For actual events meeting the threshold criteria of Attachment 1, in accordance with Requirement R1 parts 1.1, 1.2 and 1.3 *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* o For review and updating of the Operating Plan, in accordance with Requirement R1 parts 1.4 and 1.5" Note that I believe that if the SDT decides to not combine R2 and R3, then we disagree with the distinction between the two requirements. *Requirements R2 and R3 have been combined. Requirement 1, Part 1.4 was removed.* The division of implementing R1 through R2 and R3 as presented is "implementing" vs. "reporting". We believe that the correct division should rather be "implementation" of the plan (which includes reporting) vs. revisions to the plan. *The DSR SDT has updated Requirement R2 to read as: "R2. Each Responsible Entity shall implement the Operating Plan that meets Requirement R1 for events listed in Attachment 1."* *FERC Order 693 section 617 states "…the Commission directs the ERO to develop a*

Organization	Yes or No	Question 2 Comment
		modification to EOP-004-1 through the reliability Standards development process that includes any Requirement necessary for users, owners, and operators of the Bulk-Power System to provide data…". In order for entities to provide data they are required to implement their Operating Plan.
Response: Thank you for your comment. Please see response above.		
Ameren	No	(1) The new wording while well intentioned, effectively does not add clarity and leads to confusion. From our perspective, R1, which requires and Operating Plan, which is defined by the NERC glossary as: "A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan." *The DSR SDT has maintained Requirement 1 with the wording of "Operating Plan" which gives entities the flexibility of containing an Operating Process or Operating Procedure, as stated as "An Operating Plan may contain Operating Procedures and Operating Processes. Please note the use of "may contain" in the NERC approved definition.* *Requirement 1 now reads as"* *Each Responsible Entity shall have an Operating Plan that includes:* *1.1. A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the*

Organization	Yes or No	Question 2 Comment
		Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies. (2) Is not a proper location for an after-the-fact reporting standard? In fact it could be argued that after-the-fact reports in and of themselves do not affect the reliability of the bulk electric system. *The DSR SDT does not agree with this comment. Reporting of an event will give the Electric Reliability Organization and your Reliability Coordinator the situational awareness of what has occurred on your part of the BES. Plus as described in your Operating Plan, you would have communicated the event as you saw fit. By broadcasting that an event has occurred you will increase the awareness of your company (as described in your Operating Plan) and increase the awareness of the Electric Reliability Organization and your Reliability Coordinator.* (3) But considering the proposed standard as written with the Operating Plan in requirement R1, and implementation of the Operating Plan in requirement R2 (except the actual reporting which is in R3) and then R3 which requires implementing the reporting section R1.3, it is not clear how these requirements can be kept separate in either implementation nor by the CEA. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2).* *The test and review requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting*

Organization	Yes or No	Question 2 Comment
		procedures." (4) The second sentence in the second paragraph of "Rationale for R1" states: "The main issue is to make sure an entity can a) identify when an event has occurred and b) be able to gather enough information to complete the report." This is crucial for a Standard like this that is intended to mandate actions for events that are frequently totally unexpected and beyond normal planning criteria. This language needs to be added to Attachment 1 by the DSR SDT as explained in the rest of our comments *The DSR SDT has updated the Rationale for Part 1.2 (previous Part 1.3) to read as: "Part 1.2 could include a process flowchart, identification of internal and external personnel or entities to be notified, or a list of personnel by name and their associated contact information." Whereas Part 1.2 now states:* *"1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."*
Response: Thank you for your comment. Please see response above.		
American Electric Power	No	AEP prefers to avoid requirements that are purely administrative in nature. Requirements should be clear in their actions of supporting of the BES. For example, we would prefer requirements which state what is to be expected, and allowing the entities to develop their programs, processes, and procedures accordingly. It has been our understanding that industry, and perhaps NERC as well, seeks to reduce the amount to administrative (i.e. document-based) requirements. We are confident

Organization	Yes or No	Question 2 Comment
		that the appropriate documentation and administrative elements would occur as a natural course of implementing and adhering to action-based requirements. In light of this perspective, we believe that that R1 and R2 is not necessary, and that R3 would be sufficient by itself. Our comments above notwithstanding, AEP strongly encourages the SDT to consider that R2 and R3, if kept, be merged into a single requirement as a violation of R2 would also be a violation of R3. Two violations would then occur for what is essentially only a single incident. Rather than having both R2 and R3, might R3 be sufficient on its own? R2 is simply a means to an end of achieving R3. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2).* . *The test and review requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."* If there is a need to explicitly reference implementation, that could be addressed as part of R1. For example, R1 could state "Each Responsible Entity shall implement an Operating Plan that includes..."R1 seems disjointed, as subparts 1.4 and 1.5 (updating and reviewing the Operating Plan) do not align well with subparts 1.1 through 1.3 which are process related. If 1.4 and 1.5 are indeed needed, we recommend that they be a part of their own requirement(s). Furthermore, the action of these requirements should be changed from emphasizing provision(s) of a process to demonstrating the underlying activity.

Organization	Yes or No	Question 2 Comment
		The DSR SDT has maintained Requirement 1 with the wording of "Operating Plan" which gives entities the flexibility of containing an Operating Process or Operating Procedure, as stated as "An Operating Plan may contain Operating Procedures and Operating Processes. Please note the use of "may contain" in the NERC approved definition. *Requirement 1 now reads as "Each Responsible Entity shall have an Operating Plan that includes:* *1.1. A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.* 1.4 AEP is concerned by the vagueness of requiring provision(s) for updating the Operating Plan for "changes", as such changes could occur frequently and unpredictably. *Part 1.4 was removed from the standard.* *It is the sole responsibility of the Applicable Entity to determine when an annual review of the Operating Plan is required. The Operating Plan has the minimum requirement for an annual review. You may review your Operating Plan as often as you see appropriate.*
Response: Thank you for your comment. Please see response above.		
Occidental Power Services,	No	Attachment 1 and R3 require event reports to be sent to the ERO and the entity's RC and to others "as appropriate." Although this gives the entity some discretion, it

Organization	Yes or No	Question 2 Comment
Inc. (OPSI)		might also create some "Monday morning quarterbacking" situations. This is especially true for the one hour reporting situations as personnel that would be responding to these events are the same ones needed to report the event. OPSI suggests that the SDT reconsider and clarify reporting obligations with the objective of sending initial reports to the minimum number of entities on a need-to-know basis. *Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to communicate events to as stated in the entity's Operating Plan.* *The DSR SDT also received many comments regarding the various events of Attachment 1. Many commenters questioned the reliability benefit of reporting events to the ERO and their Reliability Coordinator within 1 hour. Most of the events with a one hour reporting requirement were revised to 24 hours based on stakeholder comments as well as those types of events are currently required to be reported within 24 hours in the existing mandatory and enforceable standards. The only remaining type of event that is to be reported within one hour is "A reportable Cyber Security Incident" as it required by CIP-008.* *FERC Order 706, paragraph 673 states: "…each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event within one hour of the event…"*
Response: Thank you for your comment. Please see response above.		
Ingleside Cogeneration LP	No	Attachment 1 and requirement R3 are written in a manner which would seem to indicate that internal personnel and law enforcement personnel would have to be copied on the submitted form - either Attachment 2 or OE-417. We believe the intent is to submit such forms to the appropriate recipients only (e.g.; the ERO and

Organization	Yes or No	Question 2 Comment
		the DOE). The requirement should be re-written to clarify that this is the case. *The DSR SDT thanks you for your comment. Requirement 1 has been updated and now reads as"* *Each Responsible Entity shall have an Operating Plan that includes:* *1.1. A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.* *The Applicable Entity's Operating Plan is to contain the process for reporting events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and for communicating to others as defined in the Responsible Entity's Operating Plan. All events in Attachment 1 are required to be reported to the Electric Reliability Organization and the Responsible Entity's Reliability Coordinator. The Operating Plan may include: internal company personnel, your Regional Entity, law enforcement, and governmental or provisional agencies, as you identify within your Operating Plan. This gives you the flexibility to tailor your Operating Plan to fit your company's needs and wants.*
Response: Thank you for your comment. Please see response above.		
Florida Municipal Power Agency	No	Both requirements are to implement the Operating Plan. Hence, R3 should be a bullet under R2 and not a separate requirement. In addition, for R2, the phrase "actual event" is ambiguous and should mean: "actual event that meets the criteria of Attachment 1"We suggest the following wording to R2 (which will result in eliminating R3)"Each Responsible Entity shall implement its Operating Plan: o For actual events meeting the threshold criteria of Attachment 1 in accordance with

Organization	Yes or No	Question 2 Comment
		Requirement R1 parts 1.1, 1.2 and 1.3 *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* o For review and updating of the Operating Plan in accordance with Requirement R1 parts 1.4 and 1.5"Note that we believe that if the SDT decides to not combine R2 and R3, then we disagree with the distinction between the two requirements. *The test and review requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."* The division of implementing R1 through R2 and R3 as presented is "implementing" vs. "reporting". We believe that the correct division should rather be "implementation" of the plan (which includes reporting) vs. revisions to the plan. *The DSR SDT has updated Requirement R2 to read as: "R2. Each Responsible Entity shall implement the Operating Plan that meets Requirement R1 for events listed in Attachment 1."* *FERC Order 693 section 617 states "…the Commission directs the ERO to develop a modification to EOP-001-1 through the reliability Standards development process that includes any Requirement necessary for users, owners, and operators of the*

Organization	Yes or No	Question 2 Comment
		Bulk-Power System to provide data…". In order for entities to provide data they are required to implement their Operating Plan.
Response: Thank you for your comment. Please see response above.		
Indiana Municipal Power Agency	No	Both requirements seem to be implementing the Operating Plan which means R3 should be a bullet under R2 and not a separate requirement. IMPA supports making R2 and R3 one requirement and eliminating the current R3 requirement. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* In addition, R2 needs to be clarified when addressing an actual event. IMPA recommends saying "an actual event that meets the criteria of Attachment 1." *The DSR SDT has implemented your suggestion.* *Requirement R2now reads as: "Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1.".*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 2 Comment
CenterPoint Energy	No	CenterPoint Energy believes the current R2 is unnecessary and duplicative. Upon reporting events as required by R3, entities will be implementing the relevant parts of their Operating Plan that address R1.1 and R1.2. This duplication is clear when reading M2 and M3. Acceptable evidence is an event report. R2 should be modified to remove this duplicative requirement. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."*
Response: Thank you for your comment. Please see response above.		
Orange and Rockland Utilities, Inc./Consolidated Edison Co. Of NY, Inc.	No	Comments: o R1.3 should be revised as follows: A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as determined by the responsible entity: ["appropriate: - deleted] [otherwise it is not clear who determines what communication level is appropriate] o R1.4 should be revised as follows: Provision(s) for updating the Operating Plan following ["within 90 calendar days of any" - deleted] change in assets or personnel (if the Operating Plan specifies personnel or assets) , ["other circumstances" - deleted] that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3. o R1.5 should be deleted. Responsible Entities can determine the frequency of Operating Plan updates. Requirement 1.4 requires updating the Operating Plan within 90 calendar days for changes in "assets, personnel.... or incorporating lessons

Organization	Yes or No	Question 2 Comment
		learned". *Requirement 1 has been updated and now reads as"* *Each Responsible Entity shall have an Operating Plan that includes:* *1.1. A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.* This requirement eliminates the need for Requirement 1.5 requiring a review of the Operating Plan on an annual basis. *The test and review requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
ISO New England	No	In accordance with the results-based standards concept, all that is required, for the "what" is that company X reported on event Y in accordance with the reporting requirements in attachment Z of the draft standard. Therefore, we proposed the only requirement that is necessary is R3, which should be re-written to read..."Each

Organization	Yes or No	Question 2 Comment
		Responsible Entity shall report to address the events listed in Attachment 1." *Requirement 1 and 2 is the basis of the "what" you have described in your comment. Whereas Attachment 1 contains a minimum list of events that apply to Requirement 1, this is why Requirement R2 was rewritten as: "R2. Each Responsible Entity shall implement the Operating Plan that meets Requirement R1 for events listed in Attachment 1."* *The DSR SDT was directed to incorporate certain items such as; FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
SERC OC Standards Review Group	No	It is confusing why R3 is not considered part of R2, which deals with implementation of the Operating Plan and it appears that R3 could be interpreted as double jeopardy. We suggest deleting R3. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement the Operating Plan that meets Requirement R1 for events listed in Attachment 1."*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 2 Comment
Oncor Electric Delivery Company LLC	No	NERC's Event Analysis Program tends to parallel many of the reporting requirements as outlined in EOP-004 Version 2. Oncor recommends that NERC considers ways of streamlining the reporting process by either incorporating the Event Analysis obligations into EOP-004-2 or reducing the scope of the Event Analysis program as currently designed to consist only of "exception" reporting. *The Event Analysis Program may use a reported event as a basis to analyze an event. The reporting required in EOP-004-2 provides the input to the Events Analysis Process. The processes of the Event Analysis Program fall outside the scope of this project, but the DSR SDT has collaborated with them of events contained in Attachment 1.*
Response: Thank you for your comment. Please see response above.		
NV Energy	No	On my read of the Standard, R2 and R3 appear to be duplicative, and I can't really distinguish the difference between the two. The action required appears to be the same for both requirements. Even the Measures for these two sound similar. It is not clear to me what it means to "implement" other than to have evidence of the existence and understanding of roles and responsibilities under the "Operating Plan." I suggest elimination of R2 and inclusion of a line item in Measure 1 calling for evidence of the existence of an "Operating Plan" including all the required elements in R1. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2 Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."*

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comment. Please see response above.		
Northeast Power Coordinating Council	No	R1.3 should be revised as follows: A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as determined by the responsible entity:...Without this change it is not clear who determines what communication level is appropriate. *Requirement 1, Part 1.3 (now Part 1.2) was updated per comments received.* *1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.* R1.4 should be revised as follows: Provision(s) for updating the Operating Plan following any change in assets or personnel (if the Operating Plan specifies personnel or assets), that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3. R1.5 should be deleted. Responsible Entities can determine the frequency of Operating Plan updates. Requirement 1.4 requires updating the Operating Plan within 90 calendar days for changes in "assets, personnel.... or incorporating lessons learned", (or our preceding proposed revision). *Requirement 1, part 1.4 has been deleted and Requirement R2 has been updated to read as: "R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* This requirement eliminates the need for Requirement 1.5 requiring a review of the Operating Plan on an annual basis.

Organization	Yes or No	Question 2 Comment
		The only true requirement that is results-based, not administrative and is actually required to support the Purpose of the Standard is R3. *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:* *"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."*
Response: Thank you for your comment. Please see response above.		
Illinois Municipal Electric Agency	No	R2 is not necessary, and should be removed. Subrequirement R1.4 is also not necessary and should be removed. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."*
Response: Thank you for your comment. Please see response above.		
Kansas City Power & Light	No	Requirement R1.1 is confusing regarding the "process for identifying events listed in Attachment 1". Considering Attachment 1, the Events Table, already identifies the events required for reporting, please clearly describe in the requirement what the "process" referred to in requirement R1.1 represents. *The DSR SDT has reviewed FERC Order 693 and paragraph 471 states: "…(2) specify*

Organization	Yes or No	Question 2 Comment
		baseline requirement regarding what issues should be addressed in the procedures for recognizing sabotage events and making personnel aware of such events…" *The DSR SDT has written Requirement 1, Part 1.1 to read as: "A process for recognizing each of the events listed in EOP-004 Attachment 1". An Applicable Entity may rely on SCADA alarms as a process for recognizing an event or being made aware of an event through a scheduled Facility check. The DSR SDT has not been overly prescriptive on part 1.1 but has allowed each Applicable Entity to determine their own process for recognizing events listed in Attachment 1.*
Response: Thank you for your comment. Please see response above.		
Luminant Power	No	Requirements R1, R2, and R4 are burdensome administrative requirements and are contradictory to the NERC stated Standards Development goals of reducing administrative requirements by moving to performance requirements. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* *Requirement R1, Part 1.3 (now Part 1.2) was revised to indicate that the Responsible Entity is to define its process for reporting and with whom to report events. Part 1.2 now reads:* *"1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004*

Organization	Yes or No	Question 2 Comment
		Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies." There is only one Requirement needed in this standard: "The Responsible Entity shall report events in accordance with Attachment 1." Attachment 1 should describe how events should be reported by what Entity to which party within a defined timeframe. If this requirement is met, all the other proposed requirements have no benefit to the reliability of the Bulk Electric System. Per the NERC Standard Development guidelines, only items that provide a reliability benefit should be included in a standard. *The DSR SDT has updated Attachment 1 to a minimum threshold for Applicable Entities to report contained events. Requirement R2 has been updated to reflect that Applicable Entities shall implement their Operating Plan per Requirement 1 for events listed in Attachment 1. Requirement R2 reads as: "R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."*
Response: Thank you for your comment. Please see response above.		
Xcel Energy	No	Suggest modifying R3 to indicate this is related to R 1.3.Each Responsible Entity shall report events to entities specified in R1.3 and as identified as appropriate in its Operating Plan. *Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3*

Organization	Yes or No	Question 2 Comment
		(now R2) *R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."*
Response: Thank you for your comment. Please see response above.		
Colorado Springs Utilities	No	The act of implementing the plan needs to include reporting events per R1, sub-requirement 1.3. R2 should simply state something like, "Each Responsible Entity shall implement the Operating Plan that meets the requirements of R1, as applicable, for an actual event or as specified." Suggest eliminating R3 which, seems to create double jeopardy effect. *Requirement R2 was updated to reflect comments received to read as: "R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1." R3 was deleted.*
Response: Thank you for your comment. Please see response above.		
Intellibind	No	The language proposed is not clear and will continue to add confusion to entities who are trying to meet these requirements. It is not clear that the drafting team can put itself in the position of how the auditors will interpret and implement compliance against thithe R2 requirement. Requirements should be written to stand alone, not reference other requirements (or parts of the requirments. If the R1 parts 1.1, 1.2, 1.4 and 1.5 are so significant for this requirement, then they should be rewritten in R2. *Most stakeholders believed that Requirements R2 and R3 were redundant and having*

Organization	Yes or No	Question 2 Comment
		both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read: *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."*
Response: Thank you for your comment. Please see response above.		
Southern Company	No	These requirements as drafted in this revised standard potentially create a situation where an entity could be deemed non-compliant for both R2 and R3. For example, if a Responsible Entity included a reporting obligation in its Operating Plan, and failed to report an event, the Responsible Entity could be deemed non-compliant for R2 for not "implementing" its plan and for R3 for not reporting the event to the appropriate entities. A potential solution to address this would be to add Requirement 1, Part 1.3 to Requirement 2 and remove Requirement 3 in its entirety. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."* We also request clarification on Measure M3. Which records should have "dated and time-stamped transmittal records to show that the event was reported"? Some of the communication is handled via face-to-face conversation or through telephone

Organization	Yes or No	Question 2 Comment
		conversation. *Measurement 3 has been deleted since Requirement 3 has been deleted. The new Measurement 2 allows for "…or other documentation". This may be in any form that the Applicable Entity wishes to maintain that they met Requirement 2. The Electric Reliability Organization does allow "Attestations" along with voice recordings as proof of compliance.*
Response: Thank you for your comment. Please see response above.		
Independent Electricity System Operator	No	We agree with the revision to R2 and R3, but assess that a requirement to enforce implementation of Part 1.3 in Requirement R1 is missing. Part 1.3 in Requirement R1 stipulates that:1.3. A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate: o Internal company personnel o The Responsible Entity's Regional Entity o Law enforcement o Governmental or provincial agenciesThe implementation of Part 1.3 is not enforced by R2 or R3 or any other Requirements in the standard. Suggest to add another requirement or expand Requirement R4 (and M4) to require the implementation of this Part in addition to verifying the process. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."* *Requirement 1 has been updated and now reads as"*

Organization	Yes or No	Question 2 Comment
		Each Responsible Entity shall have an Operating Plan that includes: *1.1 A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.*
Response: Thank you for your comment. Please see response above.		
Independent Electricity System Operator	Affirmative	The IESO believes that a requirement to enforce implementation of Part 1.3 in Requirement R1 is missing. Part 1.3 in Requirement R1 stipulates that: 1.3. A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate: o Internal company personnel o The Responsible Entity's Regional Entity o Law enforcement o Governmental or provincial agencies The implementation of Part 1.3 is not enforced by R2 or R3 or any other Requirements in the standard. The IESO suggests that another requirement be added or Requirement R4 (and M4) be expanded to require the implementation of this Part in addition to verifying the process. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the*

Organization	Yes or No	Question 2 Comment
		timeframe specified in EOP-004 Attachment 1." *Requirement 1 has been updated and now reads as"* *Each Responsible Entity shall have an Operating Plan that includes:* *1.1 A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.*
Response: Thank you for your comment. Please see response above.		
Bonneville Power Administration	Yes	BPA believes the measures for R2 are unclear since they are similar to R3's reporting measures.
Response: Thank you for your comment. The SDT has revised the standard to have a single implementation requirement with a single associated measure.		
Compliance & Responsbility Office	Yes	See comments in response to Question 4.
Response: Thank you for your comment. See response to Question 4.		
Constellation Energy on behalf of Baltimore Gas & Electric, Constellation Power Generation, Constellation Energy Commodities Group,	Yes	While we support the delineation of the different activities associated with implementation and reporting, further clarification would be helpful. R1. 1.3: As currently written, it is somewhat confusing, in particular the use of the qualifier "as appropriate". *The DSR SDT has updated Requirement 1, Part 1.2 to read as: "A process for*

Organization	Yes or No	Question 2 Comment
Constellation Control and Dispatch, Constellation NewEnergy and Constellation Energy Nuclear Group.		*communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."* In addition, the use of the word "communicating" to capture both reporting to reliability authorities and notifying others may leave the requirement open to question. Below is a proposed revision: 1.3 A process for reporting events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and for communicating to others as defined in the Responsible Entity's Operating Plan, such as: o Internal company personnel o The Responsible Entity's Regional Entity o Law Enforcement o Government or provincial agenciesR1, 1.4: the last phrase of the requirements seems to be leftover from an earlier version. The requirement should end after the word "Plan".R1, 1.5: "Process" should not be capitalized. While we understand the intent of the draft language and appreciate the effort to streamline the requirements, we propose an adjusted delineation below that we feel tracks more cleanly to the structure of a compliance program. Proposed revised language:R2. Each Responsible Entity shall implement its Operating Plan to meet Requirement R1, parts 1.1 and 1.2 for an actual event(s).M2. Responsible Entities shall provide evidence that it implemented it Operating Plan to meet Requirement R1, Parts 1.1 and 1.2 for an actual event. *The DSR SDT has updated Requirement 1, Part 1.2 to read as: "A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator;*

Organization	Yes or No	Question 2 Comment
		law enforcement governmental or provincial agencies." *The Applicable Entity's Operating Plan is to contain the process for reporting events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and for communicating to others as defined in the Responsible Entity's Operating Plan. All events in Attachment 1 are required to be reported to the Electric Reliability Organization and the Responsible Entity's Reliability Coordinator. The Operating Plan may include: internal company personnel, your Regional Entity, law enforcement, and governmental or provisional agencies, as you identify within your Operating Plan. This gives you the flexibility to tailor your Operating Plan to fit your company's needs and wants.* *DSR SDT has revised R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1.* *DSR SDT has revised M2. "Each Responsible Entity will have, for each event experienced, a dated copy of the completed EOP-004 Attachment 2 form or DOE form OE-417 report submitted for that event; and dated and time-stamped transmittal records to show that the event was reported supplemented by operator logs or other operating documentation. Other forms of evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other operating documentation for situations where filing a written report was not possible.* Evidence may include, but is not limited to, an submitted event report form (Attachment 2) or a submitted OE-417 report, operator logs, or voice recording.R3. Each Responsible Entity shall implement its Operating Plan to meet Requirement R1, parts 1.4 and 1.5.M3. Responsible Entities shall provide evidence that it implemented it Operating Plan to meet Requirement R1, Parts 1.4 and 1.5. Evidence may include, but is not limited to, dated documentation of review and update of the Operating Plan.

Organization	Yes or No	Question 2 Comment
		R4. Each Responsible Entity shall verify (through implementation for an actual event, or through a drill, exercise or table top exercise) the communication process in its Operating Plan, created pursuant to Requirement 1, Part 1.3, at least annually (once per calendar year), with no more than 15 calendar months between verification. M4. The Responsible Entity shall provide evidence that it verified the communication process in its Operating Plan for events created pursuant to Requirement R1, Part 1.3. Either implementation of the communication process as documented in its Operating Plan for an actual event or documented evidence of a drill, exercise, or table top exercise may be used as evidence to meet this requirement. The time period between verification shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or dated documentation of a verification. *Requirement 4 (now R3) was revised as:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]* *M3. Each Responsible Entity will have dated and time-stamped records to show that the annual test of Part 1.2 was conducted. Such evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other communication documentation. The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. (R3)*
Response: Thank you for your comment. Please see response above.		
Exelon	Yes	Why is the reference to R1.3 missing from EOP-004-2 Requirement R2?

Organization	Yes or No	Question 2 Comment
		R1.3 was associated with implementation in R3 which was removed from the standard. DSR SDT has revised R2 to read as: "Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."
Response: Thank you for your comment. Please see response above.		
Pacific Northwest Small Public Power Utility Comment Group	Yes	
Southwest Power Pool Regional Entity	Yes	
BC Hydro	Yes	
ZGlobal on behalf of City of Ukiah, Alameda Municipal Power, Salmen River Electric, City of Lodi	Yes	
MRO NSRF	Yes	
Western Electricity Coordinating Council	Yes	
Imperial Irrigation District	Yes	
Santee Cooper	Yes	

Organization	Yes or No	Question 2 Comment
Sacramento Municipal Utility District (SMUD)	Yes	
SPP Standards Review Group	Yes	
Dominion	Yes	
FirstEnergy	Yes	
PPL Electric Utilities and PPL Supply Organizations`	Yes	
Electric Compliance	Yes	
PacifiCorp	Yes	
Arizona Public Service Company	Yes	
Salt River Project	Yes	
Westar Energy	Yes	
APX Power Markets (NCR-11034)	Yes	
Clallam County PUD No.1	Yes	
ITC	Yes	
Springfield Utility Board	Yes	

Organization	Yes or No	Question 2 Comment
Manitoba Hydro	Yes	
Duke Energy	Yes	
Liberty Electric Power	Yes	
Public Utility District No. 1 of Snohomish County	Yes	
South Carolina Electric and Gas	Yes	
American Transmission Company, LLC	Yes	
Nebraska Public Power District	Yes	
Seattle City Light	Yes	
PSEG	Yes	
MidAmerican Energy	Yes	
Georgia System Operations Corporation	Yes	
FEUS	Yes	
Lower Colorado River Authority	Yes	

Organization	Yes or No	Question 2 Comment
American Public Power Association	Yes	
Northeast Utilities	Yes	
City of Austin dba Austin Energy	Yes	
Energy Northwest - Columbia	Yes	
Electric Reliability Council of Texas, Inc.	Yes	
		R2 and R3 appear redundant.
Progress Energy		
Los Angeles Department of Water and Power		
Texas Reliability Entity		
ReliabilityFirst		
NRECA		
Entergy Services		
Thompson Coburn LLP on behalf of Miss. Delta Energy Agency		

Organization	Yes or No	Question 2 Comment
Southwestern Power Administration		

3. The DSR SDT revised reporting times for many events listed in Attachment 1 from one hour to 24 hours. Do you agree with these revisions? If not, please explain in the comment area below.

Summary Consideration: The DSR SDT appreciates the industry comments on the difficulty associated with reporting events that impact reliability. However, the SDT desires to point out that it is not the objective of this standard to provide an analysis of the event; but to provide the known facts of the events at the reporting threshold of onehour or 24hours depending upon the type of event. The SDT worked with the DOE and the NERC EAWG to develop reporting timelines consistent between the parties in an effort to promote consistency and uniformity.

The SDT has not established any requirement for a final or follow up report. The obligation is to report the facts known at the time. Once the report has been provided to the parties identified in the Operating Plan, no further action is required. All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:

> **"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."**

For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report, and is consistent with current in-force standard EOP-004-1.

Organization	Yes or No	Question 3 Comment
Ameren Services	Negative	(6)By our count there are still six of the nineteen events listed with a one hour reporting requirement and the rest are all within 24 hour after the occurrence (or recognition of the event). This in our opinion, is reporting in real-time, which is against one of the key concepts listed in the background section:"The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of

Organization	Yes or No	Question 3 Comment
		standards). The proposed standard deals exclusively with after-the-fact reporting." *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.* (7)We believe the earliest preliminary report required in this standard should at the close of the next business day. Operating Entities, such as the RC, BA, TOP, GOP, DP, and LSE should not be burdened with unnecessary after-the-fact reporting while they are addressing real-time operating conditions. Entities should have the ability to allow their support staff to perform this function during the next business day as needed. We acknowledge it would not be an undue burden to cc: NERC on other required governmental reports with shorter reporting timeframes, but NERC should not expand on this practice. *No preliminary report is required within the revised standard. Also, timelines have been revised (Please see response to item (6) above).* (8)We agree with the extension in reporting times for events that now have 24 hours of reporting time. As a GO there are still too many potential events that still require a 1 hour reporting time that is impractical, unrealistic and could lead to inappropriate escalation of normal failures. For example, the sudden loss of several control room display screens for a BES generator at 2 AM in the morning, with only 1 hour to report something, might be mistakenly interpreted as a cyber-attack. The reality is

Organization	Yes or No	Question 3 Comment
		most likely something far more mundane such as the unexpected failure of an instrument transformer, critical circuit board, etc. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.* (9) The "EOP-004 Attachment 1: Events Table" is quite lengthy and written in a manner that can be quite subjective in interpretation when determining if an event is reportable. We believe this table should be clear and unambiguous for consistent and repeatable application by both reliability entities and a CEA. The table should be divided into sections such as: 9a) Events that affect the BES that are either clearly sabotage or suspected sabotage after review by an entity's security department and local/state/federal law enforcement.(b) Events that pose a risk to the BES and that clearly reach a defined threshold, such as load loss, generation loss, public appeal, EEAs, etc. that entities are required to report by the end of the next business day.(c) Other events that may prove valuable for lessons learned, but are less definitive than required reporting events. These events should be reported voluntarily and not be subject to a CEA for non-reporting.(d)Events identified through other means outside of entity reporting, but due to their nature, could benefit the industry by an event report with lessons learned. Requests to report and perform analysis on these type of events should be vetted through a ERO/Functional Entity process to ensure resources provided to this effort have an effective reliability benefit.

Organization	Yes or No	Question 3 Comment
		The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows: • *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* • *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.* *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* (10)Any event reporting shall not in any manner replace or inhibit an Entity's responsibility to coordinate with other Reliability Entities (such as the RC, TOP, BA, GOP as appropriate) as required by other Standards, and good utility practice to operate the electric system in a safe and reliable manner. *The DSR SDT agrees and believes the revised reporting timelines support that concept.* (11) The 1 hour reporting maximum time limit for all GO events in Attachment 1 should be lengthened to something reasonable - at least 24 hours. Operators in our energy centers are well-trained and if they have good reason to suspect an event

Organization	Yes or No	Question 3 Comment
		that might have serious impact on the BES will contact the TOP quickly. However, constantly reporting events that turn out to have no serious BES impact and were only reported for fear of a violation or self-report will quickly result in a cry wolf syndrome and a great waste of resources and risk to the GO and the BES. The risk to the GO will be potential fines, and the risk to the BES will be ignoring events that truly have an impact of the BES. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.* (12)The 2nd and 3rd Events on Attachment 1 should be reworded so they do not use terms that may have been deleted from the NERC Glossary by the time FERC approves this Standard. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* (13) The terms "destruction" and "damage" are key to identifying reportable events. Neither has been defined in the Standard. The term destruction is usually defined as 100% unusable. However, the term damage can be anywhere from 1% to 99%

Organization	Yes or No	Question 3 Comment
		unusable and take anywhere from 5 minutes to 5 months to repair. How will we know what the SDT intended, or an auditor will expect, without additional information? *The 'Damage or Destruction' event category has been revised to say ' ...to a Facility', (a defined term) and thresholds have be modified to provide clarity.* *The DSR SDT used the defined term "Facility" to add clarity for several events listed in Attachment 1. A Facility is defined as:* *"A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"* *The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.* (14)We also do not understand why "destruction of BES equipment" (first item Attachment 1, first page) must be reported < 1 hour, but "system separation (islanding) > 100 MW" (Attachment 1, page 3) does not need to be reported for 24 hours. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the*

Organization	Yes or No	Question 3 Comment
		incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. (15)The first 2 Events in Attachment 1 list criteria Threshold for Reporting as "...operational error, equipment failure, external cause, or intentional or unintentional human action." The term "intentional or unintentional human action" appears to cover "operational error" so these terms appear redundant and create risk of misreporting. Can this be clarified? *The second event has been deleted and the language has been clarified in the 'Threshold for Reporting' column in the 'Damage or Destruction' event category. The updated Threshold for Reporting now reads as:* *"Damage or destruction of a Facility that:* • *Affects an IROL (per FAC-014)* *OR* • *Results in the need for actions to avoid an Adverse Reliability Impact* *OR* • *Results from intentional human action."* (16)The footnote of the first page of Attachment 1 includes the explanation "...ii) Significantly affects the reliability margin of the system..." However, the GO is prevented from seeing the system and has no idea what BES equipment can affect the reliability margin of the system. Can this be clarified by the SDT? *The footnote has been deleted and relevant information moved to the 'Threshold for Reporting column in the 'Damage or Destruction' event category.* (17) The use of the term "BES equipment" is problematic for a GO. NERC Team 2010-

Organization	Yes or No	Question 3 Comment
		17 (BES Definition) has told the industry its next work phase will include identify *The term "BES equipment" is no longer used. The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity.* *The DSR SDT used the defined term "Facility" to add clarity for several events listed in Attachment 1. A Facility is defined as:* *"A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"* *The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.*
Response: Thank you for your comment. Please see response above.		
Beaches Energy Services, City of Green Cove Springs	Negative	3. Att. 1, going from 1 to 24 hrs: The times don't seem aggressive enough for some of the Events related to generation capacity shortages, e.g., we would think public appeal, system wide voltage reduction and manual firm load shedding ought to be within an hour. These are indicators that the BES is "on the edge" and to help BES reliability, communication of this status is important to Interconnection-wide reliability. *This standard concerns after-the-fact reporting. It is assumed that Responsible Entities will make appropriate real-time notifications as per other applicable standards, operating agreements, and good utility practice. This standard does not preclude a Responsible Entity from reporting more quickly than required by Attachment 1.*

Organization	Yes or No	Question 3 Comment
		4. The Rules of Procedure language for data retention (first paragraph of the Evidence Retention section) should not be included in the standard, but instead referred to within the standard (e.g., "Refer to Rules of Procedure, Appendix 4C: Compliance Monitoring and Enforcement Program, Section 3.1.4.2 for more retention requirements") so that changes to the RoP do not necessitate changes to the standard. *The DSR SDT believes that although the evidence retention language is the same as the current RoP, it is not specifically linked, so changes to the RoP will not necessitate changes to the standard.* In R4, it might be worth clarifying that, in this case, implementation of the plan for an event that does not meet the criteria of Attachment 1 and going beyond the requirements R2 and R3 could be used as evidence. Consider adding a phrase as such to M4, or a descriptive footnote that in this case, "actual event" may not be limited to those in Attachment 1. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1. "* Comments to Attachment 1 table: On "Damage or destruction of Critical Asset" and "... Critical Cyber Asset", Version 5 of the CIP standards is moving away from the

Organization	Yes or No	Question 3 Comment
		binary critical/non-critical paradigm to a high/medium/low risk paradigm. Suggest adding description that if version 5 is approved by FERC, that "critical" would be replaced with "high or medium risk", or include changing this standard to the scope of the CIP SDT, or consider posting multiple versions of this standard depending on the outcome of CIP v5 in a similar fashion to how FAC-003 was posted as part of the GO/TO effort of Project 2010-07. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* On "forced intrusion", the phrase "at BES facility" is open to interpretation as "BES Facility" (e.g., controversy surrounding CAN-0016) which would exclude control centers and other critical/high/medium cyber system Physical Security Perimeters (PSPs). We suggest changing this to "BES Facility or the PSP or Defined Physical Boundary of critical/high/medium cyber assets". This change would cause a change to the applicability of this reportable event to coincide with CIP standard applicability. On "Risk to BES equipment", that phrase is open to too wide a range of interpretation; we suggest adding the word "imminent" in front of it, i.e., "Imminent risk to BES equipment". For instance, heavy thermal loading puts equipment at risk, but not imminent risk. Also, "non-environmental" used as the threshold criteria is ambiguous. For instance, the example in the footnote, if the BES equipment is near railroad tracks, then trains getting derailed can be interpreted as part of that BES equipment's "environment", defined in Webster's as "the circumstances, objects, or conditions by which one is surrounded". It seems that the SDT really means "non-weather related", or "Not risks due to Acts of Nature". *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen*

Organization	Yes or No	Question 3 Comment
		because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples. On "public appeal", in the threshold, the descriptor "each" should be deleted, e.g., if a single event causes an entity to be short of capacity, do you really want that entity reporting each time they issue an appeal via different types of media, e.g., radio, TV, etc., or for a repeat appeal every several minutes for the same event? *To clarify your point, the threshold has been changed to 'Public appeal or load reduction event'.* Should LSE be an applicable entity to "loss of firm load"? As proposed, the DP is but the LSE is not. In an RTO market, will a DP know what is firm and what is non-firm load? Suggest eliminating DP from the applicability of "system separation". The system separation we care about is separation of one part of the BES from another which would not involve a DP. *The DSR SDT believes the current applicability is correct and the threshold provides sufficient discrimination to drive the proper Applicable Entities to report.* On "Unplanned Control Center Evacuation", CIP v5 might add GOP to the applicability, another reason to add revision of EOP-004-2 to the scope of the CIP v5 drafting team, or in other ways coordinate this SDT with that SDT. Consider posting a couple of versions of the standard depending on the outcome of CIP v5 in a similar fashion to the multiple versions of FAC-003 posted with the GO/TO effort of Project 2010-07. *The DSR SDT believes the current applicability is correct. The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed*

Organization	Yes or No	Question 3 Comment
		from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds. Note that EOP-008-0 is only Applicable to Balancing Authorities, Transmission Operators and Reliability Coordinators, this is the basis for the "Entity with reporting Responsibilities" and reads as" "Each RC, BA, TOP that experiences the event".
Response: Thank you for your comment. Please see response above.		
Arkansas Electric Cooperative Corporation	Negative	AECC appreciates the efforts of the SDT to address our comments from the previous posting and feels the Standards have shown great improvement in the current posting. Our negative vote stems from concerns around the 1 hour reporting requirements for events having no size thresholds and ambiguity for external entity reporting in R1.3. Please refer to the comments submitted by the SPP Standards Review Group. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"…direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 3 Comment
PowerSouth Energy Cooperative	Negative	Attachment 1 needs to be eliminated. It is confusing to operators and doesn't enhance the reliability of the BES. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.*
Response: Thank you for your comment. Please see response above.		
Clark Public Utilities	Negative	Attachment 1 provides confusion not clarification. Just use the OE-417 reporting form for any and all events identified in that form for any one-hour or six-hour reporting. Utilities are required by law to provide the DOE notification and the SDT has just confused the situation by attempting (as it appears) to rename the one-hour reporting events. In some instances, Attachment 1 contradicts the DOE reporting. Public appeals for load reduction are required within 24 hours (according to the Events Table) but OE-417 requires such pubic appeals to be reported within one

Organization	Yes or No	Question 3 Comment
		hour. Clark recommends the Events Table show first the one hour reporting of OE-417, then the six hour reporting of OE-417, and finally any additional reporting that is desired but not reportable to DOE. This will help in not confusing seemingly related events. The table should indicate which form is to be used and should mandate Form OE-417 for all DOE reportable events and the Attachment 2: Event Reporting Form for all reportable events not subject to the DOE reporting requirements. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.* Clark questions whether the event labeled Forced Intrusion really needs to be reported in one hour. It can take several hours to determine if a forced entry actually occurred. Clark is also unsure if reporting forced intrusions at these facilities (if no other disturbance occurs) will provide any information useful in preventing system disturbances but believes this event should be changed to a 24 hour notification.

Organization	Yes or No	Question 3 Comment
		'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. The event labeled Detection of a reportable Cyber Security Incident should have the Entity with Reporting Responsibility changed to the following: "Applicable Entities under CIP-008." The Threshold for Reporting on this event is based on the criteria in CIP-008. If an entity is not an applicable entity under CIP-008, it should not have a reporting requirement based on CIP-008 that appears in EOP-004. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.*
Response: Thank you for your comment. Please see response above.		
City of Farmington	Negative	Attachment 1: BES equipment is too vague - consider changing to BES facility and including that reduces the reliability of the BES in the footnote. Is the footnote an and or an or? *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity.* *The DSR SDT used the defined term "Facility" to add clarity for several events listed in Attachment 1. A Facility is defined as:*

Organization	Yes or No	Question 3 Comment
		"A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)" *The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.* Attachment 1: Version 5 of CIP Requirements the use of the terms Critical Asset and Critical Cyber Asset. The drafting team should consider revising the table to be flexible so it will not require modification when new versions of CIP become effective. Clarify if Damage or Destruction is physical damage (aka - cyber incidents would be part of CIP-008 covered separately in Attachment 1.) *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Attachment 1: Unplanned Control Center evacuation - remove "potential" from the reporting responsibility Attachment 1: *The 'potential' language has been removed. The threshold for Reporting now reads as: "Each RC, BA, TOP that experiences the event".* SOL Tv - is not defined. *The SOL Violation (WECC only) event has been revised to remove Tv and replace it with "30 minutes" to be consistent with TOP-007-WECC requirements. The event has*

Organization	Yes or No	Question 3 Comment
		also been revised to indicate an SOL associated with a Major WECC transfer path. Attachment 2 - 3: change to, "Did the event originate in your system?" The requirement only requires reporting for Events - not potential events. This implies if there is potential for an event to occur, the entity should report (potential of a public appeal or potential to shed firm load) *The 'actual or potential' language has been removed.* Attachment 2 4: "Damage or Destruction to BES equipment" should be "Destruction of BES Equipment" like it is in Attachment 1 and "forced intrusion risk to BES equipment" remove "risk" *The 'Damage or Destruction' event category has been revised to say '...to a Facility', (a defined term) and thresholds have be modified to provide clarity. Also, the reporting timeline is now 24 hours.* *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.* The OE-417 requires several of the events listed in Attachment 1 be reported within 1 hour. FEUS recommends the drafting team review the events and the OE-417 form and align the reporting window requirements. For example, public appeals, load shedding, and system separation have a 1 hour requirement in OE-417. *OE-417, as well as, the EAWG's requirements were considered in creating Attachment*

Organization	Yes or No	Question 3 Comment
		1, but there remain differences for the following reasons: • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.*
Response: Thank you for your comment. Please see response above.		
Wisconsin Public Service Corp.	Negative	EOP-004 Attachment 1 states: That any Damage or destruction of a Critical Cyber Asset per CIP-002 Applicable Entities under CIP-002 Through intentional or unintentional human action. Requires reporting in 1 hour of recognition of event. This is too low of a threshold for reporting. Unintentional damage could be caused by an individual spilling coffee on a laptop. Hardly the item for a report. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 3 Comment
ACES Power Marketing, Hoosier Energy Rural Electric Cooperative, Inc., Sunflower Electric Power Corporation, Great River Energy	Negative	For many of the events listed in Attachment 1, there would be duplicate reporting the way it is written right now. For example, in the case of a fire in a substation (Destruction of BES equipment), the RC, BA, TO, TOP and perhaps the GO and GOP could all experience the event and each would have to report on it. This seems quite excessive and redundant. We recommend eliminating this duplicate reporting. *The DSR SDT has tried to minimize duplicative reporting, but recognizes there may be events that trigger more than one report. The current applicability ensures an event that could affect just one of the entities with reporting responsibility isn't missed.*
Response: Thank you for your comment. Please see response above.		
Consumers Energy	Negative	Forced intrusion needs to be specifically defined. A 1-hour report requirement is not necessary but for critical events that would have wide-ranging impact. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*

Organization	Yes or No	Question 3 Comment
		Requirements 2 and 3 should be combined into a single requirement. *The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."*
Response: Thank you for your comment. Please see response above.		
MidAmerican Energy Co.	Negative	MidAmerican Energy believes Attachment 1 expands the scope of what must be reported beyond what is required by FERC directives and beyond what is needed to improve security of the BES. Based on our understanding of Attachment 1, the category of "damage or destruction of a critical cyber asset" will likely result in hundreds or thousands of small equipment failures being reported to NERC and DOE, with no improvement to security. For example, hard drive failures, server failures, PLC failures and relay failures could all meet the criteria of "damage or destruction of a critical cyber asset." which would be required reporting in 1 hour. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat*

Organization	Yes or No	Question 3 Comment
		that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred. EOP-004-2 needs to clearly state that initial reports can be made by a phone call, email or another method, in accordance with paragraph 674 of FERC Order 706. MidAmerican recommends replacing Attachment 1 and Attachment 2 with the categories and timeframes that are listed in OE-417. This eliminates confusion between government requirements in OE-417 and NERC standards. *Attachment 1 provides the flexibility to make a verbal report. The header of Attachment 1 states:* *"NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per R1 and provide as much information as is available at the time of the notification. Reports to the ERO should be submitted to one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422."* *Attachment 2 provides the flexibility to make a verbal report. The header of Attachment 2 states:* *"This form is to be used to report events. The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Reports to the ERO should be submitted via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422."* *OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs;*

Organization	Yes or No	Question 3 Comment
		accommodation of other reporting obligations was considered as an opportunity not a 'must-have' • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.*
Response: Thank you for your comment. Please see response above.		
MidAmerican Energy Co.	Negative	MidAmerican Energy believes Attachment 1 expands the scope of what must be reported beyond what is required by FERC directives and beyond what is needed to improve security of the BES. EOP-004-2 needs to clearly state that initial reports can be made by a phone call, email or another method, in accordance with paragraph 674 of FERC Order 706. MidAmerican recommends replacing Attachment 1 and Attachment 2 with the categories and timeframes that are listed in OE-417. This eliminates confusion between government requirements in OE-417 and NERC standards. *Attachment 1 provides the flexibility to make a verbal report. The header of Attachment 1 states:* *"NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible*

Organization	Yes or No	Question 3 Comment
		Entity shall notify parties per R1 and provide as much information as is available at the time of the notification. Reports to the ERO should be submitted to one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422." *Attachment 2 provides the flexibility to make a verbal report. The header of Attachment 2 states:* *"This form is to be used to report events. The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Reports to the ERO should be submitted via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422."* *OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.*

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comment. Please see response above.		
Seattle City Light	Negative	Overarching Concern related to EOP-004-2 draft: The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes, as well as the CIP standards Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definitions of a BES element could change significantly and Critical Assets may no longer exist. As it relates to the proposed reporting criteria, it is debatable as to whether or not the destruction of, for example, one relay would be a reportable incident under this definition going forward given the current drafting team efforts. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Related to "Reportable Events" of Attachment 1: 1. A reportable event is stated as, "Risk to the BES", the threshold for reporting is, "From a non-environmental physical threat". This appears to be a catch-all event, and basically every other event in Attachment 1 should be reported because it is a risk to the BES. Due to the subjectivity of this event, suggest removing it from the list. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as*

Organization	Yes or No	Question 3 Comment
		a threat, not when it may have first occurred. 2. A reportable event is stated as, "Damage or destruction of Critical Asset per CIP-002". The term"Damage" would have to be defined in order for an entity to determine a threshold for what qualifies as "Damage" to a CA. One could argue that normal"Damage" can occur on a CA that is not necessary to report. There should also be caution here in adding CIP interpretation within this standard. Reporting Thresholds 1. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* The SDT made attempts to limit nuisance reporting related to copper thefts and so on which is supported. However a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could congest the reporting process with nuisance reporting and reviewing. An example is the "BES Emergency requiring manual firm load shedding of greater than or equal to 100 MW or the Loss of Firm load for = 15 Minutes that is greater than or equal to 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases these low thresholds represent reporting of minor wind events or other seasonal system issues on Local Network used to provide distribution service. *These thresholds reflect those used in the current in-force EOP-004-1, and haven't congested the reporting process to date.* Firm Demand 1. The use of Firm Demand in the context of the draft Standards could be used to describe commercial arrangements with a customer rather than a

Organization	Yes or No	Question 3 Comment
		reliability issue. Clarification of Firm Demand would be helpful *The DSR SDT did not use the words 'Firm Demand' anywhere in the proposed standard.*
Response: Thank you for your comment. Please see response above.		
Constellation Energy; Constellation Energy Commodities Group; Constellation Power Source Generation, Inc.	Negative	Please see the comments offered in the concurrent comment form. While Constellation is voting negative on this ballot, we recognize the progress made by the drafting team and find the proposal very close to acceptable. It should be noted that our negative vote is due to remaining concerns with the Attachment 1: Event Table categories language. In the comment form Constellation proposes revisions to both the requirement language and to the Event Table language; however, the Event Table language is the greater hurdle *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comment. Please see response above.		
Salt River Project	Negative	Related to "Reportable Events" of Attachment 1: 1. A reportable event is stated as, "Risk to the BES", the threshold for reporting is, "From a non-environmental physical threat". This as appears to be a catch-all event, and basically every other event should be reported because it is a risk to the BES. Due to the subjectivity of this event, suggest removing it from the list. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.* 2. A reportable event is stated as, "Damage or destruction of Critical Asset per CIP-002". The term "Damage" would have to be defined in order for an entity to determine a threshold for what qualifies as "Damage" to a CA. One could argue that normal "Damage" can occur on a CA that is not necessary to report. There should also be caution here in adding CIP interpretation within this standard. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.*
Response: Thank you for your comment. Please see response above.		
Southern California Edison Co.	Negative	SCE and WECC are in agreement on one key point (removing the requirement to

Organization	Yes or No	Question 3 Comment
		determine if an act was "sabotage"), however, I continue to believe SCE will find the one-hour reporting requirement difficult to manage. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		
City of Redding	Negative	The following comments are directed toward Attachment 1: We commend the SDT for properly addressing the sabotage issue. However, additional confusion is caused by introducing term "damage". As "damage" is not a defined term it would be beneficial for the drafting team to provide clarification for what is meant by "damage". *The 'Damage or Destruction' event category has been revised to say '...to a Facility', (a defined term) and thresholds have be modified to provide clarity. Also, the reporting timeline is now 24 hours.*

Organization	Yes or No	Question 3 Comment
		The threshold for reporting "Each public Appeal for load reduction" should clearly state the triggering is for the BES Emergency as routine "public appeal" for conservation could be considered a threshold for the report triggering.. *The DSR SDT believes the current language of the event category 'BES Emergency…' clearly excludes routine conservation requests. The Threshold for Reporting has been updated to read as: "Public appeal for load reduction event".* Regarding the SOL violations in Attachment 1 the SOL violations should only be those that affect the WECC Paths. *The SOL Violation (WECC only) event has been revised to remove Tv and replace it with "30 minutes" to be consistent with TOP-007-WECC requirements. The event is now "SOL for Major WECC Transfer Paths (WECC only)". .*
Response: Thank you for your comment. Please see response above.		
Avista Corp.	Negative	The VSLs associated with not reporting in an hour for some of the events (Destruction of BES Equipment) is too severe. Operators need to be able to deal with events and not worry about reporting until the system is secure. Back office personnel are only available 40-50 hours per week, so the reporting burden falls on the Operator. *The DSR SDT believes the VSL is appropriate for the only remaining 1 hour event.*
Response: Thank you for your comment. Please see response above.		
Avista Corp.	Negative	There is definitely a need to communicate and report out system events to NERC, RCs, and adjacent utilities. However, this new standard has gone too far with regards to reporting of certain events within a 1 hour timeframe and the associated VSLs for going beyond the hour time period. Operators need to be able to deal with the system events and not worry about reporting out for the "Destruction of BES

Organization	Yes or No	Question 3 Comment
		equipment" (first row in Attachment 1 -Reportable Events). Operators only have 40-50 hours out of 168 hours in a week where supporting personnel are also on shift, so this reporting burden will usually fall on the Operators not back office support. Again this is another example of the documentation requirements of a standard being more important than actually operating the system. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.* The "Destruction of BES equipment" event is too ambiguous and will lead to interpretations by auditors to determine violations. The ambiguity will also lead to the reporting of all BES equipment outages to avoid potential violations of the standard. It usually takes more than an hour to determine the cause and extent of an outage. *The 'Damage or Destruction' event category has been revised to say '...to a Facility', (a defined term) and thresholds have be modified to provide clarity. Also, the reporting timeline is now 24 hours.*

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comment. Please see response above.		
National Association of Regulatory Utility Commissioners	Negative	Therequirement that any event with the potential to impact reliability be reported is overly broad and requires more focus. *'Forced intrusion' and 'Risk to BES Equipment' (which this footnote referenced) have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		
Alameda Municipal Power, Salmon River Electric Cooperative	Negative	We feel that the drafting team has done an excellent job of providing clarify and reasonable reporting requirements to the right functional entity. We support the modifications but would like to have two additional minor modification in order to provide additional clarification to the Attachment I Event Table. We suggest the following clarifications: For the Event: BES Emergency resulting in automatic firm load shedding Modify the Entity with Reporting Responsibility to: Each DP or TOP that experiences the automatic load shedding within their respective distribution serving or Transmission Operating area. *The DSR SDT believes the current language is sufficient and cannot envision how a BA, TOP, or DP could 'experience the automatic load shedding' if it didn't take place in its balancing, transmission operating, or distribution serving area.*

Organization	Yes or No	Question 3 Comment
		For the Event: Loss of Firm load for = 15 Minutes Modify the Entity with Reporting Responsibility to: Each BA, TOP, DP that experiences the loss of firm load within their respective balancing, Transmission operating, or distribution serving area. With these modifications or similar modifications we fully support the proposed Standard. *The DSR SDT believes the current language is sufficient and cannot envision how a BA, TOP, or DP could 'experience the loss of firm load' if it didn't take place in its balancing, transmission operating, or distribution serving area.*
Response: Thank you for your comment. Please see response above.		
Orange and Rockland Utilities, Inc.	No	o Generally speaking the SDT should work with the NERC team drafting the Events Analysis Process (EAP) to ensure that the reporting events align and use the same descriptive language. o EOP-004 should use the exact same events as OE-417. These could be considered a baseline set of reportable events. If the SDT believes that there is justification to add additional reporting events beyond those identified in OE-417, then the event table could be expanded. o If the list of reportable events is expanded beyond the OE-417 event list, the supplemental events should be the same in both EOP-004-2 and in the EAP Categories 1 through 5. *OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may*

Organization	Yes or No	Question 3 Comment
		trigger further information requests from EAWG as necessary *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004.* o It is not clear what the difference is between a footnote and "Threshold for Reporting". All information should be included in the body of the table, there should be no footnotes. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* o Event: "Risk to BES equipment" should be deleted. This is too vague and subjective. Will result in many "prove the negative" situations.' *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.* o Event: "Destruction of BES equipment" is again too vague. The footnote refers to equipment being "damaged or destroyed". There is a major difference between

Organization	Yes or No	Question 3 Comment
		destruction and damage. *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity.* o Event: "Damage or Destruction of a Critical Asset or Critical Cyber Asset" should be deleted. Disclosure policies regarding sensitive information could limit an entity's ability to report. Unintentional damage to a CCA does not warrant a report. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* o Event: "BES Emergency requiring public appeal for load reduction" should be modified to note that this does not apply to routine requests for customer conservation during high load periods *The DSR SDT believes the current language of the event category 'BES Emergency…' clearly excludes routine conservation requests.*
Response: Thank you for your comment. Please see response above.		
Ameren	No	(1)By our count there are still six of the nineteen events listed with a one hour reporting requirement and the rest are all within 24 hour after the occurrence (or recognition of the event). This in our opinion, is reporting in real-time, which is against one of the key concepts listed in the background section:"The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of

Organization	Yes or No	Question 3 Comment
		standards). The proposed standard deals exclusively with after-the-fact reporting." *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.* (2)We believe the earliest preliminary report required in this standard should at the close of the next business day. Operating Entities, such as the RC, BA, TOP, GOP, DP, and LSE should not be burdened with unnecessary after-the-fact reporting while they are addressing real-time operating conditions. Entities should have the ability to allow their support staff to perform this function during the next business day as needed. We acknowledge it would not be an undue burden to cc: NERC on other required governmental reports with shorter reporting timeframes, but NERC should not expand on this practice. *No preliminary report is required within the revised standard.* (3)We agree with the extension in reporting times for events that now have 24 hours of reporting time. As a GO there are still too many potential events that still require

Organization	Yes or No	Question 3 Comment
		a 1 hour reporting time that is impractical, unrealistic and could lead to inappropriate escalation of normal failures. For example, the sudden loss of several control room display screens for a BES generator at 2 AM in the morning, with only 1 hour to report something, might be mistakenly interpreted as a cyber-attack. The reality is most likely something far more mundane such as the unexpected failure of an instrument transformer, critical circuit board, etc. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		
Duke Energy	No	All events in Attachment 1 should have reporting times of no less than 24 hours. As stated on page 6 of the current draft of the standard: "The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting."We maintain

Organization	Yes or No	Question 3 Comment
		that a report which is required to be made within one hour after an event is, in fact, a real time report. In the first hour or even several hours after an event the operator may appropriately still be totally committed to restoring service or returning to a stable bulk power system state, and should not stop that recovery activity in order to make this "after-the-fact" report. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		
American Public Power Association	No	APPA echoes the comments made by Central Lincoln: We do not believe the SDT has adequately addressed the FERC Order to "Consider whether separate, less burdensome requirements for smaller entities may be appropriate." The one and 24 hour reporting requirements continue to be burdensome to the smaller entities that do not maintain 24/7 dispatch centers. The one hour reporting requirement means that an untimely "recognition" starts the clock and reporting will become a higher

Organization	Yes or No	Question 3 Comment
		priority than restoration. The note regarding adverse conditions does not help unless we were to consider the very lack of 24/7 dispatch to be such a condition. APPA recommends the SDT evaluate a less burdensome requirement for smaller entities with reporting requirements in Attachment 1. This exception needs to address the fact that not all entities have 24 hour 7 day a week operating personnel. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.* *The DSR SDT believes that reliability is best served by imposing reporting criteria based on impact to the BES rather than an arbitrary entity size threshold. With these latest revisions, all the proposed event categories provide thresholds that will capture the appropriate entities and provide a manageable timeframe.* However, APPA cautions the SDT that changes to this standard may expose entities to reporting violations on DOE-OE-417 which imposes civil and criminal penalties on reporting events to the Department of Energy. APPA recommends that the SDT reach out to DOE for clarification of reporting requirements for DOE-OE-417 for small entities, asking DOE to change their reporting requirement to match EOP-004-2. If

Organization	Yes or No	Question 3 Comment
		DOE cannot change their reporting requirement the SDT should provide an explanation in the guidance section of Reliability Standard EOP-004-2 that addresses these competing FERC/DOE directives. *OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.*
Response: Thank you for your comment. Please see response above.		
BC Hydro	No	As an event would be verbally reported to the RC, all the one hour requirements to submit a written report should be moved from one hour to 24 hours. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact*

Organization	Yes or No	Question 3 Comment
		appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…" *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		
Bonneville Power Administration	No	BPA believes that the first three elements in Attachment 1 are too generic and should be with only the intentional human criterion. The suspicious device needs to be determined as a threat (and not left behind tools) before requiring a report. *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity. These thresholds include intentional human action as well as impact-based for those cases when cause isn't known. The determination of a threat as you suggest is now part of the revised event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.*

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comment. Please see response above.		
CenterPoint Energy	No	CenterPoint Energy agrees with the revision that allows more time for reporting some events; however, some 1 hour requirements remain. The Company does not agree with this timeframe for any event. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment Please see response above.		
Consolidated Edison Co. of NY, Inc.	No	Comments: We have a number of comments on Attachment 1 and will make them here: o Generally speaking the SDT should work with the NERC team drafting the Events Analysis Process (EAP) to ensure that the reporting events align and use the same descriptive language. o EOP-004 should use the exact same events as OE-417. These could be considered a baseline set of reportable events. If the SDT believes that there is justification to add additional reporting events beyond those identified in OE-417, then the event table could be expanded. o If the list of reportable events

Organization	Yes or No	Question 3 Comment
		is expanded beyond the OE-417 event list, the supplemental events should be the same in both EOP-004-2 and in the EAP Categories 1 through 5. *OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004.* o It is not clear what the difference is between a footnote and "Threshold for Reporting". All information should be included in the body of the table, there should be no footnotes. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'Any physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* o Event: "Risk to BES equipment" should be deleted. This is too vague and subjective. Will result in many "prove the negative" situations.'

Organization	Yes or No	Question 3 Comment
		'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. o Event: "Destruction of BES equipment" is again too vague. The footnote refers to equipment being "damaged or destroyed". There is a major difference between destruction and damage. *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity.* o Event: "Damage or Destruction of a Critical Asset or Critical Cyber Asset" should be deleted. Disclosure policies regarding sensitive information could limit an entity's ability to report. Unintentional damage to a CCA does not warrant a report. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* o Event: "BES Emergency requiring public appeal for load reduction" should be modified to note that this does not apply to routine requests for customer conservation during high load periods.

Organization	Yes or No	Question 3 Comment
		The DSR SDT believes the current language 'BES Emergency…' clearly excludes routine conservation requests.
Response: Thank you for your comment. Please see response above.		
Electric Reliability Council of Texas, Inc.	No	Destruction of BES equipment: 1. Request that the term "destruction" be clarified. *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity.* Damage or destruction of Critical Asset per CIP-002: 1. Request that the terms "damage" and "destruction" be clarified. 2. Is the expectation that an entity report each individual device or system equipment failure or each mistake made by someone administering a system? *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* 3. Request that "initial indication of the event" be changed to "confirmation of the event". Event monitoring and management systems may receive many events that are determined to be harmless and put the entity at no risk. This can only be determined after analysis of the associated events is performed. *The 'initial indication of the event' is no longer part of the threshold for 'Damage or Destruction of a Facility'* Risk to BES equipment: Request that the terms "risk" be clarified. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'.*

Organization	Yes or No	Question 3 Comment
		Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.
Response: Thank you for your comment. Please see response above.		
Exelon	No	Due to the size of the service territories in ComEd and PECO it's difficult to get to some of the stations within in an hour to analyze an event which causes concern with the 1 hour criteria. It is conceivable that the evaluation of an event could take longer then one hour to determine if it is reportable. Exelon cannot support this version of the standard until the 1 hour reporting criteria is clarified so that the reporting requirements are reasonable and obtainable. Exelon has concerns about the existing 1 hour reporting requirements and feels that additional guidance and verbiage is required for clarification. We would like a better understanding when the 1 hour clock starts please consider using the following clarifying statement, in the statements that read, "recognition of events" please consider replacing the word "recognition" with the word "confirmation" as in a "confirmed event" *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force*

Organization	Yes or No	Question 3 Comment
		standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.
Response: Thank you for your comment. Please see response above.		
Energy Northwest - Columbia	No	Energy Northwest - Columbia (ENWC) has concerns about the existing 1 hour reporting requirements and feels that additional guidance and verbiage is required for clarification. ENWC would like the word "recognition" in the statement that reads, "recognition of events," be replaced by "confirmation" as in "confirmed event."Also, we would like clarification as to when the 1 hour clock starts. Please consider changing recognition in "within 1 hour of recognition of event" and incorporating in "confirmation." *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 3 Comment
Indiana Municipal Power Agency	No	IMPA believes that some of the times may not be aggressive enought that are related to generation capacity shortages. *This standard concerns after-the-fact reporting. It is assumed that Responsible Entities will make appropriate real-time notifications as per other applicable standards, operating agreements, and good utility practice. This standard does not preclude a Responsible Entity from reporting more quickly than required by Attachment 1.* In addition, IMPA believes clarity needs to be added when saying within 1 hour of recognition of event. For example, A fence cutting may not be discovered for days at a remote substation and then a determination has to be made if it was "forced intrusion" - Does that one hour apply once the determination is made that is was "forced intrusion" or from the time the discovery was made? Some of the 1 hour time limits can be expanded to allow for more time, such as forced intrusion, destruction of BES equipment, Risk to BES equipment, etc. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'Any physical threat that could impact the operability of a Facility'. Timelines start at the moment the Responsible Entity determines the event represents a threat, not when it first occurred.*
Response: Thank you for your comment. Please see response above.		
Luminant Power	No	Luminant agrees with the changes the SDT made, however, the timeline should be modified to put higher priority activities before reporting requirements. The SDT should consider allowing entities the ability to put the safety of personnel, safety of the equipment, and possibly the stabilization of BES equipment efforts prior to initiating the one hour reporting timeline. Reporting requirements should not be prioritized above these important activities. The requirement to report one hour after the recognition of such an event may not be sufficient in all instances. Entities

Organization	Yes or No	Question 3 Comment
		should not have a potential violation as a result of putting these priority issues first and not meeting the one hour reporting timeline. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *Actions taken to maintain the reliability of the BES in real-time always take precedence over reporting. The revised thresholds should ensure there is no perverse driver to act differently.*
Response: Thank you for your comment. Please see response above.		
MidAmerican Energy	No	MidAmerican Energy agrees with the direction of consolidating CIP-001, EOP-004 and portions of CIP-008. However, we have concerns with some of the events included in Attachment 1 and reporting timelines. EOP-004-2 needs to clearly state that initial reports can be made by a phone call, email or another method, in accordance with paragraph 674 of FERC Order 706. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*

Organization	Yes or No	Question 3 Comment
		MidAmerican Energy believes draft Attachment 1 expands the scope of what must be reported beyond what is required by FERC directives and beyond what is needed to improve security of the BES. Based on our understanding of Attachment 1, the category of "damage or destruction of a critical cyber asset" will result in hundreds or thousands of small equipment failures being reported to NERC and DOE, with no improvement to security. For example, hard drive failures, server failures, PLC failures and relay failures could all meet the criteria of "damage or destruction of a critical cyber asset." *The DSR SDT agrees and the 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* We recommend replacing Attachment 1 and Attachment 2 with the categories and timeframes that are listed in OE-417. This eliminates confusion between government requirements in OE-417 and NERC standards. *OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may*

Organization	Yes or No	Question 3 Comment
		trigger further information requests from EAWG as necessary *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004.* Reporting timelines and reporting formFERC Order 706, paragraph 676, directed NERC to require a responsible entity to "at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report." In paragraph 674, FERC stated that the Commission agrees that, in the "aftermath of a cyber attack, restoring the system is the utmost priority." They clarified: "the responsible entity does not need to initially send a full report of the incident...To report to appropriate government authorities and industry participants within one hour, it would be sufficient to simply communicate a preliminary report, including the time and nature of the incident and whatever useful preliminary information is available at the time. This could be accomplished by a phone call or another method." While FERC did not order completion of a full report within one hour in Order 706, the draft EOP-004 Attachment 1 appears to require submittal of formal reports within one hour for six of the categories, unless there have been "certain adverse conditions" (in which case, as much information as is available must be submitted at the time of notification). *It is assumed that Responsible Entities will make appropriate real-time notifications as per other applicable standards, operating agreements, and good utility practice. As stated above, all one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673. For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions, which would certainly include the aftermath of a cyber attack that had*

Organization	Yes or No	Question 3 Comment
		major impact on the BES. The Violation Severity Levels are extreme for late submittal of a report. For example, it would be a severe violation to submit a report more than three hours following an event for an event requiring reporting in one hour. *The DSR SDT believes the VSL is appropriate now that it only applies to the remaining 1 hour reportable event, which is the Reportable Cyber Event under CIP-008.* MidAmerican Energy suggests incorporating the language from FERC Order 706, paragraph 674, into the EOP-004 reporting requirement to allow preliminary reporting within one hour to be done through a phone call or another method to allow the responsible entity to focus on recovery and/or restoration, if needed.MidAmerican Energy agrees with the use of DOE OE-417 for submittal of the full report of incidents under EOP-004 and CIP-008. We would note there are two parts to this form -- Schedule 1-Alert Notice, and Schedule 2-Narrative Description. Since OE-417 already requires submittal of a final report that includes Schedule 2 within 48 hours of the event, MidAmerican Energy believes it is not necessary to include a timeline for completion of the final report within the EOP-004 standard. We would note that Schedule 2 has an estimated public reporting burden time of two hours so it is not realistic to expect Schedule 2 to be completed within one hour. Events included in Attachment 1:MidAmerican Energy believes draft Attachment 1 expands the scope of what must be reported beyond what is required by FERC directives and beyond what is needed to improve security of the BES. The categories listed in Attachment 1 with one-hour reporting timelines cause the greatest concern. None of these categories are listed in OE-417, and all but the last row would not be considered a Cyber Security Incident under CIP-008, unless there was malicious or suspicious intent. *All one hour reporting timelines have been changed to 24 hours with the exception of*

Organization	Yes or No	Question 3 Comment
		a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673: *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*
Response: Thank you for your comment. Please see response above.		
SERC OC Standards Review Group	No	No event should have a reporting time less than at the close of the next business day. Any reporting of an event that requires a less reporting time should only be to entities that can help mitigate an event such as an RC or other Reliability Entity. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 3 Comment
Southwestern Power Administration	No	One hour is not enough time to make these assessments for all of the six items in attachment 1. All timing requirements should be made the same in order to simplify the reporting process. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*
Response: Thank you for your comment. Please see response above.		
ITC	No	See comments to Question #4
Response: Thank you for your comment. See response to Question 4.		
Southern Company	No	Southern request clarification on one of the entries in Attachment 1. The concern is with the last row on page 21 of Draft 3. What is the basis for "Voltage deviations"? The Threshold is Â±10% sustained for â‰¥ 15 minutes. Is the voltage deviation based on the Voltage Schedule for that particular timeframe, or is it something else (pre-contingency voltage level, nominal voltage, etc.)? *A sustained voltage deviation of ± 10% on the BES is significant deviation and is indicative of a shortfall of reactive resources either pre- or post-contingency. The DSR SDT is indifferent to which of nominal, pre-contingency, or scheduled voltage, is used*

Organization	Yes or No	Question 3 Comment
		as the baseline, but for simplicity and to promote a common understanding suggest using nominal voltage. In addition, the second row of Attachment 1 lists "Damage or destruction of a Critical Cyber Asset per CIP-002" as a reportable event. The threshold includes "...intentional or unintentional human action" and gives us 1 hour to report. The term "damage" may be overly broad and, without definition, is not limited in any way. If a person mistypes a command and accidentally deletes a file, or renames something, or in any way changes anything on the CCA in error, then this could be considered "damage" and becomes a reportable event. The SDT should consider more thoroughly defining what is meant by "damage". Should it incorporate the idea that the essential functions that the CCA is performing must be adversely impacted? *The DSR SDT agrees and the 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Lastly, no event should have a reporting time shorter than at the close of the next business day. Any reporting of an event that requires a shorter reporting time should only be to entities that can help mitigate an event such as an RC or other Reliability Entity. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber*

Organization	Yes or No	Question 3 Comment
		security incident as soon as possible, but in any event, within one hour of the event…" *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*
Response: Thank you for your comment. Please see response above.		
FEUS	No	The OE-417 requires several of the events listed in Attachment 1 be reported within 1 hour. FEUS recommends the drafting team review the events and the OE-417 form and align the reporting window requirements. For example, public appeals, load shedding, and system seperation have a 1 hour requirement in OE-417. *OE-417 thresholds and reporting timelines were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America. Non-US Responsible Entities cannot be obligated to report in shorter timelines simply to make the two forms line up. The current in-force EOP-004 requires 24 hour reporting on the items you have identified and so does the latest version of EOP-004-2* • *NERC has no control over the criteria in OE-417, which can change at any time* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004.*

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comment. Please see response above.		
SPP Standards Review Group	No	The purpose of the reporting requirement should be clear either in the text of the requirements or through an explanation that is embodied in the language of the approved set of standards. This would be consistent with a "Results-based" architecture. What is lacking in the proposed language of this standard is recognition that registered entities differ in size and relevance of their impact on the Bulk Electric System. Also, events that are reportable differ in their impact on the registered entity. A "one-size fits all" approach to this standard may cause smaller entities with low impact on the grid to take extraordinary measures to meet the reporting/timing requirements and yet be too "loose" for larger more sophisticated and impacting entities to meet the same requirements. Therefore, we believe language of the standard must clearly state the intent that entities must provide reports in a manner consistent with their capabilities from a size/reliability impact perspective and from a communications availability perspective. Timing requirements should allow for differences and consider these variables.Also, we would suggest including language to specifically exclude situations where communications facilities may not be available for reporting. For example, in situations where communications facilities have been lost, initial reports would be due within 6 hours of the restoration of those communication facilities. *The DSR SDT has reviewed Attachment 1 and made revisions to Event types, used the NERC approved term 'Facility', and revised some of the language under 'Entity with Reporting Responsibility' to ensure that these reportable events correctly represent the relative impact to the BES. Also, all one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"*

Organization	Yes or No	Question 3 Comment
		For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. We would also suggest that Attachment 1 be broken into two distinct parts such that those events which must be reported within 1 hour standout from those events that have to be reported within 24 hours. *The DSR SDT agrees and has implemented your suggestion.*
Response: Thank you for your comment. Please see response above.		
Kansas City Power & Light	No	The reportable events listed in Attachment 1 can be categorized as events that have had a reliability impact and those events that could have a reliability impact. The listed events that could have a reliability impact should have a 24 hour reporting requirement and the events that have had a reliability impact are appropriate at a 1 hour reporting. The following events with a 1 hour report requirement are recommended to change to 24 hour: Forced Intrusion and Risk to BES Equipment. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*

Organization	Yes or No	Question 3 Comment
		In addition, the Attachment 1 Events Table is incomplete as many of the listed events are incomplete regarding reporting time requirements and event descriptions. *Attachment 1 has been revised to more clearly indicate reporting timelines and some of the event descriptions were changed to add clarity.* Also recommend removing (ii) from note 5 with event "Destruction of BES equipment" as this part of the note is already described in the event description and insinuates reporting of equipment losses that do not have a reliability impact. *This footnote has been deleted* The events, "Damage or destruction of Critical Asset per CIP-002" and "Damage or destruction of a Critical Cyber Asset per CIP-002", does not have sufficient clarity regarding what that represents. A note similar in nature to Note 5 for BES equipment is recommended. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.*
Response: Thank you for your comment. Please see response above.		
Los Angeles Department of Water and Power	No	The reporting time of within 1 hour of recognition for a "Forced Intrusion" (last event category on page 20 of Draft 3, dated October 25, 2011) when considered with the associated footnote "Report if you cannot reasonably determine likely motivation" is overly burdensome and unrealistic. What is "reasonably determine likely motivation" is too general and requires further clarity. For example, LADWP has numerous facilities with extensive perimeter fencing. There is a significant

Organization	Yes or No	Question 3 Comment
		difference between a forced intrusion like a hole or cut in a property line fence of a facility versus a forced intrusion at a control house. Often cuts in fences, after further investigation, are determined to be cases of minor vandalism. An investigation of this nature will take much more than the allotted hour. The NERC Design Team needs to develop difference levels for the term "Force Intrusion" that fit the magnitude of the event and provide for adequate time to determine if the event was only a case of minor vandalism or petty thief. The requirement, as currently written, would unnecessarily burden an entity in reporting events that after given more time to investigate would more than likely not have been a reportable event. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		
Northeast Power Coordinating Council	No	The SDT should work with the NERC team drafting the Events Analysis Process (EAP) to ensure that the reporting events align and use the same descriptive language.EOP-004 should use the exact same events as OE-417. These could be considered a baseline set of reportable events. If the SDT believes that there is justification to add additional reporting events beyond those identified in OE-417, then the event table could be expanded. If the list of reportable events is expanded beyond the OE-417 event list, the supplemental events should be the same in both EOP-004-2 and

Organization	Yes or No	Question 3 Comment
		in the EAP Categories 1 through 5. *OE-417 thresholds and reporting timelines were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America. Non-US Responsible Entities cannot be obligated to report in shorter timelines simply to make the two forms line up. The current in-force EOP-004 requires 24 hour reporting on the items you have identified and so does the latest version of EOP-004-2* • *NERC has no control over the criteria in OE-417, which can change at any time* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004.* It is not clear what the difference is between a footnote and "Threshold for Reporting". All information should be included in the body of the table, there should be no footnotes. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* Event: Risk to BES equipment should be deleted. This is too vague and subjective. This will result in many "prove the negative" situations. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new*

Organization	Yes or No	Question 3 Comment
		event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Event: Damage or Destruction of a Critical Asset or Critical Cyber Asset should be deleted. Disclosure policies regarding sensitive information could limit an entity's ability to report. Unintentional damage to a CCA does not warrant a report. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Event: BES Emergency requiring public appeal for load reduction should be modified to note that this does not apply to routine requests for customer conservation during high load periods. *The DSR SDT believes the current language of the event category 'BES Emergency…' clearly excludes routine conservation requests.*
Response: Thank you for your comment. Please see response above.		
Florida Municipal Power Agency	No	The times don't seem aggressive enough for some of the Events related to generation capacity shortages, e.g., we would think public appeal, system wide voltage reduction and manual firm load shedding ought to be within an hour. These are indicators that the BES is "on the edge" and to help BES reliability,

Organization	Yes or No	Question 3 Comment
		communication of this status is important to Interconnection-wide reliability. *This standard concerns after-the-fact reporting. It is assumed that Responsible Entities will make appropriate real-time notifications as per other applicable standards, operating agreements, and good utility practice. This standard does not preclude a Responsible Entity from reporting more quickly than required by Attachment 1.*
Response: Thank you for your comment. Please see response above.		
NorthWestern Energy	Affirmative	In Attachment 1 NorthWestern Eneergy does not agree with the Transmission loss event, the threshold for reporting is "Unintentional loss of Three or more Transmission Facilities (excluding successful automatic reclosing)." There are lots of instances where this can happen and not have any major impacts to the BES. This reporting requirement is stemming from the Event Analysis Reporting Requirements and in many instances does not constitute an emergency. *You are correct. This event is used as a trigger to the Events Analysis Process.* Also, in Attachment 1 it is not clear when the DOE OE-417 form MUST be submitted. It give an option to use this form or another form but does not state when it must be used - confusing. *For the purposes of EOP-004, Responsible Entities may use either Attachment 2 or OE-417. Submission of OE-417 to the DOE is mandatory for US entities and outside the scope of NERC. Giving you the option to submit OE-417 to NERC and your RC to satisfy EOP-004 is permitted as a matter of convenience so you don't have to submit two different forms for the same event.*
Response: Thank you for your comment. Please see response above.		
Rutherford EMC	Affirmative	The SDT should consider adding a clause in the standard exempting small DP/LSEs

Organization	Yes or No	Question 3 Comment
		from the standard if the DP/LSE annually reviews and approves that it owns no facilities or equipment creating an event as decribed in Attachment 1. *The DSR SDT believes that reliability is best served by imposing reporting criteria based on impact to the BES rather than an arbitrary entity size threshold. With these latest revisions, all the proposed event categories provide thresholds that will capture the appropriate entities and provide a manageable timeframe.*
Response: Thank you for your comment. Please see response above.		
Fort Pierce Utilities Authority	Affirmative	The triggering event "Detection of a reportable Cyber Security Incident" listed in Attachment 1 assigns essentially all utilities reporting responsibility. This is not in line its reporting threshold, which is an event meeting the criteria in CIP-008. Shouldn't the responsibility fall on only those responsible for compliance with CIP-008, version 3 or 4, as determined by CIP-002? The SDT should also give additional consideration to necessary provisions to make it align with the proposed CIP-008-5. *The 'Entity with Reporting Responsibility' has been changed to reflect your comment to 'Each Responsible Entity applicable under CIP-008 that experiences the Cyber Security Incident.*
Response: Thank you for your comment. Please see response above.		
Nebraska Public Power District	Yes	Although 24 hours is a vast improvement, one business day would make more sense for after the fact reporting. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber*

Organization	Yes or No	Question 3 Comment
		security incident as soon as possible, but in any event, within one hour of the event…" *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*
Response: Thank you for your comment. Please see response above.		
FirstEnergy	Yes	Although we agree with the timeframes for reporting, we have other concerns as listed in our response to Question 4.
Response: Thank you for your comment. Please see response to question 4.		
Intellibind	Yes	Does this reporting conflict with reporting for DOE, and Regions? If so, what reporting requirements will the entity be held accountable to? Managing multiple reporting requirements for the multiple agencies is very problematic for entities and this standard should resolve those reporting requirments, as well as reduce the reporting down to one form and one submission. Reporting to ESISAC should take care of all reporting by the company. NERC should route all reports to the DOE, and regions through this mechanism. *OE-417 thresholds and reporting timelines were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America. Non-US Responsible Entities cannot be obligated to report in shorter timelines simply to make the two forms line up. NERC has no control over the criteria in OE-417, which can change at any time*

Organization	Yes or No	Question 3 Comment
		In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. NERC cannot take on the statutory obligation of US entities to report to the DOE.
Response: Thank you for your comment. Please see response above.		
Dominion	Yes	Dominion appreciates the changes that have been made to increase the 1 hr reporting time to 24 hours.
Response: Thank you for your comment.		
APX Power Markets (NCR-11034)	Yes	In my opinion the remaining items with 1 hour reporting requirements will in most cases require the input of in-complete information, since you maybe aware of the outage/disturbance, but not aware of any reason for it. If that is acceptable just to get the intitial report that there was an outage/disturbance then we are OK. I believe it would help to have that clarifed in the EOP, or maybe a CAN can be created for that. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comment. Please see response above.		
Compliance & Responsbility Office	Yes	See comments in response to Question 4.
Response: Thank you for your comment. See response to Question 4.		
Lower Colorado River Authority	Yes	The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. EOP-004 has an "optional" Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify whether Registered Entities will still be required to submit both forms. Please also ensure there will not be duplication of efforts between the two reports. Although this is fairly minor, the clarification should be addressed. *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary.*
Response: Thank you for your comment. Please see response above.		
City of Austin dba Austin Energy	Yes	The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. EOP-004 has an "optional" Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify whether Registered Entities will still be required to submit both forms. Please also ensure there will not be duplication of efforts between the two reports. Although this is fairly minor, the clarification should be addressed. *Reports made under EOP-004 provide a minimum set of information, which may*

Organization	Yes or No	Question 3 Comment
		trigger further information requests from EAWG as necessary.
Response: Thank you for your comment. Please see response above.		
Public Utility District No. 1 of Snohomish County	Yes	The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. The EOP-004 has an "optional" Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify if both forms will still be required to be submitted. We also need to ensure that there won't be a duplication of efforts between the two reports. This is fairly minor, but the clarification need should be addressed. *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary.*
Response: Thank you for your comment. Please see response above.		
Seattle City Light	Yes	The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. The EOP-004 has an "optional" Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify if both forms will still be required to be submitted. We also need to ensure that there won't be a duplication of efforts between the two reports. This is fairly minor, but the clarification need should be addressed. *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 3 Comment
Salt River Project	Yes	The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the NERC Event Analysis process, but there is some duplication of efforts. EOP-004 has an "optional" Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify whether Registered Entities will still be required to submit both forms. Please also ensure there will not be duplication of efforts between the two reports. Although this is fairly minor, the clarification should be addressed. *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary.*
Response: Thank you for your comment. Please see response above.		
Constellation Energy on behalf of Baltimore Gas & Electric, Constellation Power Generation, Constellation Energy Commodities Group, Constellation Control and Dispatch, Constellation NewEnergy and Constellation Energy Nuclear Group.	Yes	We agree with the change to the reporting times in Attachment 1. While this is an improvement, other concerns with the language in the events table language remain. Please see additional details below:General items: o All submission instructions (column 4 in Events Table) should qualify the recognition of the event as "of recognition of event as a reportable event." *Column 4 has been deleted. The table headings now state that Responsible Entities must submit the report within X hours of recognition of event.* o Is the ES-ISAC the appropriate contact for the ERO given that these two entities are separate even though they are currently managed by NERC? *Yes. This is the current reporting contact and this is the advice that the DSR SDT team received from NERC.* In addition, are the phone numbers in the Attachment 1 NOTE accurate? Is it possible they will change in a different cycle than the standard?

Organization	Yes or No	Question 3 Comment
		Yes. The standard will require updating should the phone number change. Specific Event Language: o Destruction of BES Equipment, footnote: Footnote 1, item iii confuses the clarification added in items i. and ii. Footnote 1 should be modified to state BES equipment that (i) an entity knows will affect an IROL or has been notified the loss affects an IROL; (ii) significantly affects the reserve margin of a Balancing Authority or Reserve Sharing Group. Item iii should be dropped. *The 'Damage or Destruction' event category has been revised to say "to a Facility', (a defined term) and thresholds have be modified to provide clarity. Footnotes for this event have been deleted.* o Damage or destruction of Critical Asset per CIP-002: Within the currently developing revisions to CIP-002 (version 5), Critical Asset will be retired as a glossary term. As well as addressing the durability of this event category, additional delineation is needed regarding which asset disruptions are to be reported. A CA as currently defined incorporates assets in a broad perspective, for instance a generating plant may be a Critical Asset. As currently written in Attachment 1, reporting may be required for unintended events, such as a boiler leak that takes a plant offline for a minor repair. Event #1 - Destruction of BES Equipment - captures incidents at the relevant equipment regardless of whether they are a Critical Asset or not. We recommend dropping this event. However, if reference to CIP-002 assets remains, it will be important to capture reporting of the events relevant to reliability and not just more events. o Damage or destruction of a Critical Cyber Asset per CIP-002: Because CCAs are defined at the component level, including this trigger is appropriate; however, as with CAs, the CCA term is scheduled to be retired under CIP-002 version 5. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately*

Organization	Yes or No	Question 3 Comment
		addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds. o Forced Intrusion: The footnote confuses the goal of including this event category. In addition, "forced" doesn't need to define the incident. Constellation proposes the following to better define the event:Intrusion that affects or attempts to affect the reliable operation of the BES (1)(1) Examples of "affecting reliable operation of the BES are": (i) device operations, (ii) protective equipment degradation, (iii) communications systems degradation including telemetered values and device status. o Risk to BES equipment: This category is too vague to be effective and the footnote further complicates the expectations around this event. The catch all concept of reporting potential risks to BES equipment is problematic. It's not clear what the reliability goal of this category is. Risk is not an event, it is an analysis. How are entities to comply with this "event", never mind within an hour? It appears that the information contemplated within this scenario would be better captured within the greater efforts underway by NERC to assess risks to the BES. This event should be removed from the Attachment 1 list in EOP-004. *'Forced intrusion' and 'Risk to BES Equipment' (which this footnote referenced) have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.* o BES Emergency requiring system-wide voltage reduction: the Entity with Reporting Responsibility should be limited to RC and TOP.

Organization	Yes or No	Question 3 Comment
		Entity with Reporting Responsibility states 'Initiating entity is responsible for reporting', which the DSR SDT feels is adequate direction in conjunction with the event: BES Emergency requiring system-wide voltage reduction. o Voltage deviations on BES Facilities: The Threshold for Reporting language needs more detail to explain +/- 10% of what? Proposed revision: Â± 10% outside the voltage schedule band sustained for â‰¥ 15 continuous minutes o IROL Violation (all Interconnections) or SOL Violation (WECC only): Should "Interconnections" be capitalized? o Transmission loss: The reporting threshold should provide more specifics around what constitutes Transmission Facilities. One minor item, under the Threshold for Reporting, "Three" does not need to be capitalized. *Both Transmission and Facilities are defined terms and the DSR SDT feels this gives sufficient direction.*
Response: Thank you for your comment. Please see response above.		
Pacific Northwest Small Public Power Utility Comment Group	Yes	While we agree with the revisions as far as they went, we do not believe the SDT has adequately addressed the FERC Order to "Consider whether separate, less burdensome requirements for smaller entities may be appropriate." The one and 24 hour reporting requirements continue to be burdensome to the smaller entities that do not maintain 24/7 dispatch centers. The one hour reporting requirement means that an untimely "recognition" starts the clock and reporting will become a higher priority than restoration. The note regarding adverse conditions does not help unless we were to consider the very lack of 24/7 dispatch to be such a condition. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber*

Organization	Yes or No	Question 3 Comment
		security incident as soon as possible, but in any event, within one hour of the event…" *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.* *The DSR SDT believes that reliability is best served by imposing reporting criteria based on impact to the BES rather than an arbitrary entity size threshold. With these latest revisions, all the proposed event categories provide thresholds that will capture the appropriate entities and provide a manageable timeframe.*
Response: Thank you for your comment. Please see response above.		
Clallam County PUD No.1	Yes	While we agree with the revisions as far as they went, we do not believe the SDT has adequately addressed the FERC Order to "Consider whether separate, less burdensome requirements for smaller entities may be appropriate." The one and 24 hour reporting requirements continue to be burdensome to the smaller entities that do not maintain 24/7 dispatch centers. The one hour reporting requirement means that an untimely "recognition" starts the clock and reporting will become a higher priority than restoration. The note regarding adverse conditions does not help unless we were to consider the very lack of 24/7 dispatch to be such a condition. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber*

Organization	Yes or No	Question 3 Comment
		security incident as soon as possible, but in any event, within one hour of the event…" *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.* *The DSR SDT believes that reliability is best served by imposing reporting criteria based on impact to the BES rather than an arbitrary entity size threshold. With these latest revisions, all the proposed event categories provide thresholds that will capture the appropriate entities and provide a manageable timeframe.*
Response: Thank you for your comment. Please see response above.		
Illinois Municipal Electric Agency	Yes	With the understanding this is within 24 hrs., and good professional judgment determines the amount of time to report the event to appropriate parties.
Response: Thank you for your comment.		
Ingleside Cogeneration LP	Yes	Yes. Any reporting that is mandated during the first hour of an event must be subject to close scrutiny. Many of the same resources that are needed to troubleshoot and stabilize the local system will be engaged in the reporting - which will impair reliability if not carefully applied. We believe that the ERO should reassess the need for any immediate reporting requirements on a regular basis to confirm that it provides some value to the restoration process. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706,*

Organization	Yes or No	Question 3 Comment
		Paragraph 673: *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		
Southwest Power Pool Regional Entity	Yes	
ZGlobal on behalf of City of Ukiah, Alameda Municipal Power, Salmen River Electric, City of Lodi	Yes	
MRO NSRF	Yes	
Western Electricity Coordinating Council	Yes	
Imperial Irrigation District	Yes	

Organization	Yes or No	Question 3 Comment
ACES Power Marketing Standards Collaborators	Yes	
Santee Cooper	Yes	
Sacramento Municipal Utility District (SMUD)	Yes	
Electric Compliance	Yes	
PacifiCorp	Yes	
Arizona Public Service Company	Yes	
Westar Energy	Yes	
Springfield Utility Board	Yes	
Manitoba Hydro	Yes	
Xcel Energy	Yes	
Liberty Electric Power	Yes	
Colorado Springs Utilities	Yes	
Independent Electricity System Operator	Yes	
South Carolina Electric and	Yes	

Organization	Yes or No	Question 3 Comment
Gas		
ISO New England	Yes	
American Transmission Company, LLC	Yes	
PSEG	Yes	
American Electric Power	Yes	
Georgia System Operations Corporation	Yes	
NV Energy	Yes	
Occidental Power Services, Inc. (OPSI)	Yes	
Northeast Utilities	Yes	
Great River Energy	Yes	
Oncor Electric Delivery Company LLC	Yes	
PPL Electric Utilities and PPL Supply Organizations`		
Progress Energy		

Organization	Yes or No	Question 3 Comment
Texas Reliability Entity		
ReliabilityFirst		
NRECA		
Entergy Services		
Thompson Coburn LLP on behalf of Miss. Delta Energy Agency		

4. Do you have any other comment, not expressed in questions above, for the DSR SDT?

Summary Consideration: The issues addressed in this question resulted in the DSR SDT reviewing and updating each requirement, Attachment 1 and Attachment 2. The DSR SDT has removed ambiguous language such as "risk" and "potential" based on comments received. All of the time frames in Attachment 1 have been moved to 24 hours upon recognition with the exception to reporting of CIP-008 events that remains one hour per FERC Order 706. Attachment 2 has been rewritten to mirror Attachment 1 events for entities who wish to use Attachment 2 in lieu of the DOE Form OE 417. VSLs have been reviewed to match the updated requirements.

Organization	Yes or No	Question 4 Comment
Cleco Corporation, Cleco Power, Cleco Power LLC	Abstain	Cleco does not use the VSL or VRF.
Response: Thank you for your comment		
Oklahoma Gas and Electric Co.	Abstain	Please see comments on SPP ballot
Response: Thank you for your comment. See response to those comments.		
Alberta Electric System Operator	Abstain	The Alberta Electric System Operator will need to modify parts of this standard to fit the provincial model when it develops the Alberta Reliability Standard.
Response: Thank you for your comment.		
Gainesville Regional Utilities	Affirmative	Looking forward to the added clarity.
Response: Thank you for your comment.		

Organization	Yes or No	Question 4 Comment
Manitoba Hydro	Affirmative	Manitoba Hydro is voting affirmative but would like to point out the following issues: -Attachment 1: The term 'Transmission Facilities' used in Attachment 1 is capitalized, but it is not a defined term in the NERC glossary. The drafting team should clarify what is meant by 'Transmission Facilities' and remove the capitalization. – *The DSR SDT has reviewed the NERC Glossary of Terms and notes that Transmission and Facilities are both defined. The combination of these two definitions are what the DSR SDT has based the applicability of "Transmission Facilities" in Attachment 1.* Attachment 2: The inclusion of 'fuel supply emergency' in Attachment 2 creates confusion as it infers that reporting a 'fuel supply emergency' may be required by the standard even though it is not listed as a reportable event in Attachment 1. On a similar note, it is not clear what the drafting team is hoping to capture by including a checkbox for 'other' in Attachment 2. *The DSR SDT has removed both "fuel supply emergency" and "other" from Attachment 2.*
Response: Thank you for your comment. Please see response above.		
Oncor Electric Delivery	Affirmative	NERC's Event Analysis Program tends to parallel many of the reporting requirements as outlined in EOP-004 Version 2. Oncor recommends that NERC consider ways of streamlining the reporting process by either incorporating the Event Analysis obligations into EOP-004-2 or reducing the scope of the Event Analysis program as currently designed to consist only of "exception" reporting. *The reporting of events as required in EOP-004 is the input to the Events Analysis Program. Events are reported to the ERO and the EAP will follow up as per the EAP processes and procedures.*

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comment. Please see response above.		
City Utilities of Springfield, Missouri	Affirmative	SPRM supports the comments from SPP.
Response: Thank you for your comment. Please see response to comments from SPP.		
Kootenai Electric Cooperative	Affirmative	The changes are an improvement over the existing standards.
Response: Thank you for your comment.		
Empire District Electric Co.	Affirmative	We agree with the comments provided by SPP
Response: Thank you for your comment. Please see response to SPP comments.		
Lakeland Electric	Negative	1. Further clarity is needed. For example the standard stipulates in R1.3 ". .as appropriate." Who deems what is appropriate? Also in R1.4 ". .other circumstances" is open to interpretation. *Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to communicate events to as stated in the entity's Operating Plan.* *Requirement R1, Part 1.4 was removed from the standard* 2. Remove paragraph 1 of the data retention section as it parrots the Rules of Procedure, Appendix 4C: Compliance Monitoring and Enforcement Program, Section 3.1.4.2. Possibly place a pointer to the CMEP in the data retention section. *The item in question is standard boilerplate language that is being placed in all NERC standards.*

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comment. Please see response above.		
CPS Energy	Negative	oR1.4: CPS Energy believes that "updating the Operating Plan within 90 calendar days of any change..." is a very burdensome compliance documentation requirement. *Requirement R1, Part 1.4 was removed from the standard.* oAttachment 1: Events Table: In DOE OE-417 local electrical systems with less than 300MW are excluded from reporting certain events since they are not significant to the BES. CPS Energy believes that the benefit of reporting certain events on systems below this value would outweigh the compliance burden placed on these small systems. *Upon review of the DOE OE 417, it states "Local Utilities in Alaska, Hawaii, Puerto Rico, the U.S. Virgin Islands, and the U.S. Territories - If the local electrical system is less than 300 MW, then only file if criteria 1, 2, 3 or 4 are met". Please be advised this exception applies to entities outside the continental USA.*
Response: Thank you for your comment. Please see response above.		
Lakeland Electric	Negative	An issue of possible differences in interpretation between entities and compliance monitoring and enforcement is the phrase in 1.3 that states "the following as appropriate". Who has the authority to deem what is appropriate? *Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to communicate events to as stated in the entity's Operating Plan*

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comment. Please see response above.		
Dynegy Inc.; Southern Illinois Power Coop.; Louisville Gas and Electric Co.	Negative	Comments submitted as part of the SERC OC; I agree with the comments of the SERC OC Standards Review group that have been provided to NERC.; We are a signatory to the SERC OC RRG comments filed last week.
Response: Thank you for your comment. Please see response to the SERC OC RRG comments.		
Hydro One Networks, Inc.	Negative	First and foremost we are not supportive of continuance of standards that are not "results based". Standards written to gather data, make reports etc. should not be written. There should be other processes for reporting in place that will not be subject to ERO oversight and further compliance burdens. *The DSR SDT has been following the guidance set by NERC to write a "results based" standard. As with any process there may be many different ways to achieve the same outcome. The NERC Quality Process has not indicated any request to update this Standard, concerning the Results Based Standard format.* o We are disappointed that the standard does not appear to reduce reporting requirements nor does it promote more efficient reporting. We encourage the SDT to take a results based approach and coordinate and reduce reporting through efficiencies between the various agencies and NERC. *The DSR SDT is staying within scope of the approved SAR and will be forwarding your concern of efficiencies between various agencies and NERC* o The Purpose statement is very broad, and "...by requiring the reporting of events with the potential to impact reliability and their causes..." on the Bulk Electric System it can be said that every event occurring on the Bulk Electric System would have to be reported. There is already an event analysis process in place. Could this reporting

Organization	Yes or No	Question 4 Comment
		be effectively performed in that effort? *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:* *"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."* o The standard prescribes different sets of criteria, and forms. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.* o There should be one recipient of event information. That recipient should be a

Organization	Yes or No	Question 4 Comment
		"clearinghouse" to ensure the proper dissemination of information. *The DSR SDT is proposing revisions to the NERC Rules of Procedure that address your comment:* *812. NERC Reporting Clearinghouse* *NERC will establish a system to collect report forms as established for this section or standard, from any Registered Entities, pertaining to data requirements identified in Section 800 of this Procedure. Upon receipt of the submitted report, the system shall then forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary. This can include state, federal, and provincial organizations.* o Why is this standard applicable to the ERO? *The ERO is applicable to CIP-008 and therefore is applicable to this proposed Standard.*
Response: Thank you for your comment. Please see response above.		
FirstEnergy Corp., FirstEnergy Energy Delivery, FirstEnergy Solutions, Ohio Edison Company	Negative	FirstEnergy appreciates the hard work of the drafting team and believes it has made great improvements to the standards. However, we must vote negative at this time until a few issues are clarified per our comments submitted through the formal comment period.
Response: Thank you for your comment. Please see response to your other comments.		
Lakeland Electric	Negative	In general; here has not been sufficient prudency review for the standard, especially R1, to justify a performance based standard around a Frequency Response Measure *Based on your short comment, Requirement 1 has been modified as requested by stakeholders. The DSR SDT cannot answer the issue of Frequency Response Measures*

Organization	Yes or No	Question 4 Comment
		since it is not within the scope of the SAR.
Response: Thank you for your comment. Please see response above.		
Northeast Power Coordinating Council	Negative	NPCC believes that further revision of the standard is necessary so is not able to support the VSLs at this time. Comments to the standard will be made in the formal comment period.
Response: Thank you for your comment. Please see responses to your other comments.		
Central Lincoln PUD; Blachly-Lane Electric Co-op; Central Electric Cooperative, Inc. (Redmond, Oregon); Clearwater Power Co.; Consumers Power Inc.; Coos-Curry Electric Cooperative, Inc; Fall River Rural Electric Cooperative; Lane Electric Cooperative, Inc.; Northern Lights Inc.; Pacific Northwest Generating Cooperative; Raft River Rural Electric Cooperative; Umatilla Electric Cooperative; West Oregon Electric Cooperative, Inc.; Cowlitz County PUD	Negative	Please see comments submitted by the Pacific Northwest Small Public Power Utility Comment Group.
Response: Thank you for your comment. Please see responses to comments of the Pacific Northwest Small Public Power Utility		

Organization	Yes or No	Question 4 Comment
Comment Group.		
Rochester Gas and Electric Corp.	Negative	RG&E supports comments to be submitted to NPCC.
New Brunswick System Operator	Negative	See comments submitted by the NPCC Reliability Standards Committee and the IRC Standards Review Committee.
Florida Municipal Power Pool	Negative	See FMPA's comments
Response: Thank you for your comment. See responses to those comments.		
Commonwealth of Massachusetts Department of Public Utilities	Negative	Standards written to gather data, make reports etc. should not be written. There should be other processes for reporting in place that will not be subject to ERO oversight and further compliance burdens. *FERC Order 693 section 617 states "...the Commission directs the ERO to develop a modification to EOP-004-1 through the reliability Standards development process that includes any Requirement necessary for users, owners, and operators of the Bulk-Power System to provide data...". In order for entities to provide data they are required to implement their Operating Plan. EOP-004-2 will satisfy this FERC directive.*
Response: Thank you for your comment. Please see response above.		
Hydro One Networks, Inc.	Negative	Suggested key concepts for the SDT consideration in this standard: ? Develop a single form to report disturbances and events that threaten the reliability of the bulk electric system ? Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements ? Establish clear criteria for reporting ? *The DSR SDT has only provided one form within this proposed Standard, please see*

Organization	Yes or No	Question 4 Comment
		Attachment 2. Based on stakeholder feedback, the DSR SDT has allowed stakeholders to use the DOE Form OE 417. Please note that not every Stakeholder in NERC wishes to use the DOE Form OE 417. Establish consistent reporting timelines ? *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.* Provide clarity around who will receive the information and how it will be used ? Explore other opportunities beside a standard to effectively achieve the same outcome. Standards should be strictly results based, whose purpose is to achieve an adequate level of reliability on the BES. *The DSR SDT has clearly stated who will receive the information: Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to report events. Part 1.2 now reads:* *"1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations*

Organization	Yes or No	Question 4 Comment
		needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies." *The information received will be mainly used for situational awareness and other processes.*
Response: Thank you for your comment. Please see response above.		
Orlando Utilities Commission	Negative	The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes, as well as the CIP standards Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definitions of a BES element could change significantly and Critical Assets may no longer exist. As it relates to the proposed reporting criteria, it is debatable as to whether or not the destruction of, for example, one relay would be a reportable incident under this definition going forward given the current drafting team efforts. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.*
Response: Thank you for your comment. Please see response above.		
James A Maenner	Negative	The information in section "5 Background" should be moved from the standard to a supporting document. *The DSR SDT will refer to guidance within the Standards Development process on the proper place to maintain Background information.*

Organization	Yes or No	Question 4 Comment
		The reporting exemption language for weather in the Note on Attachment 1 - Events Table should be included in R3, not just a note. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2based on stakeholder comments and revised R3 (now R2) to:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."* The "Guideline and Technical Basis", last 3 pages, should be moved from the standard to a supporting document. *The Guideline and Technical Basis section is a part of the Results-Based Standard format and the information contained in it is in the correct place.*
Response: Thank you for your comment. Please see response above.		
Kansas City Power & Light Co.	Negative	The proposed Standard is in need of additional work to complete the Attachment 1, complete the VSL's, and clarify language and content within the proposed standard. *The DSR SDT has reviewed and revamped all Requirements and both Attachments based on stakeholders feedback. This will provide clarity for entities to follow.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 4 Comment
SERC Reliability Corporation	Negative	The purpose of the standard "To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of events with the potential to impact reliability and their causes, if known, by the Responsible Entities" has not been achieved as written. There is the potential for the information and data contemplated by this standard to be useful in achieving the stated purpose through follow-on activities of the industry, the regions, and NERC. However, as drafted, Attachment 1 will inform the ERO of the existence of only a portion of the "events with the potential to impact reliability and their causes, if known". *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:* *"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."* Events listed in Appendix E to the ERO Event Analysis Process document should be incorporated into the standard instead of hardwiring inconsistency by requiring a different set of events. Alternatively, the SDT should explore deleting Attachment 1 and instead referencing the ERO Event Analysis process (which as a learning organization will have systematic changes to the reporting thresholds over time). At first this may seem contrary to the SDT objective of eliminating fill-in-the-blank aspects of the existing standard but the SDT should explore the Commission's willingness to accept a reference document for reporting thresholds. Additionally, it is unclear how NERC's role as the ES-ISAC is supported through the requirements of this reliability standard. It appears to undermine the ability of NERC (ES-ISAC) to be made timely aware of threats to the critical infrastructure--at odds with it's purpose. Thus, this draft does not achieve the elimination of redundant reporting envisioned in the SAR, nor does it achieve the objective of supporting NERC in the analysis of disturbances or blackouts. *The DSR SDT is following NERC's ANSI approved process for standards development.*

Organization	Yes or No	Question 4 Comment
		The ERO Events Analysis process does not have the frame work as required by the ANSI development process. Within this proposed Standard, when an Attachment 1 event is recognized, the ERO (which is the ES-ISAC) will be one of the first to be notified, as will the entities Reliability Coordinator. This will enhance situational awareness as per the entity's Operation Plan and this Standard. *FERC Order 693 section 617 states "…the Commission directs the ERO to develop a modification to EOP-004-1 through the reliability Standards development process that includes any Requirement necessary for users, owners, and operators of the Bulk-Power System to provide data…". In order for entities to provide data they are required to implement their Operating Plan. EOP-004-2 will satisfy this FERC directive.*
Response: Thank you for your comment. Please see response above.		
Tucson Electric Power Co.	Negative	The tie between an Operating Plan and reportable disturbance events is not clear. Being the exception, I feel that a reportable disturbance methodology should be part of an Emergency Operating Plan. *EOP-004-2 provides Applicable Entities with the minimum report requirements for events contained in Attachment 1. NERC has defined Operating Plan in part as: "A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes." An entity may include a reportable disturbance methodology within their Operating Plan since this Standard does not preclude it.*
Response: Thank you for your comment. Please see response above.		
United Illuminating Co.	Negative	The VSL table is mistyped. R2 lists 1.1 and 1.5. R4 VRF should be lower.

Organization	Yes or No	Question 4 Comment
		Requirement R4 (now R3) calls for conducting an annual test of the communications process in Requirement 1, Part 1.2. It is not strictly administrative in nature and therefore does not meet the VRF guideline for a Lower VRF. .
Response: Thank you for your comment. Please see response above.		
PSEG Energy Resources & Trade LLC, PSEG Fossil LLC, Public Service Electric and Gas Co.	Negative	There are several items that need clarification. See PSEG's separately provided comments.
Response: Thank you for your comment. Please see response to your other comments.		
Kansas City Power & Light Co.	Negative	There is no VSL for R4. *The VSL for Requirement R4 was inadvertently redlined in the redline version of the standard, but it was present in the clean version.*
Response: Thank you for your comment. Please see response above.		
Ameren Services	Negative	We believe that these [VRFs and VSLs] will change as we expect some changes in the draft standard.
Response: Thank you for your comment.		
New York State Department of Public Service	Negative	While the proposed standard consolidates many reporting requirements, the requirement that any event with the "potential to impact reliability" be reported is overly broad and will prove to be burdensome and distracting to system operations. *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:*

Organization	Yes or No	Question 4 Comment
		"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."
Response: Thank you for your comment. Please see response above.		
Springfield Utility Board		o The Draft 3 Version History still lists the term "Impact Event" instead of "Event". *This has been corrected.* o Draft 3 of EOP-004-2 - Event Reporting does not provide a definition for the term "Event" nor does the NERC Glossary of Terms Used in Reliability Standards. SUB recommends that "Event" be listed and defined in "Definitions and Terms Used in the Standard" as well as the NERC Glossary, providing a framework and giving guidance to entities for how to determine what should be considered an "Event" (ex: sabotage, unusual occurrence, metal theft, etc.). *The DSR SDT has reviewed this issue and has changed "Event" to "event". Attachment 1 contains each reportable 'event".*
Response: Thank you for your comment. Please see response above.		
Northeast Utilities		- Incorporate NERC Event Analysis Reporting into this standard. Make the requirements more specific to functional registrations as opposed to having requirements applicable to "Responsible Entities".- The description of a Transmission Loss Event in A *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1. The DSR SDT has reviewed and reworded "Entities with Reporting Responsibilities" to require the minimum amount of entities who will be required to report each event.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 4 Comment
Progress Energy		(1) Attachment 1 lists "Destruction of BES Equipment" as a reportable event but then lists "equipment failure" as one of several thresholds for reporting, with a one hour time limit for reporting. It is simply not common sense to think of the simple failure of a single piece of equipment as "destruction of BES equipment". Does the standard really expect that every BES equipment failure must be reported within one hour, regardless of cause or impact to BES reliability? What is the purpose of such extensive reporting? *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* (2) The same comment as (1) above is applicable to the "Damage or destruction of Critical Asset" because one threshold is simple "equipment failure" as well. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* (3) Footnote 2 (page 20) says copper theft is not reportable "unless it effects the reliability of the BES", but footnote 1 on the same page says copper theft is reportable if "it degrades the ability of equipment to operate properly". In this instance, the proposed standard provides two different criteria for reporting one of the most common events on the same page. *The DSR SDT has removed all footnotes with the exception of the updated event within Attachment 1 that states: "A physical threat that could impact the operability of a Facility". This event has the following footnote, which states: "Examples include a*

Organization	Yes or No	Question 4 Comment
		train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility." (4) Forced Intrusion must be reported if "you cannot determine the likely motivation", and not based on a conclusion that the intent was to commit sabotage or intentional damage. This would require reporting many theft related instances of cut fences and forced doors (including aborted theft attempts where nothing is stolen) which would consume a great deal of time and resources and accomplish nothing. This criteria is exactly the opposite of the existing philosophy of only reporting events if there is an indication of an intent to commit sabotage or cause damage. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.* (5) "Risk to BES equipment…from a non-environmental physical threat" is reportable, but this is an example of a vague, open ended reporting requirement that will either

Organization	Yes or No	Question 4 Comment
		generate a high volume of unproductive reports or will expose reporting entities to audit risk for not reporting potential threats that could have been reported. The standard helpfully lists train derailments and suspicious devices as examples of reportable events. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.* The existing CAN for CIP-001 (CAN-0016) is already asking for a list of events that were analyzed so the auditors can determine if a violation was committed due to failure to report. I can envision the CAN for this new standard requiring a list of all "non-environmental physical threats" that were analyzed during the audit period to determine if applicable events were reported. This could generate a great deal of work simply to provide audit documentation even if no events actually occur that are reportable. It would also be easy for an audit team to second guess a decision that was made by an entity not to report an event (what is risk?...how much risk was present due to the event?...). Also, the reporting for this vague criteria must be done within one hour. Any event with a one hour reporting requirement should be crystal clear and unambiguous. *The DSR SDT has reworded and updated Attachment 1 per comments received and believes that the language used obviates the need for CAN-016. CAN-0016 has been*

Organization	Yes or No	Question 4 Comment
		remanded. (6) Transmission Loss...of three or more Transmission Facilities" is reportable. "Facility" is a defined term in the NERC Glossary, but "Transmission Facility" is not a defined term, which will lead to confusion when this criteria is applied. This requirement raises many confusing questions. What if three or more elements are lost due to two separate or loosely related events - is this reportable or not? What processes will need to be put in place to count elements that are lost for each event and determine if reporting is required? Why must events be reported that fit an arbitrary numerical criteria without regard to any material impact on BES reliability? *The DSR SDT used the defined term "Facility" to add clarity for several events listed in Attachment 1. A Facility is defined as:* *"A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"* *The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.* *Both Transmission and Facilities are defined terms and the DSR SDT feels this gives sufficient direction.*
Response: Thank you for your comment. Please see response above.		
MRO NSRF		: The MRO NSRF wishes to thank the SDT for incorporating changes that the industry had with reporting time periods and aligning this with the Events Analysis Working Group and Department of Energy's OE 417 reporting form.

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comment.		
FirstEnergy		1. Attachment 1 - Regarding the 1st event listed in the table, "Destruction of BES Equipment" and its accompanying Footnote 1, we believe that this event should be broken into two separate events that incorporate the specifics in the footnote as follows: a. "Destruction of BES equipment that associated with an IROL per FAC-014-2." Regarding the 1st event we have proposed - We have proposed this be made specific to IROL as stated in Footnote 1 part i. Also, we believe that only the RC and TOP would have the ability to quickly determine and report within 1 hour if the destruction is associated with an IROL. The other entities listed would not necessarily know if the event affects and IROL. Therefore, we also propose that the Entities with Reporting Responsibilities (column 2) be revised to only include the RC and TOP. *The DSR SDT agrees with your comment and made the following changes:* *'Threshold for Reporting' column in the 'Damage or Destruction' event category. The updated Threshold for Reporting now reads as:* *"Damage or destruction of a Facility that:* • *Affects an IROL (per FAC-014)* *OR* • *Results in the need for actions to avoid an Adverse Reliability Impact* *OR* • *Results from intentional human action."* b. "Destruction of BES equipment that removes the equipment from service." Regarding the 3rd event we have proposed - We have proposed this be made specific to destruction of BES equipment that removes the equipment from service as stated in Footnote 1 part iii. Also, the other part of footnote 1 part iii which states "Damaged or destroyed due to intentional or unintentional human action" is not

Organization	Yes or No	Question 4 Comment
		required since it is covered in the threshold for reporting. Also the term "Damaged" in this part iii is not appropriate since these events are limited to equipment that has been destroyed. We also propose that the Entities with Reporting Responsibilities (column 2) for this event would remain the same as it states now since any of those entities may observe out of service BES equipment.Regarding part ii of footnote 1, we do not believe that this event needs to be separated. Regarding the phrase "significantly affects the reliability margin of the system be clarified so that it is not left up to the entity to interpret a "significant" affect. Lastly, since we have incorporated parts i and iii into the two separate events and removed part ii as proposed above, the only statement that needs to be left in the Footnote 1 is: "Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative)." *The DSR SDT has removed all footnotes with the exception of the updated event within Attachment 1 that states: "Any physical threat that could impact the operability of a Facility". This event has the following footnote, which states: "Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* 2. Attachment 1 - We ask that the team add an "Event #" column to the table so that each of the events listed can be referred to by #, such as Event 1, Event 2, etc. *The DSR SDT believes that the minimum reporting attributes are contained in Attachment 1.* 3. Attachment 1 - Event titled "Damage or destruction of a Critical Cyber Asset per

Organization	Yes or No	Question 4 Comment
		CIP-002", the proposed threshold for reporting seems incomplete. We suggest the threshold for this event match the threshold for the Critical Asset event which states: "Initial indication the event was due to operational error, equipment failure, external cause, or intentional or unintentional human action."4. Attachment 1 - Events titled "Damage or destruction of a Critical Assets per CIP-002" and "Damage or destruction of a Critical Cyber Asset per CIP-002" seem ambiguous due to the term "damage". We suggest removal of "damage" or clarity as to what is considered a damaged asset.5. VSL Table - Instead of listing every entity, it may be more efficient to simply say "The Responsible Entity" in the VSL for each requirement.6. Guideline and Technical Basis section - This section does not provide guidance on each of the requirements of the standard. We suggest the team consider adding guidance for the requirements. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.*
Response: Thank you for your comment. Please see response above.		
Southwest Power Pool Regional Entity		1. EOP-004-2 R1.4 states entities must update their Operating Plans within 90 calendar days of incorporating lessons learned pursuant to R3. However, neither R3 nor Attachment 1 include a timeline for incorporating lessons learned. It is unclear when the "clock starts" on incorporating improvements or lessons learned. Within 90 days of what? 90 days of the event? 90 days from when management approved the lesson learned? Auditors need to know the trigger for the 90-day clock. *Requirement R1, Part 1.4 was removed from the standard.* 2. The Event Analysis classification includes Category 1C "failure or misoperation of

Organization	Yes or No	Question 4 Comment
		the BPS SPS/RAS". This category is not included in EOP-004-2's Attachment 1. This event, "failure or misoperation of the BPS SPS/RAS", needs to either be added to Attachment 1 or removed from the Event Analysis classification. It is important that EOP-004-2 Attachment 1 and the Event Analysis categories match up.Thank you for your work on this standard. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.*
Response: Thank you for your comment. Please see response above.		
Independent Electricity System Operator		1. Measures M1, M2 and M3: Suggest to achieve consistent wording among them by saying the leading part to "Each Responsible Entity shall provide...." *The DSR SDT is following the guidance within the Standards Development process on*

Organization	Yes or No	Question 4 Comment
		the wording pertaining to items outside the realm of a requirement. 2. In our comments on the previous version, we suggested the SDT to review the need to include IA, TSP and LSE for some of the reporting requirements in Attachment 1. The SDT's responded that it had to follow the requirements of the standards as they currently apply. Since these entities are applicable to the underlying standards identified in Attachment 1, they will be subject to reporting. We accept this rationale. However, the revised Attachment 1 appears to be still somewhat discriminative on who needs to report an event. For example, the event of "Detection of a reportable Cyber Security Incident" (6th row in the table) requires reporting by a list of responsible entities based on the underlying requirements in CIP-008, but the list does not include the IA, TSP and LSE. We again suggest the SDT to review the need for listing the specific entities versus leaving it general by saying: "Applicable Entities under CIP-008" for this particular item, and review and establish a consistent approach throughout Attachment 1. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008.* 3. VSLs: a. Suggest to not list all the specific entities, but replace them with "Each Responsible Entity" to simplify the write-up which will allow readers to get to the violation condition much more quickly. b. For R1, it is not clear whether the conditions listed under the four columns are "OR" or "AND". We believe it means "OR", but this needs to be clarified in the VSL table.4. The proposed implementation plan conflicts with Ontario regulatory practice respecting the effective date of the standard. It is suggested that this conflict be removed by appending to the implementation plan wording, after "applicable regulatory approval" in the Effective Dates Section on P. 2 of the draft standard and P. 1 of the draft implementation plan, to the following effect: ", or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities." *The DSR SDT is following the guidance within the Standards Development process on*

Organization	Yes or No	Question 4 Comment
		the wording pertaining to items outside the realm of a requirement.
Response: Thank you for your comment. Please see response above.		
NRECA		1. Please ensure that the work of the SDT is done in close coordination with Events Analysis Process (EAP) work being undertaken by the PC/OC and BOT, and with any NERC ROP additions or modifications. NRECA is concerned that the EAP work being done by these groups is not closely coordinated even though their respective work products are closely linked -- especially since the EAP references information in EOP-004. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.*

Organization	Yes or No	Question 4 Comment
		2. The SDT needs to be consistent in its use of "BES" and "BPS" - boths acronyms are used throughout the SDT documents. NRECA strongly prefers the use of "BES" since that is what NERC standards are written for. *The DSR SDT has used BES within EOP-004-2. All references to BPS have been removed.* 3. Under "Purpose" section of standard, 3rd line, add "BES" between "impact" and "reliability." Without making this change the "Purpose" section could be misconstrued to refer to reliability beyond the BES. *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:* *"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."* 4. In the Background section there is reference to the Events Analysis Program. Is that the same thing as the Events Analysis Process? Is it something different? Is it referring to a specific department at NERC? Please clarify in order to reduce confusion. Also in the Background section there is reference to the Events Analysis Program personnel. Who is this referring to -- NERC staff in a specific department? Please clarify. *The DSR SDT was explaining that the DSR SDT and has been coordinating with the "Events Analysis Working Group.* 5. In M1 please be specific regarding what "dated" means. *This is a common term used with many NERC Standards and simply means that your evidence is dated and time stamped.* 6. In M3 please make it clear that if there wasn't an event, this measure is not applicable

Organization	Yes or No	Question 4 Comment
		The DSR SDT has not implied that Applicable Entities need to prove that something did not happen. 7. In R4 it is not clear what "verify" means. Please clarify. *R4 (now R3) was revised to remove "verify"* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* 8. In Attachment 1 there are references to Critical Asset and Critical Cyber Asset. These terms will likely be eliminated from the NERC Glossary of Terms when CIP V5 moves forward and is ultimately approved by FERC. This could create future problems with EOP-004 if CIP V5 is made effective as currently drafted. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008.* 9. In Attachment 1 the one hour timeframe for submitting data for the first 7 items listed is very tight. Other than being required by the EOE)E-417 form, NRECA requests that the SDT provide further support for this timeframe. If there are not distinct reasons why 1 hour is the right timeframe for this, then other timeframes should be explored with DOE. *The DSR SDT also received many comments regarding the various events of Attachment 1. Many commenters questioned the reliability benefit of reporting events to the ERO and their Reliability Coordinator within 1 hour. Most of the events with a one hour reporting requirement were revised to 24 hours based on stakeholder comments as well as those types of events are currently required to be reported within 24 hours in the existing mandatory and enforceable standards. The only remaining type of event that is to be reported within one hour is "A reportable Cyber*

Organization	Yes or No	Question 4 Comment
		Security Incident" as it required by CIP-008. *FERC Order 706, paragraph 673 states: "...each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event within one hour of the event..."* *Note that members of NRECA may be required to submit the DOE Form OE 417, and this agency's reporting requirements are not within scope of the project.* 10. While including Footnote 1 is appreciated, NRECA is concerned that this footnote will create confusion in the compliance and audit areas and request the SDT to provide more definitive guidance to help explain what these "Events" refer to. NRECA has the same comment on Footnote 2 and 3. Specifically in Footnote 3, how do you clearly determine and audit from a factual standpoint something that "could have damaged" or "has the potential to damage the equiment?" *The DSR SDT has removed all footnotes with the exception of the updated event within Attachment 1 that states: "A physical threat that could impact the operability of a Facility". This event has the following footnote, which states: "Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* 11. In the Guideline and Technical Basis section, in the 1st bullet, how do you determine, demonstrate and audit for something that "may impact" BES reliability? *This statement has been removed per comments received.* 12. On p. 28, first line, this sentence seems to state that NERC, law enforcement and other entities - not the responsible entity - will be doing event analysis. My understanding of the current and future Event Analysis Process is that the

Organization	Yes or No	Question 4 Comment
		responsible entity does the event analysis. Please confirm and clarify. *EOP-004-2 requires Applicable Entities to "report " and "communicate" as stated in Requirement 1, Part 1.2: "A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."* *The Event Analysis Program may use a reported event as a basis to analyze an event. The processes of the Event Analysis Program fall outside the scope of this project, but the DSR SDT has collaborated with them of events contained in Attachment 1.* *The Standard does not require the Applicable Entity to analyze a reported event.*
Response: Thank you for your comment. Please see response above.		
Exelon		1. Please replace the text "Operating Plan" with procedure(s). Many companies have procedure(s) for the reporting and recognition of sabotage events. These procedures extend beyond operating groups and provide guidance to the entire company. *Thank you for your comment. The DSR SDT intends on keeping "Operating Plan" within EOP-004-2 since NERC has it defined as:* *"A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan". As stated, the Operating Plan may contain Operating procedures or Operating Processes. This will give Applicable Entities the greatest flexibility in achieving compliance with this Standard.*

Organization	Yes or No	Question 4 Comment
		2. The Loss of Off-site power event criteria is much improved from the last draft of EOP 004-2; however, some clarification is needed to more accurately align with NERC Standard NUC-001 in both nomenclature and intent. Specifically, as Exelon has previously commented, there are many different configurations supplying offsite power to a nuclear power plant and it is essential that all configurations be accounted for. As identified in the applicability section of NUC-001 the applicable transmission entities may include one or more of the following (TO, TOP, TP, TSP, BA, RC, PC, DP, LSE, and other non-nuclear GO/GOPs). Based on the response to previous comments submitted for Draft 2, Exelon understands that the DSR SDT evaluated the use of the word "source" but dismissed the use in favor of "supply" with the justification "[that] 'supply' encompasses all sources". Exelon again suggests that the word "source" is used as the event criteria in EOP-004-2 as this nomenclature is commonly used in the licensing basis of a nuclear power plant. By revising the threshold criteria to "one or more" Exelon believes the concern the DSR SDT noted is addressed and ensures all sources are addressed. In addition, by revising the threshold for reporting to a loss of "one or more" will ensure that all potential events (regardless of configuration of off-site power supplies) will be reported by any applicable transmission entity specifically identified in the nuclear plant site specific NPIRs.As previously suggested, Exelon again proposes that the loss of an off-site power source be revised to an "unplanned" loss to account for planned maintenance that is coordinated in advance in accordance with the site specific NPIRs and associated Agreements. This will also eliminate unnecessary reporting for planned maintenance.Although the loss of one off-site power source may not result in a nuclear generating unit trip, Exelon agrees that an unplanned loss of an off-site power source regardless of impact should be reported within the 24 hour time limit as proposed. Suggest that the Loss of Offsite power to a nuclear generating plant event be revised as follows:Event: Unplanned loss of any off-site power source to a Nuclear Power PlantEntity with Reporting Responsibility: The applicable Transmission Entity that owns and/or operates the off-site power source to a

Organization	Yes or No	Question 4 Comment
		Nuclear Power Plant as defined in the applicable Nuclear Plant Interface Requirements (NPIRs) and associated Agreements.Threshold for Reporting: Unplanned loss of one or more off-site power sources to a Nuclear Power Plant per the applicable NPIRs. *Based on comments received, this event has been updated within Attachment 1 to read as:* *"Complete loss of off-site power to a nuclear generating plant (grid supply)".* 3. Attachment 1 Generation loss event criteria Generation lossThe â‰¥ 2000 MW/â‰¥ 1000 MW generation loss criteria do not provide a time threshold or location criteria. If the 2000 MW/1000 MW is intended to be from a combination of units in a single location, what is the time threshold for the combined unit loss? For example, if a large two unit facility in the Eastern Interconnection with an aggregate full power output of 2200 MW (1100 MW per unit) trips one unit (1100 MW) [T=0 loss of 1100 MW] and is ramping back the other unit from 100% power and 2 hours later the other unit trips at 50% power [550 MW at time of trip]. The total loss is 2200 MW; however, the loss was sustained over a 2 hour period. Would this scenario require reporting in accordance with Attachment 1? What if it happened in 15 minutes? 1 hour? 24 hours? Exelon suggests the criteria revised to include a time threshold for the total loss at a single location to provide this additional guidance to the GOP (e.g., within 15 minutes to align with other similar threshold conditions). Threshold for Reporting ï€ â‰¥ 2,000 MW unplanned total loss at a single location within 15 minutes for entities in the Eastern or Western Interconnection â‰¥ 1000 MW unplanned total loss at a single location within 15 minutes for entities in the ERCOT or Quebec Interconnection *The DSR SDT has not modified this event since it is being maintained as it is presently enforceable within EOP-004-1.* 4. Exelon appreciates that the DSR SDT has added the NRC to the list of Stakeholders in the Reporting Process, but does not agree with the SDT response to FirstEnergy's

Organization	Yes or No	Question 4 Comment
		comment to Question 17 [page 206] that stated "NRC requirements or comments fall outside the scope of this project." Quite the contrary, this project should be communicated and coordinated with the NRC to eliminate confusion and duplicative reporting requirements. There are unique and specific reporting criteria and coordination that is currently in place with the NRC, the FBI and the JTTF for all nuclear power plants. If an event is in progress at a nuclear facility, consideration should be given to coordinating such reporting as to not duplicate effort, introduce conflicting reporting thresholds, or add unnecessary burden on the part of a nuclear GO/GOP who's primary focus is to protect the health and safety of the public during a potential radiological sabotage event (as defined by the NRC) in conjunction with potential impact to the reliability of the BES. *The DSR SDT has established a minimum amount of reporting for events listed in Attachment 1. The NRC does not fall under the jurisdiction of NERC and so therefore it is not within scope of this project.* 5. Attachment 1 Detection of a reportable Cyber Security Incident event criteria.The threshold for reporting is "that meets the criteria in CIP-008". If an entity is exempt from CIP-008, does that mean that this reportable event is therefore also not applicable in accordance with EOP-004-2 Attachment 1? *If an entity is exempt from CIP-008, then they do not have to report this type of event. Entities can report any situation at anytime to whomever they wish. If an entity is responsible for items that fall under a Cyber Security Incident, then they would report per this standard.*
Response: Thank you for your comment. Please see response above.		
Duke Energy		1. Reporting under EOP-004-2 should be more closely aligned with Events Analysis Reporting. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating*

Organization	Yes or No	Question 4 Comment
		Attachment 1, but there remain differences for the following reasons: • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.* 2. Attachment 1 - Under the column titled "Entity with Reporting Responsibility", several Events list multiple entities, using the phrase "Each RC, BA, TO, TOP, GO, GOP, DP that experiences..." or a similar phrase requiring that multiple entities report the same event. We believe these entries should be changed so that multiple reports aren't required for the same event. *The DSR SDT agrees that there may be some dual reporting for the same event. The minimum Applicable Entities have been review and updated where updates could be made. The DSR SDT believes that a dual report will provide a clearer picture of the breadth and depth of an event the Electric Reliability Organization and the Applicable Entities Reliability Coordinator.* 3. Attachment 1 - The phrase "BES equipment" is used several times in the Events Table and footnotes to the table. "Equipment" is not a defined term and lacks clarity. "Element" and "Facility" are defined terms. Replace "BES equipment" with

Organization	Yes or No	Question 4 Comment
		"BES Element" or "BES Facility". *The DST SDT has removed the term "equipment" from Attachment 1 per comments received.* 4. Attachment 1 - The Event "Risk to BES equipment" is unclear, since some amount of risk is always present. Reword as follows: "Event that creates additional risk to a BES Element or Facility." *The DSR SDT has removed this event from Attachment 1. Several stakeholders expressed concerns relating to the "Forced Intrusion" event. Their concerns related to ambiguous language in the footnote. The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* 5. Attachment 1 - The Threshold for Reporting Voltage deviations on BES Facilities is identified as "+ 10% sustained for > 15 continuous minutes." Need to clarify + 10% of what voltage? We think it should be nominal voltage. *A sustained voltage deviation of ± 10% on the BES is significant deviation and is indicative of a shortfall of reactive resources either pre- or post-contingency. The DSR SDT is indifferent to which of nominal, pre-contingency, or scheduled voltage, is used as the baseline, but for simplicity and to promote a common understanding suggest using nominal voltage.* 6. Attachment 1 - Footnote 1 contains the phrase "has the potential to". This phrase should be struck because it creates an impossibly broad compliance responsibility. Similarly, Footnote 3 contains the same phrase, as well as the word "could" several times, which should be changed so that entities can reasonably comply.

Organization	Yes or No	Question 4 Comment
		The DSR SDT has removed all footnotes with the exception of the updated event within Attachment 1 that states: "A physical threat that could impact the operability of a Facility". This event has the following footnote, which states: "Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility." 7. Attachment 1 - The "Unplanned Control Center evacuation" Event has the word "potential" in the column under "Entity with Reporting Responsibility". The word "potential" should be struck.8. Attachment 2 - Includes "fuel supply emergency", which is not listed on Attachment 1. *The DSR SDT has removed the word "potential" from this event. It now reads as: "Each RC, BA, TOP that experiences the event"*
Response: Thank you for your comment. Please see response above.		
Energy Northwest - Columbia		1. The Loss of Off-site power event criteria is much improved from the last draft of EOP 004-2; however, some clarification is needed to more accurately align with NERC Standard NUC-001 in both nomenclature and intent. Specifically, there are many different configurations supplying offsite power to a nuclear power plant and it is essential that all configurations be accounted for. As identified in the applicability section of NUC-001 the applicable transmission entities may include one or more of the following (TO, TOP, TP, TSP, BA, RC, PC, DP, LSE, and other non-nuclear GO/GOPs). Based on the response to previous comments submitted for Draft 2, Energy Northwest understands that the DSR SDT evaluated the use of the word "source" but dismissed the use in favor of "supply" with the justification "[that] 'supply' encompasses all sources". Energy Northwest suggests that the word

Organization	Yes or No	Question 4 Comment
		"source" is used as the event criteria in EOP-004-2 as this nomenclature is commonly used in the licensing basis of a nuclear power plant. By revising the threshold criteria to "one or more" Energy Northwest believes the concern the DSR SDT noted is addressed and ensures all sources are addressed. In addition, by revising the threshold for reporting to a loss of "one or more" will ensure that all potential events (regardless of configuration of off-site power supplies) will be reported by any applicable transmission entity specifically identified in the nuclear plant site specific NPIRs.Energy Northwest proposes that the loss of an off-site power source be revised to an "unplanned" loss to account for planned maintenance that is coordinated in advance in accordance with the site specific NPIRs and associated Agreements. This will also eliminate unnecessary reporting for planned maintenance.Although the loss of one off-site power source may not result in a nuclear generating unit trip, Energy Northwest agrees that an unplanned loss of an off-site power source regardless of impact should be reported within the 24 hour time limit as proposed. Suggest that the Loss of Offsite power to a nuclear generating plant event be revised as follows:Event: Unplanned loss of any off-site power source to a Nuclear Power PlantEntity with Reporting Responsibility: The applicable Transmission Entity that owns and/or operates the off-site power source to a Nuclear Power Plant as defined in the applicable Nuclear Plant Interface Requirements (NPIRs) and associated Agreements.Threshold for Reporting: Unplanned loss of one or more off-site power sources to a Nuclear Power Plant per the applicable NPIRs. *Based on comments received, this event has been updated within Attachment 1 to read as:* *"Complete loss of off-site power to a nuclear generating plant (grid supply)".* 2. Please consider changing "Operating Plan" with "Procedure(s)". Procedures extend beyond operating groups and provide guidance to the entire company.

Organization	Yes or No	Question 4 Comment
		The DSR SDT intends on keeping "Operating Plan" within EOP-004-2 since NERC has it defined as: *"A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan". As stated, the Operating Plan may contain Operating procedures or Operating Processes. This will give Applicable Entities the greatest flexibility in achieving compliance with this Standard.*
Response: Thank you for your comment. Please see response above.		
Colorado Springs Utilities		Agree with concept to combine CIP-001 into EOP-004. Agree with elimination of "sabotage" concept. Appreciate the attempt to combine reporting requirements, but it seems that in practice will still have separate reporting to DOE and NERC/Regional Entities. EOP-004-2 A.5. "Summary of Key Concepts" refers to Att. 1 Part A and Att. 1 Part B. I believe these have now been combined. EOP-004-2 A.5. "Summary of Key Concepts" refers to development of an electronic reporting form and inclusion of regional reporting requirements. It is unfortunate no progress was made on this front.
Response: Thank you for your comment. The DSR SDT is providing a proposed revision to the NERC Rules of Procedure to address the electronic reporting concept. These proposed revisions will be posted with the standard.		
American Transmission Company, LLC		ATC appreciates the work of the SDT in incorporating changes that the industry had with reporting time periods and aligning this with the Events Analysis Working Group and Department of Energy's OE 417 reporting form.
Response: Thank you for your comment.		

Organization	Yes or No	Question 4 Comment
Manitoba Hydro		Attachment 1 - The term 'Transmission Facilities' used in Attachment 1 is capitalized, but it is not a defined term in the NERC glossary. The drafting team should clarify this issue. *Both Transmission and Facilities are defined terms and the DSR SDT feels this gives sufficient direction.* Attachment 2 - The inclusion of 'Fuel supply emergency' in Attachment 2 creates confusion as it infers that reporting a 'fuel supply emergency' may be required by the standard even though 'fuel supply emergency' is not listed in Attachment 1. On a similar note, it is not clear what the drafting team is hoping to capture by including a checkbox for 'other' in Attachment 2. *The DSR SDT has removed both "fuel supply emergency" and "other" from Attachment 2.*
Response: Thank you for your comment. Please see response above.		
NV Energy		Attachment 1 includes an item "Detection of a reportable cyber security incident." The reporting requirement is a report via Attachment 2 or the OE417 report form submittal. However, under CIP-008, to which this requirement is linked, the reporting is accomplished via NERC's secure CIPIS reporting tool. This appears to be a conflict in that the entity is directed to file reporting under CIP-008 that differs from this subject standard. *CIP-008-4, Requirement 1, Part 1.3 states that an entity must have:* *1.3 Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.*

Organization	Yes or No	Question 4 Comment
		EOP-004-2 also allows for submittal of the report to the ESISAC. Attachment 1 also includes a provision for reporting the "loss of firm load greater than or equal to 15 minutes in an amount of 200MW (or 300MW for peaks greater than 3000MW). This appears to be a rather low threshold, particularly in comparison with the companion loss of generation reporting threshold elsewhere in the attachment. The volume of reports triggered by this low threshold will likely lead to an inordinate number of filed reports, sapping NERC staff time and deflecting resources from more severe events that require attention. I suggest either an increase in the threshold, or the addition of the qualifier "caused by interruption/loss of BES facilities" in this reporting item. This qualifier would therefore exclude distribution-only outages that are not indicative of a BES reliability issue. *The DSR SDT has not modified this event since it is being maintained as it is presently enforceable within EOP-004-1.*
Response: Thank you for your comment. Please see response above.		
BC Hydro		Attachment 1: Reportable Events: BC Hydro recommends further defining "BES equipment" for the events Destruction of BES equipment and Risk to BES equipment. Attachment 1: Reportable Events: BC Hydro recommends defining the Forced intrusion event as the wording is very broad and open to each entities interpretation. What would be a forced intrusion ie entry or only if equipment damage occurs? *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say ' to a Facility', (a defined term) and thresholds have be modified to provide clarity.*

Organization	Yes or No	Question 4 Comment
		The footnote was deleted • *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.* *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.*
Response: Thank you for your comment. Please see response above.		
ISO New England		Attachment 1should be revisited. "Equipment Damage" is overly vague and will also potentially result in reporting on equipment failures which may simply be related to the age and/or vintage of equipment. *The DSR SDT has revised this event based on comments received. The new event is "Damage or destruction of a Facility" which has a threshold of "Damage or destruction of a Facility that:* *Affects an IROL (per FAC-014)* *OR* *Results in the need for actions to avoid an Adverse Reliability Impact* *OR*

Organization	Yes or No	Question 4 Comment
		Results from intentional human action."
Response: Thank you for your comment. Please see response above.		
Constellation Energy on behalf of Baltimore Gas & Electric, Constellation Power Generation, Constellation Energy Commodities Group, Constellation Control and Dispatch, Constellation NewEnergy and Constellation Energy Nuclear Group.		Background Section: The background section in this revision of EOP-004 reads more like guidance than a background of the development of the event reporting standard. Because of the background remains as part of the standard, the language raises questions as to role it plays relative to the standard language. For instance, the Law Enforcement Reporting section states:"Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES." It's not clear how "potential to impact to a wider area of the BES" is defined and where it fits into the standard. As well, and perhaps more problematic, is the Reporting Hierarchy for Reportable Events flow chart. While the flow chart concept is quite useful as a guidance tool, the flow chart currently in the Background raises questions. For instance, the Procedure to Report to Law Enforcement sequence does not map to language in the requirements. Further, Entities would not know about the interaction between law enforcement agencies. *The DSR SDT included the flow chart as an example of how an entity might report and communicate an event. For clarity, we have added the phrase "Example of Reporting Process Including Law Enforcement" to the top of the page.* Please see additional recommended revisions to the requirement language and to the Events Table in the Q2 and Q3 responses. *The DSR SDT has removed the wording of "potential" based on comments received.* Attachment 2: Event Reporting Form: The review of the form is one of the many aspects to compare with the developments within the Events Analysis Process (EAP) developments. We support the effort to create one form for submissions. The

Organization	Yes or No	Question 4 Comment
		recent draft EAP posted as part of Planning Committee and Operating Committee agendas includes a form requiring a few bits of additional relevant information when compared to the EOP-004 form. This may be a valuable approach to avoid follow up inquiries that may result if the form is too limited. We suggest that consideration be given to the proposed EAP form. One specific note on the Proposed EOP-004 Attachment 2: The "Potential event" box in item 3 should be eliminated to track with the removal of the "Risk to the BES" category. *The DSR SDT has updated Attachment 2 to remove potential event and "Risk to the BES" category based on comments received.*
Response: Thank you for your comment. Please see response above.		
Bonneville Power Administration		BPA believes that Attachment 1 has too many added reportable items because unintentional, equipment failure & operational errors are included in the first three items. A. Change to only "intentional human action". Otherwise, the first item "destruction of BES equipment" is too burdensome, along with its short time reporting time: i. - If a single transformer fails that shouldn't require a report. ii.- Emergency actions have to be taken for any failure of equipment, e.g. a loss of line reduces a path SOL and requires curtailments to reduce risk to the system. *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* B. The item for "risk to BES" is not necessary until the suspicious object has been identified as a threat. If what turns out to be air impact wrench left next to BES

Organization	Yes or No	Question 4 Comment
		equipment, that should not be a reportable incident as this current table implies. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.* *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* C. The nuclear "LOOP" should be only reported if total loss of offsite source (i.e. 2 of 2 or 3 of 3) when supplying the plants load. If lightning or insulator fails causing one of the line sources to trip that's not a system disturbance especially if it is just used as a backup. It should only be a NRC process if they want to monitor that. *The DSR SDT has updated this event per your comment, it now reads as: "Complete loss of off-site power to a nuclear generating plant (grid supply)"* The VRF/VSL: BPA believes that the VRF for R2 & R4 should be "Lower". *The DSR SDT has reviewed and updated the two new requirements and believe the VRF's follow the NERC Standard development process.*
Response: Thank you for your comment. Please see response above.		
CenterPoint Energy		CenterPoint Energy appreciates the SDT's consideration of comments and removal of the term, Impact Event. However, the Company still suggests removing the phrase "with the potential to impact" from the purpose as it is vast and vague. An

Organization	Yes or No	Question 4 Comment
		alternative purpose would be "To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of events that impact reliability and their causes if known". The focus should remain on those events that truly impact the reliability of the BES. *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:* *"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."* CenterPoint Energy remains very concerned about the types of events that the SDT has retained in Attachment 1 as indicated in the following comments: Destruction of BES Equipment - The loss of BES equipment should not be reportable unless the reliability of the BES is impacted. *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* Footnote 5, iii should be modified to tie the removal of a piece of equipment from service back to reliability of the BES. Risk to BES equipment: This Event is too vague to be meaningful and should be deleted. The Event should be modified to "Detection of an imminent physical threat to BES equipment". *The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".*

Organization	Yes or No	Question 4 Comment
		Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. *The footnote regarding this event type was expanded to provide additional guidance in:* *"Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* Any reporting time frame of 1 hour is unreasonable; Entities will still be responding to the Event and gathering information. A 24 hour reporting time frame would be more reasonable and would still provide timely information. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.*

Organization	Yes or No	Question 4 Comment
		System Separation: The 100 MW threshold is too low for a reliability impact. A more appropriate threshold is 500 MW. *The DSR SDT has reviewed your request and have determined the event as written "Each separation resulting in an island of generation and load ≥ 100 MW" does impact the reliability of the BES.* Loss of Monitoring or all voice communication capability: The two elements of this Event should be separated for clarity as follows: "Loss of monitoring of Real-Time conditions" and "Loss of all voice communication capability." *The DSR SDT has broken this event down into two distinct events: "Loss of all voice communication capability" and "Complete or partial loss of monitoring capability", per comments received.*
Response: Thank you for your comment. Please see response above.		
Orange and Rockland Utilities, Inc./Consolidated Edison Co. of NY, Inc.		Comments: o Requirement 4 does not specifically state details necessary for an entity to achieve compliance. Requirement 4 should provide more guidance as to what is required in a drill. Audit / enforcement of any requirement language that is too broad will potentially lead to Regional interpretation, inconsistency, and additional CANs. o R4 should be revised to delete the 15 month requirement. CAN-0010 recognizes that entities may determine the definition of annual. *Requirement R4 has been revised as you suggested.* o The Purpose of the Standard should be revised because some of the events being reported on have no impact on the BES. Revise Purpose as follows: To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of [add] "major system events." [delete - "with the potential to impact

Organization	Yes or No	Question 4 Comment
		reliability and their causes, if known, by the Responsible Entities."] *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:* *"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."*
Response: Thank you for your comment. Please see response above.		
Entergy Services		Entergy agrees with and supports comments submitted by the SERC OC Standards Review group.
Response: Thank you for your comment.		
ITC		Footnote 1 and the corresponding Threshold For Reporting associated with the first Event in Attachment 1 are not consistent and thus confusing. Qualifying the term BES equipment through a footnote is inappropriate as it leads to this confusion. For instance, does iii under Footnote 1 apply only to BES equipment that meet i and ii or is it applicable to all BES equipment? *The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.*

Organization	Yes or No	Question 4 Comment
		The footnote regarding this event type was expanded to provide additional guidance in: *"Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* The inclusion of equipment failure, operational error and unintentional human action within the threshold of reporting for "destruction" required in the first 3 Events listed in Attachment 1 is also not appropriate. It is clear through operational history that the intent of the equipment applied to the system, the operating practices and personnel training developed/delivered to operate the BES is to result in reliable operation of the BES which has been accomplished exceedingly well given past history. This is vastly different than for intentional actions and should be excluded from the first 3 events listed in Attachment. To the extent these issues are present in another event type they will be captured accordingly. *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* • *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its*

Organization	Yes or No	Question 4 Comment
		Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples. *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* Footnote 1 should be removed and the Threshold for Reporting associated with the first three events in Attachment 1 should be updated only to include intentional human action. This will also result in including all BES equipment that was intentionally damaged in the reporting requirement and not just the small subset qualified by the existing footnote 1. This provides a much better data sample for law enforcement to make assessments from than the smaller subset qualified by what we believe the intent of footnote 1 is. *The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.* *The footnote regarding this event type was expanded to provide additional guidance in:*

Organization	Yes or No	Question 4 Comment
		"Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."
Response: Thank you for your comment. Please see response above.		
APX Power Markets (NCR-11034)		For Attachment 1 and the events titled "Unplanned Control Center evacuation" and "Loss of monitoring or all voice communication capabiliy".RC, BA, and TOP are the only listed entity types listed for reporting responsibility. We are a GOP that offers a SCADA service in several regions and those type of events could result in a loss of situational awareness for the regions we provide services. I believe the requirement for reporting should not be limited to Entity Type, but on their impact for situational awareness to the BES based on the amount of generation they control (specific to our case), or other criteria that would be critical to the BES (i.e. voltage, frequency). *Note that EOP-008-0 is only applicable to Balancing Authorities, Transmission Operators and Reliability Coordinators, this is the basis for the "Entity with reporting Responsibilities" and reads as" "Each RC, BA, TOP that experiences the event".*
Response: Thank you for your comment. Please see response above.		
ACES Power Marketing Standards Collaborators/ Great River Energy		For many of the events listed in Attachment 1, there would be duplicate reporting the way it is written right now. For example, in the case of a fire in a substation (Destruction of BES equipment), the RC, BA, TO, TOP and perhaps the GO and GOP could all experience the event and each would have to report on it. This seems quite excessive and redundant. We recommend eliminating this duplicate reporting. *The DSR SDT has tried to minimize duplicative reporting, but recognizes there may be*

Organization	Yes or No	Question 4 Comment
		events that trigger more than one report. The current applicability ensures an event that could affect just one of the entities with reporting responsibility isn't missed.
Response: Thank you for your comment. Please see response above.		
Intellibind		I do not see that the rewrite of this standard is meeting the goal of clear reliability standards, and in fact the documents are looking more like legal documents. Though the original EOP-004 and CIP-001 was problematic at times, this rewrite, and the need to have such extensive guidance, attachments, and references for EOP-004-2 will create an even more difficult standard to properly meet to ensure compliance during an audit. Though CIP-001 and EOP-004 were related, combining them in a single standard is not resolving the issues, and is in fact complicating the tasks.Requirements in this standard should deal with only one specific issue, not deal with multiple tasks. I am not sure how an auditor will consistently audit against R2, and how a violation will be categorized when an entity implements all portions of their Operating Plan, however fails to fully address all the requirements in R1, thereby not fully implementing R2, in strict interpretation. *The DSR SDT does not agree that the proposed EOP-004-2 "will create an even more difficult standard to properly meet to ensure compliance during an audit". The DSR SDT main concern is the reporting of events per Attachment 1 is in-line with the Purpose of this Standard that states: "To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities." The NERC Reliability Standards are designed to support the reliability of the BES.* *Requirement R2has been updated to read as: ""R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1." Based on comments received.* The drafting team should not set up a situation where an entity is in double jeopardy for missing an element of a requirement.I also suggest that EOP-004-2 be given a

Organization	Yes or No	Question 4 Comment
		new EOP designation rather than calling it a revision. This way implementation can be better controlled, since most companies have written specific CIP-001 and EOP-004 document that will not simple transfer over to the new version. This standard is a drastic departure from the oringial versions. I appreciate the level of work that is going into EOP-004-2, it appears that significant time and effort has been going into the supporting documentation. It is my opinion that if this much material has to be created to state what the standard really requires, then the standard is flawed. When there are 21 pages of explanation for five requirements, especially when we have previously had 16 pages that originally covered 2 separate reliability standards, we need to reevaluate what we are really doing. *The DSR SDT has revised EOP-004 and CIP-001 using the results based standard development process. This process calls for the drafting team to develop documentation regarding its thoughts during the development process. This allows for a more robust standard which contains background material for an entity to have sufficient guidance to show compliance with the standard.*
Response: Thank you for your comment. Please see response above.		
Imperial Irrigation District		IID strongly believes the reporting flowchart should not be part of a standard. The suggestion is to replace it with a more clear, right to the point requirement. *The DSR SDT has discussed this issue and believes it would be too prescriptive to have a flow chart as a requirement. If desired, an entity can have a flow chart as part of the Operating Plan as stated in Requirement 1.*
Response: Thank you for your comment. Please see response above.		
Illinois Municipal Electric Agency		IMEA appreciates this opportunity to comment. IMEA appreciates the SDT's efforts to simplify reporting requirements by combining CIP-001 with EOP-004. [IMEA encourages NERC to continue working towards a one-stop-shop to simplify reporting on ES-ISAC.] IMEA supports, and encourages SDT consideration of, comments

Organization	Yes or No	Question 4 Comment
		submitted by APPA and Florida Municipal Power Agency.
Response: Thank you for your comment. Please see the responses to the other comments that you mention.		
Westar Energy		In Requirement 1.3, the statement "and the following as appropriate" is vague and subject to interpretation. Who determines what is appropriate? We feel it would be better if the SDT would specify for each event, which party should be notified. *Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to report events. Part 1.2 now reads:* *"1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."*
Response: Thank you for your comment. Please see response above.		
South Carolina Electric and Gas		In terms of receiving reports, is it the drafting teams expectation that separate reports be developed by both the RC and the TOP, GO, BA, etc. for an event that occurs on a company's system that is within the RC's footprint? One by the RC and one by the TOP, GO, BA, etc. In terms of meeting reporting thresholds, is it the drafting teams expectation that the RC aggregate events within its RC Area to determine whether a reporting threshold has been met within its area for the quantitative thresholds? *The DSR SDT has tried to minimize duplicative reporting, but recognizes there may be events that trigger more than one report. The current applicability ensures an event*

Organization	Yes or No	Question 4 Comment
		that could affect just one of the entities with reporting responsibility isn't missed. *It is possible for the Applicable Entities within the Reliability Coordinator's area to be part of a JRO/CFR but this is outside the scope of this Project.*
Response: Thank you for your comment. Please see response above.		
Occidental Power Services, Inc. (OPSI)		Load Serving Entities that do not own or operate BES assets should not be included in the Applicability. In current posting, the SDT states that it includes LSEs based on CIP-002; however, if the LSE does not have any BES assets, CIP-002 should also not be applicable, because the LSE could not have any Critical Assets or Critical Cyber Assets. It is understood that the SDT is trying to comply with FERC Order 693, Section 460 and 461; however, Section 461 also states "Further, when addressing such applicability issues, the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate to address these concerns." A qualifier in the Applicability of EOP-004-2 that would include only LSEs that own or operate BES assets would seem appropriate. The proposed CIP-002 Version V has such a qualifier in that it applies to a "Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: o A UFLS program required by a NERC or Regional Reliability Standard o A UVLS program required by a NERC or Regional Reliability Standard"The SDT should consider the same wording in the Applicability section of EOP-004-2 on order to be consistent with what will become the standing version of CIP-002 (Version 5). *The DSR SDT has "considered" section 460 and 461 of FERC Order 693 and has tried to minimize duplicative reporting, but recognizes there may be events that trigger more than one report. The current applicability ensures an event that could affect just one of the entities with reporting responsibility isn't missed.* *The DSR SDT wishes to draw your attention to section 459 of FERC Order 693 which states: " … an adversary may target a small user, owner or operator because it may*

Organization	Yes or No	Question 4 Comment
		have similar equipment or protections as a larger facility, that is, the adversary may use an attack against a smaller facility as a training 'exercise'".
Response: Thank you for your comment. Please see response above.		
American Electric Power		M4: Recommend removing the text "for events" so that it instead reads "The Responsible Entity shall provide evidence that it verified the communication process in its Operating Plan created pursuant to Requirement R1, Part 1.3."R4: It is not clear to what extent the verification needs to be applied if the process used is complex and includes a variety of paths and/or tasks. The draft team may wish to consider changing the wording to simply state "each Responsible Entity shall test each of the communication paths in the operating plan". We also recommend dropping "once per calendar year" as it is inconstant with the measure itself which allows for 15 months. *The DSR SDT has revised R4 (now R3 and the associated measure M3:* *M3. Each Responsible Entity will have dated and time-stamped records to show that the annual test of Part 1.2 was conducted. Such evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other communication documentation. The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. (R3)*
Response: Thank you for your comment. Please see response above.		
Indiana Municipal Power Agency		Many of the items listed in Attachment 1 are onerous and burdensome when it comes to making judgments or determinations. What one may consider "Risk to BES equipment" another person may not make the same determination. Clarity needs to

Organization	Yes or No	Question 4 Comment
		be added to make the events easier to determine and that will result in less issues when it comes to compliance audits. IMPA does not understand the usage of the terms Critical Asset and Critical Cyber Asset as they will be retired with CIP version 5.IMPA believes the data retention requirements are way too complicated and need to be simplified. It seems like it would be less complicated if one data retention period applied to all data associated with this standard. *The DSR has revised many of the events listed in Attachment 1 to provide clarity. We have also removed the references to Critical Asset and Critical Cyber Asset.* On "public appeal", in the threshold, the descriptor "each" should be deleted, e.g., if a single event causes an entity to be short of capacity, do you really want that entity reporting each time they issue an appeal via different types of media, e.g., radio, TV, etc., or for a repeat appeal every several minutes for the same event? *The DSR SDT has updated the Public Appeal event to read as: "Public appeal for load reduction event" based on comments received.*
Response: Thank you for your comment. Please see response above.		
MidAmerican Energy		MidAmerican proposes eliminating the phrase "with no more than 15 months between reviews" from R1.5. While we agree this is best practice, it creates the need to track two conditions for the review, eliminates flexibility for the responsible entity and does not improve security to the Bulk Electric System. There has not been a directive from FERC to specify the definition of annual within the standard itself. In conjunction with this comment, the Violation Severity Levels for R4 should be revised to remove the references to months. *The DSR SDT has removed this phrase from the requirement (now R3).*

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comment. Please see response above.		
Oncor Electric Delivery Company LLC		NERC's Event Analysis Program tends to parallel many of the reporting requirements as outlined in EOP-004 Version 2. Oncor recommends that NERC considers ways of streamlining the reporting process by either incorporating the Event Analysis obligations into EOP-004-2 or reducing the scope of the Event Analysis program as currently designed to consist only of "exception" reporting. *The DSR SDT has reviewed the Event Analysis Programs criteria. The DSR SDT has determined that Attachment 1 covers the minimum reporting requirements.*
Response: Thank you for your comment. Please see response above.		
Compliance & Responsbility Office		NextEra Energy, Inc. (NextEra) appreciates the DSR SDT revising proposed EOP-004-2, based on the previous comments of NextEra and the stakeholders. NextEra, however, believes that EOP-004-2 needs additional refinement prior to approval. R1.3In R1.3, NextEra is concerned that the term “internal company personnel” is unclear and may be misinterpreted. For example, NextEra does not believe this term should include all company or corporate personnel, or even all personnel in the Responsible Entity’s company or business unit. Instead, the definition of personnel should be limited to those who could be directly impacted by the event or are working on the event. Thus, NextEra suggests that the language in R1.3 be revised to read: “Internal Responsible Entity personnel whose tasks require them to take specific actions to mitigate, stop the spread and/or normalize the event, or personnel who are directly impacted by the event.” NextEra is concerned that R1.3, as written, will be interpreted differently from company to company, region to region, auditor to auditor, and, therefore, may result in considerable confusion during actual events as well as during the audits/stop checks of EOP-004-2 compliance.

Organization	Yes or No	Question 4 Comment
		The DSR SDT has written Requirement R1, Part 1.2 in a way to allow the entity to determine who should receive the communication within your company as stated in your Operating Plan. Also, in R1.3, NextEra is concerned that many of the events listed in Attachment A already must be reported to NERC under its trial (soon to be final) Event Analysis Reporting requirements (Event Analysis). NextEra believes duplicative and different reporting requirements in EOP-004-2 and the Event Analysis rules will cause confusion and inefficiencies during an actual event, which will likely be counterproductive to promoting reliability of the bulk power system. Thus, NextEra believes that any event already covered by NERC's Event Analysis should be deleted from Attachment 1. Events already covered include, for example, loss of monitoring or all voice, loss of firm load and loss of generation. If this approach is not acceptable, NextEra proposes, in the alternative, that the reporting requirements between EOP-004-2 and Event Analysis be identical. For instance, in EOP-004-2, there is a requirement to report any loss of firm load lasting for more than 15 minutes, while the Event Analysis only requires reporting the of loss of firm load above 300 megawatts and lasting more than 15 minutes. Similarly, EOP-004-2 requires the reporting of any unplanned control center evacuation, while the Event Analysis only requires reporting after the evacuation of the control center that lasted 30 minutes or more. Thus, NextEra requests that either EOP-004-2 not address events that are already set forth in NERC's Event Analysis, or, in the alternative, for those duplicative events to be reconciled and made identical, so the thresholds set forth in the Event Analysis are also used in EOP-004-2. *The DSR SDT has worked with the EAWG to develop Attachment 1. At one point they matched. The event for loss of load matches and we revised the "unplanned control center evacuation" event to be for 30 minutes or more.* In addition, NextEra believes that a reconciliation between the language "of recognition" in Attachment 1 and "process to identify" in R1.1 is necessary. NextEra prefers that the language in Attachment 1 be revised to read " . . . of the

Organization	Yes or No	Question 4 Comment
		identification of the event under the Responsible Entity's R1.1 process." For instance, the first event under the "Submit Attachment 2 . . . ." column should read: "The parties identified pursuant to R1.3 within 1 hour of the identification of an event under the Responsible Entity's R1.1 process." This change will help eliminate confusion, and will also likely address (and possibly make moot) many of the footnotes and qualifications in Attachment 1, because a Responsible Entity's process will likely require that possible events are properly vetted with subject matter experts and law enforcement, as appropriate, prior to identifying them as "events". Thus, only after any such vetting and a formal identification of an event would the one hour or twenty-four hour reporting clock start to run. R1.4, R1.5, R3 and R4NextEra is concerned with the wording and purpose of R1.4, R1.5, R3 and R4. *The language was revised in Requirement 1, Part 1.1 to "recognize" based on other comments received.* For example, R1.4 requires an update to the Operating Plan for ". . . any change in assets, personnel, other circumstances . . . ." This language is much too broad to understand what is required or its purpose. Further, R1.4 states that the Operating Plan shall be updated for lessons learned pursuant to R3, but R3 does not address lessons learned. Although there may be lessons learned during a post event assessment, there is no requirement to conduct such an assessment. Stepping back, it appears that the proposed EOP-004-2 has a mix of updates, reviews and verifications, and the implication that there will be lessons learned. Given that EOP-004-2 is a reporting Standard, and not an operational Standard, NextEra is not inclined to agree that it needs the same testing and updating requirements like EOP-005 (restoration) or EOP-008 (control centers). Thus, it is NextEra's preference that R1.4, R1.5 and R4 be deleted, and replaced with a new R1.4 as follows:R1.4 A process for ensuring that the Responsibly Entity reviews, and updates, as appropriate its Operating Plan at least annually (once each calendar year) with no more than 15 months between reviews.If the DSR SDT does not agree with this approach, NextEra, in the alternative, proposes a second approach that consolidates R1.4, R1.5 and R4 in a new R1.4 as follows:R1.4 A process for ensuring that the Responsibly Entity tests

Organization	Yes or No	Question 4 Comment
		and reviews its Operating Plan at least annually (once each calendar year) with no more than 15 months between a test and review. Based on the test and review, the Operating Plan shall be updated, as appropriate, within 90 calendar days. If an actual event occurs, the Responsible Entity shall conduct a post event assessment to identify any lessons learned within 90 calendar days of the event. If the Responsible Entity identifies any lessons learned in post event assessment, the lessons learned shall be incorporated in the Operating Plan within 90 calendar days of the date of the final post event assessment. NextEra purposely did not add language regarding "any change in assets, personnel etc," because that language is not sufficiently clear or understandable for purposes of a mandatory requirement. Although it may be argued that it is a best practice to update an Operating Plan for certain changes, unless the DST SDT can articulate specific, concrete and understandable issues that require an updated Operating Plan prior to an annual review, NextEra recommends that the concept be dropped. *Requirement 1, Part 1.4 was merged with Part 1.5 as well as R4. The resulting requirement is now Requirement 3:* *"Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]* Nuclear Specific ConcernsEOP-004-2 identifies the Nuclear Regulatory Commission (NRC) as a stakeholder in the Reporting Process, but does not address the status of reporting to the NRC in the Event Reporting flow diagram on page 9. Is the NRC considered Law Enforcement as is presented in the diagram? Since nuclear stations are under a federal license, some of the events that would trigger local/state law enforcement at non-nuclear facilities would be under federal jurisdiction at a nuclear site. *The process flowchart is an example of how an entity might operate. If an event requires notification of the NRC, this would be an example of notification of a regulatory authority. It is anticipated that the reporting entity would also notify law*

Organization	Yes or No	Question 4 Comment
		enforcement if appropriate. There are some events listed in Attachment 1 that seem redundant or out of place. For example, a forced intrusion is a one hour report to NERC. However, if there is an ongoing forced intrusion at a nuclear power plant, there are many actions taking place, with the NRC Operations Center as the primary contact which will mobilize the local law enforcement agency, etc. *The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "Any physical threat that could impact the operability of a Facility".* It is unclear that reporting to NERC in one hour promotes reliability or the resolution of an emergency in progress. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.* Also, is there an ability to have the NRC in an emergency notify NERC? The same concerns related to cyber security events.Procedures versus PlanNextEra also suggests replacing "Operating Plan" with "procedures". Given that EOP-004-2 is a reporting Standard and not an operational Standard, it is typical for procedures that address this standard to reside in other departments, such as Information Management and Security. In other words, the procedures needed to address the requirements of EOP-004-2 are likely broader than the NERC-defined Operating Plan.

Organization	Yes or No	Question 4 Comment
		Within your Operating Plan you are required to "report" events to the ERO and your RC and communicate this information (to others) as you define it within your company's Operating Plan. This will allow you to customize any events as you see fit. Clean-Up ItemsIn Attachment 1, Control Centers should be capitalized in all columns so as not to be confused with control rooms. *Since "control center" is not a defined term, it has been revised to lower case.* Also, the final product should clearly state that the process flow chart that is set forth before the Standard is for illustrative purposes, so there is no implication that a Registered Entity must implement multiple procedures versus one comprehensive procedure to address different reporting requirements. *The introduction of the flow chart is clearly marked "Example of Reporting Process including Law Enforcement".*
Response: Thank you for your comment. Please see response above.		
PacifiCorp		No comment.
Arizona Public Service Company		No comments
PPL Electric Utilities and PPL Supply Organizations`		Our comments center around the footnotes and events 'Destruction of BES equipment' and 'Loss of Off-site power to a nuclear generating plant'. We request the SDT consider adding a statement to the standard that acknowledges that not all registered entities have visibility to the information in the footnotes. E.G. Destruction of BES equipment. A GO/GOP does not necessarily know if loss of specific BES equipment would affect any IROL and therefore would not be able to consider this criteria in its reporting decision. Loss of BES equipment would be reported to the BA/RC and the BA/RC would know of an IROL impact and the BA/RC

Organization	Yes or No	Question 4 Comment
		is the appropriate entity to report. We request the SDT consider the information in the footnotes for inclusion in the table directly. Consider Event 'Destruction of BES equipment'. Is footnote 1 a scoping statement? Is it part of the threshold? Is it the impact? Is it defining Destruction? If the BES equipment was destroyed by weather and does not affect an IROL, then is no report is needed? Alternatively, do you still apply the threshold and say it was external cause and therefore report? *Several event categories were removed or combined to improve Attachment 1. The footnotes that you mention were removed and included in the threshold for reporting column. If an entity does not experience an event, then they should not report on it. As you suggest, most GO /GOPs do not see the transmission system. It is anticipated that they will report for events on their Facilities.* We suggest including a flowchart on how to use Attachment 1 with an example. The flowchart would explain the order in which to consider the event and the threshold, and footnotes if they remain. Regarding Attachment 1 Footnote 1 'do not report copper theft...unless it degrades the ability of equipment to operate correctly.', is this defining destruction as not operating correctly ? or is the entirety of footnote 1 a definition of destruction? Regarding Attachment 1 Footnote 1, iii, we request this be changed for consistency with the Event and suggest removing damage from the footnote. i.e. The event is 'destruction' whereas the footnote says 'damaged or destroyed'. The standard does not provide guidance on damage vs destruction which could lead to differing reporting conclusions. Is the reporting line out of service, beyond repair, or is it timeframe based? Regarding Attachment 1 Footnote 2 ' to steal copper... unless it affects the reliability of the BES', is affecting the reliability of the BES a consideration in all the events? PPL believes this is the case and request this statement be made. This could be included in the flowchart as a decision point. Regarding Event 'Loss of Off-site power to a nuclear generating plant', the threshold for reporting does not designate if the off-site loss is planned and/or unplanned - or if the reporting threshold includes the loss of one source of off-site power or is the reporting limited to when all off-site sources are unavailable. PPL recommends the event be 'Total unplanned loss of offsite power to a nuclear generating plant (grid

Organization	Yes or No	Question 4 Comment
		supply)'Thank you for considering our comments. *The SDR SDT discussed "Forced Intrusion" as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.* *The footnote regarding this event type was expanded to provide additional guidance in:* *"Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* *The DSR SDT has updated the Requirements based on comments received along with updating Attachment 1 and 2. Please review the updated standard for all your concerns.*
Response: Thank you for your comment. Please see response above.		
City of Austin dba Austin		Overarching Concern related to EOP-004-2 draft:The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes

Organization	Yes or No	Question 4 Comment
Energy		and CIP Standards Version 5 could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definition of a BES element could change significantly and the concepts of "Critical Assets" and "Critical Cyber Assets" no longer exist in Version 5 of the CIP Standards. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Additionally, it is debatable whether the destruction of, for example, one relay would be a reportable incident given the proposed language. Related to "Reportable Events" of Attachment 1:1. The "Purpose" section of the Standard indicates it is designed to require the reporting of events "with the potential to impact reliability" of the BES. Footnote 1 and the "Threshold for Reporting" associated with the Event described as "Destruction of BES equipment" expand the reporting scope beyond that intent. For example, a fan on a generation unit can be destroyed because a plant employee drops a screwdriver into it. We believe such an event should not be reportable under EOP-004-2. Yet, as written, a Responsible Entity could interpret that event as reportable (because it would be "unintentional human action" that destroyed a piece of equipment associated with the BES). If the goal of the SDT was to include such events, we think the draft Standard goes too far in requiring reporting. If the SDT did not intend to include such events, the draft Standard should be revised to make that fact clear. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT*

Organization	Yes or No	Question 4 Comment
		believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. 2. Item iii) in Footnote 1 seems redundant with the Threshold for Reporting.3. The word "Significantly" in item ii) of footnote 1 introduces an element of subjectivity. What is "significant" to one person may not be significant to someone else.4. The word "unintentional" in Item iii) of footnote 1 may introduce nuisance reporting. The SDT should consider: (1) changing the Event description to "Damage or destruction of BES equipment" (2) removing the footnote and (3) replacing the existing "Threshold for Reporting" with the following language:"Initial indication the event: (i) was due to intentional human action, (ii) affects an IROL or (iii) in the opinion of the Responsible Entity, jeopardizes the reliability margin of the system (e.g., results in the need for emergency actions)" *The SDR SDT revised this event to "Damage or destruction of a Facility" and removed the footnote. The threshold for reporting now reads:* *Damage or destruction of a Facility that:* *Affects an IROL (per FAC-014)* *OR* *Results in the need for actions to avoid an Adverse Reliability Impact* *OR* *Results from intentional human action.* 5. One reportable event is "Risk to the BES" and the threshold for reporting is, "From a non-environmental physical threat." This appears to be intended as a catch-all reportable event. Due to the subjectivity of this event description, we suggest removing it from the list. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical*

Organization	Yes or No	Question 4 Comment
		Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds. 6. One reportable event is "Damage or destruction of Critical Asset per CIP-002." The SDT should define the term "Damage" in order for an entity to determine a threshold for what qualifies as "Damage" to a CA. Normal "damage" can occur on a CA that should not be reportable (e.g. the screwdriver example, above). *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* 7. For the event called "BES Emergency requiring public appeal for load reduction," the SDT should make it clear who should report such an event. For example, in the ERCOT Region, there is a requirement that ERCOT issue public appeals for load reduction (See ERCOT Protocols Section 6.5.9.4). As the draft of EOP-004-2 is currently written, every Registered Entity in the ERCOT Region would have to file a report when ERCOT issues such an appeal. Such a requirement is overly burdensome and does not enhance the reliability of the BES. The Standard should require that the Reliability Coordinator file a report when it issues a public appeal to reduce load. *The DSR SDT has tried to minimize duplicative reporting, but recognizes there may be events that trigger more than one report. The current applicability ensures an event that could affect just one of the entities with reporting responsibility isn't missed.* Reporting Thresholds1. See Paragraph 1 in the "Related to 'Reportable Events' of Attachment 1" section, above. 2. We believe damage or destruction of Critical

Organization	Yes or No	Question 4 Comment
		Assets or CCAs resulting from operational error, equipment failure or unintentional human action should not be reportable under this Standard. We recommend changing the thresholds for "Damage or destruction of Critical Asset..." and "Damage or destruction of a [CCA]" to "Initial Indication the event was due to external cause or intentional human action." 3. We support the SDT's attempted to limit nuisance reporting related to copper thefts. However, a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could clog the reporting process with nuisance reporting and reviewing. An example is the "BES Emergency requiring manual firm load shedding" of â‰¥ 100 MW or "Loss of Firm load for â‰¥ 15 Minutes" that is â‰¥ 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases, those low thresholds would require reporting minor wind events or other seasonal system issues on a local network used to provide distribution service. Firm Load1. The use of the term "Firm load" in the context of the draft Standard seems inappropriate. "Firm load" is not defined in the NERC Glossary (although "Firm Demand" is defined). If the SDT intended to use "Firm Demand," they should revise the draft Standard to use that language. If the SDT wishes to use the term "Firm load" they should define it. [For example, we understand that some load agrees to be dropped in an emergency. In fact, in the ERCOT Region, we have a paid service referred to as "Emergency Interruptible Load Service" (EILS). If the SDT intends that "Firm load" means load other than load which has agreed to be dropped, it should make that fact clear.] *The thresholds and events listed in Attachment 1 are currently required under DOE OE-417 and NERC reporting requirements.* Comments to Attachment 21. The checkbox for "fuel supply emergency" should be deleted because it is not listed as an Event on Attachment 1. *The DSR SDT has removed both "fuel supply emergency" and "other" from Attachment 2.*

Organization	Yes or No	Question 4 Comment
		2. There should be separation between "forced intrusion" and "Risk to BES equipment." They are separate Events on Attachment 1. *Several stakeholders expressed concerns relating to the "Forced Intrusion" event. Their concerns related to ambiguous language in the footnote. The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.* Comments to Guideline and Technical BasisThe last paragraph appears to state NERC will accept an OE-417 form as long as it contains all of the information required by the NERC form and goes on to state the DOE form "may be included or attached to the NERC report." If the intent is for NERC to accept the OE-417 in lieu of the NERC report, this paragraph should be clarified. *The DSR SDT received many comments requesting consistency with DOE OE-417 thresholds and timelines. These items as well as the Events Analysis Working Group's (EAWG) requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across*

Organization	Yes or No	Question 4 Comment
		North America • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use the OE-417 form rather than Attachment 2 to report under EOP-004. The SDT was informed by the DOE of its new online process coming later this year. In this process, entities may be able to record email addresses associated with their Operating Plan so that when the report is submitted to DOE, it will automatically be forwarded to the posted email addresses, thereby eliminating some administrative burden to forward the report to multiple organizations and agencies.*
Response: Thank you for your comment. Please see response above.		
Salt River Project/ Lower Colorado River Authority		Overarching Concern related to EOP-004-2 draft:The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes and CIP Standards Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definition of a BES element could change significantly and the concepts of "Critical Assets" and "Critical Cyber Assets" no longer exist in Version 5 of the CIP Standards. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Additionally, it is debatable whether the destruction of, for example, one relay would

Organization	Yes or No	Question 4 Comment
		be a reportable incident given the proposed language. Related to "Reportable Events" of Attachment 1:1. The "Purpose" section of the Standard indicates it is designed to require the reporting of events "with the potential to impact reliability" of the BES. Footnote 1 and the "Threshold for Reporting" associated with the Event described as "Destruction of BES equipment" expand the reporting scope beyond that intent. For example, a fan on a generation unit can be destroyed because a plant employee drops a screwdriver into it. We believe such an event should not be reportable under EOP-004-2. Yet, as written, a Responsible Entity could interpret that event as reportable (because it would be "unintentional human action" that destroyed a piece of equipment associated with the BES). If the goal of the SDT was to include such events, we think the draft Standard goes too far in requiring reporting. If the SDT did not intend to include such events, the draft Standard should be revised to make that fact clear. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.* 2. Item iii) in Footnote 1 seems redundant with the Threshold for Reporting.3. The word "Significantly" in item ii) of footnote 1 introduces an element of subjectivity. What is "significant" to one person may not be significant to someone else.4. The word "unintentional" in Item iii) of footnote 1 may introduce nuisance reporting. The SDT should consider: (1) changing the Event description to "Damage or destruction of BES equipment" (2) removing the footnote and (3) replacing the

Organization	Yes or No	Question 4 Comment
		existing "Threshold for Reporting" with the following language:"Initial indication the event: (i) was due to intentional human action, (ii) affects an IROL or (iii) in the opinion of the Responsible Entity, jeopardizes the reliability margin of the system (e.g., results in the need for emergency actions)" *The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.* *The footnote regarding this event type was expanded to provide additional guidance in:* *"Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* 5. One reportable event is, "Risk to the BES" and the threshold for reporting is, "From a non-environmental physical threat." This appears to be intended as a catch-all reportable event. Due to the subjectivity of this event description, we suggest removing it from the list. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical*

Organization	Yes or No	Question 4 Comment
		Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds. 6. One reportable event is, "Damage or destruction of Critical Asset per CIP-002." The SDT should define the term "Damage" in order for an entity to determine a threshold for what qualifies as "Damage" to a CA. Normal "damage" can occur on a CA that should not be reportable (e.g. the screwdriver example, above). Reporting Thresholds1. We believe damage or destruction of Critical Assets or CCAs resulting from operational error, equipment failure or unintentional human action should not be reportable under this Standard. We recommend changing the thresholds for "Damage or destruction to Critical Assets ..." and "Damage or destruction of a [CCA]" to "Initial Indication the event was due to external cause or intentional human action." *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* 2. We support the SDT's attempted to limit nuisance reporting related to copper thefts. However, a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could clog the reporting process with nuisance reporting and reviewing. An example is the "BES Emergency requiring manual firm load shedding" of â‰¥ 100 MW or "Loss of Firm load for â‰¥ 15 Minutes" that is â‰¥ 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases, those low thresholds would require reporting minor wind events or other seasonal system issues on a local network used to provide distribution service. Firm Demand1. The use of the term "Firm load" in the context of the draft Standard seems inappropriate.

Organization	Yes or No	Question 4 Comment
		"Firm load" is not defined in the NERC Glossary (although "Firm Demand" is defined). If the SDT intended to use "Firm Demand," they should revised the draft Standard. If the SDT wishes to use the term "Firm load" they should define it. [For example, we understand that some load agrees to be dropped in an emergency. In fact, in the ERCOT Region, we have a paid service referred to as "Emergency Interruptible Load Service" (EILS). If the SDT intends that "Firm load" means load other than load which has agreed to be dropped, it should make that fact clear.] *The thresholds and event types in Attachment 1 are from current DOE OE-417 and NERC reporting requirements.* Comments to Attachment 21. The checkbox for "fuel supply emergency" should be deleted because it is not listed as an Event on Attachment 1. *The DSR SDT has removed both "fuel supply emergency" and "other" from Attachment 2.* 2. There should be separation between "forced intrusion" and "Risk to BES equipment." They are separate Events on Attachment 1. *Several stakeholders expressed concerns relating to the "Forced Intrusion" event. Their concerns related to ambiguous language in the footnote. The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events*

Organization	Yes or No	Question 4 Comment
		meaningful to industry awareness are reported. Comments to Guideline and Technical BasisThe last paragraph appears to state NERC will accept an OE-417 form as long as it contains all of the information required by the NERC form and goes on to state the DOE form "may be included or attached to the NERC report." If the intent is for NERC to accept the OE-417 in lieu of the NERC report, this paragraph should be clarified. *The DSR SDT received many comments requesting consistency with DOE OE-417 thresholds and timelines. These items as well as the Events Analysis Working Group's (EAWG) requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use the OE-417 form rather than Attachment 2 to report under EOP-004. The SDT was informed by the DOE of its new online process coming later this year. In this process, entities may be able to record email addresses associated with their Operating Plan so that when the report is submitted to DOE, it will automatically be forwarded to the posted email addresses, thereby eliminating some administrative burden to forward the report to multiple organizations and agencies.*

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comment. Please see response above.		
Public Utility District No. 1 of Snohomish County/Seattle City Light		Overarching Concern related to EOP-004-2 draft:The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes, as well as the CIP standards Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definitions of a BES element could change significantly and Critical Assets may no longer exist. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* As it relates to the proposed reporting criteria, it is debatable as to whether or not the destruction of, for example, one relay would be a reportable incident under this definition going forward given the current drafting team efforts. Related to "Reportable Events" of Attachment 1:1. A reportable event is stated as, "Risk to the BES", the threshold for reporting is, "From a non-environmental physical threat". This appears to be a catch-all event, and basically every other event in Attachment 1 should be reported because it is a risk to the BES. Due to the subjectivity of this event, suggest removing it from the list. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that*

Organization	Yes or No	Question 4 Comment
		events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. 2. A reportable event is stated as, "Damage or destruction of Critical Asset per CIP-002". The term "Damage" would have to be defined in order for an entity to determine a threshold for what qualifies as "Damage" to a CA. One could argue that normal "Damage" can occur on a CA that is not necessary to report. There should also be caution here in adding CIP interpretation within this standard. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Reporting Thresholds1. The SDT made attempts to limit nuisance reporting related to copper thefts and so on which is supported. However a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could congest the reporting process with nuisance reporting and reviewing. An example is the "BES Emergency requiring manual firm load shedding of greater than or equal to 100 MW or the Loss of Firm load for â‰¥ 15 Minutes that is greater than or equal to 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases these low thresholds represent reporting of minor wind events or other seasonal system issues on Local Network used to provide distribution service. Firm Demand1. The use of Firm Demand in the context of the draft Standards could be used to describe commercial arrangements with a customer rather than a reliability issue. Clarification of Firm Demand would be helpful *The DSR SDT has updated the requirements based on comments received along with updating Attachment 1 and 2. Please review the updated standard for all your*

Organization	Yes or No	Question 4 Comment
		concerns.
Response: Thank you for your comment. Please see response above.		
Pacific Northwest Small Public Power Utility Comment Group		Project 2008-06 proposes to withdraw the terms "Critical Asset" and "Critical Cyber Asset" from the NERC Glossary. In order to avoid a reliability gap when this occurs, we propose including High and Medium Impact BES Cyber Systems and Assets. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* The revised wording to add, "as appropriate" to R1.3 is a concern. We understand the SDT's intent to not require all the bulleted parties to be notified for every event type. But will a good faith effort on the part of the registered entity to deem appropriateness be subject to second guessing and possible sanctions by the Compliance Enforcement Authority if they disagree? We note that CIP-001 required an interpretation to address this issue, but cannot assume that interpretation will carry over. We suggest spelling out exactly who shall deem appropriateness. *The phrase "as appropriate" was removed and Requirement 1, Part 1.2 was revised to:* *A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.* R4 continues to be an onerous requirement for smaller entities. Verification was not

Organization	Yes or No	Question 4 Comment
		part of the SAR and we are not convinced it is needed for reliability. We are unsure how a DP with no generation, no BES assets, no Critical Cyber Assets, and less than 100 MW of load; would meet R4. Shall they drill for impossible events? We ask that R4 be removed. At a minimum it should exclude entities that cannot experience the events of Attachment 1.Entities that cannot experience the events of Attachment 1should likewise be exempt from R1.2, 1.3, R2, and R3. *Requirement R4 (now R3) was revised to :* *Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *Requirement R1, Part 1.1 specifies that an entity must have a process for recognizing "applicable events". An entity is only required to have the Operating Plan as it relates to events applicable to that entity. The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. This language does not preclude the verification of contact information taking place during a training event. The DSR SDT has updated the Requirements based on comments received along with updating Attachment 1 and 2. Please review the updated Standard for all your concerns.*
Response: Thank you for your comment. Please see response above.		
Clallam County PUD No.1		Project 2008-06 proposes to withdraw the terms "Critical Asset" and "Critical Cyber Asset" from the NERC Glossary. In order to avoid a reliability gap when this occurs,

Organization	Yes or No	Question 4 Comment
		we propose including High and Medium Impact BES Cyber Systems and Assets. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* The revised wording to add, "as appropriate" to R1.3 is a concern. We understand the SDT's intent to not require all the bulleted parties to be notified for every event type. But will a good faith effort on the part of the registered entity to deem appropriateness be subject to second guessing and possible sanctions by the Compliance Enforcement Authority if they disagree? We note that CIP-001 required an interpretation to address this issue, but cannot assume that interpretation will carry over. We suggest spelling out exactly who shall deem appropriateness. Part 1.3 (now Part 1.2 was revised to: 1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies. R4 continues to be an onerous requirement for smaller entities. Verification was not part of the SAR and we are not convinced it is needed for reliability. We are unsure how a DP with no generation, no BES assets, no Critical Cyber Assets, and less than 100 MW of load; would meet R4. Shall they drill for impossible events? We ask that R4 be removed. At a minimum it should exclude entities that cannot experience the events of Attachment 1. Entities that cannot experience the events of Attachment 1should likewise be exempt from R1.2, 1.3, R2, and R3. *Part 1.1 has been revised to include "applicable events listed in EOP-004, Attachment*

Organization	Yes or No	Question 4 Comment
		1." If an entity cannot experience an event, then it would not be an applicable event. *Requirement R4 (now R3) has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]* *The DSR SDT envisions that the testing under R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. This language does not preclude the verification of contact information taking place during a training event.*
Response: Thank you for your comment. Please see response above.		
FEUS		R4 requires verification through a drill or exercise the communication process created as part of R1.3. Clarification of what a drill or exercise should be considered. In order to show compliance to R4 would the entity have to send a pseudo event report to Internal Personnel, the Regional Entity, NERC ES-ISAC, Law Enforcement, and Governmental or provincial agencies listed in R1.3 to verify the communications plan? It would not be a burden on the entity so much, however, I'm not sure the external parties want to be the recipient of approximately 2000 psuedo event reports annually. *Requirement R4 (now R3) related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. Requirement R1, R3 now reads: "Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2."The DSR SDT envisions that the testing under Requirement 3 will include*

Organization	Yes or No	Question 4 Comment
		verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. This language does not preclude the verification of contact information taking place during a training event. Attachment 1: BES equipment is too vague - consider changing to BES facility and including that reduces the reliability of the BES in the footnote. Is the footnote an and or an or?Attachment 1: Version 5 of CIP Requirements remove the terms Critical Asset and Critical Cyber Asset. The drafting team should consider revising the table to include BES Cyber Systems. Clarify if Damage or Destruction is physical damage (aka - cyber incidents would be part of CIP-008.) *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Attachment 1: Unplanned Control Center evacuation - remove "potential" from the reporting responsibility *The DSR SDT has removed both "fuel supply emergency" and "other" from Attachment 2.* Attachment 2 - 3: change to, "Did the event originate in your system?" The requirement only requires reporting for Events - not potential events. *The DSR SDT has streamlined Attachment 2, per comments received.*

Organization	Yes or No	Question 4 Comment
		Attachment 2 4: “Damage or Destruction to BES equipment” should be “Destruction of BES Equipment” like it is in Attachment 1 and “forced intrusion risk to BES equipment” remove “risk” *The DSR SDT has streamlined Attachment 2 to reflect the events of Attachment 1, per comments received.*
Response: Thank you for your comment. Please see response above.		
ReliabilityFirst		ReliabilityFirst thanks the SDT for their effort on this project. ReliabilityFirst has a number of concerns/questions related to the draft EOP-004-2 standard which include the following:1. General Comment - The SDT should consider any possible impacts that could arise related to the applicability of Generator Owners that may or may not own transmission facilities. This will help alleviate any potential or unforeseen impacts on these Generator Owners *The DSR SDT cannot apply items such as GO/TO issues when NERC and the Regions are not in agreement to what the issue and solution is.* 2. General Comment - Though the rationale boxes contain useful editorial information for each requirement, they should rather contain the technical rationale or answer the question “why is this needed” for each requirement. The rationale boxes currently seem to contain suggestions on how to meet the requirements. ReliabilityFirst suggests possibly moving some of the statements in the “Guideline and Technical Basis” into the rationale boxes, as some of the rationale seems to be contained in that section. *The DSR SDT will continue to update rationale boxes per comments received.* 3. General comment - The end of Measure M4 is incorrectly pointing to R3. This should refer to R4. *Measurement 4 has been corrected.* 4. General Comment - ReliabilityFirst recommends the “Reporting Hierarchy for

Organization	Yes or No	Question 4 Comment
		Reportable Events" flowchart should be removed from the "Background" section and put into an appendix. ReliabilityFirst believes the flowchart is not really background information, but an outline of the proposed process found in the new standard. *The DSR SDT provided a flow chart for stakeholders to use if desired. EOP-004-2 sets a minimum level of reporting per the events described in Attachment 1. The DSR SDT has received negative feedback in past drafts, the DSR SDT was too prescriptive.* 5. Applicability Comment - ReliabilityFirst questions the newly added applicability for both the Regional Entity (RE) and ERO. Standards, as outlined in many, if not all, the FERC Orders, should have applicability to users, owners and operators of the BES and not to the compliance monitoring entities (e.g. RE and ERO). Any requirements regarding event reporting for the RE and ERO should be dealt with in the NERC Rules of Procedure and/or Regional Delegation Agreements. It is also unclear who would enforce compliance on the ERO if the ERO remains an applicable entity. *The ERO is an Applicable Entity under the current version of CIP-008 and therefore they are held to EOP-004-2. Note, this proposed Standard has been through two Quality Reviews and there has been no rejection from NERC .* 6. Requirement Comment - ReliabilityFirst believes the process for communicating events in Requirement R1, Part 1.3 should be all inclusive and therefore include the bullet points. Bullet points are considered to be "OR" statements and thus ReliabilityFirst believes they should be characterized as sub-parts. Listed below is an example:1.3. A process for communicating events listed in Attachment 1 to the following:1.3.1 Electric Reliability Organization, 1.3.2 Responsible Entity's Reliability Coordinator 1.3.3 Internal company personnel 1.3.4 The Responsible Entity's Regional Entity 1.3.5 Law enforcement 1.3.6 Governmental or provincial agencies *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. Requirement R3 now reads: "Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in*

Organization	Yes or No	Question 4 Comment
		Part 1.2. ". The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. 7. Requirement Comment - ReliabilityFirst questions why Requirement R1, Part 1.1 and Part 1.2 are not required to be verified when performing a drill or exercise in Requirement R4? ReliabilityFirst believes that performing a drill or exercise utilizing the process for identifying events (Part 1.1) and the process for gathering information (Part 1.2) are needed along with the verification of the process for communicating events as listed in Part 1.3. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. Requirement R3 now reads: "Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. ". The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* 8. Compliance Section Comment - Section 1.1 states "If the Responsible Entity works for the Regional Entity..." and ReliabilityFirst questions the intent of this language. ReliabilityFirst is unaware of any Responsible Entities who work for a Regional Entity. Also, if the Regional Entity and ERO remain as applicable entities, in Section 1.1 of

Organization	Yes or No	Question 4 Comment
		the standard, it is unclear who will act as the Compliance Enforcement Authority (CEA). *The DSR SDT has followed the guidance in the Standards Development process to assure that "template" information is correct. The language included is directly from NERC guideline documents* 9. Compliance Section Comment - ReliabilityFirst recommends removing the second, third and fourth paragraphs from Section 1.2 since ReliabilityFirst believes entities should retain evidence for the entire time period since their last audit. *The DSR SDT has followed the guidance in the Standards Development process to assure that "template" information is correct. The language included is directly from NERC guideline documents* 10. Compliance Section Comment - ReliabilityFirst recommends modifying the fifth paragraph from Section 1.2 as follows: "If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or until a data hold release is issued by the CEA." ReliabilityFirst believes, as currently stated, the CEA would be required to retain information for an indefinite period of time. *The DSR SDT has followed the guidance in the Standards Development process to assure that "template" information is correct. The language included is directly from NERC guideline documents.* 11. Compliance Section Comment - ReliabilityFirst recommends removing the sixth paragraph from Section 1.2 since the requirement for the CEA to keep the last audit records and all requested and submitted subsequent audit records is already covered in the NERC ROP. *The DSR SDT has followed the guidance in the Standards Development process to assure that "template" information is correct. The language included is directly from*

Organization	Yes or No	Question 4 Comment
		NERC guideline documents 12. Attachment 1 Comment - It is unclear what the term/acronym "Tv" is referring to. It may be beneficial to include a footnote clarifying what the term "Tv" stands for. *Tv is based on FAC-010 and the DSR SDT believes that this is clear to affected stakeholders.* 13. VSL General Comment - although ReliabilityFirst believes that the applicability is not appropriate, as the REs and ERO are not users, owners, or operators of the Bulk Electric System, the Regional Entity and ERO are missing from all four sets of VSLs, if the applicability as currently written stays as is. If the Regional Entity and ERO are subject to compliance for all four requirements, they need to be included in the VSLs as well. Furthermore, for consistency with other standards, each VSL should begin with the phrase "The Responsible Entity..." *The DSR SDT will follow the guidance in the Standards Development process to assure that "template" information is correct.* 14. VSL 4 Comment - The second "OR" statement under the "Lower" VSL should be removed. By not verifying the communication process in its Operating Plan within the calendar year, the responsible entity completely missed the intent of the requirement and is already covered under the "Severe" VSL category. *The DSR SDT will follow the guidance in the Standards Development process to assure that "template" information is correct.*
Response: Thank you for your comment. Please see response above.		
Northeast Power Coordinating		Requirement 4 does not specifically state the details necessary for an entity to

Organization	Yes or No	Question 4 Comment
Council		achieve compliance. Requirement 4 should provide more guidance as to what is required in a drill. Audit/enforcement of any requirement language that is too broad will potentially lead to Regional interpretation, inconsistency, and additional CANs.R4 should be revised to delete the 15 month requirement. CAN-0010 recognizes that entities may determine the definition of annual.The standard is too specific, and drills down into entity practices, when the results are all that should be looked for.The standard is requiring multiple reports. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. Requirement R3 now reads: "Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. ". The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* The Purpose of the Standard is very broad and should be revised because some of the events being reported on have no impact on the BES. Revise Purpose wording as follows: To improve industry awareness and the reliability of the Bulk Electric System "by requiring the reporting of major system events with the potential to impact reliability and their causes..." on the Bulk Electric System it can be said that every event occurring on the Bulk Electric System would have to be reported. *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:* *"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."*

Organization	Yes or No	Question 4 Comment
		Referring to Requirement R4, the testing of the communication process is the responsibility of the Responsible Entity. There is an event analysis process already in place.The standard prescribes different sets of criteria, and forms.There should be one recipient of event information. That recipient should be a "clearinghouse" to ensure the proper dissemination of information. *EOP-004 is a standard that requires reporting of events to the ERO. The events analysis program receives these reports and determines whether further analysis is appropriate.* Why is this standard applicable to the ERO? *NERC as the ERO is currently a Responsible Entity under CIP-008, and therefore the proposed EOP-004-2 has the ERO as a Responsible Entity.* Requirement R2 is not necessary. It states the obvious.Requirements R2 and R3 are redundant.The standard mentions collecting information for Attachment 2, but nowhere does it state what to do with Attachment 2. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to:* *"Requirement R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."*

Organization	Yes or No	Question 4 Comment
		None of the key concepts identified on page 5 of the standard are clearly stated or described in the requirements: o Develop a single form to report disturbances and events that threaten the reliability of the bulk electric system. *OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.* o Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements. o Establish clear criteria for reporting. o Establish consistent reporting timelines. *The DSR SDT does allow entities to use the DOE Form OE 417 in lieu of Attachment 2 to report an event. Attachment 1 has been updated to provide consistent criteria for reporting as well as reporting timelines. All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:*

Organization	Yes or No	Question 4 Comment
		"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..." *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.* o Provide clarity for who will receive the information and how it will be used. The standard's requirements should be reviewed with an eye for deleting those that are redundant, or do not address the Purpose or intent of the standard. *Requirement R1 has been updated and now reads as"* *Each Responsible Entity shall have an Operating Plan that includes:* *1.1. A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.* *The Applicable Entity's Operating Plan is to contain the process for reporting events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and for communicating to others as defined in the Responsible Entity's Operating Plan. All events in Attachment 1 are required to be reported to the Electric Reliability Organization and the Responsible Entity's Reliability Coordinator. The Operating Plan may include: internal company personnel, your Regional Entity, law enforcement, and governmental or provisional agencies, as you identify within your Operating Plan. This gives you the flexibility to tailor your Operating Plan to fit your*

Organization	Yes or No	Question 4 Comment
		company's needs and wants.
Response: Thank you for your comment. Please see response above.		
American Public Power Association		Requirement R1:1.3. A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate: o Internal company personnel o The Responsible Entity's Regional Entity o Law enforcement o Governmental or provincial agencies APPA believes that including the list of other entities needing to be included in a process for communicating events under 1.3 may open this requirement up for interpretation. APPA requests that the SDT remove from the requirement the listing of; "Internal company personnel, The Responsible Entity's Regional Entity, Law enforcement & Governmental or provincial agencies" and include these references in a guidance document. The registered entities need to communicate with the ERO and the RC if applicable for compliance with this standard and to maintain the reliability of the BES. Communication with other entities such as internal company personnel, law enforcement and the Regional Entity are expected, but do not impact the reliability of the BES. This will simplify the reporting structure and will not be burdensome to registered entities when documenting compliance. If this is not an acceptable solution, APPA suggests revising 1.3 to remove the wording "the following as appropriate" and add "other entities as determined by the Responsible Entity. Examples of other entities may include, but are not limited to:" Then it is clear that the list is examples and should not be enforced by the auditor. *Requirement R1 has been updated and now reads as* *"Each Responsible Entity shall have an Operating Plan that includes:* *1.1. A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004*

Organization	Yes or No	Question 4 Comment
		Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies. *The Applicable Entity's Operating Plan is to contain the process for reporting events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and for communicating to others as defined in the Responsible Entity's Operating Plan. All events in Attachment 1 are required to be reported to the Electric Reliability Organization and the Responsible Entity's Reliability Coordinator. The Operating Plan may include: internal company personnel, your Regional Entity, law enforcement, and governmental or provisional agencies, as you identify within your Operating Plan. This gives you the flexibility to tailor your Operating Plan to fit your company's needs and wants.* 1.4. Provision(s) for updating the Operating Plan within 90 calendar days of any change in assets, personnel, other circumstances that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3. APPA understands that the SDT is following the FERC order requiring a 90 day limit on updates to any changes to the plan. However, APPA believes that "updating the Operating Plan within 90 calendar days of any change..." is a very burdensome compliance documentation requirement. APPA reminds the SDT that including DPs in this combined standard has increased the number of small Responsible Entities that will be required to document compliance. APPA requests that the SDT combine requirement 1.4 and 1.5 so the Operating Plan will be reviewed and updated with any changes on a yearly basis. If this is not an acceptable solution, APPA suggests that the "Lower VSL" exclude a violation to 1.4. The thought being, a violation of 1.4 by itself is a documentation error and should not be levied a penalty. *Requirement 1, Part 1.4 has been removed from the standard.* Attachment 1: Events TableAPPA believes that the intent of the SDT was to mirror the DOE OE-417 criteria in reporting requirements. With the inclusion of DP in the

Organization	Yes or No	Question 4 Comment
		Applicability, however, APPA believes the SDT created an unintended excessive reporting requirement for DPs during insignificant events. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.* APPA recommends that a qualifier be added to the events table. In DOE OE-417 local electrical systems with less than 300MW are excluded from reporting certain events since they are not significant to the BES. APPA believes that the benefit of reporting certain events on systems below this value would not outweigh the compliance burden placed on these small systems. Therefore, APPA requests that the standard drafting team add the following qualifier to the Events Table of Attachment 1: "For systems with greater than 300MW peak load." This statement should be placed in the Threshold for Reporting column for the following Events: BES Emergency requiring appeal for load reduction, BES

Organization	Yes or No	Question 4 Comment
		Emergency requiring system-wide voltage reduction, BES Emergency requiring manual firm load shedding, BES Emergency resulting in automatic firm load shedding. This will match the DOE OE-417 reporting criteria and relieve the burden on small entities. *Upon review of the DOE OE 417, it states "Local Utilities in Alaska, Hawaii, Puerto Rico, the U.S. Virgin Islands, and the U.S. Territories - If the local electrical system is less than 300 MW, then only file if criteria 1, 2, 3 or 4 are met". Please be advised this exception applies to entities outside the continental USA.* *The DSR SDT has tried to minimize duplicative reporting, but recognizes there may be events that trigger more than one report. The current applicability ensures an event that could affect just one of the entities with reporting responsibility isn't missed.* Definition of "Risk to BES equipment":The SDT attempted to give examples of the Event category "Risk to BES equipment" in a footnote. This footnote gives the Responsible Entity and the Auditor a lot of room for interpretation. APPA suggests that the SDT either define this term or give a triggering mechanism that the industry would understand. One suggestion would be "Risk to BES equipment: An event that forces a Facility Owner to initiate an unplanned, non-standard or conservative operating procedure." Then list; "Examples include train derailment adjacent to BES Facilities that either could have damaged the equipment directly or has the potential to damage the equipment..." This will allow the entity to have an operating procedure linked to the event. If this suggestion is taken by the SDT then the Reporting column of Attachment 1 needs to be changed to: "The parties identified pursuant to R1.3 within 1 hour of initiating conservative operating procedures." *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and*

Organization	Yes or No	Question 4 Comment
		determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.
Response: Thank you for your comment. Please see response above.		
Western Electricity Coordinating Council		Results-based standards should include, within each requirement, the purpose or reason for the requirement. The requirements of this standard, while we support the requirements, do not include the goal or proupose of meeting each stated requirement. The Measures all include language stating "the responsible entity shall provide...". During a quality review of a WECC Regional Reliability Standard we were told that the "shall provide" language is essentially another requirement to provide something. If it is truly necessary to provide this it should be in the requirements. It was suggested to us that we drop the "shall provide" language and just start each Measure with the "Evidence may include but is not limited to...". *The DSR SDT changed each instance of "shall" to "will" within the measures. We will defer to NERC Quality Review comments for any additional revisions.*
Response: Thank you for your comment. Please see response above.		
Sacramento Municipal Utility District (SMUD)		SMUD and BANC agree with the revised language in EOP-004-1 requirements, but we have identified the following issues in A-1:We commend the SDT for properly addressing the sabotage issue. However, additional confusion is caused by introducing term "damage". As "damage" is not a defined term it would be beneficial for the drafting team to provide clarification for what is meant by "damage".

Organization	Yes or No	Question 4 Comment
		The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows: • *The 'Damage or Destruction' event category has been revised to say ' to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* • *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.* *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* *As discussed in prior comment forms, the DSR SDT has elected not to define "sabotage". As defined in an Entity's operating Plan, the requirement is to report and communicate an event as listed in Attachment 1. EOP-004-2 does not require analysis of any event listed in Attachment 1.* The threshold for reporting "Each public Appeal for load reduction" should clearly state the triggering is for the BES Emergency as routine "public appeal" for conservation could be considered a threshold for the report triggering. *To clarify your point, the threshold has been changed to 'Public appeal or load reduction event'.*

Organization	Yes or No	Question 4 Comment
		Regarding the SOL Violations in Attachment 1 the SOL Violations should only be those that affect the WECC paths. *The DSR SDT has included the following language for WECC's SOL violation in Attachment 1:* *"IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only)"* The SDT made attempts to limit nuisance reporting related to copper thefts and so on which is supported. However a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could congest the reporting process with nuisance reporting and reviewing. *The DSR SDT made reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary.*
Response: Thank you for your comment. Please see response above.		
Southern Comnpany		Southern has the following comments:(1) In Requirement R1.4, we request the SDT to clarify what is meant by the term "assets"? *The DSR SDT has deleted Requirement R1, Part 1.4, thus "assets" is not contained in EOP-004-2 based on comments received.* 2) If requirement 4 is not deleted, should we have to test every possible event described in our Operating Plan or each event listed in Attachment 1 to verify communications? *The DSR SDT has deleted Requirement R4 based on comments received.* (3) In the last paragraph of the "Summary of Key Concepts" section on page 6 of

Organization	Yes or No	Question 4 Comment
		Draft 3, there is a statement that "Real-time reporting is achieved through the RCIS..." The only reporting required on RCIS by the Standards is for EEAs and TLRs. Please review and modify this language as needed. *The DSR SDT believes "The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting" is correct.* (4) Evidence Retention (page 12 of Draft 3): The 3 calendar year reference has no bearing on a Standard that may be audited on a cycle greater than 3 years. *The DSR SDT has updated the Evidence Retention section with standard language provided by NERC staff.* (5) In the NOTE for Attachment 1 (page 20 of Draft 3), what is meant by "periodic verbal updates" and to whom should the updates be made? *The DSR SDT has updated the note in question to remove the language of "periodic verbal updates", it now reads as:* *"NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per R1 and provide as much information as is available at the time of the notification. Reports to the ERO should be submitted to one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422."* (6) There are Prerequisite Approvals listed in the Implementation Plan. Is it appropriate to ask industry to vote on this Standard Revision that has a prerequisite approval of changes in the Rules of Procedure that have not been approved? *The proposed revisions to the Rules of Procedure should have been posted with the*

Organization	Yes or No	Question 4 Comment
		standard. This posting will occur with the successive ballot of EOP-004-2. (7) We believe the reporting of the events in Attachment 1 has no reliability benefit to the Bulk Electric System. We suggest that Attachment 1 should be removed. *The DSR SDT disagrees with this comment. Attachment 1 is the minimum set of events that will be required to report and communicate per your Operating Plan will be aware of system conditions.*
Response: Thank you for your comment. Please see response above.		
Texas Reliability Entity		Substantive comments:1.ERO and Regional Entities should not be included in the Applicability of this standard. Just because they may be subject to some CIP requirements does not mean they also have to be included here. The ERO and Regional Entities do not operate equipment or systems that are integral to the operation of the BES. Also, none of the VSLs apply to the ERO or to Regional Entities. *The DSR SDT is following guidance that NERC has provided to the DSR SDT. The ERO and the RE are applicable entities under CIP-008. Reporting of Cyber Security Incidents is the responsibility of the ERO and the RE.* 2.The first entry in the Events Table should say "Damage or destruction of BES equipment." Equipment may be rendered inoperable without being "destroyed," and entities should not have to determine within one hour whether damage is sufficient to cause the equipment to be considered "destroyed." Footnote 1 refers to equipment that is "damaged or destroyed." *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity.* *The DSR SDT used the defined term "Facility" to add clarity for several events listed in*

Organization	Yes or No	Question 4 Comment
		Attachment 1. A Facility is defined as: *"A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"* *The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.* 3.In the Events Table, consider whether the item for "Voltage deviations on BES facilities" should also be applicable to GOPs, because a loss of voltage control at a generator (e.g. failure of an automatic voltage regulator and power system stabilizer) could have a similar impact on the BES as other reportable items. *The DSR SDT disagrees with this comment. Attachment 1 is the minimum set of events that will be required to report and communicate per your Operating Plan will be aware of system conditions.* 4.In the Events Table, under Transmission Loss, does this item require that at least three Facilities owned by one entity must be lost to trigger the reporting requirement, or is the reporting requirement also to be triggered by loss of three Facilities during one event or occurrence that are owned by two or three different entities? *The DSR SDT has stated in Attachment 1 that "Each TOP that experiences the transmission loss". This would mean per individual TOP.* 5.In the Events Table, under Transmission Loss, it is unclear how Facilities are to be counted to determine when "three or more" Facilities are lost. In the NERC Glossary, Facility is ambiguously defined as "a set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In many cases, a "set of electrical equipment" can be selected and counted in different ways, which makes this item ambiguous.

Organization	Yes or No	Question 4 Comment
		Both Transmission and Facilities are defined terms and the DSR SDT feels this gives sufficient direction. 6.In the Events Table, under Transmission Loss, it appears that a substation bus failure would only count as a loss of one Facility, even though it might interrupt flow between several transmission lines. We believe this type of event should be reported under this standard, and appropriate revisions should be made to this entry. *The DSR SDT used the defined term "Facility" to add clarity for this event as well as other events in Attachment 1. A Facility is defined as:* *"A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"* *The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.* 7.In the Events Table, under Transmission Loss, consider including generators that are lost as a result of transmission loss events when counting Facilities. For example, if a transmission line and a transformer fail, resulting in a generator going off-line, that should count as a loss of "three or more" facilities and be reportable under this standard. *Attachment 1 is the minimum set of events that will be required to report and communicate per your Operating Plan will be aware of system conditions.* 8.In the Events Table, under "Unplanned Control Center evacuation" and "Loss of monitoring or all voice communication capability," GOPs should be included. GOPs also operate control centers that would be subject to these kinds of occurrences. *Attachment 1 is the minimum set of events that will be required to report and*

Organization	Yes or No	Question 4 Comment
		communicate per your Operating Plan will be aware of system conditions. 9.In the Events Table, under "Loss of monitoring or all voice communication capability," we suggest adding that if there is a failure at one control center, that event is not reportable if there is a successful failover to a backup system or control center. *The DSR SDT has split this event into two separate events based on comments received, it now reads as: "Loss of all voice communication capability" and "Complete or partial loss of monitoring capability".* 10."Fuel supply emergency" is included in the Event Reporting Form, but not in Attachment 1, so there is no reporting threshold or deadline provided for this type of event. *Attachment 2 was updated to reflect the revisions to Attachment 1. The reference to "actual or potential events" was removed. Also, the event type of "other" and "fuel supply emergency" was removed as well.* Clean-up items:1.In R1.5, capitalize "Responsible Entity" and lower-case "process". *The DSR SDT has deleted Requirement 1, part 1.5.* 2.In footnote 1, add "or" before "iii)" to clarify that this event type applies to equipment that satisfies any one of these three conditions. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* 3.In the Event Reporting Form, "forced intrusion" and "Risk to BES equipment" are run together and should be separated. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new*

Organization	Yes or No	Question 4 Comment
		event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. VSLs:1.We support the substance of the VSLs, but the repeated long list of entities makes the VSLs extremely difficult to read and decipher. The repeated list of entities should be replaced by "Responsible Entities." 2.If the ERO and Regional Entities are to be subject to requirements in this standard (which we oppose), they need to be added to the VSLs. *The DSR SDT has revised the VSLs to eliminate the list of entities and lead with "Responsible Entity".*
Response: Thank you for your comment. Please see response above.		
		Suggest removing 1.4 since 1.5 ensures a annual review. . The implementation of the plan should also include the necessary reporting. *Requirement R1, Part 1.4 has been removed.*
Response: Thank you for your comment. Please see response above.		
Electric Compliance		The concepts of "Critical Assets" and "Critical Cyber Assets" no longer exist in Version 5 of the CIP Standards and so this may cause confusion. Recommend modifying to be in accordance with Version 5. Additionally, it is debatable whether the

Organization	Yes or No	Question 4 Comment
		destruction of, for example, one relay would be a reportable incident given the proposed language. We recommend modifying the language to insure nuisance reporting is minimized. One reportable event is, "Risk to the BES" and the threshold for reporting is, "From a non-environmental physical threat." This appears to be a catch-all reportable event. Due to the subjectivity of this event description, we suggest removing it from the list. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as stakeholders pointed out that these events were adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility "reporting thresholds. CIP-008 addresses Cyber Security Incidents which are defined as:* *"Any malicious act or suspicious event that:* *• Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,* *• Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset."* *A Critical Asset is defined as:* *"Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."* *Since there is an existing event category for damage or destruction of Facilities, having a separate event for "Damage or Destruction of a Critical Asset" is unnecessary.* Footnote 1 and the "Threshold for Reporting" associated with the Event described as "Destruction of BES equipment" expand the reporting scope. For example, a fan on a

Organization	Yes or No	Question 4 Comment
		transformer can be destroyed because a technician drops a screwdriver into it. We believe such an event should not be reportable under EOP-004-2. Yet, as written, a Responsible Entity could interpret that event as reportable (because it would be "unintentional human action" that destroyed a piece of equipment associated with the BES). If the goal of the SDT was to include such events, we think the draft Standard goes too far in requiring reporting. If the SDT did not intend to include such events, the draft Standard should be revised to make that fact clear. Proposed Footnote: BES equipment that become damaged or destroyed due to intentional or unintentional human action which removes the BES equipment from service that i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii). Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative). *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* The word "Significantly" in item ii) of footnote 1 and "as appropriate" in section 1.3 introduces elements of subjectivity. What is "significant" or "appropriate" to one person may not be to someone else. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* In section 1.4, we believe that revising the plan within 90 days of "any" change should be changed to 180 days or else classes of events should be made so that only

Organization	Yes or No	Question 4 Comment
		substantial changes are required to made within the 90 day timeframe. *Requirement R1, Part 1.4 was removed from the standard.*
Response: Thank you for your comment. Please see response above.		
Georgia System Operations Corporation		The ERO and the Regional Entity should not be listed as Responsible Entities. The ERO and the Regional Entity should not have to meet the requirements of this standard, especially reporting to itself. *The ERO and the RE are applicable under the CIP-008 standard and are therefore applicable under EOP-004.* Attachment 1 (all page numbers are from the clean draft):Page 20, destruction of BES equipment: part iii) of the footnote adds damage as an event but the heading is for destruction. Is it just for destruction? Or is it for damage or destruction? *The DSR SDT has modified Attachment 1 to bring more clarity. The 'Destruction' event category has been revised to include damage or destruction of a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* Page 21, Risk to BES equipment: Footnote 3 gives an example where there is flammable or toxic cargo. These are environmental threats. However, the threshold for reporting is for non-environmental threats. Which is it? *For this event, environmental threats are considered to be severe weather, earthquakes, etc. rather than an external threat.* Page 21, BES emergency requiring public appeal for load reduction: A small deficient

Organization	Yes or No	Question 4 Comment
		entity within a BA may not initiate public appeals. The BA is typically the entity which initiates public appeals when the entire BA is deficient. The initiating entity should be the responsible entity not the deficient entity. *The DSR SDT revised this event to indicate the "initiating" entity is responsible for reporting.* Page 21, BES emergency requiring manual firm load shedding: If a RC directs a DP to shed load and the DP initiates manually shedding its load as directed, is the RC the initiating entity? Or is it the DP? *The DSR SDT believes the wording of "initiating entity" provides enough clarity for each applicable entity to understand. In this case, the RC made the call to shed load and therefore should report.* Page 22, system separation (islanding): a DP does not have a view of the system to see that the system separated or how much generation and load are in the island. Remove DP. *The DSR SDT disagrees with your comment. DP's may be the first to recognize that they are islanded or separated from the system.* Attachment 2 (all page numbers are from the clean draft):Page 25: fuel supply emergencies will no longer be reportable under the current draft. *The DSR SDT has removed both "fuel supply emergency" and "other" from Attachment 2 based on comments received.* Miscellaneous typos and quality issues (all page numbers are from the clean draft):Page 5, the last paragraph: There are two cases where Parts A or B are referred to. Attachment 1 no longer has two parts (A & B).Page 27, Discussion of Event Reporting: the second paragraph has a typo at the beginning of the sentence.

Organization	Yes or No	Question 4 Comment
		The DSR SDT has corrected these typos.
Response: Thank you for your comment. Please see response above.		
Thompson Coburn LLP on behalf of Miss. Delta Energy Agency		The first three incident categories designated on Attachment 1 as reportable events should be modified. As the Standard is current drafted, each incident category (i.e., destruction of BES equipment, damage or destruction of Critical Assets, and damage or destruction of Critical Cyber Assets) requires reporting if the event was due to unintentional human action. For example, under the reporting criteria as drafted, inadvertently dropping and damaging a piece of computer equipment designated as a Critical Cyber Asset while moving or installing it would appear to require an event report within an hour of the incident. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as stakeholders pointed out that these events were adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility "reporting thresholds. CIP-008 addresses Cyber Security Incidents which are defined as:* *"Any malicious act or suspicious event that:* *• Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,* *• Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset."* *A Critical Asset is defined as:* *"Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."*

Organization	Yes or No	Question 4 Comment
		Since there is an existing event category for damage or destruction of Facilities, having a separate event for "Damage or Destruction of a Critical Asset" is unnecessary. MDEA requests that the Drafting Team consider modifying footnote 1 and each of the first three event categories to reflect that reportable events include only those that (i) affect an IROL; (ii) significantly affect the reliability margin of the system; or (iii) involve equipment damage or destruction due to intentional human action that results in the removal of the BES equipment, Critical Assets, and/or Critical Cyber Assets, as applicable, from service. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* Footnote 2 (which now pertains only to the fourth incident category - forced intrusions) should also apply to the first three event categories. Specifically, responsible entities should report intentional damage or destruction of BES equipment, damage or destruction of Critical Assets, and damage or destruction of Critical Cyber Assets if either the damage/destruction was clearly intentional or if motivation for the damage or destruction cannot reasonably be determined and the damage or destruction affects the reliability of the BES. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* Attachment 1 is also unclear to the extent that the incident category involving reports for the detection of reportable Cyber Security Incidents includes a reference to CIP-008 as the reporting threshold. While entities in various functional categories

Organization	Yes or No	Question 4 Comment
		(i.e., RCs, BAs, TOPs/TOs, GOPs/GOs, and DPs) are listed as being responsible for the reporting of such events, some entities in these functional categories may not currently be subject to CIP-008. If it is the Drafting Team's intent to limit event reports for Cyber Security Incidents to include only registered entities subject to CIP-008, that clarification should be incorporated into the listing of entities with reporting responsibility for this incident category in Attachment 1. *The "Entity with reporting responsibility" for the event "A reportable Cyber Security Incident" has been revised to "Each Responsible Entity applicable under CIP-008-4 or its successor that experiences the Cyber Security Incident".*
Response: Thank you for your comment. Please see response above.		
Luminant Power		The following comments all apply to Attachment 1: o As a general comment, SDT should specifically list the entities the reportable event applies to in the table for clarity. Do not use general language referencing another standard or statements such as "Deficient entity is responsible for reporting", "Initiating entity is responsible for reporting", or other similar statements used currently in the table. This leaves this open and subject to interpretation. *The DSR SDT disagrees with your comment. This language provides the most flexibility for applicable entities and maintains a minimum level of who is required to report or communicate events based an entity's Operating Plan, as described in Requirement 1.* Also, there are a number of events that do not apply to all entities. o Destruction of BES equipment should be Intentional Damage or Destruction of BES equipment. Unintentional actions occur and should not be a requirement for reporting under disturbance reporting. *The event for "Destruction of BES equipment" has been revised to "Damage or destruction of a Facility". The threshold for reporting information was expanded for*

Organization	Yes or No	Question 4 Comment
		clarity: *"Damage or destruction of a Facility that: affects an IROL* *OR* *Results in the need for actions to avoid an Adverse Reliability Impact* *OR* *Results from intentional human action."* o Actions or situations affecting equipment or generation unit availability due to human error, equipment failure, unintentional human action, external cause, etc. are reported in real time to the BA and other entities as required by other NERC Standards. Disturbance reporting should avoid the type of events that, for instance, would cause the total or partial loss of a generating unit under normal operational circumstances. There are a number of issues with the table in this regard. *The DSR SDT has removed such language based on comments received.* o For clarity, consider changing the table to identify for each event type "who" should be notified. This appears to be missing from the table overall. *The DSR SDT has updated Requirement R1, Part 1.2 to read as: ""1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."* o Reportable Events, the meaning for the Event labeled "Destruction of BES equipment" is not clear. Footnote 1 adds the language "iii) Damaged or destroyed due to intentional or unintentional human action which removes the BES equipment

Organization	Yes or No	Question 4 Comment
		from service." This language can be interpreted to mean that any damage to any BES equipment caused by human action, regardless of intention, must be reported within 1 hour of recognition of the event. This requirement will be overly burdensome. If this is not the intent of the definition of "Destruction of BES equipment", the footnote should be re-worded. As such, it is subjective and left open to interpretation. It should focus only on intentional actions to damage or interrupt BES functionality. It should not be worded as such that every item that trips a unit or every item that is damaged on a unit requires a report. That is where the language right now is not clear. There are and will continue to be unintentional human error that results in taking equipment out of service. This standard was meant to replace sabotage reporting. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* o Damage or destruction of Critical Asset per CIP-002 and Damage or destruction of a Critical Cyber Asset per CIP-002 should be removed from the table as Intentional Damage or Destruction of BES equipment would cover this as well. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as stakeholders pointed out that these events were adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility "reporting thresholds. CIP-008 addresses Cyber Security Incidents which are defined as:* *"Any malicious act or suspicious event that:* *• Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,* *• Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber*

Organization	Yes or No	Question 4 Comment
		Asset." *A Critical Asset is defined as:* *"Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."* *Since there is an existing event category for damage or destruction of Facilities, having a separate event for "Damage or Destruction of a Critical Asset" is unnecessary.* o Risk to BES equipment should be removed from the table as it is very subjective and broad. At a minimum, the 1 hour reporting timeline should begin after recognition and assessment of the incident. As an example, a fire close to BES equipment may not truly be a threat to the equipment and will not be known until an assessment can be made to determine the risk. *The DSR SDT has removed this event based on comments received.* o Detection of a Reportable Cyber Security incident should be removed from the table as this is covered by CIP-008 requirements. Having this in two separate standards is double jeopardy and confusing to entities. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as stakeholders pointed out that these events were adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility "reporting thresholds. CIP-008 addresses Cyber Security Incidents which are defined as:* *"Any malicious act or suspicious event that:*

Organization	Yes or No	Question 4 Comment
		• Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, *• Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset."* *A Critical Asset is defined as:* *"Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."* *Since there is an existing event category for damage or destruction of Facilities, having a separate event for "Damage or Destruction of a Critical Asset" is unnecessary.* o Generation Loss event reporting should only apply to the BA. These authorities have the ability and right to contact generation resources to supply necessary information needed for reporting. This would also eliminate redundant reporting by multiple entities for the same event. *The DSR SDT has tried to minimize duplicative reporting, but recognizes there may be events that trigger more than one report. The current applicability ensures an event that could affect just one of the entities with reporting responsibility isn't missed.* o Suggest that Generation Loss MW loss would match up with the 1500 MW level identified in CIP Version 4 or Version 5 for consistency between future CIP standards and this disturbance reporting standard. This would then cover CIP and significant MW losses that should be reported. *The DSR SDT disagrees as this threshold is based on the current EOP-004-1.* o The Generation Loss MW loss amount needs to have a time boundary. Luminant

Organization	Yes or No	Question 4 Comment
		would suggest a loss of 1500 MW within 15 minutes. *The DSR SDT disagrees as this threshold is based on the current EOP-004-1.* o Unplanned Control Center evacuation should not apply to entities that have backup Control Centers where normal operations can continue without impact to the BES. *The DSR SDT disagrees with your comment. By reporting and communicating per an entity's Operating Plan, you will provide situational awareness to entities per your Operating Plan.* o Loss of monitoring or all voice communication capability should be separated. Also the 24 hour reporting requirement may not be feasible if communications is down for longer than 24 hours. *The DSR SDT has split this event into two separate events based on comments received, it now reads as: "Loss of all voice communication capability" and "Complete or partial loss of monitoring capability".* Luminant would suggest removal of the communication reporting event as there are a number of things that could cause this to occur for longer than the reporting requirement allows, thus putting entities at jeopardy of a potential violation that is out of their control. How does an entity report if all systems and communications are down for more than 24 hours? What about in instances of a partial or total blackout? These events could last much longer than 24 hours. All computer communication would likely also be down thus rendering electronic reporting unavailable. *EOP-004-2 only requires an entity to report and communicate per their Operating Plan within the time frames set in Attachment 1.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 4 Comment
Kansas City Power & Light		The implementation plan indicates that much of CIP-008 is retained. The reporting requirements in CIP-008 and the required reportable events outlined in Attachment 1 are an overlap with CIP-008-3 R1.1 which says "Procedures to characterize and classify events as reportable Cyber Security Incidents" and CIP-008-3 R1.3 which requires processes to address reporting to the ES-ISAC. There is also a NERC document titled, Security Guideline for the Electricity Sector: Threat and Incident Reporting, which is a guideline to "assist entities to identify and classify incidents for reporting to the ES-ISAC". The SDT should consider the content of the Security Guideline for the Electricity Sector: Threat and Incident Reporting when considering the reporting requirements proposed EOP-004. The efforts to incorporate CIP-008 into EOP-004 are insufficient and will result in serious confusion between proposed EOP-004 and CIP-008 and reporting expectations. Considering the complexity CIP incident reporting and the interests of ES-ISAC, it may be beneficial to leave CIP-008 out of the proposed EOP-004 and limit EOP-004 to the reporting interests of NERC. *Attachment 2 (or the DOE Form OE 417) is the reporting form to be used for reporting a "Cyber Security Incident".* The flowchart states, "Notification Protocol to State Agency Law Enforcement". Please correct this to, "Notification to State, Provincial, or Local Law Enforcement", to be consistent with the language in the background section part, "A Reporting Process Solution - EOP-004". *The DSR SDT has updated the "Example of reporting _Process including Law Enforcement", and please note that this is only an "example".* Measure 4 is not clear enough regarding the extent to which drills should be performed. Does the measure mean that all events in the events list need to be drilled or is drilling a subset of the events list sufficient? Please clearly indicate the extent of drilling that is required or clearly indicate in the requirement the extent of the drills to be performed is the responsibility of the Responsible Entity to identify in their "processes".

Organization	Yes or No	Question 4 Comment
		Requirement R4 (now R3) has been revised and the measure now reads: *Each Responsible Entity will have dated and time-stamped records to show that the annual test of Part 1.2 was conducted. Such evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other communication documentation. (R3)* Evidence Retention - it is not clear what the phrase "prior 3 calendar years" represents in the third paragraph of this section regarding data retention for requirements and measures for R2, R3, R4 and M2, M3, M4 respectively. Please clarify what this means. Is that different than the meaning of "since the last audit for 3 calendar years" for R1 and M1? *This has been revised for clarity and to be consistent with NERC Guidance documents. The new evidence retention reads:* *Each Responsible Entity shall retain the current, in force document plus the 'date change page' from each version issued since the last audit or the current and previous version for Requirements R1, R4 and Measures M1, M4.* *Each Responsible Entity shall retain evidence from prior 3 calendar years for Requirements R2, R3 and Measures M2, M3.* VSL for R2 under Severe regarding R1.1 may require revision considering the comment regarding R1.1 in item 2 previously stated. In addition, the VRF for R2 is MEDIUM. R2 is administrative regarding the implementation of the requirements specified in R1. Documentation and maintenance should be considered LOWER. There is no VSL for R4 and a VSL for R4 needs to be proposed. *The DSR SDT reviewed and updated both VSL's for the new requirements.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 4 Comment
SPP Standards Review Group		The inclusion of optional entities to which to report events in R1.3 introduces ambiguity into the standard that we feel needs to be eliminated. We propose the following replacement language for R1.3:A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the Responsible Entity's Regional Entity.We would also propose to incorporate the law enforcement and governmental or provincial agencies mentioned in R1.3 in Attachment 1 by adding them to the existing language for each of the event cells. For example, the first cell in that column would read:The parties identified pursuant to R1.3 and applicable law enforcement and governmental or provincial agencies within 1 hour of recognition of event.Similarly, the phrase '...and applicable law enforcement and governmental or provincial agencies...' should be inserted in all the remaining cells in the 4th column. *Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to report events. Requirement R1,Part 1.2 now reads:* *"1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."*
Response: Thank you for your comment. Please see response above.		
Santee Cooper		The on-going development of the definition of the BES could have significant impacts on reporting requirements associated with this standard.The event titled "Risk to the

Organization	Yes or No	Question 4 Comment
		BES" appears to be a catch-all event and more guidance needs to be provided on this category. *Several stakeholders expressed concerns relating to the "Forced Intrusion" event. Their concerns related to ambiguous language in the footnote. The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.* The event titled "Damage or Destruction of a Critical Asset or Critical Cyber Asset per CIP-002" is ambiguous and further guidance is recommended. Ambiguity in a standard leaves it open to interpretation for all involved. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as stakeholders pointed out that these events were adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility "reporting thresholds. CIP-008 addresses Cyber Security Incidents which are defined as:* *"Any malicious act or suspicious event that:* *• Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,*

Organization	Yes or No	Question 4 Comment
		• Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset." *A Critical Asset is defined as:* *"Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."* *Since there is an existing event category for damage or destruction of Facilities, having a separate event for "Damage or Destruction of a Critical Asset" is unnecessary.*
Response: Thank you for your comment. Please see response above.		
Florida Municipal Power Agency		The Rules of Procedure language for data retention (first paragraph of the Evidence Retention section) should not be included in the standard, but instead referred to within the standard (e.g., "Refer to Rules of Procedure, Appendix 4C: Compliance Monitoring and Enforcement Program, Section 3.1.4.2 for more retention requirements") so that changes to the RoP do not necessitate changes to the standard. *The language incorporated in this section of the standard is boilerplate language provided by NERC staff for inclusion in each standard.* In R4, it might be worth clarifying that, in this case, implementation of the plan for an event that does not meet the criteria of Attachment 1 and going beyond the requirements R2 and R3 could be used as evidence. Consider adding a phrase as such to M4, or a descriptive footnote that in this case, "actual event" may not be limited to those in Attachment 1.

Organization	Yes or No	Question 4 Comment
		Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2based on stakeholder comments and revised R3 (now R2) to: *"Requirement R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."* Comments to Attachment 1 table:On "Damage or destruction of Critical Asset" and "... Critical Cyber Asset", Version 5 of the CIP standards is moving away from the binary critical/non-critical paradigm to a high/medium/low risk paradigm. Suggest adding description that if version 5 is approved by FERC, that "critical" would be replaced with "high or medium risk", or include changing this standard to the scope of the CIP SDT, or consider posting multiple versions of this standard depending on the outcome of CIP v5 in a similar fashion to how FAC-003 was posted as part of the GO/TO effort of Project 2010-07. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as stakeholders pointed out that these events were adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility "reporting thresholds. CIP-008 addresses Cyber Security Incidents which are defined as:* *"Any malicious act or suspicious event that:* *• Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,* *• Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber*

Organization	Yes or No	Question 4 Comment
		Asset." *A Critical Asset is defined as:* *"Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."* *Since there is an existing event category for damage or destruction of Facilities, having a separate event for "Damage or Destruction of a Critical Asset" is unnecessary.* On "forced intrusion", the phrase "at BES facility" is open to interpretation as "BES Facility" (e.g., controversy surrounding CAN-0016) which would exclude control centers and other critical/high/medium cyber system Physical Security Perimeters (PSPs). We suggest changing this to "BES Facility or the PSP or Defined Physical Boundary of critical/high/medium cyber assets". This change would cause a change to the applicability of this reportable event to coincide with CIP standard applicability. *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say ' to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* • *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its*

Organization	Yes or No	Question 4 Comment
		Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples. *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* On "Risk to BES equipment", that phrase is open to too wide a range of interpretation; we suggest adding the word "imminent" in front of it, i.e., "Imminent risk to BES equipment". For instance, heavy thermal loading puts equipment at risk, but not imminent risk. Also, "non-environmental" used as the threshold criteria is ambiguous. For instance, the example in the footnote, if the BES equipment is near railroad tracks, then trains getting derailed can be interpreted as part of that BES equipment's "environment", defined in Webster's as "the circumstances, objects, or conditions by which one is surrounded". It seems that the SDT really means "non-weather related", or "Not risks due to Acts of Nature". *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say ' to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* • *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its*

Organization	Yes or No	Question 4 Comment
		Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples. *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* On "public appeal", in the threshold, the descriptor "each" should be deleted, e.g., if a single event causes an entity to be short of capacity, do you really want that entity reporting each time they issue an appeal via different types of media, e.g., radio, TV, etc., or for a repeat appeal every several minutes for the same event? *The DSR SDT has updated the event concerning "public appeals" based on comments received and now reads as: "Public appeal for load reduction event".* Should LSE be an applicable entity to "loss of firm load"? As proposed, the DP is but the LSE is not. In an RTO market, will a DP know what is firm and what is non-firm load? Suggest eliminating DP from the applicability of "system separation". The system separation we care about is separation of one part of the BES from another which would not involve a DP. *The DSR SDT believes the "Entity with Reporting Responsibility" maintains the minimum number and type of entities that will be required to report such an event.* On "Unplanned Control Center Evacuation", CIP v5 might add GOP to the applicability, another reason to add revision of EOP-004-2 to the scope of the CIP v5 drafting team, or in other ways coordinate this SDT with that SDT. Consider posting a couple of versions of the standard depending on the outcome of CIP v5 in a similar fashion to the multiple versions of FAC-003 posted with the Go/TO effort of Project 2010-07.

Organization	Yes or No	Question 4 Comment
		The DSR SDT can only provide information on approved standards, not yet to be defined standards.
Response: Thank you for your comment. Please see response above.		
Dominion		There is still inconsistency in Attachment 1 vs. the DOE OE-417 form; in future changes, Dominion suggests align/rename events similar to that of the 'criteria for filing' events listed in the DOE OE-417, by working in coordination with the DOE. *Thank you for your comment. Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.* *Please note that not all entities in North America are required to submit the DOE Form OE 417.* Minor comment; in the Background section, the drafting team refers to bulk power

Organization	Yes or No	Question 4 Comment
		system (redline page 5; 1st paragraph and page 7; 2nd paragraph) rather than bulk electric system. *This has been revised to Bulk Electric System.* The note in Attachment 1 states in part that "the affected Responsible Entity shall notify parties per R1 and ..." Dominion believes the correct reference to be R3. In addition, capitalized terms "Event" and "Event Report" are used in this note. Dominion believes the terms should be non-capitalized as they are not NERC defined terms. *The DSR SDT has updated this note based on comments received and now reads as: "NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written event report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per R1 and provide as much information as is available at the time of the notification. Reports to the ERO should be submitted to one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422."* Attachment 1 - "Detection of a reportable Cyber Security Incident - That meets the criteria in CIP-008". This essentially equates the criteria to be defined by the entity in its procedures as required by CIP-008 R1.1., additional clarification should be added in Attachment 1 to make this clear. *The DSR SDT believes that this event language provides enough clarity by providing the minimum events to be reported.* The last sentence in Attachment 2 instructions should clarify that the email, facsimile and voice communication methods are for ERO notification only. *The DSR SDT agrees and has revised the sentence to include "to the ERO".* Dominion continues to believe that the drill or exercise specified in R4 is

Organization	Yes or No	Question 4 Comment
		unnecessary. Dominion suggests deleting this activity in the requirement. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. Requirement R3 now reads: "Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. ".* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.*
Response: Thank you for your comment. Please see response above.		
Ingleside Cogeneration LP		We are encouraged that the 2009-01 project team has eliminated duplicate reporting requirements from multiple organizations and governmental agencies. Ingleside Cogeneration LP believes that there are further improvements that can be made in this area - as the remaining overlap seem to be a result of legalities and preferences, not technical issues. We would like to see an ongoing commitment by NERC for a single process that will consolidate and automate data entry, submission, and distribution. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an*

Organization	Yes or No	Question 4 Comment
		opportunity not a 'must-have' • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.* *Please note that not all entities in North America are required to submit the DOE Form OE 417.*
Response: Thank you for your comment. Please see response above.		
SERC OC Standards Review Group		We believe that reporting of the events in Attachment 1 has no reliability benefit to the bulk electric system. In addition, Attachment 1, in its current form, is likely to be impossible to implement consistently across North America. A requirement, to be considered a reliability requirement, must be implementable. We suggest that Attachment 1 should be removed. *The DSR SDT disagrees with this comment. Attachment 1 is the minimum set of events that will be required to report and communicate per your Operating Plan will be aware of system conditions.* We have a question about what looks like a gap in this standard: Assuming one of thedrivers for the standard is to protect against a coordinated physical or cyber attack on the grid, what happens if the attack occurs in 3-4 geographically diverse areas? State or provisional law enforcement officials are not accountable under the standard, so we have no way of knowing if they report the attack to the FBI or the

Organization	Yes or No	Question 4 Comment
		RCMP. Even if one or two of them did, might not the FBI, in different parts of the country, interpret it as vandalism, subject to local jurisdiction?It seems that NERC is the focal point that would have all the reports and, ideally, some knowledge how the pieces fit together. It looks like NERC's role is to solely pass information on "applicable" events to the FERC. Unless the FERC has a 24x7 role not shown in the standard, should not NERC have some type of assessment responsibility to makes inquiries at the FBI/RCMP on whether they are aware of the potential issue and are working on it?"The comments expressed herein represent a consensus of the views of the above named members of the SERC OC Standards Review group only and should not be construed as the position of SERC Reliability Corporation, its board or its officers." *Requirement R1, Part 1.2 was updated and now reads as: "A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."* *By reporting to the ERO all events, this will allow the ERO to coordinate with other agencies as they see fit.*
Response: Thank you for your comment. Please see response above.		
ZGlobal on behalf of City of Ukiah, Alameda Municipal Power, Salmen River Electric, City of Lodi		We feel that the drafting team has done an excellent job of providing clarification and reasonable reporting requirements to the right functional entity. However we feel additional clarification should be made in the Attachment I Event Table. We suggest the following modifications:For the Event: BES Emergency resulting in automatic firm load sheddingModify the Entity with Reporting Responsibility to: Each DP or TOP that experiences the automatic load shedding within their respective distribution serving or Transmission Operating area. *The DSR SDT believes the "Entity with Reporting Responsibility" contains the minimum*

Organization	Yes or No	Question 4 Comment
		entities that will be required to report and reads as: "Each DP or TOP that experiences the automatic load shedding" For the Event: Loss of Firm load for â‰¥ 15 MinutesModify the Entity with Reporting Responsibility to: Each BA, TOP, DP that experiences the loss of firm load within their respective balancing, Transmission operating, or distribution serving area. *The DSR SDT believes the "Entity with Reporting Responsibility" contains the minimum entities that will be required to report and reads as: "Each BA, TOP, DP that experiences the loss of firm load"*
Response: Thank you for your comment. Please see response above.		
PSEG		We have several comments:1. The "Law Enforcement Reporting" section on p. 6 is unclearly written. The first three sentences are excerpted here: "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement."The outages described prior to the last sentence are "vandalism and terrorism." The next sentence states "Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES." If the SDT intended to only have events reported to law enforcement that could to Cascading, it should state so clearly and succinctly. But other language implies otherwise. *The DSR SDT has updated the "Example of reporting _Process including Law Enforcement", and please note that this is only an "example".* a. The footnote 1 on Attachment 1 (p. 20) states: "Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g.,

Organization	Yes or No	Question 4 Comment
		removal of grounding straps rendering protective relaying inoperative)." Rendering a relay inoperative may or may not lead to Cascading. *The DSR SDT has removed all footnotes with the exception of the updated event within Attachment 1 that states: "A physical threat that could impact the operability of a Facility". This event has the following footnote, which states: "Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* b. With regard to "forced intrusion," footnote 2 on Attachment 1 states: "Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects (sic) the reliability of the BES." The criterion, or criteria, for reporting an event to law enforcement needs to be unambiguous. The SDT needs to revise this "Law Enforcement Section" so that is achieved. The "law enforcement reporting" criterion, or criteria, should also be added to the flow chart on p. 9. We suggest the following as a starting point for the team to discuss: there should be two criteria for reporting an event to law enforcement: (1) BES equipment appears to have been deliberately damaged, destroyed, or stolen, whether by physical or cyber means, or (2) someone has gained, or attempted to gain, unauthorized access by forced or unauthorized entry (e.g., via a stolen employee keycard badge) into BES facilities, including by physical or cyber means. *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* *The 'Damage or Destruction' event category has been revised to say ' to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was*

Organization	Yes or No	Question 4 Comment
		deleted *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.* *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* 2. The use of the terms "communicating events" in R1.3, and the use of the term "communication process" are confusing because in other places such as R3 the term "reporting" is used. If the SDT intends "communicating" to mean "reporting" as that later term is used in R3, it should use the same "reporting" term in lieu of "communicating" or "communication" elsewhere. Inconsistent terminology causes confusion. PSEG prefers the word "reporting" because it is better understood. *Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to report events. Requirement R1, Part 1.2 now reads:* *"1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."*

Organization	Yes or No	Question 4 Comment
		The SDT envisions that most entities will only need to slightly modify their existing CIP-001 Sabotage Reporting procedures in order to comply with the Operating Plan requirement in this proposed standard. As many of the features of both are substantially similar, the SDT feels that some information may need to updated and verified. 3. Attachment 1 needs to more clearly define what is meant by "recognition of an event."a. When equipment or a facility is involved, it would better state within "X" time (e.g., 1 hour) of "of confirmation of an event by the entity that either owns or operates the Element or Facility." *Based on stakeholder comments, Requirement R1 was revised for clarity. Requirement R1, Part 1.1 was revised to replace the word "identifying" with "recognizing" and Part 1.2 was eliminated. This also aligns the language of the standard with FERC Order 693, Paragraph 471.* *"(2) specify baseline requirements regarding what issues should be addressed in the procedures for recognizing {emphasis added} sabotage events and making personnel aware of such events;"* b. Other reports should have a different specification of the starting time of the reporting deadline clock. For example, in the requirement for reporting a "BES Emergency requiring public appeal for load reduction," it is unclear what event is required to be reported - the "BES Emergency requiring public appeal" or "public appeal for load reduction." If the later is intended, then the event should be reported within "24 hours after a public appeal for load reduction is first issued." These statements need to be reviewed and customized for each event by the SDT so they are unambiguous. *All one hour reporting timelines have been changed to 24 hours with the exception of a*

Organization	Yes or No	Question 4 Comment
		'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673: *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.* In summary, the starting time for the reporting clock to start running should be made clear for each event. This will require that the SDT review each event and customize the starting time appropriately. The phrase "recognition of an event" should not be used because it is too vague. *Based on stakeholder comments, Requirement R1 was revised for clarity. Part 1.1 was revised to replace the word "identifying" with "recognizing" and Part 1.2 was eliminated. This also aligns the language of the standard with FERC Order 693, Paragraph 471.* *"(2) specify baseline requirements regarding what issues should be addressed in the procedures for recognizing {emphasis added} sabotage events and making personnel aware of such events;"* 4. When EOP-004-2 refers to other standards, it frequently omits the version of the standard. Example: see the second and third row of Attachment 1 that refers to "CIP-002." Include the version on all standards referenced. *References to CIP-002 have been removed from the standard. The intent of referencing those standards is to prevent rewriting the standard within EOP-004-2. The threshold for reporting CIP-008 events is written as "That meets the criteria in CIP-008-4 or its successor."*

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comment. Please see response above.		
Ameren		Yes. We have the other comments as follow:(1) The "EOP-004 Attachment 1: Events Table" is quite lengthy and written in a manner that can be quite subjective in interpretation when determining if an event is reportable. We believe this table should be clear and unambiguous for consistent and repeatable application by both reliability entities and a CEA. *The DSR SDT has reviewed and further revised Attachment 1 based on comments received. We believe that it is both concise and easily interpreted.* The table should be divided into sections such as: 9a) Events that affect the BES that are either clearly sabotage or suspected sabotage after review by an entity's security department and local/state/federal law enforcement.(b) Events that pose a risk to the BES and that clearly reach a defined threshold, such as load loss, generation loss, public appeal, EEAs, etc. that entities are required to report by the end of the next business day.(c) Other events that may prove valuable for lessons learned, but are less definitive than required reporting events. These events should be reported voluntarily and not be subject to a CEA for non-reporting. *The DSR SDT received many comments regarding the various entries of Attachment 1. Many commenters questioned the reliability benefit of reporting events to the ERO within 1 hour. Most of the events with a one hour reporting requirement were revised to 24 hours based on stakeholder comments as well as those types of events are currently required to be reported within 24 hours in the existing mandatory and enforceable standards. The only remaining type of event that is to be reported within one hour is "A reportable Cyber Security Incident" as it required by CIP-008 and FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a*

Organization	Yes or No	Question 4 Comment
		cyber security incident as soon as possible, but in any event, within one hour of the event…" *The table was reformatted to separate one hour reporting and 24 hour reporting. The last column of the table was also deleted and the information contained in it was transferred to the sentence above each table. These sentences are:* *"One Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the event."* *"Twenty-four Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within twenty-four hour of recognition of the event."* (d)Events identified through other means outside of entity reporting, but due to their nature, could benefit the industry by an event report with lessons learned. Requests to report and perform analysis on these type of events should be vetted through a ERO/Functional Entity process to ensure resources provided to this effort have an effective reliability benefit. *The DSR SDT has deleted the "lessons learned" language. Requirement R4 now only requires an annual review of the Operating Plan - the '90 days' and ' other circumstances' elements have been removed.* (2)Any event reporting shall not in any manner replace or inhibit an Entity's responsibility to coordinate with other Reliability Entities (such as the RC, TOP, BA, GOP as appropriate) as required by other Standards, and good utility practice to operate the electric system in a safe and reliable manner. *The DSR SDT concurs with your comment.*

Organization	Yes or No	Question 4 Comment
		(3) The 1 hour reporting maximum time limit for all GO events in Attachment 1 should be lengthened to something reasonable - at least 24 hours. Operators in our energy centers are well-trained and if they have good reason to suspect an event that might have serious impact on the BES will contact the TOP quickly. However, constantly reporting events that turn out to have no serious BES impact and were only reported for fear of a violation or self-report will quickly result in a cry wolf syndrome and a great waste of resources and risk to the GO and the BES. The risk to the GO will be potential fines, and the risk to the BES will be ignoring events that truly have an impact of the BES. *The DSR SDT received many comments regarding the various entries of Attachment 1. Many commenters questioned the reliability benefit of reporting events to the ERO within 1 hour. Most of the events with a one hour reporting requirement were revised to 24 hours based on stakeholder comments as well as those types of events are currently required to be reported within 24 hours in the existing mandatory and enforceable standards. The only remaining type of event that is to be reported within one hour is "A reportable Cyber Security Incident" as it required by CIP-008 and FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *The table was reformatted to separate one hour reporting and 24 hour reporting. The last column of the table was also deleted and the information contained in it was transferred to the sentence above each table. These sentences are:* *"One Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the*

Organization	Yes or No	Question 4 Comment
		event." *"Twenty-four Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within twenty-four hour of recognition of the event."* (4)The 2nd and 3rd Events on Attachment 1 should be reworded so they do not use terms that may have been deleted from the NERC Glossary by the time FERC approves this Standard. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* (5) The terms "destruction" and "damage" are key to identifying reportable events. Neither has been defined in the Standard. The term destruction is usually defined as 100% unusable. However, the term damage can be anywhere from 1% to 99% unusable and take anywhere from 5 minutes to 5 months to repair. How will we know what the SDT intended, or an auditor will expect, without additional information? *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* *The 'Damage or Destruction' event category has been revised to say ' to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new*

Organization	Yes or No	Question 4 Comment
		event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples. *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* (6)We also do not understand why "destruction of BES equipment" (first item Attachment 1, first page) must be reported < 1 hour, but "system separation (islanding) > 100 MW" (Attachment 1, page 3) does not need to be reported for 24 hours. *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting*

Organization	Yes or No	Question 4 Comment
		timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples. *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* (7)The first 2 Events in Attachment 1 list criteria Threshold for Reporting as "...operational error, equipment failure, external cause, or intentional or unintentional human action." The term "intentional or unintentional human action" appears to cover "operational error" so these terms appear redundant and create risk of misreporting. Can this be clarified? *The DSR SDT has updated this language based on comments received and now reads as: " Damage or destruction of a Facility that:* *Affects an IROL (per FAC-014)* *OR* *Results in the need for actions to avoid an Adverse Reliability Impact* *OR* *Results from intentional human action."* (8)The footnote of the first page of Attachment 1 includes the explanation "...ii) Significantly affects the reliability margin of the system..." However, the GO is prevented from seeing the system and has no idea what BES equipment can affect the reliability margin of the system. Can this be clarified by the SDT? *The DSR SDT has removed all footnotes with the exception of the updated event within Attachment 1 that states: "A physical threat that could impact the operability of a Facility". This event has the following footnote, which states: "Examples include a*

Organization	Yes or No	Question 4 Comment
		train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility." (9) The use of the term "BES equipment" is problematic for a GO. NERC Team 2010-17 (BES Definition) has told the industry its next work phase will include identifying the interface between the generator and the transmission system. The 2010-17 current effort at defining the BES still fails to clearly define whether or not generator tie-lines are part of the BES. In addition, NERC Team 2010-07 may also be assigned the task of defining the generator/transmission interface and possibly whether or not these are BES facilities. Can the SDT clarify the use of this term? For example, does it include the entire generator lead-line from the GSU high-side to the point of interconnection? Does it include any station service transformer supplied from the interconnected BES? *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say ' to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* • *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it*

Organization	Yes or No	Question 4 Comment
		may have first occurred. Also, the footnote only contains examples. *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.*
Response: Thank you for your comment. Please see response above.		
Performance Analysis Subcommittee		There continues to be some confusion regarding whether the loss of firm load was consistent with the planned operation of the system or was an unintended consequence. As such it might be helpful if instead of a single check box for loss of firm load there were two check boxes 1) loss of firm load – consequential and 2) loss of firm load non-consequential. *Thank you for your comment. The DSR SDT believes that Attachment 2 contains the minimum amount of information under this standard. Any entity reporting an event can add as much information as they see fit.*
Response: Thank you for your comment. Please see response above.		
Southwestern Power Administration's		"Attachment 1 contains elements that do not need to be included, and redundant elements such as: Forced intrusion at BES Facility - A facility break-in does not necessarily mean that the facility has been impacted or has undergone damage or destruction. *The DSR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was*

Organization	Yes or No	Question 4 Comment
		revised to "Any physical threat that could impact the operability of a Facility". *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.* *The footnote regarding this event type was expanded to provide additional guidance in:* *"Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* Detection of a reportable Cyber Security Incident per CIP-008 - If entities are addressing this requirement in CIP-008, why do so again in EOP-004 (Attachment 2-EOP-004, Reporting Requirement number 5)? *The reporting aspects of CIP-008 have been removed from CIP-008 and are included in EOP-004. Please see the Implementation Plan with regards to the retirement of CIP-008, R1.3* Transmission Loss: Each TOP that experiences transmission loss of three or more facilities - This element should be removed or rewritten so that it only applies when the loss includes a contingent element of an IROL facility." *The DSR SDT disagrees with limiting this type of event to only "a contingent element*

Organization	Yes or No	Question 4 Comment
		of an IROL facility." It is important for situational awareness and trending analysis to have these types of events reported.
Response: Thank you for your comment. Please see response above.		
The Performance Analysis Subcommittee		There continues to be some confusion regarding whether the loss of firm load was consistent with the planned operation of the system or was an unintended consequence. As such it might be helpful if instead of a single check box for loss of firm load there were two check boxes 1) loss of firm load – consequential and 2) loss of firm load non-consequential. *The DSR SDT believes that this information should be obtained in follow up through the Events Analysis Program. The reporting entity may have concerns or difficulties in determining if load is consequential or non-consequential in its initial analysis for the report. Further investigation outside of the reporting time of 24 hours may be needed to make this determination.*
Response: Thank you for your comment. Please see response above.		
Xcel Energy		
Los Angeles Department of Water and Power		
Liberty Electric Power		
Nebraska Public Power District		
Southwestern Power Administration		

Organization	Yes or No	Question 4 Comment
Electric Reliability Council of Texas, Inc.		

END OF REPORT

Consideration of Comments

Disturbance and Sabotage Reporting – Project 2009-01

The Disturbance and Sabotage Reporting Drafting Team thanks all commenters who submitted comments on the draft standard EOP-004-2. This standard was posted for a 30-day public comment period from April 25, 2012 through May 24, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 87 sets of comments, including comments from approximately 210 different people from approximately 135 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page:

http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President of Standards and Training, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual:
http://www.nerc.com/files/Appendix_3A_Standard_Processes_Manual_Rev%201_20110825.pdf

Summary Consideration: The DSR SDT received several suggestions for improvement to the standard. As a result of these revisions, the DSR SDT is posting the standard for a second successive ballot period.

The DSR SDT has removed reporting of Cyber Security Incidents from EOP-004 and have asked the team developing CIP-008-5 to retain this reporting. With this revision, the Interchange Coordinator, Transmission Service Providers, Load-Serving Entity, Electric Reliability Organization and Regional Entity were removed as Responsible Entities.

Most of the language contained in the "Background" Section was moved to the "Guidelines and Technical Basis" Section. Minor language changes were made to the measures and the data retention section. Attachment 2 was revised to list events in the same order in which they appear in Attachment 1.

Requirement R1 was revised to include the Parts in the main body of the Requirement. The Measure and VSLs were updated accordingly.

Following review of the industry's comments, the SDT has re-examined the FERC Directive in Order 693 and has dropped both R3 and R4, as they were written and established a new Requirement R3 to have the Registered Entity "validate" the contact information in the contact list(s) they may have for the events applicable to them. This validation needs to be performed each calendar year to ensure that the list(s) have current and up-to-date contact data.

> R3. Each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1each calendar year. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

The SDT reviewed, discussed and updated Attachment 1 based on comments received for commenters, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Under the Event Column, the SDT starts to classify each type of an event by assigning an "Event" title. The DSRSDT then updated the "Entity with Reporting Responsibilities" column to simply state which entity has the responsibility to report if they experience an event. The last column, "Threshold for Reporting" is a bright line that, if reached, the entity needs to report that they experienced the applicable event per Requirement 1.

The DSR SDT proposed a revision to the NERC Rules of Procedure (Section 812). The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.

Index to Questions, Comments, and Responses

1. The DSR SDT has revised EOP-004-2 by removing Requirement 1, Part 1.4 and separating Parts 1.3 and 1.5 into new Requirements R3 and R4. Requirement R3 calls for an annual test of the communications portion of the Operating Plan and Requirement R4 requires an annual review of the Operating Plan. Do you agree with this revision? If not, please explain in the comment area below. 19
2. The DSR SDT made clarifying revisions to Attachment 1 based on stakeholder feedback. Do you agree with these revisions? If not, please explain in the comment area below. 46
3. The DSR SDT has proposed a new Section 812 to be incorporated into the NERC Rules of Procedure. Do you agree with the proposed addition? If not, please explain in the comment area below. 169
4. Do you have any other comment, not expressed in the questions above, for the DSR SDT? .... .183

The Industry Segments are:

1 — Transmission Owners

2 — RTOs, ISOs

3 — Load-serving Entities

4 — Transmission-dependent Utilities

5 — Electric Generators

6 — Electricity Brokers, Aggregators, and Marketers

7 — Large Electricity End Users

8 — Small Electricity End Users

9 — Federal, State, Provincial Regulatory or other Government Entities

10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10

Group/Individual	Commenter	Organization		Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
2.	Greg Campoli	NewYorkI Independent System Operator	NPCC	2									
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1									
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1									
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10									
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5									
7.	Kathleen Goodman	ISO - New England	NPCC	2									
8.	Michael Jones	National Grid	NPCC	1									
9.	David Kiguel	Hydro One Networks Inc.	NPCC	1									
10.	Michael Lombardi	Northeast Utilities	NPCC	1									
11.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9									
12.	Bruce Metruck	New York Power Authority	NPCC	6									
13.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5									
14.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10									
15.	Robert Pellegrini	The United Illuminating Company	NPCC	1									
16.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1									
17.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
18.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3									
19.	Michael Schiavone	National Grid	NPCC	1									
20.	Wayne Sipperly	New York Power Authority	NPCC	5									
21.	Tina Teng	Independent Electricity System Operator	NPCC	2									
22.	Donald Weaver	New Brunswick System Operator	NPCC	2									
23.	Ben Wu	Orange and Rockland Utilities	NPCC	1									
2.	Group	Kent Kujala	DECo			X	X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Barbara Holland		RFC	3, 4, 5
2.	Alexander Eizans		RFC	3, 4, 5

3.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

4.	Group	Brenda Hampton	Luminant						X				

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company, LLC		5

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Chris Higgins	Bonneville Power Administration	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	James	Burns	WECC	1
2.	John	Wylder	WECC	1
3.	Kristy	Humphrey	WECC	1

7.	Group	Jesus Sammy Alcaraz	Imperial Irrigation District (IID)	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joel Fugett	IID	WECC	1, 3, 4, 5, 6
2.	Cathy Bretz	IID	WECC	1, 3, 4, 5, 6

8.	Group	Connie Lowe	Dominion	X		X		X	X				

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

	Additional Member	Additional Organization	Region	Segment Selection
1.	Michael Crowley		SERC	1, 3, 5, 6
2.	Mike Garton		NPCC	5, 6
3.	Randi Heise		MRO	5
4.	Louis Slade		RFC	5

9.	Group	Robert Rhodes	SPP Standards Review Group		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Matt Bordelon	CLECO Power	SPP	1, 3, 5
2.	Michelle Corley	CLECO Power	SPP	1, 3, 5
3.	Gary Cox	Southwestern Power Administration	SPP	1, 5
4.	Dan Lusk	Xcel Energy	SPP	1, 3, 5, 6
5.	Stephen McGie	City of Coffeyville	SPP	NA
6.	John Payne	KEPCO	SPP	4
7.	Terri Pyle	Oklahoma Gas & Electric	SPP	1, 3, 5
8.	Sean Simpson	Board of Public Utilities, City of McPherson, KS	SPP	NA
9.	Ashley Stringer	Oklahoma Municipal Power Authority	SPP	4

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
10. Mike Swearingen	Tri-County Electric Cooperative	SPP 4										
11. Michael Veillon	CLECO Power	SPP 1, 3, 5										
12. Mark Wurm	Board of Public Utilities, City of McPherson, KS	SPP NA										
13. Jonathan Hayes	Southwest Power Pool	SPP 2										
14. Julie Lux	Westar Energy	SPP 1, 3, 5, 6										
15. Greg McAuley	Oklahoma Gas & Electric	SPP 1, 3, 5										
10. Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				

Additional Member	Additional Organization	Region	Segment Selection
1. Timothy Beyrle	City of New Smyrna Beach	FRCC	4
2. Jim Howard	Lakeland Electric	FRCC	3
3. Greg Woessner	Kissimmee Utility Authority	FRCC	3
4. Lynne Mila	City of Clewiston	FRCC	3
5. Joe Stonecipher	Beaches Energy Services	FRCC	1
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4
7. Randy Hahn	Ocala Utility Services	FRCC	3

11. Group	Brent Ingebrigtson	LG&E and KU Services	X		X		X	X				
No additional members listed.												

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
12.	Group	WILL SMITH	MRO NSRF	X	X	X	X	X	X				X

	Additional Member	Additional Organization	Region	Segment Selection
1.	MAHMOOD SAFI	OPPD	MRO	1, 3, 5, 6
2.	CHUCK LAWRENCE	ATC	MRO	1
3.	TOM WEBB	WPS	MRO	3, 4, 5, 6
4.	JODI JENSON	WAPA	MRO	1, 6
5.	KEN GOLDSMITH	ALTW	MRO	4
6.	ALICE IRELAND	XCEL	MRO	1, 3, 5, 6
7.	DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6
8.	ERIC RUSKAMP	LES	MRO	1, 3, 5, 6
9.	JOE DEPOORTER	MGE	MRO	3, 4, 5, 6
10.	SCOTT NICKELS	RPU	MRO	4
11.	TERRY HARBOUR	MEC	MRO	3, 5, 6, 1
12.	MARIE KNOX	MISO	MRO	2
13.	LEE KITTELSON	OTP	MRO	1, 3, 4, 5
14.	SCOTT BOS	MPW	MRO	1, 3, 5, 6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
15. TONY EDDLEMAN	NPPD	MRO 1, 3, 5										
16. MIKE BRYTOWSKI	GRE	MRO 1, 3, 5, 6										
17. THERESA ALLARD	MPC	MRO 1, 3, 5, 6										
13. Group	Stephen J. Berger	PPL Corporation NERC Registered Affiliates					X	X				

Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC 5
2.			WECC 5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO 6
4.			NPCC 6
5.			SERC 6
6.			SPP 6
7.			RFC 6
8.			WECC 6

14. Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X			

Additional Member	Additional Organization	Region	Segment Selection

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
1. Kevin Smith	BANC	WECC 1										
15. Group	Albert DiCaprio	ISO/RTO Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Terry Bilke	MISO	RFC	2
2.	Greg Campoli	NY ISO	NPCC	2
3.	Gary DeShazo	CAISO	WECC	2
4.	Matt Goldberg	ISO NE	NPCC	2
5.	Kathleen Goodman	ISO NE	NPCC	2
6.	Stephanie Monzon	PJM	RFC	2
7.	Steve Myers	ERCOT	ERCOT	2
8.	Bill Phillips	MSO	RFC	2
9.	Don Weaver	NBSO	NPCC	2
10.	Charles Yeung	SPP	SPP	2

16. Group	Sam Ciccone	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Bill Duge	FE	RFC	

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
2. Doug Hohlbaugh	FE	RFC										
17. Group	Jason Marshall	ACES Power Marketing Standards Collaborators						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
2.	Robert A. Thomasson	Big Rivers Electric Corporation	SERC	1
3.	Shari Heino	Brazos Electric Power Cooperative	ERCOT	1
4.	John Shaver	Arizona Electric Power Cooperative	WECC	4, 5
5.	John Shaver	Southwest Transmission Cooperative	WECC	1
6.	Michael Brytowski	Great River Energy	MRO	1, 3, 5, 6
7.	Scott Brame	North Carolina Electric Membership Corporation	SERC	1, 3, 4, 5

18. Group	Pawel Krupa	Seattle City Light	X		X	X						

	Additional Member	Additional Organization	Region	Segment Selection
1.	Pawel Krupa	Seattle City Light	WECC	1
2.	Dana Wheelock	Seattle City Light	WECC	3
3.	Hao Li	Seattle City Light	WECC	4

19. Group	Scott Kinney	Avista	X		X		X					

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

	Additional Member	Additional Organization	Region	Segment Selection
1.	Ed Groce	Avista Corp	WECC	5
2.	Bob Lafferty	Avista Corp	WECC	3

20.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3
7.	Rick Crinklaw	Lane Electric Cooperative	WECC	3
8.	Annie Terracciano	Northern Lights Inc.	WECC	3
9.	Aleka Scott	PNGC Power	WECC	4
10.	Heber Carpenter	Raft River Rural Electric Cooperative	WECC	3
11.	Steve Eldrige	Umatilla Electric Cooperative	WECC	1, 3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
12. Marc Farmer		West Oregon Electric Cooperative	WECC 4										
13. Margaret Ryan		PNGC Power	WECC 8										
14. Stuart Sloan		Consumers Power Inc.	WECC 1										
21.	Group	Jennifer Eckels	Colorado Springs Utilities	X		X		X	X				
Additional Member		Additional Organization	Region Segment Selection										
1. Lisa Rosintoski			WECC 6										
2. Charlie Morgan			WECC 3										
3. Paul Morland			WECC 1										
22.	Individual	Janet Smith, Regulatory Affairs Supervisor	Arizona Public Service Company	X		X		X	X				
23.	Individual	Antonio Grayson	Southern Company Services	X		X		X	X				
24.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
25.	Individual	Sasa Maljukan	Hydro One	X									
26.	Individual	John Brockhan	CenterPoint Energy	X									
27.	Individual	Philip Huff	Arkansas Electric Cooperative Corporation			X	X		X				
28.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
29.	Individual	Brian Evans-Mongeon	Utility Services								X		
30.	Individual	E Hahn	MWDSC	X									
31.	Individual	Scott McGough	Georgia System Operations Corporation			X	X						
32.	Individual	Don Jones	Texas Reliability Entity										X

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
34.	Individual	Dan Roethemeyer	Dynegy Inc.					X					
35.	Individual	Anthony Jablonski	ReliabilityFirst										X
36.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
37.	Individual	Michelle R. D'Antuono	Ingleside Cogeneration LP					X					
38.	Individual	Tim Soles	Occidental Power Services, Inc.			X			X				
39.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
40.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
41.	Individual	Thad Ness	American Electric Power	X		X		X	X				
42.	Individual	Ed Davis	Entergy	X		X		X	X				
43.	Individual	Jack Stamper	Clark Public Utilities	X									
44.	Individual	Tracy Richardson	Springfield Utility Board			X							
45.	Individual	Wayne Sipperly	New York Power Authority	X		X		X	X				
46.	Individual	David Thorne	Pepco Holdings Inc	X		X							
47.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				
48.	Individual	David Burke	Orange and Rockland Utilities, Inc.	X		X							
49.	Individual	Larry Raczkowski	FirstEnergy Corp	X		X	X	X	X				
50.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
51.	Individual	Michael Falvo	Independent Electricity System Operator		X								
52.	Individual	John Seelke	Public Service Enterprise Group	X		X		X	X				
53.	Individual	Terry Harbour	MidAmerican Energy	X		X		X	X				
54.	Individual	Brenda Lyn Truhe	PPL Electric Utilities	X									
55.	Individual	John Martinsen	Public Utility District No. 1 of Snohomish County	X		X	X	X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
56.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
57.	Individual	Thomas Washburn	FMPP						X				
58.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
59.	Individual	Andrew Z. Pusztai	Amercican Transmission Company, LLC	X									
60.	Individual	Brenda Frazer	Edison Mission Marketing & Trading, Inc.	X				X					
61.	Individual	Kenneth A Goldsmith	Alliant Energy				X						
62.	Individual	Eric Salsbury	Consumers Energy			X	X	X					
63.	Individual	Kirit Shah	Ameren	X		X		X	X				
64.	Individual	Howard Rulf	We Energies			X	X	X					
65.	Individual	Brian J Murphy	NextEra Energy Inc	X		X		X	X				
66.	Individual	Kathleen Goodman	ISO New England Inc		X								
67.	Individual	Mark B Thompson	Alberta Electric System Operator		X								
68.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				
69.	Individual	Keith Morisette	Tacoma Power	X		X	X	X	X				
70.	Individual	Dennis Sismaet	Seattle City Light						X				
71.	Individual	Scott Miller	MEAG Power	X		X		X					
72.	Individual	Patrick Brown	Essential Power, LLC					X					
73.	Individual	Gregory Campoli	New York Independent System Operator		X								
74.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
75.	Individual	David Revill	GTC	X									
76.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
77.	Individual	Christine Hasha	ERCOT		X								
78.	Individual	Molly Devine	Idaho Power Co.	X									
79.	Individual	Rebecca Moore Darrah	MISO		X								

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
80.	Individual	Nathan Mitchell	American Public Power Association			X							
81.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
82.	Individual	Darryl Curtis	Oncor Electric Delivery	X									
83.	Individual	Denise Lietz	Puget Sound Energy, Inc.	X		X		X					
84.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
85.	Individual	Mauricio Guardado	Los Angeles Department of Water and Power	X		X		X	X				
86.	Individual	James Tucker	Deseret Power	X									
87.	Individual	Michael Gammon	Kansas City Power & Light	X		X		X	X				

1. **The SDT has revised EOP-004-2 by removing Requirement 1, Part 1.4 and separating Parts 1.3 and 1.5 into new Requirements R3 and R4. Requirement R3 calls for an annual test of the communications portion of the Operating Plan and Requirement R4 requires an annual review of the Operating Plan. Do you agree with this revision? If not, please explain in the comment area below.**

Summary Consideration: Following review of the industry's comments, the SDT has re-examined the FERC Directive in Order 693 and has dropped both R3 and R4, as they were written and established a new Requirement R3 to have the Registered Entity "validate" the contact information in the contact list(s) they may have for the applicable events to their functional registration(s). This validation needs to be performed on a calendar year period to ensure that the list(s) have current and up-to-date contact data.

Organization	Yes or No	Question 1 Comment
Northeast Power Coordinating Council	No	Regarding Requirement R3, add the following wording from Measure M3 to the end of R3 after the wording "in Part 1.2.": The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. This language must be in the Requirement to be considered during an audit. Measures are not auditable. Regarding Requirement R4, replace the words "an annual review" with the words "a periodic review. "Add the following to R4: The frequency of such periodic reviews shall be specified in the Operating Plan and the time between periodic reviews shall not exceed five (5) years. This does not preclude an annual review in an Entity's operating plan. The Entity will then be audited to its plan. If the industry approves a five (5) year periodic review 'cap', and FERC disagrees, then FERC will have to issue a directive, state its reasons and provide justification for an annual review that is not arbitrary or capricious. Adding the one year "test" requirement adds to the administrative tracking burden and adds no reliability value.

Organization	Yes or No	Question 1 Comment
Response: The SDT thanks you for your comment. The SDT has removed R4 and revised R3 that calls for the responsible entity to validate contact information contain in the Operating Plan each calendar year as described in Requirement R1. The "Annual review" is used to ensure that the event reporting Operating Plan is up to date. If an entity experiences an event, communication evidence from the event may be used to show compliance.		
DECo	No	Should only have annual "review" requirement rather than test.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comment.		
Duke Energy	No	Under R3, we agree with testing communications internally. Just as the ERO is excluded under R3, other external entities should also be excluded. External communications should be verified under R4.
Response: The SDT thanks you for your comment. Due to industry opposition, the SDT revised Requirement R3 to remove test to "validate" contact information contained in the Operating Plan. If an entity experiences an actual event, communication evidence from the event may be used to show compliance with the validation requirement for the specific contacts used for the event.		
Dominion	No	While Dominion believes these are positive changes, we are concerned that placing actual calls to each of the "other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies" may be seen by one or more of those called as a 'nuisance call'. Given the intent is to insure validity of the contact information (phone number, email, etc), we suggest revising the standard language to support various forms of validation to include, documented send/receipt of email, documented verification of phone number (use of phone book, directory assistance, etc).
Response: The SDT thanks you for your comment. The SDT has made changes to the requirement highlighted in your comment.		

Organization	Yes or No	Question 1 Comment
SPP Standards Review Group	No	There needs to be a more granular definition of which entities should be included in the annual testing requirement in R3. To clarify what must be tested we propose the following language to replace the last sentence in M3. The annual test requirement is considered to be met if the responsible entity implements any communications process in the Operating Plan during an actual event. If no actual event was reported during the year, at least one of the communication processes in the Operating Plan must be tested to satisfy the requirement. We do not believe the time-stamping requirement in M3 and M4 contribute to the reliability of the BES. A dated review should be sufficient.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirement highlighted in your comments. The Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. If an entity experiences an actual event, communication evidence from the event may be used to show compliance with the validation requirement for the specific contacts used for the event. Time-stamping has been removed.		
Florida Municipal Power Agency	No	First, FMPA believes the standard is much improved from the last posting and we thank the SDT or their hard work. Having said that, there are still a number of issues, mostly due to ambiguity in terms, which cause us to vote Negative. R3 and R4 should be combined into a single requirement with two subparts, one for annual testing, and another to incorporate lessons learned from the annual testing into the plan (as opposed to an annual review).The word “test” is ambiguous as used in R3, e.g., does a table top drill count as a “test”? Is the intent to “test” the plan, or “test” the phone numbers, or what?
Response: The SDT thanks you for your comment. The SDT has made changes to the requirement highlighted in your comment.		
MRO NSRF	No	R3 states: Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. R1.2 states: A process for communicating each of the

Organization	Yes or No	Question 1 Comment
		applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies. With the use of "i.e." the SDT is mandating that each other entity must be contacted. The NSRF believes that the SDT meant that "e.g." should be used to provide examples. The SDT may wish to add another column to Attachment 1 to provide clarity. R3 requires and annual test that would include notification of:"other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies."Since NERC see no value in receiving these test notification we are doubtful other entities identified in R1.2 would find them of value. The real purpose of this requirement appears to be to assure operators are trained in the use of the procedure, process, or plan that assures proper notification. PER-005 already requires a systematic approach to training. It is hard to comprehend an organization not identifying this as a Critical Task, and if they failed to identify it as a Critical Task that this would not be a violation. Therefore this requirement is not required. Furthermore organizations test their response to events in accordance with CIP-008 R1.6. Therefore this requirement is covered by other standards and is not needed. The SDT may need to address this within M3, by stating "... that the annual test of the communication process of 1.2 (e.g. communication via e-mail, fax, phone, etc) was conducted". R4 states: Each Responsible Entity shall conduct an annual review of the event reporting Operating Plan in Requirement R1. We question the value of requiring an annual review. If the Standard does not change, there seems little value in requiring an annual review. This appears to be an administrative requirement with little reliability value. It would likely be identified as a requirement that that should be eliminated as part of the

Organization	Yes or No	Question 1 Comment
		request by FERC to identify strictly administrative requirements in FERC's recent order on FFTR. We suggest it be eliminated.
Response: The SDT thanks you for your comment. Requirement R3 called for test of all contact information contain. The SDT deleted Requirement R4 based on stakeholder comments and revised R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization. **The annual review requirement was maintained to meet the intent of NERC Order 693, Paragraph 466. The Commission does not specify a review period, as suggested; rather, believes that the appropriate period should be determined through the ERO's Reliability Standards.** **"The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."**		
ISO/RTO Standards Review Committee	No	The SRC offers comments regarding the posted draft requirements; however, by so doing, the SRC does not indicate support of the proposed requirements. Following these comments, please see the latter part of the SRC's response to Question 4 below for an SRC proposed alternative approach: Regarding the proposed posted requirements, without indicating support of those requirements, the SRC concurs with the changes as they provide better streamlining of the four key requirements, with enhanced clarity. However, we are unclear on the intent of Requirement R3, in particular the phrase "not including notification to the Electric Reliability Organization" which begs the question on whether or not the test requires notifying all the other entities as if it were a real event. This may create confusion in ensuring compliance and during audits. Suggest the SDT to review and modify this requirement as appropriate. Regarding part 1.2, the SRC requests that the text be terminated after the word "type" and before "i.e." As written, the requirement does not allow for the entity to add/remove others as necessary. Please consider combining R3 and R4.

Organization	Yes or No	Question 1 Comment
		These can be accomplished at the same time. The process should be evaluated to determine effectiveness when an exercise or test is conducted. The SDT is asked to review the proposal and to address the issue of requirements vs. bullets vs. sub-requirements. It is suggested that each requirement be listed independently, and that each sub-step be bulleted.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirement highlighted in your comment.		
ACES Power Marketing Standards Collaborators	No	(1) We agree with removing Part 1.4 and we agree with a requirement to periodically review the event reporting Operating Plan. However we are not convinced the review of the Operating Plan needs to be conducted annually. The event reporting Operating Plan likely will not change frequently so a biannual review seems more appropriate. (2) We also do not believe that Requirement R3 is needed at all. Requirement R3 compels the responsible entity to test their Operating Plan annually. We do not see how testing an Operating Plan that is largely administrative in nature contributes to reliability. Given that the drafting team is obligated to address the FERC directive regarding periodic testing, we suggest the Operating Plan should be tested biannually. This would still meet the FERC directive requiring periodic testing.
Response: The SDT thanks you for your comment. The SDT deleted Requirement R4 based on stakeholder comments and revised R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.		
Southern Company Services	No	There are approximately 17 event types for which Responsible Entities must have a process for communicating such events to the appropriate entities and R3 states that "The Responsible Entity shall conduct an annual test of the communications process". It is likely that the same communications process will be used to report multiple event types, so Southern suggest that

Organization	Yes or No	Question 1 Comment
		the Responsible Entities conduct an annual test for each unique communications process. Southern suggest that this requirement be revised to state "Each Responsible Entity shall conduct an annual test of each unique communications process addressed in R1.2". o In Attachment 1, for Event: "Damage or destruction of a Facility", SDT should consider removing "Results from actual or suspected intentional human action" from the "Threshold for Reporting" column. The basis for this suggestion is as follows: o The actual threshold should be measurable, similar to the thresholds specified for other events in Attachment 1. [Note: The first two thresholds identified (i.e., "Affects and IROL" and "Results in the need for actions to avoid an Adverse Reliability Impact") are measurable and sufficiently qualify which types of Facility damage should be reported.] o The determination of human intent is too subjective. Including this as a threshold will cause many events to be reported that otherwise may not need to be reported. (e.g., Vandalism and copper theft, while addressed under physical threats, is more appropriately classified as damage. These are generally intentional human acts and would qualify for reporting under the current guidance in Attachment 1. They may be excluded from reporting by the threshold criteria regarding IROLs and Adverse Reliability Impact, if the human intent threshold is removed.) o It may be more appropriate to address human intent in the event description as follows: "Damage or destruction of a Facility, whether from natural or human causes". Let the thresholds related to BES impact dictate the reporting requirement. o In Attachment 1, for Event: "Complete or partial loss of monitoring capability", SDT should consider changing the threshold criteria to state: "Affecting a BES control center for â‰¥ 30 continuous minutes such that analysis capability (State Estimator, Contingency Analysis) is rendered

Organization	Yes or No	Question 1 Comment
		inoperable." There may be instances where the tools themselves are out of commission, but the control center personnel have sufficiently accurate models and alternate methods of performing the required analyses.

Response: The SDT thanks you for your comment. The SDT has made changes to the requirement highlighted in your initial comment.

The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Under the Event Column, the SDT starts to classify each type of an event by assigning an "Event" title. The DSR SDT then updated the "Entity with Reporting Responsibilities" column to simply state what entity has the responsibility to report if they experience an event. The last column, "Threshold for Reporting" is a bright line that, if reached, the entity needs to report that they experienced the applicable event per Requirement 1.

Damage or destruction of a Facility:

The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state;

Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency.

This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).

This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.

Organization	Yes or No	Question 1 Comment
Progress Energy	No	It should be clear that the Operating Plan can be multiple procedures. It is an unnecessary burden to have entities create a new document outlining the Operating Plan. Having to create a new Operating Plan would not improve reliability and would further burden limited resources. The annual testing required by R3 should be clarified. Do all communication paths need to be annually tested or just one path? An actual event may only utilize one communication 'leg' or 'path' and leave others untested and utilized. Entities may have a corporate level procedure that 'hand-shakes' with more localized procedures that make up the entire Operating Plan. Must all communications processes be tested to fulfill the requirement? If an entity has 'an actual event' it is not necessarily true that their Operating Plan has been exercised completely, yet this one 'actual event' would satisfy M3 as written.
Response: The SDT thanks you for your comment. Regarding your initial comment on the need to create a new document, the SDT believes that a Registered Entity with a procedure under CIP-001 will be able to utilize that document as the starting point for the Operating Plan here. The SDT feels that many of the necessary components will already exist in that document and the Registered Entity should only need to edit it accordingly for the types of Events applicable to them. The SDT has made changes to the standard highlighted in your comment.		
Hydro One	No	In the Requirement R3, we suggest adding the following wording from Measure M3 to the end of R3 after the wording "in Part 1.2.": The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. This language must be in the Requirement to be considered during an audit. Measures are not auditable. Statement "... not including notification to the ERO..." as it stands now is confusing. We suggest that this statement is either reworded (and explained in the Rational for this requirement) or outright removed for clarity purposes In the requirement R4, we suggest replacing the words "an annual

Organization	Yes or No	Question 1 Comment
		review" with the words "a periodic review." Add the following to R4: The frequency of such periodic reviews shall be specified in the Operating Plan and the time between periodic reviews shall not exceed five (5) years. This does not preclude an annual review in an Entity's operating plan. The Entity will then be audited to its plan. If the industry approves a five (5) year periodic review 'cap,' and FERC disagrees, then FERC will have to issue a directive, state it reasons and provide justification for an annual review that is not arbitrary or capricious. Adding the one year "test" requirement adds to the administrative tracking burden and adds no reliability value. The table in the standard is clear regarding what events need to be reported. An auditor may want to see a test for "each" of the applicable events listed in EOP-004 Attachment 1.If the requirement for "an" annual test remains in the standard in R3, then it should be made clear that a test is not required for "each" of the applicable events listed in Attachment 1 (reference to R1.2.)
Response: The SDT thanks you for your comment. Each Responsible Entity must report and communicate events according to its Operating Plan based on the information in EOP-004 Attachment 1. The SDT removed the Operating Plan Process from Requirement 1 and revised the measure to meet the communications of Requirement R1, "to implement an operating plan within the time frames specified in Attachment 1." Requirement R3 called for test of all contact information contained. The SDT deleted Requirement R4 based on stakeholder comments and revised R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.		
CenterPoint Energy	No	CenterPoint Energy recommends that "and implement" be added after "Each Responsible Entity shall have" in Requirement R1. After such revision, Requirement R2 will not be needed as noted in previous comments submitted by the Company.

Organization	Yes or No	Question 1 Comment
		CenterPoint Energy also believes that Requirement R3 is not needed as an annual review encompassing the elements of the test described in the draft is sufficient.
Response: The SDT thanks you for your comment. The SDT considered the consolidation of the first and second requirements. However, since the requirements have the Registered Entity perform two distinct steps, a single requirement cannot be written to achieve multiple tasks. Each task must stand on its own and be judged singly. **The annual review helps ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.**		
Arkansas Electric Cooperative Corporation	No	AECC supports the comments submitted by ACES Power Marketing.
Response: The SDT thanks you for your comment. Please review the response directed to them.		
MWDSC	No	Transmission Owners (TO) should not be included as a "Responsible Entity" for this or other requirements because the Operating Plan is usually prepared by the Transmission Operator (TOP). For TOs who are not also TOPs, there are usually delegation agreements. CIP-001 never directly applied to TOs.
Response: The SDT thanks you for your comment. The SDT disagrees with your assessment, as the TOs are physical owners of the equipment that would be affected by this standard. As Owners of the equipment, they need to be reporting on what is happening to their equipment.		
Manitoba Hydro	No	(R1.1 and 1.2) It is unclear whether or not R1.1 and R1.2 require a separate recognition and communication process for each of the event types listed in Attachment 1 or if event types can be grouped as determined appropriate by the responsible entity given that identical processes will apply for multiple types of events. Manitoba Hydro suggests that wording is revised so

Organization	Yes or No	Question 1 Comment
		that multiple event types can be addressed by a single process as deemed appropriate by the Responsible Entity. (R3) It is unclear whether or not R3 requires the testing of the communications process for each separate event type identified in Attachment 1. If so, this would be extremely onerous. Manitoba Hydro suggests that only unique communication processes (as identified by the Responsible Entity in R1.2) require an annual test and that testing should not be required for each type of event listed in Attachment 1. As well, Manitoba Hydro believes that testing the communications process alone is not as effective as also providing training to applicable personnel on the communications process. Manitoba Hydro suggests that R3 be revised to require annual training to applicable personnel on the communications process and that only 1 test per unique communications process be required annually.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comments. Each Responsible Entity must report and communicate events according to its Operating Plan based on the information in EOP-004 Attachment 1. The SDT has attempted to clarify that it is the choice of the Registered Entity on whether one, or more than one, contact list(s) is needed for the differing types applicable to them. Depending upon your needs of who you have an obligation to report, you can elect to have one or multiple lists. **Requirement R3 called for test of all contact information contained. The SDT deleted Requirement R4 based on stakeholder comments and revised R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.**		
Occidental Power Services, Inc.	No	There should be an exception for LSEs with no BES assets from having an Operating Plan and, therefore, from testing and review of such plan. These LSEs have no reporting responsibilities under Attachment 1 and, if they have nothing ever to report, why would they have to have an Operating Plan and have to test and review it? This places an undue burden on small entities

Organization	Yes or No	Question 1 Comment
		that cannot impact the BES.
Response: The SDT thanks you for your comment. LSEs, as being applicable under the Cyber Security standards, were included in the applicability of this standard. Since the SDT is proposing to keep the Cyber Security reporting requirements in CIP-008, LSEs have been removed from the applicability of this standard. This action will not negate the LSE responsibilities under that standard and your comments will need to be addressed there.		
Xcel Energy	No	1) In R1.2, We understand what the drafting team had intended here. However, we are concerned that the way this requirement is drafted, using i.e., it could easily be interpreted to mean that you must notify all of those entities listed. Instead, we are suggesting that the requirement be rewritten to require entities to define in their Operating Plan the minimum organizations/entities that would need to be notified for applicable events. We believe this would remove any ambiguity and make it clear for both the registered entity and regional staff. We recommend the requirement read something like this: 1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to applicable internal and external organizations needed for the event type, as defined in the Responsible Entity's Operating Plan. 2) We also suggest that R3 be clarified as to whether communications to all organizations must be tested or just those applicable to the test event type/scenario.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comments.		
American Electric Power	No	R3: How many different scenarios need to be tested? For example, reporting sabotage-related events might well be different than reporting reliability-related events such as those regarding loss of Transmission. While these

Organization	Yes or No	Question 1 Comment
		examples might vary a great deal, other such scenarios may be very similar in nature in terms of communication procedures. Perhaps solely testing the most complex procedure would be sufficient. AEP agrees with the changes with R3 calling for an annual test provided the requirement R2 is modified to include the measure language "The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event." M3: While we agree that "the annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event", we believe it would be preferable to include this text in R3 in addition to M3. Measures included in earlier standards (some of which are still enforced today) had little correlation to the requirement itself, and as a result, those measures were seldom referenced. M3: It would be unfair to assume that every piece of evidence required to prove compliance would be dated and time-stamped, so we recommend removing the text "dated and time-stamped" from the first sentence so that it reads "Each Responsible Entity will have records to show that the annual test of Part 1.2 was conducted." The language regarding dating and time stamps in regards to "voice recordings and operating logs or other communication" is sufficient.
Response: The SDT thanks you for your comment. Based on stakeholder comments the SDT revised R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization. The SDT agrees with the point raised on time-stamping and has removed it from the standard.		
Entergy	No	The requirement for a "time stamped record" of annual review is unreasonable and unnecessary. A dated document showing that a review was performed should be sufficient.

Organization	Yes or No	Question 1 Comment
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comment. The SDT has removed time-stamping from the standard.		
New York Power Authority	No	Please see comments submitted by NPCC Regional Standards Committee (RSC).
Response: The SDT thanks you for your comment. Please review the response to the commenter.		
Consolidated Edison Co. of NY, Inc.	No	Requirement R3: Following the sentence ending "in Part 1.2" add the following wording from the Measure to R3: The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. This language must be in the Requirement to be considered during an audit. Measures are not auditable. Requirement R4: Replace the words "an annual review" with the words "a periodic review."Following the first sentence in R4 add: The frequency of such periodic reviews shall be specified in the Operating Plan and the time between periodic reviews shall not exceed five (5) years.
Orange and Rockland Utilities, Inc.	No	Requirement R3: Following the sentence ending "in Part 1.2" add the following wording from the Measure to R3: The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. This language must be in the Requirement to be considered during an audit. Measures are not auditable. Requirement R4: Replace the words "an annual review" with the words "a periodic review." Following the first sentence in R4 add: The frequency of such periodic reviews shall be specified in the Operating Plan and the time between periodic reviews shall not exceed five (5) years.
Response: The SDT thanks you for your comment. Based on stakeholder comments the SDT revised R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively		

Organization	Yes or No	Question 1 Comment
report events to assure situational awareness to the Electric Reliability Organization. The SDT considered various time frames for the action needed and felt that a calendar year was necessary due to the FERC Directive in Order 693 and to ensure that contact information remained useful in a timely manner.		
MidAmerican Energy	No	See the NSRF comments. The real purpose of this requirement appears to be to assure operators are trained in the use of the procedure, process, or plan that assures proper notification. PER-005 already requires a systematic approach to training. Reporting to other affected entities is a PER-005 system operator task. Therefore this requirement already covered by PER-005 and is not required. Organizations are also required to test their response to events in accordance with CIP-008 R1.6. Therefore this requirement is covered by other standards and is not needed. Inclusion of this standard would place entities in a double or possible triple jeopardy. The SDT may need to expand M3 reporting options, by stating "... that the annual test of the communication process of 1.2 (e.g. communication via e-mail, fax, phone, ect) was conducted". R4 is an administrative requirement with little reliability value and should be deleted. It would likely be identified as a requirement that that should be eliminated as part of the request by FERC to identify strictly administrative requirements in FERC's recent order on FFTR.
Response: The SDT thanks you for your comment. The SDT asks you to review the response to that commenter. The SDT disagrees with your understanding of the real purpose. Reporting of events listed in Attachment 1 is necessary for personnel beyond the operators. **The SDT deleted Requirement R4 based on stakeholder comments and revised Requirement R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.**		
Illinois Municipal Electric Agency	No	IMEA reluctantly (in recognition of the SDT's efforts and accomplishments to date) cast a Negative vote for this project primarily based on R3 because it is

Organization	Yes or No	Question 1 Comment
		attempting to fix a problem that does not exist and impacts small entity resources in particular. IMEA is not aware of seeing any information regarding a trend, or even a single occurrence for that matter, in a failure to report an event due to failure in reporting procedures. A small entity is less likely to experience a reportable event, and therefore is less likely to be able to take advantage of the provision in M3 to satisfy the annual testing through implementation of an actual event. If there is a problem that needs to be fixed, it would make much more sense to replace the language in R3 with a simple requirement for the RC, BA, IC, TSP, TOP, etc. to inform the TO, DP, LSE if there is a change in contact information for reporting an event. It is hard to believe that an RC, BA, IC, TSP, TOP, etc. is going to want to be annually handling numerous inquiries from entities regarding the accuracy of contact information. The impact of unnecessary requirements on entity resources, particularly small entities', is finally starting to get some meaningful attention at NERC and FERC. It would be a mistake to adopt another unnecessary requirement as currently specified in R3.
Response: The SDT thanks you for your comment. The SDT has revised Requirement R3 to help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.		
Amercican Transmission Company, LLC	No	ATC recommends eliminating R4 altogether. If R3, the annual test, is conducted as part of the Operating Plan, R4 is merely administrative, and does not add value to reliability.
Response: The SDT thanks you for your comment. The SDT deleted Requirement R4 based on stakeholder comments and revised Requirement R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.		
NextEra Energy Inc	No	NextEra Energy, Inc. (NextEra) does not agree that annual reviews and

Organization	Yes or No	Question 1 Comment
		annual tests should be mandated via Reliability Standards; instead, NextEra believes it is more appropriate to require that the Operating Plan be up-to-date and reviewed/tested as the Responsible Entity deems necessary. These enhancements provide for a robust Operating Plan, without arbitrary deadlines for a review and testing. It also provides Responsible Entities of different sizes and configurations the flexibility to efficiently and effectively integrate compliance with operations. Thus, NextEra requests that R1 be revised to read: "Each Responsible Entity shall have an up-to-date event reporting Operating Plan that is tested and reviewed as the Responsible Entity deems necessary and includes: ...". Consistent with these changes NextEra also requests that R3 and R4 be deleted.
Response: The SDT thanks you for your comment. While the SDT recognizes the simplicity that your comment would bring, it cannot be implemented in that manner. For auditability reasons, each task must be separate and distinct in order for the performance to be assessed. Alternatively, the SDT has re-constructed three distinct requirements that can be judged and evaluated on their own with compromising the others.		
ISO New England Inc	No	Due to the FERC mandate to assign VRFs/VSLs, we do not support using subrequirements and, instead, favor the use of bullets when the subrequirements are not standalone but rely on the partent requirement.
Response: The SDT thanks you for your comment. The SDT has revised the language and removed all subrequirements.		
Exelon Corporation and its affiliates	No	It's not clear that R3 and R4 need to be separated. Consider revising R3 to read: "Through use or testing, verify the operability of the plan on an annual basis" and dropping R4.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comment.		

Organization	Yes or No	Question 1 Comment
Indiana Municipal Power Agency	No	IMPA does not believe that both R3 and R4 are necessary and they are redundant to a degree. Generally, when performing an annual review of a process or procedure, the call numbers for agencies or entities are verified to be up to date. Also, in R3, what does “test” mean. It could mean have different meanings to registered entities and to auditors which does not promote consistency among the industry. IMPA recommends going with an annual review of the process and having the telephone numbers verified that are in the event reporting Operating Plan. IMPA also believes that the local and federal law enforcement agencies would rather go with a verification of contact information over being besieged by "test" reports. The way R3 is written gives the appearance that the SDT did not want to overwhelm the ERO with all of the "test" reports from the registered entities (by excluding them from the test notification).
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comment.		
ERCOT	No	ERCOT has joined the IRC comments on this project and offers these additional comments. ERCOT requests that the measure be updated to say “acceptable evidence may include”. As written, the measure reads that there is only one way to comply with the requirement. The Standards should note "what" an entity is required to do and not prescribe the "how".
Response: The SDT thanks you for your comment. The SDT has made changes to the standard highlighted in your comment.		
Brazos Electric Power Cooperative	No	Please see the comments submitted by ACES Power Marketing.
Response: The SDT thanks you for your comment. Please review the response to that commenter.		
Central Lincoln	No	The new language of R3 and R4 provide nothing to clarify the word “annual.” We note that while a Compliance Application Notice was written on this,

Organization	Yes or No	Question 1 Comment
		Central Lincoln believes that standards should be written so they do not rely on the continually changing CANs. CAN-0010 itself implies that "annual" should be defined within the standards themselves. We suggest: R3 Each Responsible Entity shall conduct a test of the communications process in R1 Part 1.2, not including notification to the Electric Reliability Organization, at least once per calendar year with no more than 15 calendar months between tests.R4 Each Responsible Entity shall conduct a review of the event reporting Operating Plan in Requirement R1. at least at least once per calendar year with no more than 15 calendar months between reviews.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comment.		
Kansas City Power & Light	No	Requirement 3 requires a test of the communications in the operating plan. A test implies a simulation of the communications part of the operating plan by actual communications being conducted pursuant to the plan. It is not appropriate to burden agencies with testing of communications under a test environment. Recommend the drafting team consider a confirmation of the contact information with various agencies as the operations plan dictates.
Response: The SDT thanks you for your comment. SDT has made changes to the requirements highlighted in your comment.		
Bonneville Power Administration	Yes	BPA believes that the annual testing and review as described in R3 is too cumbersome and unnecessary for entities with large footprints to inundate federal and local enforcement bodies such as the FBI for "only" testing and the documenting for auditing purposes. BPA suggests that testing be performed on a bi-annual or longer basis.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comment; however, the SDT has decided that the period will be shorter than your suggestion based upon comments received from all parties.		

Organization	Yes or No	Question 1 Comment
Seattle City Light	Yes	This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
Response: The SDT thanks you for your comment. Please review the response to Question 4.		
Utility Services	Yes	While agreeing with the change, confusion may exist with the CAN that exists for the term "Annual". Utility Services suggests that the language be changed to "Every calendar year" or something equivalent. Given everything that transpired in the discussion on the term annual, using a different phrase may be advantageous.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirement highlighted in your comment.		
United Illuminating Company	Yes	R3 should be clear that the annual test of the plan does not mean each communication path for each applicable event on an annual basis.
Response: The SDT thanks you for your comment. Requirement R3 has been rewritten to address comments like yours and other industry members. While testing is no longer a part of the requirement, validating the contact information associated with each contact list for each applicable event type is.		
Ingleside Cogeneration LP	Yes	Ingleside Cogeneration LP agrees that it is appropriate to test reporting communications on an annual basis, primarily to validate that phone numbers, email ids, and contact information is current. We appreciate the project team's elimination of the terms "exercise" and "drill", which we believe connotates a formalized planning and assessment process. An annual review of the Operating Plan implies a confirmation that linkages to sub-processes remain intact and that new learnings are captured. We also agree that it is appropriate only to require an updated Revision Level Control chart entry as evidence of compliance - it is very likely that no updates are required after the review is complete. In our view, both of these requirements are sufficient to assure an effective assessment of all facets of

Organization	Yes or No	Question 1 Comment
		the Operating Plan. As such, we fully agree with the project team's decision to delete the requirement to update the plan within 90 days of a change. In most cases, our internal processes will address the updates much sooner, but there is no compelling reason to include it as an enforceable requirement.
Response: The SDT thanks you for your comment.		
City of Austin dba Austin Energy	Yes	Austin Energy (AE) supports the requirements for (1) an annual test of the communications portion of the Operating Plan (R3) and (2) an annual review of the Operating Plan (R4); however, we offer a slight modification to the measures associated with those requirements. AE does not believe that records evidencing such test and reviews need to be time-stamped to adequately demonstrate compliance with the requirements. In each case, we recommend that the first sentence of M3 and M4 start with "Each Responsible Entity will have dated records to show that the annual ..."
Response: The SDT thanks you for your comment. The SDT has removed the time-stamping provision in the standard.		
Springfield Utility Board	Yes	o SUB supports the removal of Requirement 1, Part 1.4, as well the separation of Parts 1.3 and 1.5, agreeing that they are their own separate actions. o The Draft 4 Version History still lists the term "Impact Event" rather than "Event".
Response: The SDT thanks you for your comment. The SDT has made changes highlighted in your comment.		
FirstEnergy Corp	Yes	FE agrees with the revision but has the following comments and suggestions: 1. We request clarity and guidance on R3 (See our comments in Question 4 for further consideration). Also, we suggest a change in the phrase "shall conduct an annual test" to "shall conduct a test each calendar year, not to exceed 15 calendar months between tests". This wording is consistent with other

Organization	Yes or No	Question 1 Comment
		standards in development such as CIP Version 5.2. 2. In R4 we suggest a change in the phrase "shall conduct an annual review" to "shall conduct a review each calendar year, not to exceed 15 calendar months between reviews". This wording is consistent with other standards in development such as CIP Version 5.
Response: The SDT thanks you for your comment. The SDT deleted Requirement R4 based on stakeholder comments and revised Requirement R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.		
Independent Electricity System Operator	Yes	We concur with the changes as they provide better streamlining of the four key requirements, with enhanced clarity. However, we are unclear on the intent of Requirement R3, in particular the phrase "not including notification to the Electric Reliability Organization" which begs the question on whether or not the test requires notifying all the other entities as if it were a real event. This may create confusion in ensuring compliance and during audits. Suggest the SDT to review and modify this requirement as appropriate.
Response: The SDT thanks you for your comment. The SDT has revised the standard's language to address this concern.		
Public Utility District No. 1 of Snohomish County	Yes	This is an excellent improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
Seattle City Light	Yes	This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
MEAG Power	Yes	This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
Response: The SDT thanks you for your comment. Please review the response to Question 4.		

Organization	Yes or No	Question 1 Comment
Tacoma Power	Yes	Tacoma Power agrees with the requirement but would suggest removing all instances the word "Operating" from the Standard. The requirements should read, " Each Responsible Entity shall have an "Event Reporting Plan...".The term Operating in this context is confusing as there are many other "Operating Plans" for other defined emergencies. This standard is about "Reporting" and should be confined to that.
Response: The SDT thanks you for your comment. The SDT has chosen to include "Operating" due to the definition in the NERC Glossary. The SDT believes Operating Plan clearly defines what is needed in this standard.		
Idaho Power Co.	Yes	But this is going to require that we create a new Operating Plan with test procedures and revision history.
Response: The SDT thanks you for your comment. The SDT believes that an existing procedure, that meets the requirements of CIP-001-2a, may well be the starting point for the Operating Plan in this standard, or could go a long way towards achieving the requirements in this standard. The SDT revised Requirement R3 to remove test to "validate" contact information contained in the Operating Plan. If an entity experiences an actual event, communication evidence from the event may be used to show compliance with the validation requirement for the specific contacts used for the event.		
American Public Power Association	Yes	APPA appreciates the SDT making these requirements clearer as requested in our comments on the previous draft standard.
Response: The SDT thanks you for your comment.		
Puget Sound Energy, Inc.	Yes	This draft is a considerable improvement on the previous draft in terms of clarity and will be much easier for Responsible Entities to implement. Puget Sound Energy appreciates the drafting team's responsiveness to stakeholder's concerns and the opportunity to comment on the current draft. The drafting team should revise Requirement R2 to state that the "activation" of the Operating Plan is required only when an event occurs, instead of using the term "implement". "Implementation" could also refer

Organization	Yes or No	Question 1 Comment
		to the activities such as distributing the plan to operating personnel and training operating personnel on the use of the plan. These activities are not triggered by any event and, since it is clear from the measure that this requirement is intended to apply only when there has been a reportable event, the requirement should be revised to state that as well. The drafting team should revise measure M2 to require reports to be "supplemented by operator logs or other reporting documentation" only "as necessary". In many cases, the report itself and time-stamped record of transmittal will be the only documents necessary to demonstrate compliance with requirement R2.Under Requirement R3, using an actual event as sufficient for meeting the requirement for conducting an annual test would likely fall short of demonstrating compliance with the entire scope of the Operating Plan. R1.2 requires "a process for communicating EACH of the applicable events listed....". If the actual event is only one of many "applicable" events, is it sufficient to only exercise one process flow? If there is no actual event during the annual time-frame, do all the process flows then have to be exercised?
Response: The SDT thanks you for your comment. The SDT appreciates the suggestion; however, to be consistent with other reliability standards, the SDT has elected to continue to use the word "Implement." Your suggestion could end up creating confusion and misunderstandings since the context is not used elsewhere. **The SDT has revised the language the requirements and measures as a result of your and other commenter's remarks.**		
FMPP		See FMPA's comments
Response: The SDT thanks you for your comment. Please review the response to the FMPA comments.		

Organization	Yes or No	Question 1 Comment
Luminant	Yes	
BC Hydro	Yes	
Imperial Irrigation District (IID)	Yes	
LG&E and KU Services	Yes	
PPL Corporation NERC Registered Affiliates	Yes	
Avista	Yes	
PNGC Comment Group	Yes	
Colorado Springs Utilities	Yes	
Arizona Public Service Company	Yes	
Georgia System Operations Corporation	Yes	
Texas Reliability Entity	Yes	
Dynegy Inc.	Yes	
Clark Public Utilities	Yes	
Pepco Holdings Inc	Yes	
Farmington Electric Utility System	Yes	

Organization	Yes or No	Question 1 Comment
Public Service Enterprise Group	Yes	
PPL Electric Utilities	Yes	
Cowlitz County PUD	Yes	
Edison Mission Marketing & Trading, Inc.	Yes	
Ameren	Yes	
We Energies	Yes	
GTC	Yes	
MISO	Yes	
Oncor Electric Delivery	Yes	
Los Angeles Department of Water and Power	Yes	
Deseret Power	Yes	

2. The SDT made clarifying revisions to Attachment 1 based on stakeholder feedback. Do you agree with these revisions? If not, please explain in the comment area below.

Summary Consideration:

The SDT reviewed, discussed and updated Attachment 1 based on comments received for commenters, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Under the Event Column, the SDT starts to classify each type of an event by assigning an "Event" title. The DSR SDT then updated the "Entity with Reporting Responsibilities" column to simply state which entity has the responsibility to report if they experience an event. The last column, "Threshold for Reporting" is a bright line that, if reached, the entity needs to report that they experienced the applicable event per Requirement 1.

Organization	Yes or No	Question 2 Comment
Northeast Power Coordinating Council	No	Regarding Attachment 1, language identical to event descriptions in the NERC Event Analysis Process and FERC OE-417 should be used. Creating a third set of event descriptions is not helpful to system operators. Recommend aligning the Attachment 1 wording with that contained in Attachment 2, DOE Form OE-417 and the EAP whenever possible. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Using identical terminology will be difficult to achieve as the DOE form and EAP have differing processes for identification of the reportable incidences. The SDT has tried to set up the reportable events in the standard to be as similar as possible to the other organizations without being tied to their specific language. Attachment 2 has been modified to match the events types listed in Attachment 1.** The following pertains to Attachment 1:Replace the Attachment 1 "NOTE" with the following clarifying wording: NOTE: The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of Attachment 2 if the entity is required to submit an OE-417 report. Submit reports to

Organization	Yes or No	Question 2 Comment
		the ERO via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422. Initial submittal by Voice within the reporting time frame is acceptable for all events when followed by a hardcopy submittal by Facsimile or e-mail as and if required. **The SDT thanks you with your comment. First, the SDT believes that you intended the comment to address the "Note" on Attachment 2, not Attachment 1. The SDT does not believe that a hardcopy report is necessary if the organization has made voice contact.** The proposed "events" are subjective and will lead to confusion and questions as to what has to be reported. **The SDT disagrees and has established "events" to be reported based on bright line criteria. The events are consistent with previous versions of the CIP-001 and EOP-004 standards, as well as incidences being reporting to the DOE and EAP.** Event: A reportable Cyber Security Incident. All reportable Cyber Security Incidents may not require "One Hour Reporting." A "one-size fits all" approach may not be appropriate for the reporting of all Cyber Security Incidents. The NERC "Security Guideline for the Electricity Sector: Threat and Incident Reporting" document provides time-frames for Cyber Security Incident Reporting. For example, a Cyber Security Compromise is recommended to be reported within one hour of detection, however, Information Theft or Loss is recommended to be reported within 48 hours. Recommend listing the Event as "A confirmed reportable Cyber Security Incident. The existing NERC "Security Guideline for the Electricity Sector: Threat and Incident Reporting" document uses reporting time-frames based on "detection" and "discovery." Recommend using the word confirmed because of the investigation time that may be required from the point of initial "detection" or "discovery" to the point of confirmation, when the compliance "time-clock" would start for the reporting requirement in EOP-004-2. **The SDT is revising the standard to not contain reporting for Cyber Security incidents. Under the revisions, CIP-008-3 and successive versions will retain the**

Organization	Yes or No	Question 2 Comment
		reporting requirements. Event: Damage or destruction of a Facility Threshold for Reporting: revise language on third item to read: Results from actual or suspected intentional human action, excluding unintentional human errors. **The SDT reviewed, discussed and updated "Damage and destruction of a Facility" based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. The new "threshold" now states:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** Event: Any physical threat that could impact the operability of a Facility This Event category should be deleted. The word "could" is hypothetical and therefore

Organization	Yes or No	Question 2 Comment
		unverifiable and un-auditable. The word "impact" is undefined. Please delete this reporting requirement, or provide a list of hypothetical "could impact" events, as well as a specific definition and method for determining a specific physical impact threshold for "could impact" events other than "any." **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whomever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** Event: BES Emergency requiring public appeal for load reduction. Replace wording in the Event column with language from #8 on the OE-417 Reporting Form to eliminate reporting confusion. Following this sentence add, "This shall exclude other public

Organization	Yes or No	Question 2 Comment
		appeals, e.g., made for weather, air quality and power market-related conditions, which are not made in response to a specific BES event." **The SDT disagrees with quantifying a use of public appeals reporting for different types of events. The important item here is that a public appeal was issued for load reduction. A report is required to inform the ERO (and whoever else the entity wishes to inform per Requirement R1) of your current status and provide them with the situational awareness of the status of your system.** Event: Complete or partial loss of monitoring capability Event wording: Delete the words "or partial" to conform the wording to the NERC Event Analysis Process. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event now only applies to "Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.** Event: Transmission Loss Revise to BES Transmission Loss **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** Event: Generation Loss Revise to BES Generation Loss **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT**

Organization	Yes or No	Question 2 Comment
		removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."** **The SDT believes that if an entity reaches this threshold, it needs to be reported and most likely this will be BES connected generation assets.**
Response: The SDT thanks you for your comment.		
DECo	No	On pg 17 in the Rationale Box for EOP-004 Attachment 1: The set of terms is specific then includes the word ETC. Then further lists areas to exclude. Then on Pg 23 of document it includes train derailment near a transmission right of way and forced entry attempt into a substation facility as reportable. These conflict. Also see conflict when in pg 21 states the DOE OE417 would be excepted in lieu of the NERC form, but on the last pg it states the DOE OE417 should be attached to the NERC report indicating the NERC report is still required.
Response: The SDT thanks you for your comment. While the SDT would like to point out the "etc." is the last word in the definition of Facility; the SDT has removed footnote 1 and the forced intrusion statement has been removed. The SDT has updated to remove the conflict of "attached to the NERC report…" The SDT agrees with your comments and have revised the standard to address these discrepancies.		
Duke Energy	No	(1)We disagree with reporting CIP-008 incidents under this standard. We agree with the one-hour notification timeframe, but believe it should be in CIP-008 to avoid double jeopardy. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one-hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement.** (2)Damage or destruction of a Facility - Need clarity on how a vertically integrated

Organization	Yes or No	Question 2 Comment
		entity must report. For example a GOP probably won't know if an IROL will be affected. Also, there shouldn't be multiple reports from different functional entities for the same event. Suggest splitting this table so that GO, GOP, DP only reports "Results from actual or suspected intentional human action". **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of its Facility that results from actual or suspected intentional human action.** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per R1) the situational awareness that the Facility was 'damaged or destroyed' intentionally by a human."** **This event was written to cover the increase of "Entity with Reporting Responsibility," and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** (3)Generation Loss - Need more clarity on the threshold for reporting. For example if

Organization	Yes or No	Question 2 Comment
		we lose one 1000 MW generator at 6:00 am and another 1000 MW generator at 4:00 pm, is that a reportable event? **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."**
Response: The SDT thanks you for your comment.		
Luminant	No	Luminant appreciates the work of the SDT to modify Attachment 1 to address the concerns of the stakeholders. However, we are concerned that the threshold for reporting a Generation Loss in the ERCOT interconnection established by this revision is set at â‰¥ 1,000MW, which is not consistent with the level of single generation contingency used in ERCOT planning and operating studies. That level of contingency is currently set at the size of the largest generating unit in ERCOT, which is 1,375MW. For this reason, Luminant believes that the minimum threshold for reporting of a disturbance should be > 1,375MW for the ERCOT Interconnection.
Response: The SDT thanks you for your comment. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."** **The SDT discussed this issue and believes that ERCOT could change contingency level in the future, and this event is also applicable to the Quebec Interconnection.**		

Organization	Yes or No	Question 2 Comment
BC Hydro	No	BC Hydro supports the revisions to EOP-004 and would vote Affirmative with the following change. Attachment 1 has a One Hour Reporting requirement. BC Hydro proposes a One Hour Notification with the Report submitted within a specified timeframe afterward.
Response: The SDT thanks you for your comment. The SDT has removed all incidences involving one-hour reporting threshold; therefore, the SDT does not see the need to make this change.		
Bonneville Power Administration	No	BPA believes that clarifying language should be added to transmission loss event. (Page 19) [a report should not be required if the number of elements is forced because of pre-designed or planned configuration. System studies have to take such a configuration into account possible wording could be. Unintentional loss of three or more Transmission Facilities (excluding successful automatic reclosing or planned operating configuration)] **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** In addition, under the "Event" of Complete or partial loss of monitoring capability, BPA believes that "partial loss" is not sufficiently specific for BPA to write compliance operating procedures and suggest defining partial loss or removing it from the standard. Should the drafting team add clarifying language to remove "or partial loss" and address BPA's concerns on over emphasis on software tool to the operation of the system. BPA would change its negative position to affirmative. **The SDT has revised the language on this point in Attachment 1.**
Response: The SDT thanks you for your comment.		

Organization	Yes or No	Question 2 Comment
SPP Standards Review Group	No	To obtain an understanding of the drivers behind the events in Attachment 1, we would like to see where these events come from. If the events are required in standards, refer to them. If they are in the existing event reporting list, indicate so. If they are coming from the EAP, let us know. We have a concern that, as it currently exists, Attachment 1 can increase our reporting requirements considerably. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Reportable events should be similar, but not identical to the events reported to DOE or EAP.** We also have concerns about what appears to be a lack of coordination between EAP reporting requirements and those contained in Attachment 1. For example, the EAP reporting requirement is for the complete loss of monitoring capability whereas Attachment 1 adds the requirement for reporting a partial loss of monitoring capability. It appears that some of the EAP reporting requirements are contained in Attachment 1. We have concerns that this is beyond the scope of the SAR and should not be incorporated in this standard. **The SDT has revised the language on this point in Attachment 1. It should be noted that the EAP can use reports submitted under EOP-004-2 as the initial notification of an event that could be further addressed in the EAP.** We have concern with several of the specific event descriptions as contained in Attachment 1: Damage or destruction of a Facility - We are comfortable with the proposed definition of Adverse Reliability Impact but have concerns with the existing definition of ARI. Any physical threat that could impact the operability of a Facility1 - We take exception to this event in that is goes beyond what is currently required in EOP-004-1, including DOE reporting requirements, and the EAP reporting requirements. We do not understand the need for this event type and object to the potential for excessive

Organization	Yes or No	Question 2 Comment
		reporting required by such an event type. Additionally, we are concerned about the potential for multiple reporting of a single event. This same concern applies to several other events including Damage or destruction of a Facility, Loss of firm load for â‰¥ 15 minutes, System separation, etc. When multiple entities are listed as the Entity with Reporting Responsibility, Attachment 1 appears to require each entity in the hierarchy to submit a report. There should only be one report and it should be filed by the entity owning the event. The SDT addressed this issue in its last posting but the issue still remains and should be reviewed again. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** **The SDT understands that there may be several reports of a single event; and as the SDT has stated before, that this will give the ERO a better understanding of the**

Organization	Yes or No	Question 2 Comment
		depth and breathe of system conditions based on the given event. BES Emergency resulting in automatic firm load shedding - For some reason, not stipulated in the Consideration of Comments, the action word in the Entity with Reporting Responsibility was changed from 'experiences' to 'implements'. We recommend changing it back to 'experiences'. Automatic load shedding is not implemented. It does not require human intervention. It's automatic. Voltage deviation on a Facility - Similar to the comment on automatic load shedding above, the action word was changed from 'experiences' to 'observes'. We again recommend that it be changed back to 'experiences'. Using observes obligates a TOP, who is able to see a portion of a neighboring TOP's area, to submit a report if that TOP observed a voltage deviation in the neighboring TOP's area. The only reporting entity in this event should be the TOP within whose area the voltage deviation occurred. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Automatic firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)."** **This language clearly states that an entity reports if the threshold is reached.** Complete or partial loss of monitoring capability - Clarification on partial loss of monitoring capability and inoperable are needed. Also, the way the Threshold is written, it implies that a State Estimator and Contingency Analysis are required. To tone this down, insert the qualifier 'such as' in front of State Estimator. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event now only applies to "Complete loss of monitoring capabilities" for a RC, BA, or TOP when there is a complete loss of monitoring**

Organization	Yes or No	Question 2 Comment
		capabilities for 30 continuous minutes where their State Estimator or Contingency Analysis is inoperable. This will only apply to an RC, BA, or TOP who have this capability to start with.
Response: The SDT thanks you for your comment.		
Florida Municipal Power Agency	No	The bullet on "any physical threat" is un-measurable. What constitutes a "threat"? FMPA likes the language used in the comment form discussing this item concerning the judgment of the Responsible Entity, but, the way it is worded in Attachment 1 will mean the judgment of the Compliance Enforcement Authority, not the Responsible Entity. Presumably, the Responsible Entity will need to develop methods to identify physical threats in accordance with R1; hence, FMPA suggests rewording to: "Any physical threat recognized by the Responsible Entity through processes established in R1 bullet 1.1". We understand this introduces circular logic, but, it also introduces the "judgment of the Responsible Entity" into the bullet. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility." This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or**

Organization	Yes or No	Question 2 Comment
		activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event, unless it degrades the normal operation of a Facility. On the row of the table on voltage deviation, replace the word "observes" with "experiences". It is possible for one TOP to "observe" a voltage deviation on another TOP's system. It should be the responsibility of the TOP experiencing the voltage deviation on its system to report, not the one who "observes". On the row on islanding, it does not make sense to report islanding for a system with load less than the loss of load metrics and we suggest using the same 300 MW threshold for a reporting threshold. On the row on generation loss, some clarification on what type of generation loss (especially in the time domain) would help it be more measurable, e.g., concurrent forced outages. One the row on transmission loss, the same clarity is important, e.g., three or more concurrent forced outages. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Automatic firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)."** **This language clearly states that an entity reports if the threshold is reached.** On the row on loss of monitoring, while FMPA likes the threshold for "partial loss of monitoring capability" for those systems that have State Estimators, small BAs and TOPs will not need or have State Estimators and the reporting threshold becomes ambiguous. We suggest adding something like loss of monitoring for 25% of monitored points for those BAs and TOPs that do not have State Estimators.

Organization	Yes or No	Question 2 Comment
		The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event now only applies to "Complete loss of monitoring capabilities" for a RC, BA, or TOP when there is a complete loss of monitoring capabilities for 30 continuous minutes where their State Estimator or Contingency Analysis is inoperable. This will only apply to an RC, BA, or TOP who have this capability to start with.
Response: The SDT thanks you for your comment.		
LG&E and KU Services	No	The SDT should consider more clearly defining the Threshold for Reporting for the Event: "Any physical threat that could impact the operability of a Facility" to only address those events that have an Adverse Reliability Impact. Some proposed language might be: "Threat to a Facility excluding weather related threats that could result in an Adverse Reliability Impact."For those events specifically defined in the ERO Events Analysis Process, the SDT should consider revising the language to be more consistent with the language included in the ERO Events Analysis Process. Here is some recommended language: 1. EVENT: Transmission loss THRESHOLD FOR REPORTING: "Unintentional loss, contrary to design, of three or more BES Transmission Facilities (excluding successful automatic reclosing) caused by a common disturbance. **The SDT has taken your comment into consideration and this threshold for reporting now states:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** 2. EVENT: "Complete or partial loss of monitoring capability" - could be revised to read "Complete loss of SCADA control or monitoring functionality" THRESHOLD FOR REPORTING: "Affecting a BES control center for â‰¥ 30 continuous minutes such that analysis tools (e.g. State Estimator, Contingency Analysis) are rendered inoperable". **The SDT reviewed, discussed and updated Attachment 1 based on comments**

Organization	Yes or No	Question 2 Comment
		received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event now only applies to: **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.**
Response: The SDT thanks you for your comment.		
MRO NSRF	No	R1.2 states: A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies. This implies not only does NERC need to be notified within the specified time period but that: "other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies." are also required to be notified within in the time periods specified. We suggest a forth column be added to the table to clearly identify who must be notified within the specified time period or that R1.2 be revised to clearly state that only NERC must be notified to comply with the standard. With the use of "i.e." the SDT is mandating that each other entity must be contacted. The NSRF believes that the SDT meant that "e.g." should be used to provide examples. The SDT may wish to add another column to Attachment 1 to provide clarity. **The SDT has made the required change concerning replacing "i.e." with "e.g."** Also with regards to Attachment 1, the following comments are provided: 1. Instead of referring to CIP-008 (in the 1 hour reporting section), quote the words from CIP-008, this will require coordination of future revisions but will assure clarity in reporting requirements. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we**

Organization	Yes or No	Question 2 Comment
		have remanded the one-hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement. 2. Under "Damage or destruction of a Facility" a. The wording "affects an IROL (per FAC-014)," is too vague. Many facilities could affect an IROL, not as many if lost would cause an IROL. b. Adverse Reliability Impact is defined as:"The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection."There are an infinite number of routine events that result in the loss of generation plants due to inadvertent actions that somehow also damaged equipment. Any maintenance activity that damaged a piece of equipment that causes a unit to trip or results in a unit being taken off line in a controlled manner would now be reportable. This seems to be an excessive reporting requirement. Recommend that Adverse Reliability Impact be deleted and be replaced with actual EEA 2 or EEA 3 level events. c. The phrase "Results from actual or suspected intentional human action." This line item used the term "suspected" which relates to "sabotage". Recommend the following: Results from actual or malicious human action intended to damage the BES. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency.** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any**

Organization	Yes or No	Question 2 Comment
		abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** 3. "Any physical threat that could impact the operability of a Facility1"The example provided by the drafting team of a train derailment exemplifies why this requirement should be deleted. A train derailment of a load of banana's more than likely would not threaten a nearby BES Facility. However a train carrying propane that derails carrying propane could even if it were 10 miles away. Whose calculation will be used to determine if an event could have impacted the asset? As worded there is too much ambiguity left to the auditor. We suggest the drafting team clarify by saying "Any event that requires the a BES site be evacuated for safety reasons" Furthermore if weather events are excluded, we are hard pressed to understand why this information is important enough to report to NERC. So barring an explanation of the purpose of this requirement, including why weather events would be excluded, we suggest the requirement be deleted. Please note that if you align this with "Physical attack" with #1 of the OE-417. This clearly states what the SDT is looking for. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry**

Organization	Yes or No	Question 2 Comment
		comments to state: **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** 4. The phrase "or partial loss of monitoring capability" is too vague. Further definitions of "inoperable" are required to assure consistent application of this requirement. Recommend that "Complete loss of SCADA affecting a BES control center for â‰¥ 30 continuous minutes such that analysis tools of State Estimator and/or Contingency Analysis are rendered inoperable. Or, Complete loss of the ability to perform a State Estimator or Contingency Analysis function, the threshold of 30 mins is too short. A 60 min threshold will align with EOP-008-1, R1.8. Since this is the time to implement the contingency back up control center plan. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event now only applies to:** **"Complete loss of monitoring capability affecting a BES control center for 30**

Organization	Yes or No	Question 2 Comment
		continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with. 5. Event: Voltage deviation on a Facility. ATC believes that the term "observes" for Entity with Reporting Responsibility be changed back to "experiences" as originally written. The burden should rest with the initiating entity in consistency with other Reporting Responsibilities. Also, for Threshold for Reporting, ATC believes the language should be expanded to - plus or minus 10% "of target voltage" for greater than or equal to 15 continuous minutes. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.** 6. Event: Transmission loss. ATC recommends that Threshold for Reporting be changed to read "Unintentional loss of four, or more Transmission Facilities, excluding successful automatic reclosing, within 30 seconds of the first loss experienced and for 30 continuous minutes. Technical justification or Discussion for this recommended change: In the instance of a transformer-line-transformer, scenario commonly found close-in to Generating stations, consisting of 3 defined "facilities", 1 lightning strike can cause automatic unintentional loss by design. Increase the number of facilities to 4. In a normal shoulder season day, an entity may experience the unintentional loss of a 138kv line from storm activity, at point A in the morning, a loss of a 115kv line from a different storm 300 miles from point A in the afternoon, and a loss of 161kv line in the evening 500 miles from point A due to a

Organization	Yes or No	Question 2 Comment
		failed component, if it is an entity of significant size. Propose some type of time constraint. Add time constraint as proposed, 30 seconds, other than automatic reclosing. In the event of dense lightning occurrence, the loss of multiple transmission facilities may occur over several minutes to several hours with no significant detrimental effect to the BES, as load will most certainly be affected (lost due to breaker activity on the much more exposed Distribution system) as well. Any additional loss after 30 seconds must take into account supplemental devices with intentional relay time delays, such as shunt capacitors, reactors, or load tap changers on transformers activating as designed, arresting system decay. In addition, Generator response after this time has significant impact. Please clarify or completely delete why this is included within this version when no basis has been give and it is not contained within the current enforceable version. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2.** **The SDT has taken your comment into consideration and this threshold for reporting now states:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** 7. Modify the threshold of "BES emergency requiring a public appeal…" to include, "Public appear for a load reduction event resulting for a RC or BA implementing its emergency operators plans documented in EOP-001." The reason is that normal public appeals for conservation should be clearly excluded. **The SDT disagrees since it is clearly stated that a report is required for "Public appeal for load reduction event." The SDT has not discussed a reporting mechanism for "conservation."** 8. Add a time threshold to complete loss of off-site power to a nuclear plant. Nuclear plants are to have backup diesel generation that last for a minimum amount of time. A threshold recognizing this 4 hour or longer window needs to be added

Organization	Yes or No	Question 2 Comment
		such as complete loss of off-site power to a nuclear plant for more than 4 hours. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2.** **The SDT has taken your comment into consideration and this threshold for reporting now states:** **"Complete loss of off-site power affecting a nuclear generating station per the Nuclear Plant Interface Requirement." As stated in this event Threshold, the TOP's NIPR may have additional guidance concerning the complete loss of offsite power affecting a nuclear plant.** 9. Delete "Transmission loss". The loss of a specific number of elements has no direct bearing on the risk of a system cascade. Faults and storms can easily result in "unintentional" the loss of multiple elements. This is a flawed concept and needs to be deleted **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2.** **The SDT has taken your comment into consideration and this threshold for reporting now states:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."**
Response: The SDT thanks you for your comment.		
PPL Corporation NERC Registered Affiliates	No	1.) PPL Generation thanks the SDT for the changes made in this latest proposal. We feel our previous comments were addressed. PPL Generation offers the following additional comments. Regarding the event 'Transmission Loss': For your consideration, please consider adding a footnote to the event 'Transmission Loss' such that weather events do not need to be reported. Also please consider including operation contrary to design in the language and not just in the example. E.g. consistent with the NERC Event Analysis table, the threshold would be, 'Unintentional loss, contrary to design, of three or more

Organization	Yes or No	Question 2 Comment
		BES Transmission Facilities.' **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2.** **The SDT has taken your comment into consideration and this threshold for reporting now states:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)." The SDT has removed all footnotes within Attachment 1.** 2.) PPL Generation proposes the following changes in Attachment 1 to the first entry in the "Threshold for Reporting" column to make it clear that independent GO/GOPs are required to act only within their sphere of operation and based on the information that is available to the GO/GOPs: Damage or destruction of a Facility that: Affects an IROL (per FAC-014, not applicable to GOs and GOPs) OR Results in the need for actions to avoid an Adverse Reliability Impact (not applicable to GOs and GOPs) OR Results from actual or suspected intentional human action (applicable to all). **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any**

Organization	Yes or No	Question 2 Comment
		abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s). The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within

Organization	Yes or No	Question 2 Comment
		their Operating Plan.
Response: The SDT thanks you for your comment.		
ISO/RTO Standards Review Committee	No	The SRC response to this question does not indicate support of the proposed requirement. Please see the latter part of the SRC's response to Question 4 below for an SRC proposed alternative approach:
Response: The SDT thanks you for your comment. Please review response to Question 4 comment.		
ACES Power Marketing Standards Collaborators	No	The drafting team made a number of positive changes to Attachment 1. However, there are a few changes that have introduced new issues and there are a number of existing issues that have yet to be fully addressed. One of the existing issues is that the reporting requirements will result in duplicate reporting. Considering that one of the stated purposes is to eliminate redundancy, we do not see how the scope of the SAR can be considered to be met until all duplicate reporting is eliminated. **The SDT acknowledges that reporting of the same event will come from multiple parties. However, as the industry has learned from recent events, NERC needs to have perspectives from a variety of entities instead of just one party's viewpoint. Reliability can be improved from learning how the differing parties see or experience the event. Sometimes, the differing perspectives have provided valuable insight on the true nature of the event. Therefore, the SDT believes that having multiple reports will aid reliability as we can learn from everyone's experiences.**

Organization	Yes or No	Question 2 Comment
		More specifics on our concerns are provided in the following discussion. (1) In the "Damage or destruction of a Facility" event, the statement "Affects an IROL (per FAC-014)" in the "Threshold for Reporting" is ambiguous. What does it mean? If the loss of a Facility will have a 1 MW flow change on the Facilities to which the IROL applies, is this considered to have affected the IROL? We suggest a more direct statement that damage or destruction occurred on a Facility to which the IROL applies or to one of the Facilities that comprise an IROL contingency as identified in FAC-014-2 R5.1.3. Otherwise, there will continue to be ambiguity over what constitutes "affects". (2) In the "Damage or destruction of a Facility" event, the threshold regarding "intentional human action" is ambiguous and suffers from the same difficulties as defining sabotage. What constitutes intentional? How do we know something was intentional without a law enforcement investigation? This is the same issue that prevented the drafting team from defining sabotage. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency.** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to**

Organization	Yes or No	Question 2 Comment
		prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s). The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within

Organization	Yes or No	Question 2 Comment
		their Operating Plan. (3) In the "Damage or destruction of a Facility" and "Any physical threat that could impact the operability of a Facility" events, Distribution Provider should be removed. Per the Function Model, the Distribution Provider does not have any Facilities (line, generator, shunt compensator, transformer). The only Distribution Provider equipment that even resembles a Facility would be capacitors (i.e. shunt compensator) but they do not qualify because they are not Bulk Electric System Elements. **The SDT agrees that if a DP does not own or operate a Facility then this event would not be applicable to them. However, if a DP does experience an event such as those listed, then it is a reportable incident under this standard.** (4) The "Any physical threat that could impact the operability of a Facility" event requires duplicate reporting. For example, if a large generating plant experiences such a threat, who should report the event? What if loss of the plant could cause capacity and energy shortages as well as transmission limits? The end result is that the RC, BA, TOP, GO and GOP could all end up submitting a report for the same event. For a given operating area, only one report should be required from one registered entity for each event. **The SDT acknowledges that multiple reports could result from an event. If an entity experiences an applicable event type, then they required to report it. As previously stated, the industry can benefit from having such differing perspectives when events occur.** (5) The "Any physical threat that could impact the operability of a Facility" event should not apply to a single Facility but rather multiple Facilities which if lost would impact BES reliability. As written now, a train derailment near a single 138 kV transmission line or small generator with minimal reliability impact would require reporting. **The SDT removed all language under "Entity with Reporting Responsibility," with**

Organization	Yes or No	Question 2 Comment
		the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** (6) The "BES Emergency resulting in automatic firm load shedding" should not apply to the DP. In the existing EOP-004 standard, Distribution Provider is not included and the load shed information still gets reported. **The SDT believes that the DP should be required to report "automatic firm load shedding…" to the ERO (and whoever else the entity wishes to inform per Requirement R1).** (7) The "Voltage deviation on a Facility" event needs to be clarified that the TOP only reports voltage deviations in its Transmission Operator Area. Because TOPs may view

Organization	Yes or No	Question 2 Comment
		into other Transmission Operator Areas, it could technically be required to report another TOP's voltage deviation because one of its System Operators observed the neighboring TOP's voltage deviation. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes ."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.** **The SDT understands that there may be several reports of a single event; and as the SDT has stated before, that this will give the ERO a better understanding of the depth and breathe of system conditions based on the given event.** (8) For the "Loss of firm load greater than 15 minutes" event, the potential for duplicate reporting needs to be eliminated. Every time a DP experiences this event, the DP, TOP and BA all appear to be required to report since the DP is within both the Balancing Authority Area and Transmission Operator Area. Only one report is necessary and should be sent. Given that the existing EOP-004 standard does not include the DP, we suggest eliminating the DP to eliminate one level of duplicate reporting. **The SDT understands that there may be several reports of a single event; and as the SDT has stated before, that this will give the ERO a better understanding of the depth and breathe of system conditions based on the given event.** (9) For the "System separation (islanding)" event, please remove DP. As long as any island remains viable, the Distribution Provider will not even be aware that an island occurred. It is not responsible for monitoring frequency or having a wide area view.

Organization	Yes or No	Question 2 Comment
		The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. **This event is now only applicable to RC, BA, and TOP.** (10) For the "System separation (islanding)" event, please remove BA. Because islanding and system separation, involve Transmission Facilities automatically being removed from service, this is largely a Transmission Operator issue. This position is further supported by the approval of system restoration standard (EOP-005-2) that gives the responsibility to restore the system to the TOP. (11) For the "System separation (islanding)" event, please eliminate duplicate reporting by clarifying that the RC should submit the report when more than one TOP is involved. If only one TOP is involved, then the single TOP can submit the report or the RC could agree to do it on their behalf. Only one report is necessary. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified.** **This event is now only applicable to RC, BA, and TOP. The SDT understands that there may be several reports of a single event; and as the SDT has stated before, that this will give the ERO a better understanding of the depth and breathe of system conditions based on the given event.** (12) For the "Generation loss" event, duplicate reporting should be eliminated. It is not necessary for both the BA and GOP to submit two separate reports with nearly identical information. Only one entity should be responsible for reporting. **The SDT understands that there may be several reports of a single event; and as the SDT has stated before, that this will give the ERO a better understanding of the depth and breathe of system conditions based on the given event.** (13) For the "Complete loss of off-site power to a nuclear generating plant", the

Organization	Yes or No	Question 2 Comment
		associated GO or GOP should be required to report rather than the TO or TOP. Maintaining power to cooling systems is ultimately the responsibility of the nuclear plant operator. At the very least, TO should be removed because it is not an operating entity and loss of off-site power is an operational issue. If the TOP remains in the reporting responsibility, it should be clarified that it is only a TOP with an agreement pursuant to NUC-001. All of this is further complicated because NUC-001 was written for a non-specific transmission entity because there was no one functional entity from which the nuclear plant operator gets it off-site power. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2.** **The SDT has taken your comment into consideration and this threshold for reporting now states:** **"Complete loss of off-site power affecting a nuclear generating station per the Nuclear Plant Interface Requirement." As stated in this event Threshold, the TOP's NIPR may have additional guidance concerning the complete loss of offsite power affecting a nuclear plant.** (14) For the "Complete or partial loss of monitoring capability", partial loss needs to be further clarified. Is loss of a single RTU a partial loss of monitoring capability? For a large RC is loss of ICCP to a single small TOP, considered a partial loss? We suggest as long as the entity has the ability to monitor their system through other means that the event should not be reported. For the loss of a single RTU, if the entity has a solving state estimator that provides estimates for the area impacted, the partial threshold loss would not be considered. If the entity has another entity (i.e. perhaps the RC is still receiving data for its TOP area, the RC can monitor for the TOP) that can monitor their system as a backup, the partial loss has not been met. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event now only applies to:** **"Complete loss of monitoring capability affecting a BES control center for 30**

Organization	Yes or No	Question 2 Comment
		continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.
Response: The SDT thanks you for your comment.		
Southern Company Services	No	It appears that the SDT has incorporated the reporting requirements for CIP-008 "reportable Cyber Security Incidents"; however, the "recognition" requirements remain in CIP-008 Reliability Standard. Southern understands the desire to consolidate reporting requirements into a single standard, but it would be clearer for Cyber Security Incidents if both the recognition and reporting requirements were in one reliability standard and not spread across multiple standards. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement.** As it relates to the event type "Loss of Firm Load for > 15 minutes", Southern suggests that the SDT clarify if weather related loss of firm load is excluded from the reporting requirement. **The SDT believes that it is important to report this event based on the threshold regardless of the cause. This will give the ERO (and whoever else the entity wishes to inform per Requirement R1) a better understanding of the depth and breathe of system conditions based on the given event.** As it relates to the event type "Loss of all voice communication capability", Southern suggest that the SDT clarify if this means both primary and backup voice communication systems or just primary voice communication systems. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry**

Organization	Yes or No	Question 2 Comment
		comments to state: **"Complete loss of voice communications capabilities affecting a BES control center for 30 continuous minutes or more." The SDT intends "complete" to mean all capabilities, including back up capabilities.** Referring to "CIP-008-3 or its successor" in Requirement R1.1 is problematic. This arrangement results in a variable requirement for EOP-004-2 R1. The requirements in a particular version of a standard should be fixed and not variable. If exceptions to applicable events change, a revision should be made to EOP-004 to reflect the modified requirement. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008.**
Response: The SDT thanks you for your comment.		
Hydro One	No	In the Attachment 1, language identical to event descriptions in the NERC Event Analysis Process and FERC OE-417 should be used. Creating a third set of event descriptions is not helpful to system operators. Recommend aligning the Attachment 1 wording with that contained in Attachment 2, DOE Form OE-417 and the EAP whenever possible. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Using identical terminology will be difficult to achieve as the DOE form and EAP have differing processes for identification of the reportable incidences. The SDT has tried to set up the reportable events in the standard to be as similar as possible to the other organizations without being tied to their specific language. Attachment 2 has been modified to match the events types listed in Attachment 1.** The proposed "events" are subjective and will lead to confusion and questions as to what has to be reported. - Event: A reportable Cyber Security Incident. All reportable Cyber Security Incidents may not require "One Hour Reporting." A "one-size fits all" approach may not be appropriate for the reporting of all Cyber Security

Organization	Yes or No	Question 2 Comment
		Incidents. The NERC "Security Guideline for the Electricity Sector: Threat and Incident Reporting" document provides time-frames for Cyber Security Incident Reporting. For example, a Cyber Security Compromise is recommended to be reported within one hour of detection, however, Information Theft or Loss is recommended to be reported within 48 hours. Recommend listing the Event as "A confirmed reportable Cyber Security Incident. The existing NERC "Security Guideline for the Electricity Sector: Threat and Incident Reporting" document uses reporting time-frames based on "detection" and "discovery." Recommend using the word confirmed because of the investigation time that may be required from the point of initial "detection" or "discovery" to the point of confirmation, when the compliance "time-clock" would start for the reporting requirement in EOP-004-2. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement. Note that the existing NERC "Security Guideline for the Electricity Sector: Threat and Incident Reporting" document is a "guideline" to assist entities. It should not be confused with a mandatory and enforceable Reliability Standard.** - Event: Damage or destruction of a Facility Threshold for Reporting: revise language on third item to read: "Results from actual or suspected intentional human action, excluding unintentional human errors". **The SDT reviewed, discussed and updated "Damage and destruction of a Facility" based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. The new "threshold" not states:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any**

Organization	Yes or No	Question 2 Comment
		abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** - Event: Any physical threat that could impact the operability of a Facility This Event category should be deleted. The word "could" is hypothetical and therefore unverifiable and un-auditable. The word "impact" is undefined. Please delete this reporting requirement, or provide a list of hypothetical "could impact" events, as well as a specific definition and method for determining a specific physical impact threshold for "could impact" events other than "any." **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility**

Organization	Yes or No	Question 2 Comment
		Do not report copper theft unless it degrades normal operations of a Facility." **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** - Event: BES Emergency requiring public appeal for load reduction. Replace wording in the Event column with language from #8 on the OE-417 Reporting Form to eliminate reporting confusion. Following this sentence add, "This shall exclude other public appeals, e.g., made for weather, air quality and power market-related conditions, which are not made in response to a specific BES event." **The SDT disagrees with quantifying a use of public appeals reporting for different types of events. The important item here is that a public appeal was issued for load reduction. A report is require to inform the ERO (and whoever else the entity wishes to inform per Requirement R1) of your current status and provide them with the situational awareness of the status of your system.** - Event: Complete or partial loss of monitoring capability Event wording: Delete the words "or partial" to conform the wording to the NERC Event Analysis Process. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event now only applies to:** **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.**

Organization	Yes or No	Question 2 Comment
		Event: Transmission Loss Revise to BES Transmission Loss **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** Event: Generation Loss Revise to BES Generation Loss **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."** **The SDT believes that if an entity reaches this threshold, it needs to be reported.**
Response: The SDT thanks you for your comment.		
CenterPoint Energy	No	CenterPoint Energy appreciates the revisions made to Attachment 1 based on stakeholder feedback; however, the Company continues to have concerns regarding certain events and thresholds for reporting and offers the following recommendations. (1) CenterPoint Energy recommends the deletion of "per Requirement R1" in the "Note" under Attachment 1 as it contains a circular reference back to R1 which includes timeframes.

Organization	Yes or No	Question 2 Comment
		The SDT has updated Requirement R1 due to industry comments to read: "R1. Each Responsible Entity shall have an event reporting Operating Plan that includes communication protocol(s) for applicable events listed in, and within the time frames specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations based on the event type (e.g. the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, governmental or provincial agencies)." (2) CenterPoint Energy maintains that a required 1 hour threshold for reporting of any event is unreasonable. CenterPoint Energy is confident that given dire circumstances Responsible Entities will act quickly on responding to and communication of any impending threat to the reliability of the Bulk Electric System. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement.** (3) For the event of "Damage or destruction of a Facility", CenterPoint Energy is concerned that the use of the term "suspected" is too broad and proposes that the SDT delete "suspected" and add "that causes an Adverse Reliability Impact…" to the threshold for reporting regarding human action. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."**

Organization	Yes or No	Question 2 Comment
		This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s). The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility

Organization	Yes or No	Question 2 Comment
		was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan. (4) CenterPoint Energy believes that the event, "Any physical threat that could impact the operability of a Facility" is too broad and should be deleted. Alternatively, CenterPoint Energy recommends that the SDT delete "could" or change the event description to "A physical incident that causes an Adverse Reliability Impact". Additionally, in footnote 1, the example of a train derailment uses the phrase "could have damaged". CenterPoint Energy is concerned that as beauty is the eye of the beholder, this phrase is open to interpretation and therefore recommends that the phrase, "causes an Adverse Reliability Impact" be incorporated into the description. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event and footnote 1. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this**

Organization	Yes or No	Question 2 Comment
		will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility. (5) The Company proposes that the threshold for reporting the event, "BES Emergency requiring manual firm load shedding" is too low. It appears the SDT was attempting to align this threshold with the DOE reporting requirement. However, as the SDT stated above, there are several valid reasons why this should not be done; therefore, CenterPoint Energy recommends the threshold be revised to "Manual firm load shedding â‰¥ 300 MW". **The SDT disagrees as this is currently enforceable within EOP-004-1.** (6) CenterPoint Energy also recommends a similar revision to the threshold for reporting associated with the "BES Emergency resulting in automatic firm load shedding" event. ("Firm load shedding â‰¥ 300 MW (via automatic under voltage or under frequency load shedding schemes, or SPS/RAS") **The SDT disagrees as we have aligned this with "manual firm load shedding." As written a report will be required for load shedding of 100MW for automatic or manual actions.** (7) CenterPoint Energy is uncertain of the event, "Loss of firm load for â‰¥ 15 minutes" and its fit with BES Emergency requiring manual firm load shedding or BES Emergency resulting in automatic firm load shedding. The Company believes that this event is already covered with manual firm load shedding and automatic firm load shedding and should therefore be deleted. **The SDT disagrees, as "Loss of firm load" is due to an action other than loss of load due to "automatic" or "manual" actions by the BA, TOP, or DP. The intent is to capture that load was loss by some other action. Note that this is a currently enforceable item within EOP-004-1.**

Organization	Yes or No	Question 2 Comment
		(8) For the event of "System separation (islanding)", CenterPoint Energy believes that 100 MW is inconsequential and proposes 300 MW instead. **The SDT disagrees, as this has been vetted through the industry with very little negative feedback.** (9) For "Generation loss", CenterPoint Energy suggests that the SDT add "only if multiple units" to the criteria of "1,000 MW for entities in the ERCOT or Quebec Interconnection". **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."** (10) Finally, CenterPoint Energy recommends that the SDT delete the term "partial" under the "Entity with Reporting Responsibility" for "Complete or partial loss of monitoring capability". The Company proposes revising the event description to "Loss of monitoring capability for > 30 minutes that causes system analysis tools to be inoperable". **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event is now written to state:** **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or**

Organization	Yes or No	Question 2 Comment
		TOP who have this capability to start with.
Response: The SDT thanks you for your comment.		
Arkansas Electric Cooperative Corporation	No	AECC supports the comments submitted by ACES Power Marketing.
Response: The SDT thanks you for your comment. Please review the response to that commenter.		
MWDSC	No	See comment for question 1
Response: The SDT thanks you for your comment. Please review the response to Question 1.		
Georgia System Operations Corporation	No	See comments under no. 4 below.
Response: The SDT thanks you for your comment. Please review the response to Question 4.		
Texas Reliability Entity	No	(1) In the Events Table, consider whether the item for "Voltage deviation on Facility" should also be applicable to GOPs, because a loss of voltage control at a generator (e.g. failure of an automatic voltage regulator or power system stabilizer) could have a similar impact on the BES as other reportable items. Note: We made this comment last time, and the SDT's posted response was non-responsive to this concern. **The SDT reviewed TRE's comment and believe that our consideration of comments during that last posting clearly stated the SDT view correctly. We stated "The SDT disagrees with this comment. Attachment 1 is the minimum set of events that will be required to report and communicate per your Operating Plan will be aware of system conditions." Further, we note that such events do not rise to the level of notification to the ERO. When events like the ones you mention occur, then entity has obligations to notify other parties according to reliability standards relating to that equipment. The NERC Standards Process Manual does allow TRE to apply for a variance if they have special concerns that GOPs should submit a report to the ERO.** (2) In the Events Table, under Transmission Loss, the SDT indicated that reporting is triggered only if three or more Transmission Facilities operated by a single TOP are lost. What if four Facilities are lost, with two Facilities operated by each of two TOPs?

Organization	Yes or No	Question 2 Comment
		That is a larger event than three Facilities lost by one TOP, but there is no reporting requirement? Determining event status by facility ownership is not an appropriate measure. The reporting requirements should be based on the magnitude, duration, or impact of the event, and not on what entities own or operate the facilities. (3) In the Events Table, under Transmission Loss, the criteria "loss of three or more Transmission Facilities" is very indefinite and ambiguous. For example, how will bus outages be considered? Many entities consider a bus as a single "Facility," but loss of a single bus may impact as many as six 345kV transmission lines and cause a major event. It is not clear if this type of event would be reportable under the listed event threshold? Is the single-end opening of a transmission line considered as a loss of a Facility under the reporting criteria? (4) Combinations of events should be reportable. For example, a single event resulting in the loss of two Transmission Facilities (line and transformer) and a 950 MW generator would not be reportable under this standard. But loss of two lines and a transformer, or a 1000 MW generator, would be reportable. It is important to capture all events that have significant impacts. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** **The SDT has reviewed Attachment 1 as a minimum level of reporting thresholds. There may be times where an entity may wish to report when a threshold has not been reached because of their experience with their system. EOP-004-2 does not prevent any entity from reporting any type of situation (event) at anytime. Note that the SDT has received industry feedback and it is not within scope of a results**

Organization	Yes or No	Question 2 Comment
		based Standards concept to be very prescriptive in nature. (5) In the Events Table, under "Unplanned control center evacuation," "Loss of all voice communication capability" and "Complete or partial loss of monitoring capability," GOPs should be included. GOPs also operate control centers that are subject to these kinds of occurrences, with potentially major impacts to the BES. Note that large GOP control centers are classified as "High Impact" facilities in the CIP Version 5 standards, and a single facility can control more than 10,000 MW of generation. **The SDT appreciates your suggestion; however, as we understand the point, it doesn't apply continent-wide. The SDT has applied these events to RCs, BAs, and TOPs.** (6) The "BES Emergency resulting in automatic firm load shedding" event row within Attachment 1 should include the BA as a responsible entity for reporting. Note that EOP-003-1 requires the BA to shed load in emergency situations (R1, R5 as examples), and any such occurrence should be reported. **The SDT has reviewed your comment and would like to note that manual load shedding is only reportable if 100 MW or more is activated. Automatic load shedding is intended to be when a "relay" performs a breaker action that sheds load without human interaction and achieves a level of 100 MW or more.**
Response: The SDT thanks you for your comment.		
Occidental Power Services, Inc.	No	There are no requirements in Attachment 1 for LSEs without BES assets so these entities should not be in the Applicability section.
Response: The SDT thanks you for your comment. The LSE obligation in this standard was tied to applicability in CIP-008 for cyber incident reporting. Reporting under CIP-008 is no longer proposed to be a part of EOP-004-2 so this applicability has been removed. Please note that LSEs will be obligated to report under CIP-008 until that standard has been changed.		
Xcel Energy	No	1) The event Damage or destruction of a Facility appears to need 'qualifying'. Is this intended for only malicious intent? Otherwise, weather related or other operational events will often meet this criteria. For example adjustment in generation or changes

Organization	Yes or No	Question 2 Comment
		in line limits to "avoid an Adverse Reliability Impact" could occur during a weather related outage. We suggest adjusting this event and criteria to clearly exclude certain items or identify what is included. **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and**

Organization	Yes or No	Question 2 Comment
		identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** 2) Also recommend placing the information in footnote 1 into the associated Threshold for Reporting column, and removing the footnote. **The SDT has removed the footnote per industry comments and concerns.**
Response: The SDT thanks you for your comment.		
American Electric Power	No	If CIP-008 is now out of scope within the requirements of this standard, any references to it should also be removed from Attachment 1. **The SDT has removed the one-hour reporting requirement as requested within**

Organization	Yes or No	Question 2 Comment
		comments received. The Threshold for Reporting column on page 26 includes "Results from actual or suspected intentional human action." This wording is too vague as many actions by their very nature are intentional. In addition, it should actually be used as a qualifying event rather than a threshold. We recommend removing it entirely from the Threshold column, and placing it in the Events column and also replacing the first row as follows: "Actual or suspected intentional human action with the goal of damage to, or destruction of, the Facility." On page 27, the event "Any physical threat that could impact the operability of a Facility" is too vague and broad. Using the phrases "any physical threat" and "could impact" sets too high a bar on what would need to be reported. On page 28, for the event "Complete loss of off-site power to a nuclear generating plant (grid supply)", TO and TOP should be removed and replaced by GOP. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has**

Organization	Yes or No	Question 2 Comment
		the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.
Response: The SDT thanks you for your comment.		
Clark Public Utilities	No	I agree with all but one. The event is "Damage or destruction of a Facility" and the threshold for reporting is "Results from actual or suspected intentional human action." I understand and agree that destruction of a facility due to actual or suspected intentional human action should always be reported. However, I do not know what level of damage should be reported. Obviously the term "damage" is meant to signify and event that is less than destruction. As a result, damage could be extensive, minimal, or hardly noticeable. There needs to be some measure of what the damage entails if the standard is to contain a broad requirement for the reporting of damage intentionally caused by human action. Whether that measure is based on the actual impacts to the BES from the damage or whether the measure is based on the ability of the damaged equipment to continue to function at 100%, 50% or some capability would be acceptable but currently it is too open ended.
Response: The SDT thanks you for your comment. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.**		

Organization	Yes or No	Question 2 Comment
This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s). The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.		
New York Power Authority	No	Please see comments submitted by NPCC Regional Standards Committee (RSC).
Response: Thank you for your comment. Please see response to the comments.		
Consolidated Edison Co. of NY, Inc.	No	General comment regarding Attachment 1:SDT should strive to use identical language to event descriptions in the NERC Event Analysis Process and FERC OE-417. Creating a third set of event descriptions is not helpful to system operators. We recommend aligning the Attachment 1 wording with that contained in Attachment 2, DOE Form OE-417 and the EAP whenever possible. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Using identical terminology will be difficult to achieve as the DOE form and EAP have differing processes for identification of the reportable incidences. The SDT has tried to set up the reportable events in the standard to be as similar as possible to the other organizations without being tied to their specific language. Attachment 2 has been modified to match the events types listed in Attachment 1.** Replace the Attachment 1 "NOTE" with the following clarifying wording: NOTE: The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of Attachment 2 if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422. Initial submittal by Voice within the reporting time frame is acceptable for all events when followed by a hardcopy submittal by Facsimile or e-mail as and if required.

Organization	Yes or No	Question 2 Comment
		The SDT thanks you with your comment. First, the SDT believes that you intended the comment to address the "Note" on Attachment 2, not Attachment 1. The SDT does not believe that a hardcopy report is necessary if the organization has made voice contact. Event: Damage or destruction of a Facility Threshold for Reporting: revise language on third item to read, Results from actual or suspected intentional human action, excluding unintentional human errors. **The SDT reviewed, discussed and updated "Damage and destruction of a Facility" based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. The new "threshold" not states:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable**

Organization	Yes or No	Question 2 Comment
		operations of each interconnection. Event: Any physical threat that could impact the operability of a Facility This Event category should be deleted. The word "could" is hypothetical and therefore unverifiable and un-auditable. The word "impact" is undefined. Please delete this reporting requirement, or please provide a list of hypothetical "could impact" events, as well as a specific definition and method for determining a specific physical impact threshold for "could impact" events other than "any." **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement**

Organization	Yes or No	Question 2 Comment
		R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility. Event: BES Emergency requiring public appeal for load reduction. Replace Event wording with language from #8 on OE-417 reporting form to eliminate reporting confusion. Following this sentence add, "This shall exclude other public appeals, e.g., made for weather, air quality and power market-related conditions, which are not made in response to a specific BES event. **The SDT disagrees with quantifying a use of public appeals reporting for different types of events. The important item here is that a public appeal was issued for load reduction. A report is require to inform the ERO (and whoever else the entity wishes to inform per Requirement R1) of your current status and provide them with the situational awareness of the status of your system.** "Event: Complete or partial loss of monitoring capability Event wording: Delete the words "or partial" to conform the wording to NERC Event Analysis Process. Event: Transmission Loss Modify to BES Transmission Loss Event Generation Loss Modify to BES Generation Loss
Orange and Rockland Utilities, Inc.	No	General comment regarding Attachment 1: SDT should strive to use identical language to event descriptions in the NERC Event Analysis Process and FERC OE-417. Creating a third set of event descriptions is not helpful to system operators. We recommend aligning the Attachment 1 wording with that contained in Attachment 2, DOE Form OE-417 and the EAP whenever possible. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Using identical terminology will be difficult to achieve as the DOE form and EAP have differing processes for identification of the reportable incidences. The SDT has tried to set up the reportable events in the standard to be as similar as possible to the other organizations without being tied to their specific**

Organization	Yes or No	Question 2 Comment
		language. Attachment 2 has been modified to match the events types listed in Attachment 1. Replace the Attachment 1 "NOTE" with the following clarifying wording: NOTE: The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of Attachment 2 if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422. Initial submittal by Voice within the reporting time frame is acceptable for all events when followed by a hardcopy submittal by Facsimile or e-mail as and if required. **The SDT thanks you for your comment. First, the SDT believes that you intended the comment to address the "Note" on Attachment 2, not Attachment 1. The SDT does not believe that a hardcopy report is necessary if the organization has made voice contact.** Event: Damage or destruction of a Facility Threshold for Reporting: revise language on third item to read, Results from actual or suspected intentional human action, excluding unintentional human errors. **The SDT reviewed, discussed and updated "Damage and destruction of a Facility" based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. The new "threshold" not states:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could**

Organization	Yes or No	Question 2 Comment
		adversely affect the reliability of the Bulk Electric System). **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** Event: Any physical threat that could impact the operability of a Facility This Event category should be deleted. The word "could" is hypothetical and therefore unverifiable and un-auditable. The word "impact" is undefined. Please delete this reporting requirement, or please provide a list of hypothetical "could impact" events, as well as a specific definition and method for determining a specific physical impact threshold for "could impact" events other than "any." **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or**

Organization	Yes or No	Question 2 Comment
		Suspicious device or activity at a Facility **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** Event: BES Emergency requiring public appeal for load reduction. Replace Event wording with language from #8 on OE-417 reporting form to eliminate reporting confusion. Following this sentence add, "This shall exclude other public appeals, e.g., made for weather, air quality and power market-related conditions, which are not made in response to a specific BES event." **The SDT disagrees with quantifying a use of public appeals reporting for different types of events. The important item here is that a public appeal was issued for load reduction. A report is require to inform the ERO (and whoever else the entity wishes to inform per Requirement R1) of your current status and provide them with the situational awareness of the status of your system.** Event: Complete or partial loss of monitoring capability Event wording: Delete the words "or partial" to conform the wording to NERC Event Analysis Process. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event is now written to state:** **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or**

Organization	Yes or No	Question 2 Comment
		TOP who have this capability to start with. **Event: Transmission Loss Modify to BES Transmission Loss** **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** Event Generation Loss Modify to BES Generation Loss **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."**
Response: The SDT thanks you for your comment.		
FirstEnergy Corp	No	FE requests the following changes be made to Attachment 1:1. Pg. 19 / Event: "Voltage deviation on a Facility". The term "observes" for Entity with Reporting Responsibility be changed to "experiences". The burden should rest with the

Organization	Yes or No	Question 2 Comment
		initiating entity in consistency with other Reporting Responsibilities. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes."** 2. In "Threshold for Reporting", the language should be expanded to - plus or minus 10% "of nominal voltage" for greater than or equal to 15 continuous minutes. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.** 3. Pg.20 /Event: "Complete or partial loss of monitoring capability". The term "partial" should be deleted from the event description to read as follows: Complete loss of monitoring capability and the reporting responsibility requirements to read "Each RC, BA, and TOP that experiences the complete loss of monitoring capability." **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004**

Organization	Yes or No	Question 2 Comment
		into EOP-004-2. This event is now written to state: **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.**
Response: The SDT thanks you for your comment.		
Farmington Electric Utility System	No	The reporting threshold for "Complete or partial loss of monitoring capability" should be modified to include the loss of additional equipment and not be limited to State Estimator and Contingency Analysis. Some options have been included: Affecting a BES control center for â‰¥ 30 continuous minutes such that Real-Time monitoring tools are rendered inoperable. Affecting a BES control center for â‰¥ 30 continuous minutes to the extent a Constrained Facility would not be identified or an Adverse Reliability Impact event could occur due to lack of monitoring capability. Affecting a BES control center for â‰¥ 30 continuous minutes such that an Emergency would not be identified or ma
Response: The SDT thanks you for your comment. The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event is now written to state: **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.**		
Public Service Enterprise Group	No	We agreed with most of the revisions. However, for the 24-hour reporting time frame portion of the EOP-004 Attachment 1: Reportable Event that starts on p. 18, we have these concerns: a. Why was "RC" left out in the first row? RC is in the second row that also addresses a "Facility." We believe that "RC" was inadvertently

Organization	Yes or No	Question 2 Comment
		left out. b. In the first row, entities such as a BA, TO, GO, GOP, or DP would not know whether damage or destruction of one of its Facilities either "Affects an IROL (per FAC-014)" or "Results in the need for actions to avoid an Adverse Reliability Impact." FAC-014-2, R5.1.1 requires Reliability Coordinators provide information for each IROL on the "Identification and status of the associated Facility (or group of Facilities) that is (are) critical to the derivation of the IROL" to entities that do NOT include the entities listed above. And frankly, those entities would not need to know. The reporting requirements associated with "Damage or destruction of a Facility" need to be changed so that the criteria for reporting by an entity whose Facilities experience damage or destruction does not rely upon information that the entity does not possess. c. A possible route to achieve the results in b. above is described below: i. All Facilities that are damaged or destroyed that "Results from actual or suspected intentional human action" would be reported to the ERO by the entity experiencing the damage or destruction. ii. All Facilities that are damaged or destroyed OTHER THAN THAT due to an "actual or suspected intentional human action" would be reported to the RC by the entity experiencing the damage or destruction. Based upon those reports, the RC would be required to report whether the reported damage or destruction of a Facility "Affects an IROL (per FAC-010)" or "Results in the need for actions to Avoid an Adverse Reliability Consequence." (The RC may need to modify its data specifications in IRO-010-1a - Reliability Coordinator Data Specification and Collection - to specify outages due to "damage or destruction of a Facility." We also note that "DP" is not included in IRO-010-1a, but "LSE" is included. DPs are required to also register as LSEs if they meet certain criteria. See the "Statement of Compliance Registry Criteria, Rev. 5.0", p.7. For this reason, we suggest that DP be replaced with LSE in EOP-004-2.) d. To implement the changes in c. above, we suggest that the first row be divided into two rows: i. FIRST ROW: This would be like the existing first row on page 18, except "RC" would be added to the column for "Entity with Reporting Responsibility" and the only reporting threshold would be ""Results from actual or suspected intentional human action." ii. SECOND ROW: The Event would be "Damage or destruction of a Facility of a BA, TO, TOP, GO,

Organization	Yes or No	Question 2 Comment
		GOP, or LSE," the Entity, the Reporting Responsibility would be "The RC that has the BA, TOP, GO, GOP, or LSE experiencing the damage or destruction in its area," and the Threshold for Reporting would be "Affects an IROL (per FAC-010)" or "Results in the need for actions to avoid an Adverse Reliability Consequence."

Response: The SDT thanks you for your comment. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:

"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."

This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).

This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.

The SDT also developed another to read:

Organization	Yes or No	Question 2 Comment
"Damage or destruction of its Facility that results from actual or suspected intentional human action." **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.**		
MidAmerican Energy	No	Several modifications need to be made to Table 1 to enhance clarity and delete unnecessary or duplicate items. The stated reliability objective of EOP-004 and the drafting team is to reduce and prevent outages which could lead to cascading through reporting. It is understood that the EOP-004 Attachment 1 is to cover similar items to the DOE OE-417 form. Last, remember that FERC recently asked the question of what standards did not provide system reliability benefits. Those reports that cannot show a direct threat to a potential cascade need to be eliminated. Table 1 should always align with the cascade risk objectives and OE-417 where possible. Therefore Table 1 should be modified as follows: 1. Completely divorce CIP-008 from EOP-004. Constant changes, the introduction of new players such as DOE and DHS, and repeated congressional bills, make coordination with CIP-008 nearly impossible. Cyber security and operational performance under EOP-004 remain separate and different despite best efforts to combine the two concepts. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we**

Organization	Yes or No	Question 2 Comment
		have remanded the one hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement. 2. Modify R1.2 to state that ERO notification only is required for Table 1. This is similar to the DOE OE-417 notification. Notification of other entities is a best practice, not a mandatory NERC standard. If entities want to notify neighboring entities, they may do so as a best practice guideline. **The SDT has updated R1 based on comments received to read as:** **"R1. Each Responsible Entity shall have an event reporting Operating Plan that includes communication protocol(s) for applicable events listed in, and within the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations based on the event type (e.g. the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, governmental or provincial agencies)."** 3. Better clarity for communicating each of the applicable events listed in the EOP-004 Attachment 1 in accordance with the timeframes specified are needed. MidAmerican suggests a forth column be added to the table to clearly identify who must be notified within the specified time period or at a minimum, that R1.2 be revised to clearly state that only the ERO must be notified to comply with the standard. **The SDT disagrees but believes that per your Operating Plan contained in Requirement R1, an entity could take Attachment 1 and insert another column to assist whoever is designated to report an event within your company. The SDT does not want to be too prescriptive within Attachment 1.** 4. Consolidate OE-417 concepts on physical attack and cyber events by consolidating OE-417 items 1, 2, 9 and 10 to: Verifiable, credible, and malicious physical damage (excluding natural weather events) to a BES generator, line, transformer, or bus that when reported requires an appropriate Reliability Coordinator or Balancing Authority to issue an Energy Emergency Alert Level 2 or higher. The whole attempt to discuss a

Organization	Yes or No	Question 2 Comment
		NERC Facility and avoid adverse reliability impacts overreaches the fundamental principal or reporting for an emergency that could result in a cascade. **The SDT disagrees since the OE-417 (and EAP) does not follow the ANSI process as NERC does in the Standards Development Process.** 5. The wording "affects an IROL (per FAC-014)," is too vague and not measurable. Many facilities could affect an IROL, but fewer facilities if lost would cause an IROL. Change "affects" to "results in" **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed"**

Organization	Yes or No	Question 2 Comment
		Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. 6. Recommend that Adverse Reliability Impact be deleted and be replaced with actual EEA 2 or EEA 3 level events. **The SDT has removed Adverse Reliability Impact based on industry feedback and rewrote the event:** **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are**

Organization	Yes or No	Question 2 Comment
		required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. **The SDT also developed another to read:** **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** 7. The phrase "results from actual or suspected intentional human action" is vague

Organization	Yes or No	Question 2 Comment
		and not measurable. This line item used the term "suspected" which relates to "sabotage". MidAmerican recommends that "Results from actual or suspected intentional human action" be deleted. If not deleted the phrase should be replaced with "Results from verifiable, credible, and malicious human action intended to damage the BES." 8. Delete "Any physical threat..." as vague, and difficult to measure in a "perfect" zero defect audit environment, and as already covered by item 1 above. If not deleted, at a minimum replace "Any physical threat", with "physical attack" as being measureable and consistent with DOE OE-417. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).**

Organization	Yes or No	Question 2 Comment
		The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan. 9. With the use of "i.e." the SDT is mandating that each other entity must be contacted. The NSRF believes that the SDT meant that "e.g." should be used to provide examples. The SDT may wish to add another column to Attachment 1 to provide clarity. **The SDT has made the required change concerning replacing "i.e." with "e.g."** 10. The phrase "or partial loss of monitoring capability" is too vague and should be deleted. In addition, the 30 minute window is too short for EMS and IT staff to effectively be notified and troubleshoot systems before being subjected to a federal law requiring reporting and potential violations. The time frame should be consistent with the EOP-008 standard. If not deleted, replace with "Complete loss of SCADA affecting a BES control center for â‰¥ 60 continuous minutes such that analysis tools of State Estimator and/or Contingency Analysis are rendered inoperable. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event is now written to state:** **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.** 11. Transmission loss should be deleted. The number of transmission elements out does not directly correlate to BES stability and cascading. For that reason alone, this

Organization	Yes or No	Question 2 Comment
		item should be deleted or it would have already been included in the past EOP-004 standard. In addition, large footprints can have multiple storms or weather events resulting in normal system outages. This should not be a reportable event that deals with potential cascading. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** 12. Modify the threshold of "BES emergency requiring a public appeal..." to include, "Public appeal for a load reduction event resulting from a RC or BA implementing its emergency energy and capacity plans documented in EOP-001." Public appeals for conservation that aren't used to avoid capacity and energy emergencies should be clearly excluded. **The SDT disagrees as your request makes the event very prescriptive. The threshold is written to state: "Public appeal for load reduction event." The SDT understands that there may be several reports of a single event and as the SDT has stated before, that this will give the ERO a better understanding of the depth and breathe of system conditions based on the given event.** 13. Add a time threshold to complete loss of off-site power to a nuclear plant. Nuclear plants are to have backup diesel generation that last for a minimum amount of time. A threshold recognizing this 4 hour or longer window needs to be added such as complete loss of off-site power to a nuclear plant for more than 4 hours. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT**

Organization	Yes or No	Question 2 Comment
		removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Complete loss of off-site power affecting a nuclear generating station per the Nuclear Plant Interface Requirement."** **As stated in this event Threshold, the TOP's NIPR may have additional guidance concerning the complete loss of offsite power affecting a nuclear plant.** Also see the NSRF comments. **Please review the responses to that commenter.**
Response: The SDT thanks you for your comment.		
Illinois Municipal Electric Agency	No	Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Response: The SDT thanks you for your comment. Please review the responses to that commenter.		
Amercican Transmission Company, LLC	No	ATC is proposing changes to the following Events in Attachment 1: (Reference Clean Copy of the Standard) 1) Pg. 18/ Event: Any Physical threat that could impact the operability of a Facility. ATC is proposing a language change to the Threshold- "Meets Registered Entities criteria stated in its Event Reporting Operating Plan, in addition to excluding weather." **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry**

Organization	Yes or No	Question 2 Comment
		comments to state: **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** 2) Pg. 19 / Event: Voltage deviation on a Facility. ATC believes that the term "observes" for Entity with Reporting Responsibility be changed back to "experiences" as originally written. The burden should rest with the initiating entity in consistency with other Reporting Responsibilities. Also, for Threshold for Reporting, ATC believes the language should be expanded to - plus or minus 10% "of target voltage" for greater than or equal to 15 continuous minutes. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and**

Organization	Yes or No	Question 2 Comment
		identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes ."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.** 3) Pg. 19/ Event: Transmission loss. ATC recommends that Threshold for Reporting be changed to read "Unintentional loss of four, or more Transmission Facilities, excluding successful automatic reclosing, within 30 seconds of the first loss experienced and for 30 continuous minutes. Technical justification or Discussion for this recommended change: In the instance of a transformer-line-transformer, scenario commonly found close-in to Generating stations, consisting of 3 defined "facilities", 1 lightning strike can cause automatic unintentional loss by design. Increase the number of facilities to 4.In a normal shoulder season day, an entity may experience the unintentional loss of a 138kv line from storm activity, at point A in the morning, a loss of a 115kv line from a different storm 300 miles from point A in the afternoon, and a loss of 161kv line in the evening 500 miles from point A due to a failed component, if it is an entity of significant size. Propose some type of time constraint. Add time constraint as proposed, 30 seconds, other than automatic reclosing. In the event of dense lightning occurrence, the loss of multiple transmission facilities may occur over several minutes to several hours with no significant detrimental effect to the BES, as load will most certainly be affected (lost due to breaker activity on the much more exposed Distribution system) as well. Any additional loss after 30 seconds must take into account supplemental devices with intentional relay time delays, such as shunt capacitors, reactors, or load tap changers on transformers activating as designed, arresting system decay. In addition, Generator response after this time has significant impact. **The SDT removed all language under "Entity with Reporting Responsibility," with**

Organization	Yes or No	Question 2 Comment
		the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** 4) Pg.20 /Event: Complete or partial loss of monitoring capability. ATC recommends that the term "partial" be deleted from the event description.ATC recommends that the term "partial" be deleted for the Entity with Reporting Responsibility and changed to read: Each RC, BA, and TOP that experiences the complete loss of monitoring capability. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event is now written to state:** **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.**
Response: The SDT thanks you for your comment.		
Alliant Energy	No	In the first Event for twenty four hour reporting, the last item in "Threshold for Reporting" should be revised to "Results from actual or suspected intentional malicious human action." An employee may be performing maintenance and make a mistake, which could impact the BES. In the second Event for twenty four hour reporting the event should be revised to "Any physical attack that could impact the operability of a Facility." Alliant Energy believes this is clearer and easier to measure.

Organization	Yes or No	Question 2 Comment

Response: The SDT thanks you for your comment. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:

"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."

This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).

This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.

The SDT also developed another to read:

"Damage or destruction of its Facility that results from actual or suspected intentional human action."

This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.

This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).

The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the

Organization	Yes or No	Question 2 Comment
situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.		
Consumers Energy	No	The term "Facility" seems to be much more broad and even more vague than the use of BES equipment. We recommend reverting back to use of BES equipment.
Response: The SDT thanks you for your comment. The SDT disagrees since BES is used within the definition of Facility. NERC defines Facility as: "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)."		
Ameren	No	We appreciate the efforts of the SDT and believe this latest Draft is greatly improved over the previous version. However, we propose the following suggestions: (1) The first Event category in Attachment 1 under 24 Hour Reporting is Applicable to GO and GOP entities. Yet the first 2 of 3 Thresholds for Reporting require data that is unobtainable for GO and GOP entities. Specifically, Events that "Affects an IROL (per FAC-014)" and "Results in the need for actions to avoid an Adverse Reliability Impact". We believe these thresholds, and the use of the NERC Glossary term Adverse Reliability Impact, clearly show the SDT's intent to limit reporting only to Events that have a major and significant reliability impact on the BES. GO or GOP does not have access to the wide-area view of the transmission system, making them to make this determination is impossible. As a result, we do not believe GO and GOP entities should have Reporting Responsibility for these types of Events. (2) For GO and GOP entities, the third Threshold is confusing as to which facilities in the plant it would be applicable to; because the definition of "Facility" does not provide a clear guidance in that respect. For example, would a damage to ID fan qualify as a reportable event? **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry**

Organization	Yes or No	Question 2 Comment
		comments to state: "Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency." This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24

Organization	Yes or No	Question 2 Comment
		hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** (3) The second Event category in Attachment 1 under 24 Hour Reporting, "Any physical threat that could impact the operability of a Facility" is wide open to interpretation and thus impracticable to comply with. For example, a simple car accident that threatens any transmission circuit, whether it impacts the BES (as listed in the Threshold for the previous event in the table or any other measure) or not, is reportable. This list could become endless without the events having any substantial impact on the system. To continue this point, the Footnote 1 can also include, among many other examples, the following:(a) A wild fire near a generating plant, (b) Low river levels that might shut down a generating plant, (c) A crane that has partially collapsed near a generator switchyard, (d) Damage to a rail line into a coal plant, and/or (v) low gas pressure that might limit or stop operation of a natural gas generating plant. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT**

Organization	Yes or No	Question 2 Comment
		removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** (4) The category, "Transmission Loss" is a concern also. If the meaning of Transmission Facility is included in the meaning of Facility as described in the event list, it may be acceptable; but, we still have a question how would a loss of a bus and the multiple radial element that may be connected to that bus would be treated? Also, how would a breaker failure affect this type of an event? The loss of a circuit is

Organization	Yes or No	Question 2 Comment
		"intentional" (as opposed to Unintentional as listed in the threshold) for the failure of breaker, how will it be treated in counting three or more? We suggest a clarification for such types of scenarios. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** (5) Requirement R1.: 1.1 includes an exception from compliance with this Standard if there is a Cyber Security Incident according to CIP-008-3. However, note that the CIP-008-3 may not apply to all GO and GOP facilities. While the exception is warranted to eliminate duplicative event reporting plans, the language of this requirement is confusing as it does not clearly provides that message. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have proposed remanding the one hour event back to CIP-008.** (6) The second paragraph in Section C.1.1.2. Includes the phrases "...shall retain the current, document..." and "...the "date change page" from each version..." Is the "document" intended to be the Operating Plan? We do not see a defining reference in the text around this phrase; also, is a "date change page" mandatory for compliance with this Standard? We request additional clarification of wording in the Evidence Retention section of the Standard. (7) Page 19 / Event: Voltage deviation on a Facility: We believe that the term "observes" for Entity with Reporting Responsibility be changed back to "experiences" as originally written. The burden should rest with the initiating entity in consistency with other Reporting Responsibilities. In addition, for Threshold for Reporting, We

Organization	Yes or No	Question 2 Comment
		believe the language should be expanded to - plus or minus 10%"of nominal voltage" for greater than or equal to 15 continuous minutes. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes ."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.** (8) Page 20 /Event: Complete or partial loss of monitoring capability. We suggest to the SDT that the term "partial" be deleted from the event description. (9) We suggest to the SDT that the term "partial" be deleted for the Entity with Reporting Responsibility and changed to read: Each RC, BA, and TOP that experiences the complete loss of monitoring capability. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event is now written to state:** **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.**
Response: The SDT thanks you for your comment.		
We Energies	No	Submitting reports to the ERO: NERC and all of the Regional Entities are the ERO. If I

Organization	Yes or No	Question 2 Comment
		send a report to any Regional Entity (and not NERC), I have sent it to the ERO. **The SDT would like to point out the FERC has approved NERC to be the ERO. And the NERC has a delegation agreement with each Regional Entities. This Requirement R1 requires you send a report to the ERO (and whoever else the entity wishes to inform per Requirement R1 including the applicable regions if you are so obligated or its' your desire).** Damage or Destruction of a Facility: A DP may not have a Facility by the NERC Glossary definition. All distribution is not a Facility. Did you mean to exclude all distribution? **The SDT agrees that if a DP does not own or operate a Facility then this event would not be applicable to them.** Any Physical threat that could impact the operability of a Facility: An RC does not have Facilities by the NERC Glossary definition. An RC will not have to report this. BES Emergency... Reporting Responsibility: If meeting the Reporting Threshold was due to a directive from the RC, who is the Initiating entity? **The SDT agrees concerning the RC does not own a Facility and has removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or**

Organization	Yes or No	Question 2 Comment
		Suspicious device or activity at a Facility **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** Voltage deviation on a Facility Threshold for Reporting: 10% of what voltage? Nominal, rated, scheduled, design, actual at an instant? **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.**
Response: The SDT thanks you for your comment.		
NextEra Energy Inc	No	As stated in NextEra's past comments, we continue to be concerned that EOP-004-2 does not appropriately address actual sabotage that threatens the Bulk Electric

Organization	Yes or No	Question 2 Comment
		System (BES) versus random acts that are isolated and pose no risk to the BES. Therefore, NextEra repeats a portion of its past comments below in the hope that the next revision of EOP-004-2 will more adequately address NextEra's concerns. Specifically, NextEra's requests that its definition of sabotage set forth below replace Attachment 1's "Damage and Destruction of Equipment" and "Any physical threat that could impact the operability of a Facility." In Order No. 693, FERC stated its interest in NERC revising CIP-001 to better define sabotage and requiring notification to the certain appropriate federal authorities, such as the Department of Homeland Security. FERC Order No. 693 at PP 461, 462, 467, 468, 471. NextEra has provided an approach that accomplishes FERC's objectives and remains within the framework of the drafting team, but also focuses the process of determining and reporting on only those sabotage acts that could affect other BES systems. Today, there are too many events that are being reported as sabotage to all parties in the Interconnection, when in reality these acts have no material affect or potential impact to other BES systems other than the one that experienced it. For example, while the drafting team notes the issue of copper theft is a localized act, there are other localized acts of sabotage that are committed by an individual, and these acts pose little, if any, impact or threat to other BES systems. Reporting sabotage that does not need to be sent to everyone does not add to the security or reliability of the BES. Relatedly, there is a need to clarify some of the current industry confusion on who should (and has the capabilities to) be reporting to a broader audience of entities. Hence, the NextEra approach provides a clear definition of sabotage, as well as the process for determining and reporting sabotage. New Definition for Sabotage. Attempted or Actual Sabotage: an intentional act that attempts to or does destroy or damage BES equipment for the purpose of disrupting the operations of BES equipment, or the BES, and has a potential to materially threaten or impact the reliability of one or more BES systems (i.e., one act of sabotage on BES equipment is only reportable if it is determined to be part of a larger conspiracy to threaten the reliability of the Interconnection or more than one BES system).
Response: The SDT thanks you for your comment. The SDT has stated in our "Consideration of Issues and Directives – March 15,		

Organization	Yes or No	Question 2 Comment
2012" that was posted with the last posting stated: **The SDT has not proposed a definition for inclusion in the NERC Glossary because it is impractical to define every event that should be reported without listing them in the definition. Attachment 1 is the de facto definition of "event". The SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that without the intervention of law enforcement after the fact, it was almost impossible to determine if an act or event was that of sabotage or merely vandalism. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.** **The SDT has discussed this with FERC Staff and we agree that sabotage could be a state of mind; and, therefore, the real issue: Was there an event or not?**		
ISO New England Inc	No	
Response: The SDT thanks you for your participation.		
Nebraska Public Power District	No	1. The following comments are in regard to Attachment 1:A. The row [Event] titled "Damage or destruction of Facility": 1. In column 3 [Threshold for Reporting], the word "Affect" is vague note the following concerns: i. Does "Affect" include a broken crossarm damaged without the Facility relaying out of service. This could be considered to have an "Affect" on the IROL. ii. Would the answer be different if the line relayed out of service and auto-reclosed (short interruption) for the same damaged crossarm? We need clarity from the SDT in order to know when a report is due. 2. For clarification: Who initiates the report when the IROL interfaces spans between multiple entities? We know of an IROL that has no less that four entities that operate Facilities within the interface. Who initiates the report of the IROL is affected? All? **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and**

Organization	Yes or No	Question 2 Comment
		identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: "Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency." This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action."

Organization	Yes or No	Question 2 Comment
		This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** B. The row [Event] titled "Any physical threat that could impact the operability of a Facility":1. In Column 1 [Event] change the word "threat" to "attack", this aligns with the OE-417 report.2. In Column 3 [Threshold for Reporting], align the threshold with the OE-417 form. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility**

Organization	Yes or No	Question 2 Comment
		Or **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** C. The row [Event] titled "Transmission loss", in column 3 [Threshold for Reporting], the defined term "Transmission Facilities" is too vague. There needs to be a more description such that an entity clearly understands when an event is reportable and for what equipment. We would recommend the definition used in the Event Reporting Field Trial: An unexpected outage, contrary to design, of three or more BES elements caused by a common disturbance. Excluding successful automatic reclosing. For example: a. The loss of a combination of NERC-defined Facilities. b. The loss of an entire generation station of three or more generators (aggregate generation of 500 MW to 1,999 MW); combined cycle units are represented as one unit. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry**

Organization	Yes or No	Question 2 Comment
		comments to state: **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** D. The row [Event] titled "Complete or partial loss of monitoring": 1. In column 1 [Event], delete the words "or partial". This is subjective without definition, delete. 2. Also in column 1 [Event], delete the word "monitoring" and replace with Supervisory Control and Data Acquisition (SCADA). SCADA is defined term that explicitly calls out in the definition "monitoring and control" and is understood by the industry as such. 3. In column 2 [Entity with Reporting Responsibility], delete the words "or partial"; also delete the word "monitoring" and replace with SCADA. 4. In column 3 [Threshold for Reporting], reword to state "Complete loss of SCADA affecting a BES control center for >/= 30 continuous minutes". **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event is now written to state:** **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.**
Response: The SDT thanks you for your comment.		
GTC	No	Page 17 & 18, One Hour Reporting and Twenty-four Hour Reporting: append the introductory statements with the following: "meeting the threshold for reporting" after recognition of the event. Example: Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within twenty-four hours of recognition of the event meeting the threshold for reporting. Page 19, system separation (islanding); Clarify the intent of this threshold for reporting: Load >= 100 MW and any generation; or Load >= 100 MW and Generation

Organization	Yes or No	Question 2 Comment
		>= 100 MW, or some combination of load and generation totaling 100 MW.
Response: The SDT thanks you for your comment. The SDT has chosen not add the requested language as we believe the intent is understood that the time frames means from "meeting the threshold for reporting." The SDT has revised the language regarding islanding and we believe it addresses your concern.		
Indiana Municipal Power Agency	No	The event "any physical threat that could impact the operability of a Facility" is not measurable and can be interpreted many ways by entities or auditors. IMPA recommend incorporating language that let's this be the judgment of the registered entity only. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or**

Organization	Yes or No	Question 2 Comment
		activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility. On the "voltage deviation on a Facility", IMPA recommends that only the TOP the experiences a voltage deviation be the one responsible for reporting. **The SDT has made this change per comments received from the industry.** For generation loss and transmission loss, IMPA believes that the amount of loss needs to be associated with a time period or event (concurrent forced outages).
Response: The SDT thanks you for your comment.		
Idaho Power Co.	No	I think that the category "Damage or destruction of a Facility" is too ambiguous, and the Threshold for Reporting criteria does not help to clarify the question. Any loss of a facility may result in the need for actions to get to the new operating point, would this be a reportable disturbance? **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."**

Organization	Yes or No	Question 2 Comment
		This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).

Organization	Yes or No	Question 2 Comment
		The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.
Response: The SDT thanks you for your comment.		
MISO	No	
American Public Power Association	No	APPA in our comments on the previous draft of EOP-004-2 requested relief for small entities from this reporting/documentation standard. APPA suggested setting a 300 MW threshold for some of the criteria in Attachment 1. This suggestion was not accepted by the SDT. However, the SDT is still directed by FERC to "consider whether separate, less burdensome requirements for smaller entities may be appropriate. Therefore, APPA requests that the SDT provide relief to small entities by providing separate requirements for small entities by requiring reporting only when one of the four criteria in DOE-OE-417 are met: 1. Actual physical attack, 2. Actual cyber attack, 3. Complete operational failure, or 4. Electrical System Separation. APPA recommends this information should be reported to the small entity's BA as allowed in the DOE-OE-417 joint filling process.
Response: The SDT thanks you for your comment. The SDT has taken your concerns into consideration (as directed by FERC) and believes that "small entities" will most likely not meet the thresholds for reporting since items are predicated on "Facilities" or they don't meet the Threshold for reporting.		
Brazos Electric Power Cooperative	No	Please see the comments submitted by ACES Power Marketing.

Organization	Yes or No	Question 2 Comment
Response: The SDT thanks you for your comment. Please review the response to those comments.		
Puget Sound Energy, Inc.	No	The Note at the beginning of Attachment 1 references notifying parties per Requirement R1; however, notification occurs in conjunction with Requirement R2.The term "Adverse Reliability Impact" is used in the threshold section of the event "Damage or destruction of a Facility". At this time, there are two definitions for that term in the NERC Glossary. The FERC-approved definition for this term is "The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection." If the drafting team instead means to use the definition that NERC approved on 8/4/2011 (as seems likely, since that definition more closely aligns with the severity level indicated by the other two threshold statements) then the definition should be included in the Implementation Plan as a prerequisite approval. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could**

Organization	Yes or No	Question 2 Comment
		adversely affect the reliability of the Bulk Electric System). **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** In addition, would the threshold of "Results from actual or suspected intentional human action" include results from actual intentional human action which produced an accidental result, meaning, someone was intentionally doing some authorized action but unintentionally made a mistake, leading to damage of a facility? The event "Any physical threat that could impact the operability of a Facility" will require reporting for many events that have little or no significance to reliable operation of the Bulk Electric System. For example, a balloon lodged in a 115 kV transmission line is a "physical threat" that could definitely "impact the operability" of that Facility and, yet, will probably have little reliability impact. So, too, could a car-pole accident that causes a pole to lean, a leaning tree, or an unfortunately-located bird's nest. The drafting team should develop appropriate threshold language so that reporting is required only for events that do threaten the reliability of the Bulk Electric System. **The SDT also developed another to read:** **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per**

Organization	Yes or No	Question 2 Comment
		Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** With respect to the event "Unplanned control center evacuation", the standard drafting team should include the term "complete" in the description and/or threshold statement to avoid having partial evacuations trigger the need to report. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unplanned evacuation from BES control center facility for 30 continuous minutes or more." The SDT does not believe the word "complete" needs to be added.**
Response: The SDT thanks you for your comment.		
Central Lincoln	No	1) We appreciate the changes made to reduce the short time reporting requirements.

Organization	Yes or No	Question 2 Comment
		The SDT has removed the one-hour reporting time frame, and all events are to be reported within 24 hours of recognition of the event. 2) We would like to point out that the 24 hour reporting threshold for "Damage or destruction of a Facility" resulting from intentional human action will still be non-proportional BES risk for certain events. The discovery of a gunshot 115 kV insulator will start the 24 hour clock running, no matter how busy the discoverer is performing restoration or other duties that are more important. The damage may have been done a year earlier, but upon discovery the report suddenly becomes the priority task. To hit the insulator, the shooter likely had to take aim and pull the trigger, so intent is at least suspected if not actual. And the voltage level ensures the insulator is part of a Facility. **The SDT has updated Damage or destruction of a facility into 2 different thresholds:** **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).**

Organization	Yes or No	Question 2 Comment
		This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s). The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could

Organization	Yes or No	Question 2 Comment
		further define what a suspected intentional human action is within their Operating Plan. 3) We also note that the theft of in service copper is not a physical threat, it is actual damage. The reference to Footnote 1 should be relocated or copied to the cell above the one it resides in now. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** 4) We support the APPA comments regarding small entities. **The SDT has taken your concerns into consideration (as directed by FERC) and believes that "small entities" will most likely not meet the thresholds for reporting**

Organization	Yes or No	Question 2 Comment
		since items are predicated on "Facilities."
Response: The SDT thanks you for your comment.		
Los Angeles Department of Water and Power	No	LADWP has the following comments:#1 - "Any physical threat that could impact the operability of a Facility" is still vague and "operability" is too low a threshold. There needs to be a potential impact to BES reliability. **The SDT has updated Damage or destruction of a facility into 2 different thresholds:** **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed"**

Organization	Yes or No	Question 2 Comment
		Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. **The SDT also developed another to read:** **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** #2 - "Voltage Deviation on a Facility" I think the threshold definition needs to be more specific: Is it 10% from nominal? 10% from normal min/max operating

Organization	Yes or No	Question 2 Comment
		tables/schedules? Another entities 10% might be different than mine. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes ."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.** #3 - "Transmission Loss" The threshold of three facilities is still too vague. A generator and a transformer and a gen-tie are likely to have overlapping zones of protection that could routinely take out all three. The prospect of penalties would likely cause unneeded reporting. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."**
Response: The SDT thanks you for your comment.		
Deseret Power	No	The threshold for reporting is way too low. A gun shot insulator is not an act of

Organization	Yes or No	Question 2 Comment
		terrorism... vandalism yes... and a car hit pole would be reportable on a 138 kv line. these seem to be too aggressive in reporting.
Response: The SDT thanks you for your comment. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.**		
Kansas City Power & Light	No	For the event, "Damage or destruction of a Facility", the "Threshold for reporting" includes "Results from actual or suspected intentional human action". This is too broad and could include events such as damage to equipment resulting from stealing cooper or wire which has no intentional motivation to disrupt the reliability of the bulk electric system. Reports of this type to law enforcement and governmental agencies will quickly appear as noise and begin to be treated as noise. This may result in overlooking a report that deserves attention. Recommend the drafting team consider making this threshold conditional on the judgment by the entity on the

Organization	Yes or No	Question 2 Comment
		human action intended to be a potential threat to the reliability of the bulk electric system. For the event, "Any physical threat that could impact the operability of a Facility", the same comment as above applies. The footnote states to include copper theft if the Facility operation is impacted. Again, it is recommended to make a report of this nature conditional on the judgment of the entity on the intent to be a potential threat to the reliability of the bulk electric system.

Response: The SDT thanks you for your comment. The SDT has updated Damage or destruction of a facility into 2 different thresholds:

The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:

"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."

This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).

This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each

Organization	Yes or No	Question 2 Comment
interconnection. **The SDT also developed another to read:** **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.**		
Dominion	Yes	Comments: While Dominion agrees that the revisions are a much appreciated improvement, we are concerned that Attachment 1 does not explicitly contain the 'entities which must be, at a minimum, notified. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified.** Attachment 2 appears to indicate that only the ERO and the Reliability Coordinator for the Entity with Reporting Responsibility need be informed. However, the background section indicates that the Entity with Reporting Responsibility is also

Organization	Yes or No	Question 2 Comment
		expected to contact local law enforcement. We therefore suggest that Attachment 2 be modified to include local law enforcement. **The SDT has adapted the language in Attachment 2 along the lines of your concern.** Page 26 redline; Attachment 1; Event - Damage or destruction of a Facility; Threshold for Reporting - Results from actual or suspected intentional human action; Dominion is concerned with the ambiguity that this could be interpreted as applying to distribution. Page 27 redline; Attachment 1; Event - Any physical threat that could impact the operability of a Facility; Dominion is concerned the word "could" is hypothetical and therefore unverifiable and un-auditable. **The SDT has updated Damage or destruction of a facility into 2 different thresholds:** **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).**

Organization	Yes or No	Question 2 Comment
		This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s). The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within

Organization	Yes or No	Question 2 Comment
		their Operating Plan. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** The SDT could provide a list of hypothetical "could impact" events, as well as a specific definition and method for determining a specific physical impact threshold for "could impact" events other than "any."

Organization	Yes or No	Question 2 Comment
		The SDT cannot provide a list of hypothetical events, but will remind the entity that the Operating Plan that is required per Requirement R1 could contain a basis to report concerning your unique system equipment or configuration of your system.
Response: The SDT thanks you for your comment.		
Seattle City Light	Yes	This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
Response: The SDT thanks you for your comment. Please review the response to Question 4.		
Avista	Yes	In general the SDT has made significant improvements to Attachment 1. Avista does have a suggestion to further improve Attachment 1.In Attachment 1 under the 24 hour Reporting Matrix, the second event states "Any physical threat that could impact the operability of a Facility" and the Threshold for Reporting states "Threat to a Facility excluding weather related threats". This is extremely open ended. We suggest adding the following language to the Threshold for Reporting for Any Physical Threat: Threat to a facility that: Could affect an IROL (per FAC-014) OR Could result in the need for actions to avoid and Adverse Reliability Impact This new language would be consistent with the reporting threshold for a Damage event.
Response: The SDT thanks you for your comment. The SDT has updated Damage or destruction of a facility into 2 different thresholds: **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator**		

Organization	Yes or No	Question 2 Comment
Area that results in the need for actions to avoid a BES Emergency." This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s). The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT		

Organization	Yes or No	Question 2 Comment
envisions that entities could further define what a suspected intentional human action is within their Operating Plan.		
PNGC Comment Group	Yes	We agree with reservations. Our comments are below and we are seeking clarification of the Applicability section of the standard. We are voting "no" but if slight changes are made to the applicability section we will change our votes to "yes". NERC and FERC have expressed a willingness to address the compliance burden on smaller entities that pose minimal risk to the Bulk Electric System. The PNGC Comment Group understands the SDT's intent to categorize reportable events and achieve an Adequate Level of Reliability while also understanding the costs associated. Given the changes made by the SDT to Attachment 1, we believe you have gone a long way in alleviating the potential for needless reporting from small entities that does not support reliability. **The SDT has taken your concerns into consideration (as directed by FERC) and believes that "small entities" will most likely not meet the thresholds for reporting since items are predicated on "Facilities."** One remaining concern we have are potential reporting requirements in the Event types; "Damage or destruction of a Facility" and "Any physical threat that could impact the operability of a Facility". These two event types have the following threshold language; "Results from actual or suspected intentional human action" and "Threat to a Facility excluding weather related threats" respectively. We believe these two thresholds could lead to very small entities filing reports for events that really are not a threat to the BES or Reliability. **The SDT has updated Damage or destruction of a facility into 2 different thresholds:** **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:**

Organization	Yes or No	Question 2 Comment
		"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency." This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or

Organization	Yes or No	Question 2 Comment
		destroyed" intentionally by a human. **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** Note: For vandalism, sabotage or suspected terrorism, even the smallest entities will file a police report and at that point local law enforcement will follow their terrorism reporting procedures if necessary, as you've rightly indicated in your "Law Enforcement Reporting" section. We believe extraneous reporting could be alleviated with a small tweak to the Applicability section for 4.1.9 to exclude the smallest Distribution Providers. As stated before, even if these very small entities are excluded from filing reports under EOP-004-2, threats to Facilities that they may have will still be reported to local law enforcement while not cluttering up the NERC/DOE reporting process for real threats to the BES. Our suggested change:4.1.9. Distribution Provider: with peak load >= 200 MWs. The PNGC Comment Group arrived at the 200 MWs threshold after reviewing Attachment 1, Event "Loss of firm load for >= 15 Minutes". We agree with the SDT's intent to exclude these small firm load losses from reporting through EOP-004-2.Another approach we could support is that taken by the Project 2008-06 SDT with respect to Distribution Provider Facilities:4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

Organization	Yes or No	Question 2 Comment
		The SDT has discussed this very issue and would like to point out that the Threshold for Reporting limits are the same as in the enforceable Reliability Standard, EOP-004-1. The SDT believes that small entities (200mw or less) would not be applicable to this event. The SDT has attempted to place these types of limits to reduce small entities from having these applicable reporting requirements. o A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more o A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard o A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard o Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started. We're not advocating this exact language but rather the approach that narrows the focus to what is truly impactful to reliability while minimizing costs and needless compliance burden. One last issue we have is with the language in Attachment 1, Event "BES Emergency resulting in automatic firm load shedding." Under "Entity with Reporting Responsibility", you state that the DP or TOP that "implements" automatic load shedding of >= 100 MWs must report (Also please review the CIP threshold of 300 MWs as this may be a more appropriate threshold). We believe rather than specifying a DP or TOP report, it would be appropriate for the UFLS Program Owner to file the report per EOP-004-2. In our situation we have DPs that own UFLS relays that are part of the TOP's program and this could lead to confusing reporting requirements. Also we don't believe that an entity can "Implement" "Automatic" load shedding but this is purely a semantic issue. **The SDT has updated Damage or destruction of a facility into 2 different thresholds:** **The SDT removed all language under "Entity with Reporting Responsibility" with**

Organization	Yes or No	Question 2 Comment
		the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: "Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency." This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected

Organization	Yes or No	Question 2 Comment
		intentional human action." **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.**
Response: The SDT thanks you for your comment.		
United Illuminating Company	Yes	The phrasing of the event labeled as Event Damage or Destruction of a Facility may be improved in the Threshold for Reporting Column. Suggest the introduction sentence for this event should be phrased as Where the Damage or Destruction of a Facility: etc. The rationale for the change is that as written it is unclear if the list that follows is meant to modify the word Facilities or the overall introductory sentence. The confusion being caused by the word That. What is important to be reported is if a Facility is damaged and then an IROL is affected it should be reported, not that if a Facility is comprising an IROL Facility is damaged but there is no impact on the IROL.

Organization	Yes or No	Question 2 Comment
		The SDT has updated Damage or destruction of a facility into 2 different thresholds: The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency. This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read:

Organization	Yes or No	Question 2 Comment
		"Damage or destruction of its Facility that results from actual or suspected intentional human action." **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** Second, the top of each table is the phrase Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the event. This creates the requirement that the actual form is required to be transmitted to parties other than NERC/DOE. The suggested revision is Submit EOP-004 Attachment 2 or DOE-OE-417 report to NERC and/or DOE, and complete notification to other organizations identified pursuant to Requirement R1 Part 1.2 within one hour etc.. **The SDT has revised Attachment 2 heading to read "Use this form to report events. The Electric Reliability Organization will accept the DOE OE-417 form in lieu of this**

Organization	Yes or No	Question 2 Comment
		form if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net voice: 404-446-9780." Based on industry comments.
Response: The SDT thanks you for your comment.		
Ingleside Cogeneration LP	Yes	Ingleside Cogeneration LP agrees with the removal of nearly all one hour reporting requirements. In our view there must be a valid contribution expected of the recipients of any reporting that takes place this early in the process. Any non-essential communications will impede the progress of the front-line personnel attempting to resolve the issue at hand - which has to be the priority. Secondly, there is a risk that early reporting may include some speculation of the cause, which may be found to be incorrect as more information becomes available. Recipients must temper their reactions to account for this uncertainty. In fact, Ingleside Cogeneration LP recommends that the single remaining one-hour reporting scenario be eliminated. It essentially defers the reporting of a cyber security incident to CIP-008 anyways, and may even lead to a multiple violation of both Standards if exceeded.
Response: The SDT thanks you for your comment. The SDT agrees and has removed the one-hour reporting requirement based on comments received.		
Springfield Utility Board	Yes	o Spell out Requirement 1, rather than "parties per R1" in NOTE. o On page 44, "Examples of such events include" should say, "include, but are not limited to". o SUB appreciates clarification regarding events, particularly the discussion regarding "sabotage", and recommends listing and defining "Event" in Definitions and Terms Used in NERC Standards. **The SDT has stated in our "Consideration of Issues and Directives – March 15, 2012" that was posted with the last posting stated:** **The SDT has not proposed a definition for inclusion in the NERC Glossary because it is impractical to define every event that should be reported without listing them in**

Organization	Yes or No	Question 2 Comment
		the definition. Attachment 1 is the de facto definition of "event." The SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that without the intervention of law enforcement after the fact, it was almost impossible to determine if an act or event was that of sabotage or merely vandalism. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The SDT believes that this is an equally effective and efficient means of addressing the FERC Directive. **The SDT has discussed this with FERC Staff and we agree that sabotage could be a state of mind and therefore the real issue was there an event or not.** o The Guideline and Technical Basis provides clarity, and SUB agrees with the removal of "NERC Guideline: Threat and Incident Reporting". o In the flow chart on page 9 there are parallel paths going from "Refer to Ops Plan for Reporting" to the 'Report Event to ERO, Reliability Coordinator' via both the Yes and No response. It seems like the yes/no decision should follow after "Refer to Ops Plan" for communication to law enforcement. **The SDT has offered the flowchart as an example of how an entity could handle the notification to law enforcement agencies. There is no requirement to follow the flowchart. Entities are free to develop their own procedures based upon their needs to report.**
Response: The SDT thanks you for your comment.		
PPL Electric Utilities	Yes	PPL EU thanks the SDT for the changes made in this latest proposal. We feel our prior comments were addressed. Regarding the event 'Transmission Loss': For your consideration, please consider adding a footnote to the event 'Transmission Loss' such that weather events do not need to be reported. Also please consider including 'operation contrary to design' in the threshold language. E.g. consistent with the

Organization	Yes or No	Question 2 Comment
		NERC Event Analysis table, the threshold would be, 'Unintentional loss, contrary to design, of three or more BES Transmission Facilities.'
Response: The SDT thanks you for your comment. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."**		
Tacoma Power	Yes	Tacoma Power supports the revisions. It appears that all agencies and entities are willing to support the use of the DOE Form OE-417 as the initial notification form (although EOP-004 does include their own reporting form as an attachment to the Standard). Tacoma is already using the OE-417 and distributing it to all applicable Entities and Agencies.
Response: The SDT thanks you for your comment.		
Seattle City Light	Yes	This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
Response: The SDT thanks you for your comment. Please review the response to Question 4.		
MEAG Power	Yes	This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
Response: The SDT thanks you for your comment. Please review the response to Question 4.		
Public Utility District No. 1 of Snohomish County		This is an excellent improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.

Organization	Yes or No	Question 2 Comment
Response: The SDT thanks you for your comment. Please review the response to Question 4.		
Imperial Irrigation District (IID)	Yes	
Colorado Springs Utilities	Yes	
Arizona Public Service Company	Yes	
Utility Services	Yes	
Dynegy Inc.	Yes	
Manitoba Hydro	Yes	
City of Austin dba Austin Energy	Yes	
Entergy	Yes	
Pepco Holdings Inc	Yes	
Independent Electricity System Operator	Yes	
Cowlitz County PUD	Yes	
Edison Mission Marketing & Trading, Inc.	Yes	
Exelon Corporation and its affiliates	Yes	

Organization	Yes or No	Question 2 Comment
ERCOT	Yes	
Oncor Electric Delivery	Yes	

3. **The SDT has proposed a new Section 812 to be incorporated into the NERC Rules of Procedure. Do you agree with the proposed addition? If not, please explain in the comment area below.**

Summary Consideration: The DSR SDT proposed a revision to the NERC Rules of Procedure (Section 812). The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.

Organization	Yes or No	Question 3 Comment
Northeast Power Coordinating Council	No	The proposed new section does not contain specifics of the proposed system nor the interfacing outside of the system to support the report collecting.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
SPP Standards Review Group	No	We have two concerns about the proposed change to the RoP. One, we have concerns that our information and data will be circulated to an as yet undetermined audience which appears to be solely under NERC's control. Secondly, there isn't sufficient detail in the clearinghouse concept to support comments at this time.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
ISO/RTO Standards Review Committee	No	The SRC offers comments regarding the posted draft requirements; however, by so doing, the SRC does not indicate support of the proposed requirements. Following these comments, please see the latter part of the SRC's response to Question 4 below for an SRC proposed alternative approach: The SRC is unable to comment on the proposed new section as the section does not contain any description of the proposed process or the interface requirements to support the report collecting system. We reserve judgment on this proposal and our right to comment on the

Organization	Yes or No	Question 3 Comment
		proposal when the proposed addition is posted.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
ACES Power Marketing Standards Collaborators	No	(1) It is not clear to us what is the driving the need for the Rules of Procedure proposal. NERC is already collecting event and disturbance reports without memorializing the change in the Rules of Procedure. (2) The language potentially conflicts with other subsections in Section 800. For instance, the proposal says that the system will apply to collect report forms "for this section". This section would refer to Section 800. Section 800 covers NERC alerts and GADS. Electronic GADS (eGADS) already has been established to collect GADS data? Will this section cause NERC to have to incorporate eGADS into this report collection system? Incorporating NERC Alerts is also problematic because when reports are required as a result of a NERC alert, the report must be submitted through the NERC Alert system.(3) The statement that "a system to collect report forms as established for this section or standard" causes additional confusion regarding to which standards it applies. Does it only apply to this new EOP-004-2 or to all standards? If it applies to all standards, does this create a potential issue for CIP-008-3 R1.3 which requires reporting to the ES-ISAC and not this clearinghouse?
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Seattle City Light	No	Seattle City Light follows MEAG and believes this type of activity and process is better suited to NAESBE than it is to NERC Compliance.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Hydro One	No	The proposed new section does not contain specifics of the proposed system nor the

Organization	Yes or No	Question 3 Comment
		interfacing outside of the system to support the report collecting.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
CenterPoint Energy	No	CenterPoint Energy does not agree with the SDT's proposed section 812. The proposal for NERC to establish a system that will "...forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary. This can include state, federal, and provincial organizations." is redundant with the draft Standard. Responsible entities are already required to report applicable events to NERC, applicable regional entities, registered entities, and appropriate governmental, law enforcement, and regulatory agencies. CenterPoint Energy believes if the SDT's intent is to require NERC to distribute these system event reports, then EOP-004-2 should be revised to require responsible entities to only report the event to NERC. As far as distribution to appropriate NERC departments, CenterPoint Energy believes that is an internal NERC matter and does not need to be included in the Rules of Procedure.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Arkansas Electric Cooperative Corporation	No	AECC supports the comments submitted by ACES Power Marketing.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
National Rural Electric Cooperative Association (NRECA)	No	NRECA is concerned with the drafting team's proposal to add a new Section 812 to the NERC ROP. NRECA does not see the need for the drafting team to make such a proposal as it relates to the new EOP-004 that the drafting team is working on. The

Organization	Yes or No	Question 3 Comment
		requirements in the draft standard clearly require what is necessary for this Event Reporting standard. NRECA requests that the drafting team withdraw its proposed ROP Section 812 from consideration. The proposed language is unclear to the point of not being able to understand who is being required to do what. Further, the language is styled in more of a proposal, and not in the style of what would appropriately be included in the NERC ROP. Finally, the SDT has not adequately supported the need for such a modification to the NERC ROP. Without that support, NRECA is not able to agree with the need for this addition to the ROP. Again, NRECA requests that the drafting team withdraw its proposed ROP Section 812 from consideration.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Occidental Power Services, Inc.	No	This section should reference the confidentiality requirements in the ROP and should have a statement about the system for collection and dissemination of disturbance reports being "subject to the confidentiality requirements of the NERC ROP."
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Pepco Holdings Inc	No	This could create confusion.This new ROP section states that "... the system shall then forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary." Standard Section R1.2 states "A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies." If NERC is going to be the "clearinghouse" forwarding reports to the RE and DOE, does that mean that

Organization	Yes or No	Question 3 Comment
		the reporting entity only needs to make a single submission to NERC for distribution? If the reporting entity is required to make all notifications, per R1.2, what is the purpose of NERC's duplication of sending out reports? It would be very helpful to the reporting entities if R1.2 was revised to state that NERC would forward the event form to the RE and DOE and the reporting entity would only be responsible for providing notice verbally to its associated BA, TOP, RC, etc. as appropriate and for notifying appropriate law enforcement as required.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Independent Electricity System Operator	No	We are unable to comment on the proposed new section as the section does not contain any description of the proposed process or the interface requirements to support the report collecting system. We reserve judgment on this proposal and our right to comment on the proposal when the proposed addition is posted.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
MidAmerican Energy	No	See the NSRF comments. The NERC Rules of Procedure Section 807 already addresses the dissemination of Disturbance data, as does Appendix 8 Phase 1 with the activation of NERC's crisis communication plan, and the ESISAC Concept of Operations. The addition of proposed Section 812 is not necessary. The Reliability Coordinator, through the use of the RCIS, would disseminate reliability notifications if it is in turn notified per R1.2. (As stated in the in the Clean copy of EOP-004-2)
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Public Utility District No. 1 of Snohomish County	No	This type of activity and process is better suited to NAESBE than it is to NERC Compliance.

Organization	Yes or No	Question 3 Comment
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Illinois Municipal Electric Agency	No	Illinois Municipal Electric Agency supports comments submitted by ATC.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Amercian Transmission Company, LLC	No	ATC believes that the NERC Rules of Procedure Section 807 already addresses the dissemination of Disturbance data, as does Appendix 8 Phase 1 with the activation of NERC's crisis communication plan, and the ESISAC Concept of Operations. The addition of proposed Section 812 is not necessary. The Reliability Coordinator, through the use of the RCIS, would disseminate reliability notifications if it is in turn notified per R1.2. (As stated in the in the Clean copy of EOP-004-2)
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Ameren	No	If the SDT keeps new Section 812 we suggest to the SDT a wording change for the second sentence, underlined: "Upon receipt of the submitted report, the system shall then forward the report to the appropriate NERC department for review. After review, the report will be forwarded to the applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary."
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
We Energies	No	Section 812 refers to the section as a standard and as a Procedure. That is not correct.Section 812 reads to me as if NERC (the system) will be forwarding everything

Organization	Yes or No	Question 3 Comment
		specified anywhere in RoP 800.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Exelon Corporation and its affiliates	No	While we don't have any immediate objection to revising the Rules of Procedures (ROP) to allow for report collecting under Section 800 relative to the EOP-004 standard, the proposed language is unclear and confusing. Please consider the following revision:"812. NERC Reporting Clearinghouse NERC will establish a system to collect reporting forms as required for Section 800 or per FERC approved standards from any Registered Entities. NERC shall distribute the reports to the appropriate governmental, law enforcement, regulatory agencies as required per Section 800 or the applicable standard."Further, NERC should post ROP revisions along with a discussion justifying the revision for industry comment specific to the ROP. There may be significant implications to this revision beyond the efforts relative to EOP-004.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Tacoma Power	No	Tacoma Power disagrees with the requirement to perform annual testing of each communication plan. We do not see any added value in performing annual testing of each communication plan. There are already other Standard requirements to performing routine testing of communications equipment and emergency communications with other agencies.The "proof of compliance" to the Standard should be in the documentation of the reports filed for any qualifying event, within the specified timelines and logs or phone records that it was communicated per each specified communication plan.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		

Organization	Yes or No	Question 3 Comment
Seattle City Light	No	Seattle City Light follows MEAG and believes this type of activity and process is better suited to NAESBE than it is to NERC Compliance.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
MEAG Power	No	This type of activity and process is better suited to NAESBE than it is to NERC Compliance.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
ERCOT	No	ERCOT has joined the IRC comments on this project.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Idaho Power Co.	No	No opinion
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
MISO	No	MISO agrees with and adopts the Comments of the IRC on this issue.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Brazos Electric Power Cooperative	No	Please see the comments submitted by ACES Power Marketing.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports		

Organization	Yes or No	Question 3 Comment
to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Kansas City Power & Light	No	Rules stipulating the extent of how reported information will be treated by NERC is an important consideration, however, the proposed section 812 proposes to provide reports to other governmental agencies and regulatory bodies beyond that of NERC and FERC. NERC should be treating the event information reported to NERC as confidential and should not take it upon itself to distribute such information beyond the boundaries of the national interest at NERC and FERC.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Dominion	Yes	While Dominion supports this addition, we suggest adding to the sentence "NERC will establish a system to collect report forms as established for this section or reliability standard....."
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
MRO NSRF	Yes	ATC believes that the NERC Rules of Procedure Section 807 already addresses the dissemination of Disturbance data, as does Appendix 8 Phase 1 with the activation of NERC's crisis communication plan, and the ESISAC Concept of Operations. The addition of proposed Section 812 is not necessary. The Reliability Coordinator, through the use of the RCIS, would disseminate reliability notifications if it is in turn notified per R1.2. (As stated in the in the Clean copy of EOP-004-2)
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Ingleside Cogeneration LP	Yes	Ingleside Cogeneration is encouraged by NERC's willingness to act as central data gathering point for event information. However, we see this only as a starting point.

Organization	Yes or No	Question 3 Comment
		There are still multiple internal and external reporting demands that are similar to those captured in EOP-004-2 - examples include the DOE, RAPA (misoperations), EAWG (events analysis), and ES-ISAC (cyber security). Although we appreciate the difference in reporting needs expressed by each of these organizations, there are very powerful reporting applications available which capture a basic set of data and publish them in multiple desirable formats. We ask that NERC spearhead this initiative - as it is a natural part of the ERO function.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
American Electric Power	Yes	While we have no objections at this point, we would like specific details on what our obligations would be as a result of these changes. For example, would the clearinghouse tool provide verifications that the report(s) had been received as well as forwarded? In addition, if DOE OE-417 is the form being submitted, would the NERC Reporting Clearinghouse forward that report to the DOE?
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Springfield Utility Board	Yes	o SUB supports the new Section 812 being incorporated into the NERC ROP. This addition provides clarity for what is required by whom and takes away any possible ambiguity.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
FirstEnergy Corp	Yes	FE agrees but asks that the defined term “registered entities” in the second sentence be capitalized.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports		

Organization	Yes or No	Question 3 Comment
to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
GTC	Yes	With the exception of the RC and company personnel, it appears this proposed section captures the same reporting obligations and to the same entities via R1.2. Recommend adjustments to R1.2 such that reportable events are submitted to NERC, RC, and company personnel.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Central Lincoln	Yes	Thank you for minimizing the number of necessary reports.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Xcel Energy		We believe such a tool would be useful, however we are indifferent as to if it is required to be established by the Rules of Procedure.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
ISO New England Inc		We unable to comment on the proposed new section as the section does not contain any description of the proposed process or the interface requirements to support the report collecting system. We reserve judgment on this proposal and our right to comment on the proposal when the proposed addition is posted.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Indiana Municipal Power Agency		no comment

Organization	Yes or No	Question 3 Comment
Los Angeles Department of Water and Power		LADWP does not have a comment on this question at this time
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
DECo	Yes	
Duke Energy	Yes	
Luminant	Yes	
Bonneville Power Administration	Yes	
Imperial Irrigation District (IID)	Yes	
Florida Municipal Power Agency	Yes	
LG&E and KU Services	Yes	
PPL Corporation NERC Registered Affiliates	Yes	
PNGC Comment Group	Yes	
Colorado Springs Utilities	Yes	
Arizona Public Service Company	Yes	

Organization	Yes or No	Question 3 Comment
Southern Company Services	Yes	
Utility Services	Yes	
Georgia System Operations Corporation	Yes	
Manitoba Hydro	Yes	
Clark Public Utilities	Yes	
New York Power Authority	Yes	
Consolidated Edison Co. of NY, Inc.	Yes	
Orange and Rockland Utilities, Inc.	Yes	
Farmington Electric Utility System	Yes	
Public Service Enterprise Group	Yes	
PPL Electric Utilities	Yes	
Cowlitz County PUD	Yes	
Edison Mission Marketing & Trading, Inc.	Yes	

Organization	Yes or No	Question 3 Comment
American Public Power Association	Yes	
Oncor Electric Delivery	Yes	
Deseret Power	Yes	

4. Do you have any other comment, not expressed in the questions above, for the SDT?

Summary Consideration: The DSR SDT received several suggestions for improvement to the standard. The DSR SDT has removed reporting of Cyber Security Incidents from EOP-004 and have asked the team developing CIP-008-5 to retain this reporting. Most of the language contained in the "Background" Section was moved to the "Guidelines and Technical Basis" Section. Minor language changes were made to the measures and the data retention section. Attachment 2 was revised to list events in the same order in which they appear in Attachment 1.

Organization	Yes or No	Question 4 Comment
Texas Reliability Entity		(1) The ERO and Regional Entities should not be included in the Applicability of this standard. The only justification given for including them was they are required to comply with CIP-008. CIP-008 contains its own reporting requirements, and no additional reliability benefit is provided by including ERO and Regional Entities in EOP-004. Furthermore, stated NERC policy is to avoid writing requirements that apply to the ERO and Regional Entities, and we do not believe there is any sufficient reason to deviate from that policy in this standard. **The SDT is revising the standard to not contain reporting for Cyber Security Incidences. Under the revisions, CIP-008-3 and successive versions will retain the reporting requirements. The Applicability section has been revised to address this situation.** (2) Under Compliance, in section 1.1, all the words in "Compliance Enforcement Authority" should be capitalized. **The SDT agrees and has adopted this suggestion.** (3) Under Evidence Retention, it is not sufficient to retain only the "date change page" from prior versions of the Plan. It is not unduly burdensome for the entity to retain all prior versions of its "event reporting Operating Plan" since the last audit, and it should be required to do so. (What purpose is supposed to be served by

Organization	Yes or No	Question 4 Comment
		retaining only the "date change pages"?) **The SDT has revised the standard to require the retention of previous versions, not just the date change page.** (4) The title of part F, "Interpretations," is incorrect on page 23. Should perhaps be "Associated Documents." **The SDT has revised Part F and it now contains the Guidelines and Technical Basis.**
Response: The SDT thanks you for your comment.		
ACES Power Marketing Standards Collaborators		(1) IC, TSP, TO, GO, and DP should be all removed from the applicability of the standard. Previous versions of the standard did not apply to them and we see no reason to expand applicability to them. IC and TSP are not even mentioned in any of the "Entity with Reporting Responsibility" sections. For the sections that do not mention specific entities, IC and TSP would have no responsibility for any of the events. The TO and GO are not operating entities so the reporting should not apply to them. DP was not included in any previous versions of CIP-001 or EOP-004. Any information (such as load) that was necessary regarding DPs was always gathered by the BA or TOP and included in their reports. There is no indication that this process was not working and, therefore, it should not be changed. Furthermore, including the DP potentially expands the standard outside of the Bulk Electric System which is contrary to recent statements that NERC Legal has made at the April 11 and 12, 2012 SC meeting. Their comments indicated the standards are written for the Bulk Electric System. What information does a DP have to report except load loss which can easily be reported by the BA or TOP? **The SDT disagrees with some of your suggestions. As the standard is to report events associated with physical assets, it is incumbent for the asset owners to file the reports associated with any events. Thus DP, TO, and GO were added to the Applicability of this standard. Their perspectives on events can be useful in evaluating situational awareness and providing NERC with information on lessons learned. Further, this standard limits reporting to BES Elements except where**

Organization	Yes or No	Question 4 Comment
		noted. This is consistent with NERC and SC Standard Process design. Where this standard had included other functional registrations associated with the inclusion of CIP-008; those registrations have been removed from the standard. (2) Measure M2 needs to clarify an attestation is an acceptable form of evidence if there are no events. **Registered Entities must determine how to best demonstrate they have met the performance obligation of a requirement. The use of an attestation statement is already permitted and recognized with the NERC Compliance Program if that is the best means of demonstrating your performance under the requirement. Auditors will then assess whether or not an attestation meets the requirement in one's audit. Attestations cannot be specifically permitted for use.** (3) The rationale box for R3 and R4 should be modified. It in essence states that updating the event reporting Operating Plan and testing it will assure that the BES remains secure. While these requirements might contribute to reliability, these two requirements collectively will not assure BES security and stability. **The SDT has revised the rationale box language based upon the changes it has made to the requirements. It should be noted that upon acceptance of the standard, the language in the rationale boxes are removed from the standard.** (4) We disagree with the VSLs for Requirement R2. While the VSLs associated with late reporting for a 24-hour reporting requirement include four VSLs, the one-hour reporting requirement only includes three VSLs. There seems to be no justification for this inconsistency. Four VSLs should be written for the one-hour reporting requirement. **As the standard has been revised to remove the one-hour reporting provision, your suggestion is moot.** (5) Reporting of reportable Cyber Security Incidents does not appear to be fully coordinated with version 5 of the CIP standards. For instance, EOP-004-2 R1, Part 1.2 requires a process for reporting events to external entities and CIP-008-5 Part 1.5

Organization	Yes or No	Question 4 Comment
		requires identifying external groups to which to communicate Reportable Cyber Security Incidents. Thus, it appears the Cyber Security Incident response plan in CIP-008-5 R1 and the event reporting Operating Plan in EOP-004-2 R1 will compel duplication of external reporting at least in the document of the Operating Plain and Reportable Cyber Security Incident response plan. This needs to be resolved. **While the SDT had worked this through with the other standard team to resolve this concern; it is now irrelevant, as reporting of Cyber Security Incidences are no longer part of EOP-004-2.** (6) In the effective date section of the implementation plan, the statement that the prior version of the standard remains in effect until the new version is accepted by all applicable regulatory authorities is not correct. In areas where regulatory approval is required, it will only remain in effect in the areas where the regulator has not approved it. **The SDT finds that the two statements are making the same point; that the new standard does not become enforceable until all regulatory authorities have approved it.** (7) On page 6 in the background section, the statement attributing RCIS reporting to the TOP standards is not accurate. There is no requirement in the TOP standards to report events across RCIS. In fact, the only mention of RCIS in the standards occurs in EOP-002-3 and COM-001-1.1. **The SDT agrees and adopts your suggestion.** (8) On page 6 in the background section, the first sentence of the third paragraph is not completely aligned with the purpose statement of the standard. The statement in the background section indicates that the reliability objective "is to prevent outages which could lead to Cascading by effectively reporting events". However, the purpose states that the goal is to improve reliability. We think it would make more sense for the reliability objective to match the purpose statement more closely. **The SDT has revised the Background section to match the standard's purpose**

Organization	Yes or No	Question 4 Comment
		statement. (9) On page 7 in the first paragraph, "industry facility" should be changed to "Facility". **The SDT agrees and adopts your suggestion.**
Response: The SDT thanks you for your comment.		
Seattle City Light		1) Seattle City Light follows MEAG and questions if these administrative activities better should be sent over to NAESB? R1: There is merit in having a plan as identified in R1, but is this a need to support reliability or is it a business practice? Should it be in NAESB's domain? R2, R3 & R4: These are not appropriate for a Standard. If you don't annually review the plan, will reliability be reduced and the BES be subject to instability, separation and cascading? If DOE needs a form filled out, fill it out and send it to DOE. NERC doesn't need to pile on. Mike Moon and Jim Merlo have been stressing results and risk based, actual performance based, event analysis, lessons learned and situational awareness. EOP-004 is primarily a business preparedness topic and identifies administrative procedures that belong in the NAESB domain. **The SDT believes this standard is needed to provide Situational Awareness and can help in providing lessons learned to the industry. The SDT has revised the requirements to address this need. While it may be appropriate to have NAESB to adopt this obligation at some in the future, the SDT was charged with addressing deficiencies at this time. The SDT has removed all references to filing reports to DOE from the earlier versions. Today's only reference provides for NERC's acceptance of the use of their form when it is appropriate.** 2) Seattle City Light finds that even though efforts were made to differentiate between sabotage vs. criminal damage, the difference still appears to be confusing. Sabotage clearly requires FBI notification, but criminal damage (i.e. copper theft, trespassing, equipment theft) is best handled by local law agencies. A key point on how to determine the difference is to always go with the evidence. If you have a hole in the fence and cut grounding wires, this would only require local law enforcement

Organization	Yes or No	Question 4 Comment
		notification. If there is a deliberate attack on a utility's BES infrastructure for intent of sabotage and or terrorism--this is a FBI notification event. One area where a potential for confusion arises is with the term "intentional human action" in defining damage. Shooting insulators on a rural transmission tower is not generally sabotage, but removing bolts from the tower may well be. Seattle understands the difficulty in differentiating these two cases, for example, and supports the proposed Standard, but would encourage additional clarification in this one area. **The SDT appreciates the concern you raise. The SDT decided early that trying to set a definition for sabotage across the continent would be impossible as there are many differing viewpoints; particularly within the law enforcement agencies. There was consensus that even if we were able to set a definition, it may be consistent or recognized by other agencies. Therefore, the SDT decided to set event types that warranted reporting. Entities best know who they have to report to and under what considerations those reports need to be submitted. This is basis for this standard. The SDT wanted to provide entities with the result that was necessary but not prescribe how to do it. This concept has been embraced throughout this project. We believe that entities can create a single or multiple contact lists that have the right people being notified when an event type occurs. The SDT has revised the language on "intentional human action" in Attachment 1 in an attempt to provide you the clarification you requested.**
Response: Thank you for your comment.		
Essential Power, LLC		1. As this Standard does not deal with real-time reporting or analysis, and is simply considered an after the fact reporting process, I question the need for the Standard at all. This is a process that could be handled through a change to the Rules of Procedure rather than through a Standard. Developing this process as a Reliability Standard is, in my opinion, contrary to the shift toward Reliability-Based Standards Development.2. I do not believe that establishing a reporting requirement improves the reliability of the BES, as stated in the purpose statement. The reporting requirement, however, would improve situational awareness. I recommend the

Organization	Yes or No	Question 4 Comment
		purpose statement be changed to reflect this, and included with the process in the NERC Rules of Procedure.
Response: The SDT thanks you for your comment. The SDT believes this standard is needed to provide Situational Awareness and can help in providing lessons learned to the industry. The SDT has revised the requirements to address this need. The vast majority of commenters support the Purpose statement as written.		
Georgia System Operations Corporation		a) Reporting most of these items ... o Does not "provide for reliable operation of the BES" o Does not include "requirements for the operation of existing BES facilities" o Is not necessary to "provide for reliable operation of the BES"... and is therefore not in accordance with the statutory and regulatory definitions of a Reliability Standard. They should not be in a Reliability Standard. Most of this is an administrative activity to provide information for NERC to perform some mandated analysis. **The SDT believes this standard is needed to provide Situational Awareness and can help in providing lessons learned to the industry. The SDT has revised the requirements to address this need.** b) A reportable Cyber Security Incident: Delete this item from the table. It is covered in another standard and does not need to be duplicated in another standard. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement.** c) Damage or destruction of a Facility: Entities MAY only need to slightly modify their existing CIP-001 Sabotage Reporting procedures from a compliance perspective of HAVING an Operating Plan but not from a perspective of complying with the Plan. A change from an entity reporting "sabotage" on "its" facilities (especially when the common understanding of CIP-001 is to report sabotage on facilities as "one might consider facilities in everyday discussions") to reporting "damage on its Facilities" (as defined in the Glossary) is a significant change. An operator does not know off the top of his head the definition of Facility or Element. He will not know for any particular electrical device whether or not reporting is required. Although the term is

Organization	Yes or No	Question 4 Comment
		useful for legal and regulatory needs, it is problematic for practical operational needs. This creates the need for a big change in guidance, training, and tools for an operator to know which pieces of equipment this applies to. There is the need to translate from NERC-ese to Operator-ese. Much more time is needed to implement. The third threshold ("Results from actual or suspected intentional human action") perpetuates the problem of knowing the human's intention. Also, what if the action was intended but the result was not intended? The third threshold is ambiguous and subject to interpretation. The original intent of this project was to get away from the problem of the term sabotage due to its ambiguity and subjectivity. This latest change reverses all of the work so far toward that original goal. Instead of the drafted language, change this item to reporting "Damage or destruction of a Facility and any involved human action" and use only the first two threshold criteria. **The SDT has stated in our "Consideration of Issues and Directives – March 15, 2012" that was posted with the last posting stated:** **The SDT has not proposed a definition for inclusion in the NERC Glossary because it is impractical to define every event that should be reported without listing them in the definition. Attachment 1 is the de facto definition of "event." The SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that without the intervention of law enforcement after the fact, it was almost impossible to determine if an act or event was that of sabotage or merely vandalism. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.** **The SDT has discussed this with FERC Staff and we agree that sabotage could be a**

Organization	Yes or No	Question 4 Comment
		state of mind and therefore the real issue was there an event or not. **The SDT also uses the NERC defined term of "Facility: A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)."** d) Any physical threat that could impact the operability of a Facility: See comment above about the term "Facility" and the need for a much longer implementation time. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to**

Organization	Yes or No	Question 4 Comment
		operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility. e) Transmission loss: This item is very unclear. What is meant by "loss?" Above, it says to report damage or destruction of a Facility. This says to report the loss of 3 Facilities. Is the intent here to report when there are 3 or more Facilities that are unintentionally and concurrently out of service for longer than a certain threshold of time? The intent should not be to include equipment failure? Three is very arbitrary. An entity with a very large footprint with a very large number of electrical devices is highly likely to have 3 out of service at one time. An entity with very few electrical devices is less likely to have 3. Delete the word Transmission. It is somewhat redundant. A Facility is BES Element. I believe all BES Elements are Transmission Facilities. A Facility operates as a single "electrical device." What if more than 3 downstream electrical devices are all concurrently out of service due to the failure of one upstream device? Would that meet the criteria? A situation meeting the criteria will be difficult to detect. Need better operator tools, specific procedures for this, training, and more implementation time. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state"** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** f) The implementation plan says current version stays in effect until accepted by ALL regulatory authorities but it also says that the new version takes effect 12 months after the BOT or the APPLICABLE authorities accept it. It is possible that ONE regulatory authority will not accept it for 13 months and both versions will be in

Organization	Yes or No	Question 4 Comment
		effect. It is also possible for ALL regulatory authorities to accept it at the same time, the current version to no longer be in effect, but the new version will not be in effect for 12 months. **The SDT intends for this standard to not become enforceable until all regulatory authorities have approved it. The SDT will work with NERC and others to ensure a timely enforcement period without overlap.**
Response: Thank you for your comment.		
We Energies		Applicability: Change Electric Reliability Organization to NERC or delete Regional Entity. The ERO is NERC and all the Regional Entities.R1.2: The ERO is NERC and all the REs. If I report to any one on the REs (only and not to NERC), I have reported to the ERO. Change ERO to NERC. M1 refers to R1.1 and R1.2 as Parts. It would be clearer to refer to them as requirements or sub-requirements. **The SDT is limited to listing functional registrations in the Applicability section. The applicable entities are the ERO and Regional Entity, not NERC. The SDT notes that the Applicability section has nothing to do with the reporting obligations. The Applicability section denotes who has obligations within the standard to report. The Applicability section has been revised in accordance with comments received on who needs to report on event types.** M2: Add a comma after "that the event was reported" and "supplemented by operator logs". It will be easier to read. **The SDT has revised the requirement and associated language.** R3: This should be clarified to state that no reporting will be done for the annual test, not just exclude the ERO. **The SDT has revised the requirement.** M4: An annual review will not be time stamped. **The SDT has removed the time-stamp provision.**

Organization	Yes or No	Question 4 Comment
Response: The SDT thanks you for your comment.		
City of Austin dba Austin Energy		Austin Energy makes the following comments: (1) Comment on the Background section titled "A Reporting Process Solution - EOP-004": This section includes the sentence, "Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state OR PROVINCIAL OR LOCAL level law enforcement agency." (emphasis added) The corresponding flowchart includes a step, "Notification Protocol to State Agency Law Enforcement." Austin Energy requests that the SDT update the flowchart to match the language of the associated paragraph and include "state or provincial or local" agencies. **The SDT wishes to point out that the flowchart is an example only – it was not meant to show every permutation. The entity can choose to use the flowchart or develop one for their own use.** (2) Comments on VSLs: Austin Energy recommends that the SDT amend the VSLs for R2 to include the "recognition of" events throughout. That is, update the R2 VSLs to state "... X hours after "recognizing" an event ..." in all locations where the phrase occurs. **The DSR SDT believes the current language is sufficient as Table 1 clearly states that the reporting 'clock' starts after recognition of the event.** (3) Austin Energy has a concern with the inclusion of the word "damage" to the phrase "damage or destruction of a Facility." We agree that any "destruction" of a facility that meets any of the three criteria be a reportable event. However, if the Standard is going to include "damage," some objective definition for "damage" (that sets a floor) ought to be included. Much like the copper theft issue, we do not see the benefit of reporting to NERC vandalism that does not rise to a certain threshold (e.g. someone who takes a pot shot at an insulator) unless the damage has some tangible impact on the reliability of the BES or is an act of an orchestrated sabotage (e.g.

Organization	Yes or No	Question 4 Comment
		removal of a bolt in a transmission structure). **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** **The SDT removed all language under "Entity with Reporting Responsibility," with**

Organization	Yes or No	Question 4 Comment
		the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** (4) Austin Energy voted to approve the revised Standard because it is an improvement over the existing Standard. In light of FERC's comments in Paragraph 81 of the Order approving the Find, Fix, Track and Report initiative, however, Austin Energy would propose that this Standard is the type of Standard that does not truly

Organization	Yes or No	Question 4 Comment
		enhance reliability of the BES and is, instead, an administrative activity. As such, we recommend that NERC consider whether EOP-004-2 ought to be retired. **The SDT appreciates the suggestion; however, we note that a standard cannot be retired prior to its effective and enforcement dates. Further, the SDT has been charged with addressing deficiencies that are present in current standards which the industry has determined to be needed through approval of the SAR. If the P81 process should ultimately decide to retire this standard, then the process will have made that decision. The SDT cannot presume that the P81 effort will become effective.**
Response: The SDT thanks you for your comment.		
Bonneville Power Administration		BPA believes that the VSL should allow for amending the form after a NERC specified time period without penalty and suggests that a window of 48 hours be given to amend the form to make adjustments without needing to file a self report. Should the standard be revised to allow a time period for amending the form without having to file a self report, BPA would change its negative position to affirmative.
Response: The SDT thanks you for your comment. The SDT would like to point that a window is not needed as the standard requires a report at a 24-hour time frame which provides information on what is known at the time. The standard does not require any follow up or update report. If the entity wishes to file a follow up report, it can do so on its own. A self report should only be needed if the 24-hour report was not filed.		
CenterPoint Energy		CenterPoint Energy proposes that the purpose be enhanced to reflect risk and response. For example, the purpose could read "To sustain and improve reliability of the Bulk Electric System by identifying common risks reported by Responsible Entities as a source of lessons learned."In the Background section under Law Enforcement Reporting, "the" should be added in front of "Bulk Electric System". Also under the Background section - "Present expectations of the industry under CIP-001-1a", CenterPoint Energy is not aware of any current annual requirements for CIP-001 and suggests that this section be revised to reflect that fact. CenterPoint Energy strongly

Organization	Yes or No	Question 4 Comment
		believes that the Violation Severity Levels (VSL) should not be high or severe unless an Adverse Reliability Impact occurred. CenterPoint Energy is requesting that Requirement R2 be deleted and the phrase, "as a result of not implementing the plan/insufficient or untimely report, an Adverse Reliability Impact occurred" be added to the Requirement R1 VSL. Regarding the VSL for Requirement R4, the Violation Risk Factor should be "Lower" and read "the entity did not perform the annual test of the operating plan" as annual is to be defined by the entity or according to the CAN-0010.
Response: The SDT thanks you for your comment. The vast majority of commenters support the Purpose statement as written. The missing 'the' has been added to the background section under 'Law Enforcement Reporting.' 'Annual' has been changed to 'These'. VSLs refer to how closely the entity met the requirements of the standard; it is the VRF that measures impact to reliability. The DSR SDT believes use of the high and severe VSLs is appropriate. R4 has been deleted along with its VRF/VSLs.		
Cowlitz County PUD		Cowlitz is pleased with changes made to account for the difficulties small entities have in regard to reporting time frames. Although Cowlitz is confident that the current draft is manageable for small entities, we propose that the resulting reports this Standard will generate will contain many insignificant events from the event types "Damage or destruction of a Facility," and "Any physical threat that could impact the operability of a Facility." In particular, examples would be limited target practice on insulators, car-pole accidents, and accidental contact from tree trimming or construction activities. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area,**

Organization	Yes or No	Question 4 Comment
		Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency." This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human

Organization	Yes or No	Question 4 Comment
		action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** Cowlitz suggests that at least a >= 100 MW (200 MW would be better) and/or >= N-2 impact threshold be established for these event types. Also, Cowlitz suggests the statement "results from actual or suspected intentional human action" be changed to "results from actual or suspected intentional human action to damage or destroy a Facility." A human action may be intentional which can result in damage to a facility, but the intent may have been of good standing, and not directed at the Facility. For example, the intent may have been to legally harvest a tree, or move equipment under a line. Cowlitz believes the above proposed changes would benefit the ERO, both in reduction of nuisance reports and possible violations over minimal to no impact BES events. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and**

Organization	Yes or No	Question 4 Comment
		identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.**
Response: The SDT thanks you for your comment.		
Colorado Springs Utilities		CSU is concerned with the word 'damage'. We support any 'destruction' of a facility that meets any of the three criteria be a reportable issue, but 'damage', if it's going to be included should have some objective definition that sets a baseline.
Response: The SDT thanks you for your comment. The SDT removed all language under "Entity with Reporting Responsibility,"		

Organization	Yes or No	Question 4 Comment
with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: "Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency." This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1)		

Organization	Yes or No	Question 4 Comment
the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.**		
Dominion		Dominion believes that the reporting of "Any physical threat that could impact the operability of a Facility4" may overwhelm the Reliability Coordinator staff with little to no value since the event may have already passed. This specific event uses the phrase "operability of a Facility" yet "operability" is not defined and is therefore ambiguous. We do support the reporting to law enforcement and the ERO but do not generally support reporting events that have passed to the Reliability Coordinator. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility**

Organization	Yes or No	Question 4 Comment
		Do not report copper theft unless it degrades normal operations of a Facility." **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** Attachment 2; section 4 Event Identification and Description: The type of events listed should match the events as they are exactly written in Attachment 1. As it is currently written, it leaves room for ambiguity. **The SDT agrees and has adopted your suggestion.** M3 - Dominion objects to having to provide additional supplemental evidence (i.e. operator logs), and the SDT maybe want to include a requirement for NERC to provide a confirmation that the report has been received. **The SDT believes that you are referring to M2. We have added "which may be" prior to "supplemented by operator logs," indicating that this is optional. The SDT has opted not to develop a requirement for the ERO to provide receipt conformation of a report.**
Response: The SDT thanks you for your comment.		
Entergy		Entergy does not agree with the Time Horizon for R2. The rationale for R2 contains phrases related to situational awareness and keeping people/agencies aware of the "current situation." However, this standard is related to after the fact event reporting, not real-time reporting via RCIS, as discussed on page 6 of the red-lined standard. Therefore the time horizon for R2 should indicate that this is an after the

Organization	Yes or No	Question 4 Comment
		fact requirement expected to be performed either in 1 hour or 24 hours after an event occurs, not in the operations assessment time frame. This change should also be made on page 15 of the redline in the Table of compliance elements for R2. Page 18 of the redline document contains a VSL for R2 which states that it will be considered a violation if the Responsible Entity submitted a report in the appropriate timeframe but failed to provide all of the required information. It has long been the practice to submit an initial report and provide additional information as it becomes available. On page 24 of the redlined document, this is included in the following "...and provide as much information as is available at the time of the notification to the ERO..." But the compliance elements table now imposes that if the entity fails to provide ALL required information at the time the initial report is required, the entity will be non compliant with the standard. This imposes an unreasonable burden to the Reliability Entity. This language should be removed. The compliance element table for R3 and R4 make it a high or severe violation to be late on either the annual test or the annual review of the Operating plan for communication. While Entergy supports that periodically verifying the information in the plan and having a test of the operating plan have value, it does not necessarily impose additional risk to the BES to have a plan that exceeds its testing or review period by two to three months. This is an administrative requirement and the failure to test or review should be a lower or moderate VSL, which would be consistent with the actual risk imposed by a late test or review. On page 24 of the redlined draft, there is a statement that says "In such cases, the affected Responsible Entity shall notify parties per Requirement R1 and provide as much information as if available at the time of the notification..." Since R1 is the requirement to have a plan, and R2 is the requirement to implement the plan for applicable events, it seems that the reference in this section should be to Requirement R2, not Requirement R1.
Response: The SDT thanks you for your comment. There is no longer a requirement for this 'two-step' reporting. The initial report is the only report an entity must make. The note at the top of Attachment 1 is to give entities the flexibility to make a quick 'something big just happened, but I don't know the extent' phone call, but realistically the reporting time frame is 24 hours which should give ample time to make one written report using OE-417 or Attachment 2. You will also notice that the amount of		

Organization	Yes or No	Question 4 Comment
information you must provide is minimal – the idea is that this is a trigger for NERC or the Event Analysis process and they will contact you if further details are required. **VSLs refer to how closely the entity met the requirements of the standard; it is the VRF that measures impact to reliability. The DSRSDT believes use of the high and severe VSLs is appropriate. Also, R4 has been deleted along with its VRF/VSLs.**		
ERCOT		ERCOT has joined the IRC comments on this project and offers these additional comments. ERCOT supports the alternative approach submitted by the IRC. ERCOT requests that time horizons be added for each of the requirements as have been with other recent Reliability Standards projects. With regards to Attachment 1, ERCOT requests the following changes: o Modify "Generation loss" from "â‰¥ 1,000 MW for entities in the ERCOT or Quebec Interconnection" to "â‰¥ 1,100 MW for entities in the ERCOT Interconnection" and "â‰¥ 1,000 MW for entities in the Quebec Interconnection". This is consistent with the DCS threshold and eliminates possible operator confusion since DCSs event are reported in the ERCOT interconnection at 80% of single largest contingency which equates to 1100 MW. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."** **The NERC SPM does allow TRE to apply for a variance if they have special concerns that GOPs should submit a report to the ERO.**

Organization	Yes or No	Question 4 Comment
		o Modify "Transmission loss" from "Unintentional loss of three or more Transmission Facilities (excluding successful automatic reclosing)" to "Inconsequential loss of three or more Transmission Facilities not part of a single rated transmission path (excluding successful automatic reclosing)." If a single line is comprised of 3 or more sections, this should not be part of what is reported here as it is intended to be when you have a single event trip of 3 or more transmission facilities that is not part of its intended design. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** **The NERC SPM does allow TRE to apply for a variance if they have special concerns that GOPs should submit a report to the ERO.** o ERCOT requests review of footnote 1. The footnote does not seem appropriate in including an example of a control center as the definition of a BES facility does not include control centers. **The SDT removed all foot notes within Attachment based on comments received.**
Response: The SDT thanks you for your comment.		
FirstEnergy Corp		FE supports the standard and has the following additional comments and suggestions:1. Guideline/Technical Basis Section - FE requests the SDT add specific guidance for each requirement. Much of the information in this section is either included, or should be included in the Background section of the standard. One example of guidance that would help is for Requirement R3 on how an entity could

Organization	Yes or No	Question 4 Comment
		perform the annual test. The comment form for this posting has the following paragraph on pg. 2 which could be used as guidance for R3: "the annual test will include verification that communication information contained in the Operating Plan is correct. As an example, the annual update of the Operating Plan could include calling "others as defined in the Responsibility Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. Note that there is no requirement to test the reporting of events to the Electric Reliability Organization and the Responsible Entity's Reliability Coordinator."2. With regard to the statement in the comment form (pg 2 paragraph 7)"Note that there is no requirement to test the reporting of events to the Electric Reliability Organization and the Responsible Entity's Reliability Coordinator.", requirement R3 only includes the ERO as an entity and should also include the Reliability Coordinator. 3. The measure M3 says that an entity can use an actual event as a test to meet R3. Does this mean just 1 actual event will meet R3, or is the intent that all possible events per 1.2 are tested? Would like some clarity on this measure.
Response: The SDT thanks you for your comment. The requirements have been revised and these revisions along with the 'Rationale' boxes should provide the clarity you seek.		
Indiana Municipal Power Agency		For 1.2 under R1, is the SDT leaving it up to the registered entities do decide which organizations will be contacted for each event listed in attachment 1 or do all of those organization need to be contacted for each event listed in attachment 1? The requirement needs to clearly communicate this clarification and be independent of the rationale language. Auditors will go by the requirement and not the rationale for the requirement. For 1.1 under R1, does each event need its own process of recognition or can one process be used to cover all the applicable events? The requirement needs to clearly communicate this clarification and be independent of the rationale language. Auditors will go by the requirement and not the rationale for the requirement. For 1.2 under R1, company personnel is used as an example but in the rationale for R1, the third line uses operating personnel. IMPA recommends

Organization	Yes or No	Question 4 Comment
		changing the example in 1.2 to operating personnel which is used in the current version of CIP-001.
Response: The SDT thanks you for your comment. The SDT does not believe that it has the ability (or desire) to programmatically prescribe whether entities have a single or multiple contact lists. Entities themselves know best who and under what conditions do reports need to be provided. Further, the industry in past comment periods, clearly indicated that they did not wish to have the SDT provide the "how."		
GTC		For R2, please clarify how an entity can demonstrate that no reportable events were experienced. GTC recommends an allowance for a letter of attestation within M2.
Response: Thank you for your comment. Registered Entities must determine how to best demonstrate they have met the performance obligation of a requirement. The use of an attestation statement is already permitted and recognized with the NERC Compliance Program if that is the best means of demonstrating your performance under the requirement. Auditors will then assess whether or not an attestation meets the requirement in one's audit. Attestations cannot be specifically permitted for use.		
Orange and Rockland Utilities, Inc.		Form EOP-004, Attachment 2: Event Reporting Form: Delete the Task words "or partial." Delete the Task words "physical threat that could impact the operability of a Facility." Make any changes to the VSL's necessary to align them with the reviewed wording provided above.
Consolidated Edison Co. of NY, Inc.		Form EOP-004, Attachment 2: Event Reporting Form: Delete the Task words "or partial." Delete the Task words "physical threat that could impact the operability of a Facility." Make any changes to the VSL's necessary to align them with the reviewed wording provided above.
Response: The SDT thanks you for your comment. The SDT has updated Attachment 2 to reflect the events listed in Attachment 1.		
NextEra Energy Inc		Given that Responsible Entities are already required by other Reliability Standards to communicate threats to reliability to their Reliability Coordinator (RC), NextEra does not believe that EOP-004-2 is a Reliability Standard that promotes the reliability of the bulk power system, as envisioned by Section 215 of the Federal Power Act.

Organization	Yes or No	Question 4 Comment
		Because an RC reporting requirement is already covered in other Standards, EOP-004-2 essentially is a reporting out requirement to the Regional Reliability Organization (RRO). NextEra does not agree that the reporting of events to the RROs should be subject to fines under the Reliability Standard regulatory framework. The reporting to RROs, as required by EOP-004-2, while informative and helpful for lessons learned, etc., is not necessary to address an immediate threat to reliability. In addition, NextEra does not believe it would be constructive to fine Responsible Entities for failure to report to a RRO within a mandated deadline during times when these entities are attempting to address potential sabotage on their system. NextEra would, therefore, prefer that the EOP-004-2 Standards Drafting Team be disbanded, and instead that EOP-004-2's reporting requirements be folded in to the event analysis reporting requirements. Therefore, NextEra requests that the new Section 812 be revised to include EOP-004-2 as a data request for lessons learn or for informational purposes only, and, also, for EOP-004-2 project to be disbanded.
Response: The SDT thanks you for your comment. While the SDT appreciates your viewpoint, the SDT has been charged with addressing deficiencies identified in current standards. The SDT believes that the standard will provide NERC with the situational awareness it needs as well as providing the industry valuable information through lessons learned.		
Illinois Municipal Electric Agency		Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Response: The SDT thanks you for your comment. Please review the response to that commenter.		
Florida Municipal Power Agency		In R1, bullet, it is a bit ambiguous whether the list of organizations to be communicated with is an exhaustive list (i.e.) or a list of examples (e.g.). The list is preceded by an "i.e." which indicates the former, but includes an "or" which indicates the latter. We are interpreting this as meaning the list is exhaustive as separated by semi-colons, but that the last phrase separated by commas is a list of examples. Is this the correct interpretation? **The SDT has made the required change concerning replacing "i.e." with "e.g."**

Organization	Yes or No	Question 4 Comment
		The Rules of Procedure language for data retention (first paragraph of the Evidence Retention section) should not be included in the standard, but instead referred to within the standard (e.g., "Refer to Rules of Procedure, Appendix 4C: Compliance Monitoring and Enforcement Program, Section 3.1.4.2 for more retention requirements") so that changes to the RoP do not necessitate changes to the standard. **The language that you mention is part of the standard boilerplate and is included in all standards. The SDT has chosen to keep the language as is at this time.**
Response: The SDT thanks you for your comment.		
Ingleside Cogeneration LP		Ingleside Cogeneration LP strongyly believes that LSEs that do not own BES assets should be excluded from the Applicability section of this standard.
Response: The SDT thanks you for your comment. The LSE obligation in this standard was tied to applicability in CIP-008 for cyber incident reporting. Reporting under CIP-008 is no longer part of EOP-004-2 so this applicability has been removed.		
Los Angeles Department of Water and Power		LADWP does not have any other comments at this time
Response: The SDT thanks you for your participation.		
Manitoba Hydro		Manitoba Hydro is voting negative on EOP-004-2 for the reasons identified in our response to Question 1. In addition, Manitoba Hydro has the following comments:(Background section) - The section has inconsistent references to EOP-004 (eg. EOP-004 and EOP-004-2 are used). Wording should be made consistent. (Background section) - The section references entities, and responsible entities. Suggest wording is made consistent and changed to Responsible Entities. (General comment) - References in the standard to 'Part 1.2' should be changed to R1.2 as it is unclear if Part 1.2 refers to, for example, R1.2 or part 1.2 'Evidence Retention'.

Organization	Yes or No	Question 4 Comment
		(M4) -Please clarify what is meant by 'date change page'.
Response: The SDT thanks you for your comment. The SDT appreciates the points you raise and we continually review the document to make sure the language is consistent and unambiguous.		
Southern Company Services		Move the Background Section (pages 4-9) to the Guideline and Technical Basis section. They are not needed in the main body of the standard. **The SDT agrees and adopts your suggestion.** Each "Entity with Reporting Responsibility" in the one-hour reporting table (p. 17) should be explicitly listed in the table, not pointed to another variable location. The criterion for "Threshold for Reporting" in the one-hour reporting table (p. 17) should be explicitly listed in the table, not pointed to another variable location. Please specify the voltage base against which the +/- 10% voltage deviation on a Facility is to be measured in the twenty-four hour reporting table (p. 19). **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes ."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.**
Response: The SDT thanks you for your comment.		
Oncor Electric Delivery		Oncor takes the position that the proposed objectives as prescribed in Project 2009-01 - Disturbance and Sabotage Reporting, is a "good" step forward. Currently, NERC

Organization	Yes or No	Question 4 Comment
		reporting obligations related to disturbances occurs over multiple standards including CIP-001, EOP-004-1, TOP-007-0, CIP-008-3 and Event Analysis (EA). Oncor is especially pleased that the Event Analysis Working Group (EAWG) is actively working to find ways of streamlining the disturbance reporting process especially to agencies outside of NERC such as FERC, and state agencies. Oncor is in agreement that an addition to the NERC Rules of Procedure in section 800 to develop a Reporting Clearinghouse for disturbance events by the establishment of a system to collect report and then forward completed forms to various requesting agencies, is also a very positive step."
Response: The SDT thanks you for your comment. The SDT would like to point out that the EAP is a voluntary program where the entity analyzes an issue or system condition. EOP-004-2 is a Reporting Standard where an entity informs the ERO (and whoever else per Requirement R1) of a current event. This will give other the situational awareness that their system may be degraded. Please refer to the Southwest Outage Report for more situational awareness issues that failed.		
Occidental Power Services, Inc.		OPSI continues to believe that LSEs that do not own BES assets should be excluded from the Applicability section of this standard. It is disingenuous of both the SDT and FERC to promote an argument to support this inclusion such as that stated in Section 459 of Order 693 (and referred to by the SDT in their Consideration of Comments in the last posting). The fact is that no reportable disturbance can be caused by an "attack" on an LSE that does not own BES assets. The SDT has yet to point out such an event.
Response: The SDT thanks you for your comment. The LSE obligation in this standard was tied to applicability in CIP-008 for cyber incident reporting. Reporting under CIP-008 is no longer part of EOP-004-2 so this applicability has been removed. The SDT notes that LSEs will still be subject to reporting under CIP-008 until such time they are removed from that standard.		
New York Power Authority		Please see comments submitted by NPCC Regional Standards Committee (RSC).
Response: The SDT thanks you for your comment. Please review the response to that commenter.		
MRO NSRF		R1 states: "Each Responsible Entity shall have an event reporting Operating Plan that

Organization	Yes or No	Question 4 Comment
		includes:"The definition of Operating Plan is:"A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan." This appears to us to be too prescriptive and could be interpreted to require a series of documents to for reporting issues to NERC. We suggest the following wording: R1. Each Responsible Entity shall have document methodology(ies) or process(es) for: 1.1. Recognizing each of the applicable events listed in EOP-004 Attachment 1.1.2. Reporting each of the applicable events listed in EOP-004 Attachment 1 in accordance with the time framess specified in EOP-004 Attachment 1 to the Electric Reliability Organization. LES Comment: [R1] We are concerned by the significant amount of detail an entity would be required to contain within the Operating Plan as part of Requirement R1. Rather than specifying an entity must have a documented process for recognizing each of the events listed in EOP-004-2 Attachment 1, at a minimum, consider removing the term "process" in R1.1 and replacing with "guideline" to ensure operating personnel are not forced to adhere to a specific sequence of steps and still have the flexibility to exercise their own judgment. Section 5 of the standard (Background) should be moved to the Guideline and Technical Basis document. A background that long does not belong in the standard piece as it detracts from the intent of the standard itself.
Response: The SDT thanks you for your comment. The background and Guidelines and Technical Basis sections have been combined.		
ReliabilityFirst		ReliabilityFirst votes in the Affirmative for this standard because the standard further enhances reliability by clearing up confusion and ambiguity of reporting events which were previously reported under the EOP-004-1 and CIP-001-1 standards. Even though ReliabilityFirst votes in the Affirmative, we offer the following comments for consideration: 1. Requirement R1, Part 1.2a. ReliabilityFirst recommends further prescribing whom the Responsible Entity needs to communicate with. The phrase "...

Organization	Yes or No	Question 4 Comment
		and other organizations needed for the event type…" in Part 1.2 essentially leaves it up to the Responsible Entity to determine (include in their process) whom they should communicate each applicable event to. ReliabilityFirst recommends added a fourth column under Attachment 1, which lists whom the Responsible Entity is required to communicate with, for each applicable event. 2. VSL for Requirement R2a. Requirement R2 requires the Responsible Entity to "implement its event reporting Operating Plan" and does not require the entity to submit a report. For consistency with the requirement, ReliabilityFirst recommends modifying the VSLs to begin with the following type of language: "The Responsible Entity implemented its event reporting Operating Plan more than 24 hours but…" This recommendation is based on the FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement.
Response: The SDT thanks you for your comment. The SDT believes that implementing your Operating Plan means that you report an event. Therefore the VSLs are entirely consistent with the requirement.		
DECo		Requirement R3 for annual test specifically states that ERO is not included during test. Implies that local law enforcement or state law enforcement will be included in test. Hard to coordinate with many Local organizations in our area.
Response: The SDT thanks you for your comment. The SDT has revised the language in Requirement R3 and believes that the changes will address your suggestion.		
Alliant Energy		Section 5 of the standard (Background) should be moved to the Guideline and Technical Basis document. A background that long does not belong in the standard piece as it detracts from the intent of the standard itself.
Response: The SDT thanks you for your comment. The background and Guidelines and Technical Basis sections have been combined.		

Organization	Yes or No	Question 4 Comment
MidAmerican Energy		See the NSRF comments.
Response: The SDT thanks you for your participation. Please review the response to that commenter.		
MEAG Power		Should these administrative activities be sent over to NAESB? R1: There is merit in having a plan as identified in R1, but is this a need to support reliability or is it a business practice? Should it be in NAESB's domain? R2, R3 & R4: These are not appropriate for a Standard. If you don't annually review the plan, will reliability be reduced and the BES be subject to instability, separation and cascading? If DOE needs a form filled out, fill it out and send it to DOE. NERC doesn't need to pile on. Mike Moon and Jim Merlo have been stressing results and risk based, actual performance based, event analysis, lessons learned and situational awareness. EOP-004 is primarily a business preparedness topic and identifies administrative procedures that belong in the NAESB domain.
Public Utility District No. 1 of Snohomish County		SNPD suggest moving these administrative activities to NAESB. R1: There is merit in having a plan as identified in R1, but is this a need to support reliability or is it a business practice? Should it be in NAESB's domain? R2, R3 & R4: These are not appropriate for a Standard. If you don't annually review the plan, will reliability be reduced and the BES be subject to instability, separation and cascading? If DOE needs a form filled out, fill it out and send it to DOE. NERC doesn't need to pile on. Gerry Cauley and Mike Moon have been stressing results and risk based, actual performance based, event analysis, lessons learned and situational awareness. EOP-004 is primarily a business preparedness topic and identifies administrative procedures that belong in the NAESB domain.
Response: The SDT thanks you for your comment. SDT believes this standard is needed to provide Situational Awareness and can help in providing lessons learned to the industry. The SDT has revised the requirements to address this need. While it may be appropriate to have NAESB to adopt this obligation at some in the future, the SDT was charged with addressing deficiencies at this time. The SDT has removed all references to filing reports to DOE from the earlier versions. Today's only reference provides for NERC's acceptance of the use of their form when it is appropriate.		

Organization	Yes or No	Question 4 Comment
Springfield Utility Board		SUB appreciates the opportunity to provide comments. While Staff was concerned with the consolidation of CIP and non-CIP NERC Reliability Standards (as to how they'll be audited), the Project 2009-01 SDT has done an excellent job in providing clarification around identifying and reporting events, particularly related to the varying definitions of "sabotage".
Response: The SDT thanks you for your support.		
Tacoma Power		Tacoma Power disagrees with the requirement to perform annual testing of each communication plan. We do not see any added value in performing annual testing of each communication plan. There are already other Standard requirements to performing routine testing of communications equipment and emergency communications with other agencies. The "proof of compliance" to the Standard should be in the documentation of the reports filed for any qualifying event, within the specified timelines and logs or phone records that it was communicated per each specified communication plan. Tacoma Power has none at this time. Thank you for considering our comments.
Response: The SDT thanks you for your comment. The SDT has revised Requirement R3 and we believe that our changes address your suggestion.		
Exelon Corporation and its affiliates		Thanks to the SDT. Significant progress was made in revising the proposed standard language. We appreciate the effort and have only a few remaining requests: o We understand that CIP-008 dictates the 1-hour reporting obligation for Cyber Security Incidents and this iteration of EOP-004 delineates the CIP-008 requirements. Please confirm that per the exemption language in the CIP standards (as consistent with the March 10, 2011 FERC Order (docket # RM06-22-014) nuclear generating units are not subject to this reporting requirement. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008. The next version of EOP-004-2**

Organization	Yes or No	Question 4 Comment
		will not contain a one-hour reporting requirement. o EOP-004 still lists "Generation Loss" as a 24 hour reporting criteria without any time threshold guidance for the generation loss. Exelon previously commented to the SDT (without the comment being addressed) that Generation Loss should provide some type of time threshold. If the 2000 MW is from a combination of units in a single location, what is the time threshold for the combined unit loss? In considering clarification language, the SDT should review the BAL standards on the disturbance recovery period for appropriate timing for closeness of trips. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."** o The "physical threat that could impact" requirement remains vague and it's not clear the relevance of such information to NERC or the Regions. If a train derailment occurred near a generation facility (as stated in the footnote), are we to expect that NERC is going to send out a lesson learned with suggested corrective actions to protect generators from that occurring? The value in that event reporting criteria seems low. The requirement should be removed. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated**

Organization	Yes or No	Question 4 Comment
		based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** o The event concerning voltage deviation of +/- 10% does not specify which type of voltage. In response to this comment in the previous comment period, the SDT indicated that the entity could determine the type of voltage. It would be clearer to specify in the standard and avoid future interpretation at the audit level. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:**

Organization	Yes or No	Question 4 Comment
		"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes ." **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.** o As requested previously, for nuclear facilities, EOP-004 reporting should be coordinated with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security or cyber event. Please contact the NRC about this project to ensure that required communication and reporting in response to a radiological sabotage event (as defined by the NRC) or any incident that has impacted or has the potential to impact the BES does not create duplicate reporting, conflicting reporting thresholds or confusion on the part of the nuclear generator operator. Each nuclear generating site licensee must have an NRC approved Security Plan that outlines applicable notifications to the FBI. Depending on the severity of the security event, the nuclear licensee may initiate the Emergency Plan (E-Plan). Exelon again asks that the proposed reporting process and flow chart be coordinated with the NRC to ensure it does not conflict with existing expected NRC requirements and protocol associated with site specific Emergency and Security Plans. In the alternative, the EOP-004 language should include acceptance of NRC required reporting to meet the EOP-004 requirements. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Complete loss of off-site power affecting a nuclear generating station per the Nuclear Plant Interface Requirement."** **As stated in this event Threshold, the TOP's NIPR may have additional guidance concerning the complete loss of offsite power affecting a nuclear plant.**

Organization	Yes or No	Question 4 Comment
		o The proposed standard notes that the text boxes will be moved to the Guideline and Technical Basis Section which we support. However, it's not clear whether all the information in the background section will remain part of the standard. If this section is to remain as proposed concerted revision is needed to ensure that the discussion language matches the requirement language. At present, it does not. For instance, the flow chart on page 9 indicates when to report to law enforcement while the requirements merely state that communications to law enforcement be addressed within the operating plan. **The background sections will remain in the standard. The flowchart on Page 9 is an example only and may differ from your Operating Plan.** o Exelon voted negative vote on this ballot due to the need for further clarification and reconciliation between NERC EOP-004 and the NRC. **The SDT team does not believe that reporting under EOP-004 can in anyway 'conflicts' with any other reporting obligations that nuclear or any other type of GO/GOP may have. By allowing applicable entities to use the OE-417 form, the drafting team believes it has given industry reasonable accommodation to reduce duplicative reporting. The same is true for other agencies as well. If an entity submits to NERC the same that was submitted to the other regulatory agency, then this submission will be acceptable. Based on the historical frequency with which GO/GOPs report under the current EOP-004-1 the drafting team does not believe this places and inordinate burden on the applicable entities.**
Response: The SDT thanks you for your comment.		
Alberta Electric System Operator		The Alberta Electric System Operator will need to modify parts of this standard to fit the provincial model and current legislation when it develops the Alberta Reliability Standard.
Response: The SDT thanks you for your comment.		

Organization	Yes or No	Question 4 Comment
Puget Sound Energy, Inc.		The effective date language in the Implementation Plan is inconsistent with the effective date language in the proposed standard. **The SDT checked the language and found both to be identical.** In addition, the statement of effective date in the Implementation Plan is ambiguous - will EOP-004-2 be effective in accordance with the first paragraph or when it is "assigned an effective date" as stated in the second paragraph? **The second paragraph deals with EOP-004-1, the currently mandatory and enforceable standard.** All requirements should be assigned a Lower Violation Risk Factor. Medium risk factors require direct impact on the Bulk Electric System and the language there regarding "instability, separation, or cascading failures" is present to distinguish the Medium risk factor from the High risk factor. Since all of the requirements address after-the-fact reporting, there can be no direct impact on the Bulk Electric System. In addition, if having an Operating Plan under Requirement R1 is a Lower risk factor, then it does not make sense that reviewing that Operating Plan annually under Requirement R4 has a higher risk factor. **The SDT disagrees. Please review the VRF documentation that was posted with the standard for the analysis of the requirements.** The shift away from "the distracting element of motivation", i.e., removing "Sabotage" from the equation, runs the risk of focusing solely on what happened, how to fix it, and waiting for the next event to occur. That speaks to a reactive approach rather than a proactive one. There is a concern with the removal of the FBI from the reporting mix. Basically, the new standard will involve reporting a suspicious event or attack to local law enforcement and leaving it up to them to decide on reporting to the FBI. Depending on their evaluation, an event which is significant for a responsible entity might not rise to the priority level of the local law enforcement agency for them to report it to the FBI. While this might reduce the reporting requirements a bit, it might do so to the responsible entity's detriment.

Organization	Yes or No	Question 4 Comment
		The Operating Plan developed by each responsible entity may indeed have certain event types reported directly to the FBI. It is up the entity to determine the appropriate notifications. Entities in Canada would not report anything to the FBI. In Attachment 2 - item 4, would it be possible for the boxes be either alpha-sorted or sorted by priority? **The SDT has made changes to Attachment 2 to list the Events in order of their listing in Attachment 1.** There is a disconnect between footnote 1 on page 18 (Don't report copper theft) and the Guideline section, which suggests reporting forced intrusion attempt at a substation. **Forced Intrusion was removed from the Guidelines section. The SDT has deleted footnote 1 based on comments received from the industry, however, retained the concept in the event type "Physical threats to a Facility" as:** **"Do not report copper theft unless it degrades normal operation of a Facility."** Also, in the section discussing the removal of sabotage, the Guideline mentions certain types of events that should be reported to NERC, DHS, FBI, etc., while that specificity with respect to entities has been removed from the reporting requirement. **The SDT disagrees with your assessment on reporting. Entities know best to whom and what reporting obligations they have on the applicable event types. The SDT has learned that states vary in organization of their law enforcement agencies. As such it is impossible for the SDT to outline those obligations in a consistent and uniform manner. Entities can establish a single or multiple contact lists as needed for the different event types.**
Response: The SDT thanks you for your comments.		
Kansas City Power & Light		The flowchart states, "Notification Protocol to State Agency Law Enforcement".

Organization	Yes or No	Question 4 Comment
		Please correct this to, "Notification to State, Provincial, or Local Law Enforcement", to be consistent with the language in the background section part, "A Reporting Process Solution - EOP-004". Evidence Retention - it is not clear what the phrase "prior 3 calendar years" represents in the third paragraph of this section regarding data retention for requirements and measures for R2, R3, R4 and M2, M3, M4 respectively. Please clarify what this means. Is that different than the meaning of "since the last audit for 3 calendar years" for R1 and M1?
Response: The SDT thanks you for your comment. The flowchart is an example only and was not meant to show every permutation. The evidence retention paragraph has been revised to reflect the 'since last audit' language.		
United Illuminating Company		The measures M3 and M4 require evidence to be dated and time stamped. The time stamp is excessive and provides no benefit. A dated document is sufficient. The measure M2 requires in addition to a record of the transmittal of the EOP-004 Attachment 2 form or DOE-417 form that an operator log or other operating documentation is provided. It is unclear why this supplemental evidence of operator logs is required. We are assuming that the additional operator logs or documentation is required to demonstrate that the communication was completed to organizations other than NERC and DOE of the event. If true then the measure should be clear on this topic. For communication to NERC and DOE use the EOP-004 Form or OE-417 form and retain the transmittal record. For communication to other organizations pursuant to R1 Part 1.2 evidence may include but not limited to, operator logs, transmittal record, attestations, or voice recordings.
Response: The SDT thanks you for your comment. The SDT has removed the time-stamp provision. The SDT agrees and adopts your suggestion.		
New York Independent System Operator		The NYISO is part of and supports comments submitted by NPCC Reliability Standards Committee and the IRC Standards Review Committee. However the NYISO would also like to comment on the following items: o NERC has been proposing the future

Organization	Yes or No	Question 4 Comment
		development of performance based standards, which is directly related to reliability performance. Requirement 2 of this standard is simply a reporting requirement. We believe that this does not fall into a category of a performance based standard. NERC has the ability to ask for reports on events through ROP provisions and now the new Event Analysis Process. It does not have to make it part of the compliance program. Some have indicated that need for timely reporting of cyber or sabotage events. The counter argument is that the requirement is reporting when confirmed which would delay any useful information to fend off a simultaneous threat. Also NERC has not provided any records of how previous timely (1 hour) reporting has mitigated reliability risks. o The NERC Event Analysis Process was recently approved by the NERC OC and is in place. This was the model program for reporting outside the compliance program that the industry was asking for. This should replace the need for EOP-004.o NERC has presented Risk Based Compliance Monitoring (RBCM) to the CCC, MRC, BOT and at Workshops. This involves audit teams monitoring an entities controls to ensure they have things in place to maintain compliance with reliability rules. The proposed EOP-004 has created requirements that are controls to requirement R2, which is to file a report on predefined incidents. The RBCM is being presented as the auditor will make determinations on the detail of the sampling for compliance based on the assessment of controls an entity has in place to maintain compliance. It is also noted that compliance will not be assessed against these controls. As the APS example for COM-002 is presented in the Workshop slides, the issue is that EOP-004 R1, R3 and R4 are controls for reporting; 1) have a plan, 2) test the plan, and 3) review the plan. While R2 is the only actionable requirement. The NYISO believes that all reporting requirements have been met by OE-417 and EAP reporting requirements and that EOP-004 has served its time. At a minimum, the NYISO would suggest that EOP-004 be simplified to just R2 (reporting requirement) and the other requirements be placed at the end of the RSAW to demonstrate a culture of compliance as presented by NERC.
Response: The SDT thanks you for your comment. Please review the responses to those commenters. The SDT appreciates your suggestion, however, most of your comment is beyond the scope of the SDT's charge. The SDT would like to note your statement		

Organization	Yes or No	Question 4 Comment
on reporting requirements having been met by the OE-417 and EAP requirements. The SDT fails to see how NERC gains situational awareness and the opportunity to pass along lessons learned when the aforementioned reports are not forwarded to the appropriate ERO group. The SDT would also note that the ERO does not have access to the OE-417 filings unless they are provided and the EAP does not include reporting for some of the event types listed in Attachment 1. The SDT will forward your comment to appropriate officials for their consideration.		
Hydro One		The proposed standard is not consistent with NERC's new Risk Based Compliance Monitoring. - The performance based action to "implement its event reporting Operating Plan" on defined events, as required in R2, could be considered a valid requirement. However, the concern is that this requirement could be superseded by the NERC Events Analysis Process and existing OE-417 Reporting.- The requirements laid out in R1, R3 and R4 are specific controls to ensure that the proposed requirement to report (R2) is carried out. However, controls should not be part of a compliance requirement. The only requirement proposed in this standard that is not a control is R2.NERC does not need to duplicate the enforcement of reporting already imposed by the DOE. DOE-417 is a well-established process that has regulatory obligations. NERC enforcement of reporting is redundant. NERC has the ability to request copies of these reports without making them part of the Reliability Rules. **The SDT appreciates your suggestion, however, most of your comment is beyond the scope of the SDT's charge. The SDT would like to note your statement on reporting requirements having been met by the OE-417 and EAP requirements. This statement is not true for Canadian entities. The SDT fails to see how NERC gains situational awareness and the opportunity to pass along lessons learned when the aforementioned reports are not forwarded to the appropriate ERO group. The SDT would also note that the ERO does not have access to the OE-417 filings unless they are provided and the EAP does not include reporting for some of the event types listed in Attachment 1. The SDT will forward your comment to appropriate officials for their consideration.** Form EOP-004, Attachment 2: Event Reporting Form: - Delete from the Task column

Organization	Yes or No	Question 4 Comment
		the words "or partial".- Delete from the Task column the words "physical threat that could impact the operability of a Facility". **The SDT has proposed changes to the language within Attachment 2 which we believe corrects the point made.** VSL's may have to be revised to reflect revised wording. The standard as proposed is not supportive of Gerry Cauley's performance based standard initiative **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.**

Organization	Yes or No	Question 4 Comment
Response: The SDT thanks you for your comment.		
Northeast Power Coordinating Council		The proposed standard is not consistent with NERC's new Risk Based Compliance Monitoring. a. The performance based action to "implement its event reporting Operating Plan" on defined events, as required in R2, could be considered a valid requirement. However, the concern is that this requirement could be superseded by the NERC Events Analysis Process and existing OE-417 Reporting. b. The requirements laid out in R1, R3 and R4 are specific controls to ensure that the proposed requirement to report (R2) is carried out. However, controls should not be part of a compliance requirement. The only requirement proposed in this standard that is not a control is R2.NERC does not need to duplicate the enforcement of reporting already imposed by the DOE. DOE-417 is a well established process that has regulatory obligations. NERC enforcement of reporting is redundant. NERC has the ability to request copies of these reports without making them part of the Reliability Rules. **The SDT appreciates your suggestion however; most of your comment is beyond the scope of the SDT's charge. The SDT would like to note your statement on reporting requirements having been met by the OE-417 and EAP requirements. This statement is not true for Canadian entities. The SDT fails to see how NERC gains situational awareness and the opportunity to pass along lessons learned when the aforementioned reports are not forwarded to the appropriate ERO group. The SDT would also note that the ERO does not have access to the OE-417 filings unless they are provided and the EAP does not include reporting for some of the event types listed in Attachment 1. The SDT will forward your comment to appropriate officials for their consideration.** Form EOP-004, Attachment 2: Event Reporting Form: Delete from the Task column the words "or partial". Delete from the Task column the words "physical threat that

Organization	Yes or No	Question 4 Comment
		could impact the operability of a Facility". **The SDT has proposed changes to the language within Attachment 2 which we believe corrects the point made.** VSL's may have to be revised to reflect revised wording. **The SDT agrees and adopts your suggestion.**
Response: The SDT thanks you for your comment.		
American Public Power Association		The SDT needs to provide some relief for the small entities in regards to the VSL in the compliance section. APPA believes there should be no High or Severe VSLs for this standard. This is a reporting/documentation standard and does not affect BES reliability at all. It is APPA's opinion that this standard should be removed from the mandatory and enforceable NERC Reliability Standards and turned over to a working group within the NERC technical committees. Timely reporting of this outage data is already mandatory under Section 13(b) of the Federal Energy Administration Act of 1974. There are already civil and criminal penalties for violation of that Act. This standard is a duplicative mandatory reporting requirement with multiple monetary penalties for US registered entities. If this standard is approved, NERC must address this duplication in their filing with FERC. This duplicative reporting and the differences in requirements between DOE-OE-417 and NERC EOP-004-2 require an analysis by FERC of the small entity impact as required by the Regulatory Flexibility of Act of 1980
Response: The SDT thanks you for your comment. VSLs refer to how closely the entity met the requirements of the standard; it is the VRF that measures impact to reliability. The SDT believes use of the high and severe VSLs is appropriate. The SDT believes that size is not the important criteria in determining an impact on reliability. The reporting thresholds are based on the BES. No entity, including small entities is required to report on equipment that is not categorized as BES, which should give small entities relief from reporting on non-impactive assets.		
Pepco Holdings Inc		The SDT's efforts have resulted in a very good draft.

Organization	Yes or No	Question 4 Comment
Response: The SDT thanks you for your support.		
ISO/RTO Standards Review Committee		The SRC offers some other comments regarding the posted draft requirements; however, by so doing, the SRC does not indicate support of the proposed requirements. Following these comments, please see below for an SRC proposed alternative approach: The SRC does not agree with the MEDIUM VRF assigned to Requirement R4. R4 is a requirement to conduct an annual review of the Event Reporting Operating Plan mandated in Requirement R1. R1 however is assigned a VRF of LOWER. We are unable to rationalize why a subsequent review of a plan should have a higher reliability risk impact than the development of the plan itself. Hypothetically, if an entity doesn't develop a plan to begin with, then it will be assigned a LOWER VRF, and the entity will have no plan to review annually and hence it will not be deemed non-compliant with requirement R4. The entity can avoid being assessed violating a requirement with a MEDIUM VRF by not having the plan to begin with, for which the entity will be assessed violating a requirement with a LOWER VRF. We suggest changing the R4 VRF to LOWER. **The SDT has revised the requirements and R4 has been deleted along with its VRF/VSL.** The SRC requests that the SDT post the following Alternative Proposal for Industry comments as required by the Standards Process to obtain Industry consensus and as permitted by FERC: An equally effective alternative is to withdraw this standard and to make the contents of the SDT's posted standard a NERC Guideline. a. This alternative is more in line with new NERC and FERC proposals b. This alternative retains the reporting format Comments 1. The FERC Order 693 directives regarding "sabotage" have already been addressed by the SDT (i.e. the concept was found outside the scope of NERC standards) 2. Current Industry actions already address the needs cited in the Order:

Organization	Yes or No	Question 4 Comment
		a. Approved Reporting Processes already exists i. The Operating Committee's Event Analysis Process ii. Alert Reporting b. The Data already exists i. Reliability Coordinators Information System (which creates hundred if not thousands of "reports" per year) ii. The DOE's OE 417 Report itself provides part of the FERC discussed data 3. The proposed standard is not supportive of Gerry Cauley's performance based standard initiative or of FERC's offer to reduce procedural standards a. The proposed requirement is a process not an outcome i. The proposal is more focused on reporting and could divert the attention of reliability entities from addressing a situation to collecting data for a report b. The proposed "events" are subjective and if followed will create an unmanageable burden on NERC staff i. Reporting "damage" to facilities can be interpreted as anything from a dent in a generator to the total destruction of a transformer ii. The reporting requirements on all applicable entities will create more questions about differences between the reports of the various entities - rather than leading to conclusions about patterns among events that indicate a global threat iii. Reporting any "physical threat" is too vague and subjective iv. Reporting "damage to a facility that affects an IROL" is subjective and can be seen to require reporting of damage on every facility in an interconnected area. v. Reporting "Partial loss of monitoring" is a data quality issue that can be anything from the loss of a single data point to the loss of an entire SCADA system vi. Testing the filling out of a Report does not make it easier to fill out the report later (moreover the reporting is already done often enough -see 2.b.i)c. The proposed requirements will create a disincentive to improving current Reporting practices (the more an entity designs into its own system the more it will be expected to do and the more likely it will be penalized for failing to comply)i. Annual reviews of the reporting practices fall into the same category, why have a detailed process to review when a simple one will suffice?

Organization	Yes or No	Question 4 Comment
		4. The proposed standard does not provide a feedback loop to either the data suppliers or to potentially impacted functional entities a. If the "wide area" data analysis indicates a threat, there is no requirement to inform the impacted entities b. As a BES reliability issue there is no performance indicators or metrics to show the value of this standard i. The SRC recognizes that specific incidents cannot be identified but if this is to be a reliability standard some information must be provided. A Guideline could be designed to address this concern. 5. The proposed standard is not consistent with NERC's new Risk Based Compliance Monitoring. a. The performance based action to report on defined events, as required in R2, could be considered a valid requirement. However we have concerns as noted in Bullet 3 above. The requirements laid out in R1, R3 and R4 are specific controls to ensure that the proposed requirement to report (R2) is carried out. NERC is moving in the direction to assess entities' controls, outside of the compliance enforcement arm. The industry is being informed that NERC Audit staff will conduct compliance audits based on the controls that the entity has implemented to ensure compliance. The SRC is interested in supporting this effort and making it successful. However, if this is the direction NERC is moving, we should not be making controls part of a compliance requirement. The only requirement proposed in this standard that is not a control is R2. 6. For FERC-jurisdictional entities, NERC does not need to duplicate the enforcement of reporting already imposed by the DOE. DOE-417 is a well established process that has regulatory obligations. NERC enforcement of reporting would be redundant. NERC has the ability to request copies of these reports without making them part of the Reliability Rules.
Response: The SDT thanks you for your comment. The SDT will bring this request to the attention of the SC for consideration as this request is beyond the scope of work identified in this project.		
LG&E and KU Services		The Violation Severity Level for Requirement R2 should be revised to read "...hours

Organization	Yes or No	Question 4 Comment
		after recognizing an event requiring reporting..." This will make the language in the VSL consistent with the language in Attachment 1.
Response: The SDT thanks you for your comment. The VSLs have been reviewed and revised based upon the revisions to the requirements.		
SPP Standards Review Group		The VRF for R1 is Lower which is fine. The issue is that R4, which is the review of the plan contained in R1, has a Medium VRF. We recommend moving the VRF of R4 to Lower.We recommend deleting the phrase '...supplemented by operator logs or other operating documentation...' as found in the first sentence of M2. A much clearer reference is made to operator logs and other operating documentation in the second sentence. The duplication is unnecessary.What will happen with the accompanying information contained in the Background section in the draft standard? Will it be moved to the Guideline and Technical Basis at the end of the standard as the information contained in the text boxes? This is valuable information and should not be lost.
Response: The SDT thanks you for your comment. The SDT has revised the requirements and R4 has been deleted along with its VRF/VSL. The background has been moved to the Guidelines and Technical Basis section.		
Utility Services		There are no other comments at this time.
Response: The SDT thanks you for your participation.		
Dynegy Inc.		Use of the term "Part x.x" throughout the Standard is somewhat confusing. I can't recall other Standards using that type of term. Suggest using the term "Requirement" instead.
Response: The SDT thanks you for your comment. The standard has been rewritten and revised in accordance with your suggestion.		
Central Lincoln		We agree with the comments provided by both PNGC and APPA.

Organization	Yes or No	Question 4 Comment
Response: The SDT thanks you for your comment. Please review the responses to those commenters.		
PNGC Comment Group		We appreciate the hard work of the SDT.
Response: The SDT thanks you for your support.		
PPL Corporation NERC Registered Affiliates		We appreciate the inclusion of the Process Flowchart on Page 9 of the draft standard. We submit for your consideration, removing the line from the NO decision box to the 'Report Event to ERO, Reliability Coordinator' box. It seems if the event does not need reporting per the decision box, this line is not needed.The decision box on 'Report to Law Enforcement ?' does not have a Yes or No. Perhaps, this decision box is misplaced, or is it intended to occur always and not have a different path with different actions? Ie. should it be a process box? Thank you for your work on this standard.
PPL Electric Utilities		We appreciate the inclusion of the Process Flowchart on Page 9 of the draft standard. We submit for your consideration, removing the line from the NO decision box to the 'Report Event to ERO, Reliability Coordinator' box. It seems if the event does not need reporting per the decision box, this line is not needed.For clarity in needed actions, please consider using a decision box following flowcharting standards such as, a decision box containing a question with a Yes and a No path. The decision box on 'Report to Law Enforcement ?' does not have a Yes or No. Perhaps, this decision box is misplaced, or is it intended to occur always and not have a different path with different actions? Ie. should it be a process box?Thank you for your work on this standard.
Response: The SDT thanks you for your comment. The flowchart was provided as an example and guidance for entities to use if they so choose. Entities can elect to create their own flowchart based upon their needs.		
Independent Electricity System Operator		We do not agree with the MEDIUM VRF assigned to Requirement R4. Re stipulates a requirement to conduct an annual review of the event reporting Operating Plan in

Organization	Yes or No	Question 4 Comment
		Requirement R1, which itself is assigned a VRF of LOWER. We are unable to rationalize why a subsequent review of a plan should have a higher reliability risk impact than the development of the plan itself. Hypothetically, if an entity doesn't develop a plan to begin with, then it will be assigned a LOWER VRF, and the entity will have no plan to review annually and hence it will not be deemed non-compliant with requirement R4. The entity can avoid being assessed violating a requirement with a MEDIUM VRF by not having the plan to begin with, for which the entity will be assessed violating a requirement with a LOWER VRF. We suggest changing the R4 VRF to LOWER.
Response: The SDT thanks you for your comment. The SDT has revised the requirements and R4 has been deleted along with its VRF/VSL.		
SMUD & BANC		We feel issues were addressed, but still have concern with 'damage'. We certainly support that any 'destruction' of a facility that meets any of the three criteria be a reportable issue. But 'damage', if it's going to be included should have some objective definition that sets a floor. Much like the copper theft issue, we don't see the benefit of reporting plain vandalism (gun-shot insulators results from actual or suspected intentional human action) to NERC unless the 'damage' has some tangible impact on the reliability of the system or are acts of an orchestrated sabotage (i.e. removal of bolt in a transmission structure).
Response: The SDT thanks you for comment. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:		

Organization	Yes or No	Question 4 Comment
		"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency." **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state;** **Damage or destruction of its Facility that results from actual or suspected intentional human action.** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.**
ISO New England Inc		We requests that the SDT post the following Alternative Proposal for Industry

Organization	Yes or No	Question 4 Comment
		comments as required by the Standards Process to obtain Industry consensus and as permitted by FERC: An equally effective alternative is to withdraw this standard and to make the contents of the SDT's posted standard a NERC Guideline.a. This alternative is more in line with new NERC and FERC proposalsb. This alternative retains the reporting formatComments1. The FERC Order 693 directives regarding "sabotage" have already been addressed by the SDT (i.e. the concept was found outside the scope of NERC standards)2. Current Industry actions already address the needs cited in the Order:a. Approved Reporting Processes already existsi. The Operating Committee's Event Analysis Processii. Alert Reporting b. The Data already existsi. Reliability Coordinators Information System (which creates hundred if not thousands of "reports" per year)ii. The DOE's OE 417 Report itself provides part of the FERC discussed data3. The proposed standard is not supportive of Gerry Cauley's performance based standard initiative or of FERC's offer to reduce procedural standardsa. The proposed requirement is a process not an outcomei. The proposal is more focused on reporting and could divert the attention of reliability entities from addressing a situation to collecting data for a reportb. The proposed "events" are subjective and if followed will create an unmanageable burden on NERC staffi. Reporting "damage" to facilities can be interpreted as anything from a dent in a generator to the total destruction of a transformerii. The reporting requirements on all applicable entities will create more questions about differences between the reports of the various entities - rather than leading to conclusions about patterns among events that indicate a global threatiii. Reporting any "physical threat" is too vague and subjective iv. Reporting "damage to a facility that affects an IROL" is subjective and can be seen to require reporting of damage on every facility in an interconnected area. v. Reporting "Partial loss of monitoring" is a data quality issue that can be anything from the loss of a single data point to the loss of an entire SCADA system vi. Testing the filling out of a Report does not make it easier to fill out the report later (moreover the reporting is already done often enough -see 2.b.i)c. The proposed requirements will create a disincentive to improving current Reporting practices (the

Organization	Yes or No	Question 4 Comment
		more an entity designs into its own system the more it will be expected to do and the more likely it will be penalized for failing to comply)i. Annual reviews of the reporting practices fall into the same category, why have a detailed process to review when a simple one will suffice?4. The proposed standard does not provide a feedback loop to either the data suppliers or to potentially impacted functional entitiesa. If the "wide area" data analysis indicates a threat, there is no requirement to inform the impacted entitiesb. As a BES reliability issue there is no performance indicators or metrics to show the value of this standardi. We recognize that specific incidents cannot be identified but if this is to be a reliability standard some information must be provided. A Guideline could be designed to address this concern. 5. The proposed standard is not consistent with NERC's new Risk Based Compliance Monitoring. a. The performance based action to report on defined events, as required in R2, could be considered a valid requirement. However we have concerns as noted in Bullet 3 above.The requirements laid out in R1, R3 and R4 are specific controls to ensure that the proposed requirement to report (R2) is carried out. NERC is moving in the direction to assess entities' controls, outside of the compliance enforcement arm. The industry is being informed that NERC Audit staff will conduct compliance audits based on the controls that the entity has implemented to ensure compliance. We are interested in supporting this effort and making it successful. However, if this is the direction NERC is moving, we should not be making controls part of a compliance requirement. The only requirement proposed in this standard that is not a control is R2. 6. For FERC-jurisdictional entities, NERC does not need to duplicate the enforcement of reporting already imposed by the DOE. DOE-417 is a well established process that has regulatory obligations. NERC enforcement of reporting would be redundant. NERC has the ability to request copies of these reports without making them part of the Reliability Rules.
Response: The SDT thanks you for your comment. The SDT will bring this request to the attention of the SC for consideration as this request is beyond the scope of work identified in this project.		
Brazos Electric Power		We thank the work of the SDT on this project. However, additional improvements

Organization	Yes or No	Question 4 Comment
Cooperative		should be made as described in the comments submitted by ACES Power Marketing.
Response: The SDT thanks you for your comment. Please review the responses to that commenter.		
FirstEnergy		While FE voted affirmative on this draft, upon further review we request clarification be made in the next draft of the standard regarding the applicability of the Nuclear Generator Operator. Per FE's previous comments, nuclear generator operators already have specific regulatory requirements to notify the NRC for certain notifications to other governmental agencies in accordance with 10 CFR 50.72(b)(s)(xi). We had asked that the SDT contact the NRC about this project to ensure that existing communication and reporting that a licensee is required to perform in response to a radiological sabotage event (as defined by the NRC) or any incident that has impacted or has the potential to impact the BES does not create either duplicate reporting, conflicting reporting thresholds or confusion on the part of the nuclear generator operator. In addition, EOP-004 must acknowledge that there may be NRC reporting forms that have the equivalent information contained in their Attachment 2. For what the NRC considers a Reportable Event, Nuclear plants are required to fill out NRC form 361 and/or form 366. We do not agree with the drafting team's response to ours and Exelon's comments that "The NRC does not fall under the jurisdiction of NERC and so therefore it is not within scope of this project." While the statement is correct, we believe that requirements should not conflict with or duplicate other regulatory requirements. We remain concerned that the standard with regard to Nuclear GOP applicability causes duplicative regulatory reporting with existing reporting requirements of the NRC. Therefore, we ask:1. That NERC and the drafting team please investigate these issues further and revise the standard to clarify the scope for nuclear GOPs, and2. For any reporting deemed in the scope for nuclear GOP after NERC's and the SDT's investigation per our request in #1 above, that the SDT consider the ability to utilize information from NRC reports as meeting the EOP-004-2 requirements similar to the allowance of using the DOE form as presently proposed.

Organization	Yes or No	Question 4 Comment
Response: The SDT thanks you for your comment. The SDT team does not believe that reporting under EOP-004 can in anyway 'conflicts' with any other reporting obligations that nuclear or any other type of GO/GOP may have. By allowing applicable entities to use the OE-417 form, the drafting team believes it has given industry reasonable accommodation to reduce duplicative reporting. The same is true for other agencies as well. If an entity submits to NERC the same that was submitted to the other regulatory agency, then this submission will be acceptable. Based on the historical frequency with which GO/GOPs report under the current EOP-004-1 the drafting team does not believe this places and inordinate burden on the applicable entities.		
American Electric Power		While we do not necessarily disagree with modifying this standard, we do have serious concerns with the possibility that Form OE-417 form would not also be modified to match any changes made to this standard. To the degree they would be different, this would create unnecessary confusion and burden on operators. **While we appreciate the point raised, the SDT does have any authority with regard to the language contained within the DOE OE-417 form. The Department of Energy is responsible for the design and contents of the 417 form. As a part of the SDT's work in this proposal, we met with and collaborated with the DOE staff responsible for the 417 form establish a common understanding of reportable events. We hope that if the DOE desires to make further changes, they will pass along information for consideration in a future NERC SAR.** If CIP-008 is now out of scope within the requirements of this standard, the task "reportable Cyber Security Incident" should be removed from Attachment 2. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement.**
Response: The SDT thanks you for your comment.		
Progress Energy		Within attachment 1 (Reportable Events) an exclusion is allowed for weather related threats. PGN recommends a more generic approach to include natural events such as forest fires, sink holes, etc. This would alleviate some reporting burdens in areas that

Organization	Yes or No	Question 4 Comment
		are prone to these types of events.
Response: The SDT thanks you for your comment. The SDT has revised the language in accordance with your suggestion to "weather or natural disaster related threats".		
Xcel Energy		Xcel Energy appreciates the work of the drafting team and believes the current draft is an improvement over the existing standard. However, we would like to see the comments provided here and above addressed prior to submitting an AFFIRMATIVE vote.1) Suggest enhancing the "Example of Reporting Process..." flowchart as follows: EVENT > Refer to Ops Plan for Event Reporting > Refer to Law Enforcement? > Yes/No > .... **The SDT has provided the flowchart as an example and guidance for entities. Entities can choose to create their own version of the flowchart for use in their Operating Plan.** 2) Attachment 1 - in both the 1 hour and the 24 hour reporting they are qualified with "within x hours of recognition of the event". Is this the intent, so that if an entity recognizes at some point after an event that the time clock starts? **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement.** **The SDT envisions when the entity is made aware of an applicable event contained in Attachment 1, that they would report the event within 24 hours. Any entity could enhance their Operating Plan to describe as much detail as they wanted to provide to their employees as they see fit.** 3) VSLs - R3 & R4 "Severe" should remove the "OR....", as this is redundant. Once an entity has exceeded the 3 calendar months, the Severe VSL is triggered. **The SDT has revised the requirements and accordingly the VSLs.** 4) The Guideline and Technical Basis page 22 should be corrected to read "The

Organization	Yes or No	Question 4 Comment
		changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). These standards deal exclusively with after-the-fact reporting." **Response: Thank you for the grammatical correction.** 5) Also in the following section of the Guideline and Technical Basis (page 23) the third bullet item should be qualified to exclude copper theft: Examples of such events include: o Bolts removed from transmission line structures o Detection of cyber intrusion that meets criteria of CIP-008-3 or its successor standard o Forced intrusion attempt at a substation (excluding copper theft) o Train derailment near a transmission right-of-way o Destruction of Bulk Electric System equipment **Response: Thank you for the correction; however, as a result of other changes made to the standard, the SDT is proposing to remove the third bulleted item from this list.**
Response: The SDT thanks you for your comment.		
Edison Mission Marketing & Trading, Inc.		No
Idaho Power Co.		No
Arizona Public Service Company		None

END OF REPORT

Consideration of Comments

Project 2009-01 Disturbance Sabotage and Reporting

The Project 2009-01 Drafting Team thanks all commenters who submitted comments on Draft 5 of EOP-004-2. The standard was posted for a 30-day public comment period from August 29, through September 27, 2012. Stakeholders were asked to provide feedback on the standard and associated documents through a special electronic comment form. There were 56 sets of comments, including comments from approximately 181 different people from approximately 125 companies, representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

Summary Consideration:

The Disturbance and Sabotage Reporting standard drafting team has opted to pursue a recirculation ballot for EOP-004-2 after making a few clarifications to the Guidelines and Technical Basis section to address stakeholder concerns raised during the second successive ballot:

- Distribution Providers – Some concerns were raised with respect to applicability of the standard to all Distribution Providers. The concerns relate to DPs that do not own BES Facilities. While these entities would not have any events to report under R2, they would still be applicable under R1 and R3. The team discussed this issue and has addressed this concern with additional language in the Guidelines and Technical Basis Section of the standard as follows:

  "Distribution Provider Applicability Discussion

  The DSR SDT has included Distribution Providers (DP) as an applicable entity under this standard. The team realizes that not all DPs will own BES Facilities and will not meet the "Threshold for Reporting" for any event listed in Attachment 1. These DPs will not have

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

any reports to submit under Requirement R2. However, these DPs will be responsible for meeting Requirements R1 and R3. The DSR SDT does not intend for these entities to have a detailed Operating Plan to address events that are not applicable to them. In this instance, the DSR SDT intends for the DP to have a very simple Operating Plan that includes a statement that there are no applicable events in Attachment 1 (to meet R1) and that the DP will review the list of events in Attachment 1 each year (to meet R3). The team does not think this will be a burden on any entity as the development and annual validation of the Operating Plan should not take more that 30 minutes on an annual basis. If a DP discovers applicable events during the annual review, it is expected that the DP will develop a more detailed Operating Plan to comply with the requirements of the standard."

- Duplicative Reporting – If an entity is registered as an RC, BA and TOP, they should only have to submit a single report. The team discussed and has addressed this concern with additional language in the Guidelines and Technical Basis Section of the standard as follows:

  "Multiple Reports for a Single Organization

  For entities that have multiple registrations, the DSR SDT intends that these entities will only have to submit one report for any individual event. For example, if an entity is registered as a Reliability Coordinator, Balancing Authority and Transmission Operator, the entity would only submit one report for a particular event rather submitting three reports as each individual registered entity."

  With regards to the concern regarding multiple entities submitting a report for the same event, the team does not see this as being an issue for industry and will not make any further revisions to address this.

Other issues were raised by stakeholders and a discussion of those is below:

- **24 Hour Reporting** – Several stakeholders had concerns regarding the 24 hour reporting requirement. Commenters suggest that events or situations affecting real time reliability to the system already are required to be reported to appropriate Functional Entities that have the responsibility to take action. Adding one more responsibility to system operators increases the operator's burden, which reduces the operator's effectiveness when operating the system. Care should be given when placing additional responsibility on the system operators. Allowing reporting at the end of the next business day gives operators the flexibility to allow support staff to assist with after-the-fact reporting requirements. To this end, the DSR SDT has added clarifying language to R2 as follows:

R2. Each Responsible Entity shall report events per their Operating Plan within 24 hours of recognition of meeting an event type threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

- **Paragraph 81** – On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 of that order ("P81"), invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program.

- **Reporting** – Some comments were submitted regarding the reporting burden of this standard. The revised standard combines two standards into one and removes the analysis portion of the current mandatory and enforceable standards (EOP-004-1 and CIP-001-2a). The analysis provisions will be addressed in the NERC Events Analysis Program upon approval of EOP-004-2. This revised standard involves notification only and does not require any investigation or analysis.

- **Attachment 1 comments** – Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. . The team has elected to move forward to recirculation ballot.

- **Violation Risk Factors** - Many stakeholders had concerns with the VRFs for R2 and R3 being assigned as "medium". The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower

the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.

- **Violation Severity Levels** - Other stakeholders suggested revision to the VSLs for Requirement R1 based on if the event reporting Operating Plan fails to include one or more of the event types listed in Attachment 1. The SDT agrees and has revised the VSLs for R1 as follows:

  Lower: The Responsible Entity had an Operating Plan, but failed to include one applicable event type.

  Moderate: The Responsible Entity had an Operating Plan, but failed to include two applicable event types.

  High: The Responsible Entity had an Operating Plan, but failed to include three applicable event types.

  Severe: The Responsible Entity had an Operating Plan, but failed to include four or more applicable event types OR the Responsible Entity failed to have an event reporting Operating Plan.

Index to Questions, Comments, and Responses

1. The DSR SDT has revised EOP-004-2 by combining Requirements R3 and R4 into a single requirement (Requirement R3) to, "… validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year." Do you agree with this revision? If not, please explain in the comment area below. 15
2. The DSR SDT has revised the VSLs to reflect the language in the revised requirements. Do you agree with the proposed VRFs and VSLs? If not, please explain in the comment area below. 25
3. Do you have any other comment, not expressed in the questions above, for the DSR SDT?.....37

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Carmen Agavriloai	Independent Electricity System Operator	NPCC	2
3.	Greg Campoli	New York Independent System Operator	NPCC	2
4.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
5.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
7.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
8.	Kathleen Goodman	ISO - New England	NPCC	2

Group/Individual		Commenter	Organization		Registered Ballot Body Segment									
					1	2	3	4	5	6	7	8	9	10
9.	Michael Jones	National Grid	NPCC	1										
10.	David Kiguel	Hydro One Networks Inc.	NPCC	1										
11.	Michael Lombardi	Northeast Utilities	NPCC	1										
12.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9										
13.	Bruce Metruck	New York Power Authority	NPCC	6										
14.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5										
15.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10										
16.	Robert Pellegrini	The United Illuminating Company	NPCC	1										
17.	Si-Truc Phan	Hydro-Quebec TransEnergie	NPCC	1										
18.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5										
19.	Brian Robinson	Utility Services	NPCC	8										
20.	Michael Schiavone	National Grid	NPCC	1										
21.	Wayne Sipperly	New York Power Authority	NPCC	5										
22.	Donald Weaver	New Brunswick System Operator	NPCC	2										
23.	Ben Wu	Orange and Rockland Utilities	NPCC	1										
24.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3										
2.	Group	Ron Sporseen	PNGC Comment Group		X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumer's Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3
7.	Rick Crinklaw	Lane Electric Cooperative	WECC	3
8.	Annie Terracciano	Northern Lights Inc.	WECC	3
9.	Aleka Scott	PNGC Power	WECC	4
10.	Heber Carpenter	Raft River Electric Cooperative	WECC	3
11.	Steve Eldrige	Umatilla Electric Cooperative	WECC	1, 3
12.	Marc Farmer	West Oregon Electric Cooperative	WECC	4

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
13.	Margaret Ryan	PNGC Power	WECC 8										
14.	Rick Paschall	PNGC Power	WECC 3										
3.	Group	Greg Rowland	Duke Energy	X		X		X	X				
	Additional Member	**Additional Organization**	**Region** / **Segment Selection**										
1.	Doug Hils	Duke Energy	RFC 1										
2.	Lee Schuster	Duke Energy	FRCC 3										
3.	Dale Goodwine	Duke Energy	SERC 5										
4.	Greg Cecil	Duke Energy	RFC 6										
4.	Group	Chang Choi	Tacoma Public Utilities	X		X	X	X	X				
	Additional Member	**Additional Organization**	**Region** / **Segment Selection**										
1.	Chang Choi	City of Tacoma	WECC 1										
2.	Travis Metcalfe	Tacoma Public Utilities	WECC 3										
3.	Keith Morisette	Tacoma Public Utilities	WECC 4										
4.	Chris Mattson	Tacoma Power	WECC 5										
5.	Michael Hill	Tacoma Public Utilities	WECC 6										
5.	Group	Kent Kujala	Detroit Edison			X	X	X					
	Additional Member	**Additional Organization**	**Region** / **Segment Selection**										
1.	Alexander Eizans		RFC 3, 4, 5										
2.	Barbara Holland		RFC 3, 4, 5										
3.	Jeffrey DePriest		RFC 3, 4, 5										
6.	Group	Gerry Beckerle	SERC OC Standards Review Group	X		X							
	Additional Member	**Additional Organization**	**Region** / **Segment Selection**										
1.	Roger Powers	City of Springfield, IL - CWLP	SERC 1, 3										
2.	Dan Roethemeyer	Dynegy	SERC 5										
3.	Melinda Montgomery	Entergy	SERC 1, 3, 6										
4.	Terry Bilke	MISO	SERC 2										
5.	Scott Brame	NCEMC	SERC 4, 1, 3, 5										
6.	William Berry	OMU	SERC 3, 5										

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Tim Hattaway	PowerSouth	SERC 1, 5										
8. Brett Koelsch	Progress Energy Carolinas	SERC 1, 3, 5, 6										
9. Vicky Budreau	SCPSA	SERC 1, 3, 5, 6										
10. Gary Hutson	SMEPA	SERC 1, 3, 5, 6										
11. Marsha Morgan	Southern Co. Services	SERC 1, 5										
12. Randy Hubbert	Southern Co. Services	SERC 1, 5										
13. Joel Wise	TVA	SERC 1, 3, 5, 6										
14. Stuart Goza	TVA	SERC 1, 3, 5, 6										
15. Jim Case	Entergy	SERC 1, 3, 6										
16. Mike Bryson	PJM	SERC 2										
17. Mike Hirst	Cogentrix	SERC 5										
7. Group	Larry Raczkowski	FirstEnergy	X		X	X	X	X				
Additional Member	**Additional Organization**	**Region** / **Segment Selection**										
1. William J Smith	FirstEnergy Corp	RFC 1										
2. Stephan Kern	FirstEnergy Energy Delivery	RFC 3										
3. Douglas Hohlbaugh	Ohio Edison Company	RFC 4										
4. Kenneth Dresner	FirstEnergy Solutions	RFC 5										
5. Kevin Querry	FirstEnergy Solutions	RFC 6										
8. Group	Mike Garton	Dominion	X		X	X	X					
Additional Member	**Additional Organization**	**Region** / **Segment Selection**										
1. Louis Slade	Dominion Resources Services, Inc.	RFC 5, 6										
2. Randi Heise	Dominion Resources Services, Inc.	MRO 5, 6										
3. Connie Lowe	Dominion Resources Services, Inc.	NPCC 5, 6										
4. Mike Crowley	Virginia Electric and Power Company	SERC 1, 3, 5, 6										
9. Group	WILL SMITH	MRO NSRF	X	X	X	X	X	X				
Additional Member	**Additional Organization**	**Region** / **Segment Selection**										

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

1.	CHUCK LAWRENCE	ATC	MRO	1
2.	TOM BREENE	WPS	MRO	3, 4, 5, 6
3.	JODI JENSON	WAPA	MRO	1, 6
4.	KEN GOLDSMITH	ALTW	MRO	4
5.	ALICE IRELAND	XCEL/NSP	MRO	1, 3, 5, 6
6.	DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6
7.	ERIC RUSKAMP	LES	MRO	1, 3, 5, 6
8.	JOE DEPOORTER	MGE	MRO	3, 4, 5, 6
9.	SCOTT NICKELS	RPU	MRO	4
10.	TERRY HARBOUR	MEC	MRO	1, 3, 5, 6
11.	MARIE KNOX	MISO	MRO	2
12.	LEE KITTELSON	OTP	MRO	1, 3, 5
13.	SCOTT BOS	MPW	MRO	1, 3, 5
14.	TONY EDDLEMAN	NPPD	MRO	1, 3, 5
15.	MIKE BRYTOWSKI	GRE	MRO	1, 3, 5, 6
16.	DAN INMAN	MPC	MRO	1, 3, 5, 6

				1	2	3	4	5	6	7	8	9	10
10.	Group	Chris Higgins	Bonneville Power Administration	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Jim Burns	BPA, Technical Operations	WECC	1
2.	Fran Halpin	BPA, Duty Scheduling	WECC	5
3.	Erika Doot	BPA, Generation Support	WECC	3, 5, 6
4.	John Wylder	BPA, Transmission	WECC	1
5.	Deanna Phillips	BPA, FERC Compliance	WECC	1, 3, 5, 6
6.	Russell Funk	BPA, Transmission	WECC	1

				1	2	3	4	5	6	7	8	9	10
11.	Group	Robert Rhodes	SPP Standards Review Group		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Allen	City Utilities of Springfield	SPP	1, 4
2.	Doug Callison	Grand River Dam Authority	SPP	1, 3, 5
3.	Jonathan Hayes	Southwest Power Pool	SPP	2
4.	Bo Jones	Westar Energy	SPP	1, 3, 5, 6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
5. Allen Klassen	Westar Energy	SPP	1, 3, 5, 6										
6. Tiffany Lake	Westar Energy	SPP	1, 3, 5, 6										
7. Tara Lightner	Sunflower Electric Power Corporation	SPP	1										
8. Kyle McMenamin	Xcel Energy	SPP	1, 3, 5, 6										
9. Jerry McVey	Sunflower Electric Power Corporation	SPP	1										
10. Fred Meyer	Empire District Electric Company	SPP	1										
11. Terri Pyle	Oklahoma Gas & Electric Company	SPP	1, 3, 5										
12. Don Schmit	Nebraska Publlic Power District	MRO	1, 3, 5										
13. Katie Shea	Westar Energy	SPP	1, 3, 5, 6										
14. Sean Simpson	Board of Public Utilities, City of McPherson	SPP	NA										
15. Bryan Taggart	Westar Energy	SPP	1, 3, 5, 6										
16. Mark Wurm	Board of Public Utilities, City of McPherson	SPP	NA										
12. Group	Jason Marshall	ACES Power Marketing Standards Collaborators							X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Susan Sosbe	Wabash Valley Power Association	RFC	3										
2. Clem Cassmeyer	Western Farmers Electric Cooperative	SPP	1, 5										
3. Megan Wagner	Sunflower Electric Power Corporation	SPP	1										
4. Scott Brame	North Carolina Electric Membership Corporation	SERC	1, 3, 4, 5										
5. Bob Solomon	Hoosier Energy	RFC	1										
6. Robert Thomasson	Big Rivers Electric Corporation	SERC											
7. Shari Heino	Brazos Electric Power Cooperative	ERCOT	1, 5										
8. John Shaver	Arizona Electric Power Cooperative	WECC	4, 5										
9. John Shaver	Southwest Transmission Cooperative	WECC	1										
10. Mohan Sachdeva	Buckeye Power	RFC	3, 4										
11. Michael Brytowski	Great River Energy	MRO	1, 3, 5, 6										
13. Individual	Janet Smith, Regulatory Affairs Supervisor	Arizona Public Service Company		X		X		X	X				
14. Individual	Emily Pennel	Southwest Power Pool Regional Entity											X

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
15.	Individual	Antonio Grayson	Southern Company	X		X		X	X				
16.	Individual	Daniela Hammons	CenterPoint Energy	X									
17.	Individual	Lee Layton	Blue Ridge EMC	X		X							
18.	Individual	Anthony Jablonski	ReliabilityFirst										X
19.	Individual	Jonathan Appelbaum	The United Illuminating Company	X									
20.	Individual	Russ Schneider	Flathead Electric Cooperative, Inc.			X	X						
21.	Individual	Oliver Burke	Entergy Services, Inc. (Transmission)	X									
22.	Individual	Nazra Gladu	Manitoba Hydro	X		X		X	X				
23.	Individual	Steve Grega	Lewis County PUD	X				X					
24.	Individual	Steve Alexanderson P.E.	Central Lincoln			X	X					X	
25.	Individual	Jack Stamper	Clark Public Utilities	X									
26.	Individual	Russell A. Noble	Cowlitz PUD			X	X	X					
27.	Individual	Chantel Haswell	Public Service Enterprise Group	X		X		X	X				
28.	Individual	Mike Hirst	Cogentrix Energy					X					
29.	Individual	Dave Willis	Idaho Power Co.	X		X							
30.	Individual	Michelle R D'Antuono	Ingelside Cogeneration LP					X					
31.	Individual	Howard Rulf	Wisconsin Electric Power company dba We Energies			X	X	X					
32.	Individual	Melissa Kurtz	US Army Corps of Engineers					X					
33.	Individual	David Jendras	Ameren Services	X		X		X	X				
34.	Individual	Michael Falvo	Independent Electricity System Operator		X								
35.	Individual	RoLynda Shumpert	South Carolina Electric and Gas	X		X		X	X				
36.	Individual	David Revill	Georgia Transmission Corporation	X									
37.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
38.	Individual	Andrew Z.Pusztai	american Transmission Company	X									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
39.	Individual	Don Schmit	Nebraska Public Power Disstrict	X		X		X					
40.	Individual	Terry Harbour	MidAmerican Energy	X		X		X	X				
41.	Individual	Kathleen Goodman	ISO New England Inc.		X								
42.	Individual	d mason	City and County of San Francisco - Hetch Hetchy Water and Power					X					
43.	Individual	Tracy Richardson	Springfield Utility Board			X							
44.	Individual	Rich Salgo	NV Energy	X		X		X					
45.	Individual	Thad Ness	American Electric Power	X		X		X	X				
46.	Individual	Charles Yeung	Southwest Power Pool RTO		X								
47.	Individual	Nathan Mitchell	American Public Power Association			X	X						
48.	Individual	Don Jones	Texas Reliability Entity										X
49.	Individual	Christine Hasha	ERCOT		X								
50.	Individual	Denise M. Lietz	Puget Sound Energy Inc.	X		X		X					
51.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				
52.	Individual	Christina Bigelow	Midwest Independent Transmission System Operator, Inc.		X								
53.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
54.	Individual	Darryl Curtis	Oncor Electric Delivery	X									
55.	Individual	Tony Kroskey	Brazos Electric Power Cooperative, Inc.	X									
56.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				

If you wish to express support for another entity's comments without entering any additional comments, you may do so here.

Organization	Supporting Comments of "Entity Name"
PNGC Comment Group	Central Lincoln PUD
Blue Ridge EMC	R3 is another example of a "paper chase", creating (or rather continuing) an administrative burden for the utility. The standard should only require that the entity have a plan and the accountability should be "did the entity follow the plan when needed, including proving that the appropriate contacts were made?"
Response: Thank you for your comment. Requirement R3 is in direct response to a FERC directive in Order 693 and as such, the SDT included this provision. Also, if the information in the plan is out of date, then the plan will not be effective.	
Flathead Electric Cooperative, Inc.	Central Lincoln
US Army Corps of Engineers	MRO NSRF
Nebraska Public Power District	Midwest Reliability Organization (MRO) NERC Standards Review Forum (NSRF); AND Southwest Power Pool RTO
MidAmerican Energy	MidAmerican supports the MRO NSRF comments
ISO New England Inc.	NPCC

1. **The DSR SDT has revised EOP-004-2 by combining Requirements R3 and R4 into a single requirement (Requirement R3) to, "… validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year." Do you agree with this revision? If not, please explain in the comment area below.**

Summary Consideration: The majority of stakeholders agree with the combination of R3 and R4 and with the new language of R3 to "validate" the contact information. A few commenters suggested that Requirement R3 is administrative and should be removed under the provisions of "Paragraph 81". On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 ("P81") invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program.

Organization	Yes or No	Question 1 Comment
CenterPoint Energy	No	CenterPoint Energy supports the concept of combining Requirements R3 and R4; however, the Company still prefers an annual review requirement which would include validating the contact information and content of the Operating Plan overall. Therefore, CenterPoint Energy recommends the following revised language for Requirement R3: "Each Responsible Entity shall review and update the Operating Plan at least every 15 months." The Company also suggests that the Measure be worded as follows: "Evidence may include, but is not limited to dated documentation reflecting changes to the Operating Plan including updated contact information if necessary."

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comment. The SDT appreciates the suggestion on validating the content of the Operating Plan, but at this time, we feel that the step is not necessary to meet the directive from FERC Order 693. As to the comment on extending the review period to 15 months, following much discussion and review of the industry comments, we are staying with the language as proposed.		
American Electric Power	No	In the spirit of Paragraph 81 efforts, we request the removal of R3 as it is solely administrative in nature, existing only to support R2. This is more of an internal control and does not appear to rise to the level of being an industry-wide requirement. In addition, having two requirements rather than one increases the likelihood of being found non-compliant for multiple requirements rather than a single requirement.
Response: Thank you for your comment. Requirement R3 is in direct response to a FERC directive in Order 693 and as such, the SDT included this provision. On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 ("P81") invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. , CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program. As the SDT is moving forward with a Recirculation Ballot, your suggestions will be forwarded to NERC for future consideration.		
City and County of San Francisco - Hetch Hetchy Water and Power	No	Measure M3 specifically identifies two types of acceptable compliance evidence: Voice Recording and Log entries. Specifying only these two forms of evidence creates a risk that some auditors will reject other forms of R3 compliance evidence which are equally valid, such as emails or written call records. Although M3 states that acceptable evidence is not limited to Voice Recordings or Log Entries, we have concern that other

Organization	Yes or No	Question 1 Comment
		methods of complying with R3 may not be accepted.
Response: Thank you for your comment. The SDT believes that the phrase "may include, but are not limited to" addresses your concern. The SDT will present your comment to the NERC Compliance staff in an effort to inform audit staffs on what evidence is permissible.		
Blue Ridge EMC	No	See previous comments
Response: Thank you for previous comments. Requirement R3 is in direct response to a FERC directive in Order 693 and as such, the SDT included this provision. Also, if the information in the plan is out of date, then the plan will not be effective.		
Detroit Edison	No	The requirement is too prescriptive and difficult to document. Requirement should be for annual review of Operating Plan. This allows for entity to review plan and document this the same as other Standards that require annual review (i.e. annual review blocks on documents).The requirement as written is vague and difficult to document. Annual review of reporting process is already a requirement.
Response: Thank you for your comments. While the SDT appreciates the view that the Operating Plan should be reviewed annually, the SDT feels that the requirement only needs to address the validity of the contact information contained within the Operating Plan in order to meet the FERC directive in Order 693. If the entity is aware of changes within its operations that would make a more extensive review advisable, it can choose to do so; but where there have been no significant changes to an entity's operations in the last year, ensuring the validity of the contact information should be sufficient.		
Manitoba Hydro	No	This seems like an administrative only requirement. It would be too difficult to validate or measure.
Response: Thank you for your comment. Requirement R3 is in direct response to a FERC directive in Order 693 and as such, the SDT included this provision. The measure calls for an entity to have "dated records to show that it validated all contact information contained in the Operating Plan each calendar year. Such evidence may include, but are not limited to, dated voice recordings and operating logs or other communication documentation." The SDT does not believe that this is an administrative		

Organization	Yes or No	Question 1 Comment
requirement because, if the information in the Operating Plan is out of date, then the plan will not be effective.		
ACES Power Marketing Standards Collaborators	No	We believe that the revision to R3 and elimination of R4 are great improvements to the standard as a lot of the unnecessary burdens have been removed. However, Requirement R3 is still not needed, has several issues with it and should be eliminated. (1) While validating contact information annually in a reporting plan makes sense, it does not rise to level of importance of requiring sanctions for failure to do so. Furthermore, it does nothing to assure reliability. Shortly after the contact information has been updated, it could change. This does not mean that validation should be more frequent but simply that is an unnecessary administrative burden. If contact information changes, the registered entity will have to find it. For reliability purposes, why does it matter if they do this in the 24-hour reporting period after the event or annually before the event? (2) Requirement R3 is administrative and is not consistent with the recent direction that NERC and FERC have taken toward compliance. Violations of this requirement are likely to be candidates for FFT treatment and this is exactly the kind of requirement that FERC invited NERC to propose for retirement in Paragraph 81 of the order approving the FFT process. Furthermore, it appears to meet at least two criteria (Administrative and periodic updates) that the Paragraph 81 drafting team has proposed to use to identify candidate requirements for retirement. The requirement is also not consistent with the direction NERC has taken on internal controls. How is an auditor reviewing that contact information has been updated in an Operating Plan forward looking or for that matter beneficial to reliability? Imagine a registered entity fails to update their contact information but still reports an event within the 24 hour reporting time frame to the appropriate parties. They are in technical violation of R3 but have met the spirit of the standard. (3) Requirement R3 is not a results-based requirement. It simply compels a registered entity "how to" meet reporting deadlines. Certainly, if a

Organization	Yes or No	Question 1 Comment
		registered entity has current contact information on hand, it will be easier to notify appropriate parties of events quickly. However, it does limit a registered entity's ability to identify its own unique and possibly better way to meet a requirement. "How to" requirements prevent unique and superior solutions.
Response: Thank you for your comment. Requirement R3 is in direct response to a FERC directive in Order 693 and as such, the SDT included this provision. The SDT does not believe that this is an administrative requirement because, if the information in the Operating Plan is out of date, then the plan will not be effective. **On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 ("P81") invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program. As the SDT is moving forward with a Recirculation Ballot, your suggestions will be forwarded to NERC for future consideration.**		
NV Energy	No	Without further clarification of what is expected by "validate all contact information" I cannot support this requirement. On the surface, "validate" appears to be acceptable terminology, as it means to me a review of the contact names and contact information (perhaps cell #, home phone, text address, email address, etc) that would be evidenced through an attestation of completion of review along with records showing the updates made to the contact information pursuant to the review. However, when the Measure is considered, it refers to evidence such as operator logs, voice recordings, etc. This seems to indicate that the

Organization	Yes or No	Question 1 Comment
		expectation is that each contact is tested, by dialing, texting, emailing, etc with some sort of confirmation that each contact was successful. If this is what is necessary to satisfy the "validate" requirement, I believe it is excessive, burdensome and unnecessary. I suggest modification of the Measure language to clearly allow for an entity to demonstrate compliance by a showing that it reviewed the contact information and made changes as deemed necessary by its review, and to remove the reference to operator logs and voice recordings as the evidence of measure.
Response: Thank you for your comment. The SDT agrees with your comment and views your direction as being consistent with the standard's intent. The SDT will submit your comment to NERC Compliance staff for their consideration. The SDT intends for operator logs and voice recordings to be acceptable as evidence, but not the only acceptable evidence. The use of the language "such as" in the measure indicates this.		
Bonneville Power Administration	Yes	BPA agrees with the revision and recognizes that it will involve a large amount of validation workload for entities with a large footprint.
Response: Thank you for your comment.		
Dominion	Yes	Dominion supports the combination of Requirements R3 and R4 into a single requirement (Requirement R3), although we remain concerned that validation requiring a phone call could be perceived as a nuisance by that entity.
Response: Thank you for your comment. The SDT appreciates this concern but feels that the requirement is necessary to address the FERC directive in the Order 693. The SDT does not believe that validation of the contact information will be a nuisance. If the information in the Operating Plan is out of date, then the plan will not be effective.		
Duke Energy	Yes	Duke Energy commends the excellent work of the Standard Drafting Team in incorporating previous comments into the current posted draft of the

Organization	Yes or No	Question 1 Comment
		standard.
Response: Thank you for your comment.		
ERCOT	Yes	ERCOT considers replacing R3 and R4 with the new R3 is an improvement and we thank the drafting team for making the change.
Response: Thank you for your comment.		
ReliabilityFirst	Yes	Even though ReliabilityFirst votes in the Affirmative, we offer the following comment regarding Requirement R3 for consideration. ReliabilityFirst recommends changing the word "validate" to "verify" in Requirement R3. ReliabilityFirst believes not only does the entity need to validate contact information is correct, they should verify (i.e. authenticate though test) that the contact information is correct.
Response: Thank you for your comment. The SDT feels that the action you define is consistent with our intent.		
Independent Electricity System Operator	Yes	IESO agrees that the intent of Requirement R3 to have the Registered Entities validate the contact information in the contact lists that they may have for the events applicable to them is achieved. IESO also agrees that the elimination of conducting an annual test of the communications process and review of the event reporting Operating Plan in merging the previous R3 and R4 into this new R3 will give entities an opportunity to develop a plan that suits its business needs.
Response: Thank you for your comment.		
Indiana Municipal Power Agency	Yes	IMPA agrees with the removal of a "test" and going with a validation requirement for the contact information in the Operating Plan.

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comment.		
Ingelside Cogeneration LP	Yes	Ingleside Cogeneration believes that an annual validation of contact information is sufficient for a reporting procedure. R2 provides sufficient impetus for Responsible Entities to keep their Operating plan current - as a missed report will lead to a violation. Furthermore, external agencies and law enforcement officials will be reluctant to participate in validation tests, as dozens of nearby BES entities will overwhelm them with such requests.
Response: Thank you for your comment. Requirement R3 is in direct response to a FERC directive in Order 693 and as such, the SDT included this provision. If the information in the Operating Plan is out of date, then the plan will not be effective.		
SPP Standards Review Group	Yes	We feel that replacing R3 and R4 with the new R3 is an improvement and we thank the drafting team for making the change.
Response: Thank you for your support.		
PNGC Comment Group	Yes	
Tacoma Public Utilities	Yes	
SERC OC Standards Review Group	Yes	
FirstEnergy	Yes	
MRO NSRF	Yes	
Arizona Public Service Company	Yes	
Southwest Power Pool Regional Entity	Yes	

Organization	Yes or No	Question 1 Comment
Southern Company	Yes	
The United Illuminating Company	Yes	
Entergy Services, Inc. (Transmission)	Yes	
Lewis County PUD	Yes	
Central Lincoln	Yes	
Clark Public Utilities	Yes	
Cowlitz PUD	Yes	
Public Service Enterprise Group	Yes	
Cogentrix Energy	Yes	
Idaho Power Co.	Yes	
Wisconsin Electric Power company dba We Energies	Yes	
Ameren Services	Yes	
South Carolina Electric and Gas	Yes	
Georgia Transmission Corporation	Yes	
City of Austin dba Austin Energy	Yes	
american Transmission Company	Yes	

Organization	Yes or No	Question 1 Comment
MidAmerican Energy	Yes	
Springfield Utility Board	Yes	
Southwest Power Pool RTO	Yes	
American Public Power Association	Yes	
Texas Reliability Entity	Yes	
Puget Sound Energy Inc.	Yes	
Exelon Corporation and its affiliates	Yes	
Midwest Independent Transmission System Operator, Inc.	Yes	
Oncor Electric Delivery	Yes	
Xcel Energy	Yes	

2. The DSR SDT has revised the VSLs to reflect the language in the revised requirements. Do you agree with the proposed VRFs and VSLs? If not, please explain in the comment area below.

Summary Consideration: Many stakeholders had concerns with the VRFs for R2 and R3 being assigned as "medium". The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.

Other stakeholders suggested revision to the VSLs for Requirement R1 based on if the event reporting Operating Plan fails to include one or more of the event types listed in Attachment 1. The SDT agrees and has added the following VSLs to R1, in addition to the language that was previously included in the "Severe" VSL:

Lower: The Responsible Entity had an Operating Plan, but failed to include one applicable event type.

Moderate: The Responsible Entity had an Operating Plan, but failed to include two applicable event types.

High: The Responsible Entity had an Operating Plan, but failed to include three applicable event types.

Severe: The Responsible Entity had an Operating Plan, but failed to include four or more applicable event types.

Organization	Yes or No	Question 2 Comment
Detroit Edison	No	Under VSLs for R2- We disagree with the reporting time frames. Making the time requirement as soon as 24 hours puts this reporting requirement on the real time operators. Many of the situations listed in the EOP-004 attachment are not included in the OE-417 report. The Unofficial Comment Form states the reporting obligations serve to provide input to the NERC Event Analysis Program. This program has removed the 24 hour reporting requirement and

Organization	Yes or No	Question 2 Comment
		changed it to 5 business days.
Response: Thank you for your comments. The reporting obligation under this standard is to provide notification of events to NERC Situation Awareness group. The SDT, in consultation with the DOE and NERC Events Analysis group, have recognized the where there is duplication of reporting and provided for the common use of the different group's forms. This standard is not a replacement or substitution for any other obligations to other agencies. However, the SDT recognizes the concern with having real time operations staff submitting the report. To this end, the DSR SDT has added clarifying language to R2 as follows: **R2. Each Responsible Entity shall report events per their Operating Plan within 24 hours of meeting an event type threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). [Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]**		
Texas Reliability Entity	No	(1) VSLs for R1 should have a lower level VSL if the event reporting Operating Plan fails to include one or more of the event types listed in Attachment 1. (2) VSL for R1 is incorrectly stated as there are no "parts" to R1.
Response: Thank you for your comment. 1) The SDT agrees and has added the following VSLs for R1, in addition to the language that was previously included in the "Severe" VSL: **Lower: The Responsible Entity had an Operating Plan, but failed to include one applicable event type.** **Moderate: The Responsible Entity had an Operating Plan, but failed to include two applicable event types.** **High: The Responsible Entity had an Operating Plan, but failed to include three applicable event types.** **Severe: The Responsible Entity had an Operating Plan, but failed to include four or more applicable event types.** **2) This was correct in the clean version of the standard.**		
ACES Power Marketing Standards Collaborators	No	Because R3 is administrative, the VRF should be Lower. The requirement simply compels that that registered entity update a document which is purely administrative.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a		

Organization	Yes or No	Question 2 Comment
is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.		
Bonneville Power Administration	No	BPA does not agree with the VRFs and VSLs. BPA believes that the violation levels for administrative errors are too high. For more information, please reference comments to question #3.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF. Please see the response to your question 3 comments.		
CenterPoint Energy	No	CenterPoint Energy suggests that the phrase "which caused a negative impact to the Bulk Electric System" be added to each Violation Severity Level. For example, the wording would appear as follows: "The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 24 hours but less than or equal to 36 hours after meeting an event threshold for reporting which caused a negative impact to the Bulk Electric System". Additionally or alternatively, the Company proposes that the above phrase be added to the Threshold(s) for Reporting in Attachment 1 to focus on events that have an impact or effect on the Bulk Electric System.
Response: Thank you for your comment. The SDT does not believe such a change is necessary. Each event type listed is applicable to BES reliability.		

Organization	Yes or No	Question 2 Comment
MidAmerican Energy	No	Change the VRFs / VSLs to match suggested changes in Question 3
Response: Thank you for your comment. The SDT followed the NERC guidelines for VSLs in setting the appropriate levels. Please see the response to your question 3 comments.		
The United Illuminating Company	No	Do not agree that the VRF for R3 is medium. Failure to Validate contact information will not likely lead to instability and Cascade. Reporting under EOP-004 is not an immediate action, and given a 24 hour reporting window a proper contact point can be identified on-the-fly. R2 is properly identified as the Medium VRF since a failure to report whether due to an improper Operating plan or improper contact list may lead to a BES cascade.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.		
Southwest Power Pool Regional Entity	No	In R2, SPP RE does not understand why the VSLs are based on who was or was not contacted rather than when it was reported. An entity could decide to put only two entities in its Event Reporting Operating Plan. If the entity fails to submit an appropriate event report, it is open to a Severe VSL on the top set of VSLs but only a moderate on the lower set of VSLs. This seems to be a disconnect for applying the VSLs for the same facts and circumstances.
Response: Thank you for your comment. The SDT followed the NERC guidelines for VSLs in setting the appropriate levels. The VSLs were written based on two potential failures to meet the requirement. The first is based on the time the report was submitted while the second was based on the entity submitting the report within 24 hours but not to all applicable entities.		

Organization	Yes or No	Question 2 Comment
Midwest Independent Transmission System Operator, Inc.	No	MISO agrees with the comments submitted by the SERC Operating Committee that the VRFs for R2 and R3 should be "Lower" instead of "Medium," since these are administrative requirements. MISO further respectfully suggests that implementing another standard that requires reporting every incident identified in a plan within 24 hours and that classifies failure to do so a "Severe" violation, will likely cause entities to limit the scope of their plans. NERC, therefore, would not receive information that appears unimportant to a single entity but could be important in the context of similar events across the country.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF. **The SDT does not agree with your second comment and believes that entities will report the appropriate events.**		
Oncor Electric Delivery	No	Oncor suggest the following additions to VSL language for R1 to align more closely with the measures described in M1Lower VSL - Entity has one applicable event type not properly identified in its event reporting Operating Plan. High VSL - Entity has more than one applicable event type not properly identified in its event reporting Operating Plan. Severe VSL - The Responsible Entity failed to have an event reporting Operating Plan
Response: Thank you for your comment. Based on comments from you and others, we have added the following VSLs for R1, in addition to the language that was previously included in the "Severe" VSL: **Lower: The Responsible Entity had an Operating Plan, but failed to include one applicable event type.**		

Organization	Yes or No	Question 2 Comment
Moderate: The Responsible Entity had an Operating Plan, but failed to include two applicable event types. **High: The Responsible Entity had an Operating Plan, but failed to include three applicable event types.** **Severe: The Responsible Entity had an Operating Plan, but failed to include four or more applicable event types.**		
Exelon Corporation and its affiliates	No	R2 VSLs - By measuring the amount of time taken to report and the number of entities to receive the report, the VSLs track more with size and location than with a failure to report. For instance, an entity failing to report at all to one entity would be deemed a lower VSL while an entity reporting to many, but failing to report to three entities would be deemed a high VSL. R3 VSL - The severe VSLs do not seem commensurate to oversight. A three month delay in validating that phone numbers are correct, for phone numbers that are accurate, does not track with a severe infraction.
Response: Thank you for your comment. The SDT followed the NERC guidelines for VSLs in setting the appropriate levels. The SDT will forward your suggestions to NERC for future consideration of the VSL language.		
Blue Ridge EMC	No	R3 VSLs are silly.
Response: Thank you for your comment. The SDT followed the NERC guidelines for setting the appropriate VSLs.		
Tacoma Public Utilities	No	Regarding the Severe VSL for R1, the reference to "Parts 1.1 and 1.2" appears to be outdated. For R2, change "the Responsible Entity failed to submit an event report...to X entity(ies) within 24 hours" to "the Responsible Entity failed to submit an event report...to only X entity(ies) within 24 hours." (Add 'only.')
Response: Thank you for your comment. The SDT agrees with your first suggestion and this was correct in the clean version of the standard that was posted. Your second suggestion will be forwarded to NERC for future consideration.		

Organization	Yes or No	Question 2 Comment
SPP Standards Review Group	No	Since EOP-004 is about after-the-fact reporting, we suggest that all the VRFs be Lower. This would mean lowering R2 and R3 from Medium. The third component of the Severe VSL for R2 is more severe than the other two components. In an attempt to be more consistent across all the VSLs, we propose the following for the High VSL for R2: The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 48 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to three or more entities identified in its event reporting Operating Plan within 24 hours. We propose the following, deleting the first two components as shown in the current draft, for the Severe VSL for R2: The Responsible Entity failed to submit a report for an event in EOP-004 Attachment 1.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF. **The VSLs were written to account for tardiness of reports, for failing to report to certain entities and for not submitting a report at all. The investigators will apply the appropriate VSL based on the type of violation found.**		
ERCOT	No	Since EOP-004 is related to ex-post reporting, which has nothing to do with operational or planning risk, this is an administrative requirement and, accordingly, the VRFs should all be Low. This would mean lowering the VRF for R2 and R3 to Low. The third component of the Severe VSL for R2 is more severe than the other two components. In an attempt to be more consistent across all the VSLs, we

Organization	Yes or No	Question 2 Comment
		propose the following for the High VSL for R2: The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 48 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to three or more entities identified in its event reporting Operating Plan within 24 hours. ERCOT proposes that the first two components of the Severe VSL for R2 be deleted and replaced with: The Responsible Entity failed to submit a report for an event in EOP-004 Attachment 1.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF. **The VSLs were written to account for tardiness of reports, for failing to report to certain entities and for not submitting a report at all. The investigators will apply the appropriate VSL based on the type of violation found.**		
Duke Energy	No	The Lower VSL for R3 should be clarified. The phrase "validated 75% or more" should be modified to say "validated at least 75% but less than 100%".
Response: Thank you for your comment. The SDT agrees and has made the correction.		
SERC OC Standards Review Group	No	The VRF for R2 should be "Lower" instead of "Medium" since it is administrative which involves reporting events to entities not identified in the Functional Model that have operating responsibilities listed. The VRF for R3 should also be "Lower" instead of "Medium" since it is an administrative requirement.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC		

Organization	Yes or No	Question 2 Comment
Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.		
Southern Company	No	The VRF for R2 should be "Lower" instead of "Medium" since it is administrative which involves reporting events to entities not identified in the Functional Model that have operating responsibilities listed. The VRF for R3 should also be "Lower" instead of "Medium" since it is an administrative requirement. In addition we suggest that the VSL for R1 should have a lower level VSL for an Operating Plan that may have one event type missing from the Operating Plan.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.		
Cogentrix Energy	No	The VRF for R2 should be "Lower" instead of "Medium" since it is administrative which involves reporting events to entities not identified in the Functional Model that have operating responsibilities listed. The VRF for R3 should also be "Lower" instead of "Medium" since it is an administrative requirement.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a		

Organization	Yes or No	Question 2 Comment
is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.		
Xcel Energy	No	The VSLs for column for R2 provide a range of severity based on the number of contacts made (or not made) but this seems to be arbitrarily defined. A smaller entity may only have two or three contacts so missing one or more here may be a much higher risk than for a larger utility that may have ten or more contacts. The VSLs should be drafted to include percentages instead of whole numbers. The Lower VSL column for R3 states,"...OR The Responsible Entity validated 75% or more of the contact information contained in the operating plan." This could be interpreted that even someone completed 100% (which is more than 75%) a low VSL could be assigned. This VSL should be drafted in similar fashion to the Moderate, High and Severe VSLs and include a range (i.e. less than 100% but more than 75%).
Response: Thank you for your comment. The SDT followed the NERC guidelines for VRFs and VSLs in setting the appropriate levels. The SDT will forward your suggestions to NERC for future consideration.		
Manitoba Hydro	No	This seems like an administrative only requirement. It would be too difficult to validate or measure.
Response: Thank you for your comment. Please see the response to your comment in question 1.		
Independent Electricity System Operator	No	We agree with the VRF for R2, but have a concern over the VRFs assigned to R1 (Lower) and R3 (Medium).Having an event reporting operating plan (R1) is a first step toward meeting the intent of this standard, annually validating it (R3) is a maintenance requirement which arguably can be regarded as equally important but its reliability risk impact for failure to comply should be no higher

Organization	Yes or No	Question 2 Comment
		than having no plan to begin with. We therefore suggest that the VRFs for R1 and R3 be at least the same, or that R1's VRF be higher than that for R3.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.		
Southwest Power Pool RTO	No	We question the reliability benefits of this requirement.
Response: Thank you for your comment. Requirement R3 is in direct response to a FERC directive in Order 693 and as such, the SDT included this provision. If the information in the Operating Plan is out of date, then the plan will not be effective.		
Lewis County PUD	No	
American Electric Power	No	
Response: Thank you for your participation.		
ReliabilityFirst	Yes	Even though ReliabilityFirst votes in the Affirmative, we offer the following comments for consideration regarding the VSLs: VSL for Requirement R2 - ReliabilityFirst questions whether there is justification for the gradation of VSLs out to 60 hours for the reporting an event. Without justification, ReliabilityFirst believes the timeframe should be shortened to eight hour increments with a severe VSL being more than 48 hours late. ReliabilityFirst believes that being more than a day late (24 hours) falls within the entity completely not meeting the intent of submitting the report with the required 24 hour timeframe.
Response: Response: Thank you for your comment. The SDT followed the NERC guidelines for VRFs and VSLs in setting the		

Organization	Yes or No	Question 2 Comment
appropriate levels.		
PNGC Comment Group	Yes	
FirstEnergy	Yes	
Arizona Public Service Company	Yes	
Entergy Services, Inc. (Transmission)	Yes	
Clark Public Utilities	Yes	
Public Service Enterprise Group	Yes	
Idaho Power Co.	Yes	
Ingelside Cogeneration LP	Yes	
Wisconsin Electric Power company dba We Energies	Yes	
Ameren Services	Yes	
South Carolina Electric and Gas	Yes	
Georgia Transmission Corporation	Yes	
City of Austin dba Austin Energy	Yes	
Springfield Utility Board	Yes	
American Public Power Association	Yes	

3. Do you have any other comment, not expressed in the questions above, for the DSR SDT?

Summary Consideration: Most stakeholders who responded to this question provide comments suggesting specific revisions to the requirements or to the event types listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.

Organization	Question 3 Comment
Detroit Edison	"Suspicious activity" and "suspicious device" should be eliminated from Attachment 1, Event types: 'Physical threats to a Facility' and 'Physical threat to a BES Control Center'. By including 'suspicious activity' in the standard, I believe the project team went outside of the scope of the project, which was intended to be a merger of the two standards. Regarding standard CIP 001, the threshold for reporting is “Disturbances or unusual occurrences, suspected or determined to be caused by sabotage....”, as its title suggested: Sabotage Reporting. Suspicious activity, which is not defined by the standard, clearly has a much lower threshold than sabotage, or even suspected sabotage. The reporting requirement of 24 hours, also increases the burden on the entity to either rush to investigate and make a determination regarding suspicious activity in less than 24 hours, or not perform due diligence and report uninvestigated “suspicious” activity, which normally turns out to not be a "Physical Threat”. Suspicious activity should be duly investigated by the entity, local law enforcement, or the FBI as appropriate; and then reported if it has been determined to be a physical threat, or cannot be explained. Reporting within 24 hours will devalue the information inputted, as most cases of suspicious activity are innocuous, and the standard lacks a process of follow up, which would remove the those incidents from intelligence databases. Regarding suspicious devices, determination is usually immediate, (in less than 24 hours), and then the device would be classified as either "sabotage" or "no threat". The standard is not clear whether suspicious devices still have to be reported, even if they are immediately determined as not a "Physical Threat to a Facility or BES Control Center." Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-

Organization	Question 3 Comment
	01) - Reporting Concepts states: The changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). These standards deal exclusively with after-the-fact reporting." Attachment 1 in existing EOP-004-1 is much easier to follow (specifies time requirement to file). Also R2 states DOE OE-417 may be utilized to file reports, however Standard time requirement for update report is 48 hours, OE-417 has changed time requirement on updated filing to 72 hours. Difference can cause confusion and possible penalties. The real time operator must focus on maintaining system reliability. Putting unnecessary reporting obligations on RT puts more importance on the reporting structure than on maintaining reliability. Let 8/5 support personnel perform the reporting tasks and keep the 24/7 on shift operators focusing on the BES.
Response: Thank you for the comment. The SDT disagrees with your position on the inclusion of suspicious activities. Suspicious activities are events and notification of such events is a part of the existing and CIP-001 and EOP-004 standards. Reporting under EOP-004 is for notification purposes only. The standard does not require any analysis of events and does not require any follow up reports as you suggest.	
City of Austin dba Austin Energy	(1) City of Austin dba Austin Energy (AE) requests that the SDT clarify whether R3 requires that each Registered Entity subject to EOP-004-2 verify NERC's contact information each year. It appears this would be overly burdensome for NERC to respond to individual requests. (2) AE also asks that NERC's fax number be included in the contact information at the beginning of Attachment 1 and at the Event Reporting Form in Attachment 2. NERC included the fax number as a viable contact method in its recent NERC Alert notifying the industry of the changed information. (3) AE requests that the SDT increase the threshold for reporting loss of firm load to â‰¥ 300 MW for all entities to align the reporting threshold with the OE-417 threshold. Otherwise, smaller entities would have to report firm load losses between 200 and 299 MW to NERC but not to the DOE. This could be administratively confusing to those responsible for reporting. (4) Attachment 1 lists the threshold for reporting generation loss at â‰¥ 1,000MW for the ERCOT Interconnection. ERCOT planning is based on a single contingency of 1,375MW. For this reason, AE believes the minimum threshold for a

Organization	Question 3 Comment
	disturbance should be greater than the single contingency amount of >1,375MW for the ERCOT Interconnection.
Response: Thank you for your comment. The SDT does not feel it is necessary to specific how the validation occurs and has left this to the entity to determine how to do this. The SDT agrees with the inclusion of the fax number. The SDT will forward the other suggestions to NERC for future consideration. However, it should be noted that these suggestions have not been adopted due to consistency with other standards.	
ACES Power Marketing Standards Collaborators	(1) For the first "Damage or destruction of a Facility" event in Attachment 1, the threshold for reporting should be modified. The threshold for reporting would only include damage or destruction that necessitates the need for action to prevent an Emergency. It does not include if an Emergency actually occurs. Based on the definition of Emergency which states that it is an "abnormal system condition that requires... action to prevent or limit", we think the threshold should be changed to "Damage or destruction of a Facility... that results in a BES Emergency". Per the definition, the Emergency is what necessitates action which is what the threshold appeared to be focused on. (2) In the second "Damage or destruction of a Facility" event in Attachment 1, the threshold regarding "intentional human action" is ambiguous and suffers from the same difficulties as defining sabotage. What constitutes intentional? How do we know something was intentional without a law enforcement investigation? If a car runs into a transmission tower, was this an accident or intentional human action? It could be either. This appears to be the same issue that prevented the drafting team from defining sabotage.(3) Under the "Physical threats to a BES control center" event in Attachment 1, the event should very clearly define if this applies to backup control centers or not. (4) Under the "Complete loss of off-site power to a nuclear generating plant (grid supply)" event" in Attachment 1, the entity with reporting responsibility is not coordinated with NUC-001. NUC-001 used the term transmission entity to mean an entity that is responsible for providing NPIR services. They did not use only TOP because there are other entities that provide this service. Please coordinate the "Entity with Reporting Responsibility" with that standard. (5) We continue to believe that the draft standard has not satisfied the complete scope of the SAR regarding elimination of redundancy. The draft standard will continue to require redundant reporting by various entities. For instance, under the event "Loss of Firm Load" in Attachment

Organization	Question 3 Comment
	1, the DP, TOP, and BA all are required to report. The response to our last set of comments regarding this issue was that "the industry can benefit from having such differing perspectives when events occur". This response seems to confuse event analysis with event reporting. The purpose of the standard is to simply report that an event happened. In fact, the reporting form only requires the submitting entity to report the type of event. The description of what happened is optional. What additional perspectives could be gained from having multiple registered entities in the same electrical footprint report that an event happened. If the purpose is to analyze the event, this is covered in the events analysis process. Furthermore, once NERC becomes aware of the event they have the authority to request data and information from other registered entities. Please eliminate the duplicate reporting requirements. Other events that may require duplicate reporting include: Damage or destruction of a Facility, Physical threats to a Facility, BES Emergency resulting in automatic firm load shedding, Loss of firm load, System separation, Generation loss, and Complete loss of off-site power to a nuclear generating plant.(6) In the second "Damage or destruction of a Facility" event and "Physical Threats to a Facility" events, Distribution Provider should be removed. The Distribution Provider does not have any Facilities which is defined as "a set of electrical equipment that operates as a single Bulk Electric System Element". The DP's transformers interconnecting to the BES are not Facilities and the latest NERC BOT definition explicitly does not include them in Inclusion I1. If a DP did own Facilities, it would be registered as a TO or GO. Inclusion of the DP will compel the DP to provide evidence that it does not have Facilities which is an unnecessary compliance burden that does not support reliability. (7) The "BES Emergency resulting in automatic firm load shedding" should not apply to the DP. In the existing EOP-004 standard, Distribution Provider is not included and the load shed information still gets reported. (8) For the "Voltage deviation on a Facility" event in Attachment 1, we suggest changing "area" in the threshold for reporting to "Transmission Operator Area" as it is a defined term. (9) For the "System separation (islanding)" event, please remove BA. Because islanding and system separation, involve Transmission Facilities automatically being removed from service, this is largely a Transmission Operator issue. This position is further supported by the approval of system restoration standard (EOP-005-2) that gives the responsibility to restore the system to the TOP. (10) The response to our comments requesting that Measure 2 specifically identify that attestations are

Organization	Question 3 Comment
	acceptable forms of evidence to indicate that no events have occurred indicated that the measure cannot permit use of attestations. Other standards that have been recently approved by the board specifically permit the use of attestations. FAC-003-2 M1 and M2, TOP-001-2 M1-M11 and TOP-003-2 M5 all permit the use of attestations. We ask that the drafting team to reconsider including a specific reference that an attestation is acceptable to indicate no event has occurred given these new facts. (11) In requirement R1, we suggest changing "in accordance with EOP-004-2 Attachment 1" to "to report events identified in EOP-004-2 Attachment 1". It makes more sense since the attachment is a list of events that require reporting. The other language sounds like additional requirements will be established in Attachment 1.
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Southwest Power Pool Regional Entity	(1) SPP RE thinks the following Generation reporting threshold is unclear: "Total generation loss, within one minute, of â‰¥ 2,000 MW for entities in the Eastern or Western Interconnection". What has to happen within one minute? It reads as if you have to make a report within one minute. If the intent is that a report has to be made within 24 hours if the loss is for more than one minute it should read, "Total generation loss â‰¥ 2,000 MW for more than one minute for entities in the Eastern or Western Interconnection". What is the intent of the one minute requirement? (2) It appears per R1 that entities are no longer required to include Regional Entities in their reporting chains. SPP RE believes Regional Entities must be included in the reporting chain so they can fulfill their obligations under their delegation agreements. (3) SPP RE thinks this standard was changed substantially enough that it should have been opened for a new ballot pool.

Organization	Question 3 Comment
Response: Thank you for comment. 1) The intent of the "one minute" language is to avoid having to report when a generator has a slow run back rather than a sudden loss. Typically, a unit will trip instantly and the loss will be clear. Other times, the generation will slowly decline and the SDT does not intend for this to be reported. The reporting requirement is to submit a report for an applicable event within 24 hours. 2) Entities are required to report to the ERO only and may submit reports to others, including the RE. The SDT envisions the reports generated through EOP-004-2 act as an input to the Events Analysis Process which includes participation by the Regional Entity. 3) The SDT followed the standards development process which allows significant revision to the standards a long as it proceeds to a successive ballot. The NERC Standard Processes Manual clearly states that a ballot pool stays in place until balloting is completed on a standard. On occasion, the Standards Committee has determined that it is necessary to form a new ballot pool for a project because the ballot pool has been in place for several years and many of the original ballot pool members are no longer available to vote, but this is not the normal practice.	
Ameren Services	(1) This draft refers to a number of activities in the Operations Plan that each entity is to have on hand as the primary guide of actions to be taken when an event occurs. Although there is information related to the requirements that should be included in the Operations Plan, the drafting team has not defined a structure on the format, the minimum information to be included or the direct audience for the Operations Plan. In addition, there is no guidance on the disposition, distribution of the Operations Plan which is left to the entity to determine. We request that the drafting team provide a defined structure for entities concerning the development and implementation of the Operations Plan. (2) Page 14 (Attachment 2) - Voltage Deviation of a Facility - This appears to be a contradiction to VAR-001-2 R10 for TOP which states IROL events will be corrected within 30 minutes. We request the 15 minute reporting criteria be changed to also state 30 minutes. (3) Throughout Document - "Report to the ERO and Regional Entity" - NERC and DHS established the ES-ISAC as a confidential location to report all events that happen on the BES. As these events are of a Sabotage / Disturbance nature, they should all go through the ES-ISAC both as a single location for distribution, and as a best practice that the industry has started. (4) There seems to be some differences between the red-line and clean versions which may need some clarification. For example, (a) In the redline version, the revision history box appears to indicate the inclusion of parts of CIP-008, and in the "Clean" version this has been

Organization	Question 3 Comment
	removed from the revision history box. (b) The red-line version includes a drawing at two places versus once in the clean version. (c) The correlation between the clean and redline documents is not very clear and there appears to be gaps in the reporting and tracking framework structure.
Response: Thank you for comment. 1)-3) Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot. 4) In removing tables and diagrams, the redline version tends to show both the old and new with only a red line down the side of the page. The clean version of the standard is the final version.	
Texas Reliability Entity	(A) Regional Entity should be capitalized in R1. (B) COMMENTS ON ATTACHMENT 1:In the previous comment period on this Standard, Texas RE submitted comments that we feel were not adequately addressed. There were several responses to comments regarding the Events Table that need deeper review and consideration:(1) In the Events Table, under Transmission Loss, the SDT indicated that reporting is triggered only if three or more Transmission Facilities operated by a single TOP are lost. Also, generators that are lost as a result of transmission loss events must be included when counting Facilities. As Texas RE indicated in previous comments to this Standard, determining event reporting requirements by the entity that owns/operates the facility is not an appropriate measure. If the industry wants to learn from events, these types of issues must be addressed. Including the RC as one of the Entity(s) with Reporting Responsibility may alleviate this concern. The RC would have overall view of the system and could provide the reports on multi-element events where the elements are owned/operated by different entities. For the SDT to believe that “There may be times where an entity may wish to report when a threshold has not been reached because of their experience with their system” is worthy to note but falls short of the reliability implications caused by those entities that will not report. The industry needs to learn from events and failure to report will facilitate failure to learn. (2) In the Events Table, under Transmission Loss, there has been considerable discussion

Organization	Question 3 Comment
	recently within the Events Analysis Subcommittee (EAS) regarding the definition of the phrase "contrary to design." The EAS is currently working on possible guidelines to interpret this event type. The SDT may want to consider including the EAS language into the Guidelines and Technical Basis for this Standard. (3) In the Events Table, under "Unplanned BES Control Center evacuation" and "Complete loss of voice communication capability," and "Complete loss of monitoring capability," GOPs should be included. GOPs also operate control centers that would be subject to these kinds of occurrences. As Texas RE indicated in previous comments to this Standard, in CIP-002-5 Attachment 1 there is a "High Impact Rating" for the following: "1.4 Each Control Center, backup Control Center, and associated data centers used to perform the functional obligations of the Generation Operator that includes control 1) for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection or 2) that includes control of one or more of the generation assets that meet criteria 2.3, 2.6, and 2.9." In the ERCOT Region, we experienced an event where a GOP control center lost an ICCP link that carried real-time information regarding its generation fleet (over 10,000 MWs). Without inclusion of the GOP here the event may not get recorded. While it was a "virtual" loss, the impact to the BES through generation control actions could be significant and the event should be reported and analyzed. For the GOP control centers that do exist, the reporting of such events should be a requirement. Based on the minimum of these two examples, why would the SDT NOT include GOP as being applicable? (4) In the Events Table, under "BES Emergency requiring public appeal for load reduction," the definition of Emergency is "Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities...." Is it the intent of the SDT to exclude public appeals issued in anticipation of a possible emergency, before a BES Emergency is officially declared? (5) In the Events Table, under "BES Emergency resulting in automatic firm load shedding," the SDT may want to consider including the RC as one of the Entity(s) with Reporting Responsibility. The RC would have overall view of the system and should provide the reports on events where the multiple entities may be involved. We have UVLS schemes in our region

Organization	Question 3 Comment
	where the total MW shed is greater than 100 MW, but the individual TOP MW shed is less than 100 MW. (6) In the Events Table, consider whether the item for "Voltage deviation on Facility" should also be applicable to GOPs, because a loss of voltage control at a generator (e.g. failure of an automatic voltage regulator or power system stabilizer) could have a similar impact on the BES as other reportable items. Note: We made this comment last time, and the SDT's posted response was non-responsive to this concern. The SDT noted "Further, we note that such events do not rise to the level of notification to the ERO" but the SDT failed to recognize that "Voltage deviation on a Facility" does exactly that - notifies the ERO but from a TOP perspective only. Texas RE is trying to establish the correct Responsible Entity for reporting "Voltage deviation on a Facility" (in this case a generator regardless of the cause and other obligations the owner may have with other Reliability Standards).
Response: Thank you for comment. A) The SDT agrees and has made the correction. B) Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Central Lincoln	1) Central Lincoln must again point out the lack of proportionality for gunshot insulators and similar events under "Damage or destruction of a Facility." Please see our last set of comments. These incidents are fairly common in the west, and typically do not cause an immediate outage. They are generally discovered months after the fact, yet the discovery starts the 24 hour clock running as if the situation had suddenly changed. Prior SDT response: "... this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human." There is already a great lag in awareness regarding the damaged insulator. Months or more can pass prior to discovery by the entity. We fail to see how it becomes so urgent upon discovery. Prior SDT response: "The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan."We do not share the SDT's

Organization	Question 3 Comment
	vision. If an Operating Plan redefined suspected intentional human action so the act of preparing a gun for firing, aligning the sights on an insulator and pulling the trigger was not included, we believe the entity that operates under that plan would be found non-compliant under the language of this standard. We do not offer a simple change in text that will fix the problem, we are only pointing out the problem exists. Murphy dictates discovery will occur at the most inopportune time, which will be during an after hours outage on a stormy holiday weekend night when many employees are out of town and those that are available are already fully engaged. The entity is then faced with choosing to delay restoration or violating the standard. When proposing a zero defect event driven requirement event driven such as this one, we ask the SDT to consider all possible scenarios in which the event may occur. 2) We note that Distribution Providers are listed in the Applicability Section. We also note that there is no requirement in the Statement of Compliance Registry Criteria for Distribution Providers to own or operate BES Facilities, own or operate UFLS or UVLS of 100 MW, or to have load exceeding 200 MW. DP's that cannot meet any of the thresholds of Attachment 1 would still need an Operating Plan under R1 and annually validate the possibly null contact list in its OP under R3. We suggest that DPs that cannot meet the thresholds of Attachment 1 be removed from the Applicability Section.

Response: Thank you for comment. 1) Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.

2) To your suggestion on DPs, the SDT has clarified, in the Guidelines and Technical Basis Section of the standard, that DPs who do not meet the threshold reporting requirements can conduct an annual review of the threshold requirements and be exempted from R1 and R3 for that period. Once the DP has met the threshold reporting requirements, they will then have to comply with the standard.

"Distribution Provider Applicability Discussion

The DSR SDT has included Distribution Providers (DP) as an applicable entity under this standard. The team realizes that not

Organization	Question 3 Comment
	all DPs will own BES Facilities and will not meet the "Threshold for Reporting" for any event listed in Attachment 1. These DPs will not have any reports to submit under Requirement R2. However, these DPs will be responsible for meeting Requirements R1 and R3. The DSR SDT does not intend for these entities to have a detailed Operating Plan to address events that are not applicable to them. In this instance, the DSR SDT intends for the DP to have a very simple Operating Plan that includes a statement that there are no applicable events in Attachment 1 (to meet R1) and that the DP will review the list of events in Attachment 1 each year (to meet R3). The team does not think this will be a burden on any entity as the development and annual validation of the Operating Plan should not take more that 30 minutes on an annual basis. If a DP discovers applicable events during the annual review, it is expected that the DP will develop a more detailed Operating Plan to comply with the requirements of the standard."
Duke Energy	1) There are discrepancies between the red-lined EOP-004-2 and the Clean EOP-004-2 that were posted for this project. Our comments are based upon the Clean EOP-004-2. 2) Attachment 1 and Attachment 2 have the ERO email and phone number listed. If these ever change, does the standard have to go through the revision and balloting process again, or is there an easier way to incorporate such changes? 3) Attachment 1 - When an event occurs that meets the Threshold for Reporting, it's not clear whether all listed entities have to report or not. Several Event Types need this clarity added. For example, if a TOP loses voice communication capability, do both the TOP and RC have to report? 4) Attachment 1 - Damage or destruction of a Facility, applicable to BA, TO, TOP, GO, GOP, DP. The Threshold for Reporting should be further clarified by adding the sentence "Do not report theft or damage unless it degrades normal operation of a Facility." This would eliminate unnecessary reporting of copper theft or vandalism. 5) Attachment 1 - Physical threats to a Facility. The Threshold for Reporting should be modified by deleting the sentence "Do not report theft unless it degrades normal operation of a Facility". This sentence isn't needed here, and fits better with "Damage or destruction of a Facility" as noted in 4) above. 6) Attachment 1 - Transmission loss. This event type should be deleted because it is duplicated

Organization	Question 3 Comment
	under TADS reporting and PRC-004 Protection System Misoperations reporting. 7) Attachment 1 - Unplanned BES control center evacuation, Complete loss of voice communication capability, and Complete loss of monitoring capability. The Threshold for Reporting on all three of these Event Types is 30 minutes, and should be extended to 2 hours, consistent with the transition time identified in EOP-008 "Loss of Control Center Functionality".
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
ERCOT	As a general matter, this standard imposes an ex-post reporting obligation. Consistent with the ongoing P 81 standard review/elimination effort, this standard is arguably a candidate for elimination under the principles guiding that effort. The obligation proposed in the standards are better suited for inclusion in the Rules of Procedure or as a guideline because they are strictly administrative in nature. **Response: On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 ("P81") invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-**

Organization	Question 3 Comment
	004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program. As the SDT is moving forward with a Recirculation Ballot, your suggestions will be forwarded to NERC for future consideration. To the extent the SDT continues to pursue this effort, ERCOT offers the following additional comments. ERCOT has commented on the listing in the Entity with Reporting Responsibility column of Attachment 1. Consistent with those prior comments, the current version still fails to adequately create a bright line threshold for particular events. For example, in the Transmission loss event, although the TOP is listed, there is no direction regarding which TOP is required to file the event report. Is it the TOP in whose TOP area the loss occurred or is it a neighboring TOP who observes the loss? Clearly, the responsibility for reporting lies with the host system, but that responsibility is not clearly designated. There are several other similar events where there is no bright line. We suggest that the drafting team return the deleted language to the Entity with Reporting Responsibility column in those instances where the current version fails to provide a bright line in the Threshold column. Regarding multiple reports for a single event, that aspect of the proposed draft should be revised to only require a single report. While additional information may be available from others, let the Event Analysis team perform their function. This would eliminate the redundant reporting that is currently required as the standard is written. **Response: Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.** ERCOT requests that the reference to “cyber attack” be removed from the Guideline and Technical Basis section of the document since all reporting of cyber events has been removed from the standard and retained in CIP-008. **Response: This correction has been made.**

Organization	Question 3 Comment
Response: Thank you for comment. Please see responses above.	
American Public Power Association	As stated in our comments on the previous draft: It is APPA's opinion that this standard should be removed from the mandatory and enforceable NERC Reliability Standards and turned over to a working group within the NERC technical committees. Timely reporting of this outage data is already mandatory under Section 13(b) of the Federal Energy Administration Act of 1974. There are already civil and criminal penalties for violation of that Act. This standard is a duplicative mandatory reporting requirement with multiple monetary penalties for US registered entities. If this standard is approved, NERC must address this duplication in their filing with FERC. This duplicative reporting and the differences in requirements between DOE-OE-417 and NERC EOP-004-2 require an analysis by FERC of the small entity impact as required by the Regulatory Flexibility of Act of 1980
Response: Thank you for the comment. The SDT does not believe that there is duplicative reporting. The reports that you mention do not go to NERC under the FPA. We will forward your suggestion to NERC for consideration in the preparation of the filing for approval.	
NV Energy	Aside from the comment referring to the new R3 and the term "validate", I applaud the SDT for the improvements made in the remainder of the Standard. This is a much simpler and straightforward approach to meeting the directives in this project and greatly simplifies the processes necessary on the part of the registered entities.
Response: Thank you for your comment.	
CenterPoint Energy	CenterPoint Energy appreciates the revisions made to the draft Standard based on stakeholder feedback and believes that the changes made are positive overall. However, the Company recommends the additional changes noted below for a favorable vote. In the Rationale for R1, CenterPoint Energy recommends that the 2nd sentence in the 1st paragraph be revised as follows, "In addition, these event reports may serve as input to the NERC Events Analysis Program.", as not all events listed in Attachment 1 will serve as input in to the NERC Events Analysis Program. CenterPoint Energy also proposes that the Standard Drafting Team (SDT)

Organization	Question 3 Comment
	add "There cannot be a violation of Requirement R2 without an event." as noted in the Consideration of Issues and Directives to the Requirement. For Attachment 1, CenterPoint Energy recommends the following revisions: CenterPoint Energy continues to be concerned that the uses of the terms “suspicious” and “suspected” are too broad. The Company proposes that the SDT remove the terms from the Thresholds for Reporting or add “which caused a negative impact to the Bulk Electric System” or “that causes an Adverse Reliability Impact..." to each phrase where the terms are used. CenterPoint Energy proposes that the threshold for reporting the event, “BES Emergency requiring manual firm load shedding” is too low. It appears the SDT was attempting to align this threshold with the DOE reporting requirement. However, as the SDT has stated, there are several valid reasons why this should not be done. Therefore, CenterPoint Energy recommends the threshold be revised to “Manual firm load shedding â‰¥ 300 MW”. CenterPoint Energy also recommends a similar revision to the threshold for reporting associated with the “BES Emergency resulting in automatic firm load shedding” event. (“Firm load shedding â‰¥ 300 MW (via automatic under voltage or under frequency load shedding schemes, or SPS/RAS”) For the event of “System separation (islanding)”, CenterPoint Energy believes that 100 MW is inconsequential and proposes 300 MW instead. For “Generation loss”, CenterPoint Energy suggests that the SDT add "only if multiple units” to the criteria of “1,000 MW for entities in the ERCOT or Quebec Interconnection”.
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
PNGC Comment Group	Comments: The PNGC Comment group remains concerned that the “Applicability” section will inadvertently subject Distribution Providers to requirements that they should be excluded from. Please consider the two examples below and note that we’re talking about probably hundreds of small DPs being subject to these unnecessary requirements without any increase to the reliability of the BES. Example 1: Small DP with a peak load of 50 MWs. They have no

Organization	Question 3 Comment
	BES Facilities and their system is radial. Even though this utility will never have a reporting requirement per Attachment A, they are still subject to R1 and R3 plus the associated compliance (read financial) risk for non-conformance. An easy fix to this issue would be for DPs without BES Facilities and with less than 200 MW annual peak load to be excluded in the Applicability section. Example 2: Small DP with a peak load of 50 MWs. Their only BES Facilities are two Automatic UFLS relays that are capable of shedding 15 MWs. DP's Host Balance Authority (HBA) has a peak load of 10,000 MWs, meaning their UFLS plan requires them to have the capacity to shed 3000 MWs should system conditions warrant. Is it the SDT's intent for this DP to have an Operating Plan in place for "damage", "destruction", or "physical threat" for these two relays that are capable of shedding only 15 MWs out of a 3000 MW HBA UFLS plan? The SDT set a 100 MW threshold for reporting of automatic UFLS load shedding so why have reporting requirements for the threat to 15 MWs worth of UFLS relays? Once again the easy fix is to modify the Applicability section. We suggest: 4.1.7. Distribution Provider: with >= 200 MW annual peak load, or;>= 100 MW Automatic firm load shedding

Response: Thank you for comment. To your suggestion on DPs, the SDT has clarified, in the Guidelines and Technical Basis of the Standard, that DPs who do not meet the threshold reporting requirements can conduct an annual review of the threshold requirements and be exempted from R1 and R3 for that period. Once the DP has met the threshold reporting requirements, they will then have to comply with the standard.

"Distribution Provider Applicability Discussion

The DSR SDT has included Distribution Providers (DP) as an applicable entity under this standard. The team realizes that not all DPs will own BES Facilities and will not meet the "Threshold for Reporting" for any event listed in Attachment 1. These DPs will not have any reports to submit under Requirement R2. However, these DPs will be responsible for meeting Requirements R1 and R3. The DSR SDT does not intend for these entities to have a detailed Operating Plan to address events that are not applicable to them. In this instance, the DSR SDT intends for the DP to have a very simple Operating Plan that includes a statement that there are no applicable events in Attachment 1 (to meet R1) and that the DP will review the list of events in Attachment 1 each year (to meet R3). The team does not think this will be a burden on any entity as the development and annual validation of the Operating Plan should not take more that 30 minutes on an annual basis. If a DP discovers applicable events during the annual review, it is expected that the DP will develop a more detailed Operating Plan

Organization	Question 3 Comment
to comply with the requirements of the standard."	
Cowlitz PUD	Cowlitz approves of the improvement efforts on Attachment 1. However, Cowlitz must again point out the fallacy of potentially inundating the ERO with nuisance reporting of minor vandalism and accidental damage. For example, gunshot "target practice" of insulators and structures will apply under "Damage or destruction of a Facility." Such incidents are fairly common in the west, and typically do not cause an immediate outage. They are generally discovered months or years after the fact, yet the discovery starts the 24 hour compliance clock running as if the urgency is just as important as a recent event. If there is already a great lag in awareness regarding the damaged Facility, Cowlitz fails to see how it becomes so urgent upon discovery.----------Again, Cowlitz points out the sentence structure "Damage or destruction of its Facility that results from actual or suspected intentional human action" does not restrict the human action as malicious or sabotage. "Intentional human action" could be innocent, such as a land owner attempting to fall a tree for fire wood. The intent was not to damage the Facility, but the "intentional human action" to obtain fire wood resulted in the damage of the Facility. This does not comport with prior SDT response: "... this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was 'damaged or destroyed' intentionally by a human." Therefore, if this is the SDT's intent Cowlitz suggests this change: Damage or destruction of its Facility that causes immediate impaired operation or loss of the Facility from suspected or actual malicious human intent. Do not report mischievous vandalism, as defined in the Operating Plan, where immediate loss of, or immediate impaired operation of the Facility has not occurred. ----------Prior SDT response: "The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan." Cowlitz does not share the SDT's vision. The Standard as written does not specifically address the ability to "further define" terms used in the Attachment. Past allowance of audit teams to allow registered entity definitions, e.g. "annual," was to address gaps in standards until the standards could be revised. If this is truly the intent of the SDT, then requirement R1 would need revision such as: "The Operating plan shall define what a suspected intentional human action is." Cowlitz respectfully requests that ambiguity be avoided.---------- Cowlitz notes that Distribution Providers are listed in the Applicability Section with no qualifiers. Cowlitz

Organization	Question 3 Comment
	points out that there is no requirement in the Statement of Compliance Registry Criteria for Distribution Providers to own or operate BES Facilities, own or operate UFLS or UVLS of 100 MW, or to have load exceeding 200 MW. DP's that cannot meet any of the thresholds of Attachment 1 would still need an Operating Plan under R1 and annually validate the possibly null contact list in its OP under R3. Cowlitz requests that DPs that cannot meet the thresholds of Attachment 1 be removed from the Applicability Section. Not doing so will increase compliance risk without any reliability return.
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot. **To your suggestion on DPs, the SDT has clarified, in the Guidelines and Technical Basis Section of the Standard, that DPs who do not meet the threshold reporting requirements can conduct an annual review of the threshold requirements and be exempted from R1 and R3 for that period. Once the DP has met the threshold reporting requirements, they will then have to comply with the standard.** **"Distribution Provider Applicability Discussion** **The DSR SDT has included Distribution Providers (DP) as an applicable entity under this standard. The team realizes that not all DPs will own BES Facilities and will not meet the "Threshold for Reporting" for any event listed in Attachment 1. These DPs will not have any reports to submit under Requirement R2. However, these DPs will be responsible for meeting Requirements R1 and R3. The DSR SDT does not intend for these entities to have a detailed Operating Plan to address events that are not applicable to them. In this instance, the DSR SDT intends for the DP to have a very simple Operating Plan that includes a statement that there are no applicable events in Attachment 1 (to meet R1) and that the DP will review the list of events in Attachment 1 each year (to meet R3). The team does not think this will be a burden on any entity as the development and annual validation of the Operating Plan should not take more that 30 minutes on an annual basis. If a DP discovers applicable events during the annual review, it is expected that the DP will develop a more detailed Operating Plan to comply with the requirements of the standard."**	
Wisconsin Electric Power company	Damage or destruction of a Facility, Damage or destruction of its Facility that results from

Organization	Question 3 Comment
dba We Energies	actual or suspected intentional human action.: By the Functional Model, I do not believe the BA function has Facilities by the NERC Glossary definition. This would not apply to a BA. The line above this would adequately cover BA reporting. Remove a BA from applicability for this line. Physical threats to a Facility: The BA function does not have Facilities. Remove a BA from applicability for this line. There could be a separate line for Physical Threats to a Facility within an RC, FOP, BA Area as there is for Damage or Destruction of a Facility. Voltage deviation on a Facility: Please specify what voltage this is, nominal, rated, etc. This should also be > 10% deviation. Exactly at 10% could be at the edge of an allowed range.
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Manitoba Hydro	Does the Background, Guidelines and Technical Basis form part of the standard itself once published? Or are these just parts of the package that accompany the standard during circulation for comment? **The background, guidance and technical basis will remain with the standard and provides clarification on the SDT's intent and direction** Compliance 1.2: The reference to Responsible Entity is bracketed and in lowercase. We are not clear why. **This was corrected in the clean version.** VSLs, R1, Severe VSL: The words "in the event reporting Operating Plan" are missing from the end of this sentence. **This was corrected in the clean version.**

Organization	Question 3 Comment
	VSLS, R2, Lower VSL: The violation occurs if the Responsible Entity has submitted an event report to one entity whereas Moderate VSL, High VSL and Severe VSL, the level of severity of the VSL increases depending on the number of entities that the Responsible Entity fails to submit an event report to. The drafting here is not as precise as it should be. The way the Lower VSL is written, it will also be triggered when the Responsible Entity has complied with the requirement. For example, if the Responsible Entity is required to report an event to 5 entities, and it does, it will still mean that it has "submitted an event report to one entity identified in the event reporting (also, the 'ing' is missing on the Lower VSL reference)Operating Plan". It is also duplicative. For example, if the Responsible Entity submitted a report to only one entity, and failed to submit a report to 4 others, they fall under the Lower VSL and the Higher VSL (we are assuming in this case, the violation will be found to be the higher VSL). Perhaps what the drafting team intended to do was to make the Lower VSL, which the Responsible Entity failed to submit an event report...to one entity identified.... **The SDT followed the NERC guidelines for VSLs in setting the appropriate levels. The VSLs were written based on two potential failures to meet the requirement. The first is based on the time the report was submitted while the second was based on the entity submitting the report within 24 hours but not to all applicable entities. If a violation is determined, it will be for either being late with the report or for not submitting the report to everyone. The appropriate VSL will be applied ONLY if a violation is found.** The Guidelines and Technical Basis contain a reference to R4 which no longer exists in the standard. **This reference has been removed.**
Response: Thank you for comment. Please see responses above.	
Dominion	Dominion reads Requirement R1 as explicitly requiring only the inclusion of reporting to the ERO in the Operating Plan. We acknowledge that the requirement also contains additional entities in parenthesis which infers the inclusion of a larger group (and which appears to be supported by the rationale box). Dominion suggests the SDT explicitly state which entities, at a minimum, be included, for reporting, in the Operating Plan. We suggest adding a column to

Organization	Question 3 Comment
	Attachment 1 and including entities to which the event must be reported. As an examples; o All event types should include local law enforcement o Events for which the BA, RC, TOP bear responsibility should probably also be reported to the regional entity o Events for which the Facility Owner bears responsibility should probably also be reported to the respective BA and TOP, who would in turn determine whether to notify their respective RC. The RC would in turn determine if additional entities need to be contacted. Requirement R2 establishes a 24 hour reporting threshold; however, the "NOTE" provided on Attachment 1 seems to contradict Requirement 2 and could therefore lead to compliance issues. Dominion suggests that Requirement R2 be revised to agree with the "NOTE" on Attachment 1. For example, Requirement R2 could be reworded as: Except as noted on Attachment 1, Each Responsible Entity shall...Also under the "NOTE" in Attachment 1, why has the facsimile number for the ERO been removed? The DOE still provides a facsimile number for reporting. Attachment 2: Event Reporting Form #4; need to update the below to reflect the same naming convention of the events in Attachment 1, the "t" should not be capitalized in Physical Threat and add an 's' behind threat. Add (islanding) behind System separation and capitalize the 'U' in unplanned control center evacuation.
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Southern Company	**NOTE: The SDT received assistance from Southern Company personnel in parsing these comments as show below. As submitted, the formatting of the original comments was lost and very difficult for the SDT to read and understand.** Event Type Entity with Reporting Responsibility Threshold for Reporting SOCO Comment: **Damage or destruction of a Facility** RC, BA, TOP Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area, excluding weather or natural disaster related threats, that results in actions to avoid a BES

Organization	Question 3 Comment
	Emergency. – No Comment **Damage or destruction of a Facility** BA, TO, TOP, GO, GOP, DP Damage or destruction of its Facility that results from actual or suspected intentional human action.: Do not report damage unless it degrades normal operation of a Facility. How does the SDT define "intentional human action?" Further, how is the phrase "suspected intentional human action" defined? This phrase is very broad. Is "intentional human action" identified as actions intended to damage facilities or does it include accidental actions by individuals? For example, if a person accidentally shot insulators off of a 230 kV line resulting in damage, would that be considered reportable "intentional human action?" In addition, what is that actual trigger for reporting? Does it require that the action has been discovered or is it from the time the event occurs? Further, 24 hours is a very brief time period -- how is an entity to conduct an investigation within that time period to determine if damage or destruction could have resulted from "actual or suspected" human action and also determine if it could have been "intentional"? In Southern's cases, and likely in other entities case, operating personnel submit the reports to the regulatory entities for events that fall under this standard. Southern is concerned, that the threshold for reporting for "Damage or destruction of a Facility" and "Physical threats to a Facility" is so broad that numerous reports would need to be filed that 1) may be a result of something that does not pose harm to reliability and should not be of interest to the regulators, and 2) would introduce additional burden to operating personnel that are monitoring the system every moment of the day. With the current proposed "Threshold for Reporting", the reporting requirement would hamper the ability of system operating personnel to perform their core real-time system operator tasks which would harm reliability. **Physical threats to a Facility** BA, TO, TOP, GO, GOP, DP Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. OR Suspicious device or activity at a Facility. Do not report theft

Organization	Question 3 Comment
	unless it degrades normal operation of a Facility. Please provide some clarity as to what is considered suspicious activity. For example, would someone taking a photo of a BES substation fall into this category? Please provide examples of what may be considered suspicious activity and how NERC and others may use this information and what actions they would take as a result of receiving this information. In addition, what is that actual trigger for reporting? Is it when the threat is discovered or from when it should have or could have been discovered? Further, 24 hours is a very brief time period -- how is an entity to conduct an investigation within that time period in order to determine if the physical threat has the potential to degrade the normal operation of the Facility or that the "suspicious activity"? **Physical threats to a BES control center** RC, BA, TOP Physical threat to its BES control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. OR Suspicious device or activity at a BES control center. – No Comment **BES Emergency requiring public appeal for load reduction** Initiating entity is responsible for reporting. Public appeal for load reduction event. It is unclear which entity would be responsible for reporting this event. For example, if the RC/TOP/BA were to identify the need to do this and instruct an LSE to issue the public appeal, who would report the event? **BES Emergency requiring system-wide voltage reduction** Initiating entity is responsible for reporting System wide voltage reduction of 3% or more. It is unclear which entity would be responsible for reporting this event. For example, if the RC were to identify the need to do this and instruct a TOP to reduce voltage, who would report the event? **BES Emergency requiring manual firm load shedding** Initiating entity is responsible for reporting Manual firm load shedding â‰¥ 100 MW. – No Comment

Organization	Question 3 Comment
	BES Emergency resulting in automatic firm load shedding DP, TOP Automatic firm load shedding â‰¥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS). – No Comment **Voltage deviation on a Facility** TOP Observed within its area a voltage deviation of ± 10% of nominal voltage sustained for >or= 15 continuous minutes. Please change “nominal” to “expected” or “scheduled” **IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only)** RC Operate outside the IROL for time greater than IROL Tv (all Interconnections) or Operate outside the SOL for more than 30 minutes for Major WECC Transfer Paths (WECC only). – No Comment **Loss of firm load** BA, TOP, DP Loss of firm load due to equipment failures/system operational actions for >or= 15 Minutes: >or= 300 MW for entities with previous year’s demand >or= 3,000 MW OR >or= 200 MW for all other entities This should not be as a result of weather or natural disasters. **System separation(islanding)** RC, BA, TOP Each separation resulting in an island â‰¥ 100 MW – No Comment **Generation loss** BA, GOP Total generation loss, within one minute, of â‰¥ 2,000 MW for entities in the Eastern or Western Interconnection OR â‰¥ 1,000 MW for entities in the ERCOT or Quebec Interconnection – No Comment **Complete loss of off-site power to a nuclear generating plant (grid supply)** TO, TOP Complete loss of off-site power affecting a nuclear generating station per the Nuclear Plant Interface Requirement – No Comment **Transmission loss** TOP Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing). – No Comment **Unplanned BES control center evacuation** RC, BA, TOP Unplanned evacuation from BES control center facility for 30 continuous minutes or more. – No Comment

Organization	Question 3 Comment
	Complete loss of voice communication capability RC, BA, TOP Complete loss of voice communication capability affecting a BES control center for 30 continuous minutes or more. – No Comment **Complete loss of monitoring capability** RC, BA, TOP Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (i.e., State Estimator or Contingency Analysis) is rendered inoperable. – No Comment **Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.**Guideline and Technical Basis Comments In the Summary of Key Concepts section of the Guideline and Technical Basis, the DSR SDT explains that the proposed Standard does not include any real-time operating notifications for events listed in Attachment 1. The DSR SDT should consider language in the Standard which codifies this approach. Southern Company notes that the proposed standard does not mention any exclusion of real-time notification. **Response: The SDT does not believe that this revision is necessary as the requirement R2 clearly states that events are to be reported within 24 hours.** The Law Enforcement Reporting section of the Guideline and Technical Basis unintentionally expands on the purpose of the Standard by stating that "The Standard is intended to reduce the risk of Cascading events." The stated purpose of the Standard is "To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities." The phrase in the Guideline should be removed or modified in order to avoid any uncertainty about the Standard's purpose. **Response: The SDT has made the requested clarification to the Guidelines and Technical Basis section.**

Organization	Question 3 Comment
	The DSR SDT should consider integrating the content of the Concept Paper into the Guideline and Technical Basis. Presently, the Concept Paper appears as an add-on at the end of the document. When the Concept Paper existed as a stand-alone document, various segments such as "Introduction" and "Summary of Concepts and Assumptions" were helpful to stakeholders and standards developers. The revised merged document in the present draft does not need two separate sections addressing concepts nor does it need an introduction at the midway point. Additionally, two other areas are either duplicative or contribute to ambiguity within the supplemental information. First, it is not clear that the segment on Concepts and Assumptions includes any actual assumptions. The section should be modified or deleted to address this concern. Second, the segment entitled 'What about sabotage?' seems to contain topics similar to those on the first page of the Guideline. Again, the DSR SDT should consider integrating all of the necessary information into a more comprehensive document. **Response: The SDT has chosen to leave these sections in tact because it helps convey the development process as well as the information about the team's insights.**
Response: Thank you for comment. Please see responses above.	
FirstEnergy	FirstEnergy Corp (FE) appreciates the work done by the SDT by incorporating the comments and revisions from the previous draft. FE would like to see the time parameters in Requirement 3 and Measure 3 to be changed from "each calendar year" to "at least once every 12 months". This is similar to the wording that is being used in the CIP standards
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Oncor Electric Delivery	For reporting consistency, under the Event Type labeled "Generation Loss", in Appendix 1 of EOP-004-2, Oncor recommends that the reporting threshold of 1,000 KW for the ERCOT Interconnection be raised to 1,400 MW to match the 1,000 MW level in the current version of

Organization	Question 3 Comment
	the ERO Event Analysis Program. Under the Event Type labeled "Damage or Destruction of a "Facility", Appendix 1, with the threshold that states," Damage or destruction of its Facility that results from actual or suspected intentional human action", Oncor suggest the addition of the following language to address intentional human action that is theft in nature but is not intended to disrupt the normal operation of the BES: "Do not report theft unless it degrades the normal operation of a Facility."
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Georgia Transmission Corporation	GTC recommends a minor change to Attachment 2 associated with the complete loss of off-site power to nuclear generating plant. NUC-001-2 R9.3.5 describes provisions for restoration of off-site power and applies to both the Nuclear Plant Generator Operator and the applicable Transmission Entities. To maintain consistency, GTC recommends modification to this row in EOP-004-2 Attachment 2 such that the "Nuclear Plant Generator Operator" is the Responsible Entity with reporting responsibility. (A TO may not have visibility to all off-site power resources for a nuclear generating plant if multiple TO's are providing off-site power.)At a minimum, GTC recommends if the SDT believes the TO and TOP should remain involved, these entities should be limited to "TO and TOP that are responsible for providing services related to Nuclear Plant Interface Requirements (NPIRs)" which is also consistent with NUC-001-2.
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	

Organization	Question 3 Comment
South Carolina Electric and Gas	Has the drafting team considered how reports from R2 tie in with reports required by the NERC Event Analysis process? It appears that reporting deadlines conflict between the two. The SDT should clarify that the event types "Damage or Destruction" listed in attachment 1 do not pertain to "cyber events", to avoid duplication of the CIP-008 requirements.
Response: Thank you for comment. Reporting under this standard is for the notification of events to the NERC Situation Awareness Group. Reports in this standard can be the initial reports for the EA group, but are not designed to address the balance of the EA program. The SDT had removed the cyber security obligations in this draft.	
Xcel Energy	In attachment one, the "Threshold for Reporting" under Damage or Destruction of a Facility appears to closely follow the definition of sabotage that EOP-004-2 says it is trying to do away with. This definition should be drafted to better correlate with the other physical threats and include the language, "which has the potential to degrade the normal operation of the Facility". Additionally in Attachment 1, both the Physical threats to a Facility and Physical threats to a BES control center include the wording, "Suspicious device or activity...". What constitutes suspicious activity? With no definition this interpretation is left to the Entity which is again something the DSR SDT says they would like to eliminate. Lastly, in the Guideline and Technical Basis section, under A Reporting Process Solution - EOP-004 it states, "A proposal discussed with the FBI, FERC Staff, NERC Standards Project Coordinator and the SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Reportable Events). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial or local level law enforcement agency. The state or provincial or local level law enforcement agency will coordinate with law enforcement with jurisdiction to investigate. If the state or provincial or local level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial or local level law enforcement agency will notify and coordinate with the FBI or the RCMP." This appears to be in direct conflict with the Rationale for R1 which states, "An existing procedure that meets the requirements of CIP-001-2a may be included in this Operating Plan along with other processes, procedures or plans to meet this requirement."

Organization	Question 3 Comment
	CIP-001-2a required "communication contacts, as applicable, with local Federal Bureau of Investigation (FBI)..." so if the CIP-001-2a procedure is included this does not seem to meet the requirements of the operating plan required under EOP-004-2. Also, if the intent of the Operating Plan is to include all local law enforcement and not FBI the operating plan would become very detailed and when validated annually as required in R3, this becomes very burdensome on an entity.
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
American Electric Power	In the spirit of Paragraph 81 efforts, we request the removal of R1. R1 is administrative in nature, existing only to support R2. Reporting an event externally might necessitate the need for a plan/procedure/policy/job aide, but requiring it is an overreach. Having two requirements rather than one increases the likelihood of being found non-compliant for multiple requirements rather than a single requirement. The Paragraph 81 project team has already recommended removing the requirement to have contact information with law enforcement from CIP-001 R4. Notwithstanding our comments above, we recommend removing the phrase "and other organizations..." from R1. If this requirement is to remain, it needs to be very specific regarding who needs to be included in the reporting.R2 – We recommend removing "per their Operating Plan" from R2 so it reads "Each Responsible Entity shall report events within 24 hours of meeting an event type threshold for reporting." If an entity deviates from its plan but still meets the intent of the requirement (e.g. reporting to NERC with 24 hours), this could be viewed as a finding of non-compliance. We need to get away from "compliance for compliance's sake", and focus solely on those efforts which will benefit the reliability of the BES. Attachment 1 Page 13, Row 1 (Clean Version): This is too open-ended and would likely lead to voluminous reporting. As it currently reads, "Damage or destruction of a Facility within its

Organization	Question 3 Comment
	Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in actions to avoid a BES Emergency" could bring all copper thefts into scope. Thefts should not need to be reported unless the theft results in reliability concerns as specified by other criteria or parameters in Attachment 1. Attachment 1 Page 13, Row 2 (Clean Version): The threshold "Damage or destruction of its Facility that results from actual or suspected intentional human action" should be eliminated entirely. For the event Damage or destruction of a Facility, the threshold for reporting is set too low. Attachment 1 Page 13, Row 3 (Clean Version): We suggest modifying the text to read "Do not report theft... unless the theft results in reliability concerns as specified by other criteria or parameters in Attachment 1." Attachment 1 Page 14, Row 4 (Clean Version): Regarding "Loss of Firm Load", we suggest making it clear that the MW threshold is an aggregate value for those entities whose TOP is responsible for multiple operating companies or legal entities. In addition, is it necessary to include the DP as an entity with reporting responsibility? Its inclusion could create confusion by further segmenting the established threshold. Attachment 1 Page 15, Row 1 (Clean Version): Including "Transmission loss" as currently drafted would result in much more reporting than is necessary or warranted. As currently drafted, it could bring more events into scope than intended, especially for larger entities. EOP-004 Attachment 2: Event Reporting Form: AEP remains concerned that industry would be required to report similar information to multiple Federal entities, in this case to both NERC (Attachment 2) and the DOE (OE-417). In addition, the reporting requirement are not clear for every kind of event as to which entity the reports must be forwarded to, and it is unclear how information would be passed to other entities as necessary. EOP-004 Attachment 2: Event Reporting Form: This form is a further example of mixing security concepts with operational concepts. Not only is not advisable, it does not serve the interests of either concept.

Organization	Question 3 Comment
Response: Thank you for your comment. On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 ("P81") invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program. As the SDT is moving forward with a Recirculation Ballot, your suggestions will be forwarded to NERC for future consideration. As the Paragraph 81 efforts are beyond the scope of this project, the SDT can only pass along your suggestion to that project team for action there. **Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.**	
Midwest Independent Transmission System Operator, Inc.	MISO respectfully submits that several of the thresholds for reporting in EOP-004 - Attachment 1 should be modified to clarify when the reporting obligation is triggered, and to ensure that entities are reporting events of the type and significance intended. In particular, MISO focuses on the following draft thresholds in EOP-004 - Attachment 1: o The requirement that an entity report when "[d]amage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in actions to avoid a BES Emergency." A BES Emergency is defined as "Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System."RCs and BAs take actions each and every day to "avoid a BES Emergency." At the time of those actions, they are reacting to conditions that their operating personnel are observing on the

Organization	Question 3 Comment
	BES. There is no way for an RC or a BA to discern whether the conditions to which they reacted resulted from the "damage or destruction of a Facility" and there is no requirement for Transmission Operators and/or Owners to report "damage or destruction of a Facility" to their BA or RC. Accordingly, RCs and BAs will likely, often not be sufficiently informed to determine if their actions require them to submit a report. Responsible entities are likely to expend significant time and resources reporting daily operations and actions routinely taken to respond to observed BES conditions as they present themselves. These actions may be in response to congestion, equipment outages, relay malfunctions, etc. Whether or not the initiating factor was "damage to or destruction of a Facility" will often be an unknown factor and - even if such is known - the genesis of that damage and/or what constitutes damage (as discussed below) present further potential for confusion and over-reporting, Nonetheless, the lack of clarity in the standard is likely to result in some RCs and BAs preparing reports whether or not they definitely ascertain the underlying cause for the system conditions that prompted them to take actions "to avoid a BES Emergency." The preparation and submission of such reports, in many cases, will not facilitate the stated objective of this standard, which is the improvement of the reliability of the Bulk Electric System. In addition, with respect to damage or destruction of a Facility, it is debatable as to what would be considered "damage." For example, would an improper repair or outage that results in damage to a Facility that requires a more extended repair or outage be deemed "damage" to that Facility under this standard? These ambiguities will likely result in significant over-reporting, over-burdening responsible entities, and inundating Regional Entities and NERC with information that is not useful for the purpose of facilitating the reliable operation of the Bulk Electric System. These effects would undermine the express purpose of the standard and the potential value of information if the reporting obligations are appropriately defined, assigned, and scoped. For these reasons, MISO recommends that the SDT revise the standard to: (1) remove the requirement for RCs and BAs to report the "damage or destruction of a Facility" as it is redundant of the immediately subsequent requirement, (2) to remove reporting responsibility from BAs to report the "damage or destruction of a Facility" as this obligation is more properly placed with the TO, TOP, GO , GOP, and DP, and (3) provide guidance to the remaining responsible entities, TO, TOP, GO , GOP, and DP, regarding when "damage" to a Facility should be reported, e.g., an illustrative list of the types of "damage" that would yield information and/or trends that

Organization	Question 3 Comment
	would facilitate the improvement of the reliability of the BES. o The requirement to report "[p]hysical threats to a Facility" and/or "[p]hysical threats to a BES Control Center"With respect to physical threats to Facilities or BES Control Centers, what is considered a "physical threat" and/or a "suspicious device or activity"? Is a crank call count that the building is on fire a physical threat? Is the return of a disgruntled employee suspicious? MISO understands and supports the reporting and analysis of threats and even certain types of suspicious activities, etc. It is merely concerned that the reporting threshold expressed in this standard will result in the reporting of substantial amounts of data that will not facilitate the improvement of the reliability of the BES and that the volume of reports may delay or otherwise obscure the detection of notable trends. Accordingly, MISO recommends that the SDT revise the standard to: (1) require the reporting only of substantial physical threats that are likely to have an adverse impact on the reliable operation of the Bulk Electric System, and (2) to provide an illustrative list of the types of "suspicious activity or devices" as guidance to responsible entities. o Timing of reports Finally, MISO respectfully suggests that NERC re-assess the timing requirements as related to the objectives expressed within this standard. MISO believes that NERC should clarify that its "situational awareness" staff will review submitted information to determine whether there are indications of possible coordinated attack and to quickly inform responsible entities that there are signals of possible coordinated attack. This clarification could be made in the standard, or the standard could describe the process that NERC staff will use. Unless such review and information is provided, the need that the standard attempts to address will not be fully met. Conversely, many of the events listed in Attachment A that require reporting do not need to be reported within 24 hours and would not offer significant benefit or value if reported within that time period as NERC and Regional Entities primarily utilize such information to capture metrics or perform after-the-fact events analysis. Accordingly, MISO respectfully suggests that, while performing analysis to determine clarifications that would result in the appropriate definition, assignment, and scope of reporting obligations, NERC should also examine the events and identify those events for which a longer time period for reporting would be suitable. This would significantly reduce the administrative burden on responsible entities and likely result in more comprehensive,

Organization	Question 3 Comment
	rigorous, and beneficial reporting.
Response: Thank you for your comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Indiana Municipal Power Agency	On page 6 of 23 of the draft standard document, second paragraph under Rationale for R1, the SDT uses the words "Every industry participant that owns or operates elements or devices on the grid has a formal or informal process..." The use of these words implies that this requirement and others in this standard may apply to every industry entity regardless if they are a registered entity or not. IMPA understands that standards can only apply to entities that are registered with NERC, but we still prefer to see different wording in this sentence. IMPA recommends using "Every registered entity that owns or operates elements or devices on the grid has a formal or informal process..." **We have revised "industry participants" to Registered Entity".** Another concern is on pages 18, 19, and 20 of 23. It is not clear what exactly is required of a registered entity and the law enforcement reporting process. IMPA understands it is up to the entity to decide just how its event reporting Operating Plan is made up and who is contacted for the events in attachment 1. These pages are confusing when it comes to the listing of stakeholders in the reporting process on page 18 of 23 and then when the SDT states that an entity may just notify the state or provincial or local level law enforcement agency. The SDT needs to clarify that the listing of stakeholders on page 18 of 23 is just a suggestive listing and that if the entity so decides per its reporting Operating Plan that notification of the local law enforcement agency is sufficient (the thought that the local law enforcement agency can coordinate with additional law enforcement agencies if it sees the need). The requirement to contact the FBI in CIP-001 is not a requirement in EOP-004-2 unless the registered entity puts that requirement in its event reporting Operating Plan. **The information on law enforcement in the Guidelines and Technical Basis section is**

Organization	Question 3 Comment
	designed to provide *one* example of how an entity *could* report to law enforcement. It is not intended to be the *only* possible way. As a clarification, in the Background section's second paragraph, it should read "retiring both EOP-004-1 and CIP-001-2a" as opposed to CIP-002-2a as written above in this comment document. **We have searched the comment form and cannot find this.**
Response: Thank you for your comment. Please see responses above.	
Cogentrix Energy	Overall: The standard makes good stride in eliminating the redundancy of CIP-001 and EOP-004. M1 States: "... and each organization identified to receive an event report for event types specified in EOP-004-2 Attachment 1". It is an unclear in the statement that the protocols go with Attachment 1 and entities to receive report are part of Attachment 2While this draft is an improvement on the previous draft, the proposed R2 is unacceptable, and should be amended to, at a minimum, require reporting by the end of the next business day, instead of within 24 hours. Events or situations affecting real time reliability to the system already are required to be reported to appropriate Functional Entities that have the responsibility to take action. Adding one more responsibility to system operators increases the operator's burden, which reduces the operator's effectiveness when operating the system. Care should be given when placing additional responsibility on the system operators. Allowing reporting at the end of the next business day gives operators the flexibility to allow support staff to assist with after-the-fact reporting requirements. For some event types where in order to provide real time situational awareness over a wide area (for example coordinated sabotage event) it may be appropriate to have more timely reporting. If the intent of this standard is to address sabotage reporting there needs to be an understanding of the actions to be taken by those receiving the reports so the reporting entities can incorporate those actions into their plan. As a minimum, NERC should have a process in place to assess the reports and take appropriate actions. Attachment 1: Threshold for reporting should not be defined such that multiple reports would be required for the same event. For example, both the TOP and RC being required to report

Organization	Question 3 Comment
	the outage of a transmission line. 2nd event type (Damage or destruction of a Facility): Add the following sentence to the Threshold for Reporting: "Do not report theft or damage unless it degrades normal operation of a Facility." 4th event type (Physical threats to a BES control center): The term "BES control center" needs to be clarified. 5th, 6th, and 7th event types: In instances where a reliability directive is issued, is the "initiating entity" the entity that issues the directive or the entity that carried out the directive. 9th event type (Voltage deviation on a Facility): Change "nominal" to "expected or scheduled." 15th event type (Transmission loss): It is not clear what is meant by "contrary to design." This is so broad that it could be interpreted as requiring reporting misoperations within the reporting time frame before even an initial investigation can begin. This needs to be clarified and tied to the impact on the reliability of the BES.
Response: Thank you for your comment. The full Measure M1 states: "Each Responsible Entity will have a dated event reporting Operating Plan that includes, but is not limited to the protocol(s) and each organization identified to receive an event report for event types specified in EOP-004-2 Attachment 1 and in accordance with the entity responsible for reporting." It is expected that the Operating Plan will contain the entities to which a report will be submitted. The Measure indicates evidence needs to be provided showing that these entities received the event report. The protocol(s) refer to the Operating Plan and could include any procedures for identification of events as well as communicating to other entities. **In response to your suggestion on Requirement R2, the DSR SDT has added clarifying language to R2 as follows:** **R2. Each Responsible Entity shall report events per their Operating Plan within 24 hours of meeting an event type threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). [Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]** **Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation**	

Organization	Question 3 Comment
ballot.	
Northeast Power Coordinating Council	Paragraph 81 efforts are underway to eliminate requirements that have little or no reliability benefit. This Standard only addresses documentation and has no impact on reliability.
Response: Thank you for your comment. On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 ("P81") invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program. As the Paragraph 81 efforts are beyond the scope of this project, the SDT can only pass along your suggestion to that project team for action there.	
Puget Sound Energy Inc.	Puget Sound Energy appreciates the Standard Drafting Team's work to streamline and clarify the proposed standard. In addition, we understand that the Standard Drafting Team faces a significant challenge in developing workable thresholds for reporting under this standard. Unfortunately, Puget Sound Energy cannot support the proposed standard because the reporting thresholds remain too vague and, thus, too broad - especially those related to damage or destruction of a Facility and those related to physical threats. The first four events listed on Attachment 1 are not brightline rules, because they each involve significant elements of judgment and interpretation. An example of our concern relates to the phrase "... that results from actual or suspected intentional human action." Puget Sound Energy, like many regulated entities, is staffed only with System Operators at night and on weekends. As a result, the 24-hour reporting requirement necessarily requires the System Operators to submit the required reports. So, how is a System Operator going to judge whether a human action is "intentional"? As a result, it will be necessary to report any event in which human action is

Organization	Question 3 Comment
	involved because there is no way for a System Operator to know for sure whether the action is intentional or not. And, regulated entities will need to instruct their System Operators to make such reports, because the failure to submit a report of even one event listed in EOP-004 Attachment 1 is assigned a severe VSL under the proposed standard. We believe that the proposed threshold language will likely result in a flood of event reports that will not improve situation awareness.
Response: Thank you for your comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot. **In response to your concern on the 24-hour reporting requirement, the DSR SDT has added clarifying language to R2 as follows:** **R2. Each Responsible Entity shall report events per their Operating Plan within 24 hours of recognition of meeting an event type threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). [Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]**	
Exelon Corporation and its affiliates	Thanks to the drafting team for all the work on this revision. Significant progress was made, though Exelon has some remaining comments: o It's not clear why the team separated 'Damage or destruction of a Facility' into two rows. Please advise. **Response: The first row applies to the RC, which may not own any Facilities but has them under their operational control. This event applies to damage or destruction whereby the RC, TOP or BA has to take action to avoid a BES Emergency. The second row is simply damage or destruction of a Facility. It is expected that this second type of event would not be severe enough to have to take action to avoid a BES Emergency.** o Damage or destruction of a Facility - The threshold for "damage or destruction of a Facility"

Organization	Question 3 Comment
	is too open-ended without qualifying the device or activity as “confirmed”. Event reporting for nuclear generating units are initiated when an incident such as tampering is "confirmed". EOP-004 should include some threshold of proof for a reason to believe that no other possibility exists for "damage or destruction of a facility" event other than actual or suspected intentional human action. **Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.** o Physical threats to a Facility - Reporting of every “suspicious activity” such as photographing equipment or site could result in an unwieldy volume of reports and dilute the data from depicting quality insight. For example, nuclear generating units are required to report all unauthorized and/or suspicious activity to the NRC. Please confirm that the intent of this threshold for notification would include all unauthorized and/or suspicious activity. **The SDT concurs that the intent of the threshold for notification would include all unauthorized and/or suspicious activity.** o Physical threats to a BES control center - please confirm that reporting responsibility falls to the RC, BA, TOP and not GOs. In addition, please confirm that by use of the lower case “control center” other definitions in development through other standards development projects (e.g. CIP version 5) and that may be added to the NERC Glossary will not apply until formally vetted in a future EOP-004 standards development project. **The entities listed for this event type are the RC, BA and TOP only. No other entities are applicable for this event type. If the lower case “control center” is replaced by a definition developed in future standards actions, a change to EOP-004-2 to use the defined term would require notice to the industry and a ballot of the revised standard in some manner. The DSR**

Organization	Question 3 Comment
	SDT does not have control over how that would be accomplished. o Loss of firm load - "Loss of firm load for â‰¥ 15 Minutes: â‰¥ 300 MW for entities with previous year's demand â‰¥ 3,000 MW". Please clarify whether the team intends for this to apply to a single event a loss of more than 300 MW due to non-concurrent multiple distribution outages that total > 300MW. **This event relates to a single incident of the loss of firm load.** o Generation loss - Exelon appreciates the timing clarification added to the generation loss threshold. The phrase "within one minute" should also be included in the threshold for the ERCOT and Quebec Interconnections to read: "Total generation loss, within one minute, of â‰¥ 2,000 MW for entities in the Eastern or Western Interconnection OR Total generation loss, within one minute, of â‰¥ 1,000 MW for entities in the ERCOT or Quebec Interconnection" **The phrase "within one minute" applies to everything listed in the event. To clarify this, we have inserted a colon after the word "of" and moved "≥ 2,000 MW for entities in the Eastern or Western Interconnection" down one line.** o The Law Enforcement Reporting section in the Guideline and Technical Basis states: "The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of the BES from malicious physical or cyber attack." Since CIP-008 now covers reporting of cyber incidents the reference to cyber should be removed. **We have made the correction in your last point regarding "cyber attacks" and have removed it from the Guidelines and Technical Basis section.**
Response: Thank you for your comment. Please see responses embedded above.	
MRO NSRF	The NSRF requests that the SDT address the following concerns and clarifications in Attachment 1; 1) Please explore redundancy reporting event Item #14; Complete loss of off-site power to a

Organization	Question 3 Comment
	nuclear generating plant with obligations of NUC-001-2.1 R9.4.4."Provisions for supplying information necessary to report to government agencies, as related to NPIRs." The NSRF understands the importance concerning safety issues with a nuclear plant. A multiple unit coal facility may have a larger reliability impact to the BES than a nuclear plant. The SDT is stating that the fuel source is a reporting issue, not the reliability of a plant loosing off sight power. Recommend that this item be deleted. 2) Item 2 in Attachment 1 would obligate an entity to report any loss of (copper) grounds either on a T-Line or grounds associated with a transformer or breakers and that this level of reporting should not rise to the NERC level. Believes that additional qualifying language similar to Item 1 be incorporated into the threshold and read as follows:"Damage or destruction of its Facility that results from actual or suspected intentional human action that results in actions to avoid a BES Emergency." 3) Item 3 Attachment 1 needs clarification since a physical threat needs to be actual and confirmed so that the TO or TOP repositions the system. In addition, the SDT needs to clarify what the phrase "normal operations" means. (Is this a ratings issue? or a result in how the System Operator operates the system.) 4) Item 3 should provide clarification as to "Suspicious device or activity at a Facility" to determine when threshold raises to the level of reporting. We are concerned that, based on an Auditors perception, these words could be interpreted in several different ways. In addition, we believe that language needs to be included that the threat causes the reporting entity to change to an abnormal operating state. This situation could be interpreted differently by the auditor or the entity at the time of the event. Recommend the following language: "Suspicious device or activity at a Facility with the potential to degrade the normal operation of the Facility". This language is similar to the first threshold. 5) The term Initiating entity is used three times within Attachment 1 and needs to be more clearly defined or reworded. Is it the entity that identifies the needs of a Public Appeal or the entity that makes the public appeal the initiating entity? The word "initiating" does not provide clarity but only provides uncertainty to the industry. The Standard needs to be clear on who has the responsibility as the "initiating". Recommend the following: a. For public

Organization	Question 3 Comment
	appeal, under Entity with Reporting Responsibility; "entity that issues a public appeal to the public" b. For system wide voltage reduction, under Entity with Reporting Responsibility; "entity that activates a voltage reduction" c. For manual load shedding, under Entity with Reporting Responsibility; "entity that activates manual load shedding" 6) The NSRF recommends transmission loss to read as: "contrary to protection system design" found in threshold for reporting within the Attachment for a Transmission loss event. 7) In Requirement 2/ Measure 2, recommend adding "upon recognition of " as a starting point to the 24 hour reporting requirement, within the threshold of reporting where perceived threats are the threshold, or transmission loss, when contrary to design is determined.
Response: Thank you for your comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot. **7) This was the intent of the drafting team and we have made this clarification to R2 and M2.**	
Independent Electricity System Operator	The proposed implementation plan may conflict with Ontario regulatory practice respecting the effective date of the standard. It is suggested that this conflict be removed by: Moving the last part ", or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities." to right after "this standard is approved by applicable regulatory approval" in the Effective Dates Section on P.2 of the draft standard, and the proposed Implementation Plan.
Response: Thank you for your comment. The SDT used the standard language provide by NERC Legal and intended to address all of the jurisdictions in which the standard may become enforceable. We will refer your suggestion to NERC Legal for consideration in the preparation of the filing.	
Bonneville Power Administration	The proposed standard does not have any oral reporting option for system operators and thus appears to be administrative in nature. Due to this and the fact that administrative staff are

Organization	Question 3 Comment
	not available on weekends, the "24 hour" reporting requirements should be modified to "Next Business Day" to allow for weekend delays in reporting.BPA believes that there are too many minor events that have to be reported within 24 hours. Reporting during the next business day would suffice. Some examples include: A 115 shunt capacitor bank failure for the first event type does not seem important enough to require reporting within 24 hours just because action has to be taken to raise generation or switching of line. A failure of a line tower that has proper protective action to clear the line and also has automatic (SPS) to properly protect as designed the BES system (a good normal practice) from overloads or voltage issues does not seem important enough to require reporting within 24 hours either.
Response: Thank you for your comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Clark Public Utilities	The SDT has not adequately addressed my comments from the last draft regarding damage or destruction of its facility that results from actual or suspected intentional human action. The SDT needs to limit what it means by damage. As an example, if someone breaks into a substation and paints graffiti on a breaker that is part of the BES, the breaker has been "damaged." However, the breaker's ability to function has not been compromised and there are no emergency actions that need to be taken. There is no reason for an emergency reporting procedure to require this to be reported. The SDT needs to add the same modifier for damage that it added in the previous event threshold for reporting. The reference for this type of damage should be as follows:Event: Damage or destruction of a Facility.Entity with Reporting Responsibility: BA, TO, TOP, GO, GOP, DP.Threshold for Reporting: Damage or destruction of its Facility that results from actual or suspected intentional human action that results in actions to avoid a BES Emergency.
Response: Thank you for your comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has	

Organization	Question 3 Comment
reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Lewis County PUD	We are a small utility with little impact to the BES with a small hydro on the end of a 230kV line. CIP-001 requires us to contact the FBI who has repeatedly instructed us to call the local sheriff office. The sheriff office has instructed us to call 911 and they will contact the FBI as needed. Therefore, 911 is our only contact number and our plan if vandalism, property destruction or sabotage is to have a supervisor call 911 and report. I do not think calling 911 to confirm the contact number serves any propose. Our plan will be simple with not a lot detail. The drafting team should recognize the reality of small utilities and state the required plan may be simple and not follow the flowchart in the draft standard.
Response: Thank you for your comment. The SDT did recognize your circumstances and set the requirements to provide the flexibility to address the diversity of entities to which the standard is intended to apply.	
SPP Standards Review Group	We have made previous comments in the past regarding the listing in the Entity with Reporting Responsibility column of Attachment 1. While we concur with some of the changes that the drafting team has made regarding the addition of a bright line in the Threshold for Reporting column, there remain events where there is no line at all. For example, in the Transmission loss event, the TOP is listed and there is no distinction regarding which TOP is required to file the event report. Is it the TOP in whose TOP area the loss occurred or is it a neighboring TOP who observes the loss. Clearly, the responsibility for reporting lies with the host system. There are several other similar events where the bright line is non-existent and needs to be added. We suggest that the drafting team return the deleted language to the Entity with Reporting Responsibility column in those instances where the bright line has not been added in the Threshold column. Regarding multiple reports for a single event, we again believe that only a single report should be required. While additional information may be available from others, let the Event Analysis personnel do their job investigating an event and eliminate any redundant reporting that is currently required as the standard is written. If not, this standard, if approved, would then appear to be a likely candidate for Phase 2 of the

Organization	Question 3 Comment
	Paragraph 81 project.
Response: Thank you for your comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot. On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 ("P81") invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program. As the SDT is moving forward with a Recirculation Ballot, your suggestions will be forwarded to NERC for future consideration.	
SERC OC Standards Review Group	While this draft is an improvement on the previous draft, the proposed R2 is unacceptable, and should be amended to, at a minimum, require reporting by the end of the next business day, instead of within 24 hours. Events or situations affecting real time reliability to the system already are required to be reported to appropriate Functional Entities that have the responsibility to take action. Adding one more responsibility to system operators increases the operator's burden, which reduces the operator's effectiveness when operating the system. Care should be given when placing additional responsibility on the system operators. Allowing reporting at the end of the next business day gives operators the flexibility to allow support staff to assist with after-the-fact reporting requirements. For some event types where in order to provide real time situational awareness over a wide area (for example coordinated sabotage event) it may be appropriate to have more timely reporting .If the intent of this standard is to address sabotage reporting there needs to be an understanding of the actions to be taken by those receiving the reports so the reporting entities can incorporate those actions into their

Organization	Question 3 Comment
	plan. As a minimum, NERC should have a process in place to assess the reports and take appropriate actions. Attachment 1: Threshold for reporting should not be defined such that multiple reports would be required for the same event. For example, both the TOP and RC being required to report the outage of a transmission line. 2nd event type (Damage or destruction of a Facility): Add the following sentence to the Threshold for Reporting: "Do not report theft or damage unless it degrades normal operation of a Facility." 4th event type (Physical threats to a BES control center): The term "BES control center" needs to be clarified. 5th, 6th, and 7th event types: In instances where a reliability directive is issued, is the "initiating entity" the entity that issues the directive or the entity that carried out the directive. 9th event type (Voltage deviation on a Facility): Change "nominal" to "expected or scheduled." 15th event type (Transmission loss): It is not clear what is meant by "contrary to design." This is so broad that it could be interpreted as requiring reporting misoperations within the reporting time frame before even an initial investigation can begin. This needs to be clarified and tied to the impact on the reliability of the BES. The comments expressed herein represent a consensus of the views of the above named members of the SERC OC Standards Review Group only and should not be construed as the position of SERC Reliability Corporation, its board, or its officers.
Response: Thank you for your comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Tacoma Public Utilities	Why does the text "...but is not limited to..." in M1 have to be included? Does this mean that

Organization	Question 3 Comment
	there are unwritten requirements that an auditor might look for? What if, in trying to validate contact information, contacts do not confirm their information? Regarding the Loss of firm load row in Attachment 1, an exception should be made for weather or natural disaster related threats in the Threshold for Reporting. Regarding the Transmission loss row in Attachment 1, it is not quite clear which types of BES Elements would meet the Threshold for Reporting. Is it just lines, buses, and transformers? What about reactive resources? What about generators that unexpectedly trip offline during a fault on the transmission system?
Response: Thank you for your comment. In Measure M1 the text "but is not limited to" is intended to provide flexibility for each entity to determine, based on its assets and unique situation, to develop an Operating Plan that appropriately supports reliability. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
MidAmerican Energy	Yes. 1) MidAmerican Energy agrees with and supports MRO NSRF comments. 2) Add additional wording to clearly provide for compliance when events are found more than 24 hours after an event. Add the following to the end of R2. Add, Events not identified until sometime later after they occurred shall be reported within 24 hours. 3) In R3 add "external" for R3 to read Validate "external" contact information. 4) In EOP-004-2 Attachment 1 - the wording "Damage or destruction of its Facility that results from actual or suspected intentional human action that results in actions to avoid a BES Emergency" is not specific or measureable and therefore ambiguous. Zero defect standards which carry penalties must be specific. Please reword to "Intentional human action to destroy a NERC BES facility whose loss could result in actions to avoid a BES Emergency". This clearly aligns with the EOP-004 intent of sabotage and emergency reporting. EOP-004 should not report on unexpected conditions such as when a system operator attempts to reclose a line

Organization	Question 3 Comment
	during a storm believing the line tripped for a temporary fault due to debris, when in fact the fault was permanent and damaged a transformer.
Response: Thank you for your comment. See response to MRO NSF comments. **Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.**	
american Transmission Company	Yes A. ATC requests that the Standards Drafting Team address the following concerns and clarifications in Attachment 1: a.) Reporting event #14 in Attachment 1, is duplicative with respect to Nuclear Reliability Standard NUC-001-2.1 R 9.4.4. Reporting event #14 requires entities to report to NERC a "Complete loss of off-site power to a nuclear generating plant" while Nuclear Reliability Standard NUC-001-2.1 R9.4.4., i.e. includes "Provisions for supplying information necessary to report to government agencies, as related to Nuclear Plant Interface Requirements (NPIRs)". In addition, ATC believes the reporting related to event #14 in Attachment 1 is not a "reliability" issue, and more appropriately covered under Standard NUC-001 as a "Nuclear Safety Shutdown" issue. Therefore, ATC recommends that Item #14 in Attachment 1 of EOP-004-2 be deleted. b.) In Attachment 1, reporting event #2, i.e. Damage or destruction of a Facility" could obligate an entity to report any loss of copper grounds either on a T-Line or grounds associated with a transformer or breakers. ATC believes this does not rise to a reporting level such as NERC. ATC believes that additional qualifying language similar to reporting item #1 be incorporated into the threshold and read as follows: "Damage or destruction of its Facility that results from actual or suspected intentional human action that results in actions to avoid a BES Emergency." c.) In Attachment 1, reporting event #3 i.e. "Physical threats to a Facility" needs clarification

Organization	Question 3 Comment
	since a physical threat needs to be actual and confirmed so that the TO or TOP repositions the system. In addition, the SDT needs to clarify what the phrase "normal operations" means. Is this a ratings issue? Or a result in how the Operator operates the system. d.) In Attachment 1, reporting event #3 threshold i.e. "Suspicious device or activity at a Facility" needs clarification to determine when it raises to the level of reporting. These words could be interpreted in several different ways. In addition, ATC believe that language needs to be added that the threat causes the reporting entity to change to an abnormal operating state. ATC recommends the threshold be revised to read: "Suspicious device or activity at a Facility with the potential to degrade the normal operation of the Facility". e.) In Attachment 1, the term "Initiating entity" is used three times for reporting events and needs to be clearly defined or reworded. Is it the entity that identifies the needs of a Public Appeal or the entity that makes the public appeal the initiating entity? The Standard needs to be clear on who has the responsibility as the "initiating" party, especially when multiple parties may be involved. ATC recommends the following:1) For public appeal, under Entity with Reporting Responsibility; it is the "entity that issues a public appeal to the public"2) For system wide voltage reduction, under Entity with Reporting Responsibility; it is the "entity that activates a voltage reduction"3) For manual load shedding, under Entity with Reporting Responsibility; it is the "entity that activates manual load shedding" f.) In Attachment 1, reporting event #15 i.e. "Transmission Loss", the threshold includes the phrase "contrary to design". ATC recommends this be clarified to read "contrary to protection system design". B. In EOP-004-2 Requirement 2/ Measure 2 both have the following language:"Each Responsible Entity shall report events per their Operating Plan within 24 hours of meeting an event type threshold for reporting." ATC recommends adding "upon recognition" as a starting point to the 24 hour reporting requirement. This would be revised to read: "Each Responsible Entity shall report events per their Operating Plan within 24 hours of recognition of an event type threshold"
Response: Thank you for your comment. A) Many suggestions were made regarding the language of certain events listed in	

Organization	Question 3 Comment
	Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot. **B) This was the intent of the drafting team and we have made this clarification to R2 and M2.**

END OF REPORT

Exhibit E

Analysis of how VRFs and VSLs Were Determined Using Commission Guidelines

Violation Risk Factor and Violation Severity Level Assignments

Project 2009-01 – Disturbance and Sabotage Reporting

This document provides the drafting team's justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in

EOP-004-2 — Event Reporting

Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the ERO Sanction Guidelines.

Justification for Assignment of Violation Risk Factors in EOP-004-2

The Disturbance and Sabotage Reporting Standard Drafting Team applied the following NERC criteria when proposing VRFs for the requirements in EOP-004-2:

High Risk Requirement
A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement
A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

The SDT also considered consistency with the FERC Violation Risk Factor Guidelines for setting VRFs:[1]

Guideline (1) — Consistency with the Conclusions of the Final Blackout Report
The Commission seeks to ensure that Violation Risk Factors assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System.

In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:[2]

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) — Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement Violation Risk Factor assignments and the main Requirement Violation Risk Factor assignment.

[1] North American Electric Reliability Corp., 119 FERC ¶ 61,145, order on reh'g and compliance filing, 120 FERC ¶ 61,145 (2007) ("VRF Rehearing Order").
[2] Id. at footnote 15.

Guideline (3) — Consistency among Reliability Standards

The Commission expects the assignment of Violation Risk Factors corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) — Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular Violation Risk Factor level conforms to NERC's definition of that risk level.

Guideline (5) — Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

The following discussion addresses how the SDT considered FERC's VRF Guidelines 2 through 5. The team did not address Guideline 1 directly because of an apparent conflict between Guidelines 1 and 4. Whereas Guideline 1 identifies a list of topics that encompass nearly all topics within NERC's Reliability Standards and implies that these requirements should be assigned a "High" VRF, Guideline 4 directs assignment of VRFs based on the impact of a specific requirement to the reliability of the system. The SDT believes that Guideline 4 is reflective of the intent of VRFs in the first instance and therefore concentrated its approach on the reliability impact of the requirements.

VRF for EOP-004-2:

There are three requirements in EOP-004-2. Requirement R1 was assigned a Lower VRF while Requirements R2 and R3 were assigned a Medium VRF.

VRF for EOP-004-2, Requirements R1:

- FERC's Guideline 2 — Consistency within a Reliability Standard. The Requirement specifies which entities are required to have processes for recognition of events and for communicating with other entities. This Requirement is the only administrative Requirement within the Standard. The VRF is only applied at the Requirement level. FERC's Guideline 3 — Consistency among Reliability Standards. This requirement calls for an entity to have processes for recognition of events and communicating with other entities. This requirement is administrative in nature and deals with the means to report events after the fact. All event reporting requirements in Attachment 1 are for 24 hours after recognition that an event has occurred. The current approved VRFs for EOP-004-1 are

all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program.

- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. Failure to have an event reporting Operating Plan is not likely to directly affect the electrical state or the capability of the bulk electric system. Development of the Operating Plan is a requirement that is administrative in nature and is in a planning time frame that, if violated, would not, under emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system.. Therefore this requirement was assigned a Lower VRF.
- FERC's Guideline 5 — Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R1 contains only one objective which is to have an Operating Plan with two distinct processes. Since the requirement is to have an Operating Plan, only one VRF was assigned.

VRF for EOP-004-2, Requirement R2:

- FERC's Guideline 2 — Consistency within a Reliability Standard. This Requirement calls for the Responsible Entity to implements its Operating Plan and is assigned a Medium VRF. There is one other similar Requirement in this Standard which specify an annual validation of the information contained in the Operating Plan (R3). Both of these Requirements are assigned a Medium VRF.
- FERC's Guideline 3 — Consistency among Reliability Standards. EOP-004-2, Requirement R2 is a requirement for entities to report events using the process for recognition of events per Attachment 1. Failure to report events within 24 hours is not likely to "directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system." However, violation of a medium risk requirement should also be "unlikely to lead to bulk electric system instability, separation, or cascading failures…" Such an instance could occur if personnel do not report events. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. EOP-004-2, Requirement R2 mandates that Responsible Entities implement their Operating Plan. Bulk power system instability, separation, or cascading failures are not likely to occur due to a failure to notify another entity of the event failure, but there is a slight chance that it could occur. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 5 - Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R2 addresses a single objective and has a single VRF.

VRF for EOP-004-2, Requirement R3:

- FERC's Guideline 2 — Consistency within a Reliability Standard. This Requirement calls for the Responsible Entity to perform an annual validation of the information contained in the Operating Plan and is assigned a Medium VRF. There is one other similar Requirement in this Standard which specifies that the Responsible Entity implement its Operating Plan (R2).. Both of these Requirements is assigned a Medium VRF.
- FERC's Guideline 3 — Consistency among Reliability Standards. EOP-004-2, Requirement R3 is a requirement for entities to perform an annual validation of the information contained of the information in the Operating Plan. Failure to perform an annual validation of the information contained in the Operating Plan is not likely to "directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system." However, violation of a medium risk requirement should also be "unlikely to lead to bulk electric system instability, separation, or cascading failures…" Such an instance could occur if personnel do not perform an annual test of the Operating Plan and it is out of date or contains erroneous information. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. EOP-004-2, Requirement R3 mandates that Responsible Entities perform an annual validation of the information contained of the information in the Operating Plan. Bulk power system instability, separation, or cascading failures are not likely to occur due to a failure to perform an annual test of the Operating Plan, but there is a slight chance that it could occur if the Operating Plan is out of date or contains erroneous information. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 5 - Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R3 addresses a single objective and has a single VRF.

Justification for Assignment of Violation Severity Levels for EOP-004-2:

In developing the VSLs for the EOP-004-2 standard, the SDT anticipated the evidence that would be reviewed during an audit, and developed its VSLs based on the noncompliance an auditor may find during a typical audit. The SDT based its assignment of VSLs on the following NERC criteria:

Lower	Moderate	High	Severe
Missing a minor element (or a small percentage) of the required performance The performance or product measured has significant value as it almost meets the full intent of the requirement.	Missing at least one significant element (or a moderate percentage) of the required performance. The performance or product measured still has significant value in meeting the intent of the requirement.	Missing more than one significant element (or is missing a high percentage) of the required performance or is missing a single vital component. The performance or product has limited value in meeting the intent of the requirement.	Missing most or all of the significant elements (or a significant percentage) of the required performance. The performance measured does not meet the intent of the requirement or the product delivered cannot be used in meeting the intent of the requirement.

FERC's VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in EOP-004-2 meet the FERC Guidelines for assessing VSLs:

Guideline 1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

> Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline 2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

> A violation of a "binary" type requirement must be a "Severe" VSL.
>
> Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline 3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline 4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

. . . unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VSLs for EOP-004-2 Requirements R1:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R1	Meets NERC's VSL guidelines. The requirement calls for the entity to have an Operating Plan and is binary in nature. The VSL is therefore set to "Severe".	The proposed requirement is a revision of CIP-001-1, R1-R4, and EOP-004-1, R2. The Requirement has no Parts and is binary in nature. The binary VSL does not lower the current level of Compliance.	The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed binary VSL uses the same terminology as used in the associated requirement, and is, therefore, consistent with the requirement.	The VSLs are based on a single violation and not cumulative violations.

VSLs for EOP-004-2 Requirement R2:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R2	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is a revision of EOP-004-1, R3. There is only a Severe VSL for that requirement. However, the reporting of events is based on timing intervals listed in EOP-004 Attachment 1. Based on the VSL Guidance, the DSR SDT developed four VSLs based on tardiness of the submittal of the report. If a report is not submitted, then the VSL is Severe. This maintains the current VSL.	The proposed VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSLs use the same terminology as used in the associated requirement, and are, therefore, consistent with the requirement.	The VSLs are based on a single violation and not cumulative violations.

VSLs for EOP-004-2 Requirement R3:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R3	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is a new Requirement. The test of the Operating Plan is based on the calendar year. Based on the VSL Guidance, the DSR SDT developed four VSLs based on tardiness of the submittal of the report. If a test is not performed, then the VSL is Severe.	The proposed VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSLs use the same terminology as used in the associated requirement, and are, therefore, consistent with the requirement.	The VSLs are based on a single violation and not cumulative violations.

Exhibit F

Record of Development of Proposed Reliability Standard

Project 2009-01
Disturbance and Sabotage Reporting

Related Files

Status:
Adopted by the Board of Trustees on November 6, 2012, pending regulatory approval.

Background:
This project will entail revision to the following existing standards:

- CIP-001-1 – Sabotage Reporting
- EOP-004-1 – Disturbance Reporting

Stakeholders have indicated that identifying potential acts of "sabotage" is difficult to do in real time, and additional clarity is needed to identify thresholds for reporting potential acts of sabotage in CIP-001-1. Stakeholders have also reported that EOP-004-1 has some requirements that reference out-of-date Department of Energy forms, making the requirements ambiguous. EOP-004-1 also has some 'fill-in-the-blank' components to eliminate.

The project will include addressing previously identified stakeholder concerns and FERC directives; will bring the standards into conformance with the latest approved version of the ERO Rules of Procedure; and may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

Draft	Action	Dates	Results	Consideration of Comments
Draft 6 **EOP-004-2** Clean**(89)** | Redline to last posted**(90)** Implementation Plan Clean**(91)** **Supporting Materials:** Mapping Document**(92)**	Recirculation Ballot and Non-binding poll Info**(97)** Vote>>	10/24/12 - 11/05/12 (closed)	Summary**(98)** Ballot Results**(99)** Non-binding Poll Results**(100)**	

Consideration of Issues and Directives(93) VRF/VSL Justification(94) CIP-001-2a(95) EOP-004-1(96)				
Draft 5 EOP-004-2 Clean (71)| Redline to Last Posted(72) Implementation Plan Clean(73) | Redline to Last Posted(74) **Supporting Materials:** Comment Form (Word)(75) Mapping Document(76) Consideration of Issues and Directives(77) VRF/VSL Justification(78) CIP-001-2a(79) EOP-004-1(80)	Successive Ballot and Non-binding Poll Info(81) Vote>>	09/18/12 - 09/27/12 (closed)	Updated Summary(83) Ballot Results(84) Non-binding Poll Results(85)	
	Comment Period Info(82) Submit Comments>>	08/29/12 - 09/27/12 (closed)	Comments Received(86) Meeting Results(87)	Consideration of Comments(88)
Draft 4 **EOP-004-2** Clean(51) | Redline to Last Posted (52)	Successive Ballot and Non-binding Poll Updated Info(63)	05/15/12-05/24/12 (closed)	Summary(66) Ballot Results(67)	

Supporting Materials: Comment Form (Word)**(53)** Implementation Plan Clean**(54)** | Redline to Last Posted**(55)** Mapping Document**(56)** Consideration of Issues and Directives**(57)** VRF/VSL Justification**(58)** Proposed NERC RoP Section 812**(59)** CIP-001-2a**(60)** CIP-008-3**(61)** EOP-004-1**(62)**	Info**(64)** Vote>>		Non-binding Poll Results**(68)**	
	Comment Period Info**(65)** Submit Comments>>	04/25/12 - 05/24/12 (closed)	Comments Received**(69)**	Consideration of Comments**(70)**
Draft 3 EOP-004-2 Clean**(34)** | Redline to Last Posted**(35)** **Supporting Materials:** Comment Form (Word)**(36)** Implementation Plan Clean**(37)** | Redline to Last Posted**(38)** Mapping	Join Ballot Pools>>	10/28/11 - 11/28/11 (closed)		Consideration of Comments**(50)**
	Formal Comment Period Info**(43)** Submit Comments>>	10/28/11 - 12/12/11 (closed)	Comments Received**(46)**	
	Initial Ballot and Non-Binding Poll Updated Info**(44)** Info**(45)** Vote>>	12/02/11 - 12/12/11 (closed)	Summary**(47)** Full Record**(48)** Non-Binding Poll	

Document(39) VRF/VSL Justification(40) CIP-001-1(41) EOP-004-1(42)			Results(49)	
Draft 2 **EOP-004-2** clean(25) | redline to last posted(26) **Supporting Materials:** Comment Form (Word)(27) Implementation Plan(28) CIP-001-1(29) EOP-004-1(30)	Info(31) Formal Comment Period>>	03/09/11 - 04/08/11	Comments Received(32)	Consideration of Comments(33)
Draft 1 **EOP-004-2** EOP-004-2(19) **Supporting Materials:** Comment Form (Word)(20) Mapping Document(21)	Informal Comment Period Submit Comments>> Info(22)	09/15/10 – 10/15/10	Comments Received(23)	Consideration of Comments(24)
Concept Paper Supporting Disturbance and Sabotage Reporting Concept Paper(12)	Comment Period Submit Comments>> Info (16)	03/17/10 - 04/16/10 (closed)	Comments Received (17)	Consideration of Comments (18)

Supporting Materials: Comment Form (Word)**(13)** CIP-001-1 - Sabotage Reporting**(14)** EOP-004-1 - Disturbance Reporting**(15)**				
Nominations for Standard Drafting Team **Supporting Materials:** Nomination Form (Word)**(10)**	Info**(11)** Submit Nomination>>	09/16/09 - 09/30/09 (closed)		
Draft 2 Disturbance and Sabotage Reporting SAR 2 Clean**(8)** | Redline to Last Posting **(9)**				
Nominations for SAR Drafting Team **Supporting Materials:** Nomination Form (Word)**(6)**	Info**(7)** Submit Nomination>>	04/29/09 - 05/13/09 (closed)		
Proposed SAR Draft SAR	Comment Period Info**(3)** Submit Comments>>	04/22/09 - 05/21/09 (closed)	Comments Received**(4)**	Consideration of Comments**(5)**

Version 1**(1)** **Supporting Materials:** Comment Form (Word)**(2)**				

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request Form

Title of Proposed Project:	Disturbance and Sabotage Reporting (Project 2009-01)
Request Date	April 2, 2009
Approved by SC for posting:	April 15, 2009

SAR Requester Information		**SAR Type** (*Check a box for each one that applies.*)	
Name	Patrick Brown	☐	New Standard
Primary Contact Manager, NERC and Regional Coordination PJM Interconnection	Patrick Brown	☒	Revision to existing Standards: CIP-001-1 and EOP-004-1
Telephone	610-666-4597	☒	Withdrawal of existing Standard
E-mail	brownp@pjm.com	☐	Urgent Action

Purpose **(Describe the proposed standard action: Nomination of a proposed standard, revision to a standard, or withdrawal of a standard and describe what the standard action will achieve.)**

This project will entail revision to existing standards CIP-001-1 – Sabotage Reporting and EOP-004-1 – Disturbance Reporting. The standards may be merged to eliminate redundancy and provide clarity on sabotage events. EOP-004 has some 'fill-in-the-blank' components to eliminate. The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

Industry Need (Provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

The existing requirements need to be revised to be more specific – and there needs to be more clarity in what sabotage looks like.

Brief Description (Provide a paragraph that describes the scope of this standard action.)

CIP-001 may be merged with EOP-004 to eliminate redundancies. Acts of sabotage have to be reported to the DOE as part of EOP-004. Specific references to the DOE form need to be

eliminated. EOP-004 has some ‘fill-in-the-blank’ components to eliminate. The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards (see tables for each standard at the end of this SAR for more detailed information).
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR.) See “Issues to be Considered by Drafting Team” tables for each standard at the end of this SAR for more detailed information.

Reliability Functions

The Standard will Apply to the Following Functions *(Check box for each one that applies.)*		
☒	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☐	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☐	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☐	Distribution Provider	Delivers electrical energy to the End-use customer.
☐	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☒	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check box for all that apply.)*	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☒	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*
1. A reliability standard shall not give any market participant an unfair competitive advantage. Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes

Related Standards

Standard No.	Explanation
COM-003-1	Operations Communications Protocols – this standard may include some requirements that require coordination with the requirements addressed in this project

Related SARs

SAR ID	Explanation

Regional Variances

Region	Explanation
ERCOT	
FRCC	
MRO	
NPCC	
SERC	
RFC	
SPP	
WECC	

Issues to be Considered by Drafting Team Project 2009-01 — Disturbance and Sabotage Reporting	
Standard #	**Title**
CIP-001-0	Sabotage Reporting
Issues	FERC Order 693

	Disposition: Approved with modifications • Consider the need for wider application of the standard. Consider whether separate, less burdensome requirements for smaller entities may be appropriate. • Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event. • In the interim, provide advice to entities about the reporting of particular circumstances as they arise. • Consider FirstEnergy's suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality. • Incorporate a periodic review or updating of the sabotage reporting procedures and for their periodic testing. Consider a staggered schedule of annual testing and formal review every two to three years. • Include a requirement to report a sabotage event to the proper government authorities. Develop the language to specifically implement this directive. • Explore ways to reduce redundant reporting, including central coordination of sabotage reports and a uniform reporting format. V0 Industry Comments • Object to multi-site requirement • Definition of sabotage required VRF comments • Adequate procedures will insure it is unlikely to lead to bulk electric system instability, separation, or cascading failures. Other • Modify standard to conform to the latest version of NERC's Reliability Standards Development Procedure, the NERC Standard Drafting Team Guidelines, and the ERO Rules of Procedure. NERC Audit and Observation Team • Applicability — How does this standard pertain to Load Serving Entities, LSE's. • Registered Entities have sabotage reporting processes and procedures in place but not all personnel has been trained. • Question: How do you "and make the operator aware" • R4 — "What is meant by: "establish contact with the FBI". Is a phone number adequate? Many entities which call the FBI are referred back to the local authority. The AOT noted that on the FBI website it states to contact the local authorities. Is this a question for Homeland Security to deal with for us?" • R4 — Establish communications contacts, as applicable with local FBI and RAMP officials. Some entities are very remote and the sheriff is the only local authority does the FBI still need to be contacted? FERC's December 20, 2007 and April 4, 2008 Orders in Docket Nos. RC07-004-000, RC07-6-000, and RC07-7-000 • In FERC's December 20, 2007 Order, the Commission reversed NERC's Compliance Registry decisions with respect to three load serving entities in the ReliabilityFirst (RFC) footprint. The distinguishing feature of these three LSEs is that none owned physical assets. Both NERC and RFC assert that there will be a "reliability gap" if retail marketers are not registered as LSEs. To avoid a possible gap, a consistent, uniform approach to

	ensure that appropriate Reliability Standards and associated requirements are applied to retail marketers must be applied. Each drafting team responsible for reliability standards applicable to LSEs is to review and change as necessary, requirements in the applicable reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. For additional information see: • FERC's December 20, 2007 Order (http://www.nerc.com/files/LSE_decision_order.pdf) • NERC's March 4, 2008 (http://www.nerc.com/files/FinalFiledLSE3408.pdf), • FERC's April 4, 2008 Order (http://www.nerc.com/files/AcceptLSECompFiling-040408.pdf) and • NERC's July 31, 2008 (http://www.nerc.com/files/FinalFiled-CompFiling-LSE-07312008.pdf) compliance filings to FERC on this subject.

Issues to be Considered by Drafting Team Project 2009-01 — Disturbance and Sabotage Reporting	
Standard #	**Title**
EOP-004-1	Disturbance Reporting
Issues	FERC Order 693 Disposition: Approved with modification • Include any requirements for users, owners, and operators of the bulk power system to provide data that will assist NERC in the investigation of a blackout or disturbance. • Change NERC's Rules of Procedure to assure the Commission receives these reports in the same frame as the DOE. • Consider APPA's concern about generator operators and LSEs analyzing performance of their equipment and provide data and information on the equipment to assist others with analysis. • Consider all comments offered in a future modification of the reliability standard. Fill-in-the-Blank Team Comments • Consider changes to R1 and R3.4 to standardize the disturbance reporting requirements (requirements for disturbance reporting need to be added to this standard) • Regions currently have procedures, but not in the form of a standard. The drafting team will need to review regional requirements to determine reporting requirements for the North American standard. V0 Industry Comments • R3 – too many reports, narrow requirement to RC • How does this apply to generator operator? Other • Modify standard to conform to the latest version of NERC's Reliability Standards Development Procedure, the NERC Standard Drafting Team Guidelines, and the ERO Rules of Procedure. NERC Audit and Observation Team • R3.1 — Can there be a violation without an event?

	Event Analysis Team
	• Reliability Issue: Coordination and follow up on lessons learned from event analyses Consider adding to EOP-004 – Disturbance Reporting. Proposed requirement: Regional Entities (REs) shall work together with Reliability Coordinators, Transmission Owners, and Generation Owners to develop an Event Analysis Process to prevent similar events from happening and follow up with the recommendations. This process shall be defined within the appropriate NERC Standard.
	
	FERC's December 20, 2007 and April 4, 2008 Orders in Docket Nos. RC07-004-000, RC07-6-000, and RC07-7-000
	• In FERC's December 20, 2007 Order, the Commission reversed NERC's Compliance Registry decisions with respect to three load serving entities in the ReliabilityFirst (RFC) footprint. The distinguishing feature of these three LSEs is that none owned physical assets. Both NERC and RFC assert that there will be a "reliability gap" if retail marketers are not registered as LSEs. To avoid a possible gap, a consistent, uniform approach to ensure that appropriate Reliability Standards and associated requirements are applied to retail marketers must be applied. Each drafting team responsible for reliability standards applicable to LSEs is to review and change as necessary, requirements in the applicable reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. For additional information see:
	  • FERC's December 20, 2007 Order (http://www.nerc.com/files/LSE_decision_order.pdf)
	  • NERC's March 4, 2008 (http://www.nerc.com/files/FinalFiledLSE3408.pdf),
	  • FERC's April 4, 2008 Order (http://www.nerc.com/files/AcceptLSECompFiling-040408.pdf) and
	  • NERC's July 31, 2008 (http://www.nerc.com/files/FinalFiled-CompFiling-LSE-07312008.pdf) compliance filings to FERC on this subject.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form for Project 2009-01 — SAR for Disturbance and Sabotage Reporting

Please **DO NOT** use this comment form. Please use the electronic comment form located at the link below to submit comments on the proposed SAR for revisions to the existing Disturbance and Sabotage Reporting standards. Comments must be submitted by **May 21, 2009**. If you have questions please contact Stephen Crutchfield at Stephen.crutchfield@nerc.net or by telephone at 609-651-9455.

http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Background Information

This project will entail revision to the following existing standards:

- CIP-001-1 — Sabotage Reporting
- EOP-004-1 — Disturbance Reporting

Stakeholders have indicated that identifying potential acts of "sabotage" is difficult to identify in real-time, and additional clarity is needed to identify thresholds for reporting potential acts of sabotage in CIP-001-1. Stakeholders have also reported that EOP-004-1 has some requirements that reference out-of-date Department of Energy forms, making the requirements ambiguous. EOP-004 also has some 'fill-in-the-blank' components to eliminate.

The project will include addressing previously identified stakeholder concerns and FERC directives, will bring the standards into conformance with the latest approved version of the ERO Rules of Procedure, and may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

***Please use the electronic comment form to submit your final responses to NERC.**

1. Do you agree that there is a reliability-related reason to support modifying CIP-001-1 and EOP-004-1? If not, please explain in the comment area.

   ☐ Yes

   ☐ No

   Comments:

2. Do you agree with the scope of the proposed SAR? If not, please explain what should be added or deleted to the proposed scope.

   ☐ Yes

   ☐ No

   Comments:

3. Are you aware of any associated business practices that we should consider with this SAR? If yes, please explain in the comment area.

   ☐ Yes

   ☐ No

   Comments:

4. CIP-001-1 applies to the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, and the Load-serving Entity. EOP-004-1 applies to the same entities, plus the Regional Reliability Organization. Do you agree with the applicability of the existing CIP-001-1 and the existing EOP-004-1? If no, please identify what you believe should be modified.

   ☐ Yes

   ☐ No

   Comments:

5. If you have any other comments on the SAR or proposed modifications to CIP-001-1 and EOP-004-1 that you haven't provided in response to the previous questions, please provide them here.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Comment Period Open
April 22–May 21, 2009

Now available at: http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Project Name:
2009-01 — Disturbance and Sabotage Reporting

Due Date and Submittal Information:
The comment period is open **until 8 p.m. EDT on May 21, 2009**. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Lauren Koller at Lauren.Koller@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page: http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Content for Comment Period:
- A proposed SAR for revisions to the existing Disturbance and Sabotage Reporting standards

Other Materials Posted:
- CIP-001-1 — Sabotage Reporting
- EOP-004-1 — Disturbance Reporting

Project Background:
This project will entail revision to the following existing standards:
- CIP-001-1 — Sabotage Reporting
- EOP-004-1 — Disturbance Reporting

Stakeholders have indicated that identifying potential acts of "sabotage" is difficult to do in real time, and additional clarity is needed to identify thresholds for reporting potential acts of sabotage in CIP-001-1. Stakeholders have also reported that EOP-004-1 has some requirements that reference out-of-date Department of Energy forms, making the requirements ambiguous. EOP-004-1 also has some 'fill-in-the-blank' components to eliminate.

The project will include addressing previously identified stakeholder concerns and FERC directives; will bring the standards into conformance with the latest approved version of the ERO Rules of Procedure; and may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

Applicability of Standards in Project:

- Reliability Coordinators
- Balancing Authorities
- Transmission Operators
- Generator Operators
- Load Serving Entities
- Regional Reliability Organizations

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Project 2009-01 Disturbance and Sabotage Reporting Comment Received

April 29, 2009 through May 13, 2009

Individual or group. (40 Responses)
Name (28 Responses)
Organization (28 Responses)
Group Name (12 Responses)
Contact Organization (12 Responses)
Question 1 (39 Responses)
Question 1 Comments (40 Responses)
Question 2 (40 Responses)
Question 2 Comments (40 Responses)
Question 3 (38 Responses)
Question 3 Comments (40 Responses)
Question 4 (39 Responses)
Question 4 Comments (40 Responses)
Question 5 (0 Responses)
Question 5 Comments (40 Responses)

Individual
Stephen V. Fisher
Lands Energy Consulting
Yes
I have worked with 5 Northwest public utilities on developing procedures related to CIP-001-1 and EOP-004-1. All 5 utilities operate electric systems in fairly remote locations and are embedded in a larger utility's Balancing Authority/Transmission Operator area. A. CIP-001-1 - Developing procedures to unambiguously identify acts of sabotage has been particularly challenging for these systems. In general, it's hard for them to determine whether the most prevalent forms of malicious and intentional system damage that they incur - copper theft and gun shot insulators/equipment - should qualify as acts of sabotage. Although none of the systems consider copper theft to be acts of sabotage, two of the systems consider gun shot insulators/equipment to be acts of sabotage. The other systems look for intent to disrupt electric system operations as a key component of their sabotage identification procedures. Additional guidance from NERC in the form of CIP-001-1 modifications or a companion guidelines document on sabotage identification would provide much needed guidance for these procedures. B. EOP-004-1 - This standard was clearly drafted with the larger electric systems in mind. I have one client that serves 3300 commercial/residential customers from 4-115/13 kV substation transformers and one large industrial customer (80% of its energy load) from a 230/13 kV substation. 75% of the client's load is served from three substations attached to a long, 115 kV transmission line operated by the Bonneville Power Administration. Whenever the line relays open on a permanent fault (which happens 2-3 times per year), the client loses over 50% of its customers (but no more than 10-15 MW during winter peak), thereby necessitating the preparation of a Disturbance Report. To allow utilities to concentrate on operating their systems, without fear of violating EOP-004-1 for failure to report trivial outages, I would remove LSEs from the obligation to report disturbances - leave the reporting to the BA/TOP for large outages in their footprint.
No
I would like to see the SAR expanded to cover the issues I mentioned in my prior comment. Otherwise, the scope of the SAR looks fine to me.
No
No
CIP-001-1 - Yes. In many cases, the staff of an LSE embedded in another entity's BA/TOP area is more

likely to discover an act of sabotage directed toward a BA/TOP-owned facility that could affect the BES than the asset owner. This is because the LSE likely has more operating staff in the area. I have included a requirement in my clients' Sabotage Identification and Reporting Procedures that the client treat acts of sabotage to a third party's system discovered by client employees as though the act was directed toward client facilities. EOP-004-1 - As mentioned before, I would eliminate the LSE from the applicability list and leave the responsibility for disturbance reporting and response to the TOP/BA. However, I would retain a responsibility for the LSEs to cooperate (when requested) with any disturbance investigation.
One final comment on CIP-001-1. My clients received universally rude treatment from the FBI field offices when they attempted to establish the contacts required by the Standard. If the FBI doesn't see value in establishing these contacts, remove the requirement from the Standard. Making sure the LSE knows the FBI field office phone number is probably all the Standard should require.
Individual
Brent Hebert
Calpine Corporation
Yes
Communication of facility status or emergencies between merchant generators registered as GOP and the RC, BA, GOP, or LSE in which the facility resides should be coordinated for EOP -004 reporting. The reporting to NERC/DOE should come from the RC, BA, GOP, or LSE.
Yes
No
The reporting requirements of EOP - 004 are needed for the RC, BA, LSE and the GOP that operates or controls generation in a system as defined by NERC. (System – A combination of generation, transmission, and distribution components). A disturbance is described as an unplanned event that produces and abnormal system condition, any perturbation to the electric system, and the unexpected change in ACE that is caused by the sudden failure of generation or interruption of load. The GOP operating/controlling generation within a system has the ability to analyze system conditions to determine if reporting is necessary. A NERC registered GOP that is a merchant generator within another company's system does not have the ability for a wide area view and cannot analyze system conditions beyond the interconnection point of the facility. Moreover, in most cases the reporting requirements outlined in the Interconnection Reliability Operating Limits and Preliminary Disturbance Report do not apply to the merchant generator that is not a generation only BA. The applicability of the standard does encompass the true merchant generation entities required to register as GOP. Similarly, the OE-417 table 1 reporting requirements generally do not apply to a true merchant generating entity that is required to register as a GOP.
Individual
Steve Toth
Covanta
Yes
Yes - the key to Sabotage reporting requirements is identifying what the 'definition' is of an actual or potential 'Sabotage' event. Like any other standard, if FERC/NERC leave it up to 2000+ entities to establish their own definitions of 'Sabotage', you may likely get 2000+ answers. That is not a controlled and coordinated approach. I offer the following definition, "Sabotage - Deliberate or malicious destruction of property, obstruction of normal operations, or injury to personnel by outside agents." Examples of sabotage events could include, but are not limited to, suspicious packages left near site electrical generating or electrical transmission assets, identified destruction of generating assets, telephone/e mail received threats to destroy or interrupt electrical generating efforts, etc." These have passed multiple NERC regional audits and reviews to date.
Yes

No
Yes
It would be a welcome enhancement to the end users to understand to communication link between all "appropriate parties" who shall be notified of potential or actual sabotage events.... which also needs to be defined.
Individual
Harvie Beavers
Colmac Clarion
Yes
Yes
No
Yes
Need single report for Sabotage so whatever is required results in notification of all parties (State Emergency Management, Homeland Security, FBI, Grid Reliability Chain of Command). Any and all of these can 'expand' knowledge later but all seem to require 'instant' notification.
Individual
Russell A. Noble
Cowlitz County PUD
Yes
The standards as written now create reporting on local customer quality of service outage events not related to BPS disturbances. Sabotage reporting has degenerated into reporting of mischievous vandalism and minor theft occurences. This creates compliance documentation overburden and waste of limited funds needed for true BPS reliability concerns, and also adds nuisance calls to the FBI and Homeland Security.
No
Added to the scope: For EOP-004 add a provision for a reporting flow rather than everything going to the RE and NERC, that is something going like the DP and TOP reports to the BA, the BA to the RE, and the RE to NERC. This would allow for multiple related reports to be combined into a single coherent report as the reporting goes up the chain. For CIP-001 consider reporting flow as above with local law enforcement notification. Let an upper entity in the reporting chain decide when to contact Federal Agencies such as the BA or the RC.
No
No
Replace LSE with DP, and the Regional Reliability Organization with the Regional Entity.
Local Law enforcement agencies often are not friendly to Federal involvement with smaller problems they consider their "turf." Need to make sure the small stuff stays with them, however have a system of internal reporting that will catch coordinated sabotage efforts (multiple attacks on DPs and small BAs) at the RC or RE level who then can report to the Federal agencies. Currently EOP-004-1 requires small entities to report a "disturbance" if half of their firm customer load is lost. For some entities, this can be one small substation going down due to a bird. The "50% of total demand" requirement should be removed or improved to better define a true BPS disturbance.
Individual
Michael Puscas

United Illuminating
Yes
Yes
No
No
Add Distribution Provider
Individual
George Pettyjohn
Reliant Energy
Yes
EOP-004-1 indicates that Generators should analyze disturbances on the bulk electrical system or their facilities. Generators do not have the capability of analyzing the bulk electrical system other than Frequency. Even so, generators can not unilaterlly respond to what it thinks are disturbances. In the case of CAISO The Participating Generator Agreement prevents me from making any unilateral moves save for the direst frequency emergencies. If the System operator or Reliability Coordinator informs the generator that there is a disturbance and that logs and readouts etc. are required then the generator should respond with all available informaiton for the subject hours or time. Clearer responsibilities provide clearer results.
No
I think Generator opeators shuld be excluded accept to provide requested information from the System Operator or Reliability coordinator.
No
No
EOOP-004-1 should exclude the generator operator from disturbance reporting except providing the system operator or reliability coordinator with appropriate unit operation informaiton upon request. Acts of sabotage should be identified clearley and reported to the indicated authorities.
Individual
Judith A. James
Texas Regional Entity
Yes
Yes
No
No
Add GO and TO to the list of applicability. The intent of CIP-001-1 when it was first written was to have the proper and most likely entities associated directly with operations to be the ones to begin the reporting process in the case of sabotage on the system. In the ERCOT Region and other regions in the US, the GOP may not be physically located at the site. The GOP is often removed from the minute-by-minute responsibilities of plant operations and, therefore, may be less able to react to physical sabotage at the location/plant/facility in a timely manner. The concern is that, in the case of an actual sabotage event, the failure to report to the appropriate authorities in a timely manner may jeopardize the reliability of the BPS. Therefore, the Generator Owner (GO) should be added to the list of applicability for CIP-001-1, because it is

the GO that is more likely to be on location at the generation site and thus aware of sabotage when it first occurs. This would disallow for any possible communication gap and put responsibility on all of the appropriate entities to report such an event. Additionally, and for the same reasons as adding the GO, the Transmission Owner (TO) should also be added to the list of applicability for reporting sabotage on its facilities.
Individual
Edward C. Stein
self
Yes
Yes
No
Yes
Individual
Chris Scanlon
Exelon
Yes
Yes
Consolidation of redundant requiremnts and clarifications of difficult to follow / interpret standards should be a high priority at NERC.
No
We are not sure what this question means. Who's Associated Business practices, NERC, Applicable Entities in the Standard, our business practices?
No
CIP-001, remove LSE's from the standard for the reasons identified in the FERC LSE order. Ad TO and DP. EOP-004, remove LSE's from the standard for the reasons identified in the FERC LSE order. Remove RRO's, they are not a user, owner, operator of the BES. Add DP or TO. Consider conditional applicability as in the UFLS standards, " the TO or DP who performs the functions specified in the standard..."
Exelon agrees this is a worthwhile project and that reliability will be enhanced and the compliance process will be simplified by clarifying terminology and reporting requirements in these standards. If nothing else, defining "Sabotage" so as to end interpretations of this term and the related requirements is necessary.
Group
SERC OC Standards Review Group
Entergy Services, Inc
No
The EOP-004-1 standard is an unnecessary duplication of existing DOE reporting requirements. This essentially exposes an entity to fines by NERC, enforced by FERC, for failure to comply with a DOE regulation, which seems improper to us. In addition, reporting requirements do not have an impact on the reliability of the BES
Yes
No

Business practices should not be considered in a standard.
No
The EOP-004-1 standard should not apply to the RRO.
Group
WECC
WECC
Yes
Yes
No
Yes
No
Group
Project 2007-02 Operating Personnel Comms Protocols SDT
NERC OPCP SDT
No
The Operating Personnel Communication Protocols standard drafting team respectfully requests that the Sabotage Reporting SAR Drafting Team incorporate the following into your proposed SAR: “Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have procedures for the communication of information concerning the Cyber and Physical emergency alerts in accordance with the conditions described in Attachment 1 Security Emergency Alerts .” The Operating Personnel Communications Protocols Project 2007-02 was initiated to ensure that real time system operators use standardized communication protocols during normal and emergency operations to improve situational awareness and shorten response time. The SDT developed a new COM-003-1 Standard that has yet to be posted and is dependent upon revising at least two other standards (CIP-001 and TOP Standard). COM-003 contains requirements that specify: 1. Use of three-part communication; 2. English language; 3. Common time zone; 4. NATO alpha-numeric alphabet; 5. Mutually agreed line identifiers; 6. The use of pre-defined system condition terminology such as those contained in the RCWG Alert Level Guide and EOP-002-2. This request is based on recent NERC Standards Committee direction to our team to incorporate the Reliability Coordinator Working Group’s (RCWG) Alert Level Guide into a Standard. The consensus of our team is that a TOP Standard is the most appropriate location for the Transmission Emergency Alert language from the Guide as the energy emergency alert language is currently described in EOP-002-2. The RCWG Guide proposes the use of pre-defined system condition descriptions for use during emergencies for reliability related information. This guide was developed in response to a Blackout Report recommendation. Our team placed the Transmission Emergency Alert language into a TOP standard. Since the Sabotage Reporting SAR DT intends to modifyCIP-001, we seek your consent to incorporate the cyber and physical security alert language to comply with the wishes of the Standards Committee. We believe that the CIP-001 Standard is the most appropriate location for this language for the following reasons: • The levels of emergency conditions related to the cyber and physical security of the electric system is directly related to Critical Infrastructure Protection. • The current version of CIP-001 already requires the timely reporting of actual and suspected security emergency conditions and the use of pre-defined terminology supports the efficient sharing of such information. The OPCP SDT includes the following text for the record. It is a proposed draft revision of CIP-001. A. Introduction 1. Title: Security Incidents 2. Number: CIP-001-2 3. Purpose: To ensure the recognition, communication and response to cyber and physical security incidents suspected or determined to be caused by sabotage. 4. Applicability 4.1. Reliability Coordinators. 4.2. Balancing Authorities. 4.3. Transmission Operators. 4.4. Generator Operators. 4.5. Load Serving Entities. 5. Effective

Date: The standard is effective the first day of the first calendar quarter after applicable regulatory approvals (or the standard otherwise becomes effective the first day of the first calendar quarter after NERC BOT adoption in those jurisdictions where regulatory approval is not required). B. Requirements R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of security threats on its facilities and multi site security threats affecting larger portions of the Interconnection. R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning the physical and cyber security status of their facilities in accordance with the conditions described in Attachment 1-CIP-001-1. R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with security threat or incident response guidelines, including personnel to contact, for reporting security threats and incidents. R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances. C. Measures M1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement 1 M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements 2 and 3. M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to procedures, policies, a letter of understanding, communication records, or other equivalent evidence that will be used to confirm that it has established communications contacts with the applicable, local FBI or RCMP officials to communicate sabotage events (Requirement 4). D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Enforcement Authority Regional Entity 1.2. Compliance Monitoring Period and Reset One or more of the following methods will be used to verify compliance: - Compliance Audits - Self-certifications - Spot Checking - Compliance Violation Investigations - Self-Reporting - Complaints 1.3. Data Retention The Transmission Operator, Transmission Owner, Balancing Authority, Reliability Coordinator, Generator Operator and Distribution Provider shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation: o The Transmission Operator, Transmission Owner, Balancing Authority, Reliability Coordinator, Generator Operator and Distribution Provider shall retain its current, in force document and any documents in force since the last compliance audit. o If a Transmission Operator, Transmission Owner, Balancing Authority, Reliability Coordinator, Generator Operator or Distribution Provider is found non-compliant, it shall keep information related to the non-compliance until found compliant. o The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records. 1.4. Additional Compliance Information None. 2. Levels of Non-Compliance: 2.1. Level 1: There shall be a separate Level 1 non-compliance, for every one of the following requirements that is in violation: 2.1.1 Does not have procedures for the recognition of and for making its operating personnel aware of sabotage events (R1). 2.1.2 Does not have procedures or guidelines for the communication of information concerning sabotage events to appropriate parties in the Interconnection (R2). 2.1.3 Has not established communications contacts, as specified in R4. 2.2. Level 2: Not applicable. 2.3. Level 3: Has not provided its operating personnel with sabotage response procedures or guidelines (R3). 2.4. Level 4:.Not applicable. E. Regional Differences None. Version History Version Date Action Change Tracking 0 April 1, 2005 Effective Date New 0 August 8, 2005 Removed “Proposed” from Effective Date Errata 1 November 1, 2006 Adopted by Board of Trustees Amended 1 April 4, 2007 Regulatory Approval — Effective Date New 2 March 2009 Added SEA attachment and updates to Effective Date and Compliance sections. New Attachment 1-CIP-001-2 Physical Security Emergency Alerts General Requirements 1. Initiation by Reliability Coordinator. A Physical Security Emergency Alert may be initiated only by a Reliability Coordinator at: a. The Reliability Coordinator’s own decision, b. By request from a Transmission Operator, c. By request from a Balancing Authority, or d. By request from federal, state, or local Law Enforcement Officials. 2. Situations for initiating alert. An Alert may be initiated for the following reasons: a. A physical threat affecting a control center, grid or generator asset has been identified, or b. A physical attack affecting a control center, grid or generator asset has occurred or is imminent. 3.

Notification. A Reliability Coordinator who initiates a Physical Security Emergency Alert shall notify all Transmission Operators and Balancing Authorities in its Reliability Area. The Reliability Coordinator shall also notify other Reliability Coordinators of the situation via the Reliability Coordinator Information System (RCIS) using the “CIP” category. Additionally, conference calls between Reliability Coordinators shall be held as necessary to communicate system conditions. The Reliability Coordinator shall also notify all Transmission Operators and Balancing Authorities in its Reliability Area and other Reliability Coordinators when the alert has changed levels or ended. Physical Security Emergency Alert Levels To ensure that all Reliability Coordinators clearly understand potential and actual Physical Security Emergency Alerts, NERC has established three levels of Security Emergency Alerts. The Reliability Coordinators will use these terms when explaining security alerts to each other. The Reliability Coordinator may declare whatever alert level is necessary, and need not proceed through the alerts sequentially. 1. Alert 1 – “Control Center / Bulk Electric System asset threat identified” Circumstances: A credible threat of physical attack on a Bulk Electric System asset has been communicated to the Reliability Coordinator. No physical attack has occurred at this point. Determining the credibility of any threat is a subjective process, but the following factors should be considered: a. The nature and specificity of the threat, b. The timing of the threat, c. Mode of threat communication, and d. The criticality of the threatened asset. During a Physical Security Emergency Alert Level 1, Reliability Coordinators, Transmission Operators and Balancing Authorities shall have the following responsibilities: i. Notification The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall post the declaration of the alert level along with the location of the affected facility on the RCIS under “CIP” and notify all Transmission Operators and Balancing Authorities in its Reliability Area. ii. Updating Status during the Physical Security Emergency Alert The declaring Entity shall update the Reliability Coordinator of any changes in the situation until the Alert Level 1 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 2. Alert 2 – “Verified Physical attack at a single site” Circumstances: A Reliability Coordinator, Transmission Operator, or Balancing Authority has identified a physical attack upon a control center, generator asset, or other bulk electric system asset. During a Physical Security Emergency Alert Level 2, Reliability Coordinators, Transmission Operators and Balancing Authorities shall have the following responsibilities: i. Notification The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall post the declaration of the alert level along with the location of the affected facility on the RCIS under “CIP” and notify all Transmission Operators and Balancing Authorities in its Reliability Area. ii. Updating Status during the Physical Security Emergency Alert The declaring Entity shall update the Reliability Coordinator of the situation a minimum of once per hour until the Alert Level 2 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 3. Alert 3 – “Verified Physical attack at multiple sites” Circumstances: Multiple attacks have been confirmed on control centers, generator assets or other bulk electric system assets. A Reliability Coordinator shall declare a Physical Security Emergency Alert 3 whenever: a. A Transmission Operator or Balancing Authority reports multiple physical attacks on bulk electric system assets, b. Multiple Transmission Operators or Balancing Authorities report one or more physical attacks on their bulk electric system assets. i. Notification The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall post the declaration of the alert level along with the location of the affected facility on the RCIS under “CIP” and notify all Transmission Operators and Balancing Authorities in its Reliability Area. ii. Updating Status during the Physical Security Emergency Alert The declaring Entity(ies) shall update the Reliability Coordinator of the situation a minimum of once per hour until the Alert Level 3 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 4. Alert 0 – “Termination of Alert Level” Circumstances: The threat which prompted the Physical Security Emergency Alert Level has diminished or has been removed. i. Notification The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall notify all other Reliability Coordinators via the RCIS, and it shall also notify all Transmission Operators and Balancing Authorities in its Reliability Area that the Alert Level has been terminated. Cyber Security Emergency Alerts Cyber Assets – Those programmable electronic devices and communication networks, including hardware, software, and data, associated with bulk electric system assets. Cyber Security Incident – Any malicious act or suspicious event that compromises, or attempts to compromise, the electronic or physical security perimeter of a critical cyber asset or disrupts or attempts to disrupt the operation of a critical cyber asset. Critical Cyber Asset – Those cyber assets essential to the reliable operation of critical assets. Electronic Security Perimeter – The logical border surrounding the network or group of sub-networks to which the critical cyber assets are connected, and for which access is controlled. Physical Security Perimeter – The physical border surrounding computer rooms, telecommunications rooms, operations

centers and other locations in which critical cyber assets are housed and for which access is controlled. General Requirements 1. Initiation - A Cyber Security Emergency Alert shall be initiated by: a. The Reliability Coordinator's analysis, b. By request from any NERC functional Model entitiy that Com-003-0 is applicable to. c. By request from federal, state, or local Law Enforcement Officials. 2. Situations for initiating alert. An Alert shall be initiated for the following reasons: a. A cyber threat affecting a control center or bulk electric system asset has been identified, or b. A cyber attack affecting a control center or bulk electric system has occurred or is imminent. 3. Notification. An entity who initiates a Cyber Security Emergency Alert shall make notification as per the NERC Functional model or as Regional / local instruction. The Reliability Coordinator shall notify FBI local office, Electricity Sector Information Sharing Analysis Center (ESISAC) and Department of Homeland Security. The Reliability Coordinator shall also notify as necessary other Reliability Coordinators of the situation via the Reliability Coordinator Information System (RCIS) using the "CIP" category. The Reliability Coordinator shall notify all Transmission Operators and Balancing Authorities in its Reliability Area and other Reliability Coordinators when the alert has changed levels or ended. Cyber Security Emergency Alert Levels To ensure that all applicable entities clearly understand potential and actual Cyber Security Emergency Alerts, three levels of Security Emergency Alerts shall be used. The Reliability Coordinators will use these terms when communicating security alerts to each other. When declaring the applicable alert level it is important to note that the applicable level can be determined without sequentially proceeding through levels. As an example given circumstances an Alert Level 3 could be called without previously being in an Alert Level 1 or Level 2 state. 1. Alert 1 – "Verified Control Center / Bulk Electric System Cyber Asset threat identified or imminent" What is "verified" - unknown or unauthorized access to a cyber device, unknown or unauthorized change to a cyber device (i,e., config file, O/S, firmware change. 'Verified' could mean the elimination of a false positive in your security monitoring system. 'Verified' could also be the differentiation between malicious and non-malicious (ie human error, not following policy, etc) intent. What is a "threat" - A threat can be perceived as any action or event that occurs where the monitoring authority was not previously made aware that that action would occur. With flimsy change control or access controls, field staff or technical staff performing troubleshooting or other maintenance may access or change devices without notifying the monitoring entity. The monitoring entity would have to treat this as a threat and take appropriate action to either isolate that device from the rest of the system, notify appropriate authority, dispatch a crew, etc Examples of threats - Over and above the examples above, another threat example could be a notification from DHS or other security agency that they have reason to believe a hack, virus or other cyber terrorism activity could occur. Also, noticing a distinct change in network traffic which could imply someone has intercepted your data and can manipulate it before sending it from the control room to the device being controlled or manipulating the data coming from the device before a controller seeing it and forcing them to perform an incorrect control event in reaction to erroneous data. Circumstances: A credible threat of Cyber attack on a Control Center or Bulk Electric System asset has been communicated to the Reliability Coordinator. No cyber attack has occurred at this point. Determining the credibility of any threat is a subjective process, but the following factors should be considered: a. The nature and specificity of the threat, b. The timing of the threat, c. Mode of threat communication, and d. The criticality of the threatened asset. During a Cyber Security Emergency Alert Level 1, applicable entities shall have the following responsibilities: i. Notification An entity who initiates a Cyber Security Emergency Alert Level 1 shall make notification as per the NERC Functional model or as Regional / local instruction. The Reliability Coordinator shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area. The Reliability Coordinator shall also notify as necessary the FBI local office, Electricity Sector Information Sharing Analysis Center (ESISAC) and Department of Homeland Security. ii. Updating Status during the Cyber Security Emergency Alert The declaring Entity shall update those applicable entities of any changes in the situation until the Alert Level 1 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 2. Alert 2 – "Verified Cyber attack on a Control Center or Bulk Electric System asset" Circumstances: An applicable entity has identified a cyber attack upon a control center or bulk electric system asset. During a Cyber Security Emergency Alert Level 2, applicable entities shall have the following responsibilities: i. Notification An entity who initiates a Cyber Security Emergency Alert Level 2 shall make notification as per the NERC Functional model or as Regional / local instruction. The Reliability Coordinator responsible shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area. The Reliability Coordinator shall also notify the FBI local office,

Electricity Sector Information Sharing Analysis Center (ESISAC) and Department of Homeland Security. ii. Updating Status during the Cyber Security Emergency Alert The declaring Entity shall provide updates of the situation a minimum of once per hour until the Alert Level 2 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 3. Alert 3 – “Verified Cyber attack at one or more Control Center or Bulk Electric System cyber asset” Circumstances: An applicable entity has identified a cyber attack upon a control center or bulk electric system asset and shall declare a Cyber Security Emergency Alert 3 whenever: a. A Transmission Operator or Balancing Authority reports one or more cyber attacks on bulk electric system that render an asset(s) unavailable. i. Notification An entity who initiates a Cyber Security Emergency Alert Level 3 shall make notification as per the NERC Functional model or as Regional / local instruction. The Reliability Coordinator shall post the declaration of the alert level along with the location of the affected facility on the RCIS under “CIP” and notify all Transmission Operators and Balancing Authorities in its Reliability Area. The Reliability Coordinator shall also notify the FBI local office, Electricity Sector Information Sharing Analysis Center (ESISAC) and Department of Homeland Security. ii. Updating Status during the Cyber Security Emergency Alert The declaring Entity(ies) shall provide an update of the situation a minimum of once per hour until the Alert Level 3 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 4. Alert 0 – “Termination of Alert Level” Circumstances: The threat which prompted the Cyber Security Emergency Alert Level has diminished or has been removed. i. Notification An entity who initiates a Cyber Security Emergency Alert shall make notification as per the NERC Functional model or as Regional / local instruction when situation has diminished or returned to normal. The Reliability Coordinator shall notify all other Reliability Coordinators via the RCIS, and it shall also notify all Transmission Operators and Balancing Authorities in its Reliability Area that the Alert Level has been terminated.
Individual
Jimmy Hartmann
ERCOT ISO
Yes
No
The scope should be modified to provide for a different treatment of reporting requirements that are administrative in nature, or that are after-the-fact (thus cannot impact reliability unless analysis and follow-up is not performed; even then, the impact would be at some future time). Reporting requirements which are of the nature to assist in identification of system concerns or which serve to prevent or mitigate on-going system problems (including, but not limited to, actual or attempted sabotage activity) should remain in standards, but should be separate and apart from the administrative reporting.
No
No
The Regional Reliability Organization is not a registered Functional Entity in the NERC registry. The applicability must be revised to more appropriately assign the requirements to registered functional entities. Also, the industry needs to recognize that there are other resources than generation for which the operators need to be included. Perhaps a demand-side resource should have a resource operator. This particular SAR may not be the appropriate venue for this, but control of resources which can be used to mitigate sabotage events or disturbance events may need to be addressed.
Due to the fact that both the CIP-001-1 and EOP-004-1 have similar reporting standards, initially combining the two sounds like a correct analysis. However, after further consideration and due to the critical nature of its intended function involving Security aspects, the CIP-001 should be intensely evaluated to determine if its intended purpose meets the threshold or criteria to stand alone. The existing standards for CIP-001-1 Sabotage Reporting may help prevent future mitigation actions caused by sabotage events. EOP-004-1 Disturbance Reporting is administrative in nature, thus the jeopardy of the Bulk Electric System reliability is

impacted only if analysis is not performed or if corrective follow-up actions are not implemented. Combining EOP-004 Standard requirements under the umbrella of the CIP -001 Standard would create a high profile Disturbance Reporting Standard. The industry would be better served if information defining sabotage was provided as well as a technical reference document on recognizing sabotage that would also clarify or state any personnel training requirements. All aspects of the intended functions must be reviewed before merging the two standards. At a minimum, we must consider modification that provides improved understanding of the reporting standards and implications as they are currently written.
Group
PSEG Enterprise Group Inc Companies
Public Service Electric and Gas Company
Yes
Yes
No
Yes
The PSEG Companies ask that the drafting team allow sufficient flexibilty for sabotage recognigion and reporting requirements such that nothing precludes ultilizing a single corporate-wide program for both bulk electic system assets and other businesses. PSEG's Sabotage Recognition, Response and Reporting Program is directed to all business areas which are directed to follow the same internal protocol that also satisfies the NERC Standards requirements. For example, for gas assets, PSEG's gas distribution business follows the PSEG corporate-wide program for sabotage recognition and response. PSEG agrees that some modifications should be made to CIP-001 (ex. better define or give examples of sabotage) and EOP-004 to make them clearer • If they are merged, then Sabotage will not be in the title (or the primary focus) because several of the Disturbances that reporting is required for in EOP-004 have nothing to do with sabotage. • EOP-004 has criteria listed in 4 places to determine when to send a report: o Criteria listed in EOP-004 Attachment 1 o Criteria listed in EOP-004 Attachment 2 o Criteria listed in top portion of Table 1-EOP-004 o Criteria listed in bottom potion of Table 1-EOP-004 Therefore, it would be much easier if there was one table of criteria for reference that addressed all of the reportable conditions and all of the applicable reports. • If the 2 standards are merged as suggested in the SAR, any differences in the reporting obligation for actual or attempted sabotage and reporting of disturbances must be clear.
Group
Northeast Power Coordinating Council
Northeast Power Coordinating Council
Yes
No
The SAR needs to be more specific in defining its objectives. CIP-001 Requirement R1 currently states: R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SDT needs to include the following objectives: 1. Develop clear definitions for the terms “operating personnel” and “sabotage events.” The definition of “operating personnel,” should be clarified and limited to staff at BES facilities. Operating personnel should report only those events which meet a clear, recognizable threshold as reportable potential sabotage events. There should be a consistent continent-wide list of examples or typical reportable and non-reportable events to help guide operating personnel. The term “sabotage event” needs to be defined. Clarification is required regarding when the determination of a sabotage event is made, e.g., upon first observation (requiring operating personnel be educated in discerning sabotage events), or upon later investigation by trained security personnel and law enforcement

individuals. The terms potential or suspected sabotage event for reporting purposes should be clarified or defined. 2. Define the obligations of Registered Entity operating personnel - who are required to be “aware of” such “sabotage events,” e.g., who, what, where, when, why and how, and what they are to do in response to this awareness. The SDT should clarify the use of the term “aware” in the standard. “Aware” can be interpreted in accordance with its largely passive, dictionary-based meaning, where being “aware” simply means knowing about something, such as a sabotage event. Alternatively, the Reliability Standard meaning of “aware” could refer to more active wording, involving more than mere awareness, e.g., “alert and quick to respond,” pointing to and requiring a specific affirmative response, i.e., reporting to the appropriate systems, governmental agencies, and regulatory bodies. EOP-004 The SDT needs to work on the following areas. 1. NERC reporting needs to be clarified. For example, Attachment 1 paragraph 6c states: Introduction …The entity on whose system a reportable disturbance occurs shall notify NERC ... 6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in: … c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance …” The sense of Attachment 1 is internally inconsistent between the introduction (“occurs”) and the required actions in 6c (“could have resulted in a system disturbance”). The initial intent appears to be only to report actual system disturbances. Yet, paragraph 6c adds the phrase “or could have resulted in” a potential system disturbance. This inconsistency should be clarified.

No

Yes

Individual

Rick Terrill

Luminant Power

Yes

Yes

Yes

The SAR drafting team should include in the SAR scope a review of the NRC sabotage and event reporting requirements to ensure there are no overlapping or conflicting requirements between NERC, FERC, and the NRC. The SAR scope should include a review of the CIP Cyber Security Standards and coordination with the CIP SDT to ensure that cyber sabotage reporting definitions are in concert, and ensure that cyber sabotage reporting requirements are not duplicated in multiple standards.

Yes

None

Individual

Rao Somayajula

ReliabilityFirst Corporation

Yes

Yes

No

Yes

Individual
Tony Kroskey
Brazos Electric Power Cooperative, Inc.
Yes
Yes
No
No
May need to consider adding Transmission Owner. I don't see a need for the RRO to be included as they are not owner/operators of grid facilities.
Individual
Paul Golden
PacifiCorp
Yes
Yes
No
No
LSE's don't generally own/operate facilities/systems that would experience a logical or physical sabotage event.
Group
Kansas City Power & Light
Kansas City Power & Light
Yes
Agree with the SAR that clarity would be helpful in establishing criteria regarding what constitutes sabotage reporting.
No
Agree with the scope of the SAR except for the applicable entities. See response to question #4.
No
No
Do not agree Load Serving Entities need to continue to be included for sabotage. According the NERC Functional Model, an LSE provides for estimating customer load and provides for the acquisition of transmission and energy to meet customer load demand. An LSE has no real impact on maintaining the reliability of electric network short of their planning function. Unfortunately, an LSE needs to be included for disturbance reporting to the DOE under certain conditions for loss of customer load. This may be a reason to maintain a separation of CIP-001 and EOP-004 so as not to unnecessarily include an LSE when it is not needed.
If it is desirable to keep CIP-001 and EOP-004 separate, it is recommended the SDT consider adding a reference in CIP-001 to the DOE reporting form either by name or by internet link in the standard.

Individual
Terry Harbour
MidAmerican Energy
No
MidAmerican Energy believes only EOP-004-1 is confusing and needs to modified or clarified. There is no need to combine the two standards. Standard EOP-004 could be clarified to eliminate references to sabotage which are already covered by CIP-001-1. Standard EOP-004 should be strictly limited to system events, not sabotage.
No
See the responses to questions 1 and 5.
Yes
Attachment TOP-005, section 2.9 speaks of “Multi-site sabotage” with no definition. The ES-ISAC 2008 advisory is an associated standard or practice on sabotage. All references to sabotage should be eliminated or retired except for CIP-001.
No
MidAmerican Energy believes the requirement for the Regional Reliability Organization should be removed from EOP-004-1 since the RRO is a holdover from making the standards enforceable. It is no longer appropriate for the regions to be named as responsible entities within the standards.
Conflicting time frames exist from document updates. Reporting should be consolidated to one form and / or site to minimize conflicts, confusion, and errors. 1) Reporting requirements for the outage of 50,000 or more customers in EOP-004-1 requires a report to be made within one hour while the form OE-417 requires a report be made within six hours of the outage. The six hour reference on the updated OE-417 form is the correct reference. 2) Reporting for either CIP-001 or EOP-004 should center on the DOE Form OE-417. This would eliminate confusion, simplify reporting for system operators thereby directly enhancing reliability during system events. This would also eliminate much of the duplicate material and attachments in EOP-004 3) Although it is beyond the scope of this SAR, the industry would benefit if there was a central location or link on the NERC website containing all reporting forms, including FERC, NERC, DOE, and ESIAC. This would enable System Operators to more efficiently locate and report events.
Individual
Darryl Curtis
Oncor Electric Delivery
Yes
Yes
No
Yes
No Additional Comments
Individual
Chris de Graffenried on behalf of Con Edison & O&R
Consolidated Edison Co. of New York, Inc.
Yes
No
GENERAL – CECONY and ORU support the general objectives of the SAR to merge existing standards CIP-001-1 – Sabotage Reporting and EOP-004-1 – Disturbance Reporting to improve clarity and remove redundancy. However, the SAR needs to be more specific in defining its objectives. CIP-001 Requirement R1

currently states: R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SDT needs to include the following objectives: 1. Develop clear definitions for the terms “operating personnel” and “sabotage events.” The definition of “operating personnel,” should be clarified and limited to staff at BES facilities. Operating personnel should report only those events which meet a clear, recognizable threshold as reportable potential sabotage events. There should be a consistent continent-wide list of examples or typical reportable and non-reportable events to help guide operating personnel. The term “sabotage event” needs to be defined. Clarification is required regarding when the determination of a sabotage event is made, e.g., upon first observation (requiring operating personnel be educated in discerning sabotage events), or upon later investigation by trained security personnel and law enforcement individuals. The terms potential or suspected sabotage event for reporting purposes should be clarified or defined. 2. Define the obligations of Registered Entity operating personnel - who are required to be “aware of” such “sabotage events,” e.g., who, what, where, when, why and how, and what they are to do in response to this awareness. The SDT should clarify the use of the term “aware” in the standard. “Aware” can be interpreted in accordance with its largely passive, dictionary-based meaning, where being “aware” simply means knowing about something, such as a sabotage event. Alternatively, the Reliability Standard meaning of “aware” could refer to more active wording, involving more than mere awareness, e.g., “alert and quick to respond,” pointing to and requiring a specific affirmative response, i.e., reporting to the appropriate systems, governmental agencies, and regulatory bodies. EOP-004 The SDT needs to work on the following areas. 1. NERC reporting needs to be clarified. For example, Attachment 1 paragraph 6c states: Introduction …The entity on whose system a reportable disturbance occurs shall notify NERC ... 6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in: … c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance …” The sense of Attachment 1 is internally inconsistent between the introduction (“occurs”) and the required actions in 6c (“could have resulted in a system disturbance”). The initial intent appears to be only to report actual system disturbances. Yet, paragraph 6c adds the phrase “or could have resulted in” a potential system disturbance. This inconsistency should be clarified.

No

Yes

Individual

Wayne Pourciau

Georgia System Operations Corp.

Yes

There is a need to eliminate burdensome reporting deadlines which interfere with the reliable operations or recovery of the BES. There is also a need to move requirements for reporting to NERC or Regional Entities (except for reporting of threats to physical or cyber security) from the Requirements section of Reliability Standards to elsewhere.

No

The scope of the SAR should be to move all requirements to report to NERC or Regional Entities out of the Requirements section of all Reliability Standards to elsewhere. This does not include reporting, communicating, or coordinating between reliability entities. The NERC/Region reporting requirements could be consolidated in another document and referenced in the Supporting References section of the Reliability Standards. The deadlines for reporting should be changed to realistic timeframes that do not interfere with operating the BES or responding to incidents yet still allow NERC and the Regions to accomplish their missions.

No

Business practices should not be part of a Reliability Standard. Neither should NERC/Region reporting requirements (except for reporting of threats to physical or cyber security). NERC may need to take some action in the case of threats but does not and cannot take any operational action for most of the reporting requirements that are presently in the Requirements section of the Reliability Standards.
No
EOP-004 should be retired. CIP-001 should not apply to LSEs other than those that are retail marketers.
Entity reporting to NERC/Regions is needed by NERC and the Regions to accomplish their missions of overseeing the reliability of the BES and enforcing compliance with Reliability Standards. An entity not reporting as quickly as possible does not harm the integrity of the Interconnection. In fact, it increases the risk to the BES to be investigating details and filling out forms during a time when attention should be on correcting or mitigating an incident.
Individual
Bob Thomas
Illinois Municipal Electric Agency
Yes
Simplification of reporting requirements should facilitate reliability.
Yes
Yes
A one-stop reporting tool/site would facilitate efficient reporting and compliance; e.g., further development of the ES-ISAC/CIPIS to include all reportable categories and automatic notification of required parties. A single report form would be best.
Yes
IMEA recommends the following considerations: Simplification of reportable events and the reporting process should be the overriding objective. NERC's Security Guideline for the Electricity Sector: Threat and Incident Reporting (Version 2.0) should be updated to support this standards developement initiative. At some point in the process, it may help if examples are given of events actually reported that did not need to be reported.
Individual
Kasia Mihalchuk
Manitoba Hydro
Yes
Yes
No
Yes
Group
IRC Standards Review Committee
IESO
Yes
Yes

No
No
We agree with the applicability of CIP-001-1 but question the need to include the RRO in EOP-004-1. Requirement R1 of EOP-004-1 can be turned into an industry developed and approved procedural requirement with details included in an appendix; whereas R5 can be changed to a requirement for the responsible entities to act on recommendations and to self-report compliance. Tracking and reviewing status of recommendation do not need to be performed by the RRO, or any entity for that matter, if a self-reporting mechanism is developed.
We suggest that the revision not be conducted with a preconceived notion that the two standards must be combined since there are some differences between sabotage and emergency system conditions, and in the communication and reporting processes and channels. We suggest the SDT start off with a neutral position to focus on improving the standards, then assess the pros and cons of merging the two based on technical merit only.
Group
Pepco Holdings, Inc. - Affiliates
Pepco Holdings, Inc.
Yes
PHI recommends merging these two standards into one.
Yes
No
No
As specified in Order 693, Regional Reliability Organizations are not to be assigned applicability. The revised standard(s) should contain the reporting form either directly or by reference and the RRO should be removed. The other EOP-004 requirements for RROs are now considered normal monitoring activities of the Regional Entities.
Consider CIP-008-2 as potentially having overlaps with the proposed standard
Individual
Jim Sorrels
AEP
Yes
No
Sabotage is a term of intent that is often determined after the fact by the registered entity and/or law enforcement officials. In fact, it is often difficult to determine in real-time the intent of a suspicious event. We would suggest that suspicious events become reportable at the point that the event is determined to have had sabotage intent. The entities should have a methodology to collect evidence, to have the evidence analyzed, and to report those events that are determined to have had the intent of sabotage.
Yes
The current reporting process necessitates multiple reports be sent to multiple parties, which is inefficient and may, inadvertently, result in alignment issues between the separate reports. We would recommend that a single report that combines NERC (CIPIS) and NERC ESISAC information be provided to NERC (CIPIS) that is systematically (programmatically) forwarded to all necessary entities. Further, updates to incidents would also go through NERC with the same electronic processing. Currently, we are not aware of a formal method to report incidents to the FBI, which should be also included in the distribution. The current reporting mechanism to the FBI JTTF is by telephone and the NERC platform described would provide more consistent reporting.
No

We would recommend that the Load Serving Entity (LSE) be removed from both standards, and that the Generator Owner and Transmission Owner be added to the resulting standard.
Group
FirstEnergy
FirstEnergy Corp.
Yes
Yes
We agree with the scope but would also like to see the following considered: 1. References to the DOE reporting process in EOP-004 need to be revised. They currently refer to the old EIA form. 2. Besides "sabotage", it may be helpful to clearly define "vandalism". It is vaguely written in the standards. Also, the process of "public appeals" for the DOE reportable requirements needs to be more clearly defined. 3. Consolidate documents covering reporting requirements. There are currently several documents that require reporting (EOP-004, CIP-001, DOE oe-417, and NERC's Security Guideline for the Electricity Sector: Threat and Incident Reporting). NERC also has the "Bulk Power System Disturbance Classification Scale" that does not completely align with all the reporting requirements. Therefore we recommend keeping this as simple as possible by combining all the reporting requirements into one standard. It would be beneficial to not require operators to have to go to 4 different documents to determine what to report on.
No
Although we are not aware of any NAESB business practices that need to be reviewed in conjunction with these proposed revisions, the SDT should consider reviewing current RTO procedures and practices that may require the need for variances in the revised standards.
No
The Regional Reliability Organization should be removed from the applicability of EOP-004-1. Any report they receive would be from the other entities listed. For consistency, the entities should report to the appropriate law enforcement agency. A report to the Reliability Entity should also be made for that entities information only.
1. Under Industry Need it states: "The existing requirements need to be revised to be more specific – and there needs to be more clarity in what sabotage looks like." The use of the phrase "more specific" should be qualified by adding "while not being too prescriptive". As with other reliability standards, we do not want a standard that causes unwarranted and unnecessary additional work and costs to an entity to comply. 2. As pointed out by the NERC Audit and Observation Team in the "Issues to be considered" for CIP-001, clarification is needed regarding contacting the FBI. Prior audits dwelled heavily on FBI notification. For example, our policy states that Corporate Security notifies the FBI. In recent events it appears that local law enforcement handles day to day activities. The notification process for contacting the FBI needs clarification along with specific instances in which to call them. Who should make the call to the FBI? It appears that a protocol needs to be developed to clarify what events require notifying the FBI. It could be as simple as after an incident a standard form is completed and forwarded to the FBI, letting them decide if follow up is needed. 3. We suggest aligning all reporting requirements for consistency. The items requiring reporting and the timelines to report are very inconsistent between NERC and the DOE. NERC's timelines are also not consistent with their own Security Guideline for the Electricity Sector: Threat and Incident Reporting.
Individual
Greg Rowland
Duke Energy
Yes
We agree that additional clarity is needed regarding sabotage and disturbance reporting. Requirements should be tightened up and triggering events/thresholds of materiality need to be better defined.
No
While we agree with the need for clarity in sabotage and disturbance reporting, we believe that the Standards Drafting Team should carefully consider whether there is a reliability-related need for each

requirement. Some disturbance reporting requirements are triggered not just to assist in real-time reliability but also to identify lessons-learned opportunities. If disturbance and sabotage reporting continue to be reliability standards, we believe that all linkages to lessons-learned/improvements need to be stripped out. We have other forums to identify lessons-learned opportunities and to follow-up on those opportunities. Also, requirements to report possible non-compliances should be eliminated. We strongly support voluntary self-reporting, but not mandatory self-reporting.
No
No
It's unclear to us that the RRO should continue to be an applicable entity.
Individual
Howard Rulf
We Energies
Yes
No
Consider including the sabotage issues in IRO-014-1 R 1.1.1 footnote 1 and TOP-005-1 Attachment 1, 2.9.
No
Yes
Group
Electric Market Policy
Dominion Resources Inc.
Yes
Comments: Agree with the statement that sabotage is hard to determine in real time by operations staffs. The determination of sabotage should be left up to law enforcement. They have the knowledge and peer contacts needed to adequately determine whether physical or cyber intrusions are merely malicious acts or coordinated efforts (sabotage). The operators should only be required to report physical and cyber intrusions to law enforcement. All other reporting requirements should apply to law enforcement once a determination of sabotage has been made. If the recommendations above are not to be accepted, then we have the following comments: CIP-001-1 1) R1 – states entities "shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and "multi-site sabotage" affecting larger portions of the Interconnection. The SAR notes that the industry objects to the multi-site requirement, most likely because the term is ambiguous. If this term remains in the standard, it needs to be clearly defined and responsibilities for obtaining (how do you get this information and from whom?) and distributing need to be included. 2) R1 – audits have shown confusion over the requirement to make operating personnel aware of sabotage events. The term operating personnel needs to be defined. Are they the individuals responsible for operating the facility, coordinating with other entities (i.e., RC, BA, TOP, GOP, and LSE)? It has been suggested that notification is required to all personnel at a facility. Keep in mind the purpose of the standard is to ensure sabotage events are properly reported, not to address emergency response. 3) R1 – The SAR (NERC Audit and Observation Team) notes that Registered Entities have processes and procedures in place, but not all personnel have been trained. There is no specific training requirement in the standard. 4) R2 & R3 – I agree with the SAR that sabotage needs to be defined and these requirements should be more specific with respect to the information to be communicated. It seems to me that the standard should mirror the criteria contained in DOE OE-417. The emphasis should be placed on ensuring that the same information communicated to DOE is shared with the appropriate parties in the Interconnection. 5) R4 – I agree with the SAR (NERC Audit and Observation Team) comments regarding the intention of this requirement. There is no language that directs contact with FBI or RCMP

although that is what is implied by the Purpose statement. 6) VRF Comments – I'm not sure what is intended by the statement "Adequate procedures will insure it is unlikely to lead to bulk electric system instability, separation, or cascading failures." The purpose of the standard is that of communication. No operational decisions or actions are directed by this standard, nor does it require entities to address operational aspects resulting from sabotage. 7) The potential exists for overlapping sabotage reporting requirements at nuclear power plants due to multiple regulators (Nuclear Regulatory Commission (NRC) – 10 CFR 73 and Federal Energy Regulatory Commission (FERC) – NUC-001-1). Some entities may have revised existing NRC driven procedures to accommodate reporting requirements of both regulators. Because of the restrictions placed on NRC driven documents (i.e., procedures are classified as "safeguards information"), it can be difficult to demonstrate compliance to NERC and/or FERC without ensuring that the individuals are qualified for receipt of such information per 10 CFR 73. Additionally, multiple procedures may have the unintended consequence of delaying appropriate communication. EOP-004-1 Consider removing Attachment 2 as the information is duplicated in DOE Form OE-417. A simple reference to the form should suffice.
Yes
No
No
Applicability should not apply to LSE unless they have physical assets. If they do not have such assets, they are unable to determine how many customers are out, how much load was lost or the duration of an outage. We continue to question the need for the LSE entity in reliability standards. End use customer load is either connected to transmission or distribution facilities. So, the applicable planner has to plan for that load when designing its facilities or the load will not have reliable service. To the extent that energy and capacity for that load is supplied by an entity other than the TO or DP, the TO or DP should have interconnection requirements that compel the supplier to provide any and all data necessary to meet the requirements of reliability standards.
CIP-008-1 Incident Reporting and Response Planning – include some requirements that require coordination with the requirements addressed in this project.
Individual
Jianmei Chai
Consumers Energy Company
Yes
Yes
No
Yes
Individual
Mike Sonnelitter
NextEra Energy Resources, LLC
Yes
No
The scope of the SAR should not include Generator Operators.
No

No
The scope of the proposed SAR should not include the Generator Operator.
No comment.
Individual
D. Bryan Guy
Progress Energy
No
No. It is not clear that the issues listed in a revised standard will improve reliability. Revision based on redundancy is not sufficient reason for combination. Extensive documentation efforts have been made to comply with the current Standards. Unless combining these Standards provides compelling Reliability benefit, it is not worth the industry's resources to revise existing documentation and processes for the sake of eliminating redundancy. Redundancy issues were raised prior to the ERO adopting the initial Standard set into law. We have noted the other issues raised in the SAR, however, it is still unclear where the Reliability benefit of this SAR is evidenced.
No
No. If this SAR moves forward other standards may need to be considered. For example, in CIP-008, incident reporting for cyber incidents leads to filing of the OE-417 form.
Yes
Yes. If this SAR moves forward other practices such as those required by CIP-008 (cyber incident reporting via the OE-417 form) may need to be considered.
Yes
Group
Bonneville Power Administration
BPA Transmission Reliability Program
No
Eliminating a single standard by consolidating two standards does not improve reliability. All of the defined actions are indeed being taken now.
No
Leave as is, all requiremnets for reporting are now covered. A common definition of sabotage is already widely available.
No
Yes
Individual
Kirit Shah
Ameren
Yes
No
There seems to be an open slate including the following language in the scope "The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards (see tables for each standard at the end of this SAR for more detailed information)." The unnamed improvements should be limited to those requirements that relate only to Disturbance and Sabotage NOT a general wish list(or witch hunt).

No
Yes
None
Group
MRO NERC Standards Review Subcommittee
Michael Brytowski
Yes
No
The MRO NSRS would like to keep the references to the DOE reporting form.
Yes
No
As FERC has directed, the RRO should be removed since they are not owners or operators of the BES.
A. The SAR states that there may be impact on a related standard, COM-003-1 (page SAR-5). Is the SDT referring to Project 2007-02, Operating Personnel Communication Protocols? If so, this is a SAR too and should not be used as a reference. B. CIP-001-1 and EOP-004-1 should be combined into one EOP Standard. C. Within EOP-004-1 there is industry confusion on what form to submit in the event of an event. There should only be one form for the new combination Standard eliminating the need for reporting form attachments. It should be the DOE Form, OE-417. Although it is beyond the scope of this SAR, it would greatly benefit industry if there was a central location on the NERC website containing ALL reporting forms, including FERC, NERC, DOE, and ESIAC. This would enable the System Operators to efficiently locate the most current version of the appropriate form in order to report events. D. The word Disturbance is primarily used in other Standards as in, Disturbance Control Standard or system separation due to a disturbance. Should the NERC definition be updated? Should the word “Sabotage” be defined by NERC? Additionally, we recommend that one definition of “Sabotage” be utilized industry-wide, instead of varying definitions by multiple groups like the DOE, ESIAC, etc.

Consideration of Comments on Project 2009-01 — SAR for Disturbance and Sabotage Reporting

The Disturbance and Sabotage Reporting SAR Drafting Team (DSR SAR DT) thanks all commenters who submitted comments on the first draft SAR. The SAR was posted for a 30-day public comment period from April 22, 2009 through May 21, 2009. The stakeholders were asked to provide feedback on the documents through a special Electronic Comment Form. There were 40 sets of comments, including comments from more than 120 different people from over 60 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

The majority of stakeholders agree that there is a reliability related need to support modifying CIP-001-1 and EOP-004-1. Of those stakeholders providing comments, they predominantly agreed with the reliability-related reason for the SAR but offered the following concerns:

1) Concerns with applicability of the requirements: The SAR DT notes that applicability will be determined by the final requirements that are written for the standard.
2) Concerns on combining the standards: The SAR DT notes that the Purpose of the SAR indicates that the standards *may* be merged to eliminate redundancy and provide clarity. It will be up to the Standard Drafting team to make this determination through the Standard Development Process (with stakeholder input).
3) Concerns with the definition of sabotage and the inclusion of vandalism, thresholds for defining sabotage, etc.
4) Concerns on onerous or duplicative reporting: The Brief Description section of the SAR states "Specific references to the DOE form need to be eliminated". This should address its concerns.

The SAR DT does not feel that the SAR should be revised based on these comments. The SAR DT will forward these comments to the Standard Drafting Team for its consideration in the drafting of the standards.

The majority of stakeholders agree with the scope of the SAR. Several stakeholders offered suggestions for items to include in the SAR, however the SAR DT believes that these comments may be too prescriptive to include with the SAR. The team feels that inclusion of these types of comments would prevent the Standard Drafting Team from having the ability to develop standard(s) based on stakeholder consensus. The SAR DT will forward these comments to the Standard Drafting Team for its consideration. Some of the comments received include:

1) The inclusion of specific definitions in the SAR (operating personnel, sabotage events, obligations): The SAR DT believes that this would be too prescriptive and believe that this should be addressed by the Standard Drafting Team.
2) Consolidate documents covering reporting requirements: The SAR DT agrees and suggests that the Standard Drafting Team investigate a "one-stop-shopping" solution for the various reports required, including the DOE report.

Stakeholders did not identify any associated business practices for consideration under the SAR. One stakeholder identified a related standard that references multi-site sabotage. The team has included a reference to TOP-005, section 2.9 (Appendix 1) in the SAR under Related Standards. Two stakeholders suggested that Business Practices should not be considered in a standard. The SAR DT notes that standard development projects must not invalidate business practices that are already in place and aids in coordination with North American Energy Standards Board (NAESB).

Many stakeholders had comments regarding applicability of the two standards. Based on these comments, the SAR DT has added Transmission Owner, Generator Owner and Distribution Provider to the Applicability section of the SAR as *possible* entities in the standard(s) developed under this SAR as the Standard Drafting team may have a need to include them in the standard(s). The applicability of Load-Serving Entity or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements through the Standard Development Process. The three main comments were:

1) Regional Reliability Organization applicability: Several commenters do not feel the RRO should be in the standards. The DSR SAR DT concurs and notes that the SAR states that "EOP-004 has some 'fill-in-the-blank' components to eliminate". This will remove the RRO from applicability.
2) Load-Serving Entity/Distribution Provider: Several stakeholders do not feel that the standards should be applicable to LSEs, but should apply to Distribution Providers. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the standard as the Standard Drafting team may have a need to include them in the standard(s). The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements through the Standard Development Process.
3) Transmission Owner/Generator Owner: Several stakeholders have indicated a need to include the TO as an applicable entity. A couple of those would also include the GO. The SAR DT discussed the addition of the TO and GO. The team has a concern that there may be duplication of requirements between the TO/TOP and GO/GOP if the TO and GO are added to the SAR. That being said, the team added the TO and GO to the applicability of the SAR so that the Standard Drafting team may consider these entities for applicability. The applicability of requirements will ultimately be determined by the Standard Drafting Team as it develops the requirements through the Standard Development Process.

Stakeholders provided many good comments that should be considered in the development of the standards under this project. The SAR DT does not believe that these comments require any significant revisions to the SAR, but will forward these comments to the Standard Drafting Team for its consideration in drafting the standard(s). The comments include:

1) Consolidation of reports: The SAR DT agrees with this concept and will forward the comment to the Standard Drafting Team for its consideration.
2) Concerns about pre-determination of combining CIP-001 and EOP-004 into one standard: The SAR states: CIP-001 may be merged with EOP-004 to eliminate redundancies. The two standards may be left separate.

3) Reporting criteria in multiple tables: The team agrees that it would be easier if there were only one table. Part of this scope of this project is to eliminate redundancies and make general improvements to the standard. The team also agrees that the requirements developed should be clear in their reliability objective.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

1. Do you agree that there is a reliability-related reason to support modifying CIP-001-1 and EOP-004-1? If not, please explain in the comment area. 12

2. Do you agree with the scope of the proposed SAR? If not, please explain what should be added or deleted to the proposed scope. 20

3. Are you aware of any associated business practices that we should consider with this SAR? If yes, please explain in the comment area. 38

4. CIP-001-1 applies to the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, and the Load-serving Entity. EOP-004-1 applies to the same entities, plus the Regional Reliability Organization. Do you agree with the applicability of the existing CIP-001-1 and the existing EOP-004-1? If no, please identify what you believe should be modified. 43

5. If you have any other comments on the SAR or proposed modifications to CIP-001-1 and EOP-004-1 that you haven't provided in response to the previous questions, please provide them here. 51

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Jim Case	SERC OC Standards Review Group	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Al McMeekin	SCE&G	SERC	1, 3, 5
2.	Eugene Warnecke	Ameren	SERC	1, 3, 5
3.	Gary Hutson	SMEPA	SERC	1, 3, 5
4.	Melinda Montgomery	Entergy	SERC	1, 3
5.	Tom Sims	Southern	SERC	1, 3, 5
6.	Marc Butts	Southern	SERC	1, 3, 5
7.	Chris Bradley	BREC	SERC	1, 3, 5
8.	Tom Kanzlik	SCE&G	SERC	1, 3, 5
9.	Paul Turner	Ga Systems Operations Corp.	SERC	3
10.	Phil Creech	Progress Energy Carolinas	SERC	1, 3, 5
11.	Vicky Budreau	SCPSA	SERC	1, 3, 5, 9
12.	Renee Free	SCPSCA	SERC	9
13.	Mike Clements	TVA	SERC	1, 3, 5, 9
14.	Travis Sykes	TVA	SERC	1, 3, 5

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
15.	John Troha		SERC	RFC						10			
2.	Group	Harry Tom	Project 2007-02 Operating Personnel Comms Protocols SDT	X	X			X				X	X
	Additional Member		**Additional Organization**	**Region**						**Segment Selection**			
1.	Lloyd Snyder		GSOC	SERC						1			
2.	Tom Irvine		HydroOne	NPCC						1, 9			
3.	Alan Allgower		ERCOT	ERCOT						10			
4.	Harvie Beavers		Colmac Clarion/Piney Creek LP	RFC						5			
5.	Mark L. Bradley		ITC	MRO						1			
6.	Mike Brost		JEA	FRCC						1			
7.	William D Ellard		CAISO	WECC						10			
8.	Ronald Goins		MISO	MRO						10			
9.	Leanne Harrison		PJM	RFC						10			
10.	James McGovern		ISO-NE	NPCC						10			
11.	Wayne Mitchell		Entergy	SERC						1			
12.	John Stephens		City Utilities of Springfield	RFC						1			
13.	Fred Waites		Southern Company	SERC						1			
3.	Group	Kenneth D. Brown	PSEG Enterprise Group Inc Companies	X		X							
	Additional Member		**Additional Organization**	**Region**						**Segment Selection**			
1.	Clint Bogan		PSEG Fossil LLC	RFC						5			
2.	James Hebson		PSEG Energy Resources & Trade	RFC						6			
3.	Gary Grysko		PSEG Power Connecticut	NPCC						5			
4.	Dominic DiBari		PSEG Texas LLC	ERCOT						5			
4.	Group	Guy Zito	Northeast Power Coordinating Council										X
	Additional Member		**Additional Organization**	**Region**						**Segment Selection**			
1.	Ralph Rufrano		New York Power Authority	NPCC						5			
2.	Alan Adamson		New York State Reliability Council	NPCC						10			

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Greg Campoli		New York Independent System Operator	NPCC						2			
4.	Roger Champagne		Hydro-Quebec TransEnergie	NPCC						2			
5.	Kurtis Chong		Independent Electricity System Operator	NPCC						2			
6.	Sylvain Clermont		Hydro-Quebec TransEnergie	NPCC						1			
7.	Manuel Couto		National Grid	NPCC						1			
8.	Chris de Graffenried		Consolidated Edison Co. of New York, Inc.	NPCC						1			
9.	Brian Evans-Mongeon		Utility Services	NPCC						8			
10.	Mike Garton		Dominion Resources Services, inc.	NPCC						5			
11.	Mike Gildea		Constellation Energy	NPCC						6			
12.	Brian Gooder		Ontario Power Generation Incorporated	NPCC						5			
13.	Kathleen Goodman		ISO - New England	NPCC						2			
14.	David Kiguel		Hydro One Networks, Inc.	NPCC						1			
15.	Michael Lombardi		Northeast Utilities	NPCC						1			
16.	Randy MacDonald		New Brunswick System Operator	NPCC						2			
17.	Bruce Metruck		New York Power Authority	NPCC						6			
18.	Robert Pellegrini		The United Illuminating Company	NPCC						1			
19.	Michael Schiavone		National Grid	NPCC						1			
20.	Michael Sonnelitter		FPL Energy/NextEra Energy	NPCC						5			
21.	Peter Yost		Consolidated Edison Co. of New York, Inc.	NPCC						3			
22.	Lee Pedowicz		Northeast Power Coordinating Council	NPCC						10			
23.	Gerry Dunbar		Northeast Power Coordinating Council	NPCC						10			
5.	Group	Michael Gammon	Kansas City Power & Light	X		X		X	X				
	Additional Member		Additional Organization	Region						Segment Selection			
1.	Joe Doetzl		Kansas City Power & Light	SPP						1, 3, 5, 6			
2.	John Breckenridge		Kansas City Power & Light	SPP						1, 3, 5, 6			
6.	Group	Ben Li	IRC Standards Review Committee		X								
	Additional Member		Additional Organization	Region						Segment Selection			

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1. James Castle			NYISO	NPCC						2			
2. Charles Yeung			SPP	SPP						2			
3. Anita Lee			AESO	WECC						2			
4. Matt Goldberg			ISO-NE	NPCC						2			
5. Bill Phillips			MISO	MRO						2			
6. Steve Myers			ERCOT	ERCOT						2			
7. Lourdes Estrada-Salinero			CAISO	WECC						2			
7.	Group	Richard Kafka	Pepco Holdings, Inc. - Affiliates	X		X		X	X				
Additional Member			Additional Organization	Region						Segment Selection			
1. Kara Dundas			Conectiv Energy Supply, Inc.	RFC						5			
2. Tony Gabrielli			Conectiv Energy Supply, Inc.	RFC						5			
3. George Gacser			Potomac Electric Power Co.	RFC						1, 3, 5			
4. E. W. Stowe			Pepco Holdings, Inc	RFC						1, 3, 5			
5. Mark Godfrey			Pepco Holdings, Inc	RFC						1, 3			
8.	Group	Sam Ciccone	FirstEnergy	X		X	X	X	X				
Additional Member			Additional Organization	Region						Segment Selection			
1. Jim Eckels			FE	RFC						1			
2. John Martinez			FE	RFC						1			
3. John Reed			FE	RFC						1			
4. Dave Folk			FE	RFC						1, 3, 4, 5, 6			
5. Doug Hohlbaugh			FE	RFC						1, 3, 4, 5, 6			
6. Larry Hartley			FE	RFC						3			
9.	Group	Jalal Babik	Electric Market Policy	X		X		X	X				
Additional Member			Additional Organization	Region						Segment Selection			
1. Louis Slade				SERC						6			
2. Mike Garton				NPCC						5			

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
10.	Group	Denise Koehn	Bonneville Power Administration	X		X		X	X				

Additional Member	Additional Organization	Region	Segment Selection
1. Theodore Snodgrass	Dispatch	WECC	1

11.	Group	Michael Brytowski	MRO NERC Standards Review Subcommittee										X

Additional Member	Additional Organization	Region	Segment Selection
1. Carol Gerou	MRO	MRO	10
2. Neal Balu	WPS	MRO	3, 4, 5, 6
3. Pam Sordet	XCEL	MRO	1, 3, 5, 6
4. Joe DePoorter	MGE	MRO	3, 4, 5, 6
5. Ken Goldsmith	ALTW	MRO	4
6. Jim Haigh	WAPA	MRO	1, 6
7. Terry Harbour	MEC	MRO	1, 3, 5, 6
8. Joseph Knight	GRE	MRO	1, 3, 5, 6
9. Scott Nickels	RPU	MRO	3, 4, 5, 6
10. Dave Rudolph	BEPC	MRO	1, 3, 5, 6
11. Eric Ruskamp	LES	MRO	1, 3, 5, 6

12.	Individual	Stephen V. Fisher	Lands Energy Consulting										
13.	Individual	Brent Hebert	Calpine Corporation					X					
14.	Individual	Steve Toth	Covanta					X					
15.	Individual	Harvie Beavers	Colmac Clarion					X					
16.	Individual	Russell A. Noble	Cowlitz County PUD			X							
17.	Individual	Michael Puscas	United Illuminating	X		X							
18.	Individual	George Pettyjohn	Reliant Energy					X					

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
19.	Individual	Judith A. James	Texas Regional Entity										
20.	Individual	Edward C. Stein	self								X		
21.	Individual	Chris Scanlon	Exelon	X		X		X	X				
22.	Individual	Mike Davis	WECC										X
23.	Individual	Jimmy Hartmann	ERCOT ISO		X								
24.	Individual	Rick Terrill	Luminant Power					X					
25.	Individual	Rao Somayajula	ReliabilityFirst Corporation										X
26.	Individual	Tony Kroskey	Brazos Electric Power Cooperative, Inc.	X									
27.	Individual	Paul Golden	PacifiCorp	X		X		X	X				
28.	Individual	Terry Harbour	MidAmerican Energy	X									
29.	Individual	Darryl Curtis	Oncor Electric Delivery	X									
30.	Individual	Chris de Graffenried on behalf of Con Edison & O&R	Consolidated Edison Co. of New York, Inc.	X		X			X				
31.	Individual	Wayne Pourciau	Georgia System Operations Corp.			X							
32.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
33.	Individual	Kasia Mihalchuk	Manitoba Hydro	X		X		X	X				
34.	Individual	Jim Sorrels	AEP	X		X		X	X				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
35.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
36.	Individual	Howard Rulf	We Energies			X	X	X					
37.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
38.	Individual	Mike Sonnelitter	NextEra Energy Resources, LLC					X					
39.	Individual	D. Bryan Guy	Progress Energy	X		X		X					
40.	Individual	Kirit Shah	Ameren	X		X		X	X				

1. Do you agree that there is a reliability-related reason to support modifying CIP-001-1 and EOP-004-1? If not, please explain in the comment area.

Summary Consideration: The majority of stakeholders agree that there is a reliability related need to support modifying CIP-001-1 and EOP-004-1. Of those stakeholders providing comments, they predominantly agreed with the reliability-related reason for the SAR but offered the following concerns:

1) Applicability of the requirements: The SAR DT notes that applicability will be determined by the final requirements that are written for the standard.
2) Combining the standards: The SAR DT notes that the Purpose of the SAR indicates that the standards *may* be merged to eliminate redundancy and provide clarity. It will be up to the Standard Drafting team to make this determination through the Standard Development Process (with stakeholder input).
3) Definition of sabotage and the inclusion of vandalism, thresholds for defining sabotage, etc.
4) Onerous or duplicative reporting: The Brief Description section of the SAR states "Specific references to the DOE form need to be eliminated". This should address any concerns.

The SAR DT will forward these comments to the Standard Drafting Team for its consideration in the drafting of the standards.

Organization	Yes or No	Question 1 Comment
SERC OC Standards Review Group	No	The EOP-004-1 standard is an unnecessary duplication of existing DOE reporting requirements. This essentially exposes an entity to fines by NERC, enforced by FERC, for failure to comply with a DOE regulation, which seems improper to us. In addition, reporting requirements do not have an impact on the reliability of the BES
Response: The DSR SAR DT thanks you for your comment. The Brief Description section of the SAR states "Specific references to the DOE form need to be eliminated".		
MidAmerican Energy	No	MidAmerican Energy believes only EOP-004-1 is confusing and needs to modified or clarified. There is no need to combine the two standards. Standard EOP-004 could be clarified to eliminate references to sabotage which are already covered by CIP-001-1. Standard EOP-004 should be strictly limited to system events, not sabotage.
Response: The DSR SAR DT thanks you for your comment. The SAR DT notes that the Purpose of the SAR indicates that the standards *may* be merged to eliminate redundancy and provide clarity. It will be up to the Standard Drafting Team to make this determination through the Standard Development Process (with stakeholder input).		

Organization	Yes or No	Question 1 Comment
Bonneville Power Administration	No	Eliminating a single standard by consolidating two standards does not improve reliability. All of the defined actions are indeed being taken now.
Response: The DSR SAR DT thanks you for your comment. The SAR DT notes that the Purpose of the SAR indicates that the standards *may* be merged to eliminate redundancy and provide clarity. It will be up to the Standard Drafting team to make this determination through the Standard Development Process (with stakeholder input).		
Progress Energy	No	No. It is not clear that the issues listed in a revised standard will improve reliability. Revision based on redundancy is not sufficient reason for combination. Extensive documentation efforts have been made to comply with the current Standards. Unless combining these Standards provides compelling Reliability benefit, it is not worth the industry's resources to revise existing documentation and processes for the sake of eliminating redundancy. Redundancy issues were raised prior to the ERO adopting the initial Standard set into law. We have noted the other issues raised in the SAR, however, it is still unclear where the Reliability benefit of this SAR is evidenced.
Response: The DSR SAR DT thanks you for your comment. Industry consensus indicates that eliminating redundancy between standards is required to avoid potential double jeopardy issues with compliance to the standards. Furthermore, one of the FERC Order 693 directives for CIP-001 is: **Explore ways to reduce redundant reporting, including central coordination of sabotage reports and a uniform reporting format.**		
Kansas City Power & Light	Yes	Agree with the SAR that clarity would be helpful in establishing criteria regarding what constitutes sabotage reporting.
Response: The DSR SAR DT thanks you for your comment. One of the FERC Order 693 directives for CIP-001 is: **Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event.**		
Pepco Holdings, Inc. - Affiliates	Yes	PHI recommends merging these two standards into one.
Response: The DSR SAR DT thanks you for your comment. The SAR DT notes that the Purpose of the SAR indicates that the standards *may* be merged to eliminate redundancy and provide clarity. It will be up to the Standard Drafting team to make this determination through the Standard Development Process (with stakeholder input).		
Electric Market Policy	Yes	Comments: Agree with the statement that sabotage is hard to determine in real time by operations staffs. The determination of sabotage should be left up to law enforcement. They have the knowledge and peer contacts needed to adequately determine whether physical or cyber intrusions are merely malicious acts or coordinated efforts (sabotage).

Organization	Yes or No	Question 1 Comment
		The operators should only be required to report physical and cyber intrusions to law enforcement. All other reporting requirements should apply to law enforcement once a determination of sabotage has been made. If the recommendations above are not to be accepted, then we have the following comments: CIP-001-1 1) R1 states entities shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SAR notes that the industry objects to the multi-site requirement, most likely because the term is ambiguous. If this term remains in the standard, it needs to be clearly defined and responsibilities for obtaining (how do you get this information and from whom?) and distributing need to be included. 2) R1 audits have shown confusion over the requirement to make operating personnel aware of sabotage events. The term operating personnel needs to be defined. Are they the individuals responsible for operating the facility, coordinating with other entities (i.e., RC, BA, TOP, GOP, and LSE)? It has been suggested that notification is required to all personnel at a facility. Keep in mind the purpose of the standard is to ensure sabotage events are properly reported, not to address emergency response. 3) R1 The SAR (NERC Audit and Observation Team) notes that Registered Entities have processes and procedures in place, but not all personnel have been trained. There is no specific training requirement in the standard. 4) R2 & R3 I agree with the SAR that sabotage needs to be defined and these requirements should be more specific with respect to the information to be communicated. It seems to me that the standard should mirror the criteria contained in DOE OE-417. The emphasis should be placed on ensuring that the same information communicated to DOE is shared with the appropriate parties in the Interconnection. 5) R4 I agree with the SAR (NERC Audit and Observation Team) comments regarding the intention of this requirement. There is no language that directs contact with FBI or RCMP although that is what is implied by the Purpose statement. 6) VRF Comments I'm not sure what is intended by the statement Adequate procedures will insure it is unlikely to lead to bulk electric system instability, separation, or cascading failures? The purpose of the standard is that of communication. No operational decisions or actions are directed by this standard, nor does it require entities to address operational aspects resulting from sabotage. 7) The potential exists for overlapping sabotage reporting requirements at nuclear power plants due to multiple regulators (Nuclear Regulatory Commission (NRC) 10 CFR 73 and Federal Energy Regulatory Commission (FERC) NUC-001-1). Some entities may have revised existing NRC driven procedures to accommodate reporting requirements of both regulators. Because of the restrictions placed on NRC driven documents (i.e., procedures are classified as safeguards information), it can be difficult to demonstrate compliance to NERC and/or FERC without ensuring that the individuals are qualified for receipt of such information per 10 CFR 73. Additionally, multiple procedures may have the unintended consequence of delaying appropriate communication.EOP-004-1Consider removing Attachment 2 as the information is

Organization	Yes or No	Question 1 Comment
		duplicated in DOE Form OE-417. A simple reference to the form should suffice.
Response: The DSR SAR DT thanks you for your comment. The team notes that your comments relate directly to potential revisions of the standard requirements. The team will pass your comments along to the Standards Drafting Team for its consideration. For item 4, one of the FERC Order 693 directives for CIP-001 is: **Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event.**		
Lands Energy Consulting	Yes	I have worked with 5 Northwest public utilities on developing procedures related to CIP-001-1 and EOP-004-1. All 5 utilities operate electric systems in fairly remote locations and are embedded in a larger utility's Balancing Authority/Transmission Operator area. A. CIP-001-1 - Developing procedures to unambiguously identify acts of sabotage has been particularly challenging for these systems. In general, it's hard for them to determine whether the most prevalent forms of malicious and intentional system damage that they incur - copper theft and gun shot insulators/equipment - should qualify as acts of sabotage. Although none of the systems consider copper theft to be acts of sabotage, two of the systems consider gun shot insulators/equipment to be acts of sabotage. The other systems look for intent to disrupt electric system operations as a key component of their sabotage identification procedures. Additional guidance from NERC in the form of CIP-001-1 modifications or a companion guidelines document on sabotage identification would provide much needed guidance for these procedures. B. EOP-004-1 - This standard was clearly drafted with the larger electric systems in mind. I have one client that serves 3300 commercial/residential customers from 4-115/13 kV substation transformers and one large industrial customer (80% of its energy load) from a 230/13 kV substation. 75% of the client's load is served from three substations attached to a long, 115 kV transmission line operated by the Bonneville Power Administration. Whenever the line relays open on a permanent fault (which happens 2-3 times per year), the client loses over 50% of its customers (but no more than 10-15 MW during winter peak), thereby necessitating the preparation of a Disturbance Report. To allow utilities to concentrate on operating their systems, without fear of violating EOP-004-1 for failure to report trivial outages, I would remove LSEs from the obligation to report disturbances - leave the reporting to the BA/TOP for large outages in their footprint.
Response: The DSR SAR DT thanks you for your comment. **A. The team notes that your comments relate directly to potential revisions of the standard requirements. The team will pass your comments along to the Standards Drafting Team for its consideration.** **B. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the standard as the Standard Drafting team may have a need to include them in the standard(s). The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements through the Standard Development Process. The team**		

Organization	Yes or No	Question 1 Comment
will pass your comments along to the Standards Drafting Team for its consideration.		
Calpine Corporation	Yes	Communication of facility status or emergencies between merchant generators registered as GOP and the RC, BA, GOP, or LSE in which the facility resides should be coordinated for EOP -004 reporting. The reporting to NERC/DOE should come from the RC, BA, GOP, or LSE.
Response: The DSR SAR DT thanks you for your comment. The team concurs that reporting should be coordinated and will pass your comments along to the Standards Drafting Team for its consideration.		
Covanta	Yes	Yes - the key to Sabotage reporting requirements is identifying what the 'definition' is of an actual or potential 'Sabotage' event. Like any other standard, if FERC/NERC leave it up to 2000+ entities to establish their own definitions of 'Sabotage', you may likely get 2000+ answers. That is not a controlled and coordinated approach. I offer the following definition, "Sabotage - Deliberate or malicious destruction of property, obstruction of normal operations, or injury to personnel by outside agents." Examples of sabotage events could include, but are not limited to, suspicious packages left near site electrical generating or electrical transmission assets, identified destruction of generating assets, telephone/e mail received threats to destroy or interrupt electrical generating efforts, etc." These have passed multiple NERC regional audits and reviews to date.
Response: The DSR SAR DT thanks you for your comment. One of the FERC Order 693 directives for CIP-001 is: **Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event.** **The team will pass your comments along to the Standards Drafting Team for its consideration.**		
Cowlitz County PUD	Yes	The standards as written now create reporting on local customer quality of service outage events not related to BPS disturbances. Sabotage reporting has degenerated into reporting of mischievous vandalism and minor theft occurences. This creates compliance documentation overburden and waste of limited funds needed for true BPS reliability concerns, and also adds nuisance calls to the FBI and Homeland Security.
Response: The DSR SAR DT thanks you for your comment. One of the FERC Order 693 directives for CIP-001 is: **Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event.** **This should address the concern of sabotage vs. vandalism/theft reporting.**		
Reliant Energy	Yes	EOP-004-1 indicates that Generators should analyze disturbances on the bulk electrical system or their facilities. Generators do not have the capability of analyzing the bulk electrical system other than Frequency. Even so, generators can not unilaterally respond to what it thinks are disturbances. In the case of CAISO The Participating Generator

Organization	Yes or No	Question 1 Comment
		Agreement prevents me from making any unilateral moves save for the direst frequency emergencies. If the System operator or Reliability Coordinator informs the generator that there is a disturbance and that logs and readouts etc. are required then the generator should respond with all available information for the subject hours or time. Clearer responsibilities provide clearer results.
Response: The DSR SAR DT thanks you for your comment. While the team agrees that generators may not have the capability to analyze events, the team note that you concern is regarding applicability of requirements. The final wording of the requirements developed by the Standard Drafting Team will determine the applicability.		
Georgia System Operations Corp.	Yes	There is a need to eliminate burdensome reporting deadlines which interfere with the reliable operations or recovery of the BES. There is also a need to move requirements for reporting to NERC or Regional Entities (except for reporting of threats to physical or cyber security) from the Requirements section of Reliability Standards to elsewhere.
Response: The DSR SAR DT thanks you for your comment. Specific revisions to the requirements will be vetted during the standard development process.		
Illinois Municipal Electric Agency	Yes	Simplification of reporting requirements should facilitate reliability.
Response: The DSR SAR DT thanks you for your comment.		
Duke Energy	Yes	We agree that additional clarity is needed regarding sabotage and disturbance reporting. Requirements should be tightened up and triggering events/thresholds of materiality need to be better defined.
Response: The DSR SAR DT thanks you for your comment. One of the FERC Order 693 directives for this project is: Define “sabotage” and provide guidance on triggering events that would cause an entity to report an event.		
MRO NERC Standards Review Subcommittee	Yes	
Colmac Clarion	Yes	
United Illuminating	Yes	

Organization	Yes or No	Question 1 Comment
PSEG Enterprise Group Inc Companies	Yes	
Northeast Power Coordinating Council	Yes	
IRC Standards Review Committee	Yes	
FirstEnergy	Yes	
Texas Regional Entity	Yes	
Edward C. Stein	Yes	
Exelon	Yes	
WECC	Yes	
ERCOT ISO	Yes	
Luminant Power	Yes	
ReliabilityFirst Corporation	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	

Organization	Yes or No	Question 1 Comment
PacifiCorp	Yes	
Oncor Electric Delivery	Yes	
Consolidated Edison Co. of New York, Inc.	Yes	
Manitoba Hydro	Yes	
AEP	Yes	
We Energies	Yes	
Consumers Energy Company	Yes	
NextEra Energy Resources, LLC	Yes	
Ameren	Yes	

2. Do you agree with the scope of the proposed SAR? If not, please explain what should be added or deleted to the proposed scope.

Summary Consideration: The majority of stakeholders agree with the scope of the SAR. Several stakeholders offered suggestions for items to include in the SAR, however the SAR DT believes that these comments may be too prescriptive to include with the SAR. The team feels that inclusion of these types of comments would prevent the Standard Drafting Team from having the ability to develop standard(s) based on stakeholder consensus. The SAR DT will forward these comments to the Standard Drafting Team for its consideration. Some of the comments received include:

1 The inclusion of specific definitions in the SAR (operating personnel, sabotage events, obligations): The SAR DT believes that this would be too prescriptive and believe that this should be addressed by the Standard Drafting Team.

2 Consolidate documents covering reporting requirements: The SAR DT agrees and suggests that the Standard Drafting Team investigate a "one-stop-shopping" solution for the various reports required, including the DOE report.

Organization	Yes or No	Question 2 Comment
Project 2007-02 Operating Personnel Comms Protocols SDT	No	The Operating Personnel Communication Protocols standard drafting team respectfully requests that the Sabotage Reporting SAR Drafting Team incorporate the following into your proposed SAR: "Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have procedures for the communication of information concerning the Cyber and Physical emergency alerts in accordance with the conditions described in "Attachment 1 Security Emergency Alerts." The Operating Personnel Communications Protocols Project 2007-02 was initiated to ensure that real time system operators use standardized communication protocols during normal and emergency operations to improve situational awareness and shorten response time. The SDT developed a new COM-003-1 Standard that has yet to be posted and is dependent upon revising at least two other standards (CIP-001 and TOP Standard). COM-003 contains requirements that specify: 1. Use of three-part communication; 2. English language; 3. Common time zone; 4. NATO alpha-numeric alphabet; 5. Mutually agreed line identifiers; 6. The use of pre-defined system condition terminology such as those contained in the RCWG Alert Level Guide and EOP-002-2.

Organization	Yes or No	Question 2 Comment
		This request is based on recent NERC Standards Committee direction to our team to incorporate the Reliability Coordinator Working Group's (RCWG) Alert Level Guide into a Standard. The consensus of our team is that a TOP Standard is the most appropriate location for the Transmission Emergency Alert language from the Guide as the energy emergency alert language is currently described in EOP-002-2. The RCWG Guide proposes the se of pre-defined system condition descriptions for use during emergencies for reliability related formation. This guide was developed in response to a Blackout Report recommendation. Our team placed the Transmission Emergency Alert language into a TOP standard. Since the Sabotage Reporting SAR DT intends to modify CIP-001, we seek your consent to incorporate the cyber and physical security alert language to comply with the wishes of the Standards Committee. We believe that the CIP-001 Standard is the most appropriate location for this language for the following reasons: • The levels of emergency conditions related to the cyber and physical security of the electric system is directly related to Critical Infrastructure Protection. • The current version of CIP-001 already requires the timely reporting of actual and suspected security emergency conditions and the use of pre-defined terminology supports the efficient haring of such information. The OPCP SDT includes the following text for the record. It is a proposed draft revision of CIP-001. **A. Introduction** 1. Title: Security Incidents 2. Number: CIP-001-2 3. Purpose: To ensure the recognition, communication and response to cyber and physical security incidents suspected or determined to be caused by sabotage. 4. Applicability 4.1. Reliability Coordinators. 4.2. Balancing Authorities. 4.3. Transmission Operators. 4.4. Generator Operators. 4.5. Load Serving Entities. 5. Effective Date: The standard is effective the first day of the first calendar quarter after applicable regulatory approvals (or the standard otherwise becomes effective the first day of the first calendar quarter after NERC OT adoption in those jurisdictions where regulatory approval is not required).

Organization	Yes or No	Question 2 Comment
		B. Requirements R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of security threats on its facilities and multi site security threats affecting larger portions of the Interconnection. R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning the physical and cyber security status of their facilities in accordance with the conditions described in Attachment 1-CIP-001-1. R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with security threat or incident response guidelines, including personnel to contact, for reporting security threats and incidents. R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances. **C. Measures** M1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement 1 M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements 2 and 3. M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited o procedures, policies, a letter of understanding, communication records, or other equivalent evidence that will be used to confirm that it has established communications contacts with the applicable, local FBI or CMP officials to communicate sabotage events (Requirement 4). **D. Compliance** 1. Compliance Monitoring Process 1.1. Compliance Enforcement Authority Regional Entity 1.2. Compliance Monitoring Period and Reset One or more of the following methods will be used to verify compliance: - Compliance Audits

Organization	Yes or No	Question 2 Comment
		- Self-Certifications - Spot Checking - Compliance Violation Investigations - Self-Reporting - Complaints 1.3. Data Retention The Transmission Operator, Transmission Owner, Balancing Authority, Reliability Coordinator, Generator Operator and Distribution Provider shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation: o The Transmission Operator, Transmission Owner, Balancing Authority, Reliability Coordinator, Generator Operator and Distribution Provider shall retain its current, in force document and any documents in force since the last compliance audit. o If a Transmission Operator, Transmission Owner, Balancing Authority, Reliability Coordinator, Generator Operator or Distribution Provider is found non-compliant, it shall keep information related to the non-compliance until found compliant. o The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records. 1.4. Additional Compliance Information None. 2. Levels of Non-Compliance: 2.1. Level 1: There shall be a separate Level 1 non-compliance, for every one of the following requirements that is in violation: 2.1.1 Does not have procedures for the recognition of and for making its operating personnel aware of sabotage events (R1). 2.1.2 Does not have procedures or guidelines for the communication of information concerning sabotage events to appropriate parties in the Interconnection (R2). 2.1.3 Has not established communications contacts, as specified in R4. 2.2. Level 2: Not applicable.

Organization	Yes or No	Question 2 Comment
		2.3. Level 3: Has not provided its operating personnel with sabotage response procedures or guidelines (R3). 2.4. Level 4:.Not applicable. E. Regional Differences None. Version History Version Date Action Change Tracking 0 April 1, 2005 Effective Date New 0 August 8, 2005 Removed "Proposed" from Effective ate Errata 1 November 1, 2006 Adopted by Board of Trustees Amended 1 April 4, 2007 Regulatory approval — Effective Date New 2 March 2009 Added SEA attachment and updates to Effective Date and compliance sections. New **Attachment 1-CIP-001-2 Physical Security Emergency Alerts** General requirements 1. Initiation by Reliability Coordinator. A Physical Security Emergency Alert may be initiated only by a Reliability Coordinator at: a. The Reliability Coordinator's own decision, b. By request from a Transmission Operator, c. By request from a Balancing Authority, or d. By request from federal, state, or cal Law Enforcement Officials. 2. Situations for initiating alert. An Alert may be initiated for the following reasons: a. A physical threat affecting a control center, grid or generator asset has been identified, or b. A physical attack affecting a control center, grid or generator asset has occurred or is imminent. 3. Notification. A Reliability Coordinator who initiates a Physical Security Emergency Alert shall notify all Transmission Operators and Balancing Authorities in its Reliability Area. The Reliability Coordinator shall also notify other Reliability Coordinators of the situation via the Reliability Coordinator Information System (RCIS) using the "CIP" category. Additionally, conference calls between Reliability Coordinators shall be held as necessary to communicate system conditions. The Reliability Coordinator shall also notify all Transmission Operators and Balancing Authorities in its Reliability Area and other Reliability Coordinators hen the alert has changed levels or ended.

Organization	Yes or No	Question 2 Comment
		Physical Security Emergency Alert Levels To ensure that all Reliability Coordinators clearly understand potential and actual Physical Security Emergency Alerts, NERC as established three levels of Security Emergency Alerts. The Reliability Coordinators will use these terms hen explaining security alerts to each other. The Reliability Coordinator may declare whatever alert level is necessary, and need not proceed through the alerts sequentially. 1. Alert 1 – "Control Center / Bulk Electric system asset threat identified" Circumstances: A credible threat of physical attack on a Bulk Electric System asset has been communicated to the Reliability Coordinator. No physical attack has occurred at this point. Determining the credibility of any threat is a subjective process, but the following factors should be considered: a. The nature and specificity of the threat, b. The timing of the threat, c. Mode of threat communication, and d. The criticality of the threatened asset. During a Physical Security Emergency Alert Level 1, Reliability Coordinators, Transmission Operators and Balancing Authorities shall have the following responsibilities: i. Notification: The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area. ii. Updating Status during the Physical Security Emergency Alert The declaring Entity shall update the reliability Coordinator of any changes in the situation until the Alert Level 1 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 2. Alert 2 – "Verified Physical attack at a single site" circumstances: A Reliability Coordinator, Transmission Operator, or Balancing Authority has identified a physical attack upon a control center, generator asset, or other bulk electric system asset. During a Physical Security Emergency Alert Level 2, Reliability Coordinators, Transmission Operators and Balancing Authorities shall have the following responsibilities: i. Notification: The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area. ii. Updating Status during the Physical Security Emergency Alert The Declaring Entity shall update the Reliability Coordinator of the situation a minimum of once per hour until the Alert Level 2 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 3. Alert 3– "Verified Physical attack at multiple sites" Circumstances: Multiple attacks have been confirmed on control centers, generator assets or other bulk electric system assets. A Reliability Coordinator shall declare Physical Security

Organization	Yes or No	Question 2 Comment
		Emergency Alert 3 whenever: a. A Transmission Operator or Balancing Authority reports multiple physical attacks on bulk electric system assets, b. Multiple Transmission Operators or Balancing authorities report one or more physical attacks on their bulk electric system assets. i. Notification: The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area. ii. Updating Status during the Physical Security Emergency Alert The declaring Entity(ies) shall update the Reliability Coordinator of the situation a minimum of once per hour until the Alert Level 3 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 4. Alert 0 – "Termination of Alert Level" Circumstances: The threat which prompted the Physical Security Emergency Alert Level has diminished or has been removed. i. Notification The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall notify all other Reliability Coordinators via the RCIS, and it shall also notify all Transmission Operators and Balancing Authorities in its Reliability Area that the Alert Level has been terminated. Cyber Security Emergency Alerts Cyber Assets – Those programmable electronic devices and communication networks, including hardware, software, and data, associated with bulk electric system assets. Cyber Security Incident - Any malicious act or suspicious event that compromises, or attempts to compromise, the electronic or physical security perimeter of a critical cyber asset or disrupts or attempts to disrupt the operation of a critical cyber asset. Critical Cyber Asset – Those cyber assets essential to the reliable operation of critical assets. Electronic Security Perimeter – The logical border surrounding the network or group of sub-networks to which the critical cyber assets are connected, and for which access is controlled. Physical Security Perimeter – The physical border surrounding computer rooms, telecommunications rooms, operations centers and other locations in which critical cyber assets are housed and for which access is controlled. General Requirements 1. Initiation - A Cyber Security Emergency Alert shall be initiated by: a. The Reliability Coordinator's analysis, b. By request from any NERC functional Model entity that Com-003-0 is applicable to.

Organization	Yes or No	Question 2 Comment
		c. By request from federal, state, or local Law Enforcement Officials. 2. Situations for initiating alert. An Alert shall be initiated for the following reasons: a. A cyber threat affecting a control center or bulk electric system asset has been identified, or b. A cyber attack affecting a control center or bulk electric system has occurred or is imminent. 3. Notification. An entity who initiates a Cyber Security Emergency Alert shall make notification as per the NERC Functional model or as Regional / local instruction. The Reliability Coordinator shall notify FBI local office, Electricity Sector Information Sharing Analysis Center ESISAC) and Department of Homeland Security. The Reliability Coordinator shall also notify as necessary other Reliability Coordinators of the situation via the Reliability Coordinator Information System (RCIS) sing the "CIP" category. The Reliability Coordinator shall notify all Transmission Operators and Balancing Authorities in its Reliability Area and other Reliability Coordinators when the alert has changed levels or ended. Cyber Security Emergency Alert Levels To ensure that all applicable entities clearly understand potential and actual Cyber Security Emergency Alerts, three levels of Security Emergency Alerts shall be sed. The Reliability Coordinators will use these terms when communicating security alerts to each other. When declaring the applicable alert level it is important to note that the applicable level can be determined without sequentially proceeding through levels. As an example given circumstances an Alert Level 3 could be called without previously being in an Alert Level 1 or Level 2 state. 1. Alert 1 – "Verified Control Center / Bulk Electric System Cyber Asset threat identified or imminent" What is "verified" - unknown or unauthorized access to a cyber device, unknown or unauthorized change to a cyber device (i,e., config file, /S, firmware change. 'Verified' could mean the elimination of a false positive in your security monitoring system. 'Verified' could also be the differentiation between malicious and non-malicious (ie human error, not following policy, etc) intent. What is a "threat" - A threat can be perceived as any action or event that occurs where the monitoring authority was not previously made aware that that action would occur. With flimsy change control or access controls, field staff or technical staff performing troubleshooting or other maintenance may access or change devices without notifying the monitoring entity. The monitoring entity would have to treat this as a threat and take appropriate action to either isolate that device from the rest of the system, notify appropriate authority, dispatch a crew, etc. Examples of threats - Over and above the examples above, another threat example could be a notification from DHS or other security agency that they have reason to believe a hack, virus or other cyber terrorism activity could occur. Also, noticing a distinct change in network traffic which could imply someone has intercepted your data and can manipulate

Organization	Yes or No	Question 2 Comment
		before sending it from the control room to the device being controlled or manipulating the data coming from the device before a controller seeing it and forcing them to perform an incorrect control event in reaction to erroneous data. Circumstances: A credible threat of Cyber attack on a Control Center or Bulk Electric System asset has been communicated to the Reliability Coordinator. No cyber attack has occurred t this point. Determining the credibility of any threat is a subjective process, but the following factors should be considered: a. The nature and specificity of the threat, b. The timing of the threat, c. Mode of threat communication, and d. The criticality of the threatened asset. During a Cyber Security Emergency Alert Level 1, applicable entities shall have the following responsibilities: i. Notification An entity who initiates a Cyber Security Emergency Alert Level 1 shall make notification as per the NERC Functional model r as Regional / local instruction. The Reliability Coordinator shall post the declaration of the alert level long with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area. The Reliability Coordinator shall also notify as necessary the BI local office, Electricity Sector Information Sharing Analysis Center (ESISAC) and Department of Homeland Security. ii. Updating Status during the Cyber Security Emergency Alert The declaring Entity shall update those applicable entities of any changes in the situation until the Alert Level 1 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 2. Alert 2 – "Verified Cyber attack on a Control Center or Bulk Electric System asset" Circumstances: An applicable entity has identified a cyber attack upon a control center or bulk electric system asset. During a Cyber Security Emergency Alert Level 2, applicable entities shall have the following responsibilities: i. Notification An entity who initiates a Cyber Security Emergency Alert Level 2 shall make notification as per the NERC Functional model or as Regional / cal instruction. The Reliability Coordinator responsible shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area. The Reliability Coordinator shall also notify the FBI local office, Electricity Sector Information Sharing Analysis Center (ESISAC) and Department of Homeland Security. ii. Updating Status during the Cyber Security Emergency Alert The declaring Entity shall provide updates of the situation a minimum of once per hour until the Alert Level 2 is terminated. The Reliability Coordinator shall update the RCIS as changes occur.

Organization	Yes or No	Question 2 Comment
		3. Alert 3 – "Verified Cyber attack at one or more Control Center or Bulk Electric System cyber asset" Circumstances: An applicable entity has identified a cyber attack upon a control center or bulk electric system asset and shall declare a Cyber Security Emergency Alert 3 whenever: a. A Transmission Operator or Balancing Authority reports one or more cyber attacks on bulk electric system that render an asset(s) unavailable. i. Notification An entity who initiates a Cyber Security Emergency Alert Level 3 shall make notification as per the NERC Functional model or as Regional / local instruction. The Reliability Coordinator shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities its Reliability Area. The Reliability Coordinator shall also notify the FBI local office, Electricity Sector Information Sharing Analysis Center (ESISAC) and Department of Homeland Security. ii. Updating Status during the Cyber Security Emergency Alert The declaring Entity(ies) shall provide an update of the situation minimum of once per hour until the Alert Level 3 is terminated. The Reliability Coordinator shall update he RCIS as changes occur. 4. Alert 0 – "Termination of Alert Level" Circumstances: The threat which prompted the Cyber Security Emergency Alert Level has diminished or has been removed. i. Notification An entity who initiates a Cyber Security Emergency Alert shall make notification as per the NERC Functional model or as Regional / local instruction when situation has diminished or returned to normal. The Reliability Coordinator shall notify all other Reliability Coordinators via the RCIS, and it shall also notify all Transmission Operators and Balancing Authorities in its Reliability Area that the Alert Level has been terminated.
Response: The DSR SAR DT thanks you for your comment. The standards in this Project 2009-01 SAR are designed to specify reporting requirements for disturbance and sabotage events. The DSR SAR DT believes that the suggested additions go beyond the intended scope of the revisions to the standards, and do not feel that communications protocols belong in these reporting standards. The proposed revisions and Alert Levels are real-time requirements, and the team feels that these would be more appropriately addressed in an IRO or COM standard.		
Northeast Power Coordinating Council	No	The SAR needs to be more specific in defining its objectives. CIP-001Requirement R1 currently states: R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SDT needs to include the following objectives: 1. Develop clear definitions for the terms "operating personnel" and "sabotage events." The definition of "operating personnel," should be clarified and limited to staff at BES facilities. Operating personnel should report only those events

Organization	Yes or No	Question 2 Comment
		which meet a clear, recognizable threshold as reportable potential sabotage events. There should be a consistent continent-wide list of examples or typical reportable and non-reportable events to help guide operating personnel. The term "sabotage event" needs to be defined. Clarification is required regarding when the determination of a sabotage event is made, e.g., upon first observation (requiring operating personnel be educated in discerning sabotage events), or upon later investigation by trained security personnel and law enforcement individuals. The terms potential or suspected sabotage event for reporting purposes should be clarified or defined. 2. Define the obligations of Registered Entity operating personnel - who are required to be aware of such "sabotage events," e.g., who, what, where, when, why and how, and what they are to do in response to this awareness. The SDT should clarify the use of the term "aware" in the standard. "Aware" can be interpreted in accordance with its largely passive, dictionary-based meaning, where being "aware" simply means knowing about something, such as a sabotage event. Alternatively, the Reliability Standard meaning of "aware" could refer to more active wording, involving more than mere awareness, e.g., "alert and quick to respond," pointing to and requiring a specific affirmative response, i.e., reporting to the appropriate systems, governmental agencies, and regulatory bodies. EOP-004 - The SDT needs to work on the following areas. 1. NERC reporting needs to be clarified. For example, Attachment 1 paragraph 6c states: Introduction "The entity on whose system a reportable disturbance occurs shall notify NERC ... 6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in: c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance - The sense of Attachment 1 is internally inconsistent between the introduction ("occurs") and the required actions in 6c (could have resulted in a system disturbance). The initial intent appears to be only to report actual system disturbances. Yet, paragraph 6c adds the phrase "or could have resulted in" a potential system disturbance. This inconsistency should be clarified.
Response: The DSR SAR DT thanks you for your comment. **CIP-001: The inclusion of specific definitions in the SAR as you suggest (operating personnel, sabotage events, obligations) are too prescriptive and could prevent better definitions from being developed during the Standards Development stage of the project. The team will pass your comments along to the standard drafting team for its consideration.** **EOP-004: Your comment addresses specific revisions to the standard. The team will pass your comments along to the standard drafting team for its consideration.**		
Kansas City Power & Light	No	Agree with the scope of the SAR except for the applicable entities. See response to question #4.
Response: The DSR SAR DT thanks you for your comment. Please see response to Q4.		

Organization	Yes or No	Question 2 Comment
MRO NERC Standards Review Subcommittee	No	The MRO NSRS would like to keep the references to the DOE reporting form.
Response: The DSR SAR DT thanks you for your comment. The DSR SAR DT understands your comment to indicate that you would like to see a "one stop" reporting form for disturbances and sabotage events. The DSR SAR DT agrees with you and will pass this comment along to the standard drafting team for its consideration in developing the standard(s).		
Lands Energy Consulting	No	I would like to see the SAR expanded to cover the issues I mentioned in my prior comment. Otherwise, the scope of the SAR looks fine to me.
Response: The DSR SAR DT thanks you for your comment. Please see response to Q1 on other issues.		
Bonneville Power Administration	No	Leave as is, all requirements for reporting are now covered. A common definition of sabotage is already widely available.
Response: The DSR SAR DT thanks you for your comment. Most stakeholders desire more clarity around the definition of sabotage as well as examples of what is and is not sabotage as opposed to vandalism.		
Cowlitz County PUD	No	Added to the scope: For EOP-004 add a provision for a reporting flow rather than everything going to the RE and NERC. That is something going like the DP and TOP reports to the BA, the BA to the RE, and the RE to NERC. This would allow for multiple related reports to be combined into a single coherent report as the reporting goes up the chain. For CIP-001 consider reporting flow as above with local law enforcement notification. Let an upper entity in the reporting chain decide when to contact Federal Agencies such as the BA or the RC.
Response: The DSR SAR DT thanks you for your comment. The DSR SAR DT feels that your comments are "how" comments that should be addressed in standard drafting stage. The team will pass this comment along to the standard drafting team for its consideration.		
Reliant Energy	No	I think Generator operators should be excluded except to provide requested information from the System Operator or Reliability coordinator.
Response: The DSR SAR DT thanks you for your comment. Other commenters have questioned the ability of Generator Operators to have a wide area view and to be able to analyze disturbances on the system. The team agrees that generators may not have a wide area view and the capability to analyze system events. The final wording of the requirements (i.e. reporting vs. data provision) developed by the Standard Drafting Team will		

Organization	Yes or No	Question 2 Comment
determine the applicability to GOPs. The team will pass your comment on to the Standard Drafting Team for its consideration.		
ERCOT ISO	No	The scope should be modified to provide for a different treatment of reporting requirements that are administrative in nature, or that are after-the-fact (thus cannot impact reliability unless analysis and follow-up is not performed; even then, the impact would be at some future time). Reporting requirements which are of the nature to assist in identification of system concerns or which serve to prevent or mitigate on-going system problems (including, but not limited to, actual or attempted sabotage activity) should remain in standards, but should be separate and apart from the administrative reporting.
Response: The DSR SAR DT thanks you for your comment. The team concurs with the concepts on reporting as you suggest, however the team does not feel that this should be addressed in the SAR. The team suggests that this is more appropriately addressed in the standard drafting process, and the team will pass your comment along to the standard drafting team for its consideration in drafting the standard.		
MidAmerican Energy	No	See the responses to questions 1 and 5.
Response: The DSR SAR DT thanks you for your comment. Please see responses to Q1 and Q5.		
We Energies	No	Consider including the sabotage issues in IRO-014-1 R 1.1.1 footnote 1 and TOP-005-1 Attachment 1, 2.9.
Response: The DSR SAR DT thanks you for your comment. The team has added references to these two standards in the "Related Standards" section for the SAR.		
NextEra Energy Resources, LLC	No	The scope of the SAR should not include Generator Operators.
Response: The DSR SAR DT thanks you for your comment. Other commenters have questioned the ability of Generator Operators to have a wide area view and to be able to analyze disturbances on the system. The team agrees that generators may not have a wide area view and the capability to analyze system events. The final wording of the requirements (i.e. reporting vs. data provision) developed by the Standard Drafting Team will determine the applicability to GOPs. The team will pass your comment on to the Standards Drafting Team for its consideration.		
Progress Energy	No	No. If this SAR moves forward other standards may need to be considered. For example, in CIP-008, incident reporting for cyber incidents leads to filing of the OE-417 form.
Response: The DSR SAR DT thanks you for your comment. The SAR states "Specific references to the DOE form need to be eliminated." **This will remove the linkage that you identify between CIP-001 and CIP-008. There is also a directive from FERC Order 693 in the SAR that states:**		

Organization	Yes or No	Question 2 Comment
Consider FirstEnergy's suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality. **This allows the standard drafting team to delineate physical and cyber assets. The DSR SAR DT also notes that CIP-008 might be a good framework for drafting the standard requirements pertaining to sabotage and disturbance reporting of physical assets.**		
Ameren	No	There seems to be an open slate including the following language in the scope. The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards (see tables for each standard at the end of this SAR for more detailed information). The unnamed improvements should be limited to those requirements that relate only to Disturbance and Sabotage NOT a general wish list (or witch hunt).
Response: The DSR SAR DT thanks you for your comment. The passage that you mention is the intent of each SAR and is a stock statement that is included in almost every SAR. The SAR is limited to the standards listed in the SAR which is approved by the NERC SC to move to standards development.		
Consolidated Edison Co. of New York, Inc.	No	GENERAL CECONY and ORU support the general objectives of the SAR to merge existing standards CIP-001-1 Sabotage Reporting and EOP-004-1 Disturbance Reporting to improve clarity and remove redundancy. However, the SAR needs to be more specific in defining its objectives. CIP-001Requirement R1 currently states: R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SDT needs to include the following objectives: 1. Develop clear definitions for the terms operating personnel and sabotage events. The definition of operating personnel, should be clarified and limited to staff at BES facilities. Operating personnel should report only those events which meet a clear, recognizable threshold as reportable potential sabotage events. There should be a consistent continent-wide list of examples or typical reportable and non-reportable events to help guide operating personnel. The term sabotage event needs to be defined. Clarification is required regarding when the determination of a sabotage event is made, e.g., upon first observation (requiring operating personnel be educated in discerning sabotage events), or upon later investigation by trained security personnel and law enforcement individuals. The terms potential or suspected sabotage event for reporting purposes should be clarified or defined. 2. Define the obligations of Registered Entity operating personnel - who are required to be aware of such sabotage events, e.g., who, what, where, when, why and how, and what they are to do in response to this awareness. The SDT should clarify the use of the term aware in the standard. Aware can be interpreted in accordance with its largely passive, dictionary-

Organization	Yes or No	Question 2 Comment
		based meaning, where being aware simply means knowing about something, such as a sabotage event. Alternatively, the Reliability Standard meaning of aware could refer to more active wording, involving more than mere awareness, e.g., alert and quick to respond, pointing to and requiring a specific affirmative response, i.e., reporting to the appropriate systems, governmental agencies, and regulatory bodies. EOP-004 - The SDT needs to work on the following areas. 1. NERC reporting needs to be clarified. For example, Attachment 1 paragraph 6c states: Introduction The entity on whose system a reportable disturbance occurs shall notify NERC ... 6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in: ?c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance. The sense of Attachment 1 is internally inconsistent between the introduction (occurs) and the required actions in 6c (could have resulted in a system disturbance). The initial intent appears to be only to report actual system disturbances. Yet, paragraph 6c adds the phrase or could have resulted in a potential system disturbance. This inconsistency should be clarified.
Response: The DSR SAR DT thanks you for your comment. **CIP-001: The inclusion of specific definitions in the SAR as you suggest (operating personnel, sabotage events, obligations) are too prescriptive and could prevent better definitions from being developed during the standard drafting stage of the project. The team will pass your comments along to the standard drafting team for its consideration.** **EOP-004: Your comment addresses specific revisions to the standard. The team will pass your comments along to the standard drafting team for its consideration.**		
Georgia System Operations Corp.	No	The scope of the SAR should be to move all requirements to report to NERC or Regional Entities out of the Requirements section of all Reliability Standards to elsewhere. This does not include reporting, communicating, or coordinating between reliability entities. The NERC/Region reporting requirements could be consolidated in another document and referenced in the Supporting References section of the Reliability Standards. The deadlines for reporting should be changed to realistic timeframes that do not interfere with operating the BES or responding to incidents yet still allow NERC and the Regions to accomplish their missions.
Response: The DSR SAR DT thanks you for your comment. The team does not feel that this should be addressed explicitly in the SAR, but suggests that this is more appropriately addressed in the standard drafting stage for full industry vetting of the concepts. The team will pass your comment along to the standard drafting team for its consideration in developing the standard.		

Organization	Yes or No	Question 2 Comment
AEP	No	Sabotage is a term of intent that is often determined after the fact by the registered entity and/or law enforcement officials. In fact, it is often difficult to determine in real-time the intent of a suspicious event. We would suggest that suspicious events become reportable at the point that the event is determined to have had sabotage intent. The entities should have a methodology to collect evidence, to have the evidence analyzed, and to report those events that are determined to have had the intent of sabotage.
Response: The DSR SAR DT thanks you for your comment. The team concurs that it is difficult to determine sabotage in real-time. The teamdoes not feel that this should be addressed explicitly in the SAR and suggests that this is more appropriately addressed in the standard drafting stage for full industry vetting of the concepts. The team will pass your comment along to the standard drafting team for its consideration in developing the standard.		
Duke Energy	No	While we agree with the need for clarity in sabotage and disturbance reporting, we believe that the Standards Drafting Team should carefully consider whether there is a reliability-related need for each requirement. Some disturbance reporting requirements are triggered not just to assist in real-time reliability but also to identify lessons-learned opportunities. If disturbance and sabotage reporting continue to be reliability standards, we believe that all linkages to lessons-learned/improvements need to be stripped out. We have other forums to identify lessons-learned opportunities and to follow-up on those opportunities. Also, requirements to report possible non-compliances should be eliminated. We strongly support voluntary self-reporting, but not mandatory self-reporting.
Response: The DSR SAR DT thanks you for your comment. The team concurs that each requirement should be evaluated for its reliability need, and the team will pass your comment along to the standard drafting team for its consideration in the drafting stage of the standard.		
FirstEnergy	Yes	We agree with the scope but would also like to see the following considered: 1. References to the DOE reporting process in EOP-004 need to be revised. They currently refer to the old EIA form. 2. Besides "sabotage", it may be helpful to clearly define "vandalism". It is vaguely written in the standards. Also, the process of "public appeals" for the DOE reportable requirements needs to be more clearly defined. 3. Consolidate documents covering reporting requirements. There are currently several documents that require reporting (EOP-004, CIP-001, DOE oe-417, and NERC's Security Guideline for the Electricity Sector: Threat and Incident Reporting). NERC also has the "Bulk Power System Disturbance Classification Scale" that does not completely align with all the reporting requirements. Therefore we recommend keeping this as simple as possible by combining all the reporting requirements into one standard. It would be beneficial to not require operators to have to go to 4 different documents to determine what to report on.
Response: The DSR SAR DT thanks you for your comment.		

Organization	Yes or No	Question 2 Comment
The Brief Description of the SAR states: Specific references to the DOE form need to be eliminated. **The team will pass your comment along to the standard drafting team for its consideration.** **The team concurs that this should be considered in drafting the standards. The team will pass your comment along to the standard drafting team for its consideration.**		
Exelon	Yes	Consolidation of redundant requirements and clarifications of difficult to follow / interpret standards should be a high priority at NERC.
Response: The DSR SAR DT thanks you for your comment. One of the FERC directives for CIP-001 is: Explore ways to reduce redundant reporting, including central coordination of sabotage reports and a uniform reporting format.		
Electric Market Policy	Yes	
SERC OC Standards Review Group	Yes	
PSEG Enterprise Group Inc Companies	Yes	
IRC Standards Review Committee	Yes	
Pepco Holdings, Inc. - Affiliates	Yes	
Calpine Corporation	Yes	
Covanta	Yes	
Colmac Clarion	Yes	

Organization	Yes or No	Question 2 Comment
United Illuminating	Yes	
Texas Regional Entity	Yes	
Edward C. Stein	Yes	
WECC	Yes	
Luminant Power	Yes	
ReliabilityFirst Corporation	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	
PacifiCorp	Yes	
Oncor Electric Delivery	Yes	
Illinois Municipal Electric Agency	Yes	
Manitoba Hydro	Yes	
Consumers Energy Company	Yes	

3. Are you aware of any associated business practices that we should consider with this SAR? If yes, please explain in the comment area.

Summary Consideration: Stakeholders did not identify any associated business practices for consideration under the SAR. One stakeholder identified a related standard that references multi-site sabotage. The team has included a reference to TOP-005, section 2.9 (Appendix 1) in the SAR under Related Standards. Two stakeholders suggested that Business Practices should not be considered in a standard. The SAR DT notes that standard development projects must not invalidate business practices that are already in place. This question is required to be asked per the Standard Drafting Team Guidelines (page 8) and aids in coordination with North American Energy Standards Board. One stakeholder suggested a "one-stop-shopping" solution. The SAR DT agrees with this approach and will forward this comment to the Standard Drafting Team.

Organization	Yes or No	Question 3 Comment
MRO NERC Standards Review Subcommittee	Yes	
Luminant Power	Yes	The SAR drafting team should include in the SAR scope a review of the NRC sabotage and event reporting requirements to ensure there are no overlapping or conflicting requirements between NERC, FERC, and the NRC. The SAR scope should include a review of the CIP Cyber Security Standards and coordination with the CIP SDT to ensure that cyber sabotage reporting definitions are in concert, and ensure that cyber sabotage reporting requirements are not duplicated in multiple standards.
Response: The DSR SAR DT thanks you for your comment. The team notes that your comments relate directly to potential revisions of the standard itself. Part of this SAR is to eliminate redundancies as well. The team will pass your comments along to the Standards Drafting Team for its consideration. This project is designed to address physical asset reporting, not cyber assets. Therefore, cyber assets will not be included in this SAR.		
MidAmerican Energy	Yes	Attachment TOP-005, section 2.9 speaks of "Multi-site sabotage" with no definition. The ES-ISAC 2008 advisory is an associated standard or practice on sabotage. All references to sabotage should be eliminated or retired except for CIP-001.
Response: The DSR SAR DT thanks you for your comment. The team has included a reference to TOP-005, section 2.9 (Appendix 1) in the SAR under Related Standards. Project 2009-01 is designed to address physical asset reporting, not cyber asset sabotage and disturbance reporting. The standard drafting team will remove redundancies per the SAR.		

Organization	Yes or No	Question 3 Comment
Illinois Municipal Electric Agency	Yes	A one-stop reporting tool/site would facilitate efficient reporting and compliance; e.g., further development of the ES-ISAC/CIPIS to include all reportable categories and automatic notification of required parties. A single report form would be best.
Response: The DSR SAR DT thanks you for your comment. The team agrees with your suggestion and will pass this along to the Standard Drafting Team for its consideration in developing standards.		
AEP	Yes	The current reporting process necessitates multiple reports be sent to multiple parties, which is inefficient and may, inadvertently, result in alignment issues between the separate reports. We would recommend that a single report that combines NERC (CIPIS) and NERC ESISAC information be provided to NERC (CIPIS) that is systematically (programmatically) forwarded to all necessary entities. Further, updates to incidents would also go through NERC with the same electronic processing. Currently, we are not aware of a formal method to report incidents to the FBI, which should be also included in the distribution. The current reporting mechanism to the FBI JTTF is by telephone and the NERC platform described would provide more consistent reporting.
Response: The DSR SAR DT thanks you for your comment. The team agrees with your suggestion and will pass this along to the Standard Drafting Team for its consideration in developing standards. This project is designed to address physical asset reporting, not cyber assets.		
Progress Energy	Yes	Yes. If this SAR moves forward other practices such as those required by CIP-008 (cyber incident reporting via the OE-417 form) may need to be considered.
Response: The DSR SAR DT thanks you for your comment. The SAR states "Specific references to the DOE form need to be eliminated."**This will remove the linkage that you identify between CIP-001 and CIP-008. There is also a directive from FERC Order 693 in the SAR that states:** **Consider FirstEnergy's suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality.** **This allows the standard drafting team to delineate physical and cyber assets. The DSR SAR DT also notes that the general layout and sequencing of requirements in CIP-008 might be a good framework for drafting the standard requirements pertaining to sabotage and disturbance reporting of physical assets.**		
Exelon	No	We are not sure what this question means. Who's Associated Business practices, NERC, Applicable Entities in the Standard, our business practices?
Response: The DSR SAR DT thanks you for your comment. "Business practices" refers to any business practice of any stakeholder (e.g. North American Energy Standards Board business practices).		

Organization	Yes or No	Question 3 Comment
SERC OC Standards Review Group	No	Business practices should not be considered in a standard.
Response: The DSR SAR DT thanks you for your comment. Standard development projects must not invalidate business practices that are already in place. This question is required to be asked per the Standard Drafting Team Guidelines (page 8) and aids in coordination with North American Energy Standards Board.		
FirstEnergy	No	Although we are not aware of any NAESB business practices that need to be reviewed in conjunction with these proposed revisions, the SDT should consider reviewing current RTO procedures and practices that may require the need for variances in the revised standards.
Response: The DSR SAR DT thanks you for your comment. The Standard Drafting Team will review any procedures or practices that are identified for potential variances.		
Georgia System Operations Corp.	No	Business practices should not be part of a Reliability Standard. Neither should NERC/Region reporting requirements (except for reporting of threats to physical or cyber security). NERC may need to take some action in the case of threats but does not and cannot take any operational action for most of the reporting requirements that are presently in the Requirements section of the Reliability Standards.
Response: The DSR SAR DT thanks you for your comment. Standard development projects must not invalidate business practices that are already in place. This question is required to be asked per the Standard Drafting Team Guidelines (page 8) and aids in coordination with North American Energy Standards Board. The team disagrees with your assertion about reporting. Instances of sabotage are often not identified until after the fact, and these should be reported to alert other entities of the sabotage and for "lessons learned".		
PSEG Enterprise Group Inc Companies	No	
Northeast Power Coordinating Council	No	
Kansas City Power & Light	No	
IRC Standards Review Committee	No	

Organization	Yes or No	Question 3 Comment
Pepco Holdings, Inc. - Affiliates	No	
Electric Market Policy	No	
Bonneville Power Administration	No	
Lands Energy Consulting	No	
Covanta	No	
Colmac Clarion	No	
Cowlitz County PUD	No	
United Illuminating	No	
Reliant Energy	No	
Texas Regional Entity	No	
Edward C. Stein	No	
PacifiCorp	No	
WECC	No	
ERCOT ISO	No	
ReliabilityFirst Corporation	No	

Organization	Yes or No	Question 3 Comment
Brazos Electric Power Cooperative, Inc.	No	
Oncor Electric Delivery	No	
Consolidated Edison Co. of New York, Inc.	No	
Manitoba Hydro	No	
Duke Energy	No	
We Energies	No	
Consumers Energy Company	No	
NextEra Energy Resources, LLC	No	
Ameren	No	

4. CIP-001-1 applies to the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, and the Load-serving Entity. EOP-004-1 applies to the same entities, plus the Regional Reliability Organization. Do you agree with the applicability of the existing CIP-001-1 and the existing EOP-004-1? If no, please identify what you believe should be modified.

Summary Consideration: Many stakeholders had comments regarding applicability of the two standards. The three main concerns were:

1 Regional Reliability Organization applicability: Many commenters do not feel the RRO should be in the standards. The DSR SAR DT concurs and notes that the SAR states that "EOP-004 has some 'fill-in-the-blank' components to eliminate". This will remove the RRO from applicability.

2 Load-Serving Entity/Distribution Provider: Many stakeholders do not feel that the standards should be applicable to LSEs, but should apply to Distribution Providers. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team added DP to the applicability of the standard as the Standard Drafting team may have a need to include them in the standard(s). The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements through the Standard Development Process.

3 Transmission Owner/Generator Owner: Many stakeholders have indicated a need to include the TO as an applicable entity. A couple of those would also include the GO. The SAR DT discussed the addition of both the TO and GO. The team has a concern that there will be duplication of requirements between the TO/TOP and GO/GOP if the TO and GO are added to the SAR. That being said, the team added the TO and GO to the applicability of the SAR so that the Standard Drafting team may consider these entities for applicability. The applicability of requirements will ultimately be determined by the Standard Drafting Team as it develops the requirements through the Standard Development Process.

Organization	Yes or No	Question 4 Comment
SERC OC Standards Review Group	No	The EOP-004-1 standard should not apply to the RRO.
Response: The DSR SAR DT thanks you for your comment. The team concurs and notes that the SAR states: EOP-004 has some 'fill-in-the-blank' components to eliminate. This will remove the RRO from applicability.		
Kansas City Power &	No	Do not agree Load Serving Entities need to continue to be included for sabotage. According the NERC Functional Model,

Organization	Yes or No	Question 4 Comment
Light		an LSE provides for estimating customer load and provides for the acquisition of transmission and energy to meet customer load demand. An LSE has no real impact on maintaining the reliability of electric network short of their planning function. Unfortunately, an LSE needs to be included for disturbance reporting to the DOE under certain conditions for loss of customer load. This may be a reason to maintain a separation of CIP-001 and EOP-004 so as not to unnecessarily include an LSE when it is not needed.
Response: The DSR SAR DT thanks you for your comment. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team added DP to the applicability of the standard as the Standard Drafting team may have a need to include them in the standard(s). The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements through the standard drafting stage of the process. The team will pass your comment along to the Standard Drafting Team for its consideration.		
IRC Standards Review Committee	No	We agree with the applicability of CIP-001-1 but question the need to include the RRO in EOP-004-1. Requirement R1 of EOP-004-1 can be turned into an industry developed and approved procedural requirement with details included in an appendix; whereas R5 can be changed to a requirement for the responsible entities to act on recommendations and to self-report compliance. Tracking and reviewing status of recommendation do not need to be performed by the RRO, or any entity for that matter, if a self-reporting mechanism is developed.
Response: The DSR SAR DT thanks you for your comment. The team concurs and notes that the SAR states: EOP-004 has some 'fill-in-the-blank' components to eliminate. This will remove the RRO from applicability.		
Pepco Holdings, Inc. - Affiliates	No	As specified in Order 693, Regional Reliability Organizations are not to be assigned applicability. The revised standard(s) should contain the reporting form either directly or by reference and the RRO should be removed. The other EOP-004 requirements for RROs are now considered normal monitoring activities of the Regional Entities.
Response: The DSR SAR DT thanks you for your comment. The team concurs and notes that the SAR states: EOP-004 has some 'fill-in-the-blank' components to eliminate. This will remove the RRO from applicability.		
FirstEnergy	No	The Regional Reliability Organization should be removed from the applicability of EOP-004-1. Any report they receive would be from the other entities listed. For consistency, the entities should report to the appropriate law enforcement agency. A report to the Reliability Entity should also be made for that entities information only.
Response: The DSR SAR DT thanks you for your comment. The team concurs and notes that the SAR states: EOP-004 has some 'fill-in-the-blank' components to eliminate. This will remove the RRO from applicability.		
Electric Market Policy	No	Applicability should not apply to LSE unless they have physical assets. If they do not have such assets, they are unable to

Organization	Yes or No	Question 4 Comment
		determine how many customers are out, how much load was lost or the duration of an outage. We continue to question the need for the LSE entity in reliability standards. End use customer load is either connected to transmission or distribution facilities. So, the applicable planner has to plan for that load when designing its facilities or the load will not have reliable service. To the extent that energy and capacity for that load is supplied by an entity other than the TO or DP, the TO or DP should have interconnection requirements that compel the supplier to provide any and all data necessary to meet the requirements of reliability standards.
Response: The DSR SAR DT thanks you for your comment. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the standard as the Standard Drafting team may have a need to include them in the standard(s). The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting stage of the process. The team will pass your comment along to the Standard Drafting Team for its consideration.		
MRO NERC Standards Review Subcommittee	No	As FERC has directed, the RRO should be removed since they are not owners or operators of the BES.
Response: The DSR SAR DT thanks you for your comment. The team concurs and notes that the SAR states: EOP-004 has some 'fill-in-the-blank' components to eliminate. **This will remove the RRO from applicability.**		
Lands Energy Consulting	No	CIP-001-1 - Yes. In many cases, the staff of an LSE embedded in another entity's BA/TOP area is more likely to discover an act of sabotage directed toward a BA/TOP-owned facility that could affect the BES than the asset owner. This is because the LSE likely has more operating staff in the area. I have included a requirement in my clients' Sabotage Identification and Reporting Procedures that the client treat acts of sabotage to a third party's system discovered by client employees as though the act was directed toward client facilities. EOP-004-1 - As mentioned before, I would eliminate the LSE from the applicability list and leave the responsibility for disturbance reporting and response to the TOP/BA. However, I would retain a responsibility for the LSEs to cooperate (when requested) with any disturbance investigation.
Response: The DSR SAR DT thanks you for your comment. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the standard as the Standard Drafting team may have a need to include them in the standard(s). The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting stage of the process. The team will pass your comment along to the Standard Drafting Team for its consideration.		
Calpine Corporation	No	The reporting requirements of EOP - 004 are needed for the RC, BA, LSE and the GOP that operates or controls generation in a system as defined by NERC. (System - A combination of generation, transmission, and distribution components). A disturbance is described as an unplanned event that produces and abnormal system condition, any

Organization	Yes or No	Question 4 Comment
		perturbation to the electric system, and the unexpected change in ACE that is caused by the sudden failure of generation or interruption of load. The GOP operating/controlling generation within a system has the ability to analyze system conditions to determine if reporting is necessary. A NERC registered GOP that is a merchant generator within another company's system does not have the ability for a wide area view and cannot analyze system conditions beyond the interconnection point of the facility. Moreover, in most cases the reporting requirements outlined in the Interconnection Reliability Operating Limits and Preliminary Disturbance Report do not apply to the merchant generator that is not a generation only BA. The applicability of the standard does encompass the true merchant generation entities required to register as GOP. Similarly, the OE-417 table 1 reporting requirements generally do not apply to a true merchant generating entity that is required to register as a GOP.
Response: The DSR SAR DT thanks you for your comment. The team agrees that generators may not have a wide area view and the capability to analyze events. The final wording of the requirements developed by the Standard Drafting Team will determine the applicability. The team will pass your comment on to the Standards Drafting Team for its consideration. The SAR calls for the removal of references to the DOE form OE-417.		
Cowlitz County PUD	No	Replace LSE with DP, and the Regional Reliability Organization with the Regional Entity.
Response: The DSR SAR DT thanks you for your comment. The team has added DP to the applicability of the SAR. The SAR calls for removing the fill-in-the-blank standard elements which will remove the RRO.		
United Illuminating	No	Add Distribution Provider
Response: The DSR SAR DT thanks you for your comment. The team has added DP to the applicability of the SAR.		
Reliant Energy	No	EOOP-004-1 should exclude the generator operator from disturbance reporting except providing the system operator or reliability coordinator with appropriate unit operation information upon request. Acts of sabotage should be identified clearly and reported to the indicated authorities.
Response: The DSR SAR DT thanks you for your comment. Other commenters have questioned the ability of Generator Operators to have a wide area view and to be able to analyze disturbances on the system. The team agrees that generators may not have a wide area view and the capability to analyze system events. The final wording of the requirements (i.e. reporting vs. data provision) developed by the Standard Drafting Team will determine the applicability to GOPs. The team will pass your comment on to the Standards Drafting Team for its consideration.		
Texas Regional Entity	No	Add GO and TO to the list of applicability. The intent of CIP-001-1 when it was first written was to have the proper and most likely entities associated directly with operations to be the ones to begin the reporting process in the case of sabotage on the system. In the ERCOT Region and other regions in the US, the GOP may not be physically located at the site. The GOP is often removed from the minute-by-minute responsibilities of plant operations and, therefore, may be less

Organization	Yes or No	Question 4 Comment
		able to react to physical sabotage at the location/plant/facility in a timely manner. The concern is that, in the case of an actual sabotage event, the failure to report to the appropriate authorities in a timely manner may jeopardize the reliability of the BPS. Therefore, the Generator Owner (GO) should be added to the list of applicability for CIP-001-1, because it is the GO that is more likely to be on location at the generation site and thus aware of sabotage when it first occurs. This would disallow for any possible communication gap and put responsibility on all of the appropriate entities to report such an event. Additionally, and for the same reasons as adding the GO, the Transmission Owner (TO) should also be added to the list of applicability for reporting sabotage on its facilities.
Response: The DSR SAR DT thanks you for your comment. The SAR DT discussed the addition of the TO and GO. The team was concerned that there may be duplication of requirements between the TO/TOP and GO/GOP if the TO and GO are added to the SAR. That being said, the team added the TO and GO to the applicability of the SAR so that the Standard Drafting team may consider these entities for applicability. The applicability of requirements will ultimately be determined by the Standard Drafting Team as it develops the requirements through the standard drafting Process. The team will pass your comment along to the Standard Drafting Team for its consideration concerning applicability.		
NextEra Energy Resources, LLC	No	The scope of the proposed SAR should not include the Generator Operator.
Response: The DSR SAR DT thanks you for your comment. Other commenters have questioned the ability of Generator Operators to have a wide area view and to be able to analyze disturbances on the system. The team agrees that generators may not have a wide area view and the capability to analyze system events. The final wording of the requirements (i.e. reporting vs. data provision) developed by the Standard Drafting Team will determine the applicability to GOPs. The team will pass your comment on to the Standards Drafting Team for its consideration.		
Exelon	No	CIP-001, remove LSE's from the standard for the reasons identified in the FERC LSE order. Ad TO and DP. EOP-004, remove LSE's from the standard for the reasons identified in the FERC LSE order. Remove RRO's, they are not a user, owner, operator of the BES. Add DP or TO. Consider conditional applicability as in the UFLS standards, " the TO or DP who performs the functions specified in the standard..."
Response: The DSR SAR DT thanks you for your comment. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the SAR. The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting stage of the process. The SAR DT discussed the addition of the TO. The team is concerned that there may be duplication of requirements between the TO/TOP if the TO is added to the SAR. That being said, the team added the TO and GO to the applicability of the SAR so that the Standard Drafting team may consider these entities for applicability. The applicability of requirements will ultimately be determined by the Standard Drafting Team as it develops the requirements through the standard drafting Process. The SAR calls for elimination of fill in the blanks elements, which will remove the RRO from the standard. The team will pass your comment along to the Standard Drafting Team for its consideration concerning conditional applicability.		

Organization	Yes or No	Question 4 Comment
ERCOT ISO	No	The Regional Reliability Organization is not a registered Functional Entity in the NERC registry. The applicability must be revised to more appropriately assign the requirements to registered functional entities. Also, the industry needs to recognize that there are other resources than generation for which the operators need to be included. Perhaps a demand-side resource should have a resource operator. This particular SAR may not be the appropriate venue for this, but control of resources which can be used to mitigate sabotage events or disturbance events may need to be addressed.
Response: The DSR SAR DT thanks you for your comment. The SAR calls for elimination of fill-in-the-blank elements, which will remove the RRO from the standard. The applicability of requirements will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting stage of the process. The team will pass your comment along to the Standard Drafting Team for its consideration concerning conditional applicability. This SAR is for reporting rather than control actions as you mention.		
Brazos Electric Power Cooperative, Inc.	No	May need to consider adding Transmission Owner. I don't see a need for the RRO to be included as they are not owner/operators of grid facilities.
Response: The DSR SAR DT thanks you for your comment. The SAR DT discussed the addition of the TO. The team is concerned that there may be duplication of requirements between the TO/TOP if the TO is added to the SAR. That being said, the TO has been added to the applicability of the SAR so that the Standard Drafting team may consider these entities for applicability. The applicability of requirements will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting stage of the process. The SAR calls for elimination of fill in the blank elements, which will remove the RRO from the standard. The team will pass your comment along to the Standard Drafting Team for its consideration concerning conditional applicability.		
PacifiCorp	No	LSE's don't generally own/operate facilities/systems that would experience a logical or physical sabotage event.
Response: The DSR SAR DT thanks you for your comment. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the SAR. The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting stage of the process.		
MidAmerican Energy	No	MidAmerican Energy believes the requirement for the Regional Reliability Organization should be removed from EOP-004-1 since the RRO is a holdover from making the standards enforceable. It is no longer appropriate for the regions to be named as responsible entities within the standards.
Response: The DSR SAR DT thanks you for your comment. The SAR calls for elimination of fill-in-the-blank elements, which will remove the RRO from the standard.		

Organization	Yes or No	Question 4 Comment
Georgia System Operations Corp.	No	EOP-004 should be retired. CIP-001 should not apply to LSEs other than those that are retail marketers.
Response: The DSR SAR DT thanks you for your comment. The SAR calls for EOP-004 to be revised. The Standard Drafting Team may, with stakeholder approval, retire it. CIP-001: NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the SAR. The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting process.		
AEP	No	We would recommend that the Load Serving Entity (LSE) be removed from both standards, and that the Generator Owner and Transmission Owner be added to the resulting standard.
Response: The DSR SAR DT thanks you for your comment. NERC has recognized, through its Compliance Registry, that there are asset owning LSEs and non-asset owning LSEs. The SAR DT believes that an asset owning LSE may be a Distribution Provider based on the Functional Model v4. The team has added DP to the applicability of the SAR. The applicability of LSE or Distribution Provider will ultimately be determined by the Standard Drafting Team as it develops the requirements in the standard drafting stage of the process. The SAR DT discussed the addition of the TO and GO. The team has a concern that there may be duplication of requirements between the TO/TOP and GO/GOP if the TO and GO are added to the SAR. That being said, the team added the TO and GO to the applicability of the SAR so that the Standard Drafting team may consider these entities for applicability. The applicability of requirements will ultimately be determined by the Standard Drafting Team as it develops the requirements through the standard drafting Process. The team will pass your comment along to the Standard Drafting Team for its consideration concerning applicability.		
Duke Energy	No	It's unclear to us that the RRO should continue to be an applicable entity.
Response: The DSR SAR DT thanks you for your comment. The team concurs and notes that the SAR states: EOP-004 has some 'fill-in-the-blank' components to eliminate. **This will remove the RRO from applicability.**		
Covanta	Yes	It would be a welcome enhancement to the end users to understand to communication link between all "appropriate parties" who shall be notified of potential or actual sabotage events.... which also needs to be defined.
Response: The DSR SAR DT thanks you for your comment. The team concurs, and will pass this comment on to the standard drafting team for its consideration.		
Edward C. Stein	Yes	
WECC	Yes	

Organization	Yes or No	Question 4 Comment
Luminant Power	Yes	
ReliabilityFirst Corporation	Yes	
Oncor Electric Delivery	Yes	
Consolidated Edison Co. of New York, Inc.	Yes	
Illinois Municipal Electric Agency	Yes	
Manitoba Hydro	Yes	
We Energies	Yes	
Consumers Energy Company	Yes	
PSEG Enterprise Group Inc Companies	Yes	
Northeast Power Coordinating Council	Yes	
Bonneville Power Administration	Yes	
Colmac Clarion	Yes	
Progress Energy	Yes	
Ameren	Yes	

5. If you have any other comments on the SAR or proposed modifications to CIP-001-1 and EOP-004-1 that you haven't provided in response to the previous questions, please provide them here.

Summary Consideration: Stakeholders provided many good comments that should be considered in the development of the standards under this project. The SAR DT does not believe that these require any revisions to the SAR and will forward these comments to the Standard Drafting Team for its consideration in developing the standard(s). These include:

1 Consolidation of reports: The SAR DT agrees with this concept and will forward the comment to the Standard Drafting Team for its consideration.

2 Concerns about pre-determination of combining CIP-001 and EOP-004 into one standard: The SAR states: CIP-001 *may* be merged with EOP-004 to eliminate redundancies. The two standards may be left separate.

3 Reporting criteria in multiple tables: The team agrees that it would be easier if there were only one table. Part of this SAR is to eliminate redundancies and make general improvements to the standard. The team also agrees that the requirements developed should be clear in their reliability objective.

Organization	Question 5 Comment
PSEG Enterprise Group Inc Companies	The PSEG Companies ask that the drafting team allow sufficient flexibility for sabotage recognition and reporting requirements such that nothing precludes utilizing a single corporate-wide program for both bulk electric system assets and other businesses. PSEG's Sabotage Recognition, Response and Reporting Program is directed to all business areas which are directed to follow the same internal protocol that also satisfies the NERC Standards requirements. For example, for gas assets, PSEG's gas distribution business follows the PSEG corporate-wide program for sabotage recognition and response. PSEG agrees that some modifications should be made to CIP-001 (ex. better define or give examples of sabotage) and EOP-004 to make them clearer? If they are merged, then Sabotage will not be in the title (or the primary focus) because several of the Disturbances that reporting is required for in EOP-004 have nothing to do with sabotage. EOP-004 has criteria listed in 4 places to determine when to send a report: o Criteria listed in EOP-004 Attachment 1 o Criteria listed in EOP-004 Attachment 2 o Criteria listed in top portion of Table 1-EOP-004 o Criteria listed in bottom potion of Table 1-EOP-004 Therefore, it would be much easier if there was one table of criteria for reference that addressed all of the reportable conditions and all of the applicable reports. If the 2 standards are merged as suggested in the SAR, any differences in the reporting obligation for actual or attempted sabotage and reporting of disturbances must be clear.

Organization	Question 5 Comment
Response: The DSR SAR DT thanks you for your comment. The team agrees that it would be easier if there were only one table. Part of this project is to eliminate redundancies and make general improvements to the standard. The team also agrees that the requirements developed should be clear in their reliability objective. The team will forward your comment to the standard drafting team for its consideration in the drafting of the standard.	
Kansas City Power & Light	If it is desirable to keep CIP-001 and EOP-004 separate, it is recommended the SDT consider adding a reference in CIP-001 to the DOE reporting form either by name or by internet link in the standard.
Response: The DSR SAR DT thanks you for your comment. The SAR SDT recommends eliminating all references to the DOE report, so there won't be a reference to it in CIP-001.	
IRC Standards Review Committee	We suggest that the revision not be conducted with a preconceived notion that the two standards must be combined since there are some differences between sabotage and emergency system conditions, and in the communication and reporting processes and channels. We suggest the SDT start off with a neutral position to focus on improving the standards, then assess the pros and cons of merging the two based on technical merit only.
Response: The DSR SAR DT thanks you for your comment. The SAR states: CIP-001 may be merged with EOP-004 to eliminate redundancies. The two standards may be left separate.	
Pepco Holdings, Inc. - Affiliates	Consider CIP-008-2 as potentially having overlaps with the proposed standard
Response: The DSR SAR DT thanks you for your comment. The SAR states "Specific references to the DOE form need to be eliminated." This will remove the linkage that you identify between CIP-001 and CIP-008. There is also a directive from FERC Order 693 in the SAR that states: **Consider FirstEnergy's suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality.** **This allows the standard drafting team to delineate physical and cyber assets. The DSR SAR DT also notes that CIP-008 might be a good framework for drafting the standard requirements pertaining to sabotage and disturbance reporting of physical assets.**	
FirstEnergy	1. Under Industry Need it states: "The existing requirements need to be revised to be more specific and there needs to be more clarity in what sabotage looks like." The use of the phrase "more specific" should be qualified by adding "while not being too prescriptive". As with other reliability standards, we do not want a standard that causes unwarranted and unnecessary additional work and costs to an entity to comply. 2. As pointed out by the NERC Audit and Observation Team in the "Issues to be considered" for CIP-001, clarification is needed regarding contacting the FBI. Prior audits dwelled heavily on FBI notification. For example, our policy states that Corporate Security notifies the FBI. In recent events it appears that local law enforcement handles day to day activities. The notification process for

Organization	Question 5 Comment
	contacting the FBI needs clarification along with specific instances in which to call them. Who should make the call to the FBI? It appears that a protocol needs to be developed to clarify what events require notifying the FBI. It could be as simple as after an incident a standard form is completed and forwarded to the FBI, letting them decide if follow up is needed. 3. We suggest aligning all reporting requirements for consistency. The items requiring reporting and the timelines to report are very inconsistent between NERC and the DOE. NERC's timelines are also not consistent with their own Security Guideline for the Electricity Sector: Threat and Incident Reporting.
Response: The DSR SAR DT thanks you for your comment. **The team concurs that the standards should provide the "what" without the "how". The standard drafting team will develop the standards using the NERC Standard Development Process that includes stakeholder consensus. The team does not feel it is necessary to add the "not too prescriptive" qualifier to the SAR.** **The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).** **The team concurs with your comment and notes that other commenters have suggested "one stop shopping" reporting for disturbances and sabotage. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).**	
Electric Market Policy	CIP-008-1 Incident Reporting and Response Planning include some requirements that require coordination with the requirements addressed in this project.
Response: The DSR SAR DT thanks you for your comment. The SAR states "Specific references to the DOE form need to be eliminated." This will remove the linkage that you identify between CIP-001 and CIP-008. There is also a directive from FERC Order 693 in the SAR that states: **Consider FirstEnergy's suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality.** **This allows the standard drafting team to delineate physical and cyber assets. The DSR SAR DT also notes that CIP-008 might be a good framework for drafting the standard requirements pertaining to sabotage and disturbance reporting of physical assets.**	
MRO NERC Standards Review Subcommittee	A. The SAR states that there may be impact on a related standard, COM-003-1 (page SAR-5). Is the SDT referring to Project 2007-02, Operating Personnel Communication Protocols? If so, this is a SAR too and should not be used as a reference. B. CIP-001-1 and EOP-004-1 should be combined into one EOP Standard. C. Within EOP-004-1 there is industry confusion on what form to submit in the event of an event. There should only be one form for the new combination Standard eliminating the need for reporting form attachments. It should be the DOE Form, OE-417. Although it is beyond the scope of this SAR, it would greatly benefit industry if there was a central location on the NERC website containing ALL reporting forms, including FERC, NERC, DOE, and ESIAC. This would enable the System Operators to efficiently locate the most current version of the appropriate form in order to report events.

Organization	Question 5 Comment
	D. The word Disturbance is primarily used in other Standards as in, Disturbance Control Standard or system separation due to a disturbance. Should the NERC definition be updated? Should the word "Sabotage" be defined by NERC? Additionally, we recommend that one definition of "Sabotage" be utilized industry-wide, instead of varying definitions by multiple groups like the DOE, ESIAC, etc.
Response: The DSR SAR DT thanks you for your comment. **A. It does reference project 2007-02, and it has been noted in the SAR.** **B. Will forward this comment to the standard drafting team for its consideration in developing the standard(s).** **C. The team concurs with your comment and notes that other commenters have suggested "one stop shopping" reporting for disturbances and sabotage. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).** **D. References to DOE are to be removed from the standards per the SAR. FERC Order 693 directives include definition of sabotage for CIP-001.**	
Lands Energy Consulting	One final comment on CIP-001-1. My clients received universally rude treatment from the FBI field offices when they attempted to establish the contacts required by the Standard. If the FBI doesn't see value in establishing these contacts, remove the requirement from the Standard. Making sure the LSE knows the FBI field office phone number is probably all the Standard should require.
Response: The DSR SAR DT thanks you for your comment. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).	
Colmac Clarion	Need single report for Sabotage so whatever is required results in notification of all parties (State Emergency Management, Homeland Security, FBI, Grid Reliability Chain of Command). Any and all of these can 'expand' knowledge later but all seem to require 'instant' notification.
Response: The DSR SAR DT thanks you for your comment. The team concur with your comment and notes that other commenters have suggested "one stop shopping" reporting for disturbances and sabotage. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).	
Cowlitz County PUD	Local Law enforcement agencies often are not friendly to Federal involvement with smaller problems they consider their "turf." Need to make sure the small stuff stays with them, however have a system of internal reporting that will catch coordinated sabotage efforts (multiple attacks on DPs and small BAs) at the RC or RE level who then can report to the Federal agencies. Currently EOP-004-1 requires small entities to report a "disturbance" if half of their firm customer load is lost. For some entities, this can be one small substation going down due to a bird. The "50% of total demand" requirement should be removed or improved to better define a true BPS disturbance.

Organization	Question 5 Comment
Response: The DSR SAR DT thanks you for your comment. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).	
Exelon	Exelon agrees this is a worthwhile project and that reliability will be enhanced and the compliance process will be simplified by clarifying terminology and reporting requirements in these standards. If nothing else, defining "Sabotage" so as to end interpretations of this term and the related requirements is necessary.
Response: The DSR SAR DT thanks you for your comment.	
ERCOT ISO	Due to the fact that both the CIP-001-1 and EOP-004-1 have similar reporting standards, initially combining the two sounds like a correct analysis. However, after further consideration and due to the critical nature of its intended function involving Security aspects, the CIP-001 should be intensely evaluated to determine if its intended purpose meets the threshold or criteria to stand alone. The existing standards for CIP-001-1 Sabotage Reporting may help prevent future mitigation actions caused by sabotage events. EOP-004-1 Disturbance Reporting is administrative in nature, thus the jeopardy of the Bulk Electric System reliability is impacted only if analysis is not performed or if corrective follow-up actions are not implemented. Combining EOP-004 Standard requirements under the umbrella of the CIP -001 Standard would create a high profile Disturbance Reporting Standard. The industry would be better served if information defining sabotage was provided as well as a technical reference document on recognizing sabotage that would also clarify or state any personnel training requirements. All aspects of the intended functions must be reviewed before merging the two standards. At a minimum, we must consider modification that provides improved understanding of the reporting standards and implications as they are currently written.
Response: The DSR SAR DT thanks you for your comment. The SAR states: CIP-001 *may* be merged with EOP-004 to eliminate redundancies. The two standards may be left separate. One of the FERC Order 693 directives for CIP-001 states: **Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event.** **The Standard Drafting Team will follow the NERC Standard Development Process in making revisions under this SAR, including a thorough review of the requirements of both standards. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).**	
MidAmerican Energy	Conflicting time frames exist from document updates. Reporting should be consolidated to one form and / or site to minimize conflicts, confusion, and errors. 1) Reporting requirements for the outage of 50,000 or more customers in EOP-004-1 requires a report to be made within one hour while the form OE-417 requires a report be made within six hours of the outage. The six hour reference on the updated OE-417 form is the correct reference. 2) Reporting for either CIP-001 or EOP-004 should center on the DOE Form OE-417. This would eliminate confusion and simplify reporting for system operators thereby directly enhancing reliability during system events. This would also eliminate much of the duplicate material and attachments in EOP-004. 3) Although it is beyond the scope of this SAR, the industry would benefit if there was a central location or link on the NERC website containing all

Organization	Question 5 Comment
	reporting forms, including FERC, NERC, DOE, and ESIAC. This would enable System Operators to more efficiently locate and report events.
Response: The DSR SAR DT thanks you for your comment. The team notes that other commenters have suggested "one stop shopping" reporting for disturbances and sabotage. The team concurs that timeframes for similar reports should be the same. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s).	
Georgia System Operations Corp.	Entity reporting to NERC/Regions is needed by NERC and the Regions to accomplish their missions of overseeing the reliability of the BES and enforcing compliance with Reliability Standards. An entity not reporting as quickly as possible does not harm the integrity of the Interconnection. In fact, it increases the risk to the BES to be investigating details and filling out forms during a time when attention should be on correcting or mitigating an incident.
Response: The DSR SAR DT thanks you for your comment. The team agrees that non-reporting, in the administrative sense, may not harm the integrity of the Interconnection. The team suggests that the appropriate avenue for addressing this concern is through the development of Violation Risk Factors and Violation Severity Levels for each requirement. These compliance elements will be developed during the standard drafting stage of the development process.	
Illinois Municipal Electric Agency	IMEA recommends the following considerations: Simplification of reportable events and the reporting process should be the overriding objective. NERC's Security Guideline for the Electricity Sector: Threat and Incident Reporting (Version 2.0) should be updated to support this standards development initiative. At some point in the process, it may help if examples are given of events actually reported that did not need to be reported.
Response: The DSR SAR DT thanks you for your comment. The team notes that other commenters have suggested "one stop shopping" reporting for disturbances and sabotage. The team agrees that NERC's Security Guide should be in sync with the standards. The team will forward this comment to the standard drafting team for its consideration in developing the standard(s). One of the FERC Order 693 directives for CIP-001 states: **Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event.** **Events that were reported, but didn't need to be, may be identified in "lessons learned".**	
WECC	No
Luminant Power	None
Oncor Electric Delivery	No Additional Comments

Organization	Question 5 Comment
NextEra Energy Resources, LLC	No comment.
Ameren	None

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form for SAR Drafting Team for Disturbance and Sabotage Reporting (Project 2009-01)

Please use the electronic nomination form located at the link below. If you have any questions, please contact David Taylor at david.taylor@nerc.net or by telephone at 609-651-5089.

http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

By submitting the following information you are indicating your commitment to actively participate in SAR Drafting Team meetings if appointed to the SAR Drafting Team by the Standards Committee.

Name: Organization: Address: Telephone: E-mail:
Project 2009-01 Disturbance and Sabotage Reporting will entail revising existing standards CIP-001 — Sabotage Reporting and EOP-004 — Disturbance Reporting to eliminate redundancies and provide clarity on sabotage events. The project includes addressing several issues identified by stakeholders, FERC directives from Order 693, and may include improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards. Please briefly describe (no more than a couple of paragraphs) your experience and qualifications directly related to the issues to be addressed by the Disturbance and Sabotage Reporting SAR Drafting Team. We are seeking a cross section of the industry to participate on the team, but in particular are seeking individuals with experience in management of real-time bulk power operations activities. Please include any previous experience related to developing or applying IEEE or other industry related standards as this type of experience might be beneficial to include on the team, but is not a requisite to be appointed to the team.

Are you currently a member of any NERC or Regional Entity SAR or standard drafting team? If yes, please list each team here.	☐ No ☐ Yes:
Have you previously worked on any NERC or Regional Entity SAR or standard drafting teams? If yes, please list them here.	☐ No ☐ Yes:

Please identify the NERC Region(s) for which you are able to represent your company's position relative to the topics addressed in the SAR:	Please identify the Industry Segment(s) for which you are able to represent your company's position relative to the topics addressed in the SAR:	
☐ ERCOT ☐ FRCC ☐ MRO ☐ NPCC ☐ RFC ☐ SERC ☐ SPP ☐ WECC ☐ Not Applicable or None of the Above	☐	1 — Transmission Owners
	☐	2 — RTOs and ISOs
	☐	3 — Load-serving Entities
	☐	4 — Transmission-dependent Utilities
	☐	5 — Electric Generators
	☐	6 — Electricity Brokers, Aggregators, and Marketers
	☐	7 — Large Electricity End Users
	☐	8 — Small Electricity End Users
	☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
	☐	10 — Regional Reliability Organizations and Regional Entities
	☐	Not applicable
Please identify the Functional Entities[1] for which you are able to represent your company's position relative to the topics addressed in the SAR:		

[1] These functions are defined in the NERC Functional Model, which is available on the NERC Web site.

☐ Balancing Authority	☐ Planning Coordinator
☐ Compliance Enforcement Authority	☐ Transmission Operator
☐ Distribution Provider	☐ Transmission Owner
☐ Generator Operator	☐ Transmission Planner
☐ Generator Owner	☐ Transmission Service Provider
☐ Interchange Authority	☐ Purchasing-selling Entity
☐ Load-serving Entity	☐ Resource Planner
☐ Market Operator	☐ Reliability Coordinator

Please provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group. NERC staff may contact these references.

Name and Title:	Office Telephone:
Organization:	E-mail:
Name and Title:	Office Telephone:
Organization:	E-mail:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Nomination Period Opens for Standard Authorization Request (SAR) Drafting Team
April 29–May 13, 2009

Now available at: http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Nominations for SAR Drafting Team (Project 2009-01 — Disturbance and Sabotage Reporting)

The Standards Committee is seeking industry experts to serve on the Disturbance and Sabotage Reporting SAR Drafting Team (see project background below). The SAR drafting team will assist the requester in further developing the SAR and considering stakeholder comments.

If you are interested in serving on this standard drafting team, please complete the following electronic nomination form **by May 13, 2009**:
https://www.nerc.net/nercsurvey/Survey.aspx?s=bf869d5cbde94f9788c7606a2f50829f

Please contact Dave Taylor at david.taylor@nerc.net or at 609-651-5089 with any questions about the team.

Project Background:

Project 2009-01 — Disturbance and Sabotage Reporting will entail revising existing standards CIP-001-1 — Sabotage Reporting and EOP-004-1 — Disturbance Reporting to eliminate redundancies and provide clarity on sabotage events. The project includes addressing several issues identified by stakeholders, FERC directives from Order 693, and may include improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

More information about the project is available on the following page:
http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request Form

Title of Proposed Standard: Disturbance and Sabotage reporting (Project 2009-01)
Request Date: April 2, 2009
Approved by SC for posting: April 15, 2009
Revision Date: August 13, 2009

SAR Requester Information	**SAR Type** (*Check a box for each one that applies.*)	
Name: Patrick Brown	☐	New Standard
Primary Contact: Patrick Brown Manager, NERC and Regional Coordination PJM Interconnection	☒	Revision to existing Standard
Telephone: 610-666-4597	☒	Withdrawal of existing Standard
E-mail: brownp@pjm.com	☐	Urgent Action

Purpose **(Describe the proposed standard action: Nomination of a proposed standard, revision to a standard, or withdrawal of a standard and describe what the standard action will achieve.)**

This project will entail revision to existing standards CIP-001-1 – Sabotage Reporting and EOP-

004-1 – Disturbance Reporting. The standards may be merged to eliminate redundancy and provide clarity on sabotage events. EOP-004 has some 'fill-in-the-blank' components to eliminate. The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

Industry Need (Provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

The existing requirements need to be revised to be more specific – and there needs to be more clarity in what sabotage looks like.

Brief Description (Provide a paragraph that describes the scope of this standard action.)

CIP-001 may be merged with EOP-004 to eliminate redundancies. Acts of sabotage have to be reported to the DOE as part of EOP-004. Specific references to the DOE form need to be eliminated.

EOP-004 has some 'fill-in-the-blank' components to eliminate.

The development may include other improvements to the standards deemed appropriate by

the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards (see tables for each standard at the end of this SAR for more detailed information).
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR.) See "Issues to be Considered by Drafting Team" tables for each standard at the end of this SAR for more detailed information.

Reliability Functions

The Standard will Apply to the Following Functions *(Check box for each one that applies.)*		
☒	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☐	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☒	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check box for all that apply.)*	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☒	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*
1. A reliability standard shall not give any market participant an unfair competitive advantage. Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes

Related Standards

Standard No.	Explanation
COM-003-1	Operations Communications Protocols – this standard may include some requirements that require coordination with the requirements addressed in this project. (still in standard development stage)
IRO-014-1	R1.1.1, footnote 1 lists sabotage. The standard drafting team should consider this reference and the impact of their work on this specific item.
TOP-005-1.1	Attachment 1, item 2.9 is “Multi-site sabotage”. The standard drafting team should consider this reference and the impact of their work on this specific item.

Related SARs

SAR ID	Explanation

Regional Variances

Region	Explanation
ERCOT	
FRCC	
MRO	
NPCC	
SERC	
RFC	
SPP	
WECC	

Issues to be Considered by Drafting Team Project 2009-01 — Disturbance and Sabotage Reporting	
Standard #	**Title**
CIP-001-0	Sabotage Reporting

Issues

FERC Order 693

Disposition: Approved with modifications

- Consider the need for wider application of the standard. Consider whether separate, less burdensome requirements for smaller entities may be appropriate.
- Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event.
- In the interim, provide advice to entities about the reporting of particular circumstances as they arise.
- Consider FirstEnergy's suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality.
- Incorporate a periodic review or updating of the sabotage reporting procedures and for their periodic testing. Consider a staggered schedule of annual testing and formal review every two to three years.
- Include a requirement to report a sabotage event to the proper government authorities. Develop the language to specifically implement this directive.
- Explore ways to reduce redundant reporting, including central coordination of sabotage reports and a uniform reporting format.

V0 Industry Comments

- Object to multi-site requirement
- Definition of sabotage required

VRF comments

- Adequate procedures will insure it is unlikely to lead to bulk electric system instability, separation, or cascading failures.

Other

- Modify standard to conform to the latest version of NERC's Reliability Standards Development Procedure, the NERC Standard Drafting Team Guidelines, and the ERO Rules of Procedure.

NERC Audit and Observation Team

- Applicability — How does this standard pertain to Load Serving Entities, LSE's.
- Registered Entities have sabotage reporting processes and procedures in place but not all personnel has been trained.
- Question: How do you "and make the operator aware"
- R4 — "What is meant by: "establish contact with the FBI". Is a phone number adequate? Many entities which call the FBI are referred back to the local authority. The AOT noted that on the FBI website it states

	to contact the local authorities. Is this a question for Homeland Security to deal with for us?"
	• R4 — Establish communications contacts, as applicable with local FBI and RAMP officials. Some entities are very remote and the sheriff is the only local authority does the FBI still need to be contacted?
	FERC's December 20, 2007 and April 4, 2008 Orders in Docket Nos. RC07-004-000, RC07-6-000, and RC07-7-000
	• In FERC's December 20, 2007 Order, the Commission reversed NERC's Compliance Registry decisions with respect to three load serving entities in the ReliabilityFirst (RFC) footprint. The distinguishing feature of these three LSEs is that none owned physical assets. Both NERC and RFC assert that there will be a "reliability gap" if retail marketers are not registered as LSEs. To avoid a possible gap, a consistent, uniform approach to ensure that appropriate Reliability Standards and associated requirements are applied to retail marketers must be applied. Each drafting team responsible for reliability standards applicable to LSEs is to review and change as necessary, requirements in the applicable reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. For additional information see:
	  • FERC's December 20, 2007 Order (http://www.nerc.com/files/LSE_decision_order.pdf)
	  • NERC's March 4, 2008 (http://www.nerc.com/files/FinalFiledLSE3408.pdf),
	  • FERC's April 4, 2008 Order (http://www.nerc.com/files/AcceptLSECompFiling-040408.pdf) and
	  • NERC's July 31, 2008 (http://www.nerc.com/files/FinalFiled-CompFiling-LSE-07312008.pdf) compliance filings to FERC on this subject.

Issues to be Considered by Drafting Team Project 2009-01 — Disturbance and Sabotage Reporting	
Standard #	**Title**
EOP-004-1	Disturbance Reporting
Issues	FERC Order 693 Disposition: Approved with modification • Include any requirements for users, owners, and operators of the bulk power system to provide data that will assist NERC in the investigation of a blackout or disturbance. • Change NERC's Rules of Procedure to assure the Commission receives these reports in the same frame as the DOE. • Consider APPA's concern about generator operators and LSEs analyzing performance of their equipment and provide data and information on the equipment to assist others with analysis. • Consider all comments offered in a future modification of the reliability standard.

	Fill-in-the-Blank Team Comments
	• Consider changes to R1 and R3.4 to standardize the disturbance reporting requirements (requirements for disturbance reporting need to be added to this standard)
	• Regions currently have procedures, but not in the form of a standard. The drafting team will need to review regional requirements to determine reporting requirements for the North American standard.
	V0 Industry Comments
	• R3 – too many reports, narrow requirement to RC
	• How does this apply to generator operator?
	Other
	• Modify standard to conform to the latest version of NERC's Reliability Standards Development Procedure, the NERC Standard Drafting Team Guidelines, and the ERO Rules of Procedure.
	NERC Audit and Observation Team
	• R3.1 — Can there be a violation without an event?
	Event Analysis Team
	• Reliability Issue: Coordination and follow up on lessons learned from event analyses Consider adding to EOP-004 – Disturbance Reporting. Proposed requirement: Regional Entities (REs) shall work together with Reliability Coordinators, Transmission Owners, and Generation Owners to develop an Event Analysis Process to prevent similar events from happening and follow up with the recommendations. This process shall be defined within the appropriate NERC Standard.
	FERC's December 20, 2007 and April 4, 2008 Orders in Docket Nos. RC07-004-000, RC07-6-000, and RC07-7-000
	• In FERC's December 20, 2007 Order, the Commission reversed NERC's Compliance Registry decisions with respect to three load serving entities in the ReliabilityFirst (RFC) footprint. The distinguishing feature of these three LSEs is that none owned physical assets. Both NERC and RFC assert that there will be a "reliability gap" if retail marketers are not registered as LSEs. To avoid a possible gap, a consistent, uniform approach to ensure that appropriate Reliability Standards and associated requirements are applied to retail marketers must be applied. Each drafting team responsible for reliability standards applicable to LSEs is to review and change as necessary, requirements in the applicable reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. For additional information see:
	  • FERC's December 20, 2007 Order (http://www.nerc.com/files/LSE_decision_order.pdf)
	  • NERC's March 4, 2008 (http://www.nerc.com/files/FinalFiledLSE3408.pdf),
	  • FERC's April 4, 2008 Order (http://www.nerc.com/files/AcceptLSECompFiling-040408.pdf) and
	  • NERC's July 31, 2008 (http://www.nerc.com/files/FinalFiled-CompFiling-LSE-07312008.pdf) compliance filings to FERC on this subject.

Comments received on Project 2009-01 — Disturbance and Sabotage Reporting

The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) received many suggestions for improvements to the standards during the SAR comment period. These comments do not indicate any revisions to the SAR, but the DSRSDT thought that these comments merited further consideration during the standard drafting phase of the project. The comments below are being compiled for use by the Standard Development Team.

Organization	Comment
Electric Market Policy	Comments: Agree with the statement that sabotage is hard to determine in real time by operations staffs. The determination of sabotage should be left up to law enforcement. They have the knowledge and peer contacts needed to adequately determine whether physical or cyber intrusions are merely malicious acts or coordinated efforts (sabotage). The operators should only be required to report physical and cyber intrusions to law enforcement. All other reporting requirements should apply to law enforcement once a determination of sabotage has been made. If the recommendations above are not to be accepted, then we have the following comments: CIP-001-1 1) R1 states entities shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SAR notes that the industry objects to the multi-site requirement, most likely because the term is ambiguous. If this term remains in the standard, it needs to be clearly defined and responsibilities for obtaining (how do you get this information and from whom?) and distributing need to be included. 2) R1 audits have shown confusion over the requirement to make operating personnel aware of sabotage events. The term operating personnel needs to be defined. Are they the individuals responsible for operating the facility, coordinating with other entities (i.e., RC, BA, TOP, GOP, and LSE)? It has been suggested that notification is required to all personnel at a facility. Keep in mind the purpose of the standard is to ensure sabotage events are properly reported, not to address emergency response. 3) R1 The SAR (NERC Audit and Observation Team) notes that Registered Entities have processes and procedures in place, but not all personnel have been trained. There is no specific training requirement in the standard. 4) R2 & R3 I agree with the SAR that sabotage needs to be defined and these requirements should be more specific with respect to the information to be communicated. It seems to me that the standard should mirror the criteria contained in DOE OE-417. The emphasis should be placed on ensuring that the same information communicated to DOE is shared with the appropriate parties in the Interconnection. 5) R4 I agree with the SAR (NERC Audit and Observation Team) comments regarding the intention of this requirement. There is no language that directs contact with FBI or RCMP although that is what is implied by the Purpose statement.

Organization	Comment
	6) VRF Comments I'm not sure what is intended by the statement Adequate procedures will insure it is unlikely to lead to bulk electric system instability, separation, or cascading failures? The purpose of the standard is that of communication. No operational decisions or actions are directed by this standard, nor does it require entities to address operational aspects resulting from sabotage. 7) The potential exists for overlapping sabotage reporting requirements at nuclear power plants due to multiple regulators (Nuclear Regulatory Commission (NRC) 10 CFR 73 and Federal Energy Regulatory Commission (FERC) NUC-001-1). Some entities may have revised existing NRC driven procedures to accommodate reporting requirements of both regulators. Because of the restrictions placed on NRC driven documents (i.e., procedures are classified as safeguards information), it can be difficult to demonstrate compliance to NERC and/or FERC without ensuring that the individuals are qualified for receipt of such information per 10 CFR 73. Additionally, multiple procedures may have the unintended consequence of delaying appropriate communication.EOP-004-1Consider removing Attachment 2 as the information is duplicated in DOE Form OE-417. A simple reference to the form should suffice.
Lands Energy Consulting	I have worked with 5 Northwest public utilities on developing procedures related to CIP-001-1 and EOP-004-1. All 5 utilities operate electric systems in fairly remote locations and are embedded in a larger utility's Balancing Authority/Transmission Operator area. A. CIP-001-1 - Developing procedures to unambiguously identify acts of sabotage has been particularly challenging for these systems. In general, it's hard for them to determine whether the most prevalent forms of malicious and intentional system damage that they incur - copper theft and gun shot insulators/equipment - should qualify as acts of sabotage. Although none of the systems consider copper theft to be acts of sabotage, two of the systems consider gun shot insulators/equipment to be acts of sabotage. The other systems look for intent to disrupt electric system operations as a key component of their sabotage identification procedures. Additional guidance from NERC in the form of CIP-001-1 modifications or a companion guidelines document on sabotage identification would provide much needed guidance for these procedures. B. EOP-004-1 - This standard was clearly drafted with the larger electric systems in mind. I have one client that serves 3300 commercial/residential customers from 4-115/13 kV substation transformers and one large industrial customer (80% of its energy load) from a 230/13 kV substation. 75% of the client's load is served from three substations attached to a long, 115 kV transmission line operated by the Bonneville Power Administration. Whenever the line relays open on a permanent fault (which happens 2-3 times per year), the client loses over 50% of its customers (but no more than 10-15 MW during winter peak), thereby necessitating the preparation of a Disturbance Report. To allow utilities to concentrate on operating their systems, without fear of violating EOP-004-1 for failure to report trivial outages, I would remove LSEs from the obligation to report disturbances - leave the reporting to the BA/TOP for large outages in their footprint.
Calpine Corporation	Communication of facility status or emergencies between merchant generators registered as GOP and the RC, BA,

Organization	Comment
	GOP, or LSE in which the facility resides should be coordinated for EOP -004 reporting. The reporting to NERC/DOE should come from the RC, BA, GOP, or LSE.
Covanta	Yes - the key to Sabotage reporting requirements is identifying what the 'definition' is of an actual or potential 'Sabotage' event. Like any other standard, if FERC/NERC leave it up to 2000+ entities to establish their own definitions of 'Sabotage', you may likely get 2000+ answers. That is not a controlled and coordinated approach. I offer the following definition, "Sabotage - Deliberate or malicious destruction of property, obstruction of normal operations, or injury to personnel by outside agents." Examples of sabotage events could include, but are not limited to, suspicious packages left near site electrical generating or electrical transmission assets, identified destruction of generating assets, telephone/e mail received threats to destroy or interrupt electrical generating efforts, etc." These have passed multiple NERC regional audits and reviews to date.
Northeast Power Coordinating Council	The SAR needs to be more specific in defining its objectives. CIP-001Requirement R1 currently states: R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SDT needs to include the following objectives: 1. Develop clear definitions for the terms “operating personnel” and “sabotage events.” The definition of “operating personnel,” should be clarified and limited to staff at BES facilities. Operating personnel should report only those events which meet a clear, recognizable threshold as reportable potential sabotage events. There should be a consistent continent-wide list of examples or typical reportable and non-reportable events to help guide operating personnel. The term “sabotage event” needs to be defined. Clarification is required regarding when the determination of a sabotage event is made, e.g., upon first observation (requiring operating personnel be educated in discerning sabotage events), or upon later investigation by trained security personnel and law enforcement individuals. The terms potential or suspected sabotage event for reporting purposes should be clarified or defined. 2. Define the obligations of Registered Entity operating personnel - who are required to be aware of such “sabotage events,” e.g., who, what, where, when, why and how, and what they are to do in response to this awareness. The SDT should clarify the use of the term “aware” in the standard. “Aware” can be interpreted in accordance with its largely passive, dictionary-based meaning, where being “aware” simply means knowing about something, such as a sabotage event. Alternatively, the Reliability Standard meaning of “aware” could refer to more active wording, involving more than mere awareness, e.g., “alert and quick to respond,” pointing to and requiring a specific affirmative response, i.e., reporting to the appropriate systems, governmental agencies, and regulatory bodies.

Organization	Comment
	EOP-004 - The SDT needs to work on the following areas. 1. NERC reporting needs to be clarified. For example, Attachment 1 paragraph 6c states: Introduction “The entity on whose system a reportable disturbance occurs shall notify NERC ... 6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in: c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance - The sense of Attachment 1 is internally inconsistent between the introduction (“occurs”) and the required actions in 6c (could have resulted in a system disturbance). The initial intent appears to be only to report actual system disturbances. Yet, paragraph 6c adds the phrase “or could have resulted in” a potential system disturbance. This inconsistency should be clarified.
FirstEnergy	We agree with the scope but would also like to see the following considered: 1. References to the DOE reporting process in EOP-004 need to be revised. They currently refer to the old EIA form. 2. Besides "sabotage", it may be helpful to clearly define "vandalism". It is vaguely written in the standards. Also, the process of "public appeals" for the DOE reportable requirements needs to be more clearly defined. 3. Consolidate documents covering reporting requirements. There are currently several documents that require reporting (EOP-004, CIP-001, DOE oe-417, and NERC's Security Guideline for the Electricity Sector: Threat and Incident Reporting). NERC also has the "Bulk Power System Disturbance Classification Scale" that does not completely align with all the reporting requirements. Therefore we recommend keeping this as simple as possible by combining all the reporting requirements into one standard. It would be beneficial to not require operators to have to go to 4 different documents to determine what to report on.
MRO NERC Standards Review Subcommittee	The MRO NSRS would like to keep the references to the DOE reporting form.
Cowlitz County PUD	Added to the scope: For EOP-004 add a provision for a reporting flow rather than everything going to the RE and NERC. That is something going like the DP and TOP reports to the BA, the BA to the RE, and the RE to NERC. This would allow for multiple related reports to be combined into a single coherent report as the reporting goes up the chain. For CIP-001 consider reporting flow as above with local law enforcement notification. Let an upper entity in the reporting chain decide when to contact Federal Agencies such as the BA or the RC.
Reliant Energy	I think Generator operators should be excluded except to provide requested information from the System Operator or

Organization	Comment
	Reliability coordinator.
ERCOT ISO	The scope should be modified to provide for a different treatment of reporting requirements that are administrative in nature, or that are after-the-fact (thus cannot impact reliability unless analysis and follow-up is not performed; even then, the impact would be at some future time). Reporting requirements which are of the nature to assist in identification of system concerns or which serve to prevent or mitigate on-going system problems (including, but not limited to, actual or attempted sabotage activity) should remain in standards, but should be separate and apart from the administrative reporting.
Consolidated Edison Co. of New York, Inc.	GENERAL CECONY and ORU support the general objectives of the SAR to merge existing standards CIP-001-1 Sabotage Reporting and EOP-004-1 Disturbance Reporting to improve clarity and remove redundancy. However, the SAR needs to be more specific in defining its objectives. CIP-001Requirement R1 currently states: R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SDT needs to include the following objectives: 1. Develop clear definitions for the terms operating personnel and sabotage events. The definition of operating personnel, should be clarified and limited to staff at BES facilities. Operating personnel should report only those events which meet a clear, recognizable threshold as reportable potential sabotage events. There should be a consistent continent-wide list of examples or typical reportable and non-reportable events to help guide operating personnel. The term sabotage event needs to be defined. Clarification is required regarding when the determination of a sabotage event is made, e.g., upon first observation (requiring operating personnel be educated in discerning sabotage events), or upon later investigation by trained security personnel and law enforcement individuals. The terms potential or suspected sabotage event for reporting purposes should be clarified or defined. 2. Define the obligations of Registered Entity operating personnel - who are required to be aware of such sabotage events, e.g., who, what, where, when, why and how, and what they are to do in response to this awareness. The SDT should clarify the use of the term aware in the standard. Aware can be interpreted in accordance with its largely passive, dictionary-based meaning, where being aware simply means knowing about something, such as a sabotage event. Alternatively, the Reliability Standard meaning of aware could refer to more active wording, involving more than mere awareness, e.g., alert and quick to respond, pointing to and requiring a specific affirmative response, i.e., reporting to the appropriate systems, governmental agencies, and regulatory bodies. EOP-004 - The SDT needs to work on the following areas.

Organization	Comment
	1. NERC reporting needs to be clarified. For example, Attachment 1 paragraph 6c states: Introduction The entity on whose system a reportable disturbance occurs shall notify NERC ... 6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in: ?c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance. The sense of Attachment 1 is internally inconsistent between the introduction (occurs) and the required actions in 6c (could have resulted in a system disturbance). The initial intent appears to be only to report actual system disturbances. Yet, paragraph 6c adds the phrase or could have resulted in a potential system disturbance. This inconsistency should be clarified.
Georgia System Operations Corp.	The scope of the SAR should be to move all requirements to report to NERC or Regional Entities out of the Requirements section of all Reliability Standards to elsewhere. This does not include reporting, communicating, or coordinating between reliability entities. The NERC/Region reporting requirements could be consolidated in another document and referenced in the Supporting References section of the Reliability Standards. The deadlines for reporting should be changed to realistic timeframes that do not interfere with operating the BES or responding to incidents yet still allow NERC and the Regions to accomplish their missions.
AEP	Sabotage is a term of intent that is often determined after the fact by the registered entity and/or law enforcement officials. In fact, it is often difficult to determine in real-time the intent of a suspicious event. We would suggest that suspicious events become reportable at the point that the event is determined to have had sabotage intent. The entities should have a methodology to collect evidence, to have the evidence analyzed, and to report those events that are determined to have had the intent of sabotage.
Duke Energy	While we agree with the need for clarity in sabotage and disturbance reporting, we believe that the Standards Drafting Team should carefully consider whether there is a reliability-related need for each requirement. Some disturbance reporting requirements are triggered not just to assist in real-time reliability but also to identify lessons-learned opportunities. If disturbance and sabotage reporting continue to be reliability standards, we believe that all linkages to lessons-learned/improvements need to be stripped out. We have other forums to identify lessons-learned opportunities and to follow-up on those opportunities. Also, requirements to report possible non-compliances should be eliminated. We strongly support voluntary self-reporting, but not mandatory self-reporting.
NextEra Energy Resources, LLC	The scope of the SAR should not include Generator Operators.

Organization	Comment
Luminant Power	The SAR drafting team should include in the SAR scope a review of the NRC sabotage and event reporting requirements to ensure there are no overlapping or conflicting requirements between NERC, FERC, and the NRC. The SAR scope should include a review of the CIP Cyber Security Standards and coordination with the CIP SDT to ensure that cyber sabotage reporting definitions are in concert, and ensure that cyber sabotage reporting requirements are not duplicated in multiple standards.
Illinois Municipal Electric Agency	A one-stop reporting tool/site would facilitate efficient reporting and compliance; e.g., further development of the ES-ISAC/CIPIS to include all reportable categories and automatic notification of required parties. A single report form would be best.
AEP	The current reporting process necessitates multiple reports be sent to multiple parties, which is inefficient and may, inadvertently, result in alignment issues between the separate reports. We would recommend that a single report that combines NERC (CIPIS) and NERC ESISAC information be provided to NERC (CIPIS) that is systematically (programmatically) forwarded to all necessary entities. Further, updates to incidents would also go through NERC with the same electronic processing. Currently, we are not aware of a formal method to report incidents to the FBI, which should be also included in the distribution. The current reporting mechanism to the FBI JTTF is by telephone and the NERC platform described would provide more consistent reporting.
Kansas City Power & Light	Do not agree Load Serving Entities need to continue to be included for sabotage. According the NERC Functional Model, an LSE provides for estimating customer load and provides for the acquisition of transmission and energy to meet customer load demand. An LSE has no real impact on maintaining the reliability of electric network short of their planning function. Unfortunately, an LSE needs to be included for disturbance reporting to the DOE under certain conditions for loss of customer load. This may be a reason to maintain a separation of CIP-001 and EOP-004 so as not to unnecessarily include an LSE when it is not needed.
Electric Market Policy	Applicability should not apply to LSE unless they have physical assets. If they do not have such assets, they are unable to determine how many customers are out, how much load was lost or the duration of an outage. We continue to question the need for the LSE entity in reliability standards. End use customer load is either connected to transmission or distribution facilities. So, the applicable planner has to plan for that load when designing its facilities or the load will not have reliable service. To the extent that energy and capacity for that load is supplied by an entity other than the TO or DP, the TO or DP should have interconnection requirements that compel the supplier to provide any and all data necessary to meet the requirements of reliability standards.
Lands Energy Consulting	CIP-001-1 - Yes. In many cases, the staff of an LSE embedded in another entity's BA/TOP area is more likely to discover an act of sabotage directed toward a BA/TOP-owned facility that could affect the BES than the asset owner. This is because the LSE likely has more operating staff in the area. I have included a requirement in my clients'

Organization	Comment
	Sabotage Identification and Reporting Procedures that the client treat acts of sabotage to a third party's system discovered by client employees as though the act was directed toward client facilities. EOP-004-1 - As mentioned before, I would eliminate the LSE from the applicability list and leave the responsibility for disturbance reporting and response to the TOP/BA. However, I would retain a responsibility for the LSEs to cooperate (when requested) with any disturbance investigation.
Calpine Corporation	The reporting requirements of EOP - 004 are needed for the RC, BA, LSE and the GOP that operates or controls generation in a system as defined by NERC. (System - A combination of generation, transmission, and distribution components). A disturbance is described as an unplanned event that produces and abnormal system condition, any perturbation to the electric system, and the unexpected change in ACE that is caused by the sudden failure of generation or interruption of load. The GOP operating/controlling generation within a system has the ability to analyze system conditions to determine if reporting is necessary. A NERC registered GOP that is a merchant generator within another company's system does not have the ability for a wide area view and cannot analyze system conditions beyond the interconnection point of the facility. Moreover, in most cases the reporting requirements outlined in the Interconnection Reliability Operating Limits and Preliminary Disturbance Report do not apply to the merchant generator that is not a generation only BA. The applicability of the standard does encompass the true merchant generation entities required to register as GOP. Similarly, the OE-417 table 1 reporting requirements generally do not apply to a true merchant generating entity that is required to register as a GOP.
Covanta	It would be a welcome enhancement to the end users to understand to communication link between all "appropriate parties" who shall be notified of potential or actual sabotage events.... which also needs to be defined.
Reliant Energy	EOOP-004-1 should exclude the generator operator from disturbance reporting except providing the system operator or reliability coordinator with appropriate unit operation information upon request. Acts of sabotage should be identified clearly and reported to the indicated authorities.
Texas Regional Entity	Add GO and TO to the list of applicability. The intent of CIP-001-1 when it was first written was to have the proper and most likely entities associated directly with operations to be the ones to begin the reporting process in the case of sabotage on the system. In the ERCOT Region and other regions in the US, the GOP may not be physically located at the site. The GOP is often removed from the minute-by-minute responsibilities of plant operations and, therefore, may be less able to react to physical sabotage at the location/plant/facility in a timely manner. The concern is that, in the case of an actual sabotage event, the failure to report to the appropriate authorities in a timely manner may jeopardize the reliability of the BPS. Therefore, the Generator Owner (GO) should be added to the list of applicability for CIP-001-1, because it is the GO that is more likely to be on location at the generation site and thus aware of sabotage when it first occurs. This would disallow for any possible communication gap and put responsibility on all of the appropriate entities to report such an event. Additionally, and for the same reasons as adding the GO, the Transmission Owner

Organization	Comment
	(TO) should also be added to the list of applicability for reporting sabotage on its facilities.
Exelon	CIP-001, remove LSE's from the standard for the reasons identified in the FERC LSE order. Ad TO and DP. EOP-004, remove LSE's from the standard for the reasons identified in the FERC LSE order. Remove RRO's, they are not a user, owner, operator of the BES. Add DP or TO. Consider conditional applicability as in the UFLS standards, " the TO or DP who performs the functions specified in the standard..."
ERCOT ISO	The Regional Reliability Organization is not a registered Functional Entity in the NERC registry. The applicability must be revised to more appropriately assign the requirements to registered functional entities. Also, the industry needs to recognize that there are other resources than generation for which the operators need to be included. Perhaps a demand-side resource should have a resource operator. This particular SAR may not be the appropriate venue for this, but control of resources which can be used to mitigate sabotage events or disturbance events may need to be addressed.
AEP	We would recommend that the Load Serving Entity (LSE) be removed from both standards, and that the Generator Owner and Transmission Owner be added to the resulting standard.
NextEra Energy Resources, LLC	The scope of the proposed SAR should not include the Generator Operator.
PSEG Enterprise Group Inc Companies	The PSEG Companies ask that the drafting team allow sufficient flexibility for sabotage recognition and reporting requirements such that nothing precludes utilizing a single corporate-wide program for both bulk electric system assets and other businesses. PSEG's Sabotage Recognition, Response and Reporting Program is directed to all business areas which are directed to follow the same internal protocol that also satisfies the NERC Standards requirements. For example, for gas assets, PSEG's gas distribution business follows the PSEG corporate-wide program for sabotage recognition and response. PSEG agrees that some modifications should be made to CIP-001 (ex. better define or give examples of sabotage) and EOP-004 to make them clearer? If they are merged, then Sabotage will not be in the title (or the primary focus) because several of the Disturbances that reporting is required for in EOP-004 have nothing to do with sabotage. EOP-004 has criteria listed in 4 places to determine when to send a report: o Criteria listed in EOP-004 Attachment 1 o Criteria listed in EOP-004 Attachment 2 o Criteria listed in top portion of Table 1-EOP-004 o Criteria listed in bottom potion of Table 1-EOP-004 Therefore, it would be much easier if there was one table of criteria for reference that addressed all of the reportable

Organization	Comment
	conditions and all of the applicable reports. If the 2 standards are merged as suggested in the SAR, any differences in the reporting obligation for actual or attempted sabotage and reporting of disturbances must be clear.
FirstEnergy	2. As pointed out by the NERC Audit and Observation Team in the "Issues to be considered" for CIP-001, clarification is needed regarding contacting the FBI. Prior audits dwelled heavily on FBI notification. For example, our policy states that Corporate Security notifies the FBI. In recent events it appears that local law enforcement handles day to day activities. The notification process for contacting the FBI needs clarification along with specific instances in which to call them. Who should make the call to the FBI? It appears that a protocol needs to be developed to clarify what events require notifying the FBI. It could be as simple as after an incident a standard form is completed and forwarded to the FBI, letting them decide if follow up is needed. 3. We suggest aligning all reporting requirements for consistency. The items requiring reporting and the timelines to report are very inconsistent between NERC and the DOE. NERC's timelines are also not consistent with their own Security Guideline for the Electricity Sector: Threat and Incident Reporting.
MRO NERC Standards Review Subcommittee	B. CIP-001-1 and EOP-004-1 should be combined into one EOP Standard. C. Within EOP-004-1 there is industry confusion on what form to submit in the event of an event. There should only be one form for the new combination Standard eliminating the need for reporting form attachments. It should be the DOE Form, OE-417. Although it is beyond the scope of this SAR, it would greatly benefit industry if there was a central location on the NERC website containing ALL reporting forms, including FERC, NERC, DOE, and ESIAC. This would enable the System Operators to efficiently locate the most current version of the appropriate form in order to report events.
Lands Energy Consulting	One final comment on CIP-001-1. My clients received universally rude treatment from the FBI field offices when they attempted to establish the contacts required by the Standard. If the FBI doesn't see value in establishing these contacts, remove the requirement from the Standard. Making sure the LSE knows the FBI field office phone number is probably all the Standard should require.
Colmac Clarion	Need single report for Sabotage so whatever is required results in notification of all parties (State Emergency Management, Homeland Security, FBI, Grid Reliability Chain of Command). Any and all of these can 'expand' knowledge later but all seem to require 'instant' notification.
Cowlitz County PUD	Local Law enforcement agencies often are not friendly to Federal involvement with smaller problems they consider their "turf." Need to make sure the small stuff stays with them, however have a system of internal reporting that will catch coordinated sabotage efforts (multiple attacks on DPs and small BAs) at the RC or RE level who then can report to the Federal agencies. Currently EOP-004-1 requires small entities to report a "disturbance" if half of their firm customer

Organization	Comment
	load is lost. For some entities, this can be one small substation going down due to a bird. The "50% of total demand" requirement should be removed or improved to better define a true BPS disturbance.
ERCOT ISO	Due to the fact that both the CIP-001-1 and EOP-004-1 have similar reporting standards, initially combining the two sounds like a correct analysis. However, after further consideration and due to the critical nature of its intended function involving Security aspects, the CIP-001 should be intensely evaluated to determine if its intended purpose meets the threshold or criteria to stand alone. The existing standards for CIP-001-1 Sabotage Reporting may help prevent future mitigation actions caused by sabotage events. EOP-004-1 Disturbance Reporting is administrative in nature, thus the jeopardy of the Bulk Electric System reliability is impacted only if analysis is not performed or if corrective follow-up actions are not implemented. Combining EOP-004 Standard requirements under the umbrella of the CIP -001 Standard would create a high profile Disturbance Reporting Standard. The industry would be better served if information defining sabotage was provided as well as a technical reference document on recognizing sabotage that would also clarify or state any personnel training requirements. All aspects of the intended functions must be reviewed before merging the two standards. At a minimum, we must consider modification that provides improved understanding of the reporting standards and implications as they are currently written.
MidAmerican Energy	Conflicting time frames exist from document updates. Reporting should be consolidated to one form and / or site to minimize conflicts, confusion, and errors. 1) Reporting requirements for the outage of 50,000 or more customers in EOP-004-1 requires a report to be made within one hour while the form OE-417 requires a report be made within six hours of the outage. The six hour reference on the updated OE-417 form is the correct reference. 2) Reporting for either CIP-001 or EOP-004 should center on the DOE Form OE-417. This would eliminate confusion and simplify reporting for system operators thereby directly enhancing reliability during system events. This would also eliminate much of the duplicate material and attachments in EOP-004. 3) Although it is beyond the scope of this SAR, the industry would benefit if there was a central location or link on the NERC website containing all reporting forms, including FERC, NERC, DOE, and ESIAC. This would enable System Operators to more efficiently locate and report events.
Illinois Municipal Electric Agency	IMEA recommends the following considerations: Simplification of reportable events and the reporting process should be the overriding objective. NERC's Security Guideline for the Electricity Sector: Threat and Incident Reporting (Version 2.0) should be updated to support this standards development initiative. At some point in the process, it may help if examples are given of events actually reported that did not need to be reported.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request Form

Title of Proposed Standard:	Disturbance and Sabotage reporting (Project 2009-01)
Request Date:	April 2, 2009
Approved by SC for posting:	April 15, 2009
Revision Date:	~~July 22, 2009~~August 13, 2009

SAR Requester Information	**SAR Type** (*Check a box for each one that applies.*)	
Name: Patrick Brown	☐	New Standard
Primary Contact: Patrick Brown Manager, NERC and Regional Coordination PJM Interconnection	☒	Revision to existing Standard
Telephone: 610-666-4597	☒	Withdrawal of existing Standard
E-mail: brownp@pjm.com	☐	Urgent Action

Purpose (Describe the proposed standard action: Nomination of a proposed standard, revision to a standard, or withdrawal of a standard and describe what the standard action will achieve.)

This project will entail revision to existing standards CIP-001-1 – Sabotage Reporting and EOP-

004-1 – Disturbance Reporting. The standards may be merged to eliminate redundancy and provide clarity on sabotage events. EOP-004 has some 'fill-in-the-blank' components to eliminate. The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

Industry Need (Provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

The existing requirements need to be revised to be more specific – and there needs to be more clarity in what sabotage looks like.

Brief Description (Provide a paragraph that describes the scope of this standard action.)

CIP-001 may be merged with EOP-004 to eliminate redundancies. Acts of sabotage have to be reported to the DOE as part of EOP-004. Specific references to the DOE form need to be eliminated.

EOP-004 has some 'fill-in-the-blank' components to eliminate.

The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards (see tables for each standard at the end of this SAR for more detailed information).
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR.) See "Issues to be Considered by Drafting Team" tables for each standard at the end of this SAR for more detailed information.

Reliability Functions

The Standard will Apply to the Following Functions *(Check box for each one that applies.)*		
☒	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☐	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☒	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles

Applicable Reliability Principles *(Check box for all that apply.)*	
☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☒	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles? *(Select 'yes' or 'no' from the drop-down box.)*
1. A reliability standard shall not give any market participant an unfair competitive advantage. Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes

Related Standards

Standard No.	Explanation
COM-003-1	Operations Communications Protocols – this standard may include some requirements that require coordination with the requirements addressed in this project. (still in standard development stage)
IRO-014-1	R1.1.1, footnote 1 lists sabotage. The standard drafting team should consider this reference and the impact of their work on this specific item.
TOP-005-1.1	Attachment 1, item 2.9 is "Multi-site sabotage". The standard drafting team should consider this reference and the impact of their work on this specific item.

Related SARs

SAR ID	Explanation

Regional Variances

Region	Explanation
ERCOT	
FRCC	
MRO	
NPCC	
SERC	
RFC	
SPP	
WECC	

Issues to be Considered by Drafting Team Project 2009-01 — Disturbance and Sabotage Reporting	
Standard #	**Title**
CIP-001-0	Sabotage Reporting

Issues

FERC Order 693

Disposition: Approved with modifications

- Consider the need for wider application of the standard. Consider whether separate, less burdensome requirements for smaller entities may be appropriate.
- Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event.
- In the interim, provide advice to entities about the reporting of particular circumstances as they arise.
- Consider FirstEnergy's suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality.
- Incorporate a periodic review or updating of the sabotage reporting procedures and for their periodic testing. Consider a staggered schedule of annual testing and formal review every two to three years.
- Include a requirement to report a sabotage event to the proper government authorities. Develop the language to specifically implement this directive.
- Explore ways to reduce redundant reporting, including central coordination of sabotage reports and a uniform reporting format.

V0 Industry Comments

- Object to multi-site requirement
- Definition of sabotage required

VRF comments

- Adequate procedures will insure it is unlikely to lead to bulk electric system instability, separation, or cascading failures.

Other

- Modify standard to conform to the latest version of NERC's Reliability Standards Development Procedure, the NERC Standard Drafting Team Guidelines, and the ERO Rules of Procedure.

NERC Audit and Observation Team

- Applicability — How does this standard pertain to Load Serving Entities, LSE's.
- Registered Entities have sabotage reporting processes and procedures in place but not all personnel has been trained.
- Question: How do you "and make the operator aware"
- R4 — "What is meant by: "establish contact with the FBI". Is a phone number adequate? Many entities which call the FBI are referred back to the local authority. The AOT noted that on the FBI website it states to

	contact the local authorities. Is this a question for Homeland Security to deal with for us?"
	• R4 — Establish communications contacts, as applicable with local FBI and RAMP officials. Some entities are very remote and the sheriff is the only local authority does the FBI still need to be contacted?
	FERC's December 20, 2007 and April 4, 2008 Orders in Docket Nos. RC07-004-000, RC07-6-000, and RC07-7-000
	• In FERC's December 20, 2007 Order, the Commission reversed NERC's Compliance Registry decisions with respect to three load serving entities in the ReliabilityFirst (RFC) footprint. The distinguishing feature of these three LSEs is that none owned physical assets. Both NERC and RFC assert that there will be a "reliability gap" if retail marketers are not registered as LSEs. To avoid a possible gap, a consistent, uniform approach to ensure that appropriate Reliability Standards and associated requirements are applied to retail marketers must be applied. Each drafting team responsible for reliability standards applicable to LSEs is to review and change as necessary, requirements in the applicable reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. For additional information see:
	  • FERC's December 20, 2007 Order (http://www.nerc.com/files/LSE_decision_order.pdf)
	  • NERC's March 4, 2008 (http://www.nerc.com/files/FinalFiledLSE3408.pdf),
	  • FERC's April 4, 2008 Order (http://www.nerc.com/files/AcceptLSECompFiling-040408.pdf) and
	  • NERC's July 31, 2008 (http://www.nerc.com/files/FinalFiled-CompFiling-LSE-07312008.pdf) compliance filings to FERC on this subject.

Issues to be Considered by Drafting Team Project 2009-01 — Disturbance and Sabotage Reporting	
Standard #	**Title**
EOP-004-1	Disturbance Reporting
Issues	FERC Order 693 Disposition: Approved with modification • Include any requirements for users, owners, and operators of the bulk power system to provide data that will assist NERC in the investigation of a blackout or disturbance. • Change NERC's Rules of Procedure to assure the Commission receives these reports in the same frame as the DOE. • Consider APPA's concern about generator operators and LSEs analyzing performance of their equipment and provide data and information on the equipment to assist others with analysis. • Consider all comments offered in a future modification of the reliability standard.

	Fill-in-the-Blank Team Comments
	• Consider changes to R1 and R3.4 to standardize the disturbance reporting requirements (requirements for disturbance reporting need to be added to this standard)
	• Regions currently have procedures, but not in the form of a standard. The drafting team will need to review regional requirements to determine reporting requirements for the North American standard.
	V0 Industry Comments
	• R3 – too many reports, narrow requirement to RC
	• How does this apply to generator operator?
	Other
	• Modify standard to conform to the latest version of NERC's Reliability Standards Development Procedure, the NERC Standard Drafting Team Guidelines, and the ERO Rules of Procedure.
	NERC Audit and Observation Team
	• R3.1 — Can there be a violation without an event?
	Event Analysis Team
	• Reliability Issue: Coordination and follow up on lessons learned from event analyses Consider adding to EOP-004 – Disturbance Reporting. Proposed requirement: Regional Entities (REs) shall work together with Reliability Coordinators, Transmission Owners, and Generation Owners to develop an Event Analysis Process to prevent similar events from happening and follow up with the recommendations. This process shall be defined within the appropriate NERC Standard.
	FERC's December 20, 2007 and April 4, 2008 Orders in Docket Nos. RC07-004-000, RC07-6-000, and RC07-7-000
	• In FERC's December 20, 2007 Order, the Commission reversed NERC's Compliance Registry decisions with respect to three load serving entities in the ReliabilityFirst (RFC) footprint. The distinguishing feature of these three LSEs is that none owned physical assets. Both NERC and RFC assert that there will be a "reliability gap" if retail marketers are not registered as LSEs. To avoid a possible gap, a consistent, uniform approach to ensure that appropriate Reliability Standards and associated requirements are applied to retail marketers must be applied. Each drafting team responsible for reliability standards applicable to LSEs is to review and change as necessary, requirements in the applicable reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. For additional information see:
	  • FERC's December 20, 2007 Order (http://www.nerc.com/files/LSE_decision_order.pdf)
	  • NERC's March 4, 2008 (http://www.nerc.com/files/FinalFiledLSE3408.pdf),
	  • FERC's April 4, 2008 Order (http://www.nerc.com/files/AcceptLSECompFiling-040408.pdf) and
	  • NERC's July 31, 2008 (http://www.nerc.com/files/FinalFiled-CompFiling-LSE-07312008.pdf) compliance filings to FERC on this subject.

Comments received on Project 2009-01 — Disturbance and Sabotage Reporting

The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) received many suggestions for improvements to the standards during the SAR comment period. These comments do not indicate any revisions to the SAR, but the DSRSDT thought that these comments merited further consideration during the standard drafting phase of the project. The comments below are being compiled for use by the Standard Development Team.

Organization	Comment
Electric Market Policy	Comments: Agree with the statement that sabotage is hard to determine in real time by operations staffs. The determination of sabotage should be left up to law enforcement. They have the knowledge and peer contacts needed to adequately determine whether physical or cyber intrusions are merely malicious acts or coordinated efforts (sabotage). The operators should only be required to report physical and cyber intrusions to law enforcement. All other reporting requirements should apply to law enforcement once a determination of sabotage has been made. If the recommendations above are not to be accepted, then we have the following comments: CIP-001-1 1) R1 states entities shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SAR notes that the industry objects to the multi-site requirement, most likely because the term is ambiguous. If this term remains in the standard, it needs to be clearly defined and responsibilities for obtaining (how do you get this information and from whom?) and distributing need to be included. 2) R1 audits have shown confusion over the requirement to make operating personnel aware of sabotage events. The term operating personnel needs to be defined. Are they the individuals responsible for operating the facility, coordinating with other entities (i.e., RC, BA, TOP, GOP, and LSE)? It has been suggested that notification is required to all personnel at a facility. Keep in mind the purpose of the standard is to ensure sabotage events are properly reported, not to address emergency response. 3) R1 The SAR (NERC Audit and Observation Team) notes that Registered Entities have processes and procedures in place, but not all personnel have been trained. There is no specific training requirement in the standard. 4) R2 & R3 I agree with the SAR that sabotage needs to be defined and these requirements should be more specific with respect to the information to be communicated. It seems to me that the standard should mirror the criteria contained in DOE OE-417. The emphasis should be placed on ensuring that the same information communicated to DOE is shared with the appropriate parties in the Interconnection. 5) R4 I agree with the SAR (NERC Audit and Observation Team) comments regarding the intention of this requirement. There is no language that directs contact with FBI or RCMP although that is what is implied by the Purpose statement.

Organization	Comment
	6) VRF Comments I'm not sure what is intended by the statement Adequate procedures will insure it is unlikely to lead to bulk electric system instability, separation, or cascading failures? The purpose of the standard is that of communication. No operational decisions or actions are directed by this standard, nor does it require entities to address operational aspects resulting from sabotage. 7) The potential exists for overlapping sabotage reporting requirements at nuclear power plants due to multiple regulators (Nuclear Regulatory Commission (NRC) 10 CFR 73 and Federal Energy Regulatory Commission (FERC) NUC-001-1). Some entities may have revised existing NRC driven procedures to accommodate reporting requirements of both regulators. Because of the restrictions placed on NRC driven documents (i.e., procedures are classified as safeguards information), it can be difficult to demonstrate compliance to NERC and/or FERC without ensuring that the individuals are qualified for receipt of such information per 10 CFR 73. Additionally, multiple procedures may have the unintended consequence of delaying appropriate communication.EOP-004-1Consider removing Attachment 2 as the information is duplicated in DOE Form OE-417. A simple reference to the form should suffice.
Lands Energy Consulting	I have worked with 5 Northwest public utilities on developing procedures related to CIP-001-1 and EOP-004-1. All 5 utilities operate electric systems in fairly remote locations and are embedded in a larger utility's Balancing Authority/Transmission Operator area. A. CIP-001-1 - Developing procedures to unambiguously identify acts of sabotage has been particularly challenging for these systems. In general, it's hard for them to determine whether the most prevalent forms of malicious and intentional system damage that they incur - copper theft and gun shot insulators/equipment - should qualify as acts of sabotage. Although none of the systems consider copper theft to be acts of sabotage, two of the systems consider gun shot insulators/equipment to be acts of sabotage. The other systems look for intent to disrupt electric system operations as a key component of their sabotage identification procedures. Additional guidance from NERC in the form of CIP-001-1 modifications or a companion guidelines document on sabotage identification would provide much needed guidance for these procedures. B. EOP-004-1 - This standard was clearly drafted with the larger electric systems in mind. I have one client that serves 3300 commercial/residential customers from 4-115/13 kV substation transformers and one large industrial customer (80% of its energy load) from a 230/13 kV substation. 75% of the client's load is served from three substations attached to a long, 115 kV transmission line operated by the Bonneville Power Administration. Whenever the line relays open on a permanent fault (which happens 2-3 times per year), the client loses over 50% of its customers (but no more than 10-15 MW during winter peak), thereby necessitating the preparation of a Disturbance Report. To allow utilities to concentrate on operating their systems, without fear of violating EOP-004-1 for failure to report trivial outages, I would remove LSEs from the obligation to report disturbances - leave the reporting to the BA/TOP for large outages in their footprint.
Calpine Corporation	Communication of facility status or emergencies between merchant generators registered as GOP and the RC, BA, GOP, or LSE in which the facility resides should be coordinated for EOP -004 reporting. The reporting to NERC/DOE should

Organization	Comment
	come from the RC, BA, GOP, or LSE.
Covanta	Yes - the key to Sabotage reporting requirements is identifying what the 'definition' is of an actual or potential 'Sabotage' event. Like any other standard, if FERC/NERC leave it up to 2000+ entities to establish their own definitions of 'Sabotage', you may likely get 2000+ answers. That is not a controlled and coordinated approach. I offer the following definition, "Sabotage - Deliberate or malicious destruction of property, obstruction of normal operations, or injury to personnel by outside agents." Examples of sabotage events could include, but are not limited to, suspicious packages left near site electrical generating or electrical transmission assets, identified destruction of generating assets, telephone/e mail received threats to destroy or interrupt electrical generating efforts, etc." These have passed multiple NERC regional audits and reviews to date.
Northeast Power Coordinating Council	The SAR needs to be more specific in defining its objectives. CIP-001Requirement R1 currently states: R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SDT needs to include the following objectives: 1. Develop clear definitions for the terms “operating personnel” and “sabotage events.” The definition of “operating personnel,” should be clarified and limited to staff at BES facilities. Operating personnel should report only those events which meet a clear, recognizable threshold as reportable potential sabotage events. There should be a consistent continent-wide list of examples or typical reportable and non-reportable events to help guide operating personnel. The term “sabotage event” needs to be defined. Clarification is required regarding when the determination of a sabotage event is made, e.g., upon first observation (requiring operating personnel be educated in discerning sabotage events), or upon later investigation by trained security personnel and law enforcement individuals. The terms potential or suspected sabotage event for reporting purposes should be clarified or defined. 2. Define the obligations of Registered Entity operating personnel - who are required to be aware of such “sabotage events,” e.g., who, what, where, when, why and how, and what they are to do in response to this awareness. The SDT should clarify the use of the term “aware” in the standard. “Aware” can be interpreted in accordance with its largely passive, dictionary-based meaning, where being “aware” simply means knowing about something, such as a sabotage event. Alternatively, the Reliability Standard meaning of “aware” could refer to more active wording, involving more than mere awareness, e.g., “alert and quick to respond,” pointing to and requiring a specific affirmative response, i.e., reporting to the appropriate systems, governmental agencies, and regulatory bodies. EOP-004 - The SDT needs to work on the following areas.

Organization	Comment
	1. NERC reporting needs to be clarified. For example, Attachment 1 paragraph 6c states: Introduction "The entity on whose system a reportable disturbance occurs shall notify NERC ... 6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in: c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance - The sense of Attachment 1 is internally inconsistent between the introduction ("occurs") and the required actions in 6c (could have resulted in a system disturbance). The initial intent appears to be only to report actual system disturbances. Yet, paragraph 6c adds the phrase "or could have resulted in" a potential system disturbance. This inconsistency should be clarified.
FirstEnergy	We agree with the scope but would also like to see the following considered: 1. References to the DOE reporting process in EOP-004 need to be revised. They currently refer to the old EIA form. 2. Besides "sabotage", it may be helpful to clearly define "vandalism". It is vaguely written in the standards. Also, the process of "public appeals" for the DOE reportable requirements needs to be more clearly defined. 3. Consolidate documents covering reporting requirements. There are currently several documents that require reporting (EOP-004, CIP-001, DOE oe-417, and NERC's Security Guideline for the Electricity Sector: Threat and Incident Reporting). NERC also has the "Bulk Power System Disturbance Classification Scale" that does not completely align with all the reporting requirements. Therefore we recommend keeping this as simple as possible by combining all the reporting requirements into one standard. It would be beneficial to not require operators to have to go to 4 different documents to determine what to report on.
MRO NERC Standards Review Subcommittee	The MRO NSRS would like to keep the references to the DOE reporting form.
Cowlitz County PUD	Added to the scope: For EOP-004 add a provision for a reporting flow rather than everything going to the RE and NERC. That is something going like the DP and TOP reports to the BA, the BA to the RE, and the RE to NERC. This would allow for multiple related reports to be combined into a single coherent report as the reporting goes up the chain. For CIP-001 consider reporting flow as above with local law enforcement notification. Let an upper entity in the reporting chain decide when to contact Federal Agencies such as the BA or the RC.
Reliant Energy	I think Generator operators should be excluded except to provide requested information from the System Operator or Reliability coordinator.

Organization	Comment
ERCOT ISO	The scope should be modified to provide for a different treatment of reporting requirements that are administrative in nature, or that are after-the-fact (thus cannot impact reliability unless analysis and follow-up is not performed; even then, the impact would be at some future time). Reporting requirements which are of the nature to assist in identification of system concerns or which serve to prevent or mitigate on-going system problems (including, but not limited to, actual or attempted sabotage activity) should remain in standards, but should be separate and apart from the administrative reporting.
Consolidated Edison Co. of New York, Inc.	GENERAL CECONY and ORU support the general objectives of the SAR to merge existing standards CIP-001-1 Sabotage Reporting and EOP-004-1 Disturbance Reporting to improve clarity and remove redundancy. However, the SAR needs to be more specific in defining its objectives. CIP-001Requirement R1 currently states: R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SDT needs to include the following objectives: 1. Develop clear definitions for the terms operating personnel and sabotage events. The definition of operating personnel, should be clarified and limited to staff at BES facilities. Operating personnel should report only those events which meet a clear, recognizable threshold as reportable potential sabotage events. There should be a consistent continent-wide list of examples or typical reportable and non-reportable events to help guide operating personnel. The term sabotage event needs to be defined. Clarification is required regarding when the determination of a sabotage event is made, e.g., upon first observation (requiring operating personnel be educated in discerning sabotage events), or upon later investigation by trained security personnel and law enforcement individuals. The terms potential or suspected sabotage event for reporting purposes should be clarified or defined. 2. Define the obligations of Registered Entity operating personnel - who are required to be aware of such sabotage events, e.g., who, what, where, when, why and how, and what they are to do in response to this awareness. The SDT should clarify the use of the term aware in the standard. Aware can be interpreted in accordance with its largely passive, dictionary-based meaning, where being aware simply means knowing about something, such as a sabotage event. Alternatively, the Reliability Standard meaning of aware could refer to more active wording, involving more than mere awareness, e.g., alert and quick to respond, pointing to and requiring a specific affirmative response, i.e., reporting to the appropriate systems, governmental agencies, and regulatory bodies. EOP-004 - The SDT needs to work on the following areas. 1. NERC reporting needs to be clarified. For example, Attachment 1 paragraph 6c states:

Organization	Comment
	Introduction The entity on whose system a reportable disturbance occurs shall notify NERC ... 6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in: ?c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance. The sense of Attachment 1 is internally inconsistent between the introduction (occurs) and the required actions in 6c (could have resulted in a system disturbance). The initial intent appears to be only to report actual system disturbances. Yet, paragraph 6c adds the phrase or could have resulted in a potential system disturbance. This inconsistency should be clarified.
Georgia System Operations Corp.	The scope of the SAR should be to move all requirements to report to NERC or Regional Entities out of the Requirements section of all Reliability Standards to elsewhere. This does not include reporting, communicating, or coordinating between reliability entities. The NERC/Region reporting requirements could be consolidated in another document and referenced in the Supporting References section of the Reliability Standards. The deadlines for reporting should be changed to realistic timeframes that do not interfere with operating the BES or responding to incidents yet still allow NERC and the Regions to accomplish their missions.
AEP	Sabotage is a term of intent that is often determined after the fact by the registered entity and/or law enforcement officials. In fact, it is often difficult to determine in real-time the intent of a suspicious event. We would suggest that suspicious events become reportable at the point that the event is determined to have had sabotage intent. The entities should have a methodology to collect evidence, to have the evidence analyzed, and to report those events that are determined to have had the intent of sabotage.
Duke Energy	While we agree with the need for clarity in sabotage and disturbance reporting, we believe that the Standards Drafting Team should carefully consider whether there is a reliability-related need for each requirement. Some disturbance reporting requirements are triggered not just to assist in real-time reliability but also to identify lessons-learned opportunities. If disturbance and sabotage reporting continue to be reliability standards, we believe that all linkages to lessons-learned/improvements need to be stripped out. We have other forums to identify lessons-learned opportunities and to follow-up on those opportunities. Also, requirements to report possible non-compliances should be eliminated. We strongly support voluntary self-reporting, but not mandatory self-reporting.
NextEra Energy Resources, LLC	The scope of the SAR should not include Generator Operators.
Luminant Power	The SAR drafting team should include in the SAR scope a review of the NRC sabotage and event reporting requirements to ensure there are no overlapping or conflicting requirements between NERC, FERC, and the NRC. The SAR scope

Organization	Comment
	should include a review of the CIP Cyber Security Standards and coordination with the CIP SDT to ensure that cyber sabotage reporting definitions are in concert, and ensure that cyber sabotage reporting requirements are not duplicated in multiple standards.
Illinois Municipal Electric Agency	A one-stop reporting tool/site would facilitate efficient reporting and compliance; e.g., further development of the ES-ISAC/CIPIS to include all reportable categories and automatic notification of required parties. A single report form would be best.
AEP	The current reporting process necessitates multiple reports be sent to multiple parties, which is inefficient and may, inadvertently, result in alignment issues between the separate reports. We would recommend that a single report that combines NERC (CIPIS) and NERC ESISAC information be provided to NERC (CIPIS) that is systematically (programmatically) forwarded to all necessary entities. Further, updates to incidents would also go through NERC with the same electronic processing. Currently, we are not aware of a formal method to report incidents to the FBI, which should be also included in the distribution. The current reporting mechanism to the FBI JTTF is by telephone and the NERC platform described would provide more consistent reporting.
Kansas City Power & Light	Do not agree Load Serving Entities need to continue to be included for sabotage. According the NERC Functional Model, an LSE provides for estimating customer load and provides for the acquisition of transmission and energy to meet customer load demand. An LSE has no real impact on maintaining the reliability of electric network short of their planning function. Unfortunately, an LSE needs to be included for disturbance reporting to the DOE under certain conditions for loss of customer load. This may be a reason to maintain a separation of CIP-001 and EOP-004 so as not to unnecessarily include an LSE when it is not needed.
Electric Market Policy	Applicability should not apply to LSE unless they have physical assets. If they do not have such assets, they are unable to determine how many customers are out, how much load was lost or the duration of an outage. We continue to question the need for the LSE entity in reliability standards. End use customer load is either connected to transmission or distribution facilities. So, the applicable planner has to plan for that load when designing its facilities or the load will not have reliable service. To the extent that energy and capacity for that load is supplied by an entity other than the TO or DP, the TO or DP should have interconnection requirements that compel the supplier to provide any and all data necessary to meet the requirements of reliability standards.
Lands Energy Consulting	CIP-001-1 - Yes. In many cases, the staff of an LSE embedded in another entity's BA/TOP area is more likely to discover an act of sabotage directed toward a BA/TOP-owned facility that could affect the BES than the asset owner. This is because the LSE likely has more operating staff in the area. I have included a requirement in my clients' Sabotage Identification and Reporting Procedures that the client treat acts of sabotage to a third party's system discovered by client employees as though the act was directed toward client facilities. EOP-004-1 - As mentioned before, I would eliminate the

Organization	Comment
	LSE from the applicability list and leave the responsibility for disturbance reporting and response to the TOP/BA. However, I would retain a responsibility for the LSEs to cooperate (when requested) with any disturbance investigation.
Calpine Corporation	The reporting requirements of EOP - 004 are needed for the RC, BA, LSE and the GOP that operates or controls generation in a system as defined by NERC. (System - A combination of generation, transmission, and distribution components). A disturbance is described as an unplanned event that produces and abnormal system condition, any perturbation to the electric system, and the unexpected change in ACE that is caused by the sudden failure of generation or interruption of load. The GOP operating/controlling generation within a system has the ability to analyze system conditions to determine if reporting is necessary. A NERC registered GOP that is a merchant generator within another company's system does not have the ability for a wide area view and cannot analyze system conditions beyond the interconnection point of the facility. Moreover, in most cases the reporting requirements outlined in the Interconnection Reliability Operating Limits and Preliminary Disturbance Report do not apply to the merchant generator that is not a generation only BA. The applicability of the standard does encompass the true merchant generation entities required to register as GOP. Similarly, the OE-417 table 1 reporting requirements generally do not apply to a true merchant generating entity that is required to register as a GOP.
Covanta	It would be a welcome enhancement to the end users to understand to communication link between all "appropriate parties" who shall be notified of potential or actual sabotage events.... which also needs to be defined.
Reliant Energy	EOOP-004-1 should exclude the generator operator from disturbance reporting except providing the system operator or reliability coordinator with appropriate unit operation information upon request. Acts of sabotage should be identified clearly and reported to the indicated authorities.
Texas Regional Entity	Add GO and TO to the list of applicability. The intent of CIP-001-1 when it was first written was to have the proper and most likely entities associated directly with operations to be the ones to begin the reporting process in the case of sabotage on the system. In the ERCOT Region and other regions in the US, the GOP may not be physically located at the site. The GOP is often removed from the minute-by-minute responsibilities of plant operations and, therefore, may be less able to react to physical sabotage at the location/plant/facility in a timely manner. The concern is that, in the case of an actual sabotage event, the failure to report to the appropriate authorities in a timely manner may jeopardize the reliability of the BPS. Therefore, the Generator Owner (GO) should be added to the list of applicability for CIP-001-1, because it is the GO that is more likely to be on location at the generation site and thus aware of sabotage when it first occurs. This would disallow for any possible communication gap and put responsibility on all of the appropriate entities to report such an event. Additionally, and for the same reasons as adding the GO, the Transmission Owner (TO) should also be added to the list of applicability for reporting sabotage on its facilities.
Exelon	CIP-001, remove LSE's from the standard for the reasons identified in the FERC LSE order. Ad TO and DP. EOP-004,

Organization	Comment
	remove LSE's from the standard for the reasons identified in the FERC LSE order. Remove RRO's, they are not a user, owner, operator of the BES. Add DP or TO. Consider conditional applicability as in the UFLS standards, " the TO or DP who performs the functions specified in the standard..."
ERCOT ISO	The Regional Reliability Organization is not a registered Functional Entity in the NERC registry. The applicability must be revised to more appropriately assign the requirements to registered functional entities. Also, the industry needs to recognize that there are other resources than generation for which the operators need to be included. Perhaps a demand-side resource should have a resource operator. This particular SAR may not be the appropriate venue for this, but control of resources which can be used to mitigate sabotage events or disturbance events may need to be addressed.
AEP	We would recommend that the Load Serving Entity (LSE) be removed from both standards, and that the Generator Owner and Transmission Owner be added to the resulting standard.
NextEra Energy Resources, LLC	The scope of the proposed SAR should not include the Generator Operator.
PSEG Enterprise Group Inc Companies	The PSEG Companies ask that the drafting team allow sufficient flexibility for sabotage recognition and reporting requirements such that nothing precludes utilizing a single corporate-wide program for both bulk electric system assets and other businesses. PSEG's Sabotage Recognition, Response and Reporting Program is directed to all business areas which are directed to follow the same internal protocol that also satisfies the NERC Standards requirements. For example, for gas assets, PSEG's gas distribution business follows the PSEG corporate-wide program for sabotage recognition and response. PSEG agrees that some modifications should be made to CIP-001 (ex. better define or give examples of sabotage) and EOP-004 to make them clearer? If they are merged, then Sabotage will not be in the title (or the primary focus) because several of the Disturbances that reporting is required for in EOP-004 have nothing to do with sabotage. EOP-004 has criteria listed in 4 places to determine when to send a report: o Criteria listed in EOP-004 Attachment 1 o Criteria listed in EOP-004 Attachment 2 o Criteria listed in top portion of Table 1-EOP-004 o Criteria listed in bottom potion of Table 1-EOP-004 Therefore, it would be much easier if there was one table of criteria for reference that addressed all of the reportable conditions and all of the applicable reports. If the 2 standards are merged as suggested in the SAR, any differences in the reporting obligation for actual or attempted sabotage and reporting of disturbances must be clear.

Organization	Comment
FirstEnergy	2. As pointed out by the NERC Audit and Observation Team in the "Issues to be considered" for CIP-001, clarification is needed regarding contacting the FBI. Prior audits dwelled heavily on FBI notification. For example, our policy states that Corporate Security notifies the FBI. In recent events it appears that local law enforcement handles day to day activities. The notification process for contacting the FBI needs clarification along with specific instances in which to call them. Who should make the call to the FBI? It appears that a protocol needs to be developed to clarify what events require notifying the FBI. It could be as simple as after an incident a standard form is completed and forwarded to the FBI, letting them decide if follow up is needed. 3. We suggest aligning all reporting requirements for consistency. The items requiring reporting and the timelines to report are very inconsistent between NERC and the DOE. NERC's timelines are also not consistent with their own Security Guideline for the Electricity Sector: Threat and Incident Reporting.
MRO NERC Standards Review Subcommittee	B. CIP-001-1 and EOP-004-1 should be combined into one EOP Standard. C. Within EOP-004-1 there is industry confusion on what form to submit in the event of an event. There should only be one form for the new combination Standard eliminating the need for reporting form attachments. It should be the DOE Form, OE-417. Although it is beyond the scope of this SAR, it would greatly benefit industry if there was a central location on the NERC website containing ALL reporting forms, including FERC, NERC, DOE, and ESIAC. This would enable the System Operators to efficiently locate the most current version of the appropriate form in order to report events.
Lands Energy Consulting	One final comment on CIP-001-1. My clients received universally rude treatment from the FBI field offices when they attempted to establish the contacts required by the Standard. If the FBI doesn't see value in establishing these contacts, remove the requirement from the Standard. Making sure the LSE knows the FBI field office phone number is probably all the Standard should require.
Colmac Clarion	Need single report for Sabotage so whatever is required results in notification of all parties (State Emergency Management, Homeland Security, FBI, Grid Reliability Chain of Command). Any and all of these can 'expand' knowledge later but all seem to require 'instant' notification.
Cowlitz County PUD	Local Law enforcement agencies often are not friendly to Federal involvement with smaller problems they consider their "turf." Need to make sure the small stuff stays with them, however have a system of internal reporting that will catch coordinated sabotage efforts (multiple attacks on DPs and small BAs) at the RC or RE level who then can report to the Federal agencies. Currently EOP-004-1 requires small entities to report a "disturbance" if half of their firm customer load is lost. For some entities, this can be one small substation going down due to a bird. The "50% of total demand" requirement should be removed or improved to better define a true BPS disturbance.

Organization	Comment
ERCOT ISO	Due to the fact that both the CIP-001-1 and EOP-004-1 have similar reporting standards, initially combining the two sounds like a correct analysis. However, after further consideration and due to the critical nature of its intended function involving Security aspects, the CIP-001 should be intensely evaluated to determine if its intended purpose meets the threshold or criteria to stand alone. The existing standards for CIP-001-1 Sabotage Reporting may help prevent future mitigation actions caused by sabotage events. EOP-004-1 Disturbance Reporting is administrative in nature, thus the jeopardy of the Bulk Electric System reliability is impacted only if analysis is not performed or if corrective follow-up actions are not implemented. Combining EOP-004 Standard requirements under the umbrella of the CIP -001 Standard would create a high profile Disturbance Reporting Standard. The industry would be better served if information defining sabotage was provided as well as a technical reference document on recognizing sabotage that would also clarify or state any personnel training requirements. All aspects of the intended functions must be reviewed before merging the two standards. At a minimum, we must consider modification that provides improved understanding of the reporting standards and implications as they are currently written.
MidAmerican Energy	Conflicting time frames exist from document updates. Reporting should be consolidated to one form and / or site to minimize conflicts, confusion, and errors. 1) Reporting requirements for the outage of 50,000 or more customers in EOP-004-1 requires a report to be made within one hour while the form OE-417 requires a report be made within six hours of the outage. The six hour reference on the updated OE-417 form is the correct reference. 2) Reporting for either CIP-001 or EOP-004 should center on the DOE Form OE-417. This would eliminate confusion and simplify reporting for system operators thereby directly enhancing reliability during system events. This would also eliminate much of the duplicate material and attachments in EOP-004. 3) Although it is beyond the scope of this SAR, the industry would benefit if there was a central location or link on the NERC website containing all reporting forms, including FERC, NERC, DOE, and ESIAC. This would enable System Operators to more efficiently locate and report events.
Illinois Municipal Electric Agency	IMEA recommends the following considerations: Simplification of reportable events and the reporting process should be the overriding objective. NERC's Security Guideline for the Electricity Sector: Threat and Incident Reporting (Version 2.0) should be updated to support this standards development initiative. At some point in the process, it may help if examples are given of events actually reported that did not need to be reported.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form for Standard Drafting Team for Disturbance and Sabotage Reporting (Project 2009-01)

Please **DO NOT** use this form. Please use the electronic nomination form located at the link below. If you have any questions, please contact Stephen Crutchfield at stephen.crutchfield@nerc.net or by telephone at 609-651-9455.

http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

By submitting the following information you are indicating your commitment to actively participate (including physically attending face-to-face) Standard Drafting Team meetings if appointed to the Standard Drafting Team by the Standards Committee.

Name:	
Organization:	
Address:	
Telephone:	
E-mail:	

Project 2009-01 Disturbance and Sabotage Reporting will entail revising existing standards CIP-001 — Sabotage Reporting and EOP-004 — Disturbance Reporting to eliminate redundancies and provide clarity on sabotage events. The project includes addressing several issues identified by stakeholders, FERC directives from Order 693, and may include improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

Please briefly describe (no more than a couple of paragraphs) your experience and qualifications directly related to the issues to be addressed by the Disturbance and Sabotage Reporting Standard Drafting Team. We are seeking a cross section of the industry to participate on the team, but in particular are seeking individuals with experience in management of real-time bulk power operations activities. Please include any previous experience related to developing or applying IEEE or other industry related standards as this type of experience might be beneficial to include on the team, but is not a requisite to be appointed to the team.

Are you currently a member of any NERC or Regional Entity SAR or standard drafting team? If yes, please list each	☐ No ☐ Yes:

team here.	
Have you previously worked on any NERC or Regional Entity SAR or standard drafting teams? If yes, please list them here.	☐ No ☐ Yes:

Please identify the NERC Region(s) for which you are able to represent your company's position relative to the topics addressed in the SAR:		Please identify the Industry Segment(s) for which you are able to represent your company's position relative to the topics addressed in the SAR:
☐ ERCOT	☐	1 — Transmission Owners
☐ FRCC	☐	2 — RTOs and ISOs
☐ MRO	☐	3 — Load-serving Entities
☐ NPCC	☐	4 — Transmission-dependent Utilities
☐ RFC	☐	5 — Electric Generators
☐ SERC	☐	6 — Electricity Brokers, Aggregators, and Marketers
☐ SPP	☐	7 — Large Electricity End Users
☐ WECC	☐	8 — Small Electricity End Users
☐ Not Applicable or None of the Above	☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
	☐	10 — Regional Reliability Organizations and Regional Entities
	☐	Not applicable

Please identify the Functional Entities[1] for which you are able to represent your company's position relative to the topics addressed in the SAR:

☐ Balancing Authority	☐ Planning Coordinator
☐ Compliance Enforcement Authority	☐ Transmission Operator
☐ Distribution Provider	☐ Transmission Owner
☐ Generator Operator	☐ Transmission Planner
☐ Generator Owner	☐ Transmission Service Provider
☐ Interchange Authority	☐ Purchasing-selling Entity
☐ Load-serving Entity	☐ Resource Planner
☐ Market Operator	☐ Reliability Coordinator

[1] These functions are defined in the NERC Functional Model, which is available on the NERC Web site.

Please provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group. NERC staff may contact these references.			
Name and Title:		Office Telephone:	
Organization:		E-mail:	
Name and Title:		Office Telephone:	
Organization:		E-mail:	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Nomination Period Opens for Standard Drafting Team
September 16-30, 2009

Now available at: http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Project 2009-01: Disturbance and Sabotage Reporting

The Standards Committee is seeking industry experts to serve on the Disturbance and Sabotage Reporting Standard Drafting Team. The nomination period is open **until September 30, 2009.**

Instructions

If you are interested in serving on this standard drafting team, please complete the following electronic nomination form**:** https://www.nerc.net/nercsurvey/Survey.aspx?s=ba96a1dc8506404889e26d05aaf490c6 . Please contact Dave Taylor at david.taylor@nerc.net or 609-651-5089 with any questions about the team.

Project Background

Project 2009-01 — Disturbance and Sabotage Reporting will entail revising existing standards CIP-001-1 — Sabotage Reporting and EOP-004-1 — Disturbance Reporting to eliminate redundancies and provide clarity on sabotage events. The project includes addressing several issues identified by stakeholders, FERC directives from Order 693, and may include improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

More information about the project is available on the following page:
http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01)
Reporting Concepts

Introduction

The SAR for Project 2009-01 Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and is progressing toward developing standards based on the SAR. This concepts paper is designed to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed.

The standards listed under the SAR are:

- CIP-001 — Sabotage Reporting
- EOP-004 — Disturbance Reporting

The DSR SDT is also proposing to investigate incorporation of the cyber incident reporting aspects of CIP-008 under this project. This will be coordinated with the Cyber Security — Order 706 Standard Drafting Team (Project 2008-06).

The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC database and FERC Order 693 Directives to determine a prudent course of action with respect to these standards.

This concept paper provides stakeholders with a proposed "road map" that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. This concept paper provides the background information and thought process of the DSR SDT.

The proposed changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. TOP). The proposed standards deal exclusively with after-the-fact reporting.

The DSR SDT is proposing to consolidate disturbance and event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts and Assumptions:

The Standard Will: Require use of a single form to report disturbances and "impact events" that threaten the reliability of the bulk electric system

- Provide clear criteria for reporting
- Include consistent reporting timelines
- Identify appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- Provide clarity around of who will receive the information

The drafting team will explore other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements

Discussion of Disturbance Reporting

Disturbance reporting requirements currently exist in EOP-004. The current approved definition of Disturbance from the NERC Glossary of Terms is:

1. An unplanned event that produces an abnormal system condition.
2. Any perturbation to the electric system.
3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.

Disturbance reporting requirements and criteria are in the existing EOP-004 standard and its attachments. The DST SDT discussed the reliability needs for disturbance reporting and will consider guidance found in the document "NERC Guideline: Threat and Incident Reporting" in the development of requirements, which will include clear criteria for reporting. The new/revised standard will specify who has access to reported information about disturbances.

The DSR SDT is considering developing a reporting hierarchy that requires the Reliability Coordinator (RC) to submit the disturbance report. Any entity (Distribution Provider, Load-Serving Entity, Generator Operator) that experiences a disturbance would report the appropriate information to the Transmission Operator or Balancing Authority (if applicable) who would then report to the RC. The RC would then submit the report to NERC, the affected Regional Entity (RE) and/or Department of Energy (DOE) as appropriate. By having the RC submit the report, situational awareness would be enhanced. All affected entities would be aware of the disturbance and relevant information. Also, the flow of information between entities would be enhanced and a more comprehensive report could be developed.

Discussion of "Impact Event" Reporting

There are situations worthy of reporting because they have the potential to impact reliability. The DSR SDT proposes calling such incidents 'impact events' with the following definition:

> An impact event is any situation that has the potential to significantly impact the reliability of the Bulk Electric System. Such events may originate from malicious intent, accidental behavior, or natural occurrences.

Impact event reporting facilitates situational awareness, which allows potentially impacted parties to prepare for and possibly mitigate the reliability risk. It also provides the raw material, in the case of certain potential reliability threats, to see emerging patterns.

Examples of impact events include:

- Bolts removed from transmission line structures
- Detection of cyber intrusion that meets criteria of CIP-008
- Forced intrusion attempt at a substation
- Train derailment near a transmission right-of-way
- Destruction of Bulk Electrical System equipment

What about sabotage?
One thing became clear in the DSR SDT's discussion concerning sabotage: everyone has a different definition. The current standard CIP-001 elicited the following response from FERC in FERC Order 693, paragraph 471 which states in part: *". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."*

Often, the underlying reason for an event is unknown or cannot be confirmed. The DSR SDT believes that reporting material risks to the Bulk Electrical System using the impact event categorization, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.

The DSR SDT discussed the reliability needs for impact event reporting and will consider guidance found in the document "NERC Guideline: Threat and Incident Reporting" in the development of requirements, which will include clear criteria for reporting.

Certain types of impact events should be reported to NERC, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and/or Provincial or local law enforcement. Other types of impact events may have different reporting requirements. For example, an impact event that is related to copper theft may only need to be reported to the local law enforcement authorities. The new standard will specify who has access to reported information about impact events.

Potential Uses of Reportable Information

Event analysis, correlation of data, and trend identification are a few potential uses for the information reported under this standard. As envisioned, the standard will only require Functional entities to report the incidents and provide information or data necessary for these analyses. Other entities (e.g. – NERC, Law Enforcement, etc) will be responsible for performing the analyses. The NERC Rules of Procedure (section 800) provide an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for reliability.

Jurisdictional agencies (which may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE) have other duties and responsibilities.

Collection of Reportable Information or "One stop shopping"

The goal of the DSR SDT is to have one reporting form for all functional entities (US, Canada, Mexico) to submit to NERC. Ultimately, it may make sense to develop an electronic version to expedite completion, sharing and storage. Ideally, entities would complete a single form which could then be distributed to jurisdictional agencies and functional entities as appropriate. Specific reporting forms[1] that exist today (i.e. - OE-417, etc) could be included as part of the electronic form to accommodate US entities with a requirement to submit the form. Or may be removed (but still be mandatory for US entities under Public Law 93-275) to streamline the proposed consolidated reliability standard for all North American entities (US, Canada, Mexico). Jurisdictional agencies may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE. Functional entities may include the RC, TOP, and BA for situational awareness. Applicability of the standard will be determined based on the specific requirements.

The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT is planning to update the listing of reportable events from discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences may still exist.

The reporting proposed by the DSR SDT is intended to meet the uses and purposes of NERC. The DSR SDT recognizes that other requirements for reporting exist (e.g., DOE-417 reporting), which may duplicate or overlap the information required by NERC. To the extent that other reporting is required, the DSR SDT envisions that duplicate entry of information is not necessary, and the submission of the alternate report will be acceptable to NERC so long as all information required by NERC is submitted. For example, if the NERC Report duplicates information from the DOE form, the DOE report may be included or attached to the NERC report, in lieu of entering that information on the NERC report.

---

[1] The DOE Reporting Form, OE-417 is currently a part of the EOP-004 standard. If this report is removed from the standard, it should be noted that this form is still required by law as noted on the form: NOTICE: This report is mandatory under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. Title 18 USC 1001 makes it a criminal offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form for Project 2009-01 — Disturbance and Sabotage Reporting

Please **DO NOT** use this form to submit comments. Please use the electronic form located at the site below to submit comments on the proposed Concepts Paper for Disturbance and Sabotage Reporting. Comments must be submitted by **April 16, 2010**. If you have questions please contact Stephen Crutchfield by email at Stephen.crutchfield@nerc.net or by telephone at 609-651-9455.

http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Background:
The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and is progressing toward developing standards based on the SAR. The concepts paper was developed to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed. Please review the redlined SAR and then answer the following questions.

This initial comment period is requesting industry input on the direction herein proposed by the DSR SDT. Should your organization feel that the direction proposed is not the direction that should be pursued then your comments on what direction the SDT should take would be greatly appreciated. The "concept paper" lays out the foundation for the reporting requirements in the standard. We are not seeking input or guidance on the definition of physical or cyber sabotage, what type of disturbances should be reported, who should do reporting, or to whom or what organizations will be receiving the reports. All of these points will be addressed by the SDT in later phases of the project and we will be seeking important industry guidance at those times. The SDT does recognize the importance of all of that data and information, but at this time, we are only seeking input on the direction of the concepts we propose to build upon.

1. The details of reporting requirements and criteria are in the existing EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and will consider guidance found in the document "NERC Guideline: Threat and Incident Reporting" in the development of requirements. Do you agree with using the existing guidance as the foundation for disturbance reporting? Please explain your response (yes or no) in the comment area.

   ☐ Yes

   ☐ No

   Comments:

2. The DSR SDT is considering developing a reporting hierarchy for disturbances that requires entities to submit information to the Reliability Coordinator and then for the Reliability Coordinator to submit the report. Do you agree with this hierarchy concept? Please explain your response (yes or no) in the comment area.

   ☐ Yes

   ☐ No

   Comments:

3. The goal of the DSR SDT is to have one report form for all functional entities (US, Canada, Mexico) to submit to NERC. Do you agree with this change? Please explain your response (yes or no) in the comment area.

   ☐ Yes

   ☐ No

   Comments:

4. The goal of the DSR SDT is to eliminate the need to file duplicate reports. The standards will specify information required by NERC for reliability. To the extent that this information is also required for other reports (e.g. DOE OE-417), those reports will be allowed to supplement the NERC report in lieu of duplicating the entries in the NERC report. Do you agree with this concept? Please explain your response (yes or no) in the comment area.

   ☐ Yes

   ☐ No

   Comments:

5. In its discussion concerning sabotage, the DSR SDT has determined that the spectrum of all sabotage-type events is not well understood throughout the industry. In an effort to provide clarity and guidance, the DSR SDT developed the concept of an impact event.

By developing impact events, it allows us to identify situations in the "gray area" where sabotage is not clearly defined. Other types of events may need to be reported for situational awareness and trend identification. Do you agree with this concept? Please explain your response (yes or no) in the comment area.

☐ Yes

☐ No

Comments:

6. If you are aware of any regional reporting requirements beyond the scope of CIP-001, CIP-008 and EOP-004 please provide them here.

   Comments:

7. If you have any other comments on the Concepts Paper that you haven't already provided in response to the previous questions, please provide them here.

   Comments:

A. Introduction

1. **Title:** **Sabotage Reporting**

2. **Number:** CIP-001-1

3. **Purpose:** Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.

4. **Applicability**

   4.1. Reliability Coordinators.

   4.2. Balancing Authorities.

   4.3. Transmission Operators.

   4.4. Generator Operators.

   4.5. Load Serving Entities.

5. **Effective Date:** January 1, 2007

B. Requirements

R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.

R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

C. Measures

M1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement 1

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements 2 and 3.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to procedures, policies, a letter of understanding, communication records, or other equivalent evidence that will be used to confirm that it has established communications contacts with the applicable, local FBI or RCMP officials to communicate sabotage events (Requirement 4).

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organizations shall be responsible for compliance monitoring.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to verify compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Reliability Coordinator, Transmission Operator, Generator Operator, Distribution Provider, and Load Serving Entity shall have current, in-force documents available as evidence of compliance as specified in each of the Measures.

If an entity is found non-compliant the entity shall keep information related to the non-compliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

None.

2. **Levels of Non-Compliance:**

2.1. **Level 1:** There shall be a separate Level 1 non-compliance, for every one of the following requirements that is in violation:

2.1.1 Does not have procedures for the recognition of and for making its operating personnel aware of sabotage events (R1).

2.1.2 Does not have procedures or guidelines for the communication of information concerning sabotage events to appropriate parties in the Interconnection (R2).

2.1.3 Has not established communications contacts, as specified in R4.

2.2. **Level 2:** Not applicable.

2.3. **Level 3:** Has not provided its operating personnel with sabotage response procedures or guidelines (R3).

2.4. **Level 4:**.Not applicable.

E. Regional Differences

None indicated.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Amended

A. Introduction

1. **Title:** **Disturbance Reporting**

2. **Number:** EOP-004-1

3. **Purpose:** Disturbances or unusual occurrences that jeopardize the operation of the Bulk Electric System, or result in system equipment damage or customer interruptions, need to be studied and understood to minimize the likelihood of similar events in the future.

4. **Applicability**

   4.1. Reliability Coordinators.

   4.2. Balancing Authorities.

   4.3. Transmission Operators.

   4.4. Generator Operators.

   4.5. Load Serving Entities.

   4.6. Regional Reliability Organizations.

5. **Effective Date:** January 1, 2007

B. Requirements

R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.

R2. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.

R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.

R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.

R3.2. Applicable reporting forms are provided in Attachments 1-EOP-004 and 2-EOP-004.

R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that

time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.

R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.

R4. When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.

R5. The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.

C. Measures

M1. The Regional Reliability Organization shall have and provide upon request as evidence, its current regional reporting procedure that is used to facilitate preparation of preliminary and final disturbance reports. (Requirement 1)

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, the preliminary report, computer printouts, operator logs, or other equivalent evidence that will be used to confirm that it prepared and delivered the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that will be used to confirm that it provided information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours. (Requirement 3.3)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

NERC shall be responsible for compliance monitoring of the Regional Reliability Organizations.

Regional Reliability Organizations shall be responsible for compliance monitoring of Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load-serving Entities.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to assess compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Regional Reliability Organization shall have its current, in-force, regional reporting procedure as evidence of compliance. (Measure 1)

Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that is either involved in a Bulk Electric System disturbance or has a reportable incident shall keep data related to the incident for a year from the event or for the duration of any regional investigation, whichever is longer. (Measures 2 through 4)

If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

See Attachments:

- EOP-004 Disturbance Reporting Form
- Table 1 EOP-004

2. Levels of Non-Compliance for a Regional Reliability Organization

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: No current procedure to facilitate preparation of preliminary and final disturbance reports as specified in R1.

3. Levels of Non-Compliance for a Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load- Serving Entity:

3.1. Level 1: There shall be a level one non-compliance if any of the following conditions exist:

3.1.1 Failed to prepare and deliver the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1

3.1.2 Failed to provide disturbance information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours as specified in R3.3

3.1.3 Failed to prepare a final report within 60 days as specified in R3.4

3.2. Level 2: Not applicable.

3.3. Level 3: Not applicable

3.4. Level 4: Not applicable.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	May 23, 2005	Fixed reference to attachments 1-EOP-004-0 and 2-EOP-004-0, Changed chart title 1-FAC-004-0 to 1-EOP-004-0, Fixed title of Table 1 to read 1-EOP-004-0, and fixed font.	Errata
0	July 6, 2005	Fixed email in Attachment 1-EOP-004-0 from info@nerc.com to esisac@nerc.com.	Errata

0	July 26, 2005	Fixed Header on page 8 to read EOP-004-0	Errata
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised
1	March 22, 2007	Updated Department of Energy link and references to Form OE-411	Errata

Attachment 1-EOP-004
NERC Disturbance Report Form

Introduction

These disturbance reporting requirements apply to all Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load Serving Entities, and provide a common basis for all NERC disturbance reporting. The entity on whose system a reportable disturbance occurs shall notify NERC and its Regional Reliability Organization of the disturbance using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. Reports can be sent to NERC via email (esisac@nerc.com) by facsimile (609-452-9550) using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. If a disturbance is to be reported to the U.S. Department of Energy also, the responding entity may use the DOE reporting form when reporting to NERC. Note: All Emergency Incident and Disturbance Reports (Schedules 1 and 2) sent to DOE shall be simultaneously sent to NERC, preferably electronically at esisac@nerc.com.

The NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports are to be made for any of the following events:

1. The loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations. Generally, a disturbance report will be required if the event results in actions such as:
   a. Modification of operating procedures.
   b. Modification of equipment (e.g. control systems or special protection systems) to prevent reoccurrence of the event.
   c. Identification of valuable lessons learned.
   d. Identification of non-compliance with NERC standards or policies.
   e. Identification of a disturbance that is beyond recognized criteria, i.e. three-phase fault with breaker failure, etc.
   f. Frequency or voltage going below the under-frequency or under-voltage load shed points.
2. The occurrence of an interconnected system separation or system islanding or both.
3. Loss of generation by a Generator Operator, Balancing Authority, or Load-Serving Entity — 2,000 MW or more in the Eastern Interconnection or Western Interconnection and 1,000 MW or more in the ERCOT Interconnection.
4. Equipment failures/system operational actions which result in the loss of firm system demands for more than 15 minutes, as described below:
   a. Entities with a previous year recorded peak demand of more than 3,000 MW are required to report all such losses of firm demands totaling more than 300 MW.
   b. All other entities are required to report all such losses of firm demands totaling more than 200 MW or 50% of the total customers being supplied immediately prior to the incident, whichever is less.
5. Firm load shedding of 100 MW or more to maintain the continuity of the bulk electric system.

6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in:
   a. Sustained voltage excursions equal to or greater than ±10%, or
   b. Major damage to power system components, or
   c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance as defined by steps 1 through 5 above.
7. An Interconnection Reliability Operating Limit (IROL) violation as required in reliability standard TOP-007.
8. Any event that the Operating Committee requests to be submitted to Disturbance Analysis Working Group (DAWG) for review because of the nature of the disturbance and the insight and lessons the electricity supply and delivery industry could learn.

NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report

☐ Check here if this is an Interconnection Reliability Operating Limit (IROL) violation report.

1.	Organization filing report.		
2.	Name of person filing report.		
3.	Telephone number.		
4.	Date and time of disturbance. Date:(mm/dd/yy) Time/Zone:		
5.	Did the disturbance originate in your system?	Yes ☐ No ☐	
6.	Describe disturbance including: cause, equipment damage, critical services interrupted, system separation, key scheduled and actual flows prior to disturbance and in the case of a disturbance involving a special protection or remedial action scheme, what action is being taken to prevent recurrence.		
7.	Generation tripped. MW Total List generation tripped		
8.	Frequency. Just prior to disturbance (Hz): Immediately after disturbance (Hz max.): Immediately after disturbance (Hz min.):		
9.	List transmission lines tripped (specify voltage level of each line).		
10.		FIRM	INTERRUPTIBLE
	Demand tripped (MW):		
	Number of affected Customers:		

	Demand lost (MW-Minutes):		
11.	Restoration time.	INITIAL	FINAL
	Transmission:		
	Generation:		
	Demand:		

Attachment 2-EOP-004
U.S. Department of Energy Disturbance Reporting Requirements

Introduction

The U.S. Department of Energy (DOE), under its relevant authorities, has established mandatory reporting requirements for electric emergency incidents and disturbances in the United States. DOE collects this information from the electric power industry on Form OE-417 to meet its overall national security and Federal Energy Management Agency's Federal Response Plan (FRP) responsibilities. DOE will use the data from this form to obtain current information regarding emergency situations on U.S. electric energy supply systems. DOE's Energy Information Administration (EIA) will use the data for reporting on electric power emergency incidents and disturbances in monthly EIA reports. In addition, the data may be used to develop legislative recommendations, reports to the Congress and as a basis for DOE investigations following severe, prolonged, or repeated electric power reliability problems.

Every Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity must use this form to submit mandatory reports of electric power system incidents or disturbances to the DOE Operations Center, which operates on a 24-hour basis, seven days a week. All other entities operating electric systems have filing responsibilities to provide information to the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity when necessary for their reporting obligations and to file form OE-417 in cases where these entities will not be involved. EIA requests that it be notified of those that plan to file jointly and of those electric entities that want to file separately.

Special reporting provisions exist for those electric utilities located within the United States, but for whom Reliability Coordinator oversight responsibilities are handled by electrical systems located across an international border. A foreign utility handling U.S. Balancing Authority responsibilities, may wish to file this information voluntarily to the DOE. Any U.S.-based utility in this international situation needs to inform DOE that these filings will come from a foreign-based electric system or file the required reports themselves.

Form EIA-417 must be submitted to the DOE Operations Center if any one of the following applies (see Table 1-EOP-004-0 — Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies):

1. Uncontrolled loss of 300 MW or more of firm system load for more than 15 minutes from a single incident.
2. Load shedding of 100 MW or more implemented under emergency operational policy.
3. System-wide voltage reductions of 3 percent or more.
4. Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the electric power system.
5. Actual or suspected physical attacks that could impact electric power system adequacy or reliability; or vandalism, which target components of any security system. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.

6. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.
7. Fuel supply emergencies that could impact electric power system adequacy or reliability.
8. Loss of electric service to more than 50,000 customers for one hour or more.
9. Complete operational failure or shut-down of the transmission and/or distribution electrical system.

The initial DOE Emergency Incident and Disturbance Report (form OE-417 – Schedule 1) shall be submitted to the DOE Operations Center within 60 minutes of the time of the system disruption. Complete information may not be available at the time of the disruption. However, provide as much information as is known or suspected at the time of the initial filing. If the incident is having a critical impact on operations, a telephone notification to the DOE Operations Center (202-586-8100) is acceptable, pending submission of the completed form OE-417. Electronic submission via an on-line web-based form is the preferred method of notification. However, electronic submission by facsimile or email is acceptable.

An updated form OE-417 (Schedule 1 and 2) is due within 48 hours of the event to provide complete disruption information. Electronic submission via facsimile or email is the preferred method of notification. Detailed DOE Incident and Disturbance reporting requirements can be found at: http://www.oe.netl.doe.gov/oe417.aspx.

Table 1-EOP-004-0 Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Uncontrolled loss of Firm System Load	≥ 300 MW – 15 minutes or more	OE – Sch-1 OE – Sch-2	1 hour 48 hour
2	Load Shedding	≥ 100 MW under emergency operational policy	OE – Sch-1 OE – Sch-2	1 hour 48 hour
3	Voltage Reductions	3% or more – applied system-wide	OE – Sch-1 OE – Sch-2	1 hour 48 hour
4	Public Appeals	Emergency conditions to reduce demand	OE – Sch-1 OE – Sch-2	1 hour 48 hour
5	Physical sabotage, terrorism or vandalism	On physical security systems – suspected or real	OE – Sch-1 OE – Sch-2	1 hour 48 hour
6	Cyber sabotage, terrorism or vandalism	If the attempt is believed to have or did happen	OE – Sch-1 OE – Sch-2	1 hour 48 hour
7	Fuel supply emergencies	Fuel inventory or hydro storage levels ≤ 50% of normal	OE – Sch-1 OE – Sch-2	1 hour 48 hour
8	Loss of electric service	≥ 50,000 for 1 hour or more	OE – Sch-1 OE – Sch-2	1 hour 48 hour
9	Complete operation failure of electrical system	If isolated or interconnected electrical systems suffer total electrical system collapse	OE – Sch-1 OE – Sch-2	1 hour 48 hour
All DOE OE-417 Schedule 1 reports are to be filed within 60-minutes after the start of an incident or disturbance All DOE OE-417 Schedule 2 reports are to be filed within 48-hours after the start of an incident or disturbance				
All entities required to file a DOE OE-417 report (Schedule 1 & 2) shall send a copy of these reports to NERC simultaneously, but no later than 24 hours after the start of the incident or disturbance.				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Loss of major system component	Significantly affects integrity of interconnected system operations	NERC Prelim Final report	24 hour 60 day

2	Interconnected system separation or system islanding	Total system shutdown Partial shutdown, separation, or islanding	NERC Prelim Final report	24 hour 60 day
3	Loss of generation	≥ 2,000 – Eastern Interconnection ≥ 2,000 – Western Interconnection ≥ 1,000 – ERCOT Interconnection	NERC Prelim Final report	24 hour 60 day
4	Loss of firm load ≥15-minutes	Entities with peak demand ≥3,000: loss ≥300 MW All others ≥200MW or 50% of total demand	NERC Prelim Final report	24 hour 60 day
5	Firm load shedding	≥100 MW to maintain continuity of bulk system	NERC Prelim Final report	24 hour 60 day
6	System operation or operation actions resulting in:	• Voltage excursions ≥10% • Major damage to system components • Failure, degradation, or misoperation of SPS	NERC Prelim Final report	24 hour 60 day
7	IROL violation	Reliability standard TOP-007.	NERC Prelim Final report	72 hour 60 day
8	As requested by ORS Chairman	Due to nature of disturbance & usefulness to industry (lessons learned)	NERC Prelim Final report	24 hour 60 day
All NERC Operating Security Limit and Preliminary Disturbance reports will be filed within 24 hours after the start of the incident. If an entity must file a DOE OE-417 report on an incident, which requires a NERC Preliminary report, the Entity may use the DOE OE-417 form for both DOE and NERC reports.				
Any entity reporting a DOE or NERC incident or disturbance has the responsibility to also notify its Regional Reliability Organization.				

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Comment Period Open
March 17–April 16, 2010

Now available at: http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Project 2009-01: Disturbance and Sabotage Reporting

The Disturbance and Sabotage Reporting Drafting Team is seeking comments on a proposed concepts paper for disturbance and sabotage reporting **until 8 p.m. Eastern on April 16, 2010.**

The concepts paper lays out the foundation for the reporting requirements in the standard and was developed to solicit stakeholder input regarding the drafting team's proposed reporting concepts.

Instructions

Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Lauren Koller at Lauren.Koller@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page: http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Next Steps

The drafting team will draft and post responses to comments received during this period.

Project Background

This project will entail revising existing standards CIP-001-1 — Sabotage Reporting and EOP-004-1 — Disturbance Reporting to eliminate redundancies and provide clarity on sabotage events. The project will address several issues identified by stakeholders, as well as FERC directives from Order 693. The other changes may include improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Lauren Koller at Lauren.Koller@nerc.net

Individual or group. (41 Responses)
Name (26 Responses)
Organization (26 Responses)
Group Name (15 Responses)
Contact Organization (15 Responses)
Question 1 (39 Responses)
Question 1 Comments (41 Responses)
Question 2 (40 Responses)
Question 2 Comments (41 Responses)
Question 3 (38 Responses)
Question 3 Comments (41 Responses)
Question 4 (39 Responses)
Question 4 Comments (41 Responses)
Question 5 (37 Responses)
Question 5 Comments (41 Responses)
Question 6 (0 Responses)
Question 6 Comments (41 Responses)
Question 7 (0 Responses)
Question 7 Comments (41 Responses)

-	-
	Group
	Exelon
	Exelon Transmission Strategy & Compliance
	Yes
	No
	Some of the DOE related reporting is driven by distribution events, i.e. outages greater then 50,000 customers, is it realistic to expect the RC, whose focus is on the transmission system to perform distribution related reporting?
	Yes
	Yes
	No
	We agree with the direction to identify impact events examples that would trigger reporting and not be limited to sabotage reporting only. It is important to note that when an incident occurs, some level of investigation is required before a determination can be made as to the event is sabotage or not. The focus should be on reporting events when they occur and allow follow-up investigations to make the sabotage determination. That being said, care must be taken in the development of any list of impact events so that it doesn't become or is misinterpreted to be a definitive list. Therefore if it is not on the list, it is not reportable.
	At the 2010 RFC Spring Workshop the following disturbance reporting Criteria was rolled out: All events that are required to be reported by the OE-417 and EOP-004 criteria will use those published procedures. For other events that do not meet the OE-417 and EOP-004 reporting criteria, ReliabilityFirst expects to receive notification of any events involving a sustained outage of multiple BES facilities (buses, lines, generators, and/or transformers, etc.) that are in close proximity (electrically) to one another and occur in a short time frame (such as a few minutes).
	You should consider providing clear and concise instructions as to the expectation on submitting forms, i.e. the DOE 417. There should be no guessing as to when and how reports should be submitted and who should receive them. Specific details on reporting criteria should be included.
	Individual
	Steve Fisher
	Lands Energy Consulting
	No
	My firm provides compliance consulting services to a number of smaller (50-700 MW peak load) LSE/DP registered entities. EOP-004 creates an obligation for LSEs to report "disturbances" that affect their systems. A few of the smaller of these systems receive service from Bonneville-owned transmission lines that serve only 4-6 substations. The NERC Form establishes loss of 50% of the LSE's retail customers as a reportable disturbances. One of my clients receives service from BPA at 5 substations. A single industrial customer with a substantially dedicated

	substation comprises 90% of the utility's MWH load. Were it not for this customer, the utility would have been well below the registration requirement for a DP/LSE. The balance of the load, about 15 MW of peak and 4000 retail customers, is served from 5 substations. Four of these substations serving 3000 customers are served from a long Bonneville 115 kV BES transmission line that runs through a heavily treed right of way. Every time this single line experiences a permanent outage (which will happen a few times a year), the utility loses less than 10 MW of load, but 75% of its retail customers. Under the disturbance reporting criteria, this outage would constitute a reportable disturbance for the utility. When the NERC disturbance reporting criteria were adopted, I doubt that anyone conceived that they would apply to cases like I just desribed. Reporting trivial events like I've just described constitutes a nuisance to the entity making the report and NERC/WECC for having to process the report. The outage has no earthly effect on the reliability of the BES and certainly doesn't warrant preparation of any kind of disturbance report.
	Yes
	I would give the RC the authority to establish impact thresholds for reporting. Consistent with my earlier comment, I would set the materiality threshold for disturbance reporting purposes at LSEs (or a combination of LSEs in the case of BPA) serving at least 90,000 customers.
	Yes
	I think that the impact approach makes sense and that EOP-004 and CIP-001 are logically connected. Many entities of which I am aware link Sabotage Reporting Training to Disturbance Reporting obligation awareness already.
	Yes
	Less paperwork and fewer requirements to keep in mind during what may be once in a lifetime events are always good.
	No
	The level of complexity described will overwhelm the 20-200 employee utilities that have yet to see - and will never see - the kind of sabotage event that scares the Department of Homeland Security.
	I believe WECC sets its loss of load criteria for disturbance reporting at 200 MW rather than the 300 MW in the NERC reporting form.
	The lack of common sense that leads to a 15 MW loss of load resulting from a 115 kV line outage being catagorized as a "reportable disturbance" really hurts the credibility of the entire NERC Compliance Program. The smaller utilities look at application of EOP-004 in particular to their operation and conclude that either the EO/RRO is: a. stupid; or b. Out to persecute the smaller utilities. In reality, EOP-004 was drafted for application to Southern California Edison, where loss of 50% of customers would be 2-3 million customers. Now that's really disturbing!
	Individual
	David Kahly
	Kootenai Electric Cooperative
	No
	Impact events seems to add another layer of uncertainty to the reporting. Define a transmission line. Our transmission lines have very little impact on the grid. It is possible for our lines to cause a local area outage on our transmission provider - but neither is of national security interest or even regional interest. There is no power flow going on across the lines other than local power delivery supply. It seems you run more risk of losing the important reports in the snow of reporting - similar to what we have to avoid on our SCADA systems for our operators to see the key information.
	Group
	Northeast Power Coordinating Council
	Northeast Power Coordinating Council
	Yes
	In considering guidance found in the document “NERC Guideline: Threat and Incident Reporting”, the SDT should maintain focus on only those items that are absolutely necessary to maintain the reliability of the Bulk Electric System. In fact, the purpose of reporting per EOP-004 is that disturbances... need to be studied and understood to minimize the likelihood of similar events in the future.
	No
	This is not a standards issue, and NERC should not dictate the reporting structure. It should be left to the RCs and their members.
	Yes

	We agree with the concept that there should be one report form for all functional entities (whether located in the US, Canada, Mexico) for use in reporting to NERC. This would provide for a consistent reporting format across the continent.
	Yes
	We agree with the objective of eliminating duplicate reporting. However, EOP-004 currently allows substitution of DOE OE-417 in place of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report. As suggested in the Concept Paper, entities meeting the criteria of OE-417 are still obligated to file a report with DOE. Given that and the fact that CIP-001 requires no actual reporting, it is not clear where duplication exists today. We agree with the recommendation to eliminate the need for filing duplicate reports such as the DOE form OE-417. There is no benefit with regard to CIP-001 in filing separate reports. Duplicate reports introduce the potential for incomplete information to be supplied to responsible parties. Removing jurisdictional agencies from the Standard, and having NERC provide either query or situational awareness to those agencies being considered, might not be easy to achieve. There is an obligation under law to require entities to report to the DOE on the OE-417 form as amended or modified. This might drive the “omitted” agencies to have reporting laws enacted as well.
	No
	We believe that physical and cyber events must be investigated before a determination of sabotage or impact event can be made. The purpose of the NERC Standards is to maintain the reliability of the BES. Therefore, impact events should define or clarify the circumstances that would or could affect reliability. Reportable items should be based on impact to reliability, not on ‘newsworthy’ events or to gather information for trending. It is the law enforcement industry’s responsibility to make a determination of “sabotage” or other. This determination cannot definitively be made by industry personnel, there is no expertise or time to investigate causes. It is the industry’s job to mitigate effects. Examples would help provide for better guidance/direction. Industry examples would be welcomed to help reinforce developed internal processes for compliance.
	SERC and RFC are developing additional requirements at this time. We suggest that reporting be based on impact to reliability, not on ‘newsworthy’ events. We therefore do not agree with such regional efforts and would prefer a continent wide reporting requirement.
	a. NERC should focus efforts on developing specific event reporting criteria and not base the requirement on the definition of the term ‘sabotage’, but on the reporting criteria itself. See comments above. b. The “opportunities for efficiency” discussed in the Concept Paper would be best achieved by focusing on those items that are absolutely necessary to maintain the reliability of the Bulk Electric System. If there are elements that need to be reported that do not support this objective, then that reporting should not be required in reliability standards. Consider making NERC the distributor of reports to other agencies. We recognize that the key is to simplify reporting to a single form, and to the extent possible, to one agency. “Front line” reliability personnel must have the “timely” knowledge to know when a situation warrants local, area, regional, or national involvement.
	Individual
	Darryl Curtis
	Oncor Electric Delivery Company LLC
	Yes
	NERC Guideline: Threat and Incident Reporting" document should be used for guidance as it identifies best practices for reporting.
	Yes
	Oncor agrees that with this reporting hierarchy, in that dual reporting should be elminated
	Yes
	Oncor agrees that by using the same type reporting format, there should be consistency in regard to each functional entity's expectations.
	Yes
	Oncor agrees that this effort should eliminate file duplication
	Yes
	Oncor agrees that there are no broadly used guidance documents that detail how an event may be accurately defined.
	Oncor is not aware of any regional reporting requirements beyond the scope of CIP-001, CIP-008 and EOP-004.
	Group
	SERC Reliability Coordinator Sub-committee (RCS)
	SERC RCS
	No
	Routine minor incidents such as copper theft and gun shots to insulators should not be reported. These types of minor events do not affect the reliability of the BPS. Existing reporting requirements are satisfactory. The focus of reporting should be on reliability related incidents and not incidents related to vandalism as such.

	No
	The RC should not be responsible for submitting the report to FERC, NERC or the RRO. The RC may not have the necessary first hand information concerning the facts of the event. Situation awareness can be maintained by including the RC in the distribution of any sabotage related reporting.
	Yes
	There should only be one report for all functional entities.
	No
	The requirement should be a single report that satisfies the need for all US governmental agencies as well as NERC and the RRO's.
	No
	Impact events that do not afffect reliability should not be reported.
	We are not aware of any regional reporting requirements beyond the requirements of CIP-001, CIP-008 and EOP-004. However, the SERC RRO has shared a list of events of interest that it would like to be made aware of to maintain situation awareness.
	None.
	Group
	Arizona Public Service Company
	Arizona Public Service Company
	No
	APS supports standard revisions which streamline the reporting process for security incidents with a single form, which aligns both with EIA reporting and NERC Standards requirements, particularly those identified in the NERC Threat and Incident Reporting Guidelines. This would eliminate users issuing reports to multiple locations/government entities without a standard form or format. The DOE 417 form which is currently utilized for reporting purposes is out-dated and does not account for the types of incidents as identified in the NERC Threat and Incident Reporting Guidelines. The guidelines state that an entity can report security incidents to the ESISAC , through CIPIS (Critical Infrastructure Protection Information System), and or RCIS (Reliability Coordinator Information Center). CIPIS refers an entity to the NICC and to the WECC. Additionally, APS proposes that the terms and timelines of reporting security incidents be clearly identified. Events are often detected quickly or immediately. Determining whether or not the event was sabotage and/or a reportable event; however, typically takes much longer. There is no time allowance for an entity to investigate the event to determine what actually occurred. Currently, DOE 417 provides that acts of sabotage should be reported within one hour of detection if the impact could affect the reliable operation of the bulk power system. This may affect the accuracy of the information being provided by an entity on it's initial reporting. Finally, provisions should be incorporated to address the privacy of information being submitted, including handling and storage.
	Yes
	All disturbance reporting should go through the RC.
	Yes
	APS supports the standardization of the form for consistency and format.
	Yes
	APS supports eliminating the need to file duplicate reports. This standardized form should generate and send the DOE OE-417 report, totally eliminating duplicate work. Streamline the process.
	Individual
	Edward Bedder
	Orange and Rockland Utilities, Inc.
	Yes
	However, the SDT needs to maintain clear demarcation for the criteria for reporting events, and only those events that directly effect the reliability of the BES.
	Yes
	Having the reporting flow through the Reliability Coordinator supports the reliability objective of assessing, monitoring, and maintaining a wide-area view of the reliability of the Bulk Electric System. The reporting hierarchy should be to submit the information to the Reliability Coordinator, and to have the RC submit the report. This would eliminate the duplication of information.

	Yes
	We agree with the concept that there should be one report form for all functional entities (whether located in the US, Canada, Mexico) for use in reporting to NERC. This would provide for a consistent reporting format across the continent.
	Yes
	No
	Physical and cyber events must be investigated before a determination of sabotage or impact event can be made. Impact events should define or clarify the circumstances that would or could affect reliability. Reportable items should be based on impact to reliability, not on 'newsworthy' events or to gather information for trending. It is the law enforcement industry's responsibility to make a determination of "sabotage" or other. This determination cannot definitively be made by industry (operating) personnel. If NERC's definition is expanded for CIP-001 and/or EOP-004, responsibility and timing of reporting needs to addressed so that appropriate agencies conduct the investigation and assessment. Operating personnel need to remain focused on the primary responsibility of mitigating the effects.
	NERC's SDT effort requires a clear, consistent, and comprehensive continent-wide approach, thus mitigating any need for regional reporting requirements.
	Individual
	Kasia Mihalchuk
	Manitoba Hydro
	Yes
	The "Threat and Incident Reporting" document contains a lot of detailed information which greatly assists in determining reporting events and weaning out non important events. The document contains some examples and expected reporting time lines. Attachment 1-EOP-004, though considerably smaller and condensed it does contain some detail not mentioned in "Threat and Incident Reporting". Integrating the "Threat and Incident Reporting" into Attachment 1-EOP-004, though large in size, has lots of information and is easy to follow would be a large improvement to existing protocol OR SEE QUESTION 3 COMMENTS. Incidences we have experienced on our system, in past were difficult to delineate as reportable, who to report to and when. An improvement to this Standard is welcome.
	Yes
	The Reporting Concept states that the new hierarchy is, " Affected entity to TOP/ BA to RC. Then the RC will then submit to NERC and DOE (if required)". This will enhance the existing requirement EOP-004-1 R4 which states that the RC shall assist the affected entity by providing representatives to assist in the investigation (this is also all reiterated in Attachment 1-EOP-004) . In an disturbance, the local resources would be tied up in the rectification of the problem. Analyzing and reporting the event (is it reportable, who to report to, what is the timeline) is distracting and time consuming. By leaving the final upper level steps of reporting to NERC/DOE by the RC would be efficient.
	Yes
	This is a promising idea, though there would be different requirements for the three countries, this could easily be rectified with "drop down menus". This electronic form could contain a lot of information without distracting clutter as you "tree" down the menu depending on the event that occurred. This could also contain electronic references to information located in Attachment 1-EOP-004 and Threat and Incident Reporting.
	Yes
	This could be easily incorporated into the electronic form. You could be prompted for information required immediately, and notified for information that could be entered later. This form could contain all the enterable data that all agencies could require. If the form is live and on line, all entities could be notified (depending on the entries) of an going event immediately. Form could be web based similar to ARS program or even integrated into the ARS program.
	Yes
	Though there are some specific events already included in this new definition, more could be added to dissolve specific "gray areas" and as new ones come up. Again these examples could be added into the electronic form and could contain a large data base which would be available depending on the event that occurred.
	No. CIP-001 contains references to NERC and the DOE. CIP-008 makes exclusions for facilities regulated by US Nuclear Regulatory Commission and Canadian Nuclear Safety Commission. It also contains references to ES ISAC (Electricity Sector Information Sharing and Analysis Center). EOP-004 contains reference to NERC and DOE There is no reference to Homeland Security, FBI, etc or to Canadian equivalent references in any of these Standards. When NERC is notified of an event, it is likely other organizations will have to be notified. There should be some sort of consistency to cover all these Standards and all notifiable parties at a NERC Standards level.
	No
	Individual
	Brian Bartos
	Bandera Electric Cooperative, Inc.

	Yes
	Yes
	This approach, while I suspect will not be universally agreed to, should provide some definitive guidance in reporting.
	No preference in this area.
	Yes
	One can only assume the number of reports required in this area will continue to increase in terms of scope and to which agency wants this data. The SDT is encouraged to attempt to find a reporting format and scope that does not needlessly duplicate or complicate overall reporting obligations.
	Yes
	In principle, I agree with this concept. Would like for the SDT to pursue this further and seek additional comments at that time.
	No.
	I commend the SDT for working on this effort and wish them success.
	Group
	PacifiCorp
	PacifiCorp
	Yes
	Yes
	Yes
	Yes
	Yes
	Group
	E.ON U.S. LLC
	E.ON U.S.LLC
	Yes
	E.ON U.S. believe that the guidelines provide greater clarity for reporting forced outages caused by disturbances and sabotage but there remains issues that in need of further clarification. For example, there remains too much subjectivity on the reporting of forced outages when there is “identification of valuable lessons learned”
	Yes
	The hierarchy will simplify reporting from the entity in that the RC is always notified and then the RC notifies other parties as required, (with the exception of OE-417, which still has to be filled out per law) E.ON U.S. recommends that the drafting team pay particular attention to the report process to make sure that duplicate reports are not being required. Currently information on forced outages is already communicated to the RC so formalizing a requirement to provide data to the RC may represent duplication to reports already provided.
	Yes
	E.ON U.S. supports the proposal.
	No
	Reliability standards are federal law enforced by fines that can reach up to $1,000,000 per day of violation. There is no reason to deliberately include ambiguity, i.e. “gray areas,” in requirements such that registered entities are left unable to determine what it is they must do or refrain from doing to remain compliant. “Sabotage” for the purposes of these standards must be defined. .

	Individual
	John T. Walker
	Portland General Electric
	Yes
	This process is in place and utilities are familiar with it. This is a good place to start.
	Yes
	PGE is familiar with and works closely with WECC today so the hierarchial consideration makes sense.
	Yes
	PGE supports the efforts of the Standards Drafting Team on the SAR for Project 2009-01 to consolidate the disturbance and saborage reporting processes as outlined in the concept paper.
	Yes
	PGE supports reducing the duplication of reporting.
	Yes
	PGE supports the DSR SDT's efforts to bring clarity and guidance to the spectrum of sabotage-type events.
	Individual
	Gregory Miller
	BGE
	Yes
	We have no problem with NERC using the existing guidance as the foundation for disturbance reporting; however, since this project proposes to investigate incorporation of the Cyber Incident reporting aspects of CIP-008, we feel that if adopted, this concept should be added to the NERC Guideline document "Threat and Incident Reporting".
	No
	As currently worded, BGE opposes the reporting hierarchy concept, since insufficient guidelines were proposed to prevent translation errors between the responsible entity (RE) and the RC. In addition to creating possible reporting errors, this also opens a risk that the RC could misrepresent the true intent of an RE's report contents if called upon to explain/justify a submitted report. Reporting delays are another concern with this proposal because the RE would basically be relinquishing control of the reporting process to the RC, while ultimately retaining the responsibility for ensuring the report gets submitted within the required timeframe. However, BGE recognizes that avoiding duplication and conflicting reports as well as encouraging communication are valuable. To make the reporting hierarchy concept acceptable to BGE, the DSR SDT must develop proper controls to ensure the RE has the ability to control or approve the information submitted and/or subsequently discussed with the respective authorities, and that it is done within the permissible timeframe to satisfy compliance requirements.
	Yes
	One form makes sense to us; less is better is the sense that it makes filing reports easier by not creating unnecessary complications.
	Yes
	We agree with this approach, as long as the latest version of the DOE OE-417 form is fully incorporated in the new single-reporting form, so that it maintains its credibility with the DOE.
	Yes
	We agree that "the spectrum of all sabotage-type events is not well understood throughout the industry"; however, we feel that the proposed concept of an "Impact Event" falls short of clarifying what constitutes such events. We believe that "Impact Events" needs further clarification to eliminate "gray areas" and to provide more reporting consistency between entities.
	We are not aware of any regional requirements beyond the scope of CIP-001, CIP-008 and EOP-004.
	1. If we move to a "one size fits all" single reporting form, it is important that the form be properly developed to cover any foreseeable event, which appears to be the intent of the DSR SDT, as outlined on page 4 of the concept document. Such an approach should also incorporate a single point of contact for reporting information, to avoid any confusion. 2. We would like clarification that any proposed CIP-008-related reporting requirement (including any linked reporting requirement between CIP-008 and CIP-001) is only applicable in situations where the incident/event involves a registered entity's Critical Cyber Asset.

	Individual
	Dan Roethemeyer
	Dynegy Inc.
	Yes
	We agree with using the guidance; however, please consider revising the NERC Guideline: Threat and Incident Reporting document to (i) lengthen the reporting timelines related to attempted sabotage to allow for additional time to deem the threat credible, (ii) expand the description of forced outage of generation greater than 2000 MW to include whether it is at the BA or GO level and if GO level, whether it is for one site or the combined GO's sites in a Region, and (iii) add a Responsible Party column to the Appendix A matrix.
	Yes
	This seems to be straightforward approach in that the RC is the best judge of threats to the overall system and could eliminate multiple reports of a single event.
	Yes
	Please keep it short and simple.
	Yes
	Short and simple should be the goal.
	Yes
	We agree with the concept but please provide specific examples. Also, please consider whether their are any penalties for misinterpreting an incident, who would determine if an event was a threat, and whether this could result in over reporting non-threats.
	Please consider MISO RTO-OP-023.
	N/A
	Group
	Electric Market Policy
	Dominion Resources Services, Inc.
	Yes
	Yes; however, in considering guidance found in the document “NERC Guideline: Threat and Incident Reporting” the SDT should maintain focus on only those items that are absolutely necessary to maintain the reliability of the Bulk Electric System. In fact, the purpose of reporting per EOP-004 is that disturbances... need to be studied and understood to minimize the likelihood of similar events in the future.
	Yes
	Having the reporting flow through the Reliability Coordinator supports the reliability objective of assessing, monitoring, and maintaining a wide-area view of the reliability of the Bulk Electric System.
	Yes
	Yes, we agree with the concept that there should be one report form for all functional entities (whether located in the US, Canada, Mexico) for use in reporting to NERC.
	Yes
	Yes, we agree with the objective of eliminating duplicate reporting; however, EOP-004 currently allows substitution of DOE OE-417 in place of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report. As suggested in the Concept Paper, entities meeting the criteria of OE-417 are still obligated to file a report with DOE. Given that and the fact that CIP-001 requires no actual reporting, it is not clear where duplication exists today.
	Yes
	We believe that physical and cyber events must be investigated before a determination of sabotage or impact event can be made.
	SERC and RFC are developing additional requirements at this time. We suggest that reporting be based on impact to reliability, not on ‘newsworthy’ events. We therefore do not agree with such regional efforts and would prefer a continent wide reporting requirements.
	a. NERC should focus efforts on developing specific event reporting criteria and not base the requirement on the definition of the term ‘sabotage’ but on the reporting criteria itself. b. The “opportunities for efficiency” discussed in the Concept Paper would be best achieved by focusing on those items that are absolutely necessary to maintain the reliability of the Bulk Electric System. If there are elements that need to be reported that do not support this objective, than that reporting should not be required in reliability standards.
	Individual
	Rick Terrill
	Luminant

	No
	While the guidance is generally ok in the “NERC Guideline: Threat and Incidence Reporting”, the reporting timelines include 1 hour, 2 hours, 4 hours, 6 hours, 8 hours, 24 hours, and 48 hours. Please simplify and reduce the variation in timelines. When it comes to Sabotage reporting, some time requirements start with detection, some start with determination of sabotage and some events do not specify the trigger for the reporting clock to start. Again, please provide clarity and consistency around the start of the timeline for reporting. Generally, the reporting timing should start with the recognition or determination that a suspected or known sabotage event occurred.
	Yes
	Luminant believes that one report should be filed with the Reliability Coordinator or one responsible entity, who then files the report with all applicable entities.
	Yes
	Luminant agrees with the concept of reducing reporting requirements, but asks the SDT to go even further. In the concept paper, the SDT discussed that information would not be duplicated on the NERC report and the DOE OE-417 report. The concept paper described a process where one report would simply supplement the other, but two reports would still be filed when required. Can the NERC SDT work with the DOE to develop one report to meet the needs of NERC and the DOE?
	No
	Luminant would prefer to report disturbances and sabotage events. The reporting of impact events could lead to unnecessary reporting. A definition of an “impact event” may be even more confusing than sabotage events.
	Luminant disagrees with the direction of utilizing impact events, as this is an expansion in scope beyond the simplification of sabotage and disturbance reporting.
	Group
	MRO's NERC Standards Review Subcommittee
	Midwestreliability Organization
	No
	We agree with using the present documentation but would like just one reporting form. We are concerned that the guidelines and reporting periods specified within the DOE OE-417 report conflict with the NERC Guidelines. For example. DOE OE-417 report requires “Suspected Physical or Cyber Impairment” to be reported within 6 hours. The NERC guidelines indicate “Suspected Activities” are to be reported within 1 hour. We recommend the SDT use the DOE OE-417 report as a guiding document, and then determine additional reporting requirements using guidance from the NERC Guideline. FERC Order 693 appears to indicate conflicts and confusion with NERC reporting requirements and DOE reporting requirements should be eliminated.
	No
	We agree a coordinated reporting process is beneficial for the entity and the Reliability Coordinator (RC). However, a hierarchy would likely lengthen the reporting timeframe, or reduce the allotted time for each entity to provide notification to the RC in order to meet DOE or NERC timelines. Communication and coordination with the RC would likely provide more accurate and complete data submissions within a timely process and create shared accountability for the report being submitted.
	Yes
	However, We believe the primary goal should focus on “each entity” being able to submit one report for all functional requirements. Entities in the US that are required to submit the DOE OE-417 form should not be required to submit an additional form developed for other entities (Canada & Mexico). One approach to satisfy this goal is for NERC to require all entities (US, Canada, & Mexico) to complete the DOE OE-417 form as their report.
	Yes
	We agree with the concept to eliminate duplicate reports. However, we are concerned with the reference of the DOE OE-417 report being a “supplement” of the NERC report rather than “accepted” as the NERC report.
	No
	Rather than attempting to define a new term (impact event), we suggest that the concept of impact event be replaced with further defining sabotage and providing guidance on trigger events (impact event) that would cause an entity to report.
	No Comment.
	Confusion often arises in the industry between the CIP standards and other reliability standards based on CIP-001 naming convention. We would suggest the SDT retire CIP-001 and incorporate requirements within the EOP-004 standard or a new EOP-xxx standard to avoid confusion rising from CIP and other NERC Reliability Standards. Additionally, we assume the SDT has been created to specifically address FERC Order 693 directives to the ERO which appears to include the following items: 1. Applicability – “possible revisions to CIP-001-1 that address our concerns regarding the need for wider application of the Reliability Standard… the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate” (FERC, 2007, para. 460). 2. Definition of Sabotage – “we direct that the ERO further define the term and provide guidance on triggering events

	that would cause an entity to report an event… we believe the term sabotage is commonly understood and that common understanding should suffice in most instances… the ERO should consider FirstEnergy's suggestions to differentiate between cyber and physical sabotage and develop a threshold of materiality." (FERC, 2007, para. 461-462) 3. Periodic Review and Testing – "directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures." (FERC, 2007, para. 466) 4. Redundant Reporting – "now direct the ERO to address our underlying concern regarding mandatory reporting of a sabotage event… Regarding the potential for redundant reporting under CIP-001-1 and other government reporting standards, and the need for greater coordination… We direct the ERO to explore ways to address these concerns – including central coordination of sabotage reports and a uniform reporting format… with the appropriate governmental agencies that have levied the reporting requirements." (FERC, 2007, para. 468-469) 5. Specified Time – "the Commission directs the ERO to modify CIP-001-1 to require an applicable entity to contact appropriate governmental authorities in the event of sabotage within a specified period of time… the ERO should consider suggestions raised… to define the specified period for reporting an incident beginning from when an event is discovered or suspected to be sabotage" (FERC, 2007, para. 470). 6. Summary of CIP-001-1 – "the Commission directs the ERO to develop the following modifications… (1) further define sabotage and provide guidance as to the triggering events… (2) specify baseline requirements regarding… procedures for recognizing sabotage events… (3) incorporate a periodic review… and for the periodic testing… (4) require an applicable specified period of time. In addition… address our concerns regarding applicability to smaller entities… consolidation of the sabotage reporting forms and the sabotage reporting channels with the appropriate governmental authorities to minimize the impact of these reporting requirements on all entities." (FERC, 2007, para. 471) 7. Analyze Performance – "at a minimum, generator operators and LSEs should analyze the performance of their equipment and provide the data… The Commission directs the ERO to consider this concern in future revisions… that includes any Requirements necessary for users, owners and operators… to provide data that will assist NERC" (FERC, 2007, para. 613, 617). 8. Reporting Time Frames – "The Commission directs the ERO to change its Rules of Procedures to assure that the Commission also receives these reports within the same time frames as the DOE." (FERC, 2007, para. 618)
	Individual
	James Stanton
	SPS Consulting Group Inc.
	No
	At least not exclusively. The current standards and the guidance fail to consider that different registered entities will have different scopes of awareness for when disturbances may take place. We want to avoid the situation where a generator (for example) is cited for failure to report a disturbance of which they have way of knowing occurred.
	Yes
	Yes
	There should have probably been one report all along.
	Yes
	Duplication is inefficient and casts the whole reporting mechanism in a questionable light.
	Yes
	The term sabotage was always too narrow a concept for the standards. At times, questionable activities are not confirmed as sabotage events until well after the fact, forcing the registered entity to speculate on whether or not to report an activity that may not be a confirmed sabotage event at the time, and hence encounter another silly violation based on imprecise terminology.
	Again, please consider the unique scope of the entities to which these standards are to comply. Don't dump all the requirements on all the applicable entities and perpetuate the current practice of forcing them to parse the requirements into what is logical or illogical from their perspective. The drafting team should have the expertise to do this. Identify which requirements apply to which applicable entity.
	Individual
	Andrew Gallo
	Calpine Corp.
	Yes
	Yes
	A Functional Entity such as a Generator Owner/Operator is not always aware that an event, such as a plant trip, is part of a wider system disturbance that rises to the level of a reportable event under EOP-004. A reporting hierarchy that allows a Generator to report the facts to its Transmission Operator and have that entity take a wider view to determine whether there is a disturbance should facilitate the reporting of actual disturbances. The SDT needs to ensure that some thought goes into the flow of information within the hierarchy and what triggers are needed to drive the reporting up the hierarchy.

	Yes
	A single approach is desirable, particularly for those entities that find themselves in multiple regions or countries.
	Yes
	Clarification, simplicity and the removal of duplicate reporting is beneficial.
	Yes
	Individual
	Steve Alexanderson
	Central Lincoln
	No
	The guidance document makes no distinction between entities that operate 24/7 dispatch and those that don't. The 1 hour and even the 24 hour reporting requirements in some cases will be impossible for entities without 24/7 dispatch to meet without changing business practices. These are the same entities that present little or no risk to the BES.
	Yes
	In the west at least, this hierarchy should be extended to include BA's as indicated in the Concepts Paper. See http://www.bpa.gov/corporate/business/reliability/Docs/2007/PNSC_RE_Data_Letter_2_070723.pdf for the RC's policy on which entities it chooses to communicate with.
	Yes
	The existing reporting is needlessly complex. We appreciate the SDT's goal.
	Yes
	The existing reporting is needlessly complex. We appreciate the SDT's goal.
	Yes
	An act of vandalism may have impact. An act of sabotage may not be impactful alone, but may be part of a wider coordinated attack. Dictionary definitions speaking of "intent" are not helpful in this regard, since acts of vandalism and sabotage are both generally committed intentionally. Saboteurs, though, work for a higher cause. That cause may be political, social, environmental, etc. We ask that the SDT look beyond dictionary definitions in developing a definition of sabotage.
	Individual
	Brenda Frazer
	Edison Mission Marketing & Trading
	Yes
	Yes
	Yes
	With the realization that having a common report form may be difficult to coordinate between differen agencies.
	Yes
	No
	There are too many special circumstances to try and capture. I feel this would be best delivered as a guideline.
	I don't know of any.
	No other comments.
	Individual
	Martin Bauer

USBR
Yes
The reporting outlined in the proposed plan does not include a clear indication of how NERC will use the information they collect from the entities. Care needs to be taken in addressing the reporting requirements to not create a more confusing or onerous reporting process.
No
The existing reporting methods collect reports of disturbances and analyze them by committees of the respective coordinating councils. The new process would introduce a duplicate layer and associated staffing. It would be better to ensure communication between the existing committees of the respective coordinating councils and the RC rather than creating a new layer of review tracking and analysis. While the layered reporting hierarchy discussed in the Disturbance Reporting section of the paper will eventually help with overall event awareness, the additional delays the hierarchical approach could result in a decrease in situational (timely) awareness. Having more comprehensive information as a result of the potential enhancements each layer adds to the chain of reporting may not be more valuable than timely and well disseminated information in an actual disturbance situation. We would suggest the SDT give careful consideration to this proposed direction. It may be appropriate to consider that expedited reporting of operational impacts would outweigh the benefit of administratively intensive reporting procedures. The events reported through the existing process have not yielded material feedback other than statistical analysis. Statistical analysis is not as sensitive to timely reporting. Operational impacts which may be the result of possible sabotage may be evident through assessment of widespread outage patterns or following event analysis. Comprehensive event analysis can take anywhere from 15 days to 90 days depending on the event.
Yes
The Bureau of Reclamation utilizes a form for tracking unexpected events. This form contains information which the agency considers important for its one reliability improvement program. The form is also used to meet NERC standard requirements for protection system operations analysis. This form contains most of information required by DOE. The SDT should consider requiring the submission of specific information rather than lock responses in one specific form. In this manner the agency would be avoid duplicate forms, one for NERC, the other for agency purposes.
Yes
It should be clear what information is to be supplemented. The fewer times the information has to be handled the more efficient the process becomes. If the information exists on a required form, that legal form should be allowed. Also, if the form is already submitted, then reference to it should be sufficient rather than requiring resubmission of the form. That would require handling the information again. As explained in the previous answer, the SDT should recognize that responsible entities have already developed internal reporting processes which utilize forms for consistent responses. Those forms may contain more information than is needed by the new standard to be proposed. The entity should be allowed to submit the internal form or else duplication would be created, which may reduce the effectiveness of an entities reliability improvement program.
Yes
There should be a clear distinction between a cyber event and a cyber event that has a material impact on the reliability of the bulk electric system. Not all CIP-008 events will carry such a distinction. That being said, CIP 008 cannot be completely incorporated in this process. Denying access to a cyber asset is noteworthy under CIP008 but may not pose a threat to the reliability of the bulk electric system. Consider recognizing the impact on the bulk electric system when modifying definitions of adding the bulk electric system description to the definitions. This will help to clarify that disturbances, as discussed in this effort, are situations that produce an abnormal condition on the electric power system, not necessarily on ancillary or supporting systems, such as SCADA systems or the water-related systems at hydroelectric dams.
The concept of "threat" evaluation criteria is somewhat vague and a great care is needed to ensure it is clear enough that the most individuals would be able to analyze an event and end up at the same threat. Otherwise it would be almost impossible to ensure compliance with a requirement which cannot accurately describe criteria to be used to ensure that proper evaluation has occurred.
Individual
John Alberts
Wolverine Power Supply Cooperative, Inc.
Yes
I agree with referencing existing guidelines - However: My concern is that, until all reportable incidents are anaylzed by the parties to which they are reported, their "impact" on the BES will not be quantified. Therefore, the tendency to want to "report all events so that their impact can be determined" or "report all events because the information can be utilized for informational purposes, regardless of impact on BES" might lead to expanded reporting requirements, some of which may have questionable value from a reliability standpoint.
Yes
From the persepective of a TOP, this seems to alleviate reporting burden and move it upline. I can understand the logic in wanting the reporting to flow through the RC for awareness purposes, but I can understand the RC's reluctance to bear the additional potential burden. Again, a focused effort to minimize the necessary reporting to 'true impact events" should be kept in mind, regardless of who has to report. Collecting reams of data and figuring out what

	impact it has later should not be the goal.
	Yes
	I can't see how anyone would disgaree with this concept - However - I question how practical it will be to implement, since various agencies would have to collaborate and coordinate to accomplish this task.
	Yes
	I agree with the concept of minimizing duplication - See previous question 3 for concerns.
	Yes
	I agree with the concept of focusing on impact instead of the type of event (sabotage, accident, vandalism, etc.) I hope that the reporting proposal that comes out of this project will clearly make a separation between true impact events that must be reported per the standards (enforceable), vs. "other" information that may be (electively - not enforceable) reported, per some set of guidelines.
	The concepts of removing duplication, consolidation, and focusing on "impact events" sound logical. I am concerned that the focus may drift to expanded reporting, not reduced reporting.
	Individual
	Thad Ness
	American Electric Power
	Yes
	Yes
	This approach may work as long as there is a uniform process across all of the Reliability Coordinators. AEP owns and operates BES facilities under three separate RCs and having differing rules and processes would create confusion and additional burdens. There are some concerns about the time lag of reporting the information and this might not work well in all cases especially if the information and knowledge are at the local level. AEP recommends that the standard could have a default hierarchy, but this should not prohibit any entity from reporting directly.
	Yes
	Yes
	Yes
	Individual
	James McCloskey
	Central Hudson Gas & Electric
	Yes
	Central Hudson agrees with using the “NERC Guideline: Threat and Incident Reporting” in the development of requirements. Central Hudson has currently in place a NERC-DOE Threat and Incident Reporting Table developed from this NERC Guideline that allows for a quick-reference to all threat and incident reporting criteria (arranged by category)with a cross-reference to the specfic reporting form (NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report, DOE Form OE-417, or NERC ES-ISAC Threat and Incident Report Form). Central Hudson recommends maintaining the option of utilizing only 1 form, the DOE Form OE-417, for incidents that require reporting to the DOE and NERC to maintain the streamlined approach to this reporting process.
	Yes
	Central Hudson agrees with this reporting hierarchy for disturbances given the "wider-view" of the Reliability Coordinator as opposed to an entity such as a Transmission Owner or Load-Serving Entity. While, based on past experience, the current process works if reports are filed to the DOE, RRO, and RC simultaneously via email for example. However, the RC is in a better position to identify multi-site incidents and escalate the reporting process if necessary.
	Yes
	Central Hudson agress with this goal if the intent is to develop and implement an electronic version that would meet DOE requirements as well.
	Yes

	Central Hudson agrees with this concept and, as stated in a previous response, recommends that the ability of utilizing the DOE OE-417 to supplement the NERC report be maintained.
	Yes
	Central Hudson agrees with this concept, particularly if the reporting hierarchy through the RC is implemented in order to better identify trends.
	Although not beyond the scope of these standards, NPCC maintains a document and reporting form (Document C-17 - Procedures for Monitoring and Reporting Critical Operating Tool Failures) that outlines the reporting requirements, responsibilities, and obligations of NPCC RCs in response to unforeseen critical operating tool failures.
	The NERC Guideline: Threat and Incident Reporting Attachment A matrix is an extremely beneficial document that organizes reporting criteria. However, it identifies communications systems failure sub-category under the Equipment And/Or Systems Failure category as reportable with a reference to OE-417 - Schedule 1, Item 10. Item 10 on Schedule 1 addresses only failures due to attacks (not failures for other resaons).
	Individual
	Deborah Schaneman
	Platte River Power Authority
	Yes
	Yes
	Situational awareness would be enhanced. All affected entities would be aware of the disturbance and relevant information. Also, the flow of information between entities would be enhanced and a more comprehensive report could be developed.
	Yes
	Yes
	Yes
	Individual
	Howard Rulf
	We Energies
	No
	While the NERC Guideline includes readily discernible information (and we would like to see that format carried forward into any future documentation), utilize OE-417 as the foundation document in order to eliminate reporting redundancies. If supplemental references are necessary for the proposed resolution, list the document as an official attachment to the standard. Minimize the need to search in multiple locations for guideline information – some may not be aware supporting documentation exists without explicit reference within the standard.
	Yes
	A hierarchical approach in conjunction with a single, electronic form would provide consistent reporting timelines, provide clarity in the reporting process, and provide more accurate and meaningful data submissions while having shared accountability. Confusion in the current method could be alleviated while providing more consistency in the reporting of an "impact event".
	Yes
	Agree in conjunction with proposed concept that DOE OE-417 will be allowed to supplement the NERC report in lieu of duplicating entries.
	Yes
	However, also evaluate whether or not DOE OE-417 is sufficient in lieu of a NERC report. If additional information is required, duplicate format of DOE-OE-417 with additional NERC information listed at the end of the form.
	Yes
	We would prefer to refer to all sabotage, vandalism, cyber attacks, and other criminal behavior as impact events. Focusing more on the event's impact on reliability and its ramifications on the systems seems to be more useful than to try to determine the intent of the perpetrator.
	What is meant by beyond the scope of the referenced standards? We Energies also has reporting obligations with the MISO RC (MISO OP-023), RFC (PRC-002-RFC-01), and the Wisconsin and Michigan Public Service Commissions.

	Give consideration to combining CIP-001 and EOP-004-1 through a common categorization. For example, “System Risk Reporting” could encompass both actual and potential events and would minimize the need to cross reference both standards, and provide one location for event and potential-event reporting. Much of the challenge in this project is in achieving a common understanding of the words sabotage and terrorism. There are nuances of meaning in the words that imply a relationship between the attacker and the victim, or a motive other than simple profit or mischief. This nuance of meaning requires the victim of the damage to discern a relationship or motive which may not be discoverable in the relatively brief time window during which the entity must report the event. In fact, they may never be known. Consequently, We Energies recommends elimination of the words sabotage and terrorism from these standards. We also recommend elimination of the word vandalism since it also implies an ability and duty to discern whether a particular act (barbed wire thrown over transformer bushings) was done out of pure mischief (vandalism) or with intent to destroy equipment for a political purpose (terrorism). And if the act was committed by a disgruntled employee, it becomes sabotage. No wonder there is confusion and indecision. Instead, We Energies recommends using the simple words “criminal damage”. One need not be a prosecuting attorney or FBI Special Agent to know what this means. Simply ask, “Does is look like somebody damaged it (or hacked in) intentionally?” and, “Did we give consent?” and you’re done. With elimination of sabotage, terrorism and vandalism, and all of their baggage, comes the ability to integrate both CIP 001 and EOP 004. We now have criminal damage (or cyber attack) as just another event to be evaluated against certain pre-defined impact measures. No value judgments, no speculation. Another benefit of using these simple words and tests is that operating personnel, whether in the field or at the console, will not require special awareness training in discerning these nuances of meaning. They already have experience with the equipment or cyber systems and its normal performance. Operating personnel can readily assess whether an impact event is due to equipment failure, weather or animal contact vs. intentionally caused by a person. If it appears to be criminal damage, call the local police agency. Report the event and the impact. Cooperate with the investigation. Share your knowledge of the normal condition of the equipment or performance of the system. Share your experience with similar events. It will be important to highlight that the theft of all the grounding pigtails in a substation is different from the act of simply snipping each of them to leave the equipment electrically floating. The technical condition is the same, but this allows the police to make an inference with respect to motive, suspect profile, sophistication, etc. That’s their job. They may ask us to speculate on the motive or skills of the attacker. That's okay. But at least we don't have to know or guess at it for the purpose of determining whether to report the event. No training required. With respect to notification to the FBI, We Energies recommends that the standard merely state that the owner of the damaged asset ensure the local office of the FBI is notified. The standard should permit documentation of either a direct phone call by the asset owner or obtaining an assurance from the local police that they will do so. There should be no need to prove earlier establishment of a relationship with the FBI. There should be no expectation that the entity have a signed letter from the FBI Special Agent in Charge acknowledging his agency’s duty. This document means nothing. With respect to reporting within the industry, We Energies recommends that the only events to be reported “up the chain” are those that we choose to characterize as “impact events”. That is, the events that meet some measurable threshold with respect to BES impact. We should describe these efficiently to avoid over-reporting of trivial events. It is apparent that we are already over-reporting since DHS HITRAC recently fed back to the industry that copper thieves attacked a substation in San Bernardino, CA taking some of the grounding conductors. The industry should have the option to report non-impact events that are unusual in some respect and which may have some mutual industry benefit in terms of prevention, awareness or recovery. Attack attempts with no impact, or observations of suspicious activity could fall into this optional category. These optional reports could be aggregated by the entity for the purpose of detecting patterns or trends, or be reported ad hoc. The ES-ISAC should be the recipient of the reports. It should be the single point of contact since it has the industry insight, engineering expertise and cross-sector relationships to analyze and return valuable intelligence to the industry. With the ES-ISAC as the recipient of the reports, efficient sharing with Federal agencies, with the regional entities and with neighboring asset owners could be automated and rapid. There is much benefit to be gained from this project, primarily in the area of creating clarity and uniformity. There is some risk that the reporting requirements will become onerous and prescriptive.
	Individual
	Jianmei Chai
	Consumers Energy Company
	No
	The existing guidelines ignore the fact that there are currently three overlapping and inconsistent reporting requirements for disturbances of various types: CIP-001, EOP-004, and DOE OE-417. The reporting should be such that any single event type needs to be reported only once, and to only a single agency, for any disturbance. First, CIP-001 events should be reported to the ES-ISAC under one specific requirement (or set of requirements) and removed from OE-417 and EOP-004, such that all interested agencies obtain their information from only that one source. Second, OE-417 events should be reportable ONLY to DOE, and, again, other agencies should obtain their information from only that one source. If NERC wishes to make such reporting mandatory and enforceable, the NERC requirements should indicate ONLY that such reporting should be made in accordance with OE-417. Finally, EOP-004 (or similar requirements) should require reporting to NERC ONLY in the case of events that don’t fit under CIP-001 or OE-417 requirements. Alternatively, OE-417 should be submitted ONLY to NERC and they should disseminate the information. EOP-004 has several issues and inconsistencies: a. EOP-004 requires that the entity that submits form DOE-417 to provide copies to NERC. The DOE-417 form intermixes NERC entity definitions (e.g. BA, LSE, TO) with generic terms such as “Electric Utilities” and “Generating Entities”. Is it the Generator Owner or Generator Operator that is required to submit the information? There should be one form or at least well defined definitions that apply to both forms. b. EOP-004-1 R3.1 requires submittal within 24 hours, however Table 1-EOP-004-0 which purports to summarize the standard appears to change this requirement to 1 hour for several disturbances. Additionally, it incorrectly summaries the reporting time for 50,000 customers, which is 6 hours in DOE-417 and summarized in Table 1-EOP-004-0 as 1-hour. An attachment to a standard should not be allowed to supersede the standard or create additional rules. c. EOP-004-1 R3.1 requires submittal within 24 hours, however Table 1-EOP-004-

	0 which purports to summarize the standard appears to change the standard. R3.1 clearly states that events are to be reported within 24 hours of identification, however Table 1-EOP-004-0 state that the events are to be reported on the basis of the start of the disturbance. An attachment to a standard should not be allowed to supersede the standard or create additional rules. d. EOP-004-1 R3.1 requires submittal within 24 hours, however Table 1-EOP-004-0 which purports to summarize the standard appears to change the standard. R3.1 clearly states that events are to be reported within 24 hours of identification, however Table 1-EOP-004-0 states that copies of DOE-417 are required to be submitted “simultaneously”. It also states that schedules 1 and 2 are due within 24 hours of start of the event instead of 48 hours for per DOE-417 for schedule 2. An attachment to a standard should not be allowed to supersede the standard or create additional rules. e. The requirement of loss of customers should be scaled based on customers served. Loss of 50,000 customers to a utility that serves 100,000 customers is different than loss of 50,000 customers to a utility that serves 2,000,000 customers.
	No
	It would be inefficient for RC’s to accumulate ALL disturbance data and submit it, and to bifurcate the reporting based on type of disturbance above and beyond OE-417 data (which should go ONLY to DOE) would make a standard very involved for an entity to comply with. We’re discussing after-event data here, not data needed for current operations – and there’s no reason to make it any more complicated than necessary.
	Yes
	Agreed – to the extent that it’s consistent with the concept that any specific type of data is submitted to ONLY one entity.
	No
	NERC should either coordinate with DOE for a single reporting process or simply adopt the DOE’s standard.
	Yes
	We agree with the concept, however, based on the information provided, it may be too vague to be of value. Terms such as “potential” and “significant” can be subjective and therefore provide little direction. We would like to see something more specific. Also, inclusion of the destruction of BES assets may be too inclusive and needs to be restricted to BES assets that will cause a specific level of impact on reliability.
	Group
	Western Electricity Coodinating Council
	WECC
	Yes
	It is comprehensive; however, we must keep in mind that the OE-417 is required under Public Law 93-275 and needs to be attached if applicable in the US.
	Yes
	There should be an established time sequence that allows the RC to review the entities material prior to forwarding to NERC. By channelling all reports through the RC situational awareness will be enhanced. Instead of "submit information", it should be clarified that entities submit complete written reports to RC in electronic format.
	Yes
	Canadian and Mexican entities should be consulted on content of report form to assure their "buy in".
	No
	This will work well for the USA entities to save us time in re-entering the same information. We believe that FERC and NERC and the Regions should have one common reporting form for North America. The OE-417 is not required by law outside of the United States. Canadian and Mexican entities may feel that US DOE has no juristiction in these countries, and therefore no right to required reporting as is stated on the OE-417.
	Yes
	This will help eliminate regional differences in sabotage reporting. The definition should be broad enough so it covers new types of sabotage that may evolve. Event analysis facilitates situational awareness and if it requires further investigation regarding developing patterns and severity, it should be handled by law enforcement if need be.
	There is a need to learn what reporting requirements are required by the Mexican and Canadian entities.
	As stated previously, for "One stop shopping" we need "buy in" from the foreign nationals. The way to do this is to engage their opinions and respect their juristictional agencies as well.
	Individual
	Amir Hammad
	Constellation Power Source Generation
	Yes
	The existing guidance is an excellent base on which to build changes to EOP-004 and CIP-001. However, the SDT

	must challenge each item in the different event categories and clarify or omit bullet points that are seemingly vague. For example, under System Disturbances, a forced outage report is needed when “a generation asset of 500 MW or above is on a forced outage for unknown reasons, or a forced outage of generation of 2,000 MW occurs…” Simply removing the 500 MW criteria would make this criterion less vague. There are other examples of this in the guideline.
	Yes
	As stated in the concept paper, a hierarchy ensures proper communications, but it has the added benefit of reducing redundancy on the Registered Entities, so long as responsibilities and accountability are clearly established.
	Yes
	Yes
	Constellation agrees with the concept of eliminating the need to file duplicate reports. If the single NERC reporting form is both comprehensive and easy to use, then using a single report should not be an issue. It is essential that all elements of DOE OE-417, and any similar documents, be incorporated into this single report. Not incorporating all elements will result in gaps in reporting for all Registered Entities.
	No
	Although defining an impact event would bring clarity to defining sabotage events, adding another situation would further complicate things. Furthermore, the examples of impact events used all fall under the Sabotage category in the Threat and Incident Reporting Guideline. Constellation Power Generation suggests the SDT further clarifies the items in the Sabotage category to ensure all grey area situations are included. Clarification is also needed in how a Cyber Security Incident (CIP-008) would map into the categories of Disturbance/Impact Events (CIP-001). To that point, Constellation Power Generation questions whether cyber related incidents should fall under the spectrum of sabotage type events, or remain separate and be incorporated in the CIP revisions. Having cyber related incidents separate from other sabotage events would provide the clarity and guidance that the DSR SDT is striving to achieve.
	Constellation Power Generation would like clarification that any proposed CIP-008-related reporting requirement (including any linked reporting requirement between CIP-008 and CIP-001) is only applicable in situations where the incident/event involves a registered entity’s Critical Cyber Asset. In that vein, we want to emphasize the importance of the DSR SDT working with the CIP SDT on the cyber related events. If the DSR SDT is going to be adding clarity to cyber related events, then coordination with the CIP SDT is needed to ensure the same verbiage is being used. Furthermore, having any duplication of requirements will cause a double jeopardy scenario which would go against the SAR for the DSR SDT. As stated earlier, Constellation Power Generation also questions whether cyber related incidents should fall under the spectrum of sabotage type events, or remain separate and be incorporated in the CIP revisions.
	Group
	Public Service Enterprise Group Companies
	PSE&G
	Yes
	EOP reportable disturbances are familiar concepts in the industry.
	Yes
	The PSEG Companies believe that all entities with a reportable disturbance should report to the RC. The RC is best positioned to evaluate the impact of the event and forward the information to the appropriate entities. There should not be any intermediate entities to relay information to the RC as that can introduce delay and has the potential to introduce transcription errors. Sabotage events should be reported to the RC as well as to law enforcement. CIP-008 reporting is highly specialized and should be retained in the set of cyber security standards, not merged with CIP-001 and EOP-004.
	No
	While simplification and consistency is a laudable goal, it should not be applied to different governmental agencies (USA, Canada, Mexico) which may have different structures and processes. Moreover, results based standards should not include administrative matters such as reporting forms.
	Yes
	The PSEG Companies agree with the avoidance of duplicate reports. NERC report forms should not include anything in the DOE form, and NERC Regional report forms should not include anything in the DOE or NERC forms. Hence, a DOE report should not "supplement" a NERC form, but rather replace it unless the NERC form calls for other information for the same reportable incident, and likewise for the DOE - NERC - Regional form structure. DOE forms would be filed with DOE, NERC and the Regional Entity where the event originated. NERC forms would be filed with NERC and the region where the event originated and the Regional form filed only with the Region. In designing the NERC and Regional forms, the need to file multiple reports should be minimized, and in no event should any of the three (DOE, NERC, Region) forms contain duplicative information requests.
	Yes
	The PSEG Companies agree with the concept, but reserve judgment on the descriptions of the impacts. There is clearly a need to better define what constitutes a sabotage incident versus common theft or vandalism. Moreover,

	where it may be impossible to determine if any given incident (e.g., several loose bolts on a transmission tower cross brace could be sabotage or could be human error in construction) falls within sabotage, a registered entity should not be second guessed in an audit if the registered entity determines not to report. Excessive unnecessary reporting can mask real incidents.
	The PSEG Companies believe that RFC is developing a regional disturbance reporting requirement for events not meeting the criteria of current DOE and NERC reports.
	If reporting does become the responsibility of the Reliability Coordinators, the RCIS should be made available view-only to registered entities with a notification when RC's have posted new entries. That will enhance the situational awareness of registered entities. The PSEG Companies disagree with inclusion of CIP-008 reporting requirements as part of the CIP-001 and EOP-004 initiative. CIP-008 reporting as part of the cyber security set of NERC standards is usually managed by specialized corporate organizations separate from those involved with the other NERC standards, and with highly specialized cyber skill sets. CIP-008 reporting requirements should remain where they are, and any perceived need for improvement addressed in the ongoing CIP Version 4 development process.
	Individual
	Greg Rowland
	Duke Energy
	Yes
	No
	The RC should not be responsible for submitting the report to FERC, NERC or the RRO. The RC may not have the necessary first hand information concerning the facts of the event. Situation awareness can be maintained by including the RC in the distribution of any sabotage related reporting.
	Yes
	There should only be one report for all functional entities to submit to NERC.
	Yes
	Since the OE-417 is a DOE required report, it must be submitted. Including the OE-417 as part of the NERC electronic form will facilitate reporting to NERC.
	No
	As FERC ordered in Order No. 693, the drafting team should further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event. Suggested definition: “Sabotage – the malicious destruction of, or damage to assets of the electric industry, with the intention of disrupting or adversely affecting the reliability of the electric grid for the purposes of weakening the critical infrastructure of our nation.”
	None
	We don’t think CIP-001, EOP-004 and cyber incident reporting aspects of CIP-008 should all be combined into one standard, because of the significant differences between sabotage and disturbances. We have suggested that the drafting team further define sabotage, and we have included a suggested definition in our response to question #5 above. Sabotage is very specific due to the intent (for the purpose of weakening the critical infrastructure), and the potential impact to the BES. We believe that sabotage and cyber incident reporting should remain a part of the CIP Standards due to the emphasis placed on the criticality and vulnerability of the assets needed to support reliable operation of the BES. Cyber Security and Physical Security could be placed together in the same standard (remain in CIP) and other disturbances (i.e., accidental, natural) in a separate standard. “One stop shopping” for reporting is still possible as long as the OE-417 form is included as part of the NERC electronic form. And while we agree with the need for additional clarity in sabotage and disturbance reporting, we believe that the Standards Drafting Team should carefully consider whether there is a reliability-related need for each requirement. Some disturbance reporting requirements are triggered not just to assist in real-time reliability but also to identify lessons-learned opportunities. If disturbance and sabotage reporting continue to be reliability standards, we believe that all linkages to lessons-learned/improvements need to be stripped out. We have other forums to identify lessons-learned opportunities and to follow-up on those opportunities.
	Group
	ERCOT ISO
	ERCOT ISO
	Parts of the Guideline are helpful, but the guideline goes beyond the scope of the requirements of the current standards, which could pose potential audit concerns. ERCOT ISO strongly feels this approach for reporting should be focused on physical events only and cyber event reporting should be contained within CIP-008 only. Continue to keep physical separate from cyber.
	No
	There are some events that are truly local and should be handled by local entities and reported to local authorities (i.e. theft). If there is an impact or potential to have an impact to the BES or to the region, then hierarchical reporting would be appropriate.
	Yes

	Standardization ensures consistency and relevance of the information received.
	ERCOT ISO agrees with the concept of eliminating the need to file duplicate reports, but as stated in the Concept Paper, the DOE form (OE-417) is required by law. Based on this, the elimination of EOP-004 (after the fact reporting) is essential, since the OE-417 is mandatory and all-inclusive.
	ERCOT ISO recognizes the risks associated with “gray areas” not being clarified. While “gray areas” pose compliance risk due to differing interpretations, a risk remains that some items will go unreported. A more prescriptive approach raises an even greater risk of events not being reported. People will not report events that are not specifically listed, and will not use judgment in determining the need for reporting.
	All references to CIP-008 should be removed and we reassert that physical and cyber reporting should be separate. There is documentation available from the CIPC that the drafting team considered CIP-001 related physical sabotage reporting and specified cyber incident reporting requirements in CIP-008. ERCOT ISO requests the DSR SDT to continue to improve its guidelines and to post those guidelines for all to use, but not to create sanctionable standards whose good intentions could result in unintended adverse consequences for the Industry. ERCOT ISO also suggests that all reporting forms and guidance should be located in a central, easily accessible location, eliminating confusion and simplify reporting for system operators thereby directly enhancing reliability during system events. The industry would benefit from a central location or link on the NERC website containing all reporting forms.
	Group
	ISO RTO Council Standards Review Committee
	IESO
	Yes
	The guidelines in EOP-004 and its attachments should be retained as the foundation for reporting disturbances. One would note that such EOP Disturbances are relatively well defined reliability impacts. Thus EOP-004 disturbances are based on HOW certain events impacted the BES. [Sabotage on the other hand requires an implication of WHY an event occurred.] The original EOP-004 represents a common sense approach to defining reliability events that may be useful to analyze on a regional basis. In the current environment, Regions are not sanctionable entities but they still are valuable sources to collect, analyze and trend the few disturbances that occur in each region. To make use of Regions, however, precludes the use of sanctionable NERC standards. EOP-004 as written does not meet the NERC requirements for standards but it does meet the Industry needs for a guideline for reporting events that deserve to be reviewed. The SDT should propose deleting EOP-004 and use it as a Disturbance Reporting Guideline.
	No
	The idea of a reporting hierarchy provides an easy to follow pro forma approach. But disturbance reports should not always follow a common reporting path. A disturbance on the transmission system for example need not be routed through an “if applicable” Balancing Authority. To mandate that a BA be in the path is inappropriate. To leave the applicability open is to create a subjective compliance problem for the impacted BA. Copper theft is another example that should not require reporting up through the RC. It is a local issue and the Transmission Owner should be able to report this directly to the appropriate parties. How would a DP, LSE or GO know if an event is an “impact event”? The posed impact events are a series of conditions for sabotage but not for EOP-type disturbances. The aforementioned entities have no requirement to monitor and analyze the BES, which then means every event would be an impact event for those entities (not an EOP disturbance but an impact event). Thus every theft of copper is an impact event mandating a Disturbance Report even though the SDT notes the RC only has to send it to the “local authorities”. This seems to be a misuse of the RC resources; every train derailment is an impact event requiring a Disturbance report (is that a commercial train, regional rail line a local trolley car); every teenage prank would also generate an impact event mandating a disturbance report. The SDT defined impact events are not appropriate for use in defining disturbances. There is a big difference from creating a set of guidelines to follow as opposed to creating sanctionable standards
	No
	The SRC supports NERC’s initiative for Results Based Standards. The SRC understood RBS to mean the results were reliability based quantities not administrative quantities. There is no need for a NERC Reliability standard on reporting. The idea that all functional entities in each of the said countries will use one form would be a good idea if and only if all the countries and all of their agencies were willing to accept that form. The SRC does not believe that those agencies will be willing to cede what information they ask for to NERC; nor that NERC will be able to create a single form that all such agencies will accept.
	No
	The concept of eliminating duplication is laudable, but the idea of writing a standard to mandate reporting that involves reporting to governmental areas does not make sense unless NERC will do all of the reporting for the Industry. A governmental agency is as likely as not to change the forms they require which would then mean two different reports (one for NERC and one for the given agency) or that the standard would have to be re-written every time there is a change.
	No
	The nature of the fact that “gray areas” exists preclude the idea of using a standard to report; particularly a standard for the vague topic of motivation such as sabotage events and the more defined disturbance events.
	The FERC Order merely asked NERC to “further define sabotage and provide guidance as to the triggering events

	that would cause an entity to report a sabotage event." There is no requirement to create a Reporting Standard and no mention of Disturbance events. There is a strong need to avoid heavy-handed use of NERC standards particularly for such post event reporting guidelines. The SRC would urge the DSR SDT to continue to improve its guidelines and to post those guidelines for all to use, but not to create sanctionable standards whose good intentions will inevitably result in many unintended adverse consequences for the Industry. Rather, the SDT should seek to retire sanctionable requirements that require event reporting in favor of guidelines for reporting.
	Group
	Bonneville Power Administration
	BPA, Transmission Reliability Program
	No
	BPA likes the idea of consolidating information and eliminating duplication of reported information. In the report, don't include every detail possible found in the "Threat Guideline". TOP's are supposed to be operating the electrical system, not doing investigative work for copper theft incidents (see comment on #5).
	No
	The RC is made aware of these type of incidents and goes right back to incorporating that in their awareness and to focusing on system reliability. If the RC is the recipient for further distribution of information of this type they will be forever going back for more information. Eliminate the middleman in whatever concept you propose, folks have plenty to do now. Let people make good judgments with the direct field people on the seriousness of the breach with their security personnel contacting the appropriate law enforcement agency. (Or are you looking to do a simple RE reports to the RC who marks various category items on a secure website Yes/No category item indicator that can be rolled up in ES-ISAC mapboard.?)
	Yes
	As long as we don't make one form that requires extraneous information for the sake of having agreement.
	Yes
	Minimizing the number of reports is a good thing. The concept of actually sharing information should be utilized as much as practical.
	Yes
	BPA agrees with providing an industry-wide definition and guideline. We do NOT agree with requiring reports for every instance of every activity. If your definition is good, you'll get what is needed and not much chaff.
	Individual
	Kirit Shah
	Ameren
	Yes
	We agree that it makes sense to build upon existing documentation. However, we do not believe it is necessary to require event reporting to be in an enforceable standard. Rather the drafting team should consider developing a reporting guideline document and retiring the EOP-004 standard.
	Yes
	The heirarchy is appealing in the fact that the TOP/BA will be kept in the loop and receive critical information from the Generators, Distribution, LSE, etc. But there will be an inherent delay in reporting due to the fact that at every hand-off of information there will be questions for additional and/or clarified information, and there is always a possibility for the loss of information due to the transfer from one entity to the next. Further, this reporting through a heirarchy could also take away from the operators ability to respond to system events due to being tied to an information transfer ladder.
	Yes
	One report would be great for this standard. While this standard needs simplification and automation, we strongly suggest developing a guideline for reporting rather than enforceable standards.
	No
	The DOE OE-417 report should not supplement the NERC report due to the fact that the majority of reportable events are defined in/come from the OE-417 report. The NERC reporting form should be based on the OE-417 report and then include additional reporting requirements defined by NERC. However, it does not make sense to require reporting to the governmental agencies through enforceable NERC standards. The governmental agencies already have legal authority to compel reporting.
	While we are not opposed to the concept of identifying impact events, we are concerned that the drafting team may actually be expanding reporting requirements. We do not support expansion of reporting requirements unless a clear

	reliability or legal need is identified. Some of the impact events are almost never sabotage and do not warrant reporting for reliability needs and should not be included. For example, copper theft should not require reporting, in general, because it is almost never sabotage and rarely impacts reliability. If it does impact reliability because, for example, the protection system is impacted and causes more significant potential contingencies, then reporting could be required. Why is a train derailment near a transmission right of way significant? It would only be significant if an investigation identified sabotage as the reason. Furthermore, what is considered near?
	Group
	Midwest ISO Standards Collaborators
	Midwest ISO
	Yes
	We agree that it makes sense to build upon existing documentation. However, we do not believe it is necessary to require event reporting to be in an enforceable standard. Rather the drafting team should consider developing a reporting guideline document and retiring the EOP-004 standard. This is further supported by the fact that there is a role in the existing standard for the Regional Entities even though these requirements can't be enforced against the Regional Entities because they are not a user, owner or operator of the system.
	No
	We do not agree with developing a hierarchy for reporting for all disturbances and impacting events. For instance, copper theft is an example of an item that should be reported to the appropriate entities directly by the Transmission Owner. The RC does not need to be made aware of every copper theft unless it has a direct impact on reliability (affects rating, protection system, etc.) and the RC should not be burdened with expending resources for this reporting. A further example in which the hierarchy is not needed would be the case in which only one entity is impacted. If a significant event occurs on one TOP's system, then the TOP should be able to handle the reporting of all entities under its purview.. If more than one TOP is involved, then it would be necessary to involve the RC in the reporting.
	Yes
	We agree with the goal of having a single report form but believe there will be a significant challenge to get varying governmental agencies to agree on single report format.
	No
	It certainly makes sense to eliminate duplication in reporting and to allow supplemental information to be submitted in other reports. However, it does not make sense to require reporting to other governmental agencies through NERC enforceable NERC standards. Those governmental agencies already have legal authority to compel reporting. Again, we support developing a guideline for reporting rather than enforceable standards. The guideline could certainly explain the various reporting requirements and supplemental reporting requirements mentioned in the question without causing the issues we have identified in our comments.
	No
	We agree with the idea of identifying impact events but do not support the requirement for these to be always reported through the hierarchical structure identified in question 2. If an impact event only affects one entity, that entity should have the reporting requirement.
	While we are not opposed to the concept of identifying impact events, we are concerned that the drafting team may actually be expanding reporting requirements. We do not support expansion of reporting requirements unless a clear reliability or legal need is identified. Some of the impact events are almost never sabotage and do not warrant reporting for reliability needs and should not be included. For example, copper theft should not require reporting, in general, because it is almost never sabotage and rarely impacts reliability. If it does impact reliability because, for example, the protection system is impacted and causes more significant potential contingencies, then reporting could be required. Why is a train derailment near a transmission right of way significant? It would only be significant if an investigation identified sabotage as the reason. Furthermore, what is considered near?
	Group
	FirstEnergy
	FirstEnergy Corp.
	Yes
	This guideline appears to be a good starting point for developing consistency in reporting. However, we believe that after-the-fact event reporting is administrative in nature and seldom rises to the level of mandated reliability standard requirements. It is not clear what reporting would be made through this effort and how it differs from reporting made through the NERC Reliability Coordinator Information System (RCIS). With the initiative for more results-based standards being the goal of NERC, true after the fact reporting-type requirements should become administrative procedures and only be included in standards if they are truly required for preserving an Adequate Level of Reliability. If there are aspects that rise to be retained in a mandatory and enforceable reliability standard, we propose that those associated with sabotage be moved to CIP-001 and that EOP-004 be focused on operational disturbances that warrant a wide area knowledge. However, if the RCIS is the mechanism to convey real-time information and that is presently occurring outside of reliability standards, it is unclear what the delta improvement this project aims to achieve.

	No
	While we appreciate the team's effort to serialize the reporting process, with the electronic communication methods available today, it seems that reporting can be accomplished simultaneously to multiple entities without shifting the burden of reporting to others along the communications path. This is particularly true if the reporting format is standardized to a one-size-fits-all report. Additionally, it would be a great burden to the Reliability Coordinator to review all events perceived by entities to be malicious sabotage events.
	No
	While one consistent form for reporting may simplify reporting requirements, it would be very difficult to get all governmental agencies to agree to a one-size-fits all approach.
	Yes
	We agree that the simplification and consistency of reporting will improve the reporting of this information. We support the drafting team's efforts in this area and hope that all regulatory agencies will as well. However, as we have mentioned in our other comments, the reporting requirements should not be in a reliability standard unless they are proven to be necessary to maintain an Adequate Level of Reliability of the BES. Reporting of these events should be required by NERC in arenas outside of the standards.
	Yes
	The concept paper makes good progress in this area and the drafting team is on the right track, and agree that better clarity needs to be developed surrounding sabotage events. However, some of the examples stated in the paper are too vague and do not address extenuating circumstances or reasons for the events. One example sighted in the paper is "Bolts removed from transmission line structures." This statement may be too broad. For instance, if the bolts are removed from the tower and the organization is not experiencing a labor dispute, it could be considered a sabotage event with wide area implications. However, if the organization is in the middle of a labor dispute, this would be vandalism and would most likely not be of a wide area concern. Also, the number and location of towers affected could be an important determination related to the risk the event imposes on the Bulk Electric System.
	We fully agree that sabotage events need to be more clearly defined and reporting requirements need to be better coordinated. But as we have stated in previous comments, the drafting team needs to determine if standard requirements need to be developed for this type of reporting or if this is better left to administrative requirements outside the standards arena. Also, while we appreciate the team's effort to simplify reporting requirements for entities, we are concerned with the serial communication offered by the concept paper. As an example, the team proposes to have LSE report the incident to the BA and/or TOP and then have the BA and/or TOP report it to the RC and the RC to report it to NERC and the NERC report to the regulatory agencies. While this simplifies it for each individual organization, this method introduces many opportunities for errors and miscommunications. Since this is after-the-fact reporting, it is difficult to defend this type of communication path when one consistent report could be sent simultaneously to all agencies at the same time from the originating location.
	Individual
	Dan Rochester
	Independent Electricity System Operator
	Yes
	Yes
	We do not agree with the need of such a hierarchy setup solely for the purpose of making reports to the need-to-know entities. All responsible entities (RC, BA, TOP, etc.) need to file a report. With the proposed set up noted under Q3, which we support, these reports should go directly to NERC. The RC should not be held responsible for forwarding other entities' reports to NERC, and in doing so subject itself to potential non-compliance.
	Yes
	Yes, this will simplify the reporting effort. NERC may forward the reports to the other need-to-know entities.
	Yes
	We support this concept since it works well for those entities that are not required to file reports with the US agencies, e.g. the DOE.
	Yes
	We agree with the general concept. However, we suggest that the classification of "events" to be compatible if not identical to those which need to be reported in real time as required in CIP-001, for otherwise it will create confusion and unnecessary, extra work. Also, this proposal appears to focus on the sabotage-type events only but the SAR deals with both sabotage and other disturbances (e.g. emergency type of events) reporting. A parallel type of "impact event" is needed for non-sabotage-type of events.
	In the Background Section of the comment form, it is indicated that the SDT "…is NOT seeking input or guidance on the definition of physical or cyber sabotage, what type of disturbances should be reported, who should do reporting, or to whom or what organizations will be receiving the reports." Yet there are proposed definitions, with examples, in the concept paper. The SDT should make it absolutely clear that by supporting the general concept as described in

	the paper, the commenting entities are not endorsing the proposed definitions, nor the examples as elements to be included in the standard.
	Individual
	Roger Champagne
	Hydro-Québec TransÉnergie (HQT)
	Yes
	In considering guidance found in the document “NERC Guideline: Threat and Incident Reporting”, the SDT should maintain focus on only those items that are absolutely necessary to maintain the reliability of the Bulk Electric System. In fact, the purpose of reporting per EOP-004 is that disturbances... need to be studied and understood to minimize the likelihood of similar events in the future.
	Yes
	Having the reporting flow through the Reliability Coordinator supports the reliability objective of assessing, monitoring, and maintaining a wide-area view of the reliability of the Bulk Electric System. The reporting hierarchy should be to submit the information to the Reliability Coordinator, and to have the RC submit the report. This would eliminate the duplication of information.
	Yes
	We agree with the concept that there should be one report form for all functional entities (whether located in the US, Canada, Mexico) for use in reporting to NERC. This would provide for a consistent reporting format across the continent.
	Yes
	We agree with the objective of eliminating duplicate reporting. However, EOP-004 currently allows substitution of DOE OE-417 in place of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report. As suggested in the Concept Paper, entities meeting the criteria of OE-417 are still obligated to file a report with DOE. Given that and the fact that CIP-001 requires no actual reporting, it is not clear where duplication exists today. We agree with the recommendation to eliminate the need for filing duplicate reports such as the DOE form OE-417. There is no benefit with regard to CIP-001 in filing separate reports. Duplicate reports introduce the potential for incomplete information to be supplied to responsible parties. Removing jurisdictional agencies from the Standard, and having NERC provide either query or situational awareness to those agencies being considered, might not be easy to achieve. There is an obligation under law to require entities to report to the DOE on the OE-417 form as amended or modified. This might drive the “omitted” agencies to have reporting laws enacted as well.
	No
	We believe that physical and cyber events must be investigated before a determination of sabotage or impact event can be made. The purpose of the NERC Standards is to maintain the reliability of the BES. Therefore, impact events should define or clarify the circumstances that would or could affect reliability. Reportable items should be based on impact to reliability, not on ‘newsworthy’ events or to gather information for trending. It is the law enforcement industry’s responsibility to make a determination of “sabotage” or other. This determination cannot definitively be made by industry personnel, there is no expertise or time to investigate causes. It is the industry’s job to mitigate effects. Examples would help provide for better guidance/direction. Industry examples would be welcomed to help reinforce developed internal processes for compliance.
	SERC and RFC are developing additional requirements at this time. We suggest that reporting be based on impact to reliability, not on ‘newsworthy’ events. We therefore do not agree with such regional efforts and would prefer a continent wide reporting requirement.
	a. NERC should focus efforts on developing specific event reporting criteria and not base the requirement on the definition of the term ‘sabotage’, but on the reporting criteria itself. See comments above. b. The “opportunities for efficiency” discussed in the Concept Paper would be best achieved by focusing on those items that are absolutely necessary to maintain the reliability of the Bulk Electric System. If there are elements that need to be reported that do not support this objective, then that reporting should not be required in reliability standards. Consider making NERC the distributor of reports to other agencies. We recognize that the key is to simplify reporting to a single form, and to the extent possible, to one agency. “Front line” reliability personnel must have the “timely” knowledge to know when a situation warrants local, area, regional, or national involvement. Finally, the SDT should keep in mind the fact that Canadian stakeholders might have some difference in the way reports are made to Security Agencies.

Consideration of Comments on Disturbance and Sabotage Reporting — Project 2009-01

The Disturbance and Sabotage Reporting Standard Drafting Team thanks all commenters who submitted comments on the proposed Concepts Paper for Disturbance and Sabotage Reporting. The document was posted for a 30-day public comment period from March 17, 2010 through April 16, 2010. Stakeholders were asked to provide feedback on the standards through a special Electronic Comment Form. There were 41 sets of comments, including comments from more than 95 different people from approximately 50 companies representing 8 of the 10 Industry Segments as shown in the table on the following pages.

The comments have been sorted and organized by question number in this report; the comments are shown in the original format on the following project web page:

http://www.nerc.com/filez/standards/Project2009-1_Disturbance_Sabotage_Reporting.html

Summary Consideration:

Use of "NERC Guideline: Threat and Incident Reporting"

Most stakeholders agree that existing guidance should be used as the foundation for disturbance reporting. Most commenters felt that the "NERC Guideline: Threat and Incident Reporting" document contains a lot of detailed information which greatly assists in determining reporting events and weaning out non important events. The most common desire was one, common form to be used for reporting and the OE-417 was considered to be a good starting point. Most respondents thought the form could be streamlined. The DSR SDT was urged to focus on applicable events and reporting timelines which are not clear now and to report items that are clearly essential to the reliability of the BES. There was some concern expressed about "over-reporting", out of fear of non-compliance rather than the over the reliability of the BES. There was also a clear desire to separate out vandalism & copper theft from reporting requirements.

Hierarchy for Reporting Disturbances

Most stakeholders (about 2/3) agree with the concept of developing a reporting hierarchy for disturbances. Stakeholders who disagreed believed that the RC should be one of many to receive information on impact events (DOE, RRO, etc.). Such a hierarchy would lead to reporting delays (leading to lack of situational awareness), be cumbersome and complicated and clouds responsibility for who is to report what to whom. Other negative comments believed that a hierarchy would distract the RC's focus from its primary responsibility. Those stakeholders who agreed commented that the RC should be the collection point for reports and information and take the responsibility to forward as required. This is from the concept that the RC has the "wider view" and can recognize patterns, and has the ability to "escalate" the reporting process. This would also minimize duplication of reports and information.

Single Form for All Agencies

Most stakeholders agreed with the concept of having one reporting form for all entities. Several commenters suggested that there is no need for a standard on reporting as they considered it administrative in nature. Most dissenters thought there should be a guideline, rather than an enforceable standard. There is widespread agreement that the one-size-fits-all approach would be very difficult to get agreement on, given the different countries and

agencies involved. Many stakeholders pointed out that consistency and simplification were drivers for one report form. Having multiple recipients, with different information requirements, seems to support an electronic format that would guide information only to those who need it. The concept of an electronic reporting tool will need to be further vetted and developed.

Supplements to NERC Form

Most stakeholders agreed with the concept of entities being able to use information from other sources such as the OE-417 form, to supplement the NERC report form. Some thought that duplicate reports were acceptable, as long as the information was not duplicated (if # of customers lost is required on form A, don't ask on forms B & C). Several stakeholders commented on the need for an electronic, one stop reporting tool. This would avoid duplication while ensuring that the information reported goes only to intended recipients. With an electronic, one stop reporting tool, reports can be updated/corrected instantly, without repeating previously submitted information. Some stakeholders cautioned that the OE-417 can change every three years and this should be taken into account when developing an electronic reporting tool. Again, such a reporting tool would need to be vetted and developed to meet reliability needs.

Impact Events

The majority of stakeholders agreed with the concept of "impact events." Some stakeholders felt that the introduction of impact events increased the risk that some items will go unreported. However, most felt that impact events would dramatically increase the number of reports being submitted, and it would be difficult to separate important information from background noise. Several respondents felt that the SDT ignored the FERC Directive, and did not define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event. Many respondents supplied the SDT with their own definition of "Sabotage". The DSR SDT believes that the concept of impact events and the specificity of what needs to be reported in the standard will be an equally efficient and effective means of address the FERC directive regarding sabotage. Some stakeholders felt that impact events add another layer of uncertainty to the reporting. Even with the switch from sabotage to impact events, several felt that "intent" was still key to determining reportability.

Regional Differences

Several commenters provided information on regional reporting. The SDT will consider whether these should be included in the continent-wide standard. These include:

1. NPCC maintains a document and reporting form (Document C-17 - Procedures for Monitoring and Reporting Critical Operating Tool Failures) that outlines the reporting requirements, responsibilities, and obligations of NPCC RCs in response to unforeseen critical operating tool failures.

2. For other events that do not meet the OE-417 and EOP-004 reporting criteria, ReliabilityFirst expects to receive notification of any events involving a sustained outage of multiple BES facilities (buses, lines, generators, and/or transformers, etc.) that are in close proximity (electrically) to one another and occur in a short time frame (such as a few minutes).

3. WECC sets its loss of load criteria for disturbance reporting at 200 MW rather than the 300 MW in the NERC reporting form.

4. SERC and RFC are developing additional requirements at this time. We suggest that reporting be based on impact to reliability, not on 'newsworthy'

events. We therefore do not agree with such regional efforts and would prefer a continent wide reporting requirements.

5. Some entities identified some in-force Regional Standards and other regional reporting requirements.

Project Scope

Some stakeholders suggested that the SDT has gone beyond its approved scope to "further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event." Further, there is no requirement to create a Reporting Standard to define sabotage. The SDT contends that the development of impact events and the reporting requirements for them will provide the clarity sought in the directive. Other stakeholders suggested that the SDT should seek to retire sanctionable requirements that require event reporting in favor of guidelines for reporting. Several commenters suggested that the introduction of impact events actually expands the reporting requirements. It should be noted that the list of impact events is expected to be explicit as to who is to report what to whom and within certain timelines.

Electronic Tool

Several stakeholders provided input as to what they believed an electronic reporting tool should contain:

1 If the decision is made to go to a single reporting form, it should be developed to cover any foreseeable event.

2 The SDT should work toward a single form, located in a central location, and submitted to one common entity (NERC)

3 Reports should be forwarded to the ES-ISAC, not NERC, as the infrastructure is already in place for efficient sharing with Federal agencies, with the regional entities and with neighboring asset owners. Reports should flow to all affected entities in parallel, rather than series (timing issues).

Commenters also suggested that the SDT should consider the impacts of the reporting requirements on the small and very small utilities.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Herbert Schrayshuen, at 609-452-8060 or at Herb.Schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

1. The details of reporting requirements and criteria are in the existing EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and will consider guidance found in the document "NERC Guideline: Threat and Incident Reporting" in the development of requirements. Do you agree with using the existing guidance as the foundation for disturbance reporting? Please explain your response (yes or no) in the comment area..... 12

2. The DSR SDT is considering developing a reporting hierarchy for disturbances that requires entities to submit information to the Reliability Coordinator and then for the Reliability Coordinator to submit the report. Do you agree with this hierarchy concept? Please explain your response (yes or no) in the comment area..... 24

3. The goal of the DSR SDT is to have one report form for all functional entities (US, Canada, Mexico) to submit to NERC. Do you agree with this change? Please explain your response (yes or no) in the comment area. 34

4. The goal of the DSR SDT is to eliminate the need to file duplicate reports. The standards will specify information required by NERC for reliability. To the extent that this information is also required for other reports (e.g. DOE OE-417), those reports will be allowed to supplement the NERC report in lieu of duplicating the entries in the NERC report. Do you agree with this concept? Please explain your response (yes or no) in the comment area. 42

5. In its discussion concerning sabotage, the DSR SDT has determined that the spectrum of all sabotage-type events is not well understood throughout the industry. In an effort to provide clarity and guidance, the DSR SDT developed the concept of an impact event. By developing impact events, it allows us to identify situations in the "gray area" where sabotage is not clearly defined. Other types of events may need to be reported for situational awareness and trend identification. Do you agree with this concept? Please explain your response (yes or no) in the comment area. 51

6. If you are aware of any regional reporting requirements beyond the scope of CIP-001, CIP-008 and EOP-004 please provide them here..... 61

7. If you have any other comments on the Concepts Paper that you haven't already provided in response to the previous questions, please provide them here..... 65

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	John Bee	Exelon	X		X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Dan Brotzman	ComEd	RFC	1
2.	Dave Weaver	PECO	RFC	1
3.	Ron Schloendorn	PECO	RFC	1
4.	John Garavaglia	ComEd	RFC	1
5.	Karl Perman	Exelon	NA - Not Applicable	NA
6.	Dave Belanger	Exelon Generation Co., LLC	RFC	5
7.	Alison MacKellar	Exelon Generation Co., LLC	RFC	5
8.	Tom Leeming	ComEd	RFC	1
9.	Tom Hunt	PECO	RFC	1

2.	Group	Guy Zito	Northeast Power Coordinating Council											X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	NA
2.	Michael Schiavone	National Grid	NPCC	1

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Roger Champagne		Hydro-Quebec TransEnergie	NPCC					2				
4.	Kurtis Chong		Independent Electricity System Operator	NPCC					2				
5.	Sylvain Clermont		Hydro-Quebec TransEnergie	NPCC					1				
6.	Chris de Graffenried		Consolidated Edison Co. of New York, Inc.	NPCC					1				
7.	Gerry Dunbar		Northeast Power Coordinating Council	NPCC					10				
8.	Ben Eng		New York Power Authority	NPCC					4				
9.	Brian Evans-Mongeon		Utility Services	NPCC					8				
10.	Mike Garton		Dominion Resources Services, Inc.	NPCC					5				
11.	Brian L. Gooder		Ontario Power Generation Incorporated	NPCC					5				
12.	Peter Yost		Consolidated Edison Co. of New York, Inc.	NPCC					3				
13.	David Kiguel		Hydro One Networks Inc.	NPCC					1				
14.	Michael R. Lombardi		Northeast Utilities	NPCC					1				
15.	Randy MacDonald		New Brunswick System Operator	NPCC					2				
16.	Bruce Metruck		New York Power Authority	NPCC					6				
17.	Lee Pedowicz		Northeast Power Coordinating Council	NPCC					10				
18.	Robert Pellegrini		The United Illuminating Company	NPCC					1				
19.	Saurabh Saksena		National Grid	NPCC					1				
20.	Kathleen Goodman		ISO - New England	NPCC					2				
21.	Greg Campoli		New York ISO	NPCC					2				
3.	Group	Wes Davis (SERC Staff) and Steve Corbin (Chair of SERC RCS)	SERC Reliability Coordinator Sub-committee (RCS)										X
	Additional Member		Additional Organization	Region					Segment Selection				
1.	Steve Corbin		Southeastern RC	SERC					NA				
2.	Joel Wise		TVA RC	SERC					NA				
3.	Don Reichenbach		VACAR South RC	SERC					NA				
4.	Don Shipley		ICTE RC	SERC					NA				
5.	Robert Rhodes		SPP RC	SERC					NA				
6.	Stan Williams		PJM RC	SERC									

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
7. Tim Aliff			Midwest ISO RC	SERC					NA				
4.	Group	Mike Garton	Electric Market Policy	X		X		X	X				
	Additional Member		Additional Organization	Region					Segment Selection				
1. Michael Gildea			Dominion Resources Services, Inc.	RFC					3				
2. Louis Slade			Dominion Resources Services, Inc.	SERC					6				
5.	Group	Carol Gerou	MRO's NERC Standards Review Subcommittee										X
	Additional Member		Additional Organization	Region					Segment Selection				
1.	Chuck Lawrence		American Transmission Company	MRO					1				
2.	Tom Webb		WPS Corporation	MRO					3, 4, 5, 6				
3.	Terry Bilke		Midwest ISO Inc.	MRO					2				
4.	Jodi Jenson		Western Area Power Administration	MRO					1, 6				
5.	Ken Goldsmith		Alliant Energy	MRO					4				
6.	Dave Rudolph		Basin Electric Power Cooperative	MRO					1, 3, 5, 6				
7.	Eric Ruskamp		Lincoln Electric System	MRO					1, 3, 5, 6				
8.	Joseph Knight		Great River Energy	MRO					1, 3, 5, 6				
9.	Scott Nickels		Rochester Public Utilties	MRO					4				
10.	Terry Harbour		MidAmerican Energy Company	MRO					1, 3, 5, 6				
6.	Group	Linda Perea	Western Electricity Coodinating Council										X
	Additional Member		Additional Organization	Region					Segment Selection				
1. Steve Rueckert			WECC	WECC					10				
7.	Group	Kenneth D. Brown	Public Service Enterprise Group Companies	X		X		X	X				
	Additional Member		Additional Organization	Region					Segment Selection				
1.	Ron Wharton		PSE&G	RFC					1, 3				
2.	Dave Murray		PSEG Power Connecticut	NPCC					5				
3.	Jim Hebson		PSEG Energy Resource & Trade	ERCOT					6				
4.	Jerzy Sluarz		PSEG Fossil	RFC					5				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
5.		Bruce Wertz	Odessa Ector Power Partners	ERCOT					5				
6.		Peter Dolan	PSEG Energy Resource & Trade	RFC					6				
8.	Group	Laura Zotter	ERCOT ISO		X								X
	Additional Member		**Additional Organization**	**Region**					**Segment Selection**				
1.	Steve Myers		ERCOT ISO	ERCOT					2, 10				
2.	Jimmy Hartmann		ERCOT ISO	ERCOT					2, 10				
3.	Christine Hasha		ERCOT ISO	ERCOT					2, 10				
9.	Group	Ben Li	ISO RTO Council Standards Review Committee		X								
	Additional Member		**Additional Organization**	**Region**					**Segment Selection**				
1.	Al Dicaprio		PJM	RFC					2				
2.	Jame Castle		NYISO	NPCC					2				
3.	Lourdes Estrada-Salinero		CAISO	WECC					2				
4.	Matt Goldberg		ISO-NE	NPCC					2				
5.	Steve Myers		ERCOT	ERCOT					2				
6.	Bill Phillips		MISO	RFC					2				
7.	Mark Thompson		AESO	WECC					2				
8.	Charles Yeung		SPP	SPP					2				
10.	Group	Denise Koehn	Bonneville Power Administration	X		X		X	X				
	Additional Member		**Additional Organization**	**Region**					**Segment Selection**				
1.	Tedd Snodgrass		BPA, Transmission Dispatch	WECC					1				
2.	Jim Burns		BPA, Transmission Technical Operations	WECC					1				
3.	Jeff Millennor		BPA, Security & Emergency Response	WECC					1, 3, 5, 6				
11.	Group	Jason L. Marshall	Midwest ISO Standards Collaborators		X								
	Additional Member		**Additional Organization**	**Region**					**Segment Selection**				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1. Bob Thomas			IMEA	SERC					4				
2. Jim Cyrulewski			JDRJC Associates, LLC	RFC					8				
3. Joe Knight			Great River Energy	MRO					1, 3, 5, 6				
4. Randi Woodward			Minnesota Power	MRO					1				
5. Kirit Shah			Ameren	SERC					1				
12.	Group	Sam Ciccone	FirstEnergy	X		X	X	X	X				
	Additional Member		Additional Organization	Region					Segment Selection				
1. Doug Hohlbaugh			FE	RFC					1, 3, 4, 5, 6				
2. Dave Folk			FE	RFC					1, 3, 4, 5, 6				
13.	Individual	Thomas Glock	Arizona Public Service Company	X		X		X					
14.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
15.	Individual	Brent Ingebrigtson	E.ON U.S. LLC	X		X		X	X				
16.	Individual	Steve Fisher	Lands Energy Consulting										
17.	Individual	David Kahly	Kootenai Electric Cooperative			X							
18.	Individual	Darryl Curtis	Oncor Electric Delivery Company LLC	X									
19.	Individual	Edward Bedder	Orange and Rockland Utilities, Inc.	X									
20.	Individual	Kasia Mihalchuk	Manitoba Hydro	X		X		X	X				
21.	Individual	Brian Bartos	Bandera Electric Cooperative, Inc.	X		X							
22.	Individual	John T. Walker	Portland General Electric	X									
23.	Individual	Gregory Miller	BGE	X									

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
24.	Individual	Dan Roethemeyer	Dynegy Inc.					X					
25.	Individual	Rick Terrill	Luminant					X					
26.	Individual	James Stanton	SPS Consulting Group Inc.								X		
27.	Individual	Andrew Gallo	Calpine Corp.					X					
28.	Individual	Steve Alexanderson	Central Lincoln			X							
29.	Individual	Brenda Frazer	Edison Mission Marketing & Trading					X					
30.	Individual	Martin Bauer	USBR					X					
31.	Individual	John Alberts	Wolverine Power Supply Cooperative, Inc.	X		X	X	X	X				
32.	Individual	Thad Ness	American Electric Power	X		X		X	X				
33.	Individual	James McCloskey	Central Hudson Gas & Electric	X		X							
34.	Individual	Deborah Schaneman	Platte River Power Authority	X		X		X					
35.	Individual	Howard Rulf	We Energies			X	X	X					
36.	Individual	Jianmei Chai	Consumers Energy Company			X	X						
37.	Individual	Amir Hammad	Constellation Power Source Generation					X					
38.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
39.	Individual	Kirit Shah	Ameren	X		X		X	X				
40.	Individual	Dan Rochester	Independent Electricity System Operator		X								

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
41.	Individual	Roger Champagne	Hydro-Québec TransEnergie (HQT)	X									

1. The details of reporting requirements and criteria are in the existing EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and will consider guidance found in the document "NERC Guideline: Threat and Incident Reporting" in the development of requirements. Do you agree with using the existing guidance as the foundation for disturbance reporting? Please explain your response (yes or no) in the comment area.

Summary Consideration: Most stakeholders agree that existing guidance should be used as the foundation for disturbance reporting. Most commenters felt that the "NERC Guideline: Threat and Incident Reporting" document contains a lot of detailed information which greatly assists in determining reporting events and weaning out non important events. The most common desire expressed was to have one common form for all reporting, and the OE-417 was suggested as a good starting point. Most respondents thought the form could be streamlined. The DSR SDT was urged to focus on applicable events and reporting timelines which are not clear now and to report items that are clearly essential to the reliability of the BES. There was some concern expressed about "over-reporting", out of fear of non-compliance rather reporting based on the reliability of the BES. There was also a clear desire to exclude vandalism & copper theft from reporting requirements.

Several specific suggestions were made to modify existing reporting requirements, and the drafting team will consider these when developing the proposed requirements.

Organization	Yes or No	Question 1 Comment
ERCOT ISO	Possible Yes	Parts of the Guideline are helpful, but the guideline goes beyond the scope of the requirements of the current standards, which could pose potential audit concerns. ERCOT ISO strongly feels this approach for reporting should be focused on physical events only and cyber event reporting should be contained within CIP-008 only. Continue to keep physical separate from cyber.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has not determined at this time what bright line will be used for the yet to be drafted Standard(s). The DSR SDT will take into consideration your comment on keeping cyber and physical events separate.		
Arizona Public Service Company	No Then Yes	APS supports standard revisions which streamline the reporting process for security incidents with a single form, which aligns both with EIA reporting and NERC Standards requirements, particularly those identified in the NERC Threat and Incident Reporting Guidelines. This would eliminate users issuing reports to multiple locations/government entities without a standard form or format. The DOE 417 form which is currently utilized

Organization	Yes or No	Question 1 Comment
		for reporting purposes is out-dated and does not account for the types of incidents as identified in the NERC Threat and Incident Reporting Guidelines. The guidelines state that an entity can report security incidents to the ESISAC , through CIPIS (Critical Infrastructure Protection Information System), and or RCIS (Reliability Coordinator Information Center). CIPIS refers an entity to the NICC and to the WECC. Additionally, APS proposes that the terms and timelines of reporting security incidents be clearly identified. Events are often detected quickly or immediately. Determining whether or not the event was sabotage and/or a reportable event; however, typically takes much longer. There is no time allowance for an entity to investigate the event to determine what actually occurred. Currently, DOE 417 provides that acts of sabotage should be reported within one hour of detection if the impact could affect the reliable operation of the bulk power system. This may affect the accuracy of the information being provided by an entity on it's initial reporting. Finally, provisions should be incorporated to address the privacy of information being submitted, including handling and storage.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has not determined at this time what bright line will be used for the yet to be drafted Standard(s) which should streamline the reporting process (what events and what timeline should be used). c		
SPS Consulting Group Inc.	No	At least not exclusively. The current standards and the guidance fail to consider that different registered entities will have different scopes of awareness for when disturbances may take place. We want to avoid the situation where a generator (for example) is cited for failure to report a disturbance of which they have way of knowing occurred.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT will take into consideration what Registered Entities are to be included within the yet to be written standard(s) based on the SAR and the facilities each type of Registered Entity is required to have.		
Bonneville Power Administration	No Then Yes	BPA likes the idea of consolidating information and eliminating duplication of reported information. In the report, don't include every detail possible found in the "Threat Guideline". TOP's are supposed to be operating the electrical system, not doing investigative work for copper theft incidents (see comment on #5).
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has not determined at this time what bright line will be used for the yet to be drafted Standard(s). We will consider your specific suggestion for not requiring reporting of incidents such as copper threat, when we develop the proposed requirements.		

Organization	Yes or No	Question 1 Comment
Lands Energy Consulting	No	My firm provides compliance consulting services to a number of smaller (50-700 MW peak load) LSE/DP registered entities. EOP-004 creates an obligation for LSEs to report "disturbances" that affect their systems. A few of the smaller of these systems receive service from Bonneville-owned transmission lines that serve only 4-6 substations. The NERC Form establishes loss of 50% of the LSE's retail customers as a reportable disturbances. One of my clients receives service from BPA at 5 substations. A single industrial customer with a substantially dedicated substation comprises 90% of the utility's MWH load. Were it not for this customer, the utility would have been well below the registration requirement for a DP/LSE. The balance of the load, about 15 MW of peak and 4000 retail customers, is served from 5 substations. Four of these substations serving 3000 customers are served from a long Bonneville 115 kV BES transmission line that runs through a heavily treed right of way. Every time this single line experiences a permanent outage (which will happen a few times a year), the utility loses less than 10 MW of load, but 75% of its retail customers. Under the disturbance reporting criteria, this outage would constitute a reportable disturbance for the utility. When the NERC disturbance reporting criteria were adopted, I doubt that anyone conceived that they would apply to cases like I just described. Reporting trivial events like I've just described constitutes a nuisance to the entity making the report and NERC/WECC for having to process the report. The outage has no earthly effect on the reliability of the BES and certainly doesn't warrant preparation of any kind of disturbance report.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT will take into consideration what Registered Entities are to be included within the yet to be written standard(s) based on the NERC Standards Committee approved SAR. The DSR SDT will review the Commissions concern that, an adversary might determine that a small LSE is the appropriate target when the adversary aims at a particular population or facility, as stated in FERC Order 693, paragraph 459. The intent of the proposed standard(s) is to address reporting needed for after-the-fact analyses of events as well as reporting necessary for situational awareness.		
SERC Reliability Coordinator Sub-committee (RCS)	No	Routine minor incidents such as copper theft and gun shots to insulators should not be reported. These types of minor events do not affect the reliability of the BPS. Existing reporting requirements are satisfactory. The focus of reporting should be on reliability related incidents and not incidents related to vandalism as such.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). Reporting threasholds will be determined during the next step of the Standards Development process. The DSR SDT agrees with your comments on vandalism but a balance must be further explored to meet industry and regulatory requirements specifically under FERC Order 693.		
Consumers Energy Company	No	The existing guidelines ignore the fact that there are currently three overlapping and inconsistent reporting requirements for disturbances of various types: CIP-001, EOP-004, and DOE OE-417. The reporting should be such that any single event type needs to be reported only once, and to only a single agency, for any

Organization	Yes or No	Question 1 Comment
		disturbance. First, CIP-001 events should be reported to the ES-ISAC under one specific requirement (or set of requirements) and removed from OE-417 and EOP-004, such that all interested agencies obtain their information from only that one source. Second, OE-417 events should be reportable ONLY to DOE, and, again, other agencies should obtain their information from only that one source. If NERC wishes to make such reporting mandatory and enforceable, the NERC requirements should indicate ONLY that such reporting should be made in accordance with OE-417. Finally, EOP-004 (or similar requirements) should require reporting to NERC ONLY in the case of events that don't fit under CIP-001 or OE-417 requirements. Alternatively, OE-417 should be submitted ONLY to NERC and they should disseminate the information.EOP-004 has several issues and inconsistencies: a. EOP-004 requires that the entity that submits form DOE-417 to provide copies to NERC. The DOE-417 form intermixes NERC entity definitions (e.g. BA, LSE, TO) with generic terms such as "Electric Utilities" and "Generating Entities". Is it the Generator Owner or Generator Operator that is required to submit the information? There should be one form or at least well defined definitions that apply to both forms. b. EOP-004-1 R3.1 requires submittal within 24 hours, however Table 1-EOP-004-0 which purports to summarize the standard appears to change this requirement to 1 hour for several disturbances. Additionally, it incorrectly summaries the reporting time for 50,000 customers, which is 6 hours in DOE-417 and summarized in Table 1-EOP-004-0 as 1-hour. An attachment to a standard should not be allowed to supersede the standard or create additional rules. c. EOP-004-1 R3.1 requires submittal within 24 hours, however Table 1-EOP-004-0 which purports to summarize the standard appears to change the standard. R3.1 clearly states that events are to be reported within 24 hours of identification, however Table 1-EOP-004-0 state that the events are to be reported on the basis of the start of the disturbance. An attachment to a standard should not be allowed to supersede the standard or create additional rules. d. EOP-004-1 R3.1 requires submittal within 24 hours, however Table 1-EOP-004-0 which purports to summarize the standard appears to change the standard. R3.1 clearly states that events are to be reported within 24 hours of identification, however Table 1-EOP-004-0 states that copies of DOE-417 are required to be submitted "simultaneously". It also states that schedules 1 and 2 are due within 24 hours of start of the event instead of 48 hours for per DOE-417 for schedule 2. An attachment to a standard should not be allowed to supersede the standard or create additional rules. e. The requirement of loss of customers should be scaled based on customers served. Loss of 50,000 customers to a utility that serves 100,000 customers is different than loss of 50,000 customers to a utility that serves 2,000,000 customers.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and		

Organization	Yes or No	Question 1 Comment
ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT agrees that present Reliability Standards can be complicated and lead to confusion when working on maintaining system reliability in the area of reporting per CIP-001-1 and EOP-004-1. We will consider the disagreements you've identified in existing reporting requirements when we develop the proposed requirements.		
Central Lincoln	No	The guidance document makes no distinction between entities that operate 24/7 dispatch and those that don't. The 1 hour and even the 24 hour reporting requirements in some cases will be impossible for entities without 24/7 dispatch to meet without changing business practices. These are the same entities that present little or no risk to the BES.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT will take into consideration what Registered Entities are to be included within the yet to be written standard(s) based on the SAR. The DSR SDT will establish the "requirements necessary for users, owners, and operators of the Bulk-Power-System" as stated in FERC Order 693, paragraph 617 and the difference in reporting of events on the BES, as stated in the Purpose statement of EOP-004-1. The intent of the proposed standard(s) is to address reporting needed for after-the-fact analyses of events as well as reporting necessary for situational awareness.		
MRO's NERC Standards Review Subcommittee	No Then Yes	We agree with using the present documentation but would like just one reporting form. We are concerned that the guidelines and reporting periods specified within the DOE OE-417 report conflict with the NERC Guidelines. For example. DOE OE-417 report requires "Suspected Physical or Cyber Impairment" to be reported within 6 hours. The NERC guidelines indicate "Suspected Activities" are to be reported within 1 hour. We recommend the SDT use the DOE OE-417 report as a guiding document, and then determine additional reporting requirements using guidance from the NERC Guideline. FERC Order 693 appears to indicate conflicts and confusion with NERC reporting requirements and DOE reporting requirements should be eliminated.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT is looking to streamline required reporting actions and remove any redundant reporting requirements if at all possible. The DOE Form OE-417 is currently mandatory under Public Law 93-275 for entities within the juristicion of the U.S Department of Energy. We will consider the disagreements you've identified in existing reporting requirements when we develop the proposed requirements.		
Luminant	No Then Yes	While the guidance is generally ok in the "NERC Guideline: Threat and Incidence Reporting", the reporting timelines include 1 hour, 2 hours, 4 hours, 6 hours, 8 hours, 24 hours, and 48 hours. Please simplify and reduce the variation in timelines. When it comes to Sabotage reporting, some time requirements start with detection, some start with determination of sabotage and some events do not specify the trigger for the reporting clock to start. Again, please provide clarity and consistency around the start of the timeline for

Organization	Yes or No	Question 1 Comment
		reporting. Generally, the reporting timing should start with the recognition or determination that a suspected or known sabotage event occurred.
Response: The DSR SDT thanks you for your comment. The DSR SDT is looking to streamline required reporting actions and remove any redundant reporting requirements if at all possible. The DSR SDT agrees that present Reliability Standards can be complicated and lead to confusion when working on maintaining system reliability in the area of reporting per CIP-001-1 and EOP-004-1. We will consider your specific suggestion for less variation in reporting timeframes, when we develop the proposed requirements.		
We Energies	No Then Yes	While the NERC Guideline includes readily discernible information (and we would like to see that format carried forward into any future documentation), utilize OE-417 as the foundation document in order to eliminate reporting redundancies. If supplemental references are necessary for the proposed resolution, list the document as an official attachment to the standard. Minimize the need to search in multiple locations for guideline information - some may not be aware supporting documentation exists without explicit reference within the standard.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT is looking to streamline required reporting actions and remove any redundant reporting requirements if at all possible. The DSR SDT agrees that present Reliability Standards can be complicated and lead to confusion when working on maintaining system reliabiltiy in the area of reporting per CIP-001-1 and EOP-004-1. The DOE Form OE-417 is currently mandatory under Public Law 93-275 for entities within the juristicion of the U.S Department of Energy. We will consider your recommendation regarding listing supplemental references within the body of the standard when we draft the proposed standard(s).		
American Electric Power	Yes	
Bandera Electric Cooperative, Inc.	Yes	
Calpine Corp.	Yes	
Duke Energy	Yes	
Edison Mission Marketing & Trading	Yes	

Organization	Yes or No	Question 1 Comment
Exelon	Yes	
Independent Electricity System Operator	Yes	
PacifiCorp	Yes	
Platte River Power Authority	Yes	
Central Hudson Gas & Electric	Yes	Central Hudson agrees with using the "NERC Guideline: Threat and Incident Reporting" in the development of requirements. Central Hudson has currently in place a NERC-DOE Threat and Incident Reporting Table developed from this NERC Guideline that allows for a quick-reference to all threat and incident reporting criteria (arranged by category)with a cross-reference to the specfic reporting form (NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report, DOE Form OE-417, or NERC ES-ISAC Threat and Incident Report Form). Central Hudson recommends maintaining the option of utilizing only 1 form, the DOE Form OE-417, for incidents that require reporting to the DOE and NERC to maintain the streamlined approach to this reporting process.
Response: The DSR SDT thanks you for your comment. The DSR SDT is looking to have a single reporting report form (per question 3) and streamline the reporting processes that may be developed within ~~a~~ yet to be written requirement(s).		
E.ON U.S. LLC	Yes	E.ON U.S. believe that the guidelines provide greater clarity for reporting forced outages caused by disturbances and sabotage but there remains issues that in need of further clarification. For example, there remains too much subjectivity on the reporting of forced outages when there is "identification of valuable lessons learned"
Response: The DSR SDT thanks you for your comment. The DSR SDT concurs that further clarification is required with the ambigious statement "identification of valuable lessons learned" contained in the guideline – use of this phrase does not meet the technical writing threshold required for inclusion in a NERC Standard. The DSR SDT's intent was to look at the posted NERC Guideline and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). Recommendation of changes to the "NERC Guideline: Threat and Incident Reporting" should be submitted to NERC via the Critical Infrastructure Protection Committee. I		
Public Service Enterprise Group Companies	Yes	EOP reportable disturbances are familiar concepts in the industry.

Organization	Yes or No	Question 1 Comment
Response: The DSR SDT thanks you for your comment and support.		
Orange and Rockland Utilities, Inc.	Yes	However, the SDT needs to maintain clear demarcation for the criteria for reporting events, and only those events that directly effect the reliability of the BES.
Response: The DSR SDT thanks you for your comment. The DSR SDT has been directed to review all disturbance type activities and submit to the industry a well thought out set of requirements that clearly define disturbance events and what information is required to enhance an entity'ssituational awareness. Clear demarcation for the criteria for reporting will be determined in the near future based on the approved SAR and industry feedback. The intent of the proposed standard(s) is to address reporting needed for after-the-fact analyses of events as well as reporting necessary for situational awareness.		
Wolverine Power Supply Cooperative, Inc.	Yes	I agree with referencing existing guidelines - However: My concern is that, until all reportable incidents are analyzed by the parties to which they are reported, their "impact" on the BES will not be quantified. Therefore, the tendency to want to "report all events so that their impact can be determined" or "report all events because the information can be utilized for informational purposes, regardless of impact on BES" might lead to expanded reporting requirements, some of which may have questionable value from a reliability standpoint.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if the DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has been directed to review all disturbance type activities and submit to the industry a well thought out set of requirements that clearly define reportable events and what information is required to enhance an entity's situational awareness. Clear demarcation for the criteria for reporting will be determined in the near future based on the approved SAR and industry feedback. The intent of the proposed standard(s) is to address reporting needed for after-the-fact analyses of events as well as reporting necessary for situational awareness.		
Hydro-Québec TransEnergie (HQT)	Yes	In considering guidance found in the document "NERC Guideline: Threat and Incident Reporting", the SDT should maintain focus on only those items that are absolutely necessary to maintain the reliability of the Bulk Electric System. In fact, the purpose of reporting per EOP-004 is that disturbances... need to be studied and understood to minimize the likelihood of similar events in the future.
Northeast Power Coordinating Council	Yes	In considering guidance found in the document "NERC Guideline: Threat and Incident Reporting", the SDT should maintain focus on only those items that are absolutely necessary to maintain the reliability of the Bulk Electric System. In fact, the purpose of reporting per EOP-004 is that disturbances... need to be studied and understood to minimize the likelihood of similar events in the future.
Response: The DSR SDT thanks you for your comment. The DSR SDT will establish the "requirements necessary for users, owners, and operators of		

Organization	Yes or No	Question 1 Comment
the Bulk-Power-System" as stated in FERC Order 693, paragraph 617 and the difference in reporting of events on the BES, as stated in the Purpose statement of EOP-004-1. The intent of the proposed standard(s) is to address reporting needed for after-the-fact analyses of events as well as reporting necessary for situational awareness.		
Western Electricity Coordinating Council	Yes	It is comprehensive; however, we must keep in mind that the OE-417 is required under Public Law 93-275 and needs to be attached if applicable in the US.
Response: The DSR SDT thanks you for your comment.		
Oncor Electric Delivery Company LLC	Yes	NERC Guideline: Threat and Incident Reporting" document should be used for guidance as it identifies best practices for reporting.
Response: The DSR SDT thanks you for your comment.		
Manitoba Hydro	Yes	The "Threat and Incident Reporting" document contains a lot of detailed information which greatly assists in determining reporting events and weaning out non important events. The document contains some examples and expected reporting time lines. Attachment 1-EOP-004, though considerably smaller and condensed it does contain some detail not mentioned in "Threat and Incident Reporting". Integrating the "Threat and Incident Reporting" into Attachment 1-EOP-004, though large in size, has lots of information and is easy to follow would be a large improvement to existing protocol OR SEE QUESTION 3 COMMENTS. Incidences we have experienced on our system, in past were difficult to delineate as reportable, who to report to and when. An improvement to this Standard is welcome.
Response: The DSR SDT thanks you for your comment. The DSR SDT is looking to streamline and remove any redundancies within the NERC Standard's requirements.		
Constellation Power Source Generation	Yes	The existing guidance is an excellent base on which to build changes to EOP-004 and CIP-001. However, the SDT must challenge each item in the different event categories and clarify or omit bullet points that are seemingly vague. For example, under System Disturbances, a forced outage report is needed when "a generation asset of 500 MW or above is on a forced outage for unknown reasons, or a forced outage of generation of 2,000 MW occurs..." Simply removing the 500 MW criteria would make this criterion less vague. There are other examples of this in the guideline.
Response: The DSR SDT thanks you for your comment. The DSR SDT is looking to streamline and remove any redundancies within the NERC Standard's requirements. It is the intent of the SDT to carefully review the different event categories and provide clarity where needed to remove ambiguity.		

Organization	Yes or No	Question 1 Comment
ISO RTO Council Standards Review Committee	Yes	The guidelines in EOP-004 and its attachments should be retained as the foundation for reporting disturbances. One would note that such EOP Disturbances are relatively well defined reliability impacts. Thus EOP-004 disturbances are based on HOW certain events impacted the BES. [Sabotage on the other hand requires an implication of WHY an event occurred.]The original EOP-004 represents a common sense approach to defining reliability events that may be useful to analyze on a regional basis. In the current environment, Regions are not sanctionable entities but they still are valuable sources to collect, analyze and trend the few disturbances that occur in each region. To make use of Regions, however, precludes the use of sanctionable NERC standards. EOP-004 as written does not meet the NERC requirements for standards but it does meet the Industry needs for a guideline for reporting events that deserve to be reviewed. The SDT should propose deleting EOP-004 and use it as a Disturbance Reporting Guideline.
Response: The DSR SDT thanks you for your comment. Regions are required to comply with requirements in NERC Reliability Standards – however Regions are not sanctioned the same way as users, owners and operators of the bulk power system – if a Region fails to comply with a NERC Reliability Standard, it can be fined for failure to comply under the ERO's Rules of Procedure.		
USBR	Yes	The reporting outlined in the proposed plan does not include a clear indication of how NERC will use the information they collect from the entities. Care needs to be taken in addressing the reporting requirements to not create a more confusing or onerous reporting process.
Response: The DSR SDT thanks you for your comment. It is anticipated that NERC will analyze events to assess trends and identify lessons learned for industry feedback and reliability improvement.		
FirstEnergy	Yes	This guideline appears to be a good starting point for developing consistency in reporting. However, we believe that after-the-fact event reporting is administrative in nature and seldom rises to the level of mandated reliability standard requirements. It is not clear what reporting would be made through this effort and how it differs from reporting made through the NERC Reliability Coordinator Information System (RCIS). With the initiative for more results-based standards being the goal of NERC, true after the fact reporting-type requirements should become administrative procedures and only be included in standards if they are truly required for preserving an Adequate Level of Reliability. If there are aspects that rise to be retained in a mandatory and enforceable reliability standard, we propose that those associated with sabotage be moved to CIP-001 and that EOP-004 be focused on operational disturbances that warrant wide-area knowledge. However, if the RCIS is the mechanism to convey real-time information and that is presently occurring outside of reliability standards, it is unclear what the delta improvement this project aims to achieve.
Response: The DSR SDT thanks you for your comment. As stated in FERC Order, 693, paragraph 611, "Complete and timely data is essential for analyzing system disturbances" and in paragraph 617, "the Commission directs the ERO to develop a modification to EOP-004-1 through the		

Organization	Yes or No	Question 1 Comment
Reliabiloity Standards development process that includes any requirements necessary for users, owners, and operators of the Bulk-Power-System to provide data that will assist NERC in the investigation of a blackout or disturbance". Some data is needed, therefore, for after-the-fact analyses. In addition, some data is needed much more quickly for situational awareness. The DSR SDT will analize and determine what constitues a reportable event and what information is required for situational awareness as opposed to after the fact analyses of events.		
Portland General Electric	Yes	This process is in place and utilities are familiar with it. This is a good place to start.
Response: The DSR SDT thanks you for your comment and support.		
Ameren	Yes	We agree that it makes sense to build upon existing documentation. However, we do not believe it is necessary to require event reporting to be in an enforceable standard. Rather the drafting team should consider developing a reporting guideline document and retiring the EOP-004 standard.
Response: The DSR SDT thanks you for your comment. As stated in FERC Order, 693, paragraph 611, "Complete and timely data is essential for analyzing system disturbances" and in paragraph 617, "the Commission directs the ERO to develop a modification to EOP-004-1 through the Reliabiloity Standards development process that includes any requirements necessary for users, owners, and operators of the Bulk-Power-System to provide data that will assist NERC in the investigation of a blackout or disturbance". Some data is needed, therefore, for after-the-fact analyses. In addition, some data is needed much more quickly for situational awareness. As envisioned, the requirements developed under this project will address both types of reporting requirements.		
Midwest ISO Standards Collaborators	Yes	We agree that it makes sense to build upon existing documentation. However, we do not believe it is necessary to require event reporting to be in an enforceable standard. Rather the drafting team should consider developing a reporting guideline document and retiring the EOP-004 standard. This is further supported by the fact that there is a role in the existing standard for the Regional Entities even though these requirements can't be enforced against the Regional Entities because they are not a user, owner or operator of the system.
Response: The DSR SDT thanks you for your comment. As stated in FERC Order, 693, paragraph 611, "Complete and timely data is essential for analyzing system disturbances" and in paragraph 617, "the Commission directs the ERO to develop a modification to EOP-004-1 through the Reliabiloity Standards development process that includes any requirements necessary for users, owners, and operators of the Bulk-Power-System to provide data that will assist NERC in the investigation of a blackout or disturbance". Some data is needed, therefore, for after-the-fact analyses. In addition, some data is needed much more quickly for situational awareness. As envisioned, the requirements developed under this project will address both types of reporting requirements.		
Dynegy Inc.	Yes	We agree with using the guidance; however, please consider revising the NERC Guideline: Threat and Incident Reporting document to (i) lengthen the reporting timelines related to attempted sabotage to allow for

Organization	Yes or No	Question 1 Comment
		additional time to deem the threat credible, (ii) expand the description of forced outage of generation greater than 2000 MW to include whether it is at the BA or GO level and if GO level, whether it is for one site or the combined GO's sites in a Region, and (iii) add a Responsible Party column to the Appendix A matrix.
Response: The DSR SDT thanks you for your comment. Recommendation of changes to the "NERC Guideline: Threat and Incident Reporting" should submitted to NERC via the Critical Infrastructure Protection Committee since that falls outside the scope of the SAR. **We will consider your specific suggestions for revisions to reporting requirements when we develop the proposed requirements.**		
BGE	Yes	We have no problem with NERC using the existing guidance as the foundation for disturbance reporting; however, since this project proposes to investigate incorporation of the Cyber Incident reporting aspects of CIP-008, we feel that if adopted, this concept should be added to the NERC Guideline document "Threat and Incident Reporting".
Response: The DSR SDT thanks you for your comment. Recommendation of changes to the "NERC Guideline: Threat and Incident Reporting" should submitted to NERC via the Critical Infrastructure Protection Committee since that falls outside the scope of the SAR.		
Electric Market Policy	Yes	Yes; however, in considering guidance found in the document "NERC Guideline: Threat and Incident Reporting" the SDT should maintain focus on only those items that are absolutely necessary to maintain the reliability of the Bulk Electric System. In fact, the purpose of reporting per EOP-004 is that disturbances... need to be studied and understood to minimize the likelihood of similar events in the future.
Response: The DSR SDT thanks you for your comment. The DSR SDT will establish the "requirements necessary for users, owners, and operators of the Bulk-Power-System" as stated in FERC Order 693, paragraph 617 and the difference in reporting of events on the BES, as stated in the Purpose statement of EOP-004-1. As envisioned, the requirements developed under this project will address reporting requirements that are used for after-the-fact analyses as well as reporting requirements that are associated with situational awareness.		

2. The DSR SDT is considering developing a reporting hierarchy for disturbances that requires entities to submit information to the Reliability Coordinator and then for the Reliability Coordinator to submit the report. Do you agree with this hierarchy concept? Please explain your response (yes or no) in the comment area.

Summary Consideration: Most stakeholders (about 2/3) agree with the concept of developing a reporting hierarchy for disturbances. Stakeholders who disagreed believed that the RC should be one of many to receive information on impact events (DOE, RRO, etc.). Such a hierarchy would lead to reporting delays (leading to lack of situational awareness), be cumbersome and complicated and clouds responsibility for who is to report what to whom. Other negative comments believed that a hierarchy would distract the RC's focus from its primary responsibility. Thos stakeholders who agreed commented that the RC should be the collection point for reports and information and take the responsibility to forward as required. This is from the concept that the RC has the "wider view" and can recognize patterns, and has the ability to "escalate" the reporting process. This would also minimize duplication of reports and information.

Organization	Yes or No	Question 2 Comment
BGE	No	As currently worded, BGE opposes the reporting hierarchy concept, since insufficient guidelines were proposed to prevent translation errors between the responsible entity (RE) and the RC. In addition to creating possible reporting errors, this also opens a risk that the RC could misrepresent the true intent of an RE's report contents if called upon to explain/justify a submitted report. Reporting delays are another concern with this proposal because the RE would basically be relinquishing control of the reporting process to the RC, while ultimately retaining the responsibility for ensuring the report gets submitted within the required timeframe. However, BGE recognizes that avoiding duplication and conflicting reports as well as encouraging communication are valuable. To make the reporting hierarchy concept acceptable to BGE, the DSR SDT must develop proper controls to ensure the RE has the ability to control or approve the information submitted and/or subsequently discussed with the respective authorities, and that it is done within the permissible timeframe to satisfy compliance requirements.
Response: The DSR SDT thanks you for your comment. If the reporting hierarchy concept is adopted, it will include controls to ensure timely reporting, clear accountability so that risk is not transferred, and a mechansim to ensure the Responsible Entity's reported information remains as submitted.		

Organization	Yes or No	Question 2 Comment
Consumers Energy Company	No	It would be inefficient for RC's to accumulate ALL disturbance data and submit it, and to bifurcate the reporting based on type of disturbance above and beyond OE-417 data (which should go ONLY to DOE) would make a standard very involved for an entity to comply with. We're discussing after-event data here, not data needed for current operations - and there's no reason to make it any more complicated than necessary.
Response: The DSR SDT thanks you for your comment. In order for a reporting hierarchy concept to be adopted, it will result in real effiency gains by eliminating duplication of reports. It will not be pursued if the result is a complicated or burdensome process for responsible entities.		
Exelon	No	Some of the DOE related reporting is driven by distribution events, i.e. outages greater then 50,000 customers, is it realistic to expect the RC, whose focus is on the transmission system to perform distribution related reporting?
Response: The DSR SDT thanks you for your comment. The DOE Reporting Form OE 417 is currently mandatory by Public Law and only applies to US entities and contains reporting thresholds that are not required by NERC. Our goal is to derive reporting thresholds that meet NERC's needs for information on bulk electric system disturbances and real-time events, not distribution level-only problems.		
USBR	No	The existing reporting methods collect reports of disturbances and analyze them by committees of the respective coordinating councils. The new process would introduce a duplicate layer and associated staffing. It would be better to ensure communication between the existing committees of the respective coordinating councils and the RC rather than creating a new layer of review tracking and analysis. While the layered reporting hierarchy discussed in the Disturbance Reporting section of the paper will eventually help with overall event awareness, the additional delays the hierarchical approach could result in a decrease in situational (timely) awareness. Having more comprehensive information as a result of the potential enhancements each layer adds to the chain of reporting may not be more valuable than timely and well disseminated information in an actual disturbance situation. We would suggest the SDT give careful consideration to this proposed direction. It may be appropriate to consider that expedited reporting of operational impacts would outweigh the benefit of administratively intensive reporting procedures. The events reported through the existing process have not yielded material feedback other than statistical analysis. Statistical analysis is not as sensitive to timely reporting. Operational impacts which may be the result of possible sabotage may be evident through assessment of widespread outage patterns or following event analysis. Comprehensive event analysis can take anywhere from 15 days to 90 days depending on the event.
Response: The DSR SDT thanks you for your comment. We agree that reporting timeliness must be weighed against the percieved benefits of a reporting hierarchy. If the reporting hierarchy concept is adopted, it should include controls to ensure timely reporting, clear accountability so that risk of a violation of the standard is not transferred, and a process to ensure the responsible entities' reported information remains as submitted. Also it must result in real effiency gains and support the reliability of the bulk electric system.		

Organization	Yes or No	Question 2 Comment
ISO RTO Council Standards Review Committee	No	The idea of a reporting hierarchy provides an easy to follow pro forma approach. But disturbance reports should not always follow a common reporting path. A disturbance on the transmission system for example need not be routed through an "if applicable" Balancing Authority. To mandate that a BA be in the path is inappropriate. To leave the applicability open is to create a subjective compliance problem for the impacted BA. Copper theft is another example that should not require reporting up through the RC. It is a local issue and the Transmission Owner should be able to report this directly to the appropriate parties. How would a DP, LSE or GO know if an event is an "impact event"? The posed impact events are a series of conditions for sabotage but not for EOP-type disturbances. The aforementioned entities have no requirement to monitor and analyze the BES, which then means every event would be an impact event for those entities (not an EOP disturbance but an impact event). Thus every theft of copper is an impact event mandating a Disturbance Report even though the SDT notes the RC only has to send it to the "local authorities". This seems to be a misuse of the RC resources; every train derailment is an impact event requiring a Disturbance report (is that a commercial train, regional rail line a local trolley car); every teenage prank would also generate an impact event mandating a disturbance report. The SDT defined impact events are not appropriate for use in defining disturbances. There is a big difference from creating a set of guidelines to follow as opposed to creating sanctionable standards
Response: The DSR SDT thanks you for your comment. Furthermore, impact events should not include copper theft or other conditions that pose no threat to the reliability of the BES. A train derailment is only an impact event if it threatens some element of the bulk electric system such as a transmission line corridor - the derailment in itself is not an impact event. See more on impact events under the responses to Question 3.		
Bonneville Power Administration	No	The RC is made aware of these type of incidents and goes right back to incorporating that in their awareness and to focusing on system reliability. If the RC is the recipient for further distribution of information of this type they will be forever going back for more information. Eliminate the middleman in whatever concept you propose, folks have plenty to do now. Let people make good judgments with the direct field people on the seriousness of the breach with their security personnel contacting the appropriate law enforcement agency. (Or are you looking to do a simple RE reports to the RC who marks various category items on a secure website Yes/No category item indicator that can be rolled up in ES-ISAC map board?)
Response: The DSR SDT thanks you for your comment. The Reliability Coordinator's suggested role in this is to allow them to incorporate the relevant data from responsible entities in their footprint for further analysis.		
Duke Energy	No	The RC should not be responsible for submitting the report to FERC, NERC or the RRO. The RC may not have the necessary first hand information concerning the facts of the event. Situation awareness can be maintained by including the RC in the distribution of any sabotage related reporting.

Organization	Yes or No	Question 2 Comment
SERC Reliability Coordinator Sub-committee (RCS)	No	The RC should not be responsible for submitting the report to FERC, NERC or the RRO. The RC may not have the necessary first hand information concerning the facts of the event. Situation awareness can be maintained by including the RC in the distribution of any sabotage related reporting.
Response: The DSR SDT thanks you for your comment. If the reporting hierarchy concept is adopted, it will include controls to ensure timely reporting, clear accountability so that risk of a violation of the standard is not transferred, and a process to ensure the responsible entities' reported information remains as submitted. Also it must result in real effiency gains and support the reliability of the bulk electric system.		
ERCOT ISO	No	There are some events that are truly local and should be handled by local entities and reported to local authorities (i.e. theft). If there is an impact or potential to have an impact to the BES or to the region, then hierarchical reporting would be appropriate.
Response: The DSR SDT thanks you for your comment. We agree - a clearly defined impact event criteria would do just as you suggest - leave local issues on the local level.		
Northeast Power Coordinating Council	No	This is not a standards issue, and NERC should not dictate the reporting structure. It should be left to the RCs and their members.
Response: The DSR SDT thanks you for your comment. In defining a disturbance reporting hierarchy we sought to realize efficencies. If the reporting hierarchy concept is adopted, it must result in real effiency gains and support the reliability of the bulk electric system. It will not be adopted if the result in a complicated or burdensome process for responsible entities.		
MRO's NERC Standards Review Subcommittee	No	We agree a coordinated reporting process is beneficial for the entity and the Reliability Coordinator (RC). However, a hierarchy would likely lengthen the reporting timeframe, or reduce the allotted time for each entity to provide notification to the RC in order to meet DOE or NERC timelines. Communication and coordination with the RC would likely provide more accurate and complete data submissions within a timely process and create shared accountability for the report being submitted.
Response: The DSR SDT thanks you for your comment. If the reporting hierarchy concept is adopted, it will include controls to ensure timely reporting, clear accountability so that risk of a violation of the standard is not transferred, and some mechansim to ensure the responsible entities's reported information remains as submitted.		

Organization	Yes or No	Question 2 Comment
Midwest ISO Standards Collaborators	No	We do not agree with developing a hierarchy for reporting for all disturbances and impacting events. For instance, copper theft is an example of an item that should be reported to the appropriate entities directly by the Transmission Owner. The RC does not need to be made aware of every copper theft unless it has a direct impact on reliability (affects rating, protection system, etc.) and the RC should not be burdened with expending resources for this reporting. A further example in which the hierarchy is not needed would be the case in which only one entity is impacted. If a significant event occurs on one TOP's system, then the TOP should be able to handle the reporting of all entities under its purview. If more than one TOP is involved, then it would be necessary to involve the RC in the reporting.
Response: The DSR SDT thanks you for your comment. The reporting hierarchy concept is meant to apply only to disturbance reporting. We agree that copper theft and other situations that do not pose a direct threat to reliability shouldn't be reported to NERC through this standard.		
FirstEnergy	No	While we appreciate the team's effort to serialize the reporting process, with the electronic communication methods available today, it seems that reporting can be accomplished simultaneously to multiple entities without shifting the burden of reporting to others along the communications path. This is particularly true if the reporting format is standardized to a one-size-fits-all report. Additionally, it would be a great burden to the Reliability Coordinator to review all events perceived by entities to be malicious sabotage events.
Response: The DSR SDT thanks you for your comment. The reporting hierarchy concept would only apply to disturbance reporting, not impact events. The Reliability Coordinator's suggested role in this to allow them to incorporate the relevent datea from responsible entities in their footprint for further analysis. We will consider your suggestion of simulataneous submissions as a means to effectively notify the necessary parties.		
Edison Mission Marketing & Trading	Yes	
PacifiCorp	Yes	
SPS Consulting Group Inc.	Yes	
Calpine Corp.	Yes	A Functional Entity such as a Generator Owner/Operator is not always aware that an event, such as a plant trip, is part of a wider system disturbance that rises to the level of a reportable event under EOP-004. A reporting hierarchy that allows a Generator to report the facts to its Transmission Operator and have that entity take a wider view to determine whether there is a disturbance should facilitate the reporting of actual disturbances. The SDT needs to ensure that some thought goes into the flow of information within the hierarchy and what triggers are needed to drive the reporting up the hierarchy.

Organization	Yes or No	Question 2 Comment
Response: The DSR SDT thanks you for your comment. A reporting hierarchy process must include clear triggers for reporting and provide an efficient, well-defined information flow.		
We Energies	Yes	A hierarchical approach in conjunction with a single, electronic form would provide consistent reporting timelines, provide clarity in the reporting process, and provide more accurate and meaningful data submissions while having shared accountability. Confusion in the current method could be alleviated while providing more consistency in the reporting of an "impact event".
Response: The DSR SDT thanks you for your comment.		
Arizona Public Service Company	Yes	All disturbance reporting should go through the RC.
Response: The DSR SDT thanks you for your comment.		
Constellation Power Source Generation	Yes	As stated in the concept paper, a hierarchy ensures proper communications, but it has the added benefit of reducing redundancy on the Registered Entities, so long as responsibilities and accountability are clearly established.
Response: The DSR SDT thanks you for your comment.		
Central Hudson Gas & Electric	Yes	Central Hudson agrees with this reporting hierarchy for disturbances given the "wider-view" of the Reliability Coordinator as opposed to an entity such as a Transmission Owner or Load-Serving Entity. While, based on past experience, the current process works if reports are filed to the DOE, RRO, and RC simultaneously via email for example. However, the RC is in a better position to identify multi-site incidents and escalate the reporting process if necessary.
Response: The DSR SDT thanks you for your comment.		
Wolverine Power Supply Cooperative, Inc.	Yes	From the perspective of a TOP, this seems to alleviate reporting burden and move it up line. I can understand the logic in wanting the reporting to flow through the RC for awareness purposes, but I can understand the RC's reluctance to bear the additional potential burden. Again, a focused effort to minimize the necessary reporting to 'true impact events" should be kept in mind, regardless of who has to report. Collecting reams of data and figuring out what impact it has later should not be the goal.

Organization	Yes or No	Question 2 Comment
Response: The DSR SDT thanks you for your comment. We agree that regardless of any reporting hierarchy, the goal is to report on disturbances and events with meaningful impact on the bulk electric system. See Question 3 responses for more information on how we view impact events.		
Electric Market Policy	Yes	Having the reporting flow through the Reliability Coordinator supports the reliability objective of assessing, monitoring, and maintaining a wide-area view of the reliability of the Bulk Electric System.
Hydro-Québec TransEnergie (HQT)	Yes	Having the reporting flow through the Reliability Coordinator supports the reliability objective of assessing, monitoring, and maintaining a wide-area view of the reliability of the Bulk Electric System. The reporting hierarchy should be to submit the information to the Reliability Coordinator, and to have the RC submit the report. This would eliminate the duplication of information.
Orange and Rockland Utilities, Inc.	Yes	Having the reporting flow through the Reliability Coordinator supports the reliability objective of assessing, monitoring, and maintaining a wide-area view of the reliability of the Bulk Electric System. The reporting hierarchy should be to submit the information to the Reliability Coordinator, and to have the RC submit the report. This would eliminate the duplication of information.
Response: The DSR SDT thanks you for your comment.		
Lands Energy Consulting	Yes	I would give the RC the authority to establish impact thresholds for reporting. Consistent with my earlier comment, I would set the materiality threshold for disturbance reporting purposes at LSEs (or a combination of LSEs in the case of BPA) serving at least 90,000 customers.
Response: The DSR SDT thanks you for your comment. Reporting thresholds in the standard will meet NERC requirements: Reliability Coordinator's may have different reporting criteria to meet Regional requirements, but they will not appear in this yet to be written Standard.		
Central Lincoln	Yes	In the west at least, this hierarchy should be extended to include BA's as indicated in the Concepts Paper. See: http://www.bpa.gov/corporate/business/reliability/Docs/2007/PNSC_RE_Data_Letter_2_070723.pdf for the RC's policy on which entities it chooses to communicate with.

Organization	Yes or No	Question 2 Comment
Response: The DSR SDT thanks you for your comment. The hierarchy concept includes BAs as appropriate in the reporting structure.		
Luminant	Yes	Luminant believes that one report should be filed with the Reliability Coordinator or one responsible entity, who then files the report with all applicable entities.
Response: The DSR SDT thanks you for your comment.		
Oncor Electric Delivery Company LLC	Yes	Oncor agrees that with this reporting hierarchy, in that dual reporting should be eliminated
Response: The DSR SDT thanks you for your comment.		
Portland General Electric	Yes	PGE is familiar with and works closely with WECC today so the hierarchial consideration makes sense.
Response: The DSR SDT thanks you for your comment.		
Platte River Power Authority	Yes	Situational awareness would be enhanced. All affected entities would be aware of the disturbance and relevant information. Also, the flow of information between entities would be enhanced and a more comprehensive report could be developed.
Response: The DSR SDT thanks you for your comment.		
Ameren	Yes	The hierarchy is appealing in the fact that the TOP/BA will be kept in the loop and receive critical information from the Generators, Distribution, LSE, etc. But there will be an inherent delay in reporting due to the fact that at every hand-off of information there will be questions for additional and/or clarified information, and there is always a possibility for the loss of information due to the transfer from one entity to the next. Further, this reporting through a hierarchy could also take away from the operators ability to respond to system events due to being tied to an information transfer ladder.
Response: The DSR SDT thanks you for your comment. If the reporting hierarchy concept is adopted, it will include controls to ensure timely reporting, clear accountability so that risk of a violation of the standard is not transferred, and some process to ensure the responsible entities' reported information remains as submitted. It must also ensure that it does not place any extra burden on operators that could create an additional risk to reliability.		

Organization	Yes or No	Question 2 Comment
E.ON U.S. LLC	Yes	The hierarchy will simplify reporting from the entity in that the RC is always notified and then the RC notifies other parties as required, (with the exception of OE-417, which still has to be filled out per law) E.ON U.S. recommends that the drafting team pay particular attention to the report process to make sure that duplicate reports are not being required. Currently information on forced outages is already communicated to the RC so formalizing a requirement to provide data to the RC may represent duplication to reports already provided.
Response: The DSR SDT thanks you for your comment. Avoiding duplication is a key goal of the drafting team.		
Public Service Enterprise Group Companies	Yes	The PSEG Companies believe that all entities with a reportable disturbance should report to the RC. The RC is best positioned to evaluate the impact of the event and forward the information to the appropriate entities. There should not be any intermediate entities to relay information to the RC as that can introduce delay and has the potential to introduce transcription errors. Sabotage events should be reported to the RC as well as to law enforcement. CIP-008 reporting is highly specialized and should be retained in the set of cyber security standards, not merged with CIP-001 and EOP-004.
Response: The DSR SDT thanks you for your comment. Detection of cyber events may be specialized but report of them is not. Threats to reliability must be reported no matter what the cause. The DSR SDT proposes using the thresholds found in CIP-008 - this standard would provide a one stop form to submit the information. Note that the current CIP-008 has a reporting requirement to the ES-ISAC only.		
Manitoba Hydro	Yes	The Reporting Concept states that the new hierarchy is, “Affected entity to TOP/ BA to RC. Then the RC will then submit to NERC and DOE (if required)”.This will enhance the existing requirement EOP-004-1 R4 which states that the RC shall assist the affected entity by providing representatives to assist in the investigation (this is also all reiterated in Attachment 1-EOP-004) .In an disturbance, the local resources would be tied up in the rectification of the problem. Analyzing and reporting the event (is it reportable, who to report to, what is the timeline) is distracting and time consuming. By leaving the final upper level steps of reporting to NERC/DOE by the RC would be efficient.
Response: The DSR SDT thanks you for your comment.		
Western Electricity Coordinating Council	Yes	There should be an established time sequence that allows the RC to review the entities material prior to forwarding to NERC. By channeling all reports through the RC situational awareness will be enhanced. Instead of "submit information", it should be clarified that entities submit complete written reports to RC in electronic format.
Response: The DSR SDT thanks you for your comment. If the reporting hierarchy concept is adopted, it will include controls to ensure timely reporting, clear accountability so that risk of a violation of the standard is not transferred, and a process to ensure the responsible entities’ reported information remains as submitted.		

Organization	Yes or No	Question 2 Comment
American Electric Power	Yes	This approach may work as long as there is a uniform process across all of the Reliability Coordinators. AEP owns and operates BES facilities under three separate RCs and having differing rules and processes would create confusion and additional burdens. There are some concerns about the time lag of reporting the information and this might not work well in all cases especially if the information and knowledge are at the local level. AEP recommends that the standard could have a default hierarchy, but this should not prohibit any entity from reporting directly.
Response: The DSR SDT thanks you for your comment. Our goal is uniform reporting criteria to meet specified requirements. We will consider the risks and benefits of allowing a default hierarchical reporting structure with the ability for responsible entities to report directly to NERC.		
Bandera Electric Cooperative, Inc.	Yes	This approach, while I suspect will not be universally agreed to, should provide some definitive guidance in reporting.
Response: The DSR SDT thanks you for your comment.		
Dynegy Inc.	Yes	This seems to be straightforward approach in that the RC is the best judge of threats to the overall system and could eliminate multiple reports of a single event.
Response: The DSR SDT thanks you for your comment.		
Independent Electricity System Operator	Yes	We do not agree with the need of such a hierarchy setup solely for the purpose of making reports to the need-to-know entities. All responsible entities (RC, BA, TOP, etc.) need to file a report. With the proposed set up noted under Q3, which we support, these reports should go directly to NERC. The RC should not be held responsible for forwarding other entities' reports to NERC, and in doing so subject itself to potential non-compliance.
Response: The DSR SDT thanks you for your comment. If the reporting hierarchy concept is adopted, it will include controls to ensure timely reporting, clear accountability so that risk of a violation of the standard is not transferred, and a process to ensure the responsible entities' reported information remains as submitted.		

3. The goal of the DSR SDT is to have one report form for all functional entities (US, Canada, Mexico) to submit to NERC. Do you agree with this change? Please explain your response (yes or no) in the comment area.

Summary Consideration: Most stakeholders agreed with the concept of having one reporting form for all entities.

Several commenters suggested that there is no need for a standard on reporting as they considered it administrative in nature. Most thought it should be a guideline, rather than an enforceable standard.

There is widespread agreement that the one-size-fits-all approach would be very difficult to get agreement on, given the different countries and agencies involved. Many stakeholders pointed out that consistency and simplification were drivers for one report form.

Having multiple recipients, with different information requirements, seem to support an electronic format that would guide information only to those who need it. The concept of an electronic reporting tool would need to be further vetted and developed.

Organization	Yes or No	Question 3 Comment
Bandera Electric Cooperative, Inc.		No preference in this area.
ISO RTO Council Standards Review Committee	No	The SRC supports NERC's initiative for Results Based Standards. The SRC understood RBS to mean the results were reliability based quantities not administrative quantities. There is no need for a NERC Reliability standard on reporting. The idea that all functional entities in each of the said countries will use one form would be a good idea if and only if all the countries and all of their agencies were willing to accept that form. The SRC does not believe that those agencies will be willing to cede what information they ask for to NERC; nor that NERC will be able to create a single form that all such agencies will accept.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements. The set of results-based standards is intended to provide a 'defense-in-depth' approach to protecting reliability of the bulk power system. While many reports are administrative and are only used to assess compliance with specific requirements, the reporting addressed in this project is focused on providing data needed to support		

Organization	Yes or No	Question 3 Comment
after-the-fact analyses of events, and reporting information needed to maintain situaitional awareness. As such, the SDT believes that these reporting requirements do need to be enforceable.		
FirstEnergy	No	While one consistent form for reporting may simplify reporting requirements, it would be very difficult to get all governmental agencies to agree to a one-size-fits all approach.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		
Public Service Enterprise Group Companies	No	While simplification and consistency is a laudable goal, it should not be applied to different governmental agencies (USA, Canada, Mexico) which may have different structures and processes. Moreover, results based standards should not include administrative matters such as reporting forms.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements. The set of results-based standards is intended to provide a 'defense-in-depth' approach to protecting reliability of the bulk power system. While many reports are administrative and are only used to assess compliance with specific requirements, the reporting addressed in this project is focused on providing data needed to support after-the-fact analyses of events, and reporting information needed to maintain situaitional awareness. As such, the SDT believes that these reporting requirements do need to be enforceable.		
American Electric Power	Yes	
Constellation Power Source Generation	Yes	
Exelon	Yes	
PacifiCorp	Yes	
Platte River Power Authority	Yes	

Organization	Yes or No	Question 3 Comment
Calpine Corp.	Yes	A single approach is desirable, particularly for those entities that find themselves in multiple regions or countries.
Response: The DSR SDT thanks you for your comment.		
We Energies	Yes	Agree in conjunction with proposed concept that DOE OE-417 will be allowed to supplement the NERC report in lieu of duplicating entries.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		
Consumers Energy Company	Yes	Agreed - to the extent that it's consistent with the concept that any specific type of data is submitted to ONLY one entity.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		
Arizona Public Service Company	Yes	APS supports the standardization of the form for consistency and format.
Response: The DSR SDT thanks you for your comment.		
Bonneville Power Administration	Yes	As long as we don't make one form that requires extraneous information for the sake of having agreement.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		

Organization	Yes or No	Question 3 Comment
Western Electricity Coordinating Council	Yes	Canadian and Mexican entities should be consulted on content of report form to assure their "buy in".
Response: The DSR SDT thanks you for your comment. It is DSR SDT's intent to discuss the need for information with appropriate jurisdictional agencies.		
Central Hudson Gas & Electric	Yes	Central Hudson agrees with this goal if the intent is to develop and implement an electronic version that would meet DOE requirements as well.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		
E.ON U.S. LLC	Yes	E.ON U.S. supports the proposal.
Response: The DSR SDT thanks you for your comment.		
MRO's NERC Standards Review Subcommittee	Yes	However, We believe the primary goal should focus on "each entity" being able to submit one report for all functional requirements. Entities in the US that are required to submit the DOE OE-417 form should not be required to submit an additional form developed for other entities (Canada & Mexico). One approach to satisfy this goal is for NERC to require all entities (US, Canada, & Mexico) to complete the DOE OE-417 form as their report.
Response: The DSR SDT thanks you for your comment.		
Wolverine Power Supply Cooperative, Inc.	Yes	I can't see how anyone would disagree with this concept - However - I question how practical it will be to implement, since various agencies would have to collaborate and coordinate to accomplish this task.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		

Organization	Yes or No	Question 3 Comment
Lands Energy Consulting	Yes	I think that the impact approach makes sense and that EOP-004 and CIP-001 are logically connected. Many entities of which I am aware link Sabotage Reporting Training to Disturbance Reporting obligation awareness already.
Response: The DSR SDT thanks you for your comment.		
Oncor Electric Delivery Company LLC	Yes	Oncor agrees that by using the same type reporting format, there should be consistency in regard to each functional entity's expectations.
Response: The DSR SDT thanks you for your comment.		
BGE	Yes	One form makes sense to us; less is better is the sense that it makes filing reports easier by not creating unnecessary complications.
Response: The DSR SDT thanks you for your comment.		
Ameren	Yes	One report would be great for this standard. While this standard needs simplification and automation, we strongly suggest developing a guideline for reporting rather than enforceable standards.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements. The set of results-based standards is intended to provide a 'defense-in-depth' approach to protecting reliability of the bulk power system. While many reports are administrative and are only used to assess compliance with specific requirements, the reporting addressed in this project is focused on providing data needed to support after-the-fact analyses of events, and reporting information needed to maintain situaitional awareness. As such, the SDT believes that these reporting requirements do need to be enforceable.		
Portland General Electric	Yes	PGE supports the efforts of the Standards Drafting Team on the SAR for Project 2009-01 to consolidate the disturbance and sabotage reporting processes as outlined in the concept paper.
Response: The DSR SDT thanks you for your comment.		
Dynegy Inc.	Yes	Please keep it short and simple.

Organization	Yes or No	Question 3 Comment
Response: The DSR SDT thanks you for your comment.		
ERCOT ISO	Yes	Standardization ensures consistency and relevance of the information received.
Response: The DSR SDT thanks you for your comment.		
USBR	Yes	The Bureau of Reclamation utilizes a form for tracking unexpected events. This form contains information which the agency considers important for its one reliability improvement program. The form is also used to meet NERC standard requirements for protection system operations analysis. This form contains most of information required by DOE. The SDT should consider requiring the submission of specific information rather than lock responses in one specific form. In this manner the agency would be avoid duplicate forms, one for NERC, the other for agency purposes.
Response: The DSR SDT thanks you for your comment.		
Central Lincoln	Yes	The existing reporting is needlessly complex. We appreciate the SDT's goal.
Response: The DSR SDT thanks you for your comment.		
SPS Consulting Group Inc.	Yes	There should have probably been one report all along.
Response: The DSR SDT thanks you for your comment.		
Duke Energy	Yes	There should only be one report for all functional entities to submit to NERC.
Response: The DSR SDT thanks you for your comment.		
SERC Reliability Coordinator Sub-committee (RCS)	Yes	There should only be one report for all functional entities.
Response: The DSR SDT thanks you for your comment.		
Manitoba Hydro	Yes	This is a promising idea, though there would be different requirements for the three countries, this could easily be rectified with "drop down menus". This electronic form could contain a lot of information without distracting clutter as you "tree" down the menu depending on the event that occurred. This could also contain electronic

Organization	Yes or No	Question 3 Comment
		references to information located in Attachment 1-EOP-004 and Threat and Incident Reporting.
Response: The DSR SDT thanks you for your comment. We will consider your specific suggestions when we develop the reporting requirements.		
Hydro-Québec TransEnergie (HQT)	Yes	We agree with the concept that there should be one report form for all functional entities (whether located in the US, Canada, Mexico) for use in reporting to NERC. This would provide for a consistent reporting format across the continent.
Response: The DSR SDT thanks you for your comment.		
Northeast Power Coordinating Council	Yes	We agree with the concept that there should be one report form for all functional entities (whether located in the US, Canada, Mexico) for use in reporting to NERC. This would provide for a consistent reporting format across the continent.
Response: The DSR SDT thanks you for your comment.		
Orange and Rockland Utilities, Inc.	Yes	We agree with the concept that there should be one report form for all functional entities (whether located in the US, Canada, Mexico) for use in reporting to NERC. This would provide for a consistent reporting format across the continent.
Response: The DSR SDT thanks you for your comment.		
Midwest ISO Standards Collaborators	Yes	We agree with the goal of having a single report form but believe there will be a significant challenge to get varying governmental agencies to agree on single report format.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		
Edison Mission Marketing & Trading	Yes	With the realization that having a common report form may be difficult to coordinate between differen agencies.
Response: The DSR SDT thanks you for your comment. The DSR SDT acknowledges the difficulty in attempting to present a single form. However, the DSR SDT believes it may be possible to achieve consolidation since the various reports ask repetitive questions. For example, having to provide		

Organization	Yes or No	Question 3 Comment
contact names, telephone numbers, email addresses on multiple forms is not an effective use of time or resources. Similarly, answering the question "Describe the event" or "What steps did you take" on multiple reporting forms is also not effective. The DSR SDT does recongnize that it may not be possible to eliminate reporting to multiple jurisdicational agencies due to legislative or regulatory requirements.		
Independent Electricity System Operator	Yes	Yes, this will simplify the reporting effort. NERC may forward the reports to the other need-to-know entities.
Response: The DSR SDT thanks you for your comment.		
Electric Market Policy	Yes	Yes, we agree with the concept that there should be one report form for all functional entities (whether located in the US, Canada, Mexico) for use in reporting to NERC.
Response: The DSR SDT thanks you for your comment.		

4. The goal of the DSR SDT is to eliminate the need to file duplicate reports. The standards will specify information required by NERC for reliability. To the extent that this information is also required for other reports (e.g. DOE OE-417), those reports will be allowed to supplement the NERC report in lieu of duplicating the entries in the NERC report. Do you agree with this concept? Please explain your response (yes or no) in the comment area.

Summary Consideration: Most stakeholders agreed with the concept of entities being able to use information from other sources such as the OE-417 form, to supplement the NERC report form. Some thought that duplicate reports were acceptable, as long as the information was not duplicated (if # of customers lost is required on form A, don't ask on forms B & C). Several stakeholders commented on the need for an electronic, one stop reporting tool. This would avoid duplication while ensuring that the information reported goes only to intended recipients. With an electronic, one stop reporting tool, reports can be updated/corrected instantly, without repeating previously submitted information. Some stakeholders cautioned that the OE-417 can change every three years and this should be taken into account when developing an electronic reporting tool. Again, such a reporting tool would need to be vetted and developed to meet reliability needs.

Organization	Yes or No	Question 4 Comment
ERCOT ISO		ERCOT ISO agrees with the concept of eliminating the need to file duplicate reports, but as stated in the Concept Paper, the DOE form (OE-417) is required by law. Based on this, the elimination of EOP-004 (after the fact reporting) is essential, since the OE-417 is mandatory and all-inclusive.
Response: The DSR SDT thanks you for your comment. We agree that the OE-417 compiles a baseline set of information for disturbances, however, it does not function as an all-inclusive report of sabotage and cyber security incidents. The DSR SDT certainly seeks to gain effienciencies through the modification of EOP-004 and CIP-001, which may include the elimination of one or both. Further, the OE-417 is only mandatory for US entities.		
Midwest ISO Standards Collaborators	No	It certainly makes sense to eliminate duplication in reporting and to allow supplemental information to be submitted in other reports. However, it does not make sense to require reporting to other governmental agencies through NERC enforceable NERC standards. Those governmental agencies already have legal authority to compel reporting. Again, we support developing a guideline for reporting rather than enforceable standards. The guideline could certainly explain the various reporting requirements and supplemental reporting requirements mentioned in the question without causing the issues we have identified in our comments.
Response: The DSR SDT thanks you for your comment. The DSR SDT does not envision a NERC standard mandating submission of reports to DOE, which is mandatory under Public Law for US entities. If the DSR SDT is able to develop a one-stop-shopping electronic form, we plan to develop an		

Organization	Yes or No	Question 4 Comment
option to have the report submitted to NERC, DOE and FERC simultaneously. If an entity chooses to submit the report manually, they will then also be responsible for following DOE regulations and other mandatory requirements.		
Consumers Energy Company	No	NERC should either coordinate with DOE for a single reporting process or simply adopt the DOE's standard.
Response: The DSR SDT thanks you for your comment. The DSR SDT does not envision a NERC standard mandating submission of reports to DOE, which is mandatory under Public Law for US entities. If the DSR SDT is able to develop a one-stop-shopping electronic form, we plan to develop an option to have the report submitted to NERC, DOE and FERC simultaneously. If an entity chooses to submit the report manually, they will then also be responsible for following DOE regulations and other mandatory requirements. The DOE report does not collect all the information that NERC needs.		
E.ON U.S. LLC	No	Reliability standards are federal law enforced by fines that can reach up to $1,000,000 per day of violation. There is no reason to deliberately include ambiguity, i.e. "gray areas," in requirements such that registered entities are left unable to determine what it is they must do or refrain from doing to remain compliant. "Sabotage" for the purposes of these standards must be defined.
Response: The DSR SDT thanks you for your comment. The intent of the DSR SDT is to develop requirements for reporting that will be clear and unambiguous with respect to compliance issues. Sabotage will be included in the reporting for "impact events", but may not be called 'sabotage' as there are many different interpretations of "sabotage".		
ISO RTO Council Standards Review Committee	No	The concept of eliminating duplication is laudable, but the idea of writing a standard to mandate reporting that involves reporting to governmental areas does not make sense unless NERC will do all of the reporting for the Industry. A governmental agency is as likely as not to change the forms they require which would then mean two different reports (one for NERC and one for the given agency) or that the standard would have to be re-written every time there is a change.
Response: The DSR SDT thanks you for your comment. The DSR SDT does not envision a NERC standard mandating submission of reports to DOE, which is mandatory under Public Law for US entities. If the DSR SDT is able to develop a one-stop-shopping electronic form, we plan to develop an option to have the report submitted to NERC, DOE and FERC simultaneously. If an entity chooses to submit the report manually, they will then also be responsible for following DOE regulations and other mandatory requirements.		
Ameren	No	The DOE OE-417 report should not supplement the NERC report due to the fact that the majority of reportable events are defined in/come from the OE-417 report. The NERC reporting form should be based on the OE-417 report and then include additional reporting requirements defined by NERC. However, it does not make sense to require reporting to the governmental agencies through enforceable NERC standards. The governmental agencies already have legal authority to compel reporting.

Organization	Yes or No	Question 4 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT does not envision a NERC standard mandating submission of reports to DOE, which is mandatory under Public Law for US entities. If the DSR SDT is able to develop a one-stop-shopping electronic form, we plan to develop an option to have the report submitted to NERC, DOE and FERC simultaneously. If an entity chooses to submit the report manually, they will then also be responsible for following DOE regulations and other mandatory requirements.		
SERC Reliability Coordinator Sub-committee (RCS)	No	The requirement should be a single report that satisfies the need for all US governmental agencies as well as NERC and the RRO's.
Response: The DSR SDT thanks you for your comment. The intent of the DSR SDT is to develop standards to address the reliability needs for NERC and not governmental agency reporting criteria.		
Western Electricity Coordinating Council	No	This will work well for the USA entities to save us time in re-entering the same information. We believe that FERC and NERC and the Regions should have one common reporting form for North America. The OE-417 is not required by law outside of the United States. Canadian and Mexican entities may feel that US DOE has no jurisdiction in these countries, and therefore no right to required reporting as is stated on the OE-417.
Response: The DSR SDT thanks you for your comment. We agree that the OE-417 report is not required for Canadian or Mexican entities. The DSR SDT does not envision a NERC standard mandating submission of reports to DOE. If the DSR SDT is able to develop a one-stop-shopping electronic form, we plan to develop an option to have the report submitted (or not) to NERC, DOE and FERC simultaneously. If an entity chooses to submit the report manually, they will then also be responsible for following DOE regulations and other mandatory requirements.		
American Electric Power	Yes	
Edison Mission Marketing & Trading	Yes	
Exelon	Yes	
Orange and Rockland Utilities, Inc.	Yes	
PacifiCorp	Yes	
Platte River Power Authority	Yes	

Organization	Yes or No	Question 4 Comment
Arizona Public Service Company	Yes	APS supports eliminating the need to file duplicate reports. This standardized form should generate and send the DOE OE-417 report, totally eliminating duplicate work. Streamline the process.
Response: The DSR SDT thanks you for your comment.		
Central Hudson Gas & Electric	Yes	Central Hudson agrees with this concept and, as stated in a previous response, recommends that the ability of utilizing the DOE OE-417 to supplement the NERC report be maintained.
Response: The DSR SDT thanks you for your comment.		
Calpine Corp.	Yes	Clarification, simplicity and the removal of duplicate reporting is beneficial.
Response: The DSR SDT thanks you for your comment.		
Constellation Power Source Generation	Yes	Constellation agrees with the concept of eliminating the need to file duplicate reports. If the single NERC reporting form is both comprehensive and easy to use, then using a single report should not be an issue. It is essential that all elements of DOE OE-417, and any similar documents, be incorporated into this single report. Not incorporating all elements will result in gaps in reporting for all Registered Entities.
Response: The DSR SDT thanks you for your comment.		
SPS Consulting Group Inc.	Yes	Duplication is inefficient and casts the whole reporting mechanism in a questionable light.
Response: The DSR SDT thanks you for your comment.		
We Energies	Yes	However, also evaluate whether or not DOE OE-417 is sufficient in lieu of a NERC report. If additional information is required, duplicate format of DOE-OE-417 with additional NERC information listed at the end of the form.
Response: The DSR SDT thanks you for your comment.		
Wolverine Power Supply Cooperative, Inc.	Yes	I agree with the concept of minimizing duplication - See previous question 3 for concerns.
Response: The DSR SDT thanks you for your comment.		

Organization	Yes or No	Question 4 Comment
USBR	Yes	It should be clear what information is to be supplemented. The fewer times the information has to be handled the more efficient the process becomes. If the information exists on a required form, that legal form should be allowed. Also, if the form is already submitted, then reference to it should be sufficient rather than requiring resubmission of the form. That would require handling the information again. As explained in the previous answer, the SDT should recognize that responsible entities have already developed internal reporting processes which utilize forms for consistent responses. Those forms may contain more information than is needed by the new standard to be proposed. The entity should be allowed to submit the internal form or else duplication would be created, which may reduce the effectiveness of an entities reliability improvement program.
Response: The DSR SDT thanks you for your comment. The DSR SDT envisions a one-stop-shopping form that allows reports to be saved, revised and resubmitted at a later date without re-entry of data or information. However, as a caution the DSR SDT cannot guarantee the possibility to submit custom forms.		
Lands Energy Consulting	Yes	Less paperwork and fewer requirements to keep in mind during what may be once in a lifetime events are always good.
Response: The DSR SDT thanks you for your comment.		
Luminant	Yes	Luminant agrees with the concept of reducing reporting requirements, but asks the SDT to go even further. In the concept paper, the SDT discussed that information would not be duplicated on the NERC report and the DOE OE-417 report. The concept paper described a process where one report would simply supplement the other, but two reports would still be filed when required. Can the NERC SDT work with the DOE to develop one report to meet the needs of NERC and the DOE?
Response: The DSR SDT thanks you for your comment. We will consult with the DOE to see if it one report will meet the reporting needs for NERC and the DOE. NERC reliability needs will take precedence.		
Bonneville Power Administration	Yes	Minimizing the number of reports is a good thing. The concept of actually sharing information should be utilized as much as practical.
Response: The DSR SDT thanks you for your comment.		
Oncor Electric Delivery Company LLC	Yes	Oncor agrees that this effort should eliminate file duplication

Organization	Yes or No	Question 4 Comment
Response: The DSR SDT thanks you for your comment.		
Bandera Electric Cooperative, Inc.	Yes	One can only assume the number of reports required in this area will continue to increase in terms of scope and to which agency wants this data. The SDT is encouraged to attempt to find a reporting format and scope that does not needlessly duplicate or complicate overall reporting obligations.
Response: The DSR SDT thanks you for your comment. We will consult with the DOE and FERC to see if it one report will meet the reporting needs for NERC, FERC and the DOE. NERC reliability needs will take precedence.		
Portland General Electric	Yes	PGE supports reducing the duplication of reporting.
Response: The DSR SDT thanks you for your comment.		
Dynegy Inc.	Yes	Short and simple should be the goal.
Response: The DSR SDT thanks you for your comment.		
Duke Energy	Yes	Since the OE-417 is a DOE required report, it must be submitted. Including the OE-417 as part of the NERC electronic form will facilitate reporting to NERC.
Response: The DSR SDT thanks you for your comment. We will consult with the DOE to see if it one report will meet the reporting needs for NERC and the DOE. NERC reliability needs will take precedence.		
Central Lincoln	Yes	The existing reporting is needlessly complex. We appreciate the SDT's goal.
Response: The DSR SDT thanks you for your comment.		
Public Service Enterprise Group Companies	Yes	The PSEG Companies agree with the avoidance of duplicate reports. NERC report forms should not include anything in the DOE form, and NERC Regional report forms should not include anything in the DOE or NERC forms. Hence, a DOE report should not "supplement" a NERC form, but rather replace it unless the NERC form calls for other information for the same reportable incident, and likewise for the DOE - NERC - Regional form structure. DOE forms would be filed with DOE, NERC and the Regional Entity where the event originated. NERC forms would be filed with NERC and the region where the event originated and the Regional form filed only with the Region. In designing the NERC and Regional forms, the need to file multiple reports should be minimized, and in no event should any of the three (DOE, NERC, Region) forms contain

Organization	Yes or No	Question 4 Comment
		duplicative information requests.
Response: The DSR SDT thanks you for your comment. We will consider your comment in the development of the reporting structure / forms.		
Manitoba Hydro	Yes	This could be easily incorporated into the electronic form. You could be prompted for information required immediately, and notified for information that could be entered later. This form could contain all the enterable data that all agencies could require. If the form is live and on line, all entities could be notified (depending on the entries) of an going event immediately. Form could be web based similar to ARS program or even integrated into the ARS program.
Response: The DSR SDT thanks you for your comment. We will consider your comment in the development of the reporting structure / forms.		
FirstEnergy	Yes	We agree that the simplification and consistency of reporting will improve the reporting of this information. We support the drafting team's efforts in this area and hope that all regulatory agencies will as well. However, as we have mentioned in our other comments, the reporting requirements should not be in a reliability standard unless they are proven to be necessary to maintain an Adequate Level of Reliability of the BES. Reporting of these events should be required by NERC in arenas outside of the standards.
Response: The DSR SDT thanks you for your comment. The information provided in the reports is either used after the fact for analyses or used to maintain situational awareness, and is needed for reliability.		
MRO's NERC Standards Review Subcommittee	Yes	We agree with the concept to eliminate duplicate reports. However, we are concerned with the reference of the DOE OE-417 report being a “supplement” of the NERC report rather than “accepted” as the NERC report.
Response: The DSR SDT thanks you for your comment. Future NERC reliability reporting needs may not totally align with DOE report information. Therefore, the OE-417 report would not necessarily substitute for the NERC report. The DOE Reporting Form OE 417 is currently mandatory by Public for US entities.		
Hydro-Québec TransEnergie (HQT)	Yes	We agree with the objective of eliminating duplicate reporting. However, EOP-004 currently allows substitution of DOE OE-417 in place of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report. As suggested in the Concept Paper, entities meeting the criteria of OE-417 are still obligated to file a report with DOE. Given that and the fact that CIP-001 requires no actual reporting, it is not clear where duplication exists today. We agree with the recommendation to eliminate the need for filing duplicate reports such as the DOE form OE-417. There is no benefit with regard to CIP-001 in filing separate reports. Duplicate reports introduce the potential for incomplete information to be supplied to responsible parties.

Organization	Yes or No	Question 4 Comment
		Removing jurisdictional agencies from the Standard, and having NERC provide either query or situational awareness to those agencies being considered, might not be easy to achieve. There is an obligation under law to require entities to report to the DOE on the OE-417 form as amended or modified. This might drive the "omitted" agencies to have reporting laws enacted as well.
Northeast Power Coordinating Council	Yes	We agree with the objective of eliminating duplicate reporting. However, EOP-004 currently allows substitution of DOE OE-417 in place of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report. As suggested in the Concept Paper, entities meeting the criteria of OE-417 are still obligated to file a report with DOE. Given that and the fact that CIP-001 requires no actual reporting, it is not clear where duplication exists today. We agree with the recommendation to eliminate the need for filing duplicate reports such as the DOE form OE-417. There is no benefit with regard to CIP-001 in filing separate reports. Duplicate reports introduce the potential for incomplete information to be supplied to responsible parties. Removing jurisdictional agencies from the Standard, and having NERC provide either query or situational awareness to those agencies being considered, might not be easy to achieve. There is an obligation under law to require entities to report to the DOE on the OE-417 form as amended or modified. This might drive the "omitted" agencies to have reporting laws enacted as well.
Response: The DSR SDT thanks you for your comment. The DSR SDT has discussed the possibility of consolidating CIP-001 and EOP-004 to create a single reporting standard. FERC directives require modifications to the standards which also may impose additional reporting requirements (see paragraph 470 of Order 693). **We concur with your comments regarding the legal obligations to submit certain reports. The DSR SDT is attempting to consult with appropriate governmental aencies to address this.**		
BGE	Yes	We agree with this approach, as long as the latest version of the DOE OE-417 form is fully incorporated in the new single-reporting form, so that it maintains its credibility with the DOE.
Response: The DSR SDT thanks you for your comment. The intent is to maintain credibility with the DOE reporting requirements.		
Independent Electricity System Operator	Yes	We support this concept since it works well for those entities that are not required to file reports with the US agencies, e.g. the DOE.
Response: The DSR SDT thanks you for your comment.		
Electric Market Policy	Yes	Yes, we agree with the objective of eliminating duplicate reporting; however, EOP-004 currently allows

Organization	Yes or No	Question 4 Comment
		substitution of DOE OE-417 in place of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report. As suggested in the Concept Paper, entities meeting the criteria of OE-417 are still obligated to file a report with DOE. Given that and the fact that CIP-001 requires no actual reporting, it is not clear where duplication exists today.
Response: The DSR SDT thanks you for your comment. The DSR SDT has discussed the possibility of consolidating CIP-001 and EOP-004 to create a single reporting standard. FERC directives require modifications to the standards which also may impose additional reporting requirements (see paragraph 470 of Order 693).		

5. In its discussion concerning sabotage, the DSR SDT has determined that the spectrum of all sabotage-type events is not well understood throughout the industry. In an effort to provide clarity and guidance, the DSR SDT developed the concept of an impact event. By developing impact events, it allows us to identify situations in the "gray area" where sabotage is not clearly defined. Other types of events may need to be reported for situational awareness and trend identification. Do you agree with this concept? Please explain your response (yes or no) in the comment area.

Summary Consideration: The majority of stakeholders agreed with the concept of impact events. Some stakeholders felt that the introduction of impact events increased the risk that some items will go unreported. However, most felt that impact events would dramatically increase the number of reports being submitted, and it would be difficult to separate important information from background noise. Several respondents felt that the SDT ignored the FERC Directive, and did not define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event. Many respondents supplied the SDT with their own definition of "Sabotage". The DSR SDT believes that the concept of impact events and the specificity of what needs to be reported in the standard will be an equally efficient and effective means of addressing the FERC directive regarding sabotage. Some stakeholders felt that impact events add another layer of uncertainty to the reporting. Even with the switch from sabotage to impact events, several felt that "intent" was still key to determining reportability.

Organization	Yes or No	Question 5 Comment
ERCOT ISO		ERCOT ISO recognizes the risks associated with "gray areas" not being clarified. While "gray areas" pose compliance risk due to differing interpretations, a risk remains that some items will go unreported. A more prescriptive approach raises an even greater risk of events not being reported. People will not report events that are not specifically listed, and will not use judgment in determining the need for reporting.
Response: The DSR SDT thanks you for your comment. We agree that a more prescriptive approach could pose greater risks but we will attempt to clarify and define an approach to assist the industry and stakeholders for reporting impact events.		
Constellation Power Source Generation	No	Although defining an impact event would bring clarity to defining sabotage events, adding another situation would further complicate things. Furthermore, the examples of impact events used all fall under the Sabotage category in the Threat and Incident Reporting Guideline. Constellation Power Generation suggests the SDT further clarifies the items in the Sabotage category to ensure all grey area situations are included. Clarification is also needed in how a Cyber Security Incident (CIP-008) would map into the categories of Disturbance/Impact Events (CIP-001). To that point, Constellation Power Generation questions whether cyber related incidents should fall under the spectrum of sabotage type events, or remain separate and be incorporated in the CIP revisions. Having cyber related incidents separate from other sabotage events would

Organization	Yes or No	Question 5 Comment
		provide the clarity and guidance that the DSR SDT is striving to achieve.
Response: The DSR SDT thanks you for your comment. We are suggesting the term "Impact Event" be substituted to include all events that would impact the reliability of the BES. Events now included in reporting requirements that do not impact the reliability of the BES would be excluded from the reporting unless the DSR SDT clarifies why it should be included and under what specific instances or examples.		
Duke Energy	No	As FERC ordered in Order No. 693, the drafting team should further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event. Suggested definition: "Sabotage - the malicious destruction of, or damage to assets of the electric industry, with the intention of disrupting or adversely affecting the reliability of the electric grid for the purposes of weakening the critical infrastructure of our nation."
Response: The DSR SDT thanks you for your comment. The SDR SDT struggles with terms that deal with determing "intent" which may not be determined until after a lengthy investigation. We will continue to discuss for inclusion in a future draft of this project. The DSR SDT believes that the concept of impact events and the specificity of what needs to be reported in the standard will be an equally efficient and effective means of addressing the FERC directive regarding sabotage.		
Kootenai Electric Cooperative	No	Impact events seems to add another layer of uncertainty to the reporting. Define a transmission line. Our transmission lines have very little impact on the grid. It is possible for our lines to cause a local area outage on our transmission provider - but neither is of national security interest or even regional interest. There is no power flow going on across the lines other than local power delivery supply. It seems you run more risk of losing the important reports in the snow of reporting - similar to what we have to avoid on our SCADA systems for our operators to see the key information.
Response: The DSR SDT thanks you for your comment. The DSR SDT understands your concern and this was discussed a great deal. It is our belief that criteria of the "impact events" to be reported will be properly defined and discriminated from local events that have no impact on the reliability of the BES.		
SERC Reliability Coordinator Sub-committee (RCS)	No	Impact events that do not affect reliability should not be reported.
Response: The DSR SDT thanks you for your comment. The DSR SDT agrees but a balance must be further explored to meet industry and regulatory requirements specifically under FERC Order 693.		
Luminant	No	Luminant would prefer to report disturbances and sabotage events. The reporting of impact events could lead to unnecessary reporting. A definition of an "impact event" may be even more confusing than sabotage

Organization	Yes or No	Question 5 Comment
		events.
Response: The DSR SDT thanks you for your comment. The DSR SDT understands your concern and this was discussed a great deal. It is our belief that criteria of the "impact events" to be reported will be properly defined and discriminated from local events that have no impact on the reliability of the BES. We are suggesting the term "Impact Event" be substituted to include only events that would impact the reliability of the BES. Events now included in reporting requirements that do not impact reliabiltiy of the BES would be excluded from the reporting unless the DSR SDT clarifies why it should be included and under what specific instances or examples.		
Orange and Rockland Utilities, Inc.	No	Physical and cyber events must be investigated before a determination of sabotage or impact event can be made. Impact events should define or clarify the circumstances that would or could affect reliability. Reportable items should be based on impact to reliability, not on 'newsworthy' events or to gather information for trending. It is the law enforcement industry's responsibility to make a determination of "sabotage" or other. This determination cannot definitively be made by industry (operating) personnel. If NERC's definition is expanded for CIP-001 and/or EOP-004, responsibility and timing of reporting needs to addressed so that appropriate agencies conduct the investigation and assessment. Operating personnel need to remain focused on the primary responsibility of mitigating the effects.
Response: The DSR SDT thanks you for your comment. The SDR SDT struggles with terms that deal with determing "intent" which may not be determined until after a lengthy investigation. We will continue to discuss these ideas for inclusion in a future draft of this project. Timing of the reporting process will be further clarified based upon your comments and those in the industry that have voiced similar concerns.		
MRO's NERC Standards Review Subcommittee	No	Rather than attempting to define a new term (impact event), we suggest that the concept of impact event be replaced with further defining sabotage and providing guidance on trigger events (impact event) that would cause an entity to report.
Response: The DSR SDT thanks you for your comment. We will continue to discuss the FERC "Clarification of sabotage" directive and seek further guidance to meet this directive. The term sabotage has created conflict in its meaning among stakeholders as to when its determined and by whom and how long an investigation would take to make that call on the intent of the saboteur. The DSR SDT is reviewing what a reportable disturbance actually is and sabotage may be a sub component of a reportable disturbance event.		
Lands Energy Consulting	No	The level of complexity described will overwhelm the 20-200 employee utilities that have yet to see - and will never see - the kind of sabotage event that scares the Department of Homeland Security.
Response: The DSR SDT thanks you for your comment. The DSR SDT does not intend for the reporting of impact events to overwhelm smaller entities. If events do not affect the reliability of the BES, then it is our intent that they will be excluded from reporting requirements under our proposal. We will attempt to clarify and define an approach to assist the industry and stakeholders for reporting impact events. FERC cautioned the		

Organization	Yes or No	Question 5 Comment
industry that acts of sabotage may be "tested" on smaller entities and ultimately on larger entities.		
ISO RTO Council Standards Review Committee	No	The nature of the fact that "gray areas" exists preclude the idea of using a standard to report; particularly a standard for the vague topic of motivation such as sabotage events and the more defined disturbance events.
Response: The DSR SDT thanks you for your comment. We will attempt to clarify and define an approach to assist the industry and stakeholders for reporting impact events.		
Edison Mission Marketing & Trading	No	There are too many special circumstances to try and capture. I feel this would be best delivered as a guideline.
Response: The DSR SDT thanks you for your comment. We are suggesting the term "Impact Event" be substituted to include only events that would impact the reliability of the BES. Events now included in reporting requirements that do not impact reliability of the BES would be excluded from the reporting unless the DSR SDT clarifies why it should be included and under what specific instances or examples.		
Exelon	No	We agree with the direction to identify impact events examples that would trigger reporting and not be limited to sabotage reporting only. It is important to note that when an incident occurs, some level of investigation is required before a determination can be made as to the event is sabotage or not. The focus should be on reporting events when they occur and allow follow-up investigations to make the sabotage determination. That being said, care must be taken in the development of any list of impact events so that it doesn't become or is misinterpreted to be a definitive list. Therefore if it is not on the list, it is not reportable.
Response: The DSR SDT thanks you for your comment. We concur and plan to allow reports to be submitted, edited and re-submitted in the one-stop-shopping reporting tool. We are suggesting the term "Impact Event" be substituted for sabotage andinclude only events that would impact the reliability of the BES. Events now included in reporting requirements that do not impact reliability of the BES would be excluded from the reporting unless the DSR SDT clarifies why it should be included and under what specific instances or examples.		
Midwest ISO Standards Collaborators	No	We agree with the idea of identifying impact events but do not support the requirement for these to be always reported through the hierarchical structure identified in question 2. If an impact event only affects one entity, that entity should have the reporting requirement.
Response: The DSR SDT thanks you for your comment. The DSRSDT will continue to explore the benefits and weaknesses of the hierarchy reporting structure.		
Hydro-Québec TransEnergie (HQT)	No	We believe that physical and cyber events must be investigated before a determination of sabotage or impact event can be made. The purpose of the NERC Standards is to maintain the reliability of the BES. Therefore,

Organization	Yes or No	Question 5 Comment
		impact events should define or clarify the circumstances that would or could affect reliability. Reportable items should be based on impact to reliability, not on 'newsworthy' events or to gather information for trending. It is the law enforcement industry's responsibility to make a determination of "sabotage" or other. This determination cannot definitively be made by industry personnel, there is no expertise or time to investigate causes. It is the industry's job to mitigate effects. Examples would help provide for better guidance/direction. Industry examples would be welcomed to help reinforce developed internal processes for compliance.
Northeast Power Coordinating Council	No	We believe that physical and cyber events must be investigated before a determination of sabotage or impact event can be made. The purpose of the NERC Standards is to maintain the reliability of the BES. Therefore, impact events should define or clarify the circumstances that would or could affect reliability. Reportable items should be based on impact to reliability, not on 'newsworthy' events or to gather information for trending. It is the law enforcement industry's responsibility to make a determination of "sabotage" or other. This determination cannot definitively be made by industry personnel, there is no expertise or time to investigate causes. It is the industry's job to mitigate effects. Examples would help provide for better guidance/direction. Industry examples would be welcomed to help reinforce developed internal processes for compliance.
Response: The DSR SDT thanks you for your comment. The SDR SDT struggles with terms that deal with determing "intent" which may not be determined until after a lengthy investigation. We will continue to discuss issues with sabotage for inclusion in a future draft of this project. Timing of the reporting process will be further clarified based upon your comments and those in the industry that have voiced similar concerns.		
American Electric Power	Yes	
Calpine Corp.	Yes	
PacifiCorp	Yes	
Platte River Power Authority	Yes	
Central Lincoln	Yes	An act of vandalism may have impact. An act of sabotage may not be impactful alone, but may be part of a wider coordinated attack. Dictionary definitions speaking of "intent" are not helpful in this regard, since acts of vandalism and sabotage are both generally committed intentionally. Saboteurs, though, work for a higher cause. That cause may be political, social, environmental, etc. We ask that the SDT look beyond dictionary definitions in developing a definition of sabotage.

Organization	Yes or No	Question 5 Comment
Response: The DSR SDT thanks you for your comment. The SDR SDT struggles with terms that deal with determing "intent". The term sabotage has created conflict in its meaning among stakeholders as to when its determined and by whom and how long an investigation would take to make that call on the intent of the saboteur. We will strive to meet this challenge with the input on the right language from government agencies and industry experience expertise.		
Bonneville Power Administration	Yes	BPA agrees with providing an industry-wide definition and guideline. We do NOT agree with requiring reports for every instance of every activity. If your definition is good, you'll get what is needed and not much chaff.
Response: The DSR SDT thanks you for your comment.		
Central Hudson Gas & Electric	Yes	Central Hudson agrees with this concept, particularly if the reporting hierarchy through the RC is implemented in order to better identify trends.
Response: The DSR SDT thanks you for your comment. The DSRSDT will continue to explore the benefits and weaknesses of the hierarchy reporting structure.		
Wolverine Power Supply Cooperative, Inc.	Yes	I agree with the concept of focusing on impact instead of the type of event (sabotage, accident, vandalism, etc.)I hope that the reporting proposal that comes out of this project will clearly make a separation between true impact events that must be reported per the standards (enforceable), vs. "other" information that may be (electively - not enforceable) reported, per some set of guidelines.
Response: The DSR SDT thanks you for your comment. We agree reportable items should be based on impact to reliability and with other commenters that expressed a desire to avoid reporting on 'newsworthy' events but to gather meaningful information for trending. We are suggesting the term "Impact Event" be substituted for sabotage to include only events that would impact the reliability of the BES.		
Bandera Electric Cooperative, Inc.	Yes	In principle, I agree with this concept. Would like for the SDT to pursue this further and seek additional comments at that time.
Response: The DSR SDT thanks you for your comment. We will seek further comments on the concept and will prepare the beginnings of the first draft soon.		
Oncor Electric Delivery Company LLC	Yes	Oncor agrees that there are no broadly used guidance documents that detail how an event may be accurately defined.
Response: The DSR SDT thanks you for your comment. We agree that further industry guidance of a clear and understandable standard should be sought under the new Results Based approach. We will attempt to clarify and define an approach to assist the industry and stakeholders in reporting		

Organization	Yes or No	Question 5 Comment
impact events.		
Portland General Electric	Yes	PGE supports the DSR SDT's efforts to bring clarity and guidance to the spectrum of sabotage-type events.
Response: The DSR SDT thanks you for your comment.		
FirstEnergy	Yes	The concept paper makes good progress in this area and the drafting team is on the right track, and agree that better clarity needs to be developed surrounding sabotage events. However, some of the examples stated in the paper are too vague and do not address extenuating circumstances or reasons for the events. One example sighted in the paper is "Bolts removed from transmission line structures." This statement may be too broad. For instance, if the bolts are removed from the tower and the organization is not experiencing a labor dispute, it could be considered a sabotage event with wide area implications. However, if the organization is in the middle of a labor dispute, this would be vandalism and would most likely not be of a wide area concern. Also, the number and location of towers affected could be an important determination related to the risk the event imposes on the Bulk Electric System.
Response: The DSR SDT thanks you for your comment. We concur with your comments that the number and location of the towers affected may have a "local" vs "wide area" concern. However, under the "impact event" reporting that we are proposing, both scenarios above should be reported as impact events as long as it affects the BES.		
Public Service Enterprise Group Companies	Yes	The PSEG Companies agree with the concept, but reserve judgment on the descriptions of the impacts. There is clearly a need to better define what constitutes a sabotage incident versus common theft or vandalism. Moreover, where it may be impossible to determine if any given incident (e.g., several loose bolts on a transmission tower cross brace could be sabotage or could be human error in construction) falls within sabotage, a registered entity should not be second guessed in an audit if the registered entity determines not to report. Excessive unnecessary reporting can mask real incidents.
Response: The DSR SDT thanks you for your comment. The DSR SDT agrees with clearly defining a reportable impact versus common theft. Concern over reporting an incident and the audit process are within the discussions of the DSR SDT and will be fully explored to assist with the 1st Draft. The ability to identify trends could be very important compared to isolated incidents that do not impact the BES. Every effort to explore this balance of reporting will be taken into account.		
SPS Consulting Group Inc.	Yes	The term sabotage was always too narrow a concept for the standards. At times, questionable activities are not confirmed as sabotage events until well after the fact, forcing the registered entity to speculate on whether or not to report an activity that may not be a confirmed sabotage event at the time, and hence encounter another silly violation based on imprecise terminology.

Organization	Yes or No	Question 5 Comment
Response: The DSR SDT thanks you for your comment. We are suggesting the term "Impact Event" be substituted to include all events that would impact the reliability of the BES. Events now included in reporting requirements that do not impact reliability of the BES would be excluded from the reporting unless the DSR SDT clarifies why it should be included and under what specific instances or examples. Tightening the reporting criteria of impact events could possibly address the concern expressed by a "violation based on imprecise terminology."		
USBR	Yes	There should be a clear distinction between a cyber event and a cyber event that has a material impact on the reliability of the bulk electric system. Not all CIP-008 events will carry such a distinction. That being said, CIP 008 cannot be completely incorporated in this process. Denying access to a cyber asset is noteworthy under CIP008 but may not pose a threat to the reliability of the bulk electric system. Consider recognizing the impact on the bulk electric system when modifying definitions of adding the bulk electric system description to the definitions. This will help to clarify that disturbances, as discussed in this effort, are situations that produce an abnormal condition on the electric power system, not necessarily on ancillary or supporting systems, such as SCADA systems or the water-related systems at hydroelectric dams.
Response: The DSR SDT thanks you for your comment. We are suggesting in our discusssion to consolidate the location of reporting into one standard. The industry has demonstrated by comments that it favors streamlining the reporting process to achieve a "one stop shop" approach. We will continue to explore the possibilities to achieve the best results for all stakeholders. A discussion of advantages /disadvantages will continue to discover options and alternatives with input from all stakeholders.		
Western Electricity Coordinating Council	Yes	This will help eliminate regional differences in sabotage reporting. The definition should be broad enough so it covers new types of sabotage that may evolve. Event analysis facilitates situational awareness and if it requires further investigation regarding developing patterns and severity, it should be handled by law enforcement if need be.
Response: The DSR SDT thanks you for your comment. The DSR SDT will continue to explore the "Impact Event" definition to allow for new types of events. Event analysis is clearly a goal of reporting as is situational awareness and hopefully this project will enhance the understanding and clearly define obligations to all stakeholders.		
Manitoba Hydro	Yes	Though there are some specific events already included in this new definition, more could be added to dissolve specific "gray areas" and as new ones come up. Again these examples could be added into the electronic form and could contain a large data base which would be available depending on the event that occurred.
Response: The DSR SDT thanks you for your comment.		

Organization	Yes or No	Question 5 Comment
BGE	Yes	We agree that "the spectrum of all sabotage-type events is not well understood throughout the industry"; however, we feel that the proposed concept of an "Impact Event" falls short of clarifying what constitutes such events. We believe that "Impact Events" needs further clarification to eliminate "gray areas" and to provide more reporting consistency between entities.
Response: The DSR SDT thanks you for your comment. The DSR SDT will continue to clarify the impact events concept and eliminate "gray areas" while including language to give clarity to the reporting process.		
Dynegy Inc.	Yes	We agree with the concept but please provide specific examples. Also, please consider whether there are any penalties for misinterpreting an incident, who would determine if an event was a threat, and whether this could result in over reporting non-threats.
Response: The DSR SDT thanks you for your comment. The DSR SDT may include specific examples of impact events and types of reportables events in the 1st draft of the standard (or in supplemental guidance) to help illustrate reportable criteria.		
Consumers Energy Company	Yes	We agree with the concept, however, based on the information provided, it may be too vague to be of value. Terms such as "potential" and "significant" can be subjective and therefore provide little direction. We would like to see something more specific. Also, inclusion of the destruction of BES assets may be too inclusive and needs to be restricted to BES assets that will cause a specific level of impact on reliability.
Response: The DSR SDT thanks you for your comment. The SDR SDT struggles with terms that deal with determing "potential" and "significant". Specific examples of criteria is being explored and discussed. We will strive to meet this challenge with the input on the right language from government agencies and industry experience expertise. Your suggestion of restricting to BES assets that will cause a specific level of impact on reliability will be discussed with the DSR SDT.		
Independent Electricity System Operator	Yes	We agree with the general concept. However, we suggest that the classification of "events" to be compatible if not identical to those which need to be reported in real time as required in CIP-001, for otherwise it will create confusion and unnecessary, extra work. Also, this proposal appears to focus on the sabotage-type events only but the SAR deals with both sabotage and other disturbances (e.g. emergency type of events) reporting. A parallel type of "impact event" is needed for non-sabotage-type of events.
Response: The DSR SDT thanks you for your comment. The DSR SDT notes that impacts events include both sabotage and non-sabotage types of events and these events include CIP-001 events.		
Electric Market Policy	Yes	We believe that physical and cyber events must be investigated before a determination of sabotage or impact

Organization	Yes or No	Question 5 Comment
		event can be made.
Response: The DSR SDT thanks you for your comment. We agree that sabotage requires investigation. The term "impact event" was developed to allow immediate reporting of events based on impact to the BES rather than intent.		
We Energies	Yes	We would prefer to refer to all sabotage, vandalism, cyber attacks, and other criminal behavior as impact events. Focusing more on the event's impact on reliability and its ramifications on the systems seems to be more useful than to try to determine the intent of the perpetrator.
Response: The DSR SDT thanks you for your comment. The DSR SDT agrees with your assessment and will pursue the clarity and criteria examples to achieve reporting.		

6. If you are aware of any regional reporting requirements beyond the scope of CIP-001, CIP-008 and EOP-004 please provide them here.

Summary Consideration: Several commenters provided information on regional reporting. The SDT will consider whether these should be included in the continent-wide standard. These include:

1. NPCC maintains a document and reporting form (Document C-17 - Procedures for Monitoring and Reporting Critical Operating Tool Failures) that outlines the reporting requirements, responsibilities, and obligations of NPCC Reliability Coordinators in response to unforeseen critical operating tool failures.
2. For other events that do not meet the OE-417 and EOP-004 reporting criteria, ReliabilityFirst expects to receive notification of any events involving a sustained outage of multiple BES facilities (buses, lines, generators, and/or transformers, etc.) that are in close proximity (electrically) to one another and occur in a short time frame (such as a few minutes).
3. WECC sets its loss of load criteria for disturbance reporting at 200 MW rather than the 300 MW in the NERC reporting form.
4. SERC and RFC are developing additional requirements at this time.
5. We suggest that reporting be based on impact to reliability, not on 'newsworthy' events. We therefore do not agree with such regional efforts and would prefer a continent wide reporting requirements.
6. MISO RC (MISO OP-023) and RFC (PRC-002-RFC-01).

Organization	Question 6 Comment
Central Hudson Gas & Electric	Although not beyond the scope of these standards, NPCC maintains a document and reporting form (Document C-17 - Procedures for Monitoring and Reporting Critical Operating Tool Failures) that outlines the reporting requirements, responsibilities, and obligations of NPCC RCs in response to unforeseen critical operating tool failures.
Response: The DSR SDT thanks you for your comment. The DSR SDT will examine regional reporting criteria and requirements to determine whether it should be included in a continent wide standard.	
Exelon	At the 2010 RFC Spring Workshop the following disturbance reporting Criteria was rolled out: All events that are required to be reported by the OE-417 and EOP-004 criteria will use those published procedures. For other events that do not meet the OE-417 and EOP-004 reporting criteria, ReliabilityFirst expects to receive notification of any events involving a sustained outage of multiple BES facilities (buses, lines, generators, and/or transformers, etc.) that are in close proximity (electrically) to one another and occur in a short time frame (such as a few minutes).

Organization	Question 6 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT will examine regional reporting criteria and requirements to determine whether it should be included in a continent wide standard.	
Lands Energy Consulting	I believe WECC sets its loss of load criteria for disturbance reporting at 200 MW rather than the 300 MW in the NERC reporting form.
Response: The DSR SDT thanks you for your comment. The DSR SDT will consider regional criteria when developing reporting thresholds.	
Edison Mission Marketing & Trading	I don't know of any.
Orange and Rockland Utilities, Inc.	NERC's SDT effort requires a clear, consistent, and comprehensive continent-wide approach, thus mitigating any need for regional reporting requirements.
Response: The DSR SDT thanks you for your comment. The SDR SDT feels in many instances that region specific standards may be needed. However, the SDT will provide a clear reporting standard that can be consistently followed continent-wide.	
MRO's NERC Standards Review Subcommittee	No Comment.
Duke Energy	None
Bandera Electric Cooperative, Inc.	No.
Manitoba Hydro	No.CIP-001 contains references to NERC and the DOE.CIP-008 makes exclusions for facilities regulated by US Nuclear Regulatory Commission and Canadian Nuclear Safety Commission. It also contains references to ES ISAC (Electricity Sector Information Sharing and Analysis Center).EOP-004 contains reference to NERC and DOE. There is no reference to Homeland Security, FBI, etc or to Canadian equivalent references in any of these Standards. When NERC is notified of an event, it is likely other organizations will have to be notified. There should be some sort of consistency to cover all these Standards and all notifiable parties at a NERC Standards level.
Response: The DSR SDT thanks you for your comment. The DSR SDT absolutely understands your provided comment and have had detailed conversations surrounding "who" should be notified and "when". Most importantly, a level of consistency should exist when reporting disturbances and sabotage events negatively impacting the BES.	

Organization	Question 6 Comment
Oncor Electric Delivery Company LLC	Oncor is not aware of any regional reporting requirements beyond the scope of CIP-001, CIP-008 and EOP-004.
Response: The DSR SDT thanks you for your comment.	
Dynegy Inc.	Please consider MISO RTO-OP-023.
Response: The DSR SDT thanks you for your comment. The DSR SDT will examine regional reporting criteria and requirements to determine whether it should be included in a continent wide standard. Please provide a copy of the subject document.	
Electric Market Policy	SERC and RFC are developing additional requirements at this time. We suggest that reporting be based on impact to reliability, not on 'newsworthy' events. We therefore do not agree with such regional efforts and would prefer a continent wide reporting requirements.
Hydro-Québec TransEnergie (HQT)	
Northeast Power Coordinating Council	
Response: The DSR SDT thanks you for your comment. The DSR SDT will examine regional reporting criteria and requirements to determine whether it should be included in a continent wide standard.	
Public Service Enterprise Group Companies	The PSEG Companies believe that RFC is developing a regional disturbance reporting requirement for events not meeting the criteria of current DOE and NERC reports.
Response: The DSR SDT thanks you for your comment. The DSR SDT will examine regional reporting criteria and requirements to determine whether it should be included in a continent wide standard.	
Western Electricity Coordinating Council	There is a need to learn what reporting requirements are required by the Mexican and Canadian entities.
Response: The DSR SDT thanks you for your comment. The DSR SDT is comprised of international members and we are currently researching requirements that Mexico and Canada may have.	
SERC Reliability Coordinator Sub-committee (RCS)	We are not aware of any regional reporting requirements beyond the requirements of CIP-001, CIP-008 and EOP-004. However, the SERC RRO has shared a list of events of interest that it would like to be made aware of to maintain situation

Organization	Question 6 Comment
	awareness.
Response: The DSR SDT thanks you for your comment. The SDR SDT feels there will always be a need for the Regional Entities to be kept aware of certain "hot topic" issues. However, it is the SDT's intent to provide clear and concise reporting requirements for events impacting the BES.	
BGE	We are not aware of any regional requirements beyond the scope of CIP-001, CIP-008 and EOP-004.
Response: The DSR SDT thanks you for your comment.	
We Energies	What is meant by beyond the scope of the referenced standards? We Energies also has reporting obligations with the MISO RC (MISO OP-023), RFC (PRC-002-RFC-01), and the Wisconsin and Michigan Public Service Commissions.
Response: The DSR SDT thanks you for your comment. The DSR SDT will examine regional reporting criteria and requirements to determine whether it should be included in a continent wide standard. Please provide a copy of the subject reporting requirements for the SDT to review.	

7. If you have any other comments on the Concepts Paper that you haven't already provided in response to the previous questions, please provide them here.

Summary Consideration: Several stakeholders provided comments in this section. Some stakeholders suggested that the SDT has gone beyond its approved scope to "further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event." Further, there is no requirement to create a Reporting Standard to define sabotage. The SDT contends that the development of impact events and the reporting requirements for them will provide the clarity sought in the directive.

Other stakeholders suggested that the SDT should seek to retire sanctionable requirements that require event reporting in favor of guidelines for reporting.

Several commenters suggested that the introduction of impact events actually expands the reporting requirements. It should be noted that the list of impact events is expected to be explicit as to who is to report what to whom and within certain timelines.

Several stakeholders provided input as to what they believed an electronic reporting tool should contain:

1 If the decision is made to go to a single reporting form, it should be developed to cover any foreseeable event.

2 The SDT should work toward a single form, located in a central location, and submitted to one common entity (NERC)

3 Reports should be forwarded to the ES-ISAC, not NERC, as the infrastructure is already in place for efficient sharing with Federal agencies, with the regional entities and with neighboring asset owners. Reports should flow to all affected entities in parallel, rather than series (timing issues).

Commenters also suggested that the SDT should consider the impacts of the reporting requirements on the small, and very small utilities.

Organization	Question 7 Comment
BGE	1. If we move to a "one size fits all" single reporting form, it is important that the form be properly developed to cover any foreseeable event, which appears to be the intent of the DSR SDT, as outlined on page 4 of the concept document. Such an approach should also incorporate a single point of contact for reporting information, to avoid any confusion. 2. We would like clarification that any proposed CIP-008-related reporting requirement (including any linked reporting requirement between CIP-008 and CIP-001) is only applicable in situations where the incident/event involves a registered entity's Critical Cyber Asset.

Organization	Question 7 Comment
Response (Questions 3&6): The DSR SDT thanks you for your comment. The drafting team will explore clarification that any proposed CIP-008 related reporting requirement between CIP-008 and CIP-001 is only applicable where the incident/event involves a registered entity's CCA. Note that CIP-002 through CIP-009 are undergoing revision under project 2008-06 – Order 706 SDT. Note that the current CIP-008 has a reporting requirement to the ES-ISAC only.	
Electric Market Policy	a. NERC should focus efforts on developing specific event reporting criteria and not base the requirement on the definition of the term 'sabotage' but on the reporting criteria itself. b. The "opportunities for efficiency" discussed in the Concept Paper would be best achieved by focusing on those items that are necessary to maintain the reliability of the Bulk Electric System. If there are elements that need to be reported that, do not support this objective, than that reporting should not be required in reliability standards.
Hydro-Québec TransEnergie (HQT)	a. NERC should focus efforts on developing specific event reporting criteria and not base the requirement on the definition of the term 'sabotage', but on the reporting criteria itself. See comments above. b. The "opportunities for efficiency" discussed in the Concept Paper would be best achieved by focusing on those items that are necessary to maintain the reliability of the Bulk Electric System. If there are elements that need to be reported that do not support this objective, then that reporting should not be required in reliability standards. Consider making NERC the distributor of reports to other agencies. We recognize that the key is to simplify reporting to a single form, and to the extent possible, to one agency. "Front line" reliability personnel must have the "timely" knowledge to know when a situation warrants local, area, regional, or national involvement. Finally, the SDT should keep in mind the fact that Canadian stakeholders might have some difference in the way reports are made to Security Agencies.
Northeast Power Coordinating Council	a. NERC should focus efforts on developing specific event reporting criteria and not base the requirement on the definition of the term 'sabotage', but on the reporting criteria itself. See comments above b. The "opportunities for efficiency" discussed in the Concept Paper would be best achieved by focusing on those items that are absolutely necessary to maintain the reliability of the Bulk Electric System. If there are elements that need to be reported that do not support this objective, then that reporting should not be required in reliability standards. Consider making NERC the distributor of reports to other agencies. We recognize that the key is to simplify reporting to a single form, and to the extent possible, to one agency. "Front line" reliability personnel must have the "timely" knowledge to know when a situation warrants local, area, regional, or national involvement.
Response: The DSR SDT thanks you for your comment. The DSR SDT agrees to focus efforts to specific event reporting criteria. SDT believes that by reporting material risks to the Bulk Electrical System using the impact event categorization it will be easier to get the relevant information for mitigation, awareness, and tracking, not based on the requirement of defining "sabotage". The SDT believes that it is the submitter's responsibility to submit OE-417 forms to the DOE, as stated by Public Law for US entities. The DSR SDT does recognize that it may not be possible to eliminate	

Organization	Question 7 Comment
reporting to multiple jurisdictional agencies due to legislative or regulatory requirements.	
SPS Consulting Group Inc.	Again, please consider the unique scope of the entities to which these standards are to comply. Don't dump all the requirements on all the applicable entities and perpetuate the current practice of forcing them to parse the requirements into what is logical or illogical from their perspective. The drafting team should have the expertise to do this. Identify which requirements apply to which applicable entity.
Response: The DSR SDT thanks you for your comment. The DSR SDT will take into consideration what registered entities and thresholds are to be included in the revised standard(s) based on the SAR. The DSR SDT will establish the "requirements necessary for users, owners, and operators of the Bulk-Power-System" as stated in FERC Order 693 and the difference in reporting of events on the BES, as stated in the Purpose statement of EOP-004-1.	
ERCOT ISO	All references to CIP-008 should be removed and we reassert that physical and cyber reporting should be separate. There is documentation available from the CIPC that the drafting team considered CIP-001 related physical sabotage reporting and specified cyber incident reporting requirements in CIP-008.ERCOT ISO requests the DSR SDT to continue to improve its guidelines and to post those guidelines for all to use, but not to create sanctionable standards whose good intentions could result in unintended adverse consequences for the Industry. ERCOT ISO also suggests that all reporting forms and guidance should be located in a central, easily accessible location, eliminating confusion and simplify reporting for system operators thereby directly enhancing reliability during system events. The industry would benefit from a central location or link on the NERC website containing all reporting forms.
Response: The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if the DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has not determined at this time what bright line will be used for the yet to be drafted Standard(s). The DSR SDT will take into consideration your comment on keeping cyber and physical events separate. We are suggesting in our discussion to consolidate the location of reporting into one standard. The industry has demonstrated by its comments that it prefers that the reporting process be streamlined to achieve a "one stop shop" approach. We will continue to explore the possibilities to achieve the best results for all stakeholders. A discussion of advantages /disadvantages will continue to discover options and alternatives with input from all stakeholders.	
Western Electricity Coordinating Council	As stated previously, for "One stop shopping" we need "buy in" from the foreign nationals. The way to do this is to engage their opinions and respect their jurisdictional agencies as well.
Response (Question 6): The DSR SDT thanks you for your comment. The DSR SDT does recognize that it may not be possible to eliminate reporting to multiple jurisdictional agencies due to legislative or regulatory requirements. The SDT acknowledges that it is possible to consolidate various reports that ask repetitive questions and through this process can work with foreign nationals to receive their "buy in" for a one report form for all functional entities to submit to NERC.	

Organization	Question 7 Comment
MRO's NERC Standards Review Subcommittee	Confusion often arises in the industry between the CIP standards and other reliability standards based on CIP-001 naming convention. We would suggest the SDT retire CIP-001 and incorporate requirements within the EOP-004 standard or a new EOP-xxx standard to avoid confusion rising from CIP and other NERC Reliability Standards. Additionally, we assume the SDT has been created to specifically address FERC Order 693 directives to the ERO which appears to include the following items: 1. Applicability - "possible revisions to CIP-001-1 that address our concerns regarding the need for wider application of the Reliability Standard... the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate" (FERC, 2007, para. 460). 2. Definition of Sabotage - "we direct that the ERO further define the term and provide guidance on triggering events that would cause an entity to report an event... we believe the term sabotage is commonly understood and that common understanding should suffice in most instances... the ERO should consider FirstEnergy's suggestions to differentiate between cyber and physical sabotage and develop a threshold of materiality." (FERC, 2007, para. 461-462) 3. Periodic Review and Testing - "directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures." (FERC, 2007, para. 466) 4. Redundant Reporting - "now direct the ERO to address our underlying concern regarding mandatory reporting of a sabotage event... Regarding the potential for redundant reporting under CIP-001-1 and other government reporting standards, and the need for greater coordination... We direct the ERO to explore ways to address these concerns - including central coordination of sabotage reports and a uniform reporting format... with the appropriate governmental agencies that have levied the reporting requirements." (FERC, 2007, para. 468-469) 5. Specified Time - "the Commission directs the ERO to modify CIP-001-1 to require an applicable entity to contact appropriate governmental authorities in the event of sabotage within a specified period of time... the ERO should consider suggestions raised... to define the specified period for reporting an incident beginning from when an event is discovered or suspected to be sabotage" (FERC, 2007, para. 470). 6. Summary of CIP-001-1 - "the Commission directs the ERO to develop the following modifications... (1) further define sabotage and provide guidance as to the triggering events... (2) specify baseline requirements regarding... procedures for recognizing sabotage events... (3) incorporate a periodic review... and for the periodic testing... (4) require an applicable specified period of time. In addition... address our concerns regarding applicability to smaller entities... consolidation of the sabotage reporting forms and the sabotage reporting channels with the appropriate governmental authorities to minimize the impact of these reporting requirements on all entities." (FERC, 2007, para. 471) 7. Analyze Performance - "at a minimum, generator operators and LSEs should analyze the performance of their equipment and provide the data... The Commission directs the ERO to consider this concern in future revisions... that includes any Requirements necessary for users, owners and operators... to provide data that will assist NERC" (FERC,

Organization	Question 7 Comment
	2007, para. 613, 617). 8. Reporting Time Frames - "The Commission directs the ERO to change its Rules of Procedures to assure that the Commission also receives these reports within the same time frames as the DOE." (FERC, 2007, para. 618)
Response: The DSR SDT thanks you for your comment. The DSR SDT agrees with your comments to specifically address FERC Order 693 directives to the ERO and will determine a prudent course of action with respect to these standards and pursue the suggestion to retire CIP-001 and incorporate requirements within the EOP-004 standard to avoid confusion rising from CIP and other NERC Reliability Standards.	
Constellation Power Source Generation	Constellation Power Generation would like clarification that any proposed CIP-008-related reporting requirement (including any linked reporting requirement between CIP-008 and CIP-001) is only applicable in situations where the incident/event involves a registered entity's Critical Cyber Asset. In that vein, we want to emphasize the importance of the DSR SDT working with the CIP SDT on the cyber related events. If the DSR SDT is going to be adding clarity to cyber related events, then coordination with the CIP SDT is needed to ensure the same verbiage is being used. Furthermore, having any duplication of requirements will cause a double jeopardy scenario which would go against the SAR for the DSR SDT. As stated earlier, Constellation Power Generation also questions whether cyber related incidents should fall under the spectrum of sabotage type events, or remain separate and be incorporated in the CIP revisions.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has not determined at this time what bright line will be used for the yet to be drafted Standard(s). Note that CIP-002 through CIP-009 are undergoing revision under project 2008-06 – Order 706 SDT.	
We Energies	Give consideration to combining CIP-001 and EOP-004-1 through a common categorization. For example, "System Risk Reporting" could encompass both actual and potential events and would minimize the need to cross reference both standards, and provide one location for event and potential-event reporting. Much of the challenge in this project is in achieving a common understanding of the words sabotage and terrorism. There are nuances of meaning in the words that imply a relationship between the attacker and the victim, or a motive other than simple profit or mischief. This nuance of meaning requires the victim of the damage to discern a relationship or motive which may not be discoverable in the relatively brief time window during which the entity must report the event. In fact, they may never be known. Consequently, We Energies recommends elimination of the words sabotage and terrorism from these standards. We also recommend elimination of the word vandalism since it also implies an ability and duty to discern whether a particular act (barbed wire thrown over transformer bushings) was done out of pure mischief (vandalism) or with intent to destroy equipment for a political purpose (terrorism). And if the act was committed by a disgruntled employee, it becomes sabotage. No wonder there is confusion and indecision. Instead, We Energies recommends using the simple words "criminal damage". One need not be a prosecuting attorney or FBI Special Agent to know what this means. Simply ask, "Does is look like somebody damaged it (or hacked in) intentionally?" and, "Did we give consent?" and you're done. With

Organization	Question 7 Comment
	elimination of sabotage, terrorism and vandalism, and all of their baggage, comes the ability to integrate both CIP 001 and EOP 004. We now have criminal damage (or cyber attack) as just another event to be evaluated against certain pre-defined impact measures. No value judgments, no speculation. Another benefit of using these simple words and tests is that operating personnel, whether in the field or at the console, will not require special awareness training in discerning these nuances of meaning. They already have experience with the equipment or cyber systems and its normal performance. Operating personnel can readily assess whether an impact event is due to equipment failure, weather or animal contact vs. intentionally caused by a person. If it appears to be criminal damage, call the local police agency. Report the event and the impact. Cooperate with the investigation. Share your knowledge of the normal condition of the equipment or performance of the system. Share your experience with similar events. It will be important to highlight that the theft of all the grounding pigtails in a substation is different from the act of simply snipping each of them to leave the equipment electrically floating. The technical condition is the same, but this allows the police to make an inference with respect to motive, suspect profile, sophistication, etc. That's their job. They may ask us to speculate on the motive or skills of the attacker. That's okay. But at least we don't have to know or guess at it for the purpose of determining whether to report the event. No training required. With respect to notification to the FBI, We Energies recommends that the standard merely state that the owner of the damaged asset ensure the local office of the FBI is notified. The standard should permit documentation of either a direct phone call by the asset owner or obtaining an assurance from the local police that they will do so. There should be no need to prove earlier establishment of a relationship with the FBI. There should be no expectation that the entity have a signed letter from the FBI Special Agent in Charge acknowledging his agency's duty. This document means nothing. With respect to reporting within the industry, We Energies recommends that the only events to be reported "up the chain" are those that we choose to characterize as "impact events". That is, the events that meet some measurable threshold with respect to BES impact. We should describe these efficiently to avoid over-reporting of trivial events. It is apparent that we are already over-reporting since DHS HITRAC recently fed back to the industry that copper thieves attacked a substation in San Bernardino, CA taking some of the grounding conductors. The industry should have the option to report non-impact events that are unusual in some respect and which may have some mutual industry benefit in terms of prevention, awareness or recovery. Attack attempts with no impact, or observations of suspicious activity could fall into this optional category. These optional reports could be aggregated by the entity for the purpose of detecting patterns or trends, or be reported ad hoc. The ES-ISAC should be the recipient of the reports. It should be the single point of contact since it has the industry insight, engineering expertise and cross-sector relationships to analyze and return valuable intelligence to the industry. With the ES-ISAC as the recipient of the reports, efficient sharing with Federal agencies, with the regional entities and with neighboring asset owners could be automated and rapid. There is much benefit to be gained from this project, primarily in the area of creating clarity and uniformity. There is some risk that the reporting requirements will become onerous and prescriptive.
Response: The DSR SDT thanks you for your comment. The DSR SDT is proposing to consolidate disturbance and event reporting under a single standard. The DSR SDT believes that reporting material risks to the Bulk Electrical System by using the impact event categorization, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation by the elimination of the term "sabotage". The intent is to allow potentially impacted parties to prepare for and possibly mitigate the reliability risk. The NERC Rules of	

Organization	Question 7 Comment
Procedure (section 800) provides an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for reliability. The SDT is proposing that the new standard specify who has access to reported information and who should be notified about impact events, because agencies such as the DHS and FBI have other duties and responsibilities - an impact event that is related to copper theft may only need to be reported to the local law enforcement authorities. The goal of the DSR SDT is create clarity and uniformity by developing a single reporting form for all functional entities without regard to nationality (US, Canada, Mexico) to submit to NERC with guidance. Ideally, entities would complete a single form, which could then be distributed to jurisdictional agencies and functional entities as appropriate. The DSR SDT agrees with your assessment that there should be no expectation that the entity have a signed letter from the FBI Special Agent.	
Bandera Electric Cooperative, Inc.	I commend the SDT for working on this effort and wish them success.
Response: The DSR SDT thanks you for your comment.	
Public Service Enterprise Group Companies	If reporting does become the responsibility of the Reliability Coordinators, the RCIS should be made available view-only to registered entities with a notification when RC's have posted new entries. That will enhance the situational awareness of registered entities. The PSEG Companies disagree with inclusion of CIP-008 reporting requirements as part of the CIP-001 and EOP-004 initiative. CIP-008 reporting as part of the cyber security set of NERC standards is usually managed by specialized corporate organizations separate from those involved with the other NERC standards, and with highly specialized cyber skill sets. CIP-008 reporting requirements should remain where they are, and any perceived need for improvement addressed in the ongoing CIP Version 4 development process.
Response: The DSR SDT thanks you for your comment. The RCIS is a real-time communication and reporting tool and is outside the scope of the SDT. The goal of the DSR SDT is to develop a form to expedite report completion, sharing and storage. Ideally, entities would complete a single form, which could then be distributed to jurisdictional agencies and functional entities as appropriate. Functional entities may include the RC, TOP, and BA for situational awareness. The DSR SDT will take into consideration your comment with inclusion to CIP-008 reporting. However, the drafting team will explore clarification that any proposed CIP-008-related reporting requirement between CIP-008 and CIP-001 is only applicable where the incident/event involves a registered entity's CCA. Note that CIP-002 through CIP-009 are undergoing revision under project 2008-06 – Order 706 SDT.	
Independent Electricity System Operator	In the Background Section of the comment form, it is indicated that the SDT "...is NOT seeking input or guidance on the definition of physical or cyber sabotage, what type of disturbances should be reported, who should do reporting, or to whom or what organizations will be receiving the reports." Yet there are proposed definitions, with examples, in the concept paper. The SDT should make it absolutely clear that by supporting the general concept as described in the paper, the commenting entities are not endorsing the proposed definitions, nor the examples as elements to be included in the standard.

Organization	Question 7 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT will continue to clarify the impact events concept and eliminate "gray areas" while including language to give clarity to the reporting process. Standards developed under this project will be posted for comment on specific content.	
Luminant	Luminant disagrees with the direction of utilizing impact events, as this is an expansion in scope beyond the simplification of sabotage and disturbance reporting.
Response: The DSR SDT thanks you for your comment. We are suggesting the term "Impact Event" be substituted to include only events that would impact the reliability of the BES. The DSR SDT has reviewed the existing standards, the SAR; issues from the NERC database and FERC Order 693 Directives and determine this was a prudent course of action with respect to these standards to provide clear criteria for reporting.	
Dynegy Inc.	N/A
Manitoba Hydro	No
Edison Mission Marketing & Trading	No other comments.
SERC Reliability Coordinator Sub-committee (RCS)	None.
USBR	The concept of "threat" evaluation criteria is somewhat vague and a great care is needed to ensure it is clear enough that the most individuals would be able to analyze an event and end up at the same threat. Otherwise it would be almost impossible to ensure compliance with a requirement which cannot accurately describe criteria to be used to ensure that proper evaluation has occurred.
Response: The DSR SDT thanks you for your comment. We are suggesting the term "Impact Event" be substituted to include only events that would impact the reliability of the BES as opposed to requiring a threat evaluation. The DSR SDT intends to develop criteria that will assist entities in determining which events should be reported.	
Wolverine Power Supply Cooperative, Inc.	The concepts of removing duplication, consolidation, and focusing on "impact events" sound logical. I am concerned that the focus may drift to expanded reporting, not reduced reporting.
Response: The DSR SDT thanks you for your comment. The DST SDT discussed the reporting of "impact events" and will consider guidance found in the document, "NERC Guideline: Threat and Incident Reporting" which will include clear criteria to eliminate erroneous or expanded reporting.	

Organization	Question 7 Comment
ISO RTO Council Standards Review Committee	The FERC Order merely asked NERC to "further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event." There is no requirement to create a Reporting Standard and no mention of Disturbance events. There is a strong need to avoid heavy-handed use of NERC standards particularly for such post event reporting guidelines. The SRC would urge the DSR SDT to continue to improve its guidelines and to post those guidelines for all to use, but not to create sanctionable standards whose good intentions will inevitably result in many unintended adverse consequences for the Industry. Rather, the SDT should seek to retire sanctionable requirements that require event reporting in favor of guidelines for reporting.
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if the DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has not determined at this time what bright line will be used for the yet to be drafted Standard(s). The DSR SDT will take into consideration your comment on keeping cyber and physical events separate. We are suggesting in our discussion to consolidate the location of reporting into one standard. The industry has demonstrated by its comments that the reporting process be streamlined to achieve a "one stop shop" approach. We will continue to explore the possibilities to achieve the best results for all stakeholders. A discussion of advantages /disadvantages will continue to discover options and alternatives with input from all stakeholders.	
Lands Energy Consulting	The lack of common sense that leads to a 15 MW loss of load resulting from a 115 kV line outage being categorized as a "reportable disturbance" really hurts the credibility of the entire NERC Compliance Program. The smaller utilities look at application of EOP-004 in particular to their operation and conclude that either the EO/RRO is: a. stupid; or b. Out to persecute the smaller utilities. In reality, EOP-004 was drafted for application to Southern California Edison, where loss of 50% of customers would be 2-3 million customers. Now that's really disturbing!
Response: The DSR SDT thanks you for your comment. The DSR SDT intends to develop criteria that will assist entities in determining which events should be reported. Acts of sabotage may be "tested" on smaller entities before the saboteurs move on the larger entities.	
Central Hudson Gas & Electric	The NERC Guideline: Threat and Incident Reporting Attachment A matrix is an extremely beneficial document that organizes reporting criteria. However, it identifies communications systems failure sub-category under the Equipment And/Or Systems Failure category as reportable with a reference to OE-417 - Schedule 1, Item 10. Item 10 on Schedule 1 addresses only failures due to attacks (not failures for other reasons).
Response: The DSR SDT thanks you for your comment. The intent was to look at the posted "NERC Guideline: Threat and Incident Reporting" and ask the industry if the DSR SDT should consider existing guidelines for possible inclusion into the yet to be written requirement(s). The DSR SDT has not determined at this time what bright line will be used for the yet to be drafted Standard(s). Loss of communications would be considered an impact event. The reason for the loss of communications is irrelevant.	

Organization	Question 7 Comment
Duke Energy	We don't think CIP-001, EOP-004 and cyber incident reporting aspects of CIP-008 should all be combined into one standard, because of the significant differences between sabotage and disturbances. We have suggested that the drafting team further define sabotage, and we have included a suggested definition in our response to question #5 above. Sabotage is very specific due to the intent (for the purpose of weakening the critical infrastructure), and the potential impact to the BES. We believe that sabotage and cyber incident reporting should remain a part of the CIP Standards due to the emphasis placed on the criticality and vulnerability of the assets needed to support reliable operation of the BES. Cyber Security and Physical Security could be placed together in the same standard (remain in CIP) and other disturbances (i.e., accidental, natural) in a separate standard. "One stop shopping" for reporting is still possible as long as the OE-417 form is included as part of the NERC electronic form. And while we agree with the need for additional clarity in sabotage and disturbance reporting, we believe that the Standards Drafting Team should carefully consider whether there is a reliability-related need for each requirement. Some disturbance reporting requirements are triggered not just to assist in real-time reliability but also to identify lessons-learned opportunities. If disturbance and sabotage reporting continue to be reliability standards, we believe that all linkages to lessons-learned/improvements need to be stripped out. We have other forums to identify lessons-learned opportunities and to follow-up on those opportunities.
Response: The DSR SDT thanks you for your comment. The DSR SDT is still evaluating inclusion of CIP-008 reporting requirements with CIP-001 and EOP-004 requirements, Note that the current CIP-008 has a reporting requirement to the ES-ISAC only. The DSR SDT developed the more inclusive term "impact events" to eliminate using more confusing terms like sabotage (which is not likely to be determined until after a lengthy investigation). These standards may be combined to have all reporting requirements in a single standard, not because the items to be reported are necessarily related.	
FirstEnergy	We fully agree that sabotage events need to be more clearly defined and reporting requirements need to be better coordinated. But as we have stated in previous comments, the drafting team needs to determine if standard requirements need to be developed for this type of reporting or if this is better left to administrative requirements outside the standards arena. Also, while we appreciate the team's effort to simplify reporting requirements for entities, we are concerned with the serial communication offered by the concept paper. As an example, the team proposes to have LSE report the incident to the BA and/or TOP and then have the BA and/or TOP report it to the RC and the RC to report it to NERC and the NERC report to the regulatory agencies. While this simplifies it for each individual organization, this method introduces many opportunities for errors and miscommunications. Since this is after-the-fact reporting, it is difficult to defend this type of communication path when one consistent report could be sent simultaneously to all agencies at the same time from the originating location.
Response: The DSR SDT thanks you for your comment. The Reliability Coordinator's suggested role in this is to allow them to incorporate the relevant data from responsible entities in their footprint for further analysis. We will consider your suggestion of simultaneous submissions as a means to effectively notify the necessary parties. The SDT believes that it is the submitter's responsibility to submit OE-417 forms to the DOE. The DSR SDT does recognize that it may not be possible to eliminate reporting to multiple jurisdictional agencies due to legislative or regulatory	

Organization	Question 7 Comment
requirements.	
Ameren	While we are not opposed to the concept of identifying impact events, we are concerned that the drafting team may actually be expanding reporting requirements. We do not support expansion of reporting requirements unless a clear reliability or legal need is identified. Some of the impact events are almost never sabotage and do not warrant reporting for reliability needs and should not be included. For example, copper theft should not require reporting, in general, because it is almost never sabotage and rarely impacts reliability. If it does, impact reliability because, for example, the protection system is impacted and causes more significant potential contingencies, then reporting could be required. Why is a train derailment near a transmission right of way significant? It would only be significant if an investigation identified sabotage as the reason. Furthermore, what is considered near?
Midwest ISO Standards Collaborators	While we are not opposed to the concept of identifying impact events, we are concerned that the drafting team may actually be expanding reporting requirements. We do not support expansion of reporting requirements unless a clear reliability or legal need is identified. Some of the impact events are almost never sabotage and do not warrant reporting for reliability needs and should not be included. For example, copper theft should not require reporting, in general, because it is almost never sabotage and rarely impacts reliability. If it does impact reliability because, for example, the protection system is impacted and causes more significant potential contingencies, then reporting could be required. Why is a train derailment near a transmission right of way significant? It would only be significant if an investigation identified sabotage as the reason. Furthermore, what is considered near?
Response: The DSR SDT thanks you for your comment. It is not the intent of the DSR SDT to expand reporting requirements but rather to attempt to clarify and define an approach to assist the industry and stakeholders in reporting impact events. Furthermore, impact events should not include copper theft or other conditions that pose no threat to the reliability of the BES. A train derailment is only an impact event if it threatens some element of the power system such as a transmission line corridor - the derailment in itself is not an impact event.	
Exelon	You should consider providing clear and concise instructions as to the expectation on submitting forms, i.e. the DOE 417. There should be no guessing as to when and how reports should be submitted and who should receive them. Specific details on reporting criteria should be included.
Response : The DSR SDT thanks you for your comment. The DSR SDT intends to develop criteria for reporting impact events.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SC approved SAR for initial posting (April, 2009).
2. SAR posted for comment (April 22 – May 21, 2009).
3. SC authorized moving the SAR forward to standard development (September 2009).
4. Concepts Paper posted for comment (March 17 – April 16, 2010).

Proposed Action Plan and Description of Current Draft
This is the first posting of the proposed standard in accordance with Results-Based Criteria. The drafting team requests posting for a 30-day formal comment period.

Future Development Plan

Anticipated Actions	Anticipated Date
Initial Comment Period	September 2010
Drafting team considers comments, makes conforming changes, and proceed to second comment	October – December 2010
Comment Period/Initial Ballot	December 2010-January 2011
Successive Comment/Ballot period	February – March 2011
Receive BOT approval	April 2011

Effective Dates

1. USA: First calendar day of the first calendar quarter one year after applicable regulatory authority approval for all requirements

2. Canada and Mexico: First calendar day of the first calendar quarter one year following Board of Trustees adoption unless governmental authority withholds approval

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-1 and EOP-004-1 into EOP-004-2; Retired EOP-004-1, R1, R3.2, R3.3, R3.4, R4, R5 and associated measures, evidence retention and VSLs. Added new requirements for ERO – R1, R7, R8.	Revision to entire standard (Project 2009-01)

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

When this standard has received ballot approval, the text boxes will be moved to the Guideline and Technical Basis Section.

Introduction

1. Title: Impact Event and Disturbance Assessment, Analysis, and Reporting

2. Number: EOP-004-2

3. Purpose: Responsible Entities shall report impact events and their known causes to support situational awareness and the reliability of the Bulk Electric System (BES).

4. Applicability

4.1. Functional Entities:

4.1.1. Reliability Coordinator

4.1.2. Balancing Authority

4.1.3. Transmission Owner

4.1.4. Transmission Operator

4.1.5. Generator Owner

4.1.6. Generator Operator

4.1.7. Distribution Provider

4.1.8. Electric Reliability Organization

5. Background:

NERC established a SAR Team in 2009 to investigate revisions to the CIP-001 and EOP-004 Reliability Standards.

1. CIP-001 may be merged with EOP-004 to eliminate redundancies.
2. Acts of sabotage have to be reported to the DOE as part of EOP-004.
3. Specific references to the DOE form need to be eliminated.
4. EOP-004 has some 'fill-in-the-blank' components to eliminate.

The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards (see tables for each standard at the end of this SAR for more detailed information).

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC SC in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009. A "concepts paper" was designed

to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed.

The concept paper sought comments from stakeholders on the "road map" that will be used by the SDR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the SDR SDT.

The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC database and FERC Order 693 Directives in order to determine a prudent course of action with respect to these standards.

The DSR SDT has proposed the following concept for ***impact event***:

> *An impact event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action.*

To support this concept, the DSR SDT has provided specific event for reporting including types of impact events and timing thresholds pertaining to the different types of impact events and who's responsibility for reporting under the different impact events. This information is outlined in Attachment 1 to the proposed standard.

The DSR SDT wishes to make clear that the proposed changes do not include any real-time operating notifications for the types of events covered by CIP-001, EOP-004. This is achieved through the RCIS and is covered in other standards (e.g. TOP). The proposed standard deals exclusively with after-the-fact reporting.

The DSR SDT is proposing to consolidate disturbance and impact event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts

- A single form to report disturbances and impact events that threaten the reliability of the bulk electric system
- Other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements
- Clear criteria for reporting
- Consistent reporting timelines
- Clarity around of who will receive the information and how it will be used

Requirements and Measures

R1. The ERO shall establish, maintain and utilize a system for receiving and distributing impact event reports, received pursuant to Requirement R6, to applicable government, provincial or law enforcement agencies and Registered Entities to enhance and support situational awareness.

M1. The ERO shall provide evidence that it established, maintained and utilized a system for the distribution of the reports it receives to the various organizations or agencies. Such evidence could include, but is not limited to, dated records indicating that reports were distributed as shown on the submitted report or electronic logs indicating distribution of reports. (R1)

Rationale for R1

The goal of the DSR SDT is to have a generic reporting form and a system for all functional entities (US, Canada, Mexico) to submit impact event reports to NERC and other entities. Ultimately, it may make sense to develop an electronic version of the form to expedite completion, sharing and storage. Ideally, entities would complete a single electronic form on-line which could then be electronically forwarded or distributed to jurisdictional agencies and functional entities as appropriate using check boxes or other coding within the electronic form. Specific reporting forms that exist today (i.e. - OE-417, etc) could be included as part of the electronic form to accommodate US entities with a requirement to submit the form or may be removed (but still be mandatory for US entities under Public Law 93-275) to streamline the proposed consolidated reliability standard for all North American entities (US, Canada, Mexico). Jurisdictional agencies may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE. Functional entities may include the RC, TOP, and BA for situational awareness. Applicability of the standard will be determined based on the specific requirements.

The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT is planning to update the listing of reportable events from discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences may still exist.

Responsible entities will ultimately be responsible for ensuring that OE-417 reports are received at the DOE.

R2. Each Applicable Entity identified in Attachment 1 shall have an Operating Plan(s) for identifying, assessing and reporting impact events listed in Attachment 1 that includes the following components:

2.1. Method(s) for identifying impact events

2.2. Method(s) for assessing cause(s) of impact events

2.3. Method(s) for making internal and external notifications pursuant to Parts 2.5 and 2.6

2.4. List of internal company personnel responsible for making initial notification(s) pursuant to Parts 2.5.and 2.6.

2.5. List of internal company personnel to notify

2.6. List of external organizations to notify to include but not limited to NERC, Regional Entity, Law Enforcement, and Governmental or Provincial Agencies.

2.7. Method(s) for updating the Operating Plan when there is a component change within 30 days of the notification of the change.

2.8. A provision for updating the Operating Plan based on lessons learned from an exercise or implementation of the Operating Plan within 30 days of identifying the lessons learned.

2.9. A provision for updating the Operating Plan based on applicable lessons learned from the annual NERC report issued pursuant to Requirement R8 within 30 days of NERC publishing lessons learned.

M2. Each Applicable Entity shall provide the current in force Operating Plan to the Compliance Enforcement Authority upon request. (R2)

Rationale for R2

Every industry participant that owns or operates elements or devices on the grid has a formal or informal process, procedure, or steps it takes to assess what happened and why it happened when impact events occur. This requirement has the Registered Entity establish documentation on how that procedure, process, or plan is organized.

For the Operating Plan, the DSR SDT envisions that “assessing” includes performing sufficient analysis to be able to complete the report for reportable impact events. The main issue is to make sure an entity can a) identify when an impact event has occurred and b) be able to gather enough information to complete the report.

Parts 3.3 and 3.4 include, but not limited to, operating personnel who could be involved with any aspect of the operating plan.

The Operating Plan may include, but not be limited to, the following: how the entity is notified of event’s occurrence, person(s) initially tasked with the overseeing the assessment or analytical study, investigatory steps typically taken, and documentation of the assessment / remedial action plan.

R3. Each Applicable Entity shall identify and assess initial probable cause of impact events listed in Attachment 1 in accordance with its Operating Plan documented in Requirement R2.

M3. To the extent that an Applicable Entity has an impact event on its Facilities, the Applicable Entity shall provide documentation of its assessment or analysis. Such evidence could include, but is not limited to, operator logs, voice recordings, or power flow analysis cases. (R3)

Rationale for R3

The DSR SDT intends for each Applicable Entity to assess the causes of the reportable impact event and gather enough information to complete the report that is required to be filed.

R4. Each Applicable Entity shall conduct a drill, exercise, or Real-time implementation of its Operating Plan for reporting created pursuant to Requirement R2 at least annually, with no more than 15 months between exercises or actual use.

M4. The Applicable Entity shall provide evidence that it conducted a drill, exercise or Real-time implementation of the Operating Plan for reporting as specified in the requirement. Such evidence could include, but is not limited to, a dated, exercise scenario with notes on the exercise or operator logs, voice recordings, or power flow analysis cases for an actual implementation of the Operating Plan. (R4)

Rationale for R4

The DSR SDT intends for each Applicable Entity to conduct a drill or exercise of it Operating Plan as often as merited but no longer than 15 months from the previous exercise to prevent a long cycle of exercises (i.e., conducting an exercise in January of one year and then December of the next year). Multiple exercises in a 15 month period is not a violation of the requirement and would be encouraged to improve reliability. A drill or exercise may be a table-top exercise, a simulation or an actual implementation of the Operating Plan.

R5. Each Applicable Entity shall provide training to all internal personnel identified in its Operating Plan for reporting pursuant to Requirement R2 subject to the following:

5.1 The training includes the personnel required to respond and their required actions under the Operating Plan.

5.2 Training conducted at least once per calendar year, with no more than 15 months between training sessions for personnel with existing responsibilities.

5.3 If the Operating Plan is revised (with the exception of contact information revisions), training shall be conducted within 30 days of the Operating Plan revisions.

5.4 For internal personnel added to the Operating Plan or those with revised responsibilities under the Operating Plan, training shall be conducted prior to assuming the responsibilities in the plan.

Rationale for R5

The SDT is not prescribing how training is to be conducted and leaves that decision to each Applicable Entity as they best know how to conduct such activities. Conduct of an exercise constitutes training for compliance with this requirement.

For changes to the Operating Plan (5.3), the training may simply consist of a review of the revised responsibilities and a "sign-off" that personnel have reviewed the revisions.

M5. Applicable Entities shall provide the actual training material presented to verify content and the association between the people listed in the plan and those who participated in the training, documentation showing who was trained and when internal personnel were trained on the responsibilities in the Operating Plan as well as dates for personnel changes and evidence that the training was conducted following personnel changes. (R5)

R6. Each Applicable Entity shall report impact events in accordance with its Operating Plan created pursuant to Requirement R2 and the timelines outlined in Attachment 1.

M6. Registered Entities shall provide evidence demonstrating the submission of reports using the Operating Plan created pursuant to Requirement R2 for impact events. Such evidence will include a copy of the original impact event report submitted, evidence to support the type of impact event experienced; the date and time of the impact event ; as well as evidence of report submittal that includes date and time. (R6)

R7. The ERO shall annually review and propose revisions to the impact event table (Attachment 1) if warranted based on its analysis of reported impact events. Revisions to Attachment 1 shall follow the Reliability Standards Development Procedure.

M7. The ERO shall provide evidence that it reviewed the impact event table. If applicable, the ERO shall provide evidence that it followed the Reliability Standards Development Procedure to propose and implement revisions to Attachment 1. Such evidence may include, but not be limited to, documentation that compares or assesses the list of impact events (Attachment 1) against the analysis of reported impact events. (R7)

Rationale for R7-R8

Some of the concepts contained in Requirements R7 and R8 are contained in the NERC Rules of Procedure, section 800. The DSR SDT felt that, in order to have a complete standard for reporting impact events that improved reliability, there needed to be feedback to industry on a regular basis as well as when issues are discovered. The analysis of impact events is crucial and the subsequent dissemination of the results of that analysis must be performed.

In accordance with Sections 401(2) and 405 of the Rules of Procedures, the ERO can be set as an applicable entity in a requirement or standard. After careful consideration, the DSR SDT believes that these requirements (R7-8) are best applicable to the ERO.

R8. The ERO shall publish a quarterly report of the year's reportable impact events subject to the following:

8.1 Issued no later than 30 days following the end of the calendar quarter

8.2 Identifies trends on the BES

8.3 Identifies threats to the BES

8.4 Identifies other vulnerabilities to the BES

8.5 Documents lessons learned

8.6 Includes recommended actions.

Rationale for R8

The ERO will analyze Impact Events that are reported through requirement R6. The DSR SDT envisions the ERO issuing reports identifying trends, threats or other vulnerabilities when available or at least quarterly. The report will include lessons learned and recommended actions (such as mitigation plans) to improve reliability as applicable.

M8. The ERO shall provide evidence that it issued a report identifying trends, threats, or other vulnerabilities on the bulk electric system at least quarterly. Such evidence will include a copy of the report as well as dated evidence of the report's issuance. (R8)

Compliance

Compliance Enforcement Authority

- Regional Entity
- For requirements applicable to the ERO, an entity contracted to perform an audit.

Compliance Monitoring and Enforcement Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

Evidence Retention

Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator and Distribution Provider shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

The ERO shall retain evidence of Requirements 1, 7 and 8, Measures 1, 7, and 8 for three calendar years.

Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator and Distribution Provider shall retain data or evidence of Requirements 2, 3, 4, and 5 and Measures 2, 3, 4, and 5 for three calendar years for the duration of any regional investigation, whichever is longer to show compliance unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator and Distribution Provider shall retain data or evidence of Requirement 6 and Measure 6 for three calendar years for the duration of any regional investigation, whichever is longer to show compliance unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

Additional Compliance Information

To be determined.

Variances

None

Interpretations

None

EOP-004 - Attachment 1: Impact Events Table

NOTE: Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by an impact event and issue a written Impact Event Report within the timing in the table below. In such cases, the affected Applicable Entity shall notify its Regional Entity(ies) and NERC, and verbally provide as much information as is available at that time. The affected Applicable Entity shall then provide periodic verbal updates until adequate information is available to issue a written Preliminary Impact Event Report.

EOP-004 – Attachment 1 - Actual Reliability Impact – Part A			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Time to Submit Report**
Energy Emergency requiring Public appeal for load reduction	RC, BA	To reduce consumption in order to maintain the continuity of the BES Each public appeal for load reduction	Within 1 hour of issuing a public appeal
Energy Emergency requiring system-wide voltage reduction	RC, TO, TOP, DP	System wide voltage reduction of 3% or more	Within 1 hour after occurrence is identified
Energy Emergency requiring firm load shedding	RC, BA, TOP, DP	Firm load shedding ≥ 100 MW (manually or via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)	Within 24 hours after occurrence
Voltage Deviations	RC, TOP, GOP	± 10% sustained for ≥ 15 minutes	Within 24 hours after 15 minute threshold
Frequency Deviations	RC, BA	± Deviations ≥ than Frequency Trigger Limit (FTL) more than 15 minutes	Within 24 hours after 15 minute threshold
IROL Violation	RC, TOP	Operate outside the IROL for time greater than IROL Tv	Within 24 hours after Tv threshold
Loss of Firm load for ≥ 15 Minutes	RC, BA, TO, TOP, DP	• ≥ 300 MW for entities with previous year's demand ≥ 3000 MW • ≥ 200 MW for all other entities	Within 24 hours after 15 minute thresh
System Separation (Islanding)	RC, BA, TOP, DP	Each separation resulting in an island of generation and load ≥ 100 MW	Within 1 hour after occurrence is identified
Generation loss	RC, BA, GO, GOP	• ≥ 2,000 MW for entities in the Eastern or Western Interconnection	Within 24 hours after occurrence

EOP-004 – Attachment 1 - Actual Reliability Impact – Part A			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Time to Submit Report**
		• ≥ 1000 MW for entities in the ERCOT or Quebec Interconnection • An entire generating station of ≥ 5 generators with aggregate capacity of ≥ 500 MW	
Transmission loss	RC, TO, TOP	• An entire DC converter station • Multiple BES transmission elements (simultaneous or common-mode event)	Within 24 hours after occurrence
Damage or destruction of BES equipment[1]	RC, BA, TO, TOP, GO, GOP, DP	Through operational error, equipment failure, or external cause	Within 1 hour after occurrence is identified

Examples:

a. BES equipment that is:
   i. A critical asset
   ii. Affects an IROL
   iii. Significantly affects the reliability margin of the system e.g., has the potential to result in the need for emergency actions
   iv. Damaged or destroyed due to a non-environmental external cause

b. Report copper theft from BES equipment only if it degrades the ability of equipment to operate correctly e.g., removal of grounding straps rendering protective relaying ineffective

EOP-004 – Attachment 1 - Potential Reliability Impact – Part B			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Time to Submit Report**
Unplanned Control Center evacuation	RC, BA, TOP	Unplanned evacuation from BES control center facility	report within 1 hour after occurrence
Fuel supply emergency	RC, BA, GO, GOP	Affecting BES reliability[1]	report within 1 hour after occurrence
Loss of off-site power (grid supply)	RC, BA, TO, TOP, GO, GOP	Affecting a nuclear generating station	report within 1 hour after occurrence
Loss of all monitoring or voice communication capability	RC, BA, TOP	Affecting a BES control center for ≥ 30 minutes	report within 1 hour after occurrence
Forced intrusion[2]	RC, BA, TO, TOP, GO, GOP	At a BES facility	report within 24 hours after occurrence
Risk to BES equipment[3]	RC, BA, TO, TOP, GO, GOP, DP	From a non-environmental physical threat	report within 24 hours after occurrence
Detection of a cyber intrusion to critical cyber assets	RC, BA, TO, TOP, GO, GOP, DP	That meets the criteria in CIP-008 (or its successor)	report within 24 hours after occurrence

1. Report if problems with the fuel supply chain result in the projected need for emergency actions to manage reliability.
2. Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects the reliability of the BES).
3. Examples include a train derailment adjacent to BES equipment, that either could have damaged the equipment directly or has the potential to damage the equipment (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center).

EOP-002 - Attachment 2: Impact Event Reporting Form

EOP-004 – Confidential Impact Event Report		
	Task	**Comments**
1.	Entity filing the report (include Compliance Registration ID number):	
2.	Date and Time of impact event. Date: (mm/dd/yy) Time/Zone:	
3.	Name of contact person: Email address: Telephone Number:	
4.	Did the impact event originate in your system?	Yes ☐ No☐
5.	Under which NERC function are you reporting?	
6.	Brief Description of impact event: (More detail should be provided in the Sequence of Events section below.)	

EOP-004 – Confidential Impact Event Report			
	Task	Comments	
7.	Generation tripped off-line. MW Total List units tripped		
8.	Frequency. Just prior to impact event (Hz): Immediately after impact event (Hz max): Immediately after impact event (Hz min):		
9.	List transmission facilities (lines, transformers, buses, etc.) tripped and locked-out. (Specify voltage level of each facility listed).		
10.		FIRM	INTERRUPTIBLE
	Demand tripped (MW):		
	Number of affected customers:		
	Demand lost (MW-Minutes):		

EOP-004 – Confidential Impact Event Report			
	Task	Comments	
11.	Restoration Time.	INITIAL	FINAL
	Transmission:		
	Generation:		
	Demand:		
12.	Sequence of Events:		
13.	Identify the initial probable cause or known root cause of the impact event:		

EOP-004 – Confidential Impact Event Report		
	Task	Comments
14.	Identify any protection system misoperation(s):	
15.	Additional Information that the helps to further explain the event if needed. A one-line diagram may be attached, if readily available, to assist in the evaluation of the event.:	

Guideline and Technical Basis

Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01) - Reporting Concepts

Introduction

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and is progressing toward developing standards based on the SAR. This concepts paper is designed to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed.

The standards listed under the SAR are:

- CIP-001 — Sabotage Reporting
- EOP-004 — Disturbance Reporting

The DSR SDT also proposed to investigate incorporation of the cyber incident reporting aspects of CIP-008 under this project. This will be coordinated with the Cyber Security - Order 706 SDT (Project 2008-06).

The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC database and FERC Order 693 Directives to determine a prudent course of action with respect to these standards.

This concept paper provides stakeholders with a proposed “road map” that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. This concept paper provides the background information and thought process of the DSR SDT.

The proposed changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). The proposed standards deal exclusively with after-the-fact reporting.

The DSR SDT is proposing to consolidate disturbance and event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts and Assumptions:

The Standard Will: Require use of a single form to report disturbances and "impact events" that threaten the reliability of the bulk electric system

- Provide clear criteria for reporting
- Include consistent reporting timelines
- Identify appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- Provide clarity around of who will receive the information

The drafting team will explore other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements

Discussion of Disturbance Reporting
Disturbance reporting requirements currently exist in EOP-004. The current approved definition of Disturbance from the NERC Glossary of Terms is:

1. An unplanned event that produces an abnormal system condition.
2. Any perturbation to the electric system.
3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.

Disturbance reporting requirements and criteria are in the existing EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and developed the list of impact events that are to be reported under this standard (attachment 1).

Discussion of "impact event" Reporting
There are situations worthy of reporting because they have the potential to impact reliability. The DSR SDT proposes calling such incidents 'impact events' with the following concept:

> An impact event is any situation that has the potential to significantly impact the reliability of the Bulk Electric System. Such events may originate from malicious intent, accidental behavior, or natural occurrences.

Impact event reporting facilitates situational awareness, which allows potentially impacted parties to prepare for and possibly mitigate the reliability risk. It also provides the raw material, in the case of certain potential reliability threats, to see emerging patterns.

Examples of impact events include:

- Bolts removed from transmission line structures
- Detection of cyber intrusion that meets criteria of CIP-008 or its successor standard
- Forced intrusion attempt at a substation
- Train derailment near a transmission right-of-way
- Destruction of Bulk Electrical System equipment

What about sabotage?

One thing became clear in the DSR SDT's discussion concerning sabotage: everyone has a different definition. The current standard CIP-001 elicited the following response from FERC in FERC Order 693, paragraph 471 which states in part: *". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."*

Often, the underlying reason for an event is unknown or cannot be confirmed. The DSR SDT believes that reporting material risks to the Bulk Electrical System using the impact event categorization, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.

The DST SDT discussed the reliability needs for impact event reporting and will consider guidance found in the document "NERC Guideline: Threat and Incident Reporting" in the development of requirements, which will include clear criteria for reporting.

Certain types of impact events should be reported to NERC, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and/or Provincial or local law enforcement. Other types of impact events may have different reporting requirements. For example, an impact event that is related to copper theft may only need to be reported to the local law enforcement authorities.

Potential Uses of Reportable Information

Event analysis, correlation of data, and trend identification are a few potential uses for the information reported under this standard. As envisioned, the standard will only require Functional entities to report the incidents and provide information or data necessary for these analyses. Other entities (e.g. – NERC, Law Enforcement, etc) will be responsible for performing the analyses. The NERC Rules of Procedure (section 800) provide an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for reliability. Jurisdictional agencies (which may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE) have other duties and responsibilities.

Collection of Reportable Information or "One stop shopping"

The goal of the DSR SDT is to have one reporting form for all functional entities (US, Canada, Mexico) to submit to NERC. Ultimately, it may make sense to develop an electronic version to expedite completion, sharing and storage. Ideally, entities would complete a single form which could then be distributed to jurisdictional agencies and functional entities as appropriate. Specific reporting forms[1] that exist today (i.e. - OE-417, etc) could be included as part of the

[1] The DOE Reporting Form, OE-417 is currently a part of the EOP-004 standard. If this report is removed from the standard, it should be noted that this form is still required by law as noted on the form: NOTICE: This report is mandatory under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. Title 18 USC 1001 makes it a criminal

electronic form to accommodate US entities with a requirement to submit the form, or may be removed (but still be mandatory for US entities under Public Law 93-275) to streamline the proposed consolidated reliability standard for all North American entities (US, Canada, Mexico). Jurisdictional agencies may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE. Functional entities may include the RC, TOP, and BA for situational awareness. Applicability of the standard will be determined based on the specific requirements.

The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT is planning to update the listing of reportable events from discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences may still exist.

The reporting proposed by the DSR SDT is intended to meet the uses and purposes of NERC. The DSR SDT recognizes that other requirements for reporting exist (e.g., DOE-417 reporting), which may duplicate or overlap the information required by NERC. To the extent that other reporting is required, the DSR SDT envisions that duplicate entry of information is not necessary, and the submission of the alternate report will be acceptable to NERC so long as all information required by NERC is submitted. For example, if the NERC Report duplicates information from the DOE form, the DOE report may be included or attached to the NERC report, in lieu of entering that information on the NERC report.

offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Comment Form for the first draft of EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting [Project 2009-01]

Please **DO NOT** use this form to submit comments on the proposed reliability standard, EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting. Comments must be submitted by **October 15, 2010**. If you have questions please contact Stephen Crutchfield by email at Stephen.crutchfield@nerc.net or by telephone at 609-651-9455.

Background Information:

NERC established a SAR Team in 2009 to investigate revisions to the CIP-001 and EOP-004 Reliability Standards.

1. CIP-001 may be merged with EOP-004 to eliminate redundancies.
2. Acts of sabotage have to be reported to the DOE as part of EOP-004.
3. Specific references to the DOE form need to be eliminated.
4. EOP-004 has some 'fill-in-the-blank' components to eliminate.

The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards (see tables for each standard at the end of this SAR for more detailed information).

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC SC in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009. A "concepts paper" was designed to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed.

The concept paper sought comments from stakeholders on the "road map" that will be used by the SDR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the SDR SDT.

The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC database and FERC Order 693 Directives in order to determine a prudent course of action with respect to these standards.

The DSR SDT has proposed the following concept for ***impact event***:

> *An impact event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action.*

To support this concept, the DSR SDT has provided specific event for reporting including types of impact events and timing thresholds pertaining to the different types of impact events and who's responsibility for reporting under the different impact events. This information is outlined in Attachment 1 to the proposed standard.
The DSR SDT wishes to make clear that the proposed changes do not include any real-time operating notifications for the types of events covered by CIP-001, EOP-004. This is achieved through the RCIS and is covered in other standards (e.g. TOP). The proposed standard deals exclusively with after-the-fact reporting.

The DSR SDT is proposing to consolidate disturbance and impact event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts

- A single form to report disturbances and impact events that threaten the reliability of the bulk electric system
- Other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements
- Clear criteria for reporting
- Consistent reporting timelines
- Clarity around of who will receive the information and how it will be used

You do not have to answer all questions. Enter All Comments in Simple Text Format.

Insert a "check" mark in the appropriate boxes by double-clicking the gray areas.

1. Do you agree with the purpose statement of the proposed standard? Please explain in the comment box below.

   ☐ Yes
   ☐ No

   Comments:

2. Do you agree with the applicable entities in the Applicability Section as well as assignment of applicable entities noted in Attachment 1? Please explain in the comment box below.

   ☐ Yes
   ☐ No

   Comments:

3. Do you agree with the requirement R1 and measure M1? Please explain in the comment box below.

   ☐ Yes
   ☐ No

   Comments:

4. Do you agree with the requirement R2 and measure M2? Please explain in the comment box below.

   ☐ Yes
   ☐ No

   Comments:

5. Do you agree with the requirement R3 and measure M3? Please explain in the comment box below.

   ☐ Yes
   ☐ No

   Comments:

6. Do you agree with the requirement R4 and measure M4? Please explain in the comment box below.

☐ Yes
☐ No

Comments:

7. Do you agree with the requirement R5 and measure M5? Please explain in the comment box below.

☐ Yes
☐ No

Comments:

8. Do you agree with the requirement R6 and measure M6? Please explain in the comment box below.

☐ Yes
☐ No

Comments:

9. Do you agree with the requirements for the ERO (R7-R8) or is this adequately covered in the Rules of Procedure (section 802)? Please explain in the comment box below.

☐ Yes
☐ No

Comments:

10. Do you agree with the impact event list in Attachment 1? Please explain in the comment box below and provide suggestions for additions to the list of impact events.

☐ Yes
☐ No

Comments:

11. Do you agree with the use of the Preliminary Impact Event Report (Attachment 2)? Please explain in the comment box below.

☐ Yes
☐ No

Comments:

12. The DSR SDT has replaced the terms "disturbance" and "sabotage" with the term "impact events". Do you agree that the term "impact events" adequately replaces the terms "disturbance" and "sabotage" and addresses the FERC directive to "further define sabotage" in an equally efficient and effective manner? Please explain in the comment box below.

☐ Yes
☐ No

Comments:

13. The DSR SDT has combined EOP-004 and CIP-001 into one standard (please review the mapping document that shows the translation of requirements from the already approved versions of CIP-001 and EOP-004 to the proposed EOP-004), EOP-004-3 and retiring CIP-001. Do you agree that there is no reliability gap between the existing standards and the proposed standard? **Please** explain in the comment box below.

☐ Yes
☐ No

Comments:

14. Do you agree with the proposed effective dates? Please explain in the comment box below.

☐ Yes
☐ No

Comments:

15. Do you have any other comments that you have not identified above?

☐ Yes
☐ No

Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document Showing Translation of CIP-001-1 – Sabotage Reporting and EOP-004-1 – Disturbance Reporting, into EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting

Standard: CIP-001-1 – Sabotage Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting**
R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.	Moved into EOP-004-2, R2	R2. Each Applicable Entity identified in Attachment 1 shall have an Operating Plan(s) for identifying, assessing and reporting impact events listed in Attachment 1 that includes the following components: 2.1. Method(s) for identifying impact events 2.2. Method(s) for assessing cause(s) of impact events 2.3. Method(s) for making internal and external notifications pursuant to Parts 2.5 and 2.6 2.4. List of internal company personnel responsible for making initial notification(s) pursuant to Parts 2.5.and 2.6. 2.5. List of internal company personnel to notify 2.6. List of external organizations to notify to include but not limited to NERC, Regional Entity, Law Enforcement, and Governmental or Provincial Agencies. 2.7. Method(s) for updating the Operating Plan when there is a component change within 30 days of the notification of the change. 2.8. A provision for updating the Operating Plan based on lessons learned from an exercise or implementation of the Operating Plan within 30 days of identifying the lessons learned. 2.9. A provision for updating the Operating Plan based on applicable lessons learned from the annual NERC report issued pursuant to Requirement R8 within 30 days of NERC publishing lessons learned.

R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	Moved into EOP-004-2, R2	
R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.	Moved into EOP-004-2, R2	
R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.	Moved into EOP-004-2, R2	

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting Comments**
R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.	Retire this fill-in-the-blank requirement. Replace with new reporting procedure developed by NERC EAWG.	*(The NERC EAWG is working to develop continent wide reporting guidelines applicable under the NERC Rules of Procedure.)*
R2. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.	Translated into EOP-004-2, R1	R1. Each Applicable Entity shall have a documented Operating Plan for identifying and assessing impact events listed in Attachment 1.
R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity experiencing a reportable incident shall	Translated into EOP-004-2, R6	R6. Each Applicable Entity shall report impact events in accordance with its Operating Plan created pursuant to Requirement R2 and the timelines

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting Comments**
provide a preliminary written report to its Regional Reliability Organization and NERC.		outlined in Attachment 1.
R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.	Translated into EOP-004-2, R6	R6. Each Applicable Entity shall report impact events in accordance with its Operating Plan created pursuant to Requirement R2 and the timelines outlined in Attachment 1.
R3.2. Applicable reporting forms are provided in Attachments 022-1 and 022-2.	Retire – informational statement	
R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.	Retire as a requirement. Added as a "Note" to EOP-004-Attachment1-Impact Events Table	*NOTE: Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by an impact event and issue a written Impact Event Report within the timing in the table below. In such cases, the affected Applicable Entity shall notify its Regional Entity(ies) and NERC, and verbally provide as much information as is available at that time. The affected Applicable Entity shall then provide periodic verbal updates until adequate information is available to issue a written Preliminary Impact Event Report.*
R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity in which a disturbance occurred, a final report is required,	Retire this fill-in-the-blank requirement. Replace with new	*(The NERC EAWG is working to develop continent wide reporting guidelines applicable under the NERC Rules of Procedure.)*

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting Comments**
the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.	reporting procedure developed by NERC EAWG.	
R4. When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.	Retire this fill-in-the-blank requirement. Replace with new reporting procedure developed by NERC EAWG.	*(The NERC EAWG is working to develop continent wide reporting guidelines applicable under the NERC Rules of Procedure.)*
R5. The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.	Retire this fill-in-the-blank requirement. Replace with new reporting procedure developed by NERC EAWG.	*(The NERC EAWG is working to develop continent wide reporting guidelines applicable under the NERC Rules of Procedure.)*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

30-Day Informal Comment Period Open
September 15 - October 15, 2010

Now available at: http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Project 2009-01 Disturbance and Sabotage Reporting

The Disturbance and Sabotage Reporting Standard Drafting Team is seeking comments on its preliminary draft of EOP-004-2 – Impact Event and Disturbance Assessment, Analysis, and Reporting **until 8 p.m. EDT on October 15, 2010**.

Transition from Reliability Standards Development Procedure Version 7 – to Standard Processes Manual

In accordance with the Standard Processes Manual approved by FERC on September 3, 2010, the drafting team is using an "informal" comment period to solicit stakeholder feedback. The new standard development process allows drafting teams to use informal comment periods. Unlike formal comment periods where a drafting team provides a response to each comment submitted, with informal comment periods the drafting team provides a summary response to each question asked on its comment form, but the team is not obligated to provide an individual response to each comment submitted. The summary response will indicate whether stakeholders support the proposal and will identify any additional changes made based on stakeholder comments. With informal comment periods drafting teams are not required to provide an individual response to each comment submitted. This change to the process is intended to give drafting teams more time to deliberate on technical issues, as opposed to deliberating on individual responses to comments. Note that while informal comment periods are allowed in the new standard process for preliminary drafts of proposed standards, formal comment periods are still required for the final draft of each standard.

Instructions

Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page:
http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Next Steps

The drafting team will draft and post a summary response to the comments received and conforming revisions to the standard. The next will be either another 30-day informal comment period or a 30-day formal comment period on the complete standard.

Project Background

This project involves revising existing standards CIP-001-1 — Sabotage Reporting and EOP-004-1 — Disturbance Reporting to eliminate redundancies and provide clarity on sabotage events. The project will address several issues identified by stakeholders, as well as FERC directives from Order 693, including a directive to provide greater clarity to requirements associated with "sabotage."

EOP-004-2 was drafted using the "results-based" criteria for developing a reliability standard. The results-based approach includes considerably more emphasis on the "concepts and assumptions" underlying the development of requirements and goes beyond the steps most drafting teams have previously used when developing a standard. Accordingly, the "look and feel" of a results-based standard is quite different than NERC's existing standards. However, at the core is a set of mandatory and enforceable requirements with useful guidance supporting these requirements, an approach NERC's legal counsel has reviewed and finds acceptable. More information about results-based standards can be found at: http://www.nerc.com/filez/standards/Project2010-06_Results-based_Reliability_Standards.html

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson,
Standards Process Administrator, at monica.benson@nerc.net or at 609.452.8060

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Individual or group. (60 Responses)
Name (37 Responses)
Organization (37 Responses)
Group Name (23 Responses)
Lead Contact (23 Responses)
Question 1 (56 Responses)
Question 1 Comments (60 Responses)
Question 2 (58 Responses)
Question 2 Comments (60 Responses)
Question 3 (54 Responses)
Question 3 Comments (60 Responses)
Question 4 (56 Responses)
Question 4 Comments (60 Responses)
Question 5 (54 Responses)
Question 5 Comments (60 Responses)
Question 6 (55 Responses)
Question 6 Comments (60 Responses)
Question 7 (55 Responses)
Question 7 Comments (60 Responses)
Question 8 (54 Responses)
Question 8 Comments (60 Responses)
Question 9 (49 Responses)
Question 9 Comments (60 Responses)
Question 10 (55 Responses)
Question 10 Comments (60 Responses)
Question 11 (52 Responses)
Question 11 Comments (60 Responses)
Question 12 (53 Responses)
Question 12 Comments (60 Responses)
Question 13 (52 Responses)
Question 13 Comments (60 Responses)
Question 14 (49 Responses)
Question 14 Comments (60 Responses)
Question 15 (54 Responses)
Question 15 Comments (60 Responses)

-
Group
Northeast Power Coordinating Council
Guy Zito
No
The proposed requirements in the standard are not focused on the core industry concern that current requirements are unclear as to what types of events warrant entities to report. Per draft 2 of the SAR, “The existing requirements need to be revised to be more specific – and there needs to be more clarity in what sabotage looks like.” Instead this proposed standard includes requirements that are more focused on “how” to report, rather than “what” to report. The draft 2 SAR has never been balloted for approval prior to standard drafting. In fact, the SAR states, “The development may include other improvements to the standards deemed appropriate by the drafting team, with consensus on the stakeholders (emphasis added), consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.” The scope of the SAR, and likewise the proposed standard, is inappropriate to the fundamental reliability purpose of what events need to be reported. The proposed administrative requirements are difficult to interpret, implement and measure, and do not clarify what type of sabotage information entities need to report. Although the use of procedures and an understanding by those personnel accountable seems helpful for ensuring reports are made, the fundamental purpose of clarifying what types of events should be reported and more importantly what types do not have to be reported, is lacking in the standard. Also, one of the first issues identified in the SAR for consideration by the drafting team seems to be ignored: “Consider whether separate, less burdensome requirements for smaller entities may be appropriate.” The requirements for entities to develop Operating Plans and to have training

for those plans, further adds uncertainty and increases complexity of how entities, large and small, will have to comply with this standard. The term “impact events” does not draw a clear boundary around those events that are affected by this standard. Since this is not a defined term, nor is intended to be a defined term in the NERC Glossary, this standard lacks clarity and is likely to produce significant conflict as an applicable entity attempts to establish procedures to assure compliance. It appears that situational awareness could not be improved with this standard since it is only dealing with events after-the-fact, not within the time frame to allow corrective action by the system operator. This draft standard should not have this high a priority while other standards having a greater impact on Bulk Electric System reliability remain incomplete or unfinished. Regional reporting requirements should be in Regional Standards, and not be included in a NERC Standard.

No

Having the ERO as an applicable entity raises the issue that they are also the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. For example, establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC’s open process. NERC has also offered the opinion that since NERC is not a “user, owner, or operator” Standards are not enforceable against the ERO. In Attachment 1 the time frames listed are not consistent for similar events. For example, EEAs are either reported within one or 24 hours depending on the nuance. Having multiple entities reporting the same event is troublesome, i.e., why does a RC have to report an EEA if the BA is going to report it? This will lead to unnecessary and possibly conflicting reports for the same event. Attachment 1 seems to be consolidating time frames from other standards into one for reporting. However, this subject is more complex than this table reveals, and the table needs more clarification. Entities that have information about possible sabotage events should report these to NERC after the fact, and the standard should simply reflect that. While we agree with the list of functional entities identified in the Applicability Section, we do not agree with their application in Attachment 1. As the functional entities are identified in Attachment 1, it is likely that there is going to be duplicate reporting. Several of the events require filing a written formal report within one hour. For example, system separation is going to require an “all hands on deck” response to the actual event. The paragraph above the table in Attachment 1 indicates that a verbal report would be allowed in certain circumstances, but this is the same issue with the formal report in that the system operators are concerned with the event and not the reporting requirements. There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements through NERC that cross federal agency jurisdictions.

No

Having the ERO as an applicable entity raises a concern because they are also the Compliance Enforcement Authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. Establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC’s open process. At this stage it is not clear how the ERO will develop or effectively maintain a list of “applicable government, provincial or law enforcement agencies” for distribution as defined in R1. The “rationale for R1” states that OE-417 could be included as part of the electronic form, but responsible entities will ultimately be responsible for ensuring that OE-417 reports are received at DOE. This requirement needs to be more definitive with respect to OE-417. The better approach would be for the entities to complete OE-417 form and this standard simply require a copy.

No

This is an overly prescriptive requirement given that the intent of this standard is after-the-fact reporting. The requirement to create an Operating Plan is an unnecessary burden that offers no additional improvements to the reliability of the Bulk Electric System, and this is not, in fact, an Operating Plan. At most, it may be a reporting plan. Most of these requirements are administrative and procedural in nature and, therefore, do not belong as requirements in a Reliability Standard. Perhaps they could be characterized as a best practice and have an associated set of Guidelines developed and posted on the subject. As proposed, the Operating Plan is not required to ensure Bulk Electric System reliability. As stated in the purpose of this standard, it does not cover any real-time operating notifications for the types of events covered by CIP-001, EOP-004. Since these incidents are meant to be reportable after-the-fact, familiarity with the reporting requirements and time frames is sufficient. Stating reporting requirements directly in the standard would produce a more uniform and effective result across the industry, contributing towards a more reliable Bulk Electric System. R2.6 establishes an external organization list for Applicable Entity reporting, yet R1 suggests that external reporting will be accomplished via submittal of impact event reports. How will the two requirements be coordinated? What governmental agencies are appropriate, and how will duplicative reporting be addressed (for example, DOE, Nuclear Regulatory Commission)? Also, in the “rationale for R2”, please explain the reference to Parts 3.3 and 3.4.

No

"Impact event” needs to be defined in the NERC Glossary to provide the clarity the industry needs to build auditable compliance procedures. Although it is useful for entities to make an initial assessment of a probable cause of an event, this requirement should stand alone and does not need to be tied to requirement R2, Operating Plan. Quite often, it takes a considerable amount of time for an actual cause to be determined. The determination process may require a complex root cause analysis. Further, in the case of suspected or potential sabotage, the industry can only say it doesn’t know, but it may be possible. Law enforcement agencies make the determination of whether sabotage is involved, and the information may not be made available until an investigation is completed, if indeed it is ever made

available.
No
The need for a periodic drill has not been established, and appears to be overly restrictive given the intent of the standard is the reporting of impact events. Suggest this requirement be eliminated. Similar to our comments on R2 for an Operating Plan, a drill, exercise, or Real-time implementation of its Operating Plan for reporting is unnecessary. Such things are training practices. There are already existing standards requirements regarding training. There is no imminent threat to reliability that requires these events to be reported in as short a time frame as may be required for real-time operating conditions notifications.
No
The need for a periodic drill has not been established, and appears to be overly restrictive given that the intent of the standard is reporting of impact events. Suggest this requirement be eliminated. There are training standards in place that cover these requirements. The relevant personnel should be “aware” of the reporting requirements. But there is not a need to have a training program with specific time frames for reporting impact events. Awareness of these reporting requirements can be achieved through whatever means are available for entities to employ to train on any of the NERC standards, and need not be dictated by requirements.
No
Entities are already required by other agencies (e.g., DOE, NRC) to report certain events. We see no need to develop redundant reporting requirements for NERC that cross other federal agency jurisdictions. There is no need for an Operating Plan as proposed. This is not truly an Operating Plan. There are already other standards which create the requirements for an Operating Plan. This is an administrative reporting plan and any associated impact upon reliability is far beyond real-time operations which is implied by the label “Operating Plan".
No
Having the ERO as an applicable entity raises concern as it is also the compliance enforcement authority. Requirement R7 is unnecessary as there are already requirements in place for three year reviews of all Standards. R8 contains requirements to release information that should be protected, such as identification of trends and threats against the Bulk Electric System. This may trigger more threats because it will be published to unwanted persons in the private sector. We do not support an annual time frame to update the events list. The list should be updated as needed through the Reliability Standards Development Process. Any changes to a standard must be made through the standards development process, and may not be done at the direction of the ERO without going through the process.
No
1) A particular Event could be applicable to multiple entities and Attachment 1 would require each applicable entity to report the event. This is duplicative and would overburden the reporting system. 2) Loss of off-site power (grid supply) reporting for nuclear plants is duplicative of reporting done to satisfy NRC requirements. Given the activity at a nuclear plant during this event, this additional reporting is not desired. 3) Cyber intrusion remains an event that would need to be reported multiple times (e.g., this standard, OE-417, NRC requirements, etc.). 4) Since external reporting for other regulators (e.g., DOE, NRC, etc.) remains an obligation of the Applicable Entity, suggest that Attachment 1 only contain impact events as defined in the current version of EOP-004. What are the examples at the bottom of page 14 supposed to illustrate? Critical Asset should have the appropriate capitalization as being a defined term. Is Critical Asset what is intended to be used here? Should the “a” list be read as ANDs or Ors? Does “loss of all monitoring communications” mean “loss of all BES monitoring “communications”? Does “loss of all voice communications” mean “loss of all BES voice communications?” Are the blue boxes footnotes or examples? Does “forced intrusion” mean “physical intrusion” (which is different from “cyber intrusion”)? Regarding “Risk to BES Equipment,” request clarification of “non-environmental”. Regarding the train derailment example, the mixture of BES equipment and facility is confusing. Request clarification for when the clock starts ticking. Regarding “Detection of a cyber intrusion to critical cyber assets”, there is concern that this creates a double jeopardy situation between CIP-008 and EOP-004-2 R2.6. Suggest physical incident reporting be part of EOP-004 and cyber security reporting be part of CIP-008.
No
There is already a DOE requirement to report certain events. There is no need to develop redundant reporting requirements to NERC that cross other federal agency jurisdictions. The heading on page 16 refers to EOP-002, but this is Standard EOP-004. If some questions do not require an answer all of the time, then the form should state that or provide a NA checkbox. While Attachment 1 details some cyber thresholds, Attachment 2 provides no means to report – which is acceptable if cyber incidents are handled by CIP-008 per the comment provided for Question 10. The Event Report Template in Appendix A is different from the most recent version, which is available at: http://www.nerc.com/docs/eawg/Event_Analysis_Process_WORKINGDRAFT_100110-Clean.pdf
No
The use of the term “impact events” has simply replaced the terms “disturbance” and “sabotage”, and has not further defined sabotage as directed by FERC. We do feel that “impact events” needs to be a defined term. While we agree with the SDT’s new direction, the FERC directive has not been met. This term and the FERC directive do not recognize limitations in what a registered entity can do to determine whether an act of sabotage has been committed. This term should recognize law enforcement and other specialized agencies, including international agencies roles in defining acts of sabotage, and not hold the registered entity wholly responsible to do so.
No

Per the mapping document, some of the existing requirements are awaiting a new reporting procedure being developed by the NERC EAWG. For those requirements that were transferred over, the resulting standard seems overly complex and lacks clarity. EOP-004-3 should be EOP-004-2.
No
The effective dates in Canada need to be defined. The first bullet should be sufficient. If the training and Operation Plan requirements are adopted as proposed, this may not allow sufficient time for some entities to comply, particularly those with limited number of staff, but perform functions that have multiple event reporting requirements.
Yes
Request clarification on how RCIS is part of this Standard. The form should be filled out in two stages. First stage would be the immediately available information. The second stage would be the additional information such as one line diagrams. There is concern with burdening the reporting operator on filling out forms instead of operating the Bulk Electric System. Most of the draft requirements are written as administrative in nature, and this is not most effective. Changes need to be made to (or possibly elimination of) R1, R2, R3. The standards should be changed to define what a “disturbance” is for reporting in EOP-004. Sabotage reporting as per CIP-001 should be rescinded as EOP-004 already has such a requirement.
Group
Tenaska
Brian Pillittere
Yes
Yes
Yes
No
We have adequate compliance procedures already in place for the existing CIP-001-1 and EOP-004-1 Standards. The list of required “Operating Plan” components in the proposed R2 is too specific. Maintaining the “Operating Plan” described in R2 would increase the burden on Registered Entities to comply with the Standard and this type of "laundry list" Requirement would make it more difficult to prove compliance with EOP-004-2 during an audit.
No
The probable cause of a reportable event is already required to be submitted on the OE-417 form. This Requirement is redundant.
No
This Requirement is too specific and places additional burdens on Registered Entities.
No
This Requirement is too specific and places additional burdens on Registered Entities.
No
The reporting timelines are currently listed on the OE-417 form. This Requirement is redundant.
Yes
Since the proposed EOP-004-2 Standard does not eliminate the OE-417 reporting requirement, it does not streamline the existing CIP-001-1 and EOP-004-1 reporting requirements for GO/GOP’s. The "laundry list" of components required in the Operating Plan described in R2 is too specific and would make it more difficult to prove compliance during an audit. We prefer that the existing CIP-001-1 and EOP-004-1 Standards remain unchanged.
Individual
Brenda Lyn Truhe
PPL Electric Utilities
Yes
No
While we agree with the applicable entities in the Applicability Section of the revised standard, we would like the SDT to

reconsider the applicable entities identified on Attachment 1, specifically regarding duplication of reporting e.g. should TO and TOP report?
Yes
No
While we agree with documenting our process, we feel the use of the defined term Operating Plan is not required and possibly a misuse of the term. We would like to suggest using the term ‘procedure’. Additionally, we would like the SDT to confirm/clarify whether Attachment 1 is a complete list of impact events. Also, please confirm that the Proposed R2.1 language ‘Method(s) for identifying impact events’ means identifying impact event occurrence as opposed to identifying list of impact events. i.e. does R2.1 mean recognize impact event occurrence?
No
We believe the rationale for R3 is good and provides value. However, we feel the clarity was lost when the rationale was translated to the standards language. Please consider revising language to refocus on rationale of assess and report per Attachment 1 as opposed to identify. We suggest changing the word “identify” to “recognize” and add the Rationale statement to the requirement as follows: “Each Applicable Entity shall assess the causes of the reportable event and gather available information to the complete the report.”
Yes
No
We agree with the need for training on one’s process. However, we suggest changes to R5.3. Consider expanding the exception criteria to exempt non-substantive changes such as errata changes, minor editorial changes, contact information changes, etc. We also suggest saying ‘…,training shall be conducted, or notification of changes made, within 30 days of the procedure revisions.’
No
We understand the rationale for this standard and support the project to combine EOP-004 and CIP-001 as well as the reporting requirement in CIP-008. We are concerned that it may be difficult to meet Attachment 1 Part B Potential Reliability Impact submittal times as the time to submit is 1 or 24 hour after occurrence. E.g. Risk to BES equipment, the example given is a major event and easy to conclude. Consider forced intrusion, risk to BES equipment (increased violence in remote area), or cyber intrusion – should Attachment 1 state ‘report within 24 hours after detection’?
Yes
No
While we think providing an impact event list is beneficial, we would like to see Attachment 1 revised and/or clarified. Refer to response to Question 2 considering duplicate reporting. Regarding impact event ‘Damage or destruction of BES equipment’ and considering the first example in the ‘Examples’ section, does ‘example a. i.’ mean if the BES equipment that is damaged is not identified as a critical asset per CIP-002 that no reporting is required? Clarify the Part A and Part B, specifically: Attachment 1 Part A is labeled ‘Actual Reliability Impact’. Does this title mean that for all events listed that the ‘threshold for reporting’ is only met if the event occurs AND there is an actual reliability impact? As opposed to Part B where the threshold for reporting is met when the event occurs and there is a potential for reliability impact? This could be broad for event ‘risk to BES equipment’. Providing as much clarity as possible on the ‘threshold for reporting’ is beneficial to the industry and will help eliminate confusion with the existing CIP-001 standard regarding ‘potential sabotage’.
Yes
For ease, timeliness, and accuracy of reporting an application with an easy to use interface would be preferred. If the reporting is done via an application, the ability to enter partial data, save and add additional info prior to submission would be helpful. Additionally, an application with drop downs to select from for impact event, NERC function, etc would be helpful. #1 - Is the ‘Compliance Registration ID number’ the same as the NCR number? If this is required, include as separate entry. #2 – is this the date of occurrence or detection?
Yes
Refer to clarification requested in question 10 comments.
Yes
Yes
Yes
Combining EOP-004, CIP-001 and CIP-008’s reporting requirements reduces redundancy and will add clarity to the compliance activities.
Group
SERC OC Standards Review Group

Jim Case, SERC OC Chair
No
The term “impact events” does not draw a clear boundary around those events that are affected by this standard. Since this is not a defined term, nor is intended to be a defined term in the NERC glossary, this standard lacks clarity and is likely to produce significant conflict as an applicable entity attempts to establish procedures to assure compliance. It appears that situational awareness could not be improved with this standard since it is only dealing with events after-the-fact, not within the time frame to allow corrective action by the system operator.
No
We find it interesting that the ERO is listed as an applicable entity. The ERO can’t be an applicable entity because they are the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. NERC seems to be attempting to evade FERC jurisdiction by having a standard that enables it to write new rules that don’t pass through the normal standards development process with ultimate approval by FERC. Attachment 1 is troublesome. The time frames listed are not consistent for similar events. For example, EEAs are either reported within one or 24 hours depending on the nuance. Having multiple entities reporting the same event is troublesome, i.e., why does an RC have to report an EEA if the BA is going to report it? This will lead to conflicting reports for the same event. Attachment 1 seems to be consolidating time frames from other standards into one for reporting. However, we believe this subject is more complex than this table reveals and the table needs more clarification or it should be eliminated and leave the time frames in the other standards. Several of the events require filing a written formal report within one hour. For example, system separation certainly is going to require an “all hands on deck” response to the actual event. We note that the paragraph above the table in attachment 1 indicates that a verbal report would be allowed in certain circumstances, but this is the same issue with the formal report in that the system operators are concerned with the event and not the reporting requirements. There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
No
The ERO cannot be subject to a requirement for which it is the compliance enforcement authority. The governance in this situation appears incomplete.
No
This is an overly prescriptive requirement that dictates details of documentation and, as such, has no place in a reliability standard. NERC needs to trust the RCs to do their jobs; this standard and this requirement in particular seems to be attempting to codify the actions that an RC would take in response to an event. The cost and burden of becoming auditably compliant with this requirement is extreme and unrealistic, especially on small entities
No
We think “impact event” needs to be defined in the NERC Glossary to provide the clarity the industry needs to build auditably compliant procedures.
No
We think this requirement is unclear – we think it requires a drill for “reporting”, which seems absurd! We recommend the elimination of this requirement.
No
While we support training on an annual basis for the operating plan, the concept of requiring training on reporting of after-the-fact events does not support or enhance bulk electric system reliability. We recommend the elimination of this requirement.
No
There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
No
The ERO cannot be subject to a requirement for which it is the compliance enforcement authority. The governance in this situation appears incomplete.
No
Will all reporting requirements be removed from other standards to avoid duplication? And will all future standard revisions include revisions to this standard to incorporate associated reporting requirements? There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
No
There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
Yes
We do feel that this needs to be a defined term
No

Yes
Yes
We find it disturbing that NERC is headed down a path of codifying requirements that are redundant to existing DOE requirements. How does redundancy in reporting requirements improve or enhance bulk electric system reliability? Disclaimer: “The comments expressed herein represent a consensus of the views of the above named members of the SERC OC Standards Review group only and should not be construed as the position of SERC Reliability Corporation, its board or its officers.”
Group
PacifiCorp
Sandra Shaffer
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Group
Luminant Energy
Brad Jones
Yes
No
Inclusion of both GO and GOP will result in duplicate reporting as both are responsible for reporting resource-related events such as Generation Loss, Fuel Supply Emergencies and Loss of Off-site power (grid supply). Recommend including only the GOP as it is critical that the GOP gather and communicate relevant information to the Reliability Coordinator.
Yes

Yes
Yes
No
We support the requirements outlined in R2 which create significant obligations to maintain and update the required Operating Plan. However, we believe annual drilling for a reporting process seems unnecessary, particularly given the response horizon of 24 hours for the majority of impact events. If drilling is required, the standard should allow actual events to fulfill a drilling requirement as stated in the Rationale for R4 and within the text of M4.
No
Operating Plan revisions communicated through procedure updates and employee acknowledgements of the same are sufficient when coupled with a procedural training program that occurs according to a programmed schedule.
Yes
Yes
Continually refining the Impact Event table to better define which events should be reported would be extremely valuable. Section 802 does not adequately require such refinement, thus R7 and R8 are appropriate inclusions to this standard.
No
The Impact Events Table might be easier to clarify if organized by Reporting Entity rather than Event Type as events vary substantially based on the affected BES component. For example, a GO or GOP cannot adequately determine if an event will significantly affect the reliability margin of the system or if an event results in an IROL. Examples specific to Reporting Entities would assist in more appropriate report submissions. Additionally, the footnote under examples of Damage or Destruction of BES Equipment, cites “A critical asset”. This term must be clarified to indicate whether this refers to a Critical Asset as defined by CIP 002-1. Finally, the Fuel Supply Emergency item requires additional definitions as neither a GO nor a GOP can reasonably project if an individual fuel supply chain problem will result in the need for emergency actions by the RC or BA.
Yes
No
The term “Impact Event” does not adequately replace the term “Sabotage” The Impact Events table seems to provide the definition of the term “Impact Event”. This table does not include sufficient definition for actual sabotage events. Additionally, it does not include any provision for suspected sabotage events. Assuming the Damage or Destruction of BES Equipment event type is intended to cover actual sabotage, the Threshold for Reporting column should include specific levels of materiality that are specific to Functional Entity. For instance, a GO and GOP could have a MW level to define materiality as a GO or GOP cannot assess impact to an IROL or system reliability margin due to equipment damage. A threshold value consistent with “Generation Loss” in the proposed EOP-004 Attachment 1 would be appropriate.
No
CIP-001-1 R3.1 includes instructions associated with the DOE OE-417 form. EOP-004-2 R2.6 should include the DOE as an example of an external organization requiring notification. Additionally, the Rationale for R1 discusses the possibility of one electronic form satisfying US entities with related disturbance reporting requirements but does not include any information about the likelihood of this outcome. Please elaborate on the process required to combine these reports.
Yes
No
Individual
Greg Froehling
Green Country Energy
Yes
Yes
Yes

No
Highly administrative version of what could accomplish the same thing. A requirement that the applicable entitiy shall make appropriate notificatiions as required by attachment A and B events. I can see the need for review and lessons learned but that needs to be done at a higher level since many entities may be involved in an "event"
No
Actually yes and no... An event may be caused, analyzed and corrected by one entity but most likely it will involve more. Low Voltage or frequency may not be caused by a generator but the generator will see the event and to have the generator assess the probable cause seems inappropriate. I can see reporting the event and duration and making notifications.
No
Another training requirement with what benefit? We must train on all of our NERC requirements now anyway to insure compliance and that's not a requirement, thats implied and I think thats enough.
Same as my comment for question 6
Yes
Now this is an excellent example of all that is needed for this requirement!
Yes
I realize this is another burden for the ERO but the information would be good to know what is going on outside the plant .
Yes
Yes
No
Yes and no ... Yes impact events is an adequit term however since it is restrained by the tables it may be helpful to define the term and scope of the term to be more inclusive of sabotage events.
Yes
With the provision that definition and scope of "impact event" are developed and tables adjusted as needed to address FERCs concerns specifically . "(1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."
Yes
Yes
I think the drafting team has done a wonderful job of beginning the task of combining two related standards. I ask them to keep in mind the small generators, and others who do not have the wide view capability, that more than likely react to events that occur wih no knowledge of why they occured, and limited staff to address administrative standard requirements. Many times the KISS approach is the best approach.
Individual
TransAlta Centralia Generation, LLC
TransAlta Corporation
Yes
Yes
Electrical Reliability Organization (ERO) does not appear to be a defined term in the NERC Glossary of Terms on the NERC website. Last updated April 20, 2010.
Yes
Yes
No
Clarity required Does an entity have to report on the cause of every “applicable” impact event they witness even though the event did not originate at their plant, system or region and did not adversely affect them? Essentially this would require every entity that witnessed an “applicable” event to report on its cause. In most cases they will not know the cause if they did not create the event. Measure M3 should reference Attachment 1 to indicate the Time to Submit Report’.
Yes

No
Measure M5 states applicable entities shall provide training material presented… This measure is unclear as to whether the meaning is for internal personnel or to be provided to external entities upon request? Please clarify.
No
R6 should reference Attachment 2 to make it clear that this report form must be used. M6 seems to be requesting evidence that the Confidential Impact Event Report was submitted. TransAlta suggests the submission of the actual report is evidence the report was submitted. Records of this submission can be provided on request. Web Reports Project 2009-01 has indicated online reporting is the direction they are going. If the impact report becomes an online Web report the entity submitting the report has no way of confirming the report ended up at the Compliance Enforcement Authority office after it is submitted. There needs to be some method that demonstrates the report was submitted and received.
Yes
Yes
No
We recommend the 'time to Submit Report' to start when the event is recognized verses when it occurred.
Yes
Yes
Yes
Yes
A Confidential Impact Event Report form is included in attachment 2 but nowhere in the standard does it say to use this form. This form appears to be similar to the "Preliminary Disturbance Report" form used in EOP-004-1. Clarity is required.
Individual
Doug Smeall
ATCO Electric Ltd.
Yes
Yes
Yes
Yes
Yes
Yes
No
R5.3 requires an entity to conduct training within 30 days of a revision to the Operating Plan. For an entity that covers a wide area, 30 days may not be sufficient to reach all employees.
Yes
Yes
No
Attachment 1: Part A - Transmission Loss: Only sustained outages should be reportable. Also the reporting threshold needs to be quantified for impact events, for example: a) Size of DC converter Station > 200 MW. b) Impact of loss of Multiples BES transmission elements in terms of significant load (> 200 MW for > 15 min).
No
Attachment 2 Item 4 implies that an entity is required to analyse and report on an impact event that occurred outside its

system. This is not practical as the entity will not have access to the necessary information.
Yes
Yes
Yes
No
Individual
Dan Roethemeyer
Dynegy Inc.
Yes
Statement is broad enough to cover both Standards.
Yes
Yes
No
For 2.7, 2.8, 2.9, 30 days is to stringent. Some changes may not warrant changes until a cumulative amount of changes occur. Suggest making it no later than an annual review.
Yes
No
What is the basis for the drill being annual. This is to stringent. I suggest it be every 3 years.
No
The annual training seems excessive especially if their have been no changes. You have included one exception for contact information revisions; however, it should be expanded to include exceptions for minor/non-substantial changes. Also, make training requirements (after initial training)be required for substantive changes only.
Yes
Yes
No
A 2000 MW loss needs to be more clearly defined by either the BA, ISO, RC, etc. for the applicable enity. Also, what is the distinction between the "damage or destruction of BES equipment" and the generation loss of >= 2000 MWs if it is a Critical Asset which is currently drafted as those greater than 1500 MW in current draft of CIP-002-4. This could lead to 2 events with different thresholds (i.e. 1500 MW and 2000 MWs). Possibly get rid of the 2000MW criteria and let the threshhold level be the same as the Critical Asset MW level. Or remove the Critical Asset threshhold in the footnote to Attachment 1.
Yes
No
The term is fine but FERC wants more specific examples. GO/GOP can't determine the effect on the BES.
Yes
Yes
Yes
This does not address the inability of a GO/GOP to determine effects on the BES. Surrounding BES knowledge is limited for a GO/GOP.
Group
City of Garland
David Grubbs
Yes

Yes
No
Reason 1 Most of this is duplication of existing processes - More “Big Government” and/or “Overhead” is not needed. There are already processes in place to notify “real time” 24 X 7 organizations that take action (RC, BA, TOP, DOE, FBI, Local Law Enforcement, etc) in response to an “impact event”. It is stated in your document on page five (5) “The proposed standard deals exclusively with after-the –fact reporting.” The combining of CIP 001 & EOP 004 should not expand on existing implemented reporting requirements nor should it result in NERC forming a 24 X 7 department to handle 1 hour (near real time) reporting requirements. Reason 2 If this should go forward as drafted, NERC should not establish a “clearing house” for reporting requirements for Registered Entities without also taking legal responsibility for distributing those reports to required entities. It states in at least 2 places (Page 6 & Page 22) in the document that Responsible Entities are ultimately responsible for ensuring that OE-417 is received at the DOE. Thus, a Registered Entity could be penalized for violating this new standard if it did not file the reports with NERC or it could still be penalized (both criminal & civil) if they filed the reports with NERC but NERC (for whatever reason) did not follow through with ensuring the report was properly filed at the DOE.
No
There are 4 “methods” and 2 “provision” required for this requirement – in other words, 6 “paperwork” items that auditors will audit and likely penalize entities for. On page 1, the statement is made “…proposed standard in accordance with Results-Based Criteria.” Having to have 4 methods and 2 provisions to end with a report (all of which is paperwork) is not a “result based” standard. It is like being required to have a "plan to plan on planning on composing and filing a report". Events need to be analyzed, communicated, and reported and should be audited as such (results based) – not audited on whether they have a book filled with methods and provisions.
No
Should be part of R2 or R6 – this is unnecessary duplication
No
Existing CIP 001 and EOP 004 are reporting standards – neither currently requires annual drills or exercises. Combining these two (2) should not entail expanding the requirements to include drills or exercises. There are existing drills / exercises that must be performed annually for compliance with CIP 008 & CIP 009 which require the same basic identifying, assessing, developing lessons learned, responding, and reporting skill sets. Requiring additional drills or exercises for this new combined standard will provide additional “business overhead” that results in basically nothing that is not obtained by the CIP 008 / 009 drills as far as securing or making the BES reliable. It does, however, result in additional audit risk at audit time.
No
This expands beyond the original CIP 001 and EOP 004 – neither explicitly requires training – combining does not mean expanding. In reality, what practical skill are you going to train on? People who perform the analysis on an event are going to have job specific training external to this standard and those same folks will maintain their skill set external to this standard. If it is going to be a results based criteria standard, then let the entities be responsible. Training on methods to fill out and file paper work does not make the BES more reliable. The vast majority of other standards do not have a training requirement section and yet, entities manage to be compliant with those standards. Compared to all the other reliability standards and their requirements, are penalties for training on filling out paper work really making the BES more secure and reliable?
No
1. The reporting requirements should not be expanded beyond CIP 001 and EOP 004-1. The goal for combining the two should be to make the process more efficient – not add on extra requirements for procedures on how to report, drills on reporting, training on reporting, etc. 2. The timelines requiring 1 hour reporting to the ERO are not needed and provide little realtime benefit to the BES. Real time or near real time reporting for “people on the ground” such as the RC, BA, TOP, FBI, Local Law Enforcement, DOE, etc. is necessary. They are in a position to take action in response to an event. On page 5, it states “The proposed standard deals exclusively with after-the-fact reporting. 1 Hour reporting requirements to the ERO in addition to existing reporting are not reasonable “after-the-fact” reporting requirements in the midst of an emergency. Also, there is not a 24X7 ERO center to report events to – why build and staff one when they already exists at the RC, BA, TOP, DOE, FBI, Local Law Enforcement, etc. – An ERO 24X7 center would be extra overhead that would provide no additional benefit in the first hour or hours of an emergency.
Yes
R7 – Yes as long as any changes to attachment 1 follow the “Reliability Standards Development Procedure. R8 - Yes as long as R8.6 is strictly “recommended actions.” They should not become “required actions” as this bypasses the standard development process.
No
This report should follow exactly the OE-417 to avoid redundant, possible conflicting, and overall confusion in reporting. Note: The table has entries that are in conflict with the OE-417 and thus can cause confusion in filing multiple reports potentially causing an entity to violate Federal Law due to the confusion. By submiting the same information on

different timelines, i.e. one hour reporting under OE-417 and 24 hours under this Standard, the reports may be significantly different causing confusion from differing reports of the same event. Although we prfer the events to match the OE-417 events exactly, if the SDT decides to include a seperate events table we make the following suggestions: Energy Emergency requiring system-wide voltage reduction: should be reportable at 5% not 3% voltage reduction. The standard should clearly state this was applicable for BES energy emergency conditions only, not voltage reductions for other reasons. On voltage deviations: it should be clear that this applies to widespread effects on the BES not a single distribution feeder that has a low voltage. For the Frequency deviation: Did not see a definition for the FTL (frequency trigger limit) Generation loss: the reportable loss of generation should be significantly more than 500 MW. The number of units at the locaton is irrelevent. Ten units at 50 MW each is no more critical than a single 500 MW unit. Under this standard, if the plant with ten 50 MW units trips it is reportable but an 800 MW single unit is not reportable. The trip of the 800 MW unit has much more effect on the sytem reliability. Damage or destruction of BES equipment: Should be limited to specific equipment such as a 765 kV autotransformer not a 138 kV lightning arrestor. This needs to be eliminated or significantly limited as to the equipment type that is reportable.
No
The report filed should be the OE-417 ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT and should be filed only on OE-417 reportable incidents. If this report is implemented as drafted, companies with multiple registration numbers and functions should only have to file one report for all functions and registrations.
No
1 In keeping with a Results Based Standard, the impact event should be a trigger for filing a report. At the time of the event, one may not know if the event was caused by sabotage. Sabotage that does not affect the BES should not be a reportable event. 2. To comply with the Commissoners request to define sabotage, Impact Event does not adequately replace “sabotage”. If someone reports sabotage, people universally have a concept that someone(s) have taken some type of action to purposely harm, disable, cripple, etc something. Impact Event does not convey that same concept. 3. If Sabotage is left as a “trigger,” it should not include minor acts of vandalism but only acts that impact reliability of the BES
No
EOP-004-1 R2 did not get translated to EOP-004-2 R2 - table states it is mapped to R1
No
Do not agree with this proposed draft - instead of combining 2 standards to gain efficiency, this expands the standard with unnecessary paperwork, drills, training, etc.
Yes
Do not agree with this proposed draft - instead of combining 2 standards to gain efficiency, this expands the standard with unnecessary paperwork, drills, training, etc. For reports required under this standard, companies with multiple registration numbers and functions should only have to file one report for all functions and registrations.
Individual
Kasia Mihalchuk
Manitoba Hydro
No
Though new purpose greatly clarifies the proposed EOP-004-2 and using “situational awareness” is the key to this purpose, further clarification of specific items should be added to the purpose. “Responsible Entities shall report SIGNIFICANT events to support interconnection situational awareness on events that impact the integrity of the Bulk Electric System, such as islanding, generation, transmission and load losses, load shedding, operation errors, IROL/SOL violations, sustained voltage excursions, equipment and protection failures and on suspected or acts of sabotage.”
No
Since this Standard is to support situational awareness, more entities should be included such as Load Serving Entities (which was removed from EOP-004-1).
Yes
Yes, keeping R1 generic and pointing to “government”, “Provincial”, “law” encompasses all entities in all major interconnections.
Yes
R2 – 2.1 to 2.9 detail what is expected of an Operating Plan for Impact Events. The attachment 1 details the event, the threshold parameters and time line. Though the threshold parameters in the attachment may be questioned, this greatly clarifies the expectations of reporting events. Further events should be added to this list: “Detection of suspected or actual or acts or threats of physical sabotage”
No
Though each local entity should identify and assess initial probable cause of impact events as per their Operating Plan, the creation of this Operating Plan could be labor intensive and also guidelines for consistency within an RC region should be created. So “NO” is entered simply because a large time line would be needed to properly and efficiently implement R3 and R4.

No
Drills and exercise for implementation of the Operating Plan are important and critical, but as in question 5, or Requirement R3, careful and detailed creation of the Operating Plan are crucial to facilitate proper training, drills and exercises. So “NO” is entered simply because a large time line would be needed to properly and efficiently implement R4 and R3.
No
The comments in Question 6 and 7 encompass the training aspect of this requirement.
Yes
Attachment 1 details the impact events and the thresholds of which they should be reported.
No
Rules of Procedure appear to have a different focus then R7 and R8. Briefing on Rules of Procedure 802 Assess, review and report on: 1.1 overall electric operation 1.2 uncertainties and risks 1.3 self assessment of supply and reliability 1.4 projects on customer demand 1.5 impact of evolving electric market practices that could affect the present and future of the BES Briefing on R7 and R8 R7 – ERO shall review and propose revisions to Attachment 1 R8- ERO shall publish quarterly reports on trends, threats, vulnerabilities, lessons learned and recommended actions.
Yes
Though R7 indicated Attachment 1 will be reviewed and revised reguarily the immediate addition of: “Detection of suspected or actual or acts or threats of physical sabotage” should be added.
No
Though a “Confidential Impact Event Report” is much needed the Attachment 2 needs refinement. Provide an explanation for each “task”. Isolate and simplify the “Who, When and What” section. Isolate the description of event. Remove items 7 to 10. Modify Attachment 1, add columns to indicate time of event, quantity, restore time, etc as required. The Attachment 1 can be attached to Attachment 2. This could simply and speed the reporting process.
No
The majority of the items listed in Attachment 1 are typically and historically operating events. Yes these are all “impact events”. Sabotage, cyber and security are typically viewed as separate events. These events are not part of “a typical day of BES operations”. These are outside event and though qualify as “impact events” should still be treated separately.
No
Though CIP-001-1a already contained provisions for sabotage response guidelines, the new EOP-004-2 R2 (2.1 to 2.9) will require reexamination of existing policies to remain compliant. Upon the approval of Attachment 1, the existing disturbance guidelines will also have to be reexamined. With the addition of R3 (Identify and assess), R4 (Drills) and R5 (Training), will also require redevelopment of existing processes.
No
Individual
Philip Savage
PacifiCorp
Yes
Yes
Yes
All efforts need to be made to include OE-417 reporting requirements to safeguard against duplicate reporting and / or delinquent reporting. One report for all events is more preferable than multiple reports for one event.
Yes
Yes
Yes
No
Training required within 30 days of a revision to the Operating Plan is not feasible with 5 or 6 week shift rotations. A sixty day requirement would be more realistic.
Yes

Yes
No
Energy Emergency requiring firm load shedding - An SPS/RAS could operate shedding firm load but no Energy Emergency may exist. This requires clarification. Transmission Loss - Multiple BES transmission elements. Loss of two transmission lines in the same corridor due to a wildfire could qualify for this reporting. Once again clarification needed.
No
As previously mentioned all effort should be made to ensure duplicate reporting is not required. OE-417 requirements should be covered by this one form.
Yes
Yes
Yes
Yes
This is yet another standard with training requirements not covered under any PER standards. Having different training requirements spread throughout the standards makes it increasingly difficult to ensure all training requirements are met. Developing a "Training Standard" that lists ALL required training would streamline the process and aid greatly in compliance monitoring.
Individual
Brian Reich
Idaho Power Company
Yes
Yes
Yes
the SDT must ensure that only a single form is required for compliance (such example OE-417)
No
The SDT needs to clarify Requirement 2.9 references an annual report issued persuant to requirement R8, however Requirement 8 references a quarterly report. These requirements should have the same time frames.
Yes
Yes
No
The 30 day Requirement is limited with real time operations. Most entities with real time operations utilize a 5 or 6 week rotating schedule to comply with PER-002. the NERC Continuing Education Program allows up to 60 days to comply, this allows the operating shifts to accomadate training within the operating schedule. The requirement 5.3 should allow 60 days to complete the training.
Yes
Yes
Yes
No
there should only be on report, utilized OE-417
Yes
Yes
Yes

Yes
By including training requirements in each standard, creates confusion and compliance or failure to comply potentian. PER standards are in place for personel training, these standards should be utilized for adding requirements that require training for NERC Standards.
Individual
Chris Hajovsky
RRI Energy, Inc.
No
The purpose does not need to mention "and the reliability of the Bulk Electric System." This is the Congressional mandate in FPA Section 215, and could be attached to every Standard, guide, notice and direction issued by FERC, NERC and Regional Entities. In addition, the purpose references "Responsible Entities." However, section 4 on "Applicability" references "Functional Entities." These terms should be consistent. Therefore, the purpose statement of the proposed standard should be corrected to read, "Functional Entities identified in Section 4 shall report impact events and their known causes to support situational awareness." CONSIDERATION: Is the phrase "shall report impact events and their known causes" really a purpose of the Proposed Standard, or is it instead merely a means to achieve the purpose of situational awareness? If the latter, the purpose statement can be further shortened to read, "Functional Entities identified in Section 4 shall support situational awareness of impact events and their known causes."
No
Agree with the "Applicability" section functional categories. Agree with the Attachment 1 lists of "Entity with Reporting Responsibility," with the following exceptions: PART A "Damage or Destruction of BES Equipment" - This item has a footnote 1 listed, but nothing at the bottom of the page for a footnote. Assuming the footnote reference is intended to reference the "Examples" at the bottom of the page, the following concerns exist: (i) "critical asset" - Is this term intended to reference a "Critical Asset" identified pursuant to the CIP-002 risk-based assessment methodology? If so, it should be capitalized. If not, who determines what constitutes a lower case "critical asset"? (ii) "Significantly affects the reliability margin of the system…" - If this is intended to be enforceable, several words need significant clarification and definition, such as "Significantly," "reliability margin," "system" (BES?), "potential," and "emergency action." The combined ambiguity of just two of those phrases would most likely result in a court holding this statement as so vague as to be unenforceable. The combined lack of clarity of all the highlighted words or phrases render this sentence meaningless. (iii) "Damaged or destroyed due to a non-environmental external cause" - "Non-environmental external cause" should be a defined term because, as is the case in item (ii) above, it is vague and subject to broad, random or arbitrary interpretation. Part B provides examples of "non-environmental physical threat" for "Risk to BES equipment." Those examples could be referenced here, or different examples included that are more applicable to the Event. The items highlighted in items (ii) and (iii) above are very similar to the unintended string of CIP-001 violations that Registered Entities experienced in 2007 and 2008 for failing to provide their own definition of "sabotage" under a sabotage reporting standard that failed to provide any guidance to the industry within the standard as to what constituted "sabotage." PART B "Detection of a cyber intrusion to critical cyber assets" - Capitalize "Critical Cyber Asset."
Yes
While including the phrase "to enhance and support situational awareness" is a good use of the Results-Based Standards development tools and framework, the phrase is already included in the purpose statement. As such, it is unnecessary in Requirement 1. If it were to be included in Requirement 1, then it would also need to be included in each of the other Requirements 2 through 8. The "Purpose" statement captures this aptly.
No
1. R2 includes the phrase "for identifying, assessing and reporting," followed by R2.1 which states "identifying," R2.2 which states "assessing" and both R2.3 and R2.6 state "notify" or "making internal and external notifications" (i.e., reporting). The language is unnecessarily redundant. RECOMMENDATION: Reword R2 phrase "for identifying, assessing and reporting," to simply state, "for addressing." 2. Rationale for R2 - The rationale section for R2 references in the third paragraph "Parts 3.3 and 3.4." Was this intended to reference R2.3 and R2.4?
No
"Identify and assess" - Auditors are as much in need of clearly worded, unambiguous Reliability Standards are as Registered Entities. This phrase leaves much too wide a range of interpretations, almost guaranteeing regular and frequent disagreements during an audit between Registered Entity and Regional Entity auditor as to what constitutes "identify and assess" sufficient to meet the intent of this Requirement. Compounding this issue is the Rationale for R3 that states an Applicable Entity (which should probably read "applicable Functional Entity") should "gather enough information to complete the report that is required to be filed." While Rationale statements are not technically part of the standard, this emphasizes the current wording of the requirement as subject to random and arbitrary interpretation by auditors and Registered Entities. RECOMMENDATION: Change "identify and assess" to "document," so that the Requirement now reads "Each Applicable Entity shall document initial probable cause of impact events…" including an option for "cause not determined".
No
Every employee in a Registered Entity might potentially have exposure to an impact event, and therefore result in a list

of thousands of employees subject to the EOP-004-2 Operating Plan. Does this mean, for example, an applicable Functional Entity with 3,000 employees, each capable of potentially observing an impact event, must include them in the drill, exercise, or Real-Time implementation? Such an expectation would require a hypothetical email notice to be sent to 3,000 employees, advising them "This is a test - You observe a suspicious vehicle driving around the fence of your power plant. Perform the next action you should take." The result in this hypothetical might be 3,000 phone calls and emails to the responsible employee in the applicable Functional Entity, each needing to be documented and retained for the audit period. As stated above in question 5, auditors need guidance as much as Registered Entities. Otherwise, it is observed that they will seek the most stringent approach they observe from the best of the best practices over the first year of implementation and apply that expectation as the base-case, under which all other approaches will be deemed violations.
No
1. This Requirement is structured to result in the same heavy-handed, zero-tolerance approach that has made CIP-004 one of the top three violated Reliability Standards. The failure in CIP-004 is that, for example, a seven-year background check or annual training program that is tardy by one day results in a violation. There is no margin of error, proviso, or cure scenario. Likewise, the proposed R5 in EOP-004-2 makes it a violation if someone takes their newly established training on the day after the end of 15 months. Systems configurations are often based on quarterly monitoring for individuals needing to take training. In addition, when dealing with potentially thousands of employees, it is inevitable that any one of hundreds of reasons might result in an employee not being included in the tracking system, and rolling past the 15th month. RECOMMENDATION: To avoid further burden to Regional Entity audit and enforcement personnel as has been the case in CIP-004, develop a cure process that allows the Registered Entity to correct the training or background check tardiness with prompt correction, fill out a notification report to submit to NERC, and proceed with protecting the reliable operation of the BES, rather than tying up Registered Entity and Regional Entity staffs with data requests, enforcement paperwork and administrative actions. 2. The proposed R5.3 requires the entire applicable staff to redo the entire training within 30 days of a change to the Operating Plan. These Operating Plans will not be short documents, and formal training will not involve a 5 minute soundbite. However, for such a significant procedure as the Operating Plan, frequent changes and revisions are going to be very common, especially given the likelihood of frequent clarifications, Compliance Action Notices ("CANs"), and lessons learned issued by NERC and Regional Entities over this very detailed set of new obligations. It is not unreasonable to expect a Registered Entity to make three or more revisions to their Operating Plan in a year, which would require training for thousands of employees three times a year, for what might amount to a single sentence revision. Furthermore, the obligation to retrain on the entire training program is not limited in this requirement to only those individuals impacted by the revision. Where a change or revision only impacts 3 possible employees, this standard would require a company with 1,500 employees subject to the Operating Plan to retake the entire training. RECOMMENDATION: Clarify that upon changes to the Operating Plan, the Registered Entity may either require full training, or instead distribute a summary of the change(s) via email to affected personnel only.
No
RECOMMENDATION: Clarify that the reporting of impact events shall be to those entities identified in the Operation Plan section developed specifically in Section 2.6. Reference to Attachment 1 indicates reporting to "external" parties is the intent for R6.
Yes
We support the concept that Reliability Standard requirements and obligations that are subject to violations and penalties should all be contained in the four-corners of the Reliability Standard. If an obligation exists in the Rules of Procedures that creates a stand-alone responsibility that is subject to violation and penalty, it should be removed from the Rules of Procedure and inserted into the appropriate Reliability Standard.
Yes
Yes
Yes
Agree. However, strongly encourage this to be made into a defined term in the Glossary of Terms.
Yes
Assume reference to EOP-004-3 in the question 13 was meant to reference version 2 (EOP-004-2).
Yes
No
Individual
Bill Keagle
BGE
Yes

Yes
No
R1 With the definition of "Impact Event", are we eliminating the term "Disturbance Reporting"? If we eliminate disturbance reporting, SDT should remove the reference from the Summary of Concepts and from the title, otherwise further definition on the distinction between the two terms is needed. R1. What is the "system" described here? What type of system is anticipated – electronic, programmatic or can it be better described by using “standard reporting form”? M1. Needs to seek evidence that the "system" was used for receiving reports, as well as distributing them. M1. Examples are more appropriately used in guidance documentation than in the standard. Rationale for R1 – Final statement regarding OE-417 needs to be removed. The ERO will establish the requirement in their “system” if the standard remains as is. The Requirement does not require the responsible entities to send OE-417 to DOE.
No
R2.1 Creates the opportunity for differences in identifying impact events. BGE recommends additional clarity in the statement. Are we to use Attachment 1 as a “bright line” or can we use our Operating Plan to identify what an impact event is? R2.4 - 2.6 Does a standard need to specify both internal and external lists? 2.7 – is “component” defined anywhere? Is it a component of the BES or a component of the Operating Plan or a component of the three lists in 2.4 to 2.6? Rationale --- Parts 3.3 and 3.4?? Do you mean 2.3 and 2.4? Is the Operating Plan under scrutiny (mandatory and compensable) for all items in the last paragraph of the rationale?
No
R3. Limits responsibility to Attachment 1 events only and mandates that an “initial probable cause” be identified. Are we at liberty to define “initial probable cause” and define time period for completion in the Operating Plan? BGE believes this could cause wide difference between Operating Plans and the standard should be more prescriptive by relating to a time-table for the life of an impact event, including expected identification time, initial assessment time and analysis time leading to the reporting deadlines. BGE recommends not including examples of evidence in a measure but include it in a Guideline. Including in a measure will be translated as a requirement by an auditor.
No
M4. BGE recommends not including examples of evidence in a measure but include it in a Guideline. Including in a measure will be translated as a requirement by an auditor. Rationale for R4: If multiple exercises are performed are all of them subject to the sub-R2 requirements and to audit/audit findings?
No
Suggested revision to clarify R5: Each Applicable Entity shall provide training to all internal personnel identified in its Operating Plan on the Operating Plan annually. Training is only on Reporting, pursuant to R2, not on the Operating Plan? BGE does not believe the SDT needs to identify sub bullets on this requirement. R5.1 is not logical --- what does it mean?
Yes
Comments for clarification: R6. Use of Capital letters in Operating Plan makes it unnecessary to state "created pursuant to Requirement 2
No
R7. Make Impact Event Table all Capital Letters(it is a title). R8. Is the term "reportable impact events" new or is impact event intended to be capitalized? R8. Does a quarterly report of the year’s reportable impact events include 12 months of "reportable impact events"? This is confusing. R8. In the Rationale for R8 Impact Events appears with Capital letters - why now? Shouldn’t it appear with all Capital letters throughout the document as it is a defined term? R8. There are no previous requirements to report threats (R8.3) or lessons learned (R8.5) or trends (R8.2) to an ERO. Is this information from reports to the ERO or from ERO research?
No
TOP determines "system-wide" voltage reductions; why place this responsibility on a TO or DP? - Load Shedding is automatic load shedding; why 100MW? Does a DP need to provide a Report when directed by the RC, BA or TOP to shed load or reduce voltage? - No examples should be included in the standard! Need to define a "BES Transmission Element". - Table shows multiple entities in "Entity with Reporting Responsibility"; is it one or is it all entities report? - In an audit who determines "reasonably determined likely motivation" - Is it justified to expect to have "motivation" knowledge within one hour of an event? - Why are the Responsible Entities reporting Interruptible Demand tripped / lost?
No
There is considerable difference between this form and OE-417 necessitating that two forms be completed. BGE believes that the purpose of combining the standards was to reduce the number of reporting entities and number of reports to be generated by each entity. BGE believes this fails to accomplish this purpose.
Yes
The defined term “impact events” should be capitalized throughout the document to identify it as a defined term. Additionally, BGE has noted in several comments that another term is used instead of “impact events”. These terms

should be eliminated and use “impact events” instead.
Yes
None.
Yes
None.
Yes
One item that is properly addressed is the removal of Load Serving Entity from the Applicable Functional Entities. There may be a need to provide some guidance to Functional Entities when there are separate Transmission Owners and Transmission Operators or Generation Owners and Generation Operators. If they are separate, there may be redundancy in reporting. From the documentation, it doesn’t seem like the SDT are combining all reports into one form as we would like to see. In the rational for R1 section, it talks of getting both forms (NERC and OE-417) together in one document (however it sounds like the forms within the document are still separate), available electronically, which only seems like a step forward. However, it does not take away the confusing process for the operators of which part of the form would need to be filled, who should be set this form depending on what part is filled, if one part of the form is filled out do the other parts need to be filled, etc. If the forms cannot be consolidated, BGE would rather the forms be separate to reduce confusion. BGE believes all these reports should require one form with one set of recipients, period. This may mean that NERC needs to get DOE to modify their OE-417 form.
Individual
John Brockhan
CenterPoint Energy
No
CenterPoint Energy does not agree with the purpose statement of the proposed standard. The directive from the Commission in FERC Order 693 and restated in the Guideline and Technical Basis is “…the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: 1) further define sabotage and provide guidance as to the triggering events that would cause and entity to report a sabotage event.” Instead the SDT has introduced another term, impact event, to address concerns regarding different definitions. The term, impact event and its proposed concept is too broad. Specifically the concept that an impact event “…has the potential to impact the reliability of the Bulk Electric System” leaves too much room for an entity and a regulatory body to have a difference of opinion as to whether an event should be reported. Required reporting should be limited to actual events. The reporting to follow could become overwhelming for the Responsible Entities, the ERO, and other various organization and agencies. Furthermore, situational awareness is a term that is associated with aspects of real-time. Given the analysis required before a report can be submitted, the report will not be real-time and will not sustain a purpose of supporting situational awareness. (See also comments on Q10 regarding the “Time to Submit Report”.) A purpose that is more aligned with consolidation of the EOP-004 and CIP-001 standards would be as follows: Responsible Entities shall report disturbance events and acts of sabotage to support the reliability of the BES through industry awareness.
No
CenterPoint Energy does not agree with the addition of Transmission Owner and Distribution Provider to the Applicability section. Transmission Owner and Distribution provider are not currently applicable entities for either CIP-001 or EOP-004 and should not be included in the proposed combined standard. However, CenterPoint Energy does agree that LSE should be removed from the Applicability section. CenterPoint Energy appreciates the SDT’s efforts in assigning entities to each event in Attachment 1. This is an improvement over the existing EOP-004 standard. It is clear, however, that with multiple entities responsible for reporting each event, there is no need to expand the Applicability Section to include Transmission Owner and Distribution Provider.
No
The ERO does not need to establish a “system for receiving reports” as the “system for receiving reports” is inherent given the requirements for reporting. The requirement also seems to add redundancy versus eliminating redundancy in the distribution of reports to applicable government, provincial or law enforcement agencies on matters already reported by Responsible Entities. If an event is suspected to be an intentional criminal act, i.e. “sabotage”, the Responsible Entity would have contacted appropriate provincial or law enforcement agencies. The ERO is not in a position to add meaningful value to these reports as any information the ERO may provide is second hand. CenterPoint Energy recommends R1 and M1 be deleted.
No
CenterPoint Energy does not agree with R2 and M2 as they are focused on process and procedure. Compliance with a reporting requirement should be based on a complete and accurate report submitted in a timely manner. The process an entity uses to accomplish that task is of no consequence. CenterPoint Energy recommends R2 and M2 be deleted. However, if the SDT feels it is necessary to include this process based requirement, CenterPoint Energy believes the SDT, in requiring an overly prescriptive Operating Plan, has expanded the requirement beyond the current CIP-001-1 and EOP-004-1 which only require “…procedures for the recognition of and for making operating personnel aware…” (CIP-001-1) and “…shall promptly analyze…” (EOP-004-1). Specifically, R2.2 is not found in the current Standards. “Methods for assessing causes(s) of impact events” would vary greatly depending upon the type and severity of the

event. Responsible Entities would have a difficult time cataloging these various methods to any specific degree and if they are not specific then CenterPoint Energy questions their value in a documented method. R2.3 is not found in the current Standards and is an unnecessary requirement as the method of notification is irrelevant so long as the notification is made. R2.7, R2.8, and R2.9 are also unnecessary expansions beyond what is currently in CIP-001-1 and EOP-004-1. CIP-001-1 requires the Responsible Entity review its procedures annually and CenterPoint Energy believes this is sufficient. When taken in total, R2 requires seven (7) different processes, provisions, and methods. CenterPoint Energy recommends R2.2, R2.3, R2.7, R2.8 and R2.9 be deleted and believes this will not result in a reliability gap.

No

CenterPoint Energy does not agree with R3 and M3 as written as the Company does not agree with the requirement to have an Operating Plan (see comments to Q4 above). However, if R2 and M2 were to be deleted, and R3 was revised to read; “Each Applicable Entity shall identify and assess initial probable cause of events listed in Attachment 1.”, CenterPoint Energy could agree with this requirement.

No

CenterPoint Energy does not agree with R4 and M4. See comments to Q4 above. In addition to the process vs. results based issue stated above, CenterPoint Energy believes conducting a drill to verify recognition, analysis, and reporting procedures is a waste of valuable resources and time.

No

CenterPoint Energy believes that R5 and M5 are not necessary and should be deleted. CenterPoint Energy supports an entity training its staff in any reporting responsibilities; however, such training should be the responsibility of each entity and such requirements do not belong in a NERC standard. In addition, CenterPoint Energy believes any necessary training requirements are covered in the PER Standards and therefore the addition of this requirement adds redundancy to the Standards. If a majority of the industry supports such a requirement, CenterPoint Energy cannot support R5 and M5 as written as we do not agree with the requirement to develop and maintain an Operating Plan (see comments to Q4 above). CenterPoint Energy offers the following alternate language: “Each Applicable Entity shall provide training concerning reporting requirements contained in this Standard to internal personnel involved in the recognition or analysis of events listed in Attachment 1.

No

CenterPoint Energy does not agree with R6 and M6 as written as we do not agree with the requirement to develop and maintain an Operating Plan (see comments to Q4 above) In addition CenterPoint Energy does not agree with the timelines required in Attachment 1 (see comments on Q10). CenterPoint Energy offers the following alternate language: “Each Applicable Entity shall report events outlined in Attachment 1 to applicable entities including but not limited to; NERC, and appropriate law enforcement agencies."

No

CenterPoint Energy does not believe this requirement is necessary; however, if the SDT insists on keeping this requirement then CenterPoint Energy believes it should remain as written. Any change to Attachment 1 should go through the Reliability Standards Development Procedure.

No

CenterPoint Energy appreciates the efforts of the SDT in identifying the entity with reporting responsibility. This is an improvement to the event table. CenterPoint Energy is concerned with multiple entities being listed as having Reporting Responsibility. CenterPoint Energy recommends the SDT limit this to one entity having responsibility for reporting each event. This would not preclude that entity from coordinating with other entities to gather data necessary to complete the report. In addition, CenterPoint Energy believes there are several events that should be removed from the list. “Transmission Loss” is covered by the TPL standards and does not need to be identified or reported under EOP-004. The loss of a DC converter station or multiple BES transmission elements may or may not disrupt the reliable operation of the BES, i.e. result in blackout, cascading outages, or voltage collapse. Likewise “Damage or destruction of BES equipment” in and of itself should not be the subject of reporting. If the damage or destruction results in true disruption to the reliable operation of the BES, that impact would be reported under one of the other identified events. “Voltage Deviations” is another unnecessary event. CenterPoint Energy believes a voltage event of the proposed magnitude will, more than likely, result in other events identified in Attachment 1 such as; IROL Violation or Generation Loss and would be reported under one of those triggers. Another concern is the threshold trigger of +/- 10% for 15 minutes or more. CenterPoint Energy is unclear as to the starting point to determine the deviation. In other words is the 10% deviation from nominal voltage, such as 138kV or 345kV, or the actual voltage at the time of the event? Additionally, must the deviation occur over a “wide area” or is such a deviation at one buss enough to trigger a report? Based upon these ambiguities and concerns CenterPoint Energy recommends “Voltage Deviations” be deleted from Attachment 1. The examples that follow on page 14 should also be deleted.

No

CenterPoint Energy does not agree that the term “impact event” adequately replaces “disturbances” and “sabotage”. CenterPoint Energy suggests that just as the SDT has come to consensus on a concept for impact event, a definition could be derived for sabotage. “Potential”, as used in the SDT’s concept, is a vague term and indicates an occurrence that hasn’t happened. Required reporting should be limited to actual events. CenterPoint Energy offers the following

definition of “sabotage”: “An actual or attempted act that intentionally disrupts the reliable operation of the BES or results in damage to, destruction or misuse of BES facilities that result in large scale customer outages (i.e. 300MW or more).”
Yes
CenterPoint Energy agrees that there is no reliability gap between the existing standards and the proposed standard. However, CenterPoint Energy believes that the SDT went too far in developing the proposed EOP-004-2 and added additional unnecessary requirements. If the comments made above to Q1 – Q12 were to be incorporated into the proposed Standard, CenterPoint Energy believes the product would be closer to a results based Standard with no reliability gap.
Yes
CenterPoint Energy appreciates the efforts of the SDT in removing outdated and unnecessary language from the existing EOP-004 standard. Additionally, CenterPoint Energy urges the SDT to also remove the proposed “how to” prescriptive requirements. CenterPoint Energy believes the SDT team’s focus should be on drafting a results-based standard for reporting actual system disturbances and acts of sabotage that disrupt the reliable operation of the BES. The SDT should not delve into trying to identify a list of events that have a potential reliability impact. As stated in response to Q10, CenterPoint Energy strongly believes that cyber-related events should not be in the scope of this standard since they are already required to be identified and reported to appropriate entities under CIP-008. Excluding cyber events from this standard further supports the elimination of redundancies within the body of standards.
Individual
Joylyn Faust
Consumers Energy
No
R 2.7, R 2.8 and R 2.9 are creating a requirement to have procedures to update procedures. Having updated procedures should be the requirement, no more.
No
NERC should either standardize on a 12 month year or an annual year for reviews.
No
Again, either 12 month year or annual year, NERC needs to standardize on one or the other. Training should apply only to those that must take action relevant the reliability of the BES. A plan would likely include notification of senior officers, however they don’t need to be included in drills and training if they have no active role.
Individual
Doug White
North Carolina Electric Coops
No
The term “impact event” is not a defined term in the NERC glossary and does not draw a clear boundary or give concise guidance to aid in event recognition.
No
There is a conflict between the ERO being listed as an applicable entity and the fact that the ERO is the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that other applicable entities would be required to meet. Attachment 1 has inconsistent time frames listed for similar events. For example, EEA’s are either reported within one or 24 hours depending on the nuance. Also, having more than one entity reporting an EEA can lead to conflicting information for the same event. Attachment 1 has the RC and the BA both reporting the same EEA event. Attachment 1 consolidates time frames from other standards for reporting purposes. There should either be a separate standard for “reporting” that encompasses reporting requirements for all standards or leave the time frames

and reporting requirements in the original individual standards. Several of the events require filing a written formal report within one hour. For large events like cascading outages or system separation, “all hands on deck” attention will need to be given to the actual event. Although a verbal report would be allowed in certain circumstances, attention to the actual event should take precedence over formal reporting requirements. There is already a DOE requirement to report certain events and no need to develop redundant reporting requirements in the NERC arena when this information is already available at the federal level at other agencies.
No
The ERO cannot be subject to a requirement for which it is the compliance enforcement authority.
No
This requirement dictates details of documentation of after-the-fact reporting of events which cannot impact reliability of the BES and, as such, should not be a reliability standard. The cost and burden of becoming auditably compliant with this requirement can be extreme for small entities.
No
The term “impact event” needs to be defined in the NERC Glossary to provide the clarity the industry needs to build auditably compliant procedures and give guidance on what is proper to report.
No
Requiring a drill for “reporting” is unnecessary and burdensome. Reporting is covered in processes and procedures and during the normal training cycle. We recommend the elimination of this requirement.
No
Requiring training to report of after-the-fact events does not improve the reliability of the BES. We recommend the elimination of this requirement.
No
There is already a DOE requirement to report certain events. NERC should not be developing redundant reporting requirements when this information is already available at the federal level from other agencies.
No
The ERO cannot be subject to a requirement for which it is the compliance enforcement authority.
No
This list is too similar and redundant to the DOE requirements and does not provide any additional clarity on recognition of sabotage.
No
There is already a DOE requirement to report certain events. NERC should not be developing redundant reporting requirements when this information is already available at the federal level from other agencies.
Yes
No
Yes
Yes
Keep in mind that redundancy in reporting requirements from the DOE does not improve or enhance bulk electric system reliability but rather creates more work for the reporting entity.
Individual
Lauri Jones
Pacific Gas and Electric Company
No
PG&E recognizes this is an after the fact report, however, the purpose statement should reflect the fact that this proposed standard is for after-the-fact reporting. If the future intent is for this report to replace current reporting criteria the purpose statement should be expanded to reflect the true intent of the Standard.
No
PG&E recognizes the ERO is in R1, however, it does not see where the ERO’s applicability is applied in Attachment 1.
Yes
No
PG&E would like clarification on whether the 30 days, is calendar days or business days.
Yes

No
PG&E believes the addition of a drill constitutes additional training and should be added to R5. PG&E is concerned as to who the target audience for this annual training would affect.
No
PG&E believes 30 days is too restrictive due to real-time operations schedule requirements. The schedule is six weeks and individuals may be on either long change or vacation and therefore unable to complete the training within 30 days of the identification of the need. Suggest extending to 60 days to meet the training criteria which follows the NERC Continuing Education revised submittal date for the Individual Learning Activities (ILA).
No
PG&E believes that if the standard is intended to be an after the fact report, we question the one and/or twenty-four hour reporting criteria and then the 30 day criteria?
Yes
Yes
No
PG&E believes the report is duplicative to the OE-417 reporting criteria.
No
PG&E believes Attachment 1 Part A or B do not clearing specify “sabotage” events, other than “forced entry” and the proposed definition of “impact event” does not meet FERC’s directive to “further define sabotage” nor does it take into consideration their request to address the applicability to smaller entities.
Yes
Yes
Yes
PG&E believes as the training requirements continue to expand, having one training standard that captures all the training required within the NERC standards will allow for better clarity for the training departments in providing and meeting all NERC Standard compliance issues.
Individual
Laurie Williams
PNM Resources
No
PNM believes the purpose statement should reflect the fact that this proposed standard is for after-the-fact reporting. It is misleading and may have many thinking it is duplicative work.
No
PNM OTS does not see where the ERO’s applicability is applied in Attachment 1.
Yes
No
PNM would like clarification on whether the 30 days, is calendar days or business days.
Yes
No
PNM feels the addition of a drill or exercise constitutes additional training and believes R4 should be added to R5. The WECC OTS also is interested as to what level does the annual training target, for instance, the field personnel. Will they have to complete the exercise/drill?
No
PNM believes 30 days is too restrictive due to real-time operations schedule requirements. Most work schedules are either five or six weeks and individuals may be on either long change or vacation and therefore unable to complete the training within 30 days of the identification of the need. Based on the NERC Continuing Education revised submittal date for the Individual Learning Activities (ILA), PNM would recommend 60 days. Creating an Impact Event Report is duplicative and redundant and the WECC OTS feels this is not necessary.
No
PNM believes there seems to be redundancy in reporting based on the time frames in Attachment 1, i.e. OE-417 and other required reports. If this standard is intended to be an after the fact report, why is there one/twenty-four hour

reporting criteria?
Yes
Yes
No
PNM believes the report is duplicative to the OE-417 reporting criteria.
No
PNM believes the proposed definition of “impact event” does not meet FERC’s directive to “further define sabotage” nor does it take into consideration their request to address the applicability to smaller entities. Attachment 1 Part A or B do not clearing specify “sabotage” events, other than “forced entry”.
Yes
Yes
Yes
PNM believes that having one training standard that captures all the training required within the NERC standards will allow for better clarity for the training departments in providing and meeting all NERC Standard compliance issues. This will become even more of an issue as training requirements continue to expand.
Individual
Val Lehner
ATC
Yes
ATC agrees with the purpose statement. However, we do not agree with the implied definition of “impact events” as represented in Attachment 1. (See specific comments about what is included in Attachment 1 for the type of events that qualify as an “impact event”.)
No
The Functional Entities identified in Attachment 1 do not align with the current CIP Standard obligations (e.g. Load Serving Entities are not included).
No
ATC does not agree with R1 for three reasons: 1. The ERO cannot be assigned obligations in NERC Standards. The requirements for the ERO should be addressed by a revision to Section 801 of the Rules of Procedure. 2. This is a fill-in-the-blank requirement. The requirement, positioned as R1, does not allow for the obligations to be clearly defined. It refers to R6 which refers to R2 and Attachment 1. A clearer structure to the Standard would be to simply state that the Functional Entities have to meet the reporting obligations documented in Attachment 1 and delete the current R1.
No
The requirement should be rewritten to simply state that the Functional Entities has to meet the reporting obligations documented in Attachment 1. How the Functional Entity meets the obligations documented in Attachment 1 should be determined by the Functional Entity, not the requirement. The prescriptive nature of this requirement does not support the performance-based Standards that the industry and NERC are striving towards. In addition, requirement 2.9 creates an alternate method for NERC to develop Standards outside of the ANSI process. This requirement dictates that Functional Entities are required to incorporate lessons learned from NERC reports into their Plan, which is a requirement of this Standard.
No
ATC believes that this requirement should be deleted and that the SDT should coordinate its goal with the EAWG. We believe that the lessons learned process and identification of root cause is better covered under that process than through the NERC Mandatory Standards.
No
We do not believe that a drill that exercises a written reporting obligation will add additional reliability to the BES.
No
ATC believes it is an inherent obligation of all Functional Entities to train their appropriate staff to meet all applicable NERC Standards. Including a training requirement in some, but not all, Standards implies that the other Standards do not necessitate training. Although this is an important Standard and one that should be included in a Functional Entities’ training program, ATC does not believe that this Standard is more important than the other NERC Standards and, therefore, requires a separate training provision
Yes
ATC does agree that applicable entities report on events identified in Attachment 1 (See our comments about

Attachment 1), but we do not agree that applicable entities should be required by this standard to have an Operational Plan. Please see our comments to question 4.
No
ATC feels the ERO obligations should be covered in the Rules of Procedure. We do not agree with the requirements assigned to the ERO, but believe that they should be incorporated into the ERO's Rules of Procedure
No
ATC has several areas of concern regarding Attachment 1. 1. The one hour requirement for reporting will take the Functional Entities' focus off of addressing the immediate reliability issues and instead force the FE to devote valuable resources to filling out forms which will potentially reduce reliability. 2. Part A: a. Provide a definition of "system wide" for the Energy Emergency requiring system-wide voltage reduction. b. Add in the clarity that for Energy Emergency requiring firm load shed pertains to a single event, not cumulative events. c. Insert the word "continuous" for Voltage Deviations. d. Take off the TOP for IROL violations. (We believe that an IROL violation should be reported by the RC and not by the TOP based on the nature of the event. Requiring both the RC and TOP to report will only result in multiple reports for a single event. The RC is in the best position to report on an IROL violation for its RC area.) e. Take off the TO, TOP and add the LSE for Loss of Firm Load. (As a transmission only company ATC does not have contracts with end load users. Because of this the Loss of Firm Load should be the reporting obligations of the entity closes to the end load users which is the BA, DP or LSE. Failure to modify this requirement will cause confusion as to which entity has to report Loss of Firm Load. f. Define a timeframe for Generation Loss g. Multiple should be changed to "4 or more" for Transmission Loss.(ATC is concerned that this would require reporting of events that have little or no industry wide benefits but would take up considerable Registered Entity resources.) h. Provide clarity to and tighten the definition of Damage or destruction of BES equipment. The way it is written now would require over-reporting of all damaged or destroyed equipment due to a non-environmental external cause (e.g. broken insulator). 3. Part B: a. Take off the TO and TOP for Loss of off-site power. (The GOP has the responsibility to acquire off-site power and we believe it is the GOP's sole responsibility to report the Loss of off-site power. Failure to correct this would result in multiple reporting for the same event.) b. Take off RC for Risk to BES equipment. (The RC function does not own BES equipment and we believe it is impossible for them to report on risk to BES equipment if they are not the owner or operator of that equipment. This standard should be required of the entity that owns/operates BES equipment. c. Provide guidance to the phrase "reasonably determine" in footnote. d. Examples provided do not provide a clear obligation for an entity to follow. (Question: How close is the train to the substation? (Inches away from the substation fence, ten feet away from the substation fence or 500 feet away from the substation fence.) In addition, this standard is so open to interpretation that no entity can demonstrate compliance with the action. We believe that the only solution is to delete this reporting requirement. Overall: Multiple Functional Entities impacted by the same event are required to report. No lead entity is identified. This will result in multiple reports of the same event. ATC does not believe that this built-in duplicity enhances reliability?
No
No. NERC does not have the authority to absolve the Functional Entities of the reporting obligations for the DOE Form OE-417. Therefore, there will be duplicate reporting requirements and the one hour timeframes required in Attachment 1 will take valuable resources away from mitigating the event to filling out duplicative paperwork. It is ATC's position that the OE-417 report be used as the main reporting template until NERC and the DOE can develop a single reporting template. Task #14 in the report should be modified to say, "Identify any known protection system misoperation(s)." If this report is to be filed within 24 hrs, there will not be enough time to assess all operations to determine any misoperation. As a case in point, it typically takes at least 24 hrs to receive final lightning data; therefore, not all data is available to make a determination.
Yes
Yes, if ATC's recommended changes are made to Attachment 1 and the Standard.
Yes
ATC agrees with this effort and does not currently see a reliability gap
Yes
Yes, if ATC's recommended changes are made to the Standard. However, if the changes are not supported then ATC recommends that the implantation time be changed to two years. Entities will need time to develop both the plan called for in this standard and to train the personnel identified in the plan.
Yes
ATC believes that it is not evident in this draft that the SDT has worked collaboratively with the Events Analysis working group to leverage their work. ATC believes that NERC must coordinate this project and the EAWG efforts. The EAWG is proposing to modify NERC Rules of Procedure but the SDT is suggesting requirement for the ERO be build within the standard. We believe that the Rules of Procedure is the proper course to take to for identifying NERC obligations, but what is clear is that NERC itself does not seem to have an overall plan for event reporting and analysis. Lastly, ATC would like to see the SDT expand the mapping document to include the work of the EAWG. The industry needs to be presented with a clear picture as to how all these things will work together along with their reporting obligations. The definition of an "impact event" needs to be revised. First, if these events are to include any equipment failure or mis-operation that impacts the BES, the standard is requiring more than is intended based upon the reading of the requirements. PRC-004 already covers the reporting of protection system mis-operations, and if reading this definition

verbatim, it would lead one to conclude that those same mis-operations reported under PRC-004 shall also be reported under EOP-004. The definition should be revised to something like: “An impact event is a system disturbance affecting the Bulk Electric System beyond loss of a single element under normal operating conditions and does not include events normally reported under PRC-004. Such events may be caused by…”
Group
Santee Cooper
Terry L. Blackwell
No
Since this standard is written to report events after-the-fact and not for a System Operator to perform corrective action, we believe the words situational awareness should be removed from the purpose. Situational Awareness is typically used for real-time operations. Also, any events that require reporting should be clearly defined in Attachment 1 and leave no room for interpretation by an entity.
No
Standards cannot be applicable to an ERO because they are the compliance enforcement authority, and the ERO is not a user, owner, or operator of the BES. Since we are reporting events that may affect the BES, why does a DP need to be included as an applicable entity for this standard? If the DOE form is going to continue to be required by DOE, then NERC should accept this form. Entities do not have time to fill out duplicate forms within the time limits allowed for an event. This is burdensome on an entity. If NERC is going to require a separate reporting of events from DOE, then NERC should look at these events closely to determine if any of the defined events should be eliminated or modified from the current DOE form. (For example: Is shedding 100 MW of firm load really a threat to the BES?) Why does Attachment 1 have multiple entities reporting the same event? An RC should not have to report an EEA if the BA is required to report it. This will lead to conflicting reports for the same event. Attachment 1 is just a consolidation of the time frame from other standards. It appears no review was done for consistency of time frames for similar events.
No
It cannot apply to the ERO.
No
The words “operating plan” should be removed from the requirement. This standard deals exclusively with after-the-fact reporting. This requirement is also overly prescriptive.
No
Does the initial probable cause have to be reported within the timing associated in Attachment 1? Entities may not have enough information that soon to report the initial probable cause. This should be done with events analysis.
No
There is no need to drill for administrative reporting! This requirement should be deleted.
No
The concept of requiring training on reporting of after-the-fact events does not support or enhance bulk electric system reliability. We recommend the elimination of this requirement.
No
If the DOE form is going to continue to be required by DOE, then NERC should accept this form. Entities do not have time to fill out duplicate forms within the time limits allowed for an event. This is burdensome on an entity
No
Standards cannot be applicable to an ERO because they are the compliance enforcement authority, and the ERO is not a user, owner, or operator of the BES.
No
The SDT should review the list of events closely to determine if the defined events actually impact the BES. (For example: Is shedding 100 MW of firm load really a threat to the BES?)
No
If the DOE form is going to continue to be required by DOE, then NERC should accept this form. Entities do not have time to fill out duplicate forms within the time limits allowed for an event. This is burdensome on an entity.
No
The term "impact events" needs to be more clearly defined.
No
It is very difficult to assess this question with the standard as currently written.
No
With the proposed training and drill requirements in the current written standard, one year is not enough time.
Yes
We don’t believe that entities should be subjected to duplicate reporting to existing DOE requirements. How does redundancy in reporting requirements improve or enhance bulk electric system reliability?

Individual
Martin Bauer
US Bureau of Reclamation
No
The purpose is more closely related to the concept that "Responsible Entities shall document and analyze impact events and their known causes and disseminate the impact event documentation to support situational awareness". Not all impact events are to be reported. The analysis of the impact events is what is needed to achieve a lessons learned.
Yes
The question is focused on a limited area of Attachment A. There other problematic areas of Attachment 1 will be addressed in subsequent comments.
No
This standard should describe the ERO process of event documentation, analysis, and dissemination. Allowing the ERO to develop a event documentation, analysis, and dissemination process, which becomes a requirement on the Entities, must be derived through the Standards Development Process. The requirement, as it is currently worded, allows the ERO to develop standard requirements. If the intent is to only develop a means of collecting, which does not impose a requirement, the wording should state so. Otherwise, if the ERO wants to require that reports are posted to a specific location by the Entity, then it is a requirement and must go through the Standards Development Process. Secondly, there is already a single reporting form identified. It is not clear why the SDT could not accept that form as the reporting tool.
No
R2 does not reconcile with Attachment A or the sub paragraphs. As an example, the requirement 2.6 states "List of organizations to notify ...." All sub paragraphs use the term notify. Notify as used in Attachment A is when a report cannot be provided in the time frame listed in Attachment A. Therefore there is no requirement in this standard for the Operating Plan to have a provision for reporting. The subparagraph 2.8 indicates that the Entity must update it plan based on the lessons learned published by NERC. It would be appropriate to require a review and update of the plan based on the lessons learned.
Yes
This is provided that the report submitted in Attachment A does not include the probable cause. It is highly unlikely that a probable cause may be determined within the reporting timelines.
No
There is no rationale offered on why 15 months was selected. Without a defined basis the time period is arbitrary. It would be appropriate to let the Entity determine and document the time interval. That would allow the time frame to be sensitive to the complexity of the Operating Plan. Some entities are geographically dispersed and a single Operating Plan may be difficult to test at one time or within 15 months. The allowance for real time events or actual use is a good move and may make it easier to define a suitable time frame by the Entity.
No
The measure is vague and redundant. The Entity is required to provide information to be used to "verify content". The information may be used to demonstrate compliance but who will verify the content is adequate and on what basis. Secondly, the measure requires training information be provided twice, once to demonstrate who participated and then to show who was trained. This is all unnecessary and could be remedied by simply stating that "evidence shall demonstrate that all individuals listed in the plan have received training on their role in the plan"
Yes
No
Requirements 7 and 8 are covered in the Section 801. 801. Objectives of the Reliability Assessment and Performance Analysis Program. The objectives of the NERC reliability assessment and performance analysis program are to: (1) conduct, and report the results of, an independent assessment of the overall reliability and adequacy of the interconnected North American bulk power systems, both as existing and as planned; (2) analyze off-normal events on the bulk power system; (3) identify the root causes of events that may be precursors of potentially more serious events; (4) assess past reliability performance for lessons learned; (5) disseminate findings and lessons learned to the electric industry to improve reliability performance; and (6) develop reliability performance benchmarks. The final reliability assessment reports shall be approved by the board for publication to the electric industry and the general public.
No
The Attachment is very vague and without modification creates a Pseudo definition of BES equipment in the example provided. The example now indicates that something is BES equipment if it is "Damaged or destroyed due to a non-environmental external cause". Perhaps the example should be reworded to "BES equipment whose operation effects or causes:" and then adjust each of the line items to clarify what was intended. Next, the Attachment A example redefines reportable levels for Risk to BES Equipment - From a non-environmental physical threat as "Report copper theft from BES equipment only if it degrades the ability of equipment to operate correctly". Who makes that

determination? Not all events will be known within 24 hours. As example, Risk to BES Equipment - From a non-environmental physical threat may not be known until more thorough examination or investigation takes place. Also the reportable level appears to be defined by the Entity. While agree with that, we will end up with the same criticism from FERC when the level is set to "high" in FERC's mind. The reporting times are unrealistic for complicated events. Notification is reasonable but not reporting. Many organizations's have internal processes the reports must be vetted through before they become public and subject to compliance scrutiny.
No
There is already a reporting form for disturbances. The SDT should reconcile this standard with all the other reporting that is being requested and not add more.
No
The two are distinctly different. Disturbances are what happened, sabotage is why. We can easily tell what happened. Determining why it happened (e.g. sabotage) takes time.
No
The two could be combined with no realibility gap based on the concept rather than the proposed standard. As the standard is currently written, there is a reliability gap. Consider that after the fact reporting of a sabotage event (other than criminal acts which may have been witnessed) usually take some time to investigate and analyze.
No
There is a 15 month training requirement. If the standard goes into effect in one year, most entities will not have had an opportunity to develop their new Operating Plans and train their staff. The effective date should recognize Operating Plans need to be revised and then training needs to be implemented. The most aggressive schedule is 18 months. Two years would be more appropriate. The implementation date could recognize the Operating Plan development as one phase and the training as the second.
Yes
The SDT should consider that in reality it would be more streamlined to require immediate notification of an event for situational awareness, and then give adequate time for analysis of the cause. Reports that have an arbitrary rush will be diseased with low quality information and not much value in the long run to the BES. The Attachment A should be constructed around notification of situational awareness. The reporting timeline should be constructed around the different levels severity. The more severe the event, usually the more complicated the event is to analyze. Simple events usually do not have a significant impact.
Individual
Wayne Pourciau
Georgia System Operations Corporation
Yes
No
This standard should not apply to distribution systems or Distribution Providers. It should apply only to the BES.
Yes
Yes it would reduce duplication of effort and should ensure that the various entities and agencies all have consistent information. It should be simpler and quicker to file than what is needed to meet the current standard. However, the system should allow for partial reporting and hierarchical reporting. Entities up the ladder in a reporting hierarchy may fill in additional info (usually from a wider scope of view) than what lower level entities are aware of. It would be better for information to go up a hierarchy than for bits and pieces to go to the ERO from many entities. Terminology may be different in each of the bits and pieces yet the same idea may be intended. The ERO may mistake multiple reports as being different events when they are all related to one event. The system should give an entity the ability to select the entities that should receive the impact event report. If hierarchical reporting is not enabled by the system, then entities should be allowed to work out a reporting hierarchy as a group and entities at lower levels should not be required to report over the NERC system. Some higher level entity would enter the information on the NERC system as coordinated by the entities within a group.
Yes
An entity-developed Operating Plan will allow the flexibility needed to address different entity relationships around the country, e.g., generating companies, cooperatives, munis, large IOUs, small IOUs, RTOs/ISOs, non-independent market area, and so on. However, all applicable entities should not be required to report directly to NERC or the region. The system should allow for partial reporting and hierarchical reporting. Entities within an area should be allowed to coordinate their plans to define reporting procedures within their area. They could have an entity at some wide scope top level that reports to NERC and the region the information collected from multiple narrow scope lower levels within their wide area. If every small lower level entity directly reported to NERC and the Region, it could create situational confusion rather then situation awareness.
Yes
It directly supports the purpose of the standard.
Yes

We agree with R4 with "… at least annually, with no more than 15 months …" replaced with "… at least once per calendar year, with no more than 15 months …" as in R5.

Yes

Yes

It directly supports the purpose of the standard.

No

It should not be necessary for the ERO to require itself to do these things. NERC's authority should be sufficient to do these things as part of its mission. With quarterly trending and analysis of threats, vulnerabilities, lessons learned, and recommended actions in R8, R7 (an annual review) should not be necessary. The quarterly activity could include proposing revisions to Attachment 1 if warranted. An alternative would be to perform annual trending and analysis of threats, vulnerabilities, lessons learned, recommended actions, and proposed revisions to Attachment 1 if warranted. Also, the Reliability Standards Development Procedure has been replaced with the Standard Processes Manual.

Yes

We support the concept of Impact Events and listing and describing them in a table. However, we have some concerns. Reporting of impact events should not be applicable to a DP. The timelines outlined in Attachment 1 should be targets to try to meet but it should not be a compliance violation of the reporting requirement if it is not met. Regarding the NOTE before the table, verbal reports and updates should be allowed for other than certain adverse conditions like severe weather as well as adverse conditions. The first priority for all entities should be addressing the effects of the impact event. It may not be possible to assess the damage or the cause of an impact event in the allotted time. All entities should make their best effort to quickly report under any circumstances what they know about the event even if it is not complete. They should be allowed to report up through a hierarchy. The written report should not be issued until adequate information is available. Change "Preliminary Impact Event Report" to "Confidential Impact Event Report." Capitalization throughout this table is inconsistent. Sometimes an event is all capitalized. Sometimes not. It is not in synch with the NERC Glossary. All terms that remain capitalized in the next draft (other than when used as a title or heading) should be defined in the Glossary of Terms Used in NERC Reliability Standards. Examples of inconsistencies: Unplanned Control Center evacuation, Loss of off-site power, Voltage Deviations. -Energy Emergency requiring a public appeal or a system-wide voltage reduction: All The NERC Glossary defines Energy Emergency as a condition when a LSE has exhausted all other options and can no longer provide its customers' expected energy requirements. The events should not be described as an Energy Emergency requiring public appeal or system-wide voltage reductions. If public appeal and system-wide voltage reductions are still an option then all options have not been exhausted, the LSE can still provide its customers' energy requirements, and it is not an Energy Emergency. We suggest using "Energy Emergency Alert" rather than "Energy Emergency." -Energy Emergency requiring firm load shedding: load shedding via automatic UFLS or UVLS would not necessarily be due to an Energy Emergency. Other events could cause frequency or voltage to trigger a load shed. Most likely an entity would be seeing the Energy Emergency coming and would be using manual load shedding. -Forced intrusion and detection of cyber intrusion to critical cyber assets: CIP-008 is not referrenced for a forced intrusion. CIP-008 is referenced for a detection of cyber intrusion impact event. Aren't there reportable events per CIP-008 that involve physical intrusion that are not intrusions at a BES facility? -Risk to BES equipment: The threshold states that it is for a non-environmental threat but the examples given are environmental threats. Please clarify.

Yes

We support having one form for reporting however every applicable entity should not be required to fill it out and send it to NERC. See previous comments about hierarchical reporting. The title of the report is "Confidential Impact Event Report." Some suggested modifications: The form could have a blank added to enter the event "description" as described in the first column of Attachment 1. The first seven lines contain information that would most likely be filled out every time. The other lines except line 13 may or may not be applicable every time. It is required (R3) for an entity to access the initial probable cause of all impact events so line 13 will most likely be filled out every time. Please move the probable cause line up to line 7 or 8 (depending on if the event description line is added).

Yes

The new term is much more clear than those two terms. This will improve uncertainty and confusion regarding whether or not something should be reported.

Yes

The new single standard will cover all necessary reporting requirements that are in the current two standards. They are being combined into EOP-004-2 not EOP-004-3.

Yes

Yes

Light years better than the current CIP-001-1 and EOP-004-1! With some changes from this comment period, we should have a clearer set of realistic requirements which could likely pass the ballot. Thanks go out to the drafting team for bringing clarity to this topic. Capitalization throughout this document is inconsistent. It is not in synch with the NERC Glossary. All terms that remain capitalized in the next draft (other than when used as a title or heading) should be

defined in the Glossary of Terms Used in NERC Reliability Standards. Examples of not in synch with the Glossary: Registered Entity, Responsible Entity, Law Enforcement. These are not defined in the Glossary. The requirements that apply to entities should not use the word "analysis." "Assessment" should be used. Analysis is a different process (an ERO process) and is being addressed by another group within NERC (Dave Nevius). This EOP-004 drafting team and the NERC analysis group should closely coordinate such that there are no conflicts and the combined requirements/processes are realistic (mainly regarding timelines).
Individual
Rex Roehl
Indeck Energy Services
No
Suggestion: "Functional Entities identified in Section 4 shall support situational awareness of impact events and their known causes."
No
---ERO should not be included in this or any other standard! FERC can decide whether NERC is doing a good job without having standards requirements to audit to. If NERC needs to be included in a standard, then it should a stand-alone one so that the RSAW for all of the other audits don't need to include those requirements. ---"Loss of off-site power (grid supply)" is important at control centers and other large generators. The SDT must use a well-defined standard such as potentially cause a Reportable Disturbance, to differentiate significant events from others. ---"Footnote 1. Report if problems with the fuel supply chain result in the projected need for emergency actions to manage reliability." is ambiguous. Everything in the Standards program can "Affecting BES reliability". The SDT must use a well-defined standard such as potentially cause a Reportable Disturbance, to differentiate significant events from others. ---"Footnote 2. Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects the reliability of the BES)." is well intentioned but ambiguous. For example, if I know the motivation is to blow up the plant, then by this footnote, I don't have to report. The SDT must use a well-defined standard such as potentially cause a Reportable Disturbance, to differentiate significant events from others. ---All terms should be used from or added to the Glossary.
No
This standard is an inappropriate place to define this requirement. NERC needs to be held accountable, but it should be independent of the standard. What if NERC fails to do it by the effective date of the standard, all Registered Entities will violate the standard until NERC is done. The effective date needs to be set based on NERC completing the system defined in R1.
No
R2 needs to state that the Operating Plan needs to only those Attachment 1 events applicable to the Registered Entity. The Operating Plan should contain a list of these events so that the other Requirements can reference the Operating Plan and not Attachment 1 for the list of events. For example a GO/GOP <2,000 MW would not need to address this type of event and it wouldn't be listed in its Operating Plan. It would be unnecessarily cumbersome, to describe events which are not covered within the Operating Plan.
No
R3 should reference the events covered by the Operating Plan, as listed in it, rather than in Attachment 1. If the Plan is deficient, it is a violation of R2 and not every other Requirement that references the Plan.
No
In M4, it is suggested that data from a real event would be evidence. R4 should be satisfied if the Operating Plan is used for a real event within 15 months of the last drill or event.
No
It is wholly unreasonable to re-train everyone for each change to the Operating Plan. Suggestion: Clarify that upon changes to the Operating Plan, the Registered Entity may either require full training, or instead distribute a summary of the change to affected personnel only.
No
---This is the first mention of the time lines in Attachment 1. If they are part of the standard, then they should be incorporated to the Operating Plan in R2 and then need not be mentioned again, only compliance with the plan. ---In M6, the last part, "evidence to support the type of impact event experienced; the date and time of the impact event ; as well as evidence of report submittal that includes date and time" is redundant. All of that should be in the report to NERC. If not, then it's not important to keep.
No
Reviewing Attachment 1 annually is unnecessary. Events don't change much and if they do, a SAR is needed to consider the changes. NERC should not be included in any standard!
No
Loss of off-site power is important to more than just nuclear plants--but which ones? Control centers or other large generators. But not small generators! Should there be a common element to Attachment 1, like the potential to cause a Reportable Disturbance, or maybe there need to be multiple criteria like that.

No
The form needs to identify whether it is a preliminary or final report. An identifier should be created to tie the final to the preliminary one. Some fields, 1,2 3 5 & 6, are required for the preliminary report and should be labeled as such. With the 1 hour reporting deadline for some events, the details may not be known. 12 & 13 should be required for the final report. 13 should designate whether the cause is preliminary or final. 7-11 & 14 are optional, and the form should state this, and based on some types of events. It's confusing to have irrelevant blanks on the form.
No
Impact Events is OK. It needs to be balloted as a definition for the Glossary like Protection System.
No
Bomb threat has totally been lost.
Yes
Good start on a unified event reporting standard!
Individual
Jonathan Appelbaum
United Illuminating
No
UI suggests adding the phrase: and the ERO shall provide quarterly reports; Responsible Entities shall report impact events and their known causes, and the ERO shall provide quarterly reports, to support situational awareness and the reliability of the Bulk Electric System (BES).
Yes
Yes
No
R2.9 requires provisions to update the Operating Plan based on the annual ERO report developed in R8. The ERO report does not appear to be providing lessons learned to be applied to the Operating Plan for impact event reporting, but more focsed on trends and threats to the BES. Also 30 days after the report is published by NERC is not enough time for the entity to read, and assess the report, and then to administratively update the Operating Plan. UI agrees that the Operating Plan should be reviewed annually and updated subsequent to the review within 30 days.
Yes
Yes
Suggest R4 be improved to state that a Registered Entity is only required to conduct a drill or execute real-time implementation of the Operating Pan for one impact event listed in the attachment. In other words the Registered Entity is not required to drill on reporting each type of impact event on an annual basis.
Yes
R5.3 coupled with the rationale provided is a sensible approach. It is important that the rational is not forgotten.
Yes
No
The rules of procedure adequately cover this.
No
UI agrees but the listing needs to be improved for clarity in certain instances. For example, EOP-004 Attachment 1 Part A – Example iii – uses the phrase “significantly affects the reliability margin of the system.” Significantly is an immeasurable concept and does not provide guidance to the Entity. The phrase “reliability margin” is not defined and is open to interpretation. Perhaps utilize “resource adequacy”, if that is all that intended, or use “adequate level of reliability”.
No
The standard does not appear to require the use of Attachment 2. Placing the form within the Standard may require the use of the Standards Development Process to modify the form. UI suggests the form is maintained outside the Standard to allow it to be adjusted. UI would prefer NERC to establish an internet based reporting tool to convey the initial reports.
Yes
The term impact event can substitute for sabotage and disturbance. The use of Forced Intrusion is a bright line for reporting.
Yes

No
UI believes the implementation should be staged. For R1 and R2: First calendar day of the first calendar quarter one year after applicable regulatory authority approval for all. This provides sufficient time to draft a procedure Then time needs to be provided to provide training prior to implementation of R3 and R6. UI believes two calendar quarters should be provided to complete training; therefore R3and R6 is effective six calendar quarters following regulatory approval. Implementation for R4 should state that the initial calendar year begins on the date R2 is effective and entities have 12 months following that date to complete their first drill. R5 requires training once per calendar year. Implementation for R5 should state that the initial calendar year begins on the date R2 is effective and entities have 12 months following that date to complete their first drill.
No
Group
Arizona Public Service Company
Jana Van Ness, Director Regulatory Compliance
Yes
No
AZPS recommends excluding 4.1.7 Distribution Providers, as Distribution Providers generally operate at levels below 100kV.
Yes
Yes
AZPS agrees with R2, however, the use of the term "Operating Plan" is confusing. A more accurate term would be "Event Reporting Plan."
Yes
Yes
AZPS agrees with R4, however, the use of the term "Operating Plan" is confusing and leads one to believe an Operating Drill is necessary for a "reporting plan drill." A more accurate term to use would be "Event Reporting Plan."
No
AZPS believes the required training is too restrictive for minor changes/edits to the Event Reporting Plan.
Yes
AZPS believes that Operating Plan should be replaced with "Event Reporting Plan."
No
AZPS believes that the list in Attachment 1 would be complete, as long as the text box of examples is included. The examples demonstrate what is necessary.
Yes
Yes
Yes
Yes
No
Group
Pacific Northwest Small Public Power Utility Comment Group
Steve Alexanderson
Yes
No
See #15

No
See #15
No
Comments: When applying R3 to row 11 of attachment 1, the comment group notes that applicable entities are expected to assess probable cause of BES equipment damage, including that which may be the result of criminal behavior. At best this would needlessly duplicate the efforts of law enforcement. A more likely result is that entity involvement would interfere with law enforcement and ultimately hinder prosecution of those responsible. Also See #15
No
See #15
No
See #15
No
See #15
No
Footnote 1 is missing from Part A, although it is referenced in column 1 row 11. Is this the Examples? The purpose of the Examples is unclear. Is it meant to limit the scope to those enumerated? This is not stated, but if not it should be removed since it adds confusion. What is meant by non-environmental? All external causes of damage or destruction come from the environment by definition. Please specify what is intended or remove the word.
No
We found no “Preliminary Impact Event Report” in the posted draft standard, so we assume the question is regarding the “Confidential Impact Report” (Attachment 2). It is unclear what role the form plays, since no requirement refers to it. If this is the form to report impact events per R6, then R6 should reference it. The comment group cautions that the use of the word “confidential” should be carefully considered, since many filled out forms that originally contained the word are now posted on the NERC website for all to see. If there are limits to the extent and/or duration of the confidentiality this should be clearly stated in the form, or the word should be avoided. Protection System misoperation reporting is already covered by PRC-004. Including it here is redundant, and doubly jeopardizes an entity for the same event.
No
The comment group fails to see how changing the words meet the directive. Sabotage implies an organized intentional attack that may or may not result in an electrical disturbance. The distinction between sabotage and vandalism is important since sabotage on a small system may be the first wave of an attack on many entities. The proposed standard asks us to treat insulator damage caused by a frustrated hunter (an act of vandalism) the same as attack by an unfriendly foreign government (an act of sabotage). The comment group does not agree that these should be treated equally.
Yes
The proposed standard has a huge impact on small DPs. DPs that presently do not maintain 24/7 dispatch centers will need to begin doing so to meet the reporting deadlines such as 1 hour after an occurrence is identified (possibly identified by a third party) or 24 hour after an occurrence (regardless of when it was discovered by the DP). The planning, assessing, drilling, training, and reporting requirements (R2-R6), as well as documentation (M2-M6) by small entities will cause utility rates to rise, will reduce local level of service, and will not represent a corresponding increase to the reliability of the BES. The SDT concept of clear criteria for reporting has not been met, since R2 effectively directs the applicable entities to develop their own criteria. The decision of which types of events will be reported to which external organizations has been left up to the applicable entity. The comment group notes that there is no coordination of effort required between the applicable entities and the RCs or TOs that issue reliability directives. Energy Emergencies requiring voltage reduction or load shedding are likely to be communicated to applicable entities via directives. The likely result of this lack of coordination is that entities will plan, drill, and train for an event, but when the directive comes it will not be the one planned, drilled, and trained for. Coordination between those sending and receiving directives would ensure the probable events and directed responses are the ones planned, drilled, and trained for.
Group
NERC Staff
Mallory Huggins
Yes
Yes

No
NERC staff is concerned about this requirement's applicability to the ERO. We feel that such a responsibility needs mentioning in the Rules of Procedure, the Compliance Monitoring and Enforcement Program (CMEP), or in a guideline document rather than in a standard requirement. Further, the requirement specifies "how" to manage the event data, not "what" should be monitored.
Yes
Yes
Yes
Yes
Yes
No
NERC staff believes that requirements R7 and R8 are not needed because they are intrinsic expectations from its Rules of Procedure. Furthermore, these elements are necessary for analysis in support of the Reliability Metrics efforts NERC is leading under its Reliability Assessment and Performance Analysis program.
No
The SDT should clarify its use of the term "critical asset" in the Examples section under Part A of the table. The term or versions of the term are used in different contexts in the NERC Reliability Standards. For instance, in CIP-002-1, Requirement 1, the Critical Asset Identification Method is used to identify its critical assets. In EOP-008-0, Requirement 1.3, the applicable entity is required to list its "critical facilities" in its contingency plan for the loss of control center functionality. The team should confirm what it is referring to in this proposed standard. To avoid confusion, the SDT may want to consider using a different term here or better clarify its meaning. Further, there exists the potential to have disparate reporting criteria in this proposed standard relative to the criteria being proposed by the Events Analysis Working Group as part of the Events Analysis Process document dated October 1, 2010. In particular, the following areas should be reconciled between the drafting team and the EAWG to ensure a consistent set of threshold criteria: Voltage Deviations --EOP-004-2: Greater than or equal to 15 minutes --EAWG Process: Greater than or equal to 5 minutes System Separation (Islanding) --EOP-004-2: Greater than or equal to 100 MW --EAWG Process: Greater than or equal to 1000 MWs System Separation (Islanding) --EOP-004-2: Does not address intentional islanding as in the case of Alberta, Florida, New Brunswick --EAWG Process: Addresses intentional islanding as in the case of Alberta, Florida, New Brunswick SPS/RAS --EOP-004-2: Does not expressly address proper SPS/RAS operations or failure, degradation, or misoperation of SPS/RAS --EAWG Process: Expressly addresses proper SPS/RAS operations or failure, degradation, or misoperation of SPS/RAS Transmission Loss --EOP-004-2: Identifies Multiple BES transmission elements --EAWG Process: Provides specificity in Category 1a and 1b regarding transmission events Damage or destruction of BES equipment --EOP-004-2: Through operational error, equipment failure, or external cause but not linked to loss of load --EAWG Process: Identifies in Category 2h equipment failures linked to loss of firm system demands Forced intrusion --EOP-004-2: Addressed --EAWG Process: Not addressed Risk to BES equipment --EOP-004-2: Addressed --EAWG Process: Not addressed Detection of a cyber intrusion to critical cyber assets --EOP-004-2: Addressed --EAWG Process: Not addressed
No
Item 15: A one-line diagram should be attached to assist in the understanding and evaluation of the event. Two additional items are recommended: --Ongoing reliability impacts/system vulnerability – this would capture areas where one is not able to meet operating reserves or is in an overload condition, below voltage limits, etc. in real-time --Reliability impacts with next contingency – this would capture potential impacts as outlined above with the next contingency.
No
NERC staff is concerned with the ambiguity of the term "impact event." The definition of the term is not clear, in part because it includes using the words "impact" and "event" (and thus violates the frowned-up practice of using a word to define the word itself). NERC staff recommends the SDT consider using the term "Event." The following definition (modified from the one used the INPO Human Performance Fundamentals Desk Reference, P. 11) would apply: Event: "An unwanted, undesirable change in the state of plants, systems or components that leads to undesirable consequences to the safe and reliable operation of the Bulk Electric System." Supporting statement following the definition: "An event is often driven by deficiencies in barriers and defenses, latent organizational weaknesses and conditions, errors in human performance and factors, and equipment design or maintenance issues." Further, if this is intended for use in this standard, it should be presented as an addition to Glossary to avoid confusion with the use of the term event in other standards. Of course, this would require an analysis of how the term "Event" as defined herein would affect the other standards to which the term is used. In the end, this is the cleanest manner for the standards.

Yes
No
In order to provide explicit dates, the language should be modified to state: “First calendar day of the first calendar quarter one year after the date of the order providing applicable regulatory authority approval for all requirements.”
Yes
NERC staff commends the SDT on its work so far. Merging CIP-001 and EOP-004 is a significant improvement and eliminates some current redundancies for reporting events. NERC staff believes opportunities to improve the proposed standard still exist. In particular, the team should consider possible redundancies with the Reliability Coordinator Working Group (RCWG) reporting guidelines, the Electricity Sector - Information Sharing and Analysis Center (ES-ISAC) reporting requirements for sharing information across sectors, and the Events Analysis Working Group (EAWG) efforts to develop event reporting processes. Ideally, the SDT and the EAWG should work together to develop a single consistent set of reporting criteria that can be utilized in both the EAWG event reporting process and in the requirements of the EOP-004-2 Reliability Standard.
Group
MRO's NERC Standards Review Subcommittee
Carol Gerou
Yes
Thank you for the clarification of “known causes”, this will allow entities to report what they currently know when submitting an impact report.
Yes
The NSRS believes it is important for the ERO to provide valuable Lessons learned to our electrical industry, thus enhancing the reliability of the BES.
Yes
No
A. As detailed in R2, the Operating Plan shall contain provisions for “identifying, assessing, and reporting impact events”. R2.8, and R2.9 do not have a correlation to R2’s Operating Plan. Where, R2.7 states to update the Operating Plan when there is a component change. The NSRS believes the components of this Operating Plan are only 1) indentifying impact events, 2) assessing impact events, and 3) reporting impact events. R2.8 and R2.9 are based on Lessons Learned (from internal and external sources) and do not fit in the components of an entity’s Operating Plan. R2.7 requires the Operating Plan to be updated. As written, every memo, simulations, blog, etc that contain the words “lessons learned” would be required to be in your Operating Plan. It is solely up to an entity to implement a “Lesson Learned” and not the place for this SDT to require an Operating Plan to contain Lessons Learned. Recommend that R2.8 and R2.9 be deleted for this requirement. If R2.8 and R2.9 are not removed, R5.3 will be in a constant state of change. B. In R2.8 & R2.9, It may be difficult to implement lessons learned within 30 days. The NSRS recommends to incorporate lessons learned within 12 calendar months if lesson learned are not deleted from the R2.8 & R2.9.
Yes
The NSRS thanks the SDT for stating “initial probable cause” as this is in direct correlation to the Purpose which states “known causes”.
Yes
The NSRS agrees that to enhance reliability and situational awareness of the BES, the Operating Plan be exercised once per calendar year.
No
R5.2. The NSRS agrees that to enhance reliability and situational awareness of the BES, the Operating Plan be trained once per calendar year. R5.3 As detailed in R2, the Operating Plan shall contain provisions for “identifying, assessing, and reporting impact events”. Where, R2.7 states to update the Operating Plan when there is a component change. The NSRS believes the components of this Operating Plan are 1) indentifying impact events, 2) assessing impact events, and 3) reporting impact events. These components relate to training when the Operating Plan is revised per, R5.3, only. As written, every memo, simulations, blog, etc that contain the words “lessons learned” would be required to be in your Operating Plan and trained on every time one was issued or heard about internally or externally. Recommend that the Operating Plan be revised and training occurs when a change occurs to the entity’s Operating Plan, consisting of 1) indentifying impact events, 2) assessing impact events, and 3) reporting impact events, only.
Yes
Yes
Should read “In accordance with Sections 401(2) and 405 of the Rules of Procedures, the ERO can be set as an applicable entity in a requirement or standard”. As stated in the text box.
No

Please provide a phone number and provision within the Note of EOP-004 – Attachment 1: Impact Events table for an entity to contact NERC if unable to contact NERC within the time described. Voltage Deviations – recommend adding the word “(continuous)” after sustained in Threshold column. This could be interpreted as an aggregate value over any length of time. Frequency deviations - recommend adding the word “(continuous)” after 15 minutes’ in Threshold column. This could be interpreted as an aggregate value over any length of time. CIP-008 R1.3 states the entity is to report Cyber Security Incidents to the ES_ISAC. Does the EOP-004 Attachment 2 fulfill this requirement?
No
Number 4 of the reporting form does not take into consideration of potential impact events. Recommend that “Did the impact event originate in your system?” to “Did the impact event originate or affect your system?”. This will provide clarity to entities.
Yes
As an industry we have looked at sabotage as a sub component of a disturbance. Sabotage is hard to measure since it is based on a perpetrator’s intent and thus very hard to determine.
Yes
Within the above question, the SDT is asking about EOP-004-2 not -3.
Yes
Yes
Please provide an e-mail address for the submittal of the report to NERC (and any other parties above a Regional Entity) within this Standard and a fax number as a backup to electronic submittal. EOP-004 Attachment 2: Impact Event Reporting Form (note in the proposed standards it states EOP-002) seems to be written for Actual Impact Events only. Perhaps another section could be added for “Potential” Impact Events.
Individual
Amir Y Hammad
Constellation Power Generation and Constellation Commodities Group
Yes
No
Constellation Power Generation and Constellation Commodities Group disagrees with the inclusion of Generator Owners. Since one of the goals in revising this standard is to streamline impact event reporting obligations, Generator Operators are the appropriate entity to manage event reporting as the entity most aware of events should they arise. At times, the information required to complete a report may warrant input from entities connected to generation, but the operator remains the best entity to fulfill the reporting obligation.
Yes
No
Constellation Power Generation and Constellation Commodities Group has several issues with this requirement, but in general, this requirement is heavily prescriptive, administrative in nature, and is unclear whether it will positively impact BES reliability. As examples of administrative requirements that have no impact on reliability, please consider the following comments: •Listing personnel in R2.4, - merely having a list of personnel does not add to the sufficiency of an Operating Plan, but it does create a burdensome obligation to maintain a list. As well, specifying “personnel” may limit plans from designating job titles or other designations that may more appropriately and consistently carry reporting responsibility in the Operating Plan. •R2.5 is unclear as to the intent of the requirement – what is threshold of notification? Is the list to be those that have a role in the event response or a list of all within the facility who may receive news notification of the event? Also, as explained above for 2.4, a list is not a beneficial to reliability, but is administratively burdensome. •What is the reasoning for the 30 day timeframe in R2.7 R2.8 and R2.9? The timeframe is not based on a specific necessity, and creates an unreasonable time frame for changing the Operating Plan, in particular if lessons learned are either short turn adjustments or comprehensive programmatic changes what warrant more time to properly institute. In addition, coupled with other requirements (R4, R5, R8), the updating requirements of R2.7, R2.8 and R2.8 potentially create a continually updating Operating Plan which could create enough confusion to reduce the effectiveness of the Operating Plan. The updating and time frame requirements do not impact reliability, but again impose significant administrative burden and compliance exposure. •R2.9 is particularly problematic for its connection to R8. R8 requires NERC to create quarterly reports with lessons learned and R2.9 requires the registered entities to amend their Operating Plans? What if NERC doesn’t write an annual or quarterly report? Are the registered entities out of compliance? The “summary of concepts” for this latest revision, as written by the SDT, includes the following items: •A single form to report disturbances and impact events that threaten the reliability of the bulk electric system •Other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements •Clear criteria for reporting •Consistent reporting timelines •Clarity around of who will receive the information and how it will be used Many of the sub-requirements in R2 do not address any of these items and do not serve to establish a high quality, enforceable and reliability focused standard. Constellation Power Generation therefore

recommends that R2 be amended to read as follows: R2. Each Applicable Entity identified in Attachment 1 shall have an Operating Plan(s) for identifying, assessing and reporting impact events listed in Attachment 1 that includes the following components: 2.1. Method(s) for identifying impact events listed in Attachment 1 2.2. Method(s) for assessing cause(s) of impact events listed in Attachment 1 2.3. Method(s) for making internal and external notifications should an impact event listed in Attachment 1 occur. 2.4. Method(s) for updating the Operating Plan. 2.5 Method(s) for making operation personnel aware of changes to the Operating Plan.

No

This requirement introduces double jeopardy for registered entities. If an entity does not include methods for identifying impact events and for assessing cause per R2.1 and R2.2 in their Operating Plan, they will be out of compliance with R2. Without the methods in R2 the registered entity is out of compliance with R3 as well for failing to identify and assess. Constellation Power Generation therefore recommends that R3 be amended to be incremental to R2 and read as follows: R3. Each Applicable Entity shall implement their Operating Plan(s) to identify and assess cause of impact events listed in Attachment 1.

No

It is not clear how this requirement to conduct drills and exercises relates to the concepts spelled out by the SDT: oA single form to report disturbances and impact events that threaten the reliability of the bulk electric system oOther opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements oClear criteria for reporting oConsistent reporting timelines oClarity around of who will receive the information and how it will be used R4 does not address any of the above items and should therefore be removed from this standard.

No

Constellation Power Generation questions how R5 relates to the SDT's "summary of concepts": oA single form to report disturbances and impact events that threaten the reliability of the bulk electric system oOther opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements oClear criteria for reporting oConsistent reporting timelines oClarity around of who will receive the information and how it will be used However, Constellation Power Generation believes that security awareness is an important aspect of personnel security and proposes an annual training similar to what was in the previous standards. Constellation Power Generation therefore recommends two requirement changes that would achieve security awareness without the burdensome administrative aspects. First, as stated earlier, a sub requirement in R2 should be added which reads as follows: R2.5 Method(s) for making operation personnel aware of changes to the Operating Plan. Second, this training requirement should be rewritten as follows: Each Applicable Entity shall provide training to all operation personnel at least annually.

Yes

No

The impact event table (Attachment #1), as part of a standard, would have to be FERC approved every time it is edited. That would cause it to go through NERC's Standard Development Process, and would cause a revision to the standard each time. This will also cause revisions to each and every registered entity's Operating Plan. Overall, this requirement causes a large administrative burden on all entities, and does not improve reliability. As stated earlier, the "summary of concepts" for this latest revision, as written by the SDT, includes the following items: oA single form to report disturbances and impact events that threaten the reliability of the bulk electric system oOther opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements oClear criteria for reporting oConsistent reporting timelines oClarity around of who will receive the information and how it will be used Requirement 7 and 8 do not address any of these items. Furthermore, for R8, it is requiring NERC to send out quarterly reports, yet entities are supposed to amend their Operating Plans based on an annual NERC report. This requirement is confusing and is not consistent with earlier requirements. Constellation Power Generation believes that these two requirements should be removed.

No

Constellation Power Generation and Constellation Commodities Group questions why the generation loss line item includes generating facilities of 5 or more generators with an aggregate of 500 MW or greater? The number of units makes no difference for reporting, as is evident in the generation thresholds written before this inclusion. The examples of damaged or destroyed BES equipment are confusing, and do not clarify the reporting event. What if a GSU at a small plant (20 MW) were to fail? Is that reportable? Constellation Power Generation believes that equipment failures that are not suspicious do not need to be reported. Finally, Constellation Power Generation and Constellation Commodities Group believes that the "loss of offsite power affecting a nuclear generation station" should be removed for the following reasons: 1)The purpose of this reliability standard is stated as being: "Responsible Entities shall report impact events and their known causes to support situational awareness and the reliability of the Bulk Electric System (BES). " While the "situational awareness" portion of the purpose could be interpreted as all-inclusive, the real element deals with BES reliability. Off-site power sources to nuclear units have nothing to do with BES reliability. Why should nuclear units be treated differently? 2)The issue of concern for a loss of offsite power at a nuclear station is continued power supply (other than emergency diesels) to power equipment to cool the reactor core. A nuclear unit automatically shuts down when off-site power supply is lost. Availability of off-site power is a reactor safety concern (i.e., NRC

regulatory concern and a one-hour report to the NRC) – not a reliability concern that FERC/NERC would have jurisdiction over. 3)There is a nuclear-specific reliability standard (NUC-001) that contemplated off-site power availability. That standard contained no reporting requirements outside of those that may be already established in current procedures. Why try to impose one here? 4)A loss of offsite power will result in an emergency declaration at the nuclear facility. Notifications will be made to federal (NRC), state, and local authorities. The control room crew is already overly-burdened with notifications – any additional call to NERC/Regional Reliability orgs will add insult-to-injury for no beneficial reason. If NERC is interested, they should obtain info from NRC. 5)If all else fails and the item is to remain on the table, it needs to be clarified as a “complete” loss of off-site power lasting greater than X minutes (i.e., would we have to report a complete momentary loss that was rectified in short order by an auto-reclose or quick operator action?).
No
It is unclear if an entity has to answer all the questions. In addition, “Preliminary” is not currently included in the report title.
Yes
Yes
No
Based on the drastic differences between the previous revisions to these standards, and this proposed revision, 24 months would be a more reasonable timeframe for an effective date.
Yes
As stated earlier, the “summary of concepts” for this latest revision, as written by the SDT, includes the following items: oA single form to report disturbances and impact events that threaten the reliability of the bulk electric system oOther opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements oClear criteria for reporting oConsistent reporting timelines oClarity around of who will receive the information and how it will be used Each and every requirement should be mapped to one of these 5 items; otherwise, it should not be included in this standard. Summarizing all of the comments above, Constellation Power Generation proposes the following revision to EOP-004-2: 1. Title: Impact Event and Disturbance Assessment, Analysis, and Reporting 2. Number: EOP-004-2 3. Purpose: Responsible Entities shall report impact events and their known causes to support situational awareness and the reliability of the Bulk Electric System (BES). 4. Applicability 4.1. Functional Entities: 4.1.1. Reliability Coordinator 4.1.2. Balancing Authority 4.1.3. Transmission Operator 4.1.4. Generator Operator 4.1.5. Distribution Provider 4.1.6. Electric Reliability Organization Requirements and Measures R1. The ERO shall establish, maintain and utilize a system for receiving and distributing impact event reports, received pursuant to Requirement R6, to applicable government, provincial or law enforcement agencies and Registered Entities to enhance and support situational awareness. R2. Each Applicable Entity identified in Attachment 1 shall have an Operating Plan(s) for identifying, assessing and reporting impact events listed in Attachment 1 that includes the following components: 2.1. Method(s) for identifying impact events listed in Attachment 2.2. Method(s) for assessing cause(s) of impact events listed in Attachment 1 2.3. Method(s) for making internal and external notifications should an impact event listed in Attachment 1 occur. 2.4. Method(s) for updating the Operating Plan. 2.5 Method(s) for making operation personnel aware of changes to the Operating Plan. R3. Each Applicable Entity shall implement their Operating Plan(s) to identify and assess cause of impact events listed in Attachment 1. R4. Each Applicable Entity shall provide training to all operation personnel at least annually. R5. Each Applicable Entity shall report impact events in accordance with its Operating Plan created pursuant to Requirement 2 and the timelines outlined in Attachment 1.
Group
FirstEnergy
Sam Ciccone
No
Since this standard is after-the-fact reporting, the phrase "situational awareness" may not be appropriate since that phrase is attributed by a large part of the industry to real-time, minute-to-minute awareness of the system. We suggest the following rewording of the purpose statement: "To ensure Applicable Entities report impact events and their known causes to enhance and support the reliability of the Bulk Electric System (BES)".
No
We do not support the ERO as an applicable entity of a reliability standard because they are not a user, owner or operator of the bulk electric system. Any expectation of the ERO should be defined in the Rules of Procedure.
No
FirstEnergy proposes that requirement R1 and Measure M1 be deleted. A requirement assignment to the ERO is problematic and should not appear in a reliability standard. The team should keep in mind that all requirements will require VSL assignments that form the basis of sanctions. FE does not believe it is appropriate for the ERO to be exposed to a compliance violation investigation as the ERO is not a functional entity as envisioned by the Functional Model. If this "after-the-fact" reporting is truly needed for reliability then the standard must be written in a manner that does not obligate the ERO to reliability requirements. It would be acceptable and appropriate for a requirement to

reference the "ERO Process" desired by R1, however, that process should be reflected in the Rules of Procedure and not a reliability standard.
No
The term Operating Plan(s) is not the appropriate term for this standard. These should be called Reporting Plan(s). Operating Plans are usually designed to be applied during the operating timeframe. Parts 2.2 and 2.6 – We suggest changes to these two subparts as well as a new 2.2.1 and 2.6.1 as follows: 2.2. Method(s) for assessing the initial probable cause(s) of impact events (Add) 2.2.1. Method(s) for assessing the external organizations to be notified. 2.6. List of external organizations to notify in accordance with Part 2.2.1. to include but not limited to NERC, Regional Entity, and Governmental Agencies. (Add) 2.6.1. Method(s) for notifying Law Enforcement as determined by Part 2.2.1. Parts 2.4 and 2.6: This should be a list of job titles for ease of maintenance. An entity may choose to use someone in a job position that is a 24 by 7 operation with several personnel that cover that position over the 24 by 7 period. Listing each person by name should not be required as personnel change while the operating responsibility related to the job title can remain constant. We suggest changing the wording to "2.4. List of the job titles of internal company personnel responsible for making initial notification(s) in accordance with Parts 2.5.and 2.6. 2.5. List of the job titles of internal company personnel to notify." Part 2.6 – We are under the impression that the phrase "include but not limited to" should not be used according to the NEW SDT guidelines. We suggest changing this to say "List of external organizations to notify that includes at a minimum, NERC, Regional Entity, and Governmental Agencies. (A provincial agency is a governmental agency)." Part 2.7. is overly burdensome. FE suggests the team revise to simply reflect annual updates that should consider component changes and updates from lessons learned. This also permits parts 2.8 and 2.9 to be deleted. FE proposes the following text for Requirement R2.7 "Annual review, not to exceed 15 months between reviews, and update as needed of the Reporting Plan that considers component changes and continuous improvement changes from lessons learned." Parts 2.8 and 2.9 - FE proposes to delete part 2.8 and 2.9. We do not see a need for these changes since the plan must be updated annually and will cover lessons learned.
No
M3 – Power flow analysis would be used to assess the impact of the event on the BES, not to determine initial probable cause. It is more likely that DME would provide the data for the initial probable cause evaluation. We suggest rewording M3 as follows: "To the extent that an Applicable Entity has an impact event on its Facilities, the Applicable Entity shall provide documentation of its assessment or analysis. Such evidence could include, but is not limited to, operator logs, voice recordings, or disturbance monitoring equipment reports. (R3)"
No
FE suggests that this requirement be deleted. FE does not see a reliability need for conducting a drill on reporting. This is overly burdensome and should not be included within this reliability standard. Training on the plan and periodic reminder of reporting obligations should suffice.
No
Requirement R5 and Part 5.1 – The wording in Part 5.1 is too prescriptive and shouldnot require training on the specific actions of personnel. Also, R5 should not require training for personnel that may only receive the report and are not required to do anything. Therefore we suggest rewording R5 and 5.1 as follows: "R5. Each Applicable Entity identified in Attachment 1 shall have a Reporting Plan(s) for identifying, assessing and reporting impact events listed in Attachment 1 that includes the following components: 5.1 The training includes the personnel required to respond under the Reporting Plan." Part 5.3 – We suggest removing subpart 5.3. This requirement is overly burdensome and not necessary. We believe that the requirements for annual review and update of the plan as well as training sufficiently cover reviews of changes to the plan. Part 5.4 – The last phrase "training shall be conducted prior to assuming the responsibilities in the plan" should account for emergency situations when the entity does not have time to train the replacement before they are to assume a responsibility.
No
M6 – NERC's system should be capable of making this evidence available for the entities and provide a "return-receipt" of the reports that we send them. Also, M6 should be revised to state "Applicable Entities" as opposed to "Registered Entities".
No
FE disagrees with the ERO as an applicable entity within a reliability standard. See our responses to Questions 2 and 3 above. We do not believe the desired ERO process is adequately covered in section 802. Section 802 deals with assessments and not event reporting.
No
1. The table in Att. 1 and the requirements should alleviate the potential for duplicate reporting. For example, If the RC submits a report regarding a Voltage deviation in its footprint, the report should be submitted by the RC on behalf of the RC, TOP, and GOP, and not require the TOP and GOP to submit duplicate reports. 2. Regarding the "Note" before the table – We agree that under certain conditions it is not possible to issue a written report in a given time period. However, the ERO and RE should also be required to confirm receipt of the verbal communication in writing to prove that the entity communicated the event as these verbal notifications may be done by an entity using an unrecorded line. 3. Organizations with many registered entities should be permitted to submit one report to cover multiple entities under one parent company name. We suggest this be made clear in the Tables, the reporting form, and in the requirements. 4. Voltage Deviations Event – We suggest the team provide more clarity with regard to the types and locations of

voltage deviations that constitute an event. 5. Examples of BES Equipment in Part A of "Actual Reliability Impact" Table – Is the phrase "critical asset" referring to the CIP defined term? If so, this should be capitalized. 6. Under the "Time to Submit Report" column of the table, we suggest that all of the phrases end in "after identification of the occurrence". 7. Frequency Trigger Limit (FTL) for the Frequency Deviation event should be replaced with the values the FTL represent. The FTL is part of the BAAL Standards which have not been approved by the industry and are not in effect. It is possible that these terms are not used by those not participating in the field trial of the BAAL standards.
Yes
Although we agree with the report, it should be clear that organizations with many registered entities can submit one report to cover multiple entities under one parent company.
No
For the most part we support this definition of impact events. However, we have the following suggestions: 1. We believe that it warrants an official NERC glossary definition. 2. The term "potential" in the definition should point to the specific events detailed in Attachment 1 Part B. 3. Since the standard does not cover environmental events, the phrase "environmental conditions" in the definition is not an impact event in the context of this standard.
Yes
Yes
No
Individual
Carol Bowman
City of Austin dba Austin Energy
Yes
Yes
Yes
Austin Energy would like to see OE-417 incorporated into the electronic form This will reduce the callout of EOP-004-2 and OE-417 forms in our checklists / documents and one form can be submitted to NERC and DOE.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Austin Energy would like to see OE-417 incorporated into the electronic form This will reduce the callout of EOP-004-2 and OE-417 forms in our checklists / documents and one form can be submitted to NERC and DOE.
Yes
Yes
If we can used OE 417 for NERC and DOE we do not perceive a reliability gap.
Group
Electric Market Policy
Mike Garton

No
The term “impact events” does not draw a clear boundary around those events that are affected by this standard. Since this is not a defined term, nor is intended to be a defined term in the NERC glossary, this standard lacks clarity and is likely to produce significant conflict as an applicable entity attempts to establish procedures to assure compliance. It appears that situational awareness could not be improved with this standard since it is only dealing with events after-the-fact, not within the time frame to allow corrective action by the system operator. As conveyed in Dominion’s comments on NERC Reliability Standards Development Plan 2011 – 2013, Dominion does not see this draft standard as needing to be in the queue while other standards having more impact to bulk electric reliability remain incomplete or unfinished.
No
Having the ERO as an applicable entity is concerning as they are also the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. For example, establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC’s open process. Attachment 1 is troublesome. The time frames listed are not consistent for similar events. For example, EEAs are either reported within one or 24 hours depending on the nuance. Having multiple entities reporting the same event is troublesome, i.e., why does a RC have to report an EEA if the BA is going to report it? This will lead to conflicting reports for the same event. Attachment 1 seems to be consolidating time frames from other standards into one for reporting. However, we believe this subject is more complex than this table reveals and the table needs more clarification. Several of the events require filing a written formal report within one hour. For example, system separation certainly is going to require an “all hands on deck” response to the actual event. We note that the paragraph above the table in attachment 1 indicates that a verbal report would be allowed in certain circumstances, but this is the same issue with the formal report in that the system operators are concerned with the event and not the reporting requirements. There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
No
Having the ERO as an applicable entity is concerning as they are also the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. Establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC’s open process. At this stage it is not clear how the ERO will develop or effectively maintain a list of “applicable government, provincial or law enforcement agencies” for distribution as defined in R1. The “rationale for R1” states that OE-417 could be included as part of the electronic form, but responsible entities will ultimately be responsible for ensuring that OE-417 reports are received at DOE. This requirement needs to be more definitive with respect to OE-417. It seems like the better approach would be for the entities to complete OE-417 form and this standard simply require a copy.
No
This is an overly prescriptive requirement given the intent of this standard is after-the-fact reporting. The requirement to create an Operating Plan lacks continuity with the ERO Event Analysis Process that is currently slated to begin industry field testing on October 25, 2010. Suggest the SDT coordinate EOP-004-2 efforts with this process. R2.6 establishes an external organization list for Applicable Entity reporting, yet R1 suggests that external reporting will be accomplished via submittal of impact event reports. How will the two requirements be coordinated? What governmental agencies are appropriate and how will duplicative reporting be addressed (for example, DOE, Nuclear Regulatory Commission)? Also, in the “rationale for R2”, please explain the reference to Parts 3.3 and 3.4.
No
We think “impact event” needs to be defined in the NERC Glossary to provide the clarity the industry needs to build audit ready compliant procedures.
No
The need for a periodic drill has not been established and appears to be overly restrictive given the intent of the standard is reporting of impact events. Suggest this requirement be eliminated.
No
The need for a periodic training has not been established and appears to be overly restrictive given the intent of the standard is reporting of impact events. Suggest this requirement be eliminated.
No
Entities are already required by other agencies (e.g., DOE, NRC) to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
No
Having the ERO as an applicable entity is concerning as they are also the compliance enforcement authority.
No
1) A particular Event could be applicable to multiple entities and Attachment 1 would require each applicable entity to report the event. This is duplicative and would appear to overburden the reporting system. 2) Loss of off-site power (grid supply) reporting for nuclear plants is duplicative of reporting done to satisfy NRC requirements. Given the activity

at a nuclear plant during this event, this additional reporting is not desired. 3) Cyber intrusion remains an event that would need to be reported multiple times (e.g., this standard, OE-417, NRC requirements, etc.). 4) Since external reporting for other regulators (e.g., DOE, NRC, etc.) remains an obligation of the Applicable Entity, suggest that Attachment 1 only contain impact events as defined in the current version of EOP-004.
No
There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
Yes
The use of the term “impact events’ has simply replaced the terms “disturbance” and “sabotage” and has not further defined sabotage as directed by FERC. We do feel that impact events needs to be a defined term.
No
Per the mapping document, some of the existing requirements are awaiting a new reporting procedure being developed by NERC EAWG. For those requirements that were transferred over, the resulting standard seems overly complex and lacks clarity.
Yes
No
Individual
John Bee
Exelon
No
The purpose states that Responsible Entities SHALL report impact events – this implies that ALL impact events need to be reported regardless of magnitude, suggest rewording to say "… shall report applicable impact events …" to allow for evaluation of each impact for applicability in accordance with Attachment 1).
No
Attachment 1, Part B, footnote 1. A GO is unlikely to know if a fuel supply problem would cause a reliability concern because one GO may not know the demand for an entire region. Attachment 1, Part B, footnote 1. What is the definition of an "emergency" related to problems with a fuel supply chain? What time threshold of projected need would constitute a 1 hour report? Attachment 1, Part A – Voltage Deviations - A GOP may not be able to make the determination of a +/- 10% voltage deviation for ≥ 15 minutes, this should be a TOP RC function only. Attachment 1, Part A – Generation Loss of ≥ 2, 000 MW for a GO/GOP does not provide a time threshold. If the 2, 000 MW is from a combination of units in a single location, what is the time threshold for the combined unit loss? Attachment 1, Part A – Damage or destruction of BES equipment • The event criteria is ambiguous and does not provide clear guidance; specifically, the note needs to provide more explicit criteria related to parts (iii) and (iv) to remove the need for interpretation especially since this is a 1 hour reportable occurrence. In addition, determination of the aggregate impact of damage may not be immediately understood – does the 1 hour report time clock start on initiation of event or following confirmation of event? • The initiating event needs to explicitly state that it is a physical and not cyber. Events related to cyber sabotage are reported in accordance with CIP-008, "Cyber Security – Incident Reporting and Response Planning," and therefore any type of event that is cyber initiated should be removed from this Standard. • If the damage or destruction is related to a deliberate act, consideration should also be given to coordinating such reporting with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security event. Attachment 1, Part B – Loss of off-site power (grid supply) affecting a nuclear generating station – this event classification should be removed from EOP-004. The impact of loss of off-site power on a nuclear generation unit is dependent on the specific plant design and may not result in a loss of generation (i.e., unit trip); furthermore, if a loss of off-site power were to result in a unit trip, an Emergency Notification System (ENS) would be required to the Nuclear Regulatory Commission (NRC). The 1 hour notification in EOP-004 on a loss of off-site power (grid supply) to a nuclear generating station should be commensurate with other federal required notifications. Depending on the unit design, the notification to the NRC may be 1 hour, 8 hours or none at all. Consideration should be given to coordinating such reporting with existing required notifications to the NRC as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential transient on the unit. Attachment 1, Part B – Forced intrusion at a BES facility – Consideration should also be given to coordinating such reporting with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security event. Attachment 1, Part B – Risk to BES equipment from a non-environmental physical threat – this event leaves the interpretation of what constitutes a "risk" with the reporting entity. Need more specific criteria for this event. Attachment 1, Part B – Detection of a cyber intrusion to critical cyber assets - Events related to cyber sabotage are reported in accordance with CIP-008, "Cyber Security – Incident Reporting and Response Planning," and therefore any type of event that is cyber initiated should be removed from this Standard.
No
This requirement should include explicit communications to the NRC (if applicable) of any reports including a nuclear

generating unit as a jurisdictional agency to ensure notifications to other external agencies are coordinated with the NRC. Depending on the event, a nuclear generator operator (NRC licensee) has specific regulatory requirements to notify the NRC for certain notifications to other governmental agencies in accordance with 10 CFR 50.72(b)(2)(xi). In general, the DSR SDT should include discussions with the NRC to ensure communications are coordinated or consider utilizing existing reporting requirements currently required by the NRC for each nuclear generator operator for consistency.

No

R.2.4 and 2.5 - should not be required to have a list of internal personnel. If an entity has an Operating Plan that covers internal and external notifications that should be sufficient. R2.2.7, 2.8, 2.9 – R4 requires an annual drill. Updating the plan if required following an annual drill should be sufficient Why does an entity need to develop a stand alone Operating Plan if there is an existing process to address identification, assessing and reporting certain events? 30 day implementation for a component change or lesson learned does not seem reasonable or commensurate with the potential impact to the BES and should not be a required element of EOP-004. What is the communication protocol for lessons learned outside of the annual NERC report? What process will be followed and who will review, evaluate, and disseminate lessons learned that warrant updating the Operating Plan?

No

: Agree that Each Applicable Entity shall identify and assess initial probable cause of impact events; disagree with aspects and time requirements in Attachment 1.

No

If drills remain as a component of the standard, an effort to consolidate updating an entities plan with a requirement to drill the plan should be made. . Each entity/utility should be able to dictate/determine if they need a drill for a particular event. Is this document implying a drill for every type of event?

No

Exelon doesn’t feel that the 30 day requirement is achievable and recommends an annual review. Training for all participants in a plan should not be required. Many organizations have dozens if not hundreds of procedures that a particular individual must use in the performance of various tasks and roles. Checking a box which states someone read a procedure does not add any value, it is an administrative burden with no contribution to reliability. It is Exelon’s opinion that training requirements should be covered in the PER standards and that the audience to be trained should be identified. R5.4 requires internal personnel that have responsibilities related to the Operating Plan cannot assume the responsibilities unless they have completed training. This requirement places an unnecessary burden on the registered entities to track and maintain a data base of all personnel trained and should not be a requirement for job function. A current procedure and/or operating plan that addresses each threshold for reporting should provide adequate assurance that the notifications will be made per an individual's core job responsibilities.

No

The time durations in the attachment are too short, it would be impossible to collect all the data necessary to report out on an impact event in the defined time to report. The SDT should evaluate each event for the most appropriate entity responsible to ensure there is minimal confusion on who has the responsibility and eliminate duplication of reporting when feasible.

No

The listed Impact Events is lacking specific physical security related events. . In general, all impact events need to be as explicit as possible in threshold criteria to eliminate any interpretation on the part of a reporting entity. Ambiguity in what constitutes an "impact event" and what the definition of "occurrence" is will ultimately lead to confusion and differing interpretations.

No

Exelon agrees with the use of the report but feels that # 5 should consist of check boxes. #12, 13, and 14 will take more time then allotted by the reporting requirements to acquire, cannot be accomplished in an hour. Attachment 2 should have a provision for the reporting entity to enter (N/A) based on function (see below) Check box #8 A GO/GOP may not have the information to determine what the frequency was prior to or immediately after an impact event. This information should be the responsibility of a TOP or RC. Check box #9 A GO/GOP may not have the information to determine what transmission facilities tripped and locked out. This information should be the responsibility of a TO, TOP or RC. Check box #10 A GO/GOP may not have the information to determine the number of affected customers or the demand lost (MW-Minutes). This information should be the responsibility of a TO, TOP, or RC.

No

Need to better define sabotage and provide examples, the term “impact events” create confusions as to what constitutes an event. The definition of impact event is vague and needs to be quantified or qualified with a term such as “significant”. Otherwise, almost any event could be deemed to be an impact event. Attachment 1 needs to clearly define that damage or destruction of BES equipment does not include cyber sabotage. Events related to cyber sabotage are reported in accordance with CIP-008, "Cyber Security – Incident Reporting and Response Planning," and therefore any type of event that is cyber initiated should be removed from this Standard. In general, all impact events need to be as explicit as possible in threshold criteria to eliminate any interpretation on the part of a reporting entity.

Ambiguity in what constitutes an "impact event" and what the definition of "occurrence" is will ultimately lead to confusion and differing interpretations.
No
Reporting form doesn't allow for investigations which result in no impact events found or identified.
Yes
Agree with the proposed implementation date. A 12 month implementation will provide adequate time to generate, implement and provide any necessary training by a registered entity.
Yes
The standard is lacking guidance for DOE Form OE-417 reporting as outlined in the current version of EOP-004 and doesn't contain any non-BES related reporting. What is the governing process for OE-417 reporting?. Need clarification if one entity can respond on behalf to all entities in one company. Need a provision for entities to provide one report for all entities. Radiological sabotage is a defined term within the NRC glossary of terms. It would seem that a deliberate act directed towards a plant would also constitute an "impact event." In general, the DSR SDT should include discussions with the NRC to ensure communications are coordinated or consider utilizing existing reporting requirements currently required by the NRC for each nuclear generator operator for consistency. The definition of sabotage is defined by NRC is as follows: Any deliberate act directed against a plant or transport in which an activity licensed pursuant to 10 CFR Part 73 of NRC's regulations is conducted or against a component of such a plant or transport that could directly or indirectly endanger the public health and safety by exposure to radiation.
Individual
Kirit Shah
Ameren
No
The purpose talks about reporting impact events and their known causes. We have no problem with this generic intent, but the purpose says nothing about the very burdensome expectation of verbal updates to NERC and Regional Entities (Attachment 1, top of first page), Preliminary Impact Event Reports (Attachment 1, top of first page, are these Attachment 2?), "Actual" Impact Event Reports (Attachment 1 - Part A) and "Potential" Impact Event Reports (Attachment 1 - Part B). These multiple levels of reporting and events need to be greatly reduced.
Yes
Yes
No
While we agree with the intent to list certain minimum requirments for the Operating Plan, the draft list is too lengthy and prescriptive. This merely creates opportunites for failure to comply rather the real purpose of reporting data that can be used to meaningfully increase the reliability of the BES by identifying trends of events that may otherwise be ignored.
No
There are too many missing details on how this will be accomplished. As stated before, this Draft requires too much time be invested in verbal reports, "Preliminary" reports, "Final" reports and even "Confidential" reports (Attachment 2). If the goal is to report ASAP details on events which could impact BES reliability, all of these reports will need to be made at the worst possible time - when Operators are trying to collect data, analyze what they find and correct major problems on the system. And if the reports are wrong or not issued fast enough, the Operators will be keenly aware of potential fines and violations.
No
Establishing a program with trigger actions expected to require reporting several times a year, combined with adequate initial, and on-going, training should preclude the need for mandatory drills as an added compliance burden.
Yes
Yes
No
NERC's current heavy case load should justify reviewing the impact review table only once every 2 years.
No
We have numerous comments about the Attachments. (1) What are the requirements for "verbal" reporting to NERC and Regional entities? (2) What are the requirements for a "Preliminary" Impact Event Report? (3) The Voltage Deviations Event is unclear (a) Are these consecutive minutes? (b) Where is the voltage measured? (generator terminals? Point of Interconnections? Anywhere?) (c) must each Entity report separately? (d) What is the +/- 10% measured against (Generator Voltage Schedule?) (4) For Generation loss events how is an "entity" defined? (a

corporate parent? each registered entity? other?) (5) Are the "Examples" in the Attachment 1 - Part A really Examples, or mandatory situations? (6) Can you define "Damage"? (7) Can you define "external cause"? (8) Can you give examples of "non-environmental external causes"? (9) The footnote 1 reference for "Damage or destruction of BES equipment" doesn't match up with the a. and b. footnotes or the 1. footnote of Attachment A - Part B. (10) How is the Operator supposed to determine what Event affects the reliability of the BES fast enough to decide whether or not to report? (11) is the Loss of off-site power (grid supply) event to a nuclear plant already covered by NUC-001?(12) What are "critcal cyber assets" since CIP-002-4 will eliminate that term? (13) When is Attachment 2 supposed to be used? (14) What is meant by the word "Confidential" in the title of the Attachment 2 report? How would the SDT propose a GO/GOP handle the reporting for the following situation? A CTG unit is dispatched and the unit is started, synchronized and put on the bus. Immediately the Operator receives a high gas alarm from the GSU. The Operator quickly shuts the unit down and de-energizes the GSU. There are no relay targets and no obvious reason for the problem. After several weeks of analysis it's determined there was an internal fault in the GSU and it must be replaced. How would the SDT recommend all the reporting requirments in this situation be addressed with the current draft?
No
It is unclear when this should be used, or why.
Yes
However, the term Impact Event should be a new defined term. When the SDT determines this, it should use the term consistenly on both pages 5 and 21 of the SDT document.
No
It appears that all requirements have been addressed from the existing standards. However, we believe there is a reliability gap that continues from the existing standards because sabotage is not defined any better than in the existing standards.
Yes
Yes
We are concerned with the Future Development Plan. It shows an initial ballot period starting in December. This standard has significant issues and will need another distinct comment period (and not the formal comment period in parallel with balloting) prior to balloting.
Individual
Thad Ness
American Electric Power (AEP)
No
It is unclear what the relationship between this project and the newly revamped NERC Event Analysis Process. We support moving towards one process opposed to separate obligations that may be in conflict. In addition, AEP supports the concept of a central clearinghouse such as the RCIS that is shared by the industry. We support fewer punitive requirements and more prompting for using tools to make multiple entities aware of reliability related issues shortly after the fact.
No
AEP does not agree with the addition of the Generator Owner to the standard. The Generator Owner does not have visibility to the real time operational status of a unit. As a result, the Generator Owner lacks the ability to recognize impact events and report them to the Regional Entity or NERC within the time frames specified in the standard. Reporting requirements for impact events should be the responsibility of the Generator Operator.
Yes
Overall we support the concepts; however, it is unclear if the ERO can be held accountable for compliance with NERC Requirements. If this requirement is removed there needs to be some mechanism for the ERO to establish a single clearinghouse.
No
Component 2.2 “Method(s) of assessing cause(s) of impact events” is very vague. Furthermore, there are concerns whether these methods can be accomplished within one hour as might be required per Attachment 1, in addition to operating the system. Component 2.6 – need to add the statement “as appropriate for type of impact event” Components 2.7 through 2.9 – are good concepts to consider for future inclusion, but at this point in time these appear to be overreaching objectives. We recommend the SDT take smaller increments towards future progress at measure and reasonable pace. Furthermore, if Component 2.9 is retained it should only pertain to lessons learned on the reporting of impact events not all recommendations regarding remediation of the impact events themselves. Furthermore, the 30 day window to update the Operating Plans is aggressive considering the other priorities that may be present day to day.
No
Not clear how this is different from R6 since it relies on the same timetable in Attachment 1.
Yes

Yes
No
It is not clear how this is different from R3 since it relies on the same timetable in Attachment 1.
No
Are the times listed for the initial probable reporting under R3 or the reporting under R6? Many of these items do not constitute emergency conditions. We view many of these as too onerous and would divert operating staff from monitoring and operating the BES. In addition, some terms (i.e. Frequency Trigger Limits) are not currently defined terms. Furthermore, there are existing requirements that have obligations for entities to provide this information to the RC. For example “Detection of a cyber intrusion to critical cyber assets” is already covered under CIP-008. This creates duplicate (and potentially competing) requirements. AEP also contends that some of the timelines are very aggressive and not consummate with perceived need for the information. Transmission loss of multiple BES transmission elements (simultaneous or common-mode event)within 24 hours after occurrence is overly aggressive and should provide more specific criteria.
Yes
Yes
Yes
The standard needs to be modified to allow the ability for one entity to report on behalf of other entities. For example the loss of Generation over the threshold could be reported by the RC opposed to the GO individually, if mutually agreed upon before the fact.
Group
Bonneville Power Administration
Denise Koehn
Yes
Known causes are difficult under 1 hour reporting requirements (Unusual events are even harder to narrow down in 24 hours and may take weeks.) The System Operators and RC’s handle situational awareness and reliability events, this is an extra wide view and learning for reporting only.
Yes
Yes
As long as the 2.4 list is position based, not based on each individual that fills the position. (There is a concern of listing all 2.4 monitoring/reporting personnel in the company that cover the impact event, since there are different function groups and shift work. Documentation trails are difficult with personnel changes.) Because the CIP is being added, it requires an Operating Plan (instead of procedure) with 30 day revision timelines, so it increases the burden for electrical grid event reporting function. R2.9 language refers to R8 “annual” report; however R8 language is “quarterly” reporting of past year. It appears this standard is going to be in an update status 4 times per year, plus any event modifications plus personnel changes. This could be overly burdensome due to the expanding world of cyber security.
Yes
Known causes are difficult under 1 hour reporting requirements. (Unusual events are even harder to narrow down in 24 hours and may take weeks.)
No
There was no drill required for CIP-001 (a drill was in CIP-008, but the purpose did not list combining CIP-008). A drill is not needed for reporting Electrical Grid events, designate it as excluded in the intent of the requirement.
Yes
There was no training required for CIP-001 or in CIP-008. (The proposed EOP-008 purpose did not list incorporating CIP-008). Training was not really needed for reporting Electrical Grid events.
Yes
The requirement needs to specify who (ERO) to report to. Attachment 1 doesn’t say to report to the ERO either. Clarify or remove the difference between the report submitted and evidence of the type of impact event required in the measurement.

Yes
R2.9 language refers to R8 “annual” report; however R8 language is “quarterly” reporting. It appears this standard is going to be in an update status 4 times per year minimum, plus any event modifications plus personnel changes. Overly burdensome.
No
BPA suggests the following: Change loss of multiple BES to 3 or more. Loss of a double circuit configuration due to lightning doesn’t need a report (it’s a studied contingency). Add qualifier to damage/destruction of BES equipment, since a failed PCB or a system transformer normally doesn’t have a MAJOR impact to the grid. Add qualifier to Loss of “ALL” off-site power affecting nuclear… The unplanned evacuation of control center is a busy time for the backup control center, yet this standard requires 1 hour reporting. Suggest changing to 24 hours.
Yes
Item 8: list Hz minimum on the second line prior to Hz max since that is the typical frequency excursion order. The Operating Plan is going to have to include the Compliance Registration ID number, since Operating Personnel don’t carry that information around and it is not readily available.
The definition of an impact event in EOP-004-2 seems clear, however the term "mis-operation" still may imply intent in the action of an individual. The SDT should consider further defining that term.
No
BPA supports the concept behind the revisions to EOP-004-2. Creating a single reporting methodology will improve the processes and lead to more consistency. BPA recommends that the Standards Drafting Team (SDT) coordinate any revisions in the reporting requirements with those found in CIP-008-3 to ensure that there are no conflicts. BPA asks the SDT to consider the impact of these changes on CIP-008-3 and work with the CIP SDT to ensure that the wording of the two requirements is similar and clear. Based on Attachment 1 part A of EOP-004-2, certain cyber security events, intrusions for example, would have to be reported under both EOP-004-2 and CIP-008-3. That puts a burden on a Registered Entity to take additional steps to coordinate reporting or face potential compliance risk for correctly reporting an event under one standard and failing to report it under the other standard. The mapping document had errors: a. CIP-001 R1 to EOP-004 R2.9 (annual vs quarterly). b. EOP-004-1 R2 was translated to R2 & R3 of version 2. c. EOP-004-1 R3 was translated to R6 of version 2 (which doesn’t say to whom to report).
Yes
Yes
The document retention times in EOP-004-3 should be spelled out more clearly. The Compliance summary does so (but needs some punctuation clarification regarding investigation), the SDT should consider making that part of the requirements or clarifying the wording in the requirements.
Group
PSEG Companies
Kenneth D. Brown
No
The following sentence should be added. "This standard is not intended to be for real-time operations reporting."
No
For many items, there are multiple entities listed with reporting obligations. For example, loss of off-site power to a nuclear plant lists RC, BA, TOP, TO, GO and GOP. This appears to result in the potential for the sending of 6 separate reports within the hour for the same event, which in wide area disturbances overload the recipients. The drafting team should consider revising the lists where possible to a single, or absolute minimum number, entity. Those items reportable OE-417 should be removed from Attachment 1. For example, voltage reduction, loss of load for greater than 15 minutes. The trigger for voltage reduction should be the time of issuance of the directive to reduce voltage in an emergency, not when "identified."
No
The top of this form should have the following statement added: "This form is not required if OE-417 is required to be filed."

Group
E.ON U.S. LLC
Brent Ingebrigtson
No
The proposed standard does not list the Load Serving Entity as an Applicable Entity, but the possible events that the standard addresses are within the scope of the LSE. Some functions of the LSE listed within the Functional Model are addressed in the proposed standard. Existing CIP-001-1a and EOP-004-1 are both applicable to the LSE.
No
The Version History contained with EOP-004-2 indicates that CIP-001-1 and EOP-004-1 are “Merged”, however, the actions do not reflect the retirement of CIP-001-1a and therefore, it is unclear if there will be remaining redundancies or potential gaps with the new version EOP-004-2 and CIP-001-1a.
Yes
The new standard should incorporate all other disturbance, sabotage, or “impact event” reporting standards, such as CIP-008-3. At the very least it should reference those other standards that have within their scope same/similar events in order to ensure complete reporting and full compliance. Suggesting that one standard provides the single reporting procedure, when in actuality it does not, is counterproductive. The discussion of “impact event” clearly indicates the SDT’s intent to include sabotage events in the proposed standard EOP-004-2.
Individual
Joe Knight
Great River Energy
Yes
Thank you for the clarification of “known causes”, this will allow entities to report what they currently know when submitting an impact report.
Yes
We believe that it is important for the ERO to provide valuable Lessons learned to our electrical industry, thus enhancing the reliability of the BES.
Yes
No
A. As detailed in R2, the Operating Plan shall contain provisions for “identifying, assessing, and reporting impact events”. R2.8, and R2.9 do not have a correlation to R2’s Operating Plan. Where, R2.7 states to update the Operating Plan when there is a component change. We believe that the components of this Operating Plan are only 1) indentifying impact events, 2) assessing impact events, and 3) reporting impact events. R2.8 and R2.9 are based on Lessons Learned (from internal and external sources) and do not fit in the components of an entity’s Operating Plan. R2.7 requires the Operating Plan to be updated. As written, every memo, simulations, blog, etc that contain the words “lessons learned” would be required to be in your Operating Plan. It is solely up to an entity to implement a “Lesson Learned” and not the place for this SDT to require an Operating Plan to contain Lessons Learned. Recommend that R2.8 and R2.9 be deleted for this requirement. If R2.8 and R2.9 are not removed, R5.3 will be in a constant state of change. B. In R2.8 & R2.9, It may be difficult to implement lessons learned within 30 days. We suggest that lessons learned should be incorporated within 12 calendar months if lessons learned are not deleted from the R2.8 & R2.9.
Yes
While we agree that it makes sense to report on the cause of an event, we disagree with the need for an Operating

Plan as identified in R2
No
We disagree with the need to conduct a drill for reporting
No
We believe that this task should be incorporated into the Job Task Analysis for the System Operators and that this requirement should be deleted as being redundant.
No
We believe the reporting time lines are too aggressive for some events. Reporting events within an hour is not reasonable as an entity may still be dealing the event. This will particularly difficult when support personnel are not present such as during nights, holidays and weekends.
Yes
No
Comments: Please provide a phone number and provision within the Note of EOP-004 – Attachment 1: Impact Events table for an entity to contact NERC if unable to contact NERC within the time described. Voltage Deviations – recommend adding the word “(continuous)” after sustained in Threshold column. This could be interpreted as an aggregate value over any length of time. Frequency deviations - recommend adding the word “(continuous)” after 15 minutes’ in Threshold column. This could be interpreted as an aggregate value over any length of time. CIP-008 R1.3 states the entity is to report Cyber Security Incidents to the ES_ISAC. Does the EOP-004 Attachment 2 fulfill this requirement? We request clarification on the Transmission Loss threshold events that constitute reporting. We also want clarification on what constitutes the loss of a DC Converter station and is there a time duration that constitutes the need for reporting or does each trip need to be reported? For example during a commutation spike the DC line could be lost for less than a minute. Does this loss require a report to be submitted? Is the SDT stating that each time a company loses their DC line, they are required to file a report even though it may not have an effect on the bulk system? What is the threshold for this loss? The SDT needs to clarify that duplicative reporting is not required and that only one entity needs to report. For instance, the first three categories regarding energy emergencies could be interpreted to require the BA and RC to both report. The reporting responsibilities in this table should be clarified based on who has primary reporting responsibility for the task per the NERC Functional Model and require only one report. For instance, since balancing load, generation and interchange is the primary function of a BA per the NERC Functional Model, only the BA should be required to provide this report. The term Frequency Trigger Limit (FTL) is not currently defined in the NERC Glossary. The term FTL needs to be introduced at the beginning of the standard and defined as a new term.
No
NERC and the DOE need to coordinate and decide on which report they want to use and whichever report it is needs to include all information required by both entities. The way this standard is currently written there is the potential that two government entities may need to be reported to is a relatively short period of time. It is not clear what benefit providing the Compliance Registration ID number provides. Many of the registered entities employees that will likely have to submit the report, particularly given the one-hour reporting requirement for some impact events, will not be aware of this registration ID. However, they will know for what functions they are registered. We recommend removing the need to enter this compliance registration ID or extending the time frame for reporting to allow back office personnel to complete the form. For item two, please change “Time/Zone:” with “Time (include time zone)”. As written it is a little confusing.
No
We believe the SAR scope regarding addressing sabotage has not been addressed at all. It appears that impact event essentially replaces sabotage. This standard needs to make it clear that sabotage, in some cases, cannot be identified until an investigation is performed by the appropriate policing agencies such as the FBI. Intent plays an important role in determining sabotage and only these agencies are equipped to make these assessments.
No
It appears that all requirements have been addressed from the existing standards. However, we believe there is a reliability gap that continues from the existing standards because sabotage is not defined any better than in the existing standards.
Yes
Yes
We are concerned with the Future Development Plan. It shows an initial ballot period starting in December. This standard has significant issues and will need another distinct comment period (and not the formal comment period in parallel with balloting) prior to balloting. Please provide an e-mail address for the submittal of the report to NERC (and any other parties above a Regional Entity) within this Standard and a fax number as a backup to electronic submittal.
Individual
Greg Rowland

Duke Energy
No
The Purpose statement says that reporting under this standard supports situational awareness. However this is in conflict with Section 5. Background, where the DSR SDT makes clear that this standard includes no real-time operating notifications, and that this proposed standard deals exclusively with after-the-fact reporting. We also disagree with the stated concept of “impact event”. Including the phrase “or has the potential to impact” in the concept makes it impossibly broad for practical application and compliance.
Yes
No
The requirement again states the intent is to “enhance and support situational awareness”, which doesn’t sync with “after-the-fact reporting”. We question why NERC needs to create this report and system for distributing impact event reports to various organizations and agencies for after-the-fact reporting, when we are still required to make real-time reports under other standards. For example, the Rational specifically recognizes that this standard won’t release us from the DOE’s OE-417 reporting requirement. We don’t see that this provides value, unless NERC can find a way to eliminate redundancy in reporting.
No
Sections 2.4 and 2.5 should allow identification of responsible positions/job titles rather than specific people. Section 2.9 only allows 30 days for updates to our plan based upon lessons learned coming out of an annual report. 60-90 days would be more appropriate. Also, Section 2.9 says it’s an annual report, while R8 only requires quarterly reports.
Yes
Yes
No
Strike the word “all” in the requirement. All personnel don’t need to be trained – for example, the plan may contain references to some personnel as potential sources of the information that will then be reported. Also, Section 5.3 only allows 30 days for training, which may be impossible with rotating shift personnel and training schedules. 60 days is more appropriate.
Yes
Yes
However, R8 only addresses quarterly reports, and R2 Section 2.9 states that there will be an annual report.
No
• General Comment – many timeframes in Attachment 1 are within one hour. This is inconsistent with the stated aim of the standard, which is after-the-fact reporting, as opposed to real-time operating notifications under RCIS and other standards (e.g. TOP). This standard should not be structured to require another layer of real-time reporting. • Voltage Deviation – Plus or minus 10% of what voltage? • Frequency Deviation – this is Interconnection-wide. Do you really want a report from every RC and BA in the Eastern Interconnection?? • Transmission Loss – “Multiple BES transmission elements” should be changed to “Three or more BES transmission elements”. Also, the time to submit the report should be based upon 24 hours after the occurrence is identified. • Damage or destruction of BES equipment – need clarity on the “Examples”. Is the intent to report an event that meets any one of the four “part a.” sub-bullets? i. – critical asset should be capitalized. Disagree with the phrase “has the potential to result” in section iii. – it should just say “results”. Section iv. is too wide open. It should instead say “Damaged or destroyed with malicious intent to disrupt or adversely affect the reliability of the electric grid.” • Unplanned Control Center evacuation – see our General Comment above. Clearly in this case the reporting individuals are evacuating and cannot report in one hour. 24 hours should be more than adequate for after-the-fact reporting. • Fuel Supply Emergency, Loss of off-site power, and Loss of all monitoring or voice communication capability – see our General Comment above. Time to report should be 24 hours after occurrence is identified. • Forced intrusion, Risk to BES equipment, Detection of a cyber intrusion to critical cyber assets – time to report should be 24 hours after occurrence is identified, and critical cyber assets should be capitalized.
Yes
However, Attachment 2 is titled “Impact Event Reporting Form”.
No
We disagree with the stated concept of “impact event”. Including the phrase “or has the potential to significantly impact” in the concept makes it impossibly broad for practical application and compliance. By not attempting to define “sabotage”, the standard creates a broad reporting requirement. “Disturbance” is already adequately defined. “Sabotage” should be defined as “the malicious destruction of, or damage to assets of the electric industry, with the intention of disrupting or adversely affecting the reliability of the electric grid for the purposes of weakening the critical infrastructure of our nation.”

Yes
Yes
No
Individual
Nathan Lovett
Georgia Transmission Corporation
No
These events generally are Operator Functions and should not apply to a TO. 1. Energy Emergency requiring system-wide voltage reduction 2. Loss of firm load greater than 15 min. 3. Transmission loss (multiple BES transmission elements) 4. Damage or destruction to BES equipment (thru operational error or equipment failure) 5. Loss of off-site power affecting a nuclear generating station
No
The only two events that apply to a TO are the ones related to CIP: 1. Forced intrusion (report if motivation cannot be determined, i.e. to steal copper) 2. Detection of a cyber intrusion to critical cyber assets (criteria of CIP-008) Everything in this standard applies to a TOP and therefore E-004-2 and CIP-001 should not be combined
Group
WECC
Steve Rueckert
No
The purpose statement should reflect the fact that this proposed standard is for after-the-fact reporting. It is misleading and may have many thinking it is duplicative work.
No
The ERO's applicability is not applied in Attachment 1.
R1 is appropriate for after-the-fact reporting. However, as proposed this standard eliminates all real-time notifications, including the CIP-001-1 R3 notice to appropriate parities in the Interconnection. New requirement R2.6 lists external parties to notify but it does not include the Reliability Coordinator. It is important that the RC be notified of suspected sabotage. The RC's wide-area interconnection view and interaction with BAs may help recognize coordinated sabotage actions. Any "impact event" where sabotage is suspected as the root cause should require additional and real-time notifications.
No
Need clarification on whether the 30 days is calendar days or business days. As noted in the comment to question 3, any impact event where sabotage is suspected should be treated differently from those where sabotage is not suspected.
Yes
No
The addition of a drill or exercise constitutes additional training and believes R4 should be added to R5. Clarification is needed as to what level does the annual training target, for instance, the field personnel. Will they have to complete the exercise/drill?
No

Thirty days is too restrictive due to real-time operations schedule requirements. Most work schedules are either five or six weeks and individuals may be on either long change or vacation and therefore unable to complete the training within 30 days of the identification of the need. Based on the NERC Continuing Education revised submittal date for the Individual Learning Activities (ILA), the requirement should be changed to require training to be conducted within 60 days.
No
There seems to be redundancy in reporting based on the time frames in Attachment 1, i.e. OE-417 and other required reports. If this standard is intended to be an after the fact report, why is there one/twenty-four hour reporting criteria?
Yes
For strictly after-the-fact reporting the list of Attachment 1 is appropriate. However, as noted in our earlier comments, actual or suspected sabotage events can have a potentially significant impact on reliability and should be treated differently, with additional real-time reporting requirements. It is important that such events be identified and recognized for reliability purposes and that notices include the RC.
No
The report is duplicative to the OE-417 reporting criteria.
No
The proposed definition of “impact event” does not meet FERC’s directive to “further define sabotage” nor does it take into consideration their request to address the applicability to smaller entities. Attachment 1 Part A or B do not clearing specify “sabotage” events, other than “forced entry”. The purpose of CIP-001-1 and its requirements is to address the specific issue of possible sabotage of BES facilities. This is entirely different than a “disturbance” or an “event” on the BES. The proposed definition for “impact events” is essentially any event that has either impacted the BES or has the potential to impact the BES, caused only by three specific things; equipment failure or misoperation, environmental conditions, or human action. Several of these “impact events could be a result of sabotage. Actual or potential sabotage clearly poses a risk to the reliability of the BES. It is important that the risks related to sabotage be reflected in either EOP or CIP
A potential gap may exist. Attacks on BES facilities, via either vandalism or sabotage, are very different events than impact events on the system. From a Compliance standpoint, a revised standard to address the FERC directive on sabotage should be developed as an EOP standard (that is grouped with 693 Standards) rather than as a CIP Standard (CIP-001-1).
Yes
Yes
Having one training standard that captures all the training required within the NERC standards will allow for better clarity for the training departments in providing and meeting all NERC Standard compliance issues. This will become even more of an issue as training requirements continue to expand. CIP-001-1 has surprisingly been one of the most violated standards during the initial period. However, most entities have now developed and demonstrated a decent compliance process. Unless a revised standard to address the FERC directive on sabotage is developed (as suggested in 13 above) this proposed standard appears to eliminate sabotage reporting as a reliability standard to the potential detriment of BES reliability.
Individual
Chris de Graffenried
Consolidated Edison Co. of NY, Inc.
No
Comments: The purpose is not clear because it uses the term “impact events”. This term should be a defined in the NERC glossary, and should not include words such as “potential”.
No
Comments: NERC’s role as the Standard enforcement organization for the power industry will be in conflict if NERC is also identified as an applicable entity. What compliance organization will audit NERC’s performance? This is presently not clear.
No
See response to Question 2.
No
Requirement R2 • Lead-in paragraph - Following the words “Attachment 1” add a period and the words “The Operating Plans shall” and then delete “that” and make “includes” singular. • R2.1, 2.2, 2.3, 2.7 - Replace the word “Method(s)” with the word “Procedure(s)”. • 2.6 – After the word “notify” add a period, then insert the words “For example, external organizations may include” and delete the words “to include but not limited to.” • 2.8 – After the words “Operating Plan based on” add the word “applicable”. Rational R2 After the words “Every industry participant that owns or operates,” add the words “Bulk Electric System.” Then delete the words “on the grid.”

Yes
We agree, however, the term “impact event” must be part of the NERC glossary.
Yes
No
Requirement 5 – Training should be targeted only at those responsible for implementing the Operating Plan (OP), not all those mentioned in the OP. R5 – After the words “internal personnel” add the words “responsible for implementing.” The delete the words “identified in” and “for reporting pursuant to Requirement R2.” 5.4 – Following the words “For internal personnel” add the words “responsible for implementing the Operation Plan.” Between the words “revised responsibilities” add the word “implementation.” M5 – After the words “between the people” add the words “responsible for implementing the Operating Plan”
No
R2 requires applicable entities to have an Operating Plan which are company specific procedures and process required to be compliant with EOP-004. Therefore, R6 should be deleted since it is redundant with R2.
No
See response to Question 2 Requirement 7 Delete the words “and propose revisions to” Following the words (Attachment 1) add a period. Following that period add the words “The ERO shall revise the table” Requirement 8 RECOMMEND DELETION OF R8 – CONFIDENTIALITY CONCERNS WILL MAKE ESTABLISHING A PUBLICATION REQUIRMENT EXTREMELY CHALLENGING.
No
It is absolutely essential that the work on EOP-004 and that on the NERC Event Analysis Process (EAP) be fully coordinated. We find that there are a number of inconsistencies between these two documents. The EAP and EOP-004 are not aligned. In order to operate and report effectively entities need consistent requirements. Attachment 1 Frequency Deviations – The term “Frequency Trigger Limit (FTL)” is not defined. Only defined terms should be used, or the term should be defined. If the term is defined in another standard it should be moved to the Glossary of Terms for wider use. Loss of Firm load for 15 Minutes – The text under the rightmost column entitled, Time to Submit Report, appears to be incomplete in our copy. Transmission loss and Damage or destruction of BES equipment – At the end of the wording for both under the column entitled “Threshold for Reporting” add the words “that significantly affects the integrity of interconnected system operations.” Examples – Capitalize “Critical Asset” as this is a defined term.
No
It is not clear why the DOE form cannot be used. NERC should make every effort to minimize paper work for entities responding to system events.
No
The definition is open for interpretation beyond events identified in Attachment 1. In addition, all Standards are supposed to have Rationales. In the Draft Standard, the Rationales do not address the concept of Potential, and how it relates to an actual system event. Additional work needs to be done addressing the meaning of “potential”.
Yes
Yes
Yes
Overriding Comment and Concern: It is absolutely essential that the work on EOP-004 and that on the NERC Event Analysis Process (EAP) be fully coordinated. We find that there are a number of inconsistencies between these two documents. The EAP and EOP-004 are not aligned. In order to operate and report effectively entities need consistent requirements.
Group
Pepco Holdings, Inc - Affiliates
Richard Kafka
Yes
Yes
Yes
No
For R 2.7, 2.8 and 2.9, 30 days may be too short a time for large entities with multiple subsidiaries to do the necessary notice and coordination. PHI suggests 90 days.

Yes
Yes
No
30 days may be too short a time for large entities with multiple subsidiaries to do the necessary notice and coordination. PHI suggests 90 days.
Yes
Yes
No
Some items with one hour reporting (such as Unplanned Control Center evacuation) may be so disruptive to operations that one hour is too short. 4 hours suggested.
No
The list of events misses many items considered as suspicious or potential sabotage, such as suspicious observation of critical facilities.
No
The list of events misses many items considered as suspicious or potential sabotage, such as suspicious observation of critical facilities.
No
The list of events misses many items considered as suspicious or potential sabotage, such as suspicious observation of critical facilities.
Yes
Yes
The EAWG is developing processes that will be enforced through the Rules of Procedure. It may be inappropriate to reference the EAWG process in the Mapping Document.
Individual
Kathleen Goodman
ISO New England Inc.
No
The proposed requirements in the standard are not focused on the core industry concern that current requirements are unclear as to what types of events warrant entities to report. Per draft 2 of the SAR, “The existing requirements need to be revised to be more specific – and there needs to be more clarity in what sabotage looks like.” Instead this proposed standard includes requirements that are more focused on “how” to report, rather than “what” to report. The draft 2 SAR has never been balloted for approval prior to standard drafting. In fact, the SAR states, “The development may include other improvements to the standards deemed appropriate by the drafting team, with consensus on the stakeholders (emphasis added), consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.” The scope of the SAR, and likewise the proposed standard, is inappropriate to the fundamental reliability purpose of what events need to be reported. The proposed administrative requirements are difficult to interpret, implement and measure, and do not clarify what type of sabotage information entities need to report. Although the use of procedures and an understanding by those personnel accountable seems helpful for ensuring reports are made, the fundamental purpose of clarifying what types of events should be reported and more importantly what types do not have to be reported, is lacking in the standard. Also, one of the first issues identified in the SAR for consideration by the drafting team seems to be ignored: “Consider whether separate, less burdensome requirements for smaller entities may be appropriate.” The requirements for entities to develop Operating Plans and to have training for those plans, further adds uncertainty and increases complexity of how entities, large and small, will have to comply with this standard. The term “impact events” does not draw a clear boundary around those events that are affected by this standard. Since this is not a defined term, nor is intended to be a defined term in the NERC Glossary, this standard lacks clarity and is likely to produce significant conflict as an applicable entity attempts to establish procedures to assure compliance. It appears that situational awareness could not be improved with this standard since it is only dealing with events after-the-fact, not within the time frame to allow corrective action by the system operator. This draft standard should not have this high a priority while other standards having a greater impact on Bulk Electric System reliability remain incomplete or unfinished. Regional reporting requirements should be in Regional Standards, and not be included in a NERC Standard.
No
Having the ERO as an applicable entity raises the issue that they are also the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other

applicable entities would be required to meet. For example, establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC's open process. NERC has also offered the opinion that since NERC is not a "user, owner, or operator" Standards are not enforceable against the ERO. In Attachment 1 the time frames listed are not consistent for similar events. For example, EEAs are either reported within one or 24 hours depending on the nuance. Having multiple entities reporting the same event is troublesome, i.e., why does a RC have to report an EEA if the BA is going to report it? This will lead to unnecessary and possibly conflicting reports for the same event. Attachment 1 seems to be consolidating time frames from other standards into one for reporting. However, this subject is more complex than this table reveals, and the table needs more clarification. Entities that have information about possible sabotage events should report these to NERC after the fact, and the standard should simply reflect that. While we agree with the list of functional entities identified in the Applicability Section, we do not agree with their application in Attachment 1. As the functional entities are identified in Attachment 1, it is likely that there is going to be duplicate reporting. Several of the events require filing a written formal report within one hour. For example, system separation is going to require an "all hands on deck" response to the actual event. The paragraph above the table in Attachment 1 indicates that a verbal report would be allowed in certain circumstances, but this is the same issue with the formal report in that the system operators are concerned with the event and not the reporting requirements. There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements through NERC that cross federal agency jurisdictions.

No

Having the ERO as an applicable entity raises a concern because they are also the Compliance Enforcement Authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. Establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC's open process. At this stage it is not clear how the ERO will develop or effectively maintain a list of "applicable government, provincial or law enforcement agencies" for distribution as defined in R1. The "rationale for R1" states that OE-417 could be included as part of the electronic form, but responsible entities will ultimately be responsible for ensuring that OE-417 reports are received at DOE. This requirement needs to be more definitive with respect to OE-417. The better approach would be for the entities to complete OE-417 form and this standard simply require a copy.

No

This is an overly prescriptive requirement given that the intent of this standard is after-the-fact reporting. The requirement to create an Operating Plan is an unnecessary burden that offers no additional improvements to the reliability of the Bulk Electric System, and this is not, in fact, an Operating Plan. At most, it may be a reporting plan. Most of these requirements are administrative and procedural in nature and, therefore, do not belong as requirements in a Reliability Standard. Perhaps they could be characterized as a best practice and have an associated set of Guidelines developed and posted on the subject. As proposed, the Operating Plan is not required to ensure Bulk Electric System reliability. As stated in the purpose of this standard, it does not cover any real-time operating notifications for the types of events covered by CIP-001, EOP-004. Since these incidents are meant to be reportable after-the-fact, familiarity with the reporting requirements and time frames is sufficient. Stating reporting requirements directly in the standard would produce a more uniform and effective result across the industry, contributing towards a more reliable Bulk Electric System. R2.6 establishes an external organization list for Applicable Entity reporting, yet R1 suggests that external reporting will be accomplished via submittal of impact event reports. How will the two requirements be coordinated? What governmental agencies are appropriate, and how will duplicative reporting be addressed (for example, DOE, Nuclear Regulatory Commission)? Also, in the "rationale for R2", please explain the reference to Parts 3.3 and 3.4.

No

We think "impact event" needs to be defined in the NERC Glossary to provide the clarity the industry needs to build auditable compliance procedures. Although it is useful for entities to make an initial assessment of a probable cause of an event, this requirement should stand alone and does not need to be tied to requirement R2, Operating Plan. Quite often, it takes a considerable amount of time for an actual cause to be determined. The determination process may require a complex root cause analysis. Further, in the case of suspected or potential sabotage, the industry can only say it doesn't know, but it may be possible. Law enforcement agencies make the determination of whether sabotage is involved, and the information may not be made available until an investigation is completed, if indeed it is ever made available.

No

The need for a periodic drill has not been established, and appears to be overly restrictive given the intent of the standard is the reporting of impact events. Suggest this requirement be eliminated. Similar to our comments on R2 for an Operating Plan, a drill, exercise, or Real-time implementation of its Operating Plan for reporting is unnecessary. Such things are training practices. There are already existing standards requirements regarding training. There is no imminent threat to reliability that requires these events to be reported in as short a time frame as may be required for real-time operating conditions notifications.

No

The need for a periodic drill has not been established, and appears to be overly restrictive given that the intent of the standard is reporting of impact events. Suggest this requirement be eliminated. There are training standards in place that cover these requirements. We agree the relevant personnel should be "aware" of the reporting requirements. But

there is not a need to have a training program with specific time frames for reporting impact events. Awareness of these reporting requirements can be achieved through whatever means are available for entities to employ to train on any of the NERC standards, and need not be dictated by requirements.
No
Entities are already required by other agencies (e.g., DOE, NRC) to report certain events. We see no need to develop redundant reporting requirements for NERC that cross other federal agency jurisdictions. There is no need for an Operating Plan as proposed. This is not truly an Operating Plan. There are already other standards which create the requirements for an Operating Plan. This is an administrative reporting plan and any associated impact upon reliability is far beyond real-time operations which is implied by the label “Operating Plan.”
No
Having the ERO as an applicable entity raises concern as it is also the compliance enforcement authority. Requirement R7 is unnecessary as there are already requirements in place for three year reviews of all Standards. R8 contains requirements to release information that should be protected, such as identification of trends and threats against the Bulk Electric System. This may trigger more threats because it will be published to unwanted persons in the private sector. We do not support an annual time frame to update the events list. The list should be updated as needed through the Reliability Standards Development Process. Any changes to a standard must be made through the standards development process, and may not be done at the direction of the ERO without going through the process.
No
1) A particular Event could be applicable to multiple entities and Attachment 1 would require each applicable entity to report the event. This is duplicative and would overburden the reporting system. 2) Loss of off-site power (grid supply) reporting for nuclear plants is duplicative of reporting done to satisfy NRC requirements. Given the activity at a nuclear plant during this event, this additional reporting is not desired. 3) Cyber intrusion remains an event that would need to be reported multiple times (e.g., this standard, OE-417, NRC requirements, etc.). 4) Since external reporting for other regulators (e.g., DOE, NRC, etc.) remains an obligation of the Applicable Entity, suggest that Attachment 1 only contain impact events as defined in the current version of EOP-004. What are the examples at the bottom of page 14 supposed to illustrate? Critical Asset should have the appropriate capitalization as being a defined term. Is Critical Asset what is intended to be used here? Should the “a” list be read as ANDs or Ors? Does “loss of all monitoring communications” mean “loss of all BES monitoring “communications”? Does “loss of all voice communications” mean “loss of all BES voice communications?” Are the blue boxes footnotes or examples? Does “forced intrusion” mean “physical intrusion” (which is different from “cyber intrusion”)? Regarding “Risk to BES Equipment,” request clarification of “non-environmental”. Regarding the train derailment example, the mixture of BES equipment and facility is confusing. Request clarification for when the clock starts ticking. Regarding “Detection of a cyber intrusion to critical cyber assets”, there is concern that this creates a double jeopardy situation between CIP-008 and EOP-004-2 R2.6. Suggest physical incident reporting be part of EOP-004 and cyber security reporting be part of CIP-008.
No
There is already a DOE requirement to report certain events. There is no need to develop redundant reporting requirements to NERC that cross other federal agency jurisdictions. The heading on page 16 refers to EOP-002, but this is Standard EOP-004. If some questions do not require an answer all of the time, then the form should state that or provide a NA checkbox. While Attachment 1 details some cyber thresholds, Attachment 2 provides no means to report – which is acceptable if cyber incidents are handled by CIP-008 per the comment provided for Question 10. The Event Report Template in Appendix A is different from the most recent version, which is available at: http://www.nerc.com/docs/eawg/Event_Analysis_Process_WORKINGDRAFT_100110-Clean.pdf
No
The use of the term “impact events” has simply replaced the terms “disturbance” and “sabotage”, and has not further defined sabotage as directed by FERC. We do feel that “impact events” needs to be a defined term. While we agree with the SDT’s new direction, the FERC directive has not been met. This term and the FERC directive do not recognize limitations in what a registered entity can do to determine whether an act of sabotage has been committed. This term should recognize law enforcement and other specialized agencies, including international agencies roles in defining acts of sabotage, and not hold the registered entity wholly responsible to do so.
No
Per the mapping document, some of the existing requirements are awaiting a new reporting procedure being developed by the NERC EAWG. For those requirements that were transferred over, the resulting standard seems overly complex and lacks clarity. EOP-004-3 should be EOP-004-2.
No
If the training and Operation Plan requirements are adopted as proposed, this may not allow sufficient time for some entities to comply, particularly those with limited number of staff, but perform functions that have multiple event reporting requirements.
Yes
Request clarification on how RCIS is part of this Standard. The form should be filled out in two stages. First stage would be the immediately available information. The second stage would be the additional information such as one line diagrams. There is concern with burdening the reporting operator on filling out forms instead of operating the Bulk

Electric System. Most of the draft requirements are written as administrative in nature, and this is not most effective. Changes need to be made to (or possibly elimination of) R1, R2, R3. The standards should be changed to define what a “disturbance” is for reporting in EOP-004. Sabotage reporting as per CIP-001 should be rescinded as EOP-004 already has such a requirement.
Group
We Energies
Howard Rulf
No
Impact event needs to be clarified first, and DP references in Attachment 1 clarified. Distribution is not BES.
No
The need for a DP to be included needs to be clarified. The Purpose points to BES. A DP does not have BES equipment.
Yes
No
R2.3, R2.4: “Part” is not a defined term or used in the NERC Standard Process Manual. R2: Attachments are not mentioned in the NERC Standard Process Manual. Is this a mandatory or informational part of the standard? R2.6 (and possibly R2.5): There does not seem to be discretion in notifications. Are all people or organizations on the notify lists always contacted for every impact event? Even Law Enforcement? R2.7: What is a “component? A Plan component? A BES component? R2.9: There is no annual NERC report issued pursuant to R8. R8 requires quarterly reporting.
No
A DP may not have Facilities (a BES element). See NERC Glossary definition of Facility.
Yes
No
Please clarify who is to be trained. As written, R5 requires any internal personnel identified in the plan, including CEO, Vice Presidents, etc., to be trained.
No
The proposed definition of “impact event” needs to be clarified.
Yes
No
I did not compare this standard to the OE-417 form. Please do not require operators to fill out a second form during an emergency within one hour. Energy Emergency requiring Public appeal…: “Public ” is not a defined term. Energy Emergency requiring system-wide voltage…: DP does not control BES voltage. Energy Emergency requiring firm load shed…: TOP does not have load it would shed for an Energy Emergency. Frequency Deviations: Why is a BA reporting? This will be every BA in the Interconnection reporting the same Frequency Deviation. Frequency Deviations: Frequency Trigger Limit is not a defined term, and is not defined in this standard. Loss of Firm Load…: TO and TOP may coordinate or direct load shed, but they do not serve firm load. Damage or destruction of BES… There is no footnote 1 on this page. I assume it is the examples on the page. Are these “examples” of a larger set or are these all that is required? Critical Asset is a defined term. Forced Intrusion: “facility” or Facility? An RC and BA do not have Facilities.
No
The data required to assess an impact event thoroughly will often not be available or apparent. Immediate reporting should fall to the RE with assistance/information from the affected entities. There do not seem to be provisions for when it is impossible to take the time to fill out a form or when it is impossible to send a form. I did not compare this standard to the OE-417 form. Please do not require operators to fill out a second form during an emergency within one hour.
No
Impact Event could replace disturbance and sabotage but not in its present form. The proposed definition of impact event “An impact event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action.” Is too vague. The “potential to impact the reliability” is too broad and open to interpretation. It needs to be specific so entities know what is and is not an impact event and so an auditor clearly knows what it is. Define “impact event” as the items listed in Attachment 1. As you have done, focusing on an event’s impact on reliability is more important than determining an individuals intent (sabotage v.s. theft).
Yes

Yes
Yes
Please be careful to capitalize defined terms. If the intent is to not use the defined term, use another word. "Forced intrusion" (cutting a fence, breaking in a door) may not be discovered for quite some time after it occurs. Should it be reported as soon as discovered? Even if there was no impact event (disturbance)? "Destruction of a Bulk Electric System Component" seems pretty specific. However, if a transformer kicks off line due to criminal damage, yet is considered repairable, is the event reportable?
Group
PPL Supply
Annette M. Bannon
Yes
No
While we agree with the list of functional entities identified in the Applicability Section, we do not agree with assignment of applicable entities noted in Attachment 1. As the functional entities are identified in Attachment 1, there will likely be duplicate reporting for many impact events. By applying reporting responsiblities to both the Gen Owner and Gen Operator, this will result in duplicate reporting for plants with multiple owners. It also increases the burden on the Gen Operator who is required to report the event to NERC and to other Gen Owners in a timely manner to allow other Gen Owners to meet the NERC reporting timeline. We suggest that the reporting requirements associated with generators be applied to the Gen Operator only.
Yes
No
While we agree with concept addressed in R2, we don't agree with use of the defined term Operating Plan. Consider working the requirement as follows: "Each Applicable Entity identified in Attachment 1 shall have a documented process or program that includes the following components:..." Also, please consider changing 2.1 to be"Method(s) for recognizing the occurrence of impact events." The current wording could be interpreted to mean, "create a list of the impact events."
No
Please consider changing the word "identify" to "recognize" and adding the Rationale statement to the requirement as follows: "Each Applicable Entity shall assess the causes of the reportable event and gather available information to complete the report."
Yes
No
We generally agree with R5 but recommend two changes to 5.3. Consider expanding the exception criteria to exempt non-substantive changes such as errata changes, minor editorial changes, contact information changes, etc. Also, consider changing "training shall be conducted" to "training or communication/notification of changes shall be conducted."
No
It may be difficult to meet Attachment 1 Part B Potential Reliability Impact submittal times as the time to submit is 1 or 24 hours after occurrence. Consider changing the Time to Submit Report for Forced intrusion, Risk to BES equipment, and Detection of a cyber intrusion to be "report within 24 hours after detection".
Yes
No
Attachment 1 Part A is labeled "Actual Reliability Impact". Does this title mean that for all events listed the "threshold for reporting" is only met if the event occurs AND there is an actual reliability impact? As opposed to Part B where the threshold for reporting is met when the event occurs and there is a potential for reliability impact? This could be broad for events like "Risk to BES equipment."
Yes
Yes
Yes

Yes
No
Individual
Amanda Stevenson
E.ON Climate & Renewables
Yes
No
1. Voltage deviation events are too vague for GOP. How does voltage deviations apply to GOP's or specifically renewables i.e., wind farms? 2. Define what an "entity" is. 3. Define what a "generating station" is. 4. Define what a "BES facility" is. 5. Define what a control center is. 6. Renewable energy/generators should be taken into consideration when crafting the events.
Yes
A generic ERCO approved electronic (form that can be submitted on-line) reporting form will help to add more clarity & consistency to the Impact event reporting process.
No
Administrative burden to some of the components such as 2.5.
No
Redundant with R4.
No
1. Voltage deviation events are too vague for GOP. How does voltage deviations apply to GOP's or specifically renewables i.e., wind farms? 2. Define what an "entity" is. 3. Define what a "generating station" is. 4. Define what a "BES facility" is. 6. Define what a control center is.
Yes
Suggestions on the form: if an entity has not had time to fully determine the cause of an Impact Event such as for "Question # 4: Did the impact event originate in your system, yes or no?", perhaps more time is needed that 24 hours to determine the cause.
No
Acts of Sabotage is still not defined and if the registered entities are required to reports acts of sabotage, NERC still needs to define this further.
Yes
Yes
Refrain from having redundant reporting forms if at all possible. This can create confusion and lead to unnecessary penalty amounts and violations for registered entities. potential" impacts of an event on the BES need to be clearly defined in the standard.
Individual
Christine Hasha
ERCOT ISO
No
ERCOT ISO believes that according to the timelines allotted in Attachment 1, it may not be possible for the entity to identify the "known cause" of an event. The requirements list identification of "initial probable cause". This is more reasonable under the timelines noted in Attachment 1.
No
ERCOT ISO recommends that the Electric Reliability Organization be removed from the standard. The Electric Reliability Organization should not be responsible for reliability functions and therefore should be excluded from reliability standards.
No
Recommend that requirements for the Electric Reliability Organization be removed. However, if the requirements are

retained, ERCOT ISO recommends the following wording change to be consistent with other standards. “R1. The ERO shall create, implement, and maintain a system for receiving and distributing impact event reports, received pursuant to Requirement R6, to applicable government, provincial or law enforcement agencies and Registered Entities to enhance and support situational awareness.”
No
ERCOT ISO recommends the use of “Registered Entity” in place of “Applicable Entity”. This would provide consistency with other requirements and Attachment 1. Recommend the following changes to the subrequirements. “2.6. List of external organizations to notify to include but not limited to NERC, Regional Entity, relevant entities within the interconnection, Law Enforcement, and Governmental or Provincial Agencies.” “2.7. Process for updating the Operating Plan within 30 days of any changes not of an administrative nature. This includes updates to reflect any lessons learned as a result of an exercise or actual event.” Remove requirement 2.8 and move content to requirement 2.7. “2.8. Process for updating the Operating Plan within 30 days of publication the NERC annual report of lessons learned.” Add “2.9. Process to ensure updates are communicated to personnel responsible for under the Operating Plan within 30 days of the change being completed.”
No
ERCOT ISO recommends the use of “Registered Entity” in place of “Applicable Entity”. This would provide consistency with other requirements and Attachment 1. The measure for this requirement notes the obligation for “documentation”. This is not addressed in the requirement. The measure also notes “on its Facilities”. This clarification of scope should be addressed in the requirement. R3. Each Registered Entity shall identify, assess, and document initial probable cause of impact events on its Facilities listed in Attachment 1.
No
ERCOT ISO believes that a drill or exercise of its Operating Plan is unnecessary. The intent of the drill can be addressed within the training requirements under R5.
Yes
ERCOT ISO believes the content of training can include an exercise or drill.
No
ISO recommends the following changes to the language of the requirement. R6. Each Applicable Entity shall report impact events in accordance with Attachment 1.
No
Recommend that the Electric Reliability Organization be removed. The Electric Reliability Organization should not be responsible for reliability functions and therefore should be excluded from reliability standards.
No
ERCOT ISO requests the reporting timeframes be changed to reflect a 24 hour requirement for all events in Attachment 1. During an impact event, operating personnel are generally involved in event resolution and not available immediately to submit reports. ERCOT ISO requests that the “Detection of a cyber intrusion to a critical cyber asset” be removed. There are established processes defined for incident response supporting CIP-008. By including this element in Attachment 1, the Operating requirement R2 would also require procedure documents for cyber security incident response. This would be redundant and would remove the responsibility away from the subject matter experts for cyber security incident response.
No
ERCOT ISO requests the use of a single report format to meet all requirements from NERC and DOE. There is no value added in requiring different reporting to different agencies.
No
Yes
Yes
Yes
ERCOT ISO supports the comments provided by the SRC. However, if the standard is to be established, ERCOT ISO has offered the comments contained herein as improvements to the requirements proposed. The requirements listed do not take into consideration the hierarchical reporting necessary for events (i.e.: GO to GOP to BA). The current structure will lead to redundant and conflicting reporting from multiple entities. This will lead to confusion in the analysis of the event. Any system developed and used to report impact events must include notification to the other relevant entities (i.e.: Reliability Coordinator, Balancing Authority, Transmission Operator, and Generator Operator). The proposed standard should not rely on a centralized system that does not follow the established hierarchy of dissemination of information.
Individual
Terry Harbour

MidAmerican Energy
Yes
No
While we agree with the list of functional entities identified in the Applicability Section, we do not agree with their application in Attachment 1. As the functional entities are identified in Attachment 1, there is likely going to be duplicate reporting. Why should both the RC and BA submit a report for an energy emergency requiring public appeals?
No
No
R2 and R5 coupled with R8 will drive quarterly updates (in addition to drills, etc) and training to the literally hundreds to thousands of people per company for the proper internal operating personnel and management will actually hurt the development of a culture of compliance by overwhelming personnel with constant plan changes and training. The standards drafting team should remove all 30 day references or provide the technical basis of why revising plans and training to “changes and lessons learned” quarterly all within 30 days is the right use of reliability resources to improve the grid. The addition of the 30 day constraints and new vague criteria in Attachment one such as “damage to a BES element through and external cause” or “transmission loss of multiple BES elements which could mean two or more” is the opposite of clear standards writing or results based standards. We disagree with requiring an Operating Plan for identifying, assessing, and reporting impact events. This is an administrative requirement that has no clear reliability benefit. Furthermore, it is questionable that event reporting even meets the basic definition of an Operating Plan. Per the NERC glossary of terms, Operating Plans contain Operating Procedures or Operating Processes which encompass taking action real-time on the BES not reporting on it. As detailed in R2, the Operating Plan shall contain provisions for “identifying, assessing, and reporting impact events”. R2.8, and R2.9 do not have a correlation to R2’s Operating Plan. Where, R2.7 states to update the Operating Plan when there is a component change, the components of this Operating Plan are only 1) indentifying impact events, 2) assessing impact events, and 3) reporting impact events. R2.8 and R2.9 are based on Lessons Learned (from internal and external sources) and do not fit in the components of an entity’s Operating Plan. R2.7 requires the Operating Plan to be updated. As written, every memo, simulations, blog, etc that contain the words “lessons learned” would be required to be in your Operating Plan. It is solely up to an entity to implement a “Lesson Learned” and not the place for this SDT to require an Operating Plan to contain Lessons Learned. Recommend that R2.8 and R2.9 be deleted for this requirement. If R2.8 and R2.9 are not removed, R5.3 will be in a constant state of change. In R2.8 & R2.9, It may be difficult to implement lessons learned within 30 days. The NSRS recommends to incorporate lessons learned within 12 calendar months if lesson learned are not deleted from the R2.8 & R2.9.
No
No
No
: R5.2. The NSRS agrees that to enhance reliability and situational awareness of the BES, the Operating Plan be trained once per calendar year. R5.3 As detailed in R2, the Operating Plan shall contain provisions for “identifying, assessing, and reporting impact events”. Where, R2.7 states to update the Operating We disagree with the need to provide formal training. We could agree with the need to communicate to System Operators and other pertinent personnel the criteria for reporting so that they know when system events need to be reported.
No
We believe the reporting time lines are too aggressive for some events. Reporting events within an hour is not reasonable as an entity may still be dealing the event. This will particularly difficult when support personnel are not present such as during nights, holidays and weekends.
Yes
No
New vague criteria in Attachment one such as “damage to a BES element through and external cause” or “transmission loss of multiple BES elements which could mean two or more” is the opposite of clear standards writing or results based standards.
No
Yes
Yes

Yes
Yes
This entire standard needs to be revised to consider a results based standard.
Individual
Michael Gammon
Kansas City Power & Light
Yes
Yes
Consideration should be given to the need for a preliminary impact event report to be filed by the Reliability Coordinator and the Registered Entity. If two reports should be filed, should they both contain the same information.
Yes
Although we support situational awareness for the other registered entities, impact event reports should be distributed anonymously to communicate the information while protecting the registered entity.
No
We agree with the rationale for R8 requiring NERC to analyze Impact Events that are reported through R6 and publish a report that includes lessons learned but disagree with R2.9 obligating an entity to update its Operating Plan based on applicable lessons learned from the report. Whether lessons learned are applicable to an entity is subjective. If an update based on lessons learned from an annual NERC report is required, the requirement should clearly state the necessity of the update is determined by the entity and the entity's Reliability Coordinator or NERC can not make that determination then find the entity in violation of the requirement. In addition, if an update based on lessons learned from a NERC report is required, NERC should publish the year-end report (R8) on approximately the same day annually (i.e. January 31) and allow an entity at least 60 days to analyze the report and incorporate any changes it deems necessary in its Operating Plan. In addition, the language using quarterly and annual as a requirements between R2.9 and R8 is confusing.
No
We believe R3 and M3 are unnecessary as a stand alone requirement and measure and propose combining this requirement and measure with R6 and M6. Identifying and assessing the initial probable cause of an impact event is the obvious starting point in the reporting process and ultimate completion of the required report. Evidence to support the identification and assessment of the impact event and evidence to support the completion and submittal of the report are really one in the same.
No
We believe R4 and M4 are clearly unnecessary. Thoughtful preparation of an Operating Plan per R2 that specifically addresses personnel responsibilities and appropriate evidence gathering combined with the training requirement in R5 is sufficient.
No
We agree with the need for the Operating plan and the provision of formal training to impacted personnel. We believe that the personnel references are too open-ended to be productive and measurable. This leaves all applicable entities open to subjectivity in assessment and may produce a large administrative burden to demonstrate compliance with no associated benefit to improved reliability.
No
We believe R3 and M3 are unnecessary as a stand alone requirement and measure and propose combining these requirements with R6 and M6. Identifying and assessing the initial probable cause of an impact event is the obvious starting point in the reporting process and ultimate completion of the required report. Evidence to support the identification and assessment of the impact event and evidence to support the completion and submittal of the report are really one in the same.
No
We agree with the rationale for R8 requiring NERC to analyze Impact Events that are reported through R6 and publish a report that includes lessons learned but disagree with R2.9 obligating an entity to update its Operating Plan based on applicable lessons learned from the report. Whether lessons learned are applicable to an entity is subjective. If an update based on lessons learned from an annual NERC report is required, the requirement should clearly state the necessity of the update is determined by the entity and the entity's Reliability Coordinator or NERC can not make that determination then find the entity in violation of the requirement. In addition, if an update based on lessons learned from a NERC report is required, NERC should publish the year-end report (R8) on approximately the same day annually (i.e. January 31) and allow an entity at least 60 days to analyze the report and incorporate any changes it deems necessary in its Operating Plan. Again, the language referencing annual and quarterly in these two requirements in confusing.
No

We agree with the event descriptions listed in Attachment 1 and the review and revision of the impact table by the ERO is appropriately addressed in R7 but the time periods allowed to complete the new, longer preliminary report is insufficient. The correlation of this with the timing of the reporting quarterly and annually or pushing information for other entities' situational awareness does not allow the registered entity adequate time to thoughtfully consider the event and proposed root cause.
No
For easier classification and analysis of events for both external reporting to the ERO and internal reporting for the applicable entity, the form should include Event Type. The DSR SDT should code each event type and include the codes as part of Attachment 1.
Yes
Should the word disturbance be removed from the title of EOP004-2 to avoid confusion and simply be called Impact Event and Assessment, Analysis and Reporting.
Yes
No
April 2011 is too soon for considerations applicable to the creation of an Operating Plan.
Yes
The standard addressed a preliminary report it should also address the requirements of a final report.
Group
Southern Company - Transmission
J T Wood
No
We find it interesting that the ERO is listed as an applicable entity. The ERO is responsible for multiple requirements in this standard that shapes the ultimate actual rules that the other applicable entities would be required to meet. Can the NERC/ERO be accountable for a feedback loop to the industry? Feedback is preferable but would NERC/ERO self-report a violation to the requirement?
Yes
We do have one concern in that we are hopeful that NERC will develop a system that will allow a one stop shop of reporting.
No
The Operating Plan has a different connotation for different operations folks. We suggest that we call it an Impact Event Reporting Plan.
Yes
Yes
No
We suggest that the time frame be changed to 60 or 90 days in 5.3. 5.4 needs to have a time frame associated with it; we suggest that it be 60 or 90 days.
No
The time to submit report column needs to be more flexible with time frames.
Yes
No
The time to submit report column needs to be more flexible with time frames. The Entity with Reporting Responsibility column needs to be more descriptive in which there are multiple entitles with hierarchy reporting.
Yes
Yes
Yes
Yes
Yes

The only concern that we have with the proposed standard is that it feels like it is creating dual, not quite redundant, reporting requirements for cyber intrusions in concert with CIP-008. Hopefully, there will not have to be a redundant reporting requirement if we continue to merge efforts with the CIP Drafting Team. Since we will no longer use the word SABOTAGE in the new EOP-004, we are hoping the industry and the CIP Drafting Team will give us the criteria they wish for us to use in order to report CIP-008 incidents. We will then achieve a “ONE STOP SHOP” reporting standard.
Individual
Ron Gunderson
Nebraska Public Power District
No
The background states there is no real-time reporting requirement in this standard, but the purpose states a purpose is for situational awareness. This implies real-time reporting. The purpose clearly identify the standard is for after the fact reporting to permit analysis of events, trend data, and identify lessons learned.
Yes
Yes
Yes
No
Since the reporting under this standard is for after the fact reporting, the minimum time to report should be the end of the next business day. The combination of the extremely short time periods to file a report and the amount of detail required in attachment 2 will lead to a reduction in the reliability of the BES. System Operators will be forced to take focus off their primary responsibility to respond to the event in order to complete the report within the required timeframe (within an hour for some events). During non-business hours the only personnel available to complete the reports will be those responsible for real-time operation of the BES. Since the background indicates this standard is only for after the fact reporting, the minimum required time to submit the report should be one business day to permit completion of the report without distracting from the real-time operation of the BES. Real-time reporting requirements are covered in other standards and should be to the Reliability Coordinator and from the Reliability Coordinator to NERC. For after the fact reporting, there is absolutely no reliability benefit for requiring reporting to be completed on such a short timeframe. This is especially true due to the amount of data required by Attachment 2.
No
If the standard requires submission of the report within an hour (which is not appropriate), there must be an abbreviated form that can be quickly filled out by checking boxes and not require substantial narrative. The existing form has too much free form text that takes time to enter and with the short timeframe for reporting will distract the entities responsible for real-time reliabiltiy of the BES from that task by forcing them to complete after the fact reports. It is unrealistic to expect entities to staff personnel to complete the reporting 24 x 7 for unlikely events, so the task will fall to System Operators who should be focusing on operating the BES at the time of these events instead of providing after the fact reporting to entities that do not have responsibility for real-time operation of the BES. Real-time reporting to the RC and/or BA is covered under other standards and is necessary for the RC to have situational awareness, but is not covered under this standard. The registered entities may report to the proper law enforcement entities when the situation warrants, but again this form is not the appropriate way to handle that reporting requirement.
Yes
I agree there is a lot of interpretation and confusion as to what sabotage or a Cyber Incident is, so would welcome better clarity. Whether “impact events” can more effectively clarify, is yet to be seen. “it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.” “An impact event is any situation that has the potential to significantly impact the reliability of the Bulk Electric System. Such events may originate from malicious intent, accidental behavior, or natural occurrences.” I do know that Cyber Sabotage may take time or days to become aware so not sure how that might expedite reporting and awareness.
Yes
Appears they only changed R1 for CIP-001 and moving R2-R4 directly over to EOP-004-2. R1 adds much more detail on our part for a company operating plan but would definitely help some of the present confusion.
Individual

Dan Rochester
Independent Electricity System Operator
No
(1) Our understanding of the proposed revision as conveyed in the SAR was to provide clarity and reduce redundancy on reporting the latest and even on-going events on the system that may be caused by system changes and/or sabotage. The intent is to ensure the proper authorities are informed of such events so that they may take appropriate and necessary actions to identify causes and/or mitigate or limit the extent of interruptions. We also supported a suggestion in the SAR to assess the merit of merging CIP-001 and EOP-004 to remove redundancy, although we suggested that this should not be a presumption when revising the standard(s). This posting appears to indicate that only EOP-004 will be revised at this time, and CIP-001 which deals with sabotage reporting will remain in effect. With this assumption, the proposed standard appears to contain a mixture of reporting two types of events of different time frame – the first type being those events that need to be reported soon or immediately after they occur (e.g. impact events that appear to be the result of a sabotage) with an aim to curb/contain these events by the appropriate authorities; the second type being the events that can be reported sometime well after the fact, e.g. system disturbances due to weather or switching or other known causes that are not of malicious nature. Combining the two types of requirement does not appear to be clearly conveyed in the SAR. We therefore suggest the SDT review the main purpose and content in the proposed EOP-004 to ensure consistency with the SAR, and in relation to the purpose and requirements already contained in CIP-004. (2) With respect to disseminating reports and related information after the fact, we wonder if a data collection process, such as RoP 1900, can serve the purpose without having to create a standard or a requirement to achieve this. (3) Most of the requirements appear to be administrative in nature and they stipulate the how but not the what, which in our view does not conform with the Results-based standard concept and does not rise to the level of a reliability standard. (4) A number of requirements proposed in the draft standard are quite vague and cannot be measured. Details of this assessment is provided below.
No
We do not agree with the inclusion of TO and GO. They are not operating entities and do not need to collect or provide information pertaining to impact events, which are the results and phenomena observe under operating conditions in the operation horizon, and such information collection and provision are the responsibility of the TOP and GOP.
No
R1 does not directly convey the need for reporting. The requirement could be written to require the responsible entities to report impact events to the ERO using a process to be described in the standard and according to a set of reporting criteria. Whether or not there is a “system” makes little difference if it complies with the requirement to provide the reports on time. In addition, an ERO established system which, without being included in the standard and posted for public comment and eventually balloted, may not be acceptable to the entities that are responsible for reporting to the ERO. Further, a reliability standard should not need to bother with how the ERO disseminate this information to applicable government, provincial or law enforcement agencies. This is the obligation of the ERO and if required, can be included in the Rules of Procedure.
No
R2 is not needed. An entity does not need to have an “operating plan” to identify and report on impact events; it needs only to report on the events listed in Attachment 1 in a form depicted in Attachment 2. How does the entity do this, and whether or not an operating plan is in place, or whether its staff is trained to provide the report should not need to be included in a reliability standard for so long as the responsible entity provides the report in the required form on time. If the responsible entity fails to report the listed events in the depicted format, it will be found non-compliant, and that’s it – no more and no less. If the “operating plan” really means an established data collection and reporting procedure, then the requirement should be revised to more clearly convey the intent.
No
We agree that the responsible entity needs to identify and assess initial probable cause of impact events but not in accordance with any operating plan in R2. Each operating entity (RC, BA, TOP) has an inherent responsibility to identify the cause of any system events to ensure it complies with a number of related operational standards. R3, in fact, could be revised to require the Responsible Entity to include the probable cause of impact events in its report, rather than asking it to “identify and assess” since this is not measurable. Also, the ERO may be removed from the Applicability Section depending on the response to our comments under Q9.
No
Along the line of our comments on R2 for an operating plan (whose need we do not agree with), a drill, exercise, or Real-time implementation of the Operating Plan for reporting is also not necessary.
No
Along the line of our comments on R2 for an Operating Plan (whose need we do not agree with), any training on developing and providing the report is unnecessary. What matters is that the report is provided to the needed organizations or entities on time and in the required format according to established procedure. How this is accomplished goes outside of the purpose of reliability standard requirements.
No
We agree with having a requirement to report impact events in accordance with the timelines outlined in Attachment 1,

but not with the requirements indicated in R2.
No
We agree with the need to update the list as needed, but it does not have to be the ERO who takes on a reliability standard to do so. It can simply be an annual project in the standards development work plan to review Attachment 1 as part of a standard. The industry will then be provided an opportunity to weigh on the changes. Also, we do not see the reliability results or benefits of R8. The ERO can issue the report quarterly but who are audiences? What reliability purpose does it serve if no further actions are pursued upon receiving the report? Can this be done as a standing item for the ERO at, say, the BoT meeting? Or, can this be a part of the quarterly communication from the ERO to the industry? To make this a reliability standard is an over-kill, and does not conform with the results-based standard concept. From our perspective, both R7 and R8 can be removed, and the ERO can be removed from the Applicability Section as well.
No
We do not support the 1 hour reporting time frames for Emergency Energy, System Separation, unplanned Control Center evacuation, Loss of off-site power, Loss of monitoring or voice communication. Energy emergency is broadcast on the RCIS which also goes to the ERO so its explicit reporting is not necessary (System Operations please verify). During other events listed above, the responsible entities will likely be concentrating its effort in returning the system to a stable and reliable state. Reporting to anyone not having direct actions to control, mitigate and contain the disturbances is secondary to restoring the system to t a reliable state. Since these are after the fact reports for awareness and/or analysis and not for real-time responses, these can be reported at a later time, up to 24 hours after the initial occurrence without any detriment to reliability, or at the very earliest: up to 1 hour after the system has returned to a reliable state, or after the backup control centre is fully functional, or after backup power is restored to the nuclear power plant, or after monitoring or voice communication is restored.
TBD
We do not have a view on what name is assigned to the reportable events for so long they are listed in Attachment 1. However, the heading of the Table contains the words “Actual Reliability Impact”, which does not accurately reflect the content inside the table and which may introduce confusion with the term “impact event”. We suggest to change them to “Reportable Impact Events”. As we read the Summary of Concept and Assumption, there appears to be a slightly different lists at the bottom of P. 21. With these events included, the meaning of “impact event” would seem to be too broad. Rather than calling those events listed in Attachment 1 “impact events”, why not simply call them “reportable events”?
No
We do not agree with the mapping. The proposed mapping attempts to merge the reporting in CIP-001-1 which has more of an on-going awareness nature to alert operating and government authorities of suspected sabotage to prompt investigation with a possible aim to identify the cause and develop remedies to curb the sabotage/events. The proposed EOP-004-2 appears to be more of a post-event reporting for need-to-know purpose only. This is not consistent with the purpose of the SAR.
We do not agree with the proposed standard. We therefore are unable to agree on any implementation plan.
No
Individual
Catherine Koch
Puget Sound Energy
Yes
However, further definition of "known causes" would be helpful as sometime the root cause analysis doesn't uncover the actual cause for sometime after the timeframes outlined in Attachment 1.
Yes
No
The language of R1 and M1 does not support the DSR SDT’s goal of having a single form and system for reporting. The standard should specify the form and system rather than deferring that decision to the ERO. The language of R1 and M1 leaves the form and system to the ERO’s discretion, which could lead to multiple forms and frequent revisions to them. This would lead to difficulties in tracking the reporting requirements. In addition, it is impossible to comment intelligently regarding the overall impact of the proposed standard and its requirements and measures without the reporting form and system being specified in the standard.
No
While the concept of an operating plan is reasonable, the requirements for update in sections 2.7, 2.8 and 2.9 will lead to an immense amount of work for the entities subject to the standard. In addition, constant revisions to the operating plan makes it difficult to cement a habit through this procedure. The proposed update schedule does not strike the appropriate balance between the need to respond to lessons learned and the value of plan continuity.
Yes

However, this requirement doesn't address the timing required for this analysis. This may be intentional and appreciated because at times the analysis can take months when the events are complex in nature.
Yes
No
The fact that proposed requirement R2 will require frequent updates to the operating plan means that the training required under this plan will occur quite frequently as well, leading to operator confusion. Even the comment allowing a review and “sign-off” will not completely mitigate this result.
Yes
It is assumed that for the purposes of M6, NERC and the regions would already have access to these reports.
No
This is adequately covered by section 802 of the Rules of Procedure. There seems to be some conflict between R2.9 and R8 regarding timeframes and the specific elements required.
No
The proposed standard does not adequately ensure that the impact events subject to its requirements are limited to those listed in Attachment 1. In order to ensure that this is true, the term “impact event” should be a defined term and that definition should clearly limit impact events to those listed in Attachment 1.
No
Attachment 2 is not referenced in the requirements of the proposed standard. As a result, it is not clear when its submission would be required.
No
With some of the tight timeframes for reporting, it is reasonable to focus on impact rather than motivation. Requiring further analysis of the event in order to assess the possibility that the event was caused by sabotage, however, may be necessary to address FERC’s concerns with respect to sabotage.
Yes
No
There are no effective dates listed in the proposed standard. The proposed effective date should allow at least one year for entities to implement the requirements of the standard. In addition, if requirement R1 remains, then the requirement to implement an operating plan should only be triggered by the ERO’s finalization of the form and system for reporting impact events and should provide at least six months for the implementation of the operating plan.
Yes
The DSR SDT’s concepts for implementing a new structure for reporting are appropriate. Proper implementation of those concepts is likely to result in a very much improved standard. However, the proposed standard falls well short of implementing the concepts and is not much of an improvement on the current standard.
Group
Midwest ISO Standards Collaborators
Jason L. Marshall
Yes
No
While we agree with the list of functional entities identified in the Applicability Section, we do not agree with their application in Attachment 1. As the functional entities are identified in Attachment 1, there is likely going to be duplicate reporting. Why should both the RC and BA submit a report for an energy emergency requiring public appeals?
Yes
No
We disagree with requiring an Operating Plan for identifying, assessing, and reporting impact events. This is an administrative requirement that has no clear reliability benefit. Furthermore, it is questionable that event reporting even meets the basic definition of an Operating Plan. Per the NERC glossary of terms, Operating Plans contain Operating Procedures or Operating Processes which encompass taking action real-time on the BES not reporting on it. What is an impact event? It appears that this undefined, ambiguous term was substituted for sabotage which is also undefined and ambiguous. One of the SARs stated goals was to “provide clarity on sabotage events”. This does not provide clarity.
No
While we agree that it makes sense to report on the cause of an event, we disagree with the need for an Operating Plan as identified in R2.

No
We disagree with the need to conduct a drill for reporting.
No
We disagree with the need to provide formal training. We could agree with the need to communicate to System Operators and other pertinent personnel the criteria for reporting so that they know when system events need to be reported.
No
We believe the reporting time lines are too aggressive for some events. Reporting events within an hour is not reasonable as an entity may still be dealing the event. This will particularly difficult when support personnel are not present such as during nights, holidays and weekends.
No
We do not agree with the requirements and we do not believe it is adequately covered in section 802. First, section 802 deals with assessments not event reporting. Secondly, since attachment 1 is part of a standard, it should not be modified outside of the Reliability Standards Development process.
No
Several categories require duplicate reporting. For instance, the first three categories regarding energy emergencies could be interpreted to require the BA and RC to both report. The reporting responsibilities in this table should be clarified based on who has primary reporting responsibility for the task per the NERC Functional Model and require only one report. For instance, since balancing load, generation and interchange is the primary function of a BA per the NERC Functional Model, only the BA should be required to provide this report. As another option, perhaps the registered entity initiating the action should submit the report. If the BA did not take action and the RC had to direct the BA to take action, one could argue that perhaps the RC should submit the report then. However, if the BA takes action appropriately on their own, the BA should submit it. If the TOP reduces voltage for a capacity and energy emergency per a directive of the BA, then the BA should report the event.
No
This form differs from the DOE reporting forms. We do not believe different reporting forms should be required. The DOE form should be sufficient for NERC reporting. It is not clear what benefit providing the Compliance Registration ID number provides. Many of the registered entities employees that will likely have to submit the report, particularly given the one-hour reporting requirement for some impact events, will not be aware of this registration ID. However, they will know for what functions they are registered. We recommend removing the need to enter this compliance registration ID or extending the time frame for reporting to allow back office personnel to complete the form. For item two, please change “Time/Zone:” with “Time (include time zone)”. As written it is a little confusing.
No
We believe the SAR scope regarding addressing sabotage has not been addressed at all. It appears that impact event essentially replaces sabotage. This standard needs to make it clear that sabotage, in some cases, cannot be identified until an investigation is performed by the appropriate policing agencies such as the FBI. Intent plays an important role in determining sabotage and only these agencies are equipped to make these assessments.
No
It appears that all requirements have been addressed from the existing standards. However, we believe there is a reliability gap that continues from the existing standards because sabotage is not defined any better than in the existing standards.
Yes
Yes
We are concerned with the Future Development Plan. It shows an initial ballot period starting in December. This standard has significant issues and will need another distinct comment period (and not the formal comment period in parallel with balloting) prior to balloting.
Group
IRC Standards Review Committee
Ben Li
No
The proposed requirements in the standard are not focused on the core industry concern that current requirements are unclear as to what types of events warrant entities to report. Per draft 2 of the SAR, “The existing requirements need to be revised to be more specific – and there needs to be more clarity in what sabotage looks like.” Instead this proposed standard includes requirements that are more focused on “how” to report, rather than “what” to report. The SAR states that: “The development may include other improvements to the standards deemed appropriate by the drafting team, with consensus on the stakeholders (emphasis added), consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.” The SRC believes the scope of the SAR, and likewise the proposed standard, is inappropriate to the fundamental reliability purpose of what events need to be reported. The proposed administrative requirements are difficult to interpret, implement and measure, and do not clarify what type of

sabotage information entities need to report. Although the use of procedures and an understanding by those personnel accountable seem helpful for ensuring reports are made, the fundamental purpose of clarifying what types of events should be reported and more importantly what types do not have to be reported, is lacking in the standard. Also, one of the first issues identified in the SAR for consideration by the drafting team seems to be ignored, “Consider whether separate, less burdensome requirements for smaller entities may be appropriate.” The requirements for entities to develop Operating Plans and to have training for those plans, further adds uncertainty and increases complexity of how entities, large and small, will have to comply with this standard.
No
Entities that have information about possible sabotage events should report these to NERC after the fact and the standard should simply reflect that. While we agree with the list of functional entities identified in the Applicability Section, we do not agree with their application in Attachment 1. As the functional entities are identified in Attachment 1, there is likely going to be duplicate reporting. Why should both the RC and BA submit a report for an EEA for example?
Yes
Note that ERCOT does not sign on to this particular comment.
No
The SRC suggests that this is not, in fact, an Operating Plan. At most, it may be a reporting plan or reporting procedure. Most of these requirements are administrative and procedural in nature and, therefore, do not belong as requirements in a Reliability Standard. Perhaps they could be characterized as a best practice and have an associated set of Guidelines developed and posted on the subject. As proposed, the Operating Plan is not required to ensure bulk power reliability. As stated in the purpose of this standard, it does not cover any real-time operating notifications for the types of events covered by CIP-001, EOP-004. The Operating Plan requirements as proposed seem only to be suitable for real-time notifications. Since these incidents are meant to be reportable after-the-fact, familiarity with the reporting requirements and time frames is sufficient. Unlike the real-time operating notifications which have relatively short reporting time frames, there is sufficient time for personnel to make appropriate communications within their organizations to make timely after the fact reports under NERC Section 1600 authority. Would it be feasible for NERC to issue a standing requirement for timely after-the-fact reports under NERC Section 1600 authority?
No
Although it is useful for entities to make an initial assessment of a probable cause of an event, this requirement should stand alone and does not need to be tied to requirement R2, Operating Plan. Quite often, it takes quite some time for an actual cause to be determined. The determination process may require a root cause analysis of some complexity. Further, in the case of suspected or potential sabotage, the industry can only say it doesn’t know, but it may be possible. It really is the law enforcement agencies who make the determination of whether sabotage is involved and the info may not be made available until an investigation is completed, if indeed it is ever made available.
No
Similar to our comments on R2 for an Operating Plan, a drill, exercise, or Real-time implementation of its Operating Plan for reporting is unnecessary. Such things are really training practices. There are already existing standards requirements regarding training. There is no imminent threat to reliability that requires these events to be reported in a short time frame as may be required for real-time operating notifications.
No
We do not agree with the need for R5. We do not see the need for a standard requirement that stipulates training the personnel on reporting events. What matters is that the reports are provided to the needed organizations or entities on time and in the required format according to established procedure. Stipulating a training requirement to achieve this reporting is micro-managing and overly prescriptive.
No
There is not a need for an Operating Plan as proposed. This is not truly an Operating Plan. There are already other standards which create the requirements for an Operating Plan. This is an administrative reporting plan and any associated impact upon reliability is far beyond real-time operations.
No
We do not support an annual time frame to update the events list. The list should be updated as needed through the Reliability Standards Development Process. Any changes to a standard must be made through the standards development process, and may not be done at the direction of the ERO without going through the process.
No
We do not agree with the requirement to report “detection of a cyber intrusion to critical cyber assets” as this creates a double jeopardy situation between CIP-008 and EOP-004-2 R2.6. We suggest that physical incident reporting be part of EOP-004 and cyber security reporting be part of CIP-008.
No
Attachment 2 is not referenced in the standard requirements. Is it a part of the standard that an entity must use to file the impact event reports to a specific recipient. If so, this needs to be referenced in the standard. We question the need for using a fixed format for reports that vary from “shedding firm load” to “damaging equipment”. The nature of impact events varies from one event to another and hence a fixed format or pre-determined form may not be able to provide

the appropriate template that is suitable for use for all events. We urge the SDT to reconsider the use of Attachment 2 for reporting events, with due consideration to the actual intent of the standard (as pointed out in our comments under Q1).
No
This term and the FERC directive do not recognize limitations in what a registered entity can do to determine whether an act of sabotage has been committed. This term should recognize law enforcement's and other specialized agencies', including international agencies', role in defining acts of sabotage and not hold the registered entity wholly responsible to do so.
No
If the training and Operation Plan requirements are adopted as proposed, this may not be sufficient time for some entities to comply, particularly those with limited number of staff but perform functions that have multiple event reporting requirements.
No
The standards should be changed to define what a "disturbance" is for reporting in EOP-004. Also, sabotage reporting requirements in CIP-001 should be rescinded as EOP-004 already has such requirements.

Consideration of Comments on Disturbance and Sabotage Reporting — Project 2009-01

The Disturbance and Sabotage Reporting Drafting Team thanks all commenters who submitted comments on its preliminary draft of EOP-004-2 – Impact Event and Disturbance Assessment, Analysis, and Reporting. This standard was posted for a 30-day informal comment period from September 15, 2010 through October 15, 2010. Stakeholders were asked to provide feedback on the standard through a special Electronic Comment Form. There were 60 sets of comments, including comments from more than 175 different people from approximately 100 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

In this report, the comments have been sorted by question number so that it is easier to see where there is consensus. The comments are posted in their original format on the following project page:

http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Based on stakeholder comments, and also on the results of the observations made by the Quality Review team, the drafting team made the following significant changes to the standard following the posting period that ended on October 15, 2011.

Scope: A common thread through most of the comments was that the DSR SDT went beyond the reliability intent of the standard (reporting) and concentrated too much on the analysis of the event. The DSR SDT agrees with this response, and revised the purpose as follows:

> *Original Purpose:* Responsible Entities shall report impact events and their known causes to support situational awareness and the reliability of the Bulk Electric System (BES).
>
> *Revised Purpose:* To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of Impact Events and their causes, if known, by the Responsible Entities.

Definitions:

> **Impact Event:** The DSR SDT had proposed a working definition for "impact events" to support EOP-004 - Attachment 1 as follows:
>
> "An impact event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action."
>
> Many stakeholders indicated that the definition should be added to the NERC Glossary and the DSR SDT adopted this suggestion.
>
> The types of Impact Events that are required to be reported are contained within EOP-004 - Attachment 1. Only the events identified in EOP-004 – Attachment 1 are required to be reported under this Standard.
>
> **Sabotage:** FERC Order 693, paragraph 471 states in part: ". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide

guidance as to the triggering events that would cause an entity to report a sabotage event."

The DSR SDT made a conscious, deliberate decision to exclude a strict definition of sabotage from this standard and sought stakeholder feedback on this issue. Some suggested adopting the NRC definition of the term sabotage, and the DSR SDT did consider adopting the NRC definition shown below but determined that the definition is too narrowly focused.

Any deliberate act directed against a plant or transport in which an activity licensed pursuant to 10 CFR Part 73 of NRC's regulations is conducted or against a component of such a plant or transport that could directly or indirectly endanger the public health and safety by exposure to radiation.

Most respondents agreed that in order to be labeled as an act of sabotage, the intent of the perpetrators must be known. The team felt that it was almost impossible to determine if an act or event was that of sabotage or merely vandalism without the intervention of law enforcement after the fact. This would result in further ambiguity with respect to reporting events, and the timeline associated with the reporting requirements does not lend itself to the in-depth analysis required to identify a disturbance (or potential disturbance) as sabotage. The SDT felt that a likely consequence of having to meet this criterion, in the time allotted, would be an under-reporting of events. Accordingly, all references to sabotage have been deleted from the standard.

Instead, the SDT concentrated on providing clear guidance on the events that should trigger a report. The SDT believes that this more than adequately meets the reliability intent of the Commission as expressed in paragraph 471 of Order 693 in an equally efficient and effective manner.

Situational Awareness versus Industry Awareness: Some commenters correctly pointed out that "situational awareness" is a desirable by-product of an effective event reporting system, and not the driver of that system. Accordingly, all references to "situational awareness" have been deleted from the standard. The more generic "industry awareness" has been substituted where appropriate.

Applicability:

The DSR SDT had protracted discussions on the applicability of this standard to the LSE. Per the Functional Model, the LSE does not own assets and therefore should not be an applicable entity (no equipment that could experience a "disturbance"). However, the Registry Criteria contains language that could imply that the LSE does own assets, or is at least responsible for assets. In addition, the DSR SDT modified Attachment 1 to include reporting of damage or destruction of Critical Cyber Assets per CIP-002. The LSE, as well as the Interchange Authority and Transmission Service Provider are applicable entities under CIP-002 and should be included for Impact Events under EOP-004.

There were several comments that the asset owners (GO/TO) would be less likely than the asset operators (GOP/TOP) to be aware of an impact event. The DSR SDT recognizes that this may be true in some cases, but not all. In order to meet the reliability objectives of this requirement, the applicability for GO/TO will remain as per Attachment 1.

Requirement R1:

Based on stakeholder comments, Requirement R1, which assigned the ERO the responsibility for collecting and distributing impact event reports was deleted. There was strong support for a central system for receiving and distributing impact event reports (a/k/a one stop shopping). There was general agreement that NERC was the most likely, logical entity to perform that function. However several respondents expressed their concern that the ERO could not be compelled to do so by a requirement in a Reliability Standard (not a User, Owner or Operator of the BES). In their own comments, NERC did not oppose the concept, but suggested that the more appropriate place to assign this responsibility would be the NERC Rules of Procedure. The DSR SDT concurs. The DSR SDT has removed the requirement from the standard and is proposing to make revisions to the NERC Rules of Procedure as follows:

> 812. NERC will establish a system to collect impact event reports as established for this section, from any Registered Entities, pertaining to data requirements identified in Section 800 of this Procedure. Upon receipt of the submitted report, the system shall then forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, and regulatory agencies as necessary. These reports shall be forwarded to the Federal Energy Regulatory Commission for impact events that occur in the United States. The ERO shall solicit contact information from Registered Entities appropriate governmental, law enforcement and regulatory agencies for distributing reports.

Requirement R2 (now R1 in the revised standard):

There were objections to the use of the term "Operating Plan" to describe the procedure to identify and report the occurrence of a disturbance. The DSR SDT believes that the use of a defined term is appropriate and has revised Requirement R1 to include Operating Plan, Operating Process and Operating Procedure.

Many commenters felt that the requirements around updating the Operating Plan were too prescriptive, and impossible to comply with during the time frame allowed. The DSR SDT agrees, and Requirement R2, Parts 2.5 through 2.9 have been eliminated. They have been replaced with Requirement R1,Part 1.4 to require updating the Impact Event Operating Plan within 90 days of any change to content.

R1. Each Responsible Entity shall have an Impact Event Operating Plan that includes: *[Violation Risk: Factor Medium] [Time Horizon: Long-term Planning]*:

1.1. An Operating Process for identifying Impact Events listed in Attachment 1.

1.2. An Operating Procedure for gathering information for Attachment 2 regarding observed Impact Events listed in Attachment 1.

1.3. An Operating Process for communicating recognized Impact Events to the following:

1.3.1 Internal company personnel notification(s).

1.3.2. External organizations to notify to include but not limited to the Responsible Entities' Reliability Coordinator, NERC, Responsible Entities' Regional Entity, Law Enforcement, and Governmental or Provincial Agencies.

1.4. Provision(s) for updating the Impact Event Operating Plan within 90 days of any change to its content.

Other requirements reference the Operating Plan as appropriate. The requirements of EOP-004-2 fit precisely into the definition of Operating Plan:

> Operating Plan: A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan.

Requirement R3 (now R2 in the revised standard):

Requirement R3 has been re-written to exclude the requirement to "assess the initial probable cause". The only remaining reference to "cause" is in the Impact Event Reporting Form (Attachment 2). Here, there is no longer a requirement to assess the probable cause. The probable cause only needs to be identified, and only if it is known at the time of the submittal of the report.

> R2. Each Responsible Entity shall implement its Impact Event Operating Plan documented in Requirement R1 for Impact Events listed in Attachment 1 (Parts A and B). *[Violation Risk: Factor Medium] [Time Horizon: Real-time Operations and Same-day Operations]*

Requirement R4 (now R3 in the revised standard):

The DSR SDT did a full review based on comments that were received. R3 now is stream lined to read:

> R3. Each Responsible Entity shall conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 at least annually, with no more than 15 months between such tests. .

The testing of the Operating Process for communicating recognized Impact Events (as stated in R1) is the main component of this requirement. Several commenters provided input that too much "how" was previously within R3 and the DSR DST should only provide the "what". The DSR SDT did not provide any prescriptive guidance on how to accomplish the required testing within the rewrite. Testing of the entity's procedure (R1) could be by an actual exercise of the process (testing as stated in FERC Order 693 section 471), a formal review process or real time implementation of the procedure. The DSR SDT reviewed Order 693 and section 465 directs that processes are "verify that they achieve the desired result". This is the basis of R3, above.

Requirement R5 (now R4 in the revised standard):

The DSR SDT did a full review based on comments that were received. The major issues that

were provided by commenters involved the inclusion of Requirement R5, Part 5.3 and Part 5.4.

5.3 If the Operating Plan is revised (with the exception of contact information revisions), training shall be conducted within 30 days of the Operating Plan revisions.

5.4 For internal personnel added to the Operating Plan or those with revised responsibilities under the Operating Plan, training shall be conducted prior to assuming the responsibilities in the plan.

Upon detailed review the DSR SDT agrees with the majority of comments received regarding Requirement R5, Parts 5.3 and 5.4 and has removed Parts 5.3 and 5.4 completely from the Standard. Training is still the main theme of this requirement (now R4) as it pertains to the personnel required to implement the Impact Event Operating Plan (R1).

R4 now is stream lined to read:

> R4. Each Responsible Entity shall review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan at least annually with no more than 15 calendar months between review sessions

Requirement R6 (now R5 in the revised standard):

The DSR SDT did a full review based on comments that were received. Many comments received identified concerns on the reporting time lines within Attachment 1., Several commenters wanted the ability to report impact events to their responsible parties via the DOE Form OE-417. Upon discussions with the DOE and NERC, the DSR SDT has added the ability to use the DOE Form OE-417 when the same or similar items are required to be reported to NERC and the DOE. This will reduce the need to file multiple forms when the same or similar events must be reported to the DOE and NERC. The reliability intent of reporting impact events within prescribed guidelines, to provide industry awareness and to start any required analysis processes can be met without duplicate reporting R5 now is stream lined to read:

> R5. Each Responsible Entity shall report Impact Events in accordance with its Impact Event Operating Plan pursuant to Requirement R1 and Attachment 1 using the form in Attachment 2 or the DOE OE-417 reporting form.

Requirements R7 and R8:

The DSR SDT did a full review based on comments that were received. The DSR SDT has determined that R7 and R8 are not required to be within a NERC Standard since Section 800 of the Rules of Procedure already assigns this responsibility to NERC.

Attachment 1:

The DSR SDT did a full review based on comments that were received. The DSR SDT, the Events Analysis Working Group (EAWG), NERC Staff (to include NERC Senior VP and Chief Reliability Officer) had an open discussion involving this topic. The EAWG and the DSR SDT aligned Attachment 1 with the Event Analysis Program category 1 analysis responsibilities. This will assure that impact events in EOP-004-2 reporting requirements are the starting vehicle for any required Event Analysis within the NERC Event Analysis Program. The DSR SDT reviewed the "hierarchy" of reporting within Attachment 1. To reduce multiple entities reporting the same impact event, the DSR SDT has stated that the entity that performs the action or is directly

affected by an action will report per EOP-004-2. As an example, during a system emergency, the TOP or RC may request manual load shedding by a DP or TOP. The DP or TOP would have the responsibility to report the action that it took if it meets or exceeds the bright-line criteria established in Attachment 1. Upon reporting, the NERC Event Analysis Program would be made aware of the impact event and start the Event Analysis Process which is outside the scope of this Standard. Several bright-line criteria were removed from Attachment 1. These criteria (DC converter station, 5 generator outages, and frequency trigger limits) were removed after discussions with the EAWG and NERC staff, who concurred that these items should be removed from a reporting standard and analysis process.

Several respondents expressed concern that the reporting requirements were redundant. The general sentiment was that unclear responsibility to report a disturbance could trigger a flood of event reports. Attachment 1 has been modified to assign clear responsibility for reporting, for each category of Impact Event.

Some commenters indicated a concern that the list of events in Attachment 1 isn't as comprehensive as the existing standard since the existing standard includes bomb threats and observations of suspicious activities. Others commented that the impact event list should include deliberate acts against infrastructure. The DSR SDT believes that "observation of suspicious activity" and "bomb threats" are addressed in Attachment 1 Part B – "Risk to BES equipment from a non-environmental physical threat". The SDT has added the phrase, "and report of suspicious device near BES equipment" to note 3 of the "Attachment 1, Potential Reliability – Part B" for additional clarity.

Attachment 2:

The proposed Impact Event Report (Attachment 2) generated comments regarding the duplicative nature of the form when compared to the OE-417. The DSR SDT has added language to the proposed form to clarify that NERC will accept a DOE OE-417 form in lieu of Attachment 2 if the responsible entity is required to submit an OE-417 form.

In collaboration with the NERC Event Analysis Working Group (EAWG) the DSR SDT modified the attachment to eliminate confusion. This revised form will be Attachment 2 of the Standard and collects the only information required to be reported for EOP-004-2. Further information may be requested through the Events Analysis Process (NERC Rules of Procedure), but the collection of this information is outside of the scope of EOP-004.

The DSR SDT has also clarified what the form's purpose with the following addition to the form:

> "This form is to be used to report impact events to the ERO."

Other Standard Issues:

The DSR SDT proposed that combining EOP-004 and CIP-001 would not introduce a reliability gap between the existing standards and the proposed standard and the industry comments received confirms this.

Several entities expressed their concern with the fact that Attachment 1 contained most of the elements already called for in the OE-417. The DSR SDT agrees, and Attachment 1 part 1 has

been modified to even more closely mirror the Department of Energy's OE-417 Emergency Incident and Disturbance Report form. Additionally, the standard has been modified to allow for the use of the OE-417.

There was some concern expressed that there could be confusion between the reporting requirements in this standard, and those found in CIP-008. The DSR SDT agrees, and Attachment 1 Part B, has been modified to provide the process for the reporting of a Cyber Security Incident.

The DSR SDT also believes NERC's additional concern about what data is applicable is addressed by the revisions to Attachment 1, and the inclusion of the OE-417 as an acceptable interim vehicle.

Implementation Plan:

The DSR SDT asked stakeholders to provide feedback on the proposed effective date which provided entities at least a year following board approval of the standard. Most stakeholders supported the one year minimum, however based on the revisions made to the requirements, the drafting team is now proposing that this time period be shortened to between six months and nine months. The current CIP-001 plan is adequate for the new EOP-004 and training should be met in the proposed timeline. Note that the Implementation Plan was developed for the revised Requirements, which do not include an electronic "one-stop shopping" tool. The tool for 'one stop shopping' will be addressed in the proposed revisions to the NERC Rules of Procedure.

The industry commented on the need for e-mail addresses and fax numbers for back up purposes. These details were added to the standard and the implementation plan.

The proposed ballot in December was incorrect and has been deleted from the future development plan. The plan was updated with the correct project plan dates.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Herb Schrayshuen, at 609-452-8060 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

Index to Questions, Comments, and Responses

1. ***Do you agree with the purpose statement of the proposed standard? Please explain in the comment box below. …. ……19***
2. ***Do you agree with the applicable entities in the Applicability Section as well as assignment of applicable entities noted in Attachment 1? Please explain in the***

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

comment box below. …. ……35

3. *Do you agree with the requirement R1 and measure M1? Please explain in the comment box below. …. ……53*
4. *Do you agree with the requirement R2 and measure M2? Please explain in the comment box below. …. ……67*
5. *Do you agree with the requirement R3 and measure M3? Please explain in the comment box below. …. ……90*
6. *Do you agree with the requirement R4 and measure M4? Please explain in the comment box below. …. ……103*
7. *Do you agree with the requirement R5 and measure M5? Please explain in the comment box below. …. ……115*
8. *Do you agree with the requirement R6 and measure M6? Please explain in the comment box below …. ……132*
9. *Do you agree with the requirements for the ERO (R7-R8) or is this adequately covered in the Rules of Procedure (section 802)? Please explain in the comment box below. …. ……143*
10. *Do you agree with the impact event list in Attachment 1? Please explain in the comment box below and provide suggestions for additions to the list of impact events. ……155*
11. *Do you agree with the use of the Preliminary Impact Event Report (Attachment 2)? ……182*
12. *The DSR SDT has replaced the terms "disturbance" and "sabotage" with the term "impact events". Do you agree that the term "impact events" adequately replaces the terms "disturbance" and "sabotage" and addresses the FERC directive to "further define sabotage" in an equally efficient and effective manner? Please explain in the comment box below……192*
13. *The DSR SDT has combined EOP-004 and CIP-001 into one standard (please review the mapping document that shows the translation of requirements from the already approved versions of CIP-001 and EOP-004 to the proposed EOP-004), EOP-004-3 and retiring CIP-001. Do you agree that there is no reliability gap between the existing standards and the proposed standard?……201*
14. *Do you agree with the proposed effective dates? Please explain in the comment box below……207*

15. Do you have any other comments that you have not identified above?.....213

The Industry Segments are:

1 — Transmission Owners

2 — RTOs, ISOs

3 — Load-serving Entities

4 — Transmission-dependent Utilities

5 — Electric Generators

6 — Electricity Brokers, Aggregators, and Marketers

7 — Large Electricity End Users

8 — Small Electricity End Users

9 — Federal, State, Provincial Regulatory or other Government Entities

10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Gregory Campoli	New York Independent System Operator	NPCC	2
3.	Kurtis Chong	Independent Electricity System Operator	NPCC	2

Group/Individual	Commenter	Organization		Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
4.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC		1								
5.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC		1								
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC		10								
7.	Dean Ellis	Dynegy Generation	NPCC		5								
8.	Brian Evans-Mongeon	Utility Services	NPCC		8								
9.	Mike Garton	Dominion Resources Services, Inc.	NPCC		5								
10.	Brian L. Gooder	Ontario Power Generation Incorporated	NPCC		5								
11.	Kathleen Goodman	ISO - New England	NPCC		2								
12.	Chantel Haswell	FPL Group, Inc.	NPCC		5								
13.	David Kiguel	Hydro One Networks Inc.	NPCC		1								
14.	Michael R. Lombardi	Northeast Utilities	NPCC		1								
15.	Randy MacDonald	New Brunswick System Operator	NPCC		2								
16.	Bruce Metruck	New York Power Authority	NPCC		6								
17.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC		10								
18.	Robert Pellegrini	The United Illuminating Company	NPCC		1								
19.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC		1								
20.	Saurabh Saksena	National Grid	NPCC		1								
21.	Michael Schiavone	National Grid	NPCC		1								

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
22.		Peter Yost	Consolidated Edison Co. of New York, Inc. NPCC		3								
2.	Group	Jim Case, SERC OC Chair	SERC OC Standards Review Group	X		X							

Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Garton	Dominion Virginia Power	SERC	1, 3
2.	Jim Griffith	Southern	SERC	1, 3, 5
3.	Vicky Budreau	Santee Cooper	SERC	1, 3, 5, 9
4.	Gerry Beckerle	Ameren	SERC	1, 3
5.	Eugens Warnecke	Ameren	SERC	1, 3
6.	Scott McGough	Oglethorpe Power	SERC	5
7.	John Neagle	AEC I	SERC	1, 3, 5
8.	Joel Wise	TVA	SERC	1, 3, 5, 9
9.	Jennifer Weber	TVA	SERC	1, 3, 5, 9
10.	Robert Thomasson	BREC	SERC	1, 3, 5, 9
11.	Derek Bleyle	SCE&G	SERC	1, 3, 5
12.	Gene Delk	SCE&G	SERC	1, 3, 5
13.	Dave Plauck	Calpine	SERC	5

Group/Individual	Commenter	Organization			Registered Ballot Body Segment									
					1	2	3	4	5	6	7	8	9	10
14.	Tom Hanzlik	SCE&G	SERC	1, 3, 5										
15.	Randy Castello	Mississippi Power	SERC	1, 3, 5										
16.	Doug White	NCEMC	SERC	1, 3, 5, 9										
17.	Randy Haynes	Alcoa	SERC	1, 5										
18.	Joel Rogers	SMEPA	SERC	1, 3, 5, 9										
19.	Mike Bryson	PJM	SERC	2										
20.	Rick Meyers	EEI	SERC	1, 5										
21.	Tim Hattaway	PowerSouth	SERC	1, 3, 5, 9										
22.	Barry Warner	EKPC	SERC	1, 3, 5, 9										
23.	Jack Kerr	Dominion Virginia Power. P.	SERC	1, 3										
24.	Wes Davis	SERC Reliability Corp.	SERC	10										
25.	John Troha	SERC Reliability Corp.	SERC	10										
3.	Group	Brad Jones	Luminant Energy							X				
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1.	Kevin Phillips	Luminant Energy	ERCOT	6										
4.	Group	David Grubbs	City of Garland		X									
	Additional Member	**Additional Organization**	**Region**	**Segment**										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Selection										
1.		David Grubbs	ERCOT 1										
2.		Fred Sherman	ERCOT 1										
3.		Steve Zaragoza	ERCOT 1										
4.		Billy Lee	ERCOT 1										
5.		Heather Siemens	ERCOT 1										
6.		Ronnie Hoeinghaus	ERCOT 1										
7.		Matt Carter	ERCOT 1										
5.	Group	Terry L. Blackwell	Santee Cooper	X		X		X	X				
Additional Member		**Additional Organization**	**Region** / **Segment Selection**										
1.		S. T. Abrams	Santee Cooper SERC 1										
2.		Rene' Free	Santee Cooper SERC 1										
3.		Vicky Budreau	Santee Cooper SERC 1										
4.		Glenn Stephens	Santee Cooper SERC 1										
6.	Group	Steve Alexanderson	Pacific Northwest Small Public Power Utility Comment Group			X	X						

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

Additional Member	Additional Organization	Region	Segment Selection
1.	Russell Noble	Cowlitz County PUD No. 1	WECC 3, 4, 5
2.	Dave Proebstel	Clallam County PUD	WECC 3
3.	Ronald Sporseen	Blachly-Lane Electric Cooperative	WECC 3
4.	Ronald Sporseen	Central Electric Cooperative	WECC 3
5.	Ronald Sporseen	Clearwater Power Company	WECC 3
6.	Ronald Sporseen	Douglas Electric Cooperative	WECC 3
7.	Ronald Sporseen	Consumers Power	WECC 3
8.	Ronald Sporseen	Fall River Rural Electric Cooperative	WECC 3
9.	Ronald Sporseen	Northern Lights	WECC 3
10.	Ronald Sporseen	Lane Electric Cooperative	WECC 3
11.	Ronald Sporseen	Lincoln Electric Cooperative	WECC 3
12.	Ronald Sporseen	Raft River Rural Electric Cooperative	WECC 3
13.	Ronald Sporseen	Lost River Electric Cooperative	WECC 3
14.	Ronald Sporseen	Salmon River Electric Cooperative	WECC 3
15.	Ronald Sporseen	Umatilla Electric Cooperative	WECC 3

Group/Individual		Commenter	Organization		Registered Ballot Body Segment									
					1	2	3	4	5	6	7	8	9	10
16.		Ronald Sporseen	Coos-Curry Electric Cooperative	WECC		3								
17.		Ronald Sporseen	West Oregon Electric Cooperative	WECC		3								
18.		Ronald Sporseen	Pacific Northwest Generating Cooperative	WECC		5								
19.		Ronald Sporseen	Power Resources Cooperative	WECC		5								
7.	Group	Mallory Huggins	NERC Staff											

	Additional Member	Additional Organization	Region	Segment Selection
1.	Earl Shockley	NERC	NA - Not Applicable	NA
2.	Dave Nevius	NERC	NA - Not Applicable	NA
3.	Gerry Adamski	NERC	NA - Not Applicable	NA
4.	Roman Carter	NERC	NA - Not Applicable	NA

8.	Group	Carol Gerou	MRO's NERC Standards Review Subcommittee											X

Additional Member	Additional Organization	Region	Segment Selection
1.	Mahmood Safi	Omaha Public Utility District	MRO	1, 3, 5, 6
2.	Chuck Lawrence	American Transmission Company	MRO	1

Group/Individual	Commenter	Organization		Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Tom Webb	WPS Corporation	MRO	3, 4, 5, 6									
4.	Jodi Jenson	Western Area Power Administration	MRO	1, 6									
5.	Ken Goldsmith	Alliant Energy	MRO	4									
6.	Alice Murdock	Xcel Energy	MRO	1, 3, 5, 6									
7.	Dave Rudolph	Basin Electric Power Cooperative	MRO	1, 3, 5, 6									
8.	Eric Ruskamp	Lincoln Electric System	MRO	1, 3, 5, 6									
9.	Joseph Knight	Great River Energy	MRO	1, 3, 5, 6									
10.	Joe DePoorter	Madison Gas & Electric	MRO	3, 4, 5, 6									
11.	Scott Nickels	Rochester Public Utilties	MRO	4									
12.	Terry Harbour	MidAmerican Energy Company	MRO	1, 3, 5, 6									
9. Group	Sam Ciccone	FirstEnergy		X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Dave Folk	FE	RFC	
2.	Doug Hohlbaugh	FE	RFC	
3.	Andy Hunter	FE	RFC	
4.	Kevin Querry	FE	RFC	
5.	Brian Orians	FE	RFC	

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
6. John Martinez	FE	RFC										
7. John Reed	FE	RFC										
8. Marissa McLean	FE	RFC										
9. Phil Bowers	FE	RFC										
10. Group	Mike Garton	Electric Market Policy	X		X		X	X				

Additional Member	Additional Organization	Region	Segment Selection
1.	Michael Gildea	Dominion	NPCC 5
2.	Louis Slade	Dominion	SERC 6
3.	John Loftis	Dominion Virginia Power	SERC 1

11. Group	Denise Koehn	Bonneville Power Administration	X		X		X	X				

Additional Member	Additional Organization	Region	Segment Selection
1.	Jim Burns	BPA, Transmission, Technical Operations	WECC 1
2.	Russell Funk	BPA, Transmission, DCC Data System Hardware	WECC 1
3.	John Wylder	BPA, Transmission, CC HW Dsgn/Stds Montr & Admin	WECC 1

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
12.	Group	Kenneth D. Brown	PSEG Companies	X		X		X	X				

Additional Member	Additional Organization	Region	Segment Selection
1.	Ron Wharton	PSE&G System Ops	RFC	1, 3
2.	Jerzy Slusarz	PSEG Fossil	RFC	5, 6
3.	James Hebson	PSEG ER&T	ERCOT	5, 6
4.	Dominick Grasso	PSEG Power Connecticut	NPCC	5, 6

13.	Group	Steve Rueckert	WECC										X

Additional Member	Additional Organization	Region	Segment Selection	
1.	Tom Schneider	WECC	WECC	10
2.	John McGee	WECC	WECC	10

14.	Group	Richard Kafka	Pepco Holdings, Inc - Affiliates	X		X		X	X				

Additional Member	Additional Organization	Region	Segment Selection	
1.	Vic Davis	Delmarva Power & Light Co	RFC	1
2.	Dave Thorne	Potomac Electric Power Company	RFC	1

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
15.	Group	Howard Rulf	We Energies			X	X	X					

Additional Member	Additional Organization	Region	Segment Selection
1.	Tom Eells	We Energies RFC	3, 4, 5
2.	Fred Hessen	We Energies RFC	3, 4, 5
3.	Brian Heimsch	We Energies RFC	3, 4, 5

16.	Group	Annette M. Bannon	PPL Supply					X					

Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Heimbach	PPL Martins Creek, LLC RFC	5

17.	Group	J T Wood	Southern Company - Transmission	X		X							

Additional Member	Additional Organization	Region	Segment Selection
1.	Marc Butts	Southern Company Services SERC	1
2.	Andy Tillery	Southern Company Services SERC	1
3.	Jim Busbin	Southern Company Services SERC	1
4.	Phil Winston	Southern Company Services SERC	1

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
5.		Mike Sanders	Southern Company Services SERC 1										
6.		Bob Canada	Southern Company Services SERC 1										
7.		Boyd Nation	Southern Company Services SERC 1										
8.		Phil Whitmer	Georgia Power Company SERC 3										
9.		Randy Mayfield	Alabama Power Company SERC 3										
10.		Randy Castello	Mississippi Power Company SERC 3										
18.	Group	Jason L. Marshall	Midwest ISO Standards Collaborators		X								
Additional Member		**Additional Organization**	**Region** **Segment Selection**										
1.		Jim Cyrulewski	JDRJC Associates, LLC RFC 8										
2.		Kirit Shah	Ameren SERC 1										
3.		Robert A. Thomasson Sr.	Big Rivers SERC 1, 3										
19.	Group	Ben Li	IRC Standards Review Committee		X								
Additional Member		**Additional Organization**	**Region** **Segment Selection**										
1.		Bill Phillips	MISO MRO 2										
2.		Matt Goldberg	ISO-NE NPCC 2										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Charles Yeung	SPP	SPP 2										
4.	Mark Thompson	AESO	WECC 2										
5.	James Castle	NYISO	NPCC 2										
6.	Steve Myers	ERCOT	ERCOT 2										
7.	Greg Van Pelt	CAISO	WECC 2										
8.	Patrick Brown	PJM	RFC 2										
20.	Individual	Brian Pillittere	Tenaska					X					
21.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
22.	Individual	Jana Van Ness, Director Regulatory Compliance	Arizona Public Service Company	X		X		X	X				
23.	Individual	Brent Ingebrigtson	E.ON U.S. LLC	X		X		X	X				
24.	Individual	Brenda Lyn Truhe	PPL Electric Utilities	X									
25.	Individual	Greg Froehling	Green Country Energy					X					
26.	Individual	TransAlta Centralia Generation, LLC	TransAlta Corporation					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
27.	Individual	Doug Smeall	ATCO Electric Ltd.	X									
28.	Individual	Dan Roethemeyer	Dynegy Inc.					X					
29.	Individual	Kasia Mihalchuk	Manitoba Hydro	X		X		X	X				
30.	Individual	Philip Savage	PacifiCorp	X		X							
31.	Individual	Brian Reich	Idaho Power Company	X		X							
32.	Individual	Chris Hajovsky	RRI Energy, Inc.					X	X				
33.	Individual	Bill Keagle	BGE	X									
34.	Individual	John Brockhan	CenterPoint Energy	X									
35.	Individual	Joylyn Faust	Consumers Energy			X	X	X					
36.	Individual	Doug White	North Carolina Electric Coops			X	X	X					
37.	Individual	Lauri Jones	Pacific Gas and Electric Company	X		X		X					
38.	Individual	Laurie Williams	PNM Resources	X		X							
39.	Individual	Val Lehner	ATC	X									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
40.	Individual	Martin Bauer	US Bureau of Reclamation					X					
41.	Individual	Wayne Pourciau	Georgia System Operations Corporation			X	X						
42.	Individual	Rex Roehl	Indeck Energy Services					X					
43.	Individual	Jonathan Appelbaum	United Illuminating	X									
44.	Individual	Amir Y Hammad	Constellation Power Generation and Constellation Commodities Group					X	X				
45.	Individual	Carol Bowman	City of Austin dba Austin Energy	X									
46.	Individual	John Bee	Exelon	X		X		X					
47.	Individual	Kirit Shah	Ameren	X		X		X	X				
48.	Individual	Thad Ness	American Electric Power (AEP)	X		X		X	X				
49.	Individual	Joe Knight	Great River Energy	X		X		X	X				
50.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
51.	Individual	Nathan Lovett	Georgia Transmission Corporation	X									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
52.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X									
53.	Individual	Kathleen Goodman	ISO New England Inc.		X								
54.	Individual	Amanda Stevenson	E.ON Climate & Renewables					X					
55.	Individual	Christine Hasha	ERCOT ISO		X								
56.	Individual	Terry Harbour	MidAmerican Energy	X									
57.	Individual	Michael Gammon	Kansas City Power & Light	X		X		X	X				
58.	Individual	Ron Gunderson	Nebraska Public Power District	X		X		X					
59.	Individual	Dan Rochester	Independent Electricity System Operator		X								
60.	Individual	Catherine Koch	Puget Sound Energy	X									

1. Do you agree with the purpose statement of the proposed standard? Please explain in the comment box below.

Summary Consideration: Stakeholders who responded to this question were fairly evenly divided on acceptance of the original purpose statement with about half supporting the purpose and half suggesting revisions to the purpose. A common thread through most of the comments was that the DSR SDT went beyond the intent of the standard (reporting) and concentrated too much on the analysis of the event. Based on these comments, the SDT revised the purpose statement. The new purpose is:

> To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of Impact Events and their causes, if known, by the Responsible Entities.

Several commenters noted that the term, "impact event" is not a formally defined term. The DSR SDT has used a working definition for "impact events" to develop Attachment 1 as follows:

> An impact event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action.

Many stakeholders indicated that the definition should be added to the NERC Glossary and the DSR SDT adopted this suggestion.

The types of Impact Events that are required to be reported are contained within Attachment 1. Only these events are required to be reported under this Standard.

Some commenters correctly pointed out that "situational awareness" was a desirable by-product of an effective event reporting system, and not driver of that system. Accordingly, all references to "situational awareness" have been deleted from the standard. The more generic "industry awareness" has been substituted where appropriate.

Many commenters noted that the SDT did not define sabotage. FERC Order 693, paragraph 471 states in part: ". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event." The DSR SDT made a conscious, deliberate decision to exclude a strict definition of sabotage from this standard and sought

stakeholder feedback on this issue. Some suggested adopting the NRC definition of the term sabotage, and the DSR SDT did consider adopting the NRC definition shown below but determined that the definition is too narrowly focused.

> Any deliberate act directed against a plant or transport in which an activity licensed pursuant to 10 CFR Part 73 of NRC's regulations is conducted or against a component of such a plant or transport that could directly or indirectly endanger the public health and safety by exposure to radiation.

Most respondents agreed that in order to be labeled as an act of sabotage, the intent of the perpetrators must be known. The team felt that it was almost impossible to determine if an act or event was that of sabotage or merely vandalism without the intervention of law enforcement after the fact. This would result in further ambiguity with respect to reporting events, and the timeline associated with the reporting requirements does not lend itself to the in-depth analysis required to identify a disturbance (or potential disturbance) as sabotage. The SDT felt that a likely consequence of having to meet this criterion, in the time allotted, would be an under-reporting of events. Accordingly, all references to sabotage have been deleted from the standard.

Organization	Yes or No	Question 1 Comment
Ameren	No	The purpose talks about reporting impact events and their known causes. We have no problem with this generic intent, but the purpose says nothing about the very burdensome expectation of verbal updates to NERC and Regional Entities (Attachment 1, top of first page), Preliminary Impact Event Reports (Attachment 1, top of first page, are these Attachment 2?), "Actual" Impact Event Reports (Attachment 1 - Part A) and "Potential" Impact Event Reports (Attachment 1 - Part B). These multiple levels of reporting and events need to be greatly reduced.
American Electric Power (AEP)	No	It is unclear what the relationship between this project and the newly revamped NERC Event Analysis Process. We support moving towards one process opposed to separate obligations that may be in conflict.

Organization	Yes or No	Question 1 Comment
		In addition, AEP supports the concept of a central clearinghouse such as the RCIS that is shared by the industry. We support fewer punitive requirements and more prompting for using tools to make multiple entities aware of reliability related issues shortly after the fact.
CenterPoint Energy	No	CenterPoint Energy does not agree with the purpose statement of the proposed standard. The directive from the Commission in FERC Order 693 and restated in the Guideline and Technical Basis is "...the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: 1) further define sabotage and provide guidance as to the triggering events that would cause and entity to report a sabotage event." Instead the SDT has introduced another term, impact event, to address concerns regarding different definitions. The term, impact event and its proposed concept is too broad. Specifically the concept that an impact event "...has the potential to impact the reliability of the Bulk Electric System" leaves too much room for an entity and a regulatory body to have a difference of opinion as to whether an event should be reported. Required reporting should be limited to actual events. The reporting to follow could become overwhelming for the Responsible Entities, the ERO, and other various organization and agencies. Furthermore, situational awareness is a term that is associated with aspects of real-time. Given the analysis required before a report can be submitted, the report will not be real-time and will not sustain a purpose of supporting situational awareness. (See also comments on Q10 regarding the "Time to Submit Report".) A purpose that is more aligned with consolidation of the EOP-004 and CIP-001 standards would be as follows: Responsible Entities shall report disturbance events and acts of sabotage to support the reliability of the BES through industry awareness.
Consolidated Edison Co. of NY, Inc.	No	Comments: The purpose is not clear because it uses the term "impact events". This term should be a defined in the NERC glossary, and should not include words such as "potential".

Organization	Yes or No	Question 1 Comment
Duke Energy	No	The Purpose statement says that reporting under this standard supports situational awareness. However this is in conflict with Section 5. Background, where the DSR SDT makes clear that this standard includes no real-time operating notifications, and that this proposed standard deals exclusively with after-the-fact reporting. We also disagree with the stated concept of “impact event”. Including the phrase “or has the potential to impact” in the concept makes it impossibly broad for practical application and compliance.
Electric Market Policy	No	The term “impact events” does not draw a clear boundary around those events that are affected by this standard. Since this is not a defined term, nor is intended to be a defined term in the NERC glossary, this standard lacks clarity and is likely to produce significant conflict as an applicable entity attempts to establish procedures to assure compliance. It appears that situational awareness could not be improved with this standard since it is only dealing with events after-the-fact, not within the time frame to allow corrective action by the system operator. As conveyed in Dominion’s comments on NERC Reliability Standards Development Plan 2011 - 2013, Dominion does not see this draft standard as needing to be in the queue while other standards having more impact to bulk electric reliability remain incomplete or unfinished.
ERCOT ISO	No	ERCOT ISO believes that according to the timelines allotted in Attachment 1, it may not be possible for the entity to identify the “known cause” of an event. The requirements list identification of “initial probable cause”. This is more reasonable under the timelines noted in Attachment 1.
Exelon	No	The purpose states that Responsible Entities SHALL report impact events - this implies that ALL impact events need to be reported regardless of magnitude, suggest rewording to say "... shall report applicable impact events ..." to allow for evaluation of each impact for applicability in accordance with Attachment 1).

Organization	Yes or No	Question 1 Comment
FirstEnergy	No	Since this standard is after-the-fact reporting, the phrase "situational awareness" may not be appropriate since that phrase is attributed by a large part of the industry to real-time, minute-to-minute awareness of the system. We suggest the following rewording of the purpose statement: "To ensure Applicable Entities report impact events and their known causes to enhance and support the reliability of the Bulk Electric System (BES)".
Indeck Energy Services	No	Suggestion: "Functional Entities identified in Section 4 shall support situational awareness of impact events and their known causes."
Independent Electricity System Operator	No	(1) Our understanding of the proposed revision as conveyed in the SAR was to provide clarity and reduce redundancy on reporting the latest and even on-going events on the system that may be caused by system changes and/or sabotage. The intent is to ensure the proper authorities are informed of such events so that they may take appropriate and necessary actions to identify causes and/or mitigate or limit the extent of interruptions. We also supported a suggestion in the SAR to assess the merit of merging CIP-001 and EOP-004 to remove redundancy, although we suggested that this should not be a presumption when revising the standard(s).This posting appears to indicate that only EOP-004 will be revised at this time, and CIP-001 which deals with sabotage reporting will remain in effect. With this assumption, the proposed standard appears to contain a mixture of reporting two types of events of different time frame - the first type being those events that need to be reported soon or immediately after they occur (e.g. impact events that appear to be the result of a sabotage) with an aim to curb/contain these events by the appropriate authorities; the second type being the events that can be reported sometime well after the fact, e.g. system disturbances due to weather or switching or other known causes that are not of malicious nature. Combining the two types of requirement does not appear to be clearly conveyed in the SAR. We therefore suggest the SDT review the main purpose

Organization	Yes or No	Question 1 Comment
		and content in the proposed EOP-004 to ensure consistency with the SAR, and in relation to the purpose and requirements already contained in CIP-004.(2) With respect to disseminating reports and related information after the fact, we wonder if a data collection process, such as RoP 1900, can serve the purpose without having to create a standard or a requirement to achieve this.(3) Most of the requirements appear to be administrative in nature and they stipulate the how but not the what, which in our view does not conform with the Results-based standard concept and does not rise to the level of a reliability standard.(4) A number of requirements proposed in the draft standard are quite vague and cannot be measured. Details of this assessment is provided below.
IRC Standards Review Committee	No	The proposed requirements in the standard are not focused on the core industry concern that current requirements are unclear as to what types of events warrant entities to report. Per draft 2 of the SAR, "The existing requirements need to be revised to be more specific - and there needs to be more clarity in what sabotage looks like." Instead this proposed standard includes requirements that are more focused on "how" to report, rather than "what" to report. The SAR states that: "The development may include other improvements to the standards deemed appropriate by the drafting team, with consensus on the stakeholders (emphasis added), consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards." The SRC believes the scope of the SAR, and likewise the proposed standard, is inappropriate to the fundamental reliability purpose of what events need to be reported. The proposed administrative requirements are difficult to interpret, implement and measure, and do not clarify what type of sabotage information entities need to report. Although the use of procedures and an understanding by those personnel accountable seem helpful for ensuring reports are made, the fundamental purpose of clarifying what types of events should be reported and more importantly what types do not have to be reported, is lacking in the standard. Also, one of the first issues identified in the SAR for consideration by the drafting

Organization	Yes or No	Question 1 Comment
		team seems to be ignored, "Consider whether separate, less burdensome requirements for smaller entities may be appropriate." The requirements for entities to develop Operating Plans and to have training for those plans, further adds uncertainty and increases complexity of how entities, large and small, will have to comply with this standard.
ISO New England Inc.	No	The proposed requirements in the standard are not focused on the core industry concern that current requirements are unclear as to what types of events warrant entities to report. Per draft 2 of the SAR, "The existing requirements need to be revised to be more specific - and there needs to be more clarity in what sabotage looks like." Instead this proposed standard includes requirements that are more focused on "how" to report, rather than "what" to report. The draft 2 SAR has never been balloted for approval prior to standard drafting. In fact, the SAR states, "The development may include other improvements to the standards deemed appropriate by the drafting team, with consensus on the stakeholders (emphasis added), consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards." The scope of the SAR, and likewise the proposed standard, is inappropriate to the fundamental reliability purpose of what events need to be reported. The proposed administrative requirements are difficult to interpret, implement and measure, and do not clarify what type of sabotage information entities need to report. Although the use of procedures and an understanding by those personnel accountable seems helpful for ensuring reports are made, the fundamental purpose of clarifying what types of events should be reported and more importantly what types do not have to be reported, is lacking in the standard. Also, one of the first issues identified in the SAR for consideration by the drafting team seems to be ignored: "Consider whether separate, less burdensome requirements for smaller entities may be appropriate." The requirements for entities to develop Operating Plans and to have training for those plans, further adds uncertainty and increases complexity of how entities, large and small, will have to comply with this standard.The term "impact

Organization	Yes or No	Question 1 Comment
		events" does not draw a clear boundary around those events that are affected by this standard. Since this is not a defined term, nor is intended to be a defined term in the NERC Glossary, this standard lacks clarity and is likely to produce significant conflict as an applicable entity attempts to establish procedures to assure compliance. It appears that situational awareness could not be improved with this standard since it is only dealing with events after-the-fact, not within the time frame to allow corrective action by the system operator.This draft standard should not have this high a priority while other standards having a greater impact on Bulk Electric System reliability remain incomplete or unfinished.Regional reporting requirements should be in Regional Standards, and not be included in a NERC Standard.
Manitoba Hydro	No	Though new purpose greatly clarifies the proposed EOP-004-2 and using "situational awareness" is the key to this purpose, further clarification of specific items should be added to the purpose. "Responsible Entities shall report SIGNIFICANT events to support interconnection situational awareness on events that impact the integrity of the Bulk Electric System, such as islanding, generation, transmission and load losses, load shedding, operation errors, IROL/SOL violations, sustained voltage excursions, equipment and protection failures and on suspected or acts of sabotage."
Nebraska Public Power District	No	The background states there is no real-time reporting requirement in this standard, but the purpose states a purpose is for situational awareness. This implies real-time reporting. The purpose clearly identify the standard is for after the fact reporting to permit analysis of events, trend data, and identify lessons learned.
North Carolina Electric Coops	No	The term "impact event" is not a defined term in the NERC glossary and does not draw a clear boundary or give concise guidance to aid in event recognition.
Northeast Power Coordinating	No	The proposed requirements in the standard are not focused on the core industry concern that current

Organization	Yes or No	Question 1 Comment
Council		requirements are unclear as to what types of events warrant entities to report. Per draft 2 of the SAR, "The existing requirements need to be revised to be more specific - and there needs to be more clarity in what sabotage looks like." Instead this proposed standard includes requirements that are more focused on "how" to report, rather than "what" to report. The draft 2 SAR has never been balloted for approval prior to standard drafting. In fact, the SAR states, "The development may include other improvements to the standards deemed appropriate by the drafting team, with consensus on the stakeholders (emphasis added), consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards." The scope of the SAR, and likewise the proposed standard, is inappropriate to the fundamental reliability purpose of what events need to be reported. The proposed administrative requirements are difficult to interpret, implement and measure, and do not clarify what type of sabotage information entities need to report. Although the use of procedures and an understanding by those personnel accountable seems helpful for ensuring reports are made, the fundamental purpose of clarifying what types of events should be reported and more importantly what types do not have to be reported, is lacking in the standard. Also, one of the first issues identified in the SAR for consideration by the drafting team seems to be ignored: "Consider whether separate, less burdensome requirements for smaller entities may be appropriate." The requirements for entities to develop Operating Plans and to have training for those plans, further adds uncertainty and increases complexity of how entities, large and small, will have to comply with this standard.The term "impact events" does not draw a clear boundary around those events that are affected by this standard. Since this is not a defined term, nor is intended to be a defined term in the NERC Glossary, this standard lacks clarity and is likely to produce significant conflict as an applicable entity attempts to establish procedures to assure compliance. It appears that situational awareness could not be improved with this standard since it is only dealing with events after-the-fact, not within the time frame to allow corrective action by the system operator.This draft standard should not have this high a priority while other standards having a greater impact

Organization	Yes or No	Question 1 Comment
		on Bulk Electric System reliability remain incomplete or unfinished.Regional reporting requirements should be in Regional Standards, and not be included in a NERC Standard.
Pacific Gas and Electric Company	No	PG&E recognizes this is an after the fact report, however, the purpose statement should reflect the fact that this proposed standard is for after-the-fact reporting. If the future intent is for this report to replace current reporting criteria the purpose statement should be expanded to reflect the true intent of the Standard.
PNM Resources	No	PNM believes the purpose statement should reflect the fact that this proposed standard is for after-the-fact reporting. It is misleading and may have many thinking it is duplicative work.
PSEG Companies	No	The following sentence should be added. "This standard is not intended to be for real-time operations reporting."
RRI Energy, Inc.	No	The purpose does not need to mention "and the reliability of the Bulk Electric System." This is the Congressional mandate in FPA Section 215, and could be attached to every Standard, guide, notice and direction issued by FERC, NERC and Regional Entities. In addition, the purpose references "Responsible Entities." However, section 4 on "Applicability" references "Functional Entities." These terms should be consistent. Therefore, the purpose statement of the proposed standard should be corrected to read, "Functional Entities identified in Section 4 shall report impact events and their known causes to support situational awareness."CONSIDERATION: Is the phrase "shall report impact events and their known causes" really a purpose of the Proposed Standard, or is it instead merely a means to achieve the purpose of situational awareness? If the latter, the purpose statement can be further shortened to read, "Functional Entities identified in Section 4 shall support situational awareness of impact events and their known causes."

Organization	Yes or No	Question 1 Comment
Santee Cooper	No	Since this standard is written to report events after-the-fact and not for a System Operator to perform corrective action, we believe the words situational awareness should be removed from the purpose. Situational Awareness is typically used for real-time operations.Also, any events that require reporting should be clearly defined in Attachment 1 and leave no room for interpretation by an entity.
SERC OC Standards Review Group	No	The term “impact events” does not draw a clear boundary around those events that are affected by this standard. Since this is not a defined term, nor is intended to be a defined term in the NERC glossary, this standard lacks clarity and is likely to produce significant conflict as an applicable entity attempts to establish procedures to assure compliance. It appears that situational awareness could not be improved with this standard since it is only dealing with events after-the-fact, not within the time frame to allow corrective action by the system operator.
United Illuminating	No	UI suggests adding the phrase: and the ERO shall provide quarterly reports; Responsible Entities shall report impact events and their known causes, and the ERO shall provide quarterly reports, to support situational awareness and the reliability of the Bulk Electric System (BES).
US Bureau of Reclamation	No	The purpose is more closely related to the concept that "Responsible Entities shall document and analyze impact events and their known causes and disseminate the impact event documentation to support situational awareness". Not all impact events are to be reported. The analysis of the impact events is what is needed to achieve a lessons learned.
We Energies	No	Impact event needs to be clarified first, and DP references in Attachment 1 clarified. Distribution is not BES.
WECC	No	The purpose statement should reflect the fact that this proposed standard is for after-the-fact reporting. It is

Organization	Yes or No	Question 1 Comment
		misleading and may have many thinking it is duplicative work.
ATC	Yes	ATC agrees with the purpose statement. However, we do not agree with the implied definition of “impact events” as represented in Attachment 1. (See specific comments about what is included in Attachment 1 for the type of events that qualify as an “impact event”.)
Bonneville Power Administration	Yes	Known causes are difficult under 1 hour reporting requirements (Unusual events are even harder to narrow down in 24 hours and may take weeks.) The System Operators and RC’s handle situational awareness and reliability events, this is an extra wide view and learning for reporting only.
Dynegy Inc.	Yes	Statement is broad enough to cover both Standards.
Great River Energy	Yes	Thank you for the clarification of “known causes”, this will allow entities to report what they currently know when submitting an impact report.
MRO's NERC Standards Review Subcommittee	Yes	Thank you for the clarification of “known causes”, this will allow entities to report what they currently know when submitting an impact report.
Puget Sound Energy	Yes	However, further definition of "known causes" would be helpful as sometime the root cause analysis doesn't uncover the actual cause for sometime after the timeframes outlined in Attachment 1.
Arizona Public Service Company	Yes	
ATCO Electric Ltd.	Yes	

Organization	Yes or No	Question 1 Comment
BGE	Yes	
City of Austin dba Austin Energy	Yes	
City of Garland	Yes	
Constellation Power Generation and Constellation Commodities Group	Yes	
E.ON Climate & Renewables	Yes	
Georgia System Operations Corporation	Yes	
Green Country Energy	Yes	
Idaho Power Company	Yes	
Kansas City Power & Light	Yes	
Luminant Energy	Yes	
MidAmerican Energy	Yes	

Organization	Yes or No	Question 1 Comment
Midwest ISO Standards Collaborators	Yes	
NERC Staff	Yes	
Pacific Northwest Small Public Power Utility Comment Group	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	
Pepco Holdings, Inc - Affiliates	Yes	
PPL Electric Utilities	Yes	
PPL Supply	Yes	
Tenaska	Yes	
TransAlta Corporation	Yes	

2. Do you agree with the applicable entities in the Applicability Section as well as assignment of applicable entities noted in Attachment 1? Please explain in the comment box below.

Summary Consideration: There was no consensus amongst stakeholders who responded to this question regarding the acceptability of the proposed list of functional entities and the assignment of applicable entities in Attachment 1.

Several respondents replied with their concern that the reporting requirements were redundant. The general sentiment was that unclear responsibility to report a disturbance could trigger a flood of event reports. Attachment 1 has been modified to assign clear responsibility for reporting, for each category of Impact Event. There was some concern expressed that there could be confusion between the reporting requirements in this standard, and those found in CIP-008. The DSR SDT agrees, and Attachment 1 Part B, has been modified to provide the process for the reporting of a Cyber Security Incident.

The DSR SDT had protracted discussions on the applicability of this standard to the LSE. Per the Functional Model the LSE does not own assets and therefore should not be an applicable entity (no equipment that could experience a "disturbance"). However, the Registry Criteria contains language that could imply that the LSE does own assets, or is at least responsible for assets. In addition, the DSR SDT modified Attachment 1 to include reporting of damage or destruction of Critical Cyber Assets per CIP-002. The LSE, as well as the Interchange Authority and Transmission Service Provider are applicable entities under CIP-002 and should be included for Impact Events under EOP-004.

There were several comments that the asset owners (GO/TO) would be less likely than the asset operators (GOP/TOP) to be aware of an impact event. The DSR SDT recognizes that this may be true in some cases, but not all. In order to meet the reliability objectives of this requirement, the applicability for GO/TO will remain as per Attachment 1.

Organization	Yes or No	Question 2 Comment

Organization	Yes or No	Question 2 Comment
American Electric Power (AEP)	No	AEP does not agree with the addition of the Generator Owner to the standard. The Generator Owner does not have visibility to the real time operational status of a unit. As a result, the Generator Owner lacks the ability to recognize impact events and report them to the Regional Entity or NERC within the time frames specified in the standard. Reporting requirements for impact events should be the responsibility of the Generator Operator.
Arizona Public Service Company	No	AZPS recommends excluding 4.1.7 Distribution Providers, as Distribution Providers generally operate at levels below 100kV.
ATC	No	The Functional Entities identified in Attachment 1 do not align with the current CIP Standard obligations (e.g. Load Serving Entities are not included).
CenterPoint Energy	No	CenterPoint Energy does not agree with the addition of Transmission Owner and Distribution Provider to the Applicability section. Transmission Owner and Distribution provider are not currently applicable entities for either CIP-001 or EOP-004 and should not be included in the proposed combined standard. However, CenterPoint Energy does agree that LSE should be removed from the Applicability section. CenterPoint Energy appreciates the SDT's efforts in assigning entities to each event in Attachment 1. This is an improvement over the existing EOP-004 standard. It is clear, however, that with multiple entities responsible for reporting each event, there is no need to expand the Applicability Section to include Transmission Owner and Distribution Provider.
Consolidated Edison Co. of NY, Inc.	No	Comments: NERC's role as the Standard enforcement organization for the power industry will be in conflict if NERC is also identified as an applicable entity. What compliance organization will audit NERC's

Organization	Yes or No	Question 2 Comment
		performance? This is presently not clear.
Constellation Power Generation and Constellation Commodities Group	No	Constellation Power Generation and Constellation Commodities Group disagrees with the inclusion of Generator Owners. Since one of the goals in revising this standard is to streamline impact event reporting obligations, Generator Operators are the appropriate entity to manage event reporting as the entity most aware of events should they arise. At times, the information required to complete a report may warrant input from entities connected to generation, but the operator remains the best entity to fulfill the reporting obligation.
E.ON Climate & Renewables	No	1. Voltage deviation events are too vague for GOP. How does voltage deviations apply to GOP's or specifically renewables i.e., wind farms? 2. Define what an "entity" is. 3. Define what a "generating station" is. 4. Define what a "BES facility" is. 5. Define what a control center is. 6. Renewable energy/generators should be taken into consideration when crafting the events.
E.ON U.S. LLC	No	The proposed standard does not list the Load Serving Entity as an Applicable Entity, but the possible events that the standard addresses are within the scope of the LSE. Some functions of the LSE listed within the Functional Model are addressed in the proposed standard. Existing CIP-001-1a and EOP-004-1 are both applicable to the LSE.
Electric Market Policy	No	Having the ERO as an applicable entity is concerning as they are also the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. For example, establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC's open process. Attachment 1 is troublesome. The time frames listed are not consistent for similar events. For example, EEAs are either reported within one or 24 hours depending on the nuance. Having multiple entities

Organization	Yes or No	Question 2 Comment
		reporting the same event is troublesome, i.e., why does a RC have to report an EEA if the BA is going to report it? This will lead to conflicting reports for the same event. Attachment 1 seems to be consolidating time frames from other standards into one for reporting. However, we believe this subject is more complex than this table reveals and the table needs more clarification.Several of the events require filing a written formal report within one hour. For example, system separation certainly is going to require an “all hands on deck” response to the actual event. We note that the paragraph above the table in attachment 1 indicates that a verbal report would be allowed in certain circumstances, but this is the same issue with the formal report in that the system operators are concerned with the event and not the reporting requirements.There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
ERCOT ISO	No	ERCOT ISO recommends that the Electric Reliability Organization be removed from the standard. The Electric Reliability Organization should not be responsible for reliability functions and therefore should be excluded from reliability standards.
Exelon	No	Attachment 1, Part B, footnote 1. A GO is unlikely to know if a fuel supply problem would cause a reliability concern because one GO may not know the demand for an entire region. Attachment 1, Part B, footnote 1. What is the definition of an "emergency" related to problems with a fuel supply chain? What time threshold of projected need would constitute a 1 hour report?Attachment 1, Part A - Voltage Deviations - A GOP may not be able to make the determination of a +/- 10% voltage deviation for â‰¥ 15 minutes, this should be a TOP RC function only. Attachment 1, Part A - Generation Loss of â‰¥ 2, 000 MW for a GO/GOP does not provide a time threshold. If the 2, 000 MW is from a combination of units in a single location, what is the time threshold for the combined unit loss? Attachment 1, Part A - Damage or destruction of BES equipment o The

Organization	Yes or No	Question 2 Comment
		event criteria is ambiguous and does not provide clear guidance; specifically, the note needs to provide more explicit criteria related to parts (iii) and (iv) to remove the need for interpretation especially since this is a 1 hour reportable occurrence. In addition, determination of the aggregate impact of damage may not be immediately understood - does the 1 hour report time clock start on initiation of event or following confirmation of event? o The initiating event needs to explicitly state that it is a physical and not cyber. Events related to cyber sabotage are reported in accordance with CIP-008, "Cyber Security - Incident Reporting and Response Planning," and therefore any type of event that is cyber initiated should be removed from this Standard. o If the damage or destruction is related to a deliberate act, consideration should also be given to coordinating such reporting with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security event. Attachment 1, Part B - Loss of off-site power (grid supply) affecting a nuclear generating station - this event classification should be removed from EOP-004. The impact of loss of off-site power on a nuclear generation unit is dependent on the specific plant design and may not result in a loss of generation (i.e., unit trip); furthermore, if a loss of off-site power were to result in a unit trip, an Emergency Notification System (ENS) would be required to the Nuclear Regulatory Commission (NRC). The 1 hour notification in EOP-004 on a loss of off-site power (grid supply) to a nuclear generating station should be commensurate with other federal required notifications. Depending on the unit design, the notification to the NRC may be 1 hour, 8 hours or none at all. Consideration should be given to coordinating such reporting with existing required notifications to the NRC as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential transient on the unit. Attachment 1, Part B - Forced intrusion at a BES facility - Consideration should also be given to coordinating such reporting with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security event. Attachment 1, Part B - Risk to BES equipment from a non-environmental physical threat - this event leaves

Organization	Yes or No	Question 2 Comment
		the interpretation of what constitutes a "risk" with the reporting entity. Need more specific criteria for this event.Attachment 1, Part B - Detection of a cyber intrusion to critical cyber assets - Events related to cyber sabotage are reported in accordance with CIP-008, "Cyber Security - Incident Reporting and Response Planning," and therefore any type of event that is cyber initiated should be removed from this Standard.
FirstEnergy	No	We do not support the ERO as an applicable entity of a reliability standard because they are not a user, owner or operator of the bulk electric system. Any expectation of the ERO should be defined in the Rules of Procedure.
Georgia System Operations Corporation	No	This standard should not apply to distribution systems or Distribution Providers. It should apply only to the BES.
Georgia Transmission Corporation	No	These events generally are Operator Functions and should not apply to a TO.1. Energy Emergency requiring system-wide voltage reduction2. Loss of firm load greater than 15 min.3. Transmission loss (multiple BES transmission elements)4. Damage or destruction to BES equipment (thru operational error or equipment failure)5. Loss of off-site power affecting a nuclear generating station
Indeck Energy Services	No	---ERO should not be included in this or any other standard! FERC can decide whether NERC is doing a good job without having standards requirements to audit to. If NERC needs to be included in a standard, then it should a stand-alone one so that the RSAW for all of the other audits don't need to include those requirements. ---"Loss of off-site power (grid supply)" is important at control centers and other large generators. The SDT must use a well-defined standard such as potentially cause a Reportable Disturbance, to differentiate significant events from others. ---"Footnote 1. Report if problems with the fuel supply chain result in the projected need for emergency actions to manage reliability." is ambiguous. Everything in the

Organization	Yes or No	Question 2 Comment
		Standards program can "Affecting BES reliability". The SDT must use a well-defined standard such as potentially cause a Reportable Disturbance, to differentiate significant events from others. ---"Footnote 2. Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects the reliability of the BES)." is well intentioned but ambiguous. For example, if I know the motivation is to blow up the plant, then by this footnote, I don't have to report. The SDT must use a well-defined standard such as potentially cause a Reportable Disturbance, to differentiate significant events from others. ---All terms should be used from or added to the Glossary.
Independent Electricity System Operator	No	We do not agree with the inclusion of TO and GO. They are not operating entities and do not need to collect or provide information pertaining to impact events, which are the results and phenomena observe under operating conditions in the operation horizon, and such information collection and provision are the responsibility of the TOP and GOP.
IRC Standards Review Committee	No	Entities that have information about possible sabotage events should report these to NERC after the fact and the standard should simply reflect that. While we agree with the list of functional entities identified in the Applicability Section, we do not agree with their application in Attachment 1. As the functional entities are identified in Attachment 1, there is likely going to be duplicate reporting. Why should both the RC and BA submit a report for an EEA for example?
ISO New England Inc.	No	Having the ERO as an applicable entity raises the issue that they are also the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. For example, establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC's open process. NERC has also offered the opinion that since NERC is not a "user, owner, or

Organization	Yes or No	Question 2 Comment
		operator" Standards are not enforceable against the ERO. In Attachment 1 the time frames listed are not consistent for similar events. For example, EEAs are either reported within one or 24 hours depending on the nuance. Having multiple entities reporting the same event is troublesome, i.e., why does a RC have to report an EEA if the BA is going to report it? This will lead to unnecessary and possibly conflicting reports for the same event. Attachment 1 seems to be consolidating time frames from other standards into one for reporting. However, this subject is more complex than this table reveals, and the table needs more clarification.Entities that have information about possible sabotage events should report these to NERC after the fact, and the standard should simply reflect that. While we agree with the list of functional entities identified in the Applicability Section, we do not agree with their application in Attachment 1. As the functional entities are identified in Attachment 1, it is likely that there is going to be duplicate reporting. Several of the events require filing a written formal report within one hour. For example, system separation is going to require an "all hands on deck" response to the actual event. The paragraph above the table in Attachment 1 indicates that a verbal report would be allowed in certain circumstances, but this is the same issue with the formal report in that the system operators are concerned with the event and not the reporting requirements.There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements through NERC that cross federal agency jurisdictions.
Luminant Energy	No	Inclusion of both GO and GOP will result in duplicate reporting as both are responsible for reporting resource-related events such as Generation Loss, Fuel Supply Emergencies and Loss of Off-site power (grid supply). Recommend including only the GOP as it is critical that the GOP gather and communicate relevant information to the Reliability Coordinator.
Manitoba Hydro	No	Since this Standard is to support situational awareness, more entities should be included such as Load

Organization	Yes or No	Question 2 Comment
		Serving Entities (which was removed from EOP-004-1).
MidAmerican Energy	No	While we agree with the list of functional entities identified in the Applicability Section, we do not agree with their application in Attachment 1. As the functional entities are identified in Attachment 1, there is likely going to be duplicate reporting. Why should both the RC and BA submit a report for an energy emergency requiring public appeals?
Midwest ISO Standards Collaborators	No	While we agree with the list of functional entities identified in the Applicability Section, we do not agree with their application in Attachment 1. As the functional entities are identified in Attachment 1, there is likely going to be duplicate reporting. Why should both the RC and BA submit a report for an energy emergency requiring public appeals?
North Carolina Electric Coops	No	There is a conflict between the ERO being listed as an applicable entity and the fact that the ERO is the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that other applicable entities would be required to meet.Attachment 1 has inconsistent time frames listed for similar events. For example, EEA's are either reported within one or 24 hours depending on the nuance. Also, having more than one entity reporting an EEA can lead to conflicting information for the same event. Attachment 1 has the RC and the BA both reporting the same EEA event. Attachment 1 consolidates time frames from other standards for reporting purposes. There should either be a separate standard for "reporting" that encompasses reporting requirements for all standards or leave the time frames and reporting requirements in the original individual standards.Several of the events require filing a written formal report within one hour. For large events like cascading outages or system separation, "all hands on deck" attention will need to be given to the actual event. Although a verbal report would be allowed in certain circumstances, attention to the actual event should take precedence over formal reporting requirements.There is already a

Organization	Yes or No	Question 2 Comment
		DOE requirement to report certain events and no need to develop redundant reporting requirements in the NERC arena when this information is already available at the federal level at other agencies.
Northeast Power Coordinating Council	No	Having the ERO as an applicable entity raises the issue that they are also the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. For example, establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC's open process. NERC has also offered the opinion that since NERC is not a "user, owner, or operator" Standards are not enforceable against the ERO. In Attachment 1 the time frames listed are not consistent for similar events. For example, EEAs are either reported within one or 24 hours depending on the nuance. Having multiple entities reporting the same event is troublesome, i.e., why does a RC have to report an EEA if the BA is going to report it? This will lead to unnecessary and possibly conflicting reports for the same event. Attachment 1 seems to be consolidating time frames from other standards into one for reporting. However, this subject is more complex than this table reveals, and the table needs more clarification.Entities that have information about possible sabotage events should report these to NERC after the fact, and the standard should simply reflect that. While we agree with the list of functional entities identified in the Applicability Section, we do not agree with their application in Attachment 1. As the functional entities are identified in Attachment 1, it is likely that there is going to be duplicate reporting. Several of the events require filing a written formal report within one hour. For example, system separation is going to require an "all hands on deck" response to the actual event. The paragraph above the table in Attachment 1 indicates that a verbal report would be allowed in certain circumstances, but this is the same issue with the formal report in that the system operators are concerned with the event and not the reporting requirements.There is already a DOE requirement to report certain events. We see no need to develop redundant reporting

Organization	Yes or No	Question 2 Comment
		requirements through NERC that cross federal agency jurisdictions.
Pacific Gas and Electric Company	No	PG&E recognizes the ERO is in R1, however, it does not see where the ERO's applicability is applied in Attachment 1.
Pacific Northwest Small Public Power Utility Comment Group	No	See #15
PNM Resources	No	PNM OTS does not see where the ERO's applicability is applied in Attachment 1.
PPL Electric Utilities	No	While we agree with the applicable entities in the Applicability Section of the revised standard, we would like the SDT to reconsider the applicable entities identified on Attachment 1, specifically regarding duplication of reporting e.g. should TO and TOP report?
PPL Supply	No	While we agree with the list of functional entities identified in the Applicability Section, we do not agree with assignment of applicable entities noted in Attachment 1. As the functional entities are identified in Attachment 1, there will likely be duplicate reporting for many impact events. By applying reporting responsiblities to both the Gen Owner and Gen Operator, this will result in duplicate reporting for plants with multiple owners. It also increases the burden on the Gen Operator who is required to report the event to NERC and to other Gen Owners in a timely manner to allow other Gen Owners to meet the NERC reporting timeline. We suggest that the reporting requirements associated with generators be applied to the Gen Operator only.
RRI Energy, Inc.	No	Agree with the "Applicability" section functional categories.Agree with the Attachment 1 lists of "Entity with Reporting Responsibility," with the following exceptions:PART A"Damage or Destruction of BES Equipment" - This item has a footnote 1 listed, but nothing at the bottom of the page for a footnote. Assuming the footnote

Organization	Yes or No	Question 2 Comment
		reference is intended to reference the "Examples" at the bottom of the page, the following concerns exist:(i) "critical asset" - Is this term intended to reference a "Critical Asset" identified pursuant to the CIP-002 risk-based assessment methodology? If so, it should be capitalized. If not, who determines what constitutes a lower case "critical asset"? (ii) "Significantly affects the reliability margin of the system..." - If this is intended to be enforceable, several words need significant clarification and definition, such as "Significantly," "reliability margin," "system" (BES?), "potential," and "emergency action." The combined ambiguity of just two of those phrases would most likely result in a court holding this statement as so vague as to be unenforceable. The combined lack of clarity of all the highlighted words or phrases render this sentence meaningless.(iii) "Damaged or destroyed due to a non-environmental external cause" - "Non-environmental external cause" should be a defined term because, as is the case in item (ii) above, it is vague and subject to broad, random or arbitrary interpretation. Part B provides examples of "non-environmental physical threat" for "Risk to BES equipment." Those examples could be referenced here, or different examples included that are more applicable to the Event.The items highlighted in items (ii) and (iii) above are very similar to the unintended string of CIP-001 violations that Registered Entities experienced in 2007 and 2008 for failing to provide their own definition of "sabotage" under a sabotage reporting standard that failed to provide any guidance to the industry within the standard as to what constituted "sabotage." PART B"Detection of a cyber intrusion to critical cyber assets" - Capitalize "Critical Cyber Asset."
Santee Cooper	No	Standards cannot be applicable to an ERO because they are the compliance enforcement authority, and the ERO is not a user, owner, or operator of the BES. Since we are reporting events that may affect the BES, why does a DP need to be included as an applicable entity for this standard? If the DOE form is going to continue to be required by DOE, then NERC should accept this form. Entities do not have time to fill out duplicate forms within the time limits allowed for an event. This is burdensome on an entity. If NERC is going

Organization	Yes or No	Question 2 Comment
		to require a separate reporting of events from DOE, then NERC should look at these events closely to determine if any of the defined events should be eliminated or modified from the current DOE form. (For example: Is shedding 100 MW of firm load really a threat to the BES?)Why does Attachment 1 have multiple entities reporting the same event? An RC should not have to report an EEA if the BA is required to report it. This will lead to conflicting reports for the same event.Attachment 1 is just a consolidation of the time frame from other standards. It appears no review was done for consistency of time frames for similar events.
SERC OC Standards Review Group	No	We find it interesting that the ERO is listed as an applicable entity. The ERO can't be an applicable entity because they are the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. NERC seems to be attempting to evade FERC jurisdiction by having a standard that enables it to write new rules that don't pass through the normal standards development process with ultimate approval by FERC.Attachment 1 is troublesome. The time frames listed are not consistent for similar events. For example, EEAs are either reported within one or 24 hours depending on the nuance. Having multiple entities reporting the same event is troublesome, i.e., why does an RC have to report an EEA if the BA is going to report it? This will lead to conflicting reports for the same event. Attachment 1 seems to be consolidating time frames from other standards into one for reporting. However, we believe this subject is more complex than this table reveals and the table needs more clarification or it should be eliminated and leave the time frames in the other standards.Several of the events require filing a written formal report within one hour. For example, system separation certainly is going to require an "all hands on deck" response to the actual event. We note that the paragraph above the table in attachment 1 indicates that a verbal report would be allowed in certain circumstances, but this is the same issue with the formal report in that the system operators are concerned with the event and not the reporting requirements.There is already a DOE requirement to report

Organization	Yes or No	Question 2 Comment
		certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
Southern Company - Transmission	No	We find it interesting that the ERO is listed as an applicable entity. The ERO is responsible for multiple requirements in this standard that shapes the ultimate actual rules that the other applicable entities would be required to meet. Can the NERC/ERO be accountable for a feedback loop to the industry? Feedback is preferable but would NERC/ERO self-report a violation to the requirement?
We Energies	No	The need for a DP to be included needs to be clarified. The Purpose points to BES. A DP does not have BES equipment.
WECC	No	The ERO's applicability is not applied in Attachment 1.
Great River Energy	Yes	We believe that it is important for the ERO to provide valuable Lessons learned to our electrical industry, thus enhancing the reliability of the BES.
Kansas City Power & Light	Yes	Consideration should be given to the need for a preliminary impact event report to be filed by the Reliability Coordinator and the Registered Entity. If two reports should be filed, should they both contain the same information.
MRO's NERC Standards Review Subcommittee	Yes	The NSRS believes it is important for the ERO to provide valuable Lessons learned to our electrical industry, thus enhancing the reliability of the BES.
TransAlta Corporation	Yes	Electrical Reliability Organization (ERO) does not appear to be a defined term in the NERC Glossary of Terms on the NERC website. Last updated April 20, 2010.

Organization	Yes or No	Question 2 Comment
US Bureau of Reclamation	Yes	The question is focused on a limited area of Attachment A. There other problematic areas of Attachment 1 will be addressed in subsequent comments.
Ameren	Yes	
ATCO Electric Ltd.	Yes	
BGE	Yes	
Bonneville Power Administration	Yes	
City of Austin dba Austin Energy	Yes	
City of Garland	Yes	
Duke Energy	Yes	
Dynegy Inc.	Yes	
Green Country Energy	Yes	
Idaho Power Company	Yes	
Nebraska Public Power District	Yes	
NERC Staff	Yes	

Organization	Yes or No	Question 2 Comment
PacifiCorp	Yes	
PacifiCorp	Yes	
Pepco Holdings, Inc - Affiliates	Yes	
Puget Sound Energy	Yes	
Tenaska	Yes	
United Illuminating	Yes	

3. Do you agree with the requirement R1 and measure M1? Please explain in the comment box below.

Summary Consideration: There was no consensus amongst stakeholders who responded to this question. There was strong support for a central system for receiving and distributing impact event reports (a/k/a one stop shopping). There was general agreement that NERC was the most likely, logical entity to perform that function. However several respondents expressed their concern that the ERO could not be compelled to do so by a requirement in a Reliability Standard (not a User, Owner or Operator of the BES). In their own comments, NERC did not oppose the concept, but suggested that the more appropriate place to assign this responsibility would be the NERC Rules of Procedure. The DSR SDT concurs. The DSR SDT has removed the requirement from the standard and is proposing to make revisions to the NERC Rules of Procedure as follows:

> 812. NERC will establish a system to collect impact event reports as established for this section, from any Registered Entities, pertaining to data requirements identified in Section 800 of this Procedure. Upon receipt of the submitted report, the system shall then forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary. These reports shall be forwarded to the Federal Energy Regulatory Commission for impact events that occur in the United States. This can include state, federal, and provincial organizations. The ERO shall solicit contact information from Registered Entities appropriate governmental, law enforcement and regulatory agencies contact information for distributing reports.

The DSR SDT also believes NERC's additional concern about what data is applicable is addressed by the revisions to Attachment 1, and the inclusion of the OE-417 as an acceptable interim vehicle.

Organization	Yes or No	Question 3 Comment
WECC		R1 is appropriate for after-the-fact reporting. However, as proposed this standard eliminates all real-time notifications, including the CIP-001-1 R3 notice to appropriate parities in the Interconnection. New requirement R2.6 lists external parties to notify but it does not include the Reliability Coordinator. It is

Organization	Yes or No	Question 3 Comment
		important that the RC be notified of suspected sabotage. The RC's wide-area interconnection view and interaction with BAs may help recognize coordinated sabotage actions. Any "impact event" where sabotage is suspected as the root cause should require additional and real-time notifications.
ATC	No	ATC does not agree with R1 for three reasons:1. The ERO cannot be assigned obligations in NERC Standards. The requirements for the ERO should be addressed by a revision to Section 801 of the Rules of Procedure.2. This is a fill-in-the-blank requirement. The requirement, positioned as R1, does not allow for the obligations to be clearly defined. It refers to R6 which refers to R2 and Attachment 1. A clearer structure to the Standard would be to simply state that the Functional Entities have to meet the reporting obligations documented in Attachment 1 and delete the current R1.
BGE	No	R1 With the definition of "Impact Event", are we eliminating the term "Disturbance Reporting"? If we eliminate disturbance reporting, SDT should remove the reference from the Summary of Concepts and from the title, otherwise further definition on the distinction between the two terms is needed.R1. What is the "system" described here? What type of system is anticipated - electronic, programmatic or can it be better described by using "standard reporting form"?M1. Needs to seek evidence that the "system" was used for receiving reports, as well as distributing them.M1. Examples are more appropriately used in guidance documentation than in the standard. Rationale for R1 - Final statement regarding OE-417 needs to be removed. The ERO will establish the requirement in their "system" if the standard remains as is. The Requirement does not require the responsible entities to send OE-417 to DOE.
CenterPoint Energy	No	The ERO does not need to establish a "system for receiving reports" as the "system for receiving reports" is inherent given the requirements for reporting. The requirement also seems to add redundancy versus eliminating redundancy in the distribution of reports to applicable government, provincial or law enforcement

Organization	Yes or No	Question 3 Comment
		agencies on matters already reported by Responsible Entities. If an event is suspected to be an intentional criminal act, i.e. “sabotage”, the Responsible Entity would have contacted appropriate provincial or law enforcement agencies. The ERO is not in a position to add meaningful value to these reports as any information the ERO may provide is second hand. CenterPoint Energy recommends R1 and M1 be deleted.
City of Garland	No	Reason 1Most of this is duplication of existing processes - More “Big Government” and/or “Overhead” is not needed. There are already processes in place to notify “real time” 24 X 7 organizations that take action (RC, BA, TOP, DOE, FBI, Local Law Enforcement, etc) in response to an “impact event”. It is stated in your document on page five (5) “The proposed standard deals exclusively with after-the -fact reporting.” The combining of CIP 001 & EOP 004 should not expand on existing implemented reporting requirements nor should it result in NERC forming a 24 X 7 department to handle 1 hour (near real time) reporting requirements.Reason 2If this should go forward as drafted, NERC should not establish a “clearing house” for reporting requirements for Registered Entities without also taking legal responsibility for distributing those reports to required entities. It states in at least 2 places (Page 6 & Page 22) in the document that Responsible Entities are ultimately responsible for ensuring that OE-417 is received at the DOE. Thus, a Registered Entity could be penalized for violating this new standard if it did not file the reports with NERC or it could still be penalized (both criminal & civil) if they filed the reports with NERC but NERC (for whatever reason) did not follow through with ensuring the report was properly filed at the DOE.
Consolidated Edison Co. of NY, Inc.	No	See response to Question 2.
Duke Energy	No	The requirement again states the intent is to “enhance and support situational awareness”, which doesn’t sync with “after-the-fact reporting”. We question why NERC needs to create this report and system for

Organization	Yes or No	Question 3 Comment
		distributing impact event reports to various organizations and agencies for after-the-fact reporting, when we are still required to make real-time reports under other standards. For example, the Rational specifically recognizes that this standard won't release us from the DOE's OE-417 reporting requirement. We don't see that this provides value, unless NERC can find a way to eliminate redundancy in reporting.
Electric Market Policy	No	Having the ERO as an applicable entity is concerning as they are also the compliance enforcement authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. Establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC's open process. At this stage it is not clear how the ERO will develop or effectively maintain a list of "applicable government, provincial or law enforcement agencies" for distribution as defined in R1. The "rationale for R1" states that OE-417 could be included as part of the electronic form, but responsible entities will ultimately be responsible for ensuring that OE-417 reports are received at DOE. This requirement needs to be more definitive with respect to OE-417. It seems like the better approach would be for the entities to complete OE-417 form and this standard simply require a copy.
ERCOT ISO	No	Recommend that requirements for the Electric Reliability Organization be removed. However, if the requirements are retained, ERCOT ISO recommends the following wording change to be consistent with other standards. "R1. The ERO shall create, implement, and maintain a system for receiving and distributing impact event reports, received pursuant to Requirement R6, to applicable government, provincial or law enforcement agencies and Registered Entities to enhance and support situational awareness."
Exelon	No	This requirement should include explicit communications to the NRC (if applicable) of any reports including a nuclear generating unit as a jurisdictional agency to ensure notifications to other external agencies are

Organization	Yes or No	Question 3 Comment
		coordinated with the NRC. Depending on the event, a nuclear generator operator (NRC licensee) has specific regulatory requirements to notify the NRC for certain notifications to other governmental agencies in accordance with 10 CFR 50.72(b)(2)(xi). In general, the DSR SDT should include discussions with the NRC to ensure communications are coordinated or consider utilizing existing reporting requirements currently required by the NRC for each nuclear generator operator for consistency.
FirstEnergy	No	FirstEnergy proposes that requirement R1 and Measure M1 be deleted.A requirement assignment to the ERO is problematic and should not appear in a reliability standard. The team should keep in mind that all requirements will require VSL assignments that form the basis of sanctions. FE does not believe it is appropriate for the ERO to be exposed to a compliance violation investigation as the ERO is not a functional entity as envisioned by the Functional Model. If this "after-the-fact" reporting is truly needed for reliability then the standard must be written in a manner that does not obligate the ERO to reliability requirements. It would be acceptable and appropriate for a requirement to reference the "ERO Process" desired by R1, however, that process should be reflected in the Rules of Procedure and not a reliability standard.
Indeck Energy Services	No	This standard is an inappropriate place to define this requirement. NERC needs to be held accountable, but it should be independent of the standard. What if NERC fails to do it by the effective date of the standard, all Registered Entities will violate the standard until NERC is done. The effective date needs to be set based on NERC completing the system defined in R1.
Independent Electricity System Operator	No	R1 does not directly convey the need for reporting. The requirement could be written to require the responsible entities to report impact events to the ERO using a process to be described in the standard and according to a set of reporting criteria. Whether or not there is a “system” makes little difference if it complies with the requirement to provide the reports on time. In addition, an ERO established system which, without

Organization	Yes or No	Question 3 Comment
		being included in the standard and posted for public comment and eventually balloted, may not be acceptable to the entities that are responsible for reporting to the ERO. Further, a reliability standard should not need to bother with how the ERO disseminate this information to applicable government, provincial or law enforcement agencies. This is the obligation of the ERO and if required, can be included in the Rules of Procedure.
ISO New England Inc.	No	Having the ERO as an applicable entity raises a concern because they are also the Compliance Enforcement Authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. Establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC's open process. At this stage it is not clear how the ERO will develop or effectively maintain a list of "applicable government, provincial or law enforcement agencies" for distribution as defined in R1. The "rationale for R1" states that OE-417 could be included as part of the electronic form, but responsible entities will ultimately be responsible for ensuring that OE-417 reports are received at DOE. This requirement needs to be more definitive with respect to OE-417. The better approach would be for the entities to complete OE-417 form and this standard simply require a copy.
MidAmerican Energy	No	
NERC Staff	No	NERC staff is concerned about this requirement's applicability to the ERO. We feel that such a responsibility needs mentioning in the Rules of Procedure, the Compliance Monitoring and Enforcement Program (CMEP), or in a guideline document rather than in a standard requirement. Further, the requirement specifies "how" to manage the event data, not "what" should be monitored.

Organization	Yes or No	Question 3 Comment
North Carolina Electric Coops	No	The ERO cannot be subject to a requirement for which it is the compliance enforcement authority.
Northeast Power Coordinating Council	No	Having the ERO as an applicable entity raises a concern because they are also the Compliance Enforcement Authority. The ERO is responsible for multiple requirements in this standard that shape the ultimate actual rules that the other applicable entities would be required to meet. Establishing and maintaining a system for receiving and distributing impact events, per R1, would be done solely by the ERO, outside of NERC's open process. At this stage it is not clear how the ERO will develop or effectively maintain a list of "applicable government, provincial or law enforcement agencies" for distribution as defined in R1. The "rationale for R1" states that OE-417 could be included as part of the electronic form, but responsible entities will ultimately be responsible for ensuring that OE-417 reports are received at DOE. This requirement needs to be more definitive with respect to OE-417. The better approach would be for the entities to complete OE-417 form and this standard simply require a copy.
Puget Sound Energy	No	The language of R1 and M1 does not support the DSR SDT's goal of having a single form and system for reporting. The standard should specify the form and system rather than deferring that decision to the ERO. The language of R1 and M1 leaves the form and system to the ERO's discretion, which could lead to multiple forms and frequent revisions to them. This would lead to difficulties in tracking the reporting requirements. In addition, it is impossible to comment intelligently regarding the overall impact of the proposed standard and its requirements and measures without the reporting form and system being specified in the standard.
Santee Cooper	No	It cannot apply to the ERO.
SERC OC Standards Review	No	The ERO cannot be subject to a requirement for which it is the compliance enforcement authority. The

Organization	Yes or No	Question 3 Comment
Group		governance in this situation appears incomplete.
US Bureau of Reclamation	No	This standard should describe the ERO process of event documentation, analysis, and dissemination. Allowing the ERO to develop a event documentation, analysis, and dissemination process, which becomes a requirement on the Entities, must be derived through the Standards Development Process. The requirement, as it is currently worded, allows the ERO to develop standard requirements. If the intent is to only develop a means of collecting, which does not impose a requirement, the wording should state so. Otherwise, if the ERO wants to require that reports are posted to a specific location by the Entity, then it is a requirement and must go through the Standards Development Process. Secondly, there is already a single reporting form identified. It is not clear why the SDT could not accept that form as the reporting tool.
American Electric Power (AEP)	Yes	Overall we support the concepts; however, it is unclear if the ERO can be held accountable for compliance with NERC Requirements. If this requirement is removed there needs to be some mechanism for the ERO to establish a single clearinghouse.
City of Austin dba Austin Energy	Yes	Austin Energy would like to see OE-417 incorporated into the electronic form This will reduce the callout of EOP-004-2 and OE-417 forms in our checklists / documents and one form can be submitted to NERC and DOE.
E.ON Climate & Renewables	Yes	A generic ERCO approved electronic (form that can be submitted on-line) reporting form will help to add more clarity & consistency to the Impact event reporting process.
Georgia System Operations Corporation	Yes	Yes it would reduce duplication of effort and should ensure that the various entities and agencies all have consistent information. It should be simpler and quicker to file than what is needed to meet the current

Organization	Yes or No	Question 3 Comment
		standard.However, the system should allow for partial reporting and hierarchical reporting. Entities up the ladder in a reporting hierarchy may fill in additional info (usually from a wider scope of view) than what lower level entities are aware of. It would be better for information to go up a hierarchy than for bits and pieces to go to the ERO from many entities. Terminology may be different in each of the bits and pieces yet the same idea may be intended. The ERO may mistake multiple reports as being different events when they are all related to one event.The system should give an entity the ability to select the entities that should receive the impact event report.If hierarchical reporting is not enabled by the system, then entities should be allowed to work out a reporting hierarchy as a group and entities at lower levels should not be required to report over the NERC system. Some higher level entity would enter the information on the NERC system as coordinated by the entities within a group.
Idaho Power Company	Yes	the SDT must ensure that only a single form is required for compliance (such example OE-417)
IRC Standards Review Committee	Yes	Note that ERCOT does not sign on to this particular comment.
Kansas City Power & Light	Yes	Although we support situational awareness for the other registered entities, impact event reports should be distributed anonymously to communicate the information while protecting the registered entity.
Manitoba Hydro	Yes	Yes, keeping R1 generic and pointing to “government”, “Provincial”, “law” encompasses all entities in all major interconnections.
PacifiCorp	Yes	All efforts need to be made to include OE-417 reporting requirements to safeguard against duplicate reporting and / or delinquent reporting.One report for all events is more preferable than multiple reports for one event.

Organization	Yes or No	Question 3 Comment
RRI Energy, Inc.	Yes	While including the phrase "to enhance and support situational awareness" is a good use of the Results-Based Standards development tools and framework, the phrase is already included in the purpose statement. As such, it is unnecessary in Requirement 1. If it were to be included in Requirement 1, then it would also need to be included in each of the other Requirements 2 through 8. The "Purpose" statement captures this aptly.
Southern Company - Transmission	Yes	We do have one concern in that we are hopeful that NERC will develop a system that will allow a one stop shop of reporting.
Avmeren	Yes	
Arizona Public Service Company	Yes	
ATCO Electric Ltd.	Yes	
Bonneville Power Administration	Yes	
Constellation Power Generation and Constellation Commodities Group	Yes	
Dynegy Inc.	Yes	
Great River Energy	Yes	

Organization	Yes or No	Question 3 Comment
Green Country Energy	Yes	
Luminant Energy	Yes	
Midwest ISO Standards Collaborators	Yes	
MRO's NERC Standards Review Subcommittee	Yes	
Nebraska Public Power District	Yes	
Pacific Gas and Electric Company	Yes	
PacifiCorp	Yes	
Pepco Holdings, Inc - Affiliates	Yes	
PNM Resources	Yes	
PPL Electric Utilities	Yes	
PPL Supply	Yes	

Organization	Yes or No	Question 3 Comment
Tenaska	Yes	
TransAlta Corporation	Yes	
United Illuminating	Yes	
We Energies	Yes	

4. Do you agree with the requirement R2 and measure M2? Please explain in the comment box below.

Summary Consideration: Most stakeholders who responded to this question indicated disagreement with Requiremnet R2 and M2 as originally proposed. There were objections to the use of the term "Operating Plan" to describe the procedure to identify and report the occurrence of a disturbance. The DSR SDT concurs, and Operating plan has been replaced with the generic term "procedure" where appropriate believe that the use of a defined term is appropriate and has revised Requirement 1 to include Operating Plan, Operating Process and Operating Procedure.

R1. Each Responsible Entity shall have an Impact Event Operating Plan that includes [Violation Risk: Factor Medium] [Time Horizon: Long-term Planning]:

1.1. An Operating Process for identifying Impact Events listed in Attachment 1.

1.2. An Operating Procedure for gathering information for Attachment 2 regarding observed Impact Events listed in Attachment 1.

1.3. An Operating Process for communicating recognized Impact Events to the following:

1.3.1. Internal company personnel notification(s).

1.3.2. External organizations to notify to include but not limited to the Responsible Entities' Reliability Coordinator, NERC, Responsible Entities' Regional Entity, Law Enforcement, and Governmental or Provincial Agencies.

1.4. Provision(s) for updating the Impact Event Operating Plan within 90 days of any change to its content.

Other requirements reference the Operating Plan as appropriate. The requirements of EOP-004 fit precisely into the definition of Operating Plan:

Operating Plan: A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other

entities, etc., is an example of an Operating Plan.

Note R2 has been moved to R1 due to elimination of original R1. Many commenters felt that the requirements around updating the Operating Plan were too prescriptive, and impossible to comply with during the time frame allowed. The DSR SDT agrees, and Requirement R2 Parts 2.5 through 2.9 have been eliminated. They have been replaced with Requirement R1, Part 1.4 to update the Operating Plan within 90 days of any change to content.

Organization	Yes or No	Question 4 Comment
Bonneville Power Administration		As long as the 2.4 list is position based, not based on each individual that fills the position. (There is a concern of listing all 2.4 monitoring/reporting personnel in the company that cover the impact event, since there are different function groups and shift work. Documentation trails are difficult with personnel changes.) Because the CIP is being added, it requires an Operating Plan (instead of procedure) with 30 day revision timelines, so it increases the burden for electrical grid event reporting function. R2.9 language refers to R8 "annual" report; however R8 language is "quarterly" reporting of past year. It appears this standard is going to be in an update status 4 times per year, plus any event modifications plus personnel changes. This could be overly burdensome due to the expanding world of cyber security.
Ameren	No	While we agree with the intent to list certain minimum requirments for the Operating Plan, the draft list is too lengthy and prescriptive. This merely creates opportunites for failure to comply rather the real purpose of reporting data that can be used to meaningfully increase the reliability of the BES by identifying trends of events that may otherwise be ignored.
American Electric Power (AEP)	No	Component 2.2 "Method(s) of assessing cause(s) of impact events" is very vague. Furthermore, there are concerns whether these methods can be accomplished within one hour as might be required per Attachment

Organization	Yes or No	Question 4 Comment
		1, in addition to operating the system. Component 2.6 - need to add the statement "as appropriate for type of impact event" Components 2.7 through 2.9 - are good concepts to consider for future inclusion, but at this point in time these appear to be overreaching objectives. We recommend the SDT take smaller increments towards future progress at measure and reasonable pace. Furthermore, if Component 2.9 is retained it should only pertain to lessons learned on the reporting of impact events not all recommendations regarding remediation of the impact events themselves. Furthermore, the 30 day window to update the Operating Plans is aggressive considering the other priorities that may be present day to day.
ATC	No	The requirement should be rewritten to simply state that the Functional Entities has to meet the reporting obligations documented in Attachment 1. How the Functional Entity meets the obligations documented in Attachment 1 should be determined by the Functional Entity, not the requirement. The prescriptive nature of this requirement does not support the performance-based Standards that the industry and NERC are striving towards. In addition, requirement 2.9 creates an alternate method for NERC to develop Standards outside of the ANSI process. This requirement dictates that Functional Entities are required to incorporate lessons learned from NERC reports into their Plan, which is a requirement of this Standard.
BGE	No	R2.1 Creates the opportunity for differences in identifying impact events. BGE recommends additional clarity in the statement. Are we to use Attachment 1 as a "bright line" or can we use our Operating Plan to identify what an impact event is?R2.4 - 2.6 Does a standard need to specify both internal and external lists? 2.7 - is "component" defined anywhere? Is it a component of the BES or a component of the Operating Plan or a component of the three lists in 2.4 to 2.6?Rationale --- Parts 3.3 and 3.4?? Do you mean 2.3 and 2.4?Is the Operating Plan under scrutiny (mandatory and compensable) for all items in the last paragraph of the rationale?

Organization	Yes or No	Question 4 Comment
CenterPoint Energy	No	CenterPoint Energy does not agree with R2 and M2 as they are focused on process and procedure. Compliance with a reporting requirement should be based on a complete and accurate report submitted in a timely manner. The process an entity uses to accomplish that task is of no consequence. CenterPoint Energy recommends R2 and M2 be deleted.However, if the SDT feels it is necessary to include this process based requirement, CenterPoint Energy believes the SDT, in requiring an overly prescriptive Operating Plan, has expanded the requirement beyond the current CIP-001-1 and EOP-004-1 which only require "...procedures for the recognition of and for making operating personnel aware..." (CIP-001-1) and "...shall promptly analyze..." (EOP-004-1). Specifically, R2.2 is not found in the current Standards. "Methods for assessing causes(s) of impact events" would vary greatly depending upon the type and severity of the event. Responsible Entities would have a difficult time cataloging these various methods to any specific degree and if they are not specific then CenterPoint Energy questions their value in a documented method. R2.3 is not found in the current Standards and is an unnecessary requirement as the method of notification is irrelevant so long as the notification is made. R2.7, R2.8, and R2.9 are also unnecessary expansions beyond what is currently in CIP-001-1 and EOP-004-1. CIP-001-1 requires the Responsible Entity review its procedures annually and CenterPoint Energy believes this is sufficient. When taken in total, R2 requires seven (7) different processes, provisions, and methods. CenterPoint Energy recommends R2.2, R2.3, R2.7, R2.8 and R2.9 be deleted and believes this will not result in a reliability gap.
City of Garland	No	There are 4 "methods" and 2 "provision" required for this requirement - in other words, 6 "paperwork" items that auditors will audit and likely penalize entities for. On page 1, the statement is made "...proposed standard in accordance with Results-Based Criteria." Having to have 4 methods and 2 provisions to end with a report (all of which is paperwork) is not a "result based" standard. It is like being required to have a "plan to plan on planning on composing and filing a report". Events need to be analyzed, communicated, and reported and

Organization	Yes or No	Question 4 Comment
		should be audited as such (results based) - not audited on whether they have a book filled with methods and provisions.
Consolidated Edison Co. of NY, Inc.	No	Requirement R2 o Lead-in paragraph - Following the words “Attachment 1” add a period and the words “The Operating Plans shall” and then delete “that” and make “includes” singular. o R2.1, 2.2, 2.3, 2.7 - Replace the word “Method(s)” with the word “Procedure(s)”. o 2.6 - After the word “notify” add a period, then insert the words “For example, external organizations may include” and delete the words “to include but not limited to.” o 2.8 - After the words “Operating Plan based on” add the word “applicable”.Rational R2After the words “Every industry participant that owns or operates,” add the words “Bulk Electric System.” Then delete the words “on the grid.”
Constellation Power Generation and Constellation Commodities Group	No	Constellation Power Generation and Constellation Commodities Group has several issues with this requirement, but in general, this requirement is heavily prescriptive, administrative in nature, and is unclear whether it will positively impact BES reliability. As examples of administrative requirements that have no impact on reliability, please consider the following comments: oListing personnel in R2.4, - merely having a list of personnel does not add to the sufficiency of an Operating Plan, but it does create a burdensome obligation to maintain a list. As well, specifying “personnel” may limit plans from designating job titles or other designations that may more appropriately and consistently carry reporting responsibility in the Operating Plan. oR2.5 is unclear as to the intent of the requirement - what is threshold of notification? Is the list to be those that have a role in the event response or a list of all within the facility who may receive news notification of the event? Also, as explained above for 2.4, a list is not a beneficial to reliability, but is administratively burdensome. oWhat is the reasoning for the 30 day timeframe in R2.7 R2.8 and R2.9? The timeframe is not based on a specific necessity, and creates an unreasonable time frame for changing the Operating Plan, in

Organization	Yes or No	Question 4 Comment
		particular if lessons learned are either short turn adjustments or comprehensive programmatic changes what warrant more time to properly institute. In addition, coupled with other requirements (R4, R5, R8), the updating requirements of R2.7, R2.8 and R2.8 potentially create a continually updating Operating Plan which could create enough confusion to reduce the effectiveness of the Operating Plan. The updating and time frame requirements do not impact reliability, but again impose significant administrative burden and compliance exposure. oR2.9 is particularly problematic for its connection to R8. R8 requires NERC to create quarterly reports with lessons learned and R2.9 requires the registered entities to amend their Operating Plans? What if NERC doesn't write an annual or quarterly report? Are the registered entities out of compliance? The "summary of concepts" for this latest revision, as written by the SDT, includes the following items: oA single form to report disturbances and impact events that threaten the reliability of the bulk electric system oOther opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements oClear criteria for reporting oConsistent reporting timelines oClarity around of who will receive the information and how it will be usedMany of the sub-requirements in R2 do not address any of these items and do not serve to establish a high quality, enforceable and reliability focused standard. Constellation Power Generation therefore recommends that R2 be amended to read as follows:R2. Each Applicable Entity identified in Attachment 1 shall have an Operating Plan(s) for identifying, assessing and reporting impact events listed in Attachment 1 that includes the following components: 2.1. Method(s) for identifying impact events listed in Attachment 12.2. Method(s) for assessing cause(s) of impact events listed in Attachment 12.3. Method(s) for making internal and external notifications should an impact event listed in Attachment 1 occur. 2.4. Method(s) for updating the Operating Plan.2.5 Method(s) for making operation personnel aware of changes to the Operating Plan.
Consumers Energy	No	R 2.7, R 2.8 and R 2.9 are creating a requirement to have procedures to update procedures. Having updated

Organization	Yes or No	Question 4 Comment
		procedures should be the requirement, no more.
Duke Energy	No	Sections 2.4 and 2.5 should allow identification of responsible positions/job titles rather than specific people. Section 2.9 only allows 30 days for updates to our plan based upon lessons learned coming out of an annual report. 60-90 days would be more appropriate. Also, Section 2.9 says it's an annual report, while R8 only requires quarterly reports.
Dynegy Inc.	No	For 2.7, 2.8, 2.9, 30 days is to stringent. Some changes may not warrant changes until a cumulative amount of changes occur. Suggest making it no later than an annual review.
E.ON Climate & Renewables	No	Administrative burden to some of the components such as 2.5.
Electric Market Policy	No	This is an overly prescriptive requirement given the intent of this standard is after-the-fact reporting. The requirement to create an Operating Plan lacks continuity with the ERO Event Analysis Process that is currently slated to begin industry field testing on October 25, 2010. Suggest the SDT coordinate EOP-004-2 efforts with this process.R2.6 establishes an external organization list for Applicable Entity reporting, yet R1 suggests that external reporting will be accomplished via submittal of impact event reports. How will the two requirements be coordinated? What governmental agencies are appropriate and how will duplicative reporting be addressed (for example, DOE, Nuclear Regulatory Commission)? Also, in the "rationale for R2", please explain the reference to Parts 3.3 and 3.4.
ERCOT ISO	No	ERCOT ISO recommends the use of "Registered Entity" in place of "Applicable Entity". This would provide consistency with other requirements and Attachment 1. Recommend the following changes to the subrequirements. "2.6. List of external organizations to notify to include but not limited to NERC, Regional

Organization	Yes or No	Question 4 Comment
		Entity, relevant entities within the interconnection, Law Enforcement, and Governmental or Provincial Agencies.""2.7. Process for updating the Operating Plan within 30 days of any changes not of an administrative nature. This includes updates to reflect any lessons learned as a result of an exercise or actual event."Remove requirement 2.8 and move content to requirement 2.7."2.8. Process for updating the Operating Plan within 30 days of publication the NERC annual report of lessons learned."Add "2.9. Process to ensure updates are communicated to personnel responsible for under the Operating Plan within 30 days of the change being completed."
Exelon	No	R.2.4 and 2.5 - should not be required to have a list of internal personnel. If an entity has an Operating Plan that covers internal and external notifications that should be sufficient.R2.2.7, 2.8, 2.9 - R4 requires an annual drill. Updating the plan if required following an annual drill should be sufficientWhy does an entity need to develop a stand alone Operating Plan if there is an existing process to address identification, assessing and reporting certain events?30 day implementation for a component change or lesson learned does not seem reasonable or commensurate with the potential impact to the BES and should not be a required element of EOP-004.What is the communication protocol for lessons learned outside of the annual NERC report? What process will be followed and who will review, evaluate, and disseminate lessons learned that warrant updating the Operating Plan?
FirstEnergy	No	The term Operating Plan(s) is not the appropriate term for this standard. These should be called Reporting Plan(s). Operating Plans are usually designed to be applied during the operating timeframe. Parts 2.2 and 2.6 - We suggest changes to these two subparts as well as a new 2.2.1 and 2.6.1 as follows: 2.2. Method(s) for assessing the initial probable cause(s) of impact events(Add) 2.2.1. Method(s) for assessing the external organizations to be notified.2.6. List of external organizations to notify in accordance with Part 2.2.1. to

Organization	Yes or No	Question 4 Comment
		include but not limited to NERC, Regional Entity, and Governmental Agencies.(Add) 2.6.1. Method(s) for notifying Law Enforcement as determined by Part 2.2.1.Parts 2.4 and 2.6: This should be a list of job titles for ease of maintenance. An entity may choose to use someone in a job position that is a 24 by 7 operation with several personnel that cover that position over the 24 by 7 period. Listing each person by name should not be required as personnel change while the operating responsibility related to the job title can remain constant. We suggest changing the wording to "2.4. List of the job titles of internal company personnel responsible for making initial notification(s) in accordance with Parts 2.5.and 2.6.2.5. List of the job titles of internal company personnel to notify."Part 2.6 - We are under the impression that the phrase "include but not limited to" should not be used according to the NEW SDT guidelines. We suggest changing this to say "List of external organizations to notify that includes at a minimum, NERC, Regional Entity, and Governmental Agencies. (A provincial agency is a governmental agency)."Part 2.7. is overly burdensome. FE suggests the team revise to simply reflect annual updates that should consider component changes and updates from lessons learned. This also permits parts 2.8 and 2.9 to be deleted. FE proposes the following text for Requirement R2.7 "Annual review, not to exceed 15 months between reviews, and update as needed of the Reporting Plan that considers component changes and continuous improvement changes from lessons learned."Parts 2.8 and 2.9 - FE proposes to delete part 2.8 and 2.9. We do not see a need for these changes since the plan must be updated annually and will cover lessons learned.
Great River Energy	No	A. As detailed in R2, the Operating Plan shall contain provisions for “identifying, assessing, and reporting impact events”. R2.8, and R2.9 do not have a correlation to R2’s Operating Plan. Where, R2.7 states to update the Operating Plan when there is a component change. We believe that the components of this Operating Plan are only 1) indentifying impact events, 2) assessing impact events, and 3) reporting impact events. R2.8 and R2.9 are based on Lessons Learned (from internal and external sources) and do not fit in

Organization	Yes or No	Question 4 Comment
		the components of an entity's Operating Plan. R2.7 requires the Operating Plan to be updated. As written, every memo, simulations, blog, etc that contain the words "lessons learned" would be required to be in your Operating Plan. It is solely up to an entity to implement a "Lesson Learned" and not the place for this SDT to require an Operating Plan to contain Lessons Learned. Recommend that R2.8 and R2.9 be deleted for this requirement. If R2.8 and R2.9 are not removed, R5.3 will be in a constant state of change. B. In R2.8 & R2.9, It may be difficult to implement lessons learned within 30 days. We suggest that lessons learned should be incorporated within 12 calendar months if lessons learned are not deleted from the R2.8 & R2.9.
Green Country Energy	No	Highly administrative version of what could accomplish the same thing. A requirement that the applicable entitiy shall make appropriate notificatiions as required by attachment A and B events. I can see the need for review and lessons learned but that needs to be done at a higher level since many entities may be involved in an "event"
Idaho Power Company	No	The SDT needs to clarify Requirement 2.9 references an annual report issued persuant to requirement R8, however Requirement 8 references a quarterly report. These requirements should have the same time frames.
Indeck Energy Services	No	R2 needs to state that the Operating Plan needs to only those Attachment 1 events applicable to the Registered Entity. The Operating Plan should contain a list of these events so that the other Requirements can reference the Operating Plan and not Attachment 1 for the list of events. For example a GO/GOP <2,000 MW would not need to address this type of event and it wouldn't be listed in its Operating Plan. It would be unnecessarily cumbersome, to describe events which are not covered within the Operating Plan.
Independent Electricity System	No	R2 is not needed. An entity does not need to have an "operating plan" to identify and report on impact events;

Organization	Yes or No	Question 4 Comment
Operator		it needs only to report on the events listed in Attachment 1 in a form depicted in Attachment 2. How does the entity do this, and whether or not an operating plan is in place, or whether its staff is trained to provide the report should not need to be included in a reliability standard for so long as the responsible entity provides the report in the required form on time. If the responsible entity fails to report the listed events in the depicted format, it will be found non-compliant, and that's it - no more and no less. If the "operating plan" really means an established data collection and reporting procedure, then the requirement should be revised to more clearly convey the intent.
IRC Standards Review Committee	No	The SRC suggests that this is not, in fact, an Operating Plan. At most, it may be a reporting plan or reporting procedure. Most of these requirements are administrative and procedural in nature and, therefore, do not belong as requirements in a Reliability Standard. Perhaps they could be characterized as a best practice and have an associated set of Guidelines developed and posted on the subject.As proposed, the Operating Plan is not required to ensure bulk power reliability. As stated in the purpose of this standard, it does not cover any real-time operating notifications for the types of events covered by CIP-001, EOP-004. The Operating Plan requirements as proposed seem only to be suitable for real-time notifications. Since these incidents are meant to be reportable after-the-fact, familiarity with the reporting requirements and time frames is sufficient. Unlike the real-time operating notifications which have relatively short reporting time frames, there is sufficient time for personnel to make appropriate communications within their organizations to make timely after the fact reports under NERC Section 1600 authority. Would it be feasible for NERC to issue a standing requirement for timely after-the-fact reports under NERC Section 1600 authority?
ISO New England Inc.	No	This is an overly prescriptive requirement given that the intent of this standard is after-the-fact reporting. The requirement to create an Operating Plan is an unnecessary burden that offers no additional improvements to

Organization	Yes or No	Question 4 Comment
		the reliability of the Bulk Electric System, and this is not, in fact, an Operating Plan. At most, it may be a reporting plan. Most of these requirements are administrative and procedural in nature and, therefore, do not belong as requirements in a Reliability Standard. Perhaps they could be characterized as a best practice and have an associated set of Guidelines developed and posted on the subject.As proposed, the Operating Plan is not required to ensure Bulk Electric System reliability. As stated in the purpose of this standard, it does not cover any real-time operating notifications for the types of events covered by CIP-001, EOP-004. Since these incidents are meant to be reportable after-the-fact, familiarity with the reporting requirements and time frames is sufficient.Stating reporting requirements directly in the standard would produce a more uniform and effective result across the industry, contributing towards a more reliable Bulk Electric System.R2.6 establishes an external organization list for Applicable Entity reporting, yet R1 suggests that external reporting will be accomplished via submittal of impact event reports. How will the two requirements be coordinated? What governmental agencies are appropriate, and how will duplicative reporting be addressed (for example, DOE, Nuclear Regulatory Commission)? Also, in the "rationale for R2", please explain the reference to Parts 3.3 and 3.4.
Kansas City Power & Light	No	We agree with the rationale for R8 requiring NERC to analyze Impact Events that are reported through R6 and publish a report that includes lessons learned but disagree with R2.9 obligating an entity to update its Operating Plan based on applicable lessons learned from the report. Whether lessons learned are applicable to an entity is subjective. If an update based on lessons learned from an annual NERC report is required, the requirement should clearly state the necessity of the update is determined by the entity and the entity's Reliability Coordinator or NERC can not make that determination then find the entity in violation of the requirement. In addition, if an update based on lessons learned from a NERC report is required, NERC should publish the year-end report (R8) on approximately the same day annually (i.e. January 31) and allow

Organization	Yes or No	Question 4 Comment
		an entity at least 60 days to analyze the report and incorporate any changes it deems necessary in its Operating Plan. In addition, the language using quarterly and annual as a requirements between R2.9 and R8 is confusing.
MidAmerican Energy	No	R2 and R5 coupled with R8 will drive quarterly updates (in addition to drills, etc) and training to the literally hundreds to thousands of people per company for the proper internal operating personnel and management will actually hurt the development of a culture of compliance by overwhelming personnel with constant plan changes and training.The standards drafting team should remove all 30 day references or provide the technical basis of why revising plans and training to "changes and lessons learned" quarterly all within 30 days is the right use of reliability resources to improve the grid.The addition of the 30 day constraints and new vague criteria in Attachment one such as "damage to a BES element through and external cause" or "transmission loss of multiple BES elements which could mean two or more" is the opposite of clear standards writing or results based standards. We disagree with requiring an Operating Plan for identifying, assessing, and reporting impact events. This is an administrative requirement that has no clear reliability benefit. Furthermore, it is questionable that event reporting even meets the basic definition of an Operating Plan. Per the NERC glossary of terms, Operating Plans contain Operating Procedures or Operating Processes which encompass taking action real-time on the BES not reporting on it. As detailed in R2, the Operating Plan shall contain provisions for "identifying, assessing, and reporting impact events". R2.8, and R2.9 do not have a correlation to R2's Operating Plan. Where, R2.7 states to update the Operating Plan when there is a component change, the components of this Operating Plan are only 1) indentifying impact events, 2) assessing impact events, and 3) reporting impact events. R2.8 and R2.9 are based on Lessons Learned (from internal and external sources) and do not fit in the components of an entity's Operating Plan. R2.7 requires the Operating Plan to be updated. As written, every memo, simulations, blog, etc that contain the

Organization	Yes or No	Question 4 Comment
		words "lessons learned" would be required to be in your Operating Plan. It is solely up to an entity to implement a "Lesson Learned" and not the place for this SDT to require an Operating Plan to contain Lessons Learned. Recommend that R2.8 and R2.9 be deleted for this requirement. If R2.8 and R2.9 are not removed, R5.3 will be in a constant state of change. In R2.8 & R2.9, It may be difficult to implement lessons learned within 30 days. The NSRS recommends to incorporate lessons learned within 12 calendar months if lesson learned are not deleted from the R2.8 & R2.9.
Midwest ISO Standards Collaborators	No	We disagree with requiring an Operating Plan for identifying, assessing, and reporting impact events. This is an administrative requirement that has no clear reliability benefit. Furthermore, it is questionable that event reporting even meets the basic definition of an Operating Plan. Per the NERC glossary of terms, Operating Plans contain Operating Procedures or Operating Processes which encompass taking action real-time on the BES not reporting on it. What is an impact event? It appears that this undefined, ambiguous term was substituted for sabotage which is also undefined and ambiguous. One of the SARs stated goals was to "provide clarity on sabotage events". This does not provide clarity.
MRO's NERC Standards Review Subcommittee	No	A. As detailed in R2, the Operating Plan shall contain provisions for "identifying, assessing, and reporting impact events". R2.8, and R2.9 do not have a correlation to R2's Operating Plan. Where, R2.7 states to update the Operating Plan when there is a component change. The NSRS believes the components of this Operating Plan are only 1) indentifying impact events, 2) assessing impact events, and 3) reporting impact events. R2.8 and R2.9 are based on Lessons Learned (from internal and external sources) and do not fit in the components of an entity's Operating Plan. R2.7 requires the Operating Plan to be updated. As written, every memo, simulations, blog, etc that contain the words "lessons learned" would be required to be in your Operating Plan. It is solely up to an entity to implement a "Lesson Learned" and not the place for this SDT to

Organization	Yes or No	Question 4 Comment
		require an Operating Plan to contain Lessons Learned. Recommend that R2.8 and R2.9 be deleted for this requirement. If R2.8 and R2.9 are not removed, R5.3 will be in a constant state of change. B. In R2.8 & R2.9, It may be difficult to implement lessons learned within 30 days. The NSRS recommends to incorporate lessons learned within 12 calendar months if lesson learned are not deleted from the R2.8 & R2.9.
North Carolina Electric Coops	No	This requirement dictates details of documentation of after-the-fact reporting of events which cannot impact reliability of the BES and, as such, should not be a reliability standard. The cost and burden of becoming auditably compliant with this requirement can be extreme for small entities.
Northeast Power Coordinating Council	No	This is an overly prescriptive requirement given that the intent of this standard is after-the-fact reporting. The requirement to create an Operating Plan is an unnecessary burden that offers no additional improvements to the reliability of the Bulk Electric System, and this is not, in fact, an Operating Plan. At most, it may be a reporting plan. Most of these requirements are administrative and procedural in nature and, therefore, do not belong as requirements in a Reliability Standard. Perhaps they could be characterized as a best practice and have an associated set of Guidelines developed and posted on the subject.As proposed, the Operating Plan is not required to ensure Bulk Electric System reliability. As stated in the purpose of this standard, it does not cover any real-time operating notifications for the types of events covered by CIP-001, EOP-004. Since these incidents are meant to be reportable after-the-fact, familiarity with the reporting requirements and time frames is sufficient.Stating reporting requirements directly in the standard would produce a more uniform and effective result across the industry, contributing towards a more reliable Bulk Electric System.R2.6 establishes an external organization list for Applicable Entity reporting, yet R1 suggests that external reporting will be accomplished via submittal of impact event reports. How will the two requirements be coordinated? What governmental agencies are appropriate, and how will duplicative reporting be addressed (for example, DOE,

Organization	Yes or No	Question 4 Comment
		Nuclear Regulatory Commission)? Also, in the "rationale for R2", please explain the reference to Parts 3.3 and 3.4.
Pacific Gas and Electric Company	No	PG&E would like clarification on whether the 30 days, is calendar days or business days.
Pacific Northwest Small Public Power Utility Comment Group	No	See #15
Pepco Holdings, Inc - Affiliates	No	For R 2.7, 2.8 and 2.9, 30 days may be too short a time for large entities with multiple subsidiaries to do the necessary notice and coordination. PHI suggests 90 days.
PNM Resources	No	PNM would like clarification on whether the 30 days, is calendar days or business days.
PPL Electric Utilities	No	While we agree with documenting our process, we feel the use of the defined term Operating Plan is not required and possibly a misuse of the term. We would like to suggest using the term 'procedure'. Additionally, we would like the SDT to confirm/clarify whether Attachment 1 is a complete list of impact events. Also, please confirm that the Proposed R2.1 language 'Method(s) for identifying impact events' means identifying impact event occurrence as opposed to identifying list of impact events. i.e. does R2.1 mean recognize impact event occurrence?
PPL Supply	No	While we agree with concept addressed in R2, we don't agree with use of the defined term Operating Plan. Consider working the requirement as follows: "Each Applicable Entity identified in Attachment 1 shall have a documented process or program that includes the following components:..." Also, please consider changing 2.1 to be"Method(s) for recognizing the occurrence of impact events." The current wording could be

Organization	Yes or No	Question 4 Comment
		interpreted to mean, "create a list of the impact events."
Puget Sound Energy	No	While the concept of an operating plan is reasonable, the requirements for update in sections 2.7, 2.8 and 2.9 will lead to an immense amount of work for the entities subject to the standard. In addition, constant revisions to the operating plan makes it difficult to cement a habit through this procedure. The proposed update schedule does not strike the appropriate balance between the need to respond to lessons learned and the value of plan continuity.
RRI Energy, Inc.	No	1. R2 includes the phrase "for identifying, assessing and reporting," followed by R2.1 which states "identifying," R2.2 which states "assessing" and both R2.3 and R2.6 state "notify" or "making internal and external notifications" (i.e., reporting). The language is unnecessarily redundant. RECOMMENDATION: Reword R2 phrase "for identifying, assessing and reporting," to simply state, "for addressing."2. Rationale for R2 - The rationale section for R2 references in the third paragraph "Parts 3.3 and 3.4." Was this intended to reference R2.3 and R2.4?
Santee Cooper	No	The words “operating plan” should be removed from the requirement. This standard deals exclusively with after-the-fact reporting. This requirement is also overly prescriptive.
SERC OC Standards Review Group	No	This is an overly prescriptive requirement that dictates details of documentation and, as such, has no place in a reliability standard. NERC needs to trust the RCs to do their jobs; this standard and this requirement in particular seems to be attempting to codify the actions that an RC would take in response to an event. The cost and burden of becoming auditably compliant with this requirement is extreme and unrealistic, especially on small entities

Organization	Yes or No	Question 4 Comment
Southern Company - Transmission	No	The Operating Plan has a different connotation for different operations folks. We suggest that we call it an Impact Event Reporting Plan.
Tenaska	No	We have adequate compliance procedures already in place for the existing CIP-001-1 and EOP-004-1 Standards. The list of required “Operating Plan” components in the proposed R2 is too specific. Maintaining the “Operating Plan” described in R2 would increase the burden on Registered Entities to comply with the Standard and this type of "laundry list" Requirement would make it more difficult to prove compliance with EOP-004-2 during an audit.
United Illuminating	No	R2.9 requires provisions to update the Operating Plan based on the annual ERO report developed in R8. The ERO report does not appear to be providing lessons learned to be applied to the Operating Plan for impact event reporting, but more focsed on trends and threats to the BES. Also 30 days after the report is published by NERC is not enough time for the entity to read, and assess the report, and then to administratively update the Operating Plan. UI agrees that the Operating Plan should be reviewed annually and updated subsequent to the review within 30 days.
US Bureau of Reclamation	No	R2 does not reconcile with Attachment A or the sub paragraphs. As an example, the requirement 2.6 states "List of organizations to notify ...." All sub paragraphs use the term notify. Notify as used in Attachment A is when a report cannot be provided in the time frame listed in Attachment A. Therefore there is no requirement in this standard for the Operating Plan to have a provision for reporting.The subparagraph 2.8 indicates that the Entity must update it plan based on the lessons learned published by NERC. It would be appropriate to require a review and update of the plan based on the lessons learned.

Organization	Yes or No	Question 4 Comment
We Energies	No	R2.3, R2.4: “Part” is not a defined term or used in the NERC Standard Process Manual.R2: Attachments are not mentioned in the NERC Standard Process Manual. Is this a mandatory or informational part of the standard?R2.6 (and possibly R2.5): There does not seem to be discretion in notifications. Are all people or organizations on the notify lists always contacted for every impact event? Even Law Enforcement?R2.7: What is a “component? A Plan component? A BES component?R2.9: There is no annual NERC report issued pursuant to R8. R8 requires quarterly reporting.
WECC	No	Need clarification on whether the 30 days is calendar days or business days. As noted in the comment to question 3, any impact event where sabotage is suspected should be treated differently from those where sabotage is not suspected.
Arizona Public Service Company	Yes	AZPS agrees with R2, however, the use of the term "Operating Plan" is confusing. A more accurate term would be "Event Reporting Plan."
ATCO Electric Ltd.	Yes	
City of Austin dba Austin Energy	Yes	
Georgia System Operations Corporation	Yes	An entity-developed Operating Plan will allow the flexibility needed to address different entity relationships around the country, e.g., generating companies, cooperatives, munis, large IOUs, small IOUs, RTOs/ISOs, non-independent market area, and so on.However, all applicable entities should not be required to report directly to NERC or the region. The system should allow for partial reporting and hierarchical reporting. Entities within an area should be allowed to coordinate their plans to define reporting procedures within their area. They could have an entity at some wide scope top level that reports to NERC and the region the

Organization	Yes or No	Question 4 Comment
		information collected from multiple narrow scope lower levels within their wide area. If every small lower level entity directly reported to NERC and the Region, it could create situational confusion rather then situation awareness.
Manitoba Hydro	Yes	R2 - 2.1 to 2.9 detail what is expected of an Operating Plan for Impact Events.The attachment 1 details the event, the threshold parameters and time line. Though the threshold parameters in the attachment may be questioned, this greatly clarifies the expectations of reporting events. Further events should be added to this list:"Detection of suspected or actual or acts or threats of physical sabotage"
Luminant Energy	Yes	
Nebraska Public Power District	Yes	
NERC Staff	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	
TransAlta Corporation	Yes	

5. Do you agree with the requirement R3 and measure M3? Please explain in the comment box below.

Summary Consideration: There was no consensus amongst stakeholders who responded to this question. Requirement R3 has been re-written to exclude the requirement to "assess the initial probable cause". The only remaining reference to "cause" is in the Impact Event Reporting Form (Attachment 2). Here, there is no longer a requirement to assess the probable cause. The probable cause only needs to identified, and only if it is known at the time of the submittal of the report.

Organization	Yes or No	Question 5 Comment
Ameren	No	There are too many missing details on how this will be accomplished. As stated before, this Draft requires too much time be invested in verbal reports, "Preliminary" reports, "Final" reports and even "Confidential" reports (Attachment 2). If the goal is to report ASAP details on events which could impact BES reliability, all of these reports will need to be made at the worst possible time - when Operators are trying to collect data, analyze what they find and correct major problems on the system. And if the reports are wrong or not issued fast enough, the Operators will be keenly aware of potential fines and violations.
American Electric Power (AEP)	No	Not clear how this is different from R6 since it relies on the same timetable in Attachment 1.
ATC	No	ATC believes that this requirement should be deleted and that the SDT should coordinate its goal with the EAWG. We believe that the lessons learned process and identification of root cause is better covered under that process than through the NERC Mandatory Standards.
BGE	No	R3. Limits responsibility to Attachment 1 events only and mandates that an "initial probable cause" be identified. Are we at liberty to define "initial probable cause" and define time period for completion in the Operating Plan? BGE believes this could cause wide difference between Operating Plans and the standard

Organization	Yes or No	Question 5 Comment
		should be more prescriptive by relating to a time-table for the life of an impact event, including expected identification time, initial assessment time and analysis time leading to the reporting deadlines.BGE recommends not including examples of evidence in a measure but include it in a Guideline. Including in a measure will be translated as a requirement by an auditor.
CenterPoint Energy	No	CenterPoint Energy does not agree with R3 and M3 as written as the Company does not agree with the requirement to have an Operating Plan (see comments to Q4 above). However, if R2 and M2 were to be deleted, and R3 was revised to read; "Each Applicable Entity shall identify and assess initial probable cause of events listed in Attachment 1.", CenterPoint Energy could agree with this requirement.
City of Garland	No	Should be part of R2 or R6 - this is unnecessary duplication
Constellation Power Generation and Constellation Commodities Group	No	This requirement introduces double jeopardy for registered entities. If an entity does not include methods for identifying impact events and for assessing cause per R2.1 and R2.2 in their Operating Plan, they will be out of compliance with R2. Without the methods in R2 the registered entity is out of compliance with R3 as well for failing to identify and assess. Constellation Power Generation therefore recommends that R3 be amended to be incremental to R2 and read as follows: R3. Each Applicable Entity shall implement their Operating Plan(s) to identify and assess cause of impact events listed in Attachment 1.
Electric Market Policy	No	We think "impact event" needs to be defined in the NERC Glossary to provide the clarity the industry needs to build audit ready compliant procedures.
ERCOT ISO	No	ERCOT ISO recommends the use of "Registered Entity" in place of "Applicable Entity". This would provide consistency with other requirements and Attachment 1. The measure for this requirement notes the obligation

Organization	Yes or No	Question 5 Comment
		for “documentation”. This is not addressed in the requirement. The measure also notes “on its Facilities”. This clarification of scope should be addressed in the requirement. R3. Each Registered Entity shall identify, assess, and document initial probable cause of impact events on its Facilities listed in Attachment 1.
Exelon	No	: Agree that Each Applicable Entity shall identify and assess initial probable cause of impact events; disagree with aspects and time requirements in Attachment 1.
FirstEnergy	No	M3 - Power flow analysis would be used to assess the impact of the event on the BES, not to determine initial probable cause. It is more likely that DME would provide the data for the initial probable cause evaluation. We suggest rewording M3 as follows: "To the extent that an Applicable Entity has an impact event on its Facilities, the Applicable Entity shall provide documentation of its assessment or analysis. Such evidence could include, but is not limited to, operator logs, voice recordings, or disturbance monitoring equipment reports. (R3)"
Green Country Energy	No	Actually yes and no... An event may be caused, analyzed and corrected by one entity but most likely it will involve more. Low Voltage or frequency may not be caused by a generator but the generator will see the event and to have the generator assess the probable cause seems inappropriate. I can see reporting the event and duration and making notifications.
Indeck Energy Services	No	R3 should reference the events covered by the Operating Plan, as listed in it, rather than in Attachment 1. If the Plan is deficient, it is a violation of R2 and not every other Requirement that references the Plan.
Independent Electricity System Operator	No	We agree that the responsible entity needs to identify and assess initial probable cause of impact events but not in accordance with any operating plan in R2. Each operating entity (RC, BA, TOP) has an inherent responsibility to identify the cause of any system events to ensure it complies with a number of related

Organization	Yes or No	Question 5 Comment
		operational standards. R3, in fact, could be revised to require the Responsible Entity to include the probable cause of impact events in its report, rather than asking it to "identify and assess" since this is not measurable. Also, the ERO may be removed from the Applicability Section depending on the response to our comments under Q9.
IRC Standards Review Committee	No	Although it is useful for entities to make an initial assessment of a probable cause of an event, this requirement should stand alone and does not need to be tied to requirement R2, Operating Plan. Quite often, it takes quite some time for an actual cause to be determined. The determination process may require a root cause analysis of some complexity.Further, in the case of suspected or potential sabotage, the industry can only say it doesn't know, but it may be possible. It really is the law enforcement agencies who make the determination of whether sabotage is involved and the info may not be made available until an investigation is completed, if indeed it is ever made available.
ISO New England Inc.	No	We think "impact event" needs to be defined in the NERC Glossary to provide the clarity the industry needs to build auditable compliance procedures.Although it is useful for entities to make an initial assessment of a probable cause of an event, this requirement should stand alone and does not need to be tied to requirement R2, Operating Plan. Quite often, it takes a considerable amount of time for an actual cause to be determined. The determination process may require a complex root cause analysis.Further, in the case of suspected or potential sabotage, the industry can only say it doesn't know, but it may be possible. Law enforcement agencies make the determination of whether sabotage is involved, and the information may not be made available until an investigation is completed, if indeed it is ever made available.
Kansas City Power & Light	No	We believe R3 and M3 are unnecessary as a stand alone requirement and measure and propose combining this requirement and measure with R6 and M6. Identifying and assessing the initial probable cause of an

Organization	Yes or No	Question 5 Comment
		impact event is the obvious starting point in the reporting process and ultimate completion of the required report. Evidence to support the identification and assessment of the impact event and evidence to support the completion and submittal of the report are really one in the same.
Manitoba Hydro	No	Though each local entity should identify and assess initial probable cause of impact events as per their Operating Plan, the creation of this Operating Plan could be labor intensive and also guidelines for consistency within an RC region should be created.So “NO” is entered simply because a large time line would be needed to properly and efficiently implement R3 and R4.
MidAmerican Energy	No	
Midwest ISO Standards Collaborators	No	While we agree that it makes sense to report on the cause of an event, we disagree with the need for an Operating Plan as identified in R2.
North Carolina Electric Coops	No	The term “impact event” needs to be defined in the NERC Glossary to provide the clarity the industry needs to build auditably compliant procedures and give guidance on what is proper to report.
Northeast Power Coordinating Council	No	"Impact event” needs to be defined in the NERC Glossary to provide the clarity the industry needs to build auditable compliance procedures.Although it is useful for entities to make an initial assessment of a probable cause of an event, this requirement should stand alone and does not need to be tied to requirement R2, Operating Plan. Quite often, it takes a considerable amount of time for an actual cause to be determined. The determination process may require a complex root cause analysis.Further, in the case of suspected or potential sabotage, the industry can only say it doesn’t know, but it may be possible. Law enforcement agencies make the determination of whether sabotage is involved, and the information may not be made

Organization	Yes or No	Question 5 Comment
		available until an investigation is completed, if indeed it is ever made available.
Pacific Northwest Small Public Power Utility Comment Group	No	Comments: When applying R3 to row 11 of attachment 1, the comment group notes that applicable entities are expected to assess probable cause of BES equipment damage, including that which may be the result of criminal behavior. At best this would needlessly duplicate the efforts of law enforcement. A more likely result is that entity involvement would interfere with law enforcement and ultimately hinder prosecution of those responsible. Also See #15
PPL Electric Utilities	No	We believe the rationale for R3 is good and provides value. However, we feel the clarity was lost when the rationale was translated to the standards language. Please consider revising language to refocus on rationale of assess and report per Attachment 1 as opposed to identify. We suggest changing the word “identify” to “recognize” and add the Rationale statement to the requirement as follows: “Each Applicable Entity shall assess the causes of the reportable event and gather available information to the complete the report.”
PPL Supply	No	Please consider changing the word "identify" to "recognize" and adding the Rationale statement to the requirement as follows: "Each Applicable Entity shall assess the causes of the reportable event and gather available information to complete the report."
RRI Energy, Inc.	No	"Identify and assess" - Auditors are as much in need of clearly worded, unambiguous Reliability Standards are as Registered Entities. This phrase leaves much too wide a range of interpretations, almost guaranteeing regular and frequent disagreements during an audit between Registered Entity and Regional Entity auditor as to what constitutes "identify and assess" sufficient to meet the intent of this Requirement. Compounding this issue is the Rationale for R3 that states an Applicable Entity (which should probably read "applicable

Organization	Yes or No	Question 5 Comment
		Functional Entity") should "gather enough information to complete the report that is required to be filed." While Rationale statements are not technically part of the standard, this emphasizes the current wording of the requirement as subject to random and arbitrary interpretation by auditors and Registered Entities. RECOMMENDATION: Change "identify and assess" to "document," so that the Requirement now reads "Each Applicable Entity shall document initial probable cause of impact events..." including an option for "cause not determined".
Santee Cooper	No	Does the initial probable cause have to be reported within the timing associated in Attachment 1? Entities may not have enough information that soon to report the initial probable cause. This should be done with events analysis.
SERC OC Standards Review Group	No	We think “impact event” needs to be defined in the NERC Glossary to provide the clarity the industry needs to build auditably compliant procedures.
Tenaska	No	The probable cause of a reportable event is already required to be submitted on the OE-417 form. This Requirement is redundant.
TransAlta Corporation	No	Clarity required Does an entity have to report on the cause of every “applicable” impact event they witness even though the event did not originate at their plant, system or region and did not adversely affect them? Essentially this would require every entity that witnessed an “applicable” event to report on its cause. In most cases they will not know the cause if they did not create the event. Measure M3 should reference Attachment 1 to indicate the Time to Submit Report’.
We Energies	No	A DP may not have Facilities (a BES element). See NERC Glossary definition of Facility.

Organization	Yes or No	Question 5 Comment
Bonneville Power Administration	Yes	Known causes are difficult under 1 hour reporting requirements. (Unusual events are even harder to narrow down in 24 hours and may take weeks.)
Consolidated Edison Co. of NY, Inc.	Yes	We agree, however, the term “impact event” must be part of the NERC glossary.
Georgia System Operations Corporation	Yes	It directly supports the purpose of the standard.
Great River Energy	Yes	While we agree that it makes sense to report on the cause of an event, we disagree with the need for an Operating Plan as identified in R2
MRO's NERC Standards Review Subcommittee	Yes	The NSRS thanks the SDT for stating “initial probable cause” as this is in direct correlation to the Purpose which states “known causes”.
Puget Sound Energy	Yes	However, this requirement doesn't address the timing required for this analysis. This may be intentional and appreciated because at times the analysis can take months when the events are complex in nature.
US Bureau of Reclamation	Yes	This is provided that the report submitted in Attachment A does not include the probable cause. It is highly unlikely that a probable cause may be determined within the reporting timelines.
Arizona Public Service Company	Yes	
ATCO Electric Ltd.	Yes	

Organization	Yes or No	Question 5 Comment
City of Austin dba Austin Energy	Yes	
Duke Energy	Yes	
Dynegy Inc.	Yes	
Idaho Power Company	Yes	
Luminant Energy	Yes	
NERC Staff	Yes	
Pacific Gas and Electric Company	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	
Pepco Holdings, Inc - Affiliates	Yes	
PNM Resources	Yes	
Southern Company - Transmission	Yes	

Organization	Yes or No	Question 5 Comment
United Illuminating	Yes	
WECC	Yes	

6. Do you agree with the requirement R4 and measure M4? Please explain in the comment box below.

Summary Consideration: Note R4 has been moved to R3 due to rearranging of requirements. The DSR SDT did a full review based on comments that were received. R3 now is stream lined to read:

R3. Each Responsible Entity shall conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 at least annually, with no more than 15 months between such tests. The testing of the procedure (as stated in R1) is the main component of this requirement. Several commenters provided input that too much "how" was previously within R3 and the DSR DST should only provide the "what". The DSR SDT did not provide any prescriptive guidance on how to accomplish the required verification within the rewrite. Testing of the entity's Operating Process (R1) could be by an actual exercise of the process (testing as stated in FERC Order 693 section 471), a formal review process or real time implementation of the process. The DSR SDT reviewed Order 693 and section 465 directs that processes "verify that they achieve the desired result". This is the basis of R3, above.

Organization	Yes or No	Question 6 Comment
Ameren	No	Establishing a program with trigger actions expected to require reporting several times a year, combined with adequate initial, and on-going, training should preclude the need for mandatory drills as an added compliance burden.
ATC	No	We do not believe that a drill that exercises a written reporting obligation will add additional reliability to the BES.
BGE	No	M4. BGE recommends not including examples of evidence in a measure but include it in a Guideline. Including in a measure will be translated as a requirement by an auditor.Rationale for R4: If multiple

Organization	Yes or No	Question 6 Comment
		exercises are performed are all of them subject to the sub-R2 requirements and to audit/audit findings?
Bonneville Power Administration	No	There was no drill required for CIP-001 (a drill was in CIP-008, but the purpose did not list combining CIP-008). A drill is not needed for reporting Electrical Grid events, designate it as excluded in the intent of the requirement.
CenterPoint Energy	No	CenterPoint Energy does not agree with R4 and M4. See comments to Q4 above. In addition to the process vs. results based issue stated above, CenterPoint Energy believes conducting a drill to verify recognition, analysis, and reporting procedures is a waste of valuable resources and time.
City of Garland	No	Existing CIP 001 and EOP 004 are reporting standards - neither currently requires annual drills or exercises. Combining these two (2) should not entail expanding the requirements to include drills or exercises. There are existing drills / exercises that must be performed annually for compliance with CIP 008 & CIP 009 which require the same basic identifying, assessing, developing lessons learned, responding, and reporting skill sets. Requiring additional drills or exercises for this new combined standard will provide additional "business overhead" that results in basically nothing that is not obtained by the CIP 008 / 009 drills as far as securing or making the BES reliable. It does, however, result in additional audit risk at audit time.
Constellation Power Generation and Constellation Commodities Group	No	It is not clear how this requirement to conduct drills and exercises relates to the concepts spelled out by the SDT:oA single form to report disturbances and impact events that threaten the reliability of the bulk electric systemoOther opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirementsoClear criteria for reportingoConsistent reporting timelines oClarity around of who will receive the information and how it will be usedR4 does not address any of the above items and should therefore be removed from this standard.

Organization	Yes or No	Question 6 Comment
Consumers Energy	No	NERC should either standardize on a 12 month year or an annual year for reviews.
Dynegy Inc.	No	What is the basis for the drill being annual. This is to stringent. I suggest it be every 3 years.
Electric Market Policy	No	The need for a periodic drill has not been established and appears to be overly restrictive given the intent of the standard is reporting of impact events. Suggest this requirement be eliminated.
ERCOT ISO	No	ERCOT ISO believes that a drill or exercise of its Operating Plan is unnecessary. The intent of the drill can be addressed within the training requirements under R5.
Exelon	No	If drills remain as a component of the standard, an effort to consolidate updating an entities plan with a requirement to drill the plan should be made. . Each entity/utility should be able to dictate/determine if they need a drill for a particular event. Is this document implying a drill for every type of event?
FirstEnergy	No	FE suggests that this requirement be deleted. FE does not see a reliability need for conducting a drill on reporting. This is overly burdensome and should not be included within this reliability standard. Training on the plan and periodic reminder of reporting obligations should suffice.
Great River Energy	No	We disagree with the need to conduct a drill for reporting
Green Country Energy	No	Another training requirement with what benefit? We must train on all of our NERC requirements now anyway to insure compliance and that's not a requirement, thats implied and I think thats enough.
Indeck Energy Services	No	In M4, it is suggested that data from a real event would be evidence. R4 should be satisfied if the Operating

Organization	Yes or No	Question 6 Comment
		Plan is used for a real event within 15 months of the last drill or event.
Independent Electricity System Operator	No	Along the line of our comments on R2 for an operating plan (whose need we do not agree with), a drill, exercise, or Real-time implementation of the Operating Plan for reporting is also not necessary.
IRC Standards Review Committee	No	Similar to our comments on R2 for an Operating Plan, a drill, exercise, or Real-time implementation of its Operating Plan for reporting is unnecessary. Such things are really training practices. There are already existing standards requirements regarding training. There is no imminent threat to reliability that requires these events to be reported in a short time frame as may be required for real-time operating notifications.
ISO New England Inc.	No	The need for a periodic drill has not been established, and appears to be overly restrictive given the intent of the standard is the reporting of impact events. Suggest this requirement be eliminated. Similar to our comments on R2 for an Operating Plan, a drill, exercise, or Real-time implementation of its Operating Plan for reporting is unnecessary. Such things are training practices. There are already existing standards requirements regarding training. There is no imminent threat to reliability that requires these events to be reported in as short a time frame as may be required for real-time operating conditions notifications.
Kansas City Power & Light	No	We believe R4 and M4 are clearly unnecessary. Thoughtful preparation of an Operating Plan per R2 that specifically addresses personnel responsibilities and appropriate evidence gathering combined with the training requirement in R5 is sufficient.
Luminant Energy	No	We support the requirements outlined in R2 which create significant obligations to maintain and update the required Operating Plan. However, we believe annual drilling for a reporting process seems unnecessary, particularly given the response horizon of 24 hours for the majority of impact events. If drilling is required, the

Organization	Yes or No	Question 6 Comment
		standard should allow actual events to fulfill a drilling requirement as stated in the Rationale for R4 and within the text of M4.
Manitoba Hydro	No	Drills and exercise for implementation of the Operating Plan are important and critical, but as in question 5, or Requirement R3, careful and detailed creation of the Operating Plan are crucial to facilitate proper training, drills and exercises.So "NO" is entered simply because a large time line would be needed to properly and efficiently implement R4 and R3.
MidAmerican Energy	No	
Midwest ISO Standards Collaborators	No	We disagree with the need to conduct a drill for reporting.
North Carolina Electric Coops	No	Requiring a drill for "reporting" is unnecessary and burdensome. Reporting is covered in processes and procedures and during the normal training cycle. We recommend the elimination of this requirement.
Northeast Power Coordinating Council	No	The need for a periodic drill has not been established, and appears to be overly restrictive given the intent of the standard is the reporting of impact events. Suggest this requirement be eliminated. Similar to our comments on R2 for an Operating Plan, a drill, exercise, or Real-time implementation of its Operating Plan for reporting is unnecessary. Such things are training practices. There are already existing standards requirements regarding training. There is no imminent threat to reliability that requires these events to be reported in as short a time frame as may be required for real-time operating conditions notifications.
Pacific Gas and Electric	No	PG&E believes the addition of a drill constitutes additional training and should be added to R5. PG&E is

Organization	Yes or No	Question 6 Comment
Company		concerned as to who the target audience for this annual training would affect.
Pacific Northwest Small Public Power Utility Comment Group	No	See #15
PNM Resources	No	PNM feels the addition of a drill or exercise constitutes additional training and believes R4 should be added to R5. The WECC OTS also is interested as to what level does the annual training target, for instance, the field personnel. Will they have to complete the exercise/drill?
RRI Energy, Inc.	No	Every employee in a Registered Entity might potentially have exposure to an impact event, and therefore result in a list of thousands of employees subject to the EOP-004-2 Operating Plan. Does this mean, for example, an applicable Functional Entity with 3,000 employees, each capable of potentially observing an impact event, must include them in the drill, exercise, or Real-Time implementation? Such an expectation would require a hypothetical email notice to be sent to 3,000 employees, advising them "This is a test - You observe a suspicious vehicle driving around the fence of your power plant. Perform the next action you should take." The result in this hypothetical might be 3,000 phone calls and emails to the responsible employee in the applicable Functional Entity, each needing to be documented and retained for the audit period.As stated above in question 5, auditors need guidance as much as Registered Entities. Otherwise, it is observed that they will seek the most stringent approach they observe from the best of the best practices over the first year of implementation and apply that expectation as the base-case, under which all other approaches will be deemed violations.
Santee Cooper	No	There is no need to drill for administrative reporting! This requirement should be deleted.

Organization	Yes or No	Question 6 Comment
SERC OC Standards Review Group	No	We think this requirement is unclear - we think it requires a drill for “reporting”, which seems absurd! We recommend the elimination of this requirement.
Tenaska	No	This Requirement is too specific and places additional burdens on Registered Entities.
US Bureau of Reclamation	No	There is no rationale offered on why 15 months was selected. Without a defined basis the time period is arbitrary. It would be appropriate to let the Entity determine and document the time interval. That would allow the time frame to be sensitive to the complexity of the Operating Plan. Some entities aregeographically dispersed and a single Operating Plan may be difficult to test atone time or within 15 months.The allowance for real time events or actual use is a good move and maymake it easier to define a suitable time frame by the Entity.
WECC	No	The addition of a drill or exercise constitutes additional training and believes R4 should be added to R5. Clarification is needed as to what level does the annual training target, for instance, the field personnel. Will they have to complete the exercise/drill?
American Electric Power (AEP)	Yes	
Arizona Public Service Company	Yes	AZPS agrees with R4, however, the use of the term "Operating Plan" is confusing and leads one to believe an Operating Drill is necessary for a "reporting plan drill." A more accurate term to use would be "Event Reporting Plan."
Georgia System Operations Corporation	Yes	We agree with R4 with "... at least annually, with no more than 15 months ..." replaced with "... at least once per calendar year, with no more than 15 months ..." as in R5.

Organization	Yes or No	Question 6 Comment
MRO's NERC Standards Review Subcommittee	Yes	The NSRS agrees that to enhance reliability and situational awareness of the BES, the Operating Plan be exercised once per calendar year.
United Illuminating	Yes	Suggest R4 be improved to state that a Registered Entity is only required to conduct a drill or execute real-time implementation of the Operating Pan for one impact event listed in the attachment. In other words the Registered Entity is not required to drill on reporting each type of impact event on an annual basis.
ATCO Electric Ltd.	Yes	
City of Austin dba Austin Energy	Yes	
Consolidated Edison Co. of NY, Inc.	Yes	
Duke Energy	Yes	
Idaho Power Company	Yes	
NERC Staff	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	
Pepco Holdings, Inc - Affiliates	Yes	

Organization	Yes or No	Question 6 Comment
PPL Electric Utilities	Yes	
PPL Supply	Yes	
Puget Sound Energy	Yes	
Southern Company - Transmission	Yes	
TransAlta Corporation	Yes	
We Energies	Yes	

7. Do you agree with the requirement R5 and measure M5? Please explain in the comment box below.

Summary Consideration: Most stakeholders who responded to this question indicated disagreement with the originally proposed Requirement R5 and Measure M5. (Note R5 has been moved to R4 in the revised standard.) The DSR SDT did a full review based on comments that were received. The major issues that were provided by commenters was R5.3 and R5.4 and their contents. Upon detailed review the DSR SDT agrees with the majority of comments received with R5.3 and R5.4 and have removed them completely from the Standard. Training is still the main theme of this requirement as it pertains to the personnel in the procedure (R1). R4 now is stream lined to read:

> R4. Each Responsible Entity shall review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan at least annually with no more than 15 calendar months between review sessions

Organization	Yes or No	Question 7 Comment
Green Country Energy		Same as my comment for question 6
Arizona Public Service Company	No	AZPS believes the required training is too restrictive for minor changes/edits to the Event Reporting Plan.
ATC	No	ATC believes it is an inherent obligation of all Functional Entities to train their appropriate staff to meet all applicable NERC Standards. Including a training requirement in some, but not all, Standards implies that the other Standards do not necessitate training. Although this is an important Standard and one that should be included in a Functional Entities' training program, ATC does not believe that this Standard is more important than the other NERC Standards and, therefore, requires a separate training provision
ATCO Electric Ltd.	No	R5.3 requires an entity to conduct training within 30 days of a revision to the Operating Plan. For an entity

Organization	Yes or No	Question 7 Comment
		that covers a wide area, 30 days may not be sufficient to reach all employees.
BGE	No	Suggested revision to clarify R5:Each Applicable Entity shall provide training to all internal personnel identified in its Operating Plan on the Operating Plan annually. Training is only on Reporting, pursuant to R2, not on the Operating Plan?BGE does not believe the SDT needs to identify sub bullets on this requirement. R5.1 is not logical --- what does it mean?
CenterPoint Energy	No	CenterPoint Energy believes that R5 and M5 are not necessary and should be deleted. CenterPoint Energy supports an entity training its staff in any reporting responsibilities; however, such training should be the responsibility of each entity and such requirements do not belong in a NERC standard. In addition, CenterPoint Energy believes any necessary training requirements are covered in the PER Standards and therefore the addition of this requirement adds redundancy to the Standards.If a majority of the industry supports such a requirement, CenterPoint Energy cannot support R5 and M5 as written as we do not agree with the requirement to develop and maintain an Operating Plan (see comments to Q4 above). CenterPoint Energy offers the following alternate language: “Each Applicable Entity shall provide training concerning reporting requirements contained in this Standard to internal personnel involved in the recognition or analysis of events listed in Attachment 1.
City of Garland	No	This expands beyond the original CIP 001 and EOP 004 - neither explicitly requires training - combining does not mean expanding. In reality, what practical skill are you going to train on? People who perform the analysis on an event are going to have job specific training external to this standard and those same folks will maintain their skill set external to this standard. If it is going to be a results based criteria standard, then let the entities be responsible. Training on methods to fill out and file paper work does not make the BES more reliable. The vast majority of other standards do not have a training requirement section and yet, entities manage to be

Organization	Yes or No	Question 7 Comment
		compliant with those standards. Compared to all the other reliability standards and their requirements, are penalties for training on filling out paper work really making the BES more secure and reliable?
Consolidated Edison Co. of NY, Inc.	No	Requirement 5 - Training should be targeted only at those responsible for implementing the Operating Plan (OP), not all those mentioned in the OP.R5 - After the words “internal personnel” add the words “responsible for implementing.” The delete the words “identified in” and “for reporting pursuant to Requirement R2.”5.4 - Following the words “For internal personnel” add the words “responsible for implementing the Operation Plan.” Between the words “revised responsibilities” add the word “implementation.”M5 - After the words “between the people” add the words “responsible for implementing the Operating Plan”
Constellation Power Generation and Constellation Commodities Group	No	Constellation Power Generation questions how R5 relates to the SDT’s “summary of concepts”:oA single form to report disturbances and impact events that threaten the reliability of the bulk electric systemoOther opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirementsoClear criteria for reportingoConsistent reporting timelines oClarity around of who will receive the information and how it will be usedHowever, Constellation Power Generation believes that security awareness is an important aspect of personnel security and proposes an annual training similar to what was in the previous standards. Constellation Power Generation therefore recommends two requirement changes that would achieve security awareness without the burdensome administrative aspects. First, as stated earlier, a sub requirement in R2 should be added which reads as follows: R2.5 Method(s) for making operation personnel aware of changes to the Operating Plan.Second, this training requirement should be rewritten as follows: Each Applicable Entity shall provide training to all operation personnel at least annually.
Consumers Energy	No	Again, either 12 month year or annual year, NERC needs to standardize on one or the other. Training should apply only to those that must take action relevant the reliability of the BES. A plan would likely include

Organization	Yes or No	Question 7 Comment
		notification of senior officers, however they don't need to be included in drills and training if they have no active role.
Duke Energy	No	Strike the word "all" in the requirement. All personnel don't need to be trained - for example, the plan may contain references to some personnel as potential sources of the information that will then be reported. Also, Section 5.3 only allows 30 days for training, which may be impossible with rotating shift personnel and training schedules. 60 days is more appropriate.
Dynegy Inc.	No	The annual training seems excessive especially if their have been no changes. You have included one exception for contact information revisions; however, it should be expanded to include exceptions for minor/non-substantial changes. Also, make training requirements (after initial training)be required for substantive changes only.
E.ON Climate & Renewables	No	Redundant with R4.
Electric Market Policy	No	The need for a periodic training has not been established and appears to be overly restrictive given the intent of the standard is reporting of impact events. Suggest this requirement be eliminated.
Exelon	No	Exelon doesn't feel that the 30 day requirement is achievable and recommends an annual review. Training for all participants in a plan should not be required. Many organizations have dozens if not hundreds of procedures that a particular individual must use in the performance of various tasks and roles. Checking a box which states someone read a procedure does not add any value, it is an administrative burden with no contribution to reliability. It is Exelon's opinion that training requirements should be covered in the PER standards and that the audience to be trained should be identified. R5.4 requires internal personnel that

Organization	Yes or No	Question 7 Comment
		have responsibilities related to the Operating Plan cannot assume the responsibilities unless they have completed training. This requirement places an unnecessary burden on the registered entities to track and maintain a data base of all personnel trained and should not be a requirement for job function. A current procedure and/or operating plan that addresses each threshold for reporting should provide adequate assurance that the notifications will be made per an individual's core job responsibilities.
FirstEnergy	No	Requirement R5 and Part 5.1 - The wording in Part 5.1 is too prescriptive and shouldnot require training on the specific actions of personnel. Also, R5 should not require training for personnel that may only receive the report and are not required to do anything. Therefore we suggest rewording R5 and 5.1 as follows:"R5. Each Applicable Entity identified in Attachment 1 shall have a Reporting Plan(s) for identifying, assessing and reporting impact events listed in Attachment 1 that includes the following components:5.1 The training includes the personnel required to respond under the Reporting Plan."Part 5.3 - We suggest removing subpart 5.3. This requirement is overly burdensome and not necessary. We believe that the requirements for annual review and update of the plan as well as training sufficiently cover reviews of changes to the plan. Part 5.4 - The last phrase "training shall be conducted prior to assuming the responsibilities in the plan" should account for emergency situations when the entity does not have time to train the replacement before they are to assume a responsibility.
Great River Energy	No	We believe that this task should be incorporated into the Job Task Analysis for the System Operators and that this requirement should be deleted as being redundant.
Idaho Power Company	No	The 30 day Requirement is limited with real time operations. Most entities with real time operations utilize a 5 or 6 week rotating schedule to comply with PER-002. the NERC Continuing Education Program allows up to 60 days to comply, this allows the operating shifts to accomadate training within the operating schedule. The

Organization	Yes or No	Question 7 Comment
		requirement 5.3 should allow 60 days to complete the training.
Indeck Energy Services	No	It is wholly unreasonable to re-train everyone for each change to the Operating Plan. Suggestion: Clarify that upon changes to the Operating Plan, the Registered Entity may either require full training, or instead distribute a summary of the change to affected personnel only.
Independent Electricity System Operator	No	Along the line of our comments on R2 for an Operating Plan (whose need we do not agree with), any training on developing and providing the report is unnecessary. What matters is that the report is provided to the needed organizations or entities on time and in the required format according to established procedure. How this is accomplished goes outside of the purpose of reliability standard requirements.
IRC Standards Review Committee	No	We do not agree with the need for R5. We do not see the need for a standard requirement that stipulates training the personnel on reporting events. What matters is that the reports are provided to the needed organizations or entities on time and in the required format according to established procedure. Stipulating a training requirement to achieve this reporting is micro-managing and overly prescriptive.
ISO New England Inc.	No	The need for a periodic drill has not been established, and appears to be overly restrictive given that the intent of the standard is reporting of impact events. Suggest this requirement be eliminated. There are training standards in place that cover these requirements. We agree the relevant personnel should be “aware” of the reporting requirements. But there is not a need to have a training program with specific time frames for reporting impact events. Awareness of these reporting requirements can be achieved through whatever means are available for entities to employ to train on any of the NERC standards, and need not be dictated by requirements.

Organization	Yes or No	Question 7 Comment
Kansas City Power & Light	No	We agree with the need for the Operating plan and the provision of formal training to impacted personnel. We believe that the personnel references are too open-ended to be productive and measurable. This leaves all applicable entities open to subjectivity in assessment and may produce a large administrative burden to demonstrate compliance with no associated benefit to improved reliability.
Luminant Energy	No	Operating Plan revisions communicated through procedure updates and employee acknowledgements of the same are sufficient when coupled with a procedural training program that occurs according to a programmed schedule.
Manitoba Hydro	No	The comments in Question 6 and 7 encompass the training aspect of this requirement.
MidAmerican Energy	No	: R5.2. The NSRS agrees that to enhance reliability and situational awareness of the BES, the Operating Plan be trained once per calendar year.R5.3 As detailed in R2, the Operating Plan shall contain provisions for “identifying, assessing, and reporting impact events”. Where, R2.7 states to update the OperatingWe disagree with the need to provide formal training. We could agree with the need to communicate to System Operators and other pertinent personnel the criteria for reporting so that they know when system events need to be reported.
Midwest ISO Standards Collaborators	No	We disagree with the need to provide formal training. We could agree with the need to communicate to System Operators and other pertinent personnel the criteria for reporting so that they know when system events need to be reported.
MRO's NERC Standards Review Subcommittee	No	R5.2. The NSRS agrees that to enhance reliability and situational awareness of the BES, the Operating Plan be trained once per calendar year.R5.3 As detailed in R2, the Operating Plan shall contain provisions for

Organization	Yes or No	Question 7 Comment
		"identifying, assessing, and reporting impact events". Where, R2.7 states to update the Operating Plan when there is a component change. The NSRS believes the components of this Operating Plan are 1) indentifying impact events, 2) assessing impact events, and 3) reporting impact events. These components relate to training when the Operating Plan is revised per, R5.3, only. As written, every memo, simulations, blog, etc that contain the words "lessons learned" would be required to be in your Operating Plan and trained on every time one was issued or heard about internally or externally. Recommend that the Operating Plan be revised and training occurs when a change occurs to the entity's Operating Plan, consisting of 1) indentifying impact events, 2) assessing impact events, and 3) reporting impact events, only.
North Carolina Electric Coops	No	Requiring training to report of after-the-fact events does not improve the reliability of the BES. We recommend the elimination of this requirement.
Northeast Power Coordinating Council	No	The need for a periodic drill has not been established, and appears to be overly restrictive given that the intent of the standard is reporting of impact events. Suggest this requirement be eliminated. There are training standards in place that cover these requirements. The relevant personnel should be "aware" of the reporting requirements. But there is not a need to have a training program with specific time frames for reporting impact events. Awareness of these reporting requirements can be achieved through whatever means are available for entities to employ to train on any of the NERC standards, and need not be dictated by requirements.
Pacific Gas and Electric Company	No	PG&E believes 30 days is too restrictive due to real-time operations schedule requirements. The schedule is six weeks and individuals may be on either long change or vacation and therefore unable to complete the training within 30 days of the identification of the need. Suggest extending to 60 days to meet the training criteria which follows the NERC Continuing Education revised submittal date for the Individual Learning

Organization	Yes or No	Question 7 Comment
		Activities (ILA).
Pacific Northwest Small Public Power Utility Comment Group	No	See #15
PacifiCorp	No	Training required within 30 days of a revision to the Operating Plan is not feasible with 5 or 6 week shift rotations. A sixty day requirement would be more realistic.
Pepco Holdings, Inc - Affiliates	No	30 days may be too short a time for large entities with multiple subsidiaries to do the necessary notice and coordination. PHI suggests 90 days.
PNM Resources	No	PNM believes 30 days is too restrictive due to real-time operations schedule requirements. Most work schedules are either five or six weeks and individuals may be on either long change or vacation and therefore unable to complete the training within 30 days of the identification of the need. Based on the NERC Continuing Education revised submittal date for the Individual Learning Activities (ILA), PNM would recommend 60 days.Creating an Impact Event Report is duplicative and redundant and the WECC OTS feels this is not necessary.
PPL Electric Utilities	No	We agree with the need for training on one's process. However, we suggest changes to R5.3. Consider expanding the exception criteria to exempt non-substantive changes such as errata changes, minor editorial changes, contact information changes, etc. We also suggest saying '...,training shall be conducted, or notification of changes made, within 30 days of the procedure revisions.'
PPL Supply	No	We generally agree with R5 but recommend two changes to 5.3. Consider expanding the exception criteria to exempt non-substantive changes such as errata changes, minor editorial changes, contact information

Organization	Yes or No	Question 7 Comment
		changes, etc. Also, consider changing "training shall be conducted" to "training or communication/notification of changes shall be conducted."
Puget Sound Energy	No	The fact that proposed requirement R2 will require frequent updates to the operating plan means that the training required under this plan will occur quite frequently as well, leading to operator confusion. Even the comment allowing a review and “sign-off” will not completely mitigate this result.
RRI Energy, Inc.	No	1. This Requirement is structured to result in the same heavy-handed, zero-tolerance approach that has made CIP-004 one of the top three violated Reliability Standards. The failure in CIP-004 is that, for example, a seven-year background check or annual training program that is tardy by one day results in a violation. There is no margin of error, proviso, or cure scenario. Likewise, the proposed R5 in EOP-004-2 makes it a violation if someone takes their newly established training on the day after the end of 15 months. Systems configurations are often based on quarterly monitoring for individuals needing to take training. In addition, when dealing with potentially thousands of employees, it is inevitable that any one of hundreds of reasons might result in an employee not being included in the tracking system, and rolling past the 15th month. RECOMMENDATION: To avoid further burden to Regional Entity audit and enforcement personnel as has been the case in CIP-004, develop a cure process that allows the Registered Entity to correct the training or background check tardiness with prompt correction, fill out a notification report to submit to NERC, and proceed with protecting the reliable operation of the BES, rather than tying up Registered Entity and Regional Entity staffs with data requests, enforcement paperwork and administrative actions.2. The proposed R5.3 requires the entire applicable staff to redo the entire training within 30 days of a change to the Operating Plan. These Operating Plans will not be short documents, and formal training will not involve a 5 minute soundbite. However, for such a significant procedure as the Operating Plan, frequent changes and revisions are going to

Organization	Yes or No	Question 7 Comment
		be very common, especially given the likelihood of frequent clarifications, Compliance Action Notices ("CANs"), and lessons learned issued by NERC and Regional Entities over this very detailed set of new obligations. It is not unreasonable to expect a Registered Entity to make three or more revisions to their Operating Plan in a year, which would require training for thousands of employees three times a year, for what might amount to a single sentence revision. Furthermore, the obligation to retrain on the entire training program is not limited in this requirement to only those individuals impacted by the revision. Where a change or revision only impacts 3 possible employees, this standard would require a company with 1,500 employees subject to the Operating Plan to retake the entire training. RECOMMENDATION: Clarify that upon changes to the Operating Plan, the Registered Entity may either require full training, or instead distribute a summary of the change(s) via email to affected personnel only.
Santee Cooper	No	The concept of requiring training on reporting of after-the-fact events does not support or enhance bulk electric system reliability. We recommend the elimination of this requirement.
SERC OC Standards Review Group	No	While we support training on an annual basis for the operating plan, the concept of requiring training on reporting of after-the-fact events does not support or enhance bulk electric system reliability. We recommend the elimination of this requirement.
Southern Company - Transmission	No	We suggest that the time frame be changed to 60 or 90 days in 5.3. 5.4 needs to have a time frame associated with it; we suggest that it be 60 or 90 days.
Tenaska	No	This Requirement is too specific and places additional burdens on Registered Entities.
TransAlta Corporation	No	Measure M5 states applicable entities shall provide training material presented... This measure is unclear as

Organization	Yes or No	Question 7 Comment
		to whether the meaning is for internal personnel or to be provided to external entities upon request? Please clarify.
US Bureau of Reclamation	No	The measure is vague and redundant. The Entity is required to provide information to be used to "verify content". The information may be used to demonstrate compliance but who will verify the content is adequate and on what basis. Secondly, the measure requires training information be provided twice, once to demonstrate who participated and then to show who was trained. This is all unnecessary and could be remedied by simply stating that "evidence shall demonstrate that all individuals listed in the plan have received training on their role in the plan"
We Energies	No	Please clarify who is to be trained. As written, R5 requires any internal personnel identified in the plan, including CEO, Vice Presidents, etc., to be trained.
WECC	No	Thirty days is too restrictive due to real-time operations schedule requirements. Most work schedules are either five or six weeks and individuals may be on either long change or vacation and therefore unable to complete the training within 30 days of the identification of the need. Based on the NERC Continuing Education revised submittal date for the Individual Learning Activities (ILA), the requirement should be changed to require training to be conducted within 60 days.
Bonneville Power Administration	Yes	There was no training required for CIP-001 or in CIP-008. (The proposed EOP-008 purpose did not list incorporating CIP-008). Training was not really needed for reporting Electrical Grid events.
ERCOT ISO	Yes	ERCOT ISO believes the content of training can include an exercise or drill.

Organization	Yes or No	Question 7 Comment
United Illuminating	Yes	R5.3 coupled with the rationale provided is a sensible approach. It is important that the rational is not forgotten.
Ameren	Yes	
American Electric Power (AEP)	Yes	
City of Austin dba Austin Energy	Yes	
Georgia System Operations Corporation	Yes	
NERC Staff	Yes	
PacifiCorp	Yes	

8. Do you agree with the requirement R6 and measure M6? Please explain in the comment box below.

Summary Consideration: There was no consensus amongst stakeholders who responded to this question regarding agreement with the originally proposed Requirement R6 and Measure M6. (Note R6 been moved to R5 in the revised standard.) The DSR SDT did a full review based on comments that were received. Many comments indicated concerns with the reporting timelines within Attachment 1. (The DSR SDT has addressed those comments in response to Question 10).

Several commenters wanted the ability to report impact events to their responsible parties via the DOE Form OE-417. Following discussions with the DOE and NERC, the DSR SDT has added the ability to use of the DOE Form OE-417 when the same or similar items are required to be reported to NERC and the DOE. This will reduce the need to file multiple forms when like items must be reported to the DOE and NERC for the same impact event. The underlying fact is that impact events are to be reported within prescribed guidelines, thus providing industry awareness and starting of any analysis process. R5 now is stream lined to read:

> R5. Each Responsible Entity shall report Impact Events in accordance with the Impact Event Operating Plan pursuant to Requirement R1 and Attachment 1 using the form in Attachment 2 or the DOE OE-417 reporting form.

Organization	Yes or No	Question 8 Comment
American Electric Power (AEP)	No	It is not clear how this is different from R3 since it relies on the same timetable in Attachment 1.
CenterPoint Energy	No	CenterPoint Energy does not agree with R6 and M6 as written as we do not agree with the requirement to develop and maintain an Operating Plan (see comments to Q4 above) In addition CenterPoint Energy does not agree with the timelines required in Attachment 1 (see comments on Q10). CenterPoint Energy offers the following alternate language: “Each Applicable Entity shall report events outlined in Attachment 1 to applicable entities including but not limited to; NERC, and appropriate law enforcement agencies."

Organization	Yes or No	Question 8 Comment
City of Garland	No	1. The reporting requirements should not be expanded beyond CIP 001 and EOP 004-1. The goal for combining the two should be to make the process more efficient - not add on extra requirements for procedures on how to report, drills on reporting, training on reporting, etc. 2. The timelines requiring 1 hour reporting to the ERO are not needed and provide little realtime benefit to the BES. Real time or near real time reporting for "people on the ground" such as the RC, BA, TOP, FBI, Local Law Enforcement, DOE, etc. is necessary. They are in a position to take action in response to an event. On page 5, it states "The proposed standard deals exclusively with after-the-fact reporting. 1 Hour reporting requirements to the ERO in addition to existing reporting are not reasonable "after-the-fact" reporting requirements in the midst of an emergency. Also, there is not a 24X7 ERO center to report events to - why build and staff one when they already exists at the RC, BA, TOP, DOE, FBI, Local Law Enforcement, etc. - An ERO 24X7 center would be extra overhead that would provide no additional benefit in the first hour or hours of an emergency.
Consolidated Edison Co. of NY, Inc.	No	R2 requires applicable entities to have an Operating Plan which are company specific procedures and process required to be compliant with EOP-004. Therefore, R6 should be deleted since it is redundant with R2.
Electric Market Policy	No	Entities are already required by other agencies (e.g., DOE, NRC) to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
ERCOT ISO	No	ISO recommends the following changes to the language of the requirement.R6. Each Applicable Entity shall report impact events in accordance with Attachment 1.
Exelon	No	The time durations in the attachment are too short, it would be impossible to collect all the data necessary to report out on an impact event in the defined time to report.The SDT should evaluate each event for the most

Organization	Yes or No	Question 8 Comment
		appropriate entity responsible to ensure there is minimal confusion on who has the responsibility and eliminate duplication of reporting when feasible.
FirstEnergy	No	M6 - NERC's system should be capable of making this evidence available for the entities and provide a "return-receipt" of the reports that we send them. Also, M6 should be revised to state "Applicable Entities" as opposed to "Registered Entities".
Great River Energy	No	We believe the reporting time lines are too aggressive for some events. Reporting events within an hour is not reasonable as an entity may still be dealing the event. This will particularly difficult when support personnel are not present such as during nights, holidays and weekends.
Indeck Energy Services	No	---This is the first mention of the time lines in Attachment 1. If they are part of the standard, then they should be incorporated to the Operating Plan in R2 and then need not be mentioned again, only compliance with the plan. ---In M6, the last part, "evidence to support the type of impact event experienced; the date and time of the impact event ; as well as evidence of report submittal that includes date and time" is redundant. All of that should be in the report to NERC. If not, then it's not important to keep.
Independent Electricity System Operator	No	We agree with having a requirement to report impact events in accordance with the timelines outlined in Attachment 1, but not with the requirements indicated in R2.
IRC Standards Review Committee	No	There is not a need for an Operating Plan as proposed. This is not truly an Operating Plan. There are already other standards which create the requirements for an Operating Plan. This is an administrative reporting plan and any associated impact upon reliability is far beyond real-time operations.

Organization	Yes or No	Question 8 Comment
ISO New England Inc.	No	Entities are already required by other agencies (e.g., DOE, NRC) to report certain events. We see no need to develop redundant reporting requirements for NERC that cross other federal agency jurisdictions.There is no need for an Operating Plan as proposed. This is not truly an Operating Plan. There are already other standards which create the requirements for an Operating Plan. This is an administrative reporting plan and any associated impact upon reliability is far beyond real-time operations which is implied by the label "Operating Plan."
Kansas City Power & Light	No	We believe R3 and M3 are unnecessary as a stand alone requirement and measure and propose combining these requirements with R6 and M6. Identifying and assessing the initial probable cause of an impact event is the obvious starting point in the reporting process and ultimate completion of the required report. Evidence to support the identification and assessment of the impact event and evidence to support the completion and submittal of the report are really one in the same.
MidAmerican Energy	No	We believe the reporting time lines are too aggressive for some events. Reporting events within an hour is not reasonable as an entity may still be dealing the event. This will particularly difficult when support personnel are not present such as during nights, holidays and weekends.
Midwest ISO Standards Collaborators	No	We believe the reporting time lines are too aggressive for some events. Reporting events within an hour is not reasonable as an entity may still be dealing the event. This will particularly difficult when support personnel are not present such as during nights, holidays and weekends.
North Carolina Electric Coops	No	There is already a DOE requirement to report certain events. NERC should not be developing redundant reporting requirements when this information is already available at the federal level from other agencies.

Organization	Yes or No	Question 8 Comment
Northeast Power Coordinating Council	No	Entities are already required by other agencies (e.g., DOE, NRC) to report certain events. We see no need to develop redundant reporting requirements for NERC that cross other federal agency jurisdictions.There is no need for an Operating Plan as proposed. This is not truly an Operating Plan. There are already other standards which create the requirements for an Operating Plan. This is an administrative reporting plan and any associated impact upon reliability is far beyond real-time operations which is implied by the label “Operating Plan".
Pacific Gas and Electric Company	No	PG&E believes that if the standard is intended to be an after the fact report, we question the one and/or twenty-four hour reporting criteria and then the 30 day criteria?
Pacific Northwest Small Public Power Utility Comment Group	No	See #15
PNM Resources	No	PNM believes there seems to be redundancy in reporting based on the time frames in Attachment 1, i.e. OE-417 and other required reports. If this standard is intended to be an after the fact report, why is there one/twenty-four hour reporting criteria?
PPL Electric Utilities	No	We understand the rationale for this standard and support the project to combine EOP-004 and CIP-001 as well as the reporting requirement in CIP-008. We are concerned that it may be difficult to meet Attachment 1 Part B Potential Reliability Impact submittal times as the time to submit is 1 or 24 hour after occurrence. E.g. Risk to BES equipment, the example given is a major event and easy to conclude. Consider forced intrusion, risk to BES equipment (increased violence in remote area), or cyber intrusion - should Attachment 1 state ‘report within 24 hours after detection’?

Organization	Yes or No	Question 8 Comment
PPL Supply	No	It may be difficult to meet Attachment 1 Part B Potential Reliability Impact submittal times as the time to submit is 1 or 24 hours after occurrence. Consider changing the Time to Submit Report for Forced intrusion, Risk to BES equipment, and Detection of a cyber intrusion to be "report within 24 hours after detection".
RRI Energy, Inc.	No	RECOMMENDATION: Clarify that the reporting of impact events shall be to those entities identified in the Operation Plan section developed specifically in Section 2.6. Reference to Attachment 1 indicates reporting to "external" parties is the intent for R6.
Santee Cooper	No	If the DOE form is going to continue to be required by DOE, then NERC should accept this form. Entities do not have time to fill out duplicate forms within the time limits allowed for an event. This is burdensome on an entity
SERC OC Standards Review Group	No	There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
Southern Company - Transmission	No	The time to submit report column needs to be more flexible with time frames.
Tenaska	No	The reporting timelines are currently listed on the OE-417 form. This Requirement is redundant.
TransAlta Corporation	No	R6 should reference Attachment 2 to make it clear that this report form must be used.M6 seems to be requesting evidence that the Confidential Impact Event Report was submitted. TransAlta suggests the submission of the actual report is evidence the report was submitted.Records of this submission can be provided on request.Web Reports Project 2009-01 has indicated online reporting is the direction they are

Organization	Yes or No	Question 8 Comment
		going.If the impact report becomes an online Web report the entity submitting the report has no way of confirming the report ended up at the Compliance Enforcement Authority office after it is submitted. There needs to be some method that demonstrates the report was submitted and received.
We Energies	No	The proposed definition of “impact event” needs to be clarified.
WECC	No	There seems to be redundancy in reporting based on the time frames in Attachment 1, i.e. OE-417 and other required reports. If this standard is intended to be an after the fact report, why is there one/twenty-four hour reporting criteria?
Arizona Public Service Company	Yes	AZPS believes that Operating Plan should be replaced with "Event Reporting Plan."
ATC	Yes	ATC does agree that applicable entities report on events identified in Attachment 1 (See our comments about Attachment 1), but we do not agree that applicable entities should be required by this standard to have an Operational Plan. Please see our comments to question 4.
BGE	Yes	Comments for clarification:R6. Use of Capital letters in Operating Plan makes it unnecessary to state "created pursuant to Requirement 2
Bonneville Power Administration	Yes	The requirement needs to specify who (ERO) to report to. Attachment 1 doesn’t say to report to the ERO either. Clarify or remove the difference between the report submitted and evidence of the type of impact event required in the measurement.
Georgia System Operations Corporation	Yes	It directly supports the purpose of the standard.

Organization	Yes or No	Question 8 Comment
Green Country Energy	Yes	Now this is an excellent example of all that is needed for this requirement!
Manitoba Hydro	Yes	Attachment 1 details the impact events and the thresholds of which they should be reported.
Puget Sound Energy	Yes	It is assumed that for the purposes of M6, NERC and the regions would already have access to these reports.
Ameren	Yes	
ATCO Electric Ltd.	Yes	
City of Austin dba Austin Energy	Yes	
Constellation Power Generation and Constellation Commodities Group	Yes	
Duke Energy	Yes	
Dynegy Inc.	Yes	
Idaho Power Company	Yes	
Luminant Energy	Yes	
MRO's NERC Standards Review	Yes	

Organization	Yes or No	Question 8 Comment
Subcommittee		
NERC Staff	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	
Pepco Holdings, Inc - Affiliates	Yes	
United Illuminating	Yes	
US Bureau of Reclamation	Yes	

9. Do you agree with the requirements for the ERO (R7-R8) or is this adequately covered in the Rules of Procedure (section 802)? Please explain in the comment box below.

Summary Consideration: There was no consensus amongst the commenters who responded to this question. The DSR SDT did a full review based on comments that were received. The DSR SDT has determined that R7 and R8 are not required to be within a NERC Standard since Section 800 of the Rules of Procedure already assigns this responsibility to NERC. The DSR SDT, the Events Analysis Working Group (EAWG), NERC Staff (to include NERC Senior VP and Chief Reliability Officer) had an open discussion with this item being a major topic. The DSR SDT and EAWG are working in coordination with each other to provide NERC Staff with updated language for future inclusion into the Rules of Procedure. NERC Staff, the EAWG and the DSR SDT all supported this new initiative.

Organization	Yes or No	Question 9 Comment
Ameren	No	NERC's current heavy case load should justify reviewing the impact review table only once every 2 years.
ATC	No	ATC feels the ERO obligations should be covered in the Rules of Procedure.We do not agree with the requirements assigned to the ERO, but believe that they should be incorporated into the ERO's Rules of Procedure
BGE	No	R7. Make Impact Event Table all Capital Letters(it is a title). R8. Is the term "reportable impact events" new or is impact event intended to be capitalized? R8. Does a quarterly report of the year's reportable impact events include 12 months of "reportable impact events"? This is confusing. R8. In the Rationale for R8 Impact Events appears with Capital letters - why now? Shouldn't it appear with all Capital letters throughout the document as it is a defined term? R8. There are no previous requirements to report threats (R8.3) or

Organization	Yes or No	Question 9 Comment
		lessons learned (R8.5) or trends (R8.2) to an ERO. Is this information from reports to the ERO or from ERO research?
CenterPoint Energy	No	CenterPoint Energy does not believe this requirement is necessary; however, if the SDT insists on keeping this requirement then CenterPoint Energy believes it should remain as written. Any change to Attachment 1 should go through the Reliability Standards Development Procedure.
Consolidated Edison Co. of NY, Inc.	No	See response to Question 2Requirement 7Delete the words “and propose revisions to”Following the words (Attachment 1) add a period.Following that period add the words “The ERO shall revise the table”Requirement 8RECOMMEND DELETION OF R8 - CONFIDENTIALITY CONCERNS WILL MAKE ESTABLISHING A PUBLICATION REQUIRMENT EXTREMELY CHALLENGING.
Constellation Power Generation and Constellation Commodities Group	No	The impact event table (Attachment #1), as part of a standard, would have to be FERC approved every time it is edited. That would cause it to go through NERC’s Standard Development Process, and would cause a revision to the standard each time. This will also cause revisions to each and every registered entity’s Operating Plan. Overall, this requirement causes a large administrative burden on all entities, and does not improve reliability. As stated earlier, the “summary of concepts” for this latest revision, as written by the SDT, includes the following items:oA single form to report disturbances and impact events that threaten the reliability of the bulk electric systemoOther opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirementsoClear criteria for reportingoConsistent reporting timelines oClarity around of who will receive the information and how it will be usedRequirement 7 and 8 do not address any of these items. Furthermore, for R8, it is requiring NERC to send out quarterly reports, yet entities are supposed to amend their Operating Plans based on an annual NERC report. This requirement is confusing and is not consistent with earlier requirements. Constellation Power Generation

Organization	Yes or No	Question 9 Comment
		believes that these two requirements should be removed.
Electric Market Policy	No	Having the ERO as an applicable entity is concerning as they are also the compliance enforcement authority.
ERCOT ISO	No	Recommend that the Electric Reliability Organization be removed. The Electric Reliability Organization should not be responsible for reliability functions and therefore should be excluded from reliability standards.
FirstEnergy	No	FE disagrees with the ERO as an applicable entity within a reliability standard. See our responses to Questions 2 and 3 above. We do not believe the desired ERO process is adequately covered in section 802. Section 802 deals with assessments and not event reporting.
Georgia System Operations Corporation	No	It should not be necessary for the ERO to require itself to do these things. NERC's authority should be sufficient to do these things as part of its mission.With quarterly trending and analysis of threats, vulnerabilities, lessons learned, and recommended actions in R8, R7 (an annual review) should not be necessary. The quarterly activity could include proposing revisions to Attachment 1 if warranted.An alternative would be to perform annual trending and analysis of threats, vulnerabilities, lessons learned, recommended actions, and proposed revisions to Attachment 1 if warranted.Also, the Reliability Standards Development Procedure has been replaced with the Standard Processes Manual.
Indeck Energy Services	No	Reviewing Attachment 1 annually is unnecessary. Events don't change much and if they do, a SAR is needed to consider the changes. NERC should not be included in any standard!
Independent Electricity System Operator	No	We agree with the need to update the list as needed, but it does not have to be the ERO who takes on a reliability standard to do so. It can simply be an annual project in the standards development work plan to review Attachment 1 as part of a standard. The industry will then be provided an opportunity to weigh on the

Organization	Yes or No	Question 9 Comment
		changes. Also, we do not see the reliability results or benefits of R8. The ERO can issue the report quarterly but who are audiences? What reliability purpose does it serve if no further actions are pursued upon receiving the report? Can this be done as a standing item for the ERO at, say, the BoT meeting? Or, can this be a part of the quarterly communication from the ERO to the industry? To make this a reliability standard is an over-kill, and does not conform with the results-based standard concept.From our perspective, both R7 and R8 can be removed, and the ERO can be removed from the Applicability Section as well.
IRC Standards Review Committee	No	We do not support an annual time frame to update the events list. The list should be updated as needed through the Reliability Standards Development Process. Any changes to a standard must be made through the standards development process, and may not be done at the direction of the ERO without going through the process.
ISO New England Inc.	No	Having the ERO as an applicable entity raises concern as it is also the compliance enforcement authority. Requirement R7 is unnecessary as there are already requirements in place for three year reviews of all Standards. R8 contains requirements to release information that should be protected, such as identification of trends and threats against the Bulk Electric System. This may trigger more threats because it will be published to unwanted persons in the private sector.We do not support an annual time frame to update the events list. The list should be updated as needed through the Reliability Standards Development Process. Any changes to a standard must be made through the standards development process, and may not be done at the direction of the ERO without going through the process.
Kansas City Power & Light	No	We agree with the rationale for R8 requiring NERC to analyze Impact Events that are reported through R6 and publish a report that includes lessons learned but disagree with R2.9 obligating an entity to update its Operating Plan based on applicable lessons learned from the report. Whether lessons learned are applicable

Organization	Yes or No	Question 9 Comment
		to an entity is subjective. If an update based on lessons learned from an annual NERC report is required, the requirement should clearly state the necessity of the update is determined by the entity and the entity's Reliability Coordinator or NERC can not make that determination then find the entity in violation of the requirement. In addition, if an update based on lessons learned from a NERC report is required, NERC should publish the year-end report (R8) on approximately the same day annually (i.e. January 31) and allow an entity at least 60 days to analyze the report and incorporate any changes it deems necessary in its Operating Plan. Again, the language referencing annual and quarterly in these two requirements in confusing.
Manitoba Hydro	No	Rules of Procedure appear to have a different focus then R7 and R8.Briefing on Rules of Procedure 802Assess, review and report on:1.1 overall electric operation1.2 uncertainties and risks1.3 self assessment of supply and reliability1.4 projects on customer demand1.5 impact of evolving electric market practicesthat could affect the present and future of the BESBriefing on R7 and R8R7 - ERO shall review and propose revisions to Attachment 1R8- ERO shall publish quarterly reports on trends, threats, vulnerabilities, lessons learned and recommended actions.
Midwest ISO Standards Collaborators	No	We do not agree with the requirements and we do not believe it is adequately covered in section 802. First, section 802 deals with assessments not event reporting. Secondly, since attachment 1 is part of a standard, it should not be modified outside of the Reliability Standards Development process.
NERC Staff	No	NERC staff believes that requirements R7 and R8 are not needed because they are intrinsic expectations from its Rules of Procedure. Furthermore, these elements are necessary for analysis in support of the Reliability Metrics efforts NERC is leading under its Reliability Assessment and Performance Analysis

Organization	Yes or No	Question 9 Comment
		program.
North Carolina Electric Coops	No	The ERO cannot be subject to a requirement for which it is the compliance enforcement authority.
Northeast Power Coordinating Council	No	Having the ERO as an applicable entity raises concern as it is also the compliance enforcement authority. Requirement R7 is unnecessary as there are already requirements in place for three year reviews of all Standards. R8 contains requirements to release information that should be protected, such as identification of trends and threats against the Bulk Electric System. This may trigger more threats because it will be published to unwanted persons in the private sector.We do not support an annual time frame to update the events list. The list should be updated as needed through the Reliability Standards Development Process. Any changes to a standard must be made through the standards development process, and may not be done at the direction of the ERO without going through the process.
Puget Sound Energy	No	This is adequately covered by section 802 of the Rules of Procedure. There seems to be some conflict between R2.9 and R8 regarding timeframes and the specific elements required.
Santee Cooper	No	Standards cannot be applicable to an ERO because they are the compliance enforcement authority, and the ERO is not a user, owner, or operator of the BES.
SERC OC Standards Review Group	No	The ERO cannot be subject to a requirement for which it is the compliance enforcement authority. The governance in this situation appears incomplete.
United Illuminating	No	The rules of procedure adequately cover this.
US Bureau of Reclamation	No	Requirements 7 and 8 are covered in the Section 801.801. Objectives of the Reliability Assessment and

Organization	Yes or No	Question 9 Comment
		Performance Analysis Program. The objectives of the NERC reliability assessment and performance analysis program are to: (1) conduct, and report the results of, an independent assessment of the overall reliability and adequacy of the interconnected North American bulk power systems, both as existing and as planned; (2) analyze off-normal events on the bulk power system; (3) identify the root causes of events that may be precursors of potentially more serious events; (4) assess past reliability performance for lessons learned; (5) disseminate findings and lessons learned to the electric industry to improve reliability performance; and (6) develop reliability performance benchmarks. The final reliability assessment reports shall be approved by the board for publication to the electric industry and the general public.
Bonneville Power Administration	Yes	R2.9 language refers to R8 “annual” report; however R8 language is “quarterly” reporting. It appears this standard is going to be in an update status 4 times per year minimum, plus any event modifications plus personnel changes. Overly burdensome.
City of Garland	Yes	R7 - Yes as long as any changes to attachment 1 follow the “Reliability Standards Development Procedure. R8 - Yes as long as R8.6 is strictly “recommended actions.” They should not become “required actions” as this bypasses the standard development process.
Duke Energy	Yes	However, R8 only addresses quarterly reports, and R2 Section 2.9 states that there will be an annual report.
Green Country Energy	Yes	I realize this is another burden for the ERO but the information would be good to know what is going on outside the plant .
Luminant Energy	Yes	Continually refining the Impact Event table to better define which events should be reported would be extremely valuable. Section 802 does not adequately require such refinement, thus R7 and R8 are

Organization	Yes or No	Question 9 Comment
		appropriate inclusions to this standard.
MRO's NERC Standards Review Subcommittee	Yes	Should read “In accordance with Sections 401(2) and 405 of the Rules of Procedures, the ERO can be set as an applicable entity in a requirement or standard”. As stated in the text box.
RRI Energy, Inc.	Yes	We support the concept that Reliability Standard requirements and obligations that are subject to violations and penalties should all be contained in the four-corners of the Reliability Standard. If an obligation exists in the Rules of Procedures that creates a stand-alone responsibility that is subject to violation and penalty, it should be removed from the Rules of Procedure and inserted into the appropriate Reliability Standard.
ATCO Electric Ltd.	Yes	
City of Austin dba Austin Energy	Yes	
Dynegy Inc.	Yes	
Great River Energy	Yes	
Idaho Power Company	Yes	
MidAmerican Energy	Yes	
Pacific Gas and Electric Company	Yes	

Organization	Yes or No	Question 9 Comment
PacifiCorp	Yes	
PacifiCorp	Yes	
Pepco Holdings, Inc - Affiliates	Yes	
PNM Resources	Yes	
PPL Electric Utilities	Yes	
PPL Supply	Yes	
Southern Company - Transmission	Yes	
TransAlta Corporation	Yes	
We Energies	Yes	
WECC	Yes	

10. Do you agree with the impact event list in Attachment 1? Please explain in the comment box below and provide suggestions for additions to the list of impact events.

Summary Consideration: Most commenters who responded to this question disagreed with some aspect of Attachment 1 – most commenters provided specific suggestions for improvement. The DSR SDT did a full review based on comments that were received. The DSR SDT, the Events Analysis Working Group (EAWG), NERC Staff (to include NERC Senior VP and Chief Reliability Officer) had an open discussion with this item being a major topic. The EAWG and the DSR SDT aligned Attachment 1 with the Event Analysis Program category 1 analysis responsibilities. This will assure that impact events in EOP-004-2 reporting requirements are the starting vehicle for any required Event Analysis within the Event Analysis Program. The DSR SDT agrees that there are similar items in the DOE Form OE 417 and EOP-004-2. DOE, NERC and the DSR SDT are in initial talks to try and reduce duplicate reporting requirements. Until such time in the future that a new process is established between the DOE and NERC, the DSR SDT has revised the standard to indicate that the use of either the DOE Form OE 417 or Attachment 2 is an acceptable reporting form for applicable entities. The DSR SDT reviewed the "hierarchy" of reporting within Attachment 1. To reduce multiple entities reporting the same impact event, the DSR SDT has stated that the entity that performs the action or is directly affected by an action will report per EOP-004-2. As an example, during a system emergency, the TOP or RC may request manual load shedding by a DP or TOP. The DP or TOP would have the responsibility to report the action that they took if they meet or exceed the bright-line criteria established in Attachment 1. Upon reporting, NERC Event Analysis Program would be made aware of the impact event and start the EA Process which is outside the scope of this Standard.

Several bright-line criteria were removed from Attachment 1. These criteria (DC converter station, 5 generator outages, and frequency trigger limits) were removed after discussions with the EAWG and NERC staff, who concurred that these items should be removed from a reporting standard and analysis process.

Organization	Yes or No	Question 10 Comment

Organization	Yes or No	Question 10 Comment
WECC		For strictly after-the-fact reporting the list of Attachment 1 is appropriate. However, as noted in our earlier comments, actual or suspected sabotage events can have a potentially significant impact on reliability and should be treated differently, with additional real-time reporting requirements. It is important that such events be identified and recognized for reliability purposes and that notices include the RC.
Ameren	No	We have numerous comments about the Attachments. (1) What are the requirements for "verbal" reporting to NERC and Regional entities? (2) What are the requirements for a "Preliminary" Impact Event Report? (3) The Voltage Deviations Event is unclear (a) Are these consecutive minutes? (b) Where is the voltage measured? (generator terminals? Point of Interconnections? Anywhere?) (c) must each Entity report separately? (d) What is the +/- 10% measured against (Generator Voltage Schedule?) (4) For Generation loss events how is an "entity" defined? (a corporate parent? each registered entity? other?) (5) Are the "Examples" in the Attachment 1 - Part A really Examples, or mandatory situations? (6) Can you define "Damage"? (7) Can you define "external cause"? (8) Can you give examples of "non-environmental external causes"? (9) The footnote 1 reference for "Damage or destruction of BES equipment" doesn't match up with the a. and b. footnotes or the 1. footnote of Attachment A - Part B. (10) How is the Operator supposed to determine what Event affects the reliability of the BES fast enough to decide whether or not to report? (11) is the Loss of off-site power (grid supply) event to a nuclear plant already covered by NUC-001?(12) What are "critcal cyber assets" since CIP-002-4 will eliminate that term? (13) When is Attachment 2 supposed to be used? (14) What is meant by the word "Confidential" in the title of the Attachment 2 report? How would the SDT propose a GO/GOP handle the reporting for the following situation? A CTG unit is dispatched and the unit is started, synchronized and put on the bus. Immediately the Operator receives a high gas alarm from the GSU. The Operator quickly shuts the unit down and de-energizes the GSU. There are no relay targets and no obvious reason for the problem. After several weeks of analysis it's determined there was an internal fault in the GSU

Organization	Yes or No	Question 10 Comment
		and it must be replaced. How would the SDT recommend all the reporting requirments in this situation be addressed with the current draft?
American Electric Power (AEP)	No	Are the times listed for the initial probable reporting under R3 or the reporting under R6?Many of these items do not constitute emergency conditions. We view many of these as too onerous and would divert operating staff from monitoring and operating the BES. In addition, some terms (i.e. Frequency Trigger Limits) are not currently defined terms. Furthermore, there are existing requirements that have obligations for entities to provide this information to the RC. For example "Detection of a cyber intrusion to critical cyber assets" is already covered under CIP-008. This creates duplicate (and potentially competing) requirements.AEP also contends that some of the timelines are very aggressive and not consummate with perceived need for the information.Transmission loss of multiple BES transmission elements (simultaneous or common-mode event)within 24 hours after occurrence is overly aggressive and should provide more specific criteria.
Arizona Public Service Company	No	AZPS believes that the list in Attachment 1 would be complete, as long as the text box of examples is included. The examples demonstrate what is necessary.
ATC	No	ATC has several areas of concern regarding Attachment 1.1. The one hour requirement for reporting will take the Functional Entities' focus off of addressing the immediate reliability issues and instead force the FE to devote valuable resources to filling out forms which will potentially reduce reliability.2. Part A:a. Provide a definition of "system wide" for the Energy Emergency requiring system-wide voltage reduction.b. Add in the clarity that for Energy Emergency requiring firm load shed pertains to a single event, not cumulative events.c. Insert the word "continuous" for Voltage Deviations.d. Take off the TOP for IROL violations. (We believe that an IROL violation should be reported by the RC and not by the TOP based on the nature of the event. Requiring both the RC and TOP to report will only result in multiple reports for a single event. The RC is in

Organization	Yes or No	Question 10 Comment
		the best position to report on an IROL violation for its RC area.)e. Take off the TO, TOP and add the LSE for Loss of Firm Load. (As a transmission only company ATC does not have contracts with end load users. Because of this the Loss of Firm Load should be the reporting obligations of the entity closes to the end load users which is the BA, DP or LSE. Failure to modify this requirement will cause confusion as to which entity has to report Loss of Firm Load. f. Define a timeframe for Generation Loss g. Multiple should be changed to "4 or more" for Transmission Loss.(ATC is concerned that this would require reporting of events that have little or no industry wide benefits but would take up considerable Registered Entity resources.)h. Provide clarity to and tighten the definition of Damage or destruction of BES equipment. The way it is written now would require over-reporting of all damaged or destroyed equipment due to a non-environmental external cause (e.g. broken insulator).3. Part B:a. Take off the TO and TOP for Loss of off-site power. (The GOP has the responsibility to acquire off-site power and we believe it is the GOP's sole responsibility to report the Loss of off-site power. Failure to correct this would result in multiple reporting for the same event.)b. Take off RC for Risk to BES equipment. (The RC function does not own BES equipment and we believe it is impossible for them to report on risk to BES equipment if they are not the owner or operator of that equipment. This standard should be required of the entity that owns/operates BES equipment. c. Provide guidance to the phrase "reasonably determine" in footnote.d. Examples provided do not provide a clear obligation for an entity to follow. (Question: How close is the train to the substation? (Inches away from the substation fence, ten feet away from the substation fence or 500 feet away from the substation fence.) In addition, this standard is so open to interpretation that no entity can demonstrate compliance with the action. We believe that the only solution is to delete this reporting requirement. Overall:Multiple Functional Entities impacted by the same event are required to report. No lead entity is identified. This will result in multiple reports of the same event. ATC does not believe that this built-in duplicity enhances reliability?

Organization	Yes or No	Question 10 Comment
ATCO Electric Ltd.	No	Attachment 1: Part A - Transmission Loss: Only sustained outages should be reportable. Also the reporting threshold needs to be quantified for impact events, for example:a) Size of DC converter Station > 200 MW.b) Impact of loss of Multiples BES transmission elements in terms of significant load (> 200 MW for > 15 min).
BGE	No	TOP determines "system-wide" voltage reductions; why place this responsibility on a TO or DP? - Load Shedding is automatic load shedding; why 100MW? Does a DP need to provide a Report when directed by the RC, BA or TOP to shed load or reduce voltage? - No examples should be included in the standard! Need to define a "BES Transmission Element". - Table shows multiple entities in "Entity with Reporting Responsibility"; is it one or is it all entities report? - In an audit who determines "reasonably determined likely motivation" - Is it justified to expect to have "motivation" knowledge within one hour of an event? - Why are the Responsible Entities reporting Interruptible Demand tripped / lost?
Bonneville Power Administration	No	BPA suggests the following:Change loss of multiple BES to 3 or more. Loss of a double circuit configuration due to lightning doesn't need a report (it's a studied contingency). Add qualifier to damage/destruction of BES equipment, since a failed PCB or a system transformer normally doesn't have a MAJOR impact to the grid.Add qualifier to Loss of "ALL" off-site power affecting nuclear...The unplanned evacuation of control center is a busy time for the backup control center, yet this standard requires 1 hour reporting. Suggest changing to 24 hours.
CenterPoint Energy	No	CenterPoint Energy appreciates the efforts of the SDT in identifying the entity with reporting responsibility. This is an improvement to the event table. CenterPoint Energy is concerned with multiple entities being listed as having Reporting Responsibility. CenterPoint Energy recommends the SDT limit this to one entity having responsibility for reporting each event. This would not preclude that entity from coordinating with other entities

Organization	Yes or No	Question 10 Comment
		to gather data necessary to complete the report. In addition, CenterPoint Energy believes there are several events that should be removed from the list. “Transmission Loss” is covered by the TPL standards and does not need to be identified or reported under EOP-004. The loss of a DC converter station or multiple BES transmission elements may or may not disrupt the reliable operation of the BES, i.e. result in blackout, cascading outages, or voltage collapse. Likewise “Damage or destruction of BES equipment” in and of itself should not be the subject of reporting. If the damage or destruction results in true disruption to the reliable operation of the BES, that impact would be reported under one of the other identified events. “Voltage Deviations” is another unnecessary event. CenterPoint Energy believes a voltage event of the proposed magnitude will, more than likely, result in other events identified in Attachment 1 such as; IROL Violation or Generation Loss and would be reported under one of those triggers. Another concern is the threshold trigger of +/- 10% for 15 minutes or more. CenterPoint Energy is unclear as to the starting point to determine the deviation. In other words is the 10% deviation from nominal voltage, such as 138kV or 345kV, or the actual voltage at the time of the event? Additionally, must the deviation occur over a “wide area” or is such a deviation at one buss enough to trigger a report? Based upon these ambiguities and concerns CenterPoint Energy recommends “Voltage Deviations” be deleted from Attachment 1. The examples that follow on page 14 should also be deleted.
City of Garland	No	This report should follow exactly the OE-417 to avoid redundant, possible conflicting, and overall confusion in reporting.Note: The table has entries that are in conflict with the OE-417 and thus can cause confusion in filing multiple reports potentially causing an entity to violate Federal Law due to the confusion. By submiting the same information on different timelines, i.e. one hour reporting under OE-417 and 24 hours under this Standard, the reports may be significantly different causing confusion from differing reports of the same event.Although we prfer the events to match the OE-417 events exactly, if the SDT decides to include a

Organization	Yes or No	Question 10 Comment
		seperate events table we make the following suggestions: Energy Emergency requiring system-wide voltage reduction: should be reportable at 5% not 3% voltage reduction. The standard should clearly state this was applicable for BES energy emergency conditions only, not voltage reductions for other reasons.On voltage deviations: it should be clear that this applies to widespread effects on the BES not a single distribution feeder that has a low voltage.For the Frequency deviation: Did not see a definition for the FTL (frequency trigger limit)Generation loss: the reportable loss of generation should be significantly more than 500 MW. The number of units at the locaton is irrelevent. Ten units at 50 MW each is no more critical than a single 500 MW unit. Under this standard, if the plant with ten 50 MW units trips it is reportable but an 800 MW single unit is not reportable. The trip of the 800 MW unit has much more effect on the sytem reliability. Damage or destruction of BES equipment: Should be limited to specific equipment such as a 765 kV autotransformer not a 138 kV lightning arrestor. This needs to be eliminated or significantly limited as to the equipment type that is reportable.
Consolidated Edison Co. of NY, Inc.	No	It is absolutely essential that the work on EOP-004 and that on the NERC Event Analysis Process (EAP) be fully coordinated. We find that there are a number of inconsistencies between these two documents. The EAP and EOP-004 are not aligned. In order to operate and report effectively entities need consistent requirements.Attachment 1Frequency Deviations - The term “Frequency Trigger Limit (FTL)” is not defined. Only defined terms should be used, or the term should be defined. If the term is defined in another standard it should be moved to the Glossary of Terms for wider use.Loss of Firm load for 15 Minutes - The text under the rightmost column entitled, Time to Submit Report, appears to be incomplete in our copy.Transmission loss and Damage or destruction of BES equipment - At the end of the wording for both under the column entitled “Threshold for Reporting” add the words “that significantly affects the integrity of interconnected system operations.”Examples - Capitalize “Critical Asset” as this is a defined term.

Organization	Yes or No	Question 10 Comment
Constellation Power Generation and Constellation Commodities Group	No	Constellation Power Generation and Constellation Commodities Group questions why the generation loss line item includes generating facilities of 5 or more generators with an aggregate of 500 MW or greater? The number of units makes no difference for reporting, as is evident in the generation thresholds written before this inclusion. The examples of damaged or destroyed BES equipment are confusing, and do not clarify the reporting event. What if a GSU at a small plant (20 MW) were to fail? Is that reportable? Constellation Power Generation believes that equipment failures that are not suspicious do not need to be reported. Finally, Constellation Power Generation and Constellation Commodities Group believes that the "loss of offsite power affecting a nuclear generation station" should be removed for the following reasons:1)The purpose of this reliability standard is stated as being: "Responsible Entities shall report impact events and their known causes to support situational awareness and the reliability of the Bulk Electric System (BES). " While the "situational awareness" portion of the purpose could be interpreted as all-inclusive, the real element deals with BES reliability. Off-site power sources to nuclear units have nothing to do with BES reliability. Why should nuclear units be treated differently?2)The issue of concern for a loss of offsite power at a nuclear station is continued power supply (other than emergency diesels) to power equipment to cool the reactor core. A nuclear unit automatically shuts down when off-site power supply is lost. Availability of off-site power is a reactor safety concern (i.e., NRC regulatory concern and a one-hour report to the NRC) - not a reliability concern that FERC/NERC would have jurisdiction over.3)There is a nuclear-specific reliability standard (NUC-001) that contemplated off-site power availability. That standard contained no reporting requirements outside of those that may be already established in current procedures. Why try to impose one here?4)A loss of offsite power will result in an emergency declaration at the nuclear facility. Notifications will be made to federal (NRC), state, and local authorities. The control room crew is already overly-burdened with notifications - any additional call to NERC/Regional Reliability orgs will add insult-to-injury for no beneficial reason. If NERC is interested, they should obtain info from NRC.5)If all else fails and the item is to remain on the table, it needs

Organization	Yes or No	Question 10 Comment
		to be clarified as a “complete” loss of off-site power lasting greater than X minutes (i.e., would we have to report a complete momentary loss that was rectified in short order by an auto-reclose or quick operator action?).
Duke Energy	No	o General Comment - many timeframes in Attachment 1 are within one hour. This is inconsistent with the stated aim of the standard, which is after-the-fact reporting, as opposed to real-time operating notifications under RCIS and other standards (e.g. TOP). This standard should not be structured to require another layer of real-time reporting. o Voltage Deviation - Plus or minus 10% of what voltage? o Frequency Deviation - this is Interconnection-wide. Do you really want a report from every RC and BA in the Eastern Interconnection?? o Transmission Loss - “Multiple BES transmission elements” should be changed to “Three or more BES transmission elements”. Also, the time to submit the report should be based upon 24 hours after the occurrence is identified. o Damage or destruction of BES equipment - need clarity on the “Examples”. Is the intent to report an event that meets any one of the four “part a.” sub-bullets? i. - critical asset should be capitalized. Disagree with the phrase “has the potential to result” in section iii. - it should just say “results”. Section iv. is too wide open. It should instead say “Damaged or destroyed with malicious intent to disrupt or adversely affect the reliability of the electric grid.” o Unplanned Control Center evacuation - see our General Comment above. Clearly in this case the reporting individuals are evacuating and cannot report in one hour. 24 hours should be more than adequate for after-the-fact reporting. o Fuel Supply Emergency, Loss of off-site power, and Loss of all monitoring or voice communication capability - see our General Comment above. Time to report should be 24 hours after occurrence is identified. o Forced intrusion, Risk to BES equipment, Detection of a cyber intrusion to critical cyber assets - time to report should be 24 hours after occurrence is identified, and critical cyber assets should be capitalized.

Organization	Yes or No	Question 10 Comment
Dynegy Inc.	No	A 2000 MW loss needs to be more clearly defined by either the BA, ISO, RC, etc. for the applicable enity.Also, what is the distinction between the "damage or destruction of BES equipment" and the generation loss of >= 2000 MWs if it is a Critical Asset which is currently drafted as those greater than 1500 MW in current draft of CIP-002-4. This could lead to 2 events with different thresholds (i.e. 1500 MW and 2000 MWs). Possibly get rid of the 2000MW criteria and let the threshhold level be the same as the Critical Asset MW level. Or remove the Critical Asset threshhold in the footnote to Attachment 1.
E.ON Climate & Renewables	No	1. Voltage deviation events are too vague for GOP. How does voltage deviations apply to GOP's or specifically renewables i.e., wind farms? 2. Define what an "entity" is. 3. Define what a "generating station" is. 4. Define what a "BES facility" is.6. Define what a control center is.
Electric Market Policy	No	1) A particular Event could be applicable to multiple entities and Attachment 1 would require each applicable entity to report the event. This is duplicative and would appear to overburden the reporting system. 2) Loss of off-site power (grid supply) reporting for nuclear plants is duplicative of reporting done to satisfy NRC requirements. Given the activity at a nuclear plant during this event, this additional reporting is not desired. 3) Cyber intrusion remains an event that would need to be reported multiple times (e.g., this standard, OE-417, NRC requirements, etc.). 4) Since external reporting for other regulators (e.g., DOE, NRC, etc.) remains an obligation of the Applicable Entity, suggest that Attachment 1 only contain impact events as defined in the current version of EOP-004.
ERCOT ISO	No	ERCOT ISO requests the reporting timeframes be changed to reflect a 24 hour requirement for all events in Attachment 1. During an impact event, operating personnel are generally involved in event resolution and not available immediately to submit reports. ERCOT ISO requests that the "Detection of a cyber intrusion to a

Organization	Yes or No	Question 10 Comment
		critical cyber asset" be removed. There are established processes defined for incident response supporting CIP-008. By including this element in Attachment 1, the Operating requirement R2 would also require procedure documents for cyber security incident response. This would be redundant and would remove the responsibility away from the subject matter experts for cyber security incident response.
Exelon	No	The listed Impact Events is lacking specific physical security related events. .In general, all impact events need to be as explicit as possible in threshold criteria to eliminate any interpretation on the part of a reporting entity. Ambiguity in what constitutes an "impact event" and what the definition of "occurrence" is will ultimately lead to confusion and differing interpretations.
FirstEnergy	No	1. The table in Att. 1 and the requirements should alleviate the potential for duplicate reporting. For example, If the RC submits a report regarding a Voltage deviation in its footprint, the report should be submitted by the RC on behalf of the RC, TOP, and GOP, and not require the TOP and GOP to submit duplicate reports.2. Regarding the "Note" before the table - We agree that under certain conditions it is not possible to issue a written report in a given time period. However, the ERO and RE should also be required to confirm receipt of the verbal communication in writing to prove that the entity communicated the event as these verbal notifications may be done by an entity using an unrecorded line.3. Organizations with many registered entities should be permitted to submit one report to cover multiple entities under one parent company name. We suggest this be made clear in the Tables, the reporting form, and in the requirements.4. Voltage Deviations Event - We suggest the team provide more clarity with regard to the types and locations of voltage deviations that constitute an event.5. Examples of BES Equipment in Part A of "Actual Reliability Impact" Table - Is the phrase "critical asset" referring to the CIP defined term? If so, this should be capitalized.6. Under the "Time to Submit Report" column of the table, we suggest that all of the phrases end in "after identification of the

Organization	Yes or No	Question 10 Comment
		occurrence".7. Frequency Trigger Limit (FTL) for the Frequency Deviation event should be replaced with the values the FTL represent. The FTL is part of the BAAL Standards which have not been approved by the industry and are not in effect. It is possible that these terms are not used by those not participating in the field trial of the BAAL standards.
Great River Energy	No	Comments: Please provide a phone number and provision within the Note of EOP-004 - Attachment 1: Impact Events table for an entity to contact NERC if unable to contact NERC within the time described.Voltage Deviations - recommend adding the word “(continuous)” after sustained in Threshold column. This could be interpreted as an aggregate value over any length of time.Frequency deviations - recommend adding the word “(continuous)” after 15 minutes’ in Threshold column. This could be interpreted as an aggregate value over any length of time.CIP-008 R1.3 states the entity is to report Cyber Security Incidents to the ES_ISAC. Does the EOP-004 Attachment 2 fulfill this requirement?We request clarification on the Transmission Loss threshold events that constitute reporting. We also want clarification on what constitutes the loss of a DC Converter station and is there a time duration that constitutes the need for reporting or does each trip need to be reported? For example during a commutation spike the DC line could be lost for less than a minute. Does this loss require a report to be submitted? Is the SDT stating that each time a company loses their DC line, they are required to file a report even though it may not have an effect on the bulk system? What is the threshold for this loss?The SDT needs to clarify that duplicative reporting is not required and that only one entity needs to report. For instance, the first three categories regarding energy emergencies could be interpreted to require the BA and RC to both report. The reporting responsibilities in this table should be clarified based on who has primary reporting responsibility for the task per the NERC Functional Model and require only one report. For instance, since balancing load, generation and interchange is the primary function of a BA per the NERC Functional Model, only the BA should be required to provide this report.The

Organization	Yes or No	Question 10 Comment
		term Frequency Trigger Limit (FTL) is not currently defined in the NERC Glossary. The term FTL needs to be introduced at the beginning of the standard and defined as a new term.
Indeck Energy Services	No	Loss of off-site power is important to more than just nuclear plants--but which ones? Control centers or other large generators. But not small generators! Should there be a common element to Attachment 1, like the potential to cause a Reportable Disturbance, or maybe there need to be multiple criteria like that.
Independent Electricity System Operator	No	We do not support the 1 hour reporting time frames for Emergency Energy, System Separation, unplanned Control Center evacuation, Loss of off-site power, Loss of monitoring or voice communication. Energy emergency is broadcast on the RCIS which also goes to the ERO so its explicit reporting is not necessary (System Operations please verify). During other events listed above, the responsible entities will likely be concentrating its effort in returning the system to a stable and reliable state. Reporting to anyone not having direct actions to control, mitigate and contain the disturbances is secondary to restoring the system to t a reliable state. Since these are after the fact reports for awareness and/or analysis and not for real-time responses, these can be reported at a later time, up to 24 hours after the initial occurrence without any detriment to reliability, or at the very earliest: up to 1 hour after the system has returned to a reliable state, or after the backup control centre is fully functional, or after backup power is restored to the nuclear power plant, or after monitoring or voice communication is restored.
IRC Standards Review Committee	No	We do not agree with the requirement to report “detection of a cyber intrusion to critical cyber assets” as this creates a double jeopardy situation between CIP-008 and EOP-004-2 R2.6. We suggest that physical incident reporting be part of EOP-004 and cyber security reporting be part of CIP-008.
ISO New England Inc.	No	1) A particular Event could be applicable to multiple entities and Attachment 1 would require each applicable

Organization	Yes or No	Question 10 Comment
		entity to report the event. This is duplicative and would overburden the reporting system. 2) Loss of off-site power (grid supply) reporting for nuclear plants is duplicative of reporting done to satisfy NRC requirements. Given the activity at a nuclear plant during this event, this additional reporting is not desired. 3) Cyber intrusion remains an event that would need to be reported multiple times (e.g., this standard, OE-417, NRC requirements, etc.). 4) Since external reporting for other regulators (e.g., DOE, NRC, etc.) remains an obligation of the Applicable Entity, suggest that Attachment 1 only contain impact events as defined in the current version of EOP-004.What are the examples at the bottom of page 14 supposed to illustrate? Critical Asset should have the appropriate capitalization as being a defined term. Is Critical Asset what is intended to be used here? Should the "a" list be read as ANDs or Ors? Does "loss of all monitoring communications" mean "loss of all BES monitoring "communications"? Does "loss of all voice communications" mean "loss of all BES voice communications?"Are the blue boxes footnotes or examples?Does "forced intrusion" mean "physical intrusion" (which is different from "cyber intrusion")?Regarding "Risk to BES Equipment," request clarification of "non-environmental". Regarding the train derailment example, the mixture of BES equipment and facility is confusing. Request clarification for when the clock starts ticking.Regarding "Detection of a cyber intrusion to critical cyber assets", there is concern that this creates a double jeopardy situation between CIP-008 and EOP-004-2 R2.6. Suggest physical incident reporting be part of EOP-004 and cyber security reporting be part of CIP-008.
Kansas City Power & Light	No	We agree with the event descriptions listed in Attachment 1 and the review and revision of the impact table by the ERO is appropriately addressed in R7 but the time periods allowed to complete the new, longer preliminary report is insufficient. The correlation of this with the timing of the reporting quarterly and annually or pushing information for other entities' situational awareness does not allow the registered entity adequate time to thoughtfully consider the event and proposed root cause.

Organization	Yes or No	Question 10 Comment
Luminant Energy	No	The Impact Events Table might be easier to clarify if organized by Reporting Entity rather than Event Type as events vary substantially based on the affected BES component. For example, a GO or GOP cannot adequately determine if an event will significantly affect the reliability margin of the system or if an event results in an IROL. Examples specific to Reporting Entities would assist in more appropriate report submissions. Additionally, the footnote under examples of Damage or Destruction of BES Equipment, cites "A critical asset". This term must be clarified to indicate whether this refers to a Critical Asset as defined by CIP 002-1.Finally, the Fuel Supply Emergency item requires additional definitions as neither a GO nor a GOP can reasonably project if an individual fuel supply chain problem will result in the need for emergency actions by the RC or BA.
MidAmerican Energy	No	New vague criteria in Attachment one such as "damage to a BES element through and external cause" or "transmission loss of multiple BES elements which could mean two or more" is the opposite of clear standards writing or results based standards.
Midwest ISO Standards Collaborators	No	Several categories require duplicate reporting. For instance, the first three categories regarding energy emergencies could be interpreted to require the BA and RC to both report. The reporting responsibilities in this table should be clarified based on who has primary reporting responsibility for the task per the NERC Functional Model and require only one report. For instance, since balancing load, generation and interchange is the primary function of a BA per the NERC Functional Model, only the BA should be required to provide this report. As another option, perhaps the registered entity initiating the action should submit the report. If the BA did not take action and the RC had to direct the BA to take action, one could argue that perhaps the RC should submit the report then. However, if the BA takes action appropriately on their own, the BA should submit it. If the TOP reduces voltage for a capacity and energy emergency per a directive of the BA, then the

Organization	Yes or No	Question 10 Comment
		BA should report the event.
MRO's NERC Standards Review Subcommittee	No	Please provide a phone number and provision within the Note of EOP-004 - Attachment 1: Impact Events table for an entity to contact NERC if unable to contact NERC within the time described.Voltage Deviations - recommend adding the word “(continuous)” after sustained in Threshold column. This could be interpreted as an aggregate value over any length of time.Frequency deviations - recommend adding the word “(continuous)” after 15 minutes’ in Threshold column. This could be interpreted as an aggregate value over any length of time.CIP-008 R1.3 states the entity is to report Cyber Security Incidents to the ES_ISAC. Does the EOP-004 Attachment 2 fulfill this requirement?
Nebraska Public Power District	No	Since the reporting under this standard is for after the fact reporting, the minimum time to report should be the end of the next business day. The combination of the extremely short time periods to file a report and the amount of detail required in attachment 2 will lead to a reduction in the reliability of the BES. System Operators will be forced to take focus off their primary responsibility to respond to the event in order to complete the report within the required timeframe (within an hour for some events). During non-business hours the only personnel available to complete the reports will be those responsible for real-time operation of the BES. Since the background indicates this standard is only for after the fact reporting, the minimum required time to submit the report should be one business day to permit completion of the report without distracting from the real-time operation of the BES. Real-time reporting requirements are covered in other standards and should be to the Reliability Coordinator and from the Reliability Coordinator to NERC. For after the fact reporting, there is absolutely no reliability benefit for requiring reporting to be completed on such a short timeframe. This is especially true due to the amount of data required by Attachment 2.

Organization	Yes or No	Question 10 Comment
NERC Staff	No	The SDT should clarify its use of the term “critical asset” in the Examples section under Part A of the table. The term or versions of the term are used in different contexts in the NERC Reliability Standards. For instance, in CIP-002-1, Requirement 1, the Critical Asset Identification Method is used to identify its critical assets. In EOP-008-0, Requirement 1.3, the applicable entity is required to list its “critical facilities” in its contingency plan for the loss of control center functionality. The team should confirm what it is referring to in this proposed standard. To avoid confusion, the SDT may want to consider using a different term here or better clarify its meaning. Further, there exists the potential to have disparate reporting criteria in this proposed standard relative to the criteria being proposed by the Events Analysis Working Group as part of the Events Analysis Process document dated October 1, 2010. In particular, the following areas should be reconciled between the drafting team and the EAWG to ensure a consistent set of threshold criteria:Voltage Deviations --EOP-004-2: Greater than or equal to 15 minutes --EAWG Process: Greater than or equal to 5 minutesSystem Separation (Islanding) --EOP-004-2: Greater than or equal to 100 MW --EAWG Process: Greater than or equal to 1000 MWsSystem Separation (Islanding) --EOP-004-2: Does not address intentional islanding as in the case of Alberta, Florida, New Brunswick--EAWG Process: Addresses intentional islanding as in the case of Alberta, Florida, New BrunswickSPS/RAS --EOP-004-2: Does not expressly address proper SPS/RAS operations or failure, degradation, or misoperation of SPS/RAS --EAWG Process: Expressly addresses proper SPS/RAS operations or failure, degradation, or misoperation of SPS/RASTransmission Loss --EOP-004-2: Identifies Multiple BES transmission elements --EAWG Process: Provides specificity in Category 1a and 1b regarding transmission eventsDamage or destruction of BES equipment --EOP-004-2: Through operational error, equipment failure, or external cause but not linked to loss of load--EAWG Process: Identifies in Category 2h equipment failures linked to loss of firm system demandsForced intrusion--EOP-004-2: Addressed --EAWG Process: Not addressedRisk to BES equipment --EOP-004-2: Addressed --EAWG Process: Not addressedDetection of a cyber intrusion to critical cyber assets --EOP-004-2: Addressed --

Organization	Yes or No	Question 10 Comment
		EAWG Process: Not addressed
North Carolina Electric Coops	No	This list is too similar and redundant to the DOE requirements and does not provide any additional clarity on recognition of sabotage.
Northeast Power Coordinating Council	No	1) A particular Event could be applicable to multiple entities and Attachment 1 would require each applicable entity to report the event. This is duplicative and would overburden the reporting system. 2) Loss of off-site power (grid supply) reporting for nuclear plants is duplicative of reporting done to satisfy NRC requirements. Given the activity at a nuclear plant during this event, this additional reporting is not desired. 3) Cyber intrusion remains an event that would need to be reported multiple times (e.g., this standard, OE-417, NRC requirements, etc.). 4) Since external reporting for other regulators (e.g., DOE, NRC, etc.) remains an obligation of the Applicable Entity, suggest that Attachment 1 only contain impact events as defined in the current version of EOP-004.What are the examples at the bottom of page 14 supposed to illustrate? Critical Asset should have the appropriate capitalization as being a defined term. Is Critical Asset what is intended to be used here? Should the “a” list be read as ANDs or Ors? Does “loss of all monitoring communications” mean “loss of all BES monitoring “communications”? Does “loss of all voice communications” mean “loss of all BES voice communications?”Are the blue boxes footnotes or examples?Does “forced intrusion” mean “physical intrusion” (which is different from “cyber intrusion”)?Regarding “Risk to BES Equipment,” request clarification of “non-environmental”. Regarding the train derailment example, the mixture of BES equipment and facility is confusing. Request clarification for when the clock starts ticking.Regarding “Detection of a cyber intrusion to critical cyber assets”, there is concern that this creates a double jeopardy situation between CIP-008 and EOP-004-2 R2.6. Suggest physical incident reporting be part of EOP-004 and cyber security reporting be part of CIP-008.

Organization	Yes or No	Question 10 Comment
Pacific Northwest Small Public Power Utility Comment Group	No	Footnote 1 is missing from Part A, although it is referenced in column 1 row 11. Is this the Examples? The purpose of the Examples is unclear. Is it meant to limit the scope to those enumerated? This is not stated, but if not it should be removed since it adds confusion. What is meant by non-environmental? All external causes of damage or destruction come from the environment by definition. Please specify what is intended or remove the word.
PacifiCorp	No	Energy Emergency requiring firm load shedding - An SPS/RAS could operate shedding firm load but no Energy Emergency may exist. This requires clarification.Transmission Loss - Multiple BES transmission elements. Loss of two transmission lines in the same corridor due to a wildfire could qualify for this reporting. Once again clarification needed.
Pepco Holdings, Inc - Affiliates	No	Some items with one hour reporting (such as Unplanned Control Center evacuation) may be so disruptive to operations that one hour is too short. 4 hours suggested.
PPL Electric Utilities	No	While we think providing an impact event list is beneficial, we would like to see Attachment 1 revised and/or clarified. Refer to response to Question 2 considering duplicate reporting. Regarding impact event 'Damage or destruction of BES equipment' and considering the first example in the 'Examples' section, does 'example a. i.' mean if the BES equipment that is damaged is not identified as a critical asset per CIP-002 that no reporting is required? Clarify the Part A and Part B, specifically:Attachment 1 Part A is labeled 'Actual Reliability Impact'. Does this title mean that for all events listed that the 'threshold for reporting' is only met if the event occurs AND there is an actual reliability impact? As opposed to Part B where the threshold for reporting is met when the event occurs and there is a potential for reliability impact? This could be broad for event 'risk to BES equipment'. Providing as much clarity as possible on the 'threshold for reporting' is

Organization	Yes or No	Question 10 Comment
		beneficial to the industry and will help eliminate confusion with the existing CIP-001 standard regarding 'potential sabotage'.
PPL Supply	No	Attachment 1 Part A is labeled "Actual Reliability Impact". Does this title mean that for all events listed the "threshold for reporting" is only met if the event occurs AND there is an actual reliability impact? As opposed to Part B where the threshold for reporting is met when the event occurs and there is a potential for reliability impact? This could be broad for events like "Risk to BES equipment."
PSEG Companies	No	For many items, there are multiple entities listed with reporting obligations. For example, loss of off-site power to a nuclear plant lists RC, BA, TOP, TO, GO and GOP. This appears to result in the potential for the sending of 6 separate reports within the hour for the same event, which in wide area disturbances overload the recipients. The drafting team should consider revising the lists where possible to a single, or absolute minimum number, entity.Those items reportable OE-417 should be removed from Attachment 1. For example, voltage reduction, loss of load for greater than 15 minutes.The trigger for voltage reduction should be the time of issuance of the directive to reduce voltage in an emergency, not when "identified."
Puget Sound Energy	No	The proposed standard does not adequately ensure that the impact events subject to its requirements are limited to those listed in Attachment 1. In order to ensure that this is true, the term "impact event" should be a defined term and that definition should clearly limit impact events to those listed in Attachment 1.
Santee Cooper	No	The SDT should review the list of events closely to determine if the defined events actually impact the BES. (For example: Is shedding 100 MW of firm load really a threat to the BES?)
SERC OC Standards Review	No	Will all reporting requirements be removed from other standards to avoid duplication? And will all future

Organization	Yes or No	Question 10 Comment
Group		standard revisions include revisions to this standard to incorporate associated reporting requirements?There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
Southern Company - Transmission	No	The time to submit report column needs to be more flexible with time frames. The Entity with Reporting Responsibility column needs to be more descriptive in which there are multiple entitles with hierarchy reporting.
United Illuminating	No	UI agrees but the listing needs to be improved for clarity in certain instances. For example,EOP-004 Attachment 1 Part A - Example iii - uses the phrase “significantly affects the reliability margin of the system.” Significantly is an immeasurable concept and does not provide guidance to the Entity. The phrase “reliability margin” is not defined and is open to interpretation. Perhaps utilize “resource adequacy”, if that is all that intended, or use “adequate level of reliability”.
US Bureau of Reclamation	No	The Attachment is very vague and without modification creates a Pseudo definition of BES equipment in the example provided. The example now indicates that something is BES equipment if it is "Damaged or destroyed due to a non-environmental external cause". Perhaps the example should be reworded to "BES equipment whose operation effects or causes:" and then adjust each of the line items to clarify what was intended. Next, the Attachment A example redefines reportable levels for Risk to BES Equipment - From a non-environmental physical threat as "Report copper theft from BES equipment only if it degrades the ability of equipment to operate correctly". Who makes that determination? Not all events will be known within 24 hours. As example, Risk to BES Equipment - From a non-environmental physical threat may not be known until more thorough examination or investigation takes place. Also the reportable level appears to be defined by the Entity. While agree with that, we will end up with the same criticism from FERC when the level is set to

Organization	Yes or No	Question 10 Comment
		"high" in FERC's mind. The reporting times are unrealistic for complicated events. Notification is reasonable but not reporting. Many organizations's have internal processes the reports must be vetted through before they become public and subject to compliance scrutiny.
We Energies	No	I did not compare this standard to the OE-417 form. Please do not require operators to fill out a second form during an emergency within one hour.Energy Emergency requiring Public appeal...: "Public " is not a defined term.Energy Emergency requiring system-wide voltage...: DP does not control BES voltage.Energy Emergency requiring firm load shed...: TOP does not have load it would shed for an Energy Emergency.Frequency Deviations: Why is a BA reporting? This will be every BA in the Interconnection reporting the same Frequency Deviation.Frequency Deviations: Frequency Trigger Limit is not a defined term, and is not defined in this standard.Loss of Firm Load...: TO and TOP may coordinate or direct load shed, but they do not serve firm load.Damage or destruction of BES... There is no footnote 1 on this page. I assume it is the examples on the page. Are these "examples" of a larger set or are these all that is required? Critical Asset is a defined term.Forced Intrusion: "facility" or Facility? An RC and BA do not have Facilities.
Georgia System Operations Corporation	Yes	We support the concept of Impact Events and listing and describing them in a table. However, we have some concerns.Reporting of impact events should not be applicable to a DP.The timelines outlined in Attachment 1 should be targets to try to meet but it should not be a compliance violation of the reporting requirement if it is not met. Regarding the NOTE before the table, verbal reports and updates should be allowed for other than certain adverse conditions like severe weather as well as adverse conditions. The first priority for all entities should be addressing the effects of the impact event. It may not be possible to assess the damage or the cause of an impact event in the allotted time. All entities should make their best effort to quickly report under any circumstances what they know about the event even if it is not complete. They should be allowed to

Organization	Yes or No	Question 10 Comment
		report up through a hierarchy. The written report should not be issued until adequate information is available. Change "Preliminary Impact Event Report" to "Confidential Impact Event Report."Capitalization throughout this table is inconsistent. Sometimes an event is all capitalized. Sometimes not. It is not in synch with the NERC Glossary. All terms that remain capitalized in the next draft (other than when used as a title or heading) should be defined in the Glossary of Terms Used in NERC Reliability Standards. Examples of inconsistencies: Unplanned Control Center evacuation, Loss of off-site power, Voltage Deviations.-Energy Emergency requiring a public appeal or a system-wide voltage reduction: All The NERC Glossary defines Energy Emergency as a condition when a LSE has exhausted all other options and can no longer provide its customers' expected energy requirements. The events should not be described as an Energy Emergency requiring public appeal or system-wide voltage reductions. If public appeal and system-wide voltage reductions are still an option then all options have not been exhausted, the LSE can still provide its customers' energy requirements, and it is not an Energy Emergency. We suggest using "Energy Emergency Alert" rather than "Energy Emergency."-Energy Emergency requiring firm load shedding: load shedding via automatic UFLS or UVLS would not necessarily be due to an Energy Emergency. Other events could cause frequency or voltage to trigger a load shed. Most likely an entity would be seeing the Energy Emergency coming and would be using manual load shedding. -Forced intrusion and detection of cyber intrusion to critical cyber assets: CIP-008 is not referrenced for a forced intrusion. CIP-008 is referenced for a detection of cyber intrusion impact event. Aren't there reportable events per CIP-008 that involve physical intrusion that are not intrusions at a BES facility?-Risk to BES equipment: The threshold states that it is for a non-environmental threat but the examples given are environmental threats. Please clarify.
Manitoba Hydro	Yes	Though R7 indicated Attachment 1 will be reviewed and revised reguarily the immediate addition of:"Detection of suspected or actual or acts or threats of physical sabotage"should be added.

Organization	Yes or No	Question 10 Comment
City of Austin dba Austin Energy	Yes	
Green Country Energy	Yes	
Idaho Power Company	Yes	
Pacific Gas and Electric Company	Yes	
PacifiCorp	Yes	
PNM Resources	Yes	
RRI Energy, Inc.	Yes	
TransAlta Corporation	Yes	

11. Do you agree with the use of the Preliminary Impact Event Report (Attachment 2)? Please explain in the comment box below.

Summary Consideration: Most commenters who responded to this question disagreed with some aspect of the Preliminary Impact Event Report. The proposed Preliminary Impact Event Report (Attachment 2) generated comments regarding the duplicative nature of the form when compared to the OE-417. The DSR SDT has added language to the proposed form to clarify that NERC will accept a DOE OE-417 form in lieu of Attachment 2 if the responsible entity is required to submit an OE-417 form.

In collaboration with the NERC Event Analysis Working Group (EAWG) the DSR SDT proposes to modify the attachment to eliminate confusion. This revised form will be used as Attachment 2 of the Standard and is the only required information for EOP-004-2 reporting. Further information may be requested through Events Analysis Process (NERC Rules of Procedure), but this information is outside of the scope of EOP-004.

The DSR SDT has also clarified what the form is to be used for with the following language added:

"This form is to be used to report impact events to the ERO."

Organization	Yes or No	Question 11 Comment
City of Austin dba Austin Energy		Austin Energy would like to see OE-417 incorporated into the electronic form This will reduce the callout of EOP-004-2 and OE-417 forms in our checklists / documents and one form can be submitted to NERC and DOE.
Independent Electricity System Operator		TBD
Ameren	No	It is unclear when this should be used, or why.

Organization	Yes or No	Question 11 Comment
ATC	No	No. NERC does not have the authority to absolve the Functional Entities of the reporting obligations for the DOE Form OE-417. Therefore, there will be duplicate reporting requirements and the one hour timeframes required in Attachment 1 will take valuable resources away from mitigating the event to filling out duplicative paperwork. It is ATC's position that the OE-417 report be used as the main reporting template until NERC and the DOE can develop a single reporting template. Task #14 in the report should be modified to say, "Identify any known protection system misoperation(s)." If this report is to be filed within 24 hrs, there will not be enough time to assess all operations to determine any misoperation. As a case in point, it typically takes at least 24 hrs to receive final lightning data; therefore, not all data is available to make a determination.
ATCO Electric Ltd.	No	Attachment 2 Item 4 implies that an entity is required to analyse and report on an impact event that occurred outside its system. This is not practical as the entity will not have access to the necessary information.
BGE	No	There is considerable difference between this form and OE-417 necessitating that two forms be completed. BGE believes that the purpose of combining the standards was to reduce the number of reporting entities and number of reports to be generated by each entity. BGE believes this fails to accomplish this purpose.
City of Garland	No	The report filed should be the OE-417 ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT and should be filed only on OE-417 reportable incidents. If this report is implemented as drafted, companies with multiple registration numbers and functions should only have to file one report for all functions and registrations.
Consolidated Edison Co. of NY, Inc.	No	It is not clear why the DOE form cannot be used. NERC should make every effort to minimize paper work for entities responding to system events.
Constellation Power Generation and Constellation Commodities Group	No	It is unclear if an entity has to answer all the questions. In addition, "Preliminary" is not currently included in the report title.
Electric Market Policy	No	There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.
ERCOT ISO	No	ERCOT ISO requests the use of a single report format to meet all requirements from NERC and DOE. There is no value added in requiring different reporting to different agencies.

Organization	Yes or No	Question 11 Comment
Exelon	No	Exelon agrees with the use of the report but feels that # 5 should consist of check boxes. #12, 13, and 14 will take more time then allotted by the reporting requirements to acquire, cannot be accomplished in an hour.Attachment 2 should have a provision for the reporting entity to enter (N/A) based on function (see below)Check box #8 A GO/GOP may not have the information to determine what the frequency was prior to or immediately after an impact event. This information should be the responsibility of a TOP or RC.Check box #9A GO/GOP may not have the information to determine what transmission facilities tripped and locked out. This information should be the responsibility of a TO, TOP or RC.Check box #10A GO/GOP may not have the information to determine the number of affected customers or the demand lost (MW-Minutes). This information should be the responsibility of a TO, TOP, or RC.
Great River Energy	No	NERC and the DOE need to coordinate and decide on which report they want to use and whichever report it is needs to include all information required by both entities. The way this standard is currently written there is the potential that two government entities may need to be reported to is a relatively short period of time. It is not clear what benefit providing the Compliance Registration ID number provides. Many of the registered entities employees that will likely have to submit the report, particularly given the one-hour reporting requirement for some impact events, will not be aware of this registration ID. However, they will know for what functions they are registered. We recommend removing the need to enter this compliance registration ID or extending the time frame for reporting to allow back office personnel to complete the form. For item two, please change “Time/Zone:” with “Time (include time zone)”. As written it is a little confusing.
Idaho Power Company	No	there should only be on report, utilized OE-417
Indeck Energy Services	No	The form needs to identify whether it is a preliminary or final report. An identifier should be created to tie the final to the preliminary one. Some fields, 1,2 3 5 & 6, are required for the preliminary report and should be labeled as such. With the 1 hour reporting deadline for some events, the details may not be known. 12 & 13 should be required for the final report. 13 should designate whether the cause is preliminary or final. 7-11 & 14 are optional, and the form should state this, and based on some types of events. It's confusing to have irrelevant blanks on the form.
IRC Standards Review Committee	No	Attachment 2 is not referenced in the standard requirements. Is it a part of the standard that an entity must use to file the impact event reports to a specific recipient. If so, this needs to be referenced in the standard.We question the need for using a fixed format for reports that vary from “shedding firm load” to “damaging equipment”. The nature of impact events varies from one event to another and hence a fixed format or pre-determined form may not be able to provide the appropriate template that is suitable for use for

Organization	Yes or No	Question 11 Comment
		all events. We urge the SDT to reconsider the use of Attachment 2 for reporting events, with due consideration to the actual intent of the standard (as pointed out in our comments under Q1).
ISO New England Inc.	No	There is already a DOE requirement to report certain events. There is no need to develop redundant reporting requirements to NERC that cross other federal agency jurisdictions.The heading on page 16 refers to EOP-002, but this is Standard EOP-004. If some questions do not require an answer all of the time, then the form should state that or provide a NA checkbox. While Attachment 1 details some cyber thresholds, Attachment 2 provides no means to report - which is acceptable if cyber incidents are handled by CIP-008 per the comment provided for Question 10.The Event Report Template in Appendix A is different from the most recent version, which is available at: http://www.nerc.com/docs/eawg/Event_Analysis_Process_WORKINGDRAFT_100110-Clean.pdf
Kansas City Power & Light	No	For easier classification and analysis of events for both external reporting to the ERO and internal reporting for the applicable entity, the form should include Event Type. The DSR SDT should code each event type and include the codes as part of Attachment 1.
Manitoba Hydro	No	Though a “Confidential Impact Event Report” is much needed the Attachment 2 needs refinement.Provide an explanation for each “task”.Isolate and simplify the “Who, When and What” section.Isolate the description of event.Remove items 7 to 10. Modify Attachment 1, add columns to indicate time of event, quantity, restore time, etc as required. The Attachment 1 can be attached to Attachment 2. This could simply and speed the reporting process.
MidAmerican Energy	No	
Midwest ISO Standards Collaborators	No	This form differs from the DOE reporting forms. We do not believe different reporting forms should be required. The DOE form should be sufficient for NERC reporting.It is not clear what benefit providing the Compliance Registration ID number provides. Many of the registered entities employees that will likely have to submit the report, particularly given the one-hour reporting requirement for some impact events, will not be aware of this registration ID. However, they will know for what functions they are registered. We recommend removing the need to enter this compliance registration ID or extending the time frame for reporting to allow back office personnel to complete the form. For item two, please change “Time/Zone:” with “Time (include time zone)”. As written it is a little confusing.

Organization	Yes or No	Question 11 Comment
MRO's NERC Standards Review Subcommittee	No	Number 4 of the reporting form does not take into consideration of potential impact events. Recommend that "Did the impact event originate in your system?" to "Did the impact event originate or affect your system?". This will provide clarity to entities.
Nebraska Public Power District	No	If the standard requires submission of the report within an hour (which is not appropriate), there must be an abbreviated form that can be quickly filled out by checking boxes and not require substantial narrative. The existing form has too much free form text that takes time to enter and with the short timeframe for reporting will distract the entities responsible for real-time reliabiltiy of the BES from that task by forcing them to complete after the fact reports. It is unrealistic to expect entities to staff personnel to complete the reporting 24 x 7 for unlikely events, so the task will fall to System Operators who should be focusing on operating the BES at the time of these events instead of providing after the fact reporting to entities that do not have responsibility for real-time operation of the BES. Real-time reporting to the RC and/or BA is covered under other standards and is necessary for the RC to have situational awareness, but is not covered under this standard. The registered entities may report to the proper law enforcement entities when the situation warrants, but again this form is not the appropriate way to handle that reporting requirement.
NERC Staff	No	Item 15: A one-line diagram should be attached to assist in the understanding and evaluation of the event.Two additional items are recommended:--Ongoing reliability impacts/system vulnerability - this would capture areas where one is not able to meet operating reserves or is in an overload condition, below voltage limits, etc. in real-time--Reliability impacts with next contingency - this would capture potential impacts as outlined above with the next contingency.
North Carolina Electric Coops	No	There is already a DOE requirement to report certain events. NERC should not be developing redundant reporting requirements when this information is already available at the federal level from other agencies.
Northeast Power Coordinating Council	No	There is already a DOE requirement to report certain events. There is no need to develop redundant reporting requirements to NERC that cross other federal agency jurisdictions.The heading on page 16 refers to EOP-002, but this is Standard EOP-004. If some questions do not require an answer all of the time, then the form should state that or provide a NA checkbox. While Attachment 1 details some cyber thresholds, Attachment 2 provides no means to report - which is acceptable if cyber incidents are handled by CIP-008 per the comment provided for Question 10.The Event Report Template in Appendix A is different from the most recent version, which is available at: http://www.nerc.com/docs/eawg/Event_Analysis_Process_WORKINGDRAFT_100110-Clean.pdf

Organization	Yes or No	Question 11 Comment
Pacific Gas and Electric Company	No	PG&E believes the report is duplicative to the OE-417 reporting criteria.
Pacific Northwest Small Public Power Utility Comment Group	No	We found no “Preliminary Impact Event Report” in the posted draft standard, so we assume the question is regarding the “Confidential Impact Report” (Attachment 2). It is unclear what role the form plays, since no requirement refers to it. If this is the form to report impact events per R6, then R6 should reference it. The comment group cautions that the use of the word “confidential” should be carefully considered, since many filled out forms that originally contained the word are now posted on the NERC website for all to see. If there are limits to the extent and/or duration of the confidentiality this should be clearly stated in the form, or the word should be avoided.Protection System misoperation reporting is already covered by PRC-004. Including it here is redundant, and doubly jeopardizes an entity for the same event.
PacifiCorp	No	As previously mentioned all effort should be made to ensure duplicate reporting is not required. OE-417 requirements should be covered by this one form.
Pepco Holdings, Inc - Affiliates	No	The list of events misses many items considered as suspicious or potential sabotage, such as suspicious observation of critical facilities.
PNM Resources	No	PNM believes the report is duplicative to the OE-417 reporting criteria.
PSEG Companies	No	The top of this form should have the following statement added: "This form is not required if OE-417 is required to be filed."
Puget Sound Energy	No	Attachment 2 is not referenced in the requirements of the proposed standard. As a result, it is not clear when its submission would be required.
Santee Cooper	No	If the DOE form is going to continue to be required by DOE, then NERC should accept this form. Entities do not have time to fill out duplicate forms within the time limits allowed for an event. This is burdensome on an entity.
SERC OC Standards Review Group	No	There is already a DOE requirement to report certain events. We see no need to develop redundant reporting requirements in the NERC arena that cross other federal agency jurisdictions.

Organization	Yes or No	Question 11 Comment
TransAlta Corporation	No	We recommend the 'time to Submit Report' to start when the event is recognized verses when it occurred.
United Illuminating	No	The standard does not appear to require the use of Attachment 2. Placing the form within the Standard may require the use of the Standards Development Process to modify the form. UI suggests the form is maintained outside the Standard to allow it to be adjusted. UI would prefer NERC to establish an internet based reporting tool to convey the initial reports.
US Bureau of Reclamation	No	There is already a reporting form for disturbances. The SDT should reconcile this standard with all the other reporting that is being requested and not add more.
We Energies	No	The data required to assess an impact event thoroughly will often not be available or apparent. Immediate reporting should fall to the RE with assistance/information from the affected entities.There do not seem to be provisions for when it is impossible to take the time to fill out a form or when it is impossible to send a form.I did not compare this standard to the OE-417 form. Please do not require operators to fill out a second form during an emergency within one hour.
WECC	No	The report is duplicative to the OE-417 reporting criteria.
Bonneville Power Administration	Yes	Item 8: list Hz minimum on the second line prior to Hz max since that is the typical frequency excursion order.The Operating Plan is going to have to include the Compliance Registration ID number, since Operating Personnel don't carry that information around and it is not readily available.
Duke Energy	Yes	However, Attachment 2 is titled "Impact Event Reporting Form".
E.ON Climate & Renewables	Yes	Suggestions on the form: if an entity has not had time to fully determine the cause of an Impact Event such as for "Question # 4: Did the impact event originate in your system, yes or no?", perhaps more time is needed that 24 hours to determine the cause.
FirstEnergy	Yes	Although we agree with the report, it should be clear that organizations with many registered entities can submit one report to cover multiple entities under one parent company.
Georgia System Operations	Yes	We support having one form for reporting however every applicable entity should not be required to fill it out and send it to NERC. See previous comments about hierarchical reporting.The title of the report is

Organization	Yes or No	Question 11 Comment
Corporation		"Confidential Impact Event Report." Some suggested modifications: The form could have a blank added to enter the event "description" as described in the first column of Attachment 1. The first seven lines contain information that would most likely be filled out every time. The other lines except line 13 may or may not be applicable every time. It is required (R3) for an entity to access the initial probable cause of all impact events so line 13 will most likely be filled out every time. Please move the probable cause line up to line 7 or 8 (depending on if the event description line is added).
PPL Electric Utilities	Yes	For ease, timeliness, and accuracy of reporting an application with an easy to use interface would be preferred. If the reporting is done via an application, the ability to enter partial data, save and add additional info prior to submission would be helpful. Additionally, an application with drop downs to select from for impact event, NERC function, etc would be helpful. #1 - Is the 'Compliance Registration ID number' the same as the NCR number? If this is required, include as separate entry. #2 - is this the date of occurrence or detection?
Arizona Public Service Company	Yes	
Dynegy Inc.	Yes	
Green Country Energy	Yes	
Luminant Energy	Yes	
PacifiCorp	Yes	
PPL Supply	Yes	

Organization	Yes or No	Question 11 Comment
RRI Energy, Inc.	Yes	
Southern Company - Transmission	Yes	

12. The DSR SDT has replaced the terms "disturbance" and "sabotage" with the term "impact events". Do you agree that the term "impact events" adequately replaces the terms "disturbance" and "sabotage" and addresses the FERC directive to "further define sabotage" in an equally efficient and effective manner? Please explain in the comment box below.

Summary Consideration: There was no consensus amongst commenters who responded to this question. Several commenters expressed concern that the definition should be added to the glossary. The DSR SDT has proposed a definition for "Impact Events" to support Attachment 1 as follows:

> "An Impact Event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action."

The DSR SDT has proposed this definition for inclusion in the NERC Glossary for "Impact Event". The types of Impact Events that are required to be reported are contained within Attachment 1. Only these events are required to be reported under this Standard.

Several commenters expressed concern that the team did not define 'Sabotage' and FERC directed that the modifications to this standard include a definition of sabotage. The DSR SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was that of sabotage or merely vandalism without the intervention of law enforcement after the fact. This will result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The Impact Events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

Some commenters were concerned that some of the events that require reporting that were specifically listed in the previous version of the standard are not included in the revised standard. Attachment 1, Part A is to be used for those actions that have impacted the electric system and in particular the section "Damage or destruction to equipment" clearly defines that all equipment that intentional or non intentional human error be reported. Attachment 1, Part B covers the similar items but the action has not fully occurred but may cause a risk to the electric system and is required to be reported.

Organization	Yes or No	Question 12 Comment
Bonneville Power Administration		The definition of an impact event in EOP-004-2 seems clear, however the term "mis-operation" still may imply intent in the action of an individual. The SDT should consider further defining that term.
Independent Electricity System Operator		We do not have a view on what name is assigned to the reportable events for so long they are listed in Attachment 1. However, the heading of the Table contains the words “Actual Reliability Impact”, which does not accurately reflect the content inside the table and which may introduce confusion with the term “impact event”. We suggest to change them to “Reportable Impact Events”.As we read the Summary of Concept and Assumption, there appears to be a slightly different lists at the bottom of P. 21. With these events included, the meaning of “impact event” would seem to be too broad. Rather than calling those events listed in Attachment 1 “impact events”, why not simply call them “reportable events”?
CenterPoint Energy	No	CenterPoint Energy does not agree that the term “impact event” adequately replaces “disturbances” and “sabotage”. CenterPoint Energy suggests that just as the SDT has come to consensus on a concept for impact event, a definition could be derived for sabotage. “Potential”, as used in the SDT’s concept, is a vague term and indicates an occurrence that hasn’t happened. Required reporting should be limited to actual events. CenterPoint Energy offers the following definition of “sabotage”: “An actual or attempted act that intentionally disrupts the reliable operation of the BES or results in damage to, destruction or misuse of BES facilities that result in large scale customer outages (i.e. 300MW or more).”
City of Garland	No	1 In keeping with a Results Based Standard, the impact event should be a trigger for filing a report. At the time of the event, one may not know if the event was caused by sabotage. Sabotage that does not affect the BES should not be a reportable event. 2. To comply with the Commissioners request to define sabotage, Impact Event does not adequately replace “sabotage”. If someone reports sabotage, people universally have a concept that someone(s) have taken some type of action to purposely harm, disable, cripple, etc something. Impact Event does not convey that same concept. 3. If Sabotage is left as a “trigger,” it should not include minor acts of vandalism but only acts that impact reliability of the BES
Consolidated Edison Co. of NY, Inc.	No	The definition is open for interpretation beyond events identified in Attachment 1. In addition, all Standards are supposed to have Rationales. In the Draft Standard, the Rationales do not address the concept of Potential, and how it relates to an actual system event. Additional work needs to be done addressing the

Organization	Yes or No	Question 12 Comment
		meaning of “potential”.
Duke Energy	No	We disagree with the stated concept of “impact event”. Including the phrase “or has the potential to significantly impact” in the concept makes it impossibly broad for practical application and compliance. By not attempting to define “sabotage”, the standard creates a broad reporting requirement. “Disturbance” is already adequately defined. “Sabotage” should be defined as “the malicious destruction of, or damage to assets of the electric industry, with the intention of disrupting or adversely affecting the reliability of the electric grid for the purposes of weakening the critical infrastructure of our nation.”
Dynegy Inc.	No	The term is fine but FERC wants more specific examples. GO/GOP can't determine the effect on the BES.
E.ON Climate & Renewables	No	Acts of Sabotage is still not defined and if the registered entities are required to reports acts of sabotage, NERC still needs to define this further.
ERCOT ISO	No	
Exelon	No	Need to better define sabotage and provide examples, the term “impact events” create confusions as to what constitutes an event. The definition of impact event is vague and needs to be quantified or qualified with a term such as “significant”. Otherwise, almost any event could be deemed to be an impact event. Attachment 1 needs to clearly define that damage or destruction of BES equipment does not include cyber sabotage. Events related to cyber sabotage are reported in accordance with CIP-008, "Cyber Security - Incident Reporting and Response Planning," and therefore any type of event that is cyber initiated should be removed from this Standard. In general, all impact events need to be as explicit as possible in threshold criteria to eliminate any interpretation on the part of a reporting entity. Ambiguity in what constitutes an "impact event" and what the definition of "occurrence" is will ultimately lead to confusion and differing interpretations.
FirstEnergy	No	For the most part we support this definition of impact events. However, we have the following suggestions:1. We believe that it warrants an official NERC glossary definition. 2. The term "potential" in the definition should point to the specific events detailed in Attachment 1 Part B.3. Since the standard does not cover environmental events, the phrase "environmental conditions" in the definition is not an impact event in the context of this standard.

Organization	Yes or No	Question 12 Comment
Great River Energy	No	We believe the SAR scope regarding addressing sabotage has not been addressed at all. It appears that impact event essentially replaces sabotage. This standard needs to make it clear that sabotage, in some cases, cannot be identified until an investigation is performed by the appropriate policing agencies such as the FBI. Intent plays an important role in determining sabotage and only these agencies are equipped to make these assessments.
Green Country Energy	No	Yes and no ... Yes impact events is an adequate term however since it is restrained by the tables it may be helpful to define the term and scope of the term to be more inclusive of sabotage events.
Indeck Energy Services	No	Impact Events is OK. It needs to be balloted as a definition for the Glossary like Protection System.
IRC Standards Review Committee	No	This term and the FERC directive do not recognize limitations in what a registered entity can do to determine whether an act of sabotage has been committed. This term should recognize law enforcement's and other specialized agencies', including international agencies', role in defining acts of sabotage and not hold the registered entity wholly responsible to do so.
ISO New England Inc.	No	The use of the term "impact events" has simply replaced the terms "disturbance" and "sabotage", and has not further defined sabotage as directed by FERC. We do feel that "impact events" needs to be a defined term. While we agree with the SDT's new direction, the FERC directive has not been met. This term and the FERC directive do not recognize limitations in what a registered entity can do to determine whether an act of sabotage has been committed. This term should recognize law enforcement and other specialized agencies, including international agencies roles in defining acts of sabotage, and not hold the registered entity wholly responsible to do so.
Luminant Energy	No	The term "Impact Event" does not adequately replace the term "Sabotage" The Impact Events table seems to provide the definition of the term "Impact Event". This table does not include sufficient definition for actual sabotage events. Additionally, it does not include any provision for suspected sabotage events. Assuming the Damage or Destruction of BES Equipment event type is intended to cover actual sabotage, the Threshold for Reporting column should include specific levels of materiality that are specific to Functional Entity. For instance, a GO and GOP could have a MW level to define materiality as a GO or GOP cannot assess impact to an IROL or system reliability margin due to equipment damage. A threshold value consistent with "Generation Loss" in the proposed EOP-004 Attachment 1 would be appropriate.
Manitoba Hydro	No	The majority of the items listed in Attachment 1 are typically and historically operating events. Yes these are all "impact events". Sabotage, cyber and security are typically viewed as separate events. These events are

Organization	Yes or No	Question 12 Comment
		not part of “a typical day of BES operations”. These are outside event and though qualify as “impact events” should still be treated separately.
Midwest ISO Standards Collaborators	No	We believe the SAR scope regarding addressing sabotage has not been addressed at all. It appears that impact event essentially replaces sabotage. This standard needs to make it clear that sabotage, in some cases, cannot be identified until an investigation is performed by the appropriate policing agencies such as the FBI. Intent plays an important role in determining sabotage and only these agencies are equipped to make these assessments.
NERC Staff	No	NERC staff is concerned with the ambiguity of the term “impact event.” The definition of the term is not clear, in part because it includes using the words “impact” and “event” (and thus violates the frowned-up practice of using a word to define the word itself). NERC staff recommends the SDT consider using the term “Event.” The following definition (modified from the one used the INPO Human Performance Fundamentals Desk Reference, P. 11) would apply: Event: “An unwanted, undesirable change in the state of plants, systems or components that leads to undesirable consequences to the safe and reliable operation of the Bulk Electric System. ”Supporting statement following the definition: “An event is often driven by deficiencies in barriers and defenses, latent organizational weaknesses and conditions, errors in human performance and factors, and equipment design or maintenance issues.” Further, if this is intended for use in this standard, it should be presented as an addition to Glossary to avoid confusion with the use of the term event in other standards. Of course, this would require an analysis of how the term “Event” as defined herein would affect the other standards to which the term is used. In the end, this is the cleanest manner for the standards.
Northeast Power Coordinating Council	No	The use of the term “impact events” has simply replaced the terms “disturbance” and “sabotage”, and has not further defined sabotage as directed by FERC. We do feel that “impact events” needs to be a defined term.While we agree with the SDT’s new direction, the FERC directive has not been met.This term and the FERC directive do not recognize limitations in what a registered entity can do to determine whether an act of sabotage has been committed. This term should recognize law enforcement and other specialized agencies, including international agencies roles in defining acts of sabotage, and not hold the registered entity wholly responsible to do so.
Pacific Gas and Electric Company	No	PG&E believes Attachment 1 Part A or B do not clearing specify “sabotage” events, other than “forced entry” and the proposed definition of “impact event” does not meet FERC’s directive to “further define sabotage” nor does it take into consideration their request to address the applicability to smaller entities.
Pacific Northwest Small Public	No	The comment group fails to see how changing the words meet the directive. Sabotage implies an organized

Organization	Yes or No	Question 12 Comment
Power Utility Comment Group		intentional attack that may or may not result in an electrical disturbance. The distinction between sabotage and vandalism is important since sabotage on a small system may be the first wave of an attack on many entities. The proposed standard asks us to treat insulator damage caused by a frustrated hunter (an act of vandalism) the same as attack by an unfriendly foreign government (an act of sabotage). The comment group does not agree that these should be treated equally.
Pepco Holdings, Inc - Affiliates	No	The list of events misses many items considered as suspicious or potential sabotage, such as suspicious observation of critical facilities.
PNM Resources	No	PNM believes the proposed definition of “impact event” does not meet FERC’s directive to “further define sabotage” nor does it take into consideration their request to address the applicability to smaller entities. Attachment 1 Part A or B do not clearing specify “sabotage” events, other than “forced entry”.
Puget Sound Energy	No	With some of the tight timeframes for reporting, it is reasonable to focus on impact rather than motivation. Requiring further analysis of the event in order to assess the possibility that the event was caused by sabotage, however, may be necessary to address FERC’s concerns with respect to sabotage.
Santee Cooper	No	The term "impact events" needs to be more clearly defined.
US Bureau of Reclamation	No	The two are distinctly different. Disturbances are what happened, sabotage is why. We can easily tell what happened. Determining why it happened (e.g. sabotage) takes time.
We Energies	No	Impact Event could replace disturbance and sabotage but not in its present form. The proposed definition of impact event “An impact event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action.” Is too vague. The “potential to impact the reliability” is too broad and open to interpretation. It needs to be specific so entities know what is and is not an impact event and so an auditor clearly knows what it is. Define “impact event” as the items listed in Attachment 1.As you have done, focusing on an event’s impact on reliability is more important than determining an individuals intent (sabotage v.s. theft).
WECC	No	The proposed definition of “impact event” does not meet FERC’s directive to “further define sabotage” nor does it take into consideration their request to address the applicability to smaller entities. Attachment 1 Part A or B do not clearing specify “sabotage” events, other than “forced entry”. The purpose of CIP-001-1 and its requirements is to address the specific issue of possible sabotage of BES facilities. This is entirely different

Organization	Yes or No	Question 12 Comment
		than a “disturbance” or an “event” on the BES. The proposed definition for “impact events” is essentially any event that has either impacted the BES or has the potential to impact the BES, caused only by three specific things; equipment failure or misoperation, environmental conditions, or human action. Several of these “impact events could be a result of sabotage. Actual or potential sabotage clearly poses a risk to the reliability of the BES. It is important that the risks related to sabotage be reflected in either EOP or CIP
Ameren	Yes	However, the term Impact Event should be a new defined term. When the SDT determines this, it should use the term consistently on both pages 5 and 21 of the SDT document.
ATC	Yes	Yes, if ATC’s recommended changes are made to Attachment 1 and the Standard.
BGE	Yes	The defined term “impact events” should be capitalized throughout the document to identify it as a defined term. Additionally, BGE has noted in several comments that another term is used instead of “impact events”. These terms should be eliminated and use “impact events” instead.
Electric Market Policy	Yes	The use of the term “impact events’ has simply replaced the terms “disturbance” and “sabotage” and has not further defined sabotage as directed by FERC. We do feel that impact events needs to be a defined term.
Georgia System Operations Corporation	Yes	The new term is much more clear than those two terms. This will improve uncertainty and confusion regarding whether or not something should be reported.
Kansas City Power & Light	Yes	Should the word disturbance be removed from the title of EOP004-2 to avoid confusion and simply be called Impact Event and Assessment, Analysis and Reporting.
MRO's NERC Standards Review Subcommittee	Yes	As an industry we have looked at sabotage as a sub component of a disturbance. Sabotage is hard to measure since it is based on a perpetrator’s intent and thus very hard to determine.
Nebraska Public Power District	Yes	I agree there is a lot of interpretation and confusion as to what sabotage or a Cyber Incident is, so would welcome better clarity. Whether “impact events” can more effectively clarify, is yet to be seen. “it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.” “An impact event is any situation that has the potential to significantly impact the reliability of the Bulk Electric System. Such events may originate from malicious intent, accidental behavior, or natural occurrences.” I do know that Cyber Sabotage may take time or days to become aware so not sure

Organization	Yes or No	Question 12 Comment
		how that might expedite reporting and awareness.
PPL Electric Utilities	Yes	Refer to clarification requested in question 10 comments.
RRI Energy, Inc.	Yes	Agree. However, strongly encourage this to be made into a defined term in the Glossary of Terms.
SERC OC Standards Review Group	Yes	We do feel that this needs to be a defined term
United Illuminating	Yes	The term impact event can substitute for sabotage and disturbance. The use of Forced Intrusion is a bright line for reporting.
American Electric Power (AEP)	Yes	
Arizona Public Service Company	Yes	
ATCO Electric Ltd.	Yes	
City of Austin dba Austin Energy	Yes	
Constellation Power Generation and Constellation Commodities Group	Yes	
Idaho Power Company	Yes	

Organization	Yes or No	Question 12 Comment
MidAmerican Energy	Yes	
North Carolina Electric Coops	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	
PPL Supply	Yes	
Southern Company - Transmission	Yes	
TransAlta Corporation	Yes	

13. The DSR SDT has combined EOP-004 and CIP-001 into one standard (please review the mapping document that shows the translation of requirements from the already approved versions of CIP-001 and EOP-004 to the proposed EOP-004), EOP-004-3 and retiring CIP-001. Do you agree that there is no reliability gap between the existing standards and the proposed standard? Please explain in the comment box below.

Summary Consideration: While a majority of commenters who responded to this question support combining the two standards, some commenters suggested that in combining the standards, the team left some gaps in coverage with respect to the types of events that must be reported. The DSR SDT believes that combining EOP-004 and CIP-001 does not introduce a reliability gap between the existing standards and the proposed standard and the industry comments received confirms this. Some events that were specifically identified in the original standard (such as a bomb threat) are covered more generically in the revised standard. This modification encourages entities to focus on the 'types' of events that may be impactive rather than having a finite list that may omit an event that couldn't be anticipated when drafting the requirements.

The decision to eliminate the term sabotage from the standard and the retirement of CIP-001 should alleviate all concerns regarding the term sabotage and its definition. The DSR SDT believes that "observation of suspicious activity" and "bomb threat" is considered to be included in Part B – "Risk to BES equipment from a non-environmental physical threat". We have added "and report of suspicious device near BES equipment" to note 3 of the "Attachment 1, Potential Reliability – Part B".

Organization	Yes or No	Question 13 Comment
WECC		A potential gap may exist. Attacks on BES facilities, via either vandalism or sabotage, are very different events than impact events on the system. From a Compliance standpoint, a revised standard to address the FERC directive on sabotage should be developed as an EOP standard (that is grouped with 693 Standards) rather than as a CIP Standard (CIP-001-1).
Ameren	No	It appears that all requirements have been addressed from the existing standards. However, we believe there is a reliability gap that continues from the existing standards because sabotage is not defined any better than

Organization	Yes or No	Question 13 Comment
		in the existing standards.
Bonneville Power Administration	No	BPA supports the concept behind the revisions to EOP-004-2. Creating a single reporting methodology will improve the processes and lead to more consistency. BPA recommends that the Standards Drafting Team (SDT) coordinate any revisions in the reporting requirements with those found in CIP-008-3 to ensure that there are no conflicts. BPA asks the SDT to consider the impact of these changes on CIP-008-3 and work with the CIP SDT to ensure that the wording of the two requirements is similar and clear. Based on Attachment 1 part A of EOP-004-2, certain cyber security events, intrusions for example, would have to be reported under both EOP-004-2 and CIP-008-3. That puts a burden on a Registered Entity to take additional steps to coordinate reporting or face potential compliance risk for correctly reporting an event under one standard and failing to report it under the other standard. The mapping document had errors: a. CIP-001 R1 to EOP-004 R2.9 (annual vs quarterly). b. EOP-004-1 R2 was translated to R2 & R3 of version 2. c. EOP-004-1 R3 was translated to R6 of version 2 (which doesn't say to whom to report).
City of Garland	No	EOP-004-1 R2 did not get translated to EOP-004-2 R2 - table states it is mapped to R1
E.ON U.S. LLC	No	The Version History contained with EOP-004-2 indicates that CIP-001-1 and EOP-004-1 are "Merged", however, the actions do not reflect the retirement of CIP-001-1a and therefore, it is unclear if there will be remaining redundancies or potential gaps with the new version EOP-004-2 and CIP-001-1a.
Electric Market Policy	No	Per the mapping document, some of the existing requirements are awaiting a new reporting procedure being developed by NERC EAWG. For those requirements that were transferred over, the resulting standard seems overly complex and lacks clarity.
Exelon	No	Reporting form doesn't allow for investigations which result in no impact events found or identified.
Georgia Transmission Corporation	No	The only two events that apply to a TO are the ones related to CIP:1. Forced intrusion (report if motivation cannot be determined, i.e. to steal copper)2. Detection of a cyber intrusion to critical cyber assets (criteria of CIP-008)Everything in this standard applies to a TOP and therefore E-004-2 and CIP-001 should not be combined

Organization	Yes or No	Question 13 Comment
Great River Energy	No	It appears that all requirements have been addressed from the existing standards. However, we believe there is a reliability gap that continues from the existing standards because sabotage is not defined any better than in the existing standards.
Indeck Energy Services	No	Bomb threat has totally been lost.
Independent Electricity System Operator	No	We do not agree with the mapping. The proposed mapping attempts to merge the reporting in CIP-001-1 which has more of an on-going awareness nature to alert operating and government authorities of suspected sabotage to prompt investigation with a possible aim to identify the cause and develop remedies to curb the sabotage/events. The proposed EOP-004-2 appears to be more of a post-event reporting for need-to-know purpose only. This is not consistent with the purpose of the SAR.
ISO New England Inc.	No	Per the mapping document, some of the existing requirements are awaiting a new reporting procedure being developed by the NERC EAWG. For those requirements that were transferred over, the resulting standard seems overly complex and lacks clarity. EOP-004-3 should be EOP-004-2.
Luminant Energy	No	CIP-001-1 R3.1 includes instructions associated with the DOE OE-417 form. EOP-004-2 R2.6 should include the DOE as an example of an external organization requiring notification. Additionally, the Rationale for R1 discusses the possibility of one electronic form satisfying US entities with related disturbance reporting requirements but does not include any information about the likelihood of this outcome. Please elaborate on the process required to combine these reports.
Midwest ISO Standards Collaborators	No	It appears that all requirements have been addressed from the existing standards. However, we believe there is a reliability gap that continues from the existing standards because sabotage is not defined any better than in the existing standards.
North Carolina Electric Coops	No	
Northeast Power Coordinating Council	No	Per the mapping document, some of the existing requirements are awaiting a new reporting procedure being developed by the NERC EAWG. For those requirements that were transferred over, the resulting standard seems overly complex and lacks clarity. EOP-004-3 should be EOP-004-2.

Organization	Yes or No	Question 13 Comment
Pepco Holdings, Inc - Affiliates	No	The list of events misses many items considered as suspicious or potential sabotage, such as suspicious observation of critical facilities.
Santee Cooper	No	It is very difficult to assess this question with the standard as currently written.
SERC OC Standards Review Group	No	
US Bureau of Reclamation	No	The two could be combined with no reliability gap based on the concept rather than the proposed standard. As the standard is currently written, there is a reliability gap. Consider that after the fact reporting of a sabotage event (other than criminal acts which may have been witnessed) usually take some time to investigate and analyze.
ATC	Yes	ATC agrees with this effort and does not currently see a reliability gap
BGE	Yes	None.
CenterPoint Energy	Yes	CenterPoint Energy agrees that there is no reliability gap between the existing standards and the proposed standard. However, CenterPoint Energy believes that the SDT went too far in developing the proposed EOP-004-2 and added additional unnecessary requirements. If the comments made above to Q1 - Q12 were to be incorporated into the proposed Standard, CenterPoint Energy believes the product would be closer to a results based Standard with no reliability gap.
City of Austin dba Austin Energy	Yes	If we can used OE 417 for NERC and DOE we do not perceive a reliability gap.
Georgia System Operations Corporation	Yes	The new single standard will cover all necessary reporting requirements that are in the current two standards. They are being combined into EOP-004-2 not EOP-004-3.

Organization	Yes or No	Question 13 Comment
Green Country Energy	Yes	With the provision that definition and scope of "impact event" are developed and tables adjusted as needed to address FERCs concerns specifically ."(1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."
MRO's NERC Standards Review Subcommittee	Yes	Within the above question, the SDT is asking about EOP-004-2 not -3.
Nebraska Public Power District	Yes	Appears they only changed R1 for CIP-001 and moving R2-R4 directly over to EOP-004-2. R1 adds much more detail on our part for a company operating plan but would definitely help some of the present confusion.
RRI Energy, Inc.	Yes	Assume reference to EOP-004-3 in the question 13 was meant to reference version 2 (EOP-004-2).
American Electric Power (AEP)	Yes	
Arizona Public Service Company	Yes	
ATCO Electric Ltd.	Yes	
Consolidated Edison Co. of NY, Inc.	Yes	
Constellation Power Generation and Constellation Commodities Group	Yes	
Duke Energy	Yes	
Dynegy Inc.	Yes	
ERCOT ISO	Yes	
FirstEnergy	Yes	

Organization	Yes or No	Question 13 Comment
Idaho Power Company	Yes	
Kansas City Power & Light	Yes	
MidAmerican Energy	Yes	
NERC Staff	Yes	
Pacific Gas and Electric Company	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	
PNM Resources	Yes	
PPL Electric Utilities	Yes	
PPL Supply	Yes	
Puget Sound Energy	Yes	
Southern Company - Transmission	Yes	
TransAlta Corporation	Yes	
United Illuminating	Yes	
We Energies	Yes	

14. Do you agree with the proposed effective dates? Please explain in the comment box below.

Summary Consideration: While most stakeholders who responded to this question supported the 12 months originally proposed for entities to become compliant, the drafting team has revised this to 6 months. The DSR SDT feels that six months and not more than nine months is an adequate time frame. The current CIP-001 plan is adequate for the new EOP-004 and training should be met in the proposed timeline.

The Implementation Plan was developed for the revised Requirements, which do not include an electronic "one-stop shopping" tool. This topic is to be addressed in the proposed revisions to the NERC Rules of Procedure.

Organization	Yes or No	Question 14 Comment
Independent Electricity System Operator		We do not agree with the proposed standard. We therefore are unable to agree on any implementation plan.
City of Garland	No	Do not agree with this proposed draft - instead of combining 2 standards to gain efficiency, this expands the standard with unnecessary paperwork, drills, training, etc.
Constellation Power Generation and Constellation Commodities Group	No	Based on the drastic differences between the previous revisions to these standards, and this proposed revision, 24 months would be a more reasonable timeframe for an effective date.
IRC Standards Review Committee	No	If the training and Operation Plan requirements are adopted as proposed, this may not be sufficient time for some entities to comply, particularly those with limited number of staff but perform functions that have multiple event reporting requirements.
ISO New England Inc.	No	If the training and Operation Plan requirements are adopted as proposed, this may not allow sufficient time for some entities to comply, particularly those with limited number of staff, but perform functions that have multiple event reporting requirements.
Kansas City Power & Light	No	April 2011 is too soon for considerations applicable to the creation of an Operating Plan.

Organization	Yes or No	Question 14 Comment
Manitoba Hydro	No	Though CIP-001-1a already contained provisions for sabotage response guidelines, the new EOP-004-2 R2 (2.1 to 2.9) will require reexamination of existing policies to remain compliant. Upon the approval of Attachment 1, the existing disturbance guidelines will also have to be reexamined. With the addition of R3 (Identify and assess), R4 (Drills) and R5 (Training), will also require redevelopment of existing processes.
NERC Staff	No	In order to provide explicit dates, the language should be modified to state: "First calendar day of the first calendar quarter one year after the date of the order providing applicable regulatory authority approval for all requirements."
Northeast Power Coordinating Council	No	The effective dates in Canada need to be defined. The first bullet should be sufficient. If the training and Operation Plan requirements are adopted as proposed, this may not allow sufficient time for some entities to comply, particularly those with limited number of staff, but perform functions that have multiple event reporting requirements.
Puget Sound Energy	No	There are no effective dates listed in the proposed standard. The proposed effective date should allow at least one year for entities to implement the requirements of the standard. In addition, if requirement R1 remains, then the requirement to implement an operating plan should only be triggered by the ERO's finalization of the form and system for reporting impact events and should provide at least six months for the implementation of the operating plan.
Santee Cooper	No	With the proposed training and drill requirements in the current written standard, one year is not enough time.
United Illuminating	No	UI believes the implementation should be staged. For R1 and R2: First calendar day of the first calendar quarter one year after applicable regulatory authority approval for all. This provides sufficient time to draft a procedure Then time needs to be provided to provide training prior to implementation of R3 and R6. UI believes two calendar quarters should be provided to complete training; therefore R3and R6 is effective six calendar quarters following regulatory approval. Implementation for R4 should state that the initial calendar year begins on the date R2 is effective and entities have 12 months following that date to complete their first drill. R5 requires training once per calendar year. Implementation for R5 should state that the initial calendar year begins on the date R2 is effective and entities have 12 months following that date to complete their first drill.

Organization	Yes or No	Question 14 Comment
US Bureau of Reclamation	No	There is a 15 month training requirement. If the standard goes into effect in one year, most entities will not have had an opportunity to develop their new Operating Plans and train their staff. The effective date should recognize Operating Plans need to be revised and then training needs to be implemented. The most aggressive schedule is 18 months. Two years would be more appropriate. The implementation date could recognize the Operating Plan development as one phase and the training as the second.
ATC	Yes	Yes, if ATC's recommended changes are made to the Standard. However, if the changes are not supported then ATC recommends that the implantation time be changed to two years. Entities will need time to develop both the plan called for in this standard and to train the personnel identified in the plan.
BGE	Yes	None.
Exelon	Yes	Agree with the proposed implementation date. A 12 month implementation will provide adequate time to generate, implement and provide any necessary training by a registered entity.
Ameren	Yes	
Arizona Public Service Company	Yes	
ATCO Electric Ltd.	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Co. of NY, Inc.	Yes	
Duke Energy	Yes	
Dynegy Inc.	Yes	
E.ON Climate & Renewables	Yes	
Electric Market Policy	Yes	

Organization	Yes or No	Question 14 Comment
ERCOT ISO	Yes	
FirstEnergy	Yes	
Georgia System Operations Corporation	Yes	
Great River Energy	Yes	
Green Country Energy	Yes	
Idaho Power Company	Yes	
Indeck Energy Services	Yes	
Luminant Energy	Yes	
MidAmerican Energy	Yes	
Midwest ISO Standards Collaborators	Yes	
MRO's NERC Standards Review Subcommittee	Yes	
North Carolina Electric Coops	Yes	
Pacific Gas and Electric Company	Yes	
PacifiCorp	Yes	
PacifiCorp	Yes	

Organization	Yes or No	Question 14 Comment
Pepco Holdings, Inc - Affiliates	Yes	
PNM Resources	Yes	
PPL Electric Utilities	Yes	
PPL Supply	Yes	
RRI Energy, Inc.	Yes	
SERC OC Standards Review Group	Yes	
Southern Company - Transmission	Yes	
TransAlta Corporation	Yes	
We Energies	Yes	
WECC	Yes	

15. Do you have any other comments that you have not identified above?

Summary Consideration: The DSR SDT has met with the EAWG and has put in place a process to ensure the cooperation and coordination between the DSR SDT and the EAWG. The impact event list is comprehensive and addresses the needs of the EAWG and EOP-004.

There were concerns expressed that the impact event list should include deliberate acts against infrastructure. The impact list includes "Risk to BES equipment from a non-environmental physical threat" the DSR SDT feels that this is inclusive of deliberate acts against infrastructure.

During discussions around the use and definition of the term sabotage, the DSR SDT considered the NRC definition and decided to eliminate the use of the term sabotage from EOP-004 and replaced it with impact events. The DSR SDT has developed a definition for "Impact Events" to support Attachment 1 as follows:

> "An Impact Event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action."

The DSR SDT has proposed this definition for inclusion in the NERC Glossary for "Impact Event". The types of Impact Events that are required to be reported are contained within Attachment 1. Only these events are required to be reported under this Standard. The DSR SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was that of sabotage or merely vandalism without the intervention of law enforcement after the fact. This will result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The Impact Events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive. Attachment 1, Part A is to be used for those actions that have impacted the electric system and in particular the section "Damage or destruction to equipment" clearly defines that all equipment that intentional or non intentional human error be reported. Attachment 1, Part B

covers the similar items but the action has not fully occurred but may cause a risk to the electric system and is required to be reported.

The industry commented on the need for e-mail addresses and fax numbers for back up purposes. These details were added to the standard and will also be covered in the implementation plan.

The proposed ballot in December was incorrect and has been deleted from the future development plan. The plan was updated with the correct project plan dates.

Organization	Yes or No	Question 15 Comment
Indeck Energy Services		Good start on a unified event reporting standard!
IRC Standards Review Committee	No	The standards should be changed to define what a “disturbance” is for reporting in EOP-004. Also, sabotage reporting requirements in CIP-001 should be rescinded as EOP-004 already has such requirements.
PSEG Companies		
Arizona Public Service Company	No	
ATCO Electric Ltd.	No	
Duke Energy	No	
Electric Market Policy	No	
FirstEnergy	No	
Independent Electricity System Operator	No	
Luminant Energy	No	

Organization	Yes or No	Question 15 Comment
Manitoba Hydro	No	
PacifiCorp	No	
PPL Supply	No	
RRI Energy, Inc.	No	
United Illuminating	No	
Ameren	Yes	We are concerned with the Future Development Plan. It shows an initial ballot period starting in December. This standard has significant issues and will need another distinct comment period (and not the formal comment period in parallel with balloting) prior to balloting.
American Electric Power (AEP)	Yes	The standard needs to be modified to allow the ability for one entity to report on behalf of other entities. For example the loss of Generation over the threshold could be reported by the RC opposed to the GO individually, if mutually agreed upon before the fact.
ATC	Yes	ATC believes that it is not evident in this draft that the SDT has worked collaboratively with the Events Analysis working group to leverage their work. ATC believes that NERC must coordinate this project and the EAWG efforts. The EAWG is proposing to modify NERC Rules of Procedure but the SDT is suggesting requirement for the ERO be build within the standard. We believe that the Rules of Procedure is the proper course to take to for identifying NERC obligations, but what is clear is that NERC itself does not seem to have an overall plan for event reporting and analysis. Lastly, ATC would like to see the SDT expand the mapping document to include the work of the EAWG. The industry needs to be presented with a clear picture as to how all these things will work together along with their reporting obligations. The definition of an “impact event” needs to be revised. First, if these events are to include any equipment failure or mis-operation that impacts the BES, the standard is requiring more than is intended based upon the reading of the requirements. PRC-004 already covers the reporting of protection system mis-operations, and if reading this definition verbatim, it would lead one to conclude that those same mis-operations reported under PRC-004 shall also be reported under EOP-004. The definition should be revised to something like: “An impact event is a system disturbance affecting the Bulk Electric System beyond loss of a single element under normal operating conditions and does not include events normally reported under PRC-004. Such events may be caused by...”

Organization	Yes or No	Question 15 Comment
BGE	Yes	One item that is properly addressed is the removal of Load Serving Entity from the Applicable Functional Entities. There may be a need to provide some guidance to Functional Entities when there are separate Transmission Owners and Transmission Operators or Generation Owners and Generation Operators. If they are separate, there may be redundancy in reporting.From the documentation, it doesn't seem like the SDT are combining all reports into one form as we would like to see. In the rational for R1 section, it talks of getting both forms (NERC and OE-417) together in one document (however it sounds like the forms within the document are still separate), available electronically, which only seems like a step forward. However, it does not take away the confusing process for the operators of which part of the form would need to be filled, who should be set this form depending on what part is filled, if one part of the form is filled out do the other parts need to be filled, etc. If the forms cannot be consolidated, BGE would rather the forms be separate to reduce confusion.BGE believes all these reports should require one form with one set of recipients, period.This may mean that NERC needs to get DOE to modify their OE-417 form.
Bonneville Power Administration	Yes	The document retention times in EOP-004-3 should be spelled out more clearly. The Compliance summary does so (but needs some punctuation clarification regarding investigation), the SDT should consider making that part of the requirements or clarifying the wording in the requirements.
CenterPoint Energy	Yes	CenterPoint Energy appreciates the efforts of the SDT in removing outdated and unnecessary language from the existing EOP-004 standard. Additionally, CenterPoint Energy urges the SDT to also remove the proposed "how to" prescriptive requirements. CenterPoint Energy believes the SDT team's focus should be on drafting a results-based standard for reporting actual system disturbances and acts of sabotage that disrupt the reliable operation of the BES. The SDT should not delve into trying to identify a list of events that have a potential reliability impact.As stated in response to Q10, CenterPoint Energy strongly believes that cyber-related events should not be in the scope of this standard since they are already required to be identified and reported to appropriate entities under CIP-008. Excluding cyber events from this standard further supports the elimination of redundancies within the body of standards.
City of Garland	Yes	Do not agree with this proposed draft - instead of combining 2 standards to gain efficiency, this expands the standard with unnecessary paperwork, drills, training, etc.For reports required under this standard, companies with multiple registration numbers and functions should only have to file one report for all functions and registrations.
Consolidated Edison Co. of NY, Inc.	Yes	Overriding Comment and Concern: It is absolutely essential that the work on EOP-004 and that on the NERC Event Analysis Process (EAP) be fully coordinated. We find that there are a number of inconsistencies between these two documents. The EAP and EOP-004 are not aligned. In order to operate and report

Organization	Yes or No	Question 15 Comment
		effectively entities need consistent requirements.
Constellation Power Generation and Constellation Commodities Group	Yes	As stated earlier, the "summary of concepts" for this latest revision, as written by the SDT, includes the following items: o A single form to report disturbances and impact events that threaten the reliability of the bulk electric system o Other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements o Clear criteria for reporting o Consistent reporting timelines o Clarity around of who will receive the information and how it will be used. Each and every requirement should be mapped to one of these 5 items; otherwise, it should not be included in this standard. Summarizing all of the comments above, Constellation Power Generation proposes the following revision to EOP-004-2:1. Title: Impact Event and Disturbance Assessment, Analysis, and Reporting 2. Number: EOP-004-2 3. Purpose: Responsible Entities shall report impact events and their known causes to support situational awareness and the reliability of the Bulk Electric System (BES). 4. Applicability 4.1. Functional Entities:4.1.1. Reliability Coordinator 4.1.2. Balancing Authority 4.1.3. Transmission Operator 4.1.4. Generator Operator 4.1.5. Distribution Provider 4.1.6. Electric Reliability Organization. Requirements and Measures R1. The ERO shall establish, maintain and utilize a system for receiving and distributing impact event reports, received pursuant to Requirement R6, to applicable government, provincial or law enforcement agencies and Registered Entities to enhance and support situational awareness.R2. Each Applicable Entity identified in Attachment 1 shall have an Operating Plan(s) for identifying, assessing and reporting impact events listed in Attachment 1 that includes the following components: 2.1. Method(s) for identifying impact events listed in Attachment 2.2. Method(s) for assessing cause(s) of impact events listed in Attachment 12.3. Method(s) for making internal and external notifications should an impact event listed in Attachment 1 occur. 2.4. Method(s) for updating the Operating Plan.2.5 Method(s) for making operation personnel aware of changes to the Operating Plan.R3. Each Applicable Entity shall implement their Operating Plan(s) to identify and assess cause of impact events listed in Attachment 1.R4. Each Applicable Entity shall provide training to all operation personnel at least annually.R5. Each Applicable Entity shall report impact events in accordance with its Operating Plan created pursuant to Requirement 2 and the timelines outlined in Attachment 1.
Dynegy Inc.	Yes	This does not address the inability of a GO/GOP to determine effects on the BES. Surrounding BES knowledge is limited for a GO/GOP.
E.ON Climate & Renewables	Yes	Refrain from having redundant reporting forms if at all possible. This can create confusion and lead to unnecessary penalty amounts and violations for registered entities. Potential" impacts of an event on the BES need to be clearly defined in the standard.
E.ON U.S. LLC	Yes	The new standard should incorporate all other disturbance, sabotage, or "impact event" reporting standards, such as CIP-008-3. At the very least it should reference those other standards that have within their scope

Organization	Yes or No	Question 15 Comment
		same/similar events in order to ensure complete reporting and full compliance. Suggesting that one standard provides the single reporting procedure, when in actuality it does not, is counterproductive. The discussion of "impact event" clearly indicates the SDT's intent to include sabotage events in the proposed standard EOP-004-2.
ERCOT ISO	Yes	ERCOT ISO supports the comments provided by the SRC. However, if the standard is to be established, ERCOT ISO has offered the comments contained herein as improvements to the requirements proposed. The requirements listed do not take into consideration the hierarchical reporting necessary for events (i.e.: GO to GOP to BA). The current structure will lead to redundant and conflicting reporting from multiple entities. This will lead to confusion in the analysis of the event. Any system developed and used to report impact events must include notification to the other relevant entities (i.e.: Reliability Coordinator, Balancing Authority, Transmission Operator, and Generator Operator). The proposed standard should not rely on a centralized system that does not follow the established hierarchy of dissemination of information.
Exelon	Yes	The standard is lacking guidance for DOE Form OE-417 reporting as outlined in the current version of EOP-004 and doesn't contain any non-BES related reporting. What is the governing process for OE-417 reporting?. Need clarification if one entity can respond on behalf to all entities in one company. Need a provision for entities to provide one report for all entities. Radiological sabotage is a defined term within the NRC glossary of terms. It would seem that a deliberate act directed towards a plant would also constitute an "impact event." In general, the DSR SDT should include discussions with the NRC to ensure communications are coordinated or consider utilizing existing reporting requirements currently required by the NRC for each nuclear generator operator for consistency. The definition of sabotage is defined by NRC is as follows: Any deliberate act directed against a plant or transport in which an activity licensed pursuant to 10 CFR Part 73 of NRC's regulations is conducted or against a component of such a plant or transport that could directly or indirectly endanger the public health and safety by exposure to radiation.
Georgia System Operations Corporation	Yes	Light years better than the current CIP-001-1 and EOP-004-1! With some changes from this comment period, we should have a clearer set of realistic requirements which could likely pass the ballot. Thanks go out to the drafting team for bringing clarity to this topic. Capitalization throughout this document is inconsistent. It is not in synch with the NERC Glossary. All terms that remain capitalized in the next draft (other than when used as a title or heading) should be defined in the Glossary of Terms Used in NERC Reliability Standards. Examples of not in synch with the Glossary: Registered Entity, Responsible Entity, Law Enforcement. These are not defined in the Glossary. The requirements that apply to entities should not use the word "analysis." "Assessment" should be used. Analysis is a different process (an ERO process) and is being addressed by

Organization	Yes or No	Question 15 Comment
		another group within NERC (Dave Nevius). This EOP-004 drafting team and the NERC analysis group should closely coordinate such that there are no conflicts and the combined requirements/processes are realistic (mainly regarding timelines).
Great River Energy	Yes	We are concerned with the Future Development Plan. It shows an initial ballot period starting in December. This standard has significant issues and will need another distinct comment period (and not the formal comment period in parallel with balloting) prior to balloting. Please provide an e-mail address for the submittal of the report to NERC (and any other parties above a Regional Entity) within this Standard and a fax number as a backup to electronic submittal.
Green Country Energy	Yes	I think the drafting team has done a wonderful job of beginning the task of combining two related standards. I ask them to keep in mind the small generators, and others who do not have the wide view capability, that more than likely react to events that occur wih no knowledge of why they occured, and limited staff to address administrative standard requirements. Many times the KISS approach is the best approach.
Idaho Power Company	Yes	By including training requirements in each standard, creates confusion and compliance or failure to comply potentian. PER standards are in place for personel training, these standards should be utilized for adding requirements that require training for NERC Standards.
ISO New England Inc.	Yes	Request clarification on how RCIS is part of this Standard. The form should be filled out in two stages. First stage would be the immediately available information. The second stage would be the additional information such as one line diagrams. There is concern with burdening the reporting operator on filling out forms instead of operating the Bulk Electric System. Most of the draft requirements are written as administrative in nature, and this is not most effective. Changes need to be made to (or possibly elimination of) R1, R2, R3.The standards should be changed to define what a “disturbance” is for reporting in EOP-004. Sabotage reporting as per CIP-001 should be rescinded as EOP-004 already has such a requirement.
Kansas City Power & Light	Yes	The standard addressed a preliminary report it should also address the requirements of a final report.
MidAmerican Energy	Yes	This entire standard needs to be revised to consider a results based standard.
Midwest ISO Standards Collaborators	Yes	We are concerned with the Future Development Plan. It shows an initial ballot period starting in December. This standard has significant issues and will need another distinct comment period (and not the formal comment period in parallel with balloting) prior to balloting.

Organization	Yes or No	Question 15 Comment
MRO's NERC Standards Review Subcommittee	Yes	Please provide an e-mail address for the submittal of the report to NERC (and any other parties above a Regional Entity) within this Standard and a fax number as a backup to electronic submittal.EOP-004 Attachment 2: Impact Event Reporting Form (note in the proposed standards it states EOP-002) seems to be written for Actual Impact Events only. Perhaps another section could be added for "Potential" Impact Events.
NERC Staff	Yes	NERC staff commends the SDT on its work so far. Merging CIP-001 and EOP-004 is a significant improvement and eliminates some current redundancies for reporting events. NERC staff believes opportunities to improve the proposed standard still exist. In particular, the team should consider possible redundancies with the Reliability Coordinator Working Group (RCWG) reporting guidelines, the Electricity Sector - Information Sharing and Analysis Center (ES-ISAC) reporting requirements for sharing information across sectors, and the Events Analysis Working Group (EAWG) efforts to develop event reporting processes. Ideally, the SDT and the EAWG should work together to develop a single consistent set of reporting criteria that can be utilized in both the EAWG event reporting process and in the requirements of the EOP-004-2 Reliability Standard.
North Carolina Electric Coops	Yes	Keep in mind that redundancy in reporting requirements from the DOE does not improve or enhance bulk electric system reliability but rather creates more work for the reporting entity.
Northeast Power Coordinating Council	Yes	Request clarification on how RCIS is part of this Standard. The form should be filled out in two stages. First stage would be the immediately available information. The second stage would be the additional information such as one line diagrams. There is concern with burdening the reporting operator on filling out forms instead of operating the Bulk Electric System. Most of the draft requirements are written as administrative in nature, and this is not most effective. Changes need to be made to (or possibly elimination of) R1, R2, R3.The standards should be changed to define what a "disturbance" is for reporting in EOP-004. Sabotage reporting as per CIP-001 should be rescinded as EOP-004 already has such a requirement.
Pacific Gas and Electric Company	Yes	PG&E believes as the training requirements continue to expand, having one training standard that captures all the training required within the NERC standards will allow for better clarity for the training departments in providing and meeting all NERC Standard compliance issues.
Pacific Northwest Small Public Power Utility Comment Group	Yes	The proposed standard has a huge impact on small DPs. DPs that presently do not maintain 24/7 dispatch centers will need to begin doing so to meet the reporting deadlines such as 1 hour after an occurrence is identified (possibly identified by a third party) or 24 hour after an occurrence (regardless of when it was discovered by the DP). The planning, assessing, drilling, training, and reporting requirements (R2-R6), as well as documentation (M2-M6) by small entities will cause utility rates to rise, will reduce local level of service,

Organization	Yes or No	Question 15 Comment
		and will not represent a corresponding increase to the reliability of the BES.The SDT concept of clear criteria for reporting has not been met, since R2 effectively directs the applicable entities to develop their own criteria. The decision of which types of events will be reported to which external organizations has been left up to the applicable entity. The comment group notes that there is no coordination of effort required between the applicable entities and the RCs or TOs that issue reliability directives. Energy Emergencies requiring voltage reduction or load shedding are likely to be communicated to applicable entities via directives. The likely result of this lack of coordination is that entities will plan, drill, and train for an event, but when the directive comes it will not be the one planned, drilled, and trained for. Coordination between those sending and receiving directives would ensure the probable events and directed responses are the ones planned, drilled, and trained for.
PacifiCorp	Yes	This is yet another standard with training requirements not covered under any PER standards.Having different training requirements spread throughout the standards makes it increasingly difficult to ensure all training requirements are met.Developing a "Training Standard" that lists ALL required training would streamline the process and aid greatly in compliance monitoring.
Pepco Holdings, Inc - Affiliates	Yes	The EAWG is developing processes that will be enforced through the Rules of Procedure. It may be inappropriate to reference the EAWG process in the Mapping Document.
PNM Resources	Yes	PNM believes that having one training standard that captures all the training required within the NERC standards will allow for better clarity for the training departments in providing and meeting all NERC Standard compliance issues. This will become even more of an issue as training requirements continue to expand.
PPL Electric Utilities	Yes	Combining EOP-004, CIP-001 and CIP-008's reporting requirements reduces redundancy and will add clarity to the compliance activities.
Puget Sound Energy	Yes	The DSR SDT's concepts for implementing a new structure for reporting are appropriate. Proper implementation of those concepts is likely to result in a very much improved standard. However, the proposed standard falls well short of implementing the concepts and is not much of an improvement on the current standard.
Santee Cooper	Yes	We don't believe that entities should be subjected to duplicate reporting to existing DOE requirements. How does redundancy in reporting requirements improve or enhance bulk electric system reliability?
SERC OC Standards Review	Yes	We find it disturbing that NERC is headed down a path of codifying requirements that are redundant to

Organization	Yes or No	Question 15 Comment
Group		existing DOE requirements. How does redundancy in reporting requirements improve or enhance bulk electric system reliability? Disclaimer:" The comments expressed herein represent a consensus of the views of the above named members of the SERC OC Standards Review group only and should not be construed as the position of SERC Reliability Corporation, its board or its officers."
Southern Company - Transmission	Yes	The only concern that we have with the proposed standard is that it feels like it is creating dual, not quite redundant, reporting requirements for cyber intrusions in concert with CIP-008. Hopefully, there will not have to be a redundant reporting requirement if we continue to merge efforts with the CIP Drafting Team. Since we will no longer use the word SABOTAGE in the new EOP-004, we are hoping the industry and the CIP Drafting Team will give us the criteria they wish for us to use in order to report CIP-008 incidents. We will then achieve a "ONE STOP SHOP" reporting standard.
Tenaska	Yes	Since the proposed EOP-004-2 Standard does not eliminate the OE-417 reporting requirement, it does not streamline the existing CIP-001-1 and EOP-004-1 reporting requirements for GO/GOP's. The "laundry list" of components required in the Operating Plan described in R2 is too specific and would make it more difficult to prove compliance during an audit. We prefer that the existing CIP-001-1 and EOP-004-1 Standards remain unchanged.
TransAlta Corporation	Yes	A Confidential Impact Event Report form is included in attachment 2 but nowhere in the standard does it say to use this form. This form appears to be similar to the "Preliminary Disturbance Report" form used in EOP-004-1. Clarity is required.
US Bureau of Reclamation	Yes	The SDT should consider that in reality it would be more streamlined to require immediate notification of an event for situational awareness, and then give adequate time for analysis of the cause. Reports that have an arbitrary rush will be diseased with low quality information and not much value in the long run to the BES. The Attachment A should be constructed around notification of situational awareness. The reporting timeline should be constructed around the different levels severity. The more severe the event, usually the more complicated the event is to analyze. Simple events usually do not have a significant impact.
We Energies	Yes	Please be careful to capitalize defined terms. If the intent is to not use the defined term, use another word."Forced intrusion" (cutting a fence, breaking in a door) may not be discovered for quite some time after it occurs. Should it be reported as soon as discovered? Even if there was no impact event (disturbance)? "Destruction of a Bulk Electric System Component" seems pretty specific. However, if a transformer kicks off line due to criminal damage, yet is considered repairable, is the event reportable?

Organization	Yes or No	Question 15 Comment
WECC	Yes	Having one training standard that captures all the training required within the NERC standards will allow for better clarity for the training departments in providing and meeting all NERC Standard compliance issues. This will become even more of an issue as training requirements continue to expand.CIP-001-1 has surprisingly been one of the most violated standards during the initial period. However, most entities have now developed and demonstrated a decent compliance process. Unless a revised standard to address the FERC directive on sabotage is developed (as suggested in 13 above) this proposed standard appears to eliminate sabotage reporting as a reliability standard to the potential detriment of BES reliability.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SC approved SAR for initial posting (April, 2009).
2. SAR posted for comment (April 22 – May 21, 2009).
3. SC authorized moving the SAR forward to standard development (September 2009).
4. Concepts Paper posted for comment (March 17 – April 16, 2010).
5. Initial Informal Comment Period (September 2010)

Proposed Action Plan and Description of Current Draft
This is the first posting of the proposed standard in accordance with Results-Based Criteria. The drafting team requests posting for a 30-day formal comment period.

Future Development Plan

Anticipated Actions	Anticipated Date
Drafting team considers comments, makes conforming changes, and proceed to second comment	October 2010 – February 2011
Second Comment Period	March – May 2011
Third Comment/Ballot period	June- July 2011
Recirculation Ballot period	July-August 2011
Receive BOT approval	September 2011

Effective Dates

1. The standard shall become effective on the first calendar day of the third calendar quarter after the date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, the standard shall become effective on the first calendar day of the third calendar quarter after Board of Trustees adoption.

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-1 Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2 Impact Event Reporting; Retire CIP-001-1a Sabotage Reporting and Retired EOP-004-1 Disturbance Reporting.	Revision to entire standard (Project 2009-01)

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Impact Event: Any event which has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action.

When this standard has received ballot approval, the text boxes will be moved to the Guideline and Technical Basis Section.

Introduction

1. **Title:** Impact Event Reporting

2. **Number:** EOP-004-2

3. **Purpose:** To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of Impact Events and their causes, if known, by the Responsible Entities.

4. **Applicability**

   4.1. Functional Entities: Within the context of EOP-004-2, the term "Responsible Entity" shall mean:

   4.1.1. Reliability Coordinator

   4.1.2. Balancing Authority

   4.1.3. Interchange Authority

   4.1.4. Transmission Service Provider

   4.1.5. Transmission Owner

   4.1.6. Transmission Operator

   4.1.7. Generator Owner

   4.1.8. Generator Operator

   4.1.9. Distribution Provider

   4.1.10 Load Serving Entity

5. **Background:**

NERC established a SAR Team in 2009 to investigate revisions to the CIP-001 and EOP-004 Reliability Standards.

1. CIP-001 may be merged with EOP-004 to eliminate redundancies.
2. Acts of sabotage have to be reported to the DOE as part of EOP-004.
3. Specific references to the DOE form need to be eliminated.
4. EOP-004 has some 'fill-in-the-blank' components to eliminate.

The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards (see tables for each standard at the end of this SAR for more detailed information).

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC SC in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009. A "concepts paper" was designed to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed.

The concept paper sought comments from stakeholders on the "road map" that will be used by the SDR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the SDR SDT.

The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC database and FERC Order 693 Directives in order to determine a prudent course of action with respect to these standards.

The DSR SDT has used a working definition for "Impact Events" to develop Attachment 1 as follows:

> "An Impact Event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action."

The DSR SDT has proposed this definition for inclusion in the NERC Glossary for "Impact Event". The types of Impact Events that are required to be reported are contained within Attachment 1. Only these events are required to be reported under this Standard. The DSR SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was that of sabotage or merely vandalism without the intervention of law enforcement after the fact. This will result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The Impact Events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive. Attachment 1, Part A is to be used for those actions that have impacted the electric system and in particular the section "Damage or destruction to equipment" clearly defines that all equipment that intentional or non intentional human error be reported. Attachment 1, Part B covers the similar items but the action has not fully occurred but may cause a risk to the electric system and is required to be reported.

To support this concept, the DSR SDT has provided specific event for reporting including types of Impact Events and timing thresholds pertaining to the different types of Impact Events and who's responsibility for reporting under the different Impact Events. This information is outlined in Attachment 1 to the proposed standard.

The DSR SDT wishes to make clear that the proposed changes do not include any real-time operating notifications for the types of events covered by CIP-001, EOP-004. This is achieved

through the RCIS and is covered in other standards (e.g. TOP). The proposed standard deals exclusively with after-the-fact reporting.

The DSR SDT is proposing to consolidate disturbance and Impact Event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts

- A single form to report disturbances and Impact Events that threaten the reliability of the bulk electric system
- Other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements
- Clear criteria for reporting
- Consistent reporting timelines
- Clarity around of who will receive the information and how it will be used

Law Enforcement Reporting

The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting Impact Events. Certain outages, such as those due to vandalism and terrorism, are not preventable. Entities rely upon law enforcement agencies to respond and investigate those Impact Events which have the potential of wider area affect upon the industry which enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading involving Impact Events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.

Stakeholders in the Reporting Process

- Industry
- NERC (ERO)
- FERC
- DOE
- DHS – Federal
- Homeland Security- State
- State Regulators
- Local Law Enforcement
- State Law Enforcement
- FBI

The above stakeholders have an interest in the timely notification, communication and response to an incident at an industry facility. The stakeholders have various levels of accountability and have a vested interest in the protection and response to ensure the reliability of the BES.

Present expectations of the industry under CIP-001:

It has been the understanding by industry participants that an occurrence of sabotage has to be reported to the FBI. The FBI has the jurisdictional requirements to investigate acts of sabotage and terrorism. The present CIP-001-1 standard requires a liaison relationship on behalf of the industry and FBI. Annual requirements, under the standard, of the industry have not been clear and have lead to misunderstandings and confusion in the industry as to how to demonstrate the liaison is in place and effective. FBI offices have been asked to confirm, on FBI letterhead, the existence of a working relationship to report acts of sabotage to include references to years the liaison has been in existence and confirming telephone numbers for the FBI.

Coordination of Local and State Law Enforcement Agencies with the FBI

The Joint Terrorism Task Force (JTTF) came into being with the first task force being established in 1980. JTTFs are small cells of highly trained, locally based, passionately committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. The JTTF is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. Coordination and communications largely through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs. This information flow can be most beneficial to the industry in analytical intelligence, incident response and investigation. Historically, the most immediate response to an industry incident has been local and state law enforcement agencies to suspected vandalism and criminal damages at industry facilities. Relying upon the JTTF coordination between local, state and FBI law enforcement would be beneficial to effective communications and the appropriate level of investigative response.

Coordination of Local and Provincial Law Enforcement Agencies with the RCMP

A similar law enforecment coordination hierarchy exists in Canada. Local and Provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. The Provincial law enforcement agency has a reporting relationship with the Royla Canadian Mounted Police (RCMP).

A Reporting Process Solution – EOP-004

A proposal discussed with FBI, FERC Staff, NERC Standards Project Coordinator and SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Impact Event EOP-004-2). Essentially, reporting an Impact Event to law enforcement agencies will only require the industry to notify the state or provincial level law enforcement agency. The state or provincial level law enforcement agency will coordinate with local law enforcement to investigate. If the state or provincial level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial level law enforcement agency will notify and coordinate with the FBI or the RCMP.

Reporting Hierachy for Impact Event EOP-004-2

*Canadian entities will follow law enforcement protocols applicable in their jurisdictions

Requirements and Measures

R1. Each Responsible Entity shall have an Impact Event Operating Plan that includes: *[Violation Risk: Factor Medium] [Time Horizon: Long-term Planning]*

1.1. An Operating Process for identifying Impact Events listed in Attachment 1.

1.2. An Operating Procedure for gathering information for Attachment 2 regarding observed Impact Events listed in Attachment 1.

1.3. An Operating Process for communicating recognized Impact Events to the following:

1.3.1. Internal company personnel notification(s).

1.3.2. External organizations to notify to include but not limited to the Responsible Entities' Reliability Coordinator, NERC, Responsible Entities' Regional Entity, Law Enforcement, and Governmental or Provincial Agencies.

1.4. Provision(s) for updating the Impact Event Operating Plan within 90 days of any change to its content.

M1. Each Responsible Entity shall provide the current in force Impact Event Operating Plan to the Compliance Enforcement Authority.

Rationale for R1

Every industry participant that owns or operates elements or devices on the grid has a formal or informal process, procedure, or steps it takes to gather information regarding what happened and why it happened when Impact Events occur. This requirement has the Registered Entity establish documentation on how that procedure, process, or plan is organized.

For the Impact Event Operating Plan, the DSR SDT envisions that Part 1.2 includes performing sufficient analysis and information gathering to be able to complete the report for reportable Impact Events. The main issue is to make sure an entity can a) identify when an Impact Event has occurred and b) be able to gather enough information to complete the report.

Part 1.3 could include a process flowchart, identification of internal positions to be notified and to make notifications, or a list of personnel by name as well as telephone numbers.

The Impact Event Operating Plan may include, but not be limited to, the following: how the entity is notified of event's occurrence, person(s) initially tasked with the overseeing the assessment or analytical study, investigatory steps typically taken, and documentation of the assessment / remedial action plan.

R2. Each Responsible Entity shall implement its Impact Event Operating Plan documented in Requirement R1 for Impact Events listed in Attachment 1 (Parts A and B). *[Violation Risk: Factor Medium] [Time Horizon: Real-time Operations and Same-day Operations]*

M2. To the extent that an Responsible Entity has an Impact Event on its Facilities, the Responsible Entity shall provide documentation of the implementation of its Impact Event Operating Plans. Such evidence could include, but is not limited to, operator logs, voice

recordings, or other notations and documents retained by the Registered Entity for each Impact Event.

R3. Each Responsible Entity shall conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 at least annually, with no more than 15 calendar months between tests. *[Violation Risk: Factor Medium] [Time Horizon: Long-term Planning]*

M3. In the absence of an actual Impact Event, the Responsible Entity shall provide evidence that it conducted a mock Impact Event and followed its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The time period between actual and or mock Impact Events shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or documentation. (R3)

Rationale for R3

The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized Impact Events is correct so that the entity can respond appropriately in the case of an actual Impact Event. The Responsible Entity may conduct a drill or exercise of its Operating Process for communicating recognized Impact Events as often as it desires but the time period between such drill or exercise can be no longer than 15 months from the previous drill/exercise or actual Impact Event (i.e., if you conducted an exercise/drill/actual employment of the Operating Process in January of one year, there would be another exercise/drill/actual employment by March 31 of the next calendar year)). Multiple exercises in a 15 month period are not a violation of the requirement and would be encouraged to improve reliability.

R4. Each Responsible Entity shall review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan at least annually with no more than 15 calendar months between review sessions*[Violation Risk: Factor Medium] [Time Horizon: Long-term Planning]*.

M4. Responsible Entities shall provide the materials presented to verify content and the association between the people listed in the plan and those who participated in the review, documentation showing who was present and when internal personnel were trained on the responsibilities in the plan.

R5. Each Responsible Entity shall report Impact Events in accordance with the Impact Event Operating Plan pursuant to Requirement R1 and Attachment 1 using the form in Attachment 2 or the DOE OE-417 reporting form. *[Violation Risk: Factor: Medium] [Time Horizon: Real-time Operations and Same-day Operations]*.

M5. Responsible Entities shall provide evidence demonstrating the submission of reports using the plan created pursuant to Requirement R1 and Attachment 1 using either the form in

Attachment 2 or the DOE OE-417 report. Such evidence will include a copy of the Attachment 2 form or OE-417 report submitted, evidence to support the type of Impact Event experienced; the date and time of the Impact Event; as well as evidence of report submittal that includes date and time.

Compliance

Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.

Compliance Monitoring and Enforcement Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

Evidence Retention
Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.

If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Medium	The Responsible Entity has an Impact Event Operating Plan but failed to include one of Parts 1.1 through 1.4.	The Responsible Entity has a Impact Event Operating Plan but failed to include two of Parts 1.1 through 1.4.	The Responsible Entity has an Impact Event Operating Plan but failed to include three of Parts 1.1 through 1.4.	The Responsible Entity failed to include all of Parts 1.1 through 1.4.
R2	Real-time Operations and Same-day Operations	Medium	N/A	N/A	N/A	The Responsible Entity failed to implement its Impact Event Operating Plan for an Impact Event listed in Attachment 1.
R3	Long-term Planning	Medium	The Responsible Entity failed to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part	The Responsible Entity failed to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part	The Responsible Entity failed to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part	The Responsible Entity failed to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part

			1.3 in more than 15 months but less than 18 months.	1.3in more than 18 months but less than 21 months.	1.3 in more than 21 months but less than 24 months.	1.3 in more than 24 months
R4	Long-term Planning	Medium	The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan l in more than 15 months but less than 18 months.	The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 18 months but less than 21 months.	The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 21 months but less than 24 months.	The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 24 months
R5	Real-time Operations and Same-day Operations	Medium	The Responsible Entity failed to submit a report in less than 36 hours for an Impact Event requiring reporting within 24 hours in Attachment 1.	The Responsible Entity failed to submit a report in more than 36 hours but less than or equal to 48 hours for an Impact Event requiring reporting within 24 hours in Attachment 1.	The Responsible Entity failed to submit a report in more than 48 hours but less than or equal to 60 hours for an Impact Event requiring reporting within 24 hours in Attachment 1. OR The Responsible Entity failed to submit a report in more than 1 hour but less than 2 hours for an Impact Event requiring reporting within 1 hour in Attachment 1.	The Responsible Entity failed to submit a report in more than 60 hours for an Impact Event requiring reporting within 24 hours in Attachment 1. OR The Responsible Entity failed to submit a report in more than 2 hours for an Impact Event requiring reporting within 1 hour in Attachment 1. OR The responsible entity failed to submit a

						report for an Impact Event in Attachment 1.

Variances

None

Interpretations

None

EOP-004 - Attachment 1: Impact Events Table

NOTE: Under certain adverse conditions, e.g. severe weather, it may not be possible to report the damage caused by an Impact Event and issue a written Impact Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify its Regional Entity(ies) and NERC, (e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422) and provide as much information as is available. The affected Responsible Entity shall then provide periodic verbal updates until adequate information is available to issue a written Impact Event report.

EOP-004 – Attachment 1 - Actual Reliability Impact – Part A			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Time to Submit Report**
Energy Emergency requiring Public appeal for load reduction	Initiating entity is responsible for reporting	Each public appeal for load reduction	Within 1 hour of issuing a public appeal
Energy Emergency requiring system-wide voltage reduction	Initiating entity is responsible for reporting	System wide voltage reduction of 3% or more	Within 1 hour after event is initiated
Energy Emergency requiring manual firm load shedding	Initiating entity is responsible for reporting	Manual firm load shedding ≥ 100 MW	Within 1 hour after event is initiated
Energy Emergency resulting in automatic firm load shedding	Each DP or TOP that experiences the Impact Event	Firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)	Within 1 hour after event is initiated
Voltage Deviations on BES Facilities	Each RC, TOP, GOP that experiences the Impact Event	± 10% sustained for ≥ 15 continuous minutes	Within 24 hours after 15 minute threshold
IROL Violation	Each RC, TOP that experiences the Impact Event	Operate outside the IROL for time greater than IROL Tv	Within 24 hours after Tv threshold
Loss of Firm load for ≥ 15 Minutes	Each RC, BA, TOP, DP that experiences the Impact Event	• ≥ 300 MW for entities with previous year's demand ≥ 3000 MW • ≥ 200 MW for all other entities	Within 1 hour after 15 minute threshold
System Separation	Each RC, BA, TOP, DP that	Each separation resulting in an island of	Within 1 hour after occurrence is

EOP-004 – Attachment 1 - Actual Reliability Impact – Part A			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Time to Submit Report**
(Islanding)	experiences the Impact Event	generation and load ≥ 100 MW	identified
Generation loss	Each RC, BA, GOP that experiences the Impact Event	• ≥ 2,000 MW for entities in the Eastern or Western Interconnection • ≥ 1000 MW for entities in the ERCOT or Quebec Interconnection	Within 24 hours after occurrence
Loss of Off-site power to a nuclear generating plant (grid supply)	Each RC, BA, TO, TOP, GO, GOP that experiences the Impact Event	Affecting a nuclear generating station per the Nuclear Plant Interface Requirement	Report within 24 hours after occurrence
Transmission loss	Each RC, TOP that experiences the Impact Event	Three or more BES Transmission Elements	Within 24 hours after occurrence
Damage or destruction of BES equipment[1]	Each RC, BA, TO, TOP, GO, GOP, DP that experiences the Impact Event	Through operational error, equipment failure, external cause, or intentional or unintentional human action.	Within 1 hour after occurrence is identified
Damage or destruction of Critical Asset	Applicable Entities under CIP-002 or its successor.	Through operational error, equipment failure, external cause, or intentional or unintentional human action.	Within 1 hour after occurrence is identified
Damage or destruction of a Critical Cyber Asset	Applicable Entities under CIP-002 or its successor.	Through intentional or unintentional human action.	Within 1 hour after occurrence is identified

[1]BES equipment that: i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii) Damaged or destroyed due to intentional or unintentional human action; or iv) Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly e.g., removal of grounding straps rendering protective relaying inoperative.

EOP-004 – Attachment 1 - Potential Reliability Impact – Part B			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Time to Submit Report**
Unplanned Control Center evacuation	Each RC, BA, TOP that experiences the potential Impact Event	Unplanned evacuation from BES control center facility	Report within 24 hour after occurrence
Fuel supply emergency	Each RC, BA, GO, GOP that experiences the potential Impact Event	Affecting BES reliability[2]	Report within 1 hour after occurrence
Loss of all monitoring or voice communication capability	Each RC, BA, TOP that experiences the potential Impact Event	Affecting a BES control center for ≥ 30 continuous minutes	Report within 24 hours after occurrence
Forced intrusion[3]	Each RC, BA, TO, TOP, GO, GOP that experiences the potential Impact Event	At a BES facility	Report within 1 hour after verification of intrusion

[2] Report if problems with the fuel supply chain result in the projected need for emergency actions to manage reliability.

[3] Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects the reliability of the BES).

Risk to BES equipment[4]	Each RC, BA, TO, TOP, GO, GOP, DP that experiences the potential Impact Event	From a non-environmental physical threat	Report within 1 hour after identification
Detection of a reportable Cyber Security Incident.	Each RC, BA, TO, TOP, GO, GOP, DP that experiences the potential Impact Event	That meets the criteria in CIP-008 (or its successor)	Report within 1 hour after detection

[4] Examples include a train derailment adjacent to BES equipment, that either could have damaged the equipment directly or has the potential to damage the equipment (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center) and report of suspicious device near BES equipment).

EOP-004 - Attachment 2: Impact Event Reporting Form

This form is to be used to report Impact Events to the ERO. NERC will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Reports should be submitted via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550

Impact Event Reporting for EOP-004-2		
	Task	**Comments**
1.	Entity filing the report (include company name and Compliance Registration ID number):	
2.	Date and Time of Impact Event. Date: (mm/dd/yyyy) Time/Zone:	
3.	Name of contact person: Email address: Telephone Number:	
4.	Did the actual or potential Impact Event originate in your system?	Actual Impact Event ☐ Potential Impact Event ☐ Yes ☐ No☐ Unknown ☐
5.	Under which NERC function are you reporting? (RC, TOP, BA, other)	

Impact Event Reporting for EOP-004-2			
	Task	Comments	
6.	Brief Description of actual or potential Impact Event: (More detail should be provided in the Sequence of Events section below.)		
7.	Generation tripped off-line*. MW Total List units tripped		
8.	Frequency*. Just prior to Impact Event (Hz): Immediately after Impact Event (Hz max): Immediately after Impact Event (Hz min):		
9.	List transmission facilities (lines, transformers, buses, etc.) tripped and locked-out*. (Specify voltage level of each facility listed).		
10.	Demand tripped (MW)*: Number of affected customers*:	FIRM	INTERRUPTIBLE

Impact Event Reporting for EOP-004-2			
	Task	Comments	
	Demand lost (MW-Minutes)*:		
11.	Restoration Time*.	INITIAL	FINAL
	Transmission:		
	Generation:		
	Demand:		
12.	Sequence of Events of actual or potential Impact Event (if potential Impact Event, please describe your assessment of potential impact to BES) :		

Impact Event Reporting for EOP-004-2		
	Task	**Comments**
13.	Identify the initial probable cause or known root cause of the actual or potential Impact Event if known at time of submittal of Part I of this report:	
14.	Identify any protection system misoperation(s)[1]:	
15.	Additional Information that helps to further explain the actual or potential Impact Event if needed.	

[1] Only applicable if it is part of the impact event the responsible entity is reporting on

Guideline and Technical Basis

Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01) - Reporting Concepts

Introduction

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and is progressing toward developing standards based on the SAR. This concepts paper is designed to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed.

The standards listed under the SAR are:

- CIP-001 — Sabotage Reporting
- EOP-004 — Disturbance Reporting

The DSR SDT also proposed to investigate incorporation of the cyber incident reporting aspects of CIP-008 under this project. This will be coordinated with the Cyber Security - Order 706 SDT (Project 2008-06).

The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC database and FERC Order 693 Directives to determine a prudent course of action with respect to these standards.

This concept paper provides stakeholders with a proposed “road map” that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. This concept paper provides the background information and thought process of the DSR SDT.

The proposed changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). The proposed standards deal exclusively with after-the-fact reporting.

The DSR SDT is proposing to consolidate disturbance and event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts and Assumptions:

The Standard Will: Require use of a single form to report disturbances and "Impact Events" that threaten the reliability of the bulk electric system

- Provide clear criteria for reporting
- Include consistent reporting timelines
- Identify appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- Provide clarity around of who will receive the information

The drafting team will explore other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements

Discussion of Disturbance Reporting
Disturbance reporting requirements currently exist in EOP-004. The current approved definition of Disturbance from the NERC Glossary of Terms is:

1. An unplanned event that produces an abnormal system condition.
2. Any perturbation to the electric system.
3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.

Disturbance reporting requirements and criteria are in the existing EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and developed the list of Impact Events that are to be reported under this standard (attachment 1).

Discussion of "Impact Event" Reporting
There are situations worthy of reporting because they have the potential to impact reliability. The DSR SDT proposes calling such incidents 'Impact Events' with the following concept:

> An Impact Event is any situation that has the potential to significantly impact the reliability of the Bulk Electric System. Such events may originate from malicious intent, accidental behavior, or natural occurrences.

Impact Event reporting facilitates industry awareness, which allows potentially impacted parties to prepare for and possibly mitigate the reliability risk. It also provides the raw material, in the case of certain potential reliability threats, to see emerging patterns.

Examples of Impact Events include:

- Bolts removed from transmission line structures
- Detection of cyber intrusion that meets criteria of CIP-008 or its successor standard
- Forced intrusion attempt at a substation
- Train derailment near a transmission right-of-way
- Destruction of Bulk Electrical System equipment

What about sabotage?
One thing became clear in the DSR SDT's discussion concerning sabotage: everyone has a different definition. The current standard CIP-001 elicited the following response from FERC in FERC Order 693, paragraph 471 which states in part: *". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."*

Often, the underlying reason for an event is unknown or cannot be confirmed. The DSR SDT believes that reporting material risks to the Bulk Electrical System using the Impact Event categorization, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.

The DST SDT discussed the reliability needs for Impact Event reporting and will consider guidance found in the document "NERC Guideline: Threat and Incident Reporting" in the development of requirements, which will include clear criteria for reporting.

Certain types of Impact Events should be reported to NERC, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and/or Provincial or local law enforcement. Other types of Impact Events may have different reporting requirements. For example, an Impact Event that is related to copper theft may only need to be reported to the local law enforcement authorities.

Potential Uses of Reportable Information
Event analysis, correlation of data, and trend identification are a few potential uses for the information reported under this standard. As envisioned, the standard will only require Functional entities to report the incidents and provide information or data necessary for these analyses. Other entities (e.g. – NERC, Law Enforcement, etc) will be responsible for performing the analyses. The NERC Rules of Procedure (section 800) provide an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for reliability. Jurisdictional agencies (which may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE) have other duties and responsibilities.

Collection of Reportable Information or "One stop shopping"
The goal of the DSR SDT is to have one reporting form for all functional entities (US, Canada, Mexico) to submit to NERC. Ultimately, it may make sense to develop an electronic version to expedite completion, sharing and storage. Ideally, entities would complete a single form which could then be distributed to jurisdictional agencies and functional entities as appropriate. Specific reporting forms[6] that exist today (i.e. - OE-417, etc) could be included as part of the

[6] The DOE Reporting Form, OE-417 is currently a part of the EOP-004 standard. If this report is removed from the standard, it should be noted that this form is still required by law as noted on the form: NOTICE: This report is mandatory under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. Title 18 USC 1001 makes it a criminal

electronic form to accommodate US entities with a requirement to submit the form, or may be removed (but still be mandatory for US entities under Public Law 93-275) to streamline the proposed consolidated reliability standard for all North American entities (US, Canada, Mexico). Jurisdictional agencies may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE. Functional entities may include the RC, TOP, and BA for industry awareness. Applicability of the standard will be determined based on the specific requirements.

The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT is planning to update the listing of reportable events from discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences may still exist.

The reporting proposed by the DSR SDT is intended to meet the uses and purposes of NERC. The DSR SDT recognizes that other requirements for reporting exist (e.g., DOE-417 reporting), which may duplicate or overlap the information required by NERC. To the extent that other reporting is required, the DSR SDT envisions that duplicate entry of information is not necessary, and the submission of the alternate report will be acceptable to NERC so long as all information required by NERC is submitted. For example, if the NERC Report duplicates information from the DOE form, the DOE report may be included or attached to the NERC report, in lieu of entering that information on the NERC report.

offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SC approved SAR for initial posting (April, 2009).
2. SAR posted for comment (April 22 – May 21, 2009).
3. SC authorized moving the SAR forward to standard development (September 2009).
4. Concepts Paper posted for comment (March 17 – April 16, 2010).
5. Initial Informal Comment Period (September 2010)

Proposed Action Plan and Description of Current Draft
This is the first posting of the proposed standard in accordance with Results-Based Criteria. The drafting team requests posting for a 30-day formal comment period.

Future Development Plan

Anticipated Actions	Anticipated Date
~~Initial Comment Period~~Drafting team considers comments, makes conforming changes, and proceed to second comment	~~September~~October 2010 – February 2011
~~Drafting team considers comments, makes conforming changes, and proceed to second comment~~ Second Comment Period	~~October – December 2010~~March – May 2011
Third Comment ~~Period/Initial~~ /Ballot period	~~December 2010- January~~June- July 2011
~~Successive Comment/~~Recirculation Ballot period	~~February – March~~July-August 2011
Receive BOT approval	~~April~~September 2011

Effective Dates

1. ~~USA:~~ The standard shall become effective on the ~~F~~first calendar day of the ~~first~~third calendar quarter ~~one year~~ after ~~-~~the date of the order providing applicable regulatory ~~authority~~ approval. ~~for all requirements~~

2. ~~Canada and Mexico: First calendar day of~~~~Concurrent with the~~ ~~first calendar quarter one year following Board of Trustees adoption unless governmental authority withholds approval~~~~Effective Date for the USA.~~ In those jurisdictions where no regulatory approval is required, the standard shall become effective on the first calendar day of the third calendar quarter after Board of Trustees adoption.

Formatted: Font: 12 pt

Formatted: Font: 12 pt

Formatted: Font: 12 pt

Formatted: Font: 12 pt

Formatted: Normal

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-1 Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2~~;~~ Impact Event Reporting; Retire CIP-001-1a Sabotage Reporting and Retired EOP-004-1~~, R1, R3.2, R3.3, R3.4, R4, R5 and associated measures, evidence retention and VSLs~~ Disturbance Reporting. ~~Added new requirements for ERO – R1, R7, R8.~~	Revision to entire standard (Project 2009-01)

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

~~None~~

Impact Event: Any event which has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action.

When this standard has received ballot approval, the text boxes will be moved to the Guideline and Technical Basis Section.

Introduction

1. Title: Impact Event ~~and Disturbance Assessment, Analysis, and~~ Reporting

2. Number: EOP-004-2

3. Purpose: ~~Responsible Entities shall report impact events and their known causes to support situational~~To improve industry awareness and the reliability of the Bulk Electric System ~~(BES).~~by requiring the reporting of Impact Events and their causes, if known, by the Responsible Entities.

4. Applicability

4.1. Functional Entities: Within the context of EOP-004-2, the term "Responsible Entity" shall mean:

4.1.1. Reliability Coordinator

4.1.2. Balancing Authority

4.1.3. Interchange Authority

4.1.4. Transmission Service Provider

~~4.1.3.~~4.1.5. Transmission Owner

~~4.1.4.~~4.1.6. Transmission Operator

~~4.1.5.~~4.1.7. Generator Owner

~~4.1.6.~~4.1.8. Generator Operator

~~4.1.7.~~4.1.9. Distribution Provider

~~4.1.8. Electric Reliability Organization~~

4.1.10 Load Serving Entity

5. Background:

NERC established a SAR Team in 2009 to investigate revisions to the CIP-001 and EOP-004 Reliability Standards.

1. CIP-001 may be merged with EOP-004 to eliminate redundancies.
2. Acts of sabotage have to be reported to the DOE as part of EOP-004.
3. Specific references to the DOE form need to be eliminated.
4. EOP-004 has some 'fill-in-the-blank' components to eliminate.

The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality,

enforceable and technically sufficient bulk power system reliability standards (see tables for each standard at the end of this SAR for more detailed information).

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC SC in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009. A "concepts paper" was designed to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed.

The concept paper sought comments from stakeholders on the "road map" that will be used by the SDR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the SDR SDT.

The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC database and FERC Order 693 Directives in order to determine a prudent course of action with respect to these standards.

The DSR SDT has ~~proposed the following concept for ***impact event***~~used a working definition for "Impact Events" to develop Attachment 1 as follows:

> "An ~~*impact event*~~Impact Event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action~~.~~."

The DSR SDT has proposed this definition for inclusion in the NERC Glossary for "Impact Event". The types of Impact Events that are required to be reported are contained within Attachment 1. Only these events are required to be reported under this Standard. The DSR SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was that of sabotage or merely vandalism without the intervention of law enforcement after the fact. This will result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The Impact Events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive. Attachment 1, Part A is to be used for those actions that have impacted the electric system and in particular the section "Damage or destruction to equipment" clearly defines that all equipment that intentional or non intentional human error be reported. Attachment 1, Part B covers the similar items but the action has not fully occurred but may cause a risk to the electric system and is required to be reported.

To support this concept, the DSR SDT has provided specific event for reporting including types of ~~impact events~~Impact Events and timing thresholds pertaining to the different types of ~~impact events~~Impact Events and who's responsibility for reporting under the different ~~impact events~~Impact Events. This information is outlined in Attachment 1 to the proposed standard.

EOP-004-2 — Impact Event ~~and Disturbance Assessment, Analysis, and~~ Reporting

The DSR SDT wishes to make clear that the proposed changes do not include any real-time operating notifications for the types of events covered by CIP-001, EOP-004. This is achieved through the RCIS and is covered in other standards (e.g. TOP). The proposed standard deals exclusively with after-the-fact reporting.

The DSR SDT is proposing to consolidate disturbance and ~~impact event~~Impact Event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts

- A single form to report disturbances and ~~impact events~~Impact Events that threaten the reliability of the bulk electric system
- Other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements
- Clear criteria for reporting
- Consistent reporting timelines
- Clarity around of who will receive the information and how it will be used

Law Enforcement Reporting

The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting Impact Events. Certain outages, such as those due to vandalism and terrorism, are not preventable. Entities rely upon law enforcement agencies to respond and investigate those Impact Events which have the potential of wider area affect upon the industry which enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading involving Impact Events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.

Stakeholders in the Reporting Process

- Industry

~~Rationale for R1~~

~~The goal of the DSR SDT is to have a generic reporting form and a system for all functional entities (US, Canada, Mexico) to submit impact event reports to NERC and other entities. Ultimately, it may make sense to develop an electronic version of the form to expedite completion, sharing and storage. Ideally, entities would complete a single electronic form on-line which could then be electronically forwarded or distributed to jurisdictional agencies and functional entities as appropriate using check boxes or other coding within the electronic form. Specific reporting forms that exist today (i.e. - OE-417, etc) could be included as part of the electronic form to accommodate US entities with a requirement to submit the form or may be removed (but still be mandatory for US entities under Public Law 93-275) to streamline the proposed consolidated reliability standard for all North American entities (US, Canada, Mexico). Jurisdictional agencies may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE. Functional entities may include the RC, TOP, and BA for situational awareness. Applicability of the standard will be determined based on the specific requirements.~~

~~The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT is planning to update the listing of reportable events from discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences may still exist.~~

~~Responsible entities will ultimately be responsible for ensuring that OE-417 reports are received at the DOE.~~

- NERC (ERO)
- FERC
- DOE
- DHS – Federal
- Homeland Security- State
- State Regulators
- Local Law Enforcement
- State Law Enforcement
- FBI

The above stakeholders have an interest in the timely notification, communication and response to an incident at an industry facility. The stakeholders have various levels of accountability and have a vested interest in the protection and response to ensure the reliability of the BES.

Present expectations of the industry under CIP-001:

It has been the understanding by industry participants that an occurrence of sabotage has to be reported to the FBI. The FBI has the jurisdictional requirements to investigate acts of sabotage and terrorism. The present CIP-001-1 standard requires a liaison relationship on behalf of the industry and FBI. Annual requirements, under the standard, of the industry have not been clear and have lead to misunderstandings and confusion in the industry as to how to demonstrate the liaison is in place and effective. FBI offices have been asked to confirm, on FBI letterhead, the existence of a working relationship to report acts of sabotage to include references to years the liaison has been in existence and confirming telephone numbers for the FBI.

Coordination of Local and State Law Enforcement Agencies with the FBI

The Joint Terrorism Task Force (JTTF) came into being with the first task force being established in 1980. JTTFs are small cells of highly trained, locally based, passionately committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. The JTTF is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. Coordination and communications largely through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs. This information flow can be most beneficial to the industry in analytical intelligence, incident response and investigation. Historically, the most immediate response to an industry incident has been local and state law enforcement agencies to suspected vandalism and criminal damages at industry facilities. Relying upon the JTTF coordination between local, state and FBI law enforcement would be beneficial to effective communications and the appropriate level of investigative response.

Coordination of Local and Provincial Law Enforcement Agencies with the RCMP

A similar law enforecment coordination hierarchy exists in Canada. Local and Provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. The Provincial

law enforcement agency has a reporting relationship with the Royla Canadian Mounted Police (RCMP).

A Reporting Process Solution – EOP-004

A proposal discussed with FBI, FERC Staff, NERC Standards Project Coordinator and SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Impact Event EOP-004-2). Essentially, reporting an Impact Event to law enforcement agencies will only require the industry to notify the state or provincial level law enforcement agency. The state or provincial level law enforcement agency will coordinate with local law enforcement to investigate. If the state or provincial level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial level law enforcement agency will notify and coordinate with the FBI or the RCMP.

Reporting Hierachy for Impact Event EOP-004-2

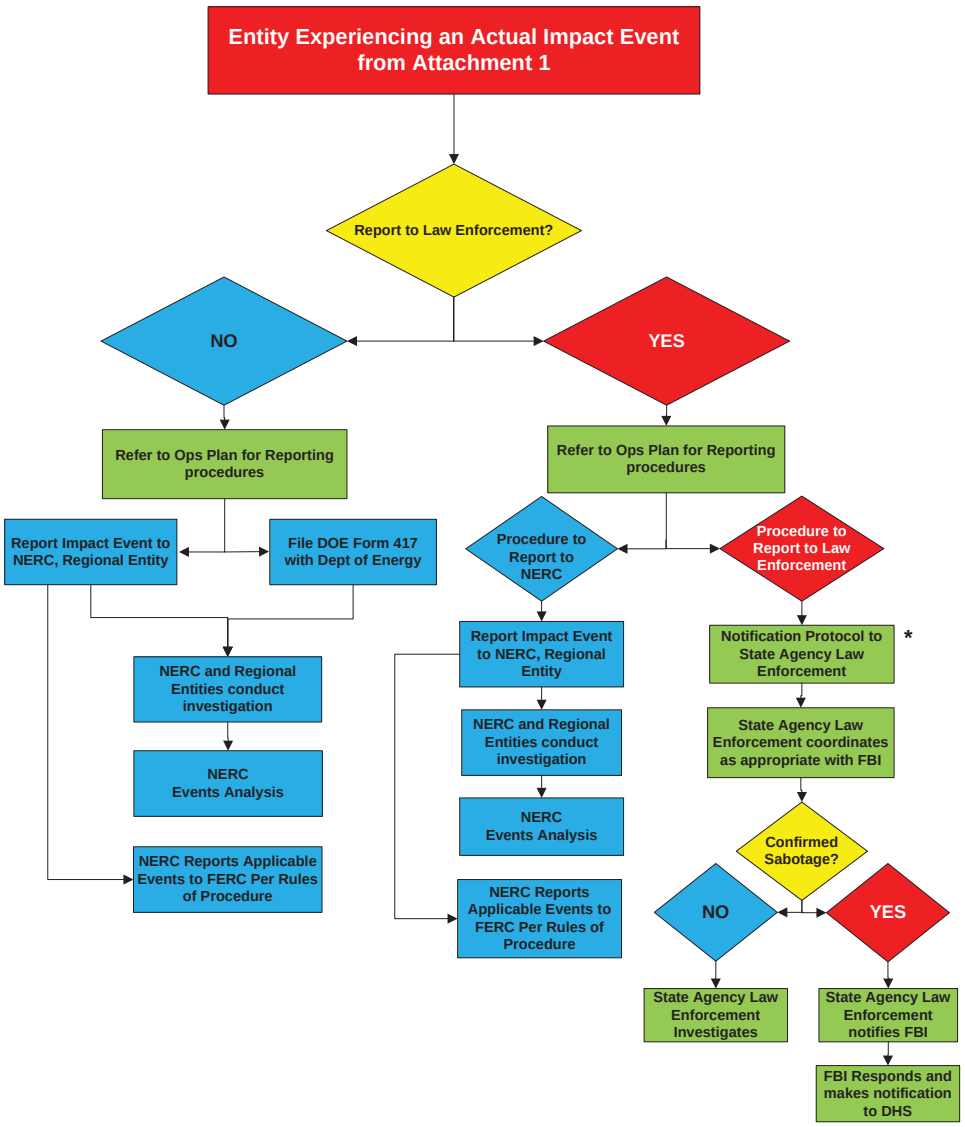

*Canadian entities will follow law enforcement protocols applicable in their jurisdictions

Requirements and Measures

R1. ~~The ERO shall establish, maintain and utilize a system for receiving and distributing impact event reports, received pursuant to Requirement R6, to applicable government, provincial or law enforcement agencies and Registered Entities to enhance and support situational awareness.~~

~~**M1.** The ERO shall provide evidence that it established, maintained and utilized a system for the distribution of the reports it receives to the various organizations or agencies. Such evidence could include, but is not limited to, dated records indicating that reports were distributed as shown on the submitted report or electronic logs indicating distribution of reports. (R1)~~

Rationale for R1

Every industry participant that owns or operates elements or devices on the grid has a formal or informal process, procedure, or steps it takes to gather information regarding what happened and why it happened when Impact Events occur. This requirement has the Registered Entity establish documentation on how that procedure, process, or plan is organized.

For the Impact Event Operating Plan, the DSR SDT envisions that Part 1.2 includes performing sufficient analysis and information gathering to be able to complete the report for reportable Impact Events. The main issue is to make sure an entity can a) identify when an Impact Event has occurred and b) be able to gather enough information to complete the report.

Part 1.3 could include a process flowchart, identification of internal positions to be notified and to make notifications, or a list of personnel by name as well as telephone numbers.

The Impact Event Operating Plan may include, but not be limited to, the following: how the entity is notified of event's occurrence, person(s) initially tasked with the overseeing the assessment or analytical study, investigatory steps typically taken, and documentation of the assessment / remedial action plan.

~~**R2.**~~ Each ~~Applicable~~Responsible Entity ~~identified in Attachment 1~~ shall have an Impact Event Operating Plan~~(s)~~ that includes: *[Violation Risk: Factor Medium] [Time Horizon: Long-term Planning]*

1.1. An Operating Process for identifying~~, assessing and reporting impact events~~ Impact Events listed in Attachment 1~~ that includes~~.

1.2. An Operating Procedure for gathering information for Attachment 2 regarding observed Impact Events listed in Attachment 1.

~~1.1.~~1.3. An Operating Process for communicating recognized Impact Events to the following~~ components~~:

~~1.2. Method(s) for identifying impact events~~

~~1.3. Method(s) for assessing cause(s) of impact events~~

~~1.4. Method(s) for making internal and external notifications pursuant to Parts 2.5 and 2.6~~

~~1.4.1.~~1.3.1. ~~List of internal~~Internal company personnel ~~responsible for making initial~~ notification(s~~) pursuant to Parts 2.5.and 2.6.~~).

~~1.5. List of internal company personnel to notify~~

~~1.5.1.~~1.3.2. ~~List of external~~External organizations to notify to include but not limited to ~~NERC,~~the Responsible Entities' Reliability Coordinator, NERC, Responsible Entities' Regional Entity, Law Enforcement, and Governmental or Provincial Agencies.

~~1.6.~~1.4. ~~Method~~Provision(s) for updating the Impact Event Operating Plan ~~when there is a component change~~ within ~~30~~90 days of ~~the notification of the~~any change~~.~~ to its content.

~~1.7. A provision for updating the Operating Plan based on lessons learned from an exercise or implementation of the Operating Plan within 30 days of identifying the lessons learned.~~

~~1.8. A provision for updating the Operating Plan based on applicable lessons learned from the annual NERC report issued pursuant to Requirement R8 within 30 days of NERC publishing lessons learned.~~

~~Rationale for R2~~

~~Every industry participant that owns or operates elements or devices on the grid has a formal or informal process, procedure, or steps it takes to assess what happened and why it happened when impact events occur. This requirement has the Registered Entity establish documentation on how that procedure, process, or plan is organized.~~

~~For the Operating Plan, the DSR SDT envisions that "assessing" includes performing sufficient analysis to be able to complete the report for reportable impact events. The main issue is to make sure an entity can a) identify when an impact event has occurred and b) be able to gather enough information to complete the report.~~

~~Parts 3.3 and 3.4 include, but not limited to, operating personnel who could be involved with any aspect of the operating plan.~~

~~The Operating Plan may include, but not be limited to, the following: how the entity is notified of event's occurrence, person(s) initially tasked with the overseeing the assessment or analytical study, investigatory steps typically taken, and documentation of the assessment / remedial action plan.~~

~~**M2**~~

M1. Each ~~Applicable~~Responsible Entity shall provide the current in force Impact Event Operating Plan to the Compliance Enforcement Authority~~ upon request. (R2)~~ .

~~**R3**~~

R2. Each ~~Applicable~~Responsible Entity shall ~~identify and assess initial probable cause of impact events listed in Attachment 1 in accordance with its~~implement its Impact Event Operating Plan documented in Requirement ~~R2.~~R1 for Impact Events listed in Attachment 1 (Parts A and B). *[Violation Risk: Factor Medium] [Time Horizon: Real-time Operations and Same-day Operations]*

~~**Rationale for R3**~~
~~The DSR SDT intends for each Applicable Entity to assess the causes of the reportable impact event and gather enough information to complete the report that is required to be filed.~~

~~**M3**~~**M2**. To the extent that an ~~Applicable~~Responsible Entity has an ~~impact event~~Impact Event on its Facilities, the ~~Applicable~~Responsible Entity shall provide documentation of ~~its assessment or analysis~~the implementation of its Impact Event Operating Plans. Such evidence could include, but is not limited to, operator logs, voice recordings, or ~~power flow analysis cases. (R3)~~other notations and documents retained by the Registered Entity for each Impact Event.

~~**R4**~~
R3. Each ~~Applicable~~Responsible Entity shall conduct a ~~drill, exercise, or Real-time implementation~~test of its Operating ~~Plan~~Process for ~~reporting~~communicating recognized Impact Events created pursuant to Requirement ~~R2~~R1, Part 1.3 at least annually, with no more than 15 calendar months between ~~exercises or~~tests. *[Violation Risk: Factor Medium] [Time Horizon: Long-term Planning]*

~~**Rationale for R4**~~
~~The DSR SDT intends for each Applicable Entity to conduct a drill or exercise of it Operating Plan as often as merited but no longer than 15 months from the previous exercise to prevent a long cycle of exercises (i.e., conducting an exercise in January of one year and then December of the next year). Multiple exercises in a 15 month period is not a violation of the requirement and would be encouraged to improve reliability. A drill or exercise may be a table-top exercise, a simulation or an actual implementation of the Operating Plan.~~

Ratic
The D
Entity
comm
correc
appro
Event
a drill
comm
often
such c
15 mo
actual
exerci
Opera
there
employment by March 31 of the next calendar year)). Multiple exercises in a 15 month period are not a violation of the requirement and would be encouraged to improve reliability.

M3. In the absence of an actual ~~use.~~ Impact Event, the Responsible Entity shall provide evidence that it conducted a mock Impact Event and followed its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The time period between actual and or mock Impact Events shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or documentation. (R3)

~~**M4.** The Applicable~~**R4.** Each Responsible Entity shall ~~provide evidence that it conducted a drill, exercise or Real-time implementation of the~~review its Impact Event Operating Plan ~~for reporting as specified in the requirement. Such evidence could include, but is not limited to, a dated, exercise scenario~~ with ~~notes on the exercise or operator logs, voice recordings, or power flow analysis cases for an actual implementation of the Operating Plan. (R4)~~

~~**R5.** Each Applicable Entity shall provide training to all internal~~ those personnel who have responsibilities identified in ~~its Operating Plan for reporting pursuant to Requirement R2 subject to the following:~~

~~5.1 The training includes the personnel required to respond and their required actions under the Operating Plan.~~

~~Training conducted~~that plan at least ~~once per calendar year,~~annually with no more than 15 calendar months between ~~training~~review sessions ~~for personnel with existing responsibilities.~~ *[Violation Risk: Factor Medium] [Time Horizon: Long-term Planning].*

~~5.2 If the Operating Plan is revised (with the exception of contact information revisions), training shall be conducted within 30 days of the Operating Plan revisions.~~

~~5.3 For internal personnel added to the Operating Plan or those with revised responsibilities under the Operating Plan, training shall be conducted prior to assuming the responsibilities in the plan.~~

~~**Rationale for R5**~~

~~The SDT is not prescribing how training is to be conducted and leaves that decision to each Applicable Entity as they best know how to conduct such activities. Conduct of an exercise constitutes training for compliance with this requirement.~~

~~For changes to the Operating Plan (5.3), the training may simply consist of a review of the revised responsibilities and a "sign-off" that personnel have reviewed the revisions.~~

~~**M5.** Applicable~~

M4. Responsible Entities shall provide the ~~actual training material~~materials presented to verify content and the association between the people listed in the plan and those who participated in the ~~training~~review, documentation showing who was ~~trained~~present and when internal personnel were trained on the responsibilities in the ~~Operating Plan as well as dates for personnel changes and evidence that the training was conducted following personnel changes. (R5)~~plan.

~~**R6**~~**R5**. Each ~~Applicable~~Responsible Entity shall report ~~impact events~~Impact Events in accordance with ~~its~~the Impact Event Operating Plan ~~created~~ pursuant to Requirement ~~R2~~R1 and Attachment 1 using the ~~timelines outlined~~form in Attachment ~~1.~~2 or the DOE OE-417 reporting form. *[Violation Risk: Factor: Medium] [Time Horizon: Real-time Operations and Same-day Operations].*

~~**M6.** Registered~~**M5.** Responsible Entities shall provide evidence demonstrating the submission of reports using the ~~Operating Plan~~plan created pursuant to Requirement ~~R2 for impact events~~R1 and Attachment 1 using either the form in Attachment 2 or the DOE OE-417 report. Such evidence will include a copy of the ~~original impact event~~Attachment 2 form or OE-417 report submitted, evidence to support the type of ~~impact event~~Impact Event

experienced; the date and time of the ~~impact event~~ Impact Event; as well as evidence of report submittal that includes date and time. ~~(R6)~~

~~**R7.** The ERO shall annually review and propose revisions to the impact event table (Attachment 1) if warranted based on its analysis of reported impact events. Revisions to Attachment 1 shall follow the Reliability Standards Development Procedure.~~

~~**M7.** The ERO shall provide evidence that it reviewed the impact event table. If applicable, the ERO shall provide evidence that it followed the Reliability Standards Development Procedure to propose and implement revisions to Attachment 1. Such evidence may include, but not be limited to, documentation that compares or assesses the list of impact events (Attachment 1) against the analysis of reported impact events. (R7)~~

~~**Rationale for R7-R8**~~

~~Some of the concepts contained in Requirements R7 and R8 are contained in the NERC Rules of Procedure, section 800. The DSR SDT felt that, in order to have a complete standard for reporting impact events that improved reliability, there needed to be feedback to industry on a regular basis as well as when issues are discovered. The analysis of impact events is crucial and the subsequent dissemination of the results of that analysis must be performed.~~

~~In accordance with Sections 401(2) and 405 of the Rules of Procedures, the ERO can be set as an applicable entity in a requirement or standard. After careful consideration, the DSR SDT believes that these requirements (R7-8) are best applicable to the ERO.~~

~~**R8.** The ERO shall publish a quarterly report of the year's reportable impact events subject to the following:~~

~~8.1 Issued no later than 30 days following the end of the calendar quarter~~

~~8.2 Identifies trends on the BES~~

~~8.3 Identifies threats to the BES~~

~~8.4 Identifies other vulnerabilities to the BES~~

~~8.5 Documents lessons learned~~

~~8.6 Includes recommended actions.~~

~~**Rationale for R8**~~

~~The ERO will analyze Impact Events that are reported through requirement R6. The DSR SDT envisions the ERO issuing reports identifying trends, threats or other vulnerabilities when available or at least quarterly. The report will include lessons learned and recommended actions (such as mitigation plans) to improve reliability as applicable.~~

~~**M8.** The ERO shall provide evidence that it issued a report identifying trends, threats, or other vulnerabilities on the bulk electric system at least quarterly. Such evidence will include a copy of the report as well as dated evidence of the report's issuance. (R8)~~

Compliance

Compliance Enforcement Authority

- Regional Entity; or
- ~~For requirements applicable to the ERO, an entity contracted to perform an audit.~~
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.

Compliance Monitoring and Enforcement Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

Evidence Retention

Each ~~Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator and Distribution Provider~~Responsible Entity shall ~~keep~~retain data or evidence ~~to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:~~

~~The ERO shall retain evidence of Requirements 1, 7 and 8, Measures 1, 7, and 8~~ for three calendar years~~.~~

~~Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator and Distribution Provider shall retain data~~ or ~~evidence of Requirements 2, 3, 4, and 5 and Measures 2, 3, 4, and 5 for three calendar years~~ for the duration of any regional or Compliance Enforcement Authority investigation~~,~~; whichever is longer ~~to show compliance unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation~~.

~~Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator and Distribution Provider shall retain data or evidence of Requirement 6 and Measure 6 for three calendar years for the duration of any regional investigation, whichever is longer to show compliance unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.~~

If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

Additional Compliance Information

~~To be determined~~.

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Medium	The Responsible Entity has an Impact Event Operating Plan but failed to include one of Parts 1.1 through 1.4.	The Responsible Entity has a Impact Event Operating Plan but failed to include two of Parts 1.1 through 1.4.	The Responsible Entity has an Impact Event Operating Plan but failed to include three of Parts 1.1 through 1.4.	The Responsible Entity failed to include all of Parts 1.1 through 1.4.
R2	Real-time Operations and Same-day Operations	Medium	N/A	N/A	N/A	The Responsible Entity failed to implement its Impact Event Operating Plan for an Impact Event listed in Attachment 1.
R3	Long-term Planning	Medium	The Responsible Entity failed to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to	The Responsible Entity failed to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to	The Responsible Entity failed to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to	The Responsible Entity failed to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to

			Requirement R1, Part 1.3 in more than 15 months but less than 18 months.	Requirement R1, Part 1.3in more than 18 months but less than 21 months.	Requirement R1, Part 1.3 in more than 21 months but less than 24 months.	Requirement R1, Part 1.3 in more than 24 months
R4	Long-term Planning	Medium	The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan l in more than 15 months but less than 18 months.	The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 18 months but less than 21 months.	The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 21 months but less than 24 months.	The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 24 months
R5	Real-time Operations and Same-day Operations	Medium	The Responsible Entity failed to submit a report in less than 36 hours for an Impact Event requiring reporting within 24 hours in Attachment 1.	The Responsible Entity failed to submit a report in more than 36 hours but less than or equal to 48 hours for an Impact Event requiring reporting within 24 hours in Attachment 1.	The Responsible Entity failed to submit a report in more than 48 hours but less than or equal to 60 hours for an Impact Event requiring reporting within 24 hours in Attachment 1. OR The Responsible Entity failed to submit a report in more than 1 hour but less than 2 hours for an Impact Event requiring reporting within 1 hour	The Responsible Entity failed to submit a report in more than 60 hours for an Impact Event requiring reporting within 24 hours in Attachment 1. OR The Responsible Entity failed to submit a report in more than 2 hours for an Impact Event requiring reporting within 1 hour in Attachment 1. OR The responsible entity

					in Attachment 1.	failed to submit a report for an Impact Event in Attachment 1.

Variances

None

Interpretations

None

EOP-004 - Attachment 1: Impact Events Table

NOTE: Under certain adverse conditions, e.g.~~,~~, severe weather, it may not be possible to ~~assess~~report the damage caused by an ~~impact event~~Impact Event and issue a written Impact Event Report within the timing in the table below. In such cases, the affected ~~Applicable~~Responsible Entity shall notify its Regional Entity(ies) and NERC, ~~and verbally~~ (e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422) and provide as much information as is available~~ at that time.~~. The affected ~~Applicable~~Responsible Entity shall then provide periodic verbal updates until adequate information is available to issue a written ~~Preliminary~~ Impact Event ~~Report~~report.

EOP-004 – Attachment 1 - Actual Reliability Impact – Part A			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Time to Submit Report**
Energy Emergency requiring Public appeal for load reduction	~~RC, BA~~Initiating entity is responsible for reporting	~~To reduce consumption in order to maintain the continuity of the BES~~ Each public appeal for load reduction	Within 1 hour of issuing a public appeal
Energy Emergency requiring system-wide voltage reduction	~~RC, TO, TOP, DP~~ Initiating entity is responsible for reporting	System wide voltage reduction of 3% or more	Within 1 hour after ~~occurrence~~event is ~~identified~~initiated
Energy Emergency requiring manual firm load shedding	Initiating entity is responsible for reporting	Manual firm load shedding ≥ 100 MW	Within 1 hour after event is initiated
Energy Emergency ~~requiring~~resulting in automatic firm load shedding	~~RC, BA, TOP, DP~~ Each DP or TOP that experiences the Impact Event	Firm load shedding ≥ 100 MW (~~manually or~~ via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)	Within ~~24 hours~~1 hour after ~~occurrence~~event is initiated
Voltage Deviations on BES Facilities	Each RC, TOP, GOP that experiences the Impact Event	± 10% sustained for ≥ 15 continuous minutes	Within 24 hours after 15 minute threshold
~~Frequency Deviations~~	~~RC, BA~~	~~± Deviations ≥ than Frequency Trigger Limit (FTL) more than 15 minutes~~	~~Within 24 hours after 15 minute threshold~~
IROL Violation	Each RC, TOP that experiences the Impact Event	Operate outside the IROL for time greater than IROL Tv	Within 24 hours after Tv threshold

EOP-004 – Attachment 1 - Actual Reliability Impact – Part A			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Time to Submit Report**
Loss of Firm load for ≥ 15 Minutes	Each RC, BA, ~~TO,~~ TOP, DP that experiences the Impact Event	• ≥ 300 MW for entities with previous year's demand ≥ 3000 MW • ≥ 200 MW for all other entities	Within ~~24 hours~~1 hour after 15 minute threshold
System Separation (Islanding)	Each RC, BA, TOP, DP that experiences the Impact Event	Each separation resulting in an island of generation and load ≥ 100 MW	Within 1 hour after occurrence is identified
Generation loss	Each RC, BA, ~~GO,~~ GOP that experiences the Impact Event	• ≥ 2,000 MW for entities in the Eastern or Western Interconnection • ≥ 1000 MW for entities in the ERCOT or Quebec Interconnection • ~~An entire generating station of ≥ 5 generators with aggregate capacity of ≥ 500 MW~~	Within 24 hours after occurrence
Loss of Off-site power to a nuclear generating plant (grid supply)	Each RC, BA, TO, TOP, GO, GOP that experiences the Impact Event	Affecting a nuclear generating station per the Nuclear Plant Interface Requirement	Report within 24 hours after occurrence
Transmission loss	Each RC, ~~TO,~~ TOP that experiences the Impact Event	• ~~An entire DC converter station~~ ~~Multiple BES transmission elements (simultaneous or common-mode event)~~Three or more BES Transmission Elements	Within 24 hours after occurrence
Damage or destruction of BES ~~equipment~~[1]equipment[1]	Each RC, BA, TO, TOP, GO, GOP, DP that experiences the Impact Event	Through operational error, equipment failure, ~~or~~ external cause, or intentional or unintentional human action.	Within 1 hour after occurrence is identified

[1]BES equipment that: i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii) Damaged or destroyed due to intentional or unintentional human action; or iv) Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly e.g., removal of grounding straps rendering protective relaying inoperative.

EOP-004 – Attachment 1 - Actual Reliability Impact – Part A			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Time to Submit Report**
Damage or destruction of Critical Asset	Applicable Entities under CIP-002 or its successor.	Through operational error, equipment failure, external cause, or intentional or unintentional human action.	Within 1 hour after occurrence is identified
Damage or destruction of a Critical Cyber Asset	Applicable Entities under CIP-002 or its successor.	Through intentional or unintentional human action.	Within 1 hour after occurrence is identified

~~**Examples:**~~

~~a. BES equipment that is:~~

~~i. A critical asset~~

~~ii. Affects an IROL~~

~~iii. Significantly affects the reliability margin of the system e.g., has the potential to result in the need for emergency actions~~

~~iv. Damaged or destroyed due to a non-environmental external cause~~

~~Report copper theft from BES equipment only if it degrades the ability of equipment to operate correctly e.g., removal of grounding straps rendering protective relaying ineffective~~

EOP-004 – Attachment 1 - Potential Reliability Impact – Part B			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Time to Submit Report**
Unplanned Control Center evacuation	Each RC, BA, TOP that experiences the potential Impact Event	Unplanned evacuation from BES control center facility	~~report~~Report within ~~1~~24 hour after occurrence
Fuel supply emergency	Each RC, BA, GO, GOP that experiences the potential Impact Event	Affecting BES ~~reliability[1]~~reliability[2]	~~report~~Report within 1 hour after occurrence
~~Loss of off-site power (grid supply)~~	~~RC, BA, TO, TOP, GO, GOP~~	~~Affecting a nuclear generating station~~	~~report within 1 hour after occurrence~~
Loss of all monitoring or voice communication capability	Each RC, BA, TOP that experiences the potential Impact Event	Affecting a BES control center for ≥ 30 continuous minutes	~~report~~Report within ~~1 hour~~24 hours after occurrence
Forced ~~intrusion[2]~~intrusion[3]	Each RC, BA, TO, TOP, GO, GOP that experiences the	At a BES facility	~~report~~Report within ~~24 hours~~1 hour after ~~occurrence~~verification of intrusion

[2] Report if problems with the fuel supply chain result in the projected need for emergency actions to manage reliability.

[3] Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects the reliability of the BES).

	potential Impact Event		
Risk to BES ~~equipment[3]~~equipment[4]	Each RC, BA, TO, TOP, GO, GOP, DP that experiences the potential Impact Event	From a non-environmental physical threat	~~report~~Report within ~~24 hours~~1 hour after ~~occurrence~~identification
Detection of a ~~cyber intrusion to critical cyber assets~~reportable Cyber Security Incident.	Each RC, BA, TO, TOP, GO, GOP, DP that experiences the potential Impact Event	That meets the criteria in CIP-008 (or its successor)	~~report~~Report within ~~24 hours~~1 hour after ~~occurrence~~detection

~~1. Report if problems with the fuel supply chain result in the projected need for emergency actions to manage reliability.~~
~~2. Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects the reliability of the BES).~~

~~Examples include a train derailment adjacent to BES equipment, that either could have damaged the equipment directly or has the potential to damage the equipment (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center).~~

[4] Examples include a train derailment adjacent to BES equipment, that either could have damaged the equipment directly or has the potential to damage the equipment (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center) and report of suspicious device near BES equipment).

EOP-~~002~~004 - Attachment 2: Impact Event Reporting Form

This form is to be used to report Impact Events to the ERO. NERC will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Reports should be submitted via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550

~~EOP-004 – Confidential~~ Impact Event ~~Report~~Reporting for EOP-004-2		
	Task	**Comments**
1.	Entity filing the report (include company name and Compliance Registration ID number):	
2.	Date and Time of ~~impact event~~Impact Event. Date: (mm/dd/~~yy~~yyyy) Time/Zone:	
3.	Name of contact person: Email address: Telephone Number:	
4.	Did the ~~impact event~~actual or potential Impact Event originate in your system?	Actual Impact Event ☐ Potential Impact Event ☐ Yes ☐ No☐ Unknown ☐
5.	Under which NERC function are you reporting? (RC, TOP, BA, other)	

Formatted Table

~~EOP-004 – Confidential~~ Impact Event ~~Report~~Reporting for EOP-004-2			
	Task	Comments	
6.	Brief Description of ~~impact event~~actual or potential Impact Event: (More detail should be provided in the Sequence of Events section below.)		
7.	Generation tripped off-line~~.~~*. MW Total List units tripped		
8.	Frequency~~.~~*. Just prior to ~~impact event~~Impact Event (Hz): Immediately after ~~impact event~~Impact Event (Hz max): Immediately after ~~impact event~~Impact Event (Hz min):		
9.	List transmission facilities (lines, transformers, buses, etc.) tripped and locked-out~~.~~*. (Specify voltage level of each facility listed).		
10.	Demand tripped (MW~~):~~)*:	FIRM	INTERRUPTIBLE

Formatted Table

~~EOP-004 – Confidential~~ Impact Event ~~Report~~Reporting for EOP-004-2			
	Task	Comments	
	Number of affected customers~~:~~*: Demand lost (MW-Minutes~~):~~)*:		
11.	Restoration Time~~.~~*.	INITIAL	FINAL
	Transmission:		
	Generation:		
	Demand:		
12.	~~Sequence of Events:~~ Sequence of Events of actual or potential Impact Event (if potential Impact Event, please describe your assessment of potential impact to BES) :		

Formatted Table

~~EOP-004 – Confidential~~ Impact Event ~~Report~~Reporting for EOP-004-2		
	Task	**Comments**
13.	Identify the initial probable cause or known root cause of the ~~impact event~~actual or potential Impact Event if known at time of submittal of Part I of this report:	
14.	Identify any protection system misoperation(s~~):~~)[1]:	
15.	Additional Information that ~~the~~ helps to further explain the ~~event~~actual or potential Impact Event if needed. ~~A one-line diagram may be attached, if readily available, to assist in the evaluation of the event.:~~	

Formatted Table

[1] Only applicable if it is part of the impact event the responsible entity is reporting on

~~EOP-004 – Confidential~~ Impact Event ~~Report~~Reporting for EOP-004-2		
	Task	Comments

Formatted Table

Guideline and Technical Basis

Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01) - Reporting Concepts

Introduction

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and is progressing toward developing standards based on the SAR. This concepts paper is designed to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed.

The standards listed under the SAR are:

- CIP-001 — Sabotage Reporting
- EOP-004 — Disturbance Reporting

The DSR SDT also proposed to investigate incorporation of the cyber incident reporting aspects of CIP-008 under this project. This will be coordinated with the Cyber Security - Order 706 SDT (Project 2008-06).

The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC database and FERC Order 693 Directives to determine a prudent course of action with respect to these standards.

This concept paper provides stakeholders with a proposed “road map” that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. This concept paper provides the background information and thought process of the DSR SDT.

The proposed changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). The proposed standards deal exclusively with after-the-fact reporting.

The DSR SDT is proposing to consolidate disturbance and event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts and Assumptions:

The Standard Will: Require use of a single form to report disturbances and "~~impact events~~Impact Events" that threaten the reliability of the bulk electric system

- Provide clear criteria for reporting
- Include consistent reporting timelines
- Identify appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- Provide clarity around of who will receive the information

The drafting team will explore other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements

Discussion of Disturbance Reporting
Disturbance reporting requirements currently exist in EOP-004. The current approved definition of Disturbance from the NERC Glossary of Terms is:

1. An unplanned event that produces an abnormal system condition.
2. Any perturbation to the electric system.
3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.

Disturbance reporting requirements and criteria are in the existing EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and developed the list of ~~impact events~~Impact Events that are to be reported under this standard (attachment 1).

Discussion of "~~impact event~~Impact Event" Reporting
There are situations worthy of reporting because they have the potential to impact reliability. The DSR SDT proposes calling such incidents '~~impact events~~'Impact Events' with the following concept:

> An ~~impact event~~Impact Event is any situation that has the potential to significantly impact the reliability of the Bulk Electric System. Such events may originate from malicious intent, accidental behavior, or natural occurrences.

Impact ~~event~~Event reporting facilitates ~~situational~~industry awareness, which allows potentially impacted parties to prepare for and possibly mitigate the reliability risk. It also provides the raw material, in the case of certain potential reliability threats, to see emerging patterns.

Examples of ~~impact events~~Impact Events include:

- Bolts removed from transmission line structures
- Detection of cyber intrusion that meets criteria of CIP-008 or its successor standard
- Forced intrusion attempt at a substation

- Train derailment near a transmission right-of-way
- Destruction of Bulk Electrical System equipment

What about sabotage?
One thing became clear in the DSR SDT's discussion concerning sabotage: everyone has a different definition. The current standard CIP-001 elicited the following response from FERC in FERC Order 693, paragraph 471 which states in part: *". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."*

Often, the underlying reason for an event is unknown or cannot be confirmed. The DSR SDT believes that reporting material risks to the Bulk Electrical System using the ~~impact event~~Impact Event categorization, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.

The DST SDT discussed the reliability needs for ~~impact event~~Impact Event reporting and will consider guidance found in the document "NERC Guideline: Threat and Incident Reporting" in the development of requirements, which will include clear criteria for reporting.

Certain types of ~~impact events~~Impact Events should be reported to NERC, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and/or Provincial or local law enforcement. Other types of ~~impact events~~Impact Events may have different reporting requirements. For example, an ~~impact event~~Impact Event that is related to copper theft may only need to be reported to the local law enforcement authorities.

Potential Uses of Reportable Information
Event analysis, correlation of data, and trend identification are a few potential uses for the information reported under this standard. As envisioned, the standard will only require Functional entities to report the incidents and provide information or data necessary for these analyses. Other entities (e.g. – NERC, Law Enforcement, etc) will be responsible for performing the analyses. The NERC Rules of Procedure (section 800) provide an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for reliability. Jurisdictional agencies (which may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE) have other duties and responsibilities.

Collection of Reportable Information or "One stop shopping"
The goal of the DSR SDT is to have one reporting form for all functional entities (US, Canada, Mexico) to submit to NERC. Ultimately, it may make sense to develop an electronic version to expedite completion, sharing and storage. Ideally, entities would complete a single form which could then be distributed to jurisdictional agencies and functional entities as appropriate. Specific reporting forms[6] that exist today (i.e. - OE-417, etc) could be included as part of the

[6] The DOE Reporting Form, OE-417 is currently a part of the EOP-004 standard. If this report is removed from the standard, it should be noted that this form is still required by law as noted on the form: NOTICE: This report is mandatory under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other

electronic form to accommodate US entities with a requirement to submit the form, or may be removed (but still be mandatory for US entities under Public Law 93-275) to streamline the proposed consolidated reliability standard for all North American entities (US, Canada, Mexico). Jurisdictional agencies may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE. Functional entities may include the RC, TOP, and BA for ~~situational~~industry awareness. Applicability of the standard will be determined based on the specific requirements.

The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT is planning to update the listing of reportable events from discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences may still exist.

The reporting proposed by the DSR SDT is intended to meet the uses and purposes of NERC. The DSR SDT recognizes that other requirements for reporting exist (e.g., DOE-417 reporting), which may duplicate or overlap the information required by NERC. To the extent that other reporting is required, the DSR SDT envisions that duplicate entry of information is not necessary, and the submission of the alternate report will be acceptable to NERC so long as all information required by NERC is submitted. For example, if the NERC Report duplicates information from the DOE form, the DOE report may be included or attached to the NERC report, in lieu of entering that information on the NERC report.

sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. Title 18 USC 1001 makes it a criminal offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction.

Unofficial Comment Form for Disturbance and Sabotage Reporting (Project 2009-01)

Please **DO NOT** use this form to submit comments. Please use the electronic comment form located at the link below to submit comments on the Second Posting of EOP-004-2, Impact Event Reporting (Project 2009-01). The electronic comment form must be completed by **April 8, 2011.**

Project 2009-01 Disturbance and Sabotage Reporting

If you have questions please contact Stephen Crutchfield at Stephen.Crutchfield@nerc.net or by telephone at 609-651-9455.

Background Information

The Disturbance and Sabotage Reporting Drafting Team posted the first draft of EOP-004-2 – Impact Event Reporting for a 30-day informal comment period from September 15, 2010 through October 15, 2010. Based on stakeholder comments, and also on the results of the observations made by the Quality Review team, the drafting team made the following significant changes to the standard following the posting period that ended on October 15, 2011.

Scope: A common thread through most of the comments was that the DSR SDT went beyond the reliability intent of the standard (reporting) and concentrated too much on the analysis of the event. The DSR SDT agrees with this response, and revised the purpose as follows:

> *Original Purpose:* Responsible Entities shall report impact events and their known causes to support situational awareness and the reliability of the Bulk Electric System (BES).
>
> *Revised Purpose:* To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of Impact Events and their causes, if known, by the Responsible Entities.

Definitions:

Impact Event: The DSR SDT had proposed a working definition for "impact events" to support EOP-004 - Attachment 1 as follows:

> "An impact event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action."

Many stakeholders indicated that the definition should be added to the NERC Glossary and the DSR SDT adopted this suggestion. The types of Impact Events that are required to be reported are contained within EOP-004 - Attachment 1. *Only the events identified in EOP-004 – Attachment 1 are required to be reported under this Standard.*

Sabotage:

FERC Order 693, paragraph 471 states in part: ". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event." The DSR SDT made a conscious, deliberate decision to exclude a strict definition of sabotage from this standard and sought stakeholder feedback on this issue. Some suggested adopting the NRC

definition of the term sabotage, and the DSR SDT did consider adopting the NRC definition shown below but determined that the definition is too narrowly focused.

> Any deliberate act directed against a plant or transport in which an activity licensed pursuant to 10 CFR Part 73 of NRC's regulations is conducted or against a component of such a plant or transport that could directly or indirectly endanger the public health and safety by exposure to radiation.

Most respondents agreed that in order to be labeled as an act of sabotage, the intent of the perpetrators must be known. The team felt that it was almost impossible to determine if an act or event was that of sabotage or merely vandalism without the intervention of law enforcement after the fact. This would result in further ambiguity with respect to reporting events, and the timeline associated with the reporting requirements does not lend itself to the in-depth analysis required to identify a disturbance (or potential disturbance) as sabotage. The SDT felt that a likely consequence of having to meet this criterion, in the time allotted, would be an under-reporting of events. Accordingly, all references to sabotage have been deleted from the standard. Instead, the SDT concentrated on providing clear guidance on the events that should trigger a report. The SDT believes that this more than adequately meets the reliability intent of the Commission as expressed in paragraph 471 of Order 693 in an equally efficient and effective manner.

Situational Awareness versus Industry Awareness: Some commenters correctly pointed out that “situational awareness” is a desirable by-product of an effective event reporting system, and not the driver of that system. Accordingly, all references to “situational awareness” have been deleted from the standard. The more generic “industry awareness” has been substituted where appropriate.

Applicability: The DSR SDT had protracted discussions on the applicability of this standard to the LSE. Per the Functional Model, the LSE does not own assets and therefore should not be an applicable entity (no equipment that could experience a “disturbance”). However, the Registry Criteria contains language that could imply that the LSE does own assets, or is at least responsible for assets. In addition, the DSR SDT modified Attachment 1 to include reporting of damage or destruction of Critical Cyber Assets per CIP-002. The LSE, as well as the Interchange Authority and Transmission Service Provider are applicable entities under CIP-002 and should be included for Impact Events under EOP-004.

There were several comments that the asset owners (GO/TO) would be less likely than the asset operators (GOP/TOP) to be aware of an impact event. The DSR SDT recognizes that this may be true in some cases, but not all. In order to meet the reliability objectives of this requirement, the applicability for GO/TO will remain as per Attachment 1.

Requirement R1: Based on stakeholder comments, Requirement R1, which assigned the ERO the responsibility for collecting and distributing impact event reports was deleted. There was strong support for a central system for receiving and distributing impact event reports (“one stop shopping”). There was general agreement that NERC was the most likely, logical entity to perform that function. However several respondents expressed their concern that the ERO could not be compelled to do so by a requirement in a Reliability Standard (not a User, Owner or Operator of the BES). In their own comments, NERC did not oppose the concept, but suggested that the more appropriate place to assign this responsibility would be the NERC Rules of Procedure. The DSR SDT concurs. The DSR SDT has removed the requirement from the standard and is proposing to make revisions to the NERC Rules of Procedure as follows:

> 812. NERC will establish a system to collect impact event reports as established for this section, from any Registered Entities, pertaining to data requirements identified in Section 800 of this Procedure. Upon receipt of the submitted report, the system shall then forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, and regulatory agencies as necessary. These reports shall be forwarded to the Federal Energy Regulatory Commission for impact events that occur in the United States. The ERO shall solicit contact information from Registered Entities appropriate governmental, law enforcement and regulatory agencies for distributing reports.

Requirement R2 (now R1 in the revised standard)
There were objections to the use of the term "Operating Plan" to describe the procedure to identify and report the occurrence of a disturbance. The DSR SDT believes that the use of a defined term is appropriate and has revised Requirement R1 to include Operating Plan, Operating Process and Operating Procedure.

Many commenters felt that the requirements around updating the Operating Plan were too prescriptive, and impossible to comply with during the time frame allowed. The DSR SDT agrees, and Requirement R2, Parts 2.5 through 2.9 have been eliminated. They have been replaced with Requirement R1, Part 1.4 to require updating the Impact Event Operating Plan within 90 days of any change to content.

R1. Each Responsible Entity shall have an Impact Event Operating Plan that includes: *[Violation Risk: Factor Medium] [Time Horizon: Long-term Planning]*:

1.1. An Operating Process for identifying Impact Events listed in Attachment 1.

1.2. An Operating Procedure for gathering information for Attachment 2 regarding observed Impact Events listed in Attachment 1.

1.3. An Operating Process for communicating recognized Impact Events to the following:

1.3.1 Internal company personnel notification(s).

1.3.2. External organizations to notify to include but not limited to the Responsible Entities' Reliability Coordinator, NERC, Responsible Entities' Regional Entity, Law Enforcement, and Governmental or Provincial Agencies.

1.4. Provision(s) for updating the Impact Event Operating Plan within 90 days of any change to its content.

Other requirements reference the Operating Plan as appropriate. The requirements of EOP-004-2 fit precisely into the definition of Operating Plan:

> Operating Plan: A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan.

Requirement R3: Requirement R3 (now R2 in the revised standard) has been re-written to exclude the requirement to "assess the initial probable cause". The only remaining reference to "cause" is in the Impact Event Reporting Form (Attachment 2). Here, there is no longer a requirement to assess the probable cause. The probable cause only needs to be identified, and only if it is known at the time of the submittal of the report.

R2. Each Responsible Entity shall implement its Impact Event Operating Plan documented in Requirement R1 for Impact Events listed in Attachment 1 (Parts A and B).

Requirement R4: (Now R3 in the revised standard.) The DSR SDT did a full review based on comments that were received. R3 now is stream lined to read:

R3. Each Responsible Entity shall conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 at least annually, with no more than 15 months between such tests.

The testing of the Operating Process for communicating recognized Impact Events (as stated in R1) is the main component of this requirement. Several commenters provided input that too much "how" was previously within R3 and the DSR DST should only provide the "what". The DSR SDT did not provide any prescriptive guidance on how to accomplish the required testing within the rewrite. Testing of the entity's procedure (R1) could be by an actual exercise of the process (testing as stated in FERC Order 693 section 471), a formal review process or real time implementation of the procedure. The DSR SDT reviewed Order 693 and section 465 directs, with respect to processes, that entities "verify that they achieve the desired result". This is the basis of R3, above.

Requirement R5: Note R5 has been moved to R4 due to rearranging of requirements. The DSR SDT did a full review based on comments that were received. The major issues that were provided by commenters involved the inclusion of Requirement R5, Part 5.3 and Part 5.4.

5.3 If the Operating Plan is revised (with the exception of contact information revisions), training shall be conducted within 30 days of the Operating Plan revisions.

5.4 For internal personnel added to the Operating Plan or those with revised responsibilities under the Operating Plan, training shall be conducted prior to assuming the responsibilities in the plan.

Upon detailed review the DSR SDT agrees with the majority of comments received regarding Requirement R5, Parts 5.3 and 5.4 and has removed Parts 5.3 and 5.4 completely from the Standard. Training is still the main theme of this requirement (now R4) as it pertains to the personnel required to implement the Impact Event Operating Plan (R1). R4 now is stream lined to read:

R4. Each Responsible Entity shall review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan at least annually with no more than 15 calendar months between review sessions.

Requirement R6: Note R6 been moved to R5 due to rearranging of requirements. The DSR SDT did a full review based on comments that were received. Many comments received identified concerns on the reporting time lines within Attachment 1. Several commenters wanted the ability to report impact events to their responsible parties via the DOE Form OE-417. Upon discussions with the DOE and NERC, the DSR SDT has added the ability to use the DOE Form OE-417 when the same or similar items are required to be reported to NERC and the DOE. This will reduce the need to file multiple forms when the same or similar events must be reported to the DOE and NERC. The reliability intent of reporting impact events within prescribed guidelines, to provide industry awareness and to

start any required analysis processes can be met without duplicate reporting. R5 now is stream lined to read:

> R5. Each Responsible Entity shall report Impact Events in accordance with its Impact Event Operating Plan pursuant to Requirement R1 and Attachment 1 using the form in Attachment 2 or the DOE OE-417 reporting form.

Requirements R7 and R8: The DSR SDT did a full review based on comments that were received. The DSR SDT has determined that R7 and R8 are not required to be within a NERC Standard since Section 800 of the Rules of Procedure already assigns this responsibility to NERC.

Attachment 1: The DSR SDT did a full review based on comments that were received. The DSR SDT, the Events Analysis Working Group (EAWG), NERC Staff (to include NERC Senior VP and Chief Reliability Officer) had an open discussion involving this topic. The EAWG and the DSR SDT aligned Attachment 1 with the Event Analysis Program category 1 analysis responsibilities. This will assure that impact events in EOP-004-2 reporting requirements are the starting vehicle for any required Event Analysis within the NERC Event Analysis Program. The DSR SDT reviewed the "hierarchy" of reporting within Attachment 1. To reduce multiple entities reporting the same impact event, the DSR SDT has stated that the entity that performs the action or is directly affected by an action will report per EOP-004-2. As an example, during a system emergency, the TOP or RC may request manual load shedding by a DP or TOP. The DP or TOP would have the responsibility to report the action that it took if it meets or exceeds the bright-line criteria established in Attachment 1. Upon reporting, the NERC Event Analysis Program would be made aware of the impact event and start the Event Analysis Process which is outside the scope of this Standard. Several bright-line criteria were removed from Attachment 1. These criteria (DC converter station, 5 generator outages, and frequency trigger limits) were removed after discussions with the EAWG and NERC staff, who concurred that these items should be removed from a reporting standard and analysis process.

Several respondents expressed concern that the reporting requirements were redundant. The general sentiment was that unclear responsibility to report a disturbance could trigger a flood of event reports. Attachment 1 has been modified to assign clear responsibility for reporting, for each category of Impact Event.

Some commenters indicated a concern that the list of events in Attachment 1 isn't as comprehensive as the existing standard since the existing standard includes bomb threats and observations of suspicious activities. Others commented that the impact event list should include deliberate acts against infrastructure. The DSR SDT believes that "observation of suspicious activity" and "bomb threats" are addressed in Attachment 1 Part B – "Risk to BES equipment from a non-environmental physical threat". The SDT has added the phrase, "and report of suspicious device near BES equipment" to note 3 of the "Attachment 1, Potential Reliability – Part B" for additional clarity.

Attachment 2: The proposed Impact Event Report (Attachment 2) generated comments regarding the duplicative nature of the form when compared to the OE-417. The DSR SDT has added language to the proposed form to clarify that NERC will accept a DOE OE-417 form in lieu of Attachment 2 if the responsible entity is required to submit an OE-417 form. In collaboration with the NERC Event Analysis Working Group (EAWG) the DSR SDT modified the attachment to eliminate confusion. This revised form will be Attachment 2 of the Standard and collects the only information required to be reported for EOP-004-2.

Further information may be requested through the Events Analysis Process (NERC Rules of Procedure), but the collection of this information is outside of the scope of EOP-004.
The DSR SDT has also clarified the form's purpose with the following addition to the form:

"This form is to be used to report impact events to the ERO."

Other Standard Issues:
The DSR SDT proposed that combining EOP-004 and CIP-001 would not introduce a reliability gap between the existing standards and the proposed standard and the industry comments received confirms this.

Several entities expressed their concern with the fact that Attachment 1 contained most of the elements already called for in the OE-417. The DSR SDT agrees, and Attachment 1 part 1 has been modified to even more closely mirror the Department of Energy's OE-417 Emergency Incident and Disturbance Report form. Additionally, the standard has been modified to allow for the use of the OE-417.

There was some concern expressed that there could be confusion between the reporting requirements in this standard, and those found in CIP-008. The DSR SDT agrees, and Attachment 1 Part B, has been modified to provide the process for reporting a Cyber Security Incident.

The DSR SDT also believes NERC's additional concern about what data is applicable is addressed by the revisions to Attachment 1, and the inclusion of the OE-417 as an acceptable interim vehicle.

Implementation Plan:
The DSR SDT asked stakeholders to provide feedback on the proposed effective date which provided entities at least a year following board approval of the standard. Most stakeholders supported the one year minimum, however based on the revisions made to the requirements, the drafting team is now proposing that this time period be shortened to between six months and nine months. The current CIP-001 plan is adequate for the new EOP-004 and training should be met in the proposed timeline. Note that the Implementation Plan was developed for the revised Requirements, which do not include an electronic "one-stop shopping" tool. The tool for "one stop shopping" will be addressed in the proposed revisions to the NERC Rules of Procedure.

You do not have to answer all questions. Enter All Comments in Simple Text Format.

Insert a "check" mark in the appropriate boxes by double-clicking the gray areas.

1. Do you agree with the revised Purpose Statement of EOP-004-2, Impact Event Reporting? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

   ☐ Yes

   ☐ No

   Comments:

2. Do you agree with the proposed definition of Impact Event? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

   ☐ Yes

   ☐ No

   Comments:

3. Do you agree that the DSR SDT has provided and equally efficient and effective solution to the FERC Order 693 directive to "further define sabotage"? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

   ☐ Yes

   ☐ No

   Comments:

4. Do you agree with the proposed applicability of EOP-004-2 shown in Section 4 and Attachment 1 of the standard? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

   ☐ Yes

   ☐ No

   Comments:

5. Stakeholders suggested removing original Requirements 1, 7 and 8 from the standard and addressing the reliability concepts in the NERC Rules of Procedure. Do you agree with the removal of original requirements 1, 7 and 8 (which were assigned to the ERO) and the proposed language for the Rules of Procedure (Paragraph 812)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

   ☐ Yes

   ☐ No

   Comments:

6. Do you agree with the proposed revisions to Requirement 2 (now R1) including the use of defined terms Operating Plan, Operating Process and Operating Procedure? If not,

please explain why not and if possible, provide an alternative that would be acceptable to you.

☐ Yes

☐ No

Comments:

7. Do you agree with the proposed revisions to Requirement 3 (now R2)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

☐ Yes

☐ No

Comments:

8. Do you agree with the proposed revisions to Requirement 4 (now R3)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

☐ Yes

☐ No

Comments:

9. Do you agree with the proposed revisions to Requirement 5 (now R4)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

☐ Yes

☐ No

Comments:

10. Do you agree with the proposed revisions to Requirement 6 (now R5) and the use of either Attachment 2 or the DOE-OE-417 form for reporting? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

☐ Yes

☐ No

Comments:

11. Do you agree with the proposed revisions to Attachment 1? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

☐ Yes

☐ No

Comments:

12. Do you agree with the proposed measures for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

☐ Yes

☐ No

Comments:

13. Do you agree with the proposed Violation Risk Factors for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

    ☐ Yes

    ☐ No

    Comments:

14. Do you agree with the proposed Violation Severity Levels for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

    ☐ Yes

    ☐ No

    Comments:

15. Do you agree with the proposed Time Horizons for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

    ☐ Yes

    ☐ No

    Comments:

16. Do you agree with the proposed Implementation Plan for EOP-004-2? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

    ☐ Yes

    ☐ No

    Comments:

17. If you have any other comments you have not already provided in response to the questions above, please provide them here.

    Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2009-01 Disturbance and Sabotage Reporting Implementation Plan

Implementation Plan for EOP-004-2 - Impact Event Assessment, Analysis, and Reporting

Prerequisite Approvals

None

Revisions to Approved Standards and Definitions

Retire all requirements of EOP-004-1 and CIP-001-1.

Compliance with the Standard

The following entities are responsible for being compliant with all requirements of EOP-004-2:

- Reliability Coordinator
- Balancing Authority
- Load-serving Entity
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Distribution Provider

Effective Date
The standard shall become effective on the first calendar day of the third calendar quarter after the date of the order providing applicable regulatory approval. In those jurisdictions where no regulatory approval is required, the standard shall become effective on the first calendar day of the third calendar quarter after Board of Trustees adoption.

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

A. Introduction

1. Title: **Sabotage Reporting**

2. Number: CIP-001-1

3. Purpose: Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.

4. Applicability

4.1. Reliability Coordinators.

4.2. Balancing Authorities.

4.3. Transmission Operators.

4.4. Generator Operators.

4.5. Load Serving Entities.

5. Effective Date: January 1, 2007

B. Requirements

R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.

R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

C. Measures

M1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement 1

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements 2 and 3.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to procedures, policies, a letter of understanding, communication records, or other equivalent evidence that will be used to confirm that it has established communications contacts with the applicable, local FBI or RCMP officials to communicate sabotage events (Requirement 4).

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organizations shall be responsible for compliance monitoring.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to verify compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Reliability Coordinator, Transmission Operator, Generator Operator, Distribution Provider, and Load Serving Entity shall have current, in-force documents available as evidence of compliance as specified in each of the Measures.

If an entity is found non-compliant the entity shall keep information related to the non-compliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

None.

2. **Levels of Non-Compliance:**

2.1. **Level 1:** There shall be a separate Level 1 non-compliance, for every one of the following requirements that is in violation:

2.1.1 Does not have procedures for the recognition of and for making its operating personnel aware of sabotage events (R1).

2.1.2 Does not have procedures or guidelines for the communication of information concerning sabotage events to appropriate parties in the Interconnection (R2).

2.1.3 Has not established communications contacts, as specified in R4.

2.2. **Level 2:** Not applicable.

2.3. **Level 3:** Has not provided its operating personnel with sabotage response procedures or guidelines (R3).

2.4. **Level 4:**.Not applicable.

E. **Regional Differences**

None indicated.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Amended

A. Introduction

1. Title: **Disturbance Reporting**

2. Number: EOP-004-1

3. Purpose: Disturbances or unusual occurrences that jeopardize the operation of the Bulk Electric System, or result in system equipment damage or customer interruptions, need to be studied and understood to minimize the likelihood of similar events in the future.

4. Applicability

4.1. Reliability Coordinators.

4.2. Balancing Authorities.

4.3. Transmission Operators.

4.4. Generator Operators.

4.5. Load Serving Entities.

4.6. Regional Reliability Organizations.

5. Effective Date: January 1, 2007

B. Requirements

R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.

R2. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.

R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.

R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.

R3.2. Applicable reporting forms are provided in Attachments 1-EOP-004 and 2-EOP-004.

R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that

time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.

R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.

R4. When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.

R5. The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.

C. Measures

M1. The Regional Reliability Organization shall have and provide upon request as evidence, its current regional reporting procedure that is used to facilitate preparation of preliminary and final disturbance reports. (Requirement 1)

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, the preliminary report, computer printouts, operator logs, or other equivalent evidence that will be used to confirm that it prepared and delivered the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that will be used to confirm that it provided information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours. (Requirement 3.3)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

NERC shall be responsible for compliance monitoring of the Regional Reliability Organizations.

Regional Reliability Organizations shall be responsible for compliance monitoring of Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load-serving Entities.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to assess compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Regional Reliability Organization shall have its current, in-force, regional reporting procedure as evidence of compliance. (Measure 1)

Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that is either involved in a Bulk Electric System disturbance or has a reportable incident shall keep data related to the incident for a year from the event or for the duration of any regional investigation, whichever is longer. (Measures 2 through 4)

If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

See Attachments:

- EOP-004 Disturbance Reporting Form
- Table 1 EOP-004

2. Levels of Non-Compliance for a Regional Reliability Organization

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: No current procedure to facilitate preparation of preliminary and final disturbance reports as specified in R1.

3. Levels of Non-Compliance for a Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load- Serving Entity:

3.1. Level 1: There shall be a level one non-compliance if any of the following conditions exist:

3.1.1 Failed to prepare and deliver the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1

3.1.2 Failed to provide disturbance information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours as specified in R3.3

3.1.3 Failed to prepare a final report within 60 days as specified in R3.4

3.2. Level 2: Not applicable.

3.3. Level 3: Not applicable

3.4. Level 4: Not applicable.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	May 23, 2005	Fixed reference to attachments 1-EOP-004-0 and 2-EOP-004-0, Changed chart title 1-FAC-004-0 to 1-EOP-004-0, Fixed title of Table 1 to read 1-EOP-004-0, and fixed font.	Errata
0	July 6, 2005	Fixed email in Attachment 1-EOP-004-0 from info@nerc.com to esisac@nerc.com.	Errata

0	July 26, 2005	Fixed Header on page 8 to read EOP-004-0	Errata
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised

Attachment 1-EOP-004
NERC Disturbance Report Form

Introduction

These disturbance reporting requirements apply to all Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load Serving Entities, and provide a common basis for all NERC disturbance reporting. The entity on whose system a reportable disturbance occurs shall notify NERC and its Regional Reliability Organization of the disturbance using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. Reports can be sent to NERC via email (esisac@nerc.com) by facsimile (609-452-9550) using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. If a disturbance is to be reported to the U.S. Department of Energy also, the responding entity may use the DOE reporting form when reporting to NERC. Note: All Emergency Incident and Disturbance Reports (Schedules 1 and 2) sent to DOE shall be simultaneously sent to NERC, preferably electronically at esisac@nerc.com.

The NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports are to be made for any of the following events:

1. The loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations. Generally, a disturbance report will be required if the event results in actions such as:
   a. Modification of operating procedures.
   b. Modification of equipment (e.g. control systems or special protection systems) to prevent reoccurrence of the event.
   c. Identification of valuable lessons learned.
   d. Identification of non-compliance with NERC standards or policies.
   e. Identification of a disturbance that is beyond recognized criteria, i.e. three-phase fault with breaker failure, etc.
   f. Frequency or voltage going below the under-frequency or under-voltage load shed points.
2. The occurrence of an interconnected system separation or system islanding or both.
3. Loss of generation by a Generator Operator, Balancing Authority, or Load-Serving Entity — 2,000 MW or more in the Eastern Interconnection or Western Interconnection and 1,000 MW or more in the ERCOT Interconnection.
4. Equipment failures/system operational actions which result in the loss of firm system demands for more than 15 minutes, as described below:
   a. Entities with a previous year recorded peak demand of more than 3,000 MW are required to report all such losses of firm demands totaling more than 300 MW.
   b. All other entities are required to report all such losses of firm demands totaling more than 200 MW or 50% of the total customers being supplied immediately prior to the incident, whichever is less.
5. Firm load shedding of 100 MW or more to maintain the continuity of the bulk electric system.

6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in:
   a. Sustained voltage excursions equal to or greater than ±10%, or
   b. Major damage to power system components, or
   c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance as defined by steps 1 through 5 above.
7. An Interconnection Reliability Operating Limit (IROL) violation as required in reliability standard TOP-007.
8. Any event that the Operating Committee requests to be submitted to Disturbance Analysis Working Group (DAWG) for review because of the nature of the disturbance and the insight and lessons the electricity supply and delivery industry could learn.

NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report

☐ Check here if this is an Interconnection Reliability Operating Limit (IROL) violation report.

1.	Organization filing report.		
2.	Name of person filing report.		
3.	Telephone number.		
4.	Date and time of disturbance. Date:(mm/dd/yy) Time/Zone:		
5.	Did the disturbance originate in your system?	Yes ☐ No ☐	
6.	Describe disturbance including: cause, equipment damage, critical services interrupted, system separation, key scheduled and actual flows prior to disturbance and in the case of a disturbance involving a special protection or remedial action scheme, what action is being taken to prevent recurrence.		
7.	Generation tripped. MW Total List generation tripped		
8.	Frequency. Just prior to disturbance (Hz): Immediately after disturbance (Hz max.): Immediately after disturbance (Hz min.):		
9.	List transmission lines tripped (specify voltage level of each line).		
10.		FIRM	INTERRUPTIBLE
	Demand tripped (MW):		
	Number of affected Customers:		

	Demand lost (MW-Minutes):		
11.	Restoration time.	INITIAL	FINAL
	Transmission:		
	Generation:		
	Demand:		

Attachment 2-EOP-004
U.S. Department of Energy Disturbance Reporting Requirements

Introduction

The U.S. Department of Energy (DOE), under its relevant authorities, has established mandatory reporting requirements for electric emergency incidents and disturbances in the United States. DOE collects this information from the electric power industry on Form EIA-417 to meet its overall national security and Federal Energy Management Agency's Federal Response Plan (FRP) responsibilities. DOE will use the data from this form to obtain current information regarding emergency situations on U.S. electric energy supply systems. DOE's Energy Information Administration (EIA) will use the data for reporting on electric power emergency incidents and disturbances in monthly EIA reports. In addition, the data may be used to develop legislative recommendations, reports to the Congress and as a basis for DOE investigations following severe, prolonged, or repeated electric power reliability problems.

Every Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity must use this form to submit mandatory reports of electric power system incidents or disturbances to the DOE Operations Center, which operates on a 24-hour basis, seven days a week. All other entities operating electric systems have filing responsibilities to provide information to the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity when necessary for their reporting obligations and to file form EIA-417 in cases where these entities will not be involved. EIA requests that it be notified of those that plan to file jointly and of those electric entities that want to file separately.

Special reporting provisions exist for those electric utilities located within the United States, but for whom Reliability Coordinator oversight responsibilities are handled by electrical systems located across an international border. A foreign utility handling U.S. Balancing Authority responsibilities, may wish to file this information voluntarily to the DOE. Any U.S.-based utility in this international situation needs to inform DOE that these filings will come from a foreign-based electric system or file the required reports themselves.

Form EIA-417 must be submitted to the DOE Operations Center if any one of the following applies (see Table 1-EOP-004-0 — Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies):

1. Uncontrolled loss of 300 MW or more of firm system load for more than 15 minutes from a single incident.
2. Load shedding of 100 MW or more implemented under emergency operational policy.
3. System-wide voltage reductions of 3 percent or more.
4. Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the electric power system.
5. Actual or suspected physical attacks that could impact electric power system adequacy or reliability; or vandalism, which target components of any security system. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.

6. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.
7. Fuel supply emergencies that could impact electric power system adequacy or reliability.
8. Loss of electric service to more than 50,000 customers for one hour or more.
9. Complete operational failure or shut-down of the transmission and/or distribution electrical system.

The initial DOE Emergency Incident and Disturbance Report (form EIA-417 – Schedule 1) shall be submitted to the DOE Operations Center within 60 minutes of the time of the system disruption. Complete information may not be available at the time of the disruption. However, provide as much information as is known or suspected at the time of the initial filing. If the incident is having a critical impact on operations, a telephone notification to the DOE Operations Center (202-586-8100) is acceptable, pending submission of the completed form EIA-417. Electronic submission via an on-line web-based form is the preferred method of notification. However, electronic submission by facsimile or email is acceptable.

An updated form EIA-417 (Schedule 1 and 2) is due within 48 hours of the event to provide complete disruption information. Electronic submission via facsimile or email is the preferred method of notification. Detailed DOE Incident and Disturbance reporting requirements can be found at: http://www.eia.doe.gov/cneaf/electricity/page/form_417.html.

Table 1-EOP-004-0 Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Uncontrolled loss of Firm System Load	≥ 300 MW – 15 minutes or more	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
2	Load Shedding	≥ 100 MW under emergency operational policy	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
3	Voltage Reductions	3% or more – applied system-wide	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
4	Public Appeals	Emergency conditions to reduce demand	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
5	Physical sabotage, terrorism or vandalism	On physical security systems – suspected or real	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
6	Cyber sabotage, terrorism or vandalism	If the attempt is believed to have or did happen	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
7	Fuel supply emergencies	Fuel inventory or hydro storage levels ≤ 50% of normal	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
8	Loss of electric service	≥ 50,000 for 1 hour or more	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
9	Complete operation failure of electrical system	If isolated or interconnected electrical systems suffer total electrical system collapse	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
All DOE EIA-417 Schedule 1 reports are to be filed within 60-minutes after the start of an incident or disturbance All DOE EIA-417 Schedule 2 reports are to be filed within 48-hours after the start of an incident or disturbance				

All entities required to file a DOE EIA-417 report (Schedule 1 & 2) shall send a copy of these reports to NERC simultaneously, but no later than 24 hours after the start of the incident or disturbance.				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Loss of major system component	Significantly affects integrity of interconnected system operations	NERC Prelim Final report	24 hour 60 day
2	Interconnected system separation or system islanding	Total system shutdown Partial shutdown, separation, or islanding	NERC Prelim Final report	24 hour 60 day
3	Loss of generation	≥ 2,000 – Eastern Interconnection ≥ 2,000 – Western Interconnection ≥ 1,000 – ERCOT Interconnection	NERC Prelim Final report	24 hour 60 day
4	Loss of firm load ≥15-minutes	Entities with peak demand ≥3,000: loss ≥300 MW All others ≥200MW or 50% of total demand	NERC Prelim Final report	24 hour 60 day
5	Firm load shedding	≥100 MW to maintain continuity of bulk system	NERC Prelim Final report	24 hour 60 day
6	System operation or operation actions resulting in:	• Voltage excursions ≥10% • Major damage to system components • Failure, degradation, or misoperation of SPS	NERC Prelim Final report	24 hour 60 day
7	IROL violation	Reliability standard TOP-007.	NERC Prelim Final report	72 hour 60 day
8	As requested by ORS Chairman	Due to nature of disturbance & usefulness to industry (lessons learned)	NERC Prelim Final report	24 hour 60 day
All NERC Operating Security Limit and Preliminary Disturbance reports will be filed within 24 hours after the start of the incident. If an entity must file a DOE EIA-417 report on an incident, which requires a NERC Preliminary report, the Entity may use the DOE EIA-417 form for both DOE and NERC reports.				
Any entity reporting a DOE or NERC incident or disturbance has the responsibility to also notify its Regional Reliability Organization.				

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-01 Disturbance and Sabotage Reporting
Formal Comment Period Open March 9 – April 8, 2011

Now available at: http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Formal 30-day Comment Period Open through 8 p.m. on April 8, 2011

The Disturbance and Sabotage Reporting SDT has posted a revised draft of EOP-004-2 — Impact Event Reporting, along with the associated implementation plan and a redline of EOP-004-2 showing changes made since an informal comment period for this project concluded in October 2010. These documents are posted for a 30-day formal comment period.

The drafting team proposes to retire CIP-001-1 and incorporate its requirements into EOP-004-2. As a result, the changes to EOP-004 are so extensive that a redline showing changes against the last approved version would be impractical. For reference, the last approved versions of EOP-004 and CIP-001 have been posted.

Instructions

Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page: http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

Next Steps

The drafting team will consider all comments and determine whether to make additional changes to the standard. The team will post its response to comments and, if changes are made to the standard and supporting documents, submit the revised documents for quality review prior to ballot.

Project Background

Stakeholders have indicated that identifying potential acts of "sabotage" is difficult to do in real time, and additional clarity is needed to identify thresholds for reporting potential acts of sabotage in CIP-001-1. Stakeholders have also reported that EOP-004-1 has some requirements that reference out-of-date Department of Energy forms, making the requirements ambiguous. EOP-004-1 also has some 'fill-in-the-blank' components to eliminate.

The project will include addressing previously identified stakeholder concerns and FERC directives; will bring the standards into conformance with the latest approved version of the ERO Rules of Procedure; and may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Individual or group. (60 Responses)
Name (39 Responses)
Organization (39 Responses)
Registered Ballot body segment (check all industry segments in which your company is registered) (39 Responses)
Group Name (21 Responses)
Lead Contact (21 Responses)
Question 1 (56 Responses)
Question 1 Comments (60 Responses)
Question 2 (57 Responses)
Question 2 Comments (60 Responses)
Question 3 (55 Responses)
Question 3 Comments (60 Responses)
Question 4 (53 Responses)
Question 4 Comments (60 Responses)
Question 5 (53 Responses)
Question 5 Comments (60 Responses)
Question 6 (55 Responses)
Question 6 Comments (60 Responses)
Question 7 (54 Responses)
Question 7 Comments (60 Responses)
Question 8 (54 Responses)
Question 8 Comments (60 Responses)
Question 9 (53 Responses)
Question 9 Comments (60 Responses)
Question 10 (55 Responses)
Question 10 Comments (60 Responses)
Question 11 (57 Responses)
Question 11 Comments (60 Responses)
Question 12 (54 Responses)
Question 12 Comments (60 Responses)
Question 13 (45 Responses)
Question 13 Comments (60 Responses)
Question 14 (41 Responses)
Question 14 Comments (60 Responses)
Question 15 (42 Responses)
Question 15 Comments (60 Responses)
Question 16 (48 Responses)
Question 16 Comments (60 Responses)
Question 17 (0 Responses)
Question 17 Comments (60 Responses)

-
Group
Progress Energy
Jim Eckelkamp
No
Progress Energy appreciates the Standard Drafting Team's work on this project. "Any potential impact" is too vague and impossible to measure. Progress is unsure of how the ERO or Regional Entity measure impact. Potential is very subjective.
Yes

Yes
Yes
Yes
Yes
Do all individuals who are assigned roles and responsibilities in the Impact Event Operating Plan have to be involved with the test each time? Since there are multiple different types of Impact Events, it seems likely that only a subset of those Impact Events would be tested during an annual test, and therefore only a subset of individuals with responsibilities in the Impact Event Operating Plan would participate. For example, one test may exercise the Operating Process for properly reporting damage to a power plant that is a Critical Asset, and personnel from the Distribution Provider would not be involved in that test. Would such a scenario meet the requirement for the annual test? If so, it seems that some aspects of the Plan may never actually be required to be tested. This is ok, since R4 requires an annual review with personnel with responsibilities in the Impact Event Operating Plan. It must be made clear what is required in the annual test.
Yes
No
Progress Energy appreciates the effort of the Standard Drafting Team, but we do have some issues with the content of Attachment 1. The loss of three Transmission Elements can occur with a single transmission line outage. Progress is concerned that the possible frequency of this type of reporting could be an extreme burden. Under the column “Entity with Reporting Responsibility,” why do all related entities have to report the same event? (i.e. do the RC and the TOP in the RC footprint both have to report an event, or is it either/or? The word ‘Each’ implies separate reports. What is the Reliability-based need for both an RC and the BA/TOP/GO within the footprint to file the same report for the same event?) For vertically integrated companies it should be clear that only one report is required per Impact Event that will cover the reporting requirements for all registered entities within that company. The “damage or destruction of BES equipment” footnote contains the language “Significantly affects the reliability margin….” The word significantly should not be used in a Standard because it is subjective. Reliability margin is also undefined. System Operators must be trained on how to comply with the Standard, and thus objective criteria must be developed for reporting. “1 hour after occurrence” places a burden on System Operators for reporting when response to and information gathering dealing with the Impact Event may still be occurring. There is a note that states that the timing guidelines may not be met “under certain conditions…” but then requires a call to both its Regional Entity and notification to NERC. The focus should be on the event response and this type of reporting should occur “within an hour or as soon as practical.” It is unclear what the voltage deviations of +-10% based on (i.e. is that +-10% of nominal voltage? This may require new alarm set-points to be placed in service in Energy Management Systems in order for entities to able to prove in an audit that they reported all occurrences of voltage exceeding the 10% limit for 15 minutes or more. It has been stated by Regional Entity audit and enforcement personnel that attestations cannot be used to “prove the positive.”) The word “potential” should be removed from Attachment 1 and from the definition of Impact Event. An event is either an Impact Event or not. If an entity has to evacuate its control center facility temporarily for a small fire, or any other such minor occurrence, then it activates its EOP-008 compliant backup control center, and there is no impact to reliability, then why does there need to be a report generated? The “Forced Intrusion” category is problematic. The footnote 3 states: “Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects (sic) the reliability of the BES).” “Reasonably determine likely motivation” makes this subjective. If someone breaks into a BES substation fence to steal copper, is interrupted and leaves, then entity personnel determine someone tried to break into the substation, but cannot determine why, then this table requires a report to be filed within an hour. It is unclear what the purpose of such a report would be. Progress agrees that multiple reports in a short time across multiple entities may indicate a larger issue.
No
M3 states that “In the absence of an actual Impact Event, the Responsible Entity shall provide evidence that it conducted a mock Impact Event…” Does this mean that, if an entity experiences an Impact Event that is reportable, then the entity does not have to perform its annual test? If so, this should be made clear in the Requirement.
No
No
Progress disagrees with the High and Severe VSLs listed for R5. If an entity experiences an Impact Event and fails to submit a report within an hour as required, it may be that there are multiple mitigating circumstances. It is not reasonable to require reporting within an hour since identifying a reportable event often takes longer than this time period.

Progress thanks the Standard Drafting Team for their efforts on this project. The BES definition is still being revised under “Project 2010-17: Proposed Definition of Bulk Electric System.” “BES equipment” is mentioned several times in this Standard. A better definition of BES is important to the effectiveness of this Standard and integral to entities ability to comply with the Standard requirements. In Attachment 2, on the Impact Event Reporting form, item 10 is “Demand Tripped” and the categories include “FIRM” and “INTERRUPTIBLE.” It is unclear why interruptible load is included on the reporting form.

Individual

John Bee

Exelon

1 - Transmission Owners, 5 - Electric Generators

No

Although Exelon agrees that the proposed revision to the purpose statement of EOP-004-2 is better than the original draft; the DSR SDT should consider aligning the definition with the existing OE-417 terms. "Impact Events" are not clearly defined as reportable criteria in the DOE forms and may create confusion. Suggest rewording the purpose statement to simply "Incident Reporting" to align with existing terminology in OE-417 and removing the addition of a new term. A Purpose Statement is defined as “The reliability outcome achieved through compliance with the requirements of the standard.” Propose that the purpose should be, “ To require a review, assessment and report of events that could have an adverse material impact on the Bulk Electric System”.

No

The definition of impact events should be reworded to align with OE-417 and to explicitly reference that only events identified in EOP-004 – Attachment 1 are to be reported. Suggest the following: "An incident that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-opeation, environmental conditions, or human action as defined in EOP-004 Attachment 1." Propose the definition be changed to include “material” impact and read as follows; “Any event which has either caused or has the potential to cause an adverse material impact to the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action”

Yes

Exelon agrees with the DSR SDT in that the currently proposed solution effectively addresses the intent of FERC Order 693 directive to both clarify the triggering event for an entity to take action and by deleting all references to "sabotage" in effect removes the very term that had no clear definition.

No

Remove LSE. As has been determined in previous filings, FERC has ruled that asset owning DP’s must be registered as LSE’s. The standard as proposed is applicable to DP’s. This addresses any concern with a “reliability gap” for reporting events that could have an adverse material impact to the BES. See FERC Docket RC-07-4-003, -6-003, -7-003 paragraphs 24 and 25. “The Commission approves … revisions to the Registry Criteria to have registered distribution providers also register as the LSE for all load directly connected to their distribution facilities… The registration of the distribution provider as the LSE for all load directly connected to its distribution facilities is for the purpose of compliance with the Reliability Standards. As NERC explains, distribution providers have both the infrastructure and access to information to enable them to comply with the Reliability Standards that apply to LSEs… The Commission finds that, based on these facts, NERC acted reasonably in determining that the distribution provider is the most appropriate entity to register as the LSE for the load directly connected to its distribution facilities.” Attachment 1, Part A – Energy Emergency requiring Public appeal for load reduction – In the current draft Standard, the applicability has been revised from an RC and BA to "initiating entity". As a GO/GOP, I cannot see any event where a GO/GOP would be the responsible "initiating entity" or have the ability to determine an "Energy Emergency". Suggest revising back to specific entities that would be likely responsible for this action (e.g., RC, BA, TOP). Attachment 1, Part A – Energy Emergency requiring system-wide voltage reduction – In the current draft Standard, the applicability has been revised from an RC, TO, TOP, and DP to "initiating entity". As a GO/GOP, I cannot see any event where a GO/GOP would be the responsible "initiating entity" or have the ability to determine an "Energy Emergency" related to system-wide voltage reduction. Suggest revising back to specific entities that would be likely responsible for this action. Attachment 1, Part A – Voltage Deviations on BES facilities - A GOP may not be able to make the determination of a +/- 10% voltage deviation for ≥ 15 continuous minutes, this should be a TOP RC function only. Attachment 1, Part A – Loss of off-site power (grid supply) affecting a nuclear generating station – this event applicability should be removed in its entirety for a Nuclear Plant Generator Operator. The impact of loss of off-site power on a nuclear generation unit is dependent on the specific plant design, if it is a partial loss of off-site power (per the plant specific NPIRs) and may not result in a loss of generation (i.e., unit trip). If a loss of off-site power were to result in a unit trip, an Emergency Notification System (ENS) would be required to the Nuclear Regulatory Commission (NRC). Depending on the unit design, the notification to the NRC may be 1 hour, 8 hours or none at all. Consideration should be given to coordinating such reporting with existing required notifications to the NRC as to not duplicate effort or add unnecessary burden on the part of a Nuclear Plant Generator Operator during a potential transient on the unit. In addition, if the loss of off-site power were to result in a unit trip, if the impact to the BES were ≥2,000 MW, then required notifications would be made

in accordance with the threshold for reporting for Attachment 1, Part A – Generation Loss. However, to align with the importance of ensuring nuclear plant safe operation and shutdown as implemented in NERC Standard NUC-001, if a transmission entity experiences an event that causes an unplanned loss of off-site power (source) as defined in the applicable Nuclear Plant Interface Requirements, then the responsible transmission entity should report the event within 24 hours after occurrence. In addition, replace the words "grid supply" to "source" to ensure that notification occurs on an unplanned loss of one or multiple sources to a nuclear power plant. Suggest rewording as follows (including replacing the words "grid supply" to "source" and adding in the word "unplanned" to eliminate unnecessary reporting of planned maintenance activities in the table below): Event Entity with Reporting Responsibility Threshold for Reporting Time to Submit Report Unplanned loss of off-site power to a Nuclear generating plant (source) as defined in the applicable Nuclear Plant Interface Requirements (NPIRs) Each transmission entity responsible for providing services related to NPIRs (e.g., RC, BA, TO, TOP, TO, GO, GOP) that experiences the event causing an unplanned loss of off-site power (source) Unplanned loss of off-site power (source) to a Nuclear Power Plant as defined in the applicable NPIRs. Within 24 hours after occurrence

Yes

No

• R.1 Does an entity need to develop a stand alone Operating Plan if there is an existing process to address identification, assessing and reporting certain events? Suggest rewording to state "Each Responsible Entity shall have an Impact Event Operating Plan or equivalent implementing process that includes:" Disagree these new terms are required. Commonly accepted descriptions of programs, processes and procedures exist in registrar entities that would suffice. For example, R1 could use “Impact Event evaluation and reporting process” as a generic term to describe what is required. This would allow an entity to utilize any existing protocols or management guidelines and naming conventions in effect in their organization.

No

Agree that each Responsible Entity shall implement the [Impact] Events listed in Attachment 1 (Parts A and B); however, disagree with certain events, reporting responsibilities, threshold for reporting and time to submit reports as currently outlined in Attachment 1 (Parts A and B). Also suggest that R.2 be reworded to state for applicable [Impact] Events listed in Attachment 1 (Parts A and B). This requirement should only be applied to those events applicable to the registered entity. R2 is redundant to R1. No entity could claim to have met R1 if their plan / process was not operational and approved in the manner consistent with any other approved program, process, guideline etc. within their company.

No

• Each entity should be able to determine if they need a drill for a particular event. Is this document implying that the annual drill covering all applicable [Impact] Events? • A provision should be added to be able to take credit for an existing drill/exercise that could incorporate the required communications to meet the intent of R.3 to alleviate the burden on conducting a stand alone annual drill. The DSR SDT needs to provide more guidance on the objectives and format of the drill expected (e.g., table top, simulator, mock drill). • A provision should be added to R.3 to allow for an actual event to be used as credit for the annual requirement. It would seem that the intent is as such based on the wording in M.3; however, it needs to be explicit in the Requirement. • Must a test include communicating to NERC or the Region?

No

• Need more guidance on what personnel are expected to participate in the annual review. Training for all participants in a plan should not be required. Many organizations have dozens if not hundreds of procedures that a particular individual must use in the performance of various tasks and roles. Checking a box that states someone read a procedure does not add any value. This is an administrative burden with no contribution to reliability. • If the intention is that internal personnel who have responsibilities related to the Operating Plan cannot assume the responsibilities unless they have completed training. This requirement places an unnecessary burden on the registered entities to track and maintain a database of all personnel trained and should not be a requirement for job function. A current procedure and/or operating plan that addresses each threshold for reporting should provide adequate assurance that the notifications will be made per an individual's core job responsibilities.

No

Agree that each Responsible Entity should be able to use either Attachment 2 or the DOE OE-417 form for reporting; however, a GO/GOP will not have the ability to respond to Attachment 2 Task numbers 8, 9, 10, 11, and 12. Suggest that the DSR SDT either evaluate a shortened form version, provide a note or provision for "N/A" based on registration, or revise form to be submitted by the most knowledgeable functional entity (e.g., TOP or RC). Need clear guidance as to which form is to be used for which Impact Event, we feel that one and only one form should be used to eliminate confusion. Attachment 2 has a asterisk on #s 7, 8, 9, 10 and 11 there is not reference corresponding to it.

No

Attachment 1, Part A – Energy Emergency requiring Public appeal for load reduction – In the current draft Standard, the applicability has been revised from an RC and BA to "initiating entity". As a GO/GOP, I cannot see any event where a GO/GOP would be the responsible "initiating entity" or have the ability to determine an "Energy Emergency". Suggest revising back to specific entities that would be likely responsible for this action (e.g., RC, BA, TOP). Attachment 1, Part

A – Energy Emergency requiring system-wide voltage reduction – In the current draft Standard, the applicability has been revised from an RC, TO, TOP, and DP to "initiating entity". As a GO/GOP, I cannot see any event where a GO/GOP would be the responsible "initiating entity" or have the ability to determine an "Energy Emergency" related to system-wide voltage reduction. Suggest revising back to specific entities that would be likely responsible for this action. Attachment 1, Part A – Voltage Deviations on BES facilities - A GOP may not be able to make the determination of a +/- 10% voltage deviation for ≥ 15 continuous minutes, this should be a TOP RC function only. Attachment 1, Part A – Generation Loss of ≥ 2, 000 MW for a GOP does not provide a time threshold. If the 2, 000 MW is from a combination of units in a single location, what is the time threshold for the combined unit loss? Suggest that a time threshold be added for clarity. Attachment 1, Part A – Loss of off-site power (grid supply) affecting a nuclear generating station – this event applicability should be removed in its entirety for a Nuclear Plant Generator Operator. The impact of loss of off-site power on a nuclear generation unit is dependent on the specific plant design, if it is a partial loss of off-site power (per the plant specific NPIRs) and may not result in a loss of generation (i.e., unit trip). If a loss of off-site power were to result in a unit trip, an Emergency Notification System (ENS) would be required to the Nuclear Regulatory Commission (NRC). Depending on the unit design, the notification to the NRC may be 1 hour, 8 hours or none at all. Consideration should be given to coordinating such reporting with existing required notifications to the NRC as to not duplicate effort or add unnecessary burden on the part of a Nuclear Plant Generator Operator during a potential transient on the unit. In addition, if the loss of off-site power were to result in a unit trip, if the impact to the BES were ≥2,000 MW, then required notifications would be made in accordance with the threshold for reporting for Attachment 1, Part A – Generation Loss. However, to align with the importance of ensuring nuclear plant safe operation and shutdown as implemented in NERC Standard NUC-001, if a transmission entity experiences an event that causes an unplanned loss of off-site power (source) as defined in the applicable Nuclear Plant Interface Requirements, then the responsible transmission entity should report the event within 24 hours after occurrence. In addition, replace the words "grid supply" to "source" to ensure that notification occurs on an unplanned loss of one or multiple sources to a nuclear power plant. Suggest rewording as follows (including replacing the words "grid supply" to "source" and adding in the word "unplanned" to eliminate unnecessary reporting of planned maintenance activities in the table below): Event Entity with Reporting Responsibility Threshold for Reporting Time to Submit Report Unplanned loss of off-site power to a Nuclear generating plant (source) as defined in the applicable Nuclear Plant Interface Requirements (NPIRs) Each transmission entity responsible for providing services related to NPIRs (e.g., RC, BA, TO, TOP, TO, GO, GOP) that experiences the event causing an unplanned loss of off-site power (source) Unplanned loss of off-site power (source) to a Nuclear Power Plant as defined in the applicable NPIRs. Within 24 hours after occurrence Attachment 1, Part A – Damage or destruction of BES equipment • The event criteria is still ambiguous and does not provide clear guidance; specifically, the determination of the aggregate impact of damage may not be immediately understood – it does not seem reasonable to expect that the 1 hour report time clock starts on identification of an occurrence. Suggest that the 1 hour report time clock begins following confirmation of event. • The initiating event needs to explicitly state that it is a physical and not cyber. • If the damage or destruction is related to a deliberate act, consideration should also be given to coordinating such reporting with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security event (see additional comments in response to item 17 below). Attachment 1, Part A – Damage or destruction of Critical Cyber Asset The events that are associated with Critical Cyber Assets should be removed from this Standard. Critical Cyber Asset related events are better addressed in the reporting of Cyber Security Incidents which is already included in Attachment 1, Part B and the CIP standards currently require details about Critical Cyber Assets to be protected with access to that information restricted to only specifically authorized personnel. Attachment 1, Part A – Damage or destruction of Critical Asset The events that are associated with Critical Assets should be removed from this Standard. Critical Assets are typically whole control centers, substations or generation plants and the damage or destruction of individual pieces of equipment at one of these locations will usually not have much impact to the BES. Any important impacts located at these sites are already addressed in the other existing [Impact] Event types or would be addressed in the Cyber Security Incident event which is already included in Attachment 1, Part B. The CIP standards also currently require that details about Critical Assets and Critical Cyber Assets must be protected with access to that information restricted to only specifically authorized personnel. The identification of Critical Asset is also only an interim step used to identify the Critical Cyber Assets that need to have cyber security protections and the NERC Project 2008-06 CSO706 Standards Drafting Team is currently expecting to eliminate the requirement to identify Critical Assets in the draft revisions they are currently working on. Attachment 1, Part B – Forced intrusion at a BES facility – Consideration should also be given to coordinating such reporting with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security event (see additional comments in response to item 17 below). Attachment 1, Part B – Risk to BES equipment from a non-environmental physical threat – this event leaves the interpretation of what constitutes a "risk" with the reporting entity. Although the DSR SDT has provided some examples, there needs to be more specific criteria for this event as this threshold still remains ambiguous and will lead to difficulty in determining within 1 hour if a report is necessary. Consideration should also be given to coordinating such reporting with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security event (see additional comments in response to item 17 below). Attachment 1, Part B – Detection of a reportable Cyber Security Incident Although the DSR SDT agreed that there may be confusion between reporting requirements in this draft and the current CIP-008, "Cyber Security – Incident Reporting and Response Planning", Part B now requires a 1 hour report after occurrence. The DSR SDT should verify the timing and reporting required for these Cyber Security Incident events is coordinated with the NERC Project 2008-06 CSO706 Standards Drafting Team.

No
• M1 - Suggest rewording to state "Each Responsible Entity shall provide the current revision of the Impact Event Operating Plan or equivalent implementing process" • M3 – Need to provide more guidance on evidence of compliance to meet R.3 The DSR SDT needs to provide more guidance on the objectives and format of the drill expected (e.g., table top, simulator, mock drill) and what evidence will be required to illustrate compliance. • M5 - Suggest that the DSR SDT provide a note or provision to allow for the DOE OE-417 reporting form be submitted by the most knowledgeable functional entity (e.g., the TOP or RC) experiencing the event.
No
R.4 should be a low risk factor, this is an administrative requirement with no contribution to reliability.
No
Suggest rewording the 1 hour reporting for High and Severe to state "communicate or submit" a report within … depending on the severity of the event, an actual report may not be feasible. Similar to an NRC event report, a provision should be made for verbal notifications in lieu of an actual submitted report. An entity should not be penalized for failing to submit a written report within 1 hour if the communications were completed within the 1 hour time period meeting the intent of the Standard.
No
The DSR SDT reduced the implementation from one year to between six and nine months based on the revised standard requirements. Exelon disagrees with the proposed shortened implementation timeframe. The current revision to EOP-004 still requires an entity to generate, implement and provide any necessary training for the "Impact Event Operating Plan" by a registered entity. Commenters previously supported a one year minimum; but the requirements for implementation have not changed measurably - six to nine months is not adequate to implement as written.
The DSR SDT makes reference to comments that were previously provided that suggested adopting the NRC definition of "sabotage." Respectfully, this commenter believes the DSR SDT did not understand the intent of the original comment. The comment made by Exelon in the October 15, 2009 submittal was to ensure that the DSR SDT made an effort to include the Nuclear Regulatory Commission (NRC) as a key Stakeholder in the Reporting Process and to consider utilizing existing reporting requirements currently required by the NRC for each nuclear generator operator. Depending on the event, a nuclear generator operator (NRC licensee) also has specific regulatory requirements to notify the NRC for certain notifications to other governmental agencies in accordance with 10 CFR 50.72, "Immediate notification requirements for operating nuclear power reactors," paragraph (b)(2)(xi). The one hour notification requirement for an intrusion event would also meet an emergency event classification at a nuclear power plant. If an operations crew is responsible for the one hour notification and if separate notifications must be completed within the Emergency Plan event response, then an evaluation in accordance with 10 CFR 50.54, "Conditions of licensees," paragraph (q), would need to be performed to ensure that this notification requirement would not impact the ability to implement the Emergency Plan. At a minimum the DSR SDT should communicate this project to the NRC to ensure that existing communication and reporting that a licensee is required to perform in response to a radiological sabotage event (as defined by the NRC) or any incident that has impacted or has the potential to impact the BES does not create either duplicate reporting, conflicting reporting thresholds or confusion on the part of the nuclear generator operator. Note that existing reporting/communication requirements are already established with the FBI, DHS, NORAD, FAA, State Police, LLEA and the NRC depending on the event. There are existing nuclear plant specific memorandums of understanding between the NRC and the FBI and each nuclear generating site licensee must have a NRC approved Security Plan that outlines applicable notifications to the FBI. Depending on the severity of the security event, the nuclear licensee may initiate the Emergency Plan. The proposed "Reporting Hierarchy for Impact Event EOP-004-2," needs to be communicated and coordinated with the NRC to ensure that the flow chart does not conflict with existing expected NRC requirements and protocol associated with site specific Emergency and Security Plans. Propose allowing for verbal reporting via telephone, for 1 hr. reporting with a follow up using the forms. With the revised standard EOP-004-2 it eliminates the #8; loss of electric service >= 50K, however, that requirement is still required for the DOE-OE-417 form. The question is do we still have to send it to NERC / Region if NERC/ Region does not specifically still have that as a requirement? Also, with that requirement, on the current EOP-004-1 it says that schedule 1 has to be filled out within 1 hour? This doe not coincide with DOE-OE-417 form. The bottom line, it looks like there is inconsistency as to what is reportable per EOP-004-2 and DOE-OE-417 form, some of the items are redundant, some are not, but better guidance is needs as to which form to use when. The SDT should have a Webaniar with the industry to create an understanding as to who is responsible to report what and at what time.
Individual
Jennifer Wright
SDG&E
1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators
No
SDG&E does not agree with the revised Purpose Statement because it does not reflect the standard's purpose of identifying reporting requirements for impact events. SDG&E recommends the following revised Purpose Statement: "To identify the reporting requirements for events considered to have an impact on the reliability of the Bulk Electric System and to allow an awareness of these Impact Events to be understood by the industry in recognizing potential

enhancements that may be made to the reliability of the BES.”
Yes
Yes
No
SDG&E recommends that “Load Serving Entity,” “Transmission Service Provider,” and “Interchange Authority” be removed from the proposed applicability shown in Section 4. These entities do not own assets that could have an impact on the Bulk Electric System. Additionally, none of these entities is listed as an “Entity with Reporting Responsibility” in Attachment 1. Finally, “Transmission Service Provider” is covered by either “Transmission Owner” or “Balancing Authority,” which are entities also listed in the proposed Applicability section, and “Load Service Entity” and “Interchange Authority” are covered by “Balancing Authority.”
No
SDG&E agrees with removing original Requirements 1, 7, 8 from the standard. In addition, SDG&E recommends that the standard reference Section 812 of the Rules of Procedure.
Yes
Yes
Yes
Yes
Yes
No
For “Detection of a reportable Cyber Security Incident,” Attachment 1 identifies the threshold for reporting as: “that meets the criteria in CIP-008 (or its successor)”; however, CIP-008 has no specified criteria, so this is an unusable threshold. Additionally, SDG&E recommends that the timing of any follow-up and/or final reports required by the standard be listed in the Attachment 1 table.
Yes
Yes
No
This Reliability Standard provides a list of reporting requirements that are applicable to registered entities, thus it is a paperwork exercise; therefore, SDG&E recommends that none of the requirements should exceed a “Moderate” Violation Severity Level. Failure on the part of an applicable Registered Entity to provide an event report will have no immediate impact on the Bulk Electric System.
No
SDG&E recommends a 9 month minimum timeframe for implementation.
Individual
Alan Gale
City of Tallahassee (TAL)
3 - Load-serving Entities, 5 - Electric Generators
Yes
No
While I agree with the overall concept, I am concerned with “or has the potential to impact”. While the standard makes reference to Attachment 1 Parts A and B, the inclusion of the attachment is not in the definition. This leaves ambiguity in the definition that could enable second guessing by auditors. Proposed: “An impact event is any event that has either impacted or has the potential to impact (above the thresholds described in EOP-004-2 Attachment 1) the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action.”

Yes
Yes
Yes
Yes
Yes
No
Comments: The verbiage “at least annually, with no more than 15 months between such tests” is an attempt to define annually. If you want every 15 months say “at least every 15 months”. Otherwise just say annual and let the entities decide what that is, as is being done with other “annual” requirements. Additionally, while the Measure (M3) implies that an actual event would suffice it is not stated in the requirement, and the entire plan should be tested, not just a component. Proposed: Each Responsible Entity shall conduct a test of its Impact Event Operating Plan at least annually. A test of the Impact Event Operating Plan can range from a paper drill, to the response to an actual event.
No
The verbiage “at least annually, with no more than 15 months between review sessions” is an attempt to define annually. If you want every 15 months say “at least every 15 months”. Otherwise just say annual and let the entities decide what that is, as is being done with other “annual” requirements.
Yes
No
One hour should be expanded. While I realize the importance of getting information to NERC/ESISAC/whoever, most of the 1-hour requirements are tied to events that may not be resolved within one hour. This will result in stopping restoration efforts or monitoring to submit paperwork. Calling in additional assistance, while certainly a possibility, may not be feasible to accomplish in sufficient time to meet the one-hour deadline. If any of these events were to truly have a detrimental effect on the BES, the effects would have already been felt. Recommend all 1-hour reports be extended to 4-hours. This should also be placed on the list to modify the OE-417 report time lines.
No
M3 & M4 should be modified if comments above (#8 and #9) are incorporated. M4 - Providing the “materials presented” is beyond the scope of compliance. This constitutes a review of the training program which is beyond the scope of the standard. Review of attendance sheets should be sufficient. The personnel will be listed in the Plan/Process/Procedure. Modify M4: Responsible Entities shall provide evidence of those who participated in the review, showing who was present and when internal personnel were trained on their responsibilities in the plan.
No
R1 is administrative in nature (must have a document) and should be Lower.
Yes
Yes
Yes
Attachment 2 (Impact Event Reporting Form) items 8, 9, 10, and 11 have an asterisk but no identification as to what the asterisks refer to.
Individual
Mace Hunter
Lakeland Electric
1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators
Yes
Yes
Yes

No
Event – Transmission loss Threshold for Reporting – Revise to “Loss of three or more BES Transmission elements within a 15 minute period”. This change would capture a sequence of transmission element losses and remove the question if timing that will arise if other transmission elements trip, cascade, due to loss of the first element. There may also be a need for a footnote to clarify that a transmission element that is removed from service by a transmission operator to prevent uncontrolled cascading would be classified as a loss (something for the SDT to consider). Event – Energy Emergency requiring Public appeal for load reduction Threshold for Reporting – Add a footnote: Repeated public appeals for the same initiating Impact Event shall be reported as one Public Appeal Event. The initiation and release to the media of the Public appeal(s) should be the reportable event. Question: would an internal request to large industrial customers for voluntary load reductions be reportable under this Event?
Yes
Yes
Individual
Nathaniel Larson
New Harquahala Generating Co.
1 - Transmission Owners, 5 - Electric Generators
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Group
PJM Interconnection LLC
Srinivas Kappagantula
Yes
No
The term "Impact Event" has been too broadly defined. According to the current definition, any event (including routine operations) can have the potential to impact the reliability of the Bulk Electric System and hence can be an Impact Event. The definition should only include unplanned events. Attachment 1 lists the events that are reportable. It seems that the definition of Impact Event refers to the events in Attachment 1 as opposed to defining “Impact Event”. As such, it is best that the SDT not define “Impact Event” but use words to the effect that requires an entity to have a plan and implement it for reporting unplanned events outlined in Attachment 1. If “Impact Event” were to be defined, we suggest the following definiton would be a better option: "An Impact Event is any unplanned event listed in Attachment I that has either adversely impacted or has the potential to adversely impact the reliability of the Bulk Electric System."
Yes
Yes
1. We agree that the entities listed should be responsible for ensuring events are reported, provided they own BES assets, but more guidance should be provided on which entity in Attachment 1 should actually file the report to avoid multiple entities reporting a single event. Current Attachment 1 results in significant duplicate reporting. 2. Although the applicable entities listed in Section 4 capture all entities that are assigned a reporting responsibility in Attachment 1, some events in Attachment 1 refer to entities applicable under a different standard (e.g CIP-002) as the responsible entites for reporting. This results in IA, TSP, and LSE (none of which, generally own Critical Assets and hence not likely own CCAs) as being repsonsible for reporting an event. We urge the SDT review the need to include IA, TSP, and LSE in applable entities. Also, why is NERC an applicable entity in CIP-002-3 but not in this standard?
No
We agree that the standard should not have requirements applicable to the ERO, but disagree with revising the NERC Rules of Procedure (RoP) to include suggested Section 812. The reporting responsibility should not be solely given to NERC. Other learning organizations must also be considered for performing this responsibility. Additionally, the proposed wording of Section 812 appears to imply that NERC will notify the appropriate law enforcement agencies as opposed to the local responsible entity.
No
1. This is an “after-the-fact” reporting requirement and should not be confused with Operating Plans that have specific operating actions and goals. Each entity should prepare its own impact event operating guideline that addresses impact events, identification of impact events, information gathering, and communication without specifying a specific format such as Operating Plans, Operating Process, and Operating Procedures. In fact, all three documents mentioned can all be a single document. 2. 1.3.2 requires notification of law enforcement agencies for all events listed in Attachment 1. This is essentially not true. For example, firm load is shed requires notification to law enforcement but an IROL violation, generation loss, or voltage deviation do not.
No
We agree with the concept but disagree with the use of the term “Operating Plan” as a defined term in line with our comments in Question 6 above.
No
1. This is an “after-the-fact” reporting requirement (administrative in nature). Annual testing of such a requirement does not add to the reliability of the BES. 2. R3 attempts to define “Annual” for the Registered Entity to test its Operating Process. We believe R3 should follow the NERC definition of Annual as defined in the NERC Compliance Application Notice (CAN) – CAN-0010 – Definition of Annual as opposed to creating a new definition of Annual – or – refer to an entity’s defined use of the term annual.
Yes
1. We agree with the concept but disagree with the use of the term “Operating Plan” as a defined term in line with our comments to Question 6 above. 3. R4 attempts to define “Annual” for the Registered Entity to review its Impact

Operating Plan. We believe R4 should follow the NERC definition of Annual as defined in the NERC Compliance Application Notice (CAN) – CAN-0010 – Definition of Annual as opposed to creating a new definition of Annual – or – refer to an entity's defined use of the term annual.
No
R5 seems redundant as R2 already requires an entity to report any Impact Events by executing/implementing its Impact Event Operating Plan. R5 merely stipulates the use of Attachment 2 or DOE-417, which an entity automatically would use for reporting purposes while implementing its Impact Event Operating Plan.
No
There is still a significant amount of duplicate reporting involved in Attachment 1, which needs to be cleared. See comments to Question 4.
No
1. We disagree with M4 as it seems to indicate that all training needs to be in person and precludes any form of Computer Based Training (CBT). 2. As indicated in 10, R5 is redundant as R2 already required an entity to report any Impact Events by executing/implementing its Impact Event Operating plan. If R5 is to remain as is, then M5 goes beyond the requirement by requiring the entity to produce evidence of compliance for the type of Impact Event experienced. It is not clear as to what additional evidence is needed to "support the type of Impact Event experienced".
No
All VRFs should be lower as Requirements 1-5 are all administrative in nature. A violation of any of these requirements does not directly or indirectly affect the reliability of the BES.
No
VSLs should reflect the comments on the VRFs above.
No
R2 and R5 should be in Operations Assessment Time Horizon as they deal with "after-the-fact" reporting.
Yes
In the Compliance Enforcement Authority Section on Page 11, the second bullet says "If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement". We are not sure what this exactly implies or means. Additional clarification is required.
Individual
Brian Pillittere
Tenaska
5 - Electric Generators
No
We already have adequate procedures in place to address sabotage and other significant events, pursuant to the existing CIP-001-1 and EOP-004-1 Standards. The requirement to develop a new Impact Event Operating Plan would increase the administrative burden on Registered Entities to comply with the proposed Standard, without providing a foreseeable improvement in system reliability. The "laundry list" of required Impact Event Operating Plan components is too specific and would make it more difficult to prove compliance with EOP-004-2 during an audit. A revised version of the proposed R5 is the only Requirement that is necessary to achieve the stated purpose of Project 2009-01.
No
The proposed Impact Event Operating Plan should not be required.
No
The proposed Impact Event Operating Plan should not be required, therefore any tests of the Operating Process should not be required.
No
The proposed Impact Event Operating Plan should not be required.
No
R5 should be changed to "Each Responsible Entity shall report Impact Events listed in Attachment 1 using the form in Attachment 2 or the DOE OE-417 reporting form". This revised version of the proposed R5 is the only Requirement that is necessary to achieve the stated purpose of Project 2009-01. The proposed R1 through R4 should be deleted and R5 should be changed to R1.

No
The proposed R1 through R4 should be deleted and a revised version of R5 should become R1. The proposed measures for the new R1 should be revised accordingly.
Individual
MIchael Johnson
APX Power Markets
8 - Small End Users
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
The reporting of Impact Events needs to be clear spelled out and if moving some of that to State Agencies it needs to be consistent in all States at the same time and which State it should be reported to. We have a 24-hour Desk in one state that handles facilites in many other States. If there is an Impact Event that needs to be reported, where is that report sent to. The State the facility resides in or the State where our 24-hour Desk resides in.
Individual
Jonathan Appelbaum
United Illuminating Co
1 - Transmission Owners
No

UI agrees with the idea but believes the statement can be improved to remove ambiguities. For example: “if known” can be modifying the word causes, or the word Impact events. To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of identified Impact Events and if known their causes, if known, by the Responsible Entities.
Yes
Yes
No
Will an entity be required to develop an Operating Process for every Impact Event in Attachment 1, or only those events that apply to its Registration. For example, does a DP require evidence of an Operating Process/Procedure for Voltage Deviations on a BES Facility? Some items in Attachment 1 state “Each RC, BA, TOP, DP that experiences the Impact Event” (such as Loss of Firm Load). DP’s may have arranged with TOP and RC to communicate the event to TOP who then will file the NERC report and OE-417. The requirements in the Standard would allow for this as long as the Operating Plan documents it. Attachment 1 though can be interpreted that this arrangement would not be allowed and each entity shall file its own and separate report. UI suggests that Attachment 1 be modified to allow for an Entities Operating Plan to rely on another Entity making the final communication to NERC. “Each RC, BA, TOP, DP that experiences the Impact Event, either individually or combined on a single filing”
Yes
No
Does R1.1 require an Operating Process for each Impact Event in attachment 1 or an Operating Process that in general applies to all Impact Events?
Yes
Yes
: FERC did state in Order 693 that the reporting procedure requires testing. UI is concerned that the scope of the requirement is unspecified. Does the exercise require only one type of Impact Event to be exercised per period, or is an entity required to simulate each Impact Event and notification
Yes
As written it is a training burden. Certain persons will have only one step in one operating procedure to perform. There is no necessity to review the entire Operating Plan with them. For example, Field Personnel need to know that if they see something not right to report it immediately. In this instance there is no benefit to review the Operating Procedure/Process for firm load shedding with them.
Yes
Put “its” before Impact Event Operating Plan.
No
R3 should be Low. It is a test of the communication Plan which is use of telephone and email.
Yes
Yes
No
The SDT should be specific that on the effective date an Entity will have the Operating documented and approved. The SDT should be specific that the first simulation is required to occur 15 months following the effective date. The SDT should be specific that the first annual review shall occur with in 15 months after the effective date.
Group
Georgia Transmission Corporation & Oglethorpe Power Corporation
David Revill
Yes
We find it unnecessary to state that the purpose of a Reliability Standard is to "improve…the reliability of the Bulk Electric System."
No
We do not think that Impact Event should be defined using a recursive definition, i.e. that the word "impact" should be

used in the definition of the term "Impact Event." Instead, we suggest using an enumerative definition in that the tables included in Attachment 1 are themselves used to define "Impact Event." If this definition is not acceptable, we suggest replacing the word "impact" in the definition with the word reduce, reduced, or …potential to reduce the reliability of the BES.
Yes
We agree with the approach taken by the SDT.
No
We do not believe that GO, TO, TSP, DP, or LSE should be included in the applicability of this standard. It is our opinion that the reporting requirements lie primarily with the applicable operator and should be limited as such. We recommend modifications as discussed in our response to question 6 to clearly define what types of events each Responsible Entity needs to prepare for. Currently, it seems that multiple entities are being required to report the same event for some events where only one entity should have a reporting responsibility. However, NERC should not decide which one entity should report a given event. The entities should have the flexibility to create a process which allows for coordination and communication at a local level and to work out with neighboring entities who might ultimately report events to the applicable organizations.
No
The terms "Operating Procedure, Operating Plan, and Operating Process," while included in the NERC glossary, are not consistently used throughout the body of NERC standards as they are used in R1 of EOP-004-2. As such, we do not see a reliability benefit in using the defined terms over the more commonly used terms of simply "plans, processes, and procedures." In part 1.1 of R1, we think that the requirement should clearly indicate that a particular Responsible Entity's Impact Event Plan should only be required to include those particular Impact Events for which the Responsible Entity has the reporting obligation. Therefore, we suggest the following modification to R1: "1.1 An Operating Process for identifying Impact Events listed in Attachment 1 for those Impact Events where the Responsible Entity is identified as having the reporting responsibility." Additionally, in part 1.3 of R1, we believe the language to be vague and will introduce the need for further clarification either through an interpretation or the CAN process in part because the verb tenses of the sub-sub-requirements do not agree and it appears to require notification to all listed parties for every Impact Event instead of only those that make sense for a particular event. As such, we suggest adding a column to the tables in Attachment 1 that identifies precisely which organizations should be notified in the case of a particular Impact Event and modifying part 1.3.2 to read: "1.3.2 External organizations to notify as specified in Attachment 1." Currently, as written, the standard could be interpreted to require notification to law enforcement for an IROL violation, for instance. Furthermore, we are concerned that as written, the standard may require that the same event must be reported by multiple responsible entities. Our current process uses notification between Responsible Entities (i.e. from a TO to a TOP and then from the TOP to NERC) to allow for a centralized and coordinated notification to law enforcement, NERC, etc. We are concerned that the requirement as written does not appear to allow this flexibility and may require both the TO and TOP to report the same event in order to prove compliance with the Standard.
No
We are concerned with having a separate requirement to implement the Plan. Is this requirement necessary on its own? Should R1 instead require a Responsible Entity to "document and implement" an Impact Event Operating Plan? More specifically, if an Entity does not have an Impact Event, are they in violation of this requirement? If merging this requirement with R1 is not acceptable we suggest moving the language from the measure to the requirement as such: "To the extent that a Reponsible Entity has an Impact Event on its Facilities, Each Responsible Entity shall implement…" Additionally, R1 uses the phrase "recognized Impact Event" where as R2 simply uses the term "Impact Event." The phrase "recognized Impact Event" should be used consistently in R2 as well.
No
With the current CAN on the definition of annual, we do not believe that the additional qualification that the test shall be conducted "with no more that 15 calendar months between tests" is necessary. If instead the team believes that, in order to support the reliability of the BES, tests should be performed at least every 15 months, then the requirement should be to perform a test at least every 15 calendar months and remove the annual component.
No
We do not believe that the requirement should specify that the plan must be reviewed with those personnel who have responsibilities identified in that plan as there is no requirement in R1 that the plan must identify any specific personnel responsibilities. Additionally, we seek clarification on whether review in this instance means train as indicated in the measure.
No
As stated above in response to question 6, we believe that a column should be added to the tables to explicitly indicate what external organizations should receive the communications of a particular Impact Event type. Additionally we have concerns with the following table items: Threshold for reporting Transmission Loss: As stated, this will require the reporting of almost all transmission outages. This is particularly true taking into consideration the current work of the drafting team to define the Bulk Electric System. The loss of a single 115kV network line could meet the threshold for

reporting as the definition of Element includes both the line itself and the circuit breakers. Instead, we recommend the following threshold "Three or more BES Transmission lines." This threshold has consistency with CIP-002-4 and draft PRC-002-2. This threshold also needs additional clarification as to the timeframe involved. Is the intent the reporting of the loss of 3 or more BES Transmission Elements anytime within a 24 hour period or must they be lost simultaneously? Also, we recommend that thtese three losses be the result of a related event to require reporting. Entity with Reporting Responsibility for Loss of Off-site power to a nuclear generating plant (grid supply): The reporting responsibility should clarify that this is only entities included in the Nuclear Plan Interface Requirements.
No
Several of the measures appear to introduce items that are not required by the standard. For instance, R3 requires that a test of the communications process be performed, however Measure 3 indicates that a mock impact event be performed. Measure 4 indicates that personnel be listed in the plan and be trained on the plan, however there is no requirement to include people in the plan or to train them.
In the discussion and related flowchart described as "A Reporting Process Solution - EOP-004," the discussion suggests that Industry should notify the state law enforcement agency and then allow the state agency to coordinate with local law enforcement. It has been our experience that we receive very good response from local law enforcement and they have existing processes to notify state or federal agencies as necessary. It appears the recommendation is to bypass the local law enforcement, but it is not clear that representatives from state or local law enforcement were included in this discussion (see proposal discussed with "FBI, FERC Staff, NERC Standards Project Coordinator and SDT Chair"). It would be helpful to see some additional clarification to understand why the state agency was chosen over local or federal agencies. Finally, we would like to express our gratitude to the DSR SDT for their hard work in making improvements to the NERC standards for event reporting.
Group
Northeast Power Coordinating Council
Guy Zito
Yes
No
Is there a need for this definition? By itself the term is not specific on the types of events that are regarded as having an “impact”. The detailed listing of events that fall into a reportable event category, hence the basis for the Impact Event, is provided in Attachment A. The events that are to be reported can be called anything. Defining the term Impact Event does not serve the purpose of replacing the details in Attachment A, and such a term is not used anywhere else in the NERC Reliability Standards. For a complete definition of Impact Event, all the elements in Attachment A must be a part of it. Suggest consider not defining the term Impact Event, but rather use words to stipulate the need to have a plan, to implement the plan and to report to the appropriate entities those events listed in Attachment A.
Yes
It is more important to report suspicious events than to determine if an event is caused by sabotage before it gets reported.
No
Disagree with the following inclusion/exclusion of several entities: a. The applicable entities listed in Section 4 capture all the entities that are assigned a reporting responsibility in Attachment 1 of the standard. While some events in Attachment 1 have specific entities identified as responsible for reporting, certain events refer to the entities listed in specific standards (e.g. CIP-002) as the responsible entities for reporting. The latter results in IA, TSP and LSE (none of which being specifically identified as having a reporting responsibility) being included in the Applicability Section. NERC should be included in the Applicability Section as it is an applicable entity identified in CIP-002-3. b. If the above approach was not strictly followed, then suggest the SDT review the need to include IA, TSP and LSE since they generally do not own any Critical Assets and hence will likely not own any Critical Cyber Assets.
Yes
Agree with the proposed removal, but have not assessed the proposed language for RoP para. 812 because unable to access it (not on the RoP page).
Yes
Yes
No
The annual testing requirement is too frequent for a reporting, and not an operational process. The testing interval

should be extended to five years.
Yes
No
R5 stipulates the use of Attachment 2 or the DOE-417, which is the vehicle for reporting only. This is the “how” part, not the “what”. The vehicle for reporting can easily be included in R2 where an entity is required to implement (execute) the Operating Plan upon detection of an Impact Event. Suggest combining R2 with R5.
No
As indicated under Question 4, we question the need to include IA, TSP and LSE in the responsible entities for reporting.
No
Concerns with M5: a. As suggested in the response to Question 10 above, R5 should be combined with R2; b. If R5 to remain as is, then M5 goes beyond the requirement in R5 in that it asks for evidence to support the type of Impact Event experienced. Attachment 2 already requires the reporting entity to provide all the details pertaining to the Impact Event. It is not clear what kind of additional evidence is needed to “support the type of Impact Event experienced”. Also, the date and time of the Impact Event is provided in the reporting form. Why the need to provide additional evidence on the date and time of the Impact Event?
No
If R5 is to remain as is, then the VRF should be a Lower, not a Medium. R5 stipulates the form to be used. It is a vehicle to convey the needed information, and as such it is an administrative requirement. Failure to use the form provided in Attachment 2 or the DOE form does not lead to unreliability.
No
No major issues with the proposed VSLs. However, because of the preceding comments, want to see the next revision of the draft.
No
For the purpose of developing and updating an Impact Event Operating Plan, there should not be any requirements that fall into the Long-term planning horizon. As the name implies, the plan is used in the operating time frame. Consistent with other plans such as system restoration plans which need to be updated and tested annually, most of the Time Horizons in that standard (EOP-005-2) are either Operations Planning or Real-time Operations. Suggest the Time Horizon for R1, R3 and R4 be changed to Operations Planning.
Yes
Individual
Kevin Koloini
American Municipal Power
3 - Load-serving Entities, 4 - Transmission-dependent Utilities, 5 - Electric Generators
Yes
The purpose is acceptable. I think it could be improved and simplified. There were not any questions on the title. Consider changing the title to Reportable Events. There were not any questions on the category. I suggest changing the category from Emergency Operations to Communications. Reporting events can trigger and be more than just Emergency Operations. I feel the reporting function performed by entities should be under the Communications category. Title: Reportable Events Purpose: To improve reliability by communicating timely information about an event or events.
Yes
The definition of Impact Event is acceptable and an improvement. I feel it could be improved and simplified further. Consider changing Impact Event to a "reportable event".
Yes
Well done.
No
No, I do not agree. The DP and LSE functions should be removed.
Yes
A software solution may provide an easy expansion for reporting EOP-004, CIP-001, and additional standards.
No
No, remove R1. R1 is not an acceptable requirement nor should this be an operation. Focusing on a plan and procedure is overly prescriptive and costly. The only requirement should be to have an entity submit a report. Let the entity decide how they want to implement the reporting.

No
No, remove R2. R2 is not an acceptable requirement nor should this be an operation. Focusing on a plan is overly prescriptive and costly. The only requirement should be to have an entity submit a report. Let the entity decide how they want to implement the reporting.
No
No, remove R3. R3 is not an acceptable requirement nor should this be an operation. Focusing on a test is overly prescriptive and costly. The only requirement should be to have an entity submit a report. Let the entity decide how they want to implement the reporting.
No
No, remove R4. R4 is not an acceptable requirement nor should this be an operation. Focusing on a plan and personnel tracking is overly prescriptive. The only requirement should be to have an entity submit a report. Let the entity decide how they want to implement the reporting.
No
R5 is not an acceptable requirement, but it can be improved. Each Responsible Entity shall report "Impact Events" to _____ (address specified in attachment 1, website, entity, email address, or fax, etc.) Focusing on a plan and procedure is overly prescriptive. The only requirement should be to have an entity submit a report. Let the entity decide how they want to implement the reporting.
Yes
No
M1-M4 should be eliminated and M5 should be revised to incorporate a simplified R5. M5 - Date and time of submitted report
No
No, this is not acceptable. Eliminate R1-R4. Change R5 to Lower.
No, this is not acceptable. Eliminate R1-R4 and change R5. Severe: n/a High VSL: n/a Medium VSL: No report for a reportable event Low VSL: Late report for a reportable event
No
Yes
Individual
Daniel Duff
Liberty Electric Power LLC
5 - Electric Generators
Yes
Yes
I am interpreting the phrase "has the potential" to exclude events which had the potential, but did not impact the BES. An example would be a generation trip - if the trip had happened during a system emergency it could have affected the BES, but since it happened under normal conditions there is no reporting responsibility. Some assurance on this interpretation would be appreciated.
Yes
Yes
Yes
Yes
Yes
No
It is not the proper role of the standards to dictate how an entity conducts training. Large utilities with backup control rooms and enough personnel can conduct routine drills without disturbing operations, but this is not always the case for small entities. Further, classroom training where emergency responses are discussed can be a better tool at times for

assuring compliance with operating procedures. I would suggest R3 read "Each entity shall assure that personnel are aware of the requirements of EOP-004 and capable of responding as required".
No
Again, the entity should determine the need for review of any procedure. Changing circumstances may dictate a shorter cycle, but no changes could dictate a longer review. I will note that spill prevention plans are required to be reviewed every five years, so I question the need for an 18-month review of the EOP plan.
Yes
Yes
A qualified yes here - please clarify footnote 1 to the table. Are the listed qualifications "and" or "or" statements -IOW, if destruction of BES equipment through human error does not have the potential to result in the need for emergency actions, is it still reportable? If a 18-240 KV step-up transformer suffers minor damage because a conservator tank was valved out, is this reportable under this definition?
No
Due to disagreement with R3 and R4.
No
See Q 12.
No
See Q 12.
Yes
Yes
Individual
Philip Huff
Arkansas Electric Cooperative Corporation
3 - Load-serving Entities, 4 - Transmission-dependent Utilities, 5 - Electric Generators, 6 - Electicity Brokers, Aggregators
No
The purpose statement reads "To improve industry awareness…of the BES". We suggest the purpose should state "To improve industry awareness and effectiveness in addressing risks to the BES". We feel the remaining purpose statement is unnecessary.
Yes
Yes
Yes
Yes
No
We appreciate the effort the team has taken in improving the requirements since the last posting. For 1.3, it appears to suggest the communication must always include communicating to internal personnel and ALL external organizations. We suggest removing the reference to 1.3.1 and 1.3.2 and move 1.3.1 and 1.3.2 to 1.4 and 1.5 respectively. For 1.3.2, modify to state "Internal company personnel notification(s) deemed necessary by the Responsible Entity". For 1.4, we feel the term "content" is too broad as used here. For example, if the FBI changes the contact info for the JTTF, the Responsible Entity may not find out until an incident or annual exercise. Or if the contact person for the state agency changes position without notifying us, it would require us to then change the plan within 90 days. We suggest an annual review of the plan is sufficient for the objective of this requirement.
Yes
Yes
No
We appreciate the effort the team has taken in improving the requirements since the last posting. We request the team

clarify if this also includes personnel observing and reporting the requirements or only those specifically listed in the plan. The measure seems to indicate it only includes those listed in the plan, but this is not clear in the requirement. If it includes those personnel involved in observing and notifying management, then this might include a significant portion of the organization. In either case, we feel the requirement should be modified as "…review applicable portions of its Impact Event Operating Plan...".
No
We appreciate the effort the team has taken in improving the requirements since the last posting. For R5, we suggest including the reporting form as part of the plan in R1. Otherwise, a violation of R5 would also indicate a violation of R2.
No
We appreciate the effort the team has taken in improving the requirements since the last posting. Event Forced Intrusion: The timeframe is very small given the possibly minimal risk to the BES. It often takes much longer than 1 hour after verification of intrusion to determine the intrusion was only for copper theft. We suggest a 24 hour time frame or tie the timeframe to the "verification of forced intrusion".
No
We applaud the drafting team's effort in crafting more meaningful measures. However, we have concerns with the measures reading like requirements in stating Responsible Entities "shall" do something. We suggest crafting the measures to provide acceptable, but not all exclusive, forms of evidence by stating something similar to "Acceptable forms of evidence may include…"
Yes
Yes
Yes
Yes
We appreciate the added context through the use of extended background information, rationale statements, and corresponding guideline and hope this context will remain in line with the Standards through the ballot and approval process. We have a few suggestions and questions related to this context. Our comments for this question relate to the contextual information. First of all, in the diagram on page 8, we suggest the appropriate question to ask is "Is event associated with potential criminal activity?" rather than "Report to Law Enforcement?" Also, it would be helpful to make clear the communication flow associated with the State Agency is the responsibility of the State Agency and not the Responsible Entity. This could be shown with a different colored background that calls this process out separately. In the rationale box for R3, it states "The DSR SDT intends…" We propose this should read similar to "The objective of this requirement is…" Overall, we suggest the SDT review the guidance document to make sure any changes made to the requirements are consistent with the guidance.
Individual
Joe Petaski
Manitoba Hydro
1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators, 6 - Electicity Brokers, Aggregators
No
”Situational Awareness” was replaced by the generic “Industry awareness”. Justification for this was that “Situational Awareness” was a “by product” of a successful event reporting system and not a “driver”. Using “Industry awareness” clouds the clarity of the purpose. If personal are properly trained and conscious of their responsibilities, then they are in fact “situationally aware”, and will therefore drive the reporting process on the detection an “Impact Event”. “Industry awareness” falsely labels this Standard as unique to the electrical industry when clearly many outside and international agencies will be notified and involved. “Situational Awareness” seems much more appropriate and encompassing. Other then that the Purpose is a large improvement from the original.
Yes
“Disturbance” has a unique and traditional meaning in the electrical industry, basically meaning “a notable electrical event causing in imbalance of load and generation”. Attempting to include the many scenarios can that can affect reliability blurred the current vision of “Disturbance” and the addition of “unusual occurrences” just added to the confusion. It never seemed appropriate to submit an “unusual occurrence” on a “Disturbance Report”. “Impact Event” is very encompassing and then detailed specifically in Attachment 1.
Yes
“Impact event”, The DSR SDT reasoning for this “A sabotage event can only be typically determined by law enforcement after the fact” is very creative and concise!
Yes
All registered entities are included. This means all field and office personal involved will create a 360 degree view of the

BES, and fulfill “Situational awareness of the industry”. In Attachment 1, the “Entity with Reporting Responsibility” entities vary. It might be clearer to leave all impact levels “Entity with Reporting Responsibility” as the RC, BA and TOP, as these are likely the only parties that will report as required. All other entities must report to the RC, BA and TOP.
Yes
Agree with R1, a central system for receiving and distributing reports. There is limited time and resources for control operators to follow up and ensure ALL required entities have received all information required in a timely manner. Agree with R7 and R8.
No
Plan, Process and Procedure are all too interchangeable with each other and have no value being used in “one paragraph” as they do not differentiate from one or other. The terms “identify”, “gather” and “communicate” better describe “Process, plan or procedure” so simplify to: 1.4. Identification of Impact Events as listed in Attachment 1. 1.5. Gathering information for inclusion into Attachment 2 regarding observed Impact Events listed in Attachment 1. 1.6. Communicate recognized Impact Events to the following:
Yes
Removing “assess the initial probable cause” from the statement removes the ambiguity in the same way as replacing sabotage with impact level. Let the staff trained in this field determine probable cause after the fact.
Yes
This requirement appears to be written so as to leave how each entity tests this procedure is up to them and not how. The testing of this procedure could vary vastly from entity to entity, meaning there is no set protocol on this procedure. As long as this requirement remains open, it is fair.
Yes
Removing the extreme details “within 30 days of revision” and “train before given responsibility” and giving leeway to when this training is necessary, will allow training to be integrated into other existing training schedules. Inclusion of 5.3 and 5.4 would require unique set of time lines and additional resources to monitor and implement.
Yes
The DOE-OE-417 appears more intuitive and descriptive (and on line ability), but having the either or option is fine. DOE-OE-417 Form is mentioned several time in this Standard, but no link to this document.
No
Reporting for CCA's should be limited to damage associated with a detected cyber security incident.
Yes
No
Reduce the Long Term Planning items to Lower VRF. The planning items will not have the same impact on the reliability of the system as real time operations.
Yes
Yes
Yes
Individual
Mike Albosta
Sweeny Cogeneration LP
5 - Electric Generators
Yes
Yes
No
The threshold for reporting what could be sabotage still leaves the door open for second guessing after-the-fact. For example, if graffiti is sprayed on a BES asset, the entity is to assume that the event is not to be reported. However, intent to harm the BES may be discovered at a later point – with ramifications to the entity who did not report it. A solution may be to strengthen footnote 3 to both reporting tables, which makes an allowance to report “if you cannot reasonably determine likely motivation” of sabotage. If acceptable methods to provide justifiable evidence that reporting was NOT required, then this loophole may be corrected.
No

In Attachment 1, Generator Operators who experience a ± 10% sustained voltage deviation for ≥ 15 continuous must issue a report For externally driven events, the GOP will have little if any knowledge of the cause or remedies taken to address it. We believe the language presently in EOP-004-1 is satisfactory that any “action taken by a Generator Operator” that results in a voltage deviation has to be reported by the GOP.
Yes
We agree that these requirements appropriately belong in the NERC Rules of Procedure. However, we are concerned with the multiple reporting requirements being driven by EOP-004-2, CIP-008-3, the ERO Events Analysis Team, the Reliability Assessment and Performance Analysis Group (RAPA). It is imperative that these efforts be consolidated into a single procedure using a single reporting template.
Yes
Yes
No
We doe not see a reliability benefit in the planning and execution of tests or drills to ensure that regulatory reporting is performed in a timely fashion. It is sufficient that penalties can be assessed against entities that do not properly respond in accordance with EOP-004-2, leaving it to us to determine how to avoid them.
Yes
Yes
No
In Attachment 1, Part A, Generator Operators who experience a ± 10% sustained voltage deviation for ≥ 15 continuous must issue a report For externally driven events, the GOP will have little if any knowledge of the cause or remedies taken to address it. We believe the language presently in EOP-004-1 is satisfactory that any “action taken by a Generator Operator” that results in a voltage deviation has to be reported by the GOP.
Yes
Yes
Yes
Yes
Yes
Individual
Thad Ness
American Electric Power
1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators, 6 - Electicity Brokers, Aggregators
Yes
No
The definition is too broad and vague. The text in the comment form has the following sentence “Only the events identified in EOP-004 – Attachment 1 are required to be reported under this Standard.” The definition should contain that caveat or something similar.
Yes
Yes
AEP agrees, but it further supports the notion that this standard should not apply to the IA, TSP, and LSE functions.
Yes
No
Even best developed plans, processes and procedures do not always lend themselves to address the issues at hand. There needs to be flexibility to allow entities to first address the reliability concern and second report correspondingly.

Currently, this requirement is overly prescriptive and places unnecessary emphasis on the means to an end and not the outcome. The outcome for this requirement is to report Impact Events.
No
Requirement 5 and Requirement 2 are redundant. We recommend Requirement 2 be replaced with the language in Requirement 5. “Each Responsible Entity shall report Impact Events in accordance with the Impact Event Operating Plan pursuant to Requirement R1 and Attachment 1 using the form in Attachment 2 or the DOE OE-417.”
No
It is unclear if actual events would qualify for a test in the requirement; however, the associated measure and rationale appear to support this. We suggest the requirement be restated to allow for actual events to count for this requirement.
Yes
No
This should be one step covered by the implementation in requirement 2. We like the ability to use one form (i.e. NERC Attachment 2 or the DOE-417); however, we would prefer to have this information only be reported once.
No
The time to submit a report for the inclusion of the damage or destruction of BES equipment, critical asset, or critical cyber asset is too aggressive. The critical cyber asset reporting is redundant with CIP-008. Furthermore, reporting equipment failures within an hour for Critical Assets is going to overwhelm operators that need to focus on the restoration efforts. Self-evident equipment failures at a Critical Asset (such as a tube leak at a generator which is a Critical Asset) should not be required to be reported. Maybe the wording should be stated as an “abnormal occurrence” rather than “equipment failure.” It would be helpful if there was a defining or a footnote that defines the nature and/or duration for loss of some equipment. For example, is a transmission loss for sustain or momentary outages?
Yes
No
With the scope of applicable functions expanding, more time will be required to develop broader processes and training. This will need to be extended for 18 months to get the process implemented and everyone trained.
We still do not agree that LSE, TSP and IA should be included in the applicability of this standard. Having processes to report to local or federal law enforcement agencies is “legislating the obvious”. The focus on this standard should only be on Impact Event reporting to reliability entities.
Group
Southern Company
Cindy Martin
Yes
Yes
There is concern that the proposed definition for Impact Event does not allow for prudent judgment and preliminary situational assessment by the entity to declare a Potential Impact Event (especially threats) as non-credible. The thresholds for reporting established in Attachment 1 – Part A provide a somewhat definitive bright line with regard to those events identified in Part A, but for some of the events in Part B there should be allowance for an assessment by the entity to reasonably determine whether the event poses a credible threat to the reliability of the BES. This is attempted in the footnote to the “Forced Intrusion” event in Attachment 1 – Part B, but we think this allowance for entity assessment and prudent judgment needs to apply more pervasively, perhaps by including the term “credible” in the definition of Impact Event or at least by adding the term “credible” wherever the term “physical threat” is used.
Yes
Yes
This will cause the duplication of reporting for some events. Reference EOP-004 Attachment 1: Impact Events Table; Event - Loss of Firm Load for ≥ 15 minutes (page 15 of standard) This requires the RC, BA, TOP, and DP to report. So if a storm front goes through our system and takes out 400MW of load in Alabama and Georgia the PCC would have to report as the RC, BA, and TOP. Alabama Power and Georgia Power would also have to report as DPs. The way it is now the PCC reports for any of these events.
Yes
Yes

Yes
Yes
This will cause all of the entities listed in R1.3.2 to receive test communications from all of the applicable entities annually.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
The implementation time should be 12 months after approval regardless of the elapsed time taken to get the standard approved.
Need guidance for incorporating disturbance reporting that is in CIP-008.
Individual
Andres Lopez
USACE
5 - Electric Generators, 9 - Federal, State, Provincial Regulatory, or other Government Entities
Yes
No
1) You cannot use the terms impact and event to define impact event. 2) The phrase “has the potential to impact” makes the definition too vague. Every action taken to modify the system or its components has the “potential to impact” the Bulk Electric System. 3) Recommend to change the definition to” “Any occurrence which has adversely affected the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action.”
No
The DSR SDT should have defined sabotage since it helps the SDT working on CIP standards further define its action. Sabotage can be defined as the deliberate act of destruction, disruption, or damage of assets to impact the reliability of the BES.
Yes
Yes
Yes
Yes
Yes
Yes
Yes

No
The "Potential Reliability Impact" table should be taken out. Refered to previous comment on our position on potentail impacts.
Yes
Yes
Yes
No
Yes
Individual
Nathaniel Larson
New Harquahala Generating Co.
1 - Transmission Owners, 5 - Electric Generators
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
M3. In the absence of an actual Impact Event, the Responsible Entity shall provide evidence that it conducted a mock Impact Event and followed its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The time period between actual and or mock Impact Events shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or documentation. (R3). The measure for R3 needs to make it clear that “exercise/drill/actual employment” can be a classroom exercise, utilizing scenarios for discussion. It should not be necessary to fully test the plan by making actual phone calls, notifications etc.
Yes
Yes
Yes
No
See R3 comments
Yes
Yes
Yes
Yes

Group
Bonneville Power Administration
Denise Koehn
Yes
Yes
Agree, but note that this will add many more situations to reporting and it will require more staff time to accomplish this.
Yes
Yes
Yes
Ensure distribution of trends.
No
Not sure that a 90-day update is needed to be sent to CEF.
No
Minimize the number of requirements. Not sure what the new R2 intends that is different than having a valid plan (signed?). Why can't R1 have develop and implement? R5 is the reporting. Implement should be with R1 or R5 depending on the interpretation.
No
Too burdensome to go through EACH and ALL individual Impacts and report each one on a drill basis with outside entities. One or two scenarios may be OK.
Yes
Yes
Reporting form OK. Note that the Frequency Maximum/Minimum Section should be clarified. A Gen Loss doesn't usually experience a high (maximum) frequency, just the low immediately following the event.
No
Generally OK, but there are too many events to report. The loss of 3 BES elements for a large geographic entity for a (5 county?) windstorm that has little impact to the system is not needed. 3 elements within the same minute could be acceptable and 6? elements still out within an hour ... or something to that affect could work.
Yes
No
R2, R3 and R4 should be lower VRFs than R5 and R1.
No
For R5 VSL's: suggest moving the 1-2 hours down one level to Moderate and move the >2 hours down to High with a range of 2-8 hours. Leave the "Failed to Submit" in the Severe category.
No
Depends on the answer to #7. If implementation means a signed and valid Plan, then it should be with Long Term. If reporting the events, then it should be Real-Time/Same Day Operations.
Yes
Work needed on Part A Damage or Destruction of BES equipment. The Note 1 is OK, but the Threshold doesn't match well. If a PCB is damaged by lightning or an earthquake, Note 1 (human action) doesn't require Reporting (proper interpretation), but the Threshold still requires "equipment damage".
Group
Midwest Reliability Organization
Carol Gerou
Yes
The addition of “industry awareness” adds to the scope of this Standard. Whereby an entity is required to inform the RC and others of actual and potential Impact Events.
No

The proposed definition is not supported by any of the established “bright line” criteria’s that are contained within attachment 1. This Results Based Standard should close any loop-holes that could be read into any section, especially the definition. According to rules of writing a definition, a definition should not contain part of the word that is being defined. Recommend the definition be enhanced to read: “Impact Event: Any Contingency which has either effected or has the potential to effect the Stability of the BES as outlined per attachment 1. Within this enhanced recommendation, presently defined NERC terms are used (Contingency and Stability), thus supporting what is current used within our industry. There is also a quantifiable aspect of “as outlined per attachment 1” that clearly defines Impact Events.
Yes
Sabotage is usually associated with a “malicious” attack. Entities have always lacked the clinical expertise to determine if an event was malicious or not. The Impact Event bright line criteria clearly states what the minimum reporting requirements are.
Yes
Yes
The ERO is not a user, owner or operator of the BES and the best place to contain their responsibilities, is in the Rules of Procedure.
Yes
This is a NERC defined term and will assist entities in maintaining compliance with this (proposed) Standard.
Yes
This clearly states that an entity’s Operating Plan is to be used for reporting of Impact Events.
Yes
Yes
Yes
This will reduce any double reporting to the ERO and FERC.
No
1) Section 9 of the Impact Reporting Form states: "List transmission facilities (lines, transformers, busses, etc.) tripped and locked out". But Part A of Attachment 1 states: "Three or more BES Transmission Elements". a. Should section 9 state: "List transmission facilities (lines, transformers, busses, etc.) tripped or locked out"? b. Should section 9 state: "List transmission elements (lines, transformers, busses, etc.) tripped or locked out"? This will align the reporting criteria with the actual reporting form. 2) Section 13 of the Impact Reporting Form states: "Identify the initial probable cause or known root cause of the actual or potential Impact Event if know at the time of submittal of Part I of this report:". Recommend that "of Part I" be removed since there is no Part 2. 3) Every Threshold in attachment 1 gives a clear measurable bright line, except: “Transmission Loss”. As presently written “Three or more BES Transmission Elements” could imply that a Report will be required to be submitted if a BES transmission substation is removed from service to perform maintenance. Or there could be three separate elements within a large substation that are out of service (and don’t effect each other) that will require a Report. Upon review of the TPL standards, there are normally planned items that our industry plans for. It is recommended that the Threshold for Reporting of Transmission Loss be enhanced to read: “Two or more BES Transmission Elements that exceed TPL Category D operating criteria or its successor”. This threshold now is based on a actively enforced NERC Standard, and each RC and TOP are aware of what this bright line is.
Yes
Yes
Yes
Yes
Yes
On the Impact Reporting Form, number 7,8,9,10, and 11 have an astrict (*) but nothing describes what the astrict means. Recommend a foot note be added to state: * If applicable to the reported Impact Event.
Group
SRP
Cynthia Oder

Yes
No
Suggest that definition include reference to the fact that this is non-desired occurence, as the word 'impact' has neither a positivie nor negative implication. This is not a well formed definition as it contains circular refernces to 'impacted' and 'event' within the definition.
Yes
No
The threshold for Reporting is broad, vague and repetitive. "Three or more BES Transmission Elements" is vauge and could be interpreted as 3 breakers in a large system.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Eric Salsbury
Consumers Energy
3 - Load-serving Entities, 4 - Transmission-dependent Utilities, 5 - Electric Generators
No
The definition of “Impact Event” seems very vague and nebulous. This definition should be modified to be clear and concise, such that entities clearly understand what is included within the definition.
No
EOP-004 does not appear to address a reliability need. Reporting “after-the-fact” information such as that described in “Impact Events” does not do anything to improve Bulk Electric System reliability. Therefore, we recommend that CIP-001 be updated to address sabotage events, and that NERC otherwise rely on the statutory reporting to the DOE that is represented by OE-417 for any “after-the fact” information. The remainder of our comments reflects detailed comments on the posted draft, presuming that our objection represented above will be disregarded.
No
Requirement R1, “Have a plan …” with all of the listed criteria, seems to present a serious compliance risk to applicable entities without a direct reliability benefit, as long as entities still indentify and report relevant events. Ad-hoc

procedures, as discussed within the R1 “Rationale” have been acknowledged within the rationale to be working effectively, and should remain sufficient without having a documented and by inference, signed, approved, dated document with revision history (as is being demanded today by compliance auditors wherever a “documented plan” is specified within the requirements).
No
We understand that DOE is migrating to an on-line reporting facility rather than the email-submitted OE-417. If they do so, the OE-417 will not be available for providing to NERC, and the reporting specified by EOP-004 will be duplicative of that for DOE. We recommend that NERC, RFC and the DOE work cooperatively to enable a single reporting system in which on-line reports are made available to all appropriate parties.
No
1. In reference to the Impact Event addressing “Loss of Firm load for greater than or equal to 15 minutes”, this is likely to occur for most entities most frequently during storm events, where the loss of load builds slowly over time. In these cases, exceeding the threshold may not be apparent until a considerable time has lapsed, making the submittal time frame impossible to meet. Even more, it may be very difficult to determine if/when 300 MW load (for the larger utilities) has been lost during storm events, as the precise load represented by distribution system outages may not be determinable, since this load is necessarily dynamic. Suggest that the threshold be modified to “Within 1 hour after detection of exceeding 15-minute threshold”. Additionally, these criteria are specifically storm related wide spread distribution system outages. These events do not pose a risk to the BES. 2. Many of the Impact Events listed are likely to occur, if they occur, at widely-distributed system facilities, making reporting “Within 1 hour after occurrence is identified” possibly impractical, particularly in order to provide any meaningful information. Please give consideration to clearly permitting some degree of investigation by the entity prior to triggering the “time to submit” 3. Referring to the “Transmission Loss” Impact Event, please provide more specificity. Is this intended to address : - anytime that three or more BES Transmission Elements are out of service, - only when three or more BES Transmission Elements are concurrently out-of-service due to unscheduled events, - only when three or more BES Transmission Elements are simultaneously automatically forced out-of-service, or - only when three or more BES Transmission Elements are forced from service in some proximity to each other? It is not unusual, for a large transmission system, that this many elements may be concurrently forced out-of-service at widely-separated locations for independent reasons. 4. Referring to the “Fuel Supply Emergency” Impact Event, OE-417 requires 6-hour reporting, where the Impact Event Table requires 1-hour reporting. The reporting period for EOP-004-2 should be consistent with OE-417. 5. For that matter, the SDT should carefully compare the Impact Event Table with OE-417. Where similar Impact Events are listed, consistent terminology should be used, and identical reporting periods specified. Where the Impact Event Table contains additional events, they should be clarified as being distinct from OE-417 to assist entities in implementation. Further, since OE-417 must be reviewed and updated every three years, EOP-004 should defer to the reporting time constraints within OE-417 wherever listed in order to assure that conflicting reporting requirements are not imposed.
No
We understand that DOE is migrating to an on-line reporting facility rather than the email-submitted OE-417. If they do so, the OE-417 will not be available for providing to NERC, and the reporting specified by EOP-004 will be duplicative of that for DOE. We recommend that NERC, RFC and the DOE work cooperatively to enable a single reporting system in which on-line reports are made available to all appropriate parties.
No
1. In reference to the Impact Event addressing “Loss of Firm load for greater than or equal to 15 minutes”, this is likely to occur for most entities most frequently during storm events, where the loss of load builds slowly over time. In these cases, exceeding the threshold may not be apparent until a considerable time has lapsed, making the submittal time frame impossible to meet. Even more, it may be very difficult to determine if/when 300 MW load (for the larger utilities) has been lost during storm events, as the precise load represented by distribution system outages may not be determinable, since this load is necessarily dynamic. Suggest that the threshold be modified to “Within 1 hour after detection of exceeding 15-minute threshold”. Additionally, these criteria are specifically storm related wide spread distribution system outages. These events do not pose a risk to the BES. 2. Many of the Impact Events listed are likely to occur, if they occur, at widely-distributed system facilities, making reporting “Within 1 hour after occurrence is identified” possibly impractical, particularly in order to provide any meaningful information. Please give consideration to clearly permitting some degree of investigation by the entity prior to triggering the “time to submit”. 3. Referring to the “Fuel Supply Emergency” Impact Event, OE-417 requires 6-hour reporting, where the Impact Event Table requires 1-hour reporting. The reporting period for EOP-004-2 should be consistent with OE-417.
No
1. In reference to the Impact Event addressing “Loss of Firm load for greater than or equal to 15 minutes”, this is likely to occur for most entities most frequently during storm events, where the loss of load builds slowly over time. In these cases, exceeding the threshold may not be apparent until a considerable time has lapsed, making the submittal time frame impossible to meet. Even more, it may be very difficult to determine if/when 300 MW load (for the larger utilities)

has been lost during storm events, as the precise load represented by distribution system outages may not be determinable, since this load is necessarily dynamic. Suggest that the threshold be modified to “Within 1 hour after detection of exceeding 15-minute threshold”. Additionally, these criteria are specifically storm related wide spread distribution system outages. These events do not pose a risk to the BES. 2. Many of the Impact Events listed are likely to occur, if they occur, at widely-distributed system facilities, making reporting “Within 1 hour after occurrence is identified” possibly impractical, particularly in order to provide any meaningful information. Please give consideration to clearly permitting some degree of investigation by the entity prior to triggering the “time to submit”. 3. Referring to the “Fuel Supply Emergency” Impact Event, OE-417 requires 6-hour reporting, where the Impact Event Table requires 1-hour reporting. The reporting period for EOP-004-2 should be consistent with OE-417.
No
1. We appreciate the aggregation of redundant standards on this subject, but have some concerns about the content of the aggregated standard as listed below and in reference to previous questions on this comment form. 2. It is not clear whether an event that meets OE-417 reporting criteria but is not defined within EOP-004-2 is an Impact Event; for example, “loss of 50,000 or more customers for 1 hour or more” is required to be reported to DOE as a OE-417 type 11 event but it is not clear whether EOP-004-2 requires that such events be also reported to NERC. The “Reporting Hierarchy” flow chart seems to suggest that any OE-417 must still be filed with NERC/RE. If the flow chart is not consistent with the intent of the Requirements, it must be clarified. 3. NERC implies active involvement of law enforcement. This assumes that law enforcement has the resources to be involved in an Impact Event investigation and fulfill the standard reporting requirements. This is an unrealistic expectation as we have experienced first-hand, a lack of response by law enforcement agencies as their resources shrink due to economic issues. Additionally, NERC is asking that we place credence in law enforcement, on our behalf, to make a definitive decision about the reporting of events. Refer to page 6 of EOP-004-2 under “Law Enforcement Reporting”: “…Entities rely upon law enforcement agencies to respond and investigate those Impact Events which have the potential of wider area affect…” In many cases, the internal security function must work with system operations personnel to thoroughly understand the system and the effects of certain events. It is unrealistic to think law enforcement would be in a position to make BES decisions within the timeframe given without having system operations experience. It is our experience that external agencies do not understand the integration / inter-connectivity, resiliency, or implications of our energy infrastructure. 4. Within Michigan, a “Michigan Fusion Center: Michigan Intelligence Operations Center (MIOC)” has been established. - Today, we share information such as substation issues and identity theft (not internal issues) to the MIOC. The MIOC is trending incidents on critical infrastructure assets and sectors around the state. The private sector is encouraged to report to the Fusion Center. If NERC is collecting this type of information for future studies and trending / analysis, they should coordinate with each state’s Fusion Center.
Individual
Michael Falvo
Independent Electricity System Operator
2 - RTOs and ISOs
Yes
Yes
We do not have any issue with the wording of the definition, but question the need for this definition since by itself the term is not specific on the types of events that are regarded as having an “impact”. The detailed listing of events that fall into a reportable event category, hence the basis for the Impact Event, is provided in Attachment A. For that matter, these events that are to be reported can be called anything. Defining the term Impact Event does not serve the purpose of replacing the details in Attachment A, and such a term is not used anywhere else in the NERC reliability standards. In fact, for the term Impact Event to be fully defined, all the elements in Attachment A must become a part of it. We therefore suggest the SDT to consider not defining the term Impact Event, but rather use words to stipulate the need to have a plan, to implement the plan and to report to the appropriate entities those events listed in Attachment A.
Yes
We agree since it is more important to report suspicious events than to determine if an event is caused by sabotage before it gets reported.
No
We disagree with the following inclusion/exclusion of several entities: a. We assess that the applicable entities listed in Section 4 capture all the entities that are assigned a reporting responsibility in Attachment 1 of the standard. While some events in Attachment 1 have specific entities identified as responsible for reporting, certain events refer to the entities listed in specific standards (e.g. CIP-002) as the responsible entities for reporting. The latter results in IA, TSP and LSE (none of which being specifically identified as having a reporting responsibility) being included in the Applicability Section. If our reasoning is correct, we question why NERC was dropped from the Applicability Section as it is an applicable entity identified in CIP-002-3. b. If the above approach was not strictly followed, then we’d suggest the SDT review the need to include IA, TSP and LSE since they generally do not own any Critical Assets and hence will likely not own any Critical Cyber Assets.

Yes
Yes
Yes
Yes
Yes
No
R5 stipulates the use of Attachment 2 or the DOE-417, which is the vehicle for reporting only. This is the “how” part, not the “what”. The vehicle for reporting can easily be included in R2 where an entity is required to implement (execute) the Operating Plan upon detection of an Impact Event. We suggest the SDT combine R2 with R5.
No
As indicated under Q4, we question the need to include IA, TSP and LSE in the responsible entities for reporting.
No
We do not have any issues with Measures M1, M2 and M4, but have a concern with M3 and a couple of concerns with M5: M3: This Measure contains a requirement for the Responsible Entities to conduct a mock Impact Event. We disagree to have this included in the Measure. R3 requires the Responsible Entity to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The Measure should adhere to this condition only. We suggest to change the wording to: The Responsible Entity shall provide evidence that it conducted a test of it its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The time period between actual and or mock Impact Events shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, documentation or a report on an actual Impact Event. M5: a. As suggested above, R5 should be combined with R2; b. If R5 to remain as is, then M5 goes beyond the requirement in R5 in that it asks for evidence to support the type of Impact Event experienced. Attachment 2 already requires the reporting entity to provide all the details pertaining to the Impact Event. It is not clear what kind of additional evidence is needed to “support the type of Impact Event experienced”. Also, the date and time of the Impact Event is provided in the reporting from. Why do we need to provide additional evidence on the date and time of the Impact Event?
No
If R5 were to remain as is, then the VRF should be a Lower, not a Medium since R5 stipulates the form to be used. It is a vehicle to convey the needed information, and as such it is an administrative requirement. Failure to use the form provided in Attachment 2 or the DOE form does not give rise to unreliability.
We do not have any major issues with the proposed VSLs. However, in view of our comments on some of the Questions, above, we reserve our comments upon seeing a revised draft.
No
For the purpose of developing and updating an Impact Event Operating Plan, there should not be any requirements that fall into the Long-term planning horizon. As the name implies, the plan is used in the operating time frame. And consistent with other plans such as system restoration plan which needs to be updated and tested annually, most of the Time Horizons in that standard (EOP-005-2) are either Operations Planning or Real-time Operations. We suggest the Time Horizon for R1, R3 and R4 be changed to Operations Planning.
Yes
Group
Western Electricity Coordinating Council
Steve Rueckert
Yes
No
We question the need for a defined term. It appears that an Impact Event is any event identified in Attachment 1. The use of the defined term combined with the language of Requirement 2 to implement the Impact Event Opeating Plan for Impact Events listed in Attachment 1 may be confusing. Is an Impact Event any event described by the proposed definition or is an Impact Event any event listed in Attachment 1?
Yes

Yes
Yes
Yes
Are "Law Enforcement" considered a "Governmental Agency" (they are listed separately and both required) If not, is there any qualifiers on whether Law Enforcement or Governmental Agency refers to municipal, county, state or federal or any combination? Since the term "Provincial" is associated with "Governmental" it tends to indicate State level. As it is written now an auditor would require documentation of “some” Law Enforcement (other than company security) and an additional communication to at least “some” Agency which could be considered Governmental. Municipal or higher. Contact with City police or Sheriff and either city or county government rep would satisfy. Additional clarity would would help from a compliance enforcement perspective.
Yes
Yes
Yes
Yes
Yes
Regarding the proposed VSLs for R3, since communication testing involves multiple parties it would be more appropriate to base severity level on the number of applicable parties which were not tested rather than how long after 15 months it took to do the test. The standard already builds in a 3 month leeway, In reality the way it is written almost guarantees a lower severity level.
Actual Reliability Impact Table comments: Note that per the NERC glossary "Energy Emergency" only is defined for an LSE. Energy Emergency is the precursor term in the first three lines. Thus logically an LSE is the only entity which would be initiating the event and responsible for reporting for first three items. We don't believe that is the intent. We suggest you consider just eliminating “Energy Emergency” and going with: • Public appeal for load reduction • system-wide voltage reduction • manual firm load shedding For Loss of Off site power at Nuc Station is reporting really expected of each of the entities listed? (lots of reports) We suggest you consider just the Nuclear GOP and perhaps the associated TOP. Perhaps you could use the CIP approach as in the next two rows and say Applicable GOP and Transmission Entities under NUC-001-2 Potential Reliability Impact Table Comments: For Fuel Supply Emergency, Forced Intrusion, Risk to BES Equipment, Cyber Security Incident where owner/operator are both listed (GO/GOP or TO/TOP) could consider perhaps reporting to be assigned to only one rather than both.
Group
PPL Supply
Annette Bannon
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Reporting consistency and timelines may need to reviewed for example: Fuel Supply Emergency - OE-417 requires reporting within 6 hours / Attachment 1 Part B requires reporting within 1 hour.
No
Recommendation: Add a column in Attachment 1 to acknowledge the events that require a OE-417 Report and list the number under Schedule 1 that required the OE-417 Report. This would add accuracy and consistency among reporting entities.
Yes
Yes
Individual
Kirit Shah
Ameren
1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators, 6 - Electicity Brokers, Aggregators
No
The original Purpose wording was clear, concise and understandable.
No
The documentation from the SDT included the reliability objective for EOP-004-2 which should be included in the definition of Impact Event. Our suggested alternate defintion for Impact Event: "An Impact Event is any event that has either caused, or has the likely potential to cause, an outage which could lead to Cascading. Such events will be identified as being caused by, to the best of the reporting entity's information: (1) equipment falure or equipment mis-operation, (2) environmental conditions, and/or (3) human actions." This alternate wording includes the reliability objective and clarifies the three known, or likely, causes of the Impact Event.
No
The SDT did not further define sabotage as directed by FERC, but instead created a new term that does not address the order. The Term Impact Event has no clarity or quantitative qualities by which an entity can determine what sould be reported. the use of the phrase "has the potential to impact reliability" has such a vague scope, an auditor can interpret to mean any "off-normal" condition, which makes this standard impossible to comply with. The SDT should use the DOE definition of sabotage as follows: Sabotage – Defined by Department of Energy (DOE) as: • An actual or suspected physical or Cyber attack that could impact electric power system adequacy or reliability • Vandalism that targets components of any security system on the Bulk Electric System • Actual or suspected Cyber or communications attacks that could impact electric power system adequacy or vulnerability, including ancillary systems which support networks (e.g. batteries) • Any other event which needs to be reported by the Balancing Authority (Transmission Operations) to the Department of Energy. Sabotage can be the work of a single saboteur, a disgruntled employee or a group of individuals.
No
The 1 hour reporting requirement, as reference in Attachment 1 is inappropriate. In the event an "Impact Event" were to be dicovered the Responsible Entity should focus on public and personnel saftey. The reporting requirement should read "Within 1 hour or as soon as conditions are deemed to be safe." This statement would be applicable to "Damage or destruction of Critical Asset" The SDT should not put personnel in the position of choosing to either comply with NERC or address public or co-worker safety. The Time to Submit Report states "within 1 hour after occurrence is identified" This gives an auditor a wide area to question. If personnel report the occurrence 1 hour after identified, but 24 hours after it occurred, we are subject to the personal beliefs of the auditor that the event was not identied 24 hours ago, and reported 24 hours late. This will also be difficult to measure as the operator will have to document in the plant log the time the event was identified, while possibly dealing with Emergency Conditions. In the Note above the Actual Reliability Impact Table, the SDT identifies that under certain conditions, NERC / RRO staff may not be available for continuous 24 hour reporting. The SDT should consider the same stipulations apply to operating personnel and they should not be held to a higher standard that NERC / RRO.

No

The "Responsible Entity" should be limited to those functions with the most oversight such as the BA, RC, or TOP. Otherwise there will be multiple DOE OE-417 reports sent by multiple entities.

No

See response to question 4.

Yes

The following is a list of our greatest concerns. (1) We are concerned about the lack of definitions and use of critical non-capitalized terms. As an example, there is a reportable Impact Event if there is a +/- 10% Voltage Deviation for 15 minutes or more on BES Facilities. As a first example, why is the term Voltage Deviation capitalized when it is not in the NERC Glossary and not proposed to be added? Where is the deviation measured - at any BES metering device? What is the deviation to be reported - the nominal voltage? the high-side of the Voltage Schedule? the low-side of the Voltage Schedule? the generator terminals? when a unit is starting up? All of these are possible interpretations, but < 1% of them would ever result in a Cascading outage - which is the reliability objective of this Standard. A second example is a Generation loss. The threshold for reporting is 2,000 MW, or more, for the Eastern or Western Interconnection. Is this simultaneous loss of capacity over the entire Interconnection? Or, cumulative loss within 1 hour? Or, cumulative loss within 24 hours? How many individual GOPs have responsibility for > 2,000 MW? It seems this would more effectively apply only to an RC and/or BA. The likelihood that one GOP would lose that much generation at once is probably remote. A third example would be the damage or destruction of BES equipment event. The term "equipment" was left lower case with a footnote explanation that includes "…due to intentional or unintentional human action…". This is likely to require the determination of intent by the human involved, which will almost certainly impossible to determine within the 1 hour reporting time. Also, what is the definition of the terms "damage" and "destruction"? Once again, if the reliability intent is to ONLY report Events that have a likely chance of leading to Cascading, this will greatly reduce the potentially enormous reporting burden. that could result without this type of clarification. (2) Without a very thorough understanding of the definitions of the terms requiring reporting, the 1 hour reporting constraint on most events will likely require that we frequently overreport events to minimize any chance of non-compliance. A webinar explaining expected reporting requirements would very useful and valuable. It is also unclear why so many Impact Events require such a short reporting time period. There will almost certainly be many times at 2:00 AM on a weekend when experts and the appropriate personnel will be available to quickly analyze an event and decide, within 1 hour, if a report is necessary. (3) Have all the new Impact Event reporting requirements been checked against reporting requirements from other Standards? For example, the Voltage Deviation Event would appear to potentially overlap/conflict with instructions from a TOP for VAR-002 compliance. Since VAR-002-2 is now in draft, has the SDT worked with that Team to determine if the requirements dovetail?

Individual

Kathleen Goodman

ISO New England, Inc

2 - RTOs and ISOs

No

The purposed states “To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of Impact Events and their causes, if known, by the Responsible Entities.” Awareness by who in the industry?

No

We question the need for this definition since by itself the term is not specific on the types of events that are regarded as having an “impact”. The detailed listing of events that fall into a reportable event category, hence the basis for the Impact Event, is provided in Attachment A. For that matter, these events that are to be reported can be called anything, or just simply be titled “Event to be Reported” without having to define them. Defining the term Impact Event does not serve the purpose of replacing the details in Attachment A, and such a term is not used anywhere else in the NERC reliability standards. In fact, for the term Impact Event to be fully defined, all the elements in Attachment A must become a part of it. We therefore suggest the SDT to consider not defining the term Impact Event, but rather use words to stipulate the need to have a plan, to implement the plan and to report to the appropriate entities those events listed in Attachment A. If the SDT still wishes to retain a definition despite our reservations noted above, we strongly suggest an improvement. The proposed definition of Impact Event is overly broad because of the use of “potential to impact” and the “Such as” list. Consider that routine switching has the potential to result in a mis-operation. In that regard most routine switching could be interpreted as an impact event. The “Such as” list should be struck and “potential” language should be struck. An alternative definition to consider: An Impact Event is any deliberate action designed to reduce

BES reliability; unintended accident that could result in an Adverse Reliability Impact; or an unusual natural event that causes or could cause an Adverse Reliability Impact.
Yes
We agree since it is more important to report suspicious events than to determine if an event is caused by sabotage before it gets reported.
No
We disagree with the following inclusion/exclusion of several entities: a. We acknowledge that the applicable entities listed in Section 4 capture all the entities that are assigned a reporting responsibility in Attachment 1 of the standard. While some events in Attachment 1 have specific entities identified as responsible for reporting, certain events refer to the entities listed in specific standards (e.g. CIP-002) as the responsible entities for reporting. The latter results in IA, TSP and LSE (none of which being specifically identified as having a reporting responsibility) being included in the Applicability Section. If our reasoning is correct, we question why NERC was dropped from the Applicability Section as it is an applicable entity identified in CIP-002-3. b. If the above approach was not strictly followed, then we'd suggest the SDT review the need to include IA, TSP and LSE since they generally do not own any Critical Assets and hence will likely not own any Critical Cyber Assets. c. There is still significant duplicate reporting included. For instance, why do both the RC and TOP to report voltage deviations? As written, a voltage deviation on the BES would require both to report. The same would hold true for IROLs. Perhaps IROLs should only be reported by the RC to be consistent with the recently FERC approved Interconnection Reliability Operating Limit standards.
Yes
No
We do not believe that the use of the Operating Process, Operating Procedure, and Operating Plan for a reporting requirement is consistent with their definitions nor with the intent of the definitions. For instance, an Operating Process is intended to meet an operating goal. What operating goal does this requirement meet? An Operating Procedure includes tasks that must be completed by "specific operating positions". This reporting requirement could be met by back office personnel. We suggest that R1.3.2 delete the list of entities to notify. The terms used to identify who to notify are not defined terms and can lead to subjective interpretations. As written, the requirement does not aid the Applicable entity or the Compliance enforcers in clearly including or excluding who to notify. We also believe that parts 1.3 and 1.3.2 under Requirement 1 will require notification of law enforcement agencies for all Impact Events defined in Attachment 1. While some should require notification to law enforcement such as when there has been destruction to BES equipment, others certainly would not. For instance, law enforcement does not need to know that an IROL violation, generation loss or voltage deviation occurred. We believe the reporting time lines are too aggressive for some events. Reporting events within an hour is not reasonable as an entity may still be dealing the event. This will be particularly difficult when support personnel are not present such as during nights, holidays and weekends. We further suggest that as explicit statement that "reliable operations must ALWAYS take precedence to reporting times" be included in the standard.
No
Fuel Supply Emergency is not a defined condition. We suggest that the SDT poll the ballot body regarding the reporting of Fuel Supply Emergencies. Fuel Supply is an economic consideration and the concept of Fuel Supply Emergency is subjective. A resource that uses coal or oil may vary its supplies based on economic considerations (the price of the fuel). For a conservative BA a fuel-on-demand supply line can be viewed as a fuel supply emergency whereas the resource owner sees the matter as good business. Moreover, the release of such reports to the public can have unintended consequences. Fuel disruptions caused by contract negotiations when reported to the public can result in non-union transportation employees being physically harmed by fuel supply organizers thus resulting in the loss of non-contract fuel. Further, this information may aggravate the situation by causing the cost of fuel to be inflated by suppliers when demand is great. If this event is not deleted, then we would suggest that the definition be constrained to "declared" fuel supply emergencies. Suggest the deletion of category: Risk to BES equipment. Because of the broad definition of BES, the risk to BES equipment is overly broad and can be applied to any risk to any "part of" any BES asset. The footnote helps identify what the SDT was intending, however, the words themselves can result in overly broad findings by compliance enforcement people.
No
We appreciate and agree with the drafting team recognizes that actual implementation of the plan for a real event should qualify as a "test". However, we are concerned that review of this requirement in isolation and without the benefit of the background material and information provided by the drafting team may cause a compliance auditor to believe that a test cannot be met by actual implementation. Furthermore, we do not believe testing a reporting procedure is necessary. Periodic reminders to personnel responsible for implementing the procedure make sense but testing it does not add to reliability. If they don't report an event, it will become obvious to compliance auditors. Recommend using language similar to CIP-009. "Each Responsible Entity shall conduct a an exercise of its operating process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 at least annually, with no more than 15 calendar months between exercises. An exercise can range from a paper drill, to a full operational exercise, to reporting of actual incident Also, we question the need to conduct a test annually. Since this is only a reporting Standard and, as such, has no direct impact on reliability, we suggest modifying the testing

requirement to once every three years.
Yes
No
R5 stipulates the use of Attachment 2 or the DOE-417, which is the vehicle for reporting only. This is the “how” part, not the “what”. The vehicle for reporting can easily be included in R2 where an entity is required to implement (execute) the Operating Plan upon detection of an Impact Event. We suggest the SDT combine R2 with R5.
No
As indicated under Q4, we question the need to include IA, TSP and LSE in the responsible entities for reporting. There is still significant duplicate reporting included. For instance, why do both the RC and TOP to report voltage deviations? As written, a voltage deviation on the BES would require both to report. The same would hold true for IROLs. Perhaps IROLs should only be reported by the RC to be consistent with the recently FERC approved Interconnection Reliability Operating Limit standards. Also, the CIP reporting requirements duplicate was is already contained in the CIP Standards, specifically CIP-008. Also, we are required to intentionally destroy Critical Cyber Assets when they are retired, why would we be required to report this?
No
We do not have any issues with Measures M1, M2 and M4, but have a comment on M3 and a couple of concerns with M5: M3: This Measure contains a requirement for the Responsible Entities to conduct a mock Impact Event. We disagree to have this included in the Measure. R3 requires the Responsible Entity to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The Measure should adhere to this condition only. We suggest to change the wording to: The Responsible Entity shall provide evidence that it conducted a test of it its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The time period between actual and or mock Impact Events shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, documentation or a report on an actual Impact Event. M5: a. As suggested above, R5 should be combined with R2; b. If R5 to remain as is, then M5 goes beyond the requirement in R5 in that it asks for evidence to support the type of Impact Event experienced. Attachment 2 already requires the reporting entity to provide all the details pertaining to the Impact Event. It is not clear what kind of additional evidence is needed to “support the type of Impact Event experienced”. Also, the date and time of the Impact Event is provided in the reporting from. Why do we need to provide additional evidence on the date and time of the Impact Event? c. We disagree with Measurement 4. It implies that the review must be conducted in person. Why couldn’t other means such as web training or a reminder memo not satisfy the requirement?
No
If R5 is to remain as is, then the VRF should be a Lower, not a Medium since R5 stipulates the form to be used. It is a vehicle to convey the needed information, and as such it is an administrative requirement. Failure to use the form provided in Attachment 2 or the DOE form has no impact on reliability. All violation risk factors should be Lower. All requirements are administrative in nature. While they are necessary because a certain amount of regulatory reporting will always be required, a violation will not in any direct or indirect affect reliability.
We do not have any major issues with the proposed VSLs. However, in view of our comments on some of the Questions, above, we reserve our comments upon seeing a revised draft.
No
For the purpose of developing and updating an Impact Event Operating Plan, there should not be any requirements that fall into the Long-term planning horizon. As the name implies, the plan is used in the operating time frame. And consistent with other plans such as system restoration plan which needs to be updated and tested annually, most of the Time Horizons in that standard (EOP-005-2) are either Operations Planning or Real-time Operations. We suggest the Time Horizon for R1, R3 and R4 be changed to Operations Planning. The Time Horizon for R2 and R5 should be changed to Operations Assessment since they both deal with after the fact reporting.
Yes
Under the “Law Enforcement Reporting” it is stated “The Standard is intended to reduce the risk of Cascading involving Impact Events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.” We question whether a reporting standard can “reduce the risk of cascading” and wonder if the reference to the threat “around them” refers to law enforcement? We would expect that the appropriate operating personnel are the only entities that would be able to mitigate the potential risk to the BES. As it currently stands there is a potential duplication between the reporting requirements under EOP-004-2 (i.e. Attachment 2 Form) and the ERO Event Analysis Process that is undergoing field test (i.e. Event Report Form). This will result in entities (potentially multiple) reporting same event under two separate processes using two very similar forms. Is this the intent or will information requirements be coordinated further prior to adoption in order to meet the declared objective that the impact event reporting under EOP-004 be “the starting vehicle for any required Event Analysis within the NERC Event Analysis Program?
Individual
Deborah Schaneman

Platte River Power Authority
1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators, 6 - Electicity Brokers, Aggregators
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Pacific Northwest Small Public Power Utility Comment Group
Steve Alexanderson
Yes
No
We believe that facilities used in the local distribution of electric energy should be excluded from these requirements due the language of 16 U.S.C. § 824o(a)(1) and 16 U.S.C. § 824o(i)(1).
Yes
No
1.4 makes no sense. The operating plan update and the change to its content occur simultaneously. Perhaps the SDT meant to say “Provision(s) for updating the Impact Event Operating Plan within 90 days of identification of a needed change to its content. This would be consistent with the “lessons learned” language of the prior version.
Yes

Yes
Yes
Yes
No
The comment group is composed of smaller entities that do not all maintain 24/7 administrative support. While many of the 1 hour reporting thresholds do not affect us, some do. Others may come into play as standards are revised, such as the CIPs. We ask the SDT to consider the identification or verification that starts the clock on these may come at inopportune times for meeting a one hour deadline for these entities. Restoration may be delayed in an attempt to meet these time limits. Safety should always be the number one priority, and restoration and continuity of service second. We see reporting of these events much further down the list. We note that FERC order 693, paragraph 471 does not dictate a specific reporting time period and therefore we suggest timing requirements that promote situational awareness but allow smaller entities needed flexibility. FERC order 693, paragraph 470 directed the ERO to consider "APPA's concerns regarding events at unstaffed or remote facilities, and triggering events occurring outside staffed hours at small entities." Our comment group does not believe the SDT has adequately responded to APPA's concerns but rather took the 1 hour Homeland security requirement referenced in paragraph 470 verbatim. While a report within an hour might be ideal, it is not always practicable. We suggest: 1) as soon as possible after service has been restored to critical services within the service territory, or 2) By the COB the first business day after discovery. Our comment group realizes the difficulty in wording standards/requirements that lump small entities in with larger ones and we believe our suggestion achieves some balance. Expecting smaller entities to achieve timing requirements that can only be normally met under ideal conditions at large entities is not feasible or fair.
No
It is unclear when reporting to the Compliance Enforcement Authority is required. Does the registered entity report initially, and then anytime a change to the plan is made, or a drill is performed. Or is the information only provided following a request of the Compliance Enforcement Authority, and if so what is the acceptable time limit to respond?
All five requirements refer to Attachment 1 Part A either directly, or indirectly by referring to R1 plans. Attachment 1 Part A, though, only provides the thresholds required for reporting (R5). No thresholds are provided for planning (R1) or the requirements referencing the plan (R2-R4). Strictly interpreted, an entity would be required to plan for any amount of firm load loss exceeding 15 minutes (for example), implement the plan for any amount and then report only those events that exceeded the applicable 200 or 300 MW level. An entity that had a peak load of less than 200 MW would still need to meet R1-R4 regarding load loss. We believe the SDT intended to use common thresholds for all the requirements. Suggest relabeling the Attachment 1 Part A column header from "Threshold for Reporting" to "Threshold." We also fail to see how an entity's size in MWh affects the threshold for reporting firm load loss.
Group
PSEG Companies
Patricia Hervochon
Yes
Yes
Yes
No
The PSEG Companies believe the defining language, roles and responsibilities outlined in Attachment 1 are unclear and inconsistent. For example fuel supply emergency reporting footnote 2 "Report if problems with the fuel supply chain result in the projected need for emergency actions to manage reliability" attempts to clarify the condition for reporting but does not. Whose "emergency actions" are being referred to in the footnote? It is not clear if those actions would be related to the specific station or the overall Bulk Electric System (BES). Can this be interpreted to imply a gas supply issue to one generating station as the result of pipeline maintenance, or local pressure issues would also requiring reporting? The PSEG Companies believe the definition of a fuel supply emergency needs to be more specific and less open to broad interpretation. In addition, the "Time to Submit Report" section of attachment 1 has a significant number of changes from the previous version. Accelerating the twenty four (24) hour to one (1) hour requirement for submitting the reports for several of the events takes resources away from managing the actual event.For the above

comments failure to submit a report within 1 hour is a high or severe VSL for a fuel supply emergency. This approach seems inconsistent with ensuring the operation and reliability of the BES. One (1) hour reporting, in most cases, is not adequate time to compile the needed information, prepare report, ensure the accuracy, submit, and simultaneously manage the actual event. We recommend 24 hour reporting for: Damage or destruction to BES, Fuel Supply Emergency, Forced Intrusion, and Risk to BES equipment sections of Attachment 1.
Yes
No
The PSEG Companies believe that sections 1.3 and 1.3.2 will require notification of law enforcement agencies for all Impact Events defined in Attachment 1. This is appropriate for some events if there has been destruction to BES equipment, for example, but not in certain operational events. It should not be necessary to notify law enforcement that a non sabotage event like an IROL violation, generation loss or voltage deviation has occurred.
No
Fuel supply emergency, as discussed in response to question 4 above, is not a defined condition. This event should be removed.
Yes
Yes
Yes
No
For the reasons cited in response to question 4 above the language roles and responsibilities remain inconsistent and unclear. The Time to Report changes are unreasonable and there is significant duplicate reporting required.
Yes
No
If Requirements 1-5 remain intact the Violation Risk Factor should be reduced to a Lower not a Medium since this is an administrative requirement and does not impact the reliability of the BES.
Individual
Phil Porter
Calpine Corp
5 - Electric Generators
No
The purpose has moved significantly from the originally approved SAR. The purpose should focus on reporting requirements for reporting electrical disturbances to the Bulk Electric System that exceed specific thresholds. Sabotage/vandalism/theft are a subset of the reportable events that could have or do cause a Bulk Electric System Electrical Disturbance. The Standard's content should focus on setting requirements to report specific types of electrical disturbance events and providing guidance for performing that reporting. Alternative language: Purpose: To establish reporting requirements for events that either cause, or have the potential to cause, significant disturbances on the Bulk Electric System.
No
Adding a definition for "Impact Event" is unnecessary and does not provide useful clarification of the actual reporting requirement for events that either impact the Bulk Electric System or have the potential to impact the Bulk Electric System. The all-encompassing nature of the proposed definition seems to conflict with the finite listing of events that actually require reporting. Although FERC specifically requested additional clarification of the term "sabotage" to clarify reporting requirements, the Drafting Team is correct in noting that "sabotage" implies intent and that the intent of human acts is not always easily determined. The fact that intent is not always determinable within the reporting timeframe can be dealt with more simply by requiring (in attachment 1) that human intrusions that have not been identified within the reporting timeframe as theft or vandalism should be reported as potential sabotage pending further clarification. This approach negates the need for an additional definition that may cause confusion regarding which events are reportable and eliminates the potential for under-reporting based on the assumption that the cause might be theft or vandalism.
No

The additional definition for “Impact Event” is unnecessary and does not provide useful clarification regarding actual reporting requirements. Sabotage, whatever the exact definition used, implies intent to damage or disrupt. The committee correctly notes that determination of actual intent is not always readily available. However, adding a general expansive definition encompasses all events that might disrupt the Bulk Electric System does not add clarity to the types of events that require reporting – which are listed in detail in Attachment 1. The issue can be more simply addressed by replacing the item “Human Intrusion” on Attachment 1, as follows: Event: Sabotage (note 3) Entity with Reporting Responsibility: All affected Responsible Entities listed in the Applicability Section of this Standard. Threshold for Reporting: Forced Intrusions at a BES facility that have not been determined within the reporting period to be theft or vandalism that does not affect the operability of BES equipment. Note 3 For purposes of reporting under Attachment 1, reportable sabotage includes all forced intrusions at BES facilities that have potential to cause, or cause, any of the disturbance events listed in Attachment 1 and have not been determined to be theft or vandalism that did not result in any event listed in Attachment 1. Responsible Entities are not required to report incidents of theft or vandalism that do not result in disturbance events. This approach also eliminates the need to reference copper theft as a particular type of theft that does not require reporting.
No
Expanding the current applicability of CIP-001-1 and EOP-004-1 to the GO function is unnecessary and will result in numerous duplicate reports, self-certifications, spot checks, and audits reviews, with no benefit to the reliability of the Bulk Electric System. The GOP is the appropriate applicable entity for generation facilities.
Yes
No
In the “Rationale for R1”, the draft states “Every industry participant that owns or operates elements or devices on the grid has formal or informal process, procedure, or steps it takes to gather information regarding what happened and why it happened when Impact Events occur. This requirement has the Registered Entity establish documentation on how that procedure, process, or plan is organized.” Absent substantial evidence that the proposed requirement addresses an actual systemic problem with the “formal or informal process, procedure, or steps it takes” for internal and external evaluation and notification of items listed in Attachment 1, there is no obvious need for this additional paperwork burden, which in most cases will result in a written procedure that documents another existing written procedure or procedures, that will be maintained for the sole purpose of demonstrating compliance with the requirement. Failure to properly report events is currently sanctionable under CIP-001-1 and EOP-004-1 and will continue to be sanctionable under proposed EOP-004-2. Adding a requirement to implement an “Impact Event Operating Plan”, “Operating Procedure”, and “Operating Process” is unnecessary. However, if the requirement is maintained, the related Measure M1 should state in plain language exactly what elements are required for compliance. Statements such as “The Impact Event Operating Plan may include, but not be limited to, the following…” begs the question regarding what other elements are required to demonstrate compliance. As written, M1 requires that entities provide an “Impact Event Operating Plan”, but does specify the required elements of the plan. In the absence of much more detailed instruction on exactly what elements must be included in the various documents, the proposed requirement will create confusion with both compliance and enforcement of the requirement. An example of each of the various required documents would be helpful. Any difficulty in developing such an example would be instructive of the probable compliance issues that would ensure from the necessarily varying approaches taken by disparate entities attempting to meet the requirement.
No
Requirement R2 is unnecessary for the same reasons listed above in answer to question 6 regarding Requirement R1. A new Reliability Standard requirement is not needed to verify that internal notifications are made within Registered Entities or to ensure that Registered Entities notify local law enforcement of suspicious activity, sabotage, theft, or vandalism. Such notifications are made by any company, and this requirement does not clearly enhance the reliability of the Bulk Electric System. Requirement R5 provides sanction in the event that events listed in Attachment 1 are not made appropriately. However, if the requirement is maintained, the related Measure M2 should state in plain language exactly what elements are required for compliance. In the absence of much more detailed instruction on exactly what elements must be included in the various documents, the proposed requirement will create confusion with both compliance and enforcement of the requirement. A detailed example of example documentation would be helpful. Any difficulty in developing such an example would be instructive of the probable compliance issues that would ensure from the necessarily varying approaches that would be taken by disparate entities attempting to meet the requirement.
No
Absent substantial evidence that the proposed requirement addresses an actual systemic problem with actual submittal of reports of electrical disturbances, Requirement R4 should be removed. Failure to properly report events is currently sanctionable under CIP-001-1 and EOP-004-1 and will continue to be sanctionable under proposed EOP-004-2. Entities are capable of implementing procedures appropriate to ensure compliance with the actual reporting requirements without the addition of this “test”. Alternately, if this requirement for annual tests is retained, it should be supplemented with a detailed example of an acceptable test and acceptable documentation of the test to avoid future compliance and enforcement issues. Stating “evidence may include, but is not limited to...” provides broad and unnecessary opportunity for future compliance and enforcement issues. Any difficulty the committee might encounter in developing such a detailed example would be instructive of the probable compliance and issues that would ensure from

implementation of the requirement.
No
Failure to properly report events is currently sanctionable under CIP-001-1 and EOP-004-1 and will continue to be sanctionable under proposed EOP-004-2. Entities are capable of implementing procedures appropriate to ensure compliance with the actual reporting requirements without the addition a formal requirement to annually review their internal procedures with personnel. In the unlikely event that an entity cannot attain this level of operating competence without implementation of a new requirement, such Entities would be subject to enforcement under Requirement R5. Absent substantial evidence of systemic problems by Entities in contacting local law enforcement properly or failures to complete event reports to appropriate agencies when provided with clear guidance on the events to be reported, this requirement is unnecessary.
No
The use of DOE OE-417 is acceptable, but the language of Requirement R5 should be modified. The disturbance event form must be filled out correctly, irrespective of the requirements of an Entity's "Impact Event Operating Plan". Reference to that Plan does not add clarity to the requirement to report events. The requirement should delete the reference to the "Impact Event Operating Plan" and simply state: Each Responsible Entity shall report events listed in Attachment 1 using the provided form, or where also required to complete the current version of DOE OE-417, that form. Although one of the primary stated purposes of the original SAR was to simplify the reporting process by creating a single form, the fact that some entities are already required to report substantially identical information to DOE argues for retention of the use of the DOE form.
No
1. Additional clarity on the nature of reportable "Fuel Emergencies" is needed. Does loss of interruptible gas transportation require reporting? 2. Additional clarity on the threshold for "damage or destruction of BES equipment" is needed. Footnote 1 on page 16 states, in part "Significantly affects the reliability margin of the system (e.g. has the potential to result the need for emergency actions". For generating facilities, does this statement refer specifically to the parallel requirement to report any loss of generation >= 2,000 in the Eastern or Western Connection or >= 1,000 in the ERCOT or Quebec Interconnection" If not, exactly what level of damage at a generating plant requires reporting? Use of imprecise terms such as "significantly" sets the stage for future compliance and enforcement confusion. 3. Additional clarity is required for "Detection of reportable Cyber Security Incident". Is this item intended to apply only to Critical Cyber Assets, or is it an extension of the requirement to all applicable entities irrespective of their Critical Asset status? If it applies only to Critical Cyber Assets, does this reporting requirement create redundant reporting (as reporting is already required under CIP-008-4)? CIP-008-4 requires reporting only of events affecting Critical Cyber Assets. If a more expansive application is intended, what equipment or systems are to be included in the reporting requirement?
No
Requirements R1, R2, R3, and R4 are unnecessary, as discussed above. The measure for Requirement R5 should focus on the need to report accurately and promptly, not on a Responsible Entity's "Operating Plan". If the Requirements are retained, the measures should state in much greater detail what actions and documentation are required for compliance.
No
Requirements R1, R2, R3, and R4 are unnecessary, as discussed above. If retained, the violation risk factors should be low for those Requirements, as they all simply support the requirement to actually report correctly stated in Requirement R5.
No
Requirements R1, R2, R3, and R4 are unnecessary, as discussed above. If retained, the violation risk factors should be low for those requirements, as they all simply support the requirement to actually report correctly stated in Requirement R5.
Focusing on reporting of actual disturbance events as listed in Attachment 1 based on potential or actual impact to the Bulk Electric System will provide maximum benefit to system reliability without adding needless levels of new documentation generated to demonstrate compliance. Absent significant evidence of systemic problems in the industry with past reporting attributable to causes other than a lack of clear guidance on the types events that require reporting, the proposed Standard should focus on the single issue of correct reporting, without attempting to micromanage how Entities internally manage such reporting.
Group
Dominion
Louis Slade
No
It is not evident how Impact Event reporting will "improve industry awareness" as suggested in the Purpose Statement. The transfer of Requirement R8 (ERO quarterly report) to the Rules of Procedure (paragraph 812) invalidates that claim within the context of this standard. Suggest removing this phrase from the Purpose Statement.

Yes
Dominion agrees with the proposed definition of Impact Events, but notes the use of the phrase “has the potential to impact” is somewhat subjective. The concern being a Responsible Entity makes a judgment on an event’s potential impact that is viewed differently after-the-fact by an auditor.
Yes
No
1) Several of the events require filing a written Impact Event report within one hour. System Separation, for example, is going to require an “all hands on deck” response to the actual event. We note that the paragraph above Attachment 1, Part A indicates that a verbal report would be allowed in certain circumstances, but this is the same issue with the formal report in that the system operators are concerned with managing the event and not the reporting requirements. Another example would be the Loss of Off-site power to a nuclear generating plant. Suggest reconsideration of one hour reporting requirement for events requiring extensive operator actions to mitigate; 2) Several events seem to have the “Threshold for Reporting” contained in footnotes rather than in the table. For example, Damage or destruction of BES equipment – Footnote 1, Fuel supply emergency – Footnote 2, etc.) Suggest moving the actual threshold into the table; 3) If one hour reporting remains as indicated in Attachment 1; align/rename events similar to that of the ‘criteria for filing’ events listed in DOE OE-417 for consistency.
Yes
No
The requirement for Responsible Entities to establish an Impact Event Operating Plan, Operating Process, and Operating Procedure seems overly cumbersome and prescriptive. The use of these NERC defined terms create additional compliance burden for little, if any, improvement to reliability. Suggest simplification by requiring the Responsible Entities to have a procedure to report Impact Events, to the appropriate parties, pursuant to EOP-004. In addition, we request clarification of R1.4. It seems circular to us in that it requires the plan to be updated within 90 days of when it changes. Is the intent that any necessary changes identified in the annual review required by R4 be incorporated in a revision to the plan within 90 days of the review? If so, R1.4 belongs under R4. If not, we do not understand the requirement. What starts the 90 day count down?
Yes
Dominion agrees subject to the comments provided in Question #6. In addition, Requirement R2 appears duplicative of Requirement R5. Suggest R2 be clarified relative to the intent.
No
: The need to conduct a test of its Operating Process has not been established and is overly restrictive given that the purpose of the standard is to report Impact Events.
No
The need to periodically review its Impact Event Operating Plan has not been established and is overly restrictive (annually) given that the purpose of the standard is to report Impact Events. Suggest removing this requirement
No
Dominion does not agree because the Requirement is too restrictive giving the Responsible Entity the choice on reporting forms as either Attachment 2 or DOE OE-417. The use of Attachment 2 or DOE OE-417 may be appropriate when reporting to NERC, however, Requirement R 1.3.2 requires the Responsible Entities Impact Event Operating Plan to address notifications to non-NERC entities such as Law Enforcement or Governmental Agencies. It is likely that these organizations have specific reporting requirements or forms that will not line up the options prescribed in Requirement R5. Suggest revising Requirement R5 to not require the use of these two forms as the only options. If these 2 forms are used; suggest aligning the Event names in Attachment 1 to be similar to the ‘criteria for filing’ event names in the DOE OE-417 to allow for consistency. Also suggest aligning the ‘time to submit’ for similar event names in each form.
No
1) A particular Event could be applicable to multiple entities and Attachment 1 would require each applicable entity to report the event. This is duplicative and would appear to overburden the reporting system. 2) Loss of off-site power (grid supply) reporting for nuclear plants is duplicative of reporting done to satisfy NRC requirements. Given the activity at a nuclear plant during this event, this additional reporting is not desired. 3) Cyber intrusion remains an event that would need to be reported multiple times (e.g., this standard, OE-417, NRC requirements, etc.). 4) Since external reporting for other regulators (e.g., DOE, NRC, etc.) remains an obligation of the Applicable Entity, suggest that Attachment 1 only contain impact events as defined in the current version of EOP-004.
No
1) M1 is open ended. Suggest adding “on request” to the end of the sentence as written; 2) M4 requires evidence of “when internal personnel were trained; however, Requirement R4 does not require training.
No
All the VRFs are "Medium". Since the requirements deal with after-the-fact reporting and the administration of reporting

plans, procedures, and processes; all VRFs should be "Lower".
Yes
Yes
Dominion agrees with the Implementation Plan; however, notes that the title for EOP-004-2 is inconsistent with the actual proposed standard.
The following comments are provided on the Reporting Hierarchy for Impact Events EOP-004-2: 1) A reference to sabotage still exists in a “decision block”; 2) The “entry block” only specifies “actual Impact Events” and does not address “potential”; 3) Hierarchy is misspelled in the title. Attachment 2: Impact Event Reporting Form; in questions 7, 8, 9, 10, 11 what is the purpose of the *(asterisk) behind each Task that is named?
Individual
Bill Keagle
BGE
1 - Transmission Owners
No
BGE believes that using the term “Impact Events” as currently defined is too vague. An alternative statement would be “… requiring the reporting of events listed in Attachment 1 and their causes, if known …” and making the definition change as noted in question 2.
No
Change the definition of “Impact Event”, to add the following phase to the definition “Any event (listed in Attachment 1) which has either…”. Also, the phrase “… or has the potential to impact the reliability…” is too vague and broad. Such broad statement is unhelpful in clarifying entities’ compliance obligation and potentially creates conflicted reporting between entities. A clear statement of how the reliability is affected should be used, i.e., results in contingency emergency situation or IROL.
Yes
No comments.
Yes
No comments.
Yes
No comments.
No
This seems overly restrictive in its use. Requirement is now telling entities how to resolve situations, not giving them a requirement to resolve the situation.
Yes
No comments.
No
Requirement 3 (formerly R4) should be removed altogether because it is covered by the new R4. The topic of Disturbance Reporting is covered several times each year during operator training classes and the operators are tested on the material. Actual issued Disturbance Reports throughout the year are also covered during training class.
Yes
No comments.
No
Language needs to be more specific on when to use Attachment 2 or DOE-OE-417.
No
For the following Events (Damage or destruction of BES equipment, Damage of destruction of Critical Asset, and Damage or destruction of a Critical Cyber Asset), submitting a report within 1 hour after occurrence is identified is too short of a time frame. Generally, the initial time period is spent in recovering from the situation and restoring either electric service or restoring computer services to assure proper operations. To distract from the restoration to normal activities to focus on a report would be detrimental to reliability. Notification of an event may perhaps be made by phone call within 1 hour but completing a report should be required no less than 6 or 12 hours. Determining a cause (especially external or intentional) could take longer than 1 hour to determine and complete a report. It is important to consider the imposition created by a compliance obligation and weigh it against the other demands before the operator at that time. A compliance obligation should avoid becoming a distraction from reliability related work. Under impact event type scenarios, in the first hour of the event, the primary concern should be coping with/resolving the event.
No position or comments.
Yes

No comments.
Yes
No comments.
No position or comments.
Yes
No comments.
Please provide a Mapping Document which shows where the four CIP-001 requirements map to in the new EOP-004-2, and note if any of the CIP-001 requirements have been eliminated. A Mapping Document was provided during the first Comment Period, but not during the second Comment Period. A Mapping Document will be very helpful to companies in aligning standard owners in reviewing this proposal and in transitioning compliance programs when the revised standard is approved.
Group
We Energies
Howard Rulf
Yes
No
From an on-line dictionary, an event is “something that happens”. Combined with the phrase “has the potential to impact” and the definition of Impact Event would include every routine operation performed by any entity. Taking a generator on or off line, switching a transmission line in or out, traffic driving past a substation, all have the “potential to impact” the BES. The Impact Event definition is overly broad and needs to be significantly narrowed.
Yes
No
Attachment 1: From the NERC Glossary, an Energy Emergency: A condition when a Load-Serving Entity has exhausted all other options and can no longer provide its customers’ expected energy requirements. The first four events listed can only apply to an LSE. Loss of Firm Load for >15 Minutes: By the NERC Glossary definitions of DP and LSE, the LSE would seem to be more appropriate than the DP. With the proposed one-hour reporting requirement, the industry would be undertaking significant regulatory risk with respect to timely reporting. The requirement to report the crime-based events in the field within one hour, as shown in Attachment 1 Part A or Part B will be difficult. We could even discover a theft in progress with the suspect trapped inside the substation fence and the police attempting to make a safe arrest. We need more reporting time, especially when they have not even resulted in an outage. The industry is keenly interested in understanding the benefit of taking on the risk. What analysis, insight, warnings or recommendations would the ES-ISAC provide to the reporting entity, the industry or to law enforcement agencies in the hours after such an incident is reported? Note too that DOE requires reporting of a physical attack within one hour only when it “causes a major interruption or major negative impact on critical infrastructure facilities or to operations.” In lesser cases, the entity gets up to six hours if it “impacts electric power system reliability”. DOE has said that it is not interested in copper theft unless it causes one of these events. If the SDT is working to ensure consistency of reporting requirements, please consider DOE requirements too. Meeting the reporting deadline will mean that available resources in the control center will be devoted to ensuring the report is filed on time instead of making the site safe and arranging for prompt repair. It may even mean that law enforcement won’t be contacted until the forms are filed with the ES-ISAC. The exception contained in footnote #1 of Attachment 1 with respect to copper theft is not an exception at all. The majority of copper theft from substations is, in fact, such grounding connectors which may or may not render the protective relaying inoperative. You could end up receiving reports from all over the USA, Canada and Mexico, mostly on Monday mornings as weekend copper thefts are discovered. Attachment 1 Part A table also contains redundancies. One of the cells reads, “Damage or Destruction of Critical Asset”. One cannot destroy something without damaging it first. Consequently, it is sufficient to simply say, “Damage to a Critical Asset”. Apply to all cells with the same phrase.
Yes
No
R1.2: By its NERC Glossary definition, an Operating Procedure is too prescriptive for data collection. An Operating Procedure requires specific steps to be taken by specific people in a specific order. We would have to predict every event that could happen to have every step in proper order to collect the data. It will be impossible to comply with this requirement. R1.3: Change “Impact Event” to “Impact Event listed in Attachment 1”.
Yes
No
A test of the Operating Process for communication would be placing telephone calls. This requirement would have virtually every entity in North America calling NERC, Regional Entities, FERC/Provincial Agency, Public Service

Commission, FBI/RCMP, local Police, etc. annually. Every entity will probably be asking for a confirmation letter from each telephone call for proof of compliance. This is an unnecessary requirement. Delete it.
No
Include that this is for internal personnel as stated in the associated measure.
Yes
No
It appears that the footnotes only apply one place in the table. Place the footnote in the table where it applies. Voltage Deviations on BES Facilities: 10% compared to what? Rated? Forced Intrusion: “At a BES facility” facility or Facility?
No
M1 contains a redundancy: It currently reads, “Each Responsible Entity shall provide the current in force Impact Event Operating Plan to the Compliance Enforcement Authority.” (“In force” is the same as “current”.) M2: Change “Impact Event” to “Impact Event listed in Attachment 1”. M3: This is an additional requirement. R3 does not require a mock Impact Event. R3 requires a test of the communicating Operating Process. As stated above, R3 and M3 should be deleted. M4: This is written assuming classroom training. R4 does not require formal training much less classroom training. R4 requires that those (internal) personnel who have responsibilities in the plan review the Impact Event Operating Plan. M5: When we report, how do we show to an auditor that we reported “using the plan”? Delete the reference to “the plan”.
No
All VRFs should be Lower. They are all administrative and will not affect BES Reliability.
No
Change the VRFs as indicated above and the Time Horizons as indicated below.
No
R2 and R5 should be Operations Assessment.
Yes
Attachment 2: What do the asterisks refer to? I didn’t see a comment or description related to them. #7 & #10: What is “tripped”? Automatic or manual or both. #13: This report has no Part 1. Flowchart: By the flowchart, the only time an OE-417 is filed is when I do not need to contact Law Enforcement. The Reporting Hierarchy flow chart should be modified. In the lower right corner it indicates that if sabotage is not confirmed, the state law enforcement agency investigates. Law enforcement agencies will not investigate an incident that is not a crime. Note too that state law enforcement agencies do not even investigate these kinds of events unless and until requested by local law enforcement. The local law enforcement agency always has initial jurisdiction until surrendered or seized by a superior agency’s authority. Evidence Retention is incomplete. From the NERC Standards Process Manual: “Evidence Retention: Identification, for each requirement in the standard, of the entity that is responsible for retaining evidence to demonstrate compliance, and the duration for retention of that evidence.”
Individual
Kenneth A Goldsmith
Alliant Energy
4 - Transmission-dependent Utilities
Yes
No
The proposed definition is not supported by any of the established “bright line” criteria that are contained within attachment 1. This Results Based Standard should close any loop-holes that could be read into any section, especially the definition. We recommend the definition be enhanced to read: “Impact Event: Any Contingency which has either effected or has the potential to effect the Stability of the BES as outlined per attachment 1. Within this enhanced recommendation, presently defined NERC terms are used (Contingency and Stability), thus supporting what is current used within our industry. There is also a quantifiable aspect of “as outlined per attachment 1” that clearly defines Impact Events. If the above definition is not adopted, we believe it should be rephrased to narrow the scope to “those events that result from malicious intent or human negligence/error.” We are concerned that by using phrases like “unintentional or intentional human action” in combination with “damage or destruction” basically means everything except copper theft becomes a reportable impact event (including planned actions we must perform to comply with CIP-007 R7).
Yes
Yes

Yes
Yes
This is a NERC defined term and will assist entities in maintaining compliance with this (proposed) Standard. We believe the reference to Attachment 2 in R1.2 should be revised to the DOE Form and utilize only one reporting form, if at all possible.
Yes
Yes
Yes
No
We believe Attachment 2 should be deleted, and NERC should work with the DOE to have one form for all events, if possible. It makes the reporting procedure much simpler, only having to use one form.
No
The item relating to Loss of Firm Load for > 15 minutes should be revised to 500 MW and 300 MW. For many companies, a storm moving across their system could cause more than 300 MW of firm load to be lost, but there is no impact on the BES, so why does the detailed reporting need to be done? The items relating to “damage or destruction” need to be revised to not be so wide. As currently written, a plan by a company to raze a facility could be considered a violation and must be reported. We believe it needs to tightened to malicious intent or human negligence/error.
Yes
Yes
Yes
Yes
Yes
Group
Pepco Holdings Inc and Affiliates
David Thorne
Yes
No
The two sentence definition will not be adequate to serve well over the course of time. People will have to read and understand the standard without benefit of the detailed information, explanations and interpretations available during the standards development process. Without additional explanation as provided in the background and the guideline and technical basis sections, to support the definition, the standard will be subject to confusion and interpretations. Consider adding a lot of the information and explanation that is in those sections to the standard. Any event could be an impact event. However, only a subset is reportable. What is really being addressed are reportable events. More specifically after the fact reporting of unplanned events.
No
See #2. With out the explanation contained in background information, over time those that have not been involved with this standard development will struggle with how to interpret the code words of non environmental and intentional human action.
Yes
More guidance is needed for which entity in Attachment 1 actually files the report to avoid duplicate filing.
Yes
Agree that NERC should not have requirements applicable to them.
No
An Operating Plan, Operating Process or Operating Procedure implies something different than an after the fact reporting activity.

Yes
Yes
Yes
Yes
No
The entity responsible for reporting is not clear. Is the initiating entity the same as requesting entity or implementing entity? In the paper it indicates the DT intent is for the entity that performs the action or is directly affected will report. It seems that the proposal would result in a significant amount of duplicate reporting.
Yes
No
This standard involves after the fact reporting of events. Other standards deal with the real time notifications. How do the risk factors between the two line up? A VRF of Low would seem appropriate, since a violation would not affect the reliability of the BES.
No
This standard involves after the fact reporting of events. Other standards deal with the real time notifications. How do the severity level between the two line up? See above VRF comments.
Yes
However, do they line up with the corresponding real time reporting procedures as mentioned above, #13 and #14?
No
The proposed time line is too short. It is easy to revise procedures. However developing training and integrating the training into the schedule takes time. Shorter time frame takes away adequate time to integrate into the training plan and disrupts operator schedules. Since notifications already exist and after the fact reporting does not impact BES reliability, why the need to expedite? There are many other training activities that must be coordinated with this.
IRO-000-1, Sec D1.5 and TOP-007, Sec D1.1 there are “after the fact” reporting requirements for IROL violations. Since IROL violations are included in this standard, should those standards be modified? Should the standard include a specific statement that this standard deals only with after the fact and other standards deal with real time reporting? Since this standard deals with after the fact reporting, consideration should be given to extending the time to report as defined in Attachment 1. One hour does not seem to be reasonable.
Individual
John Brockhan
CenterPoint Energy
1 - Transmission Owners
Yes
No
CenterPoint Energy suggests that the phrase “…or has the potential to impact…” be deleted as it makes the definition vague and broad. Similar issues encountered in trying to define sabotage may resurface, such as varying definitions or interpretations of “potential”. If this standard is to support after-the-fact reporting, the focus should be on actual events, not potential situations or events. Effective and efficient prevention would come from analysis of actual events. Resources and reporting could become overwhelmed upon having to consider “potential”. All references to “potential” should be removed from the standard, guidance, and attachments.
No
CenterPoint Energy would agree if the definition for Impact Event was changed as suggested in the response to Question 2.
Yes
Yes
No
CenterPoint Energy recommends deleting the current R2 as it is an inherent part of the current R5. For an entity to

“report Impact Events in accordance with the Impact Event Operating Plan pursuant to R1” (see R5), the entity must “implement its Impact Operating Plan documented in Requirement 1…” (see R2). Including both requirements is unnecessary and duplicative. Likewise, M2 should be deleted.
Yes
Yes
Yes
CenterPoint Energy agrees with the idea of streamlining the reporting process through the use of existing report forms. However, as noted in the response to Question 11, the Company has concerns about the DOE OE-417 Form, specifically the timeframes in which to submit reports. CenterPoint Energy will be making the same recommendation to extend reporting timeframes during the DOE OE-417 report revision process when the current form expires on 12/31/11. Any future changes to the DOE Form could also impact reporting for this requirement.
No
(1) CenterPoint Energy believes that the “Entity with Reporting Responsibility” for the first three events in Part A should be clarified. There could still be confusion regarding the “initiating entity” for events where one entity directs another to take action. From the text on page 5 of the Unofficial Comment Form, it appears that the SDT intended for the “initiating entity” to be the entity that takes action. To make this clear in Attachment 1, CenterPoint Energy recommends replacing “initiating entity” with “Each (insert applicable entities) that (insert action). For example, for “Energy Emergency requiring a Public appeal” the Entity with Reporting Responsibility should be “Each…that issues a public appeal for load reduction”. (2) Part A: The threshold for reporting “System Separation” should not be fixed at greater than or equal to 100 MW for all entities, but rather should be scaled to previous year’s demand as in “Loss of Firm load for greater than or equal to 15 minutes”, so that for entities with demand greater than or equal to 3000 MW, the island would be greater than or equal to 300MW. (3) Part A: The one hour reporting requirements are unreasonable and burdensome. The Background text indicates that “proposed changes do not include any real-time operating notifications…” CenterPoint Energy believes all one hour reporting requirements could potentially divert resources away from responding to the event. In many instances the event may still be developing within one hour. Likewise, the 24 hour reporting requirements are also burdensome. CenterPoint Energy recommends changing all reporting requirements to 48 hours. CenterPoint Energy acknowledges that the DOE OE-417 report requires certain one hour and 6 hour reporting. Those requirements should also be extended, and CenterPoint Energy will be making the same recommendation during the DOE OE-417 report revision process when the current form expires on 12/31/11. (4) Part B: CenterPoint Energy is very concerned with the “events” listed under Attachment 1 – Potential Reliability Impact – Part B and believes Part B should be deleted. These arbitrary “events” with “potential reliability impact” and reporting times place unnecessary burden on entities to report “situations” that would rarely impact the reliability of the BES. Entities should be aware of developing situations; however, this standard should not require reporting of such occurrences. (5) Part B: Of particular concern is the overly broad “Risk to BES equipment” and the example provided in the footnote. CenterPoint Energy believes the SDT has already identified the events with the greatest risk to impact the BES in Part A. Also including “potential reliability impact” situations in Part B inappropriately dilutes attention away from the truly important events. The industry, NERC and FERC should not lose sight of the forest for the trees.
No
M1: CenterPoint Energy recommends that the phrase “current in force” be updated to “current” or “currently effective”. Additionally, CenterPoint Energy suggests clarifying M1 by adding “within 30 days upon request”, which would be consistent with language found in measures in other standards. The revised measure would read, “Each Responsible Entity shall provide the currently effective Impact Event Operating Plan to the Compliance Enforcement Authority within 30 days upon request.” M2: If R2 is deleted (as recommended in response to Question 7), then M2 should be deleted.
No
CenterPoint Energy believes that the Severe VSL for R5 (Reporting) in the current draft incorrectly equates 2X reporting with failure to submit a report. CenterPoint Energy believes the VSLs for R5 should all reflect a factor increase in time. For example, the lower VSL should be 1.5X the reporting time frame. The Moderate VSL should be 2x the reporting time frame. The High VSL should be 3x the reporting time frame. The Severe VSL should be failure to report.
Yes
No
CenterPoint Energy prefers the previously accepted timeline of 1 year.
CenterPoint Energy believes the flowchart found on page 8 identifying the reporting hierarchy for EOP-004 is helpful. CenterPoint Energy believes the DOE reporting items should also be included on the right side of the chart. Some of the issues with CIP-001 were a result of law enforcement’s preference and procedures for notification. Law enforcement’s preferences and procedures should be considered for this draft. (Reference: http://www.fbi.gov/contact-us/when)

Individual
Martin Kaufman
ExxonMobil Research and Engineering
1 - Transmission Owners, 5 - Electric Generators, 7 - Large Electricity End Users
Yes
No
The use of the word potential is ominous.
Yes
Yes
No
Obstain from commenting on this question.
No
The requirement to notify State Law Enforcement deviates from existing government security requirements that Petrochemical Facilities (Cogenerators) are required to follow. Per the Maritime Transportation Security Act of 2002 (MTSA) and the Chemical Facility Anti-Terrorism Standard (CFATS), Petrochemical Facilities are required to report the security incidents identified in EOP-004 Revision 2 to the National Response Center which is staffed by the United States Coast Guard. The National Response Center coordinates incident reporting to both the Department of Homeland Security and Federal Bureau of Investigation. Requiring Petrochemical Facilities to report security incidences to State Law Enforcement agencies duplicates their reporting of incidences to the appropriate law enforcement agencies. EOP-004 Revision 2 should be modified to synergize with existing federal security regulations so that those facilities that are required to comply with the MTSA and CFATS are, by default, compliant with EOP-004 Revision 2 when they comply with these existing federal security regulations. It is unclear, from the documentation provided in this revision of EOP-004, which entities a Responsible Entity is required to notify when certain types of Impact Events occur. Previously, CIP-001 included a similarly vague instruction that required notifications to the 'appropriate parties in the interconnection' and the FBI/RCMP. The Standard Drafting Team should identify which NERC Functional Entities should be notified when each of the Impact Events identified in Attachment 1 occurs. Current revisions of CIP-001 Revision 1 or EOP-004 Revision 1 do not include corresponding requirements to update procedures within a certain time frame. It's difficult to foresee a situation where an Entity would initiate a change to its response plan without being required to update the formal response plan documentation per their management of change process. Additionally, failure to update the procedure would result in the entity deviating from the procedure any time an impact event occurred, which would automatically force a violation of EOP-004-2 R2 for failure to properly implement their Operating Process. Furthermore, the only changes occurring between review cycles should be revisions to the contact information for third parties. It is beyond an entity's power to require third parties to notify the entity when the third party changes their contact information, and, as such, this requirement burdens registered facilities with responsibility for compliance for items that are beyond their realm of control.
No
The notification requirement and documentation in Attachment 1 do not clearly identify which entities need to be notified for each type of event detailed in Attachment 1. While it makes sense to notify the Reliability Coordinator, NERC, Regional Entity, Law Enforcement and other Governmental Agencies for sabotage type events, it does not seem proper to notify Law Enforcement agencies of a system disturbance that is unrelated to improper human intervention. Furthermore, it is our belief that a time frame of 1 hour is a short window for making a verbal notification to third parties, and an impossibly short window for requiring the submittal of a completed form regardless of the simplicity. When a Petrochemical Facility experiences an impact event, the initial focus should emphasize safe control of the chemical process. For those cases where registered entities are required to submit a form within 1 hour, the Standard Drafting Team should alter the requirement to allow for verbal notification during the first few hours following the initiation of an Impact Event (i.e. allow the facility time to appropriately respond to and gain control of the situation prior to making a notification which may take several hours) and provide separate notifications windows for those parties that will need to respond to an Impact Event immediately and those entities that need to be informed that one occurred for the purposes of investigating the cause of and response to an Impact Event. For example, a GOP should immediately notify a TOP when it experiences a forced outage of generation capacity as soon as possible, but there is no immediate benefit to notify NERC when site personnel are responding to the event in order to gain control of of the situation and determine the extent of the problem. The existing standard’s requirement to file an initial report to entities, such as NERC, within 24 hours seems reasonable provided that proper real time notifications are made and the Standard Drafting Team reinstates EOP-004 Revision 1's Requirement 3.3, which allows for the extension of the 24 hour window during adverse conditions, into the requirement section of EOP-004 [the current revision locates this extension in Attachment 1, which, according to input received from Regional Entities, means that the extension would not be enforceable].
No

The annual (15 month) time window for conducting annual performance tests appears to be reasonable. However, the required scope of the test is vague. The Standard Drafting Team should modify the testing requirement to include boundary criteria such as whether notifications to third parties and law enforcement are required or if the test is limited to internal notifications and response processes. Furthermore, the current measure associated with this requirement, EOP-004 Revision 2 Measure 3, implies, that if an Impact Event occurs, the registered entity can count the activation of its Impact Event Operating Plan as a test and extend the test window 15 months from the date of activation. The Standard Drafting Team should revise the requirement to clarify that the test window resets when a site initiates its Impact Event Operating Plan in response to a real Impact Event as requirement criteria should not be included in a measure.

No

It's unclear whether R4 is a training requirement to train all individuals who may be required to implement its Impact Event Operating Plan on an annual basis or a requirement for an Entity to review the Impact Event Operating Plan with atleast one person from each position that has a role in the Impact Event Operating Plan in order to complete a quality review of the Impact Event Operating Plan. The SDT should clarify the intent of the requirement. If the intent is that both of the aforementioned interpretations is expected to occur, the SDT should break R4 into two requirements so that an entity is not violation of Requirement R4 when the entity fails to comply with one of the two imbedded requirements (e.g. if the quality review is not performed but all individuals were trained).

No

The notification requirement and documentation in Attachment 1 do not clearly identify which entities need to be notified for each type of event detailed in Attachment 1. While it makes sense to notify the Reliability Coordinator, NERC, Regional Entity, Law Enforcement and other Governmental Agencies for sabotage type events, it does not seem proper to notify Law Enforcement agencies of a system disturbance that is unrelated to improper human intervention. Furthermore, it is our belief that a time frame of 1 hour is a short window for making a verbal notification to third parties, and an impossibly short window for requiring the submittal of a completed form regardless of the simplicity. When a Petrochemical Facility experiences an impact event, the initial focus should emphasize safe control of the chemical process. For those cases where registered entities are required to submit a form within 1 hour, the Standard Drafting Team should alter the requirement to allow for verbal notification during the first few hours following the initiation of an Impact Event (i.e. allow the facility time to appropriately respond to and gain control of the situation prior to making a notification which may take several hours) and provide separate notifications windows for those parties that will need to respond to an Impact Event immediately and those entities that need to be informed that one occurred for the purposes of investigating the cause of and response to an Impact Event. For example, a GOP should immediately notify a TOP when it experiences a forced outage of generation capacity as soon as possible, but there is no immediate benefit to notify NERC when site personnel are responding to the event in order to gain control of of the situation and determine the extent of the problem. The existing standard's requirement to file an initial report to entities, such as NERC, within 24 hours seems reasonable provided that proper real time notifications are made and the Standard Drafting Team reinstates EOP-004 Revision 1's Requirement 3.3, which allows for the extension of the 24 hour window during adverse conditions, into the requirement section of EOP-004 [the current revision locates this extension in Attachment 1, which, according to input received from Regional Entities, means that the extension would not be enforceable].

No

The notification requirement and documentation in Attachment 1 do not clearly identify which entities need to be notified for each type of event detailed in Attachment 1. While it makes sense to notify the Reliability Coordinator, NERC, Regional Entity, Law Enforcement and other Governmental Agencies for sabotage type events, it does not seem proper to notify Law Enforcement agencies of a system disturbance that is unrelated to improper human intervention. Furthermore, it is our belief that a time frame of 1 hour is a short window for making a verbal notification to third parties, and an impossibly short window for requiring the submittal of a completed form regardless of the simplicity. When a Petrochemical Facility experiences an impact event, the initial focus should emphasize safe control of the chemical process. For those cases where registered entities are required to submit a form within 1 hour, the Standard Drafting Team should alter the requirement to allow for verbal notification during the first few hours following the initiation of an Impact Event (i.e. allow the facility time to appropriately respond to and gain control of the situation prior to making a notification which may take several hours) and provide separate notifications windows for those parties that will need to respond to an Impact Event immediately and those entities that need to be informed that one occurred for the purposes of investigating the cause of and response to an Impact Event. For example, a GOP should immediately notify a TOP when it experiences a forced outage of generation capacity as soon as possible, but there is no immediate benefit to notify NERC when site personnel are responding to the event in order to gain control of of the situation and determine the extent of the problem. The existing standard's requirement to file an initial report to entities, such as NERC, within 24 hours seems reasonable provided that proper real time notifications are made and the Standard Drafting Team reinstates EOP-004 Revision 1's Requirement 3.3, which allows for the extension of the 24 hour window during adverse conditions, into the requirement section of EOP-004 [the current revision locates this extension in Attachment 1, which, according to input received from Regional Entities, means that the extension would not be enforceable].

No

Measure M3 introduces a psuedo-requirement by implying you are able to reset the testing clock if you implement our

Impact Event Operating Plan in response to an Impact Event. This should be covered in Requirement R3. Measure M4 should refer to positions and evidence that people occupying those positions participated in the annual review of the Impact Event Operating Plan. Given the number of individuals involved in operations and the cycle of promotions and reassignments, it's unreasonable to expect an entity to identify specific individuals in their Impact Event Operating Plan. As the one hour time window is not long enough for entities to report all types of events when responding to the impact the Imact Event had on its facility, Measure M5 should be modified to include voice recordings and log book entries to capture verbal information reported to required parties.
No
VRFs, VSLs, and THs ideally should be based on the impact event type; alternatively a low VRF seems more appropriate for this requirements of this standard.
No
VRFs, VSLs, and THs ideally should be based on the impact event type; alternatively a low VRF seems more appropriate for this requirements of this standard.
No
VRFs, VSLs, and THs ideally should be based on the impact event type; alternatively a low VRF seems more appropriate for this requirements of this standard.
Recommend 4th calendar quarter instead of 3rd.
Group
SPP Standards Review Group
Robert Rhodes
No
We would suggest changing the purpose to read 'To improve industry awareness and effectiveness in addressing risk to the BES by requiring the reporting of Impact Events and their causes, if known, by the Responsible Entities.'
Yes
Yes
No
While the SDT has recognized the issue of applicability to GO/TO in its background information with the Unofficial Comment Form, we still do not feel comfortable with the GO/TO being listed as a responsible entity when in fact it may be days before they become aware of an event worthy of reporting. If the GOP/TOP makes the report, are the GO/TO still responsible for filing a report? If the GOP/TOP do not file the report, would the GO/TO then be non-compliant? This issue appears to put additional risk on the GO/TO over which they have no control. We need some mechanism to eliminate unnecessary risk while at the same time ensuring that we have coverage for the BES. Perhaps this could be done through delegation agreements between the entities involved or through allowances within the standard itself. For example, could the phrase 'appropriate parties in the Interconnection' as currently contained in CIP-001-1, R2 be incorporated into the standard to basically replace GO/TO?
Yes
No
We would suggest rewording Part 1.3.2 to read 'External organizations to notify may include but are not limited to the Responsible Entity's Reliability Coordinator, NERC, Responsible Entity's Regional Entity, Law Enforcement and Governmental or Provincial Agencies. We would also suggest the following for Part 1.4: 'Provision(s) for updating the Impact Event Operating Plan within 90 days of any known changes to its content.' Would also suggest adding 'as requested' at the end of M1.
Yes
No
The SDT included a formal review process in the discussion of R4 in the Background Information in the Unofficial Comment Form as one of three options for demonstrating compliance with the testing requirements of R4, yet M3 only contains two of those options – a mock Impact Event exercise and a real-time implementation of its Operating Process. The third option, a formal review process, is missing from M3 and needs to be added. We would suggest the following for M3: 'In the absence of an actual Impact Event, the Responsible Entity shall provide evidence that it conducted a mock Impact Event and followed its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 or conducted a formal review of its Operating Process. The time period between tests, actual Impact Events or formal reviews shall be no more than 15 calendar months. Evidence may include, but is not limited to, operator logs, voice recordings or documentation.
No

There is confusion surrounding the use of the term ‘review’ in R3 and R4. In R3 and the suggested revision to M3 in Question 8, review is an analysis of the plan by a specific group tasked to determine if the plan requires updating or modifying to remain viable. Review in R4 has training connotations for all personnel who have responsibilities identified in the plan. Although we understand the use of ‘review’ in R4 is new to this version of EOP-004-2, we believe it may be more appropriate to use training rather than review in R4. And further, we feel the training should be focused on those specific portions of the plan that apply to specific job functions.
No
We feel there is redundancy between R2 and R5. To eliminate this redundancy, we propose to take the phrase ‘…using the form in Attachment 2 or the DOE OE-417 reporting form’ and adding it at the end of R2. Then what’s left of R5 could be deleted. The new R2 would read ‘Each Responsible Entity shall implement its Impact Event Operating Plan documented in Requirement R1 for Impact Events listed in Attachment 1 (Parts A and B) using the form in Attachment 2 or the DOE OE-417 reporting form.’
No
Threshold for Reporting – Some of the thresholds used to trigger event reporting seem arbitrary. For example, why were three BES Transmission Elements selected for the transmission loss trigger? What’s significant with three? There may be situations where one element can impact reliability more than other situations where three or more lines may be lost. The defining line should be impact to reliability, not a simple count of elements. Also, timing of the loss of these elements is important. If the three elements are lost over a 3-day span, does this trigger an event report? We would think not and would like to see that clarification in the standard. Public appeals – Some entities may utilize load reduction (Demand Response, interruptible loads, etc) in the normal course of daily operation in lieu of committing additional generation resources. Because this is not an Energy Emergency as defined in the NERC Glossary, would such an event trigger the filing of an Impact Event report under EOP-004-2? We would like clarification on this issue. Multiple entity reporting responsibility – Several of the triggering events in Attachment 1 list multiple entity reporting responsibility. The SDT needs to clarify precisely who has the actual reporting responsibility for those events. For example, if a DP loses ≥ 300 MW (or ≥ 200 MW depending on size) of load who files the report? Is it the DP, TOP, BA or RC? Attachment 1 would lead us to believe all four are required to file reports. This redundancy is unnecessary and creates unneeded paperwork. Surely this redundancy is not the intent of the SDT. Reporting timeframe – The timeframes for reporting these after-the-fact reports need to be thoroughly reviewed and, we believe, realigned. Which is more important to the reliability of the BES, operating and controlling the BES following an Impact Event or filing a report describing that event? Most operating desks are staffed by a single operator at nights and on weekends. Their focus should be on operating the system, not filing a report with NERC or DOE within one hour. There appears to be inconsistency in the reporting times among the triggering events. There doesn’t appear to be any logic regarding how the times were selected. Shouldn’t impact to the reliability of the BES be that basis? Why is a BA with 50 MW of load who makes a public appeal to customers for load reduction required to report within 1 hour while an IROL violation doesn’t need to be reported for 24 hours? Clearly the IROL violation has a greater impact on the reliability of the BES. Therefore, shouldn’t these types of reports be filed sooner than those events with less impact on BES reliability? Risk to BES equipment – The Threshold for Reporting this event indicates that only those events associated with a non-environmental physical threat should be reported. The train derailment example in the footnote then conversely describes just such an environmental threat with flammable or toxic cargo. Which should it be? Additionally, how does one determine the applicability of a potential threat? Is this time dependent, is it threat dependent, how do we factor all this in?
No
The measures are written as if they are adding requirements to the standards. Using wording such as ‘shall provide’ gives this implication. We would suggest wording such as ‘examples of acceptable evidence to demonstrate compliance may be…’ See Question 6 for comments regarding M1. See Question 8 for comments regarding M3.
No
These are reporting requirements and therefore do not deserve the ‘medium’ VRF. We suggest making the VRFs for all requirements for EOP-004-2 ‘low’.
No
Requirement 4: We would suggest the following: Low – The Responsible Entity reviewed its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 15 calendar months but less than 18 calendar months since the last review. Moderate - The Responsible Entity reviewed its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 18 calendar months but less than 21 calendar months since the last review. High - The Responsible Entity reviewed its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 21 calendar months but less than 24 calendar months since the last review. Severe - The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan within 24 calendar months since the last review. Requirement 5: With our suggested deletion of Requirement 5, we further suggest deleting the VSLs associated with Requirement 5.
No
Based on our previous comments in response to Question 11, we feel that the Time Horizon for R2 should be lengthened. Assigning it a Real-time Operations and Same –day Operations timeframe has too much of an impact on

real-time operations. Pushing it back will allow support personnel to do the after-the-fact reporting and keep this burden off of the operators.
Yes
In Attachment 2 just before the table, the statement is made that 'NERC will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report.' But the last sentence in the Guideline and Technical Basis white paper, it is stated that ' For example, if the NERC Report duplicates information from the DOE form, the DOE report may be included or attached to the NERC report, in lieu of entering that information on the NERC report.' These are in conflict with each other. Which is correct? We prefer the former over the latter. In Attachment 2 in Tasks 7-11 an asterisk appears in those tasks. To what does this asterisk refer?
Individual
Brenda Truhe
PPL Electric Utilities
1 - Transmission Owners
Yes
Yes
PPL EU agrees with the definition. We would like to point out that our interpretation of the definition excludes maintenance work. Our interpretation also concludes that maintenance work that does not go as planned or goes awry and impacts the reliability of the BES would be an impact event and reported as required per Attachment 1.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
We would like to suggest the language be changed such that 'submission via a NERC system' would be acceptable in addition to the use of the Attachment 2 Form or the DOE OE-417 form. The standard would then accommodate the proposed revision to NERC Rules of Procedure 812. '…NERC will establish a system to collect impact events reports…'
No
We very much appreciate the work performed by SDT and consideration of all the comments received. While we agree with the majority of the Attachment 1 changes, we suggest the SDT add further clarification to Attachment 1, Part A, Event 'Transmission Loss'. Does this mean permanent loss? Do two lines and a pole constitute a loss of three elements? E.g. Consider the loss of a 230 kV line with two tapped transformers. This does not have a significant effect on the BES, yet would it be reportable? We would prefer Attachment 1, Part A, 'Threshold Reporting' be clarified. E.g. 'Three or more "unrelated" pieces of equipment for a single event'.
Yes
Yes
Yes
We thank the SDT for addressing so many Industry concerns with the 2010 draft of EOP-004-2. We feel the current draft version of EOP-004-2 is a significant improvement over current EOP-004-1 and CIP-001-1 standard and the

previous draft. Thank you for your time.
Individual
Tim Soles
Occidental Power Marketing
3 - Load-serving Entities
Yes
No
The SDT includes in the definition the "potential to impact the reliability of the BES." This seems vague, although Attachment 1 clarifies what actually has to be reported. An LSE may have limited or no knowledge of "potential to impact." The SDT may want to refine the definition,e.g., "to the extent the entities' knowledge could reasonably reveal the impact."
Yes
No
Load Serving Entities that do not own or operate BES assets (or assets that support the BES) should not be included in the Applicability. The SDT includes LSEs based on CIP-002; however, if the LSE does not have any BES assets (or assets that support the BES), CIP-002 should also not be applicable because the LSE could not have any Critical Assets or Critical Cyber Assets. It is understood that the SDT is trying to comply with FERC Order 693, Sections 460 and 461; however, Section 461 also states: "Further, when addressing such applicability issues, the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate to address these concerns." A qualifier in the Applicability of EOP-004-2 that would include only LSEs that own, operate or control BES assets (or assets that support the BES)would seem appropriate and acceptable to FERC.
Yes
Yes
However, only LSEs with BES assets (or assets that support the BES)should be included in the Applicability section of the standard.
Yes
However, only LSEs with BES assets (or assets that directly support the BES)should be included in the Applicability section of the standard.
No
We understand that this requirement is meant to comply with FERC Order 693, Section 466; however, there needs to be more specificity concerning what sort of "test" would be accepted for auditing purposes. Also, only LSEs with BES assets should be included in the Applicability section of the standard.
Yes
However, only LSEs with BES assets (or assets that directly support the BES) should be included in the Applicability section of the standard.
Yes
Yes
There does not appear to be any reportable events for LSEs that do not own, operate, or control BES assets (or assets that directly support the BES) in Attachment 1. This would support removing such entities from the Applicability.
Yes
In general, the measures are okay. However, as mentioned above for R3, there needs to be more specificity as to what is acceptable as a "mock Impact Event" for auditing purposes--especially for small entities such as LSEs that do not own, operate, or control BES assets.
Yes
Yes
Yes
Yes
Occidental Power Marketing appreciates the extensive work accomplished by the SDT and their responsiveness to

comments. Also, the presentation of this draft with its extensive explanation of the SDT's considerations during development of the draft were very helpful in preparing our comments.
Individual
Eric Ruskamp
Lincoln Electric System
1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators, 6 - Electicity Brokers, Aggregators
Yes
No
As currently drafted, the proposed definition of “Impact Event” appears vague and provides entities minimal clarity in terms of distinguishing events of significance. Recommend the drafting team reference “Attachment 1: Impact Events Tables” within the definition to direct industry towards more specific criteria.
Yes
Yes
Yes
Yes
Yes
No
As currently drafted, requirement R3 states one must “conduct a test” whereas the associated Measure requests evidence that one “conducted a mock Impact Event”. The Rationale box lends to further confusion by referencing a “drill or exercise” as a process to verify one’s Operating Process. To avoid potential confusion between R3 and M3, as well as to maintain consistency with the Rationale box, recommend the drafting team replace the word “test” with “drill or exercise” within R3 and the associated Measure.
Yes
Yes
No
While LES supports the bright line criteria listed in Attachment 1 for reporting Impact Events, we have concerns regarding the reporting threshold for “Transmission loss”. For Transmission loss of three or more Transmission Elements, LES supports the MRO NSRS’ suggested wording of “Two or more BES Transmission Elements that exceed TPL Category D operating criteria or its successor.”
Yes
Yes
Yes
Yes
Yes
Individual
Linda Jacobson
Farmington Electric Utility System
3 - Load-serving Entities
Yes
Yes

Yes
Yes
Yes
No
consider rewording 1.4; the wording implies a change to content already occurred, so it would be updated concurrently – consider, updating the plan within 90 days of discovery of content requiring a change?
Yes
No
The measure for R3 indicates an actual Impact Event would count as a test, consider aligning the requirement with the measure to clarify an Impact Event could be considered a test.
Yes
A review of the Impact Event Operating Plan can be interrupted as an informal examination of the plan. The measure for R4 indicates evidence of a review, parties conducting the review AND when internal training occurred. It should be clarified in R4 training is expected as part of the review for personnel with responsibilities. This is an improvement from the previous 5.3 and 5.4; however, the team should consider adding back, 'review/training shall be conducted prior to assuming the responsibility in the plan.'
Yes
Yes
No
See comments in requirements for R3 and R4
Yes
Yes
Yes
Yes
Nine months would be preferred
Individual
Andrew Z Pusztai
American Transmission Company
1 - Transmission Owners
Yes
No
ATC does not agree with the proposed definition and further disagrees whether a definition is needed at all. Proposed Definition: The definition, read outside of the proposed standard, does not provide Registered Entities with a clear meaning of the purpose of the definition. It is ATC's opinion that the SDT is using the term "Impact Event" as an introduction phrase to Attachment 1. ATC would be more comfortable if the definition was dropped and the team would re-write the requirement to specifically point to Attachment 1. It is our opinion that this type of structure would achieve the goal of the team to get Registered Entities to report on events identified in Attachment 1. The other option is for the team to write into the definition that the events being discussed are limited to those identified in Attachment 1. Also the language currently being used in the definition includes "potential" and "such as". These terms should be struck from the definition.
Yes
No
First, under Part A, the reporting requirement for three or more BES Transmission Elements will create confusion. The NERC definition for an Element is: "Any electrical device with terminals that may be connected to other electrical

devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An element may be comprised of one or more components." This could be interpreted to be three potential transformers on a bus section; therefore, any bus section would require a report. It is suggested that this be reworded to indicate three or more BES transmission lines, bus sections, or transformers. Second, under Part A, the reporting requirement for "Damage or destruction of BES equipment" is too broad and needs to be modified. For example, an output contact on a relay could be damaged unintentionally during routine testing resulting in a reportable event. It is suggested that the list of BES equipment and full intent of this be further defined in the footnote. The intent needs to be clarified, such as "events that have an immediate and significant impact to the stability or reliability of the BES." Third, under Part A, the reporting requirement for "Damage or destruction of a Critical Cyber Asset" is too broad and needs to be modified. For example, an output contact on a relay could be damaged unintentionally during routine testing resulting in a reportable event.
Yes
Yes
No
ATC does not agree with the proposed language in Requirement 3. ATC is concerned that, in order to demonstrate compliance, an entity will have to show that each step in the plan was followed which will likely leave entities facing the choice of choosing between different compliance violations. If the plan is not followed, but the report is made within the time given, then an entity is in violations of their plan. If the plan is followed, but the report does not get filed within the time allotted, then they face a possible violation of the time to report. ATC believes that the team should enforce the position that the report being filed in the time allotted is key, not that they necessarily follow and document that their plan was followed. Depending on the situation, the internal reporting will vary; however, based on the purpose of the Standard, the key is to get a report to NERC.
Yes
Yes
No
Attachment 2, Task #14 in the report should be modified to read, "Identify any known protection system misoperation(s)." If this report is filed quickly, there is not enough time to assess all operations to determine any misoperation. As a case in point, it typically takes at least 24 hrs. to receive final lightning data; therefore, not all data is available to make a proper determination of a misoperation
No
Energy Emergency requiring Public Appeal ATC believes that the phrase "initiating entity" is unclear and could be interpreted in multiple ways. 1) the entity has the authority to call for public appeals, 2) the entity has the authority to declare an Energy Emergency, or 3) the entity determines and identifies the need for the Energy Emergency Typically the BA's call for public appeals, so does every BA that calls for the public appeal have to make a filing? The RC declares the need for an Energy Emergency, so are they the initiating entity? A TOP could also identify the need for public appeals and notify the RC about the request. In this case, is the TOP the initiating entity? Given the above examples, ATC believes that the SDT needs to clarify who is required to make the filing. Voltage Deviations on BES Facilities ATC believes that this should be clarified because one may assume that a loss of a single bus in which voltage goes to zero for more than 15 minutes is reportable. It is ATC understands that what the SDT means is a voltage dip, not an outage to a BES facility. However, given the brief description, ATC is not 100% sure whether there is a clear understanding of the standard's intent. Energy Emergency resulting in automatic firm load shedding Please provide additional clarify. ATC believes that the SDT should not use the term "Impact Event" when identifying the entity with reporting responsibility. The term "Impact Event" is identified in the standard and points to Attachment 1 but now is being used outside of that context and requires entities to interpret what qualifies as an Impact Event. The above observation also applies to those other events that use the term "Impact Event" to describe Reporting Responsibility. Footnote 1: ATC would like the phrase "as determined by the equipment owner" added to the footnote. This simple phrase will allow entities to be sure that they are responsible for determining if the damage significantly affects the reliability margin of the system. Without this phrase, entities could be subject to non-compliance actions based on differences of opinions to the extent of the damage on the system. The other option the SDT has is to provide additional clarity on what qualifies as a significant affect. Time to Submit Report: ATC strongly disagrees with the 1 hour time to submit a report because it does not fit with the purpose of this standard. The purpose of this standard is to increase awareness, however, requiring a one-hour reporting window following the event provides little to no benefit. ATC believes that these events should have a 24 hour reporting window which allows for a reasonable amount of time to gather information and report the issue. If the SDT disagrees with this observation, ATC believes a complete explanation should be provided on why knowledge of an event within an hour is significantly better than having the knowledge of the event in a 24 hour time period. ATC strongly believes that NERC will gain as much or more knowledge of the event by giving entities time to understand the event and report.
Yes

Yes
Yes
Yes
Yes
Group
LG&E and KU Energy LLC
Brent Ingebrigtson
No
In Attachment 1, the existing EOP-004-1 Attachment 1, point 6 includes an “Or” for the entities (RC, TOP, GOP) for a, b and c. The way the SDT has pulled this apart, they have included the GOP as having an impact on the Voltage Deviations on BES Facilities. The TOP monitors the transmission system and directs GOPs when they need to change in order to protect the system reliability. This is not something the GOP is responsible for monitoring. The GOP is required to be at the TOP assigned voltage schedule and that actually falls under VAR-002 already. Please remove the GOP from the line of “Voltage Deviations on BES Equipment.” The way EOP-004-1 Attachment 1 point 6 is currently written, the GOP is an “or” and does fall into parts b or c, where part 6b is similar to the proposed line “Damage or destruction of BES equipment” identified in the proposed EOP-004-2 Attachment 1. However, currently the GO/GOP reports “Loss of Major System Components” on EOP-004-1 within 24 hours of determining damage to the equipment. The proposed “One hour” is too tight of a window as the GO/GOP often do not know the extent of damage that soon. Typically the OEM is called upon to come and do a thorough inspection and assess the extent of damage, of if there even is any damage; once the “loss of major system components” is determined, then the 24 hour clock begins today.
Individual
Michelle D'Antuono
Ingleside Cogeneration LP
5 - Electric Generators
Yes
The addition of the modifier “if known” to reporting the cause of an Impact Event is appropriate. It often proves counter-productive to speculate – as initial conjectures of the cause of an event are easy to come up with, but difficult to back out of later.
No
The SDT includes in the definition the “potential to impact the reliabilty of the BES”. This seems vague, although ultimately the events which meet the threshold of a reportable Impact Event are governed by the tables under Attachment 1. We believe that there should be close, if not perfect, synchronization between the ERO’s Event Analysis Process and Attachment 1 since they share the same ultimate goal as EOP-004-2 to improve industry awareness and BES reliability.

Yes
Sabotage cannot be confirmed until after the fact, so we support this initiative.
No
Owners and operators of facilities whose total removal from the BES would not meet any reportable threshold under Attachment 1, should not have to create and maintain Operating documents. The same would be true of any LSE, TSP, or IA that does not oversee any Critical Cyber Assets as identified under CIP-002. A statement to that effect could be made in Section 4 of EOP-004-2.
Yes
Ingleside Cogeneration agrees that the NERC Rules of Procedure are the appropriate location for ERO assigned activities. However, we would like to get a solid commitment from NERC that the Events Analysis Process and the Reliability Assessment and Performance Analysis Group (RAPA) data analysis requirements for Protection System Misoperations is coordinated through a single process. Their unique data needs are understandable, but should not require the downstream entity to evaluate what is required by each sub-committee – and which reporting template to use.
Yes
Yes
No
Since the reporting of event data to regulatory agencies does not support a front-line operations capability to mitigate or restore a BES impairment, regular simulations are not needed. Those notification items which test coordination between operating entities can be addressed in emergency operations exercises.
Yes
Yearly refresher training on the reporting process is appropriate. Ingleside Cogeneration also agrees that a “review” with those individuals with assigned responsibilities under the Operating Plan is a better way to frame the requirement.
Yes
Although our preference would be to have a single form, Ingleside Cogeneration realizes that is not likely in the near term. We would like to see that remain as a goal of the project team or the ERO.
Yes
We believe that there should be close, if not perfect, synchronization between the ERO’s Event Analysis Process and Attachment 1 since they share the same ultimate goal as EOP-004-2 to improve industry awareness and BES reliability.
Yes
Yes
Yes
Yes
Yes
Group
Midwest ISO Standards Collaborators
Marie Knox
Yes
No
The definition of Impact Event is overly broad because of the use of “potential to impact” and the “Such as” list. Consider routine switching has the potential to result in a mis-operation. This means all routine switching is an impact event. The “Such as” list should be struck and “potential” language should be struck.
No
In general, we agree that the standard drafting team has provided an equally efficient and effective alternative, but we wonder if the SDT has not in essence already defined sabotage in their description for why they can’t define sabotage. It seems that sabotage involves willful intent to destroy equipment. In general, intent would have to be determined by

an investigation of law enforcement. This could be part of the definition. There might be some obvious acts that could be included without investigation such as detonation of a bomb. Is it possible for the SDT to use the DOE definition for sabotage? We encourage the SDT to provide a definition for sabotage.
Yes
No
We see no issue with imposing requirements on NERC. However, we are not opposed to making these changes in the Rules of Procedure either.
No
We do not believe that the use of the Operating Process, Operating Procedure, and Operating Plan for a reporting requirement is consistent with their definitions and certainly not with the intent of the definitions. For instance, an Operating Process is intended to meet an operating goal. What operating goal does this requirement meet? An Operating Procedure includes tasks that must be completed by “specific operating positions”. This reporting requirement could be met by back office personnel. We also believe that parts 1.3 and 1.3.2 under Requirement 1 will require notification of law enforcement agencies for all Impact Events defined in Attachment 1. While some should require notification to law enforcement such as when firm load is shed, others certainly would not. For instance, law enforcement does not need to know that an IROL violation, generation loss or voltage deviation occurred.
Yes
No
We appreciate the drafting team recognizes that actual implementation of the plan for a real event should qualify as a “test”. However, we are concerned that review of this requirement in isolation of the background material and information provided by the drafting team may cause a compliance auditor to believe that a test cannot be met by actual implementation. Furthermore, we do not believe testing a reporting procedure is necessary. Periodic reminders to personnel responsible for implementing the procedure make sense but testing it does not add to reliability. If they don’t report an event, it will become obvious with all the tools (SAFNR project) the regulators have to observe system operations.
Yes
No
Requirement 2 and Requirement 5 appear to be very similar. Requirement 2 requires implementation of the Operating Plan, Operating Process and/or Operating Procedure in Requirement 1. The Operating Procedure requires gathering and reporting of information for the form in Attachment 2. What does Requirement 5 add that is not already covered in Requirement 2 except the ability to use the DOE OE-417 reporting form which could be included in Requirement 2?
Yes
No
We disagree with Measurement 4. It implies that the review must be conducted in person. Why could other means such as a web training or a reminder memo not satisfy the requirement? Because Requirement 1 does not require submittal of the Operating Plan, Operating Process and/or the Operating Procedure, Measurement 1 should only require submittal to the Compliance Enforcement Authority upon its request.
No
All violation risk factors should be Lower. All requirements are administrative in nature. While they are necessary because a certain amount of regulatory reporting will always be required, a violation will not in any direct or indirect way lead to reliability problem on the Bulk Electric System
Yes
No
R2 and R5 should be Operations Assessment since it deals with after the fact reporting. R3 should included Operations Assessment since an actual event could be used as the test.
Yes
We believe the reporting time lines are too aggressive for some events. Reporting events within an hour is not reasonable as an entity may still be dealing with the event. This will be particularly difficult when support personnel are not present such as during nights, holidays, and weekends.
Individual
Greg Rowland
Duke Energy

1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators, 6 - Electicity Brokers, Aggregators
Yes
However, as we have noted previously, the DSR SDT statement that the proposed changes do not include any real-time operating notifications is inconsistent with requiring notification within one hour for thirteen of the twenty listed Events in Attachment 1 “Impact Event Table”. Also, in the Background discussion, under Law Enforcement, the DSR SDT states that the objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting Impact Events. As we have previously commented, we are still required to make real-time reports under other standards. Requiring duplicate real-time reporting under EOP-004-2 is a waste of resources which could otherwise be used to improve reliability.
No
The phrase “or has the potential to impact” makes this an impossibly broad definition, and demonstrating compliance will not be straightforward.
No
Sabotage is still identified on the flowchart. Timeframes for reporting on Attachment 1 should be made consistent with DOE OE-417 reporting. Also on Attachment 1, the Threshold for Reporting on a Forced Intrusion Event should be “Affecting BES reliability” instead of “At a BES facility”.
No
Section 4 is fine, but on Attachment 1, Entity with Reporting Responsibility should just identify “Initiating entity” for every Event, as was done with the first three Events. That way you avoid errors in leaving an entity off, or including an entity incorrectly (as was done with the GOP on Voltage Deviations).
No
Proposed language for Section 812 is very confusing. Is the NERC “system” really going to perform all notifications: “applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, and regulatory agencies as necessary”? Is it intended that the NERC “system” will relieve registered entities of the obligation to make these other reports? Is there an implementation plan to achieve that objective? It appears that this current version of EOP-004-2 has the potential for significantly creating redundant reporting. Will the NERC reports be protected from FOIA disclosure? How will FERC Order 630 be followed (CEII disclosure)?
Yes
Yes
Yes
We understand that the objective of this requirement is to test the Operating Process for communicating Impact Events; and that such test could be an actual exercise, a formal review, or a real-time implementation. But given that R1.4 requires updating the Operating Plan within 90 days of any changes, we believe the VRF for R3 should be LOW instead of MEDIUM.
Yes
Yes
There is so much overlap between Attachment 2 and the DOE OE-417 that we believe the DOE OE-417 should be revised to include the additional items that must be reported to NERC, so that there is only one form to submit to NERC and DOE.
No
• Attachment 1 contains three reportable events (Damage or destruction of Critical Asset, Damage or destruction of a Critical Cyber Asset, and Detection of a reportable Cyber Security Incident) that overlap with CIP-008-3 Cyber Security Incident Reporting and Response Planning and could result in redundant or conflicting content between the two standards. We propose either of the following options: 1. Remove the requirement for reporting these events from EOP-004-2 and add the timing and reporting requirements into CIP-008-3, R1.3. “Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.” OR 2. Replace the reporting requirement in CIP-008-3, R1.3. with a reference to report as required in EOP-004-2. • Also, as noted in our comment to Question #4 above, the Attachment 1 Section “Entity with Reporting Responsibility” should just identify “Initiating entity” for every Event, as was done with the first three Events. That way you avoid errors in leaving an entity off, or including an entity incorrectly (as was done with the GOP on Voltage Deviations). We note that LSE is listed in the standard as an Applicable entity, and should be included in Attachment 1. Our suggestion would handle this oversight. We also note that CIP-001 does not include Distribution Provider in the list of applicable entities, but EOP-004-2 does include the DP. • We reiterate our comment to Question #1 above that the DSR SDT statement that the proposed changes do not include any real-time operating notifications is inconsistent with requiring notification within one hour for thirteen of the twenty listed Events in Attachment 1. • The last six events refer to the entity that experiences the potential Impact Event. We believe that the word “potential” should be struck, as this

creates an impossibly broad reporting requirement. • Footnote 1 should be revised to strike the phrase “has the potential to” from the parenthetical, as this creates an impossibly broad reporting requirement. • The Impact Event “Risk to BES equipment” should be revised to “Risk to BES equipment that results in the need for emergency actions”. The accompanying footnote 4 should be revised to read as follows: Examples could include a train derailment adjacent to BES equipment (e.g. flammable or toxic cargo that would cause the evacuation of a BES facility control center), or a report of a suspicious device near BES equipment.
Yes
Yes
Yes
Yes
Yes
Individual
Amir Hammad
Constellation Power Generation
5 - Electric Generators
Yes
While CPG generally agrees with the purpose statement, we believe that the term Impact Events should be removed. Please see CPG’s response to Question 2 discussing the term Impact Events.
No
The currently proposed definition is vague and can be easily misinterpreted. Coining a term to define the events that the DSR SDT hopes to capture in EOP-004-2 is a difficult task, one that may not be necessary. Replacing the term “Impact Events” with “events in Attachment 1,” would eliminate the need to define such a term. In addition, the phrase “… or has the potential to impact the reliability…” is too vague and broad. Such broad statement is unhelpful in clarifying entities’ compliance obligation and potentially creates conflicted reporting between entities. The language in the reporting requirements should be limited to real impact events, while information sharing on “near miss” or “deficiency” incidents should be handled as good industry practices and not subject to onerous compliance obligations. The drafting team should also give careful consideration to the existing reporting and information sharing currently in place in the industry. When an event occurs, partners in the electric sector are notified as part of existing requirements outside of NERC compliance.
Yes
No
As stated in comments to earlier versions of EOP-004-2, CPG disagrees with the inclusion of Generator Owners. Since one of the goals in revising this standard is to streamline impact event reporting obligations, Generator Operators are the appropriate entity to manage event reporting as the entity most aware of events should they arise. At times, the information required to complete a report may warrant input from entities connected to generation, but the generator operator remains the best entity to fulfill the reporting obligation.
Yes
No
Per NERC’s glossary of terms, an Operating Plan can include Operating Process documents and Operating Procedures. An Operating Process identifies general tasks while an Operating Procedure identifies specific tasks. CPG is unclear as to why R1.1 and R1.3 require the use of an Operating Process while R1.2 requires an Operating Procedure. CPG believes that R1.2 should be changed to require the use of an Operating Process instead of Operating Procedure. R1.2 is merely requiring an entity to fill out the necessary forms should an event occur, so requiring a clear and concise step by step procedure for filling out a form only adds a compliance burden to an entity instead of improving the reliability of the BES. CPG does agree with the DSR SDT that an entity should have a process in place mandating that the proper paperwork be completed in a timely manner should an event occur.
Yes
Although CPG agrees with the wording of Requirement 2, CPG has several comments and suggested changes regarding the Attachments, to which this requirement points. Please see those comments below.
No

As CPG stated in comments to earlier versions of EOP-004-2, this requirement adds a substantial compliance burden with little to no reliability improvement to the BES. Numerous entities in the NERC footprint have created fleet wide compliance programs for their facilities, instead of overseeing multiple stand alone compliance programs. This was done not just for the ease of administration, but it also greatly improves the reliability of the BES by ensuring consistency across multiple facilities. By requiring each responsible entity to test the Operating Process, those under a fleet wide compliance program will end up testing the same Operating Process numerous times. This would be inefficient, ineffective and unnecessarily costly. If the testing requirement remains, then the Responsible Entity should be able to take credit for testing of the Operating Process regardless of which entity in the fleet tested it. Alternatively, the drafting team should consider removing Requirement 3 (formerly R4) because in practice it is covered by the new R4. As discussed below R4 needs refinement, but the topic of Disturbance Reporting is covered during annual training.
No
The purpose of this requirement as currently worded is unclear. It seems to insinuate that a formal review of the Operating Plan takes place annually, and that any and all personnel identified in the plant are part of the review. If that is correct, than CPG believes this requirement is echoing Requirement 3. These two requirements can be incorporated into one. Furthermore, the Measure for R4 is too prescriptive, going so far as to specifically describe how this formal review should take place. It even states that the Responsible Entity needs to present documentation showing that the personnel in the plan were trained, yet there is no requirement for training. CPG would like the DSR SDT to revisit the purpose and intent of this requirement, alone and in concert with R3. If there are indeed similar then consolidate them into one requirement.
No
The requirements for filling out the DOE-OE-417 form are not necessarily the same as the requirements prescribed in Attachment 1. CPG suggests that the drafting team create a new requirement, spelling out when an entity is required to complete the DOE-OE-417 form.
No
CPG has the following concerns regarding Attachment 1: •Real-Time - On page 5 of the proposed standard, the team noted that “the proposed changes do not include any real-time operating notifications.” However, several events in Attachment 1 require that documentation be completed and submitted to the ERO within 1 hour. For generation sites that are unmanned, or only have 1 to 2 operators on site at all times, a 1 hour requirement is not only onerous but is essentially “real time.” •Response within 1 hour - It is important to consider the imposition created by a compliance obligation and weigh it against the other demands before the operator at that time. A compliance obligation should avoid becoming a distraction from reliability related work. Under impact event type scenarios, in the first hour of the event, the primary concern should be coping with/resolving the event. Other notification requirements exists based on required agency response relative to the concern at hand (e.g. public evacuations, fire assistance, etc.) Notification within an hour under EOP-004 does not appear to represent a relevant benefit to resolving the situation and the potential cost would be borne by reliability and recovery efforts. Anything performed within the first hour of the event must be to benefit the public or benefit the restoration of power. •Damage or destruction of BES equipment – the reporting requirement of 1 hour is extremely onerous. A good example is the failure of a major piece of equipment at a remote combustion turbine generation site. Combustion turbine generation sites are not usually manned with many people. If a failure of a major piece of equipment were to occur, the few people on site need to complete communications to affected entities, communications to their management, as well as emergency switching and ensuring that no other pieces of equipment are effected or harmed. There is little time to complete a form in 1 hour. This should be changed to 48 hours. The form is also inadequate for this type of event. o Using the example above of a failure of a major piece of equipment, CPG is not sure if it’s reportable per Attachment 1, which further proves that Attachment 1 is not clear. Per the footnote regarding damage to BES equipment, the failure would not be reportable, as it does not affect IROL, given the information at the plant it does not significantly affect the reliability margin of the system, and was not damaged or destroyed due to intentional or unintentional human action. However, it would be reportable per the table as the table states “equipment failure” and “external cause.” Clarification is needed. •Damage or destruction of Critical Asset – This item should be removed or significantly refined. For generation assets, a critical asset is essentially the entire plant, so in many cases the information reported at this level would not be useful if the valuable details reside at the equipment level. If it is not removed, then see the notes above on the 1 hour requirement for the completion of the form. •Fuel supply emergency – 1 hour for reporting the document is unreasonable. See the earlier notes. •Risk to BES equipment – “From a non-environmental physical threat” This item is too vague and subjective. A catch all category to capture a broad list of potential risks is problematic for entities to manage in their compliance programs and to audit. This should be removed.
No
See CPG’s earlier comments regarding the Requirements and Measures.
CPG has the following comments regarding Attachment 2: •Generally, this attachment is inadequate for all events. The real-life experience with the recent SW cold snap demonstrated that the questions inadequately capture what may be

of greatest concern in the situation. •Question 4 – this question is vague. It should be removed. •Question 7 – the role of generation in an event may not always be related to a trip. As experienced with the recent SW cold snap, this question may inadequately capture information relevant to the situation at hand. The drafting team should reassess how best to gather information relevant to the event and useful for evaluation. •Question 8 – generation is not required to monitor frequency during events, so this would not be answered. This question also assumes that frequency had been impacted, which is not always the case (i.e., the plant could not come online). •The asterisk on some questions in Attachment 2 is not defined.
Group
FirstEnergy
Sam Ciccone
Yes
No
Although we agree with the definition of Impact Event, we believe that it should be clear that this term is specific to the events listed in Attachment 1 of the standard. Therefore, we suggest adding the phrase “(as detailed in Attachment 1 of EOP-004-2)” in the definition.
Yes
No
Attachment 1, Part A – Energy Emergency requiring Public appeal for load reduction – In the current draft Standard, the applicability has been revised from an RC and BA to "initiating entity". We can’t see where the GO/GOP would ever make this determination. Needs to be clarified. Attachment 1, Part A – Energy Emergency requiring system-wide voltage reduction – In the current draft Standard, the applicability has been revised from an RC, TO, TOP, and DP to "initiating entity". We can’t see where the GO/GOP would ever make this determination. Needs to be clarified. Attachment 1, Part A – Voltage Deviations on BES facilities - A GOP may not be able to make the determination of a +/- 10% voltage deviation for ≥ 15 continuous minutes, this should be a TOP RC function only. Attachment 1, Part A - Loss of offsite power (LOOP) classification should not apply to nuclear generators. The impact of a LOOP is dependent on the design of the specific nuclear unit and may not necessarily result in a unit trip. If a LOOP did result in a unit trip, the NRC requires notification by the nuclear GO/GOP via the Emergency Notification System (ENS), and time allowed for that notification (1 hour, 4 hours, 8 hour, or none at all) is, as mentioned above, dependent on the design of the plant. We believe it would be beneficial if consideration were given to coordinating reporting requirements for nuclear units with existing required notifications to the NRC to avoid duplication of effort. Attachment 1 should align NERC Standard NUC-001 concerning the importance of ensuring nuclear plant safe operation and shutdown. If a transmission entity experiences an event that causes a loss of off-site power as defined in the nuclear generator’s Nuclear Plant Interface Requirements, then the responsible transmission entity should report the event within 24 hours after occurrence. Also, for clarity "grid supply" should be replaced with "source" to ensure that notification occurs on a loss of one or multiple sources to a nuclear power plant. Attachment 1, Part A – Damage or destruction of BES equipment. See Nuclear comments on question 17 below. Attachment 1, Part B – Forced intrusion at a BES facility. See Nuclear comments on question 17 below. Attachment 1, Part B – Risk to BES equipment from a non-environmental physical threat. What constitutes a "risk" to the reporting entity is still somewhat ambiguous, and although the DSR SDT has provided some examples, without more specific criteria for this event the affected entity will have difficulty in determining within 1 hour if a report is necessary. Also, see Nuclear comments on question 17 below.
Yes
No
1. We believe that the use of stringent definitions for an entity’s process requires too much of the “how” instead of the “what”. As long as the entity has a process, procedure (or whatever they want to call it) that includes the necessary information detailed in sub-parts 1.1 through 1.4 then that should suffice. 2. In sub-part 1.3, we suggest adding the phrase “as applicable” to clarify that not every event will require a notification to, for example, law enforcement. 3. In sub-part 1.4, we suggest adding clarification that the 90-day framework is only required for substantive changes and that all other minor editorial changes can be updated within a year.
Yes
No
We believe that a separate requirement for testing the reporting process is unnecessary. The FERC directive that required periodic testing was directed at sabotage events per CIP-001. Since the proposed standard moves the responsibility for classifying an event as sabotage from the entity to the applicable law enforcement authority, the need for a periodic drill is no longer necessary. We believe that Requirement R4 should suffice in ensuring that the individuals involved in the process are aware of their responsibilities.
No

We believe that Requirement 4 does not warrant a “Medium” risk factor. For example, a simple review of the process does not have the same impact on the Bulk Electric System as the implementation of the Operating Plan per R2. Therefore, we believe R4 is at best a “Low” risk to the BES.
No
We believe that Requirement 5 does not warrant a “Medium” risk factor. Not using a particular form is strictly administrative in nature and the VRF should be “Low”.
No
Nuclear facilities should be explicitly excluded from the events which have CIP standards as the threshold for reporting since they are exempt from the CIP standards.
No
Measure M4 includes the phrase “when internal personnel were trained on the responsibilities in the plan” implies the Requirement R4 requires training. R4 is only requiring the review of a document of the necessary personnel and that the rest of the measure covers the needed evidence for R4. This phrase in the measure should be removed. We suggest the following for M4: M4. Responsible Entities shall provide the materials presented to verify content and the association between the people listed in the plan and those who participated in the review, documentation showing who was present.
No
1. We believe that Requirement 5 does not warrant a “Medium” risk factor. Not using a particular form is strictly administrative in nature and the VRF should be “Low”. 2. We believe that Requirement 4 does not warrant a “Medium” risk factor. For example, a simple review of the process does not have the same impact on the Bulk Electric System as the implementation of the Operating Plan per R2. Therefore, we believe R4 is at best a “Low” risk to the BES.
Yes
No
We believe the previous proposal for a 12 month implementation was more appropriate and suggest the team revert back to that timeframe.
FE offers the following additional comments and suggestions: 1. In the Background section of EOP-004-2, on page 6 under Stakeholders in the Reporting Process, we suggest adding “Regional Entity” and “Nuclear Regulatory Commission”. 2. The DSR SDT makes reference to comments that Exelon provided that suggested adopting the NRC definition of "sabotage." We feel the comment made by Exelon in their previous submittal was to ensure that the DSR SDT included the Nuclear Regulatory Commission (NRC) as a key Stakeholder in the Reporting Process and FE agrees with this suggestion. Nuclear generator operators already have specific regulatory requirements to notify the NRC for certain notifications to other governmental agencies in accordance with 10 CFR 50.72(b)(s)(xi). We ask that the DSR SDT contact the NRC about this project to ensure that existing communication and reporting that a licensee is required to perform in response to a radiological sabotage event (as defined by the NRC) or any incident that has impacted or has the potential to impact the BES does not create either duplicate reporting, conflicting reporting thresholds or confusion on the part of the nuclear generator operator. We believe this is a similar situation as what was recently resolved between NERC and the NRC concerning the applicability of CIPs 002 – 009 for nuclear plants. Each nuclear generating site licensee must have an NRC approved Security Plan that outlines applicable notifications to the FBI. Depending on the severity of the security event, the nuclear licensee may initiate the Emergency Plan (E-Plan). We ask that the proposed "Reporting Hierarchy for Impact Event EOP-004-2," flow chart be coordinated with the NRC to ensure it does not conflict with existing expected NRC requirements and protocol associated with site specific Emergency and Security Plans.
Individual
Scott Barfield-McGinnis
Georgia System Operations Corporation
3 - Load-serving Entities, 4 - Transmission-dependent Utilities
Yes
We agree with the purpose. However, we do not agree that the purpose will be achieved as this standard is currently drafted or that the standard is ready for balloting.
No
It is not clear for the purposes of complying with this standard what it means to “impact reliability.” Impact in what way? To what degree? Do not define this term. An alternative would be to define it as those events listed in Appendix 1.
Yes
None.
No
We do not agree that this standard assigns clear responsibility for reporting. It seems that multiple entities are being required to report the same event for some events. Only one entity should report. See comments later regarding

Attachment 1. NERC should not decide which ONE entity should report. The entities should be allowed to decide this (and include it in the Impact Event Operating Plan) and to let NERC or the region know who will report (or give them a copy of the plan).
Yes
None.
No
-R1.3.2: “Law Enforcement”, “Governmental Agencies”, and “Provincial Agencies” are not proper nouns/names and are not defined in the NERC Glossary. They should not be capitalized. -R1.4: Keeping documents current and in force should be a matter of an entity’s compliance program and not of a NERC requirement. It is not clear what the difference is between “updating the Impact Event Operating Plan” and changing “its content.” How is compliance with this measured? Delete R1.4.
No
-We suggest moving the language from the measure to the requirement as such: "To the extent that a Reponsible Entity has an Impact Event on its Facilities, each Responsible Entity shall implement…" Additionally, R1 uses the phrase "recognized Impact Event" where as R2 simply uses the term "Impact Event." The phrase "recognized Impact Event" should be used consistently in R2 as well.
No
-With the current CAN on the definition of annual, we do not believe that the additional qualification that the test shall be conducted "with no more that 15 calendar months between tests" is necessary. Although we understand the additional qualification is used in the VSL matrix, we recommend removing "with no more that 15 calendar months between tests" and rely on the Responsible Entity's definition of annual and not to exceed timeframes. -We suggest moving the language from the measure to the requirement as such: "In the absense of an acutal Impact Event, each Responsible Entity shall …"
No
-With the current CAN on the definition of annual, we do not believe that the additional qualification that the test shall be conducted "with no more that 15 calendar months between reviews" is necessary. Remove "with no more that 15 calendar months between reviews". -R3 requires testing the process. R4 requires reviewing the plan. Testing a process and reviewing a plan both seem to imply verifying the process/plan is correct and the appropriate actions will take place. Training implies making personnel aware of and providing them an understanding of what the process/plan involves and not verifying whether or not it is correct or appropriate. It is not clear what is being required in R4. -The measure says that documentation showing when personnel were trained is required. R4 does not require training. The requirement and the measure should be made clear and consistent.
No
R5: This standard should not require all Responsible Entities to report the same event. Entities should be allowed to report in a hierarchical manner. They should be allowed to coordinate impact event plans and include in their plans the entity that has the responsibility for reporting various events. Flexibility should be allowed to provide different reporting entities depending on the type of event. In R5, does “Each Responsible Entity shall report Impact Events in accordance with the Impact Event Operating Plan …” allow this hierarchical reporting and flexibility? An entity should be allowed to report to another operating entity by whatever reporting form or mechanism works and then the other entity reports to NERC using the required NERC or DOE form. Add "To the extent that a Responsible Entity had an Impact Event," at the beginning of R5 and M5.
No
Energy Emergency requiring public appeal for load reduction: -The NERC Glossary defines “Energy Emergency” as a “condition when a Load-Serving Entity has exhausted all other options and can no longer provide its customers’ expected energy requirements.” Per EOP-002, an Energy Emergency Alert may be initiated by the RC upon RC sole discretion, upon BA request, or upon LSE request. -Question: Is it intended that the LSE reports the event if the LSE requests an alert, the BA reports the event if the BA requests an alert, and the RC reports it if it is a RC sole discretion decision? What if an alert is not initiated? Is it an Energy Emergency? Is it an impact event? Who must initiate the public appeal? Since it must be reported within a certain time after the issuance of the public appeal, is it not an impact event until after the initiation of the public appeal (which should be after the initiation of the alert)? Shouldn’t the reporting of the impact event be done by the initiator of the public appeal? The event should probably be the public appeal and not the Energy Emergency. -“Public” should not be capitalized. -The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained. • Energy Emergency requiring system-wide voltage reduction: See Energy Emergency requiring public appeal for load reduction above regarding requesting Energy Emergency Alerts. If this event is to be reported within a certain time after “the event”, at what time is the event marked? Or is it within a certain time after the initiation of the voltage reduction and, if so, shouldn’t the reporting of the impact event be done by the initiator of the voltage reduction? The event should probably be the system-wide voltage reduction and not the Energy Emergency. The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and NERC does not need to know this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained. Energy Emergency requiring manual firm load shedding: -See Energy Emergency requiring public appeal for load reduction above regarding requesting

Energy Emergency Alerts. If this event is to be reported within a certain time after “the event”, at what time is the event marked? Or is it a certain time after the initiation of the shedding of load, if so, shouldn’t the reporting of the impact event be done by the initiator of the shedding of the load? If the RC directs a BA to shed load, then the BA directs a DP to do it, then the DP sheds the load, who is the initiator of the load shedding? The event should probably be the firm load shedding and not the Energy Emergency. -The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained. Energy Emergency resulting in automatic firm load shedding: Whenever load is automatically shed both the DP and the TOP “experience” the event. So does the BA and the LSE. This event includes “or” between “DP” and “TOP.” Is that intentional? Other events in the table do not include either an “and” or an “or.” The entities are separated only by commas. NERC should not require multiple entities to report the same event. See comment for R5 above. If a DP "experiences" an automatic load shedding doesn't the TOP also experience it? Both should not report the same event. -The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained. Voltage deviations on BES Facilities: -Should GOs/GOPs be required instead to report to BAs when this condition exists with the BA then reporting to NERC? The idea of a deviation "on BES Facilities" is not clear. On any one Facility? On all Facilities in an area? How wide of an area? -“Voltage Deviation” is not proper noun/name and is not defined in the NERC Glossary. It should not be capitalized. IROL violation: Multiple entities should not report the same event. Please define “IROL Violation” or use lowercase. It is assumed that “IROL Violation” means operation “outside the IROL for a time greater than IROL TV.” Loss of firm load for ≥ 15 minutes: -Multiple entities should not report the same event. The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained. “Firm Demand” is defined but not “Firm load.” System separation (islanding): -Multiple entities should not report the same event. A DP separating from the transmission system should not be a reportable event for a DP in and of itself. If it leads to a sufficient loss of load, it is reportable as above. -The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained. The words “separation” and “islanding” should not be capitalized. Generation loss: -Should GOs/GOPs be required instead to report to BAs when their generation is lost with the BA then reporting to NERC when the total is ≥ 2,000 MW? A “loss” of generation should be clarified. Is the discovery of damaged equipment in an offline plant which makes the plant unavailable for an extended period of time a “loss” of generation? -It should be clarified if this event means the concurrent loss of the generation or losing the generation non-concurrently but they are concurrently unavailable. What is the time window for losing the generation? Lost within seconds of each other? Minutes? Hours? Loss of off-site power to a nuclear generating plant (grid supply): -Multiple entities should not report the same event. -“Off” should be lowercase. Transmission loss: -RCs should not be required to report the loss of transmission elements to NERC. A “loss” of a BES Transmission Element should be clarified.It should be clarified if this event means the concurrent loss of elements or the non-concurrent loss of the elements but they are concurrently unavailable. What is the time window for losing the elements? When elements are lost, it will be difficult to differentiate if they are BES Transmission Elements or not. Alarms don't immediately identify this. It could lead to gross over-reporting if no distinction is made by a TOP and the TOP reports all losses of 3 elements. It may still be over-reporting (from a reasonableness/practicality basis) even if the differentiation could be easily made and only BES Transmission Elements are reported. Threshold for reporting Transmission Loss: As stated, this will require the reporting of almost all transmission outages. This is particularly true taking into consideration the current work of the drafting team to define the Bulk Electric System. The loss of a single 115kV network line could meet the threshold for reporting as the definition of Element includes both the line itself and the circuit breakers. Instead, we recommend the following threshold "Three or more BES Transmission lines." This threshold has consistency with CIP-002-4 and draft PRC-002-2. This threshold also needs additional clarification as to the timeframe involved. Is the intent the reporting of the loss of 3 or more BES Transmission Elements anytime within a 24 hour period or must they be lost simultaneously? Also, we recommend that the three losses be the result of a related event to require reporting. Damage or destruction of BES equipment that i. affects an IROL; ii. significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); or iii. damaged or destroyed due to intentional or unintentional human action (Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly, e.g., removal of grounding straps rendering protective relaying inoperative.): -What is “BES equipment?” Would an operator know which equipment is BES equipment and which is not or which BES equipment affects an IROL (if we had one) or which does not? It is a judgment call as to whether the effect was significant or not or if it has the potential or not. Multiple entities should not report the same event. Unplanned control center evacuation: -“Control Center” should be lowercase. -The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained. Fuel supply emergency: Multiple entities should not report the same event. Should GOs/GOPs be required instead to report to BAs when they have a fuel supply emergency with the BA then reporting to NERC if the situation is projected to require emergency action at the BA level? -The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained. Loss of all monitoring or voice communication capability (affecting a BES control center for ≥ 30 minutes): -Does this event mean that ALL capability at both the primary and backup control centers or just one? Forced intrusion at a BES facility (report if you cannot reasonably determine likely motivation, i.e., intrusion to steal copper or spray graffiti is not reportable unless it affects (affects – not effects) the reliability of the BES): -What is a “BES facility?” It is not clear for the purposes of complying

with this standard what it means to affect the reliability of the BES. Deferred for ECMS review and additional comments. Risk to BES equipment (examples include a train derailment adjacent to BES equipment that either could have damaged the equipment directly or has the potential to damage the equipment, e.g., flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center, and report of suspicious device near BES equipment.): -In the footnote, delete “could have” from “…either could have damaged…” Something that could cause evacuation of a control center does not pose a risk to damaging BES equipment. The threshold is “from a non-environmental physical threat” but the example (toxic cargo) IS an environmental threat.
No
There are a lot of inconsistencies between the requirements and the measures. The measures add requirements that are not stated in the requirements. The measures need to be made consistent with the requirements and to not add to them. Also see comments on requirements earlier for language to move from the measures into the requirements. M2: Remove "on its Facilities." The word "its" leads to a lot of confusion regarding who reports what. Attachment 1 should make clear "what" needs to be reported. The entities' operating plan should make it clear as to who should report each "what." Furthermore, not all Impact Events are "on Facilities." M3: Replace "that it conducted a mock Impact Event" with "that it conducted a test of its Operating Process". Delete "The time period between actual and or mock Impact Events shall be nor more than 15 months." M4: The measure says that documentation showing when personnel were trained is required. R4 does not require training. The requirement and the measure should be made clear and consistent.
No
Failing to report to NERC any of many of the listed events does not present a reliability risk. The exception to this would be those threat events where the ES-ISAC needs to be notified. The object of the standard is to prevent or reduce the risk of Cascading. Reporting system situations to appropriate operating entities who can take some mitigating action (e.g., a LSE reporting to its BA or a BA reporting to its RC) and reporting threats to law enforcement officials could prevent or reduce the risk of Cascading but reporting to NERC (except for events where the ES-ISAC needs to know) is unlikely to do that. Reporting of most of the listed events to NERC does not meet the objective of this standard and should be removed from this standard. Such events should be reported to NERC through some other (than a Reliability Standard) requirement for reporting to NERC so that NERC can accomplish its mission of analyzing events. Analyzing events may lead to an understanding that could reduce the future risk of Cascading but analyzing events cannot be performed in time to reduce any impending risks.
No
None.
Yes
None.
No
There is nothing about the revisions that were made to the requirements that shortens the time needed by the industry to get prepared for this revision. The removal of requirements for NERC does not shorten the requirements for the industry. Eighteen months (or 12 months minimum) should be alloted to prepare for this revision.
Attachment 2: Impact Event Reporting Form -Instructions for filling out this form are needed. -Line 7, Generation tripped off-line: What is the asterisk for after this task and after the many others following? This should only be reported by a BA. Does generation “tripped off-line” mean the same as generation “lost?” -Line 9, List of transmission facilities (lines, transformers, buses, etc.) tripped and locked-out: Does this means the same as BES Transmission Elements lost? -Line 10: The column headings in white text on lighter blue background at the top do not seem to apply from this line on. -Line 11, Restoration Time: Restoration of what? Initial/Final clock time? Transmission? What about transmission? Generation/Demand? -Line 13, Identify the initial probable cause or known root cause of the actual or potential Impact Event if known at time of submittal of Part I of this report: “At the time of submittal of Part I of this report”?? Where is Part II? Did you mean Part A? Is Part B to be submitted at a different time? Background -Page 5, last sentence which is continued on page 6: This standard does not recognize the various “versions” of companies in the industry. The standard is made applicable to a long list of registered entity types. In many cases, many of these entities are wrapped into one company. A company may be responsible for “everything” in a geographic area. It may be almost every registered entity type with no other registered entities within its geographic area. There should be no conflicts or need for coordination with others for this company. Everything would be coordinated internally within that one company before being reported to NERC and no one else would be reporting to NERC. However, sometimes one company is only a LSE. When an LSE-only is having a LSE impact event, the LSE should report to some higher operating entity like its BA and should not report to NERC. Reporting should be done in a hierarchical manner within appropriate operating entities and then reported to NERC at the RC (or BA) level or as agreed among entities in any coordinated impact event reporting plans. The RC, BA, TOP, and LSE should not all be held accountable for reporting the same event. This standard does not deal exclusively with after-the-fact reporting. Some events deal with the condition of the system (risk of possible future events) or condition of an entity’s ability to operate (supplying fuel, covering load, etc.) or with a threat to the BES. -Page 6, Summary of Concepts: A single form may have been an objective but it is obviously not a concept being implemented by the standard. There are two forms. -Page 6, Law Enforcement Reporting: The object of the standard may be to prevent or reduce the risk of Cascading. Reporting system situations to appropriate operating entities who can take some mitigating action (e.g., a LSE reporting to its BA

or a BA reporting to its RC) and reporting threats to law enforcement officials could prevent or reduce the risk of Cascading but reporting to NERC is unlikely to a do that. Reporting of most of the listed events to NERC does not meet the objective of this standard and should be removed from this standard. Such events should be reported to NERC through some other (than a Reliability Standard) requirement for reporting to NERC so that NERC can accomplish its mission of analyzing events. Analyzing events may lead to an understanding that could reduce the future risk of Cascading but not any impending risks. -Page 6, Stakeholders: What is “Homeland Security – State?” We know what the Department of Homeland Security and the State Department are but this term is not clear. -Page 6, “State Regulators”, “Local Law Enforcement”, and State Law Enforcement”: These are not proper nouns/names and are not defined in the NERC Glossary. They should not be capitalized. -Pages 7 & 8, Law enforcement: Is each entity required to determine procedures for reporting to law enforcement and work it out with the state law enforcement agency? Do the state law enforcement agencies know this? Or is there a pre-determine procedure that is already worked out with the state law enforcement agency that entities are to follow?
Individual
Max Emrick
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power
1 - Transmission Owners, 3 - Load-serving Entities, 4 - Transmission-dependent Utilities, 5 - Electric Generators, 6 - Electicity Brokers, Aggregators
No
"To improve industry awareness and the reliability fo the Bulk Electric System by requiring the reporting of Impact Events and their causes, if known by the Responsible Entities" The revised purpose statement includes the phrase, “if known”. This seems like a huge loophole. They should change it to “when discovered” or “when notified”.
Yes
Yes
Yes
Yes
Yes
However, there needs to be some clarity on which government agencies (if not the FBI) are responsible for reporting these type of events.
No
There are generally several events during the year. If the process is well documented, a drill or exercise is excessive. It should be sufficient to say “provide training”.
Yes
Yes
Yes
No
The one hour reporting timeline is unrealistic for this event. In general it looks like other events requiring the 1 hour reporting timeline are for event that are ‘initiated’ by the system operator. (ie load shedding, public load reduction, EEP…). Loss of BES equipment is in general 24 hour reporting timeline. It should be, “as soon as possible but within 24 hours".
No
M3 -The testing of the Plan by drill or mock impact event is unnecessary and burdensome.
No
Yes
No
Why shorten the normal process?
No
The implementation Plan was to move up the timeline and we do not see why this needs to be pushed forward on a shortened timeline. It should remain at the one year implementation schedule especially if annual exercises are not

removed from the standard requirements as this take some time to prepare.
We like the option to use the OE_417 as the reporting form for these events.
Group
Compliance & Responsiblity Organization
Silvia Parada Mitchell
No
See comments set forth in number 2.
No
NextEra Energy Inc. (NextEra) appreciates the drafting team providing valuable ideas and a framework on how to improve and consolidate CIP-001 and EOP-004. However, NextEra also believes that the currently drafted EOP-004-2 needs to be revised and enhanced to more clearly explain the Responsible Entities' duties, the definition of sabotage and address FERC directives and concerns. For example, NextEra is not in favor using the term "Impact Event" which seems to add considerable confusion of what is or is not sabotage. In Order No. 693, FERC stated its interest in NERC revising CIP-001 to better define sabotage and requiring notification to the certain appropriate federal authorities, such as the Department of Homeland Security. FERC Order 693 at PP 461, 462, 467, 468, 471. NextEra has provided an approach that accomplishes FERC's objectives and remains within the framework of the drafting team, but also focuses the process of determining and reporting only those sabotage acts that could impact other BES systems. Today, there are too many events that are being reported as sabotage to all parties in the Interconnection, when in reality these acts have no material affect or potential impact to other BES systems other than the one that experienced it. For example, while the drafting team notes the issue of copper theft is a localized act, there are other localized acts of sabotage that are committed by an individual, and these acts pose little, if any, impact or threat to other BES systems other than the one experiencing the sabotage event. Reporting sabotage that has no need to sent of everyone does not necessary add to the security or reliability of the BES. Related, there is a need to clarify some of the current industry confusion on who should (and has the capabilities to) be reporting to a boarder audience of entities. Hence, NextEra approach provides a clear definition of sabotage, as well as the process for determining and reporting sabotage. NextEra further believes that some of the requirements can be consolidated and more clearly stated, and NextEra has attempted to do that in the approach presented below. Lastly, NextEra comments on Attachment 1 are submitted in response to question 17. NextEra Approach Delete definition of Impact Event and its use in the requirements and in Attachment 1 Delete 13, 14, 15 and 19 in Attachment 1 Delete and replace R1 through R5 with the following: New Definition Attempted or Actual Sabotage: an intentional act that attempts to or does destroy or damage BES equipment or a Critical Cyber Asset for the purpose of disrupting the operations of BES equipment, Critical Cyber Asset or the BES, and has a potential to materially threaten or impact the reliability of one or more BES systems (i.e., is one act in a larger conspiracy to threaten the reliability of the Interconnection or other BES systems). R1. Each Responsible Entity shall document and implement a procedure (either individually or jointly with other Responsible Entities) to accomplish the reporting requirements, including the time frames, assigned to the Responsible Entity as set forth in Attachment 1 items 1 through 12, 16, 17 and 18 for reporting from the Responsible Entity to its Regional Entity and NERC, using the form in Attachment 2 or the DOE OE-417 reporting form. R2. Each Responsible Entity shall document and implement a procedure (either individually or jointly with other Responsible Entities) to report to its internal personnel with a need to know and its Reliability Coordinator an act of Attempted or Actual Sabotage, using the form in Attachment 2 or the DOE OE-417 reporting form, within one hour after a determination has been made that an act Attempted or Actual Sabotage has occurred. To make a determination that an act of Attempted or Actual Sabotage has occurred, the Responsible Entity shall document and implement a procedure that requires it, as soon as practicable after the discovering an act appearing to be Attempted or Actual Sabotage, to engage local law enforcement or the Federal Bureau of Investigation or Royal Canadian Mounted Police, as deemed appropriate, to assist the Registered Entity make such a determination. Upon receiving a report of Attempted or Actual Sabotage from a Responsible Entity, the Reliability Coordinator shall within one hour forward the report to other impacted Reliability Coordinators, Responsible Entities, Regional Entities, NERC, Department of Homeland Security, and the Federal Bureau of Investigation or the Royal Canadian Mounted Police. R3. Each Responsible Entity shall review (and conduct a test for sabotage only) of its documented procedure required in R1 and R2 with no more than 15 calendar months between tests for sabotage reporting. If, based on the review or test, the Responsible Entity determines there is a need to update its documented procedure, it shall update the procedures within 90 calendar days of the review or test.
No
See comments set forth in number 2.
Yes
No
See comments to 2. Also, although NextEra agrees that a documented procedure is appropriate, NextEra does not favor the current approach of pre-defined layers of processes and documentation that seem to overly complicate, and, possibly contradict, already established internal methods by which a company implements policies, procedures and processes. Thus, NextEra's options suggest using a more generic approach that allows entities more flexibility to establish documents and processes, and demonstrate compliance. Such a generic approach was used in NextEra's

proposed options set forth in response to number 2.
No
See comments set forth in number 2.
No
See comments set forth in number 2. Also, while NextEra understands the need to have a testing requirement for sabotage (Order 693 at P 446), it does not find it necessary to have a testing requirement for the other events. At this time in the process, additional requirements for the sake of having a requirement are likely to detract from reliability. Thus, NextEra requests that the testing requirement be limited to sabotage related events.
No
See comments set forth in number 2
Yes
No
See comments set forth in number 2
No
See comments set forth in number 2.
No
See comments set forth in number 2.
No
See comments set forth in number 2.
Yes
Nuclear power plants (a need for a revised approach) With respect to sabotage, damage or destruction of BES equipment, damage or destruction of a Critical Asset, damage or destruction of a Critical Cyber Asset, forced intrusion, etc., nuclear plants already have a responsibility to report the events to the FBI and the Nuclear Regulatory Commission (NRC). Performing another report to NERC, with potentially different requirements, within 60 minutes of an event does not seem necessary or practical. It would also be difficult, during an event, to report to external organizations, including but not limited to the Responsible Entities' Reliability Coordinator, NERC, Responsible Entities' Regional Entity, Law Enforcement, and Governmental or Provincial Agencies when operations personnel are pre-occupied with an abnormal or emergency situation. Further, nuclear plants already have an obligation to report the loss of off site power to NRC. Similarly, now that cyber assets will be regulated by the NRC, these reporting requirements should not be applicable to a nuclear power plant. Thus, there is a need to exempt nuclear power plants from these requirements or provide more flexibility to such plants, given its pre-existing NRC reporting requirements. Attachment 1. There is no explanation for why a report must be submitted within one hour of a event. As stated with respect to nuclear, an entity should not be prioritizing between stabilizing the system and reporting. One approach that would help balance conflicting priorities is to start the time frame after "all is clear." Another approach could involve the use of target times, with an allowance for exceptions during emergencies or situations in which it is impracticable. Another alternative is to have two times: an earlier "target reporting time" and second later "mandatory reporting time." Further, the current wording suggests that a generator owner or generator operator will be able to determine the impact or potential impact on the BES. This is not realistic, given that impacts to the BES are generally only understood at a transmission operator or reliability coordinator level. Thus, the concept of relying on generators to determine impacts on the BES needs to be eliminated. Also, as written, for a generator, Attachment 1 appears to require a report when a lighting arrestor fails at a Critical Asset. NextEra cannot see any justification for reporting such an event, and this is another reason why Attachment 1 needs more review and revision prior to the next draft of EOP-004-2. This one reason why NextEra has suggested a materiality test for reporting in a definition of Attempted or Actual Sabotage.
Individual
Rex Roehl
Indeck Energy Services
5 - Electric Generators
No
The reporting of events does not improve the reliability of the BES. If someone takes action based on the reporting, there might be an improvement. Because many of these events are not preventable, such as sabotage or weather, reporting them won't improve reliability. The original Purpose was satisfactory.
No
It's not a definition. It needs some quantification, such as, a Reportable Disturbance (NERC glossary), a reportable event under DOE OE-417, sabotage or bomb threat. Defining it as having or potentially having an impact is no definition. What is an impact? It needs to be quantified or auditors will have license to define it any way that they want. It shouldn't be a NERC Glossary definition if its only use is in EOP-004. Within EOP-004, it can be defined as anything

in Attachment 1.
No
The SDT hasn't defined sabotage. Attachment 1 does not do justice to the concept of sabotage. Sabotage should be defined as any intentional damage to BES facilities the causes a Reportable Disturbance, reportable event under DOE OE-417 or involves a bomb or bomb threat.
No
Voltage Deviations should not be reportable by GOP. That's why we have TOP's. Damage or destruction of BES equipment should be reportable only if it causes or could cause a Reportable Disturbance, reportable DOE OE-417 event or sabotage (as defined above). Otherwise, an auditor could require reporting of a relay failure caused by human error even though the relay was in test mode and no BES impact was experienced. This category could be dropped in favor of the next one, damage to Critical Asset. Fuel Supply Emergency needs a definition. For natural gas, various conditions could be referred to as emergencies, but unless they actually affect generation, they should not need to be reported. Fuel Supply Emergencies that cause a Reportable Disturbance or reportable DOE OE-417 event should be reported. It is unclear why Forced Intrusion should be reportable under EOP-004. If it causes a problem, it will be reportable as another category and is one more unpreventable event. Forced Intrusion isn't, in many cases, as the exceptions try to define, an impact event at all, but could be a cause, which would be reported as the cause of an impact event. Risk to BES Equipment is not well defined. It should be expanded to Risk to BES Equipment from a non-environmental physical threat within a reasonable distance of the Equipment. A train derailment on the line past the plant would likely be known, whereas one that was 1/2 mile or more away with flammable materials might not be known about unless a public warning was made.
Yes
No
The terms are not important and many plans or procedures already exist and restructuring them to match the terms is wasteful. R1 is too prescriptive. R1 should state that a written document should show how the entity will comply with EOP-004. R1.2 is superfluous and should be deleted. The data must be gathered and the process will vary with the event. Trying to define the multitude of possibilities for the collection process is not productive and leaves open the possibility of missing something for an auditor to nit pick. R1.3 should just be a written communications plan/process/procedure for external notifications. R1.4 is redundant because it can't be changed within 90 days until the content has already been changed. R1.4 should be deleted. The Violation Risk Factor should be Low, if any, because this is historical reporting, with little or no reliability consequence.
No
R2 is direct and to the point. The Violation Risk Factor should be Low, if any, because this is historical reporting, with little or no reliability consequence.
No
For smaller entities, for which few of the Attachment 1 events apply (eg a 75 MW wind farm), a drill is overkill. Reviewing the procedure during training should be sufficient. The solution is to require a drill for any entity for which any of the Attachment 1 events would cause a Reportable Disturbance or reportable DOE OE-417 event and training review for any other entities. The Violation Risk Factor should be Low, if any, because this is historical reporting, with little or no reliability consequence.
R4 is redundant with R3 and should be deleted. The Violation Risk Factor should be Low, if any, because this is historical reporting, with little or no reliability consequence.
No
The Violation Risk Factor should be Low, if any, because this is historical reporting, with little or no reliability consequence.
No
Comments were included in previous comments.
No
M1 is OK. M2 should be about implementation, not about any particular events--M5 is about events. Implementation would include distribution and training. M3 should be modified to reflect a training review by entities that cannot cause a Reportable Disturbance or reportable DOE OE-417 event and for the others documentation of an actual event (which is not included in the present M3) or a drill or mock event. M4 is OK. M5 should only include the reports submitted and the date of submission. Further evidence of the event is redundant.
No
If there are any, they should all be Low because this is reporting of historical events. There is no direct effect on BES reliability. Some effect could occur if someone reacts to the reports, but many are concerning unpreventable events.
No
There should be only Lower VSL's. This is reporting of historical events and there is no direct effect on BES reliability. How does missing 3 parts of R1 compare to tripping a 4,000 MW generating station because vegetation was not properly managed? Just because there are 4 levels, doesn't mean that all Standards need to use them all. If you step

back, and think about causes of cascading outages, reporting events 1 hour or 24 hours later has no significance. There is no direct preventative causation either.
No
These requirements have no time horizon. There about history and not about the future.
Yes
This revision seriously missed the mark.
Group
SERC OC Standards Review Group
Gerald Beckerle
Yes
No
We believe the definition is too broad even considering Attachment 1, footnote1, which, for example, uses the term significantly and other ambiguous terms. Consideration should be given to limiting the definition to unplanned events.
Yes
No
We agree that all of the entities listed should be responsible for reporting an event, provided they own BES assets, but guidance should be given for which entity in Attachment 1 actually files the report to avoid duplication for a single event.
No
We agree that the ERO should not have requirements applicable to them, but disagree with changing or revising the Rules of Procedure (ROP) giving this reporting responsibility solely to NERC. This responsibility may be performed by NERC but other learning organizations should also be considered for performing this responsibility. In addition, the proposed wording of the revision to the ROP appears to place the responsibility of notifying the appropriate law enforcement with NERC rather than with the local responsible entity.
No
This is a reporting requirement and should not be confused with Operating Plans that have specific operating actions and goals. Each entity should prepare its own event reporting guideline that address impact events, identification, information gathering, and communication without specifying a specific format such as Operating Plans, Operating Process and Operating Procedures.
No
We agree with the concept, but disagree with the use of the term “Operating Plan” as a defined term in line with our comments in question 6 above.
No
Annual testing of an “after-the-fact” reporting procedure does not add to the reliability of the BES!
Yes
We agree with the concept, but disagree with the use of the term “Operating Plan” as a defined term in line with our comments in question 6 above.
Yes
We agree with the concept, but disagree with the use of the term “Operating Plan” as a defined term in line with our comments in question 6 above.
No
While we agree with the changes made, we do not believe the goal of eliminating duplicate reporting has been accomplished. In addition, the threshold for transmission loss does not adequately translate to previous “loss of major system components” which had a threshold of “significantly affects the integrity of interconnected system operations”.
No
The measures should be revised to match the general nature of the comments we have made on each requirement.
No
How can an after-the-fact report require a VRF greater than low?
No
The VSLs should reflect the comments on the requirements above.
No
R2 and R5 should be in the Operations Assessment time horizon.
Yes

In Attachment 1, the reporting timeline should be no less than the end of the next business day for after-the-fact reporting of events. If reporting in a time frame less than this is required for reliability, the groups or organizations receiving the reports should be included in the functional model. The emphasis should be on giving the operators the time to respond to events and not to reporting requirements. “The comments expressed herein represent a consensus of the views of the above named members of the SERC OC Standards Review group only and should not be construed as the position of SERC Reliability Corporation, its board or its officers.”
Individual
Patricia Robertson
BC Hydro
1 - Transmission Owners, 2 - RTOs and ISOs, 3 - Load-serving Entities, 5 - Electric Generators
Yes
Yes
For the change from 24hr to 1hr reporting for events, 1 hour goes extremely quickly in these types of events and it will be difficult to report anything meaningful. As the RC is kept informed during the event why is the report required within 1hr?
Individual
Tony Kroskey
Brazos Electric Power Cooperative
1 - Transmission Owners
No
Instead of Impact Event could simply call it Event Information Reporting.
No
Yes
No
Inclusion of LSE and DP is questionable.
No
Yes
Yes
Yes
Yes

No
Question applicability to DP.
No
M2 and M5 appear to duplicate each other.
No
A one year implementation is needed to develop and implement formal documents to meet requirements.

Stakeholders in the Reporting Process

- Industry
  - NERC (ERO)
  - FERC
  - DOE
  - DHS – Federal
  - Homeland Security- State
  - State Regulators
  - Local Law Enforcement
  - State Law Enforcement
  - FBI
  - Royal Canadian Mounted Police (RCMP) (addition)
  - Provincial Law Enforcement (addition)
  - Municipal Law Enforcement (addition)

Coordination of Local and Provincial Law Enforcement Agencies with the RCMP
A similar law enforcement coordination hierarchy exists in Canada. Local and Provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. The Provincial law enforcement agency has a reporting relationship with the Royal Canadian Mounted Police (RCMP).

The above should read as follows;

Coordination of Municipal and Provincial Law Enforcement Agencies with the RCMP
A similar law enforcement coordination hierarchy exists in Canada. Municipal and provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. Municipal and provincial law enforcement agencies have a reporting relationship with the Royal Canadian Mounted Police (RCMP).

A Reporting Process Solution – EOP-004
A proposal discussed with FBI, FERC Staff, NERC Standards Project Coordinator and SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Impact Event EOP-004-2). Essentially, reporting an Impact Event to law enforcement agencies will only require the industry to notify the state or provincial level law enforcement agency. The state or provincial level law enforcement agency will coordinate with local law enforcement to investigate. If the state or provincial level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial level law enforcement agency will notify and coordinate with the FBI or the RCMP.

The above should read as follows; (red reflects suggested changes)

A Reporting Process Solution – EOP-004
A proposal discussed with FBI, FERC Staff, NERC Standards Project Coordinator and SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Impact Event EOP-004-2). Essentially, reporting an Impact Event to law enforcement agencies will only require the industry to notify the state or provincial or local or municipal law enforcement agency. The state or provincial or local or municipal law enforcement agency will coordinate with law enforcement of jurisdiction to investigate. If the state or provincial or local or municipal law enforcement agency decides federal agency law enforcement should respond and investigate, the state or provincial or local or municipal law enforcement agency will notify and coordinate with the FBI or the RCMP.

Compliance

Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.

The above needs to reflect Canadian compliance authorities as they do not include FERC therefore I suggest the following (red reflects suggested changes/additions)

- Regional Entity; and or applicable Canadian provincial authority; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity), or applicable Canadian Provincial authority, responsible for compliance enforcement.

Consideration of Comments on Disturbance & Sabotage Reporting — Project 2009-01

The Disturbance & Sabotage Reporting Drafting Team (DSR SDT) thanks all commenters who submitted comments on the Second Posting of EOP-004-2, Impact Event Reporting (Project 2009-01).
This standard was posted for a 30-day public comment period from March 9, 2011 through April 8, 2011. The stakeholders were asked to provide feedback on the standard through a special Electronic Comment Form. There were 60 sets of comments, including comments from 188 different people from approximately 132 companies representing 10 of the 10 Industry Segments as shown in the table on the following pages.

In this report, comments have been organized by question to make it easier to see where there is consensus. Comments may be reviewed in their original format on the project page:

http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

Summary Consideration: The DSR SDT received many comments regarding the proposed definition of "Impact Event," the requirements, and event reporting in Attachment 1. The main stakeholder concerns were addressed as follows:

- Many stakeholders disagreed with the need for the definition of "Impact Event" and felt that the definition was ambiguous and created confusion. The DSR SDT agrees and has deleted the proposed definition from the standard. The list of events in Attachment 1 is all-inclusive and no further attempts to define "Impact Event" are necessary.
- Many stakeholders raised concerns with the 1 hour reporting requirement for certain types of events. The commenters believed that the restoration of service or the return to a stable bulk power system state may be jeopardized by having to report certain events within one hour. The DSR SDT agreed and revised the reporting time to 24 hours for most events, with the exception of damage or destruction of BES equipment, forced intrusion or cyber related incidents.
- Many stakeholders suggested that the reporting of events after the fact only justified a VRF of "lower" for each requirement. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF, as this requirement deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all "lower" with the exception of Requirement R2 which is a requirement to analyze

[1] The appeals process is in the Standard Processes Manual:.

events. This standard relates only to reporting events. Analysis of reported events is addressed through the NERC Events Analysis Program. Proposed changes to the Electric Reliability Organization Events Analysis Process Field Trial documents that clarify the role of the Events Analysis program in analyzing reported events will be posted for stakeholder comment separately.

- The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events to the appropriate entities in accordance with the Operating Plan based on Attachment 1. Requirement R3 makes sure that an entity can communicate information about events. Some of these events are dealing with potential sabotage events, and part of the reason to communicate these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 are consistent with the existing approved VRFs for both EOP-004 and CIP-001.
- Several commenters wanted more clarity regarding which entities report and to whom they report. Many stakeholders were confused regarding law enforcement notifications and questioned whether certain types of events (IROL, Public Appeal, etc.) needed to be reported to law enforcement. The background section of the standard provides guidance with respect to reporting events to law enforcement. For clarity, the DSR SDT has added the following sentence to the first paragraph under the heading "Law Enforcement Reporting": "These are the types of events that should be reported to law enforcement." The entire paragraph is:
    - "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES."
- Some commenters also questioned whether or not the existing applicability would result in multiple reports being submitted by different entities for the same event. NERC staff has indicated that this is acceptable and that having multiple types of entities report the same event may provide different types of information about the event.

Commenters also had concerns about the applicability of the standard to Load Serving Entities who may not own physical assets as well as to the ERO and Regional Entity. The DSR SDT agrees that the Distribution Provider owns the assets per the Functional Model; however the LSE is an applicable entity under CIP-002. Events relating the CIP-002 assets are to be reported by the LSE. These are envisioned to be cyber assets. The DSR SDT also include the ERO or the RE as applicable entities based on the applicability of CIP-002

Some commenters identified issues with the footnotes in Attachment 1. These were revised as suggested. There were a few instances where the word "sabotage" remained in the standard or the flowchart. The DSR SDT has removed all instance of "sabotage" and replaced them with "event," and revised the flowchart to remove references to sabotage.

Several commenters were concerned that the DSR SDT and the NERC Events Analysis Working Group (EAWG) may not be in alignment. The DSR SDT is working in close coordination with the EAWG and will continue to develop the standard and will make the EAWG aware of the DSR SDT's efforts.

The issue of the FERC directives relating to this project was broached by several commenters. The DSR SDT envisions EOP-004-2 to be a continent-wide reporting standard. Any follow up investigation or analysis falls under the purview of the NERC Events Analysis Program under the NERC Rules of Procedure. This process is being revised by the EAWG. Discussions with FERC staff indicate that the current efforts of the DSR SDT and the EAWG are sufficient to address the intent of the directive.

After the drafting team completed its consideration of stakeholder comments, the standards and implementation plan were submitted for quality review. Based on feedback from the quality review, the drafting team has made two significant revisions to the standard. The first revision is to add a requirement for implementation of the Operating Plan listed in Requirement R1. There was only a requirement to report events, but no requirement specifically calling for updates to the Operating Plan or the annual review. This was accomplished by having two requirements. The first is Requirement R2 which specifies that an entity must implement the Operating Plan per Requirement R1, Parts 1.1, 1.2, 1.4 and 1.5:

> R2. Each Responsible Entity shall implement the parts of its Operating Plan that meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts 1.4 and 1.5 as specified.

The second Requirement is R3 which addresses Part 1.3:

> R3. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.

The second revision based on the quality review pertains to Requirement R4. The quality review suggested revising the requirement to more closely match the language in the Rationale box that the drafting team developed. This would provide better guidance for responsible entities as well as provide more clear direction to auditors. The revised requirement is:

> R4. Each Responsible Entity shall verify (through actual implementation for an event, or through a drill or exercise) the communication process in its Operating Plan, created pursuant to Requirement 1, Part 1.3, at least annually (once per calendar year), with no more than 15 calendar months between verification or actual implementation.

Index to Questions, Comments, and Responses

1. Do you agree with the revised Purpose Statement of EOP-004-2, Impact Event Reporting? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. ….....15
2. Do you agree with the proposed definition of Impact Event? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 23
3. Do you agree that the DSR SDT has provided and equally efficient and effective solution to the FERC Order 693 directive to "further define sabotage"? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 38
4. Do you agree with the proposed applicability of EOP-004-2 shown in Section 4 and Attachment 1 of the standard? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. ….. 46
5. Stakeholders suggested removing original Requirements 1, 7 and 8 from the standard and addressing the reliability concepts in the NERC Rules of Procedure. Do you agree with the removal of original requirements 1, 7 and 8 (which were assigned to the ERO) and the proposed language for the Rules of Procedure (Paragraph 812)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 64
6. Do you agree with the proposed revisions to Requirement 2 (now R1) including the use of defined terms Operating Plan, Operating Process and Operating Procedure? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 70
7. Do you agree with the proposed revisions to Requirement 3 (now R2)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 87
8. Do you agree with the proposed revisions to Requirement 4 (now R3)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 98
9. Do you agree with the proposed revisions to Requirement 5 (now R4)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 113
10. Do you agree with the proposed revisions to Requirement 6 (now R5) and the use of either Attachment 2 or the DOE-OE-417 form for reporting? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 123
11. Do you agree with the proposed revisions to Attachment 1? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 134
12. Do you agree with the proposed measures for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 159
13. Do you agree with the proposed Violation Risk Factors for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. ….**Error! Bookmark n**
14. Do you agree with the proposed Violation Severity Levels for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. ….**Error! Bookmark n**
15. Do you agree with the proposed Time Horizons for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 189
16. Do you agree with the proposed Implementation Plan for EOP-004-2? If not, please explain why not and if possible, provide an alternative that would be acceptable to you. …. 195
17. If you have any other comments you have not already provided in response to the questions above, please provide them here. …. 201

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	David Revill	Georgia Transmission Corporation & Oglethorpe Power Corporation			X	X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Miller	Georgia Transmission Corporation	SERC	1
2.	Greg Davis	Georgia Transmission Corporation	SERC	1
3.	Jason Snodgrass	Georgia Transmission Corporation	SERC	1
4.	Scott McGough	Oglethorpe Power Corporation	SERC	5

2.	Group	Guy Zito	Northeast Power Coordinating Council					X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Gregory Campoli	New York Independent System Operator	NPCC	2
3.	Kurtis Chong	Independent Electricity System Operator	NPCC	2
4.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
5.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
7.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1

Group/Individual		Commenter	Organization		Registered Ballot Body Segment									
					1	2	3	4	5	6	7	8	9	10
8.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5										
9.	Brian L. Gooder	Ontario Power Generation Incorporated	NPCC	5										
10.	Kathleen Goodman	ISO - New England	NPCC	2										
11.	David Kiguel	Hydro One Networks Inc.	NPCC	1										
12.	Michael R. Lombardi	Northeast Utilities	NPCC	1										
13.	Randy MacDonald	New Brunswick Power Transmission	NPCC	1										
14.	Bruce Metruck	New York Power Authority	NPCC	6										
15.	Chantel Haswell	FPL Group, Inc.	NPCC	5										
16.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10										
17.	Robert Pellegrini	The United Illuminating Company	NPCC	1										
18.	Saurabh Saksena	National Grid	NPCC	1										
19.	Michael Schiavone	National Grid	NPCC	1										
20.	Wayne Sipperly	New York Power Authority	NPCC	5										
21.	Donald Weaver	New Brunswick System Operator	NPCC	1										
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1										
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3										
3.	Group	Denise Koehn	Bonneville Power Administration				X	X	X	X				
	Additional Member	Additional Organization	Region	Segment Selection										
1.	Jim Burns	BPA, Transmission, Technical Operations	WECC	1										
4.	Group	Carol Gerou	Midwest Reliability Organization		X		X		X	X				
	Additional Member	Additional Organization	Region	Segment Selection										
1.	Mahmood Safi	Omaha Public Utility District	MRO	1, 3, 5, 6										
2.	Chuck Lawrence	American Transmission Company	MRO	1										
3.	Tom Webb	Wisconsin Public Service Corporation	MRO	3, 4, 5, 6										
4.	Jodi Jenson	Western Area Power Administration	MRO	1, 6										
5.	Ken Goldsmith	Alliant Energy	MRO	4										
6.	Alice Ireland	Xcel Energy	MRO	1, 3, 5, 6										
7.	Dave Rudolph	Basin Electric Power Cooperative	MRO	1, 3, 5, 6										

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
8. Eric Ruskamp	Lincoln Electric System	MRO 1, 3, 5, 6										
9. Joseph Knight	Great River Energy	MRO 1, 3, 5, 6										
10. Joe DePoorter	Madison Gas & Electric	MRO 3, 4, 5, 6										
11. Scott Nickels	Rochester Public Utilties	MRO 4										
12. Terry Harbour	MidAmerican Energy Company	MRO 1, 3, 5, 6										
13. Richard Burt	Minnkota Power Cooperative, Inc.	MRO 1, 3, 5, 6										
5. Group	Steve Rueckert	Western Electricity Coordinating Council					X					
Additional Member	Additional Organization	Region Segment Selection										
1. Don Pape	WECC	WECC 10										
2. Phil O'Donnell	WECC	WECC 10										
6. Group	Annette Bannon	PPL Supply	X		X		X	X				
Additional Member	Additional Organization	Region Segment Selection										
1.	Mark Heimbach	PPL Martins Creek, LLC RFC 5, 6										
7. Group	Steve Alexanderson	Pacific Northwest Small Public Power Utility Comment Group					X				X	
Additional Member	Additional Organization	Region Segment Selection										
1. Dave Proebstel	Clallam County PUD No.1	WECC 3										
2. Russell A. Noble	Cowlitz County PUD No. 1	WECC 3, 4, 5										
3. Ronald Sporseen	Blachly-Lane Electric Cooperative	WECC 3										
4. Ronald Sporseen	Central Electric Cooperative	WECC 3										
5. Ronald Sporseen	Clearwater Power Company	WECC 3										
6. Ronald Sporseen	Douglas Electric Cooperative	WECC 3										
7. Ronald Sporseen	Fall River Rural Electric Cooperative	WECC 3										
8. Ronald Sporseen	Northern Lights	WECC 3										
9. Ronald Sporseen	Lane Electric Cooperative	WECC 3										
10. Ronald Sporseen	Lincoln Electric Cooperative	WECC 3										
11. Ronald Sporseen	Raft River Rural Electric Cooperative	WECC 3										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
12.	Ronald Sporseen	Lost River Electric Cooperative	WECC 3										
13.	Ronald Sporseen	Salmon River Electric Cooperative	WECC 3										
14.	Ronald Sporseen	Umatilla Electric Cooperative	WECC 3										
15.	Ronald Sporseen	Coos-Curry Electric Cooperative	WECC 3										
16.	Ronald Sporseen	West Oregon Electric Cooperative	WECC 3										
17.	Ronald Sporseen	Pacific Northwest Generating Cooperative	WECC 3, 4, 8										
18.	Ronald Sporseen	Power Resources Cooperative	WECC 5										
19.	Ronald Sporseen	Consumers Power	WECC 1, 3										
20.	Steven J. Grega	Public Utility District #1 of Lewis County	WECC 5										
8.	Group	Patricia Hervochon	PSEG Companies	X				X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Jeffrey Mueller	PSE&G		3
2.	Kenneth Brown	PSE&G		1
3.	Peter Dolan	PSEG ER&T		6
4.	Eric Schmidt	PSEG ER&T		6
5.	Clint Bogan	PSEG Fossil		5
6.	Dominic Grasso	PSEG Fossil		5
7.	Kenneth Petroff	PSEG Nuclear		5
8.	Patricia Hervochon	PSEG NERC Compliance		NA

9.	Group	Louis Slade	Dominion			X	X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Lou Roeder	Electric Transmission	SERC	1, 3
2.	Mike Garton	Electric Market Policy	NPCC	5, 6
3.	Connie Lowe	Electric Market Policy	RFC	5, 6
4.	Jack Kerr	Electric Transmission	SERC	3, 1
5.	Len Sandberg	Electric Transmission	SERC	3, 1

10.	Group	David Thorne	Pepco Holdings Inc and Affiliates		X								

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1.	Mark Godfrey		RFC	1, 3									
11.	Group	Robert Rhodes	SPP Standards Review Group	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Allen	City Utilities of Springfield, MO	SPP	1, 4
2.	George Allan	Sunflower Electric Power Corporation	SPP	1
3.	Michelle Corley	CLECO	SPP	1, 3, 5, 6
4.	Robert Cox	Lea County Electric Cooperative	SPP	1, 3
5.	Kevin Emery	Carthage Water and Electric	SPP	3
6.	Denney Fales	Kansas City Power & Light	SPP	1, 3, 5, 6
7.	Louis Guidry	CLECO	SPP	1, 3, 5, 6
8.	Jonathan Hayes	SPP	SPP	2
9.	Philip Huff	Arkansas Electric Cooperative Corporation	SPP	3, 4, 5, 6
10.	Gregory McAuley	Oklamoma Gas & Electric	SPP	1, 3, 5
11.	Terri Pyle	Oklahoma Municipal Power Authority	SPP	4
12.	Sean Simpson	Board of Public Utilities, City of McPherson, KS	SPP	1, 3, 5
13.	Tay Sing	Oklahoma Municipal Power Authority	SPP	4
14.	Chad Wasinger	Sunflower Electric Power Corporation	SPP	1
15.	Mark Wurm	Board of Public Utilities, City of McPherson, KS	SPP	1, 3, 5
16.	Ron Gunderson	Nebraska Public Power District	MRO	1, 3, 5
17.	Bruce Schutte	Nebraska Public Power District	MRO	1, 3, 5
18.	Jeff Elting	Nebraska Public Power District	MRO	1, 3, 5

12.	Group	Marie Knox	Midwest ISO Standards Collaborators		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Bob Thomas	Illinois Municipal Electric Agency	RFC	4
2.	Jim Cyrulewski	JDRJC Associates, LLC	RFC	8
3.	Terry Harbour	MidAmerican	MRO	1
4.	Joe O'Brien	NIPSCO	RFC	6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
5. Robert Thomasson		Big Rivers Electric Corp.	SERC 1, 3										
13.	Group	Sam Ciccone	FirstEnergy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hohlbaugh	FE	RFC	1, 3, 4, 5, 6
2.	Bill Duge	FE	RFC	5
3.	John Reed	FE	RFC	1
4.	Jim Eckels	FE	RFC	1
5.	Kevin Querry	FE	RFC	5
6.	Ken Dresner	FE	RFC	5

14.	Group	Gerald Beckerle	SERC OC Standards Review Group					X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	David Trego	Fayetteville PWC	SERC	1, 3, 4, 9
2.	Melinda Montgomery	Entergy	SERC	1, 3
3.	Andy Burch	EEI	SERC	1, 5
4.	Eugene Warnecke	Ameren	SERC	1, 3
5.	Chuck Feagans	TVA	SERC	1, 3, 5, 9
6.	Larry Rodriquez	Entegra Power	SERC	5, 6
7.	Gary Hutson	SMEPA	SERC	1, 3, 5, 9
8.	Jennifer Weber	TVA	SERC	1, 3, 5, 9
9.	Doug White	NCEMC	SERC	1, 3, 5, 9
10.	Shaun Anders	CWLP	SERC	1, 3, 5, 9
11.	Jake Miller	Dynegy	SERC	5, 6
12.	Reggie Wallace	Fayette PWC	SERC	1, 3, 4, 9
13.	Dan Roethemeyer	Dynegy	SERC	5, 6
14.	Alvis Lanton	SIPC	SERC	1, 3, 5, 9
15.	Marc Butts	Southern	SERC	1, 3, 5
16.	Robert Thomasson	BREC	SERC	1, 3, 5, 9
17.	Srinivas kappagantula	PJM	SERC	2

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
18.	Barry Hardy	OMU	SERC 1, 3, 5, 9										
19.	Rene' Free	Santee Cooper	SERC 1, 3, 5, 9										
20.	Greg Matejka	CWLP	SERC 1, 3, 5, 9										
21.	John Troha	SERC Reliability Corp.	SERC 10										
15.	Individual	Srinivas Kappagantula	PJM Interconnection LLC	X									
16.	Individual	Cindy Martin	Southern Company				X						
17.	Individual	Cynthia Oder	SRP	X									
18.	Individual	Howard Rulf	We Energies	X				X		X			
19.	Individual	Brent Ingebrigtson	LG&E and KU Energy LLC	X									
20.	Individual	Silvia Parada Mitchell	Compliance & Responsiblity Organization			X							
21.	Individual	John Bee	Exelon	X		X		X	X				
22.	Individual	Jennifer Wright	SDG&E			X							
23.	Individual	Alan Gale	City of Tallahassee (TAL)	X									
24.	Individual	Mace Hunter	Lakeland Electric					X					
25.	Individual	Nathaniel Larson	New Harquahala Generating Co.	X		X		X	X				
26.	Individual	Brian Pillittere	Tenaska					X					
27.	Individual	MIchael Johnson	APX Power Markets			X	X						

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
28.	Individual	Jonathan Appelbaum	United Illuminating Co	X		X	X	X	X				
29.	Individual	Kevin Koloini	American Municipal Power					X					
30.	Individual	Daniel Duff	Liberty Electric Power LLC	X	X	X		X					
31.	Individual	Philip Huff	Arkansas Electric Cooperative Corporation	X									
32.	Individual	Joe Petaski	Manitoba Hydro	X									
33.	Individual	Mike Albosta	Sweeny Cogeneration LP			X	X	X					
34.	Individual	Thad Ness	American Electric Power					X					
35.	Individual	Andres Lopez	USACE			X	X	X	X				
36.	Individual	Nathaniel Larson	New Harquahala Generating Co.	X		X		X	X				
37.	Individual	Eric Salsbury	Consumers Energy					X					
38.	Individual	Michael Falvo	Independent Electricity System Operator	X		X		X	X				
39.	Individual	Kirit Shah	Ameren					X				X	
40.	Individual	Kathleen Goodman	ISO New England, Inc	X				X					
41.	Individual	Deborah Schaneman	Platte River Power Authority			X	X	X					
42.	Individual	Phil Porter	Calpine Corp		X								
43.	Individual	Bill Keagle	BGE	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
44.	Individual	Kenneth A Goldsmith	Alliant Energy		X								
45.	Individual	John Brockhan	CenterPoint Energy	X		X		X	X				
46.	Individual	Martin Kaufman	ExxonMobil Research and Engineering					X					
47.	Individual	Brenda Truhe	PPL Electric Utilities	X									
48.	Individual	Tim Soles	Occidental Power Marketing				X						
49.	Individual	Eric Ruskamp	Lincoln Electric System	X									
50.	Individual	Linda Jacobson	Farmington Electric Utility System	X				X		X			
51.	Individual	Andrew Z Pusztai	American Transmission Company	X									
52.	Individual	Michelle D'Antuono	Ingleside Cogeneration LP			X							
53.	Individual	Greg Rowland	Duke Energy	X		X		X					
54.	Individual	Amir Hammad	Constellation Power Generation			X							
55.	Individual	Scott Barfield-McGinnis	Georgia System Operations Corporation	X									
56.	Individual	Max Emrick	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power					X					
57.	Individual	Rex Roehl	Indeck Energy Services	X		X		X	X				
58.	Individual	Patricia Robertson	BC Hydro					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
59.	Individual	Tony Kroskey	Brazos Electric Power Cooperative			X	X						
60.	Individual	Jim Eckelkamp	Progress Energy	X									

1. **Do you agree with the revised Purpose Statement of EOP-004-2, Impact Event Reporting? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.**

Summary Consideration: The majority of stakeholders agree with the purpose statement. Some commenters had concerns with the use of the words "if known" and "industry awareness" and statements on requiring information from an analysis in the report which may not be known at the time of the report. Comments on this being an "after the fact" report and not real-time reporting have been addressed by a significant revision to the change in reporting times reflected in Attachment 1.

A number of commenters offered suggestions on the use of terms "situational awareness" versus "industry awareness." The DSR SDT used "industry awareness" to address concerns about real-time reporting (which this standard does not cover) and to avoid confusion with the NERC Situational Awareness organization.

The purpose statement was slightly revised to remove the defined term "Impact Event" and replace with the phrase "events with the potential to impact reliability". No other revisions were made.

> "To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of events with the potential to impact reliability and their causes, if known, by the Responsible Entities."

Organization	Yes or No	Question 1 Comment
Exelon	No	Although Exelon agrees that the proposed revision to the purpose statement of EOP-004-2 is better than the original draft; the DSR SDT should consider aligning the definition with the existing OE-417 terms. "Impact Events" are not clearly defined as reportable criteria in the DOE forms and may create confusion. Suggest rewording the purpose statement to simply "Incident Reporting" to align with existing terminology in OE-417 and removing the addition of a new term. A Purpose Statement is defined as "The reliability outcome achieved through compliance with the requirements of the standard." Propose that the purpose should be, "To require a review, assessment and report of events that could have an adverse material impact on the Bulk Electric System."
Response: The DSR DT thanks you for your comment. Form OE-417 report is a DOE report that is not specifically related to BES reliability and is not applicable outside of the United States. The standard only requires reporting of events. Analysis occurs through the NERC Events Analysis Program.		
SDG&E	No	SDG&E does not agree with the revised Purpose Statement because it does not reflect the standard's purpose of identifying reporting requirements for impact events. SDG&E recommends the following revised Purpose Statement: "To identify the reporting requirements for events considered to have an impact on the reliability of the Bulk

Organization	Yes or No	Question 1 Comment
		Electric System and to allow an awareness of these Impact Events to be understood by the industry in recognizing potential enhancements that may be made to the reliability of the BES."
Response: The DSR SDT thanks you for your comment. The DSR SDT believes that the existing purpose statement addresses most of your suggested rewording. The last phrase "recognizing potential enhancements that may be made to the reliability of the BES" is not in the scope of the standard or this project.		
Dominion	No	It is not evident how Impact Event reporting will "improve industry awareness" as suggested in the Purpose Statement. The transfer of Requirement R8 (ERO quarterly report) to the Rules of Procedure (paragraph 812) invalidates that claim within the context of this standard. Suggest removing this phrase from the Purpose Statement.
Response: The DSR DT thanks you for your comment. The ERO will issue reports for industry awareness purposes under the Rules of Procedure. If entities do not report events to the ERO, then these reports will not be issued.		
SPP Standards Review Group	No	We would suggest changing the purpose to read "To improve industry awareness and effectiveness in addressing risk to the BES by requiring the reporting of Impact Events and their causes, if known, by the Responsible Entities."
Response: The DSR DT thanks you for your comment. The DSR SDT contends that the phrase "addressing risk to the BES" applies to the analysis of events which is not covered under the standard.		
United Illuminating Co	No	UI agrees with the idea but believes the statement can be improved to remove ambiguities. For example: "if known" can be modifying the word causes, or the word Impact events. To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of identified Impact Events and if known their causes, if known, by the Responsible Entities.
Response: The DSR SDT thanks you for your comment. The words "if known" are intended to modify the word 'causes.' The DSR SDT has revised the existing wording (from the clean version of the standard) to: *To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of events with the potential to impact reliability and their causes, if known, by the Responsible Entities.*		

Organization	Yes or No	Question 1 Comment
Arkansas Electric Cooperative Corporation	No	The purpose statement reads "To improve industry awareness of the BES." We suggest the purpose should state "To improve industry awareness and effectiveness in addressing risks to the BES." We feel the remaining purpose statement is unnecessary.
Response: The DSR SDT thanks you for your comment. The DSR SDT contends that the phrase "addressing risk to the BES" applies to the analysis of events which is not covered under the standard.		
Manitoba Hydro	No	Situational Awareness was replaced by the generic "Industry awareness." Justification for this was that Situational Awareness was a byproduct of a successful event reporting system and not a driver. Using Industry awareness clouds the clarity of the purpose. If personal are properly trained and conscious of their responsibilities, then they are in fact situationally aware, and will therefore drive the reporting process on the detection an Impact Event. Industry awareness falsely labels this Standard as unique to the electrical industry when clearly many outside and international agencies will be notified and involved. Situational Awareness seems much more appropriate and encompassing. Other then that the Purpose is a large improvement from the original.
Response: The DSR SDT thanks you for your comment. The DSR SDT changed "situational awareness" to "industry awareness" to address concerns about real-time reporting (which this standard does not cover) and to avoid confusion with the NERC Situational Awareness organization.		
Ameren	No	The original Purpose wording was clear, concise and understandable.
Response: The DSR SDT thanks you for your comment. The original purpose statement was in the form of a requirement and not a purpose statement.		
ISO New England, Inc	No	The purposed states To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of Impact Events and their causes, if known, by the Responsible Entities. Awareness by who in the industry?
Response: The DSR SDT thanks you for your comment. The requirements of this standard require that events be reported after-the-fact. The NERC Events Analysis Program will take certain events reported under this standard and analyze them to provide information to the entire body of users, owners and operators of the BES.		
Calpine Corp	No	The purpose has moved significantly from the originally approved SAR. The purpose should focus on reporting requirements for reporting electrical disturbances to the Bulk Electric System that exceed specific thresholds. Sabotage/vandalism/theft are a subset of the reportable events that could have or do cause a Bulk Electric System Electrical Disturbance. The Standards content should focus on setting requirements to

Organization	Yes or No	Question 1 Comment
		report specific types of electrical disturbance events and providing guidance for performing that reporting. Alternative language: Purpose: To establish reporting requirements for events that either cause, or have the potential to cause, significant disturbances on the Bulk Electric System.
Response: The DSR SDT thanks you for your comment**.** The purpose covers the EOP-004 and CIP-001 standards which include disturbance and sabotage. The use of the word 'events' and the definition of the specific events to be reported (see Attachment 1) is a result of combining these two standards as well as the drafting team's efforts to address FERC Order 693 Directives. The proposed purpose statement does not adequately address these items.		
BGE	No	BGE believes that using the term Impact Events as currently defined is too vague. An alternative statement would be requiring the reporting of events listed in Attachment 1 and their causes, if known and making the definition change as noted in question 2.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated the defined term "Impact Events" and uses the generic term "events: in the purpose statement. *To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of events with the potential to impact reliability and their causes, if known, by the Responsible Entities.*		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	No	"To improve industry awareness and the reliability fo the Bulk Electric System by requiring the reporting of Impact Events and their causes, if known by the Responsible Entities." The revised purpose statement includes the phrase, if known. This seems like a huge loophole. They should change it to when discovered or when notified.
Response: The DSR SDT thanks you for your comment. The intent of "if known" was to make sure that events were reported regardless of whether the cause was known. It is important for entities to report events and to return the BES to a reliable operating state. Investigation of causes can occur at a later time.		
Indeck Energy Services	No	The reporting of events does not improve the reliability of the BES. If someone takes action based on the reporting, there might be an improvement. Because many of these events are not preventable, such as sabotage or weather, reporting them won't improve reliability. The original Purpose was satisfactory.
Response: The DSR SDT thanks you for your comment. The requirements of this standard require that events be reported after-the-fact. The NERC Events Analysis Program will take certain events reported under this standard and analyze them to provide information that will lead to improvements in BES reliability.		
Brazos Electric Power Cooperative	No	Instead of Impact Event could simply call it Event Information Reporting.

Organization	Yes or No	Question 1 Comment
Response: The DSR SDT thanks you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event."		
Compliance & Responsiblity Organization	No	See comments set forth in number 2.
Georgia Transmission Corporation & Oglethorpe Power Corporation	Yes	We find it unnecessary to state that the purpose of a Reliability Standard is to "improve the reliability of the Bulk Electric System."
Response: The DSR DT thanks you for your comment. The DSR SDT disagrees. This is an integral part of the purpose of reporting events.		
Midwest Reliability Organization	Yes	The addition of "industry awareness" adds to the scope of this Standard. Whereby an entity is required to inform the RC and others of actual and potential Impact Events.
Response: The DSR DT thanks you for your comment. The DSR SDT has streamlined Attachment 1 to ensure that the proper reporting is accomplished.		
American Municipal Power	Yes	The purpose is acceptable. I think it could be improved and simplified. There were not any questions on the title. Consider changing the title to Reportable Events. There were not any questions on the category. I suggest changing the category from Emergency Operations to Communications. Reporting events can trigger and be more than just Emergency Operations. I feel the reporting function performed by entities should be under the Communications category. Title: Reportable Events Purpose: To improve reliability by communicating timely information about an event or events.
Response: The DSR SDT thanks you for your comment. The DSR SDT revised the existing title of the standard to conform to the intended purpose of reporting events. The team discussed making this a COM standard during the initial DT discussions but decided to retain the existing EOP-004 standard category and number. This is not a real-time reporting standard but requires after the fact reporting.		
Ingleside Cogeneration LP	Yes	The addition of the modifier if known to reporting the cause of an Impact Event is appropriate. It often proves counter-productive to speculate as initial conjectures of the cause of an event are easy to come up with, but difficult to back out of later.
Response: The DSR SDT thanks you for your comment.		
Duke Energy	Yes	However, as we have noted previously, the DSR SDT statement that the proposed changes do not include any real-time operating notifications is inconsistent with requiring notification within one hour for thirteen of the

Organization	Yes or No	Question 1 Comment
		twenty listed Events in Attachment 1 Impact Event Table. Also, in the Background discussion, under Law Enforcement, the DSR SDT states that the objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting Impact Events. As we have previously commented, we are still required to make real-time reports under other standards. Requiring duplicate real-time reporting under EOP-004-2 is a waste of resources which could otherwise be used to improve reliability.
Response: The DSR SDT thanks you for your comment. We have made significant revisions to Attachment 1 and the reporting time requirements to address the real-time reporting concern.		
Constellation Power Generation	Yes	While CPG generally agrees with the purpose statement, we believe that the term Impact Events should be removed. Please see CPGs response to Question 2 discussing the term Impact Events.
Response: The DSR SDT thanks you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Please see responses to comments on question 2.		
Georgia System Operations Corporation	Yes	We agree with the purpose. However, we do not agree that the purpose will be achieved as this standard is currently drafted or that the standard is ready for balloting.
Response: The DSR SDT thanks you for your comment. We have made significant revisions to the body of the standard and Attachment 1.		
Northeast Power Coordinating Council	Yes	
Bonneville Power Administration	Yes	
Western Electricity Coordinating Council	Yes	
PPL Supply	Yes	
Pacific Northwest Small Public Power Utility Comment Group	Yes	
PSEG Companies	Yes	

Organization	Yes or No	Question 1 Comment
Pepco Holdings Inc and Affiliates	Yes	
Midwest ISO Standards Collaborators	Yes	
FirstEnergy	Yes	
SERC OC Standards Review Group	Yes	
PJM Interconnection LLC	Yes	
Southern Company	Yes	
SRP	Yes	
We Energies	Yes	
City of Tallahassee (TAL)	Yes	
Lakeland Electric	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
Liberty Electric Power LLC	Yes	
Sweeny Cogeneration LP	Yes	
American Electric Power	Yes	
USACE	Yes	

Organization	Yes or No	Question 1 Comment
New Harquahala Generating Co.	Yes	
Independent Electricity System Operator	Yes	
Platte River Power Authority	Yes	
Alliant Energy	Yes	
CenterPoint Energy	Yes	
ExxonMobil Research and Engineering	Yes	
PPL Electric Utilities	Yes	
Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
American Transmission Company	Yes	
BC Hydro	Yes	

2. Do you agree with the proposed definition of Impact Event? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: The majority of the commenters do not agree with the definition and thought the definition as overly broad, too subjective and confusing. Many commenters questioned whether there was a need for a definition of Impact Event at all. The DSR SDT discussed the comments and suggestions and decided to incorporate commenters' suggestion to delete the definition and rely on the Attachment 1 to stand on its own.

The DSR SDT has deleted the Impact Event definition.

Organization	Yes or No	Question 2 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation	No	We do not think that Impact Event should be defined using a recursive definition, i.e. that the word "impact" should be used in the definition of the term "Impact Event." Instead, we suggest using an enumerative definition in that the tables included in Attachment 1 are themselves used to define "Impact Event." If this definition is not acceptable, we suggest replacing the word "impact" in the definition with the word reduce, reduced, or potential to reduce the reliability of the BES.
Response: The DSR SDT thanks you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events for the given thresholds listed in Attachment 1.		
Northeast Power Coordinating Council	No	Is there a need for this definition? By itself the term is not specific on the types of events that are regarded as having an impact. The detailed listing of events that fall into a reportable event category, hence the basis for the Impact Event, is provided in Attachment A. The events that are to be reported can be called anything. Defining the term Impact Event does not serve the purpose of replacing the details in Attachment A, and such a term is not used anywhere else in the NERC Reliability Standards. For a complete definition of Impact Event, all the elements in Attachment A must be a part of it. Suggest consider not defining the term Impact Event, but rather use words to stipulate the need to have a plan, to implement the plan and to report to the appropriate entities those events listed in Attachment A.
Response: The DSR SDT thanks you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events for the given thresholds listed in Attachment 1.		

Organization	Yes or No	Question 2 Comment
Bonneville Power Administration	Yes	Agree, but note that this will add many more situations to reporting and it will require more staff time to accomplish this.
Response: The DSR SDT thanks you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events for the given thresholds listed in Attachment 1.		
Midwest Reliability Organization	No	The proposed definition is not supported by any of the established bright line criterias that are contained within attachment 1. This Results Based Standard should close any loop-holes that could be read into any section, especially the definition. According to rules of writing a definition, a definition should not contain part of the word that is being defined. Recommend the definition be enhanced to read: Impact Event: Any Contingency which has either effected or has the potential to effect the Stability of the BES as outlined per attachment 1. Within this enhanced recommendation, presently defined NERC terms are used (Contingency and Stability), thus supporting what is current used within our industry. There is also a quantifiable aspect of as outlined per attachment 1 that clearly defines Impact Events.
Response: The DSR SDT thanks you for your comment. The DSR SDT believes the definition is embodied in Attachment 1 criteria and needs no further clarification. We have deleted the proposed defined term "Impact Events" and will use the generic term "event."		
Western Electricity Coordinating Council	No	We question the need for a defined term. It appears that an Impact Event is any event identified in Attachment 1. The use of the defined term combined with the language of Requirement 2 to implement the Impact Event Operating Plan for Impact Events listed in Attachment 1 may be confusing. Is an Impact Event any event described by the proposed definition or is an Impact Event any event listed in Attachment 1?
Response: The DSR SDT thanks you for your comment. The DSR SDT agrees the definition could be confusing. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events for the given thresholds listed in Attachment 1.		
Dominion	Yes	Dominion agrees with the proposed definition of Impact Events, but notes the use of the phrase has the potential to impact is somewhat subjective. The concern being a Responsible Entity makes a judgment on an events potential impact that is viewed differently after-the-fact by an auditor.
Response: The DSR SDT thanks you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events for the given thresholds listed in Attachment 1.		
Pepco Holdings Inc and Affiliates	No	The two sentence definition will not be adequate to serve well over the course of time. People will have to read and understand the standard without benefit of the detailed information, explanations and interpretations

Organization	Yes or No	Question 2 Comment
		available during the standards development process. Without additional explanation as provided in the background and the guideline and technical basis sections, to support the definition, the standard will be subject to confusion and interpretations. Consider adding a lot of the information and explanation that is in those sections to the standard. Any event could be an impact event. However, only a subset is reportable. What is really being addressed are reportable events. More specifically after the fact reporting of unplanned events.
Response: Thank you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events for the given thresholds listed in Attachment 1.		
Midwest ISO Standards Collaborators	No	The definition of Impact Event is overly broad because of the use of potential to impact and the Such as list. Consider routine switching has the potential to result in a mis-operation. This means all routine switching is an impact event. The Such as list should be struck and potential language should be struck.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event."		
FirstEnergy	No	Although we agree with the definition of Impact Event, we believe that it should be clear that this term is specific to the events listed in Attachment 1 of the standard. Therefore, we suggest adding the phrase (as detailed in Attachment 1 of EOP-004-2) in the definition.
Response: Thank you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
SERC OC Standards Review Group	No	We believe the definition is too broad even considering Attachment 1, footnote1, which, for example, uses the term significantly and other ambiguous terms. Consideration should be given to limiting the definition to unplanned events.
Response: Thank you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event."		
PJM Interconnection LLC	No	The term "Impact Event" has been too broadly defined. According to the current definition, any event (including routine operations) can have the potential to impact the reliability of the Bulk Electric System and hence can be an Impact Event. The definition should only include unplanned events. Attachment 1 lists the events that are reportable. It seems that the definition of Impact Event refers to the events in Attachment 1 as opposed to defining Impact Event. As such, it is best that the SDT not define Impact Event but use words to the effect that requires an entity to have a plan and implement it for reporting unplanned events outlined in Attachment 1. If Impact Event were to be defined, we suggest the following definiton would be a better

Organization	Yes or No	Question 2 Comment
		option:"An Impact Event is any unplanned event listed in Attachment I that has either adversely impacted or has the potential to adversely impact the reliability of the Bulk Electric System."
Response: Thank you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event."		
SRP	No	Suggest that definition include reference to the fact that this is non-desired occurence, as the word 'impact' has neither a positivie nor negative implication. This is not a well formed definition as it contains circular refernces to 'impacted' and 'event' within the definition.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event."		
We Energies	No	From an on-line dictionary, an event is something that happens. Combined with the phrase has the potential to impact and the definition of Impact Event would include every routine operation performed by any entity. Taking a generator on or off line, switching a transmission line in or out, traffic driving past a substation, all have the potential to impact the BES. The Impact Event definition is overly broad and needs to be significantly narrowed.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event."		
Compliance & Responsiblity Organization	No	NextEra Energy Inc. (NextEra) appreciates the drafting team providing valuable ideas and a framework on how to improve and consolidate CIP-001 and EOP-004. However, NextEra also believes that the currently drafted EOP-004-2 needs to be revised and enhanced to more clearly explain the Responsible Entities' duties, the definition of sabotage and address FERC directives and concerns. For example, NextEra is not in favor using the term "Impact Event" which seems to add considerable confusion of what is or is not sabotage. In Order No. 693, FERC stated its interest in NERC revising CIP-001 to better define sabotage and requiring notification to the certain appropriate federal authorities, such as the Department of Homeland Security. FERC Order 693 at PP 461, 462, 467, 468, 471. NextEra has provided an approach that accomplishes FERC's objectives and remains within the framework of the drafting team, but also focuses the process of determining and reporting only those sabotage acts that could impact other BES systems. Today, there are too many events that are being reported as sabotage to all parties in the Interconnection, when in reality these acts have no material affect or potential impact to other BES systems other than the one that experienced it. For example, while the drafting team notes the issue of copper theft is a localized act, there are other localized acts of sabotage that are committed by an individual, and these acts pose little, if any, impact or threat to other BES systems other than the one experiencing the sabotage event. Reporting sabotage that

Organization	Yes or No	Question 2 Comment
		has no need to sent of everyone does not necessary add to the security or reliability of the BES. Related, there is a need to clarify some of the current industry confusion on who should (and has the capabilities to) be reporting to a boarder audience of entities. Hence, NextEra approach provides a clear definition of sabotage, as well as the process for determining and reporting sabotage. NextEra further believes that some of the requirements can be consolidated and more clearly stated, and NextEra has attempted to do that in the approach presented below. Lastly, NextEra comments on Attachment 1 are submitted in response to question 17. NextEra Approach Delete definition of Impact Event and its use in the requirements and in Attachment 1 Delete 13, 14, 15 and 19 in Attachment 1 Delete and replace R1 through R5 with the following: New Definition Attempted or Actual Sabotage: an intentional act that attempts to or does destroy or damage BES equipment or a Critical Cyber Asset for the purpose of disrupting the operations of BES equipment, Critical Cyber Asset or the BES, and has a potential to materially threaten or impact the reliability of one or more BES systems (i.e., is one act in a larger conspiracy to threaten the reliability of the Interconnection or other BES systems). R1. Each Responsible Entity shall document and implement a procedure (either individually or jointly with other Responsible Entities) to accomplish the reporting requirements, including the time frames, assigned to the Responsible Entity as set forth in Attachment 1 items 1 through 12, 16, 17 and 18 for reporting from the Responsible Entity to its Regional Entity and NERC, using the form in Attachment 2 or the DOE OE-417 reporting form. R2. Each Responsible Entity shall document and implement a procedure (either individually or jointly with other Responsible Entities) to report to its internal personnel with a need to know and its Reliability Coordinator an act of Attempted or Actual Sabotage, using the form in Attachment 2 or the DOE OE-417 reporting form, within one hour after a determination has been made that an act Attempted or Actual Sabotage has occurred. To make a determination that an act of Attempted or Actual Sabotage has occurred, the Responsible Entity shall document and implement a procedure that requires it, as soon as practicable after the discovering an act appearing to be Attempted or Actual Sabotage, to engage local law enforcement or the Federal Bureau of Investigation or Royal Canadian Mounted Police, as deemed appropriate, to assist the Registered Entity make such a determination. Upon receiving a report of Attempted or Actual Sabotage from a Responsible Entity, the Reliability Coordinator shall within one hour forward the report to other impacted Reliability Coordinators, Responsible Entities, Regional Entities, NERC, Department of Homeland Security, and the Federal Bureau of Investigation or the Royal Canadian Mounted Police. R3. Each Responsible Entity shall review (and conduct a test for sabotage only) of its documented procedure required in R1 and R2 with no more than 15 calendar months between tests for sabotage reporting. If, based on the review or test, the Responsible Entity determines there is a need to update its documented procedure, it shall update the procedures within 90 calendar days of the review or test.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comments and suggestions. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Other revisions were made to the standard based on comments received on specific requirements. The DSR SDT believes that these revisions clarify the requirements and has provided additional details in response to comments from questions Q3, Q6, Q7, Q8, Q11, Q12, Q13, Q14 and Q17. Please see the revised standard. In regards to sabotage, the DSR SDT believes that the reporting of events supports the reliability of the BES. Sabotage usually is determined after the event is investigated and sabotage may be one aspect of a single event. The intent is to report events (per Thresholds of Reporting in Attachment 1) that have an impact on BES reliability. The background section of the standard provides guidance with respect to reporting events to law enforcement. For clarity, the DSR SDT has added the following sentence to the first paragraph under the heading "Law Enforcement Reporting": "These are the types of events that should be reported to law enforcement." The entire paragraph is: "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES."		
Exelon	No	The definition of impact events should be reworded to align with OE-417 and to explicitly reference that only events identified in EOP-004 ? Attachment 1 are to be reported. Suggest the following:"An incident that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-opeation, environmental conditions, or human action as defined in EOP-004 Attachment 1." Propose the definition be changed to include material impact and read as follows; Any event which has either caused or has the potential to cause an adverse material impact to the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action?
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
City of Tallahassee (TAL)	No	While I agree with the overall concept, I am concerned with "or has the potential to impact." While the standard makes reference to Attachment 1 Parts A and B, the inclusion of the attachment is not in the definition. This leaves ambiguity in the definition that could enable second guessing by auditors. Proposed: "An impact event is any event that has either impacted or has the potential to impact (above the

Organization	Yes or No	Question 2 Comment
		thresholds described in EOP-004-2 Attachment 1) the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action."
Response: Thank you for your comments. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event."		
American Electric Power	No	The definition is too broad and vague. The text in the comment form has the following sentence Only the events identified in EOP-004 Attachment 1 are required to be reported under this Standard. The definition should contain that caveat or something similar.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
USACE	No	1) You cannot use the terms impact and event to define impact event. 2) The phrase "has the potential to impact" makes the definition too vague. Every action taken to modify the system or its components has the potential to impact the Bulk Electric System. 3) Recommend to change the definition to "Any occurrence which has adversely affected the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action."
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Consumers Energy	No	The definition of Impact Event seems very vague and nebulous. This definition should be modified to be clear and concise, such that entities clearly understand what is included within the definition.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Ameren	No	The documentation from the SDT included the reliability objective for EOP-004-2 which should be included in the definition of Impact Event. Our suggested alternate defintion for Impact Event: "An Impact Event is any event that has either caused, or has the likely potential to cause, an outage which could lead to Cascading. Such events will be identified as being caused by, to the best of the reporting entity's information: (1) equipment falure or equipment mis-operation, (2) environmental conditions, and/or (3) human actions."

Organization	Yes or No	Question 2 Comment
		This alternate wording includes the reliability objective and clarifies the three known, or likely, causes of the Impact Event.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
ISO New England, Inc	No	We question the need for this definition since by itself the term is not specific on the types of events that are regarded as having an impact. The detailed listing of events that fall into a reportable event category, hence the basis for the Impact Event, is provided in Attachment A. For that matter, these events that are to be reported can be called anything, or just simply be titled "Event to be Reported" without having to define them. Defining the term Impact Event does not serve the purpose of replacing the details in Attachment A, and such a term is not used anywhere else in the NERC reliability standards. In fact, for the term Impact Event to be fully defined, all the elements in Attachment A must become a part of it. We therefore suggest the SDT to consider not defining the term Impact Event, but rather use words to stipulate the need to have a plan, to implement the plan and to report to the appropriate entities those events listed in Attachment A. If the SDT still wishes to retain a definition despite our reservations noted above, we strongly suggest an improvement. The proposed definition of Impact Event is overly broad because of the use of "potential to impact" and the "Such as" list. Consider that routine switching has the potential to result in a mis-operation. In that regard most routine switching could be interpreted as an impact event. The "Such as" list should be struck and "potential" language should be struck. An alternative definition to consider: An Impact Event is any deliberate action designed to reduce BES reliability; unintended accident that could result in an Adverse Reliability Impact; or an unusual natural event that causes or could cause an Adverse Reliability Impact.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Calpine Corp	No	Adding a definition for Impact Event is unnecessary and does not provide useful clarification of the actual reporting requirement for events that either impact the Bulk Electric System or have the potential to impact the Bulk Electric System. The all-encompassing nature of the proposed definition seems to conflict with the finite listing of events that actually require reporting. Although FERC specifically requested additional clarification of the term sabotage to clarify reporting requirements, the Drafting Team is correct in noting that sabotage implies intent and that the intent of human acts is not always easily determined. The fact that intent is not always determinable within the reporting timeframe can be dealt with more simply by requiring (in attachment

Organization	Yes or No	Question 2 Comment
		1) that human intrusions that have not been identified within the reporting timeframe as theft or vandalism should be reported as potential sabotage pending further clarification. This approach negates the need for an additional definition that may cause confusion regarding which events are reportable and eliminates the potential for under-reporting based on the assumption that the cause might be theft or vandalism.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
BGE	No	Change the definition of "Impact Event", to add the following phase to the definition "Any event (listed in Attachment 1) which has either…." Also, the phrase "…or has the potential to impact the reliability…" is too vague and broad. Such broad statement is unhelpful in clarifying entities' compliance obligation and potentially creates conflicted reporting between entities. A clear statement of how the reliability is affected should be used, i.e., results in contingency emergency situation or IROL.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Alliant Energy	No	The proposed definition is not supported by any of the established bright line criteria that are contained within attachment 1. This Results Based Standard should close any loop-holes that could be read into any section, especially the definition. We recommend the definition be enhanced to read: Impact Event: Any Contingency which has either effected or has the potential to effect the Stability of the BES as outlined per attachment 1. Within this enhanced recommendation, presently defined NERC terms are used (Contingency and Stability), thus supporting what is current used within our industry. There is also a quantifiable aspect of as outlined per attachment 1 that clearly defines Impact Events. If the above definition is not adopted, we believe it should be rephrased to narrow the scope to those events that result from malicious intent or human negligence/error. We are concerned that by using phrases like unintentional or intentional human action in combination with damage or destruction basically means everything except copper theft becomes a reportable impact event (including planned actions we must perform to comply with CIP-007 R7).
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
CenterPoint Energy	No	CenterPoint Energy suggests that the phrase "…or has the potential to impact…" be deleted as it makes the definition vague and broad. Similar issues encountered in trying to define sabotage may resurface, such as

Organization	Yes or No	Question 2 Comment
		varying definitions or interpretations of "potential." If this standard is to support after-the-fact reporting, the focus should be on actual events, not potential situations or events. Effective and efficient prevention would come from analysis of actual events. Resources and reporting could become overwhelmed upon having to consider "potential." All references to "potential" should be removed from the standard, guidance, and attachments.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
ExxonMobil Research and Engineering	No	The use of the word potential is ominous.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Occidental Power Marketing	No	The SDT includes in the definition the "potential to impact the reliability of the BES." This seems vague, although Attachment 1 clarifies what actually has to be reported. An LSE may have limited or no knowledge of "potential to impact." The SDT may want to refine the definition, e.g., "to the extent the entities' knowledge could reasonably reveal the impact."
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Lincoln Electric System	No	As currently drafted, the proposed definition of Impact Event appears vague and provides entities minimal clarity in terms of distinguishing events of significance. Recommend the drafting team reference Attachment 1: Impact Events Tables within the definition to direct industry towards more specific criteria.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
American Transmission Company	No	ATC does not agree with the proposed definition and further disagrees whether a definition is needed at all. Proposed Definition: The definition, read outside of the proposed standard, does not provide Registered Entities with a clear meaning of the purpose of the definition. It is ATCs opinion that the SDT is using the term Impact Event as an introduction phrase to Attachment 1. ATC would be more comfortable if the

Organization	Yes or No	Question 2 Comment
		definition was dropped and the team would re-write the requirement to specifically point to Attachment 1. It is our opinion that this type of structure would achieve the goal of the team to get Registered Entities to report on events identified in Attachment 1.The other option is for the team to write into the definition that the events being discussed are limited to those identified in Attachment 1. Also the language currently being used in the definition includes potential and such as. These terms should be struck from the definition.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Ingleside Cogeneration LP	No	The SDT includes in the definition the potential to impact the reliabilty of the BES. This seems vague, although ultimately the events which meet the threshold of a reportable Impact Event are governed by the tables under Attachment 1. We believe that there should be close, if not perfect, synchronization between the EROs Event Analysis Process and Attachment 1 since they share the same ultimate goal as EOP-004-2 to improve industry awareness and BES reliability.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Duke Energy	No	The phrase "…or has the potential to impact…" makes this an impossibly broad definition, and demonstrating compliance will not be straightforward.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Constellation Power Generation	No	The currently proposed definition is vague and can be easily misinterpreted. Coining a term to define the events that the DSR SDT hopes to capture in EOP-004-2 is a difficult task, one that may not be necessary. Replacing the term Impact Events with events in Attachment 1, would eliminate the need to define such a term. In addition, the phrase or has the potential to impact the reliability is too vague and broad. Such broad statement is unhelpful in clarifying entities compliance obligation and potentially creates conflicted reporting between entities. The language in the reporting requirements should be limited to real impact events, while information sharing on near miss or deficiency incidents should be handled as good industry practices and not subject to onerous compliance obligations. The drafting team should also give careful consideration to the existing reporting and information sharing currently in place in the industry. When an event occurs, partners in the electric sector are notified as part of

Organization	Yes or No	Question 2 Comment
		existing requirements outside of NERC compliance.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Georgia System Operations Corporation	No	It is not clear for the purposes of complying with this standard what it means to impact reliability. Impact in what way. To what degree. Do not define this term. An alternative would be to define it as those events listed in Appendix 1.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Indeck Energy Services	No	It's not a definition. It needs some quantification, such as, a Reportable Disturbance (NERC glossary), a reportable event under DOE OE-417, sabotage or bomb threat. Defining it as having or potentially having an impact is no definition. What is an impact? It needs to be quantified or auditors will have license to define it any way that they want. It shouldn't be a NERC Glossary definition if its only use is in EOP-004. Within EOP-004, it can be defined as anything in Attachment 1.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Progress Energy	No	Progress Energy appreciates the Standard Drafting Teams work on this project. Any potential impact is too vague and impossible to measure. Progress is unsure of how the ERO or Regional Entity measure impact. Potential is very subjective.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Brazos Electric Power Cooperative	No	
Southern Company	Yes	There is concern that the proposed definition for Impact Event does not allow for prudent judgment and preliminary situational assessment by the entity to declare a Potential Impact Event (especially threats) as non-credible. The thresholds for reporting established in Attachment 1 ? Part A provide a somewhat definitive bright line with regard to those events identified in Part A, but for some of the events in Part B there should be allowance for an assessment by the entity to reasonably determine whether the event poses a credible threat

Organization	Yes or No	Question 2 Comment
		to the reliability of the BES. This is attempted in the footnote to the Forced Intrusion event in Attachment 1 ? Part B, but we think this allowance for entity assessment and prudent judgment needs to apply more pervasively, perhaps by including the term credible in the definition of Impact Event or at least by adding the term credible wherever the term physical threat is used.
Response: Thank you for your comments. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." The word "credible" could lead to many interpretations as well. Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
American Municipal Power	Yes	The definition of Impact Event is acceptable and an improvement. I feel it could be improved and simplified further. Consider changing Impact Event to a "reportable event."
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Liberty Electric Power LLC	Yes	I am interpreting the phrase "has the potential" to exclude events which had the potential, but did not impact the BES. An example would be a generation trip - if the trip had happened during a system emergency it could have affected the BES, but since it happened under normal conditions there is no reporting responsibility. Some assurance on this interpretation would be appreciated.
Response: The DSR SDT thanks you for your comment. We have deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Manitoba Hydro	Yes	"Disturbance" has a unique and traditional meaning in the electrical industry, basically meaning "a notable electrical event causing in imbalance of load and generation." Attempting to include the many scenarios can that can affect reliability blurred the current vision of "Disturbance" and the addition of "unusual occurrences" just added to the confusion. It never seemed appropriate to submit an unusual occurrence on a "Disturbance Report." "Impact Event" is very encompassing and then detailed specifically in Attachment 1.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
Independent Electricity System Operator	Yes	We do not have any issue with the wording of the definition, but question the need for this definition since by itself the term is not specific on the types of events that are regarded as having an "impact." The detailed listing of events that fall into a reportable event category, hence the basis for the Impact Event, is provided in Attachment A. For that matter, these events that are to be reported can be called anything. Defining the term Impact Event does not serve the purpose of replacing the details in Attachment A, and such a term is not

Organization	Yes or No	Question 2 Comment
		used anywhere else in the NERC reliability standards. In fact, for the term Impact Event to be fully defined, all the elements in Attachment A must become a part of it. We therefore suggest the SDT to consider not defining the term Impact Event, but rather use words to stipulate the need to have a plan, to implement the plan and to report to the appropriate entities those events listed in Attachment A.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
PPL Electric Utilities	Yes	PPL EU agrees with the definition. We would like to point out that our interpretation of the definition excludes maintenance work. Our interpretation also concludes that maintenance work that does not go as planned or goes awry and impacts the reliability of the BES would be an impact event and reported as required per Attachment 1.
Response: Thank you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		
SDG&E	Yes	
PPL Supply	Yes	
PSEG Companies	Yes	
SPP Standards Review Group	Yes	
Lakeland Electric	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
United Illuminating Co	Yes	
Arkansas Electric Cooperative	Yes	

Organization	Yes or No	Question 2 Comment
Corporation		
Sweeny Cogeneration LP	Yes	
New Harquahala Generating Co.	Yes	
Platte River Power Authority	Yes	
Farmington Electric Utility System	Yes	
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	
BC Hydro	Yes	
Response: Thank you for your response. Most commenters who responded to this question disagreed with the proposed definition and some suggested that the definition is not needed. In response, the drafting team has deleted the proposed defined term "Impact Events" and will use the generic term "event." Reporting is only required for those events and for the given thresholds listed in Attachment 1.		

3. Do you agree that the DSR SDT has provided an equally efficient and effective solution to the FERC Order 693 directive to "further define sabotage"? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: Most stakeholders agreed that the drafting team addressed the directive to further define sabotage. Commenters generally agreed that the DSR SDT approach in the currently proposed solution effectively addresses FERC Order 693 directive. The approach clarifies the triggering event for an entity to take action and, by deleting all references to "sabotage," in effect removes the very term that had no clear definition.

Organization	Yes or No	Question 3 Comment
Pepco Holdings Inc and Affiliates	No	See #2. With out the explanation contained in background information, over time those that have not been involved with this standard development will struggle with how to interpret the code words of non environmental and intentional human action.
Response: The DSR DT thanks you for your comment. This is a Results-based standard and the format includes all of the information, with the exception of the Rationale boxes, through the ballot and filing of the standard. The background section of the proposed standard will be retained with the standard for future reference.		
Midwest ISO Standards Collaborators	No	In general, we agree that the standard drafting team has provided an equally efficient and effective alternative, but we wonder if the SDT has not in essence already defined sabotage in their description for why they cant define sabotage. It seems that sabotage involves willful intent to destroy equipment. In general, intent would have to be determined by an investigation of law enforcement. This could be part of the definition. There might be some obvious acts that could be included without investigation such as detonation of a bomb. Is it possible for the SDT to use the DOE definition for sabotage? We encourage the SDT to provide a definition for sabotage.
Response: The DSR DT thanks you for your comment. The DSR SDT believes that the reporting of events supports the reliability of the BES. Sabotage usually is determined after the event is investigated and that sabotage may be one aspect of a single event. The intent is to report (per Thresholds of Reporting in Attachment 1) events that have an impact on BES reliability. The background section of the standard provides guidance with respect to reporting events to law enforcement. For clarity, the DSR SDT has added the following sentence to the first paragraph under the heading "Law Enforcement Reporting": "These are the types of events that should be reported to law enforcement." The entire paragraph is: o "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely		

Organization	Yes or No	Question 3 Comment
upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES."		
Compliance & Responsiblity Organization	No	See comments set forth in number 2.
Response: The DSR DT thanks you for your comment. Please see the DSR DT response above for question number 2.		
Sweeny Cogeneration LP	No	The threshold for reporting what could be sabotage still leaves the door open for second guessing after-the-fact. For example, if graffiti is sprayed on a BES asset, the entity is to assume that the event is not to be reported. However, intent to harm the BES may be discovered at a later point with ramifications to the entity who did not report it. A solution may be to strengthen footnote 3 to both reporting tables, which makes an allowance to report if you cannot reasonably determine likely motivation of sabotage. If acceptable methods to provide justifiable evidence that reporting was NOT required, then this loophole may be corrected.
Response: The DSR SDT thanks you for your comment. The DSR SDT believes that the reporting of events supports the reliability of the BES. Sabotage usually is determined after the event is investigated and that Sabotage may be one aspect of a single event. The intent is to report events (per Thresholds of Reporting in Attachment 1) that have an impact on BES reliability. Attachment 1 has been updated per comments received.		
USACE	No	The DSR SDT should have defined sabotage since it helps the SDT working on CIP standards further define its action. Sabotage can be defined as the deliberate act of destruction, disruption, or damage of assets to impact the reliability of the BES.
Response: The DSR SDT thanks you for your comment. The DSR SDT believes that the reporting of events supports the reliability of the BES. Sabotage usually is determined after the event is investigated and that Sabotage may be one aspect of a single event. The intent is to report events (in Attachment 1) that have an impact on BES reliability. Attachment 1 has been updated per comments received.		
Consumers Energy	No	EOP-004 does not appear to address a reliability need. Reporting after-the-fact information such as that described in Impact Events does not do anything to improve Bulk Electric System reliability. Therefore, we recommend that CIP-001 be updated to address sabotage events, and that NERC otherwise rely on the statutory reporting to the DOE that is represented by OE-417 for any after-the fact information. The remainder of our comments reflects detailed comments on the posted draft, presuming that our objection

Organization	Yes or No	Question 3 Comment
		represented above will be disregarded.
Response: The DSR SDT thanks you for your comment. Providing event reporting information will start the event analysis process done by the current NERC Event Analysis Program. EOP-004-2 is the reporting vehicle to the ERO that will support the analysis phase of any event.		
Ameren	No	The SDT did not further define sabotage as directed by FERC, but instead created a new term that does not address the order. The Term Impact Event has no clarity or quantitative qualities by which an entity can determine what should be reported. The use of the phrase "has the potential to impact reliability" has such a vague scope, an auditor can interpret to mean any "off-normal" condition, which makes this standard impossible to comply with. The SDT should use the DOE definition of sabotage as follows: Sabotage - Defined by Department of Energy (DOE) as: An actual or suspected physical or Cyber attack that could impact electric power system adequacy or reliability Vandalism that targets components of any security system on the Bulk Electric System Actual or suspected Cyber or communications attacks that could impact electric power system adequacy or vulnerability, including ancillary systems which support networks (e.g. batteries) Any other event which needs to be reported by the Balancing Authority (Transmission Operations) to the Department of Energy. Sabotage can be the work of a single saboteur, a disgruntled employee or a group of individuals.
Response: The DSR SDT thanks you for your comment. The DSR SDT believes that the reporting of events supports the reliability of the BES. Sabotage usually is determined after the event is investigated and that Sabotage may be one aspect of a single event. The intent is to report events (per Thresholds of Reporting in Attachment 1) that have an impact on BES reliability. Attachment 1 has been updated per comments received. EOP-004-2 sets the minimum reporting requirements for events.		
Calpine Corp	No	The additional definition for “Impact Event” is unnecessary and does not provide useful clarification regarding actual reporting requirements. Sabotage, whatever the exact definition used, implies intent to damage or disrupt. The committee correctly notes that determination of actual intent is not always readily available. However, adding a general expansive definition encompasses all events that might disrupt the Bulk Electric System does not add clarity to the types of events that require reporting - which are listed in detail in Attachment 1.The issue can be more simply addressed by replacing the item “Human Intrusion” on Attachment 1, as follows: Event: Sabotage (note 3) Entity with Reporting Responsibility: All affected Responsible Entities listed

Organization	Yes or No	Question 3 Comment
		in the Applicability Section of this Standard. Threshold for Reporting: Forced Intrusions at a BES facility that have not been determined within the reporting period to be theft or vandalism that does not affect the operability of BES equipment. Note 3 For purposes of reporting under Attachment 1, reportable sabotage includes all forced intrusions at BES facilities that have potential to cause, or cause, any of the disturbance events listed in Attachment 1 and have not been determined to be theft or vandalism that did not result in any event listed in Attachment 1. Responsible Entities are not required to report incidents of theft or vandalism that do not result in disturbance events. This approach also eliminates the need to reference copper theft as a particular type of theft that does not require reporting.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event.". Attachment 1 has been updated per comments received. The DSR SDT believes that the reporting of events supports the reliability of the BES. Sabotage usually is determined after the event is investigated and that Sabotage may be one aspect of a single event. The intent is to report events (per Thresholds of Reporting in Attachment 1) that have an impact on BES reliability. Footnotes have been updated per comments received.		
CenterPoint Energy	No	CenterPoint Energy would agree if the definition for Impact Event was changed as suggested in the response to Question 2.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event.". Attachment 1 has been updated per comments received. The DSR SDT believes that the reporting of events supports the reliability of the BES.		
Duke Energy	No	Sabotage is still identified on the flowchart. Timeframes for reporting on Attachment 1 should be made consistent with DOE OE-417 reporting. Also on Attachment 1, the Threshold for Reporting on a Forced Intrusion Event should be Affecting BES reliability instead of At a BES facility.
Response: The DSR SDT thanks you for your comment. The DSR SDT has updated the flowchart. The DOE Form OE-417 is reviewed biennially by the DOE and can be updated or changed without NERC's involvement. The DSR SDT has taken into consideration the possible use of Form OE-417 to report events to NERC and agrees that this will fulfill EOP-004-2's reporting requirements. The DSR SDT has removed sabotage from the flowchart and has replaced it with: "Criminal act under federal jurisdiction."		

Organization	Yes or No	Question 3 Comment
Indeck Energy Services	No	The SDT hasn't defined sabotage. Attachment 1 does not do justice to the concept of sabotage. Sabotage should be defined as any intentional damage to BES facilities the causes a Reportable Disturbance, reportable event under DOE OE-417 or involves a bomb or bomb threat.
Response: The DSR SDT thanks you for your comment. The DSR SDT believes that the reporting of events supports the reliability of the BES. The intent is to report events (per Thresholds of Reporting in Attachment 1) that have an impact on BES reliability. Sabotage usually is determined after the event is investigated and that Sabotage may be one aspect of a single event. The DOE Form OE-417 is reviewed biennially by the DOE and can be updated or changed without NERC's involvement. The DSR SDT has taken into consideration the possible use of Form OE-417 to report events to NERC and agrees that this will fulfill EOP-004-2's reporting requirements.		
Exelon	Yes	Exelon agrees with the DSR SDT in that the currently proposed solution effectively addresses the intent of FERC Order 693 directive to both clarify the triggering event for an entity to take action and by deleting all references to "sabotage" in effect removes the very term that had no clear definition.
Response: Thank you for your comment.		
Georgia Transmission Corporation & Oglethorpe Power Corporation	Yes	We agree with the approach taken by the SDT.
Northeast Power Coordinating Council	Yes	It is more important to report suspicious events than to determine if an event is caused by sabotage before it gets reported.
Midwest Reliability Organization	Yes	Sabotage is usually associated with a malicious attack. Entities have always lacked the clinical expertise to determine if an event was malicious or not. The Impact Event bright line criteria clearly states what the minimum reporting requirements are.
Manitoba Hydro	Yes	"Impact event", The DSR SDT reasoning for this. 'A sabotage event can only be typically determined by law enforcement after the fact" is very creative and concise!
Response: The DSR SDT thanks you for your comment.		

Organization	Yes or No	Question 3 Comment
Independent Electricity System Operator	Yes	We agree since it is more important to report suspicious events than to determine if an event is caused by sabotage before it gets reported.
Response: The DSR SDT thanks you for your comment.		
ISO New England, Inc	Yes	We agree since it is more important to report suspicious events than to determine if an event is caused by sabotage before it gets reported.
Ingleside Cogeneration LP	Yes	Sabotage cannot be confirmed until after the fact, so we support this initiative.
Bonneville Power Administration	Yes	
Western Electricity Coordinating Council	Yes	
PPL Supply	Yes	
PSEG Companies	Yes	
Dominion	Yes	
SPP Standards Review Group	Yes	
FirstEnergy	Yes	
SERC OC Standards Review Group	Yes	
PJM Interconnection LLC	Yes	
Southern Company	Yes	
SRP	Yes	

Organization	Yes or No	Question 3 Comment
We Energies	Yes	
SDG&E	Yes	
City of Tallahassee (TAL)	Yes	
Lakeland Electric	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
United Illuminating Co	Yes	
American Municipal Power	Yes	Well done.
Liberty Electric Power LLC	Yes	
Arkansas Electric Cooperative Corporation	Yes	
American Electric Power	Yes	
New Harquahala Generating Co.	Yes	
Platte River Power Authority	Yes	
BGE	Yes	No comments.
Alliant Energy	Yes	
ExxonMobil Research and Engineering	Yes	

Organization	Yes or No	Question 3 Comment
PPL Electric Utilities	Yes	
Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
American Transmission Company	Yes	
Constellation Power Generation	Yes	
Georgia System Operations Corporation	Yes	None.
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	
Brazos Electric Power Cooperative	Yes	
Response: The DSR SDT thanks you for your response. Several commenters proposed revisions to the definition, and after deliberation the SDT has deleted the proposed defined term "Impact Events" and will use the generic term "event". Attachment 1 has been updated per comments received. The DSR SDT believes that the reporting of events supports the reliability of the BES.		

4. Do you agree with the proposed applicability of EOP-004-2 shown in Section 4 and Attachment 1 of the standard? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: The SDT believes that it has properly identified registered entities that may potentially have events and the appropriate types of events. A Registered Entity is only required to submit an events report for events listed in Attachment 1 if the registered entity was affected by the event. If an event occurs, only affected Registered Entities listed in Attachment 1 are required to submit a report on the event. The SDT believes that the industry will gain valuable information from having different perspectives of a single event. Differing viewpoints on the same event will provide for better clarity to all parties on the actual impact to the bulk electric system. The SDT would like to point out that reporting of events is from the time of identification not the time of the event. In response to the comments received, the SDT has made numerous enhancements to Attachment 1. **These revisions include:**

- **Added new column "Submit Attachment 2 or DOE OE-417 Report to:" which references Part 1.3 and provide the time required to submit the report.**
- **Combined Parts A and B into one table and reorganized it so that the events are listed in order of reporting times (either one hour or 24 hours)**
- **Removed references to "Impact Event" and replaced with the specific language for the event type in the "Entity with Reporting Responsibility". For example, replaced "Impact Event" with "automatic load shedding".**

The ERO and the RE were added as applicable entities to reflect CIP-002 applicability to this standard.

Organization	Yes or No	Question 4 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation	No	We do not believe that GO, TO, TSP, DP, or LSE should be included in the applicability of this standard. It is our opinion that the reporting requirements lie primarily with the applicable operator and should be limited as such. We recommend modifications as discussed in our response to question 6 to clearly define what types of events each Responsible Entity needs to prepare for. Currently, it seems that multiple entities are being required to report the same event for some events where only one entity should have a reporting responsibility. However, NERC should not decide which one entity should report a given event. The entities should have the flexibility to create a process which allows for coordination and communication at a local level and to work out with neighboring entities who might ultimately report events to the applicable

Organization	Yes or No	Question 4 Comment
		organizations.
Response: Thank you for your comments. The SDT disagrees that the operators are the only entities with obligations to report; owners and users may have very credible and valuable information relating to events. Such information may be extremely beneficial in developing lessons learned and analyzing events. Your suggestion to allow for local coordination and communication is a practical suggestion and the standard allows for it.		
Northeast Power Coordinating Council	No	Disagree with the following inclusion/exclusion of several entities: a. The applicable entities listed in Section 4 capture all the entities that are assigned a reporting responsibility in Attachment 1 of the standard. While some events in Attachment 1 have specific entities identified as responsible for reporting, certain events refer to the entities listed in specific standards (e.g. CIP-002) as the responsible entities for reporting. The latter results in IA, TSP and LSE (none of which being specifically identified as having a reporting responsibility) being included in the Applicability Section. NERC should be included in the Applicability Section as it is an applicable entity identified in CIP-002-3. b. If the above approach was not strictly followed, then suggest the SDT review the need to include IA, TSP and LSE since they generally do not own any Critical Assets and hence will likely not own any Critical Cyber Assets.
Response: The DSR SDT thanks you for your comment. The SDT believes it needs to follow the requirements of the standards as they currently apply. Since these entities are applicable to the underlying standards identified in Attachment 1, then they will be subject to reporting. If those standards are modified to remove the applicability to these functional registrations, then the appropriate SDT can modify the applicability of this standard. The SDT has reviewed the CIP-002-3 standard and has included the ERO and the RE in this standard.		
Pacific Northwest Small Public Power Utility Comment Group	No	We believe that facilities used in the local distribution of electric energy should be excluded from these requirements due the language of 16 U.S.C. ? 824o(a)(1) and 16 U.S.C. ? 824o(i)(1).
Response: The DSR SDT thanks you for your comment. The SDT constructed Attachment 1 based upon the existing requirements in the various reliability standards and established reporting obligations. The information about events and the analysis of those events will be useful to all owners, operators, and users of the bulk power system. The SDT has clarified the reporting requirement such that only those affected by the event are required to submit a report.		
PSEG Companies	No	The PSEG Companies believe the defining language, roles and responsibilities outlined in Attachment 1 are unclear and inconsistent. For example fuel supply emergency reporting footnote 2 “Report if problems with the fuel supply chain result in the projected need for emergency actions to manage reliability” attempts to clarify the condition for reporting but does not. Whose “emergency actions” are being referred to in the footnote? It is not clear if those actions would be related to the specific station or the overall Bulk Electric

Organization	Yes or No	Question 4 Comment
		System (BES). Can this be interpreted to imply a gas supply issue to one generating station as the result of pipeline maintenance, or local pressure issues would also requiring reporting? The PSEG Companies believe the definition of a fuel supply emergency needs to be more specific and less open to broad interpretation. In addition, the "Time to Submit Report" section of attachment 1 has a significant number of changes from the previous version. Accelerating the twenty four (24) hour to one (1) hour requirement for submitting the reports for several of the events takes resources away from managing the actual event. For the above comments failure to submit a report within 1 hour is a high or severe VSL for a fuel supply emergency. This approach seems inconsistent with ensuring the operation and reliability of the BES. One (1) hour reporting, in most cases, is not adequate time to compile the needed information, prepare report, ensure the accuracy, submit, and simultaneously manage the actual event. We recommend 24 hour reporting for: Damage or destruction to BES, Fuel Supply Emergency, Forced Intrusion, and Risk to BES equipment sections of Attachment 1.
Response: The DSR SDT thanks you for your comment. The SDT appreciates the observation on Fuel Supply Emergency and has adjusted Attachment 1 to address it. Reporting under the standard requires that the Registered Entity provide what information it has at the time of the report. The report may not provide the entire record or identification of the event. If the Registered Entity desires to submit an updated report, it may choose to do so; but there is no obligation to do so. The DSR SDT has significantly revised Attachment 1. We have removed the timing column and replaced it with more specific information regarding which form to submit and to whom the report is to be submitted. All events are now to be reported within 24 hours with the exception of Destruction of BES equipment, Damage or destruction of Critical Assets and Damage or destruction of Critical Cyber Asset events, Forced Intrusion, Risk to BES equipment and Detection of a reportable Cyber Security Incident. These events are to be reported within 1 hour. Notification of law enforcement (per Requirement R1, Part 1.3.2) is only required for these events. The background section of the standard provides guidance with respect to reporting events to law enforcement. For clarity, the DSR SDT has added the following sentence to the first paragraph under the heading "Law Enforcement Reporting": "These are the types of events that should be reported to law enforcement." The entire paragraph is: o "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES."		
Dominion	No	1) Several of the events require filing a written Impact Event report within one hour. System Separation, for example, is going to require an "all hands on deck" response to the actual event. We note that the paragraph above Attachment 1, Part A indicates that a verbal report would be allowed in certain circumstances, but this

Organization	Yes or No	Question 4 Comment
		is the same issue with the formal report in that the system operators are concerned with managing the event and not the reporting requirements. Another example would be the Loss of Off-site power to a nuclear generating plant. Suggest reconsideration of one hour reporting requirement for events requiring extensive operator actions to mitigate; 2) Several events seem to have the "Threshold for Reporting" contained in footnotes rather than in the table. For example, Damage or destruction of BES equipment - Footnote 1, Fuel supply emergency - Footnote 2, etc.) Suggest moving the actual threshold into the table; 3) If one hour reporting remains as indicated in Attachment 1; align/rename events similar to that of the 'criteria for filing' events listed in DOE OE-417 for consistency.
Response: Thank you for your comment. Reporting under the standard requires that the Registered Entity provide what information it has at the time of the report. The report may not provide the entire record or identification of the event. If the Registered Entity desires to submit an updated report, it may choose to do so; but there is no obligation to do so. Based upon comments received, the SDT has updated the time reporting requirements in Attachment 1. Most events are to be reported within 24 hours. The DSR SDT has retained a one-hour reporting requirement for those events the DSR SDT believes are the types of event that would be typically reported to law enforcement and are of a more urgent nature.		
SPP Standards Review Group	No	While the SDT has recognized the issue of applicability to GO/TO in its background information with the Unofficial Comment Form, we still do not feel comfortable with the GO/TO being listed as a responsible entity when in fact it may be days before they become aware of an event worthy of reporting. If the GOP/TOP makes the report, are the GO/TO still responsible for filing a report? If the GOP/TOP do not file the report, would the GO/TO then be non-compliant? This issue appears to put additional risk on the GO/TO over which they have no control. We need some mechanism to eliminate unnecessary risk while at the same time ensuring that we have coverage for the BES. Perhaps this could be done through delegation agreements between the entities involved or through allowances within the standard itself. For example, could the phrase "appropriate parties in the Interconnection" as currently contained in CIP-001-1, R2 be incorporated into the standard to basically replace GO/TO?
Response: The DSR SDT thanks you for your comment. The SDT believes that it has properly identified registered entities that may potentially have events and the appropriate types of events. A Registered Entity is only required to submit an events report for events listed in Attachment 1 if the registered entity was affected by the event. If an event occurs, only affected Registered Entities listed in Attachment 1 are required to submit a report on the event. Having reports from different entities for the same event may provide a more complete understanding of the event.		
FirstEnergy	No	1. Attachment 1, Part A - Energy Emergency requiring Public appeal for load reduction - In the current draft Standard, the applicability has been revised from an RC and BA to "initiating entity." We can't see where the GO/GOP would ever make this determination. Needs to be clarified.

Organization	Yes or No	Question 4 Comment
		2. Attachment 1, Part A - Energy Emergency requiring system-wide voltage reduction - In the current draft Standard, the applicability has been revised from an RC, TO, TOP, and DP to "initiating entity." We can't see where the GO/GOP would ever make this determination. Needs to be clarified. 3. Attachment 1, Part A - Voltage Deviations on BES facilities - A GOP may not be able to make the determination of a +/- 10% voltage deviation for ≥ 15 continuous minutes, this should be a TOP RC function only. 4. Attachment 1, Part A - Loss of offsite power (LOOP) classification should not apply to nuclear generators. The impact of a LOOP is dependent on the design of the specific nuclear unit and may not necessarily result in a unit trip. If a LOOP did result in a unit trip, the NRC requires notification by the nuclear GO/GOP via the Emergency Notification System (ENS), and time allowed for that notification (1 hour, 4 hours, 8 hour, or none at all) is, as mentioned above, dependent on the design of the plant. We believe it would be beneficial if consideration were given to coordinating reporting requirements for nuclear units with existing required notifications to the NRC to avoid duplication of effort. 5. Attachment 1 should align NERC Standard NUC-001 concerning the importance of ensuring nuclear plant safe operation and shutdown. If a transmission entity experiences an event that causes a loss of off-site power as defined in the nuclear generator's Nuclear Plant Interface Requirements, then the responsible transmission entity should report the event within 24 hours after occurrence. Also, for clarity "grid supply" should be replaced with "source" to ensure that notification occurs on a loss of one or multiple sources to a nuclear power plant. 6. Attachment 1, Part A - Damage or destruction of BES equipment. See Nuclear comments on question 17 below. 7. Attachment 1, Part B - Forced intrusion at a BES facility. See Nuclear comments on question 17 below. 8. Attachment 1, Part B - Risk to BES equipment from a non-environmental physical threat. What constitutes a "risk" to the reporting entity is still somewhat ambiguous, and although the DSR SDT has provided some examples, without more specific criteria for this event the affected entity will have difficulty in determining within 1 hour if a report is necessary. Also, see Nuclear comments on question 17 below.
Response: The DSR SDT thanks you for your comment. As a general note, the Applicability section of the standard includes each entity that will be responsible for reporting an event. Attachment 1 has a column "Entity with Reporting Responsibility" to indicate the appropriate entity that is required to report under this standard. For items 1-3 above, the GO or GOP will not be the likely deficient or initiating entity. This will most likely be the BA, TOP or the RC. For item 4, the LOOP event is to be reported by the TO and TOP, not the nuclear plant. For item 5, the TO and TOP are to report within 24 hours. The DSR discussed using "source", however this indicates a single source whereas "supply" encompasses all sources. For items 6, 7 and 8, please see response to Question 17 comments.		
SERC OC Standards Review Group	No	We agree that all of the entities listed should be responsible for reporting an event, provided they own BES assets, but guidance should be given for which entity in Attachment 1 actually files the report to avoid duplication for a single event.

Organization	Yes or No	Question 4 Comment
Response: The DSR SDT thanks you for your comment. The SDT believes that it has properly identified registered entities that may potentially have events and the appropriate types of events. A Registered Entity is only required to submit an events report for events listed in Attachment 1 if the registered entity was affected by the event. If an event occurs, only affected Registered Entities listed in Attachment 1 are required to submit a report on the event. Having reports from the different entities may provide valuable information on understanding the event.		
PJM Interconnection LLC	Yes	1. We agree that the entities listed should be responsible for ensuring events are reported, provided they own BES assets, but more guidance should be provided on which entity in Attachment 1 should actually file the report to avoid multiple entities reporting a single event. Current Attachment 1 results in significant duplicate reporting. 2. Although the applicable entities listed in Section 4 capture all entities that are assigned a reporting responsibility in Attachment 1, some events in Attachment 1 refer to entities applicable under a different standard (e.g CIP-002) as the responsible entities for reporting. This results in IA, TSP, and LSE (none of which, generally own Critical Assets and hence not likely own CCAs) as being responsible for reporting an event. We urge the SDT review the need to include IA, TSP, and LSE in applicable entities. Also, why is NERC an applicable entity in CIP-002-3 but not in this standard?
Response: Thank you for your comments. 1. The "Entity with Reporting Responsibility" column of Attachment 1 indicates who is responsible for submitting reports for each event type. It is expected that multiple reports will be received for the same event. Each entity experiencing the event may see something different. This reporting will allow for a more robust analysis process after the fact. 2. The IA. TSP and LSE are included as applicable entities for EOP-004 only because they are applicable under CIP-002. The only events that these entities are required to report are related to cyber assets. The ERO and the RE were added as applicable entities for consistency with CIP-002.		
SRP	No	The threshold for Reporting is broad, vague and repetitive. "Three or more BES Transmission Elements" is vague and could be interpreted as 3 breakers in a large system.
Response: The DSR SDT thanks you for your comment. Based upon comments received, the SDT has modified Attachment 1 accordingly.		
We Energies	No	Attachment 1: From the NERC Glossary, an Energy Emergency: A condition when a Load-Serving Entity has exhausted all other options and can no longer provide its customers' expected energy requirements. The first four events listed can only apply to an LSE. Loss of Firm Load for >15 Minutes: By the NERC Glossary definitions of DP and LSE, the LSE would seem to be more appropriate than the DP. With the proposed one-hour reporting requirement, the industry would be undertaking significant regulatory risk with respect to timely reporting. The requirement to report the crime-based events in the field within one

Organization	Yes or No	Question 4 Comment
		hour, as shown in Attachment 1 Part A or Part B will be difficult. We could even discover a theft in progress with the suspect trapped inside the substation fence and the police attempting to make a safe arrest. We need more reporting time, especially when they have not even resulted in an outage. The industry is keenly interested in understanding the benefit of taking on the risk. What analysis, insight, warnings or recommendations would the ES-ISAC provide to the reporting entity, the industry or to law enforcement agencies in the hours after such an incident is reported? Note too that DOE requires reporting of a physical attack within one hour only when it "causes a major interruption or major negative impact on critical infrastructure facilities or to operations." In lesser cases, the entity gets up to six hours if it "impacts electric power system reliability." DOE has said that it is not interested in copper theft unless it causes one of these events. If the SDT is working to ensure consistency of reporting requirements, please consider DOE requirements too. Meeting the reporting deadline will mean that available resources in the control center will be devoted to ensuring the report is filed on time instead of making the site safe and arranging for prompt repair. It may even mean that law enforcement won't be contacted until the forms are filed with the ES-ISAC. The exception contained in footnote #1 of Attachment 1 with respect to copper theft is not an exception at all. The majority of copper theft from substations is, in fact, such grounding connectors which may or may not render the protective relaying inoperative. You could end up receiving reports from all over the USA, Canada and Mexico, mostly on Monday mornings as weekend copper thefts are discovered. Attachment 1 Part A table also contains redundancies. One of the cells reads, "Damage or Destruction of Critical Asset." One cannot destroy something without damaging it first. Consequently, it is sufficient to simply say, "Damage to a Critical Asset." Apply to all cells with the same phrase.

Response: Thank you for your comments. Only Registered Entities affected by the event have to submit a report. Entities that were not affected by the event are under no obligation to submit a report. Registered Entities are to report what information they have at the submission timeline. The SDT recognizes that a final report may not be possible at the submission time. The reporting requirements are consistent with the current reporting requirements of the various authorities. The one hour reporting times are listed as "one hour within recognition of an event". This should be sufficient to allow the reporting entity time to submit the report after the event has been recognized. Based upon comments received from many stakeholders, the SDT has modified Attachment 1. The background section of the standard provides guidance with respect to reporting events to law enforcement. For clarity, the DSR SDT has added the following sentence to the first paragraph under the heading "Law Enforcement Reporting": "These are the types of events that should be reported to law enforcement." The entire paragraph is:

o "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES."

Organization	Yes or No	Question 4 Comment
Exelon	No	Remove LSE. As has been determined in previous filings, FERC has ruled that asset owning DP's must be registered as LSE's. The standard as proposed is applicable to DP's. This addresses any concern with a "reliability gap" for reporting events that could have an adverse material impact to the BES. See FERC Docket RC-07-4-003, -6-003, -7-003 paragraphs 24 and 25. "The Commission approves … revisions to the Registry Criteria to have registered distribution providers also register as the LSE for all load directly connected to their distribution facilities… The registration of the distribution provider as the LSE for all load directly connected to its distribution facilities is for the purpose of compliance with the Reliability Standards. As NERC explains, distribution providers have both the infrastructure and access to information to enable them to comply with the Reliability Standards that apply to LSEs… The Commission finds that, based on these facts, NERC acted reasonably in determining that the distribution provider is the most appropriate entity to register as the LSE for the load directly connected to its distribution facilities." Attachment 1, Part A – Energy Emergency requiring Public appeal for load reduction – In the current draft Standard, the applicability has been revised from an RC and BA to "initiating entity." As a GO/GOP, I cannot see any event where a GO/GOP would be the responsible "initiating entity" or have the ability to determine an "Energy Emergency." Suggest revising back to specific entities that would be likely responsible for this action (e.g., RC, BA, TOP). Attachment 1, Part A – Energy Emergency requiring system-wide voltage reduction – In the current draft Standard, the applicability has been revised from an RC, TO, TOP, and DP to "initiating entity." As a GO/GOP, I cannot see any event where a GO/GOP would be the responsible "initiating entity" or have the ability to determine an "Energy Emergency" related to system-wide voltage reduction. Suggest revising back to specific entities that would be likely responsible for this action. Attachment 1, Part A – Voltage Deviations on BES facilities - A GOP may not be able to make the determination of a +/- 10% voltage deviation for ≥ 15 continuous minutes, this should be a TOP RC function only. Attachment 1, Part A – Loss of off-site power (grid supply) affecting a nuclear generating station – this event applicability should be removed in its entirety for a Nuclear Plant Generator Operator. The impact of loss of off-site power on a nuclear generation unit is dependent on the specific plant design, if it is a partial loss of off-site power (per the plant specific NPIRs) and may not result in a loss of generation (i.e., unit trip). If a loss of off-site power were to result in a unit trip, an Emergency Notification System (ENS) would be required to the Nuclear Regulatory Commission (NRC). Depending on the unit design, the notification to the NRC may be 1 hour, 8 hours or none at all. Consideration should be given to coordinating such reporting with existing required notifications to the NRC as to not duplicate effort or add unnecessary burden on the part of a Nuclear Plant Generator Operator during a potential transient on the unit. In addition, if the loss of off-site power were to result in a unit trip, if the impact to the BES were ≥2,000 MW, then required notifications would be made in accordance with the threshold for reporting for Attachment 1, Part A – Generation Loss. However, to align with the importance of ensuring nuclear plant safe operation and shutdown as implemented in NERC Standard NUC-001, if a transmission entity experiences an event that causes an unplanned loss of off-site power (source) as defined in the applicable Nuclear Plant Interface Requirements, then the responsible

Organization	Yes or No	Question 4 Comment
		transmission entity should report the event within 24 hours after occurrence. In addition, replace the words "grid supply" to "source" to ensure that notification occurs on an unplanned loss of one or multiple sources to a nuclear power plant. Suggest rewording as follows (including replacing the words "grid supply" to "source" and adding in the word "unplanned" to eliminate unnecessary reporting of planned maintenance activities in the table below): Event Entity with Reporting Responsibility Threshold for Reporting Time to Submit Report Unplanned loss of off-site power to a Nuclear generating plant (source) as defined in the applicable Nuclear Plant Interface Requirements (NPIRs) Each transmission entity responsible for providing services related to NPIRs (e.g., RC, BA, TO, TOP, TO, GO, GOP) that experiences the event causing an unplanned loss of off-site power (source) Unplanned loss of off-site power (source) to a Nuclear Power Plant as defined in the applicable NPIRs. Within 24 hours after occurrence
Response: Thank you for your comments. The SDT constructed Attachment 1 based upon the existing requirements in the various reliability standards and established reporting obligations. The LSE is an applicable entity under CIP-002 and CIP-008. The types of events that you list are not applicable to a GO/GOP. The Applicability section of the standard lists each entity that is applicable for some portion of the standard. The information in Attachment 1 specifies which entity must report for which type of event. The loss of off-site power is only applicable to the TO and TOP and not the nuclear plant operator.		
SDG&E	No	SDG&E recommends that “Load Serving Entity,” “Transmission Service Provider,” and “Interchange Authority” be removed from the proposed applicability shown in Section 4. These entities do not own assets that could have an impact on the Bulk Electric System. Additionally, none of these entities is listed as an “Entity with Reporting Responsibility” in Attachment 1. Finally, “Transmission Service Provider” is covered by either “Transmission Owner” or “Balancing Authority,” which are entities also listed in the proposed Applicability section, and “Load Service Entity” and “Interchange Authority” are covered by “Balancing Authority.”
Response: Thank you for your comments. The SDT constructed Attachment 1 based upon the existing requirements in the various reliability standards and established reporting obligations. The LSE, TSP and IC are applicable entities under CIP-002 and CIP-008.		
United Illuminating Co	No	Will an entity be required to develop an Operating Process for every Impact Event in Attachment 1, or only those events that apply to its Registration. For example, does a DP require evidence of an Operating Process/Procedure for Voltage Deviations on a BES Facility? Some items in Attachment 1 state “Each RC, BA, TOP, DP that experiences the Impact Event” (such as Loss of Firm Load). DP’s may have arranged with TOP and RC to communicate the event to TOP who then will file the NERC report and OE-417. The requirements in the Standard would allow for this as long as the Operating Plan documents it. Attachment 1 though can be interpreted that this arrangement would not be allowed and each entity shall file its own and separate report. UI suggests that Attachment 1 be modified to allow for an Entities Operating Plan to rely on another Entity making the final communication to NERC. “Each RC, BA, TOP, DP that experiences the Impact Event, either individually or combined on a single filing”

Organization	Yes or No	Question 4 Comment
Response: The DSR SDT thanks you for your comment. The SDT believes that it is not necessary to develop a separate Operating Process for each event, unless the company requires it. The SDT feels that any Registered Entity affected by an event needs to submit a report. The SDT believes that the Registered Entity can utilize any resource it has available to complete the reporting obligations and does not believe that Attachment 1 inhibits any options from being used. Based upon comments received, the SDT has decided to remove the definition of Impact Event from the standard and leave as identified through Attachment 1.		
American Municipal Power	No	No, I do not agree. The DP and LSE functions should be removed.
Response: The DSR SDT thanks you for your comment. The SDT constructed Attachment based upon the existing requirements in the various reliability standards and established reporting obligations. This information will be useful to all owners, operators, and users of the bulk power system. The DP and LSE are applicable entities under CIP-002 and CIP-008.		
Sweeny Cogeneration LP	No	In Attachment 1, Generator Operators who experience a ± 10% sustained voltage deviation for ≥ 15 continuous must issue a report For externally driven events, the GOP will have little if any knowledge of the cause or remedies taken to address it. We believe the language presently in EOP-004-1 is satisfactory that any "action taken by a Generator Operator" that results in a voltage deviation has to be reported by the GOP.
Response: Thank you for your comment. Reporting of events is an obligation of affected Registered Entities. Registered Entities who do not experience an event do not have any reporting obligations.		
Independent Electricity System Operator	No	We disagree with the following inclusion/exclusion of several entities: a. We assess that the applicable entities listed in Section 4 capture all the entities that are assigned a reporting responsibility in Attachment 1 of the standard. While some events in Attachment 1 have specific entities identified as responsible for reporting, certain events refer to the entities listed in specific standards (e.g. CIP-002) as the responsible entities for reporting. The latter results in IA, TSP and LSE (none of which being specifically identified as having a reporting responsibility) being included in the Applicability Section. If our reasoning is correct, we question why NERC was dropped from the Applicability Section as it is an applicable entity identified in CIP-002-3. b. If the above approach was not strictly followed, then we'd suggest the SDT review the need to include IA, TSP and LSE since they generally do not own any Critical Assets and hence will likely not own any Critical Cyber Assets.
Response: The DSR SDT thanks you for your comment. The SDT believes it needs to follow the requirements of the standards as they currently apply. Since these entities are applicable to the underlying standards identified in Attachment 1, they will be subject to reporting. If those standards are modified to remove the applicability to these functional registrations, then the appropriate SDT can modify the applicability of this standard. The SDT has reviewed the CIP-002-3		

Organization	Yes or No	Question 4 Comment
standard and have added the ERO and the RE as applicable entities. If an IA, TSP or LSE does not own Critical Assets nor Critical Cyber Assets, then they will have nothing to report under this standard.		
Ameren	No	The 1 hour reporting requirement, as reference in Attachment 1 is inappropriate. In the event an "Impact Event" were to be discovered the Responsible Entity should focus on public and personnel safety. The reporting requirement should read "Within 1 hour or as soon as conditions are deemed to be safe." This statement would be applicable to "Damage or destruction of Critical Asset" The SDT should not put personnel in the position of choosing to either comply with NERC or address public or co-worker safety. The Time to Submit Report states "within 1 hour after occurrence is identified" This gives an auditor a wide area to question. If personnel report the occurrence 1 hour after identified, but 24 hours after it occurred, we are subject to the personal beliefs of the auditor that the event was not identified 24 hours ago, and reported 24 hours late. This will also be difficult to measure as the operator will have to document in the plant log the time the event was identified, while possibly dealing with Emergency Conditions. In the Note above the Actual Reliability Impact Table, the SDT identifies that under certain conditions, NERC / RRO staff may not be available for continuous 24 hour reporting. The SDT should consider the same stipulations apply to operating personnel and they should not be held to a higher standard that NERC / RRO.
Response: Thank you for your comment. The reporting timelines for most events have been changed from 1 hour to 24 hours. The events that retain the one hour requirement are those that are more closely related to sabotage type events. The DSR SDT chose the wording “upon identification of an event” to allow for cases where an event may not be recognized for some time due to an asset being in a remote location for example. It is expected that an auditor will follow what is written in the standard rather their personal preference. In the note above Attachment 1, it does not state that the ERO may not be available. This note is related to R3.3 of EOP_004-1 and provides for delayed reporting by an entity during storms or other such instances.		
ISO New England, Inc	No	We disagree with the following inclusion/exclusion of several entities: a. We acknowledge that the applicable entities listed in Section 4 capture all the entities that are assigned a reporting responsibility in Attachment 1 of the standard. While some events in Attachment 1 have specific entities identified as responsible for reporting, certain events refer to the entities listed in specific standards (e.g. CIP-002) as the responsible entities for reporting. The latter results in IA, TSP and LSE (none of which being specifically identified as having a reporting responsibility) being included in the Applicability Section. If our reasoning is correct, we question why NERC was dropped from the Applicability Section as it is an applicable entity identified in CIP-002-3. b. If the above approach was not strictly followed, then we’d suggest the SDT review the need to include IA, TSP and LSE since they generally do not own any Critical Assets and hence will likely not own any Critical Cyber Assets. c. There is still significant duplicate reporting included. For instance, why do both the RC and TOP to report

Organization	Yes or No	Question 4 Comment
		voltage deviations? As written, a voltage deviation on the BES would require both to report. The same would hold true for IROLs. Perhaps IROLs should only be reported by the RC to be consistent with the recently FERC approved Interconnection Reliability Operating Limit standards.
Response: The DSR SDT thanks you for your comment. (a) The SDT believes it needs to follow the requirements of the standards as they currently apply. Since these entities are applicable to the underlying standards identified in Attachment 1, then they will be subject to reporting. If those standards are modified to remove the applicability to these functional registrations, then the appropriate SDT can modify the applicability of this standard. The SDT has reviewed the CIP-002-3 standard and have added the ERO and the RE as applicable entities. (b) The IA, TSP and LSE are included in the Applicability only as it relates to CIP-002 events listed in the table. (c) The DSR SDT has removed the RC from "Voltage Deviations" and the TOP from the IROL to address the comment.		
Calpine Corp	No	Expanding the current applicability of CIP-001-1 and EOP-004-1 to the GO function is unnecessary and will result in numerous duplicate reports, self-certifications, spot checks, and audits reviews, with no benefit to the reliability of the Bulk Electric System. The GOP is the appropriate applicable entity for generation facilities.
Response: The DSR SDT thanks you for your comment. The SDT believes that it has properly identified registered entities that may potentially have events and the appropriate types of events. A Registered Entity is only required to submit an events report for events listed in Attachment 1 if the registered entity was affected by the event. If an event occurs, only affected Registered Entities listed in Attachment 1 are required to submit a report on the event. Having reports from the different entities may provide valuable information on understanding the event. The SDT would like to point out that reporting of events is from the time of identification not the time of the event.		
Occidental Power Marketing	No	Load Serving Entities that do not own or operate BES assets (or assets that support the BES) should not be included in the Applicability. The SDT includes LSEs based on CIP-002; however, if the LSE does not have any BES assets (or assets that support the BES), CIP-002 should also not be applicable because the LSE could not have any Critical Assets or Critical Cyber Assets. It is understood that the SDT is trying to comply with FERC Order 693, Sections 460 and 461; however, Section 461 also states: "Further, when addressing such applicability issues, the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate to address these concerns." A qualifier in the Applicability of EOP-004-2 that would include only LSEs that own, operate or control BES assets (or assets that support the BES) would seem appropriate and acceptable to FERC.
Response: The DSR SDT thanks you for your comment. The SDT believes it needs to follow the requirements of the standards as they currently apply. Since these entities are applicable to the underlying standards identified in Attachment 1, then they will be subject to reporting. The LSE is an applicable entity under CIP-002 and CIP-008. If those standards are modified to remove the applicability to these functional registrations, then the appropriate SDT can modify the applicability of this standard.		

Organization	Yes or No	Question 4 Comment
American Transmission Company	No	First, under Part A, the reporting requirement for three or more BES Transmission Elements will create confusion. The NERC definition for an Element is: "Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An element may be comprised of one or more components." This could be interpreted to be three potential transformers on a bus section; therefore, any bus section would require a report. It is suggested that this be reworded to indicate three or more BES transmission lines, bus sections, or transformers. Second, under Part A, the reporting requirement for "Damage or destruction of BES equipment" is too broad and needs to be modified. For example, an output contact on a relay could be damaged unintentionally during routine testing resulting in a reportable event. It is suggested that the list of BES equipment and full intent of this be further defined in the footnote. The intent needs to be clarified, such as "events that have an immediate and significant impact to the stability or reliability of the BES." Third, under Part A, the reporting requirement for "Damage or destruction of a Critical Cyber Asset" is too broad and needs to be modified. For example, an output contact on a relay could be damaged unintentionally during routine testing resulting in a reportable event.
Response: Thank you for your comments. (1) The event "Transmission Loss" has been modified to remove the word Element. This now refers to Facilities. 2. If damage to a contact on a relay poses a reliability threat, then it should be reported. There is a footnote for this the type of event that helps clarify what is expected to be reported. It states: 1 BES equipment that: i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii) Damaged or destroyed due to intentional or unintentional human action which removes the BES equipment from service. Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative). 3. This relates only to Critical Cyber Assets identified under CIP-002. If a relay contact is identified under CIP-002 as a Critical Cyber Asset, then its damage or destruction should be reported.		
Ingleside Cogeneration LP	No	Owners and operators of facilities whose total removal from the BES would not meet any reportable threshold under Attachment 1 should not have to create and maintain Operating documents. The same would be true of any LSE, TSP, or IA that does not oversee any Critical Cyber Assets as identified under CIP-002. A statement to that effect could be made in Section 4 of EOP-004-2.
Response: Thank you for your comments. Requirements under Standards can only be enforced against Registered Entities, not whether or not they own or operate certain types of assets. The SDT believes it needs to follow the requirements of the standards as they currently apply. Since these entities are applicable to the underlying standards identified in Attachment 1, then they will be subject to reporting. If those standards are modified to remove the applicability to these		

Organization	Yes or No	Question 4 Comment
functional registrations, then the appropriate SDT can modify the applicability of this standard.		
Duke Energy	No	Section 4 is fine, but on Attachment 1, Entity with Reporting Responsibility should just identify "Initiating entity" for every Event, as was done with the first three Events. That way you avoid errors in leaving an entity off, or including an entity incorrectly (as was done with the GOP on Voltage Deviations).
Response: Thank you for comment. The SDT considered your comment in the development of Attachment 1 decided against including the Initiating Entity designation as it was not appropriate in those cases. Based upon comments received, the SDT has modified Attachment 1 accordingly.		
Constellation Power Generation	No	As stated in comments to earlier versions of EOP-004-2, CPG disagrees with the inclusion of Generator Owners. Since one of the goals in revising this standard is to streamline impact event reporting obligations, Generator Operators are the appropriate entity to manage event reporting as the entity most aware of events should they arise. At times, the information required to complete a report may warrant input from entities connected to generation, but the generator operator remains the best entity to fulfill the reporting obligation.
Response: Thank you for your comment. The SDT has chosen not to distinguish between Registered Entities as far as reporting. Instead the SDT has included Registered Entities which are involved or potentially involved in the types of events. Registered Entities need to recognize that only entities that are affected by the event have the reporting obligation.		
Georgia System Operations Corporation	No	We do not agree that this standard assigns clear responsibility for reporting. It seems that multiple entities are being required to report the same event for some events. Only one entity should report. See comments later regarding Attachment 1. NERC should not decide which ONE entity should report. The entities should be allowed to decide this (and include it in the Impact Event Operating Plan) and to let NERC or the region know who will report (or give them a copy of the plan).
Response: Thank you for your comment. The SDT has chosen not to distinguish between Registered Entities as far as reporting. Instead the SDT has included Registered Entities which are involved or potentially involved in the types of events. Registered Entities need to recognize that only entities that are affected by the event have the reporting obligation.		
Indeck Energy Services	No	Voltage Deviations should not be reportable by GOP. That's why we have TOP's. Damage or destruction of BES equipment should be reportable only if it causes or could cause a Reportable Disturbance, reportable DOE OE-417 event or sabotage (as defined above). Otherwise, an auditor could require reporting of a relay failure caused by human error even though the relay was in test mode and no BES impact was experienced. This category could be dropped in favor of the next one, damage to Critical Asset. Fuel Supply Emergency needs a definition. For natural gas, various conditions could be referred to as

Organization	Yes or No	Question 4 Comment
		emergencies, but unless they actually affect generation, they should not need to be reported. Fuel Supply Emergencies that cause a Reportable Disturbance or reportable DOE OE-417 event should be reported. It is unclear why Forced Intrusion should be reportable under EOP-004. If it causes a problem, it will be reportable as another category and is one more unpreventable event. Forced Intrusion isn't, in many cases, as the exceptions try to define, an impact event at all, but could be a cause, which would be reported as the cause of an impact event. Risk to BES Equipment is not well defined. It should be expanded to Risk to BES Equipment from a non-environmental physical threat within a reasonable distance of the Equipment. A train derailment on the line past the plant would likely be known, whereas one that was 1/2 mile or more away with flammable materials might not be known about unless a public warning was made.
Response: The DSR SDT thanks you for your comment. Voltage Deviation reporting no longer applies to the GOP. There is a footnote on Damage or Destruction to BES equipment that addresses your comment. It states: [1]BES equipment that: i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii) Damaged or destroyed due to intentional or unintentional human action which removes the BES equipment from service. Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative). Fuel Supply Emergency has been removed from Attachment 1. Forced Intrusion is an event could be related to sabotage. Identification and reporting of such events may help identify trends. The footnote associated with Risk TO BES Equipment addresses your comment: Examples include a train derailment adjacent to BES equipment that either could have damaged the equipment directly or has the potential to damage the equipment (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center) and report of suspicious device near BES equipment.		
Brazos Electric Power Cooperative	No	Inclusion of LSE and DP is questionable.
Response: The DSR SDT thanks you for your comment. The SDT believes that it has properly identified registered entities that may potentially have events and the appropriate types of events. A Registered Entity is only required to submit an events report for events listed in Attachment 1 if the registered entity was affected by the event. The LSE and DP are applicable entities under CIP-002 and CIP-008. If an event occurs, only affected Registered Entities listed in Attachment 1 are required to submit a report on the event. Having reports from the different entities may provide valuable information on understanding the event. The SDT would like to point out that reporting of events is from the time of identification not the time of the event.		

Organization	Yes or No	Question 4 Comment
Manitoba Hydro	Yes	All registered entities are included. This means all field and office personal involved will create a 360 degree view of the BES, and fulfill "Situational awareness of the industry." In Attachment 1, the "Entity with Reporting Responsibility" entities vary. It might be clearer to leave all impact levels "Entity with Reporting Responsibility" as the RC, BA and TOP, as these are likely the only parties that will report as required. All other entities must report to the RC, BA and TOP.
Response: Thank you for your comment. The SDT had previously considered a hierarchal approach to report; however, this concept was rejected by the industry.		
American Electric Power	Yes	AEP agrees, but it further supports the notion that this standard should not apply to the IA, TSP, and LSE functions.
Response: The DSR SDT thanks you for your comment. The SDT constructed Attachment based upon the existing requirements in the various reliability standards and established reporting obligations. The LSE, TSP and IC are applicable entities under CIP-002 and CIP-008. The information about an event will be useful to all owners, operators, and users of the bulk power system.		
Southern Company	Yes	This will cause the duplication of reporting for some events. Reference EOP-004 Attachment 1: Impact Events Table; Event - Loss of Firm Load for ≥ 15 minutes (page 15 of standard) This requires the RC, BA, TOP, and DP to report. So if a storm front goes through our system and takes out 400MW of load in Alabama and Georgia the PCC would have to report as the RC, BA, and TOP. Alabama Power and Georgia Power would also have to report as DPs. The way it is now the PCC reports for any of these events.
Response: The DSR SDT thanks you for your comment. The SDT believes that it has properly identified registered entities that may potentially have events and the appropriate types of events. A Registered Entity is only required to submit an events report for events listed in Attachment 1 if the registered entity was affected by the event. If an event occurs, only affected Registered Entities listed in Attachment 1 are required to submit a report on the event. Having reports from the different entities for the same event may provide a more complete understanding of the event.		
Pepco Holdings Inc and Affiliates	Yes	More guidance is needed for which entity in Attachment 1 actually files the report to avoid duplicate filing.
Response: The DSR SDT thanks you for your comment. The SDT believes that it has properly identified registered entities that may potentially have events and the appropriate types of events. A Registered Entity is only required to submit an events report for events listed in Attachment 1 if the registered entity was affected by the event. If an event occurs, only affected Registered Entities listed in Attachment 1 are required to submit a report on the event. Having reports		

Organization	Yes or No	Question 4 Comment
from different entities for the same event may provide a more complete understanding of the event.		
Midwest ISO Standards Collaborators	Yes	
Bonneville Power Administration	Yes	
Midwest Reliability Organization	Yes	
Western Electricity Coordinating Council	Yes	
PPL Supply	Yes	
City of Tallahassee (TAL)	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
Liberty Electric Power LLC	Yes	
Arkansas Electric Cooperative Corporation	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Platte River Power Authority	Yes	
BGE	Yes	No comments.
Alliant Energy	Yes	

Organization	Yes or No	Question 4 Comment
ExxonMobil Research and Engineering	Yes	
PPL Electric Utilities	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	
Progress Energy	Yes	
Response: The DSR SDT thanks you for your comment. Several commenters provided suggestions that led to modifications of Attachment 1.		

5. Stakeholders suggested removing original Requirements 1, 7 and 8 from the standard and addressing the reliability concepts in the NERC Rules of Procedure. Do you agree with the removal of original requirements 1, 7 and 8 (which were assigned to the ERO) and the proposed language for the Rules of Procedure (Paragraph 812)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: Most commenters agreed with the removal of R1, R7 and R8. The SDT has provided suggested language to NERC for inclusion into the Rules of Procedure.

Organization	Yes or No	Question 5 Comment
Midwest ISO Standards Collaborators	No	We see no issue with imposing requirements on NERC. However, we are not opposed to making these changes in the Rules of Procedure either.
Response: Thank you for your comments. We are pursuing changes to the Rules of Procedure.		
SERC OC Standards Review Group	No	We agree that the ERO should not have requirements applicable to them, but disagree with changing or revising the Rules of Procedure (ROP) giving this reporting responsibility solely to NERC. This responsibility may be performed by NERC but other learning organizations should also be considered for performing this responsibility. In addition, the proposed wording of the revision to the ROP appears to place the responsibility of notifying the appropriate law enforcement with NERC rather than with the local responsible entity.
Response: Thank you for your comments. The responsibility for notifying law enforcement remains with the entity and has been clarified in Attachment 1.		
PJM Interconnection LLC	No	We agree that the standard should not have requirements applicable to the ERO, but disagree with revising the NERC Rules of Procedure (RoP) to include suggested Section 812. The reporting responsibility should not be solely given to NERC. Other learning organizations must also be considered for performing this responsibility. Additionally, the proposed wording of Section 812 appears to imply that NERC will notify the appropriate law enforcement agencies as opposed to the local responsible entity.
Response: Thank you for your comments. The responsibility for notifying law enforcement remains with the entity and has been clarified in Attachment 1.		
SDG&E	No	SDG&E agrees with removing original Requirements 1, 7, 8 from the standard. In addition, SDG&E recommends that the standard reference Section 812 of the Rules of Procedure.

Organization	Yes or No	Question 5 Comment
Response: Thank you for your comments.		
Duke Energy	No	Proposed language for Section 812 is very confusing. Is the NERC "system" really going to perform all notifications: "applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, and regulatory agencies as necessary?" Is it intended that the NERC "system" will relieve registered entities of the obligation to make these other reports? Is there an implementation plan to achieve that objective? It appears that this current version of EOP-004-2 has the potential for significantly creating redundant reporting. Will the NERC reports be protected from FOIA disclosure? How will FERC Order 630 be followed (CEII disclosure)?
Response: Thank you for your comments. The SDT expects any system would facilitate the reporting to organizations specified in the submitted report. Until such time that the system can be established, the Registered Entity will be obligated to make the notifications as specified in its Operating Plan(s). The SDT has proposed an amendment to the NERC Rules of Procedure to assist in the development of a single reporting process for all three obligations.		
ExxonMobil Research and Engineering	No	Abstain from commenting on this question.
Brazos Electric Power Cooperative	No	
Ingleside Cogeneration LP	Yes	Ingleside Cogeneration agrees that the NERC Rules of Procedure are the appropriate location for ERO assigned activities. However, we would like to get a solid commitment from NERC that the Events Analysis Process and the Reliability Assessment and Performance Analysis Group (RAPA) data analysis requirements for Protection System Misoperations is coordinated through a single process. Their unique data needs are understandable, but should not require the downstream entity to evaluate what is required by each sub-committee - and which reporting template to use.
Response: Thank you for your comments. Your comment addresses a concern that is beyond the scope of this project and cannot be addressed here. The SDT has communicated with the NERC Events Analysis Working Group and DOE in efforts to develop a single reporting process. The SDT will continue to work with those organizations to complete this task.		
Northeast Power Coordinating Council	Yes	Agree with the proposed removal, but have not assessed the proposed language for RoP para. 812 because unable to access it (not on the RoP page).
Response: Thank you for your comments.		

Organization	Yes or No	Question 5 Comment
Bonneville Power Administration	Yes	Ensure distribution of trends.
Response: Thank you for your comments.		
Midwest Reliability Organization	Yes	The ERO is not a user, owner or operator of the BES and the best place to contain their responsibilities, is in the Rules of Procedure.
Response: Thank you for your comments.		
Pepco Holdings Inc and Affiliates	Yes	Agree that NERC should not have requirements applicable to them.
Response: Thank you for your comments.		
American Municipal Power	Yes	A software solution may provide an easy expansion for reporting EOP-004, CIP-001, and additional standards.
Response: Thank you for your comments.		
Manitoba Hydro	Yes	Agree with R1, a central system for receiving and distributing reports. There is limited time and resources for control operators to follow up and ensure ALL required entities have received all information required in a timely manner. Agree with R7 and R8.
Response: Thank you for your comments.		
Sweeny Cogeneration LP	Yes	We agree that these requirements appropriately belong in the NERC Rules of Procedure. However, we are concerned with the multiple reporting requirements being driven by EOP-004-2, CIP-008-3, the ERO Events Analysis Team, the Reliability Assessment and Performance Analysis Group (RAPA). It is imperative that these efforts be consolidated into a single procedure using a single reporting template.
Response: Thank you for your comments. The DSR SDT agrees with the concept of the single reporting template and is working with other agencies to see if the single form would be achievable.		
Western Electricity Coordinating Council	Yes	

Organization	Yes or No	Question 5 Comment
PPL Supply	Yes	
Pacific Northwest Small Public Power Utility Comment Group	Yes	
PSEG Companies	Yes	
Dominion	Yes	
SPP Standards Review Group	Yes	
FirstEnergy	Yes	
Southern Company	Yes	
SRP	Yes	
We Energies	Yes	
Compliance & Responsiblity Organization	Yes	
Exelon	Yes	
City of Tallahassee (TAL)	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
United Illuminating Co	Yes	
Liberty Electric Power LLC	Yes	

Organization	Yes or No	Question 5 Comment
Arkansas Electric Cooperative Corporation	Yes	
American Electric Power	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Independent Electricity System Operator	Yes	
ISO New England, Inc	Yes	
Platte River Power Authority	Yes	
Calpine Corp	Yes	
BGE	Yes	No comments.
Alliant Energy	Yes	
CenterPoint Energy	Yes	
PPL Electric Utilities	Yes	
Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
American Transmission Company	Yes	

Organization	Yes or No	Question 5 Comment
Constellation Power Generation	Yes	
Georgia System Operations Corporation	Yes	None.
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	
Indeck Energy Services	Yes	
Progress Energy	Yes	

6. Do you agree with the proposed revisions to Requirement 2 (now R1) including the use of defined terms Operating Plan, Operating Process and Operating Procedure? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: Stakeholders were fairly evenly divided on this question. Overall, there appears to be a misconception on what is and isn't included in the Operating Plan(s). The SDT believes that current Sabotage Reporting substantially meets the requirements outlined in the standard, albeit there may be some needed alterations to accommodate the new standard. The updated subrequirement is a result of a FERC directive in Order No. 693. The DSR SDT removed references to Operating Process and Operating Procedure and revised the Requirement to:

R1. Each Responsible Entity shall have an Operating Plan that includes: [Violation Risk: Factor: Lower] [Time Horizon: Operations Planning]

1.1. A process for identifying events listed in Attachment 1.

1.2. A process for gathering information for Attachment 2 regarding events listed in Attachment 1.

1.3. A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate:

- Internal company personnel
- The Responsible Entity's Regional Entity
- Law enforcement
- Governmental or provincial agencies

1.4. Provision(s) for updating the Operating Plan within 90 calendar days of any change in assets, personnel, other circumstances that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to R3.

1.5. A Process for ensuring the responsible entity reviews the Operating Plan at least annually (once each calendar year) with no more than 15 months between reviews.

Organization	Yes or No	Question 6 Comment
Georgia Transmission Corporation & Oglethorpe Power	No	The terms "Operating Procedure, Operating Plan, and Operating Process," while included in the NERC glossary, are not consistently used throughout the body of NERC standards as they are used in R1 of EOP-

Organization	Yes or No	Question 6 Comment
Corporation		004-2. As such, we do not see a reliability benefit in using the defined terms over the more commonly used terms of simply "plans, processes, and procedures." In part 1.1 of R1, we think that the requirement should clearly indicate that a particular Responsible Entity's Impact Event Plan should only be required to include those particular Impact Events for which the Responsible Entity has the reporting obligation. Therefore, we suggest the following modification to R1: "1.1 An Operating Process for identifying Impact Events listed in Attachment 1 for those Impact Events where the Responsible Entity is identified as having the reporting responsibility." Additionally, in part 1.3 of R1, we believe the language to be vague and will introduce the need for further clarification either through an interpretation or the CAN process in part because the verb tenses of the sub-sub-requirements do not agree and it appears to require notification to all listed parties for every Impact Event instead of only those that make sense for a particular event. As such, we suggest adding a column to the tables in Attachment 1 that identifies precisely which organizations should be notified in the case of a particular Impact Event and modifying part 1.3.2 to read: "1.3.2 External organizations to notify as specified in Attachment 1." Currently, as written, the standard could be interpreted to require notification to law enforcement for an IROL violation, for instance. Furthermore, we are concerned that as written, the standard may require that the same event must be reported by multiple responsible entities. Our current process uses notification between Responsible Entities (i.e. from a TO to a TOP and then from the TOP to NERC) to allow for a centralized and coordinated notification to law enforcement, NERC, etc. We are concerned that the requirement as written does not appear to allow this flexibility and may require both the TO and TOP to report the same event in order to prove compliance with the Standard.
Response: Thank you for your comments. The SDT believes that in order for a term to become consistent with the body of the reliability standards, each SDT will have to incorporate the terms as the opportunity to revise each standard arises. The SDT envisions that each Registered Entity will develop Operating Plan(s) appropriate to meet its obligations as outlined in the standard. Part 1.3 has been revised to indicate that each report must be sent to the ERO and the Registered Entity's Reliability Coordinator and the remaining entities as appropriate. Law Enforcement would certainly not be interested in an IROL violation, but they would be interested in Forced Intrusion.		
Bonneville Power Administration	No	Not sure that a 90-day update is needed to be sent to CEF.
Response: Thank you for your comments. That is not required in the standard. The SDT believes that it is unnecessary to forward any update to any organization outside of the Registered Entity. Updates should be used to inform internal personnel of any Operating Plan changes.		

Organization	Yes or No	Question 6 Comment
Pacific Northwest Small Public Power Utility Comment Group	No	1.4 makes no sense. The operating plan update and the change to its content occur simultaneously. Perhaps the SDT meant to say "Provision(s) for updating the Impact Event Operating Plan within 90 days of identification of a needed change to its content. This would be consistent with the "lessons learned" language of the prior version.
Response: Thank you for your comment. The DSR SDT added additional detail to Part 1.4 to address the broader term "content."		
PSEG Companies	No	The PSEG Companies believe that sections 1.3 and 1.3.2 will require notification of law enforcement agencies for all Impact Events defined in Attachment 1. This is appropriate for some events if there has been destruction to BES equipment, for example, but not in certain operational events. It should not be necessary to notify law enforcement that a non sabotage event like an IROL violation, generation loss or voltage deviation has occurred.
Response: Thank you for your comments. The DSR SDT feels that the Registered Entity will establish Operating Plan(s) appropriate for its needs including the specification of how and when law enforcement agencies are contacted. Part 1.3 has been revised to indicate that each report must be sent to the ERO and the Registered Entity's Reliability Coordinator and the remaining entities as appropriate. Law Enforcement would certainly not be interested in an IROL violation, but they would be interested in Forced Intrusion. Attachment 1 language has been updated to say "The parties identified..." which should be included in the entity's Operating Plan(s).		
Dominion	No	The requirement for Responsible Entities to establish an Impact Event Operating Plan, Operating Process, and Operating Procedure seems overly cumbersome and prescriptive. The use of these NERC defined terms create additional compliance burden for little, if any, improvement to reliability. Suggest simplification by requiring the Responsible Entities to have a procedure to report Impact Events, to the appropriate parties, pursuant to EOP-004. In addition, we request clarification of R1.4. It seems circular to us in that it requires the plan to be updated within 90 days of when it changes. Is the intent that any necessary changes identified in the annual review required by R4 be incorporated in a revision to the plan within 90 days of the review? If so, R1.4 belongs under R4. If not, we do not understand the requirement. What starts the 90 day count down?
Response: Thank you for your comment. The language in Requirement R1, Part 1.4 was inserted in response to a directive in FERC Order 693. The SDT feels that the directive requires Registered Entities to update their Operating Plan(s) within 90 days of the time the entity identified the need for the change, such as a new telephone number, personnel staff name/title, or addition/deletion of person or organization. The DSR SDT has made changes to better clarify "content."		

Organization	Yes or No	Question 6 Comment
Pepco Holdings Inc and Affiliates	No	An Operating Plan, Operating Process or Operating Procedure implies something different than an after the fact reporting activity.
Response: Thank you for your comment. An Operating Plan is more than an after the fact reporting activity. The Operating Plan(s) incorporates the tasks or steps involved in the identification of events, establishing which internal personnel are to be involved in the communications and or reporting, and establishing the list of outside organizations to be contacted when an event happens.		
SPP Standards Review Group	No	We would suggest rewording Part 1.3.2 to read "External organizations to notify may include but are not limited to the Responsible Entity's Reliability Coordinator, NERC, Responsible Entity's Regional Entity, Law Enforcement and Governmental or Provincial Agencies." We would also suggest the following for Part 1.4: "Provision(s) for updating the Impact Event Operating Plan within 90 days of any known changes to its content." Would also suggest adding "as requested" at the end of M1.
Response: Thank you for your comments. (1) Requirement R1, Part 1.3 has been updated to "as appropriate" to address the parties to communicate event to. (2) The SDT agrees with your suggestions and has made similar word changes. 3) Agreed.		
Midwest ISO Standards Collaborators	No	We do not believe that the use of the Operating Process, Operating Procedure, and Operating Plan for a reporting requirement is consistent with their definitions and certainly not with the intent of the definitions. For instance, an Operating Process is intended to meet an operating goal. What operating goal does this requirement meet? An Operating Procedure includes tasks that must be completed by "specific operating positions." This reporting requirement could be met by back office personnel. We also believe that parts 1.3 and 1.3.2 under Requirement 1 will require notification of law enforcement agencies for all Impact Events defined in Attachment 1. While some should require notification to law enforcement such as when firm load is shed, others certainly would not. For instance, law enforcement does not need to know that an IROL violation, generation loss or voltage deviation occurred.
Response: Thank you for your comments. The Glossary Definition of Operating Plan is: A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan. The definition uses "goal" rather than "operating goal". The goal of the Operating Plan is to ensure that entities know how to identify the events listed in		

Organization	Yes or No	Question 6 Comment
Attachment 1 and report them to the appropriate parties. The SDT disagrees with your views on Operating Process, Operating Procedure, and Operating Plan. The SDT appropriately describes the task at hand. The SDT feels that the Operating Plan can identify when law enforcement agencies need to be notified without specification from the SDT. The Background section of the standard contains a heading for "Law Enforcement" and provides clarification regarding the types of events that should be reported to law enforcement.		
FirstEnergy	No	1. We believe that the use of stringent definitions for an entity's process requires too much of the "how" instead of the "what." As long as the entity has a process, procedure (or whatever they want to call it) that includes the necessary information detailed in sub-parts 1.1 through 1.4 then that should suffice. 2. In sub-part 1.3, we suggest adding the phrase "as applicable" to clarify that not every event will require a notification to, for example, law enforcement. 3. In sub-part 1.4, we suggest adding clarification that the 90-day framework is only required for substantive changes and that all other minor editorial changes can be updated within a year.
Response: Thank you for your comments. (1) The SDT agrees with your suggestion that the entity can best determine what is included in its Operating Plan. The SDT does not envision instructing an entity on what or how of the Operating Plan(s). (2) The SDT feels that the Operating Plan can identify when law enforcement agencies need to be notified without specification from the SDT. (3) The update requirement comes from a FERC directive in Order No. 693. The SDT has validated the intent of the directive and has included that intent in the requirement. The SDT feels that the directive requires Registered Entities to update their Operating Plan(s) within 90 days of the time the entity identified the need for the change, such as a new telephone number, personnel staff name/title, or addition/deletion of person or organization. The DSR SDT has made changes to better clarify "content."		
SERC OC Standards Review Group	No	This is a reporting requirement and should not be confused with Operating Plans that have specific operating actions and goals. Each entity should prepare its own event reporting guideline that address impact events, identification, information gathering, and communication without specifying a specific format such as Operating Plans, Operating Process and Operating Procedures.
Response: Thank you for your comment. The SDT agrees with your viewpoint and believes that your statement is consistent with the intent of the requirement.		
PJM Interconnection LLC	No	1. This is an "after-the-fact" reporting requirement and should not be confused with Operating Plans that have specific operating actions and goals. Each entity should prepare its own impact event operating guideline that addresses impact events, identification of impact events, information gathering, and communication without specifying a specific format such as Operating Plans, Operating Process, and Operating Procedures. In fact, all three documents mentioned can all be a single document. 2. 1.3.2 requires notification of law enforcement agencies for all events listed in Attachment 1. This is essentially not true. For example, firm load is shed requires notification to law enforcement but an IROL

Organization	Yes or No	Question 6 Comment
		violation, generation loss, or voltage deviation do not.
Response: Thank you for your comment. (1) The SDT disagrees with your viewpoint that this requirement specifies after-the-fact reporting. The reporting requirement is later in the standard. The SDT agrees with your viewpoint on the operating guideline you provide and believes that your statement is consistent with the intent of the requirement. (2) The SDT believes that the Registered Entity's Operating Plan(s) can establish when and how law enforcement agencies are notified.		
We Energies	No	R1.2: By its NERC Glossary definition, an Operating Procedure is too prescriptive for data collection. An Operating Procedure requires specific steps to be taken by specific people in a specific order. We would have to predict every event that could happen to have every step in proper order to collect the data. It will be impossible to comply with this requirement. R1.3: Change "Impact Event" to "Impact Event listed in Attachment 1."
Response: Thank you for your comment. The SDT has changed R1 to simply "Operating Plan. The term "Impact Event" has been removed from the standard and R1 and its Parts refer to Attachment 1 as appropriate.		
Compliance & Responsiblity Organization	No	See comments to 2. Also, although NextEra agrees that a documented procedure is appropriate, NextEra does not favor the current approach of pre-defined layers of processes and documentation that seem to overly complicate, and, possibly contradict, already established internal methods by which a company implements policies, procedures and processes. Thus, NextEra's options suggest using a more generic approach that allows entities more flexibility to establish documents and processes, and demonstrate compliance. Such a generic approach was used in NextEra's proposed options set forth in response to number 2.
Response: Thank you for your comments. The SDT believes that most entities already have plans to mostly satisfy the requirements of EOP-004. These would be the procedures that are required under existing CIP-001, R1 and R2.		
Exelon	No	R.1 Does an entity need to develop a standalone Operating Plan if there is an existing process to address identification, assessing and reporting certain events? Suggest rewording to state "Each Responsible Entity shall have an Impact Event Operating Plan or equivalent implementing process that includes:" Disagree these new terms are required. Commonly accepted descriptions of programs, processes and procedures exist in registrar entities that would suffice. For example, R1 could use "Impact Event evaluation

Organization	Yes or No	Question 6 Comment
		and reporting process" as a generic term to describe what is required. This would allow an entity to utilize any existing protocols or management guidelines and naming conventions in effect in their organization.
Response: Thank you for your comments. The SDT The SDT believes that most entities already have plans to mostly satisfy the requirements of EOP-004. These would be the procedures that are required under existing CIP-001, R1 and R2. The Registered Entity will need to examine its current processes to ensure that all aspects of the new requirements are addressed. Thank you for the suggested re-wording. The SDT revised "Impact Event Operating Plan" to just "Operating Plan", thus allowing the entity to implement the requirements as needed.		
Tenaska	No	We already have adequate procedures in place to address sabotage and other significant events, pursuant to the existing CIP-001-1 and EOP-004-1 Standards. The requirement to develop a new Impact Event Operating Plan would increase the administrative burden on Registered Entities to comply with the proposed Standard, without providing a foreseeable improvement in system reliability. The "laundry list" of required Impact Event Operating Plan components is too specific and would make it more difficult to prove compliance with EOP-004-2 during an audit. A revised version of the proposed R5 is the only Requirement that is necessary to achieve the stated purpose of Project 2009-01.
Response: Thank you for your comments. The SDT The SDT believes that most entities already have plans to mostly satisfy the requirements of EOP-004. These would be the procedures that are required under existing CIP-001, R1 and R2 and these should mostly meet the intent of EOP-004. The Registered Entity will need to examine its current processes to ensure that all aspects of the new requirements are addressed. The Parts of R1 are not prescriptive and only provide the minimum information that is required to be in the Operating Plan. The SDT has removed R2 and revised R5 (now R2) to eliminate any duplication.		
United Illuminating Co	No	Does R1.1 require an Operating Process for each Impact Event in attachment 1 or an Operating Process that in general applies to all Impact Events?
Response: Thank you for question. The SDT feels that the Registered Entity can have an Operating Plan that in general applies to all events.		
American Municipal Power	No	No, remove R1. R1 is not an acceptable requirement nor should this be an operation. Focusing on a plan and procedure is overly prescriptive and costly. The only requirement should be to have an entity submit a report. Let the entity decide how they want to implement the reporting.
Response: Thank you for your comment. The SDT agrees that the Registered Entity can decide on the how to implement the reporting; however, this requirement mandates that the Registered Entity document its process.		

Organization	Yes or No	Question 6 Comment
Arkansas Electric Cooperative Corporation	No	We appreciate the effort the team has taken in improving the requirements since the last posting. For 1.3, it appears to suggest the communication must always include communicating to internal personnel and ALL external organizations. We suggest removing the reference to 1.3.1 and 1.3.2 and move 1.3.1 and 1.3.2 to 1.4 and 1.5 respectively. For 1.3.2, modify to state "Internal company personnel notification(s) deemed necessary by the Responsible Entity." For 1.4, we feel the term "content" is too broad as used here. For example, if the FBI changes the contact info for the JTTF, the Responsible Entity may not find out until an incident or annual exercise. Or if the contact person for the state agency changes position without notifying us, it would require us to then change the plan within 90 days. We suggest an annual review of the plan is sufficient for the objective of this requirement.
Response: Thank you for your comments. The SDT has added language "as appropriate" to allow the entity to make its own determination who to contact. The term "content" has been removed and replaced with more detail. The requirement for updates requires changes within 90-days. The SDT believes that the timeline for updating can only be based upon the notification to the Registered Entity. The SDT believes that 90-days from the date the Registered Entity is notified or made aware of the change is a suitable time period to update the document.		
Manitoba Hydro	No	Plan, Process and Procedure are all too interchangeable with each other and have no value being used in "one paragraph" as they do not differentiate from one or other. The terms "identify", "gather" and "communicate" better describe "Process, plan or procedure" so simplify to:1.4. Identification of Impact Events as listed in Attachment 1.1.5. Gathering information for inclusion into Attachment 2 regarding observed Impact Events listed in Attachment 1.1.6. Communicate recognized Impact Events to the following:
Response: Thank you for your comments. The SDT has revised R1 to only include an Operating Plan. Part 1.2 has been revised to "A process for gathering information..."		
American Electric Power	No	Even best developed plans, processes and procedures do not always lend themselves to address the issues at hand. There needs to be flexibility to allow entities to first address the reliability concern and second report correspondingly. Currently, this requirement is overly prescriptive and places unnecessary emphasis on the means to an end and not the outcome. The outcome for this requirement is to report Impact Events.
Response: Thank you for your comments. While the SDT appreciates your views, it disagrees with your assessment. The outcome of this requirement is not to report events; the outcome is to ensure that the Registered Entity has Operating Plan(s) for the identification of events, establishing which internal personnel are involved, identification of outside agencies to be notified, and having a provision for updating the plan(s). Reporting of events is a requirement later in the standard.		

Organization	Yes or No	Question 6 Comment
Consumers Energy	No	Requirement R1, "Have a plan…" with all of the listed criteria, seems to present a serious compliance risk to applicable entities without a direct reliability benefit, as long as entities still indentify and report relevant events. Ad-hoc procedures, as discussed within the R1 "Rationale" have been acknowledged within the rationale to be working effectively, and should remain sufficient without having a documented and by inference, signed, approved, dated document with revision history (as is being demanded today by compliance auditors wherever a "documented plan" is specified within the requirements).
Response: Thank you for your comments. While the SDT appreciates your views, it disagrees with your assessment. The SDT believes that most entities already have plans to mostly satisfy the requirements of EOP-004. These would be the procedures that are required under existing CIP-001, R1 and R2. The measure calls for a current, dated, in force Operating Plan to be provided.		
ISO New England, Inc	No	We do not believe that the use of the Operating Process, Operating Procedure, and Operating Plan for a reporting requirement is consistent with their definitions nor with the intent of the definitions. For instance, an Operating Process is intended to meet an operating goal. What operating goal does this requirement meet? An Operating Procedure includes tasks that must be completed by "specific operating positions." This reporting requirement could be met by back office personnel. We suggest that R1.3.2 delete the list of entities to notify. The terms used to identify who to notify are not defined terms and can lead to subjective interpretations. As written, the requirement does not aid the Applicable entity or the Compliance enforcers in clearly including or excluding who to notify. We also believe that parts 1.3 and 1.3.2 under Requirement 1 will require notification of law enforcement agencies for all Impact Events defined in Attachment 1. While some should require notification to law enforcement such as when there has been destruction to BES equipment, others certainly would not. For instance, law enforcement does not need to know that an IROL violation, generation loss or voltage deviation occurred. We believe the reporting time lines are too aggressive for some events. Reporting events within an hour is not reasonable as an entity may still be dealing the event. This will be particularly difficult when support personnel are not present such as during nights, holidays and weekends. We further suggest that as explicit statement that "reliable operations must ALWAYS take precedence to reporting times" be included in the standard.
Response: Thank you for your comments. While the SDT appreciates your views, it disagrees with your assessment. (P1) The outcome of this requirement is not to report events; the outcome is to ensure that the Registered Entity has Operating Plan(s) for the identification of events, establishing which internal personnel are involved, identification of outside agencies to be notified, and having a provision for updating the plan(s). The		

Organization	Yes or No	Question 6 Comment
SDT feels that current Sabotage Reporting guides already provides much of the information needed in the new R1. (P2) We have revised Requirement R1, Part 1.3 to "A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate:" This should address your concern regarding law enforcement notification. (P3) We have revised most reporting times to 24 hours. Events of a "sabotage" type nature remain at one hour. (P4) While the DSR SDT sees the point you are trying to make, we do not believe that reporting the events in Attachment 1, under the times listed, is burdensome. At the least, this can be accomplished by back office personnel who are not involved in restoration or other reliability efforts.		
Calpine Corp	No	In the "Rationale for R1", the draft states: "Every industry participant that owns or operates elements or devices on the grid has formal or informal process, procedure, or steps it takes to gather information regarding what happened and why it happened when Impact Events occur. This requirement has the Registered Entity establish documentation on how that procedure, process, or plan is organized." Absent substantial evidence that the proposed requirement addresses an actual systemic problem with the "formal or informal process, procedure, or steps it takes" for internal and external evaluation and notification of items listed in Attachment 1, there is no obvious need for this additional paperwork burden, which in most cases will result in a written procedure that documents another existing written procedure or procedures, that will be maintained for the sole purpose of demonstrating compliance with the requirement. Failure to properly report events is currently sanctionable under CIP-001-1 and EOP-004-1 and will continue to be sanctionable under proposed EOP-004-2. Adding a requirement to implement an "Impact Event Operating Plan", "Operating Procedure", and "Operating Process" is unnecessary. However, if the requirement is maintained, the related Measure M1 should state in plain language exactly what elements are required for compliance. Statements such as "The Impact Event Operating Plan may include, but not be limited to, the following?" begs the question regarding what other elements are required to demonstrate compliance. As written, M1 requires that entities provide an "Impact Event Operating Plan", but does specify the required elements of the plan. In the absence of much more detailed instruction on exactly what elements must be included in the various documents, the proposed requirement will create confusion with both compliance and enforcement of the requirement. An example of each of the various required documents would be helpful. Any difficulty in developing such an example would be instructive of the probable compliance issues that would ensure from the necessarily varying approaches taken by disparate entities attempting to meet the requirement.
Response: The DSR SDT thanks you for your comment. Requirement R1 comes from existing CIP-001, R1. The SDT believes it has addressed these concerns by removing the terms "Operating Procedure" and "Operating Process" and has generically referred to them in the elements of the Operating Plan outlined in		

Organization	Yes or No	Question 6 Comment
Parts 1.1-1.5 of the requirement.		
BGE	No	This seems overly restrictive in its use. Requirement is now telling entities how to resolve situations, not giving them a requirement to resolve the situation.
Response: Thank you for your comments. The requirement is written so that an entity has an Operating Plan that contains certain items. The SDT does not specify in the standard how the entity meets these obligations nor does it specify the form nor format of these items.		

Organization	Yes or No	Question 6 Comment
ExxonMobil Research and Engineering	No	The requirement to notify State Law Enforcement deviates from existing government security requirements that Petrochemical Facilities (Cogenerators) are required to follow. Per the Maritime Transportation Security Act of 2002 (MTSA) and the Chemical Facility Anti-Terrorism Standard (CFATS), Petrochemical Facilities are required to report the security incidents identified in EOP-004 Revision 2 to the National Response Center which is staffed by the United States Coast Guard. The National Response Center coordinates incident reporting to both the Department of Homeland Security and Federal Bureau of Investigation. Requiring Petrochemical Facilities to report security incidences to State Law Enforcement agencies duplicates their reporting of incidences to the appropriate law enforcement agencies. EOP-004 Revision 2 should be modified to synergize with existing federal security regulations so that those facilities that are required to comply with the MTSA and CFATS are, by default, compliant with EOP-004 Revision 2 when they comply with these existing federal security regulations. It is unclear, from the documentation provided in this revision of EOP-004, which entities a Responsible Entity is required to notify when certain types of Impact Events occur. Previously, CIP-001 included a similarly vague instruction that required notifications to the 'appropriate parties in the interconnection' and the FBI/RCMP. The Standard Drafting Team should identify which NERC Functional Entities should be notified when each of the Impact Events identified in Attachment 1 occurs. Current revisions of CIP-001 Revision 1 or EOP-004 Revision 1 do not include corresponding requirements to update procedures within a certain time frame. It's difficult to foresee a situation where an Entity would initiate a change to its response plan without being required to update the formal response plan documentation per their management of change process. Additionally, failure to update the procedure would result in the entity deviating from the procedure any time an impact event occurred, which would automatically force a violation of EOP-004-2 R2 for failure to properly implement their Operating Process. Furthermore, the only changes occurring between review cycles should be revisions to the contact information for third parties. It is beyond an entity's power to require third parties to notify the entity when the third party changes their contact information, and, as such, this requirement burdens registered facilities with responsibility for compliance for items that are beyond their realm of control.

Response: Thank you for your comments. (P1) The SDT believes that the requirement does not mandate contact to State Law Enforcement agencies; but merely to include them if appropriate. While we have tried to coordinate with the US DOE, Federal security regulations are outside the scope of this project. (P2) We have revised Requirement R1, Part 1.3 to "A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate:" Each type of event should be assessed by the entity to determine whether or not law enforcement needs to be notified,

(P3)The subrequirement for updating comes from a FERC directive in Order No. 693. If the Registered Entity's Operating Plan(s) have a provision for updating, then the entity only needs to verify that the updating does not exceed 90 days from the date of being aware.

Organization	Yes or No	Question 6 Comment
Farmington Electric Utility System	No	consider rewording 1.4; the wording implies a change to content already occurred, so it would be updated concurrently ? consider, updating the plan within 90 days of discovery of content requiring a change?
Response: Thank you for your comment. The SDT agrees with your suggestion and has revised Requirement R1, Part 1.4 to: Provision(s) for updating the Operating Plan within 90 calendar days of any change in assets, personnel, other circumstances that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to R3.		
Constellation Power Generation	No	Per NERC's glossary of terms, an Operating Plan can include Operating Process documents and Operating Procedures. An Operating Process identifies general tasks while an Operating Procedure identifies specific tasks. CPG is unclear as to why R1.1 and R1.3 require the use of an Operating Process while R1.2 requires an Operating Procedure. CPG believes that R1.2 should be changed to require the use of an Operating Process instead of Operating Procedure. R1.2 is merely requiring an entity to fill out the necessary forms should an event occur, so requiring a clear and concise step by step procedure for filling out a form only adds a compliance burden to an entity instead of improving the reliability of the BES. CPG does agree with the DSR SDT that an entity should have a process in place mandating that the proper paperwork be completed in a timely manner should an event occur.
Response: Thank you for your comments. The SDT has modified Requirement R1, Part 1.1 and Part 1.3 to a "process" as part of the elements of the referenced "Operating Plan" in R1. The SDT has also changed "Operating Procedure" to a "process" in R1.2. This sub-requirement provides for establishing the list of internal personnel to be notified in the case of an event, not the reporting of the event.		
Georgia System Operations Corporation	No	-R1.3.2: "Law Enforcement", "Governmental Agencies", and "Provincial Agencies" are not proper nouns/names and are not defined in the NERC Glossary. They should not be capitalized. -R1.4: Keeping documents current and in force should be a matter of an entit
Response: Thank you for your comments. The SDT agrees with your suggestions on capitalization and has made the corrections. The update provision comes from a FERC directive in Order No. 693.		
Indeck Energy Services	No	The terms are not important and many plans or procedures already exist and restructuring them to match the

Organization	Yes or No	Question 6 Comment
		terms is wasteful. R1 is too prescriptive. R1 should state that a written document should show how the entity will comply with EOP-004. R1.2 is superfluous and should be deleted. The data must be gathered and the process will vary with the event. Trying to define the multitude of possibilities for the collection process is not productive and leaves open the possibility of missing something for an auditor to nit pick. R1.3 should just be a written communications plan/process/procedure for external notifications. R1.4 is redundant because it can't be changed within 90 days until the content has already been changed. R1.4 should be deleted. The Violation Risk Factor should be Low, if any, because this is historical reporting, with little or no reliability consequence.
Response: The SDT disagrees with your viewpoints associated with R1 because the requirement only specifies the elements required, now how to implement them. The SDT believes that many Registered Entities will be able to use their current Sabotage Reporting processes, with some slight modification to address the new sub-requirements. Requirement R1, Part 1.2: The requirement is written so that it is not prescriptive and allows the entity to identify the steps it will take to gather information for filing the report. The DSR SDT does not envision this as being a tome that contains specific data gathering protocol for each event type. Requirement R1, Part 1.3: Has been revised to: "1.3. A process for communicating recognized impact events listed in EOP-004 - Attachment 1 that includes to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and , but is not limited to the following as appropriate :" For Requirement R1, Part 1.4, the update provision comes from a FERC directive in Order No. 693. In addition, the SDT believes that the update is required within 90 days from the date of being notified of the change or update. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Midwest Reliability Organization	Yes	This is a NERC defined term and will assist entities in maintaining compliance with this (proposed) Standard.
Response: Thank you for your comment.		

Organization	Yes or No	Question 6 Comment
Western Electricity Coordinating Council	Yes	Are "Law Enforcement" considered a "Governmental Agency" (they are listed separately and both required) If not, is there any qualifiers on whether Law Enforcement or Governmental Agency refers to municipal, county, state or federal or any combination" Since the term "Provincial" is associated with "Governmental" it tends to indicate State level. As it is written now an auditor would require documentation of "some" Law Enforcement (other than company security) and an additional communication to at least "some" Agency which could be considered Governmental. Municipal or higher. Contact with City police or Sheriff and either city or county government rep would satisfy. Additional clarity would help from a compliance enforcement perspective.
Response: Thank you for your comments. The SDT expects that Registered Entities will identify the proper outside organizations needed for their organization. The SDT feels that law enforcement agencies include federal, state, provincial, or local law agencies and these are not the same as governmental or regulatory agencies. Please refer to the Background section of the standard for further clarification on law enforcement notifications.		
Alliant Energy	Yes	This is a NERC defined term and will assist entities in maintaining compliance with this (proposed) Standard. We believe the reference to Attachment 2 in R1.2 should be revised to the DOE Form and utilize only one reporting form, if at all possible.
Response: Thank you for your comments. The DSR SDT continues to work with the DOE to develop a single reporting form that is acceptable to both.		
Occidental Power Marketing	Yes	However, only LSEs with BES assets (or assets that support the BES) should be included in the Applicability section of the standard.
Response: Thank you for your comment. LSE applicability is related to their applicability under CIP-002 and CIP-008.		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	However, there needs to be some clarity on which government agencies (if not the FBI) are responsible for reporting these type of events.
Response: Thank you for your comments. Each Registered Entity should be aware of any reporting obligations it may have to various government agencies (federal, state/provincial, local). To the extent they exist, the notification needs to be included in the entity's Operating Plan(s).		
Northeast Power Coordinating	Yes	

Organization	Yes or No	Question 6 Comment
Council		
PPL Supply	Yes	
Southern Company	Yes	
SRP	Yes	
SDG&E	Yes	
City of Tallahassee (TAL)	Yes	
New Harquahala Generating Co.	Yes	
Liberty Electric Power LLC	Yes	
APX Power Markets	Yes	
Sweeny Cogeneration LP	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Independent Electricity System Operator	Yes	
Platte River Power Authority	Yes	
CenterPoint Energy	Yes	
PPL Electric Utilities	Yes	
Lincoln Electric System	Yes	

Organization	Yes or No	Question 6 Comment
American Transmission Company	Yes	
Ingleside Cogeneration LP	Yes	
Duke Energy	Yes	
Progress Energy	Yes	

7. Do you agree with the proposed revisions to Requirement 3 (now R2)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: The slight majority of commenters agreed with the language of Requirement R2. A significant minority opinion exists where commenters suggest revisiting R2 and R5 to eliminate potential redundancy and confusion. Similar comments were received pertaining to Requirement 5 (question 10 below). The DSR SDT has revised Attachment 1 to indicate that entities must submit Attachment 2 or the DOE OE-417 form. This information was contained in Requirement R5. The intent of the two requirements is to have entities make appropriate notifications and report impact events contained in Attachment 1. By eliminating R2 and revising R5 (now R2), the DSR SDT has maintained the intent of the requirements while eliminating potential confusion and redundancy. The revised requirements are shown below:

~~R2. Each Responsible Entity shall implement its Impact Event Operating Plan documented in Requirement R1 for Impact Events listed in Attachment 1 (Parts A and B). [Violation Risk: Factor Medium] [Time Horizon: Real-time Operations and Same-day Operations]~~

Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].

Organization	Yes or No	Question 7 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation	No	We are concerned with having a separate requirement to implement the Plan. Is this requirement necessary on its own? Should R1 instead require a Responsible Entity to "document and implement" an Impact Event Operating Plan? More specifically, if an Entity does not have an Impact Event, are they in violation of this requirement? If merging this requirement with R1 is not acceptable we suggest moving the language from the measure to the requirement as such: "To the extent that a Reponsible Entity has an Impact Event on its Facilities, Each Responsible Entity shall implement?" Additionally, R1 uses the phrase "recognized Impact Event" where as R2 simply uses the term "Impact Event." The phrase "recognized Impact Event" should be used consistently in R2 as well.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted requirement 2 and revised requirements 1 and 5 to address your concern. The DSR SDT believes that the requirement should remain separate to eliminate the possibility of double jeopardy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		

Organization	Yes or No	Question 7 Comment
Bonneville Power Administration	No	Minimize the number of requirements. Not sure what the new R2 intends that is different than having a valid plan (signed?). Why can't R1 have develop and implement? R5 is the reporting. Implement should be with R1 or R5 depending on the interpretation.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted requirement 2 and revised requirements 1 and 5 to address your concern. The DSR SDT believes that the requirement should remain separate to eliminate the possibility of double jeopardy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		
PSEG Companies	No	Fuel supply emergency, as discussed in response to question 4 above, is not a defined condition. This event should be removed.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Fuel Supply Emergency from Attachment 1. This item was removed in coordination with the NERC Events Analysis Working Group and the proposed Events Analysis Program.		
SERC OC Standards Review Group	No	We agree with the concept, but disagree with the use of the term “Operating Plan” as a defined term in line with our comments in question 6 above.
Response: The DSR SDT thanks you for your comment. Please see response to comments in Question 6 The DSR SDT has revised R1 to eliminate the use of Operating Process and Operating Procedure and have used more generic terms.		
PJM Interconnection LLC	No	We agree with the concept but disagree with the use of the term “Operating Plan” as a defined term in line with our comments in Question 6 above.

Organization	Yes or No	Question 7 Comment
Response: The DSR SDT thanks you for your comment. Please see response to comments in Question 6		
Compliance & Responsiblity Organization	No	See comments set forth in number 2.
Response: The DSR SDT thanks you for your comment. Please see response to question 2.		
Exelon	No	Agree that each Responsible Entity shall implement the [Impact] Events listed in Attachment 1 (Parts A and B); however, disagree with certain events, reporting responsibilities, threshold for reporting and time to submit reports as currently outlined in Attachment 1 (Parts A and B). Also suggest that R.2 be reworded to state for applicable [Impact] Events listed in Attachment 1 (Parts A and B). This requirement should only be applied to those events applicable to the registered entity.R2 is redundant to R1. No entity could claim to have met R1 if their plan / process was not operational and approved in the manner consistent with any other approved program, process, guideline etc. within their company.
Response: The DSR SDT thanks you for your comment. The DSR SDT has significantly revised Attachment 1. We have removed the timing column and replaced it with more specific information regarding which form to submit and to whom to submit the report. All events are now to be reported within 24 hours with the exception of Destruction of BES equipment, Damage or destruction of Critical Assets and Damage or destruction of Critical Cyber Asset events, Forced Intrusion, Risk to BES equipment and Detection of a reportable Cyber Security Incident. These events are to be reported within 1 hour. Notification of law enforcement per Part 1.3.2 is also required for these events only. The DSR SDT has also eliminated R2 and revised R5 for clarity and to eliminate potential redundancy. The DSR SDT believes that the requirement should remain separate to eliminate the possibility of double jeopardy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		
Tenaska	No	The proposed Impact Event Operating Plan should not be required.
Response: The DSR SDT thanks you for your comment.		

Organization	Yes or No	Question 7 Comment
The DSR SDT has revised R1 to only include development of an Operating Plan that includes the Parts of R1. This Operating Plan is required so that the entity's personnel will know what to do in the event of an event, how to report the event and to whom the report should be sent.		
American Municipal Power	No	No, remove R2. R2 is not an acceptable requirement nor should this be an operation. Focusing on a plan is overly prescriptive and costly. The only requirement should be to have an entity submit a report. Let the entity decide how they want to implement the reporting.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated R2 and revised R5 for clarity and to eliminate potential redundancy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		
American Electric Power	No	Requirement 5 and Requirement 2 are redundant. We recommend Requirement 2 be replaced with the language in Requirement 5. "Each Responsible Entity shall report Impact Events in accordance with the Impact Event Operating Plan pursuant to Requirement R1 and Attachment 1 using the form in Attachment 2 or the DOE OE-417."
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated R2 and revised R5 for clarity and to eliminate potential redundancy. The old Requirement R5 has been revised as the new Requirement R2, which reads: Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		
ISO New England, Inc	No	Fuel Supply Emergency is not a defined condition. We suggest that the SDT poll the ballot body regarding the reporting of Fuel Supply Emergencies. Fuel Supply is an economic consideration and the concept of Fuel Supply Emergency is subjective. A resource that uses coal or oil may vary its supplies based on economic considerations (the price of the fuel). For a conservative BA a fuel-on-demand supply line can be viewed as a fuel supply emergency whereas the resource owner sees the matter as good business. Moreover, the release of such reports to the public can have unintended consequences. Fuel disruptions caused by contract negotiations when reported to the public can result in non-union transportation employees being physically

Organization	Yes or No	Question 7 Comment
		harmed by fuel supply organizers thus resulting in the loss of non-contract fuel. Further, this information may aggravate the situation by causing the cost of fuel to be inflated by suppliers when demand is great. If this event is not deleted, then we would suggest that the definition be constrained to "declared" fuel supply emergencies. Suggest the deletion of category: Risk to BES equipment. Because of the broad definition of BES, the risk to BES equipment is overly broad and can be applied to any risk to any "part of" any BES asset. The footnote helps identify what the SDT was intending, however, the words themselves can result in overly broad findings by compliance enforcement people.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Fuel Supply Emergency from Attachment 1. This item was removed in coordination with the NERC Events Analysis Working Group and the proposed Events Analysis Program.		
Calpine Corp	No	Requirement R2 is unnecessary for the same reasons listed above in answer to question 6 regarding Requirement R1. A new Reliability Standard requirement is not needed to verify that internal notifications are made within Registered Entities or to ensure that Registered Entities notify local law enforcement of suspicious activity, sabotage, theft, or vandalism. Such notifications are made by any company, and this requirement does not clearly enhance the reliability of the Bulk Electric System. Requirement R5 provides sanction in the event that events listed in Attachment 1 are not made appropriately. However, if the requirement is maintained, the related Measure M2 should state in plain language exactly what elements are required for compliance. In the absence of much more detailed instruction on exactly what elements must be included in the various documents, the proposed requirement will create confusion with both compliance and enforcement of the requirement. A detailed example of example documentation would be helpful. Any difficulty in developing such an example would be instructive of the probable compliance issues that would ensure from the necessarily varying approaches that would be taken by disparate entities attempting to meet the requirement.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated R2 and revised R5 for clarity and to eliminate potential redundancy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		
CenterPoint Energy	No	CenterPoint Energy recommends deleting the current R2 as it is an inherent part of the current R5. For an entity to "report Impact Events in accordance with the Impact Event Operating Plan pursuant to R1" (see R5), the entity must "implement its Impact Operating Plan documented in Requirement 1?" (see R2). Including

Organization	Yes or No	Question 7 Comment
		both requirements is unnecessary and duplicative. Likewise, M2 should be deleted.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated R2 and revised R5 for clarity and to eliminate potential redundancy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		
ExxonMobil Research and Engineering	No	The notification requirement and documentation in Attachment 1 do not clearly identify which entities need to be notified for each type of event detailed in Attachment 1. While it makes sense to notify the Reliability Coordinator, NERC, Regional Entity, Law Enforcement and other Governmental Agencies for sabotage type events, it does not seem proper to notify Law Enforcement agencies of a system disturbance that is unrelated to improper human intervention. Furthermore, it is our belief that a time frame of 1 hour is a short window for making a verbal notification to third parties, and an impossibly short window for requiring the submittal of a completed form regardless of the simplicity. When a Petrochemical Facility experiences an impact event, the initial focus should emphasize safe control of the chemical process. For those cases where registered entities are required to submit a form within 1 hour, the Standard Drafting Team should alter the requirement to allow for verbal notification during the first few hours following the initiation of an Impact Event (i.e. allow the facility time to appropriately respond to and gain control of the situation prior to making a notification which may take several hours) and provide separate notifications windows for those parties that will need to respond to an Impact Event immediately and those entities that need to be informed that one occurred for the purposes of investigating the cause of and response to an Impact Event. For example, a GOP should immediately notify a TOP when it experiences a forced outage of generation capacity as soon as possible, but there is no immediate benefit to notify NERC when site personnel are responding to the event in order to gain control of of the situation and determine the extent of the problem. The existing standard's requirement to file an initial report to entities, such as NERC, within 24 hours seems reasonable provided that proper real time notifications are made and the Standard Drafting Team reinstates EOP-004 Revision 1's Requirement 3.3, which allows for the extension of the 24 hour window during adverse conditions, into the requirement section of EOP-004 [the current revision locates this extension in Attachment 1, which, according to input received from Regional Entities, means that the extension would not be enforceable].
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated R2 and revised R5 for clarity and to eliminate potential redundancy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment]. The DSR SDT has significantly revised Attachment 1. We have removed the timing column and replaced it with more specific information regarding which form to submit and to whom to submit the report. All events are now to be reported within 24 hours with the exception of Destruction of BES equipment, Damage or destruction of Critical Assets and Damage or destruction of Critical Cyber Asset events in Part A and Forced Intrusion, Risk to BES equipment and Detection of a reportable Cyber Security Incident in Part B. These events are to be reported within 1 hour. Notification of law enforcement per Part 1.3.2 is also required for		

Organization	Yes or No	Question 7 Comment
these events only.		
American Transmission Company	No	ATC does not agree with the proposed language in Requirement 3. ATC is concerned that, in order to demonstrate compliance, an entity will have to show that each step in the plan was followed which will likely leave entities facing the choice of choosing between different compliance violations. If the plan is not followed, but the report is made within the time given, then an entity is in violations of their plan. If the plan is followed, but the report does not get filed within the time allotted, then they face a possible violation of the time to report. ATC believes that the team should enforce the position that the report being filed in the time allotted is key, not that they necessarily follow and document that their plan was followed. Depending on the situation, the internal reporting will vary; however, based on the purpose of the Standard, the key is to get a report to NERC.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated R2 and revised R5 for clarity and to eliminate potential redundancy. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		
Georgia System Operations Corporation	No	-We suggest moving the language from the measure to the requirement as such:"To the extent that a Reponsible Entity has an Impact Event on its Facilities, each Responsible Entity shall implement?"Additionally, R1 uses the phrase "recognized Impact Event"
Response: The DSR SDT thanks you for your comment. Requirement 2 has been deleted along with its associated Measure M2. R1 no longer references “recognized” events.		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	No	There are generally several events during the year. If the process is well documented, a drill or exercise is excessive. It should be sufficient to say “provide training.”
Response: The DSR SDT thanks you for your comment. This appears to be related to R3 in question 8. If an event occurs during the year, additional testing is not required.		
Indeck Energy Services	No	R2 is direct and to the point. The Violation Risk Factor should be Low, if any, because this is historical reporting, with little or no reliability consequence.

Organization	Yes or No	Question 7 Comment
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Midwest Reliability Organization	Yes	This clearly states that an entity's Operating Plan is to be used for reporting of Impact Events.
Response: The DSR SDT thanks you for your comment.		
Dominion	Yes	Dominion agrees subject to the comments provided in Question #6. In addition, Requirement R2 appears duplicative of Requirement R5.Suggest R2 be clarified relative to the intent.
Response: The DSR SDT thanks you for your comment. Please see responses to comments in Question 6. R2 was deleted and R5 was revised. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment]. The DSR SDT has revised R1 to eliminate the use of Operating Process and Operating Procedure and have used more generic terms.		
Manitoba Hydro	Yes	Removing "assess the initial probable cause" from the statement removes the ambiguity in the same way as replacing sabotage with impact level. Let the staff trained in this field determine probable cause after the fact.
Response: The DSR SDT thanks you for your comment.		
Occidental Power Marketing	Yes	However, only LSEs with BES assets (or assets that directly support the BES) should be included in the Applicability section of the standard.
Response: The DSR SDT thanks you for your comment. Attachment 1 specifies which types of events are required to be reported by each entity.		

Organization	Yes or No	Question 7 Comment
Constellation Power Generation	Yes	Although CPG agrees with the wording of Requirement 2, CPG has several comments and suggested changes regarding the Attachments, to which this requirement points. Please see those comments below.
Response: The DSR SDT thanks you for your comment. Please see responses below.		
Northeast Power Coordinating Council	Yes	
Western Electricity Coordinating Council	Yes	
Pacific Northwest Small Public Power Utility Comment Group	Yes	
Pepco Holdings Inc and Affiliates	Yes	
SPP Standards Review Group	Yes	
Midwest ISO Standards Collaborators	Yes	
FirstEnergy	Yes	
Southern Company	Yes	
SRP	Yes	
We Energies	Yes	
SDG&E	Yes	
City of Tallahassee (TAL)	Yes	
New Harquahala Generating Co.	Yes	

Organization	Yes or No	Question 7 Comment
APX Power Markets	Yes	
United Illuminating Co	Yes	
Liberty Electric Power LLC	Yes	
Arkansas Electric Cooperative Corporation	Yes	
Sweeny Cogeneration LP	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Independent Electricity System Operator	Yes	
Platte River Power Authority	Yes	
BGE	Yes	No comments.
Alliant Energy	Yes	
PPL Electric Utilities	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
Ingleside Cogeneration LP	Yes	
Duke Energy	Yes	

Organization	Yes or No	Question 7 Comment
Brazos Electric Power Cooperative	Yes	
Progress Energy	Yes	
Response: The DSR SDT thanks you for your comment. Based on stakeholder comments, Requirement R2 was deleted and R5 was revised. Old R5, New R2. Each Responsible Entity shall report impact events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment].		

8. Do you agree with the proposed revisions to Requirement 4 (now R3)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: There were several issues that commenters raised regarding removing the requirement. Below is a summary:

1) Review annual component CAN0010 states: Regardless of the registered entity's documented definition of annual, it will not supersede any requirement stated in the standard. The DSR SDT is defining "annual" within this Standard (and only for this Standard).

2) Remove R3-requirement – Several stakeholders believed the testing to be onerous. The language of the requirement was revised to indicate that only the communications portion of the Operating Plan is required to be tested. Each Responsible Entity shall conduct a test of the communication process in its Operating Plan, created pursuant to Requirement 1, Part 1.3, at least annually (once per calendar year), with no more than 15 calendar months between tests.

3) Unclear if actual events would qualify for a test in the requirement – The language in the measure was revised to add "Implementation of the communication process as documented in its Operating Plan for an actual event may be used as evidence to meet this requirement. "

4) VRF is too high on R3 – With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.

Organization	Yes or No	Question 8 Comment

Organization	Yes or No	Question 8 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation	No	With the current CAN on the definition of annual, we do not believe that the additional qualification that the test shall be conducted "with no more that 15 calendar months between tests" is necessary. If instead the team believes that, in order to support the reliability of the BES, tests should be performed at least every 15 months, then the requirement should be to perform a test at least every 15 calendar months and remove the annual component.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. Per the CAN, "Regardless of the registered entity's documented definition of annual, it will not supersede any requirement stated in the standard." The team believes the requirement is specifying what the team believes to be appropriate.		
Northeast Power Coordinating Council	No	The annual testing requirement is too frequent for a reporting, and not an operational process. The testing interval should be extended to five years.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. We feel that five years is too long of an interval between tests as contact information contained in the plan may change more often. A one year test is more likely to catch problems with the Operating Plan. If an entity has an event, then they do not need to test the plan during the annual cycle.		
Bonneville Power Administration	No	Too burdensome to go through EACH and ALL individual Impacts and report each one on a drill basis with outside entities. One or two scenarios may be OK.
Response: The DSR SDT thanks you for your comment. It is not intended to perform a test for each type of event listed in Attachment 1. The entity is free to choose any single event to test its operating plan. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The test under R3 Operating Plan is to test the communication aspect of your Operating Plan.		
Dominion	No	: The need to conduct a test of its Operating Process has not been established and is overly restrictive given that the purpose of the standard is to report Impact Events.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can		

Organization	Yes or No	Question 8 Comment
respond appropriately in the case of an actual event. The SDT thinks it is critical to test the Operating Plan to verify that employees know the appropriate actions to take and that there are no issues with the reporting procedures. Not testing the Operating Plan could result in employees being unprepared to communicate and report for an actual event.		
SPP Standards Review Group	No	The SDT included a formal review process in the discussion of R4 in the Background Information in the Unofficial Comment Form as one of three options for demonstrating compliance with the testing requirements of R4, yet M3 only contains two of those options ? a mock Impact Event exercise and a real-time implementation of its Operating Process. The third option, a formal review process, is missing from M3 and needs to be added. We would suggest the following for M3: ?In the absence of an actual Impact Event, the Responsible Entity shall provide evidence that it conducted a mock Impact Event and followed its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 or conducted a formal review of its Operating Process. The time period between tests, actual Impact Events or formal reviews shall be no more than 15 calendar months. Evidence may include, but is not limited to, operator logs, voice recordings or documentation.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The standard now has only three requirements. The requirement to test the communications process is important so that any issues or errors in the Operating Plan can be identified. The team feels that a formal review will not be able to identify any of these errors unless the communications process is tested.		
Midwest ISO Standards Collaborators	No	We appreciate the drafting team recognizes that actual implementation of the plan for a real event should qualify as a ?test?. However, we are concerned that review of this requirement in isolation of the background material and information provided by the drafting team may cause a compliance auditor to believe that a test cannot be met by actual implementation. Furthermore, we do not believe testing a reporting procedure is necessary. Periodic reminders to personnel responsible for implementing the procedure make sense but testing it does not add to reliability. If they don?t report an event, it will become obvious with all the tools (SAFNR project) the regulators have to observe system operations.
Response: The DSR SDT thanks you for your comment. We have added the following to the measure: "Implementation of the communication process as documented in its Operating Plan for an actual event may be used as evidence to meet this requirement."		
FirstEnergy	No	We believe that a separate requirement for testing the reporting process is unnecessary. The FERC directive that required periodic testing was directed at sabotage events per CIP-001. Since the proposed standard

Organization	Yes or No	Question 8 Comment
		moves the responsibility for classifying an event as sabotage from the entity to the applicable law enforcement authority, the need for a periodic drill is no longer necessary. We believe that Requirement R4 should suffice in ensuring that the individuals involved in the process are aware of their responsibilities.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The standard now has only three requirements. The requirement to test the communications process is important so that any issues or errors in the Operating Plan can be identified.		
SERC OC Standards Review Group	No	Annual testing of an ?after-the-fact? reporting procedure does not add to the reliability of the BES!
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The standard now has only three requirements. The requirement to test the communications process is important so that any issues or errors in the Operating Plan can be identified. This will allow for reporting to the appropriate entities in the case of an actual event.		
PJM Interconnection LLC	No	1. This is an ?after-the-fact? reporting requirement (administrative in nature). Annual testing of such a requirement does not add to the reliability of the BES. 2. R3 attempts to define ?Annual? for the Registered Entity to test its Operating Process. We believe R3 should follow the NERC definition of Annual as defined in the NERC Compliance Application Notice (CAN) ? CAN-0010 ? Definition of Annual as opposed to creating a new definition of Annual ? or ? refer to an entity?s defined use of the term annual.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The standard now has only three requirements. The requirement to test the communications process is important so that any issues or errors in the Operating Plan can be identified. This will allow for reporting to the appropriate entities in the case of an actual event. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. Per the CAN, “Regardless of the registered entity’s documented definition of annual, it will not supersede any		

Organization	Yes or No	Question 8 Comment
requirement stated in the standard." The team believes the requirement is specifying what the team believes to be appropriate.		
We Energies	No	A test of the Operating Process for communication would be placing telephone calls. This requirement would have virtually every entity in North America calling NERC, Regional Entities, FERC/Provincial Agency, Public Service Commission, FBI/RCMP, local Police, etc. annually. Every entity will probably be asking for a confirmation letter from each telephone call for proof of compliance. This is an unnecessary requirement. Delete it.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The standard now has only three requirements. The requirement to test the communications process is important so that any issues or errors in the Operating Plan can be identified. This will allow for reporting to the appropriate entities in the case of an actual event.		
Compliance & Responsiblity Organization	No	See comments set forth in number 2. Also, while NextEra understands the need to have a testing requirement for sabotage (Order 693 at P 446), it does not find it necessary to have a testing requirement for the other events. At this time in the process, additional requirements for the sake of having a requirement are likely to detract from reliability. Thus, NextEra requests that the testing requirement be limited to sabotage related events.
Response: The DSR SDT thanks you for your comment. Please see responses to Question 2 above. Each entity may choose an event type for which to perform the communications process test. It need not be performed for each and every event type listed in Attachment 1. The test must include all aspects of the communications process, including NERC and the RE. The measure for R3 was revised to make it explicit that evidence for compliance for R3 includes an actual event. M3. The Responsible Entity shall provide evidence that it conducted a test of the communication process as documented in its Operating Plan impact events created pursuant to Requirement R1, Part 1.3. Implementation of the communication process as documented in its Operating Plan for an actual impact event may be used as evidence to meet this requirement. The time period between an actual impact event or test shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or dated documentation of a test. (R3)		
Exelon	No	- Each entity should be able to determine if they need a drill for a particular event. Is this document implying that the annual drill covering all applicable [Impact] Events?

Organization	Yes or No	Question 8 Comment
		- A provision should be added to be able to take credit for an existing drill/exercise that could incorporate the required communications to meet the intent of R.3 to alleviate the burden on conducting a standalone annual drill. The DSR SDT needs to provide more guidance on the objectives and format of the drill expected (e.g., table top, simulator, mock drill). - A provision should be added to R.3 to allow for an actual event to be used as credit for the annual requirement. It would seem that the intent is as such based on the wording in M.3; however, it needs to be explicit in the Requirement. - Must a test include communicating to NERC or the Region?
Response: The DSR SDT thanks you for your comment. Each entity may choose an event type for which to perform the communications process test. It need not be performed for each and every event type listed in Attachment 1. The test must include all aspects of the communications process, including NERC and the RE. The measure for R3 was revised to make it explicit that evidence for compliance for R3 includes an actual event. M3. The Responsible Entity shall provide evidence that it conducted a test of the communication process as documented in its Operating Plan impact events created pursuant to Requirement R1, Part 1.3. Implementation of the communication process as documented in its Operating Plan for an actual impact event may be used as evidence to meet this requirement. The time period between an actual impact event or test shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or dated documentation of a test. (R3)		
City of Tallahassee (TAL)	No	Comments: The verbiage “at least annually, with no more than 15 months between such tests” is an attempt to define annually. If you want every 15 months say “at least every 15 months.” Otherwise just say annual and let the entities decide what that is, as is being done with other “annual” requirements. Additionally, while the Measure (M3) implies that an actual event would suffice it is not stated in the requirement, and the entire plan should be tested, not just a component. Proposed: Each Responsible Entity shall conduct a test of its Impact Event Operating Plan at least annually. A test of the Impact Event Operating Plan can range from a paper drill, to the response to an actual event.
Response: The DSR SDT thanks you for your comment. The language now reads: “annually (once per calendar year), with no more than 15 calendar months between tests”. This comports with the intent and with the recent CAN from NERC on the use of “Annual”. The intent of the requirement is to verify that an entity’s personnel can communicate with other entities when a real event occurs. It is expected that such a test will include all aspects of the communications process. The measure was revised to clarify that an actual event can be used in lieu of a test. R3 reads: “Each Responsible Entity shall conduct a test of the communication process as documented in its Operating Plan, created pursuant to Requirement 1, Part 1.3, impact events at least annually, (once per calendar year), with no more than 15 calendar months between tests.”		

Organization	Yes or No	Question 8 Comment
Tenaska	No	The proposed Impact Event Operating Plan should not be required, therefore any tests of the Operating Process should not be required.
Response: The DSR SDT thanks you for your comment. Stakeholder consensus indicates that the majority of stakeholders agree with the Operating Plan requirement.		
American Municipal Power	No	No, remove R3. R3 is not an acceptable requirement nor should this be an operation. Focusing on a test is overly prescriptive and costly. The only requirement should be to have an entity submit a report. Let the entity decide how they want to implement the reporting.
Response: The DSR SDT thanks you for your comment. The intent of the requirement is to verify that an entity's personnel can communicate with other entities when a real event occurs. It is expected that such a test will include all aspects of the communications process. The measure was revised to clarify that an actual event can be used in lieu of a test. This should not be a costly nor burdensome requirement.		
Liberty Electric Power LLC	No	It is not the proper role of the standards to dictate how an entity conducts training. Large utilities with backup control rooms and enough personnel can conduct routine drills without disturbing operations, but this is not always the case for small entities. Further, classroom training where emergency responses are discussed can be a better tool at times for assuring compliance with operating procedures. I would suggest R3 read "Each entity shall assure that personnel are aware of the requirements of EOP-004 and capable of responding as required."
Response: The DSR SDT thanks you for your comment. The DSR SDT agrees and has removed the training Requirement, R4.		
Sweeny Cogeneration LP	No	We do not see a reliability benefit in the planning and execution of tests or drills to ensure that regulatory reporting is performed in a timely fashion. It is sufficient that penalties can be assessed against entities that do not properly respond in accordance with EOP-004-2, leaving it to us to determine how to avoid them.
Response: The DSR SDT thanks you for your comment. The intent of the requirement is to verify that an entity's personnel can communicate with other entities when a real event occurs. It is expected that such a test will include all aspects of the communications process. The measure was revised to clarify that an actual event can be used in lieu of a test.		
American Electric Power	No	It is unclear if actual events would qualify for a test in the requirement; however, the associated measure and rationale appear to support this. We suggest the requirement be restated to allow for actual events to count for this requirement.

Organization	Yes or No	Question 8 Comment
Response: The DSR SDT thanks you for your comment. The intent of the requirement is to verify that an entity's personnel can communicate with other entities when a real event occurs. It is expected that such a test will include all aspects of the communications process. The measure was revised to clarify that an actual event can be used in lieu of a test.		
New Harquahala Generating Co.	No	M3. In the absence of an actual Impact Event, the Responsible Entity shall provide evidence that it conducted a mock Impact Event and followed its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The time period between actual and or mock Impact Events shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or documentation. (R3). The measure for R3 needs to make it clear that "exercise/drill/actual employment" can be a classroom exercise, utilizing scenarios for discussion. It should not be necessary to fully test the plan by making actual phone calls, notifications etc.
Response: The DSR SDT thanks you for your comment. The intent of the requirement is to verify that an entity's personnel can communicate with other entities when a real event occurs. It is expected that such a test will include all aspects of the communications process including making actual phone calls, etc. The measure was revised to clarify that an actual event can be used in lieu of a test. The purpose of the requirement is to ensure that the communications process works.		
ISO New England, Inc	No	We appreciate and agree with the drafting team recognizes that actual implementation of the plan for a real event should qualify as a "test." However, we are concerned that review of this requirement in isolation and without the benefit of the background material and information provided by the drafting team may cause a compliance auditor to believe that a test cannot be met by actual implementation. Furthermore, we do not believe testing a reporting procedure is necessary. Periodic reminders to personnel responsible for implementing the procedure make sense but testing it does not add to reliability. If they don't report an event, it will become obvious to compliance auditors. Recommend using language similar to CIP-009. "Each Responsible Entity shall conduct a an exercise of its operating process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 at least annually, with no more than 15 calendar months between exercises." An exercise can range from a paper drill, to a full operational exercise, to reporting of actual incident Also, we question the need to conduct a test annually. Since this is only a reporting Standard and, as such, has no direct impact on reliability, we suggest modifying the testing requirement to once every three years. CIP-009-3 **R.2** Exercises —The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident. **M2.** The Responsible Entity shall make available its records documenting required exercises as specified in

Organization	Yes or No	Question 8 Comment
		Requirement R2.
Response: The DSR SDT thanks you for your comment. The intent of the requirement is to verify that an entity's personnel can communicate with other entities when a real event occurs. It is expected that such a test will include all aspects of the communications process. The measure was revised to clarify that an actual event can be used in lieu of a test.		
Calpine Corp	No	Absent substantial evidence that the proposed requirement addresses an actual systemic problem with actual submittal of reports of electrical disturbances, Requirement R4 should be removed. Failure to properly report events is currently sanctionable under CIP-001-1 and EOP-004-1 and will continue to be sanctionable under proposed EOP-004-2. Entities are capable of implementing procedures appropriate to ensure compliance with the actual reporting requirements without the addition of this "test." Alternately, if this requirement for annual tests is retained, it should be supplemented with a detailed example of an acceptable test and acceptable documentation of the test to avoid future compliance and enforcement issues. Stating "evidence may include, but is not limited to..." provides broad and unnecessary opportunity for future compliance and enforcement issues. Any difficulty the committee might encounter in developing such a detailed example would be instructive of the probable compliance and issues that would ensure from implementation of the requirement.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The requirement is written so that it is not prescriptive and allows the entity flexibility in how it tests its communications process.		
BGE	No	Requirement 3 (formerly R4) should be removed altogether because it is covered by the new R4. The topic of Disturbance Reporting is covered several times each year during operator training classes and the operators are tested on the material. Actual issued Disturbance Reports throughout the year are also covered during training class.
Response: The DSR SDT thanks you for your comment. R4 was a training requirement which has been revised and incorporated into Requirement R1, Part 1.5. This now calls for an annual review of the Operating Plan rather than training. The intent of the review is to ensure that the plan is up to date.		
Georgia System Operations Corporation	No	-With the current CAN on the definition of annual, we do not believe that the additional qualification that the test shall be conducted "with no more that 15 calendar months between tests" is necessary. Although we understand the additional qualification

Organization	Yes or No	Question 8 Comment
Response: The DSR SDT thanks you for your comment. The CAN language defers to the standard drafting team for any qualifications on "annual." The DSR SDT prefers the existing language.		
Indeck Energy Services	No	For smaller entities, for which few of the Attachment 1 events apply (eg a 75 MW wind farm), a drill is overkill. Reviewing the procedure during training should be sufficient. The solution is to require a drill for any entity for which any of the Attachment 1 events would cause a Reportable Disturbance or reportable DOE OE-417 event and training review for any other entities. The Violation Risk Factor should be Low, if any, because this is historical reporting, with little or no reliability consequence.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. Any drill or exercise that meets the intent of the requirement is acceptable. **VRF:** With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
ExxonMobil Research and Engineering	No	The annual (15 month) time window for conducting annual performance tests appears to be reasonable. However, the required scope of the test is vague. The Standard Drafting Team should modify the testing requirement to include boundary criteria such as whether notifications to third parties and law enforcement are required or if the test is limited to internal notifications and response processes. Furthermore, the current measure associated with this requirement, EOP-004 Revision 2 Measure 3, implies, that if an Impact Event occurs, the registered entity can count the activation of its Impact Event Operating Plan as a test and extend the test window 15 months from the date of activation. The Standard Drafting Team should revise the requirement to clarify that the test window resets when a site initiates its Impact Event Operating Plan in response to a real Impact Event as requirement criteria should not be included in a measure.

Organization	Yes or No	Question 8 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. It is expected that such a test will include all aspects of the communications process. The measure was revised to clarify that an actual event can be used in lieu of a test.		
Occidental Power Marketing	No	We understand that this requirement is meant to comply with FERC Order 693, Section 466; however, there needs to be more specificity concerning what sort of "test" would be accepted for auditing purposes. Also, only LSEs with BES assets should be included in the Applicability section of the standard.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The requirement is written so that it is not prescriptive and allows the entity flexibility in how it tests its communications process.		
Lincoln Electric System	No	As currently drafted, requirement R3 states one must “conduct a test” whereas the associated Measure requests evidence that one “conducted a mock Impact Event.” The Rationale box lends to further confusion by referencing a “drill or exercise” as a process to verify one’s Operating Process. To avoid potential confusion between R3 and M3, as well as to maintain consistency with the Rationale box, recommend the drafting team replace the word “test” with “drill or exercise” within R3 and the associated Measure.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. It is not a common practice to include explanatory text in a requirement. The Results-based standards format allows the Rationale boxes to serve this role. The Rationale box includes language that indicates that an actual implementation of the plan counts as a test.		
Farmington Electric Utility System	No	The measure for R3 indicates an actual Impact Event would count as a test, consider aligning the requirement with the measure to clarify an Impact Event could be considered a test.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. It is not a common practice to include explanatory text in a requirement. The Results-based standards format allows the Rationale boxes to serve this role. The Rationale box includes language that indicates that an actual implementation of the plan counts as a test.		

Organization	Yes or No	Question 8 Comment
Ingleside Cogeneration LP	No	Since the reporting of event data to regulatory agencies does not support a front-line operations capability to mitigate or restore a BES impairment, regular simulations are not needed. Those notification items which test coordination between operating entities can be addressed in emergency operations exercises.
Response: The DSR SDT thanks you for your comment. We concur with your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event.		
Constellation Power Generation	No	As CPG stated in comments to earlier versions of EOP-004-2, this requirement adds a substantial compliance burden with little to no reliability improvement to the BES. Numerous entities in the NERC footprint have created fleet wide compliance programs for their facilities, instead of overseeing multiple stand alone compliance programs. This was done not just for the ease of administration, but it also greatly improves the reliability of the BES by ensuring consistency across multiple facilities. By requiring each responsible entity to test the Operating Process, those under a fleet wide compliance program will end up testing the same Operating Process numerous times. This would be inefficient, ineffective and unnecessarily costly. If the testing requirement remains, then the Responsible Entity should be able to take credit for testing of the Operating Process regardless of which entity in the fleet tested it. Alternatively, the drafting team should consider removing Requirement 3 (formerly R4) because in practice it is covered by the new R4. As discussed below R4 needs refinement, but the topic of Disturbance Reporting is covered during annual training.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. If the intent of this requirement is fulfilled by another exercise or drill conducted by the responsible entity, then that will meet the requirement.		
Duke Energy	Yes	We understand that the objective of this requirement is to test the Operating Process for communicating Impact Events; and that such test could be an actual exercise, a formal review, or a real-time implementation. But given that R1.4 requires updating the Operating Plan within 90 days of any changes, we believe the VRF for R3 should be LOW instead of MEDIUM.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a “lower” VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is		

Organization	Yes or No	Question 8 Comment
responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Progress Energy	Yes	Do all individuals who are assigned roles and responsibilities in the Impact Event Operating Plan have to be involved with the test each time? Since there are multiple different types of Impact Events, it seems likely that only a subset of those Impact Events would be tested during an annual test, and therefore only a subset of individuals with responsibilities in the Impact Event Operating Plan would participate. For example, one test may exercise the Operating Process for properly reporting damage to a power plant that is a Critical Asset, and personnel from the Distribution Provider would not be involved in that test. Would such a scenario meet the requirement for the annual test? If so, it seems that some aspects of the Plan may never actually be required to be tested. This is ok, since R4 requires an annual review with personnel with responsibilities in the Impact Event Operating Plan. It must be made clear what is required in the annual test.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The requirement is written so that it is not prescriptive and allows the entity flexibility in how it tests its communications process.		
Manitoba Hydro	Yes	This requirement appears to be written so as to leave how each entity tests this procedure is up to them and not how. The testing of this procedure could vary vastly from entity to entity, meaning there is no set protocol on this procedure. As long as this requirement remains open, it is fair.
Response: The DSR SDT thanks you for your comment.		
United Illuminating Co	Yes	: FERC did state in Order 693 that the reporting procedure requires testing. UI is concerned that the scope of the requirement is unspecified. Does the exercise require only one type of Impact Event to be exercised per period, or is an entity required to simulate each Impact Event and notification
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. If your communications process differs by event type, then all communications should be tested.		

Organization	Yes or No	Question 8 Comment
Southern Company	Yes	This will cause all of the entities listed in R1.3.2 to receive test communications from all of the applicable entities annually.
Response: The DSR SDT thanks you for your comment. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The standard now has only three requirements. The requirement to test the communications process is important so that any issues or errors in the Operating Plan can be identified. This will allow for reporting to the appropriate entities in the case of an actual event.		
SRP	Yes	
SDG&E	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
Arkansas Electric Cooperative Corporation	Yes	
Platte River Power Authority	Yes	
Alliant Energy	Yes	
CenterPoint Energy	Yes	
USACE	Yes	
Independent Electricity System Operator	Yes	
PPL Electric Utilities	Yes	
American Transmission Company	Yes	

Organization	Yes or No	Question 8 Comment
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	
Brazos Electric Power Cooperative	Yes	
Midwest Reliability Organization	Yes	
Western Electricity Coordinating Council	Yes	
Pacific Northwest Small Public Power Utility Comment Group	Yes	
PSEG Companies	Yes	
Pepco Holdings Inc and Affiliates	Yes	

9. Do you agree with the proposed revisions to Requirement 5 (now R4)? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: A significant number of commenters indicated that there was confusion surrounding the use of the term "review" in Requirements R3 and R4. Similar comments suggested that the measure for Requirement R4 has a training connotation, which is inconsistent with the language in the requirement, which uses the term "review." The DSR SDT has eliminated Requirement R4 and added a part to Requirement 1, Part 1.5, to require a process for ensuring that the event Operating Plan is reviewed at least annually, with no more than 15 calendar months between review sessions. Eliminating R4 and adding Part 1.5 maintains the intent while eliminating potential confusion and redundancy.

Other commenters suggested revisions to the use of the term annual. The DSR SDT reviewed the NERC definition of Annual as defined in the NERC Compliance Application Notice (CAN) CAN-0010, which provides drafting teams latitude to define the term within a requirement as they intend it to be used.

Organization	Yes or No	Question 9 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation	No	We do not believe that the requirement should specify that the plan must be reviewed with those personnel who have responsibilities identified in that plan as there is no requirement in R1 that the plan must identify any specific personnel responsibilities. Additionally, we seek clarification on whether review in this instance means train as indicated in the measure.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated requirement R4 and added a Part under Requirement R1, to require a process for ensuring that the event Operating Plan is reviewed at least annually, with no more than 15 calendar months between review sessions. By adding this Part to Requirement R1, the SDT has eliminated confusion and redundancy around the use of the term "review" and the training connotation in the Measure.		
Dominion	No	The need to periodically review its Impact Event Operating Plan has not been established and is overly restrictive (annually) given that the purpose of the standard is to report Impact Events. Suggest removing this requirement
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated requirement R4 and added a Part under Requirement R1, to require a process for ensuring that the event Operating Plan is reviewed at least annually, with no more than 15 calendar months between review sessions. The DSR SDT		

Organization	Yes or No	Question 9 Comment
's intent is to ensure that there is no gap in the review of the Operating Plan even though the plan has provision(s) for updating the event Operating Plan within 90 days of any change to its content. By adding this Part to Requirement R1, the SDT has eliminated confusion and redundancy around the use of the term "review" and the training connotation in the Measure.		
SPP Standards Review Group	No	There is confusion surrounding the use of the term review in R3 and R4. In R3 and the suggested revision to M3 in Question 8, review is an analysis of the plan by a specific group tasked to determine if the plan requires updating or modifying to remain viable. Review in R4 has training connotations for all personnel who have responsibilities identified in the plan. Although we understand the use of review in R4 is new to this version of EOP-004-2, we believe it may be more appropriate to use training rather than review in R4. And further, we feel the training should be focused on those specific portions of the plan that apply to specific job functions.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated Requirement R4 and added a Part under Requirement R1, to require a process for ensuring that the event Operating Plan is reviewed at least annually, with no more than 15 calendar months between review sessions. By adding this Part to Requirement R1, the SDT has eliminated confusion and redundancy around the use of the term "review" and the training connotation in the Measure.		
FirstEnergy	No	We believe that Requirement 4 does not warrant a Medium risk factor. For example, a simple review of the process does not have the same impact on the Bulk Electric System as the implementation of the Operating Plan per R2. Therefore, we believe R4 is at best a Low risk to the BES.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated Requirement R4 and has re-evaluated the Violation Risk Factors for each requirement. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
We Energies	No	Include that this is for internal personnel as stated in the associated measure.

Organization	Yes or No	Question 9 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated Requirement R4 and the associated Measure.		
Compliance & Responsibility Organization	No	See comments set forth in number 2
Response: Thank you for your comments and suggestions. Please see responses to question 2.		
Exelon	No	Need more guidance on what personnel are expected to participate in the annual review. Training for all participants in a plan should not be required. Many organizations have dozens if not hundreds of procedures that a particular individual must use in the performance of various tasks and roles. Checking a box that states someone read a procedure does not add any value. This is an administrative burden with no contribution to reliability. If the intention is that internal personnel who have responsibilities related to the Operating Plan cannot assume the responsibilities unless they have completed training. This requirement places an unnecessary burden on the registered entities to track and maintain a database of all personnel trained and should not be a requirement for job function. A current procedure and/or operating plan that addresses each threshold for reporting should provide adequate assurance that the notifications will be made per an individual's core job responsibilities.
Response: Thank you for your comments. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The requirement is written so that it is not prescriptive and allows the entity flexibility in how it tests its communications process.		
City of Tallahassee (TAL)	No	The verbiage at least annually, with no more than 15 months between review sessions is an attempt to define annually. If you want every 15 months say at least every 15 months. Otherwise just say annual and let the entities decide what that is, as is being done with other annual requirements.
Response: Thank you for your comment. The DSR SDT took into consideration the CAN on the definition of 'Annual" and wrote the requirement to meet the intent of the team.		
Tenaska	No	The proposed Impact Event Operating Plan should not be required.
Response: The DSR SDT thanks you for your comment. The DSR SDT considers the proposed event Operating Plan a document that identifies the activities to achieve the purpose to improve industry awareness and the reliability of the Bulk Electric System. The DSR SDT has revised R1 to only include development of an Operating Plan that includes the sub-requirements of R1.		

Organization	Yes or No	Question 9 Comment
American Municipal Power	No	No, remove R4. R4 is not an acceptable requirement nor should this be an operation. Focusing on a plan and personnel tracking is overly prescriptive. The only requirement should be to have an entity submit a report. Let the entity decide how they want to implement the reporting.
Response: The DSR SDT thanks you for your comment. The DSR SDT has taken into consideration your comment, eliminated Requirement R4, and added Requirement R1, Part 1.5. The SDT agrees that the Registered Entity can decide on the how to implement the reporting; however, this requirement mandates that the Registered Entity document its process.		
Liberty Electric Power LLC	No	Again, the entity should determine the need for review of any procedure. Changing circumstances may dictate a shorter cycle, but no changes could dictate a longer review. I will note that spill prevention plans are required to be reviewed every five years, so I question the need for an 18-month review of the EOP plan.
Response: The DSR SDT thanks you for your comment. The review provisions are designed to ensure that contact information for internal and external organizations are correct and up to date.		
Arkansas Electric Cooperative Corporation	No	We appreciate the effort the team has taken in improving the requirements since the last posting. We request the team clarify if this also includes personnel observing and reporting the requirements or only those specifically listed in the plan. The measure seems to indicate it only includes those listed in the plan, but this is not clear in the requirement. If it includes those personnel involved in observing and notifying management, then this might include a significant portion of the organization. In either case, we feel the requirement should be modified as "review applicable portions of its Impact Event Operating Plan....
Response: The DSR SDT thanks you for your comment. The training provisions of the standard have been removed. The DSR SDT intent is to ensure that the Registered Entity has Operating Plan(s) for the identification of events, establishing which internal personnel are involved, identification of outside agencies to be notified, and having a provision for updating the plan(s). The SDT feels that current Sabotage Reporting guidelines already provide much of the information needed in the new R1.		
Calpine Corp	No	Failure to properly report events is currently sanctionable under CIP-001-1 and EOP-004-1 and will continue to be sanctionable under proposed EOP-004-2. Entities are capable of implementing procedures appropriate to ensure compliance with the actual reporting requirements without the addition a formal requirement to annually review their internal procedures with personnel. In the unlikely event that an entity cannot attain this level of operating competence without implementation of a new requirement, such Entities would be subject to enforcement under Requirement R5. Absent substantial evidence of systemic problems by Entities in contacting local law enforcement properly or failures to complete event reports to appropriate agencies when provided with clear guidance on the events to be reported, this requirement is unnecessary.

Organization	Yes or No	Question 9 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Requirement R2 and revised Requirements R1 and R5 to address your concern. Requirement R5 (now R2) reads: R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
ExxonMobil Research and Engineering	No	Its unclear whether R4 is a training requirement to train all individuals who may be required to implement its Impact Event Operating Plan on an annual basis or a requirement for an Entity to review the Impact Event Operating Plan with at least one person from each position that has a role in the Impact Event Operating Plan in order to complete a quality review of the Impact Event Operating Plan. The SDT should clarify the intent of the requirement. If the intent is that both of the aforementioned interpretations is expected to occur, the SDT should break R4 into two requirements so that an entity is not violation of Requirement R4 when the entity fails to comply with one of the two imbedded requirements (e.g. if the quality review is not performed but all individuals were trained).
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Requirement R4 and added a new Part 1.5 under R1 to address your concern. Part 1.5 calls for an annual review of the plan.		
Constellation Power Generation	No	The purpose of this requirement as currently worded is unclear. It seems to insinuate that a formal review of the Operating Plan takes place annually, and that any and all personnel identified in the plant are part of the review. If that is correct, than CPG believes this requirement is echoing Requirement 3. These two requirements can be incorporated into one. Furthermore, the Measure for R4 is too prescriptive, going so far as to specifically describe how this formal review should take place. It even states that the Responsible Entity needs to present documentation showing that the personnel in the plan were trained, yet there is no requirement for training. CPG would like the DSR SDT to revisit the purpose and intent of this requirement, alone and in concert with R3. If there are indeed similar then consolidate them into one requirement.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Requirement R4 and added a new Part 1.5 under R1 to address your concern. Part 1.5 calls for an annual review of the plan.		
Georgia System Operations Corporation	No	With the current CAN on the definition of annual, we do not believe that the additional qualification that the test shall be conducted "with no more that 15 calendar months between reviews" is necessary. Remove "with no more that 15 calendar months between reviews.
Response: The DSR SDT thanks you for your comment. The SDT has revised the term annual to align with the definition in the NERC Compliance Application		

Organization	Yes or No	Question 9 Comment
Notice (CAN) CAN-0010.		
SERC OC Standards Review Group	Yes	We agree with the concept, but disagree with the use of the term Operating Plan as a defined term in line with our comments in question 6 above.
Response: The DSR SDT thanks you for your comment. The DSR SDT believes that the use of a defined term "Operating Plan" to describe the procedure to identify and report the occurrence of a disturbance is appropriate and has revised Requirement R1 to remove the terms Operating Process and Operating Procedure to eliminate confusion.		
PJM Interconnection LLC	Yes	1. We agree with the concept but disagree with the use of the term Operating Plan as a defined term in line with our comments to Question 6 above. 2. R4 attempts to define Annual for the Registered Entity to review its Impact Operating Plan. We believe R4 should follow the NERC definition of Annual as defined in the NERC Compliance Application Notice (CAN) CAN-0010 Definition of Annual as opposed to creating a new definition of Annual or refer to an entities defined use of the term annual.
Response: The DSR SDT thanks you for your comment. Please see responses to question 6 above. The DSR SDT reviewed the NERC definition of Annual as defined in the NERC Compliance Application Notice (CAN) CAN-0010. The NERC CAN provides drafting teams latitude to define annual within a Requirement as they believe is appropriate in the context of a particular standard.		
United Illuminating Co	Yes	As written it is a training burden. Certain persons will have only one step in one operating procedure to perform. There is no necessity to review the entire Operating Plan with them. For example, Field Personnel need to know that if they see something not right to report it immediately. In this instance there is no benefit to review the Operating Procedure/Process for firm load shedding with them.
Response: The DSR SDT thanks you for your comment. The training requirement has been removed. The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized events is correct so that the entity can respond appropriately in the case of an actual event. The DSR SDT has removed R4 to eliminate potential confusion and redundancy around the training connotation.		
Manitoba Hydro	Yes	Removing the extreme details within 30 days of revision and train before given responsibility and giving leeway to when this training is necessary, will allow training to be integrated into other existing training schedules. Inclusion of 5.3 and 5.4 would require unique set of time lines and additional resources to monitor and implement.
Response: The DSR SDT thanks you for your comment. The training provisions of the standard have been removed.		

Organization	Yes or No	Question 9 Comment
Occidental Power Marketing	Yes	However, only LSEs with BES assets (or assets that directly support the BES) should be included in the Applicability section of the standard.
Response: The DSR SDT thanks you for your comment. Attachment 1 specifies which types of events are required to be reported by each entity. LSE is included here due to CIP-002-3 applicability.		
Farmington Electric Utility System	Yes	A review of the Impact Event Operating Plan can be interrupted as an informal examination of the plan. The measure for R4 indicates evidence of a review, parties conducting the review AND when internal training occurred. It should be clarified in R4 training is expected as part of the review for personnel with responsibilities. This is an improvement from the previous 5.3 and 5.4, however, the team should consider adding back, and review/training shall be conducted prior to assuming the responsibility in the plan.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Requirement R4 and added a new Part 1.5 under R1 to address your concern. Part 1.5 calls for an annual review of the plan.		
Ingleside Cogeneration LP	Yes	Yearly refresher training on the reporting process is appropriate. Ingleside Cogeneration also agrees that a review with those individuals with assigned responsibilities under the Operating Plan is a better way to frame the requirement.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Requirement R4 and added a new Part 1.5 under R1 to address your concern. Part 1.5 calls for an annual review of the plan.		
Indeck Energy Services		R4 is redundant with R3 and should be deleted. The Violation Risk Factor should be Low, if any, because this is historical reporting, with little or no reliability consequence.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted Requirement R4 and revised R3. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the		

Organization	Yes or No	Question 9 Comment
approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Northeast Power Coordinating Council	Yes	
Bonneville Power Administration	Yes	
Midwest Reliability Organization	Yes	
Western Electricity Coordinating Council	Yes	
Pacific Northwest Small Public Power Utility Comment Group	Yes	
PSEG Companies	Yes	
Pepco Holdings Inc and Affiliates	Yes	
Midwest ISO Standards Collaborators	Yes	
Southern Company	Yes	
SRP	Yes	
SDG&E	Yes	
New Harquahala Generating Co.	Yes	

Organization	Yes or No	Question 9 Comment
APX Power Markets	Yes	
Sweeny Cogeneration LP	Yes	
American Electric Power	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Independent Electricity System Operator	Yes	
ISO New England, Inc	Yes	
Platte River Power Authority	Yes	
BGE	Yes	No comments.
Alliant Energy	Yes	
CenterPoint Energy	Yes	
PPL Electric Utilities	Yes	
Lincoln Electric System	Yes	
American Transmission Company	Yes	
Duke Energy	Yes	
City of Tacoma, Department	Yes	

Organization	Yes or No	Question 9 Comment
of Public Utilities, Light Division, dba Tacoma Power		
Brazos Electric Power Cooperative	Yes	
Progress Energy	Yes	

10. Do you agree with the proposed revisions to Requirement 6 (now R5) and the use of either Attachment 2 or the DOE-OE-417 form for reporting? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: The slight majority of commenters suggested revisiting R2 and R5 to eliminate potential redundancy and confusion. The intent of the two requirements is to have entities utilize the DOE Form OE-417 to report events listed on Attachment 1. If the entity completes DOE Form OE-417 to report an event, it does not have to transcribe the same information onto Attachment 2 but may be required to submit the form to the DOE and NERC. By eliminating R2 and revising R5 (now R2), the DSR SDT has maintained the intent of the requirements.

R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.

Organization	Yes or No	Question 10 Comment
Northeast Power Coordinating Council	No	R5 stipulates the use of Attachment 2 or the DOE-417, which is the vehicle for reporting only. This is the how part, not the what. The vehicle for reporting can easily be included in ***R2 where an entity is required to implement (execute) the Operating Plan upon detection of an Impact Event***. Suggest combining R2 with R5.
Response: The DSR SDT thanks you for your comment. The DSR SDT has also eliminated R2 and revised R5 (now R2) for clarity and to eliminate potential redundancy. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
Dominion	No	Dominion does not agree because the Requirement is too restrictive giving the Responsible Entity the choice on reporting forms as either Attachment 2 or DOE OE-417. The use of Attachment 2 or DOE OE-417 may be appropriate when reporting to NERC, however, Requirement R 1.3.2 requires the Responsible Entities Impact Event Operating Plan to address notifications to non-NERC entities such as Law Enforcement or Governmental Agencies. It is likely that these organizations have specific reporting requirements or forms that will not line up the options prescribed in Requirement R5.Suggest revising Requirement R5 to not require the use of these two forms as the only options. If these 2 forms are used, suggest aligning the Event names in Attachment 1 to be similar to the criteria for filing event names in the DOE OE-417 to allow for consistency.

Organization	Yes or No	Question 10 Comment
		Also suggest aligning the time to submit for similar event names in each form.
Response: The DSR SDT thanks you for your comment. The DSR SDT has revised Attachment 1 to indicate that entities must submit Attachment 2 or the DOE OE-417 form. This information was contained in Requirement 5. The intent of the two requirements is to have entities make appropriate notifications and report events contained in Attachment 1. By eliminating R2 and revising R5 (now R2), the DSR SDT has maintained the intent of the requirements while eliminating potential confusion and redundancy. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1. The DSR SDT has enhanced Attachment 1 and clarified the intent of each event, threshold and reporting time limits. The DSR SDT removed the column, Time to Submit Report and replaced it with Submit Attachment 2 or DOE OE-417 Report.		
SPP Standards Review Group	No	We feel there is redundancy between R2 and R5. To eliminate this redundancy, we propose to take the phrase using the form in Attachment 2 or the DOE OE-417 reporting form and adding it at the end of R2. Then what is left of R5 could be deleted. The new R2 would read Each Responsible Entity shall implement its Impact Event Operating Plan documented in Requirement R1 for Impact Events listed in Attachment 1 (Parts A and B) using the form in Attachment 2 or the DOE OE-417 reporting form.?
Response: The DSR SDT has revised Attachment 1 to indicate that entities must submit Attachment 2 or the DOE OE-417 form. This information was contained in Requirement 5. The intent of the two requirements is to have entities make appropriate notifications and report events contained in Attachment 1. By eliminating R2 and revising R5 (now R2), the DSR SDT has maintained the intent of the requirements while eliminating potential confusion and redundancy. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
Midwest ISO Standards Collaborators	No	Requirement 2 and Requirement 5 appear to be very similar. Requirement 2 requires implementation of the Operating Plan, Operating Process and/or Operating Procedure in Requirement 1. The Operating Procedure requires gathering and reporting of information for the form in Attachment 2. What does Requirement 5 add that is not already covered in Requirement 2 except the ability to use the DOE OE-417 reporting form which
Response: The DSR SDT thanks you for your comment. The intent of the two requirements is to have entities utilize the DOE Form OE-417 to report events listed on Attachment 1. If the entity completes DOE Form OE-417 to report an event, they do not have to transcribe onto attachment 2 but may be required to submit it to the U.S. Department of Energy (DOE) and NERC. By eliminating R2 and revising R5 (now R2), the DSR SDT has maintained the intent of the requirements. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
FirstEnergy	No	We believe that Requirement 5 does not warrant a Medium risk factor. Not using a particular form is strictly

Organization	Yes or No	Question 10 Comment
		administrative in nature and the VRF should be Low.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
PJM Interconnection LLC	No	R5 seems redundant as R2 already requires an entity to report any Impact Events by executing/implementing its Impact Event Operating Plan. R5 merely stipulates the use of Attachment 2 or DOE-417, which an entity automatically would use for reporting purposes while implementing its Impact Event Operating Plan.
Response: The DSR SDT thanks you for your comment. The intent of the two requirements is to have entities utilize the DOE Form OE-417 to report events listed on Attachment 1. If the entity completes DOE Form OE-417 to report an event, they do not have to transcribe onto attachment 2 but may be required to submit it to the U.S. Department of Energy (DOE) and NERC. By eliminating R2 and revising R5 (now R2), the DSR SDT has maintained the intent of the requirements. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
Exelon	No	Agree that each Responsible Entity should be able to use either Attachment 2 or the DOE OE-417 form for reporting; however, a GO/GOP will not have the ability to respond to Attachment 2 Task numbers 8, 9, 10, 11, and 12. Suggest that the DSR SDT either evaluate a shortened form version, provide a note or provision for "N/A" based on registration, or revise form to be submitted by the most knowledgeable functional entity (e.g., TOP or RC).Need clear guidance as to which form is to be used for which Impact Event, we feel that one and only one form should be used to eliminate confusion. Attachment 2 has an asterisk on #s 7, 8, 9, 10 and 11 there is not reference corresponding to it.
Response: The DSR SDT thanks you for your comment. The DSR SDT has updated Attachment 2 to per comments received.		

Organization	Yes or No	Question 10 Comment
Tenaska	No	R5 should be changed to Each Responsible Entity shall report Impact Events listed in Attachment 1 using the form in Attachment 2 or the DOE OE-417 reporting form. This revised version of the proposed R5 is the only Requirement that is necessary to achieve the stated purpose of Project 2009-01. The proposed R1 through R4 should be deleted and R5 should be changed to R1.
Response: The DSR SDT thanks you for your comment. The SDT agrees the reporting is a fundamental aspect, but the operation plans are integral piece of the BES. The DSR SDT believes that the revisions created will provide clarity for the requirements. Please see the revised standard.		
American Municipal Power	No	R5 is not an acceptable requirement, but it can be improved. Each Responsible Entity shall report "Impact Events" to _____ (address specified in attachment 1, website, entity, email address, or fax, etc.) Focusing on a plan and procedure is overly prescriptive. The only requirement should be to have an entity submit a report. Let the entity decide how they want to implement the reporting.
Response: The DSR SDT thanks you for your comment. The DSR SDT has eliminated R2 and revised R5 (now R2) for clarity and to eliminate potential redundancy. The SDT agrees that the Registered Entity can decide on the how to implement the reporting; however, this requirement mandates that the Registered Entity document its process. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
Arkansas Electric Cooperative Corporation	No	We appreciate the effort the team has taken in improving the requirements since the last posting. For R5, we suggest including the reporting form as part of the plan in R1. Otherwise, a violation of R5 would also indicate a violation of R2.
Response: The DSR SDT thanks you for your comment. The DSR SDT has also eliminated R2 and revised R5 (now R2) for clarity and to eliminate potential redundancy. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
American Electric Power	No	This should be one-step covered by the implementation in requirement 2. We like the ability to use one form (i.e. NERC Attachment 2 or the DOE-417); however, we would prefer to have this information only be reported once.
Response: The DSR SDT thanks you for your comment. EOP-004-2 allows entities to utilize the DOE Form OE-417 to report events listed on Attachment 1. If the entity completes DOE Form OE-417 to report an event, they do not have to transcribe onto attachment 2 but may be required to submit it to the U.S. Department of Energy (DOE) and NERC.		

Organization	Yes or No	Question 10 Comment
Consumers Energy	No	We understand that DOE is migrating to an on-line reporting facility rather than the email-submitted OE-417. If they do so, Form OE-417will not be available for providing to NERC, and the reporting specified by EOP-004 will be duplicative of that for DOE. We recommend that NERC, RFC and the DOE work cooperatively to enable a single reporting system in which on-line reports are made available to all appropriate parties.
Response: The DSR SDT thanks you for your comment. The SDT agrees with the concept of the single reporting template and is working with other agencies to see if the single form would be achievable.		
Independent Electricity System Operator	No	R5 stipulates the use of Attachment 2 or the DOE-417, which is the vehicle for reporting only. This is the how part, not the what. The vehicle for reporting can easily be included in R2 where an entity is required to implement (execute) the Operating Plan upon detection of an Impact Event. We suggest the SDT combine R2 with R5.
Response: The DSR SDT thanks you for your comment. The DSR SDT has also eliminated R2 and revised R5 (now R2)for clarity and to eliminate potential redundancy. R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.		
Ameren	No	The "Responsible Entity" should be limited to those functions with the most oversight such as the BA, RC, or TOP. Otherwise there will be multiple DOE OE-417 reports sent by multiple entities.
Response: Thank you for your comments. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received.		
ISO New England, Inc	No	R5 stipulates the use of Attachment 2 or the DOE-417, which is the vehicle for reporting only. This is the how part, not the what. The vehicle for reporting can easily be included in R2 where an entity is required to implement (execute) the Operating Plan upon detection of an Impact Event. We suggest the SDT combine R2 with R5.
Response: The DSR SDT thanks you for your comment. The DSR SDT has also eliminated R2 and revised R5 (now R2) for clarity and to eliminate potential redundancy.		
Calpine Corp	No	The use of DOE OE-417 is acceptable, but the language of Requirement R5 should be modified. The disturbance event form must be filled out correctly, irrespective of the requirements of an Entities Impact Event Operating Plan. Reference to that Plan does not add clarity to the requirement to report events. The

Organization	Yes or No	Question 10 Comment
		requirement should delete the reference to the Impact Event Operating Plan? and simply state: Each Responsible Entity shall report events listed in Attachment 1 using the provided form, or where also required to complete the current version of DOE OE-417, that form. Although one of the primary stated purposes of the original SAR was to simplify the reporting process by creating a single form, the fact that some entities are already required to report substantially identical information to DOE argues for retention of the use of the DOE form.
Response: The DSR SDT thanks you for your comment. DSR SDT has deleted requirement 2 and revised requirements R1 and R5 (now R2) to address your concern. The entire Attachment 1 has been updated to reflect the comments that were received.		
BGE	No	Language needs to be more specific on when to use Attachment 2 or DOE-OE-417.
Response: The DSR SDT thanks you for your comment. Attachment 2 should be the normal reporting vehicle unless the entity is required to submit an OE-417 to the DOE. This keeps the entity from having to file two distinctly different reports for the same event.		
Alliant Energy	No	We believe Attachment 2 should be deleted, and NERC should work with the DOE to have one form for all events, if possible. It makes the reporting procedure much simpler, only having to use one form.
Response The DSR SDT thanks you for your comment. EOP-004-2 allows entities to utilize the DOE Form OE-417 to report events listed on Attachment 1. If the entity completes DOE Form OE-417 to report an event, they do not have to transcribe onto attachment 2 but may be required to submit it to the U.S. Department of Energy (DOE) and NERC. The DSR SDT is currently working with the DOE to make revisions to Form OE-417 that would achieve the objective of your comment. We will continue to pursue this.		
ExxonMobil Research and Engineering	No	The notification requirement and documentation in Attachment 1 do not clearly identify which entities need to be notified for each type of event detailed in Attachment 1. While it makes sense to notify the Reliability Coordinator, NERC, Regional Entity, Law Enforcement and other Governmental Agencies for sabotage type events, it does not seem proper to notify Law Enforcement agencies of a system disturbance that is unrelated to improper human intervention. Furthermore, it is our belief that a time frame of 1 hour is a short window for making a verbal notification to third parties, and an impossibly short window for requiring the submittal of a completed form regardless of the simplicity. When a Petrochemical Facility experiences an impact event, the initial focus should emphasize safe control of the chemical process. For those cases where registered entities are required to submit a form within 1 hour, the Standard Drafting Team should alter the requirement to allow for verbal notification during the first few hours following the initiation of an Impact Event (i.e. allow the facility time to appropriately respond to and gain control of the situation prior to making a notification which may take several hours) and provide separate notifications windows for those parties that will need to respond to an Impact Event immediately and those entities that need to be informed that one occurred for the

Organization	Yes or No	Question 10 Comment
		purposes of investigating the cause of and response to an Impact Event. For example, a GOP should immediately notify a TOP when it experiences a forced outage of generation capacity as soon as possible, but there is no immediate benefit to notify NERC when site personnel are responding to the event in order to gain control of the situation and determine the extent of the problem. The existing standards requirement to file an initial report to entities, such as NERC, within 24 hours seems reasonable provided that proper real time notifications are made and the Standard Drafting Team reinstates EOP-004 Revision 1's Requirement 3.3, which allows for the extension of the 24 hour window during adverse conditions, into the requirement section of EOP-004 [the current revision locates this extension in Attachment 1, which, according to input received from Regional Entities, means that the extension would not be enforceable].
Response: The DSR SDT thanks you for your comment. The SDT envisions that each Registered Entity will develop Operating Plan(s) appropriate to meet its obligations as outlined in the standard. The SDT doesn't feel it necessary to prescribe to the Registered Entity any particular interpretation on how to achieve compliance, including who the information should be reported to. The entire Attachment 1 has been updated to reflect the comments that were received.		
American Transmission Company	No	Attachment 2, Task #14 in the report should be modified to read, Identify any known protection system misoperation(s). If this report is filed quickly, there is not enough time to assess all operations to determine any misoperation. As a case in point, it typically takes at least 24 hrs. to receive final lightning data; therefore, not all data is available to make a proper determination of a misoperation
Response: The DSR SDT thanks you for your comment. The entire Attachment 1 has been updated to reflect your comment.		
Constellation Power Generation	No	The requirements for filling out the DOE-OE-417 form are not necessarily the same as the requirements prescribed in Attachment 1. CPG suggests that the drafting team create a new requirement, spelling out when an entity is required to complete the DOE-OE-417 form.
Response: The DSR SDT thanks you for your comment. Any entity that is obligated to submit Form OE-417 may submit that completed form to NERC in lieu of Attachment 2.		
Georgia System Operations Corporation	No	R5: This standard should not require all Responsible Entities to report the same event. Entities should be allowed to report in a hierarchical manner. They should be allowed to coordinate impact event plans and include in their plans the entity that has the responsibility for reporting various events. Flexibility should be allowed to provide different reporting entities depending on the type of event. In R5, does each Responsible Entity shall report Impact Events in accordance with the Impact Event Operating Plan? Allow this hierarchical reporting and flexibility? An entity should be allowed to report to another operating entity by whatever reporting form or mechanism works and then the other entity reports to NERC using the required NERC or DOE form. Add "To the extent that a Responsible Entity had an Impact Event," at the beginning of R5 and

Organization	Yes or No	Question 10 Comment
		M5.
Response: The DSR SDT thanks you for your comment. Each entity is required to report their portion of the event, however they can coordinate. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, will be able to provide the ERO and others with a different views of what has happened. The DSR SDT understands that there may be multiple reports (for certain events) that are required by different government agencies. NERC will continue to streamline the reporting process as we move into the future. The DSR SDT has also eliminated R2 and revised R5 (now R2) for clarity and to eliminate potential redundancy.		
Indeck Energy Services	No	The Violation Risk Factor should be Low, if any, because this is historical reporting, with little or no reliability consequence.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Bonneville Power Administration	Yes	Reporting form OK. Note that the Frequency Maximum/Minimum Section should be clarified. A Gen Loss doesn't usually experience a high (maximum) frequency, just the low immediately following the event.
Response: The DSR SDT thanks you for your comment		
Midwest Reliability Organization	Yes	This will reduce any double reporting to the ERO and FERC.
PPL Supply	Yes	Reporting consistency and timelines may need to be reviewed for example: Fuel Supply Emergency - OE-417 requires reporting within 6 hours / Attachment 1 Part B requires reporting within 1 hour.
Response: The DSR SDT thanks you for your comment The DSR SDT has significantly revised Attachment 1 and deleted Fuel Supply Emergency from Attachment 1. This item was removed in coordination with the NERC Events Analysis Working Group and the proposed Events Analysis Program. All events are		

Organization	Yes or No	Question 10 Comment
now to be reported within 24 hours with the exception of Destruction of BES equipment, Damage or destruction of Critical Assets and Damage or destruction of Critical Cyber Asset events in Part A and Forced Intrusion, Risk to BES equipment and Detection of a reportable Cyber Security Incident in Part B.		
SERC OC Standards Review Group	Yes	We agree with the concept, but disagree with the use of the term Operating Plan as a defined term in line with our comments in question 6 above.
Response: The DSR SDT thanks you for your comment. The SDT agrees with your viewpoint and believes that your statement is consistent with the intent of the requirement. (refer to question 6)		
United Illuminating Co	Yes	Put it's before Impact Event Operating Plan.
Response: The DSR SDT thanks you for your comment. Please see the revised standard.		
Manitoba Hydro	Yes	The DOE-OE-417 appears more intuitive and descriptive (and on line ability), but having the either or option is fine.DOE-OE-417 Form is mentioned several time in this Standard, but no link to this document.
Response: The DSR SDT thanks you for your comment. Please see the revised standard.		
CenterPoint Energy	Yes	CenterPoint Energy agrees with the idea of streamlining the reporting process through the use of existing report forms. However, as noted in the response to Question 11, the Company has concerns about the DOE OE-417 Form, specifically the timeframes in which to submit reports. CenterPoint Energy will be making the same recommendation to extend reporting timeframes during the DOE OE-417 report revision process when the current form expires on 12/31/11. Any future changes to the DOE Form could also impact reporting for this requirement.
Response: The entire Attachment 1 has been updated to reflect the comments that were received. Footnotes in Attachment 1 have been updated to reflect the comments that the DSR SDT received. The DOE Form OE-417 is under review by the U.S. Department of Energy (DOE) and can be updated or changed without NERC's involvement. The DSR SDT has taken into consideration the use of OE-417 to report events to NERC and agrees that this will fulfill EOP-004-2's reporting requirements.		
PPL Electric Utilities	Yes	We would like to suggest the language be changed such that submission via a NERC system would be acceptable in addition to the use of the Attachment 2 Form or the DOE OE-417 form. The standard would then accommodate the proposed revision to NERC Rules of Procedure 812. NERC will establish a system to collect impact events reports??

Organization	Yes or No	Question 10 Comment
Response: The DSR SDT thanks you for your comment. The SDT expects any system would facilitate the reporting to organizations specified in the submitted report. Until such time that the system can be established, the Registered Entity will be obligated to make the notifications as specified in its Operating Plan(s). The DSR SDT is currently working with the U.S. Department of Energy (DOE) to make revisions to Form OE-417that would achieve the objective of your comment, and will continue to pursue this.		
Ingleside Cogeneration LP	Yes	Although our preference would be to have a single form, Ingleside Cogeneration realizes that is not likely in the near term. We would like to see that remain as a goal of the project team or the ERO.
Response: The DSR SDT thanks you for your comment. The DSR SDT is currently working with the DOE to make revisions to Form Form OE-417that would achieve the objective of your comment, and will continue to pursue this.		
Duke Energy	Yes	There is so much overlap between Attachment 2 and the DOE OE-417 that we believe the DOE OE-417 should be revised to include the additional items that must be reported to NERC, so that there is only one form to submit to NERC and DOE.
Response: The DSR SDT thanks you for your comment. The DSR SDT is currently working with the DOE to make revisions to Form OE-417 that would achieve the objective of your comment, and will continue to pursue this.		
Western Electricity Coordinating Council	Yes	
Pacific Northwest Small Public Power Utility Comment Group	Yes	
PSEG Companies	Yes	
Pepco Holdings Inc and Affiliates	Yes	
Southern Company	Yes	
SRP	Yes	
We Energies	Yes	

Organization	Yes or No	Question 10 Comment
Compliance & Responsibility Organization	Yes	
SDG&E	Yes	
City of Tallahassee (TAL)	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
Liberty Electric Power LLC	Yes	
Sweeny Cogeneration LP	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Platte River Power Authority	Yes	
Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	
Brazos Electric Power Cooperative	Yes	

11. Do you agree with the proposed revisions to Attachment 1? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: Most commenters expressed concerns with the reporting times listed in Attachment 1. Upon review of comments received concerning Attachment 1, the DSR SDT did a thorough review and updated the entire document, along with all Footnotes. The DSR SDT removed the column, Time to Submit Report and replaced it with Submit Attachment 2 or DOE OE-417 Report. There were many noted comments that a one hour reporting time frame does not coincide with an after the fact reporting Standard. The DSR SDT reviewed each time frame to report and has extended most of the time frames to 24 hours. There are a few events that have a one hour reporting requirement that was not changed because these are events that would generally be reported to law enforcement authorities and prompt reporting is in the interest of BES reliability. Duplicate reporting of events was minimized where possible. There are several events that will require reporting by multiple entities to achieve a complete enough picture to facilitate industry awareness.

Organization	Yes or No	Question 11 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation	No	As stated above in response to question 6, we believe that a column should be added to the tables to explicitly indicate what external organizations should receive the communications of a particular Impact Event type. Additionally we have concerns with the following table items: Threshold for reporting Transmission Loss: As stated, this will require the reporting of almost all transmission outages. This is particularly true taking into consideration the current work of the drafting team to define the Bulk Electric System. The loss of a single 115kV network line could meet the threshold for reporting as the definition of Element includes both the line itself and the circuit breakers. Instead, we recommend the following threshold "Three or more BES Transmission lines." This threshold has consistency with CIP-002-4 and draft PRC-002-2. This threshold also needs additional clarification as to the timeframe involved. Is the intent the reporting of the loss of 3 or more BES Transmission Elements anytime within a 24 hour period or must they be lost simultaneously? Also, we recommend that these three losses be the result of a related event to require reporting.Entity with Reporting Responsibility for Loss of Off-site power to a nuclear generating plant (grid supply): The reporting responsibility should clarify that this is only entities included in the Nuclear Plan Interface Requirements.
Response: The DSR DT thanks you for your comment. Upon review the DSR SDT has included a column to indicate the minimum parties who are required to receive the entity's notification. The Threshold for Reporting has been updated to reflect comments that have been received.		
Northeast Power Coordinating	No	As indicated under Question 4, we question the need to include IA, TSP and LSE in the responsible entities

Organization	Yes or No	Question 11 Comment
Council		for reporting.
Response: The DSR DT thanks you for your comment. The DSR SDT has established that CIP-002 and CIP-008 are applicable to an IA, TSP, and LSE. These entities will report a Cyber Security Incident per Attachment 2 (or OE-417) as the vehicle to inform the ERO, their Regional Entity and their Reliability Coordinator.		
Bonneville Power Administration	No	Generally OK, but there are too many events to report. The loss of 3 BES elements for a large geographic entity for a (5 county?) windstorm that has little impact to the system is not needed. 3 elements within the same minute could be acceptable and 6? elements still out within an hour ... or something to that affect could work.
Response: The DSR DT thanks you for your comment. Upon review the DSR SDT has included a column to indicate the minimum parties who are required to receive the entity's notification. The Threshold for Reporting has been updated to reflect comments that have been received.		
Midwest Reliability Organization	No	1) Section 9 of the Impact Reporting Form states: "List transmission facilities (lines, transformers, busses, etc.) tripped and locked out." But Part A of Attachment 1 states: "Three or more BES Transmission Elements." a. Should section 9 state: "List transmission facilities (lines, transformers, busses, etc.) tripped or locked out"? b. Should section 9 state: "List transmission elements (lines, transformers, busses, etc.) tripped or locked out"? This will align the reporting criteria with the actual reporting form.2) Section 13 of the Impact Reporting Form states: "Identify the initial probable cause or known root cause of the actual or potential Impact Event if know at the time of submittal of Part I of this report:." Recommend that "of Part I" be removed since there is no Part 2.3) Every Threshold in attachment 1 gives a clear measurable bright line, except: ?Transmission Loss?. As presently written ?Three or more BES Transmission Elements? could imply that a Report will be required to be submitted if a BES transmission substation is removed from service to perform maintenance. Or there could be three separate elements within a large substation that are out of service (and don?t effect each other) that will require a Report. Upon review of the TPL standards, there are normally planned items that our industry plans for. It is recommended that the Threshold for Reporting of Transmission Loss be enhanced to read: ?Two or more BES Transmission Elements that exceed TPL Category D operating criteria or its successor?. This threshold now is based on a actively enforced NERC Standard, and each RC and TOP are aware of what this bright line is.
Response: The DSR DT thanks you for your comment. Upon review the DSR SDT has included a column to indicate the minimum parties who are required to receive the entity's notification. The Threshold for Reporting has been updated to reflect comments that have been received. Attachment 2 has been updated to reflect the changes noted in your comments and changes per the received comments.		
PPL Supply	No	Recommendation: Add a column in Attachment 1 to acknowledge the events that require a OE-417 Report

Organization	Yes or No	Question 11 Comment
		and list the number under Schedule 1 that required Form OE-417Report. This would add accuracy and consistency among reporting entities.
Response: The DSR DT thanks you for your comment. The DOE Form OE-417 is under review by the DOE and can be updated or changed without NERC's involvement. The DSR SDT has taken into consideration the use of OE-417 to report events to NERC and agrees that this will fulfill EOP-004-2's reporting requirements.		
Pacific Northwest Small Public Power Utility Comment Group	No	The comment group is composed of smaller entities that do not all maintain 24/7 administrative support. While many of the 1 hour reporting thresholds do not affect us, some do. Others may come into play as standards are revised, such as the CIPs. We ask the SDT to consider the identification or verification that starts the clock on these may come at inopportune times for meeting a one hour deadline for these entities. Restoration may be delayed in an attempt to meet these time limits. Safety should always be the number one priority, and restoration and continuity of service second. We see reporting of these events much further down the list. We note that FERC order 693, paragraph 471 does not dictate a specific reporting time period and therefore we suggest timing requirements that promote situational awareness but allow smaller entities needed flexibility. FERC order 693, paragraph 470 directed the ERO to consider ?APPA?s concerns regarding events at unstaffed or remote facilities, and triggering events occurring outside staffed hours at small entities.? Our comment group does not believe the SDT has adequately responded to APPA?s concerns but rather took the 1 hour Homeland security requirement referenced in paragraph 470 verbatim. While a report within an hour might be ideal, it is not always practicable. We suggest: 1) as soon as possible after service has been restored to critical services within the service territory, or 2) By the COB the first business day after discovery. Our comment group realizes the difficulty in wording standards/requirements that lump small entities in with larger ones and we believe our suggestion achieves some balance. Expecting smaller entities to achieve timing requirements that can only be normally met under ideal conditions at large entities is not feasible or fair.
Response: The DSR DT thanks you for your comment. Upon review the DSR SDT has included a column to indicate the minimum parties who are required to receive the entity's notification. The Threshold for Reporting has been updated to reflect comments that have been received. EOP-004-2 requires an entity to "push" information to certain parties for industry awareness. Since this Standard is an after the fact reporting Standard, reporting times for a majority of event types reporting times for a majority of event types have been extended to allow the impacted entity to recover from the event and then report. The starting time to report is upon an entity's recognized the event, per Submit Report column of Attachment 1.		
PSEG Companies	No	For the reasons cited in response to question 4 above the language roles and responsibilities remain inconsistent and unclear. The Time to Report changes are unreasonable and there is significant duplicate reporting required.

Organization	Yes or No	Question 11 Comment
Response: The DSR DT thanks you for your comment. Upon review the DSR SDT has included a column to indicate the minimum parties who are required to receive the entity's notification. The Threshold for Reporting has been updated to reflect comments that have been received. EOP-004-2 requires an entity to "push" information to certain parties for industry awareness. Since this Standard is an after the fact reporting Standard, reporting times for a majority of event types have been extended to allow the impacted entity to recover from the event and then report.		
Dominion	No	1) A particular Event could be applicable to multiple entities and Attachment 1 would require each applicable entity to report the event. This is duplicative and would appear to overburden the reporting system. 2) Loss of off-site power (grid supply) reporting for nuclear plants is duplicative of reporting done to satisfy NRC requirements. Given the activity at a nuclear plant during this event, this additional reporting is not desired. 3) Cyber intrusion remains an event that would need to be reported multiple times (e.g., this standard, OE-417, NRC requirements, etc.). 4) Since external reporting for other regulators (e.g., DOE, NRC, etc.) remains an obligation of the Applicable Entity, suggest that Attachment 1 only contain impact events as defined in the current version of EOP-004.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the functional entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The DSR SDT understands that there may be multiple reports (for certain events) that are required by different governing agencies. NERC will continue to streamline the reporting process in the future.		
Pepco Holdings Inc and Affiliates	No	The entity responsible for reporting is not clear. Is the initiating entity the same as requesting entity or implementing entity? In the paper it indicates the DT intent is for the entity that performs the action or is directly affected will report.It seems that the proposal would result in a significant amount of duplicate reporting.
Response: The DSR DT thanks you for your comment. The DSR SDT believes it is clear that the reporting entity is the entity that experiences an event or initiates the event (per Threshold for Reporting in Attachment 1). The DSR SDT will ensure that the supporting guideline clearly states this. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view to what has happened.		
SPP Standards Review Group	No	Threshold for Reporting ? Some of the thresholds used to trigger event reporting seem arbitrary. For example, why were three BES Transmission Elements selected for the transmission loss trigger? What?s significant with three? There may be situations where one element can impact reliability more than other situations where three or more lines may be lost. The defining line should be impact to reliability, not a simple count of elements. Also, timing of the loss of these elements is important. If the three elements are lost over a 3-day span, does this trigger an event report? We would think not and would like to see that clarification in the

Organization	Yes or No	Question 11 Comment
		standard.Public appeals ? Some entities may utilize load reduction (Demand Response, interruptible loads, etc) in the normal course of daily operation in lieu of committing additional generation resources. Because this is not an Energy Emergency as defined in the NERC Glossary, would such an event trigger the filing of an Impact Event report under EOP-004-2? We would like clarification on this issue.Multiple entity reporting responsibility ? Several of the triggering events in Attachment 1 list multiple entity reporting responsibility. The SDT needs to clarify precisely who has the actual reporting responsibility for those events. For example, if a DP loses ? 300 MW (or ? 200 MW depending on size) of load who files the report? Is it the DP, TOP, BA or RC? Attachment 1 would lead us to believe all four are required to file reports. This redundancy is unnecessary and creates unneeded paperwork. Surely this redundancy is not the intent of the SDT.Reporting timeframe ? The timeframes for reporting these after-the-fact reports need to be thoroughly reviewed and, we believe, realigned. Which is more important to the reliability of the BES, operating and controlling the BES following an Impact Event or filing a report describing that event? Most operating desks are staffed by a single operator at nights and on weekends. Their focus should be on operating the system, not filing a report with NERC or DOE within one hour.There appears to be inconsistency in the reporting times among the triggering events. There doesn?t appear to be any logic regarding how the times were selected. Shouldn?t impact to the reliability of the BES be that basis? Why is a BA with 50 MW of load who makes a public appeal to customers for load reduction required to report within 1 hour while an IROL violation doesn?t need to be reported for 24 hours? Clearly the IROL violation has a greater impact on the reliability of the BES. Therefore, shouldn?t these types of reports be filed sooner than those events with less impact on BES reliability?Risk to BES equipment ? The Threshold for Reporting this event indicates that only those events associated with a non-environmental physical threat should be reported. The train derailment example in the footnote then conversely describes just such an environmental threat with flammable or toxic cargo. Which should it be? Additionally, how does one determine the applicability of a potential threat? Is this time dependent, is it threat dependent, how do we factor all this in?
Response: The DSR DT thanks you for your comment. The DSR SDT believes it is clear that the reporting entity is the entity that experiences an event or initiates the event (per Threshold for Reporting in Attachment 1). The DSR SDT will ensure that the supporting guideline clearly states this. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view to what has happened. The entire Attachment 1 has been updated to reflect the comments that were received.		
FirstEnergy	No	Nuclear facilities should be explicitly excluded from the events which have CIP standards as the threshold for reporting since they are exempt from the CIP standards.
Response: The DSR DT thanks you for your comment. The DSR SDT understands that nuclear facilities are exempt from CIP Standards but the Loss of Off Site Power to a nuclear generating plant is a Transmission Owner's and Transmission Operator's responsibility and needs to be reported to the ERO and their		

Organization	Yes or No	Question 11 Comment
Regional Entity for the follow up as described by the Event Analysis Program.		
SERC OC Standards Review Group	No	While we agree with the changes made, we do not believe the goal of eliminating duplicate reporting has been accomplished. In addition, the threshold for transmission loss does not adequately translate to previous ?loss of major system components? which had a threshold of ?significantly affects the integrity of interconnected system operations?.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received.		
PJM Interconnection LLC	No	There is still a significant amount of duplicate reporting involved in Attachment 1, which needs to be cleared. See comments to Question 4.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received.		
We Energies	No	It appears that the footnotes only apply one place in the table. Place the footnote in the table where it applies.Voltage Deviations on BES Facilities: 10% compared to what? Rated?Forced Intrusion: ?At a BES facility? facility or Facility?
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. The Footnotes have been reviewed and updated per comments received.		
LG&E and KU Energy LLC	No	In Attachment 1, the existing EOP-004-1 Attachment 1, point 6 includes an ?Or? for the entities (RC, TOP, GOP) for a, b and c. The way the SDT has pulled this apart, they have included the GOP as having an impact on the Voltage Deviations on BES Facilities. The TOP monitors the transmission system and directs GOPs when they need to change in order to protect the system reliability. This is not something the GOP is responsible for monitoring. The GOP is required to be at the TOP assigned voltage schedule and that actually falls under VAR-002 already. Please remove the GOP from the line of ?Voltage Deviations on BES Equipment.? The way EOP-004-1 Attachment 1 point 6 is currently written, the GOP is an ?or? and does fall into parts b or c, where part 6b is similar to the proposed line ?Damage or destruction of BES equipment? identified in the proposed EOP-004-2 Attachment 1. However, currently the GO/GOP reports ?Loss of Major System Components? on EOP-004-1 within 24 hours of determining damage to the equipment. The proposed ?One hour? is too tight of a window as the GO/GOP often do not know the extent of damage that

Organization	Yes or No	Question 11 Comment
		soon. Typically the OEM is called upon to come and do a thorough inspection and assess the extent of damage, of if there even is any damage; once the ?loss of major system components? is determined, then the 24 hour clock begins today.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received.		
Compliance & Responsiblity Organization	No	See comments set forth in number 2
Exelon	No	Attachment 1, Part A ? Energy Emergency requiring Public appeal for load reduction ? In the current draft Standard, the applicability has been revised from an RC and BA to "initiating entity." As a GO/GOP, I cannot see any event where a GO/GOP would be the responsible "initiating entity" or have the ability to determine an "Energy Emergency." Suggest revising back to specific entities that would be likely responsible for this action (e.g., RC, BA, TOP). Attachment 1, Part A ? Energy Emergency requiring system-wide voltage reduction ? In the current draft Standard, the applicability has been revised from an RC, TO, TOP, and DP to "initiating entity." As a GO/GOP, I cannot see any event where a GO/GOP would be the responsible "initiating entity" or have the ability to determine an "Energy Emergency" related to system-wide voltage reduction. Suggest revising back to specific entities that would be likely responsible for this action.Attachment 1, Part A ? Voltage Deviations on BES facilities - A GOP may not be able to make the determination of a +/- 10% voltage deviation for ? 15 continuous minutes, this should be a TOP RC function only. Attachment 1, Part A ? Generation Loss of ? 2, 000 MW for a GOP does not provide a time threshold. If the 2, 000 MW is from a combination of units in a single location, what is the time threshold for the combined unit loss? Suggest that a time threshold be added for clarity.Attachment 1, Part A ? Loss of off-site power (grid supply) affecting a nuclear generating station ? this event applicability should be removed in its entirety for a Nuclear Plant Generator Operator. The impact of loss of off-site power on a nuclear generation unit is dependent on the specific plant design, if it is a partial loss of off-site power (per the plant specific NPIRs) and may not result in a loss of generation (i.e., unit trip). If a loss of off-site power were to result in a unit trip, an Emergency Notification System (ENS) would be required to the Nuclear Regulatory Commission (NRC). Depending on the unit design, the notification to the NRC may be 1 hour, 8 hours or none at all. Consideration should be given to coordinating such reporting with existing required notifications to the NRC as to not duplicate effort or add unnecessary burden on the part of a Nuclear Plant Generator Operator during a potential transient on the unit. In addition, if the loss of off-site power were to result in a unit trip, if the impact to the BES were ?2,000 MW, then required notifications would be made in accordance with the threshold for reporting for Attachment 1, Part A ? Generation Loss. However, to align with the importance of ensuring nuclear plant safe operation and shutdown as implemented in NERC Standard NUC-001, if a transmission entity experiences an event

Organization	Yes or No	Question 11 Comment
		that causes an unplanned loss of off-site power (source) as defined in the applicable Nuclear Plant Interface Requirements, then the responsible transmission entity should report the event within 24 hours after occurrence. In addition, replace the words "grid supply" to "source" to ensure that notification occurs on an unplanned loss of one or multiple sources to a nuclear power plant. Suggest rewording as follows (including replacing the words "grid supply" to "source" and adding in the word "unplanned" to eliminate unnecessary reporting of planned maintenance activities in the table below):Event Entity with Reporting Responsibility Threshold for Reporting Time to Submit ReportUnplanned loss of off-site power to a Nuclear generating plant (source) as defined in the applicable Nuclear Plant Interface Requirements (NPIRs) Each transmission entity responsible for providing services related to NPIRs (e.g., RC, BA, TO, TOP, TO, GO, GOP) that experiences the event causing an unplanned loss of off-site power (source) Unplanned loss of off-site power (source) to a Nuclear Power Plant as defined in the applicable NPIRs. Within 24 hours after occurrenceAttachment 1, Part A ? Damage or destruction of BES equipment ? The event criteria is still ambiguous and does not provide clear guidance; specifically, the determination of the aggregate impact of damage may not be immediately understood ? it does not seem reasonable to expect that the 1 hour report time clock starts on identification of an occurrence. Suggest that the 1 hour report time clock begins following confirmation of event. ? The initiating event needs to explicitly state that it is a physical and not cyber. ? If the damage or destruction is related to a deliberate act, consideration should also be given to coordinating such reporting with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security event (see additional comments in response to item 17 below). Attachment 1, Part A ? Damage or destruction of Critical Cyber Asset The events that are associated with Critical Cyber Assets should be removed from this Standard. Critical Cyber Asset related events are better addressed in the reporting of Cyber Security Incidents which is already included in Attachment 1, Part B and the CIP standards currently require details about Critical Cyber Assets to be protected with access to that information restricted to only specifically authorized personnel.Attachment 1, Part A ? Damage or destruction of Critical Asset The events that are associated with Critical Assets should be removed from this Standard. Critical Assets are typically whole control centers, substations or generation plants and the damage or destruction of individual pieces of equipment at one of these locations will usually not have much impact to the BES. Any important impacts located at these sites are already addressed in the other existing [Impact] Event types or would be addressed in the Cyber Security Incident event which is already included in Attachment 1, Part B. The CIP standards also currently require that details about Critical Assets and Critical Cyber Assets must be protected with access to that information restricted to only specifically authorized personnel. The identification of Critical Asset is also only an interim step used to identify the Critical Cyber Assets that need to have cyber security protections and the NERC Project 2008-06 CSO706 Standards Drafting Team is currently expecting to eliminate the requirement to identify Critical Assets in the draft revisions they are currently working on. Attachment 1, Part B ? Forced intrusion at a BES facility ? Consideration should also be given to coordinating such reporting with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a

Organization	Yes or No	Question 11 Comment
		potential security event (see additional comments in response to item 17 below).Attachment 1, Part B ? Risk to BES equipment from a non-environmental physical threat ? this event leaves the interpretation of what constitutes a "risk" with the reporting entity. Although the DSR SDT has provided some examples, there needs to be more specific criteria for this event as this threshold still remains ambiguous and will lead to difficulty in determining within 1 hour if a report is necessary. Consideration should also be given to coordinating such reporting with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security event (see additional comments in response to item 17 below).Attachment 1, Part B ? Detection of a reportable Cyber Security IncidentAlthough the DSR SDT agreed that there may be confusion between reporting requirements in this draft and the current CIP-008, "Cyber Security ? Incident Reporting and Response Planning", Part B now requires a 1 hour report after occurrence. The DSR SDT should verify the timing and reporting required for these Cyber Security Incident events is coordinated with the NERC Project 2008-06 CSO706 Standards Drafting Team.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received. The DSR SDT has worked closely with NERC Staff, the Event Analysis Working Group, Project 2008-06 and the U.S. Department of Energy to ensure that EOP-004-2 captures what FERC has directed and will improve the reliability of the BES.		
SDG&E	No	For ?Detection of a reportable Cyber Security Incident,? Attachment 1 identifies the threshold for reporting as: ?that meets the criteria in CIP-008 (or its successor)?; however, CIP-008 has no specified criteria, so this is an unusable threshold. Additionally, SDG&E recommends that the timing of any follow-up and/or final reports required by the standard be listed in the Attachment 1 table.
Response: The DSR DT thanks you for your comment. CIP-008 states that an entity will report a Cyber Security Incident to the ES-ISAC. EOP-004-2, Attachment 2 is the vehicle to report a Cyber Security Incident. It is also required to be sent to their RC which will give them the industry awareness of a single event or is it a multiple event within their area.		
City of Tallahassee (TAL)	No	One hour should be expanded. While I realize the importance of getting information to NERC/ESISAC/whoever, most of the 1-hour requirements are tied to events that may not be resolved within one hour. This will result in stopping restoration efforts or monitoring to submit paperwork. Calling in additional assistance, while certainly a possibility, may not be feasible to accomplish in sufficient time to meet the one-hour deadline. If any of these events were to truly have a detrimental effect on the BES, the effects would have already been felt.Recommend all 1-hour reports be extended to 4-hours. This should also be placed on the list to modify Form OE-417report time lines.

Organization	Yes or No	Question 11 Comment
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received. The DOE Form OE-417 is not governed by NERC but the DSR SDT is proposing to allow an entity to use it to report an event in lieu of Attachment 2.		
Lakeland Electric	No	Event ? Transmission lossThreshold for Reporting ? Revise to ?Loss of three or more BES Transmission elements within a 15 minute period?. This change would capture a sequence of transmission element losses and remove the question if timing that will arise if other transmission elements trip, cascade, due to loss of the first element. There may also be a need for a footnote to clarify that a transmission element that is removed from service by a transmission operator to prevent uncontrolled cascading would be classified as a loss (something for the SDT to consider). Event ? Energy Emergency requiring Public appeal for load reductionThreshold for Reporting ? Add a footnote: Repeated public appeals for the same initiating Impact Event shall be reported as one Public Appeal Event. The initiation and release to the media of the Public appeal(s) should be the reportable event. Question: would an internal request to large industrial customers for voluntary load reductions be reportable under this Event?
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received. Demand responsive load is not covered within this proposed Standard unless it fulfills a Threshold of Reporting within Attachment 1. Footnotes have been update to reflect comments received.		
Arkansas Electric Cooperative Corporation	No	We appreciate the effort the team has taken in improving the requirements since the last posting. Event Forced Intrusion: The timeframe is very small given the possibly minimal risk to the BES. It often takes much longer than 1 hour after verification of intrusion to determine the intrusion was only for copper theft. We suggest a 24 hour time frame or tie the timeframe to the "verification of forced intrusion."
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received.		
Manitoba Hydro	No	Reporting for CCA's should be limited to damage associated with a detected cyber security incident.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. Damage or destruction of Critical Cyber Assets s is per CIP-002 and may not fall into the category of Cyber Security Response as outlined by an entity.		
Sweeny Cogeneration LP	No	In Attachment 1, Part A, Generator Operators who experience a ? 10% sustained voltage deviation for ? 15

Organization	Yes or No	Question 11 Comment
		continuous must issue a report For externally driven events, the GOP will have little if any knowledge of the cause or remedies taken to address it. We believe the language presently in EOP-004-1 is satisfactory that any ?action taken by a Generator Operator? that results in a voltage deviation has to be reported by the GOP.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received.		
American Electric Power	No	The time to submit a report for the inclusion of the damage or destruction of BES equipment, critical asset, or critical cyber asset is too aggressive. The critical cyber asset reporting is redundant with CIP-008. Furthermore, reporting equipment failures within an hour for Critical Assets is going to overwhelm operators that need to focus on the restoration efforts. Self-evident equipment failures at a Critical Asset (such as a tube leak at a generator which is a Critical Asset) should not be required to be reported. Maybe the wording should be stated as an ?abnormal occurrence? rather than ?equipment failure.?It would be helpful if there was a defining or a footnote that defines the nature and/or duration for loss of some equipment. For example, is a transmission loss for sustain or momentary outages?
Response: The DSR DT thanks you for your comment. The Implementation Plan for this project now includes a provision to retire the requirement in CIP-008 for reporting (Requirement 1, Part 1.3). The entire Attachment 1 has been updated to reflect the comments that were received.		
USACE	No	The "Potential Reliability Impact" table should be taken out. Refered to previous comment on our position on potentail impacts.
Response: The DSR DT thanks you for your comment. The DSR SDT believes that potential events are required to be reported to provide industry awareness.		
Consumers Energy	No	1. In reference to the Impact Event addressing ?Loss of Firm load for greater than or equal to 15 minutes?, this is likely to occur for most entities most frequently during storm events, where the loss of load builds slowly over time. In these cases, exceeding the threshold may not be apparent until a considerable time has lapsed, making the submittal time frame impossible to meet. Even more, it may be very difficult to determine if/when 300 MW load (for the larger utilities) has been lost during storm events, as the precise load represented by distribution system outages may not be determinable, since this load is necessarily dynamic. Suggest that the threshold be modified to ?Within 1 hour after detection of exceeding 15-minute threshold?. Additionally, these criteria are specifically storm related wide spread distribution system outages. These events do not pose a risk to the BES.2. Many of the Impact Events listed are likely to occur, if they occur, at widely-distributed system facilities, making reporting ?Within 1 hour after occurrence is identified? possibly impractical, particularly in order to provide any meaningful information. Please give consideration to clearly permitting some degree of investigation by the entity prior to triggering the ?time to submit?3. Referring to the

Organization	Yes or No	Question 11 Comment
		?Transmission Loss? Impact Event, please provide more specificity. Is this intended to address :- anytime that three or more BES Transmission Elements are out of service, - only when three or more BES Transmission Elements are concurrently out-of-service due to unscheduled events, - only when three or more BES Transmission Elements are simultaneously automatically forced out-of-service, or- only when three or more BES Transmission Elements are forced from service in some proximity to each other? It is not unusual, for a large transmission system, that this many elements may be concurrently forced out-of-service at widely-separated locations for independent reasons.4. Referring to the ?Fuel Supply Emergency? Impact Event, OE-417 requires 6-hour reporting, where the Impact Event Table requires 1-hour reporting. The reporting period for EOP-004-2 should be consistent with OE-417.5. For that matter, the SDT should carefully compare the Impact Event Table with OE-417. Where similar Impact Events are listed, consistent terminology should be used, and identical reporting periods specified. Where the Impact Event Table contains additional events, they should be clarified as being distinct from OE-417 to assist entities in implementation. Further, since OE-417 must be reviewed and updated every three years, EOP-004 should defer to the reporting time constraints within OE-417 wherever listed in order to assure that conflicting reporting requirements are not imposed.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed' Loss of Firm Load' as a reporting event, and believe the reporting requirement currently approved in EOP-004-1 should remain in EOP-004-2. The DSR SDT has removed the 'Fuel Supply Emergencies' event after considering comments the DSR SDT received on this event. The DOE Form OE-417 is reviewed biennially by the DOE and can be updated or changed without NERC's involvement. The DSR SDT has taken into consideration the use of Form O- 417 to report events to NERC and agrees that this will fulfill EOP-004-2's reporting requirements. The entire Attachment 1 has been updated to reflect the comments that were received.		
Independent Electricity System Operator	No	As indicated under Q4, we question the need to include IA, TSP and LSE in the responsible entities for reporting.
Response: The DSR DT thanks you for your comment. The DSR SDT has established that CIP-002-4 and CIP-008-3 are applicable to an IA, TSP, and LSE. These entities will report a Cyber Security Incident per Attachment 2 (or OE-417) as the vehicle to inform the ERO, their Regional Entity and their Reliability Coordinator.		
Ameren	No	See response to question 4.
Response: The DSR DT thanks you for your comment. Please see question 4 response.		
ISO New England, Inc	No	As indicated under Q4, we question the need to include IA, TSP and LSE in the responsible entities for reporting. There is still significant duplicate reporting included. For instance, why do both the RC and TOP to report voltage deviations? As written, a voltage deviation on the BES would require both to report. The same

Organization	Yes or No	Question 11 Comment
		would hold true for IROLs. Perhaps IROLs should only be reported by the RC to be consistent with the recently FERC approved Interconnection Reliability Operating Limit standards. Also, the CIP reporting requirements duplicate was is already contained in the CIP Standards, specifically CIP-008. Also, we are required to intentionally destroy Critical Cyber Assets when they are retired, why would we be required to report this?
Response: The DSR DT thanks you for your comment. The DSR SDT has established that CIP-002-3 and CIP-008-3 are applicable to an IA, TSP, and LSE. These entities will report a Cyber Security Incident per Attachment 2 (or OE-417) as the vehicle to inform the ERO, their Regional Entity and their Reliability Coordinator. If a Critical Cyber Asset (CCA) was to be retired, the entity would declassify it as a CCA and therefore it would not be required to be reported. The Implementation Plan for this project now includes a provision to retire the requirement in CIP-008 for reporting (Requirement 1, Part 1.3)		
Calpine Corp	No	1. Additional clarity on the nature of reportable ?Fuel Emergencies? is needed. Does loss of interruptible gas transportation require reporting? 2. Additional clarity on the threshold for ?damage or destruction of BES equipment? is needed. Footnote 1 on page 16 states, in part ?Significantly affects the reliability margin of the system (e.g. has the potential to result the need for emergency actions?. For generating facilities, does this statement refer specifically to the parallel requirement to report any loss of generation >= 2,000 in the Eastern or Western Connection or >= 1,000 in the ERCOT or Quebec Interconnection? If not, exactly what level of damage at a generating plant requires reporting? Use of imprecise terms such as ?significantly? sets the stage for future compliance and enforcement confusion.3. Additional clarity is required for ?Detection of reportable Cyber Security Incident." Is this item intended to apply only to Critical Cyber Assets, or is it an extension of the requirement to all applicable entities irrespective of their Critical Asset status? If it applies only to Critical Cyber Assets, does this reporting requirement create redundant reporting (as reporting is already required under CIP-008-4)? CIP-008-4 requires reporting only of events affecting Critical Cyber Assets. If a more expansive application is intended, what equipment or systems are to be included in the reporting requirement?
Response: The DSR DT thanks you for your comment. The event of Fuel Supply Emergencies has been removed per comments the DSR SDT received. The entire Attachment 1 has been updated to reflect the comments that were received. Footnotes in Attachment 1 have been updated to reflect the comments that the DSR SDT received. Damage to BES equipment's foot note has been enhanced to mean that the BES piece of equipment is required to be removed from service. CIP-008 states that an entity will report a Cyber Security Incident to the ES-ISAC. EOP-004-2, Attachment 2 is the vehicle to report a Cyber Security Incident.		
BGE	No	For the following Events (Damage or destruction of BES equipment, Damage of destruction of Critical Asset, and Damage or destruction of a Critical Cyber Asset), submitting a report within 1 hour after occurrence is identified is too short of a time frame. Generally, the initial time period is spent in recovering from the situation and restoring either electric service or restoring computer services to assure proper operations. To

Organization	Yes or No	Question 11 Comment
		distract from the restoration to normal activities to focus on a report would be detrimental to reliability. Notification of an event may perhaps be made by phone call within 1 hour but completing a report should be required no less than 6 or 12 hours. Determining a cause (especially external or intentional) could take longer than 1 hour to determine and complete a report.It is important to consider the imposition created by a compliance obligation and weigh it against the other demands before the operator at that time. A compliance obligation should avoid becoming a distraction from reliability related work. Under impact event type scenarios, in the first hour of the event, the primary concern should be coping with/resolving the event.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. Footnotes in Attachment 1 have been updated to reflect the comments that the DSR SDT received. Damage to BES equipment's foot note has been enhanced to mean that the BES piece of equipment is required to be removed from service.		
Alliant Energy	No	The item relating to Loss of Firm Load for > 15 minutes should be revised to 500 MW and 300 MW. For many companies, a storm moving across their system could cause more than 300 MW of firm load to be lost, but there is no impact on the BES, so why does the detailed reporting need to be done?The items relating to ?damage or destruction? need to be revised to not be so wide. As currently written, a plan by a company to raze a facility could be considered a violation and must be reported. We believe it needs to tightened to malicious intent or human negligence/error.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed Loss of Firm load and believe the reporting requirement presented approved in EOP-004-1 is substantial and should remain within EOP-004-2. If a Critical Cyber Asset (CCA) was to be retired, the entity would declassify it as a CCA and therefore it would not be required to be reported.		
CenterPoint Energy	No	(1) CenterPoint Energy believes that the ?Entity with Reporting Responsibility? for the first three events in Part A should be clarified. There could still be confusion regarding the ?initiating entity? for events where one entity directs another to take action. From the text on page 5 of the Unofficial Comment Form, it appears that the SDT intended for the ?initiating entity? to be the entity that takes action. To make this clear in Attachment 1, CenterPoint Energy recommends replacing ?initiating entity? with ?Each (insert applicable entities) that (insert action). For example, for ?Energy Emergency requiring a Public appeal? the Entity with Reporting Responsibility should be ?Each?that issues a public appeal for load reduction?. (2) Part A: The threshold for reporting ?System Separation? should not be fixed at greater than or equal to 100 MW for all entities, but rather should be scaled to previous year?s demand as in ?Loss of Firm load for greater than or equal to 15 minutes?, so that for entities with demand greater than or equal to 3000 MW, the island would be greater than or equal to 300MW. (3) Part A: The one hour reporting requirements are unreasonable and burdensome. The Background text indicates that ?proposed changes do not include any real-time operating notifications?? CenterPoint Energy believes all one hour reporting requirements could potentially divert resources away from

Organization	Yes or No	Question 11 Comment
		responding to the event. In many instances the event may still be developing within one hour. Likewise, the 24 hour reporting requirements are also burdensome. CenterPoint Energy recommends changing all reporting requirements to 48 hours. CenterPoint Energy acknowledges that the DOE OE-417 report requires certain one hour and 6 hour reporting. Those requirements should also be extended, and CenterPoint Energy will be making the same recommendation during the DOE OE-417 report revision process when the current form expires on 12/31/11.(4) Part B: CenterPoint Energy is very concerned with the ?events? listed under Attachment 1 ? Potential Reliability Impact ? Part B and believes Part B should be deleted. These arbitrary ?events? with ?potential reliability impact? and reporting times place unnecessary burden on entities to report ?situations? that would rarely impact the reliability of the BES. Entities should be aware of developing situations; however, this standard should not require reporting of such occurrences.(5) Part B: Of particular concern is the overly broad ?Risk to BES equipment? and the example provided in the footnote. CenterPoint Energy believes the SDT has already identified the events with the greatest risk to impact the BES in Part A. Also including ?potential reliability impact? situations in Part B inappropriately dilutes attention away from the truly important events. The industry, NERC and FERC should not lose sight of the forest for the trees.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. Footnotes in Attachment 1 have been updated to reflect the comments that the DSR SDT received. The DOE Form OE-417 is under review by the DOE and can be updated or changed without NERC's involvement. The DSR SDT has taken into consideration the use of OE-417 to report events to NERC and agrees that this will fulfill EOP-004-2's reporting requirements.		
ExxonMobil Research and Engineering	No	The notification requirement and documentation in Attachment 1 do not clearly identify which entities need to be notified for each type of event detailed in Attachment 1. While it makes sense to notify the Reliability Coordinator, NERC, Regional Entity, Law Enforcement and other Governmental Agencies for sabotage type events, it does not seem proper to notify Law Enforcement agencies of a system disturbance that is unrelated to improper human intervention. Furthermore, it is our belief that a time frame of 1 hour is a short window for making a verbal notification to third parties, and an impossibly short window for requiring the submittal of a completed form regardless of the simplicity. When a Petrochemical Facility experiences an impact event, the initial focus should emphasize safe control of the chemical process. For those cases where registered entities are required to submit a form within 1 hour, the Standard Drafting Team should alter the requirement to allow for verbal notification during the first few hours following the initiation of an Impact Event (i.e. allow the facility time to appropriately respond to and gain control of the situation prior to making a notification which may take several hours) and provide separate notifications windows for those parties that will need to respond to an Impact Event immediately and those entities that need to be informed that one occurred for the purposes of investigating the cause of and response to an Impact Event. For example, a GOP should immediately notify a TOP when it experiences a forced outage of generation capacity as soon as possible, but there is no immediate benefit to notify NERC when site personnel are responding to the event in order to gain control of of the situation and determine the extent of the problem. The existing standard?s

Organization	Yes or No	Question 11 Comment
		requirement to file an initial report to entities, such as NERC, within 24 hours seems reasonable provided that proper real time notifications are made and the Standard Drafting Team reinstates EOP-004 Revision 1's Requirement 3.3, which allows for the extension of the 24 hour window during adverse conditions, into the requirement section of EOP-004 [the current revision locates this extension in Attachment 1, which, according to input received from Regional Entities, means that the extension would not be enforceable].
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. Footnotes in Attachment 1 have been updated to reflect the comments that the DSR SDT received.		
PPL Electric Utilities	No	We very much appreciate the work performed by SDT and consideration of all the comments received. While we agree with the majority of the Attachment 1 changes, we suggest the SDT add further clarification to Attachment 1, Part A, Event 'Transmission Loss'. Does this mean permanent loss? Do two lines and a pole constitute a loss of three elements? E.g. Consider the loss of a 230 kV line with two tapped transformers. This does not have a significant effect on the BES, yet would it be reportable? We would prefer Attachment 1, Part A, ?Threshold Reporting? be clarified. E.g. ?Three or more "unrelated" pieces of equipment for a single event?.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. Footnotes in Attachment 1 have been updated to reflect the comments that the DSR SDT received.		
Lincoln Electric System	No	While LES supports the bright line criteria listed in Attachment 1 for reporting Impact Events, we have concerns regarding the reporting threshold for ?Transmission loss?. For Transmission loss of three or more Transmission Elements, LES supports the MRO NSRS? suggested wording of ?Two or more BES Transmission Elements that exceed TPL Category D operating criteria or its successor.?
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received.		
American Transmission Company	No	Energy Emergency requiring Public AppealATC believes that the phrase ?initiating entity? is unclear and could be interpreted in multiple ways. 1) the entity has the authority to call for public appeals, 2) the entity has the authority to declare an Energy Emergency, or 3) the entity determines and identifies the need for the Energy EmergencyTypically the BA?s call for public appeals, so does every BA that calls for the public appeal have to make a filing?The RC declares the need for an Energy Emergency, so are they the initiating entity? A TOP could also identify the need for public appeals and notify the RC about the request. In this case, is the TOP the initiating entity?Given the above examples, ATC believes that the SDT needs to clarify who is required to make the filing. Voltage Deviations on BES FacilitiesATC believes that this should be clarified because one may assume that a loss of a single bus in which voltage goes to zero for more than 15 minutes

Organization	Yes or No	Question 11 Comment
		is reportable. It is ATC understands that what the SDT means is a voltage dip, not an outage to a BES facility. However, given the brief description, ATC is not 100% sure whether there is a clear understanding of the standard?s intent.Energy Emergency resulting in automatic firm load shedding Please provide additional clarify.ATC believes that the SDT should not use the term ?Impact Event? when identifying the entity with reporting responsibility. The term ?Impact Event? is identified in the standard and points to Attachment 1 but now is being used outside of that context and requires entities to interpret what qualifies as an Impact Event.The above observation also applies to those other events that use the term ?Impact Event? to describe Reporting Responsibility.Footnote 1: ATC would like the phrase ?as determined by the equipment owner? added to the footnote. This simple phrase will allow entities to be sure that they are responsible for determining if the damage significantly affects the reliability margin of the system. Without this phrase, entities could be subject to non-compliance actions based on differences of opinions to the extent of the damage on the system. The other option the SDT has is to provide additional clarity on what qualifies as a significant affect.Time to Submit Report:ATC strongly disagrees with the 1 hour time to submit a report because it does not fit with the purpose of this standard. The purpose of this standard is to increase awareness, however, requiring a one-hour reporting window following the event provides little to no benefit. ATC believes that these events should have a 24 hour reporting window which allows for a reasonable amount of time to gather information and report the issue.If the SDT disagrees with this observation, ATC believes a complete explanation should be provided on why knowledge of an event within an hour is significantly better than having the knowledge of the event in a 24 hour time period. ATC strongly believes that NERC will gain as much or more knowledge of the event by giving entities time to understand the event and report.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received.		
Duke Energy	No	? Attachment 1 contains three reportable events (Damage or destruction of Critical Asset, Damage or destruction of a Critical Cyber Asset, and Detection of a reportable Cyber Security Incident) that overlap with CIP-008-3 Cyber Security Incident Reporting and Response Planning and could result in redundant or conflicting content between the two standards. We propose either of the following options:1. Remove the requirement for reporting these events from EOP-004-2 and add the timing and reporting requirements into CIP-008-3, R1.3. ?Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.? OR2. Replace the reporting requirement in CIP-008-3, R1.3. with a reference to report as required in EOP-004-2.? Also, as noted in our comment to Question #4 above, the Attachment 1 Section ?Entity with Reporting Responsibility? should just identify ?Initiating entity? for every Event, as was done with the first three Events. That way you avoid errors in leaving an entity off, or including an entity incorrectly (as was done with the GOP on Voltage Deviations). We note that LSE is listed in the standard as an Applicable entity, and should be included in Attachment 1.

Organization	Yes or No	Question 11 Comment
		Our suggestion would handle this oversight. We also note that CIP-001 does not include Distribution Provider in the list of applicable entities, but EOP-004-2 does include the DP.? We reiterate our comment to Question #1 above that the DSR SDT statement that the proposed changes do not include any real-time operating notifications is inconsistent with requiring notification within one hour for thirteen of the twenty listed Events in Attachment 1.? The last six events refer to the entity that experiences the potential Impact Event. We believe that the word ?potential? should be struck, as this creates an impossibly broad reporting requirement.? Footnote 1 should be revised to strike the phrase ?has the potential to? from the parenthetical, as this creates an impossibly broad reporting requirement.? The Impact Event ?Risk to BES equipment? should be revised to ?Risk to BES equipment that results in the need for emergency actions?. The accompanying footnote 4 should be revised to read as follows: Examples could include a train derailment adjacent to BES equipment (e.g. flammable or toxic cargo that would cause the evacuation of a BES facility control center), or a report of a suspicious device near BES equipment.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. CIP-008 states that an entity will report a Cyber Security Incident to the ES-ISAC. EOP-004-2, Attachment 2 is the vehicle to report a Cyber Security Incident. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the ERO and others with a different view of what has happened. The DSR SDT understands that there may be multiple reports (for certain events) that are required by different government agencies. NERC will continue to streamline the reporting process as we move into the future.		
Constellation Power Generation	No	CPG has the following concerns regarding Attachment 1: ?Real-Time - On page 5 of the proposed standard, the team noted that ?the proposed changes do not include any real-time operating notifications.? However, several events in Attachment 1 require that documentation be completed and submitted to the ERO within 1 hour. For generation sites that are unmanned, or only have 1 to 2 operators on site at all times, a 1 hour requirement is not only onerous but is essentially ?real time.??Response within 1 hour - It is important to consider the imposition created by a compliance obligation and weigh it against the other demands before the operator at that time. A compliance obligation should avoid becoming a distraction from reliability related work. Under impact event type scenarios, in the first hour of the event, the primary concern should be coping with/resolving the event. Other notification requirements exists based on required agency response relative to the concern at hand (e.g. public evacuations, fire assistance, etc.) Notification within an hour under EOP-004 does not appear to represent a relevant benefit to resolving the situation and the potential cost would be borne by reliability and recovery efforts. Anything performed within the first hour of the event must be to benefit the public or benefit the restoration of power.?Damage or destruction of BES equipment ? the reporting requirement of 1 hour is extremely onerous. A good example is the failure of a major piece of equipment at a remote combustion turbine generation site. Combustion turbine generation sites are not usually manned with many people. If a failure of a major piece of equipment were to occur, the few people on site need to complete communications to affected entities, communications to their management, as well as

Organization	Yes or No	Question 11 Comment
		emergency switching and ensuring that no other pieces of equipment are effected or harmed. There is little time to complete a form in 1 hour. This should be changed to 48 hours. The form is also inadequate for this type of event. o Using the example above of a failure of a major piece of equipment, CPG is not sure if it?s reportable per Attachment 1, which further proves that Attachment 1 is not clear. Per the footnote regarding damage to BES equipment, the failure would not be reportable, as it does not affect IROL, given the information at the plant it does not significantly affect the reliability margin of the system, and was not damaged or destroyed due to intentional or unintentional human action. However, it would be reportable per the table as the table states ?equipment failure? and ?external cause.? Clarification is needed.?Damage or destruction of Critical Asset ? This item should be removed or significantly refined. For generation assets, a critical asset is essentially the entire plant, so in many cases the information reported at this level would not be useful if the valuable details reside at the equipment level. If it is not removed, then see the notes above on the 1 hour requirement for the completion of the form. ?Fuel supply emergency ? 1 hour for reporting the document is unreasonable. See the earlier notes. ?Risk to BES equipment ? ?From a non-environmental physical threat? This item is too vague and subjective. A catch all category to capture a broad list of potential risks is problematic for entities to manage in their compliance programs and to audit. This should be removed.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received.		
Georgia System Operations Corporation	No	Energy Emergency requiring public appeal for load reduction:-The NERC Glossary defines ?Energy Emergency? as a ?condition when a Load-Serving Entity has exhausted all other options and can no longer provide its customers? expected energy requirements.? Per EOP-002, an Energy Emergency Alert may be initiated by the RC upon RC sole discretion, upon BA request, or upon LSE request.-Question: Is it intended that the LSE reports the event if the LSE requests an alert, the BA reports the event if the BA requests an alert, and the RC reports it if it is a RC sole discretion decision? What if an alert is not initiated? Is it an Energy Emergency? Is it an impact event? Who must initiate the public appeal? Since it must be reported within a certain time after the issuance of the public appeal, is it not an impact event until after the initiation of the public appeal (which should be after the initiation of the alert)? Shouldn?t the reporting of the impact event be done by the initiator of the public appeal? The event should probably be the public appeal and not the Energy Emergency.-?Public? should not be capitalized.-The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained.? Energy Emergency requiring system-wide voltage reduction: See Energy Emergency requiring public appeal for load reduction above regarding requesting Energy Emergency Alerts. If this event is to be reported within a certain time after ?the event?, at what time is the event marked? Or is it within a certain time after the initiation of the voltage reduction and, if so, shouldn?t the reporting of the impact event be done by the initiator of the voltage reduction? The event should probably be the system-wide voltage reduction and not the Energy Emergency. The reliability objective

Organization	Yes or No	Question 11 Comment
		of this standard is not achieved by NERC knowing of this within 1 hour and NERC does not need to know this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained.Energy Emergency requiring manual firm load shedding:-See Energy Emergency requiring public appeal for load reduction above regarding requesting Energy Emergency Alerts. If this event is to be reported within a certain time after ?the event?, at what time is the event marked? Or is it a certain time after the initiation of the shedding of load, if so, shouldn?t the reporting of the impact event be done by the initiator of the shedding of the load? If the RC directs a BA to shed load, then the BA directs a DP to do it, then the DP sheds the load, who is the initiator of the load shedding? The event should probably be the firm load shedding and not the Energy Emergency.-The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained.Energy Emergency resulting in automatic firm load shedding:Whenever load is automatically shed both the DP and the TOP ?experience? the event. So does the BA and the LSE. This event includes ?or? between ?DP? and ?TOP.? Is that intentional? Other events in the table do not include either an ?and? or an ?or.? The entities are separated only by commas. NERC should not require multiple entities to report the same event. See comment for R5 above. If a DP "experiences" an automatic load shedding doesn't the TOP also experience it? Both should not report the same event.-The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained.Voltage deviations on BES Facilities:-Should GOs/GOPs be required instead to report to BAs when this condition exists with the BA then reporting to NERC? The idea of a deviation "on BES Facilities" is not clear. On any one Facility? On all Facilities in an area? How wide of an area?-?Voltage Deviation? is not proper noun/name and is not defined in the NERC Glossary. It should not be capitalized.IROL violation: Multiple entities should not report the same event. Please define ?IROL Violation? or use lowercase. It is assumed that ?IROL Violation? means operation ?outside the IROL for a time greater than IROL TV.?Loss of firm load for ? 15 minutes:-Multiple entities should not report the same event. The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained. ?Firm Demand? is defined but not ?Firm load.?System separation (islanding):-Multiple entities should not report the same event. A DP separating from the transmission system should not be a reportable event for a DP in and of itself. If it leads to a sufficient loss of load, it is reportable as above.-The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained. The words ?separation? and ?islanding? should not be capitalized.Generation loss:-Should GOs/GOPs be required instead to report to BAs when their generation is lost with the BA then reporting to NERC when the total is ? 2,000 MW? A ?loss? of generation should be clarified. Is the discovery of damaged equipment in an offline plant which makes the plant unavailable for an extended period of time a ?loss? of generation?-It should be clarified if this event means the concurrent loss of the generation or losing the generation non-concurrently

Organization	Yes or No	Question 11 Comment
		but they are concurrently unavailable. What is the time window for losing the generation? Lost within seconds of each other? Minutes? Hours?Loss of off-site power to a nuclear generating plant (grid supply):-Multiple entities should not report the same event.-?Off? should be lowercase.Transmission loss:-RCs should not be required to report the loss of transmission elements to NERC. A ?loss? of a BES Transmission Element should be clarified.It should be clarified if this event means the concurrent loss of elements or the non-concurrent loss of the elements but they are concurrently unavailable. What is the time window for losing the elements? When elements are lost, it will be difficult to differentiate if they are BES Transmission Elements or not. Alarms don't immediately identify this. It could lead to gross over-reporting if no distinction is made by a TOP and the TOP reports all losses of 3 elements. It may still be over-reporting (from a reasonableness/practicality basis) even if the differentiation could be easily made and only BES Transmission Elements are reported. Threshold for reporting Transmission Loss: As stated, this will require the reporting of almost all transmission outages. This is particularly true taking into consideration the current work of the drafting team to define the Bulk Electric System. The loss of a single 115kV network line could meet the threshold for reporting as the definition of Element includes both the line itself and the circuit breakers. Instead, we recommend the following threshold "Three or more BES Transmission lines." This threshold has consistency with CIP-002-4 and draft PRC-002-2. This threshold also needs additional clarification as to the timeframe involved. Is the intent the reporting of the loss of 3 or more BES Transmission Elements anytime within a 24 hour period or must they be lost simultaneously? Also, we recommend that the three losses be the result of a related event to require reporting.Damage or destruction of BES equipment that i. affects an IROL; ii. significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); or iii. damaged or destroyed due to intentional or unintentional human action (Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly, e.g., removal of grounding straps rendering protective relaying inoperative.):-What is ?BES equipment?? Would an operator know which equipment is BES equipment and which is not or which BES equipment affects an IROL (if we had one) or which does not? It is a judgment call as to whether the effect was significant or not or if it has the potential or not. Multiple entities should not report the same event. Unplanned control center evacuation:-?Control Center? should be lowercase.-The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained.Fuel supply emergency:Multiple entities should not report the same event. Should GOs/GOPs be required instead to report to BAs when they have a fuel supply emergency with the BA then reporting to NERC if the situation is projected to require emergency action at the BA level?-The reliability objective of this standard is not achieved by NERC knowing of this within 1 hour and the need for NERC to know this within 1 hour to meet its objective of analyzing events has not been justified or explained.Loss of all monitoring or voice communication capability (affecting a BES control center for ? 30 minutes):-Does this event mean that ALL capability at both the primary and backup control centers or just one?Forced intrusion at a BES facility (report if you cannot reasonably determine likely motivation, i.e., intrusion to steal copper or spray graffiti is not reportable unless it affects (affects ? not effects) the reliability

Organization	Yes or No	Question 11 Comment
		of the BES):-What is a ?BES facility?? It is not clear for the purposes of complying with this standard what it means to affect the reliability of the BES. Deferred for ECMS review and additional comments.Risk to BES equipment (examples include a train derailment adjacent to BES equipment that either could have damaged the equipment directly or has the potential to damage the equipment, e.g., flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center, and report of suspicious device near BES equipment.):-In the footnote, delete ?could have? from ??either could have damaged?? Something that could cause evacuation of a control center does not pose a risk to damaging BES equipment. The threshold is ?from a non-environmental physical threat? but the example (toxic cargo) IS an environmental threat.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. The DSR SDT reviewed the term 'Energy Emergency' and has removed it from Attachment 1.		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	No	The one hour reporting timeline is unrealistic for this event. In general it looks like other events requiring the 1 hour reporting timeline are for event that are ?initiated? by the system operator. (ie load shedding, public load reduction, EEP?). Loss of BES equipment is in general 24 hour reporting timeline. It should be, ?as soon as possible but within 24 hours."
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received.		
Indeck Energy Services	No	Comments were included in previous comments.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received.		
BC Hydro		For the change from 24hr to 1hr reporting for events, 1 hour goes extremely quickly in these types of events and it will be difficult to report anything meaningful. As the RC is kept informed during the event why is the report required within 1hr?
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. EOP-004-2 is an after the fact reporting Standard. The entity experiencing an event is required to inform their RC per other NERC Standards.		
Brazos Electric Power Cooperative	No	Question applicability to DP.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed and updated the entities that need to report an event. Some have been reduced to a single entity where others have multiple entities. These multiple entities will have different views of the event, and will be able to provide the		

Organization	Yes or No	Question 11 Comment
ERO and others with a different view of what has happened. The entire Attachment 1 has been updated to reflect the comments that were received.		
Progress Energy	No	Progress Energy appreciates the effort of the Standard Drafting Team, but we do have some issues with the content of Attachment 1. The loss of three Transmission Elements can occur with a single transmission line outage. Progress is concerned that the possible frequency of this type of reporting could be an extreme burden. Under the column ?Entity with Reporting Responsibility,? why do all related entities have to report the same event? (i.e. do the RC and the TOP in the RC footprint both have to report an event, or is it either/or? The word ?Each? implies separate reports. What is the Reliability-based need for both an RC and the BA/TOP/GO within the footprint to file the same report for the same event?) For vertically integrated companies it should be clear that only one report is required per Impact Event that will cover the reporting requirements for all registered entities within that company.The ?damage or destruction of BES equipment? footnote contains the language ?Significantly affects the reliability margin?.? The word significantly should not be used in a Standard because it is subjective. Reliability margin is also undefined. System Operators must be trained on how to comply with the Standard, and thus objective criteria must be developed for reporting. ?1 hour after occurrence? places a burden on System Operators for reporting when response to and information gathering dealing with the Impact Event may still be occurring. There is a note that states that the timing guidelines may not be met ?under certain conditions?? but then requires a call to both its Regional Entity and notification to NERC. The focus should be on the event response and this type of reporting should occur ?within an hour or as soon as practical.? It is unclear what the voltage deviations of +-10% based on (i.e. is that +-10% of nominal voltage? This may require new alarm set-points to be placed in service in Energy Management Systems in order for entities to able to prove in an audit that they reported all occurrences of voltage exceeding the 10% limit for 15 minutes or more. It has been stated by Regional Entity audit and enforcement personnel that attestations cannot be used to ?prove the positive.?)The word ?potential? should be removed from Attachment 1 and from the definition of Impact Event. An event is either an Impact Event or not. If an entity has to evacuate its control center facility temporarily for a small fire, or any other such minor occurrence, then it activates its EOP-008 compliant backup control center, and there is no impact to reliability, then why does there need to be a report generated?The ?Forced Intrusion? category is problematic. The footnote 3 states: ?Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects (sic) the reliability of the BES).? ?Reasonably determine likely motivation? makes this subjective. If someone breaks into a BES substation fence to steal copper, is interrupted and leaves, then entity personnel determine someone tried to break into the substation, but cannot determine why, then this table requires a report to be filed within an hour. It is unclear what the purpose of such a report would be. Progress agrees that multiple reports in a short time across multiple entities may indicate a larger issue.
Response: The DSR DT thanks you for your comment. The entire Attachment 1 has been updated to reflect the comments that were received. Footnotes		

Organization	Yes or No	Question 11 Comment
have been updated per comments received.		
Liberty Electric Power LLC	Yes	A qualified yes here - please clarify footnote 1 to the table. Are the listed qualifications "and" or "or" statements -IOW, if destruction of BES equipment through human error does not have the potential to result in the need for emergency actions, is it still reportable? If a 18-240 KV step-up transformer suffers minor damage because a conservator tank was valved out, is this reportable under this definition?
Response: The DSR DT thanks you for your comment. Footnotes have been update to reflect comments received. This proposed Standard is targeted at BES level Thresholds for Reporting as outlined in Attachment 1.		
Ingleside Cogeneration LP	Yes	We believe that there should be close, if not perfect, synchronization between the ERO?s Event Analysis Process and Attachment 1 since they share the same ultimate goal as EOP-004-2 to improve industry awareness and BES reliability.
Response: The DSR DT thanks you for your comment. EOP-004-2 is an after the fact reporting Standard and the reports submitted by entities complying with the standard may be used by the NERC Event Analysis Program to review reported events. The Event Analysis Program may change their categories of events at anytime, but revisions to an approved standard must follow the standards development process embodied in the NERC Standard Processes Manual. Despite the differences in process, the DSR SDT is working closely with the Event Analysis Working Group to ensure alignment between the standard and the program to the maximum extent possible.		
Occidental Power Marketing	Yes	There does not appear to be any reportable events for LSEs that do not own, operate, or control BES assets (or assets that directly support the BES) in Attachment 1. This would support removing such entities from the Applicability.
Response: The DSR DT thanks you for your comment. The DSR SDT understands that every LSE may not own or operate BES assets. If of the LSE does not own or operate BES assets, then EOP-004-2 would not be applicable to that LSE. Since CIP-002 and CIP-008 are applicable to LSEs they will be required to be applicable under EOP-004-2 for cyber incidents.		
Farmington Electric Utility System	Yes	
Platte River Power Authority	Yes	
New Harquahala Generating Co.	Yes	
Western Electricity Coordinating	Yes	

Organization	Yes or No	Question 11 Comment
Council		
Midwest ISO Standards Collaborators	Yes	
Southern Company	Yes	
SRP	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
American Municipal Power	Yes	

12. Do you agree with the proposed measures for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: The majority of commenters agree with the proposed measures. Since two requirements were removed, the DSR SDT did a complete review of the Requirements and associated Measure and assured that Measurements did not add to any Requirement. The Measures have been rewritten to reflect strict accuracy to each Requirement and provide a minimum measure required for an entity to be compliant.

Organization	Yes or No	Question 12 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation	No	Several of the measures appear to introduce items that are not required by the standard. For instance, R3 requires that a test of the communications process be performed, however Measure 3 indicates that a mock impact event be performed. Measure 4 indicates that personnel be listed in the plan and be trained on the plan, however there is no requirement to include people in the plan or to train them.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
Northeast Power Coordinating Council	No	Concerns with M5:a. As suggested in the response to Question 10 above, R5 should be combined with R2; b. If R5 to remain as is, then M5 goes beyond the requirement in R5 in that it asks for evidence to support the type of Impact Event experienced. Attachment 2 already requires the reporting entity to provide all the details pertaining to the Impact Event. It is not clear what kind of additional evidence is needed to ?support the type of Impact Event experienced?. Also, the date and time of the Impact Event is provided in the reporting form. Why the need to provide additional evidence on the date and time of the Impact Event?
Response: The DSR SDT thanks you for your comment. Requirement 2 has been deleted as requested by the industry. Requirement R5 (now R2) was revised along with the measure: R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment]. M2. Responsible Entities shall provide a record of the type of event experienced; a dated copy of the Attachment 2 form or OE-417 report; and dated and time-		

Organization	Yes or No	Question 12 Comment
stamped transmittal records to show that the event was reported.		
Pacific Northwest Small Public Power Utility Comment Group	No	It is unclear when reporting to the Compliance Enforcement Authority is required. Does the registered entity report initially, and then anytime a change to the plan is made, or a drill is performed. Or is the information only provided following a request of the Compliance Enforcement Authority, and if so what is the acceptable time limit to respond?
Response: The DSR SDT thanks you for your comment. The Measure is designed to inform applicable entities of the minimum acceptable evidence needed to prove compliance with a requirement. The reference to Compliance Enforcement Authority has been removed since it does not assist an entity in the minimum level of evidence needed per the requirement.		
Dominion	No	1) M1 is open ended. Suggest adding ?on request? to the end of the sentence as written; 2) M4 requires evidence of ?when internal personnel were trained; however, Requirement R4 does not require training.
Response: The DSR SDT thanks you for your comment. The Measure is designed to inform applicable entities of the minimum acceptable evidence needed to prove compliance with a requirement. The reference to Compliance Enforcement Authority has been removed since it does not assist an entity in the minimum level of evidence needed per the requirement.		
SPP Standards Review Group	No	The measures are written as if they are adding requirements to the standards. Using wording such as ?shall provide? gives this implication. We would suggest wording such as ?examples of acceptable evidence to demonstrate compliance may be??See Question 6 for comments regarding M1.See Question 8 for comments regarding M3.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
Midwest ISO Standards Collaborators	No	We disagree with Measurement 4. It implies that the review must be conducted in person. Why could other means such as a web training or a reminder memo not satisfy the requirement? Because Requirement 1 does not require submittal of the Operating Plan, Operating Process and/or the Operating Procedure, Measurement 1 should only require submittal to the Compliance Enforcement Authority upon its request.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement. Requirement 4 has been deleted.		
FirstEnergy	No	Measure M4 includes the phrase ?when internal personnel were trained on the responsibilities in the plan? implies the Requirement R4 requires training. R4 is only requiring the review of a document of the necessary

Organization	Yes or No	Question 12 Comment
		personnel and that the rest of the measure covers the needed evidence for R4. This phrase in the measure should be removed. We suggest the following for M4:M4. Responsible Entities shall provide the materials presented to verify content and the association between the people listed in the plan and those who participated in the review, documentation showing who was present.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement. Requirement 4 has been deleted.		
SERC OC Standards Review Group	No	The measures should be revised to match the general nature of the comments we have made on each requirement.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
PJM Interconnection LLC	No	1. We disagree with M4 as it seems to indicate that all training needs to be in person and precludes any form of Computer Based Training (CBT). 2. As indicated in 10, R5 is redundant as R2 already required an entity to report any Impact Events by executing/implementing its Impact Event Operating plan. If R5 is to remain as is, then M5 goes beyond the requirement by requiring the entity to produce evidence of compliance for the type of Impact Event experienced. It is not clear as to what additional evidence is needed to ?support the type of Impact Event experienced?.
The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
We Energies	No	M1 contains a redundancy: It currently reads, ?Each Responsible Entity shall provide the current in force Impact Event Operating Plan to the Compliance Enforcement Authority.? (?In force? is the same as ?current?.)M2: Change ?Impact Event? to ?Impact Event listed in Attachment 1?.M3: This is an additional requirement. R3 does not require a mock Impact Event. R3 requires a test of the communicating Operating Process. As stated above, R3 and M3 should be deleted.M4: This is written assuming classroom training. R4 does not require formal training much less classroom training. R4 requires that those (internal) personnel who have responsibilities in the plan review the Impact Event Operating Plan.M5: When we report, how do we show to an auditor that we reported ?using the plan?? Delete the reference to ?the plan?.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		

Organization	Yes or No	Question 12 Comment
Compliance & Responsiblity Organization	No	See comments set forth in number 2.
Exelon	No	? M1 - Suggest rewording to state "Each Responsible Entity shall provide the current revision of the Impact Event Operating Plan or equivalent implementing process"? M3 ? Need to provide more guidance on evidence of compliance to meet R.3 The DSR SDT needs to provide more guidance on the objectives and format of the drill expected (e.g., table top, simulator, mock drill) and what evidence will be required to illustrate compliance.? M5 - Suggest that the DSR SDT provide a note or provision to allow for the DOE OE-417 reporting form be submitted by the most knowledgeable functional entity (e.g., the TOP or RC) experiencing the event.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
City of Tallahassee (TAL)	No	M3 & M4 should be modified if comments above (#8 and #9) are incorporated.M4 - Providing the ?materials presented? is beyond the scope of compliance. This constitutes a review of the training program which is beyond the scope of the standard. Review of attendance sheets should be sufficient. The personnel will be listed in the Plan/Process/Procedure. Modify M4: Responsible Entities shall provide evidence of those who participated in the review, showing who was present and when internal personnel were trained on their responsibilities in the plan.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
Tenaska	No	The proposed R1 through R4 should be deleted and a revised version of R5 should become R1. The proposed measures for the new R1 should be revised accordingly.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
American Municipal Power	No	M1-M4 should be eliminated and M5 should be revised to incorporate a simplified R5. M5 - Date and time of submitted report
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		

Organization	Yes or No	Question 12 Comment
Liberty Electric Power LLC	No	Due to disagreement with R3 and R4.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
Arkansas Electric Cooperative Corporation	No	We applaud the drafting team's effort in crafting more meaningful measures. However, we have concerns with the measures reading like requirements in stating Responsible Entities "shall" do something. We suggest crafting the measures to provide acceptable, but not all exclusive, forms of evidence by stating something similar to "Acceptable forms of evidence may include??
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
New Harquahala Generating Co.	No	See R3 comments
Response: The DSR SDT thanks you for your comment. Please see R3 responses.		
Consumers Energy	No	We understand that DOE is migrating to an on-line reporting facility rather than the email-submitted OE-417. If they do so, Form OE-417will not be available for providing to NERC, and the reporting specified by EOP-004 will be duplicative of that for DOE. We recommend that NERC, RFC and the DOE work cooperatively to enable a single reporting system in which on-line reports are made available to all appropriate parties.
Response: The DSR SDT thanks you for your comment. The DSR SDT has been working with the U.S. Department of Energy (DOE) to streamline the reporting process. The DOE Form OE-417 will be accepted at NERC if you are reporting an event to the DOE.		
Independent Electricity System Operator	No	We do not have any issues with Measures M1, M2 and M4, but have a concern with M3 and a couple of concerns with M5:M3: This Measure contains a requirement for the Responsible Entities to conduct a mock Impact Event. We disagree to have this included in the Measure. R3 requires the Responsible Entity to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The Measure should adhere to this condition only. We suggest to change the wording to:The Responsible Entity shall provide evidence that it conducted a test of it its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The time period between actual and or mock Impact Events shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, documentation or a report on an actual Impact Event.M5: a. As

Organization	Yes or No	Question 12 Comment
		suggested above, R5 should be combined with R2;b. If R5 to remain as is, then M5 goes beyond the requirement in R5 in that it asks for evidence to support the type of Impact Event experienced. Attachment 2 already requires the reporting entity to provide all the details pertaining to the Impact Event. It is not clear what kind of additional evidence is needed to ?support the type of Impact Event experienced?. Also, the date and time of the Impact Event is provided in the reporting from. Why do we need to provide additional evidence on the date and time of the Impact Event?
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement. Requirement R5 (now R2) was revised along with the measure: R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment]. M2. Responsible Entities shall provide a record of the type of event experienced; a dated copy of the Attachment 2 form or OE-417 report; and dated and time-stamped transmittal records to show that the event was reported.		
ISO New England, Inc	No	We do not have any issues with Measures M1, M2 and M4, but have a comment on M3 and a couple of concerns with M5:M3: This Measure contains a requirement for the Responsible Entities to conduct a mock Impact Event. We disagree to have this included in the Measure. R3 requires the Responsible Entity to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The Measure should adhere to this condition only. We suggest to change the wording to:The Responsible Entity shall provide evidence that it conducted a test of it its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The time period between actual and or mock Impact Events shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, documentation or a report on an actual Impact Event.M5:a. As suggested above, R5 should be combined with R2;b. If R5 to remain as is, then M5 goes beyond the requirement in R5 in that it asks for evidence to support the type of Impact Event experienced. Attachment 2 already requires the reporting entity to provide all the details pertaining to the Impact Event. It is not clear what kind of additional evidence is needed to ?support the type of Impact Event experienced?. Also, the date and time of the Impact Event is provided in the reporting from. Why do we need to provide additional evidence on the date and time of the Impact Event?c. We disagree with Measurement 4. It implies that the review must be conducted in person. Why couldn?t other means such as web training or a reminder memo not satisfy the requirement?
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement. Requirement R5 (now R2) was revised along with the measure:		

Organization	Yes or No	Question 12 Comment
R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment]. M2. Responsible Entities shall provide a record of the type of event experienced; a dated copy of the Attachment 2 form or OE-417 report; and dated and time-stamped transmittal records to show that the event was reported.		
Calpine Corp	No	Requirements R1, R2, R3, and R4 are unnecessary, as discussed above. The measure for Requirement R5 should focus on the need to report accurately and promptly, not on a Responsible Entity?s ?Operating Plan?. If the Requirements are retained, the measures should state in much greater detail what actions and documentation are required for compliance.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement. Requirement R5 (now R2) was revised along with the measure: R2. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1. [Violation Risk: Factor: Medium] [Time Horizon: Operations Assessment]. M2. Responsible Entities shall provide a record of the type of event experienced; a dated copy of the Attachment 2 form or OE-417 report; and dated and time-stamped transmittal records to show that the event was reported.		
CenterPoint Energy	No	M1: CenterPoint Energy recommends that the phrase ?current in force? be updated to ?current? or ?currently effective?. Additionally, CenterPoint Energy suggests clarifying M1 by adding ?within 30 days upon request?, which would be consistent with language found in measures in other standards. The revised measure would read, ?Each Responsible Entity shall provide the currently effective Impact Event Operating Plan to the Compliance Enforcement Authority within 30 days upon request.? M2: If R2 is deleted (as recommended in response to Question 7), then M2 should be deleted.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement. R2 was deleted along with the measure M2.		
ExxonMobil Research and Engineering	No	Measure M3 introduces a psuedo-requirement by implying you are able to reset the testing clock if you implement our Impact Event Operating Plan in response to an Impact Event. This should be covered in Requirement R3. Measure M4 should refer to positions and evidence that people occupying those positions participated in the annual review of the Impact Event Operating Plan. Given the number of individuals involved in operations and the cycle of promotions and reassignments, it?s unreasonable to expect an entity

Organization	Yes or No	Question 12 Comment
		to identify specific individuals in their Impact Event Operating Plan. As the one hour time window is not long enough for entities to report all types of events when responding to the impact the Imact Event had on its facility, Measure M5 should be modified to include voice recordings and log book entries to capture verbal information reported to required parties.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
Constellation Power Generation	No	See CPG?s earlier comments regarding the Requirements and Measures.
Response: The DSR SDT thanks you for your comment. See response to comments on Requirements and Measures.		
Georgia System Operations Corporation	No	There are a lot of inconsistencies between the requirements and the measures. The measures add requirements that are not stated in the requirements. The measures need to be made consistent with the requirements and to not add to them. Also see comments on requirements earlier for language to move from the measures into the requirements.M2: Remove "on its Facilities." The word "its" leads to a lot of confusion regarding who reports what. Attachment 1 should make clear "what" needs to be reported. The entities' operating plan should make it clear as to who should report each "what." Furthermore, not all Impact Events are "on Facilities."M3: Replace "that it conducted a mock Impact Event" with "that it conducted a test of its Operating Process." Delete "The time period between actual and or mock Impact Events shall be nor more than 15 months."M4: The measure says that documentation showing when personnel were trained is required. R4 does not require training. The requirement and the measure should be made clear and consistent.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	No	M3 -The testing of the Plan by drill or mock impact event is unnecessary and burdensome.
Response: The DSR SDT thanks you for your comment. The Measure M3 has been revised as follows: M3. The Responsible Entity shall provide evidence that it conducted a test of the communication process in its Operating Plan events created pursuant to Requirement R1, Part 1.3. Implementation of the communication process as documented in its Operating Plan for an actual event may be used as evidence to meet this requirement. The time period between an actual event or test shall be no more than 15 months. Evidence may include, but is not limited to, operator logs,		

Organization	Yes or No	Question 12 Comment
voice recordings, or dated documentation of a test. (R3) The intent of R3 is to ensure that the communications process of the Operating Plan works when needed. The annual test is not burdensome and an actual event will take the place of the test.		
Farmington Electric Utility System	No	See comments in requirements for R3 and R4
Response: The DSR SDT thanks you for your comment. See response to comments on R3 and R4.		
Indeck Energy Services	No	M1 is OK. M2 should be about implementation, not about any particular events--M5 is about events. Implementation would include distribution and training. M3 should be modified to reflect a training review by entities that cannot cause a Reportable Disturbance or reportable DOE OE-417 event and for the others documentation of an actual event (which is not included in the present M3) or a drill or mock event. M4 is OK. M5 should only include the reports submitted and the date of submission. Further evidence of the event is redundant.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
Brazos Electric Power Cooperative	No	M2 and M5 appear to duplicate each other.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement. R2/M2 have been deleted and R5/M5 is now R2/M2.		
Progress Energy	No	M3 states that ?In the absence of an actual Impact Event, the Responsible Entity shall provide evidence that it conducted a mock Impact Event?? Does this mean that, if an entity experiences an Impact Event that is reportable, then the entity does not have to perform its annual test? If so, this should be made clear in the Requirement.
Response: The DSR SDT thanks you for your comment. That is the intent of the requirement. The Rationale box has been revised to express this intent. The measure now reads: The Responsible Entity shall provide evidence that it conducted a test of the communication process in its Operating Plan for events created pursuant to Requirement R1, Part 1.3. Implementation of the communication process as documented in its Operating Plan for an actual event may be used as evidence to meet this requirement. The time period between an actual event or test shall be no more than 15 months. Evidence may include, but is		

Organization	Yes or No	Question 12 Comment
not limited to, operator logs, voice recordings, or dated documentation of a test. (R3)		
Occidental Power Marketing	Yes	In general, the measures are okay. However, as mentioned above for R3, there needs to be more specificity as to what is acceptable as a "mock Impact Event" for auditing purposes--especially for small entities such as LSEs that do not own, operate, or control BES assets.
Response: The DSR SDT thanks you for your comment. Each measure has been rewritten for the associated requirement to reflect only what is within the requirement.		
SDG&E	Yes	
Lakeland Electric	Yes	
New Harquahala Generating Co.	Yes	
Bonneville Power Administration	Yes	
Midwest Reliability Organization	Yes	
PSEG Companies	Yes	
Pepco Holdings Inc and Affiliates	Yes	
Southern Company	Yes	
SRP	Yes	
APX Power Markets	Yes	
Manitoba Hydro	Yes	
Sweeny Cogeneration LP	Yes	
American Electric Power	Yes	

Organization	Yes or No	Question 12 Comment
USACE	Yes	
Ameren	Yes	
BGE		No position or comments.
Platte River Power Authority	Yes	
Alliant Energy	Yes	
PPL Electric Utilities	Yes	
Lincoln Electric System	Yes	
American Transmission Company	Yes	
Ingleside Cogeneration LP	Yes	
Duke Energy	Yes	

13. Do you agree with the proposed Violation Risk Factors for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: Many stakeholders suggested that the reporting of events after the fact only justified a VRF of Lower for each requirement. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.

Organization	Yes or No	Question 13 Comment
Northeast Power Coordinating Council	No	If R5 is to remain as is, then the VRF should be a Lower, not a Medium. R5 stipulates the form to be used. It is a vehicle to convey the needed information, and as such it is an administrative requirement. Failure to use the form provided in Attachment 2 or the DOE form does not lead to unreliability.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		

Organization	Yes or No	Question 13 Comment
Bonneville Power Administration	No	R2, R3 and R4 should be lower VRFs than R5 and R1.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
PSEG Companies	No	If Requirements 1-5 remain intact the Violation Risk Factor should be reduced to a Lower not a Medium since this is an administrative requirement and does not impact the reliability of the BES.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Dominion	No	All the VRFs are "Medium." Since the requirements deal with after-the-fact reporting and the administration of reporting plans, procedures, and processes; all VRFs should be "Lower."
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with		

Organization	Yes or No	Question 13 Comment
the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Pepco Holdings Inc and Affiliates	No	This standard involves after the fact reporting of events. Other standards deal with the real time notifications. How do the risk factors between the two line up? A VRF of Low would seem appropriate, since a violation would not affect the reliability of the BES.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
SPP Standards Review Group	No	These are reporting requirements and therefore do not deserve the "medium" VRF. We suggest making the VRFs for all requirements for EOP-004-2 "low."
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can		

Organization	Yes or No	Question 13 Comment
communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Midwest ISO Standards Collaborators	No	All violation risk factors should be Lower. All requirements are administrative in nature. While they are necessary because a certain amount of regulatory reporting will always be required, a violation will not in any direct or indirect way lead to reliability problem on the Bulk Electric System
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
FirstEnergy	No	1. We believe that Requirement 5 does not warrant a "Medium" risk factor. Not using a particular form is strictly administrative in nature and the VRF should be "Low." 2. We believe that Requirement 4 does not warrant a "Medium" risk factor. For example, a simple review of the process does not have the same impact on the Bulk Electric System as the implementation of the Operating Plan per R2. Therefore, we believe R4 is at best a "Low" risk to the BES.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these		

Organization	Yes or No	Question 13 Comment
events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
SERC OC Standards Review Group	No	How can an after-the-fact report require a VRF greater than low?
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
PJM Interconnection LLC	No	All VRFs should be lower as Requirements 1-5 are all administrative in nature. A violation of any of these requirements does not directly or indirectly affect the reliability of the BES.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
We Energies	No	All VRFs should be Lower. They are all administrative and will not affect BES Reliability.

Organization	Yes or No	Question 13 Comment
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
LG&E and KU Energy LLC		
Compliance & Responsiblity Organization	No	See comments set forth in number 2.
Response: The DSR SDT thanks you for your comment. See response to comments on Question 2.		
Exelon	No	R.4 should be a low risk factor, this is an administrative requirement with no contribution to reliability.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
City of Tallahassee (TAL)	No	R1 is administrative in nature (must have a document) and should be Lower.

Organization	Yes or No	Question 13 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT concurs and has assigned a "lower" VRF for Requirement R1.		
United Illuminating Co	No	R3 should be Low. It is a test of the communication Plan which is use of telephone and email.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
American Municipal Power	No	No, this is not acceptable. Eliminate R1-R4. Change R5 to Lower.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Liberty Electric Power LLC	No	See Q 12.
Response: The DSR SDT thanks you for your comment. Please see response to Question 12.		

Organization	Yes or No	Question 13 Comment
Manitoba Hydro	No	Reduce the Long Term Planning items to Lower VRF. The planning items will not have the same impact on the reliability of the system as real time operations.
Response: The DSR SDT thanks you for your comment. Each Requirement is in the Operations Assessment or Operations Planning time horizon. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Independent Electricity System Operator	No	If R5 were to remain as is, then the VRF should be a Lower, not a Medium since R5 stipulates the form to be used. It is a vehicle to convey the needed information, and as such it is an administrative requirement. Failure to use the form provided in Attachment 2 or the DOE form does not give rise to unreliability.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
ISO New England, Inc	No	If R5 is to remain as is, then the VRF should be a Lower, not a Medium since R5 stipulates the form to be

Organization	Yes or No	Question 13 Comment
		used. It is a vehicle to convey the needed information, and as such it is an administrative requirement. Failure to use the form provided in Attachment 2 or the DOE form has no impact on reliability. All violation risk factors should be Lower. All requirements are administrative in nature. While they are necessary because a certain amount of regulatory reporting will always be required, a violation will not in any direct or indirect affect reliability.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Calpine Corp	No	Requirements R1, R2, R3, and R4 are unnecessary, as discussed above. If retained, the violation risk factors should be low for those Requirements, as they all simply support the requirement to actually report correctly stated in Requirement R5.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
ExxonMobil Research and	No	VRFs, VSLs, and THs ideally should be based on the impact event type; alternatively a low VRF seems more

Organization	Yes or No	Question 13 Comment
Engineering		appropriate for this requirements of this standard.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Georgia System Operations Corporation	No	Failing to report to NERC any of many of the listed events does not present a reliability risk. The exception to this would be those threat events where the ES-ISAC needs to be notified. The object of the standard is to prevent or reduce the risk of Cascading. Reporting system situations to appropriate operating entities who can take some mitigating action (e.g., a LSE reporting to its BA or a BA reporting to its RC) and reporting threats to law enforcement officials could prevent or reduce the risk of Cascading but reporting to NERC (except for events where the ES-ISAC needs to know) is unlikely to do that. Reporting of most of the listed events to NERC does not meet the objective of this standard and should be removed from this standard. Such events should be reported to NERC through some other (than a Reliability Standard) requirement for reporting to NERC so that NERC can accomplish its mission of analyzing events. Analyzing events may lead to an understanding that could reduce the future risk of Cascading but analyzing events cannot be performed in time to reduce any impending risks.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for		

Organization	Yes or No	Question 13 Comment
EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Indeck Energy Services	No	If there are any, they should all be Low because this is reporting of historical events. There is no direct effect on BES reliability. Some effect could occur if someone reacts to the reports, but many are concerning unpreventable events.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement 2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement 3 is insurance to make sure that an entity can communicate information about events. Requirement 2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	No	
Progress Energy	No	
BGE	Yes	No comments.
Platte River Power Authority	Yes	
Alliant Energy	Yes	
Midwest Reliability Organization	Yes	
Southern Company	Yes	
SRP	Yes	

Organization	Yes or No	Question 13 Comment
SDG&E	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
Arkansas Electric Cooperative Corporation	Yes	
Sweeny Cogeneration LP	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
American Transmission Company	Yes	
Ingleside Cogeneration LP	Yes	
Duke Energy	Yes	

14. Do you agree with the proposed Violation Severity Levels for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: Most commenters agreed with the VSLs. The DSR SDT has deleted R4 and R2, and R5 has become R2. The VSLs have been aligned with the revised requirements. The 'Severe' rating for excessively long reporting times has been retained as the DSR SDT believes that fairly reflects the definition of 'Severe' i.e., The performance or product measured does not substantively meet the intent of the requirement.

Organization	Yes or No	Question 14 Comment
Northeast Power Coordinating Council	No	No major issues with the proposed VSLs. However, because of the preceding comments, want to see the next revision of the draft.
Response: The DSR SDT thanks you for your comment.		
Bonneville Power Administration	No	For R5 VSL's: suggest moving the 1-2 hours down one level to Moderate and move the >2 hours down to High with a range of 2-8 hours. Leave the "Failed to Submit" in the Severe category.
Response: The DSR SDT thanks you for your comment. The DSR SDT has increased most reporting timeframes to 24 hours. Those that still require 1 hour reporting have been adjusted to better align with the 24 hour VSLs. Namely, taking twice as long to report is a 'Medium' VSL. The 'Severe' rating for excessively long reporting times has been retained as the DSR SDT believes that fairly reflects the definition of 'Severe' i.e., The performance or product measured does not substantively meet the intent of the requirement.		
Western Electricity Coordinating Council		Regarding the proposed VSLs for R3, since communication testing involves multiple parties it would be more appropriate to base severity level on the number of applicable parties which were not tested rather than how long after 15 months it took to do the test. The standard already builds in a 3 month leeway, In reality the way it is written almost guarantees a lower severity level.
Response: The DSR SDT thanks you for your comment. VSLs reflect the degree to which the requirements are met. The DSR SDT envisions that communication testing will include all parties referenced in the entity's operating plan. Failure to test any part of that communication process is a failure of that Part of the requirement.		
Pepco Holdings Inc and Affiliates	No	This standard involves after the fact reporting of events. Other standards deal with the real time notifications. How do the severity level between the two line up? See above VRF comments.

Organization	Yes or No	Question 14 Comment
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the VSLs appropriately align with the NERC Guidelines.		
SPP Standards Review Group	No	Requirement 4: We would suggest the following:Low ? The Responsible Entity reviewed its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 15 calendar months but less than 18 calendar months since the last review.Moderate - The Responsible Entity reviewed its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 18 calendar months but less than 21 calendar months since the last review.High - The Responsible Entity reviewed its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 21 calendar months but less than 24 calendar months since the last review.Severe - The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan within 24 calendar months since the last review.Requirement 5: With our suggested deletion of Requirement 5, we further suggest deleting the VSLs associated with Requirement 5.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R4 and R2, and R5 has become R2.		
SERC OC Standards Review Group	No	The VSLs should reflect the comments on the requirements above.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R4 and R2, and R5 has become R2. The VSLs have been aligned with the revised requirements.		
PJM Interconnection LLC	No	VSLs should reflect the comments on the VRFs above.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the VSLs appropriately align with the NERC Guidelines.		
We Energies	No	Change the VRFs as indicated above and the Time Horizons as indicated below.
Response: The DSR SDT thanks you for your comment. Please see responses to those comments.		
Compliance & Responsiblity Organization	No	See comments set forth in number 2.
Response: The DSR SDT thanks you for your comment. Please see responses Question 2.		

Organization	Yes or No	Question 14 Comment
Exelon	No	Suggest rewording the 1 hour reporting for High and Severe to state "communicate or submit" a report within ? depending on the severity of the event, an actual report may not be feasible. Similar to an NRC event report, a provision should be made for verbal notifications in lieu of an actual submitted report. An entity should not be penalized for failing to submit a written report within 1 hour if the communications were completed within the 1 hour time period meeting the intent of the Standard.
Response: The DSR SDT thanks you for your comment. Attachment 1 allows you to provide a verbal report under the conditions you contemplate.		
SDG&E	No	This Reliability Standard provides a list of reporting requirements that are applicable to registered entities, thus it is a paperwork exercise; therefore, SDG&E recommends that none of the requirements should exceed a ?Moderate? Violation Severity Level. Failure on the part of an applicable Registered Entity to provide an event report will have no immediate impact on the Bulk Electric System.
Response: The DSR SDT thanks you for your comment. VSLs describe how fully an entity meets the requirements and are not a measure of severity or impact. These items are captured in the VRFs.		
American Municipal Power		No, this is not acceptable. Eliminate R1-R4 and change R5. Severe: n/aHigh VSL: n/aMedium VSL: No report for a reportable eventLow VSL: Late report for a reportable event
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R4 and R2, and R5 has become R2. The VSLs have been aligned with the revised requirements.		
Liberty Electric Power LLC	No	See Q 12.
Response: The DSR SDT thanks you for your comment. Please see responses to Question 12.		
Consumers Energy	No	1. In reference to the Impact Event addressing ?Loss of Firm load for greater than or equal to 15 minutes?, this is likely to occur for most entities most frequently during storm events, where the loss of load builds slowly over time. In these cases, exceeding the threshold may not be apparent until a considerable time has lapsed, making the submittal time frame impossible to meet. Even more, it may be very difficult to determine if/when 300 MW load (for the larger utilities) has been lost during storm events, as the precise load represented by distribution system outages may not be determinable, since this load is necessarily dynamic. Suggest that the threshold be modified to ?Within 1 hour after detection of exceeding 15-minute threshold?. Additionally, these criteria are specifically storm related wide spread distribution system outages. These events do not pose a risk to the BES.2. Many of the Impact Events listed are likely to occur, if they occur, at widely-distributed system facilities, making reporting ?Within 1 hour after occurrence

Organization	Yes or No	Question 14 Comment
		is identified? possibly impractical, particularly in order to provide any meaningful information. Please give consideration to clearly permitting some degree of investigation by the entity prior to triggering the ?time to submit?.3. Referring to the ?Fuel Supply Emergency? Impact Event, OE-417 requires 6-hour reporting, where the Impact Event Table requires 1-hour reporting. The reporting period for EOP-004-2 should be consistent with OE-417.
Response: The DSR SDT thanks you for your comment. The DSR SDT has increased almost all reporting timeframe to 24 hours. Also, the fuel supply emergency has been removed from Attachment 1. Reporting period was chosen to meet NERC needs, you may have more restrictive periods for OE-417, but that is outside the jurisdiction of the DSR SDT.		
Calpine Corp	No	Requirements R1, R2, R3, and R4 are unnecessary, as discussed above. If retained, the violation risk factors should be low for those requirements, as they all simply support the requirement to actually report correctly stated in Requirement R5.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R4 and R2, and R5 has become R2. The VSLs have been aligned with the revised requirements.		
CenterPoint Energy	No	CenterPoint Energy believes that the Severe VSL for R5 (Reporting) in the current draft incorrectly equates 2X reporting with failure to submit a report. CenterPoint Energy believes the VSLs for R5 should all reflect a factor increase in time. For example, the lower VSL should be 1.5X the reporting time frame. The Moderate VSL should be 2x the reporting time frame. The High VSL should be 3x the reporting time frame. The Severe VSL should be failure to report.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R4 and R2, and R5 has become R2. The VSLs have been aligned with the revised requirements. The 'Severe' rating for excessively long reporting times has been retained as the DSR SDT believes that fairly reflects the definition of 'Severe' i.e., The performance or product measured does not substantively meet the intent of the requirement.		
ExxonMobil Research and Engineering	No	VRFs, VSLs, and THs ideally should be based on the impact event type; alternatively a low VRF seems more appropriate for the requirements of this standard.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the VSLs and time horizons appropriately align with the requirements and NERC Guidelines. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2)		

Organization	Yes or No	Question 14 Comment
and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001.		
Indeck Energy Services	No	There should be only Lower VSL's. This is reporting of historical events and there is no direct effect on BES reliability. How does missing 3 parts of R1 compare to tripping a 4,000 MW generating station because vegetation was not properly managed? Just because there are 4 levels, doesn't mean that all Standards need to use them all. If you step back, and think about causes of cascading outages, reporting events 1 hour or 24 hours later has no significance. There is no direct preventative causation either.
Response: The DSR SDT thanks you for your comment. VSLs describe how fully an entity meets the requirements and are not a measure of severity or impact to the BES. These items are captured in the VRFs.		
Progress Energy	No	Progress disagrees with the High and Severe VSLs listed for R5. If an entity experiences an Impact Event and fails to submit a report within an hour as required, it may be that there are multiple mitigating circumstances. It is not reasonable to require reporting within an hour since identifying a reportable event often takes longer than this time period.
Response: The DSR SDT thanks you for your comment. The DSR SDT has increased almost all reporting timeframe to 24 hours. Also, VSLs describe how fully an entity meets the requirements and are not a measure of severity or impact to the BES. These items are captured in the VRFs.		
Georgia System Operations Corporation	No	None.
Independent Electricity System Operator		We do not have any major issues with the proposed VSLs. However, in view of our comments on some of the Questions, above, we reserve our comments upon seeing a revised draft.
Response: The DSR SDT thanks you for your comment.		
ISO New England, Inc		We do not have any major issues with the proposed VSLs. However, in view of our comments on some of the Questions, above, we reserve our comments upon seeing a revised draft.

Organization	Yes or No	Question 14 Comment
Response: The DSR SDT thanks you for your comment.		
Midwest Reliability Organization	Yes	
Midwest ISO Standards Collaborators	Yes	
Southern Company	Yes	
SRP	Yes	
City of Tallahassee (TAL)	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
United Illuminating Co	Yes	
Arkansas Electric Cooperative Corporation	Yes	
Manitoba Hydro	Yes	
Sweeny Cogeneration LP	Yes	
American Electric Power	Yes	
New Harquahala Generating Co.	Yes	
Platte River Power Authority	Yes	

Organization	Yes or No	Question 14 Comment
BGE	Yes	No comments.
Alliant Energy	Yes	
Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
American Transmission Company	Yes	
Ingleside Cogeneration LP	Yes	
Duke Energy	Yes	
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Yes	

15. Do you agree with the proposed Time Horizons for Requirements 1-5? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: Many stakeholders suggested that the Time Horizons for this standard should be Operations Assessment or Operations Planning rather than Long Term Planning. The DSR SDT agrees. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Assessment, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 has been changed to Operations Planning.

Organization	Yes or No	Question 15 Comment
Northeast Power Coordinating Council	No	For the purpose of developing and updating an Impact Event Operating Plan, there should not be any requirements that fall into the Long-term planning horizon. As the name implies, the plan is used in the operating time frame. Consistent with other plans such as system restoration plans which need to be updated and tested annually, most of the Time Horizons in that standard (EOP-005-2) are either Operations Planning or Real-time Operations. Suggest the Time Horizon for R1, R3 and R4 be changed to Operations Planning.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Assessment, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 has been changed to Operations Planning.		
Bonneville Power Administration	No	Depends on the answer to #7. If implementation means a signed and valid Plan, then it should be with Long Term. If reporting the events, then it should be Real-Time/Same Day Operations.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted the separate requirement to 'implement the plan'. The reporting obligation is now R2 with a time horizon of Operations Assessment, which is defined as 'follow-up evaluations and reporting of real time operations'.		

SPP Standards Review Group	No	Based on our previous comments in response to Question 11, we feel that the Time Horizon for R2 should be lengthened. Assigning it a Real-time Operations and Same ?day Operations timeframe has too much of an impact on real-time operations. Pushing it back will allow support personnel to do the after-the-fact reporting and keep this burden off of the operators.
Response: The DSR SDT thanks you for your comment. The reporting obligation is now R2 with a time horizon of Operations Planning, which is defined as 'follow-up evaluations and reporting of real time operations'.		
Midwest ISO Standards Collaborators	No	R2 and R5 should be Operations Assessment since it deals with after the fact reporting. R3 should included Operations Assessment since an actual event could be used as the test.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Planning, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 have been changed to Operations Planning		
SERC OC Standards Review Group	No	R2 and R5 should be in the Operations Assessment time horizon.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Planning, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 have been changed to Operations Planning		
PJM Interconnection LLC	No	R2 and R5 should be in Operations Assessment Time Horizon as they deal with ?after-the-fact? reporting.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Planning, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 have been changed to Operations Planning		
We Energies	No	R2 and R5 should be Operations Assessment.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Planning, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 have been changed to Operations Planning		

Consumers Energy	No	1. In reference to the Impact Event addressing ?Loss of Firm load for greater than or equal to 15 minutes?, this is likely to occur for most entities most frequently during storm events, where the loss of load builds slowly over time. In these cases, exceeding the threshold may not be apparent until a considerable time has lapsed, making the submittal time frame impossible to meet. Even more, it may be very difficult to determine if/when 300 MW load (for the larger utilities) has been lost during storm events, as the precise load represented by distribution system outages may not be determinable, since this load is necessarily dynamic. Suggest that the threshold be modified to ?Within 1 hour after detection of exceeding 15-minute threshold?. Additionally, these criteria are specifically storm related wide spread distribution system outages. These events do not pose a risk to the BES.2. Many of the Impact Events listed are likely to occur, if they occur, at widely-distributed system facilities, making reporting ?Within 1 hour after occurrence is identified? possibly impractical, particularly in order to provide any meaningful information. Please give consideration to clearly permitting some degree of investigation by the entity prior to triggering the ?time to submit?.3. Referring to the ?Fuel Supply Emergency? Impact Event, OE-417 requires 6-hour reporting, where the Impact Event Table requires 1-hour reporting. The reporting period for EOP-004-2 should be consistent with OE-417.
Response: The DSR SDT thanks you for your comment. The DSR SDT has increased almost all reporting timeframe to 24 hours. Also, the fuel supply emergency has been removed from Attachment 1. Reporting period was chosen to meet NERC needs, you may have more restrictive periods for OE-417, but that is outside the jurisdiction of the DSR SDT.		
Independent Electricity System Operator	No	For the purpose of developing and updating an Impact Event Operating Plan, there should not be any requirements that fall into the Long-term planning horizon. As the name implies, the plan is used in the operating time frame. And consistent with other plans such as system restoration plan which needs to be updated and tested annually, most of the Time Horizons in that standard (EOP-005-2) are either Operations Planning or Real-time Operations. We suggest the Time Horizon for R1, R3 and R4 be changed to Operations Planning.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Planning, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 have been changed to Operations Planning		

ISO New England, Inc	No	For the purpose of developing and updating an Impact Event Operating Plan, there should not be any requirements that fall into the Long-term planning horizon. As the name implies, the plan is used in the operating time frame. And consistent with other plans such as system restoration plan which needs to be updated and tested annually, most of the Time Horizons in that standard (EOP-005-2) are either Operations Planning or Real-time Operations. We suggest the Time Horizon for R1, R3 and R4 be changed to Operations Planning. The Time Horizon for R2 and R5 should be changed to Operations Assessment since they both deal with after the fact reporting.
Response: The DSR SDT thanks you for your comment. The DSR SDT has deleted R2, and R5 has become R2 with a time horizon of Operations Planning, which is defined as 'follow-up evaluations and reporting of real time operations'. R4 has been deleted and the time horizon for R1 and R3 have been changed to Operations Planning		
ExxonMobil Research and Engineering	No	VRFs, VSLs, and THs ideally should be based on the impact event type; alternatively a low VRF seems more appropriate for this requirements of this standard.
Response: The DSR SDT thanks you for your comment. With the revised standard, there are now three requirements. Requirement R1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment 1. This is procedural in nature and justifies a "lower" VRF. This requirement is administrative in nature and deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program. The two remaining requirements in EOP-004-2 are to report events based on the specifics in Attachment 1 (R2) and to test the communications protocol of the Operating Plan once per year (R3). Requirement R2 specifies that an entity is responsible for reporting events in accordance with the Operating Plan based on Attachment 1. Requirement R3 is insurance to make sure that an entity can communicate information about events. Requirement R2 specifies that the responsible entity must report an event to the appropriate entities. Some of these events are dealing with potential sabotage events. Part of the reason to report these types of events is to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events and the approved VRFs for each of the requirements is "medium." The VRFs for EOP-004-2 comport with the existing approved VRFs for both EOP-004 and CIP-001. The DSR SDT believe the VSLs and revised time horizons appropriately align.		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	No	Why shorten the normal process?
Response: The DSR SDT thanks you for your comment. The DSR SDT has revised most of the reporting timelines 24 hours.		

Indeck Energy Services	No	These requirements have no time horizon. There about history and not about the future.
Response: The DSR SDT thanks you for your comment. All NERC standards must have a time horizon associated with each requirement. Time horizons are used as a factor in determining size of a sanction.		
American Municipal Power	No	
USACE	No	
Pepco Holdings Inc and Affiliates	Yes	However, do they line up with the corresponding real time reporting procedures as mentioned above, #13 and #14?
Response: The DSR DT thanks you for your comment. Please see responses to comments #13 and #14. Since the time for reporting impact events is no more than 24 hours, the time horizon has been revised to Operations Planning.		
Midwest Reliability Organization	Yes	
PPL Supply	Yes	
Dominion	Yes	
FirstEnergy	Yes	
Southern Company	Yes	
SRP	Yes	
City of Tallahassee (TAL)	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
United Illuminating Co	Yes	

Liberty Electric Power LLC	Yes	
Arkansas Electric Cooperative Corporation	Yes	
Manitoba Hydro	Yes	
Sweeny Cogeneration LP	Yes	
New Harquahala Generating Co.	Yes	
Platte River Power Authority	Yes	
BGE		No position or comments.
Alliant Energy	Yes	
CenterPoint Energy	Yes	
PPL Electric Utilities	Yes	
Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
Farmington Electric Utility System	Yes	
American Transmission Company	Yes	
Ingleside Cogeneration LP	Yes	
Duke Energy	Yes	

Georgia System Operations Corporation	Yes	None.

16. Do you agree with the proposed Implementation Plan for EOP-004-2? If not, please explain why not and if possible, provide an alternative that would be acceptable to you.

Summary Consideration: The majority of commenters agreed with the Implementation Plan. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with. Consequently the effective date remains as first calendar day of the third calendar quarter following the regulatory approval/BOT adoption as applicable.

Organization	Yes or No	Question 16 Comment
Pepco Holdings Inc and Affiliates	No	The proposed time line is too short. It is easy to revise procedures. However developing training and integrating the training into the schedule takes time. Shorter time frame takes away adequate time to integrate into the training plan and disrupts operator schedules. Since notifications already exist and after the fact reporting does not impact BES reliability, why the need to expedite? There are many other training activities that must be coordinated with this.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
FirstEnergy	No	We believe the previous proposal for a 12 month implementation was more appropriate and suggest the team revert back to that timeframe.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
Southern Company	No	The implementation time should be 12 months after approval regardless of the elapsed time taken to get the standard approved.

Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
Exelon	No	The DSR SDT reduced the implementation from one year to between six and nine months based on the revised standard requirements. Exelon disagrees with the proposed shortened implementation timeframe. The current revision to EOP-004 still requires an entity to generate, implement and provide any necessary training for the "Impact Event Operating Plan" by a registered entity. Commenters previously supported a one year minimum; but the requirements for implementation have not changed measurably - six to nine months is not adequate to implement as written.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
SDG&E	No	SDG&E recommends a 9 month minimum timeframe for implementation.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
United Illuminating Co	No	The SDT should be specific that on the effective date an Entity will have the Operating documented and approved. The SDT should be specific that the first simulation is required to occur 15 months following the effective date. The SDT should be specific that the first annual review shall occur with in 15 months after the effective date.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
American Electric Power	No	With the scope of applicable functions expanding, more time will be required to develop broader processes and training. This will need to be extended for 18 months to get the process implemented and everyone trained.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
CenterPoint Energy	No	CenterPoint Energy prefers the previously accepted timeline of 1 year.

Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
Georgia System Operations Corporation	No	There is nothing about the revisions that were made to the requirements that shortens the time needed by the industry to get prepared for this revision. The removal of requirements for NERC does not shorten the requirements for the industry. Eighteen months (or 12 months minimum) should be alloted to prepare for this revision.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
Brazos Electric Power Cooperative	No	A one year implementation is needed to develop and implement formal documents to meet requirements.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	No	The implementation Plan was to move up the timeline and we do not see why this needs to be pushed forward on a shortened timeline. It should remain at the one year implementation schedule especially if annual exercises are not removed from the standard requirements as this take some time to prepare.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
ExxonMobil Research and Engineering		Recommend 4th calendar quarter instead of 3rd.
Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
Consumers Energy	No	
Dominion	Yes	Dominion agrees with the Implementation Plan; however, notes that the title for EOP-004-2 is inconsistent with the actual proposed standard.

Response: The DSR SDT thanks you for your comment. The DSR SDT believe the revisions made as part of this comment period have made the standard easier to implement. This latest revision more closely aligns with existing EOP-004 requirements, which entities are already complaint with.		
Farmington Electric Utility System	Yes	Nine months would be preferred
Response: The DSR SDT thanks you for your comment. The majority of stakeholders agree with the proposed implementation plan and it will remain unchanged.		
Northeast Power Coordinating Council	Yes	
Bonneville Power Administration	Yes	
Midwest Reliability Organization	Yes	
PPL Supply	Yes	
SPP Standards Review Group	Yes	
Midwest ISO Standards Collaborators	Yes	
SERC OC Standards Review Group	Yes	
PJM Interconnection LLC	Yes	
SRP	Yes	
We Energies	Yes	
Compliance & Responsiblity Organization	Yes	
City of Tallahassee (TAL)	Yes	

Lakeland Electric	Yes	
New Harquahala Generating Co.	Yes	
APX Power Markets	Yes	
American Municipal Power	Yes	
Liberty Electric Power LLC	Yes	
Arkansas Electric Cooperative Corporation	Yes	
Manitoba Hydro	Yes	
Sweeny Cogeneration LP	Yes	
USACE	Yes	
New Harquahala Generating Co.	Yes	
Independent Electricity System Operator	Yes	
ISO New England, Inc	Yes	
Platte River Power Authority	Yes	
BGE	Yes	No comments.
Alliant Energy	Yes	
PPL Electric Utilities	Yes	

Occidental Power Marketing	Yes	
Lincoln Electric System	Yes	
American Transmission Company	Yes	
Ingleside Cogeneration LP	Yes	
Duke Energy	Yes	
Indeck Energy Services	Yes	

17. If you have any other comments you have not already provided in response to the questions above, please provide them here.

Summary Consideration: The majority of comments received relate to Attachment 1 and the Flowchart in the background section. The DSR SDT has made conforming revisions to each based on the comments received. The Flowchart waqs updated to remove references to sabotage and replaced with "Criminal act invoking federal jurisdiction". In response to the comments received, the SDT has made numerous enhancements to Attachment 1. These revisions include:

- **Added new column "Submit Attachment 2 or DOE OE-417 Report to:" which references Part 1.3 and provide the time required to submit the report.**
- **Combined Parts A and B into one table and reorganized it so that the events are listed in order of reporting times (either one hour or 24 hours)**
- **Removed references to "Impact Event" and replaced with the specific language for the event type in the "Entity with Reporting Responsibility". For example, replaced "Impact Event" with "automatic load shedding".**

The ERO and the RE were added as applicable entities to reflect CIP-002 applicability to this standard.

Organization	Yes or No	Question 17 Comment
Georgia Transmission Corporation & Oglethorpe Power Corporation		In the discussion and related flowchart described as "A Reporting Process Solution - EOP-004," the discussion suggests that Industry should notify the state law enforcement agency and then allow the state agency to coordinate with local law enforcement. It has been our experience that we receive very good response from local law enforcement and they have existing processes to notify state or federal agencies as necessary. It appears the recommendation is to bypass the local law enforcement, but it is not clear that representatives from state or local law enforcement were included in this discussion (see proposal discussed with "FBI, FERC Staff, NERC Standards Project Coordinator and SDT Chair"). It would be helpful to see some additional clarification to understand why the state agency was chosen over local or federal agencies. Finally, we would like to express our gratitude to the DSR SDT for their hard work in making improvements to the NERC standards for event reporting.

Organization	Yes or No	Question 17 Comment
Response: The DSR DT thanks you for your comment. The Flowchart has been updated. The DSR SDT has reviewed all comments and believes it is the responsibility of the Reporting Entity to contact the appropriate law enforcement officials.		
Bonneville Power Administration		Work needed on Part A Damage or Destruction of BES equipment. The Note 1 is OK, but the Threshold doesn't match well. If a PCB is damaged by lightning or an earthquake, Note 1 (human action) doesn't require Reporting (proper interpretation), but the Threshold still requires "equipment damage."
Response: The DSR DT thanks you for your comment. Attachment 1 has been updated concerning Destruction of BES equipment and the associated footnote has been revised.		
Midwest Reliability Organization		On the Impact Reporting Form, number 7,8,9,10, and 11 have an astrict (*) but nothing describes what the astrict means. Recommend a foot note be added to state: * If applicable to the reported Impact Event.
Response: The DSR DT thanks you for your comment. Attachment 1, Part B has been updated to reflect these noted changes.		
Western Electricity Coordinating Council		Actual Reliability Impact Table comments: Note that per the NERC glossary "Energy Emergency" only is defined for an LSE. Energy Emergency is the precursor term in the first three lines. Thus logically an LSE is the only entity which would be initiating the event and responsible for reporting for first three items. We don't believe that is the intent.We suggest you consider just eliminating ?Energy Emergency? and going with:? Public appeal for load reduction? system-wide voltage reduction? manual firm load sheddingFor Loss of Off site power at Nuc Station is reporting really expected of each of the entities listed? (lots of reports) We suggest you consider just the Nuclear GOP and perhaps the associated TOP. Perhaps you could use the CIP approach as in the next two rows and say Applicable GOP and Transmission Entities under NUC-001-2Potential Reliability Impact Table Comments:For Fuel Supply Emergency, Forced Intrusion, Risk to BES Equipment, Cyber Security Incident where owner/operator are both listed (GO/GOP or TO/TOP) could consider perhaps reporting to be assigned to only one rather than both.
Response: The DSR DT thanks you for your comment. The DSR SDT has removed the use of "Energy Emergency" and has updated Loss of offsite power to a nuclear generating plant within Attachment 1. Fuel Supply emergency has been removed from Attachment 1 per comments received. The entire Attachment 1 has been updated per comments received.		
Pacific Northwest Small Public Power Utility Comment Group		All five requirements refer to Attachment 1 Part A either directly, or indirectly by referring to R1 plans. Attachment 1 Part A, though, only provides the thresholds required for reporting (R5). No thresholds are provided for planning (R1) or the requirements referencing the plan (R2-R4). Strictly interpreted, an entity would be required to plan for any amount of firm load loss exceeding 15 minutes (for example), implement the

Organization	Yes or No	Question 17 Comment
		plan for any amount and then report only those events that exceeded the applicable 200 or 300 MW level. An entity that had a peak load of less than 200 MW would still need to meet R1-R4 regarding load loss. We believe the SDT intended to use common thresholds for all the requirements. Suggest relabeling the Attachment 1 Part A column header from ?Threshold for Reporting? to ?Threshold.?We also fail to see how an entity?s size in MWh affects the threshold for reporting firm load loss.
Response: The DSR DT thanks you for your comment. The DSR SDT has revised each Requirement and Attachment 1. There are other events within Attachment 1 that a responsible entity will be required to report.		
Dominion		The following comments are provided on the Reporting Hierarchy for Impact Events EOP-004-2: 1) A reference to sabotage still exists in a ?decision block?; 2) The ?entry block? only specifies ?actual Impact Events? and does not address ?potential?; 3) Hierarchy is misspelled in the title.Attachment 2: Impact Event Reporting Form; in questions 7, 8, 9, 10, 11 what is the purpose of the *(asterisk) behind each Task that is named?
Response: The DSR DT thanks you for your comment. The Flowchart has been updated based on comments received. Attachment 2 has been updated to reflect comments received.		
Pepco Holdings Inc and Affiliates		IRO-000-1, Sec D1.5 and TOP-007, Sec D1.1 there are ?after the fact? reporting requirements for IROL violations. Since IROL violations are included in this standard, should those standards be modified?Should the standard include a specific statement that this standard deals only with after the fact and other standards deal with real time reporting?Since this standard deals with after the fact reporting, consideration should be given to extending the time to report as defined in Attachment 1. One hour does not seem to be reasonable.
Response: The DSR DT thanks you for your comment. The DSR SDT has reviewed TOP-007 and note that the 72 hour issue is not defined within a Requirement. This issue has been forwarded to the "NERC Issues Data base." Attachment 1 has been updated to reflect this event to 24 hours per comments received.		
SPP Standards Review Group		In Attachment 2 just before the table, the statement is made that ?NERC will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report.? But the last sentence in the Guideline and Technical Basis white paper, it is stated that ? For example, if the NERC Report duplicates information from the DOE form, the DOE report may be included or attached to the NERC report, in lieu of entering that information on the NERC report.? These are in conflict with each other. Which is correct? We prefer the former over the latter.In Attachment 2 in Tasks 7-11 an asterisk appears in those tasks. To what does this asterisk refer?

Organization	Yes or No	Question 17 Comment
Response: The DSR DT thanks you for your comment. The DSR SDT's White Paper was the initial road map for the SDT to follow. The DSR SDT has proposed allowing entities to use the DOE Form OE-417 to report events listed within Attachment 1.		
Midwest ISO Standards Collaborators		We believe the reporting time lines are too aggressive for some events. Reporting events within an hour is not reasonable as an entity may still be dealing with the event. This will be particularly difficult when support personnel are not present such as during nights, holidays, and weekends.
Response: The DSR DT thanks you for your comment. Attachment 1 has been updated per comments received.		
FirstEnergy		FE offers the following additional comments and suggestions: 1. In the Background section of EOP-004-2, on page 6 under Stakeholders in the Reporting Process, we suggest adding ?Regional Entity? and ?Nuclear Regulatory Commission?. 2. The DSR SDT makes reference to comments that Exelon provided that suggested adopting the NRC definition of "sabotage." We feel the comment made by Exelon in their previous submittal was to ensure that the DSR SDT included the Nuclear Regulatory Commission (NRC) as a key Stakeholder in the Reporting Process and FE agrees with this suggestion. Nuclear generator operators already have specific regulatory requirements to notify the NRC for certain notifications to other governmental agencies in accordance with 10 CFR 50.72(b)(s)(xi). We ask that the DSR SDT contact the NRC about this project to ensure that existing communication and reporting that a licensee is required to perform in response to a radiological sabotage event (as defined by the NRC) or any incident that has impacted or has the potential to impact the BES does not create either duplicate reporting, conflicting reporting thresholds or confusion on the part of the nuclear generator operator. We believe this is a similar situation as what was recently resolved between NERC and the NRC concerning the applicability of CIPs 002 ? 009 for nuclear plants. Each nuclear generating site licensee must have an NRC approved Security Plan that outlines applicable notifications to the FBI. Depending on the severity of the security event, the nuclear licensee may initiate the Emergency Plan (E-Plan). We ask that the proposed "Reporting Hierarchy for Impact Event EOP-004-2," flow chart be coordinated with the NRC to ensure it does not conflict with existing expected NRC requirements and protocol associated with site specific Emergency and Security Plans.
Response: The DSR DT thanks you for your comment. 1. We have added these as requested. 2. The NRC was added to the list on page 6 as requested. The events in Attachment 1 that are applicable to nuclear plants are: Generation loss (>1,000 MW WECC, >2,000 MW Elsewhere); Destruction of BES Equipment; Damage or destruction of Critical Asset per CIP-002; Damage or destruction of a Critical Cyber Asset per CIP-002; Forced Intrusion; Risk to BES Equipment; and Detection of a Reportable Cyber Security incident. Two of these events are addressed in the situation that you mention above (CIP-002). The other events should be reported to both the NRC and ERO if they occur. These are considered to be sabotage type events.		

Organization	Yes or No	Question 17 Comment
SERC OC Standards Review Group		In Attachment 1, the reporting timeline should be no less than the end of the next business day for after-the-fact reporting of events. If reporting in a time frame less than this is required for reliability, the groups or organizations receiving the reports should be included in the functional model. The emphasis should be on giving the operators the time to respond to events and not to reporting requirements.?The comments expressed herein represent a consensus of the views of the above named members of the SERC OC Standards Review group only and should not be construed as the position of SERC Reliability Corporation, its board or its officers.?
Response: The DSR DT thanks you for your comment. Attachment 1 has been updated to reflect comments received. Many of the reporting time frames have been revised to 24 hours.		
PJM Interconnection LLC		In the Compliance Enforcement Authority Section on Page 11, the second bullet says ?If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement?. We are not sure what this exactly implies or means. Additional clarification is required.
Response: The DSR DT thanks you for your comment. The statement that PJM is referring to applies to Regional Entities that also have a functional model obligation.		
Southern Company		Need guidance for incorporating disturbance reporting that is in CIP-008.
Response: The DSR DT thanks you for your comment. EOP-004-2 is the reporting vehicle for CIP-008. CIP-008-4, Requirement 1, Part 1,3 will be retired upon approval of EOP-004-2.		
We Energies		Attachment 2: What do the asterisks refer to? I didn?t see a comment or description related to them.#7 & #10: What is ?tripped?? Automatic or manual or both.#13: This report has no Part 1.Flowchart: By the flowchart, the only time an OE-417 is filed is when I do not need to contact Law Enforcement. The Reporting Hierarchy flow chart should be modified. In the lower right corner it indicates that if sabotage is not confirmed, the state law enforcement agency investigates. Law enforcement agencies will not investigate an incident that is not a crime. Note too that state law enforcement agencies do not even investigate these kinds of events unless and until requested by local law enforcement. The local law enforcement agency always has initial jurisdiction until surrendered or seized by a superior agency?s authority. Evidence Retention is incomplete. From the NERC Standards Process Manual: ?Evidence Retention: Identification, for each requirement in the standard, of the entity that is responsible for retaining evidence to demonstrate compliance, and the duration for retention of that evidence.?

Organization	Yes or No	Question 17 Comment
Response: The DSR DT thanks you for your comment. Attachment 1 and Attachment 2 have been updated per comments received. The Flowchart has been updated per your comment.		
Compliance & Responsiblity Organization		Nuclear power plants (a need for a revised approach)With respect to sabotage, damage or destruction of BES equipment, damage or destruction of a Critical Asset, damage or destruction of a Critical Cyber Asset, forced intrusion, etc., nuclear plants already have a responsibility to report the events to the FBI and the Nuclear Regulatory Commission (NRC). Performing another report to NERC, with potentially different requirements, within 60 minutes of an event does not seem necessary or practical. It would also be difficult, during an event, to report to external organizations, including but not limited to the Responsible Entities? Reliability Coordinator, NERC, Responsible Entities? Regional Entity, Law Enforcement, and Governmental or Provincial Agencies when operations personnel are pre-occupied with an abnormal or emergency situation. Further, nuclear plants already have an obligation to report the loss of off site power to NRC. Similarly, now that cyber assets will be regulated by the NRC, these reporting requirements should not be applicable to a nuclear power plant. Thus, there is a need to exempt nuclear power plants from these requirements or provide more flexibility to such plants, given its pre-existing NRC reporting requirements.Attachment 1.There is no explanation for why a report must be submitted within one hour of a event. As stated with respect to nuclear, an entity should not be prioritizing between stabilizing the system and reporting. One approach that would help balance conflicting priorities is to start the time frame after ?all is clear.? Another approach could involve the use of target times, with an allowance for exceptions during emergencies or situations in which it is impracticable. Another alternative is to have two times: an earlier ?target reporting time? and second later ?mandatory reporting time.? Further, the current wording suggests that a generator owner or generator operator will be able to determine the impact or potential impact on the BES. This is not realistic, given that impacts to the BES are generally only understood at a transmission operator or reliability coordinator level. Thus, the concept of relying on generators to determine impacts on the BES needs to be eliminated.Also, as written, for a generator, Attachment 1 appears to require a report when a lighting arrestor fails at a Critical Asset. NextEra cannot see any justification for reporting such an event, and this is another reason why Attachment 1 needs more review and revision prior to the next draft of EOP-004-2. This one reason why NextEra has suggested a materiality test for reporting in a definition of Attempted or Actual Sabotage.
Response: The DSR DT thanks you for your comment. Attachment 1 has been updated per comments received. Any NRC requirements or comments fall outside the scope of this project.		
Exelon		The DSR SDT makes reference to comments that were previously provided that suggested adopting the NRC definition of "sabotage." Respectfully, this commenter believes the DSR SDT did not understand the intent of the original comment. The comment made by Exelon in the October 15, 2009 submittal was to ensure that the DSR SDT made an effort to include the Nuclear Regulatory Commission (NRC) as a key Stakeholder in

Organization	Yes or No	Question 17 Comment
		the Reporting Process and to consider utilizing existing reporting requirements currently required by the NRC for each nuclear generator operator.Depending on the event, a nuclear generator operator (NRC licensee) also has specific regulatory requirements to notify the NRC for certain notifications to other governmental agencies in accordance with 10 CFR 50.72, "Immediate notification requirements for operating nuclear power reactors," paragraph (b)(2)(xi).The one hour notification requirement for an intrusion event would also meet an emergency event classification at a nuclear power plant. If an operations crew is responsible for the one hour notification and if separate notifications must be completed within the Emergency Plan event response, then an evaluation in accordance with 10 CFR 50.54, "Conditions of licensees," paragraph (q), would need to be performed to ensure that this notification requirement would not impact the ability to implement the Emergency Plan.At a minimum the DSR SDT should communicate this project to the NRC to ensure that existing communication and reporting that a licensee is required to perform in response to a radiological sabotage event (as defined by the NRC) or any incident that has impacted or has the potential to impact the BES does not create either duplicate reporting, conflicting reporting thresholds or confusion on the part of the nuclear generator operator. Note that existing reporting/communication requirements are already established with the FBI, DHS, NORAD, FAA, State Police, LLEA and the NRC depending on the event. There are existing nuclear plant specific memorandums of understanding between the NRC and the FBI and each nuclear generating site licensee must have a NRC approved Security Plan that outlines applicable notifications to the FBI. Depending on the severity of the security event, the nuclear licensee may initiate the Emergency Plan. The proposed "Reporting Hierarchy for Impact Event EOP-004-2," needs to be communicated and coordinated with the NRC to ensure that the flow chart does not conflict with existing expected NRC requirements and protocol associated with site specific Emergency and Security Plans. Propose allowing for verbal reporting via telephone, for 1 hr. reporting with a follow up using the forms.With the revised standard EOP-004-2 it eliminates the #8; loss of electric service >= 50K, however, that requirement is still required for the DOE-OE-417 form. The question is do we still have to send it to NERC / Region if NERC/ Region does not specifically still have that as a requirement? Also, with that requirement, on the current EOP-004-1 it says that schedule 1 has to be filled out within 1 hour? This doe not coincide with DOE-OE-417 form. The bottom line, it looks like there is inconsistency as to what is reportable per EOP-004-2 and DOE-OE-417 form, some of the items are redundant, some are not, but better guidance is needs as to which form to use when. The SDT should have a Webaniar with the industry to create an understanding as to who is responsible to report what and at what time.
Response: The DSR DT thanks you for your comment. The NRC issues falls outside the scope of this project		
City of Tallahassee (TAL)		Attachment 2 (Impact Event Reporting Form) items 8, 9, 10, and 11 have an asterisk but no identification as to what the asterisks refer to.
Response: The DSR DT thanks you for your comment. The asterisk was addressed at the bottom of the second page of the form. Attachment 2 has been		

Organization	Yes or No	Question 17 Comment
updated to align with the types of events that are to be reported.		
APX Power Markets		The reporting of Impact Events needs to be clear spelled out and if moving some of that to State Agencies it needs to be consistent in all States at the same time and which State it should be reported to. We have a 24-hour Desk in one state that handles facilites in many other States. If there is an Impact Event that needs to be reported, where is that report sent to. The State the facility resides in or the State where our 24-hour Desk resides in.
Response: The DSR DT thanks you for your comment. Attachment 1 has been updated per comments received and a new column has been added to reflect who the impacted entity is required to report to.		
Arkansas Electric Cooperative Corporation		We appreciate the added context through the use of extended background information, rationale statements, and corresponding guideline and hope this context will remain in line with the Standards through the ballot and approval process. We have a few suggestions and questions related to this context. Our comments for this question relate to the contextual information. First of all, in the diagram on page 8, we suggest the appropriate question to ask is "Is event associated with potential criminal activity?" rather than "Report to Law Enforcement?? Also, it would be helpful to make clear the communication flow associated with the State Agency is the responsibility of the State Agency and not the Responsible Entity. This could be shown with a different colored background that calls this process out separately. In the rationale box for R3, it states "The DSR SDT intends?? We propose this should read similar to "The objective of this requirement is?? Overall, we suggest the SDT review the guidance document to make sure any changes made to the requirements are consistent with the guidance.
Response: The DSR DT thanks you for your comment. The flowchart has been updated per comments received. The Rationale box will be removed upon this Standard being Filled for approval.		
American Electric Power		We still do not agree that LSE, TSP and IA should be included in the applicability of this standard. Having processes to report to local or federal law enforcement agencies is ?legislating the obvious?. The focus on this standard should only be on Impact Event reporting to reliability entities.
Response: The DSR DT thanks you for your comment. Attachment 1 has been reviewed and updated. The LSE, TSP, and IA are required under the CIP Standards and Attachment 1 is based on reporting per the CIP requirements.		
Consumers Energy		1. We appreciate the aggregation of redundant standards on this subject, but have some concerns about the content of the aggregated standard as listed below and in reference to previous questions on this comment form.2. It is not clear whether an event that meets OE-417 reporting criteria but is not defined within EOP-

Organization	Yes or No	Question 17 Comment
		004-2 is an Impact Event; for example, ?loss of 50,000 or more customers for 1 hour or more? is required to be reported to DOE as a OE-417 type 11 event but it is not clear whether EOP-004-2 requires that such events be also reported to NERC. The ?Reporting Hierarchy? flow chart seems to suggest that any OE-417 must still be filed with NERC/RE. If the flow chart is not consistent with the intent of the Requirements, it must be clarified.3. NERC implies active involvement of law enforcement. This assumes that law enforcement has the resources to be involved in an Impact Event investigation and fulfill the standard reporting requirements. This is an unrealistic expectation as we have experienced first-hand, a lack of response by law enforcement agencies as their resources shrink due to economic issues. Additionally, NERC is asking that we place credence in law enforcement, on our behalf, to make a definitive decision about the reporting of events. Refer to page 6 of EOP-004-2 under ?Law Enforcement Reporting?: ??Entities rely upon law enforcement agencies to respond and investigate those Impact Events which have the potential of wider area affect?? In many cases, the internal security function must work with system operations personnel to thoroughly understand the system and the effects of certain events. It is unrealistic to think law enforcement would be in a position to make BES decisions within the timeframe given without having system operations experience. It is our experience that external agencies do not understand the integration / inter-connectivity, resiliency, or implications of our energy infrastructure.4. Within Michigan, a ?Michigan Fusion Center: Michigan Intelligence Operations Center (MIOC)? has been established. - Today, we share information such as substation issues and identity theft (not internal issues) to the MIOC. The MIOC is trending incidents on critical infrastructure assets and sectors around the state. The private sector is encouraged to report to the Fusion Center. If NERC is collecting this type of information for future studies and trending / analysis, they should coordinate with each state?s Fusion Center.
Response: The DSR DT thanks you for your comment**.** The DSR SDT has reviewed and updated the Requirements per the comments received. Attachment 1 has been updated and the team has an additional column to reflect where a report should be sent. EOP-004-2 does not define what “law enforcement”” is and that will be left up to each entity.		
Ameren		The following is a list of our greatest concerns. (1) We are concerned about the lack of definitions and use of critical non-capitalized terms. As an example, there is a reportable Impact Event if there is a +/- 10% Voltage Deviation for 15 minutes or more on BES Facilities. As a first example, why is the term Voltage Deviation capitalized when it is not in the NERC Glossary and not proposed to be added? Where is the deviation measured - at any BES metering device? What is the deviation to be reported - the nominal voltage? the high-side of the Voltage Schedule? the low-side of the Voltage Schedule? the generator terminals? when a unit is starting up? All of these are possible interpretations, but < 1% of them would ever result in a Cascading outage - which is the reliability objective of this Standard. A second example is a Generation loss. The threshold for reporting is 2,000 MW, or more, for the Eastern or Western Interconnection. Is this simultaneous loss of capacity over the entire Interconnection? Or, cumulative loss within 1 hour? Or, cumulative loss within 24 hours? How many individual GOPs have responsibility for > 2,000 MW? It seems

Organization	Yes or No	Question 17 Comment
		this would more effectively apply only to an RC and/or BA. The likelihood that one GOP would lose that much generation at once is probably remote. A third example would be the damage or destruction of BES equipment event. The term "equipment" was left lower case with a footnote explanation that includes "?due to intentional or unintentional human action?." This is likely to require the determination of intent by the human involved, which will almost certainly impossible to determine within the 1 hour reporting time. Also, what is the definition of the terms "damage" and "destruction"? Once again, if the reliability intent is to ONLY report Events that have a likely chance of leading to Cascading, this will greatly reduce the potentially enormous reporting burden. that could result without this type of clarification. (2) Without a very thorough understanding of the definitions of the terms requiring reporting, the 1 hour reporting constraint on most events will likely require that we frequently overreport events to minimize any chance of non-compliance. A webinar explaining expected reporting requirements would very useful and valuable. It is also unclear why so many Impact Events require such a short reporting time period. There will almost certainly be many times at 2:00 AM on a weekend when experts and the appropriate personnel will be available to quickly analyze an event and decide, within 1 hour, if a report is necessary. (3) Have all the new Impact Event reporting requirements been checked against reporting requirements from other Standards? For example, the Voltage Deviation Event would appear to potentially overlap/conflict with instructions from a TOP for VAR-002 compliance. Since VAR-002-2 is now in draft, has the SDT worked with that Team to determine if the requirements dovetail?
Response: The DSR DT thanks you for your comment**.** The DSR SDT has updated the Requirements within EOP-004-2 and both Attachments 1 and 2 per comments received. Many of the reporting time frames have been extended to 24 hours per comments received. Voltage deviation is no longer capitalized. All event types are not intended to be new defined terms for the NERC Glossary and have been revised to lower case words. The reporting of voltage deviations is no longer applicable to the GOP which obviates the need to coordinate with the VAR-002 standard drafting team.		
ISO New England, Inc		Under the ?Law Enforcement Reporting? it is stated ?The Standard is intended to reduce the risk of Cascading involving Impact Events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.? We question whether a reporting standard can ?reduce the risk of cascading? and wonder if the reference to the threat ?around them? refers to law enforcement? We would expect that the appropriate operating personnel are the only entities that would be able to mitigate the potential risk to the BES.As it currently stands there is a potential duplication between the reporting requirements under EOP-004-2 (i.e. Attachment 2 Form) and the ERO Event Analysis Process that is undergoing field test (i.e. Event Report Form). This will result in entities (potentially multiple) reporting same event under two separate processes using two very similar forms. Is this the intent or will information requirements be coordinated further prior to adoption in order to meet the declared objective that the impact event reporting under EOP-004 be ?the starting vehicle for any required Event Analysis within the NERC Event Analysis Program?

Organization	Yes or No	Question 17 Comment
Response: The DSR DT thanks you for your comment. The Background section was provided to assist entities in understanding the DSR SDT's process for updating CIP-001 and EOP-004, only.		
Calpine Corp		Focusing on reporting of actual disturbance events as listed in Attachment 1 based on potential or actual impact to the Bulk Electric System will provide maximum benefit to system reliability without adding needless levels of new documentation generated to demonstrate compliance. Absent significant evidence of systemic problems in the industry with past reporting attributable to causes other than a lack of clear guidance on the types events that require reporting, the proposed Standard should focus on the single issue of correct reporting, without attempting to micromanage how Entities internally manage such reporting.
Response: The DSR DT thanks you for your comment. The DSR SDT has updated the requirements andAttachments 1 and 2 per comments received.		
BGE		Please provide a Mapping Document which shows where the four CIP-001 requirements map to in the new EOP-004-2, and note if any of the CIP-001 requirements have been eliminated. A Mapping Document was provided during the first Comment Period, but not during the second Comment Period. A Mapping Document will be very helpful to companies in aligning standard owners in reviewing this proposal and in transitioning compliance programs when the revised standard is approved.
Response: The DSR DT thanks you for your comment. The DSR SDT has a current Mapping Document and it will be updated to reflect the changes that the DSR SDT has made to EOP-004-2. This Mapping document will be posted with the standard when it is posted for comment and ballot.		
CenterPoint Energy		CenterPoint Energy believes the flowchart found on page 8 identifying the reporting hierarchy for EOP-004 is helpful. CenterPoint Energy believes the DOE reporting items should also be included on the right side of the chart. Some of the issues with CIP-001 were a result of law enforcement?s preference and procedures for notification. Law enforcement?s preferences and procedures should be considered for this draft. (Reference: http://www.fbi.gov/contact-us/when)
• **Response:** The DSR DT thanks you for your comment. The DSR SDT has updated the flowchart and a current Mapping Document and it will be updated to reflect the changes that the DSR SDT has made to EOP-004-2. The background section of the standard provides guidance with respect to reporting events to law enforcement. For clarity, the DSR SDT has added the following sentence to the first paragraph under the heading "Law Enforcement Reporting": "These are the types of events that should be reported to law enforcement." The entire paragraph is: "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact		

Organization	Yes or No	Question 17 Comment
a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES."		
PPL Electric Utilities		We thank the SDT for addressing so many Industry concerns with the 2010 draft of EOP-004-2. We feel the current draft version of EOP-004-2 is a significant improvement over current EOP-004-1 and CIP-001-1 standard and the previous draft. Thank you for your time.
Response: Thank you for your comment.		
Occidental Power Marketing		Occidental Power Marketing appreciates the extensive work accomplished by the SDT and their responsiveness to comments. Also, the presentation of this draft with its extensive explanation of the SDT's considerations during development of the draft were very helpful in preparing our comments.
Response: Thank you for your comment.		
Constellation Power Generation		CPG has the following comments regarding Attachment 2:?Generally, this attachment is inadequate for all events. The real-life experience with the recent SW cold snap demonstrated that the questions inadequately capture what may be of greatest concern in the situation. ?Question 4 ? this question is vague. It should be removed. ?Question 7 ? the role of generation in an event may not always be related to a trip. As experienced with the recent SW cold snap, this question may inadequately capture information relevant to the situation at hand. The drafting team should reassess how best to gather information relevant to the event and useful for evaluation.?Question 8 ? generation is not required to monitor frequency during events, so this would not be answered. This question also assumes that frequency had been impacted, which is not always the case (i.e., the plant could not come online). ?The asterisk on some questions in Attachment 2 is not defined.
Response: The DSR DT thanks you for your comment. The DSR SDT has updated the requirements and Attachments 1 and 2 per comments received. Attachment 2 has been streamlined to match the types of events that are to be reported. The purpose of this standard is to have events reported. Once reported, the events are included in the NERC Events Analysis Program for possible further investigation. The asterisk has been removed from Attachment 2.		
Georgia System Operations Corporation		Attachment 2: Impact Event Reporting Form-Instructions for filling out this form are needed.-Line 7, Generation tripped off-line: What is the asterisk for after this task and after the many others following? This should only be reported by a BA. Does generation ?tripped off-line? mean the same as generation ?lost??-Line 9, List of transmission facilities (lines, transformers, buses, etc.) tripped and locked-out: Does this means the same as BES Transmission Elements lost?-Line 10: The column headings in white text on lighter blue

Organization	Yes or No	Question 17 Comment
		background at the top do not seem to apply from this line on.-Line 11, Restoration Time: Restoration of what? Initial/Final clock time? Transmission? What about transmission? Generation/Demand?-Line 13, Identify the initial probable cause or known root cause of the actual or potential Impact Event if known at time of submittal of Part I of this report: ?At the time of submittal of Part I of this report??? Where is Part II? Did you mean Part A? Is Part B to be submitted at a different time?Background-Page 5, last sentence which is continued on page 6: This standard does not recognize the various ?versions? of companies in the industry. The standard is made applicable to a long list of registered entity types. In many cases, many of these entities are wrapped into one company. A company may be responsible for ?everything? in a geographic area. It may be almost every registered entity type with no other registered entities within its geographic area. There should be no conflicts or need for coordination with others for this company. Everything would be coordinated internally within that one company before being reported to NERC and no one else would be reporting to NERC.However, sometimes one company is only a LSE. When an LSE-only is having a LSE impact event, the LSE should report to some higher operating entity like its BA and should not report to NERC. Reporting should be done in a hierarchical manner within appropriate operating entities and then reported to NERC at the RC (or BA) level or as agreed among entities in any coordinated impact event reporting plans. The RC, BA, TOP, and LSE should not all be held accountable for reporting the same event.This standard does not deal exclusively with after-the-fact reporting. Some events deal with the condition of the system (risk of possible future events) or condition of an entity?s ability to operate (supplying fuel, covering load, etc.) or with a threat to the BES.-Page 6, Summary of Concepts: A single form may have been an objective but it is obviously not a concept being implemented by the standard. There are two forms.-Page 6, Law Enforcement Reporting: The object of the standard may be to prevent or reduce the risk of Cascading. Reporting system situations to appropriate operating entities who can take some mitigating action (e.g., a LSE reporting to its BA or a BA reporting to its RC) and reporting threats to law enforcement officials could prevent or reduce the risk of Cascading but reporting to NERC is unlikely to a do that. Reporting of most of the listed events to NERC does not meet the objective of this standard and should be removed from this standard. Such events should be reported to NERC through some other (than a Reliability Standard) requirement for reporting to NERC so that NERC can accomplish its mission of analyzing events. Analyzing events may lead to an understanding that could reduce the future risk of Cascading but not any impending risks.-Page 6, Stakeholders: What is ?Homeland Security ? State?? We know what the Department of Homeland Security and the State Department are but this term is not clear. -Page 6, ?State Regulators?, ?Local Law Enforcement?, and State Law Enforcement?: These are not proper nouns/names and are not defined in the NERC Glossary. They should not be capitalized.-Pages 7 & 8, Law enforcement: Is each entity required to determine procedures for reporting to law enforcement and work it out with the state law enforcement agency? Do the state law enforcement agencies know this? Or is there a pre-determine procedure that is already worked out with the state law enforcement agency that entities are to follow?
• **Response:** The DSR DT thanks you for your comment. The DSR SDT has updated the requirements and Attachments 1 and 2 per comments received.		

Organization	Yes or No	Question 17 Comment
Attachment 2 has been streamlined to match the types of events that are to be reported. The purpose of this standard is to have events reported. Once reported, the events are included in the NERC Events Analysis Program for possible further investigation. The background section of the standard provides guidance with respect to reporting events to law enforcement. For clarity, the DSR SDT has added the following sentence to the first paragraph under the heading "Law Enforcement Reporting": "These are the types of events that should be reported to law enforcement." The entire paragraph is: "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES."		
City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power		We like the option to use the OE_417 as the reporting form for these events.
Response: The DSR DT thanks you for your comment. EOP-004-2 allows entities to utilize the DOE Form OE-417 to report events.		
Indeck Energy Services		This revision seriously missed the mark.
Response: The DSR DT thanks you for your comment. The DSR SDT has updated the requirements and Attachments 1 and 2 per comments received.		
Progress Energy		Progress thanks the Standard Drafting Team for their efforts on this project.The BES definition is still being revised under ?Project 2010-17: Proposed Definition of Bulk Electric System.? ?BES equipment? is mentioned several times in this Standard. A better definition of BES is important to the effectiveness of this Standard and integral to entities ability to comply with the Standard requirements. In Attachment 2, on the Impact Event Reporting form, item 10 is ?Demand Tripped? and the categories include ?FIRM? and ?INTERRUPTIBLE.? It is unclear why interruptible load is included on the reporting form.
Response: The DSR DT thanks you for your comment. The definition of BES will apply to this standard after it is approved by stakeholders, the NERC BOT and FERC. The DSR SDT has updated the requirements, Attachments 1 and 2 per comments received. Attachment 2 has been streamlined to match the types of events that are to be reported. The purpose of this standard is to have events reported. Once reported, the events are included in the NERC Events Analysis Program for possible further investigation. Firm and Interruptible load have been removed from the list of reportable events in Attachment 1.		

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SC approved SAR for initial posting (April, 2009).
2. SAR posted for comment (April 22 – May 21, 2009).
3. SC authorized moving the SAR forward to standard development (September 2009).
4. Concepts Paper posted for comment (March 17 – April 16, 2010).
5. Initial Informal Comment Period (September 15 – October 15, 2010)
6. Second Comment Period (Formal) (March 9 – April 8, 2011)

Proposed Action Plan and Description of Current Draft
This is the third posting of the proposed standard in accordance with Results-Based Criteria. The drafting team requests posting for a 45-day formal comment period concurrent with the formation of the ballot pool and the initial ballot.

Future Development Plan

Anticipated Actions	Anticipated Date
Drafting team considers comments, makes conforming changes on second posting	April - October 2011
Third Comment/Ballot period	November-December 2011
Recirculation Ballot period	December 2011
Receive BOT approval	February 2012

Effective Dates

EOP-004-2 shall become effective on the first day of the third calendar quarter after applicable regulatory approval. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the third calendar quarter after Board of Trustees approval.

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-2a Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2 Impact Event Reporting; Retire CIP-001-2a Sabotage Reporting and Retired EOP-004-1 Disturbance Reporting. Retire CIP-008-4, Requirement 1, Part 1.3.	Revision to entire standard (Project 2009-01)

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

When this standard has received ballot approval, the text boxes will be moved to the Guideline and Technical Basis Section.

A. Introduction

1. Title: Event Reporting

2. Number: EOP-004-2

3. Purpose: To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of events with the potential to impact reliability and their causes, if known, by the Responsible Entities.

4. Applicability

4.1. Functional Entities: Within the context of EOP-004-2, the term "Responsible Entity" shall mean:

4.1.1. Reliability Coordinator

4.1.2. Balancing Authority

4.1.3. Interchange Coordinator

4.1.4. Transmission Service Provider

4.1.5. Transmission Owner

4.1.6. Transmission Operator

4.1.7. Generator Owner

4.1.8. Generator Operator

4.1.9. Distribution Provider

4.1.10. Load Serving Entity

4.1.11. Electric Reliability Organization

4.1.12. Regional Entity

5. Background:

NERC established a SAR Team in 2009 to investigate and propose revisions to the CIP-001 and EOP-004 Reliability Standards. The team was asked to consider the following:

1. CIP-001 could be merged with EOP-004 to eliminate redundancies.
2. Acts of sabotage have to be reported to the DOE as part of EOP-004.
3. Specific references to the DOE form need to be eliminated.
4. EOP-004 had some 'fill-in-the-blank' components to eliminate.

The development included other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC SC in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009.

The DSR SDT developed a concept paper to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT had developed. The posting of the concept paper sought comments from stakeholders on the "road map" that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the DSR SDT. The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC issues database and FERC Order 693 Directives in order to determine a prudent course of action with respect to revision of these standards.

Summary of Key Concepts

The DSRSDT identified the following principles to assist them in developing the standard:

- Develop a single form to report disturbances and events that threaten the reliability of the bulk electric system
- Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements
- Establish clear criteria for reporting
- Establish consistent reporting timelines
- Provide clarity around who will receive the information and how it will be used

During the development of concepts, the DSR SDT considered the FERC directive to "further define sabotage". There was concern among stakeholders that a definition may be ambiguous and subject to interpretation. Consequently, the DSR SDT decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was sabotage or vandalism without the intervention of law enforcement. The DSR SDT felt that attempting to define sabotage would result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard. The events listed in Attachment 1 were developed to provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

The types of events that are required to be reported are contained within Attachment 1. The DSR SDT has coordinated with the NERC Events Analysis Working Group to develop the list of events that are to be reported under this standard. Attachment 1, Part A pertains to those actions or events that have impacted the Bulk Electric System. These events were previously reported under EOP-004-1, CIP-001-1 or the Department of Energy form OE-417. Attachment 1, Part B covers similar items that may have had an impact on the Bulk Electric System or has the potential to have an impact and should be reported.

The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting.

Data Gathering

The requirements of EOP-004-1 require that entities "promptly analyze Bulk Electric System disturbances on its system or facilities" (Requirement R2). The requirements of EOP-004-2 specify that certain types of events are to be reported but do not include provisions to analyze events. Events reported under EOP-004-2 may trigger further scrutiny by the ERO Events Analysis Program. If warranted, the Events Analysis Program personnel may request that more data for certain events be provided by the reporting entity or other entities that may have experienced the event. Entities are encouraged to become familiar with the Events Analysis Program and the NERC Rules of Procedure to learn more about with the expectations of the program.

Law Enforcement Reporting

The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.

Stakeholders in the Reporting Process

- Industry
- NERC (ERO), Regional Entity
- FERC
- DOE
- NRC
- DHS – Federal
- Homeland Security- State
- State Regulators
- Local Law Enforcement
- State or Provincial Law Enforcement
- FBI
- Royal Canadian Mounted Police (RCMP)

The above stakeholders have an interest in the timely notification, communication and response to an incident at an industry facility. The stakeholders have various levels of accountability and have a vested interest in the protection and response to ensure the reliability of the BES.

Present expectations of the industry under CIP-001-1a:

It has been the understanding by industry participants that an occurrence of sabotage has to be reported to the FBI. The FBI has the jurisdictional requirements to investigate acts of sabotage and terrorism. The CIP-001-1-1a standard requires a liaison relationship on behalf of the industry and the FBI or RCMP. Annual requirements, under the standard, of the industry have not been clear and have lead to misunderstandings and confusion in the industry as to how to demonstrate that the liaison is in place and effective. As an example of proof of compliance with Requirement R4, responsible entities have asked FBI Office personnel to provide, on FBI letterhead, confirmation of the existence of a working relationship to report acts of sabotage, , the number of years the liaison relationship has been in existence, and the validity of the telephone numbers for the FBI.

Coordination of Local and State Law Enforcement Agencies with the FBI

The Joint Terrorism Task Force (JTTF) came into being with the first task force being established in 1980. JTTFs are small cells of highly trained, locally based, committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. The JTTF is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. Coordination and communications largely through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs. This information flow can be most beneficial to the industry in analytical intelligence, incident response and investigation. Historically, the most immediate response to an industry incident has been local and state law enforcement agencies to suspected vandalism and criminal damages at industry facilities. Relying upon the JTTF coordination between local, state and FBI law enforcement would be beneficial to effective communications and the appropriate level of investigative response.

Coordination of Local and Provincial Law Enforcement Agencies with the RCMP

A similar law enforcement coordination hierarchy exists in Canada. Local and Provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. The Provincial law enforcement agency has a reporting relationship with the Royal Canadian Mounted Police (RCMP).

A Reporting Process Solution – EOP-004

A proposal discussed with the FBI, FERC Staff, NERC Standards Project Coordinator and the SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Reportable Events). Essentially, reporting an event to law enforcement agencies will only require the industry to

notify the state or provincial or local level law enforcement agency. The state or provincial or local level law enforcement agency will coordinate with law enforcement with jurisdiction to investigate. If the state or provincial or local level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial or local level law enforcement agency will notify and coordinate with the FBI or the RCMP.

Reporting Hierarchy for Reportable Events

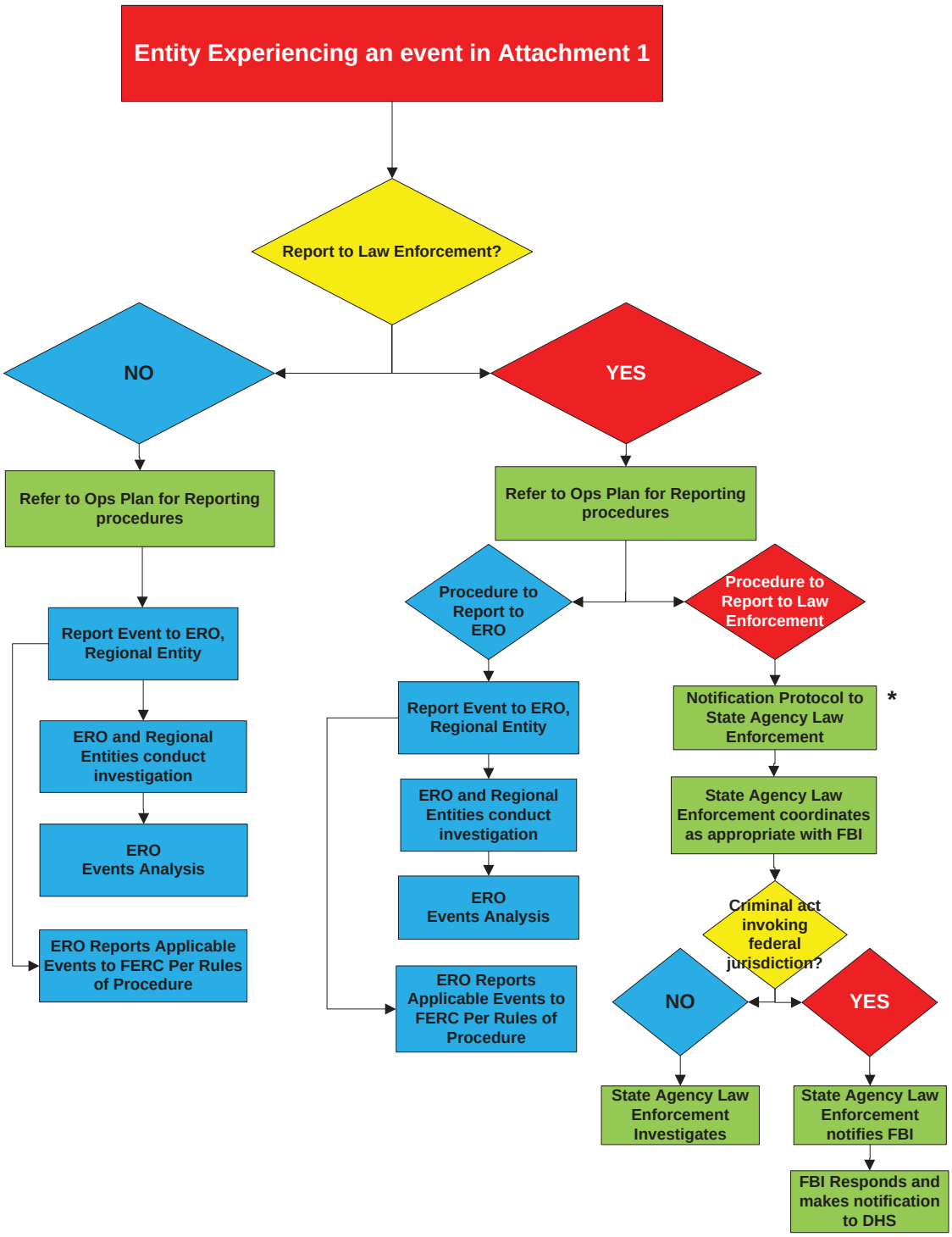

*Canadian entities will follow law enforcement protocols applicable in their jurisdictions

B. Requirements and Measures

R1. Each Responsible Entity shall have an Operating Plan that includes: *[Violation Risk: Factor: Lower] [Time Horizon: Operations Planning]*

1.1. A process for identifying events listed in Attachment 1.

1.2. A process for gathering information for Attachment 2 regarding events listed in Attachment 1.

1.3. A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate:

- Internal company personnel
- The Responsible Entity's Regional Entity
- Law enforcement
- Governmental or provincial agencies

1.4. Provision(s) for updating the Operating Plan within 90 calendar days of any change in assets, personnel, other circumstances that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3.

1.5. A Process for ensuring the responsible entity reviews the Operating Plan at least annually (once each calendar year) with no more than 15 months between reviews.

Rationale for R1

Every industry participant that owns or operates elements or devices on the grid has a formal or informal process, procedure, or steps it takes to gather information regarding what happened when events occur. This requirement has the Responsible Entity establish documentation on how that procedure, process, or plan is organized. This documentation may be a single document or a combination of various documents that achieve the reliability objective.

For the Operating Plan, Part 1.2 includes information gathering to be able to complete the report for reportable events. The main issue is to make sure an entity can a) identify when an event has occurred and b) be able to gather enough information to complete the report.

Part 1.3 could include a process flowchart, identification of internal and external personnel or entities to be notified, or a list of personnel by name and their associated telephone numbers.

M1. Each Responsible Entity will provide the current, dated, in force Operating Plan which includes Parts 1.1 - 1.5 as requested.

R2. Each Responsible Entity shall implement the parts of its Operating Plan that meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts 1.4 and 1.5 as specified. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*.

M2. Responsible Entities shall provide evidence that it implemented the parts of its Operating Plan to meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts, 1.4 and 1.5 as specified. Evidence may include, but is not limited to, an event report form (Attachment 2) or the OE-417 report submitted, operator logs, voice recordings, or dated documentation of review and update of the Operating Plan. (R2)

Rationale for R2

Each Responsible Entity must implement the various parts of Requirement R1. Parts 1.1 and 1.2 call for identifying and gathering information for actual events. Parts 1.4 and 1.5 require updating and reviewing the Operating Plan.

R3. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*.

M3. Responsible Entities shall provide a record of the type of event experienced; a dated copy of the Attachment 2 form or OE-417 report; and dated and time-stamped transmittal records to show that the event was reported. (R3)

Rationale for R3

Each Responsible Entity must report events via its Operating Plan based on Attachment 1. For each event listed in Attachment 1, there are entities listed that are to be notified as well as the time required to perform the reporting.

R4. Each Responsible Entity shall verify (through actual implementation for an event, or through a drill or exercise) the communication process in its Operating Plan, created pursuant to Requirement 1, Part 1.3, at least annually (once per calendar year), with no more than 15 calendar months between verification or actual implementation. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Rationale for R4

Each Responsible Entity must verify that its Operating Plan for communicating events is correct so that the entity can respond appropriately in the case of an actual event. The Responsible Entity may conduct a drill or exercise to test its Operating Plan for communicating events as often as it desires but the time period between tests can be no longer than 15 calendar months from the previous drill/exercise or actual event (i.e., if you conducted an exercise/drill/actual employment of the Operating Plan in January of one year, there would be another exercise/drill/actual employment by March 31 of the next calendar year). Multiple exercises in a 15 month period are not a violation of the requirement and would be encouraged to improve reliability.

Evidence showing that an entity used the communication process in its Operating Plan for an actual event qualifies as evidence to meet this requirement.

M4. The Responsible Entity shall provide evidence that it verified the communication process in its Operating Plan for events created pursuant to Requirement R1, Part 1.3. Either implementation of the communication process as documented in its Operating Plan for an actual event or documented evidence of a drill or exercise may be used as evidence to meet this requirement. The time period between an actual event or verification shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or dated documentation of a verification. (R3)

C. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

Regional Entity; or

If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement; or

Third-party monitor without vested interest in the outcome for the ERO

.

1.2 Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

Each Responsible Entity shall retain the current, in force document plus the ‘dated revision history’ from each version issued since the last audit for 3 calendar years for Requirement R1 and Measure M1.

Each Responsible Entity shall retain evidence from prior 3 calendar years for Requirements R2, R3, R4, and Measures M2, M3, M4.

Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.

If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3 Compliance Monitoring and Enforcement Processes:

Compliance Audits
Self-Certifications
Spot Checking
Compliance Violation Investigations
Self-Reporting
Complaints

1.4 Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Lower	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity has an Operating Plan but failed to include one of Parts 1.1 through 1.5.	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity has an Operating Plan but failed to include two of Parts 1.1 through 1.5.	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity has an Operating Plan but failed to include three of Parts 1.1 through 1.5.	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to include four or more of Parts 1.1 through 1.5.
R2	Real-time Operations and Same-day Operations	Medium	1.1: N/A 1.2: N/A 1.4: The Reliability Coordinator, Balancing Authority,	1.1: N/A 1.2: N/A 1.4: The Reliability Coordinator, Balancing Authority,	1.1: N/A 1.2: N/A 1.4: The Reliability Coordinator, Balancing Authority,	1.1: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator

			Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to update the Operating Plan more than 90 days of a change, but not more than 100 days after a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more	Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to update the Operating Plan more than 100 days of a change, but not more than 110 days after a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 18 calendar	Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to update the Operating Plan more than 110 days of a change, but not more than 120 days after a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 21 calendar	Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to implement the process for identifying events. 1.2: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to implement the process for gathering information for Attachment 2. 1.4: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator

			than 15 calendar months after its previous review, but not more than 18 calendar months after its previous review.	months after its previous review, but not more than 21 calendar months after its previous review.	months after its previous review, but not more than 24 calendar months after its previous review.	Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to update the Operating Plan more than 120 days of a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 24 calendar months after its previous review.
R3	Real-time Operations and Same-day Operations	Medium	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator

			Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 24 hours but less than or equal to 36 hours after an event requiring reporting within 24 hours in Attachment 1.	Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 36 hours but less than or equal to 48 hours after an event requiring reporting within 24 hours in Attachment 1. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 1 hour but less than 2 hours after an event requiring reporting within 1 hour in Attachment 1.	Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 48 hours but less than or equal to 60 hours after an event requiring reporting within 24 hours in Attachment 1. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report in more than 2 hours but less than 3 hours after an event requiring reporting within 1 hour in Attachment 1.	Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 60 hours after an event requiring reporting within 24 hours in Attachment 1. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 3 hours after an event requiring reporting within 1 hour in Attachment 1. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator,

						Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to submit a report for an event in Attachment 1.
R4	Operations Planning	Medium	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 15 calendar months after its previous test, but not more than 18 calendar months after its previous test. OR	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 18 calendar months after its previous test, but not more than 21 months after its previous test.	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 21 calendar months after its previous test, but not more than 24 months after its previous test.	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 24 calendar months after its previous test. OR The Reliability Coordinator, Balancing Authority, Interchange

			The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to verify the communication process in its Operating Plan within the calendar year.			Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to verify the communication process in its Operating Plan.

D. Variances

None.

E. Interpretations

None.

F. Interpretations

Guideline and Technical Basis (attached).

EOP-004 - Attachment 1: Events Table

NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per R1 and provide as much information as is available at the time of the notification. The affected Responsible Entity shall provide periodic verbal updates until adequate information is available to issue a written Event report. Reports to the ERO should be submitted to one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422.

Attachment 1 - Reportable Events			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Submit Attachment 2 or DOE OE-417 Report to:**
Destruction of BES equipment[1]	Each RC, BA, TO, TOP, GO, GOP, DP that experiences the destruction of BES equipment	Initial indication the event was due to operational error, equipment failure, external cause, or intentional or unintentional human action.	The parties identified pursuant to R1.3 within 1 hour of recognition of event.
Damage or destruction of Critical Asset per CIP-002	Applicable Entities under CIP-002	Initial indication the event was due to operational error, equipment failure, external cause, or intentional or unintentional human action.	The parties identified pursuant to R1.3 within 1 hour of recognition of event.
Damage or destruction of a Critical Cyber Asset per CIP-002	Applicable Entities under CIP-002.	Through intentional or unintentional human action.	The parties identified pursuant to R1.3 within 1 hour of recognition of event.
Forced intrusion[2]	Each RC, BA, TO, TOP, GO, GOP that experiences the	At a BES facility	The parties identified pursuant to R1.3 within 1 hour of recognition of

[1]BES equipment that: i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii) Damaged or destroyed due to intentional or unintentional human action which removes the BES equipment from service. Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative).

[2] Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects the reliability of the BES).

Attachment 1 - Reportable Events			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Submit Attachment 2 or DOE OE-417 Report to:**
	forced intrusion		event.
Risk to BES equipment[3]	Each RC, BA, TO, TOP, GO, GOP, DP that experiences the risk to BES equipment	From a non-environmental physical threat	The parties identified pursuant to R1.3 within 1 hour of recognition of event.
Detection of a reportable Cyber Security Incident.	Each RC, BA, TO, TOP, GO, GOP, DP, ERO or RE that experiences the Cyber Security Incident	That meets the criteria in CIP-008	The parties identified pursuant to R1.3 within 1 hour of recognition of event.
BES Emergency requiring public appeal for load reduction	Deficient entity is responsible for reporting	Each public appeal for load reduction	The parties identified pursuant to R1.3 within 24 hours of recognition of the event.
BES Emergency requiring system-wide voltage reduction	Initiating entity is responsible for reporting	System wide voltage reduction of 3% or more	The parties identified pursuant to R.1.3 within 24 hours of recognition of the event.
BES Emergency requiring manual firm load shedding	Initiating entity is responsible for reporting	Manual firm load shedding ≥ 100 MW	The parties identified pursuant to R1.3 within 24 hours of recognition of the event.
BES Emergency resulting in automatic firm load shedding	Each DP or TOP that experiences the automatic load shedding	Firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)	The parties identified pursuant to R1.3 within 24 hours of recognition of the event.
Voltage deviations on BES Facilities	Each TOP that experiences the voltage deviation	± 10% sustained for ≥ 15 continuous minutes	The parties identified pursuant to R1.3 within 24 hours after 15 minutes of exceeding the threshold.

[3] Examples include a train derailment adjacent to BES equipment that either could have damaged the equipment directly or has the potential to damage the equipment (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center) and report of suspicious device near BES equipment.

Attachment 1 - Reportable Events			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Submit Attachment 2 or DOE OE-417 Report to:**
IROL Violation (all Interconnections) or SOL Violation (WECC only)	Each RC that experiences the IROL Violation (all Interconnections) or SOL violation (WECC only)	Operate outside the IROL for time greater than IROL Tv (all Interconnections) or Operate outside the SOL for a time greater than the SOL Tv (WECC only).	The parties identified pursuant to R1.3 within 24 hours after exceeding the Tv threshold.
Loss of Firm load for ≥ 15 Minutes	Each BA, TOP, DP that experiences the loss of firm load	• ≥ 300 MW for entities with previous year's demand ≥ 3000 MW • ≥ 200 MW for all other entities	The parties identified pursuant to R1.3 24 hours after exceeding the 15 minute threshold
System Separation (Islanding)	Each RC, BA, TOP, DP that experiences the system separation	Each separation resulting in an island of generation and load ≥ 100 MW	The parties identified pursuant to R1.3 within 24 hours after occurrence is identified
Generation loss	Each BA, GOP that experiences the generation loss	• ≥ 2,000 MW for entities in the Eastern or Western Interconnection • ≥ 1000 MW for entities in the ERCOT or Quebec Interconnection	The parties identified pursuant to R1.3within 24 hours after occurrence.
Loss of Off-site power to a nuclear generating plant (grid supply)	Each TO, TOP that experiences the loss of off-site power to a nuclear generating plant	Affecting a nuclear generating station per the Nuclear Plant Interface Requirement	The parties identified pursuant to R1.3 within 24 hours after occurrence
Transmission loss	Each TOP that experiences the transmission loss	Unintentional loss of Three or more Transmission Facilities (excluding successful automatic reclosing)	The parties identified pursuant to R1.3 within 24 hours after occurrence
Unplanned Control Center evacuation	Each RC, BA, TOP that experiences the potential event	Unplanned evacuation from BES control center facility	The parties identified pursuant to R1.3 within 24 hours of recognition of event.
Loss of monitoring or all voice	Each RC, BA, TOP that experiences the loss of	Voice Communications: Affecting a BES control center for ≥ 30 continuous minutes	The parties identified pursuant to R1.3 within 24 hours of recognition

Attachment 1 - Reportable Events			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Submit Attachment 2 or DOE OE-417 Report to:**
communication capability	monitoring or all voice communication capability	Monitoring: Affecting a BES control center for ≥ 30 continuous minutes such that analysis tools (State Estimator, Contingency Analysis) are rendered inoperable.	of event.

EOP-004 - Attachment 2: Event Reporting Form

EOP-004, Attachment 2: Event Reporting Form

This form is to be used to report events to parties listed in Attachment 1, column labeled "Submit Attachment 2 or DOE OE-417 Report to:". These parties will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Reports should be submitted via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422.

	Task	Comments
1.	Entity filing the report include: Company name: Name of contact person: Email address of contact person: Telephone Number: Submitted by (name):	
2.	Date and Time of recognized event. Date: (mm/dd/yyyy) Time: (hh:mm) Time/Zone:	
3.	Did the actual or potential event originate in your system?	Actual event ☐ Potential event ☐ Yes ☐ No☐ Unknown ☐
4.	**Event Identification and Description:**	
	(Check applicable box) ☐ public appeal ☐ voltage reduction ☐ manual firm load shedding ☐ firm load shedding(undervoltage, underfrequency, SPS/RAS) ☐ voltage deviation ☐ IROL violation	Written description (optional unless Other is checked):

EOP-004, Attachment 2: Event Reporting Form

This form is to be used to report events to parties listed in Attachment 1, column labeled "Submit Attachment 2 or DOE OE-417 Report to:". These parties will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Reports should be submitted via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422.

	Task	Comments
	☐ loss of firm load ☐ system separation(islanding) ☐ generation loss ☐ loss of off-site power to nuclear generating plant ☐ transmission loss ☐ damage or destruction of BES equipment ☐ damage or destruction of Critical Asset ☐ damage or destruction of Critical Cyber Asset ☐ unplanned control center evacuation ☐ fuel supply emergency ☐ loss of all monitoring or voice communication capability ☐ forced intrusion Risk to BES equipment ☐ reportable Cyber Security Incident ☐ other	

Guideline and Technical Basis

Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01) - Reporting Concepts

Introduction

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and has developed updated standards based on the SAR.

The standards listed under the SAR are:

- CIP-001 — Sabotage Reporting
- EOP-004 — Disturbance Reporting

The changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). These standard deals exclusively with after-the-fact reporting.

The DSR SDT has consolidated disturbance and sabotage event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts and Assumptions:

The Standard:

- Requires reporting of "events" that impact or may impact the reliability of the bulk electric system
- Provides clear criteria for reporting
- Includes consistent reporting timelines
- Identifies appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- Provides clarity around of who will receive the information

Discussion of Disturbance Reporting

Disturbance reporting requirements existed in the previous version of EOP-004. The current approved definition of Disturbance from the NERC Glossary of Terms is:

1. An unplanned event that produces an abnormal system condition.
2. Any perturbation to the electric system.

3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.

Disturbance reporting requirements and criteria were in the previous EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and developed the list of events that are to be reported under this standard (attachment 1).

Discussion of Event Reporting
There are situations worthy of reporting because they have the potential to impact reliability.

t Event reporting facilitates industry awareness, which allows potentially impacted parties to prepare for and possibly mitigate any associated reliability risk. It also provides the raw material, in the case of certain potential reliability threats, to see emerging patterns.

Examples of such events include:

- Bolts removed from transmission line structures
- Detection of cyber intrusion that meets criteria of CIP-008 or its successor standard
- Forced intrusion attempt at a substation
- Train derailment near a transmission right-of-way
- Destruction of Bulk Electrical System equipment

What about sabotage?
One thing became clear in the DSR SDT's discussion concerning sabotage: everyone has a different definition. The current standard CIP-001 elicited the following response from FERC in FERC Order 693, paragraph 471 which states in part: *". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."*

Often, the underlying reason for an event is unknown or cannot be confirmed. The DSR SDT believes that by reporting material risks to the Bulk Electrical System using the event categorization in this standard, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.

Certain types of events should be reported to NERC, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and/or Provincial or local law enforcement. Other types of impact events may have different reporting requirements. For example, an event that is related to copper theft may only need to be reported to the local law enforcement authorities.

Potential Uses of Reportable Information
Event analysis, correlation of data, and trend identification are a few potential uses for the information reported under this standard. The standard requires Functional entities to report the incidents and provide known information at the time of the report. Further data gathering necessary for event analysis is provided for under the Events Analysis Program and the NERC

Rules of Procedure. Other entities (e.g. – NERC, Law Enforcement, etc) will be responsible for performing the analyses. The NERC Rules of Procedure (section 800) provide an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for reliability. Jurisdictional agencies (which may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE) have other duties and responsibilities.

Collection of Reportable Information or "One stop shopping"

The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT has updated the listing of reportable events in Attachment 1 based on discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences still exist.

The reporting required by this standard is intended to meet the uses and purposes of NERC. The DSR SDT recognizes that other requirements for reporting exist (e.g., DOE-417 reporting), which may duplicate or overlap the information required by NERC. To the extent that other reporting is required, the DSR SDT envisions that duplicate entry of information should not be necessary, and the submission of the alternate report will be acceptable to NERC so long as all information required by NERC is submitted. For example, if the NERC Report duplicates information from the DOE form, the DOE report may be included or attached to the NERC report, in lieu of entering that information on the NERC report.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SC approved SAR for initial posting (April, 2009).
2. SAR posted for comment (April 22 – May 21, 2009).
3. SC authorized moving the SAR forward to standard development (September 2009).
4. Concepts Paper posted for comment (March 17 – April 16, 2010).
5. Initial Informal Comment Period (September 15 – October 15, 2010)
6. Second Comment Period (Formal) (March 9 – April 8, 2011)

Proposed Action Plan and Description of Current Draft

This is the ~~first~~third posting of the proposed standard in accordance with Results-Based Criteria. The drafting team requests posting for a ~~30~~45-day formal comment period concurrent with the formation of the ballot pool and the initial ballot.

Future Development Plan

Anticipated Actions	Anticipated Date
Drafting team considers comments, makes conforming changes~~, and proceed to~~ on second ~~comment~~posting	April - October ~~2010 – February~~ 2011
~~Second Comment Period~~	~~March – May 2011~~
Third Comment/Ballot period	~~June - July~~November-December 2011
Recirculation Ballot period	~~July - August~~December 2011
Receive BOT approval	~~September 2011~~February 2012

Effective Dates

~~1. The standard~~EOP-004-2 shall become effective on the first ~~calendar~~ day of the third calendar quarter after ~~the date of the order providing~~ applicable regulatory approval.

~~2.~~ In those jurisdictions where no regulatory approval is required, ~~the~~this standard shall become effective on the first ~~calendar~~ day of the third calendar quarter after Board of Trustees ~~adoption~~approval.

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-~~1~~2a Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2 Impact Event Reporting; Retire CIP-001-~~1a~~2a Sabotage Reporting and Retired EOP-004-1 Disturbance Reporting.~~–~~ Retire CIP-008-4, Requirement 1, Part 1.3.	Revision to entire standard (Project 2009-01)

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

~~**Impact Event: Any event which has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action.**~~

None

When this standard has received ballot approval, the text boxes will be moved to the Guideline and Technical Basis Section.

A. Introduction

1. Title: ~~Impact~~ Event Reporting

2. Number: EOP-004-2

3. Purpose: To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of ~~Impact Events~~events with the potential to impact reliability and their causes, if known, by the Responsible Entities.

4. Applicability

4.1. Functional Entities: Within the context of EOP-004-2, the term "Responsible Entity" shall mean:

4.1.1. Reliability Coordinator

4.1.2. Balancing Authority

4.1.3. Interchange ~~Authority~~Coordinator

4.1.4. Transmission Service Provider

4.1.5. Transmission Owner

4.1.6. Transmission Operator

4.1.7. Generator Owner

4.1.8. Generator Operator

4.1.9. Distribution Provider

4.1.10. ~~4.1.10~~ Load Serving Entity

4.1.11. Electric Reliability Organization

4.1.12. Regional Entity

5. Background:

NERC established a SAR Team in 2009 to investigate and propose revisions to the CIP-001 and EOP-004 Reliability Standards. The team was asked to consider the following:

1. CIP-001 ~~may~~could be merged with EOP-004 to eliminate redundancies.
2. Acts of sabotage have to be reported to the DOE as part of EOP-004.
3. Specific references to the DOE form need to be eliminated.
4. EOP-004 ~~has~~had some 'fill-in-the-blank' components to eliminate.

The development ~~may include~~included other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards ~~(see tables for each standard at the end of this SAR for more detailed information).~~.

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC SC in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009. ~~A "concepts paper" was designed to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed.~~

~~The~~
The DSR SDT developed a concept paper to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT had developed. The posting of the concept paper sought comments from stakeholders on the "road map" that will be used by the ~~SDR~~DSR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the ~~SDR~~DSR SDT.

The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC issues database and FERC Order 693 Directives in order to determine a prudent course of action with respect to revision of these standards.

~~The DSR SDT has used a working definition for "Impact Events" to develop Attachment 1 as follows:~~

> ~~"An Impact Event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action."~~

~~The DSR SDT has proposed this definition for~~

Summary of Key Concepts

The DSRSDT identified the following principles to assist them in developing the standard:

- Develop a single form to report disturbances and events that threaten the reliability of the bulk electric system
- Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion ~~in the NERC Glossary for "Impact Event". The types of Impact Events that are required to be reported are contained within Attachment 1. Only these events are required to be reported under this Standard. The DSR SDT~~ of regional reporting requirements
- Establish clear criteria for reporting
- Establish consistent reporting timelines
- Provide clarity around who will receive the information and how it will be used

During the development of concepts, the DSR SDT considered the FERC directive to "further define sabotage~~" and~~ ". There was concern among stakeholders that a definition may be ambiguous and subject to interpretation. Consequently, the DSR SDT decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was ~~that of~~ sabotage or ~~merely~~ vandalism without the intervention of law enforcement~~ after the fact. This will~~. The DSR SDT felt that attempting to define sabotage would result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard~~ and therefore it is inappropriate to attempt to define it.~~. The ~~Impact Events~~events listed in Attachment 1 were developed to provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive. ~~Attachment 1, Part A is to be used for those actions that have impacted the electric system and in particular the section "Damage or destruction to equipment" clearly defines that all equipment that intentional or non intentional human error be reported. Attachment 1, Part B covers the similar items but the action has not fully occurred but may cause a risk to the electric system and is required to be reported.~~

~~To support this concept, the~~ The types of events that are required to be reported are contained within Attachment 1. The DSR SDT has ~~provided specific event for reporting including types of Impact~~coordinated with the NERC Events ~~and timing thresholds pertaining to~~ Analysis Working Group to develop the ~~different types of Impact Events and who's responsibility for reporting~~list of events that are to be reported under ~~the different Impact Events. This information is outlined in Attachment 1 to the proposed~~ this standard. Attachment 1, Part A pertains to those actions or events that have impacted the Bulk Electric System. These events were previously reported under EOP-004-1, CIP-001-1 or the Department of Energy form OE-417. Attachment 1, Part B covers similar items that may have had an impact on the Bulk Electric System or has the potential to have an impact and should be reported.

The DSR SDT wishes to make clear that the proposed ~~changes do~~Standard does not include any real-time operating notifications for the ~~types of~~ events ~~covered by CIP-001, EOP-004. This~~listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. ~~TOP~~the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting.

~~The DSR SDT is proposing to consolidate disturbance and Impact Event reporting under a single standard. These two components and other key concepts are discussed in the following sections.~~

~~**Summary of Concepts**~~

- ~~A single form to report disturbances and Impact Events that threaten the reliability of the bulk electric system~~
- ~~Other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements~~
- ~~Clear criteria for reporting~~
- ~~Consistent reporting timelines~~
- ~~Clarity around of who will receive the information and how it will be used~~

Data Gathering

The requirements of EOP-004-1 require that entities "promptly analyze Bulk Electric System disturbances on its system or facilities" (Requirement R2). The requirements of EOP-004-2 specify that certain types of events are to be reported but do not include provisions to analyze events. Events reported under EOP-004-2 may trigger further scrutiny by the ERO Events Analysis Program. If warranted, the Events Analysis Program personnel may request that more data for certain events be provided by the reporting entity or other entities that may have experienced the event. Entities are encouraged to become familiar with the Events Analysis Program and the NERC Rules of Procedure to learn more about with the expectations of the program.

Law Enforcement Reporting

The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting ~~Impact Events.~~events. Certain outages, such as those due to vandalism and terrorism, ~~are~~may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those ~~Impact Events~~events which have the potential ~~of~~to impact a wider area ~~affect upon the industry which~~of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading ~~involving Impact Events.~~events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.

Stakeholders in the Reporting Process

- Industry
- NERC (ERO~~)~~), Regional Entity
- FERC
- DOE
- NRC
- DHS – Federal
- Homeland Security- State
- State Regulators
- Local Law Enforcement
- State or Provincial Law Enforcement
- FBI
- Royal Canadian Mounted Police (RCMP)

The above stakeholders have an interest in the timely notification, communication and response to an incident at an industry facility. The stakeholders have various levels of accountability and have a vested interest in the protection and response to ensure the reliability of the BES.

Present expectations of the industry under CIP-001-1a:

It has been the understanding by industry participants that an occurrence of sabotage has to be reported to the FBI. The FBI has the jurisdictional requirements to investigate acts of sabotage and terrorism. The ~~present~~ CIP-001-1-1a standard requires a liaison relationship on behalf of the industry and the FBI or RCMP. Annual requirements, under the standard, of the industry have not been clear and have lead to misunderstandings and confusion in the industry as to how to demonstrate that the liaison is in place and effective. ~~FBI offices~~ As an example of proof of compliance with Requirement R4, responsible entities have ~~been~~ asked FBI Office personnel to ~~confirm~~provide, on FBI letterhead, confirmation of the existence of a working relationship to report acts of sabotage ~~to include references to~~, , the number of years the liaison relationship has been in existence, and ~~confirming~~the validity of the telephone numbers for the FBI.

Coordination of Local and State Law Enforcement Agencies with the FBI

The Joint Terrorism Task Force (JTTF) came into being with the first task force being established in 1980. JTTFs are small cells of highly trained, locally based, ~~passionately~~ committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. The JTTF is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. Coordination and communications largely through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs. This information flow can be most beneficial to the industry in analytical intelligence, incident response and investigation. Historically, the most immediate response to an industry incident has been local and state law enforcement agencies to suspected vandalism and criminal damages at industry facilities. Relying upon the JTTF coordination between local, state and FBI law enforcement would be beneficial to effective communications and the appropriate level of investigative response.

Coordination of Local and Provincial Law Enforcement Agencies with the RCMP

A similar law ~~enforecment~~enforcement coordination hierarchy exists in Canada. Local and Provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. The Provincial law enforcement agency has a reporting relationship with the ~~Royla~~Royal Canadian Mounted Police (RCMP).

A Reporting Process Solution – EOP-004

A proposal discussed with the FBI, FERC Staff, NERC Standards Project Coordinator and the SDT Chair is reflected in the flowchart below (Reporting Hierarchy for ~~Impact Event EOP-004-2~~Reportable Events). Essentially, reporting an ~~Impact Event~~event to law enforcement agencies will only require the industry to notify the state or provincial or local level law enforcement agency. The state or provincial or local level law enforcement agency will coordinate with ~~local~~ law enforcement with jurisdiction to investigate. If the state or provincial or local level law enforcement agency decides federal agency law enforcement or the RCMP should respond and

investigate, the state or provincial or local level law enforcement agency will notify and coordinate with the FBI or the RCMP.

Reporting Hierarchy for Reportable Events

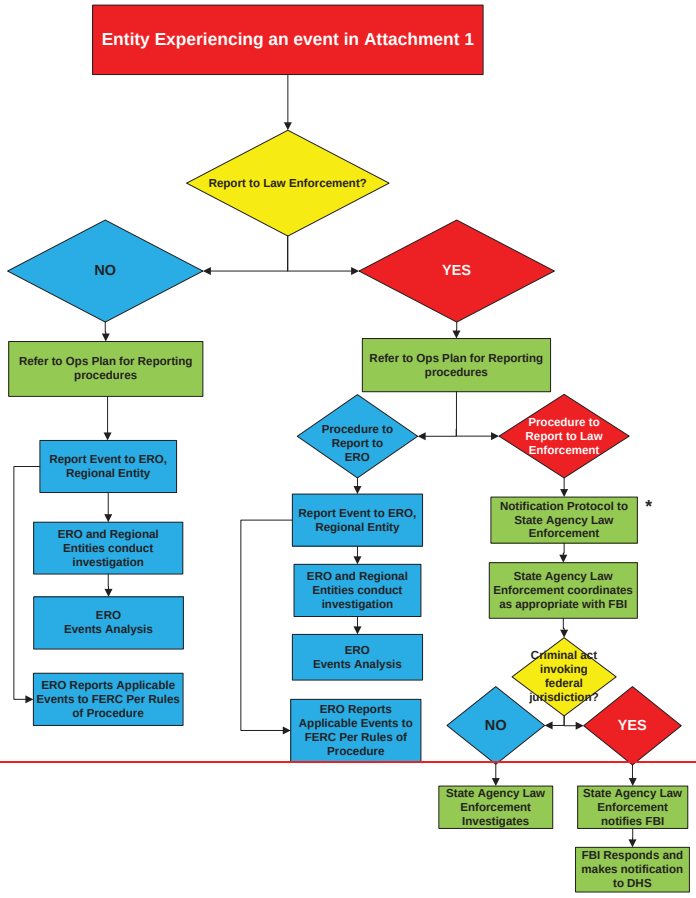

*Canadian entities will follow law enforcement protocols applicable in their jurisdictions

Reporting Hierarchy for Reportable Events

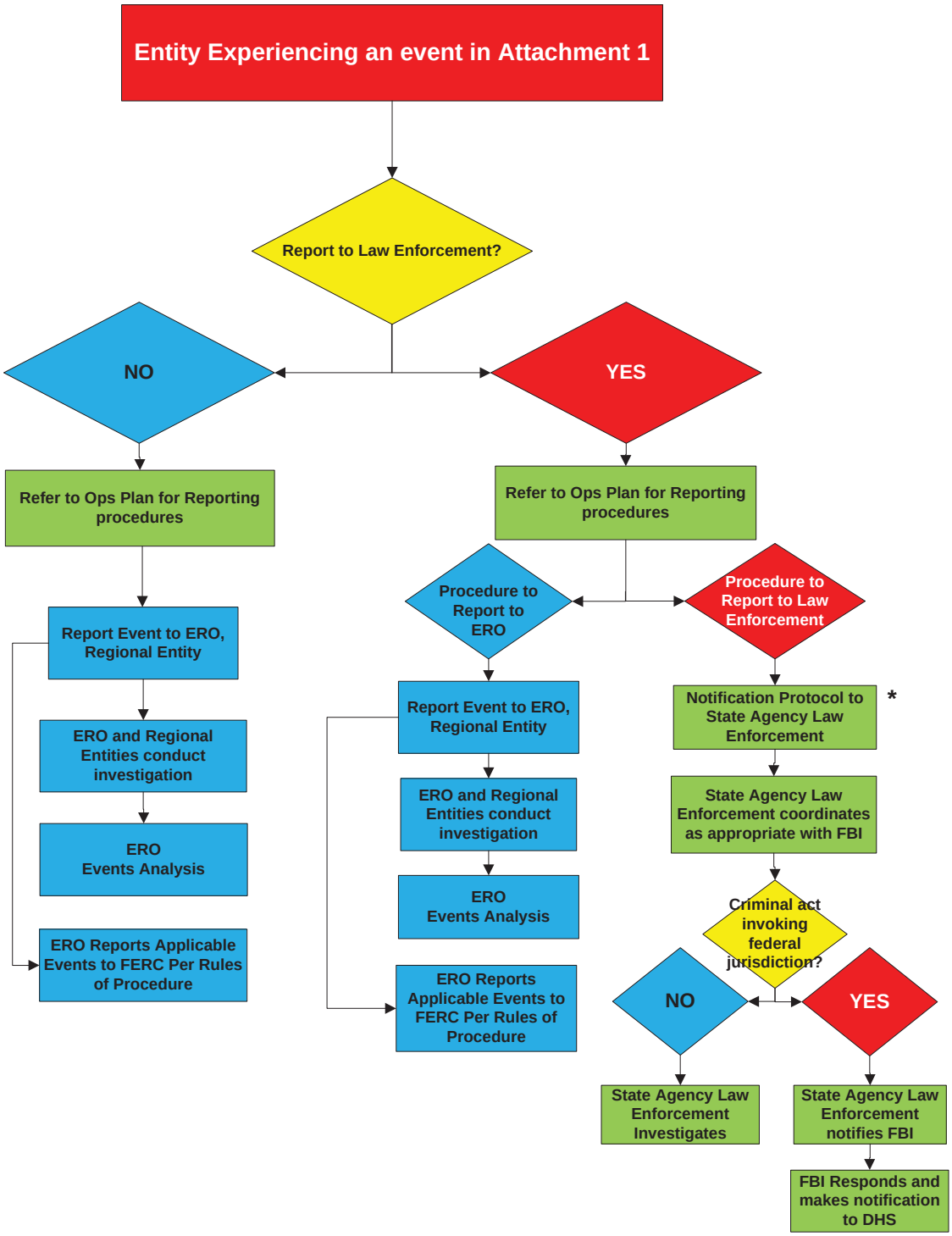

*Canadian entities will follow law enforcement protocols applicable in their jurisdictions

B. Requirements and Measures

R1. Each Responsible Entity shall have an ~~Impact Event~~ Operating Plan that includes: *[Violation Risk: Factor ~~Medium~~: Lower] [Time Horizon: ~~Long-term~~Operations Planning]*

1.1. ~~An Operating Process~~A process for identifying ~~Impact Events~~events listed in Attachment 1.

1.2. ~~An Operating Procedure~~A process for gathering information for Attachment 2 regarding ~~observed Impact Events~~events listed in Attachment 1.

1.3. ~~An Operating Process~~A process for communicating ~~recognized Impact Events~~ events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate:

- Internal company personnel ~~notification(s).~~
- ~~External organizations to notify to include but not limited to the Responsible Entities' Reliability Coordinator, NERC,~~ The Responsible ~~Entities'~~Entity's Regional Entity~~,~~
- Law ~~Enforcement, and~~ enforcement
- Governmental or ~~Provincial Agencies.~~provincial agencies

1.4. Provision(s) for updating the ~~Impact Event~~ Operating Plan within 90 calendar days of any change ~~to its content.~~ in assets, personnel, other circumstances that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3.

1.5. A Process for ensuring the responsible entity reviews the Operating Plan at least annually (once each calendar year) with no more than 15 months between reviews.

~~1.4.~~

~~Rationale for R1~~

~~Every industry participant that owns or operates elements or devices on the grid has a formal or informal process, procedure, or steps it takes to gather information regarding what happened and why it happened when Impact Events occur. This requirement has the Registered Entity establish documentation on how that procedure, process, or plan is organized.~~

~~For the Impact Event Operating Plan, the DSR SDT envisions that Part 1.2 includes performing sufficient analysis and information gathering to be able to complete the report for reportable Impact Events. The main issue is to make sure an entity can a) identify when an Impact Event has occurred and b) be able to gather enough information to complete the report.~~

~~Part 1.3 could include a process flowchart, identification of internal positions to be notified and to make notifications, or a list of personnel by name as well as telephone numbers.~~

~~The Impact Event Operating Plan may include, but not be limited to, the following: how the entity is notified of event's occurrence, person(s) initially tasked with the overseeing the assessment or analytical study, investigatory steps typically taken, and documentation of the assessment / remedial action plan.~~

M1. Each Responsible Entity ~~shall~~will provide the current, dated, in force ~~Impact Event~~ Operating Plan ~~to the Compliance Enforcement Authority~~which includes Parts 1.1 - 1.5 as requested.

R2. Each Responsible Entity shall implement the parts of its ~~Impact Event~~ Operating Plan ~~documented in~~that meet Requirement R1~~ for Impact Events listed in Attachment 1 (~~, Parts ~~A~~1.1 and ~~B).~~1.2 for an actual event and Parts 1.4 and 1.5 as specified. *[Violation Risk~~:~~ Factor: Medium] [Time Horizon: ~~Real-time~~ Operations ~~and Same-day Operations]~~Assessment].*

M2. ~~To the extent that an~~ Responsible ~~Entity has an Impact Event on its Facilities, the Responsible Entity~~Entities shall ~~documentation of~~ provide evidence that it implemented the ~~implementation~~parts of its ~~Impact Event~~ Operating ~~Plans. Such evidence could~~Plan to meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts, 1.4 and 1.5 as specified. Evidence may include, but is not limited to, an event report form (Attachment 2) or the OE-417 report submitted, operator logs, voice recordings, or ~~other notations and documents retained by the Registered Entity for each Impact Event.~~ dated documentation of review and update of the Operating Plan. (R2)

Rationale for R2

Each Responsible Entity must implement the various parts of Requirement R1. Parts 1.1 and 1.2 call for identifying and gathering information for actual events. Parts 1.4 and 1.5 require updating and reviewing the Operating Plan.

R3. Each Responsible Entity shall ~~conduct a test of~~ report events in accordance with its Operating ~~Process~~Plan developed to address the events listed in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment].*

M3. Responsible Entities shall provide a record of the type of event experienced; a dated copy of the Attachment 2 form or OE-417 report; and dated and time-stamped transmittal records to show that the event was reported. (R3)

R4. Each Responsible Entity shall verify (through actual implementation for ~~communicating recognized Impact~~

~~Rationale for R3~~

~~The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized Impact Events is correct so that the entity can respond appropriately in the case of an actual Impact Event. The Responsible Entity may conduct a drill or exercise of its Operating Process for communicating recognized Impact Events as often as it desires but the time period between such drill or exercise can be no longer than 15 months from the previous drill/exercise or actual Impact Event (i.e., if you conducted an exercise/drill/actual employment of the Operating Process in January of one year, there would be another exercise/drill/actual employment by March 31 of the next calendar year)). Multiple exercises in a 15 month period are not a violation of the requirement and would be encouraged to improve reliability.~~

R
E ing
P
e
e tual
e or
e ng
e veen
te n the
p
c e
Operating Plan in January of one year, there would be another exercise/drill/actual employment by March 31 of the next calendar year). Multiple exercises in a 15 month period are not a violation of the requirement and would be encouraged to improve reliability.
Evidence showing that an entity used the communication process in its Operating Plan for an actual event qualifies as evidence to meet this requirement.

~~Events~~an event, or through a drill or exercise) the communication process in its Operating Plan, created pursuant to Requirement ~~R1~~1, Part 1.3, at least annually~~,~~ (once per calendar year), with no more than 15 calendar months between ~~tests.~~verification or actual implementation. *[Violation Risk~~:~~ Factor: Medium] [Time Horizon: ~~Long-term~~Operations Planning]*

~~**M3**. In the absence of an actual Impact Event, the~~**M4**. The Responsible Entity shall provide evidence that it ~~conducted a mock Impact Event and followed~~verified the communication process in its Operating ~~Process~~Plan for ~~communicating recognized Impact Events~~events created pursuant to Requirement R1, Part 1.3. Either implementation of the communication process as documented in its Operating Plan for an actual event or documented evidence of a drill or exercise may be used as evidence to meet this requirement. The time period between an actual ~~and~~event or ~~mock Impact Events~~verification shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or dated documentation~~.~~ of a verification. (R3)

~~**R4.** Each Responsible Entity shall review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan at least annually with no more than 15 calendar months between review sessions*[Violation Risk: Factor Medium] [Time Horizon: Long-term Planning].*~~

~~**M4.** Responsible Entities shall provide the materials presented to verify content and the association between the people listed in the plan and those who participated in the review, documentation showing who was present and when internal personnel were trained on the responsibilities in the plan.~~

~~**R5**. Each Responsible Entity shall report Impact Events in accordance with the Impact Event Operating Plan pursuant to Requirement R1 and Attachment 1 using the form in Attachment 2 or the DOE OE-417 reporting form. *[Violation Risk: Factor: Medium] [Time Horizon: Real-time Operations and Same-day Operations].*~~

~~**M5.** Responsible Entities shall provide evidence demonstrating the submission of reports using the plan created pursuant to Requirement R1 and Attachment 1 using either the form in Attachment 2 or the DOE OE-417 report. Such evidence will include a copy of the Attachment 2 form or OE-417 report submitted, evidence to support the type of Impact Event experienced; the date and time of the Impact Event; as well as evidence of report submittal that includes date and time.~~

C. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement~~.~~; or

~~**Compliance Monitoring and Enforcement Processes:**~~

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Violation Investigations~~
- ~~Self-Reporting~~
- ~~Complaints~~

Third-party monitor without vested interest in the outcome for the ERO

.

1.2 Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

Each Responsible Entity shall retain the current, in force document plus the 'dated revision history' from each version issued since the last audit for 3 calendar years for Requirement R1 and Measure M1.

Each Responsible Entity shall retain evidence from prior 3 calendar years for Requirements R2, R3, R4, and Measures M2, M3, M4.

Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.

If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3 Compliance Monitoring and Enforcement Processes:

Compliance Audits
Self-Certifications
Spot Checking
Compliance Violation Investigations
Self-Reporting

Complaints

1.4 Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	~~Medium~~Lower	The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity has an ~~Impact Event~~ Operating Plan but failed to include one of Parts 1.1 through 1.~~4~~5.	The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity has ~~a Impact Event~~an Operating Plan but failed to include two of Parts 1.1 through 1.~~4~~5.	The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity has an ~~Impact Event~~ Operating Plan but failed to include three of Parts 1.1 through 1.~~4~~5.	The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to include ~~all~~four or more of Parts 1.1 through 1.~~4~~5.
~~**R2**~~	~~Real-time Operations and Same-day~~	~~Medium~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity failed to implement its Impact Event Operating Plan~~

	Operations					for an Impact Event listed in Attachment 1.
R3R2	Long-term PlanningReal-time Operations and Same-day Operations	Medium	1.1: N/A 1.2: N/A 1.4: The ResponsibleReliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to conduct a test of its update the Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 inPlan more than	1.1: N/A 1.2: N/A 1.4: The ResponsibleReliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to conduct a test of its update the Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3inPlan more than	1.1: N/A 1.2: N/A 1.4: The ResponsibleReliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to conduct a test of its update the Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 inPlan more than	1.1: The ResponsibleReliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to conduct a test of its implement the process for identifying events. 1.2: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator

			90 days of a change, but not more than 100 days after a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 15 calendar months ~~but less~~after its previous review, but not more than 18 calendar months~~.~~ after its previous review.	100 days of a change, but not more than 110 days after a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 18 calendar months ~~but less~~after its previous review, but not more than 21 calendar months after its previous review.	110 days of a change, but not more than 120 days after a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 21 calendar months ~~but less~~after its previous review, but not more than 24 calendar months after its previous review.	Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to implement the process for gathering information for Attachment 2. 1.4: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to update the Operating ~~Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 in~~Plan more than 120 days of a change.

						1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 24 calendar months after its previous review.
~~**R4**~~	~~Long-term Planning~~	~~Medium~~	~~The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan l in more than 15 months but less than 18 months.~~	~~The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 18 months but less than 21 months.~~	~~The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 21 months but less than 24 months.~~	~~The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 24 months~~
~~**R5**~~**R3**	Real-time	Medium	The	The	The	The ~~Responsible~~

	Operations and Same-day Operations		~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity ~~failed to submit~~submitted a report ~~in~~more than 24 hours but less than or equal to 36 hours ~~for~~after an ~~Impact Event~~event requiring reporting within 24 hours in Attachment 1.	~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity ~~failed to submit~~submitted a report ~~in~~ more than 36 hours but less than or equal to 48 hours ~~for~~after an ~~Impact Event~~event requiring reporting within 24 hours in Attachment 1. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner,	~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity ~~failed to submit~~submitted a report ~~in~~ more than 48 hours but less than or equal to 60 hours ~~for~~after an ~~Impact Event~~event requiring reporting within 24 hours in Attachment 1. OR The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider,	~~Entity failed to submit a report in~~ Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 60 hours ~~for~~after an ~~Impact Event~~event requiring reporting within 24 hours in Attachment 1. OR The ~~Responsible~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner,

				Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 1 hour but less than 2 hours after an event requiring reporting within 1 hour in Attachment 1.	Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity ~~failed to submit~~submitted a report in more than ~~1 hour~~2 hours but less than ~~2~~3 hours ~~for~~after an ~~Impact Event~~event requiring reporting within 1 hour in Attachment 1.	Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity ~~failed to submit~~submitted a report ~~in~~ more than ~~2~~3 hours ~~for~~after an ~~Impact Event~~event requiring reporting within 1 hour in Attachment 1. OR The ~~responsible entity~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to submit a report for an ~~Impact Event~~event in Attachment 1.

~~R4~~	~~Operations Planning~~	~~Medium~~	~~The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 15 calendar months after its previous test, but not more than 18 calendar months after its previous test.~~ ~~OR~~ ~~The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider,~~	~~The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 18 calendar months after its previous test, but not more than 21 months after its previous test.~~	~~The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 21 calendar months after its previous test, but not more than 24 months after its previous test.~~	~~The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 24 calendar months after its previous test.~~ ~~OR~~ ~~The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator~~

			~~Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to verify the communication process in its Operating Plan within the calendar year.~~			~~Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to verify the communication process in its Operating Plan.~~

D. Variances

None.

E. Interpretations

None.

F. Interpretations

Guideline and Technical Basis (attached).

EOP-004 - Attachment 1: ~~Impact~~ Events Table

NOTE: Under certain adverse conditions~~,~~ (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an ~~Impact Event~~event and issue a written ~~Impact~~ Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify ~~its Regional Entity(ies) and NERC, (e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422)~~parties per R1 and provide as much information as is available~~.~~ at the time of the notification. The affected Responsible Entity shall ~~then~~ provide periodic verbal updates until adequate information is available to issue a written ~~Impact~~ Event report.

~~EOP-004 – Attachment 1 – Actual Reliability Impact – Part A~~			
~~Event~~	~~Entity with Reporting Responsibility~~	~~Threshold for Reporting~~	~~Time to Submit Report~~
~~Energy Emergency requiring Public appeal for load reduction~~	~~Initiating entity is responsible for reporting~~	~~Each public appeal for load reduction~~	~~Within 1 hour of issuing a public appeal~~
~~Energy Emergency requiring system-wide voltage reduction~~	~~Initiating entity is responsible for reporting~~	~~System wide voltage reduction of 3% or more~~	~~Within 1 hour after event is initiated~~
~~Energy Emergency requiring manual firm load shedding~~	~~Initiating entity is responsible for reporting~~	~~Manual firm load shedding ≥ 100 MW~~	~~Within 1 hour after event is initiated~~
~~Energy Emergency resulting in automatic firm load shedding~~	~~Each DP or TOP that experiences the Impact Event~~	~~Firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)~~	~~Within 1 hour after event is initiated~~
~~Voltage Deviations on BES Facilities~~	~~Each RC, TOP, GOP that experiences the Impact Event~~	~~± 10% sustained for ≥ 15 continuous minutes~~	~~Within 24 hours after 15 minute threshold~~
~~IROL Violation~~	~~Each RC, TOP that experiences the Impact Event~~	~~Operate outside the IROL for time greater than IROL Tv~~	~~Within 24 hours after Tv threshold~~
~~Loss of Firm load for ≥ 15 Minutes~~	~~Each RC, BA, TOP, DP that experiences the Impact Event~~	~~• ≥ 300 MW for entities with previous year's demand ≥ 3000 MW~~ ~~• ≥ 200 MW for all other entities~~	~~Within 1 hour after 15 minute threshold~~
~~System Separation~~	~~Each RC, BA, TOP, DP that~~	~~Each separation resulting in an island of~~	~~Within 1 hour after occurrence is~~

~~EOP-004 – Attachment 1 - Actual Reliability Impact – Part A~~			
~~Event~~	~~Entity with Reporting Responsibility~~	~~Threshold for Reporting~~	~~Time to Submit Report~~
~~(Islanding)~~	~~experiences the Impact Event~~	~~generation and load ≥ 100 MW~~	~~identified~~
~~Generation loss~~	~~Each RC, BA, GOP that experiences the Impact Event~~	~~• ≥ 2,000 MW for entities in the Eastern or Western Interconnection~~ ~~• ≥ 1000 MW for entities in the ERCOT or Quebec Interconnection~~	~~Within 24 hours after occurrence~~
~~Loss of Off-site power to a nuclear generating plant (grid supply)~~	~~Each RC, BA, TO, TOP, GO, GOP that experiences the Impact Event~~	~~Affecting a nuclear generating station per the Nuclear Plant Interface Requirement~~	~~Report within 24 hours after occurrence~~
~~Transmission loss~~	~~Each RC, TOP that experiences the Impact Event~~	~~Three or more BES Transmission Elements~~	~~Within 24 hours after occurrence~~
~~Damage or destruction of BES equipment[1]~~	~~Each RC, BA, TO, TOP, GO, GOP, DP that experiences the Impact Event~~	~~Through operational error, equipment failure, external cause, or intentional or unintentional human action.~~	~~Within 1 hour after occurrence is identified~~
~~Damage or destruction of Critical Asset~~	~~Applicable Entities under CIP-002 or its successor.~~	~~Through operational error, equipment failure, external cause, or intentional or unintentional human action.~~	~~Within 1 hour after occurrence is identified~~
~~Damage or destruction of a Critical Cyber Asset~~	~~Applicable Entities under CIP-002 or its successor.~~	~~Through intentional or unintentional human action.~~	~~Within 1 hour after occurrence is identified~~

~~[1]BES equipment that: i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii) Damaged or destroyed due to intentional or unintentional human action; or iv) Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly e.g., removal of grounding straps rendering protective relaying inoperative.~~

~~EOP-004 – Attachment 1 – Potential Reliability Impact – Part B~~			
~~Event~~	~~Entity with Reporting Responsibility~~	~~Threshold for Reporting~~	~~Time to Submit Report~~
~~Unplanned Control Center evacuation~~	~~Each RC, BA, TOP that experiences the potential Impact Event~~	~~Unplanned evacuation from BES control center facility~~	~~Report within 24 hour after occurrence~~
~~Fuel supply emergency~~	~~Each RC, BA, GO, GOP that experiences the potential Impact Event~~	~~Affecting BES reliability~~[2]	~~Report within 1 hour after occurrence~~
~~Loss of all monitoring or voice communication capability~~	~~Each RC, BA, TOP that experiences the potential Impact Event~~	~~Affecting a BES control center for ≥ 30 continuous minutes~~	~~Report within 24 hours after occurrence~~
~~Forced intrusion~~[3]	~~Each RC, BA, TO, TOP, GO, GOP that experiences the potential Impact Event~~	~~At a BES facility~~	~~Report within 1 hour after verification of intrusion~~

[2] ~~Report if problems with the fuel supply chain result in the projected need for emergency actions to manage reliability.~~

[3] ~~Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects the reliability of the BES).~~

~~Risk to BES equipment~~[4]	~~Each RC, BA, TO, TOP, GO, GOP, DP that experiences the potential Impact Event~~	~~From a non-environmental physical threat~~	~~Report within 1 hour after identification~~
~~Detection of a reportable Cyber Security Incident.~~	~~Each RC, BA, TO, TOP, GO, GOP, DP that experiences the potential Impact Event~~	~~That meets the criteria in CIP-008 (or its successor)~~	~~Report within 1 hour after detection~~

[4] ~~Examples include a train derailment adjacent to BES equipment, that either could have damaged the equipment directly or has the potential to damage the equipment (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center) and report of suspicious device near BES equipment).~~

EOP-004 - Attachment 2: Impact Event Reporting Form

This form is to be used to report Impact Events Reports to the ERO. NERC will accept the DOE-OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Reports should be submitted viato one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422.

Attachment 1 - Reportable Events				
Event	Entity with Reporting Responsibility	Impact Event Threshold for Reporting for EOP-004-2	Submit Attachment 2 or DOE-OE-417 Report to:	
	Task	Comments		
1. Destruction of BES equipment[5]	Entity filing the report (include company name and Compliance Registration ID number):Each RC, BA, TO, TOP, GO, GOP, DP that experiences the destruction of BES equipment	Initial indication the event was due to operational error, equipment failure, external cause, or intentional or unintentional human action.	The parties identified pursuant to R1.3 within 1 hour of recognition of event.	
2. Damage or destruction of Critical Asset per	Applicable Entities under CIP-002	Initial indication the event was due to operational error, equipment failure, external	Date and Time of Impact Event.	

[5]BES equipment that: i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii) Damaged or destroyed due to intentional or unintentional human action which removes the BES equipment from service. Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative).

Attachment 1 - Reportable Events				
Event	Entity with Reporting Responsibility	Impact Event Threshold for Reporting for EOP-004-2	Submit Attachment 2 or DOE OE-417 Report to:	
Task		Comments		
CIP-002		cause, or intentional or unintentional human action.	Date: (mm/dd/yyyy) Time/Zone:The parties identified pursuant to R1.3 within 1 hour of recognition of event.	
3. Damage or destruction of a Critical Cyber Asset per CIP-002	Applicable Entities under CIP-002.	Through intentional or unintentional human action.	Name of contact person: Email address: Telephone Number:The parties identified pursuant to R1.3 within 1 hour of recognition of event.	
4. Forced intrusion[6]	Did the actual or potential Impact Event originate in your system?Each RC, BA, TO, TOP, GO, GOP that experiences the forced intrusion	Actual Impact Event ☐ Potential Impact Event ☐ Yes ☐ No☐ Unknown ☐At a BES facility	The parties identified pursuant to R1.3 within 1 hour of recognition of event.	

[6] Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects the reliability of the BES).

Attachment 1 - Reportable Events				
Event	Entity with Reporting Responsibility	Impact Event Threshold for Reporting for EOP-004-2	Submit Attachment 2 or DOE OE-417 Report to:	
	Task	Comments		
5. Risk to BES equipment[7]	Under which NERC function are you reporting? (RC, TOP, BA, other)Each RC, BA, TO, TOP, GO, GOP, DP that experiences the risk to BES equipment	From a non-environmental physical threat	The parties identified pursuant to R1.3 within 1 hour of recognition of event.	
6. Detection of a reportable Cyber Security Incident.	Each RC, BA, TO, TOP, GO, GOP, DP, ERO or RE that experiences the Cyber Security Incident	That meets the criteria in CIP-008	Brief Description of actual or potential Impact Event: (More detail should be provided in the Sequence of Events section below.)The parties identified pursuant to R1.3 within 1 hour of recognition of event.	

[7] Examples include a train derailment adjacent to BES equipment that either could have damaged the equipment directly or has the potential to damage the equipment (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center) and report of suspicious device near BES equipment.

Attachment 1 - Reportable Events				
Event	Entity with Reporting Responsibility	Impact Event Threshold for Reporting for EOP-004-2	Submit Attachment 2 or DOE OE-417 Report to:	
	Task	Comments		
7.	Generation tripped off-line*. MW Total List units tripped			
8. BES Emergency requiring public appeal for load reduction	Deficient entity is responsible for reporting	Each public appeal for load reduction	Frequency*. Just prior to Impact Event (Hz): Immediately after Impact Event (Hz max): Immediately after Impact Event (Hz min):The parties identified pursuant to R1.3 within 24 hours of recognition of the event.	
9. BES Emergency requiring system-wide voltage reduction	Initiating entity is responsible for reporting	List transmission facilities (lines, transformers, buses, etc.) tripped and locked-out*. (SpecifySystem wide voltage levelreduction of each facility listed).3% or	-The parties identified pursuant to R.1.3 within 24 hours of recognition of the event.	

Attachment 1 - Reportable Events			
Event	Entity with Reporting Responsibility	Impact Event Threshold for Reporting for EOP-004-2	Submit Attachment 2 or DOE OE-417 Report to:

	Task	Comments

		more	
10. BES Emergency requiring manual firm load shedding	Demand tripped (MW)*: Number of affected customers*: Demand lost (MW-Minutes)*:Initiating entity is responsible for reporting	FIRMManual firm load shedding ≥ 100 MW	INTERRUPTIBLEThe parties identified pursuant to R1.3 within 24 hours of recognition of the event.

11.			
12.			
13.			

Attachment 1 - Reportable Events			
Event	Entity with Reporting Responsibility	Impact Event Threshold for Reporting for EOP-004-2	Submit Attachment 2 or DOE OE-417 Report to:

	Task	Comments	
14.	Restoration Time*.	INITIAL	FINAL
	Transmission:		
	Generation:		
	Demand:		

15. BES Emergency resulting in automatic firm load shedding	Each DP or TOP that experiences the automatic load shedding	Sequence of Events of actual or potential Impact Event (if potential Impact Event, please describe your assessment of potential impact to BES) :	The parties identified pursuant to R1.3 within 24 hours of recognition of the event.

Attachment 1 - Reportable Events			
Event	Entity with Reporting Responsibility	Impact Event Threshold for Reporting for EOP-004-2	Submit Attachment 2 or DOE OE-417 Report to:
	Task	Comments	
		Firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)	
Voltage deviations on BES Facilities	Each TOP that experiences the voltage deviation	± 10% sustained for ≥ 15 continuous minutes	The parties identified pursuant to R1.3 within 24 hours after 15 minutes of exceeding the threshold.
16. IROL Violation (all Interconnections) or SOL Violation (WECC only)	Each RC that experiences the IROL Violation (all Interconnections) or SOL violation (WECC only)	Identify the initial probable cause or known root cause of the actual or potential Impact Event if known at time of submittal of Part I of this report: Operate outside the IROL for time greater than IROL Tv (all Interconnections) or Operate outside the SOL for	The parties identified pursuant to R1.3 within 24 hours after exceeding the Tv threshold.

Attachment 1 - Reportable Events			
Event	Entity with Reporting Responsibility	Impact Event Threshold for Reporting for EOP-004-2	Submit Attachment 2 or DOE OE-417 Report to:
Task		Comments	
		a time greater than the SOL Tv (WECC only).	
Loss of Firm load for ≥ 15 Minutes	Each BA, TOP, DP that experiences the loss of firm load	• ≥ 300 MW for entities wit demand ≥ 3000 MW • ≥ 200 MW for all other entities	The parties identified pursuant to R1.3 the entity's within 24 hours exceeding the 15 minute threshold
17. System Separation (Islanding)	Identify any protection system misoperation(s)[8]: Each RC, BA, TOP, DP that experiences the system separation	Each separation resulting in an island of generation and load ≥ 100 MW	The parties identified pursuant to R1.3 within 24 hours after occurrence is identified
Generation loss	Each BA, GOP that experiences the generation loss	• ≥ 2,000 MW for entities in the Eastern or Western Interconnection • ≥ 1000 MW for entities in the ERCOT or Quebec Interconnection	The parties identified pursuant to R1.3within 24 hours after occurrence.
Loss of Off-site	Each TO, TOP that	Affecting a nuclear	The parties identified pursuant to R1.3 within 24 hours after

[8] Only applicable if it is part of the impact event the responsible entity is reporting on

Attachment 1 - Reportable Events			
Event	Entity with Reporting Responsibility	Impact Event Threshold for Reporting for EOP-004-2	Submit Attachment 2 or DOE OE-417 Report to:
Task		Comments	
power to a nuclear generating plant (grid supply)	experiences the loss of off-site power to a nuclear generating plant	generating station per the Nuclear Plant Interface Requirement	occurrence
Transmission loss	Each TOP that experiences the transmission loss	Unintentional loss of Three or more Transmission Facilities (excluding successful automatic reclosing)	The parties identified pursuant to R1.3 within 24 hours after occurrence
Unplanned Control Center evacuation	Each RC, BA, TOP that experiences the potential event	Unplanned evacuation from BES control center facility	The parties identified pursuant to R1.3 within 24 hours of recognition of event.
18. Loss of monitoring or all voice communication capability	Additional InformationEach RC, BA, TOP that helps to further explain experiences the actual loss of monitoring or potential Impact Event if needed. all voice communication	Voice Communications: Affecting a BES control center for ≥ 30 continuous minutes Monitoring: Affecting a BES control center for ≥ 30 continuous minutes such that analysis tools (State Estimator, Contingency Analysis) are rendered inoperable.	The parties identified pursuant to R1.3 within 24 hours of recognition of event.

~~Attachment 1 - Reportable Events~~			
~~Event~~	~~Entity with Reporting Responsibility~~	Impact Event ~~Threshold for~~ Reporting for EOP-004-2	~~Submit Attachment 2 or DOE OE-417 Report to:~~
	~~Task~~	~~Comments~~	
	capability		

EOP-004 - Attachment 2: Event Reporting Form

EOP-004, Attachment 2: Event Reporting Form

This form is to be used to report events to parties listed in Attachment 1, column labeled "Submit Attachment 2 or DOE OE-417 Report to:". These parties will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Reports should be submitted via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422.

	Task	Comments
1.	Entity filing the report include: Company name: Name of contact person: Email address of contact person: Telephone Number: Submitted by (name):	
2.	Date and Time of recognized event. Date: (mm/dd/yyyy) Time: (hh:mm) Time/Zone:	
3.	Did the actual or potential event originate in your system?	Actual event ☐ Potential event ☐ Yes ☐ No☐ Unknown ☐
4.	**Event Identification and Description:**	
	(Check applicable box) ☐ public appeal ☐ voltage reduction ☐ manual firm load shedding ☐ firm load shedding(undervoltage, underfrequency, SPS/RAS) ☐ voltage deviation ☐ IROL violation	Written description (optional unless Other is checked):

EOP-004, Attachment 2: Event Reporting Form

This form is to be used to report events to parties listed in Attachment 1, column labeled "Submit Attachment 2 or DOE OE-417 Report to:". These parties will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Reports should be submitted via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422.

Task		Comments
	☐ loss of firm load ☐ system separation(islanding) ☐ generation loss ☐ loss of off-site power to nuclear generating plant ☐ transmission loss ☐ damage or destruction of BES equipment ☐ damage or destruction of Critical Asset ☐ damage or destruction of Critical Cyber Asset ☐ unplanned control center evacuation ☐ fuel supply emergency ☐ loss of all monitoring or voice communication capability ☐ forced intrusion Risk to BES equipment ☐ reportable Cyber Security Incident ☐ other	

Guideline and Technical Basis

Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01) - Reporting Concepts

Introduction

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and ~~is progressing toward developing standards based on the SAR. This concepts paper is designed to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed.~~has developed updated standards based on the SAR.

The standards listed under the SAR are:

- CIP-001 — Sabotage Reporting
- EOP-004 — Disturbance Reporting

~~The DSR SDT also proposed to investigate incorporation of the cyber incident reporting aspects of CIP-008 under this project. This will be coordinated with the Cyber Security - Order 706 SDT (Project 2008-06).~~

~~The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC database and FERC Order 693 Directives to determine a prudent course of action with respect to these standards.~~

~~This concept paper provides stakeholders with a proposed "road map" that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. This concept paper provides the background information and thought process of the DSR SDT.~~

~~The proposed~~The changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). ~~The proposed standards deal~~These standard deals exclusively with after-the-fact reporting.

The DSR SDT ~~is proposing to consolidate~~has consolidated disturbance and sabotage event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts and Assumptions:

The Standard ~~***Will:*** Require use~~***:***

- Requires reporting of ~~a single form to report disturbances and "Impact Events~~"events" that ~~threaten~~impact or may impact the reliability of the bulk electric system
- ~~Provide~~Provides clear criteria for reporting
- ~~Include~~Includes consistent reporting timelines
- ~~Identify~~Identifies appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- ~~Provide~~Provides clarity around of who will receive the information

~~The drafting team will explore other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements~~

Discussion of Disturbance Reporting

Disturbance reporting requirements ~~currently exist~~existed in the previous version of EOP-004. The current approved definition of Disturbance from the NERC Glossary of Terms is:

1. An unplanned event that produces an abnormal system condition.
2. Any perturbation to the electric system.
3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.

Disturbance reporting requirements and criteria ~~are~~were in the ~~existing~~previous EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and developed the list of ~~Impact Events~~events that are to be reported under this standard (attachment 1).

Discussion of ~~"Impact~~ Event~~"~~ Reporting

There are situations worthy of reporting because they have the potential to impact reliability. ~~The DSR SDT proposes calling such incidents 'Impact Events' with the following concept:~~

> ~~An Impact Event is any situation that has the potential to significantly impact the reliability of the Bulk Electric System. Such events may originate from malicious intent, accidental behavior, or natural occurrences.~~

~~Impact~~t Event reporting facilitates industry awareness, which allows potentially impacted parties to prepare for and possibly mitigate ~~the~~any associated reliability risk. It also provides the raw material, in the case of certain potential reliability threats, to see emerging patterns.

Examples of ~~Impact Events~~such events include:

- Bolts removed from transmission line structures
- Detection of cyber intrusion that meets criteria of CIP-008 or its successor standard
- Forced intrusion attempt at a substation

- Train derailment near a transmission right-of-way
- Destruction of Bulk Electrical System equipment

What about sabotage?
One thing became clear in the DSR SDT's discussion concerning sabotage: everyone has a different definition. The current standard CIP-001 elicited the following response from FERC in FERC Order 693, paragraph 471 which states in part: *". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."*

Often, the underlying reason for an event is unknown or cannot be confirmed. The DSR SDT believes that by reporting material risks to the Bulk Electrical System using the ~~Impact Event~~event categorization in this standard, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.

~~The DST SDT discussed the reliability needs for Impact Event reporting and will consider guidance found in the document "NERC Guideline: Threat and Incident Reporting" in the development of requirements, which will include clear criteria for reporting.~~

Certain types of ~~Impact Events~~events should be reported to NERC, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and/or Provincial or local law enforcement. Other types of ~~Impact Events~~impact events may have different reporting requirements. For example, an ~~Impact Event~~event that is related to copper theft may only need to be reported to the local law enforcement authorities.

Potential Uses of Reportable Information
Event analysis, correlation of data, and trend identification are a few potential uses for the information reported under this standard. ~~As envisioned, the~~The standard ~~will only require~~requires Functional entities to report the incidents and provide known information ~~or~~at the time of the report. Further data gathering necessary for ~~these analyses~~event analysis is provided for under the Events Analysis Program and the NERC Rules of Procedure. Other entities (e.g. – NERC, Law Enforcement, etc) will be responsible for performing the analyses. The NERC Rules of Procedure (section 800) provide an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for reliability. Jurisdictional agencies (which may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE) have other duties and responsibilities.

Collection of Reportable Information or "One stop shopping"
~~The goal of the DSR SDT is to have one reporting form for all functional entities (US, Canada, Mexico) to submit to NERC. Ultimately, it may make sense to develop an electronic version to expedite completion, sharing and storage. Ideally, entities would complete a single form which could then be distributed to jurisdictional agencies and functional entities as appropriate.~~

~~Specific reporting forms[9] that exist today (i.e. - OE-417, etc) could be included as part of the electronic form to accommodate US entities with a requirement to submit the form, or may be removed (but still be mandatory for US entities under Public Law 93-275) to streamline the proposed consolidated reliability standard for all North American entities (US, Canada, Mexico). Jurisdictional agencies may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE. Functional entities may include the RC, TOP, and BA for industry awareness. Applicability of the standard will be determined based on the specific requirements.~~

The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT ~~is planning to update~~has updated the listing of reportable events ~~from~~in Attachment 1 based on discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences ~~may~~ still exist.

The reporting ~~proposed~~required by ~~the DSR SDT~~this standard is intended to meet the uses and purposes of NERC. The DSR SDT recognizes that other requirements for reporting exist (e.g., DOE-417 reporting), which may duplicate or overlap the information required by NERC. To the extent that other reporting is required, the DSR SDT envisions that duplicate entry of information ~~is~~should not be necessary, and the submission of the alternate report will be acceptable to NERC so long as all information required by NERC is submitted. For example, if the NERC Report duplicates information from the DOE form, the DOE report may be included or attached to the NERC report, in lieu of entering that information on the NERC report.

~~[9] The DOE Reporting Form, OE-417 is currently a part of the EOP-004 standard. If this report is removed from the standard, it should be noted that this form is still required by law as noted on the form: NOTICE: This report is mandatory under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. Title 18 USC 1001 makes it a criminal offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction.~~

Unofficial Comment Form

Disturbance and Sabotage Reporting (Project 2009-01)

Please **DO NOT** use this form to submit comments. Please use the electronic comment form to submit comments on the first formal posting for Project 2009-01—Disturbance and Sabotage Reporting. The electronic comment form must be completed by **December 12, 2011.**

2009-01 Project Page

If you have questions please contact Stephen Crutchfield at stephen.crutchfield@nerc.net or by telephone at 609-651-9455.

Background

The DST SDT posted the draft standard EOP-004-2 for a formal comment period from March 9, 2011 through April 8, 2011. Based on stakeholder feedback, the DSR SDT made several revisions to the standard to improve clarity and address other concerns identified by stakeholders. The main stakeholder concerns were addressed as follows:

Definition of Impact Event. Many stakeholders disagreed with the need for the definition of "Impact Event" and felt that that the definition was ambiguous and created confusion. The DSR SDT agrees and has deleted the proposed definition from the standard. The list of events that are to be reported in Attachment 1 is inclusive and no further attempts to define "Impact Event" are necessary.

Timeframe for Reporting and Event. Many stakeholders raised concerns with the one-hour reporting requirement for certain types of events. The commenters believed that the restoration of service or the return to a stable bulk power system state may be jeopardized by having to report certain events within one hour. The DSR SDT agreed and revised the reporting time to 24 hours for most events, with the exception of damage to or destruction of BES equipment, forced intrusion or cyber related incidents.

VRFs. Many stakeholders suggested that the reporting of events after the fact only justified a VRF of "lower" for each requirement. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment A. This is procedural in nature and justifies a "lower" VRF, as this requirement deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis of reported events is addressed through the NERC Events Analysis Program in accordance with the NERC Rules of Procedure.

The three remaining requirements in EOP-004-2 require entities affected by events to report those events based on the specifics in Attachment A (Requirement R3) and to test the communications protocol of their Operating Plan once per year (R4). Requirement R2 provides for implementation of the Operating Plan as it relates to Requirement R1, Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 specifies that an entity is responsible for reporting events to the appropriate entities in accordance with the Operating Plan based on Attachment A. Requirement R4 is intended to ensure that an entity can communicate information about events. Some of these events are potential sabotage events, and communicating these events is intended to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events,

and the approved VRFs for each of the requirements is "medium." The proposed VRFs for EOP-004-2 are consistent with the existing approved VRFs for both EOP-004 and CIP-001.

Applicability. Commenters also had concerns about the applicability of the standard to Load Serving Entities, who may not own physical assets, as well as to the ERO and Regional Entity. The DSR SDT agrees that the Distribution Provider owns the assets per the Functional Model, however the LSE is an applicable entity under CIP-002, and under the CIP standards is responsible for reporting cyber security incidents. The ERO and RE are also responsible for reporting cyber security incidents under CIP-002. Therefore, the SDT determined that it was appropriate to include LSEs, the ERO and the RE in the applicability of EOP-004-2.

After the drafting team completed its consideration of stakeholder comments, the standards and implementation plan were submitted for quality review. Based on feedback from the quality review, the drafting team has made two significant revisions to the standard. The first revision is to add a requirement for implementation of the Operating Plan listed in Requirement R1. There was only a requirement to report events, but no requirement specifically calling for updates to the Operating Plan or the annual review. This was accomplished by having two requirements. The first is Requirement R2 which specifies that an entity must implement the Operating Plan per Requirement R1, Parts 1.1, 1.2, 1.4 and 1.5:

> R2. Each Responsible Entity shall implement the parts of its Operating Plan that meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts 1.4 and 1.5 as specified.

The second Requirement is R3 which addresses Part 1.3:

> R3. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.

The second revision based on the quality review pertains to Requirement R4. The quality review suggested revising the requirement to more closely match the language in the Rationale box that the drafting team developed. This would provide better guidance for responsible entities as well as provide more clear direction to auditors. The revised requirement is:

> R4. Each Responsible Entity shall verify (through actual implementation for an event, or through a drill or exercise) the communication process in its Operating Plan, created pursuant to Requirement 1, Part 1.3, at least annually (once per calendar year), with no more than 15 calendar months between verification or actual implementation.

You do not have to answer all questions. Enter all comments in Simple Text Format.

1. **The DSR SDT has revised EOP-004-2 to remove the training requirement R4 based on stakeholder comments from the second formal posting. Do you agree this revision? If not, please explain in the comment area below.**

   ☐ Yes

   ☐ No

   Comments:

2. **The DSR SDT includes two requirement regarding implementation of the Operating Plan specified in Requirement R1. The previous version of the standard had a requirement to implement the Operating plan as well as a requirement to report events. The two requirements R2 and R3 were written to delineate implementation of the Parts of R1. Do you agree with these revisions? If not, please explain in the comment area below.**

   R2. Each Responsible Entity shall implement the parts of its Operating Plan that meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts 1.4 and 1.5 as specified.

   R3. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.

   ☐ Yes

   ☐ No

   Comments:

3. **The DSR SDT revised reporting times for many events listed in Attachment 1 from one hour to 24 hours. Do you agree with these revisions? If not, please explain in the comment area below.**

   ☐ Yes

   ☐ No

   Comments:

4. **Do you have any other comment, not expressed in questions above, for the DSR SDT?**

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2009-01 Disturbance and Sabotage Reporting

Implementation Plan for EOP-004-2 – Event Reporting

Approvals Required

EOP-004-2 – Event Reporting

Prerequisite Approvals

Revisions to Sections 807 and 808 of the NERC Rules of Procedure
Addition of Section 812 to the NERC Rules of Procedure

Revisions to Glossary Terms

None

Applicable Entities

Reliability Coordinator
Balancing Authority
Interchange Coordinator
Transmission Service provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Distribution Provider
Load-Serving Entity
Electric Reliability Organization
Regional Entity

Conforming Changes to Other Standards

None

Effective Dates

EOP-004-2 shall become effective on the first day of the third calendar quarter after applicable regulatory approval. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the third calendar quarter after Board of Trustees approval.

Retirements

EOP-004-1 – Disturbance Reporting and CIP-001-2a – Sabotage Reporting should be retired at midnight of the day immediately prior to the Effective Date of EOP-004-2 in the particular jurisdiction in which the new standard is becoming effective.

CIP-008-4 – Cyber Security - Incident Reporting and Response Planning: Retire R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in EOP-004-2, Requirement 1, Part 1.3.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2009-01 Disturbance and Sabotage Reporting

Implementation Plan for EOP-004-2 – Event Reporting

Approvals Required

EOP-004-2 – Event Reporting

Prerequisite Approvals

Revisions to Sections 807 and 808 of the NERC Rules of Procedure
Addition of Section 812 to the NERC Rules of Procedure

Revisions to Glossary Terms

None

Applicable Entities

Reliability Coordinator
Balancing Authority
Interchange Coordinator
Transmission Service provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Distribution Provider
Load-Serving Entity
Electric Reliability Organization
Regional Entity

Conforming Changes to Other Standards

None

Effective Dates

EOP-004-2 shall become effective on the first day of the third calendar quarter after applicable regulatory approval. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the third calendar quarter after Board of Trustees approval.

Retirements

EOP-004-1 – Disturbance Reporting and CIP-001-2a – Sabotage Reporting should be retired at midnight of the day immediately prior to the Effective Date of EOP-004-2 in the particular jurisdiction in which the new standard is becoming effective.

CIP-008-4 – Cyber Security - Incident Reporting and Response Planning: Retire R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in EOP-004-2, Requirement 1, Part 1.3.

Project 2009-01 Disturbance and Sabotage Reporting Mapping Document

Translation of CIP-002-2a – Sabotage Reporting, EOP-004-1 – Disturbance Reporting and CIP-008-4 – Cyber Security – Incident Reporting and Response Planning (R 1.3), into EOP-004-2 – Impact Event and Disturbance Assessment, Analysis, and Reporting

Standard: CIP-001-2a – Sabotage Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting**
R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.	Moved into EOP-004-2, R1	R1. Each Responsible Entity shall have an Operating Plan that includes: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* 1.1. A process for identifying events listed in Attachment 1. 1.2. A process for gathering information for Attachment 2 regarding events listed in Attachment 1. 1.3. A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate: • Internal company personnel • The Responsible Entities' Regional Entity

		• Law enforcement • Governmental or provincial agencies 1.4. Provision(s) for updating the Operating Plan within 90 calendar days of any change in assets, personnel, other circumstances that may no longer align with the plan or incorporating lessons learned pursuant to Requirement R3. 1.5. Process for ensuring the responsible entity reviews the Operating Plan at least annually (once each calendar year) with no more than 15 months between reviews.
R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	Moved into EOP-004-2, R1	R1. Each Responsible Entity shall have an Operating Plan that includes: [Violation Risk: Factor: Lower] [Time Horizon: Operations Planning] 1.1. A process for identifying events listed in Attachment 1. 1.2. A process for gathering information for Attachment 2 regarding events listed in Attachment 1. 1.3. A process for communicating events listed in Attachment 1 that includes the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate: • Internal company personnel

		• The Responsible Entities' Regional Entity • Law enforcement • Governmental or provincial agencies 1.4. Provision(s) for updating the Operating Plan within 90 calendar days of any change in assets, personnel, other circumstances that may no longer align with the plan or incorporating lessons learned pursuant to R3. 1.5. Process for ensuring the responsible entity reviews the Operating Plan at least annually (once each calendar year) with no more than 15 months between reviews.
R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.	Moved into EOP-004-2, R1	R1. Each Responsible Entity shall have an Operating Plan that includes: [Violation Risk: Factor: Lower] [Time Horizon: Operations Planning] 1.1. A process for identifying events listed in Attachment 1. 1.2. A process for gathering information for Attachment 2 regarding events listed in Attachment 1. 1.3. A process for communicating events listed in Attachment 1 that includes the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate: • Internal company personnel

		• Responsible Entities' Regional Entity • Law enforcement • Governmental or provincial agencies 1.4. Provision(s) for updating the Operating Plan within 90 calendar days of any change in assets, personnel, other circumstances that may no longer align with the plan or incorporating lessons learned pursuant to R3. 1.5. Process for ensuring the responsible entity reviews the Operating Plan at least annually (once each calendar year) with no more than 15 months between reviews.
R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.	Moved into EOP-004-2, R1	R1. Each Responsible Entity shall have an Operating Plan that includes: [Violation Risk: Factor: Lower] [Time Horizon: Operations Planning] 1.1. A process for identifying events listed in Attachment 1. 1.2. A process for gathering information for Attachment 2 regarding events listed in Attachment 1. 1.3. A process for communicating events listed in Attachment 1 that includes the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate: • Internal company personnel

		• Responsible Entities' Regional Entity • Law enforcement • Governmental or provincial agencies 1.4. Provision(s) for updating the Operating Plan within 90 calendar days of any change in assets, personnel, other circumstances that may no longer align with the plan or incorporating lessons learned pursuant to R3. 1.5. Process for ensuring the responsible entity reviews the Operating Plan at least annually (once each calendar year) with no more than 15 months between reviews.

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting Comments**
R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.	Retire this fill-in-the-blank requirement. Replace with new reporting and analysis procedure developed by NERC EAWG.	The requirements of EOP-004-2 specify that an entity must report certain types of impact events. The NERC EAWG is developing continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure.
R2. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.	Translated into EOP-004-2, R1 and the NERC Events Analysis Process	The requirements of EOP-004-2 specify that an entity must report certain types of impact events. The NERC EAWG is developing continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure.
R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.	Translated into EOP-004-2, R3	R3. Each Responsible Entity shall report impact events in accordance with the Operating Plan developed to address events listed in Attachment 1. *[Violation Risk: Factor: Lower] [Time Horizon: Operations Assessment].*

R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until sometime after they occur shall be reported within 24 hours of being recognized.	Translated into EOP-004-2, R3	R3. Each Responsible Entity shall report impact events in accordance with the Operating Plan developed to address events listed in Attachment 1. *[Violation Risk: Factor: Lower] [Time Horizon: Operations Assessment].*
R3.2. Applicable reporting forms are provided in Attachments 022-1 and 022-2.	Retire – informational statement	

R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.	Retire as a requirement. Added as a "Note" to EOP-004-Attachment1-Impact Events Table	NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per R1 and provide as much information as is available at the time of the notification. The affected Responsible Entity shall provide periodic verbal updates until adequate information is available to issue a written Event report. Reports to the ERO should be submitted to one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422.

R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.	Retire this fill-in-the-blank requirement. Replace with new reporting procedure developed by NERC EAWG.	The requirements of EOP-004-2 specify that an entity must report certain types of impact events. The NERC EAWG is developing continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure.
R4. When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.	Retire this fill-in-the-blank requirement. Replace with new reporting procedure developed by NERC EAWG.	The requirements of EOP-004-2 specify that an entity must report certain types of impact events. The NERC EAWG is developing continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure.

R5. The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.	Retire this fill-in-the-blank requirement. Replace with new reporting procedure developed by NERC EAWG.	The requirements of EOP-004-2 specify that an entity must report certain types of impact events. The NERC EAWG is developing continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure.
Request for Interpretation of CIP-001-2a, R2: Please clarify what is meant by the term, "appropriate parties." Moreover, who within the Interconnection hierarchy deems parties to be appropriate?	Retire the interpretation	Addressed in EOP-004-2, R1 by replacing the term, 'appropriate parties' with a broader, more specific list of specific entities to contact in Part 1.3.

Standard: CIP-008-4 – Cyber Security – Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting Comments**
R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.	Translated into EOP-004-2 Requirement 1, Part 1.3 and Attachment 1.	Cyber Security Incidents are defined as: Any malicious act or suspicious event that: • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset. Such events are listed in Attachment 1 as "Detection of a reportable Cyber Security Incident" and are events that are required to be reported under Reliability Standard EOP-004-2. Requirement R1, Part 1.3 requires the Responsible Entity to have "A process for communicating events listed in Attachment 1 to the Electric Reliability Organization,..." The note at the top of Attachment 1 includes the following: "Reports to the ERO should be submitted to one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422."

Violation Risk Factor and Violation Severity Level Assignments

Project 2009-01 – Disturbance and Sabotage Reporting

This document provides the drafting team's justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in

EOP-004-2 — Event Reporting

Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the ERO Sanction Guidelines.

Justification for Assignment of Violation Risk Factors in EOP-004-2

The Disturbance and Sabotage Reporting Standard Drafting Team applied the following NERC criteria when proposing VRFs for the requirements in EOP-004-2:

High Risk Requirement
A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement
A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

The SDT also considered consistency with the FERC Violation Risk Factor Guidelines for setting VRFs:[1]

Guideline (1) — Consistency with the Conclusions of the Final Blackout Report
The Commission seeks to ensure that Violation Risk Factors assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System.

In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:[2]

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) — Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement Violation Risk Factor assignments and the main Requirement Violation Risk Factor assignment.

[1] North American Electric Reliability Corp., 119 FERC ¶ 61,145, order on reh'g and compliance filing, 120 FERC ¶ 61,145 (2007) ("VRF Rehearing Order").
[2] Id. at footnote 15.

Guideline (3) — Consistency among Reliability Standards

The Commission expects the assignment of Violation Risk Factors corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) — Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular Violation Risk Factor level conforms to NERC's definition of that risk level.

Guideline (5) — Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

The following discussion addresses how the SDT considered FERC's VRF Guidelines 2 through 5. The team did not address Guideline 1 directly because of an apparent conflict between Guidelines 1 and 4. Whereas Guideline 1 identifies a list of topics that encompass nearly all topics within NERC's Reliability Standards and implies that these requirements should be assigned a "High" VRF, Guideline 4 directs assignment of VRFs based on the impact of a specific requirement to the reliability of the system. The SDT believes that Guideline 4 is reflective of the intent of VRFs in the first instance and therefore concentrated its approach on the reliability impact of the requirements.

VRF for EOP-004-2:

There are four requirements in EOP-004-2. Requirement R1 was assigned a "Lower" VRF while Requirements R2, R3 and R4 were assigned a "Medium" VRF.

VRF for EOP-004-2, Requirements R1:

- FERC's Guideline 2 — Consistency within a Reliability Standard. The Requirement specifies which functional entities are required to have procedure(s) for recognition of events, gather information for completing an event report, and communicating with other entities. The VRFs are only applied at the Requirement level and each Requirement Part is treated equally.
- FERC's Guideline 3 — Consistency among Reliability Standards. This requirement calls for an entity to have procedure(s) for recognition of events, gather information for completing an event report, and communicating with other entities. This requirement is administrative in nature and deals with the means to report events after the fact. Most event reporting requirements in Attachment 1 are

for 24 hours after an event has occurred. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program.

- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. Failure to have a procedure(s) is not likely to directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system if an entity cannot report an event and that event led to other preventable events on the BES had the report been made in a timely fashion. Development of the procedure(s) is a requirement that is administrative in nature and is in a planning time frame that, if violated, would not, under emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system.. Therefore this requirement was assigned a lower VRF.
- FERC's Guideline 5 — Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R1 contain only one objective which is to have procedure(s). The content of the procedure is specified in Parts 1.1-1.5. Since the requirement is to have a procedure(s), only one VRF was assigned.

VRF for EOP-004-2, Requirement R2:

- FERC's Guideline 2 — Consistency within a Reliability Standard. The requirement has no sub-requirements; only one VRF was assigned so there is no conflict.
- FERC's Guideline 3 — Consistency among Reliability Standards. EOP-004-2, Requirement R4 is a requirement for entities to report events using the procedure(s) for recognition of events per Requirement R1. The Standard Drafting Team views this as an aspect of implementing the Operating Plan for reporting events. The act of reporting in and of itself is not likely to "directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system." However, violation of a medium risk requirement should also be "unlikely to lead to bulk electric system instability, separation, or cascading failures…" Such an instance could occur if personnel do not report events. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. EOP-004-2, Requirement R5 mandates that report events per their procedure(s). Bulk power system instability, separation, or cascading failures are not likely to occur due to a failure to notify another entity of the event failure, but there is a slight chance that it could occur. Therefore, this requirement was assigned a Medium VRF.

- FERC's Guideline 5 - Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R5 addresses a single objective and has a single VRF.

VRF for EOP-004-2, Requirement R3:

- FERC's Guideline 2 — Consistency within a Reliability Standard. The requirement has no sub-requirements; only one VRF was assigned so there is no conflict.
- FERC's Guideline 3 — Consistency among Reliability Standards. EOP-004-2, Requirement R4 is a requirement for entities to report events using the procedure(s) for recognition of events per Requirement R1. The act of reporting in and of itself is not likely to "directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system." However, violation of a medium risk requirement should also be "unlikely to lead to bulk electric system instability, separation, or cascading failures…" Such an instance could occur if personnel do not report events. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. EOP-004-2, Requirement R5 mandates that report events per their procedure(s). Bulk power system instability, separation, or cascading failures are not likely to occur due to a failure to notify another entity of the event failure, but there is a slight chance that it could occur. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 5 - Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R5 addresses a single objective and has a single VRF.

VRF for EOP-004-2, Requirement R4:

- FERC's Guideline 2 — Consistency within a Reliability Standard. The requirement has no sub-requirements; only one VRF was assigned so there is no conflict.
- FERC's Guideline 3 — Consistency among Reliability Standards. EOP-004-2, Requirement R3 specifies a time frame in which to verify the communications protocols developed in the procedures pursuant to Requirement R1. Both requirements have a Medium VRF.
- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. Failure to verify a communications protocol could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system if an entity cannot report an event and that event led to other preventable events on the BES had the report been made in a timely fashion. Therefore this requirement was assigned a medium VRF.
- FERC's Guideline 5 — Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R3 addresses a single objective and has a single VRF.

Justification for Assignment of Violation Severity Levels for EOP-004-2:

In developing the VSLs for the EOP-004-2 standard, the SDT anticipated the evidence that would be reviewed during an audit, and developed its VSLs based on the noncompliance an auditor may find during a typical audit. The SDT based its assignment of VSLs on the following NERC criteria:

Lower	Moderate	High	Severe
Missing a minor element (or a small percentage) of the required performance The performance or product measured has significant value as it almost meets the full intent of the requirement.	Missing at least one significant element (or a moderate percentage) of the required performance. The performance or product measured still has significant value in meeting the intent of the requirement.	Missing more than one significant element (or is missing a high percentage) of the required performance or is missing a single vital component. The performance or product has limited value in meeting the intent of the requirement.	Missing most or all of the significant elements (or a significant percentage) of the required performance. The performance measured does not meet the intent of the requirement or the product delivered cannot be used in meeting the intent of the requirement.

FERC's VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in EOP-004-2 meet the FERC Guidelines for assessing VSLs:

Guideline 1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

> Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline 2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

> A violation of a "binary" type requirement must be a "Severe" VSL.
>
> Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline 3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline 4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

. . . unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

NERC

VSLs for EOP-004-2 Requirements R1:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R1	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is a revision of CIP-001-1, R1-R4, and EOP-004-1, R2. Since the Requirement has four Parts, the VSLs were developed to count a violation of each Part equally. Therefore, four VSLs were developed.	The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSL uses the same terminology as used in the associated requirement, and is, therefore, consistent with the requirement.	The VSL is based on a single violation and not cumulative violations.

VSLs for EOP-004-2 Requirement R2:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R2.	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is for entities to implement the Operating Plan for event reporting. There are four Parts that are addressed under this requirement. Parts 1.1 and 1.2 are only applicable for an actual event and are binary in nature. Parts 1.4 and 1.5 require updates or reviews based on certain intervals. Based on the VSL Guidance, the DSR SDT developed four VSLs based on tardiness of the submittal of the report. If the update or review is not performed, then the VSL is Severe.	The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSL uses the same terminology as used in the associated requirement, and is, therefore, consistent with the requirement.	The VSL is based on a single violation and not cumulative violations.

VSLs for EOP-004-2 Requirement R3:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R2.	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is a revision of EOP-004-1, R3. There is only a Severe VSL for that requirement. However, the reporting of events is based on timing intervals listed in attachment 1. Based on the VSL Guidance, the DSR SDT developed four VSLs based on tardiness of the submittal of the report. If a report is not submitted, then the VSL is Severe. This maintains the current VSL.	The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSL uses the same terminology as used in the associated requirement, and is, therefore, consistent with the requirement.	The VSL is based on a single violation and not cumulative violations.

VSLs for EOP-004-2 Requirement R4:

R#	Compliance with NERC's Revised VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R3.	Meets NERC's VSL guidelines - Severe: The performance or product measured does not substantively meet the intent of the requirement.	The most comparable VSLs for a similar requirement is EOP-008-0, R1.7 which calls for an annual update to a plan. Based on the VSL Guidance, the DSR SDT developed four VSLs based on tardiness of the verification of the communication protocol. If the verification is not achieved, then the VSL is Severe.	The proposed VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSLs use the same terminology as used in the associated requirement, and are, therefore, consistent with the requirement.	The VSLs are based on a single violation and not cumulative violations.

A. Introduction

1. Title: **Sabotage Reporting**

2. Number: CIP-001-1

3. Purpose: Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.

4. Applicability

4.1. Reliability Coordinators.

4.2. Balancing Authorities.

4.3. Transmission Operators.

4.4. Generator Operators.

4.5. Load Serving Entities.

5. Effective Date: January 1, 2007

B. Requirements

R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.

R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

C. Measures

M1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement 1

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements 2 and 3.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to procedures, policies, a letter of understanding, communication records, or other equivalent evidence that will be used to confirm that it has established communications contacts with the applicable, local FBI or RCMP officials to communicate sabotage events (Requirement 4).

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organizations shall be responsible for compliance monitoring.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to verify compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Reliability Coordinator, Transmission Operator, Generator Operator, Distribution Provider, and Load Serving Entity shall have current, in-force documents available as evidence of compliance as specified in each of the Measures.

If an entity is found non-compliant the entity shall keep information related to the non-compliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

None.

2. **Levels of Non-Compliance:**

2.1. **Level 1:** There shall be a separate Level 1 non-compliance, for every one of the following requirements that is in violation:

2.1.1 Does not have procedures for the recognition of and for making its operating personnel aware of sabotage events (R1).

2.1.2 Does not have procedures or guidelines for the communication of information concerning sabotage events to appropriate parties in the Interconnection (R2).

2.1.3 Has not established communications contacts, as specified in R4.

2.2. **Level 2:** Not applicable.

2.3. **Level 3:** Has not provided its operating personnel with sabotage response procedures or guidelines (R3).

2.4. **Level 4:**.Not applicable.

E. **Regional Differences**

None indicated.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Amended

A. Introduction

1. Title: **Disturbance Reporting**

2. Number: EOP-004-1

3. Purpose: Disturbances or unusual occurrences that jeopardize the operation of the Bulk Electric System, or result in system equipment damage or customer interruptions, need to be studied and understood to minimize the likelihood of similar events in the future.

4. Applicability

4.1. Reliability Coordinators.

4.2. Balancing Authorities.

4.3. Transmission Operators.

4.4. Generator Operators.

4.5. Load Serving Entities.

4.6. Regional Reliability Organizations.

5. Effective Date: January 1, 2007

B. Requirements

R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.

R2. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.

R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.

R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.

R3.2. Applicable reporting forms are provided in Attachments 1-EOP-004 and 2-EOP-004.

R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that

time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.

R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.

R4. When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.

R5. The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.

C. Measures

M1. The Regional Reliability Organization shall have and provide upon request as evidence, its current regional reporting procedure that is used to facilitate preparation of preliminary and final disturbance reports. (Requirement 1)

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, the preliminary report, computer printouts, operator logs, or other equivalent evidence that will be used to confirm that it prepared and delivered the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that will be used to confirm that it provided information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours. (Requirement 3.3)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

NERC shall be responsible for compliance monitoring of the Regional Reliability Organizations.

Regional Reliability Organizations shall be responsible for compliance monitoring of Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load-serving Entities.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to assess compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Regional Reliability Organization shall have its current, in-force, regional reporting procedure as evidence of compliance. (Measure 1)

Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that is either involved in a Bulk Electric System disturbance or has a reportable incident shall keep data related to the incident for a year from the event or for the duration of any regional investigation, whichever is longer. (Measures 2 through 4)

If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

See Attachments:

- EOP-004 Disturbance Reporting Form
- Table 1 EOP-004

2. Levels of Non-Compliance for a Regional Reliability Organization

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: No current procedure to facilitate preparation of preliminary and final disturbance reports as specified in R1.

3. Levels of Non-Compliance for a Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load- Serving Entity:

3.1. Level 1: There shall be a level one non-compliance if any of the following conditions exist:

3.1.1 Failed to prepare and deliver the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1

3.1.2 Failed to provide disturbance information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours as specified in R3.3

3.1.3 Failed to prepare a final report within 60 days as specified in R3.4

3.2. Level 2: Not applicable.

3.3. Level 3: Not applicable

3.4. Level 4: Not applicable.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	May 23, 2005	Fixed reference to attachments 1-EOP-004-0 and 2-EOP-004-0, Changed chart title 1-FAC-004-0 to 1-EOP-004-0, Fixed title of Table 1 to read 1-EOP-004-0, and fixed font.	Errata
0	July 6, 2005	Fixed email in Attachment 1-EOP-004-0 from info@nerc.com to esisac@nerc.com.	Errata

0	July 26, 2005	Fixed Header on page 8 to read EOP-004-0	Errata
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised

Attachment 1-EOP-004
NERC Disturbance Report Form

Introduction

These disturbance reporting requirements apply to all Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load Serving Entities, and provide a common basis for all NERC disturbance reporting. The entity on whose system a reportable disturbance occurs shall notify NERC and its Regional Reliability Organization of the disturbance using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. Reports can be sent to NERC via email (esisac@nerc.com) by facsimile (609-452-9550) using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. If a disturbance is to be reported to the U.S. Department of Energy also, the responding entity may use the DOE reporting form when reporting to NERC. Note: All Emergency Incident and Disturbance Reports (Schedules 1 and 2) sent to DOE shall be simultaneously sent to NERC, preferably electronically at esisac@nerc.com.

The NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports are to be made for any of the following events:

1. The loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations. Generally, a disturbance report will be required if the event results in actions such as:
   a. Modification of operating procedures.
   b. Modification of equipment (e.g. control systems or special protection systems) to prevent reoccurrence of the event.
   c. Identification of valuable lessons learned.
   d. Identification of non-compliance with NERC standards or policies.
   e. Identification of a disturbance that is beyond recognized criteria, i.e. three-phase fault with breaker failure, etc.
   f. Frequency or voltage going below the under-frequency or under-voltage load shed points.
2. The occurrence of an interconnected system separation or system islanding or both.
3. Loss of generation by a Generator Operator, Balancing Authority, or Load-Serving Entity — 2,000 MW or more in the Eastern Interconnection or Western Interconnection and 1,000 MW or more in the ERCOT Interconnection.
4. Equipment failures/system operational actions which result in the loss of firm system demands for more than 15 minutes, as described below:
   a. Entities with a previous year recorded peak demand of more than 3,000 MW are required to report all such losses of firm demands totaling more than 300 MW.
   b. All other entities are required to report all such losses of firm demands totaling more than 200 MW or 50% of the total customers being supplied immediately prior to the incident, whichever is less.
5. Firm load shedding of 100 MW or more to maintain the continuity of the bulk electric system.

6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in:
   a. Sustained voltage excursions equal to or greater than ±10%, or
   b. Major damage to power system components, or
   c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance as defined by steps 1 through 5 above.
7. An Interconnection Reliability Operating Limit (IROL) violation as required in reliability standard TOP-007.
8. Any event that the Operating Committee requests to be submitted to Disturbance Analysis Working Group (DAWG) for review because of the nature of the disturbance and the insight and lessons the electricity supply and delivery industry could learn.

NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report

☐ Check here if this is an Interconnection Reliability Operating Limit (IROL) violation report.

1.	Organization filing report.		
2.	Name of person filing report.		
3.	Telephone number.		
4.	Date and time of disturbance. Date:(mm/dd/yy) Time/Zone:		
5.	Did the disturbance originate in your system?	Yes ☐ No ☐	
6.	Describe disturbance including: cause, equipment damage, critical services interrupted, system separation, key scheduled and actual flows prior to disturbance and in the case of a disturbance involving a special protection or remedial action scheme, what action is being taken to prevent recurrence.		
7.	Generation tripped. MW Total List generation tripped		
8.	Frequency. Just prior to disturbance (Hz): Immediately after disturbance (Hz max.): Immediately after disturbance (Hz min.):		
9.	List transmission lines tripped (specify voltage level of each line).		
10.		FIRM	INTERRUPTIBLE
	Demand tripped (MW):		
	Number of affected Customers:		

	Demand lost (MW-Minutes):		
11.	Restoration time.	INITIAL	FINAL
	Transmission:		
	Generation:		
	Demand:		

Attachment 2-EOP-004
U.S. Department of Energy Disturbance Reporting Requirements

Introduction

The U.S. Department of Energy (DOE), under its relevant authorities, has established mandatory reporting requirements for electric emergency incidents and disturbances in the United States. DOE collects this information from the electric power industry on Form EIA-417 to meet its overall national security and Federal Energy Management Agency's Federal Response Plan (FRP) responsibilities. DOE will use the data from this form to obtain current information regarding emergency situations on U.S. electric energy supply systems. DOE's Energy Information Administration (EIA) will use the data for reporting on electric power emergency incidents and disturbances in monthly EIA reports. In addition, the data may be used to develop legislative recommendations, reports to the Congress and as a basis for DOE investigations following severe, prolonged, or repeated electric power reliability problems.

Every Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity must use this form to submit mandatory reports of electric power system incidents or disturbances to the DOE Operations Center, which operates on a 24-hour basis, seven days a week. All other entities operating electric systems have filing responsibilities to provide information to the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity when necessary for their reporting obligations and to file form EIA-417 in cases where these entities will not be involved. EIA requests that it be notified of those that plan to file jointly and of those electric entities that want to file separately.

Special reporting provisions exist for those electric utilities located within the United States, but for whom Reliability Coordinator oversight responsibilities are handled by electrical systems located across an international border. A foreign utility handling U.S. Balancing Authority responsibilities, may wish to file this information voluntarily to the DOE. Any U.S.-based utility in this international situation needs to inform DOE that these filings will come from a foreign-based electric system or file the required reports themselves.

Form EIA-417 must be submitted to the DOE Operations Center if any one of the following applies (see Table 1-EOP-004-0 — Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies):

1. Uncontrolled loss of 300 MW or more of firm system load for more than 15 minutes from a single incident.
2. Load shedding of 100 MW or more implemented under emergency operational policy.
3. System-wide voltage reductions of 3 percent or more.
4. Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the electric power system.
5. Actual or suspected physical attacks that could impact electric power system adequacy or reliability; or vandalism, which target components of any security system. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.

6. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.
7. Fuel supply emergencies that could impact electric power system adequacy or reliability.
8. Loss of electric service to more than 50,000 customers for one hour or more.
9. Complete operational failure or shut-down of the transmission and/or distribution electrical system.

The initial DOE Emergency Incident and Disturbance Report (form EIA-417 – Schedule 1) shall be submitted to the DOE Operations Center within 60 minutes of the time of the system disruption. Complete information may not be available at the time of the disruption. However, provide as much information as is known or suspected at the time of the initial filing. If the incident is having a critical impact on operations, a telephone notification to the DOE Operations Center (202-586-8100) is acceptable, pending submission of the completed form EIA-417. Electronic submission via an on-line web-based form is the preferred method of notification. However, electronic submission by facsimile or email is acceptable.

An updated form EIA-417 (Schedule 1 and 2) is due within 48 hours of the event to provide complete disruption information. Electronic submission via facsimile or email is the preferred method of notification. Detailed DOE Incident and Disturbance reporting requirements can be found at: http://www.eia.doe.gov/cneaf/electricity/page/form_417.html.

Table 1-EOP-004-0 Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Uncontrolled loss of Firm System Load	≥ 300 MW – 15 minutes or more	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
2	Load Shedding	≥ 100 MW under emergency operational policy	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
3	Voltage Reductions	3% or more – applied system-wide	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
4	Public Appeals	Emergency conditions to reduce demand	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
5	Physical sabotage, terrorism or vandalism	On physical security systems – suspected or real	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
6	Cyber sabotage, terrorism or vandalism	If the attempt is believed to have or did happen	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
7	Fuel supply emergencies	Fuel inventory or hydro storage levels ≤ 50% of normal	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
8	Loss of electric service	≥ 50,000 for 1 hour or more	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
9	Complete operation failure of electrical system	If isolated or interconnected electrical systems suffer total electrical system collapse	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
All DOE EIA-417 Schedule 1 reports are to be filed within 60-minutes after the start of an incident or disturbance All DOE EIA-417 Schedule 2 reports are to be filed within 48-hours after the start of an incident or disturbance				

All entities required to file a DOE EIA-417 report (Schedule 1 & 2) shall send a copy of these reports to NERC simultaneously, but no later than 24 hours after the start of the incident or disturbance.				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Loss of major system component	Significantly affects integrity of interconnected system operations	NERC Prelim Final report	24 hour 60 day
2	Interconnected system separation or system islanding	Total system shutdown Partial shutdown, separation, or islanding	NERC Prelim Final report	24 hour 60 day
3	Loss of generation	≥ 2,000 – Eastern Interconnection ≥ 2,000 – Western Interconnection ≥ 1,000 – ERCOT Interconnection	NERC Prelim Final report	24 hour 60 day
4	Loss of firm load ≥15-minutes	Entities with peak demand ≥3,000: loss ≥300 MW All others ≥200MW or 50% of total demand	NERC Prelim Final report	24 hour 60 day
5	Firm load shedding	≥100 MW to maintain continuity of bulk system	NERC Prelim Final report	24 hour 60 day
6	System operation or operation actions resulting in:	• Voltage excursions ≥10% • Major damage to system components • Failure, degradation, or misoperation of SPS	NERC Prelim Final report	24 hour 60 day
7	IROL violation	Reliability standard TOP-007.	NERC Prelim Final report	72 hour 60 day
8	As requested by ORS Chairman	Due to nature of disturbance & usefulness to industry (lessons learned)	NERC Prelim Final report	24 hour 60 day
All NERC Operating Security Limit and Preliminary Disturbance reports will be filed within 24 hours after the start of the incident. If an entity must file a DOE EIA-417 report on an incident, which requires a NERC Preliminary report, the Entity may use the DOE EIA-417 form for both DOE and NERC reports.				
Any entity reporting a DOE or NERC incident or disturbance has the responsibility to also notify its Regional Reliability Organization.				

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-01 Disturbance and Sabotage Reporting
Ballot Pool Window Now Open: Oct. 28 – Nov. 28, 2011
Formal Comment Period Open: Oct. 28 – Dec. 12, 2011
Initial Ballot Window: Dec. 2 – 12, 2011

Available Now

EOP-004-2 – Event Reporting (clean and redline showing changes to the last posting), an implementation plan (clean and redline to the last posting), and several associated documents (listed below) have been posted for a formal comment period and initial ballot that will end at 8 p.m. Eastern on Monday, December 12, 2011. Two ballot pools are being formed – one for balloting the standard, and a separate ballot pool for the non-binding poll of the associated VRFs and VSLs. The ballot pool window is open through 8 a.m. Eastern on Monday, November 28. *(Please note that this is 8 a.m. on the Monday following Thanksgiving weekend – Registered Ballot Body members interested in joining the ballot pools for this project should plan accordingly).*

The following associated documents have been posted for stakeholder review and comment:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standard and supporting documents based on comments submitted during the formal comment period that ended April 8, 2011
- Mapping Document - Identifies each requirement in the two already-approved standards that are being consolidated into EOP-004-2 (EOP-004-1 and CIP-001-1a), and identifies how the requirement has been treated in the revisions proposed Draft 3 of EOP-004-2
- VRF/VSL Justification – Explains how the VRFs and VSLs the drafting team has proposed for EOP-004-2 comply with guidelines that FERC and NERC have established for VRFs and VSLs
- Unofficial comment form in Word format – This is for informal use when compiling responses – the final must be submitted electronically

Instructions for Joining Ballot Pools for EOP-004-2 and Associated VRFs/VSLs
Two separate ballot pools are being formed – one ballot pool for Registered Ballot Body (RBB) members interested in balloting of EOP-004-2, and a second for RBB members interested in casting an opinion during the non-binding poll of VRFs and VSLs associated with EOP-004-2. RBB

members who join the ballot pool for the standard **will not** be automatically entered in the ballot pool for the non-binding poll, but must elect to join the second ballot pool.

To join the ballot pool to be eligible to vote in the upcoming ballots and non-binding poll go to: Join Ballot Pool

During the pre-ballot windows, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.)

The ballot pool list server for the initial ballot is: bp-2009-01_DSR_in@nerc.com

The ballot pool list server for the non-binding poll is:
bp-2009-01_DSR_NB_2011_in@nerc.com

Instructions for Commenting
Please use this electronic form ONLY to submit comments. In order to avoid duplication, please indicate "submitted comments electronically" on the ballot and non-binding poll comment section to avoid duplication.

If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps
An initial ballot of EOP-004-2 will be conducted beginning on Friday, December 2, 2011 through 8 p.m. Eastern on Monday, December 12, 2011.

Background
Stakeholders have indicated that identifying potential acts of "sabotage" is difficult to do in real time, and additional clarity is needed to identify thresholds for reporting potential acts of sabotage in CIP-001-1. Stakeholders have also reported that EOP-004-1 has some requirements that reference out-of-date Department of Energy forms, making the requirements ambiguous. EOP-004-1 also has some 'fill-in-the-blank' components to eliminate.

The project will include addressing previously identified stakeholder concerns and FERC directives; will bring the standards into conformance with the latest approved version of the ERO Rules of Procedure; and may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

Additional information is available on the project webpage.

A stakeholder interested in following the Disturbance and Sabotage Reporting Drafting Team's development of EOP-004-2 may monitor meeting agendas and notes on the team's "Related Files" web page or may submit a request to join the team's "plus" e-mail list to receive meeting agendas and meeting notes as they are distributed to the team. To join the team's "plus" e-mail list, send an e-mail request to: sarcomm@nerc.net. Please indicate the drafting team's name in the subject line of the e-mail.

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-01 Disturbance and Sabotage Reporting
Initial Ballot Window and Non-Binding Poll
Open: December 2 –12, 2011

Available December 2nd

An initial ballot of EOP-004-2 – Event Reporting and its associated implementation plan, and a non-binding poll of the associated VRFs and VSLs, are open tomorrow through 8 p.m. Eastern on Monday, December 12, 2011.

Instructions for Balloting

Members of the ballot pools associated with this project may log in and submit their vote for the standard and opinion for the non-binding poll from the following page: https://standards.nerc.net/CurrentBallots.aspx.

Instructions for Commenting

A formal comment period is also open through 8 p.m. Eastern on Monday, December 12, 2011. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Special Instructions for Submitting Comments with a Ballot

Please note that comments submitted during the formal comment period, the ballot for the standard, and the non-binding poll of VRFs and VSLs all use the same electronic form, and it is NOT necessary for ballot pool members to submit more than one set of comments (one through the electronic form, one with the ballot, and one with the non-binding poll). **The drafting team requests that all stakeholders (ballot pool members as well as other stakeholders) submit all comments through the electronic comment form.**

Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps

The drafting team will consider all comments and determine what changes to make in response to stakeholder input from the comments.

Background

Stakeholders have indicated that identifying potential acts of "sabotage" is difficult to do in real time, and additional clarity is needed to identify thresholds for reporting potential acts of sabotage in CIP-001-1. Stakeholders have also reported that EOP-004-1 has some requirements that reference out-of-date Department of Energy forms, making the requirements ambiguous. EOP-004-1 also has some 'fill-in-the-blank' components to eliminate.

The project will include addressing previously identified stakeholder concerns and FERC directives; will bring the standards into conformance with the latest approved version of the ERO Rules of Procedure; and may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

Additional information is available on the project webpage.

A stakeholder interested in following the Disturbance and Sabotage Reporting Drafting Team's development of EOP-004-2 may monitor meeting agendas and notes on the team's "Related Files" web page or may submit a request to join the team's "plus" e-mail list to receive meeting agendas and meeting notes as they are distributed to the team. To join the team's "plus" e-mail list, send an e-mail request to: sarcomm@nerc.net. Please indicate the drafting team's name in the subject line of the e-mail.

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-01 Disturbance and Sabotage Reporting
Ballot Pool Window Now Open: Oct. 28 – Nov. 28, 2011
Formal Comment Period Open: Oct. 28 – Dec. 12, 2011
Initial Ballot Window: Dec. 2 – 12, 2011

Available Now

EOP-004-2 – Event Reporting (clean and redline showing changes to the last posting), an implementation plan (clean and redline to the last posting), and several associated documents (listed below) have been posted for a formal comment period and initial ballot that will end at 8 p.m. Eastern on Monday, December 12, 2011. Two ballot pools are being formed – one for balloting the standard, and a separate ballot pool for the non-binding poll of the associated VRFs and VSLs. The ballot pool window is open through 8 a.m. Eastern on Monday, November 28. *(Please note that this is 8 a.m. on the Monday following Thanksgiving weekend – Registered Ballot Body members interested in joining the ballot pools for this project should plan accordingly).*

The following associated documents have been posted for stakeholder review and comment:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standard and supporting documents based on comments submitted during the formal comment period that ended April 8, 2011
- Mapping Document - Identifies each requirement in the two already-approved standards that are being consolidated into EOP-004-2 (EOP-004-1 and CIP-001-1a), and identifies how the requirement has been treated in the revisions proposed Draft 3 of EOP-004-2
- VRF/VSL Justification – Explains how the VRFs and VSLs the drafting team has proposed for EOP-004-2 comply with guidelines that FERC and NERC have established for VRFs and VSLs
- Unofficial comment form in Word format – This is for informal use when compiling responses – the final must be submitted electronically

Instructions for Joining Ballot Pools for EOP-004-2 and Associated VRFs/VSLs
Two separate ballot pools are being formed – one ballot pool for Registered Ballot Body (RBB) members interested in balloting of EOP-004-2, and a second for RBB members interested in casting an opinion during the non-binding poll of VRFs and VSLs associated with EOP-004-2. RBB

members who join the ballot pool for the standard **will not** be automatically entered in the ballot pool for the non-binding poll, but must elect to join the second ballot pool.

To join the ballot pool to be eligible to vote in the upcoming ballots and non-binding poll go to: Join Ballot Pool

During the pre-ballot windows, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.)

The ballot pool list server for the initial ballot is: bp-2009-01_DSR_in@nerc.com

The ballot pool list server for the non-binding poll is:
bp-2009-01_DSR_NB_2011_in@nerc.com

Instructions for Commenting
Please use this electronic form ONLY to submit comments. In order to avoid duplication, please indicate "submitted comments electronically" on the ballot and non-binding poll comment section to avoid duplication.

If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps
An initial ballot of EOP-004-2 will be conducted beginning on Friday, December 2, 2011 through 8 p.m. Eastern on Monday, December 12, 2011.

Background
Stakeholders have indicated that identifying potential acts of "sabotage" is difficult to do in real time, and additional clarity is needed to identify thresholds for reporting potential acts of sabotage in CIP-001-1. Stakeholders have also reported that EOP-004-1 has some requirements that reference out-of-date Department of Energy forms, making the requirements ambiguous. EOP-004-1 also has some 'fill-in-the-blank' components to eliminate.

The project will include addressing previously identified stakeholder concerns and FERC directives; will bring the standards into conformance with the latest approved version of the ERO Rules of Procedure; and may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.

Additional information is available on the project webpage.

A stakeholder interested in following the Disturbance and Sabotage Reporting Drafting Team's development of EOP-004-2 may monitor meeting agendas and notes on the team's "Related Files" web page or may submit a request to join the team's "plus" e-mail list to receive meeting agendas and meeting notes as they are distributed to the team. To join the team's "plus" e-mail list, send an e-mail request to: sarcomm@nerc.net. Please indicate the drafting team's name in the subject line of the e-mail.

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Name (48 Responses)
Organization (48 Responses)
Group Name (28 Responses)
Lead Contact (28 Responses)
Question 1 (69 Responses)
Question 1 Comments (76 Responses)
Question 2 (68 Responses)
Question 2 Comments (76 Responses)
Question 3 (69 Responses)
Question 3 Comments (76 Responses)
Question 4 (0 Responses)
Question 4 Comments (76 Responses)

Individual
Bo Jones
Westar Energy
Yes
Yes
Yes
In Requirement 1.3, the statement “and the following as appropriate” is vague and subject to interpretation. Who determines what is appropriate? We feel it would be better if the SDT would specify for each event, which party should be notified.
Group
SERC OC Standards Review Group
Gerald Beckerle
No
We agree with removing the training requirement of R4; however we believe that drills and exercises are also training and R4 should be removed in its entirety because drills and exercises on an after the fact process do not enhance reliability.
No
It is confusing why R3 is not considered part of R2, which deals with implementation of the Operating Plan and it appears that R3 could be interpreted as double jeopardy. We suggest deleting R3.
No
No event should have a reporting time less than at the close of the next business day. Any reporting of an event that requires a less reporting time should only be to entities that can help mitigate an event such as an RC or other Reliability Entity.
We believe that reporting of the events in Attachment 1 has no reliability benefit to the bulk electric system. In addition, Attachment 1, in its current form, is likely to be impossible to implement consistently across North America. A requirement, to be considered a reliability requirement, must be implementable. We suggest that Attachment 1 should be removed. We have a question about what looks like a gap in this standard: Assuming one of the drivers for the standard is to protect against a coordinated physical or cyber attack on the grid, what happens if the attack occurs in 3-4 geographically diverse areas? State or provisional law enforcement officials are not accountable under the standard, so we have no way of knowing if they report the attack to the FBI or the RCMP. Even if one or two of them did, might not the FBI, in different parts of the country, interpret it as vandalism, subject to local jurisdiction? It seems that NERC is the focal point that would have all the reports and, ideally, some knowledge how the pieces fit together. It looks like NERC’s role is to solely pass information on “applicable” events to the FERC. Unless the FERC has a 24x7 role not shown in the standard, should not NERC have some type of assessment responsibility to makes inquiries at the FBI/RCMP on whether they are aware of the potential issue and are working on it? “The comments

expressed herein represent a consensus of the views of the above named members of the SERC OC Standards Review group only and should not be construed as the position of SERC Reliability Corporation, its board or its officers.”
Individual
Michael Johnson
APX Power Markets (NCR-11034)
Yes
Yes
Yes
In my opinion the remaining items with 1 hour reporting requirements will in most cases require the input of in-complete information, since you maybe aware of the outage/disturbance, but not aware of any reason for it. If that is acceptable just to get the intitial report that there was an outage/disturbance then we are OK. I believe it would help to have that clarifed in the EOP, or maybe a CAN can be created for that.
For Attachment 1 and the events titled "Unplanned Control Center evacuation" and "Loss of monitoring or all voice communication capabiliy". RC, BA, and TOP are the only listed entity types listed for reporting responsibility. We are a GOP that offers a SCADA service in several regions and those type of events could result in a loss of situational awareness for the regions we provide services. I believe the requirement for reporting should not be limited to Entity Type, but on their impact for situational awareness to the BES based on the amount of generation they control (specific to our case), or other criteria that would be critical to the BES (i.e. voltage, frequency).
Individual
David Proebstel
Clallam County PUD No.1
Yes
Yes
Yes
While we agree with the revisions as far as they went, we do not believe the SDT has adequately addressed the FERC Order to “Consider whether separate, less burdensome requirements for smaller entities may be appropriate.” The one and 24 hour reporting requirements continue to be burdensome to the smaller entities that do not maintain 24/7 dispatch centers. The one hour reporting requirement means that an untimely “recognition” starts the clock and reporting will become a higher priority than restoration. The note regarding adverse conditions does not help unless we were to consider the very lack of 24/7 dispatch to be such a condition.
Project 2008-06 proposes to withdraw the terms “Critical Asset” and “Critical Cyber Asset” from the NERC Glossary. In order to avoid a reliability gap when this occurs, we propose including High and Medium Impact BES Cyber Systems and Assets. The revised wording to add, “as appropriate” to R1.3 is a concern. We understand the SDT’s intent to not require all the bulleted parties to be notified for every event type. But will a good faith effort on the part of the registered entity to deem appropriateness be subject to second guessing and possible sanctions by the Compliance Enforcement Authority if they disagree? We note that CIP-001 required an interpretation to address this issue, but cannot assume that interpretation will carry over. We suggest spelling out exactly who shall deem appropriateness. R4 continues to be an onerous requirement for smaller entities. Verification was not part of the SAR and we are not convinced it is needed for reliability. We are unsure how a DP with no generation, no BES assets, no Critical Cyber Assets, and less than 100 MW of load; would meet R4. Shall they drill for impossible events? We ask that R4 be removed. At a minimum it should exclude entities that cannot experience the events of Attachment 1. Entities that cannot experience the events of Attachment 1should likewise be exempt from R1.2, 1.3, R2, and R3.
Group

Northeast Power Coordinating Council
Guy Zito
No
Requirement R4 is unnecessary. Whether or not the process, plan, procedure, etc. is “verified” is of no consequence. EOP standards are intended to have entities prepare for likely events (restoration/evacuation), and to provide tools for similar unforeseen events (ice storms, tornadoes, earthquakes, etc.). They should not force a script when results are what matters.
No
R1.3 should be revised as follows: A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity’s Reliability Coordinator and the following as determined by the responsible entity:… Without this change it is not clear who determines what communication level is appropriate. R1.4 should be revised as follows: Provision(s) for updating the Operating Plan following any change in assets or personnel (if the Operating Plan specifies personnel or assets), that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3. R1.5 should be deleted. Responsible Entities can determine the frequency of Operating Plan updates. Requirement 1.4 requires updating the Operating Plan within 90 calendar days for changes in “assets, personnel…. or incorporating lessons learned”, (or our preceding proposed revision). This requirement eliminates the need for Requirement 1.5 requiring a review of the Operating Plan on an annual basis. The only true requirement that is results-based, not administrative and is actually required to support the Purpose of the Standard is R3.
No
The SDT should work with the NERC team drafting the Events Analysis Process (EAP) to ensure that the reporting events align and use the same descriptive language. EOP-004 should use the exact same events as OE-417. These could be considered a baseline set of reportable events. If the SDT believes that there is justification to add additional reporting events beyond those identified in OE-417, then the event table could be expanded. If the list of reportable events is expanded beyond the OE-417 event list, the supplemental events should be the same in both EOP-004-2 and in the EAP Categories 1 through 5. It is not clear what the difference is between a footnote and “Threshold for Reporting”. All information should be included in the body of the table, there should be no footnotes. Event: Risk to BES equipment should be deleted. This is too vague and subjective. This will result in many “prove the negative” situations. Event: Destruction of BES equipment is also too vague. The footnote refers to equipment being “damaged or destroyed”. There is a major difference between destruction and damage. Event: Damage or Destruction of a Critical Asset or Critical Cyber Asset should be deleted. Disclosure policies regarding sensitive information could limit an entity’s ability to report. Unintentional damage to a CCA does not warrant a report. Event: BES Emergency requiring public appeal for load reduction should be modified to note that this does not apply to routine requests for customer conservation during high load periods.
Requirement 4 does not specifically state the details necessary for an entity to achieve compliance. Requirement 4 should provide more guidance as to what is required in a drill. Audit/enforcement of any requirement language that is too broad will potentially lead to Regional interpretation, inconsistency, and additional CANs. R4 should be revised to delete the 15 month requirement. CAN-0010 recognizes that entities may determine the definition of annual. The standard is too specific, and drills down into entity practices, when the results are all that should be looked for. The standard is requiring multiple reports. The Purpose of the Standard is very broad and should be revised because some of the events being reported on have no impact on the BES. Revise Purpose wording as follows: To improve industry awareness and the reliability of the Bulk Electric System “by requiring the reporting of major system events with the potential to impact reliability and their causes…” on the Bulk Electric System it can be said that every event occurring on the Bulk Electric System would have to be reported. Referring to Requirement R4, the testing of the communication process is the responsibility of the Responsible Entity. There is an event analysis process already in place. The standard prescribes different sets of criteria, and forms. There should be one recipient of event information. That recipient should be a “clearinghouse” to ensure the proper dissemination of information. Why is this standard applicable to the ERO? Requirement R2 is not necessary. It states the obvious. Requirements R2 and R3 are redundant. The standard mentions collecting information for Attachment 2, but nowhere does it state what to do with Attachment 2. None of the key concepts identified on page 5 of the standard are clearly stated or described in the requirements: • Develop a

single form to report disturbances and events that threaten the reliability of the bulk electric system. • Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements. • Establish clear criteria for reporting. • Establish consistent reporting timelines. • Provide clarity for who will receive the information and how it will be used. The standard's requirements should be reviewed with an eye for deleting those that are redundant, or do not address the Purpose or intent of the standard.
Group
Luminant Power
Stewart Rake
Yes
No
Requirements R1, R2, and R4 are burdensome administrative requirements and are contradictory to the NERC stated Standards Development goals of reducing administrative requirements by moving to performance requirements. There is only one Requirement needed in this standard: "The Responsible Entity shall report events in accordance with Attachment 1." Attachment 1 should describe how events should be reported by what Entity to which party within a defined timeframe. If this requirement is met, all the other proposed requirements have no benefit to the reliability of the Bulk Electric System. Per the NERC Standard Development guidelines, only items that provide a reliability benefit should be included in a standard.
No
Luminant agrees with the changes the SDT made, however, the timeline should be modified to put higher priority activities before reporting requirements. The SDT should consider allowing entities the ability to put the safety of personnel, safety of the equipment, and possibly the stabilization of BES equipment efforts prior to initiating the one hour reporting timeline. Reporting requirements should not be prioritized above these important activities. The requirement to report one hour after the recognition of such an event may not be sufficient in all instances. Entities should not have a potential violation as a result of putting these priority issues first and not meeting the one hour reporting timeline.
The following comments all apply to Attachment 1: • As a general comment, SDT should specifically list the entities the reportable event applies to in the table for clarity. Do not use general language referencing another standard or statements such as "Deficient entity is responsible for reporting", "Initiating entity is responsible for reporting", or other similar statements used currently in the table. This leaves this open and subject to interpretation. Also, there are a number of events that do not apply to all entities. • Destruction of BES equipment should be Intentional Damage or Destruction of BES equipment. Unintentional actions occur and should not be a requirement for reporting under disturbance reporting. • Actions or situations affecting equipment or generation unit availability due to human error, equipment failure, unintentional human action, external cause, etc. are reported in real time to the BA and other entities as required by other NERC Standards. Disturbance reporting should avoid the type of events that, for instance, would cause the total or partial loss of a generating unit under normal operational circumstances. There are a number of issues with the table in this regard. • For clarity, consider changing the table to identify for each event type "who" should be notified. This appears to be missing from the table overall. • Reportable Events, the meaning for the Event labeled "Destruction of BES equipment" is not clear. Footnote 1 adds the language "iii) Damaged or destroyed due to intentional or unintentional human action which removes the BES equipment from service." This language can be interpreted to mean that any damage to any BES equipment caused by human action, regardless of intention, must be reported within 1 hour of recognition of the event. This requirement will be overly burdensome. If this is not the intent of the definition of "Destruction of BES equipment", the footnote should be re-worded. As such, it is subjective and left open to interpretation. It should focus only on intentional actions to damage or interrupt BES functionality. It should not be worded as such that every item that trips a unit or every item that is damaged on a unit requires a report. That is where the language right now is not clear. There are and will continue to be unintentional human error that results in taking equipment out of service. This standard was meant to replace sabotage reporting. • Damage or destruction of Critical Asset per CIP-002 and Damage or destruction of a Critical Cyber Asset per CIP-002 should be removed from the table as Intentional Damage or Destruction of BES equipment would cover this as well. • Risk to BES

equipment should be removed from the table as it is very subjective and broad. At a minimum, the 1 hour reporting timeline should begin after recognition and assessment of the incident. As an example, a fire close to BES equipment may not truly be a threat to the equipment and will not be known until an assessment can be made to determine the risk. • Detection of a Reportable Cyber Security incident should be removed from the table as this is covered by CIP-008 requirements. Having this in two separate standards is double jeopardy and confusing to entities. • Generation Loss event reporting should only apply to the BA. These authorities have the ability and right to contact generation resources to supply necessary information needed for reporting. This would also eliminate redundant reporting by multiple entities for the same event. • Suggest that Generation Loss MW loss would match up with the 1500 MW level identified in CIP Version 4 or Version 5 for consistency between future CIP standards and this disturbance reporting standard. This would then cover CIP and significant MW losses that should be reported. • The Generation Loss MW loss amount needs to have a time boundary. Luminant would suggest a loss of 1500 MW within 15 minutes. • Unplanned Control Center evacuation should not apply to entities that have backup Control Centers where normal operations can continue without impact to the BES. • Loss of monitoring or all voice communication capability should be separated. Also the 24 hour reporting requirement may not be feasible if communications is down for longer than 24 hours. Luminant would suggest removal of the communication reporting event as there are a number of things that could cause this to occur for longer than the reporting requirement allows, thus putting entities at jeopardy of a potential violation that is out of their control. How does an entity report if all systems and communications are down for more than 24 hours? What about in instances of a partial or total blackout? These events could last much longer than 24 hours. All computer communication would likely also be down thus rendering electronic reporting unavailable.
Individual
Michael Moltane
ITC
Yes
Yes
No
See comments to Question #4
Footnote 1 and the corresponding Threshold For Reporting associated with the first Event in Attachment 1 are not consistent and thus confusing. Qualifying the term BES equipment through a footnote is inappropriate as it leads to this confusion. For instance, does iii under Footnote 1 apply only to BES equipment that meet i and ii or is it applicable to all BES equipment? The inclusion of equipment failure, operational error and unintentional human action within the threshold of reporting for “destruction” required in the first 3 Events listed in Attachment 1 is also not appropriate. It is clear through operational history that the intent of the equipment applied to the system, the operating practices and personnel training developed/delivered to operate the BES is to result in reliable operation of the BES which has been accomplished exceedingly well given past history. This is vastly different than for intentional actions and should be excluded from the first 3 events listed in Attachment. To the extent these issues are present in another event type they will be captured accordingly. Footnote 1 should be removed and the Threshold for Reporting associated with the first three events in Attachment 1 should be updated only to include intentional human action. This will also result in including all BES equipment that was intentionally damaged in the reporting requirement and not just the small subset qualified by the existing footnote 1. This provides a much better data sample for law enforcement to make assessments from than the smaller subset qualified by what we believe the intent of footnote 1 is.
Group
PacifiCorp
Sandra Shaffer
Yes
Yes

Yes
No comment.
Group
Pacific Northwest Small Public Power Utility Comment Group
Steve Alexanderson
Yes
Yes
Yes
While we agree with the revisions as far as they went, we do not believe the SDT has adequately addressed the FERC Order to “Consider whether separate, less burdensome requirements for smaller entities may be appropriate.” The one and 24 hour reporting requirements continue to be burdensome to the smaller entities that do not maintain 24/7 dispatch centers. The one hour reporting requirement means that an untimely “recognition” starts the clock and reporting will become a higher priority than restoration. The note regarding adverse conditions does not help unless we were to consider the very lack of 24/7 dispatch to be such a condition.
Project 2008-06 proposes to withdraw the terms “Critical Asset” and “Critical Cyber Asset” from the NERC Glossary. In order to avoid a reliability gap when this occurs, we propose including High and Medium Impact BES Cyber Systems and Assets. The revised wording to add, “as appropriate” to R1.3 is a concern. We understand the SDT’s intent to not require all the bulleted parties to be notified for every event type. But will a good faith effort on the part of the registered entity to deem appropriateness be subject to second guessing and possible sanctions by the Compliance Enforcement Authority if they disagree? We note that CIP-001 required an interpretation to address this issue, but cannot assume that interpretation will carry over. We suggest spelling out exactly who shall deem appropriateness. R4 continues to be an onerous requirement for smaller entities. Verification was not part of the SAR and we are not convinced it is needed for reliability. We are unsure how a DP with no generation, no BES assets, no Critical Cyber Assets, and less than 100 MW of load; would meet R4. Shall they drill for impossible events? We ask that R4 be removed. At a minimum it should exclude entities that cannot experience the events of Attachment 1. Entities that cannot experience the events of Attachment 1should likewise be exempt from R1.2, 1.3, R2, and R3.
Individual
Tracy Richardson
Springfield Utility Board
Yes
Yes
Yes
• The Draft 3 Version History still lists the term “Impact Event” instead of “Event”. • Draft 3 of EOP-004-2 – Event Reporting does not provide a definition for the term “Event” nor does the NERC Glossary of Terms Used in Reliability Standards. SUB recommends that “Event” be listed and defined in “Definitions and Terms Used in the Standard” as well as the NERC Glossary, providing a framework and giving guidance to entities for how to determine what should be considered an “Event” (ex: sabotage, unusual occurrence, metal theft, etc.).
Individual
Kasia Mihalchuk
Manitoba Hydro
Yes

Yes
Yes
Attachment 1 - The term 'Transmission Facilities' used in Attachment 1 is capitalized, but it is not a defined term in the NERC glossary. The drafting team should clarify this issue. Attachment 2 - The inclusion of 'Fuel supply emergency' in Attachment 2 creates confusion as it infers that reporting a 'fuel supply emergency' may be required by the standard even though 'fuel supply emergency' is not listed in Attachment 1. On a similar note, it is not clear what the drafting team is hoping to capture by including a checkbox for 'other' in Attachment 2.
Group
Southwest Power Pool Regional Entity
Emily Pennel
Yes
Yes
Yes
1. EOP-004-2 R1.4 states entities must update their Operating Plans within 90 calendar days of incorporating lessons learned pursuant to R3. However, neither R3 nor Attachment 1 include a timeline for incorporating lessons learned. It is unclear when the "clock starts" on incorporating improvements or lessons learned. Within 90 days of what? 90 days of the event? 90 days from when management approved the lesson learned? Auditors need to know the trigger for the 90-day clock. 2. The Event Analysis classification includes Category 1C "failure or misoperation of the BPS SPS/RAS". This category is not included in EOP-004-2's Attachment 1. This event, "failure or misoperation of the BPS SPS/RAS", needs to either be added to Attachment 1 or removed from the Event Analysis classification. It is important that EOP-004-2 Attachment 1 and the Event Analysis categories match up. Thank you for your work on this standard.
Individual
Kevin Conway
Intellibind
Yes
No
The language proposed is not clear and will continue to add confusion to entities who are trying to meet these requirements. It is not clear that the drafting team can put itself in the position of how the auditors will interpret and implement compliance against thithe R2 requirement. Requirements should be written to stand alone, not reference other requirements (or parts of the requirments. If the R1 parts 1.1, 1.2, 1.4 and 1.5 are so significant for this requirement, then they should be rewritten in R2.
Yes
Does this reporting conflict with reporting for DOE, and Regions? If so, what reporting requirements will the entity be held accountable to? Managing multiple reporting requirements for the multiple agencies is very problematic for entities and this standard should resolve those reporting requirments, as well as reduce the reporting down to one form and one submission. Reporting to ESISAC should take care of all reporting by the company. NERC should route all reports to the DOE, and regions through this mechanism.
I do not see that the rewrite of this standard is meeting the goal of clear reliability standards, and in fact the documents are looking more like legal documents. Though the original EOP-004 and CIP-001 was problematic at times, this rewrite, and the need to have such extensive guidance, attachments, and references for EOP-004-2 will create an even more difficult standard to properly meet to ensure

compliance during an audit. Though CIP-001 and EOP-004 were related, combining them in a single standard is not resolving the issues, and is in fact complicating the tasks. Requirements in this standard should deal with only one specific issue, not deal with multiple tasks. I am not sure how an auditor will consistently audit against R2, and how a violation will be categorized when an entity implements all portions of their Operating Plan, however fails to fully address all the requirements in R1, thereby not fully implementing R2, in strict interpretation. The drafting team should not set up a situation where an entity is in double jeopardy for missing an element of a requirement. I also suggest that EOP-004-2 be given a new EOP designation rather than calling it a revision. This way implementation can be better controlled, since most companies have written specific CIP-001 and EOP-004 document that will not simple transfer over to the new version. This standard is a drastic departure from the oringial versions. I appreciate the level of work that is going into EOP-004-2, it appears that significant time and effort has been going into the supporting documentation. It is my opinion that if this much material has to be created to state what the standard really requires, then the standard is flawed. When there are 21 pages of explanation for five requirements, especially when we have previously had 16 pages that originally covered 2 separate reliability standards, we need to reevaluate what we are really doing.
Group
Arizona Public Service Company
Janet Smith, Regulatory Affairs Supervisor
Yes
Yes
Yes
No comments
Individual
Chris Higgins / Jim Burns / Ted Snodgrass / Jeff Millennor / Russell Funk
Bonneville Power Administration
Yes
Yes
BPA believes the measures for R2 are unclear since they are similar to R3's reporting measures.
No
BPA believes that the first three elements in Attachment 1 are too generic and should be with only the intentional human criterion. The suspicious device needs to be determined as a threat (and not left behind tools) before requiring a report.
BPA believes that Attachment 1 has too many added reportable items because unintentional, equipment failure & operational errors are included in the first three items. A. Change to only "intentional human action". Otherwise, the first item "destruction of BES equipment" is too burdensome, along with its short time reporting time: i. - If a single transformer fails that shouldn't require a report. ii.- Emergency actions have to be taken for any failure of equipment, e.g. a loss of line reduces a path SOL and requires curtailments to reduce risk to the system. B. The item for "risk to BES" is not necessary until the suspicious object has been identified as a threat. If what turns out to be air impact wrench left next to BES equipment, that should not be a reportable incident as this current table implies. C. The nuclear "LOOP" should be only reported if total loss of off site source (i.e. 2 of 2 or 3 of 3) when supplying the plants load. If lightning or insulator fails causing one of the line sources to trip that's not a system disturbance especially if it is just used as a backup. It should only be a NRC process if they want to monitor that. The VRF/VSL: BPA believes that the VRF for R2 & R4 should be "Lower".
Individual
Chris de Graffenried
Consolidated Edison Co. of NY, Inc.

Yes
No
Comments: • R1.3 should be revised as follows: A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as determined by the responsible entity: ["appropriate: - deleted] [otherwise it is not clear who determines what communication level is appropriate] • R1.4 should be revised as follows: Provision(s) for updating the Operating Plan following ["within 90 calendar days of any" - deleted] change in assets or personnel (if the Operating Plan specifies personnel or assets) , ["other circumstances" - deleted] that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3. • R1.5 should be deleted. Responsible Entities can determine the frequency of Operating Plan updates. Requirement 1.4 requires updating the Operating Plan within 90 calendar days for changes in "assets, personnel…. or incorporating lessons learned". This requirement eliminates the need for Requirement 1.5 requiring a review of the Operating Plan on an annual basis.
No
Comments: We have a number of comments on Attachment 1 and will make them here: • Generally speaking the SDT should work with the NERC team drafting the Events Analysis Process (EAP) to ensure that the reporting events align and use the same descriptive language. • EOP-004 should use the exact same events as OE-417. These could be considered a baseline set of reportable events. If the SDT believes that there is justification to add additional reporting events beyond those identified in OE-417, then the event table could be expanded. • If the list of reportable events is expanded beyond the OE-417 event list, the supplemental events should be the same in both EOP-004-2 and in the EAP Categories 1 through 5. • It is not clear what the difference is between a footnote and "Threshold for Reporting". All information should be included in the body of the table, there should be no footnotes. • Event: "Risk to BES equipment" should be deleted. This is too vague and subjective. Will result in many "prove the negative" situations.' • Event: "Destruction of BES equipment" is again too vague. The footnote refers to equipment being "damaged or destroyed". There is a major difference between destruction and damage. • Event: "Damage or Destruction of a Critical Asset or Critical Cyber Asset" should be deleted. Disclosure policies regarding sensitive information could limit an entity's ability to report. Unintentional damage to a CCA does not warrant a report. • Event: "BES Emergency requiring public appeal for load reduction" should be modified to note that this does not apply to routine requests for customer conservation during high load periods.
Comments: • Requirement 4 does not specifically state details necessary for an entity to achieve compliance. Requirement 4 should provide more guidance as to what is required in a drill. Audit / enforcement of any requirement language that is too broad will potentially lead to Regional interpretation, inconsistency, and additional CANs. • R4 should be revised to delete the 15 month requirement. CAN-0010 recognizes that entities may determine the definition of annual. • The Purpose of the Standard should be revised because some of the events being reported on have no impact on the BES. Revise Purpose as follows: To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of [add] "major system events." [delete - "with the potential to impact reliability and their causes, if known, by the Responsible Entities."]
Individual
David Burke
Orange and Rockland Utilities, Inc.
Yes
No
Comments: • R1.3 should be revised as follows: A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as determined by the responsible entity: ["appropriate: - deleted] [otherwise it is not clear who determines what communication level is appropriate] • R1.4 should be revised as follows: Provision(s) for updating the Operating Plan following ["within 90 calendar days of any" - deleted] change in assets or personnel (if the Operating Plan specifies personnel or assets) , ["other circumstances" - deleted] that may no longer align with the Operating Plan; or incorporating lessons

learned pursuant to Requirement R3. • R1.5 should be deleted. Responsible Entities can determine the frequency of Operating Plan updates. Requirement 1.4 requires updating the Operating Plan within 90 calendar days for changes in “assets, personnel…. or incorporating lessons learned”. This requirement eliminates the need for Requirement 1.5 requiring a review of the Operating Plan on an annual basis.
No
• Generally speaking the SDT should work with the NERC team drafting the Events Analysis Process (EAP) to ensure that the reporting events align and use the same descriptive language. • EOP-004 should use the exact same events as OE-417. These could be considered a baseline set of reportable events. If the SDT believes that there is justification to add additional reporting events beyond those identified in OE-417, then the event table could be expanded. • If the list of reportable events is expanded beyond the OE-417 event list, the supplemental events should be the same in both EOP-004-2 and in the EAP Categories 1 through 5. • It is not clear what the difference is between a footnote and “Threshold for Reporting”. All information should be included in the body of the table, there should be no footnotes. • Event: “Risk to BES equipment” should be deleted. This is too vague and subjective. Will result in many “prove the negative” situations.’ • Event: “Destruction of BES equipment” is again too vague. The footnote refers to equipment being “damaged or destroyed”. There is a major difference between destruction and damage. • Event: “Damage or Destruction of a Critical Asset or Critical Cyber Asset” should be deleted. Disclosure policies regarding sensitive information could limit an entity’s ability to report. Unintentional damage to a CCA does not warrant a report. • Event: “BES Emergency requiring public appeal for load reduction” should be modified to note that this does not apply to routine requests for customer conservation during high load periods
Comments: • Requirement 4 does not specifically state details necessary for an entity to achieve compliance. Requirement 4 should provide more guidance as to what is required in a drill. Audit / enforcement of any requirement language that is too broad will potentially lead to Regional interpretation, inconsistency, and additional CANs. • R4 should be revised to delete the 15 month requirement. CAN-0010 recognizes that entities may determine the definition of annual. • The Purpose of the Standard should be revised because some of the events being reported on have no impact on the BES. Revise Purpose as follows: To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of [add] "major system events.” [delete - “with the potential to impact reliability and their causes, if known, by the Responsible Entities.”]
Individual
Alice Ireland
Xcel Energy
Yes
No
Suggest modifying R3 to indicate this is related to R 1.3. Each Responsible Entity shall report events to entities specified in R1.3 and as identified as appropriate in its Operating Plan.
Yes
Group
BC Hydro
Patricia Robertson
Yes
Yes
No
As an event would be verbally reported to the RC, all the one hour requirements to submit a written report should be moved from one hour to 24 hours.
Attachment 1: Reportable Events: BC Hydro recommends further defining “BES equipment” for the

events Destruction of BES equipment and Risk to BES equipment. Attachment 1: Reportable Events: BC Hydro recommends defining the Forced intrusion event as the wording is very broad and open to each entities interpretation. What would be a forced intrusion ie entry or only if equipment damage occurs?
Individual
Greg Rowland
Duke Energy
Yes
Yes
No
All events in Attachment 1 should have reporting times of no less than 24 hours. As stated on page 6 of the current draft of the standard: “The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting.” We maintain that a report which is required to be made within one hour after an event is, in fact, a real time report. In the first hour or even several hours after an event the operator may appropriately still be totally committed to restoring service or returning to a stable bulk power system state, and should not stop that recovery activity in order to make this “after-the-fact” report.
1. Reporting under EOP-004-2 should be more closely aligned with Events Analysis Reporting. 2. Attachment 1 – Under the column titled “Entity with Reporting Responsibility”, several Events list multiple entities, using the phrase “Each RC, BA, TO, TOP, GO, GOP, DP that experiences…” or a similar phrase requiring that multiple entities report the same event. We believe these entries should be changed so that multiple reports aren’t required for the same event. 3. Attachment 1 – The phrase “BES equipment” is used several times in the Events Table and footnotes to the table. “Equipment” is not a defined term and lacks clarity. “Element” and “Facility” are defined terms. Replace “BES equipment” with “BES Element” or “BES Facility”. 4. Attachment 1 – The Event “Risk to BES equipment” is unclear, since some amount of risk is always present. Reword as follows: “Event that creates additional risk to a BES Element or Facility.” 5. Attachment 1 – The Threshold for Reporting Voltage deviations on BES Facilities is identified as “+ 10% sustained for > 15 continuous minutes.” Need to clarify + 10% of what voltage? We think it should be nominal voltage. 6. Attachment 1 - Footnote 1 contains the phrase “has the potential to”. This phrase should be struck because it creates an impossibly broad compliance responsibility. Similarly, Footnote 3 contains the same phrase, as well as the word “could” several times, which should be changed so that entities can reasonably comply. 7. Attachment 1 – The “Unplanned Control Center evacuation” Event has the word “potential” in the column under “Entity with Reporting Responsibility”. The word “potential” should be struck. 8. Attachment 2 – Includes “fuel supply emergency”, which is not listed on Attachment 1.
Group
Progress Energy
Jim Eckelkamp
(1) Attachment 1 lists “Destruction of BES Equipment” as a reportable event but then lists “equipment failure” as one of several thresholds for reporting, with a one hour time limit for reporting. It is simply not common sense to think of the simple failure of a single piece of equipment as “destruction of BES equipment”. Does the standard really expect that every BES equipment failure must be reported within one hour, regardless of cause or impact to BES reliability? What is the purpose of such extensive reporting? (2) The same comment as (1) above is applicable to the “Damage or destruction of Critical Asset” because one threshold is simple “equipment failure” as well. (3) Footnote 2 (page 20) says copper theft is not reportable “unless it effects the reliability of the BES”, but footnote 1 on the same page says copper theft is reportable if “it degrades the ability of equipment to operate

properly". In this instance, the proposed standard provides two different criteria for reporting one of the most common events on the same page. (4) Forced Intrusion must be reported if "you cannot determine the likely motivation", and not based on a conclusion that the intent was to commit sabotage or intentional damage. This would require reporting many theft related instances of cut fences and forced doors (including aborted theft attempts where nothing is stolen) which would consume a great deal of time and resources and accomplish nothing. This criteria is exactly the opposite of the existing philosophy of only reporting events if there is an indication of an intent to commit sabotage or cause damage. (5) "Risk to BES equipment…from a non-environmental physical threat" is reportable, but this is an example of a vague, open ended reporting requirement that will either generate a high volume of unproductive reports or will expose reporting entities to audit risk for not reporting potential threats that could have been reported. The standard helpfully lists train derailments and suspicious devices as examples of reportable events. The existing CAN for CIP-001 (CAN-0016) is already asking for a list of events that were analyzed so the auditors can determine if a violation was committed due to failure to report. I can envision the CAN for this new standard requiring a list of all "non-environmental physical threats" that were analyzed during the audit period to determine if applicable events were reported. This could generate a great deal of work simply to provide audit documentation even if no events actually occur that are reportable. It would also be easy for an audit team to second guess a decision that was made by an entity not to report an event (what is risk?...how much risk was present due to the event?...). Also, the reporting for this vague criteria must be done within one hour. Any event with a one hour reporting requirement should be crystal clear and unambiguous. (6) Transmission Loss…of three or more Transmission Facilities" is reportable. "Facility" is a defined term in the NERC Glossary, but "Transmission Facility" is not a defined term, which will lead to confusion when this criteria is applied. This requirement raises many confusing questions. What if three or more elements are lost due to two separate or loosely related events – is this reportable or not? What processes will need to be put in place to count elements that are lost for each event and determine if reporting is required? Why must events be reported that fit an arbitrary numerical criteria without regard to any material impact on BES reliability?

Individual

Rodney Luck

Los Angeles Department of Water and Power

No

The reporting time of within 1 hour of recognition for a "Forced Intrusion" (last event category on page 20 of Draft 3, dated October 25, 2011) when considered with the associated footnote "Report if you cannot reasonably determine likely motivation" is overly burdensome and unrealistic. What is "reasonably determine likely motivation" is too general and requires further clarity. For example, LADWP has numerous facilities with extensive perimeter fencing. There is a significant difference between a forced intrusion like a hole or cut in a property line fence of a facility versus a forced intrusion at a control house. Often cuts in fences, after further investigation, are determined to be cases of minor vandalism. An investigation of this nature will take much more than the allotted hour. The NERC Design Team needs to develop difference levels for the term "Force Intrusion" that fit the magnitude of the event and provide for adequate time to determine if the event was only a case of minor vandalism or petty thief. The requirement, as currently written, would unnecessarily burden an entity in reporting events that after given more time to investigate would more than likely not have been a reportable event.

Individual

Daniel Duff

Liberty Electric Power

No

Training should be left in the standard as an option, along with an actual event, drill or exercise, to demonstrate that operating personnel have knowledge of the procedure.

Yes

Yes
Group
ZGlobal on behalf of City of Ukiah, Alameda Municipal Power, Salmen River Electric, City of Lodi
Mary Jo Cooper
Yes
Yes
Yes
We feel that the drafting team has done an excellent job of providing clarification and reasonable reporting requirements to the right functional entity. However we feel additional clarification should be made in the Attachment I Event Table. We suggest the following modifications: For the Event: BES Emergency resulting in automatic firm load shedding Modify the Entity with Reporting Responsibility to: Each DP or TOP that experiences the automatic load shedding within their respective distribution serving or Transmission Operating area. For the Event: Loss of Firm load for ≥ 15 Minutes Modify the Entity with Reporting Responsibility to: Each BA, TOP, DP that experiences the loss of firm load within their respective balancing, Transmission operating, or distribution serving area.
Individual
Lisa Rosintoski
Colorado Springs Utilities
Yes
No
The act of implementing the plan needs to include reporting events per R1, sub-requirement 1.3. R2 should simply state something like, “Each Responsible Entity shall implement the Operating Plan that meets the requirements of R1, as applicable, for an actual event or as specified.” Suggest eliminating R3 which, seems to create double jeopardy effect.
Yes
Agree with concept to combine CIP-001 into EOP-004. Agree with elimination of “sabotage” concept. Appreciate the attempt to combine reporting requirements, but it seems that in practice will still have separate reporting to DOE and NERC/Regional Entities. EOP-004-2 A.5. “Summary of Key Concepts” refers to Att. 1 Part A and Att. 1 Part B. I believe these have now been combined. EOP-004-2 A.5. “Summary of Key Concepts” refers to development of an electronic reporting form and inclusion of regional reporting requirements. It is unfortunate no progress was made on this front.
Individual
Michael Falvo
Independent Electricity System Operator
Yes
No
We agree with the revision to R2 and R3, but assess that a requirement to enforce implementation of Part 1.3 in Requirement R1 is missing. Part 1.3 in Requirement R1 stipulates that: 1.3. A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity’s Reliability Coordinator and the following as appropriate: • Internal company personnel • The Responsible Entity’s Regional Entity • Law enforcement • Governmental or provincial agencies The implementation of Part 1.3 is not enforced by R2 or R3 or any other Requirements in the standard. Suggest to add another requirement or expand Requirement R4 (and M4) to require the implementation of this Part in addition to verifying the process.

Yes
1. Measures M1, M2 and M3: Suggest to achieve consistent wording among them by saying the leading part to “Each Responsible Entity shall provide….” 2. In our comments on the previous version, we suggested the SDT to review the need to include IA, TSP and LSE for some of the reporting requirements in Attachment 1. The SDT’s responded that it had to follow the requirements of the standards as they currently apply. Since these entities are applicable to the underlying standards identified in Attachment 1, they will be subject to reporting. We accept this rationale. However, the revised Attachment 1 appears to be still somewhat discriminative on who needs to report an event. For example, the event of “Detection of a reportable Cyber Security Incident” (6th row in the table) requires reporting by a list of responsible entities based on the underlying requirements in CIP-008, but the list does not include the IA, TSP and LSE. We again suggest the SDT to review the need for listing the specific entities versus leaving it general by saying: “Applicable Entities under CIP-008” for this particular item, and review and establish a consistent approach throughout Attachment 1. 3. VSLs: a. Suggest to not list all the specific entities, but replace them with “Each Responsible Entity” to simplify the write-up which will allow readers to get to the violation condition much more quickly. b. For R1, it is not clear whether the conditions listed under the four columns are “OR” or “AND”. We believe it means “OR”, but this needs to be clarified in the VSL table. 4. The proposed implementation plan conflicts with Ontario regulatory practice respecting the effective date of the standard. It is suggested that this conflict be removed by appending to the implementation plan wording, after “applicable regulatory approval” in the Effective Dates Section on P. 2 of the draft standard and P. 1 of the draft implementation plan, to the following effect: “, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.”
Individual
John Bee on Behalf of Exelon
Exelon
Yes
Yes
Why is the reference to R1.3 missing from EOP-004-2 Requirement R2?
No
Due to the size of the service territories in ComEd and PECO it’s difficult to get to some of the stations within in an hour to analyze an event which causes concern with the 1 hour criteria. It is conceivable that the evaluation of an event could take longer then one hour to determine if it is reportable. Exelon cannot support this version of the standard until the 1 hour reporting criteria is clarified so that the reporting requirements are reasonable and obtainable. Exelon has concerns about the existing 1 hour reporting requirements and feels that additional guidance and verbiage is required for clarification. We would like a better understanding when the 1 hour clock starts please consider using the following clarifying statement, in the statements that read, “recognition of events” please consider replacing the word “recognition” with the word “confirmation” as in a “confirmed event”
1. Please replace the text “Operating Plan” with procedure(s). Many companies have procedure(s) for the reporting and recognition of sabotage events. These procedures extend beyond operating groups and provide guidance to the entire company. 2. The Loss of Off-site power event criteria is much improved from the last draft of EOP 004-2; however, some clarification is needed to more accurately align with NERC Standard NUC-001 in both nomenclature and intent. Specifically, as Exelon has previously commented, there are many different configurations supplying offsite power to a nuclear power plant and it is essential that all configurations be accounted for. As identified in the applicability section of NUC-001 the applicable transmission entities may include one or more of the following (TO, TOP, TP, TSP, BA, RC, PC, DP, LSE, and other non-nuclear GO/GOPs). Based on the response to previous comments submitted for Draft 2, Exelon understands that the DSR SDT evaluated the use of the word “source” but dismissed the use in favor of “supply” with the justification “[that] ‘supply’ encompasses all sources”. Exelon again suggests that the word “source” is used as the event criteria in EOP-004-2 as this nomenclature is commonly used in the licensing basis of a nuclear power plant. By revising the threshold criteria to “one or more” Exelon believes the concern the DSR SDT noted is addressed and ensures all sources are addressed. In addition, by revising the threshold for reporting to a loss of “one or more” will ensure that all potential events (regardless of configuration of off-site

power supplies) will be reported by any applicable transmission entity specifically identified in the nuclear plant site specific NPIRs. As previously suggested, Exelon again proposes that the loss of an off-site power source be revised to an “unplanned” loss to account for planned maintenance that is coordinated in advance in accordance with the site specific NPIRs and associated Agreements. This will also eliminate unnecessary reporting for planned maintenance. Although the loss of one off-site power source may not result in a nuclear generating unit trip, Exelon agrees that an unplanned loss of an off-site power source regardless of impact should be reported within the 24 hour time limit as proposed. Suggest that the Loss of Offsite power to a nuclear generating plant event be revised as follows: Event: Unplanned loss of any off-site power source to a Nuclear Power Plant Entity with Reporting Responsibility: The applicable Transmission Entity that owns and/or operates the off-site power source to a Nuclear Power Plant as defined in the applicable Nuclear Plant Interface Requirements (NPIRs) and associated Agreements. Threshold for Reporting: Unplanned loss of one or more off-site power sources to a Nuclear Power Plant per the applicable NPIRs. 3. Attachment 1 Generation loss event criteria Generation loss The ≥ 2000 MW/≥ 1000 MW generation loss criteria do not provide a time threshold or location criteria. If the 2000 MW/1000 MW is intended to be from a combination of units in a single location, what is the time threshold for the combined unit loss? For example, if a large two unit facility in the Eastern Interconnection with an aggregate full power output of 2200 MW (1100 MW per unit) trips one unit (1100 MW) [T=0 loss of 1100 MW] and is ramping back the other unit from 100% power and 2 hours later the other unit trips at 50% power [550 MW at time of trip]. The total loss is 2200 MW; however, the loss was sustained over a 2 hour period. Would this scenario require reporting in accordance with Attachment 1? What if it happened in 15 minutes? 1 hour? 24 hours? Exelon suggests the criteria revised to include a time threshold for the total loss at a single location to provide this additional guidance to the GOP (e.g., within 15 minutes to align with other similar threshold conditions). Threshold for Reporting ≥ 2,000 MW unplanned total loss at a single location within 15 minutes for entities in the Eastern or Western Interconnection ≥ 1000 MW unplanned total loss at a single location within 15 minutes for entities in the ERCOT or Quebec Interconnection 4. Exelon appreciates that the DSR SDT has added the NRC to the list of Stakeholders in the Reporting Process, but does not agree with the SDT response to FirstEnergy’s comment to Question 17 [page 206] that stated “NRC requirements or comments fall outside the scope of this project.” Quite the contrary, this project should be communicated and coordinated with the NRC to eliminate confusion and duplicative reporting requirements. There are unique and specific reporting criteria and coordination that is currently in place with the NRC, the FBI and the JTTF for all nuclear power plants. If an event is in progress at a nuclear facility, consideration should be given to coordinating such reporting as to not duplicate effort, introduce conflicting reporting thresholds, or add unnecessary burden on the part of a nuclear GO/GOP who’s primary focus is to protect the health and safety of the public during a potential radiological sabotage event (as defined by the NRC) in conjunction with potential impact to the reliability of the BES. 5. Attachment 1 Detection of a reportable Cyber Security Incident event criteria The threshold for reporting is “that meets the criteria in CIP-008”. If an entity is exempt from CIP-008, does that mean that this reportable event is therefore also not applicable in accordance with EOP-004-2 Attachment 1?
Individual
Public Utility District No. 1 of Snohomish County
John D. Martinsen
Yes
Yes
Yes
The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. The EOP-004 has an “optional” Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify if both forms will still be required to be submitted. We also need to ensure that there won’t be a duplication of efforts between the two reports. This is fairly minor, but the clarification need should be addressed.
Overarching Concern related to EOP-004-2 draft: The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes, as well as the CIP standards

Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definitions of a BES element could change significantly and Critical Assets may no longer exist. As it relates to the proposed reporting criteria, it is debatable as to whether or not the destruction of, for example, one relay would be a reportable incident under this definition going forward given the current drafting team efforts. Related to "Reportable Events" of Attachment 1: 1. A reportable event is stated as, "Risk to the BES", the threshold for reporting is, "From a non-environmental physical threat". This appears to be a catch-all event, and basically every other event in Attachment 1 should be reported because it is a risk to the BES. Due to the subjectivity of this event, suggest removing it from the list. 2. A reportable event is stated as, "Damage or destruction of Critical Asset per CIP-002". The term "Damage" would have to be defined in order for an entity to determine a threshold for what qualifies as "Damage" to a CA. One could argue that normal "Damage" can occur on a CA that is not necessary to report. There should also be caution here in adding CIP interpretation within this standard. Reporting Thresholds 1. The SDT made attempts to limit nuisance reporting related to copper thefts and so on which is supported. However a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could congest the reporting process with nuisance reporting and reviewing. An example is the "BES Emergency requiring manual firm load shedding of greater than or equal to 100 MW or the Loss of Firm load for ≥ 15 Minutes that is greater than or equal to 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases these low thresholds represent reporting of minor wind events or other seasonal system issues on Local Network used to provide distribution service. Firm Demand 1. The use of Firm Demand in the context of the draft Standards could be used to describe commercial arrangements with a customer rather than a reliability issue. Clarification of Firm Demand would be helpful
Group
MRO NSRF
WILL SMITH
Yes
Yes
Yes
: The MRO NSRF wishes to thank the SDT for incorporating changes that the industry had with reporting time periods and aligning this with the Events Analysis Working Group and Department of Energy's OE 417 reporting form.
Group
Western Electricity Coordinating Council
Steve Rueckert
Yes
Yes
Yes
Results-based standards should include, within each requirement, the purpose or reason for the requirement. The requirements of this standard, while we support the requirements, do not include the goal or proupose of meeting each stated requirement. The Measures all include language stating "the responsible entity shall provide…". During a quality review of a WECC Regional Reliability Standard we were told that the "shall provide" language is essentially another requirement to provide something. If it is truly necessary to provide this it should be in the requirements. It was suggested to us that we drop the "shall provide" language and just start each Measure with the "Evidence may include but is not limited to…".
Individual

RoLynda Shumpert
South Carolina Electric and Gas
Yes
Yes
Yes
In terms of receiving reports, is it the drafting teams expectation that separate reports be developed by both the RC and the TOP, GO, BA, etc. for an event that occurs on a company's system that is within the RC's footprint? One by the RC and one by the TOP, GO, BA, etc. In terms of meeting reporting thresholds, is it the drafting teams expectation that the RC aggregate events within its RC Area to determine whether a reporting threshold has been met within its area for the quantitative thresholds?
Individual
Kathleen Goodman
ISO New England
No
Please see further comments; we do not believe R4 is a necessary requirement in the standard and suggest it be deleted.
No
In accordance with the results-based standards concept, all that is required, for the “what” is that company X reported on event Y in accordance with the reporting requirements in attachment Z of the draft standard. Therefore, we proposed the only requirement that is necessary is R3, which should be re-written to read… "Each Responsible Entity shall report to address the events listed in Attachment 1."
Yes
Attachment 1should be revisited. “Equipment Damage” is overly vague and will also potentially result in reporting on equipment failures which may simply be related to the age and/or vintage of equipment.
Group
Imperial Irrigation District
Jesus Sammy Alcaraz
Yes
Yes
Yes
IID strongly believes the reporting flowchart should not be part of a standard. The suggestion is to replace it with a more clear, right to the point requirement.
Individual
Curtis Crews
Texas Reliability Entity
Substantive comments: 1.ERO and Regional Entities should not be included in the Applicability of this standard. Just because they may be subject to some CIP requirements does not mean they also have to be included here. The ERO and Regional Entities do not operate equipment or systems that are

integral to the operation of the BES. Also, none of the VSLs apply to the ERO or to Regional Entities. 2.The first entry in the Events Table should say “Damage or destruction of BES equipment.” Equipment may be rendered inoperable without being “destroyed,” and entities should not have to determine within one hour whether damage is sufficient to cause the equipment to be considered “destroyed.” Footnote 1 refers to equipment that is “damaged or destroyed.” 3.In the Events Table, consider whether the item for “Voltage deviations on BES facilities” should also be applicable to GOPs, because a loss of voltage control at a generator (e.g. failure of an automatic voltage regulator and power system stabilizer) could have a similar impact on the BES as other reportable items. 4.In the Events Table, under Transmission Loss, does this item require that at least three Facilities owned by one entity must be lost to trigger the reporting requirement, or is the reporting requirement also to be triggered by loss of three Facilities during one event or occurrence that are owned by two or three different entities? 5.In the Events Table, under Transmission Loss, it is unclear how Facilities are to be counted to determine when “three or more” Facilities are lost. In the NERC Glossary, Facility is ambiguously defined as “a set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In many cases, a “set of electrical equipment” can be selected and counted in different ways, which makes this item ambiguous. 6.In the Events Table, under Transmission Loss, it appears that a substation bus failure would only count as a loss of one Facility, even though it might interrupt flow between several transmission lines. We believe this type of event should be reported under this standard, and appropriate revisions should be made to this entry. 7.In the Events Table, under Transmission Loss, consider including generators that are lost as a result of transmission loss events when counting Facilities. For example, if a transmission line and a transformer fail, resulting in a generator going off-line, that should count as a loss of “three or more” facilities and be reportable under this standard. 8.In the Events Table, under “Unplanned Control Center evacuation” and “Loss of monitoring or all voice communication capability,” GOPs should be included. GOPs also operate control centers that would be subject to these kinds of occurrences. 9.In the Events Table, under “Loss of monitoring or all voice communication capability,” we suggest adding that if there is a failure at one control center, that event is not reportable if there is a successful failover to a backup system or control center. 10.“Fuel supply emergency” is included in the Event Reporting Form, but not in Attachment 1, so there is no reporting threshold or deadline provided for this type of event. Clean-up items: 1.In R1.5, capitalize “Responsible Entity” and lower-case “process”. 2.In footnote 1, add “or” before “iii)” to clarify that this event type applies to equipment that satisfies any one of these three conditions. 3.In the Event Reporting Form, “forced intrusion” and “Risk to BES equipment” are run together and should be separated. VSLs: 1.We support the substance of the VSLs, but the repeated long list of entities makes the VSLs extremely difficult to read and decipher. The repeated list of entities should be replaced by “Responsible Entities.” 2.If the ERO and Regional Entities are to be subject to requirements in this standard (which we oppose), they need to be added to the VSLs.
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
Yes
Yes
Yes
ATC appreciates the work of the SDT in incorporating changes that the industry had with reporting time periods and aligning this with the Events Analysis Working Group and Department of Energy’s OE 417 reporting form.
Individual
Anthony Jablonski
ReliabilityFirst

ReliabilityFirst thanks the SDT for their effort on this project. ReliabilityFirst has a number of concerns/questions related to the draft EOP-004-2 standard which include the following: 1. General Comment - The SDT should consider any possible impacts that could arise related to the applicability of Generator Owners that may or may not own transmission facilities. This will help alleviate any potential or unforeseen impacts on these Generator Owners 2. General Comment – Though the rationale boxes contain useful editorial information for each requirement, they should rather contain the technical rationale or answer the question “why is this needed” for each requirement. The rationale boxes currently seem to contain suggestions on how to meet the requirements. ReliabilityFirst suggests possibly moving some of the statements in the “Guideline and Technical Basis” into the rationale boxes, as some of the rationale seems to be contained in that section. 3. General comment – The end of Measure M4 is incorrectly pointing to R3. This should refer to R4. 4. General Comment – ReliabilityFirst recommends the “Reporting Hierarchy for Reportable Events” flowchart should be removed from the “Background” section and put into an appendix. ReliabilityFirst believes the flowchart is not really background information, but an outline of the proposed process found in the new standard. 5. Applicability Comment – ReliabilityFirst questions the newly added applicability for both the Regional Entity (RE) and ERO. Standards, as outlined in many, if not all, the FERC Orders, should have applicability to users, owners and operators of the BES and not to the compliance monitoring entities (e.g. RE and ERO). Any requirements regarding event reporting for the RE and ERO should be dealt with in the NERC Rules of Procedure and/or Regional Delegation Agreements. It is also unclear who would enforce compliance on the ERO if the ERO remains an applicable entity. 6. Requirement Comment - ReliabilityFirst believes the process for communicating events in Requirement R1, Part 1.3 should be all inclusive and therefore include the bullet points. Bullet points are considered to be “OR” statements and thus ReliabilityFirst believes they should be characterized as sub-parts. Listed below is an example: 1.3. A process for communicating events listed in Attachment 1 to the following: 1.3.1 Electric Reliability Organization, 1.3.2 Responsible Entity’s Reliability Coordinator 1.3.3 Internal company personnel 1.3.4 The Responsible Entity’s Regional Entity 1.3.5 Law enforcement 1.3.6 Governmental or provincial agencies 7. Requirement Comment – ReliabilityFirst questions why Requirement R1, Part 1.1 and Part 1.2 are not required to be verified when performing a drill or exercise in Requirement R4? ReliabilityFirst believes that performing a drill or exercise utilizing the process for identifying events (Part 1.1) and the process for gathering information (Part 1.2) are needed along with the verification of the process for communicating events as listed in Part 1.3. 8. Compliance Section Comment – Section 1.1 states “If the Responsible Entity works for the Regional Entity…” and ReliabilityFirst questions the intent of this language. ReliabilityFirst is unaware of any Responsible Entities who work for a Regional Entity. Also, if the Regional Entity and ERO remain as applicable entities, in Section 1.1 of the standard, it is unclear who will act as the Compliance Enforcement Authority (CEA). 9. Compliance Section Comment – ReliabilityFirst recommends removing the second, third and fourth paragraphs from Section 1.2 since ReliabilityFirst believes entities should retain evidence for the entire time period since their last audit. 10. Compliance Section Comment – ReliabilityFirst recommends modifying the fifth paragraph from Section 1.2 as follows: “If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or until a data hold release is issued by the CEA.” ReliabilityFirst believes, as currently stated, the CEA would be required to retain information for an indefinite period of time. 11. Compliance Section Comment – ReliabilityFirst recommends removing the sixth paragraph from Section 1.2 since the requirement for the CEA to keep the last audit records and all requested and submitted subsequent audit records is already covered in the NERC ROP. 12. Attachment 1 Comment – It is unclear what the term/acronym “Tv” is referring to. It may be beneficial to include a footnote clarifying what the term “Tv” stands for. 13. VSL General Comment – although ReliabilityFirst believes that the applicability is not appropriate, as the REs and ERO are not users, owners, or operators of the Bulk Electrcic System, the Regional Entity and ERO are missing from all four sets of VSLs, if the applicability as currently written stays as is. If the Regional Entity and ERO are subject to compliance for all four requirements, they need to be included in the VSLs as well. Furthermore, for consistency with other standards, each VSL should begin with the phrase “The Responsible Entity…” 14. VSL 4 Comment - The second “OR” statement under the “Lower” VSL should be removed. By not verifying the communication process in its Operating Plan within the calendar year, the responsible entity completely missed the intent of the requirement and is already covered under the “Severe” VSL category.
Individual
Don Schmit

Nebraska Public Power District
Yes
Yes
Yes
Although 24 hours is a vast improvement, one business day would make more sense for after the fact reporting.
Individual
Dennis Sismaet
Seattle City Light
Yes
Yes
Yes
The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. The EOP-004 has an “optional” Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify if both forms will still be required to be submitted. We also need to ensure that there won’t be a duplication of efforts between the two reports. This is fairly minor, but the clarification need should be addressed.
Overarching Concern related to EOP-004-2 draft: The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes, as well as the CIP standards Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definitions of a BES element could change significantly and Critical Assets may no longer exist. As it relates to the proposed reporting criteria, it is debatable as to whether or not the destruction of, for example, one relay would be a reportable incident under this definition going forward given the current drafting team efforts. Related to “Reportable Events” of Attachment 1: 1. A reportable event is stated as, “Risk to the BES”, the threshold for reporting is, “From a non-environmental physical threat”. This appears to be a catch-all event, and basically every other event in Attachment 1 should be reported because it is a risk to the BES. Due to the subjectivity of this event, suggest removing it from the list. 2. A reportable event is stated as, “Damage or destruction of Critical Asset per CIP-002”. The term “Damage” would have to be defined in order for an entity to determine a threshold for what qualifies as “Damage” to a CA. One could argue that normal “Damage” can occur on a CA that is not necessary to report. There should also be caution here in adding CIP interpretation within this standard. Reporting Thresholds 1. The SDT made attempts to limit nuisance reporting related to copper thefts and so on which is supported. However a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could congest the reporting process with nuisance reporting and reviewing. An example is the “BES Emergency requiring manual firm load shedding of greater than or equal to 100 MW or the Loss of Firm load for ≥ 15 Minutes that is greater than or equal to 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases these low thresholds represent reporting of minor wind events or other seasonal system issues on Local Network used to provide distribution service. Firm Demand 1. The use of Firm Demand in the context of the draft Standards could be used to describe commercial arrangements with a customer rather than a reliability issue. Clarification of Firm Demand would be helpful
Individual
John Seelke
PSEG
Yes

Yes
Yes
We have several comments: 1. The “Law Enforcement Reporting” section on p. 6 is unclearly written. The first three sentences are excerpted here: “The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement.” The outages described prior to the last sentence are “vandalism and terrorism.” The next sentence states “Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES.” If the SDT intended to only have events reported to law enforcement that could to Cascading, it should state so clearly and succinctly. But other language implies otherwise. a. The footnote 1 on Attachment 1 (p. 20) states: “Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative).” Rendering a relay inoperative may or may not lead to Cascading. b. With regard to “forced intrusion,” footnote 2 on Attachment 1 states: “Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects (sic) the reliability of the BES.” The criterion, or criteria, for reporting an event to law enforcement needs to be unambiguous. The SDT needs to revise this “Law Enforcement Section” so that is achieved. The “law enforcement reporting” criterion, or criteria, should also be added to the flow chart on p. 9. We suggest the following as a starting point for the team to discuss: there should be two criteria for reporting an event to law enforcement: (1) BES equipment appears to have been deliberately damaged, destroyed, or stolen, whether by physical or cyber means, or (2) someone has gained, or attempted to gain, unauthorized access by forced or unauthorized entry (e.g., via a stolen employee keycard badge) into BES facilities, including by physical or cyber means. 2. The use of the terms “communicating events” in R1.3, and the use of the term “communication process” are confusing because in other places such as R3 the term “reporting” is used. If the SDT intends “communicating” to mean “reporting” as that later term is used in R3, it should use the same “reporting” term in lieu of “communicating” or “communication” elsewhere. Inconsistent terminology causes confusion. PSEG prefers the word “reporting” because it is better understood. 3. Attachment 1 needs to more clearly define what is meant by “recognition of an event.” a. When equipment or a facility is involved, it would better state within “X” time (e.g., 1 hour) of “of confirmation of an event by the entity that either owns or operates the Element or Facility.” b. Other reports should have a different specification of the starting time of the reporting deadline clock. For example, in the requirement for reporting a “BES Emergency requiring public appeal for load reduction,” it is unclear what event is required to be reported - the “BES Emergency requiring public appeal” or “public appeal for load reduction.” If the later is intended, then the event should be reported within “24 hours after a public appeal for load reduction is first issued.” These statements need to be reviewed and customized for each event by the SDT so they are unambiguous. In summary, the starting time for the reporting clock to start running should be made clear for each event. This will require that the SDT review each event and customize the starting time appropriately. The phrase “recognition of an event” should not be used because it is too vague. 4. When EOP-004-2 refers to other standards, it frequently omits the version of the standard. Example: see the second and third row of Attachment 1 that refers to “CIP-002.” Include the version on all standards referenced.
Group
Compliance & Responsbility Office
Silvia Parada Mitchell
Yes
See comments in response to Question 4.
Yes
See comments in response to Question 4.
Yes
See comments in response to Question 4.
NextEra Energy, Inc. (NextEra) appreciates the DSR SDT revising proposed EOP-004-2, based on the

previous comments of NextEra and the stakeholders. NextEra, however, believes that EOP-004-2 needs additional refinement prior to approval. R1.3 In R1.3, NextEra is concerned that the term "internal company personnel" is unclear and may be misinterpreted. For example, NextEra does not believe this term should include all company or corporate personnel, or even all personnel in the Responsible Entity's company or business unit. Instead, the definition of personnel should be limited to those who could be directly impacted by the event or are working on the event. Thus, NextEra suggests that the language in R1.3 be revised to read: "Internal Responsible Entity personnel whose tasks require them to take specific actions to mitigate, stop the spread and/or normalize the event, or personnel who are directly impacted by the event." NextEra is concerned that R1.3, as written, will be interpreted differently from company to company, region to region, auditor to auditor, and, therefore, may result in considerable confusion during actual events as well as during the audits/stop checks of EOP-004-2 compliance. Also, in R1.3, NextEra is concerned that many of the events listed in Attachment A already must be reported to NERC under its trial (soon to be final) Event Analysis Reporting requirements (Event Analysis). NextEra believes duplicative and different reporting requirements in EOP-004-2 and the Event Analysis rules will cause confusion and inefficiencies during an actual event, which will likely be counterproductive to promoting reliability of the bulk power system. Thus, NextEra believes that any event already covered by NERC's Event Analysis should be deleted from Attachment 1. Events already covered include, for example, loss of monitoring or all voice, loss of firm load and loss of generation. If this approach is not acceptable, NextEra proposes, in the alternative, that the reporting requirements between EOP-004-2 and Event Analysis be identical. For instance, in EOP-004-2, there is a requirement to report any loss of firm load lasting for more than 15 minutes, while the Event Analysis only requires reporting the of loss of firm load above 300 megawatts and lasting more than 15 minutes. Similarly, EOP-004-2 requires the reporting of any unplanned control center evacuation, while the Event Analysis only requires reporting after the evacuation of the control center that lasted 30 minutes or more. Thus, NextEra requests that either EOP-004-2 not address events that are already set forth in NERC's Event Analysis, or, in the alternative, for those duplicative events to be reconciled and made identical, so the thresholds set forth in the Event Analysis are also used in EOP-004-2. In addition, NextEra believes that a reconciliation between the language "of recognition" in Attachment 1 and "process to identify" in R1.1 is necessary. NextEra prefers that the language in Attachment 1 be revised to read " . . . of the identification of the event under the Responsible Entity's R1.1 process." For instance, the first event under the "Submit Attachment 2 . . . ." column should read: "The parties identified pursuant to R1.3 within 1 hour of the identification of an event under the Responsible Entity's R1.1 process." This change will help eliminate confusion, and will also likely address (and possibly make moot) many of the footnotes and qualifications in Attachment 1, because a Responsible Entity's process will likely require that possible events are properly vetted with subject matter experts and law enforcement, as appropriate, prior to identifying them as "events". Thus, only after any such vetting and a formal identification of an event would the one hour or twenty-four hour reporting clock start to run. R1.4, R1.5, R3 and R4 NextEra is concerned with the wording and purpose of R1.4, R1.5, R3 and R4. For example, R1.4 requires an update to the Operating Plan for ". . . any change in assets, personnel, other circumstances . . . ." This language is much too broad to understand what is required or its purpose. Further, R1.4 states that the Operating Plan shall be updated for lessons learned pursuant to R3, but R3 does not address lessons learned. Although there may be lessons learned during a post event assessment, there is no requirement to conduct such an assessment. Stepping back, it appears that the proposed EOP-004-2 has a mix of updates, reviews and verifications, and the implication that there will be lessons learned. Given that EOP-004-2 is a reporting Standard, and not an operational Standard, NextEra is not inclined to agree that it needs the same testing and updating requirements like EOP-005 (restoration) or EOP-008 (control centers). Thus, it is NextEra's preference that R1.4, R1.5 and R4 be deleted, and replaced with a new R1.4 as follows: R1.4 A process for ensuring that the Responsibly Entity reviews, and updates, as appropriate its Operating Plan at least annually (once each calendar year) with no more than 15 months between reviews. If the DSR SDT does not agree with this approach, NextEra, in the alternative, proposes a second approach that consolidates R1.4, R1.5 and R4 in a new R1.4 as follows: R1.4 A process for ensuring that the Responsibly Entity tests and reviews its Operating Plan at least annually (once each calendar year) with no more than 15 months between a test and review. Based on the test and review, the Operating Plan shall be updated, as appropriate, within 90 calendar days. If an actual event occurs, the Responsible Entity shall conduct a post event assessment to identify any lessons learned within 90 calendar days of the event. If the Responsible Entity identifies any lessons learned in post event assessment, the lessons

learned shall be incorporated in the Operating Plan within 90 calendar days of the date of the final post event assessment. NextEra purposely did not add language regarding “any change in assets, personnel etc,” because that language is not sufficiently clear or understandable for purposes of a mandatory requirement. Although it may be argued that it is a best practice to update an Operating Plan for certain changes, unless the DST SDT can articulate specific, concrete and understandable issues that require an updated Operating Plan prior to an annual review, NextEra recommends that the concept be dropped. Nuclear Specific Concerns EOP-004-2 identifies the Nuclear Regulatory Commission (NRC) as a stakeholder in the Reporting Process, but does not address the status of reporting to the NRC in the Event Reporting flow diagram on page 9. Is the NRC considered Law Enforcement as is presented in the diagram? Since nuclear stations are under a federal license, some of the events that would trigger local/state law enforcement at non-nuclear facilities would be under federal jurisdiction at a nuclear site. There are some events listed in Attachment 1 that seem redundant or out of place. For example, a forced intrusion is a one hour report to NERC. However, if there is an ongoing forced intrusion at a nuclear power plant, there are many actions taking place, with the NRC Operations Center as the primary contact which will mobilize the local law enforcement agency, etc. It is unclear that reporting to NERC in one hour promotes reliability or the resolution of an emergency in progress. Also, is there an ability to have the NRC in an emergency notify NERC? The same concerns related to cyber security events. Procedures versus Plan NextEra also suggests replacing "Operating Plan" with "procedures". Given that EOP-004-2 is a reporting Standard and not an operational Standard, it is typical for procedures that address this standard to reside in other departments, such as Information Management and Security. In other words, the procedures needed to address the requirements of EOP-004-2 are likely broader than the NERC-defined Operating Plan. Clean-Up Items In Attachment 1, Control Centers should be capitalized in all columns so as not to be confused with control rooms. Also, the final product should clearly state that the process flow chart that is set forth before the Standard is for illustrative purposes, so there is no implication that a Registered Entity must implement multiple procedures versus one comprehensive procedure to address different reporting requirements.

Individual

Barry Lawson

NRECA

1. Please ensure that the work of the SDT is done in close coordination with Events Analysis Process (EAP) work being undertaken by the PC/OC and BOT, and with any NERC ROP additions or modifications. NRECA is concerned that the EAP work being done by these groups is not closely coordinated even though their respective work products are closely linked -- especially since the EAP references information in EOP-004. 2. The SDT needs to be consistent in its use of "BES" and "BPS" – boths acronyms are used throughout the SDT documents. NRECA strongly prefers the use of "BES" since that is what NERC standards are written for. 3. Under “Purpose” section of standard, 3rd line, add “BES” between “impact” and “reliability.” Without making this change the "Purpose" section could be misconstrued to refer to reliability beyond the BES. 4. In the Background section there is reference to the Events Analysis Program. Is that the same thing as the Events Analysis Process? Is it something different? Is it referring to a specific department at NERC? Please clarify in order to reduce confusion. Also in the Background section there is reference to the Events Analysis Program personnel. Who is this referring to -- NERC staff in a specific department? Please clarify. 5. In M1 please be specific regarding what “dated” means. 6. In M3 please make it clear that if there wasn’t an event, this measure is not applicable 7. In R4 it is not clear what “verify” means. Please clarify. 8. In Attachment 1 there are references to Critical Asset and Critical Cyber Asset. These terms will likely be eliminated from the NERC Glossary of Terms when CIP V5 moves forward and is ultimately approved by FERC. This could create future problems with EOP-004 if CIP V5 is made effective as currently drafted. 9. In Attachment 1 the one hour timeframe for submitting data for the first 7 items listed is very tight. Other than being required by the EOE)E-417 form, NRECA requests that the SDT provide further support for this timeframe. If there are not distinct reasons why 1 hour is the right timeframe for this, then other timeframes should be explored with DOE. 10. While including Footnote 1 is appreciated, NRECA is concerned that this footnote will create confusion in the compliance and audit areas and request the SDT to provide more definitive guidance to help explain what these "Events"

refer to. NRECA has the same comment on Footnote 2 and 3. Specifically in Footnote 3, how do you clearly determine and audit from a factual standpoint something that “could have damaged” or “has the potential to damage the equiment?” 11. In the Guideline and Technical Basis section, in the 1st bullet, how do you determine, demonstrate and audit for something that “may impact” BES reliability? 12. On p. 28, first line, this sentence seems to state that NERC, law enforcement and other entities – not the responsible entity – will be doing event analysis. My understanding of the current and future Event Analysis Process is that the responsible entity does the event analysis. Please confirm and clarify.
Individual
Terry Harbour
MidAmerican Energy
Yes
Yes
No
MidAmerican Energy agrees with the direction of consolidating CIP-001, EOP-004 and portions of CIP-008. However, we have concerns with some of the events included in Attachment 1 and reporting timelines. EOP-004-2 needs to clearly state that initial reports can be made by a phone call, email or another method, in accordance with paragraph 674 of FERC Order 706. MidAmerican Energy believes draft Attachment 1 expands the scope of what must be reported beyond what is required by FERC directives and beyond what is needed to improve security of the BES. Based on our understanding of Attachment 1, the category of “damage or destruction of a critical cyber asset” will result in hundreds or thousands of small equipment failures being reported to NERC and DOE, with no improvement to security. For example, hard drive failures, server failures, PLC failures and relay failures could all meet the criteria of “damage or destruction of a critical cyber asset.” We recommend replacing Attachment 1 and Attachment 2 with the categories and timeframes that are listed in OE-417. This eliminates confusion between government requirements in OE-417 and NERC standards. Reporting timelines and reporting form FERC Order 706, paragraph 676, directed NERC to require a responsible entity to “at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.” In paragraph 674, FERC stated that the Commission agrees that, in the “aftermath of a cyber attack, restoring the system is the utmost priority.” They clarified: “the responsible entity does not need to initially send a full report of the incident…To report to appropriate government authorities and industry participants within one hour, it would be sufficient to simply communicate a preliminary report, including the time and nature of the incident and whatever useful preliminary information is available at the time. This could be accomplished by a phone call or another method.” While FERC did not order completion of a full report within one hour in Order 706, the draft EOP-004 Attachment 1 appears to require submittal of formal reports within one hour for six of the categories, unless there have been “certain adverse conditions” (in which case, as much information as is available must be submitted at the time of notification). The Violation Severity Levels are extreme for late submittal of a report. For example, it would be a severe violation to submit a report more than three hours following an event for an event requiring reporting in one hour. MidAmerican Energy suggests incorporating the language from FERC Order 706, paragraph 674, into the EOP-004 reporting requirement to allow preliminary reporting within one hour to be done through a phone call or another method to allow the responsible entity to focus on recovery and/or restoration, if needed. MidAmerican Energy agrees with the use of DOE OE-417 for submittal of the full report of incidents under EOP-004 and CIP-008. We would note there are two parts to this form -- Schedule 1-Alert Notice, and Schedule 2-Narrative Description. Since OE-417 already requires submittal of a final report that includes Schedule 2 within 48 hours of the event, MidAmerican Energy believes it is not necessary to include a timeline for completion of the final report within the EOP-004 standard. We would note that Schedule 2 has an estimated public reporting burden time of two hours so it is not realistic to expect Schedule 2 to be completed within one hour. Events included in Attachment 1: MidAmerican Energy believes draft Attachment 1 expands the scope of what must be reported beyond what is required by FERC directives and beyond what is needed to improve security of the BES. The categories listed in Attachment 1 with one-hour reporting timelines cause the greatest concern. None

of these categories are listed in OE-417, and all but the last row would not be considered a Cyber Security Incident under CIP-008, unless there was malicious or suspicious intent.

MidAmerican proposes eliminating the phrase “with no more than 15 months between reviews” from R1.5. While we agree this is best practice, it creates the need to track two conditions for the review, eliminates flexibility for the responsible entity and does not improve security to the Bulk Electric System. There has not been a directive from FERC to specify the definition of annual within the standard itself. In conjunction with this comment, the Violation Severity Levels for R4 should be revised to remove the references to months.

Group

ACES Power Marketing Standards Collaborators

Jean Nitz

No

We understand and agree there should be verification of the information required for such reporting (contact information, process flow charts, etc). But we still believe improvements can be made to the draft standard, in particular to requirement R4. The use of the words “or through a drill or exercise” still implies that training is required if no actual event has occurred. When you conduct a fire “drill” you are training your employees on evacuation routes and who they need to report to. Not only are you verifying your process but you are training your employees as well. It is imperative that the information in the Event Reporting process is correct but we don't agree that performing a drill on the process is necessary. We recommend modifying the requirement to focus on verifying the information needed for appropriate communications on an event. And we agree this should take place at least annually.

No

Requirement R2 requires Responsible Entities to implement the various sub-requirements in R1. We believe it is unnecessary to state that an entity must implement their Operating Plan in a separate requirement. Having a separate requirement seems redundant. If the processes in the Operating Plan are not implemented, the entity is non-compliant with the standard. There doesn’t need to be an extra requirement saying entities need to implement their Operating Plan.

Yes

For many of the events listed in Attachment 1, there would be duplicate reporting the way it is written right now. For example, in the case of a fire in a substation (Destruction of BES equipment), the RC, BA, TO, TOP and perhaps the GO and GOP could all experience the event and each would have to report on it. This seems quite excessive and redundant. We recommend eliminating this duplicate reporting.

Individual

Thad Ness

American Electric Power

Yes

No

AEP prefers to avoid requirements that are purely administrative in nature. Requirements should be clear in their actions of supporting of the BES. For example, we would prefer requirements which state what is to be expected, and allowing the entities to develop their programs, processes, and procedures accordingly. It has been our understanding that industry, and perhaps NERC as well, seeks to reduce the amount to administrative (i.e. document-based) requirements. We are confident that the appropriate documentation and administrative elements would occur as a natural course of implementing and adhering to action-based requirements. In light of this perspective, we believe that that R1 and R2 is not necessary, and that R3 would be sufficient by itself. Our comments above notwithstanding, AEP strongly encourages the SDT to consider that R2 and R3, if kept, be merged into a single requirement as a violation of R2 would also be a violation of R3. Two violations would then occur for what is essentially only a single incident. Rather than having both R2 and R3, might R3 be sufficient on its own? R2 is simply a means to an end of achieving R3. If there is a need to explicitly reference implementation, that could be addressed as part of R1. For example, R1 could

state “Each Responsible Entity shall implement an Operating Plan that includes...” R1 seems disjointed, as subparts 1.4 and 1.5 (updating and reviewing the Operating Plan) do not align well with subparts 1.1 through 1.3 which are process related. If 1.4 and 1.5 are indeed needed, we recommend that they be a part of their own requirement(s). Furthermore, the action of these requirements should be changed from emphasizing provision(s) of a process to demonstrating the underlying activity. 1.4: AEP is concerned by the vagueness of requiring provision(s) for updating the Operating Plan for “changes”, as such changes could occur frequently and unpredictably.
Yes
M4: Recommend removing the text “for events” so that it instead reads “The Responsible Entity shall provide evidence that it verified the communication process in its Operating Plan created pursuant to Requirement R1, Part 1.3.” R4: It is not clear to what extent the verification needs to be applied if the process used is complex and includes a variety of paths and/or tasks. The draft team may wish to consider changing the wording to simply state ”each Responsible Entity shall test each of the communication paths in the operating plan”. We also recommend dropping “once per calendar year” as it is inconstant with the measure itself which allows for 15 months.
Individual
Guy Andrews
Georgia System Operations Corporation
Yes
Yes
Yes
The ERO and the Regional Entity should not be listed as Responsible Entities. The ERO and the Regional Entity should not have to meet the requirements of this standard, especially reporting to itself. Attachment 1 (all page numbers are from the clean draft): Page 20, destruction of BES equipment: part iii) of the footnote adds damage as an event but the heading is for destruction. Is it just for destruction? Or is it for damage or destruction? Page 21, Risk to BES equipment: Footnote 3 gives an example where there is flammable or toxic cargo. These are environmental threats. However, the threshold for reporting is for non-environmental threats. Which is it? Page 21, BES emergency requiring public appeal for load reduction: A small deficient entity within a BA may not initiate public appeals. The BA is typically the entity which initiates public appeals when the entire BA is deficient. The initiating entity should be the responsible entity not the deficient entity. Page 21, BES emergency requiring manual firm load shedding: If a RC directs a DP to shed load and the DP initiates manually shedding its load as directed, is the RC the initiating entity? Or is it the DP? Page 22, system separation (islanding): a DP does not have a view of the system to see that the system separated or how much generation and load are in the island. Remove DP. Attachment 2 (all page numbers are from the clean draft): Page 25: fuel supply emergencies will no longer be reportable under the current draft. Miscellaneous typos and quality issues (all page numbers are from the clean draft): Page 5, the last paragraph: There are two cases where Parts A or B are referred to. Attachment 1 no longer has two parts (A & B). Page 27, Discussion of Event Reporting: the second paragraph has a typo at the beginning of the sentence.
Group
Florida Municipal Power Agency
Frank Gaffney
No
First, we wish to thank the SDT for their hard work and making significant progress in significant improvements in the standard. We commend the direction that the SDT is taking. There are; however, a few unresolved issues that cause us to not support the standard at this time. An issue of possible differences in interpretation between entities and compliance monitoring and enforcement is the phrase in 1.3 that states “the following as appropriate”. Who has the authority to deem what is appropriate? The requirements should be clear that the Responsible Entity is the decision maker of

who is appropriate, otherwise there is opportunity for conflict between entities and compliance. In addition, 1.4 is onerous and burdensome regarding the need to revise the plan within 90 days of "any" change, especially considering the ambiguity of "other circumstances". "Other circumstances" is open to interpretation and a potential source of conflict.

No

Both requirements are to implement the Operating Plan. Hence, R3 should be a bullet under R2 and not a separate requirement. In addition, for R2, the phrase "actual event" is ambiguous and should mean: "actual event that meets the criteria of Attachment 1" We suggest the following wording to R2 (which will result in eliminating R3) "Each Responsible Entity shall implement its Operating Plan: • For actual events meeting the threshold criteria of Attachment 1 in accordance with Requirement R1 parts 1.1, 1.2 and 1.3 • For review and updating of the Operating Plan in accordance with Requirement R1 parts 1.4 and 1.5" Note that we believe that if the SDT decides to not combine R2 and R3, then we disagree with the distinction between the two requirements. The division of implementing R1 through R2 and R3 as presented is "implementing" vs. "reporting". We believe that the correct division should rather be "implementation" of the plan (which includes reporting) vs. revisions to the plan.

No

The times don't seem aggressive enough for some of the Events related to generation capacity shortages, e.g., we would think public appeal, system wide voltage reduction and manual firm load shedding ought to be within an hour. These are indicators that the BES is "on the edge" and to help BES reliability, communication of this status is important to Interconnection-wide reliability.

The Rules of Procedure language for data retention (first paragraph of the Evidence Retention section) should not be included in the standard, but instead referred to within the standard (e.g., "Refer to Rules of Procedure, Appendix 4C: Compliance Monitoring and Enforcement Program, Section 3.1.4.2 for more retention requirements") so that changes to the RoP do not necessitate changes to the standard. In R4, it might be worth clarifying that, in this case, implementation of the plan for an event that does not meet the criteria of Attachment 1 and going beyond the requirements R2 and R3 could be used as evidence. Consider adding a phrase as such to M4, or a descriptive footnote that in this case, "actual event" may not be limited to those in Attachment 1. Comments to Attachment 1 table: On "Damage or destruction of Critical Asset" and "… Critical Cyber Asset", Version 5 of the CIP standards is moving away from the binary critical/non-critical paradigm to a high/medium/low risk paradigm. Suggest adding description that if version 5 is approved by FERC, that "critical" would be replaced with "high or medium risk", or include changing this standard to the scope of the CIP SDT, or consider posting multiple versions of this standard depending on the outcome of CIP v5 in a similar fashion to how FAC-003 was posted as part of the GO/TO effort of Project 2010-07. On "forced intrusion", the phrase "at BES facility" is open to interpretation as "BES Facility" (e.g., controversy surrounding CAN-0016) which would exclude control centers and other critical/high/medium cyber system Physical Security Perimeters (PSPs). We suggest changing this to "BES Facility or the PSP or Defined Physical Boundary of critical/high/medium cyber assets". This change would cause a change to the applicability of this reportable event to coincide with CIP standard applicability. On "Risk to BES equipment", that phrase is open to too wide a range of interpretation; we suggest adding the word "imminent" in front of it, i.e., "Imminent risk to BES equipment". For instance, heavy thermal loading puts equipment at risk, but not imminent risk. Also, "non-environmental" used as the threshold criteria is ambiguous. For instance, the example in the footnote, if the BES equipment is near railroad tracks, then trains getting derailed can be interpreted as part of that BES equipment's "environment", defined in Webster's as "the circumstances, objects, or conditions by which one is surrounded". It seems that the SDT really means "non-weather related", or "Not risks due to Acts of Nature". On "public appeal", in the threshold, the descriptor "each" should be deleted, e.g., if a single event causes an entity to be short of capacity, do you really want that entity reporting each time they issue an appeal via different types of media, e.g., radio, TV, etc., or for a repeat appeal every several minutes for the same event? Should LSE be an applicable entity to "loss of firm load"? As proposed, the DP is but the LSE is not. In an RTO market, will a DP know what is firm and what is non-firm load? Suggest eliminating DP from the applicability of "system separation". The system separation we care about is separation of one part of the BES from another which would not involve a DP. On "Unplanned Control Center Evacuation", CIP v5 might add GOP to the applicability, another reason to add revision of EOP-004-2 to the scope of the CIP v5 drafting team, or in other ways coordinate this SDT with that SDT. Consider posting a couple of versions of the standard depending on the outcome of CIP v5 in a similar fashion to the multiple versions of FAC-003 posted with the Go/TO effort of

Project 2010-07.
Individual
Ed Davis
Entergy Services
Entergy agrees with and supports comments submitted by the SERC OC Standards Review group.
Individual
Margaret McNaul
Thompson Coburn LLP on behalf of Miss. Delta Energy Agency
The first three incident categories designated on Attachment 1 as reportable events should be modified. As the Standard is current drafted, each incident category (i.e., destruction of BES equipment, damage or destruction of Critical Assets, and damage or destruction of Critical Cyber Assets) requires reporting if the event was due to unintentional human action. For example, under the reporting criteria as drafted, inadvertently dropping and damaging a piece of computer equipment designated as a Critical Cyber Asset while moving or installing it would appear to require an event report within an hour of the incident. MDEA requests that the Drafting Team consider modifying footnote 1 and each of the first three event categories to reflect that reportable events include only those that (i) affect an IROL; (ii) significantly affect the reliability margin of the system; or (iii) involve equipment damage or destruction due to intentional human action that results in the removal of the BES equipment, Critical Assets, and/or Critical Cyber Assets, as applicable, from service. Footnote 2 (which now pertains only to the fourth incident category – forced intrusions) should also apply to the first three event categories. Specifically, responsible entities should report intentional damage or destruction of BES equipment, damage or destruction of Critical Assets, and damage or destruction of Critical Cyber Assets if either the damage/destruction was clearly intentional or if motivation for the damage or destruction cannot reasonably be determined and the damage or destruction affects the reliability of the BES. Attachment 1 is also unclear to the extent that the incident category involving reports for the detection of reportable Cyber Security Incidents includes a reference to CIP-008 as the reporting threshold. While entities in various functional categories (i.e., RCs, BAs, TOPs/TOs, GOPs/GOs, and DPs) are listed as being responsible for the reporting of such events, some entities in these functional categories may not currently be subject to CIP-008. If it is the Drafting Team's intent to limit event reports for Cyber Security Incidents to include only registered entities subject to CIP-008, that clarification should be incorporated into the listing of entities with reporting responsibility for this incident category in Attachment 1.
Group
Santee Cooper
Terry L. Blackwell
Yes
Yes
Yes
The on-going development of the definition of the BES could have significant impacts on reporting requirements associated with this standard. The event titled "Risk to the BES" appears to be a catch-all event and more guidance needs to be provided on this category. The event titled "Damage or Destruction of a Critical Asset or Critical Cyber Asset per CIP-002" is ambiguous and further guidance is recommended. Ambiguity in a standard leaves it open to interpretation for all involved.
Group

Sacramento Municipal Utility District (SMUD)
Joe Tarantino
Yes
Yes
Yes
SMUD and BANC agree with the revised language in EOP-004-1 requirements, but we have identified the following issues in A-1: We commend the SDT for properly addressing the sabotage issue. However, additional confusion is caused by introducing term "damage". As "damage" is not a defined term it would be beneficial for the drafting team to provide clarification for what is meant by "damage". The threshold for reporting "Each public Appeal for load reduction" should clearly state the triggering is for the BES Emergency as routine "public appeal" for conservation could be considered a threshold for the report triggering. Regarding the SOL Violations in Attachment 1 the SOL Violations should only be those that affect the WECC paths. The SDT made attempts to limit nuisance reporting related to copper thefts and so on which is supported. However a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could congest the reporting process with nuisance reporting and reviewing.
Individual
Bob Thomas
Illinois Municipal Electric Agency
No
IMEA agrees with the removal of the training requirement, but also believes verification is not a necessary requirement for this standard; therefore, R4 is not necessary and should be removed.
No
R2 is not necessary, and should be removed. Subrequirement R1.4 is also not necessary and should be removed.
Yes
With the understanding this is within 24 hrs., and good professional judgment determines the amount of time to report the event to appropriate parties.
IMEA appreciates this opportunity to comment. IMEA appreciates the SDT's efforts to simplify reporting requirements by combining CIP-001 with EOP-004. [IMEA encourages NERC to continue working towards a one-stop-shop to simplify reporting on ES-ISAC.] IMEA supports, and encourages SDT consideration of, comments submitted by APPA and Florida Municipal Power Agency.
Individual
Kirit Shah
Ameren
No
The current language in the parenthesis of R4 suggests that the training requirement was actually not removed, in that "a drill or exercise" constitutes training. As documented in the last sentence of the Summary of Key Concepts section, "The proposed standard deals exclusively with after-the-fact reporting." We feel that training, even if it is called drills or exercises is not necessary for an after-the-fact report.
No
(1) The new wording while well intentioned, effectively does not add clarity and leads to confusion. From our perspective, R1, which requires and Operating Plan, which is defined by the NERC glossary as: "A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan." (2) Is not a proper location for an after-the-fact reporting standard? In fact it could be argued that after-the-fact reports in and of themselves do not affect the reliability of the bulk

electric system. (3) But considering the proposed standard as written with the Operating Plan in requirement R1, and implementation of the Operating Plan in requirement R2 (except the actual reporting which is in R3) and then R3 which requires implementing the reporting section R1.3, it is not clear how these requirements can be kept separate in either implementation nor by the CEA. (4) The second sentence in the second paragraph of “Rationale for R1” states: “The main issue is to make sure an entity can a) identify when an event has occurred and b) be able to gather enough information to complete the report.” This is crucial for a Standard like this that is intended to mandate actions for events that are frequently totally unexpected and beyond normal planning criteria. This language needs to be added to Attachment 1 by the DSR SDT as explained in the rest of our comments

No

(1)By our count there are still six of the nineteen events listed with a one hour reporting requirement and the rest are all within 24 hour after the occurrence (or recognition of the event). This in our opinion, is reporting in real-time, which is against one of the key concepts listed in the background section:"The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting." (2)We believe the earliest preliminary report required in this standard should at the close of the next business day. Operating Entities, such as the RC, BA, TOP, GOP, DP, and LSE should not be burdened with unnecessary after-the-fact reporting while they are addressing real-time operating conditions. Entities should have the ability to allow their support staff to perform this function during the next business day as needed. We acknowledge it would not be an undue burden to cc: NERC on other required governmental reports with shorter reporting timeframes, but NERC should not expand on this practice. (3)We agree with the extension in reporting times for events that now have 24 hours of reporting time. As a GO there are still too many potential events that still require a 1 hour reporting time that is impractical, unrealistic and could lead to inappropriate escalation of normal failures. For example, the sudden loss of several control room display screens for a BES generator at 2 AM in the morning, with only 1 hour to report something, might be mistakenly interpreted as a cyber-attack. The reality is most likely something far more mundane such as the unexpected failure of an instrument transformer, critical circuit board, etc.

Yes. We have the other comments as follow: (1) The "EOP-004 Attachment 1: Events Table" is quite lengthy and written in a manner that can be quite subjective in interpretation when determining if an event is reportable. We believe this table should be clear and unambiguous for consistent and repeatable application by both reliability entities and a CEA. The table should be divided into sections such as: 9a) Events that affect the BES that are either clearly sabotage or suspected sabotage after review by an entity's security department and local/state/federal law enforcement.(b) Events that pose a risk to the BES and that clearly reach a defined threshold, such as load loss, generation loss, public appeal, EEAs, etc. that entities are required to report by the end of the next business day.(c) Other events that may prove valuable for lessons learned, but are less definitive than required reporting events. These events should be reported voluntarily and not be subject to a CEA for non-reporting.(d)Events identified through other means outside of entity reporting, but due to their nature, could benefit the industry by an event report with lessons learned. Requests to report and perform analysis on these type of events should be vetted through a ERO/Functional Entity process to ensure resources provided to this effort have an effective reliability benefit. (2)Any event reporting shall not in any manner replace or inhibit an Entity's responsibility to coordinate with other Reliability Entities (such as the RC, TOP, BA, GOP as appropriate) as required by other Standards, and good utility practice to operate the electric system in a safe and reliable manner. (3) The 1 hour reporting maximum time limit for all GO events in Attachment 1 should be lengthened to something reasonable – at least 24 hours. Operators in our energy centers are well-trained and if they have good reason to suspect an event that might have serious impact on the BES will contact the TOP quickly. However, constantly reporting events that turn out to have no serious BES impact and were only reported for fear of a violation or self-report will quickly result in a cry wolf syndrome and a great waste of resources and risk to the GO and the BES. The risk to the GO will be potential fines, and the risk to the BES will be ignoring events that truly have an impact of the BES.(4)The 2nd and 3rd Events on Attachment 1 should be reworded so they do not use terms that may have been deleted from the NERC Glossary by the time FERC approves this Standard. (5) The terms “destruction” and “damage” are key to identifying reportable events. Neither has been defined in the Standard. The term

destruction is usually defined as 100% unusable. However, the term damage can be anywhere from 1% to 99% unusable and take anywhere from 5 minutes to 5 months to repair. How will we know what the SDT intended, or an auditor will expect, without additional information? (6)We also do not understand why “destruction of BES equipment” (first item Attachment 1, first page) must be reported < 1 hour, but “system separation (islanding) > 100 MW” (Attachment 1, page 3) does not need to be reported for 24 hours. (7)The first 2 Events in Attachment 1 list criteria Threshold for Reporting as “…operational error, equipment failure, external cause, or intentional or unintentional human action.” The term “intentional or unintentional human action” appears to cover “operational error” so these terms appear redundant and create risk of misreporting. Can this be clarified? (8)The footnote of the first page of Attachment 1 includes the explanation “…ii) Significantly affects the reliability margin of the system…” However, the GO is prevented from seeing the system and has no idea what BES equipment can affect the reliability margin of the system. Can this be clarified by the SDT? (9) The use of the term “BES equipment” is problematic for a GO. NERC Team 2010-17 (BES Definition) has told the industry its next work phase will include identifying the interface between the generator and the transmission system. The 2010-17 current effort at defining the BES still fails to clearly define whether or not generator tie-lines are part of the BES. In addition, NERC Team 2010-07 may also be assigned the task of defining the generator/transmission interface and possibly whether or not these are BES facilities. Can the SDT clarify the use of this term? For example, does it include the entire generator lead-line from the GSU high-side to the point of interconnection? Does it include any station service transformer supplied from the interconnected BES?
Individual
Linda Jacobson-Quinn
FEUS
Yes
Yes
No
The OE-417 requires several of the events listed in Attachment 1 be reported within 1 hour. FEUS recommends the drafting team review the events and the OE-417 form and align the reporting window requirements. For example, public appeals, load shedding, and system seperation have a 1 hour requirement in OE-417.
R4 requires verification through a drill or exercise the communication process created as part of R1.3. Clarification of what a drill or exercise should be considered. In order to show compliance to R4 would the entity have to send a pseudo event report to Internal Personnel, the Regional Entity, NERC ES-ISAC, Law Enforcement, and Governmental or provincial agencies listed in R1.3 to verify the communications plan? It would not be a burden on the entity so much, however, I’m not sure the external parties want to be the recipient of approximately 2000 psuedo event reports annually. Attachment 1: BES equipment is too vague – consider changing to BES facility and including that reduces the reliability of the BES in the footnote. Is the footnote an and or an or? Attachment 1: Version 5 of CIP Requirements remove the terms Critical Asset and Critical Cyber Asset. The drafting team should consider revising the table to include BES Cyber Systems. Clarify if Damage or Destruction is physical damage (aka – cyber incidents would be part of CIP-008.) Attachment 1: Unplanned Control Center evacuation – remove “potential” from the reporting responsibility Attachment 2 – 3: change to, “Did the event originate in your system?” The requirement only requires reporting for Events – not potential events. Attachment 2 4: “Damage or Destruction to BES equipment” should be “Destruction of BES Equipment” like it is in Attachment 1 and “forced intrusion risk to BES equipment” remove “risk”
Individual
Tom Foreman
Lower Colorado River Authority
Yes
Yes

Yes
The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. EOP-004 has an “optional” Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify whether Registered Entities will still be required to submit both forms. Please also ensure there will not be duplication of efforts between the two reports. Although this is fairly minor, the clarification should be addressed.
Overarching Concern related to EOP-004-2 draft: The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes and CIP Standards Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definition of a BES element could change significantly and the concepts of “Critical Assets” and “Critical Cyber Assets” no longer exist in Version 5 of the CIP Standards. Additionally, it is debatable whether the destruction of, for example, one relay would be a reportable incident given the proposed language. Related to “Reportable Events” of Attachment 1: 1. The “Purpose” section of the Standard indicates it is designed to require the reporting of events “with the potential to impact reliability” of the BES. Footnote 1 and the “Threshold for Reporting” associated with the Event described as “Destruction of BES equipment” expand the reporting scope beyond that intent. For example, a fan on a generation unit can be destroyed because s plant employee drops a screwdriver into it. We believe such an event should not be reportable under EOP-004-2. Yet, as written, a Responsible Entity could interpret that event as reportable (because it would be “unintentional human action” that destroyed a piece of equipment associated with the BES). If the goal of the SDT was to include such events, we think the draft Standard goes too far in requiring reporting. If the SDT did not intend to include such events, the draft Standard should be revised to make that fact clear. 2. Item iii) in Footnote 1 seems redundant with the Threshold for Reporting. 3. The word “Significantly” in item ii) of footnote 1 introduces an element of subjectivity. What is “significant” to one person may not be significant to someone else. 4. The word “unintentional” in Item iii) of footnote 1 may introduce nuisance reporting. The SDT should consider: (1) changing the Event description to “Damage or destruction of BES equipment” (2) removing the footnote and (3) replacing the existing “Threshold for Reporting” with the following language: “Initial indication the event: (i) was due to intentional human action, (ii) affects an IROL or (iii) in the opinion of the Responsible Entity, jeopardizes the reliability margin of the system (e.g., results in the need for emergency actions)” 5. One reportable event is, “Risk to the BES” and the threshold for reporting is, “From a non-environmental physical threat.” This appears to be intended as a catch-all reportable event. Due to the subjectivity of this event description, we suggest removing it from the list. 6. One reportable event is, “Damage or destruction of Critical Asset per CIP-002.” The SDT should define the term “Damage” in order for an entity to determine a threshold for what qualifies as “Damage” to a CA. Normal “damage” can occur on a CA that should not be reportable (e.g. the screwdriver example, above). 7. For the event called “BES Emergency requiring public appeal for load reduction,” the SDT should make it clear who should report such an event. For example, in the ERCOT Region, there is a requirement that ERCOT issue public appeals for load reduction (See ERCOT Protocols Section 6.5.9.4). As the draft of EOP-004-2 is currently written, every Registered Entity in the ERCOT Region would have to file a report when ERCOT issues such an appeal. Such a requirement is overly burdensome and does not enhance the reliability of the BES. The Standard should require that the Reliability Coordinator file a report when it issues a public appeal to reduce load. Reporting Thresholds 1. See Paragraph 1 in the “Related to “Reportable Events” of Attachment 1” section, above. 2. We believe damage or destruction of Critical Assets or CCAs resulting from operational error, equipment failure or unintentional human action should not be reportable under this Standard. We recommend changing the thresholds for “Damage or destruction to Critical Assets …” and “Damage or destruction of a [CCA]” to “Initial Indication the event was due to external cause or intentional human action.” 3. We support the SDT’s attempted to limit nuisance reporting related to copper thefts. However, a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could clog the reporting process with nuisance reporting and reviewing. An example is the “BES Emergency requiring manual firm load shedding” of ≥ 100 MW or “Loss of Firm load for ≥ 15 Minutes” that is ≥ 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases, those low thresholds would require reporting minor wind events or other seasonal system issues on a local network used to provide distribution service. Firm Demand 1. The use of the term “Firm load” in the context of the

draft Standard seems inappropriate. “Firm load” is not defined in the NERC Glossary (although “Firm Demand” is defined). If the SDT intended to use “Firm Demand,” they should revise the draft Standard. If the SDT wishes to use the term “Firm load” they should define it. [For example, we understand that some load agrees to be dropped in an emergency. In fact, in the ERCOT Region, we have a paid service referred to as “Emergency Interruptible Load Service” (EILS). If the SDT intends that “Firm load” means load other than load which has agreed to be dropped, it should make that fact clear.] Comments to Attachment 2 1. The checkbox for “fuel supply emergency” should be deleted because it is not listed as an Event on Attachment 1. 2. There should be separation between “forced intrusion” and “Risk to BES equipment.” They are separate Events on Attachment 1. Comments to Guideline and Technical Basis The last paragraph appears to state NERC will accept an OE-417 form as long as it contains all of the information required by the NERC form and goes on to state the DOE form “may be included or attached to the NERC report.” If the intent is for NERC to accept the OE-417 in lieu of the NERC report, this paragraph should be clarified.
Individual
Richard Salgo
NV Energy
Yes
Thankyou for responding to the stakeholder comments on this issue.
No
On my read of the Standard, R2 and R3 appear to be duplicative, and I can't really distinguish the difference between the two. The action required appears to be the same for both requirements. Even the Measures for these two sound similar. It is not clear to me what it means to "implement" other than to have evidence of the existence and understanding of roles and responsibilities under the "Operating Plan." I suggest elimination of R2 and inclusion of a line item in Measure 1 calling for evidence of the existence of an "Operating Plan" including all the required elements in R1.
Yes
Attachment 1 includes an item "Detection of a reportable cyber security incident." The reporting requirement is a report via Attachment 2 or the OE417 report form submittal. However, under CIP-008, to which this requirement is linked, the reporting is accomplished via NERC's secure CIPIS reporting tool. This appears to be a conflict in that the entity is directed to file reporting under CIP-008 that differs from this subject standard. Attachment 1 also includes a provision for reporting the "loss of firm load greater than or equal to 15 minutes in an amount of 200MW (or 300MW for peaks greater than 3000MW). This appears to be a rather low threshold, particularly in comparison with the companion loss of generation reporting threshold elsewhere in the attachment. The volume of reports triggered by this low threshold will likely lead to an inordinate number of filed reports, sapping NERC staff time and deflecting resources from more severe events that require attention. I suggest either an increase in the threshold, or the addition of the qualifier "caused by interruption/loss of BES facilities" in this reporting item. This qualifier would therefore exclude distribution-only outages that are not indicative of a BES reliability issue.
Group
SPP Standards Review Group
Robert Rhodes
Yes
Yes
No
The purpose of the reporting requirement should be clear either in the text of the requirements or through an explanation that is embodied in the language of the approved set of standards. This would be consistent with a “Results-based” architecture. What is lacking in the proposed language of this standard is recognition that registered entities differ in size and relevance of their impact on the Bulk Electric System. Also, events that are reportable differ in their impact on the registered entity. A “one-size fits all” approach to this standard may cause smaller entities with low impact on the grid to

take extraordinary measures to meet the reporting/timing requirements and yet be too “loose” for larger more sophisticated and impacting entities to meet the same requirements. Therefore, we believe language of the standard must clearly state the intent that entities must provide reports in a manner consistent with their capabilities from a size/reliability impact perspective and from a communications availability perspective. Timing requirements should allow for differences and consider these variables. Also, we would suggest including language to specifically exclude situations where communications facilities may not be available for reporting. For example, in situations where communications facilities have been lost, initial reports would be due within 6 hours of the restoration of those communication facilities. We would also suggest that Attachment 1 be broken into two distinct parts such that those events which must be reported within 1 hour standout from those events that have to be reported within 24 hours.

The inclusion of optional entities to which to report events in R1.3 introduces ambiguity into the standard that we feel needs to be eliminated. We propose the following replacement language for R1.3: A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity’s Reliability Coordinator and the Responsible Entity’s Regional Entity. We would also propose to incorporate the law enforcement and governmental or provincial agencies mentioned in R1.3 in Attachment 1 by adding them to the existing language for each of the event cells. For example, the first cell in that column would read: The parties identified pursuant to R1.3 and applicable law enforcement and governmental or provincial agencies within 1 hour of recognition of event. Similarly, the phrase ‘…and applicable law enforcement and governmental or provincial agencies…’ should be inserted in all the remaining cells in the 4th column.

Individual

Nathan Mitchell

American Public Power Association

Yes

APPA agrees that removal of the training requirement was an appropriate revision to limit the burden on small registered entities. However, APPA requests clarification from the SDT on the current draft of R4. If no event occurs during the calendar year, a drill or exercise of the Operating Plan communication process is required. APPA believes that if this drill or exercise is required, then it should be a table top verification of the internal communication process such as verification of phone numbers and stepping through a Registered Entity specific scenario. This should not be a full drill with requirements to contact outside entities such as law enforcement, NERC, the RC or other entities playing out a drill scenario. This full drill would be a major burden for small entities.

Yes

No

APPA echoes the comments made by Central Lincoln: We do not believe the SDT has adequately addressed the FERC Order to “Consider whether separate, less burdensome requirements for smaller entities may be appropriate.” The one and 24 hour reporting requirements continue to be burdensome to the smaller entities that do not maintain 24/7 dispatch centers. The one hour reporting requirement means that an untimely “recognition” starts the clock and reporting will become a higher priority than restoration. The note regarding adverse conditions does not help unless we were to consider the very lack of 24/7 dispatch to be such a condition. APPA recommends the SDT evaluate a less burdensome requirement for smaller entities with reporting requirements in Attachment 1. This exception needs to address the fact that not all entities have 24 hour 7 day a week operating personnel. However, APPA cautions the SDT that changes to this standard may expose entities to reporting violations on DOE-OE-417 which imposes civil and criminal penalties on reporting events to the Department of Energy. APPA recommends that the SDT reach out to DOE for clarification of reporting requirements for DOE-OE-417 for small entities, asking DOE to change their reporting requirement to match EOP-004-2. If DOE cannot change their reporting requirement the SDT should provide an explanation in the guidance section of Reliability Standard EOP-004-2 that addresses these competing FERC/DOE directives.

Requirement R1: 1.3. A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity’s Reliability Coordinator and the following as appropriate: • Internal company personnel • The Responsible Entity’s Regional Entity • Law enforcement • Governmental or provincial agencies APPA believes that including the list of other

entities needing to be included in a process for communicating events under 1.3 may open this requirement up for interpretation. APPA requests that the SDT remove from the requirement the listing of; “Internal company personnel, The Responsible Entity’s Regional Entity, Law enforcement & Governmental or provincial agencies” and include these references in a guidance document. The registered entities need to communicate with the ERO and the RC if applicable for compliance with this standard and to maintain the reliability of the BES. Communication with other entities such as internal company personnel, law enforcement and the Regional Entity are expected, but do not impact the reliability of the BES. This will simplify the reporting structure and will not be burdensome to registered entities when documenting compliance. If this is not an acceptable solution, APPA suggests revising 1.3 to remove the wording “the following as appropriate” and add “other entities as determined by the Responsible Entity. Examples of other entities may include, but are not limited to:” Then it is clear that the list is examples and should not be enforced by the auditor. 1.4. Provision(s) for updating the Operating Plan within 90 calendar days of any change in assets, personnel, other circumstances that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3. APPA understands that the SDT is following the FERC order requiring a 90 day limit on updates to any changes to the plan. However, APPA believes that “updating the Operating Plan within 90 calendar days of any change…” is a very burdensome compliance documentation requirement. APPA reminds the SDT that including DPs in this combined standard has increased the number of small Responsible Entities that will be required to document compliance. APPA requests that the SDT combine requirement 1.4 and 1.5 so the Operating Plan will be reviewed and updated with any changes on a yearly basis. If this is not an acceptable solution, APPA suggests that the “Lower VSL” exclude a violation to 1.4. The thought being, a violation of 1.4 by itself is a documentation error and should not be levied a penalty. Attachment 1: Events Table APPA believes that the intent of the SDT was to mirror the DOE OE-417 criteria in reporting requirements. With the inclusion of DP in the Applicability, however, APPA believes the SDT created an unintended excessive reporting requirement for DPs during insignificant events. APPA recommends that a qualifier be added to the events table. In DOE OE-417 local electrical systems with less than 300MW are excluded from reporting certain events since they are not significant to the BES. APPA believes that the benefit of reporting certain events on systems below this value would not outweigh the compliance burden placed on these small systems. Therefore, APPA requests that the standard drafting team add the following qualifier to the Events Table of Attachment 1: “For systems with greater than 300MW peak load.” This statement should be placed in the Threshold for Reporting column for the following Events: BES Emergency requiring appeal for load reduction, BES Emergency requiring system-wide voltage reduction, BES Emergency requiring manual firm load shedding, BES Emergency resulting in automatic firm load shedding. This will match the DOE OE-417 reporting criteria and relieve the burden on small entities. Definition of “Risk to BES equipment”: The SDT attempted to give examples of the Event category “Risk to BES equipment” in a footnote. This footnote gives the Responsible Entity and the Auditor a lot of room for interpretation. APPA suggests that the SDT either define this term or give a triggering mechanism that the industry would understand. One suggestion would be “Risk to BES equipment: An event that forces a Facility Owner to initiate an unplanned, non-standard or conservative operating procedure.” Then list; “Examples include train derailment adjacent to BES Facilities that either could have damaged the equipment directly or has the potential to damage the equipment…” This will allow the entity to have an operating procedure linked to the event. If this suggestion is taken by the SDT then the Reporting column of Attachment 1 needs to be changed to: “The parties identified pursuant to R1.3 within 1 hour of initiating conservative operating procedures.”
Individual
Angela Summer
Southwestern Power Administration
Yes
No
One hour is not enough time to make these assessments for all of the six items in attachment 1. All timing requirements should be made the same in order to simplify the reporting process.
Individual

Michelle R D'Antuono
Ingleside Cogeneration LP
Yes
: Yes. Ingleside Cogeneration LP agrees that training on an incident reporting operations plan should be at the option of the entity. However, we recommend that a statement be included in the “Guideline and Technical Basis” section that encourages drills and exercises be coincident with those conducted for Emergency Operations. Since front-line operators must send out the initial alert that a reportable condition exists, such exercises may help determine how to manage their reporting obligations during the early stages of the troubleshooting process. This is especially true where a notification must be made within an hour of discovery – a very short time period.
No
Attachment 1 and requirement R3 are written in a manner which would seem to indicate that internal personnel and law enforcement personnel would have to be copied on the submitted form – either Attachment 2 or OE-417. We believe the intent is to submit such forms to the appropriate recipients only (e.g.; the ERO and the DOE). The requirement should be re-written to clarify that this is the case.
Yes
Yes. Any reporting that is mandated during the first hour of an event must be subject to close scrutiny. Many of the same resources that are needed to troubleshoot and stabilize the local system will be engaged in the reporting – which will impair reliability if not carefully applied. We believe that the ERO should reassess the need for any immediate reporting requirements on a regular basis to confirm that it provides some value to the restoration process.
We are encouraged that the 2009-01 project team has eliminated duplicate reporting requirements from multiple organizations and governmental agencies. Ingleside Cogeneration LP believes that there are further improvements that can be made in this area – as the remaining overlap seem to be a result of legalities and preferences, not technical issues. We would like to see an ongoing commitment by NERC for a single process that will consolidate and automate data entry, submission, and distribution.
Individual
Tim Soles
Occidental Power Services, Inc. (OPSI)
Yes
No
Attachment 1 and R3 require event reports to be sent to the ERO and the entity’s RC and to others “as appropriate.” Although this gives the entity some discretion, it might also create some “Monday morning quarterbacking” situations. This is especially true for the one hour reporting situations as personnel that would be responding to these events are the same ones needed to report the event. OPSI suggests that the SDT reconsider and clarify reporting obligations with the objective of sending initial reports to the minimum number of entities on a need-to-know basis.
Yes
Load Serving Entities that do not own or operate BES assets should not be included in the Applicability. In current posting, the SDT states that it includes LSEs based on CIP-002; however, if the LSE does not have any BES assets, CIP-002 should also not be applicable, because the LSE could not have any Critical Assets or Critical Cyber Assets. It is understood that the SDT is trying to comply with FERC Order 693, Section 460 and 461; however, Section 461 also states “Further, when addressing such applicability issues, the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate to address these concerns.” A qualifier in the Applicability of EOP-004-2 that would include only LSEs that own or operate BES assets would seem appropriate. The proposed CIP-002 Version V has such a qualifier in that it applies to a “Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: • A UFLS program required by a NERC or Regional Reliability Standard • A UVLS program required by a NERC or Regional Reliability

Standard" The SDT should consider the same wording in the Applicability section of EOP-004-2 on order to be consistent with what will become the standing version of CIP-002 (Version 5).
Group
Dominion
Connie Lowe
Yes
Yes
Yes
Dominion appreciates the changes that have been made to increase the 1 hr reporting time to 24 hours.
There is still inconsistency in Attachment 1 vs. the DOE OE-417 form; in future changes, Dominion suggests align/rename events similar to that of the 'criteria for filing' events listed in the DOE OE-417, by working in coordination with the DOE. Minor comment; in the Background section, the drafting team refers to bulk power system (redline page 5; 1st paragraph and page 7; 2nd paragraph) rather than bulk electric system. The note in Attachment 1 states in part that "the affected Responsible Entity shall notify parties per R1 and …" Dominion believes the correct reference to be R3. In addition, capitalized terms "Event" and "Event Report" are used in this note. Dominion believes the terms should be non-capitalized as they are not NERC defined terms. Attachment 1 – "Detection of a reportable Cyber Security Incident – That meets the criteria in CIP-008". This essentially equates the criteria to be defined by the entity in its procedures as required by CIP-008 R1.1., additional clarification should be added in Attachment 1 to make this clear. The last sentence in Attachment 2 instructions should clarify that the email, facsimile and voice communication methods are for ERO notification only. Dominion continues to believe that the drill or exercise specified in R4 is unnecessary. Dominion suggests deleting this activity in the requirement.
Individual
Michael Lombardi
Northeast Utilities
Yes
Yes
Yes
- Incorporate NERC Event Analysis Reporting into this standard. Make the requirements more specific to functional registrations as opposed to having requirements applicable to "Responsible Entities". - The description of a Transmission Loss Event in Attachment 1 should be clarified to indicate that this only pertains to the loss of three or more BES elements due to a discrete event at a single point in time as opposed to a storm/weather event which may last 24 hours or more and cause the loss of three or more transmission facilities over the course of the weather event.
Group
Southern Comnpany
Antonio Grayson
No
Southern agrees with removing the training requirement of R4 from the previous version of the standard. However, Southern suggests that drills and exercises are also training and R4 in this revised standard should be removed in its entirety
No
These requirements as drafted in this revised standard potentially create a situation where an entity could be deemed non-compliant for both R2 and R3. For example, if a Responsible Entity included a reporting obligation in its Operating Plan, and failed to report an event, the Responsible Entity could

be deemed non-compliant for R2 for not “implementing” its plan and for R3 for not reporting the event to the appropriate entities. A potential solution to address this would be to add Requirement 1, Part 1.3 to Requirement 2 and remove Requirement 3 in its entirety. We also request clarification on Measure M3. Which records should have “dated and time-stamped transmittal records to show that the event was reported”? Some of the communication is handled via face-to-face conversation or through telephone conversation.
No
Southern request clarification on one of the entries in Attachment 1. The concern is with the last row on page 21 of Draft 3. What is the basis for “Voltage deviations”? The Threshold is ±10% sustained for ≥ 15 minutes. Is the voltage deviation based on the Voltage Schedule for that particular timeframe, or is it something else (pre-contingency voltage level, nominal voltage, etc.)? In addition, the second row of Attachment 1 lists “Damage or destruction of a Critical Cyber Asset per CIP-002” as a reportable event. The threshold includes “…intentional or unintentional human action” and gives us 1 hour to report. The term “damage” may be overly broad and, without definition, is not limited in any way. If a person mistypes a command and accidentally deletes a file, or renames something, or in any way changes anything on the CCA in error, then this could be considered “damage” and becomes a reportable event. The SDT should consider more thoroughly defining what is meant by “damage”. Should it incorporate the idea that the essential functions that the CCA is performing must be adversely impacted? Lastly, no event should have a reporting time shorter than at the close of the next business day. Any reporting of an event that requires a shorter reporting time should only be to entities that can help mitigate an event such as an RC or other Reliability Entity.
Southern has the following comments: (1) In Requirement R1.4, we request the SDT to clarify what is meant by the term “assets”? (2) If requirement 4 is not deleted, should we have to test every possible event described in our Operating Plan or each event listed in Attachment 1 to verify communications? (3) In the last paragraph of the “Summary of Key Concepts” section on page 6 of Draft 3, there is a statement that “Real-time reporting is achieved through the RCIS…” The only reporting required on RCIS by the Standards is for EEAs and TLRs. Please review and modify this language as needed. (4) Evidence Retention (page 12 of Draft 3): The 3 calendar year reference has no bearing on a Standard that may be audited on a cycle greater than 3 years. (5) In the NOTE for Attachment 1 (page 20 of Draft 3), what is meant by “periodic verbal updates” and to whom should the updates be made? (6) There are Prerequisite Approvals listed in the Implementation Plan. Is it appropriate to ask industry to vote on this Standard Revision that has a prerequisite approval of changes in the Rules of Procedure that have not been approved? (7) We believe the reporting of the events in Attachment 1 has no reliability benefit to the Bulk Electric System. We suggest that Attachment 1 should be removed.
Individual
Andrew Gallo
City of Austin dba Austin Energy
Yes
Yes
Yes
The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. EOP-004 has an “optional” Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify whether Registered Entities will still be required to submit both forms. Please also ensure there will not be duplication of efforts between the two reports. Although this is fairly minor, the clarification should be addressed.
Overarching Concern related to EOP-004-2 draft: The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes and CIP Standards Version 5 could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definition of a BES element could change significantly and the concepts of “Critical Assets” and “Critical Cyber Assets” no longer exist in Version 5 of the CIP Standards. Additionally, it is debatable whether the destruction of, for example, one relay would be a

reportable incident given the proposed language. Related to “Reportable Events” of Attachment 1: 1. The “Purpose” section of the Standard indicates it is designed to require the reporting of events “with the potential to impact reliability” of the BES. Footnote 1 and the “Threshold for Reporting” associated with the Event described as “Destruction of BES equipment” expand the reporting scope beyond that intent. For example, a fan on a generation unit can be destroyed because a plant employee drops a screwdriver into it. We believe such an event should not be reportable under EOP-004-2. Yet, as written, a Responsible Entity could interpret that event as reportable (because it would be “unintentional human action” that destroyed a piece of equipment associated with the BES). If the goal of the SDT was to include such events, we think the draft Standard goes too far in requiring reporting. If the SDT did not intend to include such events, the draft Standard should be revised to make that fact clear. 2. Item iii) in Footnote 1 seems redundant with the Threshold for Reporting. 3. The word “Significantly” in item ii) of footnote 1 introduces an element of subjectivity. What is “significant” to one person may not be significant to someone else. 4. The word “unintentional” in Item iii) of footnote 1 may introduce nuisance reporting. The SDT should consider: (1) changing the Event description to “Damage or destruction of BES equipment” (2) removing the footnote and (3) replacing the existing “Threshold for Reporting” with the following language: “Initial indication the event: (i) was due to intentional human action, (ii) affects an IROL or (iii) in the opinion of the Responsible Entity, jeopardizes the reliability margin of the system (e.g., results in the need for emergency actions)” 5. One reportable event is “Risk to the BES” and the threshold for reporting is, “From a non-environmental physical threat.” This appears to be intended as a catch-all reportable event. Due to the subjectivity of this event description, we suggest removing it from the list. 6. One reportable event is “Damage or destruction of Critical Asset per CIP-002.” The SDT should define the term “Damage” in order for an entity to determine a threshold for what qualifies as “Damage” to a CA. Normal “damage” can occur on a CA that should not be reportable (e.g. the screwdriver example, above). 7. For the event called “BES Emergency requiring public appeal for load reduction,” the SDT should make it clear who should report such an event. For example, in the ERCOT Region, there is a requirement that ERCOT issue public appeals for load reduction (See ERCOT Protocols Section 6.5.9.4). As the draft of EOP-004-2 is currently written, every Registered Entity in the ERCOT Region would have to file a report when ERCOT issues such an appeal. Such a requirement is overly burdensome and does not enhance the reliability of the BES. The Standard should require that the Reliability Coordinator file a report when it issues a public appeal to reduce load. Reporting Thresholds 1. See Paragraph 1 in the “Related to 'Reportable Events' of Attachment 1” section, above. 2. We believe damage or destruction of Critical Assets or CCAs resulting from operational error, equipment failure or unintentional human action should not be reportable under this Standard. We recommend changing the thresholds for “Damage or destruction of Critical Asset…” and “Damage or destruction of a [CCA]” to “Initial Indication the event was due to external cause or intentional human action.” 3. We support the SDT’s attempted to limit nuisance reporting related to copper thefts. However, a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could clog the reporting process with nuisance reporting and reviewing. An example is the “BES Emergency requiring manual firm load shedding” of ≥ 100 MW or “Loss of Firm load for ≥ 15 Minutes” that is ≥ 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases, those low thresholds would require reporting minor wind events or other seasonal system issues on a local network used to provide distribution service. Firm Load 1. The use of the term “Firm load” in the context of the draft Standard seems inappropriate. “Firm load” is not defined in the NERC Glossary (although “Firm Demand” is defined). If the SDT intended to use “Firm Demand,” they should revise the draft Standard to use that language. If the SDT wishes to use the term “Firm load” they should define it. [For example, we understand that some load agrees to be dropped in an emergency. In fact, in the ERCOT Region, we have a paid service referred to as “Emergency Interruptible Load Service” (EILS). If the SDT intends that “Firm load” means load other than load which has agreed to be dropped, it should make that fact clear.] Comments to Attachment 2 1. The checkbox for “fuel supply emergency” should be deleted because it is not listed as an Event on Attachment 1. 2. There should be separation between “forced intrusion” and “Risk to BES equipment.” They are separate Events on Attachment 1. Comments to Guideline and Technical Basis The last paragraph appears to state NERC will accept an OE-417 form as long as it contains all of the information required by the NERC form and goes on to state the DOE form “may be included or attached to the NERC report.” If the intent is for NERC to accept the OE-417 in lieu of the NERC report, this paragraph should be clarified.

Group
FirstEnergy

Sam Ciccone
Yes
FirstEnergy supports this removal and thanks the drafting team.
Yes
Yes
Although we agree with the timeframes for reporting, we have other concerns as listed in our response to Question 4.
1. Attachment 1 – Regarding the 1st event listed in the table, “Destruction of BES Equipment” and its accompanying Footnote 1, we believe that this event should be broken into two separate events that incorporate the specifics in the footnote as follows: a. “Destruction of BES equipment that associated with an IROL per FAC-014-2.” Regarding the 1st event we have proposed – We have proposed this be made specific to IROL as stated in Footnote 1 part i. Also, we believe that only the RC and TOP would have the ability to quickly determine and report within 1 hour if the destruction is associated with an IROL. The other entities listed would not necessarily know if the event affects and IROL. Therefore, we also propose that the Entities with Reporting Responsibilities (column 2) be revised to only include the RC and TOP. b. "Destruction of BES equipment that removes the equipment from service.” Regarding the 3rd event we have proposed – We have proposed this be made specific to destruction of BES equipment that removes the equipment from service as stated in Footnote 1 part iii. Also, the other part of footnote 1 part iii which states “Damaged or destroyed due to intentional or unintentional human action” is not required since it is covered in the threshold for reporting. Also the term “Damaged” in this part iii is not appropriate since these events are limited to equipment that has been destroyed. We also propose that the Entities with Reporting Responsibilities (column 2) for this event would remain the same as it states now since any of those entities may observe out of service BES equipment. Regarding part ii of footnote 1, we do not believe that this event needs to be separated. Regarding the phrase “significantly affects the reliability margin of the system be clarified so that it is not left up to the entity to interpret a “significant” affect. Lastly, since we have incorporated parts i and iii into the two separate events and removed part ii as proposed above, the only statement that needs to be left in the Footnote 1 is: “Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative).” 2. Attachment 1 – We ask that the team add an “Event #” column to the table so that each of the events listed can be referred to by #, such as Event 1, Event 2, etc. 3. Attachment 1 – Event titled “Damage or destruction of a Critical Cyber Asset per CIP-002”, the proposed threshold for reporting seems incomplete. We suggest the threshold for this event match the threshold for the Critical Asset event which states: “Initial indication the event was due to operational error, equipment failure, external cause, or intentional or unintentional human action.” 4. Attachment 1 – Events titled “Damage or destruction of a Critical Assets per CIP-002” and “Damage or destruction of a Critical Cyber Asset per CIP-002” seem ambiguous due to the term “damage”. We suggest removal of “damage” or clarity as to what is considered a damaged asset. 5. VSL Table – Instead of listing every entity, it may be more efficient to simply say “The Responsible Entity” in the VSL for each requirement. 6. Guideline and Technical Basis section – This section does not provide guidance on each of the requirements of the standard. We suggest the team consider adding guidance for the requirements.
Group
PPL Electric Utilities and PPL Supply Organizations`
Annette M. Bannon
Yes
Yes
Our comments center around the footnotes and events 'Destruction of BES equipment' and 'Loss of Off-site power to a nuclear generating plant'. We request the SDT consider adding a statement to the standard that acknowledges that not all registered entities have visibility to the information in the footnotes. E.G. Destruction of BES equipment. A GO/GOP does not necessarily know if loss of specific

BES equipment would affect any IROL and therefore would not be able to consider this criteria in its reporting decision. Loss of BES equipment would be reported to the BA/RC and the BA/RC would know of an IROL impact and the BA/RC is the appropriate entity to report. We request the SDT consider the information in the footnotes for inclusion in the table directly. Consider Event 'Destruction of BES equipment'. Is footnote 1 a scoping statement? Is it part of the threshold? Is it the impact? Is it defining Destruction? If the BES equipment was destroyed by weather and does not affect an IROL, then is no report is needed? Alternatively, do you still apply the threshold and say it was external cause and therefore report? We suggest including a flowchart on how to use Attachment 1 with an example. The flowchart would explain the order in which to consider the event and the threshold, and footnotes if they remain. Regarding Attachment 1 Footnote 1 'do not report copper theft...unless it degrades the ability of equipment to operate correctly.', is this defining destruction as not operating correctly ? or is the entirety of footnote 1 a definition of destruction? Regarding Attachment 1 Footnote 1, iii, we request this be changed for consistency with the Event and suggest removing damage from the footnote. i.e. The event is 'destruction' whereas the footnote says 'damaged or destroyed'. The standard does not provide guidance on damage vs destruction which could lead to differing reporting conclusions. Is the reporting line out of service, beyond repair, or is it timeframe based? Regarding Attachment 1 Footnote 2 ' to steal copper... unless it affects the reliability of the BES', is affecting the reliability of the BES a consideration in all the events? PPL believes this is the case and request this statement be made. This could be included in the flowchart as a decision point. Regarding Event 'Loss of Off-site power to a nuclear generating plant', the threshold for reporting does not designate if the off-site loss is planned and/or unplanned – or if the reporting threshold includes the loss of one source of off-site power or is the reporting limited to when all off-site sources are unavailable. PPL recommends the event be 'Total unplanned loss of offsite power to a nuclear generating plant (grid supply)' Thank you for considering our comments.
Group
CenterPoint Energy
John Brockhan
Yes
No
CenterPoint Energy believes the current R2 is unnecessary and duplicative. Upon reporting events as required by R3, entities will be implementing the relevant parts of their Operating Plan that address R1.1 and R1.2. This duplication is clear when reading M2 and M3. Acceptable evidence is an event report. R2 should be modified to remove this duplicative requirement.
No
CenterPoint Energy agrees with the revision that allows more time for reporting some events; however, some 1 hour requirements remain. The Company does not agree with this timeframe for any event.
CenterPoint Energy appreciates the SDT's consideration of comments and removal of the term, Impact Event. However, the Company still suggests removing the phrase "with the potential to impact" from the purpose as it is vast and vague. An alternative purpose would be "To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of events that impact reliability and their causes if known". The focus should remain on those events that truly impact the reliability of the BES. CenterPoint Energy remains very concerned about the types of events that the SDT has retained in Attachment 1 as indicated in the following comments: Destruction of BES Equipment – The loss of BES equipment should not be reportable unless the reliability of the BES is impacted. Footnote 5, iii should be modified to tie the removal of a piece of equipment from service back to reliability of the BES. Risk to BES equipment: This Event is too vague to be meaningful and should be deleted. The Event should be modified to "Detection of an imminent physical threat to BES equipment". Any reporting time frame of 1 hour is unreasonable; Entities will still be responding to the Event and gathering information. A 24 hour reporting time frame would be more reasonable and would still provide timely information. System Separation: The 100 MW threshold is too low for a reliability impact. A more appropriate threshold is 500 MW. Loss of Monitoring or all voice communication capability: The two elements of this Event should be separated for clarity as follows: "Loss of monitoring of Real-Time conditions" and "Loss of all voice communication capability."

Individual
James Sauceda
Energy Northwest - Columbia
Yes
Yes
No
Energy Northwest - Columbia (ENWC) has concerns about the existing 1 hour reporting requirements and feels that additional guidance and verbiage is required for clarification. ENWC would like the word "recognition" in the statement that reads, "recognition of events," be replaced by "confirmation" as in "confirmed event." Also, we would like clarification as to when the 1 hour clock starts. Please consider changing recognition in "within 1 hour of recognition of event" and incorporating in "confirmation."
1. The Loss of Off-site power event criteria is much improved from the last draft of EOP 004-2; however, some clarification is needed to more accurately align with NERC Standard NUC-001 in both nomenclature and intent. Specifically, there are many different configurations supplying offsite power to a nuclear power plant and it is essential that all configurations be accounted for. As identified in the applicability section of NUC-001 the applicable transmission entities may include one or more of the following (TO, TOP, TP, TSP, BA, RC, PC, DP, LSE, and other non-nuclear GO/GOPs). Based on the response to previous comments submitted for Draft 2, Energy Northwest understands that the DSR SDT evaluated the use of the word “source” but dismissed the use in favor of “supply” with the justification “[that] ‘supply’ encompasses all sources”. Energy Northwest suggests that the word “source” is used as the event criteria in EOP-004-2 as this nomenclature is commonly used in the licensing basis of a nuclear power plant. By revising the threshold criteria to “one or more” Energy Northwest believes the concern the DSR SDT noted is addressed and ensures all sources are addressed. In addition, by revising the threshold for reporting to a loss of “one or more” will ensure that all potential events (regardless of configuration of off-site power supplies) will be reported by any applicable transmission entity specifically identified in the nuclear plant site specific NPIRs. Energy Northwest proposes that the loss of an off-site power source be revised to an “unplanned” loss to account for planned maintenance that is coordinated in advance in accordance with the site specific NPIRs and associated Agreements. This will also eliminate unnecessary reporting for planned maintenance. Although the loss of one off-site power source may not result in a nuclear generating unit trip, Energy Northwest agrees that an unplanned loss of an off-site power source regardless of impact should be reported within the 24 hour time limit as proposed. Suggest that the Loss of Offsite power to a nuclear generating plant event be revised as follows: Event: Unplanned loss of any off-site power source to a Nuclear Power Plant Entity with Reporting Responsibility: The applicable Transmission Entity that owns and/or operates the off-site power source to a Nuclear Power Plant as defined in the applicable Nuclear Plant Interface Requirements (NPIRs) and associated Agreements. Threshold for Reporting: Unplanned loss of one or more off-site power sources to a Nuclear Power Plant per the applicable NPIRs. 2. Please consider changing "Operating Plan" with "Procedure(s)". Procedures extend beyond operating groups and provide guidance to the entire company.
Group
Electric Compliance
Tom McElhinney
Yes
Yes
Yes
The concepts of “Critical Assets” and “Critical Cyber Assets” no longer exist in Version 5 of the CIP Standards and so this may cause confusion. Recommend modifying to be in accordance with Version 5. Additionally, it is debatable whether the destruction of, for example, one relay would be a reportable incident given the proposed language. We recommend modifying the language to insure

nuisance reporting is minimized. One reportable event is, “Risk to the BES” and the threshold for reporting is, “From a non-environmental physical threat.” This appears to be a catch-all reportable event. Due to the subjectivity of this event description, we suggest removing it from the list. Footnote 1 and the “Threshold for Reporting” associated with the Event described as “Destruction of BES equipment” expand the reporting scope. For example, a fan on a transformer can be destroyed because a technician drops a screwdriver into it. We believe such an event should not be reportable under EOP-004-2. Yet, as written, a Responsible Entity could interpret that event as reportable (because it would be “unintentional human action” that destroyed a piece of equipment associated with the BES). If the goal of the SDT was to include such events, we think the draft Standard goes too far in requiring reporting. If the SDT did not intend to include such events, the draft Standard should be revised to make that fact clear. Proposed Footnote: BES equipment that become damaged or destroyed due to intentional or unintentional human action which removes the BES equipment from service that i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii). Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative). The word “Significantly” in item ii) of footnote 1 and “as appropriate” in section 1.3 introduces elements of subjectivity. What is “significant” or “appropriate” to one person may not be to someone else. In section 1.4, we believe that revising the plan within 90 days of “any” change should be changed to 180 days or else classes of events should be made so that only substantial changes are required to made within the 90 day timeframe.
Individual
Scott Berry
Indiana Municipal Power Agency
No
IMPA does not believe that R4 is necessary. In addition, if a drill or exercise is used to verify the communication process, some of the parties listed in R1.3 may not want to participate in the drill or exercise every 15 months, such as law enforcement and governmental agencies. IMPA would propose a contacting these agencies every 15 months to verify their contact information only and updating their information in the plan as needed, without performing a drill or exercise.
No
Both requirements seem to be implementing the Operating Plan which means R3 should be a bullet under R2 and not a separate requirement. IMPA supports making R2 and R3 one requirement and eliminating the current R3 requirement. In addition, R2 needs to be clarified when addressing an actual event. IMPA recommends saying “an actual event that meets the criteria of Attachment 1.”
No
IMPA believes that some of the times may not be aggressive enought that are related to generation capacity shortages. In addition, IMPA believes clarity needs to be added when saying within 1 hour of recognition of event. For example, A fence cutting may not be discovered for days at a remote substation and then a determination has to be made if it was “forced intrusion” – Does that one hour apply once the determination is made that is was “forced intrusion” or from the time the discovery was made? Some of the 1 hour time limits can be expanded to allow for more time, such as forced intrusion, destruction of BES equipment, Risk to BES equipment, etc.
Many of the items listed in Attachment 1 are onerous and burdensome when it comes to making judgments or determinations. What one may consider “Risk to BES equipment” another person may not make the same determination. Clarity needs to be added to make the events easier to determine and that will result in less issues when it comes to compliance audits. IMPA does not understand the usage of the terms Critical Asset and Critical Cyber Asset as they will be retired with CIP version 5. IMPA believes the data retention requirements are way too complicated and need to be simplified. It seems like it would be less complicated if one data retention period applied to all data associated with this standard. On “public appeal”, in the threshold, the descriptor “each” should be deleted, e.g., if a single event causes an entity to be short of capacity, do you really want that entity reporting each time they issue an appeal via different types of media, e.g., radio, TV, etc., or for a repeat appeal every several minutes for the same event?
Individual
Maggy Powell

Constellation Energy on behalf of Baltimore Gas & Electric, Constellation Power Generation, Constellation Energy Commodities Group, Constellation Control and Dispatch, Constellation NewEnergy and Constellation Energy Nuclear Group.
Yes
Yes, we support removal of the training requirement.
Yes
While we support the delineation of the different activities associated with implementation and reporting, further clarification would be helpful. R1. 1.3: As currently written, it is somewhat confusing, in particular the use of the qualifier “as appropriate”. In addition, the use of the word “communicating” to capture both reporting to reliability authorities and notifying others may leave the requirement open to question. Below is a proposed revision: 1.3 A process for reporting events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity’s Reliability Coordinator and for communicating to others as defined in the Responsible Entity’s Operating Plan, such as: • Internal company personnel • The Responsible Entity’s Regional Entity • Law Enforcement • Government or provincial agencies R1, 1.4: the last phrase of the requirements seems to be leftover from an earlier version. The requirement should end after the word “Plan”. R1, 1.5: “Process” should not be capitalized. While we understand the intent of the draft language and appreciate the effort to streamline the requirements, we propose an adjusted delineation below that we feel tracks more cleanly to the structure of a compliance program. Proposed revised language: R2. Each Responsible Entity shall implement its Operating Plan to meet Requirement R1, parts 1.1 and 1.2 for an actual event(s). M2. Responsible Entities shall provide evidence that it implemented it Operating Plan to meet Requirement R1, Parts 1.1 and 1.2 for an actual event. Evidence may include, but is not limited to, an submitted event report form (Attachment 2) or a submitted OE-417 report, operator logs, or voice recording. R3. Each Responsible Entity shall implement its Operating Plan to meet Requirement R1, parts 1.4 and 1.5. M3. Responsible Entities shall provide evidence that it implemented it Operating Plan to meet Requirement R1, Parts 1.4 and 1.5. Evidence may include, but is not limited to, dated documentation of review and update of the Operating Plan. R4. Each Responsible Entity shall verify (through implementation for an actual event, or through a drill, exercise or table top exercise) the communication process in its Operating Plan, created pursuant to Requirement 1, Part 1.3, at least annually (once per calendar year), with no more than 15 calendar months between verification. M4. The Responsible Entity shall provide evidence that it verified the communication process in its Operating Plan for events created pursuant to Requirement R1, Part 1.3. Either implementation of the communication process as documented in its Operating Plan for an actual event or documented evidence of a drill, exercise, or table top exercise may be used as evidence to meet this requirement. The time period between verification shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or dated documentation of a verification.
Yes
We agree with the change to the reporting times in Attachment 1. While this is an improvement, other concerns with the language in the events table language remain. Please see additional details below: General items: • All submission instructions (column 4 in Events Table) should qualify the recognition of the event as “of recognition of event as a reportable event.” • Is the ES-ISAC the appropriate contact for the ERO given that these two entities are separate even though they are currently managed by NERC? In addition, are the phone numbers in the Attachment 1 NOTE accurate? Is it possible they will change in a different cycle than the standard? Specific Event Language: • Destruction of BES Equipment, footnote: Footnote 1, item iii confuses the clarification added in items i. and ii. Footnote 1 should be modified to state BES equipment that (i) an entity knows will affect an IROL or has been notified the loss affects an IROL; (ii) significantly affects the reserve margin of a Balancing Authority or Reserve Sharing Group. Item iii should be dropped. • Damage or destruction of Critical Asset per CIP-002: Within the currently developing revisions to CIP-002 (version 5), Critical Asset will be retired as a glossary term. As well as addressing the durability of this event category, additional delineation is needed regarding which asset disruptions are to be reported. A CA as currently defined incorporates assets in a broad perspective, for instance a generating plant may be a Critical Asset. As currently written in Attachment 1, reporting may be required for unintended events, such as a boiler leak that takes a plant offline for a minor repair. Event #1 – Destruction of BES Equipment – captures incidents at the relevant equipment regardless of whether they are a Critical Asset or not. We recommend dropping this event. However, if reference

to CIP-002 assets remains, it will be important to capture reporting of the events relevant to reliability and not just more events. • Damage or destruction of a Critical Cyber Asset per CIP-002: Because CCAs are defined at the component level, including this trigger is appropriate; however, as with CAs, the CCA term is scheduled to be retired under CIP-002 version 5. • Forced Intrusion: The footnote confuses the goal of including this event category. In addition, “forced” doesn’t need to define the incident. Constellation proposes the following to better define the event: Intrusion that affects or attempts to affect the reliable operation of the BES (1) (1) Examples of "affecting reliable operation of the BES are": (i) device operations, (ii) protective equipment degradation, (iii) communications systems degradation including telemetered values and device status. • Risk to BES equipment: This category is too vague to be effective and the footnote further complicates the expectations around this event. The catch all concept of reporting potential risks to BES equipment is problematic. It’s not clear what the reliability goal of this category is. Risk is not an event, it is an analysis. How are entities to comply with this “event”, never mind within an hour? It appears that the information contemplated within this scenario would be better captured within the greater efforts underway by NERC to assess risks to the BES. This event should be removed from the Attachment 1 list in EOP-004. • BES Emergency requiring system-wide voltage reduction: the Entity with Reporting Responsibility should be limited to RC and TOP. • Voltage deviations on BES Facilities: The Threshold for Reporting language needs more detail to explain +/- 10% of what? Proposed revision: ± 10% outside the voltage schedule band sustained for ≥ 15 continuous minutes • IROL Violation (all Interconnections) or SOL Violation (WECC only): Should “Interconnections” be capitalized? • Transmission loss: The reporting threshold should provide more specifics around what constitutes Transmission Facilities. One minor item, under the Threshold for Reporting, “Three” does not need to be capitalized.
Background Section: The background section in this revision of EOP-004 reads more like guidance than a background of the development of the event reporting standard. Because of the background remains as part of the standard, the language raises questions as to role it plays relative to the standard language. For instance, the Law Enforcement Reporting section states:”Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES.” It’s not clear how “potential to impact to a wider area of the BES” is defined and where it fits into the standard. As well, and perhaps more problematic, is the Reporting Hierarchy for Reportable Events flow chart. While the flow chart concept is quite useful as a guidance tool, the flow chart currently in the Background raises questions. For instance, the Procedure to Report to Law Enforcement sequence does not map to language in the requirements. Further, Entities would not know about the interaction between law enforcement agencies. Please see additional recommended revisions to the requirement language and to the Events Table in the Q2 and Q3 responses. Attachment 2: Event Reporting Form: The review of the form is one of the many aspects to compare with the developments within the Events Analysis Process (EAP) developments. We support the effort to create one form for submissions. The recent draft EAP posted as part of Planning Committee and Operating Committee agendas includes a form requiring a few bits of additional relevant information when compared to the EOP-004 form. This may be a valuable approach to avoid follow up inquiries that may result if the form is too limited. We suggest that consideration be given to the proposed EAP form. One specific note on the Proposed EOP-004 Attachment 2: The “Potential event” box in item 3 should be eliminated to track with the removal of the “Risk to the BES” category.
Group
Salt River Project
Brenton Lopez
Yes
Yes
Yes
The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the NERC Event Analysis process, but there is some duplication of efforts. EOP-004 has an “optional” Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify whether Registered Entities will still be required to submit both forms. Please also ensure there will not be

duplication of efforts between the two reports. Although this is fairly minor, the clarification should be addressed.
Overarching Concern related to EOP-004-2 draft: The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes and CIP Standards Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definition of a BES element could change significantly and the concepts of “Critical Assets” and “Critical Cyber Assets” no longer exist in Version 5 of the CIP Standards. Additionally, it is debatable whether the destruction of, for example, one relay would be a reportable incident given the proposed language. Related to “Reportable Events” of Attachment 1: 1. The “Purpose” section of the Standard indicates it is designed to require the reporting of events “with the potential to impact reliability” of the BES. Footnote 1 and the “Threshold for Reporting” associated with the Event described as “Destruction of BES equipment” expand the reporting scope beyond that intent. For example, a fan on a generation unit can be destroyed because a plant employee drops a screwdriver into it. We believe such an event should not be reportable under EOP-004-2. Yet, as written, a Responsible Entity could interpret that event as reportable (because it would be “unintentional human action” that destroyed a piece of equipment associated with the BES). If the goal of the SDT was to include such events, we think the draft Standard goes too far in requiring reporting. If the SDT did not intend to include such events, the draft Standard should be revised to make that fact clear. 2. Item iii) in Footnote 1 seems redundant with the Threshold for Reporting. 3. The word “Significantly” in item ii) of footnote 1 introduces an element of subjectivity. What is “significant” to one person may not be significant to someone else. 4. The word “unintentional” in Item iii) of footnote 1 may introduce nuisance reporting. The SDT should consider: (1) changing the Event description to “Damage or destruction of BES equipment” (2) removing the footnote and (3) replacing the existing “Threshold for Reporting” with the following language: “Initial indication the event: (i) was due to intentional human action, (ii) affects an IROL or (iii) in the opinion of the Responsible Entity, jeopardizes the reliability margin of the system (e.g., results in the need for emergency actions)” 5. One reportable event is, “Risk to the BES” and the threshold for reporting is, “From a non-environmental physical threat.” This appears to be intended as a catch-all reportable event. Due to the subjectivity of this event description, we suggest removing it from the list. 6. One reportable event is, “Damage or destruction of Critical Asset per CIP-002.” The SDT should define the term “Damage” in order for an entity to determine a threshold for what qualifies as “Damage” to a CA. Normal “damage” can occur on a CA that should not be reportable (e.g. the screwdriver example, above). Reporting Thresholds 1. We believe damage or destruction of Critical Assets or CCAs resulting from operational error, equipment failure or unintentional human action should not be reportable under this Standard. We recommend changing the thresholds for “Damage or destruction to Critical Assets …” and “Damage or destruction of a [CCA]” to “Initial Indication the event was due to external cause or intentional human action.” 2. We support the SDT’s attempted to limit nuisance reporting related to copper thefts. However, a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could clog the reporting process with nuisance reporting and reviewing. An example is the “BES Emergency requiring manual firm load shedding” of ≥ 100 MW or "Loss of Firm load for ≥ 15 Minutes” that is ≥ 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases, those low thresholds would require reporting minor wind events or other seasonal system issues on a local network used to provide distribution service. Firm Demand 1. The use of the term “Firm load” in the context of the draft Standard seems inappropriate. “Firm load” is not defined in the NERC Glossary (although “Firm Demand” is defined). If the SDT intended to use “Firm Demand,” they should revised the draft Standard. If the SDT wishes to use the term “Firm load” they should define it. [For example, we understand that some load agrees to be dropped in an emergency. In fact, in the ERCOT Region, we have a paid service referred to as “Emergency Interruptible Load Service” (EILS). If the SDT intends that “Firm load” means load other than load which has agreed to be dropped, it should make that fact clear.] Comments to Attachment 2 1. The checkbox for “fuel supply emergency” should be deleted because it is not listed as an Event on Attachment 1. 2. There should be separation between “forced intrusion” and “Risk to BES equipment.” They are separate Events on Attachment 1. Comments to Guideline and Technical Basis The last paragraph appears to state NERC will accept an OE-417 form as long as it contains all of the information required by the NERC form and goes on to state the DOE form “may be included or attached to the NERC report.” If the intent is for NERC to accept the OE-417 in lieu of the NERC report, this paragraph should be clarified.
Individual

Michael Brytowski
Great River Energy
No
We understand and agree there should be verification of the information required for such reporting (contact information, process flow charts, etc). But we still believe improvements can be made to the draft standard, in particular to requirement R4. The use of the words “or through a drill or exercise” still implies that training is required if no actual event has occurred. When you conduct a fire “drill” you are training your employees on evacuation routes and who they need to report to. Not only are you verifying your process but you are training your employees as well. It is imperative that the information in the Event Reporting process is correct but we don't agree that performing a drill on the process is necessary. We recommend modifying the requirement to focus on verifying the information needed for appropriate communications on an event. And we agree this should take place at least annually.
No
Requirement R2 requires Responsible Entities to implement the various subrequirements in R1. We believe it is unnecessary to state that an entity must implement their Operating Plan in a separate requirement. Having a separate requirement seems redundant. If the processes in the Operating Plan are not implemented, the entity is non-compliant with the standard. There doesn’t need to be an extra requirement saying entities need to implement their Operating Plan.
Yes
For many of the events listed in Attachment 1, there would be duplicate reporting the way it is written right now. For example, in the case of a fire in a substation (Destruction of BES equipment), the RC, BA, TO, TOP and perhaps the GO and GOP could all experience the event and each would have to report on it. This seems quite excessive and redundant. We recommend eliminating this duplicate reporting.
Individual
Christine Hasha
Electric Reliability Council of Texas, Inc.
Yes
Yes
No
Destruction of BES equipment: 1. Request that the term “destruction” be clarified. Damage or destruction of Critical Asset per CIP-002: 1. Request that the terms “damage” and “destruction” be clarified. 2. Is the expectation that an entity report each individual device or system equipment failure or each mistake made by someone administering a system? 3. Request that “initial indication of the event” be changed to “confirmation of the event”. Event monitoring and management systems may receive many events that are determined to be harmless and put the entity at no risk. This can only be determined after analysis of the associated events is performed. Damage or destruction of a Critical Cyber Asset per CIP-002: 1. Request that the terms “damage” and “destruction” be clarified. 2. Is the expectation that an entity report each individual device or system equipment failure or each mistake made by someone administering a system? 3. Request that “initial indication of the event” be changed to “confirmation of the event”. Event monitoring and management systems may receive many events that are determined to be harmless and put the entity at no risk. This can only be determined after analysis of the associated events is performed. Risk to BES equipment: Request that the terms “risk” be clarified.
Individual
Darryl Curtis
Oncor Electric Delivery Company LLC
Yes

No
NERC's Event Analysis Program tends to parallel many of the reporting requirements as outlined in EOP-004 Version 2. Oncor recommends that NERC considers ways of streamlining the reporting process by either incorporating the Event Analysis obligations into EOP-004-2 or reducing the scope of the Event Analysis program as currently designed to consist only of "exception" reporting.
Yes
NERC's Event Analysis Program tends to parallel many of the reporting requirements as outlined in EOP-004 Version 2. Oncor recommends that NERC considers ways of streamlining the reporting process by either incorporating the Event Analysis obligations into EOP-004-2 or reducing the scope of the Event Analysis program as currently designed to consist only of "exception" reporting.
Group
Kansas City Power & Light
Michael Gammon
Yes
No
Requirement R1.1 is confusing regarding the “process for identifying events listed in Attachment 1”. Considering Attachment 1, the Events Table, already identifies the events required for reporting, please clearly describe in the requirement what the “process” referred to in requirement R1.1 represents.
No
The reportable events listed in Attachment 1 can be categorized as events that have had a reliability impact and those events that could have a reliability impact. The listed events that could have a reliability impact should have a 24 hour reporting requirement and the events that have had a reliability impact are appropriate at a 1 hour reporting. The following events with a 1 hour report requirement are recommended to change to 24 hour: Forced Intrusion and Risk to BES Equipment. In addition, the Attachment 1 Events Table is incomplete as many of the listed events are incomplete regarding reporting time requirements and event descriptions. Also recommend removing (ii) from note 5 with event “Destruction of BES equipment” as this part of the note is already described in the event description and insinuates reporting of equipment losses that do not have a reliability impact. The events, “Damage or destruction of Critical Asset per CIP-002” and “Damage or destruction of a Critical Cyber Asset per CIP-002”, does not have sufficient clarity regarding what that represents. A note similar in nature to Note 5 for BES equipment is recommended.
The implementation plan indicates that much of CIP-008 is retained. The reporting requirements in CIP-008 and the required reportable events outlined in Attachment 1 are an overlap with CIP-008-3 R1.1 which says “Procedures to characterize and classify events as reportable Cyber Security Incidents” and CIP-008-3 R1.3 which requires processes to address reporting to the ES-ISAC. There is also a NERC document titled, Security Guideline for the Electricity Sector: Threat and Incident Reporting, which is a guideline to “assist entities to identify and classify incidents for reporting to the ES-ISAC”. The SDT should consider the content of the Security Guideline for the Electricity Sector: Threat and Incident Reporting when considering the reporting requirements proposed EOP-004. The efforts to incorporate CIP-008 into EOP-004 are insufficient and will result in serious confusion between proposed EOP-004 and CIP-008 and reporting expectations. Considering the complexity CIP incident reporting and the interests of ES-ISAC, it may be beneficial to leave CIP-008 out of the proposed EOP-004 and limit EOP-004 to the reporting interests of NERC. The flowchart states, “Notification Protocol to State Agency Law Enforcement”. Please correct this to, “Notification to State, Provincial, or Local Law Enforcement”, to be consistent with the language in the background section part, “A Reporting Process Solution – EOP-004”. Measure 4 is not clear enough regarding the extent to which drills should be performed. Does the measure mean that all events in the events list need to be drilled or is drilling a subset of the events list sufficient? Please clearly indicate the extent of drilling that is required or clearly indicate in the requirement the extent of the drills to be performed is the responsibility of the Responsible Entity to identify in their “processes”. Evidence Retention – it is not clear what the phrase “prior 3 calendar years” represents in the third paragraph of this section

regarding data retention for requirements and measures for R2, R3, R4 and M2, M3, M4 respectively. Please clarify what this means. Is that different than the meaning of “since the last audit for 3 calendar years” for R1 and M1? VSL for R2 under Severe regarding R1.1 may require revision considering the comment regarding R1.1 in item 2 previously stated. In addition, the VRF for R2 is MEDIUM. R2 is administrative regarding the implementation of the requirements specified in R1. Documentation and maintenance should be considered LOWER. There is no VSL for R4 and a VSL for R4 needs to be proposed.

Additional Comments Received:

Southwestern Power Administration's Comments for Project 2009-1
Submitted by Angela Summer

"Attachment 1 contains elements that do not need to be included, and redundant elements such as:

Forced intrusion at BES Facility - A facility break-in does not necessarily mean that the facility has been impacted or has undergone damage or destruction.

Detection of a reportable Cyber Security Incident per CIP-008 - If entities are addressing this requirement in CIP-008, why do so again in
EOP-004 (Attachment 2-EOP-004, Reporting Requirement number 5)?

Transmission Loss: Each TOP that experiences transmission loss of three or more facilities - This element should be removed or rewritten so that it only applies when the loss includes a contingent element of an IROL facility."

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-01 – Disturbance and Sabotage Reporting

Initial Ballot and Non-binding Poll Results

Now Available

An initial ballot of EOP-004-2 – Event Reporting and its implementation plan, and a non-binding poll of the associated VRFs and VSLs, concluded on December 12, 2011. Voting statistics are listed below, and the Ballot Results webpage provides a link to the initial ballot detailed results.

Initial Ballot Results for EOP-004-2

Quorum: 87.97%

Approval: 36.21%

Non-Binding Poll Results

85.28% of those who registered to participate provided an opinion or abstention; 45% of those who provided an opinion indicated support for the VRFs and VSLs.

Next Steps

The drafting team will consider all comments received during the comment period and ballot.

Background

Stakeholders have indicated that identifying potential acts of "sabotage" is difficult to do in real time, and additional clarity is needed to identify thresholds for reporting potential acts of sabotage in CIP-001-1. Stakeholders have also reported that EOP-004-1 has some requirements that reference out-of-date Department of Energy forms, making the requirements ambiguous. EOP-004-1 also has some 'fill-in-the-blank' components to eliminate. The project will include addressing previously identified stakeholder concerns and FERC directives; will bring the standards into conformance with the latest approved version of the ERO Rules of Procedure; and may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards. Additional information is available on the project webpage.

A stakeholder interested in following the Disturbance and Sabotage Reporting Drafting Team's development of EOP-004-2 may monitor meeting agendas and notes on the team's "Related Files" web page or may submit a request to join the team's "plus" email list to receive meeting agendas and

meeting notes as they are distributed to the team. To join the team's "plus" e-mail list, send an e-mail request to: sarcomm@nerc.net. Please indicate the drafting team's name in the subject line of the e-mail.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2009-01 Disturbance and Sabotage Reporting Initial Ballot_in
Ballot Period:	12/2/2011 - 12/12/2011
Ballot Type:	Initial
Total # Votes:	373
Total Ballot Pool:	424
Quorum:	**87.97 % The Quorum has been reached**
Weighted Segment Vote:	36.21 %
Ballot Results:	**The standard will proceed to recirculation ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	104	1	32	0.4	48	0.6	6	18
2 - Segment 2.	11	0.6	1	0.1	5	0.5	1	4
3 - Segment 3.	108	1	33	0.344	63	0.656	4	8
4 - Segment 4.	37	1	12	0.375	20	0.625	1	4
5 - Segment 5.	91	1	32	0.432	42	0.568	5	12
6 - Segment 6.	53	1	14	0.292	34	0.708	2	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	8	0.6	4	0.4	2	0.2	1	1
9 - Segment 9.	4	0.3	0	0	3	0.3	0	1
10 - Segment 10.	8	0.8	3	0.3	5	0.5	0	0
Totals	**424**	**7.3**	**131**	**2.643**	**222**	**4.657**	**20**	**51**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Abstain	
1	Avista Corp.	Scott J Kinney	Negative	View
1	Balancing Authority of Northern California	Kevin Smith	Negative	

1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Negative	View
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Negative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	View
1	CPS Energy	Richard Castrejana	Negative	View
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Affirmative	
1	Dominion Virginia Power	Michael S Crowley		
1	Duke Energy Carolina	Douglas E. Hils	Negative	View
1	East Kentucky Power Coop.	George S. Carruba		
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	View
1	Entergy Services, Inc.	Edward J Davis	Negative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		
1	Florida Power & Light Co.	Mike O'Neil		
1	Gainesville Regional Utilities	Luther E. Fair	Affirmative	View
1	Georgia Transmission Corporation	Jason Snodgrass	Abstain	
1	Grand River Dam Authority	James M Stafford		
1	Great River Energy	Gordon Pietsch	Affirmative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	View
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier		
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	View
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Negative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt	Negative	View
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Los Angeles Department of Water & Power	Ly M Le	Negative	
1	Lower Colorado River Authority	Martyn Turner		
1	Manitoba Hydro	Joe D Petaski	Affirmative	View
1	MEAG Power	Danny Dees	Abstain	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Affirmative	
1	National Grid	Saurabh Saksena		
1	Nebraska Public Power District	Cole C Brodine	Affirmative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	View
1	New York Power Authority	Arnold J. Schuff	Negative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	View
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	View
1	Orlando Utilities Commission	Brad Chase	Negative	View
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn	Negative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	

1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Negative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams		
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz		
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Negative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Negative	
1	Santee Cooper	Terry L Blackwell	Negative	View
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Sierra Pacific Power Co.	Rich Salgo	Negative	View
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Larry Akens	Abstain	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper		
2	Alberta Electric System Operator	Mark B Thompson	Abstain	View
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	View
2	California ISO	Rich Vine		
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Negative	View
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	View
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox		
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe		
2	Southwest Power Pool, Inc.	Charles Yeung		
3	AEP	Michael E Deloach	Negative	View
3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	View
3	City of Palo Alto	Eric R Scott	Affirmative	

3	City of Redding	Bill Hughes	Negative	View
3	Clatskanie People's Utility District	Brian Fawcett	Abstain	
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Negative	
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	View
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Negative	View
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	View
3	Entergy	Joel T Plessinger	Negative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Negative	View
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	View
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Kootenai Electric Cooperative	Dave Kahly	Affirmative	View
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Negative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Negative	View
3	Manitoba Hydro	Greg C. Parent	Affirmative	View
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage		
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Abstain	
3	Muscatine Power & Water	John S Bos	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	View
3	New York Power Authority	Marilyn Brown	Negative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	North Carolina Electric Membership Corp.	Doug White	Negative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	Ocala Electric Utility	David Anderson		
3	Old Dominion Electric Coop.	Bill Watson	Negative	View
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	View
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz		
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View

3	Rutherford EMC	Thomas M Haire	Affirmative	View
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	
3	Salt River Project	John T. Underhill	Negative	View
3	Santee Cooper	James M Poston	Negative	View
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen		
3	Snohomish County PUD No. 1	Mark Oens	Negative	View
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Co.	David B Coher	Negative	
3	Southern Maryland Electric Coop.	Mark R Jones	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L Donahey	Negative	
3	Tennessee Valley Authority	Ian S Grant		
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold		
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Negative	View
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Affirmative	View
4	Georgia System Operations Corporation	Guy Andrews	Negative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	View
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	Integrys Energy Group, Inc.	Christopher Plante		
4	LaGen	Richard Comeaux		
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	North Carolina Electric Membership Corp.	Bob Beadle	Negative	
4	Northern California Power Agency	Tracy R Bibb	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	
4	Seattle City Light	Hao Li	Negative	View
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	White River Electric Association Inc.	Frank L. Sampson	Abstain	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko		
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Negative	View
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Negative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	View

5	BrightSource Energy, Inc.	Chifong Thomas	Affirmative	
5	Caithness Long Island, LLC	Jason M Moore	Affirmative	
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Affirmative	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Negative	View
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cogentrix Energy, Inc.	Mike D Hirst	Affirmative	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	View
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Abstain	
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens	Negative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Negative	View
5	Dynegy Inc.	Dan Roethemeyer	Negative	View
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Energy	Ellen Oswald		
5	Electric Power Supply Association	John R Cashin		
5	Exelon Nuclear	Michael Korchynsky	Negative	
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner		
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Affirmative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	View
5	Indeck Energy Services, Inc.	Rex A Roehl		
5	JEA	John J Babik	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Negative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Manitoba Hydro	S N Fernando	Affirmative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Abstain	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Affirmative	View
5	New York Power Authority	Gerald Mannarino	Negative	
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	View
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard Kinas	Negative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	View
5	PPL Generation LLC	Annette M Bannon	Negative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn		
5	Sacramento Municipal Utility District	Bethany Hunter	Negative	
5	Salt River Project	William Alkema	Negative	

5	Santee Cooper	Lewis P Pierce	Negative	View
5	Seattle City Light	Michael J. Haynes	Negative	View
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Siemens PTI	Edwin Cano	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Leonard Rentmeester	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg	Negative	View
6	Bonneville Power Administration	Brenda S. Anderson	Negative	
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Negative	View
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Negative	View
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Negative	View
6	Entergy Services, Inc.	Terri F Benoit	Negative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	View
6	Imperial Irrigation District	Cathy Bretz	Affirmative	View
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	View
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Negative	
6	Luminant Energy	Brad Jones	Negative	View
6	Manitoba Hydro	Daniel Prowse	Affirmative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Negative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Negative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Negative	
6	Salt River Project	Steven J Hulet	Negative	
6	Santee Cooper	Michael Brown	Negative	View
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak		
6	Snohomish County PUD No. 1	William T Moojen	Negative	View
6	South California Edison Company	Lujuanna Medina	Negative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	

6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney		
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz		
8		James A Maenner	Negative	View
8	JDRJC Associates	Jim Cyrulewski	Abstain	
8	Pacific Northwest Generating Cooperative	Margaret Ryan	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Affirmative	
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	View
9	New York State Department of Public Service	Thomas Dvorsky	Negative	View
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson	Negative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	View
10	ReliabilityFirst Corporation	Anthony E Jablonski	Negative	View
10	SERC Reliability Corporation	Carter B. Edge	Negative	View
10	Southwest Power Pool RE	Emily Pennel	Affirmative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

2009-01 Disturbance and Sabotage Reporting Non-Binding Poll Results

Ballot Results	
Non-Binding Poll Name:	Project 2009-01 Disturbance And Sabotage Reporting-Non-binding Poll
Poll Period:	12/2/2011 - 12/12/2011
Total # Opinions:	264
Total Ballot Pool:	394
Summary Results:	85.28% of those who registered to participate provided an opinion or abstention; 45% of those who provided an opinion indicated support for the VRFs and VSLs.

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Abstain	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	View
1	Balancing Authority of Northern California	Kevin Smith	Negative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Abstain	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	Clark Public Utilities	Jack Stamper	Abstain	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	View
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Affirmative	

1	Dominion Virginia Power	Michael S Crowley		
1	Duke Energy Carolina	Douglas E. Hils	Negative	View
1	East Kentucky Power Coop.	George S. Carruba		
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	View
1	Entergy Services, Inc.	Edward J Davis	Negative	
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		
1	Florida Power & Light Co.	Mike O'Neil		
1	Gainesville Regional Utilities	Luther E. Fair	Affirmative	
1	Georgia Transmission Corporation	Jason Snodgrass	Abstain	
1	Grand River Dam Authority	James M Stafford		
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Abstain	
1	Hydro-Quebec TransEnergie	Bernard Pelletier		
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JEA	Ted Hobson	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt	Negative	
1	Lee County Electric Cooperative	John W Delucca	Abstain	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Los Angeles Department of Water & Power	Ly M Le	Negative	
1	Lower Colorado River Authority	Martyn Turner		
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Abstain	
1	MidAmerican Energy Co.	Terry Harbour	Negative	
1	Minnkota Power Coop. Inc.	Richard Burt	Affirmative	
1	National Grid	Saurabh Saksena		
1	Nebraska Public Power District	Cole C Brodine	Abstain	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Abstain	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	View

1	PacifiCorp	Ryan Millard	Abstain	
1	PECO Energy	Ronald Schloendorn	Negative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Negative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams		
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz		
1	Rochester Gas and Electric Corp.	John C. Allen	Abstain	
1	Sacramento Municipal Utility District	Tim Kelley	Negative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Negative	
1	Santee Cooper	Terry L Blackwell	Negative	View
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens		
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Abstain	
1	South California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Affirmative	
1	Southwestern Power Administration	Angela L Summer	Negative	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Larry Akens	Abstain	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	View
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Westar Energy	Allen Klassen	Abstain	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper		
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine		
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Negative	View
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox		
2	New Brunswick System Operator	Alden Briggs	Abstain	
2	New York Independent System	Gregory Campoli	Abstain	

	Operator			
2	PJM Interconnection, L.L.C.	Tom Bowe		
2	Southwest Power Pool, Inc.	Charles Yeung		
3	AEP	Michael E Deloach	Negative	View
3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Abstain	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	View
3	City of Redding	Bill Hughes	Negative	View
3	Clatskanie People's Utility District	Brian Fawcett	Abstain	
3	Cleco Corporation	Michelle A Corley	Abstain	View
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Negative	
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	
3	Constellation Energy	CJ Ingersoll	Abstain	
3	Consumers Energy	Richard Blumenstock	Negative	
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Abstain	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	View
3	Entergy	Joel T Plessinger	Negative	
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Negative	View
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Abstain	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Kootenai Electric Cooperative	Dave Kahly	Affirmative	

3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Negative	
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Abstain	
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage		
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Abstain	
3	Muscatine Power & Water	John S Bos	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	Marilyn Brown	Negative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Ocala Electric Utility	David Anderson		
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	View
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz		
3	Potomac Electric Power Co.	Robert Reuter	Abstain	
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	
3	Salt River Project	John T. Underhill	Negative	View
3	Santee Cooper	James M Poston	Negative	View
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen		
3	Snohomish County PUD No. 1	Mark Oens	Negative	View
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	Southern Maryland Electric Coop.	Mark R Jones	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L Donahey	Negative	
3	Tennessee Valley Authority	Ian S Grant		
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Abstain	

3	Xcel Energy, Inc.	Michael Ibold		
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Negative	View
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	View
4	Consumers Energy	David Frank Ronk	Negative	
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Abstain	
4	Georgia System Operations Corporation	Guy Andrews	Negative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante		
4	LaGen	Richard Comeaux		
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Northern California Power Agency	Tracy R Bibb	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Abstain	
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	
4	Seattle City Light	Hao Li	Negative	View
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko		
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Abstain	
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	

5	BrightSource Energy, Inc.	Chifong Thomas	Affirmative	
5	Caithness Long Island, LLC	Jason M Moore	Abstain	
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Negative	View
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Abstain	View
5	Cogentrix Energy, Inc.	Mike D Hirst	Affirmative	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	View
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Abstain	
5	Consumers Energy Company	David C Greyerbiehl	Abstain	
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens	Affirmative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	Duke Energy	Dale Q Goodwine	Negative	View
5	Dynegy Inc.	Dan Roethemeyer	Negative	View
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Energy	Ellen Oswald		
5	Electric Power Supply Association	John R Cashin		
5	Exelon Nuclear	Michael Korchynsky	Negative	
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner		
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Gainesville Regional Utilities	Karen C Alford	Abstain	
5	Great River Energy	Preston L Walsh	Affirmative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	Indeck Energy Services, Inc.	Rex A Roehl		
5	JEA	John J Babik	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Negative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Manitoba Hydro	S N Fernando	Affirmative	

5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Abstain	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Abstain	
5	New York Power Authority	Gerald Mannarino	Negative	
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	View
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Abstain	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Negative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn		
5	Sacramento Municipal Utility District	Bethany Hunter	Negative	
5	Salt River Project	William Alkema	Negative	
5	Santee Cooper	Lewis P Pierce	Negative	View
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Siemens PTI	Edwin Cano	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	View
5	Southern Company Generation	William D Shultz	Negative	
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Xcel Energy, Inc.	Liam Noailles		
6	ACES Power Marketing	Jason L Marshall	Affirmative	
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Affirmative	

6	Arkansas Electric Cooperative Corporation	Keith Sugg	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Abstain	
6	City of Redding	Marvin Briggs	Negative	View
6	Cleco Power LLC	Robert Hirchak	Abstain	View
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Negative	View
6	Constellation Energy Commodities Group	Brenda Powell	Negative	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy Carolina	Walter Yeager	Negative	View
6	Entergy Services, Inc.	Terri F Benoit	Negative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	View
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Negative	
6	Luminant Energy	Brad Jones	Negative	View
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Negative	
6	PacifiCorp	Scott L Smith	Abstain	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Negative	View
6	Progress Energy	John T Sturgeon	Negative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Negative	
6	Salt River Project	Steven J Hulet	Negative	
6	Santee Cooper	Michael Brown	Negative	View
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak		
6	Snohomish County PUD No. 1	William T Moojen	Abstain	
6	South California Edison Company	Lujuanna Medina	Negative	
6	Southern Company Generation and	John J. Ciza	Negative	View

	Energy Marketing			
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Westar Energy	Grant L Wilkerson	Abstain	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney		
6	Xcel Energy, Inc.	David F. Lemmons		
8		Roger C Zaklukiewicz		
8		Edward C Stein	Affirmative	
8		James A Maenner	Negative	
8	APX	Michael Johnson	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Abstain	
8	Power Energy Group LLC	Peggy Abbadini	Abstain	
8	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	View
10	ReliabilityFirst Corporation	Anthony E Jablonski	Negative	View
10	SERC Reliability Corporation	Carter B. Edge	Abstain	
10	Southwest Power Pool RE	Emily Pennel	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Consideration of Comments

Disturbance and Sabotage Reporting (Project 2009-01)

The Disturbance and Sabotage Reporting Drafting Team thanks all commenters who submitted comments on the second formal posting for Project 2009-01—Disturbance and Sabotage Reporting. The standard was posted for a 45-day public comment period from October 28, 2011 through December 12, 2011 and included an initial ballot during the last 10 days of the comment period. Stakeholders were asked to provide feedback on the standard and associated documents through a special electronic comment form. There were 76 sets of comments, including comments from approximately 171 different people from approximately 140 companies representing nine of the ten Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page:

http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President of Standards and Training, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

Summary Consideration

EOP-004-2 was posted for a 45-day formal comment period and initial ballot from October 28-December 12, 2011. The DSR SDT received comments from stakeholders to improve the readability and clarity of the requirements of the standard. The revisions that were made to the standard are summarized in the following paragraphs.

Purpose Statement

The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:

> "To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."

[1] The appeals process is in the Standard Processes Manual
http://www.nerc.com/files/Appendix_3A_Standard_Processes_Manual_Rev%201_20110825.pdf

Operating Plan

Based on stakeholder comments, Requirement R1 was revised for clarity. Part 1.1 was revised to replace the word "identifying" with "recognizing" and Part 1.2 was eliminated. This also aligns the language of the standard with FERC Order 693, Paragraph 471.

> "(2) specify baseline requirements regarding what issues should be addressed in the **procedures for recognizing** {emphasis added} sabotage events and making personnel aware of such events;"

Requirement R1, Part 1.3 (now Part 1.2) was revised by eliminating the phrase "as appropriate" and adding language indicating that the Responsible Entity is to define its process for reporting and with whom to report events. Part 1.2 now reads:

> "1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."

The SDT envisions that most entities will only need to slightly modify their existing CIP-001 Sabotage Reporting procedures to comply with the Operating Plan requirement in this proposed standard. As many of the features of both sabotage reporting procedures and the Operating Plan are substantially similar, the SDT feels that some information in the sabotage reporting procedures may need to updated and verified.

Operating Plan Review and Communications Testing

Requirement R1, Part 1.4 was removed and Requirement 1, Part, 1.5 was separated out as new Requirement 4. Requirement R4 was revised and is now R3. FERC Order 693, Paragraph 466 includes provisions for periodic review and update of the Operating Plan:

> "466. The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."

Requirement R3 requires an annual test of the communication portion of Requirement R1 while Requirement R4 requires an annual review of the Operating Plan.:

> "R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2."
>
> "R4. Each Responsible Entity shall conduct an annual review of the event reporting Operating Plan in Requirement R1."

The DSR SDT envisions that the annual test will include verification that communication information contained in the Operating Plan is correct. As an example, the annual update of the Operating Plan could include calling "others as defined in the Responsibility Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. Note that there is no requirement to test the reporting of events to the Electric Reliability Organization and the Responsible Entity's Reliability Coordinator.

Operating Plan Implementation

Most stakeholders indicated that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to:

> "R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."

Reporting Timelines

The DSR SDT received many comments regarding the various entries of Attachment 1. Many commenters questioned the reliability benefit of reporting events to the ERO within 1 hour. Most of the events with a one hour reporting requirement were revised to 24 hours based on stakeholder comments; those types of events are currently required to be reported within 24 hours in the existing mandatory and enforceable standards. The only remaining type of event that is to be reported within one hour is "A reportable Cyber Security Incident" as it is required by CIP-008 and FERC Order 706, Paragraph 673:

> "direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"

The table was reformatted to separate one hour reporting and 24 hour reporting. The last column of the table was also deleted and the information contained in the table was transferred to the sentence above each table. These sentences are:

> "One Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the event."

> "Twenty-four Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within twenty-four hour of recognition of the event."

Note that the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.

Cyber-Related Events

The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1. Stakeholders pointed out these events are adequately addressed through the CIP-008 and "Damage or Destruction of a Facility "reporting thresholds. CIP-008 addresses Cyber Security Incidents which are defined as:

> "Any malicious act or suspicious event that:
>
> - Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,
> - Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset."

A Critical Asset is defined as:

> "Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."

Since there is an existing event category for damage or destruction of Facilities, having a separate event for "Damage or Destruction of a Critical Asset" is unnecessary.

Damage or Destruction

The event for "Destruction of BES equipment" has been revised to "Damage or destruction of a Facility". The threshold for reporting information was expanded for clarity:

> "Damage or destruction of a Facility that: affects an IROL
> OR
> Results in the need for actions to avoid an Adverse Reliability Impact
> OR
> Results from intentional human action."

Facility Definition

The DSR SDT used the defined term "Facility" to add clarity for this event as well as other events in Attachment 1. A Facility is defined as:

> "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"

The DSR SDT did not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.

Physical Threats

Several stakeholders expressed concerns relating to the "Forced Intrusion" event. Their concerns related to ambiguous language in the footnote. The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "Any physical threat that could impact the operability of a Facility".

Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.

The footnote regarding this event type was expanded to provide additional guidance in:

> "Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also, report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."

Use of DOE OE-417

The DSR SDT received many comments requesting consistency with DOE OE-417 thresholds and timelines. These items, as well as, the Events Analysis Working Group's (EAWG) requirements were considered in creating Attachment 1, but differences remain for the following reasons:

- EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'
- OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America
- NERC has no control over the criteria in OE-417, which can change at any time
- Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary

In an effort to minimize administrative burden, US entities may use the OE-417 form rather than Attachment 2 to report under EOP-004. The SDT was informed by the DOE of its new online process coming later this year. In this process, entities may be able to record email addresses associated with their Operating Plan so that when the report is submitted to DOE, it will automatically be forwarded to the posted email addresses, thereby eliminating some administrative burden to forward the report to multiple organizations and agencies.

Miscellaneous

Other minor edits were made to Attachment 1. Several words were capitalized but not defined terms. The DSR SDT did not intend for these terms to be capitalized (defined terms) and these words were reverted to lower case. The event type "Loss of monitoring or all voice communication capability" was divided into two separate events as "Loss of monitoring capability" and "Loss of all voice communication capability".

Attachment 2 was updated to reflect the revisions to Attachment 1. The reference to "actual or potential events" was removed. Also, the event type of "other" and "fuel supply emergency" was removed as well.

It was noted that 'Transmission Facilities' is not a defined term in the NERC Glossary. Transmission and Facilities are separately defined terms. The combination of these two definitions are what the DSR SDT has based the applicability of "Transmission Facilities" in Attachment 1.

Index to Questions, Comments, and Responses

1. The DSR SDT has revised EOP-004-2 to remove the training requirement R4 based on stakeholder comments from the second formal posting. Do you agree this revision? If not, please explain in the comment area below..... 18
2. The DSR SDT includes two requirement regarding implementation of the Operating Plan specified in Requirement R1. The previous version of the standard had a requirement to implement the Operating plan as well as a requirement to report events. The two requirements R2 and R3 were written to delineate implementation of the Parts of R1. Do you agree with these revisions? If not, please explain in the comment area below..... 42

   R2. Each Responsible Entity shall implement the parts of its Operating Plan that meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts 1.4 and 1.5 as specified.

   R3. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.

3. The DSR SDT revised reporting times for many events listed in Attachment 1 from one hour to 24 hours. Do you agree with these revisions? If not, please explain in the comment area below..... .. 79
4. Do you have any other comment, not expressed in the questions above, for the DSR SDT?.....156

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Gerald Beckerle	SERC OC Standards Review Group	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Charlie Cook	TVA		5, 6, 1, 3
2.	Jake Miller	Dynegy	SERC	5
3.	Joel Wise	TVA	SERC	1, 3, 5, 6
4.	Tim Hattaway	PowerSouth	SERC	1, 5
5.	Robert Thomasson	BREC	SERC	1
6.	Shaun Anders	CWLP	SERC	1, 3
7.	Jim Case	Entergy	SERC	1, 3, 6
8.	Tim Lyons	OMU	SERC	3, 5
9.	Len Sandberg	Dominion Virginia Power	SERC	1, 3, 5, 6
10.	Brad Young	LGE-KU	SERC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
11. Larry Akens	TVA	SERC 1, 3, 5, 6										
12. Mike Hirst	Cogentrix	SERC 5										
13. Wayne Van Liere	LGE-KU	SERC 3										
14. Scott Brame	NCEMC	SERC 1, 3, 4, 5										
15. Steve Corbin	SERC Reliability Corp.	SERC 10										
16. John Johnson	SERC Reliability Corp.	SERC 10										
17. John Troha	SERC Reliability Corp.	SERC 10										
2. Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliaiblity Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Ben Wu	Orange and Rockland Utilities	NPCC	1
7.	Peter Yost	Consolidated Edison co. of New York, Inc.	NPCC	3
8.	Kathleen Goodman	ISO - New England	NPCC	2
9.	Chantel Haswell	FPL Group, Inc.	NPCC	5
10.	David Kiguel	Hydro One Networks Inc.	NPCC	1
11.	Michael R. Lombardi	Northeast Utilities	NPCC	1
12.	Randy Macdonald	New Brunswick Power Transmission	NPCC	9
13.	Bruce Metruck	New York Power Authority	NPCC	6
14.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
15.	Robert Pellegrini	The United Illuminating Company	NPCC	1
16.	Si-Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
17.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
18.	Saurabh Saksena	National Grid	NPCC	1
19.	Michael Schiavone	National Grid	NPCC	1
20.	Wayne Sipperly	New York Power Authority	NPCC	5
21.	Tina Teng	Independent Electricity System Operator	NPCC	2
22.	Donald Weaver	New Brunswick System Operator	NPCC	2

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Group	Steve Alexanderson	Pacific Northwest Small Public Power Utility Comment Group			X	X					X	

	Additional Member	Additional Organization	Region	Segment Selection
1.	Russell A. Noble	Cowlitz County PUD No. 1	WECC	3, 4, 5
2.	Ronald Sporseen	Blachly-Lane Electric Cooperative	WECC	3
3.	Ronald Sporseen	Central Electric Cooperative	WECC	3
4.	Ronald Sporseen	Consumers Power	WECC	1, 3
5.	Ronald Sporseen	Clearwater Power Company	WECC	3
6.	Ronald Sporseen	Douglas Electric Cooperative	WECC	3
7.	Ronald Sporseen	Fall River Rural Electric Cooperative	WECC	3
8.	Ronald Sporseen	Northern Lights	WECC	3
9.	Ronald Sporseen	Lane Electric Cooperative	WECC	3
10.	Ronald Sporseen	Lincoln Electric Cooperative	WECC	3
11.	Ronald Sporseen	Raft River Rural Electric Cooperative	WECC	3
12.	Ronald Sporseen	Lost River Electric Cooperative	WECC	3
13.	Ronald Sporseen	Salmon River Electric Cooperative	WECC	3
14.	Ronald Sporseen	Umatilla Electric Cooperative	WECC	3
15.	Ronald Sporseen	Coos-Curry Electric Cooperative	WECC	3
16.	Ronald Sporseen	West Oregon Electric Cooperative	WECC	3
17.	Ronald Sporseen	Pacific Northwest Generating Cooperative	WECC	3, 4, 8
18.	Ronald Sporseen	Power Resources Cooperative	WECC	5

4.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Allen	City Utilities of Springfield	SPP	1, 4
2.	Clem Cassmeyer	Western Farmer's Electric Cooperative	SPP	1, 3, 5
3.	Michelle Corley	Cleco Power	SPP	1, 3, 5
4.	Kevin Emery	Carthage Water and Electric Plant	SPP	NA
5.	Jonathan Hayes	Southwest Power Pool	SPP	2
6.	Philip Huff	Arkansas Electric Cooperative Corporation	SPP	3, 4, 5, 6
7.	Ashley Stringer	Oklahoma Municipal Power Authority	SPP	4

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

	Additional Member	Additional Organization	Region	Segment Selection
1.	Patricia Robertson	BC Hydro	WECC	1
2.	Rama Vinnakota	BC Hydro	WECC	2
3.	Pat Harrington	BC Hydro	WECC	3
4.	Clement Ma	BC Hydro	WECC	5
5.	Daniel O'Hearn	BC Hydro	WECC	6

6.	Group	Mary Jo Cooper	ZGlobal on behalf of City of Ukiah, Alameda Municipal Power, Salmen River Electric, City of Lodi			X							X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Elizabeth Kirkley	City of Lodi	WECC	3
2.	Colin Murphey	City of Ukiah	WECC	3
3.	Douglas Draeger	Alameda Municipal Power	WECC	3
4.	Ken Dizes	Salmen River Electric Coop	WECC	3

7.	Group	WILL SMITH	MRO NSRF										

	Additional Member	Additional Organization	Region	Segment Selection
1.	MAHMOOD SAFI	OPPD	MRO	1, 3, 5, 6
2.	CHUCK LAWRENCE	ATC	MRO	1
3.	TOM WEBB	WPS	MRO	3, 4, 5, 6
4.	JODI JENSON	WAPA	MRO	1, 6
5.	KEN GOLDSMITH	ALTW	MRO	4
6.	ALICE IRELAND	NSP (XCEL)	MRO	1, 3, 5, 6
7.	DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6
8.	ERIC RUSKAMP	LES	MRO	1, 3, 5, 6
9.	JOE DEPOORTER	MGE	MRO	3, 4, 5, 6
10.	SCOTT NICKELS	RPU	MRO	4
11.	TERRY HARBOUR	MEC	MRO	1, 3, 5, 6
12.	MARIE KNOX	MISO	MRO	2
13.	LEE KITTELSON	OTP	MRO	1, 3, 4, 5
14.	SCOTT BOS	MPW	MRO	1, 3, 5, 6
15.	TONY EDDLEMAN	NPPD	MRO	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
16. MIKE BRYTOWSKI	GRE	MRO	1, 3, 5, 6										
17. RICHARD BURT	MPC	MRO	1, 3, 5, 6										
8.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No Additional members listed.													
9.	Group	Jesus Sammy Alcaraz	Imperial Irrigation District	X		X	X	X	X				
Additional Member	Additional Organization	Region	Segment Selection										
1. Tino Zaragoza	IID	WECC	1										
2. Jesus Sammy Alcaraz	IID	WECC	3										
3. Diana Torres	IID	WECC	4										
4. Marcela Caballero	IID	WECC	5										
5. Cathy Bretz	IID	WECC	6										
10.	Group	Jean Nitz	ACES Power Marketing Standards Collaborators						X				
Additional Member	Additional Organization	Region	Segment Selection										
1. Chris Bradley	Big Rivers Electric Corporation	SERC	1										
2. Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5										
3. Susan Sosbe	Wabash Valley Power Association	RFC	3										
4. Scott Brame	North Carolina Electric Membership Corporation	RFC	5, 1, 3, 4										
5. Shari Heino	Brazos Electric Power Cooperative, Inc.	ERCOT	1										
6. Lindsay Shepard	Western Farmers Electric Cooperative	SPP	1, 5										
11.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				
Additional Member	Additional Organization	Region	Segment Selection										
1. Timothy Beyrle	City of New Smyrna Beach	FRCC	4										
2. Greg Woessner	KissimmeeUtility Authority	FRCC	3										
3. Jim Howard	Lakeland Electric	FRCC	3										
4. Lynne Mila	City of Clewiston	FRCC	3										
5. Joe Stonecipher	Beaches Energy Services	FRCC	1										
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4										
7. Randy Hahn	Ocala Utility Services	FRCC	3										
12.	Group	Terry L. Blackwell	Santee Cooper	X		X		X	X				
Additional Member	Additional Organization	Region	Segment Selection										

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
1. S. T. Abrams	Santee Cooper	SERC 1										
2. Wayne Ahl	Santee Cooper	SERC 1										
3. Rene Free	Santee Cooper	SERC 1										
13. Group	Joe Tarantino	Sacramento Municipal Utility District (SMUD)	X		X	X	X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Kevin Smith	BANC	WECC 1										
14. Group	Robert Rhodes	SPP Standards Review Group		X								
Additional Member	Additional Organization	Region Segment Selection										
1. John Allen	City Utilities of Springfield	SPP 1, 4										
2. Clem Cassmeyer	Western Farmer's Electric Cooperative	SPP 1, 3, 5										
3. Michelle Corley	Cleco Power	SPP 1, 3, 5										
4. Kevin Emery	Carthage Water and Electric Plant	SPP NA										
5. Jonathan Hayes	Southwest Power Pool	SPP 2										
6. Philip Huff	Arkansas Electric Cooperative Corporation	SPP 3, 4, 5, 6										
7. Ashley Stringer	Oklahoma Municipal Power Authority	SPP 4										
15. Group	Connie Lowe	Dominion	X		X		X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Louis Slade		RFC 3, 6										
2. Michael Crowley		SERC 1, 3										
3. Mike Garton		NPCC 5, 6										
4. Michael Gildea		MRO 5, 6										
16. Group	Sam Ciccone	FirstEnergy	X		X	X	X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Doug Hohlbaugh	FE	RFC 1, 3, 4, 5, 6										
2. Larry Raczkowski	FE	RFC 1, 3, 4, 5, 6										
3. Jim Eckels	FE	RFC 1										
4. John Reed	FE	RFC 1										
5. Ken Dresner	FE	RFC 5										
6. Bill Duge	FE	RFC 5										
7. Kevin Querry	FE	RFC 5										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
17.	Group	Annette M. Bannon	PPL Electric Utilities and PPL Supply Organizations`	X				X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Brenda Truhe	PPL Electric Utilities	RFC	1
2.	Annette Bannon	PPL Generation	RFC	5
3.	Annette Bannon	PPL Generation	WECC	5
4.	Mark Heimbach	PPL EnergyPlus	MRO	6
5.	Mark Heimbach	PPL EnergyPlus	NPCC	6
6.	Mark Heimbach	PPL EnergyPlus	RFC	6
7.	Mark Heimbach	PPL EnergyPlus	SERC	6
8.	Mark Heimbach	PPL EnergyPlus	SPP	6
9.	Mark Heimbach	PPL EnergyPlus	WECC	6

18.	Group	Tom McElhinney	Electric Compliance	X		X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Ted Hobson		FRCC	1
2.	John Babik		FRCC	5
3.	Garry Baker			3

19.	Group	Michael Gammon	Kansas City Power & Light	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Scott Harris	KCP&L	SPP	1, 3, 5, 6
2.	Monica Strain	KCP&L	SPP	1, 3, 5, 6
3.	Brett Holland	KCP&L	SPP	1, 3, 5, 6
4.	Jennifer Flandermeyer	KCP&L	SPP	1, 3, 5, 6

20.	Individual	Stewart Rake	Luminant Power					X					
21.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
22.	Individual	Janet Smith, Regulatory Affairs Supervisor	Arizona Public Service Company	X		X		X	X				
23.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
24.	Individual	Silvia Parada Mitchell	Compliance & Responsbility Office	X		X		X	X				
25.	Individual	Antonio Grayson	Southern Comnpany	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
26.	Individual	John Brockhan	CenterPoint Energy	X									
27.	Individual	Brenton Lopez	Salt River Project	X		X		X	X				
28.	Individual	Bo Jones	Westar Energy	X		X		X	X				
29.	Individual	Michael Johnson	APX Power Markets (NCR-11034)						X				
30.	Individual	David Proebstel	Clallam County PUD No.1			X							
31.	Individual	Michael Moltane	ITC	X									
32.	Individual	Tracy Richardson	Springfield Utility Board			X							
33.	Individual	Kasia Mihalchuk	Manitoba Hydro	X		X		X	X				
34.	Individual	Kevin Conway	Intellibind								X		
35.	Individual	Chris Higgins / Jim Burns / Ted Snodgrass / Jeff Millennor / Russell Funk	Bonneville Power Administration	X		X		X	X				
36.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				
37.	Individual	David Burke	Orange and Rockland Utilities, Inc.	X		X							
38.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
39.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
40.	Individual	Rodney Luck	Los Angeles Department of Water and Power	X		X		X	X				
41.	Individual	Daniel Duff	Liberty Electric Power					X					
42.	Individual	Lisa Rosintoski	Colorado Springs Utilities	X		X		X	X				
43.	Individual	Michael Falvo	Independent Electricity System Operator		X								
44.	Individual	John Bee on Behalf of Exelon	Exelon	X		X		X					
45.	Individual	John D. Martinsen	Public Utility District No. 1 of Snohomish County										
46.	Individual	RoLynda Shumpert	South Carolina Electric and Gas	X		X		X	X				
47.	Individual	Kathleen Goodman	ISO New England		X								

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
48.	Individual	Curtis Crews	Texas Reliability Entity										X
49.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
50.	Individual	Anthony Jablonski	ReliabilityFirst										X
51.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
52.	Individual	Dennis Sismaet	Seattle City Light	X		X	X	X	X				
53.	Individual	John Seelke	PSEG	X		X		X	X				
54.	Individual	Barry Lawson	NRECA										
55.	Individual	Terry Harbour	MidAmerican Energy	X		X		X					
56.	Individual	Thad Ness	American Electric Power	X		X		X	X				
57.	Individual	Guy Andrews	Georgia System Operations Corporation	X		X	X	X	X				
58.	Individual	Ed Davis	Entergy Services										
59.	Individual	Margaret McNaul	Thompson Coburn LLP on behalf of Miss. Delta Energy Agency										
60.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
61.	Individual	Kirit Shah	Ameren	X		X		X	X				
62.	Individual	Linda Jacobson-Quinn	FEUS			X							
63.	Individual	Tom Foreman	Lower Colorado River Authority	X		X		X	X				
64.	Individual	Richard Salgo	NV Energy										
65.	Individual	Nathan Mitchell	American Public Power Association			X							
66.	Individual	Angela Summer	Southwestern Power Administration	X									
67.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
68.	Individual	Tim Soles	Occidental Power Services, Inc. (OPSI)			X			X				
69.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
70.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
71.	Individual	James Sauceda	Energy Northwest - Columbia					X					
72.	Individual	Scott Berry	Indiana Municipal Power Agency				X						

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
73.	Individual	Maggy Powell	Constellation Energy on behalf of Baltimore Gas & Electric, Constellation Power Generation, Constellation Energy Commodities Group, Constellation Control and Dispatch, Constellation NewEnergy and Constellation Energy Nuclear Group.	X		X		X	X				
74.	Individual	Michael Brytowski	Great River Energy	X		X		X	X				
75.	Individual	Christine Hasha	Electric Reliability Council of Texas, Inc.		X								
76.	Individual	Darryl Curtis	Oncor Electric Delivery Company LLC	X									

1. The DSR SDT has revised EOP-004-2 to remove the training requirement R4 based on stakeholder comments from the second formal posting. Do you agree this revision? If not, please explain in the comment area below.

Summary Consideration: As a result of the industry comments, the SDT has further modified the standard as follows:

- Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom events are communicated.
- Combined relevant parts of Requirement R1, Parts 1.4, 1.5 and Requirement R4 into Requirement 1, Part 1.3.
- Deleted the requirement for drills or exercises
- Clarified that only Registered Entities conduct annual tests of the communication process outlined in Requirement 1, Part 1.2
- Changed the review of the Operating Plan to 'annually'

The DSR SDT envisions the testing under Requirement R1, Part 1.3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsibility Entity's Operating Plan" (see Part 1.2) to verify their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.

Despite some industry opposition, both the periodic review of the Operating Plan and the testing requirements were maintained to meet the intent of FERC Order 693, Paragraph 466:

"The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."

Organization	Yes or No	Question 1 Comment
Beaches Energy Services, City of	Negative	First, I wish to thank the SDT for their hard work and making significant progress in significant improvements in the standard. I commend the

Organization	Yes or No	Question 1 Comment
Green Cove Springs		direction that the SDT is taking. There are; however, a few unresolved issues that cause me to not support the standard at this time. 1. An issue of possible differences in interpretation between entities and compliance monitoring and enforcement is the phrase in 1.3 that states "the following as appropriate". Who has the authority to deem what is appropriate? The requirements should be clear that the Responsible Entity is the decision maker of who is appropriate, otherwise there is opportunity for conflict between entities and compliance. *Requirement R1,* Part *1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to communicate events to as stated in the entity's Operating Plan.* In addition, 1.4 is onerous and burdensome regarding the need to revise the plan within 90 days of "any" change, especially considering the ambiguity of "other circumstances". "Other circumstances" is open to interpretation and a potential source of conflict. *Requirement R1, Part 1.4 was removed from the standard.*
Response: Thank you for your comment. Please see response above.		
New Brunswick Power Transmission Corporation	Negative	It is NBPT's opinion that because this is a standard associated with reporting events after an occurrence, it is overly burdensome to require drills and exercises for verification purposes as described in R4. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications*

Organization	Yes or No	Question 1 Comment
		process in Part 1.2.
Response: Thank you for your comment. Please see response above.		
United Illuminating Co.	Negative	R4 is not clear what is expected. There is a difference between testing a process that consists of identify an event then select commuication contacts versus needing to test contacts for each event in Attachment 1 and drill each event and document each event drill. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement r3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* In R2 the phrase "as specified" should be replaced or completed, as specified by what. *The DSR SDT has deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read: "Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004*

Organization	Yes or No	Question 1 Comment
		Attachment1."
Response: Thank you for your comment. Please see response above.		
City of Farmington	Negative	R4 requires verification through a drill or exercise the communication process created as part of R1.3. Clarification of what a drill or exercise should be considered. In order to show compliance to R4 would the entity have to send a pseudo event report to Internal Personnel, the Regional Entity, NERC ES-ISAC, Law Enforcement, and Governmental or provincial agencies listed in R1.3 to verify the communications plan? It would not be a burden on the entity so much, however, I'm not sure the external parties want to be the recipient of approximately 2000 psuedo event reports annually. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.*
Response: Thank you for your comment. Please see response above.		
Hydro One Networks, Inc.	Negative	Referring to Requirement R4, the communication process can be verified without having to go through a drill or exercise. Any specific testing or

Organization	Yes or No	Question 1 Comment
		verification of the process is the responsibility of the Responsible Entity. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *Despite some industry opposition, both periodic review of the Operating Plan and the test requirements were maintained to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
Ameren Services	Negative	The current language in the parenthesis of R4 suggests that the training requirement was actually not removed, in that "a drill or exercise" constitutes training. As documented in the last sentence of the Summary of Key Concepts section, "The proposed standard deals exclusively with after-the-fact reporting." We feel that training, even if it is called drills or exercises is not necessary for an after-the-fact report. *Requirement R4 related to an annual test of the communication portion of*

Organization	Yes or No	Question 1 Comment
		Requirement R1 by a drill or exercise and this has been removed. This has been revised to: *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *Despite some industry opposition, both periodic review of the Operating Plan and the test requirements were maintained to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
Liberty Electric Power LLC	Negative	Voting no due to training not being an option to fill the "drill" requirement. The reason for R4 seems to be to assure personnel will respond to an event in accordance with the entity procedure. Entities meet their obligations for other regulatory requirements with training, and should be permitted to do so for R4. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including*

Organization	Yes or No	Question 1 Comment
		notification to the Electric Reliability Organization, of the communications process in Part 1.2. *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. This language does not preclude the verification of contact information taking place during a training event.*
Response: Thank you for your comment. Please see response above.		
ACES Power Marketing, Hoosier Energy Rural Electric Cooperative, Inc., Sunflower Electric Power Corporation, Great River Energy	Negative	We appreciate the efforts of the SDT in considering the comments of stakeholders from prior comment periods. We believe this draft is greatly improved over the previous version and we agree with the elimination of the term "sabotage" which is a difficult term to define. The determination of an act of sabotage should be left to the proper law enforcement authorities. However, we also realize that the proper authorities would be hard pressed to make these determinations without reporting from industry when there are threats to BES equipment or facilities. We understand and agree there should be verification of the information required for such reporting (contact information, process flow charts, etc). But we still believe improvements can be made to the draft standard. The use of the words "or through a drill or exercise" in Requirement R4 still implies that training is required if no actual event has occurred. When you conduct a fire "drill" you are training your employees on evacuation routes and who they need to report to. Not only are you verifying your process but you are training your employees as well. It is imperative that the information in the Event

Organization	Yes or No	Question 1 Comment
		Reporting process is correct but we don't agree that performing a drill on the process is necessary. We recommend modifying the requirement to focus on verifying the information needed for appropriate communications on an event. And we agree this should take place at least annually. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *This language does not preclude the verification of contact information taking place during a training event.*
Response: Thank you for your comment. Please see response above.		
Florida Municipal Power Agency	No	First, we wish to thank the SDT for their hard work and making significant progress in significant improvements in the standard. We commend the direction that the SDT is taking. There are; however, a few unresolved issues that cause us to not support the standard at this time. An issue of possible differences in interpretation between entities and compliance monitoring and enforcement is the phrase in 1.3 that states "the following as appropriate". Who has the authority to deem what is appropriate? The

Organization	Yes or No	Question 1 Comment
		requirements should be clear that the Responsible Entity is the decision maker of who is appropriate, otherwise there is opportunity for conflict between entities and compliance. *Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to communicate events to as stated in the entity's Operating Plan. Part 1.2 now reads: "A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."* In addition, 1.4 is onerous and burdensome regarding the need to revise the plan within 90 days of "any" change, especially considering the ambiguity of "other circumstances". "Other circumstances" is open to interpretation and a potential source of conflict. *Requirement R1, Part 1.4 was removed from the standard.*
Response: Thank you for your comment. Please see response above.		
Illinois Municipal Electric Agency	No	IMEA agrees with the removal of the training requirement, but also believes verification is not a necessary requirement for this standard; therefore, R4 is not necessary and should be removed. *Requirement R4 related to an annual test of the communication portion of Requirement 1. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including*

Organization	Yes or No	Question 1 Comment
		notification to the Electric Reliability Organization, of the communications process in Part 1.2. *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.*
Response: Thank you for your comment. Please see response above.		
Indiana Municipal Power Agency	No	IMPA does not believe that R4 is necessary. In addition, if a drill or exercise is used to verify the communication process, some of the parties listed in R1.3 may not want to participate in the drill or exercise every 15 months, such as law enforcement and governmental agencies. IMPA would propose a contacting these agencies every 15 months to verify their contact information only and updating their information in the plan as needed, without performing a drill or exercise. *This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *The testing requirement is included in the Standard to meet the intent of*

Organization	Yes or No	Question 1 Comment
		FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."
Response: Thank you for your comment. Please see response above.		
ISO New England	No	Please see further comments; we do not believe R4 is a necessary requirement in the standard and suggest it be deleted. *Requirement R4 related to an annual test of the communication portion of Requirement 1. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *The testing requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comment. Please see response above.		
Northeast Power Coordinating Council	No	Requirement R4 is unnecessary. Whether or not the process, plan, procedure, etc. is "verified" is of no consequence. EOP standards are intended to have entities prepare for likely events (restoration/evacuation), and to provide tools for similar unforeseen events (ice storms, tornadoes, earthquakes, etc.). They should not force a script when results are what matters. *Requirement R4 related to an annual test of the communication portion of Requirement 1. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *The testing requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 1 Comment
Southern Company	No	Southern agrees with removing the training requirement of R4 from the previous version of the standard. However, Southern suggests that drills and exercises are also training and R4 in this revised standard should be removed in its entirety *The "drill or exercise" language has been deleted. Requirement R4 related to an annual test of the communication portion of Requirement 1. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *The testing requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
Ameren	No	The current language in the parenthesis of R4 suggests that the training requirement was actually not removed, in that "a drill or exercise" constitutes training. As documented in the last sentence of the Summary of

Organization	Yes or No	Question 1 Comment
		Key Concepts section, "The proposed standard deals exclusively with after-the-fact reporting." We feel that training, even if it is called drills or exercises is not necessary for an after-the-fact report. *The "drill or exercise" language has been deleted. Requirement R4 related to an annual test of the communication portion of Requirement 1. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *The testing requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
Liberty Electric Power	No	Training should be left in the standard as an option, along with an actual event, drill or exercise, to demonstrate that operating personnel have knowledge of the procedure. *The "drill or exercise" language has been deleted. Requirement R4 related*

Organization	Yes or No	Question 1 Comment
		to an annual test of the communication portion of Requirement 1. This has been revised to: *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *This language does not preclude the verification of contact information taking place during a training event.*
Response: Thank you for your comment. Please see response above.		
SERC OC Standards Review Group	No	We agree with removing the training requirement of R4; however we believe that drills and exercises are also training and R4 should be removed in its entirety because drills and exercises on an after the fact process do not enhance reliability. *The "drill or exercise" language has been removed. Requirement R4 related to an annual test of the communication portion of Requirement 1 This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include*

Organization	Yes or No	Question 1 Comment
		verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. *The testing requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
ACES Power Marketing Standards Collaborators/Great River Energy	No	We understand and agree there should be verification of the information required for such reporting (contact information, process flow charts, etc). But we still believe improvements can be made to the draft standard, in particular to requirement R4. The use of the words "or through a drill or exercise" still implies that training is required if no actual event has occurred. When you conduct a fire "drill" you are training your employees on evacuation routes and who they need to report to. Not only are you verifying your process but you are training your employees as well. It is imperative that the information in the Event Reporting process is correct but we don't agree that performing a drill on the process is necessary. We recommend modifying the requirement to focus on verifying the information needed for appropriate communications on an event. And we agree this should take place at least annually. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. This has*

Organization	Yes or No	Question 1 Comment
		been revised to: *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *This language does not preclude the verification of contact information taking place during a training event.*
Response: Thank you for your comment. Please see response above.		
Ingleside Cogeneration LP	Yes	: Yes. Ingleside Cogeneration LP agrees that training on an incident reporting operations plan should be at the option of the entity. However, we recommend that a statement be included in the "Guideline and Technical Basis" section that encourages drills and exercises be coincident with those conducted for Emergency Operations. Since front-line operators must send out the initial alert that a reportable condition exists, such exercises may help determine how to manage their reporting obligations during the early stages of the troubleshooting process. This is especially true where a notification must be made within an hour of discovery - a very short time period. *The "drill or exercise" language has been removed. Requirement R4 related to an annual test of the communication portion of Requirement 1. This has*

Organization	Yes or No	Question 1 Comment
		been revised to: *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* *This language does not preclude the verification of contact information taking place during a training event.*
Response: Thank you for your comment. Please see response above.		
American Public Power Association	Yes	APPA agrees that removal of the training requirement was an appropriate revision to limit the burden on small registered entities. However, APPA requests clarification from the SDT on the current draft of R4. If no event occurs during the calendar year, a drill or exercise of the Operating Plan communication process is required. APPA believes that if this drill or exercise is required, then it should be a table top verification of the internal communication process such as verification of phone numbers and stepping through a Registered Entity specific scenario. This should not be a full drill with requirements to contact outside entities such as law enforcement, NERC, the RC or other entities playing out a drill scenario. This full drill would be a major burden for small entities. *The "drill or exercise" language has been removed. Requirement R4 related to an annual test of the communication portion of Requirement 1. This has*

Organization	Yes or No	Question 1 Comment
		been revised to: *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.*
Response: Thank you for your comment. Please see response above.		
FirstEnergy	Yes	FirstEnergy supports this removal and thanks the drafting team.
Response: Thank you for your comment. Please see response above.		
Compliance & Responsbility Office	Yes	See comments in response to Question 4.
Response: Thank you for your comment. See response to Question 4.		
NV Energy	Yes	Thank you for responding to the stakeholder comments on this issue.
Response: Thank you for your comment.		
Constellation Energy on behalf of Baltimore Gas & Electric, Constellation Power Generation, Constellation Energy Commodities	Yes	Yes, we support removal of the training requirement.

Organization	Yes or No	Question 1 Comment
Group, Constellation Control and Dispatch, Constellation NewEnergy and Constellation Energy Nuclear Group.		
Response: Thank you for your comment.		
Pacific Northwest Small Public Power Utility Comment Group	Yes	
Southwest Power Pool Regional Entity	Yes	
BC Hydro	Yes	
ZGlobal on behalf of City of Ukiah, Alameda Municipal Power, Salmen River Electric, City of Lodi	Yes	
MRO NSRF	Yes	
Western Electricity Coordinating Council	Yes	
Imperial Irrigation District	Yes	
Santee Cooper	Yes	
Sacramento Municipal Utility District (SMUD)	Yes	

Organization	Yes or No	Question 1 Comment
SPP Standards Review Group	Yes	
Dominion	Yes	
PPL Electric Utilities and PPL Supply Organizations`	Yes	
Electric Compliance	Yes	
Kansas City Power & Light	Yes	
Luminant Power	Yes	
PacifiCorp	Yes	
Arizona Public Service Company	Yes	
CenterPoint Energy	Yes	
Salt River Project	Yes	
Westar Energy	Yes	
APX Power Markets (NCR-11034)	Yes	
Clallam County PUD No.1	Yes	
ITC	Yes	
Springfield Utility Board	Yes	

Organization	Yes or No	Question 1 Comment
Manitoba Hydro	Yes	
Intellibind	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Co. of NY, Inc.	Yes	
Orange and Rockland Utilities, Inc.	Yes	
Xcel Energy	Yes	
Duke Energy	Yes	
Colorado Springs Utilities	Yes	
Independent Electricity System Operator	Yes	
Exelon	Yes	
Public Utility District No. 1 of Snohomish County	Yes	
South Carolina Electric and Gas	Yes	
American Transmission Company, LLC	Yes	
Nebraska Public Power District	Yes	

Organization	Yes or No	Question 1 Comment
Seattle City Light	Yes	
PSEG	Yes	
MidAmerican Energy	Yes	
American Electric Power	Yes	
Georgia System Operations Corporation	Yes	
FEUS	Yes	
Lower Colorado River Authority	Yes	
Southwestern Power Administration	Yes	
Occidental Power Services, Inc. (OPSI)	Yes	
Northeast Utilities	Yes	
City of Austin dba Austin Energy	Yes	
Energy Northwest - Columbia	Yes	
Electric Reliability Council of Texas, Inc.	Yes	
Oncor Electric Delivery Company LLC	Yes	

Organization	Yes or No	Question 1 Comment
Progress Energy		
Los Angeles Department of Water and Power		
Texas Reliability Entity		
ReliabilityFirst		
NRECA		
Entergy Services		
Thompson Coburn LLP on behalf of Miss. Delta Energy Agency		

2. The DSR SDT includes two requirement regarding implementation of the Operating Plan specified in Requirement R1. The previous version of the standard had a requirement to implement the Operating plan as well as a requirement to report events. The two requirements R2 and R3 were written to delineate implementation of the Parts of R1. Do you agree with these revisions? If not, please explain in the comment area below.

R2. Each Responsible Entity shall implement the parts of its Operating Plan that meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts 1.4 and 1.5 as specified.

R3. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.

Summary Consideration: Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to:

"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."

Organization	Yes or No	Question 2 Comment
Ameren Services	Negative	(2) The new wording while well intentioned, effectively does not add clarity and leads to confusion. From our perspective, R1, which requires and Operating Plan, which is defined by the NERC glossary as: "A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan." *The DSR SDT thanks you for your comment. The SDT has made changes to the*

Organization	Yes or No	Question 2 Comment
		requirements highlighted in your comments. *FERC Order 693, Paragraph 466 includes provisions for periodic review and update of the Operating Plan: "466. The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."* (3) Is not a proper location for an after-the-fact reporting standard? In fact it could be argued that after-the-fact reports in and of themselves do not affect the reliability of the bulk electric system. *The DSR SDT does not agree with this comment. Reporting of an event will give the Electric Reliability Organization and your Reliability Coordinator the situational awareness of what has occurred on your part of the BES. Plus as described in your Operating Plan, you would have communicated the event as you saw fit. By broadcasting that an event has occurred you will increase the awareness of your company (as described in your Operating Plan) and increase the awareness of the Electric Reliability Organization and your Reliability Coordinator.* (4) But considering the proposed standard as written with the Operating Plan in requirement R1, and implementation of the Operating Plan in requirement R2 (except the actual reporting which is in R3) and then R3 which requires implementing the reporting section R1.3, it is not clear how these requirements can be kept separate in either implementation nor by the CEA. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2). The test and review requirement is*

Organization	Yes or No	Question 2 Comment
		included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures." (5) The second sentence in the second paragraph of "Rationale for R1" states:"The main issue is to make sure an entity can a) identify when an event has occurred and b) be able to gather enough information to complete the report." This is crucial for a Standard like this that is intended to mandate actions for events that are frequently totally unexpected and beyond normal planning criteria. This language needs to be added to Attachment 1 by the DSR SDT as explained in the rest of our comments. *The DSR SDT has updated the Rationale for Part 1.2 (previous Part 1.3) to read as: "Part 1.2 could include a process flowchart, identification of internal and external personnel or entities to be notified, or a list of personnel by name and their associated contact information." Whereas Part 1.2 now states:* *"1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."*
Response: Thank you for your comment. Please see response above.		
Old Dominion Electric Coop.	Negative	I disagree with two things in the presently drafted standard. First, I do not feel a separate requirement to implement the plan is necessary (R2), *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of*

Organization	Yes or No	Question 2 Comment
		Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read: *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* and I do not think that verification of the communications process should require a minimum of a drill or exercise. This is verified now under th current standard CIP-001 through verifice contact with the appropriate authorities and this should be enough to verify that the communications for the plan is in place. *The "drill or exercise" language has been removed. Requirement R4 related to an annual test of the communication portion of Requirement 1. This has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.*
Response: Thank you for your comment. Please see response above.		
ACES Power Marketing, Hoosier Energy Rural Electric Cooperative, Inc., Sunflower Electric Power Corporation,	Negative	Requirement R2 requires Responsible Entities to implement the various sub-requirements in R1. We believe it is unnecessary to state that an entity must implement their Operating Plan in a separate requirement. Having a separate requirement seems redundant. If the processes in the Operating Plan are not

Organization	Yes or No	Question 2 Comment
Great River Energy/ ACES Power Marketing Standards Collaborators/ Great River Energy		implemented, the entity is non-compliant with the standard. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* There doesn't need to be an extra requirement saying entities need to implement their Operating Plan. *The test and review requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
Hydro One Networks, Inc.	Negative	Requirement R2 seems to not be necessary. Who would have a plan and not implement it? This may also introduce double jeopardy issues should some entity not have a plan as required in R1. They would be unable to implement something they did not have so automatically non-compliant with R1 and R2. o Requirements R2 and R3 seem to be redundant. Isn't implementing the Operating Plan the same as reporting events in accordance with its Operating Plan? *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of*

Organization	Yes or No	Question 2 Comment
		Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read: *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* The standard mentions collecting information for Attachment 2, but the standard does not state what to do with Attachment 2. Is it merely a record for demonstrating compliance with R3? *The DSR SDT has updated Requirement R2 to read: "Each Responsible Entity must report and communicate events according to its Operating Plan based on the information in Attachment 1."* *The DSR SDT has also added the following statement to Attachment 1 for 1 hour reporting time frame and 24 hour reporting time frame, respectfully:* *"One Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the event"* *And* *"Twenty-four Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within twenty-four hour of recognition of the event."*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 2 Comment
Beaches Energy Services, City of Green Cove Springs	Negative	Requirements R2 and R3 are to implement the Operating Plan. Hence, R3 should be a bullet under R2 and not a separate requirement. In addition, for R2, the phrase "actual event" is ambiguous and should mean: "actual event that meets the criteria of Attachment 1" I suggest the following wording to R2 (which will result in eliminating R3) "Each Responsible Entity shall implement its Operating Plan: o For actual events meeting the threshold criteria of Attachment 1, in accordance with Requirement R1 parts 1.1, 1.2 and 1.3 *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* o For review and updating of the Operating Plan, in accordance with Requirement R1 parts 1.4 and 1.5" Note that I believe that if the SDT decides to not combine R2 and R3, then we disagree with the distinction between the two requirements. *Requirements R2 and R3 have been combined. Requirement 1, Part 1.4 was removed.* The division of implementing R1 through R2 and R3 as presented is "implementing" vs. "reporting". We believe that the correct division should rather be "implementation" of the plan (which includes reporting) vs. revisions to the plan. *The DSR SDT has updated Requirement R2 to read as: "R2. Each Responsible Entity shall implement the Operating Plan that meets Requirement R1 for events listed in Attachment 1."* *FERC Order 693 section 617 states "…the Commission directs the ERO to develop a*

Organization	Yes or No	Question 2 Comment
		modification to EOP-004-1 through the reliability Standards development process that includes any Requirement necessary for users, owners, and operators of the Bulk-Power System to provide data…". In order for entities to provide data they are required to implement their Operating Plan.
Response: Thank you for your comment. Please see response above.		
Ameren	No	(1) The new wording while well intentioned, effectively does not add clarity and leads to confusion. From our perspective, R1, which requires and Operating Plan, which is defined by the NERC glossary as: "A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan." *The DSR SDT has maintained Requirement 1 with the wording of "Operating Plan" which gives entities the flexibility of containing an Operating Process or Operating Procedure, as stated as "An Operating Plan may contain Operating Procedures and Operating Processes. Please note the use of "may contain" in the NERC approved definition.* *Requirement 1 now reads as"* *Each Responsible Entity shall have an Operating Plan that includes:* *1.1. A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the*

Organization	Yes or No	Question 2 Comment
		Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies. (2) Is not a proper location for an after-the-fact reporting standard? In fact it could be argued that after-the-fact reports in and of themselves do not affect the reliability of the bulk electric system. *The DSR SDT does not agree with this comment. Reporting of an event will give the Electric Reliability Organization and your Reliability Coordinator the situational awareness of what has occurred on your part of the BES. Plus as described in your Operating Plan, you would have communicated the event as you saw fit. By broadcasting that an event has occurred you will increase the awareness of your company (as described in your Operating Plan) and increase the awareness of the Electric Reliability Organization and your Reliability Coordinator.* (3) But considering the proposed standard as written with the Operating Plan in requirement R1, and implementation of the Operating Plan in requirement R2 (except the actual reporting which is in R3) and then R3 which requires implementing the reporting section R1.3, it is not clear how these requirements can be kept separate in either implementation nor by the CEA. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2).* *The test and review requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting*

Organization	Yes or No	Question 2 Comment
		procedures." (4) The second sentence in the second paragraph of "Rationale for R1" states: "The main issue is to make sure an entity can a) identify when an event has occurred and b) be able to gather enough information to complete the report." This is crucial for a Standard like this that is intended to mandate actions for events that are frequently totally unexpected and beyond normal planning criteria. This language needs to be added to Attachment 1 by the DSR SDT as explained in the rest of our comments *The DSR SDT has updated the Rationale for Part 1.2 (previous Part 1.3) to read as: "Part 1.2 could include a process flowchart, identification of internal and external personnel or entities to be notified, or a list of personnel by name and their associated contact information." Whereas Part 1.2 now states:* *"1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."*
Response: Thank you for your comment. Please see response above.		
American Electric Power	No	AEP prefers to avoid requirements that are purely administrative in nature. Requirements should be clear in their actions of supporting of the BES. For example, we would prefer requirements which state what is to be expected, and allowing the entities to develop their programs, processes, and procedures accordingly. It has been our understanding that industry, and perhaps NERC as well, seeks to reduce the amount to administrative (i.e. document-based) requirements. We are confident

Organization	Yes or No	Question 2 Comment
		that the appropriate documentation and administrative elements would occur as a natural course of implementing and adhering to action-based requirements. In light of this perspective, we believe that that R1 and R2 is not necessary, and that R3 would be sufficient by itself. Our comments above notwithstanding, AEP strongly encourages the SDT to consider that R2 and R3, if kept, be merged into a single requirement as a violation of R2 would also be a violation of R3. Two violations would then occur for what is essentially only a single incident. Rather than having both R2 and R3, might R3 be sufficient on its own? R2 is simply a means to an end of achieving R3. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2).* . *The test and review requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."* If there is a need to explicitly reference implementation, that could be addressed as part of R1. For example, R1 could state "Each Responsible Entity shall implement an Operating Plan that includes..."R1 seems disjointed, as subparts 1.4 and 1.5 (updating and reviewing the Operating Plan) do not align well with subparts 1.1 through 1.3 which are process related. If 1.4 and 1.5 are indeed needed, we recommend that they be a part of their own requirement(s). Furthermore, the action of these requirements should be changed from emphasizing provision(s) of a process to demonstrating the underlying activity.

Organization	Yes or No	Question 2 Comment
		The DSR SDT has maintained Requirement 1 with the wording of "Operating Plan" which gives entities the flexibility of containing an Operating Process or Operating Procedure, as stated as "An Operating Plan may contain Operating Procedures and Operating Processes. Please note the use of "may contain" in the NERC approved definition. *Requirement 1 now reads as "Each Responsible Entity shall have an Operating Plan that includes:* *1.1. A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.* 1.4 AEP is concerned by the vagueness of requiring provision(s) for updating the Operating Plan for "changes", as such changes could occur frequently and unpredictably. *Part 1.4 was removed from the standard.* *It is the sole responsibility of the Applicable Entity to determine when an annual review of the Operating Plan is required. The Operating Plan has the minimum requirement for an annual review. You may review your Operating Plan as often as you see appropriate.*
Response: Thank you for your comment. Please see response above.		
Occidental Power Services,	No	Attachment 1 and R3 require event reports to be sent to the ERO and the entity's RC and to others "as appropriate." Although this gives the entity some discretion, it

Organization	Yes or No	Question 2 Comment
Inc. (OPSI)		might also create some "Monday morning quarterbacking" situations. This is especially true for the one hour reporting situations as personnel that would be responding to these events are the same ones needed to report the event. OPSI suggests that the SDT reconsider and clarify reporting obligations with the objective of sending initial reports to the minimum number of entities on a need-to-know basis. *Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to communicate events to as stated in the entity's Operating Plan.* *The DSR SDT also received many comments regarding the various events of Attachment 1. Many commenters questioned the reliability benefit of reporting events to the ERO and their Reliability Coordinator within 1 hour. Most of the events with a one hour reporting requirement were revised to 24 hours based on stakeholder comments as well as those types of events are currently required to be reported within 24 hours in the existing mandatory and enforceable standards. The only remaining type of event that is to be reported within one hour is "A reportable Cyber Security Incident" as it required by CIP-008.* *FERC Order 706, paragraph 673 states: "…each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event within one hour of the event…"*
Response: Thank you for your comment. Please see response above.		
Ingleside Cogeneration LP	No	Attachment 1 and requirement R3 are written in a manner which would seem to indicate that internal personnel and law enforcement personnel would have to be copied on the submitted form - either Attachment 2 or OE-417. We believe the intent is to submit such forms to the appropriate recipients only (e.g.; the ERO and

Organization	Yes or No	Question 2 Comment
		the DOE). The requirement should be re-written to clarify that this is the case. *The DSR SDT thanks you for your comment. Requirement 1 has been updated and now reads as"* *Each Responsible Entity shall have an Operating Plan that includes:* *1.1. A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.* *The Applicable Entity's Operating Plan is to contain the process for reporting events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and for communicating to others as defined in the Responsible Entity's Operating Plan. All events in Attachment 1 are required to be reported to the Electric Reliability Organization and the Responsible Entity's Reliability Coordinator. The Operating Plan may include: internal company personnel, your Regional Entity, law enforcement, and governmental or provisional agencies, as you identify within your Operating Plan. This gives you the flexibility to tailor your Operating Plan to fit your company's needs and wants.*
Response: Thank you for your comment. Please see response above.		
Florida Municipal Power Agency	No	Both requirements are to implement the Operating Plan. Hence, R3 should be a bullet under R2 and not a separate requirement. In addition, for R2, the phrase "actual event" is ambiguous and should mean: "actual event that meets the criteria of Attachment 1"We suggest the following wording to R2 (which will result in eliminating R3)"Each Responsible Entity shall implement its Operating Plan: o For actual events meeting the threshold criteria of Attachment 1 in accordance with

Organization	Yes or No	Question 2 Comment
		Requirement R1 parts 1.1, 1.2 and 1.3 *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* o For review and updating of the Operating Plan in accordance with Requirement R1 parts 1.4 and 1.5"Note that we believe that if the SDT decides to not combine R2 and R3, then we disagree with the distinction between the two requirements. *The test and review requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."* The division of implementing R1 through R2 and R3 as presented is "implementing" vs. "reporting". We believe that the correct division should rather be "implementation" of the plan (which includes reporting) vs. revisions to the plan. *The DSR SDT has updated Requirement R2 to read as: "R2. Each Responsible Entity shall implement the Operating Plan that meets Requirement R1 for events listed in Attachment 1."* *FERC Order 693 section 617 states "…the Commission directs the ERO to develop a modification to EOP-001-1 through the reliability Standards development process that includes any Requirement necessary for users, owners, and operators of the*

Organization	Yes or No	Question 2 Comment
		Bulk-Power System to provide data…". In order for entities to provide data they are required to implement their Operating Plan.
Response: Thank you for your comment. Please see response above.		
Indiana Municipal Power Agency	No	Both requirements seem to be implementing the Operating Plan which means R3 should be a bullet under R2 and not a separate requirement. IMPA supports making R2 and R3 one requirement and eliminating the current R3 requirement. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* In addition, R2 needs to be clarified when addressing an actual event. IMPA recommends saying "an actual event that meets the criteria of Attachment 1." *The DSR SDT has implemented your suggestion.* *Requirement R2now reads as: "Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1.".*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 2 Comment
CenterPoint Energy	No	CenterPoint Energy believes the current R2 is unnecessary and duplicative. Upon reporting events as required by R3, entities will be implementing the relevant parts of their Operating Plan that address R1.1 and R1.2. This duplication is clear when reading M2 and M3. Acceptable evidence is an event report. R2 should be modified to remove this duplicative requirement. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."*
Response: Thank you for your comment. Please see response above.		
Orange and Rockland Utilities, Inc./Consolidated Edison Co. Of NY, Inc.	No	Comments: o R1.3 should be revised as follows: A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as determined by the responsible entity: ["appropriate: - deleted] [otherwise it is not clear who determines what communication level is appropriate] o R1.4 should be revised as follows: Provision(s) for updating the Operating Plan following ["within 90 calendar days of any" - deleted] change in assets or personnel (if the Operating Plan specifies personnel or assets) , ["other circumstances" - deleted] that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3. o R1.5 should be deleted. Responsible Entities can determine the frequency of Operating Plan updates. Requirement 1.4 requires updating the Operating Plan within 90 calendar days for changes in "assets, personnel.... or incorporating lessons

Organization	Yes or No	Question 2 Comment
		learned". *Requirement 1 has been updated and now reads as"* *Each Responsible Entity shall have an Operating Plan that includes:* *1.1. A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.* This requirement eliminates the need for Requirement 1.5 requiring a review of the Operating Plan on an annual basis. *The test and review requirement is included in the Standard to meet the intent of FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
ISO New England	No	In accordance with the results-based standards concept, all that is required, for the "what" is that company X reported on event Y in accordance with the reporting requirements in attachment Z of the draft standard. Therefore, we proposed the only requirement that is necessary is R3, which should be re-written to read..."Each

Organization	Yes or No	Question 2 Comment
		Responsible Entity shall report to address the events listed in Attachment 1." *Requirement 1 and 2 is the basis of the "what" you have described in your comment. Whereas Attachment 1 contains a minimum list of events that apply to Requirement 1, this is why Requirement R2 was rewritten as: "R2. Each Responsible Entity shall implement the Operating Plan that meets Requirement R1 for events listed in Attachment 1."* *The DSR SDT was directed to incorporate certain items such as; FERC Order 693, paragraph 466: "The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."*
Response: Thank you for your comment. Please see response above.		
SERC OC Standards Review Group	No	It is confusing why R3 is not considered part of R2, which deals with implementation of the Operating Plan and it appears that R3 could be interpreted as double jeopardy. We suggest deleting R3. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement the Operating Plan that meets Requirement R1 for events listed in Attachment 1."*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 2 Comment
Oncor Electric Delivery Company LLC	No	NERC's Event Analysis Program tends to parallel many of the reporting requirements as outlined in EOP-004 Version 2. Oncor recommends that NERC considers ways of streamlining the reporting process by either incorporating the Event Analysis obligations into EOP-004-2 or reducing the scope of the Event Analysis program as currently designed to consist only of "exception" reporting. *The Event Analysis Program may use a reported event as a basis to analyze an event. The reporting required in EOP-004-2 provides the input to the Events Analysis Process. The processes of the Event Analysis Program fall outside the scope of this project, but the DSR SDT has collaborated with them of events contained in Attachment 1.*
Response: Thank you for your comment. Please see response above.		
NV Energy	No	On my read of the Standard, R2 and R3 appear to be duplicative, and I can't really distinguish the difference between the two. The action required appears to be the same for both requirements. Even the Measures for these two sound similar. It is not clear to me what it means to "implement" other than to have evidence of the existence and understanding of roles and responsibilities under the "Operating Plan." I suggest elimination of R2 and inclusion of a line item in Measure 1 calling for evidence of the existence of an "Operating Plan" including all the required elements in R1. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2 Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."*

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comment. Please see response above.		
Northeast Power Coordinating Council	No	R1.3 should be revised as follows: A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as determined by the responsible entity:...Without this change it is not clear who determines what communication level is appropriate. *Requirement 1, Part 1.3 (now Part 1.2) was updated per comments received.* *1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.* R1.4 should be revised as follows: Provision(s) for updating the Operating Plan following any change in assets or personnel (if the Operating Plan specifies personnel or assets), that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3. R1.5 should be deleted. Responsible Entities can determine the frequency of Operating Plan updates. Requirement 1.4 requires updating the Operating Plan within 90 calendar days for changes in "assets, personnel.... or incorporating lessons learned", (or our preceding proposed revision). *Requirement 1, part 1.4 has been deleted and Requirement R2 has been updated to read as: "R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* This requirement eliminates the need for Requirement 1.5 requiring a review of the Operating Plan on an annual basis.

Organization	Yes or No	Question 2 Comment
		The only true requirement that is results-based, not administrative and is actually required to support the Purpose of the Standard is R3. *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:* *"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."*
Response: Thank you for your comment. Please see response above.		
Illinois Municipal Electric Agency	No	R2 is not necessary, and should be removed. Subrequirement R1.4 is also not necessary and should be removed. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."*
Response: Thank you for your comment. Please see response above.		
Kansas City Power & Light	No	Requirement R1.1 is confusing regarding the "process for identifying events listed in Attachment 1". Considering Attachment 1, the Events Table, already identifies the events required for reporting, please clearly describe in the requirement what the "process" referred to in requirement R1.1 represents. *The DSR SDT has reviewed FERC Order 693 and paragraph 471 states: "…(2) specify*

Organization	Yes or No	Question 2 Comment
		baseline requirement regarding what issues should be addressed in the procedures for recognizing sabotage events and making personnel aware of such events…" *The DSR SDT has written Requirement 1, Part 1.1 to read as: "A process for recognizing each of the events listed in EOP-004 Attachment 1". An Applicable Entity may rely on SCADA alarms as a process for recognizing an event or being made aware of an event through a scheduled Facility check. The DSR SDT has not been overly prescriptive on part 1.1 but has allowed each Applicable Entity to determine their own process for recognizing events listed in Attachment 1.*
Response: Thank you for your comment. Please see response above.		
Luminant Power	No	Requirements R1, R2, and R4 are burdensome administrative requirements and are contradictory to the NERC stated Standards Development goals of reducing administrative requirements by moving to performance requirements. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."* *Requirement R1, Part 1.3 (now Part 1.2) was revised to indicate that the Responsible Entity is to define its process for reporting and with whom to report events. Part 1.2 now reads:* *"1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004*

Organization	Yes or No	Question 2 Comment
		Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies." There is only one Requirement needed in this standard: "The Responsible Entity shall report events in accordance with Attachment 1." Attachment 1 should describe how events should be reported by what Entity to which party within a defined timeframe. If this requirement is met, all the other proposed requirements have no benefit to the reliability of the Bulk Electric System. Per the NERC Standard Development guidelines, only items that provide a reliability benefit should be included in a standard. *The DSR SDT has updated Attachment 1 to a minimum threshold for Applicable Entities to report contained events. Requirement R2 has been updated to reflect that Applicable Entities shall implement their Operating Plan per Requirement 1 for events listed in Attachment 1. Requirement R2 reads as: "R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."*
Response: Thank you for your comment. Please see response above.		
Xcel Energy	No	Suggest modifying R3 to indicate this is related to R 1.3.Each Responsible Entity shall report events to entities specified in R1.3 and as identified as appropriate in its Operating Plan. *Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3*

Organization	Yes or No	Question 2 Comment
		(now R2) *R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."*
Response: Thank you for your comment. Please see response above.		
Colorado Springs Utilities	No	The act of implementing the plan needs to include reporting events per R1, sub-requirement 1.3. R2 should simply state something like, "Each Responsible Entity shall implement the Operating Plan that meets the requirements of R1, as applicable, for an actual event or as specified." Suggest eliminating R3 which, seems to create double jeopardy effect. *Requirement R2 was updated to reflect comments received to read as: "R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1." R3 was deleted.*
Response: Thank you for your comment. Please see response above.		
Intellibind	No	The language proposed is not clear and will continue to add confusion to entities who are trying to meet these requirements. It is not clear that the drafting team can put itself in the position of how the auditors will interpret and implement compliance against thithe R2 requirement. Requirements should be written to stand alone, not reference other requirements (or parts of the requirments. If the R1 parts 1.1, 1.2, 1.4 and 1.5 are so significant for this requirement, then they should be rewritten in R2. *Most stakeholders believed that Requirements R2 and R3 were redundant and having*

Organization	Yes or No	Question 2 Comment
		both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read: *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."*
Response: Thank you for your comment. Please see response above.		
Southern Company	No	These requirements as drafted in this revised standard potentially create a situation where an entity could be deemed non-compliant for both R2 and R3. For example, if a Responsible Entity included a reporting obligation in its Operating Plan, and failed to report an event, the Responsible Entity could be deemed non-compliant for R2 for not "implementing" its plan and for R3 for not reporting the event to the appropriate entities. A potential solution to address this would be to add Requirement 1, Part 1.3 to Requirement 2 and remove Requirement 3 in its entirety. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."* We also request clarification on Measure M3. Which records should have "dated and time-stamped transmittal records to show that the event was reported"? Some of the communication is handled via face-to-face conversation or through telephone

Organization	Yes or No	Question 2 Comment
		conversation. *Measurement 3 has been deleted since Requirement 3 has been deleted. The new Measurement 2 allows for "…or other documentation". This may be in any form that the Applicable Entity wishes to maintain that they met Requirement 2. The Electric Reliability Organization does allow "Attestations" along with voice recordings as proof of compliance.*
Response: Thank you for your comment. Please see response above.		
Independent Electricity System Operator	No	We agree with the revision to R2 and R3, but assess that a requirement to enforce implementation of Part 1.3 in Requirement R1 is missing. Part 1.3 in Requirement R1 stipulates that:1.3. A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate: o Internal company personnel o The Responsible Entity's Regional Entity o Law enforcement o Governmental or provincial agenciesThe implementation of Part 1.3 is not enforced by R2 or R3 or any other Requirements in the standard. Suggest to add another requirement or expand Requirement R4 (and M4) to require the implementation of this Part in addition to verifying the process. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."* *Requirement 1 has been updated and now reads as"*

Organization	Yes or No	Question 2 Comment
		Each Responsible Entity shall have an Operating Plan that includes: *1.1 A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.*
Response: Thank you for your comment. Please see response above.		
Independent Electricity System Operator	Affirmative	The IESO believes that a requirement to enforce implementation of Part 1.3 in Requirement R1 is missing. Part 1.3 in Requirement R1 stipulates that: 1.3. A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate: o Internal company personnel o The Responsible Entity's Regional Entity o Law enforcement o Governmental or provincial agencies The implementation of Part 1.3 is not enforced by R2 or R3 or any other Requirements in the standard. The IESO suggests that another requirement be added or Requirement R4 (and M4) be expanded to require the implementation of this Part in addition to verifying the process. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the*

Organization	Yes or No	Question 2 Comment
		timeframe specified in EOP-004 Attachment 1." *Requirement 1 has been updated and now reads as"* *Each Responsible Entity shall have an Operating Plan that includes:* *1.1 A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.*
Response: Thank you for your comment. Please see response above.		
Bonneville Power Administration	Yes	BPA believes the measures for R2 are unclear since they are similar to R3's reporting measures.
Response: Thank you for your comment. The SDT has revised the standard to have a single implementation requirement with a single associated measure.		
Compliance & Responsbility Office	Yes	See comments in response to Question 4.
Response: Thank you for your comment. See response to Question 4.		
Constellation Energy on behalf of Baltimore Gas & Electric, Constellation Power Generation, Constellation Energy Commodities Group,	Yes	While we support the delineation of the different activities associated with implementation and reporting, further clarification would be helpful. R1. 1.3: As currently written, it is somewhat confusing, in particular the use of the qualifier "as appropriate". *The DSR SDT has updated Requirement 1, Part 1.2 to read as: "A process for*

Organization	Yes or No	Question 2 Comment
Constellation Control and Dispatch, Constellation NewEnergy and Constellation Energy Nuclear Group.		*communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."* In addition, the use of the word "communicating" to capture both reporting to reliability authorities and notifying others may leave the requirement open to question. Below is a proposed revision: 1.3 A process for reporting events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and for communicating to others as defined in the Responsible Entity's Operating Plan, such as: o Internal company personnel o The Responsible Entity's Regional Entity o Law Enforcement o Government or provincial agenciesR1, 1.4: the last phrase of the requirements seems to be leftover from an earlier version. The requirement should end after the word "Plan".R1, 1.5: "Process" should not be capitalized. While we understand the intent of the draft language and appreciate the effort to streamline the requirements, we propose an adjusted delineation below that we feel tracks more cleanly to the structure of a compliance program. Proposed revised language:R2. Each Responsible Entity shall implement its Operating Plan to meet Requirement R1, parts 1.1 and 1.2 for an actual event(s).M2. Responsible Entities shall provide evidence that it implemented it Operating Plan to meet Requirement R1, Parts 1.1 and 1.2 for an actual event. *The DSR SDT has updated Requirement 1, Part 1.2 to read as: "A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator;*

Organization	Yes or No	Question 2 Comment
		law enforcement governmental or provincial agencies." *The Applicable Entity's Operating Plan is to contain the process for reporting events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and for communicating to others as defined in the Responsible Entity's Operating Plan. All events in Attachment 1 are required to be reported to the Electric Reliability Organization and the Responsible Entity's Reliability Coordinator. The Operating Plan may include: internal company personnel, your Regional Entity, law enforcement, and governmental or provisional agencies, as you identify within your Operating Plan. This gives you the flexibility to tailor your Operating Plan to fit your company's needs and wants.* *DSR SDT has revised R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1.* *DSR SDT has revised M2. "Each Responsible Entity will have, for each event experienced, a dated copy of the completed EOP-004 Attachment 2 form or DOE form OE-417 report submitted for that event; and dated and time-stamped transmittal records to show that the event was reported supplemented by operator logs or other operating documentation. Other forms of evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other operating documentation for situations where filing a written report was not possible.* Evidence may include, but is not limited to, an submitted event report form (Attachment 2) or a submitted OE-417 report, operator logs, or voice recording.R3. Each Responsible Entity shall implement its Operating Plan to meet Requirement R1, parts 1.4 and 1.5.M3. Responsible Entities shall provide evidence that it implemented it Operating Plan to meet Requirement R1, Parts 1.4 and 1.5. Evidence may include, but is not limited to, dated documentation of review and update of the Operating Plan.

Organization	Yes or No	Question 2 Comment
		R4. Each Responsible Entity shall verify (through implementation for an actual event, or through a drill, exercise or table top exercise) the communication process in its Operating Plan, created pursuant to Requirement 1, Part 1.3, at least annually (once per calendar year), with no more than 15 calendar months between verification. M4. The Responsible Entity shall provide evidence that it verified the communication process in its Operating Plan for events created pursuant to Requirement R1, Part 1.3. Either implementation of the communication process as documented in its Operating Plan for an actual event or documented evidence of a drill, exercise, or table top exercise may be used as evidence to meet this requirement. The time period between verification shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or dated documentation of a verification. *Requirement 4 (now R3) was revised as:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]* *M3. Each Responsible Entity will have dated and time-stamped records to show that the annual test of Part 1.2 was conducted. Such evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other communication documentation. The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. (R3)*
Response: Thank you for your comment. Please see response above.		
Exelon	Yes	Why is the reference to R1.3 missing from EOP-004-2 Requirement R2?

Organization	Yes or No	Question 2 Comment
		R1.3 was associated with implementation in R3 which was removed from the standard. DSR SDT has revised R2 to read as: "Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."
Response: Thank you for your comment. Please see response above.		
Pacific Northwest Small Public Power Utility Comment Group	Yes	
Southwest Power Pool Regional Entity	Yes	
BC Hydro	Yes	
ZGlobal on behalf of City of Ukiah, Alameda Municipal Power, Salmen River Electric, City of Lodi	Yes	
MRO NSRF	Yes	
Western Electricity Coordinating Council	Yes	
Imperial Irrigation District	Yes	
Santee Cooper	Yes	

Organization	Yes or No	Question 2 Comment
Sacramento Municipal Utility District (SMUD)	Yes	
SPP Standards Review Group	Yes	
Dominion	Yes	
FirstEnergy	Yes	
PPL Electric Utilities and PPL Supply Organizations`	Yes	
Electric Compliance	Yes	
PacifiCorp	Yes	
Arizona Public Service Company	Yes	
Salt River Project	Yes	
Westar Energy	Yes	
APX Power Markets (NCR-11034)	Yes	
Clallam County PUD No.1	Yes	
ITC	Yes	
Springfield Utility Board	Yes	

Organization	Yes or No	Question 2 Comment
Manitoba Hydro	Yes	
Duke Energy	Yes	
Liberty Electric Power	Yes	
Public Utility District No. 1 of Snohomish County	Yes	
South Carolina Electric and Gas	Yes	
American Transmission Company, LLC	Yes	
Nebraska Public Power District	Yes	
Seattle City Light	Yes	
PSEG	Yes	
MidAmerican Energy	Yes	
Georgia System Operations Corporation	Yes	
FEUS	Yes	
Lower Colorado River Authority	Yes	

Organization	Yes or No	Question 2 Comment
American Public Power Association	Yes	
Northeast Utilities	Yes	
City of Austin dba Austin Energy	Yes	
Energy Northwest - Columbia	Yes	
Electric Reliability Council of Texas, Inc.	Yes	
		R2 and R3 appear redundant.
Progress Energy		
Los Angeles Department of Water and Power		
Texas Reliability Entity		
ReliabilityFirst		
NRECA		
Entergy Services		
Thompson Coburn LLP on behalf of Miss. Delta Energy Agency		

Organization	Yes or No	Question 2 Comment
Southwestern Power Administration		

3. The DSR SDT revised reporting times for many events listed in Attachment 1 from one hour to 24 hours. Do you agree with these revisions? If not, please explain in the comment area below.

Summary Consideration: The DSR SDT appreciates the industry comments on the difficulty associated with reporting events that impact reliability. However, the SDT desires to point out that it is not the objective of this standard to provide an analysis of the event; but to provide the known facts of the events at the reporting threshold of onehour or 24hours depending upon the type of event. The SDT worked with the DOE and the NERC EAWG to develop reporting timelines consistent between the parties in an effort to promote consistency and uniformity.

The SDT has not established any requirement for a final or follow up report. The obligation is to report the facts known at the time. Once the report has been provided to the parties identified in the Operating Plan, no further action is required. All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:

> **"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."**

For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report, and is consistent with current in-force standard EOP-004-1.

Organization	Yes or No	Question 3 Comment
Ameren Services	Negative	(6)By our count there are still six of the nineteen events listed with a one hour reporting requirement and the rest are all within 24 hour after the occurrence (or recognition of the event). This in our opinion, is reporting in real-time, which is against one of the key concepts listed in the background section:"The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of

Organization	Yes or No	Question 3 Comment
		standards). The proposed standard deals exclusively with after-the-fact reporting." *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.* (7)We believe the earliest preliminary report required in this standard should at the close of the next business day. Operating Entities, such as the RC, BA, TOP, GOP, DP, and LSE should not be burdened with unnecessary after-the-fact reporting while they are addressing real-time operating conditions. Entities should have the ability to allow their support staff to perform this function during the next business day as needed. We acknowledge it would not be an undue burden to cc: NERC on other required governmental reports with shorter reporting timeframes, but NERC should not expand on this practice. *No preliminary report is required within the revised standard. Also, timelines have been revised (Please see response to item (6) above).* (8)We agree with the extension in reporting times for events that now have 24 hours of reporting time. As a GO there are still too many potential events that still require a 1 hour reporting time that is impractical, unrealistic and could lead to inappropriate escalation of normal failures. For example, the sudden loss of several control room display screens for a BES generator at 2 AM in the morning, with only 1 hour to report something, might be mistakenly interpreted as a cyber-attack. The reality is

Organization	Yes or No	Question 3 Comment
		most likely something far more mundane such as the unexpected failure of an instrument transformer, critical circuit board, etc. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.* (9) The "EOP-004 Attachment 1: Events Table" is quite lengthy and written in a manner that can be quite subjective in interpretation when determining if an event is reportable. We believe this table should be clear and unambiguous for consistent and repeatable application by both reliability entities and a CEA. The table should be divided into sections such as: 9a) Events that affect the BES that are either clearly sabotage or suspected sabotage after review by an entity's security department and local/state/federal law enforcement.(b) Events that pose a risk to the BES and that clearly reach a defined threshold, such as load loss, generation loss, public appeal, EEAs, etc. that entities are required to report by the end of the next business day.(c) Other events that may prove valuable for lessons learned, but are less definitive than required reporting events. These events should be reported voluntarily and not be subject to a CEA for non-reporting.(d)Events identified through other means outside of entity reporting, but due to their nature, could benefit the industry by an event report with lessons learned. Requests to report and perform analysis on these type of events should be vetted through a ERO/Functional Entity process to ensure resources provided to this effort have an effective reliability benefit.

Organization	Yes or No	Question 3 Comment
		The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows: • *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* • *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.* *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* (10)Any event reporting shall not in any manner replace or inhibit an Entity's responsibility to coordinate with other Reliability Entities (such as the RC, TOP, BA, GOP as appropriate) as required by other Standards, and good utility practice to operate the electric system in a safe and reliable manner. *The DSR SDT agrees and believes the revised reporting timelines support that concept.* (11) The 1 hour reporting maximum time limit for all GO events in Attachment 1 should be lengthened to something reasonable - at least 24 hours. Operators in our energy centers are well-trained and if they have good reason to suspect an event

Organization	Yes or No	Question 3 Comment
		that might have serious impact on the BES will contact the TOP quickly. However, constantly reporting events that turn out to have no serious BES impact and were only reported for fear of a violation or self-report will quickly result in a cry wolf syndrome and a great waste of resources and risk to the GO and the BES. The risk to the GO will be potential fines, and the risk to the BES will be ignoring events that truly have an impact of the BES. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.* (12)The 2nd and 3rd Events on Attachment 1 should be reworded so they do not use terms that may have been deleted from the NERC Glossary by the time FERC approves this Standard. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* (13) The terms "destruction" and "damage" are key to identifying reportable events. Neither has been defined in the Standard. The term destruction is usually defined as 100% unusable. However, the term damage can be anywhere from 1% to 99%

Organization	Yes or No	Question 3 Comment
		unusable and take anywhere from 5 minutes to 5 months to repair. How will we know what the SDT intended, or an auditor will expect, without additional information? *The 'Damage or Destruction' event category has been revised to say ' ...to a Facility', (a defined term) and thresholds have be modified to provide clarity.* *The DSR SDT used the defined term "Facility" to add clarity for several events listed in Attachment 1. A Facility is defined as:* *"A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"* *The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.* (14)We also do not understand why "destruction of BES equipment" (first item Attachment 1, first page) must be reported < 1 hour, but "system separation (islanding) > 100 MW" (Attachment 1, page 3) does not need to be reported for 24 hours. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the*

Organization	Yes or No	Question 3 Comment
		incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. (15)The first 2 Events in Attachment 1 list criteria Threshold for Reporting as "...operational error, equipment failure, external cause, or intentional or unintentional human action." The term "intentional or unintentional human action" appears to cover "operational error" so these terms appear redundant and create risk of misreporting. Can this be clarified? *The second event has been deleted and the language has been clarified in the 'Threshold for Reporting' column in the 'Damage or Destruction' event category. The updated Threshold for Reporting now reads as:* *"Damage or destruction of a Facility that:* • *Affects an IROL (per FAC-014)* *OR* • *Results in the need for actions to avoid an Adverse Reliability Impact* *OR* • *Results from intentional human action."* (16)The footnote of the first page of Attachment 1 includes the explanation "...ii) Significantly affects the reliability margin of the system..." However, the GO is prevented from seeing the system and has no idea what BES equipment can affect the reliability margin of the system. Can this be clarified by the SDT? *The footnote has been deleted and relevant information moved to the 'Threshold for Reporting column in the 'Damage or Destruction' event category.* (17) The use of the term "BES equipment" is problematic for a GO. NERC Team 2010-

Organization	Yes or No	Question 3 Comment
		17 (BES Definition) has told the industry its next work phase will include identify *The term "BES equipment" is no longer used. The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity.* *The DSR SDT used the defined term "Facility" to add clarity for several events listed in Attachment 1. A Facility is defined as:* *"A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"* *The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.*
Response: Thank you for your comment. Please see response above.		
Beaches Energy Services, City of Green Cove Springs	Negative	3. Att. 1, going from 1 to 24 hrs: The times don't seem aggressive enough for some of the Events related to generation capacity shortages, e.g., we would think public appeal, system wide voltage reduction and manual firm load shedding ought to be within an hour. These are indicators that the BES is "on the edge" and to help BES reliability, communication of this status is important to Interconnection-wide reliability. *This standard concerns after-the-fact reporting. It is assumed that Responsible Entities will make appropriate real-time notifications as per other applicable standards, operating agreements, and good utility practice. This standard does not preclude a Responsible Entity from reporting more quickly than required by Attachment 1.*

Organization	Yes or No	Question 3 Comment
		4. The Rules of Procedure language for data retention (first paragraph of the Evidence Retention section) should not be included in the standard, but instead referred to within the standard (e.g., "Refer to Rules of Procedure, Appendix 4C: Compliance Monitoring and Enforcement Program, Section 3.1.4.2 for more retention requirements") so that changes to the RoP do not necessitate changes to the standard. *The DSR SDT believes that although the evidence retention language is the same as the current RoP, it is not specifically linked, so changes to the RoP will not necessitate changes to the standard.* In R4, it might be worth clarifying that, in this case, implementation of the plan for an event that does not meet the criteria of Attachment 1 and going beyond the requirements R2 and R3 could be used as evidence. Consider adding a phrase as such to M4, or a descriptive footnote that in this case, "actual event" may not be limited to those in Attachment 1. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to read:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1. "* Comments to Attachment 1 table: On "Damage or destruction of Critical Asset" and "... Critical Cyber Asset", Version 5 of the CIP standards is moving away from the

Organization	Yes or No	Question 3 Comment
		binary critical/non-critical paradigm to a high/medium/low risk paradigm. Suggest adding description that if version 5 is approved by FERC, that "critical" would be replaced with "high or medium risk", or include changing this standard to the scope of the CIP SDT, or consider posting multiple versions of this standard depending on the outcome of CIP v5 in a similar fashion to how FAC-003 was posted as part of the GO/TO effort of Project 2010-07. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* On "forced intrusion", the phrase "at BES facility" is open to interpretation as "BES Facility" (e.g., controversy surrounding CAN-0016) which would exclude control centers and other critical/high/medium cyber system Physical Security Perimeters (PSPs). We suggest changing this to "BES Facility or the PSP or Defined Physical Boundary of critical/high/medium cyber assets". This change would cause a change to the applicability of this reportable event to coincide with CIP standard applicability. On "Risk to BES equipment", that phrase is open to too wide a range of interpretation; we suggest adding the word "imminent" in front of it, i.e., "Imminent risk to BES equipment". For instance, heavy thermal loading puts equipment at risk, but not imminent risk. Also, "non-environmental" used as the threshold criteria is ambiguous. For instance, the example in the footnote, if the BES equipment is near railroad tracks, then trains getting derailed can be interpreted as part of that BES equipment's "environment", defined in Webster's as "the circumstances, objects, or conditions by which one is surrounded". It seems that the SDT really means "non-weather related", or "Not risks due to Acts of Nature". *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen*

Organization	Yes or No	Question 3 Comment
		because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples. On "public appeal", in the threshold, the descriptor "each" should be deleted, e.g., if a single event causes an entity to be short of capacity, do you really want that entity reporting each time they issue an appeal via different types of media, e.g., radio, TV, etc., or for a repeat appeal every several minutes for the same event? *To clarify your point, the threshold has been changed to 'Public appeal or load reduction event'.* Should LSE be an applicable entity to "loss of firm load"? As proposed, the DP is but the LSE is not. In an RTO market, will a DP know what is firm and what is non-firm load? Suggest eliminating DP from the applicability of "system separation". The system separation we care about is separation of one part of the BES from another which would not involve a DP. *The DSR SDT believes the current applicability is correct and the threshold provides sufficient discrimination to drive the proper Applicable Entities to report.* On "Unplanned Control Center Evacuation", CIP v5 might add GOP to the applicability, another reason to add revision of EOP-004-2 to the scope of the CIP v5 drafting team, or in other ways coordinate this SDT with that SDT. Consider posting a couple of versions of the standard depending on the outcome of CIP v5 in a similar fashion to the multiple versions of FAC-003 posted with the GO/TO effort of Project 2010-07. *The DSR SDT believes the current applicability is correct. The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed*

Organization	Yes or No	Question 3 Comment
		from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds. Note that EOP-008-0 is only Applicable to Balancing Authorities, Transmission Operators and Reliability Coordinators, this is the basis for the "Entity with reporting Responsibilities" and reads as" "Each RC, BA, TOP that experiences the event".
Response: Thank you for your comment. Please see response above.		
Arkansas Electric Cooperative Corporation	Negative	AECC appreciates the efforts of the SDT to address our comments from the previous posting and feels the Standards have shown great improvement in the current posting. Our negative vote stems from concerns around the 1 hour reporting requirements for events having no size thresholds and ambiguity for external entity reporting in R1.3. Please refer to the comments submitted by the SPP Standards Review Group. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"…direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 3 Comment
PowerSouth Energy Cooperative	Negative	Attachment 1 needs to be eliminated. It is confusing to operators and doesn't enhance the reliability of the BES. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.*
Response: Thank you for your comment. Please see response above.		
Clark Public Utilities	Negative	Attachment 1 provides confusion not clarification. Just use the OE-417 reporting form for any and all events identified in that form for any one-hour or six-hour reporting. Utilities are required by law to provide the DOE notification and the SDT has just confused the situation by attempting (as it appears) to rename the one-hour reporting events. In some instances, Attachment 1 contradicts the DOE reporting. Public appeals for load reduction are required within 24 hours (according to the Events Table) but OE-417 requires such pubic appeals to be reported within one

Organization	Yes or No	Question 3 Comment
		hour. Clark recommends the Events Table show first the one hour reporting of OE-417, then the six hour reporting of OE-417, and finally any additional reporting that is desired but not reportable to DOE. This will help in not confusing seemingly related events. The table should indicate which form is to be used and should mandate Form OE-417 for all DOE reportable events and the Attachment 2: Event Reporting Form for all reportable events not subject to the DOE reporting requirements. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.* Clark questions whether the event labeled Forced Intrusion really needs to be reported in one hour. It can take several hours to determine if a forced entry actually occurred. Clark is also unsure if reporting forced intrusions at these facilities (if no other disturbance occurs) will provide any information useful in preventing system disturbances but believes this event should be changed to a 24 hour notification.

Organization	Yes or No	Question 3 Comment
		'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. The event labeled Detection of a reportable Cyber Security Incident should have the Entity with Reporting Responsibility changed to the following: "Applicable Entities under CIP-008." The Threshold for Reporting on this event is based on the criteria in CIP-008. If an entity is not an applicable entity under CIP-008, it should not have a reporting requirement based on CIP-008 that appears in EOP-004. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.*
Response: Thank you for your comment. Please see response above.		
City of Farmington	Negative	Attachment 1: BES equipment is too vague - consider changing to BES facility and including that reduces the reliability of the BES in the footnote. Is the footnote an and or an or? *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity.* *The DSR SDT used the defined term "Facility" to add clarity for several events listed in Attachment 1. A Facility is defined as:*

Organization	Yes or No	Question 3 Comment
		"A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)" *The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.* Attachment 1: Version 5 of CIP Requirements the use of the terms Critical Asset and Critical Cyber Asset. The drafting team should consider revising the table to be flexible so it will not require modification when new versions of CIP become effective. Clarify if Damage or Destruction is physical damage (aka - cyber incidents would be part of CIP-008 covered separately in Attachment 1.) *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Attachment 1: Unplanned Control Center evacuation - remove "potential" from the reporting responsibility Attachment 1: *The 'potential' language has been removed. The threshold for Reporting now reads as: "Each RC, BA, TOP that experiences the event".* SOL Tv - is not defined. *The SOL Violation (WECC only) event has been revised to remove Tv and replace it with "30 minutes" to be consistent with TOP-007-WECC requirements. The event has*

Organization	Yes or No	Question 3 Comment
		also been revised to indicate an SOL associated with a Major WECC transfer path. Attachment 2 - 3: change to, "Did the event originate in your system?" The requirement only requires reporting for Events - not potential events. This implies if there is potential for an event to occur, the entity should report (potential of a public appeal or potential to shed firm load) *The 'actual or potential' language has been removed.* Attachment 2 4: "Damage or Destruction to BES equipment" should be "Destruction of BES Equipment" like it is in Attachment 1 and "forced intrusion risk to BES equipment" remove "risk" *The 'Damage or Destruction' event category has been revised to say '...to a Facility', (a defined term) and thresholds have be modified to provide clarity. Also, the reporting timeline is now 24 hours.* *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.* The OE-417 requires several of the events listed in Attachment 1 be reported within 1 hour. FEUS recommends the drafting team review the events and the OE-417 form and align the reporting window requirements. For example, public appeals, load shedding, and system separation have a 1 hour requirement in OE-417. *OE-417, as well as, the EAWG's requirements were considered in creating Attachment*

Organization	Yes or No	Question 3 Comment
		1, but there remain differences for the following reasons: • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.*
Response: Thank you for your comment. Please see response above.		
Wisconsin Public Service Corp.	Negative	EOP-004 Attachment 1 states: That any Damage or destruction of a Critical Cyber Asset per CIP-002 Applicable Entities under CIP-002 Through intentional or unintentional human action. Requires reporting in 1 hour of recognition of event. This is too low of a threshold for reporting. Unintentional damage could be caused by an individual spilling coffee on a laptop. Hardly the item for a report. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 3 Comment
ACES Power Marketing, Hoosier Energy Rural Electric Cooperative, Inc., Sunflower Electric Power Corporation, Great River Energy	Negative	For many of the events listed in Attachment 1, there would be duplicate reporting the way it is written right now. For example, in the case of a fire in a substation (Destruction of BES equipment), the RC, BA, TO, TOP and perhaps the GO and GOP could all experience the event and each would have to report on it. This seems quite excessive and redundant. We recommend eliminating this duplicate reporting. *The DSR SDT has tried to minimize duplicative reporting, but recognizes there may be events that trigger more than one report. The current applicability ensures an event that could affect just one of the entities with reporting responsibility isn't missed.*
Response: Thank you for your comment. Please see response above.		
Consumers Energy	Negative	Forced intrusion needs to be specifically defined. A 1-hour report requirement is not necessary but for critical events that would have wide-ranging impact. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*

Organization	Yes or No	Question 3 Comment
		Requirements 2 and 3 should be combined into a single requirement. *The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."*
Response: Thank you for your comment. Please see response above.		
MidAmerican Energy Co.	Negative	MidAmerican Energy believes Attachment 1 expands the scope of what must be reported beyond what is required by FERC directives and beyond what is needed to improve security of the BES. Based on our understanding of Attachment 1, the category of "damage or destruction of a critical cyber asset" will likely result in hundreds or thousands of small equipment failures being reported to NERC and DOE, with no improvement to security. For example, hard drive failures, server failures, PLC failures and relay failures could all meet the criteria of "damage or destruction of a critical cyber asset." which would be required reporting in 1 hour. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat*

Organization	Yes or No	Question 3 Comment
		that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred. EOP-004-2 needs to clearly state that initial reports can be made by a phone call, email or another method, in accordance with paragraph 674 of FERC Order 706. MidAmerican recommends replacing Attachment 1 and Attachment 2 with the categories and timeframes that are listed in OE-417. This eliminates confusion between government requirements in OE-417 and NERC standards. *Attachment 1 provides the flexibility to make a verbal report. The header of Attachment 1 states:* *"NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per R1 and provide as much information as is available at the time of the notification. Reports to the ERO should be submitted to one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422."* *Attachment 2 provides the flexibility to make a verbal report. The header of Attachment 2 states:* *"This form is to be used to report events. The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Reports to the ERO should be submitted via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422."* *OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs;*

Organization	Yes or No	Question 3 Comment
		accommodation of other reporting obligations was considered as an opportunity not a 'must-have' • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.*
Response: Thank you for your comment. Please see response above.		
MidAmerican Energy Co.	Negative	MidAmerican Energy believes Attachment 1 expands the scope of what must be reported beyond what is required by FERC directives and beyond what is needed to improve security of the BES. EOP-004-2 needs to clearly state that initial reports can be made by a phone call, email or another method, in accordance with paragraph 674 of FERC Order 706. MidAmerican recommends replacing Attachment 1 and Attachment 2 with the categories and timeframes that are listed in OE-417. This eliminates confusion between government requirements in OE-417 and NERC standards. *Attachment 1 provides the flexibility to make a verbal report. The header of Attachment 1 states:* *"NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible*

Organization	Yes or No	Question 3 Comment
		Entity shall notify parties per R1 and provide as much information as is available at the time of the notification. Reports to the ERO should be submitted to one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422." *Attachment 2 provides the flexibility to make a verbal report. The header of Attachment 2 states:* *"This form is to be used to report events. The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Reports to the ERO should be submitted via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422."* *OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.*

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comment. Please see response above.		
Seattle City Light	Negative	Overarching Concern related to EOP-004-2 draft: The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes, as well as the CIP standards Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definitions of a BES element could change significantly and Critical Assets may no longer exist. As it relates to the proposed reporting criteria, it is debatable as to whether or not the destruction of, for example, one relay would be a reportable incident under this definition going forward given the current drafting team efforts. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Related to "Reportable Events" of Attachment 1: 1. A reportable event is stated as, "Risk to the BES", the threshold for reporting is, "From a non-environmental physical threat". This appears to be a catch-all event, and basically every other event in Attachment 1 should be reported because it is a risk to the BES. Due to the subjectivity of this event, suggest removing it from the list. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as*

Organization	Yes or No	Question 3 Comment
		a threat, not when it may have first occurred. 2. A reportable event is stated as, "Damage or destruction of Critical Asset per CIP-002". The term"Damage" would have to be defined in order for an entity to determine a threshold for what qualifies as "Damage" to a CA. One could argue that normal"Damage" can occur on a CA that is not necessary to report. There should also be caution here in adding CIP interpretation within this standard. Reporting Thresholds 1. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* The SDT made attempts to limit nuisance reporting related to copper thefts and so on which is supported. However a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could congest the reporting process with nuisance reporting and reviewing. An example is the "BES Emergency requiring manual firm load shedding of greater than or equal to 100 MW or the Loss of Firm load for = 15 Minutes that is greater than or equal to 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases these low thresholds represent reporting of minor wind events or other seasonal system issues on Local Network used to provide distribution service. *These thresholds reflect those used in the current in-force EOP-004-1, and haven't congested the reporting process to date.* Firm Demand 1. The use of Firm Demand in the context of the draft Standards could be used to describe commercial arrangements with a customer rather than a

Organization	Yes or No	Question 3 Comment
		reliability issue. Clarification of Firm Demand would be helpful *The DSR SDT did not use the words 'Firm Demand' anywhere in the proposed standard.*
Response: Thank you for your comment. Please see response above.		
Constellation Energy; Constellation Energy Commodities Group; Constellation Power Source Generation, Inc.	Negative	Please see the comments offered in the concurrent comment form. While Constellation is voting negative on this ballot, we recognize the progress made by the drafting team and find the proposal very close to acceptable. It should be noted that our negative vote is due to remaining concerns with the Attachment 1: Event Table categories language. In the comment form Constellation proposes revisions to both the requirement language and to the Event Table language; however, the Event Table language is the greater hurdle *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comment. Please see response above.		
Salt River Project	Negative	Related to "Reportable Events" of Attachment 1: 1. A reportable event is stated as, "Risk to the BES", the threshold for reporting is, "From a non-environmental physical threat". This as appears to be a catch-all event, and basically every other event should be reported because it is a risk to the BES. Due to the subjectivity of this event, suggest removing it from the list. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.* 2. A reportable event is stated as, "Damage or destruction of Critical Asset per CIP-002". The term "Damage" would have to be defined in order for an entity to determine a threshold for what qualifies as "Damage" to a CA. One could argue that normal "Damage" can occur on a CA that is not necessary to report. There should also be caution here in adding CIP interpretation within this standard. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.*
Response: Thank you for your comment. Please see response above.		
Southern California Edison Co.	Negative	SCE and WECC are in agreement on one key point (removing the requirement to

Organization	Yes or No	Question 3 Comment
		determine if an act was "sabotage"), however, I continue to believe SCE will find the one-hour reporting requirement difficult to manage. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		
City of Redding	Negative	The following comments are directed toward Attachment 1: We commend the SDT for properly addressing the sabotage issue. However, additional confusion is caused by introducing term "damage". As "damage" is not a defined term it would be beneficial for the drafting team to provide clarification for what is meant by "damage". *The 'Damage or Destruction' event category has been revised to say '...to a Facility', (a defined term) and thresholds have be modified to provide clarity. Also, the reporting timeline is now 24 hours.*

Organization	Yes or No	Question 3 Comment
		The threshold for reporting "Each public Appeal for load reduction" should clearly state the triggering is for the BES Emergency as routine "public appeal" for conservation could be considered a threshold for the report triggering.. *The DSR SDT believes the current language of the event category 'BES Emergency…' clearly excludes routine conservation requests. The Threshold for Reporting has been updated to read as: "Public appeal for load reduction event".* Regarding the SOL violations in Attachment 1 the SOL violations should only be those that affect the WECC Paths. *The SOL Violation (WECC only) event has been revised to remove Tv and replace it with "30 minutes" to be consistent with TOP-007-WECC requirements. The event is now "SOL for Major WECC Transfer Paths (WECC only)". .*
Response: Thank you for your comment. Please see response above.		
Avista Corp.	Negative	The VSLs associated with not reporting in an hour for some of the events (Destruction of BES Equipment) is too severe. Operators need to be able to deal with events and not worry about reporting until the system is secure. Back office personnel are only available 40-50 hours per week, so the reporting burden falls on the Operator. *The DSR SDT believes the VSL is appropriate for the only remaining 1 hour event.*
Response: Thank you for your comment. Please see response above.		
Avista Corp.	Negative	There is definitely a need to communicate and report out system events to NERC, RCs, and adjacent utilities. However, this new standard has gone too far with regards to reporting of certain events within a 1 hour timeframe and the associated VSLs for going beyond the hour time period. Operators need to be able to deal with the system events and not worry about reporting out for the "Destruction of BES

Organization	Yes or No	Question 3 Comment
		equipment" (first row in Attachment 1 -Reportable Events). Operators only have 40-50 hours out of 168 hours in a week where supporting personnel are also on shift, so this reporting burden will usually fall on the Operators not back office support. Again this is another example of the documentation requirements of a standard being more important than actually operating the system. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.* The "Destruction of BES equipment" event is too ambiguous and will lead to interpretations by auditors to determine violations. The ambiguity will also lead to the reporting of all BES equipment outages to avoid potential violations of the standard. It usually takes more than an hour to determine the cause and extent of an outage. *The 'Damage or Destruction' event category has been revised to say '...to a Facility', (a defined term) and thresholds have be modified to provide clarity. Also, the reporting timeline is now 24 hours.*

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comment. Please see response above.		
National Association of Regulatory Utility Commissioners	Negative	Therequirement that any event with the potential to impact reliability be reported is overly broad and requires more focus. *'Forced intrusion' and 'Risk to BES Equipment' (which this footnote referenced) have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		
Alameda Municipal Power, Salmon River Electric Cooperative	Negative	We feel that the drafting team has done an excellent job of providing clarify and reasonable reporting requirements to the right functional entity. We support the modifications but would like to have two additional minor modification in order to provide additional clarification to the Attachment I Event Table. We suggest the following clarifications: For the Event: BES Emergency resulting in automatic firm load shedding Modify the Entity with Reporting Responsibility to: Each DP or TOP that experiences the automatic load shedding within their respective distribution serving or Transmission Operating area. *The DSR SDT believes the current language is sufficient and cannot envision how a BA, TOP, or DP could 'experience the automatic load shedding' if it didn't take place in its balancing, transmission operating, or distribution serving area.*

Organization	Yes or No	Question 3 Comment
		For the Event: Loss of Firm load for = 15 Minutes Modify the Entity with Reporting Responsibility to: Each BA, TOP, DP that experiences the loss of firm load within their respective balancing, Transmission operating, or distribution serving area. With these modifications or similar modifications we fully support the proposed Standard. *The DSR SDT believes the current language is sufficient and cannot envision how a BA, TOP, or DP could 'experience the loss of firm load' if it didn't take place in its balancing, transmission operating, or distribution serving area.*
Response: Thank you for your comment. Please see response above.		
Orange and Rockland Utilities, Inc.	No	o Generally speaking the SDT should work with the NERC team drafting the Events Analysis Process (EAP) to ensure that the reporting events align and use the same descriptive language. o EOP-004 should use the exact same events as OE-417. These could be considered a baseline set of reportable events. If the SDT believes that there is justification to add additional reporting events beyond those identified in OE-417, then the event table could be expanded. o If the list of reportable events is expanded beyond the OE-417 event list, the supplemental events should be the same in both EOP-004-2 and in the EAP Categories 1 through 5. *OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may*

Organization	Yes or No	Question 3 Comment
		trigger further information requests from EAWG as necessary *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004.* o It is not clear what the difference is between a footnote and "Threshold for Reporting". All information should be included in the body of the table, there should be no footnotes. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* o Event: "Risk to BES equipment" should be deleted. This is too vague and subjective. Will result in many "prove the negative" situations.' *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.* o Event: "Destruction of BES equipment" is again too vague. The footnote refers to equipment being "damaged or destroyed". There is a major difference between

Organization	Yes or No	Question 3 Comment
		destruction and damage. *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity.* o Event: "Damage or Destruction of a Critical Asset or Critical Cyber Asset" should be deleted. Disclosure policies regarding sensitive information could limit an entity's ability to report. Unintentional damage to a CCA does not warrant a report. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* o Event: "BES Emergency requiring public appeal for load reduction" should be modified to note that this does not apply to routine requests for customer conservation during high load periods *The DSR SDT believes the current language of the event category 'BES Emergency…' clearly excludes routine conservation requests.*
Response: Thank you for your comment. Please see response above.		
Ameren	No	(1)By our count there are still six of the nineteen events listed with a one hour reporting requirement and the rest are all within 24 hour after the occurrence (or recognition of the event). This in our opinion, is reporting in real-time, which is against one of the key concepts listed in the background section:"The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of

Organization	Yes or No	Question 3 Comment
		standards). The proposed standard deals exclusively with after-the-fact reporting." *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.* (2)We believe the earliest preliminary report required in this standard should at the close of the next business day. Operating Entities, such as the RC, BA, TOP, GOP, DP, and LSE should not be burdened with unnecessary after-the-fact reporting while they are addressing real-time operating conditions. Entities should have the ability to allow their support staff to perform this function during the next business day as needed. We acknowledge it would not be an undue burden to cc: NERC on other required governmental reports with shorter reporting timeframes, but NERC should not expand on this practice. *No preliminary report is required within the revised standard.* (3)We agree with the extension in reporting times for events that now have 24 hours of reporting time. As a GO there are still too many potential events that still require

Organization	Yes or No	Question 3 Comment
		a 1 hour reporting time that is impractical, unrealistic and could lead to inappropriate escalation of normal failures. For example, the sudden loss of several control room display screens for a BES generator at 2 AM in the morning, with only 1 hour to report something, might be mistakenly interpreted as a cyber-attack. The reality is most likely something far more mundane such as the unexpected failure of an instrument transformer, critical circuit board, etc. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		
Duke Energy	No	All events in Attachment 1 should have reporting times of no less than 24 hours. As stated on page 6 of the current draft of the standard: "The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting."We maintain

Organization	Yes or No	Question 3 Comment
		that a report which is required to be made within one hour after an event is, in fact, a real time report. In the first hour or even several hours after an event the operator may appropriately still be totally committed to restoring service or returning to a stable bulk power system state, and should not stop that recovery activity in order to make this "after-the-fact" report. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		
American Public Power Association	No	APPA echoes the comments made by Central Lincoln: We do not believe the SDT has adequately addressed the FERC Order to "Consider whether separate, less burdensome requirements for smaller entities may be appropriate." The one and 24 hour reporting requirements continue to be burdensome to the smaller entities that do not maintain 24/7 dispatch centers. The one hour reporting requirement means that an untimely "recognition" starts the clock and reporting will become a higher

Organization	Yes or No	Question 3 Comment
		priority than restoration. The note regarding adverse conditions does not help unless we were to consider the very lack of 24/7 dispatch to be such a condition. APPA recommends the SDT evaluate a less burdensome requirement for smaller entities with reporting requirements in Attachment 1. This exception needs to address the fact that not all entities have 24 hour 7 day a week operating personnel. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.* *The DSR SDT believes that reliability is best served by imposing reporting criteria based on impact to the BES rather than an arbitrary entity size threshold. With these latest revisions, all the proposed event categories provide thresholds that will capture the appropriate entities and provide a manageable timeframe.* However, APPA cautions the SDT that changes to this standard may expose entities to reporting violations on DOE-OE-417 which imposes civil and criminal penalties on reporting events to the Department of Energy. APPA recommends that the SDT reach out to DOE for clarification of reporting requirements for DOE-OE-417 for small entities, asking DOE to change their reporting requirement to match EOP-004-2. If

Organization	Yes or No	Question 3 Comment
		DOE cannot change their reporting requirement the SDT should provide an explanation in the guidance section of Reliability Standard EOP-004-2 that addresses these competing FERC/DOE directives. *OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.*
Response: Thank you for your comment. Please see response above.		
BC Hydro	No	As an event would be verbally reported to the RC, all the one hour requirements to submit a written report should be moved from one hour to 24 hours. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact*

Organization	Yes or No	Question 3 Comment
		appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…" *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		
Bonneville Power Administration	No	BPA believes that the first three elements in Attachment 1 are too generic and should be with only the intentional human criterion. The suspicious device needs to be determined as a threat (and not left behind tools) before requiring a report. *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity. These thresholds include intentional human action as well as impact-based for those cases when cause isn't known. The determination of a threat as you suggest is now part of the revised event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.*

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comment. Please see response above.		
CenterPoint Energy	No	CenterPoint Energy agrees with the revision that allows more time for reporting some events; however, some 1 hour requirements remain. The Company does not agree with this timeframe for any event. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment Please see response above.		
Consolidated Edison Co. of NY, Inc.	No	Comments: We have a number of comments on Attachment 1 and will make them here: o Generally speaking the SDT should work with the NERC team drafting the Events Analysis Process (EAP) to ensure that the reporting events align and use the same descriptive language. o EOP-004 should use the exact same events as OE-417. These could be considered a baseline set of reportable events. If the SDT believes that there is justification to add additional reporting events beyond those identified in OE-417, then the event table could be expanded. o If the list of reportable events

Organization	Yes or No	Question 3 Comment
		is expanded beyond the OE-417 event list, the supplemental events should be the same in both EOP-004-2 and in the EAP Categories 1 through 5. *OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004.* o It is not clear what the difference is between a footnote and "Threshold for Reporting". All information should be included in the body of the table, there should be no footnotes. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'Any physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* o Event: "Risk to BES equipment" should be deleted. This is too vague and subjective. Will result in many "prove the negative" situations.'

Organization	Yes or No	Question 3 Comment
		'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. o Event: "Destruction of BES equipment" is again too vague. The footnote refers to equipment being "damaged or destroyed". There is a major difference between destruction and damage. *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity.* o Event: "Damage or Destruction of a Critical Asset or Critical Cyber Asset" should be deleted. Disclosure policies regarding sensitive information could limit an entity's ability to report. Unintentional damage to a CCA does not warrant a report. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* o Event: "BES Emergency requiring public appeal for load reduction" should be modified to note that this does not apply to routine requests for customer conservation during high load periods.

Organization	Yes or No	Question 3 Comment
		The DSR SDT believes the current language 'BES Emergency…' clearly excludes routine conservation requests.
Response: Thank you for your comment. Please see response above.		
Electric Reliability Council of Texas, Inc.	No	Destruction of BES equipment: 1. Request that the term "destruction" be clarified. *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity.* Damage or destruction of Critical Asset per CIP-002: 1. Request that the terms "damage" and "destruction" be clarified. 2. Is the expectation that an entity report each individual device or system equipment failure or each mistake made by someone administering a system? *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* 3. Request that "initial indication of the event" be changed to "confirmation of the event". Event monitoring and management systems may receive many events that are determined to be harmless and put the entity at no risk. This can only be determined after analysis of the associated events is performed. *The 'initial indication of the event' is no longer part of the threshold for 'Damage or Destruction of a Facility'* Risk to BES equipment: Request that the terms "risk" be clarified. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'.*

Organization	Yes or No	Question 3 Comment
		Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.
Response: Thank you for your comment. Please see response above.		
Exelon	No	Due to the size of the service territories in ComEd and PECO it's difficult to get to some of the stations within in an hour to analyze an event which causes concern with the 1 hour criteria. It is conceivable that the evaluation of an event could take longer then one hour to determine if it is reportable. Exelon cannot support this version of the standard until the 1 hour reporting criteria is clarified so that the reporting requirements are reasonable and obtainable. Exelon has concerns about the existing 1 hour reporting requirements and feels that additional guidance and verbiage is required for clarification. We would like a better understanding when the 1 hour clock starts please consider using the following clarifying statement, in the statements that read, "recognition of events" please consider replacing the word "recognition" with the word "confirmation" as in a "confirmed event" *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force*

Organization	Yes or No	Question 3 Comment
		standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.
Response: Thank you for your comment. Please see response above.		
Energy Northwest - Columbia	No	Energy Northwest - Columbia (ENWC) has concerns about the existing 1 hour reporting requirements and feels that additional guidance and verbiage is required for clarification. ENWC would like the word "recognition" in the statement that reads, "recognition of events," be replaced by "confirmation" as in "confirmed event."Also, we would like clarification as to when the 1 hour clock starts. Please consider changing recognition in "within 1 hour of recognition of event" and incorporating in "confirmation." *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 3 Comment
Indiana Municipal Power Agency	No	IMPA believes that some of the times may not be aggressive enought that are related to generation capacity shortages. *This standard concerns after-the-fact reporting. It is assumed that Responsible Entities will make appropriate real-time notifications as per other applicable standards, operating agreements, and good utility practice. This standard does not preclude a Responsible Entity from reporting more quickly than required by Attachment 1.* In addition, IMPA believes clarity needs to be added when saying within 1 hour of recognition of event. For example, A fence cutting may not be discovered for days at a remote substation and then a determination has to be made if it was "forced intrusion" - Does that one hour apply once the determination is made that is was "forced intrusion" or from the time the discovery was made? Some of the 1 hour time limits can be expanded to allow for more time, such as forced intrusion, destruction of BES equipment, Risk to BES equipment, etc. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'Any physical threat that could impact the operability of a Facility'. Timelines start at the moment the Responsible Entity determines the event represents a threat, not when it first occurred.*
Response: Thank you for your comment. Please see response above.		
Luminant Power	No	Luminant agrees with the changes the SDT made, however, the timeline should be modified to put higher priority activities before reporting requirements. The SDT should consider allowing entities the ability to put the safety of personnel, safety of the equipment, and possibly the stabilization of BES equipment efforts prior to initiating the one hour reporting timeline. Reporting requirements should not be prioritized above these important activities. The requirement to report one hour after the recognition of such an event may not be sufficient in all instances. Entities

Organization	Yes or No	Question 3 Comment
		should not have a potential violation as a result of putting these priority issues first and not meeting the one hour reporting timeline. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *Actions taken to maintain the reliability of the BES in real-time always take precedence over reporting. The revised thresholds should ensure there is no perverse driver to act differently.*
Response: Thank you for your comment. Please see response above.		
MidAmerican Energy	No	MidAmerican Energy agrees with the direction of consolidating CIP-001, EOP-004 and portions of CIP-008. However, we have concerns with some of the events included in Attachment 1 and reporting timelines. EOP-004-2 needs to clearly state that initial reports can be made by a phone call, email or another method, in accordance with paragraph 674 of FERC Order 706. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*

Organization	Yes or No	Question 3 Comment
		MidAmerican Energy believes draft Attachment 1 expands the scope of what must be reported beyond what is required by FERC directives and beyond what is needed to improve security of the BES. Based on our understanding of Attachment 1, the category of "damage or destruction of a critical cyber asset" will result in hundreds or thousands of small equipment failures being reported to NERC and DOE, with no improvement to security. For example, hard drive failures, server failures, PLC failures and relay failures could all meet the criteria of "damage or destruction of a critical cyber asset." *The DSR SDT agrees and the 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* We recommend replacing Attachment 1 and Attachment 2 with the categories and timeframes that are listed in OE-417. This eliminates confusion between government requirements in OE-417 and NERC standards. *OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may*

Organization	Yes or No	Question 3 Comment
		trigger further information requests from EAWG as necessary *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004.* Reporting timelines and reporting formFERC Order 706, paragraph 676, directed NERC to require a responsible entity to "at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report." In paragraph 674, FERC stated that the Commission agrees that, in the "aftermath of a cyber attack, restoring the system is the utmost priority." They clarified: "the responsible entity does not need to initially send a full report of the incident...To report to appropriate government authorities and industry participants within one hour, it would be sufficient to simply communicate a preliminary report, including the time and nature of the incident and whatever useful preliminary information is available at the time. This could be accomplished by a phone call or another method." While FERC did not order completion of a full report within one hour in Order 706, the draft EOP-004 Attachment 1 appears to require submittal of formal reports within one hour for six of the categories, unless there have been "certain adverse conditions" (in which case, as much information as is available must be submitted at the time of notification). *It is assumed that Responsible Entities will make appropriate real-time notifications as per other applicable standards, operating agreements, and good utility practice. As stated above, all one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673. For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions, which would certainly include the aftermath of a cyber attack that had*

Organization	Yes or No	Question 3 Comment
		major impact on the BES. The Violation Severity Levels are extreme for late submittal of a report. For example, it would be a severe violation to submit a report more than three hours following an event for an event requiring reporting in one hour. *The DSR SDT believes the VSL is appropriate now that it only applies to the remaining 1 hour reportable event, which is the Reportable Cyber Event under CIP-008.* MidAmerican Energy suggests incorporating the language from FERC Order 706, paragraph 674, into the EOP-004 reporting requirement to allow preliminary reporting within one hour to be done through a phone call or another method to allow the responsible entity to focus on recovery and/or restoration, if needed.MidAmerican Energy agrees with the use of DOE OE-417 for submittal of the full report of incidents under EOP-004 and CIP-008. We would note there are two parts to this form -- Schedule 1-Alert Notice, and Schedule 2-Narrative Description. Since OE-417 already requires submittal of a final report that includes Schedule 2 within 48 hours of the event, MidAmerican Energy believes it is not necessary to include a timeline for completion of the final report within the EOP-004 standard. We would note that Schedule 2 has an estimated public reporting burden time of two hours so it is not realistic to expect Schedule 2 to be completed within one hour. Events included in Attachment 1:MidAmerican Energy believes draft Attachment 1 expands the scope of what must be reported beyond what is required by FERC directives and beyond what is needed to improve security of the BES. The categories listed in Attachment 1 with one-hour reporting timelines cause the greatest concern. None of these categories are listed in OE-417, and all but the last row would not be considered a Cyber Security Incident under CIP-008, unless there was malicious or suspicious intent. *All one hour reporting timelines have been changed to 24 hours with the exception of*

Organization	Yes or No	Question 3 Comment
		a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673: *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*
Response: Thank you for your comment. Please see response above.		
SERC OC Standards Review Group	No	No event should have a reporting time less than at the close of the next business day. Any reporting of an event that requires a less reporting time should only be to entities that can help mitigate an event such as an RC or other Reliability Entity. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 3 Comment
Southwestern Power Administration	No	One hour is not enough time to make these assessments for all of the six items in attachment 1. All timing requirements should be made the same in order to simplify the reporting process. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*
Response: Thank you for your comment. Please see response above.		
ITC	No	See comments to Question #4
Response: Thank you for your comment. See response to Question 4.		
Southern Company	No	Southern request clarification on one of the entries in Attachment 1. The concern is with the last row on page 21 of Draft 3. What is the basis for "Voltage deviations"? The Threshold is Â±10% sustained for â‰¥ 15 minutes. Is the voltage deviation based on the Voltage Schedule for that particular timeframe, or is it something else (pre-contingency voltage level, nominal voltage, etc.)? *A sustained voltage deviation of ± 10% on the BES is significant deviation and is indicative of a shortfall of reactive resources either pre- or post-contingency. The DSR SDT is indifferent to which of nominal, pre-contingency, or scheduled voltage, is used*

Organization	Yes or No	Question 3 Comment
		as the baseline, but for simplicity and to promote a common understanding suggest using nominal voltage. In addition, the second row of Attachment 1 lists "Damage or destruction of a Critical Cyber Asset per CIP-002" as a reportable event. The threshold includes "...intentional or unintentional human action" and gives us 1 hour to report. The term "damage" may be overly broad and, without definition, is not limited in any way. If a person mistypes a command and accidentally deletes a file, or renames something, or in any way changes anything on the CCA in error, then this could be considered "damage" and becomes a reportable event. The SDT should consider more thoroughly defining what is meant by "damage". Should it incorporate the idea that the essential functions that the CCA is performing must be adversely impacted? *The DSR SDT agrees and the 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Lastly, no event should have a reporting time shorter than at the close of the next business day. Any reporting of an event that requires a shorter reporting time should only be to entities that can help mitigate an event such as an RC or other Reliability Entity. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber*

Organization	Yes or No	Question 3 Comment
		security incident as soon as possible, but in any event, within one hour of the event…" *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*
Response: Thank you for your comment. Please see response above.		
FEUS	No	The OE-417 requires several of the events listed in Attachment 1 be reported within 1 hour. FEUS recommends the drafting team review the events and the OE-417 form and align the reporting window requirements. For example, public appeals, load shedding, and system seperation have a 1 hour requirement in OE-417. *OE-417 thresholds and reporting timelines were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America. Non-US Responsible Entities cannot be obligated to report in shorter timelines simply to make the two forms line up. The current in-force EOP-004 requires 24 hour reporting on the items you have identified and so does the latest version of EOP-004-2* • *NERC has no control over the criteria in OE-417, which can change at any time* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004.*

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comment. Please see response above.		
SPP Standards Review Group	No	The purpose of the reporting requirement should be clear either in the text of the requirements or through an explanation that is embodied in the language of the approved set of standards. This would be consistent with a "Results-based" architecture. What is lacking in the proposed language of this standard is recognition that registered entities differ in size and relevance of their impact on the Bulk Electric System. Also, events that are reportable differ in their impact on the registered entity. A "one-size fits all" approach to this standard may cause smaller entities with low impact on the grid to take extraordinary measures to meet the reporting/timing requirements and yet be too "loose" for larger more sophisticated and impacting entities to meet the same requirements. Therefore, we believe language of the standard must clearly state the intent that entities must provide reports in a manner consistent with their capabilities from a size/reliability impact perspective and from a communications availability perspective. Timing requirements should allow for differences and consider these variables.Also, we would suggest including language to specifically exclude situations where communications facilities may not be available for reporting. For example, in situations where communications facilities have been lost, initial reports would be due within 6 hours of the restoration of those communication facilities. *The DSR SDT has reviewed Attachment 1 and made revisions to Event types, used the NERC approved term 'Facility', and revised some of the language under 'Entity with Reporting Responsibility' to ensure that these reportable events correctly represent the relative impact to the BES. Also, all one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"*

Organization	Yes or No	Question 3 Comment
		For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. We would also suggest that Attachment 1 be broken into two distinct parts such that those events which must be reported within 1 hour standout from those events that have to be reported within 24 hours. *The DSR SDT agrees and has implemented your suggestion.*
Response: Thank you for your comment. Please see response above.		
Kansas City Power & Light	No	The reportable events listed in Attachment 1 can be categorized as events that have had a reliability impact and those events that could have a reliability impact. The listed events that could have a reliability impact should have a 24 hour reporting requirement and the events that have had a reliability impact are appropriate at a 1 hour reporting. The following events with a 1 hour report requirement are recommended to change to 24 hour: Forced Intrusion and Risk to BES Equipment. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*

Organization	Yes or No	Question 3 Comment
		In addition, the Attachment 1 Events Table is incomplete as many of the listed events are incomplete regarding reporting time requirements and event descriptions. *Attachment 1 has been revised to more clearly indicate reporting timelines and some of the event descriptions were changed to add clarity.* Also recommend removing (ii) from note 5 with event "Destruction of BES equipment" as this part of the note is already described in the event description and insinuates reporting of equipment losses that do not have a reliability impact. *This footnote has been deleted* The events, "Damage or destruction of Critical Asset per CIP-002" and "Damage or destruction of a Critical Cyber Asset per CIP-002", does not have sufficient clarity regarding what that represents. A note similar in nature to Note 5 for BES equipment is recommended. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.*
Response: Thank you for your comment. Please see response above.		
Los Angeles Department of Water and Power	No	The reporting time of within 1 hour of recognition for a "Forced Intrusion" (last event category on page 20 of Draft 3, dated October 25, 2011) when considered with the associated footnote "Report if you cannot reasonably determine likely motivation" is overly burdensome and unrealistic. What is "reasonably determine likely motivation" is too general and requires further clarity. For example, LADWP has numerous facilities with extensive perimeter fencing. There is a significant

Organization	Yes or No	Question 3 Comment
		difference between a forced intrusion like a hole or cut in a property line fence of a facility versus a forced intrusion at a control house. Often cuts in fences, after further investigation, are determined to be cases of minor vandalism. An investigation of this nature will take much more than the allotted hour. The NERC Design Team needs to develop difference levels for the term "Force Intrusion" that fit the magnitude of the event and provide for adequate time to determine if the event was only a case of minor vandalism or petty thief. The requirement, as currently written, would unnecessarily burden an entity in reporting events that after given more time to investigate would more than likely not have been a reportable event. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		
Northeast Power Coordinating Council	No	The SDT should work with the NERC team drafting the Events Analysis Process (EAP) to ensure that the reporting events align and use the same descriptive language.EOP-004 should use the exact same events as OE-417. These could be considered a baseline set of reportable events. If the SDT believes that there is justification to add additional reporting events beyond those identified in OE-417, then the event table could be expanded. If the list of reportable events is expanded beyond the OE-417 event list, the supplemental events should be the same in both EOP-004-2 and

Organization	Yes or No	Question 3 Comment
		in the EAP Categories 1 through 5. *OE-417 thresholds and reporting timelines were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America. Non-US Responsible Entities cannot be obligated to report in shorter timelines simply to make the two forms line up. The current in-force EOP-004 requires 24 hour reporting on the items you have identified and so does the latest version of EOP-004-2* • *NERC has no control over the criteria in OE-417, which can change at any time* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004.* It is not clear what the difference is between a footnote and "Threshold for Reporting". All information should be included in the body of the table, there should be no footnotes. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* Event: Risk to BES equipment should be deleted. This is too vague and subjective. This will result in many "prove the negative" situations. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new*

Organization	Yes or No	Question 3 Comment
		event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Event: Damage or Destruction of a Critical Asset or Critical Cyber Asset should be deleted. Disclosure policies regarding sensitive information could limit an entity's ability to report. Unintentional damage to a CCA does not warrant a report. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Event: BES Emergency requiring public appeal for load reduction should be modified to note that this does not apply to routine requests for customer conservation during high load periods. *The DSR SDT believes the current language of the event category 'BES Emergency…' clearly excludes routine conservation requests.*
Response: Thank you for your comment. Please see response above.		
Florida Municipal Power Agency	No	The times don't seem aggressive enough for some of the Events related to generation capacity shortages, e.g., we would think public appeal, system wide voltage reduction and manual firm load shedding ought to be within an hour. These are indicators that the BES is "on the edge" and to help BES reliability,

Organization	Yes or No	Question 3 Comment
		communication of this status is important to Interconnection-wide reliability. *This standard concerns after-the-fact reporting. It is assumed that Responsible Entities will make appropriate real-time notifications as per other applicable standards, operating agreements, and good utility practice. This standard does not preclude a Responsible Entity from reporting more quickly than required by Attachment 1.*
Response: Thank you for your comment. Please see response above.		
NorthWestern Energy	Affirmative	In Attachment 1 NorthWestern Eneergy does not agree with the Transmission loss event, the threshold for reporting is "Unintentional loss of Three or more Transmission Facilities (excluding successful automatic reclosing)." There are lots of instances where this can happen and not have any major impacts to the BES. This reporting requirement is stemming from the Event Analysis Reporting Requirements and in many instances does not constitute an emergency. *You are correct. This event is used as a trigger to the Events Analysis Process.* Also, in Attachment 1 it is not clear when the DOE OE-417 form MUST be submitted. It give an option to use this form or another form but does not state when it must be used - confusing. *For the purposes of EOP-004, Responsible Entities may use either Attachment 2 or OE-417. Submission of OE-417 to the DOE is mandatory for US entities and outside the scope of NERC. Giving you the option to submit OE-417 to NERC and your RC to satisfy EOP-004 is permitted as a matter of convenience so you don't have to submit two different forms for the same event.*
Response: Thank you for your comment. Please see response above.		
Rutherford EMC	Affirmative	The SDT should consider adding a clause in the standard exempting small DP/LSEs

Organization	Yes or No	Question 3 Comment
		from the standard if the DP/LSE annually reviews and approves that it owns no facilities or equipment creating an event as decribed in Attachment 1. *The DSR SDT believes that reliability is best served by imposing reporting criteria based on impact to the BES rather than an arbitrary entity size threshold. With these latest revisions, all the proposed event categories provide thresholds that will capture the appropriate entities and provide a manageable timeframe.*
Response: Thank you for your comment. Please see response above.		
Fort Pierce Utilities Authority	Affirmative	The triggering event "Detection of a reportable Cyber Security Incident" listed in Attachment 1 assigns essentially all utilities reporting responsibility. This is not in line its reporting threshold, which is an event meeting the criteria in CIP-008. Shouldn't the responsibility fall on only those responsible for compliance with CIP-008, version 3 or 4, as determined by CIP-002? The SDT should also give additional consideration to necessary provisions to make it align with the proposed CIP-008-5. *The 'Entity with Reporting Responsibility' has been changed to reflect your comment to 'Each Responsible Entity applicable under CIP-008 that experiences the Cyber Security Incident.*
Response: Thank you for your comment. Please see response above.		
Nebraska Public Power District	Yes	Although 24 hours is a vast improvement, one business day would make more sense for after the fact reporting. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber*

Organization	Yes or No	Question 3 Comment
		security incident as soon as possible, but in any event, within one hour of the event…" *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*
Response: Thank you for your comment. Please see response above.		
FirstEnergy	Yes	Although we agree with the timeframes for reporting, we have other concerns as listed in our response to Question 4.
Response: Thank you for your comment. Please see response to question 4.		
Intellibind	Yes	Does this reporting conflict with reporting for DOE, and Regions? If so, what reporting requirements will the entity be held accountable to? Managing multiple reporting requirements for the multiple agencies is very problematic for entities and this standard should resolve those reporting requirments, as well as reduce the reporting down to one form and one submission. Reporting to ESISAC should take care of all reporting by the company. NERC should route all reports to the DOE, and regions through this mechanism. *OE-417 thresholds and reporting timelines were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America. Non-US Responsible Entities cannot be obligated to report in shorter timelines simply to make the two forms line up. NERC has no control over the criteria in OE-417, which can change at any time*

Organization	Yes or No	Question 3 Comment
		In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. NERC cannot take on the statutory obligation of US entities to report to the DOE.
Response: Thank you for your comment. Please see response above.		
Dominion	Yes	Dominion appreciates the changes that have been made to increase the 1 hr reporting time to 24 hours.
Response: Thank you for your comment.		
APX Power Markets (NCR-11034)	Yes	In my opinion the remaining items with 1 hour reporting requirements will in most cases require the input of in-complete information, since you maybe aware of the outage/disturbance, but not aware of any reason for it. If that is acceptable just to get the intitial report that there was an outage/disturbance then we are OK. I believe it would help to have that clarifed in the EOP, or maybe a CAN can be created for that. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions.*

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comment. Please see response above.		
Compliance & Responsbility Office	Yes	See comments in response to Question 4.
Response: Thank you for your comment. See response to Question 4.		
Lower Colorado River Authority	Yes	The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. EOP-004 has an "optional" Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify whether Registered Entities will still be required to submit both forms. Please also ensure there will not be duplication of efforts between the two reports. Although this is fairly minor, the clarification should be addressed. *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary.*
Response: Thank you for your comment. Please see response above.		
City of Austin dba Austin Energy	Yes	The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. EOP-004 has an "optional" Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify whether Registered Entities will still be required to submit both forms. Please also ensure there will not be duplication of efforts between the two reports. Although this is fairly minor, the clarification should be addressed. *Reports made under EOP-004 provide a minimum set of information, which may*

Organization	Yes or No	Question 3 Comment
		trigger further information requests from EAWG as necessary.
Response: Thank you for your comment. Please see response above.		
Public Utility District No. 1 of Snohomish County	Yes	The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. The EOP-004 has an "optional" Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify if both forms will still be required to be submitted. We also need to ensure that there won't be a duplication of efforts between the two reports. This is fairly minor, but the clarification need should be addressed. *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary.*
Response: Thank you for your comment. Please see response above.		
Seattle City Light	Yes	The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the Event Analysis process, but there is some duplication of efforts. The EOP-004 has an "optional" Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify if both forms will still be required to be submitted. We also need to ensure that there won't be a duplication of efforts between the two reports. This is fairly minor, but the clarification need should be addressed. *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 3 Comment
Salt River Project	Yes	The proposed reporting form for EOP-004-2 is less extensive than the Brief Report required by the NERC Event Analysis process, but there is some duplication of efforts. EOP-004 has an "optional" Written Description section for the event, while the Brief Report requires more detailed information such as a sequence of events, contributing causes, restoration times, etc. Please clarify whether Registered Entities will still be required to submit both forms. Please also ensure there will not be duplication of efforts between the two reports. Although this is fairly minor, the clarification should be addressed. *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary.*
Response: Thank you for your comment. Please see response above.		
Constellation Energy on behalf of Baltimore Gas & Electric, Constellation Power Generation, Constellation Energy Commodities Group, Constellation Control and Dispatch, Constellation NewEnergy and Constellation Energy Nuclear Group.	Yes	We agree with the change to the reporting times in Attachment 1. While this is an improvement, other concerns with the language in the events table language remain. Please see additional details below:General items: o All submission instructions (column 4 in Events Table) should qualify the recognition of the event as "of recognition of event as a reportable event." *Column 4 has been deleted. The table headings now state that Responsible Entities must submit the report within X hours of recognition of event.* o Is the ES-ISAC the appropriate contact for the ERO given that these two entities are separate even though they are currently managed by NERC? *Yes. This is the current reporting contact and this is the advice that the DSR SDT team received from NERC.* In addition, are the phone numbers in the Attachment 1 NOTE accurate? Is it possible they will change in a different cycle than the standard?

Organization	Yes or No	Question 3 Comment
		Yes. The standard will require updating should the phone number change. Specific Event Language: o Destruction of BES Equipment, footnote: Footnote 1, item iii confuses the clarification added in items i. and ii. Footnote 1 should be modified to state BES equipment that (i) an entity knows will affect an IROL or has been notified the loss affects an IROL; (ii) significantly affects the reserve margin of a Balancing Authority or Reserve Sharing Group. Item iii should be dropped. *The 'Damage or Destruction' event category has been revised to say "to a Facility', (a defined term) and thresholds have be modified to provide clarity. Footnotes for this event have been deleted.* o Damage or destruction of Critical Asset per CIP-002: Within the currently developing revisions to CIP-002 (version 5), Critical Asset will be retired as a glossary term. As well as addressing the durability of this event category, additional delineation is needed regarding which asset disruptions are to be reported. A CA as currently defined incorporates assets in a broad perspective, for instance a generating plant may be a Critical Asset. As currently written in Attachment 1, reporting may be required for unintended events, such as a boiler leak that takes a plant offline for a minor repair. Event #1 - Destruction of BES Equipment - captures incidents at the relevant equipment regardless of whether they are a Critical Asset or not. We recommend dropping this event. However, if reference to CIP-002 assets remains, it will be important to capture reporting of the events relevant to reliability and not just more events. o Damage or destruction of a Critical Cyber Asset per CIP-002: Because CCAs are defined at the component level, including this trigger is appropriate; however, as with CAs, the CCA term is scheduled to be retired under CIP-002 version 5. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately*

Organization	Yes or No	Question 3 Comment
		addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds. o Forced Intrusion: The footnote confuses the goal of including this event category. In addition, "forced" doesn't need to define the incident. Constellation proposes the following to better define the event:Intrusion that affects or attempts to affect the reliable operation of the BES (1)(1) Examples of "affecting reliable operation of the BES are": (i) device operations, (ii) protective equipment degradation, (iii) communications systems degradation including telemetered values and device status. o Risk to BES equipment: This category is too vague to be effective and the footnote further complicates the expectations around this event. The catch all concept of reporting potential risks to BES equipment is problematic. It's not clear what the reliability goal of this category is. Risk is not an event, it is an analysis. How are entities to comply with this "event", never mind within an hour? It appears that the information contemplated within this scenario would be better captured within the greater efforts underway by NERC to assess risks to the BES. This event should be removed from the Attachment 1 list in EOP-004. *'Forced intrusion' and 'Risk to BES Equipment' (which this footnote referenced) have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.* o BES Emergency requiring system-wide voltage reduction: the Entity with Reporting Responsibility should be limited to RC and TOP.

Organization	Yes or No	Question 3 Comment
		Entity with Reporting Responsibility states 'Initiating entity is responsible for reporting', which the DSR SDT feels is adequate direction in conjunction with the event: BES Emergency requiring system-wide voltage reduction. o Voltage deviations on BES Facilities: The Threshold for Reporting language needs more detail to explain +/- 10% of what? Proposed revision: Â± 10% outside the voltage schedule band sustained for â‰¥ 15 continuous minutes o IROL Violation (all Interconnections) or SOL Violation (WECC only): Should "Interconnections" be capitalized? o Transmission loss: The reporting threshold should provide more specifics around what constitutes Transmission Facilities. One minor item, under the Threshold for Reporting, "Three" does not need to be capitalized. *Both Transmission and Facilities are defined terms and the DSR SDT feels this gives sufficient direction.*
Response: Thank you for your comment. Please see response above.		
Pacific Northwest Small Public Power Utility Comment Group	Yes	While we agree with the revisions as far as they went, we do not believe the SDT has adequately addressed the FERC Order to "Consider whether separate, less burdensome requirements for smaller entities may be appropriate." The one and 24 hour reporting requirements continue to be burdensome to the smaller entities that do not maintain 24/7 dispatch centers. The one hour reporting requirement means that an untimely "recognition" starts the clock and reporting will become a higher priority than restoration. The note regarding adverse conditions does not help unless we were to consider the very lack of 24/7 dispatch to be such a condition. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber*

Organization	Yes or No	Question 3 Comment
		security incident as soon as possible, but in any event, within one hour of the event…" *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.* *The DSR SDT believes that reliability is best served by imposing reporting criteria based on impact to the BES rather than an arbitrary entity size threshold. With these latest revisions, all the proposed event categories provide thresholds that will capture the appropriate entities and provide a manageable timeframe.*
Response: Thank you for your comment. Please see response above.		
Clallam County PUD No.1	Yes	While we agree with the revisions as far as they went, we do not believe the SDT has adequately addressed the FERC Order to "Consider whether separate, less burdensome requirements for smaller entities may be appropriate." The one and 24 hour reporting requirements continue to be burdensome to the smaller entities that do not maintain 24/7 dispatch centers. The one hour reporting requirement means that an untimely "recognition" starts the clock and reporting will become a higher priority than restoration. The note regarding adverse conditions does not help unless we were to consider the very lack of 24/7 dispatch to be such a condition. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber*

Organization	Yes or No	Question 3 Comment
		security incident as soon as possible, but in any event, within one hour of the event…" *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.* *The DSR SDT believes that reliability is best served by imposing reporting criteria based on impact to the BES rather than an arbitrary entity size threshold. With these latest revisions, all the proposed event categories provide thresholds that will capture the appropriate entities and provide a manageable timeframe.*
Response: Thank you for your comment. Please see response above.		
Illinois Municipal Electric Agency	Yes	With the understanding this is within 24 hrs., and good professional judgment determines the amount of time to report the event to appropriate parties.
Response: Thank you for your comment.		
Ingleside Cogeneration LP	Yes	Yes. Any reporting that is mandated during the first hour of an event must be subject to close scrutiny. Many of the same resources that are needed to troubleshoot and stabilize the local system will be engaged in the reporting - which will impair reliability if not carefully applied. We believe that the ERO should reassess the need for any immediate reporting requirements on a regular basis to confirm that it provides some value to the restoration process. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706,*

Organization	Yes or No	Question 3 Comment
		Paragraph 673: *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1. Also, Attachment 1 provides the flexibility to make a verbal report under adverse conditions. For the revised event category 'A physical threat that could impact the operability of a Facility' the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.*
Response: Thank you for your comment. Please see response above.		
Southwest Power Pool Regional Entity	Yes	
ZGlobal on behalf of City of Ukiah, Alameda Municipal Power, Salmen River Electric, City of Lodi	Yes	
MRO NSRF	Yes	
Western Electricity Coordinating Council	Yes	
Imperial Irrigation District	Yes	

Organization	Yes or No	Question 3 Comment
ACES Power Marketing Standards Collaborators	Yes	
Santee Cooper	Yes	
Sacramento Municipal Utility District (SMUD)	Yes	
Electric Compliance	Yes	
PacifiCorp	Yes	
Arizona Public Service Company	Yes	
Westar Energy	Yes	
Springfield Utility Board	Yes	
Manitoba Hydro	Yes	
Xcel Energy	Yes	
Liberty Electric Power	Yes	
Colorado Springs Utilities	Yes	
Independent Electricity System Operator	Yes	
South Carolina Electric and	Yes	

Organization	Yes or No	Question 3 Comment
Gas		
ISO New England	Yes	
American Transmission Company, LLC	Yes	
PSEG	Yes	
American Electric Power	Yes	
Georgia System Operations Corporation	Yes	
NV Energy	Yes	
Occidental Power Services, Inc. (OPSI)	Yes	
Northeast Utilities	Yes	
Great River Energy	Yes	
Oncor Electric Delivery Company LLC	Yes	
PPL Electric Utilities and PPL Supply Organizations`		
Progress Energy		

Organization	Yes or No	Question 3 Comment
Texas Reliability Entity		
ReliabilityFirst		
NRECA		
Entergy Services		
Thompson Coburn LLP on behalf of Miss. Delta Energy Agency		

4. Do you have any other comment, not expressed in questions above, for the DSR SDT?

Summary Consideration: The issues addressed in this question resulted in the DSR SDT reviewing and updating each requirement, Attachment 1 and Attachment 2. The DSR SDT has removed ambiguous language such as "risk" and "potential" based on comments received. All of the time frames in Attachment 1 have been moved to 24 hours upon recognition with the exception to reporting of CIP-008 events that remains one hour per FERC Order 706. Attachment 2 has been rewritten to mirror Attachment 1 events for entities who wish to use Attachment 2 in lieu of the DOE Form OE 417. VSLs have been reviewed to match the updated requirements.

Organization	Yes or No	Question 4 Comment
Cleco Corporation, Cleco Power, Cleco Power LLC	Abstain	Cleco does not use the VSL or VRF.
Response: Thank you for your comment		
Oklahoma Gas and Electric Co.	Abstain	Please see comments on SPP ballot
Response: Thank you for your comment. See response to those comments.		
Alberta Electric System Operator	Abstain	The Alberta Electric System Operator will need to modify parts of this standard to fit the provincial model when it develops the Alberta Reliability Standard.
Response: Thank you for your comment.		
Gainesville Regional Utilities	Affirmative	Looking forward to the added clarity.
Response: Thank you for your comment.		

Organization	Yes or No	Question 4 Comment
Manitoba Hydro	Affirmative	Manitoba Hydro is voting affirmative but would like to point out the following issues: -Attachment 1: The term 'Transmission Facilities' used in Attachment 1 is capitalized, but it is not a defined term in the NERC glossary. The drafting team should clarify what is meant by 'Transmission Facilities' and remove the capitalization. – *The DSR SDT has reviewed the NERC Glossary of Terms and notes that Transmission and Facilities are both defined. The combination of these two definitions are what the DSR SDT has based the applicability of "Transmission Facilities" in Attachment 1.* Attachment 2: The inclusion of 'fuel supply emergency' in Attachment 2 creates confusion as it infers that reporting a 'fuel supply emergency' may be required by the standard even though it is not listed as a reportable event in Attachment 1. On a similar note, it is not clear what the drafting team is hoping to capture by including a checkbox for 'other' in Attachment 2. *The DSR SDT has removed both "fuel supply emergency" and "other" from Attachment 2.*
Response: Thank you for your comment. Please see response above.		
Oncor Electric Delivery	Affirmative	NERC's Event Analysis Program tends to parallel many of the reporting requirements as outlined in EOP-004 Version 2. Oncor recommends that NERC consider ways of streamlining the reporting process by either incorporating the Event Analysis obligations into EOP-004-2 or reducing the scope of the Event Analysis program as currently designed to consist only of "exception" reporting. *The reporting of events as required in EOP-004 is the input to the Events Analysis Program. Events are reported to the ERO and the EAP will follow up as per the EAP processes and procedures.*

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comment. Please see response above.		
City Utilities of Springfield, Missouri	Affirmative	SPRM supports the comments from SPP.
Response: Thank you for your comment. Please see response to comments from SPP.		
Kootenai Electric Cooperative	Affirmative	The changes are an improvement over the existing standards.
Response: Thank you for your comment.		
Empire District Electric Co.	Affirmative	We agree with the comments provided by SPP
Response: Thank you for your comment. Please see response to SPP comments.		
Lakeland Electric	Negative	1. Further clarity is needed. For example the standard stipulates in R1.3 ". .as appropriate." Who deems what is appropriate? Also in R1.4 ". .other circumstances" is open to interpretation. *Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to communicate events to as stated in the entity's Operating Plan.* *Requirement R1, Part 1.4 was removed from the standard* 2. Remove paragraph 1 of the data retention section as it parrots the Rules of Procedure, Appendix 4C: Compliance Monitoring and Enforcement Program, Section 3.1.4.2. Possibly place a pointer to the CMEP in the data retention section. *The item in question is standard boilerplate language that is being placed in all NERC standards.*

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comment. Please see response above.		
CPS Energy	Negative	oR1.4: CPS Energy believes that "updating the Operating Plan within 90 calendar days of any change..." is a very burdensome compliance documentation requirement. *Requirement R1, Part 1.4 was removed from the standard.* oAttachment 1: Events Table: In DOE OE-417 local electrical systems with less than 300MW are excluded from reporting certain events since they are not significant to the BES. CPS Energy believes that the benefit of reporting certain events on systems below this value would outweigh the compliance burden placed on these small systems. *Upon review of the DOE OE 417, it states "Local Utilities in Alaska, Hawaii, Puerto Rico, the U.S. Virgin Islands, and the U.S. Territories - If the local electrical system is less than 300 MW, then only file if criteria 1, 2, 3 or 4 are met". Please be advised this exception applies to entities outside the continental USA.*
Response: Thank you for your comment. Please see response above.		
Lakeland Electric	Negative	An issue of possible differences in interpretation between entities and compliance monitoring and enforcement is the phrase in 1.3 that states "the following as appropriate". Who has the authority to deem what is appropriate? *Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to communicate events to as stated in the entity's Operating Plan*

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comment. Please see response above.		
Dynegy Inc.; Southern Illinois Power Coop.; Louisville Gas and Electric Co.	Negative	Comments submitted as part of the SERC OC; I agree with the comments of the SERC OC Standards Review group that have been provided to NERC.; We are a signatory to the SERC OC RRG comments filed last week.
Response: Thank you for your comment. Please see response to the SERC OC RRG comments.		
Hydro One Networks, Inc.	Negative	First and foremost we are not supportive of continuance of standards that are not "results based". Standards written to gather data, make reports etc. should not be written. There should be other processes for reporting in place that will not be subject to ERO oversight and further compliance burdens. *The DSR SDT has been following the guidance set by NERC to write a "results based" standard. As with any process there may be many different ways to achieve the same outcome. The NERC Quality Process has not indicated any request to update this Standard, concerning the Results Based Standard format.* o We are disappointed that the standard does not appear to reduce reporting requirements nor does it promote more efficient reporting. We encourage the SDT to take a results based approach and coordinate and reduce reporting through efficiencies between the various agencies and NERC. *The DSR SDT is staying within scope of the approved SAR and will be forwarding your concern of efficiencies between various agencies and NERC* o The Purpose statement is very broad, and "...by requiring the reporting of events with the potential to impact reliability and their causes..." on the Bulk Electric System it can be said that every event occurring on the Bulk Electric System would have to be reported. There is already an event analysis process in place. Could this reporting

Organization	Yes or No	Question 4 Comment
		be effectively performed in that effort? *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:* *"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."* o The standard prescribes different sets of criteria, and forms. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.* o There should be one recipient of event information. That recipient should be a

Organization	Yes or No	Question 4 Comment
		"clearinghouse" to ensure the proper dissemination of information. *The DSR SDT is proposing revisions to the NERC Rules of Procedure that address your comment:* *812. NERC Reporting Clearinghouse* *NERC will establish a system to collect report forms as established for this section or standard, from any Registered Entities, pertaining to data requirements identified in Section 800 of this Procedure. Upon receipt of the submitted report, the system shall then forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary. This can include state, federal, and provincial organizations.* o Why is this standard applicable to the ERO? *The ERO is applicable to CIP-008 and therefore is applicable to this proposed Standard.*
Response: Thank you for your comment. Please see response above.		
FirstEnergy Corp., FirstEnergy Energy Delivery, FirstEnergy Solutions, Ohio Edison Company	Negative	FirstEnergy appreciates the hard work of the drafting team and believes it has made great improvements to the standards. However, we must vote negative at this time until a few issues are clarified per our comments submitted through the formal comment period.
Response: Thank you for your comment. Please see response to your other comments.		
Lakeland Electric	Negative	In general; here has not been sufficient prudency review for the standard, especially R1, to justify a performance based standard around a Frequency Response Measure *Based on your short comment, Requirement 1 has been modified as requested by stakeholders. The DSR SDT cannot answer the issue of Frequency Response Measures*

Organization	Yes or No	Question 4 Comment
		since it is not within the scope of the SAR.
Response: Thank you for your comment. Please see response above.		
Northeast Power Coordinating Council	Negative	NPCC believes that further revision of the standard is necessary so is not able to support the VSLs at this time. Comments to the standard will be made in the formal comment period.
Response: Thank you for your comment. Please see responses to your other comments.		
Central Lincoln PUD; Blachly-Lane Electric Co-op; Central Electric Cooperative, Inc. (Redmond, Oregon); Clearwater Power Co.; Consumers Power Inc.; Coos-Curry Electric Cooperative, Inc; Fall River Rural Electric Cooperative; Lane Electric Cooperative, Inc.; Northern Lights Inc.; Pacific Northwest Generating Cooperative; Raft River Rural Electric Cooperative; Umatilla Electric Cooperative; West Oregon Electric Cooperative, Inc.; Cowlitz County PUD	Negative	Please see comments submitted by the Pacific Northwest Small Public Power Utility Comment Group.
Response: Thank you for your comment. Please see responses to comments of the Pacific Northwest Small Public Power Utility		

Organization	Yes or No	Question 4 Comment
Comment Group.		
Rochester Gas and Electric Corp.	Negative	RG&E supports comments to be submitted to NPCC.
New Brunswick System Operator	Negative	See comments submitted by the NPCC Reliability Standards Committee and the IRC Standards Review Committee.
Florida Municipal Power Pool	Negative	See FMPA's comments
Response: Thank you for your comment. See responses to those comments.		
Commonwealth of Massachusetts Department of Public Utilities	Negative	Standards written to gather data, make reports etc. should not be written. There should be other processes for reporting in place that will not be subject to ERO oversight and further compliance burdens. *FERC Order 693 section 617 states "...the Commission directs the ERO to develop a modification to EOP-004-1 through the reliability Standards development process that includes any Requirement necessary for users, owners, and operators of the Bulk-Power System to provide data...". In order for entities to provide data they are required to implement their Operating Plan. EOP-004-2 will satisfy this FERC directive.*
Response: Thank you for your comment. Please see response above.		
Hydro One Networks, Inc.	Negative	Suggested key concepts for the SDT consideration in this standard: ? Develop a single form to report disturbances and events that threaten the reliability of the bulk electric system ? Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements ? Establish clear criteria for reporting ? *The DSR SDT has only provided one form within this proposed Standard, please see*

Organization	Yes or No	Question 4 Comment
		Attachment 2. Based on stakeholder feedback, the DSR SDT has allowed stakeholders to use the DOE Form OE 417. Please note that not every Stakeholder in NERC wishes to use the DOE Form OE 417. Establish consistent reporting timelines ? *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.* Provide clarity around who will receive the information and how it will be used ? Explore other opportunities beside a standard to effectively achieve the same outcome. Standards should be strictly results based, whose purpose is to achieve an adequate level of reliability on the BES. *The DSR SDT has clearly stated who will receive the information: Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to report events. Part 1.2 now reads:* *"1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations*

Organization	Yes or No	Question 4 Comment
		needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies." *The information received will be mainly used for situational awareness and other processes.*
Response: Thank you for your comment. Please see response above.		
Orlando Utilities Commission	Negative	The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes, as well as the CIP standards Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definitions of a BES element could change significantly and Critical Assets may no longer exist. As it relates to the proposed reporting criteria, it is debatable as to whether or not the destruction of, for example, one relay would be a reportable incident under this definition going forward given the current drafting team efforts. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.*
Response: Thank you for your comment. Please see response above.		
James A Maenner	Negative	The information in section "5 Background" should be moved from the standard to a supporting document. *The DSR SDT will refer to guidance within the Standards Development process on the proper place to maintain Background information.*

Organization	Yes or No	Question 4 Comment
		The reporting exemption language for weather in the Note on Attachment 1 - Events Table should be included in R3, not just a note. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2based on stakeholder comments and revised R3 (now R2) to:* *"R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."* The "Guideline and Technical Basis", last 3 pages, should be moved from the standard to a supporting document. *The Guideline and Technical Basis section is a part of the Results-Based Standard format and the information contained in it is in the correct place.*
Response: Thank you for your comment. Please see response above.		
Kansas City Power & Light Co.	Negative	The proposed Standard is in need of additional work to complete the Attachment 1, complete the VSL's, and clarify language and content within the proposed standard. *The DSR SDT has reviewed and revamped all Requirements and both Attachments based on stakeholders feedback. This will provide clarity for entities to follow.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 4 Comment
SERC Reliability Corporation	Negative	The purpose of the standard "To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of events with the potential to impact reliability and their causes, if known, by the Responsible Entities" has not been achieved as written. There is the potential for the information and data contemplated by this standard to be useful in achieving the stated purpose through follow-on activities of the industry, the regions, and NERC. However, as drafted, Attachment 1 will inform the ERO of the existence of only a portion of the "events with the potential to impact reliability and their causes, if known". *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:* *"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."* Events listed in Appendix E to the ERO Event Analysis Process document should be incorporated into the standard instead of hardwiring inconsistency by requiring a different set of events. Alternatively, the SDT should explore deleting Attachment 1 and instead referencing the ERO Event Analysis process (which as a learning organization will have systematic changes to the reporting thresholds over time). At first this may seem contrary to the SDT objective of eliminating fill-in-the-blank aspects of the existing standard but the SDT should explore the Commission's willingness to accept a reference document for reporting thresholds. Additionally, it is unclear how NERC's role as the ES-ISAC is supported through the requirements of this reliability standard. It appears to undermine the ability of NERC (ES-ISAC) to be made timely aware of threats to the critical infrastructure--at odds with it's purpose. Thus, this draft does not achieve the elimination of redundant reporting envisioned in the SAR, nor does it achieve the objective of supporting NERC in the analysis of disturbances or blackouts. *The DSR SDT is following NERC's ANSI approved process for standards development.*

Organization	Yes or No	Question 4 Comment
		The ERO Events Analysis process does not have the frame work as required by the ANSI development process. Within this proposed Standard, when an Attachment 1 event is recognized, the ERO (which is the ES-ISAC) will be one of the first to be notified, as will the entities Reliability Coordinator. This will enhance situational awareness as per the entity's Operation Plan and this Standard. *FERC Order 693 section 617 states "…the Commission directs the ERO to develop a modification to EOP-004-1 through the reliability Standards development process that includes any Requirement necessary for users, owners, and operators of the Bulk-Power System to provide data…". In order for entities to provide data they are required to implement their Operating Plan. EOP-004-2 will satisfy this FERC directive.*
Response: Thank you for your comment. Please see response above.		
Tucson Electric Power Co.	Negative	The tie between an Operating Plan and reportable disturbance events is not clear. Being the exception, I feel that a reportable disturbance methodology should be part of an Emergency Operating Plan. *EOP-004-2 provides Applicable Entities with the minimum report requirements for events contained in Attachment 1. NERC has defined Operating Plan in part as: "A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes." An entity may include a reportable disturbance methodology within their Operating Plan since this Standard does not preclude it.*
Response: Thank you for your comment. Please see response above.		
United Illuminating Co.	Negative	The VSL table is mistyped. R2 lists 1.1 and 1.5. R4 VRF should be lower.

Organization	Yes or No	Question 4 Comment
		Requirement R4 (now R3) calls for conducting an annual test of the communications process in Requirement 1, Part 1.2. It is not strictly administrative in nature and therefore does not meet the VRF guideline for a Lower VRF. .
Response: Thank you for your comment. Please see response above.		
PSEG Energy Resources & Trade LLC, PSEG Fossil LLC, Public Service Electric and Gas Co.	Negative	There are several items that need clarification. See PSEG's separately provided comments.
Response: Thank you for your comment. Please see response to your other comments.		
Kansas City Power & Light Co.	Negative	There is no VSL for R4. *The VSL for Requirement R4 was inadvertently redlined in the redline version of the standard, but it was present in the clean version.*
Response: Thank you for your comment. Please see response above.		
Ameren Services	Negative	We believe that these [VRFs and VSLs] will change as we expect some changes in the draft standard.
Response: Thank you for your comment.		
New York State Department of Public Service	Negative	While the proposed standard consolidates many reporting requirements, the requirement that any event with the "potential to impact reliability" be reported is overly broad and will prove to be burdensome and distracting to system operations. *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:*

Organization	Yes or No	Question 4 Comment
		"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."
Response: Thank you for your comment. Please see response above.		
Springfield Utility Board		o The Draft 3 Version History still lists the term "Impact Event" instead of "Event". *This has been corrected.* o Draft 3 of EOP-004-2 - Event Reporting does not provide a definition for the term "Event" nor does the NERC Glossary of Terms Used in Reliability Standards. SUB recommends that "Event" be listed and defined in "Definitions and Terms Used in the Standard" as well as the NERC Glossary, providing a framework and giving guidance to entities for how to determine what should be considered an "Event" (ex: sabotage, unusual occurrence, metal theft, etc.). *The DSR SDT has reviewed this issue and has changed "Event" to "event". Attachment 1 contains each reportable 'event".*
Response: Thank you for your comment. Please see response above.		
Northeast Utilities		- Incorporate NERC Event Analysis Reporting into this standard. Make the requirements more specific to functional registrations as opposed to having requirements applicable to "Responsible Entities".- The description of a Transmission Loss Event in A *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1. The DSR SDT has reviewed and reworded "Entities with Reporting Responsibilities" to require the minimum amount of entities who will be required to report each event.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 4 Comment
Progress Energy		(1) Attachment 1 lists "Destruction of BES Equipment" as a reportable event but then lists "equipment failure" as one of several thresholds for reporting, with a one hour time limit for reporting. It is simply not common sense to think of the simple failure of a single piece of equipment as "destruction of BES equipment". Does the standard really expect that every BES equipment failure must be reported within one hour, regardless of cause or impact to BES reliability? What is the purpose of such extensive reporting? *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* (2) The same comment as (1) above is applicable to the "Damage or destruction of Critical Asset" because one threshold is simple "equipment failure" as well. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* (3) Footnote 2 (page 20) says copper theft is not reportable "unless it effects the reliability of the BES", but footnote 1 on the same page says copper theft is reportable if "it degrades the ability of equipment to operate properly". In this instance, the proposed standard provides two different criteria for reporting one of the most common events on the same page. *The DSR SDT has removed all footnotes with the exception of the updated event within Attachment 1 that states: "A physical threat that could impact the operability of a Facility". This event has the following footnote, which states: "Examples include a*

Organization	Yes or No	Question 4 Comment
		train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility." (4) Forced Intrusion must be reported if "you cannot determine the likely motivation", and not based on a conclusion that the intent was to commit sabotage or intentional damage. This would require reporting many theft related instances of cut fences and forced doors (including aborted theft attempts where nothing is stolen) which would consume a great deal of time and resources and accomplish nothing. This criteria is exactly the opposite of the existing philosophy of only reporting events if there is an indication of an intent to commit sabotage or cause damage. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.* (5) "Risk to BES equipment…from a non-environmental physical threat" is reportable, but this is an example of a vague, open ended reporting requirement that will either

Organization	Yes or No	Question 4 Comment
		generate a high volume of unproductive reports or will expose reporting entities to audit risk for not reporting potential threats that could have been reported. The standard helpfully lists train derailments and suspicious devices as examples of reportable events. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.* The existing CAN for CIP-001 (CAN-0016) is already asking for a list of events that were analyzed so the auditors can determine if a violation was committed due to failure to report. I can envision the CAN for this new standard requiring a list of all "non-environmental physical threats" that were analyzed during the audit period to determine if applicable events were reported. This could generate a great deal of work simply to provide audit documentation even if no events actually occur that are reportable. It would also be easy for an audit team to second guess a decision that was made by an entity not to report an event (what is risk?...how much risk was present due to the event?...). Also, the reporting for this vague criteria must be done within one hour. Any event with a one hour reporting requirement should be crystal clear and unambiguous. *The DSR SDT has reworded and updated Attachment 1 per comments received and believes that the language used obviates the need for CAN-016. CAN-0016 has been*

Organization	Yes or No	Question 4 Comment
		remanded. (6) Transmission Loss...of three or more Transmission Facilities" is reportable. "Facility" is a defined term in the NERC Glossary, but "Transmission Facility" is not a defined term, which will lead to confusion when this criteria is applied. This requirement raises many confusing questions. What if three or more elements are lost due to two separate or loosely related events - is this reportable or not? What processes will need to be put in place to count elements that are lost for each event and determine if reporting is required? Why must events be reported that fit an arbitrary numerical criteria without regard to any material impact on BES reliability? *The DSR SDT used the defined term "Facility" to add clarity for several events listed in Attachment 1. A Facility is defined as:* *"A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"* *The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.* *Both Transmission and Facilities are defined terms and the DSR SDT feels this gives sufficient direction.*
Response: Thank you for your comment. Please see response above.		
MRO NSRF		: The MRO NSRF wishes to thank the SDT for incorporating changes that the industry had with reporting time periods and aligning this with the Events Analysis Working Group and Department of Energy's OE 417 reporting form.

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comment.		
FirstEnergy		1. Attachment 1 - Regarding the 1st event listed in the table, "Destruction of BES Equipment" and its accompanying Footnote 1, we believe that this event should be broken into two separate events that incorporate the specifics in the footnote as follows: a. "Destruction of BES equipment that associated with an IROL per FAC-014-2." Regarding the 1st event we have proposed - We have proposed this be made specific to IROL as stated in Footnote 1 part i. Also, we believe that only the RC and TOP would have the ability to quickly determine and report within 1 hour if the destruction is associated with an IROL. The other entities listed would not necessarily know if the event affects and IROL. Therefore, we also propose that the Entities with Reporting Responsibilities (column 2) be revised to only include the RC and TOP. *The DSR SDT agrees with your comment and made the following changes:* *'Threshold for Reporting' column in the 'Damage or Destruction' event category. The updated Threshold for Reporting now reads as:* *"Damage or destruction of a Facility that:* • *Affects an IROL (per FAC-014)* *OR* • *Results in the need for actions to avoid an Adverse Reliability Impact* *OR* • *Results from intentional human action."* b. "Destruction of BES equipment that removes the equipment from service." Regarding the 3rd event we have proposed - We have proposed this be made specific to destruction of BES equipment that removes the equipment from service as stated in Footnote 1 part iii. Also, the other part of footnote 1 part iii which states "Damaged or destroyed due to intentional or unintentional human action" is not

Organization	Yes or No	Question 4 Comment
		required since it is covered in the threshold for reporting. Also the term "Damaged" in this part iii is not appropriate since these events are limited to equipment that has been destroyed. We also propose that the Entities with Reporting Responsibilities (column 2) for this event would remain the same as it states now since any of those entities may observe out of service BES equipment.Regarding part ii of footnote 1, we do not believe that this event needs to be separated. Regarding the phrase "significantly affects the reliability margin of the system be clarified so that it is not left up to the entity to interpret a "significant" affect. Lastly, since we have incorporated parts i and iii into the two separate events and removed part ii as proposed above, the only statement that needs to be left in the Footnote 1 is: "Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative)." *The DSR SDT has removed all footnotes with the exception of the updated event within Attachment 1 that states: "Any physical threat that could impact the operability of a Facility". This event has the following footnote, which states: "Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* 2. Attachment 1 - We ask that the team add an "Event #" column to the table so that each of the events listed can be referred to by #, such as Event 1, Event 2, etc. *The DSR SDT believes that the minimum reporting attributes are contained in Attachment 1.* 3. Attachment 1 - Event titled "Damage or destruction of a Critical Cyber Asset per

Organization	Yes or No	Question 4 Comment
		CIP-002", the proposed threshold for reporting seems incomplete. We suggest the threshold for this event match the threshold for the Critical Asset event which states: "Initial indication the event was due to operational error, equipment failure, external cause, or intentional or unintentional human action."4. Attachment 1 - Events titled "Damage or destruction of a Critical Assets per CIP-002" and "Damage or destruction of a Critical Cyber Asset per CIP-002" seem ambiguous due to the term "damage". We suggest removal of "damage" or clarity as to what is considered a damaged asset.5. VSL Table - Instead of listing every entity, it may be more efficient to simply say "The Responsible Entity" in the VSL for each requirement.6. Guideline and Technical Basis section - This section does not provide guidance on each of the requirements of the standard. We suggest the team consider adding guidance for the requirements. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.*
Response: Thank you for your comment. Please see response above.		
Southwest Power Pool Regional Entity		1. EOP-004-2 R1.4 states entities must update their Operating Plans within 90 calendar days of incorporating lessons learned pursuant to R3. However, neither R3 nor Attachment 1 include a timeline for incorporating lessons learned. It is unclear when the "clock starts" on incorporating improvements or lessons learned. Within 90 days of what? 90 days of the event? 90 days from when management approved the lesson learned? Auditors need to know the trigger for the 90-day clock. *Requirement R1, Part 1.4 was removed from the standard.* 2. The Event Analysis classification includes Category 1C "failure or misoperation of

Organization	Yes or No	Question 4 Comment
		the BPS SPS/RAS". This category is not included in EOP-004-2's Attachment 1. This event, "failure or misoperation of the BPS SPS/RAS", needs to either be added to Attachment 1 or removed from the Event Analysis classification. It is important that EOP-004-2 Attachment 1 and the Event Analysis categories match up.Thank you for your work on this standard. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.*
Response: Thank you for your comment. Please see response above.		
Independent Electricity System Operator		1. Measures M1, M2 and M3: Suggest to achieve consistent wording among them by saying the leading part to "Each Responsible Entity shall provide...." *The DSR SDT is following the guidance within the Standards Development process on*

Organization	Yes or No	Question 4 Comment
		the wording pertaining to items outside the realm of a requirement. 2. In our comments on the previous version, we suggested the SDT to review the need to include IA, TSP and LSE for some of the reporting requirements in Attachment 1. The SDT's responded that it had to follow the requirements of the standards as they currently apply. Since these entities are applicable to the underlying standards identified in Attachment 1, they will be subject to reporting. We accept this rationale. However, the revised Attachment 1 appears to be still somewhat discriminative on who needs to report an event. For example, the event of "Detection of a reportable Cyber Security Incident" (6th row in the table) requires reporting by a list of responsible entities based on the underlying requirements in CIP-008, but the list does not include the IA, TSP and LSE. We again suggest the SDT to review the need for listing the specific entities versus leaving it general by saying: "Applicable Entities under CIP-008" for this particular item, and review and establish a consistent approach throughout Attachment 1. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008.* 3. VSLs: a. Suggest to not list all the specific entities, but replace them with "Each Responsible Entity" to simplify the write-up which will allow readers to get to the violation condition much more quickly. b. For R1, it is not clear whether the conditions listed under the four columns are "OR" or "AND". We believe it means "OR", but this needs to be clarified in the VSL table.4. The proposed implementation plan conflicts with Ontario regulatory practice respecting the effective date of the standard. It is suggested that this conflict be removed by appending to the implementation plan wording, after "applicable regulatory approval" in the Effective Dates Section on P. 2 of the draft standard and P. 1 of the draft implementation plan, to the following effect: ", or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities." *The DSR SDT is following the guidance within the Standards Development process on*

Organization	Yes or No	Question 4 Comment
		the wording pertaining to items outside the realm of a requirement.
Response: Thank you for your comment. Please see response above.		
NRECA		1. Please ensure that the work of the SDT is done in close coordination with Events Analysis Process (EAP) work being undertaken by the PC/OC and BOT, and with any NERC ROP additions or modifications. NRECA is concerned that the EAP work being done by these groups is not closely coordinated even though their respective work products are closely linked -- especially since the EAP references information in EOP-004. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.*

Organization	Yes or No	Question 4 Comment
		2. The SDT needs to be consistent in its use of "BES" and "BPS" - boths acronyms are used throughout the SDT documents. NRECA strongly prefers the use of "BES" since that is what NERC standards are written for. *The DSR SDT has used BES within EOP-004-2. All references to BPS have been removed.* 3. Under "Purpose" section of standard, 3rd line, add "BES" between "impact" and "reliability." Without making this change the "Purpose" section could be misconstrued to refer to reliability beyond the BES. *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:* *"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."* 4. In the Background section there is reference to the Events Analysis Program. Is that the same thing as the Events Analysis Process? Is it something different? Is it referring to a specific department at NERC? Please clarify in order to reduce confusion. Also in the Background section there is reference to the Events Analysis Program personnel. Who is this referring to -- NERC staff in a specific department? Please clarify. *The DSR SDT was explaining that the DSR SDT and has been coordinating with the "Events Analysis Working Group.* 5. In M1 please be specific regarding what "dated" means. *This is a common term used with many NERC Standards and simply means that your evidence is dated and time stamped.* 6. In M3 please make it clear that if there wasn't an event, this measure is not applicable

Organization	Yes or No	Question 4 Comment
		The DSR SDT has not implied that Applicable Entities need to prove that something did not happen. 7. In R4 it is not clear what "verify" means. Please clarify. *R4 (now R3) was revised to remove "verify"* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* 8. In Attachment 1 there are references to Critical Asset and Critical Cyber Asset. These terms will likely be eliminated from the NERC Glossary of Terms when CIP V5 moves forward and is ultimately approved by FERC. This could create future problems with EOP-004 if CIP V5 is made effective as currently drafted. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008.* 9. In Attachment 1 the one hour timeframe for submitting data for the first 7 items listed is very tight. Other than being required by the EOE)E-417 form, NRECA requests that the SDT provide further support for this timeframe. If there are not distinct reasons why 1 hour is the right timeframe for this, then other timeframes should be explored with DOE. *The DSR SDT also received many comments regarding the various events of Attachment 1. Many commenters questioned the reliability benefit of reporting events to the ERO and their Reliability Coordinator within 1 hour. Most of the events with a one hour reporting requirement were revised to 24 hours based on stakeholder comments as well as those types of events are currently required to be reported within 24 hours in the existing mandatory and enforceable standards. The only remaining type of event that is to be reported within one hour is "A reportable Cyber*

Organization	Yes or No	Question 4 Comment
		Security Incident" as it required by CIP-008. *FERC Order 706, paragraph 673 states: "...each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event within one hour of the event..."* *Note that members of NRECA may be required to submit the DOE Form OE 417, and this agency's reporting requirements are not within scope of the project.* 10. While including Footnote 1 is appreciated, NRECA is concerned that this footnote will create confusion in the compliance and audit areas and request the SDT to provide more definitive guidance to help explain what these "Events" refer to. NRECA has the same comment on Footnote 2 and 3. Specifically in Footnote 3, how do you clearly determine and audit from a factual standpoint something that "could have damaged" or "has the potential to damage the equiment?" *The DSR SDT has removed all footnotes with the exception of the updated event within Attachment 1 that states: "A physical threat that could impact the operability of a Facility". This event has the following footnote, which states: "Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* 11. In the Guideline and Technical Basis section, in the 1st bullet, how do you determine, demonstrate and audit for something that "may impact" BES reliability? *This statement has been removed per comments received.* 12. On p. 28, first line, this sentence seems to state that NERC, law enforcement and other entities - not the responsible entity - will be doing event analysis. My understanding of the current and future Event Analysis Process is that the

Organization	Yes or No	Question 4 Comment
		responsible entity does the event analysis. Please confirm and clarify. *EOP-004-2 requires Applicable Entities to "report " and "communicate" as stated in Requirement 1, Part 1.2: "A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."* *The Event Analysis Program may use a reported event as a basis to analyze an event. The processes of the Event Analysis Program fall outside the scope of this project, but the DSR SDT has collaborated with them of events contained in Attachment 1.* *The Standard does not require the Applicable Entity to analyze a reported event.*
Response: Thank you for your comment. Please see response above.		
Exelon		1. Please replace the text "Operating Plan" with procedure(s). Many companies have procedure(s) for the reporting and recognition of sabotage events. These procedures extend beyond operating groups and provide guidance to the entire company. *Thank you for your comment. The DSR SDT intends on keeping "Operating Plan" within EOP-004-2 since NERC has it defined as:* *"A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan". As stated, the Operating Plan may contain Operating procedures or Operating Processes. This will give Applicable Entities the greatest flexibility in achieving compliance with this Standard.*

Organization	Yes or No	Question 4 Comment
		2. The Loss of Off-site power event criteria is much improved from the last draft of EOP 004-2; however, some clarification is needed to more accurately align with NERC Standard NUC-001 in both nomenclature and intent. Specifically, as Exelon has previously commented, there are many different configurations supplying offsite power to a nuclear power plant and it is essential that all configurations be accounted for. As identified in the applicability section of NUC-001 the applicable transmission entities may include one or more of the following (TO, TOP, TP, TSP, BA, RC, PC, DP, LSE, and other non-nuclear GO/GOPs). Based on the response to previous comments submitted for Draft 2, Exelon understands that the DSR SDT evaluated the use of the word "source" but dismissed the use in favor of "supply" with the justification "[that] 'supply' encompasses all sources". Exelon again suggests that the word "source" is used as the event criteria in EOP-004-2 as this nomenclature is commonly used in the licensing basis of a nuclear power plant. By revising the threshold criteria to "one or more" Exelon believes the concern the DSR SDT noted is addressed and ensures all sources are addressed. In addition, by revising the threshold for reporting to a loss of "one or more" will ensure that all potential events (regardless of configuration of off-site power supplies) will be reported by any applicable transmission entity specifically identified in the nuclear plant site specific NPIRs.As previously suggested, Exelon again proposes that the loss of an off-site power source be revised to an "unplanned" loss to account for planned maintenance that is coordinated in advance in accordance with the site specific NPIRs and associated Agreements. This will also eliminate unnecessary reporting for planned maintenance.Although the loss of one off-site power source may not result in a nuclear generating unit trip, Exelon agrees that an unplanned loss of an off-site power source regardless of impact should be reported within the 24 hour time limit as proposed. Suggest that the Loss of Offsite power to a nuclear generating plant event be revised as follows:Event: Unplanned loss of any off-site power source to a Nuclear Power PlantEntity with Reporting Responsibility: The applicable Transmission Entity that owns and/or operates the off-site power source to a

Organization	Yes or No	Question 4 Comment
		Nuclear Power Plant as defined in the applicable Nuclear Plant Interface Requirements (NPIRs) and associated Agreements.Threshold for Reporting: Unplanned loss of one or more off-site power sources to a Nuclear Power Plant per the applicable NPIRs. *Based on comments received, this event has been updated within Attachment 1 to read as:* *"Complete loss of off-site power to a nuclear generating plant (grid supply)".* 3. Attachment 1 Generation loss event criteria Generation lossThe â‰¥ 2000 MW/â‰¥ 1000 MW generation loss criteria do not provide a time threshold or location criteria. If the 2000 MW/1000 MW is intended to be from a combination of units in a single location, what is the time threshold for the combined unit loss? For example, if a large two unit facility in the Eastern Interconnection with an aggregate full power output of 2200 MW (1100 MW per unit) trips one unit (1100 MW) [T=0 loss of 1100 MW] and is ramping back the other unit from 100% power and 2 hours later the other unit trips at 50% power [550 MW at time of trip]. The total loss is 2200 MW; however, the loss was sustained over a 2 hour period. Would this scenario require reporting in accordance with Attachment 1? What if it happened in 15 minutes? 1 hour? 24 hours? Exelon suggests the criteria revised to include a time threshold for the total loss at a single location to provide this additional guidance to the GOP (e.g., within 15 minutes to align with other similar threshold conditions). Threshold for Reporting ï€ â‰¥ 2,000 MW unplanned total loss at a single location within 15 minutes for entities in the Eastern or Western Interconnection â‰¥ 1000 MW unplanned total loss at a single location within 15 minutes for entities in the ERCOT or Quebec Interconnection *The DSR SDT has not modified this event since it is being maintained as it is presently enforceable within EOP-004-1.* 4. Exelon appreciates that the DSR SDT has added the NRC to the list of Stakeholders in the Reporting Process, but does not agree with the SDT response to FirstEnergy's

Organization	Yes or No	Question 4 Comment
		comment to Question 17 [page 206] that stated "NRC requirements or comments fall outside the scope of this project." Quite the contrary, this project should be communicated and coordinated with the NRC to eliminate confusion and duplicative reporting requirements. There are unique and specific reporting criteria and coordination that is currently in place with the NRC, the FBI and the JTTF for all nuclear power plants. If an event is in progress at a nuclear facility, consideration should be given to coordinating such reporting as to not duplicate effort, introduce conflicting reporting thresholds, or add unnecessary burden on the part of a nuclear GO/GOP who's primary focus is to protect the health and safety of the public during a potential radiological sabotage event (as defined by the NRC) in conjunction with potential impact to the reliability of the BES. *The DSR SDT has established a minimum amount of reporting for events listed in Attachment 1. The NRC does not fall under the jurisdiction of NERC and so therefore it is not within scope of this project.* 5. Attachment 1 Detection of a reportable Cyber Security Incident event criteria.The threshold for reporting is "that meets the criteria in CIP-008". If an entity is exempt from CIP-008, does that mean that this reportable event is therefore also not applicable in accordance with EOP-004-2 Attachment 1? *If an entity is exempt from CIP-008, then they do not have to report this type of event. Entities can report any situation at anytime to whomever they wish. If an entity is responsible for items that fall under a Cyber Security Incident, then they would report per this standard.*
Response: Thank you for your comment. Please see response above.		
Duke Energy		1. Reporting under EOP-004-2 should be more closely aligned with Events Analysis Reporting. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating*

Organization	Yes or No	Question 4 Comment
		Attachment 1, but there remain differences for the following reasons: • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.* 2. Attachment 1 - Under the column titled "Entity with Reporting Responsibility", several Events list multiple entities, using the phrase "Each RC, BA, TO, TOP, GO, GOP, DP that experiences..." or a similar phrase requiring that multiple entities report the same event. We believe these entries should be changed so that multiple reports aren't required for the same event. *The DSR SDT agrees that there may be some dual reporting for the same event. The minimum Applicable Entities have been review and updated where updates could be made. The DSR SDT believes that a dual report will provide a clearer picture of the breadth and depth of an event the Electric Reliability Organization and the Applicable Entities Reliability Coordinator.* 3. Attachment 1 - The phrase "BES equipment" is used several times in the Events Table and footnotes to the table. "Equipment" is not a defined term and lacks clarity. "Element" and "Facility" are defined terms. Replace "BES equipment" with

Organization	Yes or No	Question 4 Comment
		"BES Element" or "BES Facility". *The DST SDT has removed the term "equipment" from Attachment 1 per comments received.* 4. Attachment 1 - The Event "Risk to BES equipment" is unclear, since some amount of risk is always present. Reword as follows: "Event that creates additional risk to a BES Element or Facility." *The DSR SDT has removed this event from Attachment 1. Several stakeholders expressed concerns relating to the "Forced Intrusion" event. Their concerns related to ambiguous language in the footnote. The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* 5. Attachment 1 - The Threshold for Reporting Voltage deviations on BES Facilities is identified as "+ 10% sustained for > 15 continuous minutes." Need to clarify + 10% of what voltage? We think it should be nominal voltage. *A sustained voltage deviation of ± 10% on the BES is significant deviation and is indicative of a shortfall of reactive resources either pre- or post-contingency. The DSR SDT is indifferent to which of nominal, pre-contingency, or scheduled voltage, is used as the baseline, but for simplicity and to promote a common understanding suggest using nominal voltage.* 6. Attachment 1 - Footnote 1 contains the phrase "has the potential to". This phrase should be struck because it creates an impossibly broad compliance responsibility. Similarly, Footnote 3 contains the same phrase, as well as the word "could" several times, which should be changed so that entities can reasonably comply.

Organization	Yes or No	Question 4 Comment
		The DSR SDT has removed all footnotes with the exception of the updated event within Attachment 1 that states: "A physical threat that could impact the operability of a Facility". This event has the following footnote, which states: "Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility." 7. Attachment 1 - The "Unplanned Control Center evacuation" Event has the word "potential" in the column under "Entity with Reporting Responsibility". The word "potential" should be struck.8. Attachment 2 - Includes "fuel supply emergency", which is not listed on Attachment 1. *The DSR SDT has removed the word "potential" from this event. It now reads as: "Each RC, BA, TOP that experiences the event"*
Response: Thank you for your comment. Please see response above.		
Energy Northwest - Columbia		1. The Loss of Off-site power event criteria is much improved from the last draft of EOP 004-2; however, some clarification is needed to more accurately align with NERC Standard NUC-001 in both nomenclature and intent. Specifically, there are many different configurations supplying offsite power to a nuclear power plant and it is essential that all configurations be accounted for. As identified in the applicability section of NUC-001 the applicable transmission entities may include one or more of the following (TO, TOP, TP, TSP, BA, RC, PC, DP, LSE, and other non-nuclear GO/GOPs). Based on the response to previous comments submitted for Draft 2, Energy Northwest understands that the DSR SDT evaluated the use of the word "source" but dismissed the use in favor of "supply" with the justification "[that] 'supply' encompasses all sources". Energy Northwest suggests that the word

Organization	Yes or No	Question 4 Comment
		"source" is used as the event criteria in EOP-004-2 as this nomenclature is commonly used in the licensing basis of a nuclear power plant. By revising the threshold criteria to "one or more" Energy Northwest believes the concern the DSR SDT noted is addressed and ensures all sources are addressed. In addition, by revising the threshold for reporting to a loss of "one or more" will ensure that all potential events (regardless of configuration of off-site power supplies) will be reported by any applicable transmission entity specifically identified in the nuclear plant site specific NPIRs.Energy Northwest proposes that the loss of an off-site power source be revised to an "unplanned" loss to account for planned maintenance that is coordinated in advance in accordance with the site specific NPIRs and associated Agreements. This will also eliminate unnecessary reporting for planned maintenance.Although the loss of one off-site power source may not result in a nuclear generating unit trip, Energy Northwest agrees that an unplanned loss of an off-site power source regardless of impact should be reported within the 24 hour time limit as proposed. Suggest that the Loss of Offsite power to a nuclear generating plant event be revised as follows:Event: Unplanned loss of any off-site power source to a Nuclear Power PlantEntity with Reporting Responsibility: The applicable Transmission Entity that owns and/or operates the off-site power source to a Nuclear Power Plant as defined in the applicable Nuclear Plant Interface Requirements (NPIRs) and associated Agreements.Threshold for Reporting: Unplanned loss of one or more off-site power sources to a Nuclear Power Plant per the applicable NPIRs. *Based on comments received, this event has been updated within Attachment 1 to read as:* *"Complete loss of off-site power to a nuclear generating plant (grid supply)".* 2. Please consider changing "Operating Plan" with "Procedure(s)". Procedures extend beyond operating groups and provide guidance to the entire company.

Organization	Yes or No	Question 4 Comment
		The DSR SDT intends on keeping "Operating Plan" within EOP-004-2 since NERC has it defined as: *"A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan". As stated, the Operating Plan may contain Operating procedures or Operating Processes. This will give Applicable Entities the greatest flexibility in achieving compliance with this Standard.*
Response: Thank you for your comment. Please see response above.		
Colorado Springs Utilities		Agree with concept to combine CIP-001 into EOP-004. Agree with elimination of "sabotage" concept. Appreciate the attempt to combine reporting requirements, but it seems that in practice will still have separate reporting to DOE and NERC/Regional Entities. EOP-004-2 A.5. "Summary of Key Concepts" refers to Att. 1 Part A and Att. 1 Part B. I believe these have now been combined. EOP-004-2 A.5. "Summary of Key Concepts" refers to development of an electronic reporting form and inclusion of regional reporting requirements. It is unfortunate no progress was made on this front.
Response: Thank you for your comment. The DSR SDT is providing a proposed revision to the NERC Rules of Procedure to address the electronic reporting concept. These proposed revisions will be posted with the standard.		
American Transmission Company, LLC		ATC appreciates the work of the SDT in incorporating changes that the industry had with reporting time periods and aligning this with the Events Analysis Working Group and Department of Energy's OE 417 reporting form.
Response: Thank you for your comment.		

Organization	Yes or No	Question 4 Comment
Manitoba Hydro		Attachment 1 - The term 'Transmission Facilities' used in Attachment 1 is capitalized, but it is not a defined term in the NERC glossary. The drafting team should clarify this issue. *Both Transmission and Facilities are defined terms and the DSR SDT feels this gives sufficient direction.* Attachment 2 - The inclusion of 'Fuel supply emergency' in Attachment 2 creates confusion as it infers that reporting a 'fuel supply emergency' may be required by the standard even though 'fuel supply emergency' is not listed in Attachment 1. On a similar note, it is not clear what the drafting team is hoping to capture by including a checkbox for 'other' in Attachment 2. *The DSR SDT has removed both "fuel supply emergency" and "other" from Attachment 2.*
Response: Thank you for your comment. Please see response above.		
NV Energy		Attachment 1 includes an item "Detection of a reportable cyber security incident." The reporting requirement is a report via Attachment 2 or the OE417 report form submittal. However, under CIP-008, to which this requirement is linked, the reporting is accomplished via NERC's secure CIPIS reporting tool. This appears to be a conflict in that the entity is directed to file reporting under CIP-008 that differs from this subject standard. *CIP-008-4, Requirement 1, Part 1.3 states that an entity must have:* *1.3 Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.*

Organization	Yes or No	Question 4 Comment
		EOP-004-2 also allows for submittal of the report to the ESISAC. Attachment 1 also includes a provision for reporting the "loss of firm load greater than or equal to 15 minutes in an amount of 200MW (or 300MW for peaks greater than 3000MW). This appears to be a rather low threshold, particularly in comparison with the companion loss of generation reporting threshold elsewhere in the attachment. The volume of reports triggered by this low threshold will likely lead to an inordinate number of filed reports, sapping NERC staff time and deflecting resources from more severe events that require attention. I suggest either an increase in the threshold, or the addition of the qualifier "caused by interruption/loss of BES facilities" in this reporting item. This qualifier would therefore exclude distribution-only outages that are not indicative of a BES reliability issue. *The DSR SDT has not modified this event since it is being maintained as it is presently enforceable within EOP-004-1.*
Response: Thank you for your comment. Please see response above.		
BC Hydro		Attachment 1: Reportable Events: BC Hydro recommends further defining "BES equipment" for the events Destruction of BES equipment and Risk to BES equipment. Attachment 1: Reportable Events: BC Hydro recommends defining the Forced intrusion event as the wording is very broad and open to each entities interpretation. What would be a forced intrusion ie entry or only if equipment damage occurs? *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say ' to a Facility', (a defined term) and thresholds have be modified to provide clarity.*

Organization	Yes or No	Question 4 Comment
		The footnote was deleted • *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.* *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.*
Response: Thank you for your comment. Please see response above.		
ISO New England		Attachment 1should be revisited. "Equipment Damage" is overly vague and will also potentially result in reporting on equipment failures which may simply be related to the age and/or vintage of equipment. *The DSR SDT has revised this event based on comments received. The new event is "Damage or destruction of a Facility" which has a threshold of "Damage or destruction of a Facility that:* *Affects an IROL (per FAC-014)* *OR* *Results in the need for actions to avoid an Adverse Reliability Impact* *OR*

Organization	Yes or No	Question 4 Comment
		Results from intentional human action."
Response: Thank you for your comment. Please see response above.		
Constellation Energy on behalf of Baltimore Gas & Electric, Constellation Power Generation, Constellation Energy Commodities Group, Constellation Control and Dispatch, Constellation NewEnergy and Constellation Energy Nuclear Group.		Background Section: The background section in this revision of EOP-004 reads more like guidance than a background of the development of the event reporting standard. Because of the background remains as part of the standard, the language raises questions as to role it plays relative to the standard language. For instance, the Law Enforcement Reporting section states:"Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES." It's not clear how "potential to impact to a wider area of the BES" is defined and where it fits into the standard. As well, and perhaps more problematic, is the Reporting Hierarchy for Reportable Events flow chart. While the flow chart concept is quite useful as a guidance tool, the flow chart currently in the Background raises questions. For instance, the Procedure to Report to Law Enforcement sequence does not map to language in the requirements. Further, Entities would not know about the interaction between law enforcement agencies. *The DSR SDT included the flow chart as an example of how an entity might report and communicate an event. For clarity, we have added the phrase "Example of Reporting Process Including Law Enforcement" to the top of the page.* Please see additional recommended revisions to the requirement language and to the Events Table in the Q2 and Q3 responses. *The DSR SDT has removed the wording of "potential" based on comments received.* Attachment 2: Event Reporting Form: The review of the form is one of the many aspects to compare with the developments within the Events Analysis Process (EAP) developments. We support the effort to create one form for submissions. The

Organization	Yes or No	Question 4 Comment
		recent draft EAP posted as part of Planning Committee and Operating Committee agendas includes a form requiring a few bits of additional relevant information when compared to the EOP-004 form. This may be a valuable approach to avoid follow up inquiries that may result if the form is too limited. We suggest that consideration be given to the proposed EAP form. One specific note on the Proposed EOP-004 Attachment 2: The "Potential event" box in item 3 should be eliminated to track with the removal of the "Risk to the BES" category. *The DSR SDT has updated Attachment 2 to remove potential event and "Risk to the BES" category based on comments received.*
Response: Thank you for your comment. Please see response above.		
Bonneville Power Administration		BPA believes that Attachment 1 has too many added reportable items because unintentional, equipment failure & operational errors are included in the first three items. A. Change to only "intentional human action". Otherwise, the first item "destruction of BES equipment" is too burdensome, along with its short time reporting time: i. - If a single transformer fails that shouldn't require a report. ii.- Emergency actions have to be taken for any failure of equipment, e.g. a loss of line reduces a path SOL and requires curtailments to reduce risk to the system. *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* B. The item for "risk to BES" is not necessary until the suspicious object has been identified as a threat. If what turns out to be air impact wrench left next to BES

Organization	Yes or No	Question 4 Comment
		equipment, that should not be a reportable incident as this current table implies. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.* *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* C. The nuclear "LOOP" should be only reported if total loss of offsite source (i.e. 2 of 2 or 3 of 3) when supplying the plants load. If lightning or insulator fails causing one of the line sources to trip that's not a system disturbance especially if it is just used as a backup. It should only be a NRC process if they want to monitor that. *The DSR SDT has updated this event per your comment, it now reads as: "Complete loss of off-site power to a nuclear generating plant (grid supply)"* The VRF/VSL: BPA believes that the VRF for R2 & R4 should be "Lower". *The DSR SDT has reviewed and updated the two new requirements and believe the VRF's follow the NERC Standard development process.*
Response: Thank you for your comment. Please see response above.		
CenterPoint Energy		CenterPoint Energy appreciates the SDT's consideration of comments and removal of the term, Impact Event. However, the Company still suggests removing the phrase "with the potential to impact" from the purpose as it is vast and vague. An

Organization	Yes or No	Question 4 Comment
		alternative purpose would be "To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of events that impact reliability and their causes if known". The focus should remain on those events that truly impact the reliability of the BES. *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:* *"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."* CenterPoint Energy remains very concerned about the types of events that the SDT has retained in Attachment 1 as indicated in the following comments: Destruction of BES Equipment - The loss of BES equipment should not be reportable unless the reliability of the BES is impacted. *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* Footnote 5, iii should be modified to tie the removal of a piece of equipment from service back to reliability of the BES. Risk to BES equipment: This Event is too vague to be meaningful and should be deleted. The Event should be modified to "Detection of an imminent physical threat to BES equipment". *The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".*

Organization	Yes or No	Question 4 Comment
		Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. *The footnote regarding this event type was expanded to provide additional guidance in:* *"Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* Any reporting time frame of 1 hour is unreasonable; Entities will still be responding to the Event and gathering information. A 24 hour reporting time frame would be more reasonable and would still provide timely information. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.*

Organization	Yes or No	Question 4 Comment
		System Separation: The 100 MW threshold is too low for a reliability impact. A more appropriate threshold is 500 MW. *The DSR SDT has reviewed your request and have determined the event as written "Each separation resulting in an island of generation and load ≥ 100 MW" does impact the reliability of the BES.* Loss of Monitoring or all voice communication capability: The two elements of this Event should be separated for clarity as follows: "Loss of monitoring of Real-Time conditions" and "Loss of all voice communication capability." *The DSR SDT has broken this event down into two distinct events: "Loss of all voice communication capability" and "Complete or partial loss of monitoring capability", per comments received.*
Response: Thank you for your comment. Please see response above.		
Orange and Rockland Utilities, Inc./Consolidated Edison Co. of NY, Inc.		Comments: o Requirement 4 does not specifically state details necessary for an entity to achieve compliance. Requirement 4 should provide more guidance as to what is required in a drill. Audit / enforcement of any requirement language that is too broad will potentially lead to Regional interpretation, inconsistency, and additional CANs. o R4 should be revised to delete the 15 month requirement. CAN-0010 recognizes that entities may determine the definition of annual. *Requirement R4 has been revised as you suggested.* o The Purpose of the Standard should be revised because some of the events being reported on have no impact on the BES. Revise Purpose as follows: To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of [add] "major system events." [delete - "with the potential to impact

Organization	Yes or No	Question 4 Comment
		reliability and their causes, if known, by the Responsible Entities."] *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:* *"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."*
Response: Thank you for your comment. Please see response above.		
Entergy Services		Entergy agrees with and supports comments submitted by the SERC OC Standards Review group.
Response: Thank you for your comment.		
ITC		Footnote 1 and the corresponding Threshold For Reporting associated with the first Event in Attachment 1 are not consistent and thus confusing. Qualifying the term BES equipment through a footnote is inappropriate as it leads to this confusion. For instance, does iii under Footnote 1 apply only to BES equipment that meet i and ii or is it applicable to all BES equipment? *The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.*

Organization	Yes or No	Question 4 Comment
		The footnote regarding this event type was expanded to provide additional guidance in: *"Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* The inclusion of equipment failure, operational error and unintentional human action within the threshold of reporting for "destruction" required in the first 3 Events listed in Attachment 1 is also not appropriate. It is clear through operational history that the intent of the equipment applied to the system, the operating practices and personnel training developed/delivered to operate the BES is to result in reliable operation of the BES which has been accomplished exceedingly well given past history. This is vastly different than for intentional actions and should be excluded from the first 3 events listed in Attachment. To the extent these issues are present in another event type they will be captured accordingly. *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* • *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its*

Organization	Yes or No	Question 4 Comment
		Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples. *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* Footnote 1 should be removed and the Threshold for Reporting associated with the first three events in Attachment 1 should be updated only to include intentional human action. This will also result in including all BES equipment that was intentionally damaged in the reporting requirement and not just the small subset qualified by the existing footnote 1. This provides a much better data sample for law enforcement to make assessments from than the smaller subset qualified by what we believe the intent of footnote 1 is. *The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.* *The footnote regarding this event type was expanded to provide additional guidance in:*

Organization	Yes or No	Question 4 Comment
		"Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."
Response: Thank you for your comment. Please see response above.		
APX Power Markets (NCR-11034)		For Attachment 1 and the events titled "Unplanned Control Center evacuation" and "Loss of monitoring or all voice communication capabiliy".RC, BA, and TOP are the only listed entity types listed for reporting responsibility. We are a GOP that offers a SCADA service in several regions and those type of events could result in a loss of situational awareness for the regions we provide services. I believe the requirement for reporting should not be limited to Entity Type, but on their impact for situational awareness to the BES based on the amount of generation they control (specific to our case), or other criteria that would be critical to the BES (i.e. voltage, frequency). *Note that EOP-008-0 is only applicable to Balancing Authorities, Transmission Operators and Reliability Coordinators, this is the basis for the "Entity with reporting Responsibilities" and reads as" "Each RC, BA, TOP that experiences the event".*
Response: Thank you for your comment. Please see response above.		
ACES Power Marketing Standards Collaborators/ Great River Energy		For many of the events listed in Attachment 1, there would be duplicate reporting the way it is written right now. For example, in the case of a fire in a substation (Destruction of BES equipment), the RC, BA, TO, TOP and perhaps the GO and GOP could all experience the event and each would have to report on it. This seems quite excessive and redundant. We recommend eliminating this duplicate reporting. *The DSR SDT has tried to minimize duplicative reporting, but recognizes there may be*

Organization	Yes or No	Question 4 Comment
		events that trigger more than one report. The current applicability ensures an event that could affect just one of the entities with reporting responsibility isn't missed.
Response: Thank you for your comment. Please see response above.		
Intellibind		I do not see that the rewrite of this standard is meeting the goal of clear reliability standards, and in fact the documents are looking more like legal documents. Though the original EOP-004 and CIP-001 was problematic at times, this rewrite, and the need to have such extensive guidance, attachments, and references for EOP-004-2 will create an even more difficult standard to properly meet to ensure compliance during an audit. Though CIP-001 and EOP-004 were related, combining them in a single standard is not resolving the issues, and is in fact complicating the tasks.Requirements in this standard should deal with only one specific issue, not deal with multiple tasks. I am not sure how an auditor will consistently audit against R2, and how a violation will be categorized when an entity implements all portions of their Operating Plan, however fails to fully address all the requirements in R1, thereby not fully implementing R2, in strict interpretation. *The DSR SDT does not agree that the proposed EOP-004-2 "will create an even more difficult standard to properly meet to ensure compliance during an audit". The DSR SDT main concern is the reporting of events per Attachment 1 is in-line with the Purpose of this Standard that states: "To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities." The NERC Reliability Standards are designed to support the reliability of the BES.* *Requirement R2has been updated to read as: ""R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1." Based on comments received.* The drafting team should not set up a situation where an entity is in double jeopardy for missing an element of a requirement.I also suggest that EOP-004-2 be given a

Organization	Yes or No	Question 4 Comment
		new EOP designation rather than calling it a revision. This way implementation can be better controlled, since most companies have written specific CIP-001 and EOP-004 document that will not simple transfer over to the new version. This standard is a drastic departure from the oringial versions. I appreciate the level of work that is going into EOP-004-2, it appears that significant time and effort has been going into the supporting documentation. It is my opinion that if this much material has to be created to state what the standard really requires, then the standard is flawed. When there are 21 pages of explanation for five requirements, especially when we have previously had 16 pages that originally covered 2 separate reliability standards, we need to reevaluate what we are really doing. *The DSR SDT has revised EOP-004 and CIP-001 using the results based standard development process. This process calls for the drafting team to develop documentation regarding its thoughts during the development process. This allows for a more robust standard which contains background material for an entity to have sufficient guidance to show compliance with the standard.*
Response: Thank you for your comment. Please see response above.		
Imperial Irrigation District		IID strongly believes the reporting flowchart should not be part of a standard. The suggestion is to replace it with a more clear, right to the point requirement. *The DSR SDT has discussed this issue and believes it would be too prescriptive to have a flow chart as a requirement. If desired, an entity can have a flow chart as part of the Operating Plan as stated in Requirement 1.*
Response: Thank you for your comment. Please see response above.		
Illinois Municipal Electric Agency		IMEA appreciates this opportunity to comment. IMEA appreciates the SDT's efforts to simplify reporting requirements by combining CIP-001 with EOP-004. [IMEA encourages NERC to continue working towards a one-stop-shop to simplify reporting on ES-ISAC.] IMEA supports, and encourages SDT consideration of, comments

Organization	Yes or No	Question 4 Comment
		submitted by APPA and Florida Municipal Power Agency.
Response: Thank you for your comment. Please see the responses to the other comments that you mention.		
Westar Energy		In Requirement 1.3, the statement "and the following as appropriate" is vague and subject to interpretation. Who determines what is appropriate? We feel it would be better if the SDT would specify for each event, which party should be notified. *Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to report events. Part 1.2 now reads:* *"1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."*
Response: Thank you for your comment. Please see response above.		
South Carolina Electric and Gas		In terms of receiving reports, is it the drafting teams expectation that separate reports be developed by both the RC and the TOP, GO, BA, etc. for an event that occurs on a company's system that is within the RC's footprint? One by the RC and one by the TOP, GO, BA, etc. In terms of meeting reporting thresholds, is it the drafting teams expectation that the RC aggregate events within its RC Area to determine whether a reporting threshold has been met within its area for the quantitative thresholds? *The DSR SDT has tried to minimize duplicative reporting, but recognizes there may be events that trigger more than one report. The current applicability ensures an event*

Organization	Yes or No	Question 4 Comment
		that could affect just one of the entities with reporting responsibility isn't missed. *It is possible for the Applicable Entities within the Reliability Coordinator's area to be part of a JRO/CFR but this is outside the scope of this Project.*
Response: Thank you for your comment. Please see response above.		
Occidental Power Services, Inc. (OPSI)		Load Serving Entities that do not own or operate BES assets should not be included in the Applicability. In current posting, the SDT states that it includes LSEs based on CIP-002; however, if the LSE does not have any BES assets, CIP-002 should also not be applicable, because the LSE could not have any Critical Assets or Critical Cyber Assets. It is understood that the SDT is trying to comply with FERC Order 693, Section 460 and 461; however, Section 461 also states "Further, when addressing such applicability issues, the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate to address these concerns." A qualifier in the Applicability of EOP-004-2 that would include only LSEs that own or operate BES assets would seem appropriate. The proposed CIP-002 Version V has such a qualifier in that it applies to a "Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: o A UFLS program required by a NERC or Regional Reliability Standard o A UVLS program required by a NERC or Regional Reliability Standard"The SDT should consider the same wording in the Applicability section of EOP-004-2 on order to be consistent with what will become the standing version of CIP-002 (Version 5). *The DSR SDT has "considered" section 460 and 461 of FERC Order 693 and has tried to minimize duplicative reporting, but recognizes there may be events that trigger more than one report. The current applicability ensures an event that could affect just one of the entities with reporting responsibility isn't missed.* *The DSR SDT wishes to draw your attention to section 459 of FERC Order 693 which states: " … an adversary may target a small user, owner or operator because it may*

Organization	Yes or No	Question 4 Comment
		have similar equipment or protections as a larger facility, that is, the adversary may use an attack against a smaller facility as a training 'exercise'".
Response: Thank you for your comment. Please see response above.		
American Electric Power		M4: Recommend removing the text "for events" so that it instead reads "The Responsible Entity shall provide evidence that it verified the communication process in its Operating Plan created pursuant to Requirement R1, Part 1.3."R4: It is not clear to what extent the verification needs to be applied if the process used is complex and includes a variety of paths and/or tasks. The draft team may wish to consider changing the wording to simply state "each Responsible Entity shall test each of the communication paths in the operating plan". We also recommend dropping "once per calendar year" as it is inconstant with the measure itself which allows for 15 months. *The DSR SDT has revised R4 (now R3 and the associated measure M3:* *M3. Each Responsible Entity will have dated and time-stamped records to show that the annual test of Part 1.2 was conducted. Such evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other communication documentation. The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. (R3)*
Response: Thank you for your comment. Please see response above.		
Indiana Municipal Power Agency		Many of the items listed in Attachment 1 are onerous and burdensome when it comes to making judgments or determinations. What one may consider "Risk to BES equipment" another person may not make the same determination. Clarity needs to

Organization	Yes or No	Question 4 Comment
		be added to make the events easier to determine and that will result in less issues when it comes to compliance audits. IMPA does not understand the usage of the terms Critical Asset and Critical Cyber Asset as they will be retired with CIP version 5.IMPA believes the data retention requirements are way too complicated and need to be simplified. It seems like it would be less complicated if one data retention period applied to all data associated with this standard. *The DSR has revised many of the events listed in Attachment 1 to provide clarity. We have also removed the references to Critical Asset and Critical Cyber Asset.* On "public appeal", in the threshold, the descriptor "each" should be deleted, e.g., if a single event causes an entity to be short of capacity, do you really want that entity reporting each time they issue an appeal via different types of media, e.g., radio, TV, etc., or for a repeat appeal every several minutes for the same event? *The DSR SDT has updated the Public Appeal event to read as: "Public appeal for load reduction event" based on comments received.*
Response: Thank you for your comment. Please see response above.		
MidAmerican Energy		MidAmerican proposes eliminating the phrase "with no more than 15 months between reviews" from R1.5. While we agree this is best practice, it creates the need to track two conditions for the review, eliminates flexibility for the responsible entity and does not improve security to the Bulk Electric System. There has not been a directive from FERC to specify the definition of annual within the standard itself. In conjunction with this comment, the Violation Severity Levels for R4 should be revised to remove the references to months. *The DSR SDT has removed this phrase from the requirement (now R3).*

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comment. Please see response above.		
Oncor Electric Delivery Company LLC		NERC's Event Analysis Program tends to parallel many of the reporting requirements as outlined in EOP-004 Version 2. Oncor recommends that NERC considers ways of streamlining the reporting process by either incorporating the Event Analysis obligations into EOP-004-2 or reducing the scope of the Event Analysis program as currently designed to consist only of "exception" reporting. *The DSR SDT has reviewed the Event Analysis Programs criteria. The DSR SDT has determined that Attachment 1 covers the minimum reporting requirements.*
Response: Thank you for your comment. Please see response above.		
Compliance & Responsbility Office		NextEra Energy, Inc. (NextEra) appreciates the DSR SDT revising proposed EOP-004-2, based on the previous comments of NextEra and the stakeholders. NextEra, however, believes that EOP-004-2 needs additional refinement prior to approval. R1.3In R1.3, NextEra is concerned that the term “internal company personnel” is unclear and may be misinterpreted. For example, NextEra does not believe this term should include all company or corporate personnel, or even all personnel in the Responsible Entity’s company or business unit. Instead, the definition of personnel should be limited to those who could be directly impacted by the event or are working on the event. Thus, NextEra suggests that the language in R1.3 be revised to read: “Internal Responsible Entity personnel whose tasks require them to take specific actions to mitigate, stop the spread and/or normalize the event, or personnel who are directly impacted by the event.” NextEra is concerned that R1.3, as written, will be interpreted differently from company to company, region to region, auditor to auditor, and, therefore, may result in considerable confusion during actual events as well as during the audits/stop checks of EOP-004-2 compliance.

Organization	Yes or No	Question 4 Comment
		The DSR SDT has written Requirement R1, Part 1.2 in a way to allow the entity to determine who should receive the communication within your company as stated in your Operating Plan. Also, in R1.3, NextEra is concerned that many of the events listed in Attachment A already must be reported to NERC under its trial (soon to be final) Event Analysis Reporting requirements (Event Analysis). NextEra believes duplicative and different reporting requirements in EOP-004-2 and the Event Analysis rules will cause confusion and inefficiencies during an actual event, which will likely be counterproductive to promoting reliability of the bulk power system. Thus, NextEra believes that any event already covered by NERC's Event Analysis should be deleted from Attachment 1. Events already covered include, for example, loss of monitoring or all voice, loss of firm load and loss of generation. If this approach is not acceptable, NextEra proposes, in the alternative, that the reporting requirements between EOP-004-2 and Event Analysis be identical. For instance, in EOP-004-2, there is a requirement to report any loss of firm load lasting for more than 15 minutes, while the Event Analysis only requires reporting the of loss of firm load above 300 megawatts and lasting more than 15 minutes. Similarly, EOP-004-2 requires the reporting of any unplanned control center evacuation, while the Event Analysis only requires reporting after the evacuation of the control center that lasted 30 minutes or more. Thus, NextEra requests that either EOP-004-2 not address events that are already set forth in NERC's Event Analysis, or, in the alternative, for those duplicative events to be reconciled and made identical, so the thresholds set forth in the Event Analysis are also used in EOP-004-2. *The DSR SDT has worked with the EAWG to develop Attachment 1. At one point they matched. The event for loss of load matches and we revised the "unplanned control center evacuation" event to be for 30 minutes or more.* In addition, NextEra believes that a reconciliation between the language "of recognition" in Attachment 1 and "process to identify" in R1.1 is necessary. NextEra prefers that the language in Attachment 1 be revised to read " . . . of the

Organization	Yes or No	Question 4 Comment
		identification of the event under the Responsible Entity's R1.1 process." For instance, the first event under the "Submit Attachment 2 . . . ." column should read: "The parties identified pursuant to R1.3 within 1 hour of the identification of an event under the Responsible Entity's R1.1 process." This change will help eliminate confusion, and will also likely address (and possibly make moot) many of the footnotes and qualifications in Attachment 1, because a Responsible Entity's process will likely require that possible events are properly vetted with subject matter experts and law enforcement, as appropriate, prior to identifying them as "events". Thus, only after any such vetting and a formal identification of an event would the one hour or twenty-four hour reporting clock start to run. R1.4, R1.5, R3 and R4NextEra is concerned with the wording and purpose of R1.4, R1.5, R3 and R4. *The language was revised in Requirement 1, Part 1.1 to "recognize" based on other comments received.* For example, R1.4 requires an update to the Operating Plan for ". . . any change in assets, personnel, other circumstances . . . ." This language is much too broad to understand what is required or its purpose. Further, R1.4 states that the Operating Plan shall be updated for lessons learned pursuant to R3, but R3 does not address lessons learned. Although there may be lessons learned during a post event assessment, there is no requirement to conduct such an assessment. Stepping back, it appears that the proposed EOP-004-2 has a mix of updates, reviews and verifications, and the implication that there will be lessons learned. Given that EOP-004-2 is a reporting Standard, and not an operational Standard, NextEra is not inclined to agree that it needs the same testing and updating requirements like EOP-005 (restoration) or EOP-008 (control centers). Thus, it is NextEra's preference that R1.4, R1.5 and R4 be deleted, and replaced with a new R1.4 as follows:R1.4 A process for ensuring that the Responsibly Entity reviews, and updates, as appropriate its Operating Plan at least annually (once each calendar year) with no more than 15 months between reviews.If the DSR SDT does not agree with this approach, NextEra, in the alternative, proposes a second approach that consolidates R1.4, R1.5 and R4 in a new R1.4 as follows:R1.4 A process for ensuring that the Responsibly Entity tests

Organization	Yes or No	Question 4 Comment
		and reviews its Operating Plan at least annually (once each calendar year) with no more than 15 months between a test and review. Based on the test and review, the Operating Plan shall be updated, as appropriate, within 90 calendar days. If an actual event occurs, the Responsible Entity shall conduct a post event assessment to identify any lessons learned within 90 calendar days of the event. If the Responsible Entity identifies any lessons learned in post event assessment, the lessons learned shall be incorporated in the Operating Plan within 90 calendar days of the date of the final post event assessment. NextEra purposely did not add language regarding "any change in assets, personnel etc," because that language is not sufficiently clear or understandable for purposes of a mandatory requirement. Although it may be argued that it is a best practice to update an Operating Plan for certain changes, unless the DST SDT can articulate specific, concrete and understandable issues that require an updated Operating Plan prior to an annual review, NextEra recommends that the concept be dropped. *Requirement 1, Part 1.4 was merged with Part 1.5 as well as R4. The resulting requirement is now Requirement 3:* *"Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]* Nuclear Specific ConcernsEOP-004-2 identifies the Nuclear Regulatory Commission (NRC) as a stakeholder in the Reporting Process, but does not address the status of reporting to the NRC in the Event Reporting flow diagram on page 9. Is the NRC considered Law Enforcement as is presented in the diagram? Since nuclear stations are under a federal license, some of the events that would trigger local/state law enforcement at non-nuclear facilities would be under federal jurisdiction at a nuclear site. *The process flowchart is an example of how an entity might operate. If an event requires notification of the NRC, this would be an example of notification of a regulatory authority. It is anticipated that the reporting entity would also notify law*

Organization	Yes or No	Question 4 Comment
		enforcement if appropriate. There are some events listed in Attachment 1 that seem redundant or out of place. For example, a forced intrusion is a one hour report to NERC. However, if there is an ongoing forced intrusion at a nuclear power plant, there are many actions taking place, with the NRC Operations Center as the primary contact which will mobilize the local law enforcement agency, etc. *The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "Any physical threat that could impact the operability of a Facility".* It is unclear that reporting to NERC in one hour promotes reliability or the resolution of an emergency in progress. *All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:* *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.* Also, is there an ability to have the NRC in an emergency notify NERC? The same concerns related to cyber security events.Procedures versus PlanNextEra also suggests replacing "Operating Plan" with "procedures". Given that EOP-004-2 is a reporting Standard and not an operational Standard, it is typical for procedures that address this standard to reside in other departments, such as Information Management and Security. In other words, the procedures needed to address the requirements of EOP-004-2 are likely broader than the NERC-defined Operating Plan.

Organization	Yes or No	Question 4 Comment
		Within your Operating Plan you are required to "report" events to the ERO and your RC and communicate this information (to others) as you define it within your company's Operating Plan. This will allow you to customize any events as you see fit. Clean-Up ItemsIn Attachment 1, Control Centers should be capitalized in all columns so as not to be confused with control rooms. *Since "control center" is not a defined term, it has been revised to lower case.* Also, the final product should clearly state that the process flow chart that is set forth before the Standard is for illustrative purposes, so there is no implication that a Registered Entity must implement multiple procedures versus one comprehensive procedure to address different reporting requirements. *The introduction of the flow chart is clearly marked "Example of Reporting Process including Law Enforcement".*
Response: Thank you for your comment. Please see response above.		
PacifiCorp		No comment.
Arizona Public Service Company		No comments
PPL Electric Utilities and PPL Supply Organizations`		Our comments center around the footnotes and events 'Destruction of BES equipment' and 'Loss of Off-site power to a nuclear generating plant'. We request the SDT consider adding a statement to the standard that acknowledges that not all registered entities have visibility to the information in the footnotes. E.G. Destruction of BES equipment. A GO/GOP does not necessarily know if loss of specific BES equipment would affect any IROL and therefore would not be able to consider this criteria in its reporting decision. Loss of BES equipment would be reported to the BA/RC and the BA/RC would know of an IROL impact and the BA/RC

Organization	Yes or No	Question 4 Comment
		is the appropriate entity to report. We request the SDT consider the information in the footnotes for inclusion in the table directly. Consider Event 'Destruction of BES equipment'. Is footnote 1 a scoping statement? Is it part of the threshold? Is it the impact? Is it defining Destruction? If the BES equipment was destroyed by weather and does not affect an IROL, then is no report is needed? Alternatively, do you still apply the threshold and say it was external cause and therefore report? *Several event categories were removed or combined to improve Attachment 1. The footnotes that you mention were removed and included in the threshold for reporting column. If an entity does not experience an event, then they should not report on it. As you suggest, most GO /GOPs do not see the transmission system. It is anticipated that they will report for events on their Facilities.* We suggest including a flowchart on how to use Attachment 1 with an example. The flowchart would explain the order in which to consider the event and the threshold, and footnotes if they remain. Regarding Attachment 1 Footnote 1 'do not report copper theft...unless it degrades the ability of equipment to operate correctly.', is this defining destruction as not operating correctly ? or is the entirety of footnote 1 a definition of destruction? Regarding Attachment 1 Footnote 1, iii, we request this be changed for consistency with the Event and suggest removing damage from the footnote. i.e. The event is 'destruction' whereas the footnote says 'damaged or destroyed'. The standard does not provide guidance on damage vs destruction which could lead to differing reporting conclusions. Is the reporting line out of service, beyond repair, or is it timeframe based? Regarding Attachment 1 Footnote 2 ' to steal copper... unless it affects the reliability of the BES', is affecting the reliability of the BES a consideration in all the events? PPL believes this is the case and request this statement be made. This could be included in the flowchart as a decision point. Regarding Event 'Loss of Off-site power to a nuclear generating plant', the threshold for reporting does not designate if the off-site loss is planned and/or unplanned - or if the reporting threshold includes the loss of one source of off-site power or is the reporting limited to when all off-site sources are unavailable. PPL recommends the event be 'Total unplanned loss of offsite power to a nuclear generating plant (grid

Organization	Yes or No	Question 4 Comment
		supply)'Thank you for considering our comments. *The SDR SDT discussed "Forced Intrusion" as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.* *The footnote regarding this event type was expanded to provide additional guidance in:* *"Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* *The DSR SDT has updated the Requirements based on comments received along with updating Attachment 1 and 2. Please review the updated standard for all your concerns.*
Response: Thank you for your comment. Please see response above.		
City of Austin dba Austin		Overarching Concern related to EOP-004-2 draft:The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes

Organization	Yes or No	Question 4 Comment
Energy		and CIP Standards Version 5 could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definition of a BES element could change significantly and the concepts of "Critical Assets" and "Critical Cyber Assets" no longer exist in Version 5 of the CIP Standards. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Additionally, it is debatable whether the destruction of, for example, one relay would be a reportable incident given the proposed language. Related to "Reportable Events" of Attachment 1:1. The "Purpose" section of the Standard indicates it is designed to require the reporting of events "with the potential to impact reliability" of the BES. Footnote 1 and the "Threshold for Reporting" associated with the Event described as "Destruction of BES equipment" expand the reporting scope beyond that intent. For example, a fan on a generation unit can be destroyed because a plant employee drops a screwdriver into it. We believe such an event should not be reportable under EOP-004-2. Yet, as written, a Responsible Entity could interpret that event as reportable (because it would be "unintentional human action" that destroyed a piece of equipment associated with the BES). If the goal of the SDT was to include such events, we think the draft Standard goes too far in requiring reporting. If the SDT did not intend to include such events, the draft Standard should be revised to make that fact clear. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT*

Organization	Yes or No	Question 4 Comment
		believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. 2. Item iii) in Footnote 1 seems redundant with the Threshold for Reporting.3. The word "Significantly" in item ii) of footnote 1 introduces an element of subjectivity. What is "significant" to one person may not be significant to someone else.4. The word "unintentional" in Item iii) of footnote 1 may introduce nuisance reporting. The SDT should consider: (1) changing the Event description to "Damage or destruction of BES equipment" (2) removing the footnote and (3) replacing the existing "Threshold for Reporting" with the following language:"Initial indication the event: (i) was due to intentional human action, (ii) affects an IROL or (iii) in the opinion of the Responsible Entity, jeopardizes the reliability margin of the system (e.g., results in the need for emergency actions)" *The SDR SDT revised this event to "Damage or destruction of a Facility" and removed the footnote. The threshold for reporting now reads:* *Damage or destruction of a Facility that:* *Affects an IROL (per FAC-014)* *OR* *Results in the need for actions to avoid an Adverse Reliability Impact* *OR* *Results from intentional human action.* 5. One reportable event is "Risk to the BES" and the threshold for reporting is, "From a non-environmental physical threat." This appears to be intended as a catch-all reportable event. Due to the subjectivity of this event description, we suggest removing it from the list. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical*

Organization	Yes or No	Question 4 Comment
		Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds. 6. One reportable event is "Damage or destruction of Critical Asset per CIP-002." The SDT should define the term "Damage" in order for an entity to determine a threshold for what qualifies as "Damage" to a CA. Normal "damage" can occur on a CA that should not be reportable (e.g. the screwdriver example, above). *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* 7. For the event called "BES Emergency requiring public appeal for load reduction," the SDT should make it clear who should report such an event. For example, in the ERCOT Region, there is a requirement that ERCOT issue public appeals for load reduction (See ERCOT Protocols Section 6.5.9.4). As the draft of EOP-004-2 is currently written, every Registered Entity in the ERCOT Region would have to file a report when ERCOT issues such an appeal. Such a requirement is overly burdensome and does not enhance the reliability of the BES. The Standard should require that the Reliability Coordinator file a report when it issues a public appeal to reduce load. *The DSR SDT has tried to minimize duplicative reporting, but recognizes there may be events that trigger more than one report. The current applicability ensures an event that could affect just one of the entities with reporting responsibility isn't missed.* Reporting Thresholds1. See Paragraph 1 in the "Related to 'Reportable Events' of Attachment 1" section, above. 2. We believe damage or destruction of Critical

Organization	Yes or No	Question 4 Comment
		Assets or CCAs resulting from operational error, equipment failure or unintentional human action should not be reportable under this Standard. We recommend changing the thresholds for "Damage or destruction of Critical Asset..." and "Damage or destruction of a [CCA]" to "Initial Indication the event was due to external cause or intentional human action." 3. We support the SDT's attempted to limit nuisance reporting related to copper thefts. However, a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could clog the reporting process with nuisance reporting and reviewing. An example is the "BES Emergency requiring manual firm load shedding" of â‰¥ 100 MW or "Loss of Firm load for â‰¥ 15 Minutes" that is â‰¥ 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases, those low thresholds would require reporting minor wind events or other seasonal system issues on a local network used to provide distribution service. Firm Load1. The use of the term "Firm load" in the context of the draft Standard seems inappropriate. "Firm load" is not defined in the NERC Glossary (although "Firm Demand" is defined). If the SDT intended to use "Firm Demand," they should revise the draft Standard to use that language. If the SDT wishes to use the term "Firm load" they should define it. [For example, we understand that some load agrees to be dropped in an emergency. In fact, in the ERCOT Region, we have a paid service referred to as "Emergency Interruptible Load Service" (EILS). If the SDT intends that "Firm load" means load other than load which has agreed to be dropped, it should make that fact clear.] *The thresholds and events listed in Attachment 1 are currently required under DOE OE-417 and NERC reporting requirements.* Comments to Attachment 21. The checkbox for "fuel supply emergency" should be deleted because it is not listed as an Event on Attachment 1. *The DSR SDT has removed both "fuel supply emergency" and "other" from Attachment 2.*

Organization	Yes or No	Question 4 Comment
		2. There should be separation between "forced intrusion" and "Risk to BES equipment." They are separate Events on Attachment 1. *Several stakeholders expressed concerns relating to the "Forced Intrusion" event. Their concerns related to ambiguous language in the footnote. The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.* Comments to Guideline and Technical BasisThe last paragraph appears to state NERC will accept an OE-417 form as long as it contains all of the information required by the NERC form and goes on to state the DOE form "may be included or attached to the NERC report." If the intent is for NERC to accept the OE-417 in lieu of the NERC report, this paragraph should be clarified. *The DSR SDT received many comments requesting consistency with DOE OE-417 thresholds and timelines. These items as well as the Events Analysis Working Group's (EAWG) requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across*

Organization	Yes or No	Question 4 Comment
		North America • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use the OE-417 form rather than Attachment 2 to report under EOP-004. The SDT was informed by the DOE of its new online process coming later this year. In this process, entities may be able to record email addresses associated with their Operating Plan so that when the report is submitted to DOE, it will automatically be forwarded to the posted email addresses, thereby eliminating some administrative burden to forward the report to multiple organizations and agencies.*
Response: Thank you for your comment. Please see response above.		
Salt River Project/ Lower Colorado River Authority		Overarching Concern related to EOP-004-2 draft:The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes and CIP Standards Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definition of a BES element could change significantly and the concepts of "Critical Assets" and "Critical Cyber Assets" no longer exist in Version 5 of the CIP Standards. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Additionally, it is debatable whether the destruction of, for example, one relay would

Organization	Yes or No	Question 4 Comment
		be a reportable incident given the proposed language. Related to "Reportable Events" of Attachment 1:1. The "Purpose" section of the Standard indicates it is designed to require the reporting of events "with the potential to impact reliability" of the BES. Footnote 1 and the "Threshold for Reporting" associated with the Event described as "Destruction of BES equipment" expand the reporting scope beyond that intent. For example, a fan on a generation unit can be destroyed because a plant employee drops a screwdriver into it. We believe such an event should not be reportable under EOP-004-2. Yet, as written, a Responsible Entity could interpret that event as reportable (because it would be "unintentional human action" that destroyed a piece of equipment associated with the BES). If the goal of the SDT was to include such events, we think the draft Standard goes too far in requiring reporting. If the SDT did not intend to include such events, the draft Standard should be revised to make that fact clear. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred.* 2. Item iii) in Footnote 1 seems redundant with the Threshold for Reporting.3. The word "Significantly" in item ii) of footnote 1 introduces an element of subjectivity. What is "significant" to one person may not be significant to someone else.4. The word "unintentional" in Item iii) of footnote 1 may introduce nuisance reporting. The SDT should consider: (1) changing the Event description to "Damage or destruction of BES equipment" (2) removing the footnote and (3) replacing the

Organization	Yes or No	Question 4 Comment
		existing "Threshold for Reporting" with the following language:"Initial indication the event: (i) was due to intentional human action, (ii) affects an IROL or (iii) in the opinion of the Responsible Entity, jeopardizes the reliability margin of the system (e.g., results in the need for emergency actions)" *The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.* *The footnote regarding this event type was expanded to provide additional guidance in:* *"Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* 5. One reportable event is, "Risk to the BES" and the threshold for reporting is, "From a non-environmental physical threat." This appears to be intended as a catch-all reportable event. Due to the subjectivity of this event description, we suggest removing it from the list. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical*

Organization	Yes or No	Question 4 Comment
		Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds. 6. One reportable event is, "Damage or destruction of Critical Asset per CIP-002." The SDT should define the term "Damage" in order for an entity to determine a threshold for what qualifies as "Damage" to a CA. Normal "damage" can occur on a CA that should not be reportable (e.g. the screwdriver example, above). Reporting Thresholds1. We believe damage or destruction of Critical Assets or CCAs resulting from operational error, equipment failure or unintentional human action should not be reportable under this Standard. We recommend changing the thresholds for "Damage or destruction to Critical Assets ..." and "Damage or destruction of a [CCA]" to "Initial Indication the event was due to external cause or intentional human action." *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* 2. We support the SDT's attempted to limit nuisance reporting related to copper thefts. However, a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could clog the reporting process with nuisance reporting and reviewing. An example is the "BES Emergency requiring manual firm load shedding" of â‰¥ 100 MW or "Loss of Firm load for â‰¥ 15 Minutes" that is â‰¥ 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases, those low thresholds would require reporting minor wind events or other seasonal system issues on a local network used to provide distribution service. Firm Demand1. The use of the term "Firm load" in the context of the draft Standard seems inappropriate.

Organization	Yes or No	Question 4 Comment
		"Firm load" is not defined in the NERC Glossary (although "Firm Demand" is defined). If the SDT intended to use "Firm Demand," they should revised the draft Standard. If the SDT wishes to use the term "Firm load" they should define it. [For example, we understand that some load agrees to be dropped in an emergency. In fact, in the ERCOT Region, we have a paid service referred to as "Emergency Interruptible Load Service" (EILS). If the SDT intends that "Firm load" means load other than load which has agreed to be dropped, it should make that fact clear.] *The thresholds and event types in Attachment 1 are from current DOE OE-417 and NERC reporting requirements.* Comments to Attachment 21. The checkbox for "fuel supply emergency" should be deleted because it is not listed as an Event on Attachment 1. *The DSR SDT has removed both "fuel supply emergency" and "other" from Attachment 2.* 2. There should be separation between "forced intrusion" and "Risk to BES equipment." They are separate Events on Attachment 1. *Several stakeholders expressed concerns relating to the "Forced Intrusion" event. Their concerns related to ambiguous language in the footnote. The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events*

Organization	Yes or No	Question 4 Comment
		meaningful to industry awareness are reported. Comments to Guideline and Technical BasisThe last paragraph appears to state NERC will accept an OE-417 form as long as it contains all of the information required by the NERC form and goes on to state the DOE form "may be included or attached to the NERC report." If the intent is for NERC to accept the OE-417 in lieu of the NERC report, this paragraph should be clarified. *The DSR SDT received many comments requesting consistency with DOE OE-417 thresholds and timelines. These items as well as the Events Analysis Working Group's (EAWG) requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use the OE-417 form rather than Attachment 2 to report under EOP-004. The SDT was informed by the DOE of its new online process coming later this year. In this process, entities may be able to record email addresses associated with their Operating Plan so that when the report is submitted to DOE, it will automatically be forwarded to the posted email addresses, thereby eliminating some administrative burden to forward the report to multiple organizations and agencies.*

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comment. Please see response above.		
Public Utility District No. 1 of Snohomish County/Seattle City Light		Overarching Concern related to EOP-004-2 draft:The contemporaneous drafting efforts related to both the proposed Bulk Electric System ("BES") definition changes, as well as the CIP standards Version 5, could significantly impact the EOP-004-2 reporting requirements. Caution needs to be exercised when referencing these definitions, as the definitions of a BES element could change significantly and Critical Assets may no longer exist. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* As it relates to the proposed reporting criteria, it is debatable as to whether or not the destruction of, for example, one relay would be a reportable incident under this definition going forward given the current drafting team efforts. Related to "Reportable Events" of Attachment 1:1. A reportable event is stated as, "Risk to the BES", the threshold for reporting is, "From a non-environmental physical threat". This appears to be a catch-all event, and basically every other event in Attachment 1 should be reported because it is a risk to the BES. Due to the subjectivity of this event, suggest removing it from the list. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that*

Organization	Yes or No	Question 4 Comment
		events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. 2. A reportable event is stated as, "Damage or destruction of Critical Asset per CIP-002". The term "Damage" would have to be defined in order for an entity to determine a threshold for what qualifies as "Damage" to a CA. One could argue that normal "Damage" can occur on a CA that is not necessary to report. There should also be caution here in adding CIP interpretation within this standard. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Reporting Thresholds1. The SDT made attempts to limit nuisance reporting related to copper thefts and so on which is supported. However a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could congest the reporting process with nuisance reporting and reviewing. An example is the "BES Emergency requiring manual firm load shedding of greater than or equal to 100 MW or the Loss of Firm load for â‰¥ 15 Minutes that is greater than or equal to 200 MW (300 MW if the manual demand is greater than 3000 MW). In many cases these low thresholds represent reporting of minor wind events or other seasonal system issues on Local Network used to provide distribution service. Firm Demand1. The use of Firm Demand in the context of the draft Standards could be used to describe commercial arrangements with a customer rather than a reliability issue. Clarification of Firm Demand would be helpful *The DSR SDT has updated the requirements based on comments received along with updating Attachment 1 and 2. Please review the updated standard for all your*

Organization	Yes or No	Question 4 Comment
		concerns.
Response: Thank you for your comment. Please see response above.		
Pacific Northwest Small Public Power Utility Comment Group		Project 2008-06 proposes to withdraw the terms "Critical Asset" and "Critical Cyber Asset" from the NERC Glossary. In order to avoid a reliability gap when this occurs, we propose including High and Medium Impact BES Cyber Systems and Assets. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* The revised wording to add, "as appropriate" to R1.3 is a concern. We understand the SDT's intent to not require all the bulleted parties to be notified for every event type. But will a good faith effort on the part of the registered entity to deem appropriateness be subject to second guessing and possible sanctions by the Compliance Enforcement Authority if they disagree? We note that CIP-001 required an interpretation to address this issue, but cannot assume that interpretation will carry over. We suggest spelling out exactly who shall deem appropriateness. *The phrase "as appropriate" was removed and Requirement 1, Part 1.2 was revised to:* *A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.* R4 continues to be an onerous requirement for smaller entities. Verification was not

Organization	Yes or No	Question 4 Comment
		part of the SAR and we are not convinced it is needed for reliability. We are unsure how a DP with no generation, no BES assets, no Critical Cyber Assets, and less than 100 MW of load; would meet R4. Shall they drill for impossible events? We ask that R4 be removed. At a minimum it should exclude entities that cannot experience the events of Attachment 1.Entities that cannot experience the events of Attachment 1should likewise be exempt from R1.2, 1.3, R2, and R3. *Requirement R4 (now R3) was revised to :* *Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.* *Requirement R1, Part 1.1 specifies that an entity must have a process for recognizing "applicable events". An entity is only required to have the Operating Plan as it relates to events applicable to that entity. The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. This language does not preclude the verification of contact information taking place during a training event. The DSR SDT has updated the Requirements based on comments received along with updating Attachment 1 and 2. Please review the updated Standard for all your concerns.*
Response: Thank you for your comment. Please see response above.		
Clallam County PUD No.1		Project 2008-06 proposes to withdraw the terms "Critical Asset" and "Critical Cyber Asset" from the NERC Glossary. In order to avoid a reliability gap when this occurs,

Organization	Yes or No	Question 4 Comment
		we propose including High and Medium Impact BES Cyber Systems and Assets. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* The revised wording to add, "as appropriate" to R1.3 is a concern. We understand the SDT's intent to not require all the bulleted parties to be notified for every event type. But will a good faith effort on the part of the registered entity to deem appropriateness be subject to second guessing and possible sanctions by the Compliance Enforcement Authority if they disagree? We note that CIP-001 required an interpretation to address this issue, but cannot assume that interpretation will carry over. We suggest spelling out exactly who shall deem appropriateness. Part 1.3 (now Part 1.2 was revised to: 1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies. R4 continues to be an onerous requirement for smaller entities. Verification was not part of the SAR and we are not convinced it is needed for reliability. We are unsure how a DP with no generation, no BES assets, no Critical Cyber Assets, and less than 100 MW of load; would meet R4. Shall they drill for impossible events? We ask that R4 be removed. At a minimum it should exclude entities that cannot experience the events of Attachment 1. Entities that cannot experience the events of Attachment 1should likewise be exempt from R1.2, 1.3, R2, and R3. *Part 1.1 has been revised to include "applicable events listed in EOP-004, Attachment*

Organization	Yes or No	Question 4 Comment
		1." If an entity cannot experience an event, then it would not be an applicable event. *Requirement R4 (now R3) has been revised to:* *R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]* *The DSR SDT envisions that the testing under R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. This language does not preclude the verification of contact information taking place during a training event.*
Response: Thank you for your comment. Please see response above.		
FEUS		R4 requires verification through a drill or exercise the communication process created as part of R1.3. Clarification of what a drill or exercise should be considered. In order to show compliance to R4 would the entity have to send a pseudo event report to Internal Personnel, the Regional Entity, NERC ES-ISAC, Law Enforcement, and Governmental or provincial agencies listed in R1.3 to verify the communications plan? It would not be a burden on the entity so much, however, I'm not sure the external parties want to be the recipient of approximately 2000 psuedo event reports annually. *Requirement R4 (now R3) related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. Requirement R1, R3 now reads: "Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2."The DSR SDT envisions that the testing under Requirement 3 will include*

Organization	Yes or No	Question 4 Comment
		verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. This language does not preclude the verification of contact information taking place during a training event. Attachment 1: BES equipment is too vague - consider changing to BES facility and including that reduces the reliability of the BES in the footnote. Is the footnote an and or an or?Attachment 1: Version 5 of CIP Requirements remove the terms Critical Asset and Critical Cyber Asset. The drafting team should consider revising the table to include BES Cyber Systems. Clarify if Damage or Destruction is physical damage (aka - cyber incidents would be part of CIP-008.) *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* Attachment 1: Unplanned Control Center evacuation - remove "potential" from the reporting responsibility *The DSR SDT has removed both "fuel supply emergency" and "other" from Attachment 2.* Attachment 2 - 3: change to, "Did the event originate in your system?" The requirement only requires reporting for Events - not potential events. *The DSR SDT has streamlined Attachment 2, per comments received.*

Organization	Yes or No	Question 4 Comment
		Attachment 2 4: “Damage or Destruction to BES equipment” should be “Destruction of BES Equipment” like it is in Attachment 1 and “forced intrusion risk to BES equipment” remove “risk” *The DSR SDT has streamlined Attachment 2 to reflect the events of Attachment 1, per comments received.*
Response: Thank you for your comment. Please see response above.		
ReliabilityFirst		ReliabilityFirst thanks the SDT for their effort on this project. ReliabilityFirst has a number of concerns/questions related to the draft EOP-004-2 standard which include the following:1. General Comment - The SDT should consider any possible impacts that could arise related to the applicability of Generator Owners that may or may not own transmission facilities. This will help alleviate any potential or unforeseen impacts on these Generator Owners *The DSR SDT cannot apply items such as GO/TO issues when NERC and the Regions are not in agreement to what the issue and solution is.* 2. General Comment - Though the rationale boxes contain useful editorial information for each requirement, they should rather contain the technical rationale or answer the question “why is this needed” for each requirement. The rationale boxes currently seem to contain suggestions on how to meet the requirements. ReliabilityFirst suggests possibly moving some of the statements in the “Guideline and Technical Basis” into the rationale boxes, as some of the rationale seems to be contained in that section. *The DSR SDT will continue to update rationale boxes per comments received.* 3. General comment - The end of Measure M4 is incorrectly pointing to R3. This should refer to R4. *Measurement 4 has been corrected.* 4. General Comment - ReliabilityFirst recommends the “Reporting Hierarchy for

Organization	Yes or No	Question 4 Comment
		Reportable Events" flowchart should be removed from the "Background" section and put into an appendix. ReliabilityFirst believes the flowchart is not really background information, but an outline of the proposed process found in the new standard. *The DSR SDT provided a flow chart for stakeholders to use if desired. EOP-004-2 sets a minimum level of reporting per the events described in Attachment 1. The DSR SDT has received negative feedback in past drafts, the DSR SDT was too prescriptive.* 5. Applicability Comment - ReliabilityFirst questions the newly added applicability for both the Regional Entity (RE) and ERO. Standards, as outlined in many, if not all, the FERC Orders, should have applicability to users, owners and operators of the BES and not to the compliance monitoring entities (e.g. RE and ERO). Any requirements regarding event reporting for the RE and ERO should be dealt with in the NERC Rules of Procedure and/or Regional Delegation Agreements. It is also unclear who would enforce compliance on the ERO if the ERO remains an applicable entity. *The ERO is an Applicable Entity under the current version of CIP-008 and therefore they are held to EOP-004-2. Note, this proposed Standard has been through two Quality Reviews and there has been no rejection from NERC .* 6. Requirement Comment - ReliabilityFirst believes the process for communicating events in Requirement R1, Part 1.3 should be all inclusive and therefore include the bullet points. Bullet points are considered to be "OR" statements and thus ReliabilityFirst believes they should be characterized as sub-parts. Listed below is an example:1.3. A process for communicating events listed in Attachment 1 to the following:1.3.1 Electric Reliability Organization, 1.3.2 Responsible Entity's Reliability Coordinator 1.3.3 Internal company personnel 1.3.4 The Responsible Entity's Regional Entity 1.3.5 Law enforcement 1.3.6 Governmental or provincial agencies *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. Requirement R3 now reads: "Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in*

Organization	Yes or No	Question 4 Comment
		Part 1.2. ". The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. 7. Requirement Comment - ReliabilityFirst questions why Requirement R1, Part 1.1 and Part 1.2 are not required to be verified when performing a drill or exercise in Requirement R4? ReliabilityFirst believes that performing a drill or exercise utilizing the process for identifying events (Part 1.1) and the process for gathering information (Part 1.2) are needed along with the verification of the process for communicating events as listed in Part 1.3. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. Requirement R3 now reads: "Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. ". The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* 8. Compliance Section Comment - Section 1.1 states "If the Responsible Entity works for the Regional Entity..." and ReliabilityFirst questions the intent of this language. ReliabilityFirst is unaware of any Responsible Entities who work for a Regional Entity. Also, if the Regional Entity and ERO remain as applicable entities, in Section 1.1 of

Organization	Yes or No	Question 4 Comment
		the standard, it is unclear who will act as the Compliance Enforcement Authority (CEA). *The DSR SDT has followed the guidance in the Standards Development process to assure that "template" information is correct. The language included is directly from NERC guideline documents* 9. Compliance Section Comment - ReliabilityFirst recommends removing the second, third and fourth paragraphs from Section 1.2 since ReliabilityFirst believes entities should retain evidence for the entire time period since their last audit. *The DSR SDT has followed the guidance in the Standards Development process to assure that "template" information is correct. The language included is directly from NERC guideline documents* 10. Compliance Section Comment - ReliabilityFirst recommends modifying the fifth paragraph from Section 1.2 as follows: "If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or until a data hold release is issued by the CEA." ReliabilityFirst believes, as currently stated, the CEA would be required to retain information for an indefinite period of time. *The DSR SDT has followed the guidance in the Standards Development process to assure that "template" information is correct. The language included is directly from NERC guideline documents.* 11. Compliance Section Comment - ReliabilityFirst recommends removing the sixth paragraph from Section 1.2 since the requirement for the CEA to keep the last audit records and all requested and submitted subsequent audit records is already covered in the NERC ROP. *The DSR SDT has followed the guidance in the Standards Development process to assure that "template" information is correct. The language included is directly from*

Organization	Yes or No	Question 4 Comment
		NERC guideline documents 12. Attachment 1 Comment - It is unclear what the term/acronym "Tv" is referring to. It may be beneficial to include a footnote clarifying what the term "Tv" stands for. *Tv is based on FAC-010 and the DSR SDT believes that this is clear to affected stakeholders.* 13. VSL General Comment - although ReliabilityFirst believes that the applicability is not appropriate, as the REs and ERO are not users, owners, or operators of the Bulk Electric System, the Regional Entity and ERO are missing from all four sets of VSLs, if the applicability as currently written stays as is. If the Regional Entity and ERO are subject to compliance for all four requirements, they need to be included in the VSLs as well. Furthermore, for consistency with other standards, each VSL should begin with the phrase "The Responsible Entity..." *The DSR SDT will follow the guidance in the Standards Development process to assure that "template" information is correct.* 14. VSL 4 Comment - The second "OR" statement under the "Lower" VSL should be removed. By not verifying the communication process in its Operating Plan within the calendar year, the responsible entity completely missed the intent of the requirement and is already covered under the "Severe" VSL category. *The DSR SDT will follow the guidance in the Standards Development process to assure that "template" information is correct.*
Response: Thank you for your comment. Please see response above.		
Northeast Power Coordinating		Requirement 4 does not specifically state the details necessary for an entity to

Organization	Yes or No	Question 4 Comment
Council		achieve compliance. Requirement 4 should provide more guidance as to what is required in a drill. Audit/enforcement of any requirement language that is too broad will potentially lead to Regional interpretation, inconsistency, and additional CANs.R4 should be revised to delete the 15 month requirement. CAN-0010 recognizes that entities may determine the definition of annual.The standard is too specific, and drills down into entity practices, when the results are all that should be looked for.The standard is requiring multiple reports. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. Requirement R3 now reads: "Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. ". The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.* The Purpose of the Standard is very broad and should be revised because some of the events being reported on have no impact on the BES. Revise Purpose wording as follows: To improve industry awareness and the reliability of the Bulk Electric System "by requiring the reporting of major system events with the potential to impact reliability and their causes..." on the Bulk Electric System it can be said that every event occurring on the Bulk Electric System would have to be reported. *The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability". The Purpose statement now reads:* *"To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."*

Organization	Yes or No	Question 4 Comment
		Referring to Requirement R4, the testing of the communication process is the responsibility of the Responsible Entity. There is an event analysis process already in place.The standard prescribes different sets of criteria, and forms.There should be one recipient of event information. That recipient should be a "clearinghouse" to ensure the proper dissemination of information. *EOP-004 is a standard that requires reporting of events to the ERO. The events analysis program receives these reports and determines whether further analysis is appropriate.* Why is this standard applicable to the ERO? *NERC as the ERO is currently a Responsible Entity under CIP-008, and therefore the proposed EOP-004-2 has the ERO as a Responsible Entity.* Requirement R2 is not necessary. It states the obvious.Requirements R2 and R3 are redundant.The standard mentions collecting information for Attachment 2, but nowhere does it state what to do with Attachment 2. *Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to:* *"Requirement R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."*

Organization	Yes or No	Question 4 Comment
		None of the key concepts identified on page 5 of the standard are clearly stated or described in the requirements: o Develop a single form to report disturbances and events that threaten the reliability of the bulk electric system. *OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.* o Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements. o Establish clear criteria for reporting. o Establish consistent reporting timelines. *The DSR SDT does allow entities to use the DOE Form OE 417 in lieu of Attachment 2 to report an event. Attachment 1 has been updated to provide consistent criteria for reporting as well as reporting timelines. All one hour reporting timelines have been changed to 24 hours with the exception of a 'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673:*

Organization	Yes or No	Question 4 Comment
		"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..." *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.* o Provide clarity for who will receive the information and how it will be used. The standard's requirements should be reviewed with an eye for deleting those that are redundant, or do not address the Purpose or intent of the standard. *Requirement R1 has been updated and now reads as"* *Each Responsible Entity shall have an Operating Plan that includes:* *1.1. A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies.* *The Applicable Entity's Operating Plan is to contain the process for reporting events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and for communicating to others as defined in the Responsible Entity's Operating Plan. All events in Attachment 1 are required to be reported to the Electric Reliability Organization and the Responsible Entity's Reliability Coordinator. The Operating Plan may include: internal company personnel, your Regional Entity, law enforcement, and governmental or provisional agencies, as you identify within your Operating Plan. This gives you the flexibility to tailor your Operating Plan to fit your*

Organization	Yes or No	Question 4 Comment
		company's needs and wants.
Response: Thank you for your comment. Please see response above.		
American Public Power Association		Requirement R1:1.3. A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate: o Internal company personnel o The Responsible Entity's Regional Entity o Law enforcement o Governmental or provincial agencies APPA believes that including the list of other entities needing to be included in a process for communicating events under 1.3 may open this requirement up for interpretation. APPA requests that the SDT remove from the requirement the listing of; "Internal company personnel, The Responsible Entity's Regional Entity, Law enforcement & Governmental or provincial agencies" and include these references in a guidance document. The registered entities need to communicate with the ERO and the RC if applicable for compliance with this standard and to maintain the reliability of the BES. Communication with other entities such as internal company personnel, law enforcement and the Regional Entity are expected, but do not impact the reliability of the BES. This will simplify the reporting structure and will not be burdensome to registered entities when documenting compliance. If this is not an acceptable solution, APPA suggests revising 1.3 to remove the wording "the following as appropriate" and add "other entities as determined by the Responsible Entity. Examples of other entities may include, but are not limited to:" Then it is clear that the list is examples and should not be enforced by the auditor. *Requirement R1 has been updated and now reads as* *"Each Responsible Entity shall have an Operating Plan that includes:* *1.1. A process for recognizing each of the events listed in EOP-004 Attachment 1.* *1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004*

Organization	Yes or No	Question 4 Comment
		Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies. *The Applicable Entity's Operating Plan is to contain the process for reporting events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and for communicating to others as defined in the Responsible Entity's Operating Plan. All events in Attachment 1 are required to be reported to the Electric Reliability Organization and the Responsible Entity's Reliability Coordinator. The Operating Plan may include: internal company personnel, your Regional Entity, law enforcement, and governmental or provisional agencies, as you identify within your Operating Plan. This gives you the flexibility to tailor your Operating Plan to fit your company's needs and wants.* 1.4. Provision(s) for updating the Operating Plan within 90 calendar days of any change in assets, personnel, other circumstances that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3. APPA understands that the SDT is following the FERC order requiring a 90 day limit on updates to any changes to the plan. However, APPA believes that "updating the Operating Plan within 90 calendar days of any change..." is a very burdensome compliance documentation requirement. APPA reminds the SDT that including DPs in this combined standard has increased the number of small Responsible Entities that will be required to document compliance. APPA requests that the SDT combine requirement 1.4 and 1.5 so the Operating Plan will be reviewed and updated with any changes on a yearly basis. If this is not an acceptable solution, APPA suggests that the "Lower VSL" exclude a violation to 1.4. The thought being, a violation of 1.4 by itself is a documentation error and should not be levied a penalty. *Requirement 1, Part 1.4 has been removed from the standard.* Attachment 1: Events TableAPPA believes that the intent of the SDT was to mirror the DOE OE-417 criteria in reporting requirements. With the inclusion of DP in the

Organization	Yes or No	Question 4 Comment
		Applicability, however, APPA believes the SDT created an unintended excessive reporting requirement for DPs during insignificant events. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.* APPA recommends that a qualifier be added to the events table. In DOE OE-417 local electrical systems with less than 300MW are excluded from reporting certain events since they are not significant to the BES. APPA believes that the benefit of reporting certain events on systems below this value would not outweigh the compliance burden placed on these small systems. Therefore, APPA requests that the standard drafting team add the following qualifier to the Events Table of Attachment 1: "For systems with greater than 300MW peak load." This statement should be placed in the Threshold for Reporting column for the following Events: BES Emergency requiring appeal for load reduction, BES

Organization	Yes or No	Question 4 Comment
		Emergency requiring system-wide voltage reduction, BES Emergency requiring manual firm load shedding, BES Emergency resulting in automatic firm load shedding. This will match the DOE OE-417 reporting criteria and relieve the burden on small entities. *Upon review of the DOE OE 417, it states "Local Utilities in Alaska, Hawaii, Puerto Rico, the U.S. Virgin Islands, and the U.S. Territories - If the local electrical system is less than 300 MW, then only file if criteria 1, 2, 3 or 4 are met". Please be advised this exception applies to entities outside the continental USA.* *The DSR SDT has tried to minimize duplicative reporting, but recognizes there may be events that trigger more than one report. The current applicability ensures an event that could affect just one of the entities with reporting responsibility isn't missed.* Definition of "Risk to BES equipment":The SDT attempted to give examples of the Event category "Risk to BES equipment" in a footnote. This footnote gives the Responsible Entity and the Auditor a lot of room for interpretation. APPA suggests that the SDT either define this term or give a triggering mechanism that the industry would understand. One suggestion would be "Risk to BES equipment: An event that forces a Facility Owner to initiate an unplanned, non-standard or conservative operating procedure." Then list; "Examples include train derailment adjacent to BES Facilities that either could have damaged the equipment directly or has the potential to damage the equipment..." This will allow the entity to have an operating procedure linked to the event. If this suggestion is taken by the SDT then the Reporting column of Attachment 1 needs to be changed to: "The parties identified pursuant to R1.3 within 1 hour of initiating conservative operating procedures." *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and*

Organization	Yes or No	Question 4 Comment
		determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.
Response: Thank you for your comment. Please see response above.		
Western Electricity Coordinating Council		Results-based standards should include, within each requirement, the purpose or reason for the requirement. The requirements of this standard, while we support the requirements, do not include the goal or proupose of meeting each stated requirement. The Measures all include language stating "the responsible entity shall provide...". During a quality review of a WECC Regional Reliability Standard we were told that the "shall provide" language is essentially another requirement to provide something. If it is truly necessary to provide this it should be in the requirements. It was suggested to us that we drop the "shall provide" language and just start each Measure with the "Evidence may include but is not limited to...". *The DSR SDT changed each instance of "shall" to "will" within the measures. We will defer to NERC Quality Review comments for any additional revisions.*
Response: Thank you for your comment. Please see response above.		
Sacramento Municipal Utility District (SMUD)		SMUD and BANC agree with the revised language in EOP-004-1 requirements, but we have identified the following issues in A-1:We commend the SDT for properly addressing the sabotage issue. However, additional confusion is caused by introducing term "damage". As "damage" is not a defined term it would be beneficial for the drafting team to provide clarification for what is meant by "damage".

Organization	Yes or No	Question 4 Comment
		The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows: • *The 'Damage or Destruction' event category has been revised to say ' to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* • *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.* *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* *As discussed in prior comment forms, the DSR SDT has elected not to define "sabotage". As defined in an Entity's operating Plan, the requirement is to report and communicate an event as listed in Attachment 1. EOP-004-2 does not require analysis of any event listed in Attachment 1.* The threshold for reporting "Each public Appeal for load reduction" should clearly state the triggering is for the BES Emergency as routine "public appeal" for conservation could be considered a threshold for the report triggering. *To clarify your point, the threshold has been changed to 'Public appeal or load reduction event'.*

Organization	Yes or No	Question 4 Comment
		Regarding the SOL Violations in Attachment 1 the SOL Violations should only be those that affect the WECC paths. *The DSR SDT has included the following language for WECC's SOL violation in Attachment 1:* *"IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only)"* The SDT made attempts to limit nuisance reporting related to copper thefts and so on which is supported. However a number of the thresholds identified in EOP-004-2 Attachment 1 are very low and could congest the reporting process with nuisance reporting and reviewing. *The DSR SDT made reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary.*
Response: Thank you for your comment. Please see response above.		
Southern Comnpany		Southern has the following comments:(1) In Requirement R1.4, we request the SDT to clarify what is meant by the term "assets"? *The DSR SDT has deleted Requirement R1, Part 1.4, thus "assets" is not contained in EOP-004-2 based on comments received.* 2) If requirement 4 is not deleted, should we have to test every possible event described in our Operating Plan or each event listed in Attachment 1 to verify communications? *The DSR SDT has deleted Requirement R4 based on comments received.* (3) In the last paragraph of the "Summary of Key Concepts" section on page 6 of

Organization	Yes or No	Question 4 Comment
		Draft 3, there is a statement that "Real-time reporting is achieved through the RCIS..." The only reporting required on RCIS by the Standards is for EEAs and TLRs. Please review and modify this language as needed. *The DSR SDT believes "The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting" is correct.* (4) Evidence Retention (page 12 of Draft 3): The 3 calendar year reference has no bearing on a Standard that may be audited on a cycle greater than 3 years. *The DSR SDT has updated the Evidence Retention section with standard language provided by NERC staff.* (5) In the NOTE for Attachment 1 (page 20 of Draft 3), what is meant by "periodic verbal updates" and to whom should the updates be made? *The DSR SDT has updated the note in question to remove the language of "periodic verbal updates", it now reads as:* *"NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per R1 and provide as much information as is available at the time of the notification. Reports to the ERO should be submitted to one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422."* (6) There are Prerequisite Approvals listed in the Implementation Plan. Is it appropriate to ask industry to vote on this Standard Revision that has a prerequisite approval of changes in the Rules of Procedure that have not been approved? *The proposed revisions to the Rules of Procedure should have been posted with the*

Organization	Yes or No	Question 4 Comment
		standard. This posting will occur with the successive ballot of EOP-004-2. (7) We believe the reporting of the events in Attachment 1 has no reliability benefit to the Bulk Electric System. We suggest that Attachment 1 should be removed. *The DSR SDT disagrees with this comment. Attachment 1 is the minimum set of events that will be required to report and communicate per your Operating Plan will be aware of system conditions.*
Response: Thank you for your comment. Please see response above.		
Texas Reliability Entity		Substantive comments:1.ERO and Regional Entities should not be included in the Applicability of this standard. Just because they may be subject to some CIP requirements does not mean they also have to be included here. The ERO and Regional Entities do not operate equipment or systems that are integral to the operation of the BES. Also, none of the VSLs apply to the ERO or to Regional Entities. *The DSR SDT is following guidance that NERC has provided to the DSR SDT. The ERO and the RE are applicable entities under CIP-008. Reporting of Cyber Security Incidents is the responsibility of the ERO and the RE.* 2.The first entry in the Events Table should say "Damage or destruction of BES equipment." Equipment may be rendered inoperable without being "destroyed," and entities should not have to determine within one hour whether damage is sufficient to cause the equipment to be considered "destroyed." Footnote 1 refers to equipment that is "damaged or destroyed." *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity.* *The DSR SDT used the defined term "Facility" to add clarity for several events listed in*

Organization	Yes or No	Question 4 Comment
		Attachment 1. A Facility is defined as: *"A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"* *The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.* 3.In the Events Table, consider whether the item for "Voltage deviations on BES facilities" should also be applicable to GOPs, because a loss of voltage control at a generator (e.g. failure of an automatic voltage regulator and power system stabilizer) could have a similar impact on the BES as other reportable items. *The DSR SDT disagrees with this comment. Attachment 1 is the minimum set of events that will be required to report and communicate per your Operating Plan will be aware of system conditions.* 4.In the Events Table, under Transmission Loss, does this item require that at least three Facilities owned by one entity must be lost to trigger the reporting requirement, or is the reporting requirement also to be triggered by loss of three Facilities during one event or occurrence that are owned by two or three different entities? *The DSR SDT has stated in Attachment 1 that "Each TOP that experiences the transmission loss". This would mean per individual TOP.* 5.In the Events Table, under Transmission Loss, it is unclear how Facilities are to be counted to determine when "three or more" Facilities are lost. In the NERC Glossary, Facility is ambiguously defined as "a set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In many cases, a "set of electrical equipment" can be selected and counted in different ways, which makes this item ambiguous.

Organization	Yes or No	Question 4 Comment
		Both Transmission and Facilities are defined terms and the DSR SDT feels this gives sufficient direction. 6.In the Events Table, under Transmission Loss, it appears that a substation bus failure would only count as a loss of one Facility, even though it might interrupt flow between several transmission lines. We believe this type of event should be reported under this standard, and appropriate revisions should be made to this entry. *The DSR SDT used the defined term "Facility" to add clarity for this event as well as other events in Attachment 1. A Facility is defined as:* *"A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"* *The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.* 7.In the Events Table, under Transmission Loss, consider including generators that are lost as a result of transmission loss events when counting Facilities. For example, if a transmission line and a transformer fail, resulting in a generator going off-line, that should count as a loss of "three or more" facilities and be reportable under this standard. *Attachment 1 is the minimum set of events that will be required to report and communicate per your Operating Plan will be aware of system conditions.* 8.In the Events Table, under "Unplanned Control Center evacuation" and "Loss of monitoring or all voice communication capability," GOPs should be included. GOPs also operate control centers that would be subject to these kinds of occurrences. *Attachment 1 is the minimum set of events that will be required to report and*

Organization	Yes or No	Question 4 Comment
		communicate per your Operating Plan will be aware of system conditions. 9.In the Events Table, under "Loss of monitoring or all voice communication capability," we suggest adding that if there is a failure at one control center, that event is not reportable if there is a successful failover to a backup system or control center. *The DSR SDT has split this event into two separate events based on comments received, it now reads as: "Loss of all voice communication capability" and "Complete or partial loss of monitoring capability".* 10."Fuel supply emergency" is included in the Event Reporting Form, but not in Attachment 1, so there is no reporting threshold or deadline provided for this type of event. *Attachment 2 was updated to reflect the revisions to Attachment 1. The reference to "actual or potential events" was removed. Also, the event type of "other" and "fuel supply emergency" was removed as well.* Clean-up items:1.In R1.5, capitalize "Responsible Entity" and lower-case "process". *The DSR SDT has deleted Requirement 1, part 1.5.* 2.In footnote 1, add "or" before "iii)" to clarify that this event type applies to equipment that satisfies any one of these three conditions. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* 3.In the Event Reporting Form, "forced intrusion" and "Risk to BES equipment" are run together and should be separated. *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new*

Organization	Yes or No	Question 4 Comment
		event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. VSLs:1.We support the substance of the VSLs, but the repeated long list of entities makes the VSLs extremely difficult to read and decipher. The repeated list of entities should be replaced by "Responsible Entities." 2.If the ERO and Regional Entities are to be subject to requirements in this standard (which we oppose), they need to be added to the VSLs. *The DSR SDT has revised the VSLs to eliminate the list of entities and lead with "Responsible Entity".*
Response: Thank you for your comment. Please see response above.		
		Suggest removing 1.4 since 1.5 ensures a annual review. . The implementation of the plan should also include the necessary reporting. *Requirement R1, Part 1.4 has been removed.*
Response: Thank you for your comment. Please see response above.		
Electric Compliance		The concepts of "Critical Assets" and "Critical Cyber Assets" no longer exist in Version 5 of the CIP Standards and so this may cause confusion. Recommend modifying to be in accordance with Version 5. Additionally, it is debatable whether the

Organization	Yes or No	Question 4 Comment
		destruction of, for example, one relay would be a reportable incident given the proposed language. We recommend modifying the language to insure nuisance reporting is minimized. One reportable event is, "Risk to the BES" and the threshold for reporting is, "From a non-environmental physical threat." This appears to be a catch-all reportable event. Due to the subjectivity of this event description, we suggest removing it from the list. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as stakeholders pointed out that these events were adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility "reporting thresholds. CIP-008 addresses Cyber Security Incidents which are defined as:* *"Any malicious act or suspicious event that:* *• Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,* *• Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset."* *A Critical Asset is defined as:* *"Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."* *Since there is an existing event category for damage or destruction of Facilities, having a separate event for "Damage or Destruction of a Critical Asset" is unnecessary.* Footnote 1 and the "Threshold for Reporting" associated with the Event described as "Destruction of BES equipment" expand the reporting scope. For example, a fan on a

Organization	Yes or No	Question 4 Comment
		transformer can be destroyed because a technician drops a screwdriver into it. We believe such an event should not be reportable under EOP-004-2. Yet, as written, a Responsible Entity could interpret that event as reportable (because it would be "unintentional human action" that destroyed a piece of equipment associated with the BES). If the goal of the SDT was to include such events, we think the draft Standard goes too far in requiring reporting. If the SDT did not intend to include such events, the draft Standard should be revised to make that fact clear. Proposed Footnote: BES equipment that become damaged or destroyed due to intentional or unintentional human action which removes the BES equipment from service that i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii). Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative). *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* The word "Significantly" in item ii) of footnote 1 and "as appropriate" in section 1.3 introduces elements of subjectivity. What is "significant" or "appropriate" to one person may not be to someone else. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* In section 1.4, we believe that revising the plan within 90 days of "any" change should be changed to 180 days or else classes of events should be made so that only

Organization	Yes or No	Question 4 Comment
		substantial changes are required to made within the 90 day timeframe. *Requirement R1, Part 1.4 was removed from the standard.*
Response: Thank you for your comment. Please see response above.		
Georgia System Operations Corporation		The ERO and the Regional Entity should not be listed as Responsible Entities. The ERO and the Regional Entity should not have to meet the requirements of this standard, especially reporting to itself. *The ERO and the RE are applicable under the CIP-008 standard and are therefore applicable under EOP-004.* Attachment 1 (all page numbers are from the clean draft):Page 20, destruction of BES equipment: part iii) of the footnote adds damage as an event but the heading is for destruction. Is it just for destruction? Or is it for damage or destruction? *The DSR SDT has modified Attachment 1 to bring more clarity. The 'Destruction' event category has been revised to include damage or destruction of a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* Page 21, Risk to BES equipment: Footnote 3 gives an example where there is flammable or toxic cargo. These are environmental threats. However, the threshold for reporting is for non-environmental threats. Which is it? *For this event, environmental threats are considered to be severe weather, earthquakes, etc. rather than an external threat.* Page 21, BES emergency requiring public appeal for load reduction: A small deficient

Organization	Yes or No	Question 4 Comment
		entity within a BA may not initiate public appeals. The BA is typically the entity which initiates public appeals when the entire BA is deficient. The initiating entity should be the responsible entity not the deficient entity. *The DSR SDT revised this event to indicate the "initiating" entity is responsible for reporting.* Page 21, BES emergency requiring manual firm load shedding: If a RC directs a DP to shed load and the DP initiates manually shedding its load as directed, is the RC the initiating entity? Or is it the DP? *The DSR SDT believes the wording of "initiating entity" provides enough clarity for each applicable entity to understand. In this case, the RC made the call to shed load and therefore should report.* Page 22, system separation (islanding): a DP does not have a view of the system to see that the system separated or how much generation and load are in the island. Remove DP. *The DSR SDT disagrees with your comment. DP's may be the first to recognize that they are islanded or separated from the system.* Attachment 2 (all page numbers are from the clean draft):Page 25: fuel supply emergencies will no longer be reportable under the current draft. *The DSR SDT has removed both "fuel supply emergency" and "other" from Attachment 2 based on comments received.* Miscellaneous typos and quality issues (all page numbers are from the clean draft):Page 5, the last paragraph: There are two cases where Parts A or B are referred to. Attachment 1 no longer has two parts (A & B).Page 27, Discussion of Event Reporting: the second paragraph has a typo at the beginning of the sentence.

Organization	Yes or No	Question 4 Comment
		The DSR SDT has corrected these typos.
Response: Thank you for your comment. Please see response above.		
Thompson Coburn LLP on behalf of Miss. Delta Energy Agency		The first three incident categories designated on Attachment 1 as reportable events should be modified. As the Standard is current drafted, each incident category (i.e., destruction of BES equipment, damage or destruction of Critical Assets, and damage or destruction of Critical Cyber Assets) requires reporting if the event was due to unintentional human action. For example, under the reporting criteria as drafted, inadvertently dropping and damaging a piece of computer equipment designated as a Critical Cyber Asset while moving or installing it would appear to require an event report within an hour of the incident. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as stakeholders pointed out that these events were adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility "reporting thresholds. CIP-008 addresses Cyber Security Incidents which are defined as:* *"Any malicious act or suspicious event that:* *• Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,* *• Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset."* *A Critical Asset is defined as:* *"Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."*

Organization	Yes or No	Question 4 Comment
		Since there is an existing event category for damage or destruction of Facilities, having a separate event for "Damage or Destruction of a Critical Asset" is unnecessary. MDEA requests that the Drafting Team consider modifying footnote 1 and each of the first three event categories to reflect that reportable events include only those that (i) affect an IROL; (ii) significantly affect the reliability margin of the system; or (iii) involve equipment damage or destruction due to intentional human action that results in the removal of the BES equipment, Critical Assets, and/or Critical Cyber Assets, as applicable, from service. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* Footnote 2 (which now pertains only to the fourth incident category - forced intrusions) should also apply to the first three event categories. Specifically, responsible entities should report intentional damage or destruction of BES equipment, damage or destruction of Critical Assets, and damage or destruction of Critical Cyber Assets if either the damage/destruction was clearly intentional or if motivation for the damage or destruction cannot reasonably be determined and the damage or destruction affects the reliability of the BES. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* Attachment 1 is also unclear to the extent that the incident category involving reports for the detection of reportable Cyber Security Incidents includes a reference to CIP-008 as the reporting threshold. While entities in various functional categories

Organization	Yes or No	Question 4 Comment
		(i.e., RCs, BAs, TOPs/TOs, GOPs/GOs, and DPs) are listed as being responsible for the reporting of such events, some entities in these functional categories may not currently be subject to CIP-008. If it is the Drafting Team's intent to limit event reports for Cyber Security Incidents to include only registered entities subject to CIP-008, that clarification should be incorporated into the listing of entities with reporting responsibility for this incident category in Attachment 1. *The "Entity with reporting responsibility" for the event "A reportable Cyber Security Incident" has been revised to "Each Responsible Entity applicable under CIP-008-4 or its successor that experiences the Cyber Security Incident".*
Response: Thank you for your comment. Please see response above.		
Luminant Power		The following comments all apply to Attachment 1: o As a general comment, SDT should specifically list the entities the reportable event applies to in the table for clarity. Do not use general language referencing another standard or statements such as "Deficient entity is responsible for reporting", "Initiating entity is responsible for reporting", or other similar statements used currently in the table. This leaves this open and subject to interpretation. *The DSR SDT disagrees with your comment. This language provides the most flexibility for applicable entities and maintains a minimum level of who is required to report or communicate events based an entity's Operating Plan, as described in Requirement 1.* Also, there are a number of events that do not apply to all entities. o Destruction of BES equipment should be Intentional Damage or Destruction of BES equipment. Unintentional actions occur and should not be a requirement for reporting under disturbance reporting. *The event for "Destruction of BES equipment" has been revised to "Damage or destruction of a Facility". The threshold for reporting information was expanded for*

Organization	Yes or No	Question 4 Comment
		clarity: *"Damage or destruction of a Facility that: affects an IROL* *OR* *Results in the need for actions to avoid an Adverse Reliability Impact* *OR* *Results from intentional human action."* o Actions or situations affecting equipment or generation unit availability due to human error, equipment failure, unintentional human action, external cause, etc. are reported in real time to the BA and other entities as required by other NERC Standards. Disturbance reporting should avoid the type of events that, for instance, would cause the total or partial loss of a generating unit under normal operational circumstances. There are a number of issues with the table in this regard. *The DSR SDT has removed such language based on comments received.* o For clarity, consider changing the table to identify for each event type "who" should be notified. This appears to be missing from the table overall. *The DSR SDT has updated Requirement R1, Part 1.2 to read as: ""1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."* o Reportable Events, the meaning for the Event labeled "Destruction of BES equipment" is not clear. Footnote 1 adds the language "iii) Damaged or destroyed due to intentional or unintentional human action which removes the BES equipment

Organization	Yes or No	Question 4 Comment
		from service." This language can be interpreted to mean that any damage to any BES equipment caused by human action, regardless of intention, must be reported within 1 hour of recognition of the event. This requirement will be overly burdensome. If this is not the intent of the definition of "Destruction of BES equipment", the footnote should be re-worded. As such, it is subjective and left open to interpretation. It should focus only on intentional actions to damage or interrupt BES functionality. It should not be worded as such that every item that trips a unit or every item that is damaged on a unit requires a report. That is where the language right now is not clear. There are and will continue to be unintentional human error that results in taking equipment out of service. This standard was meant to replace sabotage reporting. *All footnotes are deleted and appropriate content moved to 'Thresholds for Reporting' with the exception of the footnote relating to the new event category 'A physical threat that could impact the operability of a Facility'. This remaining footnote provides examples only.* o Damage or destruction of Critical Asset per CIP-002 and Damage or destruction of a Critical Cyber Asset per CIP-002 should be removed from the table as Intentional Damage or Destruction of BES equipment would cover this as well. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as stakeholders pointed out that these events were adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility "reporting thresholds. CIP-008 addresses Cyber Security Incidents which are defined as:* *"Any malicious act or suspicious event that:* *• Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,* *• Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber*

Organization	Yes or No	Question 4 Comment
		Asset." *A Critical Asset is defined as:* *"Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."* *Since there is an existing event category for damage or destruction of Facilities, having a separate event for "Damage or Destruction of a Critical Asset" is unnecessary.* o Risk to BES equipment should be removed from the table as it is very subjective and broad. At a minimum, the 1 hour reporting timeline should begin after recognition and assessment of the incident. As an example, a fire close to BES equipment may not truly be a threat to the equipment and will not be known until an assessment can be made to determine the risk. *The DSR SDT has removed this event based on comments received.* o Detection of a Reportable Cyber Security incident should be removed from the table as this is covered by CIP-008 requirements. Having this in two separate standards is double jeopardy and confusing to entities. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as stakeholders pointed out that these events were adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility "reporting thresholds. CIP-008 addresses Cyber Security Incidents which are defined as:* *"Any malicious act or suspicious event that:*

Organization	Yes or No	Question 4 Comment
		• Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, *• Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset."* *A Critical Asset is defined as:* *"Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."* *Since there is an existing event category for damage or destruction of Facilities, having a separate event for "Damage or Destruction of a Critical Asset" is unnecessary.* o Generation Loss event reporting should only apply to the BA. These authorities have the ability and right to contact generation resources to supply necessary information needed for reporting. This would also eliminate redundant reporting by multiple entities for the same event. *The DSR SDT has tried to minimize duplicative reporting, but recognizes there may be events that trigger more than one report. The current applicability ensures an event that could affect just one of the entities with reporting responsibility isn't missed.* o Suggest that Generation Loss MW loss would match up with the 1500 MW level identified in CIP Version 4 or Version 5 for consistency between future CIP standards and this disturbance reporting standard. This would then cover CIP and significant MW losses that should be reported. *The DSR SDT disagrees as this threshold is based on the current EOP-004-1.* o The Generation Loss MW loss amount needs to have a time boundary. Luminant

Organization	Yes or No	Question 4 Comment
		would suggest a loss of 1500 MW within 15 minutes. *The DSR SDT disagrees as this threshold is based on the current EOP-004-1.* o Unplanned Control Center evacuation should not apply to entities that have backup Control Centers where normal operations can continue without impact to the BES. *The DSR SDT disagrees with your comment. By reporting and communicating per an entity's Operating Plan, you will provide situational awareness to entities per your Operating Plan.* o Loss of monitoring or all voice communication capability should be separated. Also the 24 hour reporting requirement may not be feasible if communications is down for longer than 24 hours. *The DSR SDT has split this event into two separate events based on comments received, it now reads as: "Loss of all voice communication capability" and "Complete or partial loss of monitoring capability".* Luminant would suggest removal of the communication reporting event as there are a number of things that could cause this to occur for longer than the reporting requirement allows, thus putting entities at jeopardy of a potential violation that is out of their control. How does an entity report if all systems and communications are down for more than 24 hours? What about in instances of a partial or total blackout? These events could last much longer than 24 hours. All computer communication would likely also be down thus rendering electronic reporting unavailable. *EOP-004-2 only requires an entity to report and communicate per their Operating Plan within the time frames set in Attachment 1.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 4 Comment
Kansas City Power & Light		The implementation plan indicates that much of CIP-008 is retained. The reporting requirements in CIP-008 and the required reportable events outlined in Attachment 1 are an overlap with CIP-008-3 R1.1 which says "Procedures to characterize and classify events as reportable Cyber Security Incidents" and CIP-008-3 R1.3 which requires processes to address reporting to the ES-ISAC. There is also a NERC document titled, Security Guideline for the Electricity Sector: Threat and Incident Reporting, which is a guideline to "assist entities to identify and classify incidents for reporting to the ES-ISAC". The SDT should consider the content of the Security Guideline for the Electricity Sector: Threat and Incident Reporting when considering the reporting requirements proposed EOP-004. The efforts to incorporate CIP-008 into EOP-004 are insufficient and will result in serious confusion between proposed EOP-004 and CIP-008 and reporting expectations. Considering the complexity CIP incident reporting and the interests of ES-ISAC, it may be beneficial to leave CIP-008 out of the proposed EOP-004 and limit EOP-004 to the reporting interests of NERC. *Attachment 2 (or the DOE Form OE 417) is the reporting form to be used for reporting a "Cyber Security Incident".* The flowchart states, "Notification Protocol to State Agency Law Enforcement". Please correct this to, "Notification to State, Provincial, or Local Law Enforcement", to be consistent with the language in the background section part, "A Reporting Process Solution - EOP-004". *The DSR SDT has updated the "Example of reporting _Process including Law Enforcement", and please note that this is only an "example".* Measure 4 is not clear enough regarding the extent to which drills should be performed. Does the measure mean that all events in the events list need to be drilled or is drilling a subset of the events list sufficient? Please clearly indicate the extent of drilling that is required or clearly indicate in the requirement the extent of the drills to be performed is the responsibility of the Responsible Entity to identify in their "processes".

Organization	Yes or No	Question 4 Comment
		Requirement R4 (now R3) has been revised and the measure now reads: *Each Responsible Entity will have dated and time-stamped records to show that the annual test of Part 1.2 was conducted. Such evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other communication documentation. (R3)* Evidence Retention - it is not clear what the phrase "prior 3 calendar years" represents in the third paragraph of this section regarding data retention for requirements and measures for R2, R3, R4 and M2, M3, M4 respectively. Please clarify what this means. Is that different than the meaning of "since the last audit for 3 calendar years" for R1 and M1? *This has been revised for clarity and to be consistent with NERC Guidance documents. The new evidence retention reads:* *Each Responsible Entity shall retain the current, in force document plus the 'date change page' from each version issued since the last audit or the current and previous version for Requirements R1, R4 and Measures M1, M4.* *Each Responsible Entity shall retain evidence from prior 3 calendar years for Requirements R2, R3 and Measures M2, M3.* VSL for R2 under Severe regarding R1.1 may require revision considering the comment regarding R1.1 in item 2 previously stated. In addition, the VRF for R2 is MEDIUM. R2 is administrative regarding the implementation of the requirements specified in R1. Documentation and maintenance should be considered LOWER. There is no VSL for R4 and a VSL for R4 needs to be proposed. *The DSR SDT reviewed and updated both VSL's for the new requirements.*
Response: Thank you for your comment. Please see response above.		

Organization	Yes or No	Question 4 Comment
SPP Standards Review Group		The inclusion of optional entities to which to report events in R1.3 introduces ambiguity into the standard that we feel needs to be eliminated. We propose the following replacement language for R1.3:A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the Responsible Entity's Regional Entity.We would also propose to incorporate the law enforcement and governmental or provincial agencies mentioned in R1.3 in Attachment 1 by adding them to the existing language for each of the event cells. For example, the first cell in that column would read:The parties identified pursuant to R1.3 and applicable law enforcement and governmental or provincial agencies within 1 hour of recognition of event.Similarly, the phrase '...and applicable law enforcement and governmental or provincial agencies...' should be inserted in all the remaining cells in the 4th column. *Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to report events. Requirement R1,Part 1.2 now reads:* *"1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."*
Response: Thank you for your comment. Please see response above.		
Santee Cooper		The on-going development of the definition of the BES could have significant impacts on reporting requirements associated with this standard.The event titled "Risk to the

Organization	Yes or No	Question 4 Comment
		BES" appears to be a catch-all event and more guidance needs to be provided on this category. *Several stakeholders expressed concerns relating to the "Forced Intrusion" event. Their concerns related to ambiguous language in the footnote. The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "A physical threat that could impact the operability of a Facility".* *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.* The event titled "Damage or Destruction of a Critical Asset or Critical Cyber Asset per CIP-002" is ambiguous and further guidance is recommended. Ambiguity in a standard leaves it open to interpretation for all involved. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as stakeholders pointed out that these events were adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility "reporting thresholds. CIP-008 addresses Cyber Security Incidents which are defined as:* *"Any malicious act or suspicious event that:* *• Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,*

Organization	Yes or No	Question 4 Comment
		• Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset." *A Critical Asset is defined as:* *"Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."* *Since there is an existing event category for damage or destruction of Facilities, having a separate event for "Damage or Destruction of a Critical Asset" is unnecessary.*
Response: Thank you for your comment. Please see response above.		
Florida Municipal Power Agency		The Rules of Procedure language for data retention (first paragraph of the Evidence Retention section) should not be included in the standard, but instead referred to within the standard (e.g., "Refer to Rules of Procedure, Appendix 4C: Compliance Monitoring and Enforcement Program, Section 3.1.4.2 for more retention requirements") so that changes to the RoP do not necessitate changes to the standard. *The language incorporated in this section of the standard is boilerplate language provided by NERC staff for inclusion in each standard.* In R4, it might be worth clarifying that, in this case, implementation of the plan for an event that does not meet the criteria of Attachment 1 and going beyond the requirements R2 and R3 could be used as evidence. Consider adding a phrase as such to M4, or a descriptive footnote that in this case, "actual event" may not be limited to those in Attachment 1.

Organization	Yes or No	Question 4 Comment
		Most stakeholders believed that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2based on stakeholder comments and revised R3 (now R2) to: *"Requirement R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1."* Comments to Attachment 1 table:On "Damage or destruction of Critical Asset" and "... Critical Cyber Asset", Version 5 of the CIP standards is moving away from the binary critical/non-critical paradigm to a high/medium/low risk paradigm. Suggest adding description that if version 5 is approved by FERC, that "critical" would be replaced with "high or medium risk", or include changing this standard to the scope of the CIP SDT, or consider posting multiple versions of this standard depending on the outcome of CIP v5 in a similar fashion to how FAC-003 was posted as part of the GO/TO effort of Project 2010-07. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as stakeholders pointed out that these events were adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility "reporting thresholds. CIP-008 addresses Cyber Security Incidents which are defined as:* *"Any malicious act or suspicious event that:* *• Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,* *• Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber*

Organization	Yes or No	Question 4 Comment
		Asset." *A Critical Asset is defined as:* *"Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."* *Since there is an existing event category for damage or destruction of Facilities, having a separate event for "Damage or Destruction of a Critical Asset" is unnecessary.* On "forced intrusion", the phrase "at BES facility" is open to interpretation as "BES Facility" (e.g., controversy surrounding CAN-0016) which would exclude control centers and other critical/high/medium cyber system Physical Security Perimeters (PSPs). We suggest changing this to "BES Facility or the PSP or Defined Physical Boundary of critical/high/medium cyber assets". This change would cause a change to the applicability of this reportable event to coincide with CIP standard applicability. *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say ' to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* • *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its*

Organization	Yes or No	Question 4 Comment
		Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples. *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* On "Risk to BES equipment", that phrase is open to too wide a range of interpretation; we suggest adding the word "imminent" in front of it, i.e., "Imminent risk to BES equipment". For instance, heavy thermal loading puts equipment at risk, but not imminent risk. Also, "non-environmental" used as the threshold criteria is ambiguous. For instance, the example in the footnote, if the BES equipment is near railroad tracks, then trains getting derailed can be interpreted as part of that BES equipment's "environment", defined in Webster's as "the circumstances, objects, or conditions by which one is surrounded". It seems that the SDT really means "non-weather related", or "Not risks due to Acts of Nature". *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say ' to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* • *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its*

Organization	Yes or No	Question 4 Comment
		Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples. *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* On "public appeal", in the threshold, the descriptor "each" should be deleted, e.g., if a single event causes an entity to be short of capacity, do you really want that entity reporting each time they issue an appeal via different types of media, e.g., radio, TV, etc., or for a repeat appeal every several minutes for the same event? *The DSR SDT has updated the event concerning "public appeals" based on comments received and now reads as: "Public appeal for load reduction event".* Should LSE be an applicable entity to "loss of firm load"? As proposed, the DP is but the LSE is not. In an RTO market, will a DP know what is firm and what is non-firm load? Suggest eliminating DP from the applicability of "system separation". The system separation we care about is separation of one part of the BES from another which would not involve a DP. *The DSR SDT believes the "Entity with Reporting Responsibility" maintains the minimum number and type of entities that will be required to report such an event.* On "Unplanned Control Center Evacuation", CIP v5 might add GOP to the applicability, another reason to add revision of EOP-004-2 to the scope of the CIP v5 drafting team, or in other ways coordinate this SDT with that SDT. Consider posting a couple of versions of the standard depending on the outcome of CIP v5 in a similar fashion to the multiple versions of FAC-003 posted with the Go/TO effort of Project 2010-07.

Organization	Yes or No	Question 4 Comment
		The DSR SDT can only provide information on approved standards, not yet to be defined standards.
Response: Thank you for your comment. Please see response above.		
Dominion		There is still inconsistency in Attachment 1 vs. the DOE OE-417 form; in future changes, Dominion suggests align/rename events similar to that of the 'criteria for filing' events listed in the DOE OE-417, by working in coordination with the DOE. *Thank you for your comment. Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'* • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.* *Please note that not all entities in North America are required to submit the DOE Form OE 417.* Minor comment; in the Background section, the drafting team refers to bulk power

Organization	Yes or No	Question 4 Comment
		system (redline page 5; 1st paragraph and page 7; 2nd paragraph) rather than bulk electric system. *This has been revised to Bulk Electric System.* The note in Attachment 1 states in part that "the affected Responsible Entity shall notify parties per R1 and ..." Dominion believes the correct reference to be R3. In addition, capitalized terms "Event" and "Event Report" are used in this note. Dominion believes the terms should be non-capitalized as they are not NERC defined terms. *The DSR SDT has updated this note based on comments received and now reads as: "NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written event report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per R1 and provide as much information as is available at the time of the notification. Reports to the ERO should be submitted to one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422."* Attachment 1 - "Detection of a reportable Cyber Security Incident - That meets the criteria in CIP-008". This essentially equates the criteria to be defined by the entity in its procedures as required by CIP-008 R1.1., additional clarification should be added in Attachment 1 to make this clear. *The DSR SDT believes that this event language provides enough clarity by providing the minimum events to be reported.* The last sentence in Attachment 2 instructions should clarify that the email, facsimile and voice communication methods are for ERO notification only. *The DSR SDT agrees and has revised the sentence to include "to the ERO".* Dominion continues to believe that the drill or exercise specified in R4 is

Organization	Yes or No	Question 4 Comment
		unnecessary. Dominion suggests deleting this activity in the requirement. *Requirement R4 related to an annual test of the communication portion of Requirement R1 by a drill or exercise and this has been removed. Requirement R3 now reads: "Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. ".* *The DSR SDT envisions that the testing under Requirement R3 will include verification of contact information contained in the Operating Plan is correct. As an example, the annual review of the Operating Plan could include calling "others as defined in the Responsible Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated.*
Response: Thank you for your comment. Please see response above.		
Ingleside Cogeneration LP		We are encouraged that the 2009-01 project team has eliminated duplicate reporting requirements from multiple organizations and governmental agencies. Ingleside Cogeneration LP believes that there are further improvements that can be made in this area - as the remaining overlap seem to be a result of legalities and preferences, not technical issues. We would like to see an ongoing commitment by NERC for a single process that will consolidate and automate data entry, submission, and distribution. *Attachment 1 is the basis for EOP-004-2; it contains the events and thresholds for reporting. OE-417, as well as, the EAWG's requirements were considered in creating Attachment 1, but there remain differences for the following reasons:* • *EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an*

Organization	Yes or No	Question 4 Comment
		opportunity not a 'must-have' • *OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America* • *NERC has no control over the criteria in OE-417, which can change at any time* • *Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary* *In an effort to minimize administrative burden, US entities may use OE-417 rather than Attachment 2 to report under EOP-004. Note you may have to report the same event more quickly to the DOE than is required by EOP-004, but this cannot be helped due to bullet point 2 above.* *Please note that not all entities in North America are required to submit the DOE Form OE 417.*
Response: Thank you for your comment. Please see response above.		
SERC OC Standards Review Group		We believe that reporting of the events in Attachment 1 has no reliability benefit to the bulk electric system. In addition, Attachment 1, in its current form, is likely to be impossible to implement consistently across North America. A requirement, to be considered a reliability requirement, must be implementable. We suggest that Attachment 1 should be removed. *The DSR SDT disagrees with this comment. Attachment 1 is the minimum set of events that will be required to report and communicate per your Operating Plan will be aware of system conditions.* We have a question about what looks like a gap in this standard: Assuming one of thedrivers for the standard is to protect against a coordinated physical or cyber attack on the grid, what happens if the attack occurs in 3-4 geographically diverse areas? State or provisional law enforcement officials are not accountable under the standard, so we have no way of knowing if they report the attack to the FBI or the

Organization	Yes or No	Question 4 Comment
		RCMP. Even if one or two of them did, might not the FBI, in different parts of the country, interpret it as vandalism, subject to local jurisdiction?It seems that NERC is the focal point that would have all the reports and, ideally, some knowledge how the pieces fit together. It looks like NERC's role is to solely pass information on "applicable" events to the FERC. Unless the FERC has a 24x7 role not shown in the standard, should not NERC have some type of assessment responsibility to makes inquiries at the FBI/RCMP on whether they are aware of the potential issue and are working on it?"The comments expressed herein represent a consensus of the views of the above named members of the SERC OC Standards Review group only and should not be construed as the position of SERC Reliability Corporation, its board or its officers." *Requirement R1, Part 1.2 was updated and now reads as: "A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."* *By reporting to the ERO all events, this will allow the ERO to coordinate with other agencies as they see fit.*
Response: Thank you for your comment. Please see response above.		
ZGlobal on behalf of City of Ukiah, Alameda Municipal Power, Salmen River Electric, City of Lodi		We feel that the drafting team has done an excellent job of providing clarification and reasonable reporting requirements to the right functional entity. However we feel additional clarification should be made in the Attachment I Event Table. We suggest the following modifications:For the Event: BES Emergency resulting in automatic firm load sheddingModify the Entity with Reporting Responsibility to: Each DP or TOP that experiences the automatic load shedding within their respective distribution serving or Transmission Operating area. *The DSR SDT believes the "Entity with Reporting Responsibility" contains the minimum*

Organization	Yes or No	Question 4 Comment
		entities that will be required to report and reads as: "Each DP or TOP that experiences the automatic load shedding" For the Event: Loss of Firm load for â‰¥ 15 MinutesModify the Entity with Reporting Responsibility to: Each BA, TOP, DP that experiences the loss of firm load within their respective balancing, Transmission operating, or distribution serving area. *The DSR SDT believes the "Entity with Reporting Responsibility" contains the minimum entities that will be required to report and reads as: "Each BA, TOP, DP that experiences the loss of firm load"*
Response: Thank you for your comment. Please see response above.		
PSEG		We have several comments:1. The "Law Enforcement Reporting" section on p. 6 is unclearly written. The first three sentences are excerpted here: "The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement."The outages described prior to the last sentence are "vandalism and terrorism." The next sentence states "Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES." If the SDT intended to only have events reported to law enforcement that could to Cascading, it should state so clearly and succinctly. But other language implies otherwise. *The DSR SDT has updated the "Example of reporting _Process including Law Enforcement", and please note that this is only an "example".* a. The footnote 1 on Attachment 1 (p. 20) states: "Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g.,

Organization	Yes or No	Question 4 Comment
		removal of grounding straps rendering protective relaying inoperative)." Rendering a relay inoperative may or may not lead to Cascading. *The DSR SDT has removed all footnotes with the exception of the updated event within Attachment 1 that states: "A physical threat that could impact the operability of a Facility". This event has the following footnote, which states: "Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* b. With regard to "forced intrusion," footnote 2 on Attachment 1 states: "Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects (sic) the reliability of the BES." The criterion, or criteria, for reporting an event to law enforcement needs to be unambiguous. The SDT needs to revise this "Law Enforcement Section" so that is achieved. The "law enforcement reporting" criterion, or criteria, should also be added to the flow chart on p. 9. We suggest the following as a starting point for the team to discuss: there should be two criteria for reporting an event to law enforcement: (1) BES equipment appears to have been deliberately damaged, destroyed, or stolen, whether by physical or cyber means, or (2) someone has gained, or attempted to gain, unauthorized access by forced or unauthorized entry (e.g., via a stolen employee keycard badge) into BES facilities, including by physical or cyber means. *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* *The 'Damage or Destruction' event category has been revised to say ' to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was*

Organization	Yes or No	Question 4 Comment
		deleted *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples.* *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* 2. The use of the terms "communicating events" in R1.3, and the use of the term "communication process" are confusing because in other places such as R3 the term "reporting" is used. If the SDT intends "communicating" to mean "reporting" as that later term is used in R3, it should use the same "reporting" term in lieu of "communicating" or "communication" elsewhere. Inconsistent terminology causes confusion. PSEG prefers the word "reporting" because it is better understood. *Requirement R1, Part 1.3 (now Part 1.2) was revised to add clarifying language by eliminating the phrase "as appropriate" and indicating that the Responsible Entity is to define its process for reporting and with whom to report events. Requirement R1, Part 1.2 now reads:* *"1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement governmental or provincial agencies."*

Organization	Yes or No	Question 4 Comment
		The SDT envisions that most entities will only need to slightly modify their existing CIP-001 Sabotage Reporting procedures in order to comply with the Operating Plan requirement in this proposed standard. As many of the features of both are substantially similar, the SDT feels that some information may need to updated and verified. 3. Attachment 1 needs to more clearly define what is meant by "recognition of an event."a. When equipment or a facility is involved, it would better state within "X" time (e.g., 1 hour) of "of confirmation of an event by the entity that either owns or operates the Element or Facility." *Based on stakeholder comments, Requirement R1 was revised for clarity. Requirement R1, Part 1.1 was revised to replace the word "identifying" with "recognizing" and Part 1.2 was eliminated. This also aligns the language of the standard with FERC Order 693, Paragraph 471.* *"(2) specify baseline requirements regarding what issues should be addressed in the procedures for recognizing {emphasis added} sabotage events and making personnel aware of such events;"* b. Other reports should have a different specification of the starting time of the reporting deadline clock. For example, in the requirement for reporting a "BES Emergency requiring public appeal for load reduction," it is unclear what event is required to be reported - the "BES Emergency requiring public appeal" or "public appeal for load reduction." If the later is intended, then the event should be reported within "24 hours after a public appeal for load reduction is first issued." These statements need to be reviewed and customized for each event by the SDT so they are unambiguous. *All one hour reporting timelines have been changed to 24 hours with the exception of a*

Organization	Yes or No	Question 4 Comment
		'Reportable Cyber Security Incident'. This is maintained due to FERC Order 706, Paragraph 673: *"...direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event..."* *For the remaining events, 24 hours should provide sufficient time to manage the incident in real-time before having to report and is consistent with current in-force standard EOP-004-1.* In summary, the starting time for the reporting clock to start running should be made clear for each event. This will require that the SDT review each event and customize the starting time appropriately. The phrase "recognition of an event" should not be used because it is too vague. *Based on stakeholder comments, Requirement R1 was revised for clarity. Part 1.1 was revised to replace the word "identifying" with "recognizing" and Part 1.2 was eliminated. This also aligns the language of the standard with FERC Order 693, Paragraph 471.* *"(2) specify baseline requirements regarding what issues should be addressed in the procedures for recognizing {emphasis added} sabotage events and making personnel aware of such events;"* 4. When EOP-004-2 refers to other standards, it frequently omits the version of the standard. Example: see the second and third row of Attachment 1 that refers to "CIP-002." Include the version on all standards referenced. *References to CIP-002 have been removed from the standard. The intent of referencing those standards is to prevent rewriting the standard within EOP-004-2. The threshold for reporting CIP-008 events is written as "That meets the criteria in CIP-008-4 or its successor."*

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comment. Please see response above.		
Ameren		Yes. We have the other comments as follow:(1) The "EOP-004 Attachment 1: Events Table" is quite lengthy and written in a manner that can be quite subjective in interpretation when determining if an event is reportable. We believe this table should be clear and unambiguous for consistent and repeatable application by both reliability entities and a CEA. *The DSR SDT has reviewed and further revised Attachment 1 based on comments received. We believe that it is both concise and easily interpreted.* The table should be divided into sections such as: 9a) Events that affect the BES that are either clearly sabotage or suspected sabotage after review by an entity's security department and local/state/federal law enforcement.(b) Events that pose a risk to the BES and that clearly reach a defined threshold, such as load loss, generation loss, public appeal, EEAs, etc. that entities are required to report by the end of the next business day.(c) Other events that may prove valuable for lessons learned, but are less definitive than required reporting events. These events should be reported voluntarily and not be subject to a CEA for non-reporting. *The DSR SDT received many comments regarding the various entries of Attachment 1. Many commenters questioned the reliability benefit of reporting events to the ERO within 1 hour. Most of the events with a one hour reporting requirement were revised to 24 hours based on stakeholder comments as well as those types of events are currently required to be reported within 24 hours in the existing mandatory and enforceable standards. The only remaining type of event that is to be reported within one hour is "A reportable Cyber Security Incident" as it required by CIP-008 and FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a*

Organization	Yes or No	Question 4 Comment
		cyber security incident as soon as possible, but in any event, within one hour of the event…" *The table was reformatted to separate one hour reporting and 24 hour reporting. The last column of the table was also deleted and the information contained in it was transferred to the sentence above each table. These sentences are:* *"One Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the event."* *"Twenty-four Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within twenty-four hour of recognition of the event."* (d)Events identified through other means outside of entity reporting, but due to their nature, could benefit the industry by an event report with lessons learned. Requests to report and perform analysis on these type of events should be vetted through a ERO/Functional Entity process to ensure resources provided to this effort have an effective reliability benefit. *The DSR SDT has deleted the "lessons learned" language. Requirement R4 now only requires an annual review of the Operating Plan - the '90 days' and ' other circumstances' elements have been removed.* (2)Any event reporting shall not in any manner replace or inhibit an Entity's responsibility to coordinate with other Reliability Entities (such as the RC, TOP, BA, GOP as appropriate) as required by other Standards, and good utility practice to operate the electric system in a safe and reliable manner. *The DSR SDT concurs with your comment.*

Organization	Yes or No	Question 4 Comment
		(3) The 1 hour reporting maximum time limit for all GO events in Attachment 1 should be lengthened to something reasonable - at least 24 hours. Operators in our energy centers are well-trained and if they have good reason to suspect an event that might have serious impact on the BES will contact the TOP quickly. However, constantly reporting events that turn out to have no serious BES impact and were only reported for fear of a violation or self-report will quickly result in a cry wolf syndrome and a great waste of resources and risk to the GO and the BES. The risk to the GO will be potential fines, and the risk to the BES will be ignoring events that truly have an impact of the BES. *The DSR SDT received many comments regarding the various entries of Attachment 1. Many commenters questioned the reliability benefit of reporting events to the ERO within 1 hour. Most of the events with a one hour reporting requirement were revised to 24 hours based on stakeholder comments as well as those types of events are currently required to be reported within 24 hours in the existing mandatory and enforceable standards. The only remaining type of event that is to be reported within one hour is "A reportable Cyber Security Incident" as it required by CIP-008 and FERC Order 706, Paragraph 673:* *"direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"* *The table was reformatted to separate one hour reporting and 24 hour reporting. The last column of the table was also deleted and the information contained in it was transferred to the sentence above each table. These sentences are:* *"One Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the*

Organization	Yes or No	Question 4 Comment
		event." *"Twenty-four Hour Reporting: Submit Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within twenty-four hour of recognition of the event."* (4)The 2nd and 3rd Events on Attachment 1 should be reworded so they do not use terms that may have been deleted from the NERC Glossary by the time FERC approves this Standard. *The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1, as these events are adequately addressed through the CIP-008 and 'Damage or Destruction of a Facility' reporting thresholds.* (5) The terms "destruction" and "damage" are key to identifying reportable events. Neither has been defined in the Standard. The term destruction is usually defined as 100% unusable. However, the term damage can be anywhere from 1% to 99% unusable and take anywhere from 5 minutes to 5 months to repair. How will we know what the SDT intended, or an auditor will expect, without additional information? *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* *The 'Damage or Destruction' event category has been revised to say ' to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new*

Organization	Yes or No	Question 4 Comment
		event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples. *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* (6)We also do not understand why "destruction of BES equipment" (first item Attachment 1, first page) must be reported < 1 hour, but "system separation (islanding) > 100 MW" (Attachment 1, page 3) does not need to be reported for 24 hours. *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* *The 'Damage or Destruction' event category has been revised to say 'to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting*

Organization	Yes or No	Question 4 Comment
		timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it may have first occurred. Also, the footnote only contains examples. *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.* (7)The first 2 Events in Attachment 1 list criteria Threshold for Reporting as "...operational error, equipment failure, external cause, or intentional or unintentional human action." The term "intentional or unintentional human action" appears to cover "operational error" so these terms appear redundant and create risk of misreporting. Can this be clarified? *The DSR SDT has updated this language based on comments received and now reads as: " Damage or destruction of a Facility that:* *Affects an IROL (per FAC-014)* *OR* *Results in the need for actions to avoid an Adverse Reliability Impact* *OR* *Results from intentional human action."* (8)The footnote of the first page of Attachment 1 includes the explanation "...ii) Significantly affects the reliability margin of the system..." However, the GO is prevented from seeing the system and has no idea what BES equipment can affect the reliability margin of the system. Can this be clarified by the SDT? *The DSR SDT has removed all footnotes with the exception of the updated event within Attachment 1 that states: "A physical threat that could impact the operability of a Facility". This event has the following footnote, which states: "Examples include a*

Organization	Yes or No	Question 4 Comment
		train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility." (9) The use of the term "BES equipment" is problematic for a GO. NERC Team 2010-17 (BES Definition) has told the industry its next work phase will include identifying the interface between the generator and the transmission system. The 2010-17 current effort at defining the BES still fails to clearly define whether or not generator tie-lines are part of the BES. In addition, NERC Team 2010-07 may also be assigned the task of defining the generator/transmission interface and possibly whether or not these are BES facilities. Can the SDT clarify the use of this term? For example, does it include the entire generator lead-line from the GSU high-side to the point of interconnection? Does it include any station service transformer supplied from the interconnected BES? *The DSR SDT has modified Attachment 1 to bring more clarity. The more subjective events were rewritten as follows:* • *The 'Damage or Destruction' event category has been revised to say ' to a Facility', (a defined term) and thresholds have be modified to provide clarity. The footnote was deleted* • *'Forced intrusion' and 'Risk to BES Equipment' have been combined under a new event type called 'A physical threat that could impact the operability of a Facility'. Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported. Note that the reporting timeline (now revised to 24 hours) starts when the situation has been determined as a threat, not when it*

Organization	Yes or No	Question 4 Comment
		may have first occurred. Also, the footnote only contains examples. *These two remaining event categories that aren't related to power system phenomena are essential as they effectively translate the intent of CIP-001 into EOP-004.*
Response: Thank you for your comment. Please see response above.		
Performance Analysis Subcommittee		There continues to be some confusion regarding whether the loss of firm load was consistent with the planned operation of the system or was an unintended consequence. As such it might be helpful if instead of a single check box for loss of firm load there were two check boxes 1) loss of firm load – consequential and 2) loss of firm load non-consequential. *Thank you for your comment. The DSR SDT believes that Attachment 2 contains the minimum amount of information under this standard. Any entity reporting an event can add as much information as they see fit.*
Response: Thank you for your comment. Please see response above.		
Southwestern Power Administration's		"Attachment 1 contains elements that do not need to be included, and redundant elements such as: Forced intrusion at BES Facility - A facility break-in does not necessarily mean that the facility has been impacted or has undergone damage or destruction. *The DSR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had overlap in the perceived reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was*

Organization	Yes or No	Question 4 Comment
		revised to "Any physical threat that could impact the operability of a Facility". *Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.* *The footnote regarding this event type was expanded to provide additional guidance in:* *"Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."* Detection of a reportable Cyber Security Incident per CIP-008 - If entities are addressing this requirement in CIP-008, why do so again in EOP-004 (Attachment 2-EOP-004, Reporting Requirement number 5)? *The reporting aspects of CIP-008 have been removed from CIP-008 and are included in EOP-004. Please see the Implementation Plan with regards to the retirement of CIP-008, R1.3* Transmission Loss: Each TOP that experiences transmission loss of three or more facilities - This element should be removed or rewritten so that it only applies when the loss includes a contingent element of an IROL facility." *The DSR SDT disagrees with limiting this type of event to only "a contingent element*

Organization	Yes or No	Question 4 Comment
		of an IROL facility." It is important for situational awareness and trending analysis to have these types of events reported.
Response: Thank you for your comment. Please see response above.		
The Performance Analysis Subcommittee		There continues to be some confusion regarding whether the loss of firm load was consistent with the planned operation of the system or was an unintended consequence. As such it might be helpful if instead of a single check box for loss of firm load there were two check boxes 1) loss of firm load – consequential and 2) loss of firm load non-consequential. *The DSR SDT believes that this information should be obtained in follow up through the Events Analysis Program. The reporting entity may have concerns or difficulties in determining if load is consequential or non-consequential in its initial analysis for the report. Further investigation outside of the reporting time of 24 hours may be needed to make this determination.*
Response: Thank you for your comment. Please see response above.		
Xcel Energy		
Los Angeles Department of Water and Power		
Liberty Electric Power		
Nebraska Public Power District		
Southwestern Power Administration		

Organization	Yes or No	Question 4 Comment
Electric Reliability Council of Texas, Inc.		

END OF REPORT

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SC approved SAR for initial posting (April, 2009).
2. SAR posted for comment (April 22 – May 21, 2009).
3. SC authorized moving the SAR forward to standard development (September 2009).
4. Concepts Paper posted for comment (March 17 – April 16, 2010).
5. Initial Informal Comment Period (September 15 – October 15, 2010)
6. Second Comment Period (Formal) (March 9 – April 8, 2011)
7. Third Comment Period and Initial Ballot (October 28 – December 12, 2011)

Proposed Action Plan and Description of Current Draft
This is the fourth posting of the proposed standard in accordance with Results-Based Criteria. The drafting team requests posting for a 30-day formal comment period concurrent with the formation of the ballot pool and the successive ballot.

Future Development Plan

Anticipated Actions	Anticipated Date
Drafting team considers comments, makes conforming changes on third posting	January - March 2012
Fourth Comment/Ballot period	March – April 2012
Recirculation Ballot period	May 2012
Receive BOT approval	June 2012
File with regulatory authorities	August 2012

Effective Dates

EOP-004-2 shall become effective on the first day of the third calendar quarter after applicable regulatory approval. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the third calendar quarter after Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-2a Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2 Event Reporting; Retire CIP-001-2a Sabotage Reporting and Retired EOP-004-1 Disturbance Reporting. Retire CIP-008-3, Requirement 1, Part 1.3.	Revision to entire standard (Project 2009-01)

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

When this standard has received ballot approval, the text boxes will be moved to the Guideline and Technical Basis Section.

A. Introduction

1. Title: Event Reporting

2. Number: EOP-004-2

3. Purpose: To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities.

4. Applicability

4.1. Functional Entities: Within the context of EOP-004-2, the term "Responsible Entity" shall include the following entities as shown in EOP-004 Attachment 1:

4.1.1. Reliability Coordinator

4.1.2. Balancing Authority

4.1.3. Interchange Coordinator

4.1.4. Transmission Service Provider

4.1.5. Transmission Owner

4.1.6. Transmission Operator

4.1.7. Generator Owner

4.1.8. Generator Operator

4.1.9. Distribution Provider

4.1.10. Load Serving Entity

4.1.11. Electric Reliability Organization

4.1.12. Regional Entity

5. Background:

NERC established a SAR Team in 2009 to investigate and propose revisions to the CIP-001 and EOP-004 Reliability Standards. The team was asked to consider the following:

1. CIP-001 could be merged with EOP-004 to eliminate redundancies.
2. Acts of sabotage have to be reported to the DOE as part of EOP-004.
3. Specific references to the DOE form need to be eliminated.
4. EOP-004 had some 'fill-in-the-blank' components to eliminate.

The development included other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient Bulk Electric System reliability standards.

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC SC in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009.

The DSR SDT developed a concept paper to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT had developed. The posting of the concept paper sought comments from stakeholders on the "road map" that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the DSR SDT. The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC issues database and FERC Order 693 Directives in order to determine a prudent course of action with respect to revision of these standards.

Summary of Key Concepts

The DSRSDT identified the following principles to assist them in developing the standard:

- Develop a single form to report disturbances and events that threaten the reliability of the Bulk Electric System
- Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements
- Establish clear criteria for reporting
- Establish consistent reporting timelines
- Provide clarity around who will receive the information and how it will be used

During the development of concepts, the DSR SDT considered the FERC directive to "further define sabotage". There was concern among stakeholders that a definition may be ambiguous and subject to interpretation. Consequently, the DSR SDT decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was sabotage or vandalism without the intervention of law enforcement. The DSR SDT felt that attempting to define sabotage would result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard. The events listed in EOP-004 Attachment 1 were developed to provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

The types of events that are required to be reported are contained within EOP-004 Attachment 1. The DSR SDT has coordinated with the NERC Events Analysis Working Group to develop the list of events that are to be reported under this standard. EOP-004 Attachment 1 pertains to those actions or events that have impacted the Bulk Electric System. These events were previously reported under EOP-004-1, CIP-001-1 or the Department of Energy form OE-417. EOP-004 Attachment 1 covers similar items that may have had an impact on the Bulk Electric System or has the potential to have an impact and should be reported.

The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in EOP-004 Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting.

Data Gathering

The requirements of EOP-004-1 require that entities "promptly analyze Bulk Electric System disturbances on its system or facilities" (Requirement R2). The requirements of EOP-004-2 specify that certain types of events are to be reported but do not include provisions to analyze events. Events reported under EOP-004-2 may trigger further scrutiny by the ERO Events Analysis Program. If warranted, the Events Analysis Program personnel may request that more data for certain events be provided by the reporting entity or other entities that may have experienced the event. Entities are encouraged to become familiar with the Events Analysis Program and the NERC Rules of Procedure to learn more about with the expectations of the program.

Law Enforcement Reporting

The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of Bulk Electric System from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.

Stakeholders in the Reporting Process

- Industry
- NERC (ERO), Regional Entity
- FERC
- DOE
- NRC
- DHS – Federal
- Homeland Security- State
- State Regulators
- Local Law Enforcement
- State or Provincial Law Enforcement
- FBI
- Royal Canadian Mounted Police (RCMP)

The above stakeholders have an interest in the timely notification, communication and response to an incident at an industry facility. The stakeholders have various levels of accountability and have a vested interest in the protection and response to ensure the reliability of the BES.

Present expectations of the industry under CIP-001-1a:

It has been the understanding by industry participants that an occurrence of sabotage has to be reported to the FBI. The FBI has the jurisdictional requirements to investigate acts of sabotage and terrorism. The CIP-001-1-1a standard requires a liaison relationship on behalf of the industry and the FBI or RCMP. Annual requirements, under the standard, of the industry have not been clear and have lead to misunderstandings and confusion in the industry as to how to demonstrate that the liaison is in place and effective. As an example of proof of compliance with Requirement R4, responsible entities have asked FBI Office personnel to provide, on FBI letterhead, confirmation of the existence of a working relationship to report acts of sabotage, the number of years the liaison relationship has been in existence, and the validity of the telephone numbers for the FBI.

Coordination of Local and State Law Enforcement Agencies with the FBI

The Joint Terrorism Task Force (JTTF) came into being with the first task force being established in 1980. JTTFs are small cells of highly trained, locally based, committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. The JTTF is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. Coordination and communications largely through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs. This information flow can be most beneficial to the industry in analytical intelligence, incident response and investigation. Historically, the most immediate response to an industry incident has been local and state law enforcement agencies to suspected vandalism and criminal damages at industry facilities. Relying upon the JTTF coordination between local, state and FBI law enforcement would be beneficial to effective communications and the appropriate level of investigative response.

Coordination of Local and Provincial Law Enforcement Agencies with the RCMP

A similar law enforcement coordination hierarchy exists in Canada. Local and Provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. The Provincial law enforcement agency has a reporting relationship with the Royal Canadian Mounted Police (RCMP).

A Reporting Process Solution – EOP-004

A proposal discussed with the FBI, FERC Staff, NERC Standards Project Coordinator and the SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Reportable Events). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial or local level law enforcement agency. The state or provincial or local level law enforcement agency will coordinate with law enforcement with jurisdiction to investigate. If the state or provincial or local level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial or local level law enforcement agency will notify and coordinate with the FBI or the RCMP.

Example of Reporting Process including Law Enforcement

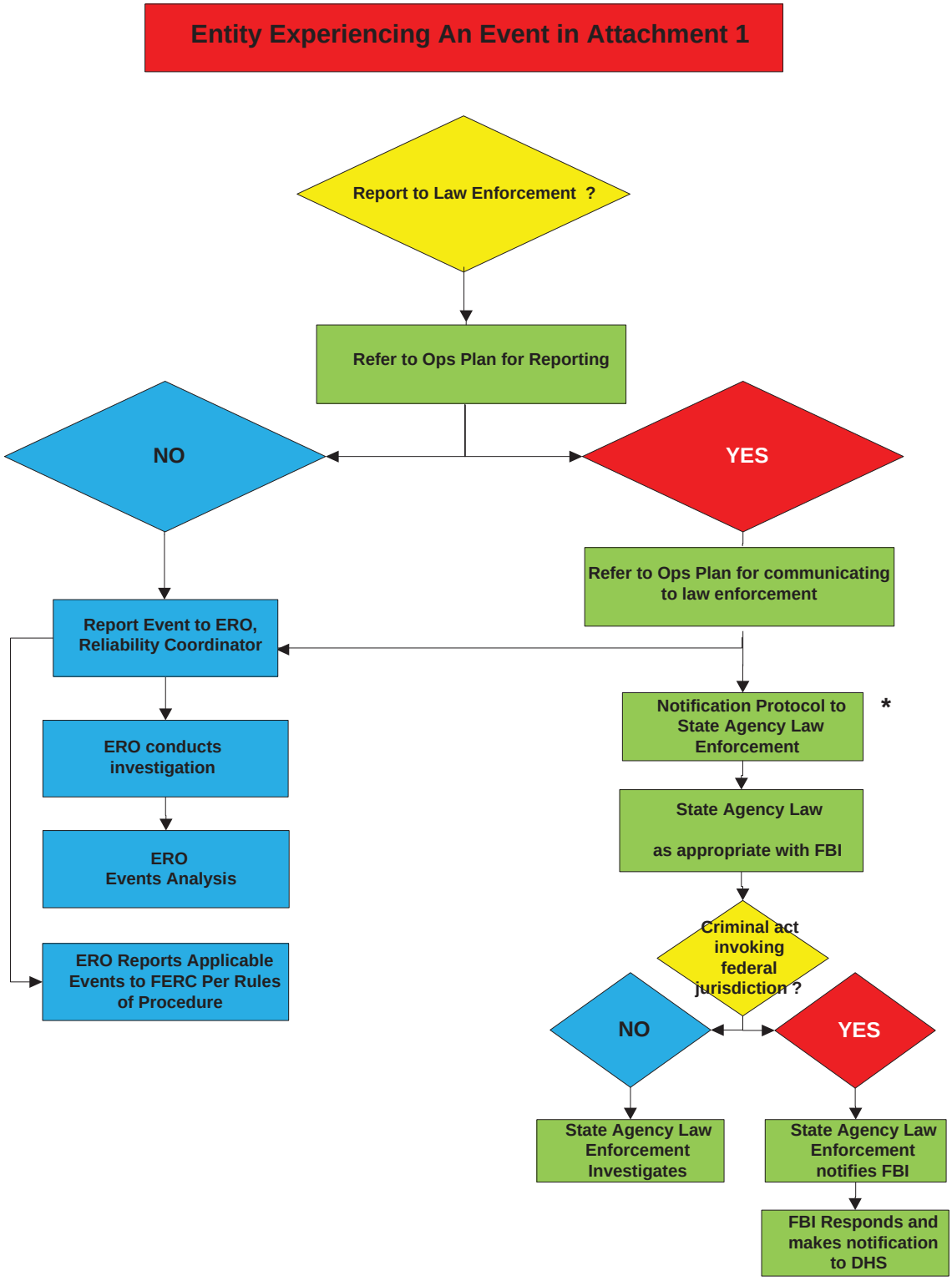

* Canadian entities will follow law enforcement protocols applicable in their jurisdictions

B. Requirements and Measures

R1. Each Responsible Entity shall have an event reporting Operating Plan that includes: *[Violation Risk: Factor: Lower] [Time Horizon: Operations Planning]*

1.1. A process for recognizing each of the applicable events listed in EOP-004 Attachment 1(except for Cyber Security Incidents characterized and classified according to the requirements in CIP-008-3 or its successor).

1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies.

M1. Each Responsible Entity will have a current, dated, event reporting Operating Plan which includes Parts 1.1 – 1.2.

Rationale for R1

The requirement to have an Operating Plan for reporting specific types of events provides the entity with a method to have its operating personnel recognize events that affect reliability and to be able to report them to appropriate parties; i.e. Regional Entities, applicable Reliability Coordinators, and law enforcement and other jurisdictional agencies when so recognized. In addition, these event reports are an input to the NERC Events Analysis Program. These other parties use this information to promote reliability, develop a culture of reliability excellence, provide industry collaboration and promote a learning organization.

Every industry participant that owns or operates elements or devices on the grid has a formal or informal process, procedure, or steps it takes to gather information regarding what happened when events occur. This requirement has the Responsible Entity establish documentation on how that procedure, process, or plan is organized. This documentation may be a single document or a combination of various documents that achieve the reliability objective.

Part 1.1 clarifies that entities must address each of the "applicable" events listed in EOP-004 Attachment 1. Not all responsible entities must address all events; e.g., some events are only applicable to the Reliability Coordinator. Part 1.1 acknowledges that Cyber Security Incidents are characterized and classified according to the requirements in CIP-008-3.

Part 1.2 could include a process flowchart, identification of internal and external personnel or entities to be notified, or a list of personnel by name and their associated contact information.

An existing procedure that meets the requirements of CIP-001-2a may be included in this Operating Plan along with other processes, procedures or plans to meet this requirement.

R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

M2. Each Responsible Entity will have, for each event experienced, a dated copy of the completed EOP-004 Attachment 2 form or DOE form OE-417 report submitted for that event; and dated and time-stamped transmittal records to show that the event was reported supplemented by operator logs or other operating documentation. Other forms of evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other operating documentation for situations where filing a written report was not possible. (R2)

R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Each Responsible Entity will have dated and time-stamped records to show that the annual test of Part 1.2 was conducted. Such evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other communication documentation. The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. (R3)

Rationale for R2

Each Responsible Entity must report and communicate events according to its Operating Plan after the fact based on the information in EOP-004 Attachment 1. By implementing the event reporting Operating Plan, the Responsible Entity will assure situational awareness to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies as deemed necessary by the Registered Entity. By communicating events per the Operating Plan, the Responsible Entity will assure that people/agencies are aware of the current situation and they may prepare to mitigate current and further events.

Rationale for R3 and R4

Requirements 3 and 4 call for annual test of the communications process in Part 1.2 as well as an annual review of the event reporting Operating Plan. These two requirements help ensure that the event reporting Operating Plan is up to date and entities will be effective in reporting events to assure situational awareness to the Electric Reliability Organization and their Reliability Coordinator . This will assure that the BES remains secure and stable by mitigation actions that the Reliability Coordinator has within its function.

R4. Each Responsible Entity shall conduct an annual review of the event reporting Operating Plan in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M4. Each Responsible Entity will have dated and time-stamped records to show that the annual review of the event reporting Operating Plan was conducted. Such evidence may include, but are not limited to, the current document plus the 'date change page' from each version that was reviewed. (R4)

C. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

The Regional Entity shall serve as the Compliance enforcement authority unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

For NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2 Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

Each Responsible Entity shall retain the current, document plus the 'date change page' from each version issued since the last audit for Requirements R1, R4 and Measures M1, M4.

Each Responsible Entity shall retain evidence from prior 3 calendar years for Requirements R2, R3 and Measure M2, M3.

If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3 Compliance Monitoring and Enforcement Processes:

Compliance Audit
Self-Certification
Spot Checking
Compliance Investigation
Self-Reporting
Complaint

1.4 Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	N/A	N/A	The Responsible Entity has an event reporting Operating Plan but failed to include one of Parts 1.1 through 1.2.	The Responsible Entity failed to include both Parts 1.1 and 1.2.
R2	Operations Assessment	Medium	The Responsible Entity submitted a report more than 24 hours but less than or equal to 36 hours after an event requiring reporting within 24 hours in EOP-004 Attachment 1. OR The Responsible Entity submitted a report in the appropriate timeframe but failed to provide all of the required information.	The Responsible Entity submitted a report more than 36 hours but less than or equal to 48 hours after an event requiring reporting within 24 hours in EOP-004 Attachment 1. OR The Responsible Entity submitted a report more than 1 hour but less than 2 hours after an event requiring reporting within 1 hour in EOP-004 Attachment 1.	The Responsible Entity submitted a report more than 48 hours but less than or equal to 60 hours after an event requiring reporting within 24 hours in EOP-004 Attachment 1. OR The Responsible Entity submitted a report in more than 2 hours but less than 3 hours after an event requiring reporting within 1 hour in EOP-004 Attachment 1.	The Responsible Entity submitted a report more than 60 hours after an event requiring reporting within 24 hours in EOP-004 Attachment 1. OR The Responsible Entity submitted a report more than 3 hours after an event requiring reporting within 1 hour in EOP-004 Attachment 1. OR The Responsible Entity failed to submit a report for an event in

						EOP-004 Attachment 1.
R3	Operations Planning	Medium	The Responsible Entity performed the annual test of the communications process in Part 1.2 but was late by less than one calendar month.	The Responsible Entity performed the annual test of the communications process in Part 1.2 but was late by one calendar month or more but less than two calendar months.	The Responsible Entity performed the annual test of the communications process in Part 1.2 but was late by two calendar months or more but less than three calendar months.	The Responsible Entity performed the annual test of the communications process in Part 1.2 but was late by three calendar months or more. OR The Responsible Entity failed to perform the annual test of the communications process in Part 1.2.
R4	Operations Planning	Medium	The Responsible Entity performed the annual review of the event reporting Operating Plan but was late by less than one calendar month.	The Responsible Entity performed the annual review of the event reporting Operating Plan but was late by one calendar month or more but less than two calendar months.	The Responsible Entity performed the annual review of the event reporting Operating Plan but was late by two calendar months or more but less than three calendar months.	The Responsible Entity performed the annual review of the event reporting Operating Plan but was late by three calendar months or more. OR The Responsible Entity failed to perform the annual review of the event reporting Operating Plan

D. Variances

None.

E. Interpretations

None.

F. Interpretations

Guideline and Technical Basis (attached).

EOP-004 - Attachment 1: Reportable Events

NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per Requirement R1 and provide as much information as is available at the time of the notification. Submit reports to the ERO via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422.

One Hour Reporting: Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the event.

Event	Entity with Reporting Responsibility	Threshold for Reporting
A reportable Cyber Security Incident.	Each Responsible Entity applicable under CIP-008-3 or its successor that experiences the Cyber Security Incident	That meets the criteria in CIP-008-3 or its successor

Rationale Box for EOP-004 Attachment 1:

The DSR SDT used the defined term "Facility" to add clarity for several events listed in Attachment 1. A Facility is defined as:

> "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"

The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.

Twenty-four Hour Reporting: Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within twenty-four hours of recognition of the event.

Event	Entity with Reporting Responsibility	Threshold for Reporting
Damage or destruction of a Facility	Each BA, TO, TOP, GO, GOP, DP that experiences the damage or destruction of a Facility	Damage or destruction of a Facility that: Affects an IROL (per FAC-014) OR Results in the need for actions to avoid an Adverse Reliability Impact OR Results from actual or suspected intentional human action.
Any physical threat that could impact the operability of a Facility[1]	Each RC, BA, TO, TOP, GO, GOP, DP that experiences the event	Threat to a Facility excluding weather related threats.
BES Emergency requiring public appeal for load reduction	Initiating entity is responsible for reporting	Public appeal for load reduction event
BES Emergency requiring system-wide voltage reduction	Initiating entity is responsible for reporting	System wide voltage reduction of 3% or more
BES Emergency requiring manual firm load shedding	Initiating entity is responsible for reporting	Manual firm load shedding ≥ 100 MW

[1] Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility.

Event	Entity with Reporting Responsibility	Threshold for Reporting
BES Emergency resulting in automatic firm load shedding	Each DP or TOP that implements automatic load shedding	Firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)
Voltage deviation on a Facility	Each TOP that observes the voltage deviation	± 10% sustained for ≥ 15 continuous minutes
IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only)	Each RC that experiences the IROL Violation (all Interconnections) or SOL violation for Major WECC Transfer Paths (WECC only)	Operate outside the IROL for time greater than IROL T_v (all Interconnections) or Operate outside the SOL for more than 30 minutes for Major WECC Transfer Paths (WECC only).
Loss of firm load for ≥ 15 Minutes	Each BA, TOP, DP that experiences the loss of firm load	• ≥ 300 MW for entities with previous year's demand ≥ 3,000 MW • ≥ 200 MW for all other entities
System separation (islanding)	Each RC, BA, TOP, DP that experiences the system separation	Each separation resulting in an island of generation and load ≥ 100 MW
Generation loss	Each BA, GOP that experiences the generation loss	• ≥ 2,000 MW for entities in the Eastern or Western Interconnection • ≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection
Complete loss of off-site power to a nuclear generating plant (grid supply)	Each TO, TOP that experiences the complete loss of off-site power to a nuclear generating plant	Affecting a nuclear generating station per the Nuclear Plant Interface Requirement
Transmission loss	Each TOP that experiences the transmission loss	Unintentional loss of three or more Transmission Facilities (excluding successful automatic reclosing)
Unplanned control center evacuation	Each RC, BA, TOP that experiences the event	Unplanned evacuation from BES control center facility for 30 minutes or more.
Loss of all voice communication capability	Each RC, BA, TOP that experiences the loss of all voice communication capability	Affecting a BES control center for ≥ 30 continuous minutes

Event	Entity with Reporting Responsibility	Threshold for Reporting
Complete or partial loss of monitoring capability	Each RC, BA, TOP that experiences the complete or partial loss of monitoring capability	Affecting a BES control center for ≥ 30 continuous minutes such that analysis tools (State Estimator, Contingency Analysis) are rendered inoperable.

EOP-004 - Attachment 2: Event Reporting Form

EOP-004 Attachment 2: Event Reporting Form

Use this form to report events. The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422.

Task		Comments
1.	Entity filing the report include: Company name: Name of contact person: Email address of contact person: Telephone Number: Submitted by (name):	
2.	Date and Time of recognized event. Date: (mm/dd/yyyy) Time: (hh:mm) Time/Zone:	
3.	Did the event originate in your system?	Yes ☐ No☐ Unknown ☐
4.	**Event Identification and Description:**	
	(Check applicable box) ☐ public appeal ☐ voltage reduction ☐ manual firm load shedding ☐ firm load shedding(undervoltage, underfrequency, SPS/RAS) ☐ voltage deviation ☐ IROL violation ☐ loss of firm load ☐ system separation (islanding) ☐ generation loss ☐ complete loss of off-site power to nuclear generating plant ☐ transmission loss ☐ damage or destruction of Facility ☐ unplanned control center evacuation ☐ loss of all voice communication capability ☐ complete or partial loss of monitoring capability ☐ physical threat that could impact the operability of a Facility ☐ reportable Cyber Security Incident	Written description (optional):

Guideline and Technical Basis

Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01) - Reporting Concepts

Introduction

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and has developed updated standards based on the SAR.

The standards listed under the SAR are:

- CIP-001 — Sabotage Reporting
- EOP-004 — Disturbance Reporting

The changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). These standard deals exclusively with after-the-fact reporting.

The DSR SDT has consolidated disturbance and sabotage event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts and Assumptions:

The Standard:

- Requires reporting of "events" that impact or may impact the reliability of the Bulk Electric System
- Provides clear criteria for reporting
- Includes consistent reporting timelines
- Identifies appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- Provides clarity around of who will receive the information

Discussion of Disturbance Reporting

Disturbance reporting requirements existed in the previous version of EOP-004. The current approved definition of Disturbance from the NERC Glossary of Terms is:

1. An unplanned event that produces an abnormal system condition.
2. Any perturbation to the electric system.

3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.

Disturbance reporting requirements and criteria were in the previous EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and developed the list of events that are to be reported under this standard (EOP-004 Attachment 1).

Discussion of Event Reporting
There are situations worthy of reporting because they have the potential to impact reliability.

Event reporting facilitates industry awareness, which allows potentially impacted parties to prepare for and possibly mitigate any associated reliability risk. It also provides the raw material, in the case of certain potential reliability threats, to see emerging patterns.

Examples of such events include:

- Bolts removed from transmission line structures
- Detection of cyber intrusion that meets criteria of CIP-008-3 or its successor standard
- Forced intrusion attempt at a substation
- Train derailment near a transmission right-of-way
- Destruction of Bulk Electric System equipment

What about sabotage?
One thing became clear in the DSR SDT's discussion concerning sabotage: everyone has a different definition. The current standard CIP-001 elicited the following response from FERC in FERC Order 693, paragraph 471 which states in part: *". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."*

Often, the underlying reason for an event is unknown or cannot be confirmed. The DSR SDT believes that by reporting material risks to the Bulk Electric System using the event categorization in this standard, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.

Certain types of events should be reported to NERC, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and/or Provincial or local law enforcement. Other types of events may have different reporting requirements. For example, an event that is related to copper theft may only need to be reported to the local law enforcement authorities.

Potential Uses of Reportable Information
Event analysis, correlation of data, and trend identification are a few potential uses for the information reported under this standard. The standard requires Functional entities to report the incidents and provide known information at the time of the report. Further data gathering necessary for event analysis is provided for under the Events Analysis Program and the NERC Rules of Procedure. Other entities (e.g. – NERC, Law Enforcement, etc) will be responsible for

performing the analyses. The NERC Rules of Procedure (section 800) provide an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for reliability. Jurisdictional agencies (which may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE) have other duties and responsibilities.

Collection of Reportable Information or "One stop shopping"

The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT has updated the listing of reportable events in EOP-004 Attachment 1 based on discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences still exist.

The reporting required by this standard is intended to meet the uses and purposes of NERC. The DSR SDT recognizes that other requirements for reporting exist (e.g., DOE-417 reporting), which may duplicate or overlap the information required by NERC. To the extent that other reporting is required, the DSR SDT envisions that duplicate entry of information should not be necessary, and the submission of the alternate report will be acceptable to NERC so long as all information required by NERC is submitted. For example, if the NERC Report duplicates information from the DOE form, the DOE report may be included or attached to the NERC report, in lieu of entering that information on the NERC report.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SC approved SAR for initial posting (April, 2009).
2. SAR posted for comment (April 22 – May 21, 2009).
3. SC authorized moving the SAR forward to standard development (September 2009).
4. Concepts Paper posted for comment (March 17 – April 16, 2010).
5. Initial Informal Comment Period (September 15 – October 15, 2010)
6. Second Comment Period (Formal) (March 9 – April 8, 2011)
7. Third Comment Period and Initial Ballot (October 28 – December 12, 2011)

Proposed Action Plan and Description of Current Draft

This is the ~~third~~fourth posting of the proposed standard in accordance with Results-Based Criteria. The drafting team requests posting for a ~~45~~30-day formal comment period concurrent with the formation of the ballot pool and the ~~initial~~successive ballot.

Future Development Plan

Anticipated Actions	Anticipated Date
Drafting team considers comments, makes conforming changes on ~~second~~third posting	~~April - October 2011~~January - March 2012
~~Third~~Fourth Comment/Ballot period	~~November - December 2011~~March – April 2012
Recirculation Ballot period	~~December 2011~~May 2012
Receive BOT approval	~~February~~June 2012
File with regulatory authorities	August 2012

Effective Dates

EOP-004-2 shall become effective on the first day of the third calendar quarter after applicable regulatory approval. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the third calendar quarter after Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-2a Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2 ~~Impact~~ Event Reporting; Retire CIP-001-2a Sabotage Reporting and Retired EOP-004-1 Disturbance Reporting. Retire CIP-008-~~4~~3, Requirement 1, Part 1.3.	Revision to entire standard (Project 2009-01)

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

When this standard has received ballot approval, the text boxes will be moved to the Guideline and Technical Basis Section.

A. Introduction

1. Title: Event Reporting

2. Number: EOP-004-2

3. Purpose: To improve ~~industry awareness and~~ the reliability of the Bulk Electric System by requiring the reporting of events ~~with the potential to impact reliability and their causes, if known, by the~~by Responsible Entities.

4. Applicability

4.1. Functional Entities: Within the context of EOP-004-2, the term "Responsible Entity" shall ~~mean~~include the following entities as shown in EOP-004 Attachment 1:

4.1.1. Reliability Coordinator

4.1.2. Balancing Authority

4.1.3. Interchange Coordinator

4.1.4. Transmission Service Provider

4.1.5. Transmission Owner

4.1.6. Transmission Operator

4.1.7. Generator Owner

4.1.8. Generator Operator

4.1.9. Distribution Provider

4.1.10. Load Serving Entity

4.1.11. Electric Reliability Organization

4.1.12. Regional Entity

5. Background:

NERC established a SAR Team in 2009 to investigate and propose revisions to the CIP-001 and EOP-004 Reliability Standards. The team was asked to consider the following:

1. CIP-001 could be merged with EOP-004 to eliminate redundancies.
2. Acts of sabotage have to be reported to the DOE as part of EOP-004.
3. Specific references to the DOE form need to be eliminated.
4. EOP-004 had some 'fill-in-the-blank' components to eliminate.

The development included other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient ~~bulk power system~~Bulk Electric System reliability standards.

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC SC in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009.

The DSR SDT developed a concept paper to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT had developed. The posting of the concept paper sought comments from stakeholders on the "road map" that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the DSR SDT. The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC issues database and FERC Order 693 Directives in order to determine a prudent course of action with respect to revision of these standards.

Summary of Key Concepts

The DSRSDT identified the following principles to assist them in developing the standard:

- Develop a single form to report disturbances and events that threaten the reliability of the ~~bulk electric system~~Bulk Electric System
- Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements
- Establish clear criteria for reporting
- Establish consistent reporting timelines
- Provide clarity around who will receive the information and how it will be used

During the development of concepts, the DSR SDT considered the FERC directive to "further define sabotage". There was concern among stakeholders that a definition may be ambiguous and subject to interpretation. Consequently, the DSR SDT decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was sabotage or vandalism without the intervention of law enforcement. The DSR SDT felt that attempting to define sabotage would result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard. The events listed in EOP-004 Attachment 1 were developed to provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

The types of events that are required to be reported are contained within EOP-004 Attachment 1. The DSR SDT has coordinated with the NERC Events Analysis Working Group to develop the list of events that are to be reported under this standard. EOP-004 Attachment 1~~, Part A~~ pertains to those actions or events that have impacted the Bulk Electric System. These events were previously reported under EOP-004-1, CIP-001-1 or the Department of Energy form OE-417.

EOP-004 Attachment 1~~, Part B~~ covers similar items that may have had an impact on the Bulk Electric System or has the potential to have an impact and should be reported.

The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in EOP-004 Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting.

Data Gathering

The requirements of EOP-004-1 require that entities "promptly analyze Bulk Electric System disturbances on its system or facilities" (Requirement R2). The requirements of EOP-004-2 specify that certain types of events are to be reported but do not include provisions to analyze events. Events reported under EOP-004-2 may trigger further scrutiny by the ERO Events Analysis Program. If warranted, the Events Analysis Program personnel may request that more data for certain events be provided by the reporting entity or other entities that may have experienced the event. Entities are encouraged to become familiar with the Events Analysis Program and the NERC Rules of Procedure to learn more about with the expectations of the program.

Law Enforcement Reporting

The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of ~~bulk power systems~~Bulk Electric System from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.

Stakeholders in the Reporting Process

- Industry
- NERC (ERO), Regional Entity
- FERC
- DOE
- NRC
- DHS – Federal
- Homeland Security- State
- State Regulators
- Local Law Enforcement
- State or Provincial Law Enforcement
- FBI
- Royal Canadian Mounted Police (RCMP)

The above stakeholders have an interest in the timely notification, communication and response to an incident at an industry facility. The stakeholders have various levels of accountability and have a vested interest in the protection and response to ensure the reliability of the BES.

Present expectations of the industry under CIP-001-1a:

It has been the understanding by industry participants that an occurrence of sabotage has to be reported to the FBI. The FBI has the jurisdictional requirements to investigate acts of sabotage and terrorism. The CIP-001-1-1a standard requires a liaison relationship on behalf of the industry and the FBI or RCMP. Annual requirements, under the standard, of the industry have not been clear and have lead to misunderstandings and confusion in the industry as to how to demonstrate that the liaison is in place and effective. As an example of proof of compliance with Requirement R4, responsible entities have asked FBI Office personnel to provide, on FBI letterhead, confirmation of the existence of a working relationship to report acts of sabotage, ~~,~~ the number of years the liaison relationship has been in existence, and the validity of the telephone numbers for the FBI.

Coordination of Local and State Law Enforcement Agencies with the FBI

The Joint Terrorism Task Force (JTTF) came into being with the first task force being established in 1980. JTTFs are small cells of highly trained, locally based, committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. The JTTF is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. Coordination and communications largely through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs. This information flow can be most beneficial to the industry in analytical intelligence, incident response and investigation. Historically, the most immediate response to an industry incident has been local and state law enforcement agencies to suspected vandalism and criminal damages at industry facilities. Relying upon the JTTF coordination between local, state and FBI law enforcement would be beneficial to effective communications and the appropriate level of investigative response.

Coordination of Local and Provincial Law Enforcement Agencies with the RCMP

A similar law enforcement coordination hierarchy exists in Canada. Local and Provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. The Provincial law enforcement agency has a reporting relationship with the Royal Canadian Mounted Police (RCMP).

A Reporting Process Solution – EOP-004

A proposal discussed with the FBI, FERC Staff, NERC Standards Project Coordinator and the SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Reportable Events). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial or local level law enforcement agency. The state or provincial or local level law enforcement agency will coordinate with law enforcement with jurisdiction to investigate. If the state or provincial or local level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial or local level law enforcement agency will notify and coordinate with the FBI or the RCMP.

Example of Reporting Process including Law Enforcement

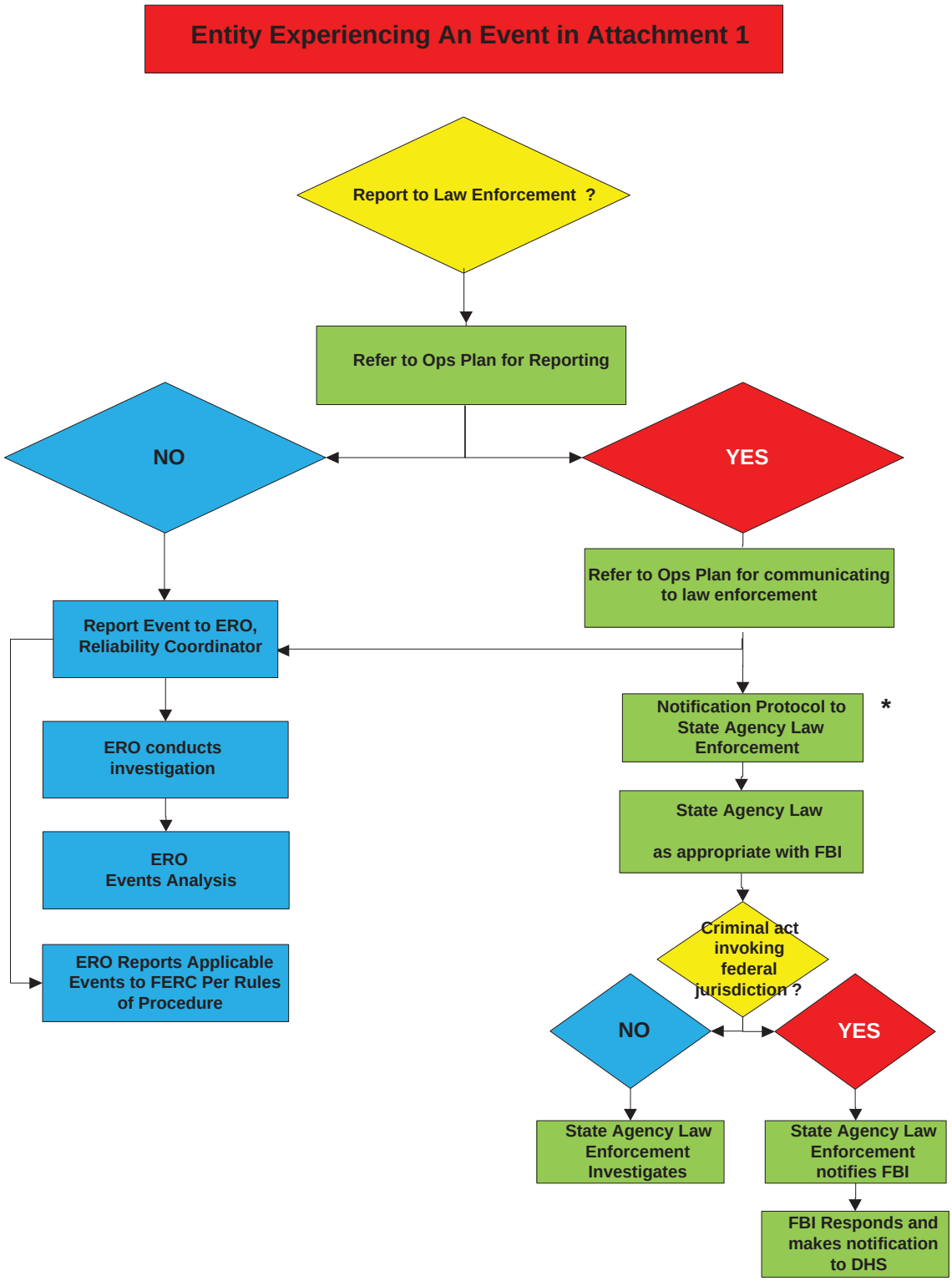

* Canadian entities will follow law enforcement protocols applicable in their jurisdictions

B. Requirements and Measures

R1. Each Responsible Entity shall have an event reporting Operating Plan that includes: *[Violation Risk: Factor: Lower] [Time Horizon: Operations Planning]*

1.1. A process for ~~identifying~~recognizing each of the applicable events listed in EOP-004 Attachment 1(except for Cyber Security Incidents characterized and classified according to the requirements in CIP-008-3 or its successor).

~~1.2. A process for gathering information for Attachment 2 regarding events listed in Attachment 1.~~

~~1.3.~~ A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization~~,~~ and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator ~~and the following as appropriate:~~

- ~~Internal company personnel~~
- ~~The Responsible Entity's Regional Entity~~
- ~~Law~~; law enforcement
- ~~Governmental~~, governmental or provincial agencies

Rationale for R1

The requirement to have an Operating Plan for reporting specific types of events provides the entity with a method to have its operating personnel recognize events that affect reliability and to be able to report them to appropriate parties; i.e. Regional Entities, applicable Reliability Coordinators, and law enforcement and other jurisdictional agencies when so recognized. In addition, these event reports are an input to the NERC Events Analysis Program. These other parties use this information to promote reliability, develop a culture of reliability excellence, provide industry collaboration and promote a learning organization.

Every industry participant that owns or operates elements or devices on the grid has a formal or informal process, procedure, or steps it takes to gather information regarding what happened when events occur. This requirement has the Responsible Entity establish documentation on how that procedure, process, or plan is organized. This documentation may be a single document or a combination of various documents that achieve the reliability objective.

Part 1.1 clarifies that entities must address each of the "applicable" events listed in EOP-004 Attachment 1. Not all responsible entities must address all events; e.g., some events are only applicable to the Reliability Coordinator. Part 1.1 acknowledges that Cyber Security Incidents are characterized and classified according to the requirements in CIP-008-3.

Part 1.2 could include a process flowchart, identification of internal and external personnel or entities to be notified, or a list of personnel by name and their associated contact information. An existing procedure that meets the requirements of CIP-001-2a may be included in this Operating Plan along with other processes, procedures or plans to meet this requirement.

~~1.4. Provision(s) for updating the Operating Plan within 90 calendar days of any change in assets, personnel, other circumstances that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3.~~

~~1.5.~~1.2. ~~A Process for ensuring the responsible entity reviews the Operating Plan at least annually (once each calendar year) with no more than 15 months between reviews~~.

M1. Each Responsible Entity will ~~provide the~~have a current, dated, ~~in force~~event reporting Operating Plan which includes Parts 1.1 ~~–~~ 1.~~5 as requested~~2.

R2. Each Responsible Entity shall implement ~~the parts of~~ its event reporting Operating Plan ~~that meet Requirement R1, Parts~~for applicable events listed in EOP-004 Attachment 1~~.1~~, and ~~1.2 for an actual event and Parts 1.4 and 1.5 as~~in accordance with the timeframe specified~~.~~ in EOP-004 Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment~~]~~.]*

M2. ~~Responsible Entities shall provide evidence that it implemented the parts of its Operating Plan to meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts, 1.4 and 1.5 as specified. Evidence may include, but is not limited to, an event report form (Attachment 2) or the OE-417 report submitted, operator logs, voice recordings, or dated documentation of review and update of the Operating Plan. (R2)~~

Rationale for R2

~~Each Responsible Entity must implement the various parts of Requirement R1. Parts 1.1 and 1.2 call for identifying and gathering information for actual events. Parts 1.4 and 1.5 require updating and reviewing the Operating Plan.~~ Each Responsible Entity must report and communicate events according to its Operating Plan after the fact based on the information in EOP-004 Attachment 1. By implementing the event reporting Operating Plan, the Responsible Entity will assure situational awareness to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies as deemed necessary by the Registered Entity. By communicating events per the Operating Plan, the Responsible Entity will assure that people/agencies are aware of the current situation and they may prepare to mitigate current and further events.

~~**R3**. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment].*~~

~~**M3.** Responsible Entities shall provide a record of the type of~~ Each Responsible Entity will have, for each event experienced~~;~~, a dated copy of the completed EOP-004 Attachment 2 form or DOE form ~~or~~ OE-417 report submitted for that event; and dated and time-stamped transmittal records to show that the event was reported~~. (R3~~ supplemented by operator logs or other operating documentation. Other forms of evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other operating documentation for situations where filing a written report was not possible. (R2)

R3. Each Responsible Entity shall conduct an annual test, not including notification to

Rationale for R3 and R4

Requirements 3 and 4 call for annual test of the communications process in Part 1.2 as well as an annual review of the event reporting Operating Plan. These two requirements help ensure that the event reporting Operating Plan is up to date and entities will be effective in reporting events to assure situational awareness to the Electric Reliability Organization and their Reliability Coordinator . This will assure that the BES remains secure and stable by mitigation actions that the Reliability Coordinator has within its function.

the Electric Reliability Organization, of the communications process in Part 1.2. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Each Responsible Entity will have dated and time-stamped records to show that the annual test of Part 1.2 was conducted. Such evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other communication documentation. The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. (R3)

R4. Each Responsible Entity shall ~~verify (through actual implementation for an event, or through a drill or exercise) the communication process in its Operating Plan, created pursuant to Requirement 1, Part 1.3, at least annually (once per calendar year), with no more than 15 calendar months between verification or actual implementation.~~ conduct an annual review of the event reporting Operating Plan in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M4. ~~The Responsible Entity shall provide evidence that it verified the communication process in its Operating Plan for events created pursuant to Requirement R1, Part 1.3. Either implementation of the communication process as documented in its Operating Plan for an actual event or documented evidence of a drill or exercise may be used as evidence to meet this requirement. The time period between an actual event or verification shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or dated documentation of a verification. (R3)~~ Each Responsible Entity will have dated and time-stamped records to show that the annual review of the event reporting Operating Plan was conducted. Such evidence may include, but are not limited to, the current document plus the 'date change page' from each version that was reviewed. (R4)

C. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

The Regional Entity~~; or~~
~~If~~ shall serve as the ~~Responsible Entity works for~~Compliance enforcement authority unless the ~~Regional Entity, then~~applicable entity is owned, operated, or controlled by the Regional Entity ~~will establish an agreement with~~. In such cases the ERO or ~~another~~a Regional entity approved by ~~the ERO and~~ FERC ~~(i.e. another Regional Entity) to be responsible for compliance enforcement; or~~or other applicable governmental authority shall serve as the CEA.

~~Third~~For NERC, a third-party monitor without vested interest in the outcome for ~~the ERO~~NERC shall serve as the Compliance Enforcement Authority.

1.2 Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

Each Responsible Entity shall retain the current, ~~in force~~ document plus the '~~dated revision history'~~date change page' from each version issued since the last audit for ~~3 calendar years for Requirement~~Requirements R1, R4 and ~~Measure~~Measures M1, M4.

Each Responsible Entity shall retain evidence from prior 3 calendar years for Requirements R2, R3~~, R4,~~ and ~~Measures~~Measure M2, M3~~, M4.~~

~~Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer~~.

If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until ~~found compliant~~mitigation is complete and approved or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3 Compliance Monitoring and Enforcement Processes:

Compliance ~~Audits~~Audit
Self-~~Certifications~~Certification
Spot Checking
Compliance ~~Violation Investigations~~Investigation
Self-Reporting
~~Complaints~~Complaint

1.4 Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	~~Long-term~~Operations Planning	Lower	~~The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity has an Operating Plan but failed to include one of Parts 1.1 through 1.5.~~ N/A	~~The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity has an Operating Plan but failed to include two of Parts 1.1 through 1.5.~~N/A	The ~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving~~Responsible Entity has an event reporting Operating Plan but failed to include ~~three~~one of Parts 1.1 through 1.~~5~~2.	The ~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving~~Responsible Entity failed to include ~~four or more of~~both Parts 1.1 ~~through~~and 1.~~5~~2.
R2	~~Real-time~~ Operations ~~and Same-day Operations~~Assessmen	Medium	~~1.1: N/A~~	The Responsible Entity submitted a report more than 36	The Responsible Entity submitted a report more than 48	~~1.1: The Reliability Coordinator, Balancing Authority,~~

	t		1.2: N/A 1.4: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to update the Operating Plan more than 90 days of a change, but not more than 100 days after a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator,	hours but less than or equal to 48 hours after an event requiring reporting within 24 hours in EOP-004 Attachment 1. OR 1.1: N/A 1.2: N/A 1.4: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to update the Operating Plan	hours but less than or equal to 60 hours after an event requiring reporting within 24 hours in EOP-004 Attachment 1. OR 1.1: N/A 1.2: N/A 1.4: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to update the Operating Plan more than 110 days of a change, but not more than 120 days after a change.	Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to implement the process for identifying events. 1.2: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to implement the

			Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 15 calendar months after its previous review, but not more than 18 calendar months after its previous review. The Responsible Entity submitted a report more than 24 hours but less than or equal to 36 hours after an event requiring reporting within 24 hours in EOP-004 Attachment 1.	more than 100 days of a change, but not more than 110 days after a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 18 calendar months after its previous review, but not more than 21 calendar months after its previous review.The	1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 21 calendar months after its previous review, but not more than 24 calendar months after its previous review. The Responsible Entity submitted a report in more than 2 hours but less than 3 hours after an event requiring reporting within 1 hour in EOP-004 Attachment 1.	process for gathering information for Attachment 2. 1.4: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to update the Operating Plan more than 120 days of a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission

			OR The Responsible Entity submitted a report in the appropriate timeframe but failed to provide all of the required information.	Responsible Entity submitted a report more than 1 hour but less than 2 hours after an event requiring reporting within 1 hour in EOP-004 Attachment 1.		~~Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 24 calendar months after its previous review.~~The Responsible Entity submitted a report more than 60 hours after an event requiring reporting within 24 hours in EOP-004 Attachment 1. OR The Responsible Entity submitted a report more than 3 hours after an event requiring reporting within 1 hour in EOP-004 Attachment 1. OR The Responsible Entity failed to submit a report for an event in EOP-004

						Attachment 1.
R3	~~Real-time~~ Operations ~~and Same-day Operations~~Planning	Medium	~~The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 24 hours but less than or equal to 36 hours after an event requiring reporting within 24 hours in Attachment 1.~~ The Responsible Entity performed the annual test of the communications process in Part 1.2 but was late by less	~~The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 36 hours but less than or equal to 48 hours after an event requiring reporting within 24 hours in Attachment 1.~~ ~~OR~~ ~~The Reliability Coordinator, Balancing Authority, Interchange~~	~~The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 48 hours but less than or equal to 60 hours after an event requiring reporting within 24 hours in Attachment 1.~~ The Responsible Entity performed the annual test of the communications process in Part 1.2 but was late by two calendar months or more but less than three calendar	~~The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 60 hours after an event requiring reporting within 24 hours in Attachment 1.~~ The Responsible Entity performed the annual test of the communications process in Part 1.2 but was late by three calendar months or more. OR The ~~Reliability~~

			than one calendar month.	Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 1 hour but less than 2 hours after an event requiring reporting within 1 hour in Attachment 1.The Responsible Entity performed the annual test of the communications process in Part 1.2 but was late by one calendar month or more but less than two calendar months.	months. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report in more than 2 hours but less than 3 hours after an event requiring reporting within 1 hour in Attachment 1.	Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 3 hours after an event requiring reporting within 1 hour in Attachment 1.Responsible Entity failed to perform the annual test of the communications process in Part 1.2. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider,

						~~Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to submit a report for an event in Attachment 1.~~
R4	-Operations Planning	Medium	~~The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan,~~	~~The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan,~~	~~The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 21 calendar months after its previous test, but not~~	The ~~Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving~~Responsible Entity ~~verified~~performed the ~~communication process in its~~annual review of the event reporting Operating

			more than 15 calendar months after its previous test, but not more than 18 calendar months after its previous test. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to verify the communication process in its Operating Plan within the calendar year.The Responsible Entity	more than 18 calendar months after its previous test, but not more than 21 months after its previous test.The Responsible Entity performed the annual review of the event reporting Operating Plan but was late by one calendar month or more but less than two calendar months.	more than 24 months after its previous test.The Responsible Entity performed the annual review of the event reporting Operating Plan but was late by two calendar months or more but less than three calendar months.	Plan, more than 24 but was late by three calendar months after its previous testor more. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to verify the communication process in its Operating Plan. The Responsible Entity failed to perform the annual review of the event reporting Operating Plan

			performed the annual review of the event reporting Operating Plan but was late by less than one calendar month.			

D. Variances

None.

E. Interpretations

None.

F. Interpretations

Guideline and Technical Basis (attached).

EOP-004 - Attachment 1: Reportable Events~~ Table~~

NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per Requirement R1 and provide as much information as is available at the time of the notification.~~ The affected Responsible Entity shall provide periodic verbal updates until adequate information is available to issue a written Event report. Reports~~ Submit reports to the ERO ~~should be submitted to~~via one of the following: e-mail: ~~esisac@nerc.com~~esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422.

One Hour Reporting: Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the event.

Event	Entity with Reporting Responsibility	Threshold for Reporting
A reportable Cyber Security Incident.	Each Responsible Entity applicable under CIP-008-~~4~~3 or its successor that experiences the Cyber Security Incident	That meets the criteria in CIP-008-~~4~~3 or its successor

Rationale Box for EOP-004 Attachment 1:

The DSR SDT used the defined term "Facility" to add clarity for several events listed in Attachment 1. A Facility is defined as:

> "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"

The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.

Twenty-four Hour Reporting: Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within twenty-four hours of recognition of the event.

Event	Entity with Reporting Responsibility	Threshold for Reporting
~~Destruction~~Damage or destruction of ~~BES equipment~~[1] a Facility	Each ~~RC,~~ BA, TO, TOP, GO, GOP, DP that experiences the damage or destruction of ~~BES equipment~~a Facility	~~Initial indication~~Damage or destruction of a Facility that: Affects an IROL (per FAC-014) OR Results in the ~~event was due~~need for actions to ~~operational error, equipment failure, external cause, or~~ avoid an Adverse Reliability Impact OR Results from actual or suspected intentional ~~or unintentional~~ human action.
~~Damage or destruction of Critical Asset per CIP-002~~	~~Applicable Entities under CIP-002~~	~~Initial indication the event was due to operational error, equipment failure, external cause, or intentional or unintentional human action.~~
~~Damage or destruction of a Critical Cyber Asset per CIP-002~~	~~Applicable Entities under CIP-002.~~	~~Through intentional or unintentional human action.~~
~~Forced intrusion~~[2]	~~Each RC, BA, TO, TOP, GO, GOP that~~	~~At a BES facility~~

~~[1] BES equipment that: i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii) Damaged or destroyed due to intentional or unintentional human action which removes the BES equipment from service. Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly (e.g., removal of grounding straps rendering protective relaying inoperative).~~

~~[2] Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects the reliability of the BES).~~

Event	Entity with Reporting Responsibility	Threshold for Reporting
	~~experiences the forced intrusion~~	
~~Risk to BES equipment~~[3]Any physical threat that could impact the operability of a Facility[4]	Each RC, BA, TO, TOP, GO, GOP, DP that experiences the ~~risk to BES equipment~~event	~~From a non-environmental physical threat~~Threat to a Facility excluding weather related threats.
~~Detection of a reportable Cyber Security Incident.~~	~~Each RC, BA, TO, TOP, GO, GOP, DP, ERO or RE that experiences the Cyber Security Incident~~	~~That meets the criteria in CIP-008~~
BES~~-~~ Emergency requiring public appeal for load reduction	~~Deficient~~Initiating entity is responsible for reporting	~~Each public~~Public appeal for load reduction event
BES Emergency requiring system-wide voltage reduction	Initiating entity is responsible for reporting	System wide voltage reduction of 3% or more
BES Emergency requiring manual firm load shedding	Initiating entity is responsible for reporting	Manual firm load shedding ≥ 100 MW
BES Emergency resulting in automatic firm load shedding	Each DP or TOP that ~~experiences the~~implements automatic load shedding	Firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)
Voltage ~~deviations~~deviation on ~~BES Facilities~~a Facility	Each ~~-~~TOP that ~~experiences~~observes the voltage deviation	± 10% sustained for ≥ 15 continuous minutes

[3] ~~Examples include a train derailment adjacent to BES equipment that either could have damaged the equipment directly or has the potential to damage the equipment (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center) and report of suspicious device near BES equipment.~~

[4] Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility.

Event	Entity with Reporting Responsibility	Threshold for Reporting
IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only)	Each RC that experiences the IROL Violation (all Interconnections) or SOL violation for Major WECC Transfer Paths (WECC only)	Operate outside the IROL for time greater than IROL T_v (all Interconnections) or Operate outside the SOL for ~~a time greater~~more than ~~the SOL T_v~~30 minutes for Major WECC Transfer Paths (WECC only).
Loss of ~~Firm~~firm load for ≥ 15 Minutes	Each BA, TOP, DP that experiences the loss of firm load	• ≥ 300 MW for entities with previous year's demand ≥ ~~3000~~3,000 MW • ≥ 200 MW for all other entities
System ~~Separation (Islanding~~separation (islanding)	Each RC, BA, TOP, DP that experiences the system separation	Each separation resulting in an island of generation and load ≥ 100 MW
Generation loss	Each BA, GOP that experiences the generation loss	• ≥ 2,000 MW for entities in the Eastern or Western Interconnection • ≥ ~~1000~~1,000 MW for entities in the ERCOT or Quebec Interconnection
~~Loss~~Complete loss of ~~Off~~off-site power to a nuclear generating plant (grid supply)	Each TO, TOP that experiences the complete loss of off-site power to a nuclear generating plant	Affecting a nuclear generating station per the Nuclear Plant Interface Requirement
Transmission loss	Each TOP that experiences the transmission loss	Unintentional loss of ~~Three~~three or more Transmission Facilities (excluding successful automatic reclosing)
Unplanned ~~Control Center~~control center evacuation	Each RC, BA, TOP that experiences the ~~potential~~ event	Unplanned evacuation from BES control center facility for 30 minutes or more.
Loss of all voice communication capability	Each RC, BA, TOP that experiences the loss of all voice communication capability	Affecting a BES control center for ≥ 30 continuous minutes
~~Loss~~Complete or partial loss of monitoring ~~or all voice communication~~ capability	Each RC, BA, TOP that experiences the complete or partial loss of monitoring ~~or all voice communication~~ capability	~~Voice Communications: Affecting a BES control center for ≥ 30 continuous minutes~~ ~~Monitoring:~~ Affecting a BES control center for ≥ 30 continuous minutes such that analysis tools (State Estimator, Contingency

Event	Entity with Reporting Responsibility	Threshold for Reporting
		Analysis) are rendered inoperable.

EOP-004 - Attachment 2: Event Reporting Form

EOP-004~~,~~ Attachment 2: Event Reporting Form

~~This~~Use this form ~~is to be used~~ to report events ~~to parties listed in Attachment 1, column labeled "Submit Attachment 2 or DOE OE-417 Report to:". These parties~~. The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. ~~Reports should be submitted~~ Submit reports to the ERO via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422.

	Task	Comments
1.	Entity filing the report include: Company name: Name of contact person: Email address of contact person: Telephone Number: Submitted by (name):	
2.	Date and Time of recognized event. Date: (mm/dd/yyyy) Time: (hh:mm) Time/Zone:	
3.	Did the ~~actual or potential~~ event originate in your system?	~~Actual event ☐ Potential event ☐~~ Yes ☐ No☐ Unknown ☐
4.	**Event Identification and Description:**	
	(Check applicable box) ☐ public appeal ☐ voltage reduction ☐ manual firm load shedding ☐ firm load shedding(undervoltage, underfrequency, SPS/RAS) ☐ voltage deviation ☐ IROL violation ☐ loss of firm load ☐ system separation (islanding) ☐ generation loss ☐ complete loss of off-site power to nuclear generating plant ☐ transmission loss ☐ damage or destruction of ~~BES equipment~~Facility ~~☐ damage or destruction of Critical Asset~~ ~~☐ damage or destruction of Critical Cyber Asset~~ ☐ unplanned control center evacuation ~~☐ fuel supply emergency~~ ☐ loss of all ~~monitoring or~~ voice communication capability	Written description (optional ~~unless Other is checked~~):

EOP-004~~,~~ Attachment 2: Event Reporting Form		
~~This~~Use this form ~~is to be used~~ to report events ~~to parties listed in Attachment 1, column labeled "Submit Attachment 2 or DOE OE-417 Report to:". These parties~~. The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. ~~Reports should be submitted~~ Submit reports to the ERO via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422.		
Task		**Comments**
	☐ ~~forced intrusion Risk to BES equipment~~complete or partial loss of monitoring capability ☐ physical threat that could impact the operability of a Facility ☐ reportable Cyber Security Incident ~~☐ other~~	

Guideline and Technical Basis

Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01) - Reporting Concepts

Introduction

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and has developed updated standards based on the SAR.

The standards listed under the SAR are:

- CIP-001 — Sabotage Reporting
- EOP-004 — Disturbance Reporting

The changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). These standard deals exclusively with after-the-fact reporting.

The DSR SDT has consolidated disturbance and sabotage event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts and Assumptions:

The Standard:

- Requires reporting of "events" that impact or may impact the reliability of the ~~bulk electric system~~Bulk Electric System
- Provides clear criteria for reporting
- Includes consistent reporting timelines
- Identifies appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- Provides clarity around of who will receive the information

Discussion of Disturbance Reporting

Disturbance reporting requirements existed in the previous version of EOP-004. The current approved definition of Disturbance from the NERC Glossary of Terms is:

1. An unplanned event that produces an abnormal system condition.
2. Any perturbation to the electric system.

3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.

Disturbance reporting requirements and criteria were in the previous EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and developed the list of events that are to be reported under this standard (~~attachment~~EOP-004 Attachment 1).

Discussion of Event Reporting
There are situations worthy of reporting because they have the potential to impact reliability.

~~t~~ Event reporting facilitates industry awareness, which allows potentially impacted parties to prepare for and possibly mitigate any associated reliability risk. It also provides the raw material, in the case of certain potential reliability threats, to see emerging patterns.

Examples of such events include:

- Bolts removed from transmission line structures
- Detection of cyber intrusion that meets criteria of CIP-008-3 or its successor standard
- Forced intrusion attempt at a substation
- Train derailment near a transmission right-of-way
- Destruction of Bulk ~~Electrical~~Electric System equipment

What about sabotage?
One thing became clear in the DSR SDT's discussion concerning sabotage: everyone has a different definition. The current standard CIP-001 elicited the following response from FERC in FERC Order 693, paragraph 471 which states in part: *". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."*

Often, the underlying reason for an event is unknown or cannot be confirmed. The DSR SDT believes that by reporting material risks to the Bulk ~~Electrical~~Electric System using the event categorization in this standard, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.

Certain types of events should be reported to NERC, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and/or Provincial or local law enforcement. Other types of ~~impact~~ events may have different reporting requirements. For example, an event that is related to copper theft may only need to be reported to the local law enforcement authorities.

Potential Uses of Reportable Information
Event analysis, correlation of data, and trend identification are a few potential uses for the information reported under this standard. The standard requires Functional entities to report the incidents and provide known information at the time of the report. Further data gathering

necessary for event analysis is provided for under the Events Analysis Program and the NERC Rules of Procedure. Other entities (e.g. – NERC, Law Enforcement, etc) will be responsible for performing the analyses. The NERC Rules of Procedure (section 800) provide an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for reliability. Jurisdictional agencies (which may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE) have other duties and responsibilities.

Collection of Reportable Information or "One stop shopping"

The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT has updated the listing of reportable events in EOP-004 Attachment 1 based on discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences still exist.

The reporting required by this standard is intended to meet the uses and purposes of NERC. The DSR SDT recognizes that other requirements for reporting exist (e.g., DOE-417 reporting), which may duplicate or overlap the information required by NERC. To the extent that other reporting is required, the DSR SDT envisions that duplicate entry of information should not be necessary, and the submission of the alternate report will be acceptable to NERC so long as all information required by NERC is submitted. For example, if the NERC Report duplicates information from the DOE form, the DOE report may be included or attached to the NERC report, in lieu of entering that information on the NERC report.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Comment Form

Project 2009-01 Disturbance and Sabotage Reporting

Please DO NOT use this form for submitting comments. Please use the electronic form to submit comments on the draft standard EOP-004-2. Comments must be submitted by May 24, 2012. If you have questions please contact Stephen Crutchfield by email or by telephone at (609) 651-9455.

Background Information

EOP-004-2 was posted for a 45-day formal comment period and initial ballot from October 28 through December 12, 2011. The DSR SDT received comments from stakeholders to improve the readability and clarity of the requirements of the standard. The revisions that were made to the standard are summarized in the following paragraphs.

Purpose Statement
The DSR SDT revised the purpose statement to remove ambiguous language "with the potential to impact reliability." The Purpose statement now reads:

> "To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities."

Operating Plan
Based on stakeholder comments, Requirement R1 was revised for clarity. Part 1.1 was revised to replace the word "identifying" with "recognizing" and Part 1.2 was eliminated. This also aligns the language of the standard with FERC Order 693, Paragraph 471.

> "(2) specify baseline requirements regarding what issues should be addressed in the **procedures for recognizing** {emphasis added} sabotage events and making personnel aware of such events;"

Requirement R1, Part 1.3 (now Part 1.2) was revised by eliminating the phrase "as appropriate" and adding language indicating that the Responsible Entity is to define its process for reporting and with whom to report events. Part 1.2 now reads:

> "1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies."

The SDT envisions that most entities will only need to slightly modify their existing CIP-001 Sabotage Reporting procedures to comply with the Operating Plan requirement in this proposed standard. As many of the features of both sabotage reporting procedures and the Operating Plan are substantially similar, the SDT feels that some information in the sabotage reporting procedures may need to updated and verified.

Operating Plan Review and Communications Testing
Requirement R1, Part 1.4 was removed and Requirement 1, Part, 1.5 was separated out as new Requirement 4. Requirement R4 was revised and is now R3. FERC Order 693, Paragraph 466 includes provisions for periodic review and update of the Operating Plan:

> "466. The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."

Requirement R3 requires an annual test of the communication portion of Requirement R1 while Requirement R4 requires an annual review of the Operating Plan.:

> "R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2."

> "R4. Each Responsible Entity shall conduct an annual review of the event reporting Operating Plan in Requirement R1."

The DSR SDT envisions that the annual test will include verification that communication information contained in the Operating Plan is correct. As an example, the annual update of the Operating Plan could include calling "others as defined in the Responsibility Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. Note that there is no requirement to test the reporting of events to the Electric Reliability Organization and the Responsible Entity's Reliability Coordinator.

Operating Plan Implementation
Most stakeholders indicated that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to:

> "R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1."

Reporting Timelines

The DSR SDT received many comments regarding the various entries of Attachment 1. Many commenters questioned the reliability benefit of reporting events to the ERO within 1 hour. Most of the events with a one hour reporting requirement were revised to 24 hours based on stakeholder comments; those types of events are currently required to be reported within 24 hours in the existing mandatory and enforceable standards. The only remaining type of event that is to be reported within one hour is "A reportable Cyber Security Incident" as it is required by CIP-008 and FERC Order 706, Paragraph 673:

> "direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…"

The table was reformatted to separate one-hour reporting and 24-hour reporting. The last column of the table was also deleted and the information contained in the table was transferred to the sentence above each table. These sentences are:

> "One Hour Reporting: Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the event."
>
> "Twenty-four Hour Reporting: Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within twenty-four hour of recognition of the event."

Note that the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.

Cyber-Related Events

The 'Damage or Destruction' events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1. Stakeholders pointed out these events are adequately addressed through the CIP-008 and "Damage or Destruction of a Facility"reporting thresholds.

CIP-008 addresses Cyber Security Incidents which are defined as:

> "Any malicious act or suspicious event that:
>
> • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,
>
> • Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset."

A Critical Asset is defined as:

> "Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."

Since there is an existing event category for damage or destruction of Facilities, having a separate event for "Damage or Destruction of a Critical Asset" is unnecessary.

Damage or Destruction

The event for "Destruction of BES equipment" has been revised to "Damage or destruction of a Facility". The threshold for reporting information was expanded for clarity:

> "Damage or destruction of a Facility that:
>
> Affects an IROL (per FAC-014)
>
> OR
>
> Results in the need for actions to avoid an Adverse Reliability Impact
>
> OR
>
> Results from actual or suspected intentional human action."

Facility Definition

The DSR SDT used the defined term "Facility" to add clarity for this event as well as other events in Attachment 1. A Facility is defined as:

> "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"

The DSR SDT did not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.

Physical Threats
Several stakeholders expressed concerns relating to the "Forced Intrusion" event. Their concerns related to ambiguous language in the footnote. The SDR SDT discussed this event as well as the event "Risk to BES equipment". These two event types had perceived overlap in the reporting requirements. The DSR SDT removed "Forced Intrusion" as a category and the "Risk to BES equipment" event was revised to "Any physical threat that could impact the operability of a Facility".

Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.

The footnote regarding this event type was expanded to provide additional guidance in:

> "Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also, report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility."

Use of DOE Form OE-417
The DSR SDT received many comments requesting consistency with DOE OE-417 thresholds and timelines. These items, as well as, the Events Analysis Working Group's (EAWG) requirements were considered in creating Attachment 1, but differences remain for the following reasons:

- EOP-004 requirements were designed to meet NERC and the industry's needs; accommodation of other reporting obligations was considered as an opportunity not a 'must-have'
- OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America
- NERC has no control over the criteria in OE-417, which can change at any time
- Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary

In an effort to minimize administrative burden, US entities may use the OE-417 form rather than Attachment 2 to report under EOP-004. The SDT was informed by the DOE of its new online process coming later this year. In this process, entities may be able to record email addresses associated with their Operating Plan so that when the report is submitted to DOE, it will automatically be forwarded to the posted email addresses, thereby eliminating some administrative burden to forward the report to multiple organizations and agencies.

Miscellaneous
Other minor edits were made to Attachment 1. Several words were capitalized that are not defined terms. The DSR SDT did not intend for these terms to be capitalized (defined terms) and these words were reverted to lower case. The event type "Loss of monitoring or all voice communication capability" was divided into two separate events as "Loss of monitoring capability" and "Loss of all voice communication capability".

Attachment 2 was updated to reflect the revisions to Attachment 1. The reference to "actual or potential events" was removed. Also, the event type of "other" and "fuel supply emergency" was removed as well.

It was noted that 'Transmission Facilities' is not a defined term in the NERC Glossary. Transmission and Facilities are separately defined terms. The combination of these two definitions are what the DSR SDT has based the applicability of "Transmission Facilities" in Attachment 1.

You do not have to answer all questions.

1. **The DSR SDT has revised EOP-004-2 by removing Requirement 1, Part 1.4 and separating Parts 1.3 and 1.5 into new Requirements R3 and R4. Requirement R3 calls for an annual test of the communications portion of the Operating Plan and Requirement R4 requires an annual review of the Operating Plan. Do you agree with this revision? If not, please explain in the comment area below.**

   ☐ Yes
   ☐ No
   Comments:

2. **The DSR SDT made clarifying revisions to Attachment 1 based on stakeholder feedback. Do you agree with these revisions? If not, please explain in the comment area below.**

   ☐ Yes
   ☐ No
   Comments:

3. **The DSR SDT has proposed a new Section 812 to be incorporated into the NERC Rules of Procedure. Do you agree with the proposed addition? If not, please explain in the comment area below.**

   ☐ Yes

   ☐ No

   Comments:

4. **Do you have any other comment, not expressed in the questions above, for the DSR SDT?**

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2009-01 Disturbance and Sabotage Reporting

Implementation Plan for EOP-004-2 – Event Reporting

Approvals Required
EOP-004-2 – Event Reporting

Prerequisite Approvals
None

Revisions to Glossary Terms
None

Note: Project 2008-06 is currently developing Version 5 of the CIP Cyber Security Standards, and, in conjunction with proposed CIP-008-5, the Project 2008-06 drafting team proposes to add the term, "Reportable Cyber Security Incident" to the Glossary of Terms used in NERC Reliability Standards. The proposed definition, as posted for formal comment and simultaneous successive ballot from April 12, 2012, through May 21, 2012, is, "Any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity." If the term "Reportable Cyber Security Incident" is added to the Glossary of Terms used in NERC Reliability Standards, as posted or substantially similar to the definition proposed in draft 2 of the CIP Cyber Security Standards by Project 2008-06, then the phrase "reportable Cyber Security Incident" shall be changed to "Reportable Cyber Security Incident" wherever that phrase occurs in EOP-004-2 upon the effective date of CIP-008-5.

Applicable Entities
Reliability Coordinator
Balancing Authority
Interchange Coordinator
Transmission Service provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Distribution Provider
Load-Serving Entity
Electric Reliability Organization

Regional Entity

Conforming Changes to Other Standards
None

Effective Dates
EOP-004-2 shall become effective on the first day of the third calendar quarter after applicable regulatory approval. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the third calendar quarter after Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

EOP-004-1 is in effect until EOP-004-2 is accepted by all applicable regulatory authorities. Upon acceptance by the applicable regulatory authorities, EOP-004-2 will be assigned an effective date. Until such effective date is attained, EOP-004-1 will remain in effect.

Retirements
EOP-004-1 – Disturbance Reporting and CIP-001-2a – Sabotage Reporting should be retired at midnight of the day immediately prior to the Effective Date of EOP-004-2 in the particular jurisdiction in which the new standard is becoming effective.

CIP-008-3 – Cyber Security - Incident Reporting and Response Planning: Retire Requirement R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in EOP-004-2, Requirement R2 and Attachment 1. If any successor version of the CIP-008-3 standard contains provisions for reporting Cyber Security Incidents, then those provisions should be retired upon the effective date of EOP-004-2.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2009-01 Disturbance and Sabotage Reporting

Implementation Plan for EOP-004-2 – Event Reporting

Approvals Required

EOP-004-2 – Event Reporting

Prerequisite Approvals

~~Revisions to Sections 807 and 808 of the NERC Rules of Procedure~~

~~Addition of Section 812 to the NERC Rules of Procedure~~

None

Revisions to Glossary Terms

None

Note: Project 2008-06 is currently developing Version 5 of the CIP Cyber Security Standards, and, in conjunction with proposed CIP-008-5, the Project 2008-06 drafting team proposes to add the term, "Reportable Cyber Security Incident" to the Glossary of Terms used in NERC Reliability Standards. The proposed definition, as posted for formal comment and simultaneous successive ballot from April 12, 2012, through May 21, 2012, is, "Any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity." If the term "Reportable Cyber Security Incident" is added to the Glossary of Terms used in NERC Reliability Standards, as posted or substantially similar to the definition proposed in draft 2 of the CIP Cyber Security Standards by Project 2008-06, then the phrase "reportable Cyber Security Incident" shall be changed to "Reportable Cyber Security Incident" wherever that phrase occurs in EOP-004-2 upon the effective date of CIP-008-5.

Applicable Entities

Reliability Coordinator
Balancing Authority
Interchange Coordinator
Transmission Service provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Distribution Provider

Load-Serving Entity
Electric Reliability Organization
Regional Entity

Conforming Changes to Other Standards

None

Effective Dates

EOP-004-2 shall become effective on the first day of the third calendar quarter after applicable regulatory approval. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the third calendar quarter after Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

EOP-004-1 is in effect until EOP-004-2 is accepted by all applicable regulatory authorities. Upon acceptance by the applicable regulatory authorities, EOP-004-2 will be assigned an effective date. Until such effective date is attained, EOP-004-1 will remain in effect.

Retirements

EOP-004-1 – Disturbance Reporting and CIP-001-2a – Sabotage Reporting should be retired at midnight of the day immediately prior to the Effective Date of EOP-004-2 in the particular jurisdiction in which the new standard is becoming effective.

CIP-008-~~4~~3 – Cyber Security - Incident Reporting and Response Planning: Retire Requirement R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in EOP-004-2, Requirement ~~1, Part 1.3~~R2 and Attachment 1. If any successor version of the CIP-008-3 standard contains provisions for reporting Cyber Security Incidents, then those provisions should be retired upon the effective date of EOP-004-2.

Project 2009-01 Disturbance and Sabotage Reporting Mapping Document

Translation of CIP-002-2a – Sabotage Reporting, EOP-004-1 – Disturbance Reporting and CIP-008-4 – Cyber Security – Incident Reporting and Response Planning (R 1.3), into EOP-004-2 – Impact Event and Disturbance Assessment, Analysis, and Reporting

Standard: CIP-001-2a – Sabotage Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting**
R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.	Moved into EOP-004-2, R1	R1. Each Responsible Entity shall have an Operating Plan that includes: *[Violation Risk: Factor: Lower] [Time Horizon: Operations Planning]* 1.1. A process for recognizing each of the applicable events listed in EOP-004 Attachment 1. 1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies.

R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	Moved into EOP-004-2, R1	R1. Each Responsible Entity shall have an Operating Plan that includes: *[Violation Risk: Factor: Lower] [Time Horizon: Operations Planning]* 1.1. A process for recognizing each of the applicable events listed in EOP-004 Attachment 1. 1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies.
R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.	Moved into EOP-004-2, R1	R1. Each Responsible Entity shall have an Operating Plan that includes: *[Violation Risk: Factor: Lower] [Time Horizon: Operations Planning]* 1.1. A process for recognizing each of the applicable events listed in EOP-004 Attachment 1. 1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies.

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.	Moved into EOP-004-2, R1	R1. Each Responsible Entity shall have an Operating Plan that includes: *[Violation Risk: Factor: Lower] [Time Horizon: Operations Planning]* 1.1. A process for recognizing each of the applicable events listed in EOP-004 Attachment 1. 1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies.

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting Comments**
R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.	Retire this fill-in-the-blank requirement. Replace with new reporting and analysis procedure developed by NERC EAWG.	The requirements of EOP-004-2 specify that an entity must report certain types of impact events. The NERC EAWG is developing continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure.
R2. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.	Translated into EOP-004-2, R1 and the NERC Events Analysis Process	The requirements of EOP-004-2 specify that an entity must report certain types of impact events. The NERC EAWG is developing continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure.
R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.	Translated into EOP-004-2, R2	R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until sometime after they occur shall be reported within 24 hours of being recognized.	Translated into EOP-004-2, R2	R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*
R3.2. Applicable reporting forms are provided in Attachments 022-1 and 022-2.	Retire – informational statement	

R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.	Retire as a requirement. Added as a "Note" to EOP-004-Attachment1-Impact Events Table	NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per Requirement R1 and provide as much information as is available at the time of the notification. Submit reports to the ERO via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422.

R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.	Retire this fill-in-the-blank requirement. Replace with new reporting procedure developed by NERC EAWG.	The requirements of EOP-004-2 specify that an entity must report certain types of impact events. The NERC EAWG is developing continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure.
R4. When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.	Retire this fill-in-the-blank requirement. Replace with new reporting procedure developed by NERC EAWG.	The requirements of EOP-004-2 specify that an entity must report certain types of impact events. The NERC EAWG is developing continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure.

R5. The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.	Retire this fill-in-the-blank requirement. Replace with new reporting procedure developed by NERC EAWG.	The requirements of EOP-004-2 specify that an entity must report certain types of impact events. The NERC EAWG is developing continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure.
Request for Interpretation of CIP-001-2a, R2: Please clarify what is meant by the term, "appropriate parties." Moreover, who within the Interconnection hierarchy deems parties to be appropriate?	Retire the interpretation	Addressed in EOP-004-2, R1 by replacing the term, 'appropriate parties' with a broader, more specific list of specific entities to contact in Part 1.2.

Standard: CIP-008-4 – Cyber Security – Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting Comments**
R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.	Translated into EOP-004-2 Requirement 1, Part 1.2 and Attachment 1.	Cyber Security Incidents are defined as: Any malicious act or suspicious event that: • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset. Such events are listed in Attachment 1 as "Detection of a reportable Cyber Security Incident" and are events that are required to be reported under Reliability Standard EOP-004-2. Requirement R1, Part 1.2 requires the Responsible Entity to have "A process for reporting events listed in Attachment 1 to the Electric Reliability Organization,..." The note at the top of Attachment 1 includes the following: "Reports to the ERO should be submitted to one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422."

Project 2009-01 Disturbance and Sabotage Reporting Consideration of Issues and Directives

Project 2009-01 Disturbance and Sabotage Reporting		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
"What is meant by: "establish contact with the FBI"? Is a phone number adequate? Many entities which call the FBI are referred back to the local authority. The AOT noted that on the FBI website it states to contact the local authorities. Is this a question for Homeland Security to deal with for us?" Establish communications contacts, as applicable with local FBI and RCMP officials. Some entities are very remote and the sheriff is the only local authority does the FBI still need to be contacted? Registered Entities have sabotage reporting processes and procedures in place but not all personnel has been trained.	CIP-001-1 NERC Audit Observation Team	The DSR SDT has been in contact with FBI staff and developed a notification flow chart for law enforcement as it pertains to EOP-004. The "Background" section of the standard outlines the reporting hierarchy that exists between local, state, provincial and federal law enforcement. The entity experiencing an event should notify the appropriate state or provincial law enforcement agency that will then coordinate with local law enforcement for investigation. These local, state and provincial agencies will coordinate with higher levels of law enforcement or other governmental agencies.

Question: How do you “and make the operator aware”	CIP-001-1 NERC Audit Observation Team	This has been removed from the standard. Requirement R1, Part 1.1 requires that the entity has a process for recognizing events.
How does this standard pertain to Load Serving Entities, LSE's.	CIP-001-1 NERC Audit Observation Team	LSE is an applicable entity since LSEs are currently applicable under CIP-008.
We direct the ERO to explore ways to address these concerns – including central coordination of sabotage reports and a uniform reporting format – in developing modifications to the Reliability Standard with the appropriate governmental agencies that have levied the reporting requirements.	CIP-001-1; Order 693	See “Background” section of the standard.

"Define “sabotage” and provide guidance on triggering events that would cause an entity to report an event. Paragraph 461. Several commenters agree with the Commission’s concern that the term “sabotage” should be defined. For the reasons stated in the NOPR, we direct that the ERO further define the term and provide guidance on triggering events that would cause an entity to report an event. However, we disagree with those commenters that suggest the term “sabotage” is so vague as to justify a delay in approval or the application of monetary penalties. As explained in the NOPR, we believe that the term sabotage is commonly understood and that common understanding should suffice in most instances.	CIP-001-1; Order 693	The DSR SDT has not proposed a definition for inclusion in the NERC Glossary because it is impractical to define every event that should be reported without listing them in the definition. Attachment 1 is the de facto definition of “event”. The DSR SDT considered the FERC directive to “further define sabotage” and decided to eliminate the term sabotage from the standard. The team felt that without the intervention of law enforcement after the fact, it was almost impossible to determine if an act or event was that of sabotage or merely vandalism. The term “sabotage” is no longer included in the standard and therefore it is inappropriate to attempt to define it. The events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

The ERO should consider suggestions raised by commenters such as FirstEnergy and Xcel to define the specified period for reporting an incident beginning from when an event is discovered or suspected to be sabotage, and APPA's concerns regarding events at unstaffed or remote facilities, and triggering events occurring outside staffed hours at small entities.	CIP-001-1; Order 693	Attachment 1 defines the timelines and events which are to be reported under this standard. The required reporting is either one hour or 24 hours (depending on the type of event) "of recognition of the event."

Modify CIP-001-1 1 to require an applicable entity to contact appropriate governmental authorities in the event of sabotage within a specific period of time, even if it is a preliminary report. Further, in the interim while the matter is being addressed by the Reliability Standards development process, we direct the ERO to provide advice to entities that have concerns about the reporting of particular circumstances as they arise.	CIP-001-1; Order 693	Per Requirement R1, the entity is to develop procedure(s) that include event reporting to law enforcement and governmental agencies. The DSR SDT also proposes revisions to the NERC Rules of Procedure to report events to the FERC. 812. NERC will establish a system to collect report forms as established for this section or standard, from any Registered Entities, pertaining to data requirements identified in Section 800 of this Procedure. Upon receipt of the submitted report, the system shall then forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary. This can include state, federal, and provincial organizations.

Consider the need for wider application of the standard. Consider whether separate, less burdensome requirements for smaller entities may be appropriate. Paragraph 458. The Commission acknowledges the concerns of the commenters about the applicability of CIP-001-1 to small entities and has addressed the concerns of small entities generally earlier in this Final Rule. Our approval of the ERO Compliance Registry criteria to determine which users, owners and operators are responsible for compliance addresses the concerns of APPA and others. 459. However, the Commission believes that there are specific reasons for applying this Reliability Standard to such entities, as discussed in the NOPR. APPA indicates that some small LSEs do not own or operate "hard assets" that are normally thought of as "at risk" to sabotage. The Commission is concerned that, an adversary might determine that a small LSE is the appropriate target when the adversary aims at a particular population or facility. Or an adversary may target a small user, owner or operator because it may have similar equipment or protections as a larger facility, that is, the adversary may use an attack against a smaller facility as a training "exercise." {continued below}	CIP-001-1; Order 693	Attachment 1 defines the timelines and events which are to be reported under this standard. The applicable entities are also identified for each type of event.

The knowledge of sabotage events that occur at any facility (including small facilities) may be helpful to those facilities that are traditionally considered to be the primary targets of adversaries as well as to all members of the electric sector, the law enforcement community and other critical infrastructures. 460. For these reasons, the Commission remains concerned that a wider application of CIP-001-1 may be appropriate for Bulk Power System reliability. Balancing these concerns with our earlier discussion of the applicability of Reliability Standards to smaller entities, we will not direct the ERO to make any specific modification to CIP-001-1 to address applicability. However, we direct the ERO, as part of its Work Plan, to consider in the Reliability Standards development process, possible revisions to CIP-001-1 that address our concerns. Regarding the need for wider application of the Reliability Standard. Further, when addressing such applicability issues, the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate to address these concerns.		

The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures. At this time, the commission does not specify a review period as suggested by FirstEnergy and MRO and, rather, believes that the appropriate period should be determined through the ERO's Reliability Standards development process. However, the Commission directs that the ERO begin this process by considering a staggered schedule of annual testing of the procedures with modifications made when warranted formal review of the procedures every two or three years.	CIP-001-1; Order 693	The standard is responsive this directive with the following language in Requirement R3: R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. The DSR SDT envisions that this will include verification that contact information contained in the Operating Plan is correct. As an example, the annual update of the Operating Plan could include calling others as defined in the Responsibility Entity's Operating Plan (see Part 1.2) to verify that their contact information is correct and current. If any discrepancies are noted, the Operating Plan would be updated.

Consider FirstEnergy's suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality. Paragraph 451. A number of commenters agree with the Commission's concern that the term sabotage" needs to be better defined and guidance provided on the triggering events that would cause an entity to report an event. FirstEnergy states that this definition should differentiate between cyber and physical sabotage and should exclude unintentional operator error. It advocates a threshold of materiality to exclude acts that do not threaten to reduce the ability to provide service or compromise safety and security. SoCal Edison states that clarification regarding the meaning of sabotage and the triggering event for reporting would be helpful and prevent over reporting.	CIP-001-1; Order 693	This addressed in Attachment 1. There are specific event types for both cyber and physical security with their respective report submittal requirements.

"Include a requirement to report a sabotage event to the proper government authorities. Develop the language to specifically implement this directive. Paragraph 467. CIP-001-1, Requirement R4, requires that each applicable entity establish communications contacts, as applicable, with the local FBI or Royal Canadian Mounted Police officials and develop reporting procedures as appropriate to its circumstances. The Commission in the NOPR expressed concern that the Reliability Standard does not require an applicable entity to actually contact the appropriate governmental or regulatory body in the event of sabotage. Therefore, the Commission proposed that NERC modify the Reliability Standard to require an applicable entity to "contact appropriate federal authorities, such as the Department of Homeland Security, in the event of sabotage within a specified period of time."212 468. As mentioned above, NERC and others object to the wording of the proposed directive as overly prescriptive and note that the reference to "appropriate federal authorities" fails to recognize the international application of the Reliability Standard. The example of the Department of Homeland Security as an "appropriate federal authority" was not intended to be an exclusive designation. Nonetheless, the Commission agrees that a reference to "federal authorities" could create confusion. Accordingly, we modify the direction in the NOPR and now direct the ERO to address our underlying concern regarding mandatory reporting of a sabotage event. The ERO's Reliability Standards development process should develop the language to implement this directive."		See Background section of Standard. A proposal discussed with FBI, FERC Staff, NERC Standards Project Coordinator and SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Event EOP-004-2). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial level law enforcement agency. The state or provincial level law enforcement agency will coordinate with local law enforcement to investigate. If the state or provincial level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial level law enforcement agency will notify and coordinate with the FBI or the RCMP.

On March 4, 2008, NERC submitted a compliance filing in response to a December 20, 2007 Order, in which the Commission reversed a NERC decision to register three retail power marketers to comply with Reliability Standards applicable to load serving entities (LSEs) and directed NERC to submit a plan describing how it would address a possible "reliability gap" that NERC asserted would result if the LSEs were not registered. NERC's compliance filing included the following proposal for a short-term plan and a long-term plan to address the potential gap: · Short-term: Using a posting and open comment process, NERC will revise the registration criteria to define "Non-Asset Owning LSEs" as a subset of Load Serving Entities and will specify the reliability standards applicable to that subset. · Longer-term: NERC will determine the changes necessary to terms and requirements in reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers and process them through execution of the three-year Reliability Standards Development Plan. In this revised Reliability Standards Development Plan, NERC is commencing the implementation of its stated long-term plan to address the issues surrounding accountability for loads served by retail marketers/suppliers. The NERC Reliability Standards Development Procedure will be used to identify the changes necessary to terms and requirements in reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. Specifically, the following description has been incorporated into the scope for	CIP-001-1 and EOP-004 ORDER ON ELECTRIC RELIABILITY ORGANIZATION REGISTRY_DETERMINATIONS; ORDER ON COMPLIANCE FILING	The LSE is an applicable entity, since LSEs are currently applicable under CIP-008. If an entity owns distribution assets, that entity will be registered as a Distribution Provider. Attachment 1 defines the timelines and events which are to be reported under this standard. The applicable entities are also identified for each type of event.

affected projects in this revised Reliability Standards Development Plan that includes a standard applicable to Load Serving Entities: Source: FERC's December 20, 2007 Order in Docket Nos. RC07-004-000, RC07-6-000, and RC07-7-000. Issue: In FERC's December 20, 2007 Order, the Commission reversed NERC's Compliance Registry decisions with respect to three load serving entities in the ReliabilityFirst (RFC) footprint. The distinguishing feature of these three LSEs is that none own physical assets. Both NERC and RFC assert that there will be a "reliability gap" if retail marketers are not registered as LSEs. To avoid a possible gap, a consistent, uniform approach to ensure that appropriate Reliability Standards and associated requirements are applied to retail marketers must be followed. Each drafting team responsible for reliability standards that are applicable to LSEs is to review and change as necessary, requirements in the reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. For additional information see: · FERC's December 20, 2007 Order (http://www.nerc.com/files/LSE_decision_order.pdf) · NERC's March 4, 2008 (http://www.nerc.com/files/FinalFiledLSE3408.pdf), · FERC's April 4, 2008 Order (http://www.nerc.com/files/AcceptLSECompFiling-040408.pdf), and · NERC's July 31, 2008 (http://www.nerc.com/files/FinalFiled-compFiling-LSE-07312008.pdf) compliance filings to FERC on this subject.		

Object to multi-site requirement	Version 0 Team CIP-001-1	The Standard was revised for clarity. Attachment 1 defines the timelines and events which are to be reported under this standard. The applicable entities are also identified for each type of event.
Definition of sabotage required VRFs Team Adequate procedures will insure it is unlikely to lead to bulk electric system instability, separation, or cascading failures.	Version 0 Team CIP-001-1	No definition for sabotage was developed The DSR SDT has not proposed a definition for inclusion in the NERC Glossary because it is impractical to define every event that should be reported without listing them in the definition. Attachment 1 is the de facto definition of "event". The DSR SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that without the intervention of law enforcement after the fact, it was almost impossible to determine if an act or event was that of sabotage or merely vandalism. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

Coordination and follow up on lessons learned from event analyses Consider adding to EOP-004 – Disturbance Reporting Proposed requirement: Regional Entities (REs) shall work together with Reliability Coordinators, Transmission Owners, and Generation Owners to develop an Event Analysis Process to prevent similar events from happening and follow up with the recommendations. This process shall be defined within the appropriate NERC Standard	Events Analysis Team Reliability Issue	The DSR SDT envisions EOP-004-2 to be a reporting standard. Any follow up investigation or analysis falls under the purview of the NERC Events Analysis Program under the NERC Rules of Procedure.
Consider changes to R1 and R3.4 to standardize the disturbance reporting requirements (requirements for disturbance reporting need to be added to this standard). Regions currently have procedures, but not in the form of a standard. The drafting team will need to review regional requirements to determine reporting requirements for the North American standard.	Fill in the Blank Team	The DSR SDT envisions EOP-004-2 to be a continent-wide reporting standard. Any follow up investigation or analysis falls under the purview of the NERC Events Analysis Program under the NERC Rules of Procedure.
Can there be a violation without an event?	NERC Audit Observation Team	The DSR SDT envisions EOP-004-2 to be a continent-wide reporting standard. In the opinion of the DSR SDT, there cannot be a violation of Requirement R2 without an event. Since Requirement R1 calls for an Operating Plan, there can be a violation of R1 without an event.

Consider APPA's concern about generator operators and LSEs analyzing performance of their equipment and provide data and information on the equipment to assist others with analysis. Paragraph 607. APPA is concerned about the scope of Requirement R2 because, in its opinion, Requirement R2 appears to impose an open-ended obligation on entities such as generation operators and LSEs that may have neither the data nor the tools to promptly analyze disturbances that could have originated elsewhere. APPA proposes that Requirement R2 be modified to require affected entities to promptly begin analyses to ensure timely reporting to NERC and DOE.	EOP-004-1 Order 693	The DSR SDT envisions EOP-004-2 to be a continent-wide reporting standard. Any follow up investigation or analysis falls under the purview of the NERC Events Analysis Program under the NERC Rules of Procedure.

From: David Cook Sent: Wednesday, July 16, 2008 6:06 PM To: Rick Sergel; Dave Nevius; David A. Whiteley; Management Subject: RE: FERC request for DOE-417s I agree the real fix is to revise the EOP-004 standard. I agree that we can't (and shouldn't try) to do that by way of amendments to our Rules of Procedure. So we should include that fix in the standards work plan, do the best we can in the meantime to provide FERC with the 417s, and I'll have the conversation with Joe McClelland about not being able to do what the Commission directed in Order 693 (i.e., change the standards by way of a change in the Rules of Procedure). David	EOP-004-1 Other	Per Requirement R1, the entity is to develop procedure(s) that include event reporting to law enforcement and governmental agencies. The DSR SDT also proposes revisions to the NERC Rules of Procedure to report events to the FERC. 812. NERC will establish a system to collect report forms as established for this section or standard, from any Registered Entities, pertaining to data requirements identified in Section 800 of this Procedure. Upon receipt of the submitted report, the system shall then forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary. This can include state, federal, and provincial organizations.

In response to a SAR submitted by Glenn Kaht of ReliabilityFirst: As part of a regional compliance violation investigation, a possible reliability gap was identified related to EOP-004-1 — Disturbance Reporting. The existing standard limits reporting of generation outages to just those outages associated with loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations. This requirement has been interpreted as meaning that only generation outages that must be reported are those that occur with the loss of a bulk power transmission element. By not reporting large generation losses that occur without the loss of a bulk power transmission element, the industry is overlooking a potential opportunity to identify and learn from these losses. Specifically, Item 1 of Attachment 1 of EOP-004 requires the reporting of events if "The loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations. Generally, a disturbance report will be required if the event results in actions such as:" The Standard then lists six different actions that may occur as a result of the event in order to be reportable. All six of these actions appear to be dependent on "The loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations" in order for the event to be reportable. Some of these events may significantly impact the reliable operation of the bulk power system. Consider a revision to EOP-004-1 — Disturbance Reporting requiring a Generator Operator (GOP) that	Standards Committee Action From 01/13/2010	The DSR SDT has worked closely with the NERC EAWG to develop the event reporting requirements shown in Attachment 1. The EAWG and the DSR SDT considered this request and weighed it against reliability needs for reporting.

experiences the loss of generation greater than 500 MW that results in modification of equipment (e.g. control systems, or Power Load Unbalancer (PLU)) to be a reportable event.		
too many reports, narrow requirement to RC	Version 0 Team	There is only one report required under this standard. An entity may submit the report using Attachment 2 or the DEO OE-417 report form.
How does this apply to generator operator?	Version 0 Team	See attachment 1 for specific generator operator applicability.

Violation Risk Factor and Violation Severity Level Assignments

Project 2009-01 – Disturbance and Sabotage Reporting

This document provides the drafting team's justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in

EOP-004-2 — Event Reporting

Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the ERO Sanction Guidelines.

Justification for Assignment of Violation Risk Factors in EOP-004-2

The Disturbance and Sabotage Reporting Standard Drafting Team applied the following NERC criteria when proposing VRFs for the requirements in EOP-004-2:

High Risk Requirement
A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement
A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

The SDT also considered consistency with the FERC Violation Risk Factor Guidelines for setting VRFs:[1]

Guideline (1) — Consistency with the Conclusions of the Final Blackout Report
The Commission seeks to ensure that Violation Risk Factors assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System.

In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:[2]

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) — Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement Violation Risk Factor assignments and the main Requirement Violation Risk Factor assignment.

[1] North American Electric Reliability Corp., 119 FERC ¶ 61,145, order on reh'g and compliance filing, 120 FERC ¶ 61,145 (2007) ("VRF Rehearing Order").
[2] Id. at footnote 15.

Guideline (3) — Consistency among Reliability Standards

The Commission expects the assignment of Violation Risk Factors corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) — Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular Violation Risk Factor level conforms to NERC's definition of that risk level.

Guideline (5) — Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

The following discussion addresses how the SDT considered FERC's VRF Guidelines 2 through 5. The team did not address Guideline 1 directly because of an apparent conflict between Guidelines 1 and 4. Whereas Guideline 1 identifies a list of topics that encompass nearly all topics within NERC's Reliability Standards and implies that these requirements should be assigned a "High" VRF, Guideline 4 directs assignment of VRFs based on the impact of a specific requirement to the reliability of the system. The SDT believes that Guideline 4 is reflective of the intent of VRFs in the first instance and therefore concentrated its approach on the reliability impact of the requirements.

VRF for EOP-004-2:

There are four requirements in EOP-004-2. Requirement R1 was assigned a Lower VRF while Requirements R2, R3 and R4 were assigned a Medium VRF.

VRF for EOP-004-2, Requirements R1:

- FERC's Guideline 2 — Consistency within a Reliability Standard. The Requirement specifies which entities are required to have processes for recognition of events and for communicating with other entities. This Requirement is the only administrative Requirement within the Standard. The VRF is only applied at the Requirement level. FERC's Guideline 3 — Consistency among Reliability Standards. This requirement calls for an entity to have processes for recognition of events and communicating with other entities. This requirement is administrative in nature and deals with the means to report events after the fact. Most event reporting requirements in Attachment 1 are for 24 hours after an event has occurred. The current approved VRFs for EOP-004-1 are all lower with the

exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program.

- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. Failure to have an event reporting Operating Plan is not likely to directly affect the electrical state or the capability of the bulk electric system. , Development of the Operating Plan is a requirement that is administrative in nature and is in a planning time frame that, if violated, would not, under emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system.. Therefore this requirement was assigned a Lower VRF.
- FERC's Guideline 5 — Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R1 contains only one objective which is to have an Operating Plan with two distinct processes. The content of the Operating Plan is specified in Parts 1.1-1.2. Since the requirement is to have an Operating Plan, only one VRF was assigned.

VRF for EOP-004-2, Requirement R2:

- FERC's Guideline 2 — Consistency within a Reliability Standard. This Requirement calls for the Responsible Entity to implements its Operating Plan and is assigned a Medium VRF. There are two other Requirements in this Standard which specify an annual test of the Operating Plan (R3) and an annual review of the Operating Plan (R4). Each of these Requirements is assigned a Medium VRF.
- FERC's Guideline 3 — Consistency among Reliability Standards. EOP-004-2, Requirement R2 is a requirement for entities to report events using the process for recognition of events per Requirement R1. Failure to report events is not likely to "directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system." However, violation of a medium risk requirement should also be "unlikely to lead to bulk electric system instability, separation, or cascading failures…" Such an instance could occur if personnel do not report events. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. EOP-004-2, Requirement R2 mandates that Responsible Entities implement their Operating Plan. Bulk power system instability, separation, or cascading failures are not likely to occur due to a failure to notify another entity of the event failure, but there is a slight chance that it could occur. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 5 - Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R2 addresses a single objective and has a single VRF.

VRF for EOP-004-2, Requirement R3:

- FERC's Guideline 2 — Consistency within a Reliability Standard. This Requirement calls for the Responsible Entity to perform an annual test of the Operating Plan and is assigned a Medium VRF. There are two other Requirements in this Standard which specify that the Responsible Entity implement its Operating Plan (R2) and perform an annual review of the Operating Plan (R4). Each of these Requirements is assigned a Medium VRF.
- FERC's Guideline 3 — Consistency among Reliability Standards. EOP-004-2, Requirement R3 is a requirement for entities to perform an annual test of the Operating Plan. Failure to perform an annual test of the Operating Plan is not likely to "directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system." However, violation of a medium risk requirement should also be "unlikely to lead to bulk electric system instability, separation, or cascading failures…" Such an instance could occur if personnel do not perform an annual test of the Operating Plan and it is out of date or contains erroneous information. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. EOP-004-2, Requirement R3 mandates that Responsible Entities perform an annual test of the Operating Plan. Bulk power system instability, separation, or cascading failures are not likely to occur due to a failure to perform an annual test of the Operating Plan, but there is a slight chance that it could occur if the Operating Plan is out of date or contains erroneous information. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 5 - Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R3 addresses a single objective and has a single VRF.

VRF for EOP-004-2, Requirement R4:

- FERC's Guideline 2 — Consistency within a Reliability Standard. This Requirement calls for the Responsible Entity to perform an annual review of the Operating Plan and is assigned a Medium VRF. There are two other Requirements in this Standard which specify that the Responsible Entity implement its Operating Plan (R2) and perform an annual test of the Operating Plan (R3). Each of these Requirements is assigned a Medium VRF.
- FERC's Guideline 3 — Consistency among Reliability Standards. EOP-004-2, Requirement R4 is a requirement for entities to perform an annual test of the Operating Plan. Failure to perform an annual review of the Operating Plan is not likely to "directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system." However, violation of a medium risk requirement should also be "unlikely to lead to bulk electric system instability, separation, or cascading failures…" Such an instance could occur if personnel do not perform an annual review of the Operating Plan and it is out of date or contains erroneous information. Therefore, this requirement was assigned a Medium VRF.

- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. EOP-004-2, Requirement R4 mandates that Responsible Entities perform an annual review of the Operating Plan. Bulk power system instability, separation, or cascading failures are not likely to occur due to a failure to notify another entity of the event failure, but there is a slight chance that it could occur if the Operating Plan is out of date or contains erroneous information. Therefore, this requirement was assigned a Medium VRF.

- FERC's Guideline 5 - Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R4 addresses a single objective and has a single VRF.

Justification for Assignment of Violation Severity Levels for EOP-004-2:

In developing the VSLs for the EOP-004-2 standard, the SDT anticipated the evidence that would be reviewed during an audit, and developed its VSLs based on the noncompliance an auditor may find during a typical audit. The SDT based its assignment of VSLs on the following NERC criteria:

Lower	Moderate	High	Severe
Missing a minor element (or a small percentage) of the required performance The performance or product measured has significant value as it almost meets the full intent of the requirement.	Missing at least one significant element (or a moderate percentage) of the required performance. The performance or product measured still has significant value in meeting the intent of the requirement.	Missing more than one significant element (or is missing a high percentage) of the required performance or is missing a single vital component. The performance or product has limited value in meeting the intent of the requirement.	Missing most or all of the significant elements (or a significant percentage) of the required performance. The performance measured does not meet the intent of the requirement or the product delivered cannot be used in meeting the intent of the requirement.

FERC's VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in EOP-004-2 meet the FERC Guidelines for assessing VSLs:

Guideline 1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

> Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline 2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

> A violation of a "binary" type requirement must be a "Severe" VSL.
>
> Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline 3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline 4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

. . . unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VSLs for EOP-004-2 Requirements R1:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R1	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is a revision of CIP-001-1, R1-R4, and EOP-004-1, R2. Since the Requirement has three Parts, the VSLs were developed to count a violation of each Part equally. Therefore, three VSLs were developed.	The proposed VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSLs use the same terminology as used in the associated requirement, and are, therefore, consistent with the requirement.	The VSLs are based on a single violation and not cumulative violations.

VSLs for EOP-004-2 Requirement R2:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R2	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is a revision of EOP-004-1, R3. There is only a Severe VSL for that requirement. However, the reporting of events is based on timing intervals listed in EOP-004 Attachment 1. Based on the VSL Guidance, the DSR SDT developed four VSLs based on tardiness of the submittal of the report. If a report is not submitted, then the VSL is Severe. This maintains the current VSL.	The proposed VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSLs use the same terminology as used in the associated requirement, and are, therefore, consistent with the requirement.	The VSLs are based on a single violation and not cumulative violations.

VSLs for EOP-004-2 Requirement R3:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R3	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is a new Requirement. The test of the Operating Plan is based on the calendar year. Based on the VSL Guidance, the DSR SDT developed four VSLs based on tardiness of the submittal of the report. If a test is not performed, then the VSL is Severe.	The proposed VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSLs use the same terminology as used in the associated requirement, and are, therefore, consistent with the requirement.	The VSLs are based on a single violation and not cumulative violations.

VSLs for EOP-004-2 Requirement R4:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R3	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is a new Requirement. The review of the Operating Plan is based on the calendar year. Based on the VSL Guidance, the DSR SDT developed four VSLs based on tardiness of the submittal of the report. If a review is not performed, then the VSL is Severe.	The proposed VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSLs use the same terminology as used in the associated requirement, and are, therefore, consistent with the requirement.	The VSLs are based on a single violation and not cumulative violations.

The Project 2009-01 Disturbance and Sabotage Reporting SDT has drafted the following addition to the NERC Rules of Procedure to support the reporting of events as required by the directive in Order No. 693 P 470.

SECTION 800 — RELIABILITY ASSESSMENT AND PERFORMANCE ANALYSIS

812. NERC Reporting Clearinghouse

NERC will establish a system to collect report forms as established for this section or standard, from any Registered Entities, pertaining to data requirements identified in Section 800 of this Procedure. Upon receipt of the submitted report, the system shall then forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary. This can include state, federal, and provincial organizations.

A. Introduction

1. **Title:** **Sabotage Reporting**

2. **Number:** CIP-001-2a

3. **Purpose:** Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.

4. **Applicability**

   4.1. Reliability Coordinators.

   4.2. Balancing Authorities.

   4.3. Transmission Operators.

   4.4. Generator Operators.

   4.5. Load Serving Entities.

   4.6. Transmission Owners (only in ERCOT Region).

   4.7. Generator Owners (only in ERCOT Region).

5. **Effective Date:** ERCOT Regional Variance will be effective the first day of the first calendar quarter after applicable regulatory approval.

B. Requirements

R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.

R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

C. Measures

M1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement 1

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements 2 and 3.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to procedures, policies, a letter of understanding, communication records, or other equivalent evidence that will be used to confirm that it has established communications contacts with the applicable, local FBI or RCMP officials to communicate sabotage events (Requirement 4).

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organizations shall be responsible for compliance monitoring.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to verify compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Reliability Coordinator, Transmission Operator, Generator Operator, Distribution Provider, and Load Serving Entity shall have current, in-force documents available as evidence of compliance as specified in each of the Measures.

If an entity is found non-compliant the entity shall keep information related to the non-compliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance:

2.1. Level 1: There shall be a separate Level 1 non-compliance, for every one of the following requirements that is in violation:

2.1.1 Does not have procedures for the recognition of and for making its operating personnel aware of sabotage events (R1).

2.1.2 Does not have procedures or guidelines for the communication of information concerning sabotage events to appropriate parties in the Interconnection (R2).

2.1.3 Has not established communications contacts, as specified in R4.

2.2. **Level 2:** Not applicable.

2.3. **Level 3:** Has not provided its operating personnel with sabotage response procedures or guidelines (R3).

2.4. **Level 4:**.Not applicable.

E. ERCOT Interconnection-wide Regional Variance

Requirements

EA.1. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.

EA.2. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

EA.3. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

EA.4. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall establish communications contacts with local Federal Bureau of Investigation (FBI) officials and develop reporting procedures as appropriate to their circumstances.

Measures

M.A.1. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement EA1.

M.A.2. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements EA2 and EA3.

M.A.3. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to, procedures, policies, a letter of understanding, communication records,

or other equivalent evidence that will be used to confirm that it has established communications contacts with the local FBI officials to communicate sabotage events (Requirement EA4).

Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity shall be responsible for compliance monitoring.

1.2. Data Retention

Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have current, in-force documents available as evidence of compliance as specified in each of the Measures.

If an entity is found non-compliant the entity shall keep information related to the non-compliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Amended
1	April 4, 2007	Regulatory Approval — Effective Date	New
1a	February 16, 2010	Added Appendix 1 — Interpretation of R2 approved by the NERC Board of Trustees	Addition
1a	February 2, 2011	Interpretation of R2 approved by FERC on February 2, 2011	Same addition
	June 10, 2010	TRE regional ballot approved variance	By Texas RE
	August 24, 2010	Regional Variance Approved by Texas RE Board of Directors	
2a	February 16, 2011	Approved by NERC Board of Trustees	

2a	August 2, 2011	FERC Order issued approving Texas RE Regional Variance	

Appendix 1

Requirement Number and Text of Requirement
CIP-001-1: **R2**. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.
Question
Please clarify what is meant by the term, "appropriate parties." Moreover, who within the Interconnection hierarchy deems parties to be appropriate?
Response
The drafting team interprets the phrase "appropriate parties in the Interconnection" to refer collectively to entities with whom the reporting party has responsibilities and/or obligations for the communication of physical or cyber security event information. For example, reporting responsibilities result from NERC standards IRO-001 Reliability Coordination — Responsibilities and Authorities, COM-002-2 Communication and Coordination, and TOP-001 Reliability Responsibilities and Authorities, among others. Obligations to report could also result from agreements, processes, or procedures with other parties, such as may be found in operating agreements and interconnection agreements. The drafting team asserts that those entities to which communicating sabotage events is appropriate would be identified by the reporting entity and documented within the procedure required in CIP-001-1 Requirement R2. Regarding "who within the Interconnection hierarchy deems parties to be appropriate," the drafting team knows of no interconnection authority that has such a role.

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-3

3. **Purpose:** Standard CIP-008-3 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-23 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

4. **Applicability**

   4.1. Within the text of Standard CIP-008-3, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Entity.

   4.2. The following are exempt from Standard CIP-008-3:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

   4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.

5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-3 for the previous full calendar year unless directed by its Compliance Enforcement

Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated Version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by NERC Board of Trustees	Update

A. Introduction

1. Title: **Disturbance Reporting**

2. Number: EOP-004-1

3. Purpose: Disturbances or unusual occurrences that jeopardize the operation of the Bulk Electric System, or result in system equipment damage or customer interruptions, need to be studied and understood to minimize the likelihood of similar events in the future.

4. Applicability

4.1. Reliability Coordinators.

4.2. Balancing Authorities.

4.3. Transmission Operators.

4.4. Generator Operators.

4.5. Load Serving Entities.

4.6. Regional Reliability Organizations.

5. Effective Date: January 1, 2007

B. Requirements

R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.

R2. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.

R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.

R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.

R3.2. Applicable reporting forms are provided in Attachments 1-EOP-004 and 2-EOP-004.

R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that

time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.

R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.

R4. When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.

R5. The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.

C. Measures

M1. The Regional Reliability Organization shall have and provide upon request as evidence, its current regional reporting procedure that is used to facilitate preparation of preliminary and final disturbance reports. (Requirement 1)

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, the preliminary report, computer printouts, operator logs, or other equivalent evidence that will be used to confirm that it prepared and delivered the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that will be used to confirm that it provided information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours. (Requirement 3.3)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

NERC shall be responsible for compliance monitoring of the Regional Reliability Organizations.

Regional Reliability Organizations shall be responsible for compliance monitoring of Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load-serving Entities.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to assess compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Regional Reliability Organization shall have its current, in-force, regional reporting procedure as evidence of compliance. (Measure 1)

Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that is either involved in a Bulk Electric System disturbance or has a reportable incident shall keep data related to the incident for a year from the event or for the duration of any regional investigation, whichever is longer. (Measures 2 through 4)

If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

See Attachments:

- EOP-004 Disturbance Reporting Form
- Table 1 EOP-004

2. Levels of Non-Compliance for a Regional Reliability Organization

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: No current procedure to facilitate preparation of preliminary and final disturbance reports as specified in R1.

3. Levels of Non-Compliance for a Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load- Serving Entity:

3.1. Level 1: There shall be a level one non-compliance if any of the following conditions exist:

3.1.1 Failed to prepare and deliver the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1

3.1.2 Failed to provide disturbance information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours as specified in R3.3

3.1.3 Failed to prepare a final report within 60 days as specified in R3.4

3.2. Level 2: Not applicable.

3.3. Level 3: Not applicable

3.4. Level 4: Not applicable.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	May 23, 2005	Fixed reference to attachments 1-EOP-004-0 and 2-EOP-004-0, Changed chart title 1-FAC-004-0 to 1-EOP-004-0, Fixed title of Table 1 to read 1-EOP-004-0, and fixed font.	Errata
0	July 6, 2005	Fixed email in Attachment 1-EOP-004-0 from info@nerc.com to esisac@nerc.com.	Errata

0	July 26, 2005	Fixed Header on page 8 to read EOP-004-0	Errata
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised

Attachment 1-EOP-004
NERC Disturbance Report Form

Introduction

These disturbance reporting requirements apply to all Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load Serving Entities, and provide a common basis for all NERC disturbance reporting. The entity on whose system a reportable disturbance occurs shall notify NERC and its Regional Reliability Organization of the disturbance using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. Reports can be sent to NERC via email (esisac@nerc.com) by facsimile (609-452-9550) using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. If a disturbance is to be reported to the U.S. Department of Energy also, the responding entity may use the DOE reporting form when reporting to NERC. Note: All Emergency Incident and Disturbance Reports (Schedules 1 and 2) sent to DOE shall be simultaneously sent to NERC, preferably electronically at esisac@nerc.com.

The NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports are to be made for any of the following events:

1. The loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations. Generally, a disturbance report will be required if the event results in actions such as:
   a. Modification of operating procedures.
   b. Modification of equipment (e.g. control systems or special protection systems) to prevent reoccurrence of the event.
   c. Identification of valuable lessons learned.
   d. Identification of non-compliance with NERC standards or policies.
   e. Identification of a disturbance that is beyond recognized criteria, i.e. three-phase fault with breaker failure, etc.
   f. Frequency or voltage going below the under-frequency or under-voltage load shed points.
2. The occurrence of an interconnected system separation or system islanding or both.
3. Loss of generation by a Generator Operator, Balancing Authority, or Load-Serving Entity — 2,000 MW or more in the Eastern Interconnection or Western Interconnection and 1,000 MW or more in the ERCOT Interconnection.
4. Equipment failures/system operational actions which result in the loss of firm system demands for more than 15 minutes, as described below:
   a. Entities with a previous year recorded peak demand of more than 3,000 MW are required to report all such losses of firm demands totaling more than 300 MW.
   b. All other entities are required to report all such losses of firm demands totaling more than 200 MW or 50% of the total customers being supplied immediately prior to the incident, whichever is less.
5. Firm load shedding of 100 MW or more to maintain the continuity of the bulk electric system.

6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in:
   a. Sustained voltage excursions equal to or greater than ±10%, or
   b. Major damage to power system components, or
   c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance as defined by steps 1 through 5 above.
7. An Interconnection Reliability Operating Limit (IROL) violation as required in reliability standard TOP-007.
8. Any event that the Operating Committee requests to be submitted to Disturbance Analysis Working Group (DAWG) for review because of the nature of the disturbance and the insight and lessons the electricity supply and delivery industry could learn.

NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report

☐ Check here if this is an Interconnection Reliability Operating Limit (IROL) violation report.

1.	Organization filing report.		
2.	Name of person filing report.		
3.	Telephone number.		
4.	Date and time of disturbance. Date:(mm/dd/yy) Time/Zone:		
5.	Did the disturbance originate in your system?	Yes ☐ No ☐	
6.	Describe disturbance including: cause, equipment damage, critical services interrupted, system separation, key scheduled and actual flows prior to disturbance and in the case of a disturbance involving a special protection or remedial action scheme, what action is being taken to prevent recurrence.		
7.	Generation tripped. MW Total List generation tripped		
8.	Frequency. Just prior to disturbance (Hz): Immediately after disturbance (Hz max.): Immediately after disturbance (Hz min.):		
9.	List transmission lines tripped (specify voltage level of each line).		
10.		FIRM	INTERRUPTIBLE
	Demand tripped (MW):		
	Number of affected Customers:		

	Demand lost (MW-Minutes):		
11.	Restoration time.	INITIAL	FINAL
	Transmission:		
	Generation:		
	Demand:		

Attachment 2-EOP-004
U.S. Department of Energy Disturbance Reporting Requirements

Introduction

The U.S. Department of Energy (DOE), under its relevant authorities, has established mandatory reporting requirements for electric emergency incidents and disturbances in the United States. DOE collects this information from the electric power industry on Form EIA-417 to meet its overall national security and Federal Energy Management Agency's Federal Response Plan (FRP) responsibilities. DOE will use the data from this form to obtain current information regarding emergency situations on U.S. electric energy supply systems. DOE's Energy Information Administration (EIA) will use the data for reporting on electric power emergency incidents and disturbances in monthly EIA reports. In addition, the data may be used to develop legislative recommendations, reports to the Congress and as a basis for DOE investigations following severe, prolonged, or repeated electric power reliability problems.

Every Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity must use this form to submit mandatory reports of electric power system incidents or disturbances to the DOE Operations Center, which operates on a 24-hour basis, seven days a week. All other entities operating electric systems have filing responsibilities to provide information to the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity when necessary for their reporting obligations and to file form EIA-417 in cases where these entities will not be involved. EIA requests that it be notified of those that plan to file jointly and of those electric entities that want to file separately.

Special reporting provisions exist for those electric utilities located within the United States, but for whom Reliability Coordinator oversight responsibilities are handled by electrical systems located across an international border. A foreign utility handling U.S. Balancing Authority responsibilities, may wish to file this information voluntarily to the DOE. Any U.S.-based utility in this international situation needs to inform DOE that these filings will come from a foreign-based electric system or file the required reports themselves.

Form EIA-417 must be submitted to the DOE Operations Center if any one of the following applies (see Table 1-EOP-004-0 — Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies):

1. Uncontrolled loss of 300 MW or more of firm system load for more than 15 minutes from a single incident.
2. Load shedding of 100 MW or more implemented under emergency operational policy.
3. System-wide voltage reductions of 3 percent or more.
4. Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the electric power system.
5. Actual or suspected physical attacks that could impact electric power system adequacy or reliability; or vandalism, which target components of any security system. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.

6. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.
7. Fuel supply emergencies that could impact electric power system adequacy or reliability.
8. Loss of electric service to more than 50,000 customers for one hour or more.
9. Complete operational failure or shut-down of the transmission and/or distribution electrical system.

The initial DOE Emergency Incident and Disturbance Report (form EIA-417 – Schedule 1) shall be submitted to the DOE Operations Center within 60 minutes of the time of the system disruption. Complete information may not be available at the time of the disruption. However, provide as much information as is known or suspected at the time of the initial filing. If the incident is having a critical impact on operations, a telephone notification to the DOE Operations Center (202-586-8100) is acceptable, pending submission of the completed form EIA-417. Electronic submission via an on-line web-based form is the preferred method of notification. However, electronic submission by facsimile or email is acceptable.

An updated form EIA-417 (Schedule 1 and 2) is due within 48 hours of the event to provide complete disruption information. Electronic submission via facsimile or email is the preferred method of notification. Detailed DOE Incident and Disturbance reporting requirements can be found at: http://www.eia.doe.gov/cneaf/electricity/page/form_417.html.

Table 1-EOP-004-0 Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Uncontrolled loss of Firm System Load	≥ 300 MW – 15 minutes or more	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
2	Load Shedding	≥ 100 MW under emergency operational policy	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
3	Voltage Reductions	3% or more – applied system-wide	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
4	Public Appeals	Emergency conditions to reduce demand	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
5	Physical sabotage, terrorism or vandalism	On physical security systems – suspected or real	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
6	Cyber sabotage, terrorism or vandalism	If the attempt is believed to have or did happen	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
7	Fuel supply emergencies	Fuel inventory or hydro storage levels ≤ 50% of normal	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
8	Loss of electric service	≥ 50,000 for 1 hour or more	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
9	Complete operation failure of electrical system	If isolated or interconnected electrical systems suffer total electrical system collapse	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
All DOE EIA-417 Schedule 1 reports are to be filed within 60-minutes after the start of an incident or disturbance All DOE EIA-417 Schedule 2 reports are to be filed within 48-hours after the start of an incident or disturbance				

All entities required to file a DOE EIA-417 report (Schedule 1 & 2) shall send a copy of these reports to NERC simultaneously, but no later than 24 hours after the start of the incident or disturbance.				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Loss of major system component	Significantly affects integrity of interconnected system operations	NERC Prelim Final report	24 hour 60 day
2	Interconnected system separation or system islanding	Total system shutdown Partial shutdown, separation, or islanding	NERC Prelim Final report	24 hour 60 day
3	Loss of generation	≥ 2,000 – Eastern Interconnection ≥ 2,000 – Western Interconnection ≥ 1,000 – ERCOT Interconnection	NERC Prelim Final report	24 hour 60 day
4	Loss of firm load ≥15-minutes	Entities with peak demand ≥3,000: loss ≥300 MW All others ≥200MW or 50% of total demand	NERC Prelim Final report	24 hour 60 day
5	Firm load shedding	≥100 MW to maintain continuity of bulk system	NERC Prelim Final report	24 hour 60 day
6	System operation or operation actions resulting in:	• Voltage excursions ≥10% • Major damage to system components • Failure, degradation, or misoperation of SPS	NERC Prelim Final report	24 hour 60 day
7	IROL violation	Reliability standard TOP-007.	NERC Prelim Final report	72 hour 60 day
8	As requested by ORS Chairman	Due to nature of disturbance & usefulness to industry (lessons learned)	NERC Prelim Final report	24 hour 60 day
All NERC Operating Security Limit and Preliminary Disturbance reports will be filed within 24 hours after the start of the incident. If an entity must file a DOE EIA-417 report on an incident, which requires a NERC Preliminary report, the Entity may use the DOE EIA-417 form for both DOE and NERC reports.				
Any entity reporting a DOE or NERC incident or disturbance has the responsibility to also notify its Regional Reliability Organization.				

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-01 Disturbance and Sabotage Reporting Ballot Windows Now Open: Successive Ballot and Non-binding Poll: May 15 – May 24, 2012

Now Available

A successive ballot of EOP-004-2 – Event Reporting and a non-binding poll of the associated VRFs and VSLs is open May 15, 2012 through **8 p.m. Eastern on Thursday, May 24, 2012**.

The following documents have been posted for stakeholder review and comment:

- EOP-004-2 (clean and redline showing changes to the last posting)
- Implementation Plan (clean and redline showing changes to the last posting)
- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standard and supporting documents based on comments submitted during the formal comment period that ended December 12, 2011
- Mapping Document - Identifies each requirement in the two already-approved standards that are being consolidated into EOP-004-2 (EOP-004-1 and CIP-001-2a), and identifies how the requirement has been treated in the proposed Draft 4 of EOP-004-2
- VRF/VSL Justification – Explains how the VRFs and VSLs the drafting team has proposed for EOP-004-2 comply with guidelines that FERC and NERC have established for VRFs and VSLs
- Unofficial comment form in Word format for informal use when compiling responses – the final must be submitted electronically

Instructions

Members of the ballot pools associated with this project may log in and submit their vote for the Standard and opinion in the non-binding poll of the associated VRFs and VSLs by clicking here.

Due to modifications to NERC's balloting software, voters will no longer be able to submit commits via the balloting software.

Next Steps

The drafting team will consider all comments submitted during this formal comment and ballot period to determine whether to make additional revisions to the standard.

Background

Stakeholders have indicated that identifying potential acts of "sabotage" is difficult to do in real time, and additional clarity is needed to identify thresholds for reporting potential acts of sabotage in CIP-001-1. Stakeholders have also reported that EOP-004-1 has some requirements that reference out-of-date Department of Energy forms, making the requirements ambiguous. EOP-004-1 also has some 'fill-in-the-blank' components to eliminate.

This project combines CIP-001-1 and EOP-004-1 into a single standard, EOP-004-2, that requires after-the-fact reporting of various types of events.

Additional information is available on the project webpage.

A stakeholder interested in following the Disturbance and Sabotage Reporting Drafting Team's development of EOP-004-2 may monitor meeting agendas and notes on the team's "Related Files" web page or may submit a request to join the team's "plus" email list to receive meeting agendas and meeting notes as they are distributed to the team. To join the team's "plus" email list, send an email request to: sarcomm@nerc.net. Please indicate the drafting team's name in the subject line of the email.

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd.NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-01 Disturbance and Sabotage Reporting
Formal Comment Period Open: April 25 – May 24, 2012
Ballot Windows Open: Successive Ballot and Non-binding Poll: May 15 – May 24, 2012

Now Available

EOP-004-2 – Event Reporting (clean and redline showing changes to the last posting), an implementation plan (clean and redline to the last posting), and several associated documents (listed below) have been posted for a formal comment period and successive ballot and non-binding poll of associated VRFs and VSLs that will end at **8 p.m. Eastern on Thursday, May 24, 2012**.

The following associated documents have been posted for stakeholder review and comment:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standard and supporting documents based on comments submitted during the formal comment period that ended December 12, 2011
- Mapping Document - Identifies each requirement in the two already-approved standards that are being consolidated into EOP-004-2 (EOP-004-1 and CIP-001-2a, and identifies how the requirement has been treated in the proposed Draft 4 of EOP-004-2
- VRF/VSL Justification – Explains how the VRFs and VSLs the drafting team has proposed for EOP-004-2 comply with guidelines that FERC and NERC have established for VRFs and VSLs
- Unofficial comment form in Word format – This is for informal use when compiling responses – the final must be submitted electronically

Instructions

All members of the ballot pool must cast a new ballot since the votes and comments from the last ballot will not be carried over. In addition, members of the ballot pool will need to cast a new opinion on the VRFs and VSLs. Members of the ballot pools associated with this project may log in and submit their vote for the Standard and non-binding poll of the associated VRFs and VSLs by clicking here.

Special Instructions for Submitting Comments with a Ballot
Please note that comments submitted during the formal comment period, the ballot and the non-binding poll use the same electronic form. Therefore, it is NOT necessary for ballot pool members to submit more than one set of comments. Companies or entities with representatives in multiple segments of the ballot pool may submit a single set of comments by identifying themselves as a "group" on the comment form. Likewise, it is preferable for a group of separate entities that develop comments jointly to submit the comments as a "group." **The drafting team requests that all stakeholders (ballot pool members as well as other stakeholders) submit all comments through the electronic comment form, and that companies in multiple segments as well as individual entities that develop joint comments with other entities submit their comments as a "group," with the list of group members and their associated Industry Segments.**

Next Steps
A successive ballot and non-binding poll of the associated VRFs and VSLs of EOP-004-2 will be conducted beginning on Tuesday, May 15, 2012 through 8 p.m. Eastern on Thursday, May 24, 2012.

Background
Stakeholders have indicated that identifying potential acts of "sabotage" is difficult to do in real time, and additional clarity is needed to identify thresholds for reporting potential acts of sabotage in CIP-001-1. Stakeholders have also reported that EOP-004-1 has some requirements that reference out-of-date Department of Energy forms, making the requirements ambiguous. EOP-004-1 also has some 'fill-in-the-blank' components to eliminate.

The project will include addressing previously identified stakeholder concerns and FERC directives; will bring the standards into conformance with the latest approved version of the ERO Rules of Procedure; and may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.
Additional information is available on the project webpage.

A stakeholder interested in following the Disturbance and Sabotage Reporting Drafting Team's development of EOP-004-2 may monitor meeting agendas and notes on the team's "Related Files" webpage or may submit a request to join the team's "plus" email list to receive meeting agendas and meeting notes as they are distributed to the team. To join the team's "plus" email list, send an email request to: sarcomm@nerc.net. Please indicate the drafting team's name in the subject line of the email.

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd.NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-01 Disturbance and Sabotage Reporting
Formal Comment Period Open: April 25 – May 24, 2012
Ballot Windows Open: Successive Ballot and Non-binding Poll: May 15 – May 24, 2012

Now Available

EOP-004-2 – Event Reporting (clean and redline showing changes to the last posting), an implementation plan (clean and redline to the last posting), and several associated documents (listed below) have been posted for a formal comment period and successive ballot and non-binding poll of associated VRFs and VSLs that will end at **8 p.m. Eastern on Thursday, May 24, 2012**.

The following associated documents have been posted for stakeholder review and comment:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standard and supporting documents based on comments submitted during the formal comment period that ended December 12, 2011
- Mapping Document - Identifies each requirement in the two already-approved standards that are being consolidated into EOP-004-2 (EOP-004-1 and CIP-001-2a, and identifies how the requirement has been treated in the proposed Draft 4 of EOP-004-2
- VRF/VSL Justification – Explains how the VRFs and VSLs the drafting team has proposed for EOP-004-2 comply with guidelines that FERC and NERC have established for VRFs and VSLs
- Unofficial comment form in Word format – This is for informal use when compiling responses – the final must be submitted electronically

Instructions

All members of the ballot pool must cast a new ballot since the votes and comments from the last ballot will not be carried over. In addition, members of the ballot pool will need to cast a new opinion on the VRFs and VSLs. Members of the ballot pools associated with this project may log in and submit their vote for the Standard and non-binding poll of the associated VRFs and VSLs by clicking here.

Special Instructions for Submitting Comments with a Ballot
Please note that comments submitted during the formal comment period, the ballot and the non-binding poll use the same electronic form. Therefore, it is NOT necessary for ballot pool members to submit more than one set of comments. Companies or entities with representatives in multiple segments of the ballot pool may submit a single set of comments by identifying themselves as a "group" on the comment form. Likewise, it is preferable for a group of separate entities that develop comments jointly to submit the comments as a "group." **The drafting team requests that all stakeholders (ballot pool members as well as other stakeholders) submit all comments through the electronic comment form, and that companies in multiple segments as well as individual entities that develop joint comments with other entities submit their comments as a "group," with the list of group members and their associated Industry Segments.**

Next Steps
A successive ballot and non-binding poll of the associated VRFs and VSLs of EOP-004-2 will be conducted beginning on Tuesday, May 15, 2012 through 8 p.m. Eastern on Thursday, May 24, 2012.

Background
Stakeholders have indicated that identifying potential acts of "sabotage" is difficult to do in real time, and additional clarity is needed to identify thresholds for reporting potential acts of sabotage in CIP-001-1. Stakeholders have also reported that EOP-004-1 has some requirements that reference out-of-date Department of Energy forms, making the requirements ambiguous. EOP-004-1 also has some 'fill-in-the-blank' components to eliminate.

The project will include addressing previously identified stakeholder concerns and FERC directives; will bring the standards into conformance with the latest approved version of the ERO Rules of Procedure; and may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.
Additional information is available on the project webpage.

A stakeholder interested in following the Disturbance and Sabotage Reporting Drafting Team's development of EOP-004-2 may monitor meeting agendas and notes on the team's "Related Files" webpage or may submit a request to join the team's "plus" email list to receive meeting agendas and meeting notes as they are distributed to the team. To join the team's "plus" email list, send an email request to: sarcomm@nerc.net. Please indicate the drafting team's name in the subject line of the email.

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd.NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Project 2009-01 Disturbance and Sabotage Reporting

Successive Ballot Results

Now Available

A successive ballot of EOP-004-2 – Event Reporting, and non-binding pools of the associated VRFs and VSLs, concluded on Thursday, May 24, 2012. Voting statistics are listed below, and the Ballot Results page provides a link to the detailed results.

Successive Ballot Results for Project 2009-01

Ballot Results	Non-binding Poll Results
Quorum: 84.43%	Quorum: 79.95%
Approval: 46.18%	Supportive Opinions: 52.67%

Next Steps
The drafting team will consider all comments submitted during the comment period and ballot, and based on the comments will determine whether to make additional changes.

Background
EOP-004-2 – Event Reporting consolidates requirements from CIP-001-2a – Sabotage Report and EOP-004-1 – Disturbance Reporting.

Standards Development Process
The Standards Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend out thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2009-01 Disturbance and Sabotage Reporting EOP-004-2 _in
Ballot Period:	5/15/2012 - 5/24/2012
Ballot Type:	Initial
Total # Votes:	358
Total Ballot Pool:	424
Quorum:	**84.43 % The Quorum has been reached**
Weighted Segment Vote:	46.18 %
Ballot Results:	**The standard will proceed to recirculation ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	104	1	41	0.5	41	0.5	6	16
2 - Segment 2.	11	0.9	2	0.2	7	0.7	2	0
3 - Segment 3.	108	1	35	0.393	54	0.607	6	13
4 - Segment 4.	37	1	15	0.484	16	0.516	2	4
5 - Segment 5.	91	1	39	0.574	29	0.426	7	16
6 - Segment 6.	53	1	18	0.474	20	0.526	3	12
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	8	0.6	4	0.4	2	0.2	0	2
9 - Segment 9.	4	0.2	0	0	2	0.2	1	1
10 - Segment 10.	8	0.5	3	0.3	2	0.2	1	2
Totals	**424**	**7.2**	**157**	**3.325**	**173**	**3.875**	**28**	**66**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	
1	American Electric Power	Paul B. Johnson		
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller	Abstain	
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Negative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Negative	
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	East Kentucky Power Coop.	George S. Carruba	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Negative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Negative	
1	Grand River Dam Authority	James M Stafford		
1	Great River Energy	Gordon Pietsch	Negative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier		
1	Idaho Power Company	Ronald D Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson		
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Affirmative	
1	Lincoln Electric System	Doug Bantam		
1	Los Angeles Department of Water & Power	Ly M Le		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	National Grid	Saurabh Saksena	Negative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Arnold J. Schuff	Affirmative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Abstain	
1	Northeast Utilities	David Boguslawski	Negative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Negative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn	Negative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	

1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Negative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Affirmative	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Abstain	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Negative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Sunflower Electric Power Corporation	Noman Lee Williams		
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry Akens	Abstain	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	
2	Alberta Electric System Operator	Mark B Thompson	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	
2	California ISO	Rich Vine	Negative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Abstain	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	
2	Midwest ISO, Inc.	Marie Knox	Negative	
2	New Brunswick System Operator	Alden Briggs	Negative	
2	New York Independent System Operator	Gregory Campoli	Abstain	
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Negative	
3	AEP	Michael E Deloach	Negative	
3	Alabama Power Company	Richard J. Mandes	Negative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Abstain	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Negative	
3	City of Garland	Ronnie C Hoeinghaus	Affirmative	
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Palo Alto	Eric R Scott	Affirmative	

3	City of Redding	Bill Hughes	Affirmative	
3	Clatskanie People's Utility District	Brian Fawcett		
3	Clearwater Power Co.	Dave Hagen	Negative	
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Negative	
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	
3	Constellation Energy	CJ Ingersoll	Abstain	
3	Consumers Energy	Richard Blumenstock	Negative	
3	Consumers Power Inc.	Roman Gillen	Negative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Negative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	
3	Entergy	Joel T Plessinger	Negative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Negative	
3	Georgia Systems Operations Corporation	William N. Phinney	Negative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Negative	
3	Gulf Power Company	Paul C Caldwell	Negative	
3	Hydro One Networks, Inc.	David Kiguel	Negative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker		
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Kootenai Electric Cooperative	Dave Kahly	Affirmative	
3	Lakeland Electric	Norman D Harryhill		
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	
3	Lincoln Electric System	Jason Fortik	Negative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Negative	
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Negative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	Marilyn Brown	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	North Carolina Electric Membership Corp.	Doug White	Negative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Negative	
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters	Negative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	

3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	Southern California Edison Co.	David B Coher	Negative	
3	Southern Maryland Electric Coop.	Mark R Jones		
3	Tacoma Public Utilities	Travis Metcalfe	Negative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	
3	Westar Energy	Bo Jones	Negative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave		
3	Xcel Energy, Inc.	Michael Ibold	Negative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Negative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Negative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	North Carolina Electric Membership Corp.	Bob Beadle	Negative	
4	Northern California Power Agency	Tracy R Bibb	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Negative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Negative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	
4	White River Electric Association Inc.	Frank L. Sampson		
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Negative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	

5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Abstain	
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Affirmative	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Abstain	
5	Consumers Energy Company	David C Greyerbiehl		
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Negative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Energy	Ellen Oswald		
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Exelon Nuclear	Michael Korchynsky	Negative	
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Negative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	Indeck Energy Services, Inc.	Rex A Roehl		
5	JEA	John J Babik	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard		
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Negative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman		
5	Luminant Generation Company LLC	Mike Laney	Negative	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Negative	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Negative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	

5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Siemens PTI	Edwin Cano		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe		
5	Southern Company Generation	William D Shultz	Negative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
5	Wisconsin Public Service Corp.	Leonard Rentmeester		
5	Xcel Energy, Inc.	Liam Noailles	Negative	
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Negative	
6	Constellation Energy Commodities Group	Brenda L Powell	Negative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Negative	
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Negative	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Negative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak		
6	Snohomish County PUD No. 1	William T Moojen		
6	South California Edison Company	Lujuanna Medina		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	
6	Tacoma Public Utilities	Michael C Hill		
6	Tampa Electric Co.	Benjamin F Smith II		

6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner		
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Pacific Northwest Generating Cooperative	Margaret Ryan	Negative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain	Abstain	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky		
10	Midwest Reliability Organization	James D Burley		
10	New York State Reliability Council	Alan Adamson	Negative	
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Non-binding Poll Results

Project 2009-01: Disturbance and Sabotage Reporting

Non-binding Poll Results	
Non-binding Poll Name:	Project 2009-01 DSR Non-binding Poll
Poll Period:	5/15/2012 - 5/24/2012
Total # Opinions:	315
Total Ballot Pool:	394
Summary Results:	79.95% of those who registered to participate provided an opinion or an abstention; 52.67% of those who provided an opinion indicated support for the VRFs and VSLs.

Individual Ballot Pool Results

Segment	Organization	Member	Opinions
1	Ameren Services	Kirit Shah	Negative
1	American Electric Power	Paul B. Johnson	
1	American Transmission Company, LLC	Andrew Z Pusztai	Abstain
1	Arizona Public Service Co.	Robert Smith	Affirmative
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative
1	Avista Corp.	Scott J Kinney	Affirmative
1	Balancing Authority of Northern California	Kevin Smith	Abstain
1	Baltimore Gas & Electric Company	Gregory S Miller	Abstain
1	BC Hydro and Power Authority	Patricia Robertson	Abstain
1	Beaches Energy Services	Joseph S Stonecipher	Negative
1	Black Hills Corp	Eric Egge	
1	Bonneville Power Administration	Donald S. Watkins	Negative
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative
1	Central Maine Power Company	Joseph Turano Jr.	Negative
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative
1	Clark Public Utilities	Jack Stamper	Affirmative
1	Colorado Springs Utilities	Paul Morland	Affirmative
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative
1	CPS Energy	Richard Castrejana	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative
1	Deseret Power	James Tucker	Abstain
1	Dominion Virginia Power	Michael S Crowley	Abstain
1	Duke Energy Carolina	Douglas E. Hils	Negative
1	East Kentucky Power Coop.	George S. Carruba	Abstain
1	Empire District Electric Co.	Ralph F Meyer	Affirmative
1	Entergy Services, Inc.	Edward J Davis	Negative

1	FirstEnergy Corp.	William J Smith	Affirmative
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative
1	Florida Power & Light Co.	Mike O'Neil	Negative
1	Gainesville Regional Utilities	Luther E. Fair	
1	Georgia Transmission Corporation	Jason Snodgrass	Abstain
1	Grand River Dam Authority	James M Stafford	
1	Great River Energy	Gordon Pietsch	Negative
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Abstain
1	Hydro One Networks, Inc.	Ajay Garg	Negative
1	Hydro-Quebec TransEnergie	Bernard Pelletier	
1	Idaho Power Company	Ronald D. Schellberg	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain
1	JEA	Ted Hobson	Affirmative
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative
1	Keys Energy Services	Stanley T Rzad	
1	Lakeland Electric	Larry E Watt	
1	Lee County Electric Cooperative	John W Delucca	Affirmative
1	Lincoln Electric System	Doug Bantam	
1	Los Angeles Department of Water & Power	Ly M Le	
1	Lower Colorado River Authority	Martyn Turner	Affirmative
1	Manitoba Hydro	Joe D Petaski	Negative
1	MEAG Power	Danny Dees	Affirmative
1	MidAmerican Energy Co.	Terry Harbour	Negative
1	Minnkota Power Coop. Inc.	Richard Burt	
1	National Grid	Saurabh Saksena	Affirmative
1	Nebraska Public Power District	Cole C Brodine	Negative
1	New Brunswick Power Transmission Corporation	Randy MacDonald	
1	New York Power Authority	Arnold J. Schuff	Affirmative
1	New York State Electric & Gas Corp.	Raymond P Kinney	Abstain
1	Northeast Utilities	David Boguslawski	Abstain
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative
1	NorthWestern Energy	John Canavan	
1	Ohio Valley Electric Corp.	Robert Mattey	Abstain
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Negative
1	Omaha Public Power District	Doug Peterchuck	Affirmative
1	Oncor Electric Delivery	Brenda Pulis	Affirmative
1	Orlando Utilities Commission	Brad Chase	Affirmative
1	PacifiCorp	Ryan Millard	Abstain
1	PECO Energy	Ronald Schloendorn	Negative
1	Platte River Power Authority	John C. Collins	Abstain
1	Portland General Electric Co.	John T Walker	Affirmative
1	PowerSouth Energy Cooperative	Larry D Avery	Negative
1	PPL Electric Utilities Corp.	Brenda L Truhe	Abstain

1	Progress Energy Carolinas	Brett A Koelsch	Negative
1	Public Service Company of New Mexico	Laurie Williams	Affirmative
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative
1	Sacramento Municipal Utility District	Tim Kelley	Abstain
1	Salmon River Electric Cooperative	Kathryn Spence	
1	Salt River Project	Robert Kondziolka	Affirmative
1	Santee Cooper	Terry L Blackwell	Negative
1	SCE&G	Henry Delk, Jr.	
1	Seattle City Light	Pawel Krupa	Affirmative
1	Sho-Me Power Electric Cooperative	Denise Stevens	Abstain
1	Sierra Pacific Power Co.	Rich Salgo	Abstain
1	Snohomish County PUD No. 1	Long T Duong	Affirmative
1	South California Edison Company	Steven Mavis	Negative
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative
1	Southern Illinois Power Coop.	William Hutchison	Negative
1	Southwest Transmission Cooperative, Inc.	James Jones	
1	Southwestern Power Administration	Angela L Summer	Abstain
1	Sunflower Electric Power Corporation	Noman Lee Williams	
1	Tampa Electric Co.	Beth Young	
1	Tennessee Valley Authority	Larry Akens	Abstain
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative
1	Tucson Electric Power Co.	John Tolo	Negative
1	United Illuminating Co.	Jonathan Appelbaum	Negative
1	Westar Energy	Allen Klassen	Negative
1	Western Area Power Administration	Brandy A Dunn	Affirmative
1	Xcel Energy, Inc.	Gregory L Pieper	
2	Alberta Electric System Operator	Mark B Thompson	Abstain
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain
2	California ISO	Rich Vine	Negative
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	
2	Independent Electricity System Operator	Barbara Constantinescu	Negative
2	Midwest ISO, Inc.	Marie Knox	Negative
2	New Brunswick System Operator	Alden Briggs	Abstain
2	New York Independent System Operator	Gregory Campoli	Abstain
2	PJM Interconnection, L.L.C.	Tom Bowe	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Abstain
3	AEP	Michael E Deloach	Abstain
3	Alabama Power Company	Richard J. Mandes	Negative
3	Ameren Services	Mark Peters	Negative
3	Anaheim Public Utilities Dept.	Kelly Nguyen	
3	APS	Steven Norris	Affirmative
3	Arkansas Electric Cooperative	Philip Huff	Affirmative

	Corporation		
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain
3	Bonneville Power Administration	Rebecca Berdahl	Negative
3	Central Lincoln PUD	Steve Alexanderson	Abstain
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative
3	City of Bartow, Florida	Matt Culverhouse	Abstain
3	City of Clewiston	Lynne Mila	Negative
3	City of Farmington	Linda R Jacobson	Abstain
3	City of Garland	Ronnie C Hoeinghaus	Affirmative
3	City of Green Cove Springs	Gregg R Griffin	
3	City of Redding	Bill Hughes	Affirmative
3	Clatskanie People's Utility District	Brian Fawcett	
3	Cleco Corporation	Michelle A Corley	Negative
3	Colorado Springs Utilities	Charles Morgan	Affirmative
3	ComEd	Bruce Krawczyk	Negative
3	Consolidated Edison Co. of New York	Peter T Yost	Negative
3	Constellation Energy	CJ Ingersoll	Abstain
3	Consumers Energy	Richard Blumenstock	Negative
3	Cowlitz County PUD	Russell A Noble	Affirmative
3	CPS Energy	Jose Escamilla	
3	Detroit Edison Company	Kent Kujala	Negative
3	Dominion Resources Services	Michael F. Gildea	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative
3	Entergy	Joel T Plessinger	Negative
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative
3	Florida Municipal Power Agency	Joe McKinney	Negative
3	Florida Power Corporation	Lee Schuster	
3	Georgia Power Company	Anthony L Wilson	Negative
3	Georgia Systems Operations Corporation	William N. Phinney	Negative
3	Grays Harbor PUD	Wesley W Gray	
3	Great River Energy	Brian Glover	Negative
3	Gulf Power Company	Paul C Caldwell	Negative
3	Hydro One Networks, Inc.	David Kiguel	Negative
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative
3	JEA	Garry Baker	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative
3	Kissimmee Utility Authority	Gregory D Woessner	Abstain
3	Kootenai Electric Cooperative	Dave Kahly	Abstain
3	Lakeland Electric	Norman D Harryhill	
3	Lincoln Electric System	Jason Fortik	Affirmative
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Abstain
3	Louisville Gas and Electric Co.	Charles A. Freibert	
3	Manitoba Hydro	Greg C. Parent	Negative
3	Manitowoc Public Utilities	Thomas E Reed	Negative
3	MidAmerican Energy Co.	Thomas C. Mielnik	Abstain
3	Mississippi Power	Jeff Franklin	Negative
3	Modesto Irrigation District	Jack W Savage	Affirmative

3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative
3	Muscatine Power & Water	John S Bos	Negative
3	Nebraska Public Power District	Tony Eddleman	Abstain
3	New York Power Authority	Marilyn Brown	Affirmative
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative
3	North Carolina Electric Membership Corp.	Doug White	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative
3	Ocala Electric Utility	David Anderson	Negative
3	Old Dominion Electric Coop.	Bill Watson	
3	Orange and Rockland Utilities, Inc.	David Burke	Negative
3	Orlando Utilities Commission	Ballard K Mutters	Abstain
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative
3	Pacific Gas and Electric Company	John H Hagen	Affirmative
3	PacifiCorp	Dan Zollner	Affirmative
3	Platte River Power Authority	Terry L Baker	Abstain
3	PNM Resources	Michael Mertz	Affirmative
3	Potomac Electric Power Co.	Robert Reuter	Abstain
3	Progress Energy Carolinas	Sam Waters	Negative
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain
3	Public Utility District No. 1 of Clallam County	David Proebstel	
3	Puget Sound Energy, Inc.	Erin Apperson	
3	Rutherford EMC	Thomas M Haire	Negative
3	Sacramento Municipal Utility District	James Leigh-Kendall	Abstain
3	Salt River Project	John T. Underhill	Affirmative
3	Santee Cooper	James M Poston	Negative
3	Seattle City Light	Dana Wheelock	Affirmative
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative
3	Snohomish County PUD No. 1	Mark Oens	
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain
3	Southern Maryland Electric Coop.	Mark R Jones	
3	Tacoma Public Utilities	Travis Metcalfe	Negative
3	Tampa Electric Co.	Ronald L Donahey	
3	Tennessee Valley Authority	Ian S Grant	Abstain
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative
3	Westar Energy	Bo Jones	Negative
3	Xcel Energy, Inc.	Michael Ibold	Abstain
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative
4	American Municipal Power	Kevin Koloini	Negative
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Abstain
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative
4	Central Lincoln PUD	Shamus J Gamache	Negative
4	City of Austin dba Austin Energy	Reza Ebrahimian	
4	City of Clewiston	Kevin McCarthy	Negative
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	

4	City of Redding	Nicholas Zettel	Affirmative
4	City Utilities of Springfield, Missouri	John Allen	Affirmative
4	Consumers Energy	David Frank Ronk	Negative
4	Cowlitz County PUD	Rick Syring	Affirmative
4	Detroit Edison Company	Daniel Herring	Affirmative
4	Flathead Electric Cooperative	Russ Schneider	Abstain
4	Florida Municipal Power Agency	Frank Gaffney	Negative
4	Fort Pierce Utilities Authority	Thomas Richards	
4	Georgia System Operations Corporation	Guy Andrews	Negative
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain
4	Imperial Irrigation District	Diana U Torres	Affirmative
4	Indiana Municipal Power Agency	Jack Alvey	Abstain
4	Integrys Energy Group, Inc.	Christopher Plante	Negative
4	LaGen	Richard Comeaux	Abstain
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain
4	Northern California Power Agency	Tracy R Bibb	Affirmative
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Abstain
4	Sacramento Municipal Utility District	Mike Ramirez	Abstain
4	Seattle City Light	Hao Li	Affirmative
4	South Mississippi Electric Power Association	Steven McElhaney	
4	Tacoma Public Utilities	Keith Morisette	Negative
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative
5	AEP Service Corp.	Brock Ondayko	Abstain
5	AES Corporation	Leo Bernier	Affirmative
5	Amerenue	Sam Dwyer	Negative
5	Arizona Public Service Co.	Edward Cambridge	Affirmative
5	Avista Corp.	Edward F. Groce	Affirmative
5	BC Hydro and Power Authority	Clement Ma	Abstain
5	Black Hills Corp	George Tatar	Affirmative
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	
5	Bonneville Power Administration	Francis J. Halpin	Negative
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain
5	Caithness Long Island, LLC	Jason M Moore	Abstain
5	Chelan County Public Utility District #1	John Yale	Abstain
5	City and County of San Francisco	Daniel Mason	Abstain
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative
5	City of Redding	Paul Cummings	Affirmative
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative
5	City of Tallahassee	Brian Horton	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative
5	Cleco Power	Stephanie Huffman	Negative

5	Cogentrix Energy, Inc.	Mike D Hirst	Affirmative
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Abstain
5	Consumers Energy Company	David C Greyerbiehl	
5	Cowlitz County PUD	Bob Essex	Affirmative
5	CPS Energy	Robert Stevens	
5	Detroit Edison Company	Christy Wicke	Affirmative
5	Dominion Resources, Inc.	Mike Garton	Abstain
5	Duke Energy	Dale Q Goodwine	Negative
5	Dynegy Inc.	Dan Roethemeyer	Abstain
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	
5	Edison Mission Energy	Ellen Oswald	
5	Electric Power Supply Association	John R Cashin	
5	Exelon Nuclear	Michael Korchynsky	Negative
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative
5	Florida Municipal Power Agency	David Schumann	Negative
5	Gainesville Regional Utilities	Karen C Alford	
5	Great River Energy	Preston L Walsh	Negative
5	Green Country Energy	Greg Froehling	
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative
5	Indeck Energy Services, Inc.	Rex A Roehl	
5	JEA	John J Babik	Affirmative
5	Kissimmee Utility Authority	Mike Blough	Negative
5	Lakeland Electric	James M Howard	
5	Liberty Electric Power LLC	Daniel Duff	
5	Lincoln Electric System	Dennis Florom	Affirmative
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative
5	Lower Colorado River Authority	Tom Foreman	
5	Luminant Generation Company LLC	Mike Laney	Affirmative
5	Manitoba Hydro	S N Fernando	Negative
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain
5	MEAG Power	Steven Grego	Affirmative
5	MidAmerican Energy Co.	Christopher Schneider	Negative
5	Muscatine Power & Water	Mike Avesing	Negative
5	Nebraska Public Power District	Don Schmit	Abstain
5	New York Power Authority	Gerald Mannarino	Affirmative
5	NextEra Energy	Allen D Schriver	Negative
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative
5	Northern California Power Agency	Hari Modi	Affirmative
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative
5	Occidental Chemical	Michelle R DAntuono	Affirmative
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative

5	Orlando Utilities Commission	Richard Kinas	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative
5	PacifiCorp	Sandra L. Shaffer	Abstain
5	Platte River Power Authority	Roland Thiel	Abstain
5	Portland General Electric Co.	Gary L Tingley	Affirmative
5	PowerSouth Energy Cooperative	Tim Hattaway	Abstain
5	PPL Generation LLC	Annette M Bannon	Affirmative
5	Progress Energy Carolinas	Wayne Lewis	Negative
5	PSEG Fossil LLC	Tim Kucey	Abstain
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative
5	Puget Sound Energy, Inc.	Tom Flynn	Negative
5	Sacramento Municipal Utility District	Bethany Hunter	Abstain
5	Salt River Project	William Alkema	Affirmative
5	Santee Cooper	Lewis P Pierce	Negative
5	Seattle City Light	Michael J. Haynes	Abstain
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative
5	Siemens PTI	Edwin Cano	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative
5	South Mississippi Electric Power Association	Jerry W Johnson	
5	Southern California Edison Co.	Denise Yaffe	
5	Southern Company Generation	William D Shultz	Negative
5	Tampa Electric Co.	RJames Rocha	Affirmative
5	Tenaska, Inc.	Scott M. Helyer	Abstain
5	Tennessee Valley Authority	David Thompson	Abstain
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative
5	U.S. Army Corps of Engineers	Melissa Kurtz	
5	Vandolah Power Company L.L.C.	Douglas A. Jensen	
5	Xcel Energy, Inc.	Liam Noailles	
6	ACES Power Marketing	Jason L Marshall	Abstain
6	AEP Marketing	Edward P. Cox	Abstain
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative
6	APS	RANDY A YOUNG	Affirmative
6	Arkansas Electric Cooperative Corporation	Keith Sugg	
6	Bonneville Power Administration	Brenda S. Anderson	Negative
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative
6	City of Redding	Marvin Briggs	Affirmative
6	Cleco Power LLC	Robert Hirchak	Negative
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Negative
6	Constellation Energy Commodities Group	Brenda Powell	
6	Dominion Resources, Inc.	Louis S. Slade	Abstain
6	Duke Energy Carolina	Walter Yeager	
6	Entergy Services, Inc.	Terri F Benoit	Negative
6	Exelon Power Team	Pulin Shah	
6	FirstEnergy Solutions	Kevin Querry	Affirmative

6	Florida Municipal Power Agency	Richard L. Montgomery	Negative
6	Florida Municipal Power Pool	Thomas Washburn	Negative
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain
6	Imperial Irrigation District	Cathy Bretz	Affirmative
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	
6	Lakeland Electric	Paul Shipps	Negative
6	Lincoln Electric System	Eric Ruskamp	Affirmative
6	Los Angeles Department of Water & Power	Brad Packer	
6	Luminant Energy	Brad Jones	Affirmative
6	Manitoba Hydro	Daniel Prowse	Negative
6	MidAmerican Energy Co.	Dennis Kimm	Abstain
6	New York Power Authority	William Palazzo	Affirmative
6	North Carolina Municipal Power Agency #1	Matthew Schull	Abstain
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative
6	Omaha Public Power District	David Ried	Affirmative
6	Orlando Utilities Commission	Claston Augustus Sunanon	
6	PacifiCorp	Scott L Smith	Abstain
6	Platte River Power Authority	Carol Ballantine	Abstain
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative
6	Progress Energy	John T Sturgeon	Negative
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain
6	Sacramento Municipal Utility District	Diane Enderby	Abstain
6	Salt River Project	Steven J Hulet	Affirmative
6	Santee Cooper	Michael Brown	Negative
6	Seattle City Light	Dennis Sismaet	Affirmative
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	
6	Snohomish County PUD No. 1	William T Moojen	
6	South California Edison Company	Lujuanna Medina	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative
6	Tacoma Public Utilities	Michael C Hill	
6	Tampa Electric Co.	Benjamin F Smith II	
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain
6	Westar Energy	Grant L Wilkerson	Negative
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative
6	Xcel Energy, Inc.	David F. Lemmons	
8		Edward C Stein	Affirmative
8		Roger C Zaklukiewicz	Affirmative
8		James A Maenner	
8	APX	Michael Johnson	Affirmative
8	JDRJC Associates	Jim Cyrulewski	Affirmative
8	Power Energy Group LLC	Peggy Abbadini	
8	Utility Services, Inc.	Brian Evans-Mongeon	Abstain

8	Volkmann Consulting, Inc.	Terry Volkmann	Negative
9	California Energy Commission	William M Chamberlain	Abstain
9	Central Lincoln PUD	Bruce Lovelin	Affirmative
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative
10	Midwest Reliability Organization	James D Burley	
10	New York State Reliability Council	Alan Adamson	Negative
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain
10	ReliabilityFirst Corporation	Anthony E Jablonski	Negative
10	SERC Reliability Corporation	Carter B Edge	Abstain
10	Southwest Power Pool RE	Emily Pennel	Affirmative
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain

Name (59 Responses)
Organization (59 Responses)
Group Name (28 Responses)
Lead Contact (28 Responses)
Question 1 (76 Responses)
Question 1 Comments (87 Responses)
Question 2 (77 Responses)
Question 2 Comments (87 Responses)
Question 3 (62 Responses)
Question 3 Comments (87 Responses)
Question 4 (0 Responses)
Question 4 Comments (87 Responses)

Individual
Brian Evans-Mongeon
Utility Services
Yes
While agreeing with the change, confusion may exist with the CAN that exists for the term "Annual". Utility Services suggests that the language be changed to "Every calendar year" or something equivalent. Given everything that transpired in the discussion on the term annual, using a different phrase may be advantageous.
Yes
Yes
There are no other comments at this time.
Individual
E Hahn
MWDSC
No
Tranmsission Owners (TO) should not be included as a "Responsible Entity" for this or other requirements because the Operating Plan is usually prepared by the Transmission Operator (TOP). For TOs who are not also TOPs, there are usually delegation agreements. CIP-001 never directly applied to TOs.
No
See comment for question 1
Individual
Scott McGough
Georgia System Operations Corporation
Yes
No
See comments under no. 4 below.
Yes
a) Reporting most of these items ... • Does not "provide for reliable operation of the BES" • Does not include "requirements for the operation of existing BES facilities" • Is not necessary to "provide for reliable operation of the BES" ... and is therefore not in accordance with the statutory and regulatory definitions of a Reliability Standard. They should not be in a Reliability Standard. Most of this is an

administrative activity to provide information for NERC to perform some mandated analysis. b) A reportable Cyber Security Incident: Delete this item from the table. It is covered in another standard and does not need to be duplicated in another standard. c) Damage or destruction of a Facility: Entities MAY only need to slightly modify their existing CIP-001 Sabotage Reporting procedures from a compliance perspective of HAVING an Operating Plan but not from a perspective of complying with the Plan. A change from an entity reporting "sabotage" on "its" facilities (especially when the common understanding of CIP-001 is to report sabotage on facilities as "one might consider facilities in everyday discussions") to reporting "damage on its Facilities" (as defined in the Glossary) is a significant change. An operator does not know off the top of his head the definition of Facility or Element. He will not know for any particular electrical device whether or not reporting is required. Although the term is useful for legal and regulatory needs, it is problematic for practical operational needs. This creates the need for a big change in guidance, training, and tools for an operator to know which pieces of equipment this applies to. There is the need to translate from NERC-ese to Operator-ese. Much more time is needed to implement. The third threshold ("Results from actual or suspected intentional human action") perpetuates the problem of knowing the human's intention. Also, what if the action was intended but the result was not intended? The third threshold is ambiguous and subject to interpretation. The original intent of this project was to get away from the problem of the term sabotage due to its ambiguity and subjectivity. This latest change reverses all of the work so far toward that original goal. Instead of the drafted language, change this item to reporting "Damage or destruction of a Facility and any involved human action" and use only the first two threshold criteria. d) Any physical threat that could impact the operability of a Facility: See comment above about the term "Facility" and the need for a much longer implementation time. e) Transmission loss: This item is very unclear. What is meant by "loss?" Above, it says to report damage or destruction of a Facility. This says to report the loss of 3 Facilities. Is the intent here to report when there are 3 or more Facilities that are unintentionally and concurrently out of service for longer than a certain threshold of time? The intent should not be to include equipment failure? Three is very arbitrary. An entity with a very large footprint with a very large number of electrical devices is highly likely to have 3 out of service at one time. An entity with very few electrical devices is less likely to have 3. Delete the word Transmission. It is somewhat redundant. A Facility is BES Element. I believe all BES Elements are Transmission Facilities. A Facility operates as a single "electrical device." What if more than 3 downstream electrical devices are all concurrently out of service due to the failure of one upstream device? Would that meet the criteria? A situation meeting the criteria will be difficult to detect. Need better operator tools, specific procedures for this, training, and more implementation time. f) The implementation plan says current version stays in effect until accepted by ALL regulatory authorities but it also says that the new version takes effect 12 months after the BOT or the APPLICABLE authorities accept it. It is possible that ONE regulatory authority will not accept it for 13 months and both versions will be in effect. It is also possible for ALL regulatory authorities to accept it at the same time, the current version to no longer be in effect, but the new version will not be in effect for 12 months.

Group

Northeast Power Coordinating Council

Guy Zito

No

Regarding Requirement R3, add the following wording from Measure M3 to the end of R3 after the wording “in Part 1.2.”: The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. This language must be in the Requirement to be considered during an audit. Measures are not auditable. Regarding Requirement R4, replace the words “an annual review” with the words “a periodic review.” Add the following to R4: The frequency of such periodic reviews shall be specified in the Operating Plan and the time between periodic reviews shall not exceed five (5) years. This does not preclude an annual review in an Entity’s operating plan. The Entity will then be audited to its plan. If the industry approves a five (5) year periodic review ‘cap’, and FERC disagrees, then FERC will have to issue a directive, state it reasons and provide justification for an annual review that is not arbitrary or capricious. Adding the one year “test” requirement adds to the administrative tracking burden and adds no reliability value.

No

Regarding Attachment 1, language identical to event descriptions in the NERC Event Analysis Process and FERC OE-417 should be used. Creating a third set of event descriptions is not helpful to system

operators. Recommend aligning the Attachment 1 wording with that contained in Attachment 2, DOE Form OE-417 and the EAP whenever possible. The following pertains to Attachment 1: Replace the Attachment 1 “NOTE” with the following clarifying wording: NOTE: The Electric Reliability Organization and the Responsible Entity’s Reliability Coordinator will accept the DOE OE-417 form in lieu of Attachment 2 if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422. Initial submittal by Voice within the reporting time frame is acceptable for all events when followed by a hardcopy submittal by Facsimile or e-mail as and if required. The proposed “events” are subjective and will lead to confusion and questions as to what has to be reported. Event: A reportable Cyber Security Incident. All reportable Cyber Security Incidents may not require “One Hour Reporting.” A “one-size fits all” approach may not be appropriate for the reporting of all Cyber Security Incidents. The NERC “Security Guideline for the Electricity Sector: Threat and Incident Reporting” document provides time-frames for Cyber Security Incident Reporting. For example, a Cyber Security Compromise is recommended to be reported within one hour of detection, however, Information Theft or Loss is recommended to be reported within 48 hours. Recommend listing the Event as “A confirmed reportable Cyber Security Incident. The existing NERC “Security Guideline for the Electricity Sector: Threat and Incident Reporting” document uses reporting time-frames based on “detection” and “discovery.” Recommend using the word confirmed because of the investigation time that may be required from the point of initial “detection” or “discovery” to the point of confirmation, when the compliance “time-clock” would start for the reporting requirement in EOP-004-2. Event: Damage or destruction of a Facility Threshold for Reporting: revise language on third item to read: Results from actual or suspected intentional human action, excluding unintentional human errors. Event: Any physical threat that could impact the operability of a Facility This Event category should be deleted. The word “could” is hypothetical and therefore unverifiable and un-auditable. The word “impact” is undefined. Please delete this reporting requirement, or provide a list of hypothetical “could impact” events, as well as a specific definition and method for determining a specific physical impact threshold for “could impact” events other than “any.” Event: BES Emergency requiring public appeal for load reduction. Replace wording in the Event column with language from #8 on the OE-417 Reporting Form to eliminate reporting confusion. Following this sentence add, “This shall exclude other public appeals, e.g., made for weather, air quality and power market-related conditions, which are not made in response to a specific BES event.” Event: Complete or partial loss of monitoring capability Event wording: Delete the words “or partial” to conform the wording to the NERC Event Analysis Process. Event: Transmission Loss Revise to BES Transmission Loss Event: Generation Loss Revise to BES Generation Loss
No
The proposed new section does not contain specifics of the proposed system nor the interfacing outside of the system to support the report collecting.
The proposed standard is not consistent with NERC’s new Risk Based Compliance Monitoring. a. The performance based action to “implement its event reporting Operating Plan” on defined events, as required in R2, could be considered a valid requirement. However, the concern is that this requirement could be superseded by the NERC Events Analysis Process and existing OE-417 Reporting. b. The requirements laid out in R1, R3 and R4 are specific controls to ensure that the proposed requirement to report (R2) is carried out. However, controls should not be part of a compliance requirement. The only requirement proposed in this standard that is not a control is R2. NERC does not need to duplicate the enforcement of reporting already imposed by the DOE. DOE-417 is a well established process that has regulatory obligations. NERC enforcement of reporting is redundant. NERC has the ability to request copies of these reports without making them part of the Reliability Rules. Form EOP-004, Attachment 2: Event Reporting Form: Delete from the Task column the words “or partial”. Delete from the Task column the words “physical threat that could impact the operability of a Facility”. VSL’s may have to be revised to reflect revised wording.
Individual
Don Jones
Texas Reliability Entity
Yes
No

(1) In the Events Table, consider whether the item for “Voltage deviation on Facility” should also be applicable to GOPs, because a loss of voltage control at a generator (e.g. failure of an automatic voltage regulator or power system stabilizer) could have a similar impact on the BES as other reportable items. Note: We made this comment last time, and the SDT’s posted response was non-responsive to this concern. (2) In the Events Table, under Transmission Loss, the SDT indicated that reporting is triggered only if three or more Transmission Facilities operated by a single TOP are lost. What if four Facilities are lost, with two Facilities operated by each of two TOPs? That is a larger event than three Facilities lost by one TOP, but there is no reporting requirement? Determining event status by facility ownership is not an appropriate measure. The reporting requirements should be based on the magnitude, duration, or impact of the event, and not on what entities own or operate the facilities. (3) In the Events Table, under Transmission Loss, the criteria “loss of three or more Transmission Facilities” is very indefinite and ambiguous. For example, how will bus outages be considered? Many entities consider a bus as a single “Facility,” but loss of a single bus may impact as many as six 345kV transmission lines and cause a major event. It is not clear if this type of event would be reportable under the listed event threshold? Is the single-end opening of a transmission line considered as a loss of a Facility under the reporting criteria? (4) Combinations of events should be reportable. For example, a single event resulting in the loss of two Transmission Facilities (line and transformer) and a 950 MW generator would not be reportable under this standard. But loss of two lines and a transformer, or a 1000 MW generator, would be reportable. It is important to capture all events that have significant impacts. (5) In the Events Table, under “Unplanned control center evacuation,” “Loss of all voice communication capability” and “Complete or partial loss of monitoring capability,” GOPs should be included. GOPs also operate control centers that are subject to these kinds of occurrences, with potentially major impacts to the BES. Note that large GOP control centers are classified as “High Impact” facilities in the CIP Version 5 standards, and a single facility can control more than 10,000 MW of generation. (6) The “BES Emergency resulting in automatic firm load shedding” event row within Attachment 1 should include the BA as a responsible entity for reporting. Note that EOP-003-1 requires the BA to shed load in emergency situations (R1, R5 as examples), and any such occurrence should be reported.
(1) The ERO and Regional Entities should not be included in the Applicability of this standard. The only justification given for including them was they are required to comply with CIP-008. CIP-008 contains its own reporting requirements, and no additional reliability benefit is provided by including ERO and Regional Entities in EOP-004. Furthermore, stated NERC policy is to avoid writing requirements that apply to the ERO and Regional Entities, and we do not believe there is any sufficient reason to deviate from that policy in this standard. (2) Under Compliance, in section 1.1, all the words in “Compliance Enforcement Authority” should be capitalized. (3) Under Evidence Retention, it is not sufficient to retain only the “date change page” from prior versions of the Plan. It is not unduly burdensome for the entity to retain all prior versions of its “event reporting Operating Plan” since the last audit, and it should be required to do so. (What purpose is supposed to be served by retaining only the “date change pages”?) (4) The title of part F, “Interpretations,” is incorrect on page 23. Should perhaps be “Associated Documents.”
Group
Arizona Public Service Company
Janet Smith, Regulatory Affairs Supervisor
Yes
Yes
Yes
None
Individual
Jonathan Appelbaum
United Illuminating Company
Yes

R3 should be clear that the annual test of the plan does not mean each communication path for each applicable event on an annual basis.

Yes

The phrasing of the event labeled as Event Damage or Destruction of a Facility may be improved in the Threshold for Reporting Column. Suggest the introduction sentence for this event should be phrased as Where the Damage or Destruction of a Facility: etc. The rationale for the change is that as written it is unclear if the list that follows is meant to modify the word Facilities or the overall introductory sentence. The confusion being caused by the word That. What is important to be reported is if a Facility is damaged and then an IROL is affected it should be reported, not that if a Facility is comprising an IROL Facility is damaged but there is no impact on the IROL. Second, the top of each table is the phrase Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the event. This creates the requirement that the actual form is required to be transmitted to parties other than NERC/DOE. The suggested revision is Submit EOP-004 Attachment 2 or DOE-OE-417 report to NERC and/or DOE, and complete notification to other organizations identified pursuant to Requirement R1 Part 1.2 within one hour etc..

The measures M3 and M4 require evidence to be dated and time stamped. The time stamp is excessive and provides no benefit. A dated document is sufficient. The measure M2 requires in addition to a record of the transmittal of the EOP-004 Attachment 2 form or DOE-417 form that an operator log or other operating documentation is provided. It is unclear why this supplemental evidence of operator logs is required. We are assuming that the additional operator logs or documentation is required to demonstrate that the communication was completed to organizations other than NERC and DOE of the event. If true then the measure should be clear on this topic. For communication to NERC and DOE use the EOP-004 Form or OE-417 form and retain the transmittal record. For communication to other organizations pursuant to R1 Part 1.2 evidence may include but not limited to, operator logs, transmittal record, attestations, or voice recordings.

Individual

Dan Roethemeyer

Dynegy Inc.

Yes

Yes

Use of the term "Part x.x" throughout the Standard is somewhat confusing. I can't recall other Standards using that type of term. Suggest using the term "Requirement" instead.

Individual

Anthony Jablonski

ReliabilityFirst

ReliabilityFirst votes in the Affirmative for this standard because the standard further enhances reliability by clearing up confusion and ambiguity of reporting events which were previously reported under the EOP-004-1 and CIP-001-1 standards. Even though ReliabilityFirst votes in the Affirmative, we offer the following comments for consideration: 1. Requirement R1, Part 1.2 a. ReliabilityFirst recommends further prescribing whom the Responsible Entity needs to communicate with. The phrase "… and other organizations needed for the event type…" in Part 1.2 essentially leaves it up to the Responsible Entity to determine (include in their process) whom they should communicate each applicable event to. ReliabilityFirst recommends added a fourth column under Attachment 1, which lists whom the Responsible Entity is required to communicate with, for each applicable event. 2. VSL for Requirement R2 a. Requirement R2 requires the Responsible Entity to "implement its event reporting Operating Plan" and does not require the entity to submit a report. For consistency with the requirement, ReliabilityFirst recommends modifying the VSLs to begin with the following type of

language: “The Responsible Entity implemented its event reporting Operating Plan more than 24 hours but…” This recommendation is based on the FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement.
Individual
Joe Petaski
Manitoba Hydro
No
(R1.1 and 1.2) It is unclear whether or not R1.1 and R1.2 require a separate recognition and communication process for each of the event types listed in Attachment 1 or if event types can be grouped as determined appropriate by the responsible entity given that identical processes will apply for multiple types of events. Manitoba Hydro suggests that wording is revised so that multiple event types can be addressed by a single process as deemed appropriate by the Responsible Entity. (R3) It is unclear whether or not R3 requires the testing of the communications process for each separate event type identified in Attachment 1. If so, this would be extremely onerous. Manitoba Hydro suggests that only unique communication processes (as identified by the Responsible Entity in R1.2) require an annual test and that testing should not be required for each type of event listed in Attachment 1. As well, Manitoba Hydro believes that testing the communications process alone is not as effective as also providing training to applicable personnel on the communications process. Manitoba Hydro suggests that R3 be revised to require annual training to applicable personnel on the communications process and that only 1 test per unique communications process be required annually.
Yes
Yes
Manitoba Hydro is voting negative on EOP-004-2 for the reasons identified in our response to Question 1. In addition, Manitoba Hydro has the following comments: (Background section) - The section has inconsistent references to EOP-004 (eg. EOP-004 and EOP-004-2 are used). Wording should be made consistent. (Background section) – The section references entities, and responsible entities. Suggest wording is made consistent and changed to Responsible Entities. (General comment) – References in the standard to ‘Part 1.2’ should be changed to R1.2 as it is unclear if Part 1.2 refers to, for example, R1.2 or part 1.2 ‘Evidence Retention’. (M4) –Please clarify what is meant by ‘date change page’.
Individual
Michelle R. D'Antuono
Ingleside Cogeneration LP
Yes
Ingleside Cogeneration LP agrees that it is appropriate to test reporting communications on an annual basis, primarily to validate that phone numbers, email ids, and contact information is current. We appreciate the project team’s elimination of the terms “exercise” and “drill”, which we believe connotates a formalized planning and assessment process. An annual review of the Operating Plan implies a confirmation that linkages to sub-processes remain intact and that new learnings are captured. We also agree that it is appropriate only to require an updated Revision Level Control chart entry as evidence of compliance – it is very likely that no updates are required after the review is complete. In our view, both of these requirements are sufficient to assure an effective assessment of all facets of the Operating Plan. As such, we fully agree with the project team’s decision to delete the requirement to update the plan within 90 days of a change. In most cases, our internal processes will address the updates much sooner, but there is no compelling reason to include it as an enforceable requirement.
Yes
Ingleside Cogeneration LP agrees with the removal of nearly all one hour reporting requirements. In our view there must be a valid contribution expected of the recipients of any reporting that takes place this early in the process. Any non-essential communications will impede the progress of the

front-line personnel attempting to resolve the issue at hand – which has to be the priority. Secondly, there is a risk that early reporting may include some speculation of the cause, which may be found to be incorrect as more information becomes available. Recipients must temper their reactions to account for this uncertainty. In fact, Ingleside Cogeneration LP recommends that the single remaining one-hour reporting scenario be eliminated. It essentially defers the reporting of a cyber security incident to CIP-008 anyways, and may even lead to a multiple violation of both Standards if exceeded.
Yes
Ingleside Cogeneration is encouraged by NERC's willingness to act as central data gathering point for event information. However, we see this only as a starting point. There are still multiple internal and external reporting demands that are similar to those captured in EOP-004-2 – examples include the DOE, RAPA (misoperations), EAWG (events analysis), and ES-ISAC (cyber security). Although we appreciate the difference in reporting needs expressed by each of these organizations, there are very powerful reporting applications available which capture a basic set of data and publish them in multiple desirable formats. We ask that NERC spearhead this initiative – as it is a natural part of the ERO function.
Ingleside Cogeneration LP strongyly believes that LSEs that do not own BES assets should be excluded from the Applicability section of this standard.
Group
DECo
Kent Kujala
No
Should only have annual "review" requirement rather than test.
No
On pg 17 in the Rationale Box for EOP-004 Attachment 1: The set of terms is specific then includes the word ETC. Then further lists areas to exclude. Then on Pg 23 of document it includes train derailment near a transmission right of way and forced entry attempt into a substation facility as reportable. These conflict. Also see conflict when in pg 21 states the DOE OE417 would be excepted in lieu of the NERC form, but on the last pg it states the DOE OE417 should be attached to the NERC report indicating the NERC report is still required.
Yes
Requirement R3 for annual test specifically states that ERO is not included during test. Implies that local law enforcement or state law enforcement will be included in test. Hard to coordinate with many Local organizations in our area.
Individual
Tim Soles
Occidental Power Services, Inc.
No
There should be an exception for LSEs with no BES assets from having an Operating Plan and, therefore, from testing and review of such plan. These LSEs have no reporting responsibilities under Attachment 1 and, if they have nothing ever to report, why would they have to have an Operating Plan and have to test and review it? This places an undue burden on small entities that cannot impact the BES.
No
There are no requirements in Attachment 1 for LSEs without BES assets so these entities should not be in the Applicability section.
No
This section should reference the confidentiality requirements in the ROP and should have a statement about the system for collection and dissemination of disturbance reports being "subject to the confidentiality requirements of the NERC ROP."
OPSI continues to believe that LSEs that do not own BES assets should be excluded from the Applicability section of this standard. It is disingenuous of both the SDT and FERC to promote an

argument to support this inclusion such as that stated in Section 459 of Order 693 (and referred to by the SDT in their Consideration of Comments in the last posting). The fact is that no reportable disturbance can be caused by an “attack” on an LSE that does not own BES assets. The SDT has yet to point out such an event.
Individual
Alice Ireland
Xcel Energy
No
1) In R1.2, We understand what the drafting team had intended here. However, we are concerned that the way this requirement is drafted, using i.e., it could easily be interpreted to mean that you must notify all of those entities listed. Instead, we are suggesting that the requirement be rewritten to require entities to define in their Operating Plan the minimum organizations/entities that would need to be notified for applicable events. We believe this would remove any ambiguity and make it clear for both the registered entity and regional staff. We recommend the requirement read something like this: 1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to applicable internal and external organizations needed for the event type, as defined in the Responsible Entity’s Operating Plan. 2) We also suggest that R3 be clarified as to whether communications to all organizations must be tested or just those applicable to the test event type/scenario.
No
1) The event Damage or destruction of a Facility appears to need ‘qualifying’. Is this intended for only malicious intent? Otherwise, weather related or other operational events will often meet this criteria. For example adjustment in generation or changes in line limits to “avoid an Adverse Reliability Impact” could occur during a weather related outage. We suggest adjusting this event and criteria to clearly exclude certain items or identify what is included. 2) Also recommend placing the information in footnote 1 into the associated Threshold for Reporting column, and removing the footnote.
We believe such a tool would be useful, however we are indifferent as to if it is required to be established by the Rules of Procedure.
Xcel Energy appreciates the work of the drafting team and believes the current draft is an improvement over the existing standard. However, we would like to see the comments provided here and above addressed prior to submitting an AFFIRMATIVE vote. 1) Suggest enhancing the “Example of Reporting Process…” flowchart as follows: EVENT > Refer to Ops Plan for Event Reporting > Refer to Law Enforcement? > Yes/No > …. 2) Attachment 1 – in both the 1 hour and the 24 hour reporting they are qualified with “within x hours of recognition of the event”. Is this the intent, so that if an entity recognizes at some point after an event that the time clock starts? 3) VSLs – R3 & R4 “Severe” should remove the “OR….”, as this is redundant. Once an entity has exceeded the 3 calendar months, the Severe VSL is triggered. 4) The Guideline and Technical Basis page 22 should be corrected to read “The changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). These standards deal exclusively with after-the-fact reporting.” 5) Also in the following section of the Guideline and Technical Basis (page 23) the third bullet item should be qualified to exclude copper theft: Examples of such events include: • Bolts removed from transmission line structures • Detection of cyber intrusion that meets criteria of CIP-008-3 or its successor standard • Forced intrusion attempt at a substation (excluding copper theft) • Train derailment near a transmission right-of-way • Destruction of Bulk Electric System equipment
Group
Duke Energy
Greg Rowland
No
Under R3, we agree with testing communications internally. Just as the ERO is excluded under R3, other external entities should also be excluded. External communications should be verified under R4.
No
(1)We disagree with reporting CIP-008 incidents under this standard. We agree with the one-hour notification timeframe, but believe it should be in CIP-008 to avoid double jeopardy. (2)Damage or

destruction of a Facility – Need clarity on how a vertically integrated entity must report. For example a GOP probably won't know if an IROL will be affected. Also, there shouldn't be multiple reports from different functional entities for the same event. Suggest splitting this table so that GO, GOP, DP only reports "Results from actual or suspected intentional human action". (3)Generation Loss – Need more clarity on the threshold for reporting. For example if we lose one 1000 MW generator at 6:00 am and another 1000 MW generator at 4:00 pm, is that a reportable event?

Yes

Group

Luminant

Brenda Hampton

Yes

No

Luminant appreciates the work of the DSR SDT to modify Attachment 1 to address the concerns of the stakeholders. However, we are concerned that the threshold for reporting a Generation Loss in the ERCOT interconnection established by this revision is set at ≥ 1,000MW, which is not consistent with the level of single generation contingency used in ERCOT planning and operating studies. That level of contingency is currently set at the size of the largest generating unit in ERCOT, which is 1,375MW. For this reason, Luminant believes that the minimum threshold for reporting of a disturbance should be > 1,375MW for the ERCOT Interconnection.

Yes

Group

BC Hydro

Patricia Robertson

Yes

No

BC Hydro supports the revisions to EOP-004 and would vote Affirmative with the following change. Attachment 1 has a One Hour Reporting requirement. BC Hydro proposes a One Hour Notification with the Report submitted within a specified timeframe afterward.

Individual

Andrew Gallo

City of Austin dba Austin Energy

Yes

Austin Energy (AE) supports the requirements for (1) an annual test of the communications portion of the Operating Plan (R3) and (2) an annual review of the Operating Plan (R4); however, we offer a slight modification to the measures associated with those requirements. AE does not believe that records evidencing such test and reviews need to be time-stamped to adequately demonstrate compliance with the requirements. In each case, we recommend that the first sentence of M3 and M4 start with "Each Responsible Entity will have dated records to show that the annual …"

Yes

Austin Energy makes the following comments: (1) Comment on the Background section titled "A Reporting Process Solution – EOP-004": This section includes the sentence, "Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state OR PROVINCIAL

OR LOCAL level law enforcement agency." (emphasis added) The corresponding flowchart includes a step, "Notification Protocol to State Agency Law Enforcement." Austin Energy requests that the SDT update the flowchart to match the language of the associated paragraph and include "state or provincial or local" agencies. (2) Comments on VSLs: Austin Energy recommends that the SDT amend the VSLs for R2 to include the "recognition of" events throughout. That is, update the R2 VSLs to state "… X hours after "recognizing" an event …" in all locations where the phrase occurs. (3) Austin Energy has a concern with the inclusion of the word "damage" to the phrase "damage or destruction of a Facility." We agree that any "destruction" of a facility that meets any of the three criteria be a reportable event. However, if the Standard is going to include "damage," some objective definition for "damage" (that sets a floor) ought to be included. Much like the copper theft issue, we do not see the benefit of reporting to NERC vandalism that does not rise to a certain threshold (e.g. someone who takes a pot shot at an insulator) unless the damage has some tangible impact on the reliability of the BES or is an act of an orchestrated sabotage (e.g. removal of a bolt in a transmission structure). (4) Austin Energy voted to approve the revised Standard because it is an improvement over the existing Standard. In light of FERC's comments in Paragraph 81 of the Order approving the Find, Fix, Track and Report initiative, however, Austin Energy would propose that this Standard is the type of Standard that does not truly enhance reliability of the BES and is, instead, an administrative activity. As such, we recommend that NERC consider whether EOP-004-2 ought to be retired.
Group
Bonneville Power Administration
Chris Higgins
Yes
BPA believes that the annual testing and review as described in R3 is too cumbersome and unnecessary for entities with large footprints to inundate federal and local enforcement bodies such as the FBI for "only" testing and the documenting for auditing purposes. BPA suggests that testing be performed on a bi-annual or longer basis.
No
BPA believes that clarifying language should be added to transmission loss event. (Page 19) [a report should not be required if the number of elements is forced because of pre-designed or planned configuration. System studies have to take such a configuration into account possible wording could be. Unintentional loss of three or more Transmission Facilities (excluding successful automatic reclosing or planned operating configuration)] In addition, under the "Event" of Complete or partial loss of monitoring capability, BPA believes that "partial loss" is not sufficiently specific for BPA to write compliance operating procedures and suggest defining partial loss or removing it from the standard. Should the drafting team add clarifying language to remove "or partial loss" and address BPA's concerns on over emphasis on software tool to the operation of the system. BPA would change its negative position to affirmative.
Yes
BPA believes that the VSL should allow for amending the form after a NERC specified time period without penalty and suggests that a window of 48 hours be given to amend the form to make adjustments without needing to file a self report. Should the standard be revised to allow a time period for amending the form without having to file a self report, BPA would change its negative position to affirmative.
Individual
Thad Ness
American Electric Power
No
R3: How many different scenarios need to be tested? For example, reporting sabotage-related events might well be different than reporting reliability-related events such as those regarding loss of Transmission. While these examples might vary a great deal, other such scenarios may be very similar in nature in terms of communication procedures. Perhaps solely testing the most complex procedure would be sufficient. AEP agrees with the changes with R3 calling for an annual test provided the requirement R2 is modified to include the measure language "The annual test requirement is considered to be met if the responsible entity implements the communications process

in Part 1.2 for an actual event." M3: While we agree that "the annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event", we believe it would be preferable to include this text in R3 in addition to M3. Measures included in earlier standards (some of which are still enforced today) had little correlation to the requirement itself, and as a result, those measures were seldom referenced. M3: It would be unfair to assume that every piece of evidence required to prove compliance would be dated and time-stamped, so we recommend removing the text "dated and time-stamped" from the first sentence so that it reads "Each Responsible Entity will have records to show that the annual test of Part 1.2 was conducted." The language regarding dating and time stamps in regards to "voice recordings and operating logs or other communication" is sufficient.

No

If CIP-008 is now out of scope within the requirements of this standard, any references to it should also be removed from Attachment 1. The Threshold for Reporting column on page 26 includes "Results from actual or suspected intentional human action." This wording is too vague as many actions by their very nature are intentional. In addition, it should actually be used as a qualifying event rather than a threshold. We recommend removing it entirely from the Threshold column, and placing it in the Events column and also replacing the first row as follows: "Actual or suspected intentional human action with the goal of damage to, or destruction of, the Facility." On page 27, the event "Any physical threat that could impact the operability of a Facility" is too vague and broad. Using the phrases "any physical threat" and "could impact" sets too high a bar on what would need to be reported. On page 28, for the event "Complete loss of off-site power to a nuclear generating plant (grid supply)", TO and TOP should be removed and replaced by GOP.

Yes

While we have no objections at this point, we would like specific details on what our obligations would be as a result of these changes. For example, would the clearinghouse tool provide verifications that the report(s) had been received as well as forwarded? In addition, if DOE OE-417 is the form being submitted, would the NERC Reporting Clearinghouse forward that report to the DOE?

While we do not necessarily disagree with modifying this standard, we do have serious concerns with the possibility that Form OE-417 form would not also be modified to match any changes made to this standard. To the degree they would be different, this would create unnecessary confusion and burden on operators. If CIP-008 is now out of scope within the requirements of this standard, the task "reportable Cyber Security Incident" should be removed from Attachment 2.

Individual

Ed Davis

Entergy

No

The requirement for a "time stamped record" of annual review is unreasonable and unnecessary. A dated document showing that a review was performed should be sufficient.

Yes

Entergy does not agree with the Time Horizon for R2. The rationale for R2 contains phrases related to situational awareness and keeping people/agencies aware of the "current situation." However, this standard is related to after the fact event reporting, not real-time reporting via RCIS, as discussed on page 6 of the red-lined standard. Therefore the time horizon for R2 should indicate that this is an after the fact requirement expected to be performed either in 1 hour or 24 hours after an event occurs, not in the operations assessment time frame. This change should also be made on page 15 of the redline in the Table of compliance elements for R2. Page 18 of the redline document contains a VSL for R2 which states that it will be considered a violation if the Responsible Entity submitted a report in the appropriate timeframe but failed to provide all of the required information. It has long been the practice to submit an initial report and provide additional information as it becomes available. On page 24 of the redlined document, this is included in the following "...and provide as much information as is available at the time of the notification to the ERO..." But the compliance elements table now imposes that if the entity fails to provide ALL required information at the time the initial report is required, the entity will be non compliant with the standard. This imposes an

unreasonable burden to the Reliability Entity. This language should be removed. The compliance element table for R3 and R4 make it a high or severe violation to be late on either the annual test or the annual review of the Operating plan for communication. While Entergy supports that periodically verifying the information in the plan and having a test of the operating plan have value, it does not necessarily impose additional risk to the BES to have a plan that exceeds its testing or review period by two to three months. This is an administrative requirement and the failure to test or review should be a lower or moderate VSL, which would be consistent with the actual risk imposed by a late test or review. On page 24 of the redlined draft, there is a statement that says “In such cases, the affected Responsible Entity shall notify parties per Requirement R1 and provide as much information as if available at the time of the notification…” Since R1 is the requirement to have a plan, and R2 is the requirement to implement the plan for applicable events, it seems that the reference in this section should be to Requirement R2, not Requirement R1.
Individual
Jack Stamper
Clark Public Utilities
Yes
No
I agree with all but one. The event is "Damage or destruction of a Facility" and the threshhold for reportin is "Results from actual or suspected intentional human action." I understand and agree that destruction of a facility due to actual or suspected intentional human action should always be reported. However, I do not know what level of damage should be reported. Obviously the term "damage" is meant to signify and event that is less than destruction. As a result, damage could be extensive, minimal, or hardly noticeable. There needs to be some measure of what the damage entails if the standard is to contain a broad requirement for the reporting of damage intentionally caused by human action. Whether that measure is based on the actual impacts to the BES from the damage or whether the measure is based on the ability of the damaged equipment to continue to function at 100%, 50% or some capability would be acceptable but currently it is too open ended.
Yes
Individual
Tracy Richardson
Springfield Utility Board
Yes
• SUB supports the removal of Requirement 1, Part 1.4, as well the separation of Parts 1.3 and 1.5, agreeing that they are their own separate actions. • The Draft 4 Version History still lists the term “Impact Event” rather than “Event”.
Yes
• Spell out Requirement 1, rather than “parties per R1” in NOTE. • On page 44, “Examples of such events include” should say, “include, but are not limited to”. • SUB appreciates clarification regarding events, particularly the discussion regarding “sabotage”, and recommends listing and defining “Event” in Definitions and Terms Used in NERC Standards. • The Guideline and Technical Basis provides clarity, and SUB agrees with the removal of “NERC Guideline: Threat and Incident Reporting”. • In the flow chart on page 9 there are parallel paths going from “Refer to Ops Plan for Reporting” to the ‘Report Event to ERO, Reliability Coordinator’ via both the Yes and No response. It seems like the yes/no decision should follow after “Refer to Ops Plan” for communication to law enforcement.
Yes
• SUB supports the new Section 812 being incorporated into the NERC ROP. This addition provides clarity for what is required by whom and takes away any possible ambiguity.
SUB appreciates the opportunity to provide comments. While Staff was concerned with the consolidation of CIP and non-CIP NERC Reliability Standards (as to how they’ll be audited), the Project 2009-01 SDT has done an excellent job in providing clarification around identifying and reporting events, particularly related to the varying definitions of “sabotage”.

Individual
Wayne Sipperly
New York Power Authority
No
Please see comments submitted by NPCC Regional Standards Committee (RSC).
No
Please see comments submitted by NPCC Regional Standards Committee (RSC).
Yes
Please see comments submitted by NPCC Regional Standards Committee (RSC).
Individual
David Thorne
Pepco Holdings Inc
Yes
Yes
No
This could create confusion. This new ROP section states that "… the system shall then forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary." Standard Section R1.2 states "A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies." If NERC is going to be the "clearinghouse" forwarding reports to the RE and DOE, does that mean that the reporting entity only needs to make a single submission to NERC for distribution? If the reporting entity is required to make all notifications, per R1.2, what is the purpose of NERC's duplication of sending out reports? It would be very helpful to the reporting entities if R1.2 was revised to state that NERC would forward the event form to the RE and DOE and the reporting entity would only be responsible for providing notice verbally to its associated BA, TOP, RC, etc. as appropriate and for notifying appropriate law enforcement as required.
The SDT's efforts have resulted in a very good draft.
Group
Imperial Irrigation District (IID)
Jesus Sammy Alcaraz
Yes
Yes
Yes
Individual
Chris de Graffenried
Consolidated Edison Co. of NY, Inc.
No
Requirement R3: Following the sentence ending "in Part 1.2" add the following wording from the Measure to R3: The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. This language must be in the Requirement to be considered during an audit. Measures are not auditable. Requirement R4: Replace

the words “an annual review” with the words “a periodic review.” Following the first sentence in R4 add: The frequency of such periodic reviews shall be specified in the Operating Plan and the time between periodic reviews shall not exceed five (5) years.

No

General comment regarding Attachment 1: SDT should strive to use identical language to event descriptions in the NERC Event Analysis Process and FERC OE-417. Creating a third set of event descriptions is not helpful to system operators. We recommend aligning the Attachment 1 wording with that contained in Attachment 2, DOE Form OE-417 and the EAP whenever possible. Replace the Attachment 1 “NOTE” with the following clarifying wording: NOTE: The Electric Reliability Organization and the Responsible Entity’s Reliability Coordinator will accept the DOE OE-417 form in lieu of Attachment 2 if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422. Initial submittal by Voice within the reporting time frame is acceptable for all events when followed by a hardcopy submittal by Facsimile or e-mail as and if required. Event: Damage or destruction of a Facility Threshold for Reporting: revise language on third item to read, Results from actual or suspected intentional human action, excluding unintentional human errors. Event: Any physical threat that could impact the operability of a Facility This Event category should be deleted. The word “could” is hypothetical and therefore unverifiable and un-auditable. The word “impact” is undefined. Please delete this reporting requirement, or please provide a list of hypothetical “could impact” events, as well as a specific definition and method for determining a specific physical impact threshold for “could impact” events other than “any.” Event: BES Emergency requiring public appeal for load reduction. Replace Event wording with language from #8 on OE-417 reporting form to eliminate reporting confusion. Following this sentence add, “This shall exclude other public appeals, e.g., made for weather, air quality and power market-related conditions, which are not made in response to a specific BES event.” Event: Complete or partial loss of monitoring capability Event wording: Delete the words “or partial” to conform the wording to NERC Event Analysis Process. Event: Transmission Loss Modify to BES Transmission Loss Event Generation Loss Modify to BES Generation Loss

Yes

Form EOP-004, Attachment 2: Event Reporting Form: Delete the Task words “or partial.” Delete the Task words “physical threat that could impact the operability of a Facility.” Make any changes to the VSL’s necessary to align them with the reviewed wording provided above.

Individual

David Burke

Orange and Rockland Utilities, Inc.

No

Requirement R3: Following the sentence ending “in Part 1.2” add the following wording from the Measure to R3: The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. This language must be in the Requirement to be considered during an audit. Measures are not auditable. Requirement R4: Replace the words “an annual review” with the words “a periodic review.” Following the first sentence in R4 add: The frequency of such periodic reviews shall be specified in the Operating Plan and the time between periodic reviews shall not exceed five (5) years.

No

General comment regarding Attachment 1: SDT should strive to use identical language to event descriptions in the NERC Event Analysis Process and FERC OE-417. Creating a third set of event descriptions is not helpful to system operators. We recommend aligning the Attachment 1 wording with that contained in Attachment 2, DOE Form OE-417 and the EAP whenever possible. Replace the Attachment 1 “NOTE” with the following clarifying wording: NOTE: The Electric Reliability Organization and the Responsible Entity’s Reliability Coordinator will accept the DOE OE-417 form in lieu of Attachment 2 if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422. Initial submittal by Voice within the reporting time frame is acceptable for all events when followed by a hardcopy submittal by Facsimile or e-mail as and if required. Event: Damage or destruction of a Facility Threshold for Reporting: revise language on third item to read, Results from actual or suspected intentional human action, excluding unintentional human errors. Event: Any physical threat

that could impact the operability of a Facility This Event category should be deleted. The word “could” is hypothetical and therefore unverifiable and un-auditable. The word “impact” is undefined. Please delete this reporting requirement, or please provide a list of hypothetical “could impact” events, as well as a specific definition and method for determining a specific physical impact threshold for “could impact” events other than “any.” Event: BES Emergency requiring public appeal for load reduction. Replace Event wording with language from #8 on OE-417 reporting form to eliminate reporting confusion. Following this sentence add, “This shall exclude other public appeals, e.g., made for weather, air quality and power market-related conditions, which are not made in response to a specific BES event.” Event: Complete or partial loss of monitoring capability Event wording: Delete the words “or partial” to conform the wording to NERC Event Analysis Process. Event: Transmission Loss Modify to BES Transmission Loss Event Generation Loss Modify to BES Generation Loss
Yes
Form EOP-004, Attachment 2: Event Reporting Form: Delete the Task words “or partial.” Delete the Task words “physical threat that could impact the operability of a Facility.” Make any changes to the VSL’s necessary to align them with the reviewed wording provided above.
Individual
Larry Raczkowski
FirstEnergy Corp
Yes
FE agrees with the revision but has the following comments and suggestions: 1. We request clarity and guidance on R3 (See our comments in Question 4 for further consideration). Also, we suggest a change in the phrase “shall conduct an annual test” to “shall conduct a test each calendar year, not to exceed 15 calendar months between tests”. This wording is consistent with other standards in development such as CIP Version 5. 2.In R4 we suggest a change in the phrase “shall conduct an annual review” to “shall conduct a review each calendar year, not to exceed 15 calendar months between reviews”. This wording is consistent with other standards in development such as CIP Version 5.
No
FE requests the following changes be made to Attachment 1: 1. Pg. 19 / Event: “Voltage deviation on a Facility”. The term “observes” for Entity with Reporting Responsibility be changed to “experiences”. The burden should rest with the initiating entity in consistency with other Reporting Responsibilities. 2. In “Threshold for Reporting”, the language should be expanded to – plus or minus 10% ”of nominal voltage” for greater than or equal to 15 continuous minutes. 3. Pg.20 /Event: “Complete or partial loss of monitoring capability”. The term “partial” should be deleted from the event description to read as follows: Complete loss of monitoring capability and the reporting responsibility requirements to read “Each RC, BA, and TOP that experiences the complete loss of monitoring capability.”
Yes
FE agrees but asks that the defined term “registered entities” in the second sentence be capitalized.
FE supports the standard and has the following additional comments and suggestions: 1. Guideline/Technical Basis Section – FE requests the SDT add specific guidance for each requirement. Much of the information in this section is either included, or should be included in the Background section of the standard. One example of guidance that would help is for Requirement R3 on how an entity could perform the annual test. The comment form for this posting has the following paragraph on pg. 2 which could be used as guidance for R3: “the annual test will include verification that communication information contained in the Operating Plan is correct. As an example, the annual update of the Operating Plan could include calling “others as defined in the Responsibility Entity’s Operating Plan” (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. Note that there is no requirement to test the reporting of events to the Electric Reliability Organization and the Responsible Entity’s Reliability Coordinator.” 2. With regard to the statement in the comment form (pg 2 paragraph 7)“Note that there is no requirement to test the reporting of events to the Electric Reliability Organization and the Responsible Entity’s Reliability Coordinator.”, requirement R3 only includes the ERO as an entity and should also include the Reliability Coordinator. 3. The measure M3 says that an entity can use an actual event as a test to meet R3. Does this mean just 1 actual event will meet R3,

or is the intent that all possible events per 1.2 are tested? Would like some clarity on this measure.
Individual
Linda Jacobson-Quinn
Farmington Electric Utility System
Yes
No
The reporting threshold for “Complete or partial loss of monitoring capability” should be modified to include the loss of additional equipment and not be limited to State Estimator and Contingency Analysis. Some options have been included: Affecting a BES control center for ≥ 30 continuous minutes such that Real-Time monitoring tools are rendered inoperable. Affecting a BES control center for ≥ 30 continuous minutes to the extent a Constrained Facility would not be identified or an Adverse Reliability Impact event could occur due to lack of monitoring capability. Affecting a BES control center for ≥ 30 continuous minutes such that an Emergency would not be identified or ma
Yes
Individual
Michael Falvo
Independent Electricity System Operator
Yes
We concur with the changes as they provide better streamlining of the four key requirements, with enhanced clarity. However, we are unclear on the intent of Requirement R3, in particular the phrase “not including notification to the Electric Reliability Organization” which begs the question on whether or not the test requires notifying all the other entities as if it were a real event. This may create confusion in ensuring compliance and during audits. Suggest the SDT to review and modify this requirement as appropriate.
Yes
No
We are unable to comment on the proposed new section as the section does not contain any description of the proposed process or the interface requirements to support the report collecting system. We reserve judgment on this proposal and our right to comment on the proposal when the proposed addition is posted.
We do not agree with the MEDIUM VRF assigned to Requirement R4. Re stipulates a requirement to conduct an annual review of the event reporting Operating Plan in Requirement R1, which itself is assigned a VRF of LOWER. We are unable to rationalize why a subsequent review of a plan should have a higher reliability risk impact than the development of the plan itself. Hypothetically, if an entity doesn’t develop a plan to begin with, then it will be assigned a LOWER VRF, and the entity will have no plan to review annually and hence it will not be deemed non-compliant with requirement R4. The entity can avoid being assessed violating a requirement with a MEDIUM VRF by not having the plan to begin with, for which the entity will be assessed violating a requirement with a LOWER VRF. We suggest changing the R4 VRF to LOWER.
Group
Southern Company Services
Antonio Grayson
No
There are approximately 17 event types for which Responsible Entities must have a process for communicating such events to the appropriate entities and R3 states that “The Responsible Entity shall conduct an annual test of the communications process”. It is likely that the same communications process will be used to report multiple event types, so Southern suggest that the Responsible Entities conduct an annual test for each unique communications process. Southern suggest that this requirement be revised to state “Each Responsible Entity shall conduct an annual

test of each unique communications process addressed in R1.2". • In Attachment 1, for Event: "Damage or destruction of a Facility", SDT should consider removing "Results from actual or suspected intentional human action" from the "Threshold for Reporting" column. The basis for this suggestion is as follows: o The actual threshold should be measurable, similar to the thresholds specified for other events in Attachment 1. [Note: The first two thresholds identified (i.e., "Affects and IROL" and "Results in the need for actions to avoid an Adverse Reliability Impact") are measurable and sufficiently qualify which types of Facility damage should be reported.] o The determination of human intent is too subjective. Including this as a threshold will cause many events to be reported that otherwise may not need to be reported. (e.g., Vandalism and copper theft, while addressed under physical threats, is more appropriately classified as damage. These are generally intentional human acts and would qualify for reporting under the current guidance in Attachment 1. They may be excluded from reporting by the threshold criteria regarding IROLs and Adverse Reliability Impact, if the human intent threshold is removed.) o It may be more appropriate to address human intent in the event description as follows: "Damage or destruction of a Facility, whether from natural or human causes". Let the thresholds related to BES impact dictate the reporting requirement. • In Attachment 1, for Event: "Complete or partial loss of monitoring capability", SDT should consider changing the threshold criteria to state: "Affecting a BES control center for ≥ 30 continuous minutes such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." There may be instances where the tools themselves are out of commission, but the control center personnel have sufficiently accurate models and alternate methods of performing the required analyses.

No

It appears that the SDT has incorporated the reporting requirements for CIP-008 "reportable Cyber Security Incidents"; however, the "recognition" requirements remain in CIP-008 Reliability Standard. Southern understands the desire to consolidate reporting requirements into a single standard, but it would be clearer for Cyber Security Incidents if both the recognition and reporting requirements were in one reliability standard and not spread across multiple standards. As it relates to the event type "Loss of Firm Load for > 15 minutes", Southern suggests that the SDT clarify if weather related loss of firm load is excluded from the reporting requirement. As it relates to the event type "Loss of all voice communication capability", Southern suggest that the SDT clarify if this means both primary and backup voice communication systems or just primary voice communication systems. Referring to "CIP-008-3 or its successor" in Requirement R1.1 is problematic. This arrangement results in a variable requirement for EOP-004-2 R1. The requirements in a particular version of a standard should be fixed and not variable. If exceptions to applicable events change, a revision should be made to EOP-004 to reflect the modified requirement.

Yes

Move the Background Section (pages 4-9) to the Guideline and Technical Basis section. They are not needed in the main body of the standard. Each "Entity with Reporting Responsibility" in the one-hour reporting table (p. 17) should be explicitly listed in the table, not pointed to another variable location. The criterion for "Threshold for Reporting" in the one-hour reporting table (p. 17) should be explicitly listed in the table, not pointed to another variable location. Please specify the voltage base against which the +/- 10% voltage deviation on a Facility is to be measured in the twenty-four hour reporting table (p. 19).

Individual

John Seelke

Public Service Enterprise Group

Yes

No

We agreed with most of the revisions. However, for the 24-hour reporting time frame portion of the EOP-004 Attachment 1: Reportable Event that starts on p. 18, we have these concerns: a. Why was "RC" left out in the first row? RC is in the second row that also addresses a "Facility." We believe that "RC" was inadvertently left out. b. In the first row, entities such as a BA, TO, GO, GOP, or DP would not know whether damage or destruction of one of its Facilities either "Affects an IROL (per FAC-014)" or "Results in the need for actions to avoid an Adverse Reliability Impact." FAC-014-2, R5.1.1 requires Reliability Coordinators provide information for each IROL on the "Identification and status of the

associated Facility (or group of Facilities) that is (are) critical to the derivation of the IROL" to entities that do NOT include the entities listed above. And frankly, those entities would not need to know. The reporting requirements associated with "Damage or destruction of a Facility" need to be changed so that the criteria for reporting by an entity whose Facilities experience damage or destruction does not rely upon information that the entity does not possess. c. A possible route to achieve the results in b. above is described below: i. All Facilities that are damaged or destroyed that "Results from actual or suspected intentional human action" would be reported to the ERO by the entity experiencing the damage or destruction. ii. All Facilities that are damaged or destroyed OTHER THAN THAT due to an "actual or suspected intentional human action" would be reported to the RC by the entity experiencing the damage or destruction. Based upon those reports, the RC would be required to report whether the reported damage or destruction of a Facility "Affects an IROL (per FAC-010)" or "Results in the need for actions to Avoid an Adverse Reliability Consequence." (The RC may need to modify its data specifications in IRO-010-1a - Reliability Coordinator Data Specification and Collection - to specify outages due to "damage or destruction of a Facility." We also note that "DP" is not included in IRO-010-1a, but "LSE" is included. DPs are required to also register as LSEs if they meet certain criteria. See the "Statement of Compliance Registry Criteria, Rev. 5.0", p.7. For this reason, we suggest that DP be replaced with LSE in EOP-004-2.) d. To implement the changes in c. above, we suggest that the first row be divided into two rows: i. FIRST ROW: This would be like the existing first row on page 18, except "RC" would be added to the column for "Entity with Reporting Responsibility" and the only reporting threshold would be ""Results from actual or suspected intentional human action." ii. SECOND ROW: The Event would be "Damage or destruction of a Facility of a BA, TO, TOP, GO, GOP, or LSE," the Entity, the Reporting Responsibility would be "The RC that has the BA, TOP, GO, GOP, or LSE experiencing the damage or destruction in its area," and the Threshold for Reporting would be "Affects an IROL (per FAC-010)" or "Results in the need for actions to avoid an Adverse Reliability Consequence."

Yes

Group

Dominion

Connie Lowe

No

While Dominion believes these are positive changes, we are concerned that placing actual calls to each of the "other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies" may be seen by one or more of those called as a 'nuisance call'. Given the intent is to insure validity of the contact information (phone number, email, etc), we suggest revising the standard language to support various forms of validation to include, documented send/receipt of email, documented verification of phone number (use of phone book, directory assistance, etc).

Yes

Comments: While Dominion agrees that the revisions are a much appreciated improvement, we are concerned that Attachment 1 does not explicitly contain the 'entities which must be, at a minimum, notified. Attachment 2 appears to indicate that only the ERO and the Reliability Coordinator for the Entity with Reporting Responsibility need be informed. However, the background section indicates that the Entity with Reporting Responsibility is also expected to contact local law enforcement. We therefore suggest that Attachment 2 be modified to include local law enforcement. Page 26 redline; Attachment 1; Event – Damage or destruction of a Facility; Threshold for Reporting – Results from actual or suspected intentional human action; Dominion is concerned with the ambugity that this could be interpreted as applying to distribution. Page 27 redline; Attachment 1; Event – Any physical threat that could impact the operability of a Facility; Dominion is concerned the word "could" is hypothetical and therefore unverifiable and un-auditable. The SDT could provide a list of hypothetical "could impact" events, as well as a specific definition and method for determining a specific physical impact threshold for "could impact" events other than "any."

Yes

While Dominion supports this addition, we suggest adding to the sentence "NERC will establish a system to collect report forms as established for this section or reliability standard…..."

Dominion believes that the reporting of “Any physical threat that could impact the operability of a Facility4” may overwhelm the Reliability Coordinator staff with little to no value since the event may have already passed. This specific event uses the phrase “operability of a Facility” yet “operability” is not defined and is therefore ambiguous. We do support the reporting to law enforcement and the ERO but do not generally support reporting events that have passed to the Reliability Coordinator. Attachment 2; section 4 Event Identification and Description: The type of events listed should match the events as they are exactly written in Attachment 1. As it is currently written, it leaves room for ambiguity. M3 – Dominion objects to having to provide additional supplemental evidence (i.e. operator logs), and the SDT maybe want to include a requirement for NERC to provide a confirmation that the report has been received.
Individual
Terry Harbour
MidAmerican Energy
No
See the NSRF comments. The real purpose of this requirement appears to be to assure operators are trained in the use of the procedure, process, or plan that assures proper notification. PER-005 already requires a systematic approach to training. Reporting to other affected entities is a PER-005 system operator task. Therefore this requirement already covered by PER-005 and is not required. Organizations are also required to test their response to events in accordance with CIP-008 R1.6. Therefore this requirement is covered by other standards and is not needed. Inclusion of this standard would place entities in a double or possible triple jeopardy. The SDT may need to expand M3 reporting options, by stating “… that the annual test of the communication process of 1.2 (e.g. communication via e-mail, fax, phone, ect) was conducted”. R4 is an administrative requirement with little reliability value and should be deleted. It would likely be identified as a requirement that that should be eliminated as part of the request by FERC to identify strictly administrative requirements in FERC’s recent order on FFTR.
No
Several modifications need to be made to Table 1 to enhance clarity and delete unnecessary or duplicate items. The stated reliability objective of EOP-004 and the drafting team is to reduce and prevent outages which could lead to cascading through reporting. It is understood that the EOP-004 Attachment 1 is to cover similar items to the DOE OE-417 form. Last, remember that FERC recently asked the question of what standards did not provide system reliability benefits. Those reports that cannot show a direct threat to a potential cascade need to be eliminated. Table 1 should always align with the cascade risk objectives and OE-417 where possible. Therefore Table 1 should be modified as follows: 1. Completely divorce CIP-008 from EOP-004. Constant changes, the introduction of new players such as DOE and DHS, and repeated congressional bills, make coordination with CIP-008 nearly impossible. Cyber security and operational performance under EOP-004 remain separate and different despite best efforts to combine the two concepts. 2. Modify R1.2 to state that ERO notification only is required for Table 1. This is similar to the DOE OE-417 notification. Notification of other entities is a best practice, not a mandatory NERC standard. If entities want to notify neighboring entities, they may do so as a best practice guideline. 3. Better clarity for communicating each of the applicable events listed in the EOP-004 Attachment 1 in accordance with the timeframes specified are needed. MidAmerican suggests a forth column be added to the table to clearly identify who must be notified within the specified time period or at a minimum, that R1.2 be revised to clearly state that only the ERO must be notified to comply with the standard. 4. Consolidate OE-417 concepts on physical attack and cyber events by consolidating OE-417 items 1, 2, 9 and 10 to: Verifiable, credible, and malicious physical damage (excluding natural weather events) to a BES generator, line, transformer, or bus that when reported requires an appropriate Reliability Coordinator or Balancing Authority to issue an Energy Emergency Alert Level 2 or higher. The whole attempt to discuss a NERC Facility and avoid adverse reliability impacts overreaches the fundamental principal or reporting for an emergency that could result in a cascade. 5. The wording “affects an IROL (per FAC-014),” is too vague and not measurable. Many facilities could affect an IROL, but fewer facilities if lost would cause an IROL. Change “affects” to “results in” 6. Recommend that Adverse Reliability Impact be deleted and be replaced with actual EEA 2 or EEA 3 level events. 7. The phrase “results from actual or suspected intentional human action” is vague and not measurable. This line item used the term “suspected” which relates to “sabotage”. MidAmerican recommends that “Results from actual or suspected intentional human action” be deleted. If not deleted the phrase should be replaced with

“Results from verifiable, credible, and malicious human action intended to damage the BES.” 8. Delete “Any physical threat…” as vague, and difficult to measure in a “perfect” zero defect audit environment, and as already covered by item 1 above. If not deleted, at a minimum replace “Any physical threat”, with “physical attack” as being measureable and consistent with DOE OE-417. 9. With the use of “i.e.” the SDT is mandating that each other entity must be contacted. The NSRF believes that the SDT meant that “e.g.” should be used to provide examples. The SDT may wish to add another column to Attachment 1 to provide clarity. 10. The phrase “or partial loss of monitoring capability” is too vague and should be deleted. In addition, the 30 minute window is too short for EMS and IT staff to effectively be notified and troubleshoot systems before being subjected to a federal law requiring reporting and potential violations. The time frame should be consistent with the EOP-008 standard. If not deleted, replace with “Complete loss of SCADA affecting a BES control center for ≥ 60 continuous minutes such that analysis tools of State Estimator and/or Contingency Analysis are rendered inoperable. 11. Transmission loss should be deleted. The number of transmission elements out does not directly correlate to BES stability and cascading. For that reason alone, this item should be deleted or it would have already been included in the past EOP-004 standard. In addition, large footprints can have multiple storms or weather events resulting in normal system outages. This should not be a reportable event that deals with potential cascading. 12. Modify the threshold of “BES emergency requiring a public appeal…” to include, “Public appeal for a load reduction event resulting from a RC or BA implementing its emergency energy and capcity plans documented in EOP-001.” Public appeals for conservation that aren't used to avoid capacity and energy emergencies should be clearly excluded. 13. Add a time threshold to complete loss of off-site power to a nuclear plant. Nuclear plants are to have backup diesel generation that last for a minimum amount of time. A threshold recognizing this 4 hour or longer window needs to be added such as complete loss of off-site power to a nuclear plant for more than 4 hours. Also see the NSRF comments.
No
See the NSRF comments. The NERC Rules of Procedure Section 807 already addresses the dissemination of Disturbance data, as does Appendix 8 Phase 1 with the activation of NERC’s crisis communication plan, and the ESISAC Concept of Operations. The addition of proposed Section 812 is not necessary. The Reliability Coordinator, through the use of the RCIS, would disseminate reliability notifications if it is in turn notified per R1.2. (As stated in the in the Clean copy of EOP-004-2)
See the NSRF comments.
Individual
Brenda Lyn Truhe
PPL Electric Utilities
Yes
Yes
PPL EU thanks the SDT for the changes made in this latest proposal. We feel our prior comments were addressed. Regarding the event 'Transmission Loss': For your consideration, please consider adding a footnote to the event ‘Transmission Loss’ such that weather events do not need to be reported. Also please consider including 'operation contrary to design' in the threshold language. E.g. consistent with the NERC Event Analysis table, the threshold would be, ‘Unintentional loss, contrary to design, of three or more BES Transmission Facilities.’
Yes
We appreciate the inclusion of the Process Flowchart on Page 9 of the draft standard. We submit for your consideration, removing the line from the NO decision box to the ‘Report Event to ERO, Reliability Coordinator’ box. It seems if the event does not need reporting per the decision box, this line is not needed. For clarity in needed actions, please consider using a decision box following flowcharting standards such as, a decision box containing a question with a Yes and a No path. The decision box on ‘Report to Law Enforcement ?’ does not have a Yes or No. Perhaps, this decision box is misplaced, or is it intended to occur always and not have a different path with different actions? Ie. should it be a process box? Thank you for your work on this standard.
Individual
John Martinsen

Public Utility District No. 1 of Snohomish County
Yes
This is an excellent improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
This is an excellent improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
No
This type of activity and process is better suited to NAESBE than it is to NERC Compliance.
SNPD suggest moving these administrative activities to NAESB. R1: There is merit in having a plan as identified in R1, but is this a need to support reliability or is it a business practice? Should it be in NAESB's domain? R2, R3 & R4: These are not appropriate for a Standard. If you don't annually review the plan, will reliability be reduced and the BES be subject to instability, separation and cascading? If DOE needs a form filled out, fill it out and send it to DOE. NERC doesn't need to pile on. Gerry Cauley and Mike Moon have been stressing results and risk based, actual performance based, event analysis, lessons learned and situational awareness. EOP-004 is primarily a business preparedness topic and identifies administrative procedures that belong in the NAESB domain.
Individual
Russell A. Noble
Cowlitz County PUD
Yes
Yes
Yes
Cowlitz is pleased with changes made to account for the difficulties small entities have in regard to reporting time frames. Although Cowlitz is confident that the current draft is manageable for small entities, we propose that the resulting reports this Standard will generate will contain many insignificant events from the event types "Damage or destruction of a Facility," and "Any physical threat that could impact the operability of a Facility." In particular, examples would be limited target practice on insulators, car-pole accidents, and accidental contact from tree trimming or construction activities. Cowlitz suggests that at least a >= 100 MW (200 MW would be better) and/or >= N-2 impact threshold be established for these event types. Also, Cowlitz suggests the statement "results from actual or suspected intentional human action" be changed to "results from actual or suspected intentional human action to damage or destroy a Facility." A human action may be intentional which can result in damage to a facility, but the intent may have been of good standing, and not directed at the Facility. For example, the intent may have been to legally harvest a tree, or move equipment under a line. Cowlitz believes the above proposed changes would benefit the ERO, both in reduction of nuisance reports and possible violations over minimal to no impact BES events.
Group
SPP Standards Review Group
Robert Rhodes
No
There needs to be a more granular definition of which entities should be included in the annual testing requirement in R3. To clarify what must be tested we propose the following language to replace the last sentence in M3. The annual test requirement is considered to be met if the responsible entity implements any communications process in the Operating Plan during an actual event. If no actual event was reported during the year, at least one of the communication processes in the Operating Plan must be tested to satisfy the requirement. We do not believe the time-stamping requirement in M3 and M4 contribute to the reliability of the BES. A dated review should be sufficient.
No
To obtain an understanding of the drivers behind the events in Attachment 1, we would like to see where these events come from. If the events are required in standards, refer to them. If they are in

the existing event reporting list, indicate so. If they are coming from the EAP, let us know. We have a concern that, as it currently exists, Attachment 1 can increase our reporting requirements considerably. We also have concerns about what appears to be a lack of coordination between EAP reporting requirements and those contained in Attachment 1. For example, the EAP reporting requirement is for the complete loss of monitoring capability whereas Attachment 1 adds the requirement for reporting a partial loss of monitoring capability. It appears that some of the EAP reporting requirements are contained in Attachment 1. We have concerns that this is beyond the scope of the SAR and should not be incorporated in this standard. We have concern with several of the specific event descriptions as contained in Attachment 1: Damage or destruction of a Facility – We are comfortable with the proposed definition of Adverse Reliability Impact but have concerns with the existing definition of ARI. Any physical threat that could impact the operability of a Facility1 – We take exception to this event in that is goes beyond what is currently required in EOP-004-1, including DOE reporting requirements, and the EAP reporting requirements. We do not understand the need for this event type and object to the potential for excessive reporting required by such an event type. Additionally, we are concerned about the potential for multiple reporting of a single event. This same concern applies to several other events including Damage or destruction of a Facility, Loss of firm load for ≥ 15 minutes, System separation, etc. When multiple entities are listed as the Entity with Reporting Responsibility, Attachment 1 appears to require each entity in the hierarchy to submit a report. There should only be one report and it should be filed by the entity owning the event. The SDT addressed this issue in its last posting but the issue still remains and should be reviewed again. BES Emergency resulting in automatic firm load shedding – For some reason, not stipulated in the Consideration of Comments, the action word in the Entity with Reporting Responsibility was changed from 'experiences' to 'implements'. We recommend changing it back to 'experiences'. Automatic load shedding is not implemented. It does not require human intervention. It's automatic. Voltage deviation on a Facility – Similar to the comment on automatic load shedding above, the action word was changed from 'experiences' to 'observes'. We again recommend that it be changed back to 'experiences'. Using observes obligates a TOP, who is able to see a portion of a neighboring TOP's area, to submit a report if that TOP observed a voltage deviation in the neighboring TOP's area. The only reporting entity in this event should be the TOP within whose area the voltage deviation occurred. Complete or partial loss of monitoring capability – Clarification on partial loss of monitoring capability and inoperable are needed. Also, the way the Threshold is written, it implies that a State Estimator and Contingency Analysis are required. To tone this down, insert the qualifier 'such as' in front of State Estimator.

No

We have two concerns about the proposed change to the RoP. One, we have concerns that our information and data will be circulated to an as yet undetermined audience which appears to be solely under NERC's control. Secondly, there isn't sufficient detail in the clearinghouse concept to support comments at this time.

The VRF for R1 is Lower which is fine. The issue is that R4, which is the review of the plan contained in R1, has a Medium VRF. We recommend moving the VRF of R4 to Lower. We recommend deleting the phrase '…supplemented by operator logs or other operating documentation…' as found in the first sentence of M2. A much clearer reference is made to operator logs and other operating documentation in the second sentence. The duplication is unnecessary. What will happen with the accompanying information contained in the Background section in the draft standard? Will it be moved to the Guideline and Technical Basis at the end of the standard as the information contained in the text boxes? This is valuable information and should not be lost.

Group

Florida Municipal Power Agency

Frank Gaffney

No

First, FMPA believes the standard is much improved from the last posting and we thank the SDT or their hard work. Having said that, there are still a number of issues, mostly due to ambiguity in terms, which cause us to vote Negative. R3 and R4 should be combined into a single requirement with two subparts, one for annual testing, and another to incorporate lessons learned from the annual testing into the plan (as opposed to an annual review). The word "test" is ambiguous as used in R3, e.g., does a table top drill count as a "test"? Is the intent to "test" the plan, or "test" the phone

numbers, or what?

No

The bullet on “any physical threat” is un-measurable. What constitutes a “threat”? FMPA likes the language used in the comment form discussing this item concerning the judgment of the Responsible Entity, but, the way it is worded in Attachment 1 will mean the judgment of the Compliance Enforcement Authority, not the Responsible Entity. Presumably, the Responsible Entity will need to develop methods to identify physical threats in accordance with R1; hence, FMPA suggests rewording to: “Any physical threat recognized by the Responsible Entity through processes established in R1 bullet 1.1”. We understand this introduces circular logic, but, it also introduces the “judgment of the Responsible Entity” into the bullet. On the row of the table on voltage deviation, replace the word “observes” with “experiences”. It is possible for one TOP to “observe” a voltage deviation on another TOP’s system. It should be the responsibility of the TOP experiencing the voltage deviation on its system to report, not the one who “observes”. One the row on islanding, it does not make sense to report islanding for a system with load less than the loss of load metrics and we suggest using the same 300 MW threshold for a reporting threshold. One the row on generation loss, some clarification on what type of generation loss (especially in the time domain) would help it be more measurable, e.g., concurrent forced outages. One the row on transmission loss, the same clarity is important, e.g., three or more concurrent forced outages. On the row on loss of monitoring, while FMPA likes the threshold for “partial loss of monitoring capability” for those systems that have State Estimators, small BAs and TOPs will not need or have State Estimators and the reporting threshold becomes ambiguous. We suggest adding something like loss of monitoring for 25% of monitored points for those BAs and TOPs that do not have State Estimators.

Yes

In R1, bullet, it is a bit ambiguous whether the list of organizations to be communicated with is an exhaustive list (i.e.) or a list of examples (e.g.). The list is preceded by an “i.e.” which indicates the former, but includes an “or” which indicates the latter. We are interpreting this as meaning the list is exhaustive as separated by semi-colons, but that the last phrase separated by commas is a list of examples. Is this the correct interpretation? The Rules of Procedure language for data retention (first paragraph of the Evidence Retention section) should not be included in the standard, but instead referred to within the standard (e.g., “Refer to Rules of Procedure, Appendix 4C: Compliance Monitoring and Enforcement Program, Section 3.1.4.2 for more retention requirements”) so that changes to the RoP do not necessitate changes to the standard.

Group

LG&E and KU Services

Brent Ingebrigtson

Yes

No

The SDT should consider more clearly defining the Threshold for Reporting for the Event: “Any physical threat that could impact the operability of a Facility” to only address those events that have an Adverse Reliability Impact. Some proposed language might be: “Threat to a Facility excluding weather related threats that could result in an Adverse Reliability Impact.” For those events specifically defined in the ERO Events Analysis Process, the SDT should consider revising the language to be more consistent with the language included in the ERO Events Analysis Process. Here is some recommended language: 1. EVENT: Transmission loss THRESHOLD FOR REPORTING: “Unintentional loss, contrary to design, of three or more BES Transmission Facilities (excluding successful automatic reclosing) caused by a common disturbance. 2. EVENT: “Complete or partial loss of monitoring capability” – could be revised to read “Complete loss of SCADA control or monitoring functionality” THRESHOLD FOR REPORTING: “Affecting a BES control center for ≥ 30 continuous minutes such that analysis tools (e.g. State Estimator, Contingency Analysis) are rendered inoperable”.

Yes

The Violation Severity Level for Requirement R2 should be revised to read “...hours after recognizing an event requiring reporting...” This will make the language in the VSL consistent with the language in

Attachment 1.
Individual
Thomas Washburn
FMPP
See FMPA's comments
Group
MRO NSRF
WILL SMITH
No
R3 states: Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. R1.2 states: A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies. With the use of "i.e." the SDT is mandating that each other entity must be contacted. The NSRF believes that the SDT meant that "e.g." should be used to provide examples. The SDT may wish to add another column to Attachment 1 to provide clarity. R3 requires and annual test that would include notification of: "other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies." Since NERC see no value in receiving these test notification we are doubtful other entities identified in R1.2 would find them of value. The real purpose of this requirement appears to be to assure operators are trained in the use of the procedure, process, or plan that assures proper notification. PER-005 already requires a systematic approach to training. It is hard to comprehend an organization not identifying this as a Critical Task, and if they failed to identify it as a Critical Task that this would not be a violation. Therefore this requirement is not required. Furthermore organizations test their response to events in accordance with CIP-008 R1.6. Therefore this requirement is covered by other standards and is not needed. The SDT may need to address this within M3, by stating "… that the annual test of the communication process of 1.2 (e.g. communication via e-mail, fax, phone, ect) was conducted". R4 states: Each Responsible Entity shall conduct an annual review of the event reporting Operating Plan in Requirement R1. We question the value of requiring an annual review. If the Standard does not change, there seems little value in requiring an annual review. This appears to be an administrative requirement with little reliability value. It would likely be identified as a requirement that that should be eliminated as part of the request by FERC to identify strictly administrative requirements in FERC's recent order on FFTR. We suggest it be eliminated.
No
R1.2 states: A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies. This implies not only does NERC need to be notified within the specified time period but that: "other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies." are also required to be notified within in the time periods specified. We suggest a forth column be added to the table to clearly identify who must be notified within the specified time period or that R1.2 be revised to clearly state that only NERC must be notified to comply with the standard. With the use of "i.e." the SDT is mandating that each other entity must be contacted. The NSRF believes that the SDT meant that "e.g." should be used to provide examples. The SDT may wish to add another column to Attachment 1 to provide clarity. Also with regards to Attachment 1, the following comments are provided: 1. Instead of referring to CIP-008 (in the 1 hour reporting section), quote the words from CIP-008, this will require coordination of future revisions but will assure clarity

in reporting requirements. 2 Under “Damage or destruction of a Facility” a. The wording “affects an IROL (per FAC-014),” is too vague. Many facilities could affect an IROL, not as many if lost would cause an IROL. b. Adverse Reliability Impact is defined as: “The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection.” There are an infinite number of routine events that result in the loss of generation plants due to inadvertent actions that somehow also damaged equipment. Any maintenance activity that damaged a piece of equipment that causes a unit to trip or results in a unit being taken off line in a controlled manner would now be reportable. This seems to be an excessive reporting requirement. Recommend that Adverse Reliability Impact be deleted and be replaced with actual EEA 2 or EEA 3 level events. c. The phrase “Results from actual or suspected intentional human action.” This line item used the term “suspected” which relates to “sabotage”. Recommend the following: Results from actual or malicious human action intended to damage the BES. 3. “Any physical threat that could impact the operability of a Facility1” The example provided by the drafting team of a train derailment exemplifies why this requirement should be deleted. A train derailment of a load of banana’s more than likely would not threaten a nearby BES Facility. However a train carrying propane that derails carrying propane could even if it were 10 miles away. Whose calculation will be used to determine if an event could have impacted the asset? As worded there is too much ambiguity left to the auditor. We suggest the drafting team clarify by saying “Any event that requires the a BES site be evacuated for safety reasons” Furthermore if weather events are excluded, we are hard pressed to understand why this information is important enough to report to NERC. So barring an explanation of the purpose of this requirement, including why weather events would be excluded, we suggest the requirement be deleted. Please note that if you align this with “Physical attack” with #1 of the OE-417. This clearly states what the SDT is looking for. 4. The phrase “or partial loss of monitoring capability” is too vague. Further definitions of “inoperable” are required to assure consistent application of this requirement. Recommend that “Complete loss of SCADA affecting a BES control center for ≥ 30 continuous minutes such that analysis tools of State Estimator and/or Contingency Analysis are rendered inoperable. Or, Complete loss of the ability to perform a State Estimator or Contingency Analysis function, the threshold of 30 mins is too short. A 60 min threshold will align with EOP-008-1, R1.8. Since this is the time to implement the contingency back up control center plan. 5. Event: Voltage deviation on a Facility. ATC believes that the term “observes” for Entity with Reporting Responsibility be changed back to “experiences” as originally written. The burden should rest with the initiating entity in consistency with other Reporting Responsibilities. Also, for Threshold for Reporting, ATC believes the language should be expanded to - plus or minus 10% ”of target voltage” for greater than or equal to 15 continuous minutes. 6. Event: Transmission loss. ATC recommends that Threshold for Reporting be changed to read “Unintentional loss of four, or more Transmission Facilities, excluding successful automatic reclosing, within 30 seconds of the first loss experienced and for 30 continuous minutes. Technical justification or Discussion for this recommended change: In the instance of a transformer-line-transformer, scenario commonly found close-in to Generating stations, consisting of 3 defined “facilities”, 1 lightning strike can cause automatic unintentional loss by design. Increase the number of facilities to 4. In a normal shoulder season day, an entity may experience the unintentional loss of a 138kv line from storm activity, at point A in the morning, a loss of a 115kv line from a different storm 300 miles from point A in the afternoon, and a loss of 161kv line in the evening 500 miles from point A due to a failed component, if it is an entity of significant size. Propose some type of time constraint. Add time constraint as proposed, 30 seconds, other than automatic reclosing. In the event of dense lightning occurrence, the loss of multiple transmission facilities may occur over several minutes to several hours with no significant detrimental effect to the BES, as load will most certainly be affected (lost due to breaker activity on the much more exposed Distribution system) as well. Any additional loss after 30 seconds must take into account supplemental devices with intentional relay time delays, such as shunt capacitors, reactors, or load tap changers on transformers activating as designed, arresting system decay. In addition, Generator response after this time has significant impact. Please clarify or completely delete why this is included within this version when no basis has been give and it is not contained w3ithin the current enforceable version. 7. Modify the threshold of “BES emergency requiring a public appeal…” to include, “Public appear for a load reduction event resulting for a RC or BA implementing its emergency operators plans documented in EOP-001.” The reason is that normal public appeals for conservation should be clearly excluded. 8. Add a time threshold to complete loss of off-site power to a nuclear plant. Nuclear plants are to have backup diesel generation that last for a minimum amount of time. A threshold recognizing this 4 hour or

longer window needs to be added such as complete loss of off-site power to a nuclear plant for more than 4 hours. 9. Delete “Transmission loss”. The loss of a specific number of elements has no direct bearing on the risk of a system cascade. Faults and storms can easily result in “unintentional” the loss of multiple elements. This is a flawed concept and needs to be deleted
Yes
ATC believes that the NERC Rules of Procedure Section 807 already addresses the dissemination of Disturbance data, as does Appendix 8 Phase 1 with the activation of NERC’s crisis communication plan, and the ESISAC Concept of Operations. The addition of proposed Section 812 is not necessary. The Reliability Coordinator, through the use of the RCIS, would disseminate reliability notifications if it is in turn notified per R1.2. (As stated in the in the Clean copy of EOP-004-2)
R1 states: “Each Responsible Entity shall have an event reporting Operating Plan that includes:” The definition of Operating Plan is: “A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan.” This appears to us to be too prescriptive and could be interpreted to require a series of documents to for reporting issues to NERC. We suggest the following wording: R1. Each Responsible Entity shall have document methodology(ies) or process(es) for: 1.1. Recognizing each of the applicable events listed in EOP-004 Attachment 1. 1.2. Reporting each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization. LES Comment: [R1] We are concerned by the significant amount of detail an entity would be required to contain within the Operating Plan as part of Requirement R1. Rather than specifying an entity must have a documented process for recognizing each of the events listed in EOP-004-2 Attachment 1, at a minimum, consider removing the term “process” in R1.1 and replacing with “guideline” to ensure operating personnel are not forced to adhere to a specific sequence of steps and still have the flexibility to exercise their own judgment. Section 5 of the standard (Background) should be moved to the Guideline and Technical Basis document. A background that long does not belong in the standard piece as it detracts from the intent of the standard itself.
Group
Progress Energy
Jim Eckelkamp
No
It should be clear that the Operating Plan can be multiple procedures. It is an unnecessary burden to have entities create a new document outlining the Operating Plan. Having to create a new Operating Plan would not improve reliability and would further burden limited resources. The annual testing required by R3 should be clarified. Do all communication paths need to be annually tested or just one path? An actual event may only utilize one communication 'leg' or 'path' and leave others untested and untilized. Entities may have a corporate level procedure that 'hand-shakes' with more localized procedures that make up the entire Operating Plan. Must all communications processes be tested to fulfill the requirement? If an entity has 'an actual event' it is not necessarily true that their Operating Plan has been exercised completely, yet this one 'actual event' would satisfy M3 as written.
Within attachment 1 (Reportable Events) an exclusion is allowed for weather related threats. PGN recommends a more generic approach to include natural events such as forest fires, sink holes, etc. This would alleviate some reporting burdens in areas that are prone to these types of events.
Individual
Bob Thomas
Illinois Municipal Electric Agency
No
IMEA reluctantly (in recognition of the SDT's efforts and accomplishments to date) cast a Negative vote for this project primarily based on R3 because it is attempting to fix a problem that does not exist and impacts small entity resources in particular. IMEA is not aware of seeing any information regarding a trend, or even a single occurance for that matter, in a failure to report an event due to

failure in reporting procedures. A small entity is less likely to experience a reportable event, and therefore is less likely to be able to take advantage of the provision in M3 to satisfy the annual testing through imiplementation of an actual event. If there is a problem that needs to be fixed, it would make much more sense to replace the language in R3 with a simple requirement for the RC, BA, IC, TSP, TOP, etc. to inform the TO, DP, LSE if there is a change in contact information for reporting an event. It is hard to believe that an RC, BA, IC, TSP, TOP, etc. is going to want to be annually handling numerous inquiries from entities regarding the accuracy of contact information. The impact of unnecessary requiements on entity resources, particularly small entities', is finally starting to get some meaningful attention at NERC and FERC. It would be a mistake to adopt another unnecessary requirement as currently specified in R3.
No
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports comments submitted by ATC.
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Individual
Andrew Z. Pusztai
Amercican Transmission Company, LLC
No
ATC recommends eliminating R4 altogether. If R3, the annual test, is conducted as part of the Operating Plan, R4 is merely administrative, and does not add value to reliability.
No
ATC is proposing changes to the following Events in Attachment 1: (Reference Clean Copy of the Standard) 1) Pg. 18/ Event: Any Physical threat that could impact the operability of a Facility. ATC is proposing a language change to the Threshold- “Meets Registered Entities criteria stated in its Event Reporting Operating Plan, in addition to excluding weather.” 2) Pg. 19 / Event: Voltage deviation on a Facility. ATC believes that the term “observes” for Entity with Reporting Responsibility be changed back to “experiences” as originally written. The burden should rest with the initiating entity in consistency with other Reporting Responsibilities. Also, for Threshold for Reporting, ATC believes the language should be expanded to - plus or minus 10% ”of target voltage” for greater than or equal to 15 continuous minutes. 3) Pg. 19/ Event: Transmission loss. ATC recommends that Threshold for Reporting be changed to read “Unintentional loss of four, or more Transmission Facilities, excluding successful automatic reclosing, within 30 seconds of the first loss experienced and for 30 continuous minutes. Technical justification or Discussion for this recommended change: In the instance of a transformer-line-transformer, scenario commonly found close-in to Generating stations, consisting of 3 defined “facilities”, 1 lightning strike can cause automatic unintentional loss by design. Increase the number of facilities to 4. In a normal shoulder season day, an entity may experience the unintentional loss of a 138kv line from storm activity, at point A in the morning, a loss of a 115kv line from a different storm 300 miles from point A in the afternoon, and a loss of 161kv line in the evening 500 miles from point A due to a failed component, if it is an entity of significant size. Propose some type of time constraint. Add time constraint as proposed, 30 seconds, other than automatic reclosing. In the event of dense lightning occurrence, the loss of multiple transmission facilities may occur over several minutes to several hours with no significant detrimental effect to the BES, as load will most certainly be affected (lost due to breaker activity on the much more exposed Distribution system) as well. Any additional loss after 30 seconds must take into account supplemental devices with intentional relay time delays, such as shunt capacitors, reactors, or load tap changers on transformers activating as designed, arresting system decay. In addition, Generator response after this time has significant impact. 4) Pg.20 /Event: Complete or partial loss of monitoring capability. ATC recommends that the term “partial” be deleted from the event description. ATC recommends that the term “partial” be deleted for the Entity with Reporting Responsibility and changed to read: Each RC, BA, and TOP that experiences the complete loss of monitoring capability.
No
ATC believes that the NERC Rules of Procedure Section 807 already addresses the dissemination of Disturbance data, as does Appendix 8 Phase 1 with the activation of NERC’s crisis communication plan, and the ESISAC Concept of Operations. The addition of proposed Section 812 is not necessary.

The Reliability Coordinator, through the use of the RCIS, would disseminate reliability notifications if it is in turn notified per R1.2. (As stated in the in the Clean copy of EOP-004-2)
Individual
Brenda Frazer
Edison Mission Marketing & Trading, Inc.
Yes
Yes
Yes
No
Group
PPL Corporation NERC Registered Affiliates
Stephen J. Berger
Yes
No
1.) PPL Generation thanks the SDT for the changes made in this latest proposal. We feel our previous comments were addressed. PPL Generation offers the following additional comments. Regarding the event 'Transmission Loss': For your consideration, please consider adding a footnote to the event 'Transmission Loss' such that weather events do not need to be reported. Also please consider including operation contrary to design in the language and not just in the example. E.g. consistent with the NERC Event Analysis table, the threshold would be, 'Unintentional loss, contrary to design, of three or more BES Transmission Facilities.' 2.) PPL Generation proposes the following changes in Attachment 1 to the first entry in the "Threshold for Reporting" column to make it clear that independent GO/GOPs are required to act only within their sphere of operation and based on the information that is available to the GO/GOPs: Damage or destruction of a Facility that: Affects an IROL (per FAC-014, not applicable to GOs and GOPs) OR Results in the need for actions to avoid an Adverse Reliability Impact (not applicable to GOs and GOPs) OR Results from actual or suspected intentional human action (applicable to all).
Yes
We appreciate the inclusion of the Process Flowchart on Page 9 of the draft standard. We submit for your consideration, removing the line from the NO decision box to the 'Report Event to ERO, Reliability Coordinator' box. It seems if the event does not need reporting per the decision box, this line is not needed. The decision box on 'Report to Law Enforcement ?' does not have a Yes or No. Perhaps, this decision box is misplaced, or is it intended to occur always and not have a different path with different actions? Ie. should it be a process box? Thank you for your work on this standard.
Individual
Kenneth A Goldsmith
Alliant Energy
No
In the first Event for twenty four hour reporting, the last item in "Threshold for Reporting" should be revised to "Results from actual or suspected intentional malicious human action." An employee may be performing maintenance and make a mistake, which could impact the BES. In the second Event for twenty four hour reporting the event should be revised to "Any physical attack that could impact the operability of a Facility." Alliant Energy believes this is clearer and easier to measure.
Section 5 of the standard (Background) should be moved to the Guideline and Technical Basis

document. A background that long does not belong in the standard piece as it detracts from the intent of the standard itself.
Individual
Eric Salsbury
Consumers Energy
No
The term "Facility" seems to be much more broad and even more vague than the use of BES equipment. We recommend reverting back to use of BES equipment.
Group
Hydro One
Sasa Maljukan
No
In the Requirement R3, we suggest adding the following wording from Measure M3 to the end of R3 after the wording “in Part 1.2.”: The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. This language must be in the Requirement to be considered during an audit. Measures are not auditable. Statement “... not including notification to the ERO...” as it stands now is confusing. We suggest that this statement is either reworded (and explained in the Rational for this requirement) or outright removed for clarity purposes In the requirement R4, we suggest replacing the words “an annual review” with the words “a periodic review.” Add the following to R4: The frequency of such periodic reviews shall be specified in the Operating Plan and the time between periodic reviews shall not exceed five (5) years. This does not preclude an annual review in an Entity’s operating plan. The Entity will then be audited to its plan. If the industry approves a five (5) year periodic review ‘cap,’ and FERC disagrees, then FERC will have to issue a directive, state it reasons and provide justification for an annual review that is not arbitrary or capricious. Adding the one year “test” requirement adds to the administrative tracking burden and adds no reliability value. The table in the standard is clear regarding what events need to be reported. An auditor may want to see a test for "each" of the applicable events listed in EOP-004 Attachment 1.If the requirement for "an" annual test remains in the standard in R3, then it should be made clear that a test is not required for "each" of the applicable events listed in Attachment 1 (reference to R1.2.)
No
In the Attachment 1, language identical to event descriptions in the NERC Event Analysis Process and FERC OE-417 should be used. Creating a third set of event descriptions is not helpful to system operators. Recommend aligning the Attachment 1 wording with that contained in Attachment 2, DOE Form OE-417 and the EAP whenever possible. The proposed “events” are subjective and will lead to confusion and questions as to what has to be reported. - Event: A reportable Cyber Security Incident. All reportable Cyber Security Incidents may not require “One Hour Reporting.” A “one-size fits all” approach may not be appropriate for the reporting of all Cyber Security Incidents. The NERC “Security Guideline for the Electricity Sector: Threat and Incident Reporting” document provides time-frames for Cyber Security Incident Reporting. For example, a Cyber Security Compromise is recommended to be reported within one hour of detection, however, Information Theft or Loss is recommended to be reported within 48 hours. Recommend listing the Event as “A confirmed reportable Cyber Security Incident. The existing NERC “Security Guideline for the Electricity Sector: Threat and Incident Reporting” document uses reporting time-frames based on “detection” and “discovery.” Recommend using the word confirmed because of the investigation time that may be required from the point of initial “detection” or “discovery” to the point of confirmation, when the compliance “time-clock” would start for the reporting requirement in EOP-004-2. - Event: Damage or destruction of a Facility Threshold for Reporting: revise language on third item to read: “Results from actual or suspected intentional human action, excluding unintentional human errors”. - Event: Any physical threat that could impact the operability of a Facility This Event category should be deleted. The word “could” is hypothetical and therefore unverifiable and un-auditable. The word “impact” is undefined. Please delete this reporting requirement, or provide a list of hypothetical “could impact” events, as well as a

specific definition and method for determining a specific physical impact threshold for “could impact” events other than “any.” - Event: BES Emergency requiring public appeal for load reduction. Replace wording in the Event column with language from #8 on the OE-417 Reporting Form to eliminate reporting confusion. Following this sentence add, “This shall exclude other public appeals, e.g., made for weather, air quality and power market-related conditions, which are not made in response to a specific BES event.” - Event: Complete or partial loss of monitoring capability Event wording: Delete the words “or partial” to conform the wording to the NERC Event Analysis Process. - Event: Transmission Loss Revise to BES Transmission Loss - Event: Generation Loss Revise to BES Generation Loss
No
The proposed new section does not contain specifics of the proposed system nor the interfacing outside of the system to support the report collecting.
The proposed standard is not consistent with NERC’s new Risk Based Compliance Monitoring. - The performance based action to “implement its event reporting Operating Plan” on defined events, as required in R2, could be considered a valid requirement. However, the concern is that this requirement could be superseded by the NERC Events Analysis Process and existing OE-417 Reporting. - The requirements laid out in R1, R3 and R4 are specific controls to ensure that the proposed requirement to report (R2) is carried out. However, controls should not be part of a compliance requirement. The only requirement proposed in this standard that is not a control is R2. NERC does not need to duplicate the enforcement of reporting already imposed by the DOE. DOE-417 is a well-established process that has regulatory obligations. NERC enforcement of reporting is redundant. NERC has the ability to request copies of these reports without making them part of the Reliability Rules. Form EOP-004, Attachment 2: Event Reporting Form: - Delete from the Task column the words “or partial”. - Delete from the Task column the words “physical threat that could impact the operability of a Facility”. VSL’s may have to be revised to reflect revised wording. The standard as proposed is not supportive of Gerry Cauley’s performance based standard initiative
Group
CenterPoint Energy
John Brockhan
No
CenterPoint Energy recommends that “and implement” be added after “Each Responsible Entity shall have” in Requirement R1. After such revision, Requirement R2 will not be needed as noted in previous comments submitted by the Company. CenterPoint Energy also believes that Requirement R3 is not needed as an annual review encompassing the elements of the test described in the draft is sufficient.
No
CenterPoint Energy appreciates the revisions made to Attachment 1 based on stakeholder feedback; however, the Company continues to have concerns regarding certain events and thresholds for reporting and offers the following recommendations. (1) CenterPoint Energy recommends the deletion of "per Requirement R1" in the “Note” under Attachment 1 as it contains a circular reference back to R1 which includes timeframes. (2) CenterPoint Energy maintains that a required 1 hour threshold for reporting of any event is unreasonable. CenterPoint Energy is confident that given dire circumstances Responsible Entities will act quickly on responding to and communication of any impending threat to the reliability of the Bulk Electric System. (3) For the event of “Damage or destruction of a Facility”, CenterPoint Energy is concerned that the use of the term “suspected” is too broad and proposes that the SDT delete "suspected" and add "that causes an Adverse Reliability Impact…" to the threshold for reporting regarding human action. (4) CenterPoint Energy believes that the event, “Any physical threat that could impact the operability of a Facility” is too broad and should be deleted. Alternatively, CenterPoint Energy recommends that the SDT delete "could” or change the event description to "A physical incident that causes an Adverse Reliability Impact". Additionally, in footnote 1, the example of a train derailment uses the phrase “could have damaged”. CenterPoint Energy is concerned that as beauty is the eye of the beholder, this phrase is open to interpretation and therefore recommends that the phrase, “causes an Adverse Reliability Impact” be incorporated into the description. (5) The Company proposes that the threshold for reporting the event, “BES Emergency requiring manual firm load shedding” is too low. It appears the SDT was attempting to align this threshold with the DOE reporting requirement. However, as the SDT stated above, there are several valid reasons why this should not be done:therefore. CenterPoint Energy recommends the threshold be revised to “Manual

firm load shedding ≥ 300 MW". (6) CenterPoint Energy also recommends a similar revision to the threshold for reporting associated with the "BES Emergency resulting in automatic firm load shedding" event. ("Firm load shedding ≥ 300 MW (via automatic under voltage or under frequency load shedding schemes, or SPS/RAS") (7) CenterPoint Energy is uncertain of the event, "Loss of firm load for ≥ 15 minutes" and its fit with BES Emergency requiring manual firm load shedding or BES Emergency resulting in automatic firm load shedding. The Company believes that this event is already covered with manual firm load shedding and automatic firm load shedding and should therefore be deleted. (8) For the event of "System separation (islanding)", CenterPoint Energy believes that 100 MW is inconsequential and proposes 300 MW instead. (9) For "Generation loss", CenterPoint Energy suggests that the SDT add "only if multiple units" to the criteria of "1,000 MW for entities in the ERCOT or Quebec Interconnection". (10) Finally, CenterPoint Energy recommends that the SDT delete the term "partial" under the "Entity with Reporting Responsibility" for "Complete or partial loss of monitoring capability". The Company proposes revising the event description to "Loss of monitoring capability for > 30 minutes that causes system analysis tools to be inoperable".

No

CenterPoint Energy does not agree with the SDT's proposed section 812. The proposal for NERC to establish a system that will "…forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary. This can include state, federal, and provincial organizations." is redundant with the draft Standard. Responsible entities are already required to report applicable events to NERC, applicable regional entities, registered entities, and appropriate governmental, law enforcement, and regulatory agencies. CenterPoint Energy believes if the SDT's intent is to require NERC to distribute these system event reports, then EOP-004-2 should be revised to require responsible entities to only report the event to NERC. As far as distribution to appropriate NERC departments, CenterPoint Energy believes that is an internal NERC matter and does not need to be included in the Rules of Procedure.

CenterPoint Energy proposes that the purpose be enhanced to reflect risk and response. For example, the purpose could read "To sustain and improve reliability of the Bulk Electric System by identifying common risks reported by Responsible Entities as a source of lessons learned." In the Background section under Law Enforcement Reporting, "the" should be added in front of "Bulk Electric System". Also under the Background section - "Present expectations of the industry under CIP-001-1a", CenterPoint Energy is not aware of any current annual requirements for CIP-001 and suggests that this section be revised to reflect that fact. CenterPoint Energy strongly believes that the Violation Severity Levels (VSL) should not be high or severe unless an Adverse Reliability Impact occurred. CenterPoint Energy is requesting that Requirement R2 be deleted and the phrase, "as a result of not implementing the plan/insufficient or untimely report, an Adverse Reliability Impact occurred" be added to the Requirement R1 VSL. Regarding the VSL for Requirement R4, the Violation Risk Factor should be "Lower" and read "the entity did not perform the annual test of the operating plan" as annual is to be defined by the entity or according to the CAN-0010.

Individual

Kirit Shah

Ameren

Yes

No

We appreciate the efforts of the DSR SDT and believe this latest Draft is greatly improved over the previous version. However, we propose the following suggestions: (1) The first Event category in Attachment 1 under 24 Hour Reporting is Applicable to GO and GOP entities. Yet the first 2 of 3 Thresholds for Reporting require data that is unobtainable for GO and GOP entities. Specifically, Events that "Affects an IROL (per FAC-014)" and "Results in the need for actions to avoid an Adverse Reliability Impact". We believe these thresholds, and the use of the NERC Glossary term Adverse Reliability Impact, clearly show the SDT's intent to limit reporting only to Events that have a major and significant reliability impact on the BES. GO or GOP does not have access to the wide-area view of the transmission system, making them to make this determination is impossible. As a result, we do not believe GO and GOP entities should have Reporting Responsibility for these types of Events. (2) For GO and GOP entities, the third Threshold is confusing as to which facilities in the plant it would be

applicable to; because the definition of "Facility" does not provide a clear guidance in that respect. For example, would a damage to ID fan qualify as a reportable event? (3) The second Event category in Attachment 1 under 24 Hour Reporting, "Any physical threat that could impact the operability of a Facility" is wide open to interpretation and thus impracticable to comply with. For example, a simple car accident that threatens any transmission circuit, whether it impacts the BES (as listed in the Threshold for the previous event in the table or any other measure) or not, is reportable. This list could become endless without the events having any substantial impact on the system. To continue this point, the Footnote 1 can also include, among many other examples, the following: (a) A wild fire near a generating plant, (b) Low river levels that might shut down a generating plant, (c) A crane that has partially collapsed near a generator switchyard, (d) Damage to a rail line into a coal plant, and/or (v) low gas pressure that might limit or stop operation of a natural gas generating plant. (4) The category, "Transmission Loss" is a concern also. If the meaning of Transmission Facility is included in the meaning of Facility as described in the event list, it may be acceptable; but, we still have a question how would a loss of a bus and the multiple radial element that may be connected to that bus would be treated? Also, how would a breaker failure affect this type of an event? The loss of a circuit is “intentional” (as opposed to Unintentional as listed in the threshold) for the failure of breaker, how will it be treated in counting three or more? We suggest a clarification for such types of scenarios. (5) Requirement R1.: 1.1 includes an exception from compliance with this Standard if there is a Cyber Security Incident according to CIP-008-3. However, note that the CIP-008-3 may not apply to all GO and GOP facilities. While the exception is warranted to eliminate duplicative event reporting plans, the language of this requirement is confusing as it does not clearly provides that message. (6) The second paragraph in Section C.1.1.2. Includes the phrases “…shall retain the current, document…” and “…the “date change page” from each version…” Is the “document” intended to be the Operating Plan? We do not see a defining reference in the text around this phrase; also, is a “date change page” mandatory for compliance with this Standard? We request additional clarification of wording in the Evidence Retention section of the Standard. (7) Page 19 / Event: Voltage deviation on a Facility: We believe that the term “observes” for Entity with Reporting Responsibility be changed back to “experiences” as originally written. The burden should rest with the initiating entity in consistency with other Reporting Responsibilities. In addition, for Threshold for Reporting, We believe the language should be expanded to - plus or minus 10%”of nominal voltage” for greater than or equal to 15 continuous minutes. (8) Page 20 /Event: Complete or partial loss of monitoring capability. We suggest to the SDT that the term “partial” be deleted from the event description. (9) We suggest to the SDT that the term “partial” be deleted for the Entity with Reporting Responsibility and changed to read: Each RC, BA, and TOP that experiences the complete loss of monitoring capability.
No
If the SDT keeps new Section 812 we suggest to the SDT a wording change for the second sentence, underlined: “Upon receipt of the submitted report, the system shall then forward the report to the appropriate NERC department for review. After review, the report will be forwarded to the applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary.”
Individual
Howard Rulf
We Energies
Yes
No
Submitting reports to the ERO: NERC and all of the Regional Entities are the ERO. If I send a report to any Regional Entity (and not NERC), I have sent it to the ERO. Damage or Distruction of a Facility: A DP may not have a Facility by the NERC Glossary definition. All distribution is not a Facility. Did you mean to exclude all distribution? Any Physical threat that could impact the operability of a Facility: An RC does not have Facilities by the NERC Glossary definition. An RC will not have to report this. BES Emergency... Reporting Responsibility: If meeting the Reporting Threshold was due to a directive from the RC, who is the Initiating entity? Voltage deviation on a Facility Threshold for Reporting: 10% of what voltage? Nominal, rated, scheduled, design, actual at an instant?
No

Section 812 refers to the section as a standard and as a Procedure. That is not correct. Section 812 reads to me as if NERC (the system) will be forwarding everything specified anywhere in RoP 800.
Applicability: Change Electric Reliability Organisation to NERC or delete Regional Entity. The ERO is NERC and all the Regional Entities. R1.2: The ERO is NERC and all the REs. If I report to any one on the REs (only and not to NERC), I have reported to the ERO. Change ERO to NERC. M1 refers to R1.1 and R1.2 as Parts. It would be clearer to refer to them as requirements or sub-requirements. M2: Add a comma after "that the event was reported" and "supplemented by operator logs". It will be easier to read. R3: This should be clarified to state that no reporting will be done for the annual test, not just exclude the ERO. M4: An annual review will not be time stamped.
Group
SMUD & BANC
Joe Tarantino
We feel issues were addressed, but still have concern with 'damage'. We certainly support that any 'destruction' of a facility that meets any of the three criteria be a reportable issue. But 'damage', if it's going to be included should have some objective definition that sets a floor. Much like the copper theft issue, we don't see the benefit of reporting plain vandalism (gun-shot insulators results from actual or suspected intentional human action) to NERC unless the 'damage' has some tangible impact on the reliability of the system or are acts of an orchestrated sabotage (i.e. removal of bolt in a transmission structure).
Individual
Brian J Murphy
NextEra Energy Inc
No
NextEra Energy, Inc. (NextEra) does not agree that annual reviews and annual tests should be mandated via Reliability Standards; instead, NextEra believes it is more appropriate to require that the Operating Plan be up-to-date and reviewed/tested as the Responsible Entity deems necessary. These enhancements provide for a robust Operating Plan, without arbitrary deadlines for a review and testing. It also provides Responsible Entities of different sizes and configurations the flexibility to efficiently and effectively integrate compliance with operations. Thus, NextEra requests that R1 be revised to read: "Each Responsible Entity shall have an up-to-date event reporting Operating Plan that is tested and reviewed as the Responsible Entity deems necessary and includes: …". Consistent with these changes NextEra also requests that R3 and R4 be deleted.
No
As stated in NextEra's past comments, we continue to be concerned that EOP-004-2 does not appropriately address actual sabotage that threatens the Bulk Electric System (BES) versus random acts that are isolated and pose no risk to the BES. Therefore, NextEra repeats a portion of its past comments below in the hope that the next revision of EOP-004-2 will more adequately address NextEra's concerns. Specifically, NextEra's requests that its definition of sabotage set forth below replace Attachment 1's "Damage and Destruction of Equipment" and "Any physical threat that could impact the operability of a Facility." In Order No. 693, FERC stated its interest in NERC revising CIP-001 to better define sabotage and requiring notification to the certain appropriate federal authorities, such as the Department of Homeland Security. FERC Order No. 693 at PP 461, 462, 467, 468, 471. NextEra has provided an approach that accomplishes FERC's objectives and remains within the framework of the drafting team, but also focuses the process of determining and reporting on only those sabotage acts that could affect other BES systems. Today, there are too many events that are being reported as sabotage to all parties in the Interconnection, when in reality these acts have no material affect or potential impact to other BES systems other than the one that experienced it. For example, while the drafting team notes the issue of copper theft is a localized act, there are other localized acts of sabotage that are committed by an individual, and these acts pose little, if any, impact or threat to other BES systems. Reporting sabotage that does not need to be sent to everyone does not add to the security or reliability of the BES. Relatedly, there is a need to clarify some of the current industry confusion on who should (and has the capabilities to) be reporting to a broader

audience of entities. Hence, the NextEra approach provides a clear definition of sabotage, as well as the process for determining and reporting sabotage. New Definition for Sabotage. Attempted or Actual Sabotage: an intentional act that attempts to or does destroy or damage BES equipment for the purpose of disrupting the operations of BES equipment, or the BES, and has a potential to materially threaten or impact the reliability of one or more BES systems (i.e., one act of sabotage on BES equipment is only reportable if it is determined to be part of a larger conspiracy to threaten the reliability of the Interconnection or more than one BES system).
Given that Responsible Entities are already required by other Reliability Standards to communicate threats to reliability to their Reliability Coordinator (RC), NextEra does not believe that EOP-004-2 is a Reliability Standard that promotes the reliability of the bulk power system, as envisioned by Section 215 of the Federal Power Act. Because an RC reporting requirement is already covered in other Standards, EOP-004-2 essentially is a reporting out requirement to the Regional Reliability Organization (RRO). NextEra does not agree that the reporting of events to the RROs should be subject to fines under the Reliability Standard regulatory framework. The reporting to RROs, as required by EOP-004-2, while informative and helpful for lessons learned, etc., is not necessary to address an immediate threat to reliability. In addition, NextEra does not believe it would be constructive to fine Responsible Entities for failure to report to a RRO within a mandated deadline during times when these entities are attempting to address potential sabotage on their system. NextEra would, therefore, prefer that the EOP-004-2 Standards Drafting Team be disbanded, and instead that EOP-004-2's reporting requirements be folded in to the event analysis reporting requirements. Therefore, NextEra requests that the new Section 812 be revised to include EOP-004-2 as a data request for lessons learn or for informational purposes only, and, also, for EOP-004-2 project to be disbanded.
Individual
Kathleen Goodman
ISO New England Inc
No
Due to the FERC mandate to assign VRFs/VSLs, we do not support using subrequirements and, instead, favor the use of bullets when the subrequirements are not standalone but rely on the partent requirement.
No
We unable to comment on the proposed new section as the section does not contain any description of the proposed process or the interface requirements to support the report collecting system. We reserve judgment on this proposal and our right to comment on the proposal when the proposed addition is posted.
We requests that the SDT post the following Alternative Proposal for Industry comments as required by the Standards Process to obtain Industry consensus and as permitted by FERC: An equally effective alternative is to withdraw this standard and to make the contents of the SDT's posted standard a NERC Guideline. a. This alternative is more in line with new NERC and FERC proposals b. This alternative retains the reporting format Comments 1. The FERC Order 693 directives regarding "sabotage" have already been addressed by the SDT (i.e. the concept was found outside the scope of NERC standards) 2. Current Industry actions already address the needs cited in the Order: a. Approved Reporting Processes already exists i. The Operating Committee's Event Analysis Process ii. Alert Reporting b. The Data already exists i. Reliability Coordinators Information System (which creates hundred if not thousands of "reports" per year) ii. The DOE's OE 417 Report itself provides part of the FERC discussed data 3. The proposed standard is not supportive of Gerry Cauley's performance based standard initiative or of FERC's offer to reduce procedural standards a. The proposed requirement is a process not an outcome i. The proposal is more focused on reporting and could divert the attention of reliability entities from addressing a situation to collecting data for a report b. The proposed "events" are subjective and if followed will create an unmanageable burden on NERC staff i. Reporting "damage" to facilities can be interpreted as anything from a dent in a generator to the total destruction of a transformer ii. The reporting requirements on all applicable entities will create more questions about differences between the reports of the various entities – rather than leading to conclusions about patterns among events that indicate a global threat iii.

Reporting any “physical threat” is too vague and subjective iv. Reporting “damage to a facility that affects an IROL” is subjective and can be seen to require reporting of damage on every facility in an interconnected area. v. Reporting “Partial loss of monitoring” is a data quality issue that can be anything from the loss of a single data point to the loss of an entire SCADA system vi. Testing the filling out of a Report does not make it easier to fill out the report later (moreover the reporting is already done often enough –see 2.b.i) c. The proposed requirements will create a disincentive to improving current Reporting practices (the more an entity designs into its own system the more it will be expected to do and the more likely it will be penalized for failing to comply) i. Annual reviews of the reporting practices fall into the same category, why have a detailed process to review when a simple one will suffice? 4. The proposed standard does not provide a feedback loop to either the data suppliers or to potentially impacted functional entities a. If the “wide area” data analysis indicates a threat, there is no requirement to inform the impacted entities b. As a BES reliability issue there is no performance indicators or metrics to show the value of this standard i. We recognize that specific incidents cannot be identified but if this is to be a reliability standard some information must be provided. A Guideline could be designed to address this concern. 5. The proposed standard is not consistent with NERC’s new Risk Based Compliance Monitoring. a. The performance based action to report on defined events, as required in R2, could be considered a valid requirement. However we have concerns as noted in Bullet 3 above. The requirements laid out in R1, R3 and R4 are specific controls to ensure that the proposed requirement to report (R2) is carried out. NERC is moving in the direction to assess entities’ controls, outside of the compliance enforcement arm. The industry is being informed that NERC Audit staff will conduct compliance audits based on the controls that the entity has implemented to ensure compliance. We are interested in supporting this effort and making it successful. However, if this is the direction NERC is moving, we should not be making controls part of a compliance requirement. The only requirement proposed in this standard that is not a control is R2. 6. For FERC-jurisdictional entities, NERC does not need to duplicate the enforcement of reporting already imposed by the DOE. DOE-417 is a well established process that has regulatory obligations. NERC enforcement of reporting would be redundant. NERC has the ability to request copies of these reports without making them part of the Reliability Rules.
Group
ISO/RTO Standards Review Committee
Albert DiCaprio
No
The SRC offers comments regarding the posted draft requirements; however, by so doing, the SRC does not indicate support of the proposed requirements. Following these comments, please see the latter part of the SRC’s response to Question 4 below for an SRC proposed alternative approach: Regarding the proposed posted requirements, without indicating support of those requirements, the SRC concurs with the changes as they provide better streamlining of the four key requirements, with enhanced clarity. However, we are unclear on the intent of Requirement R3, in particular the phrase “not including notification to the Electric Reliability Organization” which begs the question on whether or not the test requires notifying all the other entities as if it were a real event. This may create confusion in ensuring compliance and during audits. Suggest the SDT to review and modify this requirement as appropriate. Regarding part 1.2, the SRC requests that the text be terminated after the word “type” and before “i.e.” As written, the requirement does not allow for the entity to add/remove others as necessary. Please consider combining R3 and R4. These can be accomplished at the same time. The process should be evaluated to determine effectiveness when an exercise or test is conducted. The SDT is asked to review the proposal and to address the issue of requirements vs. bullets vs. sub-requirements. It is suggested that each requirement be listed independently, and that each sub-step be bulleted.
No
The SRC response to this question does not indicate support of the proposed requirement. Please see the latter part of the SRC’s response to Question 4 below for an SRC proposed alternative approach:
No
The SRC offers comments regarding the posted draft requirements; however, by so doing, the SRC does not indicate support of the proposed requirements. Following these comments, please see the latter part of the SRC’s response to Question 4 below for an SRC proposed alternative approach: The SRC is unable to comment on the proposed new section as the section does not contain any

description of the proposed process or the interface requirements to support the report collecting system. We reserve judgment on this proposal and our right to comment on the proposal when the proposed addition is posted.

The SRC offers some other comments regarding the posted draft requirements; however, by so doing, the SRC does not indicate support of the proposed requirements. Following these comments, please see below for an SRC proposed alternative approach: The SRC does not agree with the MEDIUM VRF assigned to Requirement R4. R4 is a requirement to conduct an annual review of the Event Reporting Operating Plan mandated in Requirement R1. R1 however is assigned a VRF of LOWER. We are unable to rationalize why a subsequent review of a plan should have a higher reliability risk impact than the development of the plan itself. Hypothetically, if an entity doesn't develop a plan to begin with, then it will be assigned a LOWER VRF, and the entity will have no plan to review annually and hence it will not be deemed non-compliant with requirement R4. The entity can avoid being assessed violating a requirement with a MEDIUM VRF by not having the plan to begin with, for which the entity will be assessed violating a requirement with a LOWER VRF. We suggest changing the R4 VRF to LOWER. ********** The SRC requests that the SDT post the following Alternative Proposal for Industry comments as required by the Standards Process to obtain Industry consensus and as permitted by FERC: An equally effective alternative is to withdraw this standard and to make the contents of the SDT's posted standard a NERC Guideline. a. This alternative is more in line with new NERC and FERC proposals b. This alternative retains the reporting format Comments 1. The FERC Order 693 directives regarding "sabotage" have already been addressed by the SDT (i.e. the concept was found outside the scope of NERC standards) 2. Current Industry actions already address the needs cited in the Order: a. Approved Reporting Processes already exists i. The Operating Committee's Event Analysis Process ii. Alert Reporting b. The Data already exists i. Reliability Coordinators Information System (which creates hundred if not thousands of "reports" per year) ii. The DOE's OE 417 Report itself provides part of the FERC discussed data 3. The proposed standard is not supportive of Gerry Cauley's performance based standard initiative or of FERC's offer to reduce procedural standards a. The proposed requirement is a process not an outcome i. The proposal is more focused on reporting and could divert the attention of reliability entities from addressing a situation to collecting data for a report b. The proposed "events" are subjective and if followed will create an unmanageable burden on NERC staff i. Reporting "damage" to facilities can be interpreted as anything from a dent in a generator to the total destruction of a transformer ii. The reporting requirements on all applicable entities will create more questions about differences between the reports of the various entities – rather than leading to conclusions about patterns among events that indicate a global threat iii. Reporting any "physical threat" is too vague and subjective iv. Reporting "damage to a facility that affects an IROL" is subjective and can be seen to require reporting of damage on every facility in an interconnected area. v. Reporting "Partial loss of monitoring" is a data quality issue that can be anything from the loss of a single data point to the loss of an entire SCADA system vi. Testing the filling out of a Report does not make it easier to fill out the report later (moreover the reporting is already done often enough –see 2.b.i) c. The proposed requirements will create a disincentive to improving current Reporting practices (the more an entity designs into its own system the more it will be expected to do and the more likely it will be penalized for failing to comply) i. Annual reviews of the reporting practices fall into the same category, why have a detailed process to review when a simple one will suffice? 4. The proposed standard does not provide a feedback loop to either the data suppliers or to potentially impacted functional entities a. If the "wide area" data analysis indicates a threat, there is no requirement to inform the impacted entities b. As a BES reliability issue there is no performance indicators or metrics to show the value of this standard i. The SRC recognizes that specific incidents cannot be identified but if this is to be a reliability standard some information must be provided. A Guideline could be designed to address this concern. 5. The proposed standard is not consistent with NERC's new Risk Based Compliance Monitoring. a. The performance based action to report on defined events, as required in R2, could be considered a valid requirement. However we have concerns as noted in Bullet 3 above. The requirements laid out in R1, R3 and R4 are specific controls to ensure that the proposed requirement to report (R2) is carried out. NERC is moving in the direction to assess entities' controls, outside of the compliance enforcement arm. The industry is being informed that NERC Audit staff will conduct compliance audits based on the controls that the entity has implemented to ensure compliance. The SRC is interested in supporting this effort and making it successful. However, if this is the direction NERC is moving, we should not be making controls part of a compliance requirement. The only requirement proposed in this standard that is not a control is R2. 6. For FERC-jurisdictional

entities, NERC does not need to duplicate the enforcement of reporting already imposed by the DOE. DOE-417 is a well established process that has regulatory obligations. NERC enforcement of reporting would be redundant. NERC has the ability to request copies of these reports without making them part of the Reliability Rules.
Individual
Mark B Thompson
Alberta Electric System Operator
The Alberta Electric System Operator will need to modify parts of this standard to fit the provincial model and current legislation when it develops the Alberta Reliability Standard.
Individual
Maggy Powell
Exelon Corporation and its affiliates
No
It's not clear that R3 and R4 need to be separated. Consider revising R3 to read: "Through use or testing, verify the operability of the plan on an annual basis" and dropping R4.
Yes
No
While we don't have any immediate objection to revising the Rules of Procedures (ROP) to allow for report collecting under Section 800 relative to the EOP-004 standard, the proposed language is unclear and confusing. Please consider the following revision: "812. NERC Reporting Clearinghouse NERC will establish a system to collect reporting forms as required for Section 800 or per FERC approved standards from any Registered Entities. NERC shall distribute the reports to the appropriate governmental, law enforcement, regulatory agencies as required per Section 800 or the applicable standard." Further, NERC should post ROP revisions along with a discussion justifying the revision for industry comment specific to the ROP. There may be significant implications to this revision beyond the efforts relative to EOP-004.
Thanks to the SDT. Significant progress was made in revising the proposed standard language. We appreciate the effort and have only a few remaining requests: • We understand that CIP-008 dictates the 1-hour reporting obligation for Cyber Security Incidents and this iteration of EOP-004 delineates the CIP-008 requirements. Please confirm that per the exemption language in the CIP standards (as consistent with the March 10, 2011 FERC Order (docket # RM06-22-014) nuclear generating units are not subject to this reporting requirement. • EOP-004 still lists "Generation Loss" as a 24 hour reporting criteria without any time threshold guidance for the generation loss. Exelon previously commented to the SDT (without the comment being addressed) that Generation Loss should provide some type of time threshold. If the 2000 MW is from a combination of units in a single location, what is the time threshold for the combined unit loss? In considering clarification language, the SDT should review the BAL standards on the disturbance recovery period for appropriate timing for closeness of trips. • The "physical threat that could impact" requirement remains vague and it's not clear the relevance of such information to NERC or the Regions. If a train derailment occurred near a generation facility (as stated in the footnote), are we to expect that NERC is going to send out a lesson learned with suggested corrective actions to protect generators from that occurring? The value in that event reporting criteria seems low. The requirement should be removed. • The event concerning voltage deviation of +/- 10% does not specify which type of voltage. In response to this comment in the previous comment period, the SDT indicated that the entity could determine the type of voltage. It would be clearer to specify in the standard and avoid future interpretation at the audit level. • As requested previously, for nuclear facilities, EOP-004 reporting should be coordinated with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security or cyber event. Please contact the NRC about this project to ensure that required communication and reporting in response to a radiological sabotage event (as defined by the NRC) or any incident that has impacted or has the

potential to impact the BES does not create duplicate reporting, conflicting reporting thresholds or confusion on the part of the nuclear generator operator. Each nuclear generating site licensee must have an NRC approved Security Plan that outlines applicable notifications to the FBI. Depending on the severity of the security event, the nuclear licensee may initiate the Emergency Plan (E-Plan). Exelon again asks that the proposed reporting process and flow chart be coordinated with the NRC to ensure it does not conflict with existing expected NRC requirements and protocol associated with site specific Emergency and Security Plans. In the alternative, the EOP-004 language should include acceptance of NRC required reporting to meet the EOP-004 requirements. • The proposed standard notes that the text boxes will be moved to the Guideline and Technical Basis Section which we support. However, it's not clear whether all the information in the background section will remain part of the standard. If this section is to remain as proposed concerted revision is needed to ensure that the discussion language matches the requirement language. At present, it does not. For instance, the flow chart on page 9 indicates when to report to law enforcement while the requirements merely state that communications to law enforcement be addressed within the operating plan. • Exelon voted negative vote on this ballot due to the need for further clarification and reconciliation between NERC EOP-004 and the NRC.
Individual
Keith Morisette
Tacoma Power
Yes
Tacoma Power agrees with the requirement but would suggest removing all instances the word "Operating" from the Standard. The requirements should read, " Each Responsible Entity shall have an "Event Reporting Plan…". The term Operating in this context is confusing as there are many other "Operating Plans" for other defined emergencies. This standard is about "Reporting" and should be confined to that.
Yes
Tacoma Power supports the revisions. It appears that all agencies and entities are willing to support the use of the DOE Form OE-417 as the initial notification form (although EOP-004 does include their own reporting form as an attachment to the Standard). Tacoma is already using the OE-417 and distributing it to all applicable Entities and Agencies.
No
Tacoma Power disagrees with the requirement to perform annual testing of each communication plan. We do not see any added value in performing annual testing of each communication plan. There are already other Standard requirements to performing routine testing of communications equipment and emergency communications with other agencies. The "proof of compliance" to the Standard should be in the documentation of the reports filed for any qualifying event, within the specified timelines and logs or phone records that it was communicated per each specified communication plan.
Tacoma Power disagrees with the requirement to perform annual testing of each communication plan. We do not see any added value in performing annual testing of each communication plan. There are already other Standard requirements to performing routine testing of communications equipment and emergency communications with other agencies. The "proof of compliance" to the Standard should be in the documentation of the reports filed for any qualifying event, within the specified timelines and logs or phone records that it was communicated per each specified communication plan. Tacoma Power has none at this time. Thank you for considering our comments.
Individual
Dennis Sismaet
Seattle City Light
Yes
This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
Yes
This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
No

Seattle City Light follows MEAG and believes this type of activity and process is better suited to NAESBE than it is to NERC Compliance.
1) Seattle City Light follows MEAG and questions if these administrative activities better should be sent over to NAESB? R1: There is merit in having a plan as identified in R1, but is this a need to support reliability or is it a business practice? Should it be in NAESB's domain? R2, R3 & R4: These are not appropriate for a Standard. If you don't annually review the plan, will reliability be reduced and the BES be subject to instability, separation and cascading? If DOE needs a form filled out, fill it out and send it to DOE. NERC doesn't need to pile on. Mike Moon and Jim Merlo have been stressing results and risk based, actual performance based, event analysis, lessons learned and situational awareness. EOP-004 is primarily a business preparedness topic and identifies administrative procedures that belong in the NAESB domain. 2) Seattle City Light finds that even though efforts were made to differentiate between sabotage vs. criminal damage, the difference still appears to be confusing. Sabotage clearly requires FBI notification, but criminal damage (i.e. copper theft, trespassing, equipment theft) is best handled by local law agencies. A key point on how to determine the difference is to always go with the evidence. If you have a hole in the fence and cut grounding wires, this would only require local law enforcement notification. If there is a deliberate attack on a utility's BES infrastructure for intent of sabotage and or terrorism--this is a FBI notification event. One area where a potential for confusion arises is with the term "intentional human action" in defining damage. Shooting insulators on a rural transmission tower is not generally sabotage, but removing bolts from the tower may well be. Seattle understands the difficulty in differentiating these two cases, for example, and supports the proposed Standard, but would encourage additional clarification in this one area.
Individual
Scott Miller
MEAG Power
Yes
This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
Yes
This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
No
This type of activity and process is better suited to NAESBE than it is to NERC Compliance.
Should these administrative activities be sent over to NAESB? R1: There is merit in having a plan as identified in R1, but is this a need to support reliability or is it a business practice? Should it be in NAESB's domain? R2, R3 & R4: These are not appropriate for a Standard. If you don't annually review the plan, will reliability be reduced and the BES be subject to instability, separation and cascading? If DOE needs a form filled out, fill it out and send it to DOE. NERC doesn't need to pile on. Mike Moon and Jim Merlo have been stressing results and risk based, actual performance based, event analysis, lessons learned and situational awareness. EOP-004 is primarily a business preparedness topic and identifies administrative procedures that belong in the NAESB domain.
Group
FirstEnergy
Sam Ciccone
While FE voted affirmative on this draft, upon further review we request clarification be made in the next draft of the standard regarding the applicability of the Nuclear Generator Operator. Per FE's previous comments, nuclear generator operators already have specific regulatory requirements to notify the NRC for certain notifications to other governmental agencies in accordance with 10 CFR 50.72(b)(s)(xi). We had asked that the DSR SDT contact the NRC about this project to ensure that existing communication and reporting that a licensee is required to perform in response to a radiological sabotage event (as defined by the NRC) or any incident that has impacted or has the

potential to impact the BES does not create either duplicate reporting, conflicting reporting thresholds or confusion on the part of the nuclear generator operator. In addition, EOP-004 must acknowledge that there may be NRC reporting forms that have the equivalent information contained in their Attachment 2. For what the NRC considers a Reportable Event, Nuclear plants are required to fill out NRC form 361 and/or form 366. We do not agree with the drafting team's response to ours and Exelon's comments that "The NRC does not fall under the jurisdiction of NERC and so therefore it is not within scope of this project." While the statement is correct, we believe that requirements should not conflict with or duplicate other regulatory requirements. We remain concerned that the standard with regard to Nuclear GOP applicability causes duplicative regulatory reporting with existing reporting requirements of the NRC. Therefore, we ask: 1. That NERC and the drafting team please investigate these issues further and revise the standard to clarify the scope for nuclear GOPs, and 2. For any reporting deemed in the scope for nuclear GOP after NERC's and the SDT's investigation per our request in #1 above, that the SDT consider the ability to utilize information from NRC reports as meeting the EOP-004-2 requirements similar to the allowance of using the DOE form as presently proposed.

Individual

Patrick Brown

Essential Power, LLC

1. As this Standard does not deal with real-time reporting or analysis, and is simply considered an after the fact reporting process, I question the need for the Standard at all. This is a process that could be handled through a change to the Rules of Procedure rather than through a Standard. Developing this process as a Reliability Standard is, in my opinion, contrary to the shift toward Reliability-Based Standards Development. 2. I do not believe that establishing a reporting requirement improves the reliability of the BES, as stated in the purpose statement. The reporting requirement, however, would improve situational awareness. I recommend the purpose statement be changed to reflect this, and included with the process in the NERC Rules of Procedure.

Individual

Gregory Campoli

New York Independent System Operator

The NYISO is part of and supports comments submitted by NPCC Reliability Standards Committee and the IRC Strandards Review Committee. However the NYISO would also like to comment on the following items: o NERC has been proposing the future development of performance based standards, which is directly related to reliability performance. Requirement 2 of this standard is simply a reporting requirement. We believe that this does not fall into a category of a performance based standard. NERC has the ability to ask for reports on events through ROP provisions and now the new Event Analysis Process. It does not have to make it part of the compliance program. Some have indicated that need for timely reporting of cyber or sabotage events. The counter argument is that the requirement is reporting when confirmed which would delay any useful information to fend off a simultaneous threat. Also NERC has not provided any records of how previous timely (1 hour) reporting has mitigated reliability risks. o The NERC Event Analysis Process was recently approved by the NERC OC and is in place. This was the model program for reporting outside the compliance program that the industry was asking for. This should replace the need for EOP-004. o NERC has presented Risk Based Compliance Monitoring (RBCM) to the CCC, MRC, BOT and at Workshops. This involves audit teams monitoring an entities controls to ensure they have things in place to maintain compliance with reliability rules. The proposed EOP-004 has created requirements that are controls to requirement R2, which is to file a report on predefined incidents. The RBCM is being presented as the auditor will make determinations on the detail of the sampling for compliance based on the assessment of controls an entity has in place to maintain compliance. It is also noted that compliance will not be assessed against these controls. As the APS example for COM-002 is presented in the

Workshop slides, the issue is that EOP-004 R1, R3 and R4 are controls for reporting; 1) have a plan, 2) test the plan, and 3) review the plan. While R2 is the only actionable requirement. The NYISO believes that all reporting requirements have been met by OE-417 and EAP reporting requirements and that EOP-004 has served its time. At a minimum, the NYISO would suggest that EOP-004 be simplified to just R2 (reporting requirement) and the other requirements be placed at the end of the RSAW to demonstrate a culture of compliane as presented by NERC.
Individual
Don Schmit
Nebraska Public Power District
No
1. The following comments are in regard to Attachment 1: A. The row [Event] titled “Damage or destruction of Facility”: 1. In column 3 [Threshold for Reporting], the word “Affect” is vague note the following concerns: i. Does “Affect” include a broken crossarm damaged without the Facility relaying out of service. This could be considered to have an “Affect” on the IROL. ii. Would the answer be different if the line relayed out of service and auto-reclosed (short interuption) for the same damaged crossarm? We need clarity from the SDT in order to know when a report is due. 2. For clarification: Who initiates the report when the IROL interfaces spans between multiple entities? We know of an IROL that has no less that four entities that oparate Facilities within the interface. Who initiates the report of the IROL is affected? All? B. The row [Event] titled “Any physical threat that could impact the operability of a Facility”: 1. In Column 1 [Event] change the word “threat” to “attack”, this aligns with the OE-417 report. 2. In Column 3 [Threshold for Reporting], align the threshold with the OE-417 form. C. The row [Event] titled “Transmission loss”, in column 3 [Threshold for Reporting], the defined term “Transmission Facilities” is too vague. There needs to be a more description such that an entity clearly understands when an event is reportable and for what equipment. We would recommend the definition used in the Event Reporting Field Trial: An unexpected outage, contrary to design, of three or more BES elements caused by a common disturbance. Excluding successful automatic reclosing. For example: a. The loss of a combination of NERC-defined Facilities. b. The loss of an entire generation station of three or more generators (aggregate generation of 500 MW to 1,999 MW); combined cycle units are represented as one unit. D. The row [Event] titled “Complete or partial loss of monitoring”: 1. In column 1 [Event], delete the words “or partial”. This is subjective without definition, delete. 2. Also in column 1 [Event], delete the word “monitoring” and replace with Supervisory Control and Data Acquisition (SCADA). SCADA is defined term that explicitly calls out in the definition “monitoring and control” and is understood by the industry as such. 3. In column 2 [Entity with Reporting Responsibility], delete the words “or partial”; also delete the word “monitoring” and replace with SCADA. 4. In column 3 [Threshold for Reporting], reword to state “Complete loss of SCADA affecting a BES control center for >/= 30 continuous minutes”.
Individual
David Revill
GTC
Yes
No
Page 17 & 18, One Hour Reporting and Twenty-four Hour Reporting: append the introductory statements with the following: “meeting the threshold for reporting” after recognition of the event. Example: Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within twenty-four hours of recognition of the event meeting the threshold for reporting. Page 19, system separation (islanding); Clarify the intent of this threshold for reporting: Load >= 100 MW and any generation; or Load >= 100 MW and Generation >= 100 MW, or some combination of load and generation totaling 100 MW.
Yes
With the exception of the RC and company personnel, it appears this proposed section captures the

same reporting obligations and to the same entities via R1.2. Recommend adjustments to R1.2 such that reportable events are submitted to NERC, RC, and company personnel.
For R2, please clarify how an entity can demonstrate that no reportable events were experienced. GTC recommends an allowance for a letter of attestation within M2.
Individual
Scott Berry
Indiana Municipal Power Agency
No
IMPA does not believe that both R3 and R4 are necessary and they are redundant to a degree. Generally, when performing an annual review of a process or procedure, the call numbers for agencies or entities are verified to be up to date. Also, in R3, what does “test” mean. It could mean have different meanings to registered entities and to auditors which does not promote consistency among the industry. IMPA recommends going with an annual review of the process and having the telephone numbers verified that are in the event reporting Operating Plan. IMPA also believes that the local and federal law enforcement agencies would rather go with a verification of contact information over being besieged by "test" reports. The way R3 is written gives the appearance that the SDT did not want to overwhelm the ERO with all of the "test" reports from the registered entities (by excluding them from the test notification).
No
The event "any physical threat that could impact the operability of a Facility" is not measurable and can be interpreted many ways by entities or auditors. IMPA recommend incorporating language that let's this be the judgment of the registered entity only. On the "voltage deviation on a Facility", IMPA recommends that only the TOP the experiences a voltage deviation be the one responsible for reporting. For generation loss and transmission loss, IMPA believes that the amount of loss needs to be associated with a time period or event (concurrent forced outages).
no comment
For 1.2 under R1, is the SDT leaving it up to the registered entities do decide which organizations will be contacted for each event listed in attachment 1 or do all of those organization need to be contacted for each event listed in attachment 1? The requirement needs to clearly communicate this clarification and be independent of the rationale language. Auditors will go by the requirement and not the rationale for the requirement. For 1.1 under R1, does each event need its own process of recognition or can one process be used to cover all the applicable events? The requirement needs to clearly communicate this clarification and be independent of the rationale language. Auditors will go by the requirement and not the rationale for the requirement. For 1.2 under R1, company personnel is used as an example but in the rationale for R1, the third line uses operating personnel. IMPA recommends changing the example in 1.2 to operating personnel which is used in the current version of CIP-001.
Individual
Christine Hasha
ERCOT
No
ERCOT has joined the IRC comments on this project and offers these additional comments. ERCOT requests that the measure be updated to say “acceptable evidence may include”. As written, the measure reads that there is only one way to comply with the requirement. The Standards should note "what" an entity is required to do and not prescribe the "how".
Yes
No
ERCOT has joined the IRC comments on this project.
ERCOT has joined the IRC comments on this project and offers these additional comments. ERCOT supports the alternative approach submitted by the IRC. ERCOT requests that time horizons be added for each of the requirements as have been with other recent Reliability Standards projects. With regards to Attachment 1, ERCOT requests the following changes: • Modify “Generation loss” from “≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection” to “≥ 1,100 MW for entities in the

ERCOT Interconnection" and "≥ 1,000 MW for entities in the Quebec Interconnection". This is consistent with the DCS threshold and eliminates possible operator confusion since DCSs event are reported in the ERCOT interconnection at 80% of single largest contingency which equates to 1100 MW. • Modify "Transmission loss" from "Unintentional loss of three or more Transmission Facilities (excluding successful automatic reclosing)" to "Inconsequential loss of three or more Transmission Facilities not part of a single rated transmission path (excluding successful automatic reclosing)." If a single line is comprised of 3 or more sections, this should not be part of what is reported here as it is intended to be when you have a single event trip of 3 or more transmission facilities that is not part of its intended design. • ERCOT requests review of footnote 1. The footnote does not seem appropriate in including an example of a control center as the definition of a BES facility does not include control centers.
Individual
Molly Devine
Idaho Power Co.
Yes
But this is going to require that we create a new Operating Plan with test procedures and revision history.
No
I think that the category "Damage or destruction of a Facility" is too ambiguous, and the Threshold for Reporting creteria does not help to clarify the question. Any loss of a facility may result in the need for actions to get to the new operating point, would this be a reportable disturbance?
No
No opinion
No
Individual
Rebecca Moore Darrah
MISO
Yes
No
No
MISO agrees with and adopts the Comments of the IRC on this issue.
Individual
Nathan Mitchell
American Public Power Association
Yes
APPA appreciates the SDT making these requirements clearer as requested in our comments on the previous draft standard.
No
APPA in our comments on the previous draft of EOP-004-2 requested relief for small entities from this reporting/documentation standard. APPA suggested setting a 300 MW threshold for some of the criteria in Attachment 1. This suggestion was not accepted by the SDT. However, the SDT is still directed by FERC to "consider whether separate, less burdensome requirements for smaller entities may be appropriate. Therefore, APPA requests that the SDT provide relief to small entities by providing separate requirements for small entities by requiring reporting only when one of the four criteria in DOE-OE-417 are met: 1. Actual physical attack, 2. Actual cyber attack, 3. Complete operational failure, or 4. Electrical System Separation. APPA recommends this information should be reported to the small entity's BA as allowed in the DOE-OE-417 joint filling process.
Yes

The SDT needs to provide some relief for the small entities in regards to the VSL in the compliance section. APPA believes there should be no High or Severe VSLs for this standard. This is a reporting/documentation standard and does not affect BES reliability at all. It is APPA's opinion that this standard should be removed from the mandatory and enforceable NERC Reliability Standards and turned over to a working group within the NERC technical committees. Timely reporting of this outage data is already mandatory under Section 13(b) of the Federal Energy Administration Act of 1974. There are already civil and criminal penalties for violation of that Act. This standard is a duplicative mandatory reporting requirement with multiple monetary penalties for US registered entities. If this standard is approved, NERC must address this duplication in their filing with FERC. This duplicative reporting and the differences in requirements between DOE-OE-417 and NERC EOP-004-2 require an analysis by FERC of the small entity impact as required by the Regulatory Flexibility of Act of 1980

Group

ACES Power Marketing Standards Collaborators

Jason Marshall

No

(1) We agree with removing Part 1.4 and we agree with a requirement to periodically review the event reporting Operating Plan. However we are not convinced the review of the Operating Plan needs to be conducted annually. The event reporting Operating Plan likely will not change frequently so a biannual review seems more appropriate. (2) We also do not believe that Requirement R3 is needed at all. Requirement R3 compels the responsible entity to test their Operating Plan annually. We do not see how testing an Operating Plan that is largely administrative in nature contributes to reliability. Given that the drafting team is obligated to address the FERC directive regarding periodic testing, we suggest the Operating Plan should be tested biannually. This would still meet the FERC directive requiring periodic testing.

No

The drafting team made a number of positive changes to Attachment 1. However, there are a few changes that have introduced new issues and there are a number of existing issues that have yet to be fully addressed. One of the existing issues is that the reporting requirements will result in duplicate reporting. Considering that one of the stated purposes is to eliminate redundancy, we do not see how the scope of the SAR can be considered to be met until all duplicate reporting is eliminated. More specifics on our concerns are provided in the following discussion. (1) In the "Damage or destruction of a Facility" event, the statement "Affects an IROL (per FAC-014)" in the "Threshold for Reporting" is ambiguous. What does it mean? If the loss of a Facility will have a 1 MW flow change on the Facilities to which the IROL applies, is this considered to have affected the IROL? We suggest a more direct statement that damage or destruction occurred on a Facility to which the IROL applies or to one of the Facilities that comprise an IROL contingency as identified in FAC-014-2 R5.1.3. Otherwise, there will continue to be ambiguity over what constitutes "affects". (2) In the "Damage or destruction of a Facility" event, the threshold regarding "intentional human action" is ambiguous and suffers from the same difficulties as defining sabotage. What constitutes intentional? How do we know something was intentional without a law enforcement investigation? This is the same issue that prevented the drafting team from defining sabotage. (3) In the "Damage or destruction of a Facility" and "Any physical threat that could impact the operability of a Facility" events, Distribution Provider should be removed. Per the Function Model, the Distribution Provider does not have any Facilities (line, generator, shunt compensator, transformer). The only Distribution Provider equipment that even resembles a Facility would be capacitors (i.e. shunt compensator) but they do not qualify because they are not Bulk Electric System Elements. (4) The "Any physical threat that could impact the operability of a Facility" event requires duplicate reporting. For example, if a large generating plant experiences such a threat, who should report the event? What if loss of the plant could cause capacity and energy shortages as well as transmission limits? The end result is that the RC, BA, TOP, GO and GOP could all end up submitting a report for the same event. For a given operating area, only one report should be required from one registered entity for each event. (5) The "Any physical threat that could impact the operability of a Facility" event should not apply to a single Facility but rather multiple Facilities which if lost would impact BES reliability. As written now, a train derailment near a single 138 kV transmission line or small generator with minimal reliability impact would require reporting. (6) The "BES Emergency resulting in automatic firm load shedding" should not apply to the DP. In the existing EOP-004 standard, Distribution Provider is not included and the load shed information still gets reported. (7) The "Voltage deviation on a Facility" event needs to be clarified that the TOP only

reports voltage deviations in its Transmission Operator Area. Because TOPs may view into other Transmission Operator Areas, it could technically be required to report another TOP's voltage deviation because one of its System Operators observed the neighboring TOP's voltage deviation. (8) For the "Loss of firm load greater than 15 minutes" event, the potential for duplicate reporting needs to be eliminated. Every time a DP experiences this event, the DP, TOP and BA all appear to be required to report since the DP is within both the Balancing Authority Area and Transmission Operator Area. Only one report is necessary and should be sent. Given that the existing EOP-004 standard does not include the DP, we suggest eliminating the DP to eliminate one level of duplicate reporting. (9) For the "System separation (islanding)" event, please remove DP. As long as any island remains viable, the Distribution Provider will not even be aware that an island occurred. It is not responsible for monitoring frequency or having a wide area view. (10) For the "System separation (islanding)" event, please remove BA. Because islanding and system separation, involve Transmission Facilities automatically being removed from service, this is largely a Transmission Operator issue. This position is further supported by the approval of system restoration standard (EOP-005-2) that gives the responsibility to restore the system to the TOP. (11) For the "System separation (islanding)" event, please eliminate duplicate reporting by clarifying that the RC should submit the report when more than one TOP is involved. If only one TOP is involved, then the single TOP can submit the report or the RC could agree to do it on their behalf. Only one report is necessary. (12) For the "Generation loss" event, duplicate reporting should be eliminated. It is not necessary for both the BA and GOP to submit two separate reports with nearly identical information. Only one entity should be responsible for reporting. (13) For the "Complete loss of off-site power to a nuclear generating plant", the associated GO or GOP should be required to report rather than the TO or TOP. Maintaining power to cooling systems is ultimately the responsibility of the nuclear plant operator. At the very least, TO should be removed because it is not an operating entity and loss of off-site power is an operational issue. If the TOP remains in the reporting responsibility, it should be clarified that it is only a TOP with an agreement pursuant to NUC-001. All of this is further complicated because NUC-001 was written for a non-specific transmission entity because there was no one functional entity from which the nuclear plant operator gets it off-site power. (14) For the "Complete or partial loss of monitoring capability", partial loss needs to be further clarified. Is loss of a single RTU a partial loss of monitoring capability? For a large RC is loss of ICCP to a single small TOP, considered a partial loss? We suggest as long as the entity has the ability to monitor their system through other means that the event should not be reported. For the loss of a single RTU, if the entity has a solving state estimator that provides estimates for the area impacted, the partial threshold loss would not be considered. If the entity has another entity (i.e. perhaps the RC is still receiving data for its TOP area, the RC can monitor for the TOP) that can monitor their system as a backup, the partial loss has not been met.

No

(1) It is not clear to us what is the driving the need for the Rules of Procedure proposal. NERC is already collecting event and disturbance reports without memorializing the change in the Rules of Procedure. (2) The language potentially conflicts with other subsections in Section 800. For instance, the proposal says that the system will apply to collect report forms "for this section". This section would refer to Section 800. Section 800 covers NERC alerts and GADS. Electronic GADS (eGADS) already has been established to collect GADS data? Will this section cause NERC to have to incorporate eGADS into this report collection system? Incorporating NERC Alerts is also problematic because when reports are required as a result of a NERC alert, the report must be submitted through the NERC Alert system. (3) The statement that "a system to collect report forms as established for this section or standard" causes additional confusion regarding to which standards it applies. Does it only apply to this new EOP-004-2 or to all standards? If it applies to all standards, does this create a potential issue for CIP-008-3 R1.3 which requires reporting to the ES-ISAC and not this clearinghouse?

(1) IC, TSP, TO, GO, and DP should be all removed from the applicability of the standard. Previous versions of the standard did not apply to them and we see no reason to expand applicability to them. IC and TSP are not even mentioned in any of the "Entity with Reporting Responsibility" sections. For the sections that do not mention specific entities, IC and TSP would have no responsibility for any of the events. The TO and GO are not operating entities so the reporting should not apply to them. DP was not included in any previous versions of CIP-001 or EOP-004. Any information (such as load) that was necessary regarding DPs was always gathered by the BA or TOP and included in their reports. There is no indication that this process was not working and, therefore, it should not be changed.

Furthermore, including the DP potentially expands the standard outside of the Bulk Electric System which is contrary to recent statements that NERC Legal has made at the April 11 and 12, 2012 SC meeting. Their comments indicated the standards are written for the Bulk Electric System. What information does a DP have to report except load loss which can easily be reported by the BA or TOP? (2) Measure M2 needs to clarify an attestation is an acceptable form of evidence if there are no events. (3) The rationale box for R3 and R4 should be modified. It in essence states that updating the event reporting Operating Plan and testing it will assure that the BES remains secure. While these requirements might contribute to reliability, these two requirements collectively will not assure BES security and stability. (4) We disagree with the VSLs for Requirement R2. While the VSLs associated with late reporting for a 24-hour reporting requirement include four VSLs, the one-hour reporting requirement only includes three VSLs. There seems to be no justification for this inconsistency. Four VSLs should be written for the one-hour reporting requirement. (5) Reporting of reportable Cyber Security Incidents does not appear to be fully coordinated with version 5 of the CIP standards. For instance, EOP-004-2 R1, Part 1.2 requires a process for reporting events to external entities and CIP-008-5 Part 1.5 requires identifying external groups to which to communicate Reportable Cyber Security Incidents. Thus, it appears the Cyber Security Incident response plan in CIP-008-5 R1 and the event reporting Operating Plan in EOP-004-2 R1 will compel duplication of external reporting at least in the document of the Operating Plain and Reportable Cyber Security Incident response plan. This needs to be resolved. (6) In the effective date section of the implementation plan, the statement that the prior version of the standard remains in effect until the new version is accepted by all applicable regulatory authorities is not correct. In areas where regulatory approval is required, it will only remain in effect in the areas where the regulator has not approved it. (7) On page 6 in the background section, the statement attributing RCIS reporting to the TOP standards is not accurate. There is no requirement in the TOP standards to report events across RCIS. In fact, the only mention of RCIS in the standards occurs in EOP-002-3 and COM-001-1.1. (8) On page 6 in the background section, the first sentence of the third paragraph is not completely aligned with the purpose statement of the standard. The statement in the background section indicates that the reliability objective “is to prevent outages which could lead to Cascading by effectively reporting events”. However, the purpose states that the goal is to improve reliability. We think it would make more sense for the reliability objective to match the purpose statement more closely. (9) On page 7 in the first paragraph, “industry facility” should be changed to “Facility”.
Group
Seattle City Light
Pawel Krupa
Yes
This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
Yes
This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
No
Seattle City Light follows MEAG and believes this type of activity and process is better suited to NAESBE than it is to NERC Compliance.
1) Seattle City Light follows MEAG and questions if these administrative activities better should be sent over to NAESB? R1: There is merit in having a plan as identified in R1, but is this a need to support reliability or is it a business practice? Should it be in NAESB’s domain? R2, R3 & R4: These are not appropriate for a Standard. If you don’t annually review the plan, will reliability be reduced and the BES be subject to instability, separation and cascading? If DOE needs a form filled out, fill it out and send it to DOE. NERC doesn’t need to pile on. Mike Moon and Jim Merlo have been stressing results and risk based, actual performance based, event analysis, lessons learned and situational awareness. EOP-004 is primarily a business preparedness topic and identifies administrative procedures that belong in the NAESB domain. 2) Seattle City Light finds that even though efforts were made to differentiate between sabotage vs. criminal damage, the difference still appears to be confusing. Sabotage clearly requires FBI notification, but criminal damage (i.e. copper theft, trespassing, equipment theft) is best handled by local law agencies. A key point on how to determine the difference is to always go with the evidence. If you have a hole in the fence and cut grounding

wires, this would only require local law enforcement notification. If there is a deliberate attack on a utility's BES infrastructure for intent of sabotage and or terrorism--this is a FBI notification event. One area where a potential for confusion arises is with the term "intentional human action" in defining damage. Shooting insulators on a rural transmission tower is not generally sabotage, but removing bolts from the tower may well be. Seattle understands the difficulty in differentiating these two cases, for example, and supports the proposed Standard, but would encourage additional clarification in this one area.
Individual
Tony Kroskey
Brazos Electric Power Cooperative
No
Please see the comments submitted by ACES Power Marketing.
No
Please see the comments submitted by ACES Power Marketing.
No
Please see the comments submitted by ACES Power Marketing.
We thank the work of the SDT on this project. However, additional improvements should be made as described in the comments submitted by ACES Power Marketing.
Individual
Darryl Curtis
Oncor Electric Delivery
Yes
Yes
Yes
Oncor takes the position that the proposed objectives as prescribed in Project 2009-01 – Disturbance and Sabotage Reporting, is a "good" step forward. Currently, NERC reporting obligations related to disturbances occurs over multiple standards including CIP-001, EOP-004-1, TOP-007-0, CIP-008-3 and Event Analysis (EA). Oncor is especially pleased that the Event Analysis Working Group (EAWG) is actively working to find ways of streamlining the disturbance reporting process especially to agencies outside of NERC such as FERC, and state agencies. Oncor is in agreement that an addition to the NERC Rules of Procedure in section 800 to develop a Reporting Clearinghouse for disturbance events by the establishment of a system to collect report and then forward completed forms to various requesting agencies, is also a very positive step."
Individual
Denise Lietz
Puget Sound Energy, Inc.
Yes
This draft is a considerable improvement on the previous draft in terms of clarity and will be much easier for Responsible Entities to implement. Puget Sound Energy appreciates the drafting team's responsiveness to stakeholder's concerns and the opportunity to comment on the current draft. The drafting team should revise Requirement R2 to state that the "activation" of the Operating Plan is required only when an event occurs, instead of using the term "implement". "Implementation" could also refer to the activities such as distributing the plan to operating personnel and training operating personnel on the use of the plan. These activities are not triggered by any event and, since it is clear from the measure that this requirement is intended to apply only when there has been a reportable event, the requirement should be revised to state that as well. The drafting team should revise measure M2 to require reports to be "supplemented by operator logs or other reporting documentation" only "as necessary". In many cases, the report itself and time-stamped record of transmittal will be the only documents necessary to demonstrate compliance with requirement R2. Under Requirement R3, using an actual event as sufficient for meeting the requirement for conducting

an annual test would likely fall short of demonstrating compliance with the entire scope of the Operating Plan. R1.2 requires "a process for communicating EACH of the applicable events listed....". If the actual event is only one of many "applicable" events, is it sufficient to only exercise one process flow? If there is no actual event during the annual time-frame, do all the process flows then have to be exercised?
No
The Note at the beginning of Attachment 1 references notifying parties per Requirement R1; however, notification occurs in conjunction with Requirement R2. The term “Adverse Reliability Impact” is used in the threshold section of the event “Damage or destruction of a Facility”. At this time, there are two definitions for that term in the NERC Glossary. The FERC-approved definition for this term is “The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection.” If the drafting team instead means to use the definition that NERC approved on 8/4/2011 (as seems likely, since that definition more closely aligns with the severity level indicated by the other two threshold statements) then the definition should be included in the Implementation Plan as a prerequisite approval. In addition, would the threshold of “Results from actual or suspected intentional human action” include results from actual intentional human action which produced an accidental result, meaning, someone was intentionally doing some authorized action but unintentionally made a mistake, leading to damage of a facility? The event “Any physical threat that could impact the operability of a Facility” will require reporting for many events that have little or no significance to reliable operation of the Bulk Electric System. For example, a balloon lodged in a 115 kV transmission line is a “physical threat” that could definitely “impact the operability” of that Facility and, yet, will probably have little reliability impact. So, too, could a car-pole accident that causes a pole to lean, a leaning tree, or an unfortunately-located bird’s nest. The drafting team should develop appropriate threshold language so that reporting is required only for events that do threaten the reliability of the Bulk Electric System. With respect to the event “Unplanned control center evacuation”, the standard drafting team should include the term “complete” in the description and/or threshold statement to avoid having partial evacuations trigger the need to report.
The effective date language in the Implementation Plan is inconsistent with the effective date language in the proposed standard. In addition, the statement of effective date in the Implementation Plan is ambiguous – will EOP-004-2 be effective in accordance with the first paragraph or when it is “assigned an effective date” as stated in the second paragraph? All requirements should be assigned a Lower Violation Risk Factor. Medium risk factors require direct impact on the Bulk Electric System and the language there regarding “instability, separation, or cascading failures” is present to distinguish the Medium risk factor from the High risk factor. Since all of the requirements address after-the-fact reporting, there can be no direct impact on the Bulk Electric System. In addition, if having an Operating Plan under Requirement R1 is a Lower risk factor, then it does not make sense that reviewing that Operating Plan annually under Requirement R4 has a higher risk factor. The shift away from "the distracting element of motivation", i.e., removing "Sabotage" from the equation, runs the risk of focusing solely on what happened, how to fix it, and waiting for the next event to occur. That speaks to a reactive approach rather than a proactive one. There is a concern with the removal of the FBI from the reporting mix. Basically, the new standard will involve reporting a suspicious event or attack to local law enforcement and leaving it up to them to decide on reporting to the FBI. Depending on their evaluation, an event which is significant for a responsible entity might not rise to the priority level of the local law enforcement agency for them to report it to the FBI. While this might reduce the reporting requirements a bit, it might do so to the responsible entity’s detriment. In Attachment 2 - item 4, would it be possible for the boxes be either alpha-sorted or sorted by priority? There is a disconnect between footnote 1 on page 18 (Don't report copper theft) and the Guideline section, which suggests reporting forced intrusion attempt at a substation. Also, in the section discussing the removal of sabotage, the Guideline mentions certain types of events that should be reported to NERC, DHS, FBI, etc., while that specificity with respect to entities has been removed from the reporting requirement.
Individual
Steve Alexanderson
Central Lincoln

No
The new language of R3 and R4 provide nothing to clarify the word “annual.” We note that while a Compliance Application Notice was written on this, Central Lincoln believes that standards should be written so they do not rely on the continually changing CANs. CAN-0010 itself implies that “annual” should be defined within the standards themselves. We suggest: R3 Each Responsible Entity shall conduct a test of the communications process in R1 Part 1.2, not including notification to the Electric Reliability Organization, at least once per calendar year with no more than 15 calendar months between tests. R4 Each Responsible Entity shall conduct a review of the event reporting Operating Plan in Requirement R1. at least at least once per calendar year with no more than 15 calendar months between reviews.
No
1) We appreciate the changes made to reduce the short time reporting requirements. 2) We would like to point out that the 24 hour reporting threshold for “Damage or destruction of a Facility” resulting from intentional human action will still be non-proportional BES risk for certain events. The discovery of a gunshot 115 kV insulator will start the 24 hour clock running, no matter how busy the discoverer is performing restoration or other duties that are more important. The damage may have been done a year earlier, but upon discovery the report suddenly becomes the priority task. To hit the insulator, the shooter likely had to take aim and pull the trigger, so intent is at least suspected if not actual. And the voltage level ensures the insulator is part of a Facility. 3) We also note that the theft of in service copper is not a physical threat, it is actual damage. The reference to Footnote 1 should be relocated or copied to the cell above the one it resides in now. 4) We support the APPA comments regarding small entities.
Yes
Thank you for minimizing the number of necessary reports.
We agree with the comments provided by both PNGC and APPA.
We agree with the comments provided by both PNGC and APPA.
We agree with the comments provided by both PNGC and APPA.
Individual
Mauricio Guardado
Los Angeles Department of Water and Power
Yes
No
LADWP has the following comments: #1 - “Any physical threat that could impact the operability of a Facility” is still vague and “operability” is too low a threshold. There needs to be a potential impact to BES reliability. #2 – “Voltage Deviation on a Facility” I think the threshold definition needs to be more specific: Is it 10% from nominal? 10% from normal min/max operating tables/schedules? Another entities 10% might be different than mine. #3 – “Transmission Loss” The threshold of three facilities is still too vague. A generator and a transformer and a gen-tie are likely to have overlapping zones of protection that could routinely take out all three. The prospect of penalties would likely cause unneeded reporting.
LADWP does not have a comment on this question at this time
LADWP does not have any other comments at this time
Group
Arkansas Electric Cooperative Corporation
Philip Huff
No
AECC supports the comments submitted by ACES Power Marketing.
No
AECC supports the comments submitted by ACES Power Marketing.
No
AECC supports the comments submitted by ACES Power Marketing.

Group
Avista
Scott Kinney
Yes
Yes
In general the SDT has made significant improvements to Attachment 1. Avista does have a suggestion to further improve Attachment 1. In Attachment 1 under the 24 hour Reporting Matrix, the second event states "Any physical threat that could impact the operability of a Facility" and the Threshold for Reporting states "Threat to a Facility excluding weather related threats". This is extremely open ended. We suggest adding the following language to the Threshold for Reporting for Any Physical Threat: Threat to a facility that: Could affect an IROL (per FAC-014) OR Could result in the need for actions to avoid and Adverse Reliability Impact This new language would be consistent with the reporting threshold for a Damage event.
Group
PNGC Comment Group
Ron Sporseen
Yes
Yes
We agree with reservations. Our comments are below and we are seeking clarification of the Applicability section of the standard. We are voting "no" but if slight changes are made to the applicability section we will change our votes to "yes". NERC and FERC have expressed a willingness to address the compliance burden on smaller entities that pose minimal risk to the Bulk Electric System. The PNGC Comment Group understands the SDT's intent to categorize reportable events and achieve an Adequate Level of Reliability while also understanding the costs associated. Given the changes made by the SDT to Attachment 1, we believe you have gone a long way in alleviating the potential for needless reporting from small entities that does not support reliability. One remaining concern we have are potential reporting requirements in the Event types; "Damage or destruction of a Facility" and "Any physical threat that could impact the operability of a Facility". These two event types have the following threshold language; "Results from actual or suspected intentional human action" and "Threat to a Facility excluding weather related threats" respectively. We believe these two thresholds could lead to very small entities filing reports for events that really are not a threat to the BES or Reliability. Note: For vandalism, sabotage or suspected terrorism, even the smallest entities will file a police report and at that point local law enforcement will follow their terrorism reporting procedures if necessary, as you've rightly indicated in your "Law Enforcement Reporting" section. We believe extraneous reporting could be alleviated with a small tweak to the Applicability section for 4.1.9 to exclude the smallest Distribution Providers. As stated before, even if these very small entities are excluded from filing reports under EOP-004-2, threats to Facilities that they may have will still be reported to local law enforcement while not cluttering up the NERC/DOE reporting process for real threats to the BES. Our suggested change: 4.1.9. Distribution Provider: with peak load >= 200 MWs The PNGC Comment Group arrived at the 200 MWs threshold after reviewing Attachment 1, Event "Loss of firm load for >= 15 Minutes". We agree with the SDT's intent to exclude these small firm load losses from reporting through EOP-004-2. Another approach we could support is that taken by the Project 2008-06 SDT with respect to Distribution Provider Facilities: 4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES: • A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more • A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard • A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard •

Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started. We're not advocating this exact language but rather the approach that narrows the focus to what is truly impactful to reliability while minimizing costs and needless compliance burden. One last issue we have is with the language in Attachment 1, Event "BES Emergency resulting in automatic firm load shedding." Under "Entity with Reporting Responsibility", you state that the DP or TOP that "implements" automatic load shedding of >= 100 MWs must report (Also please review the CIP threshold of 300 MWs as this may be a more appropriate threshold). We believe rather than specifying a DP or TOP report, it would be appropriate for the UFLS Program Owner to file the report per EOP-004-2. In our situation we have DPs that own UFLS relays that are part of the TOP's program and this could lead to confusing reporting requirements. Also we don't believe that an entity can "Implement" "Automatic" load shedding but this is purely a semantic issue.
Yes
We appreciate the hard work of the SDT.
Group
Colorado Springs Utilities
Jennifer Eckels
Yes
Yes
Yes
CSU is concerned with the word 'damage'. We support any 'destruction' of a facility that meets any of the three criteria be a reportable issue, but 'damage', if it's going to be included should have some objective definition that sets a baseline.
Individual
James Tucker
Deseret Power
Yes
No
The threshold for reporting is way too low. A gun shot insulator is not an act of terrorism... vandalism yes... and a car hit pole would be reportable on a 138 kv line. these seem to be too aggressive in reporting.
Yes
Group
National Rural Electric Cooperative Association (NRECA)
Barry Lawson
No
NRECA is concerned with the drafting team's proposal to add a new Section 812 to the NERC ROP. NRECA does not see the need for the drafting team to make such a proposal as it relates to the new EOP-004 that the drafting team is working on. The requirements in the draft standard clearly require what is necessary for this Event Reporting standard. NRECA requests that the drafting team withdraw its proposed ROP Section 812 from consideration. The proposed language is unclear to the point of not being able to understand who is being required to do what. Further, the language is styled in

more of a proposal, and not in the style of what would appropriately be included in the NERC ROP. Finally, the SDT has not adequately supported the need for such a modification to the NERC ROP. Without that support, NRECA is not able to agree with the need for this addition to the ROP. Again, NRECA requests that the drafting team withdraw its proposed ROP Section 812 from consideration.
Individual
Michael Gammon
Kansas City Power & Light
No
Requirement 3 requires a test of the communications in the operating plan. A test implies a simulation of the communications part of the operating plan by actual communications being conducted pursuant to the plan. It is not appropriate to burden agencies with testing of communications under a test environment. Recommend the drafting team consider a confirmation of the contact information with various agencies as the operations plan dictates.
No
For the event, “Damage or destruction of a Facility”, the “Threshold for reporting” includes “Results from actual or suspected intentional human action”. This is too broad and could include events such as damage to equipment resulting from stealing cooper or wire which has no intentional motivation to disrupt the reliability of the bulk electric system. Reports of this type to law enforcement and governmental agencies will quickly appear as noise and begin to be treated as noise. This may result in overlooking a report that deserves attention. Recommend the drafting team consider making this threshold conditional on the judgment by the entity on the human action intended to be a potential threat to the reliability of the bulk electric system. For the event, “Any physical threat that could impact the operability of a Facility”, the same comment as above applies. The footnote states to include copper theft if the Facility operation is impacted. Again, it is recommended to make a report of this nature conditional on the judgment of the entity on the intent to be a potential threat to the reliability of the bulk electric system.
No
Rules stipulating the extent of how reported information will be treated by NERC is an important consideration, however, the proposed section 812 proposes to provide reports to other governmental agencies and regulatory bodies beyond that of NERC and FERC. NERC should be treating the event information reported to NERC as confidential and should not take it upon itself to distribute such information beyond the boundaries of the national interest at NERC and FERC.
The flowchart states, “Notification Protocol to State Agency Law Enforcement”. Please correct this to, “Notification to State, Provincial, or Local Law Enforcement”, to be consistent with the language in the background section part, “A Reporting Process Solution – EOP-004”. Evidence Retention – it is not clear what the phrase “prior 3 calendar years” represents in the third paragraph of this section regarding data retention for requirements and measures for R2, R3, R4 and M2, M3, M4 respectively. Please clarify what this means. Is that different than the meaning of “since the last audit for 3 calendar years” for R1 and M1?

Consideration of Comments

Disturbance and Sabotage Reporting – Project 2009-01

The Disturbance and Sabotage Reporting Drafting Team thanks all commenters who submitted comments on the draft standard EOP-004-2. This standard was posted for a 30-day public comment period from April 25, 2012 through May 24, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 87 sets of comments, including comments from approximately 210 different people from approximately 135 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page:

http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President of Standards and Training, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual:
http://www.nerc.com/files/Appendix_3A_Standard_Processes_Manual_Rev%201_20110825.pdf

Summary Consideration: The DSR SDT received several suggestions for improvement to the standard. As a result of these revisions, the DSR SDT is posting the standard for a second successive ballot period.

The DSR SDT has removed reporting of Cyber Security Incidents from EOP-004 and have asked the team developing CIP-008-5 to retain this reporting. With this revision, the Interchange Coordinator, Transmission Service Providers, Load-Serving Entity, Electric Reliability Organization and Regional Entity were removed as Responsible Entities.

Most of the language contained in the "Background" Section was moved to the "Guidelines and Technical Basis" Section. Minor language changes were made to the measures and the data retention section. Attachment 2 was revised to list events in the same order in which they appear in Attachment 1.

Requirement R1 was revised to include the Parts in the main body of the Requirement. The Measure and VSLs were updated accordingly.

Following review of the industry's comments, the SDT has re-examined the FERC Directive in Order 693 and has dropped both R3 and R4, as they were written and established a new Requirement R3 to have the Registered Entity "validate" the contact information in the contact list(s) they may have for the events applicable to them. This validation needs to be performed each calendar year to ensure that the list(s) have current and up-to-date contact data.

> R3. Each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1each calendar year. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

The SDT reviewed, discussed and updated Attachment 1 based on comments received for commenters, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Under the Event Column, the SDT starts to classify each type of an event by assigning an "Event" title. The DSRSDT then updated the "Entity with Reporting Responsibilities" column to simply state which entity has the responsibility to report if they experience an event. The last column, "Threshold for Reporting" is a bright line that, if reached, the entity needs to report that they experienced the applicable event per Requirement 1.

The DSR SDT proposed a revision to the NERC Rules of Procedure (Section 812). The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.

Index to Questions, Comments, and Responses

1. The DSR SDT has revised EOP-004-2 by removing Requirement 1, Part 1.4 and separating Parts 1.3 and 1.5 into new Requirements R3 and R4. Requirement R3 calls for an annual test of the communications portion of the Operating Plan and Requirement R4 requires an annual review of the Operating Plan. Do you agree with this revision? If not, please explain in the comment area below. 19
2. The DSR SDT made clarifying revisions to Attachment 1 based on stakeholder feedback. Do you agree with these revisions? If not, please explain in the comment area below. 46
3. The DSR SDT has proposed a new Section 812 to be incorporated into the NERC Rules of Procedure. Do you agree with the proposed addition? If not, please explain in the comment area below. 169
4. Do you have any other comment, not expressed in the questions above, for the DSR SDT? .... .183

The Industry Segments are:

1 — Transmission Owners

2 — RTOs, ISOs

3 — Load-serving Entities

4 — Transmission-dependent Utilities

5 — Electric Generators

6 — Electricity Brokers, Aggregators, and Marketers

7 — Large Electricity End Users

8 — Small Electricity End Users

9 — Federal, State, Provincial Regulatory or other Government Entities

10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10

Group/Individual	Commenter	Organization		Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
2.	Greg Campoli	NewYorkI Independent System Operator	NPCC	2									
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1									
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1									
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10									
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5									
7.	Kathleen Goodman	ISO - New England	NPCC	2									
8.	Michael Jones	National Grid	NPCC	1									
9.	David Kiguel	Hydro One Networks Inc.	NPCC	1									
10.	Michael Lombardi	Northeast Utilities	NPCC	1									
11.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9									
12.	Bruce Metruck	New York Power Authority	NPCC	6									
13.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5									
14.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10									
15.	Robert Pellegrini	The United Illuminating Company	NPCC	1									
16.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1									
17.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
18.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3									
19.	Michael Schiavone	National Grid	NPCC	1									
20.	Wayne Sipperly	New York Power Authority	NPCC	5									
21.	Tina Teng	Independent Electricity System Operator	NPCC	2									
22.	Donald Weaver	New Brunswick System Operator	NPCC	2									
23.	Ben Wu	Orange and Rockland Utilities	NPCC	1									
2.	Group	Kent Kujala	DECo			X	X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Barbara Holland		RFC	3, 4, 5
2.	Alexander Eizans		RFC	3, 4, 5

3.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

4.	Group	Brenda Hampton	Luminant						X				

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company, LLC		5

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Chris Higgins	Bonneville Power Administration	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	James	Burns	WECC	1
2.	John	Wylder	WECC	1
3.	Kristy	Humphrey	WECC	1

7.	Group	Jesus Sammy Alcaraz	Imperial Irrigation District (IID)	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joel Fugett	IID	WECC	1, 3, 4, 5, 6
2.	Cathy Bretz	IID	WECC	1, 3, 4, 5, 6

8.	Group	Connie Lowe	Dominion	X		X		X	X				

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

	Additional Member	Additional Organization	Region	Segment Selection
1.	Michael Crowley		SERC	1, 3, 5, 6
2.	Mike Garton		NPCC	5, 6
3.	Randi Heise		MRO	5
4.	Louis Slade		RFC	5

9.	Group	Robert Rhodes	SPP Standards Review Group		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Matt Bordelon	CLECO Power	SPP	1, 3, 5
2.	Michelle Corley	CLECO Power	SPP	1, 3, 5
3.	Gary Cox	Southwestern Power Administration	SPP	1, 5
4.	Dan Lusk	Xcel Energy	SPP	1, 3, 5, 6
5.	Stephen McGie	City of Coffeyville	SPP	NA
6.	John Payne	KEPCO	SPP	4
7.	Terri Pyle	Oklahoma Gas & Electric	SPP	1, 3, 5
8.	Sean Simpson	Board of Public Utilities, City of McPherson, KS	SPP	NA
9.	Ashley Stringer	Oklahoma Municipal Power Authority	SPP	4

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
10. Mike Swearingen	Tri-County Electric Cooperative	SPP 4										
11. Michael Veillon	CLECO Power	SPP 1, 3, 5										
12. Mark Wurm	Board of Public Utilities, City of McPherson, KS	SPP NA										
13. Jonathan Hayes	Southwest Power Pool	SPP 2										
14. Julie Lux	Westar Energy	SPP 1, 3, 5, 6										
15. Greg McAuley	Oklahoma Gas & Electric	SPP 1, 3, 5										
10. Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				

Additional Member	Additional Organization	Region	Segment Selection
1. Timothy Beyrle	City of New Smyrna Beach	FRCC	4
2. Jim Howard	Lakeland Electric	FRCC	3
3. Greg Woessner	Kissimmee Utility Authority	FRCC	3
4. Lynne Mila	City of Clewiston	FRCC	3
5. Joe Stonecipher	Beaches Energy Services	FRCC	1
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4
7. Randy Hahn	Ocala Utility Services	FRCC	3

11. Group	Brent Ingebrigtson	LG&E and KU Services	X		X		X	X				
No additional members listed.												

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
12.	Group	WILL SMITH	MRO NSRF	X	X	X	X	X	X				X

	Additional Member	Additional Organization	Region	Segment Selection
1.	MAHMOOD SAFI	OPPD	MRO	1, 3, 5, 6
2.	CHUCK LAWRENCE	ATC	MRO	1
3.	TOM WEBB	WPS	MRO	3, 4, 5, 6
4.	JODI JENSON	WAPA	MRO	1, 6
5.	KEN GOLDSMITH	ALTW	MRO	4
6.	ALICE IRELAND	XCEL	MRO	1, 3, 5, 6
7.	DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6
8.	ERIC RUSKAMP	LES	MRO	1, 3, 5, 6
9.	JOE DEPOORTER	MGE	MRO	3, 4, 5, 6
10.	SCOTT NICKELS	RPU	MRO	4
11.	TERRY HARBOUR	MEC	MRO	3, 5, 6, 1
12.	MARIE KNOX	MISO	MRO	2
13.	LEE KITTELSON	OTP	MRO	1, 3, 4, 5
14.	SCOTT BOS	MPW	MRO	1, 3, 5, 6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
15. TONY EDDLEMAN	NPPD	MRO 1, 3, 5										
16. MIKE BRYTOWSKI	GRE	MRO 1, 3, 5, 6										
17. THERESA ALLARD	MPC	MRO 1, 3, 5, 6										
13. Group	Stephen J. Berger	PPL Corporation NERC Registered Affiliates					X	X				

Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC 5
2.			WECC 5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO 6
4.			NPCC 6
5.			SERC 6
6.			SPP 6
7.			RFC 6
8.			WECC 6

14. Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X			

Additional Member	Additional Organization	Region	Segment Selection

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
1. Kevin Smith	BANC	WECC 1										
15. Group	Albert DiCaprio	ISO/RTO Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Terry Bilke	MISO	RFC	2
2.	Greg Campoli	NY ISO	NPCC	2
3.	Gary DeShazo	CAISO	WECC	2
4.	Matt Goldberg	ISO NE	NPCC	2
5.	Kathleen Goodman	ISO NE	NPCC	2
6.	Stephanie Monzon	PJM	RFC	2
7.	Steve Myers	ERCOT	ERCOT	2
8.	Bill Phillips	MSO	RFC	2
9.	Don Weaver	NBSO	NPCC	2
10.	Charles Yeung	SPP	SPP	2

16. Group	Sam Ciccone	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Bill Duge	FE	RFC	

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
2. Doug Hohlbaugh	FE	RFC										
17. Group	Jason Marshall	ACES Power Marketing Standards Collaborators						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
2.	Robert A. Thomasson	Big Rivers Electric Corporation	SERC	1
3.	Shari Heino	Brazos Electric Power Cooperative	ERCOT	1
4.	John Shaver	Arizona Electric Power Cooperative	WECC	4, 5
5.	John Shaver	Southwest Transmission Cooperative	WECC	1
6.	Michael Brytowski	Great River Energy	MRO	1, 3, 5, 6
7.	Scott Brame	North Carolina Electric Membership Corporation	SERC	1, 3, 4, 5

18. Group	Pawel Krupa	Seattle City Light	X		X	X						

	Additional Member	Additional Organization	Region	Segment Selection
1.	Pawel Krupa	Seattle City Light	WECC	1
2.	Dana Wheelock	Seattle City Light	WECC	3
3.	Hao Li	Seattle City Light	WECC	4

19. Group	Scott Kinney	Avista	X		X		X					

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

	Additional Member	Additional Organization	Region	Segment Selection
1.	Ed Groce	Avista Corp	WECC	5
2.	Bob Lafferty	Avista Corp	WECC	3

20.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3
7.	Rick Crinklaw	Lane Electric Cooperative	WECC	3
8.	Annie Terracciano	Northern Lights Inc.	WECC	3
9.	Aleka Scott	PNGC Power	WECC	4
10.	Heber Carpenter	Raft River Rural Electric Cooperative	WECC	3
11.	Steve Eldrige	Umatilla Electric Cooperative	WECC	1, 3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
12. Marc Farmer		West Oregon Electric Cooperative	WECC 4										
13. Margaret Ryan		PNGC Power	WECC 8										
14. Stuart Sloan		Consumers Power Inc.	WECC 1										
21.	Group	Jennifer Eckels	Colorado Springs Utilities	X		X		X	X				
Additional Member		Additional Organization	Region Segment Selection										
1. Lisa Rosintoski			WECC 6										
2. Charlie Morgan			WECC 3										
3. Paul Morland			WECC 1										
22.	Individual	Janet Smith, Regulatory Affairs Supervisor	Arizona Public Service Company	X		X		X	X				
23.	Individual	Antonio Grayson	Southern Company Services	X		X		X	X				
24.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
25.	Individual	Sasa Maljukan	Hydro One	X									
26.	Individual	John Brockhan	CenterPoint Energy	X									
27.	Individual	Philip Huff	Arkansas Electric Cooperative Corporation			X	X		X				
28.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
29.	Individual	Brian Evans-Mongeon	Utility Services								X		
30.	Individual	E Hahn	MWDSC	X									
31.	Individual	Scott McGough	Georgia System Operations Corporation			X	X						
32.	Individual	Don Jones	Texas Reliability Entity										X

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
34.	Individual	Dan Roethemeyer	Dynegy Inc.					X					
35.	Individual	Anthony Jablonski	ReliabilityFirst										X
36.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
37.	Individual	Michelle R. D'Antuono	Ingleside Cogeneration LP					X					
38.	Individual	Tim Soles	Occidental Power Services, Inc.			X			X				
39.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
40.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
41.	Individual	Thad Ness	American Electric Power	X		X		X	X				
42.	Individual	Ed Davis	Entergy	X		X		X	X				
43.	Individual	Jack Stamper	Clark Public Utilities	X									
44.	Individual	Tracy Richardson	Springfield Utility Board			X							
45.	Individual	Wayne Sipperly	New York Power Authority	X		X		X	X				
46.	Individual	David Thorne	Pepco Holdings Inc	X		X							
47.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				
48.	Individual	David Burke	Orange and Rockland Utilities, Inc.	X		X							
49.	Individual	Larry Raczkowski	FirstEnergy Corp	X		X	X	X	X				
50.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
51.	Individual	Michael Falvo	Independent Electricity System Operator		X								
52.	Individual	John Seelke	Public Service Enterprise Group	X		X		X	X				
53.	Individual	Terry Harbour	MidAmerican Energy	X		X		X	X				
54.	Individual	Brenda Lyn Truhe	PPL Electric Utilities	X									
55.	Individual	John Martinsen	Public Utility District No. 1 of Snohomish County	X		X	X	X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
56.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
57.	Individual	Thomas Washburn	FMPP						X				
58.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
59.	Individual	Andrew Z. Pusztai	Amercican Transmission Company, LLC	X									
60.	Individual	Brenda Frazer	Edison Mission Marketing & Trading, Inc.	X				X					
61.	Individual	Kenneth A Goldsmith	Alliant Energy				X						
62.	Individual	Eric Salsbury	Consumers Energy			X	X	X					
63.	Individual	Kirit Shah	Ameren	X		X		X	X				
64.	Individual	Howard Rulf	We Energies			X	X	X					
65.	Individual	Brian J Murphy	NextEra Energy Inc	X		X		X	X				
66.	Individual	Kathleen Goodman	ISO New England Inc		X								
67.	Individual	Mark B Thompson	Alberta Electric System Operator		X								
68.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				
69.	Individual	Keith Morisette	Tacoma Power	X		X	X	X	X				
70.	Individual	Dennis Sismaet	Seattle City Light						X				
71.	Individual	Scott Miller	MEAG Power	X		X		X					
72.	Individual	Patrick Brown	Essential Power, LLC					X					
73.	Individual	Gregory Campoli	New York Independent System Operator		X								
74.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
75.	Individual	David Revill	GTC	X									
76.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
77.	Individual	Christine Hasha	ERCOT		X								
78.	Individual	Molly Devine	Idaho Power Co.	X									
79.	Individual	Rebecca Moore Darrah	MISO		X								

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
80.	Individual	Nathan Mitchell	American Public Power Association			X							
81.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
82.	Individual	Darryl Curtis	Oncor Electric Delivery	X									
83.	Individual	Denise Lietz	Puget Sound Energy, Inc.	X		X		X					
84.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
85.	Individual	Mauricio Guardado	Los Angeles Department of Water and Power	X		X		X	X				
86.	Individual	James Tucker	Deseret Power	X									
87.	Individual	Michael Gammon	Kansas City Power & Light	X		X		X	X				

1. **The SDT has revised EOP-004-2 by removing Requirement 1, Part 1.4 and separating Parts 1.3 and 1.5 into new Requirements R3 and R4. Requirement R3 calls for an annual test of the communications portion of the Operating Plan and Requirement R4 requires an annual review of the Operating Plan. Do you agree with this revision? If not, please explain in the comment area below.**

Summary Consideration: Following review of the industry's comments, the SDT has re-examined the FERC Directive in Order 693 and has dropped both R3 and R4, as they were written and established a new Requirement R3 to have the Registered Entity "validate" the contact information in the contact list(s) they may have for the applicable events to their functional registration(s). This validation needs to be performed on a calendar year period to ensure that the list(s) have current and up-to-date contact data.

Organization	Yes or No	Question 1 Comment
Northeast Power Coordinating Council	No	Regarding Requirement R3, add the following wording from Measure M3 to the end of R3 after the wording "in Part 1.2.": The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. This language must be in the Requirement to be considered during an audit. Measures are not auditable. Regarding Requirement R4, replace the words "an annual review" with the words "a periodic review. "Add the following to R4: The frequency of such periodic reviews shall be specified in the Operating Plan and the time between periodic reviews shall not exceed five (5) years. This does not preclude an annual review in an Entity's operating plan. The Entity will then be audited to its plan. If the industry approves a five (5) year periodic review 'cap', and FERC disagrees, then FERC will have to issue a directive, state its reasons and provide justification for an annual review that is not arbitrary or capricious. Adding the one year "test" requirement adds to the administrative tracking burden and adds no reliability value.

Organization	Yes or No	Question 1 Comment
Response: The SDT thanks you for your comment. The SDT has removed R4 and revised R3 that calls for the responsible entity to validate contact information contain in the Operating Plan each calendar year as described in Requirement R1. The "Annual review" is used to ensure that the event reporting Operating Plan is up to date. If an entity experiences an event, communication evidence from the event may be used to show compliance.		
DECo	No	Should only have annual "review" requirement rather than test.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comment.		
Duke Energy	No	Under R3, we agree with testing communications internally. Just as the ERO is excluded under R3, other external entities should also be excluded. External communications should be verified under R4.
Response: The SDT thanks you for your comment. Due to industry opposition, the SDT revised Requirement R3 to remove test to "validate" contact information contained in the Operating Plan. If an entity experiences an actual event, communication evidence from the event may be used to show compliance with the validation requirement for the specific contacts used for the event.		
Dominion	No	While Dominion believes these are positive changes, we are concerned that placing actual calls to each of the "other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies" may be seen by one or more of those called as a 'nuisance call'. Given the intent is to insure validity of the contact information (phone number, email, etc), we suggest revising the standard language to support various forms of validation to include, documented send/receipt of email, documented verification of phone number (use of phone book, directory assistance, etc).
Response: The SDT thanks you for your comment. The SDT has made changes to the requirement highlighted in your comment.		

Organization	Yes or No	Question 1 Comment
SPP Standards Review Group	No	There needs to be a more granular definition of which entities should be included in the annual testing requirement in R3. To clarify what must be tested we propose the following language to replace the last sentence in M3. The annual test requirement is considered to be met if the responsible entity implements any communications process in the Operating Plan during an actual event. If no actual event was reported during the year, at least one of the communication processes in the Operating Plan must be tested to satisfy the requirement. We do not believe the time-stamping requirement in M3 and M4 contribute to the reliability of the BES. A dated review should be sufficient.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirement highlighted in your comments. The Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. If an entity experiences an actual event, communication evidence from the event may be used to show compliance with the validation requirement for the specific contacts used for the event. Time-stamping has been removed.		
Florida Municipal Power Agency	No	First, FMPA believes the standard is much improved from the last posting and we thank the SDT or their hard work. Having said that, there are still a number of issues, mostly due to ambiguity in terms, which cause us to vote Negative. R3 and R4 should be combined into a single requirement with two subparts, one for annual testing, and another to incorporate lessons learned from the annual testing into the plan (as opposed to an annual review).The word “test” is ambiguous as used in R3, e.g., does a table top drill count as a “test”? Is the intent to “test” the plan, or “test” the phone numbers, or what?
Response: The SDT thanks you for your comment. The SDT has made changes to the requirement highlighted in your comment.		
MRO NSRF	No	R3 states: Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. R1.2 states: A process for communicating each of the

Organization	Yes or No	Question 1 Comment
		applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies. With the use of "i.e." the SDT is mandating that each other entity must be contacted. The NSRF believes that the SDT meant that "e.g." should be used to provide examples. The SDT may wish to add another column to Attachment 1 to provide clarity. R3 requires and annual test that would include notification of:"other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies."Since NERC see no value in receiving these test notification we are doubtful other entities identified in R1.2 would find them of value. The real purpose of this requirement appears to be to assure operators are trained in the use of the procedure, process, or plan that assures proper notification. PER-005 already requires a systematic approach to training. It is hard to comprehend an organization not identifying this as a Critical Task, and if they failed to identify it as a Critical Task that this would not be a violation. Therefore this requirement is not required. Furthermore organizations test their response to events in accordance with CIP-008 R1.6. Therefore this requirement is covered by other standards and is not needed. The SDT may need to address this within M3, by stating "... that the annual test of the communication process of 1.2 (e.g. communication via e-mail, fax, phone, etc) was conducted". R4 states: Each Responsible Entity shall conduct an annual review of the event reporting Operating Plan in Requirement R1. We question the value of requiring an annual review. If the Standard does not change, there seems little value in requiring an annual review. This appears to be an administrative requirement with little reliability value. It would likely be identified as a requirement that that should be eliminated as part of the

Organization	Yes or No	Question 1 Comment
		request by FERC to identify strictly administrative requirements in FERC's recent order on FFTR. We suggest it be eliminated.
Response: The SDT thanks you for your comment. Requirement R3 called for test of all contact information contain. The SDT deleted Requirement R4 based on stakeholder comments and revised R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization. **The annual review requirement was maintained to meet the intent of NERC Order 693, Paragraph 466. The Commission does not specify a review period, as suggested; rather, believes that the appropriate period should be determined through the ERO's Reliability Standards.** **"The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures."**		
ISO/RTO Standards Review Committee	No	The SRC offers comments regarding the posted draft requirements; however, by so doing, the SRC does not indicate support of the proposed requirements. Following these comments, please see the latter part of the SRC's response to Question 4 below for an SRC proposed alternative approach: Regarding the proposed posted requirements, without indicating support of those requirements, the SRC concurs with the changes as they provide better streamlining of the four key requirements, with enhanced clarity. However, we are unclear on the intent of Requirement R3, in particular the phrase "not including notification to the Electric Reliability Organization" which begs the question on whether or not the test requires notifying all the other entities as if it were a real event. This may create confusion in ensuring compliance and during audits. Suggest the SDT to review and modify this requirement as appropriate. Regarding part 1.2, the SRC requests that the text be terminated after the word "type" and before "i.e." As written, the requirement does not allow for the entity to add/remove others as necessary. Please consider combining R3 and R4.

Organization	Yes or No	Question 1 Comment
		These can be accomplished at the same time. The process should be evaluated to determine effectiveness when an exercise or test is conducted. The SDT is asked to review the proposal and to address the issue of requirements vs. bullets vs. sub-requirements. It is suggested that each requirement be listed independently, and that each sub-step be bulleted.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirement highlighted in your comment.		
ACES Power Marketing Standards Collaborators	No	(1) We agree with removing Part 1.4 and we agree with a requirement to periodically review the event reporting Operating Plan. However we are not convinced the review of the Operating Plan needs to be conducted annually. The event reporting Operating Plan likely will not change frequently so a biannual review seems more appropriate. (2) We also do not believe that Requirement R3 is needed at all. Requirement R3 compels the responsible entity to test their Operating Plan annually. We do not see how testing an Operating Plan that is largely administrative in nature contributes to reliability. Given that the drafting team is obligated to address the FERC directive regarding periodic testing, we suggest the Operating Plan should be tested biannually. This would still meet the FERC directive requiring periodic testing.
Response: The SDT thanks you for your comment. The SDT deleted Requirement R4 based on stakeholder comments and revised R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.		
Southern Company Services	No	There are approximately 17 event types for which Responsible Entities must have a process for communicating such events to the appropriate entities and R3 states that "The Responsible Entity shall conduct an annual test of the communications process". It is likely that the same communications process will be used to report multiple event types, so Southern suggest that

Organization	Yes or No	Question 1 Comment
		the Responsible Entities conduct an annual test for each unique communications process. Southern suggest that this requirement be revised to state "Each Responsible Entity shall conduct an annual test of each unique communications process addressed in R1.2". o In Attachment 1, for Event: "Damage or destruction of a Facility", SDT should consider removing "Results from actual or suspected intentional human action" from the "Threshold for Reporting" column. The basis for this suggestion is as follows: o The actual threshold should be measurable, similar to the thresholds specified for other events in Attachment 1. [Note: The first two thresholds identified (i.e., "Affects and IROL" and "Results in the need for actions to avoid an Adverse Reliability Impact") are measurable and sufficiently qualify which types of Facility damage should be reported.] o The determination of human intent is too subjective. Including this as a threshold will cause many events to be reported that otherwise may not need to be reported. (e.g., Vandalism and copper theft, while addressed under physical threats, is more appropriately classified as damage. These are generally intentional human acts and would qualify for reporting under the current guidance in Attachment 1. They may be excluded from reporting by the threshold criteria regarding IROLs and Adverse Reliability Impact, if the human intent threshold is removed.) o It may be more appropriate to address human intent in the event description as follows: "Damage or destruction of a Facility, whether from natural or human causes". Let the thresholds related to BES impact dictate the reporting requirement. o In Attachment 1, for Event: "Complete or partial loss of monitoring capability", SDT should consider changing the threshold criteria to state: "Affecting a BES control center for â‰¥ 30 continuous minutes such that analysis capability (State Estimator, Contingency Analysis) is rendered

Organization	Yes or No	Question 1 Comment
		inoperable." There may be instances where the tools themselves are out of commission, but the control center personnel have sufficiently accurate models and alternate methods of performing the required analyses.

Response: The SDT thanks you for your comment. The SDT has made changes to the requirement highlighted in your initial comment.

The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Under the Event Column, the SDT starts to classify each type of an event by assigning an "Event" title. The DSR SDT then updated the "Entity with Reporting Responsibilities" column to simply state what entity has the responsibility to report if they experience an event. The last column, "Threshold for Reporting" is a bright line that, if reached, the entity needs to report that they experienced the applicable event per Requirement 1.

Damage or destruction of a Facility:

The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state;

Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency.

This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).

This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.

Organization	Yes or No	Question 1 Comment
Progress Energy	No	It should be clear that the Operating Plan can be multiple procedures. It is an unnecessary burden to have entities create a new document outlining the Operating Plan. Having to create a new Operating Plan would not improve reliability and would further burden limited resources. The annual testing required by R3 should be clarified. Do all communication paths need to be annually tested or just one path? An actual event may only utilize one communication 'leg' or 'path' and leave others untested and utilized. Entities may have a corporate level procedure that 'hand-shakes' with more localized procedures that make up the entire Operating Plan. Must all communications processes be tested to fulfill the requirement? If an entity has 'an actual event' it is not necessarily true that their Operating Plan has been exercised completely, yet this one 'actual event' would satisfy M3 as written.
Response: The SDT thanks you for your comment. Regarding your initial comment on the need to create a new document, the SDT believes that a Registered Entity with a procedure under CIP-001 will be able to utilize that document as the starting point for the Operating Plan here. The SDT feels that many of the necessary components will already exist in that document and the Registered Entity should only need to edit it accordingly for the types of Events applicable to them. The SDT has made changes to the standard highlighted in your comment.		
Hydro One	No	In the Requirement R3, we suggest adding the following wording from Measure M3 to the end of R3 after the wording "in Part 1.2.": The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. This language must be in the Requirement to be considered during an audit. Measures are not auditable. Statement "... not including notification to the ERO..." as it stands now is confusing. We suggest that this statement is either reworded (and explained in the Rational for this requirement) or outright removed for clarity purposes In the requirement R4, we suggest replacing the words "an annual

Organization	Yes or No	Question 1 Comment
		review" with the words "a periodic review." Add the following to R4: The frequency of such periodic reviews shall be specified in the Operating Plan and the time between periodic reviews shall not exceed five (5) years. This does not preclude an annual review in an Entity's operating plan. The Entity will then be audited to its plan. If the industry approves a five (5) year periodic review 'cap,' and FERC disagrees, then FERC will have to issue a directive, state it reasons and provide justification for an annual review that is not arbitrary or capricious. Adding the one year "test" requirement adds to the administrative tracking burden and adds no reliability value. The table in the standard is clear regarding what events need to be reported. An auditor may want to see a test for "each" of the applicable events listed in EOP-004 Attachment 1.If the requirement for "an" annual test remains in the standard in R3, then it should be made clear that a test is not required for "each" of the applicable events listed in Attachment 1 (reference to R1.2.)
Response: The SDT thanks you for your comment. Each Responsible Entity must report and communicate events according to its Operating Plan based on the information in EOP-004 Attachment 1. The SDT removed the Operating Plan Process from Requirement 1 and revised the measure to meet the communications of Requirement R1, "to implement an operating plan within the time frames specified in Attachment 1." Requirement R3 called for test of all contact information contained. The SDT deleted Requirement R4 based on stakeholder comments and revised R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.		
CenterPoint Energy	No	CenterPoint Energy recommends that "and implement" be added after "Each Responsible Entity shall have" in Requirement R1. After such revision, Requirement R2 will not be needed as noted in previous comments submitted by the Company.

Organization	Yes or No	Question 1 Comment
		CenterPoint Energy also believes that Requirement R3 is not needed as an annual review encompassing the elements of the test described in the draft is sufficient.
Response: The SDT thanks you for your comment. The SDT considered the consolidation of the first and second requirements. However, since the requirements have the Registered Entity perform two distinct steps, a single requirement cannot be written to achieve multiple tasks. Each task must stand on its own and be judged singly. **The annual review helps ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.**		
Arkansas Electric Cooperative Corporation	No	AECC supports the comments submitted by ACES Power Marketing.
Response: The SDT thanks you for your comment. Please review the response directed to them.		
MWDSC	No	Transmission Owners (TO) should not be included as a "Responsible Entity" for this or other requirements because the Operating Plan is usually prepared by the Transmission Operator (TOP). For TOs who are not also TOPs, there are usually delegation agreements. CIP-001 never directly applied to TOs.
Response: The SDT thanks you for your comment. The SDT disagrees with your assessment, as the TOs are physical owners of the equipment that would be affected by this standard. As Owners of the equipment, they need to be reporting on what is happening to their equipment.		
Manitoba Hydro	No	(R1.1 and 1.2) It is unclear whether or not R1.1 and R1.2 require a separate recognition and communication process for each of the event types listed in Attachment 1 or if event types can be grouped as determined appropriate by the responsible entity given that identical processes will apply for multiple types of events. Manitoba Hydro suggests that wording is revised so

Organization	Yes or No	Question 1 Comment
		that multiple event types can be addressed by a single process as deemed appropriate by the Responsible Entity. (R3) It is unclear whether or not R3 requires the testing of the communications process for each separate event type identified in Attachment 1. If so, this would be extremely onerous. Manitoba Hydro suggests that only unique communication processes (as identified by the Responsible Entity in R1.2) require an annual test and that testing should not be required for each type of event listed in Attachment 1. As well, Manitoba Hydro believes that testing the communications process alone is not as effective as also providing training to applicable personnel on the communications process. Manitoba Hydro suggests that R3 be revised to require annual training to applicable personnel on the communications process and that only 1 test per unique communications process be required annually.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comments. Each Responsible Entity must report and communicate events according to its Operating Plan based on the information in EOP-004 Attachment 1. The SDT has attempted to clarify that it is the choice of the Registered Entity on whether one, or more than one, contact list(s) is needed for the differing types applicable to them. Depending upon your needs of who you have an obligation to report, you can elect to have one or multiple lists. **Requirement R3 called for test of all contact information contained. The SDT deleted Requirement R4 based on stakeholder comments and revised R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.**		
Occidental Power Services, Inc.	No	There should be an exception for LSEs with no BES assets from having an Operating Plan and, therefore, from testing and review of such plan. These LSEs have no reporting responsibilities under Attachment 1 and, if they have nothing ever to report, why would they have to have an Operating Plan and have to test and review it? This places an undue burden on small entities

Organization	Yes or No	Question 1 Comment
		that cannot impact the BES.
Response: The SDT thanks you for your comment. LSEs, as being applicable under the Cyber Security standards, were included in the applicability of this standard. Since the SDT is proposing to keep the Cyber Security reporting requirements in CIP-008, LSEs have been removed from the applicability of this standard. This action will not negate the LSE responsibilities under that standard and your comments will need to be addressed there.		
Xcel Energy	No	1) In R1.2, We understand what the drafting team had intended here. However, we are concerned that the way this requirement is drafted, using i.e., it could easily be interpreted to mean that you must notify all of those entities listed. Instead, we are suggesting that the requirement be rewritten to require entities to define in their Operating Plan the minimum organizations/entities that would need to be notified for applicable events. We believe this would remove any ambiguity and make it clear for both the registered entity and regional staff. We recommend the requirement read something like this: 1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to applicable internal and external organizations needed for the event type, as defined in the Responsible Entity's Operating Plan. 2) We also suggest that R3 be clarified as to whether communications to all organizations must be tested or just those applicable to the test event type/scenario.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comments.		
American Electric Power	No	R3: How many different scenarios need to be tested? For example, reporting sabotage-related events might well be different than reporting reliability-related events such as those regarding loss of Transmission. While these

Organization	Yes or No	Question 1 Comment
		examples might vary a great deal, other such scenarios may be very similar in nature in terms of communication procedures. Perhaps solely testing the most complex procedure would be sufficient. AEP agrees with the changes with R3 calling for an annual test provided the requirement R2 is modified to include the measure language "The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event." M3: While we agree that "the annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event", we believe it would be preferable to include this text in R3 in addition to M3. Measures included in earlier standards (some of which are still enforced today) had little correlation to the requirement itself, and as a result, those measures were seldom referenced. M3: It would be unfair to assume that every piece of evidence required to prove compliance would be dated and time-stamped, so we recommend removing the text "dated and time-stamped" from the first sentence so that it reads "Each Responsible Entity will have records to show that the annual test of Part 1.2 was conducted." The language regarding dating and time stamps in regards to "voice recordings and operating logs or other communication" is sufficient.
Response: The SDT thanks you for your comment. Based on stakeholder comments the SDT revised R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization. The SDT agrees with the point raised on time-stamping and has removed it from the standard.		
Entergy	No	The requirement for a "time stamped record" of annual review is unreasonable and unnecessary. A dated document showing that a review was performed should be sufficient.

Organization	Yes or No	Question 1 Comment
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comment. The SDT has removed time-stamping from the standard.		
New York Power Authority	No	Please see comments submitted by NPCC Regional Standards Committee (RSC).
Response: The SDT thanks you for your comment. Please review the response to the commenter.		
Consolidated Edison Co. of NY, Inc.	No	Requirement R3: Following the sentence ending "in Part 1.2" add the following wording from the Measure to R3: The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. This language must be in the Requirement to be considered during an audit. Measures are not auditable. Requirement R4: Replace the words "an annual review" with the words "a periodic review."Following the first sentence in R4 add: The frequency of such periodic reviews shall be specified in the Operating Plan and the time between periodic reviews shall not exceed five (5) years.
Orange and Rockland Utilities, Inc.	No	Requirement R3: Following the sentence ending "in Part 1.2" add the following wording from the Measure to R3: The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event. This language must be in the Requirement to be considered during an audit. Measures are not auditable. Requirement R4: Replace the words "an annual review" with the words "a periodic review." Following the first sentence in R4 add: The frequency of such periodic reviews shall be specified in the Operating Plan and the time between periodic reviews shall not exceed five (5) years.
Response: The SDT thanks you for your comment. Based on stakeholder comments the SDT revised R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively		

Organization	Yes or No	Question 1 Comment
report events to assure situational awareness to the Electric Reliability Organization. The SDT considered various time frames for the action needed and felt that a calendar year was necessary due to the FERC Directive in Order 693 and to ensure that contact information remained useful in a timely manner.		
MidAmerican Energy	No	See the NSRF comments. The real purpose of this requirement appears to be to assure operators are trained in the use of the procedure, process, or plan that assures proper notification. PER-005 already requires a systematic approach to training. Reporting to other affected entities is a PER-005 system operator task. Therefore this requirement already covered by PER-005 and is not required. Organizations are also required to test their response to events in accordance with CIP-008 R1.6. Therefore this requirement is covered by other standards and is not needed. Inclusion of this standard would place entities in a double or possible triple jeopardy. The SDT may need to expand M3 reporting options, by stating "... that the annual test of the communication process of 1.2 (e.g. communication via e-mail, fax, phone, ect) was conducted". R4 is an administrative requirement with little reliability value and should be deleted. It would likely be identified as a requirement that that should be eliminated as part of the request by FERC to identify strictly administrative requirements in FERC's recent order on FFTR.
Response: The SDT thanks you for your comment. The SDT asks you to review the response to that commenter. The SDT disagrees with your understanding of the real purpose. Reporting of events listed in Attachment 1 is necessary for personnel beyond the operators. **The SDT deleted Requirement R4 based on stakeholder comments and revised Requirement R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.**		
Illinois Municipal Electric Agency	No	IMEA reluctantly (in recognition of the SDT's efforts and accomplishments to date) cast a Negative vote for this project primarily based on R3 because it is

Organization	Yes or No	Question 1 Comment
		attempting to fix a problem that does not exist and impacts small entity resources in particular. IMEA is not aware of seeing any information regarding a trend, or even a single occurrence for that matter, in a failure to report an event due to failure in reporting procedures. A small entity is less likely to experience a reportable event, and therefore is less likely to be able to take advantage of the provision in M3 to satisfy the annual testing through implementation of an actual event. If there is a problem that needs to be fixed, it would make much more sense to replace the language in R3 with a simple requirement for the RC, BA, IC, TSP, TOP, etc. to inform the TO, DP, LSE if there is a change in contact information for reporting an event. It is hard to believe that an RC, BA, IC, TSP, TOP, etc. is going to want to be annually handling numerous inquiries from entities regarding the accuracy of contact information. The impact of unnecessary requirements on entity resources, particularly small entities', is finally starting to get some meaningful attention at NERC and FERC. It would be a mistake to adopt another unnecessary requirement as currently specified in R3.
Response: The SDT thanks you for your comment. The SDT has revised Requirement R3 to help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.		
Amercican Transmission Company, LLC	No	ATC recommends eliminating R4 altogether. If R3, the annual test, is conducted as part of the Operating Plan, R4 is merely administrative, and does not add value to reliability.
Response: The SDT thanks you for your comment. The SDT deleted Requirement R4 based on stakeholder comments and revised Requirement R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.		
NextEra Energy Inc	No	NextEra Energy, Inc. (NextEra) does not agree that annual reviews and

Organization	Yes or No	Question 1 Comment
		annual tests should be mandated via Reliability Standards; instead, NextEra believes it is more appropriate to require that the Operating Plan be up-to-date and reviewed/tested as the Responsible Entity deems necessary. These enhancements provide for a robust Operating Plan, without arbitrary deadlines for a review and testing. It also provides Responsible Entities of different sizes and configurations the flexibility to efficiently and effectively integrate compliance with operations. Thus, NextEra requests that R1 be revised to read: "Each Responsible Entity shall have an up-to-date event reporting Operating Plan that is tested and reviewed as the Responsible Entity deems necessary and includes: ...". Consistent with these changes NextEra also requests that R3 and R4 be deleted.
Response: The SDT thanks you for your comment. While the SDT recognizes the simplicity that your comment would bring, it cannot be implemented in that manner. For auditability reasons, each task must be separate and distinct in order for the performance to be assessed. Alternatively, the SDT has re-constructed three distinct requirements that can be judged and evaluated on their own with compromising the others.		
ISO New England Inc	No	Due to the FERC mandate to assign VRFs/VSLs, we do not support using subrequirements and, instead, favor the use of bullets when the subrequirements are not standalone but rely on the partent requirement.
Response: The SDT thanks you for your comment. The SDT has revised the language and removed all subrequirements.		
Exelon Corporation and its affiliates	No	It's not clear that R3 and R4 need to be separated. Consider revising R3 to read: "Through use or testing, verify the operability of the plan on an annual basis" and dropping R4.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comment.		

Organization	Yes or No	Question 1 Comment
Indiana Municipal Power Agency	No	IMPA does not believe that both R3 and R4 are necessary and they are redundant to a degree. Generally, when performing an annual review of a process or procedure, the call numbers for agencies or entities are verified to be up to date. Also, in R3, what does “test” mean. It could mean have different meanings to registered entities and to auditors which does not promote consistency among the industry. IMPA recommends going with an annual review of the process and having the telephone numbers verified that are in the event reporting Operating Plan. IMPA also believes that the local and federal law enforcement agencies would rather go with a verification of contact information over being besieged by "test" reports. The way R3 is written gives the appearance that the SDT did not want to overwhelm the ERO with all of the "test" reports from the registered entities (by excluding them from the test notification).
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comment.		
ERCOT	No	ERCOT has joined the IRC comments on this project and offers these additional comments. ERCOT requests that the measure be updated to say “acceptable evidence may include”. As written, the measure reads that there is only one way to comply with the requirement. The Standards should note "what" an entity is required to do and not prescribe the "how".
Response: The SDT thanks you for your comment. The SDT has made changes to the standard highlighted in your comment.		
Brazos Electric Power Cooperative	No	Please see the comments submitted by ACES Power Marketing.
Response: The SDT thanks you for your comment. Please review the response to that commenter.		
Central Lincoln	No	The new language of R3 and R4 provide nothing to clarify the word “annual.” We note that while a Compliance Application Notice was written on this,

Organization	Yes or No	Question 1 Comment
		Central Lincoln believes that standards should be written so they do not rely on the continually changing CANs. CAN-0010 itself implies that "annual" should be defined within the standards themselves. We suggest: R3 Each Responsible Entity shall conduct a test of the communications process in R1 Part 1.2, not including notification to the Electric Reliability Organization, at least once per calendar year with no more than 15 calendar months between tests.R4 Each Responsible Entity shall conduct a review of the event reporting Operating Plan in Requirement R1. at least at least once per calendar year with no more than 15 calendar months between reviews.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comment.		
Kansas City Power & Light	No	Requirement 3 requires a test of the communications in the operating plan. A test implies a simulation of the communications part of the operating plan by actual communications being conducted pursuant to the plan. It is not appropriate to burden agencies with testing of communications under a test environment. Recommend the drafting team consider a confirmation of the contact information with various agencies as the operations plan dictates.
Response: The SDT thanks you for your comment. SDT has made changes to the requirements highlighted in your comment.		
Bonneville Power Administration	Yes	BPA believes that the annual testing and review as described in R3 is too cumbersome and unnecessary for entities with large footprints to inundate federal and local enforcement bodies such as the FBI for "only" testing and the documenting for auditing purposes. BPA suggests that testing be performed on a bi-annual or longer basis.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirements highlighted in your comment; however, the SDT has decided that the period will be shorter than your suggestion based upon comments received from all parties.		

Organization	Yes or No	Question 1 Comment
Seattle City Light	Yes	This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
Response: The SDT thanks you for your comment. Please review the response to Question 4.		
Utility Services	Yes	While agreeing with the change, confusion may exist with the CAN that exists for the term "Annual". Utility Services suggests that the language be changed to "Every calendar year" or something equivalent. Given everything that transpired in the discussion on the term annual, using a different phrase may be advantageous.
Response: The SDT thanks you for your comment. The SDT has made changes to the requirement highlighted in your comment.		
United Illuminating Company	Yes	R3 should be clear that the annual test of the plan does not mean each communication path for each applicable event on an annual basis.
Response: The SDT thanks you for your comment. Requirement R3 has been rewritten to address comments like yours and other industry members. While testing is no longer a part of the requirement, validating the contact information associated with each contact list for each applicable event type is.		
Ingleside Cogeneration LP	Yes	Ingleside Cogeneration LP agrees that it is appropriate to test reporting communications on an annual basis, primarily to validate that phone numbers, email ids, and contact information is current. We appreciate the project team's elimination of the terms "exercise" and "drill", which we believe connotates a formalized planning and assessment process. An annual review of the Operating Plan implies a confirmation that linkages to sub-processes remain intact and that new learnings are captured. We also agree that it is appropriate only to require an updated Revision Level Control chart entry as evidence of compliance - it is very likely that no updates are required after the review is complete. In our view, both of these requirements are sufficient to assure an effective assessment of all facets of

Organization	Yes or No	Question 1 Comment
		the Operating Plan. As such, we fully agree with the project team's decision to delete the requirement to update the plan within 90 days of a change. In most cases, our internal processes will address the updates much sooner, but there is no compelling reason to include it as an enforceable requirement.
Response: The SDT thanks you for your comment.		
City of Austin dba Austin Energy	Yes	Austin Energy (AE) supports the requirements for (1) an annual test of the communications portion of the Operating Plan (R3) and (2) an annual review of the Operating Plan (R4); however, we offer a slight modification to the measures associated with those requirements. AE does not believe that records evidencing such test and reviews need to be time-stamped to adequately demonstrate compliance with the requirements. In each case, we recommend that the first sentence of M3 and M4 start with "Each Responsible Entity will have dated records to show that the annual ..."
Response: The SDT thanks you for your comment. The SDT has removed the time-stamping provision in the standard.		
Springfield Utility Board	Yes	o SUB supports the removal of Requirement 1, Part 1.4, as well the separation of Parts 1.3 and 1.5, agreeing that they are their own separate actions. o The Draft 4 Version History still lists the term "Impact Event" rather than "Event".
Response: The SDT thanks you for your comment. The SDT has made changes highlighted in your comment.		
FirstEnergy Corp	Yes	FE agrees with the revision but has the following comments and suggestions: 1. We request clarity and guidance on R3 (See our comments in Question 4 for further consideration). Also, we suggest a change in the phrase "shall conduct an annual test" to "shall conduct a test each calendar year, not to exceed 15 calendar months between tests". This wording is consistent with other

Organization	Yes or No	Question 1 Comment
		standards in development such as CIP Version 5.2. 2. In R4 we suggest a change in the phrase "shall conduct an annual review" to "shall conduct a review each calendar year, not to exceed 15 calendar months between reviews". This wording is consistent with other standards in development such as CIP Version 5.
Response: The SDT thanks you for your comment. The SDT deleted Requirement R4 based on stakeholder comments and revised Requirement R3 so that each Responsible Entity shall validate all contact information contained in the Operating Plan per Requirement R1 each calendar year. Requirement R3 will help ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization.		
Independent Electricity System Operator	Yes	We concur with the changes as they provide better streamlining of the four key requirements, with enhanced clarity. However, we are unclear on the intent of Requirement R3, in particular the phrase "not including notification to the Electric Reliability Organization" which begs the question on whether or not the test requires notifying all the other entities as if it were a real event. This may create confusion in ensuring compliance and during audits. Suggest the SDT to review and modify this requirement as appropriate.
Response: The SDT thanks you for your comment. The SDT has revised the standard's language to address this concern.		
Public Utility District No. 1 of Snohomish County	Yes	This is an excellent improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
Seattle City Light	Yes	This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
MEAG Power	Yes	This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
Response: The SDT thanks you for your comment. Please review the response to Question 4.		

Organization	Yes or No	Question 1 Comment
Tacoma Power	Yes	Tacoma Power agrees with the requirement but would suggest removing all instances the word "Operating" from the Standard. The requirements should read, " Each Responsible Entity shall have an "Event Reporting Plan...".The term Operating in this context is confusing as there are many other "Operating Plans" for other defined emergencies. This standard is about "Reporting" and should be confined to that.
Response: The SDT thanks you for your comment. The SDT has chosen to include "Operating" due to the definition in the NERC Glossary. The SDT believes Operating Plan clearly defines what is needed in this standard.		
Idaho Power Co.	Yes	But this is going to require that we create a new Operating Plan with test procedures and revision history.
Response: The SDT thanks you for your comment. The SDT believes that an existing procedure, that meets the requirements of CIP-001-2a, may well be the starting point for the Operating Plan in this standard, or could go a long way towards achieving the requirements in this standard. The SDT revised Requirement R3 to remove test to "validate" contact information contained in the Operating Plan. If an entity experiences an actual event, communication evidence from the event may be used to show compliance with the validation requirement for the specific contacts used for the event.		
American Public Power Association	Yes	APPA appreciates the SDT making these requirements clearer as requested in our comments on the previous draft standard.
Response: The SDT thanks you for your comment.		
Puget Sound Energy, Inc.	Yes	This draft is a considerable improvement on the previous draft in terms of clarity and will be much easier for Responsible Entities to implement. Puget Sound Energy appreciates the drafting team's responsiveness to stakeholder's concerns and the opportunity to comment on the current draft. The drafting team should revise Requirement R2 to state that the "activation" of the Operating Plan is required only when an event occurs, instead of using the term "implement". "Implementation" could also refer

Organization	Yes or No	Question 1 Comment
		to the activities such as distributing the plan to operating personnel and training operating personnel on the use of the plan. These activities are not triggered by any event and, since it is clear from the measure that this requirement is intended to apply only when there has been a reportable event, the requirement should be revised to state that as well. The drafting team should revise measure M2 to require reports to be "supplemented by operator logs or other reporting documentation" only "as necessary". In many cases, the report itself and time-stamped record of transmittal will be the only documents necessary to demonstrate compliance with requirement R2.Under Requirement R3, using an actual event as sufficient for meeting the requirement for conducting an annual test would likely fall short of demonstrating compliance with the entire scope of the Operating Plan. R1.2 requires "a process for communicating EACH of the applicable events listed....". If the actual event is only one of many "applicable" events, is it sufficient to only exercise one process flow? If there is no actual event during the annual time-frame, do all the process flows then have to be exercised?
Response: The SDT thanks you for your comment. The SDT appreciates the suggestion; however, to be consistent with other reliability standards, the SDT has elected to continue to use the word "Implement." Your suggestion could end up creating confusion and misunderstandings since the context is not used elsewhere. **The SDT has revised the language the requirements and measures as a result of your and other commenter's remarks.**		
FMPP		See FMPA's comments
Response: The SDT thanks you for your comment. Please review the response to the FMPA comments.		

Organization	Yes or No	Question 1 Comment
Luminant	Yes	
BC Hydro	Yes	
Imperial Irrigation District (IID)	Yes	
LG&E and KU Services	Yes	
PPL Corporation NERC Registered Affiliates	Yes	
Avista	Yes	
PNGC Comment Group	Yes	
Colorado Springs Utilities	Yes	
Arizona Public Service Company	Yes	
Georgia System Operations Corporation	Yes	
Texas Reliability Entity	Yes	
Dynegy Inc.	Yes	
Clark Public Utilities	Yes	
Pepco Holdings Inc	Yes	
Farmington Electric Utility System	Yes	

Organization	Yes or No	Question 1 Comment
Public Service Enterprise Group	Yes	
PPL Electric Utilities	Yes	
Cowlitz County PUD	Yes	
Edison Mission Marketing & Trading, Inc.	Yes	
Ameren	Yes	
We Energies	Yes	
GTC	Yes	
MISO	Yes	
Oncor Electric Delivery	Yes	
Los Angeles Department of Water and Power	Yes	
Deseret Power	Yes	

2. The SDT made clarifying revisions to Attachment 1 based on stakeholder feedback. Do you agree with these revisions? If not, please explain in the comment area below.

Summary Consideration:

The SDT reviewed, discussed and updated Attachment 1 based on comments received for commenters, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Under the Event Column, the SDT starts to classify each type of an event by assigning an "Event" title. The DSR SDT then updated the "Entity with Reporting Responsibilities" column to simply state which entity has the responsibility to report if they experience an event. The last column, "Threshold for Reporting" is a bright line that, if reached, the entity needs to report that they experienced the applicable event per Requirement 1.

Organization	Yes or No	Question 2 Comment
Northeast Power Coordinating Council	No	Regarding Attachment 1, language identical to event descriptions in the NERC Event Analysis Process and FERC OE-417 should be used. Creating a third set of event descriptions is not helpful to system operators. Recommend aligning the Attachment 1 wording with that contained in Attachment 2, DOE Form OE-417 and the EAP whenever possible. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Using identical terminology will be difficult to achieve as the DOE form and EAP have differing processes for identification of the reportable incidences. The SDT has tried to set up the reportable events in the standard to be as similar as possible to the other organizations without being tied to their specific language. Attachment 2 has been modified to match the events types listed in Attachment 1.** The following pertains to Attachment 1:Replace the Attachment 1 "NOTE" with the following clarifying wording: NOTE: The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of Attachment 2 if the entity is required to submit an OE-417 report. Submit reports to

Organization	Yes or No	Question 2 Comment
		the ERO via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422. Initial submittal by Voice within the reporting time frame is acceptable for all events when followed by a hardcopy submittal by Facsimile or e-mail as and if required. **The SDT thanks you with your comment. First, the SDT believes that you intended the comment to address the "Note" on Attachment 2, not Attachment 1. The SDT does not believe that a hardcopy report is necessary if the organization has made voice contact.** The proposed "events" are subjective and will lead to confusion and questions as to what has to be reported. **The SDT disagrees and has established "events" to be reported based on bright line criteria. The events are consistent with previous versions of the CIP-001 and EOP-004 standards, as well as incidences being reporting to the DOE and EAP.** Event: A reportable Cyber Security Incident. All reportable Cyber Security Incidents may not require "One Hour Reporting." A "one-size fits all" approach may not be appropriate for the reporting of all Cyber Security Incidents. The NERC "Security Guideline for the Electricity Sector: Threat and Incident Reporting" document provides time-frames for Cyber Security Incident Reporting. For example, a Cyber Security Compromise is recommended to be reported within one hour of detection, however, Information Theft or Loss is recommended to be reported within 48 hours. Recommend listing the Event as "A confirmed reportable Cyber Security Incident. The existing NERC "Security Guideline for the Electricity Sector: Threat and Incident Reporting" document uses reporting time-frames based on "detection" and "discovery." Recommend using the word confirmed because of the investigation time that may be required from the point of initial "detection" or "discovery" to the point of confirmation, when the compliance "time-clock" would start for the reporting requirement in EOP-004-2. **The SDT is revising the standard to not contain reporting for Cyber Security incidents. Under the revisions, CIP-008-3 and successive versions will retain the**

Organization	Yes or No	Question 2 Comment
		reporting requirements. Event: Damage or destruction of a Facility Threshold for Reporting: revise language on third item to read: Results from actual or suspected intentional human action, excluding unintentional human errors. **The SDT reviewed, discussed and updated "Damage and destruction of a Facility" based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. The new "threshold" now states:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** Event: Any physical threat that could impact the operability of a Facility This Event category should be deleted. The word "could" is hypothetical and therefore

Organization	Yes or No	Question 2 Comment
		unverifiable and un-auditable. The word "impact" is undefined. Please delete this reporting requirement, or provide a list of hypothetical "could impact" events, as well as a specific definition and method for determining a specific physical impact threshold for "could impact" events other than "any." **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whomever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** Event: BES Emergency requiring public appeal for load reduction. Replace wording in the Event column with language from #8 on the OE-417 Reporting Form to eliminate reporting confusion. Following this sentence add, "This shall exclude other public

Organization	Yes or No	Question 2 Comment
		appeals, e.g., made for weather, air quality and power market-related conditions, which are not made in response to a specific BES event." **The SDT disagrees with quantifying a use of public appeals reporting for different types of events. The important item here is that a public appeal was issued for load reduction. A report is required to inform the ERO (and whoever else the entity wishes to inform per Requirement R1) of your current status and provide them with the situational awareness of the status of your system.** Event: Complete or partial loss of monitoring capability Event wording: Delete the words "or partial" to conform the wording to the NERC Event Analysis Process. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event now only applies to "Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.** Event: Transmission Loss Revise to BES Transmission Loss **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** Event: Generation Loss Revise to BES Generation Loss **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT**

Organization	Yes or No	Question 2 Comment
		removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."** **The SDT believes that if an entity reaches this threshold, it needs to be reported and most likely this will be BES connected generation assets.**
Response: The SDT thanks you for your comment.		
DECo	No	On pg 17 in the Rationale Box for EOP-004 Attachment 1: The set of terms is specific then includes the word ETC. Then further lists areas to exclude. Then on Pg 23 of document it includes train derailment near a transmission right of way and forced entry attempt into a substation facility as reportable. These conflict. Also see conflict when in pg 21 states the DOE OE417 would be excepted in lieu of the NERC form, but on the last pg it states the DOE OE417 should be attached to the NERC report indicating the NERC report is still required.
Response: The SDT thanks you for your comment. While the SDT would like to point out the "etc." is the last word in the definition of Facility; the SDT has removed footnote 1 and the forced intrusion statement has been removed. The SDT has updated to remove the conflict of "attached to the NERC report…" The SDT agrees with your comments and have revised the standard to address these discrepancies.		
Duke Energy	No	(1)We disagree with reporting CIP-008 incidents under this standard. We agree with the one-hour notification timeframe, but believe it should be in CIP-008 to avoid double jeopardy. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one-hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement.** (2)Damage or destruction of a Facility - Need clarity on how a vertically integrated

Organization	Yes or No	Question 2 Comment
		entity must report. For example a GOP probably won't know if an IROL will be affected. Also, there shouldn't be multiple reports from different functional entities for the same event. Suggest splitting this table so that GO, GOP, DP only reports "Results from actual or suspected intentional human action". **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of its Facility that results from actual or suspected intentional human action.** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per R1) the situational awareness that the Facility was 'damaged or destroyed' intentionally by a human."** **This event was written to cover the increase of "Entity with Reporting Responsibility," and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** (3)Generation Loss - Need more clarity on the threshold for reporting. For example if

Organization	Yes or No	Question 2 Comment
		we lose one 1000 MW generator at 6:00 am and another 1000 MW generator at 4:00 pm, is that a reportable event? **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."**
Response: The SDT thanks you for your comment.		
Luminant	No	Luminant appreciates the work of the SDT to modify Attachment 1 to address the concerns of the stakeholders. However, we are concerned that the threshold for reporting a Generation Loss in the ERCOT interconnection established by this revision is set at â‰¥ 1,000MW, which is not consistent with the level of single generation contingency used in ERCOT planning and operating studies. That level of contingency is currently set at the size of the largest generating unit in ERCOT, which is 1,375MW. For this reason, Luminant believes that the minimum threshold for reporting of a disturbance should be > 1,375MW for the ERCOT Interconnection.
Response: The SDT thanks you for your comment. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."** **The SDT discussed this issue and believes that ERCOT could change contingency level in the future, and this event is also applicable to the Quebec Interconnection.**		

Organization	Yes or No	Question 2 Comment
BC Hydro	No	BC Hydro supports the revisions to EOP-004 and would vote Affirmative with the following change. Attachment 1 has a One Hour Reporting requirement. BC Hydro proposes a One Hour Notification with the Report submitted within a specified timeframe afterward.
Response: The SDT thanks you for your comment. The SDT has removed all incidences involving one-hour reporting threshold; therefore, the SDT does not see the need to make this change.		
Bonneville Power Administration	No	BPA believes that clarifying language should be added to transmission loss event. (Page 19) [a report should not be required if the number of elements is forced because of pre-designed or planned configuration. System studies have to take such a configuration into account possible wording could be. Unintentional loss of three or more Transmission Facilities (excluding successful automatic reclosing or planned operating configuration)] **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** In addition, under the "Event" of Complete or partial loss of monitoring capability, BPA believes that "partial loss" is not sufficiently specific for BPA to write compliance operating procedures and suggest defining partial loss or removing it from the standard. Should the drafting team add clarifying language to remove "or partial loss" and address BPA's concerns on over emphasis on software tool to the operation of the system. BPA would change its negative position to affirmative. **The SDT has revised the language on this point in Attachment 1.**
Response: The SDT thanks you for your comment.		

Organization	Yes or No	Question 2 Comment
SPP Standards Review Group	No	To obtain an understanding of the drivers behind the events in Attachment 1, we would like to see where these events come from. If the events are required in standards, refer to them. If they are in the existing event reporting list, indicate so. If they are coming from the EAP, let us know. We have a concern that, as it currently exists, Attachment 1 can increase our reporting requirements considerably. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Reportable events should be similar, but not identical to the events reported to DOE or EAP.** We also have concerns about what appears to be a lack of coordination between EAP reporting requirements and those contained in Attachment 1. For example, the EAP reporting requirement is for the complete loss of monitoring capability whereas Attachment 1 adds the requirement for reporting a partial loss of monitoring capability. It appears that some of the EAP reporting requirements are contained in Attachment 1. We have concerns that this is beyond the scope of the SAR and should not be incorporated in this standard. **The SDT has revised the language on this point in Attachment 1. It should be noted that the EAP can use reports submitted under EOP-004-2 as the initial notification of an event that could be further addressed in the EAP.** We have concern with several of the specific event descriptions as contained in Attachment 1: Damage or destruction of a Facility - We are comfortable with the proposed definition of Adverse Reliability Impact but have concerns with the existing definition of ARI. Any physical threat that could impact the operability of a Facility1 - We take exception to this event in that is goes beyond what is currently required in EOP-004-1, including DOE reporting requirements, and the EAP reporting requirements. We do not understand the need for this event type and object to the potential for excessive

Organization	Yes or No	Question 2 Comment
		reporting required by such an event type. Additionally, we are concerned about the potential for multiple reporting of a single event. This same concern applies to several other events including Damage or destruction of a Facility, Loss of firm load for â‰¥ 15 minutes, System separation, etc. When multiple entities are listed as the Entity with Reporting Responsibility, Attachment 1 appears to require each entity in the hierarchy to submit a report. There should only be one report and it should be filed by the entity owning the event. The SDT addressed this issue in its last posting but the issue still remains and should be reviewed again. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** **The SDT understands that there may be several reports of a single event; and as the SDT has stated before, that this will give the ERO a better understanding of the**

Organization	Yes or No	Question 2 Comment
		depth and breathe of system conditions based on the given event. BES Emergency resulting in automatic firm load shedding - For some reason, not stipulated in the Consideration of Comments, the action word in the Entity with Reporting Responsibility was changed from 'experiences' to 'implements'. We recommend changing it back to 'experiences'. Automatic load shedding is not implemented. It does not require human intervention. It's automatic. Voltage deviation on a Facility - Similar to the comment on automatic load shedding above, the action word was changed from 'experiences' to 'observes'. We again recommend that it be changed back to 'experiences'. Using observes obligates a TOP, who is able to see a portion of a neighboring TOP's area, to submit a report if that TOP observed a voltage deviation in the neighboring TOP's area. The only reporting entity in this event should be the TOP within whose area the voltage deviation occurred. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Automatic firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)."** **This language clearly states that an entity reports if the threshold is reached.** Complete or partial loss of monitoring capability - Clarification on partial loss of monitoring capability and inoperable are needed. Also, the way the Threshold is written, it implies that a State Estimator and Contingency Analysis are required. To tone this down, insert the qualifier 'such as' in front of State Estimator. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event now only applies to "Complete loss of monitoring capabilities" for a RC, BA, or TOP when there is a complete loss of monitoring**

Organization	Yes or No	Question 2 Comment
		capabilities for 30 continuous minutes where their State Estimator or Contingency Analysis is inoperable. This will only apply to an RC, BA, or TOP who have this capability to start with.
Response: The SDT thanks you for your comment.		
Florida Municipal Power Agency	No	The bullet on "any physical threat" is un-measurable. What constitutes a "threat"? FMPA likes the language used in the comment form discussing this item concerning the judgment of the Responsible Entity, but, the way it is worded in Attachment 1 will mean the judgment of the Compliance Enforcement Authority, not the Responsible Entity. Presumably, the Responsible Entity will need to develop methods to identify physical threats in accordance with R1; hence, FMPA suggests rewording to: "Any physical threat recognized by the Responsible Entity through processes established in R1 bullet 1.1". We understand this introduces circular logic, but, it also introduces the "judgment of the Responsible Entity" into the bullet. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility." This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or**

Organization	Yes or No	Question 2 Comment
		activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event, unless it degrades the normal operation of a Facility. On the row of the table on voltage deviation, replace the word "observes" with "experiences". It is possible for one TOP to "observe" a voltage deviation on another TOP's system. It should be the responsibility of the TOP experiencing the voltage deviation on its system to report, not the one who "observes". On the row on islanding, it does not make sense to report islanding for a system with load less than the loss of load metrics and we suggest using the same 300 MW threshold for a reporting threshold. On the row on generation loss, some clarification on what type of generation loss (especially in the time domain) would help it be more measurable, e.g., concurrent forced outages. One the row on transmission loss, the same clarity is important, e.g., three or more concurrent forced outages. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Automatic firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)."** **This language clearly states that an entity reports if the threshold is reached.** On the row on loss of monitoring, while FMPA likes the threshold for "partial loss of monitoring capability" for those systems that have State Estimators, small BAs and TOPs will not need or have State Estimators and the reporting threshold becomes ambiguous. We suggest adding something like loss of monitoring for 25% of monitored points for those BAs and TOPs that do not have State Estimators.

Organization	Yes or No	Question 2 Comment
		The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event now only applies to "Complete loss of monitoring capabilities" for a RC, BA, or TOP when there is a complete loss of monitoring capabilities for 30 continuous minutes where their State Estimator or Contingency Analysis is inoperable. This will only apply to an RC, BA, or TOP who have this capability to start with.
Response: The SDT thanks you for your comment.		
LG&E and KU Services	No	The SDT should consider more clearly defining the Threshold for Reporting for the Event: "Any physical threat that could impact the operability of a Facility" to only address those events that have an Adverse Reliability Impact. Some proposed language might be: "Threat to a Facility excluding weather related threats that could result in an Adverse Reliability Impact."For those events specifically defined in the ERO Events Analysis Process, the SDT should consider revising the language to be more consistent with the language included in the ERO Events Analysis Process. Here is some recommended language: 1. EVENT: Transmission loss THRESHOLD FOR REPORTING: "Unintentional loss, contrary to design, of three or more BES Transmission Facilities (excluding successful automatic reclosing) caused by a common disturbance. **The SDT has taken your comment into consideration and this threshold for reporting now states:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** 2. EVENT: "Complete or partial loss of monitoring capability" - could be revised to read "Complete loss of SCADA control or monitoring functionality" THRESHOLD FOR REPORTING: "Affecting a BES control center for â‰¥ 30 continuous minutes such that analysis tools (e.g. State Estimator, Contingency Analysis) are rendered inoperable". **The SDT reviewed, discussed and updated Attachment 1 based on comments**

Organization	Yes or No	Question 2 Comment
		received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event now only applies to: **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.**
Response: The SDT thanks you for your comment.		
MRO NSRF	No	R1.2 states: A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies. This implies not only does NERC need to be notified within the specified time period but that: "other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies." are also required to be notified within in the time periods specified. We suggest a forth column be added to the table to clearly identify who must be notified within the specified time period or that R1.2 be revised to clearly state that only NERC must be notified to comply with the standard. With the use of "i.e." the SDT is mandating that each other entity must be contacted. The NSRF believes that the SDT meant that "e.g." should be used to provide examples. The SDT may wish to add another column to Attachment 1 to provide clarity. **The SDT has made the required change concerning replacing "i.e." with "e.g."** Also with regards to Attachment 1, the following comments are provided: 1. Instead of referring to CIP-008 (in the 1 hour reporting section), quote the words from CIP-008, this will require coordination of future revisions but will assure clarity in reporting requirements. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we**

Organization	Yes or No	Question 2 Comment
		have remanded the one-hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement. 2. Under "Damage or destruction of a Facility" a. The wording "affects an IROL (per FAC-014)," is too vague. Many facilities could affect an IROL, not as many if lost would cause an IROL. b. Adverse Reliability Impact is defined as:"The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection."There are an infinite number of routine events that result in the loss of generation plants due to inadvertent actions that somehow also damaged equipment. Any maintenance activity that damaged a piece of equipment that causes a unit to trip or results in a unit being taken off line in a controlled manner would now be reportable. This seems to be an excessive reporting requirement. Recommend that Adverse Reliability Impact be deleted and be replaced with actual EEA 2 or EEA 3 level events. c. The phrase "Results from actual or suspected intentional human action." This line item used the term "suspected" which relates to "sabotage". Recommend the following: Results from actual or malicious human action intended to damage the BES. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency.** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any**

Organization	Yes or No	Question 2 Comment
		abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** 3. "Any physical threat that could impact the operability of a Facility1"The example provided by the drafting team of a train derailment exemplifies why this requirement should be deleted. A train derailment of a load of banana's more than likely would not threaten a nearby BES Facility. However a train carrying propane that derails carrying propane could even if it were 10 miles away. Whose calculation will be used to determine if an event could have impacted the asset? As worded there is too much ambiguity left to the auditor. We suggest the drafting team clarify by saying "Any event that requires the a BES site be evacuated for safety reasons" Furthermore if weather events are excluded, we are hard pressed to understand why this information is important enough to report to NERC. So barring an explanation of the purpose of this requirement, including why weather events would be excluded, we suggest the requirement be deleted. Please note that if you align this with "Physical attack" with #1 of the OE-417. This clearly states what the SDT is looking for. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry**

Organization	Yes or No	Question 2 Comment
		comments to state: **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** 4. The phrase "or partial loss of monitoring capability" is too vague. Further definitions of "inoperable" are required to assure consistent application of this requirement. Recommend that "Complete loss of SCADA affecting a BES control center for â‰¥ 30 continuous minutes such that analysis tools of State Estimator and/or Contingency Analysis are rendered inoperable. Or, Complete loss of the ability to perform a State Estimator or Contingency Analysis function, the threshold of 30 mins is too short. A 60 min threshold will align with EOP-008-1, R1.8. Since this is the time to implement the contingency back up control center plan. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event now only applies to:** **"Complete loss of monitoring capability affecting a BES control center for 30**

Organization	Yes or No	Question 2 Comment
		continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with. 5. Event: Voltage deviation on a Facility. ATC believes that the term "observes" for Entity with Reporting Responsibility be changed back to "experiences" as originally written. The burden should rest with the initiating entity in consistency with other Reporting Responsibilities. Also, for Threshold for Reporting, ATC believes the language should be expanded to - plus or minus 10% "of target voltage" for greater than or equal to 15 continuous minutes. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.** 6. Event: Transmission loss. ATC recommends that Threshold for Reporting be changed to read "Unintentional loss of four, or more Transmission Facilities, excluding successful automatic reclosing, within 30 seconds of the first loss experienced and for 30 continuous minutes. Technical justification or Discussion for this recommended change: In the instance of a transformer-line-transformer, scenario commonly found close-in to Generating stations, consisting of 3 defined "facilities", 1 lightning strike can cause automatic unintentional loss by design. Increase the number of facilities to 4. In a normal shoulder season day, an entity may experience the unintentional loss of a 138kv line from storm activity, at point A in the morning, a loss of a 115kv line from a different storm 300 miles from point A in the afternoon, and a loss of 161kv line in the evening 500 miles from point A due to a

Organization	Yes or No	Question 2 Comment
		failed component, if it is an entity of significant size. Propose some type of time constraint. Add time constraint as proposed, 30 seconds, other than automatic reclosing. In the event of dense lightning occurrence, the loss of multiple transmission facilities may occur over several minutes to several hours with no significant detrimental effect to the BES, as load will most certainly be affected (lost due to breaker activity on the much more exposed Distribution system) as well. Any additional loss after 30 seconds must take into account supplemental devices with intentional relay time delays, such as shunt capacitors, reactors, or load tap changers on transformers activating as designed, arresting system decay. In addition, Generator response after this time has significant impact. Please clarify or completely delete why this is included within this version when no basis has been give and it is not contained within the current enforceable version. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2.** **The SDT has taken your comment into consideration and this threshold for reporting now states:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** 7. Modify the threshold of "BES emergency requiring a public appeal…" to include, "Public appear for a load reduction event resulting for a RC or BA implementing its emergency operators plans documented in EOP-001." The reason is that normal public appeals for conservation should be clearly excluded. **The SDT disagrees since it is clearly stated that a report is required for "Public appeal for load reduction event." The SDT has not discussed a reporting mechanism for "conservation."** 8. Add a time threshold to complete loss of off-site power to a nuclear plant. Nuclear plants are to have backup diesel generation that last for a minimum amount of time. A threshold recognizing this 4 hour or longer window needs to be added

Organization	Yes or No	Question 2 Comment
		such as complete loss of off-site power to a nuclear plant for more than 4 hours. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2.** **The SDT has taken your comment into consideration and this threshold for reporting now states:** **"Complete loss of off-site power affecting a nuclear generating station per the Nuclear Plant Interface Requirement." As stated in this event Threshold, the TOP's NIPR may have additional guidance concerning the complete loss of offsite power affecting a nuclear plant.** 9. Delete "Transmission loss". The loss of a specific number of elements has no direct bearing on the risk of a system cascade. Faults and storms can easily result in "unintentional" the loss of multiple elements. This is a flawed concept and needs to be deleted **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2.** **The SDT has taken your comment into consideration and this threshold for reporting now states:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."**
Response: The SDT thanks you for your comment.		
PPL Corporation NERC Registered Affiliates	No	1.) PPL Generation thanks the SDT for the changes made in this latest proposal. We feel our previous comments were addressed. PPL Generation offers the following additional comments. Regarding the event 'Transmission Loss': For your consideration, please consider adding a footnote to the event 'Transmission Loss' such that weather events do not need to be reported. Also please consider including operation contrary to design in the language and not just in the example. E.g. consistent with the NERC Event Analysis table, the threshold would be, 'Unintentional loss, contrary to design, of three or more

Organization	Yes or No	Question 2 Comment
		BES Transmission Facilities.' **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2.** **The SDT has taken your comment into consideration and this threshold for reporting now states:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)." The SDT has removed all footnotes within Attachment 1.** 2.) PPL Generation proposes the following changes in Attachment 1 to the first entry in the "Threshold for Reporting" column to make it clear that independent GO/GOPs are required to act only within their sphere of operation and based on the information that is available to the GO/GOPs: Damage or destruction of a Facility that: Affects an IROL (per FAC-014, not applicable to GOs and GOPs) OR Results in the need for actions to avoid an Adverse Reliability Impact (not applicable to GOs and GOPs) OR Results from actual or suspected intentional human action (applicable to all). **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any**

Organization	Yes or No	Question 2 Comment
		abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s). The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within

Organization	Yes or No	Question 2 Comment
		their Operating Plan.
Response: The SDT thanks you for your comment.		
ISO/RTO Standards Review Committee	No	The SRC response to this question does not indicate support of the proposed requirement. Please see the latter part of the SRC's response to Question 4 below for an SRC proposed alternative approach:
Response: The SDT thanks you for your comment. Please review response to Question 4 comment.		
ACES Power Marketing Standards Collaborators	No	The drafting team made a number of positive changes to Attachment 1. However, there are a few changes that have introduced new issues and there are a number of existing issues that have yet to be fully addressed. One of the existing issues is that the reporting requirements will result in duplicate reporting. Considering that one of the stated purposes is to eliminate redundancy, we do not see how the scope of the SAR can be considered to be met until all duplicate reporting is eliminated. **The SDT acknowledges that reporting of the same event will come from multiple parties. However, as the industry has learned from recent events, NERC needs to have perspectives from a variety of entities instead of just one party's viewpoint. Reliability can be improved from learning how the differing parties see or experience the event. Sometimes, the differing perspectives have provided valuable insight on the true nature of the event. Therefore, the SDT believes that having multiple reports will aid reliability as we can learn from everyone's experiences.**

Organization	Yes or No	Question 2 Comment
		More specifics on our concerns are provided in the following discussion. (1) In the "Damage or destruction of a Facility" event, the statement "Affects an IROL (per FAC-014)" in the "Threshold for Reporting" is ambiguous. What does it mean? If the loss of a Facility will have a 1 MW flow change on the Facilities to which the IROL applies, is this considered to have affected the IROL? We suggest a more direct statement that damage or destruction occurred on a Facility to which the IROL applies or to one of the Facilities that comprise an IROL contingency as identified in FAC-014-2 R5.1.3. Otherwise, there will continue to be ambiguity over what constitutes "affects". (2) In the "Damage or destruction of a Facility" event, the threshold regarding "intentional human action" is ambiguous and suffers from the same difficulties as defining sabotage. What constitutes intentional? How do we know something was intentional without a law enforcement investigation? This is the same issue that prevented the drafting team from defining sabotage. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency.** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to**

Organization	Yes or No	Question 2 Comment
		prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s). The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within

Organization	Yes or No	Question 2 Comment
		their Operating Plan. (3) In the "Damage or destruction of a Facility" and "Any physical threat that could impact the operability of a Facility" events, Distribution Provider should be removed. Per the Function Model, the Distribution Provider does not have any Facilities (line, generator, shunt compensator, transformer). The only Distribution Provider equipment that even resembles a Facility would be capacitors (i.e. shunt compensator) but they do not qualify because they are not Bulk Electric System Elements. **The SDT agrees that if a DP does not own or operate a Facility then this event would not be applicable to them. However, if a DP does experience an event such as those listed, then it is a reportable incident under this standard.** (4) The "Any physical threat that could impact the operability of a Facility" event requires duplicate reporting. For example, if a large generating plant experiences such a threat, who should report the event? What if loss of the plant could cause capacity and energy shortages as well as transmission limits? The end result is that the RC, BA, TOP, GO and GOP could all end up submitting a report for the same event. For a given operating area, only one report should be required from one registered entity for each event. **The SDT acknowledges that multiple reports could result from an event. If an entity experiences an applicable event type, then they required to report it. As previously stated, the industry can benefit from having such differing perspectives when events occur.** (5) The "Any physical threat that could impact the operability of a Facility" event should not apply to a single Facility but rather multiple Facilities which if lost would impact BES reliability. As written now, a train derailment near a single 138 kV transmission line or small generator with minimal reliability impact would require reporting. **The SDT removed all language under "Entity with Reporting Responsibility," with**

Organization	Yes or No	Question 2 Comment
		the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** (6) The "BES Emergency resulting in automatic firm load shedding" should not apply to the DP. In the existing EOP-004 standard, Distribution Provider is not included and the load shed information still gets reported. **The SDT believes that the DP should be required to report "automatic firm load shedding…" to the ERO (and whoever else the entity wishes to inform per Requirement R1).** (7) The "Voltage deviation on a Facility" event needs to be clarified that the TOP only reports voltage deviations in its Transmission Operator Area. Because TOPs may view

Organization	Yes or No	Question 2 Comment
		into other Transmission Operator Areas, it could technically be required to report another TOP's voltage deviation because one of its System Operators observed the neighboring TOP's voltage deviation. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes ."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.** **The SDT understands that there may be several reports of a single event; and as the SDT has stated before, that this will give the ERO a better understanding of the depth and breathe of system conditions based on the given event.** (8) For the "Loss of firm load greater than 15 minutes" event, the potential for duplicate reporting needs to be eliminated. Every time a DP experiences this event, the DP, TOP and BA all appear to be required to report since the DP is within both the Balancing Authority Area and Transmission Operator Area. Only one report is necessary and should be sent. Given that the existing EOP-004 standard does not include the DP, we suggest eliminating the DP to eliminate one level of duplicate reporting. **The SDT understands that there may be several reports of a single event; and as the SDT has stated before, that this will give the ERO a better understanding of the depth and breathe of system conditions based on the given event.** (9) For the "System separation (islanding)" event, please remove DP. As long as any island remains viable, the Distribution Provider will not even be aware that an island occurred. It is not responsible for monitoring frequency or having a wide area view.

Organization	Yes or No	Question 2 Comment
		The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. **This event is now only applicable to RC, BA, and TOP.** (10) For the "System separation (islanding)" event, please remove BA. Because islanding and system separation, involve Transmission Facilities automatically being removed from service, this is largely a Transmission Operator issue. This position is further supported by the approval of system restoration standard (EOP-005-2) that gives the responsibility to restore the system to the TOP. (11) For the "System separation (islanding)" event, please eliminate duplicate reporting by clarifying that the RC should submit the report when more than one TOP is involved. If only one TOP is involved, then the single TOP can submit the report or the RC could agree to do it on their behalf. Only one report is necessary. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified.** **This event is now only applicable to RC, BA, and TOP. The SDT understands that there may be several reports of a single event; and as the SDT has stated before, that this will give the ERO a better understanding of the depth and breathe of system conditions based on the given event.** (12) For the "Generation loss" event, duplicate reporting should be eliminated. It is not necessary for both the BA and GOP to submit two separate reports with nearly identical information. Only one entity should be responsible for reporting. **The SDT understands that there may be several reports of a single event; and as the SDT has stated before, that this will give the ERO a better understanding of the depth and breathe of system conditions based on the given event.** (13) For the "Complete loss of off-site power to a nuclear generating plant", the

Organization	Yes or No	Question 2 Comment
		associated GO or GOP should be required to report rather than the TO or TOP. Maintaining power to cooling systems is ultimately the responsibility of the nuclear plant operator. At the very least, TO should be removed because it is not an operating entity and loss of off-site power is an operational issue. If the TOP remains in the reporting responsibility, it should be clarified that it is only a TOP with an agreement pursuant to NUC-001. All of this is further complicated because NUC-001 was written for a non-specific transmission entity because there was no one functional entity from which the nuclear plant operator gets it off-site power. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2.** **The SDT has taken your comment into consideration and this threshold for reporting now states:** **"Complete loss of off-site power affecting a nuclear generating station per the Nuclear Plant Interface Requirement." As stated in this event Threshold, the TOP's NIPR may have additional guidance concerning the complete loss of offsite power affecting a nuclear plant.** (14) For the "Complete or partial loss of monitoring capability", partial loss needs to be further clarified. Is loss of a single RTU a partial loss of monitoring capability? For a large RC is loss of ICCP to a single small TOP, considered a partial loss? We suggest as long as the entity has the ability to monitor their system through other means that the event should not be reported. For the loss of a single RTU, if the entity has a solving state estimator that provides estimates for the area impacted, the partial threshold loss would not be considered. If the entity has another entity (i.e. perhaps the RC is still receiving data for its TOP area, the RC can monitor for the TOP) that can monitor their system as a backup, the partial loss has not been met. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event now only applies to:** **"Complete loss of monitoring capability affecting a BES control center for 30**

Organization	Yes or No	Question 2 Comment
		continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.
Response: The SDT thanks you for your comment.		
Southern Company Services	No	It appears that the SDT has incorporated the reporting requirements for CIP-008 "reportable Cyber Security Incidents"; however, the "recognition" requirements remain in CIP-008 Reliability Standard. Southern understands the desire to consolidate reporting requirements into a single standard, but it would be clearer for Cyber Security Incidents if both the recognition and reporting requirements were in one reliability standard and not spread across multiple standards. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement.** As it relates to the event type "Loss of Firm Load for > 15 minutes", Southern suggests that the SDT clarify if weather related loss of firm load is excluded from the reporting requirement. **The SDT believes that it is important to report this event based on the threshold regardless of the cause. This will give the ERO (and whoever else the entity wishes to inform per Requirement R1) a better understanding of the depth and breathe of system conditions based on the given event.** As it relates to the event type "Loss of all voice communication capability", Southern suggest that the SDT clarify if this means both primary and backup voice communication systems or just primary voice communication systems. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry**

Organization	Yes or No	Question 2 Comment
		comments to state: **"Complete loss of voice communications capabilities affecting a BES control center for 30 continuous minutes or more." The SDT intends "complete" to mean all capabilities, including back up capabilities.** Referring to "CIP-008-3 or its successor" in Requirement R1.1 is problematic. This arrangement results in a variable requirement for EOP-004-2 R1. The requirements in a particular version of a standard should be fixed and not variable. If exceptions to applicable events change, a revision should be made to EOP-004 to reflect the modified requirement. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008.**
Response: The SDT thanks you for your comment.		
Hydro One	No	In the Attachment 1, language identical to event descriptions in the NERC Event Analysis Process and FERC OE-417 should be used. Creating a third set of event descriptions is not helpful to system operators. Recommend aligning the Attachment 1 wording with that contained in Attachment 2, DOE Form OE-417 and the EAP whenever possible. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Using identical terminology will be difficult to achieve as the DOE form and EAP have differing processes for identification of the reportable incidences. The SDT has tried to set up the reportable events in the standard to be as similar as possible to the other organizations without being tied to their specific language. Attachment 2 has been modified to match the events types listed in Attachment 1.** The proposed "events" are subjective and will lead to confusion and questions as to what has to be reported. - Event: A reportable Cyber Security Incident. All reportable Cyber Security Incidents may not require "One Hour Reporting." A "one-size fits all" approach may not be appropriate for the reporting of all Cyber Security

Organization	Yes or No	Question 2 Comment
		Incidents. The NERC "Security Guideline for the Electricity Sector: Threat and Incident Reporting" document provides time-frames for Cyber Security Incident Reporting. For example, a Cyber Security Compromise is recommended to be reported within one hour of detection, however, Information Theft or Loss is recommended to be reported within 48 hours. Recommend listing the Event as "A confirmed reportable Cyber Security Incident. The existing NERC "Security Guideline for the Electricity Sector: Threat and Incident Reporting" document uses reporting time-frames based on "detection" and "discovery." Recommend using the word confirmed because of the investigation time that may be required from the point of initial "detection" or "discovery" to the point of confirmation, when the compliance "time-clock" would start for the reporting requirement in EOP-004-2. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement. Note that the existing NERC "Security Guideline for the Electricity Sector: Threat and Incident Reporting" document is a "guideline" to assist entities. It should not be confused with a mandatory and enforceable Reliability Standard.** - Event: Damage or destruction of a Facility Threshold for Reporting: revise language on third item to read: "Results from actual or suspected intentional human action, excluding unintentional human errors". **The SDT reviewed, discussed and updated "Damage and destruction of a Facility" based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. The new "threshold" not states:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any**

Organization	Yes or No	Question 2 Comment
		abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** - Event: Any physical threat that could impact the operability of a Facility This Event category should be deleted. The word "could" is hypothetical and therefore unverifiable and un-auditable. The word "impact" is undefined. Please delete this reporting requirement, or provide a list of hypothetical "could impact" events, as well as a specific definition and method for determining a specific physical impact threshold for "could impact" events other than "any." **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility**

Organization	Yes or No	Question 2 Comment
		Do not report copper theft unless it degrades normal operations of a Facility." **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** - Event: BES Emergency requiring public appeal for load reduction. Replace wording in the Event column with language from #8 on the OE-417 Reporting Form to eliminate reporting confusion. Following this sentence add, "This shall exclude other public appeals, e.g., made for weather, air quality and power market-related conditions, which are not made in response to a specific BES event." **The SDT disagrees with quantifying a use of public appeals reporting for different types of events. The important item here is that a public appeal was issued for load reduction. A report is require to inform the ERO (and whoever else the entity wishes to inform per Requirement R1) of your current status and provide them with the situational awareness of the status of your system.** - Event: Complete or partial loss of monitoring capability Event wording: Delete the words "or partial" to conform the wording to the NERC Event Analysis Process. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event now only applies to:** **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.**

Organization	Yes or No	Question 2 Comment
		Event: Transmission Loss Revise to BES Transmission Loss **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** Event: Generation Loss Revise to BES Generation Loss **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."** **The SDT believes that if an entity reaches this threshold, it needs to be reported.**
Response: The SDT thanks you for your comment.		
CenterPoint Energy	No	CenterPoint Energy appreciates the revisions made to Attachment 1 based on stakeholder feedback; however, the Company continues to have concerns regarding certain events and thresholds for reporting and offers the following recommendations. (1) CenterPoint Energy recommends the deletion of "per Requirement R1" in the "Note" under Attachment 1 as it contains a circular reference back to R1 which includes timeframes.

Organization	Yes or No	Question 2 Comment
		The SDT has updated Requirement R1 due to industry comments to read: "R1. Each Responsible Entity shall have an event reporting Operating Plan that includes communication protocol(s) for applicable events listed in, and within the time frames specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations based on the event type (e.g. the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, governmental or provincial agencies)." (2) CenterPoint Energy maintains that a required 1 hour threshold for reporting of any event is unreasonable. CenterPoint Energy is confident that given dire circumstances Responsible Entities will act quickly on responding to and communication of any impending threat to the reliability of the Bulk Electric System. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement.** (3) For the event of "Damage or destruction of a Facility", CenterPoint Energy is concerned that the use of the term "suspected" is too broad and proposes that the SDT delete "suspected" and add "that causes an Adverse Reliability Impact…" to the threshold for reporting regarding human action. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."**

Organization	Yes or No	Question 2 Comment
		This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s). The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility

Organization	Yes or No	Question 2 Comment
		was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan. (4) CenterPoint Energy believes that the event, "Any physical threat that could impact the operability of a Facility" is too broad and should be deleted. Alternatively, CenterPoint Energy recommends that the SDT delete "could" or change the event description to "A physical incident that causes an Adverse Reliability Impact". Additionally, in footnote 1, the example of a train derailment uses the phrase "could have damaged". CenterPoint Energy is concerned that as beauty is the eye of the beholder, this phrase is open to interpretation and therefore recommends that the phrase, "causes an Adverse Reliability Impact" be incorporated into the description. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event and footnote 1. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this**

Organization	Yes or No	Question 2 Comment
		will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility. (5) The Company proposes that the threshold for reporting the event, "BES Emergency requiring manual firm load shedding" is too low. It appears the SDT was attempting to align this threshold with the DOE reporting requirement. However, as the SDT stated above, there are several valid reasons why this should not be done; therefore, CenterPoint Energy recommends the threshold be revised to "Manual firm load shedding â‰¥ 300 MW". **The SDT disagrees as this is currently enforceable within EOP-004-1.** (6) CenterPoint Energy also recommends a similar revision to the threshold for reporting associated with the "BES Emergency resulting in automatic firm load shedding" event. ("Firm load shedding â‰¥ 300 MW (via automatic under voltage or under frequency load shedding schemes, or SPS/RAS") **The SDT disagrees as we have aligned this with "manual firm load shedding." As written a report will be required for load shedding of 100MW for automatic or manual actions.** (7) CenterPoint Energy is uncertain of the event, "Loss of firm load for â‰¥ 15 minutes" and its fit with BES Emergency requiring manual firm load shedding or BES Emergency resulting in automatic firm load shedding. The Company believes that this event is already covered with manual firm load shedding and automatic firm load shedding and should therefore be deleted. **The SDT disagrees, as "Loss of firm load" is due to an action other than loss of load due to "automatic" or "manual" actions by the BA, TOP, or DP. The intent is to capture that load was loss by some other action. Note that this is a currently enforceable item within EOP-004-1.**

Organization	Yes or No	Question 2 Comment
		(8) For the event of "System separation (islanding)", CenterPoint Energy believes that 100 MW is inconsequential and proposes 300 MW instead. **The SDT disagrees, as this has been vetted through the industry with very little negative feedback.** (9) For "Generation loss", CenterPoint Energy suggests that the SDT add "only if multiple units" to the criteria of "1,000 MW for entities in the ERCOT or Quebec Interconnection". **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."** (10) Finally, CenterPoint Energy recommends that the SDT delete the term "partial" under the "Entity with Reporting Responsibility" for "Complete or partial loss of monitoring capability". The Company proposes revising the event description to "Loss of monitoring capability for > 30 minutes that causes system analysis tools to be inoperable". **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event is now written to state:** **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or**

Organization	Yes or No	Question 2 Comment
		TOP who have this capability to start with.
Response: The SDT thanks you for your comment.		
Arkansas Electric Cooperative Corporation	No	AECC supports the comments submitted by ACES Power Marketing.
Response: The SDT thanks you for your comment. Please review the response to that commenter.		
MWDSC	No	See comment for question 1
Response: The SDT thanks you for your comment. Please review the response to Question 1.		
Georgia System Operations Corporation	No	See comments under no. 4 below.
Response: The SDT thanks you for your comment. Please review the response to Question 4.		
Texas Reliability Entity	No	(1) In the Events Table, consider whether the item for "Voltage deviation on Facility" should also be applicable to GOPs, because a loss of voltage control at a generator (e.g. failure of an automatic voltage regulator or power system stabilizer) could have a similar impact on the BES as other reportable items. Note: We made this comment last time, and the SDT's posted response was non-responsive to this concern. **The SDT reviewed TRE's comment and believe that our consideration of comments during that last posting clearly stated the SDT view correctly. We stated "The SDT disagrees with this comment. Attachment 1 is the minimum set of events that will be required to report and communicate per your Operating Plan will be aware of system conditions." Further, we note that such events do not rise to the level of notification to the ERO. When events like the ones you mention occur, then entity has obligations to notify other parties according to reliability standards relating to that equipment. The NERC Standards Process Manual does allow TRE to apply for a variance if they have special concerns that GOPs should submit a report to the ERO.** (2) In the Events Table, under Transmission Loss, the SDT indicated that reporting is triggered only if three or more Transmission Facilities operated by a single TOP are lost. What if four Facilities are lost, with two Facilities operated by each of two TOPs?

Organization	Yes or No	Question 2 Comment
		That is a larger event than three Facilities lost by one TOP, but there is no reporting requirement? Determining event status by facility ownership is not an appropriate measure. The reporting requirements should be based on the magnitude, duration, or impact of the event, and not on what entities own or operate the facilities. (3) In the Events Table, under Transmission Loss, the criteria "loss of three or more Transmission Facilities" is very indefinite and ambiguous. For example, how will bus outages be considered? Many entities consider a bus as a single "Facility," but loss of a single bus may impact as many as six 345kV transmission lines and cause a major event. It is not clear if this type of event would be reportable under the listed event threshold? Is the single-end opening of a transmission line considered as a loss of a Facility under the reporting criteria? (4) Combinations of events should be reportable. For example, a single event resulting in the loss of two Transmission Facilities (line and transformer) and a 950 MW generator would not be reportable under this standard. But loss of two lines and a transformer, or a 1000 MW generator, would be reportable. It is important to capture all events that have significant impacts. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** **The SDT has reviewed Attachment 1 as a minimum level of reporting thresholds. There may be times where an entity may wish to report when a threshold has not been reached because of their experience with their system. EOP-004-2 does not prevent any entity from reporting any type of situation (event) at anytime. Note that the SDT has received industry feedback and it is not within scope of a results**

Organization	Yes or No	Question 2 Comment
		based Standards concept to be very prescriptive in nature. (5) In the Events Table, under "Unplanned control center evacuation," "Loss of all voice communication capability" and "Complete or partial loss of monitoring capability," GOPs should be included. GOPs also operate control centers that are subject to these kinds of occurrences, with potentially major impacts to the BES. Note that large GOP control centers are classified as "High Impact" facilities in the CIP Version 5 standards, and a single facility can control more than 10,000 MW of generation. **The SDT appreciates your suggestion; however, as we understand the point, it doesn't apply continent-wide. The SDT has applied these events to RCs, BAs, and TOPs.** (6) The "BES Emergency resulting in automatic firm load shedding" event row within Attachment 1 should include the BA as a responsible entity for reporting. Note that EOP-003-1 requires the BA to shed load in emergency situations (R1, R5 as examples), and any such occurrence should be reported. **The SDT has reviewed your comment and would like to note that manual load shedding is only reportable if 100 MW or more is activated. Automatic load shedding is intended to be when a "relay" performs a breaker action that sheds load without human interaction and achieves a level of 100 MW or more.**
Response: The SDT thanks you for your comment.		
Occidental Power Services, Inc.	No	There are no requirements in Attachment 1 for LSEs without BES assets so these entities should not be in the Applicability section.
Response: The SDT thanks you for your comment. The LSE obligation in this standard was tied to applicability in CIP-008 for cyber incident reporting. Reporting under CIP-008 is no longer proposed to be a part of EOP-004-2 so this applicability has been removed. Please note that LSEs will be obligated to report under CIP-008 until that standard has been changed.		
Xcel Energy	No	1) The event Damage or destruction of a Facility appears to need 'qualifying'. Is this intended for only malicious intent? Otherwise, weather related or other operational events will often meet this criteria. For example adjustment in generation or changes

Organization	Yes or No	Question 2 Comment
		in line limits to "avoid an Adverse Reliability Impact" could occur during a weather related outage. We suggest adjusting this event and criteria to clearly exclude certain items or identify what is included. **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and**

Organization	Yes or No	Question 2 Comment
		identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** 2) Also recommend placing the information in footnote 1 into the associated Threshold for Reporting column, and removing the footnote. **The SDT has removed the footnote per industry comments and concerns.**
Response: The SDT thanks you for your comment.		
American Electric Power	No	If CIP-008 is now out of scope within the requirements of this standard, any references to it should also be removed from Attachment 1. **The SDT has removed the one-hour reporting requirement as requested within**

Organization	Yes or No	Question 2 Comment
		comments received. The Threshold for Reporting column on page 26 includes "Results from actual or suspected intentional human action." This wording is too vague as many actions by their very nature are intentional. In addition, it should actually be used as a qualifying event rather than a threshold. We recommend removing it entirely from the Threshold column, and placing it in the Events column and also replacing the first row as follows: "Actual or suspected intentional human action with the goal of damage to, or destruction of, the Facility." On page 27, the event "Any physical threat that could impact the operability of a Facility" is too vague and broad. Using the phrases "any physical threat" and "could impact" sets too high a bar on what would need to be reported. On page 28, for the event "Complete loss of off-site power to a nuclear generating plant (grid supply)", TO and TOP should be removed and replaced by GOP. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has**

Organization	Yes or No	Question 2 Comment
		the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.
Response: The SDT thanks you for your comment.		
Clark Public Utilities	No	I agree with all but one. The event is "Damage or destruction of a Facility" and the threshold for reporting is "Results from actual or suspected intentional human action." I understand and agree that destruction of a facility due to actual or suspected intentional human action should always be reported. However, I do not know what level of damage should be reported. Obviously the term "damage" is meant to signify and event that is less than destruction. As a result, damage could be extensive, minimal, or hardly noticeable. There needs to be some measure of what the damage entails if the standard is to contain a broad requirement for the reporting of damage intentionally caused by human action. Whether that measure is based on the actual impacts to the BES from the damage or whether the measure is based on the ability of the damaged equipment to continue to function at 100%, 50% or some capability would be acceptable but currently it is too open ended.
Response: The SDT thanks you for your comment. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.**		

Organization	Yes or No	Question 2 Comment
This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s). The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.		
New York Power Authority	No	Please see comments submitted by NPCC Regional Standards Committee (RSC).
Response: Thank you for your comment. Please see response to the comments.		
Consolidated Edison Co. of NY, Inc.	No	General comment regarding Attachment 1:SDT should strive to use identical language to event descriptions in the NERC Event Analysis Process and FERC OE-417. Creating a third set of event descriptions is not helpful to system operators. We recommend aligning the Attachment 1 wording with that contained in Attachment 2, DOE Form OE-417 and the EAP whenever possible. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Using identical terminology will be difficult to achieve as the DOE form and EAP have differing processes for identification of the reportable incidences. The SDT has tried to set up the reportable events in the standard to be as similar as possible to the other organizations without being tied to their specific language. Attachment 2 has been modified to match the events types listed in Attachment 1.** Replace the Attachment 1 "NOTE" with the following clarifying wording: NOTE: The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of Attachment 2 if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422. Initial submittal by Voice within the reporting time frame is acceptable for all events when followed by a hardcopy submittal by Facsimile or e-mail as and if required.

Organization	Yes or No	Question 2 Comment
		The SDT thanks you with your comment. First, the SDT believes that you intended the comment to address the "Note" on Attachment 2, not Attachment 1. The SDT does not believe that a hardcopy report is necessary if the organization has made voice contact. Event: Damage or destruction of a Facility Threshold for Reporting: revise language on third item to read, Results from actual or suspected intentional human action, excluding unintentional human errors. **The SDT reviewed, discussed and updated "Damage and destruction of a Facility" based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. The new "threshold" not states:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable**

Organization	Yes or No	Question 2 Comment
		operations of each interconnection. Event: Any physical threat that could impact the operability of a Facility This Event category should be deleted. The word "could" is hypothetical and therefore unverifiable and un-auditable. The word "impact" is undefined. Please delete this reporting requirement, or please provide a list of hypothetical "could impact" events, as well as a specific definition and method for determining a specific physical impact threshold for "could impact" events other than "any." **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement**

Organization	Yes or No	Question 2 Comment
		R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility. Event: BES Emergency requiring public appeal for load reduction. Replace Event wording with language from #8 on OE-417 reporting form to eliminate reporting confusion. Following this sentence add, "This shall exclude other public appeals, e.g., made for weather, air quality and power market-related conditions, which are not made in response to a specific BES event. **The SDT disagrees with quantifying a use of public appeals reporting for different types of events. The important item here is that a public appeal was issued for load reduction. A report is require to inform the ERO (and whoever else the entity wishes to inform per Requirement R1) of your current status and provide them with the situational awareness of the status of your system.** "Event: Complete or partial loss of monitoring capability Event wording: Delete the words "or partial" to conform the wording to NERC Event Analysis Process. Event: Transmission Loss Modify to BES Transmission Loss Event Generation Loss Modify to BES Generation Loss
Orange and Rockland Utilities, Inc.	No	General comment regarding Attachment 1: SDT should strive to use identical language to event descriptions in the NERC Event Analysis Process and FERC OE-417. Creating a third set of event descriptions is not helpful to system operators. We recommend aligning the Attachment 1 wording with that contained in Attachment 2, DOE Form OE-417 and the EAP whenever possible. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. Using identical terminology will be difficult to achieve as the DOE form and EAP have differing processes for identification of the reportable incidences. The SDT has tried to set up the reportable events in the standard to be as similar as possible to the other organizations without being tied to their specific**

Organization	Yes or No	Question 2 Comment
		language. Attachment 2 has been modified to match the events types listed in Attachment 1. Replace the Attachment 1 "NOTE" with the following clarifying wording: NOTE: The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of Attachment 2 if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422. Initial submittal by Voice within the reporting time frame is acceptable for all events when followed by a hardcopy submittal by Facsimile or e-mail as and if required. **The SDT thanks you for your comment. First, the SDT believes that you intended the comment to address the "Note" on Attachment 2, not Attachment 1. The SDT does not believe that a hardcopy report is necessary if the organization has made voice contact.** Event: Damage or destruction of a Facility Threshold for Reporting: revise language on third item to read, Results from actual or suspected intentional human action, excluding unintentional human errors. **The SDT reviewed, discussed and updated "Damage and destruction of a Facility" based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. The new "threshold" not states:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could**

Organization	Yes or No	Question 2 Comment
		adversely affect the reliability of the Bulk Electric System). **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** Event: Any physical threat that could impact the operability of a Facility This Event category should be deleted. The word "could" is hypothetical and therefore unverifiable and un-auditable. The word "impact" is undefined. Please delete this reporting requirement, or please provide a list of hypothetical "could impact" events, as well as a specific definition and method for determining a specific physical impact threshold for "could impact" events other than "any." **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or**

Organization	Yes or No	Question 2 Comment
		Suspicious device or activity at a Facility **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** Event: BES Emergency requiring public appeal for load reduction. Replace Event wording with language from #8 on OE-417 reporting form to eliminate reporting confusion. Following this sentence add, "This shall exclude other public appeals, e.g., made for weather, air quality and power market-related conditions, which are not made in response to a specific BES event." **The SDT disagrees with quantifying a use of public appeals reporting for different types of events. The important item here is that a public appeal was issued for load reduction. A report is require to inform the ERO (and whoever else the entity wishes to inform per Requirement R1) of your current status and provide them with the situational awareness of the status of your system.** Event: Complete or partial loss of monitoring capability Event wording: Delete the words "or partial" to conform the wording to NERC Event Analysis Process. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event is now written to state:** **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or**

Organization	Yes or No	Question 2 Comment
		TOP who have this capability to start with. **Event: Transmission Loss Modify to BES Transmission Loss** **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** Event Generation Loss Modify to BES Generation Loss **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."**
Response: The SDT thanks you for your comment.		
FirstEnergy Corp	No	FE requests the following changes be made to Attachment 1:1. Pg. 19 / Event: "Voltage deviation on a Facility". The term "observes" for Entity with Reporting Responsibility be changed to "experiences". The burden should rest with the

Organization	Yes or No	Question 2 Comment
		initiating entity in consistency with other Reporting Responsibilities. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes."** 2. In "Threshold for Reporting", the language should be expanded to - plus or minus 10% "of nominal voltage" for greater than or equal to 15 continuous minutes. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.** 3. Pg.20 /Event: "Complete or partial loss of monitoring capability". The term "partial" should be deleted from the event description to read as follows: Complete loss of monitoring capability and the reporting responsibility requirements to read "Each RC, BA, and TOP that experiences the complete loss of monitoring capability." **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004**

Organization	Yes or No	Question 2 Comment
		into EOP-004-2. This event is now written to state: **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.**
Response: The SDT thanks you for your comment.		
Farmington Electric Utility System	No	The reporting threshold for "Complete or partial loss of monitoring capability" should be modified to include the loss of additional equipment and not be limited to State Estimator and Contingency Analysis. Some options have been included: Affecting a BES control center for â‰¥ 30 continuous minutes such that Real-Time monitoring tools are rendered inoperable. Affecting a BES control center for â‰¥ 30 continuous minutes to the extent a Constrained Facility would not be identified or an Adverse Reliability Impact event could occur due to lack of monitoring capability. Affecting a BES control center for â‰¥ 30 continuous minutes such that an Emergency would not be identified or ma
Response: The SDT thanks you for your comment. The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event is now written to state: **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.**		
Public Service Enterprise Group	No	We agreed with most of the revisions. However, for the 24-hour reporting time frame portion of the EOP-004 Attachment 1: Reportable Event that starts on p. 18, we have these concerns: a. Why was "RC" left out in the first row? RC is in the second row that also addresses a "Facility." We believe that "RC" was inadvertently

Organization	Yes or No	Question 2 Comment
		left out. b. In the first row, entities such as a BA, TO, GO, GOP, or DP would not know whether damage or destruction of one of its Facilities either "Affects an IROL (per FAC-014)" or "Results in the need for actions to avoid an Adverse Reliability Impact." FAC-014-2, R5.1.1 requires Reliability Coordinators provide information for each IROL on the "Identification and status of the associated Facility (or group of Facilities) that is (are) critical to the derivation of the IROL" to entities that do NOT include the entities listed above. And frankly, those entities would not need to know. The reporting requirements associated with "Damage or destruction of a Facility" need to be changed so that the criteria for reporting by an entity whose Facilities experience damage or destruction does not rely upon information that the entity does not possess. c. A possible route to achieve the results in b. above is described below: i. All Facilities that are damaged or destroyed that "Results from actual or suspected intentional human action" would be reported to the ERO by the entity experiencing the damage or destruction. ii. All Facilities that are damaged or destroyed OTHER THAN THAT due to an "actual or suspected intentional human action" would be reported to the RC by the entity experiencing the damage or destruction. Based upon those reports, the RC would be required to report whether the reported damage or destruction of a Facility "Affects an IROL (per FAC-010)" or "Results in the need for actions to Avoid an Adverse Reliability Consequence." (The RC may need to modify its data specifications in IRO-010-1a - Reliability Coordinator Data Specification and Collection - to specify outages due to "damage or destruction of a Facility." We also note that "DP" is not included in IRO-010-1a, but "LSE" is included. DPs are required to also register as LSEs if they meet certain criteria. See the "Statement of Compliance Registry Criteria, Rev. 5.0", p.7. For this reason, we suggest that DP be replaced with LSE in EOP-004-2.) d. To implement the changes in c. above, we suggest that the first row be divided into two rows: i. FIRST ROW: This would be like the existing first row on page 18, except "RC" would be added to the column for "Entity with Reporting Responsibility" and the only reporting threshold would be ""Results from actual or suspected intentional human action." ii. SECOND ROW: The Event would be "Damage or destruction of a Facility of a BA, TO, TOP, GO,

Organization	Yes or No	Question 2 Comment
		GOP, or LSE," the Entity, the Reporting Responsibility would be "The RC that has the BA, TOP, GO, GOP, or LSE experiencing the damage or destruction in its area," and the Threshold for Reporting would be "Affects an IROL (per FAC-010)" or "Results in the need for actions to avoid an Adverse Reliability Consequence."

Response: The SDT thanks you for your comment. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:

"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."

This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).

This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.

The SDT also developed another to read:

Organization	Yes or No	Question 2 Comment
"Damage or destruction of its Facility that results from actual or suspected intentional human action." **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.**		
MidAmerican Energy	No	Several modifications need to be made to Table 1 to enhance clarity and delete unnecessary or duplicate items. The stated reliability objective of EOP-004 and the drafting team is to reduce and prevent outages which could lead to cascading through reporting. It is understood that the EOP-004 Attachment 1 is to cover similar items to the DOE OE-417 form. Last, remember that FERC recently asked the question of what standards did not provide system reliability benefits. Those reports that cannot show a direct threat to a potential cascade need to be eliminated. Table 1 should always align with the cascade risk objectives and OE-417 where possible. Therefore Table 1 should be modified as follows: 1. Completely divorce CIP-008 from EOP-004. Constant changes, the introduction of new players such as DOE and DHS, and repeated congressional bills, make coordination with CIP-008 nearly impossible. Cyber security and operational performance under EOP-004 remain separate and different despite best efforts to combine the two concepts. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we**

Organization	Yes or No	Question 2 Comment
		have remanded the one hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement. 2. Modify R1.2 to state that ERO notification only is required for Table 1. This is similar to the DOE OE-417 notification. Notification of other entities is a best practice, not a mandatory NERC standard. If entities want to notify neighboring entities, they may do so as a best practice guideline. **The SDT has updated R1 based on comments received to read as:** **"R1. Each Responsible Entity shall have an event reporting Operating Plan that includes communication protocol(s) for applicable events listed in, and within the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations based on the event type (e.g. the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, governmental or provincial agencies)."** 3. Better clarity for communicating each of the applicable events listed in the EOP-004 Attachment 1 in accordance with the timeframes specified are needed. MidAmerican suggests a forth column be added to the table to clearly identify who must be notified within the specified time period or at a minimum, that R1.2 be revised to clearly state that only the ERO must be notified to comply with the standard. **The SDT disagrees but believes that per your Operating Plan contained in Requirement R1, an entity could take Attachment 1 and insert another column to assist whoever is designated to report an event within your company. The SDT does not want to be too prescriptive within Attachment 1.** 4. Consolidate OE-417 concepts on physical attack and cyber events by consolidating OE-417 items 1, 2, 9 and 10 to: Verifiable, credible, and malicious physical damage (excluding natural weather events) to a BES generator, line, transformer, or bus that when reported requires an appropriate Reliability Coordinator or Balancing Authority to issue an Energy Emergency Alert Level 2 or higher. The whole attempt to discuss a

Organization	Yes or No	Question 2 Comment
		NERC Facility and avoid adverse reliability impacts overreaches the fundamental principal or reporting for an emergency that could result in a cascade. **The SDT disagrees since the OE-417 (and EAP) does not follow the ANSI process as NERC does in the Standards Development Process.** 5. The wording "affects an IROL (per FAC-014)," is too vague and not measurable. Many facilities could affect an IROL, but fewer facilities if lost would cause an IROL. Change "affects" to "results in" **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed"**

Organization	Yes or No	Question 2 Comment
		Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. 6. Recommend that Adverse Reliability Impact be deleted and be replaced with actual EEA 2 or EEA 3 level events. **The SDT has removed Adverse Reliability Impact based on industry feedback and rewrote the event:** **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are**

Organization	Yes or No	Question 2 Comment
		required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. **The SDT also developed another to read:** **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** 7. The phrase "results from actual or suspected intentional human action" is vague

Organization	Yes or No	Question 2 Comment
		and not measurable. This line item used the term "suspected" which relates to "sabotage". MidAmerican recommends that "Results from actual or suspected intentional human action" be deleted. If not deleted the phrase should be replaced with "Results from verifiable, credible, and malicious human action intended to damage the BES." 8. Delete "Any physical threat..." as vague, and difficult to measure in a "perfect" zero defect audit environment, and as already covered by item 1 above. If not deleted, at a minimum replace "Any physical threat", with "physical attack" as being measureable and consistent with DOE OE-417. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).**

Organization	Yes or No	Question 2 Comment
		The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan. 9. With the use of "i.e." the SDT is mandating that each other entity must be contacted. The NSRF believes that the SDT meant that "e.g." should be used to provide examples. The SDT may wish to add another column to Attachment 1 to provide clarity. **The SDT has made the required change concerning replacing "i.e." with "e.g."** 10. The phrase "or partial loss of monitoring capability" is too vague and should be deleted. In addition, the 30 minute window is too short for EMS and IT staff to effectively be notified and troubleshoot systems before being subjected to a federal law requiring reporting and potential violations. The time frame should be consistent with the EOP-008 standard. If not deleted, replace with "Complete loss of SCADA affecting a BES control center for â‰¥ 60 continuous minutes such that analysis tools of State Estimator and/or Contingency Analysis are rendered inoperable. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event is now written to state:** **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.** 11. Transmission loss should be deleted. The number of transmission elements out does not directly correlate to BES stability and cascading. For that reason alone, this

Organization	Yes or No	Question 2 Comment
		item should be deleted or it would have already been included in the past EOP-004 standard. In addition, large footprints can have multiple storms or weather events resulting in normal system outages. This should not be a reportable event that deals with potential cascading. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** 12. Modify the threshold of "BES emergency requiring a public appeal..." to include, "Public appeal for a load reduction event resulting from a RC or BA implementing its emergency energy and capacity plans documented in EOP-001." Public appeals for conservation that aren't used to avoid capacity and energy emergencies should be clearly excluded. **The SDT disagrees as your request makes the event very prescriptive. The threshold is written to state: "Public appeal for load reduction event." The SDT understands that there may be several reports of a single event and as the SDT has stated before, that this will give the ERO a better understanding of the depth and breathe of system conditions based on the given event.** 13. Add a time threshold to complete loss of off-site power to a nuclear plant. Nuclear plants are to have backup diesel generation that last for a minimum amount of time. A threshold recognizing this 4 hour or longer window needs to be added such as complete loss of off-site power to a nuclear plant for more than 4 hours. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT**

Organization	Yes or No	Question 2 Comment
		removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Complete loss of off-site power affecting a nuclear generating station per the Nuclear Plant Interface Requirement."** **As stated in this event Threshold, the TOP's NIPR may have additional guidance concerning the complete loss of offsite power affecting a nuclear plant.** Also see the NSRF comments. **Please review the responses to that commenter.**
Response: The SDT thanks you for your comment.		
Illinois Municipal Electric Agency	No	Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Response: The SDT thanks you for your comment. Please review the responses to that commenter.		
Amercican Transmission Company, LLC	No	ATC is proposing changes to the following Events in Attachment 1: (Reference Clean Copy of the Standard) 1) Pg. 18/ Event: Any Physical threat that could impact the operability of a Facility. ATC is proposing a language change to the Threshold- "Meets Registered Entities criteria stated in its Event Reporting Operating Plan, in addition to excluding weather." **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry**

Organization	Yes or No	Question 2 Comment
		comments to state: **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** 2) Pg. 19 / Event: Voltage deviation on a Facility. ATC believes that the term "observes" for Entity with Reporting Responsibility be changed back to "experiences" as originally written. The burden should rest with the initiating entity in consistency with other Reporting Responsibilities. Also, for Threshold for Reporting, ATC believes the language should be expanded to - plus or minus 10% "of target voltage" for greater than or equal to 15 continuous minutes. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and**

Organization	Yes or No	Question 2 Comment
		identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes ."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.** 3) Pg. 19/ Event: Transmission loss. ATC recommends that Threshold for Reporting be changed to read "Unintentional loss of four, or more Transmission Facilities, excluding successful automatic reclosing, within 30 seconds of the first loss experienced and for 30 continuous minutes. Technical justification or Discussion for this recommended change: In the instance of a transformer-line-transformer, scenario commonly found close-in to Generating stations, consisting of 3 defined "facilities", 1 lightning strike can cause automatic unintentional loss by design. Increase the number of facilities to 4.In a normal shoulder season day, an entity may experience the unintentional loss of a 138kv line from storm activity, at point A in the morning, a loss of a 115kv line from a different storm 300 miles from point A in the afternoon, and a loss of 161kv line in the evening 500 miles from point A due to a failed component, if it is an entity of significant size. Propose some type of time constraint. Add time constraint as proposed, 30 seconds, other than automatic reclosing. In the event of dense lightning occurrence, the loss of multiple transmission facilities may occur over several minutes to several hours with no significant detrimental effect to the BES, as load will most certainly be affected (lost due to breaker activity on the much more exposed Distribution system) as well. Any additional loss after 30 seconds must take into account supplemental devices with intentional relay time delays, such as shunt capacitors, reactors, or load tap changers on transformers activating as designed, arresting system decay. In addition, Generator response after this time has significant impact. **The SDT removed all language under "Entity with Reporting Responsibility," with**

Organization	Yes or No	Question 2 Comment
		the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** 4) Pg.20 /Event: Complete or partial loss of monitoring capability. ATC recommends that the term "partial" be deleted from the event description.ATC recommends that the term "partial" be deleted for the Entity with Reporting Responsibility and changed to read: Each RC, BA, and TOP that experiences the complete loss of monitoring capability. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event is now written to state:** **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.**
Response: The SDT thanks you for your comment.		
Alliant Energy	No	In the first Event for twenty four hour reporting, the last item in "Threshold for Reporting" should be revised to "Results from actual or suspected intentional malicious human action." An employee may be performing maintenance and make a mistake, which could impact the BES. In the second Event for twenty four hour reporting the event should be revised to "Any physical attack that could impact the operability of a Facility." Alliant Energy believes this is clearer and easier to measure.

Organization	Yes or No	Question 2 Comment

Response: The SDT thanks you for your comment. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:

"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."

This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).

This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.

The SDT also developed another to read:

"Damage or destruction of its Facility that results from actual or suspected intentional human action."

This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.

This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).

The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the

Organization	Yes or No	Question 2 Comment
situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.		
Consumers Energy	No	The term "Facility" seems to be much more broad and even more vague than the use of BES equipment. We recommend reverting back to use of BES equipment.
Response: The SDT thanks you for your comment. The SDT disagrees since BES is used within the definition of Facility. NERC defines Facility as: "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)."		
Ameren	No	We appreciate the efforts of the SDT and believe this latest Draft is greatly improved over the previous version. However, we propose the following suggestions: (1) The first Event category in Attachment 1 under 24 Hour Reporting is Applicable to GO and GOP entities. Yet the first 2 of 3 Thresholds for Reporting require data that is unobtainable for GO and GOP entities. Specifically, Events that "Affects an IROL (per FAC-014)" and "Results in the need for actions to avoid an Adverse Reliability Impact". We believe these thresholds, and the use of the NERC Glossary term Adverse Reliability Impact, clearly show the SDT's intent to limit reporting only to Events that have a major and significant reliability impact on the BES. GO or GOP does not have access to the wide-area view of the transmission system, making them to make this determination is impossible. As a result, we do not believe GO and GOP entities should have Reporting Responsibility for these types of Events. (2) For GO and GOP entities, the third Threshold is confusing as to which facilities in the plant it would be applicable to; because the definition of "Facility" does not provide a clear guidance in that respect. For example, would a damage to ID fan qualify as a reportable event? **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry**

Organization	Yes or No	Question 2 Comment
		comments to state: "Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency." This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24

Organization	Yes or No	Question 2 Comment
		hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** (3) The second Event category in Attachment 1 under 24 Hour Reporting, "Any physical threat that could impact the operability of a Facility" is wide open to interpretation and thus impracticable to comply with. For example, a simple car accident that threatens any transmission circuit, whether it impacts the BES (as listed in the Threshold for the previous event in the table or any other measure) or not, is reportable. This list could become endless without the events having any substantial impact on the system. To continue this point, the Footnote 1 can also include, among many other examples, the following:(a) A wild fire near a generating plant, (b) Low river levels that might shut down a generating plant, (c) A crane that has partially collapsed near a generator switchyard, (d) Damage to a rail line into a coal plant, and/or (v) low gas pressure that might limit or stop operation of a natural gas generating plant. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT**

Organization	Yes or No	Question 2 Comment
		removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** (4) The category, "Transmission Loss" is a concern also. If the meaning of Transmission Facility is included in the meaning of Facility as described in the event list, it may be acceptable; but, we still have a question how would a loss of a bus and the multiple radial element that may be connected to that bus would be treated? Also, how would a breaker failure affect this type of an event? The loss of a circuit is

Organization	Yes or No	Question 2 Comment
		"intentional" (as opposed to Unintentional as listed in the threshold) for the failure of breaker, how will it be treated in counting three or more? We suggest a clarification for such types of scenarios. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** (5) Requirement R1.: 1.1 includes an exception from compliance with this Standard if there is a Cyber Security Incident according to CIP-008-3. However, note that the CIP-008-3 may not apply to all GO and GOP facilities. While the exception is warranted to eliminate duplicative event reporting plans, the language of this requirement is confusing as it does not clearly provides that message. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have proposed remanding the one hour event back to CIP-008.** (6) The second paragraph in Section C.1.1.2. Includes the phrases "...shall retain the current, document..." and "...the "date change page" from each version..." Is the "document" intended to be the Operating Plan? We do not see a defining reference in the text around this phrase; also, is a "date change page" mandatory for compliance with this Standard? We request additional clarification of wording in the Evidence Retention section of the Standard. (7) Page 19 / Event: Voltage deviation on a Facility: We believe that the term "observes" for Entity with Reporting Responsibility be changed back to "experiences" as originally written. The burden should rest with the initiating entity in consistency with other Reporting Responsibilities. In addition, for Threshold for Reporting, We

Organization	Yes or No	Question 2 Comment
		believe the language should be expanded to - plus or minus 10%"of nominal voltage" for greater than or equal to 15 continuous minutes. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes ."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.** (8) Page 20 /Event: Complete or partial loss of monitoring capability. We suggest to the SDT that the term "partial" be deleted from the event description. (9) We suggest to the SDT that the term "partial" be deleted for the Entity with Reporting Responsibility and changed to read: Each RC, BA, and TOP that experiences the complete loss of monitoring capability. **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event is now written to state:** **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.**
Response: The SDT thanks you for your comment.		
We Energies	No	Submitting reports to the ERO: NERC and all of the Regional Entities are the ERO. If I

Organization	Yes or No	Question 2 Comment
		send a report to any Regional Entity (and not NERC), I have sent it to the ERO. **The SDT would like to point out the FERC has approved NERC to be the ERO. And the NERC has a delegation agreement with each Regional Entities. This Requirement R1 requires you send a report to the ERO (and whoever else the entity wishes to inform per Requirement R1 including the applicable regions if you are so obligated or its' your desire).** Damage or Destruction of a Facility: A DP may not have a Facility by the NERC Glossary definition. All distribution is not a Facility. Did you mean to exclude all distribution? **The SDT agrees that if a DP does not own or operate a Facility then this event would not be applicable to them.** Any Physical threat that could impact the operability of a Facility: An RC does not have Facilities by the NERC Glossary definition. An RC will not have to report this. BES Emergency... Reporting Responsibility: If meeting the Reporting Threshold was due to a directive from the RC, who is the Initiating entity? **The SDT agrees concerning the RC does not own a Facility and has removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or**

Organization	Yes or No	Question 2 Comment
		Suspicious device or activity at a Facility **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** Voltage deviation on a Facility Threshold for Reporting: 10% of what voltage? Nominal, rated, scheduled, design, actual at an instant? **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.**
Response: The SDT thanks you for your comment.		
NextEra Energy Inc	No	As stated in NextEra's past comments, we continue to be concerned that EOP-004-2 does not appropriately address actual sabotage that threatens the Bulk Electric

Organization	Yes or No	Question 2 Comment
		System (BES) versus random acts that are isolated and pose no risk to the BES. Therefore, NextEra repeats a portion of its past comments below in the hope that the next revision of EOP-004-2 will more adequately address NextEra's concerns. Specifically, NextEra's requests that its definition of sabotage set forth below replace Attachment 1's "Damage and Destruction of Equipment" and "Any physical threat that could impact the operability of a Facility." In Order No. 693, FERC stated its interest in NERC revising CIP-001 to better define sabotage and requiring notification to the certain appropriate federal authorities, such as the Department of Homeland Security. FERC Order No. 693 at PP 461, 462, 467, 468, 471. NextEra has provided an approach that accomplishes FERC's objectives and remains within the framework of the drafting team, but also focuses the process of determining and reporting on only those sabotage acts that could affect other BES systems. Today, there are too many events that are being reported as sabotage to all parties in the Interconnection, when in reality these acts have no material affect or potential impact to other BES systems other than the one that experienced it. For example, while the drafting team notes the issue of copper theft is a localized act, there are other localized acts of sabotage that are committed by an individual, and these acts pose little, if any, impact or threat to other BES systems. Reporting sabotage that does not need to be sent to everyone does not add to the security or reliability of the BES. Relatedly, there is a need to clarify some of the current industry confusion on who should (and has the capabilities to) be reporting to a broader audience of entities. Hence, the NextEra approach provides a clear definition of sabotage, as well as the process for determining and reporting sabotage. New Definition for Sabotage. Attempted or Actual Sabotage: an intentional act that attempts to or does destroy or damage BES equipment for the purpose of disrupting the operations of BES equipment, or the BES, and has a potential to materially threaten or impact the reliability of one or more BES systems (i.e., one act of sabotage on BES equipment is only reportable if it is determined to be part of a larger conspiracy to threaten the reliability of the Interconnection or more than one BES system).
Response: The SDT thanks you for your comment. The SDT has stated in our "Consideration of Issues and Directives – March 15,		

Organization	Yes or No	Question 2 Comment
2012" that was posted with the last posting stated: **The SDT has not proposed a definition for inclusion in the NERC Glossary because it is impractical to define every event that should be reported without listing them in the definition. Attachment 1 is the de facto definition of "event". The SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that without the intervention of law enforcement after the fact, it was almost impossible to determine if an act or event was that of sabotage or merely vandalism. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.** **The SDT has discussed this with FERC Staff and we agree that sabotage could be a state of mind; and, therefore, the real issue: Was there an event or not?**		
ISO New England Inc	No	
Response: The SDT thanks you for your participation.		
Nebraska Public Power District	No	1. The following comments are in regard to Attachment 1:A. The row [Event] titled "Damage or destruction of Facility": 1. In column 3 [Threshold for Reporting], the word "Affect" is vague note the following concerns: i. Does "Affect" include a broken crossarm damaged without the Facility relaying out of service. This could be considered to have an "Affect" on the IROL. ii. Would the answer be different if the line relayed out of service and auto-reclosed (short interruption) for the same damaged crossarm? We need clarity from the SDT in order to know when a report is due. 2. For clarification: Who initiates the report when the IROL interfaces spans between multiple entities? We know of an IROL that has no less that four entities that operate Facilities within the interface. Who initiates the report of the IROL is affected? All? **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and**

Organization	Yes or No	Question 2 Comment
		identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: "Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency." This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action."

Organization	Yes or No	Question 2 Comment
		This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** B. The row [Event] titled "Any physical threat that could impact the operability of a Facility":1. In Column 1 [Event] change the word "threat" to "attack", this aligns with the OE-417 report.2. In Column 3 [Threshold for Reporting], align the threshold with the OE-417 form. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility**

Organization	Yes or No	Question 2 Comment
		Or **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** C. The row [Event] titled "Transmission loss", in column 3 [Threshold for Reporting], the defined term "Transmission Facilities" is too vague. There needs to be a more description such that an entity clearly understands when an event is reportable and for what equipment. We would recommend the definition used in the Event Reporting Field Trial: An unexpected outage, contrary to design, of three or more BES elements caused by a common disturbance. Excluding successful automatic reclosing. For example: a. The loss of a combination of NERC-defined Facilities. b. The loss of an entire generation station of three or more generators (aggregate generation of 500 MW to 1,999 MW); combined cycle units are represented as one unit. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry**

Organization	Yes or No	Question 2 Comment
		comments to state: **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** D. The row [Event] titled "Complete or partial loss of monitoring": 1. In column 1 [Event], delete the words "or partial". This is subjective without definition, delete. 2. Also in column 1 [Event], delete the word "monitoring" and replace with Supervisory Control and Data Acquisition (SCADA). SCADA is defined term that explicitly calls out in the definition "monitoring and control" and is understood by the industry as such. 3. In column 2 [Entity with Reporting Responsibility], delete the words "or partial"; also delete the word "monitoring" and replace with SCADA. 4. In column 3 [Threshold for Reporting], reword to state "Complete loss of SCADA affecting a BES control center for >/= 30 continuous minutes". **The SDT reviewed, discussed and updated Attachment 1 based on comments received, FERC directives and what is required for combining CIP-001 and EOP-004 into EOP-004-2. This event is now written to state:** **"Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (State Estimator, Contingency Analysis) is rendered inoperable." This will only apply to an RC, BA, or TOP who have this capability to start with.**
Response: The SDT thanks you for your comment.		
GTC	No	Page 17 & 18, One Hour Reporting and Twenty-four Hour Reporting: append the introductory statements with the following: "meeting the threshold for reporting" after recognition of the event. Example: Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within twenty-four hours of recognition of the event meeting the threshold for reporting. Page 19, system separation (islanding); Clarify the intent of this threshold for reporting: Load >= 100 MW and any generation; or Load >= 100 MW and Generation

Organization	Yes or No	Question 2 Comment
		>= 100 MW, or some combination of load and generation totaling 100 MW.
Response: The SDT thanks you for your comment. The SDT has chosen not add the requested language as we believe the intent is understood that the time frames means from "meeting the threshold for reporting." The SDT has revised the language regarding islanding and we believe it addresses your concern.		
Indiana Municipal Power Agency	No	The event "any physical threat that could impact the operability of a Facility" is not measurable and can be interpreted many ways by entities or auditors. IMPA recommend incorporating language that let's this be the judgment of the registered entity only. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or**

Organization	Yes or No	Question 2 Comment
		activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility. On the "voltage deviation on a Facility", IMPA recommends that only the TOP the experiences a voltage deviation be the one responsible for reporting. **The SDT has made this change per comments received from the industry.** For generation loss and transmission loss, IMPA believes that the amount of loss needs to be associated with a time period or event (concurrent forced outages).
Response: The SDT thanks you for your comment.		
Idaho Power Co.	No	I think that the category "Damage or destruction of a Facility" is too ambiguous, and the Threshold for Reporting criteria does not help to clarify the question. Any loss of a facility may result in the need for actions to get to the new operating point, would this be a reportable disturbance? **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."**

Organization	Yes or No	Question 2 Comment
		This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).

Organization	Yes or No	Question 2 Comment
		The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.
Response: The SDT thanks you for your comment.		
MISO	No	
American Public Power Association	No	APPA in our comments on the previous draft of EOP-004-2 requested relief for small entities from this reporting/documentation standard. APPA suggested setting a 300 MW threshold for some of the criteria in Attachment 1. This suggestion was not accepted by the SDT. However, the SDT is still directed by FERC to "consider whether separate, less burdensome requirements for smaller entities may be appropriate. Therefore, APPA requests that the SDT provide relief to small entities by providing separate requirements for small entities by requiring reporting only when one of the four criteria in DOE-OE-417 are met: 1. Actual physical attack, 2. Actual cyber attack, 3. Complete operational failure, or 4. Electrical System Separation. APPA recommends this information should be reported to the small entity's BA as allowed in the DOE-OE-417 joint filling process.
Response: The SDT thanks you for your comment. The SDT has taken your concerns into consideration (as directed by FERC) and believes that "small entities" will most likely not meet the thresholds for reporting since items are predicated on "Facilities" or they don't meet the Threshold for reporting.		
Brazos Electric Power Cooperative	No	Please see the comments submitted by ACES Power Marketing.

Organization	Yes or No	Question 2 Comment
Response: The SDT thanks you for your comment. Please review the response to those comments.		
Puget Sound Energy, Inc.	No	The Note at the beginning of Attachment 1 references notifying parties per Requirement R1; however, notification occurs in conjunction with Requirement R2.The term "Adverse Reliability Impact" is used in the threshold section of the event "Damage or destruction of a Facility". At this time, there are two definitions for that term in the NERC Glossary. The FERC-approved definition for this term is "The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection." If the drafting team instead means to use the definition that NERC approved on 8/4/2011 (as seems likely, since that definition more closely aligns with the severity level indicated by the other two threshold statements) then the definition should be included in the Implementation Plan as a prerequisite approval. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could**

Organization	Yes or No	Question 2 Comment
		adversely affect the reliability of the Bulk Electric System). **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** In addition, would the threshold of "Results from actual or suspected intentional human action" include results from actual intentional human action which produced an accidental result, meaning, someone was intentionally doing some authorized action but unintentionally made a mistake, leading to damage of a facility? The event "Any physical threat that could impact the operability of a Facility" will require reporting for many events that have little or no significance to reliable operation of the Bulk Electric System. For example, a balloon lodged in a 115 kV transmission line is a "physical threat" that could definitely "impact the operability" of that Facility and, yet, will probably have little reliability impact. So, too, could a car-pole accident that causes a pole to lean, a leaning tree, or an unfortunately-located bird's nest. The drafting team should develop appropriate threshold language so that reporting is required only for events that do threaten the reliability of the Bulk Electric System. **The SDT also developed another to read:** **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per**

Organization	Yes or No	Question 2 Comment
		Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** With respect to the event "Unplanned control center evacuation", the standard drafting team should include the term "complete" in the description and/or threshold statement to avoid having partial evacuations trigger the need to report. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unplanned evacuation from BES control center facility for 30 continuous minutes or more." The SDT does not believe the word "complete" needs to be added.**
Response: The SDT thanks you for your comment.		
Central Lincoln	No	1) We appreciate the changes made to reduce the short time reporting requirements.

Organization	Yes or No	Question 2 Comment
		The SDT has removed the one-hour reporting time frame, and all events are to be reported within 24 hours of recognition of the event. 2) We would like to point out that the 24 hour reporting threshold for "Damage or destruction of a Facility" resulting from intentional human action will still be non-proportional BES risk for certain events. The discovery of a gunshot 115 kV insulator will start the 24 hour clock running, no matter how busy the discoverer is performing restoration or other duties that are more important. The damage may have been done a year earlier, but upon discovery the report suddenly becomes the priority task. To hit the insulator, the shooter likely had to take aim and pull the trigger, so intent is at least suspected if not actual. And the voltage level ensures the insulator is part of a Facility. **The SDT has updated Damage or destruction of a facility into 2 different thresholds:** **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).**

Organization	Yes or No	Question 2 Comment
		This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s). The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could

Organization	Yes or No	Question 2 Comment
		further define what a suspected intentional human action is within their Operating Plan. 3) We also note that the theft of in service copper is not a physical threat, it is actual damage. The reference to Footnote 1 should be relocated or copied to the cell above the one it resides in now. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** 4) We support the APPA comments regarding small entities. **The SDT has taken your concerns into consideration (as directed by FERC) and believes that "small entities" will most likely not meet the thresholds for reporting**

Organization	Yes or No	Question 2 Comment
		since items are predicated on "Facilities."
Response: The SDT thanks you for your comment.		
Los Angeles Department of Water and Power	No	LADWP has the following comments:#1 - "Any physical threat that could impact the operability of a Facility" is still vague and "operability" is too low a threshold. There needs to be a potential impact to BES reliability. **The SDT has updated Damage or destruction of a facility into 2 different thresholds:** **The SDT removed all language under "Entity with Reporting Responsibility" with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed"**

Organization	Yes or No	Question 2 Comment
		Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. **The SDT also developed another to read:** **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** #2 - "Voltage Deviation on a Facility" I think the threshold definition needs to be more specific: Is it 10% from nominal? 10% from normal min/max operating

Organization	Yes or No	Question 2 Comment
		tables/schedules? Another entities 10% might be different than mine. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes ."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.** #3 - "Transmission Loss" The threshold of three facilities is still too vague. A generator and a transformer and a gen-tie are likely to have overlapping zones of protection that could routinely take out all three. The prospect of penalties would likely cause unneeded reporting. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."**
Response: The SDT thanks you for your comment.		
Deseret Power	No	The threshold for reporting is way too low. A gun shot insulator is not an act of

Organization	Yes or No	Question 2 Comment
		terrorism... vandalism yes... and a car hit pole would be reportable on a 138 kv line. these seem to be too aggressive in reporting.
Response: The SDT thanks you for your comment. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.**		
Kansas City Power & Light	No	For the event, "Damage or destruction of a Facility", the "Threshold for reporting" includes "Results from actual or suspected intentional human action". This is too broad and could include events such as damage to equipment resulting from stealing cooper or wire which has no intentional motivation to disrupt the reliability of the bulk electric system. Reports of this type to law enforcement and governmental agencies will quickly appear as noise and begin to be treated as noise. This may result in overlooking a report that deserves attention. Recommend the drafting team consider making this threshold conditional on the judgment by the entity on the

Organization	Yes or No	Question 2 Comment
		human action intended to be a potential threat to the reliability of the bulk electric system. For the event, "Any physical threat that could impact the operability of a Facility", the same comment as above applies. The footnote states to include copper theft if the Facility operation is impacted. Again, it is recommended to make a report of this nature conditional on the judgment of the entity on the intent to be a potential threat to the reliability of the bulk electric system.

Response: The SDT thanks you for your comment. The SDT has updated Damage or destruction of a facility into 2 different thresholds:

The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:

"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."

This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).

This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each

Organization	Yes or No	Question 2 Comment
interconnection. **The SDT also developed another to read:** **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.**		
Dominion	Yes	Comments: While Dominion agrees that the revisions are a much appreciated improvement, we are concerned that Attachment 1 does not explicitly contain the 'entities which must be, at a minimum, notified. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified.** Attachment 2 appears to indicate that only the ERO and the Reliability Coordinator for the Entity with Reporting Responsibility need be informed. However, the background section indicates that the Entity with Reporting Responsibility is also

Organization	Yes or No	Question 2 Comment
		expected to contact local law enforcement. We therefore suggest that Attachment 2 be modified to include local law enforcement. **The SDT has adapted the language in Attachment 2 along the lines of your concern.** Page 26 redline; Attachment 1; Event - Damage or destruction of a Facility; Threshold for Reporting - Results from actual or suspected intentional human action; Dominion is concerned with the ambiguity that this could be interpreted as applying to distribution. Page 27 redline; Attachment 1; Event - Any physical threat that could impact the operability of a Facility; Dominion is concerned the word "could" is hypothetical and therefore unverifiable and un-auditable. **The SDT has updated Damage or destruction of a facility into 2 different thresholds:** **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).**

Organization	Yes or No	Question 2 Comment
		This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s). The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within

Organization	Yes or No	Question 2 Comment
		their Operating Plan. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** The SDT could provide a list of hypothetical "could impact" events, as well as a specific definition and method for determining a specific physical impact threshold for "could impact" events other than "any."

Organization	Yes or No	Question 2 Comment
		The SDT cannot provide a list of hypothetical events, but will remind the entity that the Operating Plan that is required per Requirement R1 could contain a basis to report concerning your unique system equipment or configuration of your system.
Response: The SDT thanks you for your comment.		
Seattle City Light	Yes	This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
Response: The SDT thanks you for your comment. Please review the response to Question 4.		
Avista	Yes	In general the SDT has made significant improvements to Attachment 1. Avista does have a suggestion to further improve Attachment 1.In Attachment 1 under the 24 hour Reporting Matrix, the second event states "Any physical threat that could impact the operability of a Facility" and the Threshold for Reporting states "Threat to a Facility excluding weather related threats". This is extremely open ended. We suggest adding the following language to the Threshold for Reporting for Any Physical Threat: Threat to a facility that: Could affect an IROL (per FAC-014) OR Could result in the need for actions to avoid and Adverse Reliability Impact This new language would be consistent with the reporting threshold for a Damage event.
Response: The SDT thanks you for your comment. The SDT has updated Damage or destruction of a facility into 2 different thresholds: **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator**		

Organization	Yes or No	Question 2 Comment
Area that results in the need for actions to avoid a BES Emergency." This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s). The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT		

Organization	Yes or No	Question 2 Comment
envisions that entities could further define what a suspected intentional human action is within their Operating Plan.		
PNGC Comment Group	Yes	We agree with reservations. Our comments are below and we are seeking clarification of the Applicability section of the standard. We are voting "no" but if slight changes are made to the applicability section we will change our votes to "yes". NERC and FERC have expressed a willingness to address the compliance burden on smaller entities that pose minimal risk to the Bulk Electric System. The PNGC Comment Group understands the SDT's intent to categorize reportable events and achieve an Adequate Level of Reliability while also understanding the costs associated. Given the changes made by the SDT to Attachment 1, we believe you have gone a long way in alleviating the potential for needless reporting from small entities that does not support reliability. **The SDT has taken your concerns into consideration (as directed by FERC) and believes that "small entities" will most likely not meet the thresholds for reporting since items are predicated on "Facilities."** One remaining concern we have are potential reporting requirements in the Event types; "Damage or destruction of a Facility" and "Any physical threat that could impact the operability of a Facility". These two event types have the following threshold language; "Results from actual or suspected intentional human action" and "Threat to a Facility excluding weather related threats" respectively. We believe these two thresholds could lead to very small entities filing reports for events that really are not a threat to the BES or Reliability. **The SDT has updated Damage or destruction of a facility into 2 different thresholds:** **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:**

Organization	Yes or No	Question 2 Comment
		"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency." This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or

Organization	Yes or No	Question 2 Comment
		destroyed" intentionally by a human. **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** Note: For vandalism, sabotage or suspected terrorism, even the smallest entities will file a police report and at that point local law enforcement will follow their terrorism reporting procedures if necessary, as you've rightly indicated in your "Law Enforcement Reporting" section. We believe extraneous reporting could be alleviated with a small tweak to the Applicability section for 4.1.9 to exclude the smallest Distribution Providers. As stated before, even if these very small entities are excluded from filing reports under EOP-004-2, threats to Facilities that they may have will still be reported to local law enforcement while not cluttering up the NERC/DOE reporting process for real threats to the BES. Our suggested change:4.1.9. Distribution Provider: with peak load >= 200 MWs. The PNGC Comment Group arrived at the 200 MWs threshold after reviewing Attachment 1, Event "Loss of firm load for >= 15 Minutes". We agree with the SDT's intent to exclude these small firm load losses from reporting through EOP-004-2.Another approach we could support is that taken by the Project 2008-06 SDT with respect to Distribution Provider Facilities:4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

Organization	Yes or No	Question 2 Comment
		The SDT has discussed this very issue and would like to point out that the Threshold for Reporting limits are the same as in the enforceable Reliability Standard, EOP-004-1. The SDT believes that small entities (200mw or less) would not be applicable to this event. The SDT has attempted to place these types of limits to reduce small entities from having these applicable reporting requirements. o A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more o A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard o A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard o Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started. We're not advocating this exact language but rather the approach that narrows the focus to what is truly impactful to reliability while minimizing costs and needless compliance burden. One last issue we have is with the language in Attachment 1, Event "BES Emergency resulting in automatic firm load shedding." Under "Entity with Reporting Responsibility", you state that the DP or TOP that "implements" automatic load shedding of >= 100 MWs must report (Also please review the CIP threshold of 300 MWs as this may be a more appropriate threshold). We believe rather than specifying a DP or TOP report, it would be appropriate for the UFLS Program Owner to file the report per EOP-004-2. In our situation we have DPs that own UFLS relays that are part of the TOP's program and this could lead to confusing reporting requirements. Also we don't believe that an entity can "Implement" "Automatic" load shedding but this is purely a semantic issue. **The SDT has updated Damage or destruction of a facility into 2 different thresholds:** **The SDT removed all language under "Entity with Reporting Responsibility" with**

Organization	Yes or No	Question 2 Comment
		the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: "Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency." This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read: "Damage or destruction of its Facility that results from actual or suspected

Organization	Yes or No	Question 2 Comment
		intentional human action." **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.**
Response: The SDT thanks you for your comment.		
United Illuminating Company	Yes	The phrasing of the event labeled as Event Damage or Destruction of a Facility may be improved in the Threshold for Reporting Column. Suggest the introduction sentence for this event should be phrased as Where the Damage or Destruction of a Facility: etc. The rationale for the change is that as written it is unclear if the list that follows is meant to modify the word Facilities or the overall introductory sentence. The confusion being caused by the word That. What is important to be reported is if a Facility is damaged and then an IROL is affected it should be reported, not that if a Facility is comprising an IROL Facility is damaged but there is no impact on the IROL.

Organization	Yes or No	Question 2 Comment
		The SDT has updated Damage or destruction of a facility into 2 different thresholds: The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency. This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT also developed another to read:

Organization	Yes or No	Question 2 Comment
		"Damage or destruction of its Facility that results from actual or suspected intentional human action." **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** Second, the top of each table is the phrase Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the event. This creates the requirement that the actual form is required to be transmitted to parties other than NERC/DOE. The suggested revision is Submit EOP-004 Attachment 2 or DOE-OE-417 report to NERC and/or DOE, and complete notification to other organizations identified pursuant to Requirement R1 Part 1.2 within one hour etc.. **The SDT has revised Attachment 2 heading to read "Use this form to report events. The Electric Reliability Organization will accept the DOE OE-417 form in lieu of this**

Organization	Yes or No	Question 2 Comment
		form if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net voice: 404-446-9780." Based on industry comments.
Response: The SDT thanks you for your comment.		
Ingleside Cogeneration LP	Yes	Ingleside Cogeneration LP agrees with the removal of nearly all one hour reporting requirements. In our view there must be a valid contribution expected of the recipients of any reporting that takes place this early in the process. Any non-essential communications will impede the progress of the front-line personnel attempting to resolve the issue at hand - which has to be the priority. Secondly, there is a risk that early reporting may include some speculation of the cause, which may be found to be incorrect as more information becomes available. Recipients must temper their reactions to account for this uncertainty. In fact, Ingleside Cogeneration LP recommends that the single remaining one-hour reporting scenario be eliminated. It essentially defers the reporting of a cyber security incident to CIP-008 anyways, and may even lead to a multiple violation of both Standards if exceeded.
Response: The SDT thanks you for your comment. The SDT agrees and has removed the one-hour reporting requirement based on comments received.		
Springfield Utility Board	Yes	o Spell out Requirement 1, rather than "parties per R1" in NOTE. o On page 44, "Examples of such events include" should say, "include, but are not limited to". o SUB appreciates clarification regarding events, particularly the discussion regarding "sabotage", and recommends listing and defining "Event" in Definitions and Terms Used in NERC Standards. **The SDT has stated in our "Consideration of Issues and Directives – March 15, 2012" that was posted with the last posting stated:** **The SDT has not proposed a definition for inclusion in the NERC Glossary because it is impractical to define every event that should be reported without listing them in**

Organization	Yes or No	Question 2 Comment
		the definition. Attachment 1 is the de facto definition of "event." The SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that without the intervention of law enforcement after the fact, it was almost impossible to determine if an act or event was that of sabotage or merely vandalism. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The SDT believes that this is an equally effective and efficient means of addressing the FERC Directive. **The SDT has discussed this with FERC Staff and we agree that sabotage could be a state of mind and therefore the real issue was there an event or not.** o The Guideline and Technical Basis provides clarity, and SUB agrees with the removal of "NERC Guideline: Threat and Incident Reporting". o In the flow chart on page 9 there are parallel paths going from "Refer to Ops Plan for Reporting" to the 'Report Event to ERO, Reliability Coordinator' via both the Yes and No response. It seems like the yes/no decision should follow after "Refer to Ops Plan" for communication to law enforcement. **The SDT has offered the flowchart as an example of how an entity could handle the notification to law enforcement agencies. There is no requirement to follow the flowchart. Entities are free to develop their own procedures based upon their needs to report.**
Response: The SDT thanks you for your comment.		
PPL Electric Utilities	Yes	PPL EU thanks the SDT for the changes made in this latest proposal. We feel our prior comments were addressed. Regarding the event 'Transmission Loss': For your consideration, please consider adding a footnote to the event 'Transmission Loss' such that weather events do not need to be reported. Also please consider including 'operation contrary to design' in the threshold language. E.g. consistent with the

Organization	Yes or No	Question 2 Comment
		NERC Event Analysis table, the threshold would be, 'Unintentional loss, contrary to design, of three or more BES Transmission Facilities.'
Response: The SDT thanks you for your comment. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."**		
Tacoma Power	Yes	Tacoma Power supports the revisions. It appears that all agencies and entities are willing to support the use of the DOE Form OE-417 as the initial notification form (although EOP-004 does include their own reporting form as an attachment to the Standard). Tacoma is already using the OE-417 and distributing it to all applicable Entities and Agencies.
Response: The SDT thanks you for your comment.		
Seattle City Light	Yes	This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
Response: The SDT thanks you for your comment. Please review the response to Question 4.		
MEAG Power	Yes	This is a great improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.
Response: The SDT thanks you for your comment. Please review the response to Question 4.		
Public Utility District No. 1 of Snohomish County		This is an excellent improvement over the prior CIP and EOP versions. However, please see #4 for overall comment.

Organization	Yes or No	Question 2 Comment
Response: The SDT thanks you for your comment. Please review the response to Question 4.		
Imperial Irrigation District (IID)	Yes	
Colorado Springs Utilities	Yes	
Arizona Public Service Company	Yes	
Utility Services	Yes	
Dynegy Inc.	Yes	
Manitoba Hydro	Yes	
City of Austin dba Austin Energy	Yes	
Entergy	Yes	
Pepco Holdings Inc	Yes	
Independent Electricity System Operator	Yes	
Cowlitz County PUD	Yes	
Edison Mission Marketing & Trading, Inc.	Yes	
Exelon Corporation and its affiliates	Yes	

Organization	Yes or No	Question 2 Comment
ERCOT	Yes	
Oncor Electric Delivery	Yes	

3. **The SDT has proposed a new Section 812 to be incorporated into the NERC Rules of Procedure. Do you agree with the proposed addition? If not, please explain in the comment area below.**

Summary Consideration: The DSR SDT proposed a revision to the NERC Rules of Procedure (Section 812). The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.

Organization	Yes or No	Question 3 Comment
Northeast Power Coordinating Council	No	The proposed new section does not contain specifics of the proposed system nor the interfacing outside of the system to support the report collecting.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
SPP Standards Review Group	No	We have two concerns about the proposed change to the RoP. One, we have concerns that our information and data will be circulated to an as yet undetermined audience which appears to be solely under NERC's control. Secondly, there isn't sufficient detail in the clearinghouse concept to support comments at this time.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
ISO/RTO Standards Review Committee	No	The SRC offers comments regarding the posted draft requirements; however, by so doing, the SRC does not indicate support of the proposed requirements. Following these comments, please see the latter part of the SRC's response to Question 4 below for an SRC proposed alternative approach: The SRC is unable to comment on the proposed new section as the section does not contain any description of the proposed process or the interface requirements to support the report collecting system. We reserve judgment on this proposal and our right to comment on the

Organization	Yes or No	Question 3 Comment
		proposal when the proposed addition is posted.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
ACES Power Marketing Standards Collaborators	No	(1) It is not clear to us what is the driving the need for the Rules of Procedure proposal. NERC is already collecting event and disturbance reports without memorializing the change in the Rules of Procedure. (2) The language potentially conflicts with other subsections in Section 800. For instance, the proposal says that the system will apply to collect report forms "for this section". This section would refer to Section 800. Section 800 covers NERC alerts and GADS. Electronic GADS (eGADS) already has been established to collect GADS data? Will this section cause NERC to have to incorporate eGADS into this report collection system? Incorporating NERC Alerts is also problematic because when reports are required as a result of a NERC alert, the report must be submitted through the NERC Alert system.(3) The statement that "a system to collect report forms as established for this section or standard" causes additional confusion regarding to which standards it applies. Does it only apply to this new EOP-004-2 or to all standards? If it applies to all standards, does this create a potential issue for CIP-008-3 R1.3 which requires reporting to the ES-ISAC and not this clearinghouse?
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Seattle City Light	No	Seattle City Light follows MEAG and believes this type of activity and process is better suited to NAESBE than it is to NERC Compliance.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Hydro One	No	The proposed new section does not contain specifics of the proposed system nor the

Organization	Yes or No	Question 3 Comment
		interfacing outside of the system to support the report collecting.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
CenterPoint Energy	No	CenterPoint Energy does not agree with the SDT's proposed section 812. The proposal for NERC to establish a system that will "...forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary. This can include state, federal, and provincial organizations." is redundant with the draft Standard. Responsible entities are already required to report applicable events to NERC, applicable regional entities, registered entities, and appropriate governmental, law enforcement, and regulatory agencies. CenterPoint Energy believes if the SDT's intent is to require NERC to distribute these system event reports, then EOP-004-2 should be revised to require responsible entities to only report the event to NERC. As far as distribution to appropriate NERC departments, CenterPoint Energy believes that is an internal NERC matter and does not need to be included in the Rules of Procedure.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Arkansas Electric Cooperative Corporation	No	AECC supports the comments submitted by ACES Power Marketing.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
National Rural Electric Cooperative Association (NRECA)	No	NRECA is concerned with the drafting team's proposal to add a new Section 812 to the NERC ROP. NRECA does not see the need for the drafting team to make such a proposal as it relates to the new EOP-004 that the drafting team is working on. The

Organization	Yes or No	Question 3 Comment
		requirements in the draft standard clearly require what is necessary for this Event Reporting standard. NRECA requests that the drafting team withdraw its proposed ROP Section 812 from consideration. The proposed language is unclear to the point of not being able to understand who is being required to do what. Further, the language is styled in more of a proposal, and not in the style of what would appropriately be included in the NERC ROP. Finally, the SDT has not adequately supported the need for such a modification to the NERC ROP. Without that support, NRECA is not able to agree with the need for this addition to the ROP. Again, NRECA requests that the drafting team withdraw its proposed ROP Section 812 from consideration.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Occidental Power Services, Inc.	No	This section should reference the confidentiality requirements in the ROP and should have a statement about the system for collection and dissemination of disturbance reports being "subject to the confidentiality requirements of the NERC ROP."
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Pepco Holdings Inc	No	This could create confusion.This new ROP section states that "... the system shall then forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary." Standard Section R1.2 states "A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies." If NERC is going to be the "clearinghouse" forwarding reports to the RE and DOE, does that mean that

Organization	Yes or No	Question 3 Comment
		the reporting entity only needs to make a single submission to NERC for distribution? If the reporting entity is required to make all notifications, per R1.2, what is the purpose of NERC's duplication of sending out reports? It would be very helpful to the reporting entities if R1.2 was revised to state that NERC would forward the event form to the RE and DOE and the reporting entity would only be responsible for providing notice verbally to its associated BA, TOP, RC, etc. as appropriate and for notifying appropriate law enforcement as required.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Independent Electricity System Operator	No	We are unable to comment on the proposed new section as the section does not contain any description of the proposed process or the interface requirements to support the report collecting system. We reserve judgment on this proposal and our right to comment on the proposal when the proposed addition is posted.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
MidAmerican Energy	No	See the NSRF comments. The NERC Rules of Procedure Section 807 already addresses the dissemination of Disturbance data, as does Appendix 8 Phase 1 with the activation of NERC's crisis communication plan, and the ESISAC Concept of Operations. The addition of proposed Section 812 is not necessary. The Reliability Coordinator, through the use of the RCIS, would disseminate reliability notifications if it is in turn notified per R1.2. (As stated in the in the Clean copy of EOP-004-2)
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Public Utility District No. 1 of Snohomish County	No	This type of activity and process is better suited to NAESBE than it is to NERC Compliance.

Organization	Yes or No	Question 3 Comment
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Illinois Municipal Electric Agency	No	Illinois Municipal Electric Agency supports comments submitted by ATC.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Amercian Transmission Company, LLC	No	ATC believes that the NERC Rules of Procedure Section 807 already addresses the dissemination of Disturbance data, as does Appendix 8 Phase 1 with the activation of NERC's crisis communication plan, and the ESISAC Concept of Operations. The addition of proposed Section 812 is not necessary. The Reliability Coordinator, through the use of the RCIS, would disseminate reliability notifications if it is in turn notified per R1.2. (As stated in the in the Clean copy of EOP-004-2)
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Ameren	No	If the SDT keeps new Section 812 we suggest to the SDT a wording change for the second sentence, underlined: "Upon receipt of the submitted report, the system shall then forward the report to the appropriate NERC department for review. After review, the report will be forwarded to the applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary."
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
We Energies	No	Section 812 refers to the section as a standard and as a Procedure. That is not correct.Section 812 reads to me as if NERC (the system) will be forwarding everything

Organization	Yes or No	Question 3 Comment
		specified anywhere in RoP 800.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Exelon Corporation and its affiliates	No	While we don't have any immediate objection to revising the Rules of Procedures (ROP) to allow for report collecting under Section 800 relative to the EOP-004 standard, the proposed language is unclear and confusing. Please consider the following revision:"812. NERC Reporting Clearinghouse NERC will establish a system to collect reporting forms as required for Section 800 or per FERC approved standards from any Registered Entities. NERC shall distribute the reports to the appropriate governmental, law enforcement, regulatory agencies as required per Section 800 or the applicable standard."Further, NERC should post ROP revisions along with a discussion justifying the revision for industry comment specific to the ROP. There may be significant implications to this revision beyond the efforts relative to EOP-004.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Tacoma Power	No	Tacoma Power disagrees with the requirement to perform annual testing of each communication plan. We do not see any added value in performing annual testing of each communication plan. There are already other Standard requirements to performing routine testing of communications equipment and emergency communications with other agencies.The "proof of compliance" to the Standard should be in the documentation of the reports filed for any qualifying event, within the specified timelines and logs or phone records that it was communicated per each specified communication plan.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		

Organization	Yes or No	Question 3 Comment
Seattle City Light	No	Seattle City Light follows MEAG and believes this type of activity and process is better suited to NAESBE than it is to NERC Compliance.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
MEAG Power	No	This type of activity and process is better suited to NAESBE than it is to NERC Compliance.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
ERCOT	No	ERCOT has joined the IRC comments on this project.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Idaho Power Co.	No	No opinion
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
MISO	No	MISO agrees with and adopts the Comments of the IRC on this issue.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Brazos Electric Power Cooperative	No	Please see the comments submitted by ACES Power Marketing.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports		

Organization	Yes or No	Question 3 Comment
to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Kansas City Power & Light	No	Rules stipulating the extent of how reported information will be treated by NERC is an important consideration, however, the proposed section 812 proposes to provide reports to other governmental agencies and regulatory bodies beyond that of NERC and FERC. NERC should be treating the event information reported to NERC as confidential and should not take it upon itself to distribute such information beyond the boundaries of the national interest at NERC and FERC.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Dominion	Yes	While Dominion supports this addition, we suggest adding to the sentence "NERC will establish a system to collect report forms as established for this section or reliability standard....."
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
MRO NSRF	Yes	ATC believes that the NERC Rules of Procedure Section 807 already addresses the dissemination of Disturbance data, as does Appendix 8 Phase 1 with the activation of NERC's crisis communication plan, and the ESISAC Concept of Operations. The addition of proposed Section 812 is not necessary. The Reliability Coordinator, through the use of the RCIS, would disseminate reliability notifications if it is in turn notified per R1.2. (As stated in the in the Clean copy of EOP-004-2)
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Ingleside Cogeneration LP	Yes	Ingleside Cogeneration is encouraged by NERC's willingness to act as central data gathering point for event information. However, we see this only as a starting point.

Organization	Yes or No	Question 3 Comment
		There are still multiple internal and external reporting demands that are similar to those captured in EOP-004-2 - examples include the DOE, RAPA (misoperations), EAWG (events analysis), and ES-ISAC (cyber security). Although we appreciate the difference in reporting needs expressed by each of these organizations, there are very powerful reporting applications available which capture a basic set of data and publish them in multiple desirable formats. We ask that NERC spearhead this initiative - as it is a natural part of the ERO function.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
American Electric Power	Yes	While we have no objections at this point, we would like specific details on what our obligations would be as a result of these changes. For example, would the clearinghouse tool provide verifications that the report(s) had been received as well as forwarded? In addition, if DOE OE-417 is the form being submitted, would the NERC Reporting Clearinghouse forward that report to the DOE?
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Springfield Utility Board	Yes	o SUB supports the new Section 812 being incorporated into the NERC ROP. This addition provides clarity for what is required by whom and takes away any possible ambiguity.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
FirstEnergy Corp	Yes	FE agrees but asks that the defined term “registered entities” in the second sentence be capitalized.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports		

Organization	Yes or No	Question 3 Comment
to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
GTC	Yes	With the exception of the RC and company personnel, it appears this proposed section captures the same reporting obligations and to the same entities via R1.2. Recommend adjustments to R1.2 such that reportable events are submitted to NERC, RC, and company personnel.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Central Lincoln	Yes	Thank you for minimizing the number of necessary reports.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Xcel Energy		We believe such a tool would be useful, however we are indifferent as to if it is required to be established by the Rules of Procedure.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
ISO New England Inc		We unable to comment on the proposed new section as the section does not contain any description of the proposed process or the interface requirements to support the report collecting system. We reserve judgment on this proposal and our right to comment on the proposal when the proposed addition is posted.
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
Indiana Municipal Power Agency		no comment

Organization	Yes or No	Question 3 Comment
Los Angeles Department of Water and Power		LADWP does not have a comment on this question at this time
Response: The SDT thanks you for your comment. The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.		
DECo	Yes	
Duke Energy	Yes	
Luminant	Yes	
Bonneville Power Administration	Yes	
Imperial Irrigation District (IID)	Yes	
Florida Municipal Power Agency	Yes	
LG&E and KU Services	Yes	
PPL Corporation NERC Registered Affiliates	Yes	
PNGC Comment Group	Yes	
Colorado Springs Utilities	Yes	
Arizona Public Service Company	Yes	

Organization	Yes or No	Question 3 Comment
Southern Company Services	Yes	
Utility Services	Yes	
Georgia System Operations Corporation	Yes	
Manitoba Hydro	Yes	
Clark Public Utilities	Yes	
New York Power Authority	Yes	
Consolidated Edison Co. of NY, Inc.	Yes	
Orange and Rockland Utilities, Inc.	Yes	
Farmington Electric Utility System	Yes	
Public Service Enterprise Group	Yes	
PPL Electric Utilities	Yes	
Cowlitz County PUD	Yes	
Edison Mission Marketing & Trading, Inc.	Yes	

Organization	Yes or No	Question 3 Comment
American Public Power Association	Yes	
Oncor Electric Delivery	Yes	
Deseret Power	Yes	

4. Do you have any other comment, not expressed in the questions above, for the SDT?

Summary Consideration: The DSR SDT received several suggestions for improvement to the standard. The DSR SDT has removed reporting of Cyber Security Incidents from EOP-004 and have asked the team developing CIP-008-5 to retain this reporting. Most of the language contained in the "Background" Section was moved to the "Guidelines and Technical Basis" Section. Minor language changes were made to the measures and the data retention section. Attachment 2 was revised to list events in the same order in which they appear in Attachment 1.

Organization	Yes or No	Question 4 Comment
Texas Reliability Entity		(1) The ERO and Regional Entities should not be included in the Applicability of this standard. The only justification given for including them was they are required to comply with CIP-008. CIP-008 contains its own reporting requirements, and no additional reliability benefit is provided by including ERO and Regional Entities in EOP-004. Furthermore, stated NERC policy is to avoid writing requirements that apply to the ERO and Regional Entities, and we do not believe there is any sufficient reason to deviate from that policy in this standard. **The SDT is revising the standard to not contain reporting for Cyber Security Incidences. Under the revisions, CIP-008-3 and successive versions will retain the reporting requirements. The Applicability section has been revised to address this situation.** (2) Under Compliance, in section 1.1, all the words in "Compliance Enforcement Authority" should be capitalized. **The SDT agrees and has adopted this suggestion.** (3) Under Evidence Retention, it is not sufficient to retain only the "date change page" from prior versions of the Plan. It is not unduly burdensome for the entity to retain all prior versions of its "event reporting Operating Plan" since the last audit, and it should be required to do so. (What purpose is supposed to be served by

Organization	Yes or No	Question 4 Comment
		retaining only the "date change pages"?) **The SDT has revised the standard to require the retention of previous versions, not just the date change page.** (4) The title of part F, "Interpretations," is incorrect on page 23. Should perhaps be "Associated Documents." **The SDT has revised Part F and it now contains the Guidelines and Technical Basis.**
Response: The SDT thanks you for your comment.		
ACES Power Marketing Standards Collaborators		(1) IC, TSP, TO, GO, and DP should be all removed from the applicability of the standard. Previous versions of the standard did not apply to them and we see no reason to expand applicability to them. IC and TSP are not even mentioned in any of the "Entity with Reporting Responsibility" sections. For the sections that do not mention specific entities, IC and TSP would have no responsibility for any of the events. The TO and GO are not operating entities so the reporting should not apply to them. DP was not included in any previous versions of CIP-001 or EOP-004. Any information (such as load) that was necessary regarding DPs was always gathered by the BA or TOP and included in their reports. There is no indication that this process was not working and, therefore, it should not be changed. Furthermore, including the DP potentially expands the standard outside of the Bulk Electric System which is contrary to recent statements that NERC Legal has made at the April 11 and 12, 2012 SC meeting. Their comments indicated the standards are written for the Bulk Electric System. What information does a DP have to report except load loss which can easily be reported by the BA or TOP? **The SDT disagrees with some of your suggestions. As the standard is to report events associated with physical assets, it is incumbent for the asset owners to file the reports associated with any events. Thus DP, TO, and GO were added to the Applicability of this standard. Their perspectives on events can be useful in evaluating situational awareness and providing NERC with information on lessons learned. Further, this standard limits reporting to BES Elements except where**

Organization	Yes or No	Question 4 Comment
		noted. This is consistent with NERC and SC Standard Process design. Where this standard had included other functional registrations associated with the inclusion of CIP-008; those registrations have been removed from the standard. (2) Measure M2 needs to clarify an attestation is an acceptable form of evidence if there are no events. **Registered Entities must determine how to best demonstrate they have met the performance obligation of a requirement. The use of an attestation statement is already permitted and recognized with the NERC Compliance Program if that is the best means of demonstrating your performance under the requirement. Auditors will then assess whether or not an attestation meets the requirement in one's audit. Attestations cannot be specifically permitted for use.** (3) The rationale box for R3 and R4 should be modified. It in essence states that updating the event reporting Operating Plan and testing it will assure that the BES remains secure. While these requirements might contribute to reliability, these two requirements collectively will not assure BES security and stability. **The SDT has revised the rationale box language based upon the changes it has made to the requirements. It should be noted that upon acceptance of the standard, the language in the rationale boxes are removed from the standard.** (4) We disagree with the VSLs for Requirement R2. While the VSLs associated with late reporting for a 24-hour reporting requirement include four VSLs, the one-hour reporting requirement only includes three VSLs. There seems to be no justification for this inconsistency. Four VSLs should be written for the one-hour reporting requirement. **As the standard has been revised to remove the one-hour reporting provision, your suggestion is moot.** (5) Reporting of reportable Cyber Security Incidents does not appear to be fully coordinated with version 5 of the CIP standards. For instance, EOP-004-2 R1, Part 1.2 requires a process for reporting events to external entities and CIP-008-5 Part 1.5

Organization	Yes or No	Question 4 Comment
		requires identifying external groups to which to communicate Reportable Cyber Security Incidents. Thus, it appears the Cyber Security Incident response plan in CIP-008-5 R1 and the event reporting Operating Plan in EOP-004-2 R1 will compel duplication of external reporting at least in the document of the Operating Plain and Reportable Cyber Security Incident response plan. This needs to be resolved. **While the SDT had worked this through with the other standard team to resolve this concern; it is now irrelevant, as reporting of Cyber Security Incidences are no longer part of EOP-004-2.** (6) In the effective date section of the implementation plan, the statement that the prior version of the standard remains in effect until the new version is accepted by all applicable regulatory authorities is not correct. In areas where regulatory approval is required, it will only remain in effect in the areas where the regulator has not approved it. **The SDT finds that the two statements are making the same point; that the new standard does not become enforceable until all regulatory authorities have approved it.** (7) On page 6 in the background section, the statement attributing RCIS reporting to the TOP standards is not accurate. There is no requirement in the TOP standards to report events across RCIS. In fact, the only mention of RCIS in the standards occurs in EOP-002-3 and COM-001-1.1. **The SDT agrees and adopts your suggestion.** (8) On page 6 in the background section, the first sentence of the third paragraph is not completely aligned with the purpose statement of the standard. The statement in the background section indicates that the reliability objective "is to prevent outages which could lead to Cascading by effectively reporting events". However, the purpose states that the goal is to improve reliability. We think it would make more sense for the reliability objective to match the purpose statement more closely. **The SDT has revised the Background section to match the standard's purpose**

Organization	Yes or No	Question 4 Comment
		statement. (9) On page 7 in the first paragraph, "industry facility" should be changed to "Facility". **The SDT agrees and adopts your suggestion.**
Response: The SDT thanks you for your comment.		
Seattle City Light		1) Seattle City Light follows MEAG and questions if these administrative activities better should be sent over to NAESB? R1: There is merit in having a plan as identified in R1, but is this a need to support reliability or is it a business practice? Should it be in NAESB's domain? R2, R3 & R4: These are not appropriate for a Standard. If you don't annually review the plan, will reliability be reduced and the BES be subject to instability, separation and cascading? If DOE needs a form filled out, fill it out and send it to DOE. NERC doesn't need to pile on. Mike Moon and Jim Merlo have been stressing results and risk based, actual performance based, event analysis, lessons learned and situational awareness. EOP-004 is primarily a business preparedness topic and identifies administrative procedures that belong in the NAESB domain. **The SDT believes this standard is needed to provide Situational Awareness and can help in providing lessons learned to the industry. The SDT has revised the requirements to address this need. While it may be appropriate to have NAESB to adopt this obligation at some in the future, the SDT was charged with addressing deficiencies at this time. The SDT has removed all references to filing reports to DOE from the earlier versions. Today's only reference provides for NERC's acceptance of the use of their form when it is appropriate.** 2) Seattle City Light finds that even though efforts were made to differentiate between sabotage vs. criminal damage, the difference still appears to be confusing. Sabotage clearly requires FBI notification, but criminal damage (i.e. copper theft, trespassing, equipment theft) is best handled by local law agencies. A key point on how to determine the difference is to always go with the evidence. If you have a hole in the fence and cut grounding wires, this would only require local law enforcement

Organization	Yes or No	Question 4 Comment
		notification. If there is a deliberate attack on a utility's BES infrastructure for intent of sabotage and or terrorism--this is a FBI notification event. One area where a potential for confusion arises is with the term "intentional human action" in defining damage. Shooting insulators on a rural transmission tower is not generally sabotage, but removing bolts from the tower may well be. Seattle understands the difficulty in differentiating these two cases, for example, and supports the proposed Standard, but would encourage additional clarification in this one area. **The SDT appreciates the concern you raise. The SDT decided early that trying to set a definition for sabotage across the continent would be impossible as there are many differing viewpoints; particularly within the law enforcement agencies. There was consensus that even if we were able to set a definition, it may be consistent or recognized by other agencies. Therefore, the SDT decided to set event types that warranted reporting. Entities best know who they have to report to and under what considerations those reports need to be submitted. This is basis for this standard. The SDT wanted to provide entities with the result that was necessary but not prescribe how to do it. This concept has been embraced throughout this project. We believe that entities can create a single or multiple contact lists that have the right people being notified when an event type occurs. The SDT has revised the language on "intentional human action" in Attachment 1 in an attempt to provide you the clarification you requested.**
Response: Thank you for your comment.		
Essential Power, LLC		1. As this Standard does not deal with real-time reporting or analysis, and is simply considered an after the fact reporting process, I question the need for the Standard at all. This is a process that could be handled through a change to the Rules of Procedure rather than through a Standard. Developing this process as a Reliability Standard is, in my opinion, contrary to the shift toward Reliability-Based Standards Development.2. I do not believe that establishing a reporting requirement improves the reliability of the BES, as stated in the purpose statement. The reporting requirement, however, would improve situational awareness. I recommend the

Organization	Yes or No	Question 4 Comment
		purpose statement be changed to reflect this, and included with the process in the NERC Rules of Procedure.
Response: The SDT thanks you for your comment. The SDT believes this standard is needed to provide Situational Awareness and can help in providing lessons learned to the industry. The SDT has revised the requirements to address this need. The vast majority of commenters support the Purpose statement as written.		
Georgia System Operations Corporation		a) Reporting most of these items ... o Does not "provide for reliable operation of the BES" o Does not include "requirements for the operation of existing BES facilities" o Is not necessary to "provide for reliable operation of the BES"... and is therefore not in accordance with the statutory and regulatory definitions of a Reliability Standard. They should not be in a Reliability Standard. Most of this is an administrative activity to provide information for NERC to perform some mandated analysis. **The SDT believes this standard is needed to provide Situational Awareness and can help in providing lessons learned to the industry. The SDT has revised the requirements to address this need.** b) A reportable Cyber Security Incident: Delete this item from the table. It is covered in another standard and does not need to be duplicated in another standard. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement.** c) Damage or destruction of a Facility: Entities MAY only need to slightly modify their existing CIP-001 Sabotage Reporting procedures from a compliance perspective of HAVING an Operating Plan but not from a perspective of complying with the Plan. A change from an entity reporting "sabotage" on "its" facilities (especially when the common understanding of CIP-001 is to report sabotage on facilities as "one might consider facilities in everyday discussions") to reporting "damage on its Facilities" (as defined in the Glossary) is a significant change. An operator does not know off the top of his head the definition of Facility or Element. He will not know for any particular electrical device whether or not reporting is required. Although the term is

Organization	Yes or No	Question 4 Comment
		useful for legal and regulatory needs, it is problematic for practical operational needs. This creates the need for a big change in guidance, training, and tools for an operator to know which pieces of equipment this applies to. There is the need to translate from NERC-ese to Operator-ese. Much more time is needed to implement. The third threshold ("Results from actual or suspected intentional human action") perpetuates the problem of knowing the human's intention. Also, what if the action was intended but the result was not intended? The third threshold is ambiguous and subject to interpretation. The original intent of this project was to get away from the problem of the term sabotage due to its ambiguity and subjectivity. This latest change reverses all of the work so far toward that original goal. Instead of the drafted language, change this item to reporting "Damage or destruction of a Facility and any involved human action" and use only the first two threshold criteria. **The SDT has stated in our "Consideration of Issues and Directives – March 15, 2012" that was posted with the last posting stated:** **The SDT has not proposed a definition for inclusion in the NERC Glossary because it is impractical to define every event that should be reported without listing them in the definition. Attachment 1 is the de facto definition of "event." The SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that without the intervention of law enforcement after the fact, it was almost impossible to determine if an act or event was that of sabotage or merely vandalism. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.** **The SDT has discussed this with FERC Staff and we agree that sabotage could be a**

Organization	Yes or No	Question 4 Comment
		state of mind and therefore the real issue was there an event or not. **The SDT also uses the NERC defined term of "Facility: A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)."** d) Any physical threat that could impact the operability of a Facility: See comment above about the term "Facility" and the need for a much longer implementation time. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to**

Organization	Yes or No	Question 4 Comment
		operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility. e) Transmission loss: This item is very unclear. What is meant by "loss?" Above, it says to report damage or destruction of a Facility. This says to report the loss of 3 Facilities. Is the intent here to report when there are 3 or more Facilities that are unintentionally and concurrently out of service for longer than a certain threshold of time? The intent should not be to include equipment failure? Three is very arbitrary. An entity with a very large footprint with a very large number of electrical devices is highly likely to have 3 out of service at one time. An entity with very few electrical devices is less likely to have 3. Delete the word Transmission. It is somewhat redundant. A Facility is BES Element. I believe all BES Elements are Transmission Facilities. A Facility operates as a single "electrical device." What if more than 3 downstream electrical devices are all concurrently out of service due to the failure of one upstream device? Would that meet the criteria? A situation meeting the criteria will be difficult to detect. Need better operator tools, specific procedures for this, training, and more implementation time. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state"** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** f) The implementation plan says current version stays in effect until accepted by ALL regulatory authorities but it also says that the new version takes effect 12 months after the BOT or the APPLICABLE authorities accept it. It is possible that ONE regulatory authority will not accept it for 13 months and both versions will be in

Organization	Yes or No	Question 4 Comment
		effect. It is also possible for ALL regulatory authorities to accept it at the same time, the current version to no longer be in effect, but the new version will not be in effect for 12 months. **The SDT intends for this standard to not become enforceable until all regulatory authorities have approved it. The SDT will work with NERC and others to ensure a timely enforcement period without overlap.**
Response: Thank you for your comment.		
We Energies		Applicability: Change Electric Reliability Organization to NERC or delete Regional Entity. The ERO is NERC and all the Regional Entities.R1.2: The ERO is NERC and all the REs. If I report to any one on the REs (only and not to NERC), I have reported to the ERO. Change ERO to NERC. M1 refers to R1.1 and R1.2 as Parts. It would be clearer to refer to them as requirements or sub-requirements. **The SDT is limited to listing functional registrations in the Applicability section. The applicable entities are the ERO and Regional Entity, not NERC. The SDT notes that the Applicability section has nothing to do with the reporting obligations. The Applicability section denotes who has obligations within the standard to report. The Applicability section has been revised in accordance with comments received on who needs to report on event types.** M2: Add a comma after "that the event was reported" and "supplemented by operator logs". It will be easier to read. **The SDT has revised the requirement and associated language.** R3: This should be clarified to state that no reporting will be done for the annual test, not just exclude the ERO. **The SDT has revised the requirement.** M4: An annual review will not be time stamped. **The SDT has removed the time-stamp provision.**

Organization	Yes or No	Question 4 Comment
Response: The SDT thanks you for your comment.		
City of Austin dba Austin Energy		Austin Energy makes the following comments: (1) Comment on the Background section titled "A Reporting Process Solution - EOP-004": This section includes the sentence, "Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state OR PROVINCIAL OR LOCAL level law enforcement agency." (emphasis added) The corresponding flowchart includes a step, "Notification Protocol to State Agency Law Enforcement." Austin Energy requests that the SDT update the flowchart to match the language of the associated paragraph and include "state or provincial or local" agencies. **The SDT wishes to point out that the flowchart is an example only – it was not meant to show every permutation. The entity can choose to use the flowchart or develop one for their own use.** (2) Comments on VSLs: Austin Energy recommends that the SDT amend the VSLs for R2 to include the "recognition of" events throughout. That is, update the R2 VSLs to state "... X hours after "recognizing" an event ..." in all locations where the phrase occurs. **The DSR SDT believes the current language is sufficient as Table 1 clearly states that the reporting 'clock' starts after recognition of the event.** (3) Austin Energy has a concern with the inclusion of the word "damage" to the phrase "damage or destruction of a Facility." We agree that any "destruction" of a facility that meets any of the three criteria be a reportable event. However, if the Standard is going to include "damage," some objective definition for "damage" (that sets a floor) ought to be included. Much like the copper theft issue, we do not see the benefit of reporting to NERC vandalism that does not rise to a certain threshold (e.g. someone who takes a pot shot at an insulator) unless the damage has some tangible impact on the reliability of the BES or is an act of an orchestrated sabotage (e.g.

Organization	Yes or No	Question 4 Comment
		removal of a bolt in a transmission structure). **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency."** **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** **The SDT removed all language under "Entity with Reporting Responsibility," with**

Organization	Yes or No	Question 4 Comment
		the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Damage or destruction of its Facility that results from actual or suspected intentional human action."** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** (4) Austin Energy voted to approve the revised Standard because it is an improvement over the existing Standard. In light of FERC's comments in Paragraph 81 of the Order approving the Find, Fix, Track and Report initiative, however, Austin Energy would propose that this Standard is the type of Standard that does not truly

Organization	Yes or No	Question 4 Comment
		enhance reliability of the BES and is, instead, an administrative activity. As such, we recommend that NERC consider whether EOP-004-2 ought to be retired. **The SDT appreciates the suggestion; however, we note that a standard cannot be retired prior to its effective and enforcement dates. Further, the SDT has been charged with addressing deficiencies that are present in current standards which the industry has determined to be needed through approval of the SAR. If the P81 process should ultimately decide to retire this standard, then the process will have made that decision. The SDT cannot presume that the P81 effort will become effective.**
Response: The SDT thanks you for your comment.		
Bonneville Power Administration		BPA believes that the VSL should allow for amending the form after a NERC specified time period without penalty and suggests that a window of 48 hours be given to amend the form to make adjustments without needing to file a self report. Should the standard be revised to allow a time period for amending the form without having to file a self report, BPA would change its negative position to affirmative.
Response: The SDT thanks you for your comment. The SDT would like to point that a window is not needed as the standard requires a report at a 24-hour time frame which provides information on what is known at the time. The standard does not require any follow up or update report. If the entity wishes to file a follow up report, it can do so on its own. A self report should only be needed if the 24-hour report was not filed.		
CenterPoint Energy		CenterPoint Energy proposes that the purpose be enhanced to reflect risk and response. For example, the purpose could read "To sustain and improve reliability of the Bulk Electric System by identifying common risks reported by Responsible Entities as a source of lessons learned."In the Background section under Law Enforcement Reporting, "the" should be added in front of "Bulk Electric System". Also under the Background section - "Present expectations of the industry under CIP-001-1a", CenterPoint Energy is not aware of any current annual requirements for CIP-001 and suggests that this section be revised to reflect that fact. CenterPoint Energy strongly

Organization	Yes or No	Question 4 Comment
		believes that the Violation Severity Levels (VSL) should not be high or severe unless an Adverse Reliability Impact occurred. CenterPoint Energy is requesting that Requirement R2 be deleted and the phrase, "as a result of not implementing the plan/insufficient or untimely report, an Adverse Reliability Impact occurred" be added to the Requirement R1 VSL. Regarding the VSL for Requirement R4, the Violation Risk Factor should be "Lower" and read "the entity did not perform the annual test of the operating plan" as annual is to be defined by the entity or according to the CAN-0010.
Response: The SDT thanks you for your comment. The vast majority of commenters support the Purpose statement as written. The missing 'the' has been added to the background section under 'Law Enforcement Reporting.' 'Annual' has been changed to 'These'. VSLs refer to how closely the entity met the requirements of the standard; it is the VRF that measures impact to reliability. The DSR SDT believes use of the high and severe VSLs is appropriate. R4 has been deleted along with its VRF/VSLs.		
Cowlitz County PUD		Cowlitz is pleased with changes made to account for the difficulties small entities have in regard to reporting time frames. Although Cowlitz is confident that the current draft is manageable for small entities, we propose that the resulting reports this Standard will generate will contain many insignificant events from the event types "Damage or destruction of a Facility," and "Any physical threat that could impact the operability of a Facility." In particular, examples would be limited target practice on insulators, car-pole accidents, and accidental contact from tree trimming or construction activities. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Damage or destruction of a Facility within its Reliability Coordinator Area,**

Organization	Yes or No	Question 4 Comment
		Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency." This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human

Organization	Yes or No	Question 4 Comment
		action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.** Cowlitz suggests that at least a >= 100 MW (200 MW would be better) and/or >= N-2 impact threshold be established for these event types. Also, Cowlitz suggests the statement "results from actual or suspected intentional human action" be changed to "results from actual or suspected intentional human action to damage or destroy a Facility." A human action may be intentional which can result in damage to a facility, but the intent may have been of good standing, and not directed at the Facility. For example, the intent may have been to legally harvest a tree, or move equipment under a line. Cowlitz believes the above proposed changes would benefit the ERO, both in reduction of nuisance reports and possible violations over minimal to no impact BES events. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and**

Organization	Yes or No	Question 4 Comment
		identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.**
Response: The SDT thanks you for your comment.		
Colorado Springs Utilities		CSU is concerned with the word 'damage'. We support any 'destruction' of a facility that meets any of the three criteria be a reportable issue, but 'damage', if it's going to be included should have some objective definition that sets a baseline.
Response: The SDT thanks you for your comment. The SDT removed all language under "Entity with Reporting Responsibility,"		

Organization	Yes or No	Question 4 Comment
with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: "Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency." This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System). This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state: "Damage or destruction of its Facility that results from actual or suspected intentional human action." This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1)		

Organization	Yes or No	Question 4 Comment
the situational awareness that the Facility was "damaged or destroyed" intentionally by a human. **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.**		
Dominion		Dominion believes that the reporting of "Any physical threat that could impact the operability of a Facility4" may overwhelm the Reliability Coordinator staff with little to no value since the event may have already passed. This specific event uses the phrase "operability of a Facility" yet "operability" is not defined and is therefore ambiguous. We do support the reporting to law enforcement and the ERO but do not generally support reporting events that have passed to the Reliability Coordinator. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility**

Organization	Yes or No	Question 4 Comment
		Do not report copper theft unless it degrades normal operations of a Facility." **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** Attachment 2; section 4 Event Identification and Description: The type of events listed should match the events as they are exactly written in Attachment 1. As it is currently written, it leaves room for ambiguity. **The SDT agrees and has adopted your suggestion.** M3 - Dominion objects to having to provide additional supplemental evidence (i.e. operator logs), and the SDT maybe want to include a requirement for NERC to provide a confirmation that the report has been received. **The SDT believes that you are referring to M2. We have added "which may be" prior to "supplemented by operator logs," indicating that this is optional. The SDT has opted not to develop a requirement for the ERO to provide receipt conformation of a report.**
Response: The SDT thanks you for your comment.		
Entergy		Entergy does not agree with the Time Horizon for R2. The rationale for R2 contains phrases related to situational awareness and keeping people/agencies aware of the "current situation." However, this standard is related to after the fact event reporting, not real-time reporting via RCIS, as discussed on page 6 of the red-lined standard. Therefore the time horizon for R2 should indicate that this is an after the

Organization	Yes or No	Question 4 Comment
		fact requirement expected to be performed either in 1 hour or 24 hours after an event occurs, not in the operations assessment time frame. This change should also be made on page 15 of the redline in the Table of compliance elements for R2. Page 18 of the redline document contains a VSL for R2 which states that it will be considered a violation if the Responsible Entity submitted a report in the appropriate timeframe but failed to provide all of the required information. It has long been the practice to submit an initial report and provide additional information as it becomes available. On page 24 of the redlined document, this is included in the following "...and provide as much information as is available at the time of the notification to the ERO..." But the compliance elements table now imposes that if the entity fails to provide ALL required information at the time the initial report is required, the entity will be non compliant with the standard. This imposes an unreasonable burden to the Reliability Entity. This language should be removed. The compliance element table for R3 and R4 make it a high or severe violation to be late on either the annual test or the annual review of the Operating plan for communication. While Entergy supports that periodically verifying the information in the plan and having a test of the operating plan have value, it does not necessarily impose additional risk to the BES to have a plan that exceeds its testing or review period by two to three months. This is an administrative requirement and the failure to test or review should be a lower or moderate VSL, which would be consistent with the actual risk imposed by a late test or review. On page 24 of the redlined draft, there is a statement that says "In such cases, the affected Responsible Entity shall notify parties per Requirement R1 and provide as much information as if available at the time of the notification..." Since R1 is the requirement to have a plan, and R2 is the requirement to implement the plan for applicable events, it seems that the reference in this section should be to Requirement R2, not Requirement R1.
Response: The SDT thanks you for your comment. There is no longer a requirement for this 'two-step' reporting. The initial report is the only report an entity must make. The note at the top of Attachment 1 is to give entities the flexibility to make a quick 'something big just happened, but I don't know the extent' phone call, but realistically the reporting time frame is 24 hours which should give ample time to make one written report using OE-417 or Attachment 2. You will also notice that the amount of		

Organization	Yes or No	Question 4 Comment
information you must provide is minimal – the idea is that this is a trigger for NERC or the Event Analysis process and they will contact you if further details are required. **VSLs refer to how closely the entity met the requirements of the standard; it is the VRF that measures impact to reliability. The DSRSDT believes use of the high and severe VSLs is appropriate. Also, R4 has been deleted along with its VRF/VSLs.**		
ERCOT		ERCOT has joined the IRC comments on this project and offers these additional comments. ERCOT supports the alternative approach submitted by the IRC. ERCOT requests that time horizons be added for each of the requirements as have been with other recent Reliability Standards projects. With regards to Attachment 1, ERCOT requests the following changes: o Modify "Generation loss" from "â‰¥ 1,000 MW for entities in the ERCOT or Quebec Interconnection" to "â‰¥ 1,100 MW for entities in the ERCOT Interconnection" and "â‰¥ 1,000 MW for entities in the Quebec Interconnection". This is consistent with the DCS threshold and eliminates possible operator confusion since DCSs event are reported in the ERCOT interconnection at 80% of single largest contingency which equates to 1100 MW. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."** **The NERC SPM does allow TRE to apply for a variance if they have special concerns that GOPs should submit a report to the ERO.**

Organization	Yes or No	Question 4 Comment
		o Modify "Transmission loss" from "Unintentional loss of three or more Transmission Facilities (excluding successful automatic reclosing)" to "Inconsequential loss of three or more Transmission Facilities not part of a single rated transmission path (excluding successful automatic reclosing)." If a single line is comprised of 3 or more sections, this should not be part of what is reported here as it is intended to be when you have a single event trip of 3 or more transmission facilities that is not part of its intended design. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing)."** **The NERC SPM does allow TRE to apply for a variance if they have special concerns that GOPs should submit a report to the ERO.** o ERCOT requests review of footnote 1. The footnote does not seem appropriate in including an example of a control center as the definition of a BES facility does not include control centers. **The SDT removed all foot notes within Attachment based on comments received.**
Response: The SDT thanks you for your comment.		
FirstEnergy Corp		FE supports the standard and has the following additional comments and suggestions:1. Guideline/Technical Basis Section - FE requests the SDT add specific guidance for each requirement. Much of the information in this section is either included, or should be included in the Background section of the standard. One example of guidance that would help is for Requirement R3 on how an entity could

Organization	Yes or No	Question 4 Comment
		perform the annual test. The comment form for this posting has the following paragraph on pg. 2 which could be used as guidance for R3: "the annual test will include verification that communication information contained in the Operating Plan is correct. As an example, the annual update of the Operating Plan could include calling "others as defined in the Responsibility Entity's Operating Plan" (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. Note that there is no requirement to test the reporting of events to the Electric Reliability Organization and the Responsible Entity's Reliability Coordinator."2. With regard to the statement in the comment form (pg 2 paragraph 7)"Note that there is no requirement to test the reporting of events to the Electric Reliability Organization and the Responsible Entity's Reliability Coordinator.", requirement R3 only includes the ERO as an entity and should also include the Reliability Coordinator. 3. The measure M3 says that an entity can use an actual event as a test to meet R3. Does this mean just 1 actual event will meet R3, or is the intent that all possible events per 1.2 are tested? Would like some clarity on this measure.
Response: The SDT thanks you for your comment. The requirements have been revised and these revisions along with the 'Rationale' boxes should provide the clarity you seek.		
Indiana Municipal Power Agency		For 1.2 under R1, is the SDT leaving it up to the registered entities do decide which organizations will be contacted for each event listed in attachment 1 or do all of those organization need to be contacted for each event listed in attachment 1? The requirement needs to clearly communicate this clarification and be independent of the rationale language. Auditors will go by the requirement and not the rationale for the requirement. For 1.1 under R1, does each event need its own process of recognition or can one process be used to cover all the applicable events? The requirement needs to clearly communicate this clarification and be independent of the rationale language. Auditors will go by the requirement and not the rationale for the requirement. For 1.2 under R1, company personnel is used as an example but in the rationale for R1, the third line uses operating personnel. IMPA recommends

Organization	Yes or No	Question 4 Comment
		changing the example in 1.2 to operating personnel which is used in the current version of CIP-001.
Response: The SDT thanks you for your comment. The SDT does not believe that it has the ability (or desire) to programmatically prescribe whether entities have a single or multiple contact lists. Entities themselves know best who and under what conditions do reports need to be provided. Further, the industry in past comment periods, clearly indicated that they did not wish to have the SDT provide the "how."		
GTC		For R2, please clarify how an entity can demonstrate that no reportable events were experienced. GTC recommends an allowance for a letter of attestation within M2.
Response: Thank you for your comment. Registered Entities must determine how to best demonstrate they have met the performance obligation of a requirement. The use of an attestation statement is already permitted and recognized with the NERC Compliance Program if that is the best means of demonstrating your performance under the requirement. Auditors will then assess whether or not an attestation meets the requirement in one's audit. Attestations cannot be specifically permitted for use.		
Orange and Rockland Utilities, Inc.		Form EOP-004, Attachment 2: Event Reporting Form: Delete the Task words "or partial." Delete the Task words "physical threat that could impact the operability of a Facility." Make any changes to the VSL's necessary to align them with the reviewed wording provided above.
Consolidated Edison Co. of NY, Inc.		Form EOP-004, Attachment 2: Event Reporting Form: Delete the Task words "or partial." Delete the Task words "physical threat that could impact the operability of a Facility." Make any changes to the VSL's necessary to align them with the reviewed wording provided above.
Response: The SDT thanks you for your comment. The SDT has updated Attachment 2 to reflect the events listed in Attachment 1.		
NextEra Energy Inc		Given that Responsible Entities are already required by other Reliability Standards to communicate threats to reliability to their Reliability Coordinator (RC), NextEra does not believe that EOP-004-2 is a Reliability Standard that promotes the reliability of the bulk power system, as envisioned by Section 215 of the Federal Power Act.

Organization	Yes or No	Question 4 Comment
		Because an RC reporting requirement is already covered in other Standards, EOP-004-2 essentially is a reporting out requirement to the Regional Reliability Organization (RRO). NextEra does not agree that the reporting of events to the RROs should be subject to fines under the Reliability Standard regulatory framework. The reporting to RROs, as required by EOP-004-2, while informative and helpful for lessons learned, etc., is not necessary to address an immediate threat to reliability. In addition, NextEra does not believe it would be constructive to fine Responsible Entities for failure to report to a RRO within a mandated deadline during times when these entities are attempting to address potential sabotage on their system. NextEra would, therefore, prefer that the EOP-004-2 Standards Drafting Team be disbanded, and instead that EOP-004-2's reporting requirements be folded in to the event analysis reporting requirements. Therefore, NextEra requests that the new Section 812 be revised to include EOP-004-2 as a data request for lessons learn or for informational purposes only, and, also, for EOP-004-2 project to be disbanded.
Response: The SDT thanks you for your comment. While the SDT appreciates your viewpoint, the SDT has been charged with addressing deficiencies identified in current standards. The SDT believes that the standard will provide NERC with the situational awareness it needs as well as providing the industry valuable information through lessons learned.		
Illinois Municipal Electric Agency		Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Response: The SDT thanks you for your comment. Please review the response to that commenter.		
Florida Municipal Power Agency		In R1, bullet, it is a bit ambiguous whether the list of organizations to be communicated with is an exhaustive list (i.e.) or a list of examples (e.g.). The list is preceded by an "i.e." which indicates the former, but includes an "or" which indicates the latter. We are interpreting this as meaning the list is exhaustive as separated by semi-colons, but that the last phrase separated by commas is a list of examples. Is this the correct interpretation? **The SDT has made the required change concerning replacing "i.e." with "e.g."**

Organization	Yes or No	Question 4 Comment
		The Rules of Procedure language for data retention (first paragraph of the Evidence Retention section) should not be included in the standard, but instead referred to within the standard (e.g., "Refer to Rules of Procedure, Appendix 4C: Compliance Monitoring and Enforcement Program, Section 3.1.4.2 for more retention requirements") so that changes to the RoP do not necessitate changes to the standard. **The language that you mention is part of the standard boilerplate and is included in all standards. The SDT has chosen to keep the language as is at this time.**
Response: The SDT thanks you for your comment.		
Ingleside Cogeneration LP		Ingleside Cogeneration LP strongyly believes that LSEs that do not own BES assets should be excluded from the Applicability section of this standard.
Response: The SDT thanks you for your comment. The LSE obligation in this standard was tied to applicability in CIP-008 for cyber incident reporting. Reporting under CIP-008 is no longer part of EOP-004-2 so this applicability has been removed.		
Los Angeles Department of Water and Power		LADWP does not have any other comments at this time
Response: The SDT thanks you for your participation.		
Manitoba Hydro		Manitoba Hydro is voting negative on EOP-004-2 for the reasons identified in our response to Question 1. In addition, Manitoba Hydro has the following comments:(Background section) - The section has inconsistent references to EOP-004 (eg. EOP-004 and EOP-004-2 are used). Wording should be made consistent. (Background section) - The section references entities, and responsible entities. Suggest wording is made consistent and changed to Responsible Entities. (General comment) - References in the standard to 'Part 1.2' should be changed to R1.2 as it is unclear if Part 1.2 refers to, for example, R1.2 or part 1.2 'Evidence Retention'.

Organization	Yes or No	Question 4 Comment
		(M4) -Please clarify what is meant by 'date change page'.
Response: The SDT thanks you for your comment. The SDT appreciates the points you raise and we continually review the document to make sure the language is consistent and unambiguous.		
Southern Company Services		Move the Background Section (pages 4-9) to the Guideline and Technical Basis section. They are not needed in the main body of the standard. **The SDT agrees and adopts your suggestion.** Each "Entity with Reporting Responsibility" in the one-hour reporting table (p. 17) should be explicitly listed in the table, not pointed to another variable location. The criterion for "Threshold for Reporting" in the one-hour reporting table (p. 17) should be explicitly listed in the table, not pointed to another variable location. Please specify the voltage base against which the +/- 10% voltage deviation on a Facility is to be measured in the twenty-four hour reporting table (p. 19). **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes ."** **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.**
Response: The SDT thanks you for your comment.		
Oncor Electric Delivery		Oncor takes the position that the proposed objectives as prescribed in Project 2009-01 - Disturbance and Sabotage Reporting, is a "good" step forward. Currently, NERC

Organization	Yes or No	Question 4 Comment
		reporting obligations related to disturbances occurs over multiple standards including CIP-001, EOP-004-1, TOP-007-0, CIP-008-3 and Event Analysis (EA). Oncor is especially pleased that the Event Analysis Working Group (EAWG) is actively working to find ways of streamlining the disturbance reporting process especially to agencies outside of NERC such as FERC, and state agencies. Oncor is in agreement that an addition to the NERC Rules of Procedure in section 800 to develop a Reporting Clearinghouse for disturbance events by the establishment of a system to collect report and then forward completed forms to various requesting agencies, is also a very positive step."
Response: The SDT thanks you for your comment. The SDT would like to point out that the EAP is a voluntary program where the entity analyzes an issue or system condition. EOP-004-2 is a Reporting Standard where an entity informs the ERO (and whoever else per Requirement R1) of a current event. This will give other the situational awareness that their system may be degraded. Please refer to the Southwest Outage Report for more situational awareness issues that failed.		
Occidental Power Services, Inc.		OPSI continues to believe that LSEs that do not own BES assets should be excluded from the Applicability section of this standard. It is disingenuous of both the SDT and FERC to promote an argument to support this inclusion such as that stated in Section 459 of Order 693 (and referred to by the SDT in their Consideration of Comments in the last posting). The fact is that no reportable disturbance can be caused by an "attack" on an LSE that does not own BES assets. The SDT has yet to point out such an event.
Response: The SDT thanks you for your comment. The LSE obligation in this standard was tied to applicability in CIP-008 for cyber incident reporting. Reporting under CIP-008 is no longer part of EOP-004-2 so this applicability has been removed. The SDT notes that LSEs will still be subject to reporting under CIP-008 until such time they are removed from that standard.		
New York Power Authority		Please see comments submitted by NPCC Regional Standards Committee (RSC).
Response: The SDT thanks you for your comment. Please review the response to that commenter.		
MRO NSRF		R1 states: "Each Responsible Entity shall have an event reporting Operating Plan that

Organization	Yes or No	Question 4 Comment
		includes:"The definition of Operating Plan is:"A document that identifies a group of activities that may be used to achieve some goal. An Operating Plan may contain Operating Procedures and Operating Processes. A company-specific system restoration plan that includes an Operating Procedure for black-starting units, Operating Processes for communicating restoration progress with other entities, etc., is an example of an Operating Plan." This appears to us to be too prescriptive and could be interpreted to require a series of documents to for reporting issues to NERC. We suggest the following wording: R1. Each Responsible Entity shall have document methodology(ies) or process(es) for: 1.1. Recognizing each of the applicable events listed in EOP-004 Attachment 1.1.2. Reporting each of the applicable events listed in EOP-004 Attachment 1 in accordance with the time framess specified in EOP-004 Attachment 1 to the Electric Reliability Organization. LES Comment: [R1] We are concerned by the significant amount of detail an entity would be required to contain within the Operating Plan as part of Requirement R1. Rather than specifying an entity must have a documented process for recognizing each of the events listed in EOP-004-2 Attachment 1, at a minimum, consider removing the term "process" in R1.1 and replacing with "guideline" to ensure operating personnel are not forced to adhere to a specific sequence of steps and still have the flexibility to exercise their own judgment. Section 5 of the standard (Background) should be moved to the Guideline and Technical Basis document. A background that long does not belong in the standard piece as it detracts from the intent of the standard itself.
Response: The SDT thanks you for your comment. The background and Guidelines and Technical Basis sections have been combined.		
ReliabilityFirst		ReliabilityFirst votes in the Affirmative for this standard because the standard further enhances reliability by clearing up confusion and ambiguity of reporting events which were previously reported under the EOP-004-1 and CIP-001-1 standards. Even though ReliabilityFirst votes in the Affirmative, we offer the following comments for consideration: 1. Requirement R1, Part 1.2a. ReliabilityFirst recommends further prescribing whom the Responsible Entity needs to communicate with. The phrase "...

Organization	Yes or No	Question 4 Comment
		and other organizations needed for the event type…" in Part 1.2 essentially leaves it up to the Responsible Entity to determine (include in their process) whom they should communicate each applicable event to. ReliabilityFirst recommends added a fourth column under Attachment 1, which lists whom the Responsible Entity is required to communicate with, for each applicable event. 2. VSL for Requirement R2a. Requirement R2 requires the Responsible Entity to "implement its event reporting Operating Plan" and does not require the entity to submit a report. For consistency with the requirement, ReliabilityFirst recommends modifying the VSLs to begin with the following type of language: "The Responsible Entity implemented its event reporting Operating Plan more than 24 hours but…" This recommendation is based on the FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement.
Response: The SDT thanks you for your comment. The SDT believes that implementing your Operating Plan means that you report an event. Therefore the VSLs are entirely consistent with the requirement.		
DECo		Requirement R3 for annual test specifically states that ERO is not included during test. Implies that local law enforcement or state law enforcement will be included in test. Hard to coordinate with many Local organizations in our area.
Response: The SDT thanks you for your comment. The SDT has revised the language in Requirement R3 and believes that the changes will address your suggestion.		
Alliant Energy		Section 5 of the standard (Background) should be moved to the Guideline and Technical Basis document. A background that long does not belong in the standard piece as it detracts from the intent of the standard itself.
Response: The SDT thanks you for your comment. The background and Guidelines and Technical Basis sections have been combined.		

Organization	Yes or No	Question 4 Comment
MidAmerican Energy		See the NSRF comments.
Response: The SDT thanks you for your participation. Please review the response to that commenter.		
MEAG Power		Should these administrative activities be sent over to NAESB? R1: There is merit in having a plan as identified in R1, but is this a need to support reliability or is it a business practice? Should it be in NAESB's domain? R2, R3 & R4: These are not appropriate for a Standard. If you don't annually review the plan, will reliability be reduced and the BES be subject to instability, separation and cascading? If DOE needs a form filled out, fill it out and send it to DOE. NERC doesn't need to pile on. Mike Moon and Jim Merlo have been stressing results and risk based, actual performance based, event analysis, lessons learned and situational awareness. EOP-004 is primarily a business preparedness topic and identifies administrative procedures that belong in the NAESB domain.
Public Utility District No. 1 of Snohomish County		SNPD suggest moving these administrative activities to NAESB. R1: There is merit in having a plan as identified in R1, but is this a need to support reliability or is it a business practice? Should it be in NAESB's domain? R2, R3 & R4: These are not appropriate for a Standard. If you don't annually review the plan, will reliability be reduced and the BES be subject to instability, separation and cascading? If DOE needs a form filled out, fill it out and send it to DOE. NERC doesn't need to pile on. Gerry Cauley and Mike Moon have been stressing results and risk based, actual performance based, event analysis, lessons learned and situational awareness. EOP-004 is primarily a business preparedness topic and identifies administrative procedures that belong in the NAESB domain.
Response: The SDT thanks you for your comment. SDT believes this standard is needed to provide Situational Awareness and can help in providing lessons learned to the industry. The SDT has revised the requirements to address this need. While it may be appropriate to have NAESB to adopt this obligation at some in the future, the SDT was charged with addressing deficiencies at this time. The SDT has removed all references to filing reports to DOE from the earlier versions. Today's only reference provides for NERC's acceptance of the use of their form when it is appropriate.		

Organization	Yes or No	Question 4 Comment
Springfield Utility Board		SUB appreciates the opportunity to provide comments. While Staff was concerned with the consolidation of CIP and non-CIP NERC Reliability Standards (as to how they'll be audited), the Project 2009-01 SDT has done an excellent job in providing clarification around identifying and reporting events, particularly related to the varying definitions of "sabotage".
Response: The SDT thanks you for your support.		
Tacoma Power		Tacoma Power disagrees with the requirement to perform annual testing of each communication plan. We do not see any added value in performing annual testing of each communication plan. There are already other Standard requirements to performing routine testing of communications equipment and emergency communications with other agencies. The "proof of compliance" to the Standard should be in the documentation of the reports filed for any qualifying event, within the specified timelines and logs or phone records that it was communicated per each specified communication plan. Tacoma Power has none at this time. Thank you for considering our comments.
Response: The SDT thanks you for your comment. The SDT has revised Requirement R3 and we believe that our changes address your suggestion.		
Exelon Corporation and its affiliates		Thanks to the SDT. Significant progress was made in revising the proposed standard language. We appreciate the effort and have only a few remaining requests: o We understand that CIP-008 dictates the 1-hour reporting obligation for Cyber Security Incidents and this iteration of EOP-004 delineates the CIP-008 requirements. Please confirm that per the exemption language in the CIP standards (as consistent with the March 10, 2011 FERC Order (docket # RM06-22-014) nuclear generating units are not subject to this reporting requirement. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008. The next version of EOP-004-2**

Organization	Yes or No	Question 4 Comment
		will not contain a one-hour reporting requirement. o EOP-004 still lists "Generation Loss" as a 24 hour reporting criteria without any time threshold guidance for the generation loss. Exelon previously commented to the SDT (without the comment being addressed) that Generation Loss should provide some type of time threshold. If the 2000 MW is from a combination of units in a single location, what is the time threshold for the combined unit loss? In considering clarification language, the SDT should review the BAL standards on the disturbance recovery period for appropriate timing for closeness of trips. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection** **OR** **≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection."** o The "physical threat that could impact" requirement remains vague and it's not clear the relevance of such information to NERC or the Regions. If a train derailment occurred near a generation facility (as stated in the footnote), are we to expect that NERC is going to send out a lesson learned with suggested corrective actions to protect generators from that occurring? The value in that event reporting criteria seems low. The requirement should be removed. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated**

Organization	Yes or No	Question 4 Comment
		based on currently enforced Reliability Standards, FERC directives and industry comments to state: **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.** o The event concerning voltage deviation of +/- 10% does not specify which type of voltage. In response to this comment in the previous comment period, the SDT indicated that the entity could determine the type of voltage. It would be clearer to specify in the standard and avoid future interpretation at the audit level. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:**

Organization	Yes or No	Question 4 Comment
		"Observed voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes ." **This language clearly states that if the threshold is met, the entity needs to submit a report within 24 hours.** o As requested previously, for nuclear facilities, EOP-004 reporting should be coordinated with existing required notifications to the NRC and FBI as to not duplicate effort or add unnecessary burden on the part of a nuclear GO/GOP during a potential security or cyber event. Please contact the NRC about this project to ensure that required communication and reporting in response to a radiological sabotage event (as defined by the NRC) or any incident that has impacted or has the potential to impact the BES does not create duplicate reporting, conflicting reporting thresholds or confusion on the part of the nuclear generator operator. Each nuclear generating site licensee must have an NRC approved Security Plan that outlines applicable notifications to the FBI. Depending on the severity of the security event, the nuclear licensee may initiate the Emergency Plan (E-Plan). Exelon again asks that the proposed reporting process and flow chart be coordinated with the NRC to ensure it does not conflict with existing expected NRC requirements and protocol associated with site specific Emergency and Security Plans. In the alternative, the EOP-004 language should include acceptance of NRC required reporting to meet the EOP-004 requirements. **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Complete loss of off-site power affecting a nuclear generating station per the Nuclear Plant Interface Requirement."** **As stated in this event Threshold, the TOP's NIPR may have additional guidance concerning the complete loss of offsite power affecting a nuclear plant.**

Organization	Yes or No	Question 4 Comment
		o The proposed standard notes that the text boxes will be moved to the Guideline and Technical Basis Section which we support. However, it's not clear whether all the information in the background section will remain part of the standard. If this section is to remain as proposed concerted revision is needed to ensure that the discussion language matches the requirement language. At present, it does not. For instance, the flow chart on page 9 indicates when to report to law enforcement while the requirements merely state that communications to law enforcement be addressed within the operating plan. **The background sections will remain in the standard. The flowchart on Page 9 is an example only and may differ from your Operating Plan.** o Exelon voted negative vote on this ballot due to the need for further clarification and reconciliation between NERC EOP-004 and the NRC. **The SDT team does not believe that reporting under EOP-004 can in anyway 'conflicts' with any other reporting obligations that nuclear or any other type of GO/GOP may have. By allowing applicable entities to use the OE-417 form, the drafting team believes it has given industry reasonable accommodation to reduce duplicative reporting. The same is true for other agencies as well. If an entity submits to NERC the same that was submitted to the other regulatory agency, then this submission will be acceptable. Based on the historical frequency with which GO/GOPs report under the current EOP-004-1 the drafting team does not believe this places and inordinate burden on the applicable entities.**
Response: The SDT thanks you for your comment.		
Alberta Electric System Operator		The Alberta Electric System Operator will need to modify parts of this standard to fit the provincial model and current legislation when it develops the Alberta Reliability Standard.
Response: The SDT thanks you for your comment.		

Organization	Yes or No	Question 4 Comment
Puget Sound Energy, Inc.		The effective date language in the Implementation Plan is inconsistent with the effective date language in the proposed standard. **The SDT checked the language and found both to be identical.** In addition, the statement of effective date in the Implementation Plan is ambiguous - will EOP-004-2 be effective in accordance with the first paragraph or when it is "assigned an effective date" as stated in the second paragraph? **The second paragraph deals with EOP-004-1, the currently mandatory and enforceable standard.** All requirements should be assigned a Lower Violation Risk Factor. Medium risk factors require direct impact on the Bulk Electric System and the language there regarding "instability, separation, or cascading failures" is present to distinguish the Medium risk factor from the High risk factor. Since all of the requirements address after-the-fact reporting, there can be no direct impact on the Bulk Electric System. In addition, if having an Operating Plan under Requirement R1 is a Lower risk factor, then it does not make sense that reviewing that Operating Plan annually under Requirement R4 has a higher risk factor. **The SDT disagrees. Please review the VRF documentation that was posted with the standard for the analysis of the requirements.** The shift away from "the distracting element of motivation", i.e., removing "Sabotage" from the equation, runs the risk of focusing solely on what happened, how to fix it, and waiting for the next event to occur. That speaks to a reactive approach rather than a proactive one. There is a concern with the removal of the FBI from the reporting mix. Basically, the new standard will involve reporting a suspicious event or attack to local law enforcement and leaving it up to them to decide on reporting to the FBI. Depending on their evaluation, an event which is significant for a responsible entity might not rise to the priority level of the local law enforcement agency for them to report it to the FBI. While this might reduce the reporting requirements a bit, it might do so to the responsible entity's detriment.

Organization	Yes or No	Question 4 Comment
		The Operating Plan developed by each responsible entity may indeed have certain event types reported directly to the FBI. It is up the entity to determine the appropriate notifications. Entities in Canada would not report anything to the FBI. In Attachment 2 - item 4, would it be possible for the boxes be either alpha-sorted or sorted by priority? **The SDT has made changes to Attachment 2 to list the Events in order of their listing in Attachment 1.** There is a disconnect between footnote 1 on page 18 (Don't report copper theft) and the Guideline section, which suggests reporting forced intrusion attempt at a substation. **Forced Intrusion was removed from the Guidelines section. The SDT has deleted footnote 1 based on comments received from the industry, however, retained the concept in the event type "Physical threats to a Facility" as:** **"Do not report copper theft unless it degrades normal operation of a Facility."** Also, in the section discussing the removal of sabotage, the Guideline mentions certain types of events that should be reported to NERC, DHS, FBI, etc., while that specificity with respect to entities has been removed from the reporting requirement. **The SDT disagrees with your assessment on reporting. Entities know best to whom and what reporting obligations they have on the applicable event types. The SDT has learned that states vary in organization of their law enforcement agencies. As such it is impossible for the SDT to outline those obligations in a consistent and uniform manner. Entities can establish a single or multiple contact lists as needed for the different event types.**
Response: The SDT thanks you for your comments.		
Kansas City Power & Light		The flowchart states, "Notification Protocol to State Agency Law Enforcement".

Organization	Yes or No	Question 4 Comment
		Please correct this to, "Notification to State, Provincial, or Local Law Enforcement", to be consistent with the language in the background section part, "A Reporting Process Solution - EOP-004". Evidence Retention - it is not clear what the phrase "prior 3 calendar years" represents in the third paragraph of this section regarding data retention for requirements and measures for R2, R3, R4 and M2, M3, M4 respectively. Please clarify what this means. Is that different than the meaning of "since the last audit for 3 calendar years" for R1 and M1?
Response: The SDT thanks you for your comment. The flowchart is an example only and was not meant to show every permutation. The evidence retention paragraph has been revised to reflect the 'since last audit' language.		
United Illuminating Company		The measures M3 and M4 require evidence to be dated and time stamped. The time stamp is excessive and provides no benefit. A dated document is sufficient. The measure M2 requires in addition to a record of the transmittal of the EOP-004 Attachment 2 form or DOE-417 form that an operator log or other operating documentation is provided. It is unclear why this supplemental evidence of operator logs is required. We are assuming that the additional operator logs or documentation is required to demonstrate that the communication was completed to organizations other than NERC and DOE of the event. If true then the measure should be clear on this topic. For communication to NERC and DOE use the EOP-004 Form or OE-417 form and retain the transmittal record. For communication to other organizations pursuant to R1 Part 1.2 evidence may include but not limited to, operator logs, transmittal record, attestations, or voice recordings.
Response: The SDT thanks you for your comment. The SDT has removed the time-stamp provision. The SDT agrees and adopts your suggestion.		
New York Independent System Operator		The NYISO is part of and supports comments submitted by NPCC Reliability Standards Committee and the IRC Standards Review Committee. However the NYISO would also like to comment on the following items: o NERC has been proposing the future

Organization	Yes or No	Question 4 Comment
		development of performance based standards, which is directly related to reliability performance. Requirement 2 of this standard is simply a reporting requirement. We believe that this does not fall into a category of a performance based standard. NERC has the ability to ask for reports on events through ROP provisions and now the new Event Analysis Process. It does not have to make it part of the compliance program. Some have indicated that need for timely reporting of cyber or sabotage events. The counter argument is that the requirement is reporting when confirmed which would delay any useful information to fend off a simultaneous threat. Also NERC has not provided any records of how previous timely (1 hour) reporting has mitigated reliability risks. o The NERC Event Analysis Process was recently approved by the NERC OC and is in place. This was the model program for reporting outside the compliance program that the industry was asking for. This should replace the need for EOP-004.o NERC has presented Risk Based Compliance Monitoring (RBCM) to the CCC, MRC, BOT and at Workshops. This involves audit teams monitoring an entities controls to ensure they have things in place to maintain compliance with reliability rules. The proposed EOP-004 has created requirements that are controls to requirement R2, which is to file a report on predefined incidents. The RBCM is being presented as the auditor will make determinations on the detail of the sampling for compliance based on the assessment of controls an entity has in place to maintain compliance. It is also noted that compliance will not be assessed against these controls. As the APS example for COM-002 is presented in the Workshop slides, the issue is that EOP-004 R1, R3 and R4 are controls for reporting; 1) have a plan, 2) test the plan, and 3) review the plan. While R2 is the only actionable requirement. The NYISO believes that all reporting requirements have been met by OE-417 and EAP reporting requirements and that EOP-004 has served its time. At a minimum, the NYISO would suggest that EOP-004 be simplified to just R2 (reporting requirement) and the other requirements be placed at the end of the RSAW to demonstrate a culture of compliance as presented by NERC.
Response: The SDT thanks you for your comment. Please review the responses to those commenters. The SDT appreciates your suggestion, however, most of your comment is beyond the scope of the SDT's charge. The SDT would like to note your statement		

Organization	Yes or No	Question 4 Comment
on reporting requirements having been met by the OE-417 and EAP requirements. The SDT fails to see how NERC gains situational awareness and the opportunity to pass along lessons learned when the aforementioned reports are not forwarded to the appropriate ERO group. The SDT would also note that the ERO does not have access to the OE-417 filings unless they are provided and the EAP does not include reporting for some of the event types listed in Attachment 1. The SDT will forward your comment to appropriate officials for their consideration.		
Hydro One		The proposed standard is not consistent with NERC's new Risk Based Compliance Monitoring. - The performance based action to "implement its event reporting Operating Plan" on defined events, as required in R2, could be considered a valid requirement. However, the concern is that this requirement could be superseded by the NERC Events Analysis Process and existing OE-417 Reporting.- The requirements laid out in R1, R3 and R4 are specific controls to ensure that the proposed requirement to report (R2) is carried out. However, controls should not be part of a compliance requirement. The only requirement proposed in this standard that is not a control is R2.NERC does not need to duplicate the enforcement of reporting already imposed by the DOE. DOE-417 is a well-established process that has regulatory obligations. NERC enforcement of reporting is redundant. NERC has the ability to request copies of these reports without making them part of the Reliability Rules. **The SDT appreciates your suggestion, however, most of your comment is beyond the scope of the SDT's charge. The SDT would like to note your statement on reporting requirements having been met by the OE-417 and EAP requirements. This statement is not true for Canadian entities. The SDT fails to see how NERC gains situational awareness and the opportunity to pass along lessons learned when the aforementioned reports are not forwarded to the appropriate ERO group. The SDT would also note that the ERO does not have access to the OE-417 filings unless they are provided and the EAP does not include reporting for some of the event types listed in Attachment 1. The SDT will forward your comment to appropriate officials for their consideration.** Form EOP-004, Attachment 2: Event Reporting Form: - Delete from the Task column

Organization	Yes or No	Question 4 Comment
		the words "or partial".- Delete from the Task column the words "physical threat that could impact the operability of a Facility". **The SDT has proposed changes to the language within Attachment 2 which we believe corrects the point made.** VSL's may have to be revised to reflect revised wording. The standard as proposed is not supportive of Gerry Cauley's performance based standard initiative **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:** **"Physical threat to its Facility excluding weather related threat, which has the potential to degrade the normal operation of the Facility** **Or** **Suspicious device or activity at a Facility** **Do not report copper theft unless it degrades normal operations of a Facility."** **This language gives the required guidance that if there is a physical threat that has the potential to degrade a Facility's normal operation or a suspicious device or activity is discovered at a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility has a potential of not being able to operate as it is designed. The SDT also states that copper theft is not a reportable event unless it degrades the normal operation of a Facility.**

Organization	Yes or No	Question 4 Comment
Response: The SDT thanks you for your comment.		
Northeast Power Coordinating Council		The proposed standard is not consistent with NERC's new Risk Based Compliance Monitoring. a. The performance based action to "implement its event reporting Operating Plan" on defined events, as required in R2, could be considered a valid requirement. However, the concern is that this requirement could be superseded by the NERC Events Analysis Process and existing OE-417 Reporting. b. The requirements laid out in R1, R3 and R4 are specific controls to ensure that the proposed requirement to report (R2) is carried out. However, controls should not be part of a compliance requirement. The only requirement proposed in this standard that is not a control is R2.NERC does not need to duplicate the enforcement of reporting already imposed by the DOE. DOE-417 is a well established process that has regulatory obligations. NERC enforcement of reporting is redundant. NERC has the ability to request copies of these reports without making them part of the Reliability Rules. **The SDT appreciates your suggestion however; most of your comment is beyond the scope of the SDT's charge. The SDT would like to note your statement on reporting requirements having been met by the OE-417 and EAP requirements. This statement is not true for Canadian entities. The SDT fails to see how NERC gains situational awareness and the opportunity to pass along lessons learned when the aforementioned reports are not forwarded to the appropriate ERO group. The SDT would also note that the ERO does not have access to the OE-417 filings unless they are provided and the EAP does not include reporting for some of the event types listed in Attachment 1. The SDT will forward your comment to appropriate officials for their consideration.** Form EOP-004, Attachment 2: Event Reporting Form: Delete from the Task column the words "or partial". Delete from the Task column the words "physical threat that

Organization	Yes or No	Question 4 Comment
		could impact the operability of a Facility". **The SDT has proposed changes to the language within Attachment 2 which we believe corrects the point made.** VSL's may have to be revised to reflect revised wording. **The SDT agrees and adopts your suggestion.**
Response: The SDT thanks you for your comment.		
American Public Power Association		The SDT needs to provide some relief for the small entities in regards to the VSL in the compliance section. APPA believes there should be no High or Severe VSLs for this standard. This is a reporting/documentation standard and does not affect BES reliability at all. It is APPA's opinion that this standard should be removed from the mandatory and enforceable NERC Reliability Standards and turned over to a working group within the NERC technical committees. Timely reporting of this outage data is already mandatory under Section 13(b) of the Federal Energy Administration Act of 1974. There are already civil and criminal penalties for violation of that Act. This standard is a duplicative mandatory reporting requirement with multiple monetary penalties for US registered entities. If this standard is approved, NERC must address this duplication in their filing with FERC. This duplicative reporting and the differences in requirements between DOE-OE-417 and NERC EOP-004-2 require an analysis by FERC of the small entity impact as required by the Regulatory Flexibility of Act of 1980
Response: The SDT thanks you for your comment. VSLs refer to how closely the entity met the requirements of the standard; it is the VRF that measures impact to reliability. The SDT believes use of the high and severe VSLs is appropriate. The SDT believes that size is not the important criteria in determining an impact on reliability. The reporting thresholds are based on the BES. No entity, including small entities is required to report on equipment that is not categorized as BES, which should give small entities relief from reporting on non-impactive assets.		
Pepco Holdings Inc		The SDT's efforts have resulted in a very good draft.

Organization	Yes or No	Question 4 Comment
Response: The SDT thanks you for your support.		
ISO/RTO Standards Review Committee		The SRC offers some other comments regarding the posted draft requirements; however, by so doing, the SRC does not indicate support of the proposed requirements. Following these comments, please see below for an SRC proposed alternative approach: The SRC does not agree with the MEDIUM VRF assigned to Requirement R4. R4 is a requirement to conduct an annual review of the Event Reporting Operating Plan mandated in Requirement R1. R1 however is assigned a VRF of LOWER. We are unable to rationalize why a subsequent review of a plan should have a higher reliability risk impact than the development of the plan itself. Hypothetically, if an entity doesn't develop a plan to begin with, then it will be assigned a LOWER VRF, and the entity will have no plan to review annually and hence it will not be deemed non-compliant with requirement R4. The entity can avoid being assessed violating a requirement with a MEDIUM VRF by not having the plan to begin with, for which the entity will be assessed violating a requirement with a LOWER VRF. We suggest changing the R4 VRF to LOWER. **The SDT has revised the requirements and R4 has been deleted along with its VRF/VSL.** The SRC requests that the SDT post the following Alternative Proposal for Industry comments as required by the Standards Process to obtain Industry consensus and as permitted by FERC: An equally effective alternative is to withdraw this standard and to make the contents of the SDT's posted standard a NERC Guideline. a. This alternative is more in line with new NERC and FERC proposals b. This alternative retains the reporting format Comments 1. The FERC Order 693 directives regarding "sabotage" have already been addressed by the SDT (i.e. the concept was found outside the scope of NERC standards) 2. Current Industry actions already address the needs cited in the Order:

Organization	Yes or No	Question 4 Comment
		a. Approved Reporting Processes already exists i. The Operating Committee's Event Analysis Process ii. Alert Reporting b. The Data already exists i. Reliability Coordinators Information System (which creates hundred if not thousands of "reports" per year) ii. The DOE's OE 417 Report itself provides part of the FERC discussed data 3. The proposed standard is not supportive of Gerry Cauley's performance based standard initiative or of FERC's offer to reduce procedural standards a. The proposed requirement is a process not an outcome i. The proposal is more focused on reporting and could divert the attention of reliability entities from addressing a situation to collecting data for a report b. The proposed "events" are subjective and if followed will create an unmanageable burden on NERC staff i. Reporting "damage" to facilities can be interpreted as anything from a dent in a generator to the total destruction of a transformer ii. The reporting requirements on all applicable entities will create more questions about differences between the reports of the various entities - rather than leading to conclusions about patterns among events that indicate a global threat iii. Reporting any "physical threat" is too vague and subjective iv. Reporting "damage to a facility that affects an IROL" is subjective and can be seen to require reporting of damage on every facility in an interconnected area. v. Reporting "Partial loss of monitoring" is a data quality issue that can be anything from the loss of a single data point to the loss of an entire SCADA system vi. Testing the filling out of a Report does not make it easier to fill out the report later (moreover the reporting is already done often enough -see 2.b.i)c. The proposed requirements will create a disincentive to improving current Reporting practices (the more an entity designs into its own system the more it will be expected to do and the more likely it will be penalized for failing to comply)i. Annual reviews of the reporting practices fall into the same category, why have a detailed process to review when a simple one will suffice?

Organization	Yes or No	Question 4 Comment
		4. The proposed standard does not provide a feedback loop to either the data suppliers or to potentially impacted functional entities a. If the "wide area" data analysis indicates a threat, there is no requirement to inform the impacted entities b. As a BES reliability issue there is no performance indicators or metrics to show the value of this standard i. The SRC recognizes that specific incidents cannot be identified but if this is to be a reliability standard some information must be provided. A Guideline could be designed to address this concern. 5. The proposed standard is not consistent with NERC's new Risk Based Compliance Monitoring. a. The performance based action to report on defined events, as required in R2, could be considered a valid requirement. However we have concerns as noted in Bullet 3 above. The requirements laid out in R1, R3 and R4 are specific controls to ensure that the proposed requirement to report (R2) is carried out. NERC is moving in the direction to assess entities' controls, outside of the compliance enforcement arm. The industry is being informed that NERC Audit staff will conduct compliance audits based on the controls that the entity has implemented to ensure compliance. The SRC is interested in supporting this effort and making it successful. However, if this is the direction NERC is moving, we should not be making controls part of a compliance requirement. The only requirement proposed in this standard that is not a control is R2. 6. For FERC-jurisdictional entities, NERC does not need to duplicate the enforcement of reporting already imposed by the DOE. DOE-417 is a well established process that has regulatory obligations. NERC enforcement of reporting would be redundant. NERC has the ability to request copies of these reports without making them part of the Reliability Rules.
Response: The SDT thanks you for your comment. The SDT will bring this request to the attention of the SC for consideration as this request is beyond the scope of work identified in this project.		
LG&E and KU Services		The Violation Severity Level for Requirement R2 should be revised to read "...hours

Organization	Yes or No	Question 4 Comment
		after recognizing an event requiring reporting..." This will make the language in the VSL consistent with the language in Attachment 1.
Response: The SDT thanks you for your comment. The VSLs have been reviewed and revised based upon the revisions to the requirements.		
SPP Standards Review Group		The VRF for R1 is Lower which is fine. The issue is that R4, which is the review of the plan contained in R1, has a Medium VRF. We recommend moving the VRF of R4 to Lower.We recommend deleting the phrase '...supplemented by operator logs or other operating documentation...' as found in the first sentence of M2. A much clearer reference is made to operator logs and other operating documentation in the second sentence. The duplication is unnecessary.What will happen with the accompanying information contained in the Background section in the draft standard? Will it be moved to the Guideline and Technical Basis at the end of the standard as the information contained in the text boxes? This is valuable information and should not be lost.
Response: The SDT thanks you for your comment. The SDT has revised the requirements and R4 has been deleted along with its VRF/VSL. The background has been moved to the Guidelines and Technical Basis section.		
Utility Services		There are no other comments at this time.
Response: The SDT thanks you for your participation.		
Dynegy Inc.		Use of the term "Part x.x" throughout the Standard is somewhat confusing. I can't recall other Standards using that type of term. Suggest using the term "Requirement" instead.
Response: The SDT thanks you for your comment. The standard has been rewritten and revised in accordance with your suggestion.		
Central Lincoln		We agree with the comments provided by both PNGC and APPA.

Organization	Yes or No	Question 4 Comment
Response: The SDT thanks you for your comment. Please review the responses to those commenters.		
PNGC Comment Group		We appreciate the hard work of the SDT.
Response: The SDT thanks you for your support.		
PPL Corporation NERC Registered Affiliates		We appreciate the inclusion of the Process Flowchart on Page 9 of the draft standard. We submit for your consideration, removing the line from the NO decision box to the 'Report Event to ERO, Reliability Coordinator' box. It seems if the event does not need reporting per the decision box, this line is not needed.The decision box on 'Report to Law Enforcement ?' does not have a Yes or No. Perhaps, this decision box is misplaced, or is it intended to occur always and not have a different path with different actions? Ie. should it be a process box? Thank you for your work on this standard.
PPL Electric Utilities		We appreciate the inclusion of the Process Flowchart on Page 9 of the draft standard. We submit for your consideration, removing the line from the NO decision box to the 'Report Event to ERO, Reliability Coordinator' box. It seems if the event does not need reporting per the decision box, this line is not needed.For clarity in needed actions, please consider using a decision box following flowcharting standards such as, a decision box containing a question with a Yes and a No path. The decision box on 'Report to Law Enforcement ?' does not have a Yes or No. Perhaps, this decision box is misplaced, or is it intended to occur always and not have a different path with different actions? Ie. should it be a process box?Thank you for your work on this standard.
Response: The SDT thanks you for your comment. The flowchart was provided as an example and guidance for entities to use if they so choose. Entities can elect to create their own flowchart based upon their needs.		
Independent Electricity System Operator		We do not agree with the MEDIUM VRF assigned to Requirement R4. Re stipulates a requirement to conduct an annual review of the event reporting Operating Plan in

Organization	Yes or No	Question 4 Comment
		Requirement R1, which itself is assigned a VRF of LOWER. We are unable to rationalize why a subsequent review of a plan should have a higher reliability risk impact than the development of the plan itself. Hypothetically, if an entity doesn't develop a plan to begin with, then it will be assigned a LOWER VRF, and the entity will have no plan to review annually and hence it will not be deemed non-compliant with requirement R4. The entity can avoid being assessed violating a requirement with a MEDIUM VRF by not having the plan to begin with, for which the entity will be assessed violating a requirement with a LOWER VRF. We suggest changing the R4 VRF to LOWER.
Response: The SDT thanks you for your comment. The SDT has revised the requirements and R4 has been deleted along with its VRF/VSL.		
SMUD & BANC		We feel issues were addressed, but still have concern with 'damage'. We certainly support that any 'destruction' of a facility that meets any of the three criteria be a reportable issue. But 'damage', if it's going to be included should have some objective definition that sets a floor. Much like the copper theft issue, we don't see the benefit of reporting plain vandalism (gun-shot insulators results from actual or suspected intentional human action) to NERC unless the 'damage' has some tangible impact on the reliability of the system or are acts of an orchestrated sabotage (i.e. removal of bolt in a transmission structure).
Response: The SDT thanks you for comment. The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state:		

Organization	Yes or No	Question 4 Comment
		"Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in the need for actions to avoid a BES Emergency." **This language gives the required guidance of who has to report within its Area that results in need for actions to avoid a BES Emergency (as defined by NERC: Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System).** **This relates to either a completely destroyed Facility where an action is required to avoid a BES Emergency, or a Facility that is damaged to a point that actions are required to avoid a BES Emergency. By reporting either a "damaged or destroyed" Facility, within 24 hours, it will give the ERO (and whoever else the entity wishes to inform per R1) the situational awareness that the electrical system has been reconfigured or may need to be reconfigured, thus supporting reliable operations of each interconnection.** **The SDT removed all language under "Entity with Reporting Responsibility," with the exception of entity(s) that are required to report an applicable event. The SDT removed this language so the entities within this column are clearly stated and identified. Under the "Threshold for Reporting" column, a bright line was updated based on currently enforced Reliability Standards, FERC directives and industry comments to state;** **Damage or destruction of its Facility that results from actual or suspected intentional human action.** **This language gives the required guidance that if there is actual intentional human action that damages or destroys a Facility, it is required to be reported within 24 hours, this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human.** **This event was written to cover the increase of "Entity with Reporting Responsibility" and removing the RC since they do not own Facility(s).** **The SDT also included a second part of this event being "suspected intentional human action." This language was required to give an entity the reporting responsibility to report to the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that they suspect that their Facility was damaged or destroyed by intentional human action. The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan.**
ISO New England Inc		We requests that the SDT post the following Alternative Proposal for Industry

Organization	Yes or No	Question 4 Comment
		comments as required by the Standards Process to obtain Industry consensus and as permitted by FERC: An equally effective alternative is to withdraw this standard and to make the contents of the SDT's posted standard a NERC Guideline.a. This alternative is more in line with new NERC and FERC proposalsb. This alternative retains the reporting formatComments1. The FERC Order 693 directives regarding "sabotage" have already been addressed by the SDT (i.e. the concept was found outside the scope of NERC standards)2. Current Industry actions already address the needs cited in the Order:a. Approved Reporting Processes already existsi. The Operating Committee's Event Analysis Processii. Alert Reporting b. The Data already existsi. Reliability Coordinators Information System (which creates hundred if not thousands of "reports" per year)ii. The DOE's OE 417 Report itself provides part of the FERC discussed data3. The proposed standard is not supportive of Gerry Cauley's performance based standard initiative or of FERC's offer to reduce procedural standardsa. The proposed requirement is a process not an outcomei. The proposal is more focused on reporting and could divert the attention of reliability entities from addressing a situation to collecting data for a reportb. The proposed "events" are subjective and if followed will create an unmanageable burden on NERC staffi. Reporting "damage" to facilities can be interpreted as anything from a dent in a generator to the total destruction of a transformerii. The reporting requirements on all applicable entities will create more questions about differences between the reports of the various entities - rather than leading to conclusions about patterns among events that indicate a global threatiii. Reporting any "physical threat" is too vague and subjective iv. Reporting "damage to a facility that affects an IROL" is subjective and can be seen to require reporting of damage on every facility in an interconnected area. v. Reporting "Partial loss of monitoring" is a data quality issue that can be anything from the loss of a single data point to the loss of an entire SCADA system vi. Testing the filling out of a Report does not make it easier to fill out the report later (moreover the reporting is already done often enough -see 2.b.i)c. The proposed requirements will create a disincentive to improving current Reporting practices (the

Organization	Yes or No	Question 4 Comment
		more an entity designs into its own system the more it will be expected to do and the more likely it will be penalized for failing to comply)i. Annual reviews of the reporting practices fall into the same category, why have a detailed process to review when a simple one will suffice?4. The proposed standard does not provide a feedback loop to either the data suppliers or to potentially impacted functional entitiesa. If the "wide area" data analysis indicates a threat, there is no requirement to inform the impacted entitiesb. As a BES reliability issue there is no performance indicators or metrics to show the value of this standardi. We recognize that specific incidents cannot be identified but if this is to be a reliability standard some information must be provided. A Guideline could be designed to address this concern. 5. The proposed standard is not consistent with NERC's new Risk Based Compliance Monitoring. a. The performance based action to report on defined events, as required in R2, could be considered a valid requirement. However we have concerns as noted in Bullet 3 above.The requirements laid out in R1, R3 and R4 are specific controls to ensure that the proposed requirement to report (R2) is carried out. NERC is moving in the direction to assess entities' controls, outside of the compliance enforcement arm. The industry is being informed that NERC Audit staff will conduct compliance audits based on the controls that the entity has implemented to ensure compliance. We are interested in supporting this effort and making it successful. However, if this is the direction NERC is moving, we should not be making controls part of a compliance requirement. The only requirement proposed in this standard that is not a control is R2. 6. For FERC-jurisdictional entities, NERC does not need to duplicate the enforcement of reporting already imposed by the DOE. DOE-417 is a well established process that has regulatory obligations. NERC enforcement of reporting would be redundant. NERC has the ability to request copies of these reports without making them part of the Reliability Rules.
Response: The SDT thanks you for your comment. The SDT will bring this request to the attention of the SC for consideration as this request is beyond the scope of work identified in this project.		
Brazos Electric Power		We thank the work of the SDT on this project. However, additional improvements

Organization	Yes or No	Question 4 Comment
Cooperative		should be made as described in the comments submitted by ACES Power Marketing.
Response: The SDT thanks you for your comment. Please review the responses to that commenter.		
FirstEnergy		While FE voted affirmative on this draft, upon further review we request clarification be made in the next draft of the standard regarding the applicability of the Nuclear Generator Operator. Per FE's previous comments, nuclear generator operators already have specific regulatory requirements to notify the NRC for certain notifications to other governmental agencies in accordance with 10 CFR 50.72(b)(s)(xi). We had asked that the SDT contact the NRC about this project to ensure that existing communication and reporting that a licensee is required to perform in response to a radiological sabotage event (as defined by the NRC) or any incident that has impacted or has the potential to impact the BES does not create either duplicate reporting, conflicting reporting thresholds or confusion on the part of the nuclear generator operator. In addition, EOP-004 must acknowledge that there may be NRC reporting forms that have the equivalent information contained in their Attachment 2. For what the NRC considers a Reportable Event, Nuclear plants are required to fill out NRC form 361 and/or form 366. We do not agree with the drafting team's response to ours and Exelon's comments that "The NRC does not fall under the jurisdiction of NERC and so therefore it is not within scope of this project." While the statement is correct, we believe that requirements should not conflict with or duplicate other regulatory requirements. We remain concerned that the standard with regard to Nuclear GOP applicability causes duplicative regulatory reporting with existing reporting requirements of the NRC. Therefore, we ask:1. That NERC and the drafting team please investigate these issues further and revise the standard to clarify the scope for nuclear GOPs, and2. For any reporting deemed in the scope for nuclear GOP after NERC's and the SDT's investigation per our request in #1 above, that the SDT consider the ability to utilize information from NRC reports as meeting the EOP-004-2 requirements similar to the allowance of using the DOE form as presently proposed.

Organization	Yes or No	Question 4 Comment
Response: The SDT thanks you for your comment. The SDT team does not believe that reporting under EOP-004 can in anyway 'conflicts' with any other reporting obligations that nuclear or any other type of GO/GOP may have. By allowing applicable entities to use the OE-417 form, the drafting team believes it has given industry reasonable accommodation to reduce duplicative reporting. The same is true for other agencies as well. If an entity submits to NERC the same that was submitted to the other regulatory agency, then this submission will be acceptable. Based on the historical frequency with which GO/GOPs report under the current EOP-004-1 the drafting team does not believe this places and inordinate burden on the applicable entities.		
American Electric Power		While we do not necessarily disagree with modifying this standard, we do have serious concerns with the possibility that Form OE-417 form would not also be modified to match any changes made to this standard. To the degree they would be different, this would create unnecessary confusion and burden on operators. **While we appreciate the point raised, the SDT does have any authority with regard to the language contained within the DOE OE-417 form. The Department of Energy is responsible for the design and contents of the 417 form. As a part of the SDT's work in this proposal, we met with and collaborated with the DOE staff responsible for the 417 form establish a common understanding of reportable events. We hope that if the DOE desires to make further changes, they will pass along information for consideration in a future NERC SAR.** If CIP-008 is now out of scope within the requirements of this standard, the task "reportable Cyber Security Incident" should be removed from Attachment 2. **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement.**
Response: The SDT thanks you for your comment.		
Progress Energy		Within attachment 1 (Reportable Events) an exclusion is allowed for weather related threats. PGN recommends a more generic approach to include natural events such as forest fires, sink holes, etc. This would alleviate some reporting burdens in areas that

Organization	Yes or No	Question 4 Comment
		are prone to these types of events.
Response: The SDT thanks you for your comment. The SDT has revised the language in accordance with your suggestion to "weather or natural disaster related threats".		
Xcel Energy		Xcel Energy appreciates the work of the drafting team and believes the current draft is an improvement over the existing standard. However, we would like to see the comments provided here and above addressed prior to submitting an AFFIRMATIVE vote.1) Suggest enhancing the "Example of Reporting Process..." flowchart as follows: EVENT > Refer to Ops Plan for Event Reporting > Refer to Law Enforcement? > Yes/No > .... **The SDT has provided the flowchart as an example and guidance for entities. Entities can choose to create their own version of the flowchart for use in their Operating Plan.** 2) Attachment 1 - in both the 1 hour and the 24 hour reporting they are qualified with "within x hours of recognition of the event". Is this the intent, so that if an entity recognizes at some point after an event that the time clock starts? **The SDT has discussed this issue with Project 2008-06, Cyber Security SDT and we have remanded the one hour event back to CIP-008. The next version of EOP-004-2 will not contain a one hour reporting requirement.** **The SDT envisions when the entity is made aware of an applicable event contained in Attachment 1, that they would report the event within 24 hours. Any entity could enhance their Operating Plan to describe as much detail as they wanted to provide to their employees as they see fit.** 3) VSLs - R3 & R4 "Severe" should remove the "OR....", as this is redundant. Once an entity has exceeded the 3 calendar months, the Severe VSL is triggered. **The SDT has revised the requirements and accordingly the VSLs.** 4) The Guideline and Technical Basis page 22 should be corrected to read "The

Organization	Yes or No	Question 4 Comment
		changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). These standards deal exclusively with after-the-fact reporting." **Response: Thank you for the grammatical correction.** 5) Also in the following section of the Guideline and Technical Basis (page 23) the third bullet item should be qualified to exclude copper theft: Examples of such events include: o Bolts removed from transmission line structures o Detection of cyber intrusion that meets criteria of CIP-008-3 or its successor standard o Forced intrusion attempt at a substation (excluding copper theft) o Train derailment near a transmission right-of-way o Destruction of Bulk Electric System equipment **Response: Thank you for the correction; however, as a result of other changes made to the standard, the SDT is proposing to remove the third bulleted item from this list.**
Response: The SDT thanks you for your comment.		
Edison Mission Marketing & Trading, Inc.		No
Idaho Power Co.		No
Arizona Public Service Company		None

END OF REPORT

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SC approved SAR for initial posting (April 2009).
2. SAR posted for comment (April 22 – May 21, 2009).
3. SC authorized moving the SAR forward to standard development (September 2009).
4. Concepts Paper posted for comment (March 17 – April 16, 2010).
5. Initial Informal Comment Period (September 15 – October 15, 2010).
6. Second Comment Period (Formal) (March 9 – April 8, 2011).
7. Third Comment Period and Initial Ballot (October 28 – December 12, 2011).
8. Fourth Comment Period and Successive Ballot (April 25 – May 24, 2012).

Proposed Action Plan and Description of Current Draft
This is the fifth posting of the proposed standard in accordance with Results-Based Standards (RBS) criteria. The drafting team requests posting for a 30-day formal comment period concurrent with the formation of the ballot pool and the successive ballot.

Future Development Plan

Anticipated Actions	Anticipated Date
Drafting team considers comments, makes conforming changes on fourth posting	June - August 2012
Fifth Comment/Ballot period	August – September 2012
Recirculation Ballot period	October 2012
Receive BOT approval	November 2012
File with regulatory authorities	December 2012

Effective Dates

The first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities. In those jurisdictions where regulatory approval is not required, the standard shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-2a Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2 Event Reporting; Retire CIP-001-2a Sabotage Reporting and Retired EOP-004-1 Disturbance Reporting.	Revision to entire standard (Project 2009-01)

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

When this standard has received ballot approval, the text boxes will be moved to the Guideline and Technical Basis Section.

A. Introduction

1. Title: Event Reporting

2. Number: EOP-004-2

3. Purpose: To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities.

4. Applicability

4.1. Functional Entities: For the purpose of the Requirements and the EOP-004 Attachment 1 contained herein, the following functional entities will be collectively referred to as "Responsible Entity."

4.1.1. Reliability Coordinator

4.1.2. Balancing Authority

4.1.3. Transmission Owner

4.1.4. Transmission Operator

4.1.5. Generator Owner

4.1.6. Generator Operator

4.1.7. Distribution Provider

5. Background:

NERC established a SAR Team in 2009 to investigate and propose revisions to the CIP-001 and EOP-004 Reliability Standards. The team was asked to consider the following:

1. CIP-001 could be merged with EOP-004 to eliminate redundancies.
2. Acts of sabotage have to be reported to the DOE as part of EOP-004.
3. Specific references to the DOE form need to be eliminated.
4. EOP-004 had some 'fill-in-the-blank' components to eliminate.

The development included other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient Bulk Electric System reliability standards.

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009.

The DSR SDT developed a concept paper to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT had developed. The posting of the concept paper sought comments from stakeholders on the "road map" that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the DSR SDT. The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC issues database and FERC Order 693 Directives in order to determine a prudent course of action with respect to revision of these standards.

B. Requirements and Measures

R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the regional entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Each Responsible Entity will have a dated event reporting Operating Plan that includes, but is not limited to the protocol(s) and each organization identified to receive an event report for event types specified in EOP-004-2 Attachment 1 and in accordance with the entity responsible for reporting.

Rationale for R1

The requirement to have an Operating Plan for reporting specific types of events provides the entity with a method to have its operating personnel recognize events that affect reliability and to be able to report them to appropriate parties; e.g., Regional Entities, applicable Reliability Coordinators, and law enforcement and other jurisdictional agencies when so recognized. In addition, these event reports are an input to the NERC Events Analysis Program. These other parties use this information to promote reliability, develop a culture of reliability excellence, provide industry collaboration and promote a learning organization.

Every industry participant that owns or operates elements or devices on the grid has a formal or informal process, procedure, or steps it takes to gather information regarding what happened when events occur. This requirement has the Responsible Entity establish documentation on how that procedure, process, or plan is organized. This documentation may be a single document or a combination of various documents that achieve the reliability objective.

The communication protocol(s) could include a process flowchart, identification of internal and external personnel or entities to be notified, or a list of personnel by name and their associated contact information. An existing procedure that meets the requirements of CIP-001-2a may be included in this Operating Plan along with other processes, procedures or plans to meet this requirement.

R2. Each Responsible Entity shall report events per their Operating Plan within 24 hours of meeting an event type threshold for reporting. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

M2. Each Responsible Entity will have as evidence of reporting an event, copy of the completed EOP-004-2 Attachment 2 form or a DOE-OE-417 form; and evidence of submittal (e.g., operator log or other operating documentation, voice recording, electronic mail message, or confirmation of facsimile) demonstrating the event report was submitted within 24 hours of meeting the threshold for reporting. (R2)

Rationale for R2

Each Responsible Entity must report and communicate events according to its Operating Plan based on the information in EOP-004-2 Attachment 1. By implementing the event reporting Operating Plan the Responsible Entity will assure situational awareness to the Electric Reliability Organization so that they may develop trends and prepare for a possible next event and mitigate the current event. This will assure that the BES remains secure and stable by mitigation actions that the Responsible Entity has within its function. By communicating events per the Operating Plan, the Responsible Entity will assure that people/agencies are aware of the current situation and they may prepare to mitigate current and further events.

R3. Each Responsible Entity shall validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Each Responsible Entity will have dated records to show that it validated all contact information contained in the Operating Plan each calendar year. Such evidence may include, but are not limited to, dated voice recordings and operating logs or other communication documentation. (R3)

Rationale for R3

Requirement 3 calls for the Responsible Entity to validate the contact information contained in the Operating Plan each calendar year. This requirement helps ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization. If an entity experiences an actual event, communication evidence from the event may be used to show compliance with the validation requirement for the specific contacts used for the event.

C. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

The Regional Entity shall serve as the Compliance Enforcement Authority (CEA) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2 Evidence Retention

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain the current Operating Plan plus each version issued since the last audit for Requirements R1, and Measure M1.
- Each Responsible Entity shall retain evidence of compliance since the last audit for Requirements R2, R3 and Measure M2, M3.

If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3 Compliance Monitoring and Enforcement Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4 Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	N/A	N/A	N/A	The Responsible Entity failed to have an event reporting Operating Plan.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Assessment	Medium	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 24 hours but less than or equal to 36 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to one entity identified in its event reporting Operating Plan within 24 hours.	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 36 hours but less than or equal to 48 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to two entities identified in its event reporting Operating Plan within 24 hours.	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 48 hours but less than or equal to 60 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to three entities identified in its event reporting Operating Plan within 24 hours.	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 60 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to four or more entities identified in its event reporting Operating Plan within 24 hours. OR The Responsible Entity failed to submit a report for an event in EOP-004 Attachment 1.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Operations Planning	Medium	The Responsible Entity validated all contact information contained in the Operating Plan but was late by less than one calendar month. OR The Responsible Entity validated 75% or more of the contact information contained in the Operating Plan.	The Responsible Entity validated all contact information contained in the Operating Plan but was late by one calendar month or more but less than two calendar months. OR The Responsible Entity validated 50% and less than 75% of the contact information contained in the Operating Plan.	The Responsible Entity validated all contact information contained in the Operating Plan but was late by two calendar months or more but less than three calendar months. OR The Responsible Entity validated 25% and less than 50% of the contact information contained in the Operating Plan.	The Responsible Entity validated all contact information contained in the Operating Plan but was late by three calendar months or more. OR The Responsible Entity validated less than 25% of contact information contained in the Operating Plan.

D. Variances

None.

E. Interpretations

None.

F. References

Guideline and Technical Basis (attached)

EOP-004 - Attachment 1: Reportable Events

NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per Requirement R2 and provide as much information as is available at the time of the notification. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net or Voice: 404-446-9780.

Rationale Box for EOP-004 Attachment 1:

The DSR SDT used the defined term "Facility" to add clarity for several events listed in Attachment 1. A Facility is defined as:

> "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"

The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.

Submit EOP-004 Attachment 2 (or DOE-OE-417) pursuant to Requirements R1 and R2.

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
Damage or destruction of a Facility	RC, BA, TOP	Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in actions to avoid a BES Emergency.
Damage or destruction of a Facility	BA, TO, TOP, GO, GOP, DP	Damage or destruction of its Facility that results from actual or suspected intentional human action.
Physical threats to a Facility	BA, TO, TOP, GO, GOP, DP	Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. OR Suspicious device or activity at a Facility. Do not report theft unless it degrades normal operation of a Facility.
Physical threats to a BES control center	RC, BA, TOP	Physical threat to its BES control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. OR Suspicious device or activity at a BES control center.
BES Emergency requiring public appeal for load reduction	Initiating entity is responsible for reporting	Public appeal for load reduction event.
BES Emergency requiring system-wide voltage reduction	Initiating entity is responsible for reporting	System wide voltage reduction of 3% or more.
BES Emergency requiring manual firm load shedding	Initiating entity is responsible for reporting	Manual firm load shedding ≥ 100 MW.

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
BES Emergency resulting in automatic firm load shedding	DP, TOP	Automatic firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS).
Voltage deviation on a Facility	TOP	Observed within its area a voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes.
IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only)	RC	Operate outside the IROL for time greater than IROL T_v (all Interconnections) or Operate outside the SOL for more than 30 minutes for Major WECC Transfer Paths (WECC only).
Loss of firm load	BA, TOP, DP	Loss of firm load for ≥ 15 Minutes: ≥ 300 MW for entities with previous year's demand ≥ 3,000 MW OR ≥ 200 MW for all other entities
System separation (islanding)	RC, BA, TOP	Each separation resulting in an island ≥ 100 MW
Generation loss	BA, GOP	Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection OR ≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection
Complete loss of off-site power to a nuclear generating plant (grid supply)	TO, TOP	Complete loss of off-site power affecting a nuclear generating station per the Nuclear Plant Interface Requirement

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
Transmission loss	TOP	Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing).
Unplanned BES control center evacuation	RC, BA, TOP	Unplanned evacuation from BES control center facility for 30 continuous minutes or more.
Complete loss of voice communication capability	RC, BA, TOP	Complete loss of voice communication capability affecting a BES control center for 30 continuous minutes or more.
Complete loss of monitoring capability	RC, BA, TOP	Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (i.e., State Estimator or Contingency Analysis) is rendered inoperable.

EOP-004 - Attachment 2: Event Reporting Form

EOP-004 Attachment 2: Event Reporting Form **Use this form to report events. The Electric Reliability Organization will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net voice: 404-446-9780.**		
Task		**Comments**
1.	Entity filing the report include: Company name: Name of contact person: Email address of contact person: Telephone Number: Submitted by (name):	
2.	Date and Time of recognized event. Date: (mm/dd/yyyy) Time: (hh:mm) Time/Zone:	
3.	Did the event originate in your system?	Yes ☐ No☐ Unknown ☐
4.	**Event Identification and Description:**	
	(Check applicable box) ☐ Damage or destruction of a Facility ☐ Physical Threat to a Facility ☐ Physical Threat to a control center ☐ BES Emergency: ☐ public appeal for load reduction ☐ system-wide voltage reduction ☐ manual firm load shedding ☐ automatic firm load shedding ☐ Voltage deviation on a Facility ☐ IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only) ☐ Loss of firm load ☐ System separation ☐ Generation loss ☐ Complete loss of off-site power to a nuclear generating plant (grid supply) ☐ Transmission loss ☐ unplanned control center evacuation ☐ Complete loss of voice communication capability ☐ Complete loss of monitoring capability	Written description (optional):

Guideline and Technical Basis

Summary of Key Concepts

The DSRSDT identified the following principles to assist them in developing the standard:

- Develop a single form to report disturbances and events that threaten the reliability of the Bulk Electric System
- Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements
- Establish clear criteria for reporting
- Establish consistent reporting timelines
- Provide clarity around who will receive the information and how it will be used

During the development of concepts, the DSR SDT considered the FERC directive to "further define sabotage". There was concern among stakeholders that a definition may be ambiguous and subject to interpretation. Consequently, the DSR SDT decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was sabotage or vandalism without the intervention of law enforcement. The DSR SDT felt that attempting to define sabotage would result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard. The events listed in EOP-004 Attachment 1 were developed to provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

The types of events that are required to be reported are contained within EOP-004 Attachment 1. The DSR SDT has coordinated with the NERC Events Analysis Working Group to develop the list of events that are to be reported under this standard. EOP-004 Attachment 1 pertains to those actions or events that have impacted the Bulk Electric System. These events were previously reported under EOP-004-1, CIP-001-1 or the Department of Energy form OE-417. EOP-004 Attachment 1 covers similar items that may have had an impact on the Bulk Electric System or has the potential to have an impact and should be reported.

The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in EOP-004 Attachment 1. Real-time communication is achieved is covered in other standards. The proposed standard deals exclusively with after-the-fact reporting.

Data Gathering

The requirements of EOP-004-1 require that entities "promptly analyze Bulk Electric System disturbances on its system or facilities" (Requirement R2). The requirements of EOP-004-2 specify that certain types of events are to be reported but do not include provisions to analyze events. Events reported under EOP-004-2 may trigger further scrutiny by the ERO Events Analysis Program. If warranted, the Events Analysis Program personnel may request that more data for certain events be provided by the reporting entity or other entities that may have

experienced the event. Entities are encouraged to become familiar with the Events Analysis Program and the NERC Rules of Procedure to learn more about with the expectations of the program.

Law Enforcement Reporting

The reliability objective of EOP-004-2 is to improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of Bulk Electric System from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.

Stakeholders in the Reporting Process

- Industry
- NERC (ERO), Regional Entity
- FERC
- DOE
- NRC
- DHS – Federal
- Homeland Security- State
- State Regulators
- Local Law Enforcement
- State or Provincial Law Enforcement
- FBI
- Royal Canadian Mounted Police (RCMP)

The above stakeholders have an interest in the timely notification, communication and response to an incident at a Facility. The stakeholders have various levels of accountability and have a vested interest in the protection and response to ensure the reliability of the BES.

Present expectations of the industry under CIP-001-1a:

It has been the understanding by industry participants that an occurrence of sabotage has to be reported to the FBI. The FBI has the jurisdictional requirements to investigate acts of sabotage and terrorism. The CIP-001-1-1a standard requires a liaison relationship on behalf of the industry and the FBI or RCMP. These requirements, under the standard, of the industry have not been clear and have lead to misunderstandings and confusion in the industry as to how to demonstrate that the liaison is in place and effective. As an example of proof of compliance with Requirement R4, Responsible Entities have asked FBI Office personnel to provide, on FBI letterhead, confirmation of the existence of a working relationship to report acts of sabotage, the

number of years the liaison relationship has been in existence, and the validity of the telephone numbers for the FBI.

Coordination of Local and State Law Enforcement Agencies with the FBI

The Joint Terrorism Task Force (JTTF) came into being with the first task force being established in 1980. JTTFs are small cells of highly trained, locally based, committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. The JTTF is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. Coordination and communications largely through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs. This information flow can be most beneficial to the industry in analytical intelligence, incident response and investigation. Historically, the most immediate response to an industry incident has been local and state law enforcement agencies to suspected vandalism and criminal damages at industry facilities. Relying upon the JTTF coordination between local, state and FBI law enforcement would be beneficial to effective communications and the appropriate level of investigative response.

Coordination of Local and Provincial Law Enforcement Agencies with the RCMP

A similar law enforcement coordination hierarchy exists in Canada. Local and Provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. The Provincial law enforcement agency has a reporting relationship with the Royal Canadian Mounted Police (RCMP).

A Reporting Process Solution – EOP-004

A proposal discussed with the FBI, FERC Staff, NERC Standards Project Coordinator and the SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Reportable Events). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial or local level law enforcement agency. The state or provincial or local level law enforcement agency will coordinate with law enforcement with jurisdiction to investigate. If the state or provincial or local level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial or local level law enforcement agency will notify and coordinate with the FBI or the RCMP.

Example of Reporting Process including Law Enforcement

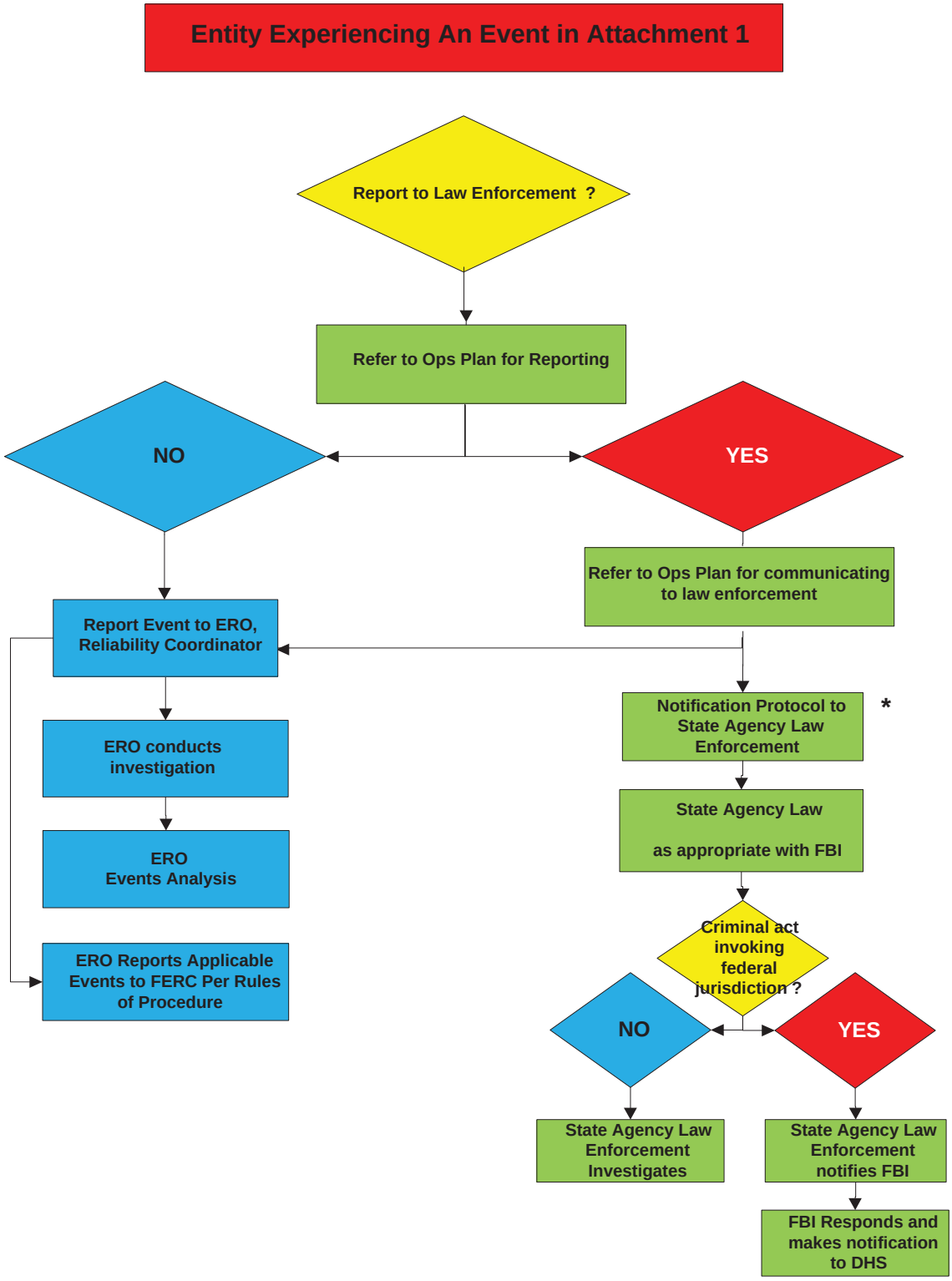

* Canadian entities will follow law enforcement protocols applicable in their jurisdictions

Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01) - Reporting Concepts

Introduction

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and has developed updated standards based on the SAR.

The standards listed under the SAR are:

- CIP-001 — Sabotage Reporting
- EOP-004 — Disturbance Reporting

The changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). These standards deal exclusively with after-the-fact reporting.

The DSR SDT has consolidated disturbance and sabotage event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts and Assumptions:

The Standard:

- Requires reporting of "events" that impact or may impact the reliability of the Bulk Electric System
- Provides clear criteria for reporting
- Includes consistent reporting timelines
- Identifies appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- Provides clarity around of who will receive the information

Discussion of Disturbance Reporting

Disturbance reporting requirements existed in the previous version of EOP-004. The current approved definition of Disturbance from the NERC Glossary of Terms is:

1. An unplanned event that produces an abnormal system condition.
2. Any perturbation to the electric system.
3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.

Disturbance reporting requirements and criteria were in the previous EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and developed the list of events that are to be reported under this standard (EOP-004 Attachment 1).

Discussion of Event Reporting
There are situations worthy of reporting because they have the potential to impact reliability.

Event reporting facilitates industry awareness, which allows potentially impacted parties to prepare for and possibly mitigate any associated reliability risk. It also provides the raw material, in the case of certain potential reliability threats, to see emerging patterns.

Examples of such events include:

- Bolts removed from transmission line structures
- Train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center)
- Destruction of Bulk Electric System equipment

What about sabotage?
One thing became clear in the DSR SDT's discussion concerning sabotage: everyone has a different definition. The current standard CIP-001 elicited the following response from FERC in FERC Order 693, paragraph 471 which states in part: *". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."*

Often, the underlying reason for an event is unknown or cannot be confirmed. The DSR SDT believes that by reporting material risks to the Bulk Electric System using the event categorization in this standard, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.

Certain types of events should be reported to NERC, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and/or Provincial or local law enforcement. Other types of events may have different reporting requirements. For example, an event that is related to copper theft may only need to be reported to the local law enforcement authorities.

Potential Uses of Reportable Information
Event analysis, correlation of data, and trend identification are a few potential uses for the information reported under this standard. The standard requires Functional entities to report the incidents and provide known information at the time of the report. Further data gathering necessary for event analysis is provided for under the Events Analysis Program and the NERC Rules of Procedure. Other entities (e.g. – NERC, Law Enforcement, etc) will be responsible for performing the analyses. The NERC Rules of Procedure (section 800) provide an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for

reliability. Jurisdictional agencies (which may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE) have other duties and responsibilities.

Collection of Reportable Information or "One stop shopping"

The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT has updated the listing of reportable events in EOP-004 Attachment 1 based on discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences still exist.

The reporting required by this standard is intended to meet the uses and purposes of NERC. The DSR SDT recognizes that other requirements for reporting exist (e.g., DOE-417 reporting), which may duplicate or overlap the information required by NERC. To the extent that other reporting is required, the DSR SDT envisions that duplicate entry of information should not be necessary, and the submission of the alternate report will be acceptable to NERC so long as all information required by NERC is submitted. For example, if the NERC Report duplicates information from the DOE form, the DOE report may be sent to the NERC in lieu of entering that information on the NERC report.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SC approved SAR for initial posting (April, 2009).
2. SAR posted for comment (April 22 – May 21, 2009).
3. SC authorized moving the SAR forward to standard development (September 2009).
4. Concepts Paper posted for comment (March 17 – April 16, 2010).
5. Initial Informal Comment Period (September 15 – October 15, 2010)
6. Second Comment Period (Formal) (March 9 – April 8, 2011)
7. Third Comment Period and Initial Ballot (October 28 – December 12, 2011)

~~7.~~8.Fourth Comment Period and Successive Ballot (April 25 – May 24, 2012).

Proposed Action Plan and Description of Current Draft

This is the fifth~~ourth~~ posting of the proposed standard in accordance with Results-Based Criteria. The drafting team requests posting for a 30-day formal comment period concurrent with the formation of the ballot pool and the successive ballot.

Future Development Plan

Anticipated Actions	Anticipated Date
Drafting team considers comments, makes conforming changes on fourth~~third~~ posting	June~~anuary~~ - August~~March~~ 2012
Fourth Comment/Ballot period	~~March – April~~August - September 2012
Recirculation Ballot period	October~~May~~ 2012
Receive BOT approval	November~~June~~ 2012
File with regulatory authorities	December~~August~~ 2012

Effective Dates

~~EOP-004-2 shall become effective on t~~The first day of the first ~~third~~ calendar quarter that is six months beyond the date that this standard is approved by ~~after~~ applicable regulatory authorities~~pproval~~. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the first ~~third~~ calendar quarter that is six months beyond the date this standard is approved by the ~~after~~ NERC Board of Trustees ~~approval~~, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-2a Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2 Event Reporting; Retire CIP-001-2a Sabotage Reporting and Retired EOP-004-1 Disturbance Reporting. Retire CIP-008-3, Requirement 1, Part 1.3.	Revision to entire standard (Project 2009-01)

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

When this standard has received ballot approval, the text boxes will be moved to the Guideline and Technical Basis Section.

A. Introduction

1. Title: Event Reporting

2. Number: EOP-004-2

3. Purpose: To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities.

4. Applicability

4.1. Functional Entities: Within the context of EOP-004-2, the term "Responsible Entity" shall include the following entities as shown in EOP-004 Attachment 1:

4.1.1. Reliability Coordinator

4.1.2. Balancing Authority

~~4.1.3. Interchange Coordinator~~

~~4.1.4. Transmission Service Provider~~

~~4.1.5.~~4.1.3. Transmission Owner

~~4.1.6.~~4.1.4. Transmission Operator

~~4.1.7.~~4.1.5. Generator Owner

~~4.1.8.~~4.1.6. Generator Operator

~~4.1.9.~~4.1.7. Distribution Provider

~~4.1.10. Load Serving Entity~~

~~4.1.11. Electric Reliability Organization~~

~~4.1.12. Regional Entity~~

5. Background:

NERC established a SAR Team in 2009 to investigate and propose revisions to the CIP-001 and EOP-004 Reliability Standards. The team was asked to consider the following:

1. CIP-001 could be merged with EOP-004 to eliminate redundancies.
2. Acts of sabotage have to be reported to the DOE as part of EOP-004.
3. Specific references to the DOE form need to be eliminated.
4. EOP-004 had some 'fill-in-the-blank' components to eliminate.

The development included other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient Bulk Electric System reliability standards.

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC SC in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009.

The DSR SDT developed a concept paper to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT had developed. The posting of the concept paper sought comments from stakeholders on the "road map" that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the DSR SDT. The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC issues database and FERC Order 693 Directives in order to determine a prudent course of action with respect to revision of these standards.

~~**Summary of Key Concepts**~~

~~The DSRSDT identified the following principles to assist them in developing the standard:~~

- ~~Develop a single form to report disturbances and events that threaten the reliability of the Bulk Electric System~~
- ~~Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements~~
- ~~Establish clear criteria for reporting~~
- ~~Establish consistent reporting timelines~~
- ~~Provide clarity around who will receive the information and how it will be used~~

~~During the development of concepts, the DSR SDT considered the FERC directive to "further define sabotage". There was concern among stakeholders that a definition may be ambiguous and subject to interpretation. Consequently, the DSR SDT decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was sabotage or vandalism without the intervention of law enforcement. The DSR SDT felt that attempting to define sabotage would result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard. The events listed in EOP-004 Attachment 1 were developed to provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.~~

~~The types of events that are required to be reported are contained within EOP-004 Attachment 1. The DSR SDT has coordinated with the NERC Events Analysis Working Group to develop the list of events that are to be reported under this standard. EOP-004 Attachment 1 pertains to those actions or events that have impacted the Bulk Electric System. These events were previously reported under EOP-004-1, CIP-001-1 or the Department of Energy form OE-417. EOP-004 Attachment 1 covers similar items that may have had an impact on the Bulk Electric System or has the potential to have an impact and should be reported.~~

~~The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in EOP-004 Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting.~~

~~Data Gathering~~

~~The requirements of EOP-004-1 require that entities "promptly analyze Bulk Electric System disturbances on its system or facilities" (Requirement R2). The requirements of EOP-004-2 specify that certain types of events are to be reported but do not include provisions to analyze events. Events reported under EOP-004-2 may trigger further scrutiny by the ERO Events Analysis Program. If warranted, the Events Analysis Program personnel may request that more data for certain events be provided by the reporting entity or other entities that may have experienced the event. Entities are encouraged to become familiar with the Events Analysis Program and the NERC Rules of Procedure to learn more about with the expectations of the program.~~

~~Law Enforcement Reporting~~

~~The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of Bulk Electric System from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.~~

~~Stakeholders in the Reporting Process~~

- ~~Industry~~
- ~~NERC (ERO), Regional Entity~~
- ~~FERC~~
- ~~DOE~~
- ~~NRC~~
- ~~DHS – Federal~~
- ~~Homeland Security- State~~
- ~~State Regulators~~
- ~~Local Law Enforcement~~
- ~~State or Provincial Law Enforcement~~
- ~~FBI~~
- ~~Royal Canadian Mounted Police (RCMP)~~

~~The above stakeholders have an interest in the timely notification, communication and response to an incident at an industry facility. The stakeholders have various levels of accountability and have a vested interest in the protection and response to ensure the reliability of the BES.~~

~~**Present expectations of the industry under CIP-001-1a:**~~

~~It has been the understanding by industry participants that an occurrence of sabotage has to be reported to the FBI. The FBI has the jurisdictional requirements to investigate acts of sabotage and terrorism. The CIP-001-1-1a standard requires a liaison relationship on behalf of the industry and the FBI or RCMP. Annual requirements, under the standard, of the industry have not been clear and have lead to misunderstandings and confusion in the industry as to how to demonstrate that the liaison is in place and effective. As an example of proof of compliance with Requirement R4, responsible entities have asked FBI Office personnel to provide, on FBI letterhead, confirmation of the existence of a working relationship to report acts of sabotage, the number of years the liaison relationship has been in existence, and the validity of the telephone numbers for the FBI.~~

~~**Coordination of Local and State Law Enforcement Agencies with the FBI**~~

~~The Joint Terrorism Task Force (JTTF) came into being with the first task force being established in 1980. JTTFs are small cells of highly trained, locally based, committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. The JTTF is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. Coordination and communications largely through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs. This information flow can be most beneficial to the industry in analytical intelligence, incident response and investigation. Historically, the most immediate response to an industry incident has been local and state law enforcement agencies to suspected vandalism and criminal damages at industry facilities. Relying upon the JTTF coordination between local, state and FBI law enforcement would be beneficial to effective communications and the appropriate level of investigative response.~~

~~**Coordination of Local and Provincial Law Enforcement Agencies with the RCMP**~~

~~A similar law enforcement coordination hierarchy exists in Canada. Local and Provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. The Provincial law enforcement agency has a reporting relationship with the Royal Canadian Mounted Police (RCMP).~~

~~A Reporting Process Solution – EOP-004~~

~~A proposal discussed with the FBI, FERC Staff, NERC Standards Project Coordinator and the SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Reportable Events). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial or local level law enforcement agency. The state or provincial or local level law enforcement agency will coordinate with law enforcement with jurisdiction to investigate. If the state or provincial or local level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial or local level law enforcement agency will notify and coordinate with the FBI or the RCMP.~~

Example of Reporting Process including Law Enforcement

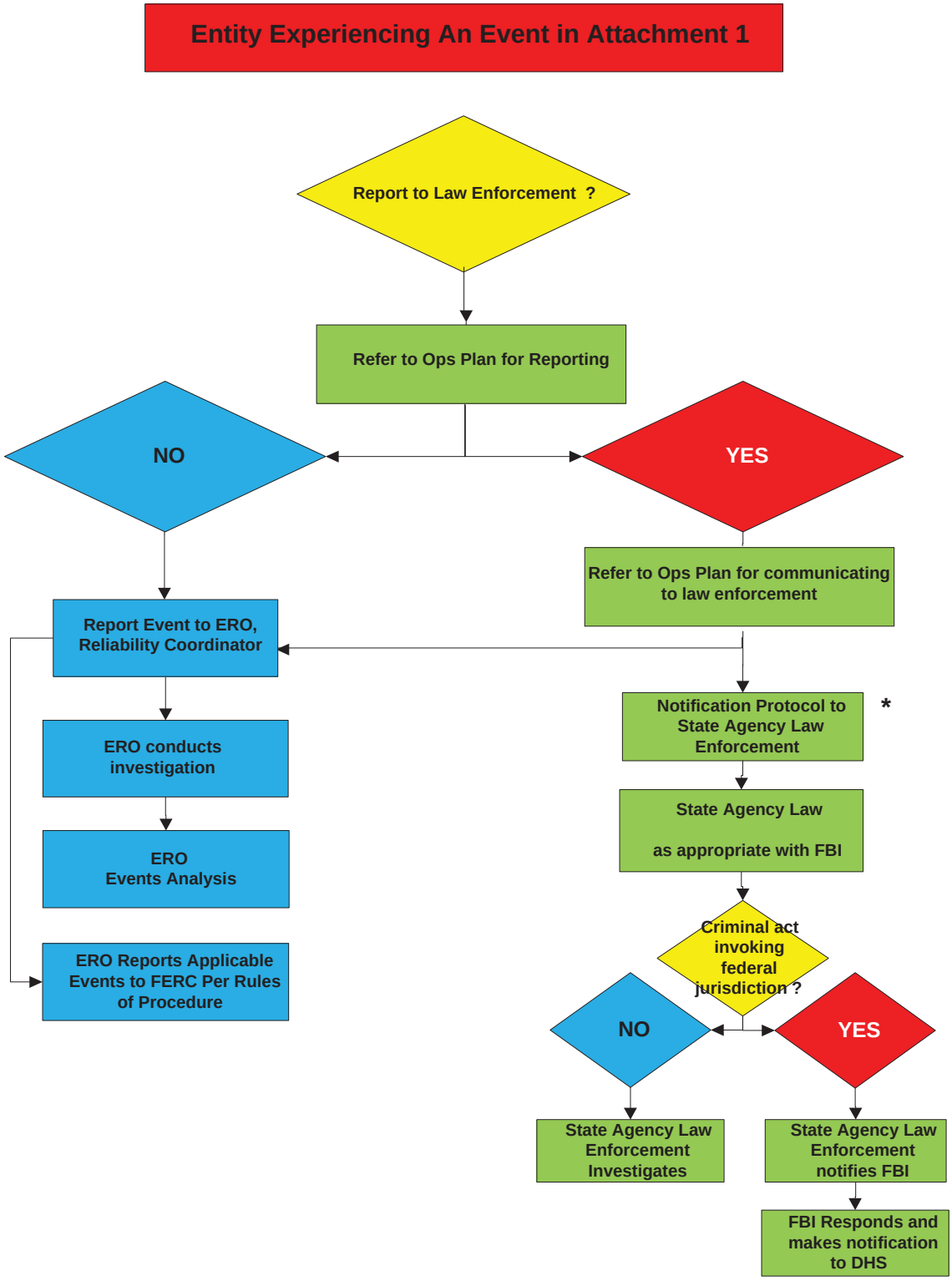

* Canadian entities will follow law enforcement protocols applicable in their jurisdictions

B. Requirements and Measures

R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the regional entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority).~~that includes:~~ *[Violation Risk: Factor: Lower] [Time Horizon: Operations Planning]*

~~1.1. A process for recognizing each of the applicable events listed in EOP-004 Attachment 1(except for Cyber Security Incidents characterized and classified according to the requirements in CIP-008-3 or its successor).~~

~~1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies.~~

Rationale for R1

The requirement to have an Operating Plan for reporting specific types of events provides the entity with a method to have its operating personnel recognize events that affect reliability and to be able to report them to appropriate parties; i.e. Regional Entities, applicable Reliability Coordinators, and law enforcement and other jurisdictional agencies when so recognized. In addition, these event reports are an input to the NERC Events Analysis Program. These other parties use this information to promote reliability, develop a culture of reliability excellence, provide industry collaboration and promote a learning organization.

Every industry participant that owns or operates elements or devices on the grid has a formal or informal process, procedure, or steps it takes to gather information regarding what happened when events occur. This requirement has the Responsible Entity establish documentation on how that procedure, process, or plan is organized. This documentation may be a single document or a combination of various documents that achieve the reliability objective.

~~Part 1.1 clarifies that entities must address each of the "applicable" events listed in EOP-004 Attachment 1. Not all responsible entities must address all events; e.g., some events are only applicable to the Reliability Coordinator. Part 1.1 acknowledges that Cyber Security Incidents are characterized and classified according to the requirements in CIP-008-3.~~

~~Part 1.2~~The protocol(s) could include a process flowchart, identification of internal and external personnel or entities to be notified, or a list of personnel by name and their associated contact information.

An existing procedure that meets the requirements of CIP-001-2a may be included in this Operating Plan along with other processes, procedures or plans to meet this requirement.

M1. Each Responsible Entity will have a current, dated, event reporting Operating Plan that includes, but is not limited to the protocol(s)~~, thresholds for reporting,~~ and each organization identified to receive an event report for event types specified in EOP-004-2 Attachment 1 and in accordance with the entity responsible for reporting~~which includes Parts 1.1 – 1.2~~.

R2. Each Responsible Entity shall report ~~implement its~~ events per their ~~reporting~~ Operating Plan within 24 hours of meeting an event type threshold for reporting~~for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1~~. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

M2. Each Responsible Entity will have as evidence of reporting an event, copy of the completed EOP-004-2 Attachment 2 form or a DOE-OE-417 form; and evidence of submittal (e.g., operator log or other operating documentation, voice recording, electronic mail message, or confirmation of facsimile) demonstrating the event report was submitted within 24 hours of meeting the threshold for reporting~~, for each event experienced, a dated copy of the completed EOP-004 Attachment 2 form or DOE form OE-417 report submitted for that event; and dated and time-stamped transmittal records to show that the event was reported supplemented by operator logs or other operating documentation. Other forms of evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other operating documentation for situations where filing a written report was not possible~~. (R2)

R3. Each Responsible Entity shall validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year~~conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2~~. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Rationale for R2

Each Responsible Entity must report and communicate events according to its Operating Plan after the fact based on the information in EOP-004 Attachment 1. By implementing the event reporting Operating Plan, the Responsible Entity will assure situational awareness to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies as deemed necessary by the Registered Entity. By communicating events per the Operating Plan, the Responsible Entity will assure that people/agencies are aware of the current situation and they may prepare to mitigate current and further events.

Rationale for R3 ~~and R4~~

Requirement~~s~~ 3 ~~and 4~~ calls for the Responsible Entity to validate the contact information contained in the Operating Plan each calendar year. This requirement helps ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization. If an entity experiences an actual event, communication evidence from the event may be used to show compliance with the validation requirement for the specific contacts used for the event~~annual test of the communications process in Part 1.2 as well as an annual review of the event reporting Operating Plan. These two requirements help ensure that the event reporting Operating Plan is up to date and entities will be effective in reporting events to assure situational awareness to the Electric Reliability Organization and their Reliability Coordinator . This will assure that the BES remains secure and stable by mitigation actions that the Reliability Coordinator has within its function~~.

M3. Each Responsible Entity will have dated records to show that it validated all contact information contained in the Operating Plan each calendar year. Such evidence may include, but are not limited to, dated voice recordings and operating logs or other communication documentation~~and time-stamped records to show that the annual test of Part 1.2 was conducted. Such evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other communication documentation. The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event~~. (R3)

~~**R4**. Each Responsible Entity shall conduct an annual review of the event reporting Operating Plan in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*~~

~~**M4.** Each Responsible Entity will have dated and time-stamped records to show that the annual review of the event reporting Operating Plan was conducted. Such evidence may include, but are not limited to, the current document plus the 'date change page' from each version that was reviewed. (R4)~~

C. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

The Regional Entity shall serve as the Compliance E~~e~~nforcement A~~a~~uthority (CEA) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~e~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

~~For NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.~~

1.2 Evidence Retention

The [responsible entity] shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:
The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to

provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain the current Operating Plan plus each version issued since the last audit for Requirements R1, and Measure M1.
- Each Responsible Entity shall retain evidence of compliance since the last audit for Requirements R2, R3 and Measure M2, M3.

~~Each Responsible Entity shall retain the current, document plus the 'date change page' from each version issued since the last audit for Requirements R1, R4 and Measures M1, M4.~~

~~Each Responsible Entity shall retain evidence from prior 3 calendar years for Requirements R2, R3 and Measure M2, M3.~~

If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3 Compliance Monitoring and Enforcement Processes:

Compliance Audit
Self-Certification
Spot Checking
Compliance Investigation
Self-Reporting
Complaint

1.4 Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	N/A	N/A	~~The Responsible Entity has an event reporting Operating Plan but failed to include one of Parts 1.1 through 1.2.~~N/A	The Responsible Entity failed to include both Parts 1.1 and 1.2.
R2	Operations Assessment	Medium	The Responsible Entity submitted a report (e.g., written or verbal) to all required recipients more than 24 hours but less than or equal to 36 hours after meeting an event threshold for reporting~~an event requiring reporting within 24 hours in EOP-004 Attachment 1~~. OR The Responsible Entity	The Responsible Entity submitted a report (e.g., written or verbal) to all required recipients more than 36 hours but less than or equal to 48 hours after meeting an event threshold for reporting~~an event requiring reporting within 24 hours in EOP-004 Attachment 1~~. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to	The Responsible Entity submitted a report (e.g., written or verbal) to all required recipients more than 48 hours but less than or equal to 60 hours after meeting an event threshold for reporting ~~an event requiring reporting within 24 hours in EOP-004 Attachment 1~~. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to three entities identified	The Responsible Entity submitted a report (e.g., written or verbal) to all required recipients more than 60 hours after meeting an event threshold for reporting~~an event requiring reporting within 24 hours in EOP-004 Attachment 1~~. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to four or more entities identified in its event

			submitted an event report (e.g., written or verbal) to one entity identified in the event report Operating Plan within 24 hours. ~~in the appropriate timeframe but failed to provide all of the required information.~~	two entities identified in its event reporting Operating Plan within 24 hours..~~The Responsible Entity submitted a report more than 1 hour but less than 2 hours after an event requiring reporting within 1 hour in EOP-004 Attachment 1.~~	in its event reporting Operating Plan within 24 hours.~~The Responsible Entity submitted a report in more than 2 hours but less than 3 hours after an event requiring reporting within 1 hour in EOP-004 Attachment 1.~~	reporting Operating Plan within 24 hours.~~The Responsible Entity submitted a report more than 3 hours after an event requiring reporting within 1 hour in EOP-004 Attachment 1.~~ OR The Responsible Entity failed to submit a report for an event in EOP-004 Attachment 1.
R3	Operations Planning	Medium	The Responsible Entity validated all contact information contained in the Operating Plan but was late by less than one calendar month. OR The Responsible Entity validated 75% or more of the contact information contained in the Operating Plan. ~~The Responsible Entity performed the annual test of the~~	The Responsible Entity validated all contact information contained in the Operating Plan but was late by one calendar month or more but less than two calendar months. OR The Responsible Entity validated 50% and less than 75% of the contact information contained in the Operating Plan.~~The Responsible Entity~~	The Responsible Entity validated all contact information contained in the Operating Plan but was late by two calendar months or more but less than three calendar months. OR The Responsible Entity validated 25% and less than 50% of the contact information contained in the Operating Plan. ~~The Responsible Entity~~	The Responsible Entity validated all contact information contained in the Operating Plan but was late by three calendar months or more. OR The Responsible Entity validated less than 25% of contact information contained in the Operating Plan. ~~The Responsible Entity performed the annual test of the~~

			~~communications process in Part 1.2 but was late by less than one calendar month.~~	~~performed the annual test of the communications process in Part 1.2 but was late by one calendar month or more but less than two calendar months.~~	~~performed the annual test of the communications process in Part 1.2 but was late by two calendar months or more but less than three calendar months.~~	~~communications process in Part 1.2 but was late by three calendar months or more.~~ ~~OR~~ ~~The Responsible Entity failed to perform the annual test of the communications process in Part 1.2.~~
~~**R4**~~	~~Operations Planning~~	~~Medium~~	~~The Responsible Entity performed the annual review of the event reporting Operating Plan but was late by less than one calendar month.~~	~~The Responsible Entity performed the annual review of the event reporting Operating Plan but was late by one calendar month or more but less than two calendar months.~~	~~The Responsible Entity performed the annual review of the event reporting Operating Plan but was late by two calendar months or more but less than three calendar months.~~	~~The Responsible Entity performed the annual review of the event reporting Operating Plan but was late by three calendar months or more.~~ ~~OR~~ ~~The Responsible Entity failed to perform the annual review of the event reporting Operating Plan~~

D. Variances

None.

E. Interpretations

None.

F. References~~Interpretations~~

Guideline and Technical Basis (attached).

EOP-004 - Attachment 1: Reportable Events

NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per Requirement R1 and provide as much information as is available at the time of the notification. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net or Voice: 404-446-9780.~~esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422~~.

~~**One Hour Reporting: Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the event.**~~

~~Event~~	~~Entity with Reporting Responsibility~~	~~Threshold for Reporting~~
~~A reportable Cyber Security Incident.~~	~~Each Responsible Entity applicable under CIP-008-3 or its successor that experiences the Cyber Security Incident~~	~~That meets the criteria in CIP-008-3 or its successor~~

Rationale Box for EOP-004 Attachment 1:

The DSR SDT used the defined term "Facility" to add clarity for several events listed in Attachment 1. A Facility is defined as:

> "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"

The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.

~~Twenty-four Hour Reporting:~~ Submit EOP-004 Attachment 2 or DOE-OE-417 report ~~to the parties identified~~ pursuant to Requirements R1 and R2~~, Part 1.2 within twenty-four hours of recognition of the event~~.

Event	Entity with Reporting Responsibility	Threshold for Reporting
Damage or destruction of a Facility	~~Each~~ RC, BA, TO~~, TO~~P~~, GO, GOP, DP that experiences the damage or destruction of a Facility~~	Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in actions to avoid a BES Emergency.~~Damage or destruction of a Facility that:~~ ~~Affects an IROL (per FAC-014)~~ ~~OR~~ ~~Results in the need for actions to avoid an Adverse Reliability Impact~~ ~~OR~~ ~~Results from actual or suspected intentional human action.~~
Damage or destruction of a Facility	BA, TO, TOP, GO, GOP, DP	Damage or destruction of its Facility that results from actual or suspected intentional human action.
~~Any p~~Physical threats to ~~that could impact the operability of~~ a Facility[1]	~~Each RC,~~ BA, TO, TOP, GO, GOP, DP ~~that experiences the event~~	Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. OR Suspicious device or activity at a Facility. Do not report theft unless it degrades normal operation of a

~~[1] Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility.~~

Event	Entity with Reporting Responsibility	Threshold for Reporting
		Facility.~~Threat to a Facility excluding weather related threats.~~
Physical threats to a BES control center	RC, BA, TOP	Physical threat to its BES control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. OR Suspicious device or activity at a BES control center.
BES Emergency requiring public appeal for load reduction	Initiating entity is responsible for reporting	Public appeal for load reduction event
BES Emergency requiring system-wide voltage reduction	Initiating entity is responsible for reporting	System wide voltage reduction of 3% or more
BES Emergency requiring manual firm load shedding	Initiating entity is responsible for reporting	Manual firm load shedding ≥ 100 MW
BES Emergency resulting in automatic firm load shedding	~~Each~~ DP, ~~or~~ TOP ~~that implements automatic load shedding~~	Automatic f~~F~~irm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)
Voltage deviation on a Facility	~~Each~~ TOP ~~that observes the voltage deviation~~	Observed within its area a voltage deviation of ± 10% sustained for ≥ 15 continuous minutes
IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only)	~~Each~~ RC ~~that experiences the IROL Violation (all Interconnections) or SOL violation for Major WECC Transfer Paths (WECC only)~~	Operate outside the IROL for time greater than IROL T_v (all Interconnections) or Operate outside the SOL for more than 30 minutes for Major WECC Transfer Paths (WECC only).
Loss of firm load ~~for ≥ 15 Minutes~~	~~Each~~ BA, TOP, DP ~~that experiences the loss of firm load~~	Loss of firm load for ≥ 15 Minutes: • ≥ 300 MW for entities with previous year's demand ≥ 3,000 MW • ≥ 200 MW for all other entities

Event	Entity with Reporting Responsibility	Threshold for Reporting
System separation (islanding)	~~Each~~ RC, BA, TOP, DP ~~that experiences the system separation~~	Each separation resulting in an island ~~of generation and load~~ ≥ 100 MW
Generation loss	~~Each~~ BA, GOP ~~that experiences the generation loss~~	Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection OR ≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection
Complete loss of off-site power to a nuclear generating plant (grid supply)	~~Each~~ TO, TOP ~~that experiences the complete loss of off-site power to a nuclear generating plant~~	Complete loss of off-site power a~~A~~ffecting a nuclear generating station per the Nuclear Plant Interface Requirement
Transmission loss	~~Each~~ TOP ~~that experiences the transmission loss~~	Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance ~~Unintentional loss of three or more Transmission Facilities~~ (excluding successful automatic reclosing)
Unplanned control center evacuation	~~Each~~ RC, BA, TOP ~~that experiences the event~~	Unplanned evacuation from BES control center facility for 30 minutes or more.
Complete ~~L~~loss of ~~all~~ voice communication capability	~~Each~~ RC, BA, TOP ~~that experiences the loss of all voice communication capability~~	Complete loss of voice communication capability a~~A~~ffecting a BES control center for ≥ 30 continuous minutes
Complete ~~or partial~~ loss of monitoring capability	~~Each~~ RC, BA, TOP ~~that experiences the complete or partial loss of monitoring capability~~	Complete loss of monitoring capability a~~A~~ffecting a BES control center for ≥ 30 continuous minutes such that analysis tools (i.e., State Estimator or~~,~~ Contingency Analysis) are rendered inoperable.

EOP-004 - Attachment 2: Event Reporting Form

EOP-004 Attachment 2: Event Reporting Form

Use this form to report events. The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net voice: 404-446-9780~~**esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422**~~**.**

	Task	Comments
1.	Entity filing the report include: Company name: Name of contact person: Email address of contact person: Telephone Number: Submitted by (name):	
2.	Date and Time of recognized event. Date: (mm/dd/yyyy) Time: (hh:mm) Time/Zone:	
3.	Did the event originate in your system?	Yes ☐ No☐ Unknown ☐
4.	**Event Identification and Description:**	
	(Check applicable box) ☐ Damage or destruction of a Facility ☐ Physical Threat to a Facility ☐ Physical Threat to a control center ☐ BES Emergency: ☐ public appeal for load reduction ☐ system-wide voltage reduction ☐ manual firm load shedding ☐ automatic firm load shedding ☐ Voltage deviation on a Facility ☐ IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only) ☐ Loss of firm load ☐ System separation ☐ Generation loss ☐ Complete loss of off-site power to a nuclear generating plant (grid supply) ☐ Transmission loss ☐ unplanned control center evacuation ☐ Complete loss of voice communication capability ☐ Complete loss of monitoring capability ~~(Check applicable box)~~ ~~☐ public appeal~~	Written description (optional):

EOP-004 Attachment 2: Event Reporting Form

Use this form to report events. The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net voice: 404-446-9780**~~esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422~~.**

	Task	Comments
	☐ ~~voltage reduction~~ ☐ ~~manual firm load shedding~~ ☐ ~~firm load shedding(undervoltage, underfrequency, SPS/RAS)~~ ☐ ~~voltage deviation~~ ☐ ~~IROL violation~~ ☐ ~~loss of firm load~~ ☐ ~~system separation (islanding)~~ ☐ ~~generation loss~~ ☐ ~~complete loss of off-site power to nuclear generating plant~~ ☐ ~~transmission loss~~ ☐ ~~damage or destruction of Facility~~ ☐ ~~unplanned control center evacuation~~ ☐ ~~loss of all voice communication capability~~ ☐ ~~complete or partial loss of monitoring capability~~ ☐ ~~physical threat that could impact the operability of a Facility~~ ☐ ~~reportable Cyber Security Incident~~	

Guideline and Technical Basis

Summary of Key Concepts

The DSRSDT identified the following principles to assist them in developing the standard:

- Develop a single form to report disturbances and events that threaten the reliability of the Bulk Electric System
- Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements
- Establish clear criteria for reporting
- Establish consistent reporting timelines
- Provide clarity around who will receive the information and how it will be used

During the development of concepts, the DSR SDT considered the FERC directive to "further define sabotage". There was concern among stakeholders that a definition may be ambiguous and subject to interpretation. Consequently, the DSR SDT decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was sabotage or vandalism without the intervention of law enforcement. The DSR SDT felt that attempting to define sabotage would result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard. The events listed in EOP-004 Attachment 1 were developed to provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

The types of events that are required to be reported are contained within EOP-004 Attachment 1. The DSR SDT has coordinated with the NERC Events Analysis Working Group to develop the list of events that are to be reported under this standard. EOP-004 Attachment 1 pertains to those actions or events that have impacted the Bulk Electric System. These events were previously reported under EOP-004-1, CIP-001-1 or the Department of Energy form OE-417. EOP-004 Attachment 1 covers similar items that may have had an impact on the Bulk Electric System or has the potential to have an impact and should be reported.

The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in EOP-004 Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting.

Data Gathering

The requirements of EOP-004-1 require that entities "promptly analyze Bulk Electric System disturbances on its system or facilities" (Requirement R2). The requirements of EOP-004-2 specify that certain types of events are to be reported but do not include provisions to analyze events. Events reported under EOP-004-2 may trigger further scrutiny by the ERO Events Analysis Program. If warranted, the Events Analysis Program personnel may request that more data for certain events be provided by the reporting entity or other entities that may have

experienced the event. Entities are encouraged to become familiar with the Events Analysis Program and the NERC Rules of Procedure to learn more about with the expectations of the program.

Law Enforcement Reporting

The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of Bulk Electric System from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.

Stakeholders in the Reporting Process

- Industry
- NERC (ERO), Regional Entity
- FERC
- DOE
- NRC
- DHS – Federal
- Homeland Security- State
- State Regulators
- Local Law Enforcement
- State or Provincial Law Enforcement
- FBI
- Royal Canadian Mounted Police (RCMP)

The above stakeholders have an interest in the timely notification, communication and response to an incident at an industry facility. The stakeholders have various levels of accountability and have a vested interest in the protection and response to ensure the reliability of the BES.

Present expectations of the industry under CIP-001-1a:

It has been the understanding by industry participants that an occurrence of sabotage has to be reported to the FBI. The FBI has the jurisdictional requirements to investigate acts of sabotage and terrorism. The CIP-001-1-1a standard requires a liaison relationship on behalf of the industry and the FBI or RCMP. Annual requirements, under the standard, of the industry have not been clear and have lead to misunderstandings and confusion in the industry as to how to demonstrate that the liaison is in place and effective. As an example of proof of compliance with Requirement R4, responsible entities have asked FBI Office personnel to provide, on FBI letterhead, confirmation of the existence of a working relationship to report acts of sabotage, the

number of years the liaison relationship has been in existence, and the validity of the telephone numbers for the FBI.

Coordination of Local and State Law Enforcement Agencies with the FBI

The Joint Terrorism Task Force (JTTF) came into being with the first task force being established in 1980. JTTFs are small cells of highly trained, locally based, committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. The JTTF is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. Coordination and communications largely through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs. This information flow can be most beneficial to the industry in analytical intelligence, incident response and investigation. Historically, the most immediate response to an industry incident has been local and state law enforcement agencies to suspected vandalism and criminal damages at industry facilities. Relying upon the JTTF coordination between local, state and FBI law enforcement would be beneficial to effective communications and the appropriate level of investigative response.

Coordination of Local and Provincial Law Enforcement Agencies with the RCMP

A similar law enforcement coordination hierarchy exists in Canada. Local and Provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. The Provincial law enforcement agency has a reporting relationship with the Royal Canadian Mounted Police (RCMP).

A Reporting Process Solution – EOP-004

A proposal discussed with the FBI, FERC Staff, NERC Standards Project Coordinator and the SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Reportable Events). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial or local level law enforcement agency. The state or provincial or local level law enforcement agency will coordinate with law enforcement with jurisdiction to investigate. If the state or provincial or local level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial or local level law enforcement agency will notify and coordinate with the FBI or the RCMP.

Example of Reporting Process including Law Enforcement

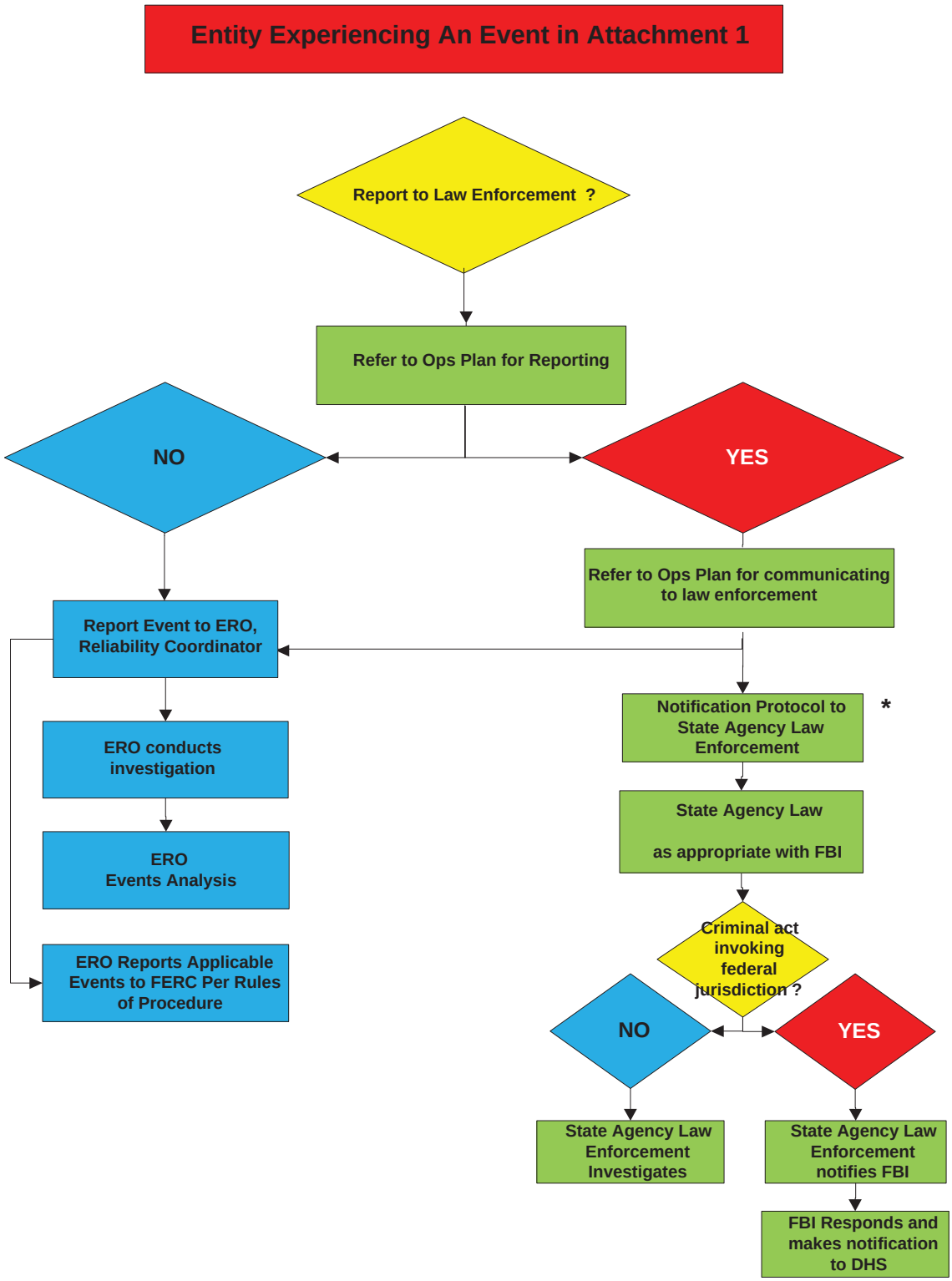

* Canadian entities will follow law enforcement protocols applicable in their jurisdictions

Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01) - Reporting Concepts

Introduction

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and has developed updated standards based on the SAR.

The standards listed under the SAR are:

- CIP-001 — Sabotage Reporting
- EOP-004 — Disturbance Reporting

The changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). These standard deals exclusively with after-the-fact reporting.

The DSR SDT has consolidated disturbance and sabotage event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts and Assumptions:

The Standard:

- Requires reporting of "events" that impact or may impact the reliability of the Bulk Electric System
- Provides clear criteria for reporting
- Includes consistent reporting timelines
- Identifies appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- Provides clarity around of who will receive the information

Discussion of Disturbance Reporting

Disturbance reporting requirements existed in the previous version of EOP-004. The current approved definition of Disturbance from the NERC Glossary of Terms is:

1. An unplanned event that produces an abnormal system condition.
2. Any perturbation to the electric system.
3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.

Disturbance reporting requirements and criteria were in the previous EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and developed the list of events that are to be reported under this standard (EOP-004 Attachment 1).

Discussion of Event Reporting
There are situations worthy of reporting because they have the potential to impact reliability.

Event reporting facilitates industry awareness, which allows potentially impacted parties to prepare for and possibly mitigate any associated reliability risk. It also provides the raw material, in the case of certain potential reliability threats, to see emerging patterns.

Examples of such events include:

- Bolts removed from transmission line structures
- ~~Detection of cyber intrusion that meets criteria of CIP-008-3 or its successor standard~~
- ~~Forced intrusion attempt at a substation~~
- Train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center)~~near a transmission right-of-way~~
- Destruction of Bulk Electric System equipment

What about sabotage?
One thing became clear in the DSR SDT's discussion concerning sabotage: everyone has a different definition. The current standard CIP-001 elicited the following response from FERC in FERC Order 693, paragraph 471 which states in part: *". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."*

Often, the underlying reason for an event is unknown or cannot be confirmed. The DSR SDT believes that by reporting material risks to the Bulk Electric System using the event categorization in this standard, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.

Certain types of events should be reported to NERC, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and/or Provincial or local law enforcement. Other types of events may have different reporting requirements. For example, an event that is related to copper theft may only need to be reported to the local law enforcement authorities.

Potential Uses of Reportable Information
Event analysis, correlation of data, and trend identification are a few potential uses for the information reported under this standard. The standard requires Functional entities to report the incidents and provide known information at the time of the report. Further data gathering necessary for event analysis is provided for under the Events Analysis Program and the NERC Rules of Procedure. Other entities (e.g. – NERC, Law Enforcement, etc) will be responsible for

performing the analyses. The NERC Rules of Procedure (section 800) provide an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for reliability. Jurisdictional agencies (which may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE) have other duties and responsibilities.

Collection of Reportable Information or "One stop shopping"

The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT has updated the listing of reportable events in EOP-004 Attachment 1 based on discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences still exist.

The reporting required by this standard is intended to meet the uses and purposes of NERC. The DSR SDT recognizes that other requirements for reporting exist (e.g., DOE-417 reporting), which may duplicate or overlap the information required by NERC. To the extent that other reporting is required, the DSR SDT envisions that duplicate entry of information should not be necessary, and the submission of the alternate report will be acceptable to NERC so long as all information required by NERC is submitted. For example, if the NERC Report duplicates information from the DOE form, the DOE report may be included or attached to the NERC report, in lieu of entering that information on the NERC report.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2009-01 Disturbance and Sabotage Reporting

Implementation Plan for EOP-004-2 – Event Reporting

Approvals Required
EOP-004-2 – Event Reporting

Prerequisite Approvals
None

Revisions to Glossary Terms
None

Applicable Entities
Reliability Coordinator
Balancing Authority
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Distribution Provider

Conforming Changes to Other Standards
None

Effective Dates
In those jurisdictions where regulatory approval is required, this standard shall become effective on the first day of the first calendar quarter that is six months after applicable regulatory approval or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Retirements

EOP-004-1 – Disturbance Reporting and CIP-001-2a – Sabotage Reporting should be retired at midnight of the day immediately prior to the Effective Date of EOP-004-2 in the particular jurisdiction in which the new standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2009-01 Disturbance and Sabotage Reporting

Implementation Plan for EOP-004-2 – Event Reporting

Approvals Required
EOP-004-2 – Event Reporting

Prerequisite Approvals
None

Revisions to Glossary Terms
None

Applicable Entities
Reliability Coordinator
Balancing Authority
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Distribution Provider

Conforming Changes to Other Standards
None

Effective Dates
In those jurisdictions where regulatory approval is required, this standard shall become effective on ~~T~~the first day of the first calendar quarter that is six months after applicable regulatory approval or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~beyond the date that this standard is approved by applicable regulatory approval.~~ In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Retirements

EOP-004-1 – Disturbance Reporting and CIP-001-2a – Sabotage Reporting should be retired at midnight of the day immediately prior to the Effective Date of EOP-004-2 in the particular jurisdiction in which the new standard is becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2009-01 Disturbance and Sabotage Reporting

Please DO NOT use this form for submitting comments. Please use the electronic form to submit comments on the draft standard EOP-004-2. Comments must be submitted by September 27, 2012. If you have questions please contact Stephen Crutchfield by email or by telephone at (609) 651-9455.

Background Information

EOP-004-2 was posted for a 30-day formal comment period and successive ballot from April 25 through May 24, 2011. The DSR SDT received suggestions from stakeholders to improve the readability and clarity of the requirements of the standard. The revisions that were made to the standard are summarized in the following paragraphs. As a result of these revisions, the DSR SDT is posting the standard for a second successive ballot period.

The DSR SDT has developed EOP-004-2 to replace the current mandatory and enforceable EOP-004-1 and CIP-001-2a standards, therefore, retiring both EOP-004-1 and CIP-002-2a. The reporting obligations under EOP-004-2 serve to provide input to the NERC Events Analysis Program. Analysis of events is not required under the proposed standard and any analysis or investigation will fall under the Event Analysis Program under the NERC Rules of Procedure.

The following changes were made as a result of comment received in the last formal comment period and successive ballot:

1. The DSR SDT has removed reporting of Cyber Security Incidents from EOP-004 and has asked the team developing CIP-008-5 to retain this reporting. With this revision, the Interchange Coordinator, Transmission Service Provides, Load-Serving Entity, Electric Reliability Organization and Regional Entity were removed as Responsible Entities.
2. Most of the language contained in the "Background" Section was moved to the "Guidelines and Technical Basis" Section. Minor language changes were made to the measures and the data retention section. Attachment 2 was revised to list events in the same order in which they appear in Attachment 1.
3. Requirement R1 was revised to include the Parts in the main body of the Requirement. The Measure and VSLs were updated accordingly.
4. Following review of the industry's comments, the SDT has re-examined the FERC Directive in Order 693 and has dropped both Requirement R4 and Requirement R5, and updated Requirement R3 to have the Registered Entity "validate" the contact information in the contact list(s) that they may have for the events applicable to them. This validation needs to be

performed each calendar year to ensure that the list(s) have current and up-to-date contact data.

R3. Each Responsible Entity shall validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]"*

5. The SDT has also updated Attachment 1 based on comments received, FERC directives, and in consideration of what is required for combining CIP-001-2a and EOP-004-1 into EOP-004-2. Under the Event Column, the SDT starts to classify each type of an event by assigning an "Event Type" title. The DSR SDT then updated the "Entity with Reporting Responsibilities" column to simply state which entity has the responsibility to report if they experience an event. The last column, "Threshold for Reporting," is a bright line that, if reached, the entity needs to report that they experienced the applicable event per Requirement 1.
6. The DSR SDT had previously proposed a revision to the NERC Rules of Procedure (Section 812). The SDT has learned that NERC has started a new effort to forward event reports to applicable government authorities. As such, Section 812 is no longer needed and will be removed from this project.

Questions

You do not have to answer all questions.

1. **The DSR SDT has revised EOP-004-2 by combining Requirements R3 and R4 into a single requirement (Requirement R3) to, "… validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year." Do you agree with this revision? If not, please explain in the comment area below.**

   ☐ Yes

   ☐ No

   Comments:

2. **The DSR SDT has revised the VSLs to reflect the language in the revised requirements. Do you agree with the proposed VRFs and VSLs? If not, please explain in the comment area below.**

   ☐ Yes

   ☐ No

   Comments:

3. **Do you have any other comment, not expressed in the questions above, for the DSR SDT?**

   Comments:

Project 2009-01 Disturbance and Sabotage Reporting Mapping Document

Translation of CIP-001-2a – Sabotage Reporting and EOP-004-1 – Disturbance Reporting into EOP-004-2 – Event Reporting

Standard: CIP-001-2a – Sabotage Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting**
R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.	Moved into EOP-004-2, R1	R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the regional entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	Moved into EOP-004-2, R1	R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the regional entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Standard: CIP-001-2a – Sabotage Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting**
R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.	Moved into EOP-004-2, R1	R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the regional entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.	Moved into EOP-004-2, R1	R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the regional entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting Comments**
R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.	Retire this fill-in-the-blank requirement. Replace with new reporting and analysis procedure developed by NERC EAWG.	The requirements of EOP-004-2 specify that an entity must report certain types of impact events. The NERC EAWG is developing continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure.
R2. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.	Translated into EOP-004-2, R1 and the NERC Events Analysis Process	The requirements of EOP-004-2 specify that an entity must report certain types of impact events. The NERC EAWG is developing continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure.
R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.	Translated into EOP-004-2, R2	R2. Each Responsible Entity shall report events per their Operating Plan within 24 hours of meeting an event type threshold for reporting. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting Comments**
R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until sometime after they occur shall be reported within 24 hours of being recognized.	Translated into EOP-004-2, R2	R2. Each Responsible Entity shall report events per their Operating Plan within 24 hours of meeting an event type threshold for reporting. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*
R3.2. Applicable reporting forms are provided in Attachments 022-1 and 022-2.	Retire – informational statement	

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting Comments**
R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.	Retire as a requirement. Added as a "Note" to EOP-004-Attachment1-Impact Events Table	NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per Requirement R2 and provide as much information as is available at the time of the notification. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net or Voice: 404-446-9780.

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting Comments**
R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.	Retire this fill-in-the-blank requirement. Replace with new reporting procedure developed by NERC EAWG.	The requirements of EOP-004-2 specify that an entity must report certain types of impact events. The NERC EAWG is developing continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure.

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting Comments**
R4. When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.	Retire this fill-in-the-blank requirement. Replace with new reporting procedure developed by NERC EAWG.	The requirements of EOP-004-2 specify that an entity must report certain types of impact events. The NERC EAWG is developing continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure.

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Impact Event and Disturbance Assessment, Analysis, and Reporting Comments**
R5. The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.	Retire this fill-in-the-blank requirement. Replace with new reporting procedure developed by NERC EAWG.	The requirements of EOP-004-2 specify that an entity must report certain types of impact events. The NERC EAWG is developing continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure.
Request for Interpretation of CIP-001-2a, R2: Please clarify what is meant by the term, "appropriate parties." Moreover, who within the Interconnection hierarchy deems parties to be appropriate?	Retire the interpretation	Addressed in EOP-004-2, R1 by replacing the term, 'appropriate parties' with a broader, more specific list of specific entities to contact in Requirement R1.

Project 2009-01 Disturbance and Sabotage Reporting Consideration of Issues and Directives

Project 2009-01 Disturbance and Sabotage Reporting		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
"What is meant by: "establish contact with the FBI"? Is a phone number adequate? Many entities which call the FBI are referred back to the local authority. The AOT noted that on the FBI website it states to contact the local authorities. Is this a question for Homeland Security to deal with for us?" Establish communications contacts, as applicable with local FBI and RCMP officials. Some entities are very remote and the sheriff is the only local authority does the FBI still need to be contacted? Registered Entities have sabotage reporting processes and procedures in place but not all personnel has been trained.	CIP-001-1 NERC Audit Observation Team	The DSR SDT has been in contact with FBI staff and developed a notification flow chart for law enforcement as it pertains to EOP-004. The "Background" section of the standard outlines the reporting hierarchy that exists between local, state, provincial and federal law enforcement. The entity experiencing an event should notify the appropriate state or provincial law enforcement agency that will then coordinate with local law enforcement for investigation. These local, state and provincial agencies will coordinate with higher levels of law enforcement or other governmental agencies.

Question: How do you “and make the operator aware”	CIP-001-1 NERC Audit Observation Team	This has been removed from the standard. Requirement R1 requires that the entity has an Operating Plan for applicable events listed in Attachment 1.
How does this standard pertain to Load Serving Entities, LSE's.	CIP-001-1 NERC Audit Observation Team	LSE has been removed as an applicable entity as there are no applicable events.
We direct the ERO to explore ways to address these concerns – including central coordination of sabotage reports and a uniform reporting format – in developing modifications to the Reliability Standard with the appropriate governmental agencies that have levied the reporting requirements.	CIP-001-1; Order 693	See “Background” section of the standard as well as the “Guidelines and Technical Basis” section.

"Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event. Paragraph 461. Several commenters agree with the Commission's concern that the term "sabotage" should be defined. For the reasons stated in the NOPR, we direct that the ERO further define the term and provide guidance on triggering events that would cause an entity to report an event. However, we disagree with those commenters that suggest the term "sabotage" is so vague as to justify a delay in approval or the application of monetary penalties. As explained in the NOPR, we believe that the term sabotage is commonly understood and that common understanding should suffice in most instances.	CIP-001-1; Order 693	The DSR SDT has not proposed a definition for inclusion in the NERC Glossary because it is impractical to define every event that should be reported without listing them in the definition. Attachment 1 is the de facto definition of "event". The DSR SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that without the intervention of law enforcement after the fact, it was almost impossible to determine if an act or event was that of sabotage or merely vandalism. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.
The ERO should consider suggestions raised by commenters such as FirstEnergy and Xcel to define the specified period for reporting an incident beginning from when an event is discovered or suspected to be sabotage, and APPA's concerns regarding events at unstaffed or remote facilities, and triggering events occurring outside staffed hours at small entities.	CIP-001-1; Order 693	Attachment 1 defines the events which are to be reported under this standard. The required reporting is within 24 hours "of recognition of the event."

Modify CIP-001-1 1 to require an applicable entity to contact appropriate governmental authorities in the event of sabotage within a specific period of time, even if it is a preliminary report. Further, in the interim while the matter is being addressed by the Reliability Standards development process, we direct the ERO to provide advice to entities that have concerns about the reporting of particular circumstances as they arise.	CIP-001-1; Order 693	Per Requirement R1, the entity is to develop an Operating Plan which includes event reporting to law enforcement and governmental agencies. The DSR SDT has been in contact with NERC Situational Awareness and has been informed that all event reports received by NERC are being forwarded to FERC.
Consider the need for wider application of the standard. Consider whether separate, less burdensome requirements for smaller entities may be appropriate. Paragraph 458. The Commission acknowledges the concerns of the commenters about the applicability of CIP-001-1 to small entities and has addressed the concerns of small entities generally earlier in this Final Rule. Our approval of the ERO Compliance Registry criteria to determine which users, owners and operators are responsible for compliance addresses the concerns of APPA and others. 459. However, the Commission believes that there are specific reasons for applying this Reliability Standard to such entities, as discussed in the NOPR. APPA indicates that some small LSEs do not own or operate “hard assets” that are normally thought of as “at risk” to sabotage. The Commission is concerned that, an adversary might determine that a small LSE is the appropriate target when the adversary aims at a particular population or facility. Or an adversary may target a small user, owner or operator because it may have similar equipment or protections as a larger facility, that is, the adversary may use an attack against a smaller facility as a training “exercise.” {continued below}	CIP-001-1; Order 693	Attachment 1 defines the events which are to be reported under this standard. The applicable entities are also identified for each type of event. Each event is to be reported within 24 hours of recognition of the event.

The knowledge of sabotage events that occur at any facility (including small facilities) may be helpful to those facilities that are traditionally considered to be the primary targets of adversaries as well as to all members of the electric sector, the law enforcement community and other critical infrastructures. 460. For these reasons, the Commission remains concerned that a wider application of CIP-001-1 may be appropriate for Bulk Power System reliability. Balancing these concerns with our earlier discussion of the applicability of Reliability Standards to smaller entities, we will not direct the ERO to make any specific modification to CIP-001-1 to address applicability. However, we direct the ERO, as part of its Work Plan, to consider in the Reliability Standards development process, possible revisions to CIP-001-1 that address our concerns. Regarding the need for wider application of the Reliability Standard. Further, when addressing such applicability issues, the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate to address these concerns.		

The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures. At this time, the commission does not specify a review period as suggested by FirstEnergy and MRO and, rather, believes that the appropriate period should be determined through the ERO's Reliability Standards development process. However, the Commission directs that the ERO begin this process by considering a staggered schedule of annual testing of the procedures with modifications made when warranted formal review of the procedures every two or three years.	CIP-001-1; Order 693	The standard is responsive this directive with the following language in Requirement R3: R3. Each Responsible Entity shall validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]* The DSR SDT envisions that this will include verification that contact information contained in the Operating Plan is correct. As an example, the annual validation could include calling others as defined in the Responsibility Entity's Operating Plan to verify that their contact information is correct and current. If any discrepancies are noted, the Operating Plan would be updated.

Consider FirstEnergy's suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality. Paragraph 451. A number of commenters agree with the Commission's concern that the term sabotage" needs to be better defined and guidance provided on the triggering events that would cause an entity to report an event. FirstEnergy states that this definition should differentiate between cyber and physical sabotage and should exclude unintentional operator error. It advocates a threshold of materiality to exclude acts that do not threaten to reduce the ability to provide service or compromise safety and security. SoCal Edison states that clarification regarding the meaning of sabotage and the triggering event for reporting would be helpful and prevent over reporting.	CIP-001-1; Order 693	This addressed in Attachment 1. There are specific event types for both cyber and physical security with their respective report submittal requirements.

"Include a requirement to report a sabotage event to the proper government authorities. Develop the language to specifically implement this directive. Paragraph 467. CIP-001-1, Requirement R4, requires that each applicable entity establish communications contacts, as applicable, with the local FBI or Royal Canadian Mounted Police officials and develop reporting procedures as appropriate to its circumstances. The Commission in the NOPR expressed concern that the Reliability Standard does not require an applicable entity to actually contact the appropriate governmental or regulatory body in the event of sabotage. Therefore, the Commission proposed that NERC modify the Reliability Standard to require an applicable entity to "contact appropriate federal authorities, such as the Department of Homeland Security, in the event of sabotage within a specified period of time."212 468. As mentioned above, NERC and others object to the wording of the proposed directive as overly prescriptive and note that the reference to "appropriate federal authorities" fails to recognize the international application of the Reliability Standard. The example of the Department of Homeland Security as an "appropriate federal authority" was not intended to be an exclusive designation. Nonetheless, the Commission agrees that a reference to "federal authorities" could create confusion. Accordingly, we modify the direction in the NOPR and now direct the ERO to address our underlying concern regarding mandatory reporting of a sabotage event. The ERO's Reliability Standards development process should develop the language to implement this directive."		See "Guidelines and Technical Basis" section of Standard. "A proposal discussed with FBI, FERC Staff, NERC Standards Project Coordinator and SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Event EOP-004-2). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial level law enforcement agency. The state or provincial level law enforcement agency will coordinate with local law enforcement to investigate. If the state or provincial level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial level law enforcement agency will notify and coordinate with the FBI or the RCMP."

On March 4, 2008, NERC submitted a compliance filing in response to a December 20, 2007 Order, in which the Commission reversed a NERC decision to register three retail power marketers to comply with Reliability Standards applicable to load serving entities (LSEs) and directed NERC to submit a plan describing how it would address a possible "reliability gap" that NERC asserted would result if the LSEs were not registered. NERC's compliance filing included the following proposal for a short-term plan and a long-term plan to address the potential gap: · Short-term: Using a posting and open comment process, NERC will revise the registration criteria to define "Non-Asset Owning LSEs" as a subset of Load Serving Entities and will specify the reliability standards applicable to that subset. · Longer-term: NERC will determine the changes necessary to terms and requirements in reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers and process them through execution of the three-year Reliability Standards Development Plan. In this revised Reliability Standards Development Plan, NERC is commencing the implementation of its stated long-term plan to address the issues surrounding accountability for loads served by retail marketers/suppliers. The NERC Reliability Standards Development Procedure will be used to identify the changes necessary to terms and requirements in reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. Specifically, the following description has been incorporated into the scope for	CIP-001-1 and EOP-004 ORDER ON ELECTRIC RELIABILITY ORGANIZATION REGISTRY_DETERMINATIONS; ORDER ON COMPLIANCE FILING	The LSE is no longer an applicable entity, since no reportable event types in Attachment apply to an LSE. If an entity owns distribution assets, that entity will be registered as a Distribution Provider. Attachment 1 defines the timelines and events which are to be reported under this standard. The applicable entities are also identified for each type of event.

affected projects in this revised Reliability Standards Development Plan that includes a standard applicable to Load Serving Entities: Source: FERC's December 20, 2007 Order in Docket Nos. RC07-004-000, RC07-6-000, and RC07-7-000. Issue: In FERC's December 20, 2007 Order, the Commission reversed NERC's Compliance Registry decisions with respect to three load serving entities in the ReliabilityFirst (RFC) footprint. The distinguishing feature of these three LSEs is that none own physical assets. Both NERC and RFC assert that there will be a "reliability gap" if retail marketers are not registered as LSEs. To avoid a possible gap, a consistent, uniform approach to ensure that appropriate Reliability Standards and associated requirements are applied to retail marketers must be followed. Each drafting team responsible for reliability standards that are applicable to LSEs is to review and change as necessary, requirements in the reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. For additional information see: · FERC's December 20, 2007 Order (http://www.nerc.com/files/LSE_decision_order.pdf) · NERC's March 4, 2008 (http://www.nerc.com/files/FinalFiledLSE3408.pdf), · FERC's April 4, 2008 Order (http://www.nerc.com/files/AcceptLSECompFiling-040408.pdf), and · NERC's July 31, 2008 (http://www.nerc.com/files/FinalFiled-compFiling-LSE-07312008.pdf) compliance filings to FERC on this subject.		

Object to multi-site requirement	Version 0 Team CIP-001-1	The Standard was revised for clarity. Attachment 1 defines the timelines and events which are to be reported under this standard. The applicable entities are also identified for each type of event.
Definition of sabotage required VRFs Team Adequate procedures will insure it is unlikely to lead to bulk electric system instability, separation, or cascading failures.	Version 0 Team CIP-001-1	No definition for sabotage was developed. The DSR SDT has not proposed a definition for inclusion in the NERC Glossary because it is impractical to define every event that should be reported without listing them in the definition. Attachment 1 is the de facto definition of "event". The DSR SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that without the intervention of law enforcement after the fact, it was almost impossible to determine if an act or event was that of sabotage or merely vandalism. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

Coordination and follow up on lessons learned from event analyses Consider adding to EOP-004 – Disturbance Reporting Proposed requirement: Regional Entities (REs) shall work together with Reliability Coordinators, Transmission Owners, and Generation Owners to develop an Event Analysis Process to prevent similar events from happening and follow up with the recommendations. This process shall be defined within the appropriate NERC Standard	Events Analysis Team Reliability Issue	The DSR SDT envisions EOP-004-2 to be a reporting standard. Any follow up investigation or analysis falls under the purview of the NERC Events Analysis Program under the NERC Rules of Procedure.
Consider changes to R1 and R3.4 to standardize the disturbance reporting requirements (requirements for disturbance reporting need to be added to this standard). Regions currently have procedures, but not in the form of a standard. The drafting team will need to review regional requirements to determine reporting requirements for the North American standard.	Fill in the Blank Team	The DSR SDT envisions EOP-004-2 to be a continent-wide reporting standard. Any follow up investigation or analysis falls under the purview of the NERC Events Analysis Program under the NERC Rules of Procedure.
Can there be a violation without an event?	NERC Audit Observation Team	The DSR SDT envisions EOP-004-2 to be a continent-wide reporting standard. In the opinion of the DSR SDT, there cannot be a violation of Requirement R2 without an event. Since Requirement R1 calls for an Operating Plan, there can be a violation of R1 without an event.

Consider APPA's concern about generator operators and LSEs analyzing performance of their equipment and provide data and information on the equipment to assist others with analysis. Paragraph 607. APPA is concerned about the scope of Requirement R2 because, in its opinion, Requirement R2 appears to impose an open-ended obligation on entities such as generation operators and LSEs that may have neither the data nor the tools to promptly analyze disturbances that could have originated elsewhere. APPA proposes that Requirement R2 be modified to require affected entities to promptly begin analyses to ensure timely reporting to NERC and DOE.	EOP-004-1 Order 693	The DSR SDT envisions EOP-004-2 to be a continent-wide reporting standard. Any follow up investigation or analysis falls under the purview of the NERC Events Analysis Program under the NERC Rules of Procedure.
From: David Cook Sent: Wednesday, July 16, 2008 6:06 PM To: Rick Sergel; Dave Nevius; David A. Whiteley; Management Subject: RE: FERC request for DOE-417s I agree the real fix is to revise the EOP-004 standard. I agree that we can't (and shouldn't try) to do that by way of amendments to our Rules of Procedure. So we should include that fix in the standards work plan, do the best we can in the meantime to provide FERC with the 417s, and I'll have the conversation with Joe McClelland about not being able to do what the Commission directed in Order 693 (i.e., change the standards by way of a change in the Rules of Procedure). David	EOP-004-1 Other	Per Requirement R1, the entity is to develop an Operating Plan which includes event reporting to law enforcement and governmental agencies. The DSR SDT has been in contact with NERC Situational Awareness and has been informed that all event reports received by NERC are being forwarded to FERC.

In response to a SAR submitted by Glenn Kaht of ReliabilityFirst: As part of a regional compliance violation investigation, a possible reliability gap was identified related to EOP-004-1 — Disturbance Reporting. The existing standard limits reporting of generation outages to just those outages associated with loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations. This requirement has been interpreted as meaning that only generation outages that must be reported are those that occur with the loss of a bulk power transmission element. By not reporting large generation losses that occur without the loss of a bulk power transmission element, the industry is overlooking a potential opportunity to identify and learn from these losses. Specifically, Item 1 of Attachment 1 of EOP-004 requires the reporting of events if "The loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations. Generally, a disturbance report will be required if the event results in actions such as:" The Standard then lists six different actions that may occur as a result of the event in order to be reportable. All six of these actions appear to be dependent on "The loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations" in order for the event to be reportable. Some of these events may significantly impact the reliable operation of the bulk power system. Consider a revision to EOP-004-1 — Disturbance Reporting requiring a Generator Operator (GOP) that	Standards Committee Action From 01/13/2010	The DSR SDT has worked closely with the NERC EAWG to develop the event reporting requirements shown in Attachment 1. The EAWG and the DSR SDT considered this request and weighed it against reliability needs for reporting.

experiences the loss of generation greater than 500 MW that results in modification of equipment (e.g. control systems, or Power Load Unbalancer (PLU)) to be a reportable event.		
too many reports, narrow requirement to RC	Version 0 Team	There is only one report required under this standard. An entity may submit the report using Attachment 2 or the DEO OE-417 report form.
How does this apply to generator operator?	Version 0 Team	See attachment 1 for specific generator operator applicability.

Violation Risk Factor and Violation Severity Level Assignments

Project 2009-01 – Disturbance and Sabotage Reporting

This document provides the drafting team's justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in

EOP-004-2 — Event Reporting

Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the ERO Sanction Guidelines.

Justification for Assignment of Violation Risk Factors in EOP-004-2

The Disturbance and Sabotage Reporting Standard Drafting Team applied the following NERC criteria when proposing VRFs for the requirements in EOP-004-2:

High Risk Requirement
A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement
A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

The SDT also considered consistency with the FERC Violation Risk Factor Guidelines for setting VRFs:[1]

Guideline (1) — Consistency with the Conclusions of the Final Blackout Report
The Commission seeks to ensure that Violation Risk Factors assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System.

In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:[2]

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) — Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement Violation Risk Factor assignments and the main Requirement Violation Risk Factor assignment.

[1] North American Electric Reliability Corp., 119 FERC ¶ 61,145, order on reh'g and compliance filing, 120 FERC ¶ 61,145 (2007) ("VRF Rehearing Order").
[2] Id. at footnote 15.

Guideline (3) — Consistency among Reliability Standards

The Commission expects the assignment of Violation Risk Factors corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) — Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular Violation Risk Factor level conforms to NERC's definition of that risk level.

Guideline (5) — Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

The following discussion addresses how the SDT considered FERC's VRF Guidelines 2 through 5. The team did not address Guideline 1 directly because of an apparent conflict between Guidelines 1 and 4. Whereas Guideline 1 identifies a list of topics that encompass nearly all topics within NERC's Reliability Standards and implies that these requirements should be assigned a "High" VRF, Guideline 4 directs assignment of VRFs based on the impact of a specific requirement to the reliability of the system. The SDT believes that Guideline 4 is reflective of the intent of VRFs in the first instance and therefore concentrated its approach on the reliability impact of the requirements.

VRF for EOP-004-2:

There are three requirements in EOP-004-2. Requirement R1 was assigned a Lower VRF while Requirements R2 and R3 were assigned a Medium VRF.

VRF for EOP-004-2, Requirements R1:

- FERC's Guideline 2 — Consistency within a Reliability Standard. The Requirement specifies which entities are required to have processes for recognition of events and for communicating with other entities. This Requirement is the only administrative Requirement within the Standard. The VRF is only applied at the Requirement level. FERC's Guideline 3 — Consistency among Reliability Standards. This requirement calls for an entity to have processes for recognition of events and communicating with other entities. This requirement is administrative in nature and deals with the means to report events after the fact. All event reporting requirements in Attachment 1 are for 24 hours after recognition that an event has occurred. The current approved VRFs for EOP-004-1 are

all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program.

- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. Failure to have an event reporting Operating Plan is not likely to directly affect the electrical state or the capability of the bulk electric system. Development of the Operating Plan is a requirement that is administrative in nature and is in a planning time frame that, if violated, would not, under emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system.. Therefore this requirement was assigned a Lower VRF.
- FERC's Guideline 5 — Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R1 contains only one objective which is to have an Operating Plan with two distinct processes. Since the requirement is to have an Operating Plan, only one VRF was assigned.

VRF for EOP-004-2, Requirement R2:

- FERC's Guideline 2 — Consistency within a Reliability Standard. This Requirement calls for the Responsible Entity to implements its Operating Plan and is assigned a Medium VRF. There is one other similar Requirement in this Standard which specify an annual validation of the information contained in the Operating Plan (R3). Both of these Requirements are assigned a Medium VRF.
- FERC's Guideline 3 — Consistency among Reliability Standards. EOP-004-2, Requirement R2 is a requirement for entities to report events using the process for recognition of events per Attachment 1. Failure to report events within 24 hours is not likely to "directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system." However, violation of a medium risk requirement should also be "unlikely to lead to bulk electric system instability, separation, or cascading failures…" Such an instance could occur if personnel do not report events. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. EOP-004-2, Requirement R2 mandates that Responsible Entities implement their Operating Plan. Bulk power system instability, separation, or cascading failures are not likely to occur due to a failure to notify another entity of the event failure, but there is a slight chance that it could occur. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 5 - Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R2 addresses a single objective and has a single VRF.

VRF for EOP-004-2, Requirement R3:

- FERC's Guideline 2 — Consistency within a Reliability Standard. This Requirement calls for the Responsible Entity to perform an annual validation of the information contained in the Operating Plan and is assigned a Medium VRF. There is one other similar Requirement in this Standard which specifies that the Responsible Entity implement its Operating Plan (R2).. Both of these Requirements is assigned a Medium VRF.
- FERC's Guideline 3 — Consistency among Reliability Standards. EOP-004-2, Requirement R3 is a requirement for entities to perform an annual validation of the information contained of the information in the Operating Plan. Failure to perform an annual validation of the information contained in the Operating Plan is not likely to "directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system." However, violation of a medium risk requirement should also be "unlikely to lead to bulk electric system instability, separation, or cascading failures…" Such an instance could occur if personnel do not perform an annual test of the Operating Plan and it is out of date or contains erroneous information. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. EOP-004-2, Requirement R3 mandates that Responsible Entities perform an annual validation of the information contained of the information in the Operating Plan. Bulk power system instability, separation, or cascading failures are not likely to occur due to a failure to perform an annual test of the Operating Plan, but there is a slight chance that it could occur if the Operating Plan is out of date or contains erroneous information. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 5 - Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R3 addresses a single objective and has a single VRF.

Justification for Assignment of Violation Severity Levels for EOP-004-2:

In developing the VSLs for the EOP-004-2 standard, the SDT anticipated the evidence that would be reviewed during an audit, and developed its VSLs based on the noncompliance an auditor may find during a typical audit. The SDT based its assignment of VSLs on the following NERC criteria:

Lower	Moderate	High	Severe
Missing a minor element (or a small percentage) of the required performance The performance or product measured has significant value as it almost meets the full intent of the requirement.	Missing at least one significant element (or a moderate percentage) of the required performance. The performance or product measured still has significant value in meeting the intent of the requirement.	Missing more than one significant element (or is missing a high percentage) of the required performance or is missing a single vital component. The performance or product has limited value in meeting the intent of the requirement.	Missing most or all of the significant elements (or a significant percentage) of the required performance. The performance measured does not meet the intent of the requirement or the product delivered cannot be used in meeting the intent of the requirement.

FERC's VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in EOP-004-2 meet the FERC Guidelines for assessing VSLs:

Guideline 1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

> Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline 2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

> A violation of a "binary" type requirement must be a "Severe" VSL.
>
> Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline 3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline 4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

. . . unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VSLs for EOP-004-2 Requirements R1:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R1	Meets NERC's VSL guidelines. The requirement calls for the entity to have an Operating Plan and is binary in nature. The VSL is therefore set to "Severe".	The proposed requirement is a revision of CIP-001-1, R1-R4, and EOP-004-1, R2. The Requirement has no Parts and is binary in nature. The binary VSL does not lower the current level of Compliance.	The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed binary VSL uses the same terminology as used in the associated requirement, and is, therefore, consistent with the requirement.	The VSLs are based on a single violation and not cumulative violations.

VSLs for EOP-004-2 Requirement R2:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R2	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is a revision of EOP-004-1, R3. There is only a Severe VSL for that requirement. However, the reporting of events is based on timing intervals listed in EOP-004 Attachment 1. Based on the VSL Guidance, the DSR SDT developed four VSLs based on tardiness of the submittal of the report. If a report is not submitted, then the VSL is Severe. This maintains the current VSL.	The proposed VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSLs use the same terminology as used in the associated requirement, and are, therefore, consistent with the requirement.	The VSLs are based on a single violation and not cumulative violations.

VSLs for EOP-004-2 Requirement R3:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R3	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is a new Requirement. The test of the Operating Plan is based on the calendar year. Based on the VSL Guidance, the DSR SDT developed four VSLs based on tardiness of the submittal of the report. If a test is not performed, then the VSL is Severe.	The proposed VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSLs use the same terminology as used in the associated requirement, and are, therefore, consistent with the requirement.	The VSLs are based on a single violation and not cumulative violations.

A. Introduction

1. **Title:** **Sabotage Reporting**

2. **Number:** CIP-001-2a

3. **Purpose:** Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.

4. **Applicability**

   4.1. Reliability Coordinators.

   4.2. Balancing Authorities.

   4.3. Transmission Operators.

   4.4. Generator Operators.

   4.5. Load Serving Entities.

   4.6. Transmission Owners (only in ERCOT Region).

   4.7. Generator Owners (only in ERCOT Region).

5. **Effective Date:** ERCOT Regional Variance will be effective the first day of the first calendar quarter after applicable regulatory approval.

B. Requirements

R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.

R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

C. Measures

M1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement 1

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements 2 and 3.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to procedures, policies, a letter of understanding, communication records, or other equivalent evidence that will be used to confirm that it has established communications contacts with the applicable, local FBI or RCMP officials to communicate sabotage events (Requirement 4).

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organizations shall be responsible for compliance monitoring.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to verify compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Reliability Coordinator, Transmission Operator, Generator Operator, Distribution Provider, and Load Serving Entity shall have current, in-force documents available as evidence of compliance as specified in each of the Measures.

If an entity is found non-compliant the entity shall keep information related to the non-compliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance:

2.1. Level 1: There shall be a separate Level 1 non-compliance, for every one of the following requirements that is in violation:

2.1.1 Does not have procedures for the recognition of and for making its operating personnel aware of sabotage events (R1).

2.1.2 Does not have procedures or guidelines for the communication of information concerning sabotage events to appropriate parties in the Interconnection (R2).

2.1.3 Has not established communications contacts, as specified in R4.

2.2. **Level 2:** Not applicable.

2.3. **Level 3:** Has not provided its operating personnel with sabotage response procedures or guidelines (R3).

2.4. **Level 4:**.Not applicable.

E. ERCOT Interconnection-wide Regional Variance

Requirements

EA.1. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.

EA.2. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

EA.3. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

EA.4. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall establish communications contacts with local Federal Bureau of Investigation (FBI) officials and develop reporting procedures as appropriate to their circumstances.

Measures

M.A.1. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement EA1.

M.A.2. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements EA2 and EA3.

M.A.3. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to, procedures, policies, a letter of understanding, communication records,

or other equivalent evidence that will be used to confirm that it has established communications contacts with the local FBI officials to communicate sabotage events (Requirement EA4).

Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity shall be responsible for compliance monitoring.

1.2. Data Retention

Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have current, in-force documents available as evidence of compliance as specified in each of the Measures.

If an entity is found non-compliant the entity shall keep information related to the non-compliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Amended
1	April 4, 2007	Regulatory Approval — Effective Date	New
1a	February 16, 2010	Added Appendix 1 — Interpretation of R2 approved by the NERC Board of Trustees	Addition
1a	February 2, 2011	Interpretation of R2 approved by FERC on February 2, 2011	Same addition
	June 10, 2010	TRE regional ballot approved variance	By Texas RE
	August 24, 2010	Regional Variance Approved by Texas RE Board of Directors	
2a	February 16, 2011	Approved by NERC Board of Trustees	

2a	August 2, 2011	FERC Order issued approving Texas RE Regional Variance	

Appendix 1

Requirement Number and Text of Requirement
CIP-001-1: **R2**. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.
Question
Please clarify what is meant by the term, "appropriate parties." Moreover, who within the Interconnection hierarchy deems parties to be appropriate?
Response
The drafting team interprets the phrase "appropriate parties in the Interconnection" to refer collectively to entities with whom the reporting party has responsibilities and/or obligations for the communication of physical or cyber security event information. For example, reporting responsibilities result from NERC standards IRO-001 Reliability Coordination — Responsibilities and Authorities, COM-002-2 Communication and Coordination, and TOP-001 Reliability Responsibilities and Authorities, among others. Obligations to report could also result from agreements, processes, or procedures with other parties, such as may be found in operating agreements and interconnection agreements. The drafting team asserts that those entities to which communicating sabotage events is appropriate would be identified by the reporting entity and documented within the procedure required in CIP-001-1 Requirement R2. Regarding "who within the Interconnection hierarchy deems parties to be appropriate," the drafting team knows of no interconnection authority that has such a role.

A. Introduction

1. Title: **Disturbance Reporting**

2. Number: EOP-004-1

3. Purpose: Disturbances or unusual occurrences that jeopardize the operation of the Bulk Electric System, or result in system equipment damage or customer interruptions, need to be studied and understood to minimize the likelihood of similar events in the future.

4. Applicability

4.1. Reliability Coordinators.

4.2. Balancing Authorities.

4.3. Transmission Operators.

4.4. Generator Operators.

4.5. Load Serving Entities.

4.6. Regional Reliability Organizations.

5. Effective Date: January 1, 2007

B. Requirements

R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.

R2. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.

R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.

R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.

R3.2. Applicable reporting forms are provided in Attachments 1-EOP-004 and 2-EOP-004.

R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that

time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.

R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.

R4. When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.

R5. The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.

C. Measures

M1. The Regional Reliability Organization shall have and provide upon request as evidence, its current regional reporting procedure that is used to facilitate preparation of preliminary and final disturbance reports. (Requirement 1)

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, the preliminary report, computer printouts, operator logs, or other equivalent evidence that will be used to confirm that it prepared and delivered the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that will be used to confirm that it provided information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours. (Requirement 3.3)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

NERC shall be responsible for compliance monitoring of the Regional Reliability Organizations.

Regional Reliability Organizations shall be responsible for compliance monitoring of Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load-serving Entities.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to assess compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Regional Reliability Organization shall have its current, in-force, regional reporting procedure as evidence of compliance. (Measure 1)

Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that is either involved in a Bulk Electric System disturbance or has a reportable incident shall keep data related to the incident for a year from the event or for the duration of any regional investigation, whichever is longer. (Measures 2 through 4)

If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

See Attachments:

- EOP-004 Disturbance Reporting Form
- Table 1 EOP-004

2. Levels of Non-Compliance for a Regional Reliability Organization

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: No current procedure to facilitate preparation of preliminary and final disturbance reports as specified in R1.

3. Levels of Non-Compliance for a Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load- Serving Entity:

3.1. Level 1: There shall be a level one non-compliance if any of the following conditions exist:

3.1.1 Failed to prepare and deliver the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1

3.1.2 Failed to provide disturbance information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours as specified in R3.3

3.1.3 Failed to prepare a final report within 60 days as specified in R3.4

3.2. Level 2: Not applicable.

3.3. Level 3: Not applicable

3.4. Level 4: Not applicable.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	May 23, 2005	Fixed reference to attachments 1-EOP-004-0 and 2-EOP-004-0, Changed chart title 1-FAC-004-0 to 1-EOP-004-0, Fixed title of Table 1 to read 1-EOP-004-0, and fixed font.	Errata
0	July 6, 2005	Fixed email in Attachment 1-EOP-004-0 from info@nerc.com to esisac@nerc.com.	Errata

0	July 26, 2005	Fixed Header on page 8 to read EOP-004-0	Errata
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised

Attachment 1-EOP-004
NERC Disturbance Report Form

Introduction

These disturbance reporting requirements apply to all Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load Serving Entities, and provide a common basis for all NERC disturbance reporting. The entity on whose system a reportable disturbance occurs shall notify NERC and its Regional Reliability Organization of the disturbance using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. Reports can be sent to NERC via email (esisac@nerc.com) by facsimile (609-452-9550) using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. If a disturbance is to be reported to the U.S. Department of Energy also, the responding entity may use the DOE reporting form when reporting to NERC. Note: All Emergency Incident and Disturbance Reports (Schedules 1 and 2) sent to DOE shall be simultaneously sent to NERC, preferably electronically at esisac@nerc.com.

The NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports are to be made for any of the following events:

1. The loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations. Generally, a disturbance report will be required if the event results in actions such as:
   a. Modification of operating procedures.
   b. Modification of equipment (e.g. control systems or special protection systems) to prevent reoccurrence of the event.
   c. Identification of valuable lessons learned.
   d. Identification of non-compliance with NERC standards or policies.
   e. Identification of a disturbance that is beyond recognized criteria, i.e. three-phase fault with breaker failure, etc.
   f. Frequency or voltage going below the under-frequency or under-voltage load shed points.
2. The occurrence of an interconnected system separation or system islanding or both.
3. Loss of generation by a Generator Operator, Balancing Authority, or Load-Serving Entity — 2,000 MW or more in the Eastern Interconnection or Western Interconnection and 1,000 MW or more in the ERCOT Interconnection.
4. Equipment failures/system operational actions which result in the loss of firm system demands for more than 15 minutes, as described below:
   a. Entities with a previous year recorded peak demand of more than 3,000 MW are required to report all such losses of firm demands totaling more than 300 MW.
   b. All other entities are required to report all such losses of firm demands totaling more than 200 MW or 50% of the total customers being supplied immediately prior to the incident, whichever is less.
5. Firm load shedding of 100 MW or more to maintain the continuity of the bulk electric system.

6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in:
   a. Sustained voltage excursions equal to or greater than ±10%, or
   b. Major damage to power system components, or
   c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance as defined by steps 1 through 5 above.
7. An Interconnection Reliability Operating Limit (IROL) violation as required in reliability standard TOP-007.
8. Any event that the Operating Committee requests to be submitted to Disturbance Analysis Working Group (DAWG) for review because of the nature of the disturbance and the insight and lessons the electricity supply and delivery industry could learn.

NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report

☐ Check here if this is an Interconnection Reliability Operating Limit (IROL) violation report.

1.	Organization filing report.		
2.	Name of person filing report.		
3.	Telephone number.		
4.	Date and time of disturbance. Date:(mm/dd/yy) Time/Zone:		
5.	Did the disturbance originate in your system?	Yes ☐ No ☐	
6.	Describe disturbance including: cause, equipment damage, critical services interrupted, system separation, key scheduled and actual flows prior to disturbance and in the case of a disturbance involving a special protection or remedial action scheme, what action is being taken to prevent recurrence.		
7.	Generation tripped. MW Total List generation tripped		
8.	Frequency. Just prior to disturbance (Hz): Immediately after disturbance (Hz max.): Immediately after disturbance (Hz min.):		
9.	List transmission lines tripped (specify voltage level of each line).		
10.		FIRM	INTERRUPTIBLE
	Demand tripped (MW):		
	Number of affected Customers:		

	Demand lost (MW-Minutes):		
11.	Restoration time.	INITIAL	FINAL
	Transmission:		
	Generation:		
	Demand:		

Attachment 2-EOP-004
U.S. Department of Energy Disturbance Reporting Requirements

Introduction

The U.S. Department of Energy (DOE), under its relevant authorities, has established mandatory reporting requirements for electric emergency incidents and disturbances in the United States. DOE collects this information from the electric power industry on Form EIA-417 to meet its overall national security and Federal Energy Management Agency's Federal Response Plan (FRP) responsibilities. DOE will use the data from this form to obtain current information regarding emergency situations on U.S. electric energy supply systems. DOE's Energy Information Administration (EIA) will use the data for reporting on electric power emergency incidents and disturbances in monthly EIA reports. In addition, the data may be used to develop legislative recommendations, reports to the Congress and as a basis for DOE investigations following severe, prolonged, or repeated electric power reliability problems.

Every Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity must use this form to submit mandatory reports of electric power system incidents or disturbances to the DOE Operations Center, which operates on a 24-hour basis, seven days a week. All other entities operating electric systems have filing responsibilities to provide information to the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity when necessary for their reporting obligations and to file form EIA-417 in cases where these entities will not be involved. EIA requests that it be notified of those that plan to file jointly and of those electric entities that want to file separately.

Special reporting provisions exist for those electric utilities located within the United States, but for whom Reliability Coordinator oversight responsibilities are handled by electrical systems located across an international border. A foreign utility handling U.S. Balancing Authority responsibilities, may wish to file this information voluntarily to the DOE. Any U.S.-based utility in this international situation needs to inform DOE that these filings will come from a foreign-based electric system or file the required reports themselves.

Form EIA-417 must be submitted to the DOE Operations Center if any one of the following applies (see Table 1-EOP-004-0 — Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies):

1. Uncontrolled loss of 300 MW or more of firm system load for more than 15 minutes from a single incident.
2. Load shedding of 100 MW or more implemented under emergency operational policy.
3. System-wide voltage reductions of 3 percent or more.
4. Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the electric power system.
5. Actual or suspected physical attacks that could impact electric power system adequacy or reliability; or vandalism, which target components of any security system. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.

6. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.
7. Fuel supply emergencies that could impact electric power system adequacy or reliability.
8. Loss of electric service to more than 50,000 customers for one hour or more.
9. Complete operational failure or shut-down of the transmission and/or distribution electrical system.

The initial DOE Emergency Incident and Disturbance Report (form EIA-417 – Schedule 1) shall be submitted to the DOE Operations Center within 60 minutes of the time of the system disruption. Complete information may not be available at the time of the disruption. However, provide as much information as is known or suspected at the time of the initial filing. If the incident is having a critical impact on operations, a telephone notification to the DOE Operations Center (202-586-8100) is acceptable, pending submission of the completed form EIA-417. Electronic submission via an on-line web-based form is the preferred method of notification. However, electronic submission by facsimile or email is acceptable.

An updated form EIA-417 (Schedule 1 and 2) is due within 48 hours of the event to provide complete disruption information. Electronic submission via facsimile or email is the preferred method of notification. Detailed DOE Incident and Disturbance reporting requirements can be found at: http://www.eia.doe.gov/cneaf/electricity/page/form_417.html.

Table 1-EOP-004-0 Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Uncontrolled loss of Firm System Load	≥ 300 MW – 15 minutes or more	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
2	Load Shedding	≥ 100 MW under emergency operational policy	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
3	Voltage Reductions	3% or more – applied system-wide	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
4	Public Appeals	Emergency conditions to reduce demand	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
5	Physical sabotage, terrorism or vandalism	On physical security systems – suspected or real	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
6	Cyber sabotage, terrorism or vandalism	If the attempt is believed to have or did happen	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
7	Fuel supply emergencies	Fuel inventory or hydro storage levels ≤ 50% of normal	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
8	Loss of electric service	≥ 50,000 for 1 hour or more	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
9	Complete operation failure of electrical system	If isolated or interconnected electrical systems suffer total electrical system collapse	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
All DOE EIA-417 Schedule 1 reports are to be filed within 60-minutes after the start of an incident or disturbance All DOE EIA-417 Schedule 2 reports are to be filed within 48-hours after the start of an incident or disturbance				

All entities required to file a DOE EIA-417 report (Schedule 1 & 2) shall send a copy of these reports to NERC simultaneously, but no later than 24 hours after the start of the incident or disturbance.				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Loss of major system component	Significantly affects integrity of interconnected system operations	NERC Prelim Final report	24 hour 60 day
2	Interconnected system separation or system islanding	Total system shutdown Partial shutdown, separation, or islanding	NERC Prelim Final report	24 hour 60 day
3	Loss of generation	≥ 2,000 – Eastern Interconnection ≥ 2,000 – Western Interconnection ≥ 1,000 – ERCOT Interconnection	NERC Prelim Final report	24 hour 60 day
4	Loss of firm load ≥15-minutes	Entities with peak demand ≥3,000: loss ≥300 MW All others ≥200MW or 50% of total demand	NERC Prelim Final report	24 hour 60 day
5	Firm load shedding	≥100 MW to maintain continuity of bulk system	NERC Prelim Final report	24 hour 60 day
6	System operation or operation actions resulting in:	• Voltage excursions ≥10% • Major damage to system components • Failure, degradation, or misoperation of SPS	NERC Prelim Final report	24 hour 60 day
7	IROL violation	Reliability standard TOP-007.	NERC Prelim Final report	72 hour 60 day
8	As requested by ORS Chairman	Due to nature of disturbance & usefulness to industry (lessons learned)	NERC Prelim Final report	24 hour 60 day
All NERC Operating Security Limit and Preliminary Disturbance reports will be filed within 24 hours after the start of the incident. If an entity must file a DOE EIA-417 report on an incident, which requires a NERC Preliminary report, the Entity may use the DOE EIA-417 form for both DOE and NERC reports.				
Any entity reporting a DOE or NERC incident or disturbance has the responsibility to also notify its Regional Reliability Organization.				

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-01 Disturbance and Sabotage Reporting

Formal Comment Period Open: August 29 – September 27, 2012

Upcoming:
Successive Ballot and Non-binding Poll: September 18 – September 27, 2012

Now Available

A formal comment period for **EOP-004-2 – Event Reporting** is open through **8 p.m. Eastern on Thursday, September 27, 2012**

The drafting team has made the following changes to the standard:

> Most of the language contained in the "Background" Section was moved to the "Guidelines and Technical Basis" Section. Minor language changes were made to the measures and the data retention section. Attachment 2 was revised to list events in the same order in which they appear in Attachment 1.
>
> Requirement R1 was revised to include the Parts in the main body of the Requirement. The Measure and VSLs were updated accordingly.
>
> Following review of the industry's comments, the SDT has re-examined the FERC Directive in Order 693 and has dropped both R3 and R4 as they were written and established a new Requirement R3 to have the Registered Entity "validate" the contact information in the contact list(s) they may have for the events applicable to them. This validation needs to be performed each calendar year to ensure that the list(s) have current and up-to-date contact data.

A redline version of EOP-004-2 is not posted because EOP-004-2 is a consolidation of CIP-001-2a and EOP-004-1. A redline version of EOP-004-2 would be difficult to follow so clean versions of CIP-001-2a and EOP-004-1 have been posted as a convenience.

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Thursday, September 27, 2012**. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Please read carefully: All stakeholders with comments (both members of the ballot pool as well as other stakeholders, including groups such as trade associations and committees) must submit comments through the electronic comment form. During the ballot window, balloters who wish to submit comments with their ballot *may no longer enter comments on the balloting screen*, but may still enter the comments through the electronic comment form. Balloters who wish to express support for comments submitted by another entity or group will have an opportunity to enter that information and are not required to answer any other questions.

Next Steps

A successive ballot of EOP-004-2 and non-binding poll of the associated VRFs and VSLs will be conducted beginning on Tuesday, September 18, 2012 through 8 p.m. Eastern on Thursday, September 27, 2012.

Background

The DSR SDT has developed EOP-004-2 to replace the current mandatory and enforceable EOP-004-1 and CIP-001-1a standards. The reporting obligations under EOP-004-2 serve to provide input to the NERC Events Analysis Program. Analysis of events is not required under the proposed standard and any analysis or investigation will fall under the Event Analysis Program under the NERC Rules of Procedure.

Additional information is available on the project page.

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd.NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-01 Disturbance and Sabotage Reporting

Formal Comment Period Open: August 29 – September 27, 2012

Upcoming:
Successive Ballot and Non-binding Poll: September 18 – September 27, 2012

Now Available

A formal comment period for **EOP-004-2 – Event Reporting** is open through **8 p.m. Eastern on Thursday, September 27, 2012**

The drafting team has made the following changes to the standard:

> Most of the language contained in the "Background" Section was moved to the "Guidelines and Technical Basis" Section. Minor language changes were made to the measures and the data retention section. Attachment 2 was revised to list events in the same order in which they appear in Attachment 1.
>
> Requirement R1 was revised to include the Parts in the main body of the Requirement. The Measure and VSLs were updated accordingly.
>
> Following review of the industry's comments, the SDT has re-examined the FERC Directive in Order 693 and has dropped both R3 and R4 as they were written and established a new Requirement R3 to have the Registered Entity "validate" the contact information in the contact list(s) they may have for the events applicable to them. This validation needs to be performed each calendar year to ensure that the list(s) have current and up-to-date contact data.

A redline version of EOP-004-2 is not posted because EOP-004-2 is a consolidation of CIP-001-2a and EOP-004-1. A redline version of EOP-004-2 would be difficult to follow so clean versions of CIP-001-2a and EOP-004-1 have been posted as a convenience.

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Thursday, September 27, 2012**. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Please read carefully: All stakeholders with comments (both members of the ballot pool as well as other stakeholders, including groups such as trade associations and committees) must submit comments through the electronic comment form. During the ballot window, balloters who wish to submit comments with their ballot *may no longer enter comments on the balloting screen*, but may still enter the comments through the electronic comment form. Balloters who wish to express support for comments submitted by another entity or group will have an opportunity to enter that information and are not required to answer any other questions.

Next Steps

A successive ballot of EOP-004-2 and non-binding poll of the associated VRFs and VSLs will be conducted beginning on Tuesday, September 18, 2012 through 8 p.m. Eastern on Thursday, September 27, 2012.

Background

The DSR SDT has developed EOP-004-2 to replace the current mandatory and enforceable EOP-004-1 and CIP-001-1a standards. The reporting obligations under EOP-004-2 serve to provide input to the NERC Events Analysis Program. Analysis of events is not required under the proposed standard and any analysis or investigation will fall under the Event Analysis Program under the NERC Rules of Procedure.

Additional information is available on the project page.

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd.NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-01 Disturbance and Sabotage Reporting

Successive Ballot and Non-Binding Poll Results

Now Available

A successive ballot of **EOP-004-2 – Event Reporting** and a non-binding poll of the associated VRFs/VSLs concluded on Thursday, September 27, 2012.

Voting statistics for each ballot are listed below, and the Ballots Results page provides a link to the detailed results.

Updated Results

Ballot Results	Non-binding Poll Results
Quorum: 78.54%	Quorum: 72.59%
Approval: 63.40%	Supportive Opinions: 63.05%

Next Steps
The drafting team is considering the comments received from the comment and ballot periods.

Background
The DSR SDT has developed EOP-004-2 to replace the current mandatory and enforceable EOP-004-1 and CIP-001-1a standards. The reporting obligations under EOP-004-2 serve to provide input to the NERC Events Analysis Program. Analysis of events is not required under the proposed standard and any analysis or investigation will fall under the Event Analysis Program under the NERC Rules of Procedure.

Additional information is available on the project page.

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd.NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2009-01 Successive Ballot DSR
Ballot Period:	9/18/2012 - 9/27/2012
Ballot Type:	Initial
Total # Votes:	333
Total Ballot Pool:	424
Quorum:	**78.54 % The Quorum has been reached**
Weighted Segment Vote:	63.40 %
Ballot Results:	**The drafting team will review comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	104	1	46	0.622	28	0.378	10	20
2 - Segment 2.	11	0.7	3	0.3	4	0.4	2	2
3 - Segment 3.	108	1	45	0.57	34	0.43	8	21
4 - Segment 4.	37	1	20	0.714	8	0.286	3	6
5 - Segment 5.	91	1	44	0.698	19	0.302	7	21
6 - Segment 6.	53	1	23	0.697	10	0.303	4	16
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	8	0.6	5	0.5	1	0.1	1	1
9 - Segment 9.	4	0.2	0	0	2	0.2	0	2
10 - Segment 10.	8	0.6	4	0.4	2	0.2	0	2
Totals	**424**	**7.1**	**190**	**4.501**	**108**	**2.599**	**35**	**91**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson		
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Abstain	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Negative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Negative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Empire District Electric Co.	Ralph F Meyer	Negative	
1	Entergy Services, Inc.	Edward J Davis		
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Grand River Dam Authority	James M Stafford	Affirmative	
1	Great River Energy	Gordon Pietsch		
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier		
1	Idaho Power Company	Ronald D Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon		
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Affirmative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Los Angeles Department of Water & Power	Ly M Le		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	Manitoba Hydro	Joe D Petaski		
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	Northeast Utilities	David Boguslawski	Abstain	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Negative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Negative	
1	Orlando Utilities Commission	Brad Chase	Abstain	
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn	Abstain	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	

1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Affirmative	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Negative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	
1	Southern Illinois Power Coop.	William Hutchison		
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	
2	Alberta Electric System Operator	Mark B Thompson	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Abstain	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	
2	Midwest ISO, Inc.	Marie Knox		
2	New Brunswick System Operator	Alden Briggs	Negative	
2	New York Independent System Operator	Gregory Campoli		
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Negative	
3	AEP	Michael E Deloach	Negative	
3	Alabama Power Company	Richard J. Mandes	Negative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Abstain	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse		
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Abstain	
3	City of Palo Alto	Eric R Scott	Affirmative	

3	City of Redding	Bill Hughes	Affirmative	
3	Clatskanie People's Utility District	Brian Fawcett		
3	Clearwater Power Co.	Dave Hagen	Negative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Abstain	
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Negative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	
3	Cowlitz County PUD	Russell A Noble	Negative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Negative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Negative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	
3	Gulf Power Company	Paul C Caldwell	Negative	
3	Hydro One Networks, Inc.	David Kiguel	Negative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker		
3	Kansas City Power & Light Co.	Charles Locke		
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Kootenai Electric Cooperative	Dave Kahly	Abstain	
3	Lakeland Electric	Norman D Harryhill		
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Negative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Negative	
3	Modesto Irrigation District	Jack W Savage		
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White		
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Negative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz		
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller		
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	

3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Co.	David B Coher		
3	Southern Maryland Electric Coop.	Mark R Jones		
3	Tacoma Public Utilities	Travis Metcalfe	Negative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	
3	Westar Energy	Bo Jones	Negative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave		
3	Xcel Energy, Inc.	Michael Ibold	Negative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Affirmative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Negative	
4	Detroit Edison Company	Daniel Herring	Negative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	North Carolina Electric Membership Corp.	Bob Beadle		
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Negative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	
4	White River Electric Association Inc.	Frank L. Sampson	Abstain	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Avista Corp.	Edward F. Groce	Abstain	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Abstain	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Abstain	
5	Bonneville Power Administration	Francis J. Halpin	Negative	

5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Negative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick		
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Affirmative	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl		
5	Cowlitz County PUD	Bob Essex	Negative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	
5	Duke Energy	Dale Q Goodwine	Negative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Energy	Ellen Oswald		
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Exelon Nuclear	Michael Korchynsky	Abstain	
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh		
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero		
5	Indeck Energy Services, Inc.	Rex A Roehl		
5	JEA	John J Babik	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider		
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Negative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	

5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Siemens PTI	Edwin Cano		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	
5	Southern Company Generation	William D Shultz	Negative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Leonard Rentmeester		
5	Xcel Energy, Inc.	Liam Noailles	Negative	
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda L Powell	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn		
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones		
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo		
6	North Carolina Municipal Power Agency #1	Matthew Schull	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak		
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II		

6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		James A Maenner	Affirmative	
8		Roger C Zaklukiewicz	Abstain	
8		Edward C Stein	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Pacific Northwest Generating Cooperative	Margaret Ryan	Negative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky		
10	Midwest Reliability Organization	James D Burley		
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Non-binding Poll Results

Project 2009-01: Disturbance and Sabotage Reporting

Non-binding Poll Results	
Non-binding Poll Name:	Project 2009-01 DSR Non-binding Poll
Poll Period:	9/18/2012 - 9/27/2012
Total # Opinions:	286
Total Ballot Pool:	394
Summary Results:	72.59% of those who registered to participate provided an opinion or an abstention; 63.05% of those who provided an opinion indicated support for the VRFs and VSLs.

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson		
1	American Transmission Company, LLC	Andrew Z Pusztai	Abstain	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Avista Corp.	Scott J Kinney		
1	Balancing Authority of Northern California	Kevin Smith	Abstain	
1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Negative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Negative	

1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Empire District Electric Co.	Ralph F Meyer	Negative	
1	Entergy Services, Inc.	Edward J Davis		
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Grand River Dam Authority	James M Stafford	Affirmative	
1	Great River Energy	Gordon Pietsch		
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Abstain	
1	Hydro-Quebec TransEnergie	Bernard Pelletier		
1	Idaho Power Company	Ronald D. Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JEA	Ted Hobson	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon		
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Affirmative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Los Angeles Department of Water & Power	Ly M Le		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	Manitoba Hydro	Joe D Petaski		
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	
1	Minnkota Power Coop. Inc.	Richard Burt	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Abstain	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	Northeast Utilities	David Boguslawski	Abstain	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Negative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis		
1	Orlando Utilities Commission	Brad Chase	Abstain	
1	PacifiCorp	Ryan Millard	Abstain	
1	PECO Energy	Ronald Schloendorn		

1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Abstain	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Abstain	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Abstain	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Negative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	
1	Southern Illinois Power Coop.	William Hutchison		
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Larry G Akens	Abstain	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper		
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Abstain	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Negative	
2	Midwest ISO, Inc.	Marie Knox		
2	New Brunswick System Operator	Alden Briggs	Abstain	
2	New York Independent System Operator	Gregory Campoli		
2	PJM Interconnection, L.L.C.	Tom Bowe	Abstain	
2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Negative	

3	Alabama Power Company	Richard J. Mandes		
3	Ameren Services	Mark Peters	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	
3	Central Lincoln PUD	Steve Alexanderson	Abstain	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse		
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Abstain	
3	City of Redding	Bill Hughes	Affirmative	
3	Clatskanie People's Utility District	Brian Fawcett		
3	Cleco Corporation	Michelle A Corley	Abstain	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Abstain	
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Negative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Detroit Edison Company	Kent Kujala	Negative	
3	Dominion Resources Services	Michael F. Gildea		
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson		
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	
3	Gulf Power Company	Paul C Caldwell	Negative	
3	Hydro One Networks, Inc.	David Kiguel	Abstain	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker		
3	Kansas City Power & Light Co.	Charles Locke		
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Kootenai Electric Cooperative	Dave Kahly	Abstain	
3	Lakeland Electric	Norman D Harryhill		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	

3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	Manitoba Hydro	Greg C. Parent	Negative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Negative	
3	Modesto Irrigation District	Jack W Savage		
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White		
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Abstain	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz		
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller		
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Abstain	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Abstain	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern Maryland Electric Coop.	Mark R Jones		
3	Tacoma Public Utilities	Travis Metcalfe	Negative	
3	Tampa Electric Co.	Ronald L Donahey		
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative	Ronnie Frizzell		

	Corporation			
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Abstain	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Affirmative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Negative	
4	Detroit Edison Company	Daniel Herring	Negative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Abstain	
4	Seattle City Light	Hao Li	Abstain	
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Negative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Avista Corp.	Edward F. Groce	Abstain	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Abstain	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Abstain	
5	Bonneville Power Administration	Francis J. Halpin	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason		

5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick		
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Cogentrix Energy, Inc.	Mike D Hirst	Negative	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl		
5	Cowlitz County PUD	Bob Essex	Negative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton		
5	Duke Energy	Dale Q Goodwine	Negative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Energy	Ellen Oswald		
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Gainesville Regional Utilities	Karen C Alford		
5	Great River Energy	Preston L Walsh		
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero		
5	Indeck Energy Services, Inc.	Rex A Roehl		
5	JEA	John J Babik	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard		
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Abstain	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider		
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Negative	

5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Negative	
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp	Sandra L. Shaffer	Abstain	
5	Platte River Power Authority	Roland Thiel	Abstain	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Sacramento Municipal Utility District	Bethany Hunter	Abstain	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Abstain	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Siemens PTI	Edwin Cano		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	
5	Southern Company Generation	William D Shultz	Negative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State G & T Association, Inc.	Barry Ingold		
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Xcel Energy, Inc.	Liam Noailles		
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Abstain	

6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn		
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones		
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo		
6	North Carolina Municipal Power Agency #1	Matthew Schull	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Abstain	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Abstain	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak		
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration -	Peter H Kinney	Affirmative	

	UGP Marketing			
6	Xcel Energy, Inc.	David F. Lemmons		
8		Roger C Zaklukiewicz	Abstain	
8		Edward C Stein	Affirmative	
8		James A Maenner	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
10	Midwest Reliability Organization	James D Burley		
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Abstain	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Individual or group. (56 Responses)
Name (40 Responses)
Organization (40 Responses)
Group Name (16 Responses)
Lead Contact (16 Responses)
Question 1 (50 Responses)
Question 1 Comments (51 Responses)
Question 2 (41 Responses)
Question 2 Comments (51 Responses)
Question 3 (0 Responses)
Question 3 Comments (51 Responses)

Group
Northeast Power Coordinating Council
Guy Zito
Paragraph 81 efforts are underway to eliminate requirements that have little or no reliability benefit. This Standard only addresses documentation and has no impact on reliability.
Individual
Lee Layton
Blue Ridge EMC
No
See previous comments
No
R3 VSLs are silly.
Group
Arizona Public Service Company
Janet Smith, Regulatory Affairs Supervisor
Yes
Yes
No Additional Comments
Individual
Anthony Jablonski
ReliabilityFirst
Yes
Even though ReliabilityFirst votes in the Affirmative, we offer the following comment regarding Requirement R3 for consideration. ReliabilityFirst recommends changing the word "validate" to "verify" in Requirement R3. ReliabilityFirst believes not only does the entity need to validate contact information is correct, they should verify (i.e. authenticate though test) that the contact information is correct.
Yes
Even though ReliabilityFirst votes in the Affirmative, we offer the following comments for consideration regarding the VSLs: VSL for Requirement R2 – ReliabilityFirst questions whether there is justification for the gradation of VSLs out to 60 hours for the reporting an event. Without justification, ReliabilityFirst believes the timeframe should be shortened to eight hour increments with a severe VSL being more than 48 hours late. ReliabilityFirst believes that being more than a day late (24 hours) falls within the entity completely not meeting the intent of submitting the report with the required 24 hour timeframe.
Group
Southwest Power Pool Regional Entity
Emily Pennel
Yes

No
In R2, SPP RE does not understand why the VSLs are based on who was or was not contacted rather than when it was reported. An entity could decide to put only two entities in its Event Reporting Operating Plan. If the entity fails to submit an appropriate event report, it is open to a Severe VSL on the top set of VSLs but only a moderate on the lower set of VSLs. This seems to be a disconnect for applying the VSLs for the same facts and circumstances.
(1) SPP RE thinks the following Generation reporting threshold is unclear: "Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection". What has to happen within one minute? It reads as if you have to make a report within one minute. If the intent is that a report has to be made within 24 hours if the loss is for more than one minute it should read, "Total generation loss ≥ 2,000 MW for more than one minute for entities in the Eastern or Western Interconnection". What is the intent of the one minute requirement? (2) It appears per R1 that entities are no longer required to include Regional Entities in their reporting chains. SPP RE believes Regional Entities must be included in the reporting chain so they can fulfill their obligations under their delegation agreements. (3) SPP RE thinks this standard was changed substantially enough that it should have been opened for a new ballot pool.
Individual
Jonathan Appelbaum
The United Illuminating Company
Yes
No
Do not agree that the VRF for R3 is medium. Failure to Validate contact information will not likely lead to instability and Cascade. Reporting under EOP-004 is not an immediate action, and given a 24 hour reporting window a proper contact point can be identified on-the-fly. R2 is properly identified as the Medium VRF since a failure to report whether due to an improper Operating plan or improper cantact list may lead to an BES cascade.
Group
PNGC Comment Group
Ron Sporseen
Yes
Yes
Comments: The PNGC Comment group remains concerned that the "Applicability" section will inadvertently subject Distribution Providers to requirements that they should be excluded from. Please consider the two examples below and note that we're talking about probably hundreds of small DPs being subject to these unnecessary requirements without any increase to the reliability of the BES. Example 1: Small DP with a peak load of 50 MWs. They have no BES Facilities and their system is radial. Even though this utility will never have a reporting requirement per Attachment A, they are still subject to R1 and R3 plus the associated compliance (read financial) risk for non-conformance. An easy fix to this issue would be for DPs without BES Facilities and with less than 200 MW annual peak load to be excluded in the Applicability section. Example 2: Small DP with a peak load of 50 MWs. Their only BES Facilities are two Automatic UFLS relays that are capable of shedding 15 MWs. DP's Host Balance Authority (HBA) has a peak load of 10,000 MWs, meaning their UFLS plan requires them to have the capacity to shed 3000 MWs should system conditions warrant. Is it the SDT's intent for this DP to have an Operating Plan in place for "damage", "destruction", or "physical threat" for these two relays that are capable of shedding only 15 MWs out of a 3000 MW HBA UFLS plan? The SDT set a 100 MW threshold for reporting of automatic UFLS load shedding so why have reporting requirements for the threat to 15 MWs worth of UFLS relays? Once again the easy fix is to modify the Applicability section. We suggest: 4.1.7. Distribution Provider: with >= 200 MW annual peak load, or; >= 100 MW Automatic firm load shedding
Individual
Russ Schneider
Flathead Electric Cooperative, Inc.
Individual
Oliver Burke
Entergy Services, Inc. (Transmission)
Yes
Yes

Individual
Nazra Gladu
Manitoba Hydro
No
This seems like an administrative only requirement. It would be too difficult to validate or measure.
No
This seems like an administrative only requirement. It would be too difficult to validate or measure.
Does the Background, Guidelines and Technical Basis form part of the standard itself once published? Or are these just parts of the package that accompany the standard during circulation for comment? Compliance 1.2: The reference to Responsible Entity is bracketed and in lowercase. We are not clear why. VSLs, R1, Severe VSL: The words "in the event reporting Operating Plan" are missing from the end of this sentence. VSLS, R2, Lower VSL: The violation occurs if the Responsible Entity has submitted an event report to one entity whereas Moderate VSL, High VSL and Severe VSL, the level of severity of the VSL increases depending on the number of entities that the Responsible Entity fails to submit an event report to. The drafting here is not as precise as it should be. The way the Lower VSL is written, it will also be triggered when the Responsible Entity has complied with the requirement. For example, if the Responsible Entity is required to report an event to 5 entities, and it does, it will still mean that it has "submitted an event report to one entity identified in the event reporting (also, the 'ing' is missing on the Lower VSL reference)Operating Plan". It is also duplicative. For example, if the Responsible Entity submitted a report to only one entity, and failed to submit a report to 4 others, they fall under the Lower VSL and the Higher VSL (we are assuming in this case, the violation will be found to be the higher VSL). Perhaps what the drafting team intended to do was to make the Lower VSL, which the Responsible Entity failed to submit an event report…to one entity identified…. The Guidelines and Technical Basis contain a reference to R4 which no longer exists in the standard.
Individual
Steve Grega
Lewis County PUD
Yes
No
We are a small utility with little impact to the BES with a small hydro on the end of a 230kV line. CIP-001 requires us to contact the FBI who has repeatedly instructed us to call the local sheriff office. The sheriff office has instructed us to call 911 and they will contact the FBI as needed. Therefore, 911 is our only contact number and our plan if vandalism, property destruction or sabotage is to have a supervisor call 911 and report. I do not think calling 911 to confirm the contact number serves any propose. Our plan will be simple with not a lot detail. The drafting team should recognize the reality of small utilities and state the required plan may be simple and not follow the flowchart in the draft standard.
Individual
Steve Alexanderson P.E.
Central Lincoln
Yes
1) Central Lincoln must again point out the lack of proportionality for gunshot insulators and similar events under "Damage or destruction of a Facility." Please see our last set of comments. These incidents are fairly common in the west, and typically do not cause an immediate outage. They are generally discovered months after the fact, yet the discovery starts the 24 hour clock running as if the situation had suddenly changed. Prior SDT response: "… this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human." There is already a great lag in awareness regarding the damaged insulator. Months or more can pass prior to discovery by the entity. We fail to see how it becomes so urgent upon discovery. Prior SDT response: "The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan." We do not share the SDT's vision. If an Operating Plan redefined suspected intentional human action so the act of preparing a gun for firing, aligning the sights on an insulator and pulling the trigger was not included, we believe the entity that operates under that plan would be found non-compliant under the language of this standard. We do not offer a simple change in text that will fix the problem, we are only pointing out the problem exists. Murphy dictates discovery will occur at the most inopportune time, which will be during an after hours outage on a stormy holiday weekend night when many employees are out of town and those that are available are already fully engaged. The entity is then faced with choosing to delay restoration or violating the standard. When proposing a zero defect event driven

requirement event driven such as this one, we ask the SDT to consider all possible scenarios in which the event may occur. 2) We note that Distribution Providers are listed in the Applicability Section. We also note that there is no requirement in the Statement of Compliance Registry Criteria for Distribution Providers to own or operate BES Facilities, own or operate UFLS or UVLS of 100 MW, or to have load exceeding 200 MW. DP's that cannot meet any of the thresholds of Attachment 1 would still need an Operating Plan under R1 and annually validate the possibly null contact list in its OP under R3. We suggest that DPs that cannot meet the thresholds of Attachment 1 be removed from the Applicability Section.
Group
Duke Energy
Greg Rowland
Yes
Duke Energy commends the excellent work of the Standard Drafting Team in incorporating previous comments into the current posted draft of the standard.
No
The Lower VSL for R3 should be clarified. The phrase "validated 75% or more" should be modified to say "validated at least 75% but less than 100%".
1) There are discrepancies between the red-lined EOP-004-2 and the Clean EOP-004-2 that were posted for this project. Our comments are based upon the Clean EOP-004-2. 2) Attachment 1 and Attachment 2 have the ERO email and phone number listed. If these ever change, does the standard have to go through the revision and balloting process again, or is there an easier way to incorporate such changes? 3) Attachment 1 – When an event occurs that meets the Threshold for Reporting, it's not clear whether all listed entities have to report or not. Several Event Types need this clarity added. For example, if a TOP loses voice communication capability, do both the TOP and RC have to report? 4) Attachment 1 – Damage or destruction of a Facility, applicable to BA, TO, TOP, GO, GOP, DP. The Threshold for Reporting should be further clarified by adding the sentence "Do not report theft or damage unless it degrades normal operation of a Facility." This would eliminate unnecessary reporting of copper theft or vandalism. 5) Attachment 1 – Physical threats to a Facility. The Threshold for Reporting should be modified by deleting the sentence "Do not report theft unless it degrades normal operation of a Facility". This sentence isn't needed here, and fits better with "Damage or destruction of a Facility" as noted in 4) above. 6) Attachment 1 – Transmission loss. This event type should be deleted because it is duplicated under TADS reporting and PRC-004 Protection System Misoperations reporting. 7) Attachment 1 – Unplanned BES control center evacuation, Complete loss of voice communication capability, and Complete loss of monitoring capability. The Threshold for Reporting on all three of these Event Types is 30 minutes, and should be extended to 2 hours, consistent with the transition time identified in EOP-008 "Loss of Control Center Functionality".
Individual
Jack Stamper
Clark Public Utilities
Yes
Yes
The SDT has not adequately addressed my comments from the last draft regarding damage or destruction of its facility that results from actual or suspected intentional human action. The SDT needs to limit what it means by damage. As an example, if someone breaks into a substation and paints graffiti on a breaker that is part of the BES, the breaker has been "damaged." However, the breaker's ability to function has not been compromised and there are no emergency actions that need to be taken. There is no reason for an emergency reporting procedure to require this to be reported. The SDT needs to add the same modifier for damage that it added in the previous event threshold for reporting. The reference for this type of damage should be as follows: Event: Damage or destruction of a Facility. Entity with Reporting Responsibility: BA, TO, TOP, GO, GOP, DP. Threshold for Reporting: Damage or destruction of its Facility that results from actual or suspected intentional human action that results in actions to avoid a BES Emergency.
Individual
Russell A. Noble
Cowlitz PUD
Yes
Cowlitz approves of the improvement efforts on Attachment 1. However, Cowlitz must again point out the fallacy of potentially inundating the ERO with nuisance reporting of minor vandalism and accidental damage. For example, gunshot "target practice" of insulators and structures will apply under "Damage or destruction of a Facility." Such incidents are fairly common in the west, and typically do not cause an immediate outage. They are generally

discovered months or years after the fact, yet the discovery starts the 24 hour compliance clock running as if the urgency is just as important as a recent event. If there is already a great lag in awareness regarding the damaged Facility, Cowlitz fails to see how it becomes so urgent upon discovery.---------- Again, Cowlitz points out the sentence structure "Damage or destruction of its Facility that results from actual or suspected intentional human action" does not restrict the human action as malicious or sabotage. "Intentional human action" could be innocent, such as a land owner attempting to fall a tree for fire wood. The intent was not to damage the Facility, but the "intentional human action" to obtain fire wood resulted in the damage of the Facility. This does not comport with prior SDT response: "… this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was 'damaged or destroyed' intentionally by a human." Therefore, if this is the SDT's intent Cowlitz suggests this change: Damage or destruction of its Facility that causes immediate impaired operation or loss of the Facility from suspected or actual malicious human intent. Do not report mischievous vandalism, as defined in the Operating Plan, where immediate loss of, or immediate impaired operation of the Facility has not occurred. ---------- Prior SDT response: "The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan." Cowlitz does not share the SDT's vision. The Standard as written does not specifically address the ability to "further define" terms used in the Attachment. Past allowance of audit teams to allow registered entity definitions, e.g. "annual," was to address gaps in standards until the standards could be revised. If this is truly the intent of the SDT, then requirement R1 would need revision such as: "The Operating plan shall define what a suspected intentional human action is." Cowlitz respectfully requests that ambiguity be avoided.---------- Cowlitz notes that Distribution Providers are listed in the Applicability Section with no qualifiers. Cowlitz points out that there is no requirement in the Statement of Compliance Registry Criteria for Distribution Providers to own or operate BES Facilities, own or operate UFLS or UVLS of 100 MW, or to have load exceeding 200 MW. DP's that cannot meet any of the thresholds of Attachment 1 would still need an Operating Plan under R1 and annually validate the possibly null contact list in its OP under R3. Cowlitz requests that DPs that cannot meet the thresholds of Attachment 1 be removed from the Applicability Section. Not doing so will increase compliance risk without any reliability return.
Group
Tacoma Public Utilities
Chang Choi
Yes
No
Regarding the Severe VSL for R1, the reference to "Parts 1.1 and 1.2" appears to be outdated. For R2, change "the Responsible Entity failed to submit an event report…to X entity(ies) within 24 hours" to "the Responsible Entity failed to submit an event report…to only X entity(ies) within 24 hours." (Add 'only.')
Why does the text "…but is not limited to…" in M1 have to be included? Does this mean that there are unwritten requirements that an auditor might look for? What if, in trying to validate contact information, contacts do not confirm their information? Regarding the Loss of firm load row in Attachment 1, an exception should be made for weather or natural disaster related threats in the Threshold for Reporting. Regarding the Transmission loss row in Attachment 1, it is not quite clear which types of BES Elements would meet the Threshold for Reporting. Is it just lines, buses, and transformers? What about reactive resources? What about generators that unexpectedly trip offline during a fault on the transmission system?
Individual
Chantel Haswell
Public Service Enterprise Group
Yes
Yes
None additional
Individual
Mike Hirst
Cogentrix Energy
Yes
No
The VRF for R2 should be "Lower" instead of "Medium" since it is administrative which involves reporting events to entities not identified in the Functional Model that have operating responsibilities listed. The VRF for R3 should also be "Lower" instead of "Medium" since it is an administrative requirement.
Overall: The standard makes good stride in eliminating the redundancy of CIP-001 and EOP-004. M1 States: "… and each organization identified to receive an event report for event types specified in EOP-004-2 Attachment 1".

It is an unclear in the statement that the protocols go with Attachment 1 and entities to receive report are part of Attachment 2 While this draft is an improvement on the previous draft, the proposed R2 is unacceptable, and should be amended to, at a minimum, require reporting by the end of the next business day, instead of within 24 hours. Events or situations affecting real time reliability to the system already are required to be reported to appropriate Functional Entities that have the responsibility to take action. Adding one more responsibility to system operators increases the operator's burden, which reduces the operator's effectiveness when operating the system. Care should be given when placing additional responsibility on the system operators. Allowing reporting at the end of the next business day gives operators the flexibility to allow support staff to assist with after-the-fact reporting requirements. For some event types where in order to provide real time situational awareness over a wide area (for example coordinated sabotage event) it may be appropriate to have more timely reporting. If the intent of this standard is to address sabotage reporting there needs to be an understanding of the actions to be taken by those receiving the reports so the reporting entities can incorporate those actions into their plan. As a minimum, NERC should have a process in place to assess the reports and take appropriate actions. Attachment 1: Threshold for reporting should not be defined such that multiple reports would be required for the same event. For example, both the TOP and RC being required to report the outage of a transmission line. 2nd event type (Damage or destruction of a Facility): Add the following sentence to the Threshold for Reporting: "Do not report theft or damage unless it degrades normal operation of a Facility." 4th event type (Physical threats to a BES control center): The term "BES control center" needs to be clarified. 5th, 6th, and 7th event types: In instances where a reliability directive is issued, is the "initiating entity" the entity that issues the directive or the entity that carried out the directive. 9th event type (Voltage deviation on a Facility): Change "nominal" to "expected or scheduled." 15th event type (Transmission loss): It is not clear what is meant by "contrary to design." This is so broad that it could be interpreted as requiring reporting misoperations within the reporting time frame before even an initial investigation can begin. This needs to be clarified and tied to the impact on the reliability of the BES.
Individual
Dave Willis
Idaho Power Co.
Yes
Yes
Individual
Michelle R D'Antuono
Ingelside Cogeneration LP
Yes
Ingleside Cogeneration believes that an annual validation of contact information is sufficient for a reporting procedure. R2 provides sufficient impetus for Responsible Entities to keep their Operating plan current − as a missed report will lead to a violation. Furthermore, external agencies and law enforcement officials will be reluctant to participate in validation tests, as dozens of nearby BES entities will overwhelm them with such requests.
Yes
Individual
Howard Rulf
Wisconsin Electric Power company dba We Energies
Yes
Yes
Damage or destruction of a Facility, Damage or destruction of its Facility that results from actual or suspected intentional human action.: By the Functional Model, I do not believe the BA function has Facilities by the NERC Glossary definition.. This would not apply to a BA. The line above this would adequately cover BA reporting. Remove a BA from applicability for this line. Physical threats to a Facility: The BA function does not have Facilities. Remove a BA from applicability for this line. There could be a separate line for Physical Threats to a Facility within an RC, FOP, BA Area as there is for Damage or Destruction of a Facility. Voltage deviation on a Facility: Please specify what voltage this is, nominal, rated, etc. This should also be > 10% deviation. Exactly at 10% could be at the edge of an allowed range.
Group

Detroit Edison
Kent Kujala
No
The requirement is too prescriptive and difficult to document. Requirement should be for annual review of Operating Plan. This allows for entity to review plan and document this the same as other Standards that require annual review (i.e. annual review blocks on documents). The requirement as written is vague and difficult to document. Annual review of reporting process is already a requirement.
No
Under VSLs for R2- We disagree with the reporting time frames. Making the time requirement as soon as 24 hours puts this reporting requirment on the real time operators. Many of the situations listed in the EOP-004 attachment are not included in the OE-417 report. The Unofficial Comment Form states the reporting obligations serve to provide input to the NERC Event Analysis Program. This program has removed the 24 hour reporting requirement and changed it to 5 business days.
"Suspicious activity" and "suspicious device" should be eliminated from Attachment 1, Event types: 'Physical threats to a Facility' and 'Physical threat to a BES Control Center'. By including 'suspicious activity' in the standard, I believe the project team went outside of the scope of the project, which was intended to be a merger of the two standards. Regarding standard CIP 001, the threshold for reporting is "Disturbances or unusual occurrences, suspected or determined to be caused by sabotage….", as its title suggested: Sabotage Reporting. Suspicious activity, which is not defined by the standard, clearly has a much lower threshold than sabotage, or even suspected sabotage. The reporting requirement of 24 hours, also increases the burden on the entity to either rush to investigate and make a determination regarding suspicious activity in less than 24 hours, or not perform due diligence and report uninvestigated "suspicious" activity, which normally turns out to not be a "Physical Threat". Suspicious activity should be duly investigated by the entity, local law enforcement, or the FBI as appropriate; and then reported if it has been determined to be a physical threat, or cannot be explained. Reporting within 24 hours will devalue the information inputted, as most cases of suspicious activity are innocuous, and the standard lacks a process of follow up, which would remove the those incidents from intelligence databases. Regarding suspicious devices, determination is usually immediate, (in less than 24 hours), and then the device would be classified as either "sabotage" or "no threat". The standard is not clear whether suspicious devices still have to be reported, even if they are immediately determined as not a "Physical Threat to a Facility or BES Control Center." Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01) - Reporting Concepts states: The changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). These standards deal exclusively with after-the-fact reporting." Attachment 1 in existing EOP-004-1 is much easier to follow (specifies time requirement to file). Also R2 states DOE OE-417 may be utilized to file reports, however Standard time requirement for update report is 48 hours, OE-417 has changed time requirement on updated filing to 72 hours. Difference can cause confussion and possible penalties. The real time operator must focus on maintaining system reliability. Putting unnecessary reporting obligations on RT puts more importance on the reporting structure than on maintaining reliability. Let 8/5 support personnel perform the reporting tasks and keep the 24/7 on shift operators focusing on the BES.
Individual
Melissa Kurtz
US Army Corps of Engineers
Individual
David Jendras
Ameren Services
Yes
Yes
(1) This draft refers to a number of activities in the Operations Plan that each entity is to have on hand as the primary guide of actions to be taken when an event occurs. Although there is information related to the requirements that should be included in the Operations Plan, the drafting team has not defined a structure on the format, the minimum information to be included or the direct audience for the Operations Plan. In addition, there is no guidance on the disposition, distribution of the Operations Plan which is left to the entity to determine. We request that the drafting team provide a defined structure for entities concerning the development and implementation of the Operations Plan. (2) Page 14 (Attachment 2) − Voltage Deviation of a Facility − This appears to be a contradiction to VAR-001-2 R10 for TOP which states IROL events will be corrected within 30 minutes. We request the 15 minute reporting criteria be changed to also state 30 minutes. (3) Throughout Document − "Report to the ERO and Regional Entity" − NERC and DHS established the ES-ISAC as a confidential location to report all events that happen on the BES. As these events are of a Sabotage / Disturbance nature, they should all go through the ES-ISAC both as a single location for distribution, and as a best practice that the industry has started.

(4) There seems to be some differences between the red-line and clean versions which may need some clarification. For example, (a) In the redline version, the revision history box appears to indicate the inclusion of parts of CIP-008, and in the "Clean" version this has been removed from the revision history box. (b) The red-line version includes a drawing at two places versus once in the clean version. (c) The correlation between the clean and redline documents is not very clear and there appears to be gaps in the reporting and tracking framework structure.
Individual
Michael Falvo
Independent Electricity System Operator
Yes
IESO agrees that the intent of Requirement R3 to have the Registered Entities validate the contact information in the contact lists that they may have for the events applicable to them is achieved. IESO also agrees that the elimination of conducting an annual test of the communications process and review of the event reporting Operating Plan in merging the previous R3 and R4 into this new R3 will give entities an opportunity to develop a plan that suits its business needs.
No
We agree with the VRF for R2, but have a concern over the VRFs assigned to R1 (Lower) and R3 (Medium). Having an event reporting operating plan (R1) is a first step toward meeting the intent of this standard, annually validating it (R3) is a maintenance requirement which arguably can be regarded as equally important but its reliability risk impact for failure to comply should be no higher than having no plan to begin with. We therefore suggest that the VRFs for R1 and R3 be at least the same, or that R1's VRF be higher than that for R3.
The proposed implementation plan may conflict with Ontario regulatory practice respecting the effective date of the standard. It is suggested that this conflict be removed by: Moving the last part ", or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities." to right after "this standard is approved by applicable regulatory approval" in the Effective Dates Section on P.2 of the draft standard, and the proposed Implementation Plan.
Individual
RoLynda Shumpert
South Carolina Electric and Gas
Yes
Yes
Has the drafting team considered how reports from R2 tie in with reports required by the NERC Event Analysis process? It appears that reporting deadlines conflict between the two. The SDT should clarify that the event types "Damage or Destruction" listed in attachment 1 do not pertain to "cyber events", to avoid duplication of the CIP-008 requirements.
Individual
David Revill
Georgia Transmission Corporation
Yes
Yes
GTC recommends a minor change to Attachment 2 associated with the complete loss of off-site power to nuclear generating plant. NUC-001-2 R9.3.5 describes provisions for restoration of off-site power and applies to both the Nuclear Plant Generator Operator and the applicable Transmission Entities. To maintain consistency, GTC recommends modification to this row in EOP-004-2 Attachment 2 such that the "Nuclear Plant Generator Operator" is the Responsible Entity with reporting responsibility. (A TO may not have visibility to all off-site power resources for a nuclear generating plant if multiple TO's are providing off-site power.) At a minimum, GTC recommends if the SDT believes the TO and TOP should remain involved, these entities should be limited to "TO and TOP that are responsible for providing services related to Nuclear Plant Interface Requirements (NPIRs)" which is also consistent with NUC-001-2.
Group
Southern Company
Antonio Grayson
Yes

No
The VRF for R2 should be "Lower" instead of "Medium" since it is administrative which involves reporting events to entities not identified in the Functional Model that have operating responsibilities listed. The VRF for R3 should also be "Lower" instead of "Medium" since it is an administrative requirement. In addition we suggest that the VSL for R1 should have a lower level VSL for an Operating Plan that may have one event type missing from the Operating Plan.
Event Type Entity with Reporting Responsibility Threshold for Reporting SOCO Comment Damage or destruction of a Facility RC, BA, TOP Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area, excluding weather or natural disaster related threats, that results in actions to avoid a BES Emergency. Damage or destruction of a Facility BA, TO, TOP, GO, GOP, DP Damage or destruction of its Facility that results from actual or suspected intentional human action. Do not report damage unless it degrades normal operation of a Facility. How does the SDT define "intentional human action?" Further, how is the phrase "suspected intentional human action" defined? This phrase is very broad. Is "intentional human action" identified as actions intended to damage facilities or does it include accidental actions by individuals? For example, if a person accidentally shot insulators off of a 230 kV line resulting in damage, would that be considered reportable "intentional human action?" In addition, what is that actual trigger for reporting? Does it require that the action has been discovered or is it from the time the event occurs? Further, 24 hours is a very brief time period -- how is an entity to conduct an investigation within that time period to determine if damage or destruction could have resulted from "actual or suspected" human action and also determine if it could have been "intentional"? In Southern's cases, and likely in other entities case, operating personnel submit the reports to the regulatory entities for events that fall under this standard. Southern is concerned, that the threshold for reporting for "Damage or destruction of a Facility" and "Physical threats to a Facility" is so broad that numerous reports would need to be filed that 1) may be a result of something that does not pose harm to reliability and should not be of interest to the regulators, and 2) would introduce additional burden to operating personnel that are monitoring the system every moment of the day. With the current proposed "Threshold for Reporting", the reporting requirement would hamper the ability of system operating personnel to perform their core real-time system operator tasks which would harm reliability. Physical threats to a Facility BA, TO, TOP, GO, GOP, DP Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. OR Suspicious device or activity at a Facility. Do not report theft unless it degrades normal operation of a Facility. Please provide some clarity as to what is considered suspicious activity. For example, would someone taking a photo of a BES substation fall into this category? Please provide examples of what may be considered suspicious activity and how NERC and others may use this information and what actions they would take as a result of receiving this information. In addition, what is that actual trigger for reporting? Is it when the threat is discovered or from when it should have or could have been discovered? Further, 24 hours is a very brief time period -- how is an entity to conduct an investigation within that time period in order to determine if the physical threat has the potential to degrade the normal operation of the Facility or that the "suspicious activity"? Physical threats to a BES control center RC, BA, TOP Physical threat to its BES control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. OR Suspicious device or activity at a BES control center. BES Emergency requiring public appeal for load reduction Initiating entity is responsible for reporting. Public appeal for load reduction event. It is unclear which entity would be responsible for reporting this event. For example, if the RC/TOP/BA were to identify the need to do this and instruct an LSE to issue the public appeal, who would report the event? BES Emergency requiring system-wide voltage reduction Initiating entity is responsible for reporting System wide voltage reduction of 3% or more. It is unclear which entity would be responsible for reporting this event. For example, if the RC were to identify the need to do this and instruct a TOP to reduce voltage, who would report the event? BES Emergency requiring manual firm load shedding Initiating entity is responsible for reporting Manual firm load shedding ≥ 100 MW. BES Emergency resulting in automatic firm load shedding DP, TOP Automatic firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS). Voltage deviation on a Facility TOP Observed within its area a voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes. Please change "nominal" to "expected" or "scheduled" IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only) RC Operate outside the IROL for time greater than IROL Tv (all Interconnections) or Operate outside the SOL for more than 30 minutes for Major WECC Transfer Paths (WECC only). Loss of firm load BA, TOP, DP Loss of firm load due to equipment failures/system operational actions for ≥ 15 Minutes: ≥ 300 MW for entities with previous year's demand ≥ 3,000 MW OR ≥ 200 MW for all other entities This should not be as a result of weather or natural disasters. System separation (islanding) RC, BA, TOP Each separation resulting in an island ≥ 100 MW Generation loss BA, GOP Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection OR ≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection Complete loss of off-site power to a nuclear generating plant (grid supply) TO, TOP Complete loss of off-site power affecting a nuclear generating station per the Nuclear Plant Interface Requirement Transmission loss TOP Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing). Unplanned BES control center evacuation RC, BA, TOP Unplanned evacuation from BES control center facility for 30 continuous minutes or more. Complete loss of voice communication capability RC, BA, TOP Complete loss of voice communication capability affecting a BES control center for 30 continuous minutes or more. Complete loss of monitoring capability RC, BA, TOP Complete loss of monitoring capability affecting a BES control center for 30

continuous minutes or more such that analysis capability (i.e., State Estimator or Contingency Analysis) is rendered inoperable. Guideline and Technical Basis Comments In the Summary of Key Concepts section of the Guideline and Technical Basis, the DSR SDT explains that the proposed Standard does not include any real-time operating notifications for events listed in Attachment 1. The DSR SDT should consider language in the Standard which codifies this approach. Southern Company notes that the proposed standard does not mention any exclusion of real-time notification. The Law Enforcement Reporting section of the Guideline and Technical Basis unintentionally expands on the purpose of the Standard by stating that "The Standard is intended to reduce the risk of Cascading events." The stated purpose of the Standard is "To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities." The phrase in the Guideline should be removed or modified in order to avoid any uncertainty about the Standard's purpose. The DSR SDT should consider integrating the content of the Concept Paper into the Guideline and Technical Basis. Presently, the Concept Paper appears as an add-on at the end of the document. When the Concept Paper existed as a stand-alone document, various segments such as "Introduction" and "Summary of Concepts and Assumptions" were helpful to stakeholders and standards developers. The revised merged document in the present draft does not need two separate sections addressing concepts nor does it need an introduction at the midway point. Additionally, two other areas are either duplicative or contribute to ambiguity within the supplemental information. First, it is not clear that the segment on Concepts and Assumptions includes any actual assumptions. The section should be modified or deleted to address this concern. Second, the segment entitled 'What about sabotage?' seems to contain topics similar to those on the first page of the Guideline. Again, the DSR SDT should consider integrating all of the necessary information into a more comprehensive document.

Individual

Andrew Gallo

City of Austin dba Austin Energy

Yes

Yes

(1) City of Austin dba Austin Energy (AE) requests that the SDT clarify whether R3 requires that each Registered Entity subject to EOP-004-2 verify NERC's contact information each year. It appears this would be overly burdensome for NERC to respond to individual requests. (2) AE also asks that NERC's fax number be included in the contact information at the beginning of Attachment 1 and at the Event Reporting Form in Attachment 2. NERC included the fax number as a viable contact method in its recent NERC Alert notifying the industry of the changed information. (3) AE requests that the SDT increase the threshold for reporting loss of firm load to ≥ 300 MW for all entities to align the reporting threshold with the OE-417 threshold. Otherwise, smaller entities would have to report firm load losses between 200 and 299 MW to NERC but not to the DOE. This could be administratively confusing to those responsible for reporting. (4) Attachment 1 lists the threshold for reporting generation loss at ≥ 1,000MW for the ERCOT Interconnection. ERCOT planning is based on a single contingency of 1,375MW. For this reason, AE believes the minimum threshold for a disturbance should be greater than the single contingency amount of >1,375MW for the ERCOT Interconnection.

Individual

Andrew Z.Pusztai

american Transmission Company

Yes

Yes A. ATC requests that the Standards Drafting Team address the following concerns and clarifications in Attachment 1: a.) Reporting event #14 in Attachment 1, is duplicative with respect to Nuclear Reliability Standard NUC-001-2.1 R 9.4.4. Reporting event #14 requires entities to report to NERC a "Complete loss of off-site power to a nuclear generating plant" while Nuclear Reliability Standard NUC-001-2.1 R9.4.4., i.e. includes "Provisions for supplying information necessary to report to government agencies, as related to Nuclear Plant Interface Requirements (NPIRs)". In addition, ATC believes the reporting related to event #14 in Attachment 1 is not a "reliability" issue, and more appropriately covered under Standard NUC-001 as a "Nuclear Safety Shutdown" issue. Therefore, ATC recommends that Item #14 in Attachment 1 of EOP-004-2 be deleted. b.) In Attachment 1, reporting event #2, i.e. Damage or destruction of a Facility" could obligate an entity to report any loss of copper grounds either on a T-Line or grounds associated with a transformer or breakers. ATC believes this does not rise to a reporting level such as NERC. ATC believes that additional qualifying language similar to reporting item #1 be incorporated into the threshold and read as follows: "Damage or destruction of its Facility that results from actual or suspected intentional human action that results in actions to avoid a BES Emergency." c.) In Attachment 1, reporting event #3 i.e. "Physical threats to a Facility" needs clarification since a physical threat needs to be actual and confirmed so that the TO or TOP repositions the system. In addition, the SDT needs to clarify what the phrase "normal operations" means. Is this a ratings issue? Or a result in how the Operator operates the system. d.) In Attachment 1, reporting event #3 threshold i.e. "Suspicious device or activity at a Facility" needs clarification to

determine when it raises to the level of reporting. These words could be interpreted in several different ways. In addition, ATC believe that language needs to be added that the threat causes the reporting entity to change to an abnormal operating state. ATC recommends the threshold be revised to read: "Suspicious device or activity at a Facility with the potential to degrade the normal operation of the Facility". e.) In Attachment 1, the term "Initiating entity" is used three times for reporting events and needs to be clearly defined or reworded. Is it the entity that identifies the needs of a Public Appeal or the entity that makes the public appeal the initiating entity? The Standard needs to be clear on who has the responsibility as the "initiating" party, especially when multiple parties may be involved. ATC recommends the following: 1) For public appeal, under Entity with Reporting Responsibility; it is the "entity that issues a public appeal to the public" 2) For system wide voltage reduction, under Entity with Reporting Responsibility; it is the "entity that activates a voltage reduction" 3) For manual load shedding, under Entity with Reporting Responsibility; it is the "entity that activates manual load shedding" f.) In Attachment 1, reporting event #15 i.e. "Transmission Loss", the threshold includes the phrase "contrary to design". ATC recommends this be clarified to read "contrary to protection system design". B. In EOP-004-2 Requirement 2/ Measure 2 both have the following language: "Each Responsible Entity shall report events per their Operating Plan within 24 hours of meeting an event type threshold for reporting." ATC recommends adding "upon recognition" as a starting point to the 24 hour reporting requirement. This would be revised to read: "Each Responsible Entity shall report events per their Operating Plan within 24 hours of recognition of an event type threshold"

Group

SERC OC Standards Review Group

Gerry Beckerle

Yes

No

The VRF for R2 should be "Lower" instead of "Medium" since it is administrative which involves reporting events to entities not identified in the Functional Model that have operating responsibilities listed. The VRF for R3 should also be "Lower" instead of "Medium" since it is an administrative requirement.

While this draft is an improvement on the previous draft, the proposed R2 is unacceptable, and should be amended to, at a minimum, require reporting by the end of the next business day, instead of within 24 hours. Events or situations affecting real time reliability to the system already are required to be reported to appropriate Functional Entities that have the responsibility to take action. Adding one more responsibility to system operators increases the operator's burden, which reduces the operator's effectiveness when operating the system. Care should be given when placing additional responsibility on the system operators. Allowing reporting at the end of the next business day gives operators the flexibility to allow support staff to assist with after-the-fact reporting requirements. For some event types where in order to provide real time situational awareness over a wide area (for example coordinated sabotage event) it may be appropriate to have more timely reporting. If the intent of this standard is to address sabotage reporting there needs to be an understanding of the actions to be taken by those receiving the reports so the reporting entities can incorporate those actions into their plan. As a minimum, NERC should have a process in place to assess the reports and take appropriate actions. Attachment 1: Threshold for reporting should not be defined such that multiple reports would be required for the same event. For example, both the TOP and RC being required to report the outage of a transmission line. 2nd event type (Damage or destruction of a Facility): Add the following sentence to the Threshold for Reporting: "Do not report theft or damage unless it degrades normal operation of a Facility." 4th event type (Physical threats to a BES control center): The term "BES control center" needs to be clarified. 5th, 6th, and 7th event types: In instances where a reliability directive is issued, is the "initiating entity" the entity that issues the directive or the entity that carried out the directive. 9th event type (Voltage deviation on a Facility): Change "nominal" to "expected or scheduled." 15th event type (Transmission loss): It is not clear what is meant by "contrary to design." This is so broad that it could be interpreted as requiring reporting misoperations within the reporting time frame before even an initial investigation can begin. This needs to be clarified and tied to the impact on the reliability of the BES. The comments expressed herein represent a consensus of the views of the above named members of the SERC OC Standards Review Group only and should not be construed as the position of SERC Reliability Corporation, its board, or its officers.

Group

FirstEnergy

Larry Raczkowski

Yes

Yes

FirstEnergy Corp (FE) appreciates the work done by the SDT by incorporating the comments and revisions from the previous draft. FE would like to see the time parameters in Requirement 3 and Measure 3 to be changed from "each calendar year" to "at least once every 12 months". This is similar to the wording that is being used in the CIP standards

Individual
Don Schmit
Nebraska Public Power Disstrict
Group
Dominion
Mike Garton
Yes
Dominion supports the combination of Requirements R3 and R4 into a single requirement (Requirement R3), although we remain concerned that validation requiring a phone call could be perceived as a nuisance by that entity.
Dominion reads Requirement R1 as explicitly requiring only the inclusion of reporting to the ERO in the Operating Plan. We acknowledge that the requirement also contains additional entities in parenthesis which infers the inclusion of a larger group (and which appears to be supported by the rationale box). Dominion suggests the SDT explicitly state which entities, at a minimum, be included, for reporting, in the Operating Plan. We suggest adding a column to Attachment 1 and including entities to which the event must be reported. As an examples; • All event types should include local law enforcement • Events for which the BA, RC, TOP bear responsibility should probably also be reported to the regional entity • Events for which the Facility Owner bears responsibility should probably also be reported to the respective BA and TOP, who would in turn determine whether to notify their respective RC. The RC would in turn determine if additional entities need to be contacted Requirement R2 establishes a 24 hour reporting threshold; however, the "NOTE" provided on Attachment 1 seems to contradict Requirement 2 and could therefore lead to compliance issues. Dominion suggests that Requirement R2 be revised to agree with the "NOTE" on Attachment 1. For example, Requirement R2 could be reworded as: Except as noted on Attachment 1, Each Responsible Entity shall… Also under the "NOTE" in Attachment 1, why has the facsimile number for the ERO been removed? The DOE still provides a facsimile number for reporting. Attachment 2: Event Reporting Form #4; need to update the below to reflect the same naming convention of the events in Attachment 1, the "t" should not be capitalized in Physical Threat and add an 's' behind threat. Add (islanding) behind System separation and capitalize the 'U' in unplanned control center evacuation.
Group
MRO NSRF
WILL SMITH
Yes
The NSRF requests that the SDT address the following concerns and clarifications in Attachment 1; 1) Please explore redundancy reporting event Item #14; Complete loss of off-site power to a nuclear generating plant with obligations of NUC-001-2.1 R9.4.4."Provisions for supplying information necessary to report to government agencies, as related to NPIRs." The NSRF understands the importance concerning safety issues with a nuclear plant. A multiple unit coal facility may have a larger reliability impact to the BES than a nuclear plant. The SDT is stating that the fuel source is a reporting issue, not the reliability of a plant loosing off sight power. Recommend that this item be deleted. 2) Item 2 in Attachment 1 would obligate an entity to report any loss of (copper) grounds either on a T-Line or grounds associated with a transformer or breakers and that this level of reporting should not rise to the NERC level. Believes that additional qualifying language similar to Item 1 be incorporated into the threshold and read as follows: "Damage or destruction of its Facility that results from actual or suspected intentional human action that results in actions to avoid a BES Emergency." 3) Item 3 Attachment 1 needs clarification since a physical threat needs to be actual and confirmed so that the TO or TOP repositions the system. In addition, the SDT needs to clarify what the phrase "normal operations" means. (Is this a ratings issue? or a result in how the System Operator operates the system.) 4) Item 3 should provide clarification as to "Suspicious device or activity at a Facility" to determine when threshold raises to the level of reporting. We are concerned that, based on an Auditors perception, these words could be interpreted in several different ways. In addition, we believe that language needs to be included that the threat causes the reporting entity to change to an abnormal operating state. This situation could be interpreted differently by the auditor or the entity at the time of the event. Recommend the following language: "Suspicious device or activity at a Facility with the potential to degrade the normal operation of the Facility". This language is similar to the first threshold. 5) The term Initiating entity is used three times within Attachment 1 and needs to be more clearly defined or reworded. Is it the entity that identifies the needs of a Public Appeal or the entity that makes the public appeal the initiating entity? The word "initiating" does not provide clarity but only provides uncertainty to the industry. The Standard needs to be clear on who has the responsibility as the "initiating". Recommend the following: a. For public appeal, under Entity with Reporting Responsibility; "entity that issues a public appeal to the public" b. For system wide voltage reduction, under Entity with Reporting Responsibility; "entity that activates a voltage reduction" c. For manual load shedding, under Entity with Reporting Responsibility; "entity that activates manual load shedding" 6) The NSRF recommends transmission loss to read as : "contrary to protection system design" found in threshold for reporting within the Attachment for

a Transmission loss event. In Requirement 2/ Measure 2, recommend adding "upon recognition of " as a starting point to the 24 hour reporting requirement, within the threshold of reporting where perceived threats are the threshold, or transmission loss, when contrary to design is determined.
Individual
Terry Harbour
MidAmerican Energy
Yes
No
Change the VRFs / VSLs to match suggested changes in Question 3
Yes. 1) MidAmerican Energy agrees with and supports MRO NSRF comments. 2) Add additional wording to clearly provide for compliance when events are found more than 24 hours after an event. Add the following to the end of R2. Add, Events not identified until sometime later after they occurred shall be reported within 24 hours. 3) In R3 add "external" for R3 to read Validate "external" contact information. 4) In EOP-004-2 Attachment 1 – the wording "Damage or destruction of its Facility that results from actual or suspected intentional human action that results in actions to avoid a BES Emergency" is not specific or measureable and therefore ambiguous. Zero defect standards which carry penalties must be specific. Please reword to "Intentional human action to destroy a NERC BES facility whose loss could result in actions to avoid a BES Emergency". This clearly aligns with the EOP-004 intent of sabotage and emergency reporting. EOP-004 should not report on unexpected conditions such as when a system operator attempts to reclose a line during a storm believing the line tripped for a temporary fault due to debris, when in fact the fault was permanent and damaged a transformer.
Individual
Kathleen Goodman
ISO New England Inc.
Individual
d mason
City and County of San Francisco - Hetch Hetchy Water and Power
No
Measure M3 specifically identifies two types of acceptable compliance evidence: Voice Recording and Log entries. Specifying only these two forms of evidence creates a risk that some auditors will reject other forms of R3 compliance evidence which are equally valid, such as emails or written call records. Although M3 states that acceptable evidence is not limited to Voice Recordings or Log Entries, we have concern that other methods of complying with R3 may not be accepted.
Individual
Tracy Richardson
Springfield Utility Board
Yes
Yes
Individual
Rich Salgo
NV Energy
No
Without further clarification of what is expected by "validate all contact information" I cannot support this requirement. On the surface, "validate" appears to be acceptable terminology, as it means to me a review of the contact names and contact information (perhaps cell #, home phone, text address, email address, etc) that would be evidenced through an attestation of completion of review along with records showing the updates made to the contact information pursuant to the review. However, when the Measure is considered, it refers to evidence such as operator logs, voice recordings, etc. This seems to indicate that the expectation is that each contact is tested, by dialing, texting, emailing, etc with some sort of confirmation that each contact was successful. If this is what is necessary to satisfy the "validate" requirement, I believe it is excessive, burdensome and unnecessary. I suggest modification of the Measure language to clearly allow for an entity to demonstrate compliance by a showinig that it reviewed the contact information and made changes as deemed necessary by its review, and to remove the reference to operator logs and voice recordings as the evidence of measure.

Aside from the comment referring to the new R3 and the term "validate", I applaud the SDT for the improvements made in the remainder of the Standard. This is a much simpler and straightforward approach to meeting the directives in this project and greatly simplifies the processes necessary on the part of the registered entities.
Individual
Thad Ness
American Electric Power
No
In the spirit of Paragraph 81 efforts, we request the removal of R3 as it is solely administrative in nature, existing only to support R2. This is more of an internal control and does not appear to rise to the level of being an industry-wide requirement. In addition, having two requirements rather than one increases the likelihood of being found non-compliant for multiple requirements rather than a single requirement.
No
In the spirit of Paragraph 81 efforts, we request the removal of R1. R1 is administrative in nature, existing only to support R2. Reporting an event externally might necessitate the need for a plan/procedure/policy/job aide, but requiring it is an overreach. Having two requirements rather than one increases the likelihood of being found non-compliant for multiple requirements rather than a single requirement. The Paragraph 81 project team has already recommended removing the requirement to have contact information with law enforcement from CIP-001 R4. Notwithstanding our comments above, we recommend removing the phrase "and other organizations…" from R1. If this requirement is to remain, it needs to be very specific regarding who needs to be included in the reporting. R2 – We recommend removing "per their Operating Plan" from R2 so it reads "Each Responsible Entity shall report events within 24 hours of meeting an event type threshold for reporting." If an entity deviates from its plan but still meets the intent of the requirement (e.g. reporting to NERC with 24 hours), this could be viewed as a finding of non-compliance. We need to get away from "compliance for compliance's sake", and focus solely on those efforts which will benefit the reliability of the BES. Attachment 1 Page 13, Row 1 (Clean Version): This is too open-ended and would likely lead to voluminous reporting. As it currently reads, "Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in actions to avoid a BES Emergency" could bring all copper thefts into scope. Thefts should not need to be reported unless the theft results in reliability concerns as specified by other criteria or parameters in Attachment 1. Attachment 1 Page 13, Row 2 (Clean Version): The threshold "Damage or destruction of its Facility that results from actual or suspected intentional human action" should be eliminated entirely. For the event Damage or destruction of a Facility, the threshold for reporting is set too low. Attachment 1 Page 13, Row 3 (Clean Version): We suggest modifying the text to read "Do not report theft… unless the theft results in reliability concerns as specified by other criteria or parameters in Attachment 1." Attachment 1 Page 14, Row 4 (Clean Version): Regarding "Loss of Firm Load", we suggest making it clear that the MW threshold is an aggregate value for those entities whose TOP is responsible for multiple operating companies or legal entities. In addition, is it necessary to include the DP as an entity with reporting responsibility? Its inclusion could create confusion by further segmenting the established threshold. Attachment 1 Page 15, Row 1 (Clean Version): Including "Transmission loss" as currently drafted would result in much more reporting than is necessary or warranted. As currently drafted, it could bring more events into scope than intended, especially for larger entities. EOP-004 Attachment 2: Event Reporting Form: AEP remains concerned that industry would be required to report similar information to multiple Federal entities, in this case to both NERC (Attachment 2) and the DOE (OE-417). In addition, the reporting requirement are not clear for every kind of event as to which entity the reports must be forwarded to, and it is unclear how information would be passed to other entities as necessary. EOP-004 Attachment 2: Event Reporting Form: This form is a further example of mixing security concepts with operational concepts. Not only is not advisable, it does not serve the interests of either concept.
Individual
Charles Yeung
Southwest Power Pool RTO
Yes
No
We quesstion the reliability benefits of this requirement.
Individual
Nathan Mitchell
American Public Power Association
Yes

Yes
As stated in our comments on the previous draft: It is APPA's opinion that this standard should be removed from the mandatory and enforceable NERC Reliability Standards and turned over to a working group within the NERC technical committees. Timely reporting of this outage data is already mandatory under Section 13(b) of the Federal Energy Administration Act of 1974. There are already civil and criminal penalties for violation of that Act. This standard is a duplicative mandatory reporting requirement with multiple monetary penalties for US registered entities. If this standard is approved, NERC must address this duplication in their filing with FERC. This duplicative reporting and the differences in requirements between DOE-OE-417 and NERC EOP-004-2 require an analysis by FERC of the small entity impact as required by the Regulatory Flexibility of Act of 1980
Group
Bonneville Power Administration
Chris Higgins
Yes
BPA agrees with the reviision and recognizes that it will involve a large amount of validation workload for entities with a large footprint.
No
BPA does not agree with the VRFs and VSLs. BPA believes that the violation levels for administrative errors are too high. For more information, please reference comments to question #3.
The proposed standard does not have any oral reporting option for system operators and thus appears to be administrative in nature. Due to this and the fact that administrative staff are not available on weekends, the "24 hour" reporting requirements should be modified to "Next Business Day" to allow for weekend delays in reporting. BPA believes that there are too many minor events that have to be reported within 24 hours. Reporting during the next business day would suffice. Some examples include: A 115 shunt capacitor bank failure for the first event type does not seem important enough to require reporting within 24 hours just because action has to be taken to raise generation or switching of line. A failure of a line tower that has proper protective action to clear the line and also has automatic (SPS) to properly protect as designed the BES system (a good normal practice) from overloads or voltage issues does not seem important enough to require reporting within 24 hours either.
Individual
Don Jones
Texas Reliability Entity
Yes
No
(1) VSLs for R1 should have a lower level VSL if the event reporting Operating Plan fails to include one or more of the event types listed in Attachment 1. (2) VSL for R1 is incorrectly stated as there are no "parts" to R1.
(A) Regional Entity should be capitalized in R1. (B) COMMENTS ON ATTACHMENT 1: In the previous comment period on this Standard, Texas RE submitted comments that we feel were not adequately addressed. There were several responses to comments regarding the Events Table that need deeper review and consideration: (1) In the Events Table, under Transmission Loss, the SDT indicated that reporting is triggered only if three or more Transmission Facilities operated by a single TOP are lost. Also, generators that are lost as a result of transmission loss events must be included when counting Facilities. As Texas RE indicated in previous comments to this Standard, determining event reporting requirements by the entity that owns/operates the facility is not an appropriate measure. If the industry wants to learn from events, these types of issues must be addressed. Including the RC as one of the Entity(s) with Reporting Responsibility may alleviate this concern. The RC would have overall view of the system and could provide the reports on multi-element events where the elements are owned/operated by different entities. For the SDT to believe that "There may be times where an entity may wish to report when a threshold has not been reached because of their experience with their system" is worthy to note but falls short of the reliability implications caused by those entities that will not report. The industry needs to learn from events and failure to report will facilitate failure to learn. (2) In the Events Table, under Transmission Loss, there has been considerable discussion recently within the Events Analysis Subcommittee (EAS) regarding the definition of the phrase "contrary to design." The EAS is currently working on possible guidelines to interpret this event type. The SDT may want to consider including the EAS language into the Guidelines and Technical Basis for this Standard. (3) In the Events Table, under "Unplanned BES Control Center evacuation" and "Complete loss of voice communication capability," and "Complete loss of monitoring capability," GOPs should be included. GOPs also operate control centers that would be subject to these kinds of occurrences. As Texas RE indicated in previous comments to this Standard, in CIP-002-5 Attachment 1 there is a "High Impact Rating" for the following: "1.4 Each Control Center, backup Control Center, and associated data centers used to perform the functional obligations of the Generation Operator that includes control 1) for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection or 2) that includes control of one or more of the generation assets that meet criteria 2.3, 2.6, and 2.9." In the ERCOT Region, we experienced an event where a GOP control

center lost an ICCP link that carried real-time information regarding its generation fleet (over 10,000 MWs). Without inclusion of the GOP here the event may not get recorded. While it was a "virtual" loss, the impact to the BES through generation control actions could be significant and the event should be reported and analyzed. For the GOP control centers that do exist, the reporting of such events should be a requirement. Based on the minimum of these two examples, why would the SDT NOT include GOP as being applicable? (4) In the Events Table, under "BES Emergency requiring public appeal for load reduction," the definition of Emergency is "Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities…." Is it the intent of the SDT to exclude public appeals issued in anticipation of a possible emergency, before a BES Emergency is officially declared? (5) In the Events Table, under "BES Emergency resulting in automatic firm load shedding," the SDT may want to consider including the RC as one of the Entity(s) with Reporting Responsibility. The RC would have overall view of the system and should provide the reports on events where the multiple entities may be involved. We have UVLS schemes in our region where the total MW shed is greater than 100 MW, but the individual TOP MW shed is less than 100 MW. (6) In the Events Table, consider whether the item for "Voltage deviation on Facility" should also be applicable to GOPs, because a loss of voltage control at a generator (e.g. failure of an automatic voltage regulator or power system stabilizer) could have a similar impact on the BES as other reportable items. Note: We made this comment last time, and the SDT's posted response was non-responsive to this concern. The SDT noted "Further, we note that such events do not rise to the level of notification to the ERO" but the SDT failed to recognize that "Voltage deviation on a Facility" does exactly that – notifies the ERO but from a TOP perspective only. Texas RE is trying to establish the correct Responsible Entity for reporting "Voltage deviation on a Facility" (in this case a generator regardless of the cause and other obligations the owner may have with other Reliability Standards).

Individual

Christine Hasha

ERCOT

Yes

ERCOT considers replacing R3 and R4 with the new R3 is an improvement and we thank the drafting team for making the change.

No

Since EOP-004 is related to ex-post reporting, which has nothing to do with operational or planning risk, this is an administrative requirement and, accordingly, the VRFs should all be Low. This would mean lowering the VRF for R2 and R3 to Low. The third component of the Severe VSL for R2 is more severe than the other two components. In an attempt to be more consistent across all the VSLs, we propose the following for the High VSL for R2: The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 48 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to three or more entities identified in its event reporting Operating Plan within 24 hours. ERCOT proposes that the first two components of the Severe VSL for R2 be deleted and replaced with: The Responsible Entity failed to submit a report for an event in EOP-004 Attachment 1.

As a general matter, this standard imposes an ex-post reporting obligation. Consistent with the ongoing P 81 standard review/elimination effort, this standard is arguably a candidate for elimination under the principles guiding that effort. The obligation proposed in the standards are better suited for inclusion in the Rules of Procedure or as a guideline because they are strictly administrative in nature. To the extent the SDT continues to pursue this effort, ERCOT offers the following additional comments. ERCOT has commented on the listing in the Entity with Reporting Responsibility column of Attachment 1. Consistent with those prior comments, the current version still fails to adequately create a bright line threshold for particular events. For example, in the Transmission loss event, although the TOP is listed, there is no direction regarding which TOP is required to file the event report. Is it the TOP in whose TOP area the loss occurred or is it a neighboring TOP who observes the loss? Clearly, the responsibility for reporting lies with the host system, but that responsibility is not clearly designated. There are several other similar events where there is no bright line. We suggest that the drafting team return the deleted language to the Entity with Reporting Responsibility column in those instances where the current version fails to provide a bright line in the Threshold column. Regarding multiple reports for a single event, that aspect of the proposed draft should be revised to only require a single report. While additional information may be available from others, let the Event Analysis team perform their function. This would eliminate the redundant reporting that is currently required as the standard is written. ERCOT requests that the reference to "cyber attack" be removed from the Guideline and Technical Basis section of the document since all reporting of cyber events has been removed from the standard and retained in CIP-008.

Individual

Denise M. Lietz

Puget Sound Energy Inc.

Yes

Puget Sound Energy appreciates the Standard Drafting Team's work to streamline and clarify the proposed

standard. In addition, we understand that the Standard Drafting Team faces a significant challenge in developing workable thresholds for reporting under this standard. Unfortunately, Puget Sound Energy cannot support the proposed standard because the reporting thresholds remain too vague and, thus, too broad - especially those related to damage or destruction of a Facility and those related to physical threats. The first four events listed on Attachment 1 are not brightline rules, because they each involve significant elements of judgment and interpretation. An example of our concern relates to the phrase "... that results from actual or suspected intentional human action." Puget Sound Energy, like many regulated entities, is staffed only with System Operators at night and on weekends. As a result, the 24-hour reporting requirement necessarily requires the System Operators to submit the required reports. So, how is a System Operator going to judge whether a human action is "intentional"? As a result, it will be necessary to report any event in which human action is involved because there is no way for a System Operator to know for sure whether the action is intentional or not. And, regulated entities will need to instruct their System Operators to make such reports, because the failure to submit a report of even one event listed in EOP-004 Attachment 1 is assigned a severe VSL under the proposed standard. We believe that the proposed threshold language will likely result in a flood of event reports that will not improve situation awareness.
Group
CenterPoint Energy
Daniela Hammons
No
CenterPoint Energy supports the concept of combining Requirements R3 and R4; however, the Company still prefers an annual review requirement which would include validating the contact information and content of the Operating Plan overall. Therefore, CenterPoint Energy recommends the following revised language for Requirement R3: "Each Responsible Entity shall review and update the Operating Plan at least every 15 months." The Company also suggests that the Measure be worded as follows: "Evidence may include, but is not limited to dated documentation reflecting changes to the Operating Plan including updated contact information if necessary."
No
CenterPoint Energy suggests that the phrase "which caused a negative impact to the Bulk Electric System" be added to each Violation Severity Level. For example, the wording would appear as follows: "The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 24 hours but less than or equal to 36 hours after meeting an event threshold for reporting which caused a negative impact to the Bulk Electric System". Additionally or alternatively, the Company proposes that the above phrase be added to the Threshold(s) for Reporting in Attachment 1 to focus on events that have an impact or effect on the Bulk Electric System.
CenterPoint Energy appreciates the revisions made to the draft Standard based on stakeholder feedback and believes that the changes made are positive overall. However, the Company recommends the additional changes noted below for a favorable vote. In the Rationale for R1, CenterPoint Energy recommends that the 2nd sentence in the 1st paragraph be revised as follows, "In addition, these event reports may serve as input to the NERC Events Analysis Program.", as not all events listed in Attachment 1 will serve as input in to the NERC Events Analysis Program. CenterPoint Energy also proposes that the Standard Drafting Team (SDT) add "There cannot be a violation of Requirement R2 without an event." as noted in the Consideration of Issues and Directives to the Requirement. For Attachment 1, CenterPoint Energy recommends the following revisions: CenterPoint Energy continues to be concerned that the uses of the terms "suspicious" and "suspected" are too broad. The Company proposes that the SDT remove the terms from the Thresholds for Reporting or add "which caused a negative impact to the Bulk Electric System" or "that causes an Adverse Reliability Impact…" to each phrase where the terms are used. CenterPoint Energy proposes that the threshold for reporting the event, "BES Emergency requiring manual firm load shedding" is too low. It appears the SDT was attempting to align this threshold with the DOE reporting requirement. However, as the SDT has stated, there are several valid reasons why this should not be done. Therefore, CenterPoint Energy recommends the threshold be revised to "Manual firm load shedding ≥ 300 MW". CenterPoint Energy also recommends a similar revision to the threshold for reporting associated with the "BES Emergency resulting in automatic firm load shedding" event. ("Firm load shedding ≥ 300 MW (via automatic under voltage or under frequency load shedding schemes, or SPS/RAS") For the event of "System separation (islanding)", CenterPoint Energy believes that 100 MW is inconsequential and proposes 300 MW instead. For "Generation loss", CenterPoint Energy suggests that the SDT add "only if multiple units" to the criteria of "1,000 MW for entities in the ERCOT or Quebec Interconnection".
Individual
Maggy Powell
Exelon Corporation and its affiliates
Yes
No
R2 VSLs – By measuring the amount of time taken to report and the number of entities to receive the report, the VSLs track more with size and location than with a failure to report. For instance, an entity failing to report at all to

one entity would be deemed a lower VSL while an entity reporting to many, but failing to report to three entities would be deemed a high VSL. R3 VSL − The severe VSLs do not seem commensurate to oversight. A three month delay in validating that phone numbers are correct, for phone numbers that are accurate, does not track with a severe infraction.
Thanks to the drafting team for all the work on this revision. Significant progress was made, though Exelon has some remaining comments: • It's not clear why the team separated 'Damage or destruction of a Facility' into two rows. Please advise. • Damage or destruction of a Facility - The threshold for "damage or destruction of a Facility" is too open-ended without qualifying the device or activity as "confirmed". Event reporting for nuclear generating units are initiated when an incident such as tampering is "confirmed". EOP-004 should include some threshold of proof for a reason to believe that no other possibility exists for "damage or destruction of a facility" event other than actual or suspected intentional human action. • Physical threats to a Facility − Reporting of every "suspicious activity" such as photographing equipment or site could result in an unwieldy volume of reports and dilute the data from depicting quality insight. For example, nuclear generating units are required to report all unauthorized and/or suspicious activity to the NRC. Please confirm that the intent of this threshold for notification would include all unauthorized and/or suspicious activity. • Physical threats to a BES control center − please confirm that reporting responsibility falls to the RC, BA, TOP and not GOs. In addition, please confirm that by use of the lower case "control center" other definitions in development through other standards development projects (e.g. CIP version 5) and that may be added to the NERC Glossary will not apply until formally vetted in a future EOP-004 standards development project. • Loss of firm load − "Loss of firm load for ≥ 15 Minutes: ≥ 300 MW for entities with previous year's demand ≥ 3,000 MW". Please clarify whether the team intends for this to apply to a single event a loss of more than 300 MW due to non-concurrent multiple distribution outages that total > 300MW. • Generation loss − Exelon appreciates the timing clarification added to the generation loss threshold. The phrase "within one minute" should also be included in the threshold for the ERCOT and Quebec Interconnections to read: "Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection OR Total generation loss, within one minute, of ≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection" • The Law Enforcement Reporting section in the Guideline and Technical Basis states: "The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of the BES from malicious physical or cyber attack." Since CIP-008 now covers reporting of cyber incidents the reference to cyber should be removed.
Group
SPP Standards Review Group
Robert Rhodes
Yes
We feel that replacing R3 and R4 with the new R3 is an improvement and we thank the drafting team for making the change.
No
Since EOP-004 is about after-the-fact reporting, we suggest that all the VRFs be Lower. This would mean lowering R2 and R3 from Medium. The third component of the Severe VSL for R2 is more severe than the other two components. In an attempt to be more consistent across all the VSLs, we propose the following for the High VSL for R2: The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 48 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to three or more entities identified in its event reporting Operating Plan within 24 hours. We propose the following, deleting the first two components as shown in the current draft, for the Severe VSL for R2: The Responsible Entity failed to submit a report for an event in EOP-004 Attachment 1.
We have made previous comments in the past regarding the listing in the Entity with Reporting Responsibility column of Attachment 1. While we concur with some of the changes that the drafting team has made regarding the addition of a bright line in the Threshold for Reporting column, there remain events where there is no line at all. For example, in the Transmission loss event, the TOP is listed and there is no distinction regarding which TOP is required to file the event report. Is it the TOP in whose TOP area the loss occurred or is it a neighboring TOP who observes the loss. Clearly, the responsibility for reporting lies with the host system. There are several other similar events where the bright line is non-existent and needs to be added. We suggest that the drafting team return the deleted language to the Entity with Reporting Responsibility column in those instances where the bright line has not been added in the Threshold column. Regarding multiple reports for a single event, we again believe that only a single report should be required. While additional information may be available from others, let the Event Analysis personnel do their job investigating an event and eliminate any redundant reporting that is currently required as the standard is written. If not, this standard, if approved, would then appear to be a likely candidate for Phase 2 of the Paragraph 81 project.
Individual
Christina Bigelow
Midwest Independent Transmission System Operator, Inc.
Yes
No

MISO agrees with the comments submitted by the SERC Operating Committee that the VRFs for R2 and R3 should be "Lower" instead of "Medium," since these are administrative requirements. MISO further respectfully suggests that implementing another standard that requires reporting every incident identified in a plan within 24 hours and that classifies failure to do so a "Severe" violation, will likely cause entities to limit the scope of their plans. NERC, therefore, would not receive information that appears unimportant to a single entity but could be important in the context of similar events across the country.

MISO respectfully submits that several of the thresholds for reporting in EOP-004 – Attachment 1 should be modified to clarify when the reporting obligation is triggered, and to ensure that entities are reporting events of the type and significance intended. In particular, MISO focuses on the following draft thresholds in EOP-004 – Attachment 1: • The requirement that an entity report when "[d]amage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in actions to avoid a BES Emergency." A BES Emergency is defined as "Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System." RCs and BAs take actions each and every day to "avoid a BES Emergency." At the time of those actions, they are reacting to conditions that their operating personnel are observing on the BES. There is no way for an RC or a BA to discern whether the conditions to which they reacted resulted from the "damage or destruction of a Facility" and there is no requirement for Transmission Operators and/or Owners to report "damage or destruction of a Facility" to their BA or RC. Accordingly, RCs and BAs will likely, often not be sufficiently informed to determine if their actions require them to submit a report. Responsible entities are likely to expend significant time and resources reporting daily operations and actions routinely taken to respond to observed BES conditions as they present themselves. These actions may be in response to congestion, equipment outages, relay malfunctions, etc. Whether or not the initiating factor was "damage to or destruction of a Facility" will often be an unknown factor and – even if such is known – the genesis of that damage and/or what constitutes damage (as discussed below) present further potential for confusion and over-reporting, Nonetheless, the lack of clarity in the standard is likely to result in some RCs and BAs preparing reports whether or not they definitely ascertain the underlying cause for the system conditions that prompted them to take actions "to avoid a BES Emergency." The preparation and submission of such reports, in many cases, will not facilitate the stated objective of this standard, which is the improvement of the reliability of the Bulk Electric System. In addition, with respect to damage or destruction of a Facility, it is debatable as to what would be considered "damage." For example, would an improper repair or outage that results in damage to a Facility that requires a more extended repair or outage be deemed "damage" to that Facility under this standard? These ambiguities will likely result in significant over-reporting, over-burdening responsible entities, and inundating Regional Entities and NERC with information that is not useful for the purpose of facilitating the reliable operation of the Bulk Electric System. These effects would undermine the express purpose of the standard and the potential value of information if the reporting obligations are appropriately defined, assigned, and scoped. For these reasons, MISO recommends that the SDT revise the standard to: (1) remove the requirement for RCs and BAs to report the "damage or destruction of a Facility" as it is redundant of the immediately subsequent requirement, (2) to remove reporting responsibility from BAs to report the "damage or destruction of a Facility" as this obligation is more properly placed with the TO, TOP, GO , GOP, and DP, and (3) provide guidance to the remaining responsible entities, TO, TOP, GO , GOP, and DP, regarding when "damage" to a Facility should be reported, e.g., an illustrative list of the types of "damage" that would yield information and/or trends that would facilitate the improvement of the reliability of the BES. • The requirement to report "[p]hysical threats to a Facility" and/or "[p]hysical threats to a BES Control Center" With respect to physical threats to Facilities or BES Control Centers, what is considered a "physical threat" and/or a "suspicious device or activity"? Is a crank call count that the building is on fire a physical threat? Is the return of a disgruntled employee suspicious? MISO understands and supports the reporting and analysis of threats and even certain types of suspicious activities, etc. It is merely concerned that the reporting threshold expressed in this standard will result in the reporting of substantial amounts of data that will not facilitate the improvement of the reliability of the BES and that the volume of reports may delay or otherwise obscure the detection of notable trends. Accordingly, MISO recommends that the SDT revise the standard to: (1) require the reporting only of substantial physical threats that are likely to have an adverse impact on the reliable operation of the Bulk Electric System, and (2) to provide an illustrative list of the types of "suspicious activity or devices" as guidance to responsible entities. • Timing of reports Finally, MISO respectfully suggests that NERC re-assess the timing requirements as related to the objectives expressed within this standard. MISO believes that NERC should clarify that its "situational awareness" staff will review submitted information to determine whether there are indications of possible coordinated attack and to quickly inform responsible entities that there are signals of possible coordinated attack. This clarification could be made in the standard, or the standard could describe the process that NERC staff will use. Unless such review and information is provided, the need that the standard attempts to address will not be fully met. Conversely, many of the events listed in Attachment A that require reporting do not need to be reported within 24 hours and would not offer significant benefit or value if reported within that time period as NERC and Regional Entities primarily utilize such information to capture metrics or perform after-the-fact events analysis. Accordingly, MISO respectfully suggests that, while performing analysis to determine clarifications that would result in the appropriate definition, assignment, and scope of reporting obligations, NERC should also examine the events and identify those events for which a longer time period for reporting would be suitable. This would significantly reduce the administrative burden on responsible entities and likely result in more comprehensive, rigorous, and beneficial reporting.

Group
ACES Power Marketing Standards Collaborators
Jason Marshall
No
We believe that the revision to R3 and elimination of R4 are great improvements to the standard as a lot of the unnecessary burdens have been removed. However, Requirement R3 is still not needed, has several issues with it and should be eliminated. (1) While validating contact information annually in a reporting plan makes sense, it does not rise to level of importance of requiring sanctions for failure to do so. Furthermore, it does nothing to assure reliability. Shortly after the contact information has been updated, it could change. This does not mean that validation should be more frequent but simply that is an unnecessary administrative burden. If contact information changes, the registered entity will have to find it. For reliability purposes, why does it matter if they do this in the 24-hour reporting period after the event or annually before the event? (2) Requirement R3 is administrative and is not consistent with the recent direction that NERC and FERC have taken toward compliance. Violations of this requirement are likely to be candidates for FFT treatment and this is exactly the kind of requirement that FERC invited NERC to propose for retirement in Paragraph 81 of the order approving the FFT process. Furthermore, it appears to meet at least two criteria (Administrative and periodic updates) that the Paragraph 81 drafting team has proposed to use to identify candidate requirements for retirement. The requirement is also not consistent with the direction NERC has taken on internal controls. How is an auditor reviewing that contact information has been updated in an Operating Plan forward looking or for that matter beneficial to reliability? Imagine a registered entity fails to update their contact information but still reports an event within the 24 hour reporting time frame to the appropriate parties. They are in technical violation of R3 but have met the spirit of the standard. (3) Requirement R3 is not a results-based requirement. It simply compels a registered entity "how to" meet reporting deadlines. Certainly, if a registered entity has current contact information on hand, it will be easier to notify appropriate parties of events quickly. However, it does limit a registered entity's ability to identify its own unique and possibly better way to meet a requirement. "How to" requirements prevent unique and superior solutions.
No
Because R3 is administrative, the VRF should be Lower. The requirement simply compels that that registered entity update a document which is purely administrative.
(1) For the first "Damage or destruction of a Facility" event in Attachment 1, the threshold for reporting should be modified. The threshold for reporting would only include damage or destruction that necessitates the need for action to prevent an Emergency. It does not include if an Emergency actually occurs. Based on the definition of Emergency which states that it is an "abnormal system condition that requires… action to prevent or limit", we think the threshold should be changed to "Damage or destruction of a Facility… that results in a BES Emergency". Per the definition, the Emergency is what necessitates action which is what the threshold appeared to be focused on. (2) In the second "Damage or destruction of a Facility" event in Attachment 1, the threshold regarding "intentional human action" is ambiguous and suffers from the same difficulties as defining sabotage. What constitutes intentional? How do we know something was intentional without a law enforcement investigation? If a car runs into a transmission tower, was this an accident or intentional human action? It could be either. This appears to be the same issue that prevented the drafting team from defining sabotage. (3) Under the "Physical threats to a BES control center" event in Attachment 1, the event should very clearly define if this applies to backup control centers or not. (4) Under the "Complete loss of off-site power to a nuclear generating plant (grid supply)" event" in Attachment 1, the entity with reporting responsibility is not coordinated with NUC-001. NUC-001 used the term transmission entity to mean an entity that is responsible for providing NPIR services. They did not use only TOP because there are other entities that provide this service. Please coordinate the "Entity with Reporting Responsibility" with that standard. (5) We continue to believe that the draft standard has not satisfied the complete scope of the SAR regarding elimination of redundancy. The draft standard will continue to require redundant reporting by various entities. For instance, under the event "Loss of Firm Load" in Attachment 1, the DP, TOP, and BA all are required to report. The response to our last set of comments regarding this issue was that "the industry can benefit from having such differing perspectives when events occur". This response seems to confuse event analysis with event reporting. The purpose of the standard is to simply report that an event happened. In fact, the reporting form only requires the submitting entity to report the type of event. The description of what happened is optional. What additional perspectives could be gained from having multiple registered entities in the same electrical footprint report that an event happened. If the purpose is to analyze the event, this is covered in the events analysis process. Furthermore, once NERC becomes aware of the event they have the authority to request data and information from other registered entities. Please eliminate the duplicate reporting requirements. Other events that may require duplicate reporting include: Damage or destruction of a Facility, Physical threats to a Facility, BES Emergency resulting in automatic firm load shedding, Loss of firm load, System separation, Generation loss, and Complete loss of off-site power to a nuclear generating plant. (6) In the second "Damage or destruction of a Facility" event and "Physical Threats to a Facility" events, Distribution Provider should be removed. The Distribution Provider does not have any Facilities which is defined as "a set of electrical equipment that operates as a single Bulk Electric System Element". The DP's transformers interconnecting to the BES are not Facilities and the latest NERC BOT definition explicitly does not include them in Inclusion I1. If a DP did own Facilities, it would be registered as a TO or GO. Inclusion of the DP will compel the DP to provide evidence that it does not have Facilities which is an unnecessary compliance burden that does not support reliability. (7)

The "BES Emergency resulting in automatic firm load shedding" should not apply to the DP. In the existing EOP-004 standard, Distribution Provider is not included and the load shed information still gets reported. (8) For the "Voltage deviation on a Facility" event in Attachment 1, we suggest changing "area" in the threshold for reporting to "Transmission Operator Area" as it is a defined term. (9) For the "System separation (islanding)" event, please remove BA. Because islanding and system separation, involve Transmission Facilities automatically being removed from service, this is largely a Transmission Operator issue. This position is further supported by the approval of system restoration standard (EOP-005-2) that gives the responsibility to restore the system to the TOP. (10) The response to our comments requesting that Measure 2 specifically identify that attestations are acceptable forms of evidence to indicate that no events have occurred indicated that the measure cannot permit use of attestations. Other standards that have been recently approved by the board specifically permit the use of attestations. FAC-003-2 M1 and M2, TOP-001-2 M1-M11 and TOP-003-2 M5 all permit the use of attestations. We ask that the drafting team to reconsider including a specific reference that an attestation is acceptable to indicate no event has occurred given these new facts. (11) In requirement R1, we suggest changing "in accordance with EOP-004-2 Attachment 1" to "to report events identified in EOP-004-2 Attachment 1". It makes more sense since the attachment is a list of events that require reporting. The other language sounds like additional requirements will be established in Attachment 1.
Individual
Scott Berry
Indiana Municipal Power Agency
Yes
IMPA agrees with the removal of a "test" and going with a validation requirement for the contact information in the Operating Plan.
no comment
On page 6 of 23 of the draft standard document, second paragraph under Rationale for R1, the SDT uses the words "Every industry participant that owns or operates elements or devices on the grid has a formal or informal process…" The use of these words implies that this requirement and others in this standard may apply to every industry entity regardless if they are a registered entity or not. IMPA understands that standards can only apply to entities that are registered with NERC, but we still prefer to see different wording in this sentence. IMPA recommends using "Every registered entity that owns or operates elements or devices on the grid has a formal or informal process…" Another concern is on pages 18, 19, and 20 of 23. It is not clear what exactly is required of a registered entity and the law enforcement reporting process. IMPA understands it is up to the entity to decide just how its event reporting Operating Plan is made up and who is contacted for the events in attachment 1. These pages are confusing when it comes to the listing of stakeholders in the reporting process on page 18 of 23 and then when the SDT states that an entity may just notify the state or provincial or local level law enforcement agency. The SDT needs to clarify that the listing of stakeholders on page 18 of 23 is just a suggestive listing and that if the entity so decides per its reporting Operating Plan that notification of the local law enforcement agency is sufficient (the thought that the local law enforcement agency can coordinate with additional law enforcement agencies if it sees the need). The requirement to contact the FBI in CIP-001 is not a requirement in EOP-004-2 unless the registered entity puts that requirement in its event reporting Operating Plan. As a clarification, in the Background section's second paragraph, it should read "retiring both EOP-004-1 and CIP-001-2a" as opposed to CIP-002-2a as written above in this comment document.
Individual
Darryl Curtis
Oncor Electric Delivery
Yes
No
Oncor suggest the following additions to VSL language for R1 to align more closely with the measures described in M1 Lower VSL - Entity has one applicable event type not properly identified in its event reporting Operating Plan High VSL - Entity has more than one applicable event type not properly identified in its event reporting Operating Plan Severe VSL - The Responsible Entity failed to have an event reporting Operating Plan
For reporting consistency, under the Event Type labeled "Generation Loss", in Appendix 1 of EOP-004-2, Oncor recommends that the reporting threshold of 1,000 KW for the ERCOT Interconnection be raised to 1,400 MW to match the 1,000 MW level in the current version of the ERO Event Analysis Program. Under the Event Type labeled "Damage or Destruction of a "Facility", Appendix 1, with the threshold that states," Damage or destruction of its Facility that results from actual or suspected intentional human action", Oncor suggest the addition of the following language to address intentional human action that is theft in nature but is not intended to disrupt the normal operation of the BES: "Do not report theft unless it degrades the normal operation of a Facility."
Individual
Tony Kroskey
Brazos Electric Power Cooperative, Inc.

Individual
Alice Ireland
Xcel Energy
Yes
No
The VSLs for column for R2 provide a range of severity based on the number of contacts made (or not made) but this seems to be arbitrarily defined. A smaller entity may only have two or three contacts so missing one or more here may be a much higher risk than for a larger utility that may have ten or more contacts. The VSLs should be drafted to include percentages instead of whole numbers. The Lower VSL column for R3 states, "…OR The Responsible Entity validated 75% or more of the contact information contained in the operating plan." This could be interpreted that even someone completed 100% (which is more than 75%) a low VSL could be assigned. This VSL should be drafted in similar fashion to the Moderate, High and Severe VSLs and include a range (i.e. less than 100% but more than 75%).
In attachment one, the "Threshold for Reporting" under Damage or Destruction of a Facility appears to closely follow the definition of sabotage that EOP-004-2 says it is trying to do away with. This definition should be drafted to better correlate with the other physical threats and include the language, "which has the potential to degrade the normal operation of the Facility". Additionally in Attachment 1, both the Physical threats to a Facility and Physical threats to a BES control center include the wording, "Suspicious device or activity…". What constitutes suspicious activity? With no definition this interpretation is left to the Entity which is again something the DSR SDT says they would like to eliminate. Lastly, in the Guideline and Technical Basis section, under A Reporting Process Solution – EOP-004 it states, "A proposal discussed with the FBI, FERC Staff, NERC Standards Project Coordinator and the SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Reportable Events). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial or local level law enforcement agency. The state or provincial or local level law enforcement agency will coordinate with law enforcement with jurisdiction to investigate. If the state or provincial or local level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial or local level law enforcement agency will notify and coordinate with the FBI or the RCMP." This appears to be in direct conflict with the Rationale for R1 which states, "An existing procedure that meets the requirements of CIP-001-2a may be included in this Operating Plan along with other processes, procedures or plans to meet this requirement." CIP-001-2a required "communication contacts, as applicable, with local Federal Bureau of Investigation (FBI)…" so if the CIP-001-2a procedure is included this does not seem to meet the requirements of the operating plan required under EOP-004-2. Also, if the intent of the Operating Plan is to include all local law enforcement and not FBI the operating plan would become very detailed and when validated annually as required in R3, this becomes very burdensome on an entity.

Meeting Results

Project 2009-01
Memo to NERC Project Ballot Body for Recirculation Ballot
October 15, 2012

The Disturbance and Sabotage Reporting standard drafting team has opted to pursue a recirculation ballot for EOP-004-2 after making a few clarifications to the Guidelines and Technical Basis section to address stakeholder concerns raised during the second successive ballot.

Distribution Providers – Some concerns were raised with respect to applicability of the standard to all Distribution Providers. The concerns relate to DPs that do not own BES Facilities. While these entities would not have any events to report under R2, they would still be applicable under R1 and R3. The team discussed this issue and has addressed this concern with additional language in the Guidelines and Technical Basis section of the standard.

Duplicative Reporting – If an entity is registered as an RC, BA and TOP, they should only have to submit a single report. The team discussed and has addressed this concern with additional language in the Guidelines and Technical Basis section of the standard. With regards to the concern regarding multiple entities submitting a report for the same event, the team does not see this as being an issue for industry and will not make any further revisions to address this.

Other issues were raised by stakeholders and a discussion of those is below:

Paragraph 81 – On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process, and in Paragraph 81 ("P81"), invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired.

In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2.

Phase 2 of the Paragraph 81 project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. Until such time, CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-004-2 is not approved by the industry, those standards will remain as is, and subject to the Compliance Monitoring and Enforcement Program.

Reporting – Some comments were submitted regarding the reporting burden of this standard. The revised standard combines two standards into one and removes the analysis portion of the current mandatory and enforceable standards (EOP-004-1 and CIP-001-2a). The analysis provisions will be addressed in the NERC Events Analysis Program upon approval of EOP-004-2. This revised standard involves notification only and does not require any investigation or analysis.

Attachment 1 comments – Many suggestions were made regarding the events listed in Attachment 1. The team has reviewed all of these comments and determined that they would be substantive changes by definition. The team has elected to move forward to recirculation ballot (which precludes substantive revisions to the standard) therefore, these suggestions cannot be incorporated at this time. These comments will be entered into the NERC Issues data base for consideration when the standard is reviewed during the required periodic review cycle.

Consideration of Comments

Project 2009-01 Disturbance Sabotage and Reporting

The Project 2009-01 Drafting Team thanks all commenters who submitted comments on Draft 5 of EOP-004-2. The standard was posted for a 30-day public comment period from August 29, through September 27, 2012. Stakeholders were asked to provide feedback on the standard and associated documents through a special electronic comment form. There were 56 sets of comments, including comments from approximately 181 different people from approximately 125 companies, representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

Summary Consideration:

The Disturbance and Sabotage Reporting standard drafting team has opted to pursue a recirculation ballot for EOP-004-2 after making a few clarifications to the Guidelines and Technical Basis section to address stakeholder concerns raised during the second successive ballot:

- Distribution Providers – Some concerns were raised with respect to applicability of the standard to all Distribution Providers. The concerns relate to DPs that do not own BES Facilities. While these entities would not have any events to report under R2, they would still be applicable under R1 and R3. The team discussed this issue and has addressed this concern with additional language in the Guidelines and Technical Basis Section of the standard as follows:

  "Distribution Provider Applicability Discussion

  The DSR SDT has included Distribution Providers (DP) as an applicable entity under this standard. The team realizes that not all DPs will own BES Facilities and will not meet the "Threshold for Reporting" for any event listed in Attachment 1. These DPs will not have

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

any reports to submit under Requirement R2. However, these DPs will be responsible for meeting Requirements R1 and R3. The DSR SDT does not intend for these entities to have a detailed Operating Plan to address events that are not applicable to them. In this instance, the DSR SDT intends for the DP to have a very simple Operating Plan that includes a statement that there are no applicable events in Attachment 1 (to meet R1) and that the DP will review the list of events in Attachment 1 each year (to meet R3). The team does not think this will be a burden on any entity as the development and annual validation of the Operating Plan should not take more that 30 minutes on an annual basis. If a DP discovers applicable events during the annual review, it is expected that the DP will develop a more detailed Operating Plan to comply with the requirements of the standard."

- Duplicative Reporting – If an entity is registered as an RC, BA and TOP, they should only have to submit a single report. The team discussed and has addressed this concern with additional language in the Guidelines and Technical Basis Section of the standard as follows:

  "Multiple Reports for a Single Organization

  For entities that have multiple registrations, the DSR SDT intends that these entities will only have to submit one report for any individual event. For example, if an entity is registered as a Reliability Coordinator, Balancing Authority and Transmission Operator, the entity would only submit one report for a particular event rather submitting three reports as each individual registered entity."

  With regards to the concern regarding multiple entities submitting a report for the same event, the team does not see this as being an issue for industry and will not make any further revisions to address this.

Other issues were raised by stakeholders and a discussion of those is below:

- **24 Hour Reporting** – Several stakeholders had concerns regarding the 24 hour reporting requirement. Commenters suggest that events or situations affecting real time reliability to the system already are required to be reported to appropriate Functional Entities that have the responsibility to take action. Adding one more responsibility to system operators increases the operator's burden, which reduces the operator's effectiveness when operating the system. Care should be given when placing additional responsibility on the system operators. Allowing reporting at the end of the next business day gives operators the flexibility to allow support staff to assist with after-the-fact reporting requirements. To this end, the DSR SDT has added clarifying language to R2 as follows:

R2. Each Responsible Entity shall report events per their Operating Plan within 24 hours of recognition of meeting an event type threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

- **Paragraph 81** – On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 of that order ("P81"), invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program.

- **Reporting** – Some comments were submitted regarding the reporting burden of this standard. The revised standard combines two standards into one and removes the analysis portion of the current mandatory and enforceable standards (EOP-004-1 and CIP-001-2a). The analysis provisions will be addressed in the NERC Events Analysis Program upon approval of EOP-004-2. This revised standard involves notification only and does not require any investigation or analysis.

- **Attachment 1 comments** – Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. . The team has elected to move forward to recirculation ballot.

- **Violation Risk Factors** - Many stakeholders had concerns with the VRFs for R2 and R3 being assigned as "medium". The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower

the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.

- **Violation Severity Levels** - Other stakeholders suggested revision to the VSLs for Requirement R1 based on if the event reporting Operating Plan fails to include one or more of the event types listed in Attachment 1. The SDT agrees and has revised the VSLs for R1 as follows:

  Lower: The Responsible Entity had an Operating Plan, but failed to include one applicable event type.

  Moderate: The Responsible Entity had an Operating Plan, but failed to include two applicable event types.

  High: The Responsible Entity had an Operating Plan, but failed to include three applicable event types.

  Severe: The Responsible Entity had an Operating Plan, but failed to include four or more applicable event types OR the Responsible Entity failed to have an event reporting Operating Plan.

Index to Questions, Comments, and Responses

1. The DSR SDT has revised EOP-004-2 by combining Requirements R3 and R4 into a single requirement (Requirement R3) to, "… validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year." Do you agree with this revision? If not, please explain in the comment area below. 15
2. The DSR SDT has revised the VSLs to reflect the language in the revised requirements. Do you agree with the proposed VRFs and VSLs? If not, please explain in the comment area below. 25
3. Do you have any other comment, not expressed in the questions above, for the DSR SDT?.....37

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Carmen Agavriloai	Independent Electricity System Operator	NPCC	2
3.	Greg Campoli	New York Independent System Operator	NPCC	2
4.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
5.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
7.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
8.	Kathleen Goodman	ISO - New England	NPCC	2

Group/Individual		Commenter	Organization		Registered Ballot Body Segment									
					1	2	3	4	5	6	7	8	9	10
9.	Michael Jones	National Grid	NPCC	1										
10.	David Kiguel	Hydro One Networks Inc.	NPCC	1										
11.	Michael Lombardi	Northeast Utilities	NPCC	1										
12.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9										
13.	Bruce Metruck	New York Power Authority	NPCC	6										
14.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5										
15.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10										
16.	Robert Pellegrini	The United Illuminating Company	NPCC	1										
17.	Si-Truc Phan	Hydro-Quebec TransEnergie	NPCC	1										
18.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5										
19.	Brian Robinson	Utility Services	NPCC	8										
20.	Michael Schiavone	National Grid	NPCC	1										
21.	Wayne Sipperly	New York Power Authority	NPCC	5										
22.	Donald Weaver	New Brunswick System Operator	NPCC	2										
23.	Ben Wu	Orange and Rockland Utilities	NPCC	1										
24.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3										
2.	Group	Ron Sporseen	PNGC Comment Group		X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumer's Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3
7.	Rick Crinklaw	Lane Electric Cooperative	WECC	3
8.	Annie Terracciano	Northern Lights Inc.	WECC	3
9.	Aleka Scott	PNGC Power	WECC	4
10.	Heber Carpenter	Raft River Electric Cooperative	WECC	3
11.	Steve Eldrige	Umatilla Electric Cooperative	WECC	1, 3
12.	Marc Farmer	West Oregon Electric Cooperative	WECC	4

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
13.	Margaret Ryan	PNGC Power	WECC 8										
14.	Rick Paschall	PNGC Power	WECC 3										
3.	Group	Greg Rowland	Duke Energy	X		X		X	X				
	Additional Member	**Additional Organization**	**Region** / **Segment Selection**										
1.	Doug Hils	Duke Energy	RFC 1										
2.	Lee Schuster	Duke Energy	FRCC 3										
3.	Dale Goodwine	Duke Energy	SERC 5										
4.	Greg Cecil	Duke Energy	RFC 6										
4.	Group	Chang Choi	Tacoma Public Utilities	X		X	X	X	X				
	Additional Member	**Additional Organization**	**Region** / **Segment Selection**										
1.	Chang Choi	City of Tacoma	WECC 1										
2.	Travis Metcalfe	Tacoma Public Utilities	WECC 3										
3.	Keith Morisette	Tacoma Public Utilities	WECC 4										
4.	Chris Mattson	Tacoma Power	WECC 5										
5.	Michael Hill	Tacoma Public Utilities	WECC 6										
5.	Group	Kent Kujala	Detroit Edison			X	X	X					
	Additional Member	**Additional Organization**	**Region** / **Segment Selection**										
1.	Alexander Eizans		RFC 3, 4, 5										
2.	Barbara Holland		RFC 3, 4, 5										
3.	Jeffrey DePriest		RFC 3, 4, 5										
6.	Group	Gerry Beckerle	SERC OC Standards Review Group	X		X							
	Additional Member	**Additional Organization**	**Region** / **Segment Selection**										
1.	Roger Powers	City of Springfield, IL - CWLP	SERC 1, 3										
2.	Dan Roethemeyer	Dynegy	SERC 5										
3.	Melinda Montgomery	Entergy	SERC 1, 3, 6										
4.	Terry Bilke	MISO	SERC 2										
5.	Scott Brame	NCEMC	SERC 4, 1, 3, 5										
6.	William Berry	OMU	SERC 3, 5										

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Tim Hattaway	PowerSouth	SERC 1, 5										
8. Brett Koelsch	Progress Energy Carolinas	SERC 1, 3, 5, 6										
9. Vicky Budreau	SCPSA	SERC 1, 3, 5, 6										
10. Gary Hutson	SMEPA	SERC 1, 3, 5, 6										
11. Marsha Morgan	Southern Co. Services	SERC 1, 5										
12. Randy Hubbert	Southern Co. Services	SERC 1, 5										
13. Joel Wise	TVA	SERC 1, 3, 5, 6										
14. Stuart Goza	TVA	SERC 1, 3, 5, 6										
15. Jim Case	Entergy	SERC 1, 3, 6										
16. Mike Bryson	PJM	SERC 2										
17. Mike Hirst	Cogentrix	SERC 5										
7. Group	Larry Raczkowski	FirstEnergy	X		X	X	X	X				
Additional Member	**Additional Organization**	**Region** / **Segment Selection**										
1. William J Smith	FirstEnergy Corp	RFC 1										
2. Stephan Kern	FirstEnergy Energy Delivery	RFC 3										
3. Douglas Hohlbaugh	Ohio Edison Company	RFC 4										
4. Kenneth Dresner	FirstEnergy Solutions	RFC 5										
5. Kevin Querry	FirstEnergy Solutions	RFC 6										
8. Group	Mike Garton	Dominion	X		X	X	X					
Additional Member	**Additional Organization**	**Region** / **Segment Selection**										
1. Louis Slade	Dominion Resources Services, Inc.	RFC 5, 6										
2. Randi Heise	Dominion Resources Services, Inc.	MRO 5, 6										
3. Connie Lowe	Dominion Resources Services, Inc.	NPCC 5, 6										
4. Mike Crowley	Virginia Electric and Power Company	SERC 1, 3, 5, 6										
9. Group	WILL SMITH	MRO NSRF	X	X	X	X	X	X				
Additional Member	**Additional Organization**	**Region** / **Segment Selection**										

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

1.	CHUCK LAWRENCE	ATC	MRO	1
2.	TOM BREENE	WPS	MRO	3, 4, 5, 6
3.	JODI JENSON	WAPA	MRO	1, 6
4.	KEN GOLDSMITH	ALTW	MRO	4
5.	ALICE IRELAND	XCEL/NSP	MRO	1, 3, 5, 6
6.	DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6
7.	ERIC RUSKAMP	LES	MRO	1, 3, 5, 6
8.	JOE DEPOORTER	MGE	MRO	3, 4, 5, 6
9.	SCOTT NICKELS	RPU	MRO	4
10.	TERRY HARBOUR	MEC	MRO	1, 3, 5, 6
11.	MARIE KNOX	MISO	MRO	2
12.	LEE KITTELSON	OTP	MRO	1, 3, 5
13.	SCOTT BOS	MPW	MRO	1, 3, 5
14.	TONY EDDLEMAN	NPPD	MRO	1, 3, 5
15.	MIKE BRYTOWSKI	GRE	MRO	1, 3, 5, 6
16.	DAN INMAN	MPC	MRO	1, 3, 5, 6

				1	2	3	4	5	6	7	8	9	10
10.	Group	Chris Higgins	Bonneville Power Administration	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Jim Burns	BPA, Technical Operations	WECC	1
2.	Fran Halpin	BPA, Duty Scheduling	WECC	5
3.	Erika Doot	BPA, Generation Support	WECC	3, 5, 6
4.	John Wylder	BPA, Transmission	WECC	1
5.	Deanna Phillips	BPA, FERC Compliance	WECC	1, 3, 5, 6
6.	Russell Funk	BPA, Transmission	WECC	1

				1	2	3	4	5	6	7	8	9	10
11.	Group	Robert Rhodes	SPP Standards Review Group		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Allen	City Utilities of Springfield	SPP	1, 4
2.	Doug Callison	Grand River Dam Authority	SPP	1, 3, 5
3.	Jonathan Hayes	Southwest Power Pool	SPP	2
4.	Bo Jones	Westar Energy	SPP	1, 3, 5, 6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
5. Allen Klassen	Westar Energy	SPP	1, 3, 5, 6										
6. Tiffany Lake	Westar Energy	SPP	1, 3, 5, 6										
7. Tara Lightner	Sunflower Electric Power Corporation	SPP	1										
8. Kyle McMenamin	Xcel Energy	SPP	1, 3, 5, 6										
9. Jerry McVey	Sunflower Electric Power Corporation	SPP	1										
10. Fred Meyer	Empire District Electric Company	SPP	1										
11. Terri Pyle	Oklahoma Gas & Electric Company	SPP	1, 3, 5										
12. Don Schmit	Nebraska Publlic Power District	MRO	1, 3, 5										
13. Katie Shea	Westar Energy	SPP	1, 3, 5, 6										
14. Sean Simpson	Board of Public Utilities, City of McPherson	SPP	NA										
15. Bryan Taggart	Westar Energy	SPP	1, 3, 5, 6										
16. Mark Wurm	Board of Public Utilities, City of McPherson	SPP	NA										
12. Group	Jason Marshall	ACES Power Marketing Standards Collaborators							X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Susan Sosbe	Wabash Valley Power Association	RFC	3										
2. Clem Cassmeyer	Western Farmers Electric Cooperative	SPP	1, 5										
3. Megan Wagner	Sunflower Electric Power Corporation	SPP	1										
4. Scott Brame	North Carolina Electric Membership Corporation	SERC	1, 3, 4, 5										
5. Bob Solomon	Hoosier Energy	RFC	1										
6. Robert Thomasson	Big Rivers Electric Corporation	SERC											
7. Shari Heino	Brazos Electric Power Cooperative	ERCOT	1, 5										
8. John Shaver	Arizona Electric Power Cooperative	WECC	4, 5										
9. John Shaver	Southwest Transmission Cooperative	WECC	1										
10. Mohan Sachdeva	Buckeye Power	RFC	3, 4										
11. Michael Brytowski	Great River Energy	MRO	1, 3, 5, 6										
13. Individual	Janet Smith, Regulatory Affairs Supervisor	Arizona Public Service Company		X		X		X	X				
14. Individual	Emily Pennel	Southwest Power Pool Regional Entity											X

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
15.	Individual	Antonio Grayson	Southern Company	X		X		X	X				
16.	Individual	Daniela Hammons	CenterPoint Energy	X									
17.	Individual	Lee Layton	Blue Ridge EMC	X		X							
18.	Individual	Anthony Jablonski	ReliabilityFirst										X
19.	Individual	Jonathan Appelbaum	The United Illuminating Company	X									
20.	Individual	Russ Schneider	Flathead Electric Cooperative, Inc.			X	X						
21.	Individual	Oliver Burke	Entergy Services, Inc. (Transmission)	X									
22.	Individual	Nazra Gladu	Manitoba Hydro	X		X		X	X				
23.	Individual	Steve Grega	Lewis County PUD	X				X					
24.	Individual	Steve Alexanderson P.E.	Central Lincoln			X	X					X	
25.	Individual	Jack Stamper	Clark Public Utilities	X									
26.	Individual	Russell A. Noble	Cowlitz PUD			X	X	X					
27.	Individual	Chantel Haswell	Public Service Enterprise Group	X		X		X	X				
28.	Individual	Mike Hirst	Cogentrix Energy					X					
29.	Individual	Dave Willis	Idaho Power Co.	X		X							
30.	Individual	Michelle R D'Antuono	Ingelside Cogeneration LP					X					
31.	Individual	Howard Rulf	Wisconsin Electric Power company dba We Energies			X	X	X					
32.	Individual	Melissa Kurtz	US Army Corps of Engineers					X					
33.	Individual	David Jendras	Ameren Services	X		X		X	X				
34.	Individual	Michael Falvo	Independent Electricity System Operator		X								
35.	Individual	RoLynda Shumpert	South Carolina Electric and Gas	X		X		X	X				
36.	Individual	David Revill	Georgia Transmission Corporation	X									
37.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
38.	Individual	Andrew Z.Pusztai	american Transmission Company	X									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
39.	Individual	Don Schmit	Nebraska Public Power Disstrict	X		X		X					
40.	Individual	Terry Harbour	MidAmerican Energy	X		X		X	X				
41.	Individual	Kathleen Goodman	ISO New England Inc.		X								
42.	Individual	d mason	City and County of San Francisco - Hetch Hetchy Water and Power					X					
43.	Individual	Tracy Richardson	Springfield Utility Board			X							
44.	Individual	Rich Salgo	NV Energy	X		X		X					
45.	Individual	Thad Ness	American Electric Power	X		X		X	X				
46.	Individual	Charles Yeung	Southwest Power Pool RTO		X								
47.	Individual	Nathan Mitchell	American Public Power Association			X	X						
48.	Individual	Don Jones	Texas Reliability Entity										X
49.	Individual	Christine Hasha	ERCOT		X								
50.	Individual	Denise M. Lietz	Puget Sound Energy Inc.	X		X		X					
51.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				
52.	Individual	Christina Bigelow	Midwest Independent Transmission System Operator, Inc.		X								
53.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
54.	Individual	Darryl Curtis	Oncor Electric Delivery	X									
55.	Individual	Tony Kroskey	Brazos Electric Power Cooperative, Inc.	X									
56.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				

If you wish to express support for another entity's comments without entering any additional comments, you may do so here.

Organization	Supporting Comments of "Entity Name"
PNGC Comment Group	Central Lincoln PUD
Blue Ridge EMC	R3 is another example of a "paper chase", creating (or rather continuing) an administrative burden for the utility. The standard should only require that the entity have a plan and the accountability should be "did the entity follow the plan when needed, including proving that the appropriate contacts were made?"
Response: Thank you for your comment. Requirement R3 is in direct response to a FERC directive in Order 693 and as such, the SDT included this provision. Also, if the information in the plan is out of date, then the plan will not be effective.	
Flathead Electric Cooperative, Inc.	Central Lincoln
US Army Corps of Engineers	MRO NSRF
Nebraska Public Power District	Midwest Reliability Organization (MRO) NERC Standards Review Forum (NSRF); AND Southwest Power Pool RTO
MidAmerican Energy	MidAmerican supports the MRO NSRF comments
ISO New England Inc.	NPCC

1. **The DSR SDT has revised EOP-004-2 by combining Requirements R3 and R4 into a single requirement (Requirement R3) to, "… validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year." Do you agree with this revision? If not, please explain in the comment area below.**

Summary Consideration: The majority of stakeholders agree with the combination of R3 and R4 and with the new language of R3 to "validate" the contact information. A few commenters suggested that Requirement R3 is administrative and should be removed under the provisions of "Paragraph 81". On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 ("P81") invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program.

Organization	Yes or No	Question 1 Comment
CenterPoint Energy	No	CenterPoint Energy supports the concept of combining Requirements R3 and R4; however, the Company still prefers an annual review requirement which would include validating the contact information and content of the Operating Plan overall. Therefore, CenterPoint Energy recommends the following revised language for Requirement R3: "Each Responsible Entity shall review and update the Operating Plan at least every 15 months." The Company also suggests that the Measure be worded as follows: "Evidence may include, but is not limited to dated documentation reflecting changes to the Operating Plan including updated contact information if necessary."

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comment. The SDT appreciates the suggestion on validating the content of the Operating Plan, but at this time, we feel that the step is not necessary to meet the directive from FERC Order 693. As to the comment on extending the review period to 15 months, following much discussion and review of the industry comments, we are staying with the language as proposed.		
American Electric Power	No	In the spirit of Paragraph 81 efforts, we request the removal of R3 as it is solely administrative in nature, existing only to support R2. This is more of an internal control and does not appear to rise to the level of being an industry-wide requirement. In addition, having two requirements rather than one increases the likelihood of being found non-compliant for multiple requirements rather than a single requirement.
Response: Thank you for your comment. Requirement R3 is in direct response to a FERC directive in Order 693 and as such, the SDT included this provision. On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 ("P81") invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. , CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program. As the SDT is moving forward with a Recirculation Ballot, your suggestions will be forwarded to NERC for future consideration.		
City and County of San Francisco - Hetch Hetchy Water and Power	No	Measure M3 specifically identifies two types of acceptable compliance evidence: Voice Recording and Log entries. Specifying only these two forms of evidence creates a risk that some auditors will reject other forms of R3 compliance evidence which are equally valid, such as emails or written call records. Although M3 states that acceptable evidence is not limited to Voice Recordings or Log Entries, we have concern that other

Organization	Yes or No	Question 1 Comment
		methods of complying with R3 may not be accepted.
Response: Thank you for your comment. The SDT believes that the phrase "may include, but are not limited to" addresses your concern. The SDT will present your comment to the NERC Compliance staff in an effort to inform audit staffs on what evidence is permissible.		
Blue Ridge EMC	No	See previous comments
Response: Thank you for previous comments. Requirement R3 is in direct response to a FERC directive in Order 693 and as such, the SDT included this provision. Also, if the information in the plan is out of date, then the plan will not be effective.		
Detroit Edison	No	The requirement is too prescriptive and difficult to document. Requirement should be for annual review of Operating Plan. This allows for entity to review plan and document this the same as other Standards that require annual review (i.e. annual review blocks on documents).The requirement as written is vague and difficult to document. Annual review of reporting process is already a requirement.
Response: Thank you for your comments. While the SDT appreciates the view that the Operating Plan should be reviewed annually, the SDT feels that the requirement only needs to address the validity of the contact information contained within the Operating Plan in order to meet the FERC directive in Order 693. If the entity is aware of changes within its operations that would make a more extensive review advisable, it can choose to do so; but where there have been no significant changes to an entity's operations in the last year, ensuring the validity of the contact information should be sufficient.		
Manitoba Hydro	No	This seems like an administrative only requirement. It would be too difficult to validate or measure.
Response: Thank you for your comment. Requirement R3 is in direct response to a FERC directive in Order 693 and as such, the SDT included this provision. The measure calls for an entity to have "dated records to show that it validated all contact information contained in the Operating Plan each calendar year. Such evidence may include, but are not limited to, dated voice recordings and operating logs or other communication documentation." The SDT does not believe that this is an administrative		

Organization	Yes or No	Question 1 Comment
requirement because, if the information in the Operating Plan is out of date, then the plan will not be effective.		
ACES Power Marketing Standards Collaborators	No	We believe that the revision to R3 and elimination of R4 are great improvements to the standard as a lot of the unnecessary burdens have been removed. However, Requirement R3 is still not needed, has several issues with it and should be eliminated. (1) While validating contact information annually in a reporting plan makes sense, it does not rise to level of importance of requiring sanctions for failure to do so. Furthermore, it does nothing to assure reliability. Shortly after the contact information has been updated, it could change. This does not mean that validation should be more frequent but simply that is an unnecessary administrative burden. If contact information changes, the registered entity will have to find it. For reliability purposes, why does it matter if they do this in the 24-hour reporting period after the event or annually before the event? (2) Requirement R3 is administrative and is not consistent with the recent direction that NERC and FERC have taken toward compliance. Violations of this requirement are likely to be candidates for FFT treatment and this is exactly the kind of requirement that FERC invited NERC to propose for retirement in Paragraph 81 of the order approving the FFT process. Furthermore, it appears to meet at least two criteria (Administrative and periodic updates) that the Paragraph 81 drafting team has proposed to use to identify candidate requirements for retirement. The requirement is also not consistent with the direction NERC has taken on internal controls. How is an auditor reviewing that contact information has been updated in an Operating Plan forward looking or for that matter beneficial to reliability? Imagine a registered entity fails to update their contact information but still reports an event within the 24 hour reporting time frame to the appropriate parties. They are in technical violation of R3 but have met the spirit of the standard. (3) Requirement R3 is not a results-based requirement. It simply compels a registered entity "how to" meet reporting deadlines. Certainly, if a

Organization	Yes or No	Question 1 Comment
		registered entity has current contact information on hand, it will be easier to notify appropriate parties of events quickly. However, it does limit a registered entity's ability to identify its own unique and possibly better way to meet a requirement. "How to" requirements prevent unique and superior solutions.
Response: Thank you for your comment. Requirement R3 is in direct response to a FERC directive in Order 693 and as such, the SDT included this provision. The SDT does not believe that this is an administrative requirement because, if the information in the Operating Plan is out of date, then the plan will not be effective. **On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 ("P81") invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program. As the SDT is moving forward with a Recirculation Ballot, your suggestions will be forwarded to NERC for future consideration.**		
NV Energy	No	Without further clarification of what is expected by "validate all contact information" I cannot support this requirement. On the surface, "validate" appears to be acceptable terminology, as it means to me a review of the contact names and contact information (perhaps cell #, home phone, text address, email address, etc) that would be evidenced through an attestation of completion of review along with records showing the updates made to the contact information pursuant to the review. However, when the Measure is considered, it refers to evidence such as operator logs, voice recordings, etc. This seems to indicate that the

Organization	Yes or No	Question 1 Comment
		expectation is that each contact is tested, by dialing, texting, emailing, etc with some sort of confirmation that each contact was successful. If this is what is necessary to satisfy the "validate" requirement, I believe it is excessive, burdensome and unnecessary. I suggest modification of the Measure language to clearly allow for an entity to demonstrate compliance by a showing that it reviewed the contact information and made changes as deemed necessary by its review, and to remove the reference to operator logs and voice recordings as the evidence of measure.
Response: Thank you for your comment. The SDT agrees with your comment and views your direction as being consistent with the standard's intent. The SDT will submit your comment to NERC Compliance staff for their consideration. The SDT intends for operator logs and voice recordings to be acceptable as evidence, but not the only acceptable evidence. The use of the language "such as" in the measure indicates this.		
Bonneville Power Administration	Yes	BPA agrees with the revision and recognizes that it will involve a large amount of validation workload for entities with a large footprint.
Response: Thank you for your comment.		
Dominion	Yes	Dominion supports the combination of Requirements R3 and R4 into a single requirement (Requirement R3), although we remain concerned that validation requiring a phone call could be perceived as a nuisance by that entity.
Response: Thank you for your comment. The SDT appreciates this concern but feels that the requirement is necessary to address the FERC directive in the Order 693. The SDT does not believe that validation of the contact information will be a nuisance. If the information in the Operating Plan is out of date, then the plan will not be effective.		
Duke Energy	Yes	Duke Energy commends the excellent work of the Standard Drafting Team in incorporating previous comments into the current posted draft of the

Organization	Yes or No	Question 1 Comment
		standard.
Response: Thank you for your comment.		
ERCOT	Yes	ERCOT considers replacing R3 and R4 with the new R3 is an improvement and we thank the drafting team for making the change.
Response: Thank you for your comment.		
ReliabilityFirst	Yes	Even though ReliabilityFirst votes in the Affirmative, we offer the following comment regarding Requirement R3 for consideration. ReliabilityFirst recommends changing the word "validate" to "verify" in Requirement R3. ReliabilityFirst believes not only does the entity need to validate contact information is correct, they should verify (i.e. authenticate though test) that the contact information is correct.
Response: Thank you for your comment. The SDT feels that the action you define is consistent with our intent.		
Independent Electricity System Operator	Yes	IESO agrees that the intent of Requirement R3 to have the Registered Entities validate the contact information in the contact lists that they may have for the events applicable to them is achieved. IESO also agrees that the elimination of conducting an annual test of the communications process and review of the event reporting Operating Plan in merging the previous R3 and R4 into this new R3 will give entities an opportunity to develop a plan that suits its business needs.
Response: Thank you for your comment.		
Indiana Municipal Power Agency	Yes	IMPA agrees with the removal of a "test" and going with a validation requirement for the contact information in the Operating Plan.

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comment.		
Ingelside Cogeneration LP	Yes	Ingleside Cogeneration believes that an annual validation of contact information is sufficient for a reporting procedure. R2 provides sufficient impetus for Responsible Entities to keep their Operating plan current - as a missed report will lead to a violation. Furthermore, external agencies and law enforcement officials will be reluctant to participate in validation tests, as dozens of nearby BES entities will overwhelm them with such requests.
Response: Thank you for your comment. Requirement R3 is in direct response to a FERC directive in Order 693 and as such, the SDT included this provision. If the information in the Operating Plan is out of date, then the plan will not be effective.		
SPP Standards Review Group	Yes	We feel that replacing R3 and R4 with the new R3 is an improvement and we thank the drafting team for making the change.
Response: Thank you for your support.		
PNGC Comment Group	Yes	
Tacoma Public Utilities	Yes	
SERC OC Standards Review Group	Yes	
FirstEnergy	Yes	
MRO NSRF	Yes	
Arizona Public Service Company	Yes	
Southwest Power Pool Regional Entity	Yes	

Organization	Yes or No	Question 1 Comment
Southern Company	Yes	
The United Illuminating Company	Yes	
Entergy Services, Inc. (Transmission)	Yes	
Lewis County PUD	Yes	
Central Lincoln	Yes	
Clark Public Utilities	Yes	
Cowlitz PUD	Yes	
Public Service Enterprise Group	Yes	
Cogentrix Energy	Yes	
Idaho Power Co.	Yes	
Wisconsin Electric Power company dba We Energies	Yes	
Ameren Services	Yes	
South Carolina Electric and Gas	Yes	
Georgia Transmission Corporation	Yes	
City of Austin dba Austin Energy	Yes	
american Transmission Company	Yes	

Organization	Yes or No	Question 1 Comment
MidAmerican Energy	Yes	
Springfield Utility Board	Yes	
Southwest Power Pool RTO	Yes	
American Public Power Association	Yes	
Texas Reliability Entity	Yes	
Puget Sound Energy Inc.	Yes	
Exelon Corporation and its affiliates	Yes	
Midwest Independent Transmission System Operator, Inc.	Yes	
Oncor Electric Delivery	Yes	
Xcel Energy	Yes	

2. The DSR SDT has revised the VSLs to reflect the language in the revised requirements. Do you agree with the proposed VRFs and VSLs? If not, please explain in the comment area below.

Summary Consideration: Many stakeholders had concerns with the VRFs for R2 and R3 being assigned as "medium". The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.

Other stakeholders suggested revision to the VSLs for Requirement R1 based on if the event reporting Operating Plan fails to include one or more of the event types listed in Attachment 1. The SDT agrees and has added the following VSLs to R1, in addition to the language that was previously included in the "Severe" VSL:

Lower: The Responsible Entity had an Operating Plan, but failed to include one applicable event type.

Moderate: The Responsible Entity had an Operating Plan, but failed to include two applicable event types.

High: The Responsible Entity had an Operating Plan, but failed to include three applicable event types.

Severe: The Responsible Entity had an Operating Plan, but failed to include four or more applicable event types.

Organization	Yes or No	Question 2 Comment
Detroit Edison	No	Under VSLs for R2- We disagree with the reporting time frames. Making the time requirement as soon as 24 hours puts this reporting requirement on the real time operators. Many of the situations listed in the EOP-004 attachment are not included in the OE-417 report. The Unofficial Comment Form states the reporting obligations serve to provide input to the NERC Event Analysis Program. This program has removed the 24 hour reporting requirement and

Organization	Yes or No	Question 2 Comment
		changed it to 5 business days.
Response: Thank you for your comments. The reporting obligation under this standard is to provide notification of events to NERC Situation Awareness group. The SDT, in consultation with the DOE and NERC Events Analysis group, have recognized the where there is duplication of reporting and provided for the common use of the different group's forms. This standard is not a replacement or substitution for any other obligations to other agencies. However, the SDT recognizes the concern with having real time operations staff submitting the report. To this end, the DSR SDT has added clarifying language to R2 as follows: **R2. Each Responsible Entity shall report events per their Operating Plan within 24 hours of meeting an event type threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). [Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]**		
Texas Reliability Entity	No	(1) VSLs for R1 should have a lower level VSL if the event reporting Operating Plan fails to include one or more of the event types listed in Attachment 1. (2) VSL for R1 is incorrectly stated as there are no "parts" to R1.
Response: Thank you for your comment. 1) The SDT agrees and has added the following VSLs for R1, in addition to the language that was previously included in the "Severe" VSL: **Lower: The Responsible Entity had an Operating Plan, but failed to include one applicable event type.** **Moderate: The Responsible Entity had an Operating Plan, but failed to include two applicable event types.** **High: The Responsible Entity had an Operating Plan, but failed to include three applicable event types.** **Severe: The Responsible Entity had an Operating Plan, but failed to include four or more applicable event types.** **2) This was correct in the clean version of the standard.**		
ACES Power Marketing Standards Collaborators	No	Because R3 is administrative, the VRF should be Lower. The requirement simply compels that that registered entity update a document which is purely administrative.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a		

Organization	Yes or No	Question 2 Comment
is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.		
Bonneville Power Administration	No	BPA does not agree with the VRFs and VSLs. BPA believes that the violation levels for administrative errors are too high. For more information, please reference comments to question #3.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF. Please see the response to your question 3 comments.		
CenterPoint Energy	No	CenterPoint Energy suggests that the phrase "which caused a negative impact to the Bulk Electric System" be added to each Violation Severity Level. For example, the wording would appear as follows: "The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 24 hours but less than or equal to 36 hours after meeting an event threshold for reporting which caused a negative impact to the Bulk Electric System". Additionally or alternatively, the Company proposes that the above phrase be added to the Threshold(s) for Reporting in Attachment 1 to focus on events that have an impact or effect on the Bulk Electric System.
Response: Thank you for your comment. The SDT does not believe such a change is necessary. Each event type listed is applicable to BES reliability.		

Organization	Yes or No	Question 2 Comment
MidAmerican Energy	No	Change the VRFs / VSLs to match suggested changes in Question 3
Response: Thank you for your comment. The SDT followed the NERC guidelines for VSLs in setting the appropriate levels. Please see the response to your question 3 comments.		
The United Illuminating Company	No	Do not agree that the VRF for R3 is medium. Failure to Validate contact information will not likely lead to instability and Cascade. Reporting under EOP-004 is not an immediate action, and given a 24 hour reporting window a proper contact point can be identified on-the-fly. R2 is properly identified as the Medium VRF since a failure to report whether due to an improper Operating plan or improper contact list may lead to a BES cascade.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.		
Southwest Power Pool Regional Entity	No	In R2, SPP RE does not understand why the VSLs are based on who was or was not contacted rather than when it was reported. An entity could decide to put only two entities in its Event Reporting Operating Plan. If the entity fails to submit an appropriate event report, it is open to a Severe VSL on the top set of VSLs but only a moderate on the lower set of VSLs. This seems to be a disconnect for applying the VSLs for the same facts and circumstances.
Response: Thank you for your comment. The SDT followed the NERC guidelines for VSLs in setting the appropriate levels. The VSLs were written based on two potential failures to meet the requirement. The first is based on the time the report was submitted while the second was based on the entity submitting the report within 24 hours but not to all applicable entities.		

Organization	Yes or No	Question 2 Comment
Midwest Independent Transmission System Operator, Inc.	No	MISO agrees with the comments submitted by the SERC Operating Committee that the VRFs for R2 and R3 should be "Lower" instead of "Medium," since these are administrative requirements. MISO further respectfully suggests that implementing another standard that requires reporting every incident identified in a plan within 24 hours and that classifies failure to do so a "Severe" violation, will likely cause entities to limit the scope of their plans. NERC, therefore, would not receive information that appears unimportant to a single entity but could be important in the context of similar events across the country.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF. **The SDT does not agree with your second comment and believes that entities will report the appropriate events.**		
Oncor Electric Delivery	No	Oncor suggest the following additions to VSL language for R1 to align more closely with the measures described in M1Lower VSL - Entity has one applicable event type not properly identified in its event reporting Operating Plan. High VSL - Entity has more than one applicable event type not properly identified in its event reporting Operating Plan. Severe VSL - The Responsible Entity failed to have an event reporting Operating Plan
Response: Thank you for your comment. Based on comments from you and others, we have added the following VSLs for R1, in addition to the language that was previously included in the "Severe" VSL: **Lower: The Responsible Entity had an Operating Plan, but failed to include one applicable event type.**		

Organization	Yes or No	Question 2 Comment
Moderate: The Responsible Entity had an Operating Plan, but failed to include two applicable event types. **High: The Responsible Entity had an Operating Plan, but failed to include three applicable event types.** **Severe: The Responsible Entity had an Operating Plan, but failed to include four or more applicable event types.**		
Exelon Corporation and its affiliates	No	R2 VSLs - By measuring the amount of time taken to report and the number of entities to receive the report, the VSLs track more with size and location than with a failure to report. For instance, an entity failing to report at all to one entity would be deemed a lower VSL while an entity reporting to many, but failing to report to three entities would be deemed a high VSL. R3 VSL - The severe VSLs do not seem commensurate to oversight. A three month delay in validating that phone numbers are correct, for phone numbers that are accurate, does not track with a severe infraction.
Response: Thank you for your comment. The SDT followed the NERC guidelines for VSLs in setting the appropriate levels. The SDT will forward your suggestions to NERC for future consideration of the VSL language.		
Blue Ridge EMC	No	R3 VSLs are silly.
Response: Thank you for your comment. The SDT followed the NERC guidelines for setting the appropriate VSLs.		
Tacoma Public Utilities	No	Regarding the Severe VSL for R1, the reference to "Parts 1.1 and 1.2" appears to be outdated. For R2, change "the Responsible Entity failed to submit an event report...to X entity(ies) within 24 hours" to "the Responsible Entity failed to submit an event report...to only X entity(ies) within 24 hours." (Add 'only.')
Response: Thank you for your comment. The SDT agrees with your first suggestion and this was correct in the clean version of the standard that was posted. Your second suggestion will be forwarded to NERC for future consideration.		

Organization	Yes or No	Question 2 Comment
SPP Standards Review Group	No	Since EOP-004 is about after-the-fact reporting, we suggest that all the VRFs be Lower. This would mean lowering R2 and R3 from Medium. The third component of the Severe VSL for R2 is more severe than the other two components. In an attempt to be more consistent across all the VSLs, we propose the following for the High VSL for R2: The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 48 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to three or more entities identified in its event reporting Operating Plan within 24 hours. We propose the following, deleting the first two components as shown in the current draft, for the Severe VSL for R2: The Responsible Entity failed to submit a report for an event in EOP-004 Attachment 1.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF. **The VSLs were written to account for tardiness of reports, for failing to report to certain entities and for not submitting a report at all. The investigators will apply the appropriate VSL based on the type of violation found.**		
ERCOT	No	Since EOP-004 is related to ex-post reporting, which has nothing to do with operational or planning risk, this is an administrative requirement and, accordingly, the VRFs should all be Low. This would mean lowering the VRF for R2 and R3 to Low. The third component of the Severe VSL for R2 is more severe than the other two components. In an attempt to be more consistent across all the VSLs, we

Organization	Yes or No	Question 2 Comment
		propose the following for the High VSL for R2: The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 48 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to three or more entities identified in its event reporting Operating Plan within 24 hours. ERCOT proposes that the first two components of the Severe VSL for R2 be deleted and replaced with: The Responsible Entity failed to submit a report for an event in EOP-004 Attachment 1.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF. **The VSLs were written to account for tardiness of reports, for failing to report to certain entities and for not submitting a report at all. The investigators will apply the appropriate VSL based on the type of violation found.**		
Duke Energy	No	The Lower VSL for R3 should be clarified. The phrase "validated 75% or more" should be modified to say "validated at least 75% but less than 100%".
Response: Thank you for your comment. The SDT agrees and has made the correction.		
SERC OC Standards Review Group	No	The VRF for R2 should be "Lower" instead of "Medium" since it is administrative which involves reporting events to entities not identified in the Functional Model that have operating responsibilities listed. The VRF for R3 should also be "Lower" instead of "Medium" since it is an administrative requirement.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC		

Organization	Yes or No	Question 2 Comment
Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.		
Southern Company	No	The VRF for R2 should be "Lower" instead of "Medium" since it is administrative which involves reporting events to entities not identified in the Functional Model that have operating responsibilities listed. The VRF for R3 should also be "Lower" instead of "Medium" since it is an administrative requirement. In addition we suggest that the VSL for R1 should have a lower level VSL for an Operating Plan that may have one event type missing from the Operating Plan.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.		
Cogentrix Energy	No	The VRF for R2 should be "Lower" instead of "Medium" since it is administrative which involves reporting events to entities not identified in the Functional Model that have operating responsibilities listed. The VRF for R3 should also be "Lower" instead of "Medium" since it is an administrative requirement.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a		

Organization	Yes or No	Question 2 Comment
is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.		
Xcel Energy	No	The VSLs for column for R2 provide a range of severity based on the number of contacts made (or not made) but this seems to be arbitrarily defined. A smaller entity may only have two or three contacts so missing one or more here may be a much higher risk than for a larger utility that may have ten or more contacts. The VSLs should be drafted to include percentages instead of whole numbers. The Lower VSL column for R3 states,"...OR The Responsible Entity validated 75% or more of the contact information contained in the operating plan." This could be interpreted that even someone completed 100% (which is more than 75%) a low VSL could be assigned. This VSL should be drafted in similar fashion to the Moderate, High and Severe VSLs and include a range (i.e. less than 100% but more than 75%).
Response: Thank you for your comment. The SDT followed the NERC guidelines for VRFs and VSLs in setting the appropriate levels. The SDT will forward your suggestions to NERC for future consideration.		
Manitoba Hydro	No	This seems like an administrative only requirement. It would be too difficult to validate or measure.
Response: Thank you for your comment. Please see the response to your comment in question 1.		
Independent Electricity System Operator	No	We agree with the VRF for R2, but have a concern over the VRFs assigned to R1 (Lower) and R3 (Medium).Having an event reporting operating plan (R1) is a first step toward meeting the intent of this standard, annually validating it (R3) is a maintenance requirement which arguably can be regarded as equally important but its reliability risk impact for failure to comply should be no higher

Organization	Yes or No	Question 2 Comment
		than having no plan to begin with. We therefore suggest that the VRFs for R1 and R3 be at least the same, or that R1's VRF be higher than that for R3.
Response: Thank you for your comment. The SDT developed the VRFs based on existing, FERC Approved VRFs and NERC Guidelines for establishment of VRFs. EOP-004-2 is a result of merging CIP-001-2a and EOP-004-1. Each requirement in CIP-001-2a is assigned a "Medium" VRF. The requirements of CIP-001-2a map to EOP-004-2 Requirements R1 and R2. Having an Operating Plan (EOP-004-2, R1) merits a "Lower" VRF. The reporting of events contained in the Operating Plan required under Requirement R1 is mandated under Requirement R2 (which maps from CIP-001-2a, R2). The SDT cannot "lower the bar" on an existing VRF per NERC and FERC guidelines. Further, since R3 requires validation of the contact information in the Operating Plan, it is also assigned a "Medium" VRF.		
Southwest Power Pool RTO	No	We question the reliability benefits of this requirement.
Response: Thank you for your comment. Requirement R3 is in direct response to a FERC directive in Order 693 and as such, the SDT included this provision. If the information in the Operating Plan is out of date, then the plan will not be effective.		
Lewis County PUD	No	
American Electric Power	No	
Response: Thank you for your participation.		
ReliabilityFirst	Yes	Even though ReliabilityFirst votes in the Affirmative, we offer the following comments for consideration regarding the VSLs: VSL for Requirement R2 - ReliabilityFirst questions whether there is justification for the gradation of VSLs out to 60 hours for the reporting an event. Without justification, ReliabilityFirst believes the timeframe should be shortened to eight hour increments with a severe VSL being more than 48 hours late. ReliabilityFirst believes that being more than a day late (24 hours) falls within the entity completely not meeting the intent of submitting the report with the required 24 hour timeframe.
Response: Response: Thank you for your comment. The SDT followed the NERC guidelines for VRFs and VSLs in setting the		

Organization	Yes or No	Question 2 Comment
appropriate levels.		
PNGC Comment Group	Yes	
FirstEnergy	Yes	
Arizona Public Service Company	Yes	
Entergy Services, Inc. (Transmission)	Yes	
Clark Public Utilities	Yes	
Public Service Enterprise Group	Yes	
Idaho Power Co.	Yes	
Ingelside Cogeneration LP	Yes	
Wisconsin Electric Power company dba We Energies	Yes	
Ameren Services	Yes	
South Carolina Electric and Gas	Yes	
Georgia Transmission Corporation	Yes	
City of Austin dba Austin Energy	Yes	
Springfield Utility Board	Yes	
American Public Power Association	Yes	

3. Do you have any other comment, not expressed in the questions above, for the DSR SDT?

Summary Consideration: Most stakeholders who responded to this question provide comments suggesting specific revisions to the requirements or to the event types listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.

Organization	Question 3 Comment
Detroit Edison	"Suspicious activity" and "suspicious device" should be eliminated from Attachment 1, Event types: 'Physical threats to a Facility' and 'Physical threat to a BES Control Center'. By including 'suspicious activity' in the standard, I believe the project team went outside of the scope of the project, which was intended to be a merger of the two standards. Regarding standard CIP 001, the threshold for reporting is “Disturbances or unusual occurrences, suspected or determined to be caused by sabotage....”, as its title suggested: Sabotage Reporting. Suspicious activity, which is not defined by the standard, clearly has a much lower threshold than sabotage, or even suspected sabotage. The reporting requirement of 24 hours, also increases the burden on the entity to either rush to investigate and make a determination regarding suspicious activity in less than 24 hours, or not perform due diligence and report uninvestigated “suspicious” activity, which normally turns out to not be a "Physical Threat”. Suspicious activity should be duly investigated by the entity, local law enforcement, or the FBI as appropriate; and then reported if it has been determined to be a physical threat, or cannot be explained. Reporting within 24 hours will devalue the information inputted, as most cases of suspicious activity are innocuous, and the standard lacks a process of follow up, which would remove the those incidents from intelligence databases. Regarding suspicious devices, determination is usually immediate, (in less than 24 hours), and then the device would be classified as either "sabotage" or "no threat". The standard is not clear whether suspicious devices still have to be reported, even if they are immediately determined as not a "Physical Threat to a Facility or BES Control Center." Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-

Organization	Question 3 Comment
	01) - Reporting Concepts states: The changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). These standards deal exclusively with after-the-fact reporting." Attachment 1 in existing EOP-004-1 is much easier to follow (specifies time requirement to file). Also R2 states DOE OE-417 may be utilized to file reports, however Standard time requirement for update report is 48 hours, OE-417 has changed time requirement on updated filing to 72 hours. Difference can cause confusion and possible penalties. The real time operator must focus on maintaining system reliability. Putting unnecessary reporting obligations on RT puts more importance on the reporting structure than on maintaining reliability. Let 8/5 support personnel perform the reporting tasks and keep the 24/7 on shift operators focusing on the BES.
Response: Thank you for the comment. The SDT disagrees with your position on the inclusion of suspicious activities. Suspicious activities are events and notification of such events is a part of the existing and CIP-001 and EOP-004 standards. Reporting under EOP-004 is for notification purposes only. The standard does not require any analysis of events and does not require any follow up reports as you suggest.	
City of Austin dba Austin Energy	(1) City of Austin dba Austin Energy (AE) requests that the SDT clarify whether R3 requires that each Registered Entity subject to EOP-004-2 verify NERC's contact information each year. It appears this would be overly burdensome for NERC to respond to individual requests. (2) AE also asks that NERC's fax number be included in the contact information at the beginning of Attachment 1 and at the Event Reporting Form in Attachment 2. NERC included the fax number as a viable contact method in its recent NERC Alert notifying the industry of the changed information. (3) AE requests that the SDT increase the threshold for reporting loss of firm load to â‰¥ 300 MW for all entities to align the reporting threshold with the OE-417 threshold. Otherwise, smaller entities would have to report firm load losses between 200 and 299 MW to NERC but not to the DOE. This could be administratively confusing to those responsible for reporting. (4) Attachment 1 lists the threshold for reporting generation loss at â‰¥ 1,000MW for the ERCOT Interconnection. ERCOT planning is based on a single contingency of 1,375MW. For this reason, AE believes the minimum threshold for a

Organization	Question 3 Comment
	disturbance should be greater than the single contingency amount of >1,375MW for the ERCOT Interconnection.
Response: Thank you for your comment. The SDT does not feel it is necessary to specific how the validation occurs and has left this to the entity to determine how to do this. The SDT agrees with the inclusion of the fax number. The SDT will forward the other suggestions to NERC for future consideration. However, it should be noted that these suggestions have not been adopted due to consistency with other standards.	
ACES Power Marketing Standards Collaborators	(1) For the first "Damage or destruction of a Facility" event in Attachment 1, the threshold for reporting should be modified. The threshold for reporting would only include damage or destruction that necessitates the need for action to prevent an Emergency. It does not include if an Emergency actually occurs. Based on the definition of Emergency which states that it is an "abnormal system condition that requires... action to prevent or limit", we think the threshold should be changed to "Damage or destruction of a Facility... that results in a BES Emergency". Per the definition, the Emergency is what necessitates action which is what the threshold appeared to be focused on. (2) In the second "Damage or destruction of a Facility" event in Attachment 1, the threshold regarding "intentional human action" is ambiguous and suffers from the same difficulties as defining sabotage. What constitutes intentional? How do we know something was intentional without a law enforcement investigation? If a car runs into a transmission tower, was this an accident or intentional human action? It could be either. This appears to be the same issue that prevented the drafting team from defining sabotage.(3) Under the "Physical threats to a BES control center" event in Attachment 1, the event should very clearly define if this applies to backup control centers or not. (4) Under the "Complete loss of off-site power to a nuclear generating plant (grid supply)" event" in Attachment 1, the entity with reporting responsibility is not coordinated with NUC-001. NUC-001 used the term transmission entity to mean an entity that is responsible for providing NPIR services. They did not use only TOP because there are other entities that provide this service. Please coordinate the "Entity with Reporting Responsibility" with that standard. (5) We continue to believe that the draft standard has not satisfied the complete scope of the SAR regarding elimination of redundancy. The draft standard will continue to require redundant reporting by various entities. For instance, under the event "Loss of Firm Load" in Attachment

Organization	Question 3 Comment
	1, the DP, TOP, and BA all are required to report. The response to our last set of comments regarding this issue was that "the industry can benefit from having such differing perspectives when events occur". This response seems to confuse event analysis with event reporting. The purpose of the standard is to simply report that an event happened. In fact, the reporting form only requires the submitting entity to report the type of event. The description of what happened is optional. What additional perspectives could be gained from having multiple registered entities in the same electrical footprint report that an event happened. If the purpose is to analyze the event, this is covered in the events analysis process. Furthermore, once NERC becomes aware of the event they have the authority to request data and information from other registered entities. Please eliminate the duplicate reporting requirements. Other events that may require duplicate reporting include: Damage or destruction of a Facility, Physical threats to a Facility, BES Emergency resulting in automatic firm load shedding, Loss of firm load, System separation, Generation loss, and Complete loss of off-site power to a nuclear generating plant.(6) In the second "Damage or destruction of a Facility" event and "Physical Threats to a Facility" events, Distribution Provider should be removed. The Distribution Provider does not have any Facilities which is defined as "a set of electrical equipment that operates as a single Bulk Electric System Element". The DP's transformers interconnecting to the BES are not Facilities and the latest NERC BOT definition explicitly does not include them in Inclusion I1. If a DP did own Facilities, it would be registered as a TO or GO. Inclusion of the DP will compel the DP to provide evidence that it does not have Facilities which is an unnecessary compliance burden that does not support reliability. (7) The "BES Emergency resulting in automatic firm load shedding" should not apply to the DP. In the existing EOP-004 standard, Distribution Provider is not included and the load shed information still gets reported. (8) For the "Voltage deviation on a Facility" event in Attachment 1, we suggest changing "area" in the threshold for reporting to "Transmission Operator Area" as it is a defined term. (9) For the "System separation (islanding)" event, please remove BA. Because islanding and system separation, involve Transmission Facilities automatically being removed from service, this is largely a Transmission Operator issue. This position is further supported by the approval of system restoration standard (EOP-005-2) that gives the responsibility to restore the system to the TOP. (10) The response to our comments requesting that Measure 2 specifically identify that attestations are

Organization	Question 3 Comment
	acceptable forms of evidence to indicate that no events have occurred indicated that the measure cannot permit use of attestations. Other standards that have been recently approved by the board specifically permit the use of attestations. FAC-003-2 M1 and M2, TOP-001-2 M1-M11 and TOP-003-2 M5 all permit the use of attestations. We ask that the drafting team to reconsider including a specific reference that an attestation is acceptable to indicate no event has occurred given these new facts. (11) In requirement R1, we suggest changing "in accordance with EOP-004-2 Attachment 1" to "to report events identified in EOP-004-2 Attachment 1". It makes more sense since the attachment is a list of events that require reporting. The other language sounds like additional requirements will be established in Attachment 1.
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Southwest Power Pool Regional Entity	(1) SPP RE thinks the following Generation reporting threshold is unclear: "Total generation loss, within one minute, of â‰¥ 2,000 MW for entities in the Eastern or Western Interconnection". What has to happen within one minute? It reads as if you have to make a report within one minute. If the intent is that a report has to be made within 24 hours if the loss is for more than one minute it should read, "Total generation loss â‰¥ 2,000 MW for more than one minute for entities in the Eastern or Western Interconnection". What is the intent of the one minute requirement? (2) It appears per R1 that entities are no longer required to include Regional Entities in their reporting chains. SPP RE believes Regional Entities must be included in the reporting chain so they can fulfill their obligations under their delegation agreements. (3) SPP RE thinks this standard was changed substantially enough that it should have been opened for a new ballot pool.

Organization	Question 3 Comment
Response: Thank you for comment. 1) The intent of the "one minute" language is to avoid having to report when a generator has a slow run back rather than a sudden loss. Typically, a unit will trip instantly and the loss will be clear. Other times, the generation will slowly decline and the SDT does not intend for this to be reported. The reporting requirement is to submit a report for an applicable event within 24 hours. 2) Entities are required to report to the ERO only and may submit reports to others, including the RE. The SDT envisions the reports generated through EOP-004-2 act as an input to the Events Analysis Process which includes participation by the Regional Entity. 3) The SDT followed the standards development process which allows significant revision to the standards a long as it proceeds to a successive ballot. The NERC Standard Processes Manual clearly states that a ballot pool stays in place until balloting is completed on a standard. On occasion, the Standards Committee has determined that it is necessary to form a new ballot pool for a project because the ballot pool has been in place for several years and many of the original ballot pool members are no longer available to vote, but this is not the normal practice.	
Ameren Services	(1) This draft refers to a number of activities in the Operations Plan that each entity is to have on hand as the primary guide of actions to be taken when an event occurs. Although there is information related to the requirements that should be included in the Operations Plan, the drafting team has not defined a structure on the format, the minimum information to be included or the direct audience for the Operations Plan. In addition, there is no guidance on the disposition, distribution of the Operations Plan which is left to the entity to determine. We request that the drafting team provide a defined structure for entities concerning the development and implementation of the Operations Plan. (2) Page 14 (Attachment 2) - Voltage Deviation of a Facility - This appears to be a contradiction to VAR-001-2 R10 for TOP which states IROL events will be corrected within 30 minutes. We request the 15 minute reporting criteria be changed to also state 30 minutes. (3) Throughout Document - "Report to the ERO and Regional Entity" - NERC and DHS established the ES-ISAC as a confidential location to report all events that happen on the BES. As these events are of a Sabotage / Disturbance nature, they should all go through the ES-ISAC both as a single location for distribution, and as a best practice that the industry has started. (4) There seems to be some differences between the red-line and clean versions which may need some clarification. For example, (a) In the redline version, the revision history box appears to indicate the inclusion of parts of CIP-008, and in the "Clean" version this has been

Organization	Question 3 Comment
	removed from the revision history box. (b) The red-line version includes a drawing at two places versus once in the clean version. (c) The correlation between the clean and redline documents is not very clear and there appears to be gaps in the reporting and tracking framework structure.
Response: Thank you for comment. 1)-3) Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot. 4) In removing tables and diagrams, the redline version tends to show both the old and new with only a red line down the side of the page. The clean version of the standard is the final version.	
Texas Reliability Entity	(A) Regional Entity should be capitalized in R1. (B) COMMENTS ON ATTACHMENT 1:In the previous comment period on this Standard, Texas RE submitted comments that we feel were not adequately addressed. There were several responses to comments regarding the Events Table that need deeper review and consideration:(1) In the Events Table, under Transmission Loss, the SDT indicated that reporting is triggered only if three or more Transmission Facilities operated by a single TOP are lost. Also, generators that are lost as a result of transmission loss events must be included when counting Facilities. As Texas RE indicated in previous comments to this Standard, determining event reporting requirements by the entity that owns/operates the facility is not an appropriate measure. If the industry wants to learn from events, these types of issues must be addressed. Including the RC as one of the Entity(s) with Reporting Responsibility may alleviate this concern. The RC would have overall view of the system and could provide the reports on multi-element events where the elements are owned/operated by different entities. For the SDT to believe that “There may be times where an entity may wish to report when a threshold has not been reached because of their experience with their system” is worthy to note but falls short of the reliability implications caused by those entities that will not report. The industry needs to learn from events and failure to report will facilitate failure to learn. (2) In the Events Table, under Transmission Loss, there has been considerable discussion

Organization	Question 3 Comment
	recently within the Events Analysis Subcommittee (EAS) regarding the definition of the phrase "contrary to design." The EAS is currently working on possible guidelines to interpret this event type. The SDT may want to consider including the EAS language into the Guidelines and Technical Basis for this Standard. (3) In the Events Table, under "Unplanned BES Control Center evacuation" and "Complete loss of voice communication capability," and "Complete loss of monitoring capability," GOPs should be included. GOPs also operate control centers that would be subject to these kinds of occurrences. As Texas RE indicated in previous comments to this Standard, in CIP-002-5 Attachment 1 there is a "High Impact Rating" for the following: "1.4 Each Control Center, backup Control Center, and associated data centers used to perform the functional obligations of the Generation Operator that includes control 1) for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection or 2) that includes control of one or more of the generation assets that meet criteria 2.3, 2.6, and 2.9." In the ERCOT Region, we experienced an event where a GOP control center lost an ICCP link that carried real-time information regarding its generation fleet (over 10,000 MWs). Without inclusion of the GOP here the event may not get recorded. While it was a "virtual" loss, the impact to the BES through generation control actions could be significant and the event should be reported and analyzed. For the GOP control centers that do exist, the reporting of such events should be a requirement. Based on the minimum of these two examples, why would the SDT NOT include GOP as being applicable? (4) In the Events Table, under "BES Emergency requiring public appeal for load reduction," the definition of Emergency is "Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities...." Is it the intent of the SDT to exclude public appeals issued in anticipation of a possible emergency, before a BES Emergency is officially declared? (5) In the Events Table, under "BES Emergency resulting in automatic firm load shedding," the SDT may want to consider including the RC as one of the Entity(s) with Reporting Responsibility. The RC would have overall view of the system and should provide the reports on events where the multiple entities may be involved. We have UVLS schemes in our region

Organization	Question 3 Comment
	where the total MW shed is greater than 100 MW, but the individual TOP MW shed is less than 100 MW. (6) In the Events Table, consider whether the item for "Voltage deviation on Facility" should also be applicable to GOPs, because a loss of voltage control at a generator (e.g. failure of an automatic voltage regulator or power system stabilizer) could have a similar impact on the BES as other reportable items. Note: We made this comment last time, and the SDT's posted response was non-responsive to this concern. The SDT noted "Further, we note that such events do not rise to the level of notification to the ERO" but the SDT failed to recognize that "Voltage deviation on a Facility" does exactly that - notifies the ERO but from a TOP perspective only. Texas RE is trying to establish the correct Responsible Entity for reporting "Voltage deviation on a Facility" (in this case a generator regardless of the cause and other obligations the owner may have with other Reliability Standards).
Response: Thank you for comment. A) The SDT agrees and has made the correction. B) Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Central Lincoln	1) Central Lincoln must again point out the lack of proportionality for gunshot insulators and similar events under "Damage or destruction of a Facility." Please see our last set of comments. These incidents are fairly common in the west, and typically do not cause an immediate outage. They are generally discovered months after the fact, yet the discovery starts the 24 hour clock running as if the situation had suddenly changed. Prior SDT response: "... this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was "damaged or destroyed" intentionally by a human." There is already a great lag in awareness regarding the damaged insulator. Months or more can pass prior to discovery by the entity. We fail to see how it becomes so urgent upon discovery. Prior SDT response: "The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan."We do not share the SDT's

Organization	Question 3 Comment
	vision. If an Operating Plan redefined suspected intentional human action so the act of preparing a gun for firing, aligning the sights on an insulator and pulling the trigger was not included, we believe the entity that operates under that plan would be found non-compliant under the language of this standard. We do not offer a simple change in text that will fix the problem, we are only pointing out the problem exists. Murphy dictates discovery will occur at the most inopportune time, which will be during an after hours outage on a stormy holiday weekend night when many employees are out of town and those that are available are already fully engaged. The entity is then faced with choosing to delay restoration or violating the standard. When proposing a zero defect event driven requirement event driven such as this one, we ask the SDT to consider all possible scenarios in which the event may occur. 2) We note that Distribution Providers are listed in the Applicability Section. We also note that there is no requirement in the Statement of Compliance Registry Criteria for Distribution Providers to own or operate BES Facilities, own or operate UFLS or UVLS of 100 MW, or to have load exceeding 200 MW. DP's that cannot meet any of the thresholds of Attachment 1 would still need an Operating Plan under R1 and annually validate the possibly null contact list in its OP under R3. We suggest that DPs that cannot meet the thresholds of Attachment 1 be removed from the Applicability Section.

Response: Thank you for comment. 1) Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.

2) To your suggestion on DPs, the SDT has clarified, in the Guidelines and Technical Basis Section of the standard, that DPs who do not meet the threshold reporting requirements can conduct an annual review of the threshold requirements and be exempted from R1 and R3 for that period. Once the DP has met the threshold reporting requirements, they will then have to comply with the standard.

"Distribution Provider Applicability Discussion

The DSR SDT has included Distribution Providers (DP) as an applicable entity under this standard. The team realizes that not

Organization	Question 3 Comment
	all DPs will own BES Facilities and will not meet the "Threshold for Reporting" for any event listed in Attachment 1. These DPs will not have any reports to submit under Requirement R2. However, these DPs will be responsible for meeting Requirements R1 and R3. The DSR SDT does not intend for these entities to have a detailed Operating Plan to address events that are not applicable to them. In this instance, the DSR SDT intends for the DP to have a very simple Operating Plan that includes a statement that there are no applicable events in Attachment 1 (to meet R1) and that the DP will review the list of events in Attachment 1 each year (to meet R3). The team does not think this will be a burden on any entity as the development and annual validation of the Operating Plan should not take more that 30 minutes on an annual basis. If a DP discovers applicable events during the annual review, it is expected that the DP will develop a more detailed Operating Plan to comply with the requirements of the standard."
Duke Energy	1) There are discrepancies between the red-lined EOP-004-2 and the Clean EOP-004-2 that were posted for this project. Our comments are based upon the Clean EOP-004-2. 2) Attachment 1 and Attachment 2 have the ERO email and phone number listed. If these ever change, does the standard have to go through the revision and balloting process again, or is there an easier way to incorporate such changes? 3) Attachment 1 - When an event occurs that meets the Threshold for Reporting, it's not clear whether all listed entities have to report or not. Several Event Types need this clarity added. For example, if a TOP loses voice communication capability, do both the TOP and RC have to report? 4) Attachment 1 - Damage or destruction of a Facility, applicable to BA, TO, TOP, GO, GOP, DP. The Threshold for Reporting should be further clarified by adding the sentence "Do not report theft or damage unless it degrades normal operation of a Facility." This would eliminate unnecessary reporting of copper theft or vandalism. 5) Attachment 1 - Physical threats to a Facility. The Threshold for Reporting should be modified by deleting the sentence "Do not report theft unless it degrades normal operation of a Facility". This sentence isn't needed here, and fits better with "Damage or destruction of a Facility" as noted in 4) above. 6) Attachment 1 - Transmission loss. This event type should be deleted because it is duplicated

Organization	Question 3 Comment
	under TADS reporting and PRC-004 Protection System Misoperations reporting. 7) Attachment 1 - Unplanned BES control center evacuation, Complete loss of voice communication capability, and Complete loss of monitoring capability. The Threshold for Reporting on all three of these Event Types is 30 minutes, and should be extended to 2 hours, consistent with the transition time identified in EOP-008 "Loss of Control Center Functionality".
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
ERCOT	As a general matter, this standard imposes an ex-post reporting obligation. Consistent with the ongoing P 81 standard review/elimination effort, this standard is arguably a candidate for elimination under the principles guiding that effort. The obligation proposed in the standards are better suited for inclusion in the Rules of Procedure or as a guideline because they are strictly administrative in nature. **Response: On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 ("P81") invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-**

Organization	Question 3 Comment
	004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program. As the SDT is moving forward with a Recirculation Ballot, your suggestions will be forwarded to NERC for future consideration. To the extent the SDT continues to pursue this effort, ERCOT offers the following additional comments. ERCOT has commented on the listing in the Entity with Reporting Responsibility column of Attachment 1. Consistent with those prior comments, the current version still fails to adequately create a bright line threshold for particular events. For example, in the Transmission loss event, although the TOP is listed, there is no direction regarding which TOP is required to file the event report. Is it the TOP in whose TOP area the loss occurred or is it a neighboring TOP who observes the loss? Clearly, the responsibility for reporting lies with the host system, but that responsibility is not clearly designated. There are several other similar events where there is no bright line. We suggest that the drafting team return the deleted language to the Entity with Reporting Responsibility column in those instances where the current version fails to provide a bright line in the Threshold column. Regarding multiple reports for a single event, that aspect of the proposed draft should be revised to only require a single report. While additional information may be available from others, let the Event Analysis team perform their function. This would eliminate the redundant reporting that is currently required as the standard is written. **Response: Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.** ERCOT requests that the reference to “cyber attack” be removed from the Guideline and Technical Basis section of the document since all reporting of cyber events has been removed from the standard and retained in CIP-008. **Response: This correction has been made.**

Organization	Question 3 Comment
Response: Thank you for comment. Please see responses above.	
American Public Power Association	As stated in our comments on the previous draft: It is APPA's opinion that this standard should be removed from the mandatory and enforceable NERC Reliability Standards and turned over to a working group within the NERC technical committees. Timely reporting of this outage data is already mandatory under Section 13(b) of the Federal Energy Administration Act of 1974. There are already civil and criminal penalties for violation of that Act. This standard is a duplicative mandatory reporting requirement with multiple monetary penalties for US registered entities. If this standard is approved, NERC must address this duplication in their filing with FERC. This duplicative reporting and the differences in requirements between DOE-OE-417 and NERC EOP-004-2 require an analysis by FERC of the small entity impact as required by the Regulatory Flexibility of Act of 1980
Response: Thank you for the comment. The SDT does not believe that there is duplicative reporting. The reports that you mention do not go to NERC under the FPA. We will forward your suggestion to NERC for consideration in the preparation of the filing for approval.	
NV Energy	Aside from the comment referring to the new R3 and the term "validate", I applaud the SDT for the improvements made in the remainder of the Standard. This is a much simpler and straightforward approach to meeting the directives in this project and greatly simplifies the processes necessary on the part of the registered entities.
Response: Thank you for your comment.	
CenterPoint Energy	CenterPoint Energy appreciates the revisions made to the draft Standard based on stakeholder feedback and believes that the changes made are positive overall. However, the Company recommends the additional changes noted below for a favorable vote. In the Rationale for R1, CenterPoint Energy recommends that the 2nd sentence in the 1st paragraph be revised as follows, "In addition, these event reports may serve as input to the NERC Events Analysis Program.", as not all events listed in Attachment 1 will serve as input in to the NERC Events Analysis Program. CenterPoint Energy also proposes that the Standard Drafting Team (SDT)

Organization	Question 3 Comment
	add "There cannot be a violation of Requirement R2 without an event." as noted in the Consideration of Issues and Directives to the Requirement. For Attachment 1, CenterPoint Energy recommends the following revisions: CenterPoint Energy continues to be concerned that the uses of the terms “suspicious” and “suspected” are too broad. The Company proposes that the SDT remove the terms from the Thresholds for Reporting or add “which caused a negative impact to the Bulk Electric System” or “that causes an Adverse Reliability Impact..." to each phrase where the terms are used. CenterPoint Energy proposes that the threshold for reporting the event, “BES Emergency requiring manual firm load shedding” is too low. It appears the SDT was attempting to align this threshold with the DOE reporting requirement. However, as the SDT has stated, there are several valid reasons why this should not be done. Therefore, CenterPoint Energy recommends the threshold be revised to “Manual firm load shedding â‰¥ 300 MW”. CenterPoint Energy also recommends a similar revision to the threshold for reporting associated with the “BES Emergency resulting in automatic firm load shedding” event. (“Firm load shedding â‰¥ 300 MW (via automatic under voltage or under frequency load shedding schemes, or SPS/RAS”) For the event of “System separation (islanding)”, CenterPoint Energy believes that 100 MW is inconsequential and proposes 300 MW instead. For “Generation loss”, CenterPoint Energy suggests that the SDT add "only if multiple units” to the criteria of “1,000 MW for entities in the ERCOT or Quebec Interconnection”.
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
PNGC Comment Group	Comments: The PNGC Comment group remains concerned that the “Applicability” section will inadvertently subject Distribution Providers to requirements that they should be excluded from. Please consider the two examples below and note that we’re talking about probably hundreds of small DPs being subject to these unnecessary requirements without any increase to the reliability of the BES. Example 1: Small DP with a peak load of 50 MWs. They have no

Organization	Question 3 Comment
	BES Facilities and their system is radial. Even though this utility will never have a reporting requirement per Attachment A, they are still subject to R1 and R3 plus the associated compliance (read financial) risk for non-conformance. An easy fix to this issue would be for DPs without BES Facilities and with less than 200 MW annual peak load to be excluded in the Applicability section. Example 2: Small DP with a peak load of 50 MWs. Their only BES Facilities are two Automatic UFLS relays that are capable of shedding 15 MWs. DP's Host Balance Authority (HBA) has a peak load of 10,000 MWs, meaning their UFLS plan requires them to have the capacity to shed 3000 MWs should system conditions warrant. Is it the SDT's intent for this DP to have an Operating Plan in place for "damage", "destruction", or "physical threat" for these two relays that are capable of shedding only 15 MWs out of a 3000 MW HBA UFLS plan? The SDT set a 100 MW threshold for reporting of automatic UFLS load shedding so why have reporting requirements for the threat to 15 MWs worth of UFLS relays? Once again the easy fix is to modify the Applicability section. We suggest: 4.1.7. Distribution Provider: with >= 200 MW annual peak load, or;>= 100 MW Automatic firm load shedding

Response: Thank you for comment. To your suggestion on DPs, the SDT has clarified, in the Guidelines and Technical Basis of the Standard, that DPs who do not meet the threshold reporting requirements can conduct an annual review of the threshold requirements and be exempted from R1 and R3 for that period. Once the DP has met the threshold reporting requirements, they will then have to comply with the standard.

"Distribution Provider Applicability Discussion

The DSR SDT has included Distribution Providers (DP) as an applicable entity under this standard. The team realizes that not all DPs will own BES Facilities and will not meet the "Threshold for Reporting" for any event listed in Attachment 1. These DPs will not have any reports to submit under Requirement R2. However, these DPs will be responsible for meeting Requirements R1 and R3. The DSR SDT does not intend for these entities to have a detailed Operating Plan to address events that are not applicable to them. In this instance, the DSR SDT intends for the DP to have a very simple Operating Plan that includes a statement that there are no applicable events in Attachment 1 (to meet R1) and that the DP will review the list of events in Attachment 1 each year (to meet R3). The team does not think this will be a burden on any entity as the development and annual validation of the Operating Plan should not take more that 30 minutes on an annual basis. If a DP discovers applicable events during the annual review, it is expected that the DP will develop a more detailed Operating Plan

Organization	Question 3 Comment
to comply with the requirements of the standard."	
Cowlitz PUD	Cowlitz approves of the improvement efforts on Attachment 1. However, Cowlitz must again point out the fallacy of potentially inundating the ERO with nuisance reporting of minor vandalism and accidental damage. For example, gunshot "target practice" of insulators and structures will apply under "Damage or destruction of a Facility." Such incidents are fairly common in the west, and typically do not cause an immediate outage. They are generally discovered months or years after the fact, yet the discovery starts the 24 hour compliance clock running as if the urgency is just as important as a recent event. If there is already a great lag in awareness regarding the damaged Facility, Cowlitz fails to see how it becomes so urgent upon discovery.----------Again, Cowlitz points out the sentence structure "Damage or destruction of its Facility that results from actual or suspected intentional human action" does not restrict the human action as malicious or sabotage. "Intentional human action" could be innocent, such as a land owner attempting to fall a tree for fire wood. The intent was not to damage the Facility, but the "intentional human action" to obtain fire wood resulted in the damage of the Facility. This does not comport with prior SDT response: "... this will give the ERO (and whoever else the entity wishes to inform per Requirement R1) the situational awareness that the Facility was 'damaged or destroyed' intentionally by a human." Therefore, if this is the SDT's intent Cowlitz suggests this change: Damage or destruction of its Facility that causes immediate impaired operation or loss of the Facility from suspected or actual malicious human intent. Do not report mischievous vandalism, as defined in the Operating Plan, where immediate loss of, or immediate impaired operation of the Facility has not occurred. ----------Prior SDT response: "The SDT envisions that entities could further define what a suspected intentional human action is within their Operating Plan." Cowlitz does not share the SDT's vision. The Standard as written does not specifically address the ability to "further define" terms used in the Attachment. Past allowance of audit teams to allow registered entity definitions, e.g. "annual," was to address gaps in standards until the standards could be revised. If this is truly the intent of the SDT, then requirement R1 would need revision such as: "The Operating plan shall define what a suspected intentional human action is." Cowlitz respectfully requests that ambiguity be avoided.---------- Cowlitz notes that Distribution Providers are listed in the Applicability Section with no qualifiers. Cowlitz

Organization	Question 3 Comment
	points out that there is no requirement in the Statement of Compliance Registry Criteria for Distribution Providers to own or operate BES Facilities, own or operate UFLS or UVLS of 100 MW, or to have load exceeding 200 MW. DP's that cannot meet any of the thresholds of Attachment 1 would still need an Operating Plan under R1 and annually validate the possibly null contact list in its OP under R3. Cowlitz requests that DPs that cannot meet the thresholds of Attachment 1 be removed from the Applicability Section. Not doing so will increase compliance risk without any reliability return.
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot. **To your suggestion on DPs, the SDT has clarified, in the Guidelines and Technical Basis Section of the Standard, that DPs who do not meet the threshold reporting requirements can conduct an annual review of the threshold requirements and be exempted from R1 and R3 for that period. Once the DP has met the threshold reporting requirements, they will then have to comply with the standard.** **"Distribution Provider Applicability Discussion** **The DSR SDT has included Distribution Providers (DP) as an applicable entity under this standard. The team realizes that not all DPs will own BES Facilities and will not meet the "Threshold for Reporting" for any event listed in Attachment 1. These DPs will not have any reports to submit under Requirement R2. However, these DPs will be responsible for meeting Requirements R1 and R3. The DSR SDT does not intend for these entities to have a detailed Operating Plan to address events that are not applicable to them. In this instance, the DSR SDT intends for the DP to have a very simple Operating Plan that includes a statement that there are no applicable events in Attachment 1 (to meet R1) and that the DP will review the list of events in Attachment 1 each year (to meet R3). The team does not think this will be a burden on any entity as the development and annual validation of the Operating Plan should not take more that 30 minutes on an annual basis. If a DP discovers applicable events during the annual review, it is expected that the DP will develop a more detailed Operating Plan to comply with the requirements of the standard."**	
Wisconsin Electric Power company	Damage or destruction of a Facility, Damage or destruction of its Facility that results from

Organization	Question 3 Comment
dba We Energies	actual or suspected intentional human action.: By the Functional Model, I do not believe the BA function has Facilities by the NERC Glossary definition. This would not apply to a BA. The line above this would adequately cover BA reporting. Remove a BA from applicability for this line. Physical threats to a Facility: The BA function does not have Facilities. Remove a BA from applicability for this line. There could be a separate line for Physical Threats to a Facility within an RC, FOP, BA Area as there is for Damage or Destruction of a Facility. Voltage deviation on a Facility: Please specify what voltage this is, nominal, rated, etc. This should also be > 10% deviation. Exactly at 10% could be at the edge of an allowed range.
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Manitoba Hydro	Does the Background, Guidelines and Technical Basis form part of the standard itself once published? Or are these just parts of the package that accompany the standard during circulation for comment? **The background, guidance and technical basis will remain with the standard and provides clarification on the SDT's intent and direction** Compliance 1.2: The reference to Responsible Entity is bracketed and in lowercase. We are not clear why. **This was corrected in the clean version.** VSLs, R1, Severe VSL: The words "in the event reporting Operating Plan" are missing from the end of this sentence. **This was corrected in the clean version.**

Organization	Question 3 Comment
	VSLS, R2, Lower VSL: The violation occurs if the Responsible Entity has submitted an event report to one entity whereas Moderate VSL, High VSL and Severe VSL, the level of severity of the VSL increases depending on the number of entities that the Responsible Entity fails to submit an event report to. The drafting here is not as precise as it should be. The way the Lower VSL is written, it will also be triggered when the Responsible Entity has complied with the requirement. For example, if the Responsible Entity is required to report an event to 5 entities, and it does, it will still mean that it has "submitted an event report to one entity identified in the event reporting (also, the 'ing' is missing on the Lower VSL reference)Operating Plan". It is also duplicative. For example, if the Responsible Entity submitted a report to only one entity, and failed to submit a report to 4 others, they fall under the Lower VSL and the Higher VSL (we are assuming in this case, the violation will be found to be the higher VSL). Perhaps what the drafting team intended to do was to make the Lower VSL, which the Responsible Entity failed to submit an event report...to one entity identified.... **The SDT followed the NERC guidelines for VSLs in setting the appropriate levels. The VSLs were written based on two potential failures to meet the requirement. The first is based on the time the report was submitted while the second was based on the entity submitting the report within 24 hours but not to all applicable entities. If a violation is determined, it will be for either being late with the report or for not submitting the report to everyone. The appropriate VSL will be applied ONLY if a violation is found.** The Guidelines and Technical Basis contain a reference to R4 which no longer exists in the standard. **This reference has been removed.**
Response: Thank you for comment. Please see responses above.	
Dominion	Dominion reads Requirement R1 as explicitly requiring only the inclusion of reporting to the ERO in the Operating Plan. We acknowledge that the requirement also contains additional entities in parenthesis which infers the inclusion of a larger group (and which appears to be supported by the rationale box). Dominion suggests the SDT explicitly state which entities, at a minimum, be included, for reporting, in the Operating Plan. We suggest adding a column to

Organization	Question 3 Comment
	Attachment 1 and including entities to which the event must be reported. As an examples; o All event types should include local law enforcement o Events for which the BA, RC, TOP bear responsibility should probably also be reported to the regional entity o Events for which the Facility Owner bears responsibility should probably also be reported to the respective BA and TOP, who would in turn determine whether to notify their respective RC. The RC would in turn determine if additional entities need to be contacted. Requirement R2 establishes a 24 hour reporting threshold; however, the "NOTE" provided on Attachment 1 seems to contradict Requirement 2 and could therefore lead to compliance issues. Dominion suggests that Requirement R2 be revised to agree with the "NOTE" on Attachment 1. For example, Requirement R2 could be reworded as: Except as noted on Attachment 1, Each Responsible Entity shall...Also under the "NOTE" in Attachment 1, why has the facsimile number for the ERO been removed? The DOE still provides a facsimile number for reporting. Attachment 2: Event Reporting Form #4; need to update the below to reflect the same naming convention of the events in Attachment 1, the "t" should not be capitalized in Physical Threat and add an 's' behind threat. Add (islanding) behind System separation and capitalize the 'U' in unplanned control center evacuation.
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Southern Company	**NOTE: The SDT received assistance from Southern Company personnel in parsing these comments as show below. As submitted, the formatting of the original comments was lost and very difficult for the SDT to read and understand.** Event Type Entity with Reporting Responsibility Threshold for Reporting SOCO Comment: **Damage or destruction of a Facility** RC, BA, TOP Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area, excluding weather or natural disaster related threats, that results in actions to avoid a BES

Organization	Question 3 Comment
	Emergency. – No Comment **Damage or destruction of a Facility** BA, TO, TOP, GO, GOP, DP Damage or destruction of its Facility that results from actual or suspected intentional human action.: Do not report damage unless it degrades normal operation of a Facility. How does the SDT define "intentional human action?" Further, how is the phrase "suspected intentional human action" defined? This phrase is very broad. Is "intentional human action" identified as actions intended to damage facilities or does it include accidental actions by individuals? For example, if a person accidentally shot insulators off of a 230 kV line resulting in damage, would that be considered reportable "intentional human action?" In addition, what is that actual trigger for reporting? Does it require that the action has been discovered or is it from the time the event occurs? Further, 24 hours is a very brief time period -- how is an entity to conduct an investigation within that time period to determine if damage or destruction could have resulted from "actual or suspected" human action and also determine if it could have been "intentional"? In Southern's cases, and likely in other entities case, operating personnel submit the reports to the regulatory entities for events that fall under this standard. Southern is concerned, that the threshold for reporting for "Damage or destruction of a Facility" and "Physical threats to a Facility" is so broad that numerous reports would need to be filed that 1) may be a result of something that does not pose harm to reliability and should not be of interest to the regulators, and 2) would introduce additional burden to operating personnel that are monitoring the system every moment of the day. With the current proposed "Threshold for Reporting", the reporting requirement would hamper the ability of system operating personnel to perform their core real-time system operator tasks which would harm reliability. **Physical threats to a Facility** BA, TO, TOP, GO, GOP, DP Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. OR Suspicious device or activity at a Facility. Do not report theft

Organization	Question 3 Comment
	unless it degrades normal operation of a Facility. Please provide some clarity as to what is considered suspicious activity. For example, would someone taking a photo of a BES substation fall into this category? Please provide examples of what may be considered suspicious activity and how NERC and others may use this information and what actions they would take as a result of receiving this information. In addition, what is that actual trigger for reporting? Is it when the threat is discovered or from when it should have or could have been discovered? Further, 24 hours is a very brief time period -- how is an entity to conduct an investigation within that time period in order to determine if the physical threat has the potential to degrade the normal operation of the Facility or that the "suspicious activity"? **Physical threats to a BES control center** RC, BA, TOP Physical threat to its BES control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. OR Suspicious device or activity at a BES control center. – No Comment **BES Emergency requiring public appeal for load reduction** Initiating entity is responsible for reporting. Public appeal for load reduction event. It is unclear which entity would be responsible for reporting this event. For example, if the RC/TOP/BA were to identify the need to do this and instruct an LSE to issue the public appeal, who would report the event? **BES Emergency requiring system-wide voltage reduction** Initiating entity is responsible for reporting System wide voltage reduction of 3% or more. It is unclear which entity would be responsible for reporting this event. For example, if the RC were to identify the need to do this and instruct a TOP to reduce voltage, who would report the event? **BES Emergency requiring manual firm load shedding** Initiating entity is responsible for reporting Manual firm load shedding â‰¥ 100 MW. – No Comment

Organization	Question 3 Comment
	BES Emergency resulting in automatic firm load shedding DP, TOP Automatic firm load shedding â‰¥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS). – No Comment **Voltage deviation on a Facility** TOP Observed within its area a voltage deviation of ± 10% of nominal voltage sustained for >or= 15 continuous minutes. Please change “nominal” to “expected” or “scheduled” **IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only)** RC Operate outside the IROL for time greater than IROL Tv (all Interconnections) or Operate outside the SOL for more than 30 minutes for Major WECC Transfer Paths (WECC only). – No Comment **Loss of firm load** BA, TOP, DP Loss of firm load due to equipment failures/system operational actions for >or= 15 Minutes: >or= 300 MW for entities with previous year’s demand >or= 3,000 MW OR >or= 200 MW for all other entities This should not be as a result of weather or natural disasters. **System separation(islanding)** RC, BA, TOP Each separation resulting in an island â‰¥ 100 MW – No Comment **Generation loss** BA, GOP Total generation loss, within one minute, of â‰¥ 2,000 MW for entities in the Eastern or Western Interconnection OR â‰¥ 1,000 MW for entities in the ERCOT or Quebec Interconnection – No Comment **Complete loss of off-site power to a nuclear generating plant (grid supply)** TO, TOP Complete loss of off-site power affecting a nuclear generating station per the Nuclear Plant Interface Requirement – No Comment **Transmission loss** TOP Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing). – No Comment **Unplanned BES control center evacuation** RC, BA, TOP Unplanned evacuation from BES control center facility for 30 continuous minutes or more. – No Comment

Organization	Question 3 Comment
	Complete loss of voice communication capability RC, BA, TOP Complete loss of voice communication capability affecting a BES control center for 30 continuous minutes or more. – No Comment **Complete loss of monitoring capability** RC, BA, TOP Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (i.e., State Estimator or Contingency Analysis) is rendered inoperable. – No Comment **Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.**Guideline and Technical Basis Comments In the Summary of Key Concepts section of the Guideline and Technical Basis, the DSR SDT explains that the proposed Standard does not include any real-time operating notifications for events listed in Attachment 1. The DSR SDT should consider language in the Standard which codifies this approach. Southern Company notes that the proposed standard does not mention any exclusion of real-time notification. **Response: The SDT does not believe that this revision is necessary as the requirement R2 clearly states that events are to be reported within 24 hours.** The Law Enforcement Reporting section of the Guideline and Technical Basis unintentionally expands on the purpose of the Standard by stating that "The Standard is intended to reduce the risk of Cascading events." The stated purpose of the Standard is "To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities." The phrase in the Guideline should be removed or modified in order to avoid any uncertainty about the Standard's purpose. **Response: The SDT has made the requested clarification to the Guidelines and Technical Basis section.**

Organization	Question 3 Comment
	The DSR SDT should consider integrating the content of the Concept Paper into the Guideline and Technical Basis. Presently, the Concept Paper appears as an add-on at the end of the document. When the Concept Paper existed as a stand-alone document, various segments such as "Introduction" and "Summary of Concepts and Assumptions" were helpful to stakeholders and standards developers. The revised merged document in the present draft does not need two separate sections addressing concepts nor does it need an introduction at the midway point. Additionally, two other areas are either duplicative or contribute to ambiguity within the supplemental information. First, it is not clear that the segment on Concepts and Assumptions includes any actual assumptions. The section should be modified or deleted to address this concern. Second, the segment entitled 'What about sabotage?' seems to contain topics similar to those on the first page of the Guideline. Again, the DSR SDT should consider integrating all of the necessary information into a more comprehensive document. **Response: The SDT has chosen to leave these sections in tact because it helps convey the development process as well as the information about the team's insights.**
Response: Thank you for comment. Please see responses above.	
FirstEnergy	FirstEnergy Corp (FE) appreciates the work done by the SDT by incorporating the comments and revisions from the previous draft. FE would like to see the time parameters in Requirement 3 and Measure 3 to be changed from "each calendar year" to "at least once every 12 months". This is similar to the wording that is being used in the CIP standards
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Oncor Electric Delivery	For reporting consistency, under the Event Type labeled "Generation Loss", in Appendix 1 of EOP-004-2, Oncor recommends that the reporting threshold of 1,000 KW for the ERCOT Interconnection be raised to 1,400 MW to match the 1,000 MW level in the current version of

Organization	Question 3 Comment
	the ERO Event Analysis Program. Under the Event Type labeled "Damage or Destruction of a "Facility", Appendix 1, with the threshold that states," Damage or destruction of its Facility that results from actual or suspected intentional human action", Oncor suggest the addition of the following language to address intentional human action that is theft in nature but is not intended to disrupt the normal operation of the BES: "Do not report theft unless it degrades the normal operation of a Facility."
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Georgia Transmission Corporation	GTC recommends a minor change to Attachment 2 associated with the complete loss of off-site power to nuclear generating plant. NUC-001-2 R9.3.5 describes provisions for restoration of off-site power and applies to both the Nuclear Plant Generator Operator and the applicable Transmission Entities. To maintain consistency, GTC recommends modification to this row in EOP-004-2 Attachment 2 such that the "Nuclear Plant Generator Operator" is the Responsible Entity with reporting responsibility. (A TO may not have visibility to all off-site power resources for a nuclear generating plant if multiple TO's are providing off-site power.)At a minimum, GTC recommends if the SDT believes the TO and TOP should remain involved, these entities should be limited to "TO and TOP that are responsible for providing services related to Nuclear Plant Interface Requirements (NPIRs)" which is also consistent with NUC-001-2.
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	

Organization	Question 3 Comment
South Carolina Electric and Gas	Has the drafting team considered how reports from R2 tie in with reports required by the NERC Event Analysis process? It appears that reporting deadlines conflict between the two. The SDT should clarify that the event types "Damage or Destruction" listed in attachment 1 do not pertain to "cyber events", to avoid duplication of the CIP-008 requirements.
Response: Thank you for comment. Reporting under this standard is for the notification of events to the NERC Situation Awareness Group. Reports in this standard can be the initial reports for the EA group, but are not designed to address the balance of the EA program. The SDT had removed the cyber security obligations in this draft.	
Xcel Energy	In attachment one, the "Threshold for Reporting" under Damage or Destruction of a Facility appears to closely follow the definition of sabotage that EOP-004-2 says it is trying to do away with. This definition should be drafted to better correlate with the other physical threats and include the language, "which has the potential to degrade the normal operation of the Facility". Additionally in Attachment 1, both the Physical threats to a Facility and Physical threats to a BES control center include the wording, "Suspicious device or activity...". What constitutes suspicious activity? With no definition this interpretation is left to the Entity which is again something the DSR SDT says they would like to eliminate. Lastly, in the Guideline and Technical Basis section, under A Reporting Process Solution - EOP-004 it states, "A proposal discussed with the FBI, FERC Staff, NERC Standards Project Coordinator and the SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Reportable Events). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial or local level law enforcement agency. The state or provincial or local level law enforcement agency will coordinate with law enforcement with jurisdiction to investigate. If the state or provincial or local level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial or local level law enforcement agency will notify and coordinate with the FBI or the RCMP." This appears to be in direct conflict with the Rationale for R1 which states, "An existing procedure that meets the requirements of CIP-001-2a may be included in this Operating Plan along with other processes, procedures or plans to meet this requirement."

Organization	Question 3 Comment
	CIP-001-2a required "communication contacts, as applicable, with local Federal Bureau of Investigation (FBI)..." so if the CIP-001-2a procedure is included this does not seem to meet the requirements of the operating plan required under EOP-004-2. Also, if the intent of the Operating Plan is to include all local law enforcement and not FBI the operating plan would become very detailed and when validated annually as required in R3, this becomes very burdensome on an entity.
Response: Thank you for comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
American Electric Power	In the spirit of Paragraph 81 efforts, we request the removal of R1. R1 is administrative in nature, existing only to support R2. Reporting an event externally might necessitate the need for a plan/procedure/policy/job aide, but requiring it is an overreach. Having two requirements rather than one increases the likelihood of being found non-compliant for multiple requirements rather than a single requirement. The Paragraph 81 project team has already recommended removing the requirement to have contact information with law enforcement from CIP-001 R4. Notwithstanding our comments above, we recommend removing the phrase "and other organizations..." from R1. If this requirement is to remain, it needs to be very specific regarding who needs to be included in the reporting.R2 – We recommend removing "per their Operating Plan" from R2 so it reads "Each Responsible Entity shall report events within 24 hours of meeting an event type threshold for reporting." If an entity deviates from its plan but still meets the intent of the requirement (e.g. reporting to NERC with 24 hours), this could be viewed as a finding of non-compliance. We need to get away from "compliance for compliance's sake", and focus solely on those efforts which will benefit the reliability of the BES. Attachment 1 Page 13, Row 1 (Clean Version): This is too open-ended and would likely lead to voluminous reporting. As it currently reads, "Damage or destruction of a Facility within its

Organization	Question 3 Comment
	Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in actions to avoid a BES Emergency" could bring all copper thefts into scope. Thefts should not need to be reported unless the theft results in reliability concerns as specified by other criteria or parameters in Attachment 1. Attachment 1 Page 13, Row 2 (Clean Version): The threshold "Damage or destruction of its Facility that results from actual or suspected intentional human action" should be eliminated entirely. For the event Damage or destruction of a Facility, the threshold for reporting is set too low. Attachment 1 Page 13, Row 3 (Clean Version): We suggest modifying the text to read "Do not report theft... unless the theft results in reliability concerns as specified by other criteria or parameters in Attachment 1." Attachment 1 Page 14, Row 4 (Clean Version): Regarding "Loss of Firm Load", we suggest making it clear that the MW threshold is an aggregate value for those entities whose TOP is responsible for multiple operating companies or legal entities. In addition, is it necessary to include the DP as an entity with reporting responsibility? Its inclusion could create confusion by further segmenting the established threshold. Attachment 1 Page 15, Row 1 (Clean Version): Including "Transmission loss" as currently drafted would result in much more reporting than is necessary or warranted. As currently drafted, it could bring more events into scope than intended, especially for larger entities. EOP-004 Attachment 2: Event Reporting Form: AEP remains concerned that industry would be required to report similar information to multiple Federal entities, in this case to both NERC (Attachment 2) and the DOE (OE-417). In addition, the reporting requirement are not clear for every kind of event as to which entity the reports must be forwarded to, and it is unclear how information would be passed to other entities as necessary. EOP-004 Attachment 2: Event Reporting Form: This form is a further example of mixing security concepts with operational concepts. Not only is not advisable, it does not serve the interests of either concept.

Organization	Question 3 Comment
Response: Thank you for your comment. On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 ("P81") invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program. As the SDT is moving forward with a Recirculation Ballot, your suggestions will be forwarded to NERC for future consideration. As the Paragraph 81 efforts are beyond the scope of this project, the SDT can only pass along your suggestion to that project team for action there. **Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.**	
Midwest Independent Transmission System Operator, Inc.	MISO respectfully submits that several of the thresholds for reporting in EOP-004 - Attachment 1 should be modified to clarify when the reporting obligation is triggered, and to ensure that entities are reporting events of the type and significance intended. In particular, MISO focuses on the following draft thresholds in EOP-004 - Attachment 1: o The requirement that an entity report when "[d]amage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in actions to avoid a BES Emergency." A BES Emergency is defined as "Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System."RCs and BAs take actions each and every day to "avoid a BES Emergency." At the time of those actions, they are reacting to conditions that their operating personnel are observing on the

Organization	Question 3 Comment
	BES. There is no way for an RC or a BA to discern whether the conditions to which they reacted resulted from the "damage or destruction of a Facility" and there is no requirement for Transmission Operators and/or Owners to report "damage or destruction of a Facility" to their BA or RC. Accordingly, RCs and BAs will likely, often not be sufficiently informed to determine if their actions require them to submit a report. Responsible entities are likely to expend significant time and resources reporting daily operations and actions routinely taken to respond to observed BES conditions as they present themselves. These actions may be in response to congestion, equipment outages, relay malfunctions, etc. Whether or not the initiating factor was "damage to or destruction of a Facility" will often be an unknown factor and - even if such is known - the genesis of that damage and/or what constitutes damage (as discussed below) present further potential for confusion and over-reporting, Nonetheless, the lack of clarity in the standard is likely to result in some RCs and BAs preparing reports whether or not they definitely ascertain the underlying cause for the system conditions that prompted them to take actions "to avoid a BES Emergency." The preparation and submission of such reports, in many cases, will not facilitate the stated objective of this standard, which is the improvement of the reliability of the Bulk Electric System. In addition, with respect to damage or destruction of a Facility, it is debatable as to what would be considered "damage." For example, would an improper repair or outage that results in damage to a Facility that requires a more extended repair or outage be deemed "damage" to that Facility under this standard? These ambiguities will likely result in significant over-reporting, over-burdening responsible entities, and inundating Regional Entities and NERC with information that is not useful for the purpose of facilitating the reliable operation of the Bulk Electric System. These effects would undermine the express purpose of the standard and the potential value of information if the reporting obligations are appropriately defined, assigned, and scoped. For these reasons, MISO recommends that the SDT revise the standard to: (1) remove the requirement for RCs and BAs to report the "damage or destruction of a Facility" as it is redundant of the immediately subsequent requirement, (2) to remove reporting responsibility from BAs to report the "damage or destruction of a Facility" as this obligation is more properly placed with the TO, TOP, GO , GOP, and DP, and (3) provide guidance to the remaining responsible entities, TO, TOP, GO , GOP, and DP, regarding when "damage" to a Facility should be reported, e.g., an illustrative list of the types of "damage" that would yield information and/or trends that

Organization	Question 3 Comment
	would facilitate the improvement of the reliability of the BES. o The requirement to report "[p]hysical threats to a Facility" and/or "[p]hysical threats to a BES Control Center"With respect to physical threats to Facilities or BES Control Centers, what is considered a "physical threat" and/or a "suspicious device or activity"? Is a crank call count that the building is on fire a physical threat? Is the return of a disgruntled employee suspicious? MISO understands and supports the reporting and analysis of threats and even certain types of suspicious activities, etc. It is merely concerned that the reporting threshold expressed in this standard will result in the reporting of substantial amounts of data that will not facilitate the improvement of the reliability of the BES and that the volume of reports may delay or otherwise obscure the detection of notable trends. Accordingly, MISO recommends that the SDT revise the standard to: (1) require the reporting only of substantial physical threats that are likely to have an adverse impact on the reliable operation of the Bulk Electric System, and (2) to provide an illustrative list of the types of "suspicious activity or devices" as guidance to responsible entities. o Timing of reports Finally, MISO respectfully suggests that NERC re-assess the timing requirements as related to the objectives expressed within this standard. MISO believes that NERC should clarify that its "situational awareness" staff will review submitted information to determine whether there are indications of possible coordinated attack and to quickly inform responsible entities that there are signals of possible coordinated attack. This clarification could be made in the standard, or the standard could describe the process that NERC staff will use. Unless such review and information is provided, the need that the standard attempts to address will not be fully met. Conversely, many of the events listed in Attachment A that require reporting do not need to be reported within 24 hours and would not offer significant benefit or value if reported within that time period as NERC and Regional Entities primarily utilize such information to capture metrics or perform after-the-fact events analysis. Accordingly, MISO respectfully suggests that, while performing analysis to determine clarifications that would result in the appropriate definition, assignment, and scope of reporting obligations, NERC should also examine the events and identify those events for which a longer time period for reporting would be suitable. This would significantly reduce the administrative burden on responsible entities and likely result in more comprehensive,

Organization	Question 3 Comment
	rigorous, and beneficial reporting.
Response: Thank you for your comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Indiana Municipal Power Agency	On page 6 of 23 of the draft standard document, second paragraph under Rationale for R1, the SDT uses the words "Every industry participant that owns or operates elements or devices on the grid has a formal or informal process..." The use of these words implies that this requirement and others in this standard may apply to every industry entity regardless if they are a registered entity or not. IMPA understands that standards can only apply to entities that are registered with NERC, but we still prefer to see different wording in this sentence. IMPA recommends using "Every registered entity that owns or operates elements or devices on the grid has a formal or informal process..." **We have revised "industry participants" to Registered Entity".** Another concern is on pages 18, 19, and 20 of 23. It is not clear what exactly is required of a registered entity and the law enforcement reporting process. IMPA understands it is up to the entity to decide just how its event reporting Operating Plan is made up and who is contacted for the events in attachment 1. These pages are confusing when it comes to the listing of stakeholders in the reporting process on page 18 of 23 and then when the SDT states that an entity may just notify the state or provincial or local level law enforcement agency. The SDT needs to clarify that the listing of stakeholders on page 18 of 23 is just a suggestive listing and that if the entity so decides per its reporting Operating Plan that notification of the local law enforcement agency is sufficient (the thought that the local law enforcement agency can coordinate with additional law enforcement agencies if it sees the need). The requirement to contact the FBI in CIP-001 is not a requirement in EOP-004-2 unless the registered entity puts that requirement in its event reporting Operating Plan. **The information on law enforcement in the Guidelines and Technical Basis section is**

Organization	Question 3 Comment
	designed to provide *one* example of how an entity *could* report to law enforcement. It is not intended to be the *only* possible way. As a clarification, in the Background section's second paragraph, it should read "retiring both EOP-004-1 and CIP-001-2a" as opposed to CIP-002-2a as written above in this comment document. **We have searched the comment form and cannot find this.**
Response: Thank you for your comment. Please see responses above.	
Cogentrix Energy	Overall: The standard makes good stride in eliminating the redundancy of CIP-001 and EOP-004. M1 States: "... and each organization identified to receive an event report for event types specified in EOP-004-2 Attachment 1". It is an unclear in the statement that the protocols go with Attachment 1 and entities to receive report are part of Attachment 2While this draft is an improvement on the previous draft, the proposed R2 is unacceptable, and should be amended to, at a minimum, require reporting by the end of the next business day, instead of within 24 hours. Events or situations affecting real time reliability to the system already are required to be reported to appropriate Functional Entities that have the responsibility to take action. Adding one more responsibility to system operators increases the operator's burden, which reduces the operator's effectiveness when operating the system. Care should be given when placing additional responsibility on the system operators. Allowing reporting at the end of the next business day gives operators the flexibility to allow support staff to assist with after-the-fact reporting requirements. For some event types where in order to provide real time situational awareness over a wide area (for example coordinated sabotage event) it may be appropriate to have more timely reporting. If the intent of this standard is to address sabotage reporting there needs to be an understanding of the actions to be taken by those receiving the reports so the reporting entities can incorporate those actions into their plan. As a minimum, NERC should have a process in place to assess the reports and take appropriate actions. Attachment 1: Threshold for reporting should not be defined such that multiple reports would be required for the same event. For example, both the TOP and RC being required to report

Organization	Question 3 Comment
	the outage of a transmission line. 2nd event type (Damage or destruction of a Facility): Add the following sentence to the Threshold for Reporting: "Do not report theft or damage unless it degrades normal operation of a Facility." 4th event type (Physical threats to a BES control center): The term "BES control center" needs to be clarified. 5th, 6th, and 7th event types: In instances where a reliability directive is issued, is the "initiating entity" the entity that issues the directive or the entity that carried out the directive. 9th event type (Voltage deviation on a Facility): Change "nominal" to "expected or scheduled." 15th event type (Transmission loss): It is not clear what is meant by "contrary to design." This is so broad that it could be interpreted as requiring reporting misoperations within the reporting time frame before even an initial investigation can begin. This needs to be clarified and tied to the impact on the reliability of the BES.
Response: Thank you for your comment. The full Measure M1 states: "Each Responsible Entity will have a dated event reporting Operating Plan that includes, but is not limited to the protocol(s) and each organization identified to receive an event report for event types specified in EOP-004-2 Attachment 1 and in accordance with the entity responsible for reporting." It is expected that the Operating Plan will contain the entities to which a report will be submitted. The Measure indicates evidence needs to be provided showing that these entities received the event report. The protocol(s) refer to the Operating Plan and could include any procedures for identification of events as well as communicating to other entities. **In response to your suggestion on Requirement R2, the DSR SDT has added clarifying language to R2 as follows:** **R2. Each Responsible Entity shall report events per their Operating Plan within 24 hours of meeting an event type threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). [Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]** **Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation**	

Organization	Question 3 Comment
ballot.	
Northeast Power Coordinating Council	Paragraph 81 efforts are underway to eliminate requirements that have little or no reliability benefit. This Standard only addresses documentation and has no impact on reliability.
Response: Thank you for your comment. On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 ("P81") invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program. As the Paragraph 81 efforts are beyond the scope of this project, the SDT can only pass along your suggestion to that project team for action there.	
Puget Sound Energy Inc.	Puget Sound Energy appreciates the Standard Drafting Team's work to streamline and clarify the proposed standard. In addition, we understand that the Standard Drafting Team faces a significant challenge in developing workable thresholds for reporting under this standard. Unfortunately, Puget Sound Energy cannot support the proposed standard because the reporting thresholds remain too vague and, thus, too broad - especially those related to damage or destruction of a Facility and those related to physical threats. The first four events listed on Attachment 1 are not brightline rules, because they each involve significant elements of judgment and interpretation. An example of our concern relates to the phrase "... that results from actual or suspected intentional human action." Puget Sound Energy, like many regulated entities, is staffed only with System Operators at night and on weekends. As a result, the 24-hour reporting requirement necessarily requires the System Operators to submit the required reports. So, how is a System Operator going to judge whether a human action is "intentional"? As a result, it will be necessary to report any event in which human action is

Organization	Question 3 Comment
	involved because there is no way for a System Operator to know for sure whether the action is intentional or not. And, regulated entities will need to instruct their System Operators to make such reports, because the failure to submit a report of even one event listed in EOP-004 Attachment 1 is assigned a severe VSL under the proposed standard. We believe that the proposed threshold language will likely result in a flood of event reports that will not improve situation awareness.
Response: Thank you for your comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot. **In response to your concern on the 24-hour reporting requirement, the DSR SDT has added clarifying language to R2 as follows:** **R2. Each Responsible Entity shall report events per their Operating Plan within 24 hours of recognition of meeting an event type threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). [Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]**	
Exelon Corporation and its affiliates	Thanks to the drafting team for all the work on this revision. Significant progress was made, though Exelon has some remaining comments: o It's not clear why the team separated 'Damage or destruction of a Facility' into two rows. Please advise. **Response: The first row applies to the RC, which may not own any Facilities but has them under their operational control. This event applies to damage or destruction whereby the RC, TOP or BA has to take action to avoid a BES Emergency. The second row is simply damage or destruction of a Facility. It is expected that this second type of event would not be severe enough to have to take action to avoid a BES Emergency.** o Damage or destruction of a Facility - The threshold for "damage or destruction of a Facility"

Organization	Question 3 Comment
	is too open-ended without qualifying the device or activity as “confirmed”. Event reporting for nuclear generating units are initiated when an incident such as tampering is "confirmed". EOP-004 should include some threshold of proof for a reason to believe that no other possibility exists for "damage or destruction of a facility" event other than actual or suspected intentional human action. **Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.** o Physical threats to a Facility - Reporting of every “suspicious activity” such as photographing equipment or site could result in an unwieldy volume of reports and dilute the data from depicting quality insight. For example, nuclear generating units are required to report all unauthorized and/or suspicious activity to the NRC. Please confirm that the intent of this threshold for notification would include all unauthorized and/or suspicious activity. **The SDT concurs that the intent of the threshold for notification would include all unauthorized and/or suspicious activity.** o Physical threats to a BES control center - please confirm that reporting responsibility falls to the RC, BA, TOP and not GOs. In addition, please confirm that by use of the lower case “control center” other definitions in development through other standards development projects (e.g. CIP version 5) and that may be added to the NERC Glossary will not apply until formally vetted in a future EOP-004 standards development project. **The entities listed for this event type are the RC, BA and TOP only. No other entities are applicable for this event type. If the lower case “control center” is replaced by a definition developed in future standards actions, a change to EOP-004-2 to use the defined term would require notice to the industry and a ballot of the revised standard in some manner. The DSR**

Organization	Question 3 Comment
	SDT does not have control over how that would be accomplished. o Loss of firm load - "Loss of firm load for â‰¥ 15 Minutes: â‰¥ 300 MW for entities with previous year's demand â‰¥ 3,000 MW". Please clarify whether the team intends for this to apply to a single event a loss of more than 300 MW due to non-concurrent multiple distribution outages that total > 300MW. **This event relates to a single incident of the loss of firm load.** o Generation loss - Exelon appreciates the timing clarification added to the generation loss threshold. The phrase "within one minute" should also be included in the threshold for the ERCOT and Quebec Interconnections to read: "Total generation loss, within one minute, of â‰¥ 2,000 MW for entities in the Eastern or Western Interconnection OR Total generation loss, within one minute, of â‰¥ 1,000 MW for entities in the ERCOT or Quebec Interconnection" **The phrase "within one minute" applies to everything listed in the event. To clarify this, we have inserted a colon after the word "of" and moved "≥ 2,000 MW for entities in the Eastern or Western Interconnection" down one line.** o The Law Enforcement Reporting section in the Guideline and Technical Basis states: "The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of the BES from malicious physical or cyber attack." Since CIP-008 now covers reporting of cyber incidents the reference to cyber should be removed. **We have made the correction in your last point regarding "cyber attacks" and have removed it from the Guidelines and Technical Basis section.**
Response: Thank you for your comment. Please see responses embedded above.	
MRO NSRF	The NSRF requests that the SDT address the following concerns and clarifications in Attachment 1; 1) Please explore redundancy reporting event Item #14; Complete loss of off-site power to a

Organization	Question 3 Comment
	nuclear generating plant with obligations of NUC-001-2.1 R9.4.4."Provisions for supplying information necessary to report to government agencies, as related to NPIRs." The NSRF understands the importance concerning safety issues with a nuclear plant. A multiple unit coal facility may have a larger reliability impact to the BES than a nuclear plant. The SDT is stating that the fuel source is a reporting issue, not the reliability of a plant loosing off sight power. Recommend that this item be deleted. 2) Item 2 in Attachment 1 would obligate an entity to report any loss of (copper) grounds either on a T-Line or grounds associated with a transformer or breakers and that this level of reporting should not rise to the NERC level. Believes that additional qualifying language similar to Item 1 be incorporated into the threshold and read as follows:"Damage or destruction of its Facility that results from actual or suspected intentional human action that results in actions to avoid a BES Emergency." 3) Item 3 Attachment 1 needs clarification since a physical threat needs to be actual and confirmed so that the TO or TOP repositions the system. In addition, the SDT needs to clarify what the phrase "normal operations" means. (Is this a ratings issue? or a result in how the System Operator operates the system.) 4) Item 3 should provide clarification as to "Suspicious device or activity at a Facility" to determine when threshold raises to the level of reporting. We are concerned that, based on an Auditors perception, these words could be interpreted in several different ways. In addition, we believe that language needs to be included that the threat causes the reporting entity to change to an abnormal operating state. This situation could be interpreted differently by the auditor or the entity at the time of the event. Recommend the following language: "Suspicious device or activity at a Facility with the potential to degrade the normal operation of the Facility". This language is similar to the first threshold. 5) The term Initiating entity is used three times within Attachment 1 and needs to be more clearly defined or reworded. Is it the entity that identifies the needs of a Public Appeal or the entity that makes the public appeal the initiating entity? The word "initiating" does not provide clarity but only provides uncertainty to the industry. The Standard needs to be clear on who has the responsibility as the "initiating". Recommend the following: a. For public

Organization	Question 3 Comment
	appeal, under Entity with Reporting Responsibility; "entity that issues a public appeal to the public" b. For system wide voltage reduction, under Entity with Reporting Responsibility; "entity that activates a voltage reduction" c. For manual load shedding, under Entity with Reporting Responsibility; "entity that activates manual load shedding" 6) The NSRF recommends transmission loss to read as: "contrary to protection system design" found in threshold for reporting within the Attachment for a Transmission loss event. 7) In Requirement 2/ Measure 2, recommend adding "upon recognition of " as a starting point to the 24 hour reporting requirement, within the threshold of reporting where perceived threats are the threshold, or transmission loss, when contrary to design is determined.
Response: Thank you for your comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot. **7) This was the intent of the drafting team and we have made this clarification to R2 and M2.**	
Independent Electricity System Operator	The proposed implementation plan may conflict with Ontario regulatory practice respecting the effective date of the standard. It is suggested that this conflict be removed by: Moving the last part ", or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities." to right after "this standard is approved by applicable regulatory approval" in the Effective Dates Section on P.2 of the draft standard, and the proposed Implementation Plan.
Response: Thank you for your comment. The SDT used the standard language provide by NERC Legal and intended to address all of the jurisdictions in which the standard may become enforceable. We will refer your suggestion to NERC Legal for consideration in the preparation of the filing.	
Bonneville Power Administration	The proposed standard does not have any oral reporting option for system operators and thus appears to be administrative in nature. Due to this and the fact that administrative staff are

Organization	Question 3 Comment
	not available on weekends, the "24 hour" reporting requirements should be modified to "Next Business Day" to allow for weekend delays in reporting.BPA believes that there are too many minor events that have to be reported within 24 hours. Reporting during the next business day would suffice. Some examples include: A 115 shunt capacitor bank failure for the first event type does not seem important enough to require reporting within 24 hours just because action has to be taken to raise generation or switching of line. A failure of a line tower that has proper protective action to clear the line and also has automatic (SPS) to properly protect as designed the BES system (a good normal practice) from overloads or voltage issues does not seem important enough to require reporting within 24 hours either.
Response: Thank you for your comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Clark Public Utilities	The SDT has not adequately addressed my comments from the last draft regarding damage or destruction of its facility that results from actual or suspected intentional human action. The SDT needs to limit what it means by damage. As an example, if someone breaks into a substation and paints graffiti on a breaker that is part of the BES, the breaker has been "damaged." However, the breaker's ability to function has not been compromised and there are no emergency actions that need to be taken. There is no reason for an emergency reporting procedure to require this to be reported. The SDT needs to add the same modifier for damage that it added in the previous event threshold for reporting. The reference for this type of damage should be as follows:Event: Damage or destruction of a Facility.Entity with Reporting Responsibility: BA, TO, TOP, GO, GOP, DP.Threshold for Reporting: Damage or destruction of its Facility that results from actual or suspected intentional human action that results in actions to avoid a BES Emergency.
Response: Thank you for your comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has	

Organization	Question 3 Comment
reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Lewis County PUD	We are a small utility with little impact to the BES with a small hydro on the end of a 230kV line. CIP-001 requires us to contact the FBI who has repeatedly instructed us to call the local sheriff office. The sheriff office has instructed us to call 911 and they will contact the FBI as needed. Therefore, 911 is our only contact number and our plan if vandalism, property destruction or sabotage is to have a supervisor call 911 and report. I do not think calling 911 to confirm the contact number serves any propose. Our plan will be simple with not a lot detail. The drafting team should recognize the reality of small utilities and state the required plan may be simple and not follow the flowchart in the draft standard.
Response: Thank you for your comment. The SDT did recognize your circumstances and set the requirements to provide the flexibility to address the diversity of entities to which the standard is intended to apply.	
SPP Standards Review Group	We have made previous comments in the past regarding the listing in the Entity with Reporting Responsibility column of Attachment 1. While we concur with some of the changes that the drafting team has made regarding the addition of a bright line in the Threshold for Reporting column, there remain events where there is no line at all. For example, in the Transmission loss event, the TOP is listed and there is no distinction regarding which TOP is required to file the event report. Is it the TOP in whose TOP area the loss occurred or is it a neighboring TOP who observes the loss. Clearly, the responsibility for reporting lies with the host system. There are several other similar events where the bright line is non-existent and needs to be added. We suggest that the drafting team return the deleted language to the Entity with Reporting Responsibility column in those instances where the bright line has not been added in the Threshold column. Regarding multiple reports for a single event, we again believe that only a single report should be required. While additional information may be available from others, let the Event Analysis personnel do their job investigating an event and eliminate any redundant reporting that is currently required as the standard is written. If not, this standard, if approved, would then appear to be a likely candidate for Phase 2 of the

Organization	Question 3 Comment
	Paragraph 81 project.
Response: Thank you for your comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot. On March 15, 2012, FERC issued an order on NERC's Find, Fix and Track process and in paragraph 81 ("P81") invited NERC and other entities to propose to remove from Commission-approved Reliability Standards unnecessary or redundant requirements. In response to P81 and the Commission's request for comments to be coordinated, during June and July 2012, various industry stakeholders, Trade Associations, staff from NERC and staff from the NERC Regions jointly discussed consensus criteria and an initial list of Reliability Standard requirements that appeared to easily satisfy the criteria, and, thus, could be retired. In Phase 1 of the Paragraph 81 effort, only two of the requirements (in total) from CIP-001 and EOP-004 met the initial threshold for being included in the P81 Project. Both of these requirements will also be retired by EOP-004-2. Phase 2 of the Paragraph 81 Project will evaluate all NERC Reliability Standards, including any modifications to EOP-004-2. CIP-001-2a and EOP-004-1 are mandatory and enforceable NERC Reliability Standards. If EOP-004-2 is not approved by the industry, those standards will remain as is and subject to the Compliance Monitoring and Enforcement Program. As the SDT is moving forward with a Recirculation Ballot, your suggestions will be forwarded to NERC for future consideration.	
SERC OC Standards Review Group	While this draft is an improvement on the previous draft, the proposed R2 is unacceptable, and should be amended to, at a minimum, require reporting by the end of the next business day, instead of within 24 hours. Events or situations affecting real time reliability to the system already are required to be reported to appropriate Functional Entities that have the responsibility to take action. Adding one more responsibility to system operators increases the operator's burden, which reduces the operator's effectiveness when operating the system. Care should be given when placing additional responsibility on the system operators. Allowing reporting at the end of the next business day gives operators the flexibility to allow support staff to assist with after-the-fact reporting requirements. For some event types where in order to provide real time situational awareness over a wide area (for example coordinated sabotage event) it may be appropriate to have more timely reporting .If the intent of this standard is to address sabotage reporting there needs to be an understanding of the actions to be taken by those receiving the reports so the reporting entities can incorporate those actions into their

Organization	Question 3 Comment
	plan. As a minimum, NERC should have a process in place to assess the reports and take appropriate actions. Attachment 1: Threshold for reporting should not be defined such that multiple reports would be required for the same event. For example, both the TOP and RC being required to report the outage of a transmission line. 2nd event type (Damage or destruction of a Facility): Add the following sentence to the Threshold for Reporting: "Do not report theft or damage unless it degrades normal operation of a Facility." 4th event type (Physical threats to a BES control center): The term "BES control center" needs to be clarified. 5th, 6th, and 7th event types: In instances where a reliability directive is issued, is the "initiating entity" the entity that issues the directive or the entity that carried out the directive. 9th event type (Voltage deviation on a Facility): Change "nominal" to "expected or scheduled." 15th event type (Transmission loss): It is not clear what is meant by "contrary to design." This is so broad that it could be interpreted as requiring reporting misoperations within the reporting time frame before even an initial investigation can begin. This needs to be clarified and tied to the impact on the reliability of the BES. The comments expressed herein represent a consensus of the views of the above named members of the SERC OC Standards Review Group only and should not be construed as the position of SERC Reliability Corporation, its board, or its officers.
Response: Thank you for your comment. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
Tacoma Public Utilities	Why does the text "...but is not limited to..." in M1 have to be included? Does this mean that

Organization	Question 3 Comment
	there are unwritten requirements that an auditor might look for? What if, in trying to validate contact information, contacts do not confirm their information? Regarding the Loss of firm load row in Attachment 1, an exception should be made for weather or natural disaster related threats in the Threshold for Reporting. Regarding the Transmission loss row in Attachment 1, it is not quite clear which types of BES Elements would meet the Threshold for Reporting. Is it just lines, buses, and transformers? What about reactive resources? What about generators that unexpectedly trip offline during a fault on the transmission system?
Response: Thank you for your comment. In Measure M1 the text "but is not limited to" is intended to provide flexibility for each entity to determine, based on its assets and unique situation, to develop an Operating Plan that appropriately supports reliability. Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.	
MidAmerican Energy	Yes. 1) MidAmerican Energy agrees with and supports MRO NSRF comments. 2) Add additional wording to clearly provide for compliance when events are found more than 24 hours after an event. Add the following to the end of R2. Add, Events not identified until sometime later after they occurred shall be reported within 24 hours. 3) In R3 add "external" for R3 to read Validate "external" contact information. 4) In EOP-004-2 Attachment 1 - the wording "Damage or destruction of its Facility that results from actual or suspected intentional human action that results in actions to avoid a BES Emergency" is not specific or measureable and therefore ambiguous. Zero defect standards which carry penalties must be specific. Please reword to "Intentional human action to destroy a NERC BES facility whose loss could result in actions to avoid a BES Emergency". This clearly aligns with the EOP-004 intent of sabotage and emergency reporting. EOP-004 should not report on unexpected conditions such as when a system operator attempts to reclose a line

Organization	Question 3 Comment
	during a storm believing the line tripped for a temporary fault due to debris, when in fact the fault was permanent and damaged a transformer.
Response: Thank you for your comment. See response to MRO NSF comments. **Many suggestions were made regarding the language of certain events listed in Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot.**	
american Transmission Company	Yes A. ATC requests that the Standards Drafting Team address the following concerns and clarifications in Attachment 1: a.) Reporting event #14 in Attachment 1, is duplicative with respect to Nuclear Reliability Standard NUC-001-2.1 R 9.4.4. Reporting event #14 requires entities to report to NERC a "Complete loss of off-site power to a nuclear generating plant" while Nuclear Reliability Standard NUC-001-2.1 R9.4.4., i.e. includes "Provisions for supplying information necessary to report to government agencies, as related to Nuclear Plant Interface Requirements (NPIRs)". In addition, ATC believes the reporting related to event #14 in Attachment 1 is not a "reliability" issue, and more appropriately covered under Standard NUC-001 as a "Nuclear Safety Shutdown" issue. Therefore, ATC recommends that Item #14 in Attachment 1 of EOP-004-2 be deleted. b.) In Attachment 1, reporting event #2, i.e. Damage or destruction of a Facility" could obligate an entity to report any loss of copper grounds either on a T-Line or grounds associated with a transformer or breakers. ATC believes this does not rise to a reporting level such as NERC. ATC believes that additional qualifying language similar to reporting item #1 be incorporated into the threshold and read as follows: "Damage or destruction of its Facility that results from actual or suspected intentional human action that results in actions to avoid a BES Emergency." c.) In Attachment 1, reporting event #3 i.e. "Physical threats to a Facility" needs clarification

Organization	Question 3 Comment
	since a physical threat needs to be actual and confirmed so that the TO or TOP repositions the system. In addition, the SDT needs to clarify what the phrase "normal operations" means. Is this a ratings issue? Or a result in how the Operator operates the system. d.) In Attachment 1, reporting event #3 threshold i.e. "Suspicious device or activity at a Facility" needs clarification to determine when it raises to the level of reporting. These words could be interpreted in several different ways. In addition, ATC believe that language needs to be added that the threat causes the reporting entity to change to an abnormal operating state. ATC recommends the threshold be revised to read: "Suspicious device or activity at a Facility with the potential to degrade the normal operation of the Facility". e.) In Attachment 1, the term "Initiating entity" is used three times for reporting events and needs to be clearly defined or reworded. Is it the entity that identifies the needs of a Public Appeal or the entity that makes the public appeal the initiating entity? The Standard needs to be clear on who has the responsibility as the "initiating" party, especially when multiple parties may be involved. ATC recommends the following:1) For public appeal, under Entity with Reporting Responsibility; it is the "entity that issues a public appeal to the public"2) For system wide voltage reduction, under Entity with Reporting Responsibility; it is the "entity that activates a voltage reduction"3) For manual load shedding, under Entity with Reporting Responsibility; it is the "entity that activates manual load shedding" f.) In Attachment 1, reporting event #15 i.e. "Transmission Loss", the threshold includes the phrase "contrary to design". ATC recommends this be clarified to read "contrary to protection system design". B. In EOP-004-2 Requirement 2/ Measure 2 both have the following language:"Each Responsible Entity shall report events per their Operating Plan within 24 hours of meeting an event type threshold for reporting." ATC recommends adding "upon recognition" as a starting point to the 24 hour reporting requirement. This would be revised to read: "Each Responsible Entity shall report events per their Operating Plan within 24 hours of recognition of an event type threshold"
Response: Thank you for your comment. A) Many suggestions were made regarding the language of certain events listed in	

Organization	Question 3 Comment
	Attachment 1. Most of these comments are about a single event type and were made by only one stakeholder. The team has reviewed all of these comments. In several cases, the same or a similar suggestion was made on an earlier draft, and the team considered it at that time. The SDT believes that stakeholder consensus has been achieved regarding these event types. The team has elected to move forward to recirculation ballot. **B) This was the intent of the drafting team and we have made this clarification to R2 and M2.**

END OF REPORT

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SC approved SAR for initial posting (April 2009).
2. SAR posted for comment (April 22 – May 21, 2009).
3. SC authorized moving the SAR forward to standard development (September 2009).
4. Concepts Paper posted for comment (March 17 – April 16, 2010).
5. Initial Informal Comment Period (September 15 – October 15, 2010).
6. Second Comment Period (Formal) (March 9 – April 8, 2011).
7. Third Comment Period and Initial Ballot (October 28 – December 12, 2011).
8. Fourth Comment Period and Successive Ballot (April 25 – May 24, 2012).

Proposed Action Plan and Description of Current Draft
This is the fifth posting of the proposed standard in accordance with Results-Based Standards (RBS) criteria. The drafting team requests posting for a 30-day formal comment period concurrent with the formation of the ballot pool and the successive ballot.

Future Development Plan

Anticipated Actions	Anticipated Date
Drafting team considers comments, makes conforming changes on fourth posting	June - August 2012
Fifth Comment/Ballot period	August – September 2012
Recirculation Ballot period	October 2012
Receive BOT approval	November 2012
File with regulatory authorities	December 2012

Effective Dates

The first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities. In those jurisdictions where regulatory approval is not required, the standard shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-2a Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2 Event Reporting; Retire CIP-001-2a Sabotage Reporting and Retired EOP-004-1 Disturbance Reporting.	Revision to entire standard (Project 2009-01)

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

When this standard has received ballot approval, the text boxes will be moved to the Guideline and Technical Basis Section.

A. Introduction

1. Title: Event Reporting

2. Number: EOP-004-2

3. Purpose: To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities.

4. Applicability

4.1. Functional Entities: For the purpose of the Requirements and the EOP-004 Attachment 1 contained herein, the following functional entities will be collectively referred to as "Responsible Entity."

4.1.1. Reliability Coordinator

4.1.2. Balancing Authority

4.1.3. Transmission Owner

4.1.4. Transmission Operator

4.1.5. Generator Owner

4.1.6. Generator Operator

4.1.7. Distribution Provider

5. Background:

NERC established a SAR Team in 2009 to investigate and propose revisions to the CIP-001 and EOP-004 Reliability Standards. The team was asked to consider the following:

1. CIP-001 could be merged with EOP-004 to eliminate redundancies.
2. Acts of sabotage have to be reported to the DOE as part of EOP-004.
3. Specific references to the DOE form need to be eliminated.
4. EOP-004 had some 'fill-in-the-blank' components to eliminate.

The development included other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient Bulk Electric System reliability standards.

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009.

The DSR SDT developed a concept paper to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT had developed. The posting of the concept paper sought comments from stakeholders on the "road map" that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the DSR SDT. The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC issues database and FERC Order 693 Directives in order to determine a prudent course of action with respect to revision of these standards.

B. Requirements and Measures

R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Each Responsible Entity will have a dated event reporting Operating Plan that includes, but is not limited to the protocol(s) and each organization identified to receive an event report for event types specified in EOP-004-2 Attachment 1 and in accordance with the entity responsible for reporting.

Rationale for R1

The requirement to have an Operating Plan for reporting specific types of events provides the entity with a method to have its operating personnel recognize events that affect reliability and to be able to report them to appropriate parties; e.g., Regional Entities, applicable Reliability Coordinators, and law enforcement and other jurisdictional agencies when so recognized. In addition, these event reports are an input to the NERC Events Analysis Program. These other parties use this information to promote reliability, develop a culture of reliability excellence, provide industry collaboration and promote a learning organization.

Every Registered Entity that owns or operates elements or devices on the grid has a formal or informal process, procedure, or steps it takes to gather information regarding what happened when events occur. This requirement has the Responsible Entity establish documentation on how that procedure, process, or plan is organized. This documentation may be a single document or a combination of various documents that achieve the reliability objective.

The communication protocol(s) could include a process flowchart, identification of internal and external personnel or entities to be notified, or a list of personnel by name and their associated contact information. An existing procedure that meets the requirements of CIP-001-2a may be included in this Operating Plan along with other processes, procedures or plans to meet this requirement.

R2. Each Responsible Entity shall report events per their Operating Plan within 24 hours of recognition of meeting an event type threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

M2. Each Responsible Entity will have as evidence of reporting an event, copy of the completed EOP-004-2 Attachment 2 form or a DOE-OE-417 form; and evidence of submittal (e.g., operator log or other operating documentation, voice recording, electronic mail message, or confirmation of facsimile) demonstrating the event report was submitted within 24 hours of recognition of meeting the threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). (R2)

Rationale for R2

Each Responsible Entity must report and communicate events according to its Operating Plan based on the information in EOP-004-2 Attachment 1. By implementing the event reporting Operating Plan the Responsible Entity will assure situational awareness to the Electric Reliability Organization so that they may develop trends and prepare for a possible next event and mitigate the current event. This will assure that the BES remains secure and stable by mitigation actions that the Responsible Entity has within its function. By communicating events per the Operating Plan, the Responsible Entity will assure that people/agencies are aware of the current situation and they may prepare to mitigate current and further events.

R3. Each Responsible Entity shall validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Each Responsible Entity will have dated records to show that it validated all contact information contained in the Operating Plan each calendar year. Such evidence may include, but are not limited to, dated voice recordings and operating logs or other communication documentation. (R3)

Rationale for R3

Requirement 3 calls for the Responsible Entity to validate the contact information contained in the Operating Plan each calendar year. This requirement helps ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization. If an entity experiences an actual event, communication evidence from the event may be used to show compliance with the validation requirement for the specific contacts used for the event.

C. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

The Regional Entity shall serve as the Compliance Enforcement Authority (CEA) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2 Evidence Retention

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain the current Operating Plan plus each version issued since the last audit for Requirements R1, and Measure M1.
- Each Responsible Entity shall retain evidence of compliance since the last audit for Requirements R2, R3 and Measure M2, M3.

If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3 Compliance Monitoring and Enforcement Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4 Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Responsible Entity had an Operating Plan, but failed to include one applicable event type.	The Responsible Entity had an Operating Plan, but failed to include two applicable event types.	The Responsible Entity had an Operating Plan, but failed to include three applicable event types.	The Responsible Entity had an Operating Plan, but failed to include four or more applicable event types. OR The Responsible Entity failed to have an event reporting Operating Plan.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Assessment	Medium	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 24 hours but less than or equal to 36 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to one entity identified in its event reporting Operating Plan within 24 hours.	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 36 hours but less than or equal to 48 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to two entities identified in its event reporting Operating Plan within 24 hours.	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 48 hours but less than or equal to 60 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to three entities identified in its event reporting Operating Plan within 24 hours.	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 60 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to four or more entities identified in its event reporting Operating Plan within 24 hours. OR The Responsible Entity failed to submit a report for an event in EOP-004 Attachment 1.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Operations Planning	Medium	The Responsible Entity validated all contact information contained in the Operating Plan but was late by less than one calendar month. OR The Responsible Entity validated 75% but less than 100% of the contact information contained in the Operating Plan.	The Responsible Entity validated all contact information contained in the Operating Plan but was late by one calendar month or more but less than two calendar months. OR The Responsible Entity validated 50% and less than 75% of the contact information contained in the Operating Plan.	The Responsible Entity validated all contact information contained in the Operating Plan but was late by two calendar months or more but less than three calendar months. OR The Responsible Entity validated 25% and less than 50% of the contact information contained in the Operating Plan.	The Responsible Entity validated all contact information contained in the Operating Plan but was late by three calendar months or more. OR The Responsible Entity validated less than 25% of contact information contained in the Operating Plan.

D. Variances

None.

E. Interpretations

None.

F. References

Guideline and Technical Basis (attached)

EOP-004 - Attachment 1: Reportable Events

NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per Requirement R2 and provide as much information as is available at the time of the notification. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net, Facsimile 404-446-9770 or Voice: 404-446-9780.

Rationale Box for EOP-004 Attachment 1:

The DSR SDT used the defined term "Facility" to add clarity for several events listed in Attachment 1. A Facility is defined as:

> "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"

The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.

Submit EOP-004 Attachment 2 (or DOE-OE-417) pursuant to Requirements R1 and R2.

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
Damage or destruction of a Facility	RC, BA, TOP	Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in actions to avoid a BES Emergency.
Damage or destruction of a Facility	BA, TO, TOP, GO, GOP, DP	Damage or destruction of its Facility that results from actual or suspected intentional human action.
Physical threats to a Facility	BA, TO, TOP, GO, GOP, DP	Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. OR Suspicious device or activity at a Facility. Do not report theft unless it degrades normal operation of a Facility.
Physical threats to a BES control center	RC, BA, TOP	Physical threat to its BES control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. OR Suspicious device or activity at a BES control center.
BES Emergency requiring public appeal for load reduction	Initiating entity is responsible for reporting	Public appeal for load reduction event.
BES Emergency requiring system-wide voltage reduction	Initiating entity is responsible for reporting	System wide voltage reduction of 3% or more.
BES Emergency requiring manual firm load shedding	Initiating entity is responsible for reporting	Manual firm load shedding ≥ 100 MW.

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
BES Emergency resulting in automatic firm load shedding	DP, TOP	Automatic firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS).
Voltage deviation on a Facility	TOP	Observed within its area a voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes.
IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only)	RC	Operate outside the IROL for time greater than IROL T_v (all Interconnections) or Operate outside the SOL for more than 30 minutes for Major WECC Transfer Paths (WECC only).
Loss of firm load	BA, TOP, DP	Loss of firm load for ≥ 15 Minutes: ≥ 300 MW for entities with previous year's demand ≥ 3,000 MW OR ≥ 200 MW for all other entities
System separation (islanding)	RC, BA, TOP	Each separation resulting in an island ≥ 100 MW
Generation loss	BA, GOP	Total generation loss, within one minute, of : ≥ 2,000 MW for entities in the Eastern or Western Interconnection OR ≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection
Complete loss of off-site power to a nuclear generating plant (grid supply)	TO, TOP	Complete loss of off-site power affecting a nuclear generating station per the Nuclear Plant Interface Requirement

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
Transmission loss	TOP	Unexpected loss within its area, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing).
Unplanned BES control center evacuation	RC, BA, TOP	Unplanned evacuation from BES control center facility for 30 continuous minutes or more.
Complete loss of voice communication capability	RC, BA, TOP	Complete loss of voice communication capability affecting a BES control center for 30 continuous minutes or more.
Complete loss of monitoring capability	RC, BA, TOP	Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (i.e., State Estimator or Contingency Analysis) is rendered inoperable.

EOP-004 - Attachment 2: Event Reporting Form

EOP-004 Attachment 2: Event Reporting Form **Use this form to report events. The Electric Reliability Organization will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net , Facsimile 404-446-9770 or voice: 404-446-9780.**		
Task		**Comments**
1.	Entity filing the report include: Company name: Name of contact person: Email address of contact person: Telephone Number: Submitted by (name):	
2.	Date and Time of recognized event. Date: (mm/dd/yyyy) Time: (hh:mm) Time/Zone:	
3.	Did the event originate in your system?	Yes ☐ No☐ Unknown ☐
4.	**Event Identification and Description:**	
	(Check applicable box) ☐ Damage or destruction of a Facility ☐ Physical Threat to a Facility ☐ Physical Threat to a control center ☐ BES Emergency: ☐ public appeal for load reduction ☐ system-wide voltage reduction ☐ manual firm load shedding ☐ automatic firm load shedding ☐ Voltage deviation on a Facility ☐ IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only) ☐ Loss of firm load ☐ System separation ☐ Generation loss ☐ Complete loss of off-site power to a nuclear generating plant (grid supply) ☐ Transmission loss ☐ unplanned control center evacuation ☐ Complete loss of voice communication capability ☐ Complete loss of monitoring capability	Written description (optional):

Guideline and Technical Basis

Distribution Provider Applicability Discussion

The DSR SDT has included Distribution Providers (DP) as an applicable entity under this standard. The team realizes that not all DPs will own BES Facilities and will not meet the "Threshold for Reporting" for any event listed in Attachment 1. These DPs will not have any reports to submit under Requirement R2. However, these DPs will be responsible for meeting Requirements R1 and R3. The DSR SDT does not intend for these entities to have a detailed Operating Plan to address events that are not applicable to them. In this instance, the DSR SDT intends for the DP to have a very simple Operating Plan that includes a statement that there are no applicable events in Attachment 1 (to meet R1) and that the DP will review the list of events in Attachment 1 each year (to meet R3). The team does not think this will be a burden on any entity as the development and annual validation of the Operating Plan should not take more that 30 minutes on an annual basis. If a DP discovers applicable events during the annual review, it is expected that the DP will develop a more detailed Operating Plan to comply with the requirements of the standard.

Multiple Reports for a Single Organization

For entities that have multiple registrations, the DSR SDT intends that these entities will only have to submit one report for any individual event. For example, if an entity is registered as a Reliability Coordinator, Balancing Authority and Transmission Operator, the entity would only submit one report for a particular event rather submitting three reports as each individual registered entity.

Summary of Key Concepts

The DSR SDT identified the following principles to assist them in developing the standard:

- Develop a single form to report disturbances and events that threaten the reliability of the Bulk Electric System
- Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements
- Establish clear criteria for reporting
- Establish consistent reporting timelines
- Provide clarity around who will receive the information and how it will be used

During the development of concepts, the DSR SDT considered the FERC directive to "further define sabotage". There was concern among stakeholders that a definition may be ambiguous and subject to interpretation. Consequently, the DSR SDT decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was sabotage or vandalism without the intervention of law enforcement. The DSR SDT felt that attempting to define sabotage would result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard. The events listed in EOP-004 Attachment 1 were developed to provide guidance for reporting both actual events as well as

events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

The types of events that are required to be reported are contained within EOP-004 Attachment 1. The DSR SDT has coordinated with the NERC Events Analysis Working Group to develop the list of events that are to be reported under this standard. EOP-004 Attachment 1 pertains to those actions or events that have impacted the Bulk Electric System. These events were previously reported under EOP-004-1, CIP-001-1 or the Department of Energy form OE-417. EOP-004 Attachment 1 covers similar items that may have had an impact on the Bulk Electric System or has the potential to have an impact and should be reported.

The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in EOP-004 Attachment 1. Real-time communication is achieved is covered in other standards. The proposed standard deals exclusively with after-the-fact reporting.

Data Gathering

The requirements of EOP-004-1 require that entities "promptly analyze Bulk Electric System disturbances on its system or facilities" (Requirement R2). The requirements of EOP-004-2 specify that certain types of events are to be reported but do not include provisions to analyze events. Events reported under EOP-004-2 may trigger further scrutiny by the ERO Events Analysis Program. If warranted, the Events Analysis Program personnel may request that more data for certain events be provided by the reporting entity or other entities that may have experienced the event. Entities are encouraged to become familiar with the Events Analysis Program and the NERC Rules of Procedure to learn more about with the expectations of the program.

Law Enforcement Reporting

The reliability objective of EOP-004-2 is to improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of Bulk Electric System from malicious physical attack. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.

Stakeholders in the Reporting Process

- Industry
- NERC (ERO), Regional Entity
- FERC
- DOE
- NRC

- DHS – Federal
- Homeland Security- State
- State Regulators
- Local Law Enforcement
- State or Provincial Law Enforcement
- FBI
- Royal Canadian Mounted Police (RCMP)

The above stakeholders have an interest in the timely notification, communication and response to an incident at a Facility. The stakeholders have various levels of accountability and have a vested interest in the protection and response to ensure the reliability of the BES.

Present expectations of the industry under CIP-001-1a:

It has been the understanding by industry participants that an occurrence of sabotage has to be reported to the FBI. The FBI has the jurisdictional requirements to investigate acts of sabotage and terrorism. The CIP-001-1-1a standard requires a liaison relationship on behalf of the industry and the FBI or RCMP. These requirements, under the standard, of the industry have not been clear and have lead to misunderstandings and confusion in the industry as to how to demonstrate that the liaison is in place and effective. As an example of proof of compliance with Requirement R4, Responsible Entities have asked FBI Office personnel to provide, on FBI letterhead, confirmation of the existence of a working relationship to report acts of sabotage, the number of years the liaison relationship has been in existence, and the validity of the telephone numbers for the FBI.

Coordination of Local and State Law Enforcement Agencies with the FBI

The Joint Terrorism Task Force (JTTF) came into being with the first task force being established in 1980. JTTFs are small cells of highly trained, locally based, committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. The JTTF is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. Coordination and communications largely through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs. This information flow can be most beneficial to the industry in analytical intelligence, incident response and investigation. Historically, the most immediate response to an industry incident has been local and state law enforcement agencies to suspected vandalism and criminal damages at industry facilities. Relying upon the JTTF coordination between local, state and FBI law enforcement would be beneficial to effective communications and the appropriate level of investigative response.

Coordination of Local and Provincial Law Enforcement Agencies with the RCMP

A similar law enforcement coordination hierarchy exists in Canada. Local and Provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. The Provincial

law enforcement agency has a reporting relationship with the Royal Canadian Mounted Police (RCMP).

A Reporting Process Solution – EOP-004

A proposal discussed with the FBI, FERC Staff, NERC Standards Project Coordinator and the SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Reportable Events). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial or local level law enforcement agency. The state or provincial or local level law enforcement agency will coordinate with law enforcement with jurisdiction to investigate. If the state or provincial or local level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial or local level law enforcement agency will notify and coordinate with the FBI or the RCMP.

Example of Reporting Process including Law Enforcement

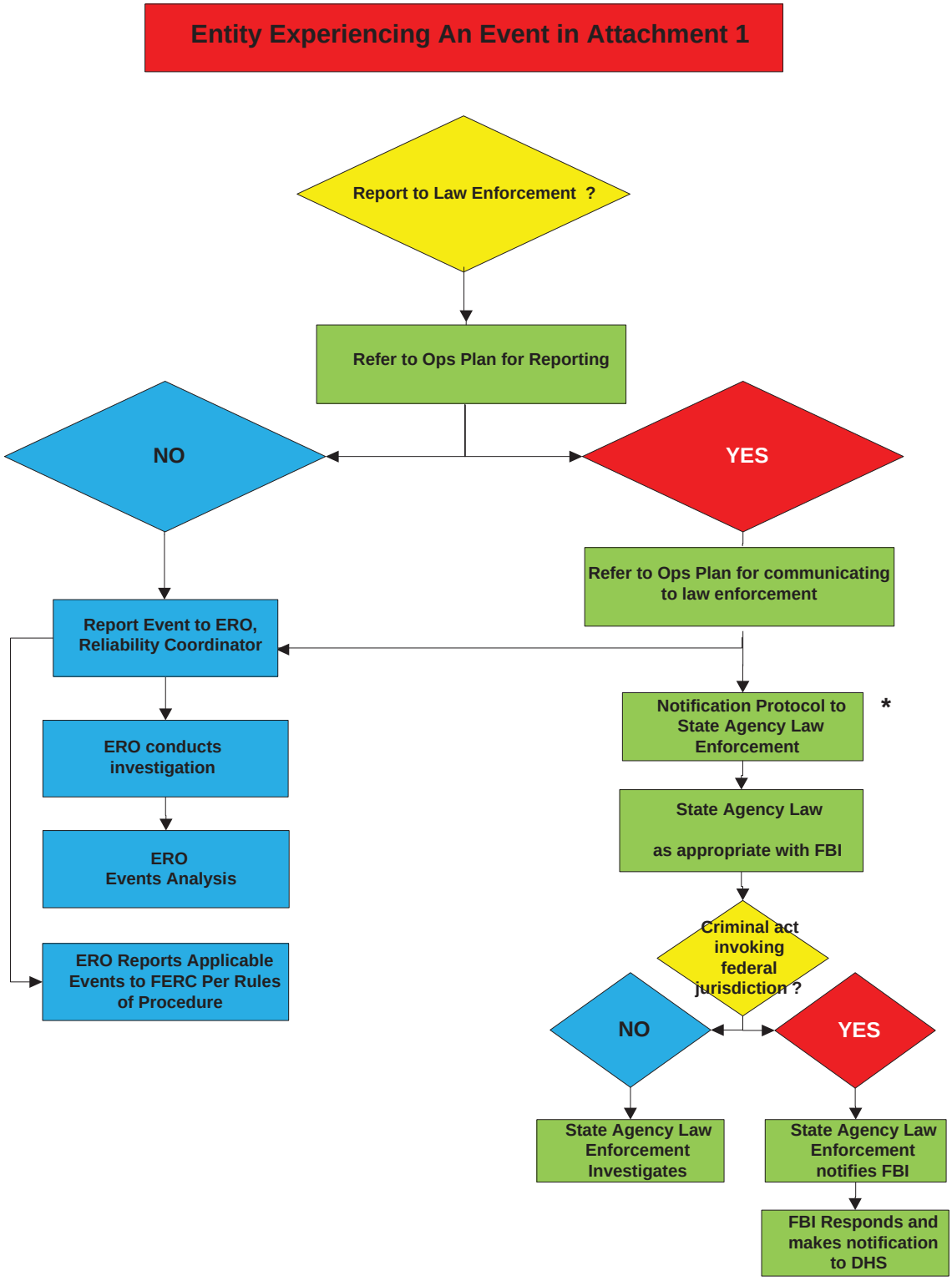

* Canadian entities will follow law enforcement protocols applicable in their jurisdictions

Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01) - Reporting Concepts

Introduction

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and has developed updated standards based on the SAR.

The standards listed under the SAR are:

- CIP-001 — Sabotage Reporting
- EOP-004 — Disturbance Reporting

The changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). These standards deal exclusively with after-the-fact reporting.

The DSR SDT has consolidated disturbance and sabotage event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts and Assumptions:

The Standard:

- Requires reporting of "events" that impact or may impact the reliability of the Bulk Electric System
- Provides clear criteria for reporting
- Includes consistent reporting timelines
- Identifies appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- Provides clarity around of who will receive the information

Discussion of Disturbance Reporting

Disturbance reporting requirements existed in the previous version of EOP-004. The current approved definition of Disturbance from the NERC Glossary of Terms is:

1. An unplanned event that produces an abnormal system condition.
2. Any perturbation to the electric system.
3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.

Disturbance reporting requirements and criteria were in the previous EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and developed the list of events that are to be reported under this standard (EOP-004 Attachment 1).

Discussion of Event Reporting
There are situations worthy of reporting because they have the potential to impact reliability.

Event reporting facilitates industry awareness, which allows potentially impacted parties to prepare for and possibly mitigate any associated reliability risk. It also provides the raw material, in the case of certain potential reliability threats, to see emerging patterns.

Examples of such events include:

- Bolts removed from transmission line structures
- Train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center)
- Destruction of Bulk Electric System equipment

What about sabotage?
One thing became clear in the DSR SDT's discussion concerning sabotage: everyone has a different definition. The current standard CIP-001 elicited the following response from FERC in FERC Order 693, paragraph 471 which states in part: *". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."*

Often, the underlying reason for an event is unknown or cannot be confirmed. The DSR SDT believes that by reporting material risks to the Bulk Electric System using the event categorization in this standard, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.

Certain types of events should be reported to NERC, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and/or Provincial or local law enforcement. Other types of events may have different reporting requirements. For example, an event that is related to copper theft may only need to be reported to the local law enforcement authorities.

Potential Uses of Reportable Information
Event analysis, correlation of data, and trend identification are a few potential uses for the information reported under this standard. The standard requires Functional entities to report the incidents and provide known information at the time of the report. Further data gathering necessary for event analysis is provided for under the Events Analysis Program and the NERC Rules of Procedure. Other entities (e.g. – NERC, Law Enforcement, etc) will be responsible for performing the analyses. The NERC Rules of Procedure (section 800) provide an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for

reliability. Jurisdictional agencies (which may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE) have other duties and responsibilities.

Collection of Reportable Information or "One stop shopping"

The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT has updated the listing of reportable events in EOP-004 Attachment 1 based on discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences still exist.

The reporting required by this standard is intended to meet the uses and purposes of NERC. The DSR SDT recognizes that other requirements for reporting exist (e.g., DOE-417 reporting), which may duplicate or overlap the information required by NERC. To the extent that other reporting is required, the DSR SDT envisions that duplicate entry of information should not be necessary, and the submission of the alternate report will be acceptable to NERC so long as all information required by NERC is submitted. For example, if the NERC Report duplicates information from the DOE form, the DOE report may be sent to the NERC in lieu of entering that information on the NERC report.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SC approved SAR for initial posting (April 2009).
2. SAR posted for comment (April 22 – May 21, 2009).
3. SC authorized moving the SAR forward to standard development (September 2009).
4. Concepts Paper posted for comment (March 17 – April 16, 2010).
5. Initial Informal Comment Period (September 15 – October 15, 2010).
6. Second Comment Period (Formal) (March 9 – April 8, 2011).
7. Third Comment Period and Initial Ballot (October 28 – December 12, 2011).
8. Fourth Comment Period and Successive Ballot (April 25 – May 24, 2012).

Proposed Action Plan and Description of Current Draft
This is the fifth posting of the proposed standard in accordance with Results-Based Standards (RBS) criteria. The drafting team requests posting for a 30-day formal comment period concurrent with the formation of the ballot pool and the successive ballot.

Future Development Plan

Anticipated Actions	Anticipated Date
Drafting team considers comments, makes conforming changes on fourth posting	June - August 2012
Fifth Comment/Ballot period	August – September 2012
Recirculation Ballot period	October 2012
Receive BOT approval	November 2012
File with regulatory authorities	December 2012

Effective Dates

The first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities. In those jurisdictions where regulatory approval is not required, the standard shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-2a Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2 Event Reporting; Retire CIP-001-2a Sabotage Reporting and Retired EOP-004-1 Disturbance Reporting.	Revision to entire standard (Project 2009-01)

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

When this standard has received ballot approval, the text boxes will be moved to the Guideline and Technical Basis Section.

A. Introduction

1. Title: Event Reporting

2. Number: EOP-004-2

3. Purpose: To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities.

4. Applicability

4.1. Functional Entities: For the purpose of the Requirements and the EOP-004 Attachment 1 contained herein, the following functional entities will be collectively referred to as "Responsible Entity."

4.1.1. Reliability Coordinator

4.1.2. Balancing Authority

4.1.3. Transmission Owner

4.1.4. Transmission Operator

4.1.5. Generator Owner

4.1.6. Generator Operator

4.1.7. Distribution Provider

5. Background:

NERC established a SAR Team in 2009 to investigate and propose revisions to the CIP-001 and EOP-004 Reliability Standards. The team was asked to consider the following:

1. CIP-001 could be merged with EOP-004 to eliminate redundancies.
2. Acts of sabotage have to be reported to the DOE as part of EOP-004.
3. Specific references to the DOE form need to be eliminated.
4. EOP-004 had some 'fill-in-the-blank' components to eliminate.

The development included other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient Bulk Electric System reliability standards.

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009.

The DSR SDT developed a concept paper to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT had developed. The posting of the concept paper sought comments from stakeholders on the "road map" that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the DSR SDT. The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC issues database and FERC Order 693 Directives in order to determine a prudent course of action with respect to revision of these standards.

B. Requirements and Measures

R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the R~~r~~egional E~~e~~ntity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Each Responsible Entity will have a dated event reporting Operating Plan that includes, but is not limited to the protocol(s) and each organization identified to receive an event report for event types specified in EOP-004-2 Attachment 1 and in accordance with the entity responsible for reporting.

Rationale for R1

The requirement to have an Operating Plan for reporting specific types of events provides the entity with a method to have its operating personnel recognize events that affect reliability and to be able to report them to appropriate parties; e.g., Regional Entities, applicable Reliability Coordinators, and law enforcement and other jurisdictional agencies when so recognized. In addition, these event reports are an input to the NERC Events Analysis Program. These other parties use this information to promote reliability, develop a culture of reliability excellence, provide industry collaboration and promote a learning organization.

Every Registered Entity~~industry participant~~ that owns or operates elements or devices on the grid has a formal or informal process, procedure, or steps it takes to gather information regarding what happened when events occur. This requirement has the Responsible Entity establish documentation on how that procedure, process, or plan is organized. This documentation may be a single document or a combination of various documents that achieve the reliability objective. The communication protocol(s) could include a process flowchart, identification of internal and external personnel or entities to be notified, or a list of personnel by name and their associated contact information. An existing procedure that meets the requirements of CIP-001-2a may be included in this Operating Plan along with other processes, procedures or plans to meet this requirement.

R2. Each Responsible Entity shall report events per their Operating Plan within 24 hours of recognition of meeting an event type threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

M2. Each Responsible Entity will have as evidence of reporting an event, copy of the completed EOP-004-2 Attachment 2 form or a DOE-OE-417 form; and evidence of submittal (e.g., operator log or other operating documentation, voice recording, electronic mail message, or confirmation of facsimile) demonstrating the event report was submitted within 24 hours of recognition of meeting the threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). (R2)

Rationale for R2

Each Responsible Entity must report and communicate events according to its Operating Plan based on the information in EOP-004-2 Attachment 1. By implementing the event reporting Operating Plan the Responsible Entity will assure situational awareness to the Electric Reliability Organization so that they may develop trends and prepare for a possible next event and mitigate the current event. This will assure that the BES remains secure and stable by mitigation actions that the Responsible Entity has within its function. By communicating events per the Operating Plan, the Responsible Entity will assure that people/agencies are aware of the current situation and they may prepare to mitigate current and further events.

R3. Each Responsible Entity shall validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Each Responsible Entity will have dated records to show that it validated all contact information contained in the Operating Plan each calendar year. Such evidence may include, but are not limited to, dated voice recordings and operating logs or other communication documentation. (R3)

Rationale for R3

Requirement 3 calls for the Responsible Entity to validate the contact information contained in the Operating Plan each calendar year. This requirement helps ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization. If an entity experiences an actual event, communication evidence from the event may be used to show compliance with the validation requirement for the specific contacts used for the event.

C. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

The Regional Entity shall serve as the Compliance Enforcement Authority (CEA) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2 Evidence Retention

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain the current Operating Plan plus each version issued since the last audit for Requirements R1, and Measure M1.
- Each Responsible Entity shall retain evidence of compliance since the last audit for Requirements R2, R3 and Measure M2, M3.

If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3 Compliance Monitoring and Enforcement Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4 Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Responsible Entity had an Operating Plan, but failed to include one applicable event type. ~~N/A~~	The Responsible Entity had an Operating Plan, but failed to include two applicable event types. ~~N/A~~	The Responsible Entity had an Operating Plan, but failed to include three applicable event types. ~~N/A~~	The Responsible Entity had an Operating Plan, but failed to include four or more applicable event types. OR The Responsible Entity failed to have an event reporting Operating Plan.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Assessment	Medium	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 24 hours but less than or equal to 36 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to one entity identified in its event reporting Operating Plan within 24 hours.	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 36 hours but less than or equal to 48 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to two entities identified in its event reporting Operating Plan within 24 hours.	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 48 hours but less than or equal to 60 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to three entities identified in its event reporting Operating Plan within 24 hours.	The Responsible Entity submitted an event report (e.g., written or verbal) to all required recipients more than 60 hours after meeting an event threshold for reporting. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to four or more entities identified in its event reporting Operating Plan within 24 hours. OR The Responsible Entity failed to submit a report for an event in EOP-004 Attachment 1.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Operations Planning	Medium	The Responsible Entity validated all contact information contained in the Operating Plan but was late by less than one calendar month. OR The Responsible Entity validated 75% but less than 100% ~~or more~~ of the contact information contained in the Operating Plan.	The Responsible Entity validated all contact information contained in the Operating Plan but was late by one calendar month or more but less than two calendar months. OR The Responsible Entity validated 50% and less than 75% of the contact information contained in the Operating Plan.	The Responsible Entity validated all contact information contained in the Operating Plan but was late by two calendar months or more but less than three calendar months. OR The Responsible Entity validated 25% and less than 50% of the contact information contained in the Operating Plan.	The Responsible Entity validated all contact information contained in the Operating Plan but was late by three calendar months or more. OR The Responsible Entity validated less than 25% of contact information contained in the Operating Plan.

D. Variances

None.

E. Interpretations

None.

F. References

Guideline and Technical Basis (attached)

EOP-004 - Attachment 1: Reportable Events

NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per Requirement R2 and provide as much information as is available at the time of the notification. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net, Facsimile 404-446-9770 or Voice: 404-446-9780.

Rationale Box for EOP-004 Attachment 1:

The DSR SDT used the defined term "Facility" to add clarity for several events listed in Attachment 1. A Facility is defined as:

> "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"

The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.

Submit EOP-004 Attachment 2 (or DOE-OE-417) pursuant to Requirements R1 and R2.

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
Damage or destruction of a Facility	RC, BA, TOP	Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in actions to avoid a BES Emergency.
Damage or destruction of a Facility	BA, TO, TOP, GO, GOP, DP	Damage or destruction of its Facility that results from actual or suspected intentional human action.
Physical threats to a Facility	BA, TO, TOP, GO, GOP, DP	Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. OR Suspicious device or activity at a Facility. Do not report theft unless it degrades normal operation of a Facility.
Physical threats to a BES control center	RC, BA, TOP	Physical threat to its BES control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. OR Suspicious device or activity at a BES control center.
BES Emergency requiring public appeal for load reduction	Initiating entity is responsible for reporting	Public appeal for load reduction event.
BES Emergency requiring system-wide voltage reduction	Initiating entity is responsible for reporting	System wide voltage reduction of 3% or more.
BES Emergency requiring manual firm load shedding	Initiating entity is responsible for reporting	Manual firm load shedding ≥ 100 MW.

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
BES Emergency resulting in automatic firm load shedding	DP, TOP	Automatic firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS).
Voltage deviation on a Facility	TOP	Observed within its area a voltage deviation of ± 10% of nominal voltage sustained for ≥ 15 continuous minutes.
IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only)	RC	Operate outside the IROL for time greater than IROL T_v (all Interconnections) or Operate outside the SOL for more than 30 minutes for Major WECC Transfer Paths (WECC only).
Loss of firm load	BA, TOP, DP	Loss of firm load for ≥ 15 Minutes: ≥ 300 MW for entities with previous year's demand ≥ 3,000 MW OR ≥ 200 MW for all other entities
System separation (islanding)	RC, BA, TOP	Each separation resulting in an island ≥ 100 MW
Generation loss	BA, GOP	Total generation loss, within one minute, of : ≥ 2,000 MW for entities in the Eastern or Western Interconnection OR ≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection
Complete loss of off-site power to a nuclear generating plant (grid supply)	TO, TOP	Complete loss of off-site power affecting a nuclear generating station per the Nuclear Plant Interface Requirement

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
Transmission loss	TOP	Unexpected loss within its area, contrary to design, of three or more BES Elements caused by a common disturbance (excluding successful automatic reclosing).
Unplanned BES control center evacuation	RC, BA, TOP	Unplanned evacuation from BES control center facility for 30 continuous minutes or more.
Complete loss of voice communication capability	RC, BA, TOP	Complete loss of voice communication capability affecting a BES control center for 30 continuous minutes or more.
Complete loss of monitoring capability	RC, BA, TOP	Complete loss of monitoring capability affecting a BES control center for 30 continuous minutes or more such that analysis capability (i.e., State Estimator or Contingency Analysis) is rendered inoperable.

EOP-004 - Attachment 2: Event Reporting Form

EOP-004 Attachment 2: Event Reporting Form **Use this form to report events. The Electric Reliability Organization will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net , Facsimile 404-446-9770 or voice: 404-446-9780.**		
Task		**Comments**
1.	Entity filing the report include: Company name: Name of contact person: Email address of contact person: Telephone Number: Submitted by (name):	
2.	Date and Time of recognized event. Date: (mm/dd/yyyy) Time: (hh:mm) Time/Zone:	
3.	Did the event originate in your system?	Yes ☐ No☐ Unknown ☐
4.	**Event Identification and Description:**	
	(Check applicable box) ☐ Damage or destruction of a Facility ☐ Physical Threat to a Facility ☐ Physical Threat to a control center ☐ BES Emergency: ☐ public appeal for load reduction ☐ system-wide voltage reduction ☐ manual firm load shedding ☐ automatic firm load shedding ☐ Voltage deviation on a Facility ☐ IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only) ☐ Loss of firm load ☐ System separation ☐ Generation loss ☐ Complete loss of off-site power to a nuclear generating plant (grid supply) ☐ Transmission loss ☐ unplanned control center evacuation ☐ Complete loss of voice communication capability ☐ Complete loss of monitoring capability	Written description (optional):

Guideline and Technical Basis

Distribution Provider Applicability Discussion

The DSR SDT has included Distribution Providers (DP) as an applicable entity under this standard. The team realizes that not all DPs will own BES Facilities and will not meet the "Threshold for Reporting" for any event listed in Attachment 1. These DPs will not have any reports to submit under Requirement R2. However, these DPs will be responsible for meeting Requirements R1 and R3. The DSR SDT does not intend for these entities to have a detailed Operating Plan to address events that are not applicable to them. In this instance, the DSR SDT intends for the DP to have a very simple Operating Plan that includes a statement that there are no applicable events in Attachment 1 (to meet R1) and that the DP will review the list of events in Attachment 1 each year (to meet R3). The team does not think this will be a burden on any entity as the development and annual validation of the Operating Plan should not take more that 30 minutes on an annual basis. If a DP discovers applicable events during the annual review, it is expected that the DP will develop a more detailed Operating Plan to comply with the requirements of the standard.

Multiple Reports for a Single Organization

For entities that have multiple registrations, the DSR SDT intends that these entities will only have to submit one report for any individual event. For example, if an entity is registered as a Reliability Coordinator, Balancing Authority and Transmission Operator, the entity would only submit one report for a particular event rather submitting three reports as each individual registered entity.

Summary of Key Concepts

The DSR SDT identified the following principles to assist them in developing the standard:

- Develop a single form to report disturbances and events that threaten the reliability of the Bulk Electric System
- Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements
- Establish clear criteria for reporting
- Establish consistent reporting timelines
- Provide clarity around who will receive the information and how it will be used

During the development of concepts, the DSR SDT considered the FERC directive to "further define sabotage". There was concern among stakeholders that a definition may be ambiguous and subject to interpretation. Consequently, the DSR SDT decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was sabotage or vandalism without the intervention of law enforcement. The DSR SDT felt that attempting to define sabotage would result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard. The events listed in EOP-004 Attachment 1 were developed to provide guidance for reporting both actual events as well as

events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

The types of events that are required to be reported are contained within EOP-004 Attachment 1. The DSR SDT has coordinated with the NERC Events Analysis Working Group to develop the list of events that are to be reported under this standard. EOP-004 Attachment 1 pertains to those actions or events that have impacted the Bulk Electric System. These events were previously reported under EOP-004-1, CIP-001-1 or the Department of Energy form OE-417. EOP-004 Attachment 1 covers similar items that may have had an impact on the Bulk Electric System or has the potential to have an impact and should be reported.

The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in EOP-004 Attachment 1. Real-time communication is achieved is covered in other standards. The proposed standard deals exclusively with after-the-fact reporting.

Data Gathering

The requirements of EOP-004-1 require that entities "promptly analyze Bulk Electric System disturbances on its system or facilities" (Requirement R2). The requirements of EOP-004-2 specify that certain types of events are to be reported but do not include provisions to analyze events. Events reported under EOP-004-2 may trigger further scrutiny by the ERO Events Analysis Program. If warranted, the Events Analysis Program personnel may request that more data for certain events be provided by the reporting entity or other entities that may have experienced the event. Entities are encouraged to become familiar with the Events Analysis Program and the NERC Rules of Procedure to learn more about with the expectations of the program.

Law Enforcement Reporting

The reliability objective of EOP-004-2 is to improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement enables and supports reliability principles such as protection of Bulk Electric System from malicious physical ~~or cyber~~ attack. ~~The Standard is intended to reduce the risk of Cascading events.~~ The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.

Stakeholders in the Reporting Process

- Industry
- NERC (ERO), Regional Entity
- FERC
- DOE

- NRC
- DHS – Federal
- Homeland Security- State
- State Regulators
- Local Law Enforcement
- State or Provincial Law Enforcement
- FBI
- Royal Canadian Mounted Police (RCMP)

The above stakeholders have an interest in the timely notification, communication and response to an incident at a Facility. The stakeholders have various levels of accountability and have a vested interest in the protection and response to ensure the reliability of the BES.

Present expectations of the industry under CIP-001-1a:

It has been the understanding by industry participants that an occurrence of sabotage has to be reported to the FBI. The FBI has the jurisdictional requirements to investigate acts of sabotage and terrorism. The CIP-001-1-1a standard requires a liaison relationship on behalf of the industry and the FBI or RCMP. These requirements, under the standard, of the industry have not been clear and have lead to misunderstandings and confusion in the industry as to how to demonstrate that the liaison is in place and effective. As an example of proof of compliance with Requirement R4, Responsible Entities have asked FBI Office personnel to provide, on FBI letterhead, confirmation of the existence of a working relationship to report acts of sabotage, the number of years the liaison relationship has been in existence, and the validity of the telephone numbers for the FBI.

Coordination of Local and State Law Enforcement Agencies with the FBI

The Joint Terrorism Task Force (JTTF) came into being with the first task force being established in 1980. JTTFs are small cells of highly trained, locally based, committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. The JTTF is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. Coordination and communications largely through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs. This information flow can be most beneficial to the industry in analytical intelligence, incident response and investigation. Historically, the most immediate response to an industry incident has been local and state law enforcement agencies to suspected vandalism and criminal damages at industry facilities. Relying upon the JTTF coordination between local, state and FBI law enforcement would be beneficial to effective communications and the appropriate level of investigative response.

Coordination of Local and Provincial Law Enforcement Agencies with the RCMP

A similar law enforcement coordination hierarchy exists in Canada. Local and Provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. The Provincial

law enforcement agency has a reporting relationship with the Royal Canadian Mounted Police (RCMP).

A Reporting Process Solution – EOP-004

A proposal discussed with the FBI, FERC Staff, NERC Standards Project Coordinator and the SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Reportable Events). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial or local level law enforcement agency. The state or provincial or local level law enforcement agency will coordinate with law enforcement with jurisdiction to investigate. If the state or provincial or local level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial or local level law enforcement agency will notify and coordinate with the FBI or the RCMP.

Example of Reporting Process including Law Enforcement

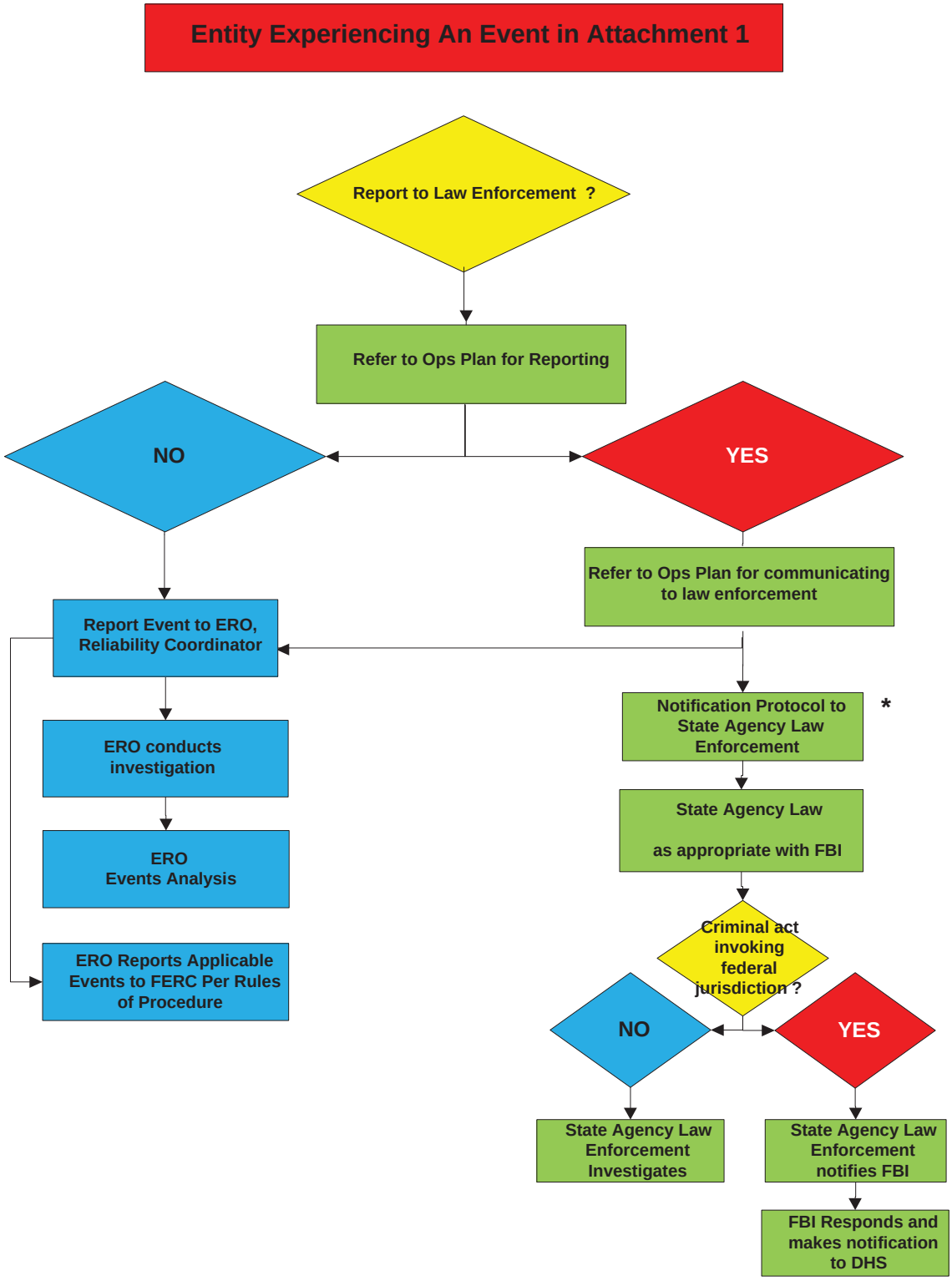

* Canadian entities will follow law enforcement protocols applicable in their jurisdictions

Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01) - Reporting Concepts

Introduction

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and has developed updated standards based on the SAR.

The standards listed under the SAR are:

- CIP-001 — Sabotage Reporting
- EOP-004 — Disturbance Reporting

The changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. EOP-002-Capacity and Energy Emergencies). These standards deal exclusively with after-the-fact reporting.

The DSR SDT has consolidated disturbance and sabotage event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts and Assumptions:

The Standard:

- Requires reporting of "events" that impact or may impact the reliability of the Bulk Electric System
- Provides clear criteria for reporting
- Includes consistent reporting timelines
- Identifies appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- Provides clarity around of who will receive the information

Discussion of Disturbance Reporting

Disturbance reporting requirements existed in the previous version of EOP-004. The current approved definition of Disturbance from the NERC Glossary of Terms is:

1. An unplanned event that produces an abnormal system condition.
2. Any perturbation to the electric system.
3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.

Disturbance reporting requirements and criteria were in the previous EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and developed the list of events that are to be reported under this standard (EOP-004 Attachment 1).

Discussion of Event Reporting
There are situations worthy of reporting because they have the potential to impact reliability.

Event reporting facilitates industry awareness, which allows potentially impacted parties to prepare for and possibly mitigate any associated reliability risk. It also provides the raw material, in the case of certain potential reliability threats, to see emerging patterns.

Examples of such events include:

- Bolts removed from transmission line structures
- Train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center)
- Destruction of Bulk Electric System equipment

What about sabotage?
One thing became clear in the DSR SDT's discussion concerning sabotage: everyone has a different definition. The current standard CIP-001 elicited the following response from FERC in FERC Order 693, paragraph 471 which states in part: *". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."*

Often, the underlying reason for an event is unknown or cannot be confirmed. The DSR SDT believes that by reporting material risks to the Bulk Electric System using the event categorization in this standard, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.

Certain types of events should be reported to NERC, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and/or Provincial or local law enforcement. Other types of events may have different reporting requirements. For example, an event that is related to copper theft may only need to be reported to the local law enforcement authorities.

Potential Uses of Reportable Information
Event analysis, correlation of data, and trend identification are a few potential uses for the information reported under this standard. The standard requires Functional entities to report the incidents and provide known information at the time of the report. Further data gathering necessary for event analysis is provided for under the Events Analysis Program and the NERC Rules of Procedure. Other entities (e.g. – NERC, Law Enforcement, etc) will be responsible for performing the analyses. The NERC Rules of Procedure (section 800) provide an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for

reliability. Jurisdictional agencies (which may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE) have other duties and responsibilities.

Collection of Reportable Information or "One stop shopping"

The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT has updated the listing of reportable events in EOP-004 Attachment 1 based on discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences still exist.

The reporting required by this standard is intended to meet the uses and purposes of NERC. The DSR SDT recognizes that other requirements for reporting exist (e.g., DOE-417 reporting), which may duplicate or overlap the information required by NERC. To the extent that other reporting is required, the DSR SDT envisions that duplicate entry of information should not be necessary, and the submission of the alternate report will be acceptable to NERC so long as all information required by NERC is submitted. For example, if the NERC Report duplicates information from the DOE form, the DOE report may be sent to the NERC in lieu of entering that information on the NERC report.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2009-01 Disturbance and Sabotage Reporting

Implementation Plan for EOP-004-2 – Event Reporting

Approvals Required
EOP-004-2 – Event Reporting

Prerequisite Approvals
None

Revisions to Glossary Terms
None

Applicable Entities
Reliability Coordinator
Balancing Authority
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Distribution Provider

Conforming Changes to Other Standards
None

Effective Dates
In those jurisdictions where regulatory approval is required, this standard shall become effective on the first day of the first calendar quarter that is six months after applicable regulatory approval or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Retirements

EOP-004-1 – Disturbance Reporting and CIP-001-2a – Sabotage Reporting should be retired at midnight of the day immediately prior to the Effective Date of EOP-004-2 in the particular jurisdiction in which the new standard is becoming effective.

Project 2009-01 Disturbance and Sabotage Reporting Mapping Document

Translation of CIP-002-2a – Sabotage Reporting and EOP-004-1 – Disturbance Reporting into EOP-004-2 – Event Reporting

Standard: CIP-001-2a – Sabotage Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Event Reporting**
R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.	Moved into EOP-004-2, R1	R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the regional entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* The specific list of events shown in Attachment 1 provides the Responsible Entity with clarity of what is required to be reported under this standard.

Standard: CIP-001-2a – Sabotage Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Event Reporting**
R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	Moved into EOP-004-2, R1 and R2.	R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the regional entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* R2. Each Responsible Entity shall implement its event reporting Operating Plan within 24 hours of meeting an event type threshold for reporting. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]* These requirements specify that the Responsible Entity must have an Operating Plan for reporting events listed in Attachment 1 to the necessary parties, including law enforcement. NERC Situational Awareness has an operating protocol to forward all event reports (for events that occur within the United States) to FERC.

Standard: CIP-001-2a – Sabotage Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Event Reporting**
R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.	Moved into EOP-004-2, R1	R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the regional entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* This requirement specifies that the Responsible Entity must have an Operating Plan for reporting events listed in Attachment 1 to the necessary parties, including law enforcement.
R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.	Moved into EOP-004-2, R1	R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the regional entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority). *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* These requirements specify that the Responsible Entity must have an Operating Plan for reporting events listed in Attachment 1 to the necessary parties, including law enforcement.

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Event Reporting**
R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.	Retire this fill-in-the-blank requirement. Replace with new reporting and analysis procedure developed by NERC EAWG.	The requirements of EOP-004-2 specify that an entity must report certain types of events. The NERC EAWG has developed continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure, Section 800.
R2. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.	The NERC Events Analysis Process	The requirements of EOP-004-2 specify that an entity must report certain types of events. The NERC EAWG has developed continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure, Section 800.
R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.	Translated into EOP-004-2, R2	R2. Each Responsible Entity shall implement its event reporting Operating Plan within 24 hours of meeting an event type threshold for reporting. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]* The requirements of EOP-004-2 specify that an entity must report certain types of events.

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Event Reporting**
R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until sometime after they occur shall be reported within 24 hours of being recognized.	Translated into EOP-004-2, R2	R2. Each Responsible Entity shall implement its event reporting Operating Plan within 24 hours of meeting an event type threshold for reporting. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]* The requirements of EOP-004-2 specify that an entity must report certain types of events.
R3.2. Applicable reporting forms are provided in Attachments 022-1 and 022-2.	Retire – informational statement	

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Event Reporting**
R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.	Retire as a requirement. Added as a "Note" to EOP-004-Attachment1-Events Table	NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report. In such cases, the affected Responsible Entity shall notify parties per Requirement R2 and provide as much information as is available at the time of the notification. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net or Voice: 404-446-9780.

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Event Reporting**
R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.	Retire this fill-in-the-blank requirement.	The requirements of EOP-004-2 specify that an entity must report certain types of events. The NERC EAWG has developed continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure, Section 800.

Standard: EOP-004-1 – Disturbance Reporting		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Proposed Language in EOP-004-2 - Event Reporting**
R4. When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.	Retire this fill-in-the-blank requirement.	The requirements of EOP-004-2 specify that an entity must report certain types of events. The NERC EAWG has developed continent wide reporting and analysis guidelines applicable under the NERC Rules of Procedure, Section 800.

Project 2009-01 Disturbance and Sabotage Reporting Consideration of Issues and Directives

Project 2009-01 Disturbance and Sabotage Reporting		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
"What is meant by: "establish contact with the FBI"? Is a phone number adequate? Many entities which call the FBI are referred back to the local authority. The AOT noted that on the FBI website it states to contact the local authorities. Is this a question for Homeland Security to deal with for us?" Establish communications contacts, as applicable with local FBI and RCMP officials. Some entities are very remote and the sheriff is the only local authority does the FBI still need to be contacted? Registered Entities have sabotage reporting processes and procedures in place but not all personnel has been trained.	CIP-001-1 NERC Audit Observation Team	The DSR SDT has been in contact with FBI staff and developed a notification flow chart for law enforcement as it pertains to EOP-004. The "Background" section of the standard outlines the reporting hierarchy that exists between local, state, provincial and federal law enforcement. The entity experiencing an event should notify the appropriate state or provincial law enforcement agency that will then coordinate with local law enforcement for investigation. These local, state and provincial agencies will coordinate with higher levels of law enforcement or other governmental agencies.

Question: How do you “and make the operator aware”	CIP-001-1 NERC Audit Observation Team	This has been removed from the standard. Requirement R1 requires that the entity has an Operating Plan for applicable events listed in Attachment 1.
How does this standard pertain to Load Serving Entities, LSE's.	CIP-001-1 NERC Audit Observation Team	LSE has been removed as an applicable entity as there are no applicable events.
Order No. 693 at Paragraph 469. We direct the ERO to explore ways to address these concerns – including central coordination of sabotage reports and a uniform reporting format – in developing modifications to the Reliability Standard with the appropriate governmental agencies that have levied the reporting requirements.	CIP-001-1; Order 693 at P 469	See “Background” section of the standard as well as the “Guidelines and Technical Basis” section.

"Define "sabotage" and provide guidance on triggering events that would cause an entity to report an event. Order No. 693 at Paragraph 461. Several commenters agree with the Commission's concern that the term "sabotage" should be defined. For the reasons stated in the NOPR, we direct that the ERO further define the term and provide guidance on triggering events that would cause an entity to report an event. However, we disagree with those commenters that suggest the term "sabotage" is so vague as to justify a delay in approval or the application of monetary penalties. As explained in the NOPR, we believe that the term sabotage is commonly understood and that common understanding should suffice in most instances.	CIP-001-1; Order 693 at P 461	The DSR SDT has not proposed a definition for inclusion in the NERC Glossary because it is impractical to define every event that should be reported without listing them in the definition. Attachment 1 is the de facto definition of "event". The DSR SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that without the intervention of law enforcement after the fact, it was almost impossible to determine if an act or event was that of sabotage or merely vandalism. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.
Order No. 693 at Paragraph 470. The ERO should consider suggestions raised by commenters such as FirstEnergy and Xcel to define the specified period for reporting an incident beginning from when an event is discovered or suspected to be sabotage, and APPA's concerns regarding events at unstaffed or remote facilities, and triggering events occurring outside staffed hours at small entities.	CIP-001-1; Order 693 at P 470	Attachment 1 defines the events which are to be reported under this standard. The required reporting is within 24 hours "of recognition of the event."

Order No. 693 at Paragraph 461. Modify CIP-001-1 1 to require an applicable entity to contact appropriate governmental authorities in the event of sabotage within a specific period of time, even if it is a preliminary report. Further, in the interim while the matter is being addressed by the Reliability Standards development process, we direct the ERO to provide advice to entities that have concerns about the reporting of particular circumstances as they arise.	CIP-001-1; Order 693 at P 461	Per Requirement R1, the entity is to develop an Operating Plan which includes event reporting to law enforcement and governmental agencies. The DSR SDT has been in contact with NERC Situational Awareness and has been informed that all event reports received by NERC are being forwarded to FERC.

Consider the need for wider application of the standard. Consider whether separate, less burdensome requirements for smaller entities may be appropriate. Order No. 693 at Paragraph 458. The Commission acknowledges the concerns of the commenters about the applicability of CIP-001-1 to small entities and has addressed the concerns of small entities generally earlier in this Final Rule. Our approval of the ERO Compliance Registry criteria to determine which users, owners and operators are responsible for compliance addresses the concerns of APPA and others. Order No. 693 at Paragraph 459. However, the Commission believes that there are specific reasons for applying this Reliability Standard to such entities, as discussed in the NOPR. APPA indicates that some small LSEs do not own or operate "hard assets" that are normally thought of as "at risk" to sabotage. The Commission is concerned that, an adversary might determine that a small LSE is the appropriate target when the adversary aims at a particular population or facility. Or an adversary may target a small user, owner or operator because it may have similar equipment or protections as a larger facility, that is, the adversary may use an attack against a smaller facility as a training "exercise." {continued below}	CIP-001-1; Order 693 at PP 458-60	Attachment 1 defines the events which are to be reported under this standard. The applicable entities are also identified for each type of event. Each event is to be reported within 24 hours of recognition of the event.

The knowledge of sabotage events that occur at any facility (including small facilities) may be helpful to those facilities that are traditionally considered to be the primary targets of adversaries as well as to all members of the electric sector, the law enforcement community and other critical infrastructures. Order No. 693 at Paragraph 460. For these reasons, the Commission remains concerned that a wider application of CIP-001-1 may be appropriate for Bulk Power System reliability. Balancing these concerns with our earlier discussion of the applicability of Reliability Standards to smaller entities, we will not direct the ERO to make any specific modification to CIP-001-1 to address applicability. However, we direct the ERO, as part of its Work Plan, to consider in the Reliability Standards development process, possible revisions to CIP-001-1 that address our concerns. Regarding the need for wider application of the Reliability Standard. Further, when addressing such applicability issues, the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate to address these concerns.		

Order No. 693 at Paragraph 466. The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures. At this time, the commission does not specify a review period as suggested by FirstEnergy and MRO and, rather, believes that the appropriate period should be determined through the ERO's Reliability Standards development process. However, the Commission directs that the ERO begin this process by considering a staggered schedule of annual testing of the procedures with modifications made when warranted formal review of the procedures every two or three years.	CIP-001-1; Order 693 at P 466	The standard is responsive this directive with the following language in Requirement R3: R3. Each Responsible Entity shall validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]* The DSR SDT envisions that this will include verification that contact information contained in the Operating Plan is correct. As an example, the annual validation could include calling others as defined in the Responsibility Entity's Operating Plan to verify that their contact information is correct and current. If any discrepancies are noted, the Operating Plan would be updated.

Consider FirstEnergy's suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality. Order No. 693 at Paragraph 451. A number of commenters agree with the Commission's concern that the term sabotage" needs to be better defined and guidance provided on the triggering events that would cause an entity to report an event. FirstEnergy states that this definition should differentiate between cyber and physical sabotage and should exclude unintentional operator error. It advocates a threshold of materiality to exclude acts that do not threaten to reduce the ability to provide service or compromise safety and security. SoCal Edison states that clarification regarding the meaning of sabotage and the triggering event for reporting would be helpful and prevent over reporting.	CIP-001-1; Order 693 at P 451, 467-68	This is addressed in Attachment 1. There are specific event types for physical security with report submittal requirements. Cyber security is addressed in the CIP version 5 standards.
471. As explained in the NOPR, while the Commission has identified concerns regarding CIP-001-1, we believe that the proposal serves an important purpose in ensuring that operating entities properly respond to sabotage events to minimize the adverse impact on the Bulk-Power System. Accordingly, the Commission approves Reliability Standard CIP-001-1 as mandatory and enforceable. In addition, pursuant to section 215(d)(5) of the FPA and § 39.5(f) of our regulations, the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process:... (2) specify baseline requirements regarding what issues should be addressed in the procedures for recognizing sabotage events and making personnel aware of such events;	CIP-001-1; Order 693 at P 471	This is addressed in Requirement R1 and Attachment 1. There are specific event types for physical security report submittal requirements. Cyber security is addressed in the CIP version 5 standards.

"Include a requirement to report a sabotage event to the proper government authorities. Develop the language to specifically implement this directive. Order No. 693 at Paragraph 467. CIP-001-1, Requirement R4, requires that each applicable entity establish communications contacts, as applicable, with the local FBI or Royal Canadian Mounted Police officials and develop reporting procedures as appropriate to its circumstances. The Commission in the NOPR expressed concern that the Reliability Standard does not require an applicable entity to actually contact the appropriate governmental or regulatory body in the event of sabotage. Therefore, the Commission proposed that NERC modify the Reliability Standard to require an applicable entity to "contact appropriate federal authorities, such as the Department of Homeland Security, in the event of sabotage within a specified period of time." Order No. 693 at Paragraph 468. As mentioned above, NERC and others object to the wording of the proposed directive as overly prescriptive and note that the reference to "appropriate federal authorities" fails to recognize the international application of the Reliability Standard. The example of the Department of Homeland Security as an "appropriate federal authority" was not intended to be an exclusive designation. Nonetheless, the Commission agrees that a reference to "federal authorities" could create confusion. Accordingly, we modify the direction in the NOPR and now direct the ERO to address our underlying concern regarding mandatory reporting of a sabotage event. The ERO's Reliability Standards development process should develop the language to implement this directive."		See "Guidelines and Technical Basis" section of Standard. "A proposal discussed with FBI, FERC Staff, NERC Standards Project Coordinator and SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Event EOP-004-2). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial level law enforcement agency. The state or provincial level law enforcement agency will coordinate with local law enforcement to investigate. If the state or provincial level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial level law enforcement agency will notify and coordinate with the FBI or the RCMP." At present NERC Situational Awareness staff forwards applicable event reports to FERC. This only includes reports for events that are subject to FERC jurisdiction (i.e. – US entities).

On March 4, 2008, NERC submitted a compliance filing in response to a December 20, 2007 Order, in which the Commission reversed a NERC decision to register three retail power marketers to comply with Reliability Standards applicable to load serving entities (LSEs) and directed NERC to submit a plan describing how it would address a possible "reliability gap" that NERC asserted would result if the LSEs were not registered. Compliance Filing of NERC in Response to December 20, 2007 Order in Docket Nos. RC07-4-000, RC07-6-000, RC07-7-000 (March 4, 2008). NERC's compliance filing included the following proposal for a short-term plan and a long-term plan to address the potential gap: · Short-term: Using a posting and open comment process, NERC will revise the registration criteria to define "Non-Asset Owning LSEs" as a subset of Load Serving Entities and will specify the reliability standards applicable to that subset. · Longer-term: NERC will determine the changes necessary to terms and requirements in reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers and process them through execution of the three-year Reliability Standards Development Plan. In this revised Reliability Standards Development Plan, NERC is commencing the implementation of its stated long-term plan to address the issues surrounding accountability for loads served by retail marketers/suppliers. The NERC Reliability Standards Development Procedure will be used to identify the changes necessary to terms and requirements in reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. Specifically, the following description has been incorporated into the scope for	CIP-001-1 and EOP-004 *Direct Energy Services, LLC, et al.*, 121 FERC ¶ 61,274 (2007)	The LSE is no longer an applicable entity, since no reportable event types in Attachment apply to an LSE. If an entity owns distribution assets, that entity will be registered as a Distribution Provider. Attachment 1 defines the timelines and events which are to be reported under this standard. The applicable entities are also identified for each type of event.

affected projects in this revised Reliability Standards Development Plan that includes a standard applicable to Load Serving Entities: Source: *Direct Energy Services, LLC, et al.*, 121 FERC ¶ 61,274 (2007) Issue: In FERC's December 20, 2007 Order, the Commission reversed NERC's Compliance Registry decisions with respect to three load serving entities in the ReliabilityFirst (RFC) footprint. The distinguishing feature of these three LSEs is that none own physical assets. Both NERC and RFC assert that there will be a "reliability gap" if retail marketers are not registered as LSEs. To avoid a possible gap, a consistent, uniform approach to ensure that appropriate Reliability Standards and associated requirements are applied to retail marketers must be followed. Each drafting team responsible for reliability standards that are applicable to LSEs is to review and change as necessary, requirements in the reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. For additional information see: · FERC's December 20, 2007 Order (http://www.nerc.com/files/LSE_decision_order.pdf) · NERC's March 4, 2008 (http://www.nerc.com/files/FinalFiledLSE3408.pdf), · FERC's April 4, 2008 Order (http://www.nerc.com/files/AcceptLSECompFiling-040408.pdf), and · NERC's July 31, 2008 (http://www.nerc.com/files/FinalFiled-compFiling-LSE-07312008.pdf) compliance filings to FERC on this subject.		

Object to multi-site requirement	Version 0 Team CIP-001-1	The Standard was revised for clarity. Attachment 1 defines the timelines and events which are to be reported under this standard. The applicable entities are also identified for each type of event.
Definition of sabotage required VRFs Team Adequate procedures will insure it is unlikely to lead to bulk electric system instability, separation, or cascading failures.	Version 0 Team CIP-001-1	No definition for sabotage was developed. The DSR SDT has not proposed a definition for inclusion in the NERC Glossary because it is impractical to define every event that should be reported without listing them in the definition. Attachment 1 is the de facto definition of "event". The DSR SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that without the intervention of law enforcement after the fact, it was almost impossible to determine if an act or event was that of sabotage or merely vandalism. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

Coordination and follow up on lessons learned from event analyses Consider adding to EOP-004 – Disturbance Reporting Proposed requirement: Regional Entities (REs) shall work together with Reliability Coordinators, Transmission Owners, and Generation Owners to develop an Event Analysis Process to prevent similar events from happening and follow up with the recommendations. This process shall be defined within the appropriate NERC Standard.	Events Analysis Team Reliability Issue	The DSR SDT envisions EOP-004-2 to be a reporting standard. Any follow up investigation or analysis falls under the purview of the NERC Events Analysis Program under the NERC Rules of Procedure.
Consider changes to R1 and R3.4 to standardize the disturbance reporting requirements (requirements for disturbance reporting need to be added to this standard). Regions currently have procedures, but not in the form of a standard. The drafting team will need to review regional requirements to determine reporting requirements for the North American standard.	Fill in the Blank Team	The DSR SDT envisions EOP-004-2 to be a continent-wide reporting standard. Any follow up investigation or analysis falls under the purview of the NERC Events Analysis Program under the NERC Rules of Procedure.
Can there be a violation without an event?	NERC Audit Observation Team	The DSR SDT envisions EOP-004-2 to be a continent-wide reporting standard. In the opinion of the DSR SDT, there cannot be a violation of Requirement R2 without an event. Since Requirement R1 calls for an Operating Plan, there can be a violation of R1 without an event.

Consider APPA's concern about generator operators and LSEs analyzing performance of their equipment and provide data and information on the equipment to assist others with analysis. Order No. 693 at Paragraph 607. APPA is concerned about the scope of Requirement R2 because, in its opinion, Requirement R2 appears to impose an open-ended obligation on entities such as generation operators and LSEs that may have neither the data nor the tools to promptly analyze disturbances that could have originated elsewhere. APPA proposes that Requirement R2 be modified to require affected entities to promptly begin analyses to ensure timely reporting to NERC and DOE. Order No. 693 at Paragraph 612. Requirement R2 of the Reliability Standard requires reliability coordinators, balancing authorities, transmission operators, generator operators and LSEs to promptly analyze disturbances on their system or facilities. APPA is concerned that generator operators and LSEs may be unable to promptly analyze disturbances, particularly those disturbances that may have originated outside of their systems, as they may have neither the data nor the tools required for such analysis. The Commission understands APPA's concern and believes that, at a minimum, generator operators and LSEs should analyze the performance of their equipment and provide the data and information on their equipment to assist others with their analyses. The Commission directs the ERO to consider this concern in future revisions to the Reliability Standard through the Reliability Standards development process.	EOP-004-1 Order 693 at PP 607, 612	The DSR SDT envisions EOP-004-2 to be a continent-wide reporting standard. Any follow up investigation or analysis falls under the purview of the NERC Events Analysis Program under the NERC Rules of Procedure.

FERC request for DOE-417s	EOP-004-1 Other	Per Requirement R1, the entity is to develop an Operating Plan which includes event reporting to law enforcement and governmental agencies. The DSR SDT has been in contact with NERC Situational Awareness and has been informed that all event reports received by NERC are being forwarded to FERC.

Violation Risk Factor and Violation Severity Level Assignments

Project 2009-01 – Disturbance and Sabotage Reporting

This document provides the drafting team's justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in

EOP-004-2 — Event Reporting

Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the ERO Sanction Guidelines.

Justification for Assignment of Violation Risk Factors in EOP-004-2

The Disturbance and Sabotage Reporting Standard Drafting Team applied the following NERC criteria when proposing VRFs for the requirements in EOP-004-2:

High Risk Requirement
A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement
A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

The SDT also considered consistency with the FERC Violation Risk Factor Guidelines for setting VRFs:[1]

Guideline (1) — Consistency with the Conclusions of the Final Blackout Report
The Commission seeks to ensure that Violation Risk Factors assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System.

In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:[2]

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) — Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement Violation Risk Factor assignments and the main Requirement Violation Risk Factor assignment.

[1] North American Electric Reliability Corp., 119 FERC ¶ 61,145, order on reh'g and compliance filing, 120 FERC ¶ 61,145 (2007) ("VRF Rehearing Order").
[2] Id. at footnote 15.

Guideline (3) — Consistency among Reliability Standards

The Commission expects the assignment of Violation Risk Factors corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) — Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular Violation Risk Factor level conforms to NERC's definition of that risk level.

Guideline (5) — Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

The following discussion addresses how the SDT considered FERC's VRF Guidelines 2 through 5. The team did not address Guideline 1 directly because of an apparent conflict between Guidelines 1 and 4. Whereas Guideline 1 identifies a list of topics that encompass nearly all topics within NERC's Reliability Standards and implies that these requirements should be assigned a "High" VRF, Guideline 4 directs assignment of VRFs based on the impact of a specific requirement to the reliability of the system. The SDT believes that Guideline 4 is reflective of the intent of VRFs in the first instance and therefore concentrated its approach on the reliability impact of the requirements.

VRF for EOP-004-2:

There are three requirements in EOP-004-2. Requirement R1 was assigned a Lower VRF while Requirements R2 and R3 were assigned a Medium VRF.

VRF for EOP-004-2, Requirements R1:

- FERC's Guideline 2 — Consistency within a Reliability Standard. The Requirement specifies which entities are required to have processes for recognition of events and for communicating with other entities. This Requirement is the only administrative Requirement within the Standard. The VRF is only applied at the Requirement level. FERC's Guideline 3 — Consistency among Reliability Standards. This requirement calls for an entity to have processes for recognition of events and communicating with other entities. This requirement is administrative in nature and deals with the means to report events after the fact. All event reporting requirements in Attachment 1 are for 24 hours after recognition that an event has occurred. The current approved VRFs for EOP-004-1 are

all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis portion is addressed through the NERC Rules of Procedure and the Events Analysis Program.

- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. Failure to have an event reporting Operating Plan is not likely to directly affect the electrical state or the capability of the bulk electric system. Development of the Operating Plan is a requirement that is administrative in nature and is in a planning time frame that, if violated, would not, under emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system.. Therefore this requirement was assigned a Lower VRF.
- FERC's Guideline 5 — Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R1 contains only one objective which is to have an Operating Plan with two distinct processes. Since the requirement is to have an Operating Plan, only one VRF was assigned.

VRF for EOP-004-2, Requirement R2:

- FERC's Guideline 2 — Consistency within a Reliability Standard. This Requirement calls for the Responsible Entity to implements its Operating Plan and is assigned a Medium VRF. There is one other similar Requirement in this Standard which specify an annual validation of the information contained in the Operating Plan (R3). Both of these Requirements are assigned a Medium VRF.
- FERC's Guideline 3 — Consistency among Reliability Standards. EOP-004-2, Requirement R2 is a requirement for entities to report events using the process for recognition of events per Attachment 1. Failure to report events within 24 hours is not likely to "directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system." However, violation of a medium risk requirement should also be "unlikely to lead to bulk electric system instability, separation, or cascading failures…" Such an instance could occur if personnel do not report events. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. EOP-004-2, Requirement R2 mandates that Responsible Entities implement their Operating Plan. Bulk power system instability, separation, or cascading failures are not likely to occur due to a failure to notify another entity of the event failure, but there is a slight chance that it could occur. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 5 - Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R2 addresses a single objective and has a single VRF.

VRF for EOP-004-2, Requirement R3:

- FERC's Guideline 2 — Consistency within a Reliability Standard. This Requirement calls for the Responsible Entity to perform an annual validation of the information contained in the Operating Plan and is assigned a Medium VRF. There is one other similar Requirement in this Standard which specifies that the Responsible Entity implement its Operating Plan (R2).. Both of these Requirements is assigned a Medium VRF.
- FERC's Guideline 3 — Consistency among Reliability Standards. EOP-004-2, Requirement R3 is a requirement for entities to perform an annual validation of the information contained of the information in the Operating Plan. Failure to perform an annual validation of the information contained in the Operating Plan is not likely to "directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system." However, violation of a medium risk requirement should also be "unlikely to lead to bulk electric system instability, separation, or cascading failures…" Such an instance could occur if personnel do not perform an annual test of the Operating Plan and it is out of date or contains erroneous information. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 4 — Consistency with NERC's Definition of a VRF. EOP-004-2, Requirement R3 mandates that Responsible Entities perform an annual validation of the information contained of the information in the Operating Plan. Bulk power system instability, separation, or cascading failures are not likely to occur due to a failure to perform an annual test of the Operating Plan, but there is a slight chance that it could occur if the Operating Plan is out of date or contains erroneous information. Therefore, this requirement was assigned a Medium VRF.
- FERC's Guideline 5 - Treatment of Requirements that Co-mingle More Than One Objective. EOP-004-2, Requirement R3 addresses a single objective and has a single VRF.

Justification for Assignment of Violation Severity Levels for EOP-004-2:

In developing the VSLs for the EOP-004-2 standard, the SDT anticipated the evidence that would be reviewed during an audit, and developed its VSLs based on the noncompliance an auditor may find during a typical audit. The SDT based its assignment of VSLs on the following NERC criteria:

Lower	Moderate	High	Severe
Missing a minor element (or a small percentage) of the required performance The performance or product measured has significant value as it almost meets the full intent of the requirement.	Missing at least one significant element (or a moderate percentage) of the required performance. The performance or product measured still has significant value in meeting the intent of the requirement.	Missing more than one significant element (or is missing a high percentage) of the required performance or is missing a single vital component. The performance or product has limited value in meeting the intent of the requirement.	Missing most or all of the significant elements (or a significant percentage) of the required performance. The performance measured does not meet the intent of the requirement or the product delivered cannot be used in meeting the intent of the requirement.

FERC's VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in EOP-004-2 meet the FERC Guidelines for assessing VSLs:

Guideline 1: Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

> Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline 2: Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

> A violation of a "binary" type requirement must be a "Severe" VSL.
>
> Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline 3: Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline 4: Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

. . . unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VSLs for EOP-004-2 Requirements R1:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R1	Meets NERC's VSL guidelines. The requirement calls for the entity to have an Operating Plan and is binary in nature. The VSL is therefore set to "Severe".	The proposed requirement is a revision of CIP-001-1, R1-R4, and EOP-004-1, R2. The Requirement has no Parts and is binary in nature. The binary VSL does not lower the current level of Compliance.	The proposed VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed binary VSL uses the same terminology as used in the associated requirement, and is, therefore, consistent with the requirement.	The VSLs are based on a single violation and not cumulative violations.

VSLs for EOP-004-2 Requirement R2:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R2	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is a revision of EOP-004-1, R3. There is only a Severe VSL for that requirement. However, the reporting of events is based on timing intervals listed in EOP-004 Attachment 1. Based on the VSL Guidance, the DSR SDT developed four VSLs based on tardiness of the submittal of the report. If a report is not submitted, then the VSL is Severe. This maintains the current VSL.	The proposed VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSLs use the same terminology as used in the associated requirement, and are, therefore, consistent with the requirement.	The VSLs are based on a single violation and not cumulative violations.

VSLs for EOP-004-2 Requirement R3:

R#	Compliance with NERC's VSL Guidelines	Guideline 1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	Guideline 2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	Guideline 4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations
R3	Meets NERC's VSL guidelines. There is an incremental aspect to the violation and the VSLs follow the guidelines for incremental violations.	The proposed requirement is a new Requirement. The test of the Operating Plan is based on the calendar year. Based on the VSL Guidance, the DSR SDT developed four VSLs based on tardiness of the submittal of the report. If a test is not performed, then the VSL is Severe.	The proposed VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.	The proposed VSLs use the same terminology as used in the associated requirement, and are, therefore, consistent with the requirement.	The VSLs are based on a single violation and not cumulative violations.

A. Introduction

1. **Title:** **Sabotage Reporting**

2. **Number:** CIP-001-2a

3. **Purpose:** Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.

4. **Applicability**

   4.1. Reliability Coordinators.

   4.2. Balancing Authorities.

   4.3. Transmission Operators.

   4.4. Generator Operators.

   4.5. Load Serving Entities.

   4.6. Transmission Owners (only in ERCOT Region).

   4.7. Generator Owners (only in ERCOT Region).

5. **Effective Date:** ERCOT Regional Variance will be effective the first day of the first calendar quarter after applicable regulatory approval.

B. Requirements

R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.

R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

C. Measures

M1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement 1

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements 2 and 3.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to procedures, policies, a letter of understanding, communication records, or other equivalent evidence that will be used to confirm that it has established communications contacts with the applicable, local FBI or RCMP officials to communicate sabotage events (Requirement 4).

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organizations shall be responsible for compliance monitoring.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to verify compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Reliability Coordinator, Transmission Operator, Generator Operator, Distribution Provider, and Load Serving Entity shall have current, in-force documents available as evidence of compliance as specified in each of the Measures.

If an entity is found non-compliant the entity shall keep information related to the non-compliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

None.

2. Levels of Non-Compliance:

2.1. Level 1: There shall be a separate Level 1 non-compliance, for every one of the following requirements that is in violation:

2.1.1 Does not have procedures for the recognition of and for making its operating personnel aware of sabotage events (R1).

2.1.2 Does not have procedures or guidelines for the communication of information concerning sabotage events to appropriate parties in the Interconnection (R2).

2.1.3 Has not established communications contacts, as specified in R4.

2.2. **Level 2:** Not applicable.

2.3. **Level 3:** Has not provided its operating personnel with sabotage response procedures or guidelines (R3).

2.4. **Level 4:**.Not applicable.

E. ERCOT Interconnection-wide Regional Variance

Requirements

EA.1. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.

EA.2. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.

EA.3. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.

EA.4. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall establish communications contacts with local Federal Bureau of Investigation (FBI) officials and develop reporting procedures as appropriate to their circumstances.

Measures

M.A.1. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement EA1.

M.A.2. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements EA2 and EA3.

M.A.3. Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to, procedures, policies, a letter of understanding, communication records,

or other equivalent evidence that will be used to confirm that it has established communications contacts with the local FBI officials to communicate sabotage events (Requirement EA4).

Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

Regional Entity shall be responsible for compliance monitoring.

1.2. Data Retention

Each Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity shall have current, in-force documents available as evidence of compliance as specified in each of the Measures.

If an entity is found non-compliant the entity shall keep information related to the non-compliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Amended
1	April 4, 2007	Regulatory Approval — Effective Date	New
1a	February 16, 2010	Added Appendix 1 — Interpretation of R2 approved by the NERC Board of Trustees	Addition
1a	February 2, 2011	Interpretation of R2 approved by FERC on February 2, 2011	Same addition
	June 10, 2010	TRE regional ballot approved variance	By Texas RE
	August 24, 2010	Regional Variance Approved by Texas RE Board of Directors	
2a	February 16, 2011	Approved by NERC Board of Trustees	

2a	August 2, 2011	FERC Order issued approving Texas RE Regional Variance	

Appendix 1

Requirement Number and Text of Requirement
CIP-001-1: **R2**. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.
Question
Please clarify what is meant by the term, "appropriate parties." Moreover, who within the Interconnection hierarchy deems parties to be appropriate?
Response
The drafting team interprets the phrase "appropriate parties in the Interconnection" to refer collectively to entities with whom the reporting party has responsibilities and/or obligations for the communication of physical or cyber security event information. For example, reporting responsibilities result from NERC standards IRO-001 Reliability Coordination — Responsibilities and Authorities, COM-002-2 Communication and Coordination, and TOP-001 Reliability Responsibilities and Authorities, among others. Obligations to report could also result from agreements, processes, or procedures with other parties, such as may be found in operating agreements and interconnection agreements. The drafting team asserts that those entities to which communicating sabotage events is appropriate would be identified by the reporting entity and documented within the procedure required in CIP-001-1 Requirement R2. Regarding "who within the Interconnection hierarchy deems parties to be appropriate," the drafting team knows of no interconnection authority that has such a role.

A. Introduction

1. Title: **Disturbance Reporting**

2. Number: EOP-004-1

3. Purpose: Disturbances or unusual occurrences that jeopardize the operation of the Bulk Electric System, or result in system equipment damage or customer interruptions, need to be studied and understood to minimize the likelihood of similar events in the future.

4. Applicability

4.1. Reliability Coordinators.

4.2. Balancing Authorities.

4.3. Transmission Operators.

4.4. Generator Operators.

4.5. Load Serving Entities.

4.6. Regional Reliability Organizations.

5. Effective Date: January 1, 2007

B. Requirements

R1. Each Regional Reliability Organization shall establish and maintain a Regional reporting procedure to facilitate preparation of preliminary and final disturbance reports.

R2. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.

R3. A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.

R3.1. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.

R3.2. Applicable reporting forms are provided in Attachments 1-EOP-004 and 2-EOP-004.

R3.3. Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that

time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.

R3.4. If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.

R4. When a Bulk Electric System disturbance occurs, the Regional Reliability Organization shall make its representatives on the NERC Operating Committee and Disturbance Analysis Working Group available to the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load Serving Entity immediately affected by the disturbance for the purpose of providing any needed assistance in the investigation and to assist in the preparation of a final report.

R5. The Regional Reliability Organization shall track and review the status of all final report recommendations at least twice each year to ensure they are being acted upon in a timely manner. If any recommendation has not been acted on within two years, or if Regional Reliability Organization tracking and review indicates at any time that any recommendation is not being acted on with sufficient diligence, the Regional Reliability Organization shall notify the NERC Planning Committee and Operating Committee of the status of the recommendation(s) and the steps the Regional Reliability Organization has taken to accelerate implementation.

C. Measures

M1. The Regional Reliability Organization shall have and provide upon request as evidence, its current regional reporting procedure that is used to facilitate preparation of preliminary and final disturbance reports. (Requirement 1)

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, the preliminary report, computer printouts, operator logs, or other equivalent evidence that will be used to confirm that it prepared and delivered the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that has a reportable incident shall have and provide upon request evidence that could include, but is not limited to, operator logs, voice recordings or transcripts of voice recordings, electronic communications, or other equivalent evidence that will be used to confirm that it provided information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours. (Requirement 3.3)

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

NERC shall be responsible for compliance monitoring of the Regional Reliability Organizations.

Regional Reliability Organizations shall be responsible for compliance monitoring of Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load-serving Entities.

1.2. Compliance Monitoring and Reset Time Frame

One or more of the following methods will be used to assess compliance:

- Self-certification (Conducted annually with submission according to schedule.)
- Spot Check Audits (Conducted anytime with up to 30 days notice given to prepare.)
- Periodic Audit (Conducted once every three years according to schedule.)
- Triggered Investigations (Notification of an investigation must be made within 60 days of an event or complaint of noncompliance. The entity will have up to 30 days to prepare for the investigation. An entity may request an extension of the preparation period and the extension will be considered by the Compliance Monitor on a case-by-case basis.)

The Performance-Reset Period shall be 12 months from the last finding of non-compliance.

1.3. Data Retention

Each Regional Reliability Organization shall have its current, in-force, regional reporting procedure as evidence of compliance. (Measure 1)

Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and/or Load Serving Entity that is either involved in a Bulk Electric System disturbance or has a reportable incident shall keep data related to the incident for a year from the event or for the duration of any regional investigation, whichever is longer. (Measures 2 through 4)

If an entity is found non-compliant the entity shall keep information related to the noncompliance until found compliant or for two years plus the current year, whichever is longer.

Evidence used as part of a triggered investigation shall be retained by the entity being investigated for one year from the date that the investigation is closed, as determined by the Compliance Monitor,

The Compliance Monitor shall keep the last periodic audit report and all requested and submitted subsequent compliance records.

1.4. Additional Compliance Information

See Attachments:

- EOP-004 Disturbance Reporting Form
- Table 1 EOP-004

2. Levels of Non-Compliance for a Regional Reliability Organization

2.1. Level 1: Not applicable.

2.2. Level 2: Not applicable.

2.3. Level 3: Not applicable.

2.4. Level 4: No current procedure to facilitate preparation of preliminary and final disturbance reports as specified in R1.

3. Levels of Non-Compliance for a Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load- Serving Entity:

3.1. Level 1: There shall be a level one non-compliance if any of the following conditions exist:

3.1.1 Failed to prepare and deliver the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports to NERC within 24 hours of its recognition as specified in Requirement 3.1

3.1.2 Failed to provide disturbance information verbally as time permitted, when system conditions precluded the preparation of a report in 24 hours as specified in R3.3

3.1.3 Failed to prepare a final report within 60 days as specified in R3.4

3.2. Level 2: Not applicable.

3.3. Level 3: Not applicable

3.4. Level 4: Not applicable.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
0	May 23, 2005	Fixed reference to attachments 1-EOP-004-0 and 2-EOP-004-0, Changed chart title 1-FAC-004-0 to 1-EOP-004-0, Fixed title of Table 1 to read 1-EOP-004-0, and fixed font.	Errata
0	July 6, 2005	Fixed email in Attachment 1-EOP-004-0 from info@nerc.com to esisac@nerc.com.	Errata

0	July 26, 2005	Fixed Header on page 8 to read EOP-004-0	Errata
0	August 8, 2005	Removed “Proposed” from Effective Date	Errata
1	November 1, 2006	Adopted by Board of Trustees	Revised

Attachment 1-EOP-004
NERC Disturbance Report Form

Introduction

These disturbance reporting requirements apply to all Reliability Coordinators, Balancing Authorities, Transmission Operators, Generator Operators, and Load Serving Entities, and provide a common basis for all NERC disturbance reporting. The entity on whose system a reportable disturbance occurs shall notify NERC and its Regional Reliability Organization of the disturbance using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. Reports can be sent to NERC via email (esisac@nerc.com) by facsimile (609-452-9550) using the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report forms. If a disturbance is to be reported to the U.S. Department of Energy also, the responding entity may use the DOE reporting form when reporting to NERC. Note: All Emergency Incident and Disturbance Reports (Schedules 1 and 2) sent to DOE shall be simultaneously sent to NERC, preferably electronically at esisac@nerc.com.

The NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Reports are to be made for any of the following events:

1. The loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations. Generally, a disturbance report will be required if the event results in actions such as:
   a. Modification of operating procedures.
   b. Modification of equipment (e.g. control systems or special protection systems) to prevent reoccurrence of the event.
   c. Identification of valuable lessons learned.
   d. Identification of non-compliance with NERC standards or policies.
   e. Identification of a disturbance that is beyond recognized criteria, i.e. three-phase fault with breaker failure, etc.
   f. Frequency or voltage going below the under-frequency or under-voltage load shed points.
2. The occurrence of an interconnected system separation or system islanding or both.
3. Loss of generation by a Generator Operator, Balancing Authority, or Load-Serving Entity — 2,000 MW or more in the Eastern Interconnection or Western Interconnection and 1,000 MW or more in the ERCOT Interconnection.
4. Equipment failures/system operational actions which result in the loss of firm system demands for more than 15 minutes, as described below:
   a. Entities with a previous year recorded peak demand of more than 3,000 MW are required to report all such losses of firm demands totaling more than 300 MW.
   b. All other entities are required to report all such losses of firm demands totaling more than 200 MW or 50% of the total customers being supplied immediately prior to the incident, whichever is less.
5. Firm load shedding of 100 MW or more to maintain the continuity of the bulk electric system.

6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in:
   a. Sustained voltage excursions equal to or greater than ±10%, or
   b. Major damage to power system components, or
   c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance as defined by steps 1 through 5 above.
7. An Interconnection Reliability Operating Limit (IROL) violation as required in reliability standard TOP-007.
8. Any event that the Operating Committee requests to be submitted to Disturbance Analysis Working Group (DAWG) for review because of the nature of the disturbance and the insight and lessons the electricity supply and delivery industry could learn.

NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report

☐ Check here if this is an Interconnection Reliability Operating Limit (IROL) violation report.

1.	Organization filing report.		
2.	Name of person filing report.		
3.	Telephone number.		
4.	Date and time of disturbance. Date:(mm/dd/yy) Time/Zone:		
5.	Did the disturbance originate in your system?	Yes ☐ No ☐	
6.	Describe disturbance including: cause, equipment damage, critical services interrupted, system separation, key scheduled and actual flows prior to disturbance and in the case of a disturbance involving a special protection or remedial action scheme, what action is being taken to prevent recurrence.		
7.	Generation tripped. MW Total List generation tripped		
8.	Frequency. Just prior to disturbance (Hz): Immediately after disturbance (Hz max.): Immediately after disturbance (Hz min.):		
9.	List transmission lines tripped (specify voltage level of each line).		
10.		FIRM	INTERRUPTIBLE
	Demand tripped (MW):		
	Number of affected Customers:		

	Demand lost (MW-Minutes):		
11.	Restoration time.	INITIAL	FINAL
	Transmission:		
	Generation:		
	Demand:		

Attachment 2-EOP-004
U.S. Department of Energy Disturbance Reporting Requirements

Introduction

The U.S. Department of Energy (DOE), under its relevant authorities, has established mandatory reporting requirements for electric emergency incidents and disturbances in the United States. DOE collects this information from the electric power industry on Form EIA-417 to meet its overall national security and Federal Energy Management Agency's Federal Response Plan (FRP) responsibilities. DOE will use the data from this form to obtain current information regarding emergency situations on U.S. electric energy supply systems. DOE's Energy Information Administration (EIA) will use the data for reporting on electric power emergency incidents and disturbances in monthly EIA reports. In addition, the data may be used to develop legislative recommendations, reports to the Congress and as a basis for DOE investigations following severe, prolonged, or repeated electric power reliability problems.

Every Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity must use this form to submit mandatory reports of electric power system incidents or disturbances to the DOE Operations Center, which operates on a 24-hour basis, seven days a week. All other entities operating electric systems have filing responsibilities to provide information to the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity when necessary for their reporting obligations and to file form EIA-417 in cases where these entities will not be involved. EIA requests that it be notified of those that plan to file jointly and of those electric entities that want to file separately.

Special reporting provisions exist for those electric utilities located within the United States, but for whom Reliability Coordinator oversight responsibilities are handled by electrical systems located across an international border. A foreign utility handling U.S. Balancing Authority responsibilities, may wish to file this information voluntarily to the DOE. Any U.S.-based utility in this international situation needs to inform DOE that these filings will come from a foreign-based electric system or file the required reports themselves.

Form EIA-417 must be submitted to the DOE Operations Center if any one of the following applies (see Table 1-EOP-004-0 — Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies):

1. Uncontrolled loss of 300 MW or more of firm system load for more than 15 minutes from a single incident.
2. Load shedding of 100 MW or more implemented under emergency operational policy.
3. System-wide voltage reductions of 3 percent or more.
4. Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the electric power system.
5. Actual or suspected physical attacks that could impact electric power system adequacy or reliability; or vandalism, which target components of any security system. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.

6. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.
7. Fuel supply emergencies that could impact electric power system adequacy or reliability.
8. Loss of electric service to more than 50,000 customers for one hour or more.
9. Complete operational failure or shut-down of the transmission and/or distribution electrical system.

The initial DOE Emergency Incident and Disturbance Report (form EIA-417 – Schedule 1) shall be submitted to the DOE Operations Center within 60 minutes of the time of the system disruption. Complete information may not be available at the time of the disruption. However, provide as much information as is known or suspected at the time of the initial filing. If the incident is having a critical impact on operations, a telephone notification to the DOE Operations Center (202-586-8100) is acceptable, pending submission of the completed form EIA-417. Electronic submission via an on-line web-based form is the preferred method of notification. However, electronic submission by facsimile or email is acceptable.

An updated form EIA-417 (Schedule 1 and 2) is due within 48 hours of the event to provide complete disruption information. Electronic submission via facsimile or email is the preferred method of notification. Detailed DOE Incident and Disturbance reporting requirements can be found at: http://www.eia.doe.gov/cneaf/electricity/page/form_417.html.

Table 1-EOP-004-0 Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Uncontrolled loss of Firm System Load	≥ 300 MW – 15 minutes or more	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
2	Load Shedding	≥ 100 MW under emergency operational policy	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
3	Voltage Reductions	3% or more – applied system-wide	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
4	Public Appeals	Emergency conditions to reduce demand	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
5	Physical sabotage, terrorism or vandalism	On physical security systems – suspected or real	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
6	Cyber sabotage, terrorism or vandalism	If the attempt is believed to have or did happen	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
7	Fuel supply emergencies	Fuel inventory or hydro storage levels ≤ 50% of normal	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
8	Loss of electric service	≥ 50,000 for 1 hour or more	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
9	Complete operation failure of electrical system	If isolated or interconnected electrical systems suffer total electrical system collapse	EIA – Sch-1 EIA – Sch-2	1 hour 48 hour
All DOE EIA-417 Schedule 1 reports are to be filed within 60-minutes after the start of an incident or disturbance All DOE EIA-417 Schedule 2 reports are to be filed within 48-hours after the start of an incident or disturbance				

All entities required to file a DOE EIA-417 report (Schedule 1 & 2) shall send a copy of these reports to NERC simultaneously, but no later than 24 hours after the start of the incident or disturbance.				
Incident No.	**Incident**	**Threshold**	**Report Required**	**Time**
1	Loss of major system component	Significantly affects integrity of interconnected system operations	NERC Prelim Final report	24 hour 60 day
2	Interconnected system separation or system islanding	Total system shutdown Partial shutdown, separation, or islanding	NERC Prelim Final report	24 hour 60 day
3	Loss of generation	≥ 2,000 – Eastern Interconnection ≥ 2,000 – Western Interconnection ≥ 1,000 – ERCOT Interconnection	NERC Prelim Final report	24 hour 60 day
4	Loss of firm load ≥15-minutes	Entities with peak demand ≥3,000: loss ≥300 MW All others ≥200MW or 50% of total demand	NERC Prelim Final report	24 hour 60 day
5	Firm load shedding	≥100 MW to maintain continuity of bulk system	NERC Prelim Final report	24 hour 60 day
6	System operation or operation actions resulting in:	• Voltage excursions ≥10% • Major damage to system components • Failure, degradation, or misoperation of SPS	NERC Prelim Final report	24 hour 60 day
7	IROL violation	Reliability standard TOP-007.	NERC Prelim Final report	72 hour 60 day
8	As requested by ORS Chairman	Due to nature of disturbance & usefulness to industry (lessons learned)	NERC Prelim Final report	24 hour 60 day
All NERC Operating Security Limit and Preliminary Disturbance reports will be filed within 24 hours after the start of the incident. If an entity must file a DOE EIA-417 report on an incident, which requires a NERC Preliminary report, the Entity may use the DOE EIA-417 form for both DOE and NERC reports.				
Any entity reporting a DOE or NERC incident or disturbance has the responsibility to also notify its Regional Reliability Organization.				

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-01 Disturbance and Sabotage Reporting

Recirculation Ballot and Non-Binding Poll Open Through 8 p.m. Friday, November 2, 2012

Now Available

A recirculation ballot of **EOP-004-2 – Event Reporting** and a non-binding poll of the associated VRFs/VSLs is open through **8 p.m. Eastern on Friday, November 2, 2012**

After considering stakeholder comments from the formal comment period and successive ballot that ended on September 27, 2012, the drafting team made no substantive changes to the Requirements of the standard, but did make a clarifying change to Requirement R2 concerning the 24-hour reporting obligation to provide flexibility for support staff to assist with after-the-fact reporting. In addition, the team provided clarification in the Guideline and Technical Basis concerning how the standard is intended to apply to Distribution Providers who do not own BES Facilities, and to clarify that entities registered for multiple functions will only need to submit a single report of an individual event.

Finally, in response to stakeholder comments, the drafting team has revised the VSLs for Requirement R1 to provide gradation in the VSL for failure to incorporate one or more event types in the entity's Operating Plan. **NOTE: Although the drafting team was not required to conduct an additional non-binding poll of the VSLs, they would like to gauge industry support for the VSLs as modified, and therefore, a non-binding poll of the VRFs and VSLs is being conducted in conjunction with the recirculation ballot.**

Instructions

In the recirculation ballot, votes are counted by exception. Only members of the ballot pool may cast a ballot; all ballot pool members may change their previously cast votes. A ballot pool member who failed to cast a ballot during the last ballot window may cast a ballot in the recirculation ballot window. If a ballot pool member does not participate in the recirculation ballot, that member's vote cast in the previous ballot will be carried over as that member's vote in the recirculation ballot.

Members of the ballot pools associated with this project may log in and submit their votes and opinions for the standard and VSL changes by clicking here.

Next Steps

The drafting team plans to submit EOP-004-2 to the Board of Trustees for adoption in November and then file the adopted standard with the appropriate regulatory authorities.

Background

The DSR SDT has developed EOP-004-2 to replace the current mandatory and enforceable EOP-004-1 and CIP-001-1a standards. The reporting obligations under EOP-004-2 serve to provide input to the NERC Events Analysis Program. Analysis of events is not required under the proposed standard and any analysis or investigation will fall under the Event Analysis Program under the NERC Rules of Procedure.

Additional information is available on the project page.

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Development Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd.NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2009-01 Disturbance and Sabotage Reporting

Recirculation Ballot and Non-Binding Poll Results

Now Available

A recirculation ballot of **EOP-004-2 – Event Reporting** and a non-binding poll of the associated VRFs/VSLs concluded on Monday, November 5, 2012.

Voting statistics for each ballot are listed below, and the Ballots Results page provides a link to the detailed results.

Approval	Non-binding Poll Results
Quorum: 85.14%	Quorum: 78.93%
Approval: 71.39%	Supportive Opinions: 71.04%

Next Steps
The standard will be presented to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Background
The DSR SDT has developed EOP-004-2 to replace the current mandatory and enforceable EOP-004-1 and CIP-001-2a standards. The reporting obligations under EOP-004-2 serve to provide input to the NERC Events Analysis Program. Analysis of events is not required under the proposed standard and any analysis or investigation will fall under the Event Analysis Program under the NERC Rules of Procedure.

Additional information is available on the project page.

Standards Process
The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Development Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd.NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2009-01 DSR Recirculation Ballot October 2012_in
Ballot Period:	10/24/2012 - 11/5/2012
Ballot Type:	Initial
Total # Votes:	361
Total Ballot Pool:	424
Quorum:	**85.14 % The Quorum has been reached**
Weighted Segment Vote:	71.39 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	104	1	57	0.704	24	0.296	9	14
2 - Segment 2.	11	0.8	4	0.4	4	0.4	2	1
3 - Segment 3.	108	1	58	0.674	28	0.326	8	14
4 - Segment 4.	37	1	22	0.759	7	0.241	3	5
5 - Segment 5.	91	1	53	0.757	17	0.243	6	15
6 - Segment 6.	53	1	30	0.789	8	0.211	5	10
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	8	0.7	6	0.6	1	0.1	0	1
9 - Segment 9.	4	0.3	2	0.2	1	0.1	0	1
10 - Segment 10.	8	0.6	4	0.4	2	0.2	0	2
Totals	**424**	**7.4**	**236**	**5.283**	**92**	**2.117**	**33**	**63**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	
1	American Electric Power	Paul B. Johnson		
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Negative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis		
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Grand River Dam Authority	James M Stafford	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon		
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Affirmative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Los Angeles Department of Water & Power	Ly M Le		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Affirmative	
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	Northeast Utilities	David Boguslawski	Abstain	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Negative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Negative	
1	Orlando Utilities Commission	Brad Chase	Abstain	
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn	Abstain	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	

1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Affirmative	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Negative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Larry G Akens	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Abstain	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Negative	
2	New York Independent System Operator	Gregory Campoli		
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Negative	
3	AEP	Michael E Deloach	Negative	
3	Alabama Power Company	Richard J. Mandes	Negative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse		
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	

3	City of Redding	Bill Hughes	Affirmative	
3	Clatskanie People's Utility District	Brian Fawcett		
3	Clearwater Power Co.	Dave Hagen	Negative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Abstain	
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Negative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	
3	Cowlitz County PUD	Russell A Noble	Negative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Negative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Negative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	
3	Gulf Power Company	Paul C Caldwell	Negative	
3	Hydro One Networks, Inc.	David Kiguel	Negative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker		
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Kootenai Electric Cooperative	Dave Kahly	Abstain	
3	Lakeland Electric	Norman D Harryhill		
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Negative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Negative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	Marilyn Brown	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Negative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Abstain	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller		
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	

3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern California Edison Co.	David B Coher		
3	Southern Maryland Electric Coop.	Mark R Jones		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	
3	Westar Energy	Bo Jones	Negative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Abstain	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Affirmative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Negative	
4	Detroit Edison Company	Daniel Herring	Negative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	North Carolina Electric Membership Corp.	Bob Beadle	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	
4	White River Electric Association Inc.	Frank L. Sampson	Abstain	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Abstain	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	

5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Negative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Affirmative	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Negative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	
5	Duke Energy	Dale Q Goodwine	Negative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Energy	Ellen Oswald		
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Exelon Nuclear	Michael Korchynsky	Abstain	
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Negative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero		
5	Indeck Energy Services, Inc.	Rex A Roehl		
5	JEA	John J Babik	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider		
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	

5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Siemens PTI	Edwin Cano		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	
5	Southern Company Generation	William D Shultz	Negative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Leonard Rentmeester	Abstain	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda L Powell	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak		
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Abstain	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II		

6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Pacific Northwest Generating Cooperative	Margaret Ryan	Negative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G. Dvorsky	Affirmative	
10	Midwest Reliability Organization	James D Burley		
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Non-binding Poll Results

Project 2009-01

Non-binding Poll Results	
Non-binding Poll Name:	Project 2009-01 Non-binding Poll DSR
Poll Period:	10/24/2012 - 11/5/2012
Total # Opinions:	311
Total Ballot Pool:	394
Summary Results:	78.93% of those who registered to participate provided an opinion for an abstention; 71.04% of those who provided an opinion indicated support for the VRFs and VSLs.

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	Comments
1	Ameren Services	Kirit Shah	Abstain	
1	American Electric Power	Paul B. Johnson		
1	American Transmission Company, LLC	Andrew Z Pusztai	Abstain	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Abstain	
1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Abstain	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	

1	Entergy Services, Inc.	Edward J Davis		
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Grand River Dam Authority	James M Stafford	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Abstain	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JEA	Ted Hobson	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon		
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Affirmative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Los Angeles Department of Water & Power	Ly M Le		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Abstain	
1	New York Power Authority	Arnold J. Schuff	Affirmative	
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	Northeast Utilities	David Boguslawski	Abstain	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Negative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis		
1	Orlando Utilities Commission	Brad Chase	Abstain	
1	PacifiCorp	Ryan Millard	Abstain	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	

1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Abstain	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Abstain	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Abstain	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Abstain	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Negative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Affirmative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young		
1	Tennessee Valley Authority	Larry G Akens	Abstain	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper		
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Abstain	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Abstain	
2	New York Independent System Operator	Gregory Campoli		
2	PJM Interconnection, L.L.C.	Tom Bowe	Abstain	
2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Negative	
3	Alabama Power Company	Richard J. Mandes		
3	Ameren Services	Mark Peters	Abstain	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	

3	Arkansas Electric Cooperative Corporation	Philip Huff	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Abstain	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse		
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	Clatskanie People's Utility District	Brian Fawcett		
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Abstain	
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Negative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Detroit Edison Company	Kent Kujala	Negative	
3	Dominion Resources Services	Michael F. Gildea		
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson		
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	
3	Gulf Power Company	Paul C Caldwell	Negative	
3	Hydro One Networks, Inc.	David Kiguel	Abstain	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker		
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Kootenai Electric Cooperative	Dave Kahly	Abstain	
3	Lakeland Electric	Norman D Harryhill		
3	Lincoln Electric System	Jason Fortik	Abstain	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	Manitoba Hydro	Greg C. Parent	Negative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Negative	

3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	Marilyn Brown	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Abstain	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Abstain	
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller		
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Abstain	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Abstain	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	Southern Maryland Electric Coop.	Mark R Jones		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L Donahey		
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Westar Energy	Bo Jones	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell		
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Abstain	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Affirmative	

4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Negative	
4	Detroit Edison Company	Daniel Herring	Negative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Abstain	
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Abstain	
4	Seattle City Light	Hao Li	Abstain	
4	South Mississippi Electric Power Association	Steven McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Abstain	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Abstain	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	

5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Negative	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Negative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	Duke Energy	Dale Q Goodwine	Negative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Energy	Ellen Oswald		
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Gainesville Regional Utilities	Karen C Alford		
5	Great River Energy	Preston L Walsh	Negative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero		
5	Indeck Energy Services, Inc.	Rex A Roehl		
5	JEA	John J Babik	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard		
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Abstain	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Abstain	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider		
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	

5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Negative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Abstain	
5	Platte River Power Authority	Roland Thiel	Abstain	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Sacramento Municipal Utility District	Bethany Hunter	Abstain	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Abstain	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Siemens PTI	Edwin Cano		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	
5	Southern Company Generation	William D Shultz	Negative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Tri-State G & T Association, Inc.	Barry Ingold		
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Xcel Energy, Inc.	Liam Noailles		
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Abstain	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Abstain	

6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Abstain	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Abstain	
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Abstain	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Abstain	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak		
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Abstain	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner	Affirmative	

8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
10	Midwest Reliability Organization	James D Burley		
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Abstain	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Exhibit G

Standard Drafting Team Roster for NERC Standards Development Project 2009-01

Project 2009-01 Disturbance and Sabotage Reporting
Drafting Team

Name and Title	Company and Address	Contact Info	Bio
Brian Evans-Mongeon – Chair	Utility Services 25 Crossroad Suite 201 Waterbury, VT 05676	802-552-4022 Brian.Evans-Mongeon@utilitysvcs.com	**Work Experience** Brian organized and created Utility Services in 2007 and has been working with registered entities on NERC related activities since that time. Prior to this, he worked for Vermont Public Power Supply Authority and Green Mountain Power Corporation in power supply, transmission, system operations, and distribution activities. Tasks have included contract negotiations, administration of tariffs and rates, coordination with transmission providers, and reporting of operational and reliability considerations. **NERC and NPCC Specific Activities** While not a registered entity, Utility Services works with the staffs of Registered Entities to ensure compliance and consistency of the standards and requirements. Presently, Utility Services works with 70 Registered Entities with over 150 functional registrations throughout all 8 NERC regions. Within the regions, Utility Services is a Member of NPCC, RFC, FRCC, MRO, and WECC. Brian has served in a number of committees, task forces, and working groups regionally and nationally; including regional standards for Disturbance Monitoring and Under Frequency Load Shedding, Disturbance and Sabotage Reporting, defining the Bulk Electric System, and the NERC CIPC Compliance and Enforcement Input WG (CEIWG) **Education** Brian has an Associates degree in Electric/Electronic Technology from Vermont Technical College and a Bachelors of Science in Business Administration from the University of Vermont.
Joseph DePoorter – Vice-Chair	Madison Gas and Electric Company 133 South Blair St., Madison, Wisconsin 53703	608-252-1599, jdepoorter@mge.com	Joseph DePoorter is the Director of NERC Compliance and Generation Operations and joined Madison Gas and Electric Company (MGE) in the spring of 2001 after retiring from the United States Marine Corps. Joe started at MGE as a Distribution Operator and becoming NERC Certified (RA) in January of 2003. Joe then became a System Operator where duties were under the auspice of a Control Area. MGE then started to enter into agreements with the Midwest ISO and Joe assisted

			the real-operations component for MGE. In March of 2007, Joe became the Manager of Reliability Compliance, focusing on the upcoming enforceable NERC Standards. Joe has lead three on sight compliance audits (from the MRO), is the Chair of the MRO NERC Standards Review Forum, Chair of the MRO Performance and Risk Oversight Sub-committee and the Vice Chair of Project 2009-01.
Michelle Draxton Security Manager - Generation Corporate Security Operations - Client Services	Exelon Corporation 300 Exelon Way Suite 320 Kennett Square, PA 19348	Office: 610.765.6942 Mobile: 410.474.2993 michelle.draxton@exeloncorp.com	Michelle Draxton joined the Constellation Energy Group (CEG)/Exelon Corporation in 1991 (CEG merged with the Exelon Corporation in 2012), following a short career in Education. During Michelle's 21 years with the company, she spent the first ten (10) years of her career working in Project Controls; Project Management and Long Range Scheduling & Cost Control (supporting shutdown safety scheduling); and the Diesel Upgrade Project. She was a Nuclear Security Training Specialist/ Nuclear Supervisor for the Security Access & Fitness Duty Program, ensuring compliance with Nuclear Regulatory Commission (NRC) and Nuclear Energy Institute (NEI) regulations/guidelines. When CE merged with Nigra Mohawk - Nine Mile Point Nuclear Facility and the Rochester Gas Electric - Ginna Nuclear Station, Michelle performed strategic alignment between the three nuclear facilities maintenance-training program and leadership programs as a Senior Organizational Development and Training Consultant. Michelle has been with Corporate and Information security for 11 years. In 2007/2008, Michelle led a cross-functional team to implement the initial NERC Critical Infrastructure Protection (CIP) Cyber Security Governance/Program and the Security Awareness Program for CEG. Michelle currently manages a team of security specialists who ensure compliance with the organization's policies and procedures, as well as protect the personnel and assets of generation facilities within the U.S. and Canada. Michelle organizes and coordinates investigations involving allegations of criminal matters, fraud, computer crimes, intellectual property and other security issues with her team and develops risk assessments and security plans to ensure compliance with multiple federal regulatory bodies.
Jimmy Hartmann	Electric Reliability Council of Texas	512-248-6986 jhartmann@ercot.c	Jimmy Hartmann is currently the Supervisor of System Operations for the Electric Reliability

	(ERCOT) 2705 West Lake Dr. Taylor, Texas 76574	om	Council of Texas, Inc (ERCOT). Overall, Jimmy has more than thirty years of combined experience in the Energy industry. His experiences include power plant operations, power marketing and system operations. In his twelve years of service to ERCOT, Jimmy has served in many capacities including System Operator, Outage Coordinator and a Shift Supervisor, all of which are responsible for ensuring the reliability of the ERCOT interconnection. Jimmy currently holds certifications as a NERC Reliability Coordinator and as an ERCOT System Operator. Prior to ERCOT, Jimmy was employed at South Texas Electric Cooperative, Inc for five years working as a System Operator, Wholesale Marketing Specialist/Energy Trader and a Lead System Operator responsible for making and carry through decisions that were required to operate their system during normal and adverse conditions. Prior to STEC, Jimmy was employed at San Miguel Electric Cooperative, Inc working at a 440MW Lignite Fired Power Plant where he also had a multitude of operational responsibilities spanning over a fourteen year period.
Robert D. Canada	North American Electric Reliability Corporation 3353 Peachtree Rd Suite 600 North Tower Atlanta, GA 30326,	Office 404-446-9709 Cell 770-608-5666 bob.canada@nerc.net	Bob Canada has been with NERC since October 2011 as a NERC Standards Specialist and is the Critical Infrastructure Protection Committee Secretary. He was with Southern Company for 29 years and served as a Business Assurance Principal focused on systematic approach to operational resiliency and physical security. He worked to coordinate and achieve a consistent corporate security strategy, policy and “all hazards” response for the four operating companies – Georgia Power, Alabama Power, Gulf Power and Mississippi Power. Canada served twice in a leadership capacity as Chairman for the Edison Electric Institute’s (EEI) Security Committee, which is the electric industry lobbyist in Washington D.C. Here he assisted with strategic work on security issues facing the electric industry such as a response to 9/11 and the many federal guidelines for regulatory agencies. Canada established the first Georgia Emergency Management Agency liaison on behalf of the Southern Company and Georgia Power with the State of Georgia to coordinate utility response during emergencies and disaster response. He served the Southeastern Reliability Council (SERC) for four years as Chairman of the Critical Infrastructure Protection Committee and presently represents SERC on the North American Electric Reliability Corporation’s (NERC) Critical

			Infrastructure Committee (CIPC) as the physical security representative and voting member. Other responsibilities included directing the Georgia Power and Southern Company Olympic planning efforts and implementation of physical security surveys and protective countermeasures to ensure the continuity and mitigation of threats to the 1996 Olympic Games. He consulted with Federal, state and local law enforcement agencies to protect the electrical infrastructure in Georgia and Metropolitan Atlanta. Canada served on the Atlanta Committee for the Olympic Games as a corporate security liaison to the utilities in Georgia. He presently serves as Vice Chair on the NERC CIPC Executive Committee and has served on the Electricity Sector Coordinating Council interfacing on policy level decision making processes with Department of Homeland Security (DHS) and the Department of Energy for initiatives and protective programs such as the Energy Sector's National Infrastructure Protection Plan. Honors included The Security Executive Council Magazine's "Most Influential" in the electric utility for 2011.
Brian Harrell CPP Critical Infrastructure Department	North American Electric Reliability Corporation 3353 Peachtree Rd Suite 600 North Tower Atlanta, GA 30326	(609) 651-0671 Brian.Harrell@nerc.net	Brian Harrell is the Manager of CIP Standards, Training, and Awareness for NERC. In this capacity he is responsible for managing ERO-wide critical infrastructure protection standards initiatives and assisting in the development of the overall CIP program strategy. Harrell has 15 years of experience in the security industry serving in organizations such as law enforcement, the military and corporate security, among others. Most recently, he served as the Manager of Critical Infrastructure Protection for SERC Reliability Corporation, where he oversaw all security- and CIP reliability-related matters for the Region. Prior to joining SERC, Harrell was the Sector Security Specialist for the Infrastructure Security Compliance Division at the U.S. Department of Homeland Security. He specialized in securing high risk critical infrastructures and Continuity of Operations (COOP) for the Department of Homeland Security. Brian also served in the U.S. Marine Corps as an Anti-Terrorism and Force Protection Instructor. Harrell has a M.A. from Central Michigan University and a B.A. from Hawaii Pacific University. He is also board certified in security management.
Scott Mix	North American	215-853-8204 scott.mix@nerc.ne	Mr. Scott R. Mix, CISSP, joined NERC in October 2006 following more than 25 years of experience

CIP Technical Manager	Electric Reliability Corporation 1325 G Street NW, Suite 600 Washington, DC 20005	t	working in various facets of the electricity industry, including as a consultant with KEMA, Inc., Infrastructure Security Manager with the Electric Power Research Institute (EPRI), Senior Security Analyst at the PJM Interconnection, and more than ten years with Leeds & Northrup Co. as a programmer/analyst and systems architect. For more than ten years, he has focused on the areas of Computer and Infrastructure Security for the Electricity Sector. At NERC, he is responsible for Critical Infrastructure Protection issues, primarily as they relate to Real Time and Control System Security, and the development of the revisions to the NERC CIP Standards. He has also been the NERC Staff Facilitator for the Critical Infrastructure Protection Committee (CIPC) and several of its working groups and task forces, and a member of the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) Staff. Throughout his career, Mr. Mix has worked closely with numerous industry and government organizations, including NERC's Critical Infrastructure Protection Committee (CIPC) and its working teams, and is the former convener of the Control System Security Working Group, has been an active and vocal observer to the NERC Cyber Security Standards Version 1 Drafting Team (and the NERC 1200 process before that), and is a former member of the OASIS "How" Working Group. He has also worked with the Department of Energy, the Department of Homeland Security, the FBI's National Infrastructure Protection Center, and the Federal Energy Regulatory Commission dealing with specific Electric Sector Security Issues. He has organized and presented at numerous industry symposia, both domestically and internationally. He has been a member and chapter secretary of the Philadelphia Chapter of InfraGard, is a member of the ISA and has participated in the ISA100 standards activities, and is a member of the IEEE as well as its Computer Society, Power Engineering Society, and Standards Association. He is a Certified Information Systems Security Professional (CISSP). Mr. Mix is a graduate of the Bloomsburg University of Pennsylvania with a Bachelor of Science degree in Computer & Information Science and Chemistry.
Stephen Crutchfield Standards Development	North American Electric Reliability Corporation 3353 Peachtree Rd	609-651-9455 Stephen.crutchfield@nerc.net	Stephen Crutchfield is the NERC Staff Coordinator for Project 2009-01, Disturbance and Sabotage Reporting. Stephen began his career with NERC in May 2007. Prior to joining NERC, Stephen was a

Coordinator	Suite 600 North Tower Atlanta, GA 30326		Project Manager with Shaw Energy Delivery Services, managing engineering and construction projects in the substation and transmission line fields. Stephen's background also includes experience with PJM as Manager of RTO Integration, working on the operations and markets integration of new members (AEP, ComEd, Dayton, Dominion and Duquesne) into PJM and southern seams operations issues with Progress Energy, Duke and TVA. Stephen also helped lead the team that was developing GridSouth in the dual roles of Organization Architect and Manager of Customer Support. Prior to GridSouth, Stephen was the Manager of Power System Operations Training at Progress Energy where he spent over 10 years training System Operators and Engineers. Overall, Stephen was with Progress Energy for 16 years. Stephen received his Bachelor of Arts in Physics from the University of Virginia and Masters of Science in Electrical Engineering from North Carolina State University. Stephen also holds a Master of Science in Management degree, also from North Carolina State University.

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)** **)**	**Docket No. RD13-_____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS VERSION 5

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
willie.phillips@nerc.net

Counsel for North American Electric Reliability Corporation

January 31, 2013

TABLE OF CONTENTS

I. Executive Summary…….. 3

II. Notices and Communications……... 7

III. Background and Regulatory Framework.....…….. 7

IV. Justification for Approval of the Proposed Modifications to Reliability Standards…….. 8

a. Basis for Approval of Proposed Reliability Standard
b. CIP Version 5 presents significant improvements to previous CIP standards
c. New Proposed Reliability Standards CIP-010-1and CIP-011-1
d. Proposed Definitions of Terms Used in CIP Version 5
e. Enforceability of the Proposed CIP Version 5 Reliability Standards
f. Violation Risk Factor and Violation Severity Level Assignments
g. NERC Reliability Standards Development Procedure

V. CIP Version 5 Satisfies All FERC Directives and Concerns …….. 30

a. Order No. 706 Directives
b. Application of NIST Framework
c. Regional Perspective

VI. Summary of the Reliability Standard Development Proceedings…….…….. 41

VII. CIP Version 5 Implementation Plan…… 42

VIII. Conclusion…….…..… 44

Exhibit A — Proposed CIP Version 5 Reliability Standards submitted for Approval and associated modifications to the Glossary of Terms used in NERC Reliability Standards
Exhibit B — Implementation Plan for Proposed CIP Version 5 Reliability Standards submitted for Approval
Exhibit C — Standard Drafting Team Roster for Project 2008-06 - Cyber Security Order 706 Version 5 CIP Standards
Exhibit D — Consideration of Comments Reports
Exhibit E — Table of VRFs and VSLs Proposed for Approval and Analysis of how VRFs and VSLs Were Determined Using Commission Guidelines
Exhibit F — Record of Development of Proposed CIP Version 5 Reliability Standards
Exhibit G — Order No. 672 Criteria for Approving Proposed Reliability Standards
Exhibit H — Consideration of Issues and Directives

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)** **)**	**Docket No. RD13-____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS VERSION 5

The North American Electric Reliability Corporation ("NERC")[1] hereby requests that the Federal Energy Regulatory Commission ("FERC" or the "Commission") approve, in accordance with Section 215(d)(1) of the Federal Power Act ("FPA")[2] and Section 39.5 of the Commission's regulations, 18 C.F.R. § 39.5 (2012), the following ten proposed Critical Infrastructure Protection ("CIP") Reliability Standards ("CIP Version 5") and find that they are just, reasonable, not unduly discriminatory or preferential and in the public interest:

- CIP–002–5 — Cyber Security — BES Cyber System Categorization
- CIP–003–5 — Cyber Security — Security Management Controls
- CIP–004–5 — Cyber Security — Personnel and Training
- CIP–005–5 — Cyber Security — Electronic Security Perimeter(s)
- CIP–006–5 — Cyber Security — Physical Security of BES Cyber Systems
- CIP–007–5 — Cyber Security — Systems Security Management
- CIP–008–5 — Cyber Security — Incident Reporting and Response Planning
- CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP–010–1 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP–011–1 — Cyber Security — Information Protection

[1] NERC was certified by the Commission as the electric reliability organization ("ERO") in accordance with Section 215 of the Federal Power Act in its order issued on July 20, 2006 in Docket No. RR06-1-000. *North American Electric Reliability Corp.*, 116 FERC ¶ 61,062 (2006) ("ERO Certification Order").
[2] 16 U.S.C. § 824o (2012).

NERC also requests approval of the proposed definitions of terms used in the proposed CIP Version 5, the associated implementation plan, and the proposed Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs").[3] This filing also addresses all remaining standards-related issues and directives from Order No. 706.[4]

Additionally, NERC requests that CIP Version 5 become effective on the first day of the eighth calendar quarter after a final rule is issued in this docket. The requested effective date: (1) is just and reasonable; (2) properly balances the urgency to implement the standards with time allowed to develop necessary procedures, software, facilities, staffing or other relevant capabilities; and (3) allows applicable entities adequate time to ensure compliance with the requirements in accordance with Order No. 672.[5]

After a successful industry ballot with the CIP Version 5 standards achieving approval ranging from to 78.59% to 95.67%, the NERC Board of Trustees approved the CIP Version 5 standards and related documents on November 26, 2012.

Exhibit A to this filing sets forth the proposed CIP Version 5 standards and associated modifications to the Glossary of Terms used in NERC Reliability Standards. **Exhibit B** contains the Implementation Plan for CIP Version 5. **Exhibit C** contains the Standard Drafting Team Roster for Project 2008-06 Cyber Security Order 706, which is the technical team responsible for developing CIP Version 5. **Exhibit D** contains the Consideration of Comments Reports for CIP

---

[3] Unless otherwise specified, capitalized terms used herein have the meanings specified in the *NERC Glossary of Terms*, available at: http://www.nerc.com/files/Glossary_of_Terms.pdf.

[4] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, *denying reh'g and granting clarification*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229 (2009), *order denying clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009) ("Order No. 706").

[5] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204 at P 333, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006) ("In considering whether a proposed Reliability Standard is just and reasonable, FERC will consider also the timetable for implementation of the new requirements, including how the proposal balances any urgency in the need to implement it against the reasonableness of the time allowed for those who must comply to develop the necessary procedures, software, facilities, staffing or other relevant capability.").

Version 5. **Exhibit E** contains a table of CIP Version 5 VRFs and VSLs proposed for approval and Commission guideline analyses. **Exhibit F** contains the development record for CIP Version 5. **Exhibit G** addresses the Order No. 672 Criteria for Approving Proposed Reliability Standards. **Exhibit H** contains the Consideration of Issues and Directives.

NERC is also filing the proposed CIP Version 5 standards and associated documents for approval with applicable governmental authorities in Canada.

I. EXECUTIVE SUMMARY

The White House and U.S. Congress have acknowledged that cybersecurity threats are increasing in number and sophistication. President Barack Obama declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity."[6]

Defense Secretary Leon Panetta warned that the nation is facing the possibility of a "cyber-Pearl Harbor" and is "increasingly vulnerable to foreign computer hackers who could dismantle the nation's power grid…."[7] Congress has also considered cybersecurity legislation "that would establish security standards to prevent large-scale cyber-attacks on the nation's critical infrastructure," — including the electrical grid.[8]

Recognizing the importance of the Bulk Power System, Congress has vested the ERO with the responsibility of developing mandatory Reliability Standards, including cybersecurity standards. Taking into consideration four years of experience since the first NERC CIP Cyber

[6] National Security Council, *Cyber Security*, http://www.whitehouse.gov/administration/eop/nsc/cybersecurity.
[7] Elizabeth Bumiller and Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, The New York Times, October 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all.
[8] Ed O'Keefe and Ellen Nakashima, *Cybersecurity Bill Fails in Senate*, The Washington Post, August 2, 2012, http://www.washingtonpost.com/world/national-security/cybersecurity-bill-fails-in-senate/2012/08/02/gJQADNOOSX_story.html.

Security Reliability Standards were implemented, as well as applicable FERC directives, NERC developed the proposed CIP Version 5 standards to better protect the reliability of the nation's Bulk Electric System ("BES")[9] from cyber-attacks.

The proposed CIP Version 5 standards were overwhelmingly supported by industry, with the industry ballot averaging nearly 90% approval. The standards also present a significant improvement over the existing CIP Version 3[10] and the Commission-approved CIP Version 4 standards.[11] For this reason, NERC seeks swift action by the Commission to approve the proposed CIP Version 5 standards as discussed in this petition.

With respect to concerns expressed by Responsible Entities regarding the transition from CIP Version 3 to Version 4 to Version 5 Reliability Standards, NERC understands that the transition could be complicated. For this reason, NERC stands ready to work with industry to address transition issues as they arise.

The proposed implementation plan for CIP Version 5, included with this filing as **Exhibit B,** provides language that would allow entities to transition from CIP Version 3 to CIP Version 5, thereby bypassing implementation of CIP Version 4 completely upon Commission approval. The proposed implementation plan specifically states:

> Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.

[9] In this petition, the terms "Bulk Power System" and "Bulk Electric System" are used interchangeably. "Bulk Electric System" is defined in the NERC Glossary of Terms, and generally includes facilities operated at voltages at and above 100 kV. *See* NERC Glossary of Terms Used in Reliability Standards at 2. "Bulk-Power System" is defined in section 215 of the FPA, and does not include a voltage threshold. *See* 16 U.S.C. 824o(a)(1).

[10] *North American Electric Reliability* Corporation, 130 FERC ¶ 61,271 (March 31, 2010) ("In this order, we approve the modified CIP Reliability Standards, with an effective date of October 1, 2010.")

[11] *See Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 139 FERC ¶ 61,058 (2012)(Noting CIP Version 4 Implementation date of April 1, 2014).

Prompt Commission approval of the CIP Version 5 standards and the implementation plan would reduce uncertainty among Responsible Entities regarding implementation of the CIP standards. Therefore, NERC reiterates its request for prompt Commission action approving the CIP Version 5 standards and associated implementation plan. Additionally, to help the industry implement the CIP Version 4 and 5 standards, NERC will initiate a series of industry workshops that will be presented across North America beginning in 2013.

The improvements included in CIP Version 5 reflect a maturity of the NERC CIP program. While the general framework of the proposed standards follow the organization of the previous CIP versions, a new process is introduced in proposed CIP-002-05 for identifying and classifying BES Cyber Systems according to "Low-Medium-High" impact.[12] Once BES Cyber Systems are identified, a Responsible Entity must then comply with proposed CIP-003-5 to CIP-011-1, according to specific criteria relating to impact and other characteristics such as communications connectivity. As such, NERC and its stakeholders have proposed the most comprehensive set of mandatory cybersecurity standards ever utilized on a widespread basis in the electric industry.

Key features of the comprehensive approach taken in CIP Version 5 include:

- Utilizing a National Institute of Standards and Technology ("NIST") based approach to categorize all cyber systems which impact the BES as "Low-Medium-High" (at the system level) and requiring at least a minimum classification of "Low Impact" for all BES Cyber Systems.

- Building on the implementation experience from prior CIP Reliability Standard versions.

- Addressing all applicable directives in Order No. 706.

- Eliminating unnecessary documentation requirements to allow entities to focus on the reliability and security of the Bulk Power System.

[12] BES Cyber Systems, discussed herein, is a proposed addition to the *Glossary of Terms used in NERC Reliability Standards*.

- Providing guidance and context within each CIP Version 5 standard.

The identification of cyber assets has evolved through the various CIP Reliability Standards versions. Building on the prior "Risk-Based Assessment Methodology" in CIP-002-3 and the "Bright-line Criteria" in CIP-002-4, the proposed CIP Version 5 standards focus on all cyber system assets that have an impact on Bulk Power System reliability, and characterizes that impact as either high, medium or low.

In Order No. 761, the Commission directed NERC to file CIP Version 5 addressing all remaining directives from Order No. 706, by March 31, 2013. With the strong support of industry, and the efforts of the diverse standard drafting team, this petition satisfies the Commission's directives two months prior to the Commission-required due date.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[13]

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco*
Senior Vice President and General Counsel
Holly A. Hawkins*
Assistant General Counsel
Willie L. Phillips*
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
willie.phillips@nerc.net

III. BACKGROUND AND REGULATORY FRAMEWORK

By enacting the Energy Policy Act of 2005 ("EPAct 2005"),[14] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Nation's Bulk Power System, and with the duty of certifying an electric reliability organization ("ERO") that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215 of the FPA states that all users, owners, and operators of the Bulk Power System in the United States will be subject to Commission-approved Reliability Standards, which include requirements for the operation of existing Bulk Power System facilities and cybersecurity protection.[15]

---

[13] Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.
[14] 16 U.S.C. § 824o (2012).
[15] *See* Section 215(b)(1)("All users, owners and operators of the bulk-power system shall comply with reliability standards that take effect under this section.").

IV. JUSTIFICATION FOR APPROVAL OF THE PROPOSED RELIABILITY STANDARDS

In this section we will discuss the following: a) the basis for approval of the proposed Reliability Standards; b) significant improvements to previous CIP standards; c) new proposed Reliability Standards CIP-010-1and CIP-011-1; d) proposed definitions of glossary terms used in CIP Version 5; e) enforceability of the proposed CIP Version 5; f) VRF and VSL assignments; and g) NERC Reliability Standards Development Procedure.

This section summarizes the development of proposed CIP Version 5 and demonstrates that the proposed modifications meet the criteria for approval established by the Commission. That is, the modifications and enhancements provided in CIP Version 5 ensure that the proposed standards are just, reasonable, not unduly discriminatory or preferential and in the public interest.[16]

The proposed CIP Version 5 standards, which were overwhelmingly approved by industry, are a significant improvement over the existing CIP standards and help protect the reliability of the BES. Thus, given the strong industry support for these improvements, NERC respectfully requests that the Commission expeditiously approve the proposed CIP Version 5 standards, as presented in **Exhibit A**.

a. Basis for Approval of Proposed Reliability Standards

Section 39.5(a) of the Commission's regulations requires the ERO to file with the Commission for its approval each Reliability Standard that the ERO proposes to become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes to be made effective. The Commission has the regulatory responsibility to approve standards that protect the reliability of the Bulk Power System and to ensure that such

[16] *See* Order No. 672.

standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest.

Section 215(d)(5) of the FPA authorizes the Commission to order the ERO to submit a new or modified Reliability Standard. Pursuant to Section 215(d)(2) of the FPA and Section 39.5(c)(1) of the Commission's regulations, the Commission is required to give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard. In Order No. 693, the Commission noted that it would defer to the "technical expertise" of the ERO with respect to the content of a Reliability Standard and explained that, through the use of directives, it provides guidance but does not dictate an outcome. Rather, the Commission will consider an equivalent alternative approach provided that the ERO demonstrates that the alternative will address the Commission's underlying concern or goal as efficiently and effectively as the Commission's proposal, example, or directive.[17]

The technical expertise of the ERO is derived from a standards drafting team consisting of participants that are considered experts in the cybersecurity arena. The members of the CIP Version 5 standard drafting team also provided a diversity of experience, ranging across North America, including both the continental United States and Canada. Detailed biographical information for each of the members is included with the standards drafting team roster in **Exhibit C**.

Order No. 672 sets forth the factors the Commission considers when determining whether proposed Reliability Standards meet the statutory criteria and are just, reasonable, not unduly discriminatory or preferential and in the public interest. Each of those factors is identified and addressed in **Exhibit G**.

---

[17] *See Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242 at PP 31, 186-187, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

The proposed CIP Version 5 serves the important reliability goal of providing a cybersecurity framework for the identification and protection of BES Cyber Systems (discussed below) to support the reliable operation of the Bulk Power System. Generally, the framework of CIP Version 5 can be divided into two groups:

1) **Categorization of risk (based on "Low-Medium-High" impact to BES reliability)**

    - CIP–002–5 — BES Cyber System Categorization

2) **Risk mitigation lifecycle (implement, evaluate, monitor, and update)**
    - CIP–003–5 — Security Management Controls
    - CIP–004–5 — Personnel and Training
    - CIP–005–5 — Electronic Security Perimeter(s)
    - CIP–006–5 — Physical Security of BES Cyber Systems
    - CIP–007–5 — Systems Security Management
    - CIP–008–5 — Incident Reporting and Response Planning
    - CIP–009–5 — Recovery Plans for BES Cyber Systems
    - CIP–010–1 — Configuration Change Management and Vulnerability Assessments
    - CIP–011–1 — Information Protection

The proposed CIP Version 5 takes a more comprehensive approach to categorizing risk, and requires Responsible Entities to identify BES Cyber Systems, but generally maintains the cybersecurity protection framework contained in previous CIP versions. Key features of the comprehensive approach taken in CIP Version 5 include:

- Utilizing a NIST-based approach to categorize all cyber systems which impact the BES as "Low-Medium-High" (at the system level) and requiring at least a minimum classification of "Low Impact" for all BES Cyber Systems.

- Building on the implementation experience from prior CIP versions.

- Addressing all applicable directives in Order No. 706.

- Eliminating unnecessary documentation requirements to allow entities to focus on the reliability and security of the Bulk Power System.

- Providing guidance and context within each CIP Version 5 standard.

The proposed CIP-002-5 Reliability Standard is the first step in identifying BES Cyber Systems. If a Responsible Entity does not identify any BES Cyber Systems – that ends the compliance review under proposed CIP-003-5 to CIP-011-1. However, a Responsible Entity that identifies BES Cyber Systems must comply with proposed CIP-003-5 to CIP-011-1, according to specific criteria that characterize the impact of the identified BES Cyber Systems.

Specifically, as discussed and analyzed in detail below, proposed CIP Version 5 uses CIP-002-5 "Attachment 1 – Impact Rating Criteria" to identify three categories of BES Cyber Systems: 1) the High Impact category that covers large Control Centers, similar to those control centers identified as Critical Assets in CIP-002-4; 2) the Medium Impact category that covers generation and transmission facilities, similar to those identified as Critical Assets in CIP-002-4, along with other control centers not identified as Critical Assets in CIP-002-4; and 3) the Low Impact category that covers all other BES Cyber Systems. In addition, the Low Impact category provides protections for systems not included in CIP Version 4 (*i.e.*, CIP-002-4).

Generally, modifications to the existing CIP Reliability Standards included in the proposed CIP Version 5 standards can be described as follows:

- **CIP-002-5** will require the identification and categorization of BES Cyber Systems according to specific criteria that characterize their impact for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES.

- **CIP-003-5** will require approval of the documented cybersecurity policies related to CIP-004-5 through CIP-009-5, CIP-010-1, and CIP-011-1. CIP-003-5, Requirement 2, will require implementation of programmatic controls related to cybersecurity awareness, physical security controls, electronic access controls, and incident response to a Cyber Security Incident for those assets that have low impact BES Cyber Systems according to CIP-002-5's categorization process. The requirement that a Cyber Security Policy be "readily available" has been deleted because of general confusion around that term and because training requirements in CIP-004-5 provide for knowledge of policy. Several portions of requirements related to

information protection in previous CIP versions have been moved to CIP-011-1 and therefore deleted from CIP-003-5.

- **CIP-004-5** will require documented processes or programs for security awareness, cyber security training, personnel risk assessment, and access management. In Requirement R2, CIP-004-5 adds specific training roles for visitor control programs, electronic interconnectivity supporting the operation and control of BES Cyber Systems, and storage media as part of the handling of BES Cyber System Information. The requirements surrounding personnel risk assessments and access management were modified in response to lessons learned from implementing previous versions. Proposed CIP-004-5, Requirement R3, now specifies that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more without specifying school, work, etc., and regardless of official residence. In Requirement R4, the primary change was in combining the access management requirements from CIP-003-4, CIP-004-4, CIP-006-4 and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to improve consistency in the authorization and review process. The requirement in CIP-004-4 Requirement R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access. Requirement R5 specifies revocation of access for a termination action concurrent with termination, to be completed within 24 hours.

- **CIP-005-5**, Requirement R1, focuses more on the discrete Electronic Access Points rather than the logical "perimeter." CIP-005-1 through CIP-005-4's Requirement R1.2 has been deleted from CIP Version 5. This requirement was definitional in nature and was used to bring dial-up modems using non-routable protocols into the scope of previous versions of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in CIP Version 5; therefore, there is no need for this requirement. CIP-005-1 through CIP-005-4's Requirements R1.1 and R1.3 were also definitional in nature, and they have been deleted from Version 5 as separate requirements; however, the concepts were integrated into the definitions of Electronic Security Perimeter ("ESP") and Electronic Access Point ("EAP"). CIP-005-5, Requirement R2, related to interactive remote access, is a new requirement to continue the efforts of the NERC Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

- **CIP-006-5** is intended to manage physical access to BES Cyber Systems by specifying a physical security plan to protect BES Cyber Systems against compromise that could lead to misoperation or instability. CIP-006-4, Requirements R8.2 and R8.3, concerning the retention of testing records, has been removed, and the retention period is specified in the compliance section of CIP-006-5.

- **CIP-007-5** will address system security by specifying technical, operational, and procedural requirements in support of protecting BES Cyber Systems against

compromise that could lead to misoperation or instability of the BES. CIP-007-5 is modified in several places to conform to the formatting approach of CIP Version 5, along with changes to address several Commission directives and to make the requirements less dependent on specific technology so that they will remain relevant for future, yet-unknown developing technologies (for example, in Requirement R3, the requirement is a competency-based requirement where the Responsible Entity must document how the malware risk is handled for each BES Cyber System, but the requirement does not prescribe a particular technical method in order to account for potential technological advancement).

- **CIP-008-5** will mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Proposed Requirement R1 now includes an obligation to report Cyber Security Incidents within 1 hour of recognition. Requirement R2 adds testing requirements to verify response plan effectiveness and consistent application in responding to a Cyber Security Incident. Requirement R3 includes provisions for an after-action review for tests or actual incidents, along with a requirement to update the Cyber Security Incident response plan based on those lessons learned. In Requirement R3, a single timeline now combines several timelines for concurrent activities related to lessons learned and updates to recovery plans in previous CIP versions, although the total time to complete the related activities remains the same. Additionally, where previous CIP versions specified "30 calendar days" for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.

- **CIP-009-5** is intended to recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement R1, adds provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized. Requirement R2 adds operational testing for recovery of BES Cyber Systems. In Requirement R3, timelines for several concurrent activities related to lessons learned and updates to recovery plans in previous versions were combined to provide one timeline, similar to CIP-009-5.

- **CIP-010-1** is a new standard that consolidates the configuration change management and vulnerability assessment-related requirements from previous versions of CIP-003, CIP-005 and CIP-007. Requirement R1 specifies the configuration change management requirements, Requirement R2 specifies the configuration monitoring requirements intended to detect unauthorized modifications to BES Cyber Systems, and Requirement R3 specifies the vulnerability assessment requirements intended to ensure proper implementation of cyber security controls along with promoting continuous improvement of cyber security posture.

- **CIP-011-1** is a new standard that consolidates the information protection requirements from previous versions of CIP-003 and CIP-007. Requirement R1

> specifies information protection requirements to prevent unauthorized access to BES Cyber System Information. Requirement R2 specifies reuse and disposal provisions intended to prevent unauthorized dissemination of protected information.

All ten of the proposed CIP Version 5 standards provide a comprehensive set of requirements to protect the BES from malicious cyber-attacks. Because there are unique aspects of cyber protection for each Responsible Entity and its assets, proposed CIP Version 5 requires Bulk Power System owners, operators, and users to identify and categorize BES Cyber Systems (which are comprised of BES Cyber Assets) as described in the proposed new defined terms provided below:

> **BES Cyber Asset**
>
> A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)
>
> **BES Cyber System**
>
> One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

As noted, once Responsible Entities identify BES Cyber Systems, the CIP Version 5 requirements are then applied according to the impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES, in accordance with proposed CIP-002-5.

Additionally, proposed CIP Version 5 requires responsible entities to establish plans, protocols, and controls to safeguard physical and electronic access (CIP-003-5 – CIP-011-1), to train personnel on security matters (CIP-004-5), to report security incidents (CIP-008-5), and to be prepared for recovery actions (CIP-009-5).[18]

b. CIP Version 5 presents significant improvements to previous CIP standards.

Modifying CIP-002-5 to require responsible entities to use a new approach to categorize all cyber systems impacting the BES as "Low-Medium-High" is the most significant improvement to the existing CIP Reliability Standards. This new approach effectively moves away from the CIP Version 4 "bright-line" approach of only identifying Critical Assets (and applying CIP requirements only to their associated Critical Cyber Assets), to requiring a minimum classification of "Low Impact" for all BES Cyber Systems.[19]

The shift to identifying and categorizing "High-Medium-Low" BES Cyber Systems (according to their impact on the BES) resulted from a review of the NIST Risk Management Framework for categorizing and applying security controls, a review that was directed by the Commission in Order No. 706.[20]

The following discussion is an analysis of each of the criterion included in Attachment 1 used to determine impact categories of BES Cyber Systems.

> **Criterion 1. High Impact Rating (H)**
> Each BES Cyber System used by and located at any of the following:
>
> **1.1.** Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

[18] The extensive development record includes successive drafts of the CIP Reliability Standards, the ballot pool, the final ballot results by registered ballot body members, and stakeholder comments received during the development of the proposed standards, as well as a discussion regarding how those comments were considered in developing them.
[19] Proposed CIP-003-5 through CIP-009-5 are consistent with the organization of CIP Versions 1 through 4.
[20] Order No. 706 at P 25.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4. Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

The High Impact rating category generally includes those BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Reliability Coordinator ("RC"), Balancing Authority ("BA"), Transmission Operator ("TOP"), or Generator Operator ("GOP"), as defined under the NERC Functional Model.[21]

Based on stakeholder comments, the standards drafting team made significant changes to Attachment 1, Criteria 1.1 to 1.4. Specifically, the standards drafting team tailored the definition of Control Center to refer to real-time reliability tasks for applicable functional entities from the functional model, which includes those necessary for situational awareness.

During the development process, one commenter noted that the proposed High Impact rating criteria do not consider the inter-connected nature of the BES Cyber Assets or BES Cyber Systems when defining threshold-based criteria. The standards drafting team responded that using inter-connections as an impact criterion ultimately scopes in all inter-connected systems in a single impact level. In addition, the standards drafting team recognized the concept of security zones, used heavily in the NIST Risk Management Framework, which allows the implementation of cybersecurity controls commensurate with the level of impact within a security boundary.

[21] NERC Reliability Functional Model, available at: http://www.nerc.com/page.php?cid=2%7C247%7C108.

For proposed CIP Version 5, BES Cyber Systems of all impact levels, with routable or dial-up connectivity, are required to be within a security zone that provides protection from outside influences using a posture of "mutual distrust". As such, no communication crossing the perimeter is trusted, regardless of where that communication originates. Therefore, BES Cyber Systems at High, Medium, and Low impact levels would be required to implement electronic perimeter protections for all routable and dial-up communications, regardless of inter-connectivity.

The 3,000 MW threshold in criterion 1.2 and the corresponding 1,500 MW threshold in criterion 2.13 for Control Centers performing BA functions were based on the NERC 2012 Control Performance Standard 2 Bounds Report.[22] This report lists the estimated peak demand for each BA, and the standards drafting team determined that a 3,000 MW and 1,500 MW threshold would capture roughly 90% and 96%, respectively, of the peak demand.

Criterion 2. Medium Impact Rating (M)
Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

[22] NERC, *2012 CPS2 Bounds*, available at: http://www.nerc.com/docs/oc/rs/2012%20CPS2%20Bounds%20Report%20Final(Update20120419).pdf.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to

operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

- **Generation – Criteria 2.1, 2.3, 2.6, 2.9, 2.11, and 2.13 (Medium Impact Rating)**

Criteria 2.1, 2.3, 2.6, 2.9, and 2.11 of Attachment 1's Medium Impact rating category apply to Generation Owners ("GOs") and Generation Operators ("GOPs"). Criterion 2.13 is applicable to Balancing Authority ("BA") Control Centers.

Criterion 2.1 designates as Medium Impact those BES Cyber Systems that Medium Impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC Reliability Standard BAL-002, whose purpose is to ensure the BA is able to utilize its Contingency Reserve to balance resources and demand, and return Interconnection frequency within defined limits following a Reportable Disturbance.

In Criterion 2.3, the standards drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact.

Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of Interconnection Reliability Operating Limits ("IROLs") and their associated contingencies, as specified by FAC-014-2, Establish and Communicate System Operating Limits, R5.1.1 and R5.1.3.

Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems ("SPS") and Remedial Action Schemes ("RAS") as medium impact. SPS and RAS's may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is needed or if it operates outside of the designed parameters. GOs and GOPs that own BES Cyber Systems for such Systems and schemes designate them as Medium Impact.

Criterion 2.11 categorizes as Medium Impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not been included in Part 1. The 1500 MW threshold omits facilities that have little impact on BES reliability, but would otherwise be captured under the newly defined term for Control Center.

Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

- **Transmission – Criteria 2.2, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, and 2.12 (Medium Impact Rating)**

Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are applicable to Transmission Owners and Operators.

Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The 1000 MVARs value used in this criterion was a value deemed reasonable for the purpose of determining criticality by the standards drafting team. Criterion 2.2 is consistent with the criteria in CIP Version 4.

Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher, because these are single facility locations and would not have the same overall grid impact as higher rated Control Centers. Criterion 2.4 is consistent with the criteria in CIP Version 4.

It should be noted that if the collector bus for a generation plant, which is smaller in aggregate than the threshold set for generation in Criterion 2.1, is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface."[23] However, such a collector bus would not be considered Medium Impact because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

Criterion 2.5 includes BES Cyber Systems for facilities at the mid-range of BES Transmission with qualifications for inclusion if they are deemed highly likely to have

[23] NERC, *Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface* (Nov. 16, 2009), available at: http://www.nerc.com/files/GO-TO_Final_Report_Complete_2009Nov16.pdf.

significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the standards drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The standards drafting team:

- Excluded radial facilities that would only provide support for single generation facilities.
- Specified interconnection to at least three transmission stations or substations to ensure that the level of impact is consistent with a medium categorization.

The standard drafting team sought to: a) ensure inclusion of BES Transmission Facilities that perform high impact BES reliability operations, including those in large geographical areas where such Facilities operate above 200 kV, but below 300 kV; and b) provide a threshold based on existing technical studies that would be applicable to Facilities operating in the range of 200 kV to 499 kV (primarily 230 kV and 345 kV Facilities).

The total aggregated weighted value of 3,000 (utilized in criterion 2.5) was derived from weighted values related to three connected 345 kV lines or five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, without taking into account the line kV rating and a mix of multiple kV rated lines. This is in contrast to the similar criterion in CIP Version 4, which used a simple count of the lines above a certain voltage level.

Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, Establish and Communicate System Operating Limits, R5.1.1 and R5.1.3.

Criterion 2.7 is sourced from the NUC-001 Reliability Standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of the Nuclear Plant Interface Requirements ("NPIRs") is harmonized through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission Service Provider "for the purpose of ensuring nuclear plant safe operation and shutdown."[24] In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

Criterion 2.8 designates as Medium Impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation Owner as to the qualification of generation Facilities connected to their Transmission systems.

Criterion 2.9 designates as Medium Impact those BES Cyber Systems for those SPS, RAS, or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.[25]

Criterion 2.10 designates as Medium Impact those BES Cyber Systems for systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The standards drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding ("UFLS") systems and undervoltage load shedding ("UVLS") systems that would be subject to a

[24] NERC Reliability Standard NUC-001-2.1 — Nuclear Plant Interface Coordination, available at: http://www.nerc.com/page.php?cid=2|20.
[25] NERC Glossary of Terms at p. 63.

regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more.

Criterion 2.12 categorizes as Medium Impact those BES Cyber Systems used by and at Control Centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact. Because Control Center is a defined term, Criterion 2.12 is only applicable to the extent that a Control Center meets the standard set in the proposed definition. Control Centers that are used to perform certain functional obligations of a Transmission Operator are categorized as high impact under criterion 1.3. All other Control Centers used to perform the functional obligations of the Transmission Operator, not otherwise categorized as high impact, are categorized as Medium Impact under Criterion 2.12.

Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Criterion 3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

- **Restoration Facilities (Low Impact Rating)**

Criterion 3 would require that all remaining BES Cyber Systems (not included under Criterion 1 or Criterion 2) be designated as Low Impact. For example, under Criterion 3.4, restoration facilities are considered as Low Impact. However, such an assignment will not relieve asset owners of all CIP-related responsibilities, as would have been the case under CIP-002-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in CIP Version 4). With the Low Impact categorization, restoration facilities will be protected in the areas of cybersecurity awareness, physical security controls, and electronic access control, and will have obligations under CIP-003-5 regarding incident response to Cyber Security Incidents.

Restoration facilities are needed in the event of a partial or complete shutdown of facilities not used for daily activities. Notably, EPAct 2005 does not authorize NERC or the Commission to order the construction of additional generation facilities.[26] Thus, consistent with EPAct 2005, assigning a Low Impact rating to restoration facilities appropriately balances the need for timely restoration response with focused requirements for these particular types of facilities.[27]

In addition, there is no mandatory requirement that a Responsible Entity have specific restoration facilities essential to BES reliability, including Blackstart Resources and Cranking Paths. Therefore, it is imperative that NERC continues to promote availability of such resources.

[26] 16 USCS § 824o(i)(2).
[27] *See* Guidelines and Technical Basis section of CIP-002-5.

- **Control Centers (Low Impact Rating)**

Under Criterion 3.1, certain Control Centers have been designated as Low Impact, according to the impact of the Control Centers on the reliability of the BES. During the development process, several commenters noted that the proposed definition for "Control Center" would include some facilities that had very little impact on BES reliability. For example, the Control Center for a BA with a scope of less than 1500 MW has a reliability impact similar to the control system managing a generating plant of roughly the same size. Since the generating plant control system does not meet the criteria to be classified as a Medium Impact BES Cyber System, it is inconsistent to require that the BA Control Center be held to a higher impact level solely because it is a Control Center. Still, at the Low Impact rating, there are requirements for electronic perimeter protections required in proposed CIP-003-5, and the concept of "mutual distrust" attaches even to Low Impact BES Cyber Systems, which utilize either routable or dial-up communications.

c. New Proposed Reliability Standards CIP-010-1and CIP-011-1.

Proposed CIP-010-1 is a new standard that contains the configuration change management and vulnerability assessment requirements previously defined across several CIP standards in prior versions. The purpose of CIP-010-1 is to prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

Similarly, proposed CIP-011-1 is a new standard that defines information protection requirements previously defined across many standards in previous versions. The purpose of CIP-011-1 is to prevent unauthorized access to BES Cyber System Information by specifying

information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

d. Modifications to the Glossary of Terms used in NERC Reliability Standards

In proposed CIP Version 5, NERC also introduces and seeks approval of 15 newly defined terms,[28] and makes modifications to four existing definitions in Glossary of Terms used in NERC Reliability Standards.[29] The newly defined terms reduce the variable application of many existing concepts from previous CIP versions. For example, the term "Control Center" is defined under CIP Version 5, although "control center" has been used since CIP Version 1 standards were approved, and the term has been subject to differing interpretations by implementing entities.

e. Enforceability of the Proposed CIP Version 5 Reliability Standards

The proposed CIP Version 5 standards are designed to be clear and unambiguous. Indeed, CIP-002-05 was modified to address commission directives in Orders No. 706. Proposed CIP-003-5 through CIP-009-5 are generally consistent with the organization of Commission-approved CIP Versions 1 through 4. New proposed standards CIP-010-1 and CIP-011-1 also address Commission concerns and further enhance BES reliability.

In addition, the "Guidelines and Technical Basis" set forth in the CIP Version 5 standards provides Responsible Entities with sufficient information to understand their compliance obligations. The Commission should, therefore, approve CIP Version 5 as clearly enforceable.

---

[28] 1) BES Cyber Asset, 2) BES Cyber System, 3) BES Cyber System Information, 4) CIP Exceptional Circumstance, 5) CIP Senior Manager, 6) Control Center, 7) Dial-up Connectivity, 8) Electronic Access Control or Monitoring Systems ("EACMS"), 9) Electronic Access Point ("EAP"), 10) External Routable Connectivity, 11) Intermediate System, 12) Physical Access Control Systems ("PACS"), 13) Protected Cyber Assets ("PCA"), 14) Interactive Remote Access, and 15) Reportable Cyber Security Incident.

[29] 1) Cyber Assets, 2) Cyber Security Incident, 3) Electronic Security Perimeter, and 4) Physical Security Perimeter. Available at: http://www.nerc.com/docs/standards/sar/CIP_V5_Definitions_clean_4_(2012-1024-1613).pdf.

f. Violation Risk Factor and Violation Severity Level Assignments

On June 29, 2011, the Commission issued a letter order approving the VRFs and VSLs for CIP Versions 2 and 3.[30] At that time, the CIP Version 4 standards were still pending before FERC. On April 19, 2012, FERC issued a final rule approving the CIP Version 4 standards, and also approving the CIP Version 4 VRFs and VSLs, with several modifications. [31]

CIP Version 4 VSLs and VRFs served as a basis for the new CIP Version 5 VRFs and VSLs. For those requirements from CIP Version 4 that were retained in CIP Version 5 (*see* mapping document included in **Exhibit F**) NERC provides a VRF and VSL Commission Guideline Analysis, included as **Exhibit E**. NERC also proposes several new VRFs and VSLs for CIP Version 5 standards developed using the Commission guidelines.

Detailed explanations for these VRF and VSL assignments are also included in the VRF and VSL Commission Guideline Analysis in **Exhibit E**.

g. NERC Reliability Standards Development Procedure

NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of the NERC Rules of Procedure and the NERC Standard Processes Manual, which is Appendix 3A to the NERC Rules of Procedure. In its ERO Certification Order, the Commission found that NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards and thus satisfies certain of the criteria for approving Reliability Standards.

---

[30] *Letter Order Re: Violation Risk Factors and Violation Severity Levels for Version 2 and Version 3 Critical Infrastructure Protection Reliability Standards*, Docket Nos. RD10-6-001 and RD09-7-003 (June 29, 2011)

[31] *Final Rule, Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (April 19, 2012) ("Order No. 761").

The work culminating in this filing originated in FERC Order No. 706, which directed the ERO to develop modifications to Standard CIP-002-1 Cyber Security – Critical Cyber Asset Identification to address concerns regarding: (1) the need for ERO guidance regarding the risk-based assessment methodology; (2) the scope of critical assets and critical cyber assets; (3) internal, management approval of the risk-based assessment; (4) external review of critical assets identification; and (5) interdependency analysis.[32]

Prior to the development of the proposed CIP Version 5 Reliability Standards, the standard drafting team developed the CIP-002-2 through CIP-009-2 standards to comply with the near-term, specific directives of FERC Order No. 706. That version of the standards was approved by FERC on September 30, 2009, with additional directives to be addressed within 90 days of the order.[33] In response, the standard drafting team developed the CIP-003-3 through CIP-009-3 standards, which were approved by FERC in March 2010.[34]

The standard drafting team for CIP Version 4 limited the scope of requirements in the development of CIP-002-4 through CIP-009-4 as an interim step to address the more immediate concerns raised in Order No. 706.[35] CIP-002-4 included "bright-line criteria" used to identify Critical Assets in lieu of an entity-defined risk-based assessment methodology. On April 19, 2012, FERC issued Order No. 761 approving CIP Version 4. In that order, the Commission also directed NERC to file the next version addressing all remaining directives from Order No. 706 by March 31, 2013.[36]

---

[32] *Id*. at P 236.
[33] *Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (September 30, 2009) ("September 30, 2009 Order").
[34] *Order on Compliance*, 130 FERC ¶61, 271 (March 31, 2010) ("March 31, 2010 Order").
[35] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058, at P 236 (2012) ("Order No. 761").
[36] Order No 761 at P 111.

A phased approach to meeting the directives in FERC Order No. 706 has consistently built upon prior versions of the CIP-002 through CIP-009 standards to enhance the reliability of the Bulk Electric System. Accordingly, the proposed CIP Version 5 standards build on the CIP-002-4 establishment of uniform criteria for the identification of assets.

The standards development process is open to any person or entity with a legitimate interest in the reliability of the Bulk Power System. NERC considers the comments of all stakeholders, and a vote of stakeholders and the NERC Board of Trustees is required to approve a Reliability Standard before the Reliability Standard is submitted to the Commission for approval. The proposed CIP Version 5 standards were approved by the NERC Board of Trustees on November 16, 2012.

V. CIP VERSION 5 SATISFIES ALL FERC DIRECTIVES AND CONCERNS

The Commission, in Order Nos. 706 and 761, approved prior versions the CIP standards and directed NERC to address numerous issues in future versions of the CIP standards. Specifically, in Order No. 761, the Commission also directed NERC to consider the application of the NIST Risk Management Framework, regional perspective, and connectivity in developing CIP Version 5. As discussed below, proposed CIP Version 5 includes enhancements to the Commission-approved CIP standards that are responsive to all remaining Commission directives and concerns.

a. Order No. 706 Directives

In Order No. 761, the Commission directed NERC to develop the CIP Version 5 standards to address all remaining directives from Order No. 706 by March 31, 2013.

> We recognize, as numerous commenters discuss, that the current schedule for completing CIP Version 5 is aggressive. We also understand that the

> volume of industry discussion is high and we agree that industry input should not be artificially rushed or curtailed. In its reply comments, NERC indicated that it anticipates filing the Version 5 CIP Reliability Standards by the third quarter of 2012. Accordingly, to allow for sufficient time beyond what NERC estimates, we establish a deadline that is 6 months from the end of the third quarter of 2012 (i.e., March 31, 2013). NERC must also submit reports at the beginning of each quarter in which the ERO is to explain whether it is on track to meet the deadline and describe the status of its standard development efforts."[37]

The proposed CIP Version 5 addresses all applicable Commission directives in Order No. 706, and **Exhibit H** provides a summary response for each of the Commission's directives and guidance statements.

b. Application of NIST Risk Management Framework

In Order No. 706, the Commission directed NERC to apply applicable features of the NIST Risk Management Framework to CIP Version 5. Order No. 761 also urged NERC to review relevant NIST standards for guidance in developing effective cybersecurity standards for the electric industry.[38]

Pursuant to Order Nos. 706 and 761, the standards drafting team for CIP Version 5 reviewed the NIST Risk Management Framework and incorporated five key features:

1. ensuring that all BES Cyber Systems associated with the Bulk Power System, based on their function, receive some level of protection;

2. a tiered approach to security controls, which specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk Power System;

3. tailoring protection to the mission and operating environment (*e.g.*, communications connectivity) of the cyber systems subject to protection;

[37] Order No 761 at P 111.
[38] Order No. 761 at P 94 (The Commission stated: "We view the approach of incorporating these applicable features of the NIST Framework into the CIP Reliability Standards as a positive step in improving cyber security for the Bulk-Power System.").

4. the concept of the BES Cyber System, and

5. the inclusion of "Assess" and "Monitor" steps by adding requirement language for "identifying, assessing, and correcting" deficiencies in controls as part of the requirements' expected performance.

Proposed CIP Version 5 achieves reliability excellence by incorporating the above features of the NIST Risk Management Framework.[39] The NIST Risk Management Framework defines "risk" as a measure of the extent to which an entity is threatened by a potential circumstance or event, and a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.[40] NIST further explains that this risk management process "changes the traditional focus of [Certification and Accreditation] as a static, procedural activity to a more dynamic approach that provides the capability to more effectively manage information system-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions." [41]

Indeed, both NERC and the Commission have acknowledged the importance of identifying and correcting risks to the Bulk Power System. NERC has stated in prior proceedings that, "Reliability excellence is achieved through the ongoing identification, correction and prevention of reliability *risks*, both big and small. Yet, accountability for reliability excellence is broader than just penalizing violations."[42] In its order accepting NERC's

[39] In 2013, NERC Compliance Operations will be revising all Reliability Standard Audit Worksheets ("RSAW"), including the RSAWs for CIP Version 5. To incorporate the NIST Risk Management Framework into CIP Version 5, the standards drafting team discussed the importance of synchronizing the "identify, assess, and correct" language with associated RSAWs, and developed a sample RSAW for proposed CIP-006-5. The sample RSAW was posted for informational purposes only and the Commission is *not* being asked to approve the sample RSAW, which is available at: http://www.nerc.com/page.php?cid=3|404.
[40] *Id*. at FN 8.
[41] NIST, Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach*, at p. 2.
[42] *NERC Petition Requesting Approval of New Enforcement Mechanisms and Submittal of Initial Find Fix and Track (FFT) Informational Filing*, at p.1, Docket No. RC11-600 (2011) (*Emphasis added*).

Find, Fix, and Track approach to enforcement, FERC agreed with NERC's assessment, stating that it "applaud[s] NERC for proposing a format that will help it and the Regional Entities focus their resources on issues that pose the greatest *risks* to reliability."[43]

Consistent with the NIST Risk Management Framework and the Commission's guidance in prior orders, the CIP Version 5 standard drafting team incorporated within several standards (*e.g.*, proposed CIP-003-5) a requirement that Responsible Entities implement cyber policies in a manner to "identify, assess, and correct" deficiencies. The "identify, assess, and correct" language is included as a performance expectation in the requirements, not as an enforcement component. An example of this language follows below:

> Each Responsible Entity shall implement**,** in a manner that identifies, assesses, and corrects deficiencies**,** one or more documented processes (or program, etc., as specified by the requirement) that collectively include each of the applicable items in [the referenced table].

The implementation of certain CIP Version 5 requirements in a manner to "identify, assess, and correct" deficiencies emulates the *FERC Policy Statement on Penalty Guidelines*, where the Commission clarified that "[a]chieving compliance, not assessing penalties, is the central goal of the Commission's enforcement efforts."[44] The *FERC Policy Statement on Penalty Guidelines* also highlights the characteristics of an effective organization compliance program, which include "(1) [exercising] due diligence to prevent and detect violations; and (2) [promoting] an organizational culture that encourages a commitment to compliance with the law."[45]

---

[43] *Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing*, 138 FERC ¶61,193 (March 15, 2012) at P 40. (*Emphasis added*).
[44] *Revised Policy Statement on Penalty Guidelines*, 132 FERC ¶ 61,216 at P 110 (2010).
[45] *Id*.

The *FERC Policy Statement on Penalty Guidelines* further explains that the promotion of an "organizational culture that encourages a commitment to compliance" requires an organization to establish standards and procedures to prevent and detect violations.[46] Therefore, the organization's governing authority should be knowledgeable of the compliance program and exercise reasonable oversight with respect to the implementation and effectiveness of the compliance program by assigning a specific individual(s) within high-level personnel overall responsibility for the compliance program. To that end, the *FERC Policy Statement on Penalty Guidelines* requires organizations to "periodically assess the *risk* of violations and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of violations identified through this process."[47]

This creation of an organizational culture of compliance, with an emphasis on assessing risk, is consistent with the approach taken in CIP Version 5 and avoids a "check-the-box" mind-set that would consume valuable industry resources without any benefit to BES reliability. For example, proposed CIP-003-5 requires Responsible Entities to identify a CIP Senior Manager. Rather than verifying that a single name appears on a document, CIP-003-5 seeks to verify that the *purpose* of the requirement is being achieved – that a CIP Senior Manager is indeed managing the implementation of CIP Version 5.

This is an example of how the lessons learned over the past four years are reflected in CIP Version 5, which includes high-level personnel (*i.e.*, the CIP Senior Manager) assessing risk. Thus, CIP Version 5 builds on the implementation and audit lessons from prior versions and is consistent with the *FERC Policy Statement on Penalty Guidelines*.

---

[46] FERC Penalty Guidelines, Chapter 1, Part B - Disgorging Gain From Violations and Effective Compliance Program, §1B2.1, Effective Compliance Program.
[47] http://www.ferc.gov/whats-new/comm-meet/2010/091610/M-1.pdf. (*Emphasis added*).

c. Regional Perspective

In Order No. 761, the Commission expressed a concern that a lack of a regional review for the identification of cyber assets might result in a reliability gap. However, CIP Version 4 adopted "bright-line" criteria for Critical Asset identification, which the Commission agreed may obviate the need for a regional review.[48] Building on the CIP Version 4 approach, the proposed CIP-002-5, Attachment 1 – Impact Rating Criteria was developed in consideration of a Wide Area view and eliminates the need for regional review.

However, in the event that there are BES Cyber Systems that NERC and the Regional Entities determine should be treated as critical, but do not meet the CIP Version 5 criteria, NERC has the authority under Section 810 of the NERC Rules of Procedure to issue a Level 2 (Recommendation) or Level 3 (Essential Action) notification. Section 810 of the NERC Rules of Procedure provides the following:

> **810. Information Exchange and Issuance of NERC Advisories, Recommendations and Essential Actions**
>
> **1.** Members of NERC and Bulk Power System owners, operators, and users shall provide NERC with detailed and timely operating experience information and data.
>
> **2.** In the normal course of operations, NERC disseminates the results of its events analysis findings, lessons learned and other analysis and information gathering to the industry. These findings, lessons learned and other information will be used to guide the Reliability Assessment Program.
>
> **3.** When NERC determines it is necessary to place the industry or segments of the industry on formal notice of its findings, analyses, and recommendations, NERC will provide such notification in the form of specific operations or equipment Advisories, Recommendations or Essential Actions:

[48] Order No. 761 at P PP 103 and 104 ("We believe that there is less need for external review where application of bright line criteria results in an objective, consistently applied approach to the identification of cyber assets.").

3.1 Level 1 (Advisories) – purely informational, intended to advise certain segments of the owners, operators and users of the Bulk Power System of findings and lessons learned;

3.2 Level 2 (Recommendations) – specific actions that NERC is recommending be considered on a particular topic by certain segments of owners, operators, and users of the Bulk Power System according to each entity's facts and circumstances;

3.3 Level 3 (Essential Actions) – specific actions that NERC has determined are essential for certain segments of owners, operators, or users of the Bulk Power System to take to ensure the reliability of the Bulk Power System. Such Essential Actions require NERC Board approval before issuance.

4. The Bulk Power System owners, operators, and users to which Level 2 (Recommendations) and Level 3 (Essential Actions) notifications apply are to evaluate and take appropriate action on such issuances by NERC. Such Bulk Power System owners, operators, and users shall also provide reports of actions taken and timely updates on progress towards resolving the issues raised in the Recommendations and Essential Actions in accordance with the reporting date(s) specified by NERC.

5. NERC will advise the Commission and other Applicable Governmental Authorities of its intent to issue all Level 1 (Advisories), Level 2 (Recommendations), and Level 3 (Essential Actions) at least five (5) business days prior to issuance, unless extraordinary circumstances exist that warrant issuance less than five (5) business days after such advice. NERC will file a report with the Commission and other Applicable Governmental Authorities no later than thirty (30) days following the date by which NERC has requested the Bulk Power System owners, operators, and users to which a Level 2 (Recommendation) or Level 3 (Essential Action) issuance applies to provide reports of actions taken in response to the notification. NERC's report to the Commission and other Applicable Governmental Authorities will describe the actions taken by the relevant owners, operators, and users of the Bulk Power System and the success of such actions taken in correcting any vulnerability or deficiency that was the subject of the notification, with appropriate protection for Confidential Information or Critical Energy Infrastructure Information.

Level 3 Alerts allow NERC (following NERC Board of Trustees approval) to require that specific actions that NERC has determined are essential for certain segments of owners, operators, or users of the Bulk Power System be taken to ensure the reliability of the Bulk Power

System. Additionally, Rule 810 states that Bulk Power System owners, operators, and users to which Level 2 (Recommendations) and Level 3 (Essential Actions) Alerts apply shall provide reports of actions taken and timely updates on progress towards resolving the issues raised in the Recommendations and Essential Actions consistent with reporting dates specified by NERC. Therefore, NERC can use Level 2 Recommendations and Level 3 Essential Actions to address assets that NERC and Regional Entities later determine should be treated as a higher impact level than would otherwise be categorized under the CIP Version 5 impact criteria.

d. Connectivity

In Order No. 761, the Commission noted that the criteria adopted for the purpose of identifying assets under CIP-002-5 should include a cyber asset's "connectivity."[49]

> We also agree with SPP RE that the CIP Reliability Standards should consider communication paths between a given cyber asset and other assets that support a reliability function. As noted by SPP RE, cyber security standards that categorize cyber systems based upon the size or scope of the assets that they control "fail to consider the interconnectivity of the BES Cyber Systems and the potential for a small control center system to be used as a vector of attack against a larger control center system." …The Commission agrees that cyber connectivity is important to address when developing future versions of the CIP Reliability Standards. That being said, we acknowledge the concern of Trade Associations that the "connectivity" and "weakest link" concepts could possess different meanings to various stakeholders. Thus, addressing connectivity should include reaching a common understanding of the term. Further, we understand and agree with the Trade Associations' concern that protection should be applied in a reasonable manner.

Order No. 761at P 88. (Citations omitted).

The CIP Version 5 standards drafting team agreed with the Commission that connectivity is a relevant consideration for the application of cybersecurity controls, and comprehensively incorporated connectivity throughout CIP Version 5 by utilizing a "mutual distrust" posture, by

[49] Order No. 761at PP 88 - 91.

eliminating any connectivity-based exclusions under CIP-002-5, Attachment 1, and thorough inclusion of connectivity and other characteristics in the applicability of the CIP Version 5 requirements.

If connectivity were used as an initial impact criterion, it could potentially expand the CIP Version 5 standards to a significant number of non-jurisdictional assets, such as interconnected distribution systems (*e.g.*, smart grid), market systems, and business systems. Furthermore, using connectivity as a basis for categorizing impact could continue the unintended consequences related to eliminating connectivity in certain circumstances, resulting in a decreased situational awareness ability and increased costs associated with not being able to readily gather data or perform necessary maintenance. Accordingly, proposed CIP Version 5 addresses the Commission's concerns related to connectivity throughout the proposed CIP Version 5 standards.

Specifically, the standards drafting team determined that, while connectivity may affect the ability to remotely access a BES Cyber System, the impact to BES reliability is determined by the electrical characteristics of a BES asset, not by the connectivity of an associated BES Cyber System. This does not, however, diminish the importance of connectivity, as the applicability of requirements consider connectivity in proposed CIP-003-5 through CIP-011-1.

Connectivity does not inform BES impact, even if it affects likelihood or risk. The role connectivity plays in affecting likelihood or risk of access or compromise to a Cyber Asset associated with a BES Cyber System is a significant reason why connectivity is more appropriately considered in the applicability of requirements throughout the CIP Version 5 standards. To illustrate, the loss of 1000 MW of Load would have the same impact to the BES regardless of whether it stemmed from the compromise of an asset's BES Cyber System (that is

routably connected) or from the compromise of an asset's BES Cyber System that has no connectivity whatsoever. The likelihood or risk of compromise to the former is arguably higher, but the impact to BES reliability—in the instant case, 1000 MW—would be the same under both circumstances. Indeed, the likelihood or risk of compromise *is* addressed by the applicability of additional requirements where routable connectivity is used, not by characterizing the BES Cyber System to a higher impact category.

In addition, Order No. 761 encourages NERC to consider the benefits of a "mutual distrust" posture as directed by the Commission in Order No. 706.[50]

> Recognizing the importance of addressing cyber connectivity in future versions of the CIP Reliability Standards, we encourage NERC to consider the benefits of a "mutual distrust" posture, or similar strategies, put forth by the ISO/RTO Council and as directed by the Commission in Order No. 706. In Order No. 706, the Commission used the term "mutual distrust" to denote how "outside world" systems are treated by those inside the control system. Specifically, a mutual distrust posture requires each responsible entity that has identified critical cyber assets to protect itself and not trust any communication crossing an electronic security perimeter, regardless of where that communication originates.
>
> Applying electronic security perimeter protections "of some form" to bulk electric system cyber systems covered by the CIP Reliability Standards will support the adoption of a "mutual distrust" posture. This posture will encourage asset owners and operators to employ sound network architectural design, thus segmenting their systems into distinct security zones protected by managed interfaces that will allow only trusted access. The managed interfaces, or electronic security perimeter access points, are intended to restrict or prohibit network access and information flow to bulk electric system cyber systems covered by the CIP Reliability Standards from unidentified, unauthenticated, and unauthorized connectivity to ensure security. Multiple electronic security perimeters can be established to protect cyber assets and adopted as part of a defense in depth strategy to limit the propagation of a threat.

Order No. 761at PP 89-90. (Citations omitted).

[50] Order No. 761 at P 89.

"Mutual distrust" signifies how "external" cyber assets are treated by those cyber assets local to the BES Cyber System. "Mutual distrust" also requires each Responsible Entity that has identified BES Cyber Systems to protect against any communication crossing an ESP, regardless of where the communication originates. As noted above, BES Cyber Systems of all impact levels, with routable or dial-up connectivity, are required to be within a security zone that provides protection from outside influences using a posture of "mutual distrust". Since, under CIP Version 5, BES Cyber Systems for "High-Medium-Low" impact levels are now required to implement electronic perimeter protections "of some form" for all routable and dial-up communications, the "mutual distrust" posture is implemented for all BES Cyber Systems.

The Commission also stated in Order No. 761 that, "we support the elimination of the blanket exemption for non-routable connected cyber systems as highlighted in NERC's comments. A continued blanket exemption in CIP Version 5 would not adequately address risk."[51] The Commission added that, "we support the concept of applying electronic security perimeter protections 'of some form' to all bulk electric system cyber systems."[52]

The standards drafting team for CIP Version 5 agreed that applying ESP protections "of some form" to BES Cyber Systems supports the "mutual distrust" posture even for low impact BES Cyber Systems that use routable or dial-up communications.[53] Ultimately, using "mutual distrust" is equally efficient and effective as considering connectivity as a basis for informing the impact categorization of BES Cyber Systems. Thus, the implementation of a "mutual distrust" posture for high, medium, and low impact BES Cyber Systems, connected using routable or dial-up communications, improves security above what is required under CIP Versions 1 through 4.

[51] Order No. 761 at P 86.
[52] Order No. 761 at 87.
[53] Order No. 761 at 87.

Moreover, in response to stakeholder comments during development, proposed CIP-003-5, requirement R2, was added so that Responsible Entities are required to document and implement perimeter-type security controls to segment Low Impact BES Cyber Systems from public (or other less trusted) network zones and to prevent access to an aggregation of low impact BES Cyber Systems. The intent of this enhancement is to mitigate the risks associated with the aggregation of Low Impact BES Cyber Systems, in order to avoid a potential increase in the overall level of impact to the BES.

Additionally, because electronic perimeter protections are now required for BES Cyber Systems (with specific requirements for High and Medium impact categories and programmatic requirements for Low impact) CIP Version 5 adequately addresses connectivity.

VI. SUMMARY OF THE RELIABILITY STANDARD DEVELOPMENT PROCEEDINGS

The development record for proposed CIP Version 5 is summarized below. **Exhibit D** contains the Consideration of Comments Reports created during the development of the Reliability Standards. **Exhibit F** contains the complete record of development for proposed CIP Version 5.

Three drafts of CIP Version 5 were posted for industry comment during the development period before being approved during recirculation ballot in draft 4. The first draft of the standards was posted for comment from November 7, 2011, through January 6, 2012. This period included twelve initial ballots (one each for the ten standards in proposed CIP Version 5, the associated definitions, and the implementation plan) that were conducted from December 16,

2011, through January 6, 2012, and they resulted in industry approvals between 22.09 and 42.06 percent.[54]

The CIP Version 5 standards drafting team then focused its efforts on preparing the next draft in response to comments received. The second draft of CIP Version 5 was posted for comment from April 12 through May 21, 2012. This period included successive ballots that were conducted from May 11 through May 21, 2012, and resulted in industry approvals between 37.37 and 67.19 percent.[55]

The standards drafting team made further refinements in an effort to address unresolved issues and to develop industry consensus in response to the second posting. The third draft of CIP Version 5 was posted for comment from September 11 through October 10, 2012. This period included successive ballots that were conducted from October 1 through October 10, 2012, and they resulted in industry approvals between 74.85 and 94.00 percent.[56]

Recirculation ballots, which constituted draft four of CIP Version 5, were conducted from October 26 through November 5, 2012, and resulted in industry approvals between 78.59 and 95.53 percent.[57] The NERC Board of Trustees approved the proposed CIP Reliability Standards on November 16, 2012.

VII. CIP VERSION 5 IMPLEMENTATION PLAN

The proposed CIP Version 5 implementation plan was overwhelmingly passed by the registered ballot body with 94.91% approval. Yet, until the Commission takes action on CIP Version 5, there may be uncertainty for Responsible Entities transitioning from CIP Version 3 to

[54] http://www.nerc.com/docs/standards/sar/Standards_Announcement_2008-06_ballot_results_010612_final.pdf.
[55] http://www.nerc.com/docs/standards/sar/Succ_Ballot_Results_2008-06_CIPV5_20120522_060612.pdf.
[56] http://www.nerc.com/docs/standards/sar/Succ_Ballot_Results_2008-06_CIPV5_20121012_rev1.pdf.
[57] http://www.nerc.com/docs/standards/sar/2008-06_CIPV5_Recirc_NPB_Results_Announc_110712_final.pdf.

CIP Version 4 to CIP Version 5. This uncertainty stems from industry stakeholders not knowing whether the Commission will act on CIP Version 5 prior to the CIP Version 4 effective date, April 1, 2014, which would trigger compliance obligations for Responsible Entities.

NERC will work with the industry on any potential implementation challenges. However, language included in the proposed implementation plan could help alleviate some of the uncertainty among industry. This language provides:

> Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.

With prompt Commission approval of the CIP Version 5 standards and the associated implementation plan, CIP Version 3 will be extended until CIP Version 5 becomes operative, bypassing implementation of CIP Version 4.

While there is significant support for the CIP Version 5 implementation plan, NERC stands ready to implement CIP Version 4, if the Commission does not act before April 1, 2014. NERC will work with industry stakeholders to address any transition issues as they arise; although NERC urges the Commission to approve the proposed CIP Version 5 standards and the associated implementation plan as soon as possible.

Prompt approval of CIP Version 5 will provide much needed clarity for Responsible Entities transitioning from CIP Version 3 to CIP Version 4 to CIP Version 5, and the improvements contained in CIP Version 5 will provide an enormous benefit to BES reliability. However, if the Commission determines that prompt approval of CIP Version 5 is infeasible, NERC respectfully requests that a timeframe for anticipated action be provided, so that NERC and industry may develop a reasonable plan to move from CIP Version 3 to CIP Version 4 to CIP Version 5.

VIII. CONCLUSION

For the reasons set forth above, NERC respectfully requests that the Commission approve the proposed CIP Version 5 Reliability Standards and related documents in accordance with this petition and Order Nos. 706 and 761.

Respectfully submitted,

/s/ Willie L. Phillips

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
willie.phillips@nerc.net

Counsel for North American Electric Reliability Corporation

Dated: January 31, 2013

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 31st day of January, 2013.

/s/ Willie L. Phillips
Willie L. Phillips
Attorney for North American Electric Reliability Corporation

Exhibit A

1.) Proposed CIP Version 5 Reliability Standards submitted for Approval
2.) Associated Modifications to the Glossary of Terms used in NERC Reliability Standards

Exhibit A

1.) Proposed CIP Version 5 Reliability Standards submitted for Approval

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-5

3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-5:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

1. **24 Months Minimum** – CIP-002-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required CIP-002-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.

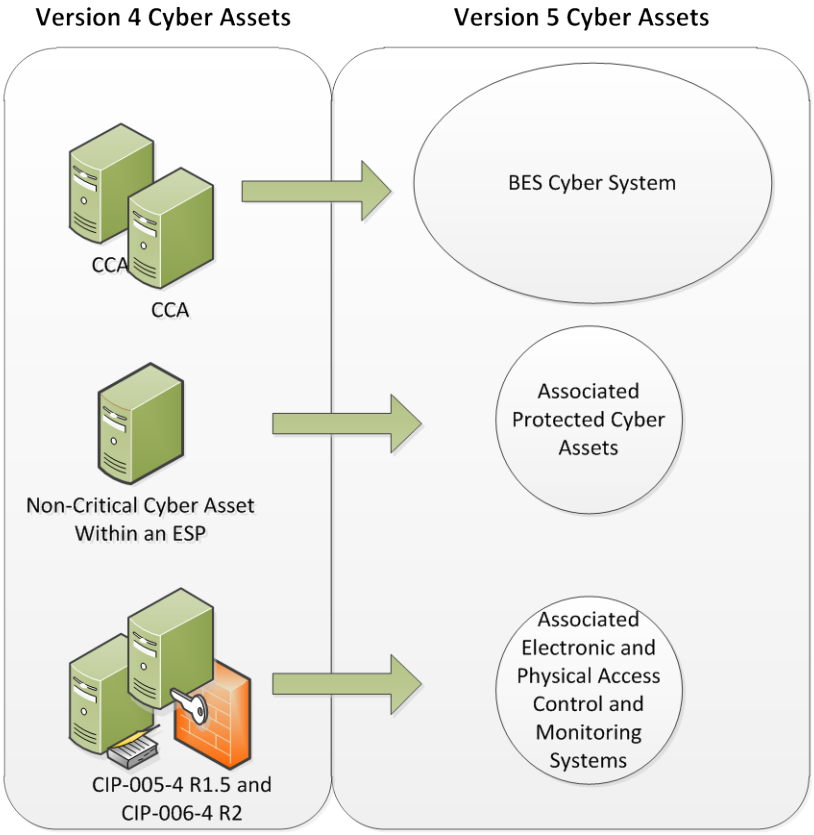

In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and

scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS") – Examples include: Electronic Access Points, Intermediate Devices, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")– Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA") – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;
ii. Transmission stations and substations;
iii. Generation resources;
iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

R2. The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5 - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)

- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

<u>High Impact Rating (H)</u>

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some

of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, BAs, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of BAs with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1. .

- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the

backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.

  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

  - 230 kV –> 700 MVA

  - 345 kV –> 1,300 MVA

  - 500 kV –> 2,000 MVA

  - 765 kV –> 3,000 MVA

  In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

  - For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities

would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.

- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as

specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.

- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric

System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

<u>Low Impact Rating (L)</u>

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to

restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.

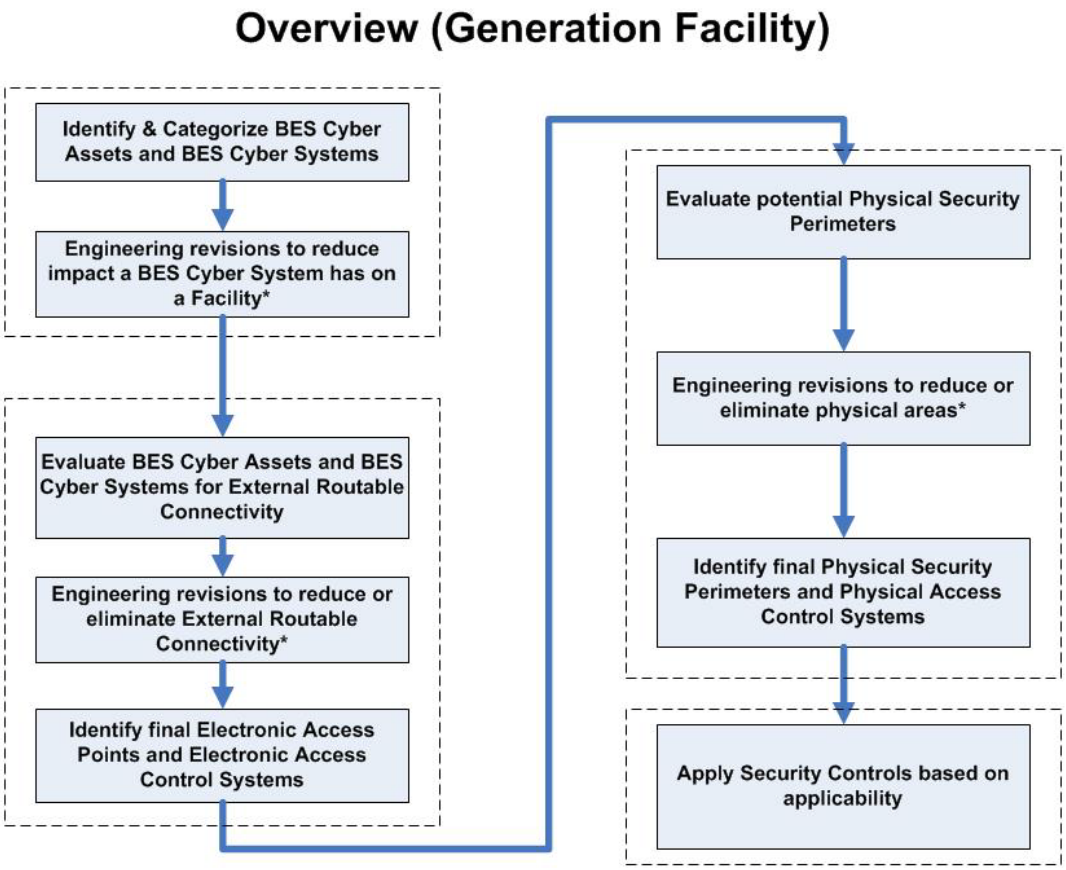

* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3.	Update

		Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

~~4.~~1. **Title:** Cyber Security — ~~Critical~~BES Cyber ~~Asset Identification~~System Categorization

~~5.~~2. **Number:** CIP-002-~~4~~5

~~6. **Purpose:** NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.~~

~~These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.~~

~~Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.~~

~~Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.~~

3. **Purpose:** To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

~~7.~~4. **Applicability:**

~~4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:~~

4.1. ~~Reliability~~ **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. **Balancing Authority**

4.1.2. **Distribution Provider that owns** one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

~~7.1.1.~~ Interchange Coordinator~~.~~

~~**7.1.2.** Balancing Authority.~~

~~4.1.3~~4.1.5. or Interchange Authority~~.~~

~~**7.1.3.** Transmission Service Provider.~~

4.1.6. Reliability Coordinator

~~4.1.5~~4.1.7. Transmission ~~Owner.~~Operator

~~**7.1.4.** **Transmission** Operator.~~

~~4.1.7~~4.1.8. ~~Generator~~ Owner~~.~~

~~**7.1.5.** Generator Operator.~~

~~**7.1.6.** Load Serving Entity.~~

~~**7.1.7.** NERC.~~

~~**7.1.8.** Regional Entity.~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

~~**4.2.**~~**4.2.3. Exemptions:** The following are exempt from Standard CIP-002-~~4:~~5:

~~**4.2.1**~~**4.2.3.1.** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~**4.2.2**~~**4.2.3.2.** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.3~~**4.2.3.3.** ~~In nuclear plants, the~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.-R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective ~~Date:~~ ~~The~~ Dates:

1. **24 Months Minimum** – CIP-002-5 shall become effective on the later of July 1, 2015, or the first ~~day of the eighth~~ calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory ~~approvals have been received (or the Reliability Standard otherwise becomes effective~~ approval.

~~5.~~2. In those jurisdictions where no regulatory approval is required CIP-002-5 shall become effective on the first day of the ninth calendar quarter ~~after BOT adoption in those jurisdictions where regulatory approval is not required)~~following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.

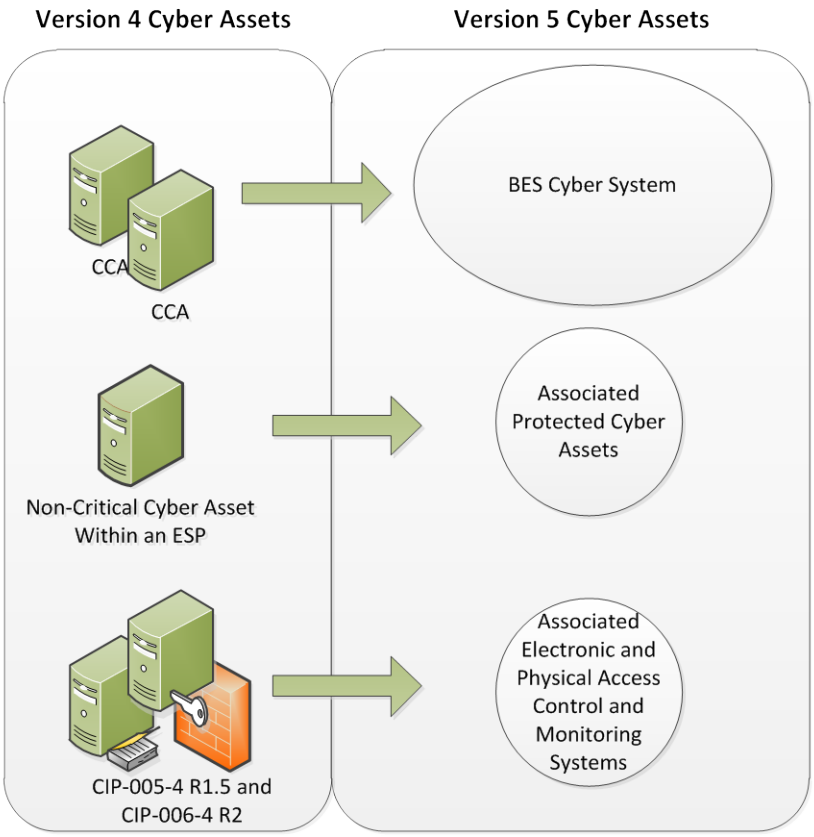

In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and

scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS") – Examples include: Electronic Access Points, Intermediate Devices, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")– Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA") – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

R1. ~~Critical Asset Identification — The~~ Each Responsible Entity shall ~~develop a list of its identified Critical Assets determined~~implement a process that considers each of the following assets for purposes of parts 1.1 through ~~an annual application~~1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;
ii. Transmission stations and substations;
iii. Generation resources;
iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
v. Special Protection Systems that support the reliable operation of the ~~criteria contained~~Bulk Electric System; and
vi. For Distribution Providers, Protection Systems specified in ~~*CIP-002-*~~ Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1~~*— Critical Asset Criteria.*~~, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

R2. The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update ~~this list as necessary, and review it~~ them if there are changes identified) at least ~~annually.~~once every 15 calendar months, even if it has no identified items in Requirement R1, and

~~Critical Cyber Asset Identification — Using~~**2.2** Have its CIP Senior Manager or delegate approve the ~~list of Critical Assets developed pursuant to~~identifications required by Requirement R1~~,~~ at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall ~~develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset.~~ serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall ~~update this list as necessary, and review it at least annually.~~keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- ~~For~~ Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5 - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units ~~(including nuclear generation) at~~ at a single plant location ~~identified in Attachment 1, criterion 1.1~~, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber ~~Assets~~Systems that ~~must be considered~~meet this criterion are those shared BES Cyber ~~Assets~~Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed ~~Attachment 1, criterion 1.1.~~ 1500 MW in a single Interconnection.

~~For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:~~

- ~~The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,~~
- ~~The Cyber Asset uses a routable protocol within a control center; or,~~
- ~~The Cyber Asset is dial-up accessible.~~

~~Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)~~

~~C. Measures~~

~~**M1.** The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.~~

~~**M2.** The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.~~

~~**M3.** The Responsible Entity shall make available its records of approvals as specified in Requirement R3.~~

~~D. Compliance~~

~~9. Compliance Monitoring Process~~

~~4.1. Compliance Enforcement Authority~~

~~**9.1.1.** The Regional Entity shall serve as the Compliance Enforcement Authority with the following exceptions:~~

- ~~For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.~~
- ~~For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.~~
- ~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.~~
- ~~For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.~~

~~4.2. Compliance Monitoring and Enforcement Processes~~

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~4.3. Data Retention~~

~~**9.3.1.** The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.~~

~~**9.3.2.** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.~~

~~**4.4. Additional Compliance Information**~~

~~**9.4.1.** None.~~

~~**10. Violation Severity Levels**~~

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1~~	~~HIGH~~	~~N/A~~	~~N/A~~	~~The Responsible Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.~~	~~The Responsible Entity did not develop a list of its identified Critical Assets even if such list is null.~~
~~R2~~	~~HIGH~~	~~N/A~~	~~N/A~~	~~The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.~~ **Voltage Value of a Line**	~~The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 even if such list is null.~~ ~~OR~~ ~~A Cyber Asset essential to the operation of the Critical Asset was identified that met at least one of the bulleted characteristics in this requirement but was not included in~~

					the Critical Cyber Asset List.Weight Value per Line
R3	LOWER	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets. OR The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Cyber Assets (even if such lists are null.)less than 200 kV (not applicable)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)(not applicable)
200 kV to 299 kV					700
300 kV to 499 kV					1300
500 kV and above					0

E. Regional Variances

None identified.

~~Version History~~

~~Version~~	~~Date~~	~~Action~~	~~Change Tracking~~
~~1~~	~~January 16, 2006~~	~~R3.2 — Change "Control Center" to "control center"~~	~~03/24/06~~
~~2~~		~~Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.~~ ~~Removal of reasonable business judgment.~~ ~~Replaced the RRO with the RE as a responsible entity.~~ ~~Rewording of Effective Date.~~ ~~Changed compliance monitor to Compliance Enforcement Authority.~~	
~~3~~		~~Updated version number from -2 to -3~~	
~~3~~	~~12/16/09~~	~~Approved by the NERC Board of Trustees~~	~~Update~~
~~4~~	~~12/30/10~~	~~Modified to add specific criteria for Critical Asset identification~~	~~Update~~
~~4~~	~~1/24/11~~	~~Approved by the NERC Board of Trustees~~	
~~4~~	~~4/19/12~~	~~FERC Order issued approving CIP-002-4 (approval becomes effective June 25, 2012)~~ ~~Added approved VRF/VSL table to section D.2.~~	

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

Each group of generating units (including nuclear generation)

1.1. Generation at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8.2.6. Transmission Facilities at a single station or substation location that are identified by theits Reliability Coordinator, Planning Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission FacilitiesTransmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.10.2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the transmission system Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assetsgeneration

Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1~~.1~~ or ~~1~~2.3.

~~**1.11.** Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.~~

~~**1.12.**~~**2.9.** Each Special Protection System (SPS), Remedial Action Scheme (RAS~~)~~), or automated switching ~~system~~System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed~~.~~ or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

~~**1.13.**~~**2.10.** Each system or ~~Facility~~ group of Elements that performs automatic ~~load~~Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing ~~Under Voltage Load Shedding~~ undervoltage load shedding (UVLS) or ~~Under Frequency Load Shedding~~ underfrequency load shedding (UFLS) ~~as required by the regional~~ under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

~~**1.14.** Each control center~~Control Center or backup ~~control center~~Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the ~~Reliability Coordinator.~~

~~**1.15.**~~**2.11.** ~~Each control center or backup control center used to control generation at multiple plant locations,~~ Generator Operator for ~~any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation~~an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

~~**1.16.** Each control center~~Control Center or backup ~~control center~~Control Center used to perform the functional obligations of the Transmission Operator ~~that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.~~

2.12. ~~Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified~~not included in ~~criteria 1.1, 1.3, 1.4, or 1.13.~~ High Impact Rating (H), above.

~~**1.17.**~~**2.13.** Each ~~control center~~Control Center or backup ~~control center~~Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	**RC**	**BA**	**TOP**	**TO**	**DP**	**GOP**	**GO**
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)

- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some

of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, BAs, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of BAs with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1. .

- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the

backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.

  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

  - 230 kV –> 700 MVA

  - 345 kV –> 1,300 MVA

  - 500 kV –> 2,000 MVA

  - 765 kV –> 3,000 MVA

  In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

  - For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities

would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.

- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as

specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.

- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric

System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to

restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.

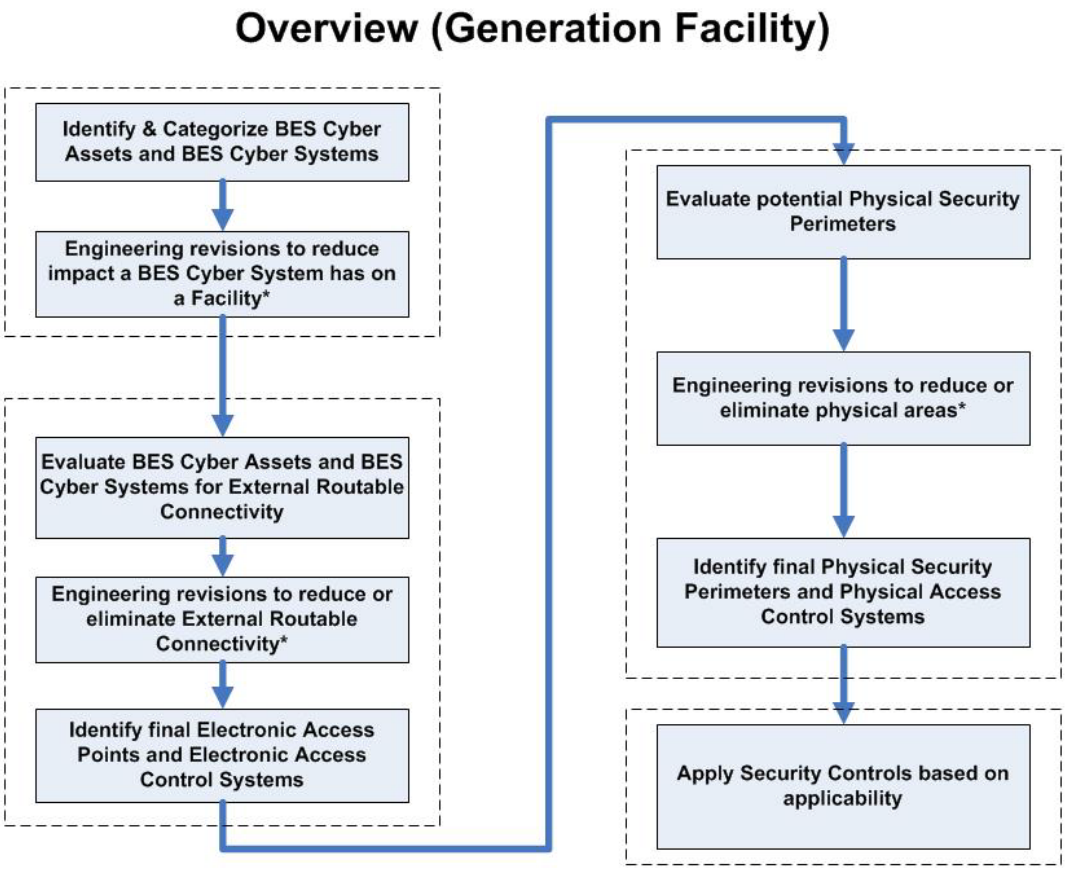

* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to	

		Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-5

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

1. **24 Months Minimum** – CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects

are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 Personnel & training (CIP-004);

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.3 Physical security of BES Cyber Systems (CIP-006);

1.4 System security management (CIP-007);

1.5 Incident reporting and response planning (CIP-008);

1.6 Recovery plans for BES Cyber Systems (CIP-009);

1.7 Configuration change management and vulnerability assessments (CIP-010);

1.8 Information protection (CIP-011); and

1.9 Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Cyber security awareness;

2.2 Physical security controls;

2.3 Electronic access controls for external routable protocol connections and Dial-up Connectivity; and

2.4 Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-5, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not

necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-5, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-5, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

Review and approval of the cyber security policy at least every 15 calendar months ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

1. **Title:** ~~———~~Cyber Security — Security Management Controls__

2. **Number:** CIP-003-~~4~~5

3. **Purpose:** ~~Standard CIP-003-4 requires that Responsible Entities have minimum~~To specify consistent and sustainable security management controls ~~in place~~that establish responsibility and accountability to protect ~~Critical~~BES Cyber ~~Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4~~Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

~~**4.1.** Within the text of Standard CIP-003-4, "Responsible Entity" shall mean:~~

4.1. ~~Reliability~~ **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

~~4.1.1~~ Interchange Coordinator~~.~~

~~**4.1.2** Balancing Authority.~~

~~4.1.3~~4.1.5 or Interchange Authority~~.~~

~~**4.1.4** Transmission Service Provider.~~

4.1.6 Reliability Coordinator

~~4.1.5~~4.1.7 Transmission ~~Owner.~~Operator

~~4.1.6~~ Transmission ~~Operator.~~

~~4.1.7~~4.1.8 ~~Generator~~ Owner~~.~~

~~**4.1.8** Generator Operator.~~

~~**4.1.9** Load Serving Entity.~~

~~**4.1.10** NERC.~~

~~**4.1.11** Regional Entity.~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first

interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

~~4.2.4~~4.2.3 Exemptions: The following are exempt from Standard CIP-003-~~4:~~5:

~~4.2.1~~4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.2~~4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.3~~4.2.3.3 ~~In nuclear plants, the~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.-R. Section 73.54.

4.2.3.4 ~~Responsible Entities~~ For Distribution Providers, the systems and equipment that~~,~~ are not included in ~~compliance with Standard CIP-002~~ section 4~~, identify that they have no Critical Cyber Assets shall only be required to comply with~~ .2.1 above.

5. Effective Dates:

~~**4.2.4**~~1. **24 Months Minimum –** CIP-003-~~4~~5, except for CIP-003-5, Requirement R2~~.~~, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval.

~~**5. Effective Date:** The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).~~

2. In those jurisdictions where no regulatory approval is required, CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-

1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

~~Cyber Security Policy — The Responsible Entity shall~~

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 Personnel & training (CIP-004);

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.3 Physical security of BES Cyber Systems (CIP-006);

1.4 System security management (CIP-007);

1.5 Incident reporting and response planning (CIP-008);

1.6 Recovery plans for BES Cyber Systems (CIP-009);

1.7 Configuration change management and vulnerability assessments (CIP-010);

1.8 Information protection (CIP-011); and

1.9 Declaring and responding to CIP Exceptional Circumstances.

~~**R1.**~~ **M1.** Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document ~~and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:~~

~~**1.1** The~~ management system that indicate review of each cyber security policy ~~addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.~~

~~**R1.2.** The~~ at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy ~~is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets~~.

~~**1.2** Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.~~

~~Leadership —~~ **R2.** Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Cyber security awareness;

2.2 Physical security controls;

2.3 Electronic access controls for external routable protocol connections and Dial-up Connectivity; and

2.4 Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

~~**R2.**~~ **R4.** The Responsible Entity shall ~~assign a single senior manager with overall responsibility and~~ implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority ~~for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.~~

~~**1.1** The senior manager shall be identified by name, title, and date of designation.~~

~~**1.2** Changes to the senior manager must be documented within thirty calendar days of the effective date.~~

~~**1.3**~~ , unless no delegations are used. Where allowed by the CIP Standards ~~CIP-002-4 through~~, the CIP ~~-009-4, the senior manager~~ Senior Manager may delegate authority for specific actions to a ~~named~~ delegate or delegates. These delegations shall be documented ~~in~~, including the ~~same manner as R2.1 and R2.2, and approved by the senior manager.~~

~~**1.4** The senior manager~~name or ~~delegate(s), shall authorize and document any exception from the requirements~~title of the ~~cyber security policy.~~

~~**R3.** Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or~~ delegate~~(s).~~

~~**R3.1.** Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being~~, the specific actions delegated, and the date of the

delegation; approved by the ~~senior manager or delegate(s).~~ CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

~~**1.1** Documented exceptions to the cyber security policy must~~**M4.** An example of evidence may include ~~an explanation as to why the exception~~, but is ~~necessary and any compensating measures.~~

~~**1.2** Authorized exceptions to the cyber security policy must be reviewed and~~not limited to, a dated document, approved ~~annually~~ by the ~~senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.~~

~~**R4.** Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.~~

~~**1.1** The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology~~CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or ~~similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.~~

~~**1.2** The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.~~

~~**R4.3.** The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies~~authorize specifically identified ~~during the assessment.~~items.

~~**R5.** Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.~~

~~**1.1** The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.~~

~~**5.1.1.** Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.~~

~~**5.1.2.** The list of personnel responsible for authorizing access to protected information shall be verified at least annually.~~

~~**1.2** The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.~~

~~**1.3** The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.~~

~~R6.~~ ~~Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.~~

~~C. Measures~~

~~M1.~~ ~~The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.~~

~~M2.~~ ~~The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.~~

~~M3.~~ ~~The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.~~

~~M4.~~ ~~The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.~~

~~M5.~~ ~~The Responsible Entity shall make available its access control documentation as specified in Requirement R5.~~

~~M6.~~ ~~The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.~~

~~D.~~C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

~~**1.2. The RE shall serve as the CEA with the following exceptions:**~~

~~**1.2.1** For entities that do not work for the Regional Entity, the~~The Regional Entity shall serve as the Compliance Enforcement Authority~~.~~

~~**1.2.2** For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.~~

~~**1.2.3** For Responsible Entities that are also Regional Entities,~~ ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by ~~the ERO and~~ FERC or other applicable governmental ~~authorities~~authority shall serve as the ~~Compliance Enforcement Authority~~CEA.

1.2. ~~For the ERO, a third-party monitor without vested interest~~**Evidence Retention:**

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in ~~the outcome~~this standard for ~~the ERO~~three calendar years.

~~**1.2.4**~~• If a Responsible Entity is found non-compliant, it shall ~~serve as~~keep information related to the non-compliance until mitigation is complete and approved or for the ~~Compliance Enforcement Authority~~time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and ~~Enforcement~~Assessment Processes~~.~~:

- Compliance ~~Audits~~Audit
- Self-~~Certifications~~Certification
- Spot Checking
- Compliance ~~Violation Investigations~~Investigation
- Self-Reporting

~~Complaints~~

~~**1.4. Data Retention**~~

~~**1.4.1** The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.~~

~~**1.4.2** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.~~

- Complaint

~~1.5.~~1.4. Additional Compliance Information~~.~~:

~~**1.5.1**~~• None

~~**2. Violation Severity Levels**~~

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~The Responsible Entity has documented but not implemented a cyber security policy.~~	~~The Responsible Entity has not documented nor implemented a cyber security policy.~~
~~R1.1.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.~~
~~R1.2.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.~~

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1.3~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~The Responsible Entity's senior manager, assigned pursuant to R2, annually reviewed but did not annually approve its cyber security policy.~~	~~The Responsible Entity's senior manager, assigned pursuant to R2, did not annually review nor approve its cyber security policy.~~
~~R2.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity has not assigned a single senior manager with overall responsibility and~~ ~~authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.~~
~~R2.1.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The senior manager is not identified by name, title, and date of designation.~~
~~R2.2.~~	~~LOWER~~	~~Changes to the senior manager were documented in greater than 30 but less than 60 days of the effective date.~~	~~Changes to the senior manager were documented in 60 or more but less than 90 days of the effective date.~~	~~Changes to the senior manager were documented in 90 or more but less than 120 days of the effective date.~~	~~Changes to the senior manager were documented in 120 or more days of the effective date.~~
~~R2.3.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation,~~ ~~OR~~ ~~The document is not approved by the senior manager,~~ ~~OR~~ ~~Changes to the delegated authority are not documented within thirty calendar days of the effective date.~~	~~A senior manager's delegate is not identified by name, title, and date~~ ~~of designation; the document delegating the authority does not identify the authority being delegated; the document~~ ~~delegating the authority is not approved by the senior manager;~~ ~~AND~~ ~~changes to the delegated authority are not documented within thirty calendar days of the effective date.~~
~~R2.4~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.~~
~~R3.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were documented, but were not authorized by the senior manager or delegate(s).~~	~~In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were not documented, and were not authorized by the senior manager or delegate(s).~~

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R3.1.~~	~~LOWER~~	~~Exceptions to the Responsible Entity's cyber security policy were documented in more than 30 but less than 60 days of being approved by the senior manager or delegate(s).~~	~~Exceptions to the Responsible Entity's cyber security policy were documented in 60 or more but less than 90 days of being approved by the senior manager or delegate(s).~~	~~Exceptions to the Responsible Entity's cyber security policy were documented in 90 or more but less than 120 days of being approved by the senior manager or delegate(s).~~	~~Exceptions to the Responsible Entity's cyber security policy were documented in 120 or more days of being approved by the senior manager or delegate(s).~~
~~R3.2.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include either:~~ ~~1) an explanation as to why the exception is necessary, or~~ ~~2) any compensating measures.~~	~~The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include both:~~ ~~1) an explanation as to why the exception is necessary, and~~ ~~2) any compensating measures.~~
~~R3.3.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were reviewed but not approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.~~	~~Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were not reviewed nor approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.~~
~~R4.~~	~~MEDIUM~~	~~N/A~~	~~The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.~~	~~The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.~~	~~The Responsible Entity did not implement nor document a program to identify, classify, and protect information associated with Critical Cyber Assets.~~
~~R4.1.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.~~	~~The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.~~
~~R4.2.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.~~
~~R4.3.~~	~~LOWER~~	~~N/A~~	~~The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, documented the assessment results, which included deficiencies identified during the assessment but did not implement a remediation plan.~~	~~The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, did not document the assessment results, and did not implement a remediation plan.~~	~~The Responsible Entity did not annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, nor implement an action plan to remediate deficiencies identified during the assessment.~~

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R5.~~	~~LOWER~~	~~N/A~~	~~The Responsible Entity implemented but did not document a program for managing access to protected Critical Cyber Asset information.~~	~~The Responsible Entity documented but did not implement a program for managing access to protected Critical Cyber Asset information.~~	~~The Responsible Entity did not implement nor document a program for managing access to protected Critical Cyber Asset information.~~
~~R5.1.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.~~	~~The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.~~
~~R5.1.1.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did identify the personnel by name and title but did not identify the information for which they are responsible for authorizing access.~~	~~The Responsible Entity did not identify the personnel by name and title nor the information for which they are responsible for authorizing access.~~
~~R5.1.2.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.~~
~~R5.2.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.~~
~~R5.3.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.~~
~~R6.~~	~~LOWER~~	~~The Responsible Entity has established but not documented a change control process~~ ~~OR~~ ~~The Responsible Entity has established but not documented a configuration management process.~~	~~The Responsible Entity has established but not documented both a change control process and configuration management process.~~	~~The Responsible Entity has not established and documented a change control process~~ ~~OR~~ ~~The Responsible Entity has not established and documented a configuration management process.~~	~~The Responsible Entity has not established and documented a change control process~~ ~~AND~~ ~~The Responsible Entity has not established and documented a configuration management process.~~

~~E.~~D. Regional Variances

None ~~identified~~.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-5, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not

necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-5, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-5, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

Review and approval of the cyber security policy at least every 15 calendar months ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. ~~Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets.~~ ~~**Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information).**~~ Changed compliance monitor to Compliance Enforcement Authority.	
~~3~~		~~Update version number from -2 to -3~~	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	~~Update~~
3	3/31/10	Approved by FERC.	
4	~~Board approved 01~~1/24/~~2011~~11	~~**Update version number from "3" to "4"**~~Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
~~4~~5	~~4/19~~11/26/12	~~FERC Order issued approving CIP-003-4 (approval becomes effective June 25, 2012)~~ ~~**Added approved VRF/VSL table to section D.2.**~~Adopted by the NERC Board	Modified to coordinate with other CIP standards and to revise format to

		of Trustees.	use RBS Template.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-5

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-004-5:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-004-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-004-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of

implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Page 6 of 52

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

Page 7 of 52

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

Page 8 of 52

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

Page 9 of 52

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

Page 10 of 52

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

Page 11 of 52

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

Page 12 of 52

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

Page 13 of 52

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Page 14 of 52

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

Page 15 of 52

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

Page 16 of 52

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Page 17 of 52

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

Page 18 of 52

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

Page 19 of 52

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

Page 20 of 52

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

Page 21 of 52

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

Page 22 of 52

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized	deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical	deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical	implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion	access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	(2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			date, and did not identify, assess and correct the deficiencies. (2.3)			
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and correct the deficiencies.	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and correct the deficiencies.	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of a subsequent calendar quarter, and did not identify, assess and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is	calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)			were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible Entity has implemented	complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more process(es) to	day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR The Responsible			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances, and did not			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identify, assess, and correct the deficiencies. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include

individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group

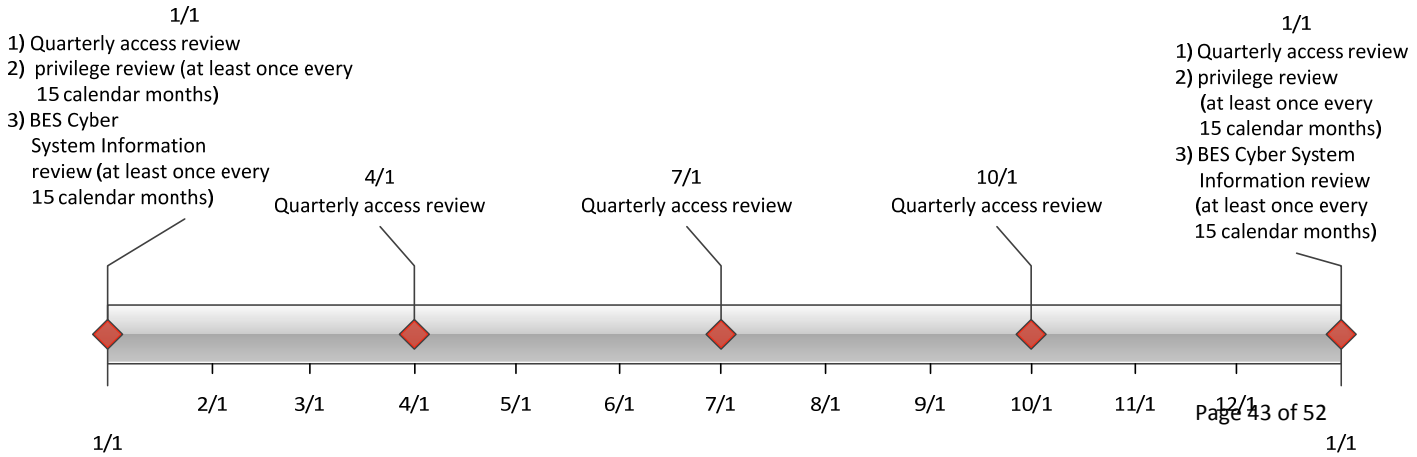

assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

Reference to prior version: (Part 1.1) CIP-004-4, R1

Change Rationale: (Part 1.1)

Changed to remove the need to ensure or prove everyone with authorized electronic or authorized unescorted physical *access "received" ongoing reinforcement – to state that security awareness has been reinforced.*

Moved example mechanisms to guidance.

Rationale for R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:

- The visitor control program
- Electronic interconnectivity supporting the operation and control of BES Cyber Systems
- Storage media as part of the handling of BES Cyber Systems information

2. Change references from Critical Cyber Assets to BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP004-4, R2.2.1

Change Rationale: (Part 2.1)

Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was

focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.

Reference to prior version: (Part 2.2) CIP004-4, R2.1

Change Rationale: (Part 2.2)

Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.

Reference to prior version: (Part 2.3) CIP004-4, R2.3

Change Rationale: (Part 2.3)

Updated to replace "annually" with "once every 15 calendar months."

Rationale for R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.

Reference to prior version: (Part 3.1) CIP004-4, R3.1

Change Rationale: (Part 3.1)

Addressed interpretation request in guidance. Specified that process for identity confirmation is required. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.

Reference to prior version: (Part 3.2) CIP004-4, R3.1

Change Rationale: (Part 3.2)

Specify that the seven year criminal history check covers all locations where the individual has resided for six months or more, including current residence regardless of duration. Added

additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.

Reference to prior version: (Part 3.3) New

Change Rationale: (Part 3.3)

There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.

Reference to prior version: (Part 3.4) CIP-004-4, R3.3

Change Rationale: (Part 3.4)

Separated into its own table item.

Reference to prior version: (Part 3.5) CIP-004-3, R3, R3.3

Change Rationale: (Part 3.5)

Whether for initial access or maintaining access, establishes that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment. CIP-004-3, R3, R3.3

Rationale for R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account

databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

Reference to prior version: (Part 4.1) CIP 003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1

Change Rationale: (Part 4.1)

Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*

Reference to prior version: (Part 4.2) CIP 004-4, R4.1

Change Rationale: (Part 4.2)

Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.

Reference to prior version: (Part 4.3) CIP 007-4, R5.1.3

Change Rationale: (Part 4.3)

Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary.

Reference to prior version: (Part 4.4) CIP-003-4, R5.1.2

Change Rationale: (Part 4.4)

Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to

confirm access privileges are correct and the minimum necessary for performing assigned work functions.

Rationale for R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate."

Reference to prior version: (Part 5.1) CIP 004-4, R4.2

Change Rationale: (Part 5.1)

The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards ***to require immediate revocation*** *for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*

Reference to prior version: (Part 5.2) CIP-004-4, R4.2

Change Rationale: (Part 5.2)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.

Reference to prior version: (Part 5.3) New

Change Rationale: (Part 5.3)

FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.

Reference to prior version: (Part 5.4) New

Change Rationale: (Part 5.4)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.

Reference to prior version: (Part 5.5) CIP-007-4, R5.2.3

Change Rationale: (Part 5.5)

To provide clarification of expected actions in managing the passwords.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

~~A.~~A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-~~4~~5

3. **Purpose:** ~~Standard CIP-004-4 requires~~To minimize the risk against compromise that ~~personnel having authorized cyber~~could lead to misoperation or ~~authorized unescorted physical access to Critical~~instability in the BES from individuals accessing BES Cyber ~~Assets, including contractors and service vendors, have~~Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness~~. Standard CIP-004-4 should be read as part~~ in support of ~~a group of standards numbered Standards CIP-002-4 through CIP-009-4.~~protecting BES Cyber Systems.

4. **Applicability:**

~~**4.1.** Within the text of Standard CIP-004-4, "Responsible Entity" shall mean:~~

4.1. ~~Reliability~~ **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

~~4.1.1~~ Interchange Coordinator~~.~~

~~**4.1.2 Balancing Authority.**~~

~~4.1.3~~4.1.5. or Interchange Authority~~.~~

~~**4.1.4 Transmission Service Provider.**~~

4.1.6. Reliability Coordinator

~~4.1.5~~4.1.7. Transmission ~~Owner.~~Operator

~~**4.1.6 Transmission Operator.**~~

~~4.1.7~~4.1.8. ~~Generator~~ Owner~~.~~

~~**4.1.8 Generator Operator.**~~

~~**4.1.9 Load Serving Entity.**~~

~~**4.1.10 NERC.**~~

~~**4.1.11 Regional Entity.**~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first

interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

~~4.2.1~~**4.2.3. Exemptions:** The following are exempt from Standard CIP-004-~~4:~~5:

~~4.2.1~~**4.2.3.1.** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.2~~**4.2.3.2.** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.3~~**4.2.3.3.** ~~In nuclear plants, the~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.4~~**4.2.3.5.** Responsible Entities that~~, in compliance with Standard CIP-002-4,~~ identify that they have no ~~Critical Cyber Assets.~~ BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective ~~Date:~~ ~~The~~Dates:

1. **24 Months Minimum** – CIP-004-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ~~eighth~~ninth calendar quarter after the effective date of the order providing applicable regulatory ~~approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in~~ approval.

~~5.~~2. In those jurisdictions where no regulatory approval is ~~not~~ required~~).~~, CIP-004-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

~~4.1.2. **Requirements**~~

~~Awareness The~~ **6. Background:**

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall* ~~establish, document,~~ *implement*~~, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in~~

~~sound security practices. The program shall~~ *one or more documented [processes, plan, etc] that include* ~~security awareness reinforcement on at least a quarterly~~*the applicable items in [Table Reference].”* The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis ~~using~~for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying “implement” as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the “. . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Page 6 of 62

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

Page 7 of 62

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

Page 8 of 62

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

Page 9 of 62

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

Page 10 of 62

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

Page 11 of 62

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

Page 12 of 62

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

Page 13 of 62

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Page 14 of 62

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

Page 15 of 62

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

Page 16 of 62

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Page 17 of 62

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

Page 18 of 62

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

Page 19 of 62

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

Page 20 of 62

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

Page 21 of 62

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

Page 22 of 62

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	Operations Planning	Lower	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized	deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical	deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical	implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion	access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	(2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			date, and did not identify, assess and correct the deficiencies. (2.3)			
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and correct the deficiencies.	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and correct the deficiencies.	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of a subsequent calendar quarter, and did not identify, assess and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is	calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)			were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible Entity has implemented	complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more process(es) to	day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR The Responsible			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances, and did not			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identify, assess, and correct the deficiencies. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms ~~such as~~and evidence, when dated, which can be used are:

- ~~R1.~~• Direct communications (e.g., emails, memos, computer based training, etc.);
- ~~R2.~~• Indirect communications (e.g., posters, intranet, brochures, etc.);

R3.• Management support and reinforcement (e.g., presentations, meetings, etc.).

- Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.**Requirement R2:**

Training shall cover the policies, access controls, and procedures as developed for the CriticalBES Cyber Assets covered by CIP-004-4,Systems and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

- The proper use of Critical Cyber Assets;
- Physical and electronic access controls to Critical Cyber Assets;
- The proper handling of Critical Cyber Asset information; and,
- Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

from Table R2. The Responsible Entity shall maintain documentation that training is conducted at least annually, includinghas the dateflexibility to define the training was completed and attendance recordsprogram and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

Personnel Risk Assessment — The Responsible Entity shall have a documented personnel risk assessment program,One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

- Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified

exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such. Identity only needs to be confirmed prior to initially granting access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.

- Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

4.1.3. Measures

The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

~~The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.~~

4.1.29. **Compliance**

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for only requires periodic confirmation according to the Regional Entity,entity's process during the Regional Entity shall serve astenure of employment, which may or may not be the Compliance Enforcement Authoritysame as the initial verification action.

1.2.2. For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3. For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4. For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1. The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2. The Responsible Entity shall keep all other documentation required by Standard CIP-004-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

~~**1.4.3.** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.~~

~~**1.5. Additional Compliance Information**~~

~~**2. Violation Severity Levels**~~

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

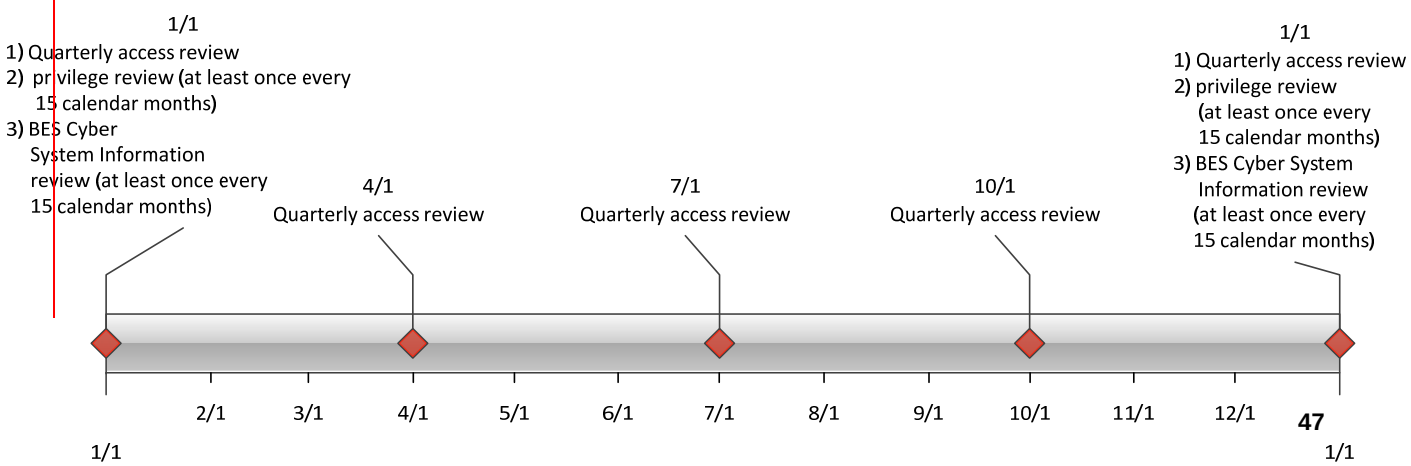

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least

privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~Scenario	~~Severe VSL~~Possible Process	
~~R1.~~	~~LOWER~~	~~The Responsible Entity established, implemented, and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive ongoing reinforcement in sound security practices.~~		~~The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.~~	~~The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.~~	~~The Responsible Entity did not establish, implement, maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.~~
~~R2.~~	~~LOWER~~	~~The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.~~		~~The Responsibility Entity did not review the training program on an annual basis.~~	~~The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized~~	~~The Responsible Entity did not establish, document, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical~~

						~~unescorted physical access to Critical Cyber Assets.~~	~~access to Critical Cyber Assets.~~
~~R2.1.~~	~~MEDIUM~~	~~At least one individual but less than 5% of personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~	~~At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~	~~At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~Immediate involuntary termination	~~15% or more of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.		
~~R2.2.~~	~~MEDIUM~~	~~N/A~~			~~The training does not include one of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.~~	~~The training does not include two of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.~~	~~The training does not include three or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.~~
~~R2.2.1.~~	~~LOWER~~	~~N/A~~			~~N/A~~	~~N/A~~	~~N/A~~
~~R2.2.2.~~	~~LOWER~~	~~N/A~~			~~N/A~~	~~N/A~~	~~N/A~~
~~R2.2.3.~~	~~LOWER~~	~~N/A~~			~~N/A~~	~~N/A~~	~~N/A~~
~~R2.2.4.~~	~~LOWER~~	~~N/A~~			~~N/A~~	~~N/A~~	~~N/A~~

~~R2.3.~~	~~LOWER~~	~~N/A~~			~~N/A~~	~~The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include either the date the training was completed or attendance records.~~	~~The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed or attendance records.~~
~~R3.~~	~~MEDIUM~~	~~N/A~~	~~The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.~~	~~The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after such personnel were granted such access except in specified circumstances such as an emergency.~~Scheduled involuntary termination	~~The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access.~~ ~~OR~~ ~~The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.~~Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.		
~~R3.1.~~	~~LOWER~~	~~N/A~~			~~N/A~~	~~The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification in the U.S.) or a seven-year criminal check.~~	~~The Responsible Entity did not ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check.~~
~~R3.2.~~	~~LOWER~~	~~N/A~~			~~The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment but did update it for cause when applicable.~~	~~The Responsible Entity did not update each personnel risk assessment for cause (when applicable) but did at least updated it every seven years after the initial personnel risk assessment.~~	~~The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment nor was it updated for cause when applicable.~~
~~R3.3.~~	~~LOWER~~	~~The Responsible Entity did not document the results of~~	~~The Responsible Entity did not document the results of personnel risk~~	~~The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel~~	~~The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-~~		

		personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4.	assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4.	with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4. Voluntary termination	004-4. Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
R4.	LOWER	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing at least one individual but less than 5% of the authorized personnel.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 5% or more but less than 10% of the authorized personnel.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 10% or more but less than 15%of the authorized personnel. Retirement where the last working day is several weeks prior to the termination date	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 15% or more of the authorized personnel. Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
R4.1.	LOWER	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel. Death	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel. Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

~~R4.2.~~	~~MEDIUM~~	~~N/A~~	~~The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.~~	~~The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.~~	~~The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.~~

~~4.1.31. Regional Variances~~

~~None identified.~~

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

Reference to prior version: (Part 1.1) CIP-004-4, R1

Change Rationale: (Part 1.1)

Changed to remove the need to ensure or prove everyone with authorized electronic or authorized unescorted physical *access "received" ongoing reinforcement – to state that security awareness has been reinforced.*

Moved example mechanisms to guidance.

Rationale for R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:

- The visitor control program
- Electronic interconnectivity supporting the operation and control of BES Cyber Systems
- Storage media as part of the handling of BES Cyber Systems information

2. Change references from Critical Cyber Assets to BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP004-4, R2.2.1

Change Rationale: (Part 2.1)

Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was

focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.

Reference to prior version: (Part 2.2) CIP004-4, R2.1

Change Rationale: (Part 2.2)

Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.

Reference to prior version: (Part 2.3) CIP004-4, R2.3

Change Rationale: (Part 2.3)

Updated to replace "annually" with "once every 15 calendar months."

Rationale for R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.

Reference to prior version: (Part 3.1) CIP004-4, R3.1

Change Rationale: (Part 3.1)

Addressed interpretation request in guidance. Specified that process for identity confirmation is required. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.

Reference to prior version: (Part 3.2) CIP004-4, R3.1

Change Rationale: (Part 3.2)

Specify that the seven year criminal history check covers all locations where the individual has resided for six months or more, including current residence regardless of duration. Added

additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.

Reference to prior version: (Part 3.3) New

Change Rationale: (Part 3.3)

There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.

Reference to prior version: (Part 3.4) CIP-004-4, R3.3

Change Rationale: (Part 3.4)

Separated into its own table item.

Reference to prior version: (Part 3.5) CIP-004-3, R3, R3.3

Change Rationale: (Part 3.5)

Whether for initial access or maintaining access, establishes that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment. CIP-004-3, R3, R3.3

Rationale for R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account

databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

Reference to prior version: (Part 4.1) CIP 003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1

Change Rationale: (Part 4.1)

Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*

Reference to prior version: (Part 4.2) CIP 004-4, R4.1

Change Rationale: (Part 4.2)

Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.

Reference to prior version: (Part 4.3) CIP 007-4, R5.1.3

Change Rationale: (Part 4.3)

Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary.

Reference to prior version: (Part 4.4) CIP-003-4, R5.1.2

Change Rationale: (Part 4.4)

Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to

confirm access privileges are correct and the minimum necessary for performing assigned work functions.

Rationale for R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate."

Reference to prior version: (Part 5.1) CIP 004-4, R4.2

Change Rationale: (Part 5.1)

The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards ***to require immediate revocation*** *for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*

Reference to prior version: (Part 5.2) CIP-004-4, R4.2

Change Rationale: (Part 5.2)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.

Reference to prior version: (Part 5.3) New

Change Rationale: (Part 5.3)

FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.

Reference to prior version: (Part 5.4) New

Change Rationale: (Part 5.4)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.

Reference to prior version: (Part 5.5) CIP-007-4, R5.2.3

Change Rationale: (Part 5.5)

To provide clarification of expected actions in managing the passwords.

Version History

Version	Date	Action	Change Tracking
1	~~01~~1/16/06	~~**D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"**~~R3.2 — Change "Control Center" to "control center."	~~03~~3/24/06
~~1~~2	~~06/01/06~~9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.~~**D.2.1.4 — Change "access control rights" to "access rights."**~~ Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	~~06/05/06~~
~~2~~3	12/16/09	**Updated version number from -2 to -3 Approved by the NERC Board of Trustees.** ~~**Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.**~~ ~~Removal of reasonable business judgment.~~ ~~Replaced the RRO with the RE as a responsible entity.~~ ~~Rewording of Effective Date.~~ ~~Reference to emergency situations.~~ ~~Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program.~~ ~~Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program.~~ ~~Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to~~	

		~~"Critical Cyber Assets".~~ ~~Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments.~~ ~~**Changed compliance monitor to Compliance Enforcement Authority.**~~	
3	3/31/10	Approved by FERC.~~Update **version number from -2 to -3**~~	
~~3~~4	12/~~**16/09**~~30/10	~~**Approved by NERC Board of Trustees**~~Modified to add specific criteria for Critical Asset identification.	Update
4	~~Board approved 01~~1/24/~~2011~~11	~~**Update version number from "3" to "4"**~~Approved by the NERC Board of Trustees.	Update~~Update to conform to changes to CIP-002-4 (Project 2008-06)~~
~~4~~5	~~**4/19**~~11/26/12	~~FERC Order issued approving CIP-004-4 (approval becomes effective June 25, 2012)~~ ~~**Added approved VRF/VSL table to section D.2.**~~Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-5

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-005-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-005-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-005-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.

- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the

Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)

E*xplicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)

Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)

Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)

Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)

Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-~~4a~~5

3. Purpose: ~~Standard CIP-005-4a requires the identification and protection of the~~ To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter~~(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.~~ in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard~~ CIP-005-4a should be read as part of a~~ .

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

~~3.~~4.1.2.4 Each Cranking Path and group of ~~standards numbered Standards CIP-002-4 through CIP-009-4.~~ Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~**4. Applicability**~~

~~**4.1.** Within the text of Standard CIP-005-4a, "Responsible Entity" shall mean:~~

4.1.3 ~~Reliability~~**Generator Operator**

4.1.4 Generator Owner

~~**4.1.1**~~ **Interchange Coordinator**~~.~~

~~**4.1.2 Balancing Authority.**~~

~~**4.1.3**~~**4.1.5 or Interchange Authority**~~.~~

~~**4.1.4 Transmission Service Provider.**~~

4.1.6 Reliability Coordinator

~~**4.1.5**~~**4.1.7 Transmission** ~~Owner.~~**Operator**

~~**4.1.6**~~ **Transmission** ~~Operator.~~

~~**4.1.7**~~**4.1.8** ~~Generator~~ **Owner**~~.~~

~~**4.1.8 Generator Operator.**~~

~~**4.1.9 Load Serving Entity.**~~

~~**4.1.10 NERC.**~~

~~**4.1.11 Regional Entity**~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.4.2.3 Exemptions: The following are exempt from Standard CIP-005-4a:5:

4.2.1.4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2.4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

4.2.4.4.2.3.3 In nuclear plants, theThe systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.-R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Date: The Dates:

1. **24 Months Minimum** – CIP-005-5 shall become effective on the later of July 1, 2015, or the first day of the eighth calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective approval.

5. 2. In those jurisdictions where no regulatory approval is required, CIP-005-5 shall become effective on the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required). -following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

B. Requirements

Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

~~a. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).~~

~~b. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.~~

~~c. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).~~

~~d. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.~~

~~Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.~~

~~e. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.~~

~~Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).~~

~~f. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.~~

~~g. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.~~

~~h. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).~~

~~i. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.~~

~~j. The required documentation shall, at least, identify and describe:~~

~~i.The processes for access request and authorization.~~

~~ii. The authentication methods.~~

~~iii. The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.~~

~~iv.The controls used to secure dial-up accessible connections.~~

~~k. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.~~

~~Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.~~

~~l. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.~~

~~m. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.~~

~~Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:~~

~~n. A document identifying the vulnerability assessment process;~~

~~o. A review to verify that only ports and services required for operations at these access points are enabled;~~

~~p. The discovery of all access points to the Electronic Security Perimeter;~~

~~q. A review of controls for default accounts, passwords, and network management community strings;~~

~~r. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.~~

~~Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4a.~~

~~The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.~~

~~The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.~~

~~The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.~~

~~C. Measures~~

~~**M1.** The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.~~

~~**M2.** The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.~~

~~**M3.** The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.~~

~~**M4.** The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.~~

~~**M5.** The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.~~

6. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident

response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.

- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

D.C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, theThe Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authoritiesauthority shall serve as the Compliance Enforcement AuthorityCEA.

1.2. For the ERO, a third-party monitor without vested interestEvidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in the outcomethis standard for the EROthree calendar years.

1.2.4• If a Responsible Entity is found non-compliant, it shall serve askeep information related to the non-compliance until mitigation is complete and approved or for the Compliance Enforcement Authoritytime specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and EnforcementAssessment Processes:

- Compliance AuditsAudit
- Self-CertificationsCertification
- Spot Checking

- Compliance ~~Violation Investigations~~Investigation
- Self-Reporting

~~Complaints~~

~~**1.4. Data Retention**~~

~~**1.4.1** The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.~~

~~**1.4.2** The Responsible Entity shall keep other documents and records required by Standard CIP-005-4a from the previous full calendar year.~~

~~**1.4.3** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.~~

- Complaint

~~1.5.~~1.4. Additional Compliance Information:

~~**2. Violation Severity Levels**~~

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1.~~	~~MEDIUM~~	~~The Responsible Entity did not document one or more access points to the Electronic Security Perimeter(s).~~	~~The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s).~~	~~The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter.~~ ~~OR~~ ~~The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s).~~	~~The Responsible Entity did not ensure that one or more Critical Cyber Assets resides within an Electronic Security Perimeter, and the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) for all Critical Cyber Assets.~~
~~R1.1.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).~~
~~R1.2.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.~~
~~R1.3.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.~~
~~R1.4.~~	~~MEDIUM~~	~~N/A~~	~~One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005.~~	~~One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005.~~	~~One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.~~
~~R1.5.~~	~~MEDIUM~~	~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of~~	~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of~~	~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3;~~	~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided without four (4) or more of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4~~

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
		~~the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.~~	~~the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.~~	~~Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.~~	~~Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.~~
~~R1.6.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset deployed for the access control and monitoring of these access points.~~	~~The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.~~
~~R2.~~	~~MEDIUM~~	~~N/A~~	~~The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).~~	~~The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).~~	~~The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).~~
~~R2.1.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.~~

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R2.2.~~	~~MEDIUM~~	~~N/A~~	~~At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity did not document, individually or by specified grouping, the configuration of those ports and services required for operation and for monitoring Cyber Assets within the Electronic Security Perimeter.~~	~~At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter but did document, individually or by specified grouping, the configuration of those ports and services.~~	~~At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and did not document, individually or by specified grouping, the configuration of those ports and services.~~
~~R2.3.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.~~	~~The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.~~
~~R2.4.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.~~
~~R2.5.~~	~~LOWER~~	~~The required documentation for R2 did not include one of the elements described in R2.5.1 through R2.5.4~~	~~The required documentation for R2 did not include two of the elements described in R2.5.1 through R2.5.4~~	~~The required documentation for R2 did not include three of the elements described in R2.5.1 through R2.5.4~~	~~The required documentation for R2 did not include any of the elements described in R2.5.1 through R2.5.4~~
~~R2.5.1.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R2.5.2.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R2.5.3.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R2.5.4.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R2.6.~~	~~LOWER~~	~~The Responsible Entity did not maintain a document identifying the content of the banner.~~ ~~OR~~ ~~Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.~~	~~Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.~~	~~Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.~~	~~Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.~~
~~R3.~~	~~MEDIUM~~	~~The Responsible Entity did not document the electronic or manual processes for monitoring and logging access to access points.~~ ~~OR~~ ~~The Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points.~~	~~The Responsible Entity did not implement electronic or manual processes monitoring and logging at 5% or more but less than 10% of the access points.~~	~~The Responsible Entity did not implement electronic or manual processes monitoring and logging at 10% or more but less than 15 % of the access points.~~	~~The Responsible Entity did not implement electronic or manual processes monitoring and logging at 15% or more of the access points.~~
~~R3.1.~~	~~MEDIUM~~	~~The Responsible Entity did not document the electronic or manual processes for monitoring access points to dial-up devices.~~ ~~OR~~ ~~Where technically~~	~~Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices.~~	~~Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices.~~	~~Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 15% or more of the access points to dial-up devices.~~

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
		~~feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at less than 5% of the access points to dial-up devices.~~			
~~R3.2.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~Where technically feasible, the Responsible Entity implemented security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses, however the alerts do not provide for appropriate notification to designated response personnel.~~	~~Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses.~~ ~~OR~~ ~~Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days~~
~~R4.~~	~~MEDIUM~~	~~The Responsible Entity did not perform a Vulnerability Assessment at least annually for less than 5% of access points to the Electronic Security Perimeter(s).~~	~~The Responsible Entity did not perform a Vulnerability Assessment at least annually for 5% or more but less than 10% of access points to the Electronic Security Perimeter(s).~~	~~The Responsible Entity did not perform a Vulnerability Assessment at least annually for 10% or more but less than 15% of access points to the Electronic Security Perimeter(s).~~	~~The Responsible Entity did not perform a Vulnerability Assessment at least annually for 15% or more of access points to the Electronic Security Perimeter(s).~~ ~~OR~~ ~~The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5.~~
~~R4.1.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R4.2.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R4.3.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R4.4.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R4.5.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R5.~~	~~LOWER~~	~~The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005-4.~~	~~The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005-4.~~	~~The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.~~	~~The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.~~
~~R5.1.~~	~~LOWER~~	~~N/A~~	~~The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005-4.~~	~~The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005-4.~~	~~The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005-4 at least annually.~~
~~R5.2.~~	~~LOWER~~	~~For less than 5% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.~~	~~For 5% or more but less than 10% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.~~	~~For 10% or more but less than 15% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.~~	~~For 15% or more of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.~~
~~R5.3.~~	~~LOWER~~	~~The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.~~	~~The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.~~	~~The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days.~~	~~The Responsible Entity retained electronic access logs for less than 45 calendar days.~~

- None

~~E.~~D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the

Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)

Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)

Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)

Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)

Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)

Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed

to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified~~.~~ in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Version History

Version	Date	Action	Change Tracking
1	~~01~~1/16/06	~~D~~R3.2~~.3.1~~ — Change "~~Critical Assets,"~~Control Center" to "~~Critical Cyber Assets" as intended.~~control center."	~~03~~3/24/06
2	~~Approved by NERC Board of Trustees 5/6/09~~9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. ~~Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s).~~	~~Revised.~~

		Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	~~Changed CIP-005-2 to CIP-005-3.~~ ~~Changed all references to CIP Version "2" standards to CIP Version "3" standards.~~ ~~**For Violation Severity Levels, changed, "To be developed later" to "Developed separately."**~~Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	~~**Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)**~~
~~2a~~3	~~02/16~~3/31/10	~~**Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010**~~Approved by FERC.	~~**Addition**~~
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
~~4a~~5	~~01/24/~~11/26/12	Adopted by the NERC Board of Trustees.	**Modified to coordinate with other CIP standards and to revise format to use RBS Template.**~~**Update** to conform to changes to CIP-002-4 (Project 2008-06)~~ ~~**Update version number from "3" to "4a"**~~
~~4a~~	~~4/19/12~~	~~FERC Order issued approving CIP-005-4a (approval becomes effective June 25, 2012)~~ ~~Added approved VRF/VSL table to section D.2.~~	

~~Appendix 1~~

~~**Requirement Number and Text of Requirement**~~
~~**Section 4.2.2** – Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.~~ ~~**Requirement R1.3** – Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).~~
~~**Question 1 (Section 4.2.2)**~~
~~What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?~~
~~**Response to Question 1**~~
~~In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.~~
~~**Question 2 (Section 4.2.2)**~~
~~Is the communication link physical or logical? Where does it begin and terminate?~~
~~**Response to Question 2**~~
~~The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.~~
~~**Question 3 (Requirement R1.3)**~~
~~Please clarify what is meant by an "endpoint"? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?~~
~~**Response to Question 3**~~
~~The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.~~

~~**Question 4 (Requirement R1.3)**~~
~~If "endpoint" is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an "access point? If two control centers are owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?~~
~~**Response to Question 4**~~
~~In the case where the "endpoint" is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an "access point." The encrypted communication tunnel termination points referred to above are "access points."~~

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-5

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-006-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-006-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The

documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management

Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. *Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.*

Summary of Changes: The entire content of CIP-006-5 is intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

Added details to address FERC Order No. 706, Paragraph 572, directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.

Reference to prior version: (Part 1.1) *CIP-006-4c, R2.1 for Physical Access Control Systems*
New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity

Change Rationale: (Part 1.1)

To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected at the same level as required in Parts 1.2 through 1.5.

Reference to prior version: (Part 1.2) CIP006-4c, R3 & R4
Change Rationale: (Part 1.2)

This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.3) CIP006-4c, R3 & R4

Change Rationale: (Part 1.3)

The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.

Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.
FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).

Reference to prior version: (Part 1.4) CIP006-4c, R5

Change Rationale: (Part 1.4)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.5) CIP006-4c, R5

Change Rationale: (Part 1.5)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.6) CIP006-4c, R5

Change Rationale: (Part 1.6)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.7) CIP006-4c, R5

Change Rationale: (Part 1.7)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.8) CIP-006-4c, R6

Change Rationale: (Part 1.8)

CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.

Examples of logging methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.9) CIP-006-4c, R7

Change Rationale: (Part 1.9)

No change.

Rationale for R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

Reference to prior version: (Part 2.1) CIP-006-4c, R1.6.2

Change Rationale: (Part 2.1)

Added the ability to not do this during CIP Exceptional Circumstances.

Reference to prior version: (Part 2.2) CIP-006-4c R1.6.1

Change Rationale: (Part 2.2)

Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.

Reference to prior version: (Part 2.3) CIP-006-4c, R7

Change Rationale: (Part 2.3)

No change

Rationale for R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

Reference to prior version: (Part 3.1) CIP-006-4c, R8.1 and R8.2

Change Rationale: (Part 3.1)

Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

1. Title: Cyber Security — Physical Security of ~~Critical~~BES Cyber ~~Assets~~Systems

2. Number: CIP-006-~~4c~~5

~~**3. Purpose:** Standard CIP-006-4c is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-4c should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.~~

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

~~**4.1.** Within the text of Standard CIP-006-4c, "Responsible Entity" shall mean:~~

~~**4.1.1** Reliability Coordinator~~

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first

interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

~~**4.1.2 Transmission Service Provider**~~

4.1.6 Reliability Coordinator

4.1.7 Transmission ~~Owner~~Operator

~~**4.1.3 Transmission Operator**~~

4.1.8 ~~Generator~~ Owner

~~**4.1.4 Generator Operator**~~

~~**4.1.5 Load Serving Entity**~~

~~**4.1.6 NERC**~~

~~**4.1.7 Regional Entity**~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first

interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

~~4.2.~~**4.2.3 Exemptions:** The following are exempt from Standard CIP-006-~~4c:~~5:

~~4.2.1~~**4.2.3.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.2~~**4.2.3.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.3~~**4.2.3.3** ~~In nuclear plants, the~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.-R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.4~~**4.2.3.5** Responsible Entities that~~, in compliance with Standard CIP-002-4,~~ identify that they have no ~~Critical Cyber Assets~~BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective ~~Date:~~ ~~The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes~~**Dates:**

1. **24 Months Minimum** – CIP-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after ~~BOT adoption in~~ the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is ~~not~~ required~~).~~, CIP-006-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

~~**B. Requirements**~~

~~**R1.** Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:~~

~~**R1.1.** All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.~~

~~**R1.2.** Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.~~

~~**R1.3.** Processes, tools, and procedures to monitor physical access to the perimeter(s).~~

~~**R1.4.** Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.~~

~~**R1.5.** Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.~~

~~**R1.6.** A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:~~

~~**R1.6.1.** Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.~~

~~**R1.6.2.** Continuous escorted access of visitors within the Physical Security Perimeter.~~

~~**R1.7.** Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.~~

~~**R1.8.** Annual review of the physical security plan.~~

~~**R2.** Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:~~

~~**R2.1.** Be protected from unauthorized physical access.~~

~~Be afforded the protective measures specified in Standard CIP-003-4;~~ **6. Background:**

~~**R2.2.**~~ Standard CIP-~~004-4 Requirement R3; Standard~~006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-~~4a Requirements R2 and R3; Standard CIP-006-4c Requirements R4 and R5; Standard~~5, CIP-006-5, CIP-007-~~4; Standard~~5, CIP-008-~~4; and Standard~~5, CIP-009-~~4.~~

~~**R3.** Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.~~

~~Physical Access Controls — The Responsible Entity shall document and implement the~~5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to ~~manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The~~mitigate risk to

BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each* *Responsible Entity shall implement one or more* ~~of the~~*documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may

include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

~~**R4.**~~ The following ~~physical access methods:~~evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database.~~-~~ Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access ~~to~~into the ~~Critical Cyber Assets.~~Physical Security Perimeter.

~~**R5.** Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4. One or more of the following monitoring methods shall be used:~~

~~Alarm Systems: Systems that alarm to indicate~~ Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for ~~immediate~~ notification within 15 minutes to ~~personnel~~individuals responsible for response.
  - ~~•~~ Human Observation of Access Points: ~~-~~Monitoring of physical access points by ~~authorized~~security personnel ~~as specified in Requirement R4.~~

~~**R6.**• Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging~~who are also controlling physical ~~entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and ~~monitoring~~alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access ~~as specified in Requirement R4~~.

~~**R7.** Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.~~

~~**R8.** Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:~~

~~**R8.1.** Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.~~

~~**R8.2.** Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.~~

~~**R8.3.** Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.~~

~~C. Measures~~

~~**M1.** The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.~~

~~**M2.** The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.~~

~~**M3.** The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.~~

~~The Responsible Entity shall make available documentation identifying the methods for~~ The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling ~~physical access to~~ access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

Requirement R2:

The logging of visitors should capture each ~~access~~ visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of ~~a~~contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

~~**M4.**~~ This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter~~ as specified in Requirement R4~~. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

~~The~~Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

~~**M5.**~~ Each Responsible Entity shall ~~make available documentation identifying the methods for monitoring~~ensure that physical access ~~as specified~~to all BES Cyber Systems is restricted and appropriately managed. *Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement ~~R5~~Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP*.

~~**M6.** The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.~~

~~**M7.** The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.~~

~~The Responsible Entity shall make available documentation to show its implementation of a~~

Summary of Changes: The entire content of CIP-006-5 is intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

~~**M8.**~~ Added details to address FERC Order No. 706, Paragraph 572, directives for physical security ~~system maintenance and testing program as specified~~defense in ~~Requirement R8.~~

~~D. Compliance~~

~~1. Compliance Monitoring Process~~

~~1.1. Compliance Enforcement Authority~~

~~1.2. The RE shall serve as the CEA with the following exceptions:~~

~~1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.~~

~~1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.~~

~~1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.~~

~~1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.~~

~~1.3. Compliance Monitoring and Enforcement Processes~~

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~1.4. Data Retention~~

~~1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.~~

~~1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records~~depth.

~~1.5.~~ Additional ~~Compliance Information~~

~~The Responsible Entity may not make exceptions in its cyber~~ guidance on physical security ~~policy to the creation, documentation, or maintenance of a~~ defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.

Reference to prior version: (Part 1.1) *CIP-006-4c, R2.1 for Physical Access Control Systems*
New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity

Change Rationale: (Part 1.1)

To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected at the same level as required in Parts 1.2 through 1.5.

Reference to prior version: (Part 1.2) CIP006-4c, R3 & R4
Change Rationale: (Part 1.2)

This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.3) CIP006-4c, R3 & R4

Change Rationale: (Part 1.3)

The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.

~~**1.5.1**~~ *Added to address FERC Order No. 706, Paragraph 572, related directives for physical security* ~~plan~~*defense in depth.*
~~For dial-up accessible Critical Cyber Assets that use non-routable protocols,~~*FERC Order No. 706, Paragraph 575, directives addressed by providing the* ~~Responsible Entity shall not be required~~*examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).*

Reference **to** ~~comply with Standard~~**prior version:** (Part 1.4) CIP006-4c, R5

Change Rationale: (Part 1.4)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.5) CIP006-4c, R5

Change Rationale: (Part 1.5)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.6) CIP006-4c, R5

Change Rationale: (Part 1.6)

Addresses the prior CIP-006-4c, Requirement R5 requirement for ~~that single~~Physical Access Control Systems.

Reference to prior version: (Part 1.7) CIP006-4c, R5

Change Rationale: (Part 1.7)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.8) CIP-006-4c, R6

Change Rationale: (Part 1.8)

~~**1.5.2**~~ *CIP-006-4c, Requirement R6 was specific to the logging of access ~~point~~ at ~~the dial-up device.~~identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.*

~~**2. Violation Severity Levels**~~

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s).~~ ~~OR~~ ~~The Responsible Entity created and implemented but did not maintain a physical security plan.~~	~~The Responsible Entity did not document, implement, and maintain a physical security plan.~~

~~R1.1.~~	~~MEDIUM~~	~~N/A~~	~~Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.~~	~~Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.~~	~~The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter.~~ ~~OR~~ ~~Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical to such Cyber Assets within the Electronic Security Perimeter.~~
~~R1.2.~~	~~MEDIUM~~	~~N/A~~	~~The Responsible Entity's physical security plan includes measures to control entry at access points but does not identify all access points through each Physical Security Perimeter.~~	~~The Responsible Entity's physical security identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.~~	~~The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.~~
~~R1.3~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity's physical security plan does not include processes, tools, and procedures to monitor physical access to the perimeter(s).~~
~~R1.4~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.~~
~~R1.5~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-4 Requirement R4.~~	~~The Responsible Entity's physical security plan does not address the process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004-4 Requirement R4.~~
~~R1.6~~	~~MEDIUM~~	~~The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor entrance or did not log the visitor exit from the Physical Security Perimeter.~~	~~The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.~~	~~The responsible Entity included a visitor control program in its physical security plan, but it does not meet the requirements of continuous escort.~~	~~The Responsible Entity did not include or implement a visitor control program in its physical security plan.~~
~~R1.6.1~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~

~~R1.6.2~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R1.7~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~The Responsible Entity's physical security plan addresses a process for updating the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration **but** the plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration.~~	~~The Responsible Entity's physical security plan does not address a process for updating the physical security plan within thirty calendar days of the completion of a physical security system redesign or reconfiguration.~~
~~R1.8~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity's physical Security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.~~
~~R2~~	~~MEDIUM~~	~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.~~	~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.~~	~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.~~	~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access.~~ ~~OR~~ ~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or more of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.~~
~~R2.1.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R2.2.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~

~~R3~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within an identified Physical Security Perimeter.~~
~~R4~~	~~MEDIUM~~	~~N/A~~	~~The Responsible Entity **has implemented but not documented** the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:~~ ~~• Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~ ~~• Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~ ~~• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices:~~ ~~Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.~~	~~The Responsible Entity **has documented but not implemented** the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:~~ ~~• Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~ ~~• Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~ ~~• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices:~~ ~~Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.~~	~~The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods:~~ ~~• Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~ ~~• Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~ ~~• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.~~ ~~• Other Authentication Devices:~~ ~~Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets..~~
~~R5~~	~~MEDIUM~~	~~N/A~~	~~The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the~~	~~The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods:~~ ~~• Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel~~	~~The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods:~~ ~~• Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible~~

			~~following monitoring methods:~~ ~~• Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.~~ ~~• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.~~	~~responsible for response.~~ ~~• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.~~	~~for response.~~ ~~• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.~~ ~~OR~~ ~~An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-4.~~
~~R6~~	~~LOWER~~	~~The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~ ~~• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method,~~ ~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement~~	~~The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~ ~~• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method,~~ ~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4,~~ ~~**but** has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week..~~	~~The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~ ~~• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method,~~ ~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.~~	~~The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~ ~~• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method,~~ ~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.~~

		~~R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.~~			
~~R7~~	~~LOWER~~	~~The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.~~	~~The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.~~	~~The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.~~	~~The Responsible Entity retained physical access logs for less than 45 calendar days.~~
~~R8~~	~~MEDIUM~~	~~The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include one of the Requirements R8.1, R8.2, and R8.3.~~	~~The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include two of the Requirements R8.1, R8.2, and R8.3.~~	~~The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include any of the Requirements R8.1, R8.2, and R8.3.~~	~~The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly.~~
~~R8.1~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R8.2~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R8.3~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~

~~E. Regional Variances~~

~~None identified.~~

Examples of logging methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.9) CIP-006-4c, R7

Change Rationale: (Part 1.9)

No change.

Rationale for R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

Reference to prior version: (Part 2.1) CIP-006-4c, R1.6.2

Change Rationale: (Part 2.1)

Added the ability to not do this during CIP Exceptional Circumstances.

Reference to prior version: (Part 2.2) CIP-006-4c R1.6.1

Change Rationale: (Part 2.2)

Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.

Reference to prior version: (Part 2.3) CIP-006-4c, R7

Change Rationale: (Part 2.3)

No change

Rationale for R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

Reference to prior version: (Part 3.1) CIP-006-4c, R8.1 and R8.2

Change Rationale: (Part 3.1)

Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.

Version History

Version	Date	Action	Change Tracking
~~1~~	~~May 2, 2006~~	~~Adopted by NERC Board of Trustees~~	
1	~~**January 18, 2008**~~1/16/06	~~**FERC Order issued approving CIP-006-1**~~R3.2 — Change "Control Center" to "control center."	3/24/06
	~~February 12, 2008~~	~~Interpretation of R1 and Additional Compliance Information Section 1.4.4 adopted by NERC Board of Trustees~~	~~Project 2007-27~~
2	9/30/09	~~Updated version number from -1 to -2~~ Modifications to ~~**remove extraneous information from**~~clarify the requirements~~**, improve readability,**~~ and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	~~**Project 2008-06**~~
~~2~~	~~May 6, 2009~~	~~Adopted by NERC Board of Trustees~~	
	~~August 5, 2009~~	~~Interpretation of R4 adopted by NERC Board of Trustees~~	~~Project 2008-15~~
~~2~~	~~September 30, 2009~~	~~FERC Order issued approving CIP-006-2~~	
3	~~**November 18, 2009**~~12/16/09	Updated ~~**version number**~~Version Number from -2 to -3	~~**Project 2009-21**~~

Version	Date	Action	Change Tracking
		~~Revised~~In Requirement 1.6, deleted the sentence pertaining to ~~add a Visitor Control program~~removing component or system from service in order to ~~the Physical Security Plan~~perform testing, in response to FERC order issued September 30, 2009. ~~In Requirement R7, the term "Responsible Entity" was capitalized. Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7~~	
~~3~~	~~December 16, 2009~~	~~Adopted by NERC Board of Trustees~~	
3	~~February~~ 12/16~~,~~ ~~2010~~/09	~~Interpretation of R1 and R1.1 adopted~~Approved by the NERC Board of Trustees~~-~~.	~~Project 2009-13~~
3	~~March~~ 3/31~~,~~ ~~2010~~/10	~~FERC Order issued approving CIP-006-3~~Approved by FERC.	
~~2a/3a~~	~~July 15, 2010~~	~~FERC Order issued approving the Interpretation of R1 and R1.1.~~ ~~Updated version numbers from -2/-3 to -2a/-3a.~~	
4	~~January~~ 1/24~~,~~ ~~2011~~/11	~~Adopted~~Approved by the NERC Board of Trustees.	
~~3c/4c~~5	~~May 19, 2011~~11/26/12	~~FERC Order issued approving two interpretations: 1) Interpretation of R1 and Additional Compliance Information Section 1.4.4; and 2) Interpretation of R4.~~ ~~Updated version number from -3/-4 to -3c/-4c.~~Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
~~4c~~	~~4/19/12~~	~~FERC Order issued approving CIP-006-4c (approval becomes effective June 25, 2012)~~ ~~Added approved VRF/VSL table to section D.2.~~	

~~Appendix 1~~

~~Requirement Number and Text of Requirement~~
~~R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:~~ ~~R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.~~
~~Question~~
~~If a completely enclosed border cannot be created, what does the phrase, "to control physical access" require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption?~~ ~~Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?~~
~~Response~~
~~For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are "physical in nature." The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.~~

~~Appendix 2~~

~~Interpretation of Requirement R1.1.~~

~~Request:~~ ~~*Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*~~

~~Interpretation:~~

~~Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border.~~

~~**CIP-006-1 — Requirement 1.1** requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.~~

> ~~**R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:**~~
>
> ~~**R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.**~~

~~**CIP-006-1 — Additional Compliance Information 1.4.4** identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.~~

> ~~**1.4. Additional Compliance Information**~~
>
> ~~**1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.**~~

~~Appendix 3~~

~~The following interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R4 was developed by the standard drafting team assigned to Project 2008-14 (Cyber Security Violation Severity Levels) on October 23, 2008.~~

~~Request:~~

1. ~~*For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*~~
2. ~~*Does the term, "time of access" mean logging when the person entered the facility or does it mean logging the entry/exit time and "length" of time the person had access to the critical asset?*~~

~~Interpretation:~~

~~No, monitoring and logging of access are only required for ingress at this time. The term "time of access" refers to the time an authorized individual enters the physical security perimeter.~~

~~Requirement Number and Text of Requirement~~

~~R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~

~~R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.~~

~~R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.~~

~~R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.~~

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-5

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-007-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-007-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The

documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact

and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only,

which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as

it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include:

(i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports.

The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are needed. Physical I/O ports were added in response to a FERC order. The unneeded physical ports in Control Centers (which are the highest risk, most impactful areas) should be protected as well.

Reference to prior version: (Part 1.1) CIP-007-4, R2.1 and R2.2

Change Rationale: (Part 1.1)

The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.

Reference to prior version: (Part 1.2) New

Change Rationale: (Part 1.2)

On March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

Rationale for R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security

upgrades for applicability within thirty calendar days of availability of the patches or upgrades" and there has been confusion as to what constitutes the availability date. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

Reference to prior version: (Part 2.1) CIP-007, R3

Change Rationale: (Part 2.1)

The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches. Documenting the source is used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.

Reference to prior version: (Part 2.2) CIP-007, R3.1

Change Rationale: (Part 2.2)

Similar to the current wording but added "from the source or sources identified in 2.1" to clarify the 35-day time frame.

Reference to prior version: (Part 2.3) CIP-007, R3.2

Change Rationale: (Part 2.3)

The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.

Reference to prior version: (Part 2.4) CIP-007, R3.2

Change Rationale: (Part 2.4)

Similar to the current wording but added that the plan must be implemented within the timeframe specified in the plan, or in a revised plan as approved by the CIP Senior Manager or delegate.

Rationale for R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of

that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.

Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"

In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

Reference to prior version: (Part 3.1) CIP-007-4, R4; CIP-007-4, R4.1

Change Rationale: (Part 3.1)

See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.

Reference to prior version: (Part 3.2) *CIP-007-4, R4; CIP-007-4, R4.1*
Change Rationale: (Part 3.2)

See the Summary of Changes.

Reference to prior version: (Part 3.3) CIP-007-4, R4; CIP-007-4, R4.2

Change Rationale: (Part 3.3)

Requirement essentially unchanged from previous versions; updated to refer to previous parts of the requirement table.

Rationale for R4:

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Summary of Changes: Beginning in Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor."

The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the System. There are a few events explicitly listed that if a Cyber Asset or BES Cyber System can log, then it must log.

In addition, this requirement sets up parameters for the monitoring and reviewing of processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

Reference to prior version: (Part 4.1) CIP-005-4, R3; CIP-007-4, R5, R5.1.2, R6.1, and R6.3

Change Rationale: (Part 4.1)

This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.

Reference to prior version: (Part 4.2) CIP-005-4, R3.2; CIP-007-4, R6.2

Change Rationale: (Part 4.2)

This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate a response.

Reference to prior version: (Part 4.3) CIP-005-4, R3.2; CIP-007-4, R6.4

Change Rationale: (Part 4.3)

No substantive change.

Reference to prior version: (Part 4.4) CIP-005-4, R3.2; CIP-007-4, R6.5

Change Rationale: (Part 4.4)

Beginning in Paragraph 525 and also 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information.

Changes to this requirement allow for an approximately biweekly summary or sampling review of logs.

Rationale for R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for

true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

Summary of Changes (From R5):

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT believes these changes strengthen the authentication

mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

Reference to prior version: (Part 5.1) CIP-007-4, R5

Change Rationale: (Part 5.1)

The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.

Reference to prior version: (Part 5.2) CIP-007-4, R5.2 and R5.2.1

Change Rationale: (Part 5.2)

CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.

Reference to prior version: (Part 5.3) CIP-007-4, R5.2.2

Change Rationale: (Part 5.3)

No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.

Reference to prior version: (Part 5.4) CIP-007-4, R5.2.1

Change Rationale: (Part 5.4)

The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.

Reference to prior version: (Part 5.5) CIP-007-4, R5.3

Change Rationale: (Part 5.5)

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password

credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.

Reference to prior version: (Part 5.6) CIP-007-4, R5.3.3

Change Rationale: (Part 5.6)

**This was originally Requirement R5.5.3, but moved to add "external routable connectivity" to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.*

Reference to prior version: (Part 5.7) *New Requirement*

Change Rationale: (Part 5.7)

Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	

3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

1. Title: Cyber Security — ~~Systems~~System Security Management

2. Number: CIP-007-~~4~~5

~~**3. Purpose:** Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.~~

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

~~**4.1.** Within the text of Standard CIP-007-4, "Responsible Entity" shall mean:~~

4.1. ~~Reliability~~ **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

~~4.1.1~~ Interchange Coordinator~~.~~

~~**4.1.2 Balancing Authority.**~~

~~4.1.3~~4.1.5 or Interchange Authority~~.~~

~~**4.1.4 Transmission Service Provider.**~~

4.1.6 Reliability Coordinator

~~4.1.5~~4.1.7 Transmission ~~Owner.~~Operator

~~4.1.6~~ Transmission ~~Operator.~~

~~4.1.7~~4.1.8 ~~Generator~~ Owner~~.~~

~~**4.1.8 Generator Operator.**~~

~~**4.1.9 Load Serving Entity.**~~

~~**4.1.10 NERC.**~~

~~**4.1.11 Regional Entity.**~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

~~**4.2.4**~~**4.2.3 Exemptions:** The following are exempt from Standard CIP-007-~~4:~~5:

~~**4.2.1**~~**4.2.3.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~**4.2.2**~~**4.2.3.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~**4.2.3**~~**4.2.3.3** ~~In nuclear plants, the~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.-R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.4**~~**4.2.3.5** Responsible Entities that~~, in compliance with Standard CIP-002-4,~~ identify that they have no ~~Critical Cyber Assets~~BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective ~~Date: The~~ Dates:

1. **24 Months Minimum** – CIP-007-5 shall become effective on the later of July 1, 2015, or the first ~~day of the eighth~~ calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory ~~approvals have been received (or the Reliability Standard otherwise becomes effective~~ approval.

~~**5.**~~ 2. In those jurisdictions where no regulatory approval is required, CIP-007-5 shall become effective on the first day of the ninth calendar quarter ~~after BOT adoption in those jurisdictions where regulatory approval is not required).~~following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

~~**B. Requirements**~~

~~Test Procedures — The~~ **6. Background:**

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural

controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall* ~~ensure that new~~*implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets ~~and significant changes to existing~~in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets** ~~within the Electronic~~ **(PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R5 – System Access Controls. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter ~~do~~ in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that

bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not ~~adversely affect existing~~ limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security ~~controls~~patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking

involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can

document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or

method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the

operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes~~ of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.~~, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

- ~~The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.~~
- ~~The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.~~
- ~~The Responsible Entity shall document test results.~~

~~Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.~~

- ~~The Responsible Entity shall enable only those ports and services required for normal and emergency operations.~~

- ~~The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).~~
- ~~In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.~~

~~Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).~~

~~The Responsible Entity shall~~ **4.4.** Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are needed. Physical I/O ports were added in response to a FERC order. The unneeded physical ports in Control Centers (which are the highest risk, most impactful areas) should be protected as well.

Reference to prior version: (Part 1.1) CIP-007-4, R2.1 and R2.2

Change Rationale: (Part 1.1)

The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.

Reference to prior version: (Part 1.2) New

Change Rationale: (Part 1.2)

On March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

Rationale for R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

~~1.1.~~ **Summary of Changes:** The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" and there has been confusion as to what constitutes the availability date. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

- ~~The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.~~

~~Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).~~

- ~~The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.~~
- ~~The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.~~

~~Account Management — The Responsible Entity shall~~**Reference to prior version:** (Part 2.1) CIP-007, R3

Change Rationale: (Part 2.1)

The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches. Documenting the source is used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.

Reference to prior version: (Part 2.2) CIP-007, R3.1

Change Rationale: (Part 2.2)

Similar to the current wording but added "from the source or sources identified in 2.1" to clarify the 35-day time frame.

Reference to prior version: (Part 2.3) CIP-007, R3.2

Change Rationale: (Part 2.3)

The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.

Reference to prior version: (Part 2.4) CIP-007, R3.2

Change Rationale: (Part 2.4)

Similar to the current wording but added that the plan must be implemented within the timeframe specified in the plan, or in a revised plan as approved by the CIP Senior Manager or delegate.

Rationale for R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.

Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"

In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

Reference to prior version: (Part 3.1) CIP-007-4, R4; CIP-007-4, R4.1

Change Rationale: (Part 3.1)

See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.

Reference to prior version: (Part 3.2) *CIP-007-4, R4; CIP-007-4, R4.1*
Change Rationale: (Part 3.2)

See the Summary of Changes.

Reference to prior version: (Part 3.3) CIP-007-4, R4; CIP-007-4, R4.2

Change Rationale: (Part 3.3)

Requirement essentially unchanged from previous versions; updated to refer to previous parts of the requirement table.

Rationale for R4:

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Summary of Changes: Beginning in Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms “security event” and “monitor.”

The term “security event” or “events related to cyber security” is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the System. There are a few events explicitly listed that if a Cyber Asset or BES Cyber System can log, then it must log.

In addition, this requirement sets up parameters for the monitoring and reviewing of processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

Reference to prior version: (Part 4.1) CIP-005-4, R3; CIP-007-4, R5, R5.1.2, R6.1, and R6.3

Change Rationale: (Part 4.1)

This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed

confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.

Reference to prior version: (Part 4.2) CIP-005-4, R3.2; CIP-007-4, R6.2

Change Rationale: (Part 4.2)

This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate a response.

Reference to prior version: (Part 4.3) CIP-005-4, R3.2; CIP-007-4, R6.4

Change Rationale: (Part 4.3)

No substantive change.

Reference to prior version: (Part 4.4) CIP-005-4, R3.2; CIP-007-4, R6.5

Change Rationale: (Part 4.4)

Beginning in Paragraph 525 and also 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for an approximately biweekly summary or sampling review of logs.

Rationale for R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most

effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

Summary of Changes (From R5):

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT believes these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

Reference to prior version: (Part 5.1) CIP-007-4, R5

Change Rationale: (Part 5.1)

The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document *controls is included in this introductory requirement. The requirement to have* technical and procedural controls ~~that enforce access authentication of, and accountability for, all user activity, and~~ *was removed because technical controls suffice when procedural documentation is already required. The phrase "*that minimize the risk of unauthorized ~~system access.~~*access" was removed and more appropriately captured in the rationale statement.*

- ~~The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.~~
  - ~~The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.~~
  - ~~The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.~~
  - ~~The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.~~

~~The Responsible Entity shall implement a policy~~ **Reference to prior version:** (Part 5.2) CIP-007-4, R5.2 and R5.2.1

Change Rationale: (Part 5.2)

~~1.2.~~ *CIP-007-4 requires entities to minimize and manage the scope and acceptable use of* ~~administrator, shared, and other generic account privileges including factory default accounts.~~*account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*

Reference to prior version: (Part 5.3) CIP-007-4, R5.2.2

Change Rationale: (Part 5.3)

No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.

Reference to prior version: (Part 5.4) CIP-007-4, R5.2.1

Change Rationale: (Part 5.4)

The ~~policy shall include~~ *requirement for the "removal, disabling*~~,~~ *or renaming of such accounts where possible*~~. For such accounts that must remain enabled,~~ *" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords* ~~shall be~~*to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.*

Reference to prior version: (Part 5.5) CIP-007-4, R5.3

Change Rationale: (Part 5.5)

~~1.2.1.~~ *CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed* ~~prior to putting any system into service.~~*to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.*

- ~~The Responsible Entity shall identify those individuals with access to shared accounts.~~
- ~~Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).~~

o ~~At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:~~

- ~~Each password shall be a minimum of six characters.~~

- ~~Each password shall consist of a combination of alpha, numeric, and "special" characters.~~
- ~~Each password shall be changed at least annually, or more frequently based on risk.~~

~~Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.~~

- ~~The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.~~
- ~~The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.~~
- ~~The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.~~
- ~~The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.~~
- ~~The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.~~

~~Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.~~

- ~~Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.~~
- ~~Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.~~
- ~~The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.~~

~~Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:~~

- ~~A document identifying the vulnerability assessment process;~~
- ~~A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;~~
- ~~A review of controls for default accounts; and,~~
- ~~Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.~~

~~Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.~~

~~C. Measures~~

~~The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.~~

~~The Responsible Entity shall make available documentation as specified in Requirement R2.~~

~~The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.~~

~~The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.~~

~~The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.~~

~~The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.~~

~~The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.~~

~~The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.~~

~~The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.~~

~~D. Compliance~~

~~1. Compliance Monitoring Process~~

~~1.1. Compliance Enforcement Authority~~

~~1.2. The RE shall serve as the CEA with the following exceptions:~~

~~1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.~~

~~1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.~~

~~1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.~~

~~1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.~~

~~1.3. Compliance Monitoring and Enforcement Processes~~

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~1.4. Data Retention~~

~~1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.~~

~~1.4.2 The Responsible Entity shall retain security-related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-4 Requirement R2.~~

~~1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.~~

~~1.5. Additional Compliance Information.~~

~~2. Violation Severity Levels~~

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1.~~	~~MEDIUM~~	~~N/A~~	~~The Responsible Entity did create, implement and maintain the test procedures as required in R1.1, **but did not document** that testing is performed as required in R1.2.~~ ~~OR~~ ~~The Responsible Entity did not document the test results as required in R1.3.~~	~~The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1.~~	~~The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1,~~ ~~AND~~ ~~The Responsible Entity did not document that testing was performed as required in R1.2~~ ~~AND~~ ~~The Responsible Entity did not document the test results as required in R1.3.~~
~~R1.1.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R1.2.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R1.3.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R2.~~	~~MEDIUM~~	~~N/A~~	~~The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.~~	~~The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.~~	~~The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.~~
~~R2.1.~~	~~MEDIUM~~	~~The Responsible Entity enabled ports and services not required for normal and emergency operations on at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).~~	~~The Responsible Entity enabled ports and services not required for normal and emergency operations on 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).~~	~~The Responsible Entity enabled ports and services not required for normal and emergency operations on 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).~~	~~The Responsible Entity enabled ports and services not required for normal and emergency operations on 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).~~

~~R2.2.~~	~~MEDIUM~~	~~The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).~~	~~The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).~~	~~The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).~~	~~The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).~~
~~R2.3.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk exposure.~~
~~R3.~~	~~LOWER~~	~~The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program **but** did not include one or more of the following:~~ ~~tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).~~	~~The Responsible Entity established (implemented) but did not document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).~~	~~The Responsible Entity documented but did not establish (implement), either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).~~	~~The Responsible Entity did not establish (implement) nor document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).~~
~~R3.1.~~	~~LOWER~~	~~The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in more than 30 but less than 60 calendar days~~	~~The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 60 or more but less than 90 calendar days after the availability of the patches and upgrades.~~	~~The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 90 or more but less than 120 calendar days after the availability of the patches and upgrades.~~	~~The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 120 calendar days or more after the availability of the patches and upgrades.~~

		~~after the availability of the patches and upgrades.~~			
~~R3.2.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did not document the implementation of applicable security patches as required in R3.~~ ~~OR~~ ~~Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk exposure.~~
~~R4.~~	~~MEDIUM~~	~~The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).~~	~~The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).~~	~~The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).~~	~~The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software ("malware") prevention tools, nor implemented compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).~~
~~R4.1.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter.~~ ~~OR~~ ~~The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.~~
~~R4.2.~~	~~MEDIUM~~	~~The Responsible Entity, as technically feasible, documented and implemented a process for the update of anti-virus and malware prevention "signatures.", but the process did not address testing and installation of the signatures.~~	~~The Responsible Entity, as technically feasible, did not document but implemented a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."~~	~~The Responsible Entity, as technically feasible, documented but did not implement a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."~~	~~The Responsible Entity, as technically feasible, did not document nor implement a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."~~
~~R5.~~	~~LOWER~~	~~N/A~~	~~The Responsible Entity implemented but did not document technical and procedural controls that enforce~~	~~The Responsible Entity documented but did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.~~	~~The Responsible Entity did not document nor implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.~~

			~~access authentication of, and accountability for, all user activity.~~		
~~R5.1.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.~~
~~R5.1.1.~~	~~LOWER~~	~~At least one user account but less than 1% of user accounts implemented by the Responsible Entity, were not approved by designated personnel.~~	~~One (1) % or more of user accounts but less than 3% of user accounts implemented by the Responsible Entity were not approved by designated personnel.~~	~~Three (3) % or more of user accounts but less than 5% of user accounts implemented by the Responsible Entity were not approved by designated personnel.~~	~~Five (5) % or more of user accounts implemented by the Responsible Entity were not approved by designated personnel.~~
~~R5.1.2.~~	~~LOWER~~	~~N/A~~	~~The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.~~	~~The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.~~	~~The Responsible Entity did not generate logs of individual user account access activity.~~
~~R5.1.3.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.~~
~~R5.2.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.~~
~~R5.2.1.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.~~	~~For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.~~
~~R5.2.2.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did not identify all individuals with access to shared accounts.~~
~~R5.2.3.~~	~~MEDIUM~~	~~N/A~~	~~Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 1 of the following 3 items:~~ ~~a) limits access to only those~~	~~Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 2 of the following 3 items:~~ ~~a) limits access to only those with authorization,~~ ~~b) has an audit trail of the account use (automated or manual),~~	~~Where such accounts must be shared, the Responsible Entity does not have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).~~

			~~with authorization,~~ ~~b) has an audit trail of the account use (automated or manual),~~ ~~c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).~~	~~c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).~~	
~~R5.3.~~	~~LOWER~~	~~The Responsible Entity requires and uses passwords as technically feasible, but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.~~	~~The Responsible Entity requires and uses passwords as technically feasible but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.~~	~~The Responsible Entity requires but does not use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.~~	~~The Responsible Entity does not require nor use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.~~
~~R5.3.1.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R5.3.2.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R5.3.3.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R6.~~	~~LOWER~~	~~The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for at least one but less than 5% of Cyber Assets inside the Electronic Security Perimeter(s).~~	~~The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for 5% or more but less than 10% of Cyber Assets inside the Electronic Security Perimeter(s).~~	~~The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 10% or more but less than 15% of Cyber Assets inside the Electronic Security Perimeter(s).~~	~~The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 15% or more of Cyber Assets inside the Electronic Security Perimeter(s).~~
~~R6.1.~~	~~MEDIUM~~	~~N/A~~	~~The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for monitoring for security events~~	~~The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.~~	~~The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.~~

			~~on all Cyber Assets within the Electronic Security Perimeter.~~		
~~R6.2.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.~~
~~R6.3.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.~~
~~R6.4.~~	~~LOWER~~	~~The Responsible Entity retained the logs specified in Requirement R6, for at least 60 days, but less than 90 days.~~	~~The Responsible Entity retained the logs specified in Requirement R6, for at least 30 days, but less than 60 days.~~	~~The Responsible Entity retained the logs specified in Requirement R6, for at least one day, but less than 30 days.~~	~~The Responsible Entity did not retain any logs specified in Requirement R6.~~
~~R6.5.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.~~
~~R7.~~	~~LOWER~~	~~The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP- 005-4 **but** did not maintain records as specified in R7.3.~~	~~The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address redeployment as specified in R7.2.~~	~~The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address disposal as specified in R7.1.~~	~~The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.~~
~~R7.1.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R7.2.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~

~~R7.3.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R8~~	~~LOWER~~	~~The Responsible Entity performed at least annually a Vulnerability Assessment that included 95% or more but less than 100% of Cyber Assets within the Electronic Security Perimeter.~~	~~The Responsible Entity performed at least annually a Vulnerability Assessment that included 90% or more but less than 95% of Cyber Assets within the Electronic Security Perimeter.~~	~~The Responsible Entity performed at least annually a Vulnerability Assessment that included more than 85% but less than 90% of Cyber Assets within the Electronic Security Perimeter.~~	~~The Responsible Entity performed at least annually a Vulnerability Assessment for 85% or less of Cyber Assets within the Electronic Security Perimeter.~~ ~~OR~~ ~~The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.~~
~~R8.1.~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R8.2.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R8.3.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R8.4.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R9~~	~~LOWER~~	~~N/A~~	~~N/A~~	~~The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually.~~ ~~OR~~ ~~The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.~~	~~The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually~~ ~~**nor**~~ ~~were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.~~

~~E. Regional Variances~~

~~None identified.~~

Reference to prior version: (Part 5.6) CIP-007-4, R5.3.3

Change Rationale: (Part 5.6)

**This was originally Requirement R5.5.3, but moved to add "external routable connectivity" to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.*

Reference to prior version: (Part 5.7) *New Requirement*

Change Rationale: (Part 5.7)

Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment ~~**and acceptance of risk.**~~. ~~Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter.~~ Replaced the RRO with the RE as a	

		responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version numbersnumber from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
34	1/24/11 12/16/09	Approved by the NERC Board of Trustees.	Update
45	Board approved 01/24/2011 11/26/12	Adopted by the NERC Board of Trustees. Update version number from "3" to "4"	Modified to coordinate with other CIP standards and to revise format to use RBS Template. Update to conform to changes to CIP-002-4 (Project 2008-06)
4	4/19/12	FERC Order issued approving CIP-007-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-5

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-008-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-008-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-008-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain records related to Reportable Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident.*

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with	The Responsible Entity has not updated the	The Responsible Entity has neither	The Responsible Entity has neither

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR	documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the	documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a Cyber Security Incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. Table top exercises (TTX) can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response

activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

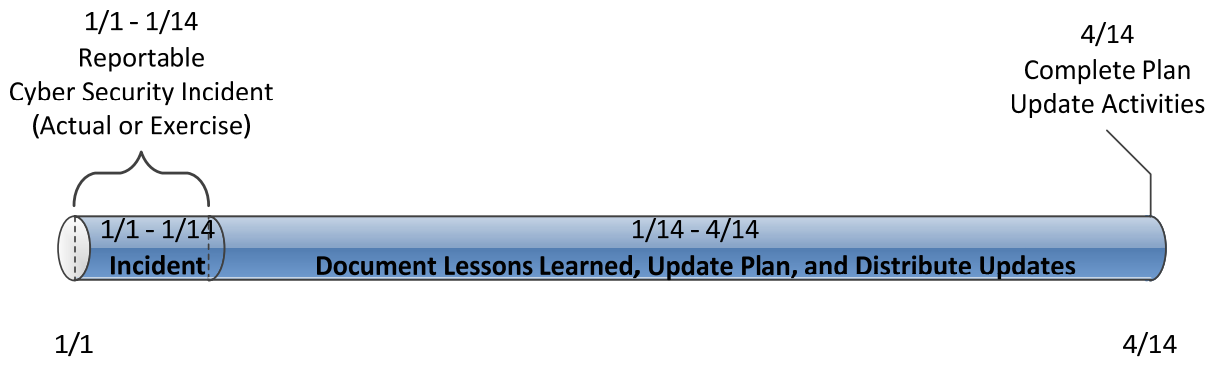

Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the incident and documenting the lessons learned as soon after the incident as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the incident response team.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

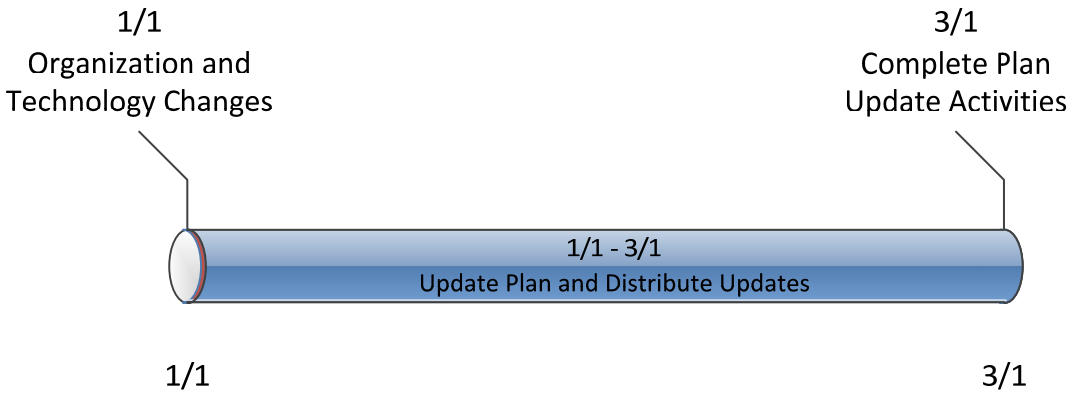

Figure 2: Timeline for Plan Changes in 3.2

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)

"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)

Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)

Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)

Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the

plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)

Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	

4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-~~4~~5

3. Purpose: ~~Standard CIP-008-4 ensures~~To mitigate the ~~identification, classification, response, and reporting~~risk to the reliable operation of the BES as the result of a Cyber Security ~~Incidents related to Critical Cyber Assets.~~ Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard ~~CIP-008-4 should be read as part of a~~ .

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

~~**3.**~~**4.1.2.4** Each Cranking Path and group of ~~standards numbered Standards CIP-002-4 through CIP-009-4.~~ Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~**4. Applicability**~~

~~**4.1.** Within the text of Standard CIP-008-4, "Responsible Entity" shall mean:~~

4.1.3 ~~Reliability~~**Generator Operator**

4.1.4 Generator Owner

~~**4.1.1**~~ **Interchange Coordinator**~~.~~

~~**4.1.2 Balancing Authority.**~~

~~**4.1.3**~~**4.1.5 or Interchange Authority**~~.~~

~~**4.1.4 Transmission Service Provider.**~~

4.1.6 Reliability Coordinator

~~**4.1.5**~~**4.1.7 Transmission** ~~Owner.~~**Operator**

~~**4.1.6**~~ **Transmission** ~~Operator.~~

~~**4.1.7**~~**4.1.8** ~~Generator~~ **Owner**~~.~~

~~**4.1.8 Generator Operator.**~~

~~**4.1.9 Load Serving Entity.**~~

~~**4.1.10 NERC.**~~

~~**4.1.11 Regional Entity.**~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

~~**4.2.4**~~**4.2.3 Exemptions:** The following are exempt from Standard CIP-008-~~4:~~5:

~~**4.2.1**~~**4.2.3.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~**4.2.2**~~**4.2.3.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~**4.2.3**~~**4.2.3.3** ~~In nuclear plants, the~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.4**~~**4.2.3.5** Responsible Entities that~~, in compliance with Standard CIP-002-4,~~ identify that they have no ~~Critical~~BES Cyber ~~Assets~~Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective ~~Date: The~~ Dates:

1. **24 Months Minimum** – CIP-008-5 shall become effective on the later of July 1, 2015, or the first ~~day of the eighth~~ calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory ~~approvals have been received (or the Reliability Standard otherwise becomes effective~~ approval.

~~**5.**~~ 2. In those jurisdictions where no regulatory approval is required, CIP-008-5 shall become effective on the first day of the ninth calendar quarter ~~after BOT adoption in those jurisdictions where regulatory approval is not required).~~following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

B. Requirements and Measures

~~Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a~~

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 –* Cyber Security Incident ~~response plan and implement the plan in response to Cyber Security Incidents. The~~ *Response Plan Specifications. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

~~**R1.**~~**M1.** Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 –* Cyber Security Incident ~~response plan shall address, at a minimum, the following:~~*Response Plan Specifications.*

~~**1.1.** Procedures to characterize and classify events as reportable Cyber Security Incidents.~~

~~**1.2.** Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.~~

~~**1.3.** Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.~~

~~**1.4.** Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.~~

~~**1.5.** Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.~~

~~**1.6.** Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.~~

~~**R2.** Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.~~

~~C. Measures~~

~~The~~

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

~~**M1.**~~**R2.** Each Responsible Entity shall ~~make available~~implement each of its documented Cyber Security Incident response ~~plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.~~plans to collectively include each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

~~**M2.** The Responsible Entity shall make available all documentation as specified in Requirement R2.~~

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain records related to Reportable Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident.*

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			

Part	Applicable Systems	Requirements	Measures
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

D.C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, theThe Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authoritiesauthority shall serve as the Compliance Enforcement AuthorityCEA.

1.2. For the ERO, a third-party monitor without vested interestEvidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in the outcomethis standard for the EROthree calendar years.

1.2.4• If a Responsible Entity is found non-compliant, it shall serve askeep information related to the non-compliance until mitigation is complete and approved or for the Compliance Enforcement Authoritytime specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and EnforcementAssessment Processes:

- Compliance AuditsAudit
- Self-CertificationsCertification
- Spot Checking
- Compliance Violation InvestigationsInvestigation
- Self-Reporting

Complaints

1.4. Data Retention

~~1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-4 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.~~

~~1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.~~

- Complaint

~~1.5.~~1.4. Additional Compliance Information:

~~1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.~~

~~1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.~~

~~2. Violation Severity Levels~~

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
2.		VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	**Long Term Planning**	LOWER **Lower**	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.N/A	The Responsible Entity has developed athe Cyber Security Incident response plan(s), but the plan does not address oneinclude the roles and responsibilities of Cyber Security Incident response groups or more of the subrequirements R1.individuals. (1 through.3) R1.6.OR The Responsible Entity has developed the Cyber Security Incident response	The Responsible Entity has not developed a Cyber Security Incident response plan orwith one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has not implemented the plan in response to developed a Cyber Security Incident. response plan, but the plan does not include one or more processes to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
2.		VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
					plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but did not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
R1.1.		LOWER	N/A	N/A	N/A	N/A
R1.2. R	Operations	LOWERLowe	N/AThe Responsible Entity has not tested	N/AThe Responsible Entity has not tested	N/AThe Responsible Entity has not tested	N/AThe Responsible Entity has not tested

2	Planning Real-time Operations	r	the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)
R1.3.	LOWER	N/A	N/A	N/A	N/A	
R1.4.	LOWER	N/A	N/A	N/A	N/A	
R1.5.	LOWER	N/A	N/A	N/A	N/A	
R1.6.	LOWER	N/A	N/A	N/A	N/A	
R2R3	Operations Assessment	LOWER Lower	The Responsible Entity has kept relevant documentation related to not notified each person or group	The Responsible Entity has kept relevant documentation related to not updated the Cyber Security Incidents reportable per Requirement R1.1	The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 forneither documented	The Responsible Entity has not kept relevant documentation relatedneither documented lessons

			with a defined role in the Cyber Security Incidents reportable per Requirement R1.1 for twoIncident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than three120 calendar years.days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	forIncident response plan based on any documented lessons learned within 90 and less than two120 calendar yearsdays of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response	lessons learned nor documented the absence of any lessons learned within 90 and less than one120 calendar yeardays of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group	learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incidents reportable per Requirement R1Incident. (3.1.1)

				plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

E.D. Regional Variances

None identified.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a Cyber Security Incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. Table top exercises (TTX) can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response

activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

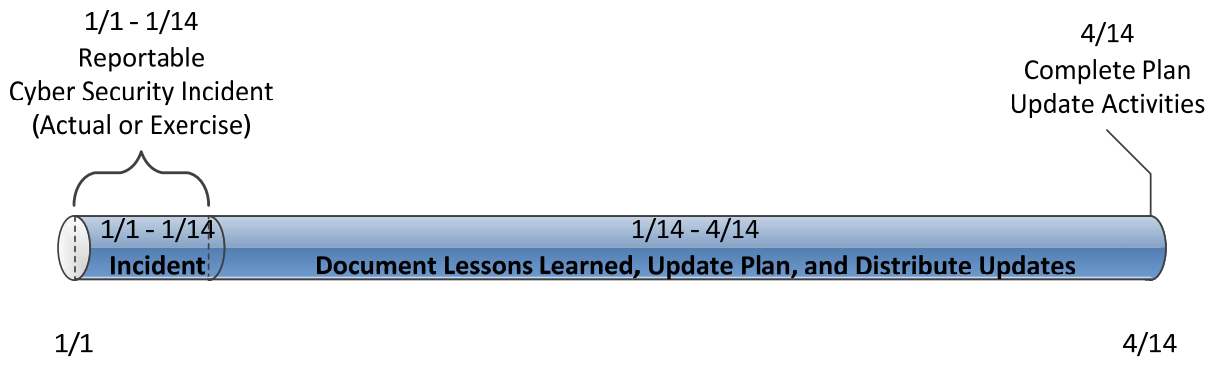

Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the incident and documenting the lessons learned as soon after the incident as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the incident response team.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

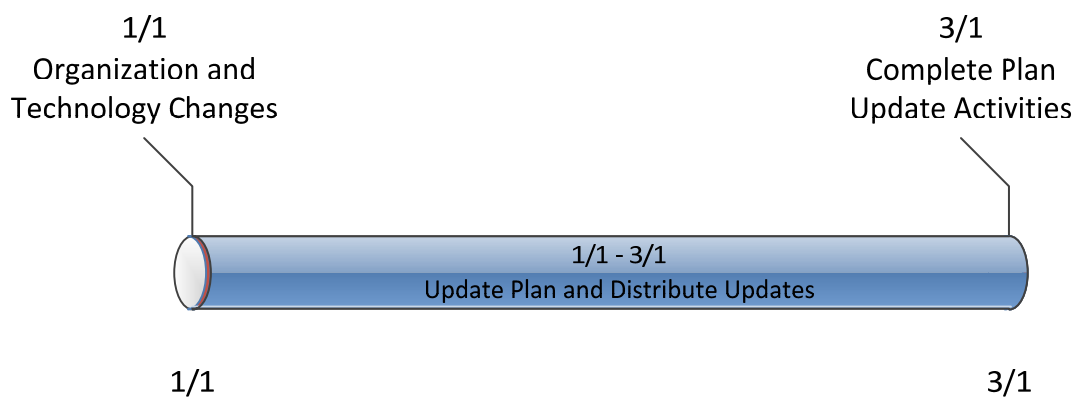

Figure 2: Timeline for Plan Changes in 3.2

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)

"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)

Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)

Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)

Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)

Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)

Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a	

		~~**responsible entity.**~~Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated ~~**Version**~~version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
~~4~~5	~~Board approved 01/24/2011~~11/26/12	~~**Update version number from "3" to "4"**~~Adopted by the NERC Board of Trustees.	~~Update to conform to changes to CIP-002-4 (Project 2008-06)~~Modified to coordinate with other CIP standards and to revise format to use RBS Template.
~~**4**~~	~~4/19/12~~	~~FERC Order issued approving CIP-008-4 (approval becomes effective June 25, 2012)~~ ~~Added approved VRF/VSL table to section D.2.~~	

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-5

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-009-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The

documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.
R2	**Operations**	**Lower**	The Responsible	The Responsible	The Responsible	The Responsible

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning **Real-time Operations**		Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests, and when tested, any	Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any deficiencies were	Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests, and when tested, any deficiencies were	Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has tested a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 and identified deficiencies, but did not assess or correct

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

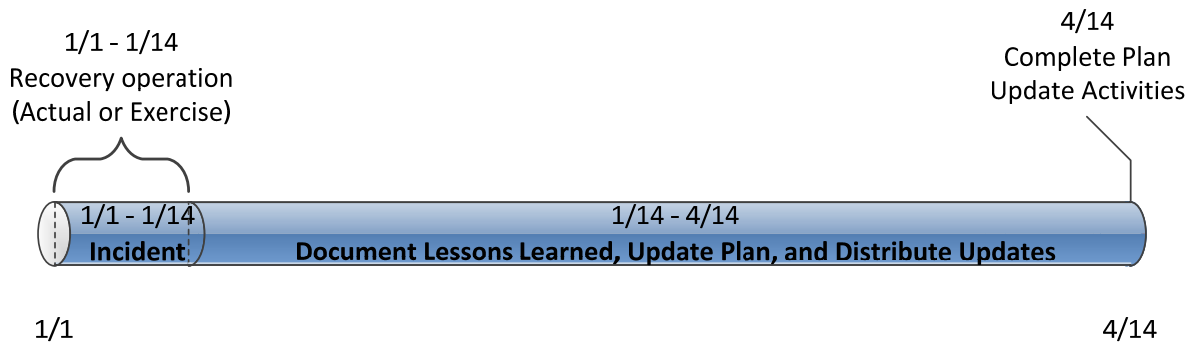

Figure 1: CIP-009-5 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

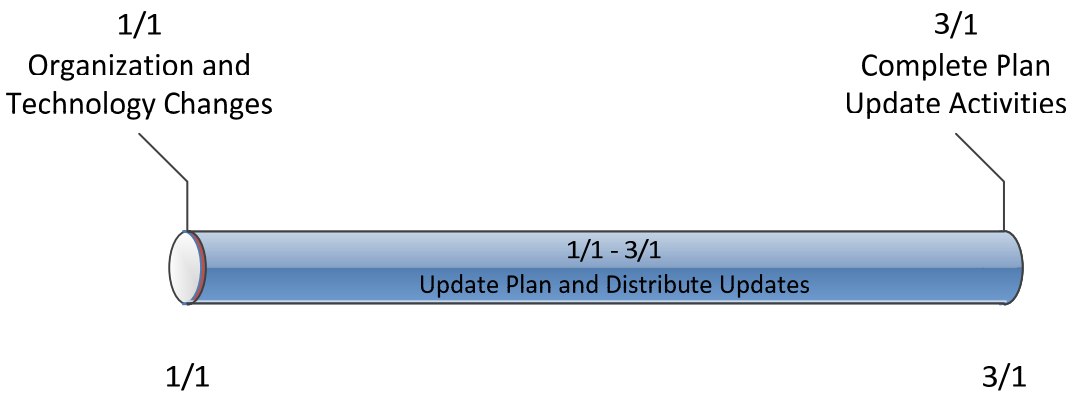

Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.

Reference to prior version: (Part 1.1) CIP-009, R1.1

Change Description and Justification: (Part 1.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.2) CIP-009, R1.2

Change Description and Justification: (Part 1.2)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.3) CIP-009, R4

Change Description and Justification: (Part 1.3)

Addresses FERC Order Paragraph 739 and 748. The modified wording was abstracted from Paragraph 744.

Reference to prior version: (Part 1.4) New Requirement

Change Description and Justification: (Part 1.4)

Addresses FERC Order Section 739 and 748.

Reference to prior version: (Part 1.5) New Requirement

Change Description and Justification: (Part 1.5)

Added requirement to address FERC Order No. 706, Paragraph 706.

Rationale for R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP-009, R2

Change Description and Justification: (Part 2.1)

Minor wording change; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-009, R5

Change Description and Justification: (Part 2.2)

Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.

Reference to prior version: (Part 2.3) CIP-009, R2

Change Description and Justification: (Part 2.3)

Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.

Rationale for R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

Summary of Changes: Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.

Reference to prior version: (Part 3.1) CIP-009, R1 and R3

Change Description and Justification: (Part 3.1)

Added the timeframes for performing lessons learned and completing the plan updates. This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.

Reference to prior version: (Part 3.2) New Requirement

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the specific changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

1. Title: Cyber Security — Recovery Plans for ~~Critical~~BES Cyber ~~Assets~~Systems

2. Number: CIP-009-~~4~~5

~~**3. Purpose:** Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.~~

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

~~**4.1.** Within the text of Standard CIP-009-3, "Responsible Entity" shall mean:~~

~~**4.1.1** Reliability Coordinator~~

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

~~**4.1.2**~~**4.1.1** **Balancing Authority**

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first

interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

~~4.1.3~~4.1.5 Interchange Coordinator or Interchange Authority

~~4.1.4 Transmission Service Provider~~

4.1.6 Reliability Coordinator

~~4.1.5~~4.1.7 Transmission ~~Owner~~Operator

~~4.1.6~~ Transmission ~~Operator~~

~~4.1.7~~4.1.8 ~~Generator~~ Owner

~~4.1.8 Generator Operator~~

~~4.1.9 Load Serving Entity~~

~~4.1.10 NERC~~

~~4.1.11 Regional Entity~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first

interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

~~4.2.4~~4.2.3 Exemptions: The following are exempt from Standard CIP-009-~~4:~~5:

~~4.2.1~~**4.2.3.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.2~~**4.2.3.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.3~~**4.2.3.3** ~~In nuclear plants, the~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.-R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.4~~ Responsible Entities that~~, in compliance with Standard CIP-002-4,~~ identify that they have no ~~Critical~~BES Cyber ~~Assets.~~

4.2.3.5 ~~**Effective Date:** The first day of the eighth calendar quarter after applicable regulatory approvals have been received (~~Systems categorized as high impact or medium impact according to the ~~Reliability Standard otherwise becomes~~CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after ~~BOT adoption in~~the effective date of the order providing applicable regulatory approval.

~~5.~~ 2. In those jurisdictions where no regulatory approval is ~~not~~ required~~).~~

~~B. Requirements~~

~~**R1.** Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s)~~, CIP-009-5 shall ~~address at a minimum the~~ become effective on the first day of the ninth calendar quarter following~~:~~

~~**1.1.** Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).~~

~~**1.2.** Define the roles and responsibilities of responders.~~

~~**R2.** Exercises — The recovery plan(s) shall be exercised at least annually. An exercise~~ Board of ~~the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.~~

~~**R3.**Change Control — Recovery plan(s) shall be updated to reflect any changes~~Trustees' approval, or ~~lessons learned as a result of an exercise or~~ as otherwise made effective pursuant to the ~~recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed~~laws applicable to such ERO governmental authorities.

~~**R4.** Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.~~

~~**R5.** Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.~~

~~C. Measures~~

~~The~~ **6. Background:**

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

~~**M1.**~~Each Responsible Entity shall ~~make available its recovery plan(s) as specified in Requirement R1~~implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

~~**M2.** The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.~~

~~**M3.** The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.~~

~~**M4.** The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.~~

~~**M5.** The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the

standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

D.C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, theThe Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authoritiesauthority shall serve as the Compliance Enforcement AuthorityCEA.

1.2. For the ERO, a third-party monitor without vested interest**Evidence Retention:**

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in the outcomethis standard for the EROthree calendar years.

1.2.4• If a Responsible Entity is found non-compliant, it shall serve askeep information related to the non-compliance until mitigation is complete and approved or for the Compliance Enforcement Authoritytime specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and EnforcementAssessment Processes:

- Compliance AuditsAudit
- Self-CertificationsCertification
- Spot Checking
- Compliance Violation InvestigationsInvestigation
- Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

- Complaint

1.5.1.4. Additional Compliance Information :

2. Violation Severity Levels

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
Requirement		VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	MEDIUM**Medium**	N/A	The Responsible Entity has not annually revieweddeveloped recovery plan(s) for Critical Cyber Assets.), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has createddeveloped recovery plan(s) for Critical Cyber Assets), but didthe plan(s) do not address onetwo of the requirements CIP-009-4 R1.included in Parts 1 or R1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for CriticalBES Cyber Assets thatSystems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address at a minimum boththe conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
Requirement		VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
						the requirements CIP-009-4 R1.1 and R1in Parts 1.2 through 1.5.
R1.1.	MEDIUM	N/A	N/A	N/A		N/A
R1.2.	MEDIUM	N/A	N/A	N/A		N/A
R2	LOWER	N/A	N/A	N/A		The Responsible Entity's recovery plan(s) have not been exercised at least annually.
R3R2	Operations Planning Real-time Operations	LOWERLower	The Responsible Entity's Entity has not tested the recovery plan(s) have been updatedaccording to reflectR2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise orEntity has not tested the recovery from an actual incident but the updatesplan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were communicated to personnel responsible for the activation	The Responsible Entity's Entity has not tested the recovery plan(s) have been updatedaccording to reflectR2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the	The Responsible Entity's recovery plan(s) haveEntity has not been updated to reflect any changes or lessons learned as a result of an exercise or tested the recovery from an actual incident.plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR

			updatesdeficiencies were communicated to personnel responsible for the activation and implementationidentified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan(s) in more than 30 but less than or equal	and implementationidentified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change. according to R2 Part 2.3 within 37	updatesdeficiencies were communicated to personnel responsible for the activation and implementationidentified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan(s) in more than 150	The Responsible Entity's Entity has tested the recovery plan(s) have been updatedaccording to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incidentR2 Part 2.1 and identified deficiencies, but the updates were communicated to personnel responsible fordid not assess or correct the activation and implementation of deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in more than 180 calendar

			according to 120 calendar days of the change.R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	calendar months, not exceeding 38 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	but less than or equal according to 180 calendar days of the change.R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	daysthe recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has tested a representative sample of the change.information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System

						functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2

						Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R4R3	**Operations Assessment**	LOWERLower	N/AThe Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	N/AThe Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the	N/AThe Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR	The Responsible Entity's Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. test or actual recovery. (3.1.1)

				recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or Technology changes.	

R5		LOWER	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.

~~E.~~D. Regional Variances

None ~~identified~~.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

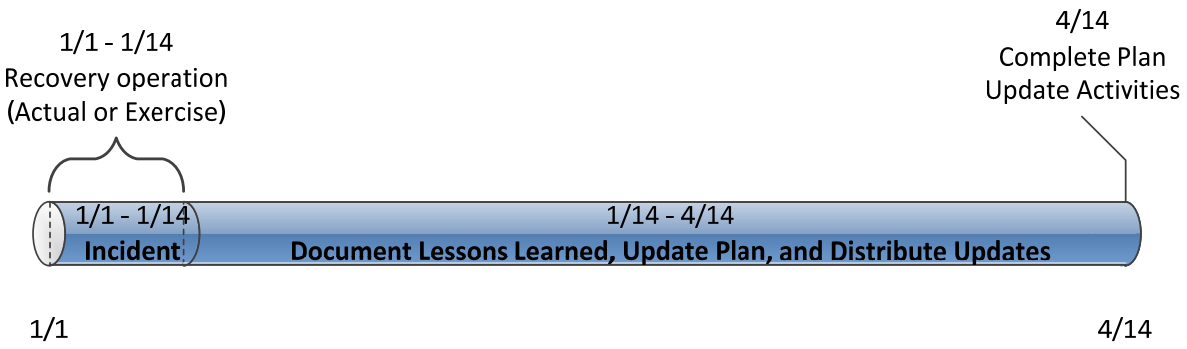

Figure 1: CIP-009-5 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

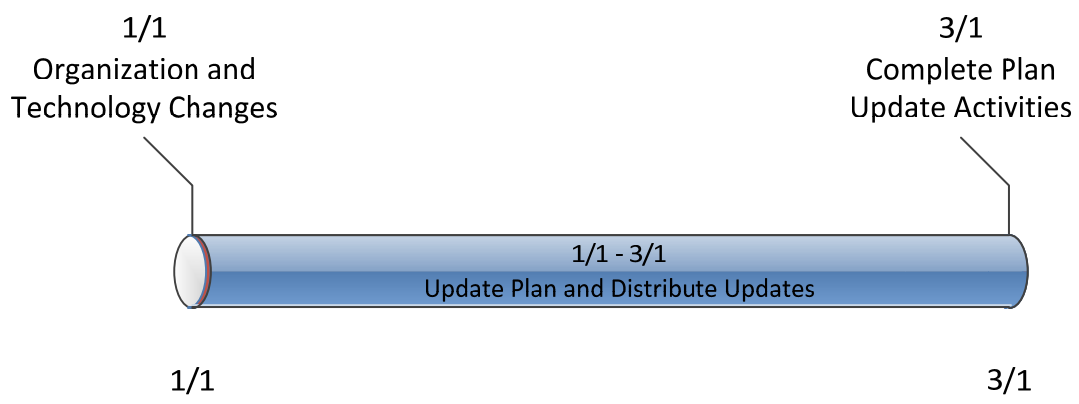

Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.

Reference to prior version: (Part 1.1) CIP-009, R1.1

Change Description and Justification: (Part 1.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.2) CIP-009, R1.2

Change Description and Justification: (Part 1.2)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.3) CIP-009, R4

Change Description and Justification: (Part 1.3)

Addresses FERC Order Paragraph 739 and 748. The modified wording was abstracted from Paragraph 744.

Reference to prior version: (Part 1.4) New Requirement

Change Description and Justification: (Part 1.4)

Addresses FERC Order Section 739 and 748.

Reference to prior version: (Part 1.5) New Requirement

Change Description and Justification: (Part 1.5)

Added requirement to address FERC Order No. 706, Paragraph 706.

Rationale for R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP-009, R2

Change Description and Justification: (Part 2.1)

Minor wording change; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-009, R5

Change Description and Justification: (Part 2.2)

Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.

Reference to prior version: (Part 2.3) CIP-009, R2

Change Description and Justification: (Part 2.3)

Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.

Rationale for R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

Summary of Changes: Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.

Reference to prior version: (Part 3.1) CIP-009, R1 and R3

Change Description and Justification: (Part 3.1)

Added the timeframes for performing lessons learned and completing the plan updates. This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.

Reference to prior version: (Part 3.2) New Requirement

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the specific changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a ~~responsible entity.~~Responsible Entity. Rewording of Effective Date. ~~Communication of revisions to the recovery~~	

		plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbersnumber from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
45	Board approved 01/24/2011 1/26/12	Update version number from "3" to "4"Adopted by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)Modified to coordinate with other CIP standards and to revise format to use RBS Template.
4	4/19/12	FERC Order issued approving CIP-009-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-1

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 **Balancing Authority**

4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 **Generator Operator**

4.1.4 **Generator Owner**

4.1.5 **Interchange Coordinator or Interchange Authority**

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-010-1:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-010-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.

2. In those jurisdictions where no regulatory approval is required, CIP-010-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-010-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The

documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately

based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)**– Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)**– Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible	identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to determine required	deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) that requires authorization and documentation for	implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct	security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline	changes that deviate from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) to update	the deficiencies. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the deficiencies in the verification documentation. (1.4.3)	configuration but did not identify, assess, or correct the deficiencies in the determination of affected security controls. (1.4.1)	baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the	The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficiencies. (1.3) OR The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2) OR The Responsible Entity has a process(es) to verify that required security controls in	required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the required controls. (1.4.2) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencies.	the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					(1.5.1) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					identified deficiencies but did not assess or correct the deficiencies. (1.5.2) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)	
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days and identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days but did not identify, assess, or correct the deficiencies. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems.	assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(3.2)			its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be

included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-5. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-5 R2.1 requires entities to track, evaluate, and install security patches, CIP-010 R1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a

major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.

3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Reference to prior version: (Part 1.1) New Requirement

Change Rationale: (Part 1.1)

The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.

Reference to prior version: (Part 1.2) CIP-007-3, R9; CIP-003-3, R6

Change Rationale: (Part 1.2)

The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3, Requirement R6.

Reference to prior version: (Part 1.3) CIP-007-3, R9; CIP-005-3, R5

Change Rationale: (Part 1.3)

Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.

Reference to prior version: (Part 1.4) CIP-007-3, R1

Change Rationale: (Part 1.4)

The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.

Reference to prior version: (Part 1.5) CIP-007-3, R1

Change Rationale: (Part 1.5)

This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.

This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.

Rationale for R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Reference to prior version: (Part 2.1) New Requirement

Change Rationale: (Part 2.1)

The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.

This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397.

Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.

Rationale for R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Reference to prior version: (Part 3.1) CIP-005-4, R4; CIP-007-4, R8

Change Rationale: (Part 3.1)

As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.

Reference to prior version: (Part 3.2) New Requirement

Change Rationale: (Part 3.2)

FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.

As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.

Reference to prior version: (Part 3.3) New Requirement

Change Rationale: (Part 3.3)
FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.

Reference to prior version: (Part 3.4) CIP-005-3, R4.5; CIP-007-3, R8.4

Change Rationale: (Part 3.4)
Added a requirement for an entity planned date of completion as per the directive in FERC Order No. 706, Paragraph 643.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-1

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-011-1:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-011-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.

2. In those jurisdictions where no regulatory approval is required, CIP-011-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-011-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented

processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management

Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)**– Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-1 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A		The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not identify, assess, or correct the	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information but did not identify,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					assess, or correct the deficiencies. (1.2)	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the

analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Summary of Changes: CIP 003-4 R4, R4.2, and R 4.3 have been moved to CIP 011 R1. CIP-003-4, Requirement R4.1 was moved to the definition of BES Cyber System Information.

Reference to prior version: (Part 1.1) CIP-003-3, R4; CIP-003-3, R4.2

Change Rationale: (Part 1.1)

The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection (e.g., confidential, public, internal use only, etc.) This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.

Reference to prior version: (Part 1.2) CIP-003-3, R4

Change Rationale: (Part 1.2)

The SDT changed the language from "protect" information to "Procedures for protecting and securely handling" to clarify the protection that is required.

Rationale for R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

Reference to prior version: (Part 2.1) CIP-007-3, R7.2

Change Rationale: (Part 2.1)

Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.

Reference to prior version: (Part 2.2) CIP-007-3, R7.1

Change Rationale: (Part 2.2)

Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.

The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.

Exhibit A

2.) Associated Modifications to the Glossary of Terms used in NERC Reliability Standards

Definitions of Terms Used in Version 5 CIP Cyber Security Standards

This section includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards and proposes terms for retirement. Terms already defined in the Glossary of Terms used in NERC Reliability Standards are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary. New defined terms are underscored. For existing glossary terms, new language is shown as underscored, while deleted language is shown as stricken. The list of terms proposed for retirement is at the end of the document.

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

BES Cyber System

One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

BES Cyber System Information

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

CIP Exceptional Circumstance

A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.

Control Center

One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

Cyber Assets

Programmable electronic devices, ~~and communication networks~~ including the hardware, software, and data in those devices.

Cyber Security Incident

~~Any~~ A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter ~~of a Critical Cyber Asset~~, or~~,~~
- Disrupts, or was an attempt to disrupt, the operation of a ~~Critical Cyber Asset~~ BES Cyber System.

Dial-up Connectivity

A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.

Electronic Access Control or Monitoring Systems ("EACMS")

Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Devices.

Electronic Access Point ("EAP")

A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Electronic Security Perimeter ("ESP")

The logical border surrounding a network to which ~~Critical Cyber Assets~~ BES Cyber Systems are connected using a routable protocol ~~and for which access is controlled~~.

External Routable Connectivity

The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.

Interactive Remote Access

User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Intermediate System

A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.

Physical Access Control Systems ("PACS")

Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Physical Security Perimeter ("PSP")

~~The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.~~

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Protected Cyber Assets ("PCA")

One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Reportable Cyber Security Incident

A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.

Terms to be retired from the *Glossary of Terms used in NERC Reliability Standards* once the standards that use those terms are replaced:

Critical Assets

Critical Cyber Assets

Exhibit B

Implementation Plan for Proposed CIP Version 5 Reliability Standards
submitted for Approval

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 5 CIP Cyber Security Standards

October 26, 2012

Prerequisite Approvals

All Version 5 CIP Cyber Security Standards and the proposed additions, modifications, and retirements of terms to the *Glossary of Terms* used in *NERC Reliability Standards* must be approved before these standards can become effective.

Applicable Standards

The following standards and definitions, collectively referred to as "Version 5 CIP Cyber Security Standards,"[1] are covered by this Implementation Plan:

CIP–002–5 — Cyber Security — BES Cyber System Categorization
CIP–003–5 — Cyber Security — Security Management Controls
CIP–004–5 — Cyber Security — Personnel and Training
CIP–005–5 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–5 — Cyber Security — Physical Security of BES Cyber Systems
CIP–007–5 — Cyber Security — Systems Security Management
CIP–008–5 — Cyber Security — Incident Reporting and Response Planning
CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems
CIP–010–1 — Cyber Security — Configuration Change Management and Vulnerability Assessments
CIP–011–1 — Cyber Security — Information Protection

"Definitions of Terms used in Version 5 CIP Cyber Security Standards" document, which includes proposed additions, modifications, and retirements of terms to the *Glossary of Terms used in NERC Reliability Standards*.

These standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

When these standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards become effective, all prior versions of these standards are retired.

[1] Although CIP-010-1 and CIP-011-1 are proposed as first versions, any reference to "Version 5 CIP Cyber Security Standards" includes CIP-010-1 and CIP-011-1, in addition to CIP-002-5 through CIP-009-5, because CIP-010-1 and CIP-011-1 were developed as part of the "Version 5 CIP Cyber Security Standards" development process.

Compliance with Standards

Once these standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards become effective, the responsible entities identified in the Applicability Section of the standard must comply with the requirements.

Proposed Effective Date for Version 5 CIP Cyber Security Standards

Responsible entities shall comply with all requirements in CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 as follows:

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[2]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5 R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Initial Performance of Certain Periodic Requirements

Specific Version 5 CIP Cyber Security Standards have periodic requirements that contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and responsible entities shall comply initially with those periodic requirements as follows:

1. On or before the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-002-5, Requirement R2
   - CIP-003-5, Requirement R1
2. On or before the Effective Date of CIP-003-5, Requirement R2 for the following requirement:
   - CIP-003-5, Requirement R2

[2] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

3. Within 14 calendar days after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-007-5, Requirement R4, Part 4.4
4. Within 35 calendar days after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-010-1, Requirement R2, Part 2.1
5. Within three calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5, Requirement R4, Part 4.2
6. Within 12 calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5, Requirement R2, Part 2.3
   - CIP-004-5, Requirement R4, Parts 4.3 and 4.4
   - CIP-006-5, Requirement R3, Part 3.1
   - CIP-008-5, Requirement R2, Part 2.1
   - CIP-009-5, Requirement R2, Parts 2.1, 2.2
   - CIP-010-1, Requirement R3, Parts 3.1
7. Within 24 calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-009-5, Requirement R2, Part 2.3
   - CIP-010-1, Requirement R3, Part 3.2
8. Within 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment for the following requirement:
   - CIP-004-5, Requirement R3, Part 3.5.

Previous Identity Verification

A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be reperformed under CIP-004-5, Requirement R3, Part 3.1.

Planned or Unplanned Changes Resulting in a Higher Categorization

Planned changes refer to any changes of the electric system or BES Cyber System as identified through the annual assessment under CIP-002-5, Requirement R2, which were planned and implemented by the responsible entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the Version 5 CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System, as identified through the annual assessment under CIP-002-5, Requirement R2, which were not planned by the responsible entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-5, Attachment 1, criteria.

For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies first medium impact or high impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 months

Applicability Reference Tables

The following tables are provided as a convenient reference to show which requirements in the Version 5 CIP Cyber Security Standards apply to specific Cyber Assets.

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-004-5 R2	Cyber Security Training Program	X	X	
CIP-004-5 R3	Personnel Risk Assessment Program	X	X	
CIP-004-5 R4	Access Management Program	X	X	
CIP-004-5 R5	Access Revocation	X	X	
CIP-005-5 R1 Part 1.2	Electronic Security Perimeter			X
CIP-005-5 R2	Remote Access Management			X
CIP-006-5 R1	Physical Security Plan	X	X	X
CIP-006-5 R2	Visitor Control Program	X		X
CIP-006-5 R3	Maintenance and Testing Program		X	

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-007-5 R1	Ports and Services	X	X	X
CIP-007-5 R2	Security Patch Management	X	X	X
CIP-007-5 R3	Malicious Code Prevention	X	X	X
CIP-007-5 R4	Security Event Monitoring	X	X	X
CIP-007-5 R5	System Access Control	X	X	X
CIP-010-1 R1	Configuration Change Management	X	X	X
CIP-010-1 R2	Configuration Monitoring	X	X	X
CIP-010-1 R3	Vulnerability Assessments	X	X	X
CIP-011-1 R1	Information Protection	X	X	
CIP-011-1 R2	BES Cyber Asset Reuse and Disposal	X	X	X

Exhibit C

Standard Drafting Team Roster for Project 2008-06 - Cyber Security Order 706 Version 5 CIP Standards

Project 2008-06 Standard Drafting Team Roster

Name and Title	Company and Address	Contact Info	Bio
Rob Antonishen, P. Eng. Section Manager, Controls and Metering Engineering and Technical Services	Ontario Power Generation 14000 Niagara Pkwy. Niagara-on-the-Lake, Ontario, Canada L0S 1J0	(905)262-2674 rob.antonishen@opg.com	After obtaining his BSc. in Electrical Engineering from Queens University in Kingston, Ontario, Canada, Rob began his 22 year career with Ontario Power Generation (then Ontario Hydro). Starting as field P&C Engineer, he has performed relaying, controls, governor, exciter and telecom maintenance, and led projects to replace hardwired relay controls with PLCs at hydro stations. He lead the teams designing, commissioning and administering OPG's corporate data acquisition and historian system, ICCP interfaces, and electronic dispatch systems. After a 5-year diversion though corporate IT and networking he is currently in Hydro-Thermal Operations as the corporate technical lead for CIP compliance, process control and cyber-security. Rob is also an active member of the NPCC Task Force on Infrastructure Security & Technology.
René Bourassa Engineer, Business Orientations, Systems & Security – Contrôle des mouvements d'énergie	Hydro-Québec TransÉnergie 6100 Des Forges, Trois-Rivières QC Canada G8Y 6K5	(819) 694-2507 bourassa.rene@hydro.qc.ca	René Bourassa is an engineer at Hydro-Québec and acts as a SCADA and Operational Technologies Cyber Security Expert. Mr. Bourassa began his 35 year career, of which more than 80% was spent in a Control Center environment, at Hydro-Québec on Gentilly nuclear power plants and Shawinigan 2 (the oldest hydraulic generation station still in operation in North America) operational activities while he was completing his Computer Science and Electrical Engineering Bachelor of Science degree. For 8 years, he taught "Programming for Engineers" and "Scientific Application Programming" at Université du Québec à Trois-Rivières. Besides his generation, transmission, and electric grid operation experience as an

Project 2008-06 Standard Drafting Team Roster

			electrical engineer, he also cumulated knowledge and experience in programming, system development, database, computer networks, computer and acquisition protocols, firewall, and other cyber security topics. Mr. Bourassa participated in commissioning one of Hydro-Québec's first Regional Telecontrol Center. As Telecontrol Main Architect and Cyber Security Coordinator, he was a major contributor to the evolution over the years of Hydro-Québec's telecontrol SCADA architecture, and he conceived and implemented the High Security Telecontrol Architecture. Since the late 1980s, he has promoted cyber security for SCADA systems and operational technology at Hydro-Québec and through presentations at RSA Conferences, SANS Process Control and SCADA Security Summits, EPRI GRPM/EIS PLC meetings, and participation in the DHS 2005 Roadmap to Secure Control Systems in the Energy Sector.
Jay Cribb Principal Information Security Analyst	Southern Company Services, Inc. 241 Ralph McGill Blvd NE Atlanta, GA 30308	(404)506-3854 jscribb@southernco.com	Jay Cribb has 27 years of experience in Information Technology within the electric utility industry. Jay is currently a Principal Information Security Analyst with Southern Company Services, Inc. where his responsibilities include working with Generation, Transmission, and numerous other business units in protecting critical infrastructure from cyber-based threats. He has been involved with the NERC CIP standards in some way since they were known as the '1200' standards. Jay has served in the past as the first cyber security representative for the SERC Region to the NERC CIPC. He has recently completed 2 years as vice-chair and 2 years as Chair of the EEI Security Committee. Jay was also the first chair of SERC's CIP Compliance working group and remains a member of the SERC CIPC.

Project 2008-06 Standard Drafting Team Roster

Sharon Edwards	Duke Energy		Sharon Edwards has worked for Duke Energy since 1989. She has served in a variety of roles and has been involved with implementing cyber security standards at Duke since the inception of Urgent Action 1200 for Cyber Security. At Duke Energy, Sharon is the Legacy Duke Program Lead for Critical Infrastructure Protection (CIP). She previously worked implementing cyber security and the associated regulations in the Telecom area at Duke. Sharon has been a member of the FERC Order 706 Standards Drafting Team since the beginning of the drafting team. She is also a member of the Critical Infrastructure Protection Committee. Ms. Edwards is a Certified Information Systems Security Professional (CISSP). She holds a bachelors degree from Xavier University in Cincinnati, Ohio, and a Master of Business Administration degree (MBA) from Thomas More College in northern Kentucky.
Gerald Freese Director, NERC CIP Compliance, Regulatory Services	American Electric Power 1 Riverside Plaza, Columbus, OH 43215	614-716-2351 gsfreese@aep.com	Gerald Freese is the Director of NERC CIP compliance and former Director of IT Security Engineering at American Electric Power. In his security role he was responsible for defining, developing and executing all information security programs to effectively protect AEP data and systems, including critical digital control systems. In his current capacity he is responsible for regulatory compliance, NERC CIP standards compliance and is actively engaged in development of cyber security standards for the energy industry. Gerald Freese is a recognized information security and critical infrastructure protection expert who brings a powerful combination of leadership, domain experience, technological vision and strategy development to American Electric Power. He is one of the company's primary compliance program architects, and a strong proponent of

Project 2008-06 Standard Drafting Team Roster

			industry and government partnerships for critical infrastructure protection. Prior to accepting a position at American Electric Power, Mr. Freese was the Director of Security Intelligence at Vigilinx, Inc., where he developed an early warning and data analysis process to identify computer-based threats and attack profiles. He has authored in depth analytical papers on cyber-activities relative to geopolitical and critical infrastructure threat environments, has testified before congress on critical infrastructure interdependencies and control system security and was the recipient of the 2009 'Security Seven' award for the electricity sector. Mr. Freese is a retired naval Cryptologic Officer with extensive experience in computer security and information warfare. He has held other leadership positions in the information technology industry with Perot Systems and General Dynamics Advanced Information Systems. Mr Freese is a Certified Information Systems Security Professional (CISSP). He holds a bachelors degree from State University of New York (Albany), and a Masters degree in Information and Telecommunications Systems from Johns Hopkins University in Baltimore, Maryland. He is a member of the NERC Critical Infrastructure Protection Committee, the FERC Order 706 Standards Drafting Team and is the Vice Chair of the recently formed Electricity Sector, Information Sharing Task Force. (ES-ISTF) He also participated on the Infrastructure Working Group with the Center for Strategic and International Studies (CSIS) Commission on Cyber security for the 44th Presidency.
Christine Hasha, Senior Compliance Analyst	Electric Reliability Council of Texas, Inc. 2705 W. Lake Dr. Taylor TX 76574	(512) 248-3909 chasha@ercot.com	Christine is a current member of Project 2008-06 Standards Drafting Team and has participated in other SDT project sub-teams. She is actively involved with the ERCOT CIP Working Group and participates on CIP

Project 2008-06 Standard Drafting Team Roster

			related issues for the ISO/RTO Council Standards Review Committee. Christine brings 20 years' experience in Information Technology with a 17 year emphasis on Information Security and regulatory compliance. She has provided standards training to ERCOT and other NERC region committees and has had guest speaker engagements for industry vendors. She has extensive experience in development of security policies, standards, and supporting procedures. Christine has been responsible for coordination of CIP implementation, audit readiness, and training of SMEs at ERCOT as well as representing ERCOT in CMEP related activities. She brings experience and training in common control frameworks including previous experience in implementing security controls for banking, Sarbanes-Oxley, GLBA, and HIPAA consistent with IS027001/27002.
Philip Huff Director of IT Security and Compliance	Arkansas Electric Cooperative Corporation 1 Cooperative Way Little Rock, AR 72119	501-570-2444 philip.huff@aecc.com	Philip Huff has ten year's experience in the electric industry programming and securing control systems. He has degrees in Mathematics and Computer Science from Harding University and a Masters in Computer Security from James Madison University. He is a CISSP and holds the Department of Defense certifications, CNSSI 4011, 4012 and 4014 for securing national defense systems.
Douglas D. Johnson, Principal Engineer	Exelon 1N301 Swift Road, Lombard, IL 60148	630-691-4593 douglas.johnson@comed.com	Douglas Johnson received a bachelor degree in Electrical Engineering and has worked at Commonwealth Edison - Exelon for over 29 years. He began his career in construction start-up testing and maintenance of nuclear generating plant electrical systems which included work on protective relays, main generators, large power transformers and high voltage switchyard equipment. Doug is currently part of the ComEd Transmission Operations Support organization with responsibilities overseeing the ComEd transmission dispatcher related SCADA, physical security and other communication systems. Doug has also been involved in Exelon's CIP compliance efforts since NERC

Project 2008-06 Standard Drafting Team Roster

			Urgent Action 1200 and has remained heavily involved throughout the implementation of the NERC CIP Cyber Security Standards.
Richard Kinas Manager of Standards Compliance	Orlando Utilities Commission 6113 Pershing Avenue Orlando, FL 32822	(407) 434-4261 rkinas@ouc.com	Richard Kinas is the Manager of Standards Compliance for Orlando Utilities Commission (OUC), a vertically integrated municipal utility within the FRCC region. Mr. Kinas has an undergraduate degree in Electrical Engineering and a Masters degree in Business Administration. He is a registered CISSP, and has been a NERC certified System Operator (Reliability Coordinator). Mr. Kinas has over 25 years of experience as a network and computer security expert, five of which were as a Senior Unix Administrator, five as a Senior Network Engineer, and five as a Network Security specialist. His current responsibilities include ensuring compliance with all O&P and CIP requirements for OUC. Mr. Kinas currently serves on the NERC Operating Committee, is a member of the FERC Order 706 Cyber Security standard drafting team, is the chair of the FRCC Compliance Committee, and is the vice chair of the FRCC Critical Infrastructure Protection subcommittee.
John Lim			John Lim is currently retired, since July 2012, from Consolidated Edison Co. of New York, Inc., an Electric, Gas and Steam Utility serving the New York City and Westchester County in New York. In his career at Consolidated Edison, John's most current position was Department Manager for IT Infrastructure Planning where he had overall responsibility for the enterprise cyber security program. He is an IT practitioner for more than 29 years, with more than 17 years in network and systems security in the electric utility industry. John has served as a member of the NERC Critical Infrastructure Protection Committee, as the primary cyber security representative for the Northeast Power Coordinating Council and has been active in many NERC cyber security task forces and working groups. A

Project 2008-06 Standard Drafting Team Roster

			member of the original NERC Cyber Security Standards Drafting Team, John is the current chair of the NERC Cyber Security Standards Drafting Team for Order 706. John also served as a member of the core drafting team for the DoE Risk Management Process Guideline and has served as a co-Vice-Chair of the SmartGrid Cyber Security Working Group of the SmartGrid Interoperability Panel (SGIP). He has also served as an IEEE technical paper reviewer for cyber security related to the Power sector and contributed to the EEI Reliability Newsletter. He is a frequent public speaker on cyber security for the electric sector. John holds an MS in Computer Systems from Baruch College, CUNY and is a Certified Information Systems Security Professional (CISSP) since 2001.
Robert Preston Lloyd Senior Technical Specialist	Southern California Edison 3 Innovation Village, 2nd Floor Pomona, CA 91768	909-274-1338 robert.lloyd@sce.com	Robert Preston Lloyd is a Senior Technical Specialist at Southern California Edison (SCE). He has over eight years of diverse experience in the electric utility industry involving circuit breakers, transformers, protective relays, automation systems, equipment reliability and risk assessment, asset management, General Rate Cases, compliance audits, process development, and standards development and implementation. Additionally, Robert has been involved in cyber security with SCE's NERC CIP Compliance Team for several years and has spent over two years with the NERC CIP Cyber Security Order 706 Standard Drafting Team. Robert is currently responsible for Substation Compliance & Asset Management. His involvement in compliance and regulatory issues includes NERC Protective Relays and Controls (PRC), NERC Critical Infrastructure Protection (CIP), Western Electricity Coordinating Council (WECC) Transmission Maintenance standards, California Independent System Operator (CAISO)

Project 2008-06 Standard Drafting Team Roster

			Compliance, State and Federal SF_6 Regulations, and various other regulatory bodies. Robert received both his Bachelor of Science in Electrical Engineering and his Master of Science in Engineering Management from the University of Southern California. He is also a licensed Professional Engineer in Electrical Engineering - Power.
Scott Mix CIP Technical Manager	North American Electric Reliability Corporation 1325 G Street NW, Suite 600 Washington, DC 20005	215-853-8204 scott.mix@nerc.net	Mr. Scott R. Mix, CISSP, joined NERC in October 2006 following more than 25 years of experience working in various facets of the electricity industry, including as a consultant with KEMA, Inc., Infrastructure Security Manager with the Electric Power Research Institute (EPRI), Senior Security Analyst at the PJM Interconnection, and more than ten years with Leeds & Northrup Co. as a programmer/analyst and systems architect. For more than ten years, he has focused on the areas of Computer and Infrastructure Security for the Electricity Sector. At NERC, he is responsible for Critical Infrastructure Protection issues, primarily as they relate to Real Time and Control System Security, and the development of the revisions to the NERC CIP Standards. He has also been the NERC Staff Facilitator for the Critical Infrastructure Protection Committee (CIPC) and several of its working groups and task forces, and a member of the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) Staff. Throughout his career, Mr. Mix has worked closely with numerous industry and government organizations, including NERC's Critical Infrastructure Protection Committee (CIPC) and its working teams, and is the former convener of the Control System Security Working Group, has been an active and vocal observer to the NERC Cyber Security Standards Version 1 Drafting Team (and the NERC 1200 process before that), and

			is a former member of the OASIS "How" Working Group. He has also worked with the Department of Energy, the Department of Homeland Security, the FBI's National Infrastructure Protection Center, and the Federal Energy Regulatory Commission dealing with specific Electric Sector Security Issues. He has organized and presented at numerous industry symposia, both domestically and internationally. He has been a member and chapter secretary of the Philadelphia Chapter of InfraGard, is a member of the ISA and has participated in the ISA100 standards activities, and is a member of the IEEE as well as its Computer Society, Power Engineering Society, and Standards Association. He is a Certified Information Systems Security Professional (CISSP). Mr. Mix is a graduate of the Bloomsburg University of Pennsylvania with a Bachelor of Science degree in Computer & Information Science and Chemistry.
David S. Revill Manager, Cyber Security Operations	Georgia Transmission Corporation 2100 East Exchange Place Tucker, GA 30084	770-270-7815 david.revill@gatrans.com	David Revill is the Manager of Cyber Security Operations for Georgia Transmission Corporation with responsibility for the cyber and physical security of GTC's field assets, including compliance with the NERC CIP Standards. He previously was the Group Lead for the Electronic Maintenance lab at GTC, which was responsible for the SCADA, Revenue Metering, and Communications at GTC's field assets. Prior to joining GTC, Mr. Revill held positions supporting SCADA/EMS systems for control centers as a SCADA Systems Support Engineer and a Process Controls Network Engineer with Entergy. Mr. Revill is a member of the leadership team for the North American Transmission Forum Security Practices Group, the NERC Critical Infrastructure Protection Committee (CIPC) representing NRECA, the SERC CIPC, and

Project 2008-06 Standard Drafting Team Roster

			has been a member of the NERC CIP Standards Drafting Team beginning with version 2 of the CIP Standards. Mr. Revill holds a Master's degree in Electrical and Computer Engineering from Georgia Tech and dual bachelor's degrees in Electrical Engineering and Computer Engineering from the Tulane University.
Kevin Sherlin, IT Director	Sacramento Municipal Utility District 6201 S Street Sacramento, CA 95817-1899	(916) 732-6452 Kevin.Sherlin@smud.org	Kevin Sherlin is the Director of Information Technology at the Sacramento Municipal Utility District (SMUD), a position he has held since April, 2010. In his position as IT Director, he is responsible for all facets of information technology, including information security, leading a team of 165 skilled individuals. His previous position at SMUD was the Manager of IT Operations where he led a workforce providing IT infrastructure (PC's, servers, network, telephones, etc.). Kevin has been with the SMUD for seven years and also served as a Supervisor of Telecommunications Engineering. Prior to joining SMUD, Kevin worked at El Paso Electric Company for 24 years. He held various positions including Substation Engineer, Communications Engineer, Manager of Relay/Communications and IT Director. Kevin is a graduate of the University of Texas at El Paso with bachelor's degrees in math and electrical engineering.
Thomas W. Stevenson, Business Manager, Electric Power Industry, NERC CIP Compliance	TAI Engineering 11155 Dolfield Boulevard, Suite 210, Owings Mills, MD 21117	(410)-227-3728 or (410)-356-3108x430 thomas.stevenson@taiengineering.com	Mr. Stevenson has over forty years experience as an Electrical & Controls system engineer and project manager in the power industry. A graduate of Virginia Tech with a BS Electrical Engineering degree and George Washington University with a MS Business Administration degree, he recently retired as General Supervisor for Electrical & Control Systems Engineering in the Technical Services division of Constellation Energy. He has worked on the E&C systems design for new and existing power plants in 9 US states, Canada and Guatemala. He served as Baltimore Section President and as a

Project 2008-06 Standard Drafting Team Roster

			Certification Board member for ISA (the International Automation Society). In the ISA Power Division he has regularly served as Session Developer, Executive Committee member, Professional Development chair, and as a member of the ISA77 power plant standards committee. He is a senior member of ISA and an IEEE member since 1971. Tom has served for the last two years as a member of the NERC CIP Standard Drafting Team.
John D. Varnell Director, Market Design and Standards	Tenaska Power Services Co. 1701 E. Lamar Blvd. Arlington, TX 76006	(817)462-1037 jvarnell@tnsk.com	John Varnell has more than 30 years of experience in IT protection and control, communications systems and network security for power plants and substations. His current work for Tenaska Power Services Co., Tenaska's power marketing affiliate, includes market design and standard aspect that affect costumers in ERCOT, MISO, PJM, SERC, WECC and SPP. Mr. Varnell has served on drafting teams for NERC Project 2008-06, Cyber Security Order 706, SAR 1300 and SDT 1300, which became CIP-002 through CIP-009, Version 1, and the NERC Functional Model Advisory Team for Demand Response. He has experience with several SCADA systems, including Ferranti International Controls' Vanguard system with RealMax add-on, ESCA's Habitat System, Siemens' Spectrum System, the ABB Ranger System, OSI International Monarch System and OSIsoft PI System. He also has experience with microwave communications systems for Harris Farinon digital radios (2 and 6 GB) and Rockwell Collins analog radios (6 GB); RTU equipment, relays and interfaces from GETAC, Ferranti, Telvent, Novatech, GE, Larscom, RFL and Schweitzer Engineering Laboratory; and special systems designed in-house for gas flow computers and their interfaces and one-off embedded devices.
William Winters IT Security Architect	Arizona Public Service 400 N 5th St Phoenix, AZ 85004	602-250-4472 william.winters@aps.com	William Winters is presently an IT Security Architect with Arizona Public Service Company (APS). He has worked in the IT industry for over 30 years and has previously held positions as an IT system operator,

Project 2008-06 Standard Drafting Team Roster

			systems programmer, systems engineer and IT manager. Over the past 27 years at APS, he has been responsible for EMS/SCADA, Distribution Outage Management Systems, and other grid operations critical applications, both as an implementer and as manager. He was responsible for implementing one of the first hot multi-site distributed SCADA installations in the industry and was the CIP Program Manager for the initial implementation of the CIP Compliance Program at APS. Currently William provides enterprise security architecture direction with a focus on advancing and integrating cyber security practices across the operations and business environments.

Exhibit D

Consideration of Comments Reports

Project 2008-06
Cyber Security Order 706 Version 5 CIP Standards

Related Files

Activity: Version 5 CIP Standards (Phase III)

Status:
The Version 5 CIP Standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1, the associated implementation plan, and the associated definitions) were approved by the NERC Board of Trustees on November 26, 2012, and they are being prepared for filing with applicable regulatory authorities.

Draft	Action	Dates	Results	Consideration of Comments
Draft 4 CIP-002-5 Clean | Redline to Last Posted CIP-003-5 Clean | Redline to Last Posted CIP-004-5 Clean | Redline to Last Posted CIP-005-5 Clean | Redline to Last Posted CIP-006-5 Clean | Redline to Last Posted CIP-007-5	Recirculation Ballots and Non-binding Poll Info>> Vote>>	10/26/12 - 11/05/12 (Closed) Non-binding Poll Extended until 11/13/12 (closed)	Summary>> Ballot Results: CIP-002-5 CIP-003-5 CIP-004-5 CIP-005-5 CIP-006-5 CIP-007-5 CIP-008-5 CIP-009-5 CIP-010-1 CIP-011-1 Implementation Plan Definitions ------- Summary>> Non-Binding Poll	

Clean | Redline to Last Posted CIP-008-5 Clean | Redline to Last Posted CIP-009-5 Clean | Redline to Last Posted CIP-010-1 Clean | Redline to Last Posted CIP-011-1 Clean | Redline to Last Posted Implementation Plan Clean | Redline to Last Posted Definitions Clean | Redline to Last Posted **Supporting Materials:** VRF and VSL Comment Form (Word) VRFs/VSLs for all Standards Clean | Redline to Last Posted Mapping Document Clean			Results	
	VRF and VSL Comment Form Info>> Submit Comments>>	10/26/12 - 11/05/12 (Closed)		

CIP-002-4 CIP-003-4 CIP-004-4 CIP-005-4a CIP-006-4c CIP-007-4 CIP-008-4 CIP-009-4 Draft Consideration of Issues and Directives Clean Consideration of Comments				
Draft 3 - Version 5 CIP Standards CIP-002-5 Clean | Redline to Last Posted (CIP-002-5: REVISED 092112) CIP-003-5 Clean | Redline to Last Posted (CIP-003-5: REVISED 09/14/12) CIP-004-5 Clean | Redline to Last Posted CIP-005-5	Successive Ballot Info>> Vote>>	10/01/12 - 10/10/12 (closed)	Summary>> Ballot Results: CIP-002-5 CIP-003-5 CIP-004-5 CIP-005-5 CIP-006-5 CIP-007-5 CIP-008-5 CIP-009-5 CIP-010-1 CIP-011-1 Implementation Plan Definitions	
	CIP-006-5 RSAW Industry	09/11/12 - 10/10/12 (closed)		

Clean | Redline to Last Posted CIP-006-5 Clean | Redline to Last Posted CIP-007-5 Clean | Redline to Last Posted	Comment Period RSAW Feedback Form>> Please send RSAW Feedback Forms to: RSAWFeedback@nerc.net			
CIP-008-5 Clean | Redline to Last Posted CIP-009-5 Clean | Redline to Last Posted CIP-010-1 Clean | Redline to Last Posted CIP-011-1 Clean | Redline to Last Posted Implementation Plan Clean | Redline to Last Posted (Implementation Plan: REVISED 09/17/12) Definitions Clean | Redline to Last Posted (Definitions: REVISED 09/21/12)	Standard Comment Period Info>> Submit Comments>>	09/11/12 - 10/10/12 (closed)	Comments Received>>	Consideration of Comments **(5)**

Supporting Materials: Unofficial Comment Form (Word) VRFs/VSLs for all Standards Clean | Redline to Last Posted Mapping Document Clean | Redline CIP-002-4 CIP-003-4 CIP-004-4 CIP-005-4a CIP-006-4c CIP-007-4 CIP-008-4 CIP-009-4 **Consideration of Comments** Consideration of Comments A CIP-002 and CIP-003 Includes Summary Consideration, Explanation, and Common Responses to Global Changes Consideration of Comments B CIP-004 through CIP-007 Consideration of				

Comments C CIP-008 through CIP-011 Consideration of Comments D Definitions and Implementation Plans Draft Consideration of Issues and Directives Clean | Redline				
Draft 2 - Version 5 CIP Standards CIP-002-5 Clean | Redline CIP-003-5 Clean | Redline CIP-004-5 Clean | Redline CIP-005-5 Clean | Redline CIP-006-5 Clean | Redline CIP-007-5 Clean | Redline	Successive Ballot Updated Info>> Info>> Request for Additional Clarity Form>> Posted Requests for Additional Clarity>> Vote>>	05/11/12 - 05/21/12 (closed)	Summary>>(updated) Ballot Results: (Updated) CIP-002-5 CIP-003-5 CIP-004-5 CIP-005-5 CIP-006-5 CIP-007-5 CIP-008-5 CIP-009-5 CIP-010-1 CIP-011-1 Implementation Plan Definitions	
CIP-008-5 Clean | Redline	Formal Comment Period	04/12/12 - 05/21/12	Comments Received:	**Consideration of Comments** Consideration of

CIP-009-5 Clean | Redline CIP-010-1 Clean | Redline CIP-011-1 (CIP-011-1: REVISED - 05/09/12) Clean | Redline Implementation Plan Clean | Redline Definitions Clean | Redline Clean and redline definitions documents updated on April 12, 2012 to reflect correct dates in the footer sections. **Supporting Materials** Unofficial Comment Form A - CIP-002 and CIP-003 Unofficial Comment Form B - CIP-004 through CIP-007 Unofficial Comment Form C - CIP-008 through CIP-011	Advanced Info>> **Submit Comments:** Comment Form A>> Comment Form B>> Comment Form C>> Comment Form D>>	(Closed)	Comment Form A Comment Form B Comment Form C Comment Form D	Comments A **(1)** CIP-002 and CIP-003 Includes Summary Consideration, Explanation, and Common Responses to Global Changes Consideration of Comments B **(2)** CIP-004 through CIP-007 Consideration of Comments C **(3)** CIP-008 through CIP-011 Consideration of Comments D **(4)** Definitions and Implementation Plans

Unofficial Comment Form D - Definitions and Implementation Plans Mapping Document Clean | Redline CIP-002-4 CIP-003-4 CIP-004-4 CIP-005-4a CIP-006-4c CIP-007-4 CIP-008-4 CIP-009-4 Consideration of Comments Draft Consideration of Issues and Directives Clean | Redline				
CIP Standards Version 5 Webinar Slides	04/10/12			
Draft 1 - Version 5 CIP Standards CIP-002-5 CIP-003-5 (CIP-003-5: REVISED -	Initial Ballot Info>> Vote>>	12/16/11 - 01/06/12 (Closed)	Summary>> Full Record Ballot Results: CIP-002-5	
	Formal Comment	11/07/11		

11/22/11) CIP-004-5 CIP-005-5 CIP-006-5 CIP-007-5 CIP-008-5 CIP-009-5 CIP-010-1 CIP-011-1 Implementation Plan Definitions **Supporting Materials** Unofficial Comment Form (Word) Mapping Document CIP-002-4 CIP-003-4 CIP-004-4 CIP-005-4a CIP-006-4c CIP-007-4 CIP-008-4 CIP-009-4 Consideration of Comments from June 2010 Informal Comment Period Draft Consideration of Issues and Directives	Period Info>> Submit Comments>>	- 01/06/12 (Closed)	CIP-003-5 CIP-004-5 CIP-005-5 CIP-006-5 CIP-007-5 CIP-008-5 CIP-009-5 CIP-010-1 CIP-011-1 CIP V5 Implementation Plan CIP V5 Definition Comments Received>> Additional Link for Comments Received_CSWG>>	
	Join Ballot Pool Info>> Join>>	11/07/11 - 12/15/11 (Closed)		

CIP Standards Version 5 Webinar Slides		08/24/2011		
CIP Standards Version 5 Presentations - August 2011 SDT Meeting		08/17/11		
CIP Standards Development Overview for FERC Technical Staff Meeting		07/28/11		

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards
Comment Form A
CIP-002 and CIP-003 Questions

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Summary Consideration, Explanation, and Common Responses to Global Changes and to Issues and Comments Frequently Repeated

In response to draft 2 of the Version 5 CIP Cyber Security Standards, the Standards Drafting Team (SDT) received significant input from a wide variety of perspectives. All of that input greatly helped the team to refine the standards and associated documents, and the set of standards now posted reflects all of that combined input. There were several varied perspectives in the comments, and the SDT attempted to address each comment as responsively as possible.

There were several changes that reflected careful consideration of several comments that affected the standards on a global basis, whether in format, style, or substance. In addition, there were several comments the SDT considered that were repeated across multiple questions, sometimes submitted by the same entity to each or to many of the questions. Rather than explaining in detail the global changes in response to each question, and rather than responding separately to the frequently repeated comments in each question, the SDT addresses those global issues and general comments in this section.

Many comments related to specific language suggestions or to specific compliance concerns. The SDT has responded to those comments in each of the individual questions summaries that follow this section. Those comments were thorough and varied, and they reflected diverse perspectives and topics. The SDT expended considerable work in reviewing, discussing, and responding to all of these inputs, and it believes that the major issues have been addressed responsively in this posted draft CIP Version 5 package. As a result, the changes have been significant and substantive in all of the draft CIP Version 5 standards and Implementation Plan. The SDT believes this posting package addresses all of the substantive issues received from the previous two iterations of comments and various other inputs.

Change in labeling of the applicability columns in the tables to "Applicable Systems"
After posting draft 1 of CIP Version 5, commenters expressed concern that merely using "Applicability" as the title of the applicability columns in the Requirement tables (in CIP-004 through CIP-011) created confusion with the actual "Applicability" section of the standards. In response, for draft 2, the SDT added specificity and labeled those columns "Applicable BES Cyber Systems and associated Cyber Assets." In response to that change in draft 2, commenters expressed concern with the length and suggested that the SDT label the applicability column "Applicability." Therefore, the SDT is proposing to label these columns, "Applicable Systems." This should eliminate any confusion with the applicability section of the standards themselves while also providing appropriate brevity.
Handling of "associated" Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCA) (and the associated change to their use in the "Applicable Systems" column of the requirement tables)
In previous drafts, in the applicability columns (now "applicable systems" columns), the standards used a term "Associated Protected Cyber Assets," "Associated Electronic Access Control or Monitoring

Systems," and "Associated Physical Access Control Systems" where it intended that the requirement part be applicable to not only the applicable high or medium impact BES Cyber Systems, but also to other Cyber Assets or systems, as specified, associated with those BES Cyber Systems. Also, for Protected Cyber Assets, the requirement applied to Cyber Assets or lower impact BES Cyber Systems that were in the same ESP as the applicable BES Cyber System. There was confusion the precise meaning or application of the "associated" systems, and the SDT has made the link more explicit in this draft. One of the fundamental concepts of CIP Version 5 is that it is adopting a systems approach, and those "associated" systems should be more closely connected with the applicable subject of the requirement. Therefore the SDT has moved the associated systems to follow immediately after the subject of the requirement and clarified that they are "associated with" that specify type of BES Cyber System or other applicable system. Mitigation for the associated systems may be accomplished through other applicable systems.

High Watermarking Concept

The CIP Version 5 Standards use a term "Protected Cyber Assets" to refer to those Cyber Assets that are within the ESP, which in previous versions of the standards were "other (non-critical) Cyber Assets within the ESP" (see CIP-005-4, Requirement R1, Part 1.4, and CIP-007-4). Additionally, in Version 5, a Protected Cyber Asset can also be a BES Cyber System of a lower impact classification if it is within the same ESP as a higher impact BES Cyber System.

For example, CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The standard does not require segmenting of BES Cyber Systems by impact classification, and many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and systems within the ESP will be elevated to the level of the highest impact BES Cyber System present in

the ESP. The standard accomplishes this by defining all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

Measures: "but not limited to"

Many commenters expressed concern about or questioned the meaning of the use of "but not limited to" in the previous draft and asked for it to be removed from the measures. The concern as the SDT understood it was that "but not limited to" could be used to request evidence beyond that which is specified in the measure even if the entity has otherwise provided what the measure describes. With respect to "but not limited to," the SDT specifically inserted that phrase to assist the Responsible Entity, particularly in light of technologies that may change. It is not intended to be used as a mechanism to request additional evidence beyond that which is required to demonstrate compliance. The SDT is concerned that removing "but not limited to" opens the same question (albeit in slightly different context) as the CIP Interpretation Drafting Team just answered with respect to the interpretation of CIP-002 (versions 1 through 4) for Duke Energy (NERC Standards Development Project 2010-INT-05). Namely, are the measures listed exhaustive/prescriptive or are they illustrative? By including a qualifier such as "but not limited to," as is common in statutory drafting and in other legal contexts, the SDT intends to signal that the measures are not exhaustive. It provides flexibility to the Responsible Entity on what is acceptable. For example and for purposes of illustration, if one said "evidence may include an orange, a lime, or a lemon," one could expect that perhaps only an orange, a lime, or a lemon would be appropriate. However, if one said, "evidence may include, but is not limited to, an orange, a lime, or a lemon," one could just as reliably expect that an orange, a lime, or a lemon would be appropriate, but it would also be reasonable that something not explicitly enumerated by the list, but similar in nature to items on the list, such as a tangerine, may also be acceptable. Importantly, that is not the same as additionally requiring a tangerine even though one already has an orange; however, that is the concern manifested in the comments. To address the commenters' concerns, however, the SDT has made a slight change in support of signaling in all measures that they are examples and that the list of examples is not exhaustive. The SDT believes that it is providing sufficient flexibility in this manner—and for the Responsible Entities' benefit—in clarifying that measures are not prescriptive lists while also attempting to allay fears that "but not limited to" will be used in a manner that expands the requirement. Rather than stating "Evidence may include, but is not limited to, . . ." the SDT has added the "example" concept to precede "evidence" (e.g., "**An example of** evidence may include, but is not limited to, . . ." or "**Examples of** evidence may include, but are not limited to, . . .").

Movement to focus on correcting deficiencies in certain requirements:
In response to several comments, the SDT has incorporated within CIP Version 5 a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. Note that, where used, the addition of language modifies "implement"; it does not itself require or specify internal controls, though it certainly enables their use for those entities that have adopted an internal controls or compliance management approach. Where used, the requirements incorporate the forward-looking language into the main requirement, which ties in with CIP Version 5's use of accompanying tables. It is presented in those requirements as follows:

> "Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** one or more documented processes (or program, etc., as specified by the requirement) that collectively include each of the applicable items in [the referenced table]."

The SDT also considered several alternatives and additions to this language. For example, some alternatives proposed modifying "process" (or program, etc.), while others suggested to add language specifying certain things that are not violations in addition to the requirement language. Many of the ideas or suggestions presented concepts that the team agrees with, but they are more appropriate for other aspects of monitoring compliance with the standards, not for inclusion within the standards themselves. Language indicating what is not a violation is more appropriate for compliance tools such as the RSAW. The SDT also notes that the VSLs will reflect this approach where the approach is used, and the SDT is actively working with NERC Compliance Operations to prepare the RSAWs for the CIP Version 5 standards. Furthermore, the SDT expects continued participation by industry in providing input into the RSAW development following approval of the standards, and the SDT notes that a draft RSAW for part of CIP-006-5 is posted for comment and for illustrative purposes.

The SDT is charged with writing straightforward requirements stating the desired behavior that will maximize reliability of the BES. The CIP requirements are written to require documented processes that must address the elements in the tables that accompany the requirements. These tables therefore set the parameters for the processes. There are no issues with documenting the processes – the entity must have the processes and they must have the parameters as outlined in the requirement tables.

The compliance concerns, especially those related to zero tolerance for deficiencies, is not related to the documenting of the processes, but in the implementation of the processes. The process should have numerous 'bright line' parameters that outline the goal the industry striving towards. A concern applies when implementing the processes in a world of tens of thousands of people and hundreds of

thousands of Cyber Assets. In certain cases, absolute perfection forever is not reasonable, even if it is desirable.

In light of the direction toward a risk-based approach to compliance monitoring by NERC, The CIP SDT had an opportunity to do to address this issue in certain requirements within the standards themselves. As described above, the SDT included a phrase to modify the verb 'implement' in several (but not all) of the requirements in CIP V5. Entities are to have the processes; the processes must meet the requirements in the tables; and the entities shall implement those processes in a manner that identifies, assesses, and corrects deficiencies.
The emphasis of the self-correcting language is on the implementation of the processes. The processes themselves cannot miss required parts or parameters as outlined in the tables.

Implementation Plan proposal to extend Version 3 until Version 5 remains unchanged in this draft
In light of the order approving the CIP Version 4 standards (FERC Order No. 761), several commenters asked about the drafting team's proposal in the implementation plan to extend Version 3 until the effective date of Version 5. The SDT's proposal, if approved—and its intent for Version 5 to supersede Version 4 and to extend the effectiveness of Version 3 until Version 5 goes into effect—remains unchanged.
In the implementation plan for the CIP Version 5 standards, the SDT has previously proposed to extend Version 3 until the effective date of Version 5. In doing so, the effective date proposes that Version 4 will be superseded by Version 5 and not go into effect. Even though Version 4 has been approved by order, the SDT always contemplated such approval during the development of the implementation plan language. That order does not change the SDT's proposal. The expectation that there would be an order in early to mid 2012 is why the SDT included language in the implementation plan's effective date to specify that the extension of Version 3 until Version 5, and that Version 4 would not go into effect, would occur "notwithstanding any order to the contrary." There is no change in the SDT's intent and proposal to extend Version 3 until Version 5, and for Version 5 to supersede Version 4, notwithstanding the recent order approving Version 4. The SDT also understands, as is the case for any standards proposal by the industry, that the proposal is subject to approval by regulatory authorities.

Stakeholders will notice that within the individual standards for CIP Version 5, the effective dates have been modified so that they are specific to the particular standard. In doing so, the reference to extending Version 3 and superseding Version 4 has been removed, as the Implementation Plan is the appropriate place for that language (where it remains, as described above). Thus, while there is no change to the SDT's proposal, the individual, standard-by-standard effective dates have been modified to comport with the style and form of other NERC Reliability Standards.

Annual v. 15 calendar months
Several commenters expressed dissatisfaction with the standards' use of the phrase ". . . at least once every calendar year, but not to exceed 15 calendar months . . ." for describing the required frequency

of performance on some requirements. Some entities expressed a desire to simply use "annual," while others suggested changing the "but" to an "or." The SDT has discussed alternative approaches and is using the term ". . . at least once every 15 months . . ." to provide reasonable flexibility to Responsible Entities while meeting the intent of the requirements. As explained in the global comment section of the response to comments for draft 2, simply using "once per calendar year" creates a potential for bi-annual bookending that the SDT does not intend. Similarly, the SDT understands that the use of both "calendar year" and "15 calendar months" was unnecessarily complicated. The SDT acknowledges that there is a CAN that addresses "annual," but that applies where the standard does not make clear what it means in its use of the term. In CIP Version 5, there is an opportunity and an obligation to unambiguously reference the periodic time parameter. Furthermore, one of the objectives of the SDT in Version 5 is to consider applicable CANs and use language that would no longer require a CAN to clarify an audit interpretation. Instead, the SDT used specific language to clarify a time parameter that approximates one year in time while also accounting for operational realities that make a 15 month parameter more reasonable. The term "annual" is no longer used in these CIP standards for periodic requirements, and, therefore, the CAN on the word "annual" can no longer apply.

TFE v. Per Cyber Asset Capability

Historically, phrases such as "where/when technically feasible" have been considered trigger language for requirements necessitating a technical feasibility exception ("TFE") in instances where a device could not meet the required parameter. The SDT has spent considerable time reviewing each use of TFE language in CIP Version 5 where it is necessary.

The SDT has also determined that there are some requirement parts that should not require a TFE, as certain parameters are not essential themselves, but should apply if a device is capable of the parameter. This is distinct from the reasoning for requirements with TFE language. In the latter requirements, a certain performance or parameter is required, regardless of technology, device, etc. By using "per (device/system) capability," the SDT does not intend that the specific parameter or performance is required regardless of capability, but only applicable on devices that have that capability. For example, proposed CIP-007-5, Requirement R4, Part 4.1 requires "Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents . . ." Here, the SDT does not intend to require event logging. However, if a Responsible Entity is using a device that can log events, it is required to enable event logging to the extent the device is capable.
The phrase "where technically feasible" indicates that the standard requires strict compliance without a TFE. As mentioned above, the drafting team does not intend for some requirements to be TFE-triggering. The underlying rationale for a TFE is that there is legacy equipment in place that is not readily compatible with a modern environment where cyber security issues are a concern.[2] Under such circumstances, the responsible entity must file a TFE that demonstrates strict compliance with an

[2] Order Approving Technical Feasibility Exception Procedures and Ordering Compliance Filing, Paragraph 3

applicable requirement is not technically possible and that there is an alternative course of action that will protect the reliability of the Bulk-Power System to an equal or greater degree than strict compliance.[3]

While a TFE requires an entity to show why strict compliance with an applicable requirement is not technically possible, "per device capability" clarifies that the requirement is only applicable to the devices for which compliance with a particular requirement is possible in the first instance. This provides reasonable flexibility to the industry while also retaining the TFE concept where necessary. Thus, the "per device capability" alternative reduces the need for TFEs and will be less onerous on entities. The SDT does not intend to eliminate TFEs altogether, but proposes to use the "per device capability" as an alternative that is effective in protecting the reliability of the Bulk-Power System.

VSLs

In previous drafts of the Version 5 CIP Cyber Security Standards, VSLs were posted concurrent with each standard. For this posting, the VSLs are presented in one document. They will continue to be prepared for posting for non-binding poll during the recirculation ballot. The VSLs should not be a basis for a ballot determination, and the SDT will continue to refine them as necessary.

Applicability Section of the standards (Introduction - Section 4 – Applicability)

There were several comments about the Applicability section of the standards in various comments related to specific standards. The SDT has reviewed those suggestions and made several changes to the applicability sections of each standard.

Several commenters stated that in part 4.2 of section 4, the criteria for qualified Distribution Providers and Load Serving Entities for UVLS/UFLS systems remain unclear. Specifically, the language was not clear on whether the 300 MW of load referred to the DPs and LSEs' share or to the total load shed. In addition, they also noted that the language for Transmission Protection systems is unclear and needs clarification to more precisely describe the protection systems that are in scope. They also suggested that these should be moved to Low Impact because there is no justification for small entities to be subjected to the requirements for Low and Medium entities. The SDT has proposed modified language to clarify the qualifications for UFLS and UVLS systems that specifies that they are those UFLS or UVLS systems that are part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard and that perform automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. With regard to the impact classification, the SDT believes that because of the function that UVLS and UFLS systems play in last ditch efforts to stabilize the BES, the 300 MW threshold provides a measure of impact that justifies the classification as medium impact systems: lower impact systems have already been removed from the scope and are not subject to these standards.

[3] Id, Paragraphs 5 and 8

Many references in the applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

Several comments indicated that LSEs should not be included in section 4 since the NERC Functional Model does not include any tasks related to the implementation and operation of load shedding systems. The SDT reviewed the LSEs tasks in the NERC Functional Model and has removed LSEs from the applicability of the CIP standards.

Several commenters suggested that the following language be added to the end of the criterion for Protection Systems: "and where the Protection System is connected to a supervisory control system providing remote operation capability." The SDT has reviewed the proposed addition to section 4.2.2 for Protection Systems and does not believe that the additional language to restrict the scope to only those Protection Systems that are remotely operated is intended or justified in the scope of section 4.2.2. The SDT notes that the proposed addition makes the assumption that all cyber vulnerabilities are based on remote operation capability. This would provide an incomplete mitigation for cyber threats that do not rely on remote operation for execution.

Several commenters stated that the inclusion of the glossary term "Systems" does not apply to DPs as used in section 4.2.2. One comment also pointed out that this is true in many other places where the term is used, while others' comments pointed out inconsistencies in the use of the term. The SDT notes that the terms Facilities, systems and equipment is always used in combination in the context of this application. The SDT has considered the intent of the terms in its uses and agrees that the glossary term "Systems" does not reflect the intent, and the SDT has made those changes where appropriate. In addition, the SDT believes that the issue is relieved with the changes made to refer to "assets" when referring to a group of Facilities, systems or equipment at a given location.

One comment stated that the statement at the beginning of the guideline and technical basis section that refers to applicability to DPs that refer to EOP-005 should be deleted since section 4.2.2 scopes more than EOP-005. In response, the SDT notes that the paragraph also includes reference to the registration criteria, in addition to EOP-005. The SDT believes the reference is appropriate.

One comment noted that in section 4, part 4.2.2, all single points of failure in the cranking paths should be protected and that where the Blackstart Resource is outside of the Responsible Entity's ownership, that the part of the cranking path that is the injection point to the cranking path to the unit to be

started should be specified. The SDT notes that Section 4.2.2 is not the criterion for determining the protection of the cranking path, but rather defines which part of a DPs equipment is in scope.

One comment suggested additional qualification in section 4 to ensure that the exemption section covers all facilities covered under a cyber security plan under the Nuclear Regulatory Commission (NRC) regulations. The SDT agrees with the clarification and has included the suggestion in the language in section 4 that covers nuclear facilities. The language has been added to section 4.2.4.3 to read: "In nuclear plants, the Systems, structures, and components that are regulated by the NRC under a cyber security plan pursuant to 10 C.F.R. Section 73.54."

One comment discussed the use of the phrase "required by a NERC standard" in section 4 and instances of affected Facilities, systems and equipment where there is no requirement to implement them by a NERC standard. The SDT agrees with the discussion and has made modifications to the language to more accurately reflect the intent.

One comment stated that section 4.2.4.2 attempts to define exemptions for communication links, but fails to include the exclusion of end points to those circuits (see CIP-005/R1.3). The SDT notes that end-points of circuits that are access points are included by the definition of Electronic Access Points (i.e. they are not "between" ESPs).

Reason for CIP Version 5

Some commenters inquired in their comments why CIP Version 5 was necessary, or they expressed a preference to continue under existing versions of the CIP Standards. To facilitate understanding of the reasons for Version 5 as part of the obligation to address the remaining directives in FERC Order No. 706, the SDT offers the following explanation and review of the previous versions of the NERC CIP Reliability Standards.

The NERC Board of Trustees adopted the first version of the CIP Reliability Standards on May 2, 2006. On August 28, 2006, NERC submitted to FERC for approval the Version 1 CIP Reliability Standards. On January 18, 2008, FERC issued its Order No. 706. In this order, FERC approved the Version 1 CIP Reliability Standards and issued more than 100 directives to NERC that included modifying the standards. An SDT began a phased-in approach to respond to the directives in FERC Order No. 706. As part of that phased-in approach, the SDT addressed the directives in the order that it could respond to quickly, and it developed a plan to address the remaining directives.

Version 2 of the CIP Reliability Standards was adopted by the NERC Board of Trustees on May 6, 2009. On May 22, 2009, NERC submitted to FERC for approval the Version 2 CIP Reliability Standards. On September 30, 2009 FERC issued its Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing. In this Order FERC approved the Version 2 CIP Reliability Standards and issued four additional directives to NERC that included modifying the

standards, with a required response in 90 days. At that time the SDT had to abandon it plan for addressing the outstanding directives in Order No. 706 and had to immediately address the newly issued directives.

Version 3 of the CIP Reliability Standards was adopted by the NERC Board of Trustees on December 16, 2009. On December 29, 2009, NERC submitted to FERC for approval the Version 3 CIP Reliability Standards. On March 31, 2010 FERC issued its Order on Compliance. In this Order FERC approved the Version 3 CIP Reliability Standards.

Version 4 of the CIP Reliability Standards (CIP-002-4 through CIP-009-4) was developed as an interim step to address the more immediate concerns from FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period. The Commission approved Version 4 on April 18, 2012.

Work has continued on further improvements to the standards, including responses to the remaining Commission directives from FERC Order No. 706, and it is these further enhanced standards that will be submitted to the Commission as Version 5. The next version of the CIP Reliability Standards will build on the Version 4 standards' establishment of uniform criteria for the identification of Critical Assets.

Version 5 of the CIP Reliability Standards provides a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

The changes in Version 5 also present many strategic advantages. Chiefly, a significant deliverable is to close out FERC Order No. 706. More importantly, Version 5 aligns to essential reliability functions and provides significant flexibility to entities in adapting requirements to individual operations.

Version 5 represents a systems-based approach to standards, which provides an opportunity to implement solutions and tailor security based on function, connectivity, risk, and impact. That flexibility represents a significant transition from the "in or out" demarcation for applying requirements in Versions 1 through 4 of the standards, as the drafting team has been able to structure Version 5 in a way that more finely tunes the applicability of each requirement based on connectivity, impact, and other characteristics.

Version 5 is also an experience-based set of standards. It is the first opportunity for the industry to evaluate, consider and incorporate lessons learned from implementation and audit of Versions 1 through 3, and the requirements aim to provide clearer emphasis on the required results. Collectively, the Version 5 standards support continued improvement in support of protecting against compromises that could lead to misoperation or instability in the Bulk Electric System.

NERC Quality Review

In addition to the changes that were made in response to comments, the SDT also submitted the set of standards to NERC for a quality review (QR). In response to the QR, the SDT made several changes for clarity, most of which related to style and form, grammar, word choice, etc.

The Applicability section was modified in response to QR to add "Interchange Authority" to the list of functional entities. The NERC Functional Model lists "Interchange Coordinator" while the registration criteria list "Interchange Authority," and they are not yet synchronized. Until that occurs, the SDT specifies that the standards apply to "Interchange Coordinator or Interchange Authority."
The SDT removed CIP-004-5, Requirement R4, Part R4.2. In previous drafts of the CIP standards (which was Requirement R6), the standard required designation of "one or more individuals" to authorize access, followed by a second requirement part for that individual to authorize based on need. The SDT has determined that the designation of one or more individuals is administrative in nature and is something that should be addressed by the Responsible Entity's plan, not by a requirement part. The performance required is now addressed through one requirement part.

The SDT also removed CIP-006, Requirement R3, Part R3.2, which required that Responsible Entities document outages for physical access control, logging, and alerting systems and retain the outage records for at least 12 calendar months. This requirement was a documentation requirement, and the SDT, in adding the modifying language to "identify, assess, and correct deficiencies" to Requirement R1, determined that the documentation requirement to log outages was not necessary.

Index to Questions, Comments, and Responses

Summary Consideration, Explanation, and Common Responses to Global Changes and to Issues and Comments Frequently Repeated 2

Questions with Summaries Included: 26

QUESTION A3 – CIP-002-5: 26

QUESTION A10 – CIP-003-5: 40

Questions with Votes Only: 44

1. Requirement R1 of draft CIP-002-5 requires the identification of high and medium impact BES Cyber Systems as described in Attachment 1. Further, it requires a Responsible Entity to review (and update as needed), the required identification within 60 calendar days of when a change to BES Elements or Facilities is placed into operation, which is planned to be in service for more than 6 calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category. Do you agree with the proposed Requirement R1? 44

2. Requirement R2 of draft CIP-002-5 states, "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once each calendar year, not to exceed 15 calendar months between approvals, even if it has no identified items in Requirement R1, Parts 1.1, 1.2, or 1.3." Do you agree with the proposed Requirement R2? 52

4. CIP-003-5 R1 states "Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall implement one or more documented cyber security policies that address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R1? 61

5. CIP-003-5 R2 states "Each Responsible Entity for its BES Cyber Systems not identified as high impact or medium impact shall implement one or more documented cyber security policies to address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2? 69

6. CIP-003-5 R3 states "Each Responsible Entity shall identify a CIP Senior Manager by name." Do you agree with the proposed Requirement R3? 77

7. CIP-003-5 R4 states "Each Responsible Entity shall review and obtain CIP Senior Manager approval for cyber security policies identified in Requirements R1 and R2, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals." Do you agree with the proposed Requirement R4? 85

8. CIP-003-5 R5 states "Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate and the date of the delegation, and approved by the CIP Senior Manager." Do you agree with the proposed Requirement R5? 93

9. CIP-003-5 R6 states "Each Responsible Entity shall document any changes to the CIP Senior Manager or any delegations within thirty calendar days of the change. Delegation changes do not need to be reinstated with a change to the delegator." Do you agree with the proposed Requirement R5? 101

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Bruce Metruck	New York Power Authority	NPCC	6
12.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
13.	Robert Pellegrini	The United Illuminating Company	NPCC	1
14.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
15.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
16.	Brian Robinson	Utility Services	NPCC	8
17.	Michael Jones	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Don Weaver	New Brunswick System Operator	NPCC	2
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3
24.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5

2.	Group	Annabelle Lee	NESCOR/NESCO										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3.	Group	Jason Marshall	ACES Power Marketing						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6. Shari Heino		Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Tim Soles	Occidental Power Services, Inc.	ERCOT	3
4.	Andy Gallo	Austin Energy	ERCOT	1
5.	Andy Gallo	Austin Energy	ERCOT	3
6.	Andy Gallo	Austin Energy	ERCOT	4
7.	Andy Gallo	Austin Energy	ERCOT	5
8.	Andy Gallo	Austin Energy	ERCOT	6

8.	Group	Emily Pennel	Southwest Power Pool Regional Entity									X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8. Annie Terracciano	Northern Lights Inc.	WECC 3										
9. Aleka Scott	PNGC	WECC 4										
10. Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11. Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12. Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13. Margaret Ryan	PNGC	WECC 8										
12. Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13. Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14. Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. M & A Electric Power Cooperative		SERC 1, 3										
4. Northeast Missouri Electric Power Cooperative		SERC 1, 3										
5. N.W. Electric Power Cooperative, Inc.		SERC 1, 3										
6. Sho-Me Power Electric Cooperative		SERC 1, 3										
15. Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X						
Additional Member	Additional Organization	Region Segment Selection										
1. Oglethorpe Power Corporation		SERC 5										
2. Georgia Transmission Corporation		SERC 1										
16. Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X
Additional Member	Additional Organization	Region Segment Selection										
1. MAHMOOD SAFI	OPPD	MRO 1, 3, 5, 6										
2. CHUCK LAWERENCE	ATC	MRO 1										
3. TOM WEBB	WPS	MRO 3, 4, 5, 6										
4. JODI JENSON	WAPA	MRO 1, 6										
5. KEN GOLDSMITH	ALTW	MRO 4										
6. DAVE RUDOLPH	BEPC	MRO 1, 3, 5, 6										
7. JOE DEPOORTER	MGE	MRO 3, 4, 5, 6										
8. SCOTT NICKELS	RPU	MRO 4										
9. TERRY HARBOUR	MEC	MRO 1, 3, 5, 6										
10. MARIE KNOX	MISO	MRO 2										
11. LEE KITTELSON	OTP	MRO 1, 3, 4, 5										
12. SCOTT BOS	MPW	MRO 6, 1, 3, 5										
13. TONY EDDLEMAN	NPPD	MRO 1, 3, 5										
14. THERESA ALLARD	MPC	MRO 1, 3, 5, 6										
17. Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing												
18. Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Timothy Beyrle	City of New Smyrna Beach	FRCC 4										
2. James Howard	Lakeland Electric	FRCC 3										

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. Greg Woessner	Kissimmee Utility Authority	FRCC	3									
4. Lynne Mila	City of Clewiston	FRCC	3									
5. Joe Stonecipher	Beaches Energy Services	FRCC	1									
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4									
7. Randy Hahn	Ocala Utility Services	FRCC	3									
19. Group	Joseph DePoorter	Madison Gas and Electric Company			X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Darl Shimko	MGE	MRO	3									
2. Joseph DePoorter	MGE	MRO	4									
3. Steve Schultz	MGE	MRO	5									
4. Jeff Keebler	MGE	MRO	6									
20. Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Mark Jones	Pepco	RFC	1									
21. Group	Rick Terrill	Luminant					X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Mike Laney	Luminant Generation Company LLC	ERCOT	5									
2. Tim Soles	Occidental Power Services, Inc.	ERCOT	6									
3. Tim Soles	Occidental Power Services, Inc.	ERCOT	3									
4. Andy Gallo	Austin Energy	ERCOT	1									
5. Andy Gallo	Austin Energy	ERCOT	3									
6. Andy Gallo	Austin Energy	ERCOT	4									
7. Andy Gallo	Austin Energy	ERCOT	5									
8. Andy Gallo	Austin Energy	ERCOT	6									
9. Brenda Hampton	Luminant Energy Company LLC											
22. Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Kevin Smith	BANC	WECC	1									
23. Group	Scott Brame	NCEMC	X				X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Rayburn Country Electric Cooperative			SPP										
2. Empire District Electric			SPP	1									
3. City Utilities of Springfield			SPP	4									
4. Westar Energy			SPP	1, 3, 5, 6									
5. Cleco Power			SPP	1, 3, 5, 6									
25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Pawel Krupa			WECC	1									
2. Dana Wheelock			WECC	3									
3. Hao Li			WECC	4									
27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Denise Lietz		Puget Sound Energy	WECC	1									
2. Erin Apperson		Puget Sound Energy	WECC	3									
28.	Group	Michael Mertz	PNM Resources	X		X							
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Laurie Williams		Public Service Co. of New Mexico	WECC	1									
2. Michael Mertz		Public Service Co. of New Mexico	WECC	3									
29.	Group	Sasa Maljukan	Hydro One	X									
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. David Kiguel		Hydro One	NPCC	1									
30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION A3 – CIP-002-5:

If you disagree with the changes made to CIP-002-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to attachment 1 and provided clarity to the requirements and associated rationales and measures. The explanations below describe the modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity in language.

Introduction - Section 4 – Applicability

There were several comments on this section in response to question A3, but the issues and responses relate generally to all of the standards. The discussion and response to comments on this section is provided earlier in this document in the Summary Consideration, Explanation, and Common Responses to Global Changes and to Issues and Comments Frequently Repeated section.

Requirement R1

Substantial changes were made to both the structure and the approach in Requirement R1: while the end result is a categorized list of high and medium impact BES Cyber Systems, there were many changes made to address concerns related to Low Impact assets and an asset based approach to deriving BES Cyber Systems. Many comments suggested a more prescriptive approach to the methodology used to arrive at the objective lists, including suggestions to add a flow-chart to the requirement: the SDT made a number of changes to address the "what" instead of the "how", and added substantive qualifications to better define the assets affected.

In particular, several commenters stated that the requirement to review and update the categorization on every change to the BES was an onerous burden in a company with a large number of constantly changing BES Facility configuration. The SDT has reviewed comments and is persuaded by the arguments presented. The SDT also considers that an annual review and update for BES Facilities, given the long term implementation of BES Facility changes, together with the requirements for BES Cyber Systems change control, provide a framework that provides the controls necessary.

Several commenters stated that the requirements for identification in Requirement R1 of CIP-002-5 be modified to require reference to “BES Sites” rather than Facilities, systems and equipment. One comment also suggested that inventories for Low Impact would allow requirements for low impact to be at the site level. Many comments suggested a Facilities impact-based approach to the derivation of the impact of BES Cyber Systems. The SDT has considered the suggestion and made modifications to the current CIP-002-5 requirements to incorporate the concepts using language already used in the criteria and Version 4 approved standards. While the terms Facilities, systems and equipment are precisely the same terms used in the definition of Critical Assets in prior versions, the SDT has made modifications to the proposed language to use the term “assets”, a term familiar to the industry in compliance activities for prior versions.

In response to numerous comments on the issue of asset-based derivation of cyber system impact, the SDT made substantive changes to Requirement R1s language and structure to include this approach. While Requirement R1 is ultimately intended to result in categorized BES Cyber Systems for the application of cyber security requirements, the SDT has made changes to the language and contents of Requirement R1 as well as the criteria in attachment 1 in consideration of comments received.

Several commenters commented on the use of the capitalized term Bulk Power in the rationale for Requirement R1. The paragraph has been deleted and the term is no longer used in the rationale.

One commenter suggested that a bullet is not required in requirement part 1.3 of Requirement R1. The comment also suggested an inconsistency between Requirement R1 and the associated VSL. The SDT has redrafted Requirement R1 in consideration of comments and the bulleted clause is now in the applicable part of the requirement. The inconsistency in the VSL has been corrected.

One commenter suggested that the SDT continues to insist there is no need to identify the low impact BES Cyber Systems and their associated Cyber Assets (e.g., R1.3) and that this causes an auditability issue. The SDT believes that an “asset” based approach in the revised draft and the requirement for the list of assets containing Low Impact BES Cyber Systems provides relief to the auditing issue.

Several commenters requested an explanation of the values used in the VSLs for Requirement R1. The SDT notes that the values are based on FERC Guidelines for VSLs that use percentages. Many entities commented on the need for absolute values for smaller entities since percentages would provide an unfair bias for small entities that would more easily reach percent based thresholds.

One comment stated that the SDT should consider reusing lists generated by other standards. The SDT notes that evidence used for other reliability standards can be presented for these CIP standards as long as they provide the evidence required to demonstrate compliance to the CIP requirement.

One commenter suggested that requirement parts 1.1, 1.2 and 1.3 should also include documentation as part of the requirement and that requirement part 1.4 should require the update prior to commissioning. The SDT's approach to requirement definition focuses on results and believes that a requirement to "document" does not directly result in the reliable operation of the BES. The SDT has defined the required functional result that directly contributes to the reliable operation of the BES. Requirement R1.4 has been removed by SDT in consideration of comments received.

One commenter suggested that by specifying requirements for Low Impact, CIP-002-5 implies a list of BES Cyber Systems. The commenter further suggested either requiring a list of Low Impact Cyber Systems or removing Low Impact altogether. The SDT notes that requirements must be explicit and that CIP-002-5 has made it clear and explicit that a list of Low Impact BES Cyber Systems is not required. However, in the new draft, a list of Low Impact assets is required to facilitate the application of policy requirements to Low Impact assets.

Several commenters suggested many editorial changes to the language used in Requirement R1. The SDT has made fundamental structural and language changes to Requirement R1 to address comments received.

Requirement R2

One commenter suggested that the rationale for Requirement R2 does not include approval of the lists. The SDT notes that the last sentence in the rationale refers to the approval process.

One commenter made many remarks on inconsistencies between the Requirement R2 language, the measure and the VSLs. The SDT has made modifications to R2 and its measures and VSLs for consistency.

Many commenters suggested alternative language, or reverting to the use of the term annual for the clause describing the annual review and approval. One commenter also inquired as to whether the clause supersedes an entity's definition of annual. The SDT has discussed alternative approaches and is using the term "at least once every 15 months" to provide reasonable flexibility to Responsible Entities while meeting the intent of the requirements. The SDT has intentionally not used the word "annual". This term is no longer used in these CIP standards for periodic requirements

and therefore, the CAN on the word annual can no longer apply in this requirement. One of the objectives of the SDT in Version 5 is to consider applicable CANs and use language that would no longer require a CAN to clarify audit interpretation. Instead, the SDT used specific language that implements its intent. This topic is also discussed in greater detail in the introductory, global section of these comment responses.

Attachment 1

Section 1 - High Impact Control Centers

One commenter stated that criteria for control centers fail to consider inter-Control Center connectivity and that the concept of mutual distrust does not work because of trusted paths. The SDT has included consideration of connectivity in the application of requirements. The applicability of mutual distrust depends on specific considerations of network configuration. A blanket statement based on an assumed configuration does not support the generalized comment. The SDT believes that requirements in the standards for protection of BES Cyber Systems provide a basis for Responsible Entities to implement the necessary protection in their network and system design.

Several commenters stated that the introductory text in High and Medium Impact criteria should be deleted or modified due to the change in approach for facilities based impact. The SDT notes that Requirement R1 still requires, ultimately, the categorization of BES Cyber Systems for the application of requirements. The SDT believes that the introductory text in the criteria for High and Medium is still required to express this result.

One commenter suggested on the inclusion of “associated data centers” in the control center criteria and argued that the BES Cyber Systems in these “data centers” would already be included. The SDT has made revisions to the definition of Control Centers, has now included data centers in the definition, and removed the phrase from attachment 1.

Many comments were received on the relationship of TO Control Centers and the functional obligations of TOPs. There was also a comment on the section in the guidance that pertains to TO Control Centers that perform the functional obligations of the TOP. In particular, one comment suggested removal of the guidance, citing ownership issues and issues with NERC Functional Entity registration. The SDT believes that the criterion in question is used to determine the impact of the BES Cyber Systems, and that, irrespective of registration issues, if these Cyber Systems perform a function that is relevant to the functional obligation of a TOP, and that this is formally delegated, then the impact should be appropriately assessed as such. The issue of ownership is a non-issue since the responsibility for compliance to the applicable requirements resides with the owner of the identified BES Cyber Systems that provide that function.

Several commenters suggested that the language used in criterion 1.3 with respect to TOP Control Centers needed clarification and that the guidance for this criterion should explicitly say that TO Control Centers that do not perform the functional obligation of the TOP should be classified as Medium. The SDT has inserted additional guidance to clarify this point. A TO facility that does not perform or does not have an obligation to perform any of the reliability tasks of a BA, TOP or GOP does not meet the definition of a Control Center and the BES Cyber Systems should be evaluated according to the criteria in attachment 1. TOs should review the functional tasks of a TOP and those of a TO and ensure they are not delegated any of these functional tasks through an agreement or a contract. In particular, TOs should note that the functional model does not list real-time operational tasks for that entity.

One commenter asked whether a TO Control Center that performs an operation under the direction of a TOP is performing a functional obligation of a TOP. The NERC Functional Model does not include operation of BES Facilities under the tasks or obligations of a TO, but does include them under the obligations of a TOP. If the TO has an obligation (contractually or because of some other formal agreement) to operate BES assets, whether it is in an emergency or in normal operational circumstances, under the direction of a TOP, then that Cyber System is used to perform the functional obligation of a TOP. The functional obligation of operational control of the BES asset has been delegated to the TO.

One commenter also asked whether a TO data center that collects data and then processes that data for transmission to the TOP is performing a functional obligation of the TOP. The SDT has moved the data center association to the definition of a Control Center and associates it with the facility hosting the operating personnel. In the scenario described, the TO data center is not associated with the BES Cyber Systems owned by the TOP. The “data center” described is analogous to field data aggregating facilities and are evaluated as BES Cyber Systems necessary for providing situation awareness for real-time operations, and should not be evaluated as TOP Control Center “data centers”.

One commenter suggested a number of modifications to the criteria aimed at better stratifying the distinction of Medium from High Impact, especially in the case of BA and TOP Control Centers. The SDT considered the suggestions and has made a number of modifications to address the comments. On another suggestion of increasing the threshold for High Impact BA and GOP Control Centers to 3000 MW, the SDT notes that the stratification of the High Impact from Medium Impact is mostly based on impact due to the wide area reliability tasks of the Functional Entities. However, the SDT has included modifications that provide some stratification of the levels for BA, TOP and GOP Control Centers which are consistent with thresholds approved in Version 4. On the subject of UFLS thresholds, the SDT reviewed recent developments in Regional Standards for UFLS and the tolerances specified in these standards as a basis for evaluation of

the current threshold: the SDT concluded that the current threshold represents a reasonable representation of the level of tolerance in these standards so far.

Several commenters suggested that Control Centers that use voice or manual instructions be categorized as Low Impact. The SDT notes that Cyber Systems that provide information to Control Center operators that use manual or voice to effect control operations on BES assets in real-time based on that information must be subject to the same protection as those that trigger automated operation. If the communication or manual operation results from information provided for real-time operations, there is no rationale for categorizing them as a lower impact.

One commenter suggested that the word "control" in the definition of Control Center requires more explanation and that the situation awareness section of the guidelines on BES Reliability Operating Services could include cyber systems used in collecting data for management and engineering analysis. The SDT has provided, in the guideline, the type of operations included in the use of the word. The definition provides further qualification in the context of the Control Center. The word "control" is used in several other standards and is a well understood concept in the BES environment. The intent of the situation awareness section in the guideline on BES Reliability Operating Services is to broadly define a reliability function and is not meant to be used solely for the qualification of applicable BES Cyber Systems: it is intended to be a first step in qualifying a population of Cyber Systems for further application of additional qualifications in the definition of BES Cyber Systems, applicable assets and the impact criteria in attachment 1.

One commenter stated that criteria 1.2 and 1.4 in attachment 1 qualify assets affected as "generation assets" and pointed out that not all assets in scope are strictly "generation assets". The SDT agrees and has made the suggested modification.

One commenter requested clarification on whether the 1500 MW in requirement parts 1.2 and 1.4 of attachment 1 referred to criterion 2.1. The SDT responds that the 1500 MW refers to total aggregate generation of 1500 MW, and is not tied to criterion 2.1.

Section 2 - Medium Impact

Several commenters stated that the 15 minute criterion in requirement part 2.1 of attachment 1 is unnecessary and redundant. Another commenter stated that this 15 minute clause was contrary to the "bright-line" concept. One commenter also stated that the inclusion of the 15 minute qualification in the criteria was inappropriate because the criteria define BES asset impact. The addition of this qualification resulted from previous comments and sought to

provide clarity in the scope of BES Cyber Systems to be included in consideration of this criterion. Where the qualification is included, the language makes it clear that it applies to the effect of the BES Cyber System.

There was a comment that the 15 minute in criterion 2.1 and 2.2 is going to be difficult to prove in an audit and suggested the term “that operate the reactive resource” instead in 2.2. As stated in the guideline, the intent of the 15 minute is to provide a boundary to the impact to real-time operations. The alternative use of the term “real-time” does not provide a useful defined term. The SDT believes that the commenter’s suggestion to use the term “that operate” in criterion 2.2 restricts the full scope of cyber systems that affect the real-time operation of the BES for reactive resources.

The commenter further suggested that criterion 2.1 should consider regional operational conditions and requested clarification on the 1000 MVAR threshold for 2.2. For 2.1, the SDT considered regional variations in determining this threshold and notes that this is the approved Version 4 criterion. For 2.2, the SDT consulted with operational and planning experts during the development of this criterion in Version 4.

One commenter stated that the commas around the words “as necessary” in criterion 2.3 were confusing. The SDT has reviewed the criterion and agrees that the commas are misplaced and have altered the intent of the criterion. The SDT has made changes to the placement of the commas to clarify the intent.

One commenter requested clarification on the use of the phrase “long term planning horizon” in criterion 2.3. The SDT notes that criterion 2.3 of attachment 1 does not use the phrase “long term planning horizon” but uses a specified one year or more near-term timeframe. The SDT notes the intent is to avoid the identification of generation facilities that could be used to remediate short term reliability issues.

Two commenters requested additional clarification in the notifications to asset owners in criteria 2.3 and 2.6. For 2.3, the notification is affected as part of the execution of a contract. For 2.6, the applicable IROL reliability standards require that the asset owners be notified. These standards do not specify how the notification is to be done, but that notification must be performed.

One commenter suggested that in requirement part 2.2 of attachment 1, the nameplate value should be qualified to account for ranges. The SDT has included a qualification of “maximum” in the criterion.

One commenter stated that criterion 2.3 references the long term planning horizon, contrary to the real-time operations aspect of the CIP standards. In addition, the commenter suggested that additional guidance be provided as to the notification of such obligations. Also, the commenter requested similar clarification in the guideline for criterion 2.8. The SDT points out that the criterion states that the designation of the asset is performed as part of a planning activity that has a time horizon of one year or more (near-term) by the Planning Coordinator or Transmission Planner, but the impact of a compromise of an affected BES Cyber System would meet the qualification for real-time operations. Additional clarification on notifications has been added to the guideline for criteria 2.3 and 2.8.

One commenter stated that the guidance section that refers to the category D contingency of TPL standards in the discussion of criterion 2.3 is unlikely and suggests removing it. The SDT has removed the reference in the guideline.

One commenter suggested using the phrase “generation interconnection facility” instead of “Transmission Facilities providing the generation interconnection required to connect generator output to the Transmission Systems Transmission Facilities” in criterion 2.8, citing the term used in Project 2010-07. Another commenter suggested on the exclusion of generation plant collector buses in criterion 2.4 and 2.5 in the guidance and suggested an explicit exclusion in the requirement. The SDT reviewed the standards in Project 2010-07 and has not found “generation interconnection facility” as a defined term in the NERC Glossary. The term is however used in the PRC standard in the project. The SDT intends that the application of this criterion to Transmission Owner/Transmission Operator owned and generator owned Transmission Facilities that provide this interconnection of generator output to the Transmission system. However, for clarity and to address the exclusion of these facilities in criteria 2.4 and 2.5 that one comment stated, the SDT has added this term as an inclusion in 2.8.

One commenter suggested alternative language for criterion 2.5 to clarify the application of the aggregate rating. The SDT made modifications to the language in 2.5 to clarify the application of the aggregate to the sum of applicable Transmission facilities at the station.

Many commenters suggested using, for criterion 2.6, the same language used in criteria 2.8 and 2.9. The SDT notes that in criterion 2.6, the criterion refers directly to the Facilities that make up the IROL and has used the exact language used in the IROL standards that require the identification of these specific Facilities. Criteria 2.8 and 2.9 apply to Facilities that could indirectly cause a violation or reduction of the IROLs.

Several comments were on the reasons for the removal of the WECC specific qualifications for those criteria that are based on IROLs. The SDT understands that the commenter has reconsidered its position on IROLs and that other changes in attachment 1 negate the need for any WECC specific qualification.

Several commenters requested information on the standards that require notification of asset owners for IROLs in criterion 2.6. One commenter also stated that the term Control Center is not a NERC defined term and to organize the guidelines by transmission, generation, etc. The SDT notes that the guidelines for criterion 2.6 provides information on the NERC Reliability Standard that contains these requirements (FAC-014) that require identification of these assets and notification to applicable owning Functional Entities. The term Control Center is a proposed defined term in this CIP standards package and the guidelines for criteria are organized by generation and transmission.

One commenter inquired as to why all facilities necessary for the NIPR (not just Transmission Facilities) are not included in criterion 2.7 (Nuclear Interface facilities). The SDT notes that the scope of applicability in NUC-001 is limited to transmission entities listed, which consists of registered entities.

One commenter requested clarification in the application guideline on how, in criterion 2.8, the TO would obtain information on whether generation it does not own or operate meets criterion 2.3. The SDT included additional guidance in the application guideline section.

One commenter stated that the UVLS/UFLS in criterion 2.10 that refers to the 300 MW threshold should specify the lowest rating in the last 12 months. Several commenters stated that the use of the highest MW rating in the guidelines and technical basis on UVLS/UFLS should be changed to “hourly integrated load”. The SDT has not specified the methodology used to determine the 300 MW and has deferred to the requirements of the applicable regional UFLS/UVLS standards.

One commenter stated that criterion 2.10 might imply that individual unconnected relays in a load shedding program under a common trip point would be included and suggested excluding these. The SDT believes that the qualification of a common control system addresses this concern and believes that the exclusion language has the unintended consequence of excluding individual relays irrespective of their impact.

One commenter stated that the language in criterion 2.10 which specifies “regional load shedding programs” is problematic since there is no such requirement and pointed out that PRC standards place the responsibility for

establishing UFLS programs on the Planning Coordinator. The SDT has made modifications to section 4 that pertains to load shedding and criterion 2.10 to more accurately reflect the requirements of the PRC standards.

There was a comment that for criterion 2.10, the language suggests that any compromised component that make up SPS, RAS or automated switching system is required to be protected regardless of if it has an effect on the IROL or not. The SDT notes that the current language does not imply this requirement. The current language only applies if the compromise, whether of one or more components of the SPS, RAS or automated switching system, would cause a violation of one or more IROLs or "cause a reduction of one or more IROLs".

One commenter suggested setting a threshold for Special Protection Systems for applicability of these CIP standards. The SDT notes that all Special Protection Systems, irrespective of any threshold, are designated as Critical Assets under Version 4. The SDT notes that this has been the case because of the critical function provided by Special Protection Systems in the reliable operation of the BES.

Numerous commenters stated that in part 2.11 of attachment 1, the threshold for generation Control Centers should be changed to 1500 MW for consistency with the generation threshold in other criteria in Medium Impact. One commenter also pointed out an inconsistent term in the flow chart in the guidelines and technical basis section. In the same area, another commenter commented that part 2.11 should be removed and that the specific hydro situation should be handled in the definition. The SDT's intent in 2.11 is to include as Medium all the remaining Control Centers not already classified as High, because of the functions provided by Control Centers. In defining a 300 MW threshold for generation Control Centers in 2.11, the SDT was attempting to address a situation specific to hydro-electric generation Facilities. The SDT has removed this artificial threshold in view of changes made to this criterion. Further, the SDT made modifications in the threshold in the criterion for generation Control Centers to address these comments. The inconsistency of terms used in the flowchart has been corrected.

Several entities commented on the removal in draft two of criteria for restoration resources (blackstart units and cranking paths) from the Medium category. Some were in favor of this removal while others were not. Specifically, one commenter made several comments regarding generation and cranking path restoration resources. One comment read that restoration resources should be rated as Medium Impact. In contrast, another commenter suggested that restoration resources should not be included in the scope of the application of the CIP standards because of the absence of the need for remote data communication in the event of a restoration and the exclusion of cranking path from the definition of the BES. In response, in addition to the justification provided as part of the draft two materials, the SDT has

further considered industry input and comments in the consideration of these criteria with respect to their effect on overall reliable operation of the BES and has now removed them from High or Medium Impact criteria. In response, the SDT notes that the assumption that remote access through data communications is necessary for the realization of cyber security threats represents an incomplete mitigation approach, and that the CIP standards are aimed at protecting cyber systems that would impact the real-time operation of the BES, not solely those that directly operate elements of the BES. NERC Reliability Standards that govern the operation of load shedding programs and the protection of the BES elements are other examples of such approaches.

Section 3 – Low Impact

One commenter noted that the criteria in section 3 of attachment 1 should include the phrase "not included in high or medium". The SDT has made the necessary clarification.

General Comments

One commenter suggested that the footnote regarding the effective date of Version 5 and the effective date of Version 4 should be moved to the main text of the effective date. The SDT considered moving this footnote, but believes that movement of the footnote could cause unnecessary confusion, since the effect would not be different. The footnote simply clarifies the effective language that Version 4 does not go into effect and is superseded by Version 5.

There was a comment that the varying language regarding the phrase "destroyed, degraded, or otherwise rendered unavailable" and its variations needs to be consistent. In addition, Southern Company provided additional clarification language for the cranking path criterion in Low Impact. The SDT has reviewed the uses of the term and has ensured consistency when referencing Facilities or BES Cyber Systems. The main difference is the addition of "destroyed" and "otherwise rendered unavailable" in the case of Facilities. The SDT has added the suggested clarification in criterion 3.3.

One comment was on the use of the word "would" instead of "could" in the standards and recommended the use of the prospective word "could". The SDT believes that the use of the word "would" is appropriate to describe the certain impact of a compromise due to an exploitation of vulnerability.

One commenter stated that the last paragraph on page seven leaves it up to the registered entity to determine the level of granularity when identifying the BES Cyber Systems and instructs the registered entity to take into consideration the operational environment and scope of management and raised questions of auditability in the text. The SDT notes that the background and guideline sections are only providing context to the standards. The only auditable parts of the

standards are the applicable definitions and requirements. The SDT directs the commenter to the definition of BES Cyber System for effective application of the requirements.

There was a comment on the examples for Electronic Access Control and Monitoring Systems in the background section, specifically the use of certificate authorities, security event monitoring systems and intrusion detection systems. The SDT uses the term "Certificate Authorities" as an example of the type of cyber assets owned by the Responsible Entity that would be subject to the CIP standards if it relates to a function that is used within the scope of a BES Cyber System. The SDT has used the generic term "security event monitoring systems" as a generic functional term and has specifically avoided the use of the various acronyms used to include this function. This is also true of the term "intrusion detection systems": the SDT is providing an example of the function, and the term "intrusion prevention systems" includes functions that are not within the scope of the requirements. The SDT acknowledges that intrusion prevention systems necessarily include an intrusion detection function.

One commenter suggested the inclusion of network attached storage and storage area networks in the examples for Protected Cyber Assets. Examples provided are not intended to be exhaustive lists, but are intended to provide some examples of the types of systems that could meet the requirements for the definition of Protected Cyber Assets. They are not intended to mean that all of these types of systems are necessarily Protected Cyber Assets, but are examples of systems that could be Protected Cyber Assets if they meet the definition.
SPP suggested footnoting the time horizon reference in requirements. Time Horizons are standard designations used in all requirements and is a standard requirement for all NERC standards requirements. They are required characteristics of each requirement in the same way that Violation Risk Factors are. The SDT believes that footnotes for these are not required as they are generically defined in other NERC documents.

One commenter requested clarification of the general use of transmission facility and its scope. In using terms such as "Facility" in the criteria, the SDT has made substantial changes to Requirement R1 that provides flexibility to the Responsible Entity to define what the term includes within the definition of the requirement. Requirement R1 now includes a listing of the types of assets to be considered that provides a more defined scope to the applicability of CIP-002-5 and the CIP cyber security standards. Within these, Responsible Entities have flexibility in defining the sets within these considerations for application of the criteria.

One commenter requested clarification on entities that have coordination responsibilities. The SDT notes that the table in the guidance provides guidance on those entities that have responsibilities for inter-entity coordination. In a

restoration scenario, those Responsible Entities that require inter-entity coordination to perform their functions that require such coordination have responsibility for this coordination.

One commenter pointed to an inconsistency between the title of the standard and the heading of the document. The SDT corrected the inconsistency.

One commenter stated that the NERC Functional Model does not define Functional Entities. The SDT notes that the current version of the Functional Model (Version 5) defines both Reliability Functions and the Functional Entity that performs the tasks. In addition, there are further responsibilities defined under Functional Entities which are specifically defined in relation with other Functional Entities.

A commenter requested additional guidance in the concept of BES Cyber System. The SDT has made several modifications to the guidance for the overall concept of BES Cyber System, including additional peripheral terms related to BES Cyber Systems, such as Protected Cyber Assets. The SDT believes these additional clarifications provide the additional guidance on the concepts.

There was a comment on the guidance on BES Reliability Operating Services provided for optional use by entities as an aid to scope BES Cyber Systems in the guideline section of the standards. One commenter also suggested removing the designation of Functional Entities for the BES Reliability Operating Services to minimize differing opinions. The SDT made several modifications to this section in consideration of these comments where appropriate. With respect to comments on voltage control and Distribution Providers, the Functional Model clearly lists voltage reduction in its tasks. The designation of Functional Entities is provided as guidance and resulted from comments from previous drafts. The SDT believes that this information provides additional guidance for some Responsible Entities in scoping their BES Cyber Systems.

One commenter suggested that the format of the standard is different and suggested moving the background to the end together with the guideline. The SDT has used the standard template for results based standards and is the recommended standards development format and approach.

There was a suggestion that the rationale should not be part of the standard. The rationale statements will be removed from the official filing and included as information, together with the guidance information.

Several comments were on the use of bright lines and the problem with a one size fits all approach without provisions for studies and engineering analysis and the requirement to require at least some protection for all BES assets. The SDT notes that the objective of Version 5 of the CIP standards is to provide some level of protection to all BES Cyber Systems according to the impact to the real-time operation of the BES assets they are supporting. The bright line based approach was approved by industry stakeholders and FERC as part of Version 4.

One commenter suggested the use of a more definitive term “prevent” in qualifying impact on functions in the reliable operation of the BES. In addition, there was a suggestion for an explanation of the use of the 15 minute window in the definition of BES Cyber Asset. The SDT believes that the word “prevent” does not provide a qualification for the full scope of applicability, but a subset. The intent of the SDT is to ensure that impacts also cover impairment as well as outright “prevention”. An explanation of the 15 minute window is in the background section of the standard under real-time operations.

One comment suggested that the stipulation of ownership for compliance responsibility is inconsistent with PRC standards that also stipulate “operate”. The SDT has consistently maintained that responsibility for compliance is the asset owner’s.

There was a general comment on the application of FISMA and the NIST framework in relation to the CIP standards. The SDT notes that CIP V5 considered the NIST framework as one of the inputs to the drafting of these standards in response to FERC Order 706. The SDT did not consider FISMA requirements, but rather the NIST Risk management framework as directed by Order 706. The SDT also considered input from several other frameworks and has used those inputs in the drafting of standards that are subject to compulsory compliance and enforcement. The NIST 800-53 series is characterized as guidelines for controls, not compliance requirements.

QUESTION A10 – CIP-003-5:

If you disagree with the changes made to CIP-003-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the major issues identified through the comment form with CIP-003-5 included (1) the list of low impact BES Cyber Systems for Requirement R2, (2) demonstration of policy implementation, (3) clarity of policy topics in Requirement R2, and (4) the reliability benefit of the annual review/approval of the cyber security policies as well as maintaining documentation of changes to the CIP Senior Manager and delegates.

List of Low Impact BES Cyber Systems for Requirement R2

Numerous commenters identified concerns that while the SDT intended to provide protection from discrete identification of Low Impact BES Cyber Systems, there was still significant concern that this would still be required in order to demonstrate compliance with the requirement. Additionally, commenters suggested that the object of the policy for Low Impact BES Cyber Systems should be on the facilities (or "sites") themselves and not specifically the Low Impact BES Cyber Systems. The SDT continues to believe that the identification of low impact BES Cyber Systems would not be required in order to comply with CIP-003-5 R2. However, the SDT also agrees with commenters that a facilities based approach to the low impact policy comes with a number of benefits. Among these being the creation of a reasonable level of abstraction (the facility) of which to refer to the low impact BES Cyber Systems, thus facilitating any necessary sampling during an audit, without explicitly needing a list of these cyber systems themselves. Consequently, CIP-003-5 R2 has leveraged a reference to CIP-002-5 where facilities with low impact BES Cyber Systems are identified. The SDT believes this approach will provide consistency of application of the policy for low impact BES Cyber Systems, provide a reasonable approach for audit oversight, and create additional clarity on the evidentiary expectations.

Policy Implementation

There were a number of comments that expressed issues with ambiguity in the use of the term "implement" as it relates to the cyber security policies in both CIP-003-5 R1 and R2. In reviewing this comment, the SDT noted that the obligation to "implement" the cyber security policy has existed since version 1 of the CIP standards. Additionally, FERC directed the ERO in Order 706 to "to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards." While this directive did not specifically direct changes to the cyber security policy, as this policy already had the obligation to implement in version 1, the SDT is cognizant that any change to the contrary would require reasonable justification.

As it relates to the CIP-003-5 R1 cyber security policy for medium impact and high impact BES Cyber Systems, the SDT believes there is sufficient justification to make a modification to the language of the requirement in order to provide the clarity that the industry desires around the obligation to "implement." The SDT strongly believes that it has not lessened the obligation to implement the cyber security policy. However, given the required scope of the CIP-003-5 R1 cyber security policies, the SDT believes that implementation of these cyber security policies is effectively demonstrated through compliance with CIP-004-5 through CIP-011-1. Therefore, the SDT has chosen to remove the term "implement" from CIP-003-5 R1. The SDT believes that this should provide clarity as to the expectation of implementation as well as to relieve concerns of double jeopardy between CIP-003-5 R1 and the entire body of CIP-004-5 though CIP-011-1.

The SDT has handled this concern differently for the low impact cyber security policies in CIP-003-5 R2. As there are no corresponding requirements in CIP-004-5 through CIP-011-1 that require explicit implementation of areas addressed by the low impact policy, there are no double jeopardy concerns. The SDT has attempted to provide structure around the obligation to implement the cyber security policies through the global modifications that provide for continuous improvement and the identification, assessment, and correction of deficiencies. The expectation of the SDT is that entities will define cyber security policies that address the four required areas and put these policies in effect using an overall framework that provides reasonable assurance that the policies are applied through methods that identify, assess, and correct any deficiencies.

Policy Topic Clarity for Low Impact Policy

In addition to ambiguity over the implementation of the cyber security policy for low impact BES Cyber Systems, commenters expressed concern over the clarity of the individual policy topics for low impact BES Cyber Systems. The SDT appreciates these comments and has made some modifications to the topic language. However, the SDT understands that these modifications do not completely alleviate the concerns around individual topical clarity. The SDT has modified the topic "Physical access controls" to "Physical security controls" and "Electronic access controls" to "Electronic access controls for external routable protocol connections and Dial-up Connectivity." The SDT chose to not add too much additional detail to these policy topics in recognition of the wide range of environmental, geographic, technical, operational, and logistical differences that may exist amongst the set of low impact BES Cyber Systems. As such, the SDT's intent is to allow Responsible Entities to have flexibility to design and implement the most efficacious security program possible for their particular set of low impact BES Cyber Systems. The modification to physical security controls over physical access controls acknowledges this approach. "Physical security controls" gives great discretion to the Responsible Entity to choose controls that are effective. The SDT believes the paradigm shifts in NERC CIP Reliability

standards allowing for multiple levels of security (high, medium, and low) and creating an atmosphere of continuous improvements through the identification, assessment, and correction of deficiencies will address the concerns of compliance risk that are driving the need for more prescriptiveness in requirements language. Additionally, the SDT added the language to R2.3 "…for external routable protocol connections and Dial-up Connectivity" to address the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact.

Reliability Benefit and Double Jeopardy Concerns of Requirements R3, R5, and R6

Numerous commenters also raised questions about either the reliability benefit or double jeopardy of requirements R3, R5, and R6. Often, these questions were tied to work going on in NERC standards related to Paragraph 81 of the FERC Order approving the FFT process. The comments about their reliability benefit sometimes hinged on them being a requirement in and of themselves, rather than a component of the requirements for R1, R2, and R4 in draft two. The double jeopardy concerns also raised similar questions as to whether a violation of R3, R5, and R6 in draft two would also constitute a violation of R1, R2, and R4 of draft two. The SDT agreed with these concerns. The SDT believes that the same reliability and security objectives will be reached, while alleviating unnecessary compliance concerns, by combining these requirements. As such, the review and approval for each of the cyber security policies has been added as an obligation in the security policy requirements (R1 and R2) themselves. Additionally, the obligation to keep the CIP Senior Manager and delegation documentation up-to-date has been added to those requirements (now R3 and R4), respectively.

Modify Signature to Approval in Measures

Several commenters mentioned the use of "signature" in the measures when the requirement called for "approval." The SDT had never intended to imply that a wet ink signature was the only acceptable form of evidence of approval. Language in the guidelines and technical basis section further clarified that hardcopy or electronic approvals were acceptable. The SDT has modified all instances of "signature" in the measures in CIP-003-5 to "approval' to prevent any confusion and better align with the language in the requirement itself.

Minority Comments

The SDT also received a number of different comments that asked various questions or raised assorted concerns about the topics that were included in Requirement R1. Among other things, these comments mentioned confusion about the guidance related to terms used in the policy topics, inclusion of Interactive Remote Access separate from ESPs, and the relationship between these topics and CIP-004-5 through CIP-011-1. The intention of the SDT was for these policy items

to individually reference each of the standards CIP-004-5 through CIP-011-1. As such, the SDT has chosen to align the policy topics with the title of the other CIP standards (with some exceptions) and include a specific reference to the standards itself in order to clarify that alignment. As mentioned in the discussion of policy implementation above, the SDT's expectation is that implementation of the cyber security policy for medium and high impact BES Cyber Systems will be demonstrated through compliance with CIP-004-5 through CIP-011-1.

Typographical Errors

Several commenters also noted a typographical error where the VRF for CIP-003-5 R2 was listed as low in the requirement and medium in the VSL table. The SDT appreciates commenters pointing this out. The intention of the SDT was for the VRF of CIP-003-5 R1 for medium and high impact BES Cyber Systems to be medium, consistent with CIP-003-4 R1 and for the VRF of CIP-003-5 R2 to be low due to the lesser risk associated with low impact BES Cyber Systems. The SDT has corrected this mistake.

VSL Comments not responded to:

One comment suggested that Requirement R6 should have four VSLs based on days late. The SDT has removed the requirement because the addition of language to identify, assess, and correct deficiencies in what is now Requirement R4 covers the documentation of delegations.

One comment stated to start missing discrete elements of a program as low VSLs in Requirement R2. The SDT has made this change.

One comment suggested to use Lower/Moderate VSLs for Requirement R2 instead. In response, the VSLs only address the degree to which entities can violate a requirement and not the risk power to the BES from said violations.

For the Requirement R4 VSLs, there was a comment that the VSL should read: Lower/Medium – Lack of Review High/Severe – Lack of Approval. This requirement has been removed because the annual review is already accomplished in Requirement R1 and the need to have a CIP Senior Manager sign the policy is administrative in nature.

There was a comment that the VSL for Requirement R3 is more detailed than the requirement itself. The SDT has updated the VSL to match the requirement.

Questions with Votes Only:

1. **Requirement R1 of draft CIP-002-5 requires the identification of high and medium impact BES Cyber Systems as described in Attachment 1. Further, it requires a Responsible Entity to review (and update as needed), the required identification within 60 calendar days of when a change to BES Elements or Facilities is placed into operation, which is planned to be in service for more than 6 calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category. Do you agree with the proposed Requirement R1?**

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
ACES Power Marketing	No
PPL Corporation NERC Registered Affiliates	No
BC Hydro	No
IRC Standards Review Committee	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No

Organization	Yes or No
Duke Energy	No
Dominion	No
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	No
MRO NSRF	No
Florida Municipal Power Agency	No
Madison Gas and Electric Company	No
Luminant	No
SMUD & BANC	No
Progress Energy	No
NCEMC	No
Dairyland Power Cooperative	No
Western Electricity Coordinating Council	No
CenterPoint Energy	No
Tri-State G&T - Transmission	No
PacifiCorp	No

Organization	Yes or No
PNM Resources	No
Hydro One	No
Southern Company Services, Inc.	No
Western Area Power Administration	No
Utility Services Inc.	No
Consumers Energy Company	No
Muscatine Power and Water	No
North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency	No
NIPSCO	No
Portland General Electric	No
TransAlta Centralia Generation LLC	No
Trans Bay Cable	No
National Grid	No
Hydro-Quebec TransEnergie	No
LCEC	No

Organization	Yes or No
Pacific Gas and Electric Company	No
Ingleside Cogeneration LP	No
Manitoba Hydro	No
Niagara Mohawk (dba National Grid)	No
PSEG	No
Bonneville Power Administration	No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Illinois Municipal Electric Agency	No
NV Energy	No
Wisconsin Electric Power Company	No
The Empire District Electric Company	No

Organization	Yes or No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Texas Reliability Entity	No
Nebraska Public Power District	No
City of Austin dba Austin Energy	No
ISO New England	No
Network & Security Technologies, Inc.	No
City Utilities of Springfield, MO	No
American Public Power Association	No
Alliant Energy	No
Springfield Utility Board	No
Exelon Corporation and its affiliates	No

Organization	Yes or No
Indiana Municipal Power Agency	No
NYISO	No
Cowlitz County PUD	No
Brazos Electric Power Cooperative	No
US Bureau of Reclamation	No
NRG Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
SPP and specific Member companies	Yes
Puget Sound Energy, Inc.	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes

Organization	Yes or No
Arizona Public Service Company	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Services Corporation	Yes
Lincoln Electric System	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Xcel Energy	Yes
Flathead Electric Co-op	Yes
Tennessee Valley Authority	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes

Organization	Yes or No
PJM Interconnection	Yes
Kansas City Power & Light	Yes
MEAG Power	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes

2. Requirement R2 of draft CIP-002-5 states, "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once each calendar year, not to exceed 15 calendar months between approvals, even if it has no identified items in Requirement R1, Parts 1.1, 1.2, or 1.3." Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
ACES Power Marketing	No
BC Hydro	No
Texas RE NERC Standards Review Subcommittee	No
NRG Companies	No
Florida Municipal Power Agency	No
SMUD & BANC	No
Progress Energy	No
PacifiCorp	No
Utility Services Inc.	No

Organization	Yes or No
NIPSCO	No
LCEC	No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
NextEra Energy, Inc.	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Texas Reliability Entity	No
City of Austin dba Austin Energy	No
ISO New England	No

Organization	Yes or No
Kansas City Power & Light	No
Indiana Municipal Power Agency	No
Brazos Electric Power Cooperative	No
PPL Corporation NERC Registered Affiliates	Yes
IRC Standards Review Committee	Yes
Southwest Power Pool Regional Entity	Yes
Duke Energy	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes

Organization	Yes or No
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Luminant	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
Hydro One	Yes

Organization	Yes or No
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency	Yes
Portland General Electric	Yes

Organization	Yes or No
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
Pattern	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes

Organization	Yes or No
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Xcel Energy	Yes
Flathead Electric Co-op	Yes
Bonneville Power Administration	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Ameren	Yes
Northeast Utilities	Yes
Oncor Electric Delivery Company LLC	Yes
Nebraska Public Power District	Yes

Organization	Yes or No
PJM Interconnection	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes
MEAG Power	Yes
American Public Power Association	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
California ISO	Yes
US Bureau of Reclamation	Yes

4. CIP-003-5 R1 states "Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall implement one or more documented cyber security policies that address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
NESCOR/NESCO	No
ACES Power Marketing	No
Duke Energy	No
Progress Energy	No
NCEMC	No
PNM Resources	No
AEP Standards based SME list	No
Xcel Energy	No
MidAmerican Energy Company	No
Ameren	No

Organization	Yes or No
NextEra Energy, Inc.	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Kansas City Power & Light	No
Brazos Electric Power Cooperative	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Southwest Power Pool Regional Entity	Yes
NRG Companies	Yes
PNGC Comment Group	Yes

Organization	Yes or No
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Florida Municipal Power Agency	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Hydro One	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes

Organization	Yes or No
Portland General Electric	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes

Organization	Yes or No
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Lakeland Electric	Yes
New York Power Authority	Yes
Tampa Electric Company	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Illinois Municipal Electric Agency	Yes
NV Energy	Yes
Wisconsin Electric Power Company	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Oncor Electric Delivery Company LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
City of Austin dba Austin Energy	Yes
ISO New England	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes
MEAG Power	Yes
American Public Power Association	Yes
Alliant Energy	Yes

Organization	Yes or No
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
California ISO	Yes
US Bureau of Reclamation	Yes

5. **CIP-003-5 R2 states "Each Responsible Entity for its BES Cyber Systems not identified as high impact or medium impact shall implement one or more documented cyber security policies to address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2?**

Summary Consideration:

Organization	Yes or No
NESCOR/NESCO	No
ACES Power Marketing	No
PPL Corporation NERC Registered Affiliates	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No
NRG Companies	No
Duke Energy	No
MRO NSRF	No
Florida Municipal Power Agency	No

Organization	Yes or No
Madison Gas and Electric Company	No
Pepco Holdings Inc & Affiliates	No
National Rural Electric Cooperative Association (NRECA)	No
Progress Energy	No
NCEMC	No
Dairyland Power Cooperative	No
AEP Standards based SME list	No
Snohomish County PUD	No
Edison Mission Marketing & Trading	No
Consumers Energy Company	No
Muscatine Power and Water	No
Lower Colorado River Authority	No
LCEC	No

Organization	Yes or No
LCRA Transmission Services Corporation	No
Ingleside Cogeneration LP	No
Xcel Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service	No

Organization	Yes or No
Corporation and Upper Pennisula Power Company	
Nebraska Public Power District	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Kansas City Power & Light	No
Network & Security Technologies, Inc.	No
MEAG Power	No
Alliant Energy	No
Exelon Corporation and its affiliates	No
Deseret Power	No
Brazos Electric Power Cooperative	No
Northeast Power Coordinating Council	Yes
BC Hydro	Yes

Organization	Yes or No
IRC Standards Review Committee	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Southern California Edison Company	Yes
SPP and specific Member companies	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes

Organization	Yes or No
PNM Resources	Yes
Hydro One	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Utility Services Inc.	Yes
NIPSCO	Yes
Portland General Electric	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes

Organization	Yes or No
Pacific Gas and Electric Company	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
New York Power Authority	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes

Organization	Yes or No
Texas Reliability Entity	Yes
ISO New England	Yes
City Utilities of Springfield, MO	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
California ISO	Yes
US Bureau of Reclamation	Yes

6. CIP-003-5 R3 states "Each Responsible Entity shall identify a CIP Senior Manager by name." Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
ACES Power Marketing	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
Florida Municipal Power Agency	No
Progress Energy	No
Southern Company Services, Inc.	No
Independent Electricity System Operator	No

Organization	Yes or No
Lakeland Electric	No
Tampa Electric Company	No
Illinois Municipal Electric Agency	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Texas Reliability Entity	No
City of Austin dba Austin Energy	No
Kansas City Power & Light	No
Network & Security Technologies, Inc.	No
American Public Power Association	No

Organization	Yes or No
Tucson Electric Power	No
Cowlitz County PUD	No
Brazos Electric Power Cooperative	No
California ISO	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
NRG Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC)	Yes

Organization	Yes or No
including OPC, GTC & GSOC	
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
Hydro One	Yes

Organization	Yes or No
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes
Portland General Electric	Yes
Trans Bay Cable	Yes
National Grid	Yes

Organization	Yes or No
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
City of Palo Alto	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Xcel Energy	Yes
Bonneville Power	Yes

Organization	Yes or No
Administration	
New York Power Authority	Yes
Tennessee Valley Authority	Yes
MidAmerican Energy Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
Wisconsin Electric Power Company	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
ISO New England	Yes
City Utilities of Springfield,	Yes

Organization	Yes or No
MO	
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

7. CIP-003-5 R4 states "Each Responsible Entity shall review and obtain CIP Senior Manager approval for cyber security policies identified in Requirements R1 and R2, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals." Do you agree with the proposed Requirement R4?

Summary Consideration:

Organization	Yes or No
NESCOR/NESCO	No
ACES Power Marketing	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
Florida Municipal Power Agency	No
Progress Energy	No
Edison Mission Marketing & Trading	No
Independent Electricity System Operator	No

Organization	Yes or No
Pattern	No
United Illuminating Company	No
Lakeland Electric	No
Tampa Electric Company	No
Tennessee Valley Authority	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
Ameren	No
NextEra Energy, Inc.	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
PJM Interconnection	No
Kansas City Power & Light	No

Organization	Yes or No
American Public Power Association	No
NYISO	No
Cowlitz County PUD	No
Brazos Electric Power Cooperative	No
California ISO	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
Texas RE NERC Standards Review Subcommittee	Yes
NRG Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes

Organization	Yes or No
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes

Organization	Yes or No
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
Hydro One	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes

Organization	Yes or No
Portland General Electric	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
Turlock Irrigation District	Yes

Organization	Yes or No
Xcel Energy	Yes
Bonneville Power Administration	Yes
New York Power Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Oncor Electric Delivery Company LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
City of Austin dba Austin Energy	Yes
ISO New England	Yes

Organization	Yes or No
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
US Bureau of Reclamation	Yes

8. CIP-003-5 R5 states "Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate and the date of the delegation, and approved by the CIP Senior Manager." Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No
NRG Companies	No
Duke Energy	No
Florida Municipal Power Agency	No
Progress Energy	No
Hydro One	No

Organization	Yes or No
Independent Electricity System Operator	No
Xcel Energy	No
Flathead Electric Co-op	No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper	No

Organization	Yes or No
Pennisula Power Company	
PJM Interconnection	No
City of Austin dba Austin Energy	No
ISO New England	No
American Public Power Association	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Cowlitz County PUD	No
California ISO	No
ACES Power Marketing	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes

Organization	Yes or No
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes

Organization	Yes or No
NIPSCO	Yes
Portland General Electric	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes

Organization	Yes or No
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Kansas City Power & Light	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield,	Yes

Organization	Yes or No
MO	
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

9. CIP-003-5 R6 states "Each Responsible Entity shall document any changes to the CIP Senior Manager or any delegations within thirty calendar days of the change. Delegation changes do not need to be reinstated with a change to the delegator." Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Texas RE NERC Standards Review Subcommittee	No
NRG Companies	No
Florida Municipal Power Agency	No
Progress Energy	No
Portland General Electric	No
Independent Electricity System Operator	No
Flathead Electric Co-op	No

Organization	Yes or No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
ISO New England	No
Kansas City Power & Light	No

Organization	Yes or No
American Public Power Association	No
Tucson Electric Power	No
Cowlitz County PUD	No
California ISO	No
ACES Power Marketing	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
Southwest Power Pool Regional Entity	Yes
Duke Energy	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric	Yes

Organization	Yes or No
Cooperative, Inc. (JRO00088, NCR01177)	
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes

Organization	Yes or No
Hydro One	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes
Trans Bay Cable	Yes

Organization	Yes or No
Pattern	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes

Organization	Yes or No
Xcel Energy	Yes
Bonneville Power Administration	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
Wisconsin Electric Power Company	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes

Organization	Yes or No
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards

Comment Form B

CIP-004 through CIP-007 Questions

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Index to Questions, Comments, and Responses

Questions with Summaries Included: 17
QUESTION B8 – CIP-004-5, R1, R2, R3, R4 or R5: 17
QUESTION B9 – CIP-004-5, R6 or R7: 22
QUESTION B12 – CIP-005-5, R1: 41
QUESTION B13 – CIP-005-5, R2: 52
QUESTION B17 – CIP-006-5: 55
QUESTION B23 – CIP-007-5, R1, R2, R3 or R4: 58
QUESTION B24– CIP-007-5 REQUIREMENT R5: 84
Questions with Votes Only: 94
1. CIP-004-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 94
2. CIP-004-5 R2 states "Each Responsible Entity shall have a role-based cyber security training program to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 101
3. CIP-004-5 R3 states "Each Responsible Entity shall implement its documented role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3? 109
4. CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4? 117
5. CIP-004-5 R5 states "Each Responsible Entity shall implement one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable elements in CIP-004-5 Table R5 –

Personnel Risk Assessment." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5? 125

6. CIP-004-5 R6 states "Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R6? 133

7. CIP-004-5 R7 states "Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R7? 141

10. CIP-005-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 149

11. CIP-005-5 R2 states "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 157

14. CIP-006-5 R1 states "Each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? .. 164

15. CIP-006-5 R2 states "Each Responsible Entity shall implement one or more documented visitor control programs that include each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 172

16. CIP-006-5 R3 states "Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3? 180

18. CIP-007-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 188

19. CIP-007-5 R2 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 196

20. CIP-007-5 R3 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3? 204

21. CIP-007-5 R4 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4? 212

22. CIP-007-5 R5 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5? 220

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Bruce Metruck	New York Power Authority	NPCC	6
12.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
13.	Robert Pellegrini	The United Illuminating Company	NPCC	1
14.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
15.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
16.	Brian Robinson	Utility Services	NPCC	8
17.	Michael Jones	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Don Weaver	New Brunswick System Operator	NPCC	2
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3
24.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5

2.	Group	Annabelle Lee	NESCOR/NESCO									

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3.	Group	Jason Marshall	ACES Power Marketing					X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6. Shari Heino		Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. Tim Soles	Occidental Power Services, Inc.	ERCOT 3										
4. Andy Gallo	Austin Energy	ERCOT 1										
5. Andy Gallo	Austin Energy	ERCOT 3										
6. Andy Gallo	Austin Energy	ERCOT 4										
7. Andy Gallo	Austin Energy	ERCOT 5										
8. Andy Gallo	Austin Energy	ERCOT 6										
8. Group	Emily Pennel	Southwest Power Pool Regional Entity										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9. Group	Alan Johnson	NRG Companies					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10. Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11. Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8. Annie Terracciano	Northern Lights Inc.	WECC 3										
9. Aleka Scott	PNGC	WECC 4										
10. Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11. Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12. Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13. Margaret Ryan	PNGC	WECC 8										
12. Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13. Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14. Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. M & A Electric Power Cooperative		SERC	1, 3									
4. Northeast Missouri Electric Power Cooperative		SERC	1, 3									
5. N.W. Electric Power Cooperative, Inc.		SERC	1, 3									
6. Sho-Me Power Electric Cooperative		SERC	1, 3									
15. Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X						
Additional Member	Additional Organization	Region	Segment Selection									
1. Oglethorpe Power Corporation		SERC	5									
2. Georgia Transmission Corporation		SERC	1									
16. Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X
Additional Member	Additional Organization	Region	Segment Selection									
1. MAHMOOD SAFI	OPPD	MRO	1, 3, 5, 6									
2. CHUCK LAWERENCE	ATC	MRO	1									
3. TOM WEBB	WPS	MRO	3, 4, 5, 6									
4. JODI JENSON	WAPA	MRO	1, 6									
5. KEN GOLDSMITH	ALTW	MRO	4									
6. DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6									
7. JOE DEPOORTER	MGE	MRO	3, 4, 5, 6									
8. SCOTT NICKELS	RPU	MRO	4									
9. TERRY HARBOUR	MEC	MRO	1, 3, 5, 6									
10. MARIE KNOX	MISO	MRO	2									
11. LEE KITTELSON	OTP	MRO	1, 3, 4, 5									
12. SCOTT BOS	MPW	MRO	6, 1, 3, 5									
13. TONY EDDLEMAN	NPPD	MRO	1, 3, 5									
14. THERESA ALLARD	MPC	MRO	1, 3, 5, 6									
17. Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing												
18. Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				
Additional Member	Additional Organization	Region	Segment Selection									
1. Timothy Beyrle	City of New Smyrna Beach	FRCC	4									
2. James Howard	Lakeland Electric	FRCC	3									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3. Greg Woessner	Kissimmee Utility Authority	FRCC	3										
4. Lynne Mila	City of Clewiston	FRCC	3										
5. Joe Stonecipher	Beaches Energy Services	FRCC	1										
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4										
7. Randy Hahn	Ocala Utility Services	FRCC	3										
19.	Group	Joseph DePoorter	Madison Gas and Electric Company			X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Darl Shimko	MGE	MRO	3										
2. Joseph DePoorter	MGE	MRO	4										
3. Steve Schultz	MGE	MRO	5										
4. Jeff Keebler	MGE	MRO	6										
20.	Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Mark Jones	Pepco	RFC	1										
21.	Group	Rick Terrill	Luminant					X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Mike Laney	Luminant Generation Company LLC	ERCOT	5										
2. Tim Soles	Occidental Power Services, Inc.	ERCOT	6										
3. Tim Soles	Occidental Power Services, Inc.	ERCOT	3										
4. Andy Gallo	Austin Energy	ERCOT	1										
5. Andy Gallo	Austin Energy	ERCOT	3										
6. Andy Gallo	Austin Energy	ERCOT	4										
7. Andy Gallo	Austin Energy	ERCOT	5										
8. Andy Gallo	Austin Energy	ERCOT	6										
9. Brenda Hampton	Luminant Energy Company LLC												
22.	Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Kevin Smith	BANC	WECC	1										
23.	Group	Scott Brame	NCEMC	X				X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				

Additional Member	Additional Organization	Region	Segment Selection
1. Rayburn Country Electric Cooperative		SPP	
2. Empire District Electric		SPP	1
3. City Utilities of Springfield		SPP	4
4. Westar Energy		SPP	1, 3, 5, 6
5. Cleco Power		SPP	1, 3, 5, 6

25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						

Additional Member	Additional Organization	Region	Segment Selection
1. Pawel Krupa		WECC	1
2. Dana Wheelock		WECC	3
3. Hao Li		WECC	4

27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					

Additional Member	Additional Organization	Region	Segment Selection
1. Denise Lietz	Puget Sound Energy	WECC	1
2. Erin Apperson	Puget Sound Energy	WECC	3

28.	Group	Michael Mertz	PNM Resources	X		X							

Additional Member	Additional Organization	Region	Segment Selection
1. Laurie Williams	Public Service Co. of New Mexico	WECC	1
2. Michael Mertz	Public Service Co. of New Mexico	WECC	3

29.	Group	Sasa Maljukan	Hydro One	X									

Additional Member	Additional Organization	Region	Segment Selection
1. David Kiguel	Hydro One	NPCC	1

30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION B8 – CIP-004-5, R1, R2, R3, R4 or R5:

If you disagree with the changes made to CIP-004-5, Requirements R1, R2, R3, R4 or R5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the requirements, measures, and VSLs associated with Requirement R1, R2 R3, R4 or R5 of CIP-004-5. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Note

In draft two, Requirement R2 required a documented process for its role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems while Requirement R3 was the implementation of that process. Requirement R4 required one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems while Requirement R5 was the implemented of the one or more documented processes. In preparing CIP-004-5 for draft 3, the SDT determined that Requirements R2 and R3 could be combined, and so could Requirements R4 and R5. In that way, the requirements more closely match most other requirements in CIP-004-5 through CIP-011-5 to implement a documented process, and it also facilitated inclusion of the correcting deficiencies approach, explained in the common response section of this comment response, so that the resulting requirements, draft 3's Requirements R2 and R3, could be implemented "in a manner that identifies, assesses, and corrects deficiencies." Therefore, Requirement R6 from draft 2 was renumbered to Requirement R4 in draft 3, and Requirement R7 from draft 2 was renumbered as Requirement R5. For the purposes of the comment summaries and responses for this question, the requirement number references refer to the requirement numbers as listed in draft 2, unless otherwise noted.

General

The applicable systems section has been reviewed and revised to help ensure consistency within CIP-004-5 and with the other CIP standards. This should also make clear that these requirements are not applicable to Low Impact BES Cyber Systems. The SDT has decided not to include the concept of authorized unescorted electronic access. Individuals with

authorized electronic access must be trained and have a personnel risk assessment performed as per the requirements. This applies to all personnel including employees, vendors and contractors. For example, the question on a vendor controlled system would require the vendor to meet the requirements as set forth in CIP-004-5.

The SDT has stricken the "attain and retain" language for the training requirement, but has chosen to keep it for the personnel risk assessment requirements. The difference between those words and "acquire and maintain" are negligible.

The SDT does not agree with the suggestion to make Requirements R2 and R3 an expansion of the awareness program instead of training. The SDT believes that for protection of these BES Cyber Systems more targeted training is needed.

The guidelines and technical basis section has been updated to better align with the new draft content and organization. One areas of focus is the training content on networking hardware and software and other issues of electronic interconnectivity. More description around the criminal history check has also been added.

Requirement R1

The SDT has added language in the change rationale section to reinforce the concept that a registered entity does not need to ensure or prove all authorized personnel have received awareness. The language in R1.1 has also been revised to further clarify this point through the use of the word, reinforces. Also, the SDT has added language to clarify that awareness of cyber security practices can include physical security information.

The SDT appreciates the suggestions to allow the registered entity to define the timeline for awareness reinforcement or their own quarters, but believes the language is best retained as written for consistency.

In the measures for Requirement R1, the SDT has removed the reference to "documented security awareness program" and has modified the language to be consistent with the other CIP standards. The language, "not limited to" has also been revised and reviewed for consistency across the standards.

Requirement R2/Requirement R3

These two requirements have been combined into a single requirement which covers the training content in R2.1, in a single table, and the training frequency in R2.2 and R2.3. Another key change in R2 is the modification of the language to clarify that the registered entity is able to determine their training program(s) to fit their needs and it can be based on role, function or responsibility. In concert with this change, Table R2 section 2.1 was deleted to help eliminate the

language focusing on role based training. Training is required of individuals with authorized, unescorted physical access or authorized electronic access as per the revised R2.2 and R2.3. In addition to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity, the SDT believes training is also needed for individuals with access to Physical Access Control Systems and Electronic Access Control or Monitoring Systems. Also, the SDT has removed the reference to BES Cyber Systems in Table R2 formerly in sections R2.2, R2.3 and R2.4. For Table R2 previous section 2.5, the Change Rationale has been modified to reflect this is a new training requirement. Also, this training should be tracked for personnel involved in the visitor control process in accordance with Table R3 section 3.2 The SDT agrees that recovery plan information referenced in Table R2, previous section 2.8 should be labeled appropriately. The training content on cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets will remain in Table R2 as it is a new requirement from FERC Order 706 and the SDT has provided additional guidance to clarify the intent of this entry.

For Table R2, previous section 2.2, the SDT believes the training should be focused on policy content, not availability, and has made no changes. In Table R2, the SDT has chosen to retain both identification of incidents and response to incidents as separate content as the personnel who need to be trained on each may be different. The scope of training on recovery plans is left to the registered entity and no changes have been made to the standard. Also, the SDT believes the focus of recovery is the specific recovery plans, not the business impact analysis. The measure for Table R2 has been modified to focus on training material as evidence and the guidance has been revised to reflect the type of content this training should include.

The SDT has edited the language formerly in R3 for clarity with removal of the role based reference and the attain/retain language. Since there are no references to evidence retention in the requirement part 1.2, evidence retention, of the compliance section of the standard applies. The reference to documentation that was in Table R3 section 3.1 has been removed as it is covered in the measure.

The SDT does not agree that access to Low Impact Cyber Systems need the training defined in R2. Also, R2 has language included (in a manner that identifies, assesses, and corrects deficiencies) as suggested by some comments to allow detection and correction of flaws. The proposal to allow the registered entity to define the timeline for training was not supported by the SDT. For 2.2 and 2.3 (formerly in Table R3 section 3.2), the SDT believes the language is sufficiently clear that the time interval is between training dates and does not need that language added. BES Cyber Systems was changed to applicable cyber assets in 2.2. The two entries on initial and recurring training are now in Table R2. The SDT

has revised the language in the measure for these two entries to make it clear the focus is on training records which should include training date and date access is granted.

Requirement R4/Requirement R5

As suggested, the SDT has combined these two requirements into one and it is now Requirement R3. The SDT has modified the language formerly in Requirement R4 to help clarify that identity confirmation and criminal history check are part of the personnel risk assessment (PRA). The PRA is the outcome of the process or criteria used by a registered entity to evaluate the results of the identity verification (for the initial PRA) and seven year criminal history records check to determine what, if any, authorized access to grant to employees, contractors or vendors. The level of documentation for the process or criteria is left to the registered entity, but should be sufficient for a third party to understand how the decision is made. In defining the seven year criminal history records check, it is not the intent for the registered entity to evaluate the individual's residence locations, education or prior employment. The language has been revised to indicate the criminal history records check should cover locations where the individual has resided/lived for six consecutive months during the past seven years. The initial identity confirmation, even if performed under prior versions of the standards, is sufficient for the employment duration of the individual. The initial identity verification, criminal history check and PRA should be retained in accordance with requirement part 1.2 in the evidence retention component of the compliance section of the standard. A PRA performed under previous versions of the standards is valid until it reaches the end of its seven year lifespan. The intent of the SDT is that the PRA in effect is no older than seven years. The SDT has provided guidance on the acceptable documentation for an exception to the seven year criminal history records check which includes agreements with labor unions. If the registered entity is unable to fully complete the seven year criminal history records check, the SDT feels it is important to document the reasons for the exception so it will not be removing that piece of the requirement. Also, the timeframe for renewal of the criminal history records check is currently seven years and the SDT believes it should remain as such. Drug and alcohol checks are typically performed by entities under an existing program and the SDT chooses not to add this to the requirement. In section 3.3 of the new Table R3, the term process is used to define the method used by a registered entity to evaluate the results of the criminal history records check. Although a "Transportation Worker Identification Credential (TWIC)-like" program would be helpful to facilitate compliance with the PRA requirements, the SDT does not have the authority to make that happen. Measures – The Measures have been revised to focus on examples consisting of documentation. For example, a dated copy of the current PRA, which was performed in the previous seven calendar years, would be sufficient.

VRF/VSL

The language in the VRF for R2 has been changed to remove the reference to role based training. The SDT reviewed the VRFs for R3, R4 and R5 (as indicated above, R3 from draft 2 is now in R2, and R4 and R5 from draft 2 have been combined into R3 in draft 3) to consider if the rating should be a Lower risk factor. The SDT believes the risk associated with violations of these requirements is higher than for R1 and R2; hence the Medium risk factor is appropriate. The VSL for R1 has been modified to include the case where the Responsible Entity failed to implement on-going security awareness for two or more consecutive quarters as the next step above the criteria for High. Since the Medium severity level is for missing two content topics, the High should follow as three or more, not four or more. Commenters also asked whether the size of the company matters in the VSL for R3 (which is now in R2). In response, the SDT has modified the VSL for High and Severe according to the suggestion. The VSL targets the BES Cyber System and does not account for company size. Commenters suggested the Moderate and High VSL language for R4 (now R3) should be swapped on the basis that not performing an identity verification and a background check is worse than failing to document the results. (Also, the incorrect reference in draft 2's R4 to "4.5", which does not exist, has been corrected). In response, the SDT has modified the language for the Severe VSL to include the case where a registered entity failed to implement its PRA processes. Commenters also asked whether the size of the company matters in the VSL for R5 (which is now in R3). In response, the VSL targets the BES Cyber System and does not account for company size.

QUESTION B9 – CIP-004-5, R6 or R7:

If you disagree with the changes made to CIP-004-5, Requirements R6 or R7 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the major concerns with CIP-004 Requirements R6 and R7 center on removal of access privileges under various categories of termination actions. In addition, there were repeated instances noting a lack of clarity regarding access approvals, personnel transfers or reassignments and the proper storage and handling of NERC CIP information.

Note

In draft two, Requirement R2 required a documented process for its role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems while Requirement R3 was the implementation of that process. Requirement R4 required one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems while Requirement R5 was the implemented of the one or more documented processes. In preparing CIP-004-5 for draft 3, the SDT determined that Requirements R2 and R3 could be combined, and so could Requirements R4 and R5. In that way, the requirements more closely match most other requirements in CIP-004-5 through CIP-011-5 to implement a documented process, and it also facilitated inclusion of the correcting deficiencies approach, explained in the common response section of this comment response, so that the resulting requirements, draft 3's Requirements R2 and R3, could be implemented "in a manner that identifies, assesses, and corrects deficiencies." Therefore, Requirement R6 from draft 2 was renumbered to Requirement R4 in draft 3, and Requirement R7 from draft 2 was renumbered as Requirement R5.

Applicability Section

As in other Version 5 standards, in CIP-004, requirement part 4.1 (formerly part 6.1), there were several comments on changing instances of Medium Impact BES Cyber Systems to "Medium Impact BES Cyber Systems with External Routable Connectivity." Commenters also commented that "dial-up connectivity" should be removed from the applicability section to be consistent with the applicability sections of other Version 5 standards. In both of these cases, the SDT has revised the standard to reflect these comments.

Requirement R4 (formerly R6) General Comments

Multiple commenters recommended that new or additional items or items currently found in the rationale section should be modified and listed as requirements at the requirement level.

Comments suggested modification to allow for self-correction in certain cases, so that each responsible entity shall implement: measure performance to detect flaws; correct detected flaws expeditiously, and if needed take corrective action to prevent recurrence of flaws. This is a general requirement that applies to the Requirement R4 (formerly R6) sub requirements. Though not necessary from a procedural perspective, more instruction on what needs to be considered in the standards is better than insufficient information. The SDT has incorporated the correcting deficiencies modification to the implementation wording in CIP-004-5 in Requirements R2, R3 and R4.

Commenters recommended that the rationale discussing controls for BES Cyber Systems without user accounts should be added to the appropriate requirements in Requirement R4 (formerly R6). The SDT has moved that discussion from the rationale section to the requirement tables.

A commenter suggested that requirement parts 4.2, and 4.3 (formerly covered in parts 6.2, 6.3 and 6.4) be modified to include requirement parts 4.11, 4.12 and 4.13 (formerly parts 6.11, 6.12 and 6.13) along with part 4.1 (formerly part 6.1) in the requirement table. The SDT has combined requirement parts 4.2, 4.3 and 4.4, which now directly reference those sub-parts in part 4.1.

R4.3 (formerly 6.3)
Commenters recommended that there be a corresponding annual review of provisioned physical security privileges necessary for performing assigned work functions. The SDT has combined requirement parts 4.2, 4.3 and 4.4 (formerly parts 6.2, 6.3 and 6.4). The measures in the new requirement part 4.2 call for signed documents, automated workflow approvals or email showing persons with access have authorizations and similar or the same records showing the consideration of appropriate privileges on the basis of need…" These measures apply to electronic access, unescorted physical access into a PSP and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Part 4.3 (formerly part 6.5)
Commenters asked for clarification on the reviews of authorized and provisioned electronic access and unescorted physical access. The SDT has modified part 4.3 to clarify the requirement. It now reads "verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records."

R4 (formerly R6)

Some commented that the measures for 4.1 (formerly part 6.1) should include unescorted electronic access. The issue with this is that electronic access, by its digital nature cannot be escorted. Consequently, there is no "unescorted" electronic access. Electronic access to data or systems is either authorized or unauthorized. One could call it "supervised" access but the problem lies with a "supervisor" having to be continuously diligent and unerringly able to determine if the supervised user is doing anything malicious. This is not possible and frankly constitutes a threat to network integrity and data confidentiality. The recommended option would be to identify those contractors who require electronic access and run them through the personnel appraisal and the training processes and grant them appropriate access privileges. There are no other means to help ensure there are no unauthorized accesses or data disclosures.

Requirement Part 4.1 (formerly 6.1)

One commented that formerly sub-requirements 6.1.1, 6.1.2 and 6.1.3 (current 4.1.1, 4.1.2 and 4.1.3) would be clearer if the requirement was written, "Designate one or more individual(s) to authorize one or more of the following types of access". The SDT has changed the requirement to "have a process to authorize". This negates the need to specifically identify an approver and highlights consideration of "need" for physical access, electronic access and access to "designated" physical and electronic storage locations for BES Cyber System Information.

One commenter suggested that current requirement part 4.1 should include the names and roles of individuals who authorize the various types of access. The SDT has changed the requirement to "have a process to authorize". This negates the need to specifically identify an approver and highlights consideration of "need" for physical access, electronic access and access to "designated" physical and electronic storage locations for BES Cyber System Information.

One commenter recommended changing the term "designate" in current requirement parts 4.1, 4.2 and 4.3 (formerly parts 6.1, 6.2 and 6.3) to "identify.' The SDT has changed requirement 4.1 to "have a process to authorize". This negates the need to specifically designate or identify an approver and highlights consideration of "need" for physical access, electronic access and access to "designated" physical and electronic storage locations for BES Cyber System Information. The SDT has also combined 4.2, 4.3 and 4.4 into a single requirement (4.2).

Several commenters pointed out that access to physical and electronic locations where BES Cyber System Information is stored should have greater clarity around the word "physical". The requirement part 4.1 (formerly part 6.1) has been

changed to clarify storage locations for BES Cyber System Information. It now reads, "access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Several commenters recommended revising the phrase "unescorted physical access" to "unescorted physical access into a PSP." The SDT agrees and has made that change.

Multiple commenters stated that requirement part 4.1 (formerly part 6.1) should allow for roles in the designation of those individuals who can authorize the various accesses. The SDT believes that changing the requirement to "have a process" allows the entity the flexibility to construct their authorization process in a way that best suits their needs.

Requirement Part 4.2 (formerly Part 6.2)

Several commenters recommended that requirement parts 6.2 and 6.3 be revised for clarity. They proposed that requirement parts 6.2 and 6.3 be changed to read, "the individual(s) or role(s) designated in requirement part 6.1 shall authorize electronic access deemed necessary by the Responsible Entity, except for CIP Exceptional Circumstances." To respond to the comment, requirement parts 4.2, 4.3 and 4.4 have been combined into a single requirement part 4.2. At the same time, the individual authorization has been replaced with a process in requirement part 4.1. The process merely provides a means to authorize, and is implemented in the manner preferred by the Responsible Entity.

Several commenters also suggested that instead of the phrase "deemed necessary," "deemed appropriate" would be more accurate – stating that deeming appropriate is easier than deeming necessary. The SDT used the term "necessary…for performing assigned work functions" to better focus on specific accesses and minimize generalization and audit interpretation issues.

One commenter suggested the phrase "Responsible Entity" be removed from parts 4.2, 4.3 and 4.4 (formerly 6.2, 6.3, and 6.4). The requirements state "that the Responsible Entity determines is necessary." The SDT believes that the term "Responsible Entity" removes a degree of specificity that could be problematic if individuals change frequently or the determination of "necessary" is made by more than one individual within the organization. The SDT has combined requirement parts 4.2, 4.3 and 4.4 and has referenced a process required in part 4.1 "have a process" that allows flexibility to establish authorization frameworks tailored to the Responsible Entity's needs.

One commenter stated that the phrase "need to know" in requirement part 4.2 (formerly Part 6.2) is difficult to quantify and is subject to interpretation. They recommended removing that phrase, believing that approvers who grant all access

"deemed necessary" strongly indicates that determinations of need to know are part of the authorization process. The SDT has removed references referring to "need to know."

Many commenters recommended revising the phrase "unescorted physical access" to read "unescorted physical access into a PSP." For clarity, the SDT has changed the wording to "access into the Physical Security Perimeter."

One commenter stated that requirement part 6.3 (now covered under new part 4.1) implies that determination of need for performing work functions is needed for each physical access. They recommended that Responsible Entities document all roles and activities in advance, negating the need for the Responsible Entity restating access they have "determined is necessary." The SDT has combined the requirement parts 4.2, 4.3 and 4.4 and established a requirement for a "process" to develop an authorization framework best suited to the Responsible Entity's needs. This will allow the commenter's company to document all roles and activities in advance if that is the company's preference.

One commenter recommended removal of the phrase "for performing assigned work functions" due to concerns with potential interpretation requests. The SDT believes that since "work functions" are not subject to audits, there is no need to remove the conditional phrase. In addition, there must be some frame of reference for authorizing accesses and work functions are a logical baseline.

Many commenters suggested changing the wording of requirement part 6.4 (now covered under new part 4.1) from "location" to designated repository. The SDT believes that specifying a designated location is less subject to interpretation and in most cases exempts portable equipment from being identified as a "repository" in the event that NERC CIP information may be temporarily resident on such equipment. The SDT has retained the term "designated locations" since a location more often connotes multiple purposes. In contrast a repository, similar to location by definition, still carries connotations of a specified area, limited to a specific function. "Location" provides flexibility and designating locations removes incidental temporary storage on non-designated devices from the audit process.

One commenter questioned the following: Is the "intent of the requirement to track authorized access to the physical and electronic locations where BES Cyber System Information is stored. Is the requirement regarding physical location intended to include physical access to file servers hosting BES Cyber System Information in electronic format or is it intended to be limited to physical access to locations where BES Cyber System Information in stored in hardcopy format?" The SDT believes that unescorted physical access includes to both hard copy data and access to equipment used for storing electronic copies. Although physical proximity to equipment does not constitute electronic access, from

an information protection standpoint, access to that equipment could result in damage or destruction of those devices storing electronic copies.

One commenter suggested that in requirement part 6.4, (now covered under new part4.1)to eliminate ambiguity, that the term “necessary for performing assigned work functions,” be replaced with “appropriate for the roles and responsibilities.” The SDT understands the concern. In this case replacing “necessary” with “appropriate” does little to eliminate ambiguity. In addition, both terms are likely to prompt interpretations. Also, not all entities are configured to grant authorizations by roles and responsibilities. To address the entirety of the CIP affected population, the SDT believes that the original wording provides more universal applicability.

One commenter believes that requirement part 6.4 (now covered in new part 4.1) should be separated into two requirements. The first requirement would be to identify the repositories that store either physical media containing BES Cyber System Information (paper copy) or the electronic storage of BES Cyber System Information. The second requirement would be the authorization of access to only those designated repositories that have been identified by the entity. The SDT believes that using the term “locations”, as long as they are “designated” serves the same purpose as an identified repository. Because “designated” has been added to the requirement, so must a measure to acknowledge the existence and itemize “designated storage locations.” This will add another measure but will also reduce the potential for audit interpretation and ambiguity.

One commenter recommended that the words “are necessary for performing assigned work functions” be replaced simply with “are necessary”. The SDT believes that this revision, although more economical, could create a situation where the question is asked “necessary for what?” To avoid that possibility “necessary for assigned work functions” is less likely to prompt questions of scope of authorizations.

One commented that the words “physical and” should be removed because it imposes a requirement to create physical access controls and authorization processes to an office that may have a printout of Cyber System Information. The SDT notes that if, as suggested by a number of other companies, “designated locations” are used, incidental, non-designated temporary locations of NERC CIP System Information will not be subject to that requirement.

Former Requirement Part 6.3

Former requirement part 6.3 prescribed specific ways to conduct authorizations and referenced individuals designated in former part 6.1. The SDT has instead changed the language in part 4.1 to require the Responsible Entity to "Have a process to authorize . . .", which could certainly include designating one or more individuals, etc., as part of the process, but the requirements do not specifically prescribe the administrative method of achieving the required performance. Thus, former Requirement Part 6.3 no longer exists in the same manner as presented during draft 2.

Several commenters stated that because of potential minor errors or mismatches associated with the required review of authorizations and provisioned individuals, requirement part 4.3 (formerly part 6.5) should be subject to the FFT process. The SDT understands the concern, but FFT is not a function of the requirement. That is a function of potential violations and determined after the fact, not in the standard requirement itself.

One commenter recommended that the following statement from the rationale for requirement part 4.3 (formerly part 6.5) be entered into the requirement or its Measures section: "If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement." While that statement offers some clarification in guidance, the SDT cannot add a requirement or measure that makes a determination whether or not a particular error is a violation.

One commenter stated that requirement parts 4.3 and 4.4 (formerly parts 6.5 and 6.6) are major scope expansions which were not directed by FERC. They further claim that the requirements overlap and are not contributing to a commensurate improvement to security. The SDT believes that reviews such as those in parts 4.3 and 4.4 (formerly parts 6.5 and 6.6) do in fact provide a means to identify indicators of malicious activities, rogue accounts, retained accounts that are no longer authorized, etc. The fact that FERC did not direct the requirement development does not negate the validity or the need for the requirements.

Several commenters recommended adding "currently" between "individuals provisioned". The SDT agrees with the recommendation and will take appropriate action. The SDT has reworded the requirement part 4.3 (formerly part 6.5) to "individuals with an *active* electronic access…"

One commenter stated that requirement part 4.5 (formerly part 6.7) should be revised as follows, “Verify, at a timeframe that the Responsible Entity deems necessary, that individuals provisioned for authorized electronic access or authorized unescorted physical access have associated authorization records.” The SDT believes that there must be a specified review period and associated evidence to ensure that Responsible Entities consistently meet the requirement.

One commenter suggested adding the words "to BES Cyber Systems" after the words "physical access" in part 4.3 (formerly part 6.5). The SDT believes this proposed revision is already addressed in the Applicable Systems section of the requirement.

One commenter suggested that in the measures section, there should be consistency of word order between "dated document of verification..." and "documentation of dated verification”. The first measure asks for “dated documentation of verification,” which simply provides a point in time wherein the verifications were performed. The second measure requires a document that provides times of specific verifications themselves, of authorization for access and provisioning of access. The SDT changed the language to provide clarity and consistency to the measure. The consistent language now reads, “dated documentation of the verification.”

Requirement Part 6.4

One commented that the measures in requirement parts 4.4 and 4.5 (formerly parts 6.6 and 6.7) contain contradictory constructions. The background section states that a numbered list includes all required evidence. In the measure, however, these parts state that evidence “may include, but is not limited to.” The SDT has added the phrase “that includes all of the following” to reconcile the format with the intent of the measure.

Several commenters stated that the wording in requirement part 4.4 (formerly part 6.6) is too prescriptive, specifically “verifications that all user accounts, user account groups, or user role categories and their specific associated privileges.” They proposed substituting that wording to read, “verifications that BES Cyber System access privileges are appropriate for the individual(s) or role(s) responsibilities.” The SDT believes that the word appropriate is too vague and subject to interpretation. The goal is to verify access to specific accounts. In this case, the existing wording maintains the scope and leaves no ambiguity around which accounts require verification. Regarding the list of measures, the SDT has revised the measure by adding “that includes all of the following” to reconcile the format with the intent of the measures.

Several commenters stated that the measures should only require verification that the entity performed the verification while leaving the results of the verification out of the measure. The SDT believes that requiring verification should

specify those items to be verified. Asking for a "listing of all accounts/account groups", a "description of privileges", "accounts assigned" and 'verification that privileges are authorized and appropriate" does not expand scope. Confirming that "verification" was performed would assume that all registered entities would perform the verification on the same lists of required items. If the items are not articulated, there are no assurances that the data would be consistently derived or complete.

One commenter recommended changing the words "performing assigned work functions" to "are appropriate". The SDT believes that the use of appropriate to define specific standard provisions is too vague and subject to interpretation.

One commenter stated that the scope of requirement part 4.4 (formerly part 6.6) has been expanded above and beyond what has been directed by FERC. The SDT has taken very positive steps to meet the requirements of the FERC directives. In establishing some requirements, the only way to effectively validate that the provisions have been met is to identify the need for specific information that links the requirement to the compliance actions. There may be an increased number of these instances. The important factor is that FERC directives do not limit the detail of the required evidence. The SDT believes that the requirement and measures increase the level of security. Unauthorized, expired or mis-assigned access to BES Cyber Systems represents potential vulnerabilities that could be exploited if not addressed with these administrative requirements.

One commenter also recommended that the wording of the "annual requirement" be worded as follows, "once each calendar year of a period not to exceed 15 calendar months between verifications." The SDT has changed the requirement to read "once every 15 calendar months to incorporate the additional 3 months of previously discretionary time directly into the requirement."

One commenter believed that the word "all", referring to user accounts is too broad. Dominion suggested that the word "applicable" be added after "all" to point to those user accounts, etc that are directly associated with the requirement. The SDT has changed the requirement to read "user accounts on all applicable cyber assets" to maintain the appropriate scope of the requirement.

One commented that requirement parts 6.6 and 6.7 should be revised to allow responsible entities to perform verifications of user accounts, user account groups or user role categories and their specific associated privileges at "a timeframe that the Responsible Entity deems necessary." NextEra also suggested that this also applies to verifying "access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity

are correct…" Although there are a number of companies that would comply with the requirement according to its intent under a self-imposed timeframe, there is no way to ensure that this would be the case. The SDT feels that the annual requirement should remain in place to help ensure consistent compliance actions.

Several commenters recommended changing requirement parts 6.6 and 6.7 to remove "all" referring to reviews of user accounts, user account groups, or user role categories. They recommend replacing "all" with "BES Cyber Systems." The SDT believes that reviews should be performed only on applicable cyber assets. The requirement has been revised as follows: "that user accounts on all applicable cyber assets, user account groups, etc.

Some commenters also commented that "locations" in requirement parts 6.4 and 6.7 should be replaced with designated repositories and include a requirement to list the repositories. The SDT has reworded the requirement to read "designated storage locations for BES Cyber System Information, whether physical or electronic." It has also added a requirement to designate storage locations and a measure to provide a list of designated storage locations. This will remove incidental temporary storage on non-designated devices from the audit process.

Some commenters suggested that the language in the second measure, "A summary description of privileges associated with each group or role", be removed. The SDT believes that understanding the privileges associated with specific roles is a necessary data point for verification that the privileges for specific groups are authorized and appropriate for the work functions performed by those assigned to the groups.

Requirement Part 6.5

Many commenters suggested in some manner to move former parts 6.1, 6.4, 6.7, and 7.3 (now, collectively, parts 4.1, 4.5, and 5.3) into CIP-011. In response, the SDT has revised former parts 6.1 and 6.4 to require a process without specifying how to conduct the authorizations. The SDT notes that CIP-004-5's authorization requirements relate to individuals' access, while CIP-011-1 specifies the information protection requirements.

Some commenters expressed concerns that the measures of requirement part 4.5 (formerly part 6.7) do not need to include the phrase "the minimum necessary for performing assigned work functions." In response, one of the most important aspects of authorizations and privileges is that they be granted using a "least privilege" approach. Otherwise the possibility exists that authorizations are provided or maintained for individuals who do not need them based on expediency rather than a comprehensive review.

One commenter suggested removing the term “minimum” from the third measure of Part 4.5 (formerly part 6.7) since it was removed from the requirement. The SDT agrees with this suggestion and has revised the measure accordingly.

One commenter recommended that the word “privileges” be added to part 4.5 (formerly Part 6.7) after the word “access.” The proposed wording of the requirement would be “verify at least once per calendar year, but not to exceed 15 calendar months between verifications, that access privileges to the designated physical and electronic repositories where BES Cyber System Information is stored by the Responsible Entity are correct and those that the Responsible Entity determines necessary for performing assigned work functions." The SDT concurs with this addition since it adds clarity to the requirement. It has added “privileges” to the requirement. In a related recommendation, another commenter suggested the word “privileges” be removed from the measure since it is not in the Part 4.5. Adding the word privileges as discussed above will alleviate those concerns.

Some commenters recommended removing requirement parts 4.4 and 4.5 (formerly parts 6.6 and 6.7) because they are too prescriptive in their attempt to accomplish requirement part 4.3 (formerly part 6.5). The SDT believes that verification of requirement part 4.3 hinges upon the existence and validation of requirements listed in 4.4 and 4.5.

One commenter also questioned whether a listing of authorizations is the same as a list of those with access. Authorizations provide a type of eligibility for access. A list of those with access may include someone without that authorization and a potential security issue. That is why the reviews of authorizations, access and privileges are critical to compliance with the standards requirements.

Requirement R5 (Formerly R7) Applicability Section

A few commenters suggested that the applicability of revocation requirements in CIP-004-5 R5 (formerly R7) for interactive remote access should be modified to exclude dial-up connectivity. In response, the dial-up connectivity reference is removed from CIP-004-5 in its entirety.

Commenters also recommended that applicability to “Medium Impact BES Cyber Systems” be limited to those with “External Routable Connectivity” to maintain consistence with other cyber systems/assets currently covered by similar requirements in CIP-004. External Routable Connectivity has already been added to the applicability section for CIP-004.

Requirement R5 (Formerly R7) General Comments

Several commenters expressed concern on requirement part 5.2 (formerly part 7.2) for transfers and reassignments. They believe that the timing of access removal should be based on the determination of when access is no longer necessary, rather than limiting it to a specific time frame related to the transfer or reassignment date. The SDT has revised part 5.2 (formerly part 7.2 as follows: "For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access".

For requirement part 5.1 (formerly part 7.1), a commenter suggested that part of the FERC Order 706 be more clearly reflected in the requirements. Specifically they would like documentation in the requirement that highlights FERC's statement that exceptions to revocation policy are allowed as long as they are properly documented for audit purposes. Paragraph 462 of Order 706 states that, "revocation should be immediate upon the employee's notification of any personnel action requiring revocation of access. However, the ERO may define what circumstances justify an exception that is other than immediate and determine what is the fastest revocation possible." In response, this is not a SDT issue. Creating exceptions for directives in a FERC Order is a separate process undertaken by the ERO. In any event, it is not simply a documentation requirement. Circumstances warranting exceptions have to be identified and then approved. This of course is done against a backdrop of "immediate" revocation stated in the order.

A few recommended that the requirement for revocation based on the "next calendar day" should be changed to "next business day." Another commenter proposed that "next calendar day" be replaced by "within 24 hours." The SDT believes that next business day does not fall under the intent of the FERC Order Directives. Next business day if a weekend or holiday period is in progress could extend the revocation process for two or three additional days. "Within 24 hours" is actually less time than is allowed by the "end of the next calendar day." For the purposes of these comment responses, the SDT feels that next calendar day best meets the FERC Order directive and provides better security than next business day.

Some commenters also expressed concern that the 24 hour revocation requirements may not realistic given numerous and diverse HR and IT processes throughout the industry. Essentially they, along with one other commenter, advocated returning to a framework that allows different time frames for different types of termination actions. The SDT has revised the requirement to state that there must be a process to initiate removal of an individual's ability for unescorted physical access and interactive remote access. This is based on the premise that removal of the ability for access may be different than deletion, disabling, revocation or removal of all access rights. Considering that what is required is initiating

a process (which may allow for internal processes that serve as trigger points) at the time of the termination action and completing the process within 24 hours, the SDT believes this is a reasonable time frame.

Requirement Part 5.1 (formerly 7.1)
Commenters recommended that the criteria for termination action timeframes should include a reference to the communication of the intention to terminate to provide a type of time stamp for gauging compliance with related requirements of the standard. While the communication of a termination action is not mentioned specifically in the requirement, initiating the process required by requirement part 5.1 (formerly part 7.1) would probably include those trigger points for individual companies. This allows greater flexibility and more concise monitoring of the required timeframe.

Several commenters expressed concern with the format of the measures in Requirements R4 and R5 (formerly Requirements R6 and R7). They are concerned that the background section states that all numbered lists in the measures are all required evidence. However, the measure list states that the "evidence may include but is not limited to." The SDT has revised the measures by adding the following statement: "An example of evidence may include, but is not limited to *documentation of all of the following*: This sentence is followed by numbered measures. This is primarily a formatting issue and this revision should alleviate the discrepancy.

One commenter suggested that the requirement should include "disable or revoke all individualized domain user accounts held by the terminated staff." The SDT believes that removing unescorted physical (preventing any entry into an entity's facilities) and interactive remote access should prevent any further access by the individual after termination.

Some commenters stated that requiring access revocation within 24 hours for all types of terminations is overly burdensome. They believe the 24 hour requirement should be limited to "for cause" terminations with additional flexibility built in for other situations. Other commenters recommended that the 24 hour time frame should apply only to High Impact Assets. The SDT has revised the requirement to state that there must be a process to initiate removal of an individual's ability for unescorted physical access and interactive remote access. This is based on the premise that removal of the ability for access may be different than deletion, disabling, revocation or removal of all access rights. Considering that what is required is initiating a process (allowing for internal processes) at the time of the termination action and completing the process within 24 hours, the SDT feels this is a reasonable time frame.

A few commenters stated that requirement parts 5.1 and 5.5 (formerly parts 7.1 and 7.5) seem inconsistent regarding shared user accounts. The SDT sees no inconsistency and believes that the current requirements are clear and sufficiently differentiated. Requirement part 5.1 considers the first tier of access; unescorted physical and interactive remote electronic access. Requirement part 5.5 specifies changing passwords for shared accounts and provides a 30-day time frame for its completion.

One commenter recommended a change to part 5.1 formerly part 7.1) that changes the 24 hour requirement to the end of the next business day after the effective date and time of the termination action. The SDT believes this falls outside of the FERC Directive intent, particularly as it applies to the "next business day." The next business day could increase the access revocation time frame to well over the 24 hours currently stated in the requirement.

One commenter recommended that requirement parts 5.1 and 5.3 (formerly parts 7.1 and 7.3) be revised to include a statement on extenuating circumstances associated with the impact of completion of revocation within 24 hours. FERC has allowed "extenuating operating circumstances" which have a specific application in requirement part 5.5 (formerly part 7.5), due to the complexity and scope of the password change task. Extenuating circumstances outside of that definition are undefined and could be misconstrued as any circumstance that is perceived as an impediment to completion of the requirement. In addition, adding "extenuating circumstances" to these requirements could set a precedent for other requirements, negating the timeliness and effectiveness of underlying security intent.

One commenter suggested clarifying language to the wording of the requirement to make it clear that the 24-hour clock is related to the initiation of the termination process, not the complete termination actions themselves. The SDT has clarified that there must be a process to initiate removal of an individual's ability for access. Initiation of the process must be concurrent with a termination action. Completion of the removal is required within 24 hours of initiating the process.

One commenter believes that termination criteria should vary according to the situation. They would like the tightest timeframes reserved for terminations for cause. The SDT has maintained the 24 hour requirement for termination actions based mainly on the FERC 706 Order requirement that termination be executed immediately.

One commenter commented on a situation where a suspended individual is terminated ten days from the suspension date. While the termination action was initiated in compliance with the requirements of R5 (formerly R7), the effective date of the termination shows up in the records as 10 days prior to the action being initiated. The SDT believes that in

these situations, documentation of the suspension along with what a suspension entails regarding any network or system accesses, and a documented company statement verifying the entities suspension procedures and subsequent termination should be sufficient to provide evidence of compliance to an auditor.

Requirement Part 5.2 (formerly 7.2)
Many commenters are concerned about the 24 hour requirement for removal of access for those individuals transferred or reassigned. The SDT understands the issue with access often being required after the transfer for various lengths of time. Rather than specify numbers of days within which an entity must complete the reassignment or transfer activities, the SDT has reworded the requirement to the following: "For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access."

One commenter would like reassignments or transfers based on the notification of reassignment or transfer. Rather than specify numbers of days within which an entity must complete the reassignment or transfer activities, the SDT has reworded the requirement and proposes the following changes: "For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

Requirement Part 5.3 (formerly 7.3)
A few commenters requested clarification on physical access to BES Cyber Systems and storage requirement wording in general. The requirement specifies that the access applies to those "designated physical and electronic locations where BES Cyber System Information is stored." In the requirement the term "designated" has been added. For the measures, evidence includes workflow or sign-off forms verifying access removal to "designated" physical areas or cyber systems. The term designated removes the unintended consequence of BES Cyber System Information temporarily resident on work stations, laptops, flash drives, etc. These areas are consequently not identified as storage "locations."

Some commenters suggested replacing the words "by the end of the next calendar day" to "within 7 days" or 30 days, respectively in the requirement. The SDT believes that since access removal in requirement part 5.1 (formerly part 7.1) will in many cases, constitute removal of access to BES Cyber System Information, that this requirement should retain its

original wording. In addition, in FERC Order 706, Paragraph 386 requires that there be "prompt revocation of access to protected information." Seven or 30 days would not be considered "prompt" by FERC.

One commenter commented that "next calendar day" for removal of access to BES Cyber System Information is too short a time span. The SDT points out that FERC Order 706 dictates prompt removal of access. The phrase "next business day" for example could mean substantially longer time periods over weekends and some holiday periods.

One commenter recommended the use of the word "repository" over "locations" in the requirement. The word "location" was chosen by the SDT to ensure there was no ambiguity within the requirement. Location is considered a general area, with multiple uses and is not limited to a specific function. A "repository" on the other hand, connotes specific use…for storage of BES Cyber Security Information. The use of location will help avoid any tendency toward requiring exclusivity of purpose and preclude potential violations.

One commenter commented that locations should be changed to designated repositories. The SDT believes that specifying a designated repository is less subject to interpretation and in most cases exempts portable equipment from being identified as a "location" in the event that NERC CIP information may be temporarily resident on such equipment. The SDT has retained the term "designated locations" since a location more often connotes multiple purposes. In contrast a repository, similar to location by definition, still carries connotations of a specified area, limited to a specific function. "Location" provides flexibility and designating locations removes incidental temporary storage on non-designated devices from the audit process.

Requirement Part 5.4 (formerly 7.4)

Some commenters would like to expand the applicability of requirement part 7.4 to include Medium Impact BES Cyber Systems. The SDT has carefully weighed the applicability of requirement parts throughout the family of Version 5 CIP standards, and, on balance, it believes that the levels of protection for Medium Impact BES Cyber Systems in other requirement parts throughout CIP-004-5 provide an appropriate balance in applying impact-based protections that are graduated between High Impact BES Cyber Systems and Medium Impact Cyber Systems.

One commenter suggested a revision for recovery of all information copied from repositories. The SDT notes that the requirements set out the requirements that must be part of the required processes. The SDT believes that the information protections in CIP-011-1 and the access requirements in CIP-004-5 adequately serve the purpose of protecting BES Cyber Systems while allowing sufficient flexibility to entities in implementing their processes or programs.

A few commenters recommended changing “Requirement parts 5.1 and 5.3 (formerly parts 7.1 and R7.3)” to “Requirement R5, Parts 5.1 and 5.3 (formerly R7 Parts 7.1 and 7.3.”)They also recommended changing the word “removal” to “revoke” for consistency with the requirement. Another commenter also suggested changing “revoke” to either remove or disable. In some systems removal results in removing all corresponding records which makes it hard to provide the proper records to the auditor. The SDT has retained “removal” in part 5.1 along with a clarification which is provided in the requirement language. The SDT retained the term “revoked” in part 5.3 to conform to the overall R5 Requirement.

One commented that the phrase "revoke individual users accounts on BES Cyber Assets" should be changed to "revoke individual access to BES Cyber Assets." The commenter believes that this is an important distinction because most field BES Cyber Assets do not have individual user accounts. In the utility field environment many brands and models of devices are being used. For those that do have individual user account capability, they are often not used because most BES Cyber Assets cannot be centrally managed. Since the process of revoking access privileges on each device can take up to a year or longer because it requires a site visit to each asset and for system with a significant number of assets which also covers a large geographic area that effort in combination with the necessary equipment outage to make the change introduces new reliability risks to the BES. It is more common for the commenter’s field organizations to place other access control devices in front of such field devices. These other devices can be centrally managed. So access is controlled to the device rather that by the device itself. Field Example: Protective Relays - Most do not have individual user accounts. Many also do not have the capability to allow central access control management. Because they don't have user accounts the only way to revoke access on the devices is to change the passwords for all access levels. This means logging on to many hundreds to possibly thousands of relays to change passwords. Because access to the relays to change passwords opens the relay at the change level, it presents an increased risk to the BES because it requires a physical equipment outage to make the change resulting in many more outages impacting potentially the state of the BES and once access is granted, one can change any type of setting on the relay. It certainly could not be accomplished in 30 days. Access can be revoked to these assets by revoking the Central Electronic Access Privileges that allow access through the access control devices to the assets. This coupled with physical access revocation (both of which can be centrally managed) provides complete revocation of access to the assets. This can be accomplished a very short time.

One comment suggested that in CIP-004 R5.4 (formerly R7.4): “For Termination actions, revoke the individuals user accounts on BES Cyber Assets...” to, for termination actions, revoke the individuals access to BES Cyber Assets...” The SDT has modified part 5.4 to read, “for termination actions, revoke the access to individual’s user accounts (unless already

revoked in accordance with requirement parts 5.1 or 5.3) (formerly parts 7.1 and 7.3) within 30 calendar days of the effective date of the termination action."

Some commenters disagreed with the statement that the word "revoke" in this case means to "delete" the user account from the system. We would disable the account and possibly change the account password but when you delete a Windows account you can never reclaim the original Globally Unique Identifier (GUID that Windows assigns to the unique account. Therefore, reporting, file ownership and anything relating to the GUID will have been lost and difficult to track past account activity. This may be true for other operating systems as well. If disabling their domain accounts and physical access effectively terminates access, do we still need the urgency of 24 hrs? I understand the logic behind this but would rather see this as a 30 day requirement. The SDT has used the term revoke to essentially make an account "inactive". It does not delete the account. Also, requirement part 5.4 has been modified in the "Applicable Systems" section. It now includes only "High Impact BES Cyber Systems and Electronic Access Control or Monitoring Systems that are associated with High Impact BES Cyber Systems." Further, the requirement allows revocation of individual's user accounts within 30 days of the effective date of the termination action.

One commenter questioned that since there is no requirement for revocation of balance of access in 5.4 (formerly part 7.4) for Medium Impact BES Cyber Systems, is there a particular timeline required? The commenter recommended that a timeline be developed that provides auditable records for removing balance of access. In response, the SDT notes that requirement part 5.4 in the applicable systems does not include Medium Impact BES Cyber Systems. Under those circumstances the audit process would not be considering Medium Impact balance of access.

Requirement Part 7.5

One commenter points out that requirement part 5.5 (formerly part 7.5) only accounts for the 30 days within the requirement and not the 10 days after "extenuating operating circumstances". The SDT has provided measure in part 5.5 to cover that previous omission.

One commenter suggested that the second bullet of the example evidence for requirement part 5.5 (formerly part 7.5) should be clarified that password reset is only required if the individual being transferred no longer needs such access in the new position or role. In response, the SDT has modified the measures to clarify that password resets must be completed within 30 days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

One commenter recommended that requirement part 5.5 (formerly part 7.5) be revised to include both terminations and reassignments or transfers. The SDT has added part 5.5 to the requirement to cover the reassignments and transfers.

One commenter suggested that the quarterly review should be converted to a quarterly “cleanup” of individual user accounts and not be considered a violation, and the SDT notes that that a cleanup could certainly a way of identifying, assessing, and correcting any deficiencies, which now modifies “implement” in the main requirement (see summary response to common issues at the beginning of this document), and for that reason, the required performance of the requirement remains a review.

One commented that if an entity can determine and document that extenuating operating circumstances require a longer time period for changing passwords; it should also apply to allow the Responsible Entity to determine and document that extenuating operating circumstances that can require a longer time period for revocation of access privileges. The SDT believes that since revoking physical and interactive remote (tier 1) access is typically a centralized and relatively uncomplicated process, that the time frames for completion are adequate. In addition, the FERC Order 706 requires “immediate” revocation of access. Providing a conditional caveat “for extenuating operating circumstances would in all probability meet with FERC resistance and result both in subjective application and interpretation.

One commenter questioned the need to modify passwords for shared user accounts if there is no corresponding requirement to disable individual accounts for the user who was reassigned or transferred. Additionally, as passwords are not a required authentication mechanism, we recommend that this requirement be modified to "change any shared authentication factors that are known." The SDT has revised requirement part 5.5 (formerly part 7.5) to accommodate reassignments and transfers as well as termination actions. Requirement part 5.5 reads, “For reassignments, or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.”

QUESTION B12 – CIP-005-5, R1:

If you disagree with the changes made in CIP-005-5, Requirement R1 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to CIP-005-5 Requirement R1.

General Comments

One commenter suggested that the communications links between ESP's should be included and that all the External Routable Connectivity exclusions should be eliminated. In response, all BES Cyber Systems have been included within the scope of Version 5 and the blanket exemption filter in CIP-002-5 has been eliminated. The ERC filter is now used on individual requirements where routable connectivity is either needed to meet the intent of the requirement or in general there is insufficient risk from other forms of communication to enforce a mandatory and auditable requirement upon every instance in every registered entity. Communication links have been excluded from this body of standards from the beginning as it is a cyber asset focused standard, and the vast majority of cyber assets used in communications between ESP's are not within the control of the registered entities but are leased services from telecommunication providers.

A few commenters requested clarity around the inclusion of serial devices and another commenter also requested specific clarification concerning the extension of ESPs over large areas via serial communications along with a request for clarification of 'direct serial' used in the guidance. In response, the SDT has focused on the communications requirements of the standards for the highest risk forms of communication – routable protocol networks and public switched telephone network (PSTN) accessible dial-up connections. It is a vital point that all BES Cyber Assets, including all serial devices, are included in the standards and are subject to all the requirements in CIP-003-5 to CIP-011-1 except those where they are specifically excluded. CIP-005-5, however, is focused on those two higher risk forms of connectivity and do not have mandatory requirements on serial, non dial-up forms of communication. As to the extension of ESPs over large areas via serial communications, the SDT notes that ESPs are for routable communication only and the SDT does not envision single BES Cyber Systems being defined in such a way that large geographical areas are involved. It is envisioned that a BES Cyber System would encompass cyber assets at a single site only – larger systems would be broken

at least into smaller systems by site. For example, a registered entity would not define all the components of an EMS including all field Remote Terminal Units (RTUs) as a single BES Cyber System. The components of that system at each location could be grouped together as the BES Cyber System for that location. Registered entities have great flexibility in their declaration of a BES Cyber System, but need to take into account ESPs and PSPs as well as all other applicable requirements as they do so. In response to the 'direct serial', that is used in the guidance as a term that refers to serial communications that is not routable protocol or dial-up in nature.

One commenter stated that clarity is needed concerning how wireless networks are impacted by CIP-005-5. In response, the SDT notes that these standards are at a higher and logical level and stay above the transport level. The SDT concentrated on protecting the BES Cyber Systems regardless of the physical transport in order to state the goal and also to future-proof the standards against an ever increasing variety of transports. Adequately addressing more detailed technical aspects would require standards per transport. However, the SDT does note that the radio/access point of a wireless network should be considered by the Responsible Entity to see if it should be included as an EAP.

Introduction Section

There was a comment that in the introduction section concerning exemptions (4.2.4) there is a reference to CIP-002-5 that should be CIP-005-5. In response, the SDT has made the change.

Background Section

One comment stated that the applicability of the background section does not address High Impact BES Cyber Systems with External Routable Connectivity and this is used in the standard. In response, the SDT agrees and has added the appropriate language which reads, "**High Impact Protected Cyber Systems with External Routable Connectivity** – Only applies to High Impact Protected Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the Protected Cyber System that cannot be directly accessed through External Routable Connectivity."

One comment read that Medium Impact BES Cyber Systems at Control Centers should be "associated with" instead of "located at". In response, the phrase 'located at' is used to appropriately limit the scope as the case could be made that

every Cyber Asset is ultimately 'associated with' a control center and could inappropriately identify every Cyber Asset as high impact.

One commenter stated that the section concerning Medium Impact BES Cyber Systems with External Routable Connectivity have the last sentence be deleted as it requires not treating the cyber system as one system, but as individual Cyber Assets. In response, there are several requirements (CIP-007-5 in particular) that do apply at the individual cyber asset level within a system and this sentence clarifies that for those requirements only those cyber assets within a system that have external routable connectivity are in scope if the requirement has this applicability.

Requirement Part 1.1

Many commenters commented that the applicability should include the ERC filter and thus remove the applicability language from the requirement itself and also make it parallel with R1.2, potentially even combining R1.1 and R1.2 into one. In response, the two requirements are purposely not parallel. R1.1 requires an ESP (a ***logical*** border) around every routable protocol network that contains a BES Cyber System even if it is an isolated network and has no external connectivity. The logical border (ESP) is used then as a boundary to define the 'associated Protected Cyber Assets' and raise the impact level of the included Cyber Assets to the 'high water mark' of the highest impact level system in the ESP. R1.2 is an additional requirement for those networks that have external routable connectivity to protect that external connectivity. In essence, Requirement R1.1 is the "identify your associated PCA's and adjust your impact levels" requirement. R1.2 is where external routable connectivity comes in and the logical border becomes more physical with the requirement of Electronic Access Points (EAPs).

Many commenters responded that the applicability needs to be removed from the requirement and the measure. Others commented that Associated Protected Cyber Assets should be included in the applicability as well. In response, the SDT has added the Associated Protected Cyber Assets to the applicable systems column.

There was one comment which stated that documentation on ESP's on isolated networks provides no reliability benefits. In response, the standards are concerned with all threat vectors, not just those originating from external networks. Portable media and insiders are two of many other threat vectors that can reach isolated networks. The SDT feels that knowing what all other network neighbors are on even isolated routable protocol networks containing a BES Cyber

System (the 'Associated Protected Cyber Assets') does have a reliability benefit. The logical border concept of the ESP also defines a 'trust zone' where all Cyber Assets sharing a network with a BES Cyber System need to be protected to equal levels, even on isolated networks.

One commenter stated that the measure should allow for documentation at the BES Cyber System level rather than the individual component level. In response, the SDT agrees and has made a change to the measure to allow documentation at either level.

One commenter requested clarification on whether ESPs are required for EACMs and PACMs. In response, the SDT clarifies that ESPs are not required on EACMs and notes that EAPs are EACMs and the standard avoids recursive effect of requiring ESPs around the cyber assets on the ESP. As for PACMs, the SDT notes that without an ability to make a distinction between "field-devices" (i.e. door readers, etc.) and "central servers", requiring ESPs would be problematic. The intent for protecting PACS is primarily through the CIP-007 requirements for authorization, access control, and logging and monitoring for these systems.

Requirement Part 1.2

One comment stated that the phrase "through the ESP" was redundant in light of the definition of External Routable Connectivity and should be deleted which would also eliminate the use of "through" twice in the existing requirement. In response, the SDT agrees and has deleted the phrase.

One commenter wrote that the measures should include a process to verify that all EAP's are identified as providing a network diagram is not sufficient. In response, the SDT notes that the requirement does not call for a verification process thus the measure should not imply that is a requirement. The requirement states the desired end goal and the entity is responsible for providing sufficient evidence. Network diagrams that depict all external routable communication paths with identified EAP's are listed as one possible example.

Several commenters stated that the applicability should be 'Associated PCA's with ERC'. In response, the SDT agrees and notes that the PCA for this requirement part are associated with high and medium impact BES Cyber Systems with External Routable Connectivity.

Requirement Part 1.3

A few commenters expressed concerns regarding the monitoring and documentation of all outbound traffic. Inbound only monitoring on PSPs is sufficient and suggest dropping the outbound on ESPs. In response, the SDT believes this is an essential element in combating today's electronic attacks and reiterates the following from the included guidance: "The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked."

Several commenters suggested that the applicability should be "Medium Impact BCS with ERC". In response, the SDT notes that the applicability is to EAPs that are associated with High or Medium Impact BES Cyber Systems specifically. If these applicable systems have no External Routable Connectivity, then they will have no EAPs and the requirement therefore does not apply to those systems.

One commenter suggested that the word "rationale" should be changed to "reason." In response, the SDT agrees as this makes the requirement language the same as that used in the measures and in the change rationale. The change has been made.

One commenter noted that tracking the rationale for 60000 ports is burdensome and asked that this be changed to allow for this on a class basis or 'criteria'. In response, the SDT notes the requirement does not require that all 65535 ports be documented as this is a 'deny by default' requirement and only the remaining open ports (those that 'grant access') should be documented. A necessary step in preventing rogue communications to or from a BES Cyber System is to know what the normal communications include and why they are needed.

Requirement Part 1.4

Multiple commenters stated that R1.4 is essentially the same as CIP-007-5 R5.1 and suggest that dial-up be added to CIP-007-5 R5.1 and R1.4 deleted to avoid potential double jeopardy. In response, the SDT notes that CIP-007 R5.1 is specific to user access, while CIP-005-5 R1.4 applies to any access including machine to machine. CIP-005 concerns the security of the 'network' level and requires that there be some form of authentication before a 'network' connection is established to the BES Cyber System. In essence, there should be some form of EAP-like functionality on dialups. Once a connection is made, then CIP-007 applies as we've moved from the 'network' level security to device level security and any user access has to be authenticated at the device.

One comment suggested that R1.4 should be deleted as it is included in R2. In response, the SDT notes that this requirement requires some form of authentication for all dialup connectivity regardless of whether it is machine or user based, while R2 only applies to 'Interactive Remote Access' which is user-based. The intent of R1.4 is that no BES Cyber System, which by definition can have a 15 minute impact on BES reliability, should be directly reachable by simply dialing a phone number, regardless of how it is intended to be used. Therefore R2 contains requirements that are in addition to R1.4 when the intent of the connection is user based Interactive Remote Access.

Several commenters asked if an entity has no dialup capability to applicable systems, are they required to have processes that would authenticate this access? The commenters suggested that the qualifier 'if applicable' be added. In response, the SDT notes the applicability column states that it only applies to systems "with dial-up connectivity" and therefore if an entity has no such systems, there are no systems to which this requirement applies and no process is required. The complete applicability of all requirements throughout the standards is contained within the applicability column and therefore every requirement in the standards has an implied 'if or where applicable' clause.

One commenter suggested that the "where technically feasible" clause should be changed to 'within system capabilities.' In response, the SDT notes that BES Cyber Systems, which by definition can have a 15 minute impact on BES reliability, should not be directly reachable by simply dialing a phone number. If that is not an inherent capability of the system,

then the SDT feels it necessary to add additional equipment with this capability to the system or file for a TFE so that a mitigation plan can be documented to handle the vulnerability.

One commenter suggested that 'where technically feasible' should be deleted. In response, the SDT notes the phrase is an indication of where TFE's may even be requested if the requirement cannot be met on a particular system. Since the SDT is not aware of all situations, it is felt that if an entity cannot meet this requirement on a system that they should be allowed to request a TFE and document a mitigation plan if the TFE is granted.

One commenter suggested that "Associated PCA's" should be added to the applicability. In response, the SDT agrees that any dialup connectivity to any system or Cyber Asset within the ESP, which by definition means the Cyber Asset is also routably connected to a BES Cyber System, should be included. The suggested change has been made.

Multiple commenters suggested that the term 'dial-up connectivity' should be defined to avoid future confusion and should include the notion of access from the PSTN. In response, the SDT is adding a proposed NERC Glossary definition of Dial-up Connectivity.

Requirement Part 1.5

Numerous commenters suggested that the measure only specifies IDS technology and should be made more generic to match the requirement. In response, the SDT agrees and has changed the measure to match the requirement, using IDS as one example.

There were multiple comments that detecting 'malicious' communications requires knowing the sender's intent. Malicious traffic may indeed appear normal. In response, the SDT is adding the phrase "known or suspected" to clarify that the intent is not to detect 100% of all malicious communications, but that communication that has attributes of known or suspected malicious communications.

Multiple commenters asked for clarity as to where the malicious communications inspection should occur and does the direction of the traffic matter. Another commenter stated that only one IDS could be utilized between all ESP's and the

Internet and one per EAP should not be required. In response, the SDT notes the applicability is set at the EAP level and therefore every EAP at Control Centers needs to be covered by the entity's method for detecting malicious communications. The specific architecture and placement is not prescribed. The SDT notes that since this applies to Control Centers, both inbound and outbound traffic should be subject to the detection and has added clarifying language to the standard. For example, if a BES Cyber System in a Control Center begins sending known malicious packets or attempting to communicate with known malicious 'command and control' hosts on the Internet that would warrant detection here and alerting through CIP-007 R4.

Several commenters suggested that the applicability should change to "Electronic Access Points associated with ESPs at High Impact Sites and Electronic Access Points associated with ESPs at Medium Impact Control Centers" as the current phrasing would suggest the need to implement external routable connectivity in otherwise isolated networks. In response, the SDT notes that the requirement is applicable to EAPs and EAPs are only required where External Routable Connectivity is present, therefore isolated networks would not have EAPs and the requirement would not be applicable. However, isolated networks do have ESPs, so bringing the term ESP into the applicability may further confuse the issue.

There were several comments that raised a concern that the requirement is subjective and may not be feasible for encrypted traffic. In response, the SDT has written this requirement in response to FERC Order 706 and the directive to have two or more security measures at each ESP. The Order further clarifies that this is not simply redundant firewalls, but two separate security measures. The SDT has already reduced the subjectivity somewhat from 'two security measures' to 'detect malicious communications'. In today's technology, this would in most cases (but not all) involve the implementation of an Intrusion Detection System, but the SDT does not want to specify products or toolsets within the CIP standards to help future-proof the requirements. If a better toolset is available in the future that is not called "IDS" we would not want these standards to preclude the use of it, so we've deliberately used admittedly more subjective language ("a method for detecting…") in this case. As to the feasibility with encrypted communications, it is true that the methods will be 'blind' to the content of encrypted sessions but it is left to the entities to determine the relative value between maintaining true end-to-end encryption over terminating the encryption and inspecting the traffic at the ESP. The SDT notes that if the traffic is 'Interactive Remote Access', the encryption must terminate per R2 at the Intermediate Device which cannot reside within the ESP.

In the measures section, there were multiple comments to change the word “and” to “or” and to use bullets. In response, the SDT feels a generic paragraph is easier for clarity than bullets. The measure reads, “Examples of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.”

One commenter suggested that the phrase “where technically feasible” should be added to the requirement. In response, the SDT notes that this requirement is limited to Control Center environments. These are the highest risk locations and the SDT feels that in these instances some form of malicious communications detection (IDS) is always possible on routable protocol communications (EAP’s are required only on routable protocol communications).

One commenter stated that External Routable Connectivity should be added to the applicability. In response, the SDT notes that the applicability is to EAP’s which are only required for routable communication points.

Several commenters stated that detection is only one half of the issue and the standard needs to require addressing or mitigating the detected threat. In response, the SDT notes that EAP’s are EACM’s and are thus covered by CIP-007 R4’s Security Event Monitoring requirements and tie into CIP-008. Therefore the SDT feels that the ‘other half’ of the issue is covered by other standards. Xcel suggests that Intrusion Prevention Systems should be included instead of detection systems. In response, the SDT notes that in a control systems environment, the impact of preventing communications that may be the result of false positives may be greater than allowing the communication. Therefore we do not feel it necessary to require in a mandatory and enforceable manner that all suspected malicious communications should be prevented in all situations. That decision is best made by the Responsible Entity based on the specific situation and potential impacts.

One commenter suggested that the Medium Impact should be removed from the applicability as many of the Cyber Assets can’t perform this requirement. In response, the SDT notes that while many Cyber Assets in substations or plants (field locations) may not be able to perform this requirement, the Medium Impact systems are limited to those in Control Centers where the SDT feels the most risk is present and control center systems typically have the most capability to meet this requirement.

Guidance Section

One commenter stated that the guidance for R1 discusses the limitations on the ability of a BES Cyber System to communicate through the EAP and an apparent conflict with the requirement for an intermediate system (jump host) that essentially denies the ability of the Cyber Asset within the ESP to communicate with any other system outside of the ESP. In response, the SDT notes that the Intermediate Device is required only for human-machine interactive login sessions ("Interactive Remote Access") while the Requirement R1 is concerned with machine to machine sessions as well, which do not require an Intermediate Device. Requirement R2 builds upon Requirement R1.4 when the session meets the definition of Interactive Remote Access.

VRF/VSL Section

There was a comment on how the math is done on the VSL for Requirement R1. The SDT has modified the VSL for R1 to remove percentage calculations. We agree the percentage would be difficult to determine in most implementations. Furthermore, the FERC VSL Order addressing CIP Standards discourages specifying failure to document processes as a lower VSL than failure to implement.

There was a comment that suggested the VSL be medium for high impact and lower for medium impact. In response, the VRF by itself does not account for violations from different types of systems, but the SDT expects the impact level of the BES Cyber System to factor into the assessment of penalties.

One commenter suggested the ROP will need to change with changes to TFEs. Although the SDT does not draft Rules of Procedure changes, the SDT expects that this will be a part of the implementation of Version 5.

One commenter recommended modifying the first "Lower" to state: "failed to implement one or more documented processes" to be consistent with the language in Requirement R2. Furthermore, the commenter recommended moving this VSL to the "Severe" category. The lower VSL is intended for the situation where the entity has only failed to document the process(es). Where the entity has failed to implement one of the technology-based solutions listed in the table, those would fall in the moderate to severe categories based on number of technology-based solutions not implemented. The Lower VSL has been revised to clarify this further. Also by the FERC Guidelines for CIP standards, the failure to document processes should be the same level as the failure to implement a process. We have corrected the VSLs for R2.

One commenter recommended that the VSL for CIP-005-5 R2 VSLs be revised to address the approach to detect flaws; correct detected flaws expeditiously. Upon review of the approach to implement preventive, detective, and corrective controls, CIP-005-5 R2 was not identified as a requirement that would be appropriate for this approach. Therefore, the VSL was not modified as requested.

One commenter agreed that the VRF should be medium for the high impact BES Cyber Systems but that the VRF should be lower for the medium impact BES Cyber Systems. In response, VRFs are assigned for an entire requirement and are not assigned to the underlying sub-requirements or parts.

QUESTION B13 – CIP-005-5, R2:

If you disagree with the changes made in CIP-005-5, Requirement R2 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the SDT has made significant changes to CIP-005-5 Requirement R2. The explanations below describe the changes made based on stakeholder comments – the SDT made other minor edits for improved clarity.

TFE Relevance

In response to concerns that the phrase "where technically feasible" should be removed to eliminate reference of maintaining the TFE process, the SDT notes that TFEs will continue to be used in appropriate requirements unless and until such time that the NERC ROP is modified to address exceptional circumstances. The SDT has reviewed each use of a TFE throughout the CIP Version 5 standards very carefully and specifically, and in each instance where that phrase is used, the SDT understands that there may be circumstances where it could be necessary for an entity.

In response to multiple comments that the applicability of TFEs is not clear within the TFE language included in the overall Requirement language, the SDT has moved the TFE language to the table elements.

Applicability

Several comments stated that instances of Medium Impact BES Cyber Systems should be changed to "Medium Impact BES Cyber Systems with External Routable Connectivity". This is a valid concern, and in response, the SDT has added the language to the applicability section of the table.

There was also a comment that the requirement should apply to Physical Access Control Systems and systems serving as ESP Access Points. In response, the SDT believes that since these systems generally do not reside within the ESP of a BES Cyber Asset, it would not be appropriate to apply these Requirements to those Cyber Asset types.

Requirement Part 2.1: Intermediate Device

There was a comment requesting that the reference to Intermediate Device be removed from the requirement. In response, the SDT notes that the Intermediate Device is a defined term that is only used within this one requirement. The device functionality is necessary to ensure that proper protections are put in place for Interactive Remote Access

sessions. The use of Intermediate Devices allow the client machine to exchange data to a Cyber Asset within an ESP without making direct communication and opening the Cyber Asset to vulnerabilities of the client machine.

Several commenters requested improvements to the language in requirement part 2.1 to clarify that a Cyber Asset cannot initiate Interactive Remote Access. In response, the SDT has clarified the language to address this concern by specifying use of an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset. However, the language was not modified to address the person using Interactive Remote Access since the requirement is intended to provide protection from malicious software and communications.

Commenters requested clarification on the location of an Intermediate Device and whether an Intermediate Device can also be an EAP. In response, the SDT notes that the definition of Intermediate Device has only one restriction on the location of the Intermediate Device and that is that the Intermediate Device must not reside in an ESP. Other requirements of the Intermediate Device remain flexible to allow the entity to implement a solution that best meets their needs.

Requirement Part 2.2: Encryption

Several commenters requested that the information regarding the purpose of encryption be removed and added to guidance. The use of "in order to protect the confidentiality and integrity of each Interactive Remote Access session" was intended to help clarify the encryption means that were appropriate.This language has been removed, allowing the Responsible Entity the flexibility to implement the level of encryption appropriate to their organization. Additional references regarding encryption are available in the *Guidance for Secure Interactive Remote Access* document. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

Several commenters requested clarification on the termination point of required encryption. The requirement states the encryption is to terminate at an Intermediate Device. The Intermediate Device may be one or more assets performing the required functions. Encryption should not be perfromed within the Electronic Security Perimeter due to the negative impact on the monitoring for malicious or suspicous communications.

Requirement Part 2.3: Multi-Factor Authentication

Several commenters requested that the examples of multi-factor authorization be removed from the requirements. In response, the SDT has removed the examples from this requirement part, and the requirement part simply reads, "Require multi-factor authentication for all Interactive Remote Access sessions."

Several comments recommended more flexibility regarding the use of multi-factor authentication to allow for future technology changes without a Standards update. In response, the SDT has made this change within the measure so that it is listed as an example, but the requirement can account for future technology changes as commenters suggest.

Many comments requested clarification as to where the multi-factor authentication needs to take place. In response, the SDT has modified the Requirement to state that multi-factor authentication to the Intermediate Device is required for all Interactive Remote Access sessions. Furthermore, the definition of Intermediate Device specifies that access control be performed at the Intermediate Device. The Intermediate Device may be one or more assets performing the required functions.

QUESTION B17 – CIP-006-5:

If you disagree with the changes made to CIP-006-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, there were changes to the applicability section, the requirement parts for added clarity, and removal of unnecessary requirement parts that were documentation related.

General

The "identifies, assesses, and corrects deficiencies" language has been added to Requirement R1 and Requirement R2 since these formerly were zero defect requirements. The SDT believes this is an improvement in the compliance process.

The applicability section was renamed to applicable systems to help clarify the scope of that requirement. Also, the applicable systems entries in each table were reviewed to ensure it matched the requirement language for consistency within this standard and with the other CIP Version 5 standards.

The SDT made changes to table R1 to address concerns on the applicability of requirement parts 1.1, 1.2, and 1.3 that had layered versus exclusive applicability. The table no longer uses layered applicability to be consistent with tables in other CIP standards.

The wording of requirement parts 1.2 and 1.3 has been revised to clarify unescorted access is restricted to those authorized for such access, but escorted individuals can enter a Physical Security Perimeter (PSP).

There was consideration of combining monitoring and issuing an alarm/alert into a single table entry, but these are separate actions and needed separate table entries. Even with separate table entries, each is part of a single requirement.

The SDT has removed the 99.9% availability requirement and requirement part 3.2 to document outages for physical access control, logging, and alerting systems. The Physical Security Plan(s) should address how an entity deals with unavailability of these systems.

Requirement parts 1.4 and 1.5 have been modified to remove the reference to circumvention of a control. The new language is monitoring and issuing alarms/alerts for detected access through a physical access point into a PSP. Designation of physical access points to the PSP should be noted in the physical security plan(s).

A PACS is not required to be within a PSP. Unauthorized physical access is to be restricted. The alarm or alert is for detection of unauthorized physical access similar to the language in requirement parts 1.4 and 1.5, although a PSP is not required.

Data retention requirements that differ from the compliance data retention requirements have explicit language in the requirement table. For example, the retention requirement of 90 days for retention of physical access entry logs is specified in requirement part 1.9.

CIP 006 Requirement R1.3

Language has been added to this table, *"… two or more different physical access controls to collectively allow unescorted physical access into Physical Security Perimeters,"* to clarify that two completely independent physical access control systems are not required. For example, a card key and biometric scan using the same Physical Access Control System for validation is acceptable. Also, the SDT has chosen not to use the words "two factor authentication" since, for example, some field locations could use two separate locks. Further, the SDT believes there may be some locations, particularly for field assets, that may not permit two or more different controls, so the TFE clause remains.

CIP 006 Requirement R1.5 & R1.7

The SDT heard the concerns expressed by industry about when the 15-minute clock begins. The language in the standard has been changed to begin once detected. Also, the language referring to the Cyber Security Incident Response Plan remains as that plan could cover physical incidents related to access to cyber assets.

CIP 006 Requirement R1.8

The SDT has chosen to retain the phrase *"… through automated means or by personnel who control entry."* It confirms in the requirement that a person cannot self-log their entry into a Physical Security Perimeter and that the use of a guard is an acceptable method to log entry.

CIP-006 Requirement R2

This requirement does not state that the visitor control program(s) has to be a standalone document/program. If the entity chooses to include the required language within the Physical Security Plan, that is acceptable.

CIP 006 Requirement R2.1

The language in the parenthetical "*(individuals who are known or guests, and not authorized for unescorted physical access)"* has been removed. A "visitor" is anyone who does not have authorized unescorted physical access inside the PSP. This could include employees, contractors, service vendors, etc. The measure indicates that evidence may include documentation of the visitor control program and visitor logs. There is no reference to "proof" that a visitor was continuously escorted.

CIP-006 Requirement R2.2

The language was edited to correct the implication that a visitor exits to a PSP. Also, the measure was modified to better match with the requirement.

CIP-006 Requirement R3

The SDT considered the suggestion to remove the term "hardware" from the phrase "… locally mounted hardware and devices…" used throughout this requirement. This same phrase has been used in previous versions and is understood to exclude hardware such as door hinges, screws, etc. Also, there is new language in the background section regarding applicable systems that provides additional information on locally mounted hardware or devices.

CIP-006 Requirement R3.1

The SDT believes the key role played by the PACS and associated hardware and devices in protecting High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity warrants a 24-month testing cycle. PACS used for Medium Impact BES Cyber Systems without External Routable Connectivity do not have this requirement.

QUESTION B23 – CIP-007-5, R1, R2, R3 or R4:

If you disagree with the changes made in CIP-007-5, Requirement R1, R2, R3 or R4 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:
Based on stakeholder comments,

General Comments
One entity commented that there is a reference in the 4.2.4 exemptions section that refers to CIP-002 but should refer to CIP-007. In response, the SDT agrees and has made the change.

Several commenters commented that either all VSLs or VSLs for certain requirements should be based on percentage of cyber assets missed. Using percentages based on Cyber Assets on CIP-007-5 Requirements is problematic because Requirements do not have a singular mapping to assets. Also, it is possible for a single Cyber Asset to have multiple violations.

One commented that all Severe VSLs should state the phrase "failed to implement one or more documented." The SDT reviewed this suggestion, and "did not implement" as the SDT proposes is consistent with the SDT's intent.

Requirement R1 General Comments
One commenter suggested that the rationale section for Requirement R1 needs to include physical ports. In response, the SDT agrees and has added this to the rationale.

Several commenters stated that throughout Requirement R1, the applicability for Medium impact should be limited to Medium Impact with external routable connectivity (ERC). In response, the SDT notes that Requirement R1.1 which applies to network accessible ports is already limited to those systems with ERC. Requirement R1.2 refers to physical ports that could be used by someone physically present to inadvertently or intentionally compromise a BES Cyber System. In this case, ERC does not matter and the SDT believes the ERC exclusion should not be considered in this case.

There were a few suggestions that the High Impact systems should include the ERC filter as well. In response, the SDT notes that since Version 1 of the CIP-002 standard, lack of external routable (or dial-up) connectivity has been a blanket exemption everywhere except Control Centers, where even standalone networks were still to be considered as Critical Cyber Assets. Since High Impact in Version 5 refers to Control Centers, the SDT cannot 'go backwards' without sufficient justification, which we believe is absent.

One commenter suggested that the words "and Services" should be dropped from the title as the requirement concerns only network ports. In response, the SDT notes that ports are opened by services and that typically a port is disabled or closed by disabling the corresponding service. The requirement also allows for services that use wide ranges of dynamic ports that need to be enabled to be documented as the service name rather than a dynamic port range. Therefore the SDT believes the 'and Services' is appropriate.

Several commenters stated that the Requirement R1 measures may also include rationale as to why ports are necessary or clarify in the requirement. In response the SDT agrees and has added a specific measure for documentation of the need for all enabled ports.

Requirement Part 1.1

One commenter suggested that the phrase "ports or services" should be "ports and services". In response, the SDT notes that the use of the word "or" is intentional to allow for circumstances where a Cyber Asset uses one service that is on one port, another service that uses a range of ports, or a service that uses dynamic ports without a defined range (e.g. may use anything over 1024). The entity should be allowed to document the enabled single ports, port ranges, or in the case of the dynamic ports, the service that is enabled. Therefore the SDT feels the word "or" is appropriate.

Two commenters suggested that the sentence in the guidance concerning cyber assets that allow for no port management and therefore all open ports are deemed 'needed' should be part of the requirement. In response, the SDT agrees and has moved the sentence to the requirement.

One commenter suggested that the phrase 'where technically feasible' should be replaced with 'within device capabilities'. In response, the SDT notes that devices that do not allow for port management will have their ports determined as 'needed' thus the TFE will be seldom used. However, the SDT wanted to allow for entities to request a TFE for any special cases.

One commenter suggested that the requirement should consider more than listening ports but should also include unexpected connected ports making outbound connections. In response, the SDT notes that this risk is covered at one level by CIP-005's new outbound rule requirement. The SDT also notes that this requirement requires evidence of a known port configuration for the cyber asset and it is unclear how an entity could perform this for 'unexpected' ports.

Several commenters asked for clarification as to how "associated PCA's" applies and is not an independent set of individual assets. In response, the SDT notes that most of CIP-007, and Requirement R1 in particular, must be implemented at an individual cyber asset level and the requirement thus starts with 'For applicable Cyber Assets'. Ports and services are enabled or disabled on individual Cyber Assets and most of CIP-007 can't be done at a 'system' level but at a Cyber Asset level. For example, if an entity does not need telnet service, then the only way to prove that it has been disabled is on an individual Cyber Asset basis – ports and services are by nature not implemented on a 'group' of Cyber Assets but on individual Cyber Assets.

FMPA and LCEC commented that the SDT should add the phrase "that initiate or receive network communications" after the word "services" or delete services and let ports handle it. In response, the SDT notes that the services is part of "port ranges or services" and are two levels at which the entity can document the enabled logical network accessible ports. This was added primarily to handle dynamic ports. Some systems will use a particular dynamic port out of a small range of ports and documenting that range is acceptable. Other services may pick a dynamic port out of all the high ports (any port between 1024 and 65535 e.g. RPC) and the SDT's intent is to allow for documenting the need at the service name level.

Some commenters suggested that clarification that the Responsible Entity determines the need of port should be included. In response, the SDT agrees and has added clarifying language.

One commenter suggested that the phrase "enable only logical network accessible ports needed" should be "enable only required logical network accessible ports." In response, the SDT notes that the intent is to document the business or technical justification for all open ports. In previous drafts, numerous comments were received to change the word "justification" to "need", which was accepted by the SDT. The SDT also notes there is a difference in "required" and "needed" and thinks "needed" is a more appropriate term due to instances where a Cyber Asset may be fully able to perform its basic function without the port enabled (thus the port is not technically "required"), but the port is "needed" for other purposes. Similarly, KCPL commented that the "needed" should be changed to "approved" for clarity. In

response, the SDT notes that these ports are part of the tracked baseline configuration in CIP-010 and approvals occur there. The SDT has therefore not brought in the approval process into CIP-007.

One commenter suggested commented that 'listening' should be replaced with 'enabled'. In response, the SDT believes the term 'listening' is more descriptive as the intended scope is those ports that can actually be reached from the network. A port can be 'enabled' at one level (a config file), but blocked by other means lower in the OS (e.g. TCP_Wrappers) such that it is not actually 'listening'. The end goal is blocking accessibility from the network to unneeded ports and the SDT believes 'listening' better captures that goal.

One commenter suggested that a fourth bullet should be added to the measures to address CIP-005-4 R2.2: Listing of access points to the ESPs, including configuration of ports and services, individually or by specified grouping. In response, the SDT agrees that EAP's should be highlighted and has added this to the first bullet point.

One commenter suggested that the measure should add the phrase "or class of Cyber assets" to the second bullet. In response, the SDT agrees and has added the phrase "individually or by group" to the bullet point.

One commenter suggested that the first bullet under the measures should be deleted as it doesn't meet the requirement. In response, the SDT agrees that a simple listing of port need is not sufficient to meet the requirement and has replaced that measure with the phrase "Documentation of the need for all enabled ports individually or by group".

One commenter suggested that the list of listening ports could be a source of double jeopardy with CIP-010's baseline configuration requirements. In response, the SDT notes that the requirement is concerned only with the enabling of only needed ports irrespective of any documentation. The list of enabled ports is a requirement in the baseline configuration requirement in CIP-010. The SDT believes that failing to maintain the baseline configuration and failing to actually go to a Cyber Asset and disable unneeded ports are two different requirement violations. The measures for this requirement refer to listings of ports as evidence, but that evidence could be the same evidence required for CIP-010. Being able to utilize a single piece of evidence for proof of compliance with two different requirements is not double jeopardy.

There was a commenter who suggested that instead of the phrase 'class of cyber asset' the language from CIP-010 should be used. Also, the requirements should address justification of enabled ports. In response, the SDT agrees and notes that justification is addressed by the phrase 'needed by the Responsible Entity' and the measure has been changed to

now call for documentation of the need for all enabled ports. The SDT also agrees with the 'class of cyber asset' comment and has incorporated the language 'individually or by group' from CIP-010 as suggested.

One commenter suggested that the reference to CIP-005-5 R1 to protect the network in the guidance should be deleted. In response, the SDT agrees and has deleted the language, leaving only the clarification that blocking ports at the ESP does not substitute for the device level requirement.

One commenter suggested that the guidance should allow for disabling ports 'inline in a non-bypassable manner'. In response, the SDT agreed with this in the draft 1 comment phase and made that change between drafts 1 and 2.

Requirement Part 1.2

There was a comment that the text should be revised to begin with the phrase "Have methods to protect against..." since the VSL is for not having methods. In response, the SDT notes that the overall Requirement R1 is to "implement documented processes" and changing this to have methods would add another level of abstraction such that the overall requirement would be "implement documented processes to have methods to protect."

A commenter suggested that this requirement should be replaced with a 'implement a policy' type requirement. In response, the SDT does not believe that a policy only requirement would meet the FERC directive in Docket No. RD10-3-000 of March 18, 2010, which is the genesis of this requirement.

Several commenters suggested that signage is a weak control that does not provide adequate protection. In response, the SDT notes that signage was never meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. The industry has made several comments as to the other preventative and detective measures that are required before physical access to a physical port is ever achieved. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who plugs his infected smart phone into an operator console USB port "just to charge the battery".

Several commenters stated that this requirement needs further justification for its existence. In response, the SDT notes that this requirement was added to address FERC's Docket No. RD10-3-000 of March 18, 2010 which states, "However, like NERC, we are concerned that neither CIP-007-2 in particular, nor the CIP reliability standards in general, adequately address technical opportunities to mitigate risks associated with unused physical ports. The practice of disabling or otherwise securing unused physical ports is a basic and integral component of sound defense-in-depth cyber security practices, yet it is absent from the current reliability standards. The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP reliability standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."

One commenter stated that entities may not be able to block physical ports based on usage using the example of unplugging a USB keyboard or mouse and using a thumb drive in that enabled port. In response, the SDT notes the requirement is to "protect against the use" and purposefully does not use the verb "prevent" in recognition that the control is not effective in prevention in many cases as the industry has pointed out. The intent of the requirement is not to be a 100% preventative control, but is a last measure in a defense in depth layered control environment to make personnel think before attaching to a BES Cyber System in the highest risk areas.

There was a comment that this requirement should be limited to network ports as portable media is handled elsewhere. In response, the SDT notes that BES Cyber System Information on portable media is handled elsewhere, not the portable media itself. Portable media is becoming a primary means of entry into entities and the SDT believes that to meet FERC's intent, portable media and console command ports should remain in scope.

One commeneter asked for clarity on whether the disabling of physical ports could potentially reclassify a device that would otherwise be considered a BES Cyber System. For instance, if a routable device had all of its physical network ports blocked then what otherwise might be a routable device cannot route. In response, the SDT notes that the ability to communicate outside of itself is not a determining factor as to whether a Cyber Asset is or is not a BES Cyber Asset or BES Cyber System; the Cyber Asset's function as it pertains to BES reliability determines that. So although a Cyber Asset may indeed be a BES Cyber Asset, if all communication ports are disabled then the BES Cyber Asset would have no External Routable Connectivity or dial-up connectivity and thus none of the requirements which have that condition in the applicability column would apply. The specific example of the programmable television monitor provided would have to be determined by the Responsible Entity as to whether the monitor met the definition of a BES Cyber Asset. If the

monitor is not a BES Cyber Asset, then it is not a part of a BES Cyber System. The SDT notes that BES Cyber Systems consist of one or more BES Cyber Assets, not every programmable electronic device.

There was a comment asking for clarity as to whether ports could be protected via a common method or must the protections be per port. In response, the SDT notes that the requirement is not prescriptive in this manner and does not preclude either as the measures and guidance allow for directive measures.

One commenter stated that the word "unnecessary" should be changed to "not required". In response, the SDT is allowing for slightly more flexibility than is denoted by terms such as "required" or "not required". A port may be "necessary" for some use of the entity but not technically "required" for the operation of the device.

Requirement R2 General Comments

Several respondents commented that patch management should apply to all applicable Cyber Assets including all Low Impact. In response, the SDT believes that while managing patches on all Cyber Assets is a best practice, making this a mandatory and auditable requirement would divert the industry's attention to managing an onerous burden of records on orders of magnitude more devices at the lowest impact level. The SDT has been careful to balance what is absolutely required in a mandatory and enforceable manner and the burden of proof such a change would entail with maintaining a high degree of industry focus on the higher risk assets. If we overburden the Low impact classes, it would be easy to divert an inordinate amount of industry focus to the lowest impact assets if we don't maintain that balance. The SDT also believes that many devices will probably have some portion of the population declared as medium impact and thus many entities will need to handle any vulnerabilities on those devices and oftentimes will just patch all devices of that type.

There were many commenters that suggested that all sub requirements should have the applicability changed to medium impact with ERC. In response, the SDT notes that managing security patches or otherwise mitigating the vulnerabilities the patches address is a core activity in protecting our critical infrastructure. While external routable connectivity does increase the risk, the lack thereof does not reduce it to an acceptable level as many threats enter the environment by other means such as thumb drives, laptops, smart phones, etc. The SDT does not believe we can adequately protect the infrastructure if we only concern ourselves with patching devices with external connectivity due to the remaining threat vectors. However, the SDT does understand the evidence burden and has made changes to this requirement to reduce that burden. The requirement now allows entities to focus on a monthly 'batch' cycle of patches rather than tracking timelines for every individual patch, and no documented mitigation plans are needed if patches are installed within the 70 day time period. It is the SDT's intent that these and other changes in this requirement will relieve the documentation

burden while still requiring the performance of this basic security activity. The essence of this requirement is to have the industry watching and aware of vulnerabilities in their BES Cyber Systems, whether they are routably connected or not, and mitigating those vulnerabilities. Many patches may address vulnerabilities that the entity has already mitigated through existing means and require no action. In fact, it is expected that the lack of external routable connectivity would be used as a major factor in many applicability decisions and/or mitigation plans where that is the case.

Several commenters stated that the requirement should not require a documented remediation plan for every patch, but outline a standard patch mgt process with documented deviations. In response, the SDT agrees and has modified part 2.3 to allow for this.

There were a couple of comments that clarification is needed on failed patches installed well after the 60 days but according to the entity's plan. In response, the SDT has modified the requirements such that a plan may be revised (see requirement part 2.4).

One commenter suggested that the word "processes" should be changed to "program" throughout R2 so it aligns with 2.1. In response, the SDT agrees the terms should match, but notes that Requirement R2 (above the tables) uses the word "processes" and has changed the term "program" in 2.1 to "process" so that the entire requirement uses the same term.

One commenter stated that the requirement in essence rewards obsolescence and never requires upgrading to a patchable system. In response, the SDT notes that the standard's intent is to secure the infrastructure that is in place without requiring equipment upgrades of currently functional equipment solely for security purposes. Cyber security risks are one factor in the decision to upgrade. The SDT also notes that cyber risk is determined by many factors, and older equipment could actually have a lower cyber security risk. These decisions are best left to the Responsible Entity to make based on the specific circumstances rather than mandated unilaterally in a cyber security standard.

There was a comment that clarity should be provided on what constitutes a "security patch" and what is "updateable". In response, the SDT agrees and has added clarifying sentences to the guidance section of the standard for part 2.1.

Requirement Part 2.1

Multiple comments stated that the phrase "security patches" should be changed to "patches and security upgrades". In response, the SDT is concerned with expanding the scope beyond patches to words such as upgrades or updates. The

SDT does not desire to create the situation where a vendor creates a new version of their software, mentions something new about security in the new version, and suddenly everyone is under mandatory compliance obligation to either upgrade or create a plan. Cyber security features are one component of an upgrade decision. The SDT believes that keeping this requirement to the word "patches", which are fixes to their existing version, is what should be mandatory. The SDT also notes that patches are a fix to a specific vulnerability, which is what the requirement is based upon as it is under obligation to mitigate the vulnerability.

One commenter suggested that applicability and compensating measures should be determined based on original source of patch (e.g. Microsoft) rather than the SCADA vendor. In response, the SDT agrees that this is a best practice so that vulnerabilities may be mitigated in the shortest timeframe possible, even before the patch is certified by the SCADA vendor. The SDT notes that the provided example is the most obvious one with Microsoft, however if included in a mandatory and auditable environment this would extend to the seemingly unlimited non-obvious situations where an entity buys a system from vendor 'X', but vendor 'X' is using software components from 20 other vendors. The entity does not know all the original sources of all components of the system. Situations such as what is the RTOS (Real Time Operating System) involved in a particular digital relay would arise, and why didn't the entity track the vulnerability info for that RTOS directly from that vendor rather than the relay vendor's firmware levels? The entity is not a direct customer of that RTOS vendor and may not have access to that information. In summary, while the SDT believes this is a best practice in some situations, making it mandatory and auditable in every situation is not something that entities can comply with as the standard expands in scope to every BES Cyber Asset in the field.

There was a recommendation that more guidance is needed on appropriate patch sources. In response, the SDT notes that the 'appropriate sources' was added to this requirement from Version 4 so that a definite start date for the evaluation timeframe could be determined. The appropriate source is going to be dependent on the situation. If the Responsible Entity has a control system from vendor who invalidates support contracts if the system is patched outside of their approval, then the vendor should be the appropriate source. If the system were custom built by the Responsible Entity, then the vendor for each of the components used to build the system would be the appropriate source.

One commenter recommended that the program should be specified in Requirement R2 and not Requirement R2.1 as a process does not include a program. In response, the SDT agrees and has changed the word "program" in R2.1 to "process" so that it agrees with Requirement R2.

Some commenters said that the process should include a periodic review (monthly) of all patch sources rather than maintaining timeframes per patch. In response, the SDT agrees and has made changes to the language to incorporate this concept.

There was a comment that the requirement should insure that documentation of sources is a onetime exercise unless new software is added to the baseline. In response, the SDT agrees and has clarified this in the guidance section of the standard.

Requirement Part 2.2
Numerous commenters suggested a change to 35 calendar days to allow for a monthly cycle. In response, the SDT agrees and has made the suggested change.

One commenter requested that the guideline states that entities are allowed to evaluate and accept risk which FERC Order 706 disallows. In response, the SDT agrees and has modified the guidance.

There were a few commenters that requested additional clarity on what the term 'applicability' means. In response, the SDT agrees and has added clarification to the guidance section.

One commenter suggested alternative wording, "Evaluate the security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified in requirement part 2.1. The assessment must include determination of the applicability of each patch to the entity's specific environment and systems as well as reason for a patch's non-applicability." In response, the SDT has modified this requirement to incorporate a monthly review of the patch sources, but has chosen not to get more prescriptive with the term applicability within the requirement. The SDT believes that evaluating applicability necessarily means that the entity will be documenting the final determination for their environment.

Requirement Part 2.3
Some commenters proposed changes to the timeframe and process such that it would allow 60 days and have no remediation plan required if the patch is installed within 60 days. In response, the SDT agrees and has modified the requirement so that applying the patch or creating or revising a mitigation plan are all choices the entity can take within the second 35 day period. The SDT notes, however, that the timeframe is 70 days total with 35 days for tracking and

determining applicability and 35 days for either installing or determining the mitigation plan. It is not 35 days plus an additional 60 days for the second step.

There were multiple comments that the word “dated” should be revised since it is open-ended. In response the SDT believes the word “dated” is necessary and the requirement would be open-ended if it had no date required for the plan. The date of the plan in requirement part 2.3 is what part 2.4 depends upon.

One commenter stated that the requirement was overly burdensome due to the sheer number of patches. In response, the SDT notes that due to the burden the auditable cyber assets are limited to High and Medium Impact Systems and associated systems. The SDT has changed the requirement so that the tracking can be on a monthly basis for all patches released that month rather than on an individual patch basis, which should help.

Some commenters suggested that specificity is needed as to a maximum timeframe. It is compliant with the requirement to state a timeframe of the phrase “End of Life Upgrade”. In response, the SDT has had numerous discussions around this issue. The SDT has decided that the reliability risk of putting prescriptive and mandatory timeframes for patching outweigh the risks of having an open-ended patching timeframe. There are numerous reasons. One reason is the industry goes through periods of time during seasons of the year that we refer to as “nobody is touching nothing” mode because the risk of any change to equipment or systems invokes an availability risk when the asset is depended upon the most. Tripping a generating unit on a 100-degree day because a standard said we were out of time to patch it to fix some minor issue is not acceptable. Another reason is we are in a largely legacy equipment environment as this standard expands outside of control centers where there are no patch management solutions. Upgrading the firmware in thousands of digital relays is something that must be planned and executed very cautiously. Firmware based devices will require planned outages for patches and present the risk of “bricking” the asset. So for these and other reasons, the SDT has decided the implementation timeframe is best left up to the entity rather than enforcing some arbitrary timeframe. The requirement is that they have a dated plan and must work towards that plan. We believe this is the best tradeoff between the risk of someone exploiting a vulnerability and the inherent risk of changing code in devices where availability is paramount. If the SDT set a maximum timeframe to handle these sorts of cases, we would have numerous comments about how the timeframe is too long. We believe that setting a timeframe to handle these cases would actually draw a line in the sand that would have the unintended consequence of all patch timeframes moving toward that timeframe. If the entity has to set its own timeframe and defend it, then they won’t all tend to move towards the maximum timeframe specified in the requirement.

Two commenters suggested that the requirement should allow for revision to an existing plan. In response, the SDT agrees and has changed the language to allow for revisions.

There were a few recommendations that the word “exposed” should be “addressed”. In response, the SDT agrees and has made the change.

There was a comment that a potential double jeopardy issue exists between requirement parts 2.2 and 2.3. In response, the SDT has made numerous changes to these requirements and believes that any double jeopardy issues have been addressed.

One commenter stated that an evaluation of the language in the change rationale should be done to determine what needs to move into the requirement itself. In response, the SDT believes that what remains in the rationale is rationale and has no actionable requirements that could be moved to the requirement itself. However the SDT agrees the language in the rationale should be preserved and has moved it to the guidance section as well.

There was a comment that addressing the vulnerability could be entirely dependent on vendor’s patch development timeframe to address a vulnerability. In response, the SDT notes that the process begins upon the release of the patch from the source identified by the Responsible Entity. The patch has been developed and is available before the process required in R2.2 and following starts.

One commenter asked about the need for TFEs where patches cannot be applied. In response, the SDT notes the intent is that TFEs are not required at any step in the process. The process has been designed to alleviate the need and guidance has been included as well to address this issue.

There was a comment that the first sentence in the guidelines for Requirement R2.3 is a restatement with different wording and may imply other requirements. In response, the SDT agrees and has changed the guidance to more closely match the requirement.

Requirement Part 2.4

Multiple commenters stated that the plans should allow for revision in other than CIP Exceptional Circumstances before the timeframe expires. In response, the SDT agrees and has added the ability to revise the plan if done through an approved process such that the revision or extension is approved by the CIP Senior Manager or delegate.

An issue was raised that there is a potential double jeopardy issue as 2.4 duplicates Requirement R2 where 'implement' is required. In response, the SDT does not believe that a double jeopardy issue exists because the implement in the overall requirement is for the patch management process, whereas the implement in R2.4 is for the individual patch. If R2.4 does not have an implement requirement at the patch level, then the 'implement' in the overall requirement only applies to drafting a plan.

One commenter suggested that guidance should be offered on how much information is expected to demonstrate implementation. In response, the SDT notes that example measures are provided and that the requirement is for the implementation of a mitigation plan, thus the measures would be records of the implementation of the plan. The plan may include such things as installing the patch and the measure would be a record of the installation, or the plan may include the disabling of an affected service, or the adding of a signature to an IDS, or a change to a host based firewall to handle the vulnerability and the measure would be the record of the completion of these changes.

There was a comment that the change rationale is from 2.2 and doesn't address 2.4. In response, the SDT agrees and has updated the rationale to match the changes in the requirement.

To address the comments that bullet 2 of the measure should read "records of vendor recommended or other appropriate mitigations" the SDT agrees and has added "or other appropriate" to the measure.

Requirement R2 VSL

One commented that the R2 and R3 VSLs increment by different ranges. In response, R3 has been modified to remove specific timeframes in the Requirement and the VSL has removed the referenced increments.

Requirement R3 General Comments

One commenter requested that the requirement should apply to all applicable Cyber Assets including all Low Impact. In response, the SDT believes that while this is a best practice, making this a mandatory and auditable requirement would divert the industry's attention to managing an onerous burden of records on orders of magnitude more devices at the lowest impact level. The SDT has been careful to balance what is absolutely required in a mandatory and enforceable manner and the burden of proof such a change would entail with maintaining a high degree of industry focus on the higher risk assets. If we overburden the Low impact classes, it would be easy to divert an inordinate amount of industry

focus to the lowest impact assets if we don't maintain that balance. The SDT believes that keeping the requirements on Low impact systems at a programmatic level rather than a device level is the only way to keep that balance.

Multiple commenters suggested that the applicability should change to all medium impact with ERC. In response, the SDT disagrees because the threat of malicious code is not limited to introduction through external routable connectivity. The threat of malicious code is arguably higher from portable media, temporarily connected cyber assets (vendor laptops, etc) and inadvertent insider actions.

Requirement Part 3.1

There were a few comments which stated that the intent should be clarified and suggested language includes "Deploy method(s) to deter, detect, or prevent malicious code based on the Cyber Asset's susceptibility to malware. Methods do not have to be used on every single Cyber Asset." In response, the SDT notes that the applicability is at the 'system' level and the intent is to keep it at that level as this is a requirement where the 'system' level is beneficial. Therefore, the SDT believes it is best to not fill the requirement with language at an individual cyber asset level.

There were several concerns that Requirements R3.1 and R3.2 are too vague. In response, the SDT notes that the requirements are indeed written at a very high level but the SDT believes it is necessarily so. Malicious code protection is at the 'forefront of the fight' and is rapidly evolving and changing to match the ever changing and morphing threat. The SDT believes the protection of our infrastructure can be better accomplished if we do not have prescriptive technical methods detailed in this requirement. This could have the unintended effect in the future of stifling innovation and the use of new and better tools that would provide better protection but not be compliant with what the SDT would specify today. It does not produce a standard that is future-proof. All previous versions of the standard did prescribe a particular technology and method that must be used on all applicable cyber assets, and while that had no vagueness it became a huge burden on the industry for TFE's, putting the industry's focus on what could not be done rather than what could be done. Therefore, the SDT is leaving this requirement at a very high level that is in essence "think through the problem of malicious code introduction, detection, and prevention and come up with the best methods to handle the problem in each particular situation, and then document and do those methods." The SDT believes reliability will be better served in the long run by a requirement like this for such areas as the malicious code 'arms race' environment that we find ourselves in.

There were multiple comments asking if the 'or' is appropriate. There was another question if an awareness campaign to deter is ok. There was a suggested that the word 'deter' should be stricken. In response, the SDT notes that the

requirement was worded with the 'or' and 'deter' to avoid zero-defect language. If the requirement was to detect or prevent all malicious code, then despite an entity's best efforts if some zero-day malware did make it onto an applicable cyber asset the entity would be in violation of the requirement. As malware detection and prevention is an inexact science and essentially an 'arms race', the SDT did not want to word the requirement in such a way that it required perfection in an imperfect environment with imperfect tools.

There was many comments that the 'Associated PCAs' are included at a Cyber Asset (device) level, not a system level and should be deleted or clarified how the 'system' concept will apply. In response, the SDT notes that malware prevention really is at a Cyber Asset level and recognizes that the associated PCA's could be included by reference in the documentation the entity supplies for Requirement R3.1.

One commented stated Requirement R3.1 and R3.2 should be revised to "deploy methods … within an ESP" to scope to routable assets within the ESP. In response, the SDT notes that ESP's are only required around routable protocol connected cyber assets, however malware protection is required on all cyber assets in scope. Malware is a risk even on isolated systems; it may not be able to easily spread in non-routable environments, but it can be coded to have a specific impact even on isolated systems (e.g. Stuxnet was coded to do its harm when it reached a specific system and could travel by USB portable media). Therefore the SDT has chosen to not limit the malware prevention requirement to only routable protocol accessible systems in ESPs.

One commenter suggested that the measures should be revised to, "Entity's performance of these processes (e.g., through traditional antivirus, system hardening, non-software policies, etc.)." In response, the SDT notes the only suggested change is the phrase 'non-software' in front of 'policies'. The SDT does not wish to make the measure more prescriptive than the requirement itself. Since malware prevention is an ever changing 'arms race' type environment where the controls needed are changing as the threat constantly evolves, the SDT is leaving this requirement at a high level. This will allow entities to adapt as the threat adapts while also reducing the need for TFEs.

One commenter stated that the last sentence of the guidance says 'should not require a TFE' making it unclear whether TFEs are an option or not. In response, the SDT agrees and has struck the phrase.

Requirement Part 3.2

One commenter recommended that the following sentence be added: “Mitigation for the Associated Protected Assets may be accomplished through other applicable systems.” In response, the SDT agrees that this is possible and the entity could state how the mitigation covers the associated PCA’s in their documentation for this requirement.

One commenter suggested that the wording “within 35 days” should be added as malware mitigation timeframe. In response, the SDT has chosen not to include a mitigation timeframe as in some cases the entity may be working with government or law enforcement in an ongoing investigation. In APT cases, quick mitigation may just force the moving of the attack while investigations are ongoing. The SDT feels that a mandatory timeframe would interfere with investigations in cases such as these.

Two commenters recommended that the measures should be limited to response actions for detected malware and remove other bullets. In response the SDT agrees and has removed the example measures that were more focused on specific technologies.

One commenter stated that in the guidelines it discusses ‘non-changeable software’ and asks if this is in conflict with definition of Cyber Asset. In response, the SDT believes it is not in conflict. Cyber Asset is a programmable electronic device and devices that are not updateable by the user, but are software or firmware based and do execute a program would still be classified as Cyber Assets.

Requirement Part 3.3

There were many comments that Medium impact locations with no remote connectivity need more than 35 days for signature updates or should not be in scope. Some commented that 35 days is too long for malware updates and it should be shortened. In response, the SDT agrees with both positions and realizes that specifying a time frame on a requirement such as this often means picking a timeframe that is usually not long enough for all of the more extreme cases while at the same time is too long for most ‘normal’ cases. The SDT has decided that it is in the best interest of reliability to revert this requirement back to its V1-V4 language that did not include a timeframe. Order 706 did not direct such a modification and the SDT is more concerned about preventing the unintended consequences of this timeframe and their resulting impacts to reliability. As one example, the SDT does not want to incent entities to remove antivirus products from systems in the field and expose them to a decade’s worth of viruses because they may not be able to get last month’s signatures on in 35 days. The SDT believes its in the best interest of reliability to allow entities to put antivirus software on all assets where they can and require processes to test and install the updates without specifying an ‘arbitrary’ timeframe that satisfies no one.

One commenter stated that 35 days is too long for malware updates and should be shortened. In response, the SDT agrees with both positions and realizes that specifying a timeframe on a requirement such as this often means picking a timeframe that is usually not long enough for all the more extreme cases while at the same time is too long for most 'normal' cases. The SDT has decided that it is in the best interest of reliability to revert this requirement back to its V1-V4 language that did not include a timeframe. Order No. 706 did not direct such a modification and the SDT is more concerned with the unintended consequences of this timeframe and the resulting impacts to reliability. As one example, the SDT does not want to incent entities to remove antivirus products from systems in the field and expose them to a decade's worth of viruses because they may not be able to get last month's signatures on in 35 days. The SDT believes it is in the best interest of reliability to allow entities to put antivirus software on all assets where they can and require processes to test and install the updates without specifying an 'arbitrary' timeframe that satisfies no one.

Several commenters wrote that the requirement is not as clear as the change rationale and the requirement could be gamed to not install any recent sigs. In response, the SDT agrees and has rewritten the requirement for clarity.

A few comments stated that signature updates need to be staged to avoid a large impact of false positives. The included guidance should address this as well. In response, the SDT agrees and has reverted the language back to its V1-V4 state that did include a process for testing and installing the signature updates.

Some commenters questioned that if an entity does not use signature based tools, if they still have a process to update the signatures per the overall requirement. In response, the SDT notes the specific sub requirement is conditional and only applies to "for those methods identified in requirement part 3.1 that use signatures or patterns…" and therefore if an entity has no such methods, the requirement does not apply.

One commenter recommended that the word "available" should be changed to "applicable". In response, the SDT has rewritten the requirement for clarity and to address this and several other comments.

A commenter suggested that the requirement should allow for other anomaly or heuristics based analysis/detection, not just signature updates. In response, Requirement R3.1 allows for any method to be used so that the requirement does not preclude the use of any technology or tool as they constantly improve to keep up with the threats. Requirement R3.3 in particular is only applicable when an entity chooses to use a signature or pattern based tool in order to keep them updated in a timely manner; it does not require their use.

One commenter asked for clarity on what TFEs are allowed for equipment that doesn't run malicious code tools. In response, the SDT notes the requirement has been written at a much higher level than previous versions. The included guidance has numerous suggested methods up to and including policy level measures. Therefore, the SDT feels that TFEs are no longer an issue as the requirement no longer prescriptively requires a single technology tool for addressing the issue.

Requirement R4 General Comments

There were several comments that the rationale language should change 'immediate' detection to 'real time detection' to be consistent with 4.2. In response, the SDT received numerous comments that pointed out issues with the term 'real time' and has deleted it, as well as removing 'immediate' in the rationale.

There was a comment seeking clarity as to whether log events are required for local, remote, or both types of access. In response, the SDT notes that the requirement applies to both High and Medium impact BES Cyber Systems as well as all associated EACMs. The EACMs will include the EAPs for the associated perimeters. Therefore the logging is for both; local access at the BES Cyber Systems themselves, and remote access through the EAP.

One commenter suggested that the guidance include NIST 800-137 as a resource. In response, the SDT agrees and has added the reference to the guidance.

Requirement Part 4.1

Many commenters recommended that the requirement should add the phrase "per device capability". In response, the SDT agrees and has added this concept to the language.

Numerous commenters asked that it be clarified that devices that cannot log do not require a TFE. In response, the SDT has added device capability condition statements to the requirement such that the requirement does not apply if the device does not log the events. In addition, the bulleted list of logged events includes the qualifier 'detected' so that if a device cannot detect such events, then there is nothing to log.

There were several suggestions that 'where technically feasible' should be added to all. In response, the SDT's intent is that the requirement is worded so that what is required matches the device's capability and no more and avoids the use of TFE's due to prescriptive requirements that assume technical capabilities of large classes of Cyber Assets.

Tucson, and SME List commented that TFE should be applied to the logging, not the alerting in 4.2 and suggest removing the TFE in 4.2. In response, the SDT has changed both 4.1 and 4.2 to include the 'per device capability' concept rather than allowing TFE's.

Multiple commenters suggested said that the applicability should change to Medium Impact with ERC. In response, the SDT notes that logging should be enabled wherever it is available. If an isolated or standalone BES Cyber Asset is compromised, then the logs on that device may be the only data the entity will have to investigate the incident.

One commenter suggested that the measures should include samples of logs showing the events are being logged. In response, the SDT agrees and has added the additional example measure.

One commenter suggested that the requirement implies 100% availability of the logging system and suggests adding the 99.9% availability. In response, the SDT notes the comments where the 99.9% was added in CIP-006 pointed out numerous issues with that approach. The SDT believes that the inclusion of Requirement R4.3 states that 100% availability is not required and handles the issue by requiring the entity to have processes in place to respond to outages in a timely manner.

Several commenters sought clarity as to log failed access attempts when deny by default means offending packets are dropped such that there is nothing to log. In response, the SDT notes that a denied access attempt is a failed access attempt.

There were several commenters who suggested that 'malicious software' should be changed to 'malicious code' to be consistent with Requirement R3. In response, the SDT agrees and has made the change.

Many commenters recommended dropping the requirement since its determined after the fact, requires knowledge of intent, and it's not possible to produce a log of 'malicious activity'. In response, the SDT agrees and has removed the sub requirement.

Several commented stated that 4.1.4 is too vague and needs more guidance as to what activities beyond 4.1.1 to 4.1.3 would be included. In response, the SDT agrees and has removed the sub requirement.

One commenter stated that malicious activity should be detected and logged 'as required in the cyber security incident response plan'. In response, the SDT notes that based on several other industry comments, this sub requirement has been removed.

Requirement Part 4.2

Several commenter stated that 'real time' is not the appropriate phrase and some suggested changing to "Have methods to generate alerts, where technically feasible, for events that the Responsible Entity determines necessary." In response, the SDT agrees and has deleted the 'real time' phrase.

Also, others commented that 'real time' should change to 15 minutes and add 'where the BES Cyber System is capable.' In response, the SDT agrees and has deleted the 'real time' phrase and the 'per Cyber Asset or BES System capability' has been added.

A few commenters recommended that 'within the BCS capabilities' be added. In response, the SDT agrees and has added the appropriate phrase.

One commenter stated that a minimum expected set of security events for which alerts should be issued should be prescribed (if the Cyber Asset is capable of detecting and logging those types of events). Examples include failed login attempt threshold exceeded, account lockout, key software failures, and virus or malware alerts. They also commented that the guidance includes alerts to a display that may not be monitored. In response, the SDT notes that detected malicious code is included, as is detected event logging failure. The SDT agrees that unsuccessful login attempt threshold should be added as it is a requirement in CIP-007 R5.7 and has made this addition. The SDT notes that account lockout is a subset (or post action) of unsuccessful login attempt threshold and has not included it.

There was a comment that the requirement should only apply to Associated Protected Cyber Assets with ERC. In response, the SDT believes that if the BES Cyber Systems have External Routable Connectivity that the associated PCAs will also have that connectivity. In the envisioned rare instance where this is not the case, the requirement allows for the entity to do what is within the device's capability and no more.

One respondent commented that we need a requirement that trained and knowledgeable people perform the event monitoring activity. In response, the SDT agrees that this is certainly reasonable, but disagrees that it should be an

auditable requirement as it raises too many audit issues, such as what do the terms 'trained' and 'knowledgeable' mean and what is sufficient for each?

A commenter questioned is an alert required for malicious activity if it is automatically quarantined? In response, the SDT notes that alerts are required for detection of malicious code regardless of any subsequent mitigation actions taken. The SDT believes that if malicious code gets through the layers of defense and makes it way on to a BES Cyber System, that is an event that needs the entity's timely attention and response so the defenses can be shored up for the zero-day that is not detected and quarantined.

One commenter wrote that it was unclear as to whether 'detected failure' refers to logging a failure of some event or failure of logging. In response, the SDT has added a clarification that it is failure of the requirement part 4.1 event logging. This would include the failure of the applicable systems logging capability.

There was a recommendation that the measures should include examples of alerts issued. In response, the SDT agrees and has added this as one of the example measures.

Multiple comments suggested that 4.2.1 should change to 'detected cyber security event' since not all events are necessarily malicious. In response, the SDT agrees and has changed this part to refer to detected malicious code rather than malicious activity.

There were numerous comments suggesting to change the wording in 4.2.1 to 'detected events per 4.1'. In response, the SDT agrees and has added the reference to 4.1 for clarity.

One commenter stated that the guidance implies that only technical means are allowed, but requirement does not preclude procedural controls. In response, the SDT notes that the requirement language is the ruling language and guidance is not auditable and is provided to provide further context or examples or assistance in how entities may want to approach meeting the requirement.

Requirement Part 4.3

There were a multitude of commenters who recommended that the requirement add the phrase "human detected event logging failure" to clarify when the clock starts. In response, the SDT agrees with the concept and has changed the

language to require that the response timeframe begins with the alert of the failure. Therefore, the timeframe begins after something or someone has detected the failure and has generated an alert as in 4.2.

One commenter suggested that 'after notification' should be added after 'next calendar day'. In response, the SDT agrees with the concept and has changed the language to require that the response timeframe begins with the alert of the failure. Therefore, the timeframe begins after something or someone has detected the failure and has generated an alert as in 4.2.

A few respondents commented that the requirement should be struck or change the verbiage to "Document the controls implemented to identify and respond to detected logging failures. Document detected logging failures along with any discrepancies between the actual response and the documented response plan." In response, the SDT agrees and has struck the requirement.

A few commenters stated that the next calendar day is not enough time to rectify issues. In response, the SDT notes the timeframe is to 'activate' a response, not to resolve the issue. The SDT has chosen this in recognition that depending on what caused the failure, there may be widely varying timeframes to resolve the issue. Therefore, the requirement is for timely initiation of a response.

One commenter noted that the requirement presumes but does not prescribe a mechanism for monitoring for logging system failures. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

Several commenter responded that the timeframe is too short due to distances or other operational situations. There was also a suggestion is to include 'next business day'. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

There was one comment that this should only apply to Cyber Assets with ERC. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

Several commenters recommended that outage handling should be standardized with CIP-006. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

There were several comments that the measure should change the word 'attestation' to 'documentation'. In response, the SDT agrees and has made the change.

One comment suggested that the measure should change 'events' to 'failures' to better align with the requirement. In response, the SDT agrees and has made the change.

Requirement Part 4.4

There was a comment that the requirement should change to "Retain BES Cyber System and BES Cyber Asset". In response, the SDT agrees with the concept that the applicability in the requirement did not match the applicability column and has removed the applicability from the requirement by replacing 'BES Cyber System' with 'applicable'.

There were several comments that the TFE language should be struck and add 'within the BCS capabilities." In response, the SDT notes that this requirement is scoped to Control Center environments where the highest degree of logging is required and has the highest degree of more capable Cyber Assets. The SDT feels that in this environment, the industry really should push for 90 days of log retention on these systems.

One commenter suggested that this should apply to all Medium's that can store logs, not just those at control centers. In response, the SDT notes that with the vastly increased numbers and types of field devices that Version 5 will bring into scope, most of which are legacy devices, that putting a mandatory requirement in place that prescribes the length of log retention is not warranted and would cause numerous TFE's.

One commenter wrote that 'identified in 4.1' should be the main qualification for log retention and delete the 'security related' portion for clarity. In response, the SDT agrees and has removed the phrasing.

Some commenters stated that this is in conflict with evidence retention section. Auditors expect to ask for any day's logs in past three years. In response, the SDT has added guidance around this topic. The requirement that is to be audited is

that applicable cyber assets maintain 90 days of logs. The compliance evidence requirement is that the entity be able to show that for the historical compliance period, the applicable cyber systems maintained 90 days of logs. The guidance speaks of records of disposition of logs after their 90 days is up.

BPA commented that a media hardware failure that results in loss of stored logs is still a violation. In response, the SDT agrees and has added "except under CIP Exceptional Circumstances" to the requirement as it includes hardware failure.

One commenter stated that this should allow for a timeframe as determined by the Responsible Entity. In response, the SDT notes that 90 days has been the precedent through the previous CIP versions and having no bound means that zero days is valid if determined by the entity. The SDT believes that 90 days is a sufficient lower bound for Control Center environments and has no justification for lowering it in the highest risk environments.

A commenter suggested that the applicability should apply to medium impact with ERC. In response, the SDT notes that this applies to Control Centers. Throughout the history of the CIP standards, all cyber assets in a Control Center are in scope regardless of external connectivity. The SDT believes there is insufficient justification to lower the standard on this point.

One commenter implied that measure 2 requests info about log data that is not in the requirement. Measures 1 and 3 cover the requirement. In response, the SDT agrees and has moved this to the guidance section with a more detailed explanation of the difference between the requirement's retention period for security purposes and the overall standard's requirement for compliance measurement purposes.

Requirement Part 4.5

Many responders commented that clarity around who determines the appropriate sampling should be added by including 'sampling as deemed appropriate by the Responsible Entity'. In response, the SDT agrees and has made the change.

Several commenters noted that the applicability should be 'High impact including associated PCA' to clarify logging reviews aren't at the device level and should exclude EACM/PACMs. In response, the SDT agrees and has modified the applicability, however EACMs should be included. Since Electronic Access Points to ESP's are EACMs, this is one of the primary logs that should be reviewed.

Several commenters expressed concern that this needs some minimum expectations for logged event review. In response, the SDT notes the intent is included in the requirement which is to identify undetected security incidents. The FERC Order in paragraphs 525 and 628 states, "However, the Commission continues to believe that, while automated review systems provide a reasonable day-to-day check of the system and a convenient screening for obvious system breaches, periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings. Furthermore, manual review is beneficial to judge the effectiveness of protection measures, such as firewall settings. If a firewall setting is incorrect or ineffective, an automated review system may not identify a cyber security intrusion. For those entities without automated log review and alerts, it is even more important to perform a manual review because this will be the only review of the logs." The SDT believes the intent is that entities manually review logs to insure that automated tools are tuned and alerting on real incidents. The SDT does not believe it should get more prescriptive with the requirement.

There were several commenters who noted that the requirement should change to "Document and implement a secondary control(s), and an associated interval, not to exceed two weeks, to assure the generation, capture, monitoring, and alerting of events as identified in 4.1." In response, the SDT notes that the FERC Order 706 in paragraphs 525 and 628 are explicit about a manual review. Also, the events identified in 4.1 are requirements so identifying events in 4.5 that should have been caught in 4.1 is a violation. The intent is for the entity to review the logs to see if there are events happening (other than those in 4.1) that the entity should be alerting on. In essence, this is a 'tuning' requirement to insure that an entity's automated Security Information and Event Management (SIEM) type tools are not missing conditions that are appearing in the logs and going undetected.

One commenter suggested that the requirement should change 'undetected' to 'potential Cyber Security Incidents not previously identified or detected'. In response, the SDT notes that in draft one the language included terms such as "unanticipated" and "potential" and received numerous comments to remove these subjective terms.

There were a number of concerns that two weeks is too short and suggest monthly or two month periodicity. In response, the SDT notes that in paragraph 628 of FERC Order 706 states, "The Commission continues to believe that, in general, logs should be reviewed at least weekly", but leaves it to the ERO to determine the appropriate timeframe. The SDT believes that bi-weekly is an appropriate timeframe given the Commission's statement concerning weekly reviews.

There was a comment that the phrase “at a minimum every two weeks” could be misconstrued and suggested to mean “at intervals no greater than 15 days.” In response, the SDT agrees that two weeks is a maximum not a minimum and adopts the suggested change.

There was a suggestion in changing the requirement to read “Review a summarization or sampling of logged events that the Responsible Entity has determined could identify previously undetected Cyber Security Incidents. Such a review will be conducted every two weeks at a minimum.” In response, the SDT agrees with the issue and has reworded the requirement based on this and other comments to utilize ‘intervals no greater than 15 days’ for greater specificity.

One commenter suggested that the timeframe should be determined by the Responsible Entity. In response, the SDT notes that in paragraph 628 of FERC Order 706 the Commission ordered the ERO to determine an appropriate timeframe that is less than the 90 days in the requirements of previous versions while stating that weekly reviews are their recommendation. The SDT sees no justification for how this directive can be met if the timeframe is left completely up to the entity to determine.

There were multiple suggestions that the applicability should only apply when automated processes and alerting are not possible or no managed service provider is utilized. In response, the SDT notes from paragraph 525 of FERC Order 706 that “the Commission continues to believe that, while automated review systems provide a reasonable day-to-day check of the system and a convenient screening for obvious system breaches, periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings.” The Commission goes on to order the inclusion of manual review even if automated alerts are employed.

One commenter stated that a SIEM is the only real solution and is too expensive for small entities. In response, the SDT notes the requirement is for a manual review, not an automated review. Paragraph 525 of Order 706 makes it clear that even if automated systems are used, the manual review is still required. The requirement does not require installation of SIEM tools, but requires manual review even if SIEM tools are in use.

Several commenters noted that the phrase “signed and” should be deleted in the measure (also in 4.1 measure). In response, the SDT agrees that a signed approval of the review is not in the requirement and this has been deleted from the measure.

QUESTION B24– CIP-007-5 REQUIREMENT R5:

If you disagree with the changes made to CIP-007-5, Requirement R5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, some of the key issues expressed by commenters included (1) the applicability to Medium Impact BES Cyber Systems with external routable connectivity, particularly in requirement part 5.1 and (2) the obligation for the CIP Senior Manager to authorize specific account types for BES Cyber Systems. The consideration of comments according to major issues and standard sections follows.

Correcting Deficiencies

One comment stated that this requirement should have a find, fix, track, and report mechanism built in so that entities can fix administrative deficiencies rather than consider them a violation of the requirement. In response, the CIP Version 5 approach to correcting deficiencies is that each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable items in the specified table. This approach of correcting deficiencies complements the compliance concept of internal controls.

Applicability to Low Impact

One commenter suggested that CIP-007-5 R5 should apply to Low Impact BES Cyber Systems. In response, we note the challenge of applying device-specific mandatory and enforceable requirements to low impact BES Cyber Systems exists in the overwhelming number of BES Cyber Assets. NERC survey results from the 2011 CIP filing indicate 90% of the facilities would be considered low impact, and each of these sites can have a potentially large number of Cyber Assets. As a result, the SDT has taken the approach of applying policy level requirements to BES Cyber Systems with the understanding and expectation that the compliance audit and enforcement of the policies will adapt to the significant increase.

TFE for all Requirement Parts

One commenter suggested adding TFE language for the entire requirement due its technical nature. In response, the SDT has identified requirement parts that intentionally allow for a safe-harbor exception process where equivalent mitigation can be shown. However, in some cases, we do not intend the technical limitations of the device to indicate a violation or need for safe-harbor (e.g. password complexity).

Multifactor Authentication
One commenter questioned if multi-factor authentication can replace password authentication without a TFE. In response, the SDT notes that the said requirement applies to password-only authentication but do not preclude other strong authentication mechanisms.

Procedural Controls
One commenter suggested, with regard to CAN-0017, procedural controls should be explicitly allowed in the requirement. However, the SDT points out that Compliance Application Notices do not carry forward to new versions of the standard. Previous versions require both procedural and technical controls for passwords, but this language is not included in the current draft. It would cause more confusion to explicitly allow procedural controls for each requirement part.

Version 5
One commenter provided its fundamental objection to Version 5 and suggested that implementation of the current CIP standards should be allowed to mature. The SDT is required to address all the FERC directives from Order 706, and FERC Order 706 has directed the ERO to complete consideration of Order 706 directives by March 31st, 2013.

Summary of Changes Section
Two commenters noted the summary of changes does not correspond to requirements for shared accounts, and in response the SDT has deleted this section which was held over from previous versions.

Requirement Part 5.1
Several entities commented this requirement part should be limited to medium impact with External Routable Connectivity, and the SDT has made this change. However, this requirement still applies to Medium Impact BES Cyber Systems at Control Centers.

Several commented that user access should be a defined term and security controls for system accounts should also exist. In response, we provide a definition in the guidelines, and we believe this term is well understood. In addition, the SDT has added a qualifier for this to apply to interactive user access. We do not define the same controls for system access due to the widely diverse way this could apply. System accounts do not uniformly apply across all devices and operating systems.

Several entities suggested rewording the phrase “where technically feasible” to “within the capability of the BES Cyber System”. In response, the alternative language would not change the TFE trigger for this requirement. There are several instances in which strict compliance can still be met in the absence of a specific technology mechanism to enforce access. The SDT has provided examples in the rationale box for requirement part 5.1 and improved the requirement language to make this point clear.

One commenter requested clarification that user access does not mean front panel read-outs on a device. In response, the SDT has changed “user access” to “interactive user access”, and the SDT has added a rationale statement further describing the intent of this requirement, in which the SDT has explicitly stated front panel read-outs do not qualify as interactive user access.

One commenter proposed that this requirement should be rephrased to limit to only electronic access. In response, the subject matter of the standard and requirement suffice to make the distinction, and we do not want to limit or confuse the possibility of using properly configured physical access controls to demonstrate compliance with this requirement.

One commenter suggested this apply to accounts and not user access. In response, the SDT has chosen to apply this to interactive user access because there may be instances where you do not want to enforce authentication for read-only access.

One commenter suggested specifying the phrase “applicable cyber assets” to qualify this requirement, but the applicability column already qualifies the requirement.

Requirement Part 5.2

Several entities suggested deleting requirement part 5.2 because it is already covered by the CIP-004-5 requirement to authorize users. In response, this requirement only deals with identifying the use of account types. It has been modified to make the intent clearer. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The requirement part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Several commenters advised removing the CIP Senior Manager as the person authorizing these account types. In response, the SDT chose not to remove this in the previous posting as suggested by our previous response to comments, and the SDT has removed the CIP Senior Manager as the person authorizing the account types in this posting.

One commenter proposed that generic accounts must be specified. In response, the SDT has added examples in the guidance section of this standard. The section added reads: "Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level."

One commenter suggested removing the word "authorized" from this requirement. The SDT has incorporated this suggestion by replacing the word "authorized" with the phrase "identify and inventory".

There was a comment submitted as to whether this requirement restricts the use of the specified account types. In response, identification of the accounts provides the necessary control. We do not specify these accounts must be disabled or removed because they are sometimes necessary for operation. Restricting these based on least privilege or need to know is already covered in CIP-004-5 R6.

One commenter suggested that authorization by "delegate(s)" be substitute for "delegate". However, the SDT has removed the requirement to authorize by CIP Senior Manager based on other commenters.

Requirement Part 5.3

Several comments suggested deleting requirement part 5.3 because it is already covered in CIP-004-5 requirements to authorize access. However, the identification of individuals with access to shared account has the additional objective of mitigating the risk of unauthorized access through shared accounts. This differs from the CIP-004-5 Requirement R6 to authorize access. An entity can authorize access and still not know who has access to a shared account. This would make it difficult to revoke access when it is no longer needed.

Several suggested incorporating the change rationale stating that the phrase "individuals storing, losing or inappropriately sharing a password is not a violation of this requirement." In response, the SDT has added this language to the rationale box for CIP-007-5 R5. The language in this section reads, "The term "authorized" is used in the

requirement to make clear that an individual storing, losing or inappropriately sharing a password is not a violation of this requirement."

Multiple commenters suggested adding the word "authorized" as a qualifier for access to correspond to the requirement language, and the SDT has made this change.

One commenter suggested that this requirement does not go far enough to restrict the use of privileged access, particularly when operating software. In response, CIP-004-5 R6 restricts the use of privileged access to only those having a documented business need. We do not specify the individual use of privileged and non-privileged access because this is not auditable for mandatory enforceable requirements. This is a good practice, but if this practice were codified in a standard, any individual not following the policy would impose monetary penalties on an organization.

One commenter suggested that the external routable connectivity qualifier should be removed for this Requirement Part in the applicability to match requirement part 5.2. In response, the requirement parts are unrelated, and the qualifier matches that of CIP-004-5 R6, which requires the authorization for electronic access.

Requirement Part 5.4

Several comments suggested revising this requirement part to address a recent RuggedCom vulnerability where a default password was unique to publicly known attributes of the device. In response, the SDT has removed the requirement exception where the "default password is unique to the device or instance of the application", and specified in the rationale that "pseudo-randomly system generated passwords are not considered default passwords".

Several commenters suggested adding the word "known" as a qualifier to default password to avoid the case where the entity was not aware of an undocumented default password by the vendor. The SDT has made this change.

There were several comments that the measure should change the phrase "new devices are deployed" to "new devices are in production" and one commenter suggested removing the phrase altogether since timeframes are covered in the implementation plan. The SDT has made this change from the word "deployed" to "in production", but the timeframe here does not conflict with the implementation timeframe and provides example, high quality evidence to meet this requirement.

One commenter requested clarification of when the default password should be changed. In response, we do not specify a timeframe (i.e. when cyber assets go into production) which could be misinterpreted. Instead, as with all requirements of CIP-007-5, this requirement must be met when a device becomes one of the applicable systems or assets.

Several commenters suggested removing the term "Cyber Assets" within the requirement to match the applicability of BES Cyber System. In response, the SDT has removed this language in deference to the applicability column.

One commenter requested clarification that default password that are unchanged would require changing according to R5.6. In response, this may be the case for interactive user accounts, but this is not necessary to state in the requirement. Changing default passwords meets a different objective to prevent unauthorized access from known credentials.

One commenter suggested excepting when a password is unique to the device. However, many commenters point out that doing so would allow for vulnerabilities where the uniqueness of the device where publicly known (i.e. MAC address).

Requirement Part 5.5

Several commenters suggested modifying the measure for requirement part 5.5 and requirement part 5.6 to better describe the attestation. Another commenter suggested replacing attestations with the ability to present a procedure. Others noted that it is not possible to obtain attestation from unionized workers and suggested adding a separate requirement to use training as a procedural control in place of attestations. In response, the SDT has used provided language to better describe the attestation evidence. The suggestion to use presentation of a procedure as a replacement cannot be used as evidence of implementing a procedure. The suggestion to have a further requirement for training is already covered in the training program specified in CIP-004-5.

One commenter stated that password complexity should be enforced to the maximum extent technically possible. In response, the SDT noted such a policy would create situations where users must write down passwords to remember them. The maximum extent could be exorbitant in some cases.

One commenter also stated that the guidelines state this requirement part is for password-only authentication, but the requirement does not include the same stipulation. BPA and Salt River Project made similar comments to distinguish the case where a PIN is used for multi-factor authentication. In response, the SDT has changed "password-based" to "password-only" in both requirement part 5.5 and 5.6.

Several commenters suggested using verbiage for requirement part 5.5.1: “Password length that is, at least, eight characters or the up to the maximum allowable by the system if that maximum is less than eight.” In response, although the proposed verbiage is cleaner, it becomes less clear once we specify “system” and the number of characters in the proposal. The SDT therefore decided to continue with the currently drafted language.

One commenter questioned if this new requirement will remove CAN-0017. In response, CANs do not apply to future versions of the standard, and the SDT has explicitly addressed the issue raised by CAN-0017 that either technical or procedural mechanisms can meet the requirement.

One commenter stated that it does not agree with the proscription of password requirements. In response, the SDT has included more prescriptive password requirements in response to a large number of industry comments against having added flexibility. However, the SDT has also attempted to remove some of the problematic provisions of the current version of password requirements that would allow entities to have stronger password policies.

One commenter suggested that the password complexity in requirement part 5.5.2 should specify or define the word “type”. In response, the examples provided in the requirement suffice for specifying password character types. The SDT believes these terms are well-understood by industry and do not necessitate further definitions.

Requirement Part 5.6

Several commenters pointed out the guidance, particularly the recommended password length table, has not updated to reflect the requirement. In response, the SDT has deleted sections of the guidance which no longer have relevance to the requirement.

Several commenters suggested adding a technical feasibility clause to this requirement part because some devices do not allow this capability. In response, the SDT notes that this only applies to user access, and the SDT has modified the requirement part to clarify this. The language as the end of this requirement part reads, “…at least once each calendar year, not to exceed 15 calendar months between changes, where technically feasible.”

One commenter suggested this requirement part explicitly apply to interactive user access, and the SDT has modified this requirement part to address the concern. The beginning of this requirement part reads, “For password-only authentication for interactive user access, either technically or procedurally enforce password changes…”

One commenter suggested adding the language “unless it impacts operation of the BES” to this requirement part. In response, the SDT has added the phrase “where technically feasible” to address these type of exceptions.

One commenter suggested the applicability of 5.6 be modified to match other requirement parts in CIP-007-5 R5. In response, the applicability to those Medium Impact BES Cyber Systems with External Routable Connectivity is due to the periodic nature of this requirement, which may only be feasible on large systems by having such connectivity. The commenter also suggested periodically is misspelled periodicity, but the SDT intends the latter as this is an attribute of the policy instead of a modifier.

One commenter suggested incorporating the language in the guidance table to include periodicity provisions for plant outages and disabled accounts. In response, for disabled accounts, a password change is not required because these do not qualify as providing interactive user authentication. The requirement does not have provisions for plant outages due to the widely varying schedules for plant outages. The SDT also notes that this requirement applies to those Medium Impact BES Cyber Systems with External Routable Connectivity.

A commenter proposed having a password change every 15 months. The SDT has incorporated this suggestion as part of an overall modification of annual periodic requirements in the CIP standards.

A commenter proposed to allow the entity to specify a password change periodicity, but the SDT has specified this periodicity based on a large number of comments against having this flexibility.

There was one comment that suggested the password change periodicity should be much shorter (i.e. quarterly). In response, the SDT notes that password change requirements should be considered in context with all of the password requirements, and shorter password change requirements can often result in poor password protection and selection by individuals.

Requirement Part 5.7

Several commenters suggested this requirement has the potential for creating a denial of service vulnerability to lockout all accounts to the system if entities configure all accounts for lockout. The SDT has not included the proposal to specify “user accounts” for limiting login attempts because it is too specific and has the potential to cause confusion. Although

the requirement does not prescribe this vulnerability, it does allow for it. Consequently, the SDT has included guidance in avoiding this configuration in the rationale.

Several commenters requested clarification on what the clause "where technically feasible" qualifies for this requirement part. In response, this requirement part has been modified to make clear the TFE triggering language qualifies both options. Furthermore, a TFE would only be necessary based on failure to implement either option.

Several commenters suggested this requirement should be deleted as it was not directed by FERC or otherwise align with the alerting requirements of CIP-007-5 requirement part 4.2. In response, this requirement is part of a more reasonable overall password security standard. As a trade-off to providing more flexibility to password policies, this requirement is highly effective to prevent online password attacks. This does not duplicate CIP-007-5 requirement part 4.2 because this alert is not required to be configured by that requirement.

One commenter requested additional guidance on the threshold for unsuccessful login attempts. The SDT has added this to the guidance section of this standard. Language was added which reads, "The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate."

Multiple commenters suggested that a minimum threshold parameter for account lockout should be specified. In response, a value is not specified here because this requirement protects against password cracking through online password cracking. Given the additional password policy requirements, the threshold for this setting can be very high, up to 100 or more.

One commenter requested the requirement part make clear these do not apply to Protected Cyber Assets such as printers and multi-function machines. In response, this requirement does apply to Protected Cyber Assets. This is a part of an overall protection against unauthorized access, which would include Protected Cyber Assets that have direct connections with the BES Cyber System.

VRFs

There was one comment that suggested the VRF should be Lower for Medium Impact BES Cyber Systems. In response, the impact level of the BES Cyber System is accounted for by the applicability of CIP-004 through CIP-011 requirements. A violation for a Medium Impact BES Cyber System cannot be considered directly with a High Impact BES Cyber System because they have less application of compensating security requirements.

VSLs

There was one comment that noted the High VSL includes the phrase “use of” where the associated requirement refers to only enablement of generic accounts and that the Severe VSL includes criteria for failure to implement password procedures, which might imply the required use of passwords. The VSL language regarding the enablement of generic account types has been updated to match the requirement. We do not agree the Severe VSL language implies a requirement to only use passwords. The VSLs are only used to describe violations, and use of authentication alternatives to passwords would not be a violation.

One commenter noted the Severe VSL is not consistent with the requirement and the SDT has updated the VSLs to align with modifications to the requirement.

Guideline

There was a recommendation that the guideline section needs to define generic accounts, and the SDT has added this to the guidelines.

Questions with Votes Only:

CIP-004, CIP-005, CIP-006 and CIP-007 Questions:

1. CIP-004-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
NESCOR/NESCO	No
ACES Power Marketing	No
Hydro One	No
Southern California Edison company	No
Progress Energy	No
Independent Electricity System Operator	No

Organization	Yes or No
NextEra Energy, Inc.	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
New York Power Authority	No
Springfield Utility Board	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC Registered Affiliates	Yes
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
Duke Energy	Yes
PNGC Comment Group	Yes

Organization	Yes or No
Dominion	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes

Organization	Yes or No
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes

Organization	Yes or No
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
MidAmerican Energy Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes

Organization	Yes or No
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Oncor Electric Delivery Company LLC	Yes
PJM Interconnection	Yes
NIPSCO	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes

Organization	Yes or No
Utility Services Inc	Yes
Alliant Energy	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

2. CIP-004-5 R2 states "Each Responsible Entity shall have a role-based cyber security training program to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
ACES Power Marketing	No

Organization	Yes or No
SPP and Member companies	No
IRC Standards Review Committee	No
CenterPoint Energy	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Arizona Public Service Company	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No

Organization	Yes or No
LCEC	No
Niagara Mohawk (dba National Grid)	No
National Grid	No
Snohomish County PUD	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Northeast Utilities	No
San Diego Gas & Electric	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No

Organization	Yes or No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Alliant Energy	No
New York Power Authority	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No
PNGC Comment Group	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc (NCR01177,	Yes

Organization	Yes or No
JRO00088)	
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes

Organization	Yes or No
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Lakeland Electric	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
PSEG	Yes
Texas Reliability Entity	Yes
NIPSCO	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes

Organization	Yes or No
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

3. CIP-004-5 R3 states "Each Responsible Entity shall implement its documented role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
ACES Power Marketing	No
IRC Standards Review Committee	No

Organization	Yes or No
CenterPoint Energy	No
PNM Resources	No
CIP Version 5 Comment SME list	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Northeast Utilities	No
Nebraska Public Power District	No

Organization	Yes or No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
Alliant Energy	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes

Organization	Yes or No
NRG Energy Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
SPP and Member companies	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Hydro One	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes

Organization	Yes or No
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
PSEG	Yes
Texas Reliability Entity	Yes
NIPSCO	Yes

Organization	Yes or No
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

4. CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
Texas RE NERC Standards Review Subcommittee	No
Colorado Springs Utilities	No
ACES Power Marketing	No
IRC Standards Review	No

Organization	Yes or No
Committee	
CenterPoint Energy	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Southern Company Services, Inc.	No
Southern California Edison company	No
Progress Energy	No
LCEC	No
Bonneville Power Administration	No
Snohomish County PUD	No
MidAmerican Energy Company	No

Organization	Yes or No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Utility Services Inc	No
New York Power Authority	No

Organization	Yes or No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
Southwest Power Pool Regional Entity	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes

Organization	Yes or No
NCEMC	Yes
SPP and Member companies	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Arizona Public Service Company	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Independent Electricity System Operator	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services	Yes

Organization	Yes or No
Corporation	
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
MEAG Power	Yes
Portland General Electric	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of	Yes

Organization	Yes or No
Water and Power	
US Bureau of Reclamation	Yes
California ISO	Yes

5. CIP-004-5 R5 states "Each Responsible Entity shall implement one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Texas RE NERC Standards Review Subcommittee	No
ACES Power Marketing	No
IRC Standards Review Committee	No
Salt River Project	No
Southern California Edison company	No
Progress Energy	No
LCEC	No
MidAmerican Energy	No

Organization	Yes or No
Company	
Lakeland Electric	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
PSEG	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Northeast Power Coordinating Council	Yes

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	Yes
NRG Energy Companies	Yes
Duke Energy	Yes
PNGC Comment Group	Yes
Dominion	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes

Organization	Yes or No
SPP and Member companies	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
BC Hydro	Yes
Hydro One	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Independent Electricity	Yes

Organization	Yes or No
System Operator	
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes

Organization	Yes or No
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
NIPSCO	Yes
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes

Organization	Yes or No
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

Organization	Yes or No
Kansas City Power & Light	Yes
California ISO	Yes

6. CIP-004-5 R6 states "Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R6?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
FirstEnergy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
Pepco Holdings Inc & Affiliates	No
SMUD & BANC	No

Organization	Yes or No
PNM Resources	No
CIP Version 5 Comment SME list	No
Southern Company Services, Inc.	No
Southern California Edison company	No
Progress Energy	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Xcel Energy	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Lakeland Electric	No
Ameren	No

Organization	Yes or No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
NYISO	No
Farmington Electric Utility System	No
Kansas City Power & Light	No
California ISO	No
Northeast Power Coordinating Council	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Hydro One	Yes
Arizona Public Service	Yes

Organization	Yes or No
Company	
Western Area Power Administration	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
NIPSCO	Yes
ISO New England Inc.	Yes

Organization	Yes or No
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes

Organization	Yes or No
US Bureau of Reclamation	Yes

7. CIP-004-5 R7 states "Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R7?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Colorado Springs Utilities	No

Organization	Yes or No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Florida Municipal Power Agency	No
SMUD & BANC	No
ACES Power Marketing	No
SPP and Member companies	No
Puget Sound Energy, Inc.	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Arizona Public Service Company	No
Southern Company Services, Inc.	No
Southern California Edison company	No

Organization	Yes or No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
ATCO Electric	No
LCEC	No
Consumers Energy Company	No
Xcel Energy	No
NV Energy	No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No

Organization	Yes or No
Lakeland Electric	No
Ameren	No
NextEra Energy, Inc.	No
Northeast Utilities	No
Texas Reliability Entity	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
MEAG Power	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Network & Security Technologies, Inc.	No
Alliant Energy	No
New York Power Authority	No
Springfield Utility Board	No
NYISO	No
Farmington Electric Utility System	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Los Angeles Department of Water and Power	No
Brazos Electric Power Cooperative	No
US Bureau of Reclamation	No
Kansas City Power & Light	No
California ISO	No

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	Yes
PNGC Comment Group	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Services	Yes

Organization	Yes or No
Corporation	
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
PSEG	Yes
Portland General Electric	Yes
Utility Services Inc	Yes
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes

Organization	Yes or No
Cowlitz County PUD	Yes

10. CIP-005-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
MRO NSRF	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
ACES Power Marketing	No

Organization	Yes or No
SPP and Member companies	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
CIP Version 5 Comment SME list	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Xcel Energy	No
Bonneville Power Administration	No
Tampa Electric Company	No
MidAmerican Energy	No

Organization	Yes or No
Company	
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Alliant Energy	No
New York Power Authority	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No

Organization	Yes or No
NRG Energy Companies	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Oncor Electric Delivery Company LLC	Yes

Organization	Yes or No
NIPSCO	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of	Yes

Organization	Yes or No
Water and Power	
US Bureau of Reclamation	Yes

11. CIP-005-5 R2 states "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No

Organization	Yes or No
ACES Power Marketing	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
Progress Energy	No
Hydro-Quebec TransEnergie	No
Lincoln Electric System	No
Bonneville Power Administration	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No

Organization	Yes or No
PSEG	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
New York Power Authority	No
NYISO	No
Tucson Electric Power	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
Southwest Power Pool Regional Entity	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Southern California Edison company	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba	Yes

Organization	Yes or No
National Grid)	
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
NIPSCO	Yes
MEAG Power	Yes

Organization	Yes or No
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

14. CIP-006-5 R1 states "Each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards	No

Organization	Yes or No
Review Subcommittee	
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Florida Municipal Power Agency	No
NCEMC	No
ACES Power Marketing	No
SPP and Member companies	No
IRC Standards Review Committee	No
CenterPoint Energy	No
Puget Sound Energy, Inc.	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Arizona Public Service	No

Organization	Yes or No
Company	
Southern Company Services, Inc.	No
Western Area Power Administration	No
Salt River Project	No
National Rural Electric Cooperative Association (NRECA)	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Lower Colorado River Authority	No
LCEC	No
LCRA Transmission Services Corporation	No

Organization	Yes or No
Lincoln Electric System	No
United illuminating Company	No
Xcel Energy	No
NV Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Lakeland Electric	No
Tennessee Valley Authority	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Northeast Utilities	No
PSEG	No

Organization	Yes or No
San Diego Gas & Electric	No
Texas Reliability Entity	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
MEAG Power	No
Portland General Electric	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Alliant Energy	No

Organization	Yes or No
Pacific Gas and Electric Company	No
NYISO	No
Exelon Corporation and its affiliates	No
Deseret Power	No
Los Angeles Department of Water and Power	No
Brazos Electric Power Cooperative	No
US Bureau of Reclamation	No
Kansas City Power & Light	No
California ISO	No
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Pepco Holdings Inc & Affiliates	Yes
Tri-State G&T - Transmission	Yes

Organization	Yes or No
Southern California Edison company	Yes
Clallam County PUD No.1	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
The Empire District Electric Company	Yes
Utility Services Inc	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Farmington Electric Utility	Yes

Organization	Yes or No
System	
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes

15. CIP-006-5 R2 states "Each Responsible Entity shall implement one or more documented visitor control programs that include each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Duke Energy	No
Dominion	No
Florida Municipal Power Agency	No
PNM Resources	No
BC Hydro	No
Western Area Power Administration	No
Progress Energy	No
Independent Electricity	No

Organization	Yes or No
System Operator	
Hydro-Quebec TransEnergie	No
LCEC	No
Xcel Energy	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Lakeland Electric	No
NextEra Energy, Inc.	No
PJM Interconnection	No
Wisconsin Electric Power Company	No
Portland General Electric	No
City Utilities of Springfield, MO	No
NYISO	No
Exelon Corporation and its	No

Organization	Yes or No
affiliates	
Deseret Power	No
Los Angeles Department of Water and Power	No
California ISO	No
Northeast Power Coordinating Council	Yes
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC)	Yes

Organization	Yes or No
including OPC, GTC & GSOC	
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Hydro One	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes

Organization	Yes or No
Southern California Edison company	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power	Yes

Organization	Yes or No
Administration	
Snohomish County PUD	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Oncor Electric Delivery Company LLC	Yes
NIPSCO	Yes
City of Austin dba Austin Energy	Yes

Organization	Yes or No
ISO New England Inc.	Yes
MEAG Power	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

Organization	Yes or No
Kansas City Power & Light	Yes

16. CIP-006-5 R3 states "Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
NESCOR/NESCO	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
IRC Standards Review Committee	No
CenterPoint Energy	No

Organization	Yes or No
PNM Resources	No
Hydro One	No
Western Area Power Administration	No
Progress Energy	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
LCEC	No
Xcel Energy	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Lakeland Electric	No
NextEra Energy, Inc.	No

Organization	Yes or No
Texas Reliability Entity	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
Portland General Electric	No
City Utilities of Springfield, MO	No
New York Power Authority	No
Los Angeles Department of Water and Power	No
PPL Corporation NERC Registered Affiliates	Yes
Duke Energy	Yes
Dominion	Yes
FirstEnergy	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Southern California Edison company	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
NIPSCO	Yes
MEAG Power	Yes
Network & Security	Yes

Organization	Yes or No
Technologies, Inc.	
Utility Services Inc	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

Organization	Yes or No
Kansas City Power & Light	Yes
California ISO	Yes

18. CIP-007-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Florida Municipal Power Agency	No
SMUD & BANC	No

Organization	Yes or No
CenterPoint Energy	No
PNM Resources	No
Western Area Power Administration	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
LCEC	No
Consumers Energy Company	No
Xcel Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
MidAmerican Energy	No

Organization	Yes or No
Company	
Lakeland Electric	No
NextEra Energy, Inc.	No
PJM Interconnection	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
NYISO	No
Exelon Corporation and its affiliates	No
Kansas City Power & Light	No
California ISO	No
Northeast Power Coordinating Council	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
MRO NSRF	Yes

Organization	Yes or No
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Hydro One	Yes
CIP Version 5 Comment SME list	Yes

Organization	Yes or No
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
NV Energy	Yes

Organization	Yes or No
Snohomish County PUD	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Oncor Electric Delivery Company LLC	Yes
NIPSCO	Yes
City of Austin dba Austin Energy	Yes

Organization	Yes or No
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

19. CIP-007-5 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
SMUD & BANC	No
CenterPoint Energy	No
PNM Resources	No

Organization	Yes or No
Hydro One	No
Arizona Public Service Company	No
Western Area Power Administration	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Hydro-Quebec TransEnergie	No
LCEC	No
Lincoln Electric System	No
Xcel Energy	No
Bonneville Power Administration	No
Tampa Electric Company	No
MidAmerican Energy Company	No

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Utility Services Inc	No
Alliant Energy	No
New York Power Authority	No

Organization	Yes or No
Pacific Gas and Electric Company	No
NYISO	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Kansas City Power & Light	No
PPL Corporation NERC Registered Affiliates	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
Dominion	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power	Yes

Organization	Yes or No
Agency	
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Independent Electricity System Operator	Yes

Organization	Yes or No
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
NIPSCO	Yes
MEAG Power	Yes
Portland General Electric	Yes
Springfield Utility Board	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power	Yes

Organization	Yes or No
Cooperative	
US Bureau of Reclamation	Yes
California ISO	Yes

20. CIP-007-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
SPP and Member companies	No
CenterPoint Energy	No

Organization	Yes or No
PNM Resources	No
Hydro One	No
CIP Version 5 Comment SME list	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Bonneville Power Administration	No
Snohomish County PUD	No
MidAmerican Energy Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No

Organization	Yes or No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Alliant Energy	No
New York Power Authority	No
Pacific Gas and Electric Company	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC	Yes

Organization	Yes or No
Registered Affiliates	
NRG Energy Companies	Yes
PNGC Comment Group	Yes
Dominion	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes

Organization	Yes or No
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes

Organization	Yes or No
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes

Organization	Yes or No
NIPSCO	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes

Organization	Yes or No
US Bureau of Reclamation	Yes

21. CIP-007-5 R4 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No

Organization	Yes or No
SMUD & BANC	No
SPP and Member companies	No
IRC Standards Review Committee	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
CIP Version 5 Comment SME list	No
Western Area Power Administration	No
Salt River Project	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No

Organization	Yes or No
Hydro-Quebec TransEnergie	No
Lower Colorado River Authority	No
LCEC	No
LCRA Transmission Services Corporation	No
Niagara Mohawk (dba National Grid)	No
National Grid	No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Lakeland Electric	No

Organization	Yes or No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
PSEG	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Utility Services Inc	No

Organization	Yes or No
Alliant Energy	No
New York Power Authority	No
Pacific Gas and Electric Company	No
NYISO	No
Tucson Electric Power	No
Los Angeles Department of Water and Power	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC Registered Affiliates	Yes
PNGC Comment Group	Yes
Dominion	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes

Organization	Yes or No
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Clallam County PUD No.1	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
United illuminating Company	Yes
Xcel Energy	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
MEAG Power	Yes
Portland General Electric	Yes
Springfield Utility Board	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes

Organization	Yes or No
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

22. CIP-007-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No

Organization	Yes or No
SMUD & BANC	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
Southern Company Services, Inc.	No
Salt River Project	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Lower Colorado River Authority	No
LCRA Transmission Services Corporation	No
Consumers Energy Company	No

Organization	Yes or No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Lakeland Electric	No
Tennessee Valley Authority	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No

Organization	Yes or No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
Portland General Electric	No
City Utilities of Springfield, MO	No
Alliant Energy	No
New York Power Authority	No
NYISO	No
Tucson Electric Power	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC Registered Affiliates	Yes
PNGC Comment Group	Yes
Associated Electric	Yes

Organization	Yes or No
Cooperative, Inc (NCR01177, JRO00088)	
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Western Area Power Administration	Yes
Clallam County PUD No.1	Yes
Hydro-Quebec TransEnergie	Yes
ATCO Electric	Yes
LCEC	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Northeast Utilities	Yes
PSEG	Yes

Organization	Yes or No
Texas Reliability Entity	Yes
NIPSCO	Yes
MEAG Power	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

Organization	Yes or No
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards
Comment Form C
CIP-008 through CIP-011

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Index to Questions, Comments, and Responses

Questions with Summaries Included: 16
QUESTION C4 – CIP-008-5: 16
QUESTION C8 – CIP-009-5: 26
QUESTION C12 – CIP-010-1: 39
QUESTION C15 – CIP-011-5: 63
Questions with Votes Only: 71
1. CIP-008-5 R1 states "Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 71
2. CIP-008-5 R2 states "Each Responsible Entity shall implement its documented Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 78
3. CIP-008-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?..... 85
5. CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?..... 92
6. CIP-009-5 R2 states "Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 99
7. CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3? 106
9. CIP-010-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration

Change Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 113

10. CIP-010-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 120

11. CIP-010-1 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3? 127

13. CIP-011-1 R1 states "Each Responsible Entity shall implement an information protection program that includes each of the applicable items in CIP-011-1 Table R1 – Information Protection." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 134

14. CIP-011-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 141

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Bruce Metruck	New York Power Authority	NPCC	6
12.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
13.	Robert Pellegrini	The United Illuminating Company	NPCC	1
14.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
15.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
16.	Brian Robinson	Utility Services	NPCC	8
17.	Michael Jones	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Don Weaver	New Brunswick System Operator	NPCC	2
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3
24.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5

2.	Group	Annabelle Lee	NESCOR/NESCO									

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3.	Group	Jason Marshall	ACES Power Marketing					X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6. Shari Heino		Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Tim Soles	Occidental Power Services, Inc.	ERCOT	3
4.	Andy Gallo	Austin Energy	ERCOT	1
5.	Andy Gallo	Austin Energy	ERCOT	3
6.	Andy Gallo	Austin Energy	ERCOT	4
7.	Andy Gallo	Austin Energy	ERCOT	5
8.	Andy Gallo	Austin Energy	ERCOT	6

8.	Group	Emily Pennel	Southwest Power Pool Regional Entity									X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8. Annie Terracciano	Northern Lights Inc.	WECC 3										
9. Aleka Scott	PNGC	WECC 4										
10. Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11. Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12. Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13. Margaret Ryan	PNGC	WECC 8										
12. Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13. Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14. Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. M & A Electric Power Cooperative		SERC 1, 3										
4. Northeast Missouri Electric Power Cooperative		SERC 1, 3										
5. N.W. Electric Power Cooperative, Inc.		SERC 1, 3										
6. Sho-Me Power Electric Cooperative		SERC 1, 3										
15. Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X						
Additional Member	Additional Organization	Region Segment Selection										
1. Oglethorpe Power Corporation		SERC 5										
2. Georgia Transmission Corporation		SERC 1										
16. Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X
Additional Member	Additional Organization	Region Segment Selection										
1. MAHMOOD SAFI	OPPD	MRO 1, 3, 5, 6										
2. CHUCK LAWERENCE	ATC	MRO 1										
3. TOM WEBB	WPS	MRO 3, 4, 5, 6										
4. JODI JENSON	WAPA	MRO 1, 6										
5. KEN GOLDSMITH	ALTW	MRO 4										
6. DAVE RUDOLPH	BEPC	MRO 1, 3, 5, 6										
7. JOE DEPOORTER	MGE	MRO 3, 4, 5, 6										
8. SCOTT NICKELS	RPU	MRO 4										
9. TERRY HARBOUR	MEC	MRO 1, 3, 5, 6										
10. MARIE KNOX	MISO	MRO 2										
11. LEE KITTELSON	OTP	MRO 1, 3, 4, 5										
12. SCOTT BOS	MPW	MRO 6, 1, 3, 5										
13. TONY EDDLEMAN	NPPD	MRO 1, 3, 5										
14. THERESA ALLARD	MPC	MRO 1, 3, 5, 6										
17. Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing												
18. Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Timothy Beyrle	City of New Smyrna Beach	FRCC 4										
2. James Howard	Lakeland Electric	FRCC 3										

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. Greg Woessner	Kissimmee Utility Authority	FRCC	3									
4. Lynne Mila	City of Clewiston	FRCC	3									
5. Joe Stonecipher	Beaches Energy Services	FRCC	1									
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4									
7. Randy Hahn	Ocala Utility Services	FRCC	3									
19. Group	Joseph DePoorter	Madison Gas and Electric Company			X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Darl Shimko	MGE	MRO	3									
2. Joseph DePoorter	MGE	MRO	4									
3. Steve Schultz	MGE	MRO	5									
4. Jeff Keebler	MGE	MRO	6									
20. Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Mark Jones	Pepco	RFC	1									
21. Group	Rick Terrill	Luminant					X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Mike Laney	Luminant Generation Company LLC	ERCOT	5									
2. Tim Soles	Occidental Power Services, Inc.	ERCOT	6									
3. Tim Soles	Occidental Power Services, Inc.	ERCOT	3									
4. Andy Gallo	Austin Energy	ERCOT	1									
5. Andy Gallo	Austin Energy	ERCOT	3									
6. Andy Gallo	Austin Energy	ERCOT	4									
7. Andy Gallo	Austin Energy	ERCOT	5									
8. Andy Gallo	Austin Energy	ERCOT	6									
9. Brenda Hampton	Luminant Energy Company LLC											
22. Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Kevin Smith	BANC	WECC	1									
23. Group	Scott Brame	NCEMC	X				X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				

Additional Member	Additional Organization	Region	Segment Selection
1. Rayburn Country Electric Cooperative		SPP	
2. Empire District Electric		SPP	1
3. City Utilities of Springfield		SPP	4
4. Westar Energy		SPP	1, 3, 5, 6
5. Cleco Power		SPP	1, 3, 5, 6

25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						

Additional Member	Additional Organization	Region	Segment Selection
1. Pawel Krupa		WECC	1
2. Dana Wheelock		WECC	3
3. Hao Li		WECC	4

27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					

Additional Member	Additional Organization	Region	Segment Selection
1. Denise Lietz	Puget Sound Energy	WECC	1
2. Erin Apperson	Puget Sound Energy	WECC	3

28.	Group	Michael Mertz	PNM Resources	X		X							

Additional Member	Additional Organization	Region	Segment Selection
1. Laurie Williams	Public Service Co. of New Mexico	WECC	1
2. Michael Mertz	Public Service Co. of New Mexico	WECC	3

29.	Group	Sasa Maljukan	Hydro One	X									

Additional Member	Additional Organization	Region	Segment Selection
1. David Kiguel	Hydro One	NPCC	1

30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION C4 – CIP-008-5:

If you disagree with the changes made to CIP-008-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, most of the comments resulted in changes that improved clarity and did not require significant structural revisions. The consideration of comments according to major issues and standard sections follows.

References to EOP-004-2

The comments received for CIP-008-5 and EOP-004-2 both indicated support for handling the reporting of Cyber Security Incidents in CIP-008-5. EOP-004-2 received a much lower ballot approval in its most recent posting primarily for the one hour timeframe required for reporting Cyber Security Incidents. The commenters concern for EOP-004-2 was the lack of a timeframe for identifying a Cyber Security Incident. The required CIP-008-5 processes make clear that reporting to the ES-ISAC occurs within one hour of the analysis to determine whether an event would constitute a Cyber Security Incident. As a result, both drafting teams agreed to move the Cyber Security Incident reporting to the ES-ISAC to CIP-008-5. However, the SDT wishes to stress the reporting threshold is not necessarily one hour from the Cyber Security Incident occurrence. Instead, the threshold accounts for the analysis that must be performed in identifying the Cyber Security Incident. The incident could even have occurred much earlier without any observable behavior. Also, entities can still have a single reporting process to comply with the new versions of EOP-004 and CIP-008.

Applicability Section

Several commented that all instances of Medium Impact BES Cyber Systems should be changed to “Medium Impact BES Cyber Systems with External Routable Connectivity”. In response, we note that CIP-008-5 addresses incident response and reporting and the lack of external routable connectivity would not address this issue. It is possible for a Cyber Security Incident to occur on such cyber systems through insider attacks or other means of penetrating the physical or electronic boundaries. This does not create an inconsistency among the standards or implied requirement for monitoring because an entity can have a monitoring program to detect incidents that does not fully meet the requirements of CIP-006-5 and CIP-007-5.

There were several comments that stated CIP-008-5 should apply to Electronic Access Control and Monitoring Systems and Physical Access Control Systems. In response, applicability to these systems is unnecessary because the incident is associated to the BES Cyber Systems. Incidents occurring on perimeter systems would target the system and not the perimeter.

Other General Comments

One commenter requested clarification why the word "dated" has been added to the measures in these requirements. In response, dated documentation is used to clarify that such evidence is necessary to demonstrate time-based requirements.

There was a comment that suggested the word "annual" should be a defined in the NERC Glossary. In response, the SDT has chosen not to define annual because the periodicity for requirements in CIP may be different than requirements in other standards, and the definition of annual may have many interpretations.

Guidelines

One commenter suggested that references to DHS and NIST should not reside in the standard because NERC does not track those documents to ensure consistency. In response, the external references are dated to a specific version to address the case where future revisions do not remain consistent with the standard.

There was a comment that the definition of Reportable Cyber Security Incident is too vague and could result in the interpretation that activation of redundant systems causes the reporting not to be considered. In response, the SDT has clarified in the guideline that this is not the case. The SDT has added a clarification that the absence of lessons learned must still be documented.

One commenter proposed revisions requirements to "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has considered this approach and has added to certain requirements "… identify, assess, and correct deficiencies…", which is explained in detail in the global summary portion of this document, above.

Background

One commenter stated that the background section for CIP-008-5 is contradictory in reference to measures by stating a numbered list is all-inclusive but measures serve only as examples. In response, the SDT notes that the background section states "A numbered list in the measure means the evidence example". This means the example evidence must include all of the items, but there may be other examples of evidence to meet the requirement. Both statements are true.

Requirement Part 1.1 and 1.2
Based on a comment, the SDT changed "Processes" to "One or more processes" for clarity.

Several commenters propose including additional specificity in the process for determining if an incident is reportable. The SDT has extensively discussed this issue, and the problem with additional specificity in Cyber Security Incidents is difficulty in exhaustively enumerating situations to report. Also, the reporting of incidents associated with damage alone can result in under-reporting, which does not meet the objective of this Requirement.

Requirement Part 1.4
Several commenters stated that 1.1 (responding) and 1.4 (handling) are essentially the same and proposed to delete 1.4**.** The SDT notes that while 1.1 addresses the initial identification and response to incidents, 1.4 addresses the actions to perform for resolving individual incidents. These are distinct activities.

One commenter suggested the that the applicability include low impact BES Cyber Systems because CIP-003-5 requires implementation of a policy addressing incident response, but CIP-003-5 intentionally centralizes all the requirements for low impact BES Cyber Systems which does not include specific elements of the plan.

There was a comment that suggested removing the parenthetical phrase for incident handling because recovery and post-incident analysis are covered elsewhere. In response, the SDT agrees that post-incident analysis is already handled in Requirement R3 of CIP-008-5 and clarifies the recover activities here pertain only to the incident. Recovery includes the confirmation that the incident has been resolved.

One commenter suggested adding wording to clarify physical security incidents need to be considered. In response, the SDT notes that the definition of Cyber Security Incidents includes physical intrusions.

Requirement Part 1.5

There was a comment that stated it is unclear if the list of internal and external contacts refer to those in EOP-004-2 or if there is a need to have a minimum list of contacts. In response, the internal or external contacts that an entity would need to include to ensure proper reporting for EOP-004-2 should be part of this list. Additional contacts are appropriate as necessary components of an incident response plan, but who resides in this list is left up to the entity.

A commenter suggested that the use of external organizations could result in double jeopardy with EOP-004-2. However, EOP-004-2 requires specific organizations whereas CIP-008-5 leaves the inclusion of additional external organizations up to the entity as a necessary part of the incident response plan. Double jeopardy does not exist here because there is not a requirement in CIP-008-5 to report.

One commenter proposed to replace the phrase "should receive communication" with "must be sent communication". In response, the SDT notes that this part of the incident response plan does not necessarily constitute required communication, but communication must be covered as a component of the plan.

Requirement R2

One commenter proposed adding an exception for the timeframes based on CIP Exceptional Circumstances. In response, the SDT notes that CIP Exceptional Circumstances have not applied to annual periodic performances requirements because of the flexibility in the timeframe of when an entity can perform this requirement.

Requirement Part 2.1

In response to a comment that 2.1 should expand to include all Cyber Security Incidents, the SDT continues to limit these requirements to Reportable Cyber Security Incidents because of the lessons learned and plan updates associated with each Reportable Cyber Security Incident. It is possible for Cyber Security Incidents to occur much more frequently.

In response to a comment, the SDT has removed the word "BES" before "BES Incident Response Plan" for consistency.

One commenter suggested revising the language of "at least once each calendar year, not to exceed 15 calendar months between executions" to "once each calendar year or a period not to exceed 15 calendar months between executions". The SDT notes that the language that exists is sufficient as currently written.

One commenter suggested using the term “exercise” instead of “test” because an actual exercise would suffice. In response, we had several comments to the contrary in the previous posting. The SDT uses test here because the word “exercise” is commonly used in reference to a planned execution.

One commenter suggested removing the lessons learned report from the measure because it is not part of the requirement. In response, we note that the measure only serves as an example, and a lessons-learned report would be an example measure for 2.1.

One commenter suggested that a full operational exercise should be required in the absence of an actual incident. In response, we suggest that the quality of an exercise does not depend on the type. It is possible to have a higher quality tabletop exercise than a full operational exercise.

One commenter suggested placing an “or” between all exercise examples, but this is not necessary because the “or” in the second bullet qualifies the entire list.

One commenter suggested expanding the scope of actual incidents that qualify as an exercise to include any Cyber Security Incident, but this would not exercise a key component of identifying and communicating a Reportable Cyber Security Incident.

One commenter proposed to remove any timeframes associated with the test. The SDT disagrees because absence of time requirements makes the expected performance of the standard less clear and does not respond to directives from the FERC Order 706.

Two commenters suggested adding a specific reference to R1 to clarify the linkage, but the context of the Requirement in its use of Cyber Security Incident response plan is clear enough to avoid needing a direct linkage.

In response to several commenters, the word “plan(s)” was modified to “each plan” for added clarity.

In response to one commenter, the SDT qualified that the phrase “when responding to” is in regards to the Reportable BES Cyber Security Incident.

Based on comments, the SDT clarified exercises were for Reportable Cyber Security Incidents.

Based on comments, the SDT has removed the word “BES” from this requirement part.

Requirement Part 2.2
One commenter stated that this requirement part should be deleted because the main requirement part already addresses implementation and documented deviations are redundant with lessons learned. In response, the SDT points out that implementation of the plan does not necessarily mean that it be used during an incident or exercise. Some entities may interpret that a plan is implemented regardless of whether or not it is actually used. This additional requirement adds clarity in the expected outcome. The same is also true of lessons learned not having the full meaning of documenting deviations from the plan. However, we agree that the documentation should not necessarily occur concurrent with the incident and have modified this requirement part accordingly.

One commenter suggested requiring documentation for the lack of deviations from the plan. In response, we do not agree this language is necessary. The absence of deviations may be a common occurrence and the requirement to have such documentation is highly administrative. We believe this is different than the case of not having any lessons learned which should be a much less common occurrence.

One commenter suggested requiring plan updates for new vulnerabilities and threats. The SDT agrees this would be appropriate if the plan were not sufficient to address new vulnerabilities and threats, but measurable criteria for what constitutes a new vulnerability or threat does not exist and could likely not be determined by anyone other than the Responsible Entity.

In response to a comment, the SDT replaced the phrase “incident response plan” with “Cyber Security Incident response plan” for consistency.

In response to several commenters, the word “plan” was changed to “plan(s)” for consistency.

Requirement Part 2.3
One commenter proposed that 2.3 should be moved to the compliance evidence section of the standard. In response, the evidence retention section cannot add a new requirement, and without 2.3 there is no requirement to retain evidence of the incident.

Several commenters suggested the language for requirement part 2.3 include a retention period, but this requirement was modified in response to comments that the retention period be covered in the compliance evidence section of the standard. As a result, part 2.3 includes the requirement to retain the records, which may not have been necessary to retain anywhere else in the standard, and the compliance evidence section defines the retention period.

There were several commenters who stated that this requirement part could have double jeopardy with EOP-004-2, but lack of documentation for reporting purposes would not be a violation of CIP-008-5. Also, EOP-004-2 evidence retention does not necessarily cover evidence related to a Cyber Security Incident.

One commenter suggested storing the evidence in encrypted form. In response, CIP-011-1 addresses the storage of BES Cyber System Information. Specific implementation of this requirement is appropriately left to the entity.

The SDT has removed the word “relevant” responding to comments that it adds unneeded subjectivity.

One commenter questioned whether three calendar years is sufficient for retaining incident evidence for law enforcement, state, and federal requirements, but the evidence retention is a minimum for the purpose of the Standard. If additional requirements outside of the NERC Reliability Standards indicate a longer retention period for a particular entity, then the entity would choose the longer period. There is no conflict.

Requirement R3

One commenter proposed that the main requirement should more closely align with CIP-009-5 R3 and focus on maintaining, and not implementing, the plan. The SDT agrees.

One commenter suggested the word “full” be deleted from “full operational exercise” because it is unclear what it implies. The SDT agrees.

Requirement Part 3.1

Several entities have commented this requirement part is duplicative with testing in R2 and monitoring for plan changes in R3. The SDT agrees and has deleted this requirement part.

In response to a comment that proposed to consider additional changes that trigger a review of the incident response plan, the lessons learned requirements suffice for updating the plan in response to incidents. Changes to the security

configuration already trigger updates in requirement part 3.4. In many cases the incident response plan is written at a high enough level to preclude necessitating changes in response to new threats and vulnerabilities.

Requirement Part 3.2

There were several comments that the various dates for updating the plan significantly increase the compliance tracking burden and that a plan has not truly updated until the entity distributes those updates to the required individuals. The SDT agrees and has collapsed previously posted requirement parts 3.2, 3.3 and 3.5 into a single requirement part 3.1. The additional requirement part 3.4 for monitoring plan changes and 3.5 has collapsed into a single requirement part 3.2. Some commenters suggested that both requirements should allow a consistent 90 days, but the updating of the plan in response to changes does not require the same level of updates as those required from lessons learned. Therefore the different timeframes in these requirement parts are appropriate.

One commenter suggested tying this requirement explicitly with both 2.1 and 2.2. In response, the cross-referencing of requirements could cause more confusion than clarity. The SDT feels this explicit tie is best accomplished in the guidance.

One comment proposed to remove any timeframes associated with plan updates. The SDT disagrees because absence of time requirements makes the expected performance of the standard less clear and does not respond to directives from the FERC Order 706.

There was a comment that suggested that 30 days may not be sufficient time to make complex changes from lessons learned. In response, the SDT believes the updated requirement allowing 90 days for the complete time is sufficient for even complex changes.

One commenter suggested changing this requirement part to include language for consistency with the ERO Event Analysis Process. The ERO Events Analysis Process is not a NERC Reliability Standard, and the SDT is not mandating referenced actions that are not developed through the NERC process or an equivalent ANSI Certified process. The SDT also notes that the proposed requirement language leaves flexible “how” to perform the requirement. Entities may choose to follow the procedures outlined in the ERO Events Analysis Process to comply with the requirement, but are not required to. The SDT also understands that the NERC CIPC is planning to form a working group to develop guidelines for analyzing cybersecurity events using a parallel process to the recently approved ERO Events Analysis Process. Specifying

that the ERO Events Analysis Process be used in response to CIP-008 Reportable Cybersecurity Incidents is premature and will remove any perceived or required flexibility in developing cybersecurity-specific procedures under that group.

Several commenters suggested clarifying the expectation when there are no lessons learned. In response, we have made this explicit in both the requirement and measure.

In response to one comment, the SDT has added examples of evidence for lessons learned.

In responses to multiple comments, the SDT changed the phrase “within 90 days” to “not to exceed 90 calendar days” for clarity.

Requirement Part 3.3
In response to a comment, it is not necessary to modify this requirement to state “update as needed” because the requirement part ties to “any lessons learned” which carries the same effect.

Requirement Part 3.4
One commenter suggested reverting to previously approved language for updates and notes that evidence to meet this requirement would include lists of technology changes. In response, the SDT notes that such evidence would be required in the previously approved version if specific technology was referenced in the plan. The changes identified here are to provide additional clarity in the types of changes that should trigger an update.

Several commenters proposed that the term “technology changes” needs to be defined. The SDT notes this only includes technology changes that would impact the ability to execute the plan. Because this term is so contextual to the plan, it would cause more problems to define it. Entities should review their plans to see whether or not they have technology as a key element of the plan. The guidance specifies that “technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.”

Requirement Part 3.5
Several commenters suggested changing the word “distribute” to “notify” for announcing changes to the incident response plan due to the uncertainty of what constitutes distribution and the possible issues with information sensitivity. The SDT agrees.

One commenter suggested the evidence examples of distributing the plan could result in a violation of confidentiality, but, while each example can specify additional mechanisms to preserve confidentiality, this was not the intention of the measure. In some cases, incident response plans may not contain confidential information.

VSLs

One commenter recommended that the documentation of the absence of any lessons learned should be included in the VSLs. In response, the absence of lessons learned has been included in the VSL.

One commenter recommended that the VSL should not include failure to follow the plan during an incident and the VSL associated with lack of documentation of deviations suffices. The SDT agrees and does not need to modify the VSLs.

QUESTION C8 – CIP-009-5:

If you disagree with the changes made in CIP-009-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the primary concerns regarding CIP-009-5 expressed in comments were (1) backup media verification procedures in requirement parts 1.4 and 2.2, (2) data preservation procedures in 1.5 and (3) timeframe requirements in Requirement R3 on the lessons learned and plan update activities. The consideration of comments according to major issues and standard sections follows.

Applicability

One commenter suggested that the applicability for all requirements in this standard should limit to Medium Impact BES Cyber Systems at Control Centers to appropriately focus on the higher risk cyber systems and avoid conflict with PRC Standards. In response, the loss of Medium Impact BES Cyber Systems has impact to the BES and the recovery operation for these cyber systems should be addressed in this standard.

The applicability is limited to high impact and medium impact at control centers, along with their associated EACs and PACs, which means testing for substations and generating plants that are not high impact is not included. A commenter asked for confirmation on whether this was the SDT's intent. Yes, it was.

One comment suggested that applicability to associated Cyber Assets should be removed because the FERC has not directed to do so. In response, these continue to apply from all prior versions to the associated Cyber Assets.

Other General Comments

One commenter proposed modifying the main requirement part and corresponding VSLs for R2 and R3 to allow for a flaw remediation process. In response, we have modified the main requirement part for R2 to eliminate the zero tolerance obligations because of the possible magnitude of plans and backup media which require testing. However, we do not incorporate the same changes for R3 because the requirements here do not have the same zero-tolerance concerns and they specify the procedures that must be in place to ensure better response plan flaw remediation.

Guidelines

Several commented that application guidelines should be included for CIP-009-5, and we have added these.

Background

One commenter suggested that the background section is contradictory by saying that measures are not all-inclusive but numbered list provide an all-inclusive example. In response, the background section states, "A numbered list in the measure means the evidence example includes all of the items in the list." This refers to the single example and is different than an all-inclusive list of evidence examples. Accordingly, if an entity did not provide all parts of the numbered list of evidence, then they would not fully meet the requirement. However, they could still provide alternate forms of evidence outside of the example.

Measures

There was a comment that the measures should be clarified with the following language: "Evidence may include, but is not limited to, a dated, revised Cyber Security Incident Response Plan(s) that (1) includes or references, as appropriate, dated documentation of lessons learned, if any, associated with tests of or actual responses using the Cyber Security Incident Response Plan(s), within 90 days after completion of such test or actual incident response; and (2) reflects changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change." The SDT notes that the language in the requirement is clear and that the measures provide adequate examples of evidence. Each requirement part addresses different levels of that may be expected.

Requirement R1

One comment proposed to add a requirement for restoring the BES Cyber System to a state where it is ready to assume its normal operating role in all respects. They also commented that the requirement should state the level of granularity required for a plan. In response, it would be problematic to standardize and audit a normal operating role. The SDT is uncertain as to the meaning of this term. The purpose of this standard is "to recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES." It is inappropriate to specify the level of detail required for a recovery plan.

Several commenters suggested that the standard is not clear whether the recovery plans are for recovery of the asset, system, or function. In response, the stated purpose for the standard is "to recover reliability functions performed by

BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES."

One commenter asked the following: "is a Business Continuity Plan, where operations are transferred from the main control center and continued at a back-up control centre, considered a recovery plan?" In response, this could constitute a recovery plan according to Requirement R1 with the additional components listed in the requirement parts. However, restoration of the reliability function meets the purpose of this standard.

Requirement Part 1.1
One commenter suggested removing "specific" activations from the measure, and we have done so.

One commenter suggested the minimum conditions for activating a response should be specified. Otherwise entities can choose an inappropriately high bar. In response, any minimum enumeration of recovery conditions would equate to defining system failure and doing so for a highly variant population of systems across the BES is not feasible.

Requirement Part 1.3
Several commenters suggested changing the phrase "BES Cyber System" to "applicable Cyber Assets". However, "restoring BES Cyber System" functionality describes the objective of the requirement part and not the applicability.

One commenter suggested addressing FERC Order 706 paragraph 748 by appending the suggested text from the Order to this Requirement Part addressing backup media. We agree this is clearer and have incorporated their suggestion in requirement part 1.4 because of the difference in applicability from 1.3.

One commenter suggested modifying this requirement part measure to provide alternate forms of evidence and avoid the interpretation that evidence must be shown for each occurrence in a high-frequency operational requirement. In response, the SDT has modified the measure according to these suggestions.

Several commenters suggested removing the qualifier word "successfully" from the measure and the SDT has done so.

One commenter suggested including documented configuration settings, documented build/restoration procedures, and retention of installation media for example evidence. The SDT has added these to the technical guidelines section of the standard.

Several commenters suggested replacing the word “recover” with “restore” to describe the purpose of the backup media. In response, we retain the use of “recover” to avoid confusion. Both words mean to return something to a normal or former condition, and the SDT finds these words can be used interchangeably while still communicating the same concept.

One commenter noted the measure is missing an “and”, and the SDT has corrected this oversight.

Requirement Part 1.4

Several commenters expressed confusion around the term “initially” in the requirement, and the SDT has removed this term by tying the verification processes to the backup and storage processes in 1.3. The resulting language should provide more clarity and eliminates the term “initially”.

One commenter suggested addressing FERC Order 706 paragraphs 732-734 in this requirement section or moving this to guidance. In response, the resulting directive in paragraph 739 is addressed by the proposed text to address 748. Another commenter also supported the proposed language in the FERC Order. In response, verifying the operability of backup media is addressed by verifying successful completion and addressing failures of the backup process. Short of performing a full restoration, monitoring the backup process provides the appropriate assurance in the integrity of the backup for constantly changing systems. We have also added further guidance for this requirement part.

One commenter stated that FERC did not express concern over Physical Access Control Systems and Electronic Access Control and Monitoring Systems and applicability for these should be removed. In response, we retain the applicability from previous versions of the standard to which the FERC Order was addressed.

Several commenters requested further clarification about the meaning of verification of backup media. In response, the verification of backup media is dependent upon the tool performing the backup. This could include checking for read/write errors or performing a checksum during the backup operation. The SDT has clarified this requirement to read verification of successful completion.

One commenter suggested this requirement part be modified to address 3rd parties performing the backup or providing a backup, and the requirement has been modified to address these concerns.

Several commented on the 90 day retention period for the logs specified in this requirement part measure. In response, the reason for having 90 day retention for BES Cyber System logs is the potentially large volume, but there is no such concern for the evidence example for this requirement part.

One commenter does not believe this requirement part belongs as written here, and we note the overall modifications to this requirement part better fits the overall objective of Requirement R1.

One commenter stated that the term "backup media" is antiquated and should be replaced with redundancy terminology. In response, we disagree the term is antiquated, but if redundancy is being used for recovery, then processes should exist to regularly verify the redundancy and address failures.

One commenter asked the following questions: If a single monthly backup succeeds, is that good enough? What is verified initially? Is this a daily check for backups or is weekly verification sufficient? If a log is printed or a snapshot taken monthly for evidence sufficient if alerting to x-number of failures is part of the process or is evidence collection required upon completion of the backup? In response to these questions, the currently proposed requirement does not specify a timing that is sufficient for verification due to the widely varying backup methodologies that exist for the applicable systems. A printed log or periodic automated sampling of the backup process would be considered sufficient evidence for this requirement.

One commenter stated that the only way to verify backup completion is to restore from backup. In response, completion of the backup process or routine is different than successful restoration, and we contend the former can be verified outside of a full restoration.

Requirement Part 1.5

Several commenters suggested replacing the word "event" with the phrase "Cyber Security Incident" to better scope when it is necessary to preserve data. In response, we have made this change and modified the requirement to better qualify the purpose of preservation. The requirement should read clearly that data must be retained until a Cyber Security Incident may be ruled out as the cause of the recovery operation.

One commenter suggested removing this requirement part because it addresses forensics and not recovery. In response, this requirement part ensures data collection procedures are included in the recovery plan to allow the performance of after-the-fact analysis. This is appropriate to require as part of the recovery operation.

One commenter suggested that with changes to the definition of CIP Exceptional Circumstances to include “an imminent or existing hardware, software, or equipment failure”, this requirement would never invoke. Their proposed language incorporates the concept of CIP Exceptional Circumstances, and we have included much of the proposed wording in the revised requirement part. The commenter also proposed to limit this requirement part to Medium Impact BES Cyber Systems at Control Centers, but neither the threat nor the operational circumstances for field assets preclude applicability for this requirement part. This requirement allows sufficient flexibility to apply in widely varying environments. The modifications here also address other comments about clarifying the procedures should not impact reliability.

One comment suggested that the PRC Standards already cover this for relay misoperation, but these standards do not address specifically the failure of a Cyber Asset nor do they address the preservation of data from Cyber Assets.

One commenter stated that this requirement implies an obligation to mirror data in the measure, should be left up to the entity to determine whether or not to delay recover for the purpose of preserving data, and an entity cannot determine the preservation of data given the many ways in which a system can fail. In response, we first note that a measure is only an example and does not imply an obligation to mirror data. Second, the SDT has taken an exception to add an explanatory note in the requirement cautioning against impeding recovery for data preservation. Finally, this requirement part does not envision an entity determining every way in which a Cyber System can fail. This only obligates the entity to include data preservation procedures in the recovery plan. There was a second comment on the guidance language in the measure, and the SDT agrees the language does not readily associate itself to the requirement and has been removed.

One comment suggested that this requirement part should be part of root-cause analysis and not impede system restoration. The SDT agrees and notes the requirement part does not address forensics but only the preservation of data to support root-cause analysis and forensics after-the-fact.

Requirement Part 2.1

One commenter suggested for this requirement part and requirement part 2.3 that the word “exercise” should be used in place of “test” since an actual recovery operation can be used for compliance. However, several commenters suggested the converse in the last posting, and we are not compelled the difference in terminology changes the meaning of the requirement.

One commenter suggested revising the language of “at least once each calendar year, not to exceed 15 calendar months between executions” to “once each calendar year or a period not to exceed 15 calendar months between executions”. The SDT notes that the language that exists is sufficient as currently written.

Several commenters requested clarity about whether or not each recovery plan must be tested annually. In response, we have modified this requirement to explicitly state that each recovery plan must be tested as was the intent. We do not specify a representative sampling of plans be tested as some suggest because the proposals do not include enough information to objectively determine what constitutes a representative sample. However, we do note that it is possible to singularly test multiple cyber systems if they are similar in nature.

One commenter suggested that all backup media should not be required for testing but only the one needed for recovery, and we have modified the requirement to include this condition.

One commenter suggested that “or” should be added to the first bullet point or it is otherwise required. In response, the or in the second bullet point modifies the entire list.

Requirement Part 2.2

One commenter asked if this requirement part includes a media test and whether this can be performed on a sample system. In response, this can include a media test on a sample system provided some verification to ensure the information is current and useable occurs. We have modified the measure for this requirement part to make this clearer.

One commenter suggested allowing an actual recovery operation to substitute for the testing of backup media, and we have made this change.

One commenter proposed to replace the requirement with “Unless covered by EOP-008, test a representative sample of information used in the recovery of BES Cyber Systems that is stored on backup media at least once each calendar

year, or a period not to exceed 15 calendar months between tests, to verify the backup media is operational and the information is useable." The concern surrounds possible double jeopardy with EOP-008 and clarity around "compatibility with current system configurations." In response for EOP-008-1 R7, failure to meet this requirement does not indicate a failure for EOP-008-1 and vise-versa. This requirement concerns the testing of backup media, which may not be used for recovery with EOP-008-1. For the proposed language, we have incorporated the "representative sample of information" in testing to clarify the obligation, but we retain the purpose of verifying compatibility with current system configurations. Only ensuring the usability of backup media does not capture the intent that the backup media is currently usable for performing the BES Cyber System function.

One commenter suggested striking the phrase "to ensure that the information is useable and is compatible with current system configurations" and believes it should be left up to the Responsible Entity to determine, whether another commenter requested further clarification about this phrase. In response, the testing of backup media alone is not specific enough to ensure clarity of the requirement. The phrase in question is necessary for entities to know what they should be testing. We have added additional technical guidelines for this requirement.

One commenter suggested that this requirement should state that a tabletop exercise should not be permitted. In response, the testing of backup media may be performed as a separate process or as a part of the recovery plan exercise. There is not a need to specify which type of exercises aligns with this process.

One commenter suggested that the term "backup media" is antiquated and should be replaced with redundancy terminology. In response, we disagree the term is antiquated, but if redundancy is being used for recovery, then processes should exist to test the redundant systems in accordance with this requirement part.

Several commenters proposed the phrase "validate the integrity of the stored information" as a substitute for current language regarding the testing of backup media. In response, validating the integrity of the information can be interpreted widely from a bit comparison to a sampling. We believe our proposed revisions provide enough specificity and flexibility to be widely applied.

One comment proposed to focus the requirement on backup media rather than information used for recovery. In response, we use the term information here because of the various ways entities implement backup policies, which may include replication technologies. Backup media was not well understood by the team and many participants to include replication.

Requirement Part 2.3

Several comment that the measure references performance of this requirement prior to the Effective Date, and that this requirement part should be included in the Implementation Plan. In response, we have removed this language from the measure and added this requirement part to the Implementation Plan.

One commenter suggested testing a representative of a plan with a rationale that High Impact BES Cyber Systems already have a requirement to test backup media annually. In response, we do not see a significant change in the proposed wording. The requirement to test backup media does not require a full operational restoration.

One commenter requested clarity that all recovery plans do not have to be tested at the same time. In response, the requirement only specifies the obligation to test recovery plans at a periodicity. It would not violate the requirement to test individual plans at different periods while still meeting the periodicity obligation.

One commenter requested a basis for the 36 months period. In response, we incorporated this timeframe from the FERC Order 706 directive.

One commenter suggested testing a “representative” rather than “each” BES Cyber System. In response, if an entity can test a representative BES Cyber System for multiple systems, then they have complied with the requirement to test “each” BES Cyber System.

One commenter noted that an entity may have several failure scenarios and it is unclear if all of these must be tested. In response, we have added guidance in the technical guidelines section of the Standard to clarify that not all failures scenarios must be tested, but that the test should ensure the plan is up to date and test at least one process to restore the applicable cyber systems.

One commenter suggested that EOP-008 R6 should suffice for this requirement part. In response, EOP-008-1 R6 requires independent backup functionality, but this does not imply an obligation to perform a functional test. The compliance processes to comply with EOP-008-1 should certainly ease compliance with this requirement part.

Several respondents asked whether a full operational exercise means a bare-metal recovery and comments that doing so would be cost prohibitive, while another commenter suggested also requested further clarification around

the term "operational exercise". In response, the SDT has provided well established definitions of operational exercises that would comply with the requirement, which do not imply a full recovery demonstration.

Requirement R3
Requirement R3 has been modified to correspond with similar commenter suggestions in CIP-008-5 R3.

One commenter suggested that Requirement R3 does not include defined roles and responsibilities. As we understand the comment, the roles and responsibilities refer to those required parts of the response plan specified in Requirement R1.

Requirement Part 3.1
Several commenters noted that the various dates for updating the plan significantly increase the compliance tracking burden and that a plan has not truly updated until the entity distributes those updates to the required individuals. The SDT agrees and has collapsed previously posted requirement parts 3.1, 3.2 and 3.4 into a single requirement part 3.1. The additional requirement part 3.3 for monitoring plan changes and 3.4 has collapsed into a single requirement part 3.2. Some comment that both requirements should allow a consistent 90 days, but the updating of the plan in response to changes does not require the same level of updates as those required from lessons learned. Therefore the different timeframes in these requirement parts are appropriate.

A few commenters suggested updating plans based on lessons learned is not necessary because these changes would be captured in technology and personnel changes. In response, the updates here capture improvements to the plan as determined through a lessons learned exercise.

One commenter suggested that the evidence collected in requirement part 1.5 should be part of the review process. They also commented that other related plans (i.e. configuration management plans) be updated as necessary as part of the review process. In response, the evidence collected in requirement part 1.5 may not be reviewed by a third party and we do not feel it is necessary to specifically call out this activity in the requirement part. Also, we cannot add an obligation to update other plans as necessary in a way that would be objectively measurable.

One commenter suggested that 30 days may not be sufficient time to make complex changes from lessons learned. In response, the SDT believes the updated requirement allowing 90 days for the complete time is sufficient for even complex changes.

Several commenters have suggested clarifying the expectation when there are no lessons learned. In response, we have made this explicit in both the requirement and measure.

Several commenters stated that requiring entities to perform lessons learned is counterproductive because it encourages entities not to admit there is a deficiency in the first place. In response, the inclusion of a lessons learned process provides a standard practice across the industry, which would otherwise be inconsistency applied at best. Furthermore, it addresses a FERC Order 706 directive to include lessons learned processes as part of a recovery plan test.

Requirement Part 3.3

One commenter suggested modifying the references to other standard requirement parts, removing references to individuals and modifying the communication of plan updates to be more specific. In response, the SDT has made several modifications to Requirement R3 to align with modifications to CIP-008-5 that address these concerns.

Several commenters proposed removing this requirement and addressing plan updates in guidance, but placing the plan items that would trigger a change in guidance would add a high degree of subjectivity to the requirement. Specifying what changes should constitute an update ensures objectivity in demonstrating compliance with this requirement.

One commenter proposed removing this requirement or clarifying the tie back to Requirement R1.2. In response, this requirement is necessary to ensure the recovery plan remains current and carries forward from the requirement to update on any changes. They also expressed concern that this requirement part could be interpreted that a change to any plan must be communicated to all individuals specified in requirement part 1.2. In response, we have removed the explicit tie to requirement part 1.2 to avoid such an interpretation.

One commenter suggested that the plan maintenance would create an undue compliance burden. In response, the SDT notes this requirement carries forward from previous versions and ensures the recovery plans remain up to date through organizational changes.

Requirement Part 3.4

Several commenters suggested changing the word “distribute” to “notify” for announcing changes to the incident response plan due to the uncertainty of what constitutes distribution and the possible issues with information sensitivity. The SDT agrees.

One commenter suggested the distribution of plan updates should include some irrefutable evidence on the part of the receiver. In response, we do not believe the added qualification would have the desired benefit. Individuals can choose to ignore the content regardless of the evidence of receipt.

One commenter stated that the example evidence for communicating plan updates is a poor choice because of the confidentiality of such information. In response, the examples do not necessitate the sharing of sensitive information but only that the individuals be notified. We have included additional guidelines to consider the sensitivity of the information when sending the required notifications.

VRF

One commenter proposed that the VRF should be Lower for consistency with other requirements. In response, we retain the previously FERC approved VRF of Medium for this requirement because failure to have restoration procedures directly affects the BES reliability function of High and Medium impact BES Cyber Systems.

VSLs

The VSLs have been updated corresponding to changes made to requirements in CIP-009-5.

One commenter suggested that “within 30 days” should be changed to “greater than 30 days”. The SDT agrees and has made this change.

Several commenters suggested that the moderate VSL for Requirement R1 should address “one” and not “all” missing elements of the plan. The SDT agrees and has made this change.

One commenter suggested that the VSL for Requirement R3 should capture not documenting the absence of lessons learned. The SDT agrees and has made this change.

One commenter proposed to replace the Requirement R3 VSLs with graduation from 90-210 days beyond the required obligation. The SDT agrees and has made this change.

One commenter noted the graduation of VSLs for requirement part 2.2 incorrectly lists a period of within 19 calendar months for the Severe category, and the SDT has modified this to be 18 calendar months.

QUESTION C12 – CIP-010-1:

If you disagree with the changes made in CIP-010-1 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the primary concerns regarding CIP-010-1 expressed in comments were (1) references to CIP-005, CIP-006, and CIP-007 within CIP-010, (2) scope of baseline configuration items in R1.1, (3) applicability including associated assets/systems and also including "external routable connectivity" language, (4) requirement language above and beyond FERC Order 706, and (5) other requirement and measure language modifications. The sections below are a summary of the comments received and include SDT responses for CIP-010-1.

CIP-010-1 General Comments

Many commenters requested an explanation for why CIP-010 depends on CIP-005, CIP-006, and CIP-007. Based on previous requirements in older versions of CIP-003, CIP-005, and CIP-007 (CIP-006 has since been removed from requirement language), the SDT combined the various requirements related to configuration change management and vulnerability assessments to create CIP-010. Both configuration change management and vulnerability assessment require validation that controls from CIP-005 and CIP-007 are not affected. Therefore, CIP-010 references CIP-005 and CIP-007. The SDT does not believe this cross-referencing creates a "double jeopardy" situation. Whether the requirement existed in CIP-005 or CIP-007, if an issue is discovered, then the issue would be a violation of where the requirement was enforced (CIP-005 or CIP-007) rather than in the requirement which enforced the search for issues (CIP-010). New "identify, assess, and correct deficiencies" requirement language will also aid in compliance concerns.

Several commenters mentioned that they desired a return to the approved language in CIP-003-4 Requirement R6 and CIP-007-1 Requirement R1 with targeted and efficient changes to address the FERC order. Another commenter further recommended a return to the draft 1 language. The SDT disagrees with their determination and believes that the current CIP-010-1 language is proper and in order. Based on this commenting period, the SDT has revised language for clarity and consistency. Language was also modified in an effort to address industry comments.

Numerous commenters recommended that all references to Medium Impact BES Cyber Systems in CIP-010 applicability include: "with External Routable Connectivity." The SDT does not agree with the addition of External Routable Connectivity to CIP-010 applicability. Whether a cyber asset has some type of connectivity or not, it can still be pervious

to vulnerabilities (i.e., Stutnex). The SDT's determination is in accordance with FERC Order 761, Paragraph 86. Therefore, external routable connectivity exclusion language was not included in the applicability for CIP-010.

One commenter proposed removing from the measures: "… and the output of the tools used to perform the assessment," since this is thought to be a part of CIP-010-1 Requirement R3.4. The SDT does not agree with this modification since CIP-010-1 Requirement R3.4 asks for the results of the assessments, while CIP-010-1 Requirements R3.1 through R3.3 are referring to the output of any tools used to perform the assessment. In consideration of this comment and other industry comments, the SDT included "any" to the requirement in the case that no tools were used to perform the assessment.

Several commenters suggested the removal of: "… but not limited to …" in CIP-010 measures. The SDT has modified measure language in consideration of their comment. The SDT also emphasizes that the: "… but not limited to …" is supposed to benefit the responsible entity and not create an item for auditors to use against them.

Multiple commenters suggested that specific controls from CIP-005 and CIP-007 be identified in CIP-010-1 Requirements R1.3, R1.4.1, and R3.1 so there would be no need for interpretations. These comments were taken into consideration, and the related requirement sub-parts were modified accordingly. The references to CIP-005 and CIP-007 were removed from some requirement sub-parts. Also, per consideration of these comments, CIP-006 was removed from requirement language where the language was present.

One commenter believed that some requirements in CIP-010 expand the scope and documentation burden beyond earlier CIP standards versions due to CIP-005 and CIP-007 references. In consideration of these comments, the SDT has modified CIP-010-1 Requirements R1.3 and R3.1 accordingly. References to CIP-005 and CIP-007 have been removed from the sub-part requirement language. It should be noted that the SDT disagreed to removing these references in Requirement R1.4.1. The SDT also added the reference to Requirement R1.5.1 for consistency across Requirement R1.

One commenter recommended adding a reference to the associated requirement part in which each CIP-010-1 VSL is related. The VSLs are written at the higher-level requirement, but do include elements that refer to the various requirement parts. Therefore, the SDT does not believe that the associated requirement part needs to be included in the VSL. One commenter continued to suggest that the VSL language should more closely mirror the requirement language. The SDT has taken into consideration this comment and modified the VSL language accordingly.

One commenter mentioned that having a documented baseline and monitoring it closely makes the vulnerability assessment prior to deployment have no benefit. The SDT does not agree with this assessment, as a vulnerability assessment is more than just monitoring for changes to the baseline. Please see the guidelines section of the standard for CIP-010-1 Requirement R3. Also, other commenters mentioned that establishing a production-like environment that could produce an active vulnerability assessment would be difficult and expensive. The SDT added the language: "… production environment where the test is performed in a manner that minimizes adverse effects …" for instances when a test environment is not available.

One commenter recommended an expanded glossary of the many terms used in CIP-010. The SDT has taken this comment into consideration and has expanded upon the guidelines to include more guidance around terms related to the baseline configuration and cyber security controls.

One commenter recommended further items to be incorporated into the baseline configuration; including communication protocols, non-standard BIOS configurations, and other items. The SDT believes that the requirement language is sufficient as written, as adding additional items into the baseline configuration at this time period would be difficult to support consensus.

One commenter recommended that CIP-010-1 have an effective date that is 12 months after the effective date of the CIP V5 standards. The SDT will take this comment into consideration, as this comment references the Implementation Plan and not necessarily language within the CIP-010-1 standard.

One commenter commented on the use of the term "Configuration" versus "configuration." The SDT has revised CIP-010-1 to only use "configuration," since it was not the SDT's intent to include "Configuration," as this is not a NERC defined glossary term. Furthermore, another commenter questioned if the terms: "configuration management," "configuration change management," and "asset management" were synonymous terms. The SDT has revised CIP-010-1 to only use "configuration change management" for less confusion. "Asset management" is not synonymous with the other words in the previously mentioned sentence. "Asset management" where it is used (R1.1 measures) refers to SAP, Maximo, Cascade, Passport, or other asset management software. Also, due to other questions around the baseline configuration, the SDT has added further guidance to aid in entities' development of their baselines.

Applicability Section

A couple comments mentioned that the exemption language in Section 4.2.4 should be changed back to the previous ballot's CIP-010-1 language or this section should be struck if it truly only applies to CIP-002-5. The difference between the initial ballot posting and successive ballot posting is 4.2.3.5, which states that: "Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes."

One commenter recommended the striking of the applicability component of the main requirement. If the commenter is referring to Section 4 of CIP-010, then this section is required for NERC standards to identify the standard's applicability to Responsible Entities, while the (newly termed) "applicable systems" columns in the tables refers to the scope of systems to which a specific requirement row applies.

Many commenters recommended removing some or all associated assets/systems from various applicability sections in the CIP-010 requirements because they represent an increase in scope from CIP V3/V4. The SDT disagrees with this assessment, as CIP Version 3 and Version 4 standards mention applicability to cyber assets within the ESP. The cyber assets that could exist within an ESP would include Associated Protected Cyber Assets, Associated Electronic Access Control or Monitoring Systems, and Associated Physical Access Control Systems. Therefore, the SDT does not believe that the assets/systems from CIP-010's applicability represent an increase in scope from CIP Version 3 and Version 4 standards.

One commenter expressed concern over 4.2.2, bullet 3, which references: "… Transmission where the Protection System is required by a NERC or Regional Reliability Standard." The concern was that CIP-010-1 was requiring the installation of a Transmission Protection System. This assessment is incorrect. CIP-010-1 does not require the installation of a Transmission Protection System, but other NERC or Regional Reliability Standards may require the installation of a Transmission Protection System.

Guidelines Section

Several commenters suggested adding the phrase: "network connectivity to identify" to the Requirement R3 guidance with regard to passive network discovery. The standard has been modified in consideration of these comments to include the phrase. One commenter made several other suggestions (such as the addition of details on baseline configurations and cyber security controls) in regards to guidance that informed the SDT's modification of that section.

Background Section

Several commenters mentioned that the third paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. The SDT believes that this third paragraph is clear in stating:

- A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence.
- The word "required" is not used to describe numbered or bulleted lists. The SDT wishes to emphasize that measures are only examples of evidence.

Requirement R1

One commenter proposed revision of the Requirement R1 to: "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has added the "in a manner that identifies, assesses, and corrects deficiencies" language to the requirement, which is described above.

One commenter proposed that the requirement be changed to a program- or performance-based level to allow more flexibility (citing FERC FFT Order, Paragraph 81). The comment furthermore mentions that programs such as Tripwire would not be able to be used. Other commenters had similar comments in regards to the prescriptive language of CIP-010-1 Requirement R1.1. Based on the revised "identify, assess, and correct deficiencies" language, the SDT believes that more flexibility is achieved through an entity's internal controls process. Furthermore, the SDT believes that programs such as Tripwire could be used to aid in compliance with CIP-010-1 Requirement R2.

One commenter believed that information in Requirement R1 should only be collected for personal computers and protective relays. The SDT disagrees with this comment, as the applicability should involve all BES Cyber Assets, BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems since these assets can be found within the same Electronic Security Perimeter.

One commenter asked if recording software "hashes" can be used as an alternative to recording version levels to verify that no unauthorized changes have been made to software on the BES Cyber Asset. The SDT attempted to provide flexibility to allow the entity to determine how to track changes. However, in regards to CIP-010-1 Requirement R1, the baseline configuration still must be documented. If an entity is able to use software "hashes" to monitor for changes to the baseline configuration of a BES Cyber System, then this solution could be used for CIP-010-1 Requirement R2.1.

One commenter proposed a modification to language in CIP-010-1 Requirement R1 to eliminate the term "baseline" so that it is not confused with the security baselines that they create today for devices. Two other commenters also wanted to remove the "baseline" from CIP-010-1 requirement language. The SDT disagrees with the proposed change and believes that the language, as is with the term "baseline," is sufficient.

Requirement Part 1.1

A few commenters emphasized that Version 4 did not apply to noncritical; but in accordance with FERC Order 761, Paragraph 86, these assets/systems should be included in CIP-010-1 Requirement R1.1. Therefore, external routable connectivity exclusion language was not included in the applicability for CIP-010-1 Requirement R1.1. Numerous commenters also alternatively recommended that CIP-010-1 Requirement R1.1 applicability only include High Impact BES Cyber Systems. The SDT disagrees and continues to cite FERC Order 761, Paragraph 86.

Several commenters disagreed with the use of the phrase: "… each Cyber Asset identified, individually or by group." The SDT has revised the requirement language in regards to their comment so as to ensure baselines can be defined at the individual or group level.

One commenter also desired a clarification of what may be grouped under CIP-010-1 Requirement R1.1. The SDT hopes that the revised requirement language provides additional clarity.

Requirement Part 1.1, Sub-Part 1.1.1

One commenter believed that this requirement is covered in CIP-009 Requirement R.1.3. The SDT disagrees with this comment as the process for the backup and storage of information required to recover BES Cyber System functionality is not required to include baseline configuration items.

Several commenters recommended replacing "exists" with "is either operating or running." Another commenter believed the wording of "is installed" is also sufficient. The SDT wants to underscore that "exists" refers to the case when an asset has firmware instead of an Operating System.

Requirement Part 1.1, Sub-Part 1.1.2

One commenter mentioned that "BES Cyber Asset" should be replaced with "applicable Cyber Asset." Other commenters had a similar position with regards to the use of "BES Cyber Asset." These comments were taken into consideration and

the related requirement sub-part was modified. The phrase "on the BES Cyber Asset" was removed from the requirement sub-part for consistency.

Multiple commenters requested clarification on the "applications." Does "applications" mean "SCADA, EMS, State Estimator, etc." instead of "device drivers and DLL applications" included in an operating system or package?" In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

One commenter believed that this requirement is covered in CIP-009 Requirement R.1.3. The SDT disagrees with this comment, as the process for the backup and storage of information required to recover BES Cyber System functionality is not required to include baseline configuration items.

A couple commenters suggested the removal of the word "intentionally" from the requirement language. The SDT believes that the use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for cyber asset use should be included. It is not the SDT's intent for notepad, calculator, DLL, device drivers, or other applications included in an operating system package to be considered as commercially available or open-source application software. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

Several entities requested clarity on how granular the version identifier should be. The SDT provides flexibility for entities to determine what version levels should be tracked. The purpose of tracking the version allows entities to keep abreast of the version levels in their inventory. If software manufacturers alert entities to vulnerabilities in their software, the affected population could be identified through software version. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

Several entities suggested that sub-part 1.1.2 should exclude anti-malware signature file version identifiers due to the volatility of frequency updates. The SDT believes that only version levels that can aid in recognizing affected software should be tracked. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

Requirement Part 1.1, Sub-Part 1.1.3

Multiple entities asked if a version control tool/system (like Concurrent Versions Systems) could demonstrate the custom software's version. In consideration of these comments, this requirement sub-part has been reworded to be "custom software installed." However, even in its successive ballot form, the requirement sub-part did not require the custom software version. Instead, the requirement sub-part requires the identification of the custom software.

One commenter believed that this requirement is covered in CIP-009 Requirement R.1.3. The SDT disagrees with this comment, as the process for the backup and storage of information required to recover BES Cyber System functionality is not required to include baseline configuration items.

Multiple commenters suggested removing "developed for the entity." The SDT has taken this comment into consideration and modified the requirement language accordingly.

There were several commenters who proposed modified language to clarify the term "custom software." The SDT disagrees with these proposed changes, but has reworded the requirement language in an attempt to provide additional clarity.

Requirement Part 1.1, Sub-Part 1.1.4

There were many commenters who believed that this requirement is covered in CIP-007. The SDT remarks that CIP-007 is evaluating what patches should be installed, while CIP-010 handles the patch being implemented (i.e., going through the configuration change management process).

One commenter believed that CIP-010-1 Requirement R1.1.4 would require the industry to account for more than a billion ports if each of 214 entities had less than 100 routable assets. Only ports which are accessible need to be included in the baseline. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

One commenter asked for clarity around "logical network accessible ports." In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

One commenter mentioned that the applicability columns from CIP-007 should match the applicability column in CIP-010-1 Requirement R1. The SDT does not agree with this comment, as the concept in CIP-010 is to identify logical network accessible ports, while CIP-007 requests entities to enable logical network accessible ports.

Requirement Part 1.1, Sub-Part 1.1.5
One commenter mentioned that CIP-010-1 Requirement R1.1.5 should be clarified to identify only those patches applied to the asset at the time the baseline is established and not all possible historic patches available for the asset. This comment was taken into consideration and the related requirement sub-part was modified.

Many commenters believed that this requirement is covered in CIP-007. The SDT remarks that CIP-007 is evaluating what should be used, while CIP-010 is the implementation.

One commenter believed that CIP-010-1 Requirement R1.1.5 would require an entity to document tens of thousands of unique patch installs for less than 200 Windows based Cyber Assets. Only historic or current patches that have been applied would be included in the baseline.

Several comments raised the concern Requirment R1.1.5 changes too frequently to be in the baseline and should be removed; that the evaluation of each patch is already included in CIP-007-5. The SDT believes that CIP-010-1 Requirment R1.1.5 is supposed to be a comprehensive listing of the patches that have been installed on the device. Patches are not required to be evaluated with this requirement. Instead, if a patch has been added to the device, then an update of the baseline is required.

Measures for Requirement Part 1.1
Per a comment, “or group” was added to CIP-0101 Requirement R1.1 measures to make consistent the requirement language and measures.

Requirement Part 1.2
One commenter proposed a rewording of CIP-010-1 Requirement R1.2 to: “Authorize changes to: security controls, operating systems, application software versions, custom software, ports or patches. Authorize changes to add or remove hardware.” The SDT disagrees with this comment, as the requirement language is consistent with other similar CIP Version 5 requirement language.

One commenter proposed indicating the appropriate authorizing individual or delegate in the requirement. The SDT believes that the requirement is sufficient, as is since it provides flexibility so that the entity can select the appropriate authorizing individual.

Measures for Requirement Part 1.2

One commenter recommended the removal of language in measures around individuals or groups with the authority to authorize the change. The SDT believes that measures are only examples of evidence. To be in compliance with the requirement language, an entity could authorize change by an individual, a group, or other entity-determined method.

There were two comments that recognized a concern with the language: "Documentation that the change was performed in accordance with the requirement." There was another suggestion to remove this language since it is not clear to what term the requirement is referring. The SDT believes that since the measure is for CIP-010-1 Requirement R1.2, that the language in the measure directly refers to CIP-010-1 Requirement R1.2 language only. While the SDT considered adding a reference to CIP-010-1 Requirement R1.2 in the measure to make explicit the requirement to which the measure language was referring, for consistency across CIP-010, this change was not made.

Requirement Part 1.3

One commenter mentioned that the applicability columns from CIP-005 and CIP-007 should match the applicability column of CIP-010-1 Requirement R1.3. This comment was taken into consideration and the related requirement sub-part was modified accordingly. The reference to CIP-005 and CIP-007 was removed from the requirement sub-part; and, therefore, the applicability columns between the standards do not need to be consistent.

There were many commenters that expressed concern with the 30-day time frame. Other commenters recommended the removal of the 30-day time frame for updating the baseline configuration. The SDT disagrees with the commenters and believes that a 30-day time frame allows entities time to update their baseline configuration documentation. Similiarly, other commenters had issues with the 30-day time frame and the references to CIP-005 and CIP-007. These issues are no longer a concern, as the SDT has removed the reference to CIP-005 and CIP-007 in regards to the 30-day time frame.

Two commenters were concerned about 'triple', or 'double' jeopardy with CIP-005 and CIP-007. One commenter suggested a revision or removal of the references, while another suggested that the requirement be moved to CIP-005 or CIP-007. In consideration of their comment, the SDT has modified CIP-010-1 Requirement R1.3 accordingly. In response, references to CIP-005 and CIP-007 have been removed from the sub-part requirement language.

Requirement Part 1.4

Many comments stated that "High Impact BES Cyber Systems" should be removed from applicability in CIP-010-1 Requirement R1.4 since this requirement sub-part is repetitious with CIP-010-1 Requirement R1.5. While CIP-010-1 Requirement R1.4 has been modified due to comments from industry, the SDT disagrees that CIP-010 Requirement R1.4 is repetitious with CIP-010-1 Requirement R1.5. CIP-010-1 Requirement R1.5 requires entities to test their baseline configuration changes in a test environment and document the results, while CIP-010-1 Requirement R1.4 requires entities to identify cyber security controls and then verify that these identified cyber security controls and system availability are not adversely affected after making the change.

A bevy of commenters believed that this requirement should include an exclusion for CIP Exceptional Circumstances. The SDT does not agree with this comment, as even after the CIP Exceptional Circumstance has happened, an entity should determine that controls were not adversely affected.

Several commenters suggested that guidance be added on cyber security controls. The SDT has taken their comment into consideration (in addition to other similar inquiries on cyber security controls) and added additional information on cyber security controls in CIP-010 guidance.

One commenter proposed the following language for this requirement part: "For a change that deviates from the existing baseline configuration or may have an impact on controls implemented for CIP-005, CIP-006, or CIP-007, [do 1.4.2]." While the SDT considered this approach, the SDT believes the current requirement language is sufficient as is.

CIP-010-1 Requirement Part 1.4, Sub-Part 1.4.1

One commenter suggested a language change of "determined" to "identified." The SDT disagrees with this proposed change and believes that the current language is sufficient as is.

One commenter believed CIP-010-1 Requirement R1.4.1 where "could be impacted" is used will cause all entities to document every control for every change in order to avoid zero-defect audit enforcement when some situation can be devised where "could be impacted" is a remote possibility. Southern believed that documenting "what could be impacted" is not a reliability benefit, it's the verification that controls are not affected by a change. The SDT agrees with their recommended change, and the requirement language has been updated accordingly in Requirement R1 with: "implement, in a manner that identifies, assesses, and corrects deficiencies," to avoid the zero-defect audit enforcement concern.

Several commenters believed that CIP-010-1 Requirement R1.4.1 could result in the Responsible Entity declaring that no cyber security controls are expected to change and, thus, no testing is required. The SDT does not agree with this assessment, as the requirement requires documentation of what could be changed followed by verification that potentially impacted controls were not affected in CIP-010-1 Requirement R1.4.2.

Many commenters recommended the removal of Requirement R1.4.1. The concept is that an entity identifies all related controls that could be impacted based on all requirements in CIP-005 and CIP-007. Therefore, the SDT believes that by mentioning CIP-005 and CIP-007, there is no need for interpretations. In fulfilling the requirement, an entity must identify that a particular change impacts CIP-005-5 Requirement R1 or CIP-005-5 Requirement R1 and CIP-005-5 Requirement R2. If all requirements in CIP-005 and CIP-007 may be affected by a deviation to the existing baseline configuration, then this would be documented in accordance to CIP-010-1 Requirement R1.4.1. It should also be mentioned that CIP-010-1 Requirement R1.4 is not repetitious with CIP-010-1 Requirement R1.5. CIP-010-1 Requirement R1.5 requires entities to test their baseline configuration changes in a test environment and document the results, while CIP-010-1 Requirement R1.4 requires entities to identify cyber security controls and then verify that these identified cyber security controls and system availability are not adversely affected after making the change.

CIP-010-1 Requirement Part 1.4, Sub-Part 1.4.2

One commenter mentioned that “BES Cyber Asset” should be replaced with “applicable Cyber Asset.” This comment was taken into consideration and the related requirement sub-part was modified. The phrase “BES Cyber System” was removed from the requirement sub-part for consistency.

Many commenters expressed concern with CIP-010-1 Requirement R1.4.2’s “availability” term. The SDT has modified the requirement language in consideration of these comments. The “available” term has been removed.

One commenter proposed that the word “determined” be changed to “identified.” The SDT disagrees with this proposed change and believes that the current language is sufficient as is.

One commenter believed the term “applicable” should be added for clarity. The SDT remarks that “applicable” is not required, as CIP-010 Requirement R1.4.2 points to CIP-010-1 Requirement R1.4.1, which ensures entities only look at the potentially impacted controls.

One commenter requested clarification of use of the term "required controls." The word required refers to the cyber security controls in CIP-005 and CIP-007 that were applied based on asset identification in CIP-002. While the SDT references all of CIP-005 and all of CIP-007, CIP-010-1 Requirement R1.4.1 requires entities to identify those controls in CIP-005 and CIP-007 that are potentially impacted. Therefore, CIP-010-1 Requirement R1.4.2 is only looking at the controls identified in CIP-010-1 Requirement R1.4.1.

One commenter proposed the addition of a time frame for how long an entity may take to make the verification required in CIP-010-1 Requirement R1.4.2. The SDT has taken this into consideration. The SDT also believes that the "identify, assess, and correct deficiencies" should provide aid in compliance concerns regarding this requirement.

CIP-010-1 Requirement Part 1.5, Sub-Part 1.5.1

Multiple commenters expressed concern with the language in CIP-010-1 Requirement R1.5.1. A few of the aforementioned organizations mentioned that the parenthetical expression in CIP-010-1 Requirement R1.5.1 should be altered to no longer include parenthesis. This comment was taken into consideration and the related requirement sub-part was modified. The language in the requirement part has been altered. Other organizations recommended changing CIP-010-1 Requirement R1.5.1 language to: "testing cyber security controls, where technically feasible, for each change that deviates from the existing baseline configuration" for clarity. The SDT has reworded requirement language based on industry comment and hopes that the changes provide additional clarity. Alternatively, other organizations proposed the removal of the following language in CIP-010-1 Requirement R1.5.1: "…that models the baseline configuration to ensure that required cyber security controls are not adversely affected." This is redundant to the concept in the last sentence, which requires documenting differences between test and production when a test environment is used. The SDT disagrees with the comment, as documenting the differences between the test and production environment is a completely separate task compared to modeling the baseline configuration. Modeling the baseline configuration is an attempt to re-create the baseline configuration on a single asset, while documenting differences between the test and production environment would simulate the rest of the assets in that environment and how they function together. Other organizations were concerned that the revised language in the posted standard removed the possibility for a technical feasibility exception. The SDT does not agree, as old, legacy systems may not be available in a test environment and there may be no way to utilize a production environment where a test can be performed in a manner that minimizes adverse effects.

One commenter asked if this requirement interferes with CIP-010-1 Requirement R1.4 for High Impact Systems. There was a suggestion to remove the overlap in applicability of the two requirements and adding clarifying language as to

what is intended and required in CIP-010-1 Requirement R1.4 vs. CIP-010-1 Requirement R1.5. The SDT wishes to underscore that CIP-010-1 Requirement R1.4 is not repetitious with CIP-010-1 R1.5. CIP-010-1 R1.5 requires entities to test their baseline configuration changes in a test environment and document the results, while CIP-010-1 Requirement R1.4 requires entities to identify cyber security controls and then verify that these identified cyber security controls and system availability are not adversely affected after making the change.

One commenter requested clarification of use of the term: "required controls." The SDT responds by claiming that "required" refers to the cyber security controls in CIP-005 and CIP-007 that were applied based on asset identification in CIP-002. Additional information on cyber security controls were added in CIP-010-1 Guidelines for Requirement R1.

Several commenters expressed concern over the "where technically feasible" language. Alliant Energy proposed that: "where technically feasible" should be changed to "where test environments exist." One commenter wanted to know what the language pertained to. The SDT does not agree with the proposed modification. The language in the requirement allows for test environments to exist in a production environment where the test is performed in a manner that minimizes adverse effects. Also, it should be made clear that the exception language refers to both CIP-010-1 Requirement R1.5.1 and Requirement R1.5.2.

Requirement Part 1.5, Sub-Part 1.5.2

Some commenters believed that the following language should be removed from the sub-requirement: "including a description of the measures used to account for any differences in operation between the test and production environments." Another commenter stated that they do not understand the intent of requiring this type of documentation, as it provides no security benefit and only invites auditors to unnecessarily critique the methods that the entity determines are appropriate to address the differences between the two environments. The SDT does not agree with this assessment and believes the documentation of the differences is important.

SPP RE and City Utilities of Springfield, MO asked if CIP-010-1 Requirement R1.5.2 permits the documentation of a stand-alone test environment with identified differences from the production environment. The SDT concurs that the requirement language requests documentation of the differences between the test and production environment, if a test environment was used. If the differences did not change from change to change, then the same documentation would be included with each change package that is processed.

Requirement R1 VRFs

Based on numerous comments, the VRFs in Table of Compliance Elements now match the VRF as identified at the requirements and measures section of the standard. This modification is for both CIP-010-1 Requirement R1 and Requirement R2.

Requirement R1 VSLs

There were two commenters who suggested that in corresponding to the proposed revisions to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. The SDT will take this into consideration, as we apply the non-zero defect forward looking compliance process.

Two commenters suggested that "any" be changed to "one or more" in the High VSL for CIP-010-1 Requirement R1. The SDT has updated the VSL language per the comment's recommended change.

One commenter believed that the phrase "and to document those changes" in the first condition of the High VSL for CIP-010-1 Requirement R1 should be deleted, as it is duplicative of the second condition. The SDT has removed the second condition due to modification to the requirement language to remove reference to other CIP standards in CIP-010-1 Requirement R1.3.

Main Requirement R2

One commenter proposed revision of the Requirement R1 to: "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has considered this approach in accordance with the FFT process. The following language has been added to requirement language: "identifies, assesses, and corrects deficiencies…"

Requirement Part 2.1

Many comments were on the initial ballot posting language, as the successive ballot posting language is not understandable. The SDT has modified the requirement in consideration of their comment.

One commenter believed that double jeopardy exists with CIP-010-1 Requirement R1 and CIP-010-1 Requirement R2.1. If a paperwork error occurs in authorizing a change and this requirement uncovers it, this should be addressed under CIP-010-1 Requirement R1, not a separate requirement. The SDT disagrees with this assessment. CIP-010-1 Requirement

R2.1 does not create a double jeopardy situation with CIP-010-1 Requirement R1 since the violation would be in CIP-010-1 Requirement R1, not in CIP-010-1 Requirement R2.1. CIP-010-1 Requirement R2.1 requires entities to document and investigate detected unauthorized changes. If one of the unauthorized changes is due to a violation of CIP-010-1 Requirement R1, then the self-report would be on CIP-010-1 Requirement R1 and not on CIP-010-1 Requirement R2.1. However, based on the new "identifies, assesses, and corrects deficiencies" language, if an issue is detected, based on an entity's internal control processes, this would not be a self-report. Other commenters stated on CIP-010-1 Requirement R2 creating a situation where a need would exist to self-report. With the new requirement language of "identifies, assesses, and corrects deficiencies," a self-report would not be necessary.

Many commenters essentially mentioned concerns centered on technical feasibility language. Some of the aforementioned organizations requested that the term "continuous" be removed from requirement language; while others proposed language that would remove the technical feasibility exception. The SDT has modified the requirement language in consideration of these comments. One commenter further commented that the language should be revised in such a way that only devices that can monitor automatically should be included; otherwise, a technical feasibility exception should be allowed. The SDT has modified the language such that monitoring could be done manually or continuously depending on the device.

One commenter suggested a change to the following language: "Document changes tracked through the entity's change management program." The SDT does not agree with this approach and believes the language is sufficient as is. One commenter recommended a similar approach of modifying the language due to their desired removal of "baseline" term use.

Many commenters suggested a different time frame for monitoring. The suggestion called for a 90-day instead of 35-day time frame, while other commenters suggested an annual or quarterly time frame. The SDT believes that a 35-day time frame is sufficient for an "express acknowledgement."

One commenter believed that the requirement will be burdensome and nothing gained from it except a lot of TFE paperwork to track. The SDT disagrees with this comment, as the requirement was added based on FERC Order 706.

One commenter asked if no change is detected during a monitoring period, how an entity can demonstrate that "no change" occurred. The requirement language mentions that only detected unauthorized changes need to be documented and investigated. If there is no change, then this would not need to be documented.

Measures for Requirement Part 2.1

One commenter emphasized that the requirement requires monitoring for all changes, yet the measure mentions calls for investigation of any unauthorized changes. They believe that the requirement language should be changed to include "unauthorized" changes such that monitoring is only necessary for unauthorized changes. The SDT does not agree with this assessment and believes that the requirement language and measures are sufficient as is.

One commenter requested clarity on the phrase "record of investigation." "Record of investigation" would be some type of documentation that shows that a detected unauthorized change was documented and investigated accordingly.

Requirement R2 VRFs

Multiple commenters stated that the VRFs in the table of compliance elements now matches the VRF as identified at the requirements and measures section of the standard. This modification is for both CIP-010-1 Requirements R1 and R2.

Requirement R2 VSLs

Several commenters suggested that in corresponding to the proposed revisions to the requirement statement, the VSLs should be revised to: "severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention." The SDT will take this into consideration as we apply the "non-zero defect forward looking compliance process."

Two commenters believed that a new gradated VSL should be introduced due to time-period language added in the previous posting. The SDT has taken this comment into consideration. While gradated VSLs were not introduced, since the requirement language includes "… identify, assess, and correct deficiencies…", the VSLs have been updated. .

Requirement R3

One commenter proposed a revision to Requirement R1 to read: "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has considered this approach in accordance with the FFT process. The following language has been added to requirement language: "identifies, assesses, and corrects deficiencies…"

A few commenters mentioned that the applicability between CIP-010-1 Requirements R3.3 and R3.4 differed. The SDT recognizes this difference and emphasizes that these are two different requirements and, hence, the applicability should be different.

One commenter asked if all Vulnerability Assessments under Requirement R3 must be performed prior to Version 5's Effective Date or whether entities have an additional year or three years from the effective date. The answer to NIPSCO's question can be found in the CIP Version 5 Implementation Plan. CIP-010-1 Requirements R3.1 and R3.2 must initially be complied with 12 months after the Effective Date of the CIP Version 5 standards.

One commenter asked why CIP-010-1 Requirement R3 does not always include Medium Impact in its scope. The SDT believes that the applicability as is can be considered sufficient. TRE also had concerns that the Requirement R3 does not include an annual vulnerability assessment. This is incorrect as CIP-010-1 Requirement R3.1 requires an annual vulnerability, while CIP-010-1 Requirement R3.2 requires a 36-month vulnerability assessment (for the applicable systems).

One commenter asked for clarity over the inclusion in applicability of Electronic Access Control or Monitoring Systems in CIP-010-1 Requirement R3. This requirement has the same applicability for these systems as in previous NERC CIP version. Therefore, the SDT believes that these systems should remain included in the applicability for CIP-010-1 Requirement R3.

One commenter asked if vulnerability assessments are required for every cyber asset or a sampling of cyber assets. Per applicable systems section, the vulnerability assessment is required for the systems listed.

Requirement Part 3.1

Commenters recommended that the requirement start with its purpose. The SDT disagrees with this comment, as the requirement language is consistent with other similar CIP V5 requirement language.

Many commenters proposed to reword Requirement R3.1 with the following language: "once each calendar year or a period not to exceed 15 calendar months between assessments." The SDT has taken these comments under consideration and is modifying the requirement sub-part language accordingly. One commenter proposed alternative language allowing an entity determined time frame. The SDT disagrees with this comment since the 15 calendar months' time frame is sufficient.

A few commenters believed that double jeopardy exists with reference to CIP-005, CIP-006, and CIP-007. The SDT does not agree, as if controls are not implemented correctly, then this would be a violation in the respective CIP standard, and not CIP-010-1.

Many commenters recommended that CIP-006 be removed from requirement language. The SDT agrees and has removed the reference to CIP-006.

Multiple commenters had concerns on what exactly constituted an active vulnerability assessment. The SDT points to guidance in CIP-010 on Requirement R3 in regards to recommended elements of an active vulnerability assessment. Also, other commenters asked if an active vulnerability assessment must be done for all systems or a representative sampling. Per the applicable systems section of the table for Requirement R3, the active vulnerability assessment must be done for all applicable systems.

One commenter requested clarification on whether an external vendor needs to perform the annual vulnerability assessment or can the Responsible Entity perform this task. The SDT provides enough flexibility in the requirement so that the RE can determine the solution that best meets its needs.

Several commenters believed that CIP-010-1 Requirement R3.1 is redundant with CIP-010-1 Requirement R1.3. The SDT does not agree, as CIP-010-1 Requirement R3.1 requires an annual vulnerability assessment, while CIP-010-1 Requirement R1.3 requires an update of the baseline configuration for a change that deviates from the existing baseline configuration.

Measure for Requirement Part 3.1
One commenter believed that reference to “individuals” in the first bulleted item needs to be removed. The SDT emphasizes that measures are only examples of evidence. However, the SDT has modified the measure language in consideration of the comment.

Requirement Part 3.2
Many commenters expressed concern with the language in CIP-010-1 R3.2. Another comment mentioned that the parenthetical expression in CIP-010-1 R3.2 should be altered to no longer include parenthesis. This comment was taken into consideration and the related requirement sub-part was modified. The language in the requirement part has been

altered. Furthermore, the commenters recommended that this requirement start with its purpose. The SDT disagrees with these comments as the requirement language is consistent with other similar CIP Version 5 requirement language.

Multiple commenters asked for clarification on CIP-010-1 Requirement R3.2 in regards to this being a paper exercise. The requirement language mentions active vulnerability assessment. In response, please see the guidance section on additional details on an active vulnerability assessment.

Multiple commenters proposed the removal of the language: "that models the baseline configuration to ensure that required cyber security controls are not adversely affected" in CIP-010-1 Requirement R3.2, commenting that it is redundant to the concept in the last sentence, which requires documenting differences between test and production when a test environment is used. The SDT does not agree with this assessment. CIP-010-1, Requirement R3.2.1 requires performing an active vulnerability assessment in an environment that models the baseline configuration of the BES Cyber System in a production environment, while CIP-010-1 Requirement R3.2.2 requires documenting the results of testing, and if, a test environment was used, documenting the differences.

One commenter asked how is this requirement differs from CIP-007. The SDT remarks that CIP-010-1 Requirement R3.2 is related to completing a vulnerability assessment every three years to assess controls in CIP-007 (and CIP-005) are implemented correctly.

One commenter believed that the following language should be removed from the sub-requirement: "including a description of the measures used to account for any differences in operation between the test and production environments." One commenter stated that they do not understand the intent of requiring this type of documentation, as it provides no security benefit and only invites auditors to unnecessarily critique the methods that the entity determines are appropriate to address the differences between the two environments. The SDT does not agree with this assessment and believes the documentation of the differences is important in establishing how the testing environments differ.

A few commenters asked if the assessment in CIP-010-1 Requirement R3.2 is in lieu of or in addition to the assessment required by CIP-010-1 Requirement R3.1 in the calendar year that the CIP-010-1 Requirement R3.2 assessment is conducted. The SDT believes that CIP-010-1 Requirement R3.2 is in lieu of CIP-010-1 Requirement R3.1 in the calendar year that CIP-010-1 Requirement R3.2 is conducted.

One commenter asked if CIP-006 is within scope of CIP-010-1 Requirement R3.2. The SDT has removed the reference to CIP-006 in CIP-010-1 Requirement R3.1, and is not a similar reference in CIP-010-1 Requirement R3.2.

One commenter proposed that the phrase: "where technically feasible" should be changed to "where test environments exist." The SDT does not agree with this modification since language in the requirement allows for "test environments" to exist in a production environment where the test is performed in a manner that minimizes adverse effects.

There was a comment mentioned that CIP-010-1 Requirement R3.2 requires assessments every three years, while CIP-007-3 Requirement R8 required vulnerability assessments annually. It was thought that we weakened the requirement; however, CIP-010-1 Requirement R3.1 requires an annual vulnerability and, therefore, the annual requirement in CIP-007-3 Requirement R8 was not weakened.

A commenter requested that associated electronic access control or monitoring systems and associated protected cyber assets should be added to the applicability for Requirement R3.2. For consistency in CIP-010-1, the SDT does not agree with the proposed change in applicability.

Requirement Part 3.3

One commenter believed it to be problematic to perform an active vulnerability assessment prior to installing a new Cyber Asset. The SDT acknowledges the concern, but emphasizes that an active vulnerability assessment is not required in the cases of a CIP Exceptional Circumstance or like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset.

One commenter believed that the term "active vulnerability assessment" is not defined. The SDT disagrees with this statement, as guidance is provided that aids in understanding an active vulnerability assessment. Furthermore, the commenter stated that since sufficient change management controls exist that an active vulnerability assessment is unnecessary. The SDT disagrees with this statement, as the configuration change management controls in CIP-010-1 Requirements R1 and R2 are in place for changes that deviate from the existing baseline configuration, while vulnerability assessments in CIP-010-1 Requirement R3 are for ensuring proper controls and detecting vulnerabilities.

One commenter mentioned that the parenthetical expression in CIP-010-1 Requirement R3.3 should be altered to no longer include parenthesis. This comment was taken into consideration and the related requirement sub-part was modified. The language in the requirement part has been altered.

Multiple commenters expressed concern around the language in CIP-010-1 Requirement R3.3. Some of the aforementioned organizations recommended that this requirement start with its purpose. Other organizations recommended a revision of the language. The SDT has taken these comments into consideration and modified the requirement language accordingly.

Multiple commenters suggested revisions to "prior to adding" language. One commenter proposed that instead of "prior to adding," that the requirement language should read: "before closing the change." Some vulnerability assessments actions only add value to assess after connected to the ESP as part of implementation and post implementation testing. The SDT disagrees with the proposed change and believes that the current language is sufficient based on other comments from industry.

One commenter believed that the parenthetical explanation of a like replacement should be moved to guidance. The SDT disagrees with the proposed change and believes that the current language is sufficient based on other comments from industry.

Several commenters believed that CIP-010-1 Requirement R3.3 appears to be missing "and" after the parenthesis. Without the parenthetical, it should read "Except for CIP Exceptional Circumstances and like replacements and prior to adding a new Cyber Asset..."

A couple commenters suggested that Physical Access Control Systems should be added in the applicable systems column. The SDT does not agree with their proposed change, as references to Physical Access Control Systems and CIP-006-1 have been removed throughout CIP-010-1.

One commenter expressed confusion around the use of the term: "new Cyber Asset." The commenter questioned if this term references a new Cyber Asset that is part of an existing Cyber System, or a new Cyber Asset per CIP-002. The SDT remarks that CIP-010-1 Requirement R3.3 is for new Cyber Assets with baseline configurations that do not currently exist. Therefore, a new Cyber Asset that is part of an existing Cyber System (and that has an existing baseline configuration) does not require an active vulnerability assessment per CIP-010-1 Requirement R3.3.

Several commenters believed that the language should be consistent among CIP-010-1 Requirements R3.1 through R3.3 in regards to vulnerability assessments. The SDT has modified the requirements accordingly in consideration of their comment.

A commenter asked if cyber assets can be placed in ESP before remediation of identified vulnerabilities. The SDT remarks that cyber assets can only be placed in ESP before remediation of identified vulnerabilities if a CIP Exceptional Circumstance exists or the cyber asset is a “like replacement.”

CIP-010-1 Requirement Part 3.4

One commenter suggested that the term "if any" be added in CIP-010-1 Requirement R3.4 to denote the need to document the results of assessments that identified no vulnerabilities. The SDT disagrees as the language in CIP-010-1 Requirement R3.4 follows closely to the language in its previous instance in an earlier CIP standards version.

Many commenters expressed concern with the phrase: “remediate or mitigate vulnerabilities” and the related documentation. Another commenter proposed to replace “remediate or mitigate vulnerabilities” with “implement lessons learned (if any)” for consistency with other standards and eliminate extra documentation tracking requirements. The SDT developed this requirement language directly from the previous CIP versions. The concept is that an entity must document how they plan to remediate or mitigate identified vulnerabilities. CIP-010-1 Requirement R3 becomes an internal controls requirement to ensure that cyber security controls are properly implemented. While other commenters asked if it is the intent that identified vulnerabilities would not constitute violations of requirements they are found against. It is not the SDT’s intent that an identified vulnerability would not constitute a violation of other requirements. While CIP-010 would not be violated, the respective CIP-005 or CIP-007 standard may be violated. The SDT does believe that the self-report mitigation plan could be used as the action plan for Requirement R3.4.

Several entities believed that the deadline for documenting the results of the assessment and the action plan should be specified. They suggested a 30-day limit. Also, they suggested including levels of gradation for not meeting the 30-day limit. One commenter took a different approach and recommended that “planned date” be changed to “estimated time frame.” The SDT believes that the requirement language is sufficient as is.

Several commenters believed that more specificity should be added around the term “assessments” in CIP-010-1 Requirement R3.4. The SDT has modified the language in consideration of these comments and the text: “conducted pursuant to Parts 3.1, 3.2, and 3.3” was added to the requirement language.

One commenter asked for clarity in regards to the phrase “planned date of completing the action plan.” Is this the completion of the formulation of the plan or the completion of the tasks within the plan? The SDT articulates that the planned date of completing the action plan is related to the completion of the tasks within the plan.

Requirement R3 VRFs

There were multiple comments on VRFs, and the VRFs in Table of Compliance Elements now matches the VRF as identified at the Requirements and Measures section of the standard. This modification is for both CIP-010-1 Requirements R1 and R2.

Requirement R3 VSLs

Several commenters believed that corresponding to the proposed revisions to the requirement statement that the VSLs should be revised to read: “severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention.” The SDT has taken this comment into consideration as we applied the “identify, assess, and correct” approach; however, that language should not be included here. The reasoning behind this decision is due to the CIP-010-1 R3 Requirement’s indirect (mentioned in R3 Guidance) reference to CIP-005 and CIP-007. The related language would relate to the timely performance of completing a vulnerability assessment instead of identifying and correcting deficiencies which may be a part of the related CIP-005 and CIP-007 langauge (CIP-005 does not include this language in its requirements).

Several commenters proposed that the third condition in Severe VSL have the word “or” instead of “and.” The SDT has modified the language in response to their comment.

One commenter believed that the VSL does not address the 36-month timeline in CIP-010-1 Requirement R3.2. Furthermore, the commenter proposed additional language to address this timeline. The SDT has taken this comment into consideration and modified the VSL language accordingly.

QUESTION C15 – CIP-011-5:

If you disagree with the changes made in CIP-011-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, there were many global comments that related not only to CIP-011, but to all of the CIP standards.

Annual Requirements

Many commenters objected to the posted language referencing annual requirements. Several suggested alternative ways to express the frequency for an annual requirement. The SDT considered all of the recommendations and decided use the phrase "at least once every 15 calendar months" (or similar) to express the frequency for annual requirements.

Use of the phrase "but not limited to" in measures language

The SDT received many comments objecting to the phrase "but not limited to" within the measures. Some comments suggested removal of the term; others recommended a default to the use of the word "or," while others suggested the use of the word "and." Commenters believed that using the "but not limited to" language creates confusion about whether the specified measures are necessary or sufficient. The SDT has considered this issue carefully. The SDT has modified the language to "examples of acceptable evidence include, but are not limited to." The phrase "but not limited to" is designed to be of benefit to the Responsible Entity, not be a back door "gotcha" for auditors. Use of the phrase allows the entity flexibility in the type of evidence they are able to provide both now and in the future.

Applicability Column Title

The length of the applicability column title caused confusion about the systems/assets that are within scope for some entities. Several commenters suggested shortening the column heading to "applicability." The SDT recalls that the title of the column as previously posted was in response to comments from the first posting. SDT has renamed the column "applicable systems."

The SDT received many comments stating that: "Medium Impact BES Cyber Systems should be limited to Medium Impact BES Cyber Systems with External Routable Connectivity to maintain consistency with the scope of cyber systems/assets currently covered by similar requirements in the CIP Version 4 standards." A main goal of the SDT is to implement the FERC directives in Order 706 and Order 761. Order 761 states that FERC: "…supports the elimination of the blanket

exemption for non-routable connected cyber systems…continued blanket exemption in Version 5 would not adequately address risk." The SDT has considered each requirement concerning handling the exemption for non-routable connections. The SDT does not agree that in CIP-011 the scope should be limited to only BES Cyber Systems with External Routable Connectivity, as recommended in some comments.

Many commenters requested the removal of all references to systems and assets in requirements and that the SDT rely on the applicability column only to specify applicability. The SDT agrees with this recommendation. Wherever possible, the assets in scope will be indicated only in the applicability column. Several commenters suggested that the SDT remove all references to applicable assets in requirements and rely on the applicability column only to specify the Cyber Assets that are in scope. The SDT agrees. Wherever possible, the requirements have been streamlined to only reference applicable Cyber Assets within the applicability column.

Some commenters stated that the rationale for CIP-011 Requirement R1 was incomplete as originally posted. On May 8, 2012, NERC was alerted that the text contained in the rationale box for Requirement R1 of CIP-011-1 appeared to be incomplete. NERC corrected this by issuing revised language that modified the text box size to display all of the text.

Some commenters recommended that entities should define their own info protection program. They suggested that compliance would be evaluated based on how the entity complied with their defined programs. The SDT discussed this comment, but disagrees. The SDT believes it would be doing the industry a disservice to leave the process completely up to the entity. As part of its change, the SDT seeks to clarify what is required to meet compliance. The SDT believes that if the requirements are not defined or entity defined, NERC will be forced to issue Compliance Application Notices in the future to provide clarity, and auditors will be forced to inject their own audit measurements. In the interest of providing clarity, the SDT believes it is important to provide a consistent threshold for compliance.

The SDT received comments asking that the team revert to legacy language used in previous versions of the CIP standards (V1 and V3). SDT considered this request, but believes that many entities have made good suggestions, which improve legacy language. Legacy language will be utilized in all cases where it is appropriate for the purposes of minimizing changes that the registered entities must make to their ongoing programs.

CIP-011 Requirement R1 calls for each Responsible Entity to implement an information protection program that includes applicable items, and Requirement R1.1 requires methods to identify such information. Many entities commented that Requirement R1.1 was too vague. In fact, several entities indicated they were confused as to whether the requirement

called for determining what information should be protected or if the requirement mandated labeling of the information. Some entities asked if specific classification was required. A few entities suggested that a specific classification, such as "confidential," should be included in the requirement. The SDT has considered this but does not believe it is appropriate to dictate a specific classification, such as "confidential." Some entities may use other classifications such as "CIP-Confidential," "Non-Public," "Highly Confidential," or many other designations. It is not the intent of the SDT to force all Registered Entities to modify their compliance documentation by mandating specific classifications. This initial part of the information protection program simply requires that the information in scope and to be protected is identified in some manner. Specific classification of information may be used as a method for identification, but is not specifically required. One commenter provided a specific recommendation to clarify that the information to be identified is that which is explained in the definition of BES Cyber System Information. The SDT agrees with this comment. The SDT is also responsive to industry comments and has enhanced the measures section of Requirement R1.

Some entities pointed out that the word "implemented" is unnecessary in the Requirement R1.1 requirement because it is contained in the overall Requirement R1 requirement language. They asked that the word "implement" be removed from Requirement R1.1 because it was redundant. Other entities stated that documentation is for measures or evidence, and the word "documented" should be removed from Requirement R1.1 requirement. The SDT has removed both "implemented" and "documented" from the requirement language. The term documented has been moved to the measures section.

There were additional comments related to the measures for Requirement R1.1. Some commenters asked how a repository could be a measure, and others asked for additional clarity. A repository could be a measure if the entity designated the repository or a section of the repository as the location for identifying and housing BES Cyber System Information and explained the protections afforded by the repository in the entity's Information Protection Program. It would be up to the entity to explain in their information protection program how the repository was used to identify their BES Cyber System Information.

In CIP-011 Requirement R1.2, many commenters again asked that additional clarification be added to the requirement concerning procedures for handling of BES Cyber System Information. The SDT agrees and has modified the requirement to clarify that handling procedures required are those which explain how the BES Cyber System Information is protected and secured.

Several comments asked for additional specifics concerning several topics regarding BES Cyber System Information; including transit, handling, and transmittal. The SDT agrees with this. The guidance section has been greatly expanded to address the topics requested.

Several entities desired additional specifics concerning the measures for Requirement R1.2. One entity commented: "This measure does not specify what records could be used …would sampling work in this case, and if so, what is the acceptable tolerance range for such sampling?" The SDT disagrees that it would serve the industry to mandate this level of specifics within CIP-011. It is the SDTs intent that the entities document their information protection program and associated procedures in accordance with the CIP-011 requirements, and that the entity maintains records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented program and associated procedures. A measure has been added which specifies this intent.

There were several comments requesting that the SDT address third party handling of BES Cyber System Information. The SDT agrees with this comment. Additional information has been added to guidance to cover this topic.

There were comments asking for more specifics concerning the topics of transit, handling, transmittal, distribution, physical access, purge, use, and disposal. The guidance section has been significantly enhanced to address the topics for which additional direction is warranted.

Some commenters recommended including procedures for reuse and disposal within Requirement R1. The SDT does not agree. SDT believes that the topic of reuse and disposal is complex and requires the specifics currently afforded the topic as specified in Requirement R2. If the topic was included in the Requirement R1 procedures, it could result in double jeopardy during audits, as auditors review compliance with Requirement R1 procedures and Requirement R2 handling during reuse and disposal.

Commenters stated that the reference to prior version under Requirement R1.2 refers to CIP-003-3, Requirement R5.3. They recommended that the reference be moved to Requirement R1.3. The SDT agrees.

The SDT received many comments related to Requirement R1.3. Many commenters recommended that the team specify that deficiencies found in the annual assessment should not be considered violations or potential violations. Some commenters asked that the SDT specify which deficiencies would be considered violations and which would not be considered violations. Commenters asked that the word "deficiencies" be changed to "lessons learned" or "flaws." The

SDT notes that the word “deficiencies” is appropriate because a deficiency notes there is a lack of completeness or insufficiency exists.

Some asked that the entire requirement be handled under the NERC FFT program and eliminated from the requirements. It is not up to the SDT to make the determination as to what is and what is not a violation. The SDT sought guidance from NERC and regional audit staff. The audit staff advised that some deficiencies could be seen as self-reportable violations or potential violations during audit if the entity failed to adhere to one of the specified sub-requirements. Other deficiencies might simply be process improvements or opportunities for improvements that do not violate any BES Cyber System Information sub-requirement from CIP-011. Further, the requirement calls for a periodic “assessment,” and such “assessment” may reveal things that went well in addition to things that could be improved. After considering industry comments and consulting with audit and NERC staff, the requirement will be handled under the Paragraph 81 project from the FERC Order on the find, fix, track and report process.

Some commenters did not like the grouping of all access control requirements within CIP 004. They asked that the requirement parts dealing with access to information be moved into CIP-011. This was discussed among the SDT. It was decided that the majority of entities favored the grouping of all access control within CIP 004. For consistency and in response to many previous comments, all access control requirements have been grouped into CIP 004. The requirement parts dealing with access control for BES Cyber System Information have, therefore, not been moved into CIP-011.

Some commenters asked where specifically the process covering reuse and disposal is required. Requirement R2 states: “Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal.” Therefore, Requirement R2 requires the entity to define their process concerning the topics within Requirement R2.

The SDT received comments questioning a discrepancy between the types of systems referenced in the definition of BES Cyber System Information vs. the applicability column for Requirement R2. Associated Protected Cyber Assets is included in the applicability column, but is not specifically referenced in the definition. The SDT’s intent is that if BES Cyber System Information as defined in the standard exists in the data storage media of applicable Cyber Assets, then Requirement R2 applies.

One commenter pointed out that the component obligations under CIP-011-1 are not clear and that the table headers under Requirement R2 may be adding to the confusion, as they are different for Requirements R2.1 and for R2.2. The SDT agrees and has corrected the table headers so that they are consistent within Requirement R2.

The second paragraph in Requirements R2.1 and R2.2 that deal with removal of the device from the PSP generated many comments. Some commenters asked that the language concerning removal from the PSP be clarified. Others asked that the language be moved to a separate part. Others stated that the language adds no value and asked that the language concerning removal from the PSP be deleted from the requirement part altogether. A few commenters suggested simplified language, and such comments were very much appreciated. The SDT has decided to remove from the requirement language dealing with removal from the PSP. The SDT will address the topic of removal from the PSP within the guidance section. The SDT made corresponding changes to the measures section.

Many commenters objected to use of the term “chain of custody” in Requirements R2.1 and R2.2. They stated that this is a legal term, and they believe it is not appropriate in the CIP standards. Others commented that the intended use of the term “who has possession,” as used in the requirement, was unclear. The SDT has decided to remove the entire second paragraph from Requirements R2.1 and R2.2, including the reference to “chain of custody.” The SDT made corresponding changes to the measures section and any reference to terms such as “chain of custody” has been removed from the measures section, as well.

Some commenters recommended combining Requirements R2.1 and R2.2 into one requirement part. The SDT disagrees with this recommendation. SDT believes there are sufficient differences in the handling of release for reuse versus disposal to warrant retaining both Requirement R2.1 and Requirement R2.2.

Within the Requirement R2.1 language, some commenters asked for additional clarity concerning the exception, which provides for reuse within other high impact or medium impact BES Cyber Systems. The SDT agrees with this comment and has added additional clarity to the guidance language specifying that the re-use exception applies to re-use in other systems that are identified in the applicable systems column as protections will continue after re-use.

The SDT received comments asking that “BES” be inserted in front of “Cyber Assets” within the reference to “applicable Cyber Assets that contain BES Cyber System Information...” within Requirements R2.1 and R2.2. The SDT disagrees with this direction. The requirement parts are applicable to Associated Physical Access Control Systems, Associated Electronic

Access Control or Monitoring Systems, and Associated Protected Cyber Assets. Therefore, the scope of Cyber Assets which may contain BES Cyber System Information is larger than the suggested term "BES Cyber Assets."

The SDT received at least one comment stating that it was unclear if Requirement R2.2 meant the storage media within the Cyber Asset, or if it also includes backup media. The requirement states: "Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media." The SDT's intent is that the scope includes the Cyber Asset data storage media. The scope of this requirement is not far reaching to include all possible locations of downstream information, such as backup copies outside the Cyber Asset. However, such copies of BES Cyber System Information would be governed by Requirement R1.

Some entities also asked for additional specifics concerning the actions a Responsible Entity shall take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media. One commenter questioned whether an attestation was specifically mandated. An attestation is not required by the standard. It is not the intent of the SDT to mandate specific actions within the requirements. However, the guidance section has been greatly expanded with guidance taken from NIST SP800-88, which provides additional assistance to entities.

One entity stated that it is not clear if requirement parts 2.1 and 2.2 permit media to be removed and possibly replaced with clean media, with the Cyber Asset then being redeployed or disposed of while the removed media continues to be maintained until separate erasure or destruction. The SDT considered this question and believes that the answer is: Yes, such actions would be permitted. The requirement calls for the entity to "take action to prevent unauthorized retrieval." This provides flexibility for the entity. As long as the entity documented the actions that they undertook; i.e., removing the media, securing the media, sanitizing the media in accord with the requirements, such action should be permitted.

SDT received the following comment: requirement part 2.1 appears to be two requirements and should be broken out if that is the intent. The current wording appears to pertain to cyber assets that contain BES Cyber System Information (i.e., network diagram). The second sentence appears to pertain to Cyber Assets within an ESP. There were other commenters asking for clarity concerning the storage media and the targets for sanitation in Requirement R2. Requirement R2 applies to any information within the Cyber Asset data storage media that meets the definition of BES Cyber System Information.

A few commenters stated that the standard needs to track the media and not necessarily the Cyber Asset the media is associated with. The SDT agrees with this comment. The Requirement R2 language has been modified to include the reference to "data storage media."

VSLs and VRFs

The SDT received at least one comment asking that the VRF for Requirement R1 be lowered. The SDT disagrees with the industry comment. The VRF for Requirement R1 is Medium in keeping with the FERC approved current VRF for this requirement. The VRF for Requirement R2 is already lower.

One commenter asked that the SDT add the "part" reference to the VSL so that the reader could easily understand the requirement number to which the VSL referred. The SDT agrees with this comment, and added the references to the VSL's.

Multiple commenters objected to the "zero defect" approach to VSL's for Requirement R2. The SDT agrees. The previously posted Requirement R2 VSLs have been modified to be less "device" specific. In the future, there will be additional emphasis on the entity providing good processes and security controls.

One commenter provided specific language for VSL's. Corresponding to recommendations that had been made concerning requirements, they asked that the VSLs should be revised to: Severe-not implemented, Higher-not measuring to detect, Moderate-not correcting detected flaws, Lower-not considering prevention. However, the requirement does not address prevention, and the VSLs must correspond to the requirements.

NERC will be sharing additional information on VRFs and VSLs in keeping with NERC's implementation of the FFT program.

Questions with Votes Only:

CIP-008, CIP-009, CIP-010 and CIP-011 Questions: Question 1

1. **CIP-008-5 R1 states "Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?**

Organization	Yes or No
Northeast Power Coordinating Council	No
Duke Energy	No
NESCOR/NESCO	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
PNM Resources	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No

Organization	Yes or No
NIPSCO	No
Xcel Energy	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Springfield Utility Board	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No

Organization	Yes or No
Kansas City Power & Light	No
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes

Organization	Yes or No
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes

Organization	Yes or No
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes

Organization	Yes or No
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
California Independent System Operator	Yes

2. **CIP-008-5 R2 states "Each Responsible Entity shall implement its documented Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?**

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
ACES Power Marketing	No
PNM Resources	No
Dairyland Power Cooperative	No

Organization	Yes or No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Lakeland Electric	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No

Organization	Yes or No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes

Organization	Yes or No
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes

Organization	Yes or No
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes

Organization	Yes or No
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Springfield Utility Board	Yes

Organization	Yes or No
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
California Independent System Operator	Yes

3. CIP-008-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
PPL Corporation NERC Registered Affiliates	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
ACES Power Marketing	No
PNM Resources	No
Progress Energy	No
CenterPoint Energy	No

Organization	Yes or No
Hydro One	No
Lakeland Electric	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Springfield Utility Board	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
MRO NSRF	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review	Yes

Organization	Yes or No
Committee	
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes

Organization	Yes or No
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes

Organization	Yes or No
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Nebraska Public Power District	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
Pacific Gas and Electric Company	Yes

Organization	Yes or No
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Kansas City Power & Light	Yes
California Independent System Operator	Yes

5. CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
PPL Corporation NERC Registered Affiliates	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No

Organization	Yes or No
Florida Municipal Power Agency	No
SMUD & BANC	No
ACES Power Marketing	No
PNM Resources	No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
NIPSCO	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
Lincoln Electric System	No
Lakeland Electric	No

Organization	Yes or No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
Utility Services Inc.	No

Organization	Yes or No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
NYISO	No
Farmington Electric Utility System	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Pepco Holdings Inc & Affiliates	Yes

Organization	Yes or No
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces	Yes

Organization	Yes or No
Corporation	
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes

Organization	Yes or No
PSEG	Yes
Liberty Electric Power, LLC	Yes
MEAG Power	Yes
Portland General Electric	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

6. CIP-009-5 R2 states "Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
MRO NSRF	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
SMUD & BANC	No
Puget Sound Energy, Inc.	No
PNM Resources	No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
Progress Energy	No

Organization	Yes or No
Hydro One	No
Independent Electricity System Operator	No
Lincoln Electric System	No
Bonneville Power Administration	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Alliant Energy	No
NYISO	No
Exelon Corporation and its affiliates	No
Los Angeles Department of Water and Power	No
California Independent System Operator	No
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
FirstEnergy	Yes

Organization	Yes or No
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes

Organization	Yes or No
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes

Organization	Yes or No
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
Oncor Electric Delivery Company LLC	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes

Organization	Yes or No
Utility Services Inc.	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes

7. CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
NRG Energy Companies	No
PPL Corporation NERC Registered Affiliates	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
SMUD & BANC	No
PNM Resources	No
Arizona Public Service Company	No
Progress Energy	No
Hydro One	No
Tampa Electric Company	No

Organization	Yes or No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
City of Austin dba Austin Energy	No
Oncor Electric Delivery Company LLC	No
CenterPoint Energy	No
Xcel Energy	No
New York Power Authority	No
MidAmerican Energy Company	No
PJM Interconnection	No
ISO New England Inc.	No
ACES Power Marketing	No
Puget Sound Energy, Inc.	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Brazos Electric Power Cooperative	No
IRC Standards Review Committee	Yes
The united illuminating Company	Yes
Lakeland Electric	Yes
Southern California Edison Company	Yes
Clallam County PUD No.1	Yes

Organization	Yes or No
Northeast Utilities	Yes
Portland General Electric	Yes
MRO NSRF	Yes
NESCOR/NESCO	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
Comment Development SME list	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes

Organization	Yes or No
Western Area Power Administration	Yes
Dairyland Power Cooperative	Yes
Tri-State G&T - Transmission	Yes
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes

Organization	Yes or No
National Grid	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
MEAG Power	Yes
Utility Services Inc.	Yes

Organization	Yes or No
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Kansas City Power & Light	Yes
California Independent System Operator	Yes
Luminant	
American Transmission Company, LLC	
Avista	

9. CIP-010-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
FirstEnergy	No
SMUD & BANC	No
ACES Power Marketing	No
PNM Resources	No

Organization	Yes or No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
Lower Colorado River Authority	No
LCRA Transmission Serivces Corporation	No
Hydro-Quebec TransEnergie	No
Lincoln Electric System	No
The united illuminating Company	No
Tampa Electric Company	No

Organization	Yes or No
MidAmerican Energy Company	No
NV Energy	No
Massachusetts Municipal Wholesale Electric Company	No
Detroit Edison Company	No
The Empire District Electric Company	No
Ameren	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No

Organization	Yes or No
Utility Services Inc.	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
Springfield Utility Board	No
NYISO	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
PPL Corporation NERC Registered Affiliates	Yes
Associated Electric	Yes

Organization	Yes or No
Cooperative, Inc. (NCR01177, JRO00088)	
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes

Organization	Yes or No
MEAG Power	Yes
Portland General Electric	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

10. CIP-010-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
MRO NSRF	No
NESCOR/NESCO	No
SMUD & BANC	No
ACES Power Marketing	No
PNM Resources	No
Southern Company Services, Inc.	No
Western Area Power Administration	No

Organization	Yes or No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
ATCO Electric	No
Hydro-Quebec TransEnergie	No
Lincoln Electric System	No
The united illuminating Company	No
Bonneville Power Administration	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy	No

Organization	Yes or No
Company	
Detroit Edison Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Electric Power Company	No
Alliant Energy	No
Springfield Utility Board	No
NYISO	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No

Organization	Yes or No
California Independent System Operator	No
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes

Organization	Yes or No
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Serivces Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes

Organization	Yes or No
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

11. CIP-010-1 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
IRC Standards Review Committee	No
PNM Resources	No
Southern Company Services, Inc.	No

Organization	Yes or No
Western Area Power Administration	No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Consumers Energy Company	No
Lincoln Electric System	No
The united illuminating Company	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy	No

Organization	Yes or No
Company	
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
Springfield Utility Board	No

Organization	Yes or No
NYISO	No
Exelon Corporation and its affiliates	No
Los Angeles Department of Water and Power	No
Kansas City Power & Light	No
California Independent System Operator	No
PPL Corporation NERC Registered Affiliates	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes

Organization	Yes or No
SPP and Member companies	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Niagara Mohawk (dba National Grid)	Yes

Organization	Yes or No
National Grid	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
MEAG Power	Yes

Organization	Yes or No
Portland General Electric	Yes
Utility Services Inc.	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes

13. CIP-011-1 R1 states "Each Responsible Entity shall implement an information protection program that includes each of the applicable items in CIP-011-1 Table R1 – Information Protection." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
PNM Resources	No
National Rural Electric Cooperative Association (NRECA)	No
Progress Energy	No
CenterPoint Energy	No

Organization	Yes or No
Tri-State G&T - Transmission	No
Xcel Energy	No
Snohomish County PUD	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
PSEG	No
Liberty Electric Power, LLC	No
Texas Reliability Entity	No
PJM Interconnection	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Exelon Corporation and its affiliates	No
Deseret Power	No
Kansas City Power & Light	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes

Organization	Yes or No
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes

Organization	Yes or No
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power	Yes

Organization	Yes or No
Administration	
Lakeland Electric	Yes
Tampa Electric Company	Yes
New York Power Authority	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
Nebraska Public Power District	Yes
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes

Organization	Yes or No
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
California Independent System Operator	Yes

14. CIP-011-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
ACES Power Marketing	No
PNM Resources	No
Southern Company Services, Inc.	No
Progress Energy	No
Tri-State G&T - Transmission	No

Organization	Yes or No
Hydro One	No
Independent Electricity System Operator	No
The united illuminating Company	No
Xcel Energy	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
Ameren	No
NextEra Energy, Inc.	No
Liberty Electric Power, LLC	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery	No

Organization	Yes or No
Company LLC	
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Pacific Gas and Electric Company	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes

Organization	Yes or No
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes

Organization	Yes or No
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes

Organization	Yes or No
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards
Comment Form D
Definitions and Implementation Plans

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Index to Questions, Comments, and Responses

Questions with Summaries Included: 15

QUESTION D8 – DEFINITIONS: 15

QUESTION D9 – DEFINITIONS: 19

QUESTION D10 – DEFINITIONS: 22

QUESTION D11 – DEFINITIONS: 25

QUESTION D12 – DEFINITIONS: 27

QUESTION D13 – DEFINITIONS: 30

QUESTION D14 – DEFINITIONS: 35

QUESTION D16 – IMPLEMENTATION PLAN: 38

QUESTION D17 – DEFINITIONS AND IMPLEMENTATION PLAN: 42

Questions with Votes Only: 51

1. Do you agree with the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset? 51

2. Do you agree with the proposed definition of Control Center? 57

3. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager? 64

4. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager? 71

5. Do you agree with the proposed definitions of Electronic Access Control or Monitoring Systems, Interactive Remote Access, and Intermediate Device? 78

6. Do you agree with the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset? 85

7. Do you agree with the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident? 92

15. Do you agree with the changes made to the proposed implementation plan since the last formal comment period? 99

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
11. Bruce Metruck	New York Power Authority	NPCC 6										
12. Lee Pedowicz	Northeast Power Coordinating Council	NPCC 10										
13. Robert Pellegrini	The United Illuminating Company	NPCC 1										
14. Si Truc Phan	Hydro-Quebec TransEnergie	NPCC 1										
15. David Ramkalawan	Ontario Power Generation, Inc.	NPCC 5										
16. Brian Robinson	Utility Services	NPCC 8										
17. Michael Jones	National Grid	NPCC 1										
18. Michael Schiavone	National Grid	NPCC 1										
19. Wayne Sipperly	New York Power Authority	NPCC 5										
20. Tina Teng	Independent Electricity System Operator	NPCC 2										
21. Don Weaver	New Brunswick System Operator	NPCC 2										
22. Ben Wu	Orange and Rockland Utilities	NPCC 1										
23. Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC 3										
24. Silvia Parada Mitchell	NextEra Energy, LLC	NPCC 5										
2. Group	Annabelle Lee	NESCOR/NESCO										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3. Group	Jason Marshall	ACES Power Marketing						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6. Shari Heino		Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Tim Soles	Occidental Power Services, Inc.	ERCOT	3
4.	Andy Gallo	Austin Energy	ERCOT	1
5.	Andy Gallo	Austin Energy	ERCOT	3
6.	Andy Gallo	Austin Energy	ERCOT	4
7.	Andy Gallo	Austin Energy	ERCOT	5
8.	Andy Gallo	Austin Energy	ERCOT	6

8.	Group	Emily Pennel	Southwest Power Pool Regional Entity									X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8. Annie Terracciano	Northern Lights Inc.	WECC 3										
9. Aleka Scott	PNGC	WECC 4										
10. Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11. Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12. Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13. Margaret Ryan	PNGC	WECC 8										
12. Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13. Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14. Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. M & A Electric Power Cooperative		SERC	1, 3									
4. Northeast Missouri Electric Power Cooperative		SERC	1, 3									
5. N.W. Electric Power Cooperative, Inc.		SERC	1, 3									
6. Sho-Me Power Electric Cooperative		SERC	1, 3									
15. Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X						
Additional Member	Additional Organization	Region	Segment Selection									
1. Oglethorpe Power Corporation		SERC	5									
2. Georgia Transmission Corporation		SERC	1									
16. Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X
Additional Member	Additional Organization	Region	Segment Selection									
1. MAHMOOD SAFI	OPPD	MRO	1, 3, 5, 6									
2. CHUCK LAWERENCE	ATC	MRO	1									
3. TOM WEBB	WPS	MRO	3, 4, 5, 6									
4. JODI JENSON	WAPA	MRO	1, 6									
5. KEN GOLDSMITH	ALTW	MRO	4									
6. DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6									
7. JOE DEPOORTER	MGE	MRO	3, 4, 5, 6									
8. SCOTT NICKELS	RPU	MRO	4									
9. TERRY HARBOUR	MEC	MRO	1, 3, 5, 6									
10. MARIE KNOX	MISO	MRO	2									
11. LEE KITTELSON	OTP	MRO	1, 3, 4, 5									
12. SCOTT BOS	MPW	MRO	6, 1, 3, 5									
13. TONY EDDLEMAN	NPPD	MRO	1, 3, 5									
14. THERESA ALLARD	MPC	MRO	1, 3, 5, 6									
17. Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing												
18. Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				
Additional Member	Additional Organization	Region	Segment Selection									
1. Timothy Beyrle	City of New Smyrna Beach	FRCC	4									
2. James Howard	Lakeland Electric	FRCC	3									

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. Greg Woessner	Kissimmee Utility Authority	FRCC	3									
4. Lynne Mila	City of Clewiston	FRCC	3									
5. Joe Stonecipher	Beaches Energy Services	FRCC	1									
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4									
7. Randy Hahn	Ocala Utility Services	FRCC	3									
19. Group	Joseph DePoorter	Madison Gas and Electric Company			X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Darl Shimko	MGE	MRO	3									
2. Joseph DePoorter	MGE	MRO	4									
3. Steve Schultz	MGE	MRO	5									
4. Jeff Keebler	MGE	MRO	6									
20. Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Mark Jones	Pepco	RFC	1									
21. Group	Rick Terrill	Luminant					X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Mike Laney	Luminant Generation Company LLC	ERCOT	5									
2. Tim Soles	Occidental Power Services, Inc.	ERCOT	6									
3. Tim Soles	Occidental Power Services, Inc.	ERCOT	3									
4. Andy Gallo	Austin Energy	ERCOT	1									
5. Andy Gallo	Austin Energy	ERCOT	3									
6. Andy Gallo	Austin Energy	ERCOT	4									
7. Andy Gallo	Austin Energy	ERCOT	5									
8. Andy Gallo	Austin Energy	ERCOT	6									
9. Brenda Hampton	Luminant Energy Company LLC											
22. Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
1. Kevin Smith	BANC	WECC	1									
23. Group	Scott Brame	NCEMC	X				X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				

Additional Member	Additional Organization	Region	Segment Selection
1. Rayburn Country Electric Cooperative		SPP	
2. Empire District Electric		SPP	1
3. City Utilities of Springfield		SPP	4
4. Westar Energy		SPP	1, 3, 5, 6
5. Cleco Power		SPP	1, 3, 5, 6

25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						

Additional Member	Additional Organization	Region	Segment Selection
1. Pawel Krupa		WECC	1
2. Dana Wheelock		WECC	3
3. Hao Li		WECC	4

27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					

Additional Member	Additional Organization	Region	Segment Selection
1. Denise Lietz	Puget Sound Energy	WECC	1
2. Erin Apperson	Puget Sound Energy	WECC	3

28.	Group	Michael Mertz	PNM Resources	X		X							

Additional Member	Additional Organization	Region	Segment Selection
1. Laurie Williams	Public Service Co. of New Mexico	WECC	1
2. Michael Mertz	Public Service Co. of New Mexico	WECC	3

29.	Group	Sasa Maljukan	Hydro One	X									

Additional Member	Additional Organization	Region	Segment Selection
1. David Kiguel	Hydro One	NPCC	1

30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION D8 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the SDT modified some of the definitions. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity. Please see the redlined version of the definitions for a complete set of revisions to each definition.

BES Cyber Asset

Several commenters stated that the definition of BES Cyber Asset was confusing, citing the complex construction of the definition and the fact that it stated that each BES Cyber Asset must be part of a BES Cyber System while the background and technical basis stated that Responsible Entities had flexibility in using BES Cyber Asset or BES Cyber Systems. Many provided alternative language. Multiple commenters asked whether there is a need for network connectivity between BES Cyber Assets to be considered a BES Cyber System. The SDT made the addition of the statement about each being part of at least one BES Cyber System to the definition of BES Cyber Asset to ensure that each Cyber Asset would be included in at least one BES Cyber System, and did not preclude the option of having a BES Cyber System that consists of a single BES Cyber Asset. The SDT believes this preserves entities' flexibility while providing better homogeneity in the application of requirements: requirements uniformly apply to BES Cyber Systems. There is no presumption of connectivity options in the definition of a BES Cyber System, but Responsible Entities may find that application of requirements and relationship with other definitions such as ESPs may be significant input to the Responsible Entities' options.

Several commenters suggested that the definition of BES Cyber Asset include an addition in its qualification for connection to a network within an ESP in addition to connection to a Cyber Asset within an ESP. The SDT believes that the clarification is useful in ensuring the application to those transient cyber assets that are connected to the network as well as directly to the Cyber Assets within an ESP and has made the modification to address the comment.

One commenter suggested modifications to definitions of Cyber Asset. The SDT considered these comments and does not believe that these suggestions are substantively different or would add clarity to the definitions.

One commenter suggested dropping the word “misused” from the definition of BES Cyber Asset. The SDT has specifically included the word “misuse” in response to comments from FERC Order 706 and believes that it includes intent of a malicious compromise that is not otherwise conveyed.

Mid-American’s comment with respect to the use of the capitalized term “Systems” has been addressed and the definition now used the more generic term “systems” instead of the defined term.

One comment was on the use of the verb phrase “affect the reliable operation…” The SDT considered these comments and believes that this verb phrase is appropriate as it applies to the Facilities, systems and equipment, not the BES Cyber System.

Many commented on the complexity of the parenthetical sentence in the definition of BES Cyber Asset and suggested alternative language: the SDT considered these comments and believes that the suggested alternatives do not add additional clarity to the definition. In addition, other commenters stated that the parenthetical qualification should be used in defining the term Transient Cyber Asset. The SDT considered the options and chose to not have a separately defined term because of the very small number of requirements where it is used.

Many entities commented on the use of “adversely impact” in the definition of BES Cyber Asset and suggested using the defined term “Adverse Reliability Impact” instead. The SDT considered the use of the defined term and believes that the defined term describes an impact which is much more severe than the intent of the term used in the definition.

Several commenters requested clarification of the terms “within 15 minutes”: the SDT has included additional clarification in the guidelines and technical basis section.

–One commenter suggested to remove the 15 minute criteria as it is believed that it will lower the security of assets by removing them from qualifications. In response, The SDT notes that, in using 15 minutes, it is attempting to articulate a time boundary for “Real-time” impact. The term “Real-time” in the Glossary of Terms used in NERC Reliability Standards did not provide enough specificity in the definition for this purpose. The SDT scoped the CIP standards to those Cyber Assets that would have an effect on Real-time operations.

Many entities commented on the qualification on "redundancy" in the definition of BES Cyber Asset. The SDT believes that the impact of a cyber asset on the function of a given Facility, system or equipment is independent on whether that Facility, system or equipment is redundant or not: in most cases, the redundancy is configured to handle loss of a Facility, but does not consider degradation or misuse of that Facility, system or equipment. The application guidelines and technical basis section contains a discussion of this concept.

One entity suggests that the definition of BES Cyber Asset is much improved still does not prescribe how to document that an asset has been connected to the BES for less than 30 days. It is not the purpose of the definition to prescribe methods of documentation. That flexibility is left to the entity. Assets connected on a transient, temporary basis are not intended to be a BES Cyber Asset, and the 30 days in the definition is intended to clarify that temporary connections, e.g., for maintenance purposes, are not intended to be included within the definition.

BES Cyber Systems

One commenter suggested replacing "to perform" with "used to facilitate the performance of…", citing examples where the BES Cyber System may not directly perform a reliability function, but may support one or more functions. The SDT believes that the introduction of the proposed language would result in further questions on the meaning of the word "facilitate" and the extent of the scope of that term.

In response to a suggestion to use the word "identified for functions…" the SDT believes that the suggested wording did not bring additional clarity to the definition of BES Cyber Systems.

One commenter stated that the use of the term "Responsible Entity" is confusing, citing overlap, redundancy or conflict with the term Functional Entity. The SDT believes that these are two distinctly different terms: the Responsible Entity refers to the set of Functional Entities that is responsible for compliance to the requirements of the standard. Within a given standard, a given set of requirements may apply to different Functional Entities, depending on the specific requirements. The term "responsible entity" is defined in the applicability section. The application of the defined term that contains the term "responsible entity" in a standard is subject to the preamble in Section 4.

Cyber Asset

Multiple comments were provided on the use of the word "programmable" in the definition of Cyber Asset, citing that it was too broad, and the need for a routable connectivity qualification. The SDT considered these comments and notes

that the definition of Cyber Asset as it pertains to "programmable electronic devices" is part of the current approved definition. The SDT further believes that consideration of connectivity in this generic definition is inappropriate.

One commenter stated that the qualification of "…data in these devices…" ignores data in motion. The SDT believes that the inclusion of data other than that in these devices has unintended consequences in the application of requirements.

Other

Multiple commenters suggested the addition of a defined term BES Site, or similar concepts: the SDT has considered the rationale and has opted to use the concepts in the drafting of new language and approach in the requirement language and attachments, instead of defining a term that would be used in only a few requirements.

One commenter requested that the language for the defined term Protected Cyber Asset be reviewed for clarity. The SDT has reviewed the definition and made modifications to the definition and added guidance in the background section to clarify the concept.

QUESTION D9 – DEFINITIONS:

Do you have any comments on the changes to the proposed definition of Control Center? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the SDT modified all of the definitions based on stakeholder comments. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity. Please see the redlined version of the definitions for a complete set of revisions to each definition.

Many commenters questioned the need for a definition of Control Center, citing standards in other reliability standards that also have control center applicability without the need for a formal definition. The SDT notes that the Control Center is subject to a number of High and Medium Impact criteria and that they host a large number of BES Cyber Systems that are essential to the reliable operation of the BES. The SDT believes that, because of these necessarily crucial functions, a formal definition is appropriate to clearly define the scope of applicability, as demonstrated by many questions on differentiation between a facility's control room, which is typically considered part of the facility, and Control Centers, which are considered separate facilities hosting operating personnel controlling and monitoring multiple facilities. Many commented that a formal definition used in the CIP context could be confusing to the industry in the context of other reliability standards that apply to control centers. The SDT believes that a formal definition clarifies the scope of applicability for Control Centers and would not affect other reliability standards that have not used the defined term, but rather a "common" undefined term for control center. NERC's standard use of capitalized terms for NERC Glossary defined terms provides clarity on when the defined term is used.

Two commenters proposed alternative language for the definition of the Control Center that uses Functional Entities. The SDT has considered the alternatives and believes that the proposals contain a circular reference that would not provide better clarity. The SDT has carefully considered the current proposed language and believes that it accurately describes the intended target of applicability.

Others suggested that Control Centers that use voice or manual instructions be categorized as Low Impact. The SDT notes that Cyber Systems that provide information to Control Center operators that use manual or voice to effect control operations on BES assets in real-time based on that information must be subject to the same protection as those that

trigger automated operation. If the communication or manual operation results from information provided for real-time operations, there is no rationale for categorizing them as a lower impact.

Multiple commenters expressed concern that in certain instances, a facility may not be performing the function of a TOP 24/7 and remains unmanned the rest of the time, and suggested the addition of the 24/7 qualification. The SDT sees no rationale in adding this qualifier, since the impact of the facility that performs these functions remains the same. In the same comment, commenters cited the case of a TOP registration for a single facility. The SDT responds that the "control and monitoring" facility of a single facility does not meet the definition of a Control Center, but rather as part of the facility it is controlling.

Several commenters suggested slightly modified language which focuses on hosted BES Cyber Systems rather than operating personnel. One commenter suggested that the Control Center is the BES Cyber System that performs these functions. The SDT believes that operating personnel is central to the traditional understanding of a Control Center facility. The definition currently specifies one or several facilities. In the facilities (or site) based approach, the identification of the BES Cyber Systems that perform the Control Center functions may bring in other facilities such as data centers that perform these functions.

Many commenters requested clarifications on the terms "facility" and "locations" used in the definition of the Control Center. The SDT uses the general term "facility" (as opposed to the glossary term "Facility") in its generic sense of one or several physical structures that comprise a Transmission substation or station, a generating plant or a Control Center. In the case of a Control Center, a facility could be considered a building or campus consisting of several closely located buildings. However, additional facilities may be brought in as the BES Cyber Systems are defined, including associated data centers that perform the reliability tasks. In the context of the definition of Control Center, a location generally refers to the set of BES Facilities at a single site, and generally constitutes a single point of connection to the BES. Because of the many types of configurations, the SDT used the generally accepted concept of geographic location rather than including all the nuances of the different ways Facilities are connected to the BES.

One commenter requested a definition for data center. The SDT believes that "data center" is a well understood term and that many definitions of data center exist elsewhere that adequately explain what they are.

One commenter pointed out that the SDT uses the term reliability functional tasks and reliability tasks interchangeably in the standard. The SDT has used the terms interchangeably for the reliability tasks defined in the NERC functional model. The SDT has made the change in the definition of Control Center to be consistent to the use of reliability tasks elsewhere.

One commenter requested further qualification of the term “operating personnel”. The SDT notes that this term is used in many reliability standards, in particular, the PER series of standards. They are used to refer to personnel that perform the real-time control and monitoring operations necessary for the real-time functions for RC, BA, TOP and GOP functional entities. The definition of the Control Center refers to these functions.

One commenter suggested the addition of “NERC Certified” to operating personnel. The SDT notes that the addition of the term NERC Certified restricts the applicability of the term to just RCs, BAs and TOPs, since there is no requirement for certification of GOP operating personnel. This is not the intent of the SDT in drafting this definition.

One commenter suggested that Control Center as it applies to the function of a Generation Operator has a threshold of generation located at two or more locations, and that this single qualifier could unintentionally sweep in the control centers for multi-location generation of very small capacity. The commenter suggested that a capacity qualifier be added to this definition. The SDT does not think that the threshold should be in the definition, but has amended the criterion for generation Control Centers in the Medium Impact category that addresses this comment. BES Cyber Systems for Control Centers below the Medium Impact threshold must still be protected as Low Impact. See the response to A03 - Attachment 1, Medium Impact.

QUESTION D10 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the comments related to these definitions largely noted minor improvements to the definitions rather than identifying major issues or disagreement.

BES Cyber System Information

Several comments about the definition of BES Cyber System Information highlighted minor issues with the structure of the definition rather than its content. Commenters suggested re-organizing the definition such that the list of examples came last. The SDT considered this comment and agreed that it made the definition more readable without changing its overall intent. This suggestion has the effect of collecting the explanatory language together to improve comprehension of the definition. Some commenters suggested that the examples should be removed from the definition altogether. The SDT noted that it is not uncommon to find examples in definitions in the NERC Glossary of Terms Used in NERC Reliability Standards (e.g. Facility, Operating Plan, Year One, etc.). Additionally, the SDT had concerns about removing the list of examples, since a similar list of examples has been used since the version 1 CIP Standard to provide direction as to what information should be included in the NERC CIP information protection program. The SDT believed that continuing to provide a list of examples would facilitate a transition between Version 3 and 4 of the CIP standards to Version 5.

Additionally, some commenters took issue with the phrase "developed by the Responsible Entity" as it relates to security procedures and security information. The commenters noted that protection of security information might be appropriate even if this information was developed by an outside party. The SDT agrees with this comment. The intent of the SDT was to prevent the inclusion of information that might be publicly available. Therefore, the SDT has modified the definition to better align with the intent and has clarified that security procedures and security information "not publicly available" are examples of BES Cyber System Information.

Some commenters noted ambiguity in the definition of BES Cyber System Information in the phrase "unauthorized distribution" of information. The SDT appreciates the concern over ambiguity, but encourages the industry to consider this definition in context of the overall information security program that is required under NERC CIP-011-1 and related

requirements in NERC CIP-004-5. Consideration of "unauthorized distribution" should be taken in the context that access to locations where information that has been judged to meet this definition is stored is required to be authorized in CIP-004-5 R4, part 4.1, element 4.1.3 and proper handling of this information is required in CIP-011-1 R1, part 1.2. The Responsible Entity should use this context to determine whether this information, in the hands of someone who has not been granted access "based on need," could lead to a compromise in security, directly or indirectly, of the BES Cyber System.

Other commenters noted ambiguity over the phrase "pose a security threat" and recommended that this phrase be removed. The concept of posing a "security threat" to the BES Cyber System should also be considered in context of the requirements of the NERC CIP Standards, particularly CIP-011-1 R1. BES Cyber System Information is intended to be identified and protected in accordance with an overall information protection program. As such, it is anticipated that the Responsible Entity will include some process to identify the information applicable to this program. As not all information will lead to directly gaining access to BES Cyber Systems but may in other ways compromise the overall security of the BES Cyber System, the SDT does feel that it is prudent to remove this phrase.

CIP Exceptional Circumstances

Several commenters identified an issue with the phrase in the definition of CIP Exceptional Circumstances that included "an imminent or existing hardware, software, or equipment failure." Commenters pointed out that the collection of forensic data in CIP-009-5 Requirement R1.5, draft 2 was subject to CIP Exceptional Circumstances. Through the inclusion of hardware, software, or equipment failure as a CIP Exceptional Circumstance, a Responsible Entity could essentially choose to never comply with the collection of forensic data. After consideration, the SDT chose to modify the requirement in CIP-009-5 R1.5 to indicate that data preservation should not impede or restrict recovery. The SDT believes that hardware, software, or equipment failure is a reasonable component to include as a CIP Exceptional Circumstance given the cyber-physical relationship of the electric grid and its supporting Cyber Assets.

Additionally, commenters noted that the involvement of the conditions identified in the definition of CIP Exceptional Circumstances is not always known ahead of time. Specifically, commenters suggested that the SDT add the phrase "threatens to involve." The SDT considered this suggestion and decided that given the supporting framework required through the cyber security policies in CIP-003-5 to invoke a CIP Exceptional Circumstance, this was a reasonable and beneficial modification to the definition.

Commenters also questioned when CIP Exceptional Circumstances can be invoked. No modification was made to the standard, but in response, the intent of the SDT is to allow the use of CIP Exceptional Circumstances only where specifically identified in the language of the requirement. Additionally, CIP Exceptional Circumstances should be declared using the provisions identified in the Responsible Entity's cyber security policy as per CIP-003-5 R1.

CIP Senior Manager

Numerous commenters suggested minor modifications to the definition of CIP Senior Manager. The intent of the SDT was to include a definition of CIP Senior Manager in the NERC Glossary of Terms Used in NERC Reliability Standards so as to make clear who the required approver is when the term is used across the body of CIP Standards. The SDT did not intend to modify the content of the definition, which has remained unchanged since version 2 of CIP-003-2 when the role of the senior manager was clarified in response to FERC Order 706, paragraph 381. The SDT was compelled, given the current state of the CIP Standards being in their 5th version, by comments that suggested that in addition to the authority and responsibility for leading and managing the implementation of the requirements, that the CIP Senior Manager should also have the overall authority and responsibility for leading and managing "continuing adherence" to the requirements within the NERC CIP standards.

The SDT also received comments that the definition of CIP Senior Manager should specifically call out CIP-002 through CIP-011 as this is the set of cyber security standards to which the CIP Senior Manager has the authority and responsibility for. The SDT received similar comments in response to draft 1 of the posting of this definition. At that time, the SDT responded that the definition was only applicable where it is specifically used in the standards. Additionally, the concern appeared to specifically reference CIP-001, which at the time was planned for retirement as part of project 2009-1. However, given the dynamic nature of project 2009-1 and the relative ease to which this definition could be modified in the future should additional standards be added to which the CIP Senior Manager authority should apply, the SDT is persuaded to include a reference specifically to "CIP-002 through CIP-011" in the definition of CIP Senior Manager.

QUESTION D11 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Physical Access Control Systems and Physical Security Perimeter? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the SDT has address all comments and has made clarifying changes to the definitions.

Physical Security Perimeter (PSP)

One commenter proposed modifying the definition to apply only for applicable BES Cyber Systems. However, applicability cannot be determined by a definition. We have clarified in the applicability column in standards CIP-004 through CIP-011 that PSPs are not applicable solely upon meeting the definition.

One commenter requested that a list of example Cyber Assets that should be included within a PSP. In response, the standards specify more clearly which Cyber Assets must reside in a PSP.

One commenter suggested the definition of PSP should reference the correct defined term: Electronic Access Control or Monitoring Systems, and the SDT has made this change.

One commenter suggested that the definition is ambiguous about (1) whether the perimeter is two or three dimensional, (2) whether there are different expectations for High and Medium BES Cyber Systems and (3) what size hole provides access. In response, the additional specificity for the perimeter and access points would limit the options entities have in applying the requirement. The SDT believes we have struck the right balance in this requirement to allow entities flexibility in their approach while describing the end result. In regard to the difference between physical protection in High and Medium Impact BES Cyber Systems, this is specified in CIP-006-5.

Physical Access Control System (PACS)

Several commenters proposed removing "alert" from the definition to avoid the interpretation that security guard workstations are included in scope. In response, the alerting component should include the system sending out the alert

and does not include all recipient persons or devices of the alert. We do not believe this needs further clarification in the definition.

One commenter suggested that examples should not be included in the definition and the wording "exclusive of devices…at the PSP" could exclude more asset than intended. In response, we note that examples should not change the definition but can be helpful in forming context. For PACS, these examples are useful for explicitly clarifying perimeter devices, which by nature cannot have the same physical protection are outside of scope.

One commenter suggested putting a comma to make clear the example applies to Cyber Assets. In response, the example does modify the locally mounted hardware and devices and not the Cyber Assets. In other words, the example is for the exclusion.

One commenter suggested that the SDT needs to ensure electronic visitor log books are not captured in the definition and that the exclusion uses "or" instead of "and" for the examples. In response, a visitor log book would not be within scope because it logs visitors and not access, and including an electronic visitor log book could cause the interpretation that any additional logging would be considered out of scope. Also, "or" and "and" are logically interchangeable in the example list, and we do not find a need to make any change.

One commenter suggested that monitoring Cyber Assets should be included in the definition. In response, we did not include monitoring devices because those are typically outside of the PSP and serve as a supplementary protection. Although these can be used to comply with monitoring requirements, it becomes problematic to apply additional CIP Standards requirements without creating a complex protection loop.

One commenter suggested changing the word "exclusive" to "excluding", but the SDT chooses to retain the originally posted wording.

One commenter suggested the definition should include workstations used to provision physical access and monitor alarms. In response, the proposal would expand the definition scope beyond what the SDT considers unacceptable risk. The level of effort required to protect this significant population of assets would far exceed the security benefit of doing so. As an example, this could include all cell phones and pagers carried by staff for responding to alarms.

QUESTION D12 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Electronic Access Control and Monitoring Systems, Interactive Remote Access, and Intermediate Device? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, clarifying language was added to each definition to highlight stakeholders concerns.

Interactive Remote Access

Several commenters requested clarification for the inclusion of dial-up access in the definition. Upon further review, this has been removed from the definition. The important part to note is that Interactive Remote Access is when using a remote access client or other remote access technology, regardless of the type of connectivity.

One commenter proposed that the definition of Interactive Remote Access be modified to exclude serially connected, non-routable, non-network connected devices. The definition did not include serially connected, non-routable, non-network connected devices. However, the definition has been modified to specifically address the use of a routable protocol.

Several commenters requested restructuring of the definition to highlight the criteria for identifying Interactive Remote Access. The definition has been updated as requested to highlight that the first criteria is the use of a remote access client or other remote access technology.

Several commenters requested more information regarding examples of a remote access client or remote access technology. Additional information is available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested that list item two, "Cyber Assets used or owned by employees" be modified as "Cyber Assets used by employees". The commenter considers employee-owned devices inappropriate for use in Interactive Remote Access. Employee-owned devices were added to the definition based on comments received in Project 2010-15:

Expedited Revisions to CIP-005-3. This was added to address industry need to have remote access not limited to use of only company-owned assets for remote access. This is in support of pandemic and other emergency planning situations.

One commenter recommended adding the words "owned by or under the control of the Responsible Entity" to prevent the inclusion of equipment owned by Managed Security Providers in the standards. Connections by vendors, contractors, and consultants should be protected to the same standard as assets owned by the entity. Assets owned or used by vendors, contractors, and consultants were added to the definition based on comments received in Project 2010-15: Expedited Revisions to CIP-005-3. This was added to address industry need to have remote access not limited to use of only company-owned assets for remote access. This is in support of pandemic and other emergency planning situations.

Multiple commenters noted that the sentence beginning with "Remote access may be initiated from ..." adds no value, does not address all circumstances, and should be deleted. They further noted it is possible to initiate remote access from assets owned by others not listed. The information was added to the definition based on comments received in Project 2010-15: Expedited Revisions to CIP-005-3. This was added to address industry need to have remote access not limited to use of only company-owned assets for remote access. Please see the opposing perspective noted by other entities. The definition states that access "may be initiated" and not "shall be initiated" to allow for flexibility and not define the three scenarios as the finite and final list.

Intermediate Device

One commenter was concerned with the phrase "performing access control" existing as part of the definition of an Intermediate Device. It is the SDTs intent that an Intermediate Device is classified as an Electronic Access Control or Monitoring System. The definition of Electronic Access Controls or Monitoring Systems has been modified to include Intermediate Device.

One commenter requested clarification as to the types of devices that could be used as an Intermediate Device. The SDT specifically did not list proxy or other technology to allow flexibility in how an entity may implement a solution that best meets their needs. Per CIP-005-5 Requirement R2.1, the Intermediate Device must be used before accessing a BES Cyber System or Protected Cyber Asset. Per the definition, the Intermediate Device must not be inside of an ESP. Additional references regarding the Intermedate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

Multiple commenters noted concerns with the language, “The Intermediate Device must not be located inside the Electronic Security Perimeter”. Comments were received that this should be added to the requirements and removed from the definition. Some consider the second sentence of the definition to be unnecessary, too prescriptive, and should be deleted. Some offered recommendations for changes to the definition to allow for future technology developments.

- The SDT considers this language to be defining and clarification of the device. The performance under the requirement is that an entity utilizes the intermediate device. Further, definitions are part of the standards and carry the same force as the requirements.
- The location of the Intermediate Device was included in the definition to address numerous industry questions on this matter both in Project 2008-06 Cyber Security Order 706 Version 5 CIP standards and Project 2010-15: Expedited Revisions to CIP-005-3. Many entities have raised questions regarding the location of the device based on termination point of encryption and other issues.
- The only restriction placed on the Intermediate Device is that it not be inside of an ESP. Access authentication should be performed before the user is granted access through the ESP. Encryption should be terminated outside of the Electronic Security Perimeter so that event logging within the ESP is not negatively impacted. The SDT specifically did not list other specifics to allow flexibility in how an entity may implement a solution that best meets their needs whether through the use of a multi-purpose device or other architecture. Additional references regarding the Intermediate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter noted concerns that the term "device" is not clear in defining the Intermediate Device. They recommend using the term “Intermediate Cyber Asset”. The definition includes the term “Cyber Asset” which is defined as “programmable electronic devices including the hardware, software, and data in those devices”. The SDT has chosen the unique term “Intermediate Device” to allow for the use of one or more Cyber Assets making up the device.

QUESTION D13 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:
Based on stakeholder comments, the SDT clarified language to the definitions.

Electronic Access Point
Multiple commenters asked for clarity if an Electronic Access Point (EAP) must be routable on both sides. In response, the SDT's intent is that if the device is accessible from outside the Electronic Security Perimeter (ESP) with a routable protocol then an EAP must be put in place. Therefore, just as in the Critical Cyber Asset Identification Guidelines of today, the 'inside' does not have to be routable. For example, if the entity has a digital relay and has the serial port used for console access (non-routable serial communications) attached to a serial-to-IP gateway such that the relay's command console is addressable from outside the ESP via a routable protocol (e.g. <IP Address>:<Port #> will connect you to the relay), then this meets the definition of External Routable Connectivity and an EAP is required.

One commenter provided an alternate definition that included the phrase "externally routable bi-directional communication" and added "or inbound communications to a Cyber Asset within the Electronic Security Perimeter" to the end. In response, the SDT notes that the direction of the communication is an aspect of External Routable Connectivity definition. The Electronic Access Point is an intentionally broader definition and its main function is to deny all access by default and only allow needed traffic to cross the ESP, regardless of direction.

One commenter asked that it be clarified as to whether an EAP is part of the ESP or not? In response, the SDT notes that an EAP is part of an ESP as it is the point where the routable communication from outside the ESP is allowed to cross the ESP to Cyber Assets inside the ESP.

One commenter suggested that the term "interface" be removed and have the definition reference a Cyber Asset. In response, the SDT notes that the inclusion of interface is meant to address the situation where an entity has a firewall as an EAP that has numerous interfaces to different networks and only one goes to a network that has applicable Cyber

Assets. The inclusion of 'interface' means the requirements would be concerned with only those interfaces that communicate with applicable Cyber Assets and not to interfaces that do not have any applicable Cyber Assets. The SDT also notes that the requirements in CIP-005 that apply directly to EAPs concern an interface (deny by default, methods for inspecting for malicious communications, etc).

One commenter suggested that the definition add "allows or is capable of allowing" to include dual homed Cyber Assets including laptops with wifi that is not hardware disabled. In response, the SDT believes that for a mandatory requirement the enforceable point should be binary – either communication is allowed to cross an ESP or it isn't – and the standards should avoid dealing with all possible capabilities.

One commenter asked for confirmation of the notion that Cyber Assets only communicate with other Cyber Assets. In response, the SDT notes that Cyber Asset is the basic unit of these standards and there is no lower level term. As Cyber Asset is a 'programmable electronic device', the SDT believes this covers most all situations. The SDT notes that Cyber Assets includes most all network gear as well, not just servers and workstations.

Electronic Security Perimeter

Several commenters suggested that examples should be included. In response, the SDT is not including examples in this term. Since terms such as ESP often refer to cyber technology that is constantly changing and developing, there is a tendency for examples to become outdated. The SDT used guidance instead to discuss examples rather than definitions. When the term is then used in a requirement, there is a tendency for the examples to then become prescriptive and mandatory, which is not the purpose of examples.

Multiple commenters provided some clarifying questions: Does an ESP presume the presence of EAP? Does a BES Cyber System with no External Routable Connectivity fall into scope? In response, the SDT clarifies that the ESP does not presume the presence of an EAP and BES Cyber Systems without External Routable Connectivity are in scope of the CIP standards. The ESP is a 'logical border' around a routable protocol network to which a BES Cyber System is connected. An isolated network with no external connectivity has an ESP; a logical border. The ESP is used to determine the 'Associated Protected Cyber Assets' as well as the collection of Cyber Systems and Assets that will be elevated to the impact level of the highest impact BES Cyber System/Asset in the ESP (see the definition of Protected Cyber Asset). If routable protocol communications cross the ESP, then an EAP is required.

Several commenters stated that this should be applicable to BES Cyber Asset instead of BES Cyber System. In response, the SDT notes that the BES Cyber System grouping is up to the entity and the concepts of electronic and physical security perimeters need to be taken into account. An entity is free to define every individual BES Cyber Asset as its own unique BES Cyber System and in essence make the entire standard Cyber Asset based. The grouping into systems is at the entity's discretion, but should be done with the requirements in mind.

External Routable Connectivity

Multiple commenters suggested that clarity is needed concerning the focus on Cyber Asset connectivity, rather than a 'system' with connectivity. Does a 'system' with one routable device mean all cyber assets in the system meet the applicability? This applies to the ESP definition as well. In response, the SDT has updated the definition to be at the Cyber Asset level rather than the BES Cyber System level. The intent is that Cyber Assets that have External Routable Connectivity must meet the applicable requirements and Cyber Assets that do not meet the definition are exempt from the requirement.

Several commenters suggested that the definition should include the OSI network layers. The SDT has chosen to not include Open System Interconnection (OSI) layers in the definition at this point. It is believed that with the history of the CIP standards being based on 'routable protocol' since its inception that there is a sufficient understanding of these terms at this point.

Multiple commenters suggested that the definition should be reworded to be a property of a BES Cyber Asset, not the asset itself. In response, the SDT agrees and has changed the definition to begin with "The ability to access…"

One commenter suggested that the definition should only apply if routable connection goes all the way to a BES Cyber Asset within the ESP. In response, the SDT is trying to incorporate the situation (identified in the current CCA Identification Guidelines) where an Ethernet/serial gateway is used at the perimeter. A BES Cyber Asset may have a serial connection from its console port to the Ethernet/serial gateway such that from outside the ESP the device's console port is directly addressable using a routable protocol, usually simply in the form of <ip address:port #>. The SDT's intent is for the definition to capture any device that is accessible from outside the ESP with a bi-directional routable protocol.

One commenter suggested that the definition needs to consider inside to outside connectivity not just outside in. In response, the SDT does consider 'inside out' connectivity in the requirements (e.g. outbound rules on EAP's). However, the intent with this definition is to focus on the higher level of threat that outside-in connectivity presents as well as to

give some credit for more secure network architectures that only push data out and don't allow outside-in connectivity (data diodes, etc.).

A few commenters commented that the definition should be Cyber Asset based rather than strictly limited to BES Cyber Systems. In response, the SDT has clarified that access is from a Cyber Asset that is outside of the BES Cyber System's associated Electronic Security Perimeter via a bi-directional routable protocol connection.

Protected Cyber Asset

Multiple commenters suggested that the parentheses should be removed, keeping the sentence concerning temporarily connected Cyber Assets. In response, the SDT agrees and has made the suggested change.

One commenter suggested that the temporarily connected Cyber Asset exclusion should be pulled out and made into a separate definition. In response, the SDT in this instance would be defining a term simply to use the term in the definition of another term. Therefore the SDT believes it is more straightforward to include a more complete definition in the ultimate term we are defining, and see no issue with stating what something is and what it is not while defining it.

Multiple commenters suggested that this should allow for network connection of temporarily connected Cyber Assets, suggesting that 'directly' be removed to allow connection within the ESP without requiring connection through a Cyber Asset. In response, the SDT notes that a network switch is a Cyber Asset and thus network connections are included. However, the SDT agrees that this point needs more clarity and has deleted the word 'directly' and clarified that it is a connection either to a Cyber Asset in the ESP or the network within an ESP.

One commenter suggested that a separate definition for Transient Cyber Asset should be included and have a requirement to scan for malware before connection. In response, the SDT notes that this was included in previous drafts but was removed in this draft in response to comments. Numerous comments were received pointing out the audit issues of such a requirement. How does one prove that a list of temporarily connected devices is complete? How does one prove that virus scans were done on a device that was there one minute and gone the next? How does one maintain and prove a complete inventory of all temporarily connected devices? Commenters also pointed out that the object of protection is the BES Cyber System – the goal is to protect BES Cyber Systems from all threats including temporarily connected devices. There were also numerous issues raised concerning TFE's as many troubleshooting and maintenance devices are 'programmable electronic devices' and would thus be Cyber Assets but have no antivirus available. A cable scanner used to diagnose cabling issues may be a programmable electronic device and then require a TFE. In response to

all these issues, the SDT decided to remove the requirement. However, the SDT notes that CIP-007 R3 requires an entity to deploy method(s) to deter, detect, or prevent malicious code and it is expected that such measures as scanning temporarily connected laptops and other similar devices may be included in these methods.

QUESTION D14 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, several changes have been made to clarify language in the definitions.

General Comments

Several commenters stated that the phrase "reliability tasks of the functional entity" is unclear and needs to be replaced or further defined. In response, the phrase reliability tasks of the functional entity comes from the definition of BES Cyber System and the reliability tasks are those specified in the NERC Functional Model.

Several commenters suggested that the terms compromise and disrupt need to have their own definition. In response, the words compromise and disrupt carry forward from the previously approved definition and we have not received compelling indication that these terms need further clarification.

Several commenters suggested that the phrase "was an attempt to compromise" is vague and should be deleted. In response, this phrase captures those incidents that do not necessarily succeed but should prompt investigation.

One commenter suggested replacing the phrase "reliability tasks of the functional entity" with "reliability tasks identified for functions in the NERC Functional Model." The SDT does not specify the NERC Functional Model, which is not a document subject to the standards development process, but the SDT believes that the phrase adequately conveys those tasks.

One comment was on the phrase "malicious and suspicious" is subject to interpretation and proposed adding the qualifying phrase, "as determined by the Responsible Entity." In response, the definition should not include this phrase because it is not a requirement, and CIP-008-5 already specifies the obligation for the Responsible Entity to make this determination.

One commenter suggested qualifying the term ESP and PSP with BES Cyber System to avoid having to demonstrate compliance with perimeters that do not protect BES Cyber Systems. In response, the requirement in CIP-008-5 makes this distinction in the applicability section.

One commenter suggested that the definition of Control Center uses a different term "reliability functional tasks" and requests clarification if this term means something different. In response, the SDT has clarified the language to read "reliability tasks".

One commenter suggested that the DOE OE-417 form should be considered to allow entities to comply with both requirements. In response, the SDT has reviewed the latest version of this form and do not find any reporting requirements that would conflict with those in CIP-008-5.

Cyber Security Incident

Several commenters suggested replacing the phrase "was an attempt" with "has the potential" in the definition of Cyber Security Incident because an attempt implies knowing the intent of the perpetrator and it excludes accidents which have the potential to compromise the BES Cyber System. In response, we have not significantly changed the currently approved definition and do not find the need to incorporate the proposed modifications. Both phrases communicate the desired result that an unsuccessful attack or compromise would be considered a Cyber Security Incident.

There was a suggestion that the definition of Cyber Security Incident now includes PSPs and the impact will be difficult to assess. In response, the current approved definition includes PSPs.

One commenter proposed to amend the definition of Cyber Security Incident to include: "Is a violation or imminent threat of a violation of computer security policies, acceptable use policies, or standard security practices impacting or within covered ESPs or PSPs." In response, violation of policies can be covered in an entity definition of a cyber security incident, but the Glossary definition has a focus on impact in order to broadly apply the standard.

One commenter suggested that physical security incidents should have its own definition and not be included as part of a Cyber Security Incident. In response, a physical security breach into a perimeter protecting the BES Cyber System provides enough cause for concern in the integrity of the BES Cyber System to warrant classification of a Cyber Security Incident. Individual entities may use distinct terms and response teams for these types of incidents, and the obligations in CIP-008-5 would still apply.

Several commenters proposed removing the phrase "suspicious event" from Cyber Security Incident. In response, the term suspicious event captures those incidents prompting further investigation in which the entity may not determine the cause or motive.

Reportable Cyber Security Incident

SPP RE expressed concerns that Reportable Cyber Security Incidents would not include those incidents in which redundancy mitigated the impact. In response, we have provided guidance in CIP-008-5 that Reportable Cyber Security Incidents would also include those that triggered an activation of redundant systems.

There was a proposal to replace "Any" with "A" to start the definition of Reportable Cyber Security Incident and we have done so.

One commenter proposed the following definition of Reportable Cyber Security Incident: "Any Cyber Security event that has compromised or disrupted one or more reliability tasks of a functional entity, which through investigation and escalation, has been determined by the Responsible Entity to be reportable to ES-ISAC." In response, this proposed definition includes a requirement, which should remain in the standard. The requirement in CIP-008-5 still provides leeway to the entity in determining Reportable Cyber Security Incidents.

One commenter stated that the definition needs to be coordinated with the EOP-004-2 drafting team. In response, both the CIP Version 5 and EOP-004-2 drafting teams have agreed to move all reporting obligations for Cyber Security Incidents to CIP-008-5.

One commenter proposed the definition for Reportable Cyber Security Incident in order to avoid using the term functional tasks, "A Cyber Security Incident that compromised the ESP or PSP or disrupted the operation of an applicable BES Cyber Asset or low BES Site."

One commenter proposed to add additional guidance in CIP-008-5. In response, the use of functional tasks ties the reportable incident to a specific reliability function. Without this qualification, the definition can easily be interpreted to include nominal security events as reportable. The SDT has already added additional guidance on distinguishing a Reportable Cyber Security Incident.

QUESTION D16 – IMPLEMENTATION PLAN:

If you disagree with the changes made to the Implementation Plan since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, there were not many changes made to the Implementation Plan, but the comments and comment responses below provide clarity into some of the concerns regarding the proposed effective date, the possibility of bypassing Version 4, and the initial performance of certain periodic requirements.

Proposed Effective Date

One commenter suggested that the effective date conflicts with the initial performance of requirements section and should specifically mention this in the effective date language as an exception. In response, we do not feel this is necessary. The implementation plan enumerates any exceptions to the effective date of the standard. The alternative of including all such exceptions in the effective date language would make the language unreasonably complex.

One commenter agreed with the approach to focus on the high and medium impact BES Cyber Systems but questions the need for an additional year of implementation time for low impact BES Cyber Systems particularly if no inventory is necessary. SPP RE also agrees an additional year for compliance with CIP-003-5 R2 is unnecessary. In response, the need for an additional year of implementation for low impact BES Cyber Systems exists to allow entities to formulate and implement effective security solutions for physical and electronic perimeter protection. Despite not requiring an inventory of low impact BES Cyber Systems, entities must still implement these policy changes in applicable locations where no perimeter protection currently exists.

Several commenters questioned why the effective date is so far out given that the standards have been in development for more than two years. In response, the development timeframe of the standards do not determine when entities begin planning compliance. Rather, entities have assurance in the finality of the standards upon FERC approval. The number of cyber systems applicable in this standard far exceeds any previous version of the standard. The SDT reasons it will take two budget cycles for entities to plan and implement these standards.

Bypassing Version 4

Several commented that language to extend the Version 3 effective period and bypass Version 4 should be removed because the recent FERC Order has solidified the effective date for Version 4 as April 1, 2014. Other comments request a

transitional plan to address the period of compliance between Version 4 and 5. In response, the SDT observes that the provisions to bypass Version 4 remain in the implementation plan and are subject to approval by the industry and FERC. This is explained in greater detail in the summary section at the beginning of this document.

Initial Performance of Certain Periodic Requirements

One commenter stated that for non-periodic requirements, the IP should state entities comply with all other requirements on the effective date. In response, this is already stated in the effective date language. The periodic requirements are exceptions to this language.

Several commented that CIP-010-1 requirement part 3.2 and CIP-009-5 requirement part 2.3 have a 36 month periodic performance requirement and should have an initial performance not exceeding 36 months after the effective date. Yet, although the periodicity for this requirement is 36 months, the initial performance should occur closer to the effective date of the standard. However, we are persuaded by arguments that initial exercises should be conducted prior to the operational exercise active vulnerability assessment.

Several commented that the language "…Notwithstanding any order to the contrary…" is unnecessary because the FERC can approve or remand any part of the implementation plan if it so chooses. While this is true, the inclusion of this language allows that decision to be made without the tremendous overhead of going through the standards development process.

One commenter argued that the periodic requirements section requires compliance as early as 14 days after the effective date, but the effective date allows 24 months. In response, this is true, and all of the specified periodic performance requirements occur after the effective date, which is at least 24 months.

One commenter argued the initial performance of the requirement should be performed prior to the effective date. They questioned why a year would be necessary to hold the first training or verify provisioned access. In response, the SDT disagrees with compliance prior to the effective date for two reasons. First, the effective date of the standard indicates when Version 5 becomes effective and previous versions retire. Requirements that obligate performance on a specific day cannot technically be compliant prior to the effective date. Second, the specified periodic requirements are mostly verification assessments or updates for existing security controls, and the objective is to have the security controls in place upon the effective date.

Based on comments received, CIP-009-5 requirement part 2.3 has been added to the list of periodic requirements that must be implemented no later than 12 months after the effective date.

One commenter noted that CIP-009-5 Requirement R1.4 still contains language requiring an initial performance. However, the intent of this requirement was not to obligate an initial periodic performance, and we have modified the requirement language to remove the word "initial".

Planned or Unplanned Changes

Several commenters suggested all new or reclassified Cyber Systems have the same timeframe of 12 months to achieve compliance. In response, we have updated the implementation plan based on changes to CIP-002-5 that remove obligations to update the BES Cyber System categorization within 60 days. This provides entities additional time to demonstrate full compliance for planned changes. Unplanned changes resulting in a higher categorization continue to allow the additional year to demonstrate full compliance for the affected BES Cyber Systems.

The Planned or Unplanned Changes section was collapsed into one section based on multiple comments, and it has been clarified that for *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System, with additional time to comply for requirements as specified and in the same manner as in the section *Initial Performance of Certain Periodic Requirements*. For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards, according to timelines specified in a separate table, following the identification and categorization of the affected BES Cyber System, with the additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Time Periods for Disaster Recovery

Several commenters requested clarity on what constitutes the completion of the Disaster Recovery. In response, the use of the defined term CIP Exceptional Circumstance throughout the CIP Cyber Security Standards eliminates the need to define a special case in the implementation plan for Disaster Recovery. Entities can take exceptions from the Requirements where CIP Exceptional Circumstances is specified.

One commenter suggested that the Disaster Recovery section seems to suggest not holding up restoration for compliance but entities would need to be compliant when restoration activities are complete. In response, this section

has been removed and we defer to the use of CIP Exceptional Circumstances throughout the CIP Cyber Security Standards to provide entities clarity on when and where exceptions to the Requirements can occur.

Applicability Reference Tables

One commenter requested additional clarification regarding the purpose of the applicability tables and others noted inconsistencies with the table. In response, we have corrected inconsistency errors, changed the title and provided introductory remarks. These tables are intended only for convenience. The SDT chose not to include this in a background or guidance section because requirement numbering will change in future revisions.

QUESTION D17 – DEFINITIONS AND IMPLEMENTATION PLAN:

If you have comments or specific suggestions that you have not been able to provide in response to the previous questions, please provide those comments here. Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the implementation plan was modified appropriately and certain areas were modified for clarity. Entities should refer to the individual responses to comments in the definitions questions for the SDT's response to comments for individual definitions. Many commenters provided comments on the positive direction of the posted draft. The SDT thanks these commenters and appreciates the encouraging remarks.

Several comments were toward the approach to requirements that result in a zero tolerance aspect for deficiencies in compliance monitoring. The SDT has proposed additional language that, together with a framework that also includes VSL language and RSAW audit guidance language, addresses the larger issue and shifts the focus of certain requirements to correcting deficiencies. This is explained in greater detail in the summary explanation at the beginning of this document.

Several commenters expressed their concerns on the protection of Low Impact BES Cyber Systems and the compliance demonstration of requirements that apply to them. The SDT has spent considerable time and effort to work with stakeholders on addressing this issue and believes that the approach in the new proposed draft addresses the concerns.

Multiple commenters reiterated concerns on the broad application of CIP V5 irrespective of connectivity. The SDT has included consideration of connectivity in the applicability of requirements and believes that this approach appropriately addresses applicability differences due to connectivity type. The SDT reiterates its posture that, while connectivity is an important vector for cyber security threats, it is not the only one and that the CIP standards encompass a holistic approach to the protection of BES Cyber Systems.

There were multiple comments that suggested the phrase "but not limited to…" may be construed as required evidence. The SDT agrees with the comment and is using the standard language "Example(s) of evidence may include, but is not limited to…" to convey two concepts in the measure: the evidence in the measure are not required evidence but represents examples of quality evidence, and entities may present other evidence that may be presented in lieu of the ones described or in addition to them.

Multiple comments were based on the definition of periodic requirements, with another commenter citing the CAN on Annual that has been published. The SDT notes that CANs provide guidance for auditors, are not interpretations of standard requirements and are not the basis for changes to requirements. The SDT has considered all outstanding CANs as additional input to the development of these standards, and where the CANs result from unclear requirement language, the SDT has drafted language with a goal of eliminating the need of a CAN for auditing purposes. Since the word annual is not used in the V5 CIP standards, the term does not apply. The SDT has drafted language that reflects its intent while providing adequate flexibility to minimize zero defect effects.

Several commenters requested a global clarification similar to section 5 of CIP-003 that explains the significance of the use of bulleted and numbered items. Another comment was on the bullets in section 4, part 4.2.2. The SDT will insert a paragraph in the background section to include such explanations.

There were several comments on the use of a single VRF for each requirement, irrespective of whether it applies to High Impact or Medium Impact. Another comment was on the VSLs and the differentiation required to handle zero defect. VRFs are used as one of many input variables used to determine the sanction in the case of a violation of a standard. The current sanction table used for calculating regulatory sanctions is based on VRFs at a requirement level. However, there are many other considerations in the determination of a sanction for a specific violation. Until the current development of the evolving enforcement model is better defined, it is premature to effect changes to the VRF. Regarding VSLs, the SDT notes that VSLs are used after the fact, i.e. when a violation has already occurred. The SDT believes that VRFs, VSLs and RSAWs, together with appropriate requirement language, must together provide a complete framework to address the zero defect issue. The ballot for VRFs and VSLs is a non-binding ballot, and there is likely to be changes to accommodate evolving concepts in handling zero defect compliance and risk based compliance assessments.

Several comments were on the compliance section on records retention and retention requirements in standards requirements. Retention requirements, when specified in requirements, are requirements for technical reasons, such as event log retention for forensic purposes. The retention periods specified in the compliance section are meant to apply to records required for demonstrating compliance. For example, if 90 day event log retention is specifically required in a requirement, the Responsible Entity is expected to retain records that demonstrate that it has kept 90 days of logged events for the 3 years, not that it has kept 3 years' worth of these event logs. Under the compliance section, these could be log entries of the process that maintains a minimum of 90 days of log events.

Several commenters suggested that all sub-requirement parts should state the goal. The SDT generally provides the goal either in the body of the main text for the requirement, or in the rationale box. The SDT believes that the goal of each subpart is mostly self-evident given the overall requirement objective, and that addition of a goal for each subpart would be redundant and unnecessary in most cases.

There were several comments surrounding the need for a definition of Control Centers. The SDT directs entities to its summary response to Question D9 on this issue.

There were several comments on the removal of restoration resources from Medium Impact criteria, and cited the need to provide adequate justification. It is not clear to the SDT whether these comments were in support of this change. However, as a matter of normal SDT stakeholder input consideration, extensive debate on this issue was conducted in the NERC operating and planning technical committees, without a clear resolution. As a matter of procedure, the SDT must provide justification for changes from one release to another and has received stakeholder comments supporting this change.

There were multiple suggestions that a summary of the CIP Version 5 standards and the interaction between the requirements and their applicability be provided by the SDT. The SDT is focused on addressing technical issues from comments on requirements and on the standards themselves. The SDT appreciates any input provided by stakeholders, and it plans to facilitate distribution of an informational summary addressing this concern that was prepared by certain stakeholders that have been collaborating with the SDT. However, the formal posting with the standards would require other types of SDT, NERC and other stakeholder groups' review and/or approval and is not an appropriate venue for making compliance management tools available to stakeholders.

There were several comments on the issue of physical access controls for High Impact, specifically on whether two different access control systems are required. The SDT has provided guidance on this issue in the guidelines and technical basis section of CIP-006 that indicate that the intent of the requirements is not to require different control systems.

Numerous commenters expressed concern with the term "Associated Protected Cyber Assets". In considering these comments, the SDT noted that the concept of high water marking for Impact Level within an ESP was not very clear. The SDT has defined a term Protected Cyber Assets to incorporate the concept of BES Cyber Systems, their associated Cyber Assets within the same ESP and the concept of High Water Marking for Impact level within an ESP.

There were several comments that a definition for dial-up connectivity is needed. The SDT has included a definition for "Dial-up Connectivity" in this draft proposal.

There were comments on the use of "Associated…" in the applicability column of requirement tables. The SDT has made some changes to the language used to clarify the applicability and has also used the defined term Protected Cyber Assets to further clarify applicability.

There were comments relating to a number of editorial and stylistic issues related to table headers, capitalization and inconsistencies of terms. The SDT has considered these comments and made the appropriate changes.

One commenter recommended that the exemptions section in the applicability section should be specific to the standard, and not say CIP-002-5 in standards other than CIP-002. The SDT agrees and has made the appropriate changes in the standards.

One commenter suggested that the application guidelines should be allowed to change from standard to standard and that glossary terms should not be defined again in the standard. The SDT disagrees that application guidelines should be the same for all standards, but does agree that there should not be any incompatibility or inconsistency between the guidelines and the standards. The SDT also agrees that there should not be any definitions repeated in a standard when they are proposed glossary terms. The SDT will ensure consistency between guidelines and standard requirements. The SDT notes that the notes on glossary terms in the guidelines or background section are intended to provide additional explanantion of the terms and not be replacement definitions for the proposed terms for the NERC glossary. The requirements in the standard are the ultimate source of authoritative text for compliance.

One commenter suggested that the requirements that should be subject to CIP Exceptional Circumstances should be extended to most requirements except those in CIP-002, CIP-003 and CIP-004, and provided a list of requirements that should be subject to CIP Exceptional Circumstances. The SDT has carefully selected requirements that it believes are appropriately suitable for a CIP Exceptional Circumstance in order to facilitate the handling of emergency situations and timely electronic and physical access for first responders. With regard to a comment on ensuring that CIP Exceptional Circumstance would not require a TFE, the SDT has no jurisdiction over Rules of Procedure and cannot predict what regulators will deem to be TFE triggering language in the future. It is not the SDT's intent that CIP Exceptional Circumstances be TFE triggering language, but rather, that the Responsible Entity has carefully defined its policies and

procedures for declaring and ending CIP Exceptional Circumstances as required in CIP-003, and that any specific CIP Exceptional Circumstance be documented as required to demonstrate compliance to the specific CIP requirement.

One commenter suggested that it should be clear that no policies or procedures are required for CIP-004 to CIP-011 Responsible Entities that do not have High or Medium Impact BES Cyber Systems. There is no requirement in CIP-004 through CIP-011 that is applicable to Low Impact BES Cyber Systems. This is clear in the applicability column of the requirements tables.

There was a comment on the incorporation of guidelines and technical basis in the standards, citing stakeholders' time constraints in reviewing guidelines during the comment period. The SDT has spent considerable time drafting guidelines and providing the technical basis for requirements as part of the structure of results based standards. The SDT believes that the guidelines and technical basis provides valuable information to stakeholders during the comment and balloting process. It provides valuable input to stakeholders on the intent of the SDT, both during the development and the implementation phases of the standards. This approach has received overwhelmingly positive feedback from stakeholders. While the SDT understands that these guidelines and technical basis are not intended to be used instead of, or in addition to requirements, the SDT believes they provide valuable context to the standards' requirements.

There was one comment on the use of attestations as measures, citing industry confusion on the appropriate use of attestations. The absence of "attestations" in the measures does not imply that attestations are not appropriate measures of compliance, but that the SDT chose to use more specific examples of evidence for these requirements. Whether attestations are appropriate measures of compliance depends on the requirement. The SDT has used attestations where it may more likely be the measure that can be produced as evidence of compliance, with no implication that it is the only way of demonstrating compliance.

One commenter suggested that part 4.2.3 of the applicability section (Section 4) may inadvertently create an exemption for Control Centers. While certain Functional Entities may not own BES Facilities as described in the NERC Glossary, they perform reliability functions as the Functional Entity listed in 4.1 for BES Facilities. The introductory paragraph of 4.2 specifically refers to "…Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above …"

One commenter requested clarification or a definition of "Adverse Reliability Impact": this term is defined in the NERC Glossary of Terms.

One commenter requested a formal definition for “Common Control System”: the SDT believes that the term control system is a widely understood term of art used in electric reliability operation and engineering and that it does not require specific definition in these standards.

One comment suggested that the standards use data and information interchangeably. The SDT notes that it has used data when referring to a set of values (numeric or otherwise) in its raw form, and to information when referring to data processed for a specific use.

One commenter noted that the CIP standards should be aligned more closely to the NIST or ISO standards. The SDT uses many frameworks (including the ones cited) as sources for the development of requirements. The SDT notes that both of the cited standards are general purpose cyber security standards and guidelines not intended for any specific industry use. The SDT believes that the mandatory nature for standards specifically for the BES poses unique challenges and requires an appropriately developed approach.

There was one comment that was extensively on the scope of applicability to asset owners and operators only, and the absence of compliance for suppliers and other third party providers. The SDT notes that these mandatory standards are developed under the jurisdiction of the ERO and that they can only be applied to NERC Registered Entities.

One comment was on the awareness and training requirement in CIP-004 R2 and role based awareness training. The comment was specific that the items in the table in R2 referred to systems while the requirement cited role based training. Table R2 contains the requirements for the required content of the training program, but the level at which the training is provided in each item is based on the role of the individual taking the training.

One comment was extensively on the 99.9% availability specification in CIP-006. The SDT has redrafted the requirement and the 99.9% specification has been removed.

There was one comment on the effect of the application of the CIP standards on small entities. The SDT notes that BES Cyber Systems are categorized based on reliability impact rather than on entity size. The SDT has developed the requirements to be commensurate with the level of impact on the BES. The SDT has not included entity size as an input to the applicability of requirements.

One comment was extensively on section 4.2.2. The SDT notes that section 4.2.2 is not intended to specify the impact criteria, but the scope. Consequently, many of the terms used are extracted from the registration criteria for DPs. Many of the comments presented have been incorporated in the proposed new draft, while a few are appropriate as part of the criteria.

One commenter made many remarks on global sections used in all standards. These will be reviewed by NERC standard staff as standard templates applicable to NERC standards.

There was a comment on the use of "where technically feasible" and the commenter suggested the use of language that would specify compensating controls. The SDT notes that there were requirements in CIP Versions 1-4 that had alternative language to allow compensating controls, but that the language was added to TFE triggers.

One commenter requested a definition of "Associated Data Centers". Please refer to the summary response on this issue to comments on D9.

One commenter was concerned with the periodic requirements, specifically on the 15 month period for periodic requirements intended to be performed annually. The commenters suggested alternative language that would ensure strict compliance with a 12 month period. The intent of the SDT in specifying a 15 month period for annual requirements is to provide some flexibility to entities in the framework of attenuating zero defect requirements. The comments imply that Responsible Entities would aim for strict minimum compliance at the cost of increased non-compliance risk. From the practical implementation standpoint, the SDT understands that most Responsible Entities will implement a process that would ensure the performance in a period less than 15 months (an annual period is easier to track from the compliance management standpoint) for assured compliance.

One comment was raised on the SDT's discussion of redundancy as not being a mitigation for cyber security vulnerabilities and stated that redundancy provide mitigation for some cyber security vulnerabilities. While redundancy provides some mitigation for recovery requirements, the SDT has not found a compelling case where strict redundancy of using an exactly mirrored system configuration would provide mitigation of a cyber security vulnerability. It is the SDT's opinion that such configurations have the unintended effect, from the cyber security (not operational) standpoint, of increasing the attack surface. The SDT does agree that configurations that provide redundancy of function rather than system redundancy can provide mitigation if implemented with systems dissimilar enough to provide mitigation of certain system specific cyber security vulnerabilities.

One comment was on the term Facility and its relation to systems, also stating that the term element is undefined. The SDT has used the term Facility in its defined meaning in the NERC Glossary when used in its capitalized form. The term Facility is used to refer to groups physical BES Elements. The NERC Glossary has a definition of Element used in the context of the BES. In cases where the SDT intends a broader scope to include systems, the SDT has used "Facilities, systems and equipment".

There was a comment on the exemption from the standards of cyber assets between discrete ESPs. In particular, the commenter suggested requirements to implement end-to-end encryption. The commenter seems to suggest that such encryption should be required for routable and non-routable protocols. In addition, the commenters suggest that EAPs should be subject to cyber security requirements. The SDT has not required specific technologies to protect information between ESPs, but has focused instead on the cyber security objectives of access control and monitoring of traffic across EAPs. The comments do not seem to take into account communication between ESPs of real-time, latency sensitive applications common in control systems. The authenticity and integrity of application data or information is not always implemented using communication encryption technology, but may be implemented at other layers of the overall stack without the latency overhead of encryption. The commenters also seem to interchangeably use EAPs and the cyber assets that implement the EAP. The CIP definition of an EAP is an interface. There are however requirements, including security event monitoring requirements, that are applicable to the Cyber Assets that perform access control and monitoring functions, including those that implement an EAP, for electronic and physical access.

A commenter suggested that BES information protection requirements should apply to third parties. The SDT agrees and expects the Responsible Entity to comply with requirements for protecting and handling BES protected information, whether such information is accessed or handled by its own employees and third parties. The requirements in CIP-011 require the Responsible Entity to implement processes to ensure such access control and handling.

One commenter provided its fundamental objection to Version 5 and suggested that implementation of the current CIP standards should be allowed to mature. The SDT is required to address all the FERC directives from Order 706, and FERC Order 706 has directed the ERO to complete consideration of Order 706 directives by March 31st, 2013.

One commenter suggested that the statement in the implementation plan that starts with "Not withstanding any order to the contrary…" should be amended in light of Order 706. The SDT believes that the window for the application of the statement is still possible given the deadline in Order 761.

One commenter inquired on when a cyber system would have to come into compliance as a result of an emergency. One commenter also inquired on how to treat temporary elevation. If the cyber system is re-categorized or is a new cyber system as a result of that emergency or unplanned change, the implementation table specifies 12 months.

There was a comment on missing requirements in item 5 of the Implementation Plan. The SDT has included these requirements.

One commenter pointed out that the background section dealing with reliable operation of the BES contains an unclear reference to the Functional Model. The SDT has added qualifications that clarify that both reliability tasks defined in the Functional Model and the functional entity's relationships with other functional entities are considered.

One commenter suggested that there are requirements where the text of the requirement specifies BES Cyber Systems when the applicability column specifies more than BES Cyber Systems. The SDT has reviewed the language of the requirements where this occurs to ensure consistency with the applicability column. In cases where more than BES Cyber Systems apply, the SDT generally uses "applicable Cyber Assets."

One commenter expressed the need for the concept of escorted electronic access for remote support using technologies such as WebEx. The fundamental concept in escorted access is not only that of continuous visibility on the actions of the escorted individual, but also the capability of timely intervention in the case of inappropriate action. The SDT believes that total support for this concept is not possible in an electronic access scenario.

One commenter stated that in its opinion, the functional entity Interchange Coordinator (IC) does not have any asset that would be included, and should therefore not be included in the applicability section. The SDT reviewed the reliability tasks for the IC function as well as the responsibilities of the IC Functional Entity in its relationship with other functional entities in the Functional Model and noted real-time responsibilities in the latter in relation to BAs and RCs.

Questions with Votes Only:

1. Do you agree with the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Madison Gas and Electric Company	No
MRO NSRF	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
FirstEnergy	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No

Organization	Yes or No
ACES Power Marketing	No
SPP and Member companies	No
Comment Development SME List	No
Dairyland Power Cooperative	No
CenterPoint Energy	No
Hydro One	No
Ingleside Cogeneration LP	No
NIPSCO	No
Trans Bay Cable	No
Consumers Energy Company	No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	No
American Transmission Company, LLC	No
Ameren	No
NextEra Energy, Inc.	No
Liberty Electric Power LLC	No
ISO New England Inc.	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No
Alliant Energy	No
New York Power Authority	No
Exelon Corporation and its affiliates	No
Wiscsonsin Electric Power Company	No
Farmington Electric Utility System	No
City Utilities of Springfield, MO	No
NYISO	No

Organization	Yes or No
Deseret Power	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
US Bureau of Reclamation	No
California Independent System Operator	No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
NCEMC	Yes
IRC Standards Review Committee	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes

Organization	Yes or No
Southern California Edison	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Xcel Energy	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Tennessee Valley Authority	Yes
PSEG	Yes
Texas Reliability Entity	Yes
PJM Interconnection	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes

2. Do you agree with the proposed definition of Control Center?

Organization	Yes or No
NRG Energy Companies	No
PNGC Comment Group	No
Madison Gas and Electric Company	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
NCEMC	No
ACES Power Marketing	No
IRC Standards Review Committee	No
National Rural Electric Cooperative Association (NRECA)	No
Southern California Edison	No

Organization	Yes or No
CenterPoint Energy	No
Manitoba Hydro	No
Xcel Energy	No
Snohomish County PUD	No
Lakeland Electric	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
NV Energy	No
NextEra Energy, Inc.	No
PSEG	No
Texas Reliability Entity	No
Liberty Electric Power LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No

Organization	Yes or No
POrtland General Electric	No
Exelon Corporation and its affiliates	No
Farmington Electric Utility System	No
Indiana Municipal Power Agency	No
Deseret Power	No
Central Lincoln	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
Northeast Power Coordinating Council	Yes
Southwest Power Pool Regional Entity	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes

Organization	Yes or No
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
SPP and Member companies	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Progress Energy	Yes
Western Area Power Administration	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
NIPSCO	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes

Organization	Yes or No
United Illuminating company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
ISO New England Inc.	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
Nebraska Public Power District	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
American Public Power Association	Yes

Organization	Yes or No
Springfield Utility Board	Yes
New York Power Authority	Yes
Wiscsonsin Electric Power Company	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Cowlitz County PUD	Yes
US Bureau of Reclamation	Yes

3. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager?

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Madison Gas and Electric Company	No
MRO NSRF	No
Dominion	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
NCEMC	No
ACES Power Marketing	No
Southern Company Services, Inc.	No
National Rural Electric	No

Organization	Yes or No
Cooperative Association (NRECA)	
Dairyland Power Cooperative	No
Tri-State G&T - Transmission	No
CenterPoint Energy	No
Manitoba Hydro	No
Xcel Energy	No
Bonneville Power Administration	No
MidAmerican Energy Company	No
Ameren	No
NextEra Energy, Inc.	No
Liberty Electric Power LLC	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No
Alliant Energy	No

Organization	Yes or No
Exelon Corporation and its affiliates	No
Deseret Power	No
Brazos Electric Power Cooperative	No
California Independent System Operator	No
Northeast Power Coordinating Council	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
SPP and Member companies	Yes

Organization	Yes or No
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Southern California Edison	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
NIPSCO	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes

Organization	Yes or No
Trans Bay Cable	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Illinois Municipal Electric Agency	Yes
NV Energy	Yes

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
PSEG	Yes
Texas Reliability Entity	Yes
PJM Interconnection	Yes
ISO New England Inc.	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
New York Power Authority	Yes
Wiscsonsin Electric Power Company	Yes

Organization	Yes or No
Farmington Electric Utility System	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

4. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager?

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Madison Gas and Electric Company	No
MRO NSRF	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
CenterPoint Energy	No
Trans Bay Cable	No
Manitoba Hydro	No

Organization	Yes or No
Snohomish County PUD	No
Lakeland Electric	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Ameren	No
NextEra Energy, Inc.	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No
Alliant Energy	No
Exelon Corporation and its affiliates	No
California Independent System Operator	No
Northeast Power Coordinating Council	Yes
NRG Energy Companies	Yes

Organization	Yes or No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Salt River Project	Yes
Southern California Edison	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
NIPSCO	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes

Organization	Yes or No
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Tampa Electric Company	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes

Organization	Yes or No
ISO New England Inc.	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
New York Power Authority	Yes
Wiscsonsin Electric Power Company	Yes
Farmington Electric Utility System	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes

Organization	Yes or No
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

5. Do you agree with the proposed definitions of Electronic Access Control or Monitoring Systems, Interactive Remote Access, and Intermediate Device?

Organization	Yes or No
Salt River Project	No
Trans Bay Cable	No
United Illuminating company	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Texas RE NERC Standards Review Subcommittee	No
Dairyland Power Cooperative	No
Lakeland Electric	No
Illinois Municipal Electric Agency	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Madison Gas and Electric Company	No

Organization	Yes or No
MRO NSRF	No
Duke Energy	No
Florida Municipal Power Agency	No
ACES Power Marketing	No
IRC Standards Review Committee	No
Comment Development SME List	No
CenterPoint Energy	No
NIPSCO	No
Bonneville Power Administration	No
MidAmerican Energy Company	No
Ameren	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No

Organization	Yes or No
Alliant Energy	No
Exelon Corporation and its affiliates	No
Wiscsonsin Electric Power Company	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
Southern California Edison	Yes
ATCO Electric	Yes
Northeast Power Coordinating Council	Yes
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
PPL Corporation NERC	Yes

Organization	Yes or No
Registered Affiliates	
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
NCEMC	Yes
SPP and Member companies	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes

Organization	Yes or No
Ingleside Cogeneration LP	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Tampa Electric Company	Yes
NV Energy	Yes

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
ISO New England Inc.	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
New York Power Authority	Yes
Farmington Electric Utility System	Yes

Organization	Yes or No
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
US Bureau of Reclamation	Yes
Luminant	
American Transmission Company, LLC	

6. Do you agree with the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Madison Gas and Electric Company	No
MRO NSRF	No
FirstEnergy	No
Duke Energy	No
Florida Municipal Power Agency	No
SPP and Member companies	No
IRC Standards Review Committee	No

Organization	Yes or No
Southern California Edison	No
Dairyland Power Cooperative	No
Hydro One	No
NIPSCO	No
Hydro-QuÃ©bec Production	No
Turlock Irrigation District	No
Bonneville Power Administration	No
Lakeland Electric	No
Illinois Municipal Electric Agency	No
NV Energy	No
NextEra Energy, Inc.	No
ISO New England Inc.	No
Nebraska Public Power District	No
Alliant Energy	No
New York Power Authority	No

Organization	Yes or No
Exelon Corporation and its affiliates	No
Wiscsonsin Electric Power Company	No
City Utilities of Springfield, MO	No
NYISO	No
California Independent System Operator	No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Texas RE NERC Standards Review Subcommittee	Yes

Organization	Yes or No
NCEMC	Yes
ACES Power Marketing	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
CenterPoint Energy	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
Independent Electricity System Operator	Yes

Organization	Yes or No
Trans Bay Cable	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Xcel Energy	Yes
Snohomish County PUD	Yes
Tampa Electric Company	Yes
MidAmerican Energy Company	Yes
Massachusetts Municipal	Yes

Organization	Yes or No
Wholesale Electric Company	
Tennessee Valley Authority	Yes
Ameren	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
City of Austin dba Austin Energy	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
Farmington Electric Utility	Yes

Organization	Yes or No
System	
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

7. Do you agree with the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Madison Gas and Electric Company	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
Duke Energy	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
Progress Energy	No

Organization	Yes or No
CenterPoint Energy	No
Hydro One	No
NIPSCO	No
Lower Colorado River Authority	No
LCRA Transmission Services Corporation	No
Xcel Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
NextEra Energy, Inc.	No
ISO New England Inc.	No

Organization	Yes or No
City of Austin dba Austin Energy	No
Utility Services Inc.	No
New York Power Authority	No
Farmington Electric Utility System	No
City Utilities of Springfield, MO	No
NYISO	No
California Independent System Operator	No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes
Dominion	Yes
FirstEnergy	Yes
NCEMC	Yes

Organization	Yes or No
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Southern California Edison	Yes
Dairyland Power Cooperative	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes

Organization	Yes or No
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes

Organization	Yes or No
Ameren	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Nebraska Public Power District	Yes
Alliant Energy	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
Wiscsonsin Electric Power Company	Yes

Organization	Yes or No
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

15. Do you agree with the changes made to the proposed implementation plan since the last formal comment period?

Organization	Yes or No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
Southern California Edison	No
Dairyland Power Cooperative	No
Hydro One	No
Trans Bay Cable	No
Turlock Irrigation District	No
NextEra Energy, Inc.	No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
MRO NSRF	No
NESCOR/NESCO	No
Duke Energy	No

Organization	Yes or No
Southern Company Services, Inc.	No
CenterPoint Energy	No
Consumers Energy Company	No
Manitoba Hydro	No
Snohomish County PUD	No
MidAmerican Energy Company	No
ISO New England Inc.	No
Nebraska Public Power District	No
Alliant Energy	No
New York Power Authority	No
Exelon Corporation and its affiliates	No
NYISO	No
Kansas City Power & Light	No
Texas RE NERC Standards Review Subcommittee	Yes

Organization	Yes or No
United Illuminating company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Brazos Electric Power Cooperative	Yes
Utility Services Inc.	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes

Organization	Yes or No
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes

Organization	Yes or No
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes
Bonneville Power Administration	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Illinois Municipal Electric Agency	Yes
NV Energy	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
PSEG	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
City of Austin dba Austin Energy	Yes

Organization	Yes or No
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
American Public Power Association	Yes
Wiscsonsin Electric Power Company	Yes
Farmington Electric Utility System	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
California Independent System Operator	Yes

Organization	Yes or No
Madison Gas and Electric Company	
Luminant	
American Transmission Company, LLC	

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments Cyber Security Order 706 Version 5 CIP Standards

Comment Form
Combined Question 1 and Question 2 Summaries
October 26, 2012

The Project 2008-06 Drafting Team thanks all commenters who submitted comments on the Version 5 of the CIP Cyber Security Standards and its Implementation Plan for consideration by the SDT in finalizing Version 5 and related documents. The 10 standards were posted for a 30-day formal comment period from September 11, 2012 through October 10, 2012 and successive ballots through October 10, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 112 sets of comments, including comments from approximately 258 different people from approximately 153 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Table of Contents

Introduction 7
"Identifies, Assesses, and Corrects Deficiencies" Comments 8
Section 4 - Applicability 10
Draft Reliability Standard Audit Worksheet 13
"Annual" and Other Time Parameters 13
Authorized Access List and Specific Rights Reviews in Multiple Standards 14
Data Retention Requirements 15
CIP-002-5 16
Requirement R1 18
Requirement R2 20
Attachment 1 20
Criterion 1.2 21
Criterion 1.4 22
Criterion 2.1 22
Criterion 2.3 23
Criterion 2.4 24
Criterion 2.5 25
Criterion 2.6 27
Criterion 2.8 27
Criterion 2.9 27
Criterion 2.10 27
Criterion 2.11 28

Criterion 2.12 28
Criterion 2.13 31
Criterion 3.1 31
Criterion 3.4 31
CIP-003-5 32
CIP Senior Manager 32
Policy Requirements 32
Requirement R2 33
Requirement R4 33
CIP-004-5 35
General 35
Requirement R1 35
Requirement R2 36
Requirement R3 37
Requirement R4 38
Requirement R5 40
CIP-005-5 43
High Water Marking 43
Background Section 43
Consideration of Data Diodes 44
Requirement R1 44
Requirement R1 VSLs 48
Requirement R2 48
CIP-006-5 52

General 52
Background Section 52
Requirement R1 52
Requirement R2 55
Requirement R3 56
Guidelines and Technical Basis 56
CIP-007-5 57
General Comments 57
Effective Dates 57
Requirement R1 57
Requirement R2 58
Requirement R3 62
Requirement R4 64
Requirement R5 68
CIP-008-5 71
General 71
Requirement R1 71
Requirement R2 72
Requirement R3 73
CIP-009-5 75
Requirement R1 75
Requirement R2 76
Requirement R3 77
Guidelines and Technical Basis 78

CIP-010-1 79
Timeframes for Configuration Control Activities 79
Cross References to CIP-005-5 and CIP-007-5 on Impacted Controls 79
Requirement R1 79
Requirement R2 80
Requirement R3 80
CIP-011-1 82
Requirement R1 82
Requirement R2 82
Implementation Plan 83
Effective Date 83
Initial Performance of Certain Periodic Requirements 85
Previous Identity Verification 86
Planned or Unplanned Changes Resulting in a Higher Categorization 86
Applicability Reference Tables 87
Definitions 88
BES Cyber Asset 88
BES Cyber System 88
BES Cyber System Information Responses 88
CIP Exceptional Circumstance Responses 88
CIP Senior Manager Responses 88
Control Center 89
Cyber Asset 89
Cyber Security Incident 90

Electronic Access Control and Monitoring System 91
Intermediate Device (now “Intermediate System”) 91
Interactive Remote Access 92
Reportable Cyber Security Incident 93

Introduction

The Standard Drafting Team (SDT) thanks all commenters for their continued focus on providing constructive and useful feedback for improving and refining the standards. In response to draft 3 of the Version 5 CIP Cyber Security Standards, the SDT received input that was focused on several issues that assisted the SDT in refining the standards to the final set of standards now posted for recirculation ballot. The SDT carefully considered all comments in determining whether to make particular changes to the standards.

In response to comments provided to draft 3, the drafting team greatly appreciates those entities that focused their comments on the issues most critical to them, as it facilitated a qualitative representative assessment of the areas requiring the greatest review. The focus on those major concerns that were essential as a condition to find consensus was greatly appreciated.

Furthermore, the SDT wishes to thank the industry for their significant engagement and support in developing these standards. Industry participants and observers, whether formally or informally, and whether in person or through other means, provided important perspectives and subject matter expertise that facilitated the SDT's consideration of the complicated issues and technical matters reflected in these standards. This truly was a collaborative process with participation from virtually every facet of our diverse and committed industry. Security and reliability were reflected in each consideration, and the extensive and consistent industry participation throughout the process is reflected in high approvals in response to the successive ballot from draft 3 that ended October 10, 2012.

At this stage, the drafting team has reached a point where it has made a good faith effort at resolving applicable objections, and it has not made any substantive changes since posting draft 3. Therefore, the team is posting the standards, related definitions and implementation plan for a recirculation ballot. As in past drafts of the Version 5 CIP Cyber Security Standards, the SDT thoroughly considered proposed changes and evaluated them carefully by considering several important variables, such as, but not limited to, whether such changes were in the interest of cyber security and reliability, whether they would improve or reduce consensus, whether they had unintended consequences for other types of entities, and whether they were in support of the SDT's obligation to respond to regulatory directives, most notably from FERC Order No. 706. The SDT has done its best to be responsive to all inputs, recognizing that it is not possible to adopt every suggestion and also recognizing the considerable diversity of entities and assets to which the standards will apply.

In the accompanying comment form for draft 3, the drafting team asked the following two questions:

1. If, after reviewing the posted standards and General Summary of Consideration of Comments, you do not support one or more of the 10 standards, the implementation plan or set of definitions, please indicate the specific item you do not support (the standard and Requirement number, specific defined term, or implementation plan) and the specific reason you cannot support it here.
2. If you have a brief comment you would like to provide that has not already been provided among the previously submitted feedback in response to draft 1 and draft 2, please provide it here. Please limit your comment to 200 words or less.

In reviewing comments, the SDT determined that some common issues were presented by different entities in response to either Question 1 or Question 2, depending on how the particular entity organized its comments. As a whole, the SDT found that the responses were thoughtful, organized, and focused. In this summary, the SDT is responding to all comments from industry that were submitted in response to both Question 1 and Question 2 in one consolidated summary form rather than providing a separate summary for each of Question 1 and Question 2. Since most issues and comments were not isolated in response to one question or the other, this single summary provides the most efficient and thorough method with which to provide the SDT's response.

Commenters addressed a wide variety of topics in their comments, but the most commented upon subjects include comments on the Transmission Operator (TOP) Control Center Criterion in CIP-002-5's Attachment 1 and comments regarding the SDT's use of the "in a manner that identifies, assesses, and corrects deficiencies" language. The TOP topic is discussed in detail under the CIP-002-5 portion of this summary, and the "identifies, assesses, and corrects deficiencies" topic is addressed immediately below as part of this summary's general discussion. Other topics are discussed relative to their particular standard or definition, and the associated table of contents for this document lists most topics of discussion.

"Identifies, Assesses, and Corrects Deficiencies" Comments

As noted in the background sections of the standards, and in response to comments from draft 2, the SDT has incorporated within CIP Version 5 a recognition that certain Requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain Requirements. The intent is to change the basis of a violation in those Requirements so that they are not focused on *whether* there is a

deficiency, but on identifying, assessing, and correcting deficiencies. Note that, where used, the addition of language modifies "implement"; it does not itself require or specify internal controls, though it certainly enables their use for those entities that have adopted an internal controls or compliance management approach. For purposes of this summary, the "identifies, assesses, and corrects deficiencies" phrase is sometimes referenced as simply "IAC."

This topic was a source of several comments on draft 3, and the SDT appreciates the comments, feedback, and the spectrum of concern or support on this issue. The SDT believes that Version 5 is the right time to take a step in a direction that promotes security and reliability by incorporating a self-correcting aspect in certain Requirements. This is a new step, but it is informed, collectively, by implementation and audit experience from Versions 1 through 3 of the CIP Cyber Security Standards.

Many commenters support the SDT's addition of a self-correcting aspect and applaud the overall shift in the emphasis of compliance from perfection to the identification, assessment, and correction of deficiencies. The commenters support the shift from zero tolerance for deficiencies to encouraging finding and correcting deficiencies. The SDT considers such self-correction as an essential component to improved reliability and security, and it thanks commenters for their support. Though there were several specific suggestions or concerns, as noted below, the consensus position of the industry is one of support for the approach, as reflected in both comments and the overwhelming approval of the standards that use the approach.

While this is a new direction, the SDT believes there is tremendous benefit in eliminating the zero-defect language in the standards, and it is therefore worthwhile of inclusion in the CIP standards. However, the SDT acknowledges this is a developing concept and encourages the industry to continue to work alongside NERC in implementing the compliance monitoring strategy for the language.

Some commenters presented concern that there is no clear mechanism with how this approach will be audited or that there may be inconsistent audits across Regions. The SDT is well aware of this concern, and it is encouraged by ongoing coordination and support among both NERC and several regions. The SDT expects that NERC will continue to develop tools such as the Reliability Standard Audit Worksheets (RSAWs) in a manner that involves the industry and the members of the SDT. Importantly, the language to "identify, assess, and correct deficiencies" modifies "implement" where used, and it is meant simply to express that implementation of the Requirement is not in a "zero defect" manner.

Commenters also questioned whether this approach indeed does require internal controls. The SDT notes that the compliance initiatives that relate to internal controls are not the same as the approach in the standard. The SDT contemplates that the "identify, assess, and correct deficiencies" language is appropriate regardless of how compliance may be monitored, while noting that the standards approach is also supportive of the compliance approach where and if used. At its core, the SDT intends in using the language to signal an important transition to self-correction as part of the expected performance of a Requirement itself as opposed to a mere deficiency constituting the basis for violation.

Some commenters also proposed alternative, additional, or supporting language to augment the "identify, assess, and correct deficiencies" language in the Requirements or other supporting components of the standards, or proposed addition of the language to other requirements. The SDT has previously considered such alternative language and evaluated carefully where the language should be used, and, upon reexamining those proposals in response to comments, the SDT continues to support those concepts in the compliance monitoring approach and documents rather than in the standards themselves. Language noting that certain actions are not violations is too prescriptive for either the Requirements or the measures, and they do not comport with the style and form of the standards. With continuing input, coordination, and education, the SDT is confident that the Requirement language as presented is the appropriate mechanism to empower the industry to focus on correcting deficiencies as part of the expected performance of the Requirements while not requiring or prescribing a particular assessment of the how the entity accomplishes it.

Additionally, in response to perspectives expressed by commenters on the "identify, assess, and correct" deficiencies language, the SDT shares the view that NERC must ensure going forward that the compliance monitoring approach is consistent. The SDT believes that most of the industry is ready to transition to a new approach and that this reflects the consensus position. The SDT and the industry have an opportunity to incorporate significant improvements and lessons learned from implementation and audit of previous versions, and the SDT is encouraged by not only industry support, but also from NERC's direction in continuing to work with the industry in implementation of risk-based initiatives. The SDT will remain engaged after approval of the standards to work with NERC to provide input into the RSAW development process.

Section 4 - Applicability

There were many comments that "group of Elements" from the standards' applicability section, parts 4.1.2.4 and 4.2.1.4 should be deleted on the bases that it is redundant with Cranking Path and would create ambiguity, citing that these and initial switching Requirements are included in the Cranking Path. The SDT considered the language that is included in Requirement R1.5 of EOP-005-2, which says: "Identification of Cranking Paths and initial switching Requirements

between each Blackstart Resource and the unit(s) to be started." The addition of the term "group of Elements" is based on this Requirement that includes "and initial switching Requirements" in addition to the Cranking Path, and it is meant to include the group of Elements that is included in these initial switching Requirements.

One commenter requested clarification on the applicability of Section 4 with respect to Distribution Providers (DPs). The SDT notes that the clarification is included in the Guidelines and Technical Basis section of the standards relating to applicability. The guidance specifically says: "Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2." This means that DPs that own assets listed in 4.2 are subject to the standard. In addition, "For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above" are excluded from applicability of the CIP standards. That means that only systems and equipment listed in 4.2.1 are subject to the CIP Cyber Security standards.

Many commenters stated that the qualifications for applicable assets in section 4 for Cranking Paths unfairly includes non-BES facilities for DPs while excluding those from Transmission Owners (TOs) and TOPs, for which all BES Facilities are defined under section 4 as applicable. Alternate language was proposed to only include BES facilities in the scope for Cranking Paths. The SDT clarifies that those TOs that own BES Facilities as well as non-BES facilities that are qualified for DPs will also be registered as DPs. A review of the registry listing from September, 2012 showed that 232 of the 340 registered TOs (68%) are also registered as DPs. The SDT further points out that the inclusion of DPs in the applicability ensures that non-BES facilities, such as those that support the restoration of the BES, that are impactful to the reliability and operability of the BES are included.

One comment read that it appears that small entities that own stand-alone UFLS systems with no communication facilities would have applicable Requirements under these standards. It is the intent of the SDT to include all UFLS systems that meet the criteria defined in section 4. These criteria do not include any exclusion based on connectivity. The SDT points out that for DPs, only those UFLS systems that can automatically shed 300 MW or more under a common control system are qualified for applicability. The Requirements that are applicable based on connectivity are specified in CIP-003 through CIP-011. The commenter also stated that, "Further a small entity that is part of a larger load shedding program should maintain their program, but the entity that is responsible should be the one with the cyber security based on the common control system." The SDT clarifies that the owner of all qualified cyber systems is the entity responsible for compliance of these cyber systems: while the common control system that is capable of shedding 300 MW qualifies that UFLS, all cyber systems that impact the reliable operation of the UFLS system become in scope. The

responsibility for the compliance of each of these cyber systems to applicable Requirements belongs to the owner of that cyber system.

One commenter stated that the Functional Entities in section 4.2.1.3 and the Impact Rating Criteria in Attachment 1, section 3.6, for DPs to include facilities containing "A Protection System that applies to Transmission ..." is a new (initially introduced in draft 2) unsubstantiated Requirement for low impact assets. The SDT points out that among the tasks of the DP in the Functional Model is to "design and maintain protective relaying systems, under-frequency Load shedding systems, under-voltage Load shedding systems, and Special Protection Systems that interface with the transmission system." Further, the NERC Statement of Compliance Registry Criteria (Appendix 5B of the NERC Rules of Procedure) includes:

> "III.b.2 Distribution Provider is the responsible entity that owns, controls, or operates Facilities that are part of any of the following Protection Systems or programs designed, installed, and operated for the protection of the Bulk Power System:
>
> - a required UFLS program.
> - a required UVLS program.
> - a required Special Protection System.
> - a required transmission Protection System."

The same commenter suggested that the inclusion of all BES Facilities in section 4 is excessive. The SDT takes the position that cyber systems that impact the real-time operation of any BES Facility must be subject to some form of protection that is commensurate with its impact. The SDT points out that only those BES Cyber Systems that have a real-time impact to the BES are included by definition. This is also in consideration of comments in FERC Order No. 761.

Another commenter wrote that the use of the defined term "BES Facilities" in the applicability section would exclude such assets as Control Centers and Protection Systems. While these facilities are not BES Facilities per se, they are facilities essential to the reliable operation of the applicable BES Facilities and are included for applicability because of the function they are providing for reliable operation of BES Facilities.

One commenter stated that the clause "is subject to one or more Requirements in a NERC or Regional Reliability Standard" was unclear and proposed "can affect the reliability of either Medium or High Impact Facilities." The SDT believes that DPs have to comply with NERC Reliability Standards for some facilities they own and that the current clause

provides certainty as to what those facilities are since these DPs are required to comply with these standards. The SDT feels that the proposed language provides less certainty and is more subjective.

One commenter noted that exempting utility owned communications infrastructure (exemption of communications facilities between ESPs) creates a cyber security issue. The SDT believes that utility owned carrier services should be treated in exactly the same way a third party carrier is viewed in terms of trust, and that adequate protection measures should be taken to protect against an untrusted (from the BES Cyber System point of view) service provider.

Draft Reliability Standard Audit Worksheet

Some commenters provided input and feedback in their comments to the draft RSAW for CIP-006-5 that NERC Compliance Operations posted concurrently with draft 3 of the CIP Cyber Security Standards. The intent of the SDT in contributing to the development of a draft RSAW for CIP-006-5 was to begin the initiative of developing RSAWs in concurrence with standard development projects. The SDT provided input to the draft of the RSAW, and it is encouraged by the opportunity for the SDT and industry to continue to provide input as the RSAWs continue to be developed subsequent to the industry's approval of these standards. The SDT has forwarded these constructive inputs to NERC Compliance Operations for their continuing consideration.

"Annual" and Other Time Parameters

Some commenters pointed out that in a few instances, the SDT inadvertently continued to use the "at least once each calendar year (or similar)" language in conjunction with the convention to not exceed 15 calendar months. The SDT has reviewed the standards and eliminated those "calendar year" references where the SDT intended to use only the phrase "at least once every 15 calendar months."

A few commenters continued to suggest alternatives or expressed preference for retaining only the "annual" reference, which would result in continued reliance on CAN-0010. The SDT has not implemented that change because within Version 5 there is an opportunity and an obligation to unambiguously reference the periodic time parameter. The SDT also explained this in greater detail in response to draft 2 of the Version 5 CIP Cyber Security Standards on pages six and seven of summary consideration of comment form A.

One commenter expressed a desire to adopt a "once per month" convention instead of using, "At least once every 35 calendar days..." where that phrase is used. This is similar to the discussion on "annual," and for similar reasons, the SDT has not made the change. The SDT intends for these time periods to be repeatable on a basis that approximates

performance on the same day per month, or more frequently. The SDT believes it is reasonable to use 35 calendar days to account for those scenarios where a month may begin or end on a weekend, or for holidays.

Authorized Access List and Specific Rights Reviews in Multiple Standards

One commenter identified possible issues with a lack of understanding and inconsistent implementation for authorized access lists and specific rights review in Versions 1 through 3 of CIP-004 Requirement R4, CIP-003 Requirement R5, and CIP-007 Requirement R5. The commenter further stated that there was a concern that the quarterly and annual verification of CIP-004-5 Requirements Parts 4.2 and 4.3 are predicated on some generalizations and/or assumptions that are not complete and will not sufficiently resolve existing issues.

Similarly to the comment above, another commenter had issues with a lack of understanding and an inconsistent implementation for authorized access list and specifics rights review with the multiple standards as mentioned in the previous paragraph. The commenter was concerned that CIP-004-5 Requirement Parts 4.2 and 4.3 quarterly and annual verifications are predicated on some generalizations and/or assumptions that are not complete and will not sufficiently resolve the existing issues. Furthermore, the commenter stated that access authorizations and provisioning warrant further clarity in the recirculation ballot because they require significant resources, involve extensive complex data and are among the most currently violated Requirements. In response to the two aforementioned comment responses, the SDT has modified Requirement Parts 4.2 through 4.5 to state up front to which type of access each Requirement Part applies. CIP-007-5 Requirement Part 5.2 is a security hardening control applying to the enabling or disabling of generic accounts (From the Technical Guidelines section: A generic account is a group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type).

The key distinction between CIP-007-5 Requirement Part 5.2 and CIP-004-5 Requirement Part 4.3 it that generic accounts and associated privileges are not authorized nor is there the same concept of "need to know." CIP-004-5 Requirement Part 4.3 applies to user accounts only and would not necessarily indicate a full listing of user accounts and privileges on the system. However, one could envision a process by which an entity finds it more efficient to perform a full account listing and thereby produce evidence in compliance for both Requirement Parts. The SDT also point out that the identification of default or generic accounts occurs only once and does not require annual verification.

The SDT acknowledges the listing of individuals with authorized access to shared accounts (CIP-007-5 Requirement Part 5.3) has a connection to the authorization of CIP-004-5 Requirement R4 because entities must know the list of individuals

authorized to a shared account in order to fully perform the quarterly and annual assessments. However, entities may comply with the Requirement to authorize access to a BES Cyber System without specifying how they obtain such access. Overall, the SDT sees valid arguments for this Requirement Part residing in both CIP-004-5 and CIP-007-5. Because of the history of prior versions, the difference in applicability, and the significance in moving a Requirement Part to a different standard, the SDT choose to retain the Requirement in its original location.

Data Retention Requirements

There were several commenters that stated specifically and in general to exclude any data retention Requirements from the standard. In response, these few Requirements are not intended to specify a retention period as done in the Compliance section of standards, but to retain information for the purpose of incident response and analysis.

CIP-002-5

Draft 3 of CIP-002-5 obtained an affirmative ballot result of 74.9% with a quorum of 80.6% of the ballot pool at its successive ballot of October 2012. This result indicates a very significant improvement from the previous ballot and achieves a high level of stakeholder consensus.

One commenter noted an inconsistency in sub-Requirement numbering in the standard. This has been corrected and the part numbers have been changed in CIP-002-5 to remove the "R" from Requirement "R1.1", etc., to "1.1", etc.

There was a comment that stated the purpose of the standard is inconsistent with the approach, further noting that "the standard as written evaluates only the impact of a degradation to a group of Facilities instead of evaluating the degradation of a BES Cyber System." The SDT notes that the standard has taken the approach that the categorization of qualified BES Cyber Systems is based on the impact of the functions performed by the assets they are supporting. This is consistent with risk management approaches that evaluate risks based on the functional objective of the organization (in this case the reliable operation of the BES). The same entity proposed a multilevel evaluation of the impact of cyber systems based on functional impact as well as the individual impact of the cyber system within the functional impact. This multilevel approach was one that was proposed to stakeholders early in the development process: industry comments called for a simpler approach which resulted in the current one.

Another commenter stated that the CIP-002-4 and Version 5 "bright-line criteria" step away from a risk based method to a prescriptive approach. The commenter further wrote that it is an inverted philosophy from the approach draft 3 used in the other CIP Version 5 standards. The SDT notes that CIP-002-5 follows on the approach used in Version 4, which has been approved by the industry and by FERC, for using bright lines instead of an entity-defined risk-based methodology for evaluating the impact of assets, and the SDT is extending the concept with a multi-tiered approach to categorizing all BES Cyber Systems according to impact.

There was a comment that the standards use the term "Transmission stations or substations," and the commenter proposed some other terms such as "switchyards." The SDT points out that a brief clarifying paragraph is included in the Guidelines and Technical Basis explaining the use of these terms in the section on Transmission criteria: "*The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain*

autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist." The SDT also made minor editorial changes when using this term for more consistency.

There was a comment that the paragraph in the Background section that deals with the 300 MW UFLS threshold should be moved to the Guidelines and Technical Basis section. The SDT points out that section 4 is a common section that is in all the standards and believes that the explanation of the 300 MW threshold used in the common section 4 should be included in the common part of the Background section to carry it into all the CIP standards in this series.

One commenter provided general feedback on the approach taken for CIP-002-5. The commenter cited concerns on the Facilities-based approach to evaluating the impact of BES Cyber Systems. The SDT had extensive discussions in the last several years on the merits of both the systems-based and facilities-based approaches. The SDT points out to the commenter that entities are free to use any method to arrive at the identified and categorized BES Cyber Systems. Regarding the evaluation of the impact based on the function of the assets, a fundamental concept in risk management frameworks, including the National Institute of Standards and Technology (NIST) Risk Management Framework, is that the evaluation of the risk for systems must be related to the mission of the organization, in this case, the reliability of the BES. The entity also commented on the lower level of protection for low impact BES Cyber Systems. This is consistent with tailoring the level of protection according to the risk (in this case, the impact) and optimizing available protection resources for the systems that most need the protection according to their impact on the mission of the organization. The commenter also commented on the consideration of "interconnectedness". The SDT has taken the approach of considering connectivity in the development and application of Requirements.

There was a comment made that the section on BES reliability operating services in the Guidelines and Technical Basis section should be removed as it contains many subjective areas. The SDT has gone through several iterations of including these in the standards or as guidance and has resolved to providing guidance on functions for applicable functional entities based on the functional model. The section has been well-received with comments requesting the included enhancements in the past drafts.

A recommendation was made that the undefined term "adversely impact" should be replaced with "Adverse Reliability Impact" throughout the standard and definitions document to be consistent with the defined term in the NERC Glossary. The SDT disagrees, because where the SDT has used the term Adverse Reliability Impact, it has used it precisely for the meaning defined in the NERC Glossary. It is not appropriate to use the NERC Glossary term when it is not the intent of

the SDT to use the meaning of the defined term. The NERC Glossary term is very specific to a level of impact on the reliability of the BES. This is not always the appropriate level or meaning in all cases where the term "adversely impact" is used.

One commenter noted that the diagram at the end of the Guidelines and Technical Basis section is confusing. In response, the SDT notes the flowchart is an actual use case provided by an observer and may not be applicable in all environments. It is meant to provide one approach used by an entity.

Requirement R1

There were several commenters that noted there was inconsistency in the words used in Requirement R1 and Attachment 1, criterion 3.4 of section 3 (Low Impact), regarding restoration, with terms used in EOP-005-2 and with terms used elsewhere in the standard. The SDT has made changes to these sections to be consistent with the terms used in EOP-005-2: Blackstart Resources and Cranking Path and initial switching Requirements.

One commenter requested that additional reference to the specific standards be included where the term "...is subject to one or more Requirements in a NERC or Regional Reliability Standard" is used. The commenter furthermore stated that this term is not specifically used in Requirement R1 or the Requirement Parts. However, it is used in section 4 to qualify UVLS/UFLS, Special Protection Systems and Protection Systems owned by DPs that are subject to these CIP standards. In response, the SDT notes the intent is to include only those assets for DPs that are covered by a NERC Reliability Standard, which would be those, by implication, that are related to the reliable operation of the BES. References to other standards within a standard are not recommended practice in NERC standards drafting.

There was a comment that the last sentence in the opening paragraph for Requirement R1 in the Guidelines and Technical Basis section for Requirement R1 is confusing. The SDT has clarified and simplified the sentence.

One commenter stated that the use of the term "considers" in Requirement R1 leads to the same confusion as exists with the existing CIP-002-3 standard as some entities will argue that "consider" does not mandate a required subsequent action. The commenter proposes that the Requirement should be restated as "For each asset type enumerated below, each Responsible Entity shall: . . ." In using the term "considers", the SDT recognized that all entities do not own all the types of assets listed. The proposed language assumes that all entities own all of the types of assets listed. In providing this consideration, the SDT seeks to avoid situations where entities end up having null lists for each one of the type of asset that it does not own.

The same commenter stated that the assertion in Requirement Part 1.3 that the entity is not required to produce a list of low impact BES Cyber Systems renders this Requirement not auditable for accuracy or completeness; and that to demonstrate that all high and medium impact BES Cyber Systems have been properly categorized, the entity must be prepared to produce a list of all BES Cyber Systems that were evaluated, the remainder of which represent the low impact BES Cyber Systems. The commenter further stated that the entity must be prepared to demonstrate the minimal Requirements applicable to low impacting BES Cyber Systems have been properly implemented, also requiring a list of impacted systems. The SDT has considered the considerable increase in the scope of cyber systems included in this version and has taken the approach that those Requirements that apply to the anticipated large number of low impact field systems should be focused on program components that provide the corresponding level of protection, rather than a disproportionate effort in managing compliance for these systems.

One commenter suggested the removal of Requirement Part 1.3 and the low impact category in Attachment 1. The SDT has taken the approach that all BES Cyber Systems should be subject to some level of protection. The SDT has provided an approach to allow the specification of the commensurate level of protection for low impact cyber systems while providing a framework that would minimize entities' compliance burden for the large number of low impact cyber systems that it anticipates.

One commenter recommended that the six asset categories included as part of Requirement R1 be removed and the drafting team instead reference Attachment 1, if needed, to ensure consistency in language as well as prevent unnecessary duplication. The inclusion of the asset types in Requirement R1 is a direct result of comments from a large number of stakeholders on draft 2 to provide some reference to asset types required to be considered in Versions 1 through 3. The SDT has made modifications to improve overall consistency within the standard.

Another commenter noted that, in Requirement Part 1.3, the intent is to provide protection at BES Facilities that do not meet Attachment 1, criteria 1.1 through 2.13. The commenter added that the wording is technically flawed and conflicts with the definitions of BES Cyber Assets and BES Cyber Systems. The commenter continued to add that, by definition, to qualify as a BES Cyber Asset and System the asset must have a 15 minute impact on reliability of the BES and that a low impact facility cannot have such an impact to the BES. The SDT points out that while the definition of the BES Cyber System and BES Cyber Asset assumes impact on the function of the Facilities, systems and equipment (asset), an asset in the low impact does not assume that it has no impact on real-time operation of the BES. The 15 minute stipulation in the definition of BES Cyber Asset describes an impact on the function performed by the low impact asset for the BES.

One question arose which asked how an auditor is to verify identification of all BES Cyber Systems that are applicable to Requirements Parts 1.1 and 1.2. There are current Requirements to identify Critical Cyber Assets in Versions 1 through 4. The SDT expects that auditors will continue to use similar methodologies used to verify compliance to such Requirements.

One commenter stated that its interpretation of Requirement R1 meant that each qualified cyber asset must be marked. This is not the intent, and the SDT does not believe that the language in Requirement R1 is specifying any such marking for cyber assets at each asset. The clause "at each asset" is purposely included in close proximity to "BES Cyber Systems," which is the phrase that "at each asset" is intended to qualify, not the word "identify". Certainly, the expectation is that the identification of the BES Cyber System would include information in some fashion about which asset it is "at". The proposed language "Identify and list each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at the asset level," does not meet the intent of the Requirement, since it must be clear that the identification must have enough information to identify the BES Cyber System, including the information on what asset it is located at.

Requirement R2

Many commenters noted that alternative, clearer language for Requirement Part 2.1 would ensure that there is no implied Requirement for updates outside of the annual Requirement review. The SDT believes the 15 month review is sufficient for categorization of BES Cyber Systems, and it has modified the language to provide additional clarity.

Attachment 1

There was a proposal that the language should be modified to specify that the applicable functional obligations referenced within criteria 1.1 through 1.4, 2.11, and 2.12 apply to only those real time tasks identified in the Functional Model. The SDT points out that the applicability of the Requirements is to BES Cyber Systems, and that the definition of BES Cyber Assets (and by reference, BES Cyber Systems) only includes those that impact real-time operation. The functional model does not define the tasks of the functional entity in terms of real-time or non-real-time, but the term real-time is used rather to describe its relationship with other functional entities.

Many commenters reiterated their comment on the rationale for categorization as high impact those Control Centers that control at least one of the medium impact facilities. The SDT responds that the localized impact of a facility at a single location is different and less impactful than the impact of a Control Center that controls one such facility and other facilities in the wide area.

There was one comment that stated Attachment 1 does not specify where within-hour generation and interchange scheduling systems related to Balancing, Managing Constraints, and Inter-Entity Coordination fall within the high-medium-low impact framework. The SDT clarifies that these systems used to perform functions that are not impactful to real-time operation of the BES, as such would not be defined as BES Cyber Systems, unless these systems are also performing functions impactful to the real-time operation of the BES. They would be included in scope in the initial scoping of supporting the functional obligations of the relevant functional entity, but systems strictly performing these functions in the absence of other functions impactful to real-time operation would fall out of scope.

There was a comment that the first bullet under the overall heading of the Guidelines and Technical Basis section for Attachment 1 makes several references to the term "BES Asset." The SDT has corrected the inappropriate capitalization of BES asset and uses the term BES asset as referenced in Requirement R1 of CIP-002-5.

One commenter expressed concerns that restoration facilities were categorized as low impact facilities. This issue was raised in comments received in previous drafts and the SDT has discussed this at length, reaching out to other NERC technical committees. After consideration of the overall risks to the availability of adequate restoration resources, the SDT's resolution was to categorize restoration facilities as low impact, as explained under the Guidelines and Technical Basis section of CIP-002-5, on pages 30 and 31.

Many criteria in Attachment 1 relate to Interconnection Reliability Operating Limits (IROLs). One commenter wrote that this may be a problem in the WECC area where the RCs have not yet defined IROLs. Consultation with WECC indicated that WECC is in the process of defining IROLs and that IROLs will be defined well within the implementation timeline of these standards.

Another commenter stated that since the term "associated data centers" has been removed from Attachment 1 and that it should be removed from the Guidelines and Technical Basis section. The term has been moved to the definition of the Control Center and an additional clarification has been included where it is referenced in the Guidelines and Technical Basis section.

Criterion 1.2

One commenter noted that the 3000 MW minimum specified in criterion 1.2 is excessive and does not appropriately reflect the potential risk a network-connected Balancing Authority (BA) has not only upon its own service area but also

upon the rest of North American BA, Reliability Coordinator (RC), and TOP registered entities with which it is directly or indirectly connected via the ICCP communication networks. The SDT carefully considered discussions from stakeholders and reviewed data on the distribution of BAs that would be affected. The SDT concluded that the threshold would include the majority of BAs with significant impact.

Criterion 1.4

Many commenters noted that this criterion would require that a 1500 MW Generator Operator (GOP) Control Center take on a High impact rating, while the rest of the Facility is medium impact. The commenter added that even if the criterion is intended to apply to multiple locations, the aggregated generation should be 3000 MW or greater - consistent with the risk level assigned to a BA Control Center. The SDT points out that a control room for a single generating plant at a single location does not meet the definition of a Control Center. The criterion has not defined a specific numeric bright line for a generation Control Center. For example, a generation Control Center could control three 1200 MW generation Facilities, for a total of 3600 MW, at more than one location, and still be qualified for a medium impact generation Control Center if none of these meet criteria 2.1, 2.3, 2.6 or 2.9. It is true that if one of the generation Facilities the Control Center controls meets criterion 2.1 for 1500 MW, it would be categorized as a high impact asset.

Criterion 2.1

One commenter requested clarification on the relationship between a single plant location and a single Interconnection used in the defined term meaning. In making these qualifications, the SDT considered scenarios where sets of units within a single plant location may service multiple Interconnections, as pointed out by the commenter. In these cases, the SDT wanted to ensure that the impact considered is consistent with the bright line defined in this criterion, which was based on numbers reviewed for each Interconnection. The same entity inquired about “multiple generators with different interconnection facilities which connect to different parts of the same substation.” It is not clear whether the commenter is using the general term interconnection (meaning connection to the Transmission System) or in the meaning of the defined term.

One commenter felt that the use of the word “by” in the first sentence of this criterion does not make sense and should be reworded. The use of the word provides an entity with the capability of evaluating groups of units when a single plant location may be servicing multiple Interconnections and is logically partitioned into more than one generation output. There are further qualifications which may provide additional grouping criteria, such as common cyber systems.

One commenter suggested that the 15 minute stipulation should be extended to 30 minutes to be consistent with some criteria in reliability standards. Some standards have used 15 minutes, which the SDT has used as its criterion. The commenter seems to suggest that the 15 minutes is "tighter" than 30 minutes. Extending the interval to 30 minutes would in fact reign in more cyber systems rather than reduce the number of cyber systems (by extending the criterion for real-time, more cyber systems are likely to meet this criterion than 15 minutes).

One commenter requested clarification on the term "commissioned generation." The term is used to specify generation resources that have been commissioned for operation and is intended to exclude generation that has not been commissioned for operation (such as mothballed generation, generation shut down for maintenance, or new generation that has not been commissioned for operation yet).

Criterion 2.3

There were many comments that the term "planning horizon of one year or more" is unclear and could be misinterpreted. The SDT has added guidance on this to make it clear that the planning horizon of one year or more means that the plan covers a reliability planning span of one year or more and that it does not necessarily mean that the operating day is over one year. The intent is to exclude generation required to operate or keep on operating to temporarily avoid reliability impacts.

There were many comments on the guidance relating to the role of the Regional Entity (RE)/ Regional Reliability Organization (RRO) and noted that the RE/RRO is not required to perform coordination of the actions resulting from planning studies. The commenter also noted that the term RRO is no longer the appropriate term. The necessary changes have been made.

One commenter asked whether the term "generation Facility" in this criterion is designed to cover a single unit at a facility, or all units at a single plant or Interconnection, as described in section 2.1. The SDT intended to include in this criterion all generation Facilities required to meet the designation: these can be a single unit, a set of units or all the units in the plant.

One commenter noted that the Guideline and Technical Basis section omitted the TP as one of the possible entities that could designate the generation Facilities. The SDT notes this has been corrected.

A commenter asked whether the phrase, “such as due to a Category C3 contingency” was intended to provide guidance to what faults to run and whether the term “Adverse Reliability Impact” which is used in Attachment 1, meant to be the criteria for all types of contingencies. The phrase “such as due to a category C3 contingency” is intended to provide an example of the type of condition that could lead a Planning Coordinator (PC) or Transmission Planner to designate “must run” generation Facilities. The term “Adverse Reliability Impact” is used here to qualify the reason the PC or TP would designate such generation Facilities. In response, the SDT notes it is intended to distinguish from designations made for power market management reasons.

One entity commented that the guidance provided in this section in the Guidelines and Technical Basis section referenced “Reliability Must Runs (RMRs)” and discussed the differences between market RMRs and what this criterion intended. The SDT points out that this is the reason it has avoided using the term “reliability must run” in the Requirement itself. However, this term has been used interchangeably in both contexts for lack of a better term, and that the meaning of the term and the reason for having these units differ depending on the context. The SDT has included an extended discussion of the underlying reason for the criterion in the Guidelines and Technical Basis, focusing on the long term remediation for BES deficiencies to avoid Adverse Reliability Impact. The SDT also made additional changes to the guidance to clarify the role of the RE in coordination and contracts.

There was a comment that the criterion is based on studies from functional entities that do not have applicability under this standard and on notifications from these entities. The SDT notes that these activities are implemented today and that there are TPL standards that require these functional entities to perform these studies. The standard also requires these planning entities to provide an action plan for remediation of identified deficiencies.

Criterion 2.4

In this section, medium impact is assigned to Transmission Facilities operated at 500kV or higher. One commenter noted that exclusion is warranted for distribution stations that are situated at the receiving end of a radial 500kV line. The commenter further noted that specific instances exist of 500/69kV stations whose only purpose is to provide distribution service. The applicability, which is section 4, stipulates applicability to BES Facilities for entities other than DPs. If the facility meets the qualification for designation as a non-BES facility under the definition of the Bulk Electric System, then it is not in scope for application of these CIP standards.

Criterion 2.5

One commenter noted that the 200kV floor specified in criterion 2.5 does not adequately consider the risk to the BES imposed by large regional areas that are predominately sub-200kV. The commenter noted the BES is defined as 100kV and above and the criterion needs to consider all of the BES in some manner. The SDT has not excluded any BES Transmission Facility in its applicability, but believes that not all BES Transmission Facilities should be protected at the medium impact level. The categorization is one that is based on impact, and the SDT believes that the inclusion of ALL BES Transmission Facilities at a single impact category is unjustified and defeats the concept of tiered levels of protection based on impact.

One commenter stated that, as currently defined, the values in the table force a label of critical on non-critical Facilities as proven by intricate studies performed by transmission planning engineers. The commenter recommends the values be revised as follows: Voltage Value of a Line 200kV - 399kV - Weight Value per Line - 800; Voltage Value of a line 400kV to 499kV - Weight Value per Line - 1300. The SDT based the values in the table on values published in an engineering report, has reviewed comments from previous drafts, and believes that it has a technical basis, as described in the Guidelines and Technical Basis section, for using these values.

A commenter provided an extensive discussion of the concerns on the application of this criterion for Direct Current (DC) Facilities. The commenter argued that in the case of DC Facilities, the impact is better assessed in a wide area perspective rather than as a localized way as specified in this criterion. The commenter further commented that such studies could be conducted to provide an impact based on MW rather than the approach used in 2.5 in the case of DC Facilities. The SDT has not considered this approach for DC Facilities and any criterion that is based on a “study” (that is not currently required by any reliability standard) to determine the impact of these DC Facilities would be contrary to the bright line approach.

One commenter requested that diagrams be provided to illustrate the bullets in the Guidelines and Technical Basis. The SDT discussed providing diagrams to illustrate the bullets, but resolved that there are many configurations that can provide these illustrations and that these would raise additional questions for entities that would not be familiar with specific configurations. Entities should use their specific configuration to apply these concepts.

One commenter requested many clarifications. These are listed below with their responses:

1. Is/how is a DC line counted?
   A DC line is counted at the operating voltage for the purpose of application of criterion 2.5.

2. If you have a tie between two subs that has a transformer in series, does the line receive a weighting factor (seems to per guidance)? Do you use the higher or lower voltage? Is it the same for both ends of the line?
   If the transformer in at the site of a Transmission station or substation, it is considered as part of the Facilities of that station or substation and lines incoming and outgoing of the station or substation are considered in the application of this criterion. If the transformer is in a dedicated station, each of the stations (including the transformer station) will consider incoming and outgoing lines of the station or substation in the application of the criterion.

3. From the guidance document, it was clarified that radial facilities that only provide support for "single generation facilities" would not be included. What is the definition of a "single generation facility"? Uncertain situations might include two base load turbines aggregated on one line or wind farm collector subs which have multiple sites feeding into a single high voltage collector sub?
   These examples are all considered as a radial connection to a single generation facility.

4. From the guidance document, in the last bullet on page 27, it is not clear what the statement "In these cases" is referring to, whether the designation as a single facility or multiple facilities.
   The clause "In these cases" is qualified further by "of these transformers being within the "fence" of the substation or station": this is referring to what is considered a single facility.

5. From the guidance document, in the last bullet on page 28. How would classification of the number of substation connections be handled if two lines are parallel between the same two subs, but one has been tapped for local, non-networked load service?"
   Assuming that the tap is at the station or substation, these would be considered connections to one other substation, but both outgoing lines would be counted for the purpose of aggregate weighting. If the tap is not at the station or substation, there is not enough information to definitively make a determination without evaluating the specific facts and circumstances.

One commenter inquired during the comment period on whether the connections to other stations or substations that are considered are only those that are operating at voltage levels between 200kV and 499kV. The SDT reviewed previous drafts and clarified the criterion to ensure that the qualification of voltage levels of 200kV and higher for these connections is more explicitly stated rather than implied.

Criterion 2.6

One comment was on the obligation for the RC with respect to IROLs. RCs are required to provide to its TOPs in its RC footprint the SOLs under FAC-014-2, Requirement R5.1. In particular, it requires the RC to provide specific information related to IROLs in the sub-Requirements of 5.1. The particular agreements between RCs, TOs and TOPs to enable the proper management of IROLs in compliance with the NERC Reliability Standards are beyond the purview of the guidance. The SDT points out that the delegation of functional obligations must be considered in these Requirements.

Criterion 2.8

A commenter noted correctly that Transmission Facilities under 2.8 that do not affect Transmission, in aggregate, for generation that is less than 1500 MW do not qualify under this criterion, even if the generation facility (plant) contain cyber systems that qualify under 2.1., (provided they do not qualify under other criteria).

Another commenter noted that, in the case where the generation is not owned by the TO/TOP would be at the mercy of the Generation Owner's (GOs) application of the standard even if the TO's facilities would not otherwise be in scope. The commenter is correct in that the TOs Facilities providing the connection would be deemed to be a medium impact. This is consistent with the impact of these Transmission Facilities on the BES.

Criterion 2.9

One commenter requested clarification on what an automated switching system is. Automated switching systems refer to systems implemented in software that perform the same automated protection functions as Special Protection Systems or Remedial Action Schemes.

Criterion 2.10

One commenter stated that the guidance document specifies that the SDT "chose the term 'each' to represent that the criterion applied to a discrete System or Facility". The commenter's interpretation of this statement is that a regional UFLS program which sheds more than 300 MW and is comprised of multiple independent UFLS relays in at different substations would not be given a Medium Impact Rating at the NERC or RRO program level and that an individual relay would only be given a Medium Impact Rating if that relay shed more than 300 MW by itself. The commenter's interpretation is partially correct in that individual independent relays that are part of a UFLS system that sheds 300 MW or more in the program Requirements, but do not shed the required load by a common control system, (e.g., they individually trigger independently, even if they are configured to trigger based on the same sensed conditions) do not qualify. However, if the individual relays are all triggered automatically by a common control system that determines

that conditions warrant the action (such as a control panel that triggers a system of relays in a substation), then they are part of a load shedding system that can automatically shed more than 300 MW and therefore qualifies. The commenter's assertion that a single relay that sheds 300 MW or more does qualify is correct.

The same commenter noted the statement on ERCOT's LaaR demand/response program is not considered as qualifying under this criterion and requested more general guidance in the Guidelines and Technical Basis section for this criterion that talks to these types of programs. The SDT has included a more general statement in this section.

Criterion 2.11

There was a comment that the Guidelines and Technical Basis section on this criterion incorrectly referenced a 300 MW threshold. The SDT has made the necessary correction.

Criterion 2.12

Many comments related to the portion of criterion 2.12 of Attachment 1 that is applicable to TOP Control Centers. Commenters stated that criterion 2.12 of Attachment 1 included all TOP Control Centers, not already categorized in the high impact category, as medium impact and that many smaller TOP entities' Control Centers should be categorized as low impact in the same manner that criteria were defined for generation and balancing authority Control Centers. Many commenters proposed alternate proposals for a threshold that could provide such a criterion to be used as a candidate for categorization as low impact, such as voltage levels lower than 200 KV or using throughput indicators similar to those used in the case of transmission substations in criterion 2.5. Others provided proposals to restructure the thresholds for all three impact levels for TOP Control Centers. One commenter also proposed an exclusion clause in criterion 2.12 that would be based on engineering analysis that demonstrated minimal impact to the BES. In response, the SDT did not find any such study that would be required by an existing NERC Reliability Standard.

As part of a consolidated response to more than one entity that provided comments on draft 2's CIP-002-5, Attachment 1, criterion 2.11 (which maps to criterion 2.12 in draft 3 and draft 4), the drafting team carefully considered comments to include a threshold for TOP Control Centers, but, to reiterate previous considerations and response to the comments related to that criterion (on page 35 of consideration of comments form A), such a threshold is not supported in consideration of the functions provided by those Control Centers. The largest concentration of cyber traffic is to and from Control Centers, and loss, compromise, or misuse of cyber systems at control centers constitutes a high risk to reliability. Furthermore, criterion 2.12 applies to "Control Centers" used to perform the functional obligations of TOPs, so it is only applicable to the extent the Control Center meets the criteria of the proposed definition.

While there is clear guidance in the NERC Reliability Standards that the SDT could use to determine bright lines for generation in the wide area (such as contingency reserve Requirements), the SDT did not find any in the Transmission area to support thresholds for TOP Control Centers. The source for transmission substation bright lines, based on throughput in a Transmission station or substation according to voltage level, provided easily measureable thresholds because of their localized nature: for a given single location, the application of the threshold criteria can be easily determined. There was no bright line that the SDT could find applicable and justifiable in a wide area situation for TOP Control Centers that control many interconnected Transmission Facilities in many locations. The SDT could not find any technical guidance, either in NERC technical studies, or in existing NERC Reliability Standards Requirements, on how the loss of interconnected Transmission Facilities could be used as a basis for establishing thresholds for TOP Control Center impact. The TOPs span of control is not limited to just Transmission lines, but to a large number of diverse Transmission Facilities that relate to the reliable operation of the BES. This complexity, together with the interrelated impact from the large number of diverse Functional Entity types that impact TOP functional obligations, make it very difficult to define a justifiable threshold that can be rationalized considering all the scenarios that could impact real-time operation for a TOP Control Center.

As stated in the guidance for CIP-002-5, the reasoning and purpose for the 1500 MW threshold for generation is different:

> "By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected."
>
> The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used."

Furthermore, the SDT has an obligation to be responsive to FERC Order No. 706, which was issued after a notice of proposed rulemaking, and several points from that order were reiterated in subsequent FERC Order No. 761. The SDT has discussed this issue very significantly in several face-to-face SDT meetings. In addition to the technical reasons and differences explained above, the SDT anticipates that any threshold for TOP Control Centers will likely be met with a directive countering such threshold upon filing for approval of these standards.

The SDT based its approach in the development of this criterion in consideration of the following comments and Directive from FERC Order No. 706 approving CIP Cyber Security Standards Version 1 and FERC Order No. 761 approving CIP Cyber Security Standards Version 4.

In its Order No. 706, Para 280, FERC supports the reasoning for its subsequent Directive in paragraph 282 with the following comment:

> "...it is difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be identified as a critical asset…"

The SDT points out that Medium and High Impact under Version 5 translate closely to "Critical Asset" under previous versions. The Directive in FERC Order No. 706, Para 282 further states:

> "Therefore, consistent with the discussion above, the Commission directs the ERO, through the Reliability Standards development process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets."

As explained earlier, the SDT's consideration of misuse of TOP Control Centers and the role they provide, pursuant to this Directive, do not support an exclusionary threshold from medium impact in CIP-002-5, Attachment 1.

In its Order 761 approving NERC CIP Cyber Security Standards Version 4, FERC commented in paragraph 21 that:

> "...Version 4 will offer an increase in the overall protection for bulk electric system components that clearly require protection, including control centers"

In the same Order 761, Para 57, FERC further commented with the following:

> "However, we continue to expect comprehensive protection of all control centers and control systems as NERC works to comply with the Requirements of Order No. 706."

Again, in the case of Generation and BA Control Centers, the SDT used the 1500 MW threshold for consistency with the rationale used for generation bright lines. As stated, no such source can be used for wide-area transmission in the non-CIP reliability standards or other published source.

Therefore, the SDT opted to keep criterion 2.12 as it applies to TOP Control Centers (i) to ensure that all TOP Control Centers are adequately protected, in the absence of technically justifiable thresholds for lower impact TOP Control Centers, (ii) because of the critical nature of their real-time reliability functions for the interconnected Transmission systems they monitor and control, and (iii) in consideration of FERC comments and Directives expressed in Order No. 706 and reiterated in Order No. 761.

Criterion 2.13

One commenter believes that the 1500 MW minimum specified in criterion 2.13 is excessive and unreasonably excludes a significant number of BAs from meaningful participation in protecting the BES from cyber-attack and that establishing criteria effectively eliminates significant numbers of interconnected control centers fails to address the specific concerns outlined in both FERC Order No. 706 and FERC Order No. 761. The SDT considered the MW distribution of BAs and determined that the 1500 MW is consistent with generation thresholds established (and approved by FERC in Version 4) in other criteria and is appropriate in including a significant number of BAs at the medium impact category. The SDT points out low impact cyber systems are still subject to protection Requirements.

Criterion 3.1

There was a comment that criterion 3.1 should specifically state that only Generation and BA Control Centers are included. While combination of the criteria for Control Centers currently results in only Generation and BA Control Centers, this criterion is intended to catch all Control Centers that have not already met a previous criterion in section 1 and 2 (high and medium impact). The current language conveys this intent.

Criterion 3.4

One commenter stated that the use of the terms “critical” and “initial system restoration” in criterion 3.4 is problematic. The commenter noted that initial system restoration is not a defined term and registered entities have regularly argued that none of their resources are critical as they have many options from which to draw upon. The SDT has made modifications to the criterion that uses language consistent to EOP-005-2 and defined terms.

The commenter also noted that the Low Impact Rating criteria needs to include automatic Load shed systems that do not shed sufficient Load to meet criterion 2.10. All Load shedding systems that are part of the BES are included automatically as stated in the Applicability section (section 4). For DPs, Load shedding systems that meet the qualifications in section 4 are included and are all included as medium impact.

CIP-003-5

CIP Senior Manager

A commenter expressed concern on the designation of the CIP Senior Manager by a "high level official" and whether that official could be the same person as the CIP Senior Manager. The SDT notes that the language regarding "high level official" is but one example in the measure. An entity is free to determine the best way to designate a CIP Senior Manager for its unique circumstance. This could be by high level official, by committee, through authorization from a board of directors, or from any number of other options.

The SDT received a comment that there was a concern that by only requiring the identification of the CIP Senior Manager by name that the Requirement was not auditable in instances where multiple individuals have the same name at the same company. The SDT appreciates that this is a very real scenario. However, the SDT believes that this is specifically the style of auditing that it sees is incompatible with the objectives it is setting out to achieve. The SDT believes that real cyber security program leadership transcends the name on the document. Audits, instead of verifying a name on a page, should instead validate the Requirement objective that the individual identified as the CIP Senior Manager is in fact leading and managing the implementation and continuous adherence to the CIP standards.

One comment indicated that "The CIP Senior Manager relies on both the definition in the CIP Glossary and the "Responsible Entity" verbiage in every standard in section 4." The SDT does not agree. The definition of a CIP Senior Manager stands alone. However, the Requirement itself is for the Responsible Entity (the entity obligated to comply with the standard) to identify a CIP Senior Manager.

Policy Requirements

One commenter expressed concern that the SDT was too prescriptive in its language around electronic access controls in the low impact policy. The SDT does not believe this to be the case. On the contrary, the SDT has some concern that it may have left the policy up for too much interpretation. However, the SDT believed that the entity is in the best place to determine the appropriate access controls for its given situation, while still implementing an ESP of some form.

Numerous commenters expressed confusion over the applicability of the policy Requirements. The SDT considered many approaches to this issue and believes that the applicability of these requirements is clear as drafted. Requirement R1 applies to high and medium BES Cyber Systems and states as much explicitly in the Requirement. The intent of

Requirement R2 is to apply to those assets that contain low impact BES Cyber Systems and not to the BES Cyber Systems themselves. This effectively allows the entity to track implementation of the policy at a higher level of abstraction (per asset rather than per BES Cyber System), and the SDT believes this will substantially reduce the burden of evidence required by the low impact policy. The reference to CIP-002-5 is to further clarify the intended reference to asset rather than BES Cyber System. The language following the numbered list specifying that "an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required" is part of the Requirement language of Requirement R2 and should be interpreted as such. This language was explicitly included to give the industry the assurance that this Requirement would be audited (sampled) at the asset (substation, generation plant, etc.) level and not the individual Cyber Asset level. The SDT also believes that entities will be able to implement internal controls to ensure the implementation of the cyber security policy at its low impact assets. The SDT does not believe that there is any double jeopardy between Requirements R1 and R2.

One commenter suggested that the SDT modify the Requirement language for the cyber security policies to clarify that multiple policy documents could "collectively" address the topics in the Requirements. The SDT agrees and has updated the standard to reflect this change.

The SDT received comments that Requirements R1 and R2 require annual review of the policy, but never explicitly require the policy to receive updates as a result of that review. The SDT believes this is implicit in the Requirement, and updates would occur as part of an entity's ongoing compliance with the Requirement.

Requirement R2

One commenter questioned the necessity of Requirement Part 2.4 considering that entities are not required to monitor for incidents to their low impact BES Cyber Systems. The SDT appreciates this concern. This element was specifically included because the SDT strongly believes that incident response is a key component of a resilient system. Even though an entity may not be constantly monitoring for a Cyber Security Incident at its low impact BES Cyber Systems, the SDT expects that should an incident be discovered, a plan should be in place for rapid execution.

Requirement R4

The SDT received comments requesting that language be added into the Requirement clarifying that the delegation authority may itself be delegated. The SDT considered adding language to the standard to clarify this, however, the SDT believed that the Requirement was clear as is and that there was no language that prevented this delegation. The SDT included the discussion on this topic in the Guidelines and Technical Basis section specifically to clarify this issue.

One commenter pointed out that Requirement R4 as written requires that the delegations from the CIP Senior Manager be updated within 30 days of the initial delegation. The SDT agrees this is confusing and has struck this language from the Requirement.

The SDT received questions on why it included the IAC language on the Requirement to delegate authority from the CIP Senior Manager. The SDT specifically included the IAC language because it believes that in a very large organization, it is likely that changes in personnel without adequate update of delegation documentation could result in very minor deficiencies that have little or no impact on the reliability of the BES. These are precisely the types of administrative violations that the SDT is attempting to eliminate from the CIP standards. The SDT believes that, given this is all a single Requirement, the documentation required in the third sentence of Requirement R4 is part of the overall process specified in the first sentence of the Requirement; consequently, the IAC language applies to all parts of Requirement R4.

CIP-004-5

General

One commenter believes that the evidence retention for verifying access should be less than the audit cycle (which is three years for BAs, RCs and TOPs), especially if the SDT plans to keep the quarterly reviews to verify that access has been properly removed. Entities are required to demonstrate compliance with the Requirements for the entire audit period for all NERC Reliability Standards, regardless of evidence retention Requirements.

One commenter noted that within each Background section (section 5) under the heading "Applicable Systems Columns in Tables" is missing the second sentence that appears in the other standards where Medium Impact BES Cyber Systems with External Routable Connectivity is also referenced in the Background sections. The SDT confirms that it intended that phrase to be consistent wherever that applicability term was used, and the SDT has modified the background to clarify that intent.

There was a comment that within CIP-004-5, the definition of EACMS appeared inconsistent with the definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards", and that it could result in misidentification, misapplication or inconsistent application of standards. The SDT has modified the background section with respect to EACMS to provide clarification that these are examples only that support the definition.

Requirement R1

A few commenters requested that Requirement R1 include the IAC language. In response, since the Requirement may be performed at any time during the quarter, the addition of the IAC language would not be appropriate.

One commenter requested clarification on the types of materials to be provided for security awareness on a quarterly basis. The Requirement is to provide an ongoing reinforcement that cannot be provided by an annual training Requirement. The SDT has written the Requirement to allow for flexibility in implementation by the entity. The measure provides some examples of how the entity may meet this Requirement.

A few commenters considered Requirement R1 to be administrative in nature and suitable for elimination pursuant to the SAR Paragraph 81 project. While this Requirement is partly administrative, it does provide the benefit of the entity being able to timely address and make staff aware of emerging threats and vulnerabilities. This awareness can improve security for the entity.

One commenter requested that Requirement Part 1.1 be modified as, “cyber security practices and/or physical security practices.” The SDT clarified that the Requirement part applies to cyber security, which may include awareness on associated physical security.

Requirement R2

One commenter recommended that the training content Requirement Part 2.1 be moved to the measures. The SDT considered the training topics listed to be worthy of being listed as a Requirement for a minimal core competency in security practices. Entities are encouraged to add more topics as relevant to their needs.

One commenter recommended that Requirement Part 2.2 be modified to address newly registered entities. In response, the compliance dates for newly registered entities are addressed in the supplementary implementation plan provided with the Version 5 standards.

One commenter considers it is a security risk to address some of the concepts listed in Requirement Parts 2.1.1 through 2.1.9 with every single person with a need for physical or cyber access to a cyber system, regardless of his or her role. The SDT believes that, as written, the Requirement is flexible to allow the entity to design and implement a security training program that fits their needs. The Requirement does not preclude an entity from using a single or multiple training courses with differing depth in the training provided.

Several commenters requested clarification on the necessary training for personnel based on individual roles, functions, or responsibilities, including changes to roles, functions, or responsibilities. The SDT believes that, as written, the Requirement is flexible to allow the entity to design and implement a security training program that fits their needs. The Requirement does not preclude an entity from using a single or multiple training courses with differing depth in the training provided. How the training program is implemented is at the discretion of the entity.

One commenter requested that CIP Exceptional Circumstances be removed from Requirement Part 2.2, as this applies to numerous parts and is stated at the policy level. The SDT believes that, as written, the Requirement provides necessary guidance related to the Requirement without introducing the need to rely on or link to other Requirements.

One commenter requested clarification on whether the training required by Requirement R2 extends to contractors and vendor support staff. The SDT notes that, as written, the Requirement is clear that training is to be provided to anyone having authorized electronic access and authorized unescorted physical access.

One commenter requested that Requirement Part 2.1.9 be removed. The SDT considers the training topic relevant to address the vulnerabilities of internetworked systems and to address the risks of systems that are integrated and reliant upon data from other sources to perform necessary tasks (interoperability).

Requirement R3

Several commenters noted concerns regarding Requirement R3 where employee history is not available, including the identity verification necessary to perform the criminal history check, and how to comply with these instances. The Requirement provides for this, "If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed."

One commenter requested that the timeline for personnel risk assessments pursuant to Requirement R3 be modified to 10 years to align with other governmental standards and practices. The SDT is not clear if the commenter means performed every 10 years or reviewing the prior 10 years for criminal history. The SDT has kept the timing Requirement of the existing standards as approved by FERC Order No. 706.

Many commenters requested clarification for Requirement R3 that ongoing identity verification is not required. The SDT has noted in guidance and the implementation plan that identity verification is required only initially. However, the Requirement is written to be flexible to allow the entity to design and implement their personnel risk assessment program in a manner that meets their needs to confirm identity. For some, this may include performing subsequent identity verification or it could include confirmation of previous verifications.

One commenter noted grammar concerns with the Requirement R3 table parts. The SDT believes that the overarching Requirement provides the necessary context and clarity for the table.

One commenter stated Requirement Part 3.3 unclear as to whether the evaluation process includes an expectation of clearly defined evaluation criteria for approval/disapproval of the access request. The SDT has modified the Requirement to make this clearer.

Two commenters considered Requirement Part 3.4 unclear as to whether the entity is to perform the evaluation or permits the contractor or service vendor to perform the evaluation using its own criteria with an assertion to the entity of compliance and acceptability. The SDT believes that, as written, the Requirement is flexible to allow the entity to design and implement a personnel risk assessment program that fits their needs. The entity is responsible for ensuring that the obligations of the Requirement are met by their contractors and service vendors.

One commenter requested that the table parts for Requirement R3 be modified to require that a personnel risk assessment must be complete before granting access. The overarching Requirement R3 states that a personnel risk assessment is required in order to obtain access.

One commenter requested that Requirement Parts 3.5 and 3.6 include a clause that it is subject to applicable law and collective bargaining unit agreements. This concern is addressed in the guidance provided for Requirement R3. As written, the Requirement is flexible to allow the entity to design and implement a personnel risk assessment program that fits its needs.

Several commenters requested clarification on whose identity must be verified. As written, the Requirement is clear that personnel risk assessment is to be performed for anyone having authorized electronic access and authorized unescorted physical access. This is further defined in Requirement Part 3.4.

One commenter recommended consolidation of Requirement Parts 3.3 and 3.4 into Requirement Part 3.2. As written, the Requirement defines each individual element to be performed and that these are each elements contained within the program specified by Requirement R3.

One commenter considered Requirement Part 3.3 redundant of Requirement Part 3.2. Requirement Part 3.2 is the performance of the criminal history records check. Requirement Part 3.3 is the evaluation of the records collected under Requirement Part 3.2.

Requirement R4

A few commenters noted concerns regarding the efficacy of Requirement Part 4.2. The SDT considers this Requirement as a key element for security. The intent of the Requirement is to review the accounts residing on the systems with the

records of what accounts are supposed to be on the systems. This helps to provide an assurance that accounts have not been added through malicious code and that provisioning processes are functioning properly.

One commenter recommended that Requirement Part 4.2 be removed and provide it as an example of an internal control that the Compliance Enforcement Authority (CEA) would expect to see. The SDT considers this Requirement as a key element for security. The intent of the Requirement is to review the accounts residing on the systems with the records of what accounts are supposed to be on the systems. This helps to provide an assurance that accounts have not been added through malicious code and that provisioning processes are functioning properly.

Several commenters requested clarity in Requirement Part 4.3 related to which accounts and types are subject to an annual review. Individual user accounts, user account groups or user roles are required to be reviewed on an annual basis. User account groups or user roles are to be reviewed where these are used to for role-based management of access permissions. While review of other account types (i.e.: default account) is a good security practice, it is not a Requirement under the CIP Version 5 standards.

One commenter requested clarification of Requirement R4 regarding the word “verify” and how an entity is expected to provide evidence of access control. The Requirements mandate that access is limited to only those requiring said access. It is the responsibility of the entity to determine how they can demonstrate this limitation through the use of technical or procedural controls. The SDT believes the Requirements are written to allow flexibility in implementation to allow the entity to develop a program that meets its needs. The use of access controls lists, key control processes, and log books should be considered as options.

There was a comment that the phrase “based on need, as determined by the Responsible Entity” within Requirement Part 4.1 does not add anything meaningful to the standard. The SDT added the language based on industry comment concerns to help clarify that the appropriateness is determined by the entity and not by the CEA.

One commenter stated that the concept of role-based privilege management has not been established adequately in the Requirement. The SDT believes that Requirement Part 4.1 is written with sufficient flexibility to allow the entity to implement access control processes that meet their needs. The Requirement does not preclude the use of role-based privilege management. Requirement Part 4.3 has been modified to address this concern.

One commenter requested clarity on the measures for Requirement Part 4.2. The measures are examples of how the Requirement may be met. They are not an all-inclusive list of possibilities. It would not be feasible to list all options available.

One commenter noted concerns regarding Requirement Part 4.3 related to the level of access permission review to be performed. The detailed access privileges are to be reviewed to determine if they are appropriate. This can include review of access to file systems. As noted in the guidance, "The privilege review at least once every 15 calendar months is more detailed…"

Several commenters requested clarification regarding the verification of access to information storage locations pursuant to Requirement Part 4.4. As noted in Requirement Part 4.1, there are three distinct types of access noted; (1) Electronic access, (2) Unescorted physical access into a Physical Security Perimeter (PSP), and (3) Access to designated storage locations, whether physical or electronic, for BES Cyber System Information. The intent of Requirement Part 4.4 is the review of access to BES Cyber System Information only.

One commenter requested clarification on the scope of physical access controls for BES Cyber System Information in Requirement Part 4.1.3. Physical access control for BES Cyber System Information only pertains to the protection of hard copies of said information. The hard copies of BES Cyber System Information are not required to be within a PSP, and therefore, CIP-006-5 may not apply.

Several commenters requested clarification on the phrase "within the last seven years." In order to obtain or retain access, a person must have had a personnel risk assessment "within the last seven years" of when access was provided and ongoing. The Requirement is written to be flexible to allow the entity to design and implement their personnel risk assessment program in a manner that meets its needs. For some, this may include performing personnel risk assessments more frequently.

Requirement R5

One commenter noted that Requirement Part 5.1 does not distinguish between termination for cause and termination without cause. The SDT removed the distinction between types of terminations to meet FERC Order No. 706, Paragraphs 460 and 461, requiring immediate revocation for any person no longer needing access regardless of termination reason.

There were an abundance of commenters that noted that the time frame listed Requirement Part 5.2 is difficult to comply with and is unnecessarily short when the employee is remaining with the company if the transfer or reassignment was in the normal course of business and not for disciplinary reasons. The Requirement allows for the entity to review the access for the individual and retain access as long as necessary for transition from the prior position. The timing was determined to be necessary to meet the to meet FERC Order No. 706, Paragraphs 460 and 461, requiring immediate revocation for any person no longer needing access which includes reassignment and transfer. Note that the timing is based on when the entity determines that the individual no longer needs access, which may not necessarily be the same date as the transfer or reassignment.

One commenter requested clarification for the word "removal" in Requirement Part 5.1. Removal refers to rendering the individual unable to use the access. This may be accomplished through deletion, disabling, revocation, or removal. The SDT wanted to provide flexibility in allowing any of these means to be used.

A few commenters requested clarification regarding Requirement Part 5.4 on what scenarios would fall into this category that are not covered within Requirement Parts 5.1 to 5.3. Requirement Part 5.1 is removing the person's ability for unescorted physical access and Interactive Remote Access. This can be accomplished by revoking just these elements (i.e.: RSA, VPN, Active Directory). Requirement Part 5.4 is to clean up the remaining accounts for the users, such as access to applications, databases, and other systems.

One commenter had concerns that Requirement Part 5.5 could negatively impact the reliability of the bulk electric system in cases where there is a high movement of staff between locations. In such cases the password may change so many times that it impacts people's ability to access BES Cyber Systems (they forget the password due to the high change rate). The SDT believes that due to the capabilities of these accounts, prompt changing of the password is appropriate to minimize the risk from separated employees and contractors.

One commenter requested that "termination action" be replaced with "termination" in Requirement Parts 5.1, 5.3, and 5.4. Please see the Guidelines and Technical Basis section of the standard for additional information regarding a termination action. This section addresses the concerns noted.

There was a request that the phrase "and time" be removed from Requirement Part 5.3, as it is unnecessary, given the reference to a calendar day rather than a twenty-four hour period. The SDT agrees with that clarification and has modified the Requirement to address this comment.

One commenter considers the time limits for revoking access upon terminations to be an extreme challenge. The SDT used the timeline for terminations to meet FERC Order No. 706, Paragraphs 460 and 461, requiring "immediate" revocation for any person no longer needing access, including all terminations, and the SDT believes the approach reflected in the standards is a reasonable means of accomplishing the directive.

One commenter requested consideration of Requirement Parts 5.4 and 5.5 to include Physical Access Control Systems (PACS) since some cyber assets in a PACS can also have individual user and shared accounts. The SDT considers all PACS devices to be subject to the same Requirements, regardless of impact categorization. While removal of access and changing of shared account passwords on all assets is a good security practice, it is not a Requirement under the CIP version 5 standards except where noted in Requirement Parts 5.4 and 5.5.

One commenter requested that Requirement Part 5.5 be changed to 35 days for consistency with other monthly Requirements. The time parameter in this requirement is different than the periodic performance time periods in requirement parts that use the 35 calendar days period. The SDT does not consider this action to be an ongoing monthly Requirement similar to those noted in CIP-007-5.

CIP-005-5

High Water Marking

There was a comment that per the Guidelines and Technical Basis section for CIP-005-5 Requirement R1, all of the Cyber Assets and Cyber Systems, even other BES Cyber Systems of lesser impact, within the Electronic Security Perimeter (ESP) will be elevated to the level of the highest impact BES Cyber System present in the ESP. The commenter recommended that this concept be included in section 5 background of every standard, not just in CIP-005-5 guidance. The SDT considered whether to include this in the background in each standard, but determined that it was most appropriate to make clarifying changes to the Guidelines and Technical Basis section in CIP-005-5.

Background Section

One commenter suggested that to ensure consistency between the standard and the list of "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" to update this section to reflect the same definition as used in this list. In response, these do not change or modify the definitions, but provide further background and guidance information.

There was a comment in the Guidelines and Technical Basis section that stated that an ESP is required around networks even if standalone regardless of impact classification. The commenter ask the SDT to confirm the Requirement in CIP-005-5 do not imply a list of Low Impact assets is needed. In response, the SDT has added the word 'applicable' before BES Cyber Systems in the guidelines to clarify this.

A question was raised regarding the scenario where a network switch may be divided into multiple ESPs and has one port outside the ESP that provides no routing between VLANs. Furthermore, the commenter questioned the following regarding Requirement R1.5: "does two distinct machines need to be utilized, one as a fire, and one as intrusion prevention or can it be done via one device and when the EAP is segmented into multiple network where one LAN is critical and one is non-critical; and does an IDS need to be on each network segment monitoring inbound/outbound traffic on the segment or just at the EAP monitoring inbound/outbound traffic." In response, the SDT is writing Requirements for the "what's" and leaving the "how's" to the entities to implement in ways that best protect their environments while still meeting the intent of the Requirement. These standards cannot and should not be exactly prescriptive in every possible technical situation. If that were the case, they would be constantly outdated or they would actually increase our risk by presenting a monoculture to adversaries where a vulnerability in one would be the same vulnerability in all. For the VLAN question, the SDT notes that an ESP (a logical border) is required around every network

to which a BES Cyber System is connected and any external connectivity to other networks must be controlled with an Electronic Access Point (EAP). The SDT has chosen to not prescribe precisely what protective functions must reside on what devices or what the standard network architecture must be for the reasons noted above. A method for detecting malicious communication must be present at each EAP for control centers (high and medium impact).

Consideration of Data Diodes

One commenter stated that CIP-005-5 should consider data diodes which possibly would exempt systems only with a data diode connection from "external connectivity" provisions. In response, the SDT notes that the definition of 'External Routable Connectivity' includes the term 'bi-directional' in order to handle data diode situations that physically enforce a uni-directional flow. Therefore systems behind a data diode do not have External Routable Connectivity.

Requirement R1

One commenter asked what the rationale was for standalone networks that have no external connectivity to other networks to must have a defined ESP. The intent is to define the 'Associated Protected Cyber Assets (PCAs)' and the high watermarking concept. In response, in previous versions of the CIP standards, Cyber Assets on the same network (within the same ESP) with a Critical Cyber Asset had to meet the CIP-007-5 Requirements. The definition of an ESP in Version 5 is required to carry this same concept forward, as well as to handle the new issue of what level of protection is required for these Cyber Assets now that we can have multiple impact levels within the same ESP. Therefore, if a BES Cyber System is connected to a routable protocol network, even an isolated network, the ESP (which is simply the 'logical border') must be defined as that also defines the 'Associated Protected Cyber Assets'. All of these Cyber Assets within that ESP then become 'Associated PCAs' of the highest impact level BES Cyber System in the ESP.

A commenter stated that the definition of Electronic Security Perimeter allows the Responsible Entity to serially connect certain Cyber Assets to a communications processor that, in turn, communicates to other Cyber Assets using a routable protocol, and in doing so declare that the Digital Protective Control Devices do not need to reside within the ESP and therefore are not subject to CIP standards. In response, the SDT notes that connectivity is no longer a filter that kicks Cyber Assets out of scope and makes them 'no longer subject to the CIP standards'. Cyber Assets are subject to the CIP standards based on their functionality and resultant potential impact to BES reliability. It is true that certain Requirements, such as CIP-005 Requirement R1, only apply if a BES Cyber System is connected to a routable protocol network, but that is because its main point is to secure what can enter or leave routable protocol networks on which BES Cyber Systems reside. CIP-005-5 is no longer a 'scoping standard' for what is or is not in scope of the CIP standards as a whole as it has been in the past. BES Cyber Systems are in scope of the CIP standards. CIP-005-5 Requirement R1

therefore is now back to a network security Requirement that requires controlling what can enter or leave a routable protocol network.

There was a comment that requested clarification text added to the Guidelines and Technical Basis section for Requirement R1, specifically Requirement Parts 1.3 and 1.5, to remove the operational barriers that may prevent entities from implementation encryption among sites on a BES Cyber System network using either encrypted tunnels or tunnel-less encryption technologies. The commenter provided possible language to be added to CIP-005-5 Requirement Parts 1.3 and 1.5:

> "Some Entities employ encryption as a strong measure for securing communications among discrete physical sites (e.g. data centers and control centers). Encryption (either via encrypted tunnels or group encrypted transport) effectively satisfies the establishment of 'discrete Electronic Security Perimeters' as referenced in Section 4.2.3.2 of each Applicability section. Provided the termination points of the encryption are protected within Physical Security Perimeters, the Requirements for CIP-005-5 R1.3 (inbound & outbound access permissions and deny-by-default) and CIP-005-5 R1.5 (inbound & outbound malicious traffic inspection) may be achieved at central firewall(s) protecting the BES Cyber System network to which the ESPs are connected. For traffic communicating within the encrypted network, the CIP-005-5 R1.3 and CIP-005-5 R1.5 Requirements do not need to be duplicated at the encryption endpoints. This enables effective implementation of encryption, which might not otherwise be operationally feasible if traffic inspection were required inside of the protected network due to the latency and convergence delays that are introduced."

In response, The SDT believes the Requirements as written do not preclude the use of encryption. However, encryption alone does not constitute an ESP or EAP. For example, if malware is introduced via portable media to a BES Cyber System and it tries to communicate outbound to a command and control server to get further instructions or provide remote access to the BES Cyber System, the fact that there is an encrypted tunnel up to the next higher level site does not provide an EAP where the communications are inspected to determine whether they should be allowed or not. If an entity wishes to state that a wide area network of sites are within one ESP, regardless of encryption, then all Cyber Assets (which includes, e.g., all communication or networking equipment) within that very large ESP become associated PCAs and must meet the Requirements of the highest level BES Cyber System in the ESP. The standards do not preclude doing this, but there are implications that Responsible Entities should take into account.

For Requirement Part 1.2, one commenter stated that the definition of External Routable Connectivity does not anticipate a situation where serial protocol may be used over IP connectivity. The commenter provided an example, where communication between two devices may take advantage of the Ethernet ports on the devices, but run serial

protocol between the devices. Furthermore, the commenter stated that by explicitly stating, "routable protocol connection" in the definition and focusing an auditor's attention on the connection, the auditor may see the Ethernet port being used and determine noncompliance. Lastly, the commenter recommended deleting the word "connection" at the end of the definition of External Routable Connectivity. In response, the SDT disagrees. The definition is based on the type of protocol, not the transport used. Ethernet is not a routable protocol; it is a transport medium with no concept of network level addressing. It should not be assumed that transport determines protocol as routable protocols can be carried on serial lines and non-routable protocols can be carried on Ethernet. It is not a matter of transport but the protocol.

There was one suggestion in Requirement Part 1.3 that the term "permissions" can be substituted with the term "controls" to align the term with the language in the measure. In the measure, the SDT uses "access control list" as an example, and the SDT has not made a change to the Requirement language, as the use of "permissions" stems from prior versions of the CIP Cyber Security Standards. The SDT believes that the term is well-understood in this context.

One commenter had a concern with the phrase "outbound access permission" in Requirement Part 1.3 which calls for requiring inbound and outbound access permission, including the reason for granting access and denying all other access by default. The commenter furthered stated that target threat vectors to the BES Cyber Systems would be inbound to those networks and those attempts inbound into the networks need to be monitored and controlled, and that while there is the possibility that could be malicious code internal to these networks communicating, that tracking all outbound communication from one trusted network to another trusted network would more than double the monitoring that is required. In addition, the commenter stated that the CIP standards have other controls to help monitor and detect the malicious code internal to the networks. In response, the SDT does not think that having an outbound rule in an EAP that allows communication from all hosts on one internal network to all hosts on another internal network is burdensome. The benefit received of being alerted to BES Cyber Systems trying to suddenly communicate with unknown networks or hosts we believe outweighs the burden of such rules. The SDT is not prescribing the level of granularity of these rules. The intent is just that EAPs function as EAPs and don't have rule sets that allow a BES Cyber System to talk to any device in existence. The Requirement is in essence "you shall not blindly trust all hosts inside the ESP to talk to any device on earth". It is up to the entity how granular they control what the hosts inside the ESP can talk to. Some may go extremely granular and specify exactly what host can talk to what host over what port; some, due to the frequency of change or other reasons, may limit it to anything on this network can talk to anything on these other internal networks. Both are compliant. But BES Cyber Systems should probably not be able to communicate directly with all home PC's on the cable company's consumer broadband network or to any machine in unfriendly nations.

One commenter stated that Requirement Part 1.5 needed to include an explicit Requirement for real-time monitoring and/or alerting upon detection of known or suspected malicious communication. The SDT notes that monitoring and alerting is addressed in CIP-007-5, which also includes Electronic Access Control or Monitoring Systems (EACMS) (CIP-007-5, Requirement R4).

With regards to Requirement R1.5, one commenter proposed the following language: "Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. ESP-to-ESP communications within a discrete BES Cyber System shall be excluded." As an example, the communication links between a primary transmission control center and its backup control center shall be excluded. The SDT disagrees. If malicious code is trying to replicate itself from a primary control center to the backup Control Center, then this Requirement should be in place. Having both the primary and backup Control Centers compromised defeats the purpose. If the primary system is compromised via malware or remote control Trojans to the point that its integrity is gone and the entity needs to fail over to the backup while the primary is rebuilt, the backup needs this protection from the malware on the primary system. If the malware walked into the primary system via portable media or other means, an Intrusion Detection System (IDS)/ Intrusion Protection System (IPS) type system may save the backup system from compromise as well.

Another comment regarding Requirement Part 1.5 states that the Requirement is still geared towards implementing an IDS/IPS and that an IDS would not provide the additional protection for an ESP if a firewall failed. Also, the commenter noted that an IDS or IPS would provide no protection against an insider threat. The commenter closed by stating that “malicious” activity cannot be determined strictly by watching for an activity and that traffic to an ESP which is malicious may in fact appear to be normal. The qualification of “malicious” vs. “normal” requires knowing an actor’s intent, which cannot always be gleaned from log entries, traffic patterns or signatures. In response, the SDT has invested many hours in these very discussions and has arrived at the current Requirement. The Order makes it clear that the alternate control is also not simply another firewall. Having two firewalls in sequence would provide no value as the rule sets would be identical. The solution the SDT arrived at for an alternate control at an EAP was to detect malicious traffic (usually implemented in today’s technology via IDS/IPS as noted, but not prescribed). This would allow that if the firewall was misconfigured (e.g. an admin puts in a temporary any/any/all rule for troubleshooting and forgets to remove it after testing) then at least there would be this alternate control looking for malicious traffic and providing some means of protection which the SDT believes is the intent of the Order. As to the issue with “malicious” implying knowledge of an

actor's intent, the SDT has responded to this in previous drafts by inserting the words "known or suspected" to clarify that it is only malicious traffic that is previously known or suspected to be malicious.

Relating to requiring IDS and IPS to have firewalls, one commenter stated that it may be onerous compared to the benefit received. In response, the SDT disagrees. The SDT has already scoped this Requirement to the highest impact BES Cyber Systems which should be subject to the more stringent Requirements. The SDT believes that the benefit received from detecting malicious communications into and out of control centers far outweighs the burden.

One commenter asked for SDT clarification related to the ESP, External Routable Connectivity, and whether serially connected Cyber Assets are within scope for Requirements applicable to BES Cyber Systems with External Routable Connectivity. The SDT confirms that all BES Cyber Assets are in scope of all the CIP Version 5 standards. However, for certain Requirements, the type of connectivity limits applicability. EAPs for example, are only required around routable protocol networks to control what can get into and out of these networks. There is no EAP for a serial connection if there is no routable protocol running over it. Note that it is protocol based, not transport based. Routable protocols can run over serial transports. The same holds true for ERC – it is routable protocol based.

Requirement R1 VSLs

There was a comment that the language in the VSL should match the same language and logic as in Requirement R2. An example was provided that, the Responsible Entity should have a low VSL for not having a sub-part in its documented process, medium for not implementing one of the applicable items, high for not implementing two applicable items and severe for not implementing three applicable items, and thus, would result in a more consistent application throughout the standard. The SDT notes that it modified the VSLs for Requirement R1 in response to comments from draft 2 because of the difficulties and impracticalities of determining the measurements for graduated VSLs for Requirement R1.

Requirement R2

There was a clarification request for Requirment Part 2.2 with regards to allowing that encryption may be terminated at a firewall that protects an Intermediate Device in additoin to the Intermediate Device itself. The SDT believes that the definition of Intermediate Device provides sufficient flexibility in implementation to allow for what the commenter had requested. Additional references regarding the Intermedate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested clarification of how CIP-007-5 Requirement Part 5.1 and CIP-005-5 Requirement Part 2.3 differ. CIP-007-5 Requirement Part 5.1 refers to all user authentication; whereas CIP-005-5 Requirement Part 2 only refers to remote access.

There was a request that "where technically feasible" be added to Requirement Parts 2.2 and 2.3. The language "where technically feasible" is included in the overarching Requirement R2 to recognize that this applies to all of the Requirement Parts contained in Requirement R2, not just Requirement Parts 2.2 and 2.3.

Several commenters stated that CIP-005-5 Requirement Part 2.1 be modified to address situations where the Intermediate Device can be locally accessed (a local administrator, for example) inside the PSP. The SDT believes that, as currently written, the Requirement provides the level of protection necessary in that the Intermediate Device cannot be within an ESP and thus provides the necessary protection of the Cyber Assets within the ESP. The remaining controls for the Intermediate Device(s) provide a defense-in-depth proteciton of those systems. Additional references regarding the Intermedate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter considered that CIP-005-5 Requirement Part 2.2 does not achieve the intention, which is to have traffic inspected by the IDS in an unencrypted state. The SDT notes that, as written, the Requirement and definition of Intermediate Device, collectively; provide sufficient flexibility in implementation to allow for what the commenter has noted. It is at the entity's discretion to design their Interactive Remote Access infrastructure and monitoring to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. Please see http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested clarification of CIP-005-5 Requirement Part 2.1 regarding the protections to be afforded to an "Intermediate Device". Per the definitions of Intermediate Device and Electronic Access Control or Monitoring Systems, these devices are subject to the protection of EACMS.

There was a request for clarification of CIP-005-5 Requirement Part 2.2 as to the reasonableness to include traffic between the "Intermediate Device " and device(s) within the ESP to be in scope of CIP, as it traverses an EAP. Many instances of Interactive Remote Access originate from systems that are not within a trusted network or across the

Internet. The encryption is required to terminate before going into the ESP through an EAP. It is at the entity's discretion to design their Interactive Remote Access infrastructure and monitoring to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested that CIP-005-5 Requirement Part 2.2 be modified as "Interactive Remote Access sessions must utilize encryption to an Intermediate Device." The SDT believes that, as written, the Requirement language achieves the same concept and result.

A recommendation was made that CIP-005-5 Requirement Part 2.3 is modified as "Interactive Remote Access sessions must utilize multifactor authentication to an Intermediate Device." The SDT considered authentication to be necessary for the session, not for each device. The user may not actually log into each Intermediate Device itself.

A request for clarification was made of CIP-005-5 Requirement Part 2.2 regarding whether the "Intermediate Device" is expected to provide the encryption or if two devices are envisioned for compliance. The SDT believes that, as written, Requirement and definition of Intermediate Device, collectively, provide sufficient flexibility in implementation to allow for what the commenters have noted. It is at the entity's discretion to design their Interactive Remote Access infrastructure to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested clarification of CIP-005-5 Requirement Part 2.3 on whether the multi-factor authentication is required for the Intermediate Device, for access to the EAP or to the individual Applicable Systems. The commenter suggested the language to read "Require multi-factor authentication for initiating all Interactive Remote Access Sessions." The SDT considered authentication to be necessary for the session, not for each device. The user may not actually log into each Intermediate Device itself.

One commenter requested clarification of CIP-005-5 Requirement Part 2.1 on whether VPN is an acceptable form of remote access. It is at the entity's discretion to design their Interactive Remote Access infrastructure to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There

are case examples showing differing implementations. Please see http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

CIP-006-5

General

There were comments that CIP-006-5 does not require an entity to define a Physical Security Perimeter (PSP) and wonders if entities must assume that it is required. In response, the SDT notes that access points to the PSP must be controlled, which by definition, requires the PSP. It is not necessary to have an additional Requirement stating the existence of a PSP.

Background Section

One commenter stated that the background section includes a definition/description of "Medium Impact BES Cyber Systems with External Routable Connectivity," that notes an exclusion in the following sentence: "This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity." When this definition/description of Cyber Systems is used for the applicability in Requirements such as CIP-006-5 Requirement Parts 1.2, 1.4, and 1.5, it is used with the added inclusion of "and their associated...PCA." It appears the inclusive "and associated PCAs" statements in the Requirements negate the exclusion statement from the "Background," and makes the intended applicability of such physical security Requirements to specific Cyber Assets unclear for Cyber Assets without direct external connectivity which reside in the same ESP as Cyber Assets with direct external connectivity. In response, the exclusion in the background section states that it only applies to those Cyber Assets which are part of the BES Cyber System and not PCAs.

Requirement R1

One commenter stated that the deficiency correction language should not be added to CIP-006-5 Requirement R1 because it is a binary Requirement to either have a plan or not. The SDT notes that while the possession of a plan is binary, the implementation is not. Entities must document a plan with all of the applicable table parts and implement the plan at applicable BES Cyber Systems.

One commenter noted that the term "BES Cyber Systems without External Routable Connectivity" should be just "BES Cyber Systems". The SDT notes that "without External Routable Connectivity" is used to distinguish lesser obligations than those applying to "BES Cyber Systems WITH External Routable Connectivity".

Several commenters stated that CIP-006-5 Requirement R1 does not answer the question of how big an opening needs to be before it is considered an access point. In response, the SDT does not agree this question needs to be answered in a

standard's Requirement. This is an implementation-specific question. An entity may choose 96 square inches as its general measure, but that should not be the Requirement. Specifying exactly the qualifications of an access point would go beyond just the 96 square inch Requirement and likely cause significantly more confusion than currently exists.

One commenter did not agree Requirement Part 1.3 is responsive to the directive in FERC Order No. 706, Paragraph 573 to provide layered and complementary security procedures. In response, the SDT notes that in paragraph 575, the Commission specifically states it was not the intent to create an inflexible rule of redundant access control. The proposed Requirement meets the objective of having multiple physical access control measures. The Cyber Asset independence of these measures is not material to meeting the directive.

More than one commenter argued that Requirement Part 1.3 presents technical challenges without any additional security benefit. They request NERC to provide compliance feedback to industry demonstrating that "one or more" physical access methods have proven ineffective. In response, the SDT is addressing the directive in FERC Order No. 706, Paragraph 572. The SDT believes the proposed wording provides the most security benefit to the industry while still meeting the FERC directive.

One commenter suggested that for Requirement Parts 1.5 and 1.7 to remove the 15 minute maximum timeframe limit for issuing an alert. In response, the SDT notes that for physical security breaches, the threat is automatically severe and immediate and the 15 minute timeframe is necessary to provide a minimum expectation for issuing an alert.

One commenter proposed the words "of the unauthorized access" should be added to the end of Requirement Parts 1.5 and 1.7, but this would be redundant since detection is already qualified singularly in the Requirement Part.

There was a request for clarification if monitoring is needed on PACS inside a PSP according to part 1.7. In reviewing the possibility of combining Requirement Parts 1.5 and 1.7, the SDT found that monitoring and alerting Requirements applying to PACs could be interpreted to mean those inside a PSP. To clarify, the SDT notes that entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

One commenter stated that in Requirement Parts 1.5 and 1.7, BES Cyber Security Incident Response Plan is not a defined term and should not be capitalized. The SDT agrees and has made this change. Furthermore, the commenter noted that unauthorized physical access should not automatically trigger the incident response plan because the physical security

team and incident response team are often separate groups, and a single instance of a detection of unauthorized physical access is not necessarily a Cyber Security Incident. The SDT notes that an attempt to compromise the PSP is by definition a Cyber Security Incident, and the organization of physical security and incident response teams should not preclude the Requirement to identify the Cyber Security Incident. The physical security team's response to unauthorized physical access could be part of the organization's incident response plan.

Several commenters stated that Requirement Part 1.7 should be modified to require response within 15 minutes of the detection rather than the actual incident, consistent with Requirement Part 1.5. The SDT agrees and has made the clarification.

One commenter proposed that Requirement Parts 1.5 and 1.7 be combined because they use similar wording, but the SDT believes entities benefit by emphasizing the applicability to PACS outside of the PSP.

There was a comment that stated that Requirement Parts 1.6 and 1.7 should include badge readers outside of the PSP and access cannot be controlled as specified. In response, these Requirement Parts are separated because they must be monitored differently than those Cyber Assets inside a PSP. The SDT also notes that badge readers, by themselves are not necessarily considered PACS if they do not control the controlling, logging or alerting of access.

One commenter noted that a responsible entity needs to monitor each PACS system for unauthorized physical access to a PACS. However, there is no Requirement that the PACS be contained within a PSP. Therefore, a question was raised as to how does one control physical access to the PACS? In response, the SDT notes that PACS must control access according to Requirement Part 1.1, which is not the same level as Requirement Parts 1.2 through 1.5, but some form of access control must still exist for the entity.

Several commenters noted that Requirement Part 1.7 requires coordination with the incident response team, but CIP-008-5 does not apply to PACS. In response, the incident response plan does not apply to individual Cyber Assets, but compromise of a PSP and associated PACS is by definition a Cyber Security Incident affecting a BES Cyber System.

One commenter requested clarification on whether the issuance of an alert according to Requirement Parts 1.5 and 1.7 is automated, manual, or by choice. The SDT clarifies this is by choice of the entity.

There was a suggestion that there is a discrepancy between the change description stating PACS does not need to be inside a PSP and Requirement Parts 1.5 and 1.7 stating obligations for monitoring and alerting for unauthorized access to PACS. In response, Requirement Parts 1.2 through 1.5 applies to the BES Cyber System. PACS have a less stringent obligation in Requirement Part 1.1 to have a plan for restricting unauthorized access, but this is not the same obligation as having a PSP. The SDT has clarified the change rationale for Requirement Part 1.1.

One commenter stated that Requirement Part 1.8 should add "initial" before entry to align with the visitor control program. In response, the situation allowed for in the visitor control program is to avoid an escort continually signing in a visitor needing to perform a maintenance activity. This is not the same concern for authorized personnel who typically badge in each time without the overhead of an escort.

One commenter stated that Requirement Part 1.9 should be moved to data retention. In response, the retention of these logs serves the reliability objective of having access logs to support incident identification and response.

Requirement R2

There was a comment that the CIP Exceptional Circumstances should be removed since it applies globally at a policy level. In response, the CIP Exceptional Circumstance provision is controlled at a policy level but does not apply globally to all Requirements in the standard. The standards specify which Requirements the exception may apply to as a response to the FERC Order No. 706 beginning with paragraph 372, which directs additional guidance on policy exceptions.

Several comments stated that the Requirement could allow a visitor to go a long span of time without signing out. In response, the SDT notes the scenario of brief exit/entry intervals provided in comments is the purpose for allowing this provision. Specifying what timeframe constitutes the necessity of an exit sign-out goes beyond the security benefit provided by this Requirement Part.

Several commenters noted that the measure in Requirement Part 2.1 does not match the Requirement because the evidence does not demonstrate continuous access but discrete points in time. In response, the Requirement to have a program that provides continuous escorted visitor access can be measured by the program document. Evidence of compliance with the procedure requires discrete sampling to provide assurance in the implementation of the program.

One comment was that Requirement Part 2.2 would require manual or automated logging of entry and exit from the physical security perimeter and the Requirement for egress has not been explicitly defined as a Requirement. In response, egress logging has been required since CIP-006-3.

There was a comment that Requirement Part 2.3 should be moved to data retention. In response, R2.3 was not included as an evidentiary requirement. The SDT notes that the retention of these logs serves the reliability objective of having access logs to support incident identification and response.

Requirement R3

One commenter stated that Requirement R3 should have the language allowing an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R3 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One comment was that the 24 month interval in Requirement Part 3.1 is excessive for a normally occupied control center. In response, a normally occupied control center would also receive a significant amount of testing in the operation of access control. The objective this Requirement primarily addresses field assets where access is not tested as frequently, and the timeframe is appropriate for these assets.

Guidelines and Technical Basis

Several commenters recommended modifying the section dealing with alarms to be from “immediately after” an incident to “within 15 minutes.” This better aligns with the Requirement and the SDT agrees.

CIP-007-5

General Comments

One commenter requested guidance on how to comply with CIP-007-5 Requirements on Medium BES Cyber Systems serially connected devices with regards to patching, anti-virus, etc. on a large number of programmable protective relays; and also why other measures implemented for substation assets, such as physical protection, are not adequate. In response, the SDT notes that BES Cyber Assets by definition can have an impact on BES reliability and therefore require basic cyber security protections offered by CIP-007-5 regardless of their connectivity. For patch management, the intent is that entities know about the security patches that are available for their BES Cyber Assets, what vulnerabilities they represent, and mitigate those vulnerabilities. If a security patch for a device is only exploitable over a routable protocol connection and the device is only attached serially with non-routable protocols, then that patch would be documented as not applicable. The anti-virus Requirements and guidance already mention that the entity is to document and implement how they protect against the introduction of malicious code to the BES Cyber System. For some of the devices in the example, the entity may document that there is no method to introduce malicious code.

Effective Dates

One commenter raised a concern that the effective date of the order providing applicable regulatory approval, and Requirement Part 5.2 shall become effective 12 months later, as to provide entities more time to identify and inventory all enabled default or other generic account types. In response, it is the intent of the SDT that the entity has the accounts inventoried on the effective date, not one year later. That is why there is a two to three year implementation period so that all these prerequisite activities have sufficient time to be completed so that the entity is fully compliant on the effective date. The Requirements that require periodic reviews may have their first performance take place after the effective date, but that is outlined in the implementation plan.

Requirement R1

One comment stated that a new term of “Control Center Environment” was introduced in this standard and it could potentially have a different meaning than “Control Center”. The commenter requested clarification, and in response, the SDT agrees and has changed the term to “Control Center.”

For CIP-007-5 Requirement Part 1.2, several questions were asked about the phrase, “Protect against the use of unnecessary physical input/output (I/O) ports used for network connectivity, console commands, or removable media.” Introduction of physical port protection is “assumed” to refer to logical ports only. First, a question was raised about

strong physical access controls to BES Cyber System be a compensating control here. Second, will having the BES cyber systems in locked cabinets suffice? The Requirement is not clear if the protection has to be on the individual devices. The measures indicate signage as a potential control however this would not satisfy the Requirement the way the Requirement is written. For CIP-007-5 Requirement Part 1.2, the commenter sought clarification regarding physical I/O ports that are externally accessible. For example, most servers have PCI slots, CPU slots, memory slots, etc, which are physical I/O ports. As the standard is currently written, it would seem organizations need to disable these ports. Additionally, the language "console commands" is too ambiguous. In response, the SDT notes that many of these issues are addressed in the included guidance. FERC has stated that the PSP does not meet the intent of their Order. The SDT agrees with the 'console commands' comment and has added additional guidance to address it.

For CIP-007-5 Requirement Part 1.1, several comments were made about the phrase, ""If a device has no provision for disabling or restricting logical ports on the device, then those ports that are open are deemed needed." The Requirement does not provide any provisions for limiting access to those ports or services that cannot be disabled. The Requirement's measures ask for host-based protective measures. For those devices that are not capable of providing localized protective measures, such as relays, there is a question as to how this Requirement would be met. Previously, when a port or service could not be disabled, a TFE would require mitigation of the potential vulnerability. Under CIP-007-5, if the entity leaves these ports and services open they are in compliance but there is a question of whether the vulnerability of the device still remains. In response, the SDT notes that the Requirement does provide provision for those ports and services that cannot be disabled which is the phrase in question. If a device has no provision for disabling or restricting the ports, they are deemed "needed" and the Requirement only requires "unneeded" ports to be disabled. The intent is to not require TFEs for devices where the device does not allow for the Requirement to be met. The Requirements in CIP-005-5 for limiting inbound and outbound communications at the ESP is a mitigating factor for devices like this that do not allow for their "unneeded" ports to be disabled.

Requirement R2

There was one comment that stated the rationale specified a 30 day time frame while the Requirement states 35 days. The commenter requested that the rationale section be revised for consistency with the Requirement language. In response, the SDT agrees and has changed the rationale to 35 days to agree with the Requirement.

One commenter suggested adding "with External Routable Connectivity" to the Medium Impact applicability for the patch management Requirements within Requirement Parts 2.1 through 2.4. As justification, the commenter stated that they understand the comments of the SDT; however, the commenter believes that a combination of no external routable

connectivity, frequency of access to medium impact facilities, and policies reduces the risks to those facilities from the insider that would introduce threats ("thumb drives, laptops, smart phones") into the environment to an acceptable level. While devices with no external connectivity may have some physical access risks associated with the use of thumb drives, laptops, etc., the fact that they are isolated from other BES devices must be considered when addressing appropriate protections. The lack of external connectivity reduces the risks to that isolated device; therefore, the risk to the BES is minimal. Additionally, physical security is adequate mitigation from the external threats as once physical security is breached; there are other immediate and evident concerns that do not involve BES Cyber Systems. Alternatively, a request was made that the timeframes for Requirement Parts 2.2 and 2.3 be revised to 90 days for Medium Impact BES Cyber Systems. In response, while routable protocol connectivity is a way that systems can be compromised, it is not the only way and in many examples today is not the primary way. Insider threats (intentional and unintentional, from both employees and non-employees, from both portable media and support laptops) are means in which systems are compromised today. Therefore the intent of this Requirement is to remain aware of the vulnerabilities in the BES Cyber Systems through the security patches that are released for them and analyze and mitigate those vulnerabilities. If a system has no connectivity and a security patch is released that can only be exploited via network connectivity, then that vulnerability is already mitigated and the patch is not applicable. As to the 90 day alternative, the SDT believes that a timely analysis and plan are necessary due to the nature of the environment we are in where 'Patch Tuesday' is immediately followed by 'Exploit Wednesday' as attackers quickly reverse engineer released security patches to create and release exploit code. The SDT has not put a maximum timeframe on implementation due to numerous reliability concerns, but the analysis and mitigation planning needs to occur in a timely fashion.

There was a comment that Requirement Part 2.1 requires the Responsible Entity to identify a source or sources that the entity will track for the release of cyber security patches. Furthermore, the commenter stated, *"the corresponding guidance suggests that the third-party SCADA system vendor is an appropriate source for patch availability notification. The ability of a Responsible Entity to wait until a SCADA system vendor "certifies" a patch before requiring the Responsible Entity to begin the assessment and follow-on patching process introduces unnecessary risk to the BES. There is a significant difference between assessing a patch for applicability and assessing a patch for installability. An applicable patch may be found to be incompatible with the third-party vendor's systems, would not be certified, and should not be installed. That does not mean the vulnerability being addressed by the patch should not be mitigated, rather it is incumbent upon the Responsible Entity to protect its systems in a timely manner. The Responsible Entity needs to select a patch availability source that is timely, including the original patch provider and well recognized general information providers like US-CERT, SANS @Risk, and nCircle. There is no harm in then waiting for the SCADA vendor to certify the patch before installing it, but the Responsible Entity is at least aware of the vulnerability, can assess the risk, and take*

appropriate interim action." In response, the SDT agrees with the concept; however, the SDT does not find it appropriate to prescribe in regulation certain 'timely' sources, including private firms, that must be used. Patch monitoring services can come and go. The SDT also believes that it should not use undefined terms such as 'timely' in a mandatory Requirement, nor should it define 'timely' as it refers to the seemingly unlimited number of patch sources that will exist with the significantly expanded scope of Version 5. The SDT believes that the reliability of the BES will be better served by mandating that all vulnerabilities in all applicable BES Cyber Systems be known and analyzed by all entities than by trying to micro-manage what must occur with each system, patch, and vendor through a one-size-fits-all process. As stated in the guidance, patching systems can cause more risk to BES reliability than having a non-patched system in a given situation and the Responsible Entity, not the SDT, is in the best place to weigh these risks and develop an appropriate plan.

For CIP-007-5 Requirement 2, part 2.1, a comment was made that the patch management process for substation or plant control systems could include security patches for Cyber Assets such as panel meters, relays, controllers, Programmable Logical Control (PLCs), and other electronic devices that are part of the BES Cyber System and do not have network connectivity. In response, the SDT agrees that any Cyber Asset that meets the definition of BES Cyber Asset is included in the CIP-007-5 patch management Requirement regardless of connectivity and that is the intent. While routable protocol connectivity is a way that systems can be compromised, it is not the only way and in many examples today is not the primary way. Insider threats (intentional and unintentional, from both employees and non-employees, from both portable media and support laptops) are means by which systems are compromised today. Therefore the intent of this Requirement is to remain aware of the vulnerabilities in the BES Cyber Systems through the security patches that are released for them and analyze and mitigate those vulnerabilities. If a system has no connectivity and a security patch is released that can only be exploited via network connectivity, then that vulnerability is already mitigated and the patch is not applicable.

One commenter requested a definition in Requirement Part 2.1 for the phrase "applicable asset," and also suggested that the phrase "Applicable Cyber Asset" should be called "Applicable System" to align with wording in the column "Applicable Systems". In response, the SDT notes that individual BES Cyber Assets have patches, not systems of Cyber Assets. A system is a logical grouping of one or more BES Cyber Assets. While the applicability is at the system level, the Requirement is to perform patch management on all of the applicable BES Cyber Assets within those applicable systems.

There was a comment made on the change from 30 days to 35 days within Requirement Part 2.2. The comment was that this change allows utilities to manage patches monthly while coinciding with vendor releases, all without running into

issues of the Requirement being less than a full month. However, the commenter stated that this should be extended to 40 days to accommodate time to review the vendor releases, and that the additional five days on top of the existing 35 days will ensure that those utilities with patch management programs are not penalized due to variations in patch release dates from month to month. In response, the intent is for a process that approximates "monthly" and the SDT has already added in at least a four period to account for holidays, weekends, and other factors. The SDT does not agree that it needs further extension. Timely analysis of security patches is the goal.

Within Requirement Parts 2.2 and 2.3, one commenter requested clarification of the use of term "mitigation plan" and how it would provide value. To clarify Requirement Part 2.2 the commenter suggested mentioning that the mitigation plan is intended as an internal document and not submitted to the RE. In response, the SDT agrees and that these plans are internal documents and not submitted to the RE. In previous drafts, these were called 'remediation plans' and the SDT received comments that this term was used for what was submitted to Regional Entities in response to violations of the standard, so the SDT changed the term to 'mitigation plan' to avoid that confusion. The SDT has added this clarification to the guidance.

There was a comment with regard to CIP-007-5 Requirement Part 2.3 that reads, "Available actions to entities should include: 1) Apply the patches 2) Develop dated implementation plan 3) Create/revise existing mitigation plan". In many cases, patches will be applied, but outside of a 35 day period to accommodate outage schedules for optimizing reliability and availability of systems. In many cases, when an applicable patch is provided by a vendor, there may be no additional mitigation implemented during the time from patch availability until installation. Requiring entities to "create a dated mitigation plan or revise an existing mitigation plan will result in a paperwork exercise and yield no reliability or security benefits for the affected cyber assets. Adding an option to "Develop dated implementation plan" without requiring a mitigation plan to be created/modified permits entities to apply resources to application of patches and optimizing reliability." In response, the SDT notes that the 'dated mitigation plan' could simply consist of the date the entity plans to implement the security patch if beyond the initial 35 day period; therefore it is not simply a paperwork exercise that provides no reliability benefit. The intent of the Requirement is to mitigate the applicable vulnerabilities either through the installation of the patch or by some other means. Implementation of the patch is mitigation and having a record of the entity's plan to implement the patch is not seen as unnecessary paperwork.

There was a comment that Requirement Part 2.3 requires the Responsible Entity to either install the patch within 35 calendar days or simply create or update a mitigation plan. Furthermore, the commenter stated "there are no boundaries of what is acceptable in a mitigation plan, no expectation of justifying the decision, and no Requirement for

the CIP Senior Manager approval, thus allowing an entity to completely avoid the Requirement to patch a critical system by creating an illogical plan with unreasonable milestone dates. The need to wait for a scheduled outage at a field asset is well understood. Allowing an entity to determine patches will only be installed when the control center server is replaced (typically every four years), as has been seen during a CIP audit, is unreasonable and poses significant risk to the reliability of the BES. This Requirement does not require compensating measures appropriate to the vulnerability to be put into place until the patch is installed, thus furthering the potential risk. In effect, the provisions of this Requirement have the potential of creating a paper exercise with little value, with an expectation that the CIP auditor simply accept the documented plan without comment. (3) Requirement Part 2.4 furthers the inaction of the Responsible Entity by requiring the entity to follow the potentially illogical plan that the entity designed to avoid having to patch in the first place. As long as an extension of the plan is not required, there is still no CIP Senior Manager or delegate approval required." In response, the SDT believes that the reliability of the BES will be better served by mandating that all vulnerabilities in all applicable BES Cyber Systems be known and analyzed by all entities than by trying to micro-manage what must occur with each system, patch, and vendor through a one-size-fits-all process. As stated in the guidance, patching systems can cause more risk to BES reliability than having a non-patched system in a given situation and the Responsible Entity, not the SDT, is in the best place to weigh these risks and develop an appropriate plan. The SDT has no way to write a mandatory Requirement for a "logical" plan.

One commenter believes that the language in Requirement Part 2.4 be aligned with the language in Requirement Part 2.3. The commenter suggests that either both or neither should specify the approval Requirement of the CIP Senior Manager of delegate. The commenter recommends that the language of "…timeframe specified in Requirement Part 2.3 is approved" be added. In response, the SDT notes the CIP Senior Manager approval was added to Requirement Part 2.4 specifically to handle situations where entities might repeatedly extend their documented timeframe with no management oversight. The intent was not to have management approval of every patch in normal day-to-day processes. Entities are free to do so, but it was not the SDT's intent to make that a mandatory Requirement. Management approval of every patch on every BES Cyber Asset would tend to become a "rubber stamp" with no meaning. The SDT's intent was to have approval of exceptions so that if someone were simply moving deadlines to avoid complying with the intent of the Requirement it would be subject to management oversight.

Requirement R3

There was a comment that within Requirement Part 3.1 to consider adding the phrase "per device capability" to the beginning of the Requirement, or otherwise, if a deter posture is selected, it may be potentially in conflict with other

Requirements. In response, the Requirement is written at the system level in order to handle the device-specific issues. The SDT believes the included guidance also provides suggestions on how to handle device abilities.

With regard to CIP-007-5 Requirement 3, parts 3.1, 3.2, and 3.3, there was a comment that these three Requirement Parts do not have any timeline for action. A question was raised if an auditor will audit when the activity occurred and audit only that a process is created and executed per the registered entities process or procedure. In response, the answer to the question is yes. Malware protection is an inexact art as we are protecting against an intelligent and always changing adversary. Malware of today is quite different than malware of just a few years ago. The intent is for entities to think about the malware problem, document what they are doing about it for each BES Cyber System, and then do it. Prescribing certain technologies/tools/timeframes is not helpful in this rapidly changing area and tends to bog the industry and the regulator down in paperwork (such as TFEs) when agility in this area is required in order to protect BES reliability.

Within Requirement Part 3.2, one commenter stated that the word 'identified' is ambiguous and inconsistent with other malicious code phrases, and the commenter suggested changing the language to 'detected'. The SDT agrees with this clarification and has made the suggested change as this is how the measures and guidance were written as well.

One comment was related to the applicability section of Requirement Part 3.2. A suggestion was provided to revise this section to apply to Medium Impact assets with external routable protocol to read: "Medium Impact BES Cyber Systems with external routable protocol and their associated". In response, the SDT's intent is for the basic security protections, including malware prevention, to be applied to all BES Cyber Systems not just those with External Routable Connectivity. BES Reliability can be threatened on isolated networks of BES Cyber Systems through the introduction of malware through portable media or laptops used for support.

One commenter requested clarification on Requirement Part 3.3 which requires the anti-malware updating process to address testing of the signature or pattern file. In support of this request, the commenter stated that a number of registered entities have taken the position in the past that they address this aspect of the existing CIP Version 3 Requirement by relying upon the vendor to test before release. In response, the Requirement is taken verbatim from previous industry and FERC approved versions of the CIP standards. If the entity is obtaining tested signature updates from their control system vendor for a turnkey product, then that is compliant. The SDT does not think more prescription as to where the testing must occur is needed.

There was one comment raised that use of the term 'deter' is ambiguous and the commenter suggested replacing this language in Requirement Part 3.2. The commenter suggested replacing the language to read: "Configure the measures implemented in Requirement Part 3.1 such that it blocks or prevents access to files with potentially harmful code." This recommendation was based on the assumption that the recommendation for removal of the term "deter" is accepted in Requirement Part 3.1. In response, the SDT has purposefully added the word 'deter' so that entities are not in immediate violation of the Requirement should zero day malicious code enter the environment. There are no 100% preventions, so the SDT has added this verb to allow for that. Antivirus software tools today do deter, but do not 100% prevent.

Requirement R4

One commenter requested clarification around the last two sentences of the guidance section. The commenter also stated that currently, an entity that neglects to enable logging would be in violation. Per the Background section, a sole instance of deficiency is not grounds for a violation so long as it is adequately identified, assessed, and corrected. The statements in the guidelines seem to be relics of a previous draft which conflict with the new approach. In response, the SDT agrees and has rewritten the guidance to properly align with the Requirement.

One comment read that CIP-007-5 Requirement R4 for security event monitoring does not state any Requirements as to when the security events, particularly in Requirement Parts 4.1 (log events) and 4.2 (event alerts) are to reviewed, escalated, and mitigated. A question followed that asked if there are any Requirements for immediate action from the IT security personnel for detected failed access attempts, failed login attempts, or specific event alerts. In response, no, there are no prescriptive timeframes for response to alerts. The Requirement is to generate an alert for security events. Alerting someone to a condition is one thing, responding to the condition is dependent upon numerous variables that cannot be prescribed.

A recommendation was made to revise this Requirement to include the sentence from the guidance section, "that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment." The SDT's intent was not for the Responsible Entity to determine in totality the events to be logged, but that it must log the listed events at a minimum (subject to device capability). The Responsible Entity is free to log events above and beyond these and is encouraged to do so. However, the Responsible Entity cannot ignore the listed events.

As currently written, CIP-007-5 Requirement Part 4.1 would necessitate the logging at every Cyber Asset that is capable when there is not a network at the BES Cyber System. A suggestion was made to rewrite this Requirement to read, "for BES Cyber Systems that have Cyber Assets connected to a network via a routable protocol, log events at the BES Cyber System Level…" In response, the SDT's intent is that if a Cyber Asset has a local log on the device, then it should be utilized. For example, a completely standalone and isolated substation relay should log security events internally if it is capable of such so that if it begins misoperating there is some log to go review on the device to see if/who/when someone has accessed it. The Requirement is not dependent on external connectivity.

In Requirement Part 4.3, one commenter suggested that this is a data retention Requirement and should not be a Requirement of the standard. In response, the SDT's intent is that this is not strictly 'data retention for the purposes of audit' Requirement, but an actual cyber security Requirement to have ready access to the past 90 days of logs for the applicable systems for quick determination of potential cyber causes of reliability-affecting events. Quickly determining whether a BES event could have had a cyber security cause is a reliability-focused Requirement and the primary way to do that is to have ready access to security event logs. Configuring a system to retain the past five minutes of security event logs is of little to no value. This is a separate issue from having evidence for audits that you maintained 90 days of logs throughout the audit period.

Within the Guidelines and Technical Basis section of CIP-007-5, Requirement R4, a question was asked if the following quotation references to NIST are the guiding principles and documentation for the development of the RSAWs and auditing of this Requirement, "Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring." In response, these guidelines are not auditable, only Requirement statements are auditable. These are provided solely for use at the discretion of Responsible Entities, several of whom have asked in previous drafts for further guidance.

One commenter requested clarification on the word "review" with regard to the statement within Requirement Part 4.4 of "Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 days to identify undetected Cyber Security Incidents." The commenter questioned if an automated SIEM technology solution, which monitors real-time, would satisfy the Requirement. In response, the SDT states that the intent, as per FERC Order No. 706, is to manually review the logged events in order to ensure that automated tools such as SIEM systems are tuned appropriately and are not missing security events.

One commenter stated that CIP-007-5, Requirement R4, part 4.1.2 calls out failed access attempts and failed login attempts and is unclear as to why the phrases "failed access attempts" and "failed login attempts" are separated. The

commenter requested clarification on the following two questions: Are “failed access attempts” referring to physical attempts, and are they referring to some other form of electronic access to undermine the login process? In response, the SDT notes that as outlined in the guidance, access attempts primarily occur at EAPs and involve ‘access’ across the ESP. Login attempts primarily occur at the BES Cyber Systems. The monitoring Requirement applies to both situations.

A comment was issued on Requirement Part 4.1.3 that this Requirement of malicious code prevention methods to log is already contained in Requirement Part 3.2. The commenter suggested removing this Requirement. In response, the SDT notes that logging and alerting when malicious code is detected is a separate Requirement from the actual response to the alert and the mitigation of the malicious code on the BES Cyber System. The SDT sees no duplication between these Requirements.

There was a comment that within CIP-007-5 Requirement Parts 4.2 through 4.4 the Requirements and sub Requirements have become less clear than previous CIP standards versions. The commenter stated it was unclear if Requirement Part 4.4 replaces the previous monitoring Requirements in their entirety or if it represents an additional manual sampling action that occurs outside of a primary monitoring process which may be automated. The commenter suggested to consider modifying the aforementioned Requirements to make it clear to registered entities which logging is required, how logs should be monitored, and what actions are required in the event of an interruption in logging. In response, the SDT notes that Requirement Part 4.4, as noted in the Rationale and Change Justification, is in response to FERC Order No. 706 and the Directive to require a manual review of logs to insure that automated tools are not missing events. Automated tools are only as good as their rule sets, which require periodic tuning.

One commenter noted that a clarification may be needed for Requirement Part 4.2 as to whether the alert needs to be generated real-time with automatic notification or if the alert can be generated by a long after-the-fact manual review of security event logs. In response, the SDT’s intent is, in general, for a real-time alert, but the SDT did not specify that as a timeframe in the Requirement because, for example, an after-the-fact review or analysis of logs would not require a computer-generated alert.

One commenter stated that Requirement Part 4.2 is a questionable and subjective Requirement as it states that an entity needs to generate alerts for security events that the entity determines necessary. In response, the SDT has set a minimum threshold of alerts that must be generated if the system is capable of it. All other types of alerts vary widely by the type of system in question and should not be prescribed. The alerts that can be generated by a Windows or Unix

server in a data center are quite different than what can be generated by some legacy purpose-built device in a substation.

A request was made to clarify Requirement Part 4.3 as to whether original source logs must be retained or if post-log analysis summaries are sufficient. In response, the SDT states that the language in the Requirement and measure provides the necessary level of clarity.

There were several comments on Requirement Part 4.4 that need to be clarified that the review of a summarization or sampling of logs is not acceptable as the primary means of log analysis and alert generation. The purpose of the manual review is to achieve a level of comfort that the log analysis tool is properly configured and is not missing important security events. A random sample review of logs otherwise runs a significant risk of completely missing security events that pose potential risk to BES reliability. Similarly, another comment for CIP 007-5, R4.4 read, in the Requirements column of the table, the draft language indicates a need to review logs to, "identify undetected Cyber Security Incidents." A question was raised if this is intended to be "identify detected Cyber Security Incidents?" Also for CIP-007-5 Requirement Part 4.4, a recommendation was made to change "undetected" to "potential". In response to the aforementioned comments, the SDT notes the intent is to review logs to insure that any automated tools or processes are tuned so that they are catching all Cyber Security Incidents, therefore the SDT believes that the 'undetected' word is correct. If attempts to breach the security of a BES Cyber System are being missed because the automated tools are not tuned or maintained, then this Requirement's intent is to catch that.

One comment read that in Requirement Part 4.4, to be consistent with other Requirements, that the phrase "15 days" be changed to "15 calendar days." In response, the SDT agrees with this clarification and has made the change.

A recommendation was provided to change the language in Requirement Part 4.2 to read "Detected failed login attempts from part 4.1." In response, the SDTs intent is that alerts be generated when it is detected that event logging has failed.

One commenter raised an issue that in Requirement Part 4.4 the words "summarization" and "sampling" components are too broad. In support of this, the commenter encouraged specificity in all measures. Additionally, the term "undetected" is unclear and confusing. The commenter stated that clarification, such as "logged but not previously selected for alerting or alarming" could be helpful. In response, the SDT has chosen to not provide further prescription but to use the words from FERC Order No. 706 to allow entities to meet the intent without prescribing exactly how to summarize or sample

the logs. Sufficient summaries or samples are dependent on many variables and do not lend themselves to a one-size-fits-all approach.

A comment was made with regard to Requirement Part 4.4 that a manual log review is a labor intensive and outdated approach. The technical guidance should allow for use of network behavior analysis or other automated review processes for this Requirement. The commenter believes that this Requirement is ambiguous. The commenter further stated that the Requirement to review 'undetected' Cyber Security Incidents is essentially a Requirement to perform manual reviews. By requiring a manual review, the entities are encouraged to record the absolute minimum event types as to minimize the burden of the manual review. Further, the Requirement to perform manual reviews would incentivize entities to not invest in systems that can perform automated log analysis and event correlation. In response, the SDT has added this Requirement in response to a directive in a FERC Order. The intent is to ensure that such automated tools are continually tuned and are not missing events that should be caught and alerted on.

A request was made to clarify Requirement Part 4.4 that the review of a summarization or sampling of logs is not acceptable as the primary means of log analysis and alert generation. Furthermore, the commenter stated that the purpose of the manual review is to achieve a level of comfort that the log analysis tool is properly configured and is not missing important security events. A random sample review of logs otherwise runs a significant risk of completely missing security events that pose potential risk to BES reliability. With regards to the Requirement column of the table for Requirement Part 4.4, the draft language indicates a need to review logs to "identify undetected Cyber Security Incidents". Is this intended to "identify detected Cyber Security Incidents"? One last comment was a suggestion to change the word "undetected" to "potential". In response, the SDT states that the intent is to review logs to insure that any automated tools or processes are tuned so that they are catching all Cyber Security Incidents, therefore the SDT believes that the 'undetected' word is correct. If attempts to breach the security of a BES Cyber System are being missed because the automated tools are not tuned or maintained, then this Requirement's intent is to catch that.

Requirement R5

There was a comment that the TFE language in CIP-007-5 Requirement Part 5.6 is unnecessary since technical or procedural controls can be used and that the phrase "per Cyber Asset capability" be used instead. In response, since many Cyber Assets used today utilize shared accounts and have no capability for individual accounts, periodically changing passwords is necessary. The SDT is aware that some systems have passwords that cannot be changed, or that if changed will break the system's functionality. Therefore, the SDT allowed for TFE's since the entity may not be able to

change the password either technically or procedurally. The SDT chose not to use the 'per Cyber Asset capability' as this is an instance where documenting and implementing some alternative control is necessary.

Within the Rationale section of CIP-007-5 Requirement R5, there was a suggestion to add the phrase “mimic display” to the second paragraph which outlines what is not included in interactive user access. In response, the SDT disagrees because the definition agreed to by the SDT is very clear and by adding another example with a non-widely used term would not add further clarity.

One commenter asked how CIP-007-5 Requirement Part 5.1 and CIP-005-5 Requirement Part 2.3 differ. The commenter stated that both appear to require authentication of Interactive Remote Access sessions. In response, CIP-007-5 Requirement Part 5.1 refers to any user access, including local access while physically present at the device. CIP-005-5 Requirement Part 2.3 refers to remote access.

A commenter believes that including specific password Requirements within a standard is contrary to new and safer technologies by the industry. In response, the SDT notes that the password Requirements have been worded in such a way that they only apply if passwords are used for authentication. If other, stronger means of authentication are used (tokens, biometrics, etc.) then the password Requirements do not apply. The Requirements are only “for password only authentication”.

One commenter stated that the term “generic account types” used in Requirement Part 5.2 is not defined and has not been well understood by entities to date. In response, the SDT notes that the term is now “default or generic” and the guidance provides some further explanation. The SDT does not believe that there is a sufficient definition of “generic” that will add any value beyond its normal dictionary definition.

One commenter suggested that within Requirement Part 5.2, alternate wording be provided to specify “known” enabled default or other generic account types. In response, the SDT agrees and has made the recommended clarification. The SDT notes this concept was already included in Requirement Part 5.4 and has included it here in Requirement Part 5.2 as well.

One commenter stated that Requirement Part 5.4 needs to be clarified that it pertains to active user accounts. The comments stated that there is no value to changing a password for an inactive or disabled user account until such time as the account is enabled. The commenter requested that the Requirement should also be clarified to require the initial

password change prior to placing the BES Cyber Asset into service. In response, the SDT disagrees. A known, published password should be changed even if the account is disabled. If the account is accidentally re-enabled, the password would be widely known. The SDT agrees that it would be a good practice to not only change the default password but also disable the default accounts if feasible, but it is not a Requirement.

There was a comment with regard to Requirement Part 5.4 that the word 'known' is ambiguous. For clarity, the commenter suggested changing the phrase "known default passwords" to "knowable default passwords". In response, the SDT disagrees that changing "known" to "knowable" solves the issue. The Requirement applies to the Responsible Entity, therefore it is "known to the Responsible Entity". Some vendors include "back door" user accounts in devices that are known only to the vendor and not the Responsible Entities. The Requirement is for the Responsible Entity to document only those that they know of.

A commenter suggested that Requirement Part 5.5's limitation to "password only" authentication is too narrow in scope and needs to include any use of a password for interactive access, even if part of a multi-factor authentication. The commenter also stated that this would need to include user accounts that are capable of being used interactively even if the intended use is only programmatic (e.g., an FTP account). Another comment to Requirement Part 5.5 was that the first paragraph uses the phrase "interactive user access" and that this is not a defined term. However, it is similar to the CIP Version 5 definitions defined term. The commenter questions whether the phrase "interactive user access" should be defined or clarified in the Guidelines and Technical Basis section. The SDT has added language clarifying "interactive user access" from the rationale for Requirement R5 to the Guidelines and Technical Basis section for Requirement Part 5.5.

One commenter recommended that the phrase "…at least once every 15 calendar months" be replaced with "at least once each calendar year." In response, and as described earlier, the SDT disagrees as it has standardized throughout the CIP standards that the original use of the word 'annual' be replaced with 'once every 15 calendar months.'

With regard to Requirement Part 5.7, one commenter requested a clarification to establish an upper bound (or maximum number of attempts) to generate an alert or initiate an account lockout. In response, the SDT disagrees that a prescriptive number of attempts is warranted. The entities will be in a better position to determine how many attempts in what time interval are needed for the particular situation. There may be widely varying circumstances to take into account such as is the login used by a process that is vital and will locking it out or slowing the interval between tries affect reliability.

CIP-008-5

General

One commenter stated that both CIP-008-5 and CIP-009-5 have plan update Requirements and should be considered for removal. In response, the SDT does not agree these should be removed in this version because we address multiple Directives in FERC Order No. 706 related to the update of plan documents.

Requirement R1

One commenter suggested adding "assess" to the required processes in Requirement Part 1.1. The SDT does not agree there is a need to include "assess" in the Requirement Part.

One commenter recommended increasing the one hour reporting threshold in Requirement Part 1.2. In response, the SDT uses this timeframe to respond to a directive in FERC Order No. 706, Paragraphs 673 and 676. The one hour also refers to the preliminary reporting required from the point at which the entity has determined an incident is a Reportable Cyber Security Incident.

Several commenters suggested that the obligation to report to the ES-ISAC in Requirement Part 1.2 may not be acceptable for some Canadians, but the SDT is unaware of any ES-ISAC reporting restrictions for Canadians. However, the SDT has clarified that such reporting to ES-ISAC is only required, unless prohibited by law, to account for scenarios where federal or provincial laws may prohibit such action.

Several commenters stated that notification of the ES-ISAC occurs only after a Cyber Security Incident is determined to be reportable and the one hour timeframe should start at the determination of the incident as being Reportable. The SDT has modified the Requirement to clarify the one hour timeframe is from determination rather than identification.

One commenter requested clarification on the term "preliminary notice." In response, we quote from the Technical Guidelines section of CIP-008-5, "This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report."

There was a comment that the one hour timestamp in Requirement Part 1.2 would require a paperwork intensive burden on the entity that may qualify for removal according to Paragraph 81 of FERC's Order on the Find, Fix, and Track process.

In response, while additional documentation may be necessary to demonstrate compliance with the timeline, the objective this Requirement goes beyond an administrative function.

One commenter suggested changing the one hour reporting threshold of Requirement Part 1.2 to 24 hours to align with EOP-004-2. In response, the one hour threshold is directed as a change in FERC Order No. 706;the SDTs for both CIP Version 5 and EOP-004-2 agrees this obligation was best left in the context of CIP-008-5.

One commenter stated that the roles and responsibilities of the incident response plans specified in Requirement Part 1.3 should be left to the Responsible Entity. They expressed concern for an auditor determining certain roles were left out of the plan. In response, the Requirement Part does not specify which roles must be in the plan, but having roles and responsibilities is a necessary part of an effective incident response plan.

Requirement R2

One comment read that Requirement R2 should have the language allowing an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R2 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One commenter proposed Requirement Part 2.1 needs clarification on whether a plan with multiple scenarios needs to have each scenario tested. In response, the SDT does not agree this clarification is necessary. It could be a benefit to consider multiple scenarios, and imposing a Requirement to test each would be a disincentive. Regardless, it is best left to the entity to determine how to test its plan.

There was a suggestion that the testing periodicity in Requirement Part 2.1 is inconsistent from the period used across other standards. The SDT agrees and has made this modification.

One commenter proposed adding wording to confirm a single incident response plan is sufficient for all High and Medium Impact BES Cyber Systems. In response, the Requirement Part does not preclude having a single plan, and the rationale in Requirement R1 suggests doing so.

One commenter suggested that documentation of a Reportable Cyber Security Incident suffers a “catch-22” in that one of the steps is a determination of whether or not an incident is Reportable. In response, the documentation of a Reportable

Cyber Security Incident can be performed after-the-fact. This is not a Requirement to document each step contemporaneously with each action.

One commenter recommended removing the documentation of deviations in Requirement Part 2.2 since it is mostly captured in the lessons learned. In response, the lessons learned activity likely will use documentation captured from the Cyber Security Incident, but there is no obligation to document the use of the plan. The SDT chose to use documentation of deviations because this is a much less documentation-centric activity than documenting how the plan was used.

Several commenters stated that Requirement Part 2.3 should be moved to data retention. In response, the retention of this information serves the purpose of supporting follow-up incident analysis and correlation activates. There is otherwise no obligation to retain this information.

Requirement R3

There was a comment that Requirement R3 should have the language allowing an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R3 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One commenter stated that CIP-008-5 Requirement R3 should allow deficiency correction. In response, the SDT does not agree this Requirement meets the criteria to be considered as high frequency, zero tolerance obligations as are the other Requirements that allow for deficiency correction.

There was a comment that in Requirement Part 3.1.2, lessons learned do not always trigger a plan update and that a qualifier “as applicable” should be added. The SDT agrees and has added the clarification, “lessons learned associated with the plan.” Corresponding changes have also been made in CIP-009-5.

There was a proposal that the timeframe in Requirement Part 3.2 could be extended to 90 calendar days consistent with 3.1. The SDT notes that Requirement Part 3.1 also includes the lessons learned obligation so the cumulative time to update should be longer.

One commenter proposed removing Requirement Part 3.2 or specifying only the affected roles and responsibilities. In response, the SDT notes that notification of all individuals is necessary for communication during a Cyber Security Incident.

One commenter stated for Requirement Parts 3.1 and 3.2, the wording needs to be rearranged to read better - the phrase 'no later than 90 calendar days after' should be added at the start of the sentence and deleted from the end. The SDT agrees and has made this change.

CIP-009-5

Requirement R1

One commenter stated that the roles and responsibilities of the recovery plans specified in Requirement Part 1.2 should be left to the Responsible Entity. They express concern for an auditor determining certain roles were left out of the plan. In response, the Requirement Part does not specify which roles must be in the plan, but having roles and responsibilities is a necessary part of an effective recovery plan.

There was a comment that Requirement Part 1.2 discusses responders without any additional clarification of who fits into this category. In response, this language has been carried forward from previous versions and the SDT has not received any additional comments supporting modification. The SDT agrees additional guidance would be helpful and has added clarification in the Technical Guidelines section of CIP-009-5.

There was one comment that stated that there should be more consistency in the applicability column of the tables and requests clarity on what applies if a Medium Impact BES Cyber System does not have a connectivity qualifier. In response, the lack of a qualifier only means that all Medium Impact BES Cyber Systems are applicable.

One commenter requested clarity on the intended frequency of performing Requirement Part 1.4. In response, the frequency is determined by the Responsible Entity. Some cyber systems may require a daily backup while other cyber systems, for example, at a power plant, may only require backups after major changes to the system.

One commenter suggested removing “and to address backup failures” from Requirement Part 1.4 because it may lead the reader to the notion of having another pre-determined plan to account for unknown issues during the backup. In response, the SDT notes that addressing backup failures meets the objective of the Requirement and purpose for verifying the successful completion of backups. Without this obligation, an entity could simply perform validation testing without performing any corrective action on the backup process.

Several commenters proposed changing Requirement Part 1.5 to “One or more processes, per device capability, to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), except where data preservation impedes or restricts recovery.” However, the rephrasing has a subtle change in meaning. The per device capability exception applies to the preservation of data and not the procedure itself.

One commenter stated that Requirement Part 1.5 can lead to delay in recovery operations, particularly in a Control Center. In response, the SDT notes the provision of the Requirement that data preservation should not impede recovery.

One commenter requested clarification of Requirement Part 1.5. They state that it would seem the activity would delay recovery. In response, planning to preserve evidence could include additional individuals assisting in the recovery or retaining failed Cyber Asset equipment during recovery operation.

One commenter suggested adding a CIP Exceptional Circumstance qualifier to Requirement Part 1.5. In response, the SDT removed this qualifier based on industry comments because an event triggering recovery could most likely be a CIP Exceptional Circumstance, and thus nullify the Requirement. However, Requirement Part 1.5 achieves the same objective in having a qualifier to avoid the disruption of restoration activities. The commenter also expressed concern about the intent of Requirement Part 1.5 and suggests moving this to CIP-008-5. In response, the objective is to have this performed in any recovery operation and not just Cyber Security Incidents.

There was a comment for Requirement Part 1.5 suggesting that the Requirements could put the registered entity into a "catch-22" scenario where it could try to comply with the Requirement by saving logs, which might impede recovery. In response, the plan should address the issue where saving information impedes recovery as indicated in the Requirement Part.

One commenter stated that in Requirement Part 1.5, the device capability should be worded to clearly qualify the preservation of data. The SDT agrees and has made this change. They also suggested the measure be updated to include the device capability qualifier. However, the qualifier itself only applies to the Requirement and does not need to have inclusion in the measure.

Requirement R2

There was one comment that the words 'between tests of the plan' are not needed. The SDT agrees and has made this clarification.

One commenter requested clarification on how an entity tests a representative sample of information if, per Requirement Part 2.1, they performed a paper drill. In response, the SDT notes that the test in Requirement Part 2.2 is not necessarily the same test performed in Requirement Part 2.1.

One commenter proposed Requirement Parts 2.1 and 2.3 need clarification on whether a plan with multiple scenarios needs to have each scenario tested. In response, the SDT does not agree this clarification is necessary. It could be a benefit to consider multiple scenarios, and imposing a Requirement to test each would be disincentive. Regardless, it is best left to the entity to determine how best to test their plan.

There was a request for clarification on the difference between 2.1 and 2.3 and for additional guidance on what types of operational exercise the SDT considers meeting the Requirement. In response, the SDT refers to the Technical Guidelines section of CIP-009-5, which states "The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, '[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims).'"

One commenter suggested that Requirement Part 2.2 needs to provide additional clarification for a "representative sample" of information used to recover BES Cyber System functionality. In response, the SDT does not think it provides a benefit to further specify a representative sample of information in this Requirement. Otherwise, this Requirement becomes focused on the sample of information rather than the recovery of information. As specified in the rationale, "Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information."

A clarification request was made on Requirement Part 2.2 regarding a representative sample. The representative sample must be determined by the Responsible Entity. It could be a test of all the most recent backup tapes or it could be a single representative test for multiple instances of the same system.

Requirement R3

There was a comment that this Requirement should include language that would allow an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R3 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One commenter suggested that a lessons learned activity should not be required for every failure of equipment in the field. In response, failure of equipment in the field does not indicate a recovery operation in all cases.

There was a proposal that the timeframe in Requirement Part 3.2 be extended to 90 calendar days consistent with 3.1. The SDT notes that Requirement Part 3.1 also includes the lessons learned obligation so the cumulative time to update should be longer.

There were several comments on parts 3.1 and 3.2 that the wording needed to be rearranged to read better - the words 'No later than 90 calendar days after' should be added at the start of the sentence and deleted from the end. The SDT agrees and has made this clarification.

Guidelines and Technical Basis

One entity commented that the guidelines state that recovery plan information is BES Cyber System Information, which is not consistent with the definition of BES Cyber System Information. The SDT agrees and has modified the guidance to state that recovery plan information may be considered BES Cyber System Information.

CIP-010-1

Timeframes for Configuration Control Activities

The SDT received comments that the timeframes for configuration control activities are inconsistent. The SDT believes that the timeframes specified are consistent and are reflective of a reasonable configuration change control process.

Cross References to CIP-005-5 and CIP-007-5 on Impacted Controls

Comments expressed concern over the cross-reference to CIP-005-5 and CIP-007-5 as it related to the controls that could potentially be impacted by a change. The commenter recommended that the Requirement be broadened to include any control rather than simply those included in CIP-005-5 and CIP-007-5. The SDT appreciates the concern expressed in this comment and wrestled with this issue itself. After changes to this issue during multiple rounds of industry comment, the SDT believes that bounding the controls that need to be assessed is the most auditable approach.

The SDT received comments regarding a concern over double jeopardy between CIP-005-5, CIP-007-5, and CIP-010-1, specifically as it relates to the documentation of logical network accessible ports. The SDT does not believe this is a double jeopardy situation. CIP-005-5 and CIP-007-5 specify how ports are to be configured whereas CIP-010-1 specifies that they be documented.

Requirement R1

The SDT received numerous comments to add the “external routable connectivity” qualifier to the applicability section in Requirement R1. The SDT appreciates the concern regarding the amount of effort involved in maintaining baseline documentation for disconnected Cyber Assets. However, since these devices are disconnected, the point in time at which the device is interacted with is the only time that the configuration may actually be validated. Given this, the SDT believes it is worthwhile to formalize the configuration change management process for these systems such that an understanding of the current configuration of the device is assured at all times.

One commenter identified confusion as it relates to comma usage in CIP-010-1 Requirement Part 1.5.1. The SDT has clarified the Requirement and removed the incorrect comma.

One commenter asked for clarification that the items in the baseline are “current” and not historical. The SDT confirms that it expects that the baseline is a current representation of the configuration and that this should be kept up to date by Requirement Part 1.3.

One comment from industry asked for clarification as it relates to Requirement Part 1.4.2 and whether this verification that security controls are in place was to be performed on the production system itself. The SDT clarifies that this is the case. The intent of the Requirement is to ensure that the production system is properly protected following a change that affected its baseline configuration.

Several commenters asked for clarification on the use of TFEs in Requirement Part 1.5 (testing of changes) and whether the SDT actually meant CIP Exceptional Circumstances. The SDT envisioned that operational issues may prevent the ability to test a change prior to its implementation. The SDT believes that the TFE process provides the protection necessary to ensure that violations are not issued for a wide range of circumstances, including but not limited to those operational issues contemplated in the CIP Exceptional Circumstances definition.

Requirement R2

Comments expressed that the IAC language should be removed from CIP-010-5 Requirement Part 2.1 because this Requirement was itself an internal control. The SDT agrees that the Requirement represents a control; however it believes that, particularly given the required periodicity, that there could be deficiencies identified in the control itself and it therefore warranted the IAC language.

Requirement R3

One commenter recommended that the language in Requirement Part 3.3 be modified to add the word applicable ("Prior to adding a new applicable Cyber Asset...") in order to clarify that this Requirement did not apply to those systems that are temporarily connected for less than 30 days. The SDT agrees that this is consistent with the intent of the language and has modified the language accordingly.

The SDT received concerns regarding the performance of active vulnerability assessment prior to the deployment of new BES Cyber Assets. The SDT agrees that these assessments may be imperfect and that there may be some applications that will not properly function outside of a full production environment. However, the SDT continues to believe that since this is the only time when active scans may be safely performed on future production equipment that it is in the best interest of the BES for an active vulnerability assessment to be performed.

The SDT received comments preferring additional specificity as to what to validate during a vulnerability assessment. The SDT appreciates these concerns, but believes that a vulnerability assessment for an EMS system may look substantially

different from an assessment of a PLC. The SDT believes that the best approach is to allow the entity to define an appropriate assessment methodology for their environment, which may then be evaluated by an auditor.

The SDT received comments that questioned the technical feasibility of monitoring for changes to the baseline configuration. The SDT originally had intended for this monitoring to occur on a more frequent basis, potentially real-time monitoring. However, it was persuaded that there are some systems for which real-time monitoring would be infeasible. The SDT does believe that given the relatively high level items included in the baseline, that periodic monitoring every 35 days is a reasonable method to ensure that changes are not taking place outside of an entity's change control program.

Numerous commenters expressed concern about the Requirement to document the differences between the test and production environments. The SDT reminds the industry that this Requirement was the result of a FERC directive. Additionally, the SDT reminds the industry that it believes that for a relatively stable testing environment, that this documentation could be done once and utilized for multiple changes or testing cycles.

Commenters asked questions about the multiple timeframes for the vulnerability assessments for high impact BES Cyber Systems. The SDT confirms that these time frames are intended. Effectively, this requires an annual paper or active vulnerability assessment, but an active vulnerability assessment must be performed at least every three years. The SDT believes that the confusion raised by the question is due to the reader not considering the entire table as itself a single Requirement.

One commenter expressed confusion on the applicability of CIP-010-1 to access points. The SDT clarifies that since access points are the point at which access is controlled, they are included in the definition of EACMS and as such are applicable to CIP-010-1.

One commenter asked for clarification that the test environment did not have to be an exact mirror of the production environment. The SDT confirms that this was the intent of using the phrase "models the baseline configuration."

CIP-011-1

Requirement R1

Commenters requested that Requirement Parts 1.1 and 1.2 of CIP-011-1 Requirement R1 be clarified to indicate that a single method or procedure was sufficient. The SDT agrees that this is the intent and has clarified the standard as requested.

Commenters suggested that CIP-011-1 Requirement Part 1.2 should contain a measure that indicates "repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program." The SDT does not see how a repository is evidence of a procedure to protect and securely handle BES Cyber System Information. The SDT agrees that an information repository may be used effectively to meet this Requirement, but it is only a component of the evidence based upon a particular manner of implementation.

Requirement R2

One commenter requested that Requirement R2 of CIP-011-1 be moved to CIP-010-1 as it could be considered part of a change control process. The SDT believes that the objective of this Requirement is the protection of the information in a BES Cyber System and therefore believes it is appropriate to include in CIP-011-1.

Commenters identified a typographical error in the measure of Requirement Part 2.2. The SDT appreciates this correction and has updated the standard.

Implementation Plan

Effective Date

Several commenters had questions or concerns about the Version 3 to Version 4 to Version 5 transition within the standards' implementation plan. Some questioned whether extending Version 3 to the effective date of Version 5, and superseding Version 4, is still possible, while others asked for a deadline for accomplishing such a transition plan. The SDT appreciates these concerns, as they are issues of efficiency, planning, effort, and cost for all of the industry. However, the SDT also acknowledges that not all entities are situated exactly the same. As such, the SDT is hesitant to provide a "deadline" or other trigger for FERC action that would serve to foreclose the opportunity for the implementation language to be adopted in time to implement moving directly from Version 3 to Version 5. The SDT expects that the filing will address this issue in a manner such that certainty about the issue may come as soon as possible, and that the filing and other coordination between NERC and FERC is the appropriate venue for supporting the implementation plan after industry approval. In the meantime, it is reasonable to expect that some entities may need to make a risk-informed judgment to proceed with Version 4 implementation by a certain date if the proposal in the implementation plan is not approved expediently. Some entities may be able to wait longer than others into 2013 before making that determination. The SDT has communicated directly with NERC to underscore the importance of coordination of this effort, and the SDT believes that having an approved set of standards, definitions, and implementation plan before the end of 2012 continues to provide a reasonable timeline to consider the implementation plan proposal.

There was one comment that 36 months to comply with CIP-003-5 Requirement R2 is excessively long since it only requires documentation of a few policies. The SDT notes that CIP-003-5 Requirement R2 requires implementation, and not just documentation of policies. This expands to a significantly large number of the overall reported BES Cyber Systems, which warrants such a timeline.

One commenter suggested that it misleads entities to allow the provision suspending compliance with Version 4. The SDT does not agree this is misleading. The SDT has been careful to communicate the risk in awaiting this order to begin planning compliance with Version 4. Furthermore, the FERC approving this provision, even if it is closer to the Version 4 Effective Date, still spares entities and auditors alike untold expenses of a compliance monitoring program for Version 4.

A few commenters asked about audits in 2015 during the expected transition window to Version 5's effective date. That is outside the scope of the SDT, but the SDT has tried to account for a smooth transition within the implementation plan,

to include specifications for initial required performances of periodic events. In response to this question and the issue of transition from Version 3 to Version 5, the SDT understands that NERC is preparing information to assist in the smooth transition among CIP standards versions, and that such information will be coordinated upon certainty that Version 5 has been approved by the industry and is no longer subject to change.

One commenter stated that the effective date language should be qualified with a statement that sufficient time should be given for completion of CIP-002-5 R2 to comply with CIP-003 through CIP-011. The SDT believes this is already well understood and ongoing communication and training will provide entities further guidance to categorize BES Cyber Systems with sufficient time to comply with CIP-003 through CIP-011.

Several entities comment that NERC and the drafting team should request FERC to suspend compliance with Version 4 and allow entities to transition from Version 3 to Version 5 on the effective date. In response, the proposed effective date does bypass Version 4 and provides the FERC the opportunity to issue an order approving this provision. In effect, this is the industry and SDT communication to the FERC requesting the bypass of Version 4.

There was a comment that suggested extending Version 3 until Version 5 becomes effective could not be accomplished in Canada through an implementation plan. In response, the SDT notes that Canadian jurisdictions would be subject to the second provision for "those jurisdictions where no regulatory approval is required." The commenter is correct that the proposal in the Implementation Plan, if approved, would supersede any other Order to the contrary. In all cases of reliability standards, the Implementation Plan is subject to regulatory or other applicable federal approval.

A few commenters noted that CIP-003-5 is dependent upon CIP-004-5 through CIP-009-5, CIP-010-1, and CIP-011-1 passing. The SDT confirms the commenters' understanding and notes that the implementation plan conditions all standards passing before any of them become effective.

One commenter expressed concern that the implementation of CIP-004 through CIP-011 should be combined into those standards. The SDT points out that the implementation of security procedures in CIP-004 through CIP-011 is included in those Requirements that have actions associated with them. The entity should refer to the high level Requirement for the implementation language.

Initial Performance of Certain Periodic Requirements

Several commenters stated some confusion with the initial performance of periodic Requirements section or suggested that it is unnecessary and, if retained, should be in guidance. The SDT notes this section was incorporated from industry comments, and moving this section to guidance would be misleading because the additional time for compliance with periodic Requirements would not be enforceable in guidance.

There was a comment that no provision for CIP Exceptional Circumstances exists for some periodic Requirements and that an entity should be allowed to track instances of non-compliance in CIP Exceptional Circumstances rather than self-report. In response, the SDT has indicated where exceptions may occur to the standards in defined CIP Exceptional Circumstances. Most of the periodic Requirements should have enough lag time built in to avoid the need for self-reporting in emergency situations. Otherwise, it is not envisioned all compliance activities should cease in a CIP Exceptional Circumstance, but only the ones indicated in the Requirements.

One commenter proposed revisions to the following initial periodic Requirements, and the SDT responds in order:

- CIP-004-5 Requirement Parts 4.2 through 4.4 should be required on or before the effective date to preclude record-keeping errors. The SDT notes that record-keeping errors, while not the most efficient, are not violations of the standard.
- CIP-006-5 Requirement Part 3.2 should tie to the previous testing interval and allow 24 months for the newly in-scope Cyber Assets. In response, tying the interval to previously in-scope Critical Cyber Assets would cause more confusion than is necessary for this Requirement, and the SDT believes the 12 calendar months are appropriate timeframes for testing PACS.
- CIP-008-5 Requirement Part 3.1 and CIP-009-5 Requirement Part 3.1 should not be included in the initial performance of periodic requirements section since they are not periodic, but are performed in response to a test. The SDT agrees.
- CIP-010-1 Requirement Parts 3.1 and 3.2 should not be included because it would be similar to part 3.3 in adding a new Cyber Asset to the BES Cyber System. In response, the SDT retains the additional timeframe because strict compliance would suggest this periodic timeframe be performed immediately on the effective dates for all BES Cyber Systems in scope, which would be infeasible for most all entities.
- CIP-009-5 Requirement Part 2.3 is included in both groups 6 and 7. The SDT notes this is not the case.

- Group 8 of the periodic Requirements dealing with the continued effectiveness of previous personnel risk assessments is already incorporated in the Requirement language. In response, strict compliance with the Requirement would otherwise suggest immediate compliance with this Requirement on the effective date.

One commenter suggested that NERC imposing Requirements before the effective date goes beyond NERC's legal authority. In response, the implementation plan does not modify the effective date of any Requirement but makes clear when the initial performance must occur for certain Requirements. By stating a Requirement can be performed prior to the effective date does not impose a different effective date. Rather, this clarifies that on the effective date, the entity has complied with the Requirement by performance of a past activity.

There was an observation that CIP-006-5 Requirement Part 3.1 and the Requirements specified in section 7 have periodicities longer than the initial performance. This is correct and intended by the SDT because even though the periodicity is longer, the benefit achieved by the initial performance puts it closer to the effective date.

Previous Identity Verification

One commenter noted an incorrect reference to CIP-004-5 Requirement Part 4.1, and the SDT expresses their gratitude for uncovering this error.

Planned or Unplanned Changes Resulting in a Higher Categorization

Several commenters suggested that the distinction between planned and unplanned changes is not clear and the timeframe for planned changes should be extended to 18-24 months. In response, the SDT carries forward this language that has been in effect since Version 2. The 12 months is also carried forward as the time entities with existing CCAs have to implement CIP Requirements on new CCAs. The SDT does not consider this 12 month timeframe unreasonable and notes in the example given that updates to a generation facility would be considered a planned change and compliance would be part of the maintenance performed during the outage.

One commenter stated that the addition of time for initial performance of periodic Requirements muddles the timeline for compliance. In response, the implementation plan would not preclude an entity from complying earlier to benefit the entity with a consistent compliance schedule, but without this provision, the periodic Requirements would need to be performed prior to the 12 month period, and this is neither reasonable nor appropriate. This language was added since the last posting in response to multiple entities' request.

There was a comment that suggested the last scenario in unplanned changes be clarified as the first high or medium impact BES Cyber System overall rather than at a facility. The SDT has made this clarification by providing a clarifying parenthetical phrase to row five of the "Scenario of Unplanned Changes After the Effective Date" table that underscores the meaning of that row in relation to and in context with rows one through four.

There was a request for clarification on the use of Effective Date in the table heading "Scenario of Unplanned Changes After the Effective Date". In response, the SDT notes that this is the effective date specified in each standard for Version 5 of the CIP Cyber Security Standards.

Applicability Reference Tables

One commenter proposed revisions to the Requirement applicability, and the SDT responds in order:

- CIP-004-5 Requirements R4 and R5 should apply to Protected Cyber Assets. In response, we have addressed most of the risk by authorizing and revoking access associated with the BES Cyber System. We carry forward the precedent of applicability in this case from previous standards, and do not find a justification for adding them to the applicability of these Requirement Parts.
- CIP-005-5 Requirement R1 should apply to PACS as it does in the current standard.
- CIP-005-5 R1 should apply to PACS as it does in the current standard. In previous versions, CIP-005 R2 applied but not R1. The SDT received significant industry feedback that this applicability was confusing and resulted in multiple interpretations. The SDT addresses access control at the device level in CIP-007-5 and avoids the confusion around the disconnect between applicability in CIP-005-4 R1 and R2, and for this reason, CIP-005-5, Requirement R1 does not apply to PACS.

There was a comment that CIP-005-5 Requirement R2 should apply to EACMS. In response, the EACMS are referenced as part of the Requirement. The confusion of recursive Requirements is not worth the reliability and security benefit gained by their inclusion.

Definitions

BES Cyber Asset

One entity commented that the definition should reference "the items in Attachment 1" instead of "Facilities, systems, or equipment," because "Facilities, systems, or equipment" is subjective and lends itself to differing interpretations, and Attachment 1 provides greater clarity and guidance on the criteria to define BES Cyber Assets. The SDT points out that a definition is used in a standard and cannot reference a part of the standard. The term "Facilities, systems or equipment" has been used as part of the definition of Critical Assets for Versions 1, 2, 3 and 4.

BES Cyber System

One commenter wrote that the definition uses the word logically that may be mistakenly interpreted to mean networked instead of validly grouped. The SDT believes that the rest of the definition of the BES Cyber System in relation to the performance of reliability functions provides clarity to the meaning used here.

BES Cyber System Information Responses

The SDT received a concern regarding the phrase "not publicly available" in that if BES Cyber System Information was made public, it would then be outside the scope of the standard. The SDT appreciates this concern; however, it believes that the meaning is ultimately clear as to the intent.

CIP Exceptional Circumstance Responses

The SDT received a request to clarify the punctuation in the definition of CIP Exceptional Circumstances. The SDT has updated the punctuation as requested.

One commenter expressed concern about the ability to declare a CIP Exceptional Circumstance for hardware, software or equipment failure. The concern of the commenter was that this could open the door to bypassing Requirements for minor issues. The SDT did not envision this as a free for all and believes that the obligation to have policy around the declaration and response to CIP Exceptional Circumstances should minimize any abuse of this definition.

CIP Senior Manager Responses

One commenter requested that the SDT address the accepted interpretation request in RFI Project 2012-INT-06. While the SDT has an obligation to incorporate existing interpretations, the response to the interpretation that was highlighted has not been posted and therefore the SDT would risk contradicting a pending standards interpretation action.

Additionally, since that interpretation has not been approved by industry, there is no way for the SDT to determine whether it reflects a level of consensus of the industry. As such, the SDT believes that this would be too large of a change to incorporate at this point in the development process.

Control Center

Many entities requested clarification on the term “associated data centers” in the definition of Control Centers and asked whether these are the "data centers" that service/support a control center”. Comments were also made that “data center” is not a defined term. The SDT believes that the term “data center” is a commonly understood term of practice and that a specific glossary definition is not required. The intent of including “associated data centers” in the definition of Control Centers is to include only those systems that are associated with the Control Center Cyber Assets and directly support the functions of the functional entities defined. These will be the BES Cyber Systems that directly provide monitoring and control functions for the Control Center operators’ use in the performance of their real-time functions, and to ensure that this does not include certain types of field data aggregating or processing assets that are associated with field transmission or generation assets. Control Center data centers do not necessarily reside in the same facility where operators are hosted, but may extend the Control Center to include facilities hosting these cyber systems outside of the facility hosting the Control Center operators.

One entity requested clarification on the meaning of “location” in the definition. The NERC Guideline for Critical Asset identification has an extensive discussion of control rooms and Control Centers. In general, a location is delineated by a physical boundary that hosts a set of BES Facilities.

One entity suggested the addition of “CIP” to the term or some indication that this is only a definition used in the CIP context. The SDT is proposing the term to be included in the NERC Glossary. The convention is that when the term is used in its capitalized form (initial letter of each word), then it is used as the NERC Glossary defined meaning of the term. Otherwise, it is used in the undefined, generic meaning. This does not have any effect on other standards that do not use the term in its capitalized form. Other standards which wish to use the NERC Glossary term as defined (or wish to amend it through the development process) can use the capitalized form.

Cyber Asset

One entity commented that the inclusion of “hardware, software and data” in the definition of Cyber Asset was redundant and proposed a simplified definition of “Entity programmable electronic devices”. The SDT’s approach to existing definitions is to make only the modifications necessary for additional clarity or intent. This definition is based on

the previous definition of Cyber Asset. The SDT believes that removing the terms “hardware, software and data” would not provide additional clarity and that the addition of “Entity” in the qualification of “programmable” would inappropriately limit the general scope of the definition of cyber asset. The protection Requirements in the standards include those necessary to ensure that proper processes are included for protection from inappropriate modification or misuse of programs not directly modified by the entity.

Another entity commented that the proposed definition could be interpreted to require utilities to demonstrate consideration of - in addition to hardware - all software and data on each programmable electronic device, which would be impracticable and overly burdensome. The entity recommends changing the definition to “Programmable electronic device.” The SDT points out that the inclusion of these qualifications has been part of the definition of cyber assets since Versions 1, 2, 3 and 4 and that the modifications to the previous definition ensures that the definition includes the data when it is on these devices.

One entity commented that the inclusion in voice communication for a Control Center operator to implement operating actions in the execution of a Control Center functional obligation would include many smaller entities as Control Centers. The determination of whether a facility is considered a Control Center is dependent on whether it meets the definition, not on size or on how it performs its functional obligations. The manner in which it implements its functional obligations will determine what are qualified BES Cyber Assets. For example, in the environment that the commenter describes, there may be many BES Cyber Assets that provide monitoring and alarming information on which the operator will initiate a real-time operation for the BES. The impact of such monitoring and alarming systems on the real-time operation of the BES warrants the protection commensurate with its function.

Cyber Security Incident

One commenter suggested modifying the definition of Cyber Security Incident to eliminate attempts of compromise or disruption because such a definition is broad enough to include any erroneous traffic. The SDT disagrees. Attempts of compromise imply intent far beyond erroneous traffic and should be analyzed and recorded as part of the CIP-008-5 incident response plan.

There was a comment that the definition of Cyber Security Incident should also apply to PCAs, EACMS and PACS. In response, the definition has no applicability, and an incident occurring on PCAs, EACMS and PACS already meets the definition of having the potential to impact the BES Cyber System.

There was a comment suggesting that it is difficult to determine the intent of an attacker, and the commenter further suggested that "suspicious" is vague. In response, the SDT intends that such determination is best left to the entity. Without the qualifiers of suspicious and malicious, it could be interpreted that many nominal events would be considered Cyber Security Incidents.

Electronic Access Control and Monitoring System

One commenter stated that the definition of EACMS is inconsistent with the definition used in the background section of Version 5 CIP Standards. In response, the guidance provided in the background section is not a definition. It only provides example EACMS for the purpose of adding context for the reader.

Intermediate Device (now "Intermediate System")

A recommendation was made that the definition of Intermediate Device be modified to remove the phrase "or collection of Cyber Assets", as they consider this limiting the scope. The SDT used "A Cyber Asset or collection of Cyber Assets" to allow for flexibility so that an entity could use one or more devices to perform the noted functional Requirements. The scope of the definition and Requirements is limited to only Interactive Remote Access to BES Cyber Systems. Further, it was noted in prior comments that entities may not be able to implement a single device that provides encryption and multifactor authentication. As a result of comments, the definition has been modified to "Intermediate System" to better align with the asset and system concepts used throughout the Version 5 standards.

One commenter requested clarification on the definition of Intermediate Device. The SDT has worked the definition to allow for flexibility in the selection and implementation of technology to meet their needs. The definition does not prevent an entity from having an Intermediate Device within an ESP, just not the ESP containing the BES Cyber Systems being remotely accessed. The definition term (not the definition's meaning) has also been modified to "Intermediate System" to better align with the asset and system concepts used throughout the Version 5 standards. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested more clarity regarding the types of devices that would qualify as intermediate devices, beyond the Requirements that they must support encryption for any interactive sessions and multifactor-authentication for access to any interactive sessions. Additional references are available in the *Guidance for Secure Interactive Remote*

Access document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

Interactive Remote Access

One commenter suggested that, as written, the definition appears to require that entities declare each of their internal networks as an ESP, including their corporate networks. The commenter discussed that many entities monitor their corporate network in much the same manner as their ESPs, and that requiring encryption within their corporate networks would introduce an unacceptable security risk by rendering their monitoring capabilities ineffective. The commenter requested appropriate clarifications or that the definition be modified to specify that Interactive Remote Access and the associated technical controls be required when traffic is traversing an untrusted or public network only. In response, the SDT notes that it is not necessary to declare the encryption termination point as a part of the ESP. It is allowable to have the termination point reside outside of the ESP, such as a corporate firewall to allow for corporate boundary systems to monitor network traffic as described. In this scenario, the corporate firewall would be considered and protected as an EACMS but still not considered to define an ESP.

There was a recommendation to remove the second sentence of the Interactive Remote Access definition. The SDT added this language to address comments and concerns raised during this project and Project 2010-15: Expedited Revisions to CIP-005-3.

One comment suggested that the definition of Interactive Remote Access be modified to remove the sentence, "Remote access can be initiated from: ... contractors and consultants." The SDT added this language to address comments and concerns raised during this project and Project 2010-15: Expedited Revisions to CIP-005-3.

There was one request that the definition be modified as “access is likely initiated…” The SDT used “may be initiated” to allow for flexibility rather than using words such as “shall be initiated” or “will be initiated” which are far more restrictive and align to the concern noted.

There was a suggestion that the definition of Interactive Remote Access be modified to remove Requirement language within the definition. The SDT considers all parts of the definition to be clarification of what is and is not Interactive Remote Access. The Requirements are the technical controls to be implemented.

Reportable Cyber Security Incident

There was a comment suggesting that the definition of Reportable Cyber Security Incident is too broad and should specifically state that a malware infection of an in-scope Cyber Asset should be reported. In response, the SDT provides additional guidance in the context of CIP-008-5 that would generally ensure the proper reporting of a malware infection. However, a malware infection itself would cause additional uncertainty in the definition. Moreover, entities would be left to wonder if a contained malware infection was reportable or not. For these reasons, the SDT does not agree with the recommendation to further specify Reportable Cyber Security Incident.

One commenter said that this definition should be removed and addressed solely within the standard. In response, the SDT believes there is sufficient consensus for the definition and moving this term to a local definition in CIP-008-5 would be a significant change and potentially cause uncertainty in the enforceability of this definition.

Exhibit E

1.) Table of VRFs and VSLs Proposed for Approval
2.) Analysis of how VRFs and VSLs Were Determined Using Commission Guidelines

Exhibit E

1.) Table of VRFs and VSLs Proposed for Approval

Project 2008-06 - Cyber Security Order No. 706 - V5

Consolidated VSLs from all standards
October 26, 2012

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES Cyber Systems have not been categorized	four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of	six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or	to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.	100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified;	medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible	or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber Systems have not been identified.	Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	
R2	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity did not complete its	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (R2.2)	approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (R2.2)	approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (R2.2)	required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			review in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1)	months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did	within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar	documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar months of the previous approval. (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				complete this approval in less than or equal to 17 calendar months of the previous approval. (R1)	months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	
R2	**Operations Planning**	**Lower**	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible	The Responsible Entity did not document or implement any cyber security policies for assets with a low impact rating that address the topics as required by R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2)	Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this	Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				the previous approval. (R2)	the previous approval. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, and	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days but did document this change in less than 40 calendar days of the change. (R4)	delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	has Identified deficiencies but did not assess or correct the deficiencies.(R4) OR The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, but did not identify, assess, or correct the deficiencies.(R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions	OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the	and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals	and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for	The Responsible Entity has a program for conducting Personnel	The Responsible Entity has a program for conducting Personnel	The Responsible Entity did not have all of the required elements as

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments	Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did not identify, assess, and	Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess,	described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including	correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)	and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)	or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors,	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess,	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess,	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted	and correct the deficiencies. (3.5)	and correct the deficiencies. (3.5)	for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter, and did not identify, assess and	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2)	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies.	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for	storage locations where BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)	BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						for four or more BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1)	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1)	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4)	OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or	OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or	access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR	more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances, and did not identify, assess, and correct			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the deficiencies. (5.5)			

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning and Same Day Operations**	**Medium**			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-5 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						outbound access permissions and deny all other access by default. (1.3) OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8) OR The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of	The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7) OR The Responsible Entity	The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies.	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity documented and implemented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			entry but did not identify, assess, or correct the deficiencies. (1.8) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)	has a process communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)	(1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5) OR The Responsible Entity has a process to	operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					monitor for unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.6) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)	deficiencies, but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						(1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						different controls, but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						correct the deficiencies. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter or to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						minutes to identified personnel(1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9)
R2	**Same-Day**	**Medium**	N/A	The Responsible Entity	The Responsible Entity	The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations			included a visitor control program that requires logging of each of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or	included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1) OR The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)	has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)		retain visitor logs for at least ninety days. (2.3)
R3	**Long Term Planning**	**Lower**	The Responsible Entity has documented and	The Responsible Entity has documented and	The Responsible Entity has documented and	The Responsible Entity has not documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						months. (3.1)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible,	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* and has identified deficiencies but did not assess or correct the deficiencies. (R1) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* but did not identify, assess, or correct the deficiencies. (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				unnecessary physical input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)	had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)	
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified and	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity did not implement or document one or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)	deficiencies. (2.1) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65	more process(es) that included the applicable items in *CIP-007-5 Table R2* but did not identify, assess, or correct the deficiencies. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the	released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the	calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources identified but did not identify, assess, or	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or	correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the	CIP Senior Manager or delegate and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4) OR The Responsible Entity documented a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or	deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or correct the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)		deficiencies. (2.4)
R3	**Same Day Operations**	**Medium**		The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and has identified deficiencies but did not assess or correct the deficiencies. (3.3) OR The Responsible Entity	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.2) OR The Responsible Entity	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R3* and has identified deficiencies but did not assess or correct the deficiencies. (R3) OR The Responsible Entity did not implement or document one or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)	has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and did not identify, assess, or correct the deficiencies. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and has identified deficiencies but did	more process(es) that included the applicable items in *CIP-007-5 Table R3* and did not identify, assess, or correct the deficiencies. (R3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.1) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					not assess or correct the deficiencies. (3.3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies. (3.3)	has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies. (3.1)
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4*

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged	an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged	by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and has identified deficiencies but did not assess or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system	and has identified deficiencies but did not assess or correct the deficiencies. (R4) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4* and did not identify, assess, or correct the deficiencies. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and has identified deficiencies but did not assess or correct	detect and log all of the required types of events described in 4.1.1 through 4.1.3 and has identified deficiencies but did not assess or correct the deficiencies. (4.1) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct the deficiencies. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and has	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and has	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and has identified deficiencies but did not assess or correct	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and has identified deficiencies but did not assess or correct the deficiencies. (R5) OR The Responsible Entity did not implement or document one or more process(es) that included the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not identify, assess, or correct the	identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and did not identify, assess, or correct the	the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System	applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and has identified deficiencies but did not assess or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies. (5.6)	deficiencies. (5.6)	Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and has identified deficiencies but did not assess or correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3)	process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and did not identify, assess, or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords and has identified deficiencies but did not assess or correct the deficiencies. (5.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only	OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within	procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					17 calendar months but less than or equal to 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal	deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					to 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and has identified deficiencies but did not assess or correct the deficiencies. (5.7) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Security Incident response plan, but did not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Cyber Security Incident occurs. (2.2)	
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities,	response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				or • Cyber Security Incident response groups or individuals, or • Technology changes.	or individuals, or • Technology changes.	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests,	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Part 2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1)	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or	OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				• Responders, or • Technology changes.	responsibilities, or • Responders, or Technology changes.	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline	identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to determine required	correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline	management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the verification documentation. (1.4.3)	security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the	configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s)	OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				existing baseline configuration but did not identify, assess, or correct the deficiencies in the determination of affected security controls. (1.4.1)	that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to verify that required	process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2) OR The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did	not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					not identify, assess, or correct the deficiencies in the required controls. (1.4.2) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process for testing changes in an	the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and identified deficiencies but did not assess or correct the	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficiencies. (1.5.2) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)	
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						calendar days. (2.1) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days and identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						to the baseline at least once every 35 calendar days but did not identify, assess, or correct the deficiencies. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems. (3.1)	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A		The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented a BES Cyber System Information protection program which	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					includes one or more procedures for protection and secure handling BES Cyber System Information but did not identify, assess, or correct the deficiencies. (1.2)	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

Exhibit E

2.) Analysis of how VRFs and VSLs Were Determined Using Commission Guidelines

Project 2008-06 - Cyber Security - Order 706 - V5

These tables provide analysis and justification for each VRF and VSL for each requirement in the Version 5 CIP Cyber Security Standards:

VRF and VSL Justifications – CIP-002-5, R1	
Proposed VRF	**HIGH**
NERC VRF Discussion	A VRF of High is assigned to this Requirement. The requirement specifies the "bright-line" criteria used to categorize Bulk Electric System (BES) Cyber Systems, and the identification of High and Medium impact BES Cyber Systems. A VRF assignment of High is consistent with the higher risk impact of a violation of the identification and categorization of High and Medium impact BES Cyber Systems, as well as the failure to identify and appropriately re-categorize the affected BES Cyber Systems after a BES reconfiguration. The compromise of these Systems due to a cyber security incident could lead to significant impact, up to and including cascading disturbances. Failure to protect High and Medium impact Cyber Assets and their potential compromise may cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. The impact categorization of BES Cyber Systems is based on their impact on the reliable operation of the BES. The criteria are based on BES functional tasks that map to the areas cited in the Blackout Report.
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The Requirement specifies the "bright-line" criteria used to categorize Bulk Electric System (BES) Systems and the identification of High and Medium impact BES Cyber Systems. The VRF is only applied at the requirement level and the requirement part is treated equally. A VRF assignment of High is consistent with the higher risk impact of a violation of the identification and categorization of High and Medium impact BES Cyber Systems, as well as the failure to identify and appropriately re-categorize the affected

VRF and VSL Justifications – CIP-002-5, R1			
	BES Cyber Systems after a BES reconfiguration. The compromise of these Systems due to a cyber security incident could lead to significant impact, up to and including cascading disturbances.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-002-3/4, R2, which has an approved VRF of High and the proposed VRF for CIP-002-5, R1 remains consistent.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to protect High and Medium impact Cyber Assets and their potential compromise may cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures. Therefore, this requirement was assigned a High VRF.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. CIP-002-5-2, Requirement R1 contains one main objective: The identification and categorization of High and Medium impact BES Cyber Systems for the application of specific protective cyber security requirements and the application of programmatic controls to Low impact BES Cyber Systems. Since the requirement focuses on the specific identification and categorization of such High and Medium impact Systems, an assignment of a High VRF is justified.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1;	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1;

VRF and VSL Justifications – CIP-002-5, R1			
OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES Cyber Systems have not been categorized or have been incorrectly	considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a	Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber	OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower

VRF and VSL Justifications – CIP-002-5, R1			
categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.	total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or	Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

VRF and VSL Justifications – CIP-002-5, R1			
	medium BES Cyber Systems have not been identified.		

VRF and VSL Justifications – CIP-002-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to the violation, and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity has correctly categorized their BES Cyber Systems but fails to identify or correctly categorize one or more of them. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The paradigm in CIP-002-5 has evolved from a binary model to a multidimensional model that includes identification and categorization. The VSLs provided reflect this paradigm and is fundamentally different from the binary model in CIP Versions 1 to 4. With this fundamental difference, the VSLs are not intended to lower the current reliability objective sought by this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs do not use any ambiguous terminology; thereby, supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-002-5, R1	
Ambiguous Language	

VRF and VSL Justifications – CIP-002-5, R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	This requirement is an identification and categorization requirement and a single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and	Not applicable since this requirement does not contain interdependent tasks of documentation and implementation.

VRF and VSL Justifications – CIP-002-5, R1	
implementation should account for their interdependence	

VRF and VSL Justifications – CIP-002-5, R2	
Proposed VRF	**LOWER**
NERC VRF Discussion	A VRF of Lower is assigned to this requirement. The requirement specifies an annual review and approval of the identification and categorization of BES Cyber Systems. The impact of a failure to review and approve the identification and categorization within the prescribed period has minimal impact on the reliability and operability of the BES. The requirement is a requirement that, if violated, would not be expected to directly or adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. A VRF assignment of Lower is, therefore, justified.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. The requirement has no bearing on the areas cited in the Blackout Report.
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement has no subpart, and its assignment of a Lower VRF is consistent with the impact of a violation of this requirement. The impact of a failure to review and approve the identification and categorization within the prescribed period has minimal impact on the reliability and operability of the BES. The requirement is administrative in nature and is a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. A VRF assignment of Lower is, therefore, justified.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps to CIP-002-4 R3, which has an assigned VRF of Lower and the proposed VRF for CIP-002-5, R2, remains consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-002-5, Requirement R2 requires an annual review and approval. The requirement is a requirement

VRF and VSL Justifications – CIP-002-5, R2			
	that, if violated, would not be expected to directly adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. Therefore, this requirement was assigned a Lower VRF.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. CIP-002-5, Requirement R2 addresses a single objective and has a single VRF.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

VRF and VSL Justifications – CIP-002-5, R2			
of the previous approval. (R2.2)	of the previous approval. (R2.2)	previous approval. (R2.2)	

VRF and VSL Justifications – CIP-002-5, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines— There is an incremental aspect to the violation, and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity has appropriately reviewed and updated their identification of BES Cyber Systems but failed to complete the review and update within the specified timeframes. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed requirement is mapped to requirement R3 of CIP-002-3. The VSLs for the previous releases were based on lists of Critical Assets and Critical Cyber Assets, with separate requirements for review and approval. This version requires identification and categorization of BES Cyber Systems within a prescribed period. The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-002-5, R2	
Ambiguous Language	

VRF and VSL Justifications – CIP-002-5, R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement; and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	This requirement is a periodic review and approval requirement and does not specify protective requirements.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and	Not applicable since this requirement does not contain interdependent tasks of documentation and implementation.

VRF and VSL Justifications – CIP-002-5, R2	
implementation should account for their interdependence	

VRF and VSL Justifications – CIP-003-5, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Security policies enable effective implementation of the CIP standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. Periodic review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems. People are a fundamental component of any security program. Consequently, proper governance must be established in order to provide some assurance of organizational behavior. Failure to provide clear governance may lead to ineffective controls, which could compromise security; and, therefore, the integrity of the Bulk Electric System. Consequently, a VRF of Medium was selected.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for the Responsible Entity to implement a documented cyber security policy that contains certain elements specified in the requirement. The VRF is only applied at the requirement level, and the requirement parts are treated in aggregate. While the requirement specifies a number of elements, not necessarily parts, that must be included in the cyber security policy, the VRF is reflective of the policy as a whole. Therefore, the assigned VRF of Medium is consistent with the risk impact of a violation across the entire requirement.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-003-3, R1, which has an approved VRF of Medium; therefore, the proposed VRF remains consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to properly implement the cyber security policy is unlikely, under Emergency, abnormal, or

VRF and VSL Justifications – CIP-003-5, R1			
	restoration conditions anticipated by the preparations to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition. Therefore, this requirement was assigned a Medium VRF.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The cyber security policy requirement encompasses a number of policy domains. The VRF is identified at the risk level represented by all of the policy domains in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1)

VRF and VSL Justifications – CIP-003-5, R1			
R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1)	R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1)	this review in less than or equal to 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar months of the previous approval. (R1)

VRF and VSL Justifications – CIP-003-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement, and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security policies but fails to address one of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps back to previously approved requirements CIP-003-3 R1 and CIP-003-3 R1.2. The VSLs were combined for these requirements using a gradated methodology. The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-003-5, R1	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement; and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security policies but fails to address one of the required topics. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The action of the requirement is to implement documented cyber security policies. Documentation of the policies is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the policy in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the policy. The drafting team's intent is that this covers both documentation and implementation and,

VRF and VSL Justifications – CIP-003-5, R1	
documentation and implementation should account for their interdependence	therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-003-5, R2	
Proposed VRF	**LOWER**
NERC VRF Discussion	A VRF of Lower was assigned to this requirement. Security policies enable effective implementation of the CIP standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. People are a fundamental component of any security program. Consequently, proper governance must be established in order to provide some assurance of organizational behavior. However, given the scoping of the this requirement to only those BES assets that contain low impact BES Cyber Systems, a VRF of Lower was selected.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for the Responsible Entity to implement a documented cyber security policy that contains certain elements specified in the requirement. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. While the requirement specifies a number of elements, not necessarily parts, that must be included in the cyber security policy, the VRF is reflective of the policy as a whole. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain low impact BES Cyber Systems.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-003-3, R1, which has an approved VRF of Lower but applies to Cyber Assets with an inherently lower risk; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to properly implement the cyber security policy would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

VRF and VSL Justifications – CIP-003-5, R2			
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The cyber security policy requirement encompasses a number of policy domains. The VRF is identified at the risk level represented by all of the policy domains in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 but did not identify, assess, or correct the	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 but did not identify, assess, or correct the deficiencies.	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify, assess, or correct the deficiencies.	The Responsible Entity did not document or implement any cyber security policies for assets with a low impact rating that address the topics as required by R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber

VRF and VSL Justifications – CIP-003-5, R2			
deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 15 calendar months but did complete this approval in less than or equal to 16 calendar	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R2)	security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 18 calendar months of the previous approval. (R2)

VRF and VSL Justifications – CIP-003-5, R2			
months of the previous approval. (R2)	approval. (R2)		

VRF and VSL Justifications – CIP-003-5, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps back to previously approved requirements CIP-003-3 R1 and CIP-003-3 R1.2. The VSLs were combined for these requirements using a gradated methodology. The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The Proposed VSLs are not binary and does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-003-5, R2	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security policies but fails to address one or more of the required topics. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The action of the requirement is to implement documented cyber security policies. Documentation of the policies is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the policy in this case; as such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the policy. The drafting team's intent is that this covers both documentation and implementation and, therefore,

VRF and VSL Justifications – CIP-003-5, R2	
documentation and implementation should account for their interdependence	accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-003-5, R3	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The identification of a single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization. Cyber security is not simply a technical endeavor. Failure to provide clear governance and organizational leadership may lead to ineffective controls, which could compromise security and, therefore, the integrity of the Bulk Electric System. Consequently, a VRF of Medium was selected.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement specifies that a CIP Senior Manager be identified. The VRF is only applied at the requirement level and the requirement parts are treated equally. As there are no requirement parts, the VRF is, therefore, consistent.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-003-3, R2, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Because the purpose of the Requirement is for entities to properly identify and document the CIP Senior Manager in order to ensure there is clear authority and ownership of the CIP program within an organization, this Requirement is appropriately assigned a Medium VRF.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement does not co-mingle more than one obligation. The only obligation included in requirement CIP-003-5 R1 is the identification of the CIP Senior Manager. Therefore, the requirement has a single VRF.

VRF and VSL Justifications – CIP-003-5, R3			
Proposed VSLs			
Lower	Moderate	High	Severe
The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)

VRF and VSL Justifications – CIP-003-5, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity identified its CIP Senior Manager but failed to document changes within the specified timeframes. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed Requirement, CIP-003-5 R3, maps to a previously approved requirement, CIP-003-3 R2. The proposed VSLs do not have the unintended consequence of lowering the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-003-5, R3	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this Requirement in that some measurable reliability benefit can be achieved if the Responsible Entity identified its CIP Senior Manager but failed to document changes within the specified timeframes.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	Not applicable since the requirement does not contain interdependent tasks of documentation and implementation.

VRF and VSL Justifications – CIP-003-5, R3	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-003-5, R4	
Proposed VRF	**LOWER**
NERC VRF Discussion	The reliability purpose of this requirement is to ensure clear lines of authority and ownership for security matters that could impact the stability and integrity of the Bulk Electric System, that delegations are kept up-to-date, and that individuals do not assume undocumented authority. As this requirement is only a part of the overall governance structure of a cyber security program, which includes additional leadership and policy, a VRF of Lower was assigned to this requirement.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement directs that the CIP Senior Manager is responsible for all approval and authorizations, but also grants the CIP Senior Manager with the ability to delegate this authority. The Requirement also calls for changes to the CIP Senior Manager and any delegations to be documented within 30 calendar days. The VRF is only applied at the requirement level, and the requirement parts are treated equally. The requirement does not contain parts and are, therefore, consistent.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-003-3, R 2.2 and R2.3, which has an approved VRF of Lower; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to show clear authorization for actions taken back to the CIP Senior Manager would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The obligation of this requirement is to demonstrate that the CIP Senior Manager is ultimately responsible for all approvals and authorizations required in the CIP Standards. This requirement allows for delegation,

VRF and VSL Justifications – CIP-003-5, R4			
	but also obligates the Responsible Entity to document these delegations. The VRF was chosen based upon the highest reliability risk objective, which is the clear line of authority to the CIP Senior Manager and are, therefore, consistent with VRF Guideline 5.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity failed to document the approval and authorization of one delegation (by title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of two delegations (by title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of three or more delegations (by title or name of the delegate) as required.

VRF and VSL Justifications – CIP-003-5, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to the violation, and the VSLs follow the guidelines for incremental violations. There is a single element upon which severity may be gradated; as such, gradated VSLs were assigned.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps back to a previously approved VSL in CIP-003-3 R2.2 and R2.3. The previously approved VSL was a binary Severe VSL. The SDT has determined that there are numerous delegations that take place, and there is a reliability benefit if the majority of those delegations are documented in compliance with the standard; and, as such, has assigned gradated VSLs to the requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore,

VRF and VSL Justifications – CIP-003-5, R4	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The requirement contains interdependent tasks of documentation and implementation. The VSL requirement presumes that the only way to demonstrate compliance is through documentation; as such, The VSLs are based upon the documentation measure, and implementation is assumed with documentation, therefore accounting for the interdependence in these tasks.

VRF and VSL Justifications – CIP-004-5, R1	
Proposed VRF	**LOWER**
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have awareness of sound security practices. Failure to meet this objective would not have adverse effect on the electrical state or capability of the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This Requirement calls for ongoing security awareness reinforcement. The VRF is only applied at the Requirement level and the requirement parts are treated equally. The single Requirement Part constitutes the required security awareness program.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-004-3, R1, which has an approved VRF of Lower; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to convey security awareness practices within a calendar quarter would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring individuals with access to BES Cyber Systems have awareness of sound security practices and, therefore, does not co-mingle more than one obligation.

VRF and VSL Justifications – CIP-004-5, R1			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)

VRF and VSL Justifications – CIP-004-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines —There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. The SDT has determined that there is a reliability benefit to partial compliance with this requirement and has therefore assigned gradated VSLs.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The Requirement maps to CIP-004-3 R1, which did not graduate VSLs according to the time beyond meeting a compliance obligation and accumulated violations as a single violation. This version corrects the oversight by gradating the violation based on the number of days past the performance requirement. Failure to meet the requirement by a given number of days appropriately maps to the severity of the violation.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore,

VRF and VSL Justifications – CIP-004-5, R1	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single lapse in protection of this Requirement does not compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-004-5, R2	
Proposed VRF	**LOWER**
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role. Failure to meet this objective would not have adverse effect on the electrical state or capability of the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for a training program for individuals needing or having access to the BES Cyber System. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-004-3, R2.2, which has an approved VRF of Medium. In this version, the training program requirements are distinct from the implementation, and the implementation in R3 has the previously approved VRF of Medium.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have a training program would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role and, therefore, does not co-mingle more than one obligation.

VRF and VSL Justifications – CIP-004-5, R2			
Proposed VSLs			
Lower	Moderate	High	Severe
The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP

VRF and VSL Justifications – CIP-004-5, R2			
the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)

VRF and VSL Justifications – CIP-004-5, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to CIP-004-3 R2.2, which did not graduate VSLs and treats all violations equally. This version corrects the oversight by gradating the violation based on the number of training elements missing in the program. Failure to meet the parts of the requirement appropriately maps to the severity of the violation.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-004-5, R2	
Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single failure of this requirement does not compromise network computer security.

VRF and VSL Justifications – CIP-004-5, R2	
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	This VSL accounts for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation.

VRF and VSL Justifications – CIP-004-5, R3	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role. Failure to meet this objective could affect the electrical state or capability of the Bulk Electric System. However, it is unlikely to lead to instability.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for implementing a training program for individuals needing or having access to the BES Cyber System. The VRF is only applied at the Requirement level and the requirement parts are treated equally. Each Requirement Part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards.

VRF and VSL Justifications – CIP-004-5, R3			
	This requirement maps from CIP-004-3, R2, which has an approved VRF of Medium.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement a security training program could effect the electrical state or capability of the Bulk Electric System. However, it is unlikely to lead to instability.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel

VRF and VSL Justifications – CIP-004-5, R3			
The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)	Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR

VRF and VSL Justifications – CIP-004-5, R3			
the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the	correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals, and did not

VRF and VSL Justifications – CIP-004-5, R3			
previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)		identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

VRF and VSL Justifications – CIP-004-5, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The Requirement maps to CIP-004-3 R2.2, which did not gradate VSLs and treats all violations equally. This version more appropriately gradates the violation based on the number of individuals with access to BES Cyber Systems who did not receive training. Failure for a given number of individuals to receive training appropriately maps to the severity of the violation.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-004-5, R3	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations. The requirement is to implement a training program and failure for a single individual to have training does not necessarily imply a single violation. An overall view of the training program must consider the number of individuals who failed to receive training for a given period.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single failure of this requirement does not compromise network computer security. Although failure to implement a training program could associatively affect the ways in which computer network security applies, it does not, by itself, indicate a failure of computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	This Requirement pertains to implementing the cyber security program and does not require procedural documentation.

VRF and VSL Justifications – CIP-004-5, R3	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-004-5, R4			
Proposed VRF	**LOWER**		
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have received a personnel risk assessment. Failure to meet this objective could have adverse effect on the electrical state or capability of the Bulk Electric System, but it is not expected to cause Bulk Electric System instability.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This Requirement calls for a personnel risk assessment program for individuals needing or having access to a BES Cyber System. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement's VRF is consistent with similar security requirements with similar risks in the other CIP standards.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have a personnel risk assessment program could have adverse effect on the electrical state or capability of the Bulk Electric System, but it is not expected to cause Bulk Electric System instability.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that documentation a personnel risk assessment is developed for individuals with access to BES Cyber Systems and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not	The Responsible Entity did not	The Responsible Entity did not	The Responsible Entity did not

VRF and VSL Justifications – CIP-004-5, R4			
verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter, and did not identify, assess and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.3)	verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the	verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR	implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2)

VRF and VSL Justifications – CIP-004-5, R4			
OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)	deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information

VRF and VSL Justifications – CIP-004-5, R4			
			storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)

VRF and VSL Justifications – CIP-004-5, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The Requirement maps to CIP-004-3 R3, which gradates the VSLs based on implementation of the Requirement. This does not lower the current level of compliance because new components of the program have been added.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-004-5, R4	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Failure to document or implement all required documented program(s) has a binary Severe VSL. Other Requirement Parts associated with the required processes do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-004-5, R4	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-004-5, R5	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This Requirement ensures prompt revocation of access for individuals no longer needing access to BES Cyber Systems and BES Cyber System Information. Failure to revoke access to BES Cyber Systems and BES Cyber System Information within the required time frame is an administrative requirement and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for procedures to revoke access to BES Cyber Systems and BES Cyber System Information when individuals no longer need access. The VRF is only applied at the requirement level, and the Requirement Parts are treated equally. Each Requirement row contributes to the objective of this Requirement.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-004-3 R4.2, which has an approved VRF of Lower, and CIP-007-3 R5.2.3., which has an approved VRF of Medium. The Requirement only addresses the securing of shared accounts for termination in CIP-007-3 R5.2.3, and not the audit trail. Because the securing of shared accounts upon termination is consistent with CIP-004-3 R4.2, then we can imply a VRF of lower for that component of the Requirement. Therefore, the proposed VRF is consistent with the approved VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to revoke access to BES Cyber Systems and BES Cyber System Information may impact the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, this Requirement, if violated, could directly affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. Requirement R5 requires prompt revocation of access for individuals no longer needing access to BES

VRF and VSL Justifications – CIP-004-5, R5			
	Cyber Systems and BES Cyber System Information. Each part of Requirement R5 specifies the obligations to revoke access in various situations when an individual no longer needs such access.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1)

VRF and VSL Justifications – CIP-004-5, R5			
do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more	for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

VRF and VSL Justifications – CIP-004-5, R5			
process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances, and did not identify, assess, and correct the deficiencies. (5.5)			

VRF and VSL Justifications – CIP-004-5, R5	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSL gradates the severity based on whether the violation includes a scenario whether the individual no longer needed access, when an individual was terminated for cause, or when both occurred. The requirement no longer differentiates on scenarios of termination for cause.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-004-5, R5	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Failure to implement programs for access revocation has a binary Severe VSL. A single lapse in protection of this Requirement does not compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	This requirement does not specify a lower VSL for lack of documentation.

VRF and VSL Justifications – CIP-004-5, R5	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-005-5, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This requirement ensures that all BES Cyber Systems are within an Electronic Security Perimeter and that all electronic routable communication and dialup communication across the perimeter is secured. Failure to properly secure the external communications to the BES Cyber Systems and the networks on which they reside could result in unauthorized access, which could directly affect the ability to control the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the requirement parts are treated equally. Both Requirements in CIP-005 are of the same VRF as both insure the proper electronic security perimeter based controls are in place for preventing unauthorized access.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement's VRF is consistent with similar security requirements with similar risks in the other CIP standards.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement documented processes and adequate safeguards to prevent unauthorized access to an entity's networks could result in unauthorized access and potential disruption of monitoring and logical control of BES Cyber Assets. Consistent with the definition of a Medium VRF, unauthorized logical access could directly affect the electrical state or the capability of the Bulk Electric System and the ability to monitor and control the BES.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R1 have a common set of objectives to ensure access to BES Cyber Systems is authorized and protected. The obligations within the requirement collectively address the objective and only one VRF is assigned.

VRF and VSL Justifications – CIP-005-5, R1			
Proposed VSLs			
Lower	Moderate	High	Severe
N/A	N/A	The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for CIP-005-5 Table R1 – Electronic Security Perimeter. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

VRF and VSL Justifications – CIP-005-5, R1			
			OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)

VRF and VSL Justifications – CIP-005-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSL's are in line with the currently approved VSL's in CIP-005-3a and therefore do not lower the current compliance level.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-005-5, R1	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	With the exception of the portion of the VSLs dealing with the method aspect of the Requirement, the proposed VSL is binary and assigns a “Severe” category for the violation of the Requirement.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the ‘weakest link’ characteristic, should apply binary VSLs	A single violation of this requirement particularly at the Severe VSL category could result in an individual obtaining unauthorized access to BES Cyber Systems. Since the Electronic Security Perimeter is one of the first level of defenses around a network (or dialup modem) containing BES Cyber Systems, any lack of implemented requirements is a binary VSL. The gradation in the VSL is for lacking documentation only. The existence of a particular ‘state’ regarding documented and implemented processes does not alone constitute the likelihood of exploitation. Several factors centered on intent, motivation, and capabilities and lack of other mitigating controls would necessarily also determine System vulnerability as well as the impact rating of the BES Cyber System in question.
FERC VSL G6 VSLs for cyber security requirements containing	Due to the increased scope of Version 5 and the corresponding increase in the number of declared Electronic Security Perimeters and therefore the order of magnitude more ports and services that will be in scope among other things, the VSL for documentation purposes only has been gradated. Any lapse in the implementation of the actual security controls remains binary.

VRF and VSL Justifications – CIP-005-5, R1	
interdependent tasks of documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-005-5, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This requirement ensures that interactive remote access to BES Cyber Systems includes documented processes and safeguards to prevent unauthorized access to an entity's networks. Failure to use intermediate devices and establish robust authentication and encryption techniques could result in unauthorized access, which could directly affect the ability to control the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for specific intermediate devices to work in conjunction with authentication and encryption procedures for access to BES Cyber Systems. The VRF is only applied at the requirement level, and the requirement parts are treated equally. Use of intermediate devices with proper authentication and encryption procedures for access share a common objective of preventing unauthorized access.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement documented processes and adequate safeguards to prevent unauthorized access to an entity's networks could result in unauthorized access and potential disruption of monitoring and logical control of BES Cyber Assets. Consistent with the definition of a Medium VRF, unauthorized logical access could directly affect the electrical state or the capability of the Bulk Electric System and the ability to monitor and control the BES.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R2 have a common set of objectives to ensure interactive remote access to BES Cyber Systems is authorized and protected. The obligations to place an inclusive subset of protective measures

VRF and VSL Justifications – CIP-005-5, R2			
	in place to authorize interactive remote access contribute collectively to the objective and only one VRF is assigned.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3.

VRF and VSL Justifications – CIP-005-5, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This is a new requirement, so this section is not applicable.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-005-5, R2	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this requirement at the low, moderate, or high VSL category would not necessarily result in an individual obtaining unauthorized interactive remote access to BES Cyber Systems. The existence of a particular 'state' regarding documented and implemented processes does not alone constitute the likelihood of exploitation. Several factors centered on intent, motivation, and capabilities and lack of other mitigating controls would necessarily also determine system vulnerability.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The action of the requirement is to implement documented cyber security policies. Documentation of the policies is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the policy in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the policy. The drafting team's intent is that this covers both documentation and implementation and,

VRF and VSL Justifications – CIP-005-5, R2	
documentation and implementation should account for their interdependence	therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-006-5, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this Requirement. The requirement specifies that each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets. Failure to restrict physical access to BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets could result in unauthorized access, which could directly affect the ability to monitor or control the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-006-3, R1, which has an approved VRF of Medium; and, therefore, the proposed VRF for CIP-006-5, R1 is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-006-5, Requirement R1 requires the implementation of documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control

VRF and VSL Justifications – CIP-006-5, R1			
	Systems and Protected Cyber Assets. A failure to implement these documented plans may impact the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, this requirement, if violated, could directly affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that Responsible Entities implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8) OR	The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for	The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not

VRF and VSL Justifications – CIP-006-5, R1			
The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry but did not identify, assess, or correct the deficiencies. (1.8) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)	unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)	process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5) OR The Responsible Entity has a process to monitor for	assess or correct the deficiencies. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified deficiencies, but did not assess or

VRF and VSL Justifications – CIP-006-5, R1			
		unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.6) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)	correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified

VRF and VSL Justifications – CIP-006-5, R1			
			deficiencies, but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and

VRF and VSL Justifications – CIP-006-5, R1			
			identified deficiencies, but did not assess or correct the deficiencies. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each

VRF and VSL Justifications – CIP-006-5, R1			
			Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel(1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical

VRF and VSL Justifications – CIP-006-5, R1			
			access logs for 90 calendar days. (1.9)

VRF and VSL Justifications – CIP-006-5, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSLs are in line with the currently approved VSLs in previous versions and therefore do not lower the current compliance level.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-006-5, R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The Requirement Parts for restricting access have a binary Severe VSL. Other Requirement Parts associated with the physical security plan do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security	Failure to document processes carries a Severe VSL.

VRF and VSL Justifications – CIP-006-5, R1	
requirements containing interdependent tasks of documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-006-5, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. This Requirement calls for one or more documented visitor control programs. Failure to implement a visitor control program is not expected to directly affect the electrical state or capability of the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for one or more documented visitor control programs. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-006-3, R1.6, which has an approved VRF of Medium; and, therefore, the proposed VRF for CIP-006-5, R2 is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement a documented visitor control program is an administrative requirement, and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that Responsible Entities implement one or more documented visitor control programs and, therefore, does not co-mingle more than one obligation.

VRF and VSL Justifications – CIP-006-5, R2			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity included a visitor control program that requires logging of each of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or correct the deficiencies. (2.2) OR	The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1) OR The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)

VRF and VSL Justifications – CIP-006-5, R2			
	The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)		

VRF and VSL Justifications – CIP-006-5, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSL's are in line with the currently approved VSL's in CIP-006-3 and therefore do not lower the current compliance level.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-006-5, R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this Requirement at the low, moderate, or high VSL category would not necessarily compromise computer network security. The Requirement to further restrict access to only authorized individuals would compensate this control.
FERC VSL G6 VSLs for cyber security	Failure to document processes carries a Severe VSL and therefore recognizes the linkage between documentation and implementation.

VRF and VSL Justifications – CIP-006-5, R2	
requirements containing interdependent tasks of documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-006-5, R3	
Proposed VRF	**LOWER**
NERC VRF Discussion	A VRF of Lower is assigned to this requirement. This Requirement calls for one or more documented Physical Access Control System maintenance and testing programs. Failure to implement Physical Access Control System maintenance and testing would not be expected to directly or adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. A VRF assignment of Lower is, therefore, justified.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for one or more documented Physical Access Control System maintenance and testing programs. The VRF is only applied at the requirement level and the Requirement Parts are treated equally. Each Requirement Part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement's VRF is consistent with similar administrative Requirements with similar risks in other NERC Reliability Standards.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement Physical Access Control System maintenance and testing programs is an administrative Requirement, and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation.

VRF and VSL Justifications – CIP-006-5, R3			
	The proposed Requirement has a single objective of ensuring that Responsible Entities implement one or more Physical Access Control System maintenance and testing programs and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	The Responsible Entity has not documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

VRF and VSL Justifications – CIP-006-5, R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSLs are in line with the currently approved VSLs in CIP-006-3 and therefore do not lower the current compliance level.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-006-5, R3	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Performing the maintenance activity obligations provides additional assurance in the physical security controls in place, but failure to do so would not necessarily compromise computer network security given other protections. Other Requirement Parts associated with physical security controls do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-006-5, R3	
requirements containing interdependent tasks of documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-007-5, R1			
Proposed VRF	**MEDIUM**		
NERC VRF Discussion	The Requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and physical I/O ports. Depending on the port and the impact classification of the affected cyber asset, a violation could lead to affecting the monitoring or control of a BES asset.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the Requirement level, and the Requirement Parts are treated equally. Unprotected logical and physical ports are both access points into a BES Cyber System.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-007-3, R4, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to disable or prevent access to a single logical or physical port on one BES Cyber System is unlikely to lead to Bulk Electric System instability, separation, or cascading failures. Therefore, this Requirement was assigned a Medium VRF.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. Unprotected logical and physical ports are both access points into a BES Cyber System.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity has implemented and documented	The Responsible Entity has implemented and documented	The Responsible Entity did not implement or document one or

VRF and VSL Justifications – CIP-007-5, R1			
	processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)	processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)	more process(es) that included the applicable items in *CIP-007-5 Table R1* and has identified deficiencies but did not assess or correct the deficiencies. (R1) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* but did not identify, assess, or correct the deficiencies. (R1)

VRF and VSL Justifications – CIP-007-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The Requirement maps to CIP-004-3 R2.2, which did not gradate VSLs and treats all violations equally. This version provides more appropriate gradation of the VSLs while still providing a Severe VSL for all types of egregious failures.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-007-5, R1	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this Requirement at the moderate or high VSL category would not necessarily compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-5, R1	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-007-5, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	The Requirement requires entities to manage security patches in a proactive way by monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner. Depending on the patch and the impact classification of the affected Cyber Asset, a violation could lead to affecting the monitoring or control of a BES asset.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the requirement parts are treated equally. The parts are required parts of a single process.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-007-3, R3, which has an approved VRF of Lower. This version more appropriately assigns a VRF as Medium given other changes in the Requirement. Failure for a given number of individuals to receive training appropriately maps to the severity of the violation.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to manage a security patch on one BES Cyber System is unlikely to lead to BES instability.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The Requirement does not co-mingle more than one obligation. It defines required steps in a single process.

VRF and VSL Justifications – CIP-007-5, R2			
Proposed VSLs			
Lower	Moderate	High	Severe
The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* but did not identify, assess, or correct the deficiencies. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber

VRF and VSL Justifications – CIP-007-5, R2			
evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the deficiencies. (2.3)	Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released	documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)	security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate and has identified deficiencies but did not assess or correct the

VRF and VSL Justifications – CIP-007-5, R2			
OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion and has identified deficiencies but did	OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or	deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity

VRF and VSL Justifications – CIP-007-5, R2			
	not assess or correct the deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	revise an existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or correct the deficiencies. (2.4)

VRF and VSL Justifications – CIP-007-5, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines— There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This Requirement maps to a previously approved VSL for CIP-007-3 R3. The proposed version more appropriately gradates the violation, which is scaled to the risk created by the severity of violation.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-007-5, R2	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A violation of this Requirement does not necessarily compromise computer network security. Failure to implement a security patch can increase the vulnerability of the BES Cyber System, but several other required protections would have to concurrently fail for actuating the vulnerability. There may be instances where the security vulnerability is so severe that failure to patch alone can comprise computer network security, but these cases are the exception.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a process as a Severe violation while also accounting for the failure to implement the process using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-5, R2	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-007-5, R3			
Proposed VRF	**MEDIUM**		
NERC VRF Discussion	The requirement requires entities to have processes to limit and detect the introduction of malicious code onto the components of a BES Cyber System. Depending on the malware and the impact classification of the affected Cyber Asset, a violation could lead to affecting the monitoring or control of a BES asset.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the Requirement Parts are treated equally. The parts are required parts of a single process.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-007-3, R4, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to manage malicious code on one BES Cyber System is unlikely to lead to BES instability.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirement does not co-mingle more than one obligation. It defines required steps in a single process.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table*

VRF and VSL Justifications – CIP-007-5, R3			
	are used, the Responsible Entity did not address testing the signatures or patterns and has identified deficiencies but did not assess or correct the deficiencies. (3.3) OR The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)	not mitigate the threat of detected malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and did not identify, assess, or correct the deficiencies. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and has identified deficiencies but did not assess or correct the deficiencies. (3.3)	*R3* and has identified deficiencies but did not assess or correct the deficiencies. (R3) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R3* and did not identify, assess, or correct the deficiencies. (R3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.1) OR The Responsible Entity has implemented one or more

VRF and VSL Justifications – CIP-007-5, R3			
		OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies. (3.3)	documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies. (3.1)

VRF and VSL Justifications – CIP-007-5, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This Requirement maps to a previously approved VSL for CIP-007-3 R4. The proposed version includes a time-based gradation for applying malicious code protection updates which violation intended to match to the degree of severity the violation would pose to the BES.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-007-5, R3	
Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A violation of this Requirement does not necessarily compromise computer network security. Failure to implement malicious code protections can increase the vulnerability of the BES Cyber System, but several other required protections would have to concurrently fail for actuating the vulnerability.
FERC VSL G6 VSLs for cyber security requirements containing	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a process as a Severe violation while also accounting for the failure to implement the process using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-5, R3	
interdependent tasks of documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-007-5, R4	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	The requirement requires entities to have processes to provide security event monitoring with the purpose of detecting unauthorized access, reconnaissance, and other malicious activity on BES Cyber Systems and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the immediate detection of an incident and (2) useful evidence in the investigation of an incident. Depending on the impact classification of the affected Cyber Asset, a violation could lead to affecting the monitoring or control of a BES asset.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the requirement parts are treated equally. The parts are required parts of a single process.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-007-3, R6, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to manage security events on one BES Cyber System is unlikely to lead to BES instability.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirement does not co-mingle more than one obligation. It defines required steps in a single process.

VRF and VSL Justifications – CIP-007-5, R4			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and has identified deficiencies but did not assess or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4* and has identified deficiencies but did not assess or correct the deficiencies. (R4) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4* and did not identify, assess, or correct the deficiencies. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of

VRF and VSL Justifications – CIP-007-5, R4			
summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and has identified deficiencies but did not assess or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1	the required types of events described in 4.1.1 through 4.1.3 and has identified deficiencies but did not assess or correct the deficiencies. (4.1) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct the deficiencies. (4.1)

VRF and VSL Justifications – CIP-007-5, R4			
		(where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify	

VRF and VSL Justifications – CIP-007-5, R4			
		undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)	

VRF and VSL Justifications – CIP-007-5, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This Requirement maps to a previously approved VSL for CIP-007-3 R5. The proposed version also includes the new requirement to manually review logs.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-007-5, R4	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated Requirement and are, therefore, consistent with the Requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The Requirement Parts for logging required types of events have a binary Severe VSL. Other Requirement Parts associated with security event monitoring do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-5, R4	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-007-5, R5	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This Requirement ensures that Responsible Entities establish, implement, and document controls for electronic access to BES Cyber Systems. This includes enforcement of authentication for all user access and CIP Senior Manager, or delegate authorization for use of administrator, shared, default, and other generic account types. It prescribes procedural controls and conditions for changing default passwords and enforcing specific parameters for password based user authentication. Finally, it helps establish a process to limit (where technically feasible) unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This Requirement calls for specific actions represented by multiple sub-requirements with a common set of objectives – to ensure the appropriate controls are in place for authorizing and establishing secure electronic access to BES Cyber Systems.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps to CIP-007-4 R5, which has an approved VRFs of Lower and Medium; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement CIP Senior Manager oversight and establish controls to protect BES Cyber Systems from unauthorized electronic access could result in unauthorized access and could directly affect the ability to monitor or control the BES. Although the previous standards versions assigned a VRF of Severe, this is not consistent with the projected risk of BES Cyber System exploitation, which is why the VRF has been modified to Medium.

VRF and VSL Justifications – CIP-007-5, R5			
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The Requirements in R5 have a common objective to provide controls to protect against unauthorized electronic access to BES Cyber Systems. The Requirements to authorize and review access, and the provided technical and procedural controls to prevent unauthorized access both specify the obligations to provide strong controls to monitor and control electronic access.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and has identified deficiencies but did not assess or correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and has identified deficiencies but did not assess or correct the deficiencies. (R5) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5) OR The Responsible Entity has

VRF and VSL Justifications – CIP-007-5, R5			
implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and has identified deficiencies but did not assess or correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did	implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and has identified deficiencies but did not assess or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and did not identify, assess, or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did

VRF and VSL Justifications – CIP-007-5, R5			
		not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce	not, per device capability, change known default passwords and has identified deficiencies but did not assess or correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and

VRF and VSL Justifications – CIP-007-5, R5			
		one of the two password parameters as described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for	has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last

VRF and VSL Justifications – CIP-007-5, R5			
		password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or

VRF and VSL Justifications – CIP-007-5, R5			
			generate alerts after a threshold of unsuccessful authentication attempts and has identified deficiencies but did not assess or correct the deficiencies. (5.7) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7)

VRF and VSL Justifications – CIP-007-5, R5	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The previous binary VSL for this Requirement has not proven accurate after several iterations of its application. Account access management and procedures for monitoring and controlling access are complex with an often intensive scope. Errors resulting in potential or single instances of unauthorized access do not have the same criticality as multiple instances and blatant lack of controls.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-007-5, R5	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations. Gradations are based on the number of unidentified account types, or number of missed controls for authentication and access represent components of the overall requirement that are necessary to fully achieve the reliability of the main requirement.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The Requirement parts that can compromise computer network security have a Severe VSL. Other Requirement Parts associated with system access control do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-5, R5	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-008-5, R1	
Proposed VRF	**LOWER**
NERC VRF Discussion	This requires each Responsible Entity to have a plan to respond to Cyber Security Incidents. Failure to have an incident response plan could delay recovery actions and hinder entities in understanding and reporting the incident. The planning component of the Requirement is administrative in nature and, if violated, would not be expected to affect the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for procedures to respond to Cyber Security Incidents. The VRF is only applied at the requirement level and the Requirement Parts are treated equally. Each requirement part is a necessary component of an incident response plan.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-008-3 R1, which has an approved VRF of Lower.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have an incident response plan could delay recovery actions and hinder entities in understanding and reporting the incident. The planning component of the Requirement is administrative in nature and, if violated, would not be expected to affect the BES.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R1 have a common objective of having a plan for responding to, handling, and reporting Cyber Security Incidents. These contribute to the overall objective to minimize the loss and destruction of Cyber Security Incidents and providing timely information about the incident.

VRF and VSL Justifications – CIP-008-5, R1			
Proposed VSLs			
Lower	Moderate	High	Severe
N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but did not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security

VRF and VSL Justifications – CIP-008-5, R1			
			Incident. (1.2)

VRF and VSL Justifications – CIP-008-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this Requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This Requirement maps from CIP-008-3 R1 and has similar VSL assignments. The previously approved VSL differentiated between High and Severe on the basis of whether the entity had maintained the plan. The change made to this version differentiates based on specific components of the plan, which provides more objectivity.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-008-5, R1	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this Requirement indicates an entity does not have a documented and consistent response to a Cyber Security Incident, but a single lapse in protection would not be expected to compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-008-5, R1	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-008-5, R2			
Proposed VRF	**LOWER**		
NERC VRF Discussion	This Requirement ensures entities implement their incident response plan(s). Failure to implement the incident response plan is an administrative requirement and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. Each Requirement row contributes to the common objective of implementing the incident response plan. The Requirement to retain incident documentation ensures the entity can review actual incidents at a later date.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-008-3 R1.6 and R2, which has an approved VRF of Lower.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement the incident response plan is an administrative Requirement and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The Requirements in R2 have a common objective of implementing incident response plans. Requirement Row 2.1 specifies the obligation to implement the plan during an incident, and Requirement Row 2.2 specifies the obligation to periodically exercise the plan. Requirement Row 2.3 specifies the obligation to retain incident documentation to ensure the entity can review actual incidents at a later date.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has not	The Responsible Entity has not	The Responsible Entity has not	The Responsible Entity has not

VRF and VSL Justifications – CIP-008-5, R2			
tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)

VRF and VSL Justifications – CIP-008-5, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed version more appropriately gradates the violation, which is scaled to the risk created by the severity of violation.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-008-5, R2	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	This requirement maps from CIP-008-3 R1 and has similar VSL assignments. The previously approved VSL was binary. The change made to this version differentiates based on the number of days late in a time-based performance. This reflects the lesser degree of risk posed to BES reliability for exceeding timed requirements. New requirements have also been incorporated into the VSL.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single lapse in protection of this Requirement does not compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-008-5, R2	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-008-5, R3			
Proposed VRF	**LOWER**		
NERC VRF Discussion	This Requirement ensures incident response plans remain up-to-date and that individuals with responsibilities in the plans have the most current version.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. Each Requirement row contributes to the common objective of keeping response plans up-to-date and communicating changes to individuals with responsibilities in the plans. The obligations to keep the response plans up-to-date include changes in response to lessons learned in an incident or organizational and technology changes.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-008-3 R1.4 and R1.5, which has an approved VRF of Lower.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to update and communicate changes to the incident response plan(s) are administrative requirements and are not expected to adversely affect the electrical state or capability of the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R2 have a common objective of keeping response plans up-to-date and communicating changes to individuals with responsibilities in the plans.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has not notified each person or group with a defined role in the Cyber	The Responsible Entity has not updated the Cyber Security	The Responsible Entity has neither documented lessons learned nor	The Responsible Entity has neither documented lessons learned nor

VRF and VSL Justifications – CIP-008-5, R3			
Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60	documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the	documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

VRF and VSL Justifications – CIP-008-5, R3			
	and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

VRF and VSL Justifications – CIP-008-5, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this Requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed Requirement has more specificity about reviewing and updating the plan than prior versions of the standard, and the failure to update the plan in a timely manner has less of an impact than not performing the review at all.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-008-5, R3	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this Requirement should not compromise the security of the BES Cyber System because this is in response to an incident which has already occurred,
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-008-5, R3	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-009-5, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This requires each Responsible Entity have a plan to recover to BES Cyber Systems. Failure to have a recovery plan could increase the downtime and destruction in a hazardous situation, which could affect the ability to effectively monitor, control, or restore the Bulk Electric System in an Emergency situation.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for procedures to recover BES Cyber Systems. The VRF is only applied at the requirement level, and the requirement parts are treated equally. Each Requirement Part is a necessary component of a recovery plan.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-009-3 R1, which has an approved VRF of Medium.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have a recovery plan could increase the downtime and destruction in a hazardous situation, which could affect the ability to effectively monitor, control, or restore the Bulk Electric System in an Emergency situation.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R1 have a common objective of having a plan for recovering BES Cyber Systems. These contribute to the overall objective to minimize downtime and destruction in a hazardous situation. T he requirement to preserve data during recovery provides information for post-event analysis, but this requirement best fits here because it involves the actions taken during recovery.

VRF and VSL Justifications – CIP-009-5, R1			
Proposed VSLs			
Lower	Moderate	High	Severe
N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

VRF and VSL Justifications – CIP-009-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this Requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This Requirement maps from CIP-009-3 R1, and has similar VSL assignments. The previously approved VSL did not have a differentiation between having a plan and missing some elements of the plan, but the severity of not having a plan is higher than missing a single element in a plan.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-009-5, R1	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this Requirement indicates an entity has not created recovery plan(s) for BES Cyber Systems, but a single lapse in protection would not be expected to compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	This requirement only specifies documentation, and not implementation.

VRF and VSL Justifications – CIP-009-5, R1	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-009-5, R2			
Proposed VRF	**LOWER**		
NERC VRF Discussion	This Requirement's VRF is consistent with similar administrative Requirements with similar risks in other NERC Reliability Standards.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. Each Requirement row contributes to the common objective of implementing and maintaining the recovery plan.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-009-3 R2, R4, and R5, which has an approved VRF of Lower.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement and maintain the recovery plan is an administrative Requirement and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R2 have a common objective of implementing and maintaining recovery plans. Requirement Rows 2.1 and 2.3 specify the obligation to implement and test the plan. Requirement Row 2.2 specifies the obligation to maintain backup information used to recover the BES Cyber System.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18

VRF and VSL Justifications – CIP-009-5, R2			
15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months	exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, and when	calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and	calendar months between tests of the plan. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR

VRF and VSL Justifications – CIP-009-5, R2			
between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	tested, any deficiencies were identified, assessed, and corrected. (2.3)	corrected. (2.3)	The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR

VRF and VSL Justifications – CIP-009-5, R2			
			The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)

VRF and VSL Justifications – CIP-009-5, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The Requirement maps to CIP-009-3 R2 and R3 and adds the obligation to perform a full operational exercise. The portions of the Requirement from CIP-009-3 carry forward similar VSLs, and the failure to perform a full operational exercise is proposed as a High VSL because it does not carry the same potential consequence of not having exercised the recovery plan. In addition, the proposed VSLs gradate failure to perform a test of the recovery plan based on the amount of time lapse between tests. This more appropriately reflects the severity of the corresponding type of violation.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-009-5, R2	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A violation of this requirement indicates the recovery plan was not properly tested and may have deficiencies, but a violation cannot immediately compromise computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	This Requirement does not specify a lower VSL for lack of documentation.

VRF and VSL Justifications – CIP-009-5, R2	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-009-5, R3			
Proposed VRF	**LOWER**		
NERC VRF Discussion	This Requirement ensures BES Cyber System plans remain up-to-date and effective and that individuals with responsibilities in the plans have the most current version.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. Each Requirement row contributes to the common objective of keeping recovery plans up-to-date and effective.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. The assignment of a Lower VRF is consistent of the impact of a violation of this Requirement and is therefore consistent among Reliability Standards.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to review, update or communicate changes to the recovery plan is administrative in nature and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The Requirements in R2 have a common objective of keeping response plans up-to-date and effective.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of

VRF and VSL Justifications – CIP-009-5, R3			
update being completed. (3.1.3)	each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or Technology changes.	each recovery plan test or actual recovery. (3.1.1)

VRF and VSL Justifications – CIP-009-5, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed Requirement has more specificity about reviewing and updating the plan than prior versions of the standard, and the failure to update the plan in a timely manner has less of an impact than not performing the review at all.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are,

VRF and VSL Justifications – CIP-009-5, R3	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and are not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this Requirement should not compromise the security of the BES Cyber System because this is in response to an incident which has already occurred.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-010-1, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The requirement calls for the implementation of one of more documented configuration change management processes. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration. The impact of a failure to implement documented configuration change management processes can have a medium impact on the reliability and operability of the BES. Although the requirement is administrative in nature and is a requirement that, if violated, poses the potential to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement calls for the implementation of one of more documented processes in relation to configuration change management. The VRF is only applied at the requirement level and the requirement parts are treated equally. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. CIP-010-1, R1 specifies the implementation of documented configuration change management processes in conjunction with CIP-010-1, R2, which specifies the implementation of documented configuration monitoring processes. Both requirements have a medium risk impact of a violation to implement their documented processes and, therefore, have a Medium VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-010-1, Requirement R1 requires the implementation of documented configuration change

VRF and VSL Justifications – CIP-010-1, R1			
	management processes. A failure to implement these documented processes has medium impact on the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, the requirement is a requirement that, if violated, poses the potential to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. CIP-010-1, Requirement R1 addresses a single objective and has a single VRF.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies.	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)

VRF and VSL Justifications – CIP-010-1, R1			
OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not	did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the	(1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) that requires authorization and	OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify,

VRF and VSL Justifications – CIP-010-1, R1			
identify, assess, or correct the deficiencies in the verification documentation. (1.4.3)	deficiencies. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the determination of affected security controls. (1.4.1)	documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.3)	assess, and correct the deficiencies. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity

VRF and VSL Justifications – CIP-010-1, R1			
		OR The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2) OR The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the required controls. (1.4.2) OR The Responsible Entity has a	does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected

VRF and VSL Justifications – CIP-010-1, R1			
		process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments	following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

VRF and VSL Justifications – CIP-010-1, R1			
		and identified deficiencies but did not assess or correct the deficiencies. (1.5.2) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)	

VRF and VSL Justifications – CIP-010-1, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed Requirement is new and has no mapping to a Requirement in a previous NERC CIP Standards Version. It does not have the unintended consequence of lowering the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore,

VRF and VSL Justifications – CIP-010-1, R1	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single lapse in protection is not expected to compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	CIP-010-1, Requirement R1 specifies that a Responsible Entity must implement and document the processes for configuration change management of BES Cyber Assets and BES Cyber Systems. Documentation of these processes is required, but this documentation is not the primary objective of the requirement. Documentation is interdependent with the implementation of the processes in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the configuration change management process. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-010-1, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The requirement calls for the implementation of one of more documented configuration monitoring processes. A VRF assignment of Medium is consistent with the lower risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration. The impact of a failure to implement documented configuration monitoring processes has medium impact on the reliability and operability of the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement calls for the implementation of one of more documented processes in relation to configuration monitoring. The VRF is only applied at the requirement level and the requirement parts are treated equally. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. CIP-010-1, R2 specifies the implementation of documented configuration monitoring processes in conjunction with CIP-010-1, R1, which specifies the implementation of documented configuration change management processes. Both requirements have a medium risk impact of a violation to implement their documented processes and, therefore, have a Medium VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-010-1, Requirement R2 requires the implementation of documented configuration monitoring processes. A failure to implement these documented processes has medium impact on the reliability and operability of the BES.

VRF and VSL Justifications – CIP-010-1, R2			
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. CIP-010-1, Requirement R2 addresses a single objective and has a single VRF.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days and identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented a

VRF and VSL Justifications – CIP-010-1, R2			
			process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days but did not identify, assess, or correct the deficiencies. (2.1)

VRF and VSL Justifications – CIP-010-1, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines — Severe: the performance measured does not substantively meet the intent of the Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed Requirement is new and has no mapping to a Requirement in a previous NERC CIP Standards Version. It does not have the unintended consequence of lowering the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSL is binary and assigns a "Severe" category for the violation of the Requirement.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the	The proposed VSLs use the same terminology as used in the associated Requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-010-1, R2	
Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The VSL is binary.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	CIP-010-1, Requirement R2 specifies that a Responsible Entity must implement and document the processes for configuration monitoring of BES Cyber Assets and BES Cyber Systems. Documentation of these processes is required, but this documentation is not the primary objective of the requirement. Documentation is interdependent with the implementation of the processes in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the configuration monitoring process. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-010-1, R3	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The Requirement calls for the implementation of one of more documented vulnerability assessment processes. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to act as a component in an overall program to periodically ensure the proper implementation of security controls of BES Cyber Assets and BES Cyber Systems. Failure to implement vulnerability assessment processes may impact the reliability and operability of the BES. The requirement is a requirement that, if violated, could directly affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement calls for the implementation of one of more documented vulnerability assessment processes. The VRF is only applied at the requirement level and the requirement parts are treated equally. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to act as a component in an overall program to periodically ensure the proper implementation of security controls of BES Cyber Assets and BES Cyber Systems.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. Requirement Part 3.1 maps from CIP-005-4, R4 (which has an assigned VRF of Medium) and CIP-007-4, R8 (which has an assigned VRF of Lower), Requirement Part 3.2 is a new requirement, while Requirement Part 3.3 maps from CIP-005-4, R4.5 (which has an assigned VRF of Medium) and CIP-007-4, R8.4 (which has an assigned VRF of Medium). Most of the aforementioned requirements had an approved VRF of Medium and, therefore, the proposed VRF for CIP-010-1, R3 is consistent. While the drafting team

VRF and VSL Justifications – CIP-010-1, R3			
	recognizes that CIP-007-4, R8 was assigned a VRF of Lower, to maintain consistency among reliability standards, an assigned VRF of Medium is appropriate.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-010-1, Requirement R3 requires the implementation of documented vulnerability assessment processes. A failure to implement these documented processes may impact the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, the requirement is a requirement that, if violated, could directly affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. CIP-010-1, Requirement R3 addresses a single objective and has a single VRF.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months

VRF and VSL Justifications – CIP-010-1, R3			
documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3)

VRF and VSL Justifications – CIP-010-1, R3			
			OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

VRF and VSL Justifications – CIP-010-1, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed requirement is mapped to Requirement R4 and R4.5 of CIP-005-4 and Requirement R8 and R8.4 of CIP-007-4. Additionally, Requirement Part 3.2 is a new requirement and has no mapping to a Requirement in a previous NERC CIP Standards Version. The binary VSL for the previous releases were based on performing vulnerability assessments annually, or not including one or more of the various elements identified in the related sub-requirements in a vulnerability assessment. This version's VSLs have evolved from this binary component model to a multidimensional component model. The proposed requirement does not have the unintended consequence of lowering the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the Requirement.

VRF and VSL Justifications – CIP-010-1, R3	
Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	This Requirement seeks to implement vulnerability assessment processes that if not done may impact the reliability and operability of the BES, but a single lapse in protection is not expected to compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	CIP-010-1, Requirement R3 specifies that a Responsible Entity must implement and document the processes for vulnerability assessments of BES Cyber Assets and BES Cyber Systems. Documentation of these processes is required, but this documentation is not the primary objective of the requirement. Documentation is interdependent with the implementation of the processes in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the vulnerability assessment process. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-011-5, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This Requirement ensures that Responsible Entities prevent unauthorized access to BES Cyber System Information. Failure to adequately identify, protect, and control access to such information could result in unauthorized access and lost, stolen, or misused Cyber System Information. Such failure represents a risk to the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for methods to identify, provide secure handling, and control access to Cyber System Information. The VRF is only applied at the requirement level and the requirement parts are treated equally. The identification, secure handling and control of access have the common objective to protect BES Cyber System Information.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps to CIP-003, R4 and CIP-003-3, R4.1, which have an approved VRF of Medium. The Requirement also maps to CIP-003-3, R4.2 and CIP-003-3, R4.3 and to CIP-003-3, R5, CIP-003-3, R5.1, CIP-003-3, R5.2, and CIP-003-3, R5.3, which have an approved VRF of Lower. The requirement has the object of securing Cyber System Information. Version 5 combines requirements to ensure consistency. The proposed VRF is consistent with the approved VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to adequately identify and protect BES Cyber System Information could result in disclosure of information to unauthorized persons, lost, stolen, or misused Cyber System Information. Such breaches of confidentiality represent a risk to the reliability of Bulk Electric System from misuse by unauthorized persons.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The sub requirements in R1 have a common objective to assure confidentiality of BES Cyber System

VRF and VSL Justifications – CIP-011-5, R1			
	Information. The obligations to identify, control access, and assure proper handling of BES Cyber System Information contribute to this objective and only one VRF is assigned.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

VRF and VSL Justifications – CIP-011-5, R1			
		Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information but did not identify, assess, or correct the deficiencies. (1.2)	

VRF and VSL Justifications – CIP-011-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The previously approved VSLs included a combination of binary and gradated VSLs. The Proposed VSLs are consistent with the approved VSLs for the CIP 011-5 R1 requirement, which maps to CIP 004-3, R4 and CIP 004-3, R5.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-011-5, R1	
Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Failure to document and implement a BES Cyber System information protection program has a binary Severe VSL. Other Requirement Parts associated with the information protection program do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Interdependent tasks of documentation, identification, and implementation are treated in a uniform manner and have not been separated for each topical area addressed in the requirement.

VRF and VSL Justifications – CIP-011-1, R2	
Proposed VRF	**LOWER**
NERC VRF Discussion	A VRF of Lower is assigned to this requirement. This requirement ensures that Responsible Entities take action to prevent unauthorized retrieval of BES Cyber System information prior to disposal or reuse of asset storage media. A violation would not be expected to affect the electrical state or capability of the Bulk-Power System or the ability to effectively monitor and control the Bulk-Power System. Several other factors, including capabilities and intention of the individual and lack of other mitigating controls, would be required to make the BES Cyber System vulnerable. Therefore, the VRF of lower is consistent with the NERC definition of VRFs.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This Requirement ensures that Responsible Entities take action to prevent unauthorized retrieval of BES Cyber System Information prior to disposal or reuse of asset storage media. The VRF is only applied at the requirement level and the requirement parts are treated equally. R2.1. calls for the Responsible Entity to take action to prevent unauthorized retrieval of BES Cyber System Information at the time of reuse. R2.2. mandates that Responsible Entities take action to prevent unauthorized retrieval of such information at the time of disposal. The VRF of lower is consistent with the risk of a violation across the requirement parts.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps to CIP-007 R7, which has a VRF of Lower. The Requirement has the object of preventing unauthorized retrieval of BES Cyber System Information from asset media prior to reuse or disposal. The proposed VRF is consistent with the approved VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to adequately protect information contained in asset storage media during reuse or disposal would not be expected to affect the electrical state or capability of the Bulk Power System or the ability to

VRF and VSL Justifications – CIP-011-1, R2			
	effectively monitor or control the Bulk-Power System. Several other factors, including capabilities and intention of the individual and lack of other mitigating controls, would be required to make the BES Cyber System vulnerable. Therefore, the VRF of lower is consistent with the NERC definition of VRFs.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirement/sub-requirements in R2 have a common objective to assure confidentiality of BES Cyber System Information. The obligations to protect such information, which may be contained on asset media, during both reuse and destruction, contribute to this objective and only one VRF is assigned.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

VRF and VSL Justifications – CIP-011-1, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The previously approved VSLs included a combination of binary and gradated VSLs. The proposed VSLs are consistent with the approved VSLs for the CIP-007 R7 requirement, which maps to this requirement. There is no unintended consequence of lowering the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement. The VSL does not expand the requirement.

VRF and VSL Justifications – CIP-011-1, R2	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Failure to document or implement all required processes has a binary Severe VSL. Other Requirement Parts associated with the required processes do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Interdependent tasks of documentation, identification, and implementation are treated in a uniform manner and have not been separated for each topical area addressed in the requirement.

Exhibit F

Record of Development of Proposed CIP Version 5 Reliability Standards

(Part 1 of 2)

Project 2008-06
Cyber Security Order 706 Version 5 CIP Standards

Related Files

Activity: Version 5 CIP Standards (Phase III)

Status:
The Version 5 CIP Standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1, the associated implementation plan, and the associated definitions) were approved by the NERC Board of Trustees on November 26, 2012, and they are being prepared for filing with applicable regulatory authorities.

Draft	Action	Dates	Results	Consideration of Comments
Draft 4 CIP-002-5 Clean **(174)** | Redline to Last Posted **(175)** CIP-003-5 Clean **(176)** | Redline to Last Posted **(177)** CIP-004-5 Clean **(178)** | Redline to Last Posted **(179)** CIP-005-5 Clean **(180)** | Redline to Last Posted **(181)** CIP-006-5 Clean **(182)** |	Recirculation Ballots and Non-binding Poll Info **(212)** Vote>>	10/26/12 - 11/05/12 (Closed) Non-binding Poll Extended until 11/13/12 (closed)	Summary **(214)** Ballot Results: CIP-002-5 **(215)** CIP-003-5 **(216)** CIP-004-5 **(217)** CIP-005-5 **(218)** CIP-006-5 **(219)** CIP-007-5 **(220)** CIP-008-5 **(221)** CIP-009-5 **(222)** CIP-010-1 **(223)** CIP-011-1 **(224)** Implementation Plan **(225)** Definitions **(226)** ------- Summary **(227)** Non-Binding	

Redline to Last Posted **(183)** CIP-007-5 Clean **(184)** | Redline to Last Posted **(185)** CIP-008-5 Clean **(186)** | Redline to Last Posted **(187)** CIP-009-5 Clean **(188)** | Redline to Last Posted **(189)** CIP-010-1 Clean **(190)** | Redline to Last Posted **(191)** CIP-011-1 Clean **(192)** | Redline to Last Posted **(193)** Implementation Plan Clean **(194)** | Redline to Last Posted **(195)** Definitions Clean **(196)** | Redline to Last Posted **(197)** **Supporting Materials:** VRF and VSL			Poll Results **(228)**	
	VRF and VSL Comment Form Info **(213)** Submit Comments>>	10/26/12 - 11/05/12 (Closed)		

Comment Form (Word) **(198)** VRFs/VSLs for all Standards Clean **(199)** | Redline to Last Posted **(200)** Mapping Document Clean **(201)** CIP-002-4 **(202)** CIP-003-4 **(203)** CIP-004-4 **(204)** CIP-005-4a **(205)** CIP-006-4c **(206)** CIP-007-4 **(207)** CIP-008-4 **(208)** CIP-009-4 **(209)** Draft Consideration of Issues and Directives Clean **(210)** Consideration of Comments **(211)**				
Draft 3 - Version 5 CIP Standards CIP-002-5 Clean **(114)** | Redline to Last Posted **(115)** (CIP-002-5: REVISED 092112) CIP-003-5 Clean **(116)** |	Successive Ballot Info **(157)** Vote>>	10/01/12 - 10/10/12 (closed)	Summary **(159)** Ballot Results: CIP-002-5 **(160)** CIP-003-5 **(161)** CIP-004-5 **(162)** CIP-005-5 **(163)** CIP-006-5 **(164)** CIP-007-5 **(165)** CIP-008-5 **(166)** CIP-009-5 **(167)** CIP-010-1 **(168)** CIP-011-1 **(169)**	

Redline to Last Posted **(117)** (CIP-003-5: REVISED 09/14/12) CIP-004-5 Clean **(118)** | Redline to Last Posted **(119)** CIP-005-5 Clean **(120)** | Redline to Last Posted **(121)** CIP-006-5 Clean **(122)** | Redline to Last Posted **(123)** CIP-007-5 Clean **(124)** | Redline to Last Posted **(125)** CIP-008-5 Clean **(126)** | Redline to Last Posted **(127)** CIP-009-5 Clean **(128)** | Redline to Last Posted **(129)** CIP-010-1 Clean **(130)** | Redline to Last Posted **(131)** CIP-011-1 Clean **(132)** | Redline to Last			Implementation Plan **(170)** Definitions **(171)**	
	CIP-006-5 RSAW Industry Comment Period RSAW Feedback Form>> Please send RSAW Feedback Forms to: RSAWFeedback@nerc.net	09/11/12 - 10/10/12 (closed)		
	Standard Comment Period Info **(158)** Submit Comments>>	09/11/12 - 10/10/12 (closed)	Comments Received **(172)**	Consideration of Comments **(173)**

Posted **(133)** Implementation Plan Clean **(134)** | Redline to Last Posted **(135)** (Implementation Plan: REVISED 09/17/12) Definitions Clean **(136)**| Redline to Last Posted **(137)** (Definitions: REVISED 09/21/12) **Supporting Materials:** Unofficial Comment Form (Word) **(138)** VRFs/VSLs for all Standards Clean **(139)** | Redline to Last Posted **(140)** Mapping Document Clean **(141)**| Redline **(142)** CIP-002-4 **(143)** CIP-003-4 **(144)** CIP-004-4 **(145)** CIP-005-4a **(146)** CIP-006-4c **(147)** CIP-007-4 **(148)** CIP-008-4 **(149)** CIP-009-4 **(150)**				

Consideration of Comments Consideration of Comments A **(151)** CIP-002 and CIP-003 Includes Summary Consideration, Explanation, and Common Responses to Global Changes Consideration of Comments B **(152)** CIP-004 through CIP-007 Consideration of Comments C **(153)** CIP-008 through CIP-011 Consideration of Comments D **(154)** Definitions and Implementation Plans Draft Consideration of Issues and Directives Clean **(155)** | Redline **(156)**				
Draft 2 - Version 5 CIP Standards CIP-002-5 Clean **(47)** | Redline **(48)**	Successive Ballot Updated Info **(88)** Info **(89)** Request for Additional Clarity Form **(90)**	05/11/12 - 05/21/12 (closed)	Summary **(93)**(updated) Ballot Results: (Updated) CIP-002-5 **(94)** CIP-003-5 **(95)**	

CIP-003-5 Clean **(49)** | Redline **(50)** CIP-004-5 Clean **(51)** | Redline **(52)** CIP-005-5 Clean **(53)** | Redline **(54)** CIP-006-5 Clean **(55)** | Redline **(56)** CIP-007-5 Clean **(57)** | Redline **(58)** CIP-008-5 Clean **(59)** | Redline **(60)** CIP-009-5 Clean **(61)** | Redline **(62)** CIP-010-1 Clean **(63)** | Redline **(64)** CIP-011-1 (CIP-011-1: REVISED - 05/09/12) Clean **(65)** | Redline **(66)** Implementation Plan Clean **(67)** | Redline **(68)**	Posted Requests for Additional Clarity **(91)** Vote>>		CIP-004-5 **(96)** CIP-005-5 **(97)** CIP-006-5 **(98)** CIP-007-5 **(99)** CIP-008-5 **(100)** CIP-009-5 **(101)** CIP-010-1 **(102)** CIP-011-1 **(103)** Implementation Plan **(104)** Definitions **(105)**	
	Formal Comment Period Advanced Info **(92)** **Submit Comments:** Comment Form A Comment Form B Comment Form C Comment Form D	04/12/12 - 05/21/12 (Closed)	Comments Received: Comment Form A **(106)** Comment Form B **(107)** Comment Form C **(108)** Comment Form D **(109)**	**Consideration of Comments** Consideration of Comments A **(110)** CIP-002 and CIP-003 Includes Summary Consideration, Explanation, and Common Responses to Global Changes Consideration of Comments B **(111)** CIP-004 through CIP-007 Consideration of Comments C **(112)** CIP-008 through CIP-011 Consideration of Comments D **(113)** Definitions and Implementation Plans

Definitions Clean **(69)** | Redline **(70)** Clean and redline definitions documents updated on April 12, 2012 to reflect correct dates in the footer sections. **Supporting Materials** Unofficial Comment Form A **(71)**- CIP-002 and CIP-003 Unofficial Comment Form B **(72)**- CIP-004 through CIP-007 Unofficial Comment Form C **(73)** - CIP-008 through CIP-011 Unofficial Comment Form D **(74)**- Definitions and Implementation Plans Mapping Document Clean **(75)** | Redline **(76)** CIP-002-4 **(77)** CIP-003-4 **(78)** CIP-004-4 **(79)** CIP-005-4a **(80)**				

CIP-006-4c **(81)** **CIP-007-4 (82)** **CIP-008-4 (83)** CIP-009-4 **(84)** Consideration of Comments **(85)** Draft Consideration of Issues and Directives Clean **(86)** | Redline **(87)**				
CIP Standards Version 5 Webinar Slides **(46)**	04/10/12			
Draft 1 - Version 5 CIP Standards CIP-002-5 **(4)** CIP-003-5 (CIP-003-5: REVISED - 11/22/11) **(5)** CIP-004-5 **(6)** CIP-005-5 **(7)** CIP-006-5 **(8)** CIP-007-5 **(9)** CIP-008-5 **(10)** CIP-009-5 **(11)** CIP-010-1 **(12)** CIP-011-1 **(13)** Implementation Plan **(14)** Definitions **(15)** **Supporting Materials**	Initial Ballot Info **(28)** Vote>>	12/16/11 - 01/06/12 (Closed)	Summary **(31)** Full Record Ballot Results: CIP-002-5 **(32)** CIP-003-5 **(33)** CIP-004-5 **(34)** CIP-005-5 **(35)** CIP-006-5 **(36)** CIP-007-5 **(37)** CIP-008-5 **(38)** CIP-009-5 **(39)** CIP-010-1 **(40)** CIP-011-1 **(41)** CIP V5 Implementation Plan **(42)** CIP V5 Definition **(43)**	
	Formal Comment Period Info **(29)** Submit Comments>>	11/07/11 - 01/06/12 (Closed)		
	Join Ballot Pool Info **(30)** Join>>	11/07/11 - 12/15/11 (Closed)		

Unofficial Comment Form (Word) **(16)** Mapping Document **(17)** CIP-002-4 **(18)** CIP-003-4 **(19)** CIP-004-4 **(20)** CIP-005-4a **(21)** CIP-006-4c **(22)** CIP-007-4 **(23)** CIP-008-4 **(24)** CIP-009-4 **(25)** Consideration of Comments from June 2010 Informal Comment Period **(26)** Draft Consideration of Issues and Directives **(27)**			Comments Received **(44)** Additional Link for Comments Received_CSWG **(45)**	
CIP Standards Version 5 Webinar Slides **(3)**		08/24/2011		
CIP Standards Version 5 Presentations - August 2011 SDT Meeting **(2)**		08/17/11		
CIP Standards Development Overview for FERC Technical Staff Meeting **(1)**		07/28/11		

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Standards Development Overview

CSSDTO706

Meeting with FERC Technical Staff

July 28, 2011

to ensure the reliability of the bulk power system

Objectives

- Historical Timeline
- CIP-002-4
- CIP-005-4
- CIP Version 5

Project 2008-06 Overview

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- **FERC Order 706**
- SDT appointed – August 2008
- CIP Version 2 – September 2009
- CIP Version 3 – March 2010
- CIP Version 4 – Ongoing Effort

CSO706 SDT Members

- 17 members – almost all asset owners
- Representation from IOUs, US and Canadian Government, Cooperatives, Municipals, Independent Power Producers, and ISO/RTO
- Worked together for 3 years
- Monthly face-to-face meetings, several interim conference calls and multiple webinars/workshops
- Worked through 3 successful ballots

CIP-002-4 Overview

- Version 4 of the CIP Standards
- Approved by Industry December 30, 2010
- Submitted to FERC February 10, 2011
  - 2,232 page filing
  - http://www.nerc.com/files/Final_Final_CIP_V4_Petition_20110210.pdf
  - Filing included CIP-002-4 through CIP-009-4, but only changes in CIP-002-4

CIP-002-4 Overview (cont.)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Replaces “risk-based assessment methodology” with “bright-line criteria”
  - Still maintains the concept of Critical Asset and Critical Cyber Asset
  - Uniform application across all entities and regions
  - Eliminates subjectivity by entities over what is “critical”
  - 17 defined criteria
  - To the greatest extent possible, bright line criteria tied to operational standards

CIP-002-4 Applicability

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.

CIP-002-4 Effective Date

Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

CIP-002-4 Requirement R1

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall update this list as necessary, and review it at least annually.

CIP-002-4 Requirement R2

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1

CIP-002-4 Requirement R3

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

Remote Access UA

- Implements requirements on “Cyber Assets” used for “monitoring or support” of Critical Cyber Assets when communication is initiated from outside an Electronic Security Perimeter
  - i.e., remote laptop or desktop systems accessing Critical Cyber Assets, but *not* for the purpose of control
  - Remote access for the purpose of control is the subject of CAN-0005
- Development now integrated into CIP Version 5

CIP V5

- The Drafting Team continues to work to address the remaining issues in Order 706
  - Using the “CIP-002 to CIP-009 +” organization
  - Monthly meetings and many conference calls
  - Initial ballot by December 2011
- The Drafting Team developed a set of development goals

Development Goals

Goal 1: To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements.	**Goal 5**: To minimize technical feasibility exceptions.
Goal 2: To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES.	**Goal 6:** To develop requirements that foster a “culture of security” and due diligence in the industry to complement a “culture of compliance”.
Goal 3: To provide guidance and context for each Standard Requirement	**Goal 7:** To develop a realistic and comprehensible implementation plan for the industry.
Goal 4: To leverage current stakeholder investments used for complying with existing CIP requirements.	

Levels of impact

- High Impact
  - Large Control Centers
  - CIP-003 through 009+
- Medium Impact
  - Generation and Transmission
  - Other Control Centers
  - Similar to CIP-003 to 009 v4
- All other BES Cyber Systems
  - Security Policy
  - Security Awareness
  - Incident Response
  - Boundary Protection

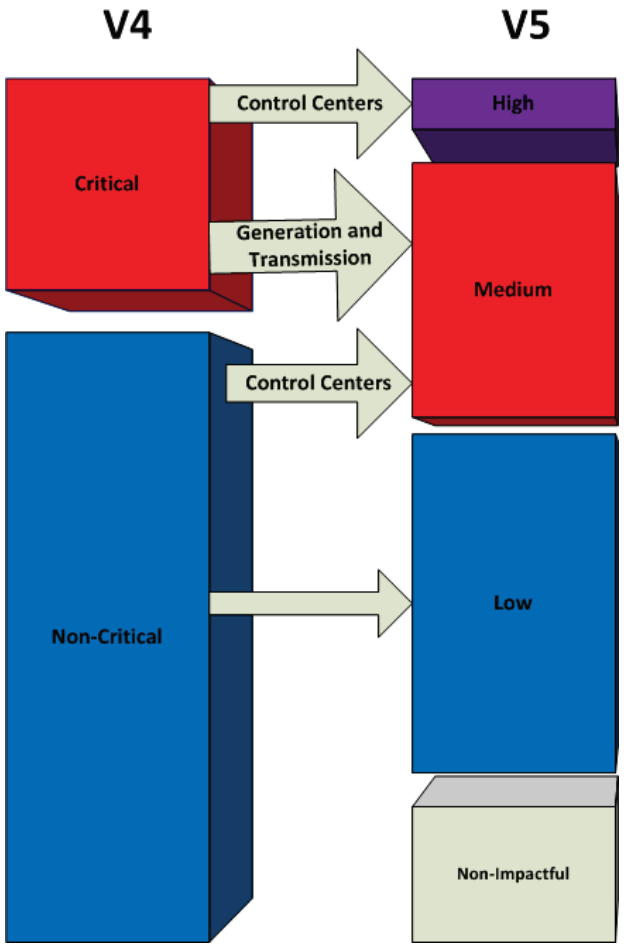

Example Format

R1. Each Responsible Entity shall implement a cyber security governance structure that includes the required items in CIP-011-1 Table R2 – Security Governance.

Rationale: *One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.*

Summary of Changes: *[Use this section to describe any broad changes applying to multiple rows in the table or removed requirements. These changes require the same level of justification as in the table rows. If all changes can be sufficiently described in the table rows, then this section can be omitted.]*

Additional Guidance: *The number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs.*

2. Rationale

3. Requirement-level change justification

4. Additional Guidance

5. Applicability

6. Requirement

7. Measurement

	CIP-011-1 Table R1 – Security Governance and Policy		
	Applicability	Each Responsible Entity shall include the following in their Account Management Documentation:	Measurement
1.1	Low	Identify a single senior management official with overall authority and responsibility for leading and managing implementation of requirements within this standard	Acceptable evidence may include documentation that identifies a single senior management official.
Reference to prior version: CIP-003 R1		**Change Justification:** Removed prescriptive requirement of how manager must be identified. Removed requirement regarding delegation. Requirement to update this within 30 days was removed. Requirement to authorize and document exceptions from the cyber security policy removed.	

8. Reference to Prior Version

9. Row-level Change Justification

Requirement Filters

- Why are we doing this? What do we hope to accomplish? What security concept are we trying to implement? If these questions cannot be answered, is the requirement necessary?
- Is it absolutely necessary to be done only this way to protect the BES? Are there other ways of accomplishing this requirement? If so, the requirement may be too specific.
- Is the timeframe arbitrary?
- Is the desired outcome clear and unambiguous? Can the measure clarify the desired outcome?

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Thank you

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Standards Development Overview

CSSDTO706

Meeting with Industry Representative

August 16 – 18 – NERC Atlanta Office

to ensure the reliability of the bulk power system

Objectives

- Historical Timeline
- CIP-002-4
- CIP-005-4
- CIP Version 5

Project 2008-06 Overview

- **FERC Order 706**
- SDT appointed – August 2008
- CIP Version 2 – September 2009
- CIP Version 3 – March 2010
- CIP Version 4 – Ongoing Effort

CSO706 SDT Members

- 17 members – almost all asset owners
- Representation from IOUs, US and Canadian Government, Cooperatives, Municipals, Independent Power Producers, and ISO/RTO
- Worked together for 3 years
- Monthly face-to-face meetings, several interim conference calls and multiple webinars/workshops
- Worked through 3 successful ballots

CIP-002-4 Overview

- Version 4 of the CIP Standards
- Approved by Industry December 30, 2010
- Submitted to FERC February 10, 2011
  - 2,232 page filing
  - http://www.nerc.com/files/Final_Final_CIP_V4_Petition_20110210.pdf
  - Filing included CIP-002-4 through CIP-009-4, but only changes in CIP-002-4

CIP-002-4 Overview (cont.)

- Replaces “risk-based assessment methodology” with “bright-line criteria”
  - Still maintains the concept of Critical Asset and Critical Cyber Asset
  - Uniform application across all entities and regions
  - Eliminates subjectivity by entities over what is “critical”
  - 17 defined criteria
  - To the greatest extent possible, bright line criteria tied to operational standards

CIP-002-4 Applicability

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.

CIP-002-4 Effective Date

Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

CIP-002-4 Requirement R1

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall update this list as necessary, and review it at least annually.

CIP-002-4 Requirement R2

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1

CIP-002-4 Requirement R3

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

Remote Access UA

- Implements requirements on “Cyber Assets” used for “monitoring or support” of Critical Cyber Assets when communication is initiated from outside an Electronic Security Perimeter
  - i.e., remote laptop or desktop systems accessing Critical Cyber Assets, but *not* for the purpose of control
  - Remote access for the purpose of control is the subject of CAN-0005
- Development now integrated into CIP Version 5

CIP V5

- The Drafting Team continues to work to address the remaining issues in Order 706
  - Using the “CIP-002 to CIP-009 +” organization
  - Monthly meetings and many conference calls
  - Initial ballot by December 2011
- The Drafting Team developed a set of development goals

Development Goals

Goal 1: To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements.	**Goal 5**: To minimize technical feasibility exceptions.
Goal 2: To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES.	**Goal 6:** To develop requirements that foster a "culture of security" and due diligence in the industry to complement a "culture of compliance".
Goal 3: To provide guidance and context for each Standard Requirement	**Goal 7:** To develop a realistic and comprehensible implementation plan for the industry.
Goal 4: To leverage current stakeholder investments used for complying with existing CIP requirements.	

Requirement Filters

- Why are we doing this? What do we hope to accomplish? What security concept are we trying to implement? If these questions cannot be answered, is the requirement necessary?
- Is it absolutely necessary to be done only this way to protect the BES? Are there other ways of accomplishing this requirement? If so, the requirement may be too specific.
- Is the timeframe arbitrary?
- Is the desired outcome clear and unambiguous? Can the measure clarify the desired outcome?

Levels of impact

- High Impact
  - Large Control Centers
  - CIP-003 through 009+
- Medium Impact
  - Generation and Transmission
  - Other Control Centers
  - Similar to CIP-003 to 009 v4
- All other BES Cyber Systems
  - Security Policy
  - Security Awareness
  - Incident Response
  - Boundary Protection

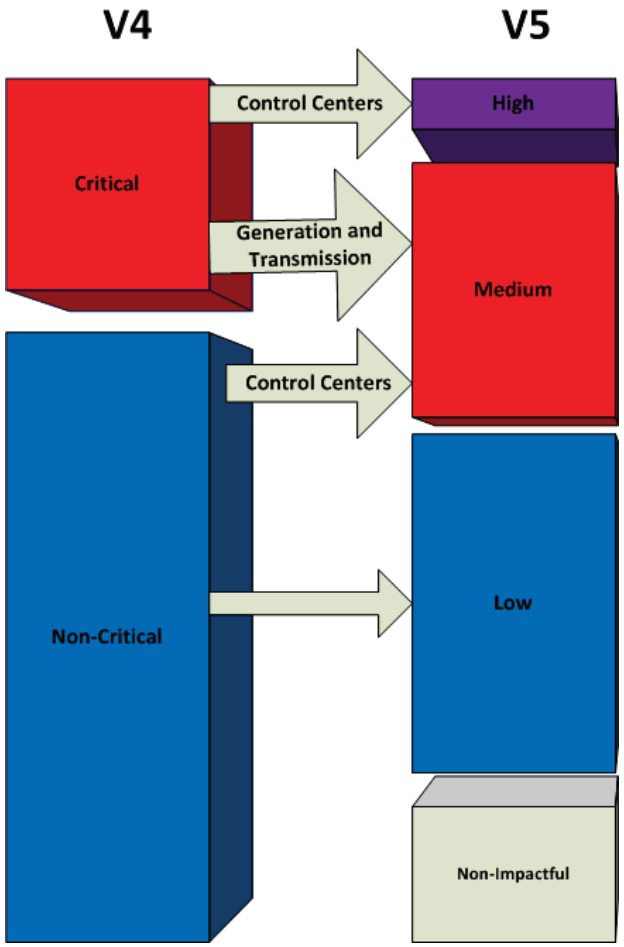

Format (1/4) – Introductory Requirement

B. Requirements

R1. Each Responsible Entity shall implement one or more documented processes that include the required items in *CIP-007-5 Table R1 – Ports and Services*.

M1. Acceptable forms of evidence include, but are not limited to, documentation of the implemented processes that include the required items in *CIP-007-5 Table R1 – Ports and Services*.

Rationale: *Ports and services refer to network accessible ports, system services and physical I/O ports. Unnecessary ports and services provide additional means of access and can increase the likelihood of vulnerabilities in a BES Cyber System. This allows more opportunity for an attacker to obtain*

- Requirement/measures for implemented procedures in most requirements
- Most requirements reference a table immediately below

Format (2/4) – Contextual Boxes

- **Rationale –** Purpose of requirement and any assumptions made about the requirement
- **Summary of Changes –** High level overview of changes in this requirement
- **Guidance –** Additional guidance in applying the requirement

Work in Progress

Rationale: *Ports and services refer to network accessible ports, system services and p*
Unnecessary ports and services provide additional means of access and can increase t
vulnerabilities in a BES Cyber System. This allows more opportunity for an attacker to
unauthorized access.

Summary of Changes: *In the March 18, 2010 FERC issued an order to approve NERC*
of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports a
refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the draftin
address unused physical ports.

Disabling ports and services refers to all of network accessible ports, any system servic
I/O ports. Each of these are broken out into separate requirement rows.

In the original CIP-007-4 R2, a Responsible Entity was required to both (R2.1) only ena
and services and (R2.2) disable all other ports and services. Disabling ports and servic
normal and emergency operations is equivalent to both of these requirements. Therefor
removed.

Additional Guidance:

3.3 Guidance: Examples of physical I/O ports include network, serial and USB ports ext
casing. BES Cyber Systems should exist within a Defined Security Boundary in which

Format (3/4) – Requirement Row

	CIP-007-5 Table R3 – Malicious Code Prevention		
	Applicability	Requirement	Measurement
3.1	High and Medium Impact BES Cyber Systems	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of acceptable evidence include, but are not limited to, policies and/or processes that show for the types of BES Cyber Assets in the BES Cyber System how the Responsible Entity is limiting the introduction of malicious code (i.e. through

- Measurement specifies acceptable evidence of **implementing** procedures associated with the requirement row.
- Measurements still a work in progress.

Format (4/4) – Applicability

- All Responsible Entities
- High Impact BES Cyber Systems
- Medium Impact BES Cyber Systems
- External Connectivity Attributes – Routable or Dial-up connectivity
- Associated Electronic Access Control Systems – CIP-005-4 R1.5
- Associated Physical Access Control Systems – CIP-006-4 R2
- Associated Protected Cyber Systems – Non-Critical Cyber Assets within an ESP

Schedule to Date – 2011

June
- Regional Audit Staff

July
- Walk-through of Generation and Transmission Environments

July
- Meet with FERC Staff

August
- Meet with Industry Representatives

September
- Prepare for NERC Quality Review

Key Dates Moving Forward

- **November 3rd –** First Posting for Comment and Ballot
  - Webinar – November 15th and 29th
  - December 9th – Ballot Opens
  - December 19th – Ballot Closing
- **March 26th –** Second Posting

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-002-5

to ensure the reliability of the bulk power system

Definitions

- **BES Reliability Operating Services**

  BES Reliability Operating Services are those services contributing to the real-time reliable operation of the Bulk Electric System (BES). They include the following Operating Services:…

- **BES Cyber Asset**

  A Cyber Asset that if rendered unavailable, degraded, or misused could, within 15 minutes cause a Disturbance to the BES and adversely impact one or more BES Reliability Operating Services.

- **BES Cyber Systems**

  One or more BES Cyber Assets grouped together for the application of common cyber security controls. These are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services.

Summary of Requirements

- Categorized list of High and Medium Impact
  - Attachment 1 criteria
- Other BES Cyber Systems deemed to be Low Impact by default
- Update for significant changes to BES that affect High/Medium categorization
- Senior manager or delegate annual review and approval

Impact Criteria (Attachment 1)

- High: Large Control Centers (e.g. RC, BA, TOP)
- Medium: Based significant impact field assets, other Control Centers
- Other BES Cyber Systems deemed to be Low Impact by default
- Based on V4 criteria
  - Review of Transmission voltage threshold by SDT for V5
  - Use of MVA bright-line under consideration

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-003-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications

- CIP-003-5 was reorganized to only include elements of policy and cyber security program governance.
  - Elements that addressed Change Control and Configuration Management were moved to CIP-010-5
  - Elements that address Information Protection were moved to CIP-011-5

Summary of Modifications

- Additional flexibility was added to the Cyber Security Policy requirement by explicitly allowing for multiple policies and specifying the topical areas (as opposed to all requirements) that the policy must address.
- The SDT has removed the requirement to document exceptions to the policy, although discussions of this approach with FERC staff are ongoing.

Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 376

"the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards."

- The SDT considers this a general management issue that is not within the scope of a compliance requirement.
- The SDT found no reliability basis in this requirement.
- The SDT has proposed removing the requirement for documented exceptions to the Cyber Security Policy.

Cyber Security Policy Changes

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Required elements of Cyber Security Policy
  - V4 - "The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations."
    - The SDT believes that this languages has caused the industry to develop Cyber Security Policies to the least common denominator, i.e. a restatement of the CIP standards.
  - V5 – "…articulates the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:
    - 1. Personnel Security
    - 2. Electronic Security Perimeters
    - 3. Remote Access
    - 4. Physical Security
    - 5. System Security
    - 6. Incident Response
    - 7. Recovery Plans
    - 8. Configuration Change Management
    - 9. Information Protection
    - 10. Provisions for emergency situations (Specified Exceptional Circumstances)

Access to the Cyber Security Policy

- Version 4 required that the Cyber Security Policy be "readily accessible to all personnel who have access to, or are responsible for, Critical Cyber Assets"
- Numerous concerns were raised as to the specific meaning of "readily accessible"
- The SDT proposes to modify this requirement by more directly stating its objective:
  - "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function."

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-004-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications (1/3)

- Security Awareness
  - Continues to be general awareness that is refreshed quarterly and not formal tracked training
- Training
  - Addition of visitor control program
  - electronic interconnectivity supporting the operation and control of BES Cyber Systems
  - storage media as part of the handling of BES Cyber Systems information
  - Reorganization of requirements into the respective requirements for “program” and “implementation” of the training.

Summary of Modifications (2/3)

- Personnel Risk Assessment
  - Changed to only initial identity verification
  - Now includes documenting the processes used to determine when to deny access
  - Reorganization of requirements into the respective requirements for “program” and “implementation”

Summary of Modifications (3/3)

- Authorization
  - Consolidated authorization and review requirements from CIP-003-4, CIP-004-4, CIP-006-4 and CIP-007-4
  - Allow quarterly and annual reviews to find and fix problems rather than self-report everything as a violation
- Revocation
  - Remove ability to access BES Cyber System when access no longer needed

Addressing FERC Directives

- FERC Order 706 P433 "we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard."
  - The SDT addressed this by identifying the training topics that should be provided in the Training Program.
- FERC Order 706 P434 "The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets."
  - The SDT added this as a topic for role specific training.

Addressing FERC Directives

- FERC Order 706 P435 "Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves."
  - The SDT does not feel security trainers need to be specially trained or certified.

Addressing FERC Directives (Immediate Revocation)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 460

"The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."

- Take actions to remove the ability to access the BES Cyber System when access is no longer required

Requirements applicable to Low Impact

- Security Awareness – A security practice program that conveys the security awareness concepts, and provides on-going reinforcement of such concepts on at least a quarterly basis.

Access Authorization Program (1/2)

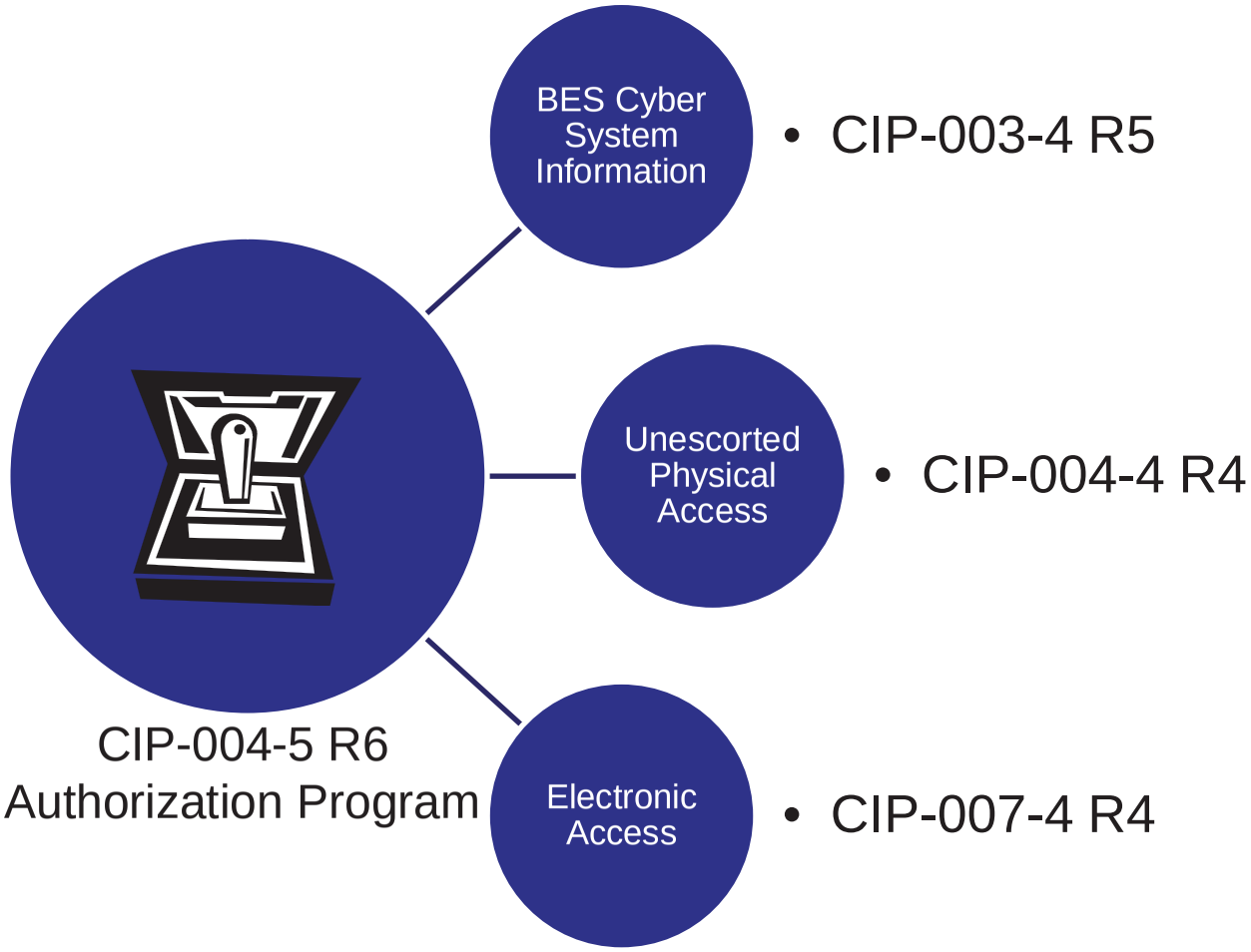

Access Authorization (2/2)

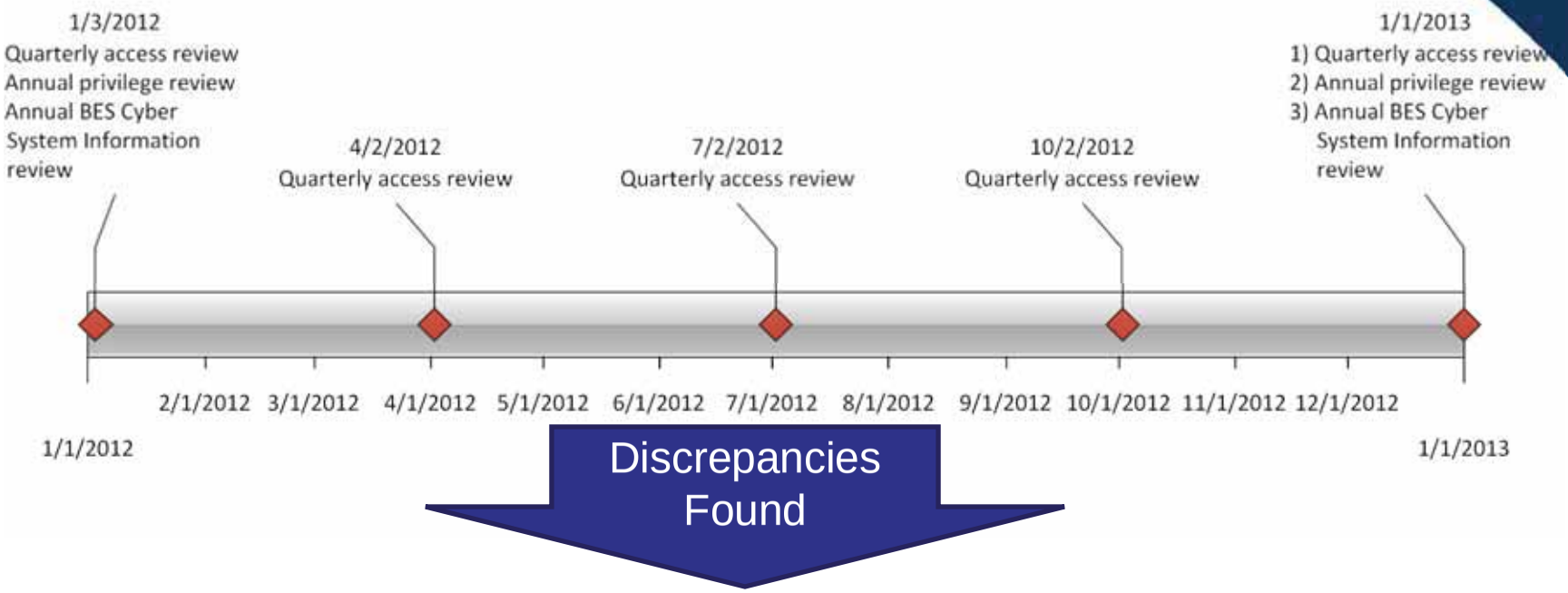

Determine the Cause → Fix or initiate Incident Response → Remediate any process deficiencies

Revocation of Access

- When access is no longer needed
  - Involuntary dismissals
  - Voluntary terminations
  - Retirements
  - Deaths
  - Transfers – Date determined by the entity
- Revoke ability to access
  - Physical access
  - Remote Access
- Complete the revocation process
  - Revoke individual user accounts within 30 days

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-005-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications

- Define ‘External Connectivity’ for scope modification
- Focus on ‘Electronic Access Points’ vs. ESP
- Require IDS at Control Centers
- Add clarity to ‘secure’ dialups
- Consolidated Monitoring and Vulnerability Assessment Requirements in CIP-007 and CIP-011 respectively
- Removed Appropriate Use Banner
- Incorporated CIP-005-4 Urgent Action revisions

Trimmed Requirements

- R1.1 – 1.6 and 2.5 – New measures, rationale and guidance allow the removal of explanatory text in the Standard
- R2.6 (Appropriate Use Banner) – Not necessary for meeting the reliability objective
- R3 (Monitoring) – Consolidated in CIP-007-5 R4 to ensure consistency
- R4 (Vulnerability Assessment) – Consolidated and moved to CIP-010-5 R3
- R5 (Documentation Review and Maintenance) – Largely administrative requirement

Addressing FERC Directives (2 Security Measures – Defense in Depth)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 496

"Commission adopts the CIP NOPR's proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter."

- Deploy methods to inspect communications and detect potential malicious communications for all External Connectivity (Intrusion Detection)

Requirements applicable to Low Impact

- R1. Electronic Security Perimeter
  - 1.1 Identify and secure Electronic Access Points
  - 1.2 Firewall controls
  - 1.3 Dial-up controls

Requirements Applicable to High Impact Only

- R1 Table 1.6
  - Deploy intrusion detection for all Electronic Access Points

Dial-Up

- Add clarity to ‘secure’ dialup
  - Secure each Electronic Access Point that utilizes dial-up access such that authentication occurs before establishing connectivity with the BES Cyber System

CIP-005-4 Urgent Action Revisions

- Addressing NERC Alert regarding remote access VPN vulnerabilities
- Creates basic requirements to protect critical systems from untrusted networks.
- Identifies protective measures that provide secure access to critical systems.
- Helps ensure secure practices by employees, contractors, and service vendors to minimize exploitation of vulnerabilities.

CIP-005-4 Urgent Action Revisions

- Addresses questions regarding ability to audit or enforce the requirement through the design of clear measures.
- Significant guidance to be provided to address implementation options for organizations of differing sizes, capabilities, and complexity.

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-006-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications

- Physical Security Program
  - Must define the operational or procedural controls to restrict physical access
  - Removed current “6 wall” wording to instead require Defined Physical Boundary
  - For High Impact, added the need to utilize two or more different and complementary physical access controls to restrict physical access
  - Testing changed to a 24 month cycle with ongoing discussions of different cycles based on environment.

Requirements applicable to Low Impact

- Define the operational or procedural controls to restrict physical access.

Addressing FERC Directives

- FERC Order 706 P572 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."
  - The SDT added this for High Impact BES Cyber Assets
- FERC Order 706 P581 "The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years,."
  - The SDT changed to a 24 month testing cycle but is also still discussing different cycles based on environment

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications (1/2)

- Addition of physical I/O port requirement
- Security Patch mgt source requirement
- Non-prescriptive malware requirement
- Security Event Monitoring failure handling
- Bi-weekly log summary/sampling reviews

Summary of Modifications (2/2)

- Simplified access-control requirements, removed TFE language while strengthening password requirements
- Added requirement for maintenance devices
- Consolidated vulnerability assessment in CIP-010-5
- Disposal requirement moved to CIP-011-5

Requirements applicable to Low Impact

- Change or have unique default passwords on production BES Cyber Assets, Electronic Access Control Systems, Physical Access Control Systems and Protected Cyber Assets, where technically feasible.

Requirements Applicable to High Impact Only

- Bi-weekly log reviews - Review a summarization or sampling of logged events every two weeks to identify unanticipated Cyber Security Incidents and potential event logging failures. Activate a response to rectify any event logging failure identified from the review before the end of the next calendar day.

Addressing FERC Directives (Log Review)

FERC Order 706 Para. 525	"The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily…"
FERC Order 706 Para. 628	"Requirement R6 of CIP-007-1 does not address the frequency with which log should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly…"

- The SDT Proposes the performance of a review of log summaries or samples every two weeks.

Addressing FERC Directives (Malware)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 620	"The Commission will not adopt Consumers' recommendation that every system in an electronic security perimeter does not need antivirus software. Critical cyber assets must be protected, regardless of the operating system being used. Consumers has not provided convincing evidence that any specific operating system is not directly vulnerable to virus attacks. Virus technology changes every day. Therefore we believe it is in the public interest to protect all cyber assets within an electronic security perimeter, regardless of the operating system being used…"
FERC Order 706 Para. 622	"The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above.

- Rewrote the requirement as a competency based requirement that does not prescribe technology.
- Added Maintenance to cover malware on removable media.

Addressing FERC Directives (Ports & Services)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

March 18th Order on ports/services

"The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."

- The SDT proposes to address this directive by having a requirement to disable or restrict use of physical I/O ports

Ports and Services

Acceptable ways to disable or restrict access.

```
!
interface Management0/0
 shutdown
 no nameif
 security-level 100
 ip address 10.1.0.24 255.255.0.0
 management-only
!
```

Configuration

Logically Disable

USB Lock

Restrict

Epoxy Glue

Permanently Disable

Security Event Monitoring

- Combines all monitoring requirements (CIP-005-4 R3, CIP-007-4 R5 and R6)
- Industry commented – What is monitoring? What are security events
  - Entity determines which events to **log** and which events necessitate **alerts**
- Draft CAN – Are logging system failures a violation?
  - Generate alerts for event logging failures

Access Control

- Moved access privilege review to CIP-004-5
- Simplified the requirement wording in controlling shared, administrative and generic accounts
- Minimize the need for TFEs for passwords
  - Password length is the minimum of 8 characters or maximum supported by the device
  - Strengthened the requirement by limiting or alerting on unsuccessful login attempts

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-008-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications

- CIP-008-5 was primarily modified to satisfy the FERC 706 directives as follows:

Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 661

"the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."

1. Added: Reportable Cyber Security Incidents are either:

- Any malicious act or suspicious event or events that compromise, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a BES Cyber System.

  or

- Any event or events which have either impacted or have the potential to impact the reliability of the Bulk Electric System (Reliability Function CIP-002-5).

2. Retired R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in EOP-004-2, Requirement 1, Part 1.3. Will need to give instruction to report as a "Reportable Cyber Security Event" in EOP-004 space.

3. See R1.1 above

4. Guidance and measurements are being developed accordingly

Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 673

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.."

Cyber Security - Incident Reporting and Response Planning: Retired R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in EOP-004-2, Requirement 1, Part 1.3 and Attachment 1

Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 676	"the Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.."

– Cyber Security - Incident Reporting and Response Planning: Retired R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in EOP-004-2, Requirement 1, Part 1.3.

Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 686

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.."

R3.3 and R3.4 Includes additional specification on update of response plan Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-009-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications

- CIP-009-5 was primarily modified to satisfy the FERC 706 directives as follows:

Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 694

"For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan..We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard"

Added specific R1 requirement to implement recovery plan

Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 739

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."

R1.5 Added requirements related to restoration processes based on review of the DHS Controls

Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 748

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."

R1.5 : Processes for the restoration of BES Cyber Systems to the most current baseline configuration

Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 706

"Preserve data for analysis"

CIP-009-5 1.6
Requires process to preserve data for analysis

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-010-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications

- The SDT proposes the development of a new Standard CIP-010-5 that consolidates all references to Configuration Change Management and Vulnerability Assessments.
  - Previously these requirements were dispersed throughout CIP-003-4, CIP-005-4, and CIP-007-4

Summary of Modifications

- The SDT has made changes the Vulnerability Assessment requirements to
  - Consolidate the previous requirements in CIP-005-4 and CIP-007-4 into a single requirement
  - Make provisions for differences between Control Centers and field assets
  - Respond to FERC Order 706 regarding the performance of “active vulnerability assessments”

Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 397

"The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes."

- The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System.
- Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment prior to their implementation in the production environment to aid in identifying any accidental consequences of the change.

Addressing FERC Directives

FERC Order 706 Para. 609	"We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."
FERC Order 706 Para. 610	"we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above."
FERC Order 706 Para. 611	"the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."

- The SDT proposes to require a "representative system" or test system for those High Impact Control Centers to use for the purposes of testing proposed changes and performing active vulnerability assessments.
- The SDT proposes using the defined baseline configuration of a BES Cyber System for the measuring stick as to whether a test system is truly representative of the production system.
- To account for any additional differences between the two systems, the SDT proposes using the words directly from FERC Order 706 "Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments."

Addressing FERC Directives

FERC Order 706 Para. 541	"we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments."
FERC Order 706. Para 542	"the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems."
FERC Order 706 Para. 547	"we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"

- The SDT has added requirements for an "active vulnerability" assessment to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System.

Addressing FERC Directives

FERC Order 706 Para. 544	"the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification."
FERC Order 706 Para. 544	"we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment"

- The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new cyber asset undergo an active vulnerability assessment.
  - An exception is made for specified exceptional circumstances such as an emergency.

Baseline Configurations

- The SDT proposes the introduction of a requirement for a baseline configuration that would be used to determine when the Configuration Change Process is invoked as well as what constitutes a representative system.
  - "Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified in CIP-002-5:
    - Physical location
    - Operating System (including version)
    - Commercially available application software (including version) intentionally installed on the BES Cyber Asset
    - Any software/scripts developed for the entity
    - Logical network accessible ports
    - Enabled system services
    - Security patch levels"

Testing of Changes

- In additional to the current requirement to verify that a change does not impact the existing cyber security controls, the SDT proposes to expand this requirement to ensure that the availability of the BES Cyber System is not affected.
- For High Impact Control Centers, the SDT proposes that the change be tested in a test environment prior to implementation in the production environment.

Vulnerability Assessments

- The Vulnerability Assessment requirement now consists of the following components
  - Conduct a review for Low Impact BES Cyber Systems
  - Conduct passive vulnerability assessments for High and Medium Impact BES Cyber Systems every 12 months
  - Conduct active vulnerability assessments in a test environment for High Impact BES Cyber Systems every 36 months
  - Conduct active vulnerability assessments on new Cyber Assets in a High Impact BES Cyber System prior to placing the Cyber Asset into production.
  - Document and implement a remediation plan to correct any deficiencies found.

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-011-5 Modifications

to ensure the reliability of the bulk power system

Summary of Modifications

- The SDT proposes the development of a new Standard CIP-011-5 that consolidates all references to Information Protection and Media Sanitization.
  - Previously these requirements were dispersed throughout CIP-003-4 and CIP-007-4
- The SDT has also moved the requirements regarding the authorization and revocation of access to BES Cyber System Information to CIP-004-5, consolidating these requirements with those for electronic and physical access.

Summary of Modifications

- The SDT has introduced a definition of a glossary term “BES Cyber System Information” which defines what needs to be protected.
  - Previously, this list was a requirement itself.

Summary of Modifications

- The SDT has shifted the focus of the requirements for media sanitization from the Cyber Asset to the information itself.
  - In version 4, these requirements are invoked when the Critical Cyber Asset is to be disposed of or redeployed.
  - In version 5, the requirement is triggered when either
    - BES Cyber System Information no longer needs to be stored on specific media, or
    - Media containing BES Cyber System Information is designated for disposal

Addressing FERC Directives

FERC Order 706 Para. 633	"The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it."
FERC Order 706 Para 635	"the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."

- The SDT has proposed that preventing unauthorized retrieval of data means to "render the data unrecoverable."
- The SDT understands that this may be too high of a bar and is continuing discussions in this area.

Information Protection

- Previous versions of the CIP Standards required that information be identified, classified, and protected.
- The SDT noted that while previous standards required that information be classified based upon its sensitivity, it did not require a difference in the protection pursuant to the information's sensitivity.
  - The SDT has thus removed the requirement to classify information without preventing an entity from performing this function if it so chooses.
- The SDT proposes for version 5 that the requirements to "protect" and manage access to information be replaced with a requirement for "labeling, handling (including storage, transit, and usage), and access control procedures."

Media Sanitization

- As previously mentioned, the SDT has shifted the focus of the media sanitization requirements from the Critical Cyber Asset to the information itself.
- The SDT has proposed the language that media be “erased, using a method to render the data unrecoverable.”
  - However, we believe that this would be difficult to audit and could be a constantly changing requirement due to the evolution of techniques to recover data, including some that are of a classified nature.

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

to ensure the reliability of the bulk power system

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Thank you

to ensure the reliability of the bulk power system

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Standards Version 5 Requirements & Status

Philip Huff – Arkansas Electric Cooperative Corporation
Doug Johnson – Commonwealth Edison Company
David Revill – Georgia Transmission Corporation

CSO706 SDT Webinar
August 24, 2011

to ensure the reliability of the bulk power system

Agenda

- Background
- Version 4 - Overview
- Version 5 – Requirements Summary
- Schedule and Implementation Plan

Project Background

Version 1

- Filed with FERC August 28, 2006
- Approved by FERC January 18, 2008
- Effective July 1, 2008 through January 1, 2010 (phased)

Version 2

- Low-hanging fruit
- Filed with FERC May 22, 2009
- Approved by FERC September 30, 2009
- Effective April 1, 2010

Version 3

- Compliance filing to Version 2
- Filed with FERC December 29, 2009
- Approved by FERC March 31, 2010
- Effective October 1, 2010

CIP-002-4 Overview

- **Version 4** of the CIP Standards
- Approved by Industry **December 30, 2010**
- Submitted to FERC **February 10, 2011**
  - 2,232 page filing
  - Filing included CIP-002-4 through CIP-009-4, but only changes in CIP-002-4

Looking Ahead to Version 5

- The SDT continues work to address the remaining 50+ issues in Order 706
  - Version 5 builds on CIP-002-4 and previous drafts of CIP-010 & 011
  - Use similar content structure and terminology as previous CIP Standards (CIP-002 through CIP-009)

Development Goals

Goal 1: To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements	**Goal 5**: To minimize technical feasibility exceptions
Goal 2: To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES	**Goal 6:** To develop requirements that foster a "culture of security" and due diligence in the industry to complement a "culture of compliance"
Goal 3: To provide guidance and context for each Standard Requirement	**Goal 7:** To develop a realistic and comprehensible implementation plan for the industry
Goal 4: To leverage current stakeholder investments used for complying with existing CIP requirements	

Levels of Impact

- High Impact
  - Large Control Centers
  - CIP-003 through 009+
- Medium Impact
  - Generation and Transmission
  - Other Control Centers
  - Similar to CIP-003 to 009 v4
- All other BES Cyber Systems
  - Security Policy
  - Security Awareness
  - Incident Response
  - Boundary Protection

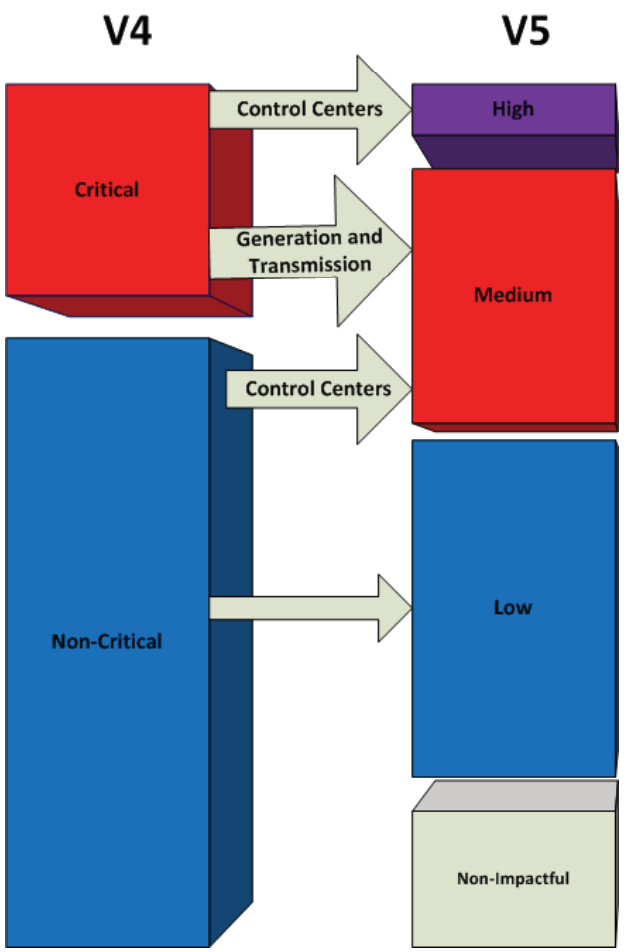

Format (1/4) – Introductory Requirement

B. Requirements

R1. Each Responsible Entity shall implement one or more documented processes that include the required items in *CIP-007-5 Table R1 – Ports and Services*.

M1. Acceptable forms of evidence include, but are not limited to, documentation of the implemented processes that include the required items in *CIP-007-5 Table R1 – Ports and Services*.

Rationale: *Ports and services refer to network accessible ports, system services and physical I/O ports. Unnecessary ports and services provide additional means of access and can increase the likelihood of vulnerabilities in a BES Cyber System. This allows more opportunity for an attacker to obtain*

- Requirement/measures for implemented procedures in most requirements
- Most requirements reference a table immediately below

Format (2/4) – Contextual Boxes

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- **Rationale –** Purpose of requirement and any assumptions made about the requirement
- **Summary of Changes –** High level overview of changes in this requirement
- **Guidance –** Additional guidance in applying the requirement

Work in Progress

Rationale: *Ports and services refer to network accessible ports, system services and p*
Unnecessary ports and services provide additional means of access and can increase t
vulnerabilities in a BES Cyber System. This allows more opportunity for an attacker to
unauthorized access.

Summary of Changes: *In the March 18, 2010 FERC issued an order to approve NERC*
of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports a
refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the draftin
address unused physical ports.

Disabling ports and services refers to all of network accessible ports, any system servic
I/O ports. Each of these are broken out into separate requirement rows.

In the original CIP-007-4 R2, a Responsible Entity was required to both (R2.1) only ena
and services and (R2.2) disable all other ports and services. Disabling ports and servic
normal and emergency operations is equivalent to both of these requirements. Therefor
removed.

Additional Guidance:

3.3 Guidance: Examples of physical I/O ports include network, serial and USB ports ext
casing. BES Cyber Systems should exist within a Defined Security Boundary in which
I/O ports have protection from unauthorized access, but it may still be possible for acci

Format (3/4) – Requirement Row

	CIP-007-5 Table R3 – Malicious Code Prevention		
	Applicability	Requirement	Measurement
3.1	High and Medium Impact BES Cyber Systems	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of acceptable evidence include, but are not limited to, policies and/or processes that show for the types of BES Cyber Assets in the BES Cyber System how the Responsible Entity is limiting the introduction of malicious code (i.e. through

- Measurement specifies acceptable evidence of compliance associated with the requirement row

Format (4/4) – Applicability

- All Responsible Entities
- High Impact BES Cyber Systems
- Medium Impact BES Cyber Systems
- External Connectivity Attributes – Routable or Dial-up connectivity
- Associated Electronic Access Control Systems – CIP-005-4 R1.5
- Associated Physical Access Control Systems – CIP-006-4 R2
- Associated Protected Cyber Systems – Non-Critical Cyber Assets within an ESP

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-002-5 – CIP-011-5

to ensure the reliability of the bulk power system

CIP-002-5 Summary of Modifications

- Categorized list of High and Medium Impact
  - Attachment 1 criteria
- Other BES Cyber Systems deemed to be Low Impact by default
- Update required lists for significant changes to BES that affect High/Medium categorization
- Senior manager or delegate annual review and approval

CIP-002-5 Impact Criteria (Attachment 1)

- High: Large Control Centers (e.g. RC, BA, TOP)
- Medium: Significant impact field assets, other Control Centers
- Other BES Cyber Systems deemed to be Low Impact by default
- Based on V4 criteria
  - Review of Transmission voltage threshold by SDT for V5
  - Use of MVA bright-line under consideration

CIP-003-5 Summary of Modifications (1/2)

- CIP-003-5 was reorganized to only include elements of policy and cyber security program governance
  - Elements that addressed Change Control and Configuration Management were moved to CIP-010-5
  - Elements that address Information Protection were moved to CIP-011-5

CIP-003-5 Summary of Modifications (2/2)

- Additional flexibility was added to the Cyber Security Policy requirement by explicitly allowing for multiple policies and specifying the topical areas (as opposed to all requirements) that the policy must address
- The SDT has removed the requirement to document exceptions to the policy, although discussions of this approach with FERC staff are ongoing

CIP-003-5 Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 376

"the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards."

- The SDT considers this a general management issue that is not within the scope of a compliance requirement.
- The SDT found no reliability basis in this requirement.
- The SDT has proposed removing the requirement for documented exceptions to the Cyber Security Policy.

CIP-004-5 Summary of Modifications (1/3)

- Security Awareness
  - Continues to be general awareness that is refreshed quarterly and not formal tracked training
- Training
  - Addition of visitor control program
  - electronic interconnectivity supporting the operation and control of BES Cyber Systems
  - storage media as part of the handling of BES Cyber Systems information
  - Reorganization of requirements into the respective requirements for “program” and “implementation” of the training.

CIP-004-5 Summary of Modifications (2/3)

- Personnel Risk Assessment
  - Changed to only initial identity verification
  - Now includes documenting the processes used to determine when to deny access
  - Reorganization of requirements into the respective requirements for “program” and “implementation”

CIP-004-5 Summary of Modifications (3/3)

- Authorization
  - Consolidated authorization and review requirements from CIP-003-4, CIP-004-4, CIP-006-4 and CIP-007-4
  - Allow quarterly and annual reviews to find and fix problems rather than self-report everything as a violation
- Revocation
  - Remove ability to access BES Cyber System when access no longer needed

CIP-004-5 Addressing FERC Directives (Training)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 433	""we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard."
FERC Order 706 Para. 434	"The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets."
FERC Order 706 Para. 435	"Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves."

- The SDT addressed this by identifying the training topics that should be provided in the Training Program.
- The SDT added this as a topic for role specific training.
- Take actions to remove the ability to access the BES Cyber System when access is no longer required

CIP-004-5 Addressing FERC Directives (Immediate Revocation)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 460

"The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."

- Take actions to remove the ability to access the BES Cyber System when access is no longer required

CIP-005-5 Summary of Modifications

- Define ‘External Connectivity’ for scope modification
- Focus on ‘Electronic Access Points’ vs. ESP
- Require IDS at Control Centers
- Add clarity to ‘secure’ dialups
- Consolidated Monitoring and Vulnerability Assessment Requirements in CIP-007 and CIP-011 respectively
- Removed Appropriate Use Banner
- Incorporated CIP-005-4 Urgent Action revisions

CIP-005-5 Addressing FERC Directives (2 Security Measures – Defense in Depth)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 496

"Commission adopts the CIP NOPR's proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter."

- Deploy methods to inspect communications and detect potential malicious communications for all External Connectivity (Intrusion Detection)

CIP-006-5 Summary of Modifications

- Physical Security Program
  - Must define the operational or procedural controls to restrict physical access
  - Removed current “6 wall” wording to instead require Defined Physical Boundary
  - For High Impact, added the need to utilize two or more different and complementary physical access controls to restrict physical access
  - Testing changed to a 24-month cycle with ongoing discussions of different cycles based on environment

CIP-006-5 Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 572

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."

- The SDT added this for High Impact BES Cyber Assets

FERC Order 706 Para. 581

"The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years,."

- The SDT changed to a 24 month testing cycle but is also still discussing different cycles based on environment

CIP-007-5 Summary of Modifications (1/2)

- Addition of physical I/O port requirement
- Security Patch mgt source requirement
- Non-prescriptive malware requirement
- Security Event Monitoring failure handling
- Bi-weekly log summary/sampling reviews

CIP-007-5 Summary of Modifications (2/2)

- Simplified access-control requirements, removed TFE language while strengthening password requirements
- Added requirement for maintenance devices
- Consolidated vulnerability assessment in CIP-010-5
- Disposal requirement moved to CIP-011-5

CIP-007-5 Addressing FERC Directives (Log Review)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 525	"The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily…"
FERC Order 706 Para. 628	"Requirement R6 of CIP-007-1 does not address the frequency with which log should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly…"

- The SDT Proposes the performance of a review of log summaries or samples every two weeks.

CIP-007-5 Addressing FERC Directives (Malware)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 620

"The Commission will not adopt Consumers' recommendation that every system in an electronic security perimeter does not need antivirus software. Critical cyber assets must be protected, regardless of the operating system being used. Consumers has not provided convincing evidence that any specific operating system is not directly vulnerable to virus attacks. Virus technology changes every day. Therefore we believe it is in the public interest to protect all cyber assets within an electronic security perimeter, regardless of the operating system being used…"

FERC Order 706 Para. 622

"The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above.

- Rewrote the requirement as a competency based requirement that does not prescribe technology.
- Added Maintenance to cover malware on removable media.

CIP-007-5 Addressing FERC Directives (Ports & Services)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

March 18th Order on ports/services

"The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."

- The SDT proposes to address this directive by having a requirement to disable or restrict use of physical I/O ports

CIP-008-5 Summary of Modifications

- Defined Reportable Cyber Security Incident
- Working to harmonize with EOP-004-2
- Includes additional specification on update and lessons learned associated with the response plan

CIP-008-5 Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 661

"the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."

A1

1. Added: Reportable Cyber Security Incidents are either:

- Any malicious act or suspicious event or events that compromise, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a BES Cyber System.

  or

- Any event or events which have either impacted or have the potential to impact the reliability of the Bulk Electric System (Reliability Function CIP-002-5).

2. Retired R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in EOP-004-2, Requirement 1, Part 1.3. Will need to give instruction to report as a "Reportable Cyber Security Event" in EOP-004 space.

3. See R1.1 above

4. Guidance and measurements are being developed accordingly

Slide 33

A1 Rework text format to be consistent with other slide formats (bullets and fonts).Applied to tother slides in CIP-008 and CIP-009 as well.

Author, 8/19/2011

CIP-008-5 Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 673

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.."

Cyber Security - Incident Reporting and Response Planning: Retired R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in EOP-004-2, Requirement 1, Part 1.3 and Attachment 1

CIP-008-5 Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 676

"the Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.."

– Cyber Security - Incident Reporting and Response Planning: Retired R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in EOP-004-2, Requirement 1, Part 1.3.

CIP-008-5 Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 686

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.."

R3.3 and R3.4 Includes additional specification on update of response plan Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls

CIP-009-5 Summary of Modifications

- Added requirement to implement the response plan
- Verification of backup media information prior to storage
- Preservation of data for analysis

CIP-009-5 Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 694

"For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan..We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard"

Added specific R1 requirement to implement recovery plan

CIP-009-5 Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 739

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."

R1.5 Added requirements related to restoration processes based on review of the DHS Controls

CIP-009-5 Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 748

"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."

R1.5 : Processes for the restoration of BES Cyber Systems to the most current baseline configuration

CIP-009-5 Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 706

"Preserve data for analysis"

CIP-009-5 1.6
Requires process to preserve data for analysis

CIP-010-5 Requirements Summary

- The SDT proposes the development of a new Standard CIP-010-5 that consolidates all references to Configuration Change Management and Vulnerability Assessments.
  - Previously these requirements were dispersed throughout CIP-003-4, CIP-005-4, and CIP-007-4

CIP-010-5 Requirements Summary

- The SDT has made changes the Vulnerability Assessment requirements to:
  - Consolidate the previous requirements in CIP-005-4 and CIP-007-4 into a single requirement
  - Make provisions for differences between Control Centers and field assets
  - Respond to FERC Order 706 regarding the performance of “active vulnerability assessments”

CIP-010-5 Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 397

"The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes."

- The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System.
- Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment prior to their implementation in the production environment to aid in identifying any accidental consequences of the change.

CIP-010-5 Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 609	"We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."
FERC Order 706 Para. 610	"we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above."
FERC Order 706 Para. 611	"the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."

- The SDT proposes to require a "representative system" or test system for those High Impact Control Centers to use for the purposes of testing proposed changes and performing active vulnerability assessments.
- The SDT proposes using the defined baseline configuration of a BES Cyber System for the measuring stick as to whether a test system is truly representative of the production system.
- To account for any additional differences between the two systems, the SDT proposes using the words directly from FERC Order 706 "Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments."

CIP-010-5 Addressing FERC Directives

FERC Order 706 Para. 541	"we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments."
FERC Order 706. Para 542	"the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems."
FERC Order 706 Para. 547	"we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"

- The SDT has added requirements for an "active vulnerability" assessment to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System.

CIP-010-5 Addressing FERC Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order 706 Para. 544	"the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification."
FERC Order 706 Para. 544	"we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment"

- The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new cyber asset undergo an active vulnerability assessment.
  - An exception is made for specified exceptional circumstances such as an emergency.

CIP-011-5 Requirements Summary

- The SDT proposes the development of a new Standard CIP-011-5 that consolidates all references to Information Protection and Media Sanitization
  - Previously these requirements were dispersed throughout CIP-003-4 and CIP-007-4
- The SDT has also moved the requirements regarding the authorization and revocation of access to BES Cyber System Information to CIP-004-5, consolidating these requirements with those for electronic and physical access

CIP-011-5 Requirements Summary

- The SDT has introduced a definition of a glossary term “BES Cyber System Information” which defines what needs to be protected
  - Previously, this list was a requirement itself

CIP-011-5 Summary

- The SDT has shifted the focus of the requirements for media sanitization from the Cyber Asset to the information itself
  - In version 4, these requirements are invoked when the Critical Cyber Asset is to be disposed of or redeployed
  - In version 5, the requirement is triggered when either:
    - BES Cyber System Information no longer needs to be stored on specific media, or
    - Media containing BES Cyber System Information is designated for disposal

CIP-011-5 Addressing FERC Directives

FERC Order 706 Para. 633	"The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it."
FERC Order 706 Para 635	"the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."

- The SDT has proposed that preventing unauthorized retrieval of data means to "render the data unrecoverable."
- The SDT understands that this may be too high of a bar and is continuing discussions in this area.

Implementation Plan

- Implementation plan is in the very early phases of development
- Current concepts include staggered Effective Dates for:
  - CIP-002-5
  - Organizational Requirements (CIP-003-5, CIP-008-5)
  - Technical Requirements (CIP-005-5, CIP-006-5, etc.)
- Technical Requirements would be further staggered by:
  - High Impact BES Cyber Systems
  - Medium Impact BES Cyber Systems
  - Low Impact Cyber Systems

Implementation Plan

- Currently evaluating a single implementation plan that would include compliance timelines for future newly identified BES Cyber Systems and those BES Cyber Systems that change categories
  - Eliminates the separate Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (IPFNICCANRE)

Schedule to Date – 2011

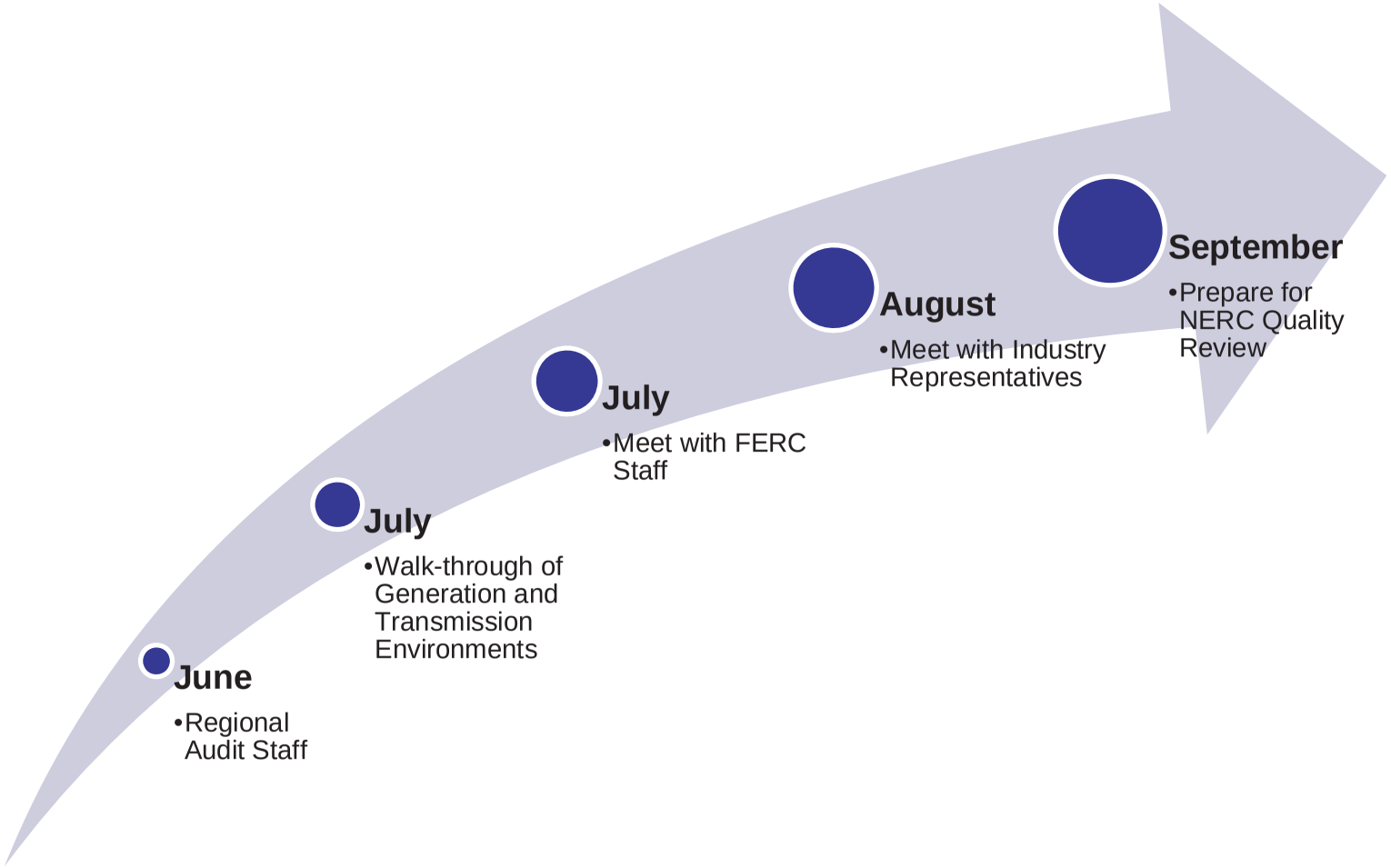

Key Dates Moving Forward

- **November 3rd, 2011 –**
  First Posting for Comment and Ballot
  - Webinars – November 15th and 29th, 2011
  - Ballot Opens – December 9th, 2011
  - Ballot Closing – December 19th, 2011

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions?

Points of Contact:

Philip Huff – philip.huff@aecc.com
Doug Johnson – douglas.johnson@comed.com
David Revill – david.revill@gatrans.com

Slides and Recording of Webinar will be Posted (on NERC Website)

to ensure the reliability of the bulk power system

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	Update
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — BES Cyber Asset and BES Cyber System Categorization

2. **Number:** CIP-002-5

3. **Purpose:** To identify and categorize BES Cyber Assets and BES Cyber Systems that execute or enable functions essential to reliable operation of the BES, for the application of cyber security requirements commensurate with the adverse impact that loss, compromise or misuse of those BES Cyber Assets and BES Cyber Systems could have on the reliability of the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard
   - A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
   - A Transmission Protection System required by a NERC or Regional Reliability Standard
   - Its Transmission Operator's restoration plan

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard

   4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Background:

This standard provides “bright-line” criteria for applicable Responsible Entities to categorize their BES Cyber Systems and BES Cyber Assets based on their impact on the real-time operation of the Bulk Electric System (BES). Several concepts provide the basis for the approach to the standard.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.

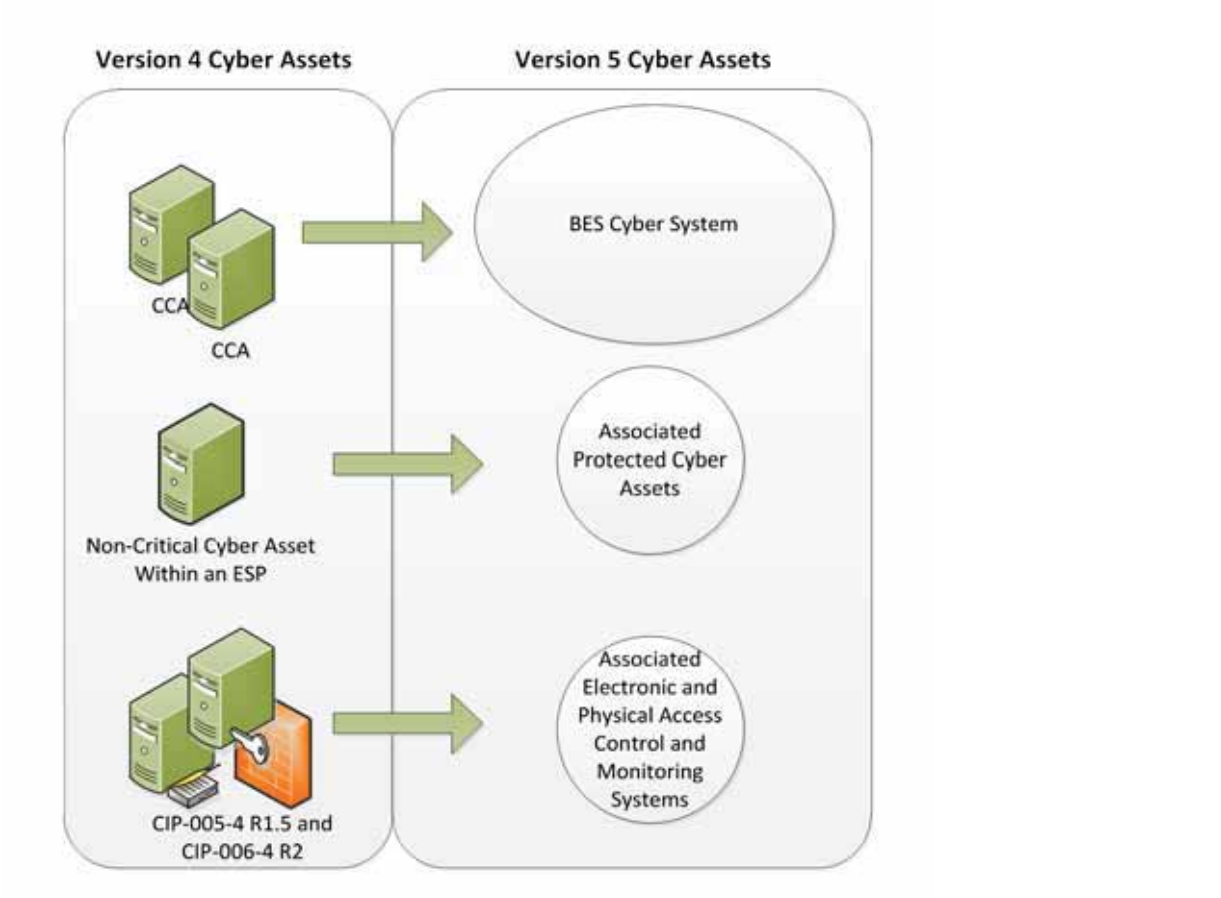

In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets. The CIP Cyber Security Standards use this term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets. So it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term BES Cyber System is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System or they might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

BES Reliability Operating Services

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Assets and BES Cyber Systems that would impact the reliable operation of the BES. In order to identify them, Responsible Entities determine whether the BES Cyber Assets perform or support any BES Reliability Operating Service. These services are functions that provide services for the reliable operation of the BES and are based on the functions defined in the NERC Functional Model. This ensures that the initial scope for consideration includes only those BES Cyber Assets and BES Cyber Systems that perform or support BES Reliability Operating Services. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliability and operability of the BES. To provide a better defined time horizon than “real-time”, BES Cyber Assets are those cyber assets that, if rendered unavailable, degraded, or misused, would impact the BES Reliability Operating Services within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES cyber assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems and their BES Cyber Assets into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems and BES Cyber Assets for those in the High and Medium categories. All other BES Cyber Systems are deemed to be Low Impact.

This general process of categorization of BES Cyber Systems and BES Cyber Assets based on impact on the BES Reliability Operating Services is consistent with risk management approaches for the purpose of application of cyber security controls in the rest of Version 5 cyber security standards.

Requirements and Measures

Rationale – R1:

Cyber Assets and Cyber Systems have varying impact on the reliability and operability of the BES. Once they have been identified, they must be categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. Attachment I provides a set of "bright-line" criteria that the Responsible Entity must use to categorize these BES Cyber Assets and BES Cyber Systems in accordance with their impact on the BES. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

The configuration of the BES is subject to changes due to new demands and requirements for Bulk Power and to environmental changes and operational events. When changes to the BES are planned, the effect of these changes on the set of identified and categorized BES Cyber Assets and BES Cyber Systems must be analyzed to ensure that the adequate level of protection is still applied to them.

R1. Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems.* All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

1.1. Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists identifying the categorization of each of its BES Cyber Assets and BES Cyber Systems in the High and Medium categories as required in R1 and list of changes to the BES (with a date for each change) that cause a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.

Rationale – R2

The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The mis-categorization or non-categorization of a BES Cyber System or BES Cyber Asset can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

R2. The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. (R2)

B. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e., another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 100 High and Medium Impact BES Cyber Assets, 5% or fewer of High and Medium Impact BES Cyber Assets have not been identified or categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer High and Medium Impact BES Cyber Assets, 5 or fewer High and Medium Impact BES Cyber Assets have not been identified or categorized or have	For Responsible Entities with more than a total of 100 High and Medium Impact BES Cyber Assets, more than 5% but less than or equal to 10% of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer High and Medium Impact and BES Cyber Assets, more than 5 but less than or equal to 10 identified BES Cyber Assets have not been categorized or have been incorrectly	For Responsible Entities with more than a total of 100 High or Medium Impact BES Cyber Assets, more than 10% but less than or equal to 15% of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer High or Medium Impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly	For Responsible Entities with more than a total of 100 High and Medium Impact BES Cyber Assets, more than 15% of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer High and Medium Impact BES Cyber Assets, more than 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			been incorrectly categorized at a lower category; Or The Responsible Entity failed to update its documentation of High and Medium Impact BES Cyber Assets in accordance with part 1.1 for more than 30, but less than or equal to 40 calendar days following the completion of the change.	categorized at a lower category; Or The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with part 1.1 for more than 40, but less than or equal to 50 calendar days following the completion of the change.	categorized at a lower category; Or The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with part 1.1 for more than 50, but less than or equal to 60 calendar days following the completion of the change.	The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with part 1.1 for more than 60 calendar days following the completion of the change.
R2	**Operations Planning**	**Lower**	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to requirement R2 for more than 30, but less than or equal to 40 calendar days of the	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to requirement R2 for more than 40, but less than or equal to 50 calendar days of the	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to requirement R2 for more than 50, but less than or equal to 60 calendar days of the	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to requirement R2 for more than 60 calendar days of the latest required date.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			latest required date.	latest required date.	latest required date.	

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

None.

CIP-002-5 - Attachment I

Impact Categorization of BES Cyber Assets and BES Cyber Systems

1. High Impact Rating (H)

Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator or Transmission Owner that includes control of one or more of the assets identified in criteria 2.2, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11 or 2.12 below.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generation Operator that includes control of one or more of the assets identified in criteria 2.1, 2.3, 2.4, or 2.12, below.

2. Medium Impact Rating (M)

Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for:

2.1. Generation with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.2. An aggregate net Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities).

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

2.4. Each Blackstart Resource identified in its Transmission Operator's restoration plan.

2.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource

- Up to and including the first interconnection point of the generation unit(s) to be started, or

- up to the point on the Cranking Path where two or more path options exist and including any single failure points in the Cranking Path to and including the first interconnection point of the generation unit(s) to be started, or
- up to and including the point on the Cranking Path where two or more path options exist to two or more independent generation unit(s) to be started as identified in its Transmission Operator's restoration plan.

2.6. Transmission Facilities operated at 500 kV or higher.

2.7. Transmission Facilities operating at 200 kV or higher, but at less than 500 kV, at a single station or substation that is connected to three or more transmission stations or substations and where the "total weighted aggregate value" of all BES Transmission Lines at a single station or substation operated at 200 KV or higher connected to other transmission stations or substations, including incoming and outgoing lines, exceeds a value of 3,000. The following "weight value per line" operated at the associated voltage value of a line will be used for the determination of the total weighted aggregate value.

Voltage Value of a Line	Weight Value per Line
200 kV to 299 kV	700
300 kV to 499 kV	1300

2.8. Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

In the WECC Region, Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of SOLs and their contingencies for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System".

2.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs), and their associated contingencies.

In the WECC Region, Flexible AC Transmission Systems (FACTS), at a single station or substation location that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of SOLs and their contingencies for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System."

2.10. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.11. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations.

In the WECC Region, each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more System Operating Limits (SOLs) violations for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System" and each RAS listed in the most current table titled " Major WECC Remedial Action Schemes (RAS)."

2.12. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by its regional load shedding program.

2.13. Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners; or (2) generation control centers that control 300 MW or more of generation.

3. Low Impact Rating (L)

All other BES Cyber Assets and BES Cyber Systems not categorized in Section 1 as having a High Impact Rating (H) or Section 2 Medium Impact Rating (M).

Guidelines and Technical Basis

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more **BES Reliability Operating Services**." The new term BES Reliability Operating Service is a defined NERC Glossary term that in turn includes a number of defined named BES Reliability Operating Services. These named, defined services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration performs which reliability operations service, which determines what each entity needs to address with their CIP program. The following provides guidance for Responsible Entities to determine applicable Reliability Operations Services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that should be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, x-formers, generators (TO, GO)
  - Zone protection for breaker failure (TO)
  - Breaker protection (TO)
  - Current, frequency, speed, phase (TO, GO)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays & breakers, possibly software (TO)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA) (RC)

- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)
- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)

- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flowgates (TOP, RC)
-

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP)
- Coordination

Situational Awareness

The Situational Awareness function includes activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include, but are not limited to:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day & Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination and Communication

The Inter-Entity coordination and communication function includes activities, actions and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include, but are not limited to:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC)

Applicability to Distribution Providers and Load Serving Entities

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC standard EOP-005.

Similarly, it is expected that only Load Serving Entities that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. These qualifications are based on the requirements for registration as a Load Serving Entity.

Requirement R1:

R1 implements the methodology for the categorization of BES Cyber Systems and BES Cyber Assets according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the systems are assumed to be vulnerable) and a probability of threat

of 1 (100%). The criteria in attachment 1 provide a measure of the impact on the reliability and operability of the BES.

Responsible Entities are required to identify and categorize those systems that have high and medium impact. Other BES Systems and BES Cyber Assets are deemed to be low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System. While the criteria are based on the scope of the BES asset, this is used here as a measure of the impact of the BES Cyber System for the purpose of categorization.

- When the drafting team uses the term "Facilities", it leaves some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases the criteria refer to a group of Facilities in a given location that support the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that support reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems . Generation Facilities are separately discussed in the Generation section below.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- A BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact

This category includes those BES Cyber Systems, used by and at Control Centers, that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), Transmission Owner (TO) or Generation Operator (GOP), as defined in the NERC Functional Model. While those entities that have been registered as the above named Functional Entities are specifically referenced, it must be noted that there may agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control

Centers that perform these functional obligations must be subject to categorization as High Impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP or GOP facilities.

Medium Impact

Generation

The criteria in Attachment 1, Medium Impact that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are parts 2.1, 2.3, 2.4, 2.5, 2.11 and 2.13.

- Part 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002 whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance". In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of generation capability higher than 1500 MW are adequately protected.

  The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In part 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator as necessary to avoid BES Adverse Reliability Impacts in the long term planning horizon are categorized as Medium Impact. These Facilities may be designated as "Reliability Must Run" and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in

the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

In the specification of the "long-term planning horizon" in this criterion, the drafting team sought to ensure that such BES facilities would be designated in the time horizon described in the NERC document "Time Horizons", which defines long-term planning horizon as "a planning horizon of one year or longer".

If it is determined through system studies that a unit must run in order to preserve the reliability of the BES, such as due to a category C3 contingency as defined in TPL-003 or a category D contingency as defined in TPL-004, then BES Cyber Systems for that unit must be categorized as Medium Impact.

- In part 2.4, BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan are categorized as Medium Impact. NERC standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired. While the definition of Blackstart Resource includes the fact that it is in a Transmission Operator's Restoration Plan, the drafting team included the term in the criterion for clarity.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 2.5 categorizes BES Cyber Systems for Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, with the qualifications stated in the requirement part. This criterion is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started. The drafting team further qualified the Facilities to be designated as subject to BES Cyber System categorization as only those in the Cranking Path up to the point where two or more paths exist to the units to be started and subject to the qualifications in the requirement part.

  Distribution Providers should note that they may have BES Cyber Systems that must be categorized as Medium Impact if they have facilities listed in the Transmission Operator's Restoration Plan.

The following illustrates the parts of the Cranking Path that are subject to CIP Cranking Path criterion.

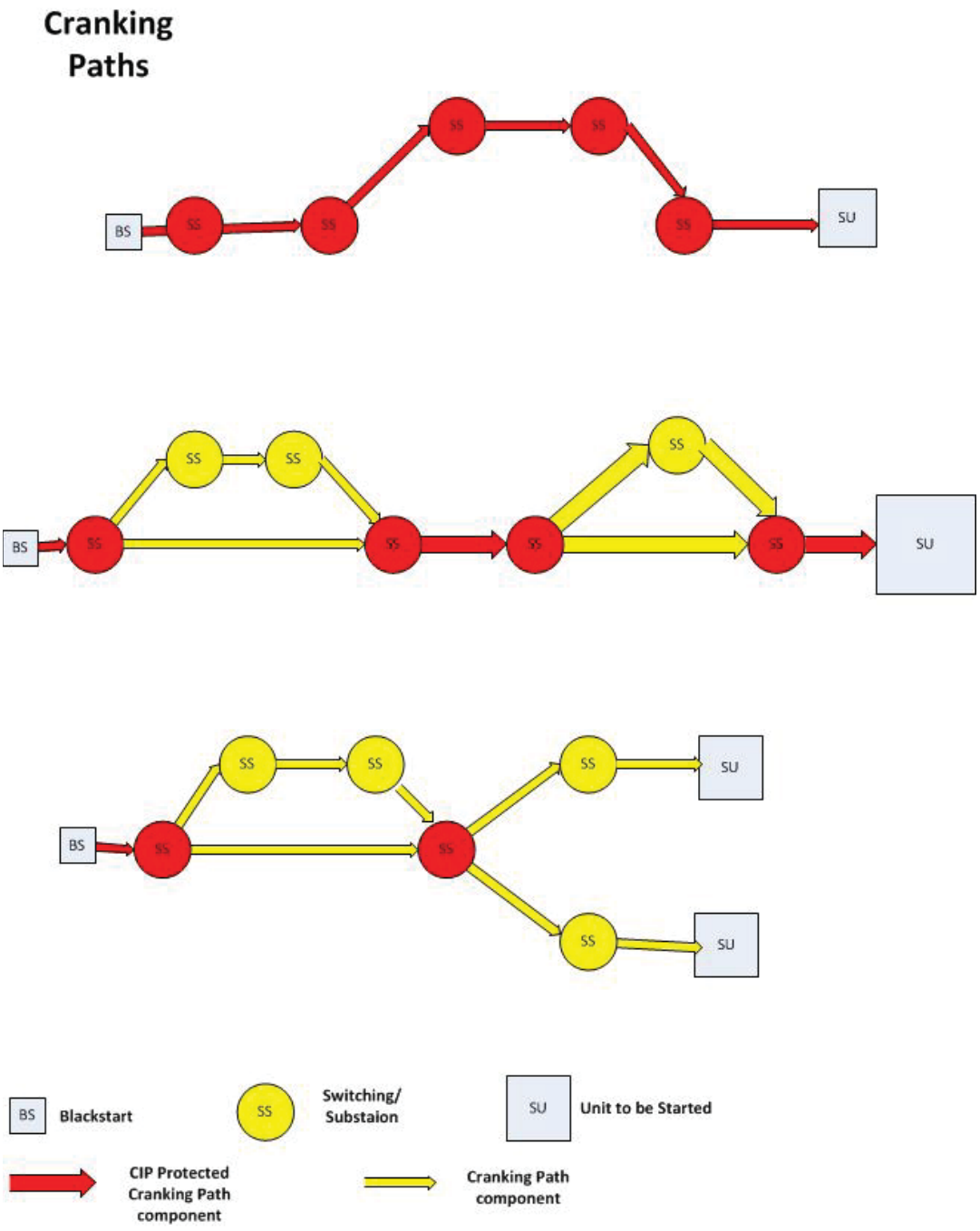

- Part 2.11 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as Medium Impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it

operates outside of the parameters it was designed for. Generation Owners and Operators which own BES Cyber Systems for such systems and schemes must designate them as Medium Impact.

- Part 2.13 categorizes as Medium Impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generation Operator for an aggregate generation of 300 MW or higher. The value of 300 MW is the same value used for UFLS and UVLS. This ensures that Control Centers for significant impact are included. Smaller Control Centers that qualify for the definition of generation Control Centers, but which are really controlling local generation for small downstream generation facilities and do not meet the 300 MW threshold are categorized as Low.

Transmission

Parts 2.1, 2.2, 2.5-2.13 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a system to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). For the WECC region where IROLs are not defined, alternative criteria are defined.

- Part 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. In the case of BES Cyber Systems and BES Cyber Assets owned by Transmission Owners and Operators, this part identifies as Medium Impact those BES Cyber Systems for Transmission Facilities that provide the generation interconnection for Generation of 1500 MW or more to the Transmission system. The intent is to ensure the availability of Facilities necessary to support those generation facilities.

- Part 2.2 includes BES Cyber Systems for those Facilities in Transmission systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- In Part 2.5, the intent is to ensure that BES Cyber Systems for the Cranking Paths and other BES Transmission Facilities required to support the Transmission Operator's restoration plan required by EOP-005-2 receive consideration for protection from cyber threats. Transmission Owners and Operators own and operate a large number of these Facilities. EOP-005-2 specifies Facilities that comprise the "Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started".

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 2.6 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the Medium Impact category.

  It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Part 1.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface". This collector bus would not be a facility for a Medium Impact BES Cyber System because it doesn't significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Part 2.7 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

  - 230 kV –> 700 MVA
  - 345 kV –> 1,300 MVA
  - 500 kV –> 2,000 MVA
  - 765 kV –> 3,000 MVA

- Parts 2.8 and 2.9 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as

specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

Alternate thresholds are used for WECC, where IROLs are not used.

- Part 2.10 is sourced from the NUC-001 NERC standard for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown". In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Part 2.11 designates as Medium Impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

  For the WECC region, alternative thresholds are defined because IROLs are not defined for the region.

- Part 2.12 designates as Medium Impact those BES Cyber Systems for systems or Facilities that are capable of performing automatic load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of criterion 2.13, and chose the term "Each" to represent that the criterion applied to a discrete system or Facility. In the drafting of this criterion, the drafting team sought to include only those systems that did not require human operator initiation, and targeted in particular those Under Frequency Load Shedding (UFLS) facilities and systems and Under Voltage Load Shedding (UVLS) facilities and systems that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. These include automated Under Frequency Load Shedding systems or Under Voltage Load Shedding Systems that are capable of load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as Medium Impact.

  Within an operational environment the drafting team understands that the real-time impact to the Bulk Electric System of a loss of load, or the equivalent amount of generation, will be similar, with loss of load resulting in a frequency high condition and a loss of generation resulting in a frequency low condition. This particular threshold (300 MW) was provided in CIP version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market.

- Part 2.13 categorizes as Medium Impact those cyber systems used by and at Transmission Operators and Owners Control Centers not already categorized as High Impact.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop and implement strategies to mitigate overall risks; and apply applicable security controls.

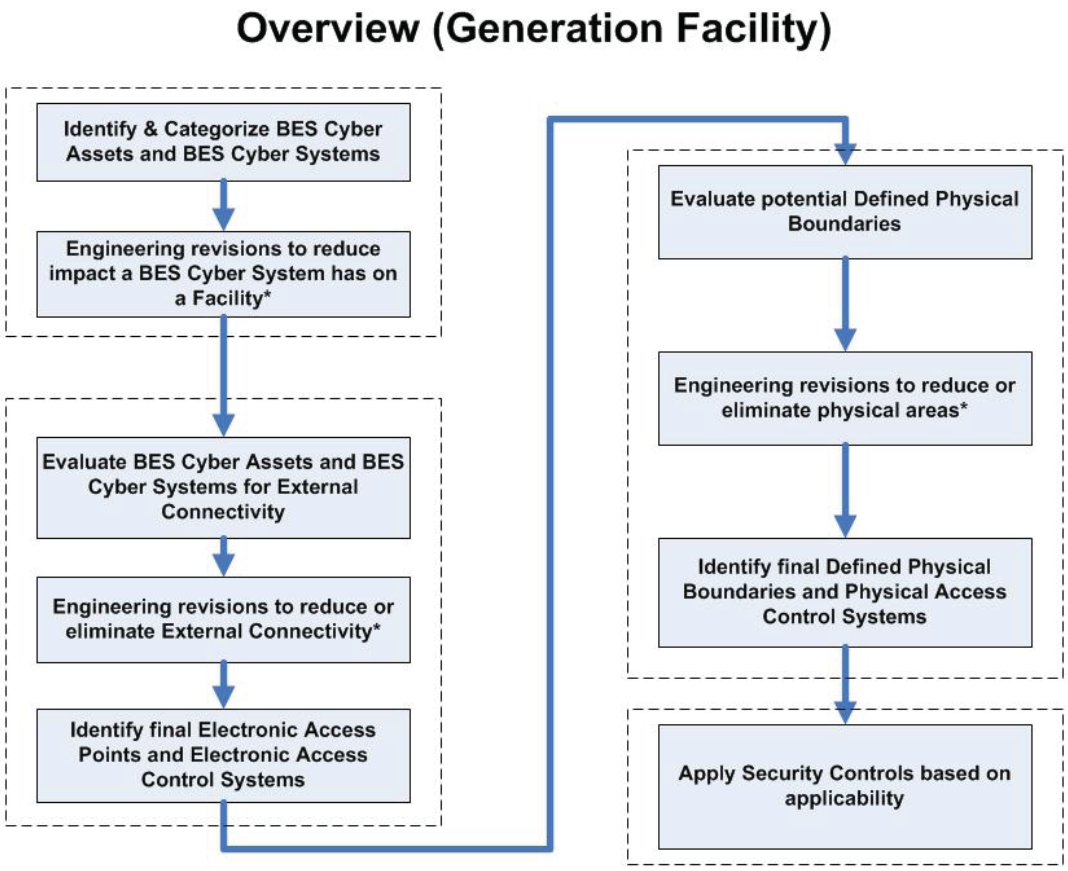

* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: On November 21, 2011, NERC was alerted that the text contained in some of the Rationale boxes for the requirements of CIP-003-5 appeared to be incomplete.

This revised draft corrects the text box size to display all of the text (none of the text was changed).

No other changes were made to this standard or any of the other CIP V5 standards currently posted.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	1/24/11	Update version from "3" to "4". Approved by the NERC Board of Trustees	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: Standard CIP-003-5 requires that Responsible Entities have minimum security management controls in place to protect BES Cyber Assets and BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-003-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Except for R1, R5 and R6, Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems

5. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural

controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with

a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale – R1:

The identification and documentation of the single CIP Senior Manager and any delegations ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43.

In FERC Order 706, paragraph 296, it requests that the SDT consider whether the single senior manager should be a corporate officer or equivalent. The SDT believes that the requirement that the senior manager have "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" ensures that the senior manager is of the sufficient position in the responsible entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R1. Each Responsible Entity shall identify, by name, a CIP Senior Manager. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M1. Evidence may include, but is not limited to:

- A dated and signed document from a high level official designating the name of the individual identified as the CIP Senior Manager
- A dated organizational chart designating the name of the individual identified as the CIP Senior Manager.

Rationale – R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

R2 Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Personnel Security

1.2. Electronic Security Perimeters

1.3. Remote Access

1.4. Physical Security

1.5. System Security

1.6. Incident Response

1.7. Recovery Plans

1.8. Configuration Change Management

1.9. Information Protection

1.10. Provisions for declaring and responding to CIP Exceptional Circumstances

M2. Evidence may include, but is not limited to:

1. One or more documented cyber security policies, and
2. Records that indicate the required ten topics were implemented.

Rationale – R3:

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R3. Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M3. Evidence may include, but is not limited to:

1. Revision history, records of review, or workflow evidence from a document management system that indicate annual review of each cyber security policy, and
2. A dated signature by the CIP Senior Manager for each cyber security policy that indicates annual approval.

Rationale – R4:

The intent of the SDT is to ensure that the responsible entity takes sufficient measures to make its cyber security policy available and accessible to personnel. It is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.

R4. Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. Evidence may include, but is not limited to:

- Policies are accessible on the corporate Intranet site
- Documented records that policies have been provided to contactors where access to BES Cyber Systems is authorized
- Policies are posted on company bulletin boards
- Policies are accessible to individuals with all types of job functions that have access to BES Cyber Systems

- Dated training records to show that individuals have received periodic training on necessary elements of the cyber security policy

Rationale – R5:

In FERC Order 706, paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations in order that this line of authority is clear and apparent from the documented delegations.

R5 The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M5. Evidence may include, but is not limited to:

- A dated document, signed by the CIP Senior Manager listing personnel (by title) who are delegated the authority to approve or authorize specifically identified items (i.e. substation maintenance manager may authorize unescorted physical access to substation control houses), or
- A dated document, signed by the CIP Senior Manager listing individuals who are delegated the authority to approve or authorize specific actions by requirement (i.e., 'name of individual' who may approve CIP-002-5 R3), or
- A dated document, signed by the CIP Senior Manager delegating to a named individual the authority for all approvals in CIP-002-5 and CIP-004-5 through CIP-011-1 as well as the authority to approve subsequent delegations; a dated document, signed by the previous named individual delegating to a 3rd named individual the authority for all approvals in CIP-004-5 through CIP-011-1 as well as the authority to approve subsequent delegations; and a dated document, signed by the 3rd named individual delegating to each of the plant managers (by title) the authority for all approvals and authorizations required in CIP-004-5 through CIP-011-1 for each of the their plants, respectively.

Rationale – R6:

The intent of the SDT is to ensure that delegations are kept up-to-date and that individuals do not assume undocumented authority.

R6. Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change[2]. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]

M6. Evidence may include, but is not limited to, dated documentation that includes the name of the CIP Senior Manager or documentation that includes the names or positions of any delegations, that is current to within 30 days with the name or position of anyone who performed a required approval or authorization.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity.
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.

[2] Delegations do not need to be reinstated with a change in the CIP Senior Manager position or other position with delegation authority.

Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.

If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	**N/A**	**N/A**	**N/A**	The Responsible Entity has not identified, by name, a single senior management official ("the CIP Senior Manager") with overall authority and responsibility for leading and managing implementation of the requirements within the CIP group of standards.
R2	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required parts 2.1 to 2.10.	The Responsible Entity has not implemented any cyber security policy, Or The Responsible Entity has implemented at least one policy but has failed to address two or more of the required parts 2.1 to 2.10.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity has reviewed its cyber security policy or policies, but not all of them have been approved by the CIP Senior Manager within the required time period.	The Responsible Entity has not reviewed the cyber security policy or policies and the CIP Senior Manager has not approved all of them within the required time period.
R4	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity has made some but not all individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function.	The Responsible Entity has not made any individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function.
R5	**Operations Planning**	**Lower**	N/A	The Responsible Entity failed to document the approval and authorization of one delegation (by position or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of two delegations (by position or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of three or more delegations (by position or name of the delegate) as required.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	**Operations Planning**	**Lower**	N/A	NA	Change to one delegation was not documented within 30 calendar days of the effective date.	A change to the CIP Senior Manager, Or more than one delegation was not documented within 30 calendar days of the effective date.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R2:

The number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the ten topical areas required by CIP-003-5 R2. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics or may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In this case of a high-level umbrella policy, it would be expected that the entity provide the high-level policy as well as the additional documentation in order to prove compliance with CIP-003-5 R2. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

2.1 Personnel Security

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account Management

2.2 Electronic Security Perimeters

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points

2.3. Remote Access

- Maintaining up-to-date anti-malware software before initiating interactive remote access
- Maintaining up-to-date patch levels for operating system and applications used to initiate the interactive remote access before initiating interactive remote access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating interactive remote access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s interactive remote access controls

2.4 Physical Security

- Strategy for protecting cyber assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress and egress

2.5 System Security

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

2.6 Incident Response

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

2.7 Recovery Plans

- Availability of spare components
- Availability of system backups

2.8 Configuration Change Management

- Initiation of change requests
- Approval of changes
- Break-fix processes

2.9 Information Protection

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

2.10 Provisions for CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The SDT has removed requirements relating to exceptions to Responsible Entity's security policies since it considers this a general management issue that is not within the scope of a compliance requirement. The SDT considers this an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy

Requirement R3:

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R5:

As indicated in the rationale for CIP-003-5 R5, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the Standard Drafting Team was not to impose any particular organizational structure, but rather the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. As detailed in the examples provided in the Measure, this requirement may be met through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to their organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of the *Version 5 CIP Cyber Security Standards* for a 45-day formal comment period. An initial concept paper, *Categorizing Cyber Systems — An Approach Based on BES Reliability Functions,* was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-5

3. **Purpose:** Standard CIP-004-5 requires that personnel having authorized cyber or authorized unescorted physical access to BES Cyber Assets and BES Cyber Systems, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or regional Reliability Standard
   - A UVLS program required by a NERC or regional Reliability Standard
   - A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard
   - A Transmission Protection System required by a NERC or regional Reliability Standard
   - Its Transmission Operator's restoration plan

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or regional Reliability Standard
   - A UVLS program required by a NERC or regional Reliability Standard

   4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or regional Reliability Standard
- A UVLS program required by a NERC or regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or regional Reliability Standard
- A UVLS program required by a NERC or regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard
- A Transmission Protection System required by a NERC or regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-004-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1

require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: Ensures that personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems maintain awareness of best security practices.

Summary of Changes: Reformatted into table structure.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R1 – Security Awareness Program			
Part	**Applicability**	**Requirements**	**Measures**
1.1	All Responsible Entities	A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	Evidence must include the documented security awareness program, and additional evidence to demonstrate that this program was implemented such as, but not limited to, the quarterly reinforcement material that has been distributed.
Reference to prior version: *CIP-004-4 R1*		**Change Rationale:** *Changed to remove the need to ensure everyone with authorized access receives this awareness. Moved example mechanisms to guidance.*	

Rationale for R2: To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems contains the proper policies, access controls, and procedures to protect BES Cyber Systems.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for
   - the visitor control program;
   - electronic interconnectivity supporting the operation and control of BES Cyber Systems
   - storage media as part of the handling of BES Cyber Systems information
2. Change references from Critical Cyber Assets to BES Cyber Systems

R2. Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*.

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Define the roles that require training.	Acceptable evidence must include a list of roles and what training is needed for each role.
Reference to prior version: NEW		**Change Rationale:** *The first thing needed in a role based training program is to understand what roles your people have to help plan what training modules you need to provide.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicability**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material on the security controls that have been implemented to protect BES Cyber Systems.
Reference to prior version: *CIP004-4 R2.2.1*		**Change Rationale:** *Minor wording changes. Changed to address cyber security issues, not the business or functional use of the BES Cyber System.*	
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material on the proper use of physical access controls for BES Cyber Systems.
Reference to prior version: *CIP004-4 R2.2.2*		**Change Rationale:** *Minor wording changes.*	
2.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.
Reference to prior version: *CIP004-4 R2.2.2*		**Change Rationale:** *Minor wording changes.*	
2.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on the visitor control program.	Evidence may include, but is not limited to, training material on the visitor control program.
Reference to prior version: *NEW*		**Change Rationale:** *Personnel administering the visitor control program and/or providing escort should be part of the core training; FERC Order 706 - paragraph 432.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicability**	**Requirements**	**Measures**
2.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on handling of BES Cyber System Information and storage media.	Evidence may include, but is not limited to, training material on the handling of BES Cyber System Information, including storage media.
Reference to prior version: *CIP004-4 R2.2.3*		**Change Rationale:** *Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage media; FERC Order 706 -paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16)*	
2.7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on identification of a potential BES Cyber Security Incident and associated notifications.	Evidence may include, but is not limited to, training material on the identification of a potential BES Cyber Security Incident and associated notifications.
Reference to prior version: *CIP004-4 R2.2.4 (new; implied but not stated in CIP-004 or CIP-008)*		**Change Rationale:** *Core training on the identification and reporting of a Cyber Security Incident; FERC Order 706 - paragraph 413; Related to CIP-008 & DHS Incident Reporting requirements for those with roles in incident reporting.*	
2.8	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on recovery plans for BES Cyber Systems.	Evidence may include, but is not limited to, training material on recovery plans for BES Cyber Systems.
Reference to prior version: *CIP004-4 R2.2.4*		**Change Rationale:** *Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order 706 - paragraph 413.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicability**	**Requirements**	**Measures**
2.9	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on response to BES Cyber Security Incidents.	Evidence may include, but is not limited to, training material on the response to a BES Cyber Security Incident.
Reference to prior version: *CIP004-4 R2.2.4*		**Change Rationale:** *Minor wording changes.*	
2.10	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Evidence may include, but is not limited to, training material on the electronic interconnectivity and interoperability with other Cyber Assets.
Reference to prior version: *NEW*		**Change Rationale:** *Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order 706 - paragraph 434.*	

Rationale for R3: To ensure that personnel with authorized electronic access or authorized unescorted physical access are trained in the policies, access controls, and procedures to protect the BES Cyber Systems.

Summary of Changes: Re-organization of the training requirements into the respective requirements for "program" and "implementation" of the training.

R3. Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in *CIP-004-5 Table R3 - Cyber Security Training. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M3. Evidence must include, but is not limited to, documentation that the training was provided as defined in *CIP-004-5 Table R3 - Cyber Security Training*.

CIP-004-5 Table R3 – Cyber Security Training			
Part	**Applicability**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, for each individual requiring access, dated individual training records, the date access was first granted, or a dated log or documentation of when CIP Exceptional Circumstances were invoked and revoked.
Reference to prior version: *CIP004-4 R2.1*		**Change Rationale:** *Addition of exceptional circumstances parameters as directed in FERC Order 706 - paragraph 431 is detailed in CIP-003-5..*	

CIP-004-5 Table R3 – Cyber Security Training			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	Evidence may include, but is not limited to, dated individual training records.
Reference to prior version: *CIP004-4 R2.3*		**Change Rationale:** *Updated to further define what "Annual" training means.*	

Rationale for R4: To ensure that individuals who need authorized electronic or unescorted physical access to BES Cyber Systems have been assessed for risk.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.

R4. Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M4. Evidence must include the documented personnel risk assessment program that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*.

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicability**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	An initial personnel risk assessment that includes identity verification.	Acceptable evidence must include the documented risk assessment program with a requirement for an initial personnel risk assessment that includes identity verification.
Reference to prior version: *CIP004-4 R3.1*		**Change Rationale:** *Addressed interpretation request in guidance. Specified that identify verification is only required for each individual's initial assessment.*	

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicability**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	Acceptable evidence must include the documented risk assessment program with a requirement for a seven year criminal history record check in accordance with Requirement R4, Part 4.2.
Reference to prior version: *CIP004-4 R3.1*		**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven year check cannot be performed.*	

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicability**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	Acceptable evidence must include the documented risk assessment program with the criteria or process identified in Requirement R4, Part 4.3.
Reference to prior version: *NEW*		**Change Rationale:** *There should be documented criteria or a process used to evaluate personnel risk assessments.*	
4.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	Acceptable evidence must include the documented risk assessment program with the criteria or process identified in Requirement R4, Part 4.4.
Reference to prior version: *CIP-004-4 R3.3*		**Change Rationale:** *Separated into its own table item.*	

Rationale for R5: To ensure that individuals who have authorized access to BES Cyber Systems have been assessed for risk.

R5. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in *CIP-004-5 Table R5 – Personnel Risk Assessment.[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R5 – Personnel Risk Assessment* and additional evidence to demonstrate that these processes were implemented as described in the Measures column of the table.

CIP-004-5 Table R5 – Personnel Risk Assessment			
Part	**Applicability**	**Requirement**	**Measures**
5.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to: • Dated records showing that personnel risk assessments were completed before access was authorized; • Dated documentation or attestations from contractors or service vendors verifying that personnel risk assessments were conducted pursuant to CIP-004-5 R4 before access was authorized.
Reference to prior version: *CIP-004-3 R3, R3.3*		**Change Rationale**: *Minor wording changes and added the ability to accept attestations from contractors or vendors.*	

CIP-004-5 Table R5 – Personnel Risk Assessment			
Part	**Applicability**	**Requirement**	**Measures**
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Update each personnel risk assessment at least once every seven calendar years after the initial personnel risk assessment.	Evidence may include, but is not limited to, current and former personnel risk assessment records.
Reference to prior version: *CIP-004-4 R3.2*		**Change Rationale:** *Eliminated the "for cause" renewal.*	

Rationale for R6: To ensure that individuals with access to BES Cyber Systems have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and part of the delegations referenced in CIP-003-5.

Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in 6.4 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in R6 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change here involves pulling the access management requirements from CIP-003-4, CIP-004-4 and CIP-007-4 into a single requirement. The requirements from version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

R6. Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in *CIP-004-5 Table R6 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations]*

M6. Evidence must include the documented processes that collectively include each of the applicable items in *CIP-004-5 Table R6 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	Evidence may include, but is not limited to: (i) a system-generated list of people with electronic access and a sampling of accounts to verify unauthorized users do not have access, (ii) a signed document, workflow or email showing such persons have authorization and (iii) similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP 007-4 R5.1, CIP 004-4 R4*		**Change Rationale:** *CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	Evidence may include, but is not limited to: (i) a system generated list of people with unescorted physical access through the Defined Physical Boundary and a sampling of accounts (for automated physical access control) to verify unauthorized users do not have access, (ii) a signed document, workflow or email showing such persons have authorization and (iii) similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP-006-4 R1.5*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	Evidence may include, but is not limited to: (i) a list of people with access to BES Cyber System Information and a sampling of accounts (on electronic document systems) to verify unauthorized users do not have access, (ii) a signed document, workflow or email showing such persons have authorization and (iii) similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP-003-4 R5.2*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003 and CIP-007 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	Evidence may include, but is not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access and a system generated list of personnel who have access • Documentation of the dated verification between a list of individuals who have been authorized for access and a list of individuals provisioned for access.
Reference to prior version: *CIP 004-4 R4.1*		**Change Rationale:** *Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4 R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	Evidence may include, but is not limited to, documentation of the review including (i) a dated listing of all accounts/account groups or roles within the system, (ii) a summary description of privileges associated with each group or role, (iii) accounts assigned to the group or role and (iv) dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.
Reference to prior version: *CIP 007-4 R5.1.3*		**Change Rationale:** *Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	Evidence may include, but is not limited to documentation of the review including (i) a dated listing of authorizations for BES Cyber System information, (ii) any privileges associated with the authorizations, and (iii) dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.
Reference to prior version: *CIP-003-4 R5.1.2*		**Change Rationale:** *Moved requirement to ensure consistency among access reviews. Clarified precise meaning in the term annual. Clarified what was necessary in performing a verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.*	

Rationale for R7: The timely revocation of electronic access to cyber systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address the FERC Order directing immediate revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (i.e. revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services).

Summary of Changes: Paragraphs 460 and 461 of FERC Order 706 state the following: The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate.

R7. Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation*. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning]*

M7. Evidence must include each of the applicable documented programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time[2] of the resignation or termination.	Evidence may include, but is not limited to (i) workflow or sign-off form verifying access removal associated with the terminations and dated concurrent or prior to the date of the termination action, and (ii) a system-generated listing of user accounts or other demonstration showing such persons no longer have access.
Reference to prior version: *CIP 004-4 R4.2*		**Change Rationale:** *The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*	

[2] Since a termination action is often recorded without consideration to the time of day, "at the time" does not require a to-the-minute or to-the-hour time-stamped comparison of access logs and the termination action.

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	Evidence may include, but is not limited to, (i) workflow or sign-off form showing the review of logical and physical authorizations dated on the same calendar day as the transfer or reassignment and (ii) a system-generated listing of user accounts or other demonstration showing such persons no longer have access where the review determined it was no longer needed.
Reference to prior version: *CIP-004-4 R4.2*		**Change Rationale:** *The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	Evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System information associated with the terminations and dated within the next calendar day of the termination action.
Reference to prior version: *NEW*		**Change Rationale:** *The FERC Order 706 Paragraph 386 directs modifications to the Standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	Evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revoking of access and dated within thirty calendar days of the termination.
Reference to prior version: *NEW*		**Change Rationale:** *The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	Evidence may include, but is not limited to: • Workflow or sign-off form showing password reset within thirty calendar days of the termination • Workflow or sign-off form showing password reset within thirty calendar days of the reassignments or transfers.
Reference to prior version: *CIP-007 R5.2.3*		**Change Rationale:** *To provide clarification of expected actions in managing the passwords*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity did not provide on-going security awareness reinforcement on at least a quarterly basis. (1.1)	The Responsible Entity did not document or implement a security awareness program. (R1)
R2	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include training for one or more of the roles as detailed in 2.2 through 2.10.	The Responsible Entity did not have the required role-based training. (R2)
R3	**Operations Planning.**	**Medium**	N/A	N/A	The Responsible Entity trained some but not all individuals authorized for electronic or unescorted physical access at least once every calendar year, but not to exceed 15	The Responsible Entity trained some, but not all individuals authorized for electronic or unescorted physical access prior to their being granted such access, except in

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					months between training. (3.2)	policy-identified CIP Exceptional Circumstances. (3.1) OR The Responsible Entity did not fully implement its cyber security training program.
R4	**Operations Planning**	**Medium**	N/A	The Responsible Entity has a personnel risk assessment program, as stated in R4, for individuals having authorized cyber or authorized unescorted physical access, but the program does not include identity verification or a criminal history records check. (4.1) (4.2)	The Responsible Entity has a personnel risk assessment program, as stated in R4, for individuals having authorized cyber or authorized unescorted physical access, but the program did not include the required documented results or the program did not include criteria or process to determine when authorized access shall not be granted. (4.3)(4.5)	The Responsible Entity did not have a personnel risk assessment program, as stated in R4, for individuals having authorized cyber or authorized unescorted physical access. (R4)
R5	**Same Day**	**Medium**	N/A	N/A	The Responsible Entity	The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations				did perform personnel risk assessments prior to granting authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances, but the personnel risk assessments are not updated at least once every seven years. (5.2)	did not perform personnel risk assessments prior to granting authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances. (5.1) OR The Responsible Entity did not have a documented process for personnel risk assessments.
R6	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work	The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work	The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work	The Responsible Entity did not have its CIP Senior Manager or delegate authorize electronic or unescorted physical access to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			functions. (6.1) (6.2) OR The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions. (6.3)	functions and 1 user was granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2) OR The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions and 1 user was granted access without CIP Senior Manger or delegate authorization. (6.3)	functions and 2 users were granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2) OR The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions and 2 users were granted access without CIP Senior Manger or delegate authorization. (6.3)	functions and 3 or more users were granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2) OR The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions and 3 or more users were granted access without CIP Senior Manger or delegate authorization. (6.3) OR The Responsible Entity did not perform a

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						quarterly verification of individuals with authorized access against one or more lists of individuals provisioned for unescorted physical or electronic access to BES Cyber Systems. (6.4) OR The Responsible Entity did not verify provisioned accounts/account groups or role categories and their specific, associated privileges according to the timeframe in CIP-004-5 6.5 to confirm that access privileges were correct and the minimum necessary to perform the assigned work functions. (6.5) OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not verify the access privileges to BES Cyber System Information according to the timeframe in CIP-004-5 6.6 to confirm that access privileges were correct and the minimum necessary to perform the assigned work functions. (6.6) OR The Responsible Entity did not identify when CIP Exceptional Circumstances were invoked and/or revoked (6.7) OR The Responsible Entity did not have a documented process for access management.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R7	**Same Day Operations and Operations Planning**	**Medium**	N/A	The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for one individuals who was terminated, resigned, reassigned, or transferred. (7.1 and 7.2)	The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for two individuals who were terminated, resigned, reassigned or transferred. (7.1 and 7.2)	The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for three or more individuals who were terminated, resigned, reassigned, or transferred. (7.1 and 7.2) OR The Responsible Entity did not have a documented process for access revocation.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reference sound security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Guidance: Describe example mechanisms used to demonstrate the availability of this information

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the following required items appropriate to personnel roles and responsibilities from Table R4. The training may consist of multiple modules and multiple delivery mechanisms.

Note: Provide guidance or a local definition of "role appropriate" as it is used in this standard.

Requirement R3:

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response.

NOTE: Program specified exceptional circumstances can include a specified individual to declare an emergency.

Requirement R4:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access when called for in CIP-011-1 Table R4 – Personnel Risk Assessment, except for program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response, to ensure that personnel who have such access have had their

identity verified, then been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, or individuals who may have resided in locations from where it is not possible to obtain a criminal history records check.

Requirement R6:

Authorization for electronic and unescorted physical access and access to BES Cyber System information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person.

This requirement specifies both quarterly and annual reviews. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The annual privilege review is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e. least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g. system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in R6 is included below.

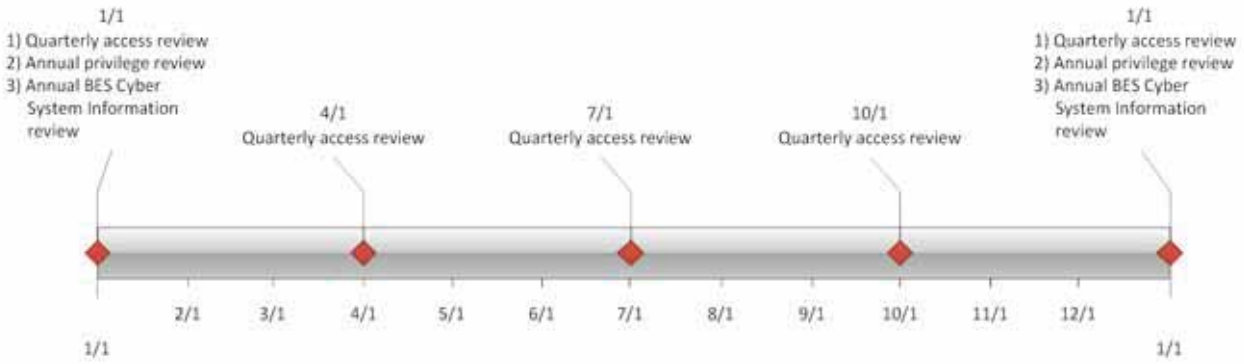

Separation of duties should be considered when performing the reviews in R6. The person reviewing should be different than the person provisioning access.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in R6 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R7:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common examples and possible processes on when the termination action occurs are provided in the following table.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resource personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Termination prior to notification	Human resource personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resource personnel are notified of the termination and works with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resource personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	No action is required.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications

of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in 7.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts on BES Cyber Assets, then the Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents an Entity from performing all of the access revocation at the time termination.

For transferred or reassigned individuals, the requirement states a review of access privileges must be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of the *Version 5 CIP Cyber Security Standards* for a 45-day formal comment period. An initial concept paper, *Categorizing Cyber Systems — An Approach Based on BES Reliability Functions,* was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-5

3. **Purpose:** Standard CIP-005-5 requires the identification of all Electronic Access Points on the Electronic Security Perimeter(s), the protection of the communication through those points, and specific protections for interactive user remote access.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard
   - A Special Protection System or Remedial Action Scheme required by a NERC or Regional reliability standard
   - A Transmission Protection System required by a NERC or Regional Reliability Standard
   - Its Transmission Operator's restoration plan

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or regional Reliability Standard

   4.1.7 NERC

   4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-005-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural

controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These

hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005 R1 has taken more of a focus on the discrete Electronic Access points rather than the logical "perimeter".

CIP-005 R1.2 has been deleted. This requirement was definitional in nature and used to bring dialup modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists, therefore there is no need for this requirement.

CIP-005 R1.1 and 1.3 were also definitional in nature and have been deleted as separate requirements but the concepts were integrated into the definitions of ESP and EAP.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicability**	**Requirements**	**Measures**
1.1	Low Impact BES Cyber Systems with External Routable Connectivity	Define technical or procedural controls to restrict unauthorized electronic access.	Evidence may include, but is not limited to, documented technical and procedural controls that exist and have been implemented.
Reference to prior version: *CIP-005 R1*		**Change Rationale:** *Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones and to prevent access to an aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Protected Cyber Assets	Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	Evidence may include, but is not limited to: • Network diagrams showing EAP identification or • A list of uniquely identifiable Cyber Assets within the BES Cyber System and associated EAPs.
Reference to prior version: *CIP-005 R1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and BES Cyber System*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicability**	**Requirements**	**Measures**
1.3	Electronic Access Points at High Impact BES Cyber Systems Electronic Access Points at Medium Impact BES Cyber Systems with External Routable Connectivity.	Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	Evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only explicit access is allowed and that each access rule has a documented reason.
Reference to prior version: *CIP-005 R2.1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having justification for what it allows through the EAP.*	
1.4	Electronic Access Points that use dial-up access for non-Interactive Remote Access at High Impact BES Cyber Systems Electronic Access Points that use dial-up access for non-Interactive Remote Access at Medium Impact BES Cyber Systems.	Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	Evidence may include, but is not limited to a documented process identified in Requirement R1, Part 1.4 that describes how the Responsible Entity is providing authenticated access through each dial up Electronic Access Point.
Reference to prior version: *CIP-005 R2.3*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point. Added clarification as to the goal of "secure", which is that the BES Cyber System should not be directly accessible with a phone number only*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicability**	**Requirements**	**Measures**
1.5	Electronic Access Points with External Routable Connectivity at High Impact BES Cyber Systems Electronic Access Points with External Routable Connectivity at Medium Impact BES Cyber Systems at Control Centers.	A documented method for detecting malicious communications at each EAP.	Evidence may include, but is not limited to: • Configuration files of an intrusion detection systems deployed at an EAP • Logs that were generated by an intrusion detection system • Documentation showing where intrusion detection systems were deployed.
Reference to prior version: *CIP-005 R1*		**Change Rationale:** *Per FERC Order 706, p 496-503, ESP's need two distinct security measures such that the cyber assets do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear this is not simple redundancy of firewalls, thus the drafting team has decided to add the security measure of malicious traffic inspection (*intrusion detection systems / intrusion protection systems*) a requirement for these ESPs.*	

Rationale for R2: Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of large electric sector entities, necessitate changes to industry security control standards. Currently, no requirements or guidance documents are available to either require or recommend how secure remote access to BES Cyber Systems can or should be accomplished. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

Additional information is provided in *Guidance for Secure Interactive Remote Access* published by NERC in July 2011.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in *CIP-005-5 Table R2 – Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*

M2. Evidence must include the documented processes that collectively address each of the applicable items in *CIP-005-5 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Remote Access Management			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Protected Cyber Assets	Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	Evidence may include, but is not limited to, network diagrams or architecture documents.
Reference to prior version: *New*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Protected Cyber Assets	Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	Evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.
Reference to prior version: *CIP-007 R3.1*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Protected Cyber Assets	Require multi-factor authentication for all Interactive Remote Access sessions.	Evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Note that a UserID is not considered an authentication factor.
Reference to prior version: *CIP-007 R3.2*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning and Same Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not define any technical or procedural controls to restrict unauthorized electronic access OR The Responsible Entity did not establish Electronic Access Points to control and secure access to its BES Cyber Systems OR The Responsible Entity did not establish explicit inbound and outbound access permissions at each identified EAP that utilizes routable protocols OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not perform authentication before establishing connectivity with the BES Cyber System for an EAP that uses dial-up access OR The Responsible Entity did not deploy methods to detect malicious communications.
R2	**Operations Planning and Same Day Operations**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not implement an Intermediate Device between the Interactive Remote Access cyber asset and the BES Cyber System or Protected Cyber Asset OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not implement encryption to protect the confidentiality and integrity of all Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for all Interactive Remote Access sessions.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

CIP-005 R1 requires that BES Cyber Systems must be segmented from other systems of differing trust levels by requiring controlled electronic access points between the different trust zones. ESP's also are used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capabilities.

BES Cyber Systems are to be protected by Electronic Access Points (EAP's) that control traffic into and out of the BES Cyber System. Responsible Entities (RE's) should know what traffic needs to cross an EAP and document those justifications and insure the EAP's limit the traffic to only those known, justified communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

This requirement applies only to communications for which 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols and dialup modems. Direct serial, non-routable connections are not included.

The intent of securing dialup connectivity is to prevent situations where connectivity is established directly to the BES Cyber Asset with only a phone number. If a dialup modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is not functioning as an Electronic Access Point. The requirement calls for some form of authentication of the calling party when connectivity is granted to the BES Cyber Asset. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use.

Since low impact BES Cyber Systems can impact BES Reliability Operating Services in real time, they should not be located directly on public networks or other networks of lesser trust. The intent is to prevent access to an aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES. Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
6. Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)
8. Version 5 of CIP-002 to CIP-011 posted for formal comment and ballot (mm-dd-yy)

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to	

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version	Date	Action	Change Tracking
		FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	1/24/11	Approved by the NERC Board of Trustees	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-5

3. **Purpose:** Standard CIP-006-5 requires the implementation of a physical security plan for the protection of BES Cyber Systems.

4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard
   - A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
   - A Transmission Protection System required by a NERC or Regional Reliability Standard
   - Its Transmission Operator's restoration plan

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard

   4.1.7 NERC

   4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-006-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural

controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required. in the documented processes.. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Low Impact BES Cyber Systems** – Applies to BES Cyber Systems not categorized as High Impact or Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These

hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale: Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed.

Summary of Changes: The entire contents of CIP-006-5 were intended to constitute a physical security program, though there was no specific requirement dictating the need for such a program, only physical security plans.

Added details to address FERC Order 706, paragraph 572 directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address FERC Order 706 p575 directive.

R1. Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations]*

M1. Evidence must includes each of the documented physical security plan or plans that collectively include each of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.1	Associated Physical Access Control Systems Low Impact BES Cyber Systems.	Define operational or procedural controls to restrict physical access.	Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented.
Reference to prior version: *CIP-006-4c R2.1 for Physical Access Control Systems* *New Requirement for Low Impact BES Cyber Systems*		**Change Description and Justification:** *To allow for programmatic protection controls as a baseline, this includes how the entity plans to protect Low Impact BES Cyber Systems and does not require detailed list of individuals with access.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems. Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.
Reference to prior version: *CIP006-4c R3 & R4*		**Change Description and Justification:** *This requirement has been made more general to allow for alternate measures of restricting physical access to reflect the change from Physical Security Perimeter to Defined Physical Boundary. The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section .*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by two or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.
Reference to prior version: CIP006-4c R3 & R4		**Change Description and Justification:** *The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.* *Added to address FERC Order 706 p572 related directives for physical security defense in depth.* *FERC Order 706 p575 directives addressed by providing the examples in the guidance document of physical security defense in depth via multifactor authentication or layered defined physical boundary(s).*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs, or other evidence that documents that these alerts were generated.
Reference to prior version: *CIP006-4c R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section..*	
1.5	Associated Physical Access Control Systems	Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that these alerts were generated
Reference to prior version: CIP006-4c R2.2		**Change Description and Justification:** *Addresses the old CIP-006-4c R5 requirement for Physical Access Control Systems.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicability**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	Evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into Defined Physical Boundaries and additional evidence to demonstrate that this logging and recording has been implemented, such as logs of physical access into Defined Physical Boundaries that show the date of entry into Defined Physical Boundaries.
Reference to prior version: CIP-006-4c R6		**Change Description and Justification:** *CIP-006-4c R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the* Defined Physical Boundary. *Examples of logging methods have been moved to the Guidelines and Technical Basis section .*	

Rationale: To control when personnel without authorized unescorted physical access can be in any Defined Physical Boundaries protecting BES Cyber Systems or Electronic Access Control Systems as applicable in table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

R2. Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M2. Evidence must include the documented visitor control program that collectively includes each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	Evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Defined Physical Boundaries and additional evidence to demonstrate that the process was implemented, such as visitor logs.
Reference to prior version: *CIP-006-4c R1.6.2*		**Change Description and Justification:** *No change.*	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicability**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	Evidence may include, but is not limited to, a visitor control program that provides logging of the entry and exit of visitors including date, time, and visitor name along with the individual point of contact; dated visitor logs for each Defined Physical Boundary that include the same required information.
Reference to prior version: *CIP-006-4c R1.6.1*		**Change Description and Justification:** *Addressed multi entry requirements and added the point of contact which is the person who can be considered the sponsor for the visitor. There is no need to document the escort or handoffs between escorts.*	

Rationale: To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order 706, paragraph 581 directives for test more frequently than every three years.

R3. Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M3. Evidence must include each of the documented maintenance and testing programs that collectively include each applicable item in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Maintenance and Testing Program			
Part	**Applicability**	**Requirement**	**Measures**
3.1	Associated Physical Access Control Systems Locally mounted hardware or devices associated with Defined Physical Boundaries	Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	Evidence may include, but is not limited to a maintenance and testing program that provides for testing the Physical Access Control Systems and locally mounted hardware or devices associated with Defined Physical Boundaries prior to commissioning and at least once every 24 calendar months thereafter, and provides additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed at least once on each applicable device or system at least once every 24 calendar months.
Reference to prior version: *CIP-006-4c R8.1*		**Change Description and Justification:** *Added details to address FERC Order 706 p581 directives to test more frequently than every three years. It was felt annually testing was too often.*	
3.2	Associated Physical Access Control or Monitoring Systems	Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	Evidence may include, but is not limited to, availability of the outage records.
Reference to prior version: *CIP-006-4c R8.3*		**Change Description and Justification:** *Outage records shall be generated but the retention period is addressed in the retention section.*	

C. Compliance

1. Compliance Monitoring Process

5.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- For responsible entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

5.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

5.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

5.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has documented and implemented physical access controls, but logging of authorized physical entry through any Defined Physical Boundary does not provide sufficient information to uniquely identify the individual and date of entry. (Part 1.7)	The Responsible Entity has documented and implemented physical access controls, but it does not alert for unauthorized physical access to Physical Access Control Systems (Part 1.5)	The Responsible Entity has documented and implemented physical access controls, but does not alert for unauthorized access through any access point in a Defined Physical Boundary. (Part 1.4) OR The Responsible Entity has documented and implemented physical access controls, but does not initiate a response within 15 minutes of a detected unauthorized physical access into a Defined Physical Boundary. (Part 1.6)	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access to only those individuals who are authorized. OR The Responsible Entity has documented and implemented physical access controls, but two or more different and complementary methods do not exist to restrict access to High Impact BES Cyber Systems. (Part 1.3)
R2	**Same-Day**	**Medium**	N/A	The Responsible Entity included a visitor control program in its	The Responsible Entity included a visitor control program in its	The Responsible Entity has failed to include or implement a visitor

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations			physical security plan, but did not log each of the entry and exit dates and times of the visitor on a daily basis, the visitor's name, and the point of contact.	physical security plan, but it does not meet the requirements of continuous escort.	control program to provide required escorted access of visitors within any Defined Physical Boundary protecting BES Cyber Systems.
R3	**Long Term Planning**	**Lower**	N/A	The Responsible Entity has documented and implemented a maintenance and testing program, but the testing is not performed on a cycle of not more than 24 months.	The Responsible Entity has documented and implemented a maintenance and testing program, but not all outage records regarding access controls, logging, and alerting are generated as required.	The Responsible Entity has not documented and implemented maintenance and testing programs.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary control for controlling, alerting and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods to restrict physical access include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Defined Physical Boundary.

Methods to alert on physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order 706 p572 directive, directed the intent of utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Defined Physical Boundaries, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin-code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in

combination with a guard-monitored remote camera and door release, where the “guard” has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (i.e. key or card key) would provide access through both.

Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Defined Physical Boundary to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

It is also felt a Point of Contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Defined Physical Boundary. This includes motion sensors, electronic lock control mechanisms and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Outage records should address when the installed control, monitor and logging systems or hardware at access points are broken or unavailable.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of the *Version 5 CIP Cyber Security Standards* for a 45-day formal comment period. An initial concept paper, *Categorizing Cyber Systems — An Approach Based on BES Reliability Functions,* was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees	
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-5

3. **Purpose:** Standard CIP-007-5 requires the implementation of technical mechanisms for reducing the risk of loss of availability due to degradation and misuse of BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard
   - A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
   - A Transmission Protection System required by a NERC or Regional Reliability Standard
   - Its Transmission Operator's restoration plan

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard

   4.1.7 NERC

   4.1.8 Regional Entity

   4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-007-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization

processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and physical I/O ports.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are documented with reasons why they are necessary. In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M1. Evidence must include the documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicability**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	Evidence may include, but is not limited to, documentation of the need for each network-accessible port and screen shots showing the accessible ports of BES Cyber Assets.
Reference to prior version: *CIP-007-4 R2.1 and R2.2*		**Change Description and Justification:** *The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	Evidence may include, but is not limited to, documentation stating specific or types of physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage.
Reference to prior version: *NEW*		**Change Description and Justification:** *In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.*	

Rationale for R2: Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source (s) to monitor for release of security related patches, hotfixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" there has been confusion as to what constitutes the availability. Due to issues that may occur regarding Control System vendor license and service agreements flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	Evidence may include, but is not limited to, a list of sources that are monitored on an individual BES Cyber System or BES Cyber Asset basis. The list could be sorted by BES Cyber System or source.
Reference to prior version: *New*		**Change Rationale:** *Defining the source(s) that a Responsible Entity monitors for the release of security related patches, hotfixes, and/or updates will provide a starting point for assessing the effectiveness of the patch management program. Documenting the source is also used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicability**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	Evidence may include, but is not limited to, an assessment conducted by, referenced by, or on behalf of a Registered Entity of security-related patches or updates released by the documented sources, and a dated remediation plan showing how the vulnerability will be addressed.
Reference to prior version: *CIP-007 R3.1*		**Change Rationale:** *Similar to the current wording but added "from the identified source" to establish where the release is from. The current wording: "The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" has led to varying opinions as to what constitutes "availability" of the patches or upgrades. The addition attempts to clarify where the release is from.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicability**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	A process for remediation, including any exceptions for CIP Exceptional Circumstances.	Evidence may include, but is not limited to: • Exports from automated patch management tools that provide installation date; • Verification screen captures that show BES Cyber System Component software revision; • Registry exports that show software has been installed; • Evidence that affected services have been disabled; • Implementation evidence of software configuration changes recommended by the operating system or Control System vendors.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *CIP-007 R3.2*		**Change Rationale:** This is the same concept as in the current CIP-007 R3.2 wording however a 30 day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used. Splitting the implementation of security related patches, hotfixes, and/or updates into a separate item from compensating measures will provide granularity. Automated processes allow the implementation to be documented and confirmed electronically in a short time period. Manual processes may take an extended period of time to complete documentation of the installation. Priority should be given to the implementation rather than the documentation.	

Rationale for R3: Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable components of a BES Cyber system. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

The requirement for Maintenance Cyber Assets or media in 3.4 is intended to ensure that devices used for maintenance do not accidently introduce malicious code into the BES Cyber System or introduce an unauthorized external access point to the BES Cyber System.

This requirement also clarifies that these devices may be temporarily connected to the BES Cyber System, but do not become a part of the BES Cyber System, nor are they considered Protected Cyber Assets. These devices may be temporarily connected locally to the BES Cyber System for maintenance, but must be protected from introducing malicious code.

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of TFE's as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of cyber assets in scope of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection.

Beginning in paragraph 619-622 of FERC Order 706, and in particular 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"

In paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R3 – Malicious Code Prevention. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M3. Evidence must include each of the documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicability**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Deploy method(s) to deter, detect, or prevent malicious code.	Evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (i.e. through traditional antivirus, system hardening, policies, etc.).
Reference to prior version: *CIP-007-4 R4* *CIP-007-4 R4.1*		**Change Rationale:** *See the Summary of Changes.*	
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Disarm or remove identified malicious code.	Evidence may include, but is not limited to: • Predetermined response actions for malicious code detection; • Configuration of anti-virus response actions (i.e. quarantine, alert, etc.) to detected malicious code; • Configuration of white-listing application to notify appropriate personnel of unauthorized applications.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-4 R4* *CIP-007-4 R4.1*		**Change Rationale:** *See the Summary of Changes.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	Evidence may include, but is not limited to, (i) current signature or pattern updates, and (ii) either screen shots showing the configuration of signature, or pattern updates for automated controls, or work logs showing the signature, or pattern updates for manual controls.
Reference to prior version: *CIP-007-4 R4* *CIP-007-4 R4.2*		**Change Rationale:** *See the Summary of Changes.*	
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *New*		**Change Rationale:** *FERC Order 706 paragraph 621 states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software. In addition, a common interpretation of the current standards is that any device connecting inside the ESP must at that point be in compliance with the full set of Standards. This requirement makes clear that the device performing maintenance is not considered a part of the BES Cyber System.*	
3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log each Transient Cyber Asset connection.	Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets.
Reference to prior version: *New*		**Change Rationale:** *FERC Order 706 paragraph 621 states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software. In addition, a common interpretation of the current standards is that any device connecting inside the ESP must at that point be in compliance with the full set of Standards. This requirement makes clear that the device performing maintenance is not considered a part of the BES Cyber System.*	

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the immediate detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor and respond to audit processing failures.

Summary of Changes: Beginning in paragraph 525 and also 628 of the FERC Order 706, the commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4 R5 and CIP-007-4 R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms “security event” and “monitor”.

The term “security event” or “events related to cyber security” is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the system.

In addition, this requirement sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

R4. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment]

M4. Evidence must include each of the documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicability**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	Evidence may include, but is not limited to, a paper or system generated listing of event classes for which the BES Cyber System is configured to generate logs. This listing must include the required event types.
Reference to prior version: *CIP-005-4 R3, CIP-007-4 R5, R5.1.2 R6.1, R6.3*		**Change Description and Justification:** *This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP as required in CIP-005-4 R3 and user access and activity logs as required in CIP-007-5 R5 are also included here.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicability**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	Evidence may include, but is not limited to paper or system-generated listing of event classes and conditions which necessitate real-time alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert; Screen-shots showing how real-time alerts are configured.
Reference to prior version: *CIP-005-4 R3.2, CIP-007-4 R6.2*		**Change Description and Justification:** *This requirement is derived from alerting requirements in CIP-005-4 R3.2 and CIP-007-4 R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicability**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Detect and activate a response to event logging failures before the end of the next calendar day.	Evidence may include, but is not limited to, (i) dated event logging failures and screen-shots showing how real-time alerts were configured (ii) dated records showing that personnel were dispatched or a work ticket was opened to review and repair logging failures.
Reference to prior version: *New Requirement*		**Change Rationale:** *This requirement was derived from NIST 800-53 version 3 AU-5, which addresses response to audit processing failures. Some interpretations of version 4 CIP Cyber Security Standards considered the failure of the security event monitoring and alerting system to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.*	
4.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	Evidence may include, but is not limited to, security-related event logs from the past ninety days and records of disposition of security-related event logs beyond ninety days up to the evidence retention period.
Reference to prior version: *CIP-005-4 R3.2, CIP-007-4 R6.4*		**Change Rationale:** *No substantive change.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicability**	**Requirements**	**Measures**
4.5	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred, and dated evidence showing that personnel were dispatched or a work ticket was opened to rectify the deficiency.
Reference to prior version: *CIP-005-4 R3.2, CIP-007-4 R6.5*		**Change Description and Justification:** *Beginning in paragraph 525 and also 628 of the FERC Order 706, the commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.*	

Rationale for R5: To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Changing default passwords closes an easily exploitable vulnerability in many systems and applications.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Summary of Changes (From R5): CIP-007-4 R5.2.2 and R5.2.3 requiring the identification and management of shared account access have been removed. These requirements already exist in the authorization, security event monitoring and revocation of access, and guidance for these requirements makes clear the consideration of shared accounts. The requirement to identify and determine acceptable use for these accounts remains and the Standard includes additional guidance on types of accounts to identify and appropriate use of these account types.

CIP-007-4 R5.3 requires the use of passwords and specifies a specific policy of 6 characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT feels these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

R5. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R5 – System Access Controls. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in CIP-007-5 Table 5 – System Access Controls and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Validate credentials before granting electronic access to each BES Cyber System.	Evidence may include, but is not limited to, documentation describing how users are authenticated before being granted access and demonstrations showing authenticated access enforcement of internal and remote paths to the BES Cyber System.
Reference to prior version: *CIP-007-4 R5*		**Change Rationale:** *The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	Evidence may include, but is not limited to, a listing of accounts by account types and signed documentation or workflow by a CIP Senior Manager or delegate showing the approval of account types in use for the BES Cyber System.
Reference to prior version: *CIP-007-4 R5.2, R5.2.1*		**Change Rationale:** *CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*	
5.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Identify individuals who have authorized access to shared accounts.	Evidence may include, but is not limited to, listing of shared accounts and the individuals who have access to each shared account.
Reference to prior version: *CIP-007-4 R5.2.2*		**Change Rationale:** *No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
5.4	All Responsible Entities	Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	Evidence may include, but is not limited to: • Demonstration showing default vendor passwords have been changed, sampled on a locational basis. • Records of a procedure that passwords are changed when new devices are deployed. • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
Reference to prior version: *CIP-007-4 R5.2.1*		**Change Rationale:** *The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	Evidence may include, but is not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length, complexity and periodicity of changing passwords. • Attestations by individuals that the procedurally enforced passwords meet the password parameters.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-4 R5.3*		**Change Rationale:** *CIP-007-4 R5.3 requires the use of passwords and specifies a specific policy of 6 characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process..*	
5.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	Evidence may include, but is not limited to: • Screen-shots of the account-lockout parameters • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.
Reference to prior version: *New Requirement*		**Change Rationale:** *Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	N/A	The Responsible Entity did not document the logical network accessible ports and include why the ports are necessary.	The Responsible Entity did not disable or restrict access to unnecessary logical network accessible ports. OR The Responsible Entity did not disable or restrict the use of unnecessary physical ports used for network connectivity, console commands, or removable media.
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity did not identify a source or sources that are monitored for the release of security related patches, hotfixes, and/or updates for all software and firmware

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						associated with the BES Cyber System or BES Cyber Assets. OR The Responsible Entity did not identify applicable security related patches, hotfixes, and/or updates and create a remediation plan, or revise an existing remediation plan within 30 days of release from the identified source. OR The Responsible Entity did not implement the remediation plan as required, except for CIP Exceptional Circumstances.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Same Day Operations**	**Medium**	N/A	N/A	The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code on all Cyber Assets, Transient Cyber Assets and removable media.	The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. OR The Responsible Entity did not disarm or remove identified malicious code. OR Where signatures or patterns are used, the Responsible Entity did not deploy method(s) to update malicious code protections within 30 days of signature or pattern update availability.
R4	**Same Day Operations and Operations**	**Medium**	N/A	The Responsible Entity failed to identify and implement methods to review a summarization of	The Responsible Entity failed to identify and implement methods to generate real-time alerts for event logging	The Responsible Entity failed to identify and implement methods to

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Assessment			logged events every two weeks to identify unanticipated Cyber Security Incidents and potential event logging failures, and activate a response before the end of the next calendar day.	failures, and activate a response to rectify the event logging failure before the end of the next calendar day. OR The Responsible Entity failed to identify and implement methods to retain BES Cyber System generated security-related events for at least the last 90 consecutive days, where technically feasible.	generate alerts for events that it determines to necessitate a real-time alert. OR The Responsible Entity failed to identify and implement methods to log generated events that it determines necessary for the identification and after-the-fact investigation of Cyber Security Incidents.
R5	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity failed to implement procedures to authorize the use of administrative, shared, default, and other generic account types. OR The Responsible Entity	The Responsible Entity failed to implement methods to validate credentials before granting electronic access to BES Cyber Systems. OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					failed to implement procedures to identify the individuals with authorized access to shared accounts.	The Responsible Entity failed to implement procedures for password-based user authentication. OR The Responsible Entity failed to implement procedures to change or have unique default passwords, where technically feasible.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

Requirement 1 exists to reduce the attack surface of BES Cyber Assets by requiring entities to disable known unnecessary ports. The intent is for the entity to know what is accessible on their assets and systems, why they are needed, and disable or restrict access to all other ports.

1.1. For the logical network ports this is most often accomplished by disabling the corresponding service or program that is listening on the port. It can also be accomplished through using host-based firewalls or other means on the device to restrict access. This control is another layer in the defense against network-based attacks, therefore it is the intent that the control be on the device itself; blocking ports at a perimeter does not satisfy this requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed necessary.

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Defined Security Boundary in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem or inserting a USB drive with auto-run capability. In cases where the Component cannot logically restrict physical ports, entities should have clear signs or obstructions indicating the unnecessary ports are not to be used.

Requirement R2:

The intent of R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an “install every security patch” requirement; its main intention is to “be aware of in a timely manner and manage all known vulnerabilities” requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with a low tier documents establishing the more detailed process followed for individual systems. Low tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. *Documenting the source is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.* The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors

could all be sources to monitor for release of security related patches, hotfixes, and/or updates. In the event that software or firmware is no longer supported by a software or firmware vendor or Control System vendor it can be noted in your source document. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. The security patches, hotfixes, and/or updates or compensating measures may reduce the reliability of the system. The Responsible Entity must be allowed to evaluate their individual risk exposure and determine if actions must be taken to secure the system.

2.2. The intent is for Responsible Entities to perform an assessment of security related patches as they are released from their monitored source and create a remediation plan for applicable patches as to how the vulnerability will or has already been remediated. An assessment should consist of determination of the applicability of the entity's specific environment and systems. IF the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, and the steps the entity has previously taken or will take. If the entity has to take steps to mitigate this new vulnerability, the remediation plan will include a timeframe. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration". The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

Common malware introduction methods include web browsing, email attachments, and portable storage media. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware, it is not practical within the standard to prescribe how malware is to be addressed on each component. Rather, the Responsible Entity determines on a BES Cyber System basis which components have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional anti-virus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or components that are of identical architecture, they may provide one process that describes how all the components are covered.

For malware detection technologies that are updated in response to evolving threats or depend on signatures of known attacks, the entity must specify how those updates are tested before implementation. The testing should not negatively impact the reliability of the BES. The testing is focused on the update itself and if it will have an adverse impact on the BES Cyber System. The testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on insuring that the update does not negatively impact the BES Cyber System before those updates are placed into production. This includes the instance where the update may provide a "false positive."

Requirement R4:

Refer to NIST 800-92 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the Standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent that if a device cannot log a particular event that a TFE must be generated. The intent is that if any of the items in the bulleted list (for example, user logouts) can be

logged by the device, but the entity disables or neglects to enable that logging, it is a violation. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3. Event logging failures occur when the components of the BES Cyber System cannot log events the Responsible Entity designated in 4.1. The most common reason for event logging failures is the event log being filled up beyond its configured storage threshold. However, there may be any number of other reasons for event logging failures.

For centralized logging systems, it should not be considered a failure if communication goes down between the cyber asset and the logging system if the cyber asset can store the logs locally for a period of time until the communication comes back up.

4.5. Reviewing logs every two weeks can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Data Base.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.

5.3. Where possible, any accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

The requirement to change passwords permits the Responsible Entity to determine the periodicity of the password change in their policies and procedures based on a number of factors. The following table suggests appropriate periodicity requirements for passwords based on these factors.

Account Type	Impact Level	Significance of passwords in preventing unauthorized access	Existing Service Agreements	Suggested Periodicity of Password Change
User account password	High	Primary access path	None.	90 days
User account password	Medium	Primary access path	None.	180 days
Shared account Password for a microprocessor relay, PLC, RTU, etc.	Medium	Local access path. Individuals must authenticate at an upstream device prior to gaining access.	None.	During regularly scheduled maintenance
Shared account password for a generation control system	Medium	Local access path. Individuals must authenticate at an upstream device prior to gaining access.	None.	During scheduled plant outages
Administrative account passphrase with 15+ characters	High or Medium	Local access path. Remote user must be authenticated using a different account	None.	1 year
System account password with 25+ pseudo-random characters	High or Medium	Local access path	None.	2 years or more

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008)
2. SC authorized moving the SAR forward to standard development (July 10, 2008)
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
6. Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)
8. Version 5 of CIP-002 to CIP-011 posted for formal comment and ballot (mm-dd-yy)

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-5

3. Purpose: Standard CIP-008-5 requires the identification, classification, response, and reporting of BES Cyber Security Incidents related to BES Cyber Assets and BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-008-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.
- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization

processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers –** Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity –** Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems –** Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems –** Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets –** Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Plans associated with High Impact BES Cyber Systems or Medium Impact BES Cyber Systems -a**pplies to any plan associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points –** Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a

Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: So that consistent responses to BES Cyber Security Incidents involving BES Cyber Assets and BES Cyber Systems occur. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Once the number and severity of events rises to the level of becoming a reportable incident NERC EOP 4 directs further external reporting actions and timing requirements. When a requirement applies to All Responsible Entities, the drafting team proposes that an enterprise or single incident response plan for all BES Cyber Systems may be submitted. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: (FERC directives, most significant items, summary of smaller items)

R1. Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications			
Part	**Applicability**	**Requirements**	**Measures**
1.1	All Responsible Entities	Processes to identify, classify, and respond to BES Cyber Security Incidents.	Evidence may include, but is not limited to, dated copies of BES Cyber Security Incident response plan(s) that include how to identify, classify, and respond to BES Cyber Security Incidents targeting the Electronic Security Perimeter or Defined Physical Boundary of a BES Cyber System and covers incidents that impact the reliability of BES.
Reference to prior version: *CIP-008 R1.1*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
1.2	All Responsible Entities	A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	Evidence may include, but is not limited to, dated documentation of process(es) that provide guidance or thresholds for determining which BES Cyber Security Incidents are also Reportable BES Cyber Security Incidents.
Reference to prior version: *CIP-008 R1.1*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications			
Part	**Applicability**	**Requirements**	**Measures**
1.3	All Responsible Entities	Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that addresses roles and responsibilities of BES Cyber Security Incident response personnel, BES Cyber Security Incident handling processes or procedures, and communication processes or procedures.
Reference to prior version: *CIP-008 R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

Rationale for R2: Added testing requirements to verify the REs response plan's effectiveness and consistent application in responding to a BES Cyber Security Incident(s) impacting a BES Cyber System.

R2. Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in *CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable items in *CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicability**	**Requirements**	**Measures**
2.1	All Responsible Entities	When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	Evidence may include, but is not limited to, incident reports, logs, and notes that were kept during the incident response process, and documentation that lists and justifies deviations taken from the plan during the incident.
Reference to prior version: *CIP-008 R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged. Allows deviation from plan during actual events or testing if deviations are recorded for review.*	

CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicability**	**Requirements**	**Measures**
2.2	All Responsible Entities	Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise.
Reference to prior version: *CIP-008 R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
2.3	All Responsible Entities	Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	Evidence may include, but is not limited to, dated documentation related to Reportable BES Cyber Security Incidents.
Reference to prior version: *CIP-008 R2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

Rationale for R3: Conduct sufficient reviews, updates and communications to verify the REs response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Summary of Changes: Addressed BES Cyber Security Incident response plan review, update, and communication specifications to ensure that BES Cyber Security Incident response plans remain updated and individuals are aware of the updates.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment and Real-Time Operations]*

M3. Evidence must include each of the applicable documented processes that include each of the applicable items in *CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update and Communication* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.1	All Responsible Entities	Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	Evidence may include, but is not limited to, dated documentation of a review of each BES Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 calendar months, and an updated BES Cyber Security Incident response plan if necessary.
Reference to prior version: *CIP-008 R1.5*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan.
Reference to prior version: *CIP-008 R1.5*		**Change Description and Justification:** *Included requirement for review after testing or actual response based on review of DHS controls*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan.
Reference to prior version: *CIP-008 R1.4*		**Change Description and Justification:** *Included additional specification on update of response plan Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls*	

CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Part**	**Part**	**Part**
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	Acceptable evidence may include, but is not limited to, updated documentation reflecting changes made to the BES Cyber Security Incident response plan in response to organizational or technology changes.
Reference to prior version: *CIP-008 R1.4*		**Change Description and Justification:** *Included additional specification on update of response plan Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls*	
3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	Evidence of communication of updates may include, but is not limited to: • Emails • USPS or other mail service • Electronic distribution system • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added specific timing requirement on communication of plan changes based on review of the DHS Controls*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed a BES Cyber Security Incident response plan, but the plan does not define the roles and responsibilities of response personnel, or does not define incident handling procedures, or does not communicate the incident to appropriate organizations.	The Responsible Entity has not developed a BES Cyber Security Incident response plan to identify, classify, and respond to BES Cyber Security Incidents. OR The Responsible Entity has developed a BES Cyber Security Incident response plan, but the plan does not identify Reportable BES Cyber Security Incidents.
R2	**Operations Planning** **Real-time Operations**	**Lower**	N/A	N/A	N/A	The Responsible Entity does not use its BES Cyber Security Incident response plan when an incident occurs. OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						has not tested the execution of its BES Cyber Security Incident response plan once each calendar year, not to exceed 15 calendar months between executions of the plan.
R3	**Operations Assessment** **Real-time Operations**	**Lower**	N/A	N/A	The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 30 calendar days of execution. OR The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans within 30 calendar days of any	The Responsible Entity has not reviewed the results of each of its BES Cyber Security Incident response plan(s), test or actual incident response, within 30 calendar days of execution. OR The Responsible Entity has reviewed and updated each of its BES Cyber Security Incident response plans but has not communicated all

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					system, organizational, or technology change that impacts one of the response plans.	updates to all responsible personnel.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

FAQ, SP99, ISA, US-CERT, NIST Guidelines, etc. as a source of materials

Requirement R1:

A Reportable BES Cyber Security Incident is a BES Cyber Security Incident that results in a necessary response action. A response action can fall into one of two categories: necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions should be designated as necessary.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
6. Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)
8. Version 5 of CIP-002 to CIP-011 posted for formal comment and ballot (mm-dd-yy)

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Assets and Systems

2. **Number:** CIP-009-5

3. **Purpose:** Standard CIP-009-5 ensures that recovery plan(s) related to the storing of backup information are put in place for BES Cyber Assets and BES Cyber Systems and that these plans support and follow established business continuity and disaster recovery techniques and practices.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard
   - A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
   - A Transmission Protection System required by a NERC or Regional Reliability Standard
   - Its Transmission Operator's restoration plan

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard

   4.1.7 NERC

   4.1.8 Regional Entity

   4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-009-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The

referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For

example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is therefore necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber Assets and BES Cyber Systems occurs.

Summary of Changes:

Added provisions to protect data that would be useful in the investigation of an event that results in the need for a cyber system recovery plan to be utilized.

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicability**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Conditions for activation of the recovery plan(s).	Evidence may include, but is not limited to one or more plans that include language identifying specific conditions for activation of the recovery plan(s).
Reference to prior version: *CIP-009 R1.1*		**Change Description and Justification:** *Reworded to address FERC Order 706 P694 and simplify the wording.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicability**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	Evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders, including identification of the individuals responsible for recovery efforts.
Reference to prior version: *CIP-009 R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and protection of information required to successfully restore a BES Cyber System.
Reference to prior version: *CIP-009 R4*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Part**	**Part**	**Part**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	Evidence may include, but is not limited to, dated evidence of the verification that the backup process completed successfully.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Addresses FERC Order Section 739 and 748.*	
1.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	Evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive, making a data mirror of the system before proceeding with recovery, or taking the important assessment steps necessary to avoid reintroducing the precipitating or corrupted data.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added requirement to address FERC Order 706, paragraph 706.*	

Rationale for R2: To verify the Responsible Entities Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

NIST SP 800-84 identifies the following types of exercises widely used in information system programs by single organizations:

Tabletop Exercises. Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.

Functional Exercises. Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, system equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements.28 Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with a full operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
Reference to prior version: *CIP-009 R2*		**Change Description and Justification:** *Minor wording change; essentially unchanged.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	Evidence may include, but is not limited to, dated evidence of a test of any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *CIP-009 R5*		**Change Description and Justification:** *Combined Requirement from CIP-009 R5 included requirement to test when initially stored. Addresses FERC Requirements (739, 748) related to testing of backups.*	
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	Evidence may include, but is not limited to: • Dated evidence of an operational exercise initially upon the effective date of the standard and at least once every 39 calendar months between exercises, that demonstrates recovery in a representative environment; • An actual incident response occurred within the 39 calendar month timeframe that implemented the recovery plans.
Reference to prior version: *CIP-009 R2*		**Change Description and Justification:** *Addresses FERC Requirement (725) to add the requirement that the recovery plan test be a full operational test once every 3 years.*	

Rationale for R3: To enable the continued effectiveness of the Responsible Entities response plan's for planned and consistent restoration of BES Cyber System(s).

Summary of Changes:

Addressed recovery plan review, update, and communication specifications to ensure that recovery plans remain updated and individuals are aware of the updates.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M3. Acceptable evidence includes, but is not limited to, each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	Evidence may include, but is not limited to, dated evidence of a review of the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, including documentation of any identified deficiencies.
Reference to prior version: *CIP-009 R1*		**Change Description and Justification:** *Added the requirements to additionally review plans after system replacement. Also added requirement for documentation of any identified deficiencies or lessons learned.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	Evidence may include, but is not limited to, dated evidence of a review of the results of each recovery plan test or actual incident recovery within thirty calendar days of the of the completion of the exercise, documenting any identified deficiencies or lessons learned.
Reference to prior version: *CIP-009 R3*		**Change Description and Justification:** *Added the timeframe for update.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	Evidence may include, but is not limited to, dated documentation of updates to the recovery plan(s).
Reference to prior version: *CIP-009 R3*		**Change Description and Justification:** *Added the timeframe for update.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Part**	**Part**	**Part**
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	Evidence may include, but is not limited to, dated documentation of organizational or technology changes, and dated documentation updates to the recovery plan(s).
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery plans stay updated.*	
3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	Evidence of communication of updates may include, but is not limited to: • Emails • USPS or other mail service • Electronic distribution system • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery personnel are aware of any changes to recovery plans.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Medium**	N/A	N/A.	The Responsible Entity has developed recovery plans, but the plans do not address all of the requirements included in Items 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Assets and BES Cyber Systems that address the conditions for activation, including roles and responsibility of responders; processes for backup, storage, and protection of information; storage of essential information to BES Cyber System recovery; and preservation of BES Cyber System Information for analysis and diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service.
R2	**Long Term**		N/A	N/A	The Responsible Entity has not tested the	The Responsible Entity has failed to conduct a

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning	**Lower**			information used in the recovery of BES Cyber Systems that is stored on backup media initially and at least once each calendar year not to exceed 15 calendar months between tests. OR The Responsible Entity has not tested the recovery plan initially upon the effective date of the standard and at least once each 3 years, not to exceed 39 calendar months between tests, that is an operational exercise in a representative environment to demonstrate readiness.	recovery plan test initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between tests.
R3	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has not reviewed and	The Responsible Entity has not reviewed its

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					documented the results of its recovery plan test or actual incident recovery within 30 calendar days of its execution. OR The Responsible Entity has not updated its recovery plan based on any documented deficiencies or lessons learned within 30 calendar days of its execution.	recovery plan(s) initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, or when BES Cyber Systems are replaced. OR The Responsible Entity has reviewed and updated all of its recovery plans but has not communicated all updates to all responsible personnel within 30 calendar days of completing the updates.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

(SEE FAQs AND CIPC GUIDELINES AS A BASIS)

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the configuration management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Configuration Management and Vulnerability Assessments

2. **Number:** CIP-010-1

3. **Purpose:** Standard CIP-010-1 requires that Responsible Entities have minimum configuration management and vulnerability assessment controls in place to protect BES Cyber Assets and BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard
   - A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
   - A Transmission Protection System required by a NERC or Regional Reliability Standard
   - Its Transmission Operator's restoration plan

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard

   4.1.7 NERC

   4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-010-1

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-010-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural

controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale – R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	Evidence may include, but is not limited to: • A spreadsheet identifying the required items of the baseline configuration for each BES Cyber Asset in the BES Cyber System; • A record in an asset management system that identifies the required items of the baseline configuration for each BES Cyber Asset in the BES Cyber System.
Reference to prior version: *New Requirement*		**Change Rationale:** *The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	Evidence may include, but is not limited to: • A change request record and associated electronic approval (performed by the individual with the authority to authorize the change) in a change management system for each change; • A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) where an individual with the authority to authorize the change was in attendance.
Reference to prior version: *CIP-007-3 R9* *CIP-003-3 R6*		**Change Rationale:** *The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3 R6.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	Evidence may include, but is not limited to: • For changes that impacted the categorization of a BES Cyber System, dated categorization documents, with a date that is within 30 days of the date of the completion of the change; • For changes that impacted the CIP-009-required recovery plan of a BES Cyber System, a dated recovery plan, with a date that is within 30 days of the date of the completion of the change.
Reference to prior version: *CIP-007-3 R9*		**Change Rationale:** *Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	Evidence includes, but is not limited to a list of security controls verified or tested along with the dated test results.
Reference to prior version: *CIP-007-3 R1*		**Change Rationale:** *The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.5	High Impact BES Cyber System	For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	Evidence includes, but is not limited to, a list of security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.
Reference to prior version: *CIP-007-3 R1*		**Change Rationale:** *This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.* *This change addresses FERC Order ,paragraphs 397, 609, 610, and 611*	

Rationale – R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R2 – Configuration Monitoring			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	Evidence may include, but is not limited to, logs from a system that is monitoring the configuration of the BES Cyber System along with records of investigation for any unauthorized changes that were detected by the system.
Reference to prior version: *New Requirement*		**Change Rationale:** *The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.* *This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order 706, paragraph 397.DHS Catalog & addresses FERC Order 706, paragraph 397.*	

Rationale – R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of security controls as well as to continually improve the security posture of BES Cyber Systems.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicability**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the output of the tools used to perform the assessment.
Reference to prior version: *CIP-005-4, R4 and CIP-007-4, R8*		**Change Rationale:** *As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order 706 p. 541, 542, 544, 547* *As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.*	
3.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems	Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new BES Cyber Asset) and the output of the tools used to perform the assessment.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order 706 p. 541, 542, 544, 547*	
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	Evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items with proposed dates of completion, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).
Reference to prior version: *CIP-005-3 R4.5* *CIP-007-3 R8.4*		**Change Rationale:** *Added a requirement for an entity planned date of completion as per the FERC directive in Order 706, paragraph 643.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for since the last completed audit or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	**N/A**	The Responsible Entity updated the baseline configuration, but failed to update the required documentation within 30-days of the change being completed.	The Responsible Entity has established a configuration management program, but failed to establish a documented baseline. OR The Responsible Entity has established a configuration management program, but failed to have the CIP Senior Manager or delegate authorize any changes to the baseline configuration and to document those changes. OR The Responsible Entity has established a configuration management program, but with respect to the	The Responsible Entity has not established any configuration management programs. OR Did not implement a configuration management program.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					changes in the baseline configuration, did not determine the required cyber security controls that could be impacted by the changes; or did not verify that the controls were not adversely affected when the change was implemented.	
R2	**Operations Planning**	**Lower**	**N/A**	**N/A**	The Responsible Entity has established a configuration monitoring process for changes to the baseline but failed to document a detected unauthorized change.	The Responsible Entity has not established a configuration monitoring process for changes to the baseline. OR The Responsible Entity has not investigated a detected unauthorized change to the baseline configuration.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Planning**	**Medium**	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months but less than 18 months since the last assessment on one of its applicable BES Cyber Systems.	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not performed an Active Vulnerability Assessment on a new BES Cyber Asset prior to adding it to an applicable BES Cyber System. OR The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months but less than 24 months since the last assessment on one of its applicable BES Cyber Systems.	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. OR The Responsible Entity has not established any vulnerability assessment processes for one of its applicable BES Cyber Systems.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				performed a vulnerability assessment more than 18 months but less than 21 months since the last assessment on one of its applicable BES Cyber Systems.		OR The Responsible Entity has established and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but failed to perform an Active Vulnerability Assessment in a test environment that models the baseline configuration of its applicable BES Cyber Systems. OR The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, and the execution status of the mitigation plans.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The physical location referred to in the baseline configuration is geographically where the BES Cyber Asset is located (e.g. Pine Valley Control Room, Generator X, Substation Y) and should be used to ensure that BES Cyber Systems receive the controls that are applicable to the environment in which the components are located (e.g. control center, transmission facility, generation facility). The physical location is not intended to be a specific floor plan location (e.g., panel A, rack B). As such, the physical location of virtual component should identify where the virtual components are being executed (e.g. Pine Valley Control Room, Generator X, Substation Y).

The Control Center test environment should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, patch level, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple.

Additionally, the entity should note that wherever a test environment is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a control center BES Cyber System which may not be able to be replicated such as a legacy map-board controller or the numerous data communication links from the field or to other control centers (such as by ICCP).

Requirement R2:

It should be understood that the intent of R2 is to require automated monitoring of the BES Cyber System. However, the Standards Drafting Team understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). It is for this reason that automated technical monitoring was not explicitly required and an entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should not that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well documented in the initial NOPR from FERC as well as FERC Order 706. In developing their Vulnerability Assessment processes, Responsible Entities are strongly encouraged to include at least the following elements:

Paper Vulnerability Assessment

1. Network Discovery - A review of all Electronic Access Points to the Electronic Security Perimeter
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification

3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications

Active Vulnerability Assessment

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-1

3. **Purpose:** Standard CIP-011-1 requires that Responsible Entities have protection controls in place to protect BES Cyber System Information.

4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard
   - A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
   - A Transmission Protection System required by a NERC or Regional Reliability Standard
   - Its Transmission Operator's restoration plan

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS program required by a NERC or Regional Reliability Standard
   - A UVLS program required by a NERC or Regional Reliability Standard

   4.1.7 NERC

   4.1.8 Regional Entity

   4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 The following are exempt from Standard CIP-011-1:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-011-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization

processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale – R1:

The intent of the information protection processes is to prevent unauthorized access to BES Cyber System Information.

Summary of Changes:

Requirement R4.1 was moved to the definition of BES Cyber System Information.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-011-1 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include the applicable items in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R1 – Information Protection			
Part	**Applicability**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	One or more methods to identify BES Cyber System Information.	Evidence may include, but is not limited to, • Indications on information (e.g., labels) that identify it as BES Cyber System Information; • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber Security Information.
Reference to prior version: *CIP-003-3 R4* *CIP-003-3 R4.2*		**Change Rationale:** *The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.*	

CIP-011-1 Table R1 – Information Protection			
Part	**Part**	**Part**	**Part**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Access control and handling procedures for BES Cyber System Information.	Evidence may include, but is not limited to: • Records indicating information that is stored, transported, and disposed in a manner consistent with the documented process; • Records from an information management system containing electronic copies of BES Cyber System Information with user access implemented on a need-to-know basis; • Hardcopies of information stored in a locked file cabinet with keys provided to only authorized individuals.
Reference to prior version: *CIP-003-3 R4* *CIP-003-3 R5.3*		**Change Rationale:** *The SDT removed the language to "protect" information and replaced it with "Implement handling and access control" to clarify the protection that is required.*	

CIP-011-1 Table R1 – Information Protection			
Part	**Part**	**Part**	**Part**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence to demonstrate that the action plan was implemented.
Reference to prior version: *CIP-003-3 R4.3*		**Change Rationale:** *No significant changes*	

Rationale – R2:

The intent of the media reuse and disposal processes is to prevent the unauthorized dissemination of BES Cyber System Information upon media reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-011-1 Table R2 – Media Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-011-1 Table R2 – Media Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	**Applicability**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Prior to the release for reuse of BES Cyber Asset media[2], the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was cleared prior to its reuse.
Reference to prior version: *CIP-007-3 R7.2*		**Change Rationale:** *(FERC Order 706 - p. 631) Consistent with FERC Order 706, paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*	

[2] For the purposes of this Standard, media should be considered to be any mass storage device onto which information from a BES Cyber Asset is recorded and stored electronically, including, but not limited to, magnetic tapes, optical disks, solid-state drives, and magnetic disks.

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	**Applicability**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was purged or destroyed prior to its disposal.
Reference to prior version: *CIP-007-3 R7.1*		**Change Rationale:** *Consistent with FERC Order 706, paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.* *The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	**N/A**	**N/A**	The Responsible Entity has implemented one or more BES Cyber System Information protection processes that include one or more methods to identify BES Cyber System Information and one or more access control and handling procedures for BES Cyber System Information, but has failed to assess adherence, either initially upon the effective date of the standard or periodically, to its BES Cyber System Information protection processes.	The Responsible Entity has not implemented one or more BES Cyber System Information protection processes. OR The Responsible Entity has implemented one or more BES Cyber System Information protection processes, but has not included one or more methods to identify BES Cyber System Information OR The Responsible Entity has implemented one or more BES Cyber System Information protection processes, but has not included one or more access control and handling

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						procedures for BES Cyber System Information.
R2	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity has documented or implemented one or more media disposal or reuse processes to prevent the unauthorized retrieval of BES Cyber System Information from the media, but the media disposal or reuse processes, including the recording of the media purge or destruction, were not followed.	The Responsible Entity has not documented or implemented any media disposal or reuse process to prevent the unauthorized retrieval of BES Cyber System Information from the media.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

Assumptions: Entities are free to utilize existing change management and asset management systems. However, the information contained within these systems must be evaluated as the information protection requirements still apply.

While separating BES Cyber System Information into separate classifications is not required as it was in version 4, responsible entities still have the flexibility to do this if they so desire. As long as the entity's information protection program includes all required elements, additional classification levels can be created that go above and beyond the requirements.

This requirement is not intended to cover publicly available information such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. Information handling procedures should detail access, sharing, copying, transmittal, distribution, and disposal or destruction of BES Cyber System Information.

Requirement R2:

Media sanitization is generally classified into 4 categories: disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly erased using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan For Version 5 CIP Cyber Security Standards

November 7, 2011

Prerequisite Approvals

All Version 5 CIP Cyber Security Standards and the proposed additions, modifications, and retirements of terms to the *Glossary of Terms Used in NERC Reliability Standards* must be approved before these standards can become effective.

Applicable Standards

The following standards and definitions, collectively referred to as "Version 5 CIP Cyber Security Standards[1]," are covered by this Implementation Plan:
CIP–002–5 —Cyber Security — BES Cyber System Identification
CIP–003–5 — Cyber Security — Security Management Controls
CIP–004–5 — Cyber Security — Personnel and Training
CIP–005–5 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–5 — Cyber Security — Physical Security
CIP–007–5 —Cyber Security — Systems Security Management
CIP–008–5 — Cyber Security — Incident Reporting and Response Planning
CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems
CIP–010–1 — Cyber Security — Configuration Change Management
CIP–011–1 — Cyber Security — Information Protection
"Definitions of Terms Used in Version 5 CIP Cyber Security Standards" document, which includes proposed additions, modifications, and retirements of terms to the *Glossary of Terms Used in NERC Reliability Standards*.

These standards and Definitions of Terms Used in Version 5 CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

When these standards and Definitions of Terms Used in Version 5 CIP Cyber Security Standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards and Definitions of Terms Used in Version 5 CIP Cyber Security Standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:
• Reliability Coordinator
• Balancing Authority

[1] Although CIP-010-1 and CIP-011-1 are proposed as first versions, any reference to "Version 5 CIP Cyber Security Standards" includes CIP-010-1 and CIP-011-1 in addition to CIP-002-5 through CIP-009-5 because CIP-010-1 and CIP-011-1 were developed as part of the "Version 5 CIP Cyber Security Standards" development process.

• Interchange Authority
• Transmission Owner
• Transmission Operator
• Generator Owner
• Generator Operator
• Load Serving Entity
• Distribution Provider
• NERC
• Regional Entity

Proposed Effective Date for Version 5 CIP Cyber Security Standards

Responsible Entities shall comply with requirements in CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1, and the Definitions of Terms Used in Version 5 CIP Cyber Security Standards as follows:

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[2]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Unplanned Changes Resulting in a Higher Categorization

Planned changes refer to any changes of the electric system or BES Cyber System as described in CIP-002-5 R1.1 which were planned and implemented by the Responsible Entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5 Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must therefore be in Compliance with the Version 5 CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

[2] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System as described in CIP-002-5 R1.1 which were not planned by the Responsible Entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5 Attachment 1. Then, later, an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified, changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, and that unchanged BES Cyber System may become a Medium Impact BES Cyber System based on the CIP-002-5 Attachment 1 criteria. The actions that cause the change in power flows would have been performed by a neighboring entity and would result in a change in impact level the of the affected BES Cyber System.

For *planned* changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System as required in CIP-002-5 R1.1

For *unplanned* changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards according to the following timelines following the identification and categorization of the affected BES Cyber System as required in CIP-002-5 R1.1:

Scenario of Unplanned Changes	Compliance Implementation
New High Impact BES Cyber System	12 months
New Medium Impact BES Cyber System	12 months
Newly categorized High Impact BES Cyber System from Medium Impact BES Cyber System	12 months for new requirements
Newly categorized Medium Impact BES Cyber System	12 months
Responsible Entity Identifies first Medium or High Impact BES Cyber System	Add 12 months from time above

Additional Guidance and Implementation Time Periods for Disaster Recovery

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003-5 R2.

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability

and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Definitions of Terms Used in Version 5 CIP Cyber Security Standards

This section includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards and proposes terms for retirement. Terms already defined in the Glossary of Terms used in NERC Reliability Standards are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary. New defined terms are underscored. For existing glossary terms, new language is shown as underscored, while deleted language is shown as stricken. The list of terms proposed for retirement is at the end of the document.

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

BES Cyber Security Incident

~~Any~~ A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter ~~or Physical Security Perimeter of a Critical Cyber Asset~~, or~~,~~
- Disrupts, or was an attempt to disrupt, the operation of a ~~Critical Cyber Asset~~ BES Cyber System, or
- Results in unauthorized physical access into a Defined Physical Boundary .

BES Cyber System

One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.

BES Cyber System Information

Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans.

BES Reliability Operating Services

BES Reliability Operating Services are those services contributing to the real-time reliable operation of the Bulk Electric System (BES). They include the following Operating Services:

Dynamic Response to BES conditions

Actions performed by BES Elements, Facilities or systems automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition.

Aspects of BES Dynamic Response include, but are not limited to:

- Spinning reserve (contingency reserves)
  - Providing actual reserves
  - Monitoring that reserves are sufficient
- Governor Response
  - Control system used to actuate governor response

- Protection Systems (transmission & generation)
  - Line, bus, x-former, generator
  - Zone protection
  - Breaker protection
  - Current, frequency, speed, phase
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays & breakers, possibly software
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers
- Power System Stabilizers

<u>Balancing Load and Generation</u>

Activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time.

Aspects of the Balancing Load and Generation Operating Service include, but are not limited to:

- Calculation of ACE
  - Field data sources (real time tie flows, frequency sources, time error, etc)
  - Software used to perform calculation
- Unit commitment
  - Know generation status & capability & restrictions (must runs, minimum run times, ramp, heat rates, etc), load schedules
- Load management
  - Ability to identify load change need
  - Ability to implement load changes
- Demand Response
  - Ability to identify load change need
  - Ability to implement load changes
- Manually Initiated Load shedding
  - Ability to identify load change need
  - Ability to implement load changes
- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time

- Start units and provide energy

Controlling Frequency (Real Power)

Activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES.

Aspects of the Controlling Frequency Operating Service include, but are not limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics
  - Software to calculate unit adjustments
  - Transmit adjustments to individual units
  - Unit controls implementing adjustments
- Regulation (regulating reserves)
  - Frequency source, schedule
  - Governor control system

Controlling Voltage (Reactive Power)

Activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES.

Aspects of the Controlling Voltage Operating Service include, but are not limited to:

- AVR (Automatic Voltage Regulation)
  - Sensors, stator control system, feedback
- Capacitive resources
  - Status, control (manual or auto), feedback
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback
- SVC (Static VAR Compensators)
  - Status, computations, control (manual or auto), feedback

Managing Constraints

Activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES.

Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC)

- Interchange schedules
- Generation re-dispatch and unit commit
- Identify and monitor SOL's & IROL's

Identify and monitor Flowgates

Monitoring & Control

Activities, actions, and conditions that provide monitoring and control of BES elements.

An example aspect of the Monitoring and Control Service is, but is not limited to:

- All methods of operating breakers and switches (such as SCADA)

Restoration of BES

Activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance.

Aspects of the Restoration of BES Operating Service include, but are not limited to:

- Blackstart restoration including planned cranking path
- Off-site power for nuclear facilities.

Situational Awareness

Activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions.

Aspects of the Situation Awareness Operating Service include, but are not limited to:

- Monitoring and alerting (such as EMS alarms)
- Change management
- Current Day & Next Day planning
- Contingency Analysis
- Frequency monitoring

Inter-Entity Real-Time Coordination and Communication

Activities, actions, and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES.

Aspects of the Inter-Entity Coordination and Communication Operating Service include, but are not limited to:

- Scheduled interchange
- Facility operational data and status
- Operational directives

CIP Exceptional Circumstance

A situation that involves one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of the requirements within the NERC CIP Standards.

Control Center

One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,
- Inter-utility exchange of BES reliability or operability data,
- Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES,
- Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function,
- Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES
- Coordination of BES restoration activities.

Cyber Assets

Programmable electronic devices ~~and communication networks~~ including the hardware, software, and data in those devices.

Defined Physical Boundary ("DPB")

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside and for which access is controlled.

Change Rationale: "Defined Physical Boundary (DPB)" replaces "Physical Security Perimeter." *Previous versions of the CIP standard focused on the development of a completely enclosed Physical Security Perimeter (PSP) ("six-wall" border) and managing access though this boundary. This has proven difficult due to the nature of the operating environment for many electrical utilities, especially in field locations. The intent of this standard is to focus on the controls put in place to restrict access rather than solely focusing on the PSP and a boundary protection model for physical security.*

Electronic Access Control or Monitoring Systems

Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems

Electronic Access Point ("EAP")

An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets.

Electronic Security Perimeter ("ESP")

~~The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.~~
A collection of Electronic Access Points that protect one or more BES Cyber Systems.

External Connectivity

Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.

External Routable Connectivity

The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.

Interactive Remote Access

Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

Intermediate Device

A Cyber Asset that 1) may be used to provide the required multi-factor authentication for the interactive remote access; 2) may be a termination point for required encrypted communication; and 3) may restrict the interactive remote access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside the Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network.

Physical Access Control Systems

Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers.

Protected Cyber Asset

A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the BES Cyber System. A Transient Cyber Asset is not considered a Protected Cyber Asset.

Reportable BES Cyber Security Incident

Any BES Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service.

Transient Cyber Asset

A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset, 2) used for data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System.

Terms to be retired from the *Glossary of Terms used in NERC Reliability Standards* once the standards that use those terms are replaced:

Critical Assets

Critical Cyber Assets

Physical Security Perimeter

Unofficial Comment Form

Request for Comments Regarding the Draft of CIP Cyber Security Standards Version 5

Please **DO NOT** use this form to submit comments. Please use the electronic comment form to submit comments on the first formal posting of Project 2008-06 – CSO706 Version 5 CIP Standards. The electronic comment form must be completed by **January 6, 2012.**

2008-06 Project Page

If you have questions please contact Steven Noess at steven.noess@nerc.net or 404-446-9691.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standards Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90 days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards-related issues of FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

- Standard CIP-002-5 requires the categorization of these BES Cyber Systems according to bright-line criteria that characterize their impact on the BES Reliability Operating Services they support to ensure the reliable operation of the Bulk Electric System. These BES Reliability Operating Services are based on the Reliability Functions provided by these applicable Responsible Entities' Functional Registration. The "bright-line" criteria contained in Attachment 1 – Impact Categorization of BES Cyber Assets and BES Cyber Systems of the draft CIP-002-5 standard provide the basis of the categorization.
- CIP-003-5 through CIP-009-5, CIP-010-1, and CIP-011-1 in the Version 5 CIP Cyber Security Standards define the cyber security requirements to be applied to the BES Cyber Systems according to the categorization performed in CIP-002-5.
- CIP-003 through CIP-009 generally follow the organization of Versions 1 through 4 of CIP-003 through CIP-009.
- CIP-010-1 is a new standard that contains the Configuration Management and Vulnerability Assessment requirements previously defined across several CIP standards in Versions 1 through 4.
- CIP-011-1 is a new standard that defines Information Protection and Media Sanitization requirements previously defined across many standards in Versions 1 through 4.

The Implementation Plan for Version 5 CIP Cyber Security Standards describes the proposed effective dates for Version 5 CIP Cyber Security Standards.

The Team is seeking industry feedback and suggestions on this Version 5 of the CIP Cyber Security Standards and its Implementation Plan. The industry feedback will be considered by the SDT in revising and refining Version 5 and related documents.

The SDT is providing this form for industry participants to offer their comments on this posted draft of Version 5 of the CIP Cyber Security Standards.

For each question, please indicate whether or not you agree with the modification being proposed. If you disagree with the proposed modification, please explain why you disagree and provide as much detail as possible regarding your disagreement including any suggestions for altering the proposed

modification that would eliminate or minimize your disagreement. The SDT would appreciate responses to as many of these questions as you are willing to supply.

You do not have to answer all questions. Enter all comments in Simple Text Format.

Questions

1. Many definitions in the Definitions document contain modified definitions from existing terms and new definitions for terms used in these standards. Do you have any suggestions that would improve the proposed definitions? If so, please explain and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

2. CIP-002-5 Attachment 1 contains criteria that provide the basis for the categorization of BES Cyber Systems and BES Cyber Assets. Most of these criteria are similar to those already approved by the industry as part of Version 4. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

3. Requirement R1 of draft CIP-002-5 states, "Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems.* All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification." Further, part 1.1 of R1 states "Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

Comments:

4. Requirement R2 of draft CIP-002-5 states, "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

5. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-002-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

   ☐ Yes

   ☐ No

   Comments:

6. CIP-003-5 R1 states "Each Responsible Entity shall identify, by name, a CIP Senior Manager." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

7. CIP-003-5 R2 states "Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

8. CIP-003-5 R3 states "Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and

at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals." Do you agree with the proposed Requirement R3? If not, please explain why and provide specific suggestions for improvement.

☐ Yes

☐ No

Comments:

9. CIP-003-5 R4 states "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function." Do you agree with the proposed Requirement R4? If not, please explain why and provide specific suggestions for improvement.

☐ Yes

☐ No

Comments:

10. CIP-003-5 R5 states "The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated." Do you agree with the proposed Requirement R5? If not, please explain why and provide specific suggestions for improvement.

☐ Yes

☐ No

Comments:

11. CIP-003-5 R6 states "Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

☐ Yes

☐ No

Comments:

12. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-003-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

    ☐ Yes

    ☐ No

    Comments:

13. CIP-004-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

    ☐ Yes

    ☐ No

    Comments:

14. CIP-004-5 R2 states "Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

    ☐ Yes

    ☐ No

    Comments:

15. CIP-004-5 R3 states "Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in *CIP-004-5 Table R3 - Cyber Security Training."* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

    ☐ Yes

    ☐ No

Comments:

16. CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

    ☐ Yes

    ☐ No

    Comments:

17. CIP-004-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in *CIP-004-5 Table R5 – Personnel Risk Assessment."* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

    ☐ Yes

    ☐ No

    Comments:

18. CIP-004-5 R6 states "Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in *CIP-004-5 Table R6 – Access Management Program."* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R6 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

    ☐ Yes

    ☐ No

    Comments:

19. CIP-004-5 R7 states "Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R7 and its parts? If not, please explain why and

provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

20. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-004-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Yes

☐ No

Comments:

21. CIP-005-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

22. CIP-005-5 R2 states "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in *CIP-005-5 Table R2 – Remote Access Management*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

23. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-005-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Yes

☐ No

Comments:

24. CIP-006-5 R1 states "Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan.*" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

    ☐ Yes

    ☐ No

    Comments:

25. CIP-006-5 R2 states "Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program.*" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

    ☐ Yes

    ☐ No

    Comments:

26. CIP-006-5 R3 states "Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in *CIP-006-5 Table R3 – Maintenance and Testing Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

    ☐ Yes

    ☐ No

    Comments:

27. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-006-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

    ☐ Yes

☐ No

Comments:

28. CIP-007-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

29. CIP-007-5 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

30. CIP-007-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R3 – Malicious Code Prevention*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

31. CIP-007-5 R4 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R4 – Security Event Monitoring*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4 and its parts? If not, please explain why and provide

specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

32. CIP-007-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R5 – System Access Controls*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

33. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-007-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Yes

☐ No

Comments:

34. CIP-008-5 R1 states "Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

35. CIP-008-5 R2 states "Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in *CIP-008-5 Table R2 –BES Cyber Security Incident Response Plan Implementation and Testing."* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed

Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

36. CIP-008-5 R3 states "Conduct sufficient reviews, updates and communications to verify the REs response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

37. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-008-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Yes

☐ No

Comments:

38. CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

39. CIP-009-5 R2 states "Each Responsible Entity shall implement one or more processes that collectively address the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing."* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide

specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

40. CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

41. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-009-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Yes

☐ No

Comments:

42. CIP-010-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

43. CIP010-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring."* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide

specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

44. CIP-010-1 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3– Vulnerability Assessments*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

45. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-010-1? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Yes

☐ No

Comments:

46. CIP-011-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-011-5 Table R1 – Information Protection*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

47. CIP-011-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-011-5 Table R2 – Media Reuse and Disposal*." The requirement then proceeds to define the requirement parts in the table. Do you agree with

the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

☐ Yes

☐ No

Comments:

48. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-011-1? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Yes

☐ No

Comments:

49. Do you agree with the proposed implementation plan? If so, please explain and provide specific suggestions for improvement.

☐ Yes

☐ No

Comments:

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Mapping Document Showing Translation of CIP-002-4 to CIP-009-4 into CIP-002-5 to CIP-009-5, CIP-010-1, and CIP-011-1

November 7, 2011

Standard: CIP-002-4 – Cyber Security—Critical Asset Identification		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-002-4 R1.	DELETED	Critical Asset Identification – Removed this requirement because new Standard identifies and categorizes BES Cyber Systems directly without declaring assets as critical.
CIP-002-4 R2.	CIP-002-5 R1	Critical Cyber Asset Identification – New Standard identifies BES Cyber Systems as a grouping of Critical Cyber Assets because it allows entities to apply some requirements at a system rather than asset level. BES Cyber Systems are also identified using BES Reliability Operating Services, which provides more detail on what it means for a Cyber Asset to be critical to reliable operation.
CIP-002-4 R2.	DELETED	Routable protocol exemption – A complete exemption or cyber assets based on communication characteristics no longer applies. This is because the vulnerability some security requirements address is not mitigated by the lack of routable protocols (e.g. training, response, recovery, etc.). Where the lack of routable protocols itself meets the requirement objective, the exemption is applied at the requirement level.
CIP-002-4 R2.	DELETED	Control Center – No longer applicable since R2 has been deleted.
CIP-002-4 R2.	DELETED	Dial-up Accessible – No longer applicable since R2 has been deleted.
CIP-002-4 R3.	CIP-002-5 R2	Annual Approval – No significant changes.
NEW	CIP-002-5 1.1	Update and re-categorize for changes to BES – Specifies timeframe for complying with all categorization and associated security requirements following a planned change.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R1.	CIP-003-5 R2	Cyber Security Policy – Clarified that the cyber security policy needs to only reference the subject matter topics at a high level rather than each individual requirement in the CIP Cyber Security Standards.
CIP-003-4 R1.1.	CIP-003-5 R2, 2.10	Provision for emergency situations – Identified the specific exceptional circumstances in which emergency exceptions can be taken in response to the directive in FERC Order 706 paragraph 443.
CIP-003-4 R1.2.	CIP-003-5 R4	The cyber security policy is readily available – The Responsible Entity only needs to make individuals aware of elements of the cyber security policy related to their job function. This was in response to general confusion around the term "readily available". Examples of how to make individuals aware are listed in the Measures.
CIP-003-4 R1.3.	CIP-003-5 R3	Annual review and approval – No significant change.
CIP-003-4 R2.	CIP-003-5 R1	Single senior manager – Created a definition of CIP Senior Manager to prevent cross referencing across Standards.
CIP-003-4 R2.1.	CIP-003-5 R1	The CIP Senior Manager shall be identified by name, title, and date of designation – The CIP Senior Manager only needs to be identified by name. The other details were considered unnecessary, administrative requirements.
CIP-003-4 R2.2.	CIP-003-5 R6	Changes to the CIP Senior Manager and any delegations must be documented within thirty calendar days of the change.

CIP-003-4 R2.3.	CIP-003-5 R5	Delegate authority – Made clear that the CIP Senior Manager can delegate the ability to delegate. For example, a senior manager can delegate the ability to further delegate responsibility for a plant control system to a plant manager.
CIP-003-4 R2.4.	DELETED	Authorize and document any exception – The FERC Order 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the Standards.
CIP-003-4 R3.	DELETED	Exceptions – The FERC Order 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the Standards.
CIP-003-4 R3.1.	DELETED	Requirement R3 is deleted.
CIP-003-4 R3.2.	DELETED	Requirement R3 is deleted.
CIP-003-4 R3.3.	DELETED	Requirement R3 is deleted.
CIP-003-4 R4.	CIP-011-1 R1, 1.1, 1.2	Information Protection - Removed the explicit requirement for classification as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business. Removed language to “protect” information and replaced with “Implement handling and access control” to clarify the protection that is required.
CIP-003-4 R4.1.	Definition	Identification – Replace this requirement with the defined term BES Cyber System Information.

CIP-003-4 R4.2.	CIP-011-1 1.1	Classification – Removed the explicit requirement for classification as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.
CIP-003-4 R4.3.	CIP-011-1 1.3	Assessment – No significant changes.
CIP-003-4 R5.	CIP-004-5 6.3, CIP-011-1 1.2	Authorize personnel for access to protected information – Clarified the "program for managing access" included the authorization of access as well as handling and access control procedures.
CIP-003-4 R5.1.	DELETED	Authorizing personnel – Personnel are still required to have authorization, and the CIP Senior Manager authorizes or delegates this responsibility. So the additional requirement to have and maintain a list is considered duplicative and unnecessary.
CIP-003-4 R5.1.1.	DELETED	Personnel shall be identified – 5.1 is deleted.
CIP-003-4 R5.1.2.	DELETED	Verification – 5.1 is deleted.
CIP-003-4 R5.2.	CIP-004-5 6.6	Verify access privileges annually – Moved requirement to ensure consistency among access reviews. Clarified precise meaning in the term annual. Clarified what was necessary in performing verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.
CIP-003-4 R5.3.	CIP-011-1 1.3	Annual Review – No significant changes.

CIP-003-4 R6.	CIP-010-1 R1, R2	Change Control and Configuration Management – Moved configuration change management to a separate Standard because of the additional requirements necessary for satisfying FERC directives and the subject matter is currently spread across CIP-003-4 and CIP-007-4. The baseline requirement is incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed. Added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-4 R6.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R1.	CIP-004-5 R1, 1.1	Security awareness program and quarterly reinforcement - Changed to remove the need to ensure everyone with authorized access receive this material and moved example mechanisms to guidance..
CIP-004-4 R2.	CIP-004-5 R2, R3	Training - Addition of identifying the roles that require training. Adding specific role-based training for the visitor control program and storage media as part of the handling of BES Cyber Systems information. Also added the FERC Order 706-directed electronic interconnectivity supporting the operation and control of BES Cyber Systems. This requirement is also reorganized into the respective requirements for "program" and "implementation" of the training.
CIP-004-4 R2.1.	CIP-004-5 3.1	Training prior to authorized access – No significant changes.
CIP-004-4 R2.2.	CIP-004-5 2.1-2.10	Training subject matter – This requirement is reorganized into the respective requirements for "program" and "implementation" of the training.
CIP-004-4 R2.2.1.	CIP-004-5 2.2	Proper use of CCAs – Minor wording changes. Changed to address cyber security issues, not the business or functional use of the BES Cyber System.
CIP-004-4 R2.2.2.	CIP-004-5 2.3,2.4	Physical and electronic access controls training – No significant changes.
CIP-004-4 R2.2.3.	CIP-004-5 2.6	Information handling training – Core training added for the handling of BES Cyber System Information, with the addition of storage media
CIP-004-4 R2.2.4.	CIP-004-5 2.7,2.8,2.9	Incident identification and notification, incident handling and CCA recovery training – Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for individuals having a role in the recovery to address FERC Order 706 paragraph 413.

CIP-004-4 R2.3.	CIP-004-5 3.2	Annual training – Replaced Annually with calendar year, not to exceed 15 months. .
CIP-004-4 R3.	CIP-004-5 R4, R5, 5.1	Personnel Risk Assessment –Split into two requirements, R4 to define the PRA program and R5 to implement the program for individuals prior to obtaining authorized access.
CIP-004-4 R3.1.	CIP-004-5 4.1, 4.2	Identification and 7 year criminal check – Addressed interpretation request in guidance. Specified that identify verification is only required for each individual's initial assessment. Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven year check cannot be performed.
CIP-004-4 R3.2.	CIP-004-5 5.2	Perform the PRA every 7 years.– Removed the "for cause" part of the requirement.
CIP-004-4 R3.3.	CIP-004-5 4.4	Addresses the contractor or vendor performed PRA.
CIP-004-4 R4.	CIP-004-5 6.1, 6.2	Authorize access - CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.
CIP-004-4 R4.1.	CIP-004-5 6.4	Quarterly review of access – Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4 R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.

CIP-004-4 R4.2.	CIP-004-5 R7	Prevent further access - The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours. For transfers, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.
NEW	CIP-004-5 2.1	Added to help facilitate understanding what roles the entity has to support the role based training program.
NEW	CIP-004-5 2.5	Visitor control program training – Personnel administering the visitor control program and/or providing escort should have be part of the core training per FERC Order 706 - paragraph 432.
NEW	CIP-004-5 2.10	Electronic interconnectivity training – Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems per FERC Order 706 - paragraph 434.
NEW	CIP-004-5 4.3	PRA failure criteria – There should be documented criteria or a process used to evaluate personnel risk assessments.

NEW	CIP-004-5 7.2	Transfers – The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.
NEW	CIP-004-5 7.3	Completion of revocation – The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
NEW	CIP-004-5 7.4	Completion of revocation (shared accounts) – To provide clarification of expected actions in managing the passwords

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R1.	CIP-005-5 R1.1	Electronic Security Perimeter identification – Changes include referencing the defined terms Electronic Access Point and BES Cyber System.
CIP-005-4a R1.1.	Definition	Access Points – This was moved to the definition of Electronic Access Points.
CIP-005-4a R1.2.	Guidance	Dial-up accessible CCA – This is a clarifying statement that was moved to guidance.
CIP-005-4a R1.3.	Guidance	Communication links between ESPs – This is a clarifying statement that was moved to guidance.
CIP-005-4a R1.4.	Applicability	Non-Critical Cyber Asset – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.5.	Applicability	Access control and monitoring cyber assets – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.6.	Measures	Maintain Documentation – This is a measure for the requirement to have an ESP.
CIP-005-4a R2.	CIP-005-5 R1	Electronic Access Controls – No significant changes.

CIP-005-4a R2.1.	CIP-005-5 1.2	Deny access by default - Changes include referring to the defined term Electronic Access Point and to focus on the entity knowing and having justification for what it allows through the EAP. The requirement explicitly states the network admission control includes both inbound and outbound connections.
CIP-005-4a R2.2.	CIP-007-5 1.1	Enable specific ports/services – Consolidated port hardening requirements to CIP-007.
CIP-005-4a R2.3.	CIP-005-5 1.3	Secure dial-up – Changed to refer to the defined term Electronic Access Point. Added clarification as to the goal of "secure", which is that the BES Cyber System should not be directly accessible with a phone number only
CIP-005-4a R2.4.	CIP-005-5 R2,2.3	Strong access control – Added a new requirement for remote access in response to increased vulnerabilities in VPN technology. This requirement also clarified strong access control meant two-factor (or more) authentication.
CIP-005-4a R2.5.	Measures	Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.1.	CIP-004-5 R6	The processes for access request and authorization – Consolidated with other similar requirements to CIP-004-5
CIP-005-4a R2.5.2.	Measures	The authentication methods - Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.3.	Measures	The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4. - Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.4.	Measures	The controls used to secure dial-up accessible connections. - Evidence requirements are considered as part of the measure.

CIP-005-4a R2.6.	DELETED	Appropriate Use Banner – The drafting team considered this requirement administrative. The objective of having an appropriate use banner is to prevent accidental use of the system and help allow prosecution of unauthorized individuals accessing the system. The drafting team did not consider either of these rising to the level of meeting a reliability objective.
CIP-005-4a R3.	CIP-007-5 R4, 4.1	Monitoring Electronic Access – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the Standards.
CIP-005-4a R3.1.	CIP-007-5 R4, 4.1	Dial-up Accessible – Removed specific references to dial-up devices. The drafting team did not feel further referencing this technology was necessary.
CIP-005-4a R3.2.	CIP-007-5, R4, 4.2	Alerts – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the Standards.
CIP-005-4a R4.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements.
CIP-005-4a R4.1.	Measures	A document identifying the vulnerability assessment process - Evidence requirements are considered as part of the measure.
CIP-005-4a R4.2.	CIP-010-1 3.1, 3.2	A review to verify that only ports and services required for operations at these access points are enabled - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.

CIP-005-4a R4.3.	CIP-010-1 3.1, 3.2	The discovery of all access points to the Electronic Security Perimeter - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-005-4a R4.4.	CIP-010-1 3.1, 3.2	A review of controls for default accounts, passwords, and network management community strings - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-005-4a R4.5.	CIP-010-1 3.4	Mitigation plan - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. Added element to have an entity defined date of completion of the mitigation plan per FERC Order 706 para 643.
CIP-005-4a R5.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.1.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.2.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.3.	CIP-007-5 4.5	Retain relevant log information – Log retention requirements are consolidated to CIP-007-5 R4

NEW	CIP-005-5 1.6	Inspect & detect potential malicious communications – Per FERC Order 706, paragraph 496-503, ESP's need two distinct security measures such that the cyber assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the drafting team has decided to add the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs.
NEW	CIP-005-5 2.1,2.2	Remote Access: intermediate device and encryption– This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R1.	CIP-006-5 R1	Physical Security Plan – Removed the requirement for Senior Management approval of the physical security plan because there is already approval of the physical security policy and delegation of the task in complying for this program. Additional approval is not considered necessary to meeting the reliability objective of physically security for the BES Cyber System.
CIP-006-4c R1.1.	CIP-006-5 1.2, 1.3	Physical Security Perimeter - Reworded to reflect the change from Physical Security Perimeter to Defined Physical Boundary.
CIP-006-4c R1.2.	DELETED	No longer requires identifing physical access points and controls at them to reflect the change from Physical Security Perimeter to Defined Physical Boundary
CIP-006-4c R1.3.	CIP-006-5 1.4	Monitor physical access – A documented plan is required as part of CIP-006-5 R1 that references the new alerting term in table row 1.4, which replaces the monitoring term. Otherwise, no significant change.
CIP-006-4c R1.4.	CIP-004-5 2.3	Appropriate use of access controls – The term “appropriate’ is subject to a high degree of subjectivity. The training requirement specifies role-based training on physical access controls.
CIP-006-4c R1.5.	CIP-004-5 R6 and R7	Review of access authorization requests and revocation of access authorization requirements were consolidated to CIP-004-5.
CIP-006-4c R1.6.	CIP-006-5 R2	Visitor control program - A documented program is required as part of CIP-006-5 R2. Otherwise, no significant change.

CIP-006-4c R1.6.1.	CIP-006-5 2.2	Log entry and exit of visitors - Addressed multi entry requirements and added the point of contact who can be considered the sponsor for the person to enter the DPB. There is no need to document the escort or handoffs between escorts.
CIP-006-4c R1.6.2.	CIP-006-5 2.1	Continuous escorted access of visitors – No significant change.
CIP-006-4c R1.7.	DELETED	Update of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R1.8.	DELETED	Annual review of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R2.	Applicability	Protection of Physical Access Control Systems – Applicability to Physical Access Control and Monitoring Systems were moved to the applicability section of each security requirement and added this as a defined term in the glossary.
CIP-006-4c R2.1.	Applicability	Physical Access Control Systems be protected from unauthorized physical access - Applicability to Physical Access Control Systems were moved to the applicability section of each security requirement. For this particular requirement see CIP-006-5 item 1.1
CIP-006-4c R2.2.	Applicability	Protection of Physical Access Control Systems - Applicability to Physical Access Control Systems were moved to the applicability section of each security requirement.
CIP-006-4c R3.	Applicability	Protection of Electronic Access Control Systems - Applicability to what protections Electronic Access Control and Monitoring Systems need were moved to the applicability section of each security requirement.

CIP-006-4c R4.	CIP-006-5 1.2, 1.3	Physical Access Controls - Reworded to reflect the change from Physical Security Perimeter to Defined Physical Boundary. Also addressed FERC Order 706 defense in depth. Examples of methods to implement have been moved to the guidance section of this requirement.
CIP-006-4c R5.	CIP-006-5 1.4, 1.5, 1.6	Monitor physical access – Changed the term to alert for unauthorized access and clarified the actions taken for review of unauthorized physical access alerts. Examples of methods to implement have been moved to the guidance section of this requirement.
CIP-006-4c R6.	CIP-006-5 1.7	Log physical access – CIP-006-4 R6 was specific to the logging of access at identified access points. This now more generally requires logging of physical access into the Defined Physical Boundary. Examples of methods to implement have been moved to the guidance section of this requirement.
CIP-006-4c R7.	CIP-008-5 Evidence Retention	Retain relevant incident related log information is addressed in CIP-008-5
CIP-006-4c R8.	CIP-006-5 R3	Maintenance and Testing
CIP-006-4c R8.1.	CIP-006-5 3.1	Physical access control system 3 yr. testing and maintenance – Shortened periodicity of testing to 2 years to address FERC Order 706 paragraph 581 directives. Added testing of locally mounted security hardware devices.
CIP-006-4c R8.2.	REMOVED	Testing and maintenance records are considered the measurement of item 3.1.
CIP-006-4c R8.3.	CIP-006-5 3.2	Retain outage records – No significant changes.
NEW	CIP-006-5 1.1	Entity based Operational or procedural controls to restrict physical access – To allow for programmatic protection controls as a baseline for Low Impact BES Cyber Assets and Physical Access Control Systems. This does not require detailed lists of individuals with access.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R1.	CIP-010-1 1.4	Assess security controls following changes - Provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order ,paragraphs 397, 609, 610, and 611
CIP-007-4 R1.1.	CIP-010-1 1.4	Test procedures – See description and justification for CIP-007-4 R1.
CIP-007-4 R1.2.	CIP-010-1 1.4	Testing reflects production environment - See description and justification for CIP-007-4 R1.
CIP-007-4 R1.3.	CIP-010-1 1.4	The Responsible Entity shall document test results. - See description and justification for CIP-007-4 R1.
CIP-007-4 R2.	CIP-007-5 R1	Ports and Services – The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.
CIP-007-4 R2.1.	CIP-007-5 1.1	Enable only those ports and services required for normal and emergency operations – See description and justification for CIP-007-4 R2.
CIP-007-4 R2.2.	CIP-007-5 1.1, 1.2	Disable other ports/services – See description and justification for CIP-007-4 R2.
CIP-007-4 R2.3.	DELETED	Compensating measures – See description and justification for CIP-007-4 R2.

CIP-007-4 R3.	CIP-007-5 R2	Security Patch Management – The existing wording or CIP-007-4 R3, R3.1, and R3.2 was separated into individual line items to provide more granularity. The documentation of a source (s) to monitor for release of security related patches, hotfixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" there has been confusion as to what constitutes the availability. Due to issues that may occur regarding Control System vendor license and service agreements flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.
CIP-007-4 R3.1.	CIP-007-5 2.2	Assess patches – Similar to the current wording but added "from the identified source" to establish where the release is from. The current wording: "The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" has led to varying opinions as to what constitutes "availability" of the patches or upgrades. The addition attempts to clarify where the release is from.
CIP-007-4 R3.2.	CIP-007-5 2.3	Implement patches - This is the same concept as in the current CIP-007 R3.2 wording however a 30 day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used. Splitting the implementation of security related patches, hotfixes, and/or updates into a separate item from compensating measures will provide granularity. Automated processes allow the implementation to be documented and confirmed electronically in a short time period. Manual processes may take an extended period of time to complete documentation of the installation. Priority should be given to the implementation rather than the documentation.

CIP-007-4 R4.	CIP-007-5 R3, 3.1, 3.2, 3.3, 3.4, 3.5	Malicious Software Prevention – In prior versions, this requirement has arguably been the single greatest generator of TFE's as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of cyber assets in scope of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. Beginning in paragraph 619-622 of FERC Order 706, and in particular 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…" In paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.
CIP-007-4 R4.1.	CIP-007-5 R3, 3.1, 3.2, 3.3	Malware prevention tools – See description and justification for CIP-007-4 R4.
CIP-007-4 R4.2.	CIP-007-5 3.4	Update malicious code detections – See description and justification for CIP-007-4 R4.

CIP-007-4 R5.	CIP-007-5 5.1	Use at least one authentication method – The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.
CIP-007-4 R5.1.	CIP-004-5 6.1	Access authorization – CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.
CIP-007-4 R5.1.1.	CIP-003-5 R5	Access authorization – CIP-003-5 R5 requires CIP Senior Manager or delegate approval for all requirements for authorization in the CIP Cyber Security Standards.
CIP-007-4 R5.1.2.	CIP-007-5 4.1	Identify security events for after-the-fact investigation – This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP as required in CIP-005-4 R3 and user access and activity logs as required in CIP-007-5 R5 are also included here.

CIP-007-4 R5.1.3.	CIP-004-5 6.5	Annual account privilege verification – Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.
CIP-007-4 R5.2.	CIP-007-5 5.2	Identify account types and determine acceptable use – CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.
CIP-007-4 R5.2.1.	CIP-007-5 5.4	Change default vendor passwords – The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.
CIP-007-4 R5.2.2.	CIP-007-5 5.2	Identify account types and determine acceptable use
CIP-007-4 R5.2.3.	CIP-007-5 5.3	Identify account types and determine acceptable use – No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.

CIP-007-4 R5.3.	CIP-007-5 5.5	Implement a password policy – CIP-007-4 R5.3 requires the use of passwords and specifies a specific policy of 6 characters or more with a combination of alpha-numeric and special characters . The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.
CIP-007-4 R5.3.1.	CIP-007-5 5.5	Password length – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.2.	CIP-007-5 5.5	Password complexity – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.3.	CIP-007-5 5.5	Password change frequency – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R6.	CIP-007-5 R4	Security Status Monitoring – Consolidated requirements for monitoring electronic events into CIP-007-5 R4.
CIP-007-4 R6.1.	CIP-007-5 4.1	Identify security events – This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term “system events related to cyber security” from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP as required in CIP-005-4 R3 and user access and activity logs as required in CIP-007-5 R5 are also included here.

CIP-007-4 R6.2.	CIP-007-5 4.2	Identify security events for real-time alerting – This requirement is derived from alerting requirements in CIP-005-4 R3.2 and CIP-007-4 R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.
CIP-007-4 R6.3.	CIP-007-5 4.1	Identify security events for after-the-fact investigation – See description and justification for CIP-007-4 R6.1.
CIP-007-4 R6.4.	CIP-007-5 4.4	Retain relevant log information – No significant changes.
CIP-007-4 R6.5.	CIP-007-5 4.3	Review logs – Beginning in paragraph 525 and also 628 of the FERC Order 706, the commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.
CIP-007-4 R7.	CIP-011-1 2.1	Erase media no longer needed to store protected information – Consistent with FERC Order 706, paragraph 631, clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word “erase” as, depending on the media itself, erasure may not be sufficient to meet this goal. Removed requirement explicitly requiring records of destruction/redeployment because this was implied as a measure of compliance.
CIP-007-4 R7.1.	CIP-011-1 2.2	Disposal – See description and justification for CIP-007-4 R7.
CIP-007-4 R7.2.	CIP-011-1 2.1	Redeployment – See description and justification for CIP-007-4 R7.

CIP-007-4 R7.3.	Measures	See description and justification for CIP-007-4 R7.
CIP-007-4 R8.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated requirements for vulnerability assessments from CIP-005-4 and CIP-007-4.
CIP-007-4 R8.1.	Measures	A document identifying the vulnerability assessment process – This is example evidence required for compliance.
CIP-007-4 R8.2.	CIP-010-1 3.1, 3.2	Ports and services review – As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-007-4 R8.3.	CIP-010-1 3.1, 3.2	A review of controls for default accounts – As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.
CIP-007-4 R8.4.	CIP-010-1 3.4	Mitigation plan – Added a requirement for an entity planned date of completion as per the FERC directive in Order 706, paragraph 643.
CIP-007-4 R9.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
NEW	CIP-007-5 1.2	Restrict physical I/O ports – In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

NEW	CIP-007-5 2.1	Identify patch sources – Defining the source(s) that a Responsible Entity monitors for the release of security related patches, hotfixes, and/or updates will provide a starting point for assessing the effectiveness of the patch management program. Documenting the source is also used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.
NEW	CIP-007-5 4.3	Generate real-time alerts and respond to audit-processing failures – This requirement was derived from NIST 800-53 version 3 AU-5, which addresses response to audit processing failures. Some interpretations of version 4 CIP Cyber Security Standards considered the failure of the security event monitoring and alerting system to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.
NEW	CIP-007-5 5.6	Limits or alerts on exceeding unsuccessful log in attempts threshold – Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.

NEW	CIP-007-5 R6	Limit malicious code on maintenance devices – This is a new requirement to address the FERC Order 706 paragraph 621 directive to protect against personnel introducing malicious code into the BES Cyber System. This requirement also clarifies that these devices may be temporarily connected to the BES Cyber System, but do not become a part of the BES Cyber System, nor are they considered Protective (Protected??) Cyber Assets. These devices may be temporarily connected locally to the BES Cyber System for maintenance, but must be protected from introducing malicious code or creating an additional electronic access point.

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-008-4 R1.	CIP-008-5 R1	Cyber Security Incident Response Plan – Separated requirement into multiple requirements in a comparable manner as CIP-009-4 where individual aspects of maintaining the plan are listed as separate requirements. The requirement to have an Incident Response Plan now applies to all Responsible Entities as a foundational element of a cyber security program for BES Cyber Systems.
CIP-008-4 R1.1.	CIP-008-5 1.1	Identify reportable cyber security events – Defined the term Reportable Cyber Security Incident and further described the meaning in relation to CIP-008-5.
CIP-008-4 R1.2.	CIP-008-5 1.2	Roles and responsibilities of incident response teams – No significant changes.
CIP-008-4 R1.3.	DELETED	Reporting cyber security incidents – Coordinating with EOP-004-2 drafting team to ensure EOP-004-2 becomes the single Standard for reporting incidents, and ensure EOP-004-2 references the defined term Reportable Cyber Security Incidents.
CIP-008-4 R1.4.	CIP-008-5 3.3	Update incident response plan following review – Included additional specification on update of response plan Addresses FERC Order 706 Paragraph 686 directive to modify on lessons learned and aspects of the DHS Controls.
CIP-008-4 R1.5.	CIP-008-5 3.1	Review incident response plans annually – No significant changes.
CIP-008-4 R1.6.	CIP-008-5 2.1	Test incident response plans annually – No significant changes.
CIP-008-4 R2.	DELETED	Cyber Security Incident Documentation – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.

NEW	CIP-008-5 3.5	Communicate incident response plan updates – Added specific timing requirement on communication of plan changes based on review of the DHS Controls and NIST 800-53 guideline.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-4 R1.	CIP-009-5 3.1	Recovery Plan – Added the requirements to additionally review plans after system replacement. Also added requirement for documentation of any identified deficiencies or lessons learned.
CIP-009-4 R1.1.	CIP-009-5 1.1	Conditions for activation of recovery plan – Reworded to address FERC Order 706 paragraph 694 directive and simplified the requirement.
CIP-009-4 R1.2.	CIP-009-5 1.2	Roles and responsibilities of recovery plan responders – No significant changes.
CIP-009-4 R2.	CIP-009-5 2.1	Test recovery plan annually – No significant changes.
CIP-009-4 R3.	CIP-009-5 3.2	Review results of recovery plan activities (tests, events) – Added the timeframe for update.
CIP-009-4 R4.	CIP-009-5 1.3	Backup processes – No significant changes.
CIP-009-4 R5.	CIP-009-5 2.2	Test information used for recovery – Combined Requirement from CIP-009-4 R5 and included requirement to test when initially stored. Addresses FERC Order 706 directives 739 and 748 related to testing of backups.
NEW	CIP-009-5 1.4	Testing of backup media – Addresses FERC Order 706 paragraph 739 and 748 directives regarding the testing of backup media.
NEW	CIP-009-5 1.6	Process to preserve data for analysis – Added requirement to address FERC Order 706, paragraph 706 regarding the necessity to have procedures in place to retain cyber asset evidence as part of the recovery planning.

NEW	CIP-009-5 3.5	Communicate recovery plan updates – This change ensures that recovery personnel are aware of any changes to recovery plans.

Standard: New Requirements in CIP-010-1 and CIP-011-1		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-1 1.1	Baseline configuration – Baseline requirement incorporated from the DHS Catalog for Control Systems Security (also NIST 800-53). The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed.
NEW	CIP-010-1 2.1	Monitor for changes to the baseline configuration – Monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes. This change addresses FERC Order 706, paragraph 397 directive and is based on a review of DHS Catalog of Security Controls (or NIST 800-53).
NEW	CIP-010-1 3.2	Live Vulnerability Assessment – Addresses FERC Order 706 paragraph 541, 542, 544 and 547 directives regarding the performance of a live vulnerability assessment in a test environment.
NEW	CIP-010-1 3.3	Perform active VA on new BES Cyber Assets - Addresses FERC Order 706 paragraph 541, 542, 544 and 547 directives regarding the performance of a vulnerability assessment prior to placing a new Cyber Asset into production.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-4

3. Purpose: NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its records of approvals as specified in Requirement R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 The Regional Entity shall serve as the Compliance Enforcement Authority with the following exceptions:

- For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.2. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change “Control Center” to “control center”	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-4

3. Purpose: Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-003-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-4 Requirement R2.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance	

		Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-4

3. Purpose: Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-004-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-004-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);

- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program. Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-4a

3. Purpose: Standard CIP-005-4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4a should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-005-4a, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-4a:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4a.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.1 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.1 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.2 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-4a from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Developed separately.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2	Approved by NERC Board of	Modifications to clarify the requirements and to bring the compliance elements into	Revised.

	Trustees 5/6/09	conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Changed CIP-005-2 to CIP-005-3. Changed all references to CIP Version "2" standards to CIP Version "3" standards. For Violation Severity Levels, changed, "To be developed later" to "Developed separately."	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010	Addition
4a	01/24/11	Adopted by the NERC Board of Trustees	Update to conform to changes to CIP-002-4 (Project 2008-06) Update version number from "3" to "4a"

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-4c

3. Purpose: Standard CIP-006-4 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-4c should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-006-4c, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-006-4c:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the

Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-4c for that single access point at the dial-up device.

2. **Violation Severity Levels (Under development by the CIP VSL Drafting Team)**

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	May 2, 2006	Adopted by NERC Board of Trustees	
1	January 18, 2008	FERC Order issued approving CIP-006-1	
	February 12, 2008	Interpretation of R1 and Additional Compliance Information Section 1.4.4 adopted by NERC Board of Trustees	Project 2007-27
2		Updated version number from -1 to -2 Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	Project 2008-06
2	May 6, 2009	Adopted by NERC Board of Trustees	
	August 5, 2009	Interpretation of R4 adopted by NERC Board of Trustees	Project 2008-15
2	September 30, 2009	FERC Order issued approving CIP-006-2	
3	November 18, 2009	Updated version number from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term “Responsible Entity” was capitalized. Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	Project 2009-21
3	December 16, 2009	Adopted by NERC Board of Trustees	
	February 16, 2010	Interpretation of R1 and R1.1 adopted by NERC Board of Trustees	Project 2009-13
3	March 31, 2010	FERC Order issued approving CIP-006-3	
2a/3a	July 15, 2010	FERC Order issued approving the Interpretation of R1 and R1.1. Updated version numbers from -2/-3 to -2a/-3a.	
4	January 24,	Adopted by NERC Board of Trustees	

	2011		
3c/4c	May 19, 2011	FERC Order issued approving two interpretations: 1) Interpretation of R1 and Additional Compliance Information Section 1.4.4; and 2) Interpretation of R4. Updated version number from -3/-4 to -3c/-4c.	

Appendix 1

Requirement Number and Text of Requirement
R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following: R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
Question
If a completely enclosed border cannot be created, what does the phrase, "to control physical access" require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption? Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?
Response
For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are "physical in nature." The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

Appendix 2

Interpretation of Requirement R1.1.

Request: *Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*

Interpretation:

Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border.

CIP-006-1 — Requirement 1.1 requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

CIP-006-1 — Additional Compliance Information 1.4.4 identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.

1.4. Additional Compliance Information

1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.

Appendix 3

The following interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R4 was developed by the standard drafting team assigned to Project 2008-14 (Cyber Security Violation Severity Levels) on October 23, 2008.

Request:

1. *For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*
2. *Does the term, "time of access" mean logging when the person entered the facility or does it mean logging the entry/exit time and "length" of time the person had access to the critical asset?*

Interpretation:

No, monitoring and logging of access are only required for ingress at this time. The term "time of access" refers to the time an authorized individual enters the physical security perimeter.

Requirement Number and Text of Requirement

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-4

3. Purpose: Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-007-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-4 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	

		Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-4

3. Purpose: Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-008-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-4 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated Version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-4

3. Purpose: Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-009-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-009-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

Consideration of Comments

Project 2008-06 Cyber Security Order 706
Draft CIP-002-4 Informal Review

The Cyber Security Order 706 Standard Drafting Team thanks all commenters who submitted comments on the proposed CIP-002-4 changes. These standards were posted for a 30-day informal comment period from May 4, 2010 through June 3, 2010. The stakeholders were asked to provide feedback on the standards through a special Electronic Comment Form. There were 119 sets of comments. The complete record of comments submitted is posted on the Project 2008-06 Version 4 CIP Standards page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President of Standards, Herb Schrayshuen at (404) 446-2560 or at Herb.Schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

1. Do you agree with the adoption of the following new or revised terms and their definitions for inclusion in the NERC Glossary: BES Cyber System Component, BES Cyber System, and Control Center? If not, please explain and supply your proposed modification..... 16

1.a. BES Cyber System Component — One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation. 16

1.b. BES Cyber System — One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES. 48

1.c. Control Center — A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:..... 74

2. The definition of BES Cyber System limits the scope of the definition and the applicability of CIP-010-1 (and CIP-011-1) to real-time operations systems with an operational time horizon of 15 minutes. Do you agree with this scope of applicability? If not, please explain why and provide specific suggestions for improvement. 95

3. Requirement R1 of draft CIP-010-1 states, "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions defined in CIP-010 – 1 Attachment I – Functions Essential to the Reliable Operation of the BES to identify BES Cyber Systems for the application of security requirements." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement. 109

4. Requirement R2 of draft CIP-010-1 states, "Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II – Impact Categorization of BES Cyber Systems to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement..... 130

5. Requirement R3 of draft CIP-010-1 states, "To ensure the application of adequate requirements on its BES Cyber Systems, each Responsible Entity shall: 146

6. CIP-010-1 Attachment I contains a listing and brief description of Functions Essential to Reliable Operation of the Bulk Electric System. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement. 163

7. CIP-010-1 Attachment II contains criteria for categorization of BES Cyber Systems for High, Medium and Low impact categories. The criteria were originally developed in collaboration with representatives of the Operating and Planning Committees, some of whom continued to provide input during the drafting of Attachment II. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement. 184

8. Do you have any other comments to improve this version of draft standard CIP-010-1? If so, please explain and provide specific suggestions for improvement. 239

9. Do you prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements? Do you prefer the alternate format, where the requirements are grouped in separate standards? Or do you have no preference? 267

10. The Purpose of draft CIP-011-1 states, "To ensure Functional Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems for which they are responsible and that execute or enable functions essential to reliable operation of the interconnected BES." Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement. 284

11. Requirement R1 of draft CIP-011-1 states, "Each Responsible Entity shall develop, implement, and annually review formal, documented cyber security policies that address the following for its BES Cyber Systems:" and then provides a list of topics that must be addressed. Do you agree with this proposal and list? If not, please explain why and provide specific suggestions for improvement 296

12. Requirements R2 to R4 of draft CIP-011-1 concern personnel training, awareness, and risk assessment, which were previously contained in CIP-004. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement. 311

13. Do you agree with the proposed definitions for external connectivity, routable protocol, and non-routable protocol? Please explain and provide any suggestions for modification... 352

14. Tables R3 and R4 provide direction concerning what impact level of BES Cyber Systems to which Requirements R3 and R4 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 366

15. Requirements R5 and R6 of draft CIP-011-1 concern procedures for physical security, which were previously contained in CIP-006. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement. 378

16. Tables R5 and R6 provide direction concerning what impact level of BES Cyber Systems to which Requirements R5 and R6 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 400

17. Requirement R7 of draft CIP-011-1 states "Each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in CIP-011-1 Table R7 – Account Management Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of electronic access control requirements that are included in Requirements table R7? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please Explain and provide any suggestions for modification. 421

18. Table R7 provides direction concerning what impact level of BES Cyber Systems to which Requirement R7 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 433

19. At the present time, the Access Control requirements for Physical Access have not been combined with the Access Control requirements related to Electronic Access. Do you agree with this method? Or would you prefer to have the Physical Access control requirements combined with the Electronic Access control requirements? Please explain and provide any suggestions for modification. 439

20. Requirement R8 of draft CIP-011-1 states "Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R8 – Account Management Implementation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R8? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each criteria as represented in the table? Please explain and provide any suggestions for modification. 445

21. Table R8 provides direction concerning what impact level of BES Cyber Systems to which Requirement R8 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 455

22. FERC has mandated immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset. Requirement R9 of draft CIP-011-1 states "Each Responsible Entity shall revoke system access to its BES Cyber Systems as specified in CIP-011-1 Table R9 – Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R9? Please explain and provide any suggestions for modification, including time proposals. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. 463

23. Table R9 provides direction concerning what impact level of BES Cyber Systems to which Requirement R9 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 483

24. Requirement R10 of draft CIP-011-1 states "Each Responsible Entity shall implement the account management access control actions specified in CIP-011-1 Table R10 – Account Access Control Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R10? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. 495

25. Table R10 provides direction concerning what impact level of BES Cyber Systems to which Requirement R10 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 519

26. Requirement R11 of draft CIP-011-1 states "Each Responsible Entity that allows remote or wireless electronic access to any of its BES Cyber Systems shall apply the criteria specified in CIP-011-1 Table R11– Wireless and Remote Electronic Access Documentation to ensure that no unauthorized access is allowed to its BES Cyber Systems. Do you agree with the list of criteria that are included in Requirements Table R11? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. 530

27. Do you agree with the definition of remote access as proposed for this standard? Please explain and provide any suggestions for modification. 542

28. Table R11 provides direction concerning what impact level of BES Cyber Systems to which Requirement R11 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 552

29. Requirement R12 of draft CIP-011-1 states "Each Responsible Entity that allows wireless and remote electronic access to any of its BES Cyber Systems shall manage that electronic access in accordance with the criteria specified in CIP-011-1 Table R12 – Wireless and Remote Electronic Access Management to ensure that no unauthorized access is allowed to its BES Cyber System." Do you agree with the list of criteria that is included in Requirements Table R12? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each item as represented in the table? Please explain and provide any suggestions for modification. 559

30. Table R12 provides direction concerning what impact level of BES Cyber Systems to which Requirement R12 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 567

31. Requirement R13 of draft CIP-011-1 states "Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 – Remote Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that is included in Requirements Table R13? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification..... 573

32. Table R13 provides direction concerning what impact level of BES Cyber Systems to which Requirement R13 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 586

33. Requirement R14 of draft CIP-011-1 states "Each Responsible Entity shall document and implement its organizational processes, technical mechanisms, and procedures for control of wireless and remote access to electronic access points to its BES Cyber Systems including wireless and remote access if it is used, that incorporate the criteria specified in CIP-011-1 Table R14 – Wireless and Remote Electronic Access Controls to ensure that no unauthorized access is allowed to its BES Cyber Systems." Do you agree with the list of criteria that is included in Requirements Table R14? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. 599

34. Table R14 provides direction concerning what impact level of BES Cyber Systems to which Requirement R14 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 610

35. Requirements R15 to R19 of draft CIP-011-1 concern procedures for system security protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R15 to R19? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification..... 615

36. Tables R15 to R19 provide direction concerning what impact level of BES Cyber Systems to which Requirements R15 to R16 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?..... 664

37. Requirements R20 to R22 of draft CIP-011-1 concern procedures for boundary protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R20 to R22? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification..... 678

38. Do you agree with the proposed definition of electronic access point? Please explain and provide any suggestions for modification. 706

39. Tables R20 to R22 provide direction concerning what impact level of BES Cyber Systems to which Requirements R20 to R22 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 717

40. The configuration change management requirement is centered on the identification of a component inventory and baseline configuration. Do you agree with the list of criteria that are included in the baseline configuration? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the baseline and managed through the configuration change management process? Do you agree with the list of criteria that are included in Requirements Table R23? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in Table R23? Please explain and provide any suggestions for modification. 726

41. Table R23 provide direction concerning what impact level of BES Cyber Systems to which Requirement R23 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 745

42. The definition of sensitive information was derived from the previous version of the CIP standards to minimize disruption to entity information protection programs that are already in place. Do you agree with the proposed definition? Please explain and provide any suggestions for modification. 752

43. Do you agree with the proposed definition of Media? Please explain and provide any suggestions for modification. 765

44. Requirements R24 and R25 of draft CIP-011-1 concern procedures for information protection and media sanitization. Do you agree with the list of criteria that are included in each Requirements Table for R24 and R25? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification. 770

45. Tables R24 and R25 provide direction concerning what impact level of BES Cyber Systems to which Requirements R24 and R25 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 784

46. The BES Cyber System Maintenance requirement is intended to cover the instances where it is necessary to directly connect a device to the BES Cyber System temporarily to perform a support function, provide appropriate controls on the maintenance device to protect the BES Cyber System. Do you agree with the definition of maintenance as provided? 788

47. Requirement R26 of draft CIP-011-1 concerns procedures for BES Cyber System maintenance. Do you agree with the list of criteria that are included in Requirements Table R26? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. 794

48. Table R26 provides direction concerning what impact level of BES Cyber Systems to which Requirement R26 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 803

49. Requirements R27 to R29 of draft CIP-011-1 concern procedures for Cyber Security Incident response. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R27 to R29? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification. 807

50. Tables R27 to R29 provide direction concerning what impact level of BES Cyber Systems to which Requirements R27 to R29 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 817

51. Requirements R30 to R32 of draft CIP-011-1 concern procedures for BES Cyber System Recovery. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R30 to R32? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification. 824

52. Tables R30 to R32 provide direction concerning what impact level of BES Cyber Systems to which Requirements R30 to R32 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest? 840

53. Which requirements in draft CIP-011-1 should allow for TFE submissions? Note that not all requirements will be considered as being applicable for TFE submissions. The drafting team has attempted to minimize the need for TFEs by modifying the language to allow for flexibility in meeting the requirements. Please provide suggestions on how the language of the standard may be modified to eliminate the need for TFEs. If TFEs are still needed, please provide specific examples to justify the inclusion of a requirement as being TFE eligible. 846

54. Do you have any other comments to improve this version of draft standard CIP-011-1? 860

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Larry Bugh	ReliabilityFirst Staff										
2.	Group	Ruth Blevins	Dominion Resources Services, Inc.										
3.	Group	Guy Zito	Northeast Power Coordinating Council										
4.	Group	Kenneth D. Brown	Public Service Enterprise Group companies										
5.	Group	Sasa Maljukan	Hydro One										
6.	Group	David Grubbs	Garland Power and Light										
7.	Group	Roger Powers	CWLP Electric Transmission, Distribution and Operations Department										
8.	Group	Guy Andrews	GTC & GSOC										
9.	Group	Tommy Drea - CIP Compliance	Dairyland Power Cooperative										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
10.	Group	Joseph DePoorter	Madison Gas and Electric Company										
11.	Group	Carol Gerou	MRO's NERC Standards Review Subcommittee										
12.	Group	Denise Koehn	Bonneville Power Administration										
13.	Group	Steve Alexanderson	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group										
14.	Group	Richard Kafka	Pepco Holdings, Inc. - Affiliates										
15.	Group	Mark Stefaniak	Detroit Edison										
16.	Group	Frank Gaffney	Florida Municipal Power Agency										
17.	Group	Nathan Mitchell	APPA Task Force										
18.	Group	Sheryl Byrd	GE Energy										
19.	Group	Ben Li	IRC Standards Review Committee										
20.	Group	John Van Boxtel	WECC										
21.	Individual	Brent Ingebrigtson	E.ON U.S.										
22.	Individual	Ronald J Slack	Exelon Corporation										
23.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)										
24.	Individual	John Lawrence	Reliability & Compliance Group										
25.	Individual	Rick Terrill	Luminant										
26.	Individual	Linda Jacobson	FEUS										
27.	Individual	Robert Ulmer	American Transmission Company										
28.	Individual	John Brockhan	CenterPoint Energy										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
29.	Individual	Susan Kurtain	Regulatory Compliance										
30.	Individual	Paul Reymann, CEO	ReymannGroup, Inc.										
31.	Individual	Silvia Parada Mitchell	NextEra Energy Corporate Compliance										
32.	Individual	Boyd Nation	Southern Company										
33.	Individual	Tracey Stewart	Southwestern Power Administration										
34.	Individual	Donald Brookhyser	Cogeneration Association of California and Energy Producers & Users Coalition										
35.	Individual	David Batz	EEI										
36.	Individual	Tom Bradish	RRI Energy										
37.	Individual	Dora Moreno	Southern California Edison Company										
38.	Individual	Sandra Shaffer	PacifiCorp										
39.	Individual	Jana Van Ness	Arizona Public Service Company										
40.	Individual	Casey Hashimoto	Turlock Irrigation District										
41.	Individual	Ken Stratton	US Army Corps of Engineers, Omaha District										
42.	Individual	Michael Gammon	Kansas City Power & Light										
43.	Individual	John Alberts	Wolverine Power										
44.	Individual	Mike Hendrix	Idaho Power Company										
45.	Individual	Tony Dodge	BCTC										
46.	Individual	Greg Froehling	Green Country Energy										
47.	Individual	Roger Fradenburgh	Network & Security Technologies Inc										
48.	Individual	John Alberts	Wolverine Power										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
49.	Individual	John Kutzer	Consultant										
50.	Individual	Melissa Kurtz	USACE - Omaha Anchor										
51.	Individual	James Stanton	SPS Consulting Group Inc.										
52.	Individual	Michael Puscas	Northeast Utilities System										
53.	Individual	Roger Pan	Emerson Process Management										
54.	Individual	Jo Ann Newton	PNM Resources, Inc.										
55.	Individual	John Hughes	Electricity Consumers Resource Council (ELCON)										
56.	Individual	Ted Risher	Ingleside Cogeneration, LP										
57.	Individual	Thad Ness	American Electric Power										
58.	Individual	Ed Goff	Progress Energy (non-Nuclear)										
59.	Individual	Mark Thompson	Alberta Electric System Operator										
60.	Individual	Dan Roethemeyer	Dynegy Inc.										
61.	Individual	CJ Ingersoll	Constellation Energy Control and Dispatch, LLC										
62.	Individual	Daniel Duff	Liberty Electric Power, LLC										
63.	Individual	Jonathan Appelbaum	The United Illuminating Co										
64.	Individual	Greg Hataway	Powersouth Energy Cooperative										
65.	Individual	Kasia Mihalchuk	Manitoba Hydro										
66.	Individual	Steven Belle	SCE&G										
67.	Individual	William Gross	Nuclear Energy Institute										
68.	Individual	Randy Schimka	San Diego Gas and Electric Co.										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
69.	Individual	Brandy A. Dunn	Western Area Power Administration										
70.	Individual	Eric Scott	Ameren										
71.	Individual	Jim Simpson	Allegheny Energy Supply										
72.	Individual	Neal Williams	Poplar Bluff Municipal Utilities										
73.	Individual	E Hahn	MWDSC										
74.	Individual	Ed Nagy	LCEC										
75.	Individual	Paul Crosby	Platte River Power Authority										
76.	Individual	Showin Fu	US Army Corps of Engineers										
77.	Individual	SPP RE Staff	Southwest Power Pool Regional Entity										
78.	Individual	William F. Watson	Old Dominion Electric Cooperative										
79.	Individual	Michael R. Lombardi	Northeast Utilities										
80.	Individual	Shawn Barrett	Michigan Public Power Agency										
81.	Individual	Fred Meyer	The Empire District Electric Company										
82.	Individual	Darryl Curtis	Oncor Electric Delivery LLC										
83.	Individual	Andres Lopez	USACE HQ										
84.	Individual	Peter Yost	Con Edison of New York										
85.	Individual	Bill Keagle	BGE										
86.	Individual	Michael Albosta	SRW Cogeneration Limited Partnership										
87.	Individual	Martin Bauer	US Bureau of Reclamation										
88.	Individual	Bob Mathews	Pacific Gas & Electric Company										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
89.	Individual	Barbara Kedrowski	We Energies										
90.	Individual	Saurabh Saksena	National Grid										
91.	Individual	Sungly Chiu	LADWP										
92.	Individual	Kenneth A. Goldsmith	Alliant Energy										
93.	Individual	Amir Y. Hammad	Constellation Power Source Generation										
94.	Individual	Kevin Cyr	Seattle City Light										
95.	Individual	Steve Newman	MidAmerican Energy Company										
96.	Individual	Bob Case	Black Hills Corporation										
97.	Individual	Jason Marshall	Midwest ISO										
98.	Individual	Steve Toth	Covanta Energy										
99.	Individual	Jon Kapitz	Xcel Energy										
100.	Individual	William J. Smith	Allegheny Power										
101.	Individual	Donovan Tindill	Matrikon Inc.										
102.	Individual	Patrick Stava	Nebraska Public Power District										
103.	Individual	Greg Rowland	Duke Energy										
104.	Individual	Kathleen Goodman	ISO New England Inc										
105.	Individual	David Martorana	Tenaska										
106.	Individual	Doug Hohlbaugh	FirstEnergy Corporation										
107.	Individual	John Falsey	Edison Mission Marketing and Trading										
108.	Individual	Stephen C. Knapp	Constellation Energy Commodities Group Inc.										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
109.	Individual	Eric Ruskamp	Lincoln Electric System										
110.	Individual	Randi Woodward	Minnesota Power										
111.	Individual	Kevin Koloini	American Municipal Power										
112.	Individual	Dave Norton	Entergy										
113.	Individual	Christine Hasha	ERCOT ISO										
114.	Individual	John Allen	City Utilities of Springfield, Missouri										
115.	Individual	Rex A Roehl	Indeck Energy Services, Inc										
116.	Individual	Cynthia Broadwell	Progress Energy - Nuclear Generation										
117.	Individual	Dan Rochester	Independent Electricity System Operator										
118.	Individual	Catherine Koch	Puget Sound Energy										
119.	Individual	Ernie Hayden	Verizon Business										

1. **Do you agree with the adoption of the following new or revised terms and their definitions for inclusion in the NERC Glossary: BES Cyber System Component, BES Cyber System, and Control Center? If not, please explain and supply your proposed modification.**

   1.a. **BES Cyber System Component — One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation.**

Summary Consideration:

Many commenters expressed concerns about the inclusion of software and data within the definition of BES Cyber System Component. One commenter observed that the definition should only include devices with routable connectivity. Many observed the laundry list of functions should be removed and replaced with the function that is more specific to the operation of the BES. A number of commenters proposed alternative language for the definition.

The SDT considered these comments and decided to define the term BES Cyber Asset to focus on the "real-time" impact on the "Reliability Operating Services" of the BES, which include those functions performed for the reliable operation of the BES. This definition now provides the foundation for the definition of BES Cyber Systems. In addition, the SDT has included clarification in the definition on the 15-minute characterization of "real-time."

The new proposed definition of **BES Cyber System** is: *One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.*

The new proposed definition of **BES Cyber Asset** is: *A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset.*

The SDT has also modified the definition of Cyber Asset to make it more specific to the device and remove ambiguity on the exact nature of what is included in the definition of the Cyber Asset.

#	Organization	Yes or No	Question 1.a. Comment
1.a	WECC		Although this language is directly from the Federal Power Act, describing electronic devices as “hardware, software and data” is redundant and inaccurate. Electronic software and data reside on some type of hardware in all cases. Suggest removing the parenthetical as it is confusing and data is addressed later in the definition and the definition is clearer without it.If data is to be addressed in the standard it should be defined and addressed separately. The word “organized” is imprecise in this context; “Implemented,” “deployed,” or “utilized” may be a better word.The following rewrite is one proposed alternative.BES Cyber System Component - A programmable electronic device utilized in a BES Cyber System.
2.a	BGE	Agree with proposed definition	1.a and 1.b should be reversed. Disposition should be defined.
3.a	Old Dominion Electric Cooperative	Agree with proposed definition	Agreement is under the assumption that the present NERC definition of BES (e.g. =>100 kV) stands.
4.a	Progress Energy - Nuclear Generation	Agree with proposed definition	Define Disturbance
5.a	Florida Municipal Power Agency	Agree with proposed definition	FMPA agrees with the intent of the definition but believes that the definition can be improved significantly. FMPA offers the following simpler definition:”A programmable electronic device which responds to a BES condition or Disturbance, or enables control and operation of the BES.”For the following reasons: (i) “one or more” seems to

#	Organization	Yes or No	Question 1.a. Comment
			describe a system, not a singular component; (ii) we do not understand how “data” can be a component; and (iii) we do not understand the value of the “laundry list” of things components do and believe the focus should be on how the component impacts the BES.
6.a	Bonneville Power Administration	Agree with proposed definition	Greatly improved. Use of "...which respond..." clarifies that the standard is talking about control systems. However, please leave the parenthetical "(including hardware, software and data)" out. It is a bit confusing since data can't do any of the things listed. By definition a cyber system is made up of the hardware, the software and the data that allows it to operate. It appears that the punctuation in this definition is incorrect. We suggest:”One or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data which respond to a BES condition or Disturbance or enables control and operation.”
7.a	Dynegy Inc.	Agree with proposed definition	I agree but request additional detail examples be provided to determine specifically what these items are.
8.a	National Grid	Agree with proposed definition	National Grid agrees with the definition but seeks clarification from the SDT if the examples cited below will be considered as BES Cyber System Component:1) As part of the Burn Management System (BMS) in the power plant, the programmable PLC device is used along with the connected thermo-couples to monitor the temperature for fuel burning. If the temperature readings are wrong, the PLC can be programmed to take action to increase the fuel input or to limit/shutoff the fuel. This could have an immediate or short term effect (within 15 minutes). The amount of fuel determines what the output of the unit will be. Is the PLC or the entire BMS (including the PLC) BES Cyber Component? 2) Generating plant connects to Transmission Substation. There are programmable microprocessor relays installed within the substation for power plant / transmission line protection. Are these microprocessor relays BES Cyber Components?

#	Organization	Yes or No	Question 1.a. Comment
			3) The new BES Cyber System Component could also include the Exciter system that exists at Northport PS. Once again, could the PLC or the entire system, including the computer, be part of the BES Cyber Systems? 4) Another system that potentially could be included under the newer broad definition would be the Precipitator Rapper system. This system has a PLC that handles the Rappers. The system is not critical to Operations, however, under a broad definition that includes the 15-minute rule, if the Rappers failed, the unit(s) could be limited due to environmental compliance. The Precipitator Rappers are not connected to any network and are isolated.
9.a	Dairyland Power Cooperative	Agree with proposed definition	Shorten the name to BES Cyber Component.
10.a	Reliability & Compliance Group	Agree with proposed definition	The definition is O.K. Need to add BES to Disturbance and BES to enable control and operation. It would be more helpful if the definition “BES” were included in this document
11.a	Black Hills Corporation	Agree with proposed definition	The definition should include tie back to “BES Cyber System” as inserted above.
12.a	FEUS	Agree with proposed definition	The drafting team should consider clarifying; or enable or control and operation "of BES" or "greater than xxkV" This could be interpreted as an RTU in a 13.8kv sub serving only customer load.
13.a	PacifiCorp	Disagree with	: PacifiCorp agrees with EEI’s suggested alternative definition::BES Cyber System Component - One or more programmable electronic devices (including hardware)

#	Organization	Yes or No	Question 1.a. Comment
		proposed definition	organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: o Voice Communication systems o media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to the reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance the reliability of the BES. The terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed. In addition, the definition of "programmable" should be provided. Is a device that is "set" considered to be programmable?
14.a	Allegheny Energy Supply	Disagree with proposed definition	1) Does this definition need to cover more than a single device since a BES Cyber System is a collection of these? 2) Software and data should not be included in this definition. Protection of the software and data should be included in security requirements but not in the definition itself. Additionally these are both terms that are easily interpreted in different ways.3) It is difficult to get a clear understanding of what the terms "disposition" and "maintenance" mean in this context.4) Suggest: BES Cyber System Component - A programmable electronic device (including hardware), that is part of a BES Cyber System, providing input/output, processing, information storage, communications, human interaction (display, trending, alarming / alerting, input, etc.),

#	Organization	Yes or No	Question 1.a. Comment
			or maintenance, which is necessary for a BES Cyber System to fully perform its function.
15.a	Consultant	Disagree with proposed definition	1. Inclusion of the word 'communication' would seem to imply that communication equipment is included in the definition. Should be clarified to clearly state what aspects of communication, if any, is included.2. A 'component' would seem to be inconsistent with 'organized for the...' A component performs an activity, the 'system' would consist of 'components organized for the...'3. Software and Data are not programmable devices. Device implies hardware; if software and data are to be included the component definition should be clarified. What is software in terms of the definition? Operating system, application, database, word processing, executable files, scripts, and batch files...4. Component is singular - programmable electronic devices is plural. This is inconsistent. Suggest identifying a component (hardware, software, or data) as singular terms.5. I think "data" should be removed from this definition. Suggested new definition: BES Cyber System Component: hardware or software that performs one of the following functions (1) input, (2) processing, (3) storage, or (4) output of data that enables control or operation of a BES Cyber System.5.BES condition has no meaning. It is not a defined term, and therefore is vague. Suggest removing this wording or clarifying the intent.6. "... enable control or operation." - Of what, and when. All the time or only during a Disturbance? Needs clarification of the intent of this phrase.7. devices... for... display of data..." It is unclear how a display device could be compromised resulting in a degradation of the BES? 8. There is published literature that addresses the concepts of Cyber-Physical Systems that distinguishes between 'hardware components', 'software components', and 'bridge components' as the makeup of cyber-physical systems. This would appear to be a better framework for defining components than the listing of multiple functions, which dims the "bright lines" for consistently defining and categorizing the many variations and configurations within the industry.
16.a	Progress Energy (non-Nuclear)	Disagree with proposed	1. We feel programmable electronic devices is too broad. Also, it seems that there should be a distinction between firmware versus a traditional OS.2. From a generation perspective, these would be likely be in scope and shouldn't be - foundation field bus, device Net, smart transmitters (Rosemount), RS232/485 Serial connections and

#	Organization	Yes or No	Question 1.a. Comment
		definition	electronic protection relaying. We need to know if this would include DCS “Smart” field instrumentation using non-routable network protocols such as Foundation Fieldbus, DeviceNet, Hart, etc. Just about every instrument connected to plant automation system is a programmable electronic device. Per CIP 11 definitions of routable and non-routable they would be considered non-routable. We need examples of components included and components that would not be included. Possibly include examples for generation facilities, ECC’s and transmission. This could include Generator Protection Panels, PLC’s, EX2000 Generator exciter, Bentley Nevada vibration system, Medium Voltage Switch gear protective relays, motor protection relays, etc, etc. These are all “Programmable” and can be accessed via non-routable, ISO layer 1&2 hardware programming by MODBUS. All these devices are already INSIDE the protected Electric and Physical perimeter umbrella.3. The Standards definitions still seem to still be written to traditional PC and IT Business platforms. The standards need to be written to target single use industrial control systems.4. Based on this definition a microprocessor relay associated with a transmission line would be in consideration as a cyber component. If a device has burned in programming, maybe it is considered but classified low impact. User programmable devices may be a higher impact. Many programmable devices may not support use banners. Redundancy will not allow us to remove devices from scope.5. This reads like an ‘or’ definition. In that case, communication connectivity is not required for a device to be considered as a cyber system component. That needs to be very clear since with past standards we were evaluating based on external connectivity and routable vs. non-routable protocols.6. What constitutes a BES "condition"? 7. If definition is limited to the "organized" Cyber subsystems (e.g. 1.b. below) we can work with that. Attachment II appears to define the impact per Cyber System not component level. Suggest removal of component level definition and focus on system level issues.8. Proprietary protocols should not be included.9.Need clarification on what ‘programmable’ means. Recommended definition: Capable of dynamically accepting a sequence of operations to be automatically performed (a device which includes only firmware defined logic which cannot be dynamically changed - such as an EPROM - would not be included). Consider clarification between

#	Organization	Yes or No	Question 1.a. Comment
			programmable and configurable.10. Strike “one or more” because “one or more” implies a system not a component
17.a	Platte River Power Authority	Disagree with proposed definition	A “System Component” should be singular. For example: BES Cyber System Component - A programmable electronic device (to include the hardware, software and data) used for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which responds to a BES condition or disturbance; or enables control and operation.
18.a	LCEC	Disagree with proposed definition	A BES Cyber System Component should not be described as "One or more". Systems can contain more than one component but components should not consist of more than one device. Enable control and operation needs to describe what is being controlled or operated.
19.a	USACE - Omaha Anchor	Disagree with proposed definition	A) This definition could include phone systems - which according to the committee were not meant to be included in this standard. Has any thought been given to an exclusion table or specifically excluding telephone systems? B) Has any thought been given to separating out classification by operating system (OS)? - Ex. Windows, Unix, Solaris - high OS; PLC - low OS or general computing device. We are still going to have TFE issues with a lot of the low OS components.
20.a	Nuclear Energy Institute	Disagree with proposed definition	Agree with the exception that: Question 2 indicates that the definition of BES Cyber System bounds the scope to real-time operations systems, yet it is not clear from the proposed definition of BES Cyber System Component. Consider revising to:”One or more programmable electronic devices (including hardware, software and data) organized for the real-time collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation.”Lastly, the term “organize for” should be clarified by description such that a set of one-or-more programmable electronic devices constituting a BES Cyber System Component may be treated as a single system with respect to the application of requirements in CIP 011-1. This would preclude a debate

#	Organization	Yes or No	Question 1.a. Comment
			about how far down into an electronic device(s) the analysis must be performed. For example, a device with two programmable logic controllers on a single board may be treated as one BES Cyber System Component rather than individually as two BES Cyber System Components. Another example might include a turbine control system with vibration monitors. The collection of programmable electronic devices supporting the turbine control system including the monitors is a single BES Cyber System Component.
21.a	NextEra Energy Corporate Compliance	Disagree with proposed definition	At the workshop the drafting team requested that the industry point out comments that move the Version 4 forward, and any fatal flaws. The comments of NextEra Energy (and its affiliates, which include NextEra Resources and Florida Power & Light Company) (NextEra) will focus on constructive comments and fatal flaws. At this time, it appears that CIP-010 does not provide the proper foundation to build a CIP Standard that is well defined, so that the industry, the Regional Entities, NERC and FERC can all understand what is being protected, what is not being protected, or what should be protected via CIP-011. CIP-010 is thus fatally flawed. It is our opinion that CIP-010 should not offer the industry, auditors and regulators such flexibility to second guess each other, which is seen currently. Rather CIP-010 should have very clear definitions of what is the Control Center, what are the Transmission and Generation Cyber Systems that need to be protect and what are the BES Cyber System Components that must be protected for the identified Cyber Systems associated with Control Centers, Generators and Transmission. The flexibility protective options and performance based approach should be in CIP-011. Accordingly, NextEra requests that the drafting team develop a specific definition of what is and is not a BES Cyber System for Control Centers, for Generators, for Transmission - and list for each the BES Cyber Components that need to be protected in each. Given the short period of time from the workshop to these comments, NextEra was not able to propose definitions or lists, but NextEra will be working such and proposing them in the future. NextEra strongly recommends that the drafting team reconsider its flexibility approach in CIP-010 and requests, from the industry, specific definitions of what is and is not a BES Cyber System for Control Centers, for Generators, and for Transmission and a list for each of the BES Cyber Components that need to be protected in each. In this spirit, NextEra recommends the following edits.BES Cyber

#	Organization	Yes or No	Question 1.a. Comment
			System Component - A programmable electronic device (including hardware, software and data) listed below. At Control Centers, BES Cyber System Components are:(List)At Transmission Facilities, BES Cyber Systems Components are:(List)At Generation Facilities, BES Cyber Systems Components are:(List)
22.a	BCTC	Disagree with proposed definition	BCTC does not consider this a good definition as more clarity is required. The following are specific areas where BCTC feels the definition should be revised: - removal of the word "communication" "software" and "data" are not programmable devices. Their placement within the definition is confusing The definition is very "loose". BCTC would like the definition to be more clear as to what is a cyber system component (i.e. must such a component have a routable protocol, etc.) - right now we find it difficult to grasp this concept based on the current definition When referring to BES System Components (and BES System) clarification is required as to whether we are referring to just 'production' environments; development or quality assurance environments are excluded from scope? If you have components of the BES Cyber System (i.e. EMS) which are considered LOW impact, can you segregate/ isolate these devices on a separate network segment w/ firewall so that these components remain categorized as LOW or must everything be considered HIGH impact if any of the components are classified as HIGH?
23.a	Manitoba Hydro	Disagree with proposed definition	BES Cyber System Component" definition needs to be clarified. The defining characteristics of the device should be clearly enumerated by using appropriate punctuation. Placement of semi-colons is confusing as drafted. Example: "A programmable electric device that: (a) is organized for the collection of... and (b) either: (i) responds to a BES condition or Disturbance; or ii) enables control and operation.
24.a	Luminant	Disagree with proposed definition	Better definition on "Data" should potentially be limited to the hardware that stores the data and not the data itself. This should exclude Black start radio systems and in plant personnel communications systems such as 450 Mhz radio systems. The semicolon after Disturbance should be removed.

#	Organization	Yes or No	Question 1.a. Comment
25.a	City Utilities of Springfield, Missouri	Disagree with proposed definition	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
26.a	ERCOT ISO	Disagree with proposed definition	Consider: "One or more programmable electronic devices (including hardware, software and data) designed for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation."
27.a	Tenaska	Disagree with proposed definition	Data integrity is out of scope because SCADA, EMS and DCS systems have software to recognize bad data. Also the display of data should be out of scope there are BES Cyber System Components that if compromised will not affect the reliability of the BES i.e. PI historian's. The Pi Historian is used to display and store data and is not used respond to a BES condition or Disturbance; or enable control and operation.
28.a	CWLP Electric Transmission, Distribution and Operations Department	Disagree with proposed definition	Data should not be included as part of a device. Communications paths should not be included.
29.a	US Army Corps of Engineers, Omaha District	Disagree with proposed definition	define term disposition [of data]
30.a	Constellation Energy Control and Dispatch, LLC	Disagree with proposed definition	Delete the term BES condition from the definition.

#	Organization	Yes or No	Question 1.a. Comment
31.a	Constellation Energy Commodities Group Inc.	Disagree with proposed definition	Delete the term maintenance and condition from the definition. The term maintenance, as used in the BES Cyber System Component statement, does not have direct impact to the reliability of the BES. Define the term disposition and describe how it applies to BES Cyber System Component.
32.a	CenterPoint Energy	Disagree with proposed definition	Disagree - CenterPoint Energy believes the definition should include a reference to an external communication connection. A disconnected cyber system component is secure. An unintended consequence of this definition may be that entities will install communication connections to isolated cyber system components to remotely manage access requirements of the standard. This defeats the benefits of isolation as a security measure. This definition as currently written would also include programmable electronic devices located in control cabinets mounted on yard equipment within the substation yard. Applying certain requirements of the current draft standards to such equipment is extremely problematic.
33.a	E.ON U.S.	Disagree with proposed definition	E ON U.S believes one or more electronic devices used exclusively to display data should not be considered a BES Cyber System Component
34.a	FirstEnergy Corporation	Disagree with proposed definition	FirstEnergy Summary Response: FirstEnergy (FE) appreciates the hard work of the CIP Standards Drafting Team in developing the version 2 CIP standards and the quick implementation of Commission directed changes reflected in version 3 CIP standards. FE strongly supports the work of the CIP SDT to develop further enhancements to the cyber security standards that improve reliability while providing clarity and certainty. Protecting and guarding against unauthorized access to cyber systems used in the protection and control of the bulk electric system is a reliability priority that FE shares. It is clear that the NERC CIP standards drafting team's fundamental approach is well-intentioned, but will result in a significant diversion of resources away from making concrete, tangible enhancements to the existing framework of cyber protections. FE

#	Organization	Yes or No	Question 1.a. Comment
			fundamentally endorses enhancements to the critical infrastructure protection standards that improve security, clarity, and certainty, but strongly believes that wholesale restructuring of the existing CIP standards is not necessary and may be counter-productive to those goals. While there are some that conclude it is not feasible to sufficiently enhance the underlying approach embodied in the existing CIP standards, these conclusions disregard the considerable investment in people, tools, and processes to address these requirements that would be abandoned in favor of an alternate formulation. Building from the existing CIP approved standards and implementation investments, while strengthening the standards to provide needed clarity and certainty offers a far expedited path to enhance cyber security, also providing greater confidence in the strength of the cyber protections in effect across the industry. A fundamental aspect the SDT proposed abandoning is the Critical Asset determination approach in favor of a wholesale impact categorization structure that introduces different terminology, concepts, and uncertainties, while offering little added clarity. We support the teams guiding principles - leveraging investments in current standards, minimizing the need for TFEs, reducing administrative overhead, etc. - however the proposed standards do not seem to practically meet the primary need for BES security. The key guiding principal for the enhanced cyber standards is clarity to which assets of the bulk electric infrastructure require cyber risk protection. The impact categorization depicted in Attachment II is a significant improvement in achieving a consistent approach for determining high impact critical assets representing the backbone of the bulk electric system. FE encourages the drafting team to focus its efforts on further developing Attachment II to obtain industry consensus on high impact assets and incorporate the work into the existing CIP-002 for consistent Critical Asset determination. To the extent essential, this work could further be integrated within the existing standards to determine another category of less-critical assets to the security of the BES, requiring respectively lesser degree of cyber security protection. Enhancing bulk electric system cyber security does not require a paradigm shift from approaches integrated into existing cyber security programs. We encourage the drafting team to maintain continuity and leverage significant industry investments in implementation of cyber

#	Organization	Yes or No	Question 1.a. Comment
			security protections undertaken over the last half-decade to achieve conformance with the CIP standards. The underlying work of the SDT reflected in the proposed CIP-010 and CIP-011 standards represent important enhancements that can, and should, be integrated with the existing CIP standard architecture, and avoid introducing new set of methodologies, definitions, and requirements that will require virtually every aspect of utility implementation to be restructured - policies, procedures, training, systems, drawings, contracts, data, compliance monitoring tools, forms, etc. These proposed changes offer little improvement in cyber security protection over what can be promptly gained by enhancing the existing standards. While the multilevel categorization is well intended, we believe the maximum security improvements can be more promptly achieved by integrating with the existing infrastructure protection requirements. In sum, FirstEnergy endorses an approach that allows for enhancements of existing implementation that affords more certainty and clarity, and avoids approaches that involve revamping the entire design of cyber protection implementation. Namely, we would like to see the SDT: Discard the concept of a wholesale rewrite of the CIP standards -- using the standards drafting team work as an input to the enhancements of the existing standards. Enhance the existing CIP-002 through CIP-009 standards to clarify and improve upon the established approach. Retain the fundamental terms, concepts, and standards numbering scheme to enable continuity. This approach would more effectively build upon the work that has already been accomplished, while allowing the industry to continue to improve on security and compliance related to critical infrastructure. We appreciate the drafting team's careful consideration of FE's views on the appropriate path forward in further enhancing the bulk electric system protections against unauthorized access to cyber assets. Although FE does not align with the team's overall approach we have thoroughly reviewed the proposed standards and offer constructive feedback to the specific questions asked by the drafting team. It's noted that our individual question responses in many instances do not reflect our primary position of enhancing BES cyber security in a manner that retains the framework and terminology of the existing standards. These responses are provided in order to provide clarity to the extent the concepts may be incorporated into revision of

#	Organization	Yes or No	Question 1.a. Comment
			the CIP-002 through CIP-009 standards. - - - - - - - - - - - - - Question 1.a Response: Suggested alternative definition:"BES Cyber System Component - One or more programmable electronic devices (hardware or software) relied upon to respond to a BES Contingency or Disturbance and supports control and operation of a critical BES Facility."Reasons for suggested changes: o The middle portion of the BES Cyber System Component definition is confusing and provides little value for distinguishing BES Cyber System Components from other components. The terms collection, storage, processing, maintenance, use, sharing, communication, disposition, or display do not add clarity and can be removed to simplify. The inclusion of the term "data" requires clarification. It's not clear how data can be considered a programmable electronic device. FE's proposal removes this term. The term 'BES condition' is vague and open to interpretation. We suggest use of the NERC defined term for Contingency. The team should also clarify for industry if configurable, but non-programmable devices are to be considered as BES Cyber System Components. Also it should be clear that communication media (fiber, wiring) and transport devices (SONET, Microwave, etc) installed between BES Cyber System Components are excluded.
35.a	ReliabilityFirst Staff	Disagree with proposed definition	For clarity, ReliabilityFirst suggests the following revision to the language of this requirement, ". . . (including each device's hardware, software and data). . ."
36.a	GTC & GSOC	Disagree with proposed definition	GTC and GSOC are concerned that there may be a component of a BES Cyber System which does not meet this definition of a BES Cyber System Component. If the intent is to apply a cyber security control to a BES Cyber System Component, the SDT should be careful that the definition indeed captures all of the individual devices that make up a BES Cyber System. We recommend the following definition. "A programmable electronic device (including the hardware, software and data necessary for the proper performance of its function) necessary for a BES Cyber System to perform its core functions."

#	Organization	Yes or No	Question 1.a. Comment
37.a	Matrikon Inc.	Disagree with proposed definition	I agree with this definition, but ask for a label/definition/category for those cyber systems that do not “respond to a BES condition or Disturbance; or enable control and operation” as they will exist in the field and will need to be labeled consistently across different entities/regions. Case and point, Responsible Entities could call them “Cyber System Components” or “Cyber Components” or “Discrete Cyber Assets” or “Cyber Assets”, all having the same meaning but different label for the Auditors to understand. I understand it is not a priority for the SDT to label those cyber assets not subject to NERC CIP compliance, but it would provide consistency for labeling those systems which have been evaluated, and confirmed no relationship to the Bulk Electric System.
38.a	American Municipal Power	Disagree with proposed definition	I disagree with the definition on the terms that it may introduce unnecessary or inappropriate interpretations.
39.a	Southwestern Power Administration	Disagree with proposed definition	I disagree with the proposed definition and offer a simpler one that clearly identifies what is in scope.BES Cyber System Component - A programmable electronic device that has the ability to control a BES Facility and/or process data for the real time operation of the BES.
40.a	Wolverine Power	Disagree with proposed definition	I have a concern relating to the definition of "BES generation" vs. "BES transmission”. The NERC definition for BES transmission is clear (100kV+), but NERC defers to each regional entity to define "BES generation “Acknowledgment of the regional entity's right to define what constitutes "BES generation" is important to the application of CIP-010 and CIP-011:As I read the standard, any generation determined to be "BES" in CIP-010/-011 must then automatically be categorized as "high, medium, or low" critical impact (per Attachment 2 of CIP-010). - Even the "low" impact introduces and mandates several cyber controls be in place. So my question is: (How do you objectively determine if specific generation resources really have a material effect on the BES? Some situations are obvious (reliability "must-run" resources on the grid for example) - But just because

#	Organization	Yes or No	Question 1.a. Comment
			a generation facility eventually interconnects with BES doesn't necessarily mean it's material to the BES. So the question of what constitutes "BES generation" is an important to clarify with respect to the application and ramifications of these proposed standards. Proposed Solution: Make reference to (explicitly mention in the standards) each regional entity's definition of "BES generation". In RFC's case, BES generation is defined as: (1) individual generation resources larger than 20 MVA or a generation plant with aggregate capacity greater than 75 MVA that is connected via a step-up transformer(s) to facilities operated at voltages of 100 kV or higher. This provides necessary clarity with respect to applying these standards. Generation listed as "blackstart" for a small TOP's restoration plan isn't necessarily material to the BES just because it can be argued that it eventually interconnects somehow with the BES - Clarity and bright line definition of BES generation is important to interpretation of this standard. The regional entities have provided clarification, and it should be acknowledged in these standards.
41.a	Green Country Energy	Disagree with proposed definition	I suggest adding "primary level" to the phrase enable control and operation. So that it would read enable primary level control and operation. I also request a definition of "respond to a BES condition" from a generator operator perspective.
42.a	Lincoln Electric System	Disagree with proposed definition	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
43.a	MidAmerican Energy Company	Disagree with proposed definition	MidAmerican Energy agrees with EEI's suggested alternative definition: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET,

#	Organization	Yes or No	Question 1.a. Comment
			Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the Bested terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed.
44.a	The Empire District Electric Company	Disagree with proposed definition	Please consider the more simple definition: BES Cyber System Component - A programmable electronic device that has the ability to control a BES Facility and/or process data for the real time operation of the BES.
45.a	US Army Corps of Engineers	Disagree with proposed definition	Please define the term disposition [of data].
46.a	Puget Sound Energy	Disagree with proposed definition	Puget Sound Energy feels that "as owned or operated by the entity" needs to be added to the definition. As the definition is currently written, the standard could be applied to telecommunication links (or the Internet) that are completely out of an entity's control to implement requirements mandated in CIP-011. Also please provide examples of how "data" is a "programmable electronic device". It seems that the hardware and software

#	Organization	Yes or No	Question 1.a. Comment
			can be programmable, but the data itself must actually reside on hardware so it's unclear how to consider it a component solely by itself.
47.a	Madison Gas and Electric Company	Disagree with proposed definition	Recommend that the word "Disturbance" be removed from the definition since the NERC definition broadens the full meaning of BES Cyber System Component. A BES condition contains both normal and emergency statuses of the BES and a disturbance is a sub component of a BES condition (taking a normal condition to an emergency condition). Disturbance reporting is currently contained in EOP-004-1 and the reporting requirements of EOP-004-1 go beyond this Project and will lead to more confusion and redundancy within the NERC Standards. Recommend that the modifier of BES be added to "or enable control and operation of the BES". Recommend changing the phrase, "display of data" to "display of data about the BES" as it is BES data and BES operation that are of interest. The new definition should read: One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of BES data; which respond to a BES condition; or enable control and operation of the BES.
48.a	Hydro One	Disagree with proposed definition	Recommend the following definition - "A programmable electronic device (including hardware and software) organized as a part of a BES Cyber System".
49.a	ISO New England Inc	Disagree with proposed definition	Recommend the following definition - A programmable electronic device (including hardware and software) utilized as a part of a BES Cyber System.
50.a	Northeast Power Coordinating Council	Disagree with proposed	Recommend the following definition - A programmable electronic device (including hardware and software) organized as a part of a BES Cyber System.

#	Organization	Yes or No	Question 1.a. Comment
		definition	
51.a	San Diego Gas and Electric Co.	Disagree with proposed definition	SDG&E recommends removing “data” and “display of data” from the definition because these terms are too vague and can potentially include many devices that should not be in-scope with these Standards (TV Monitors, strip chart recorders, digital displays, and other lower-level devices that have very little or no impact on cyber security or the reliability of the BES).SDG&E recommends the removal of the term “enable control or operation”. This seems vague and may unnecessarily roll up isolated devices (especially at substations or at Generating stations) that “enable control and operation” but have very little to do with the reliability of the BES. Many of these devices are isolated and have a very low risk of impacting the reliability of the BES.SDG&E also recommends the removal of the terms “collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data”. These terms do not help to clearly identify in-scope components and just confuse the issue as entities brainstorm all the nuances of those terms. In exchange for removing the terms identified above, we are suggesting a new revised definition for BES Cyber System Component. The centerpiece of our new suggested definition revolves around the use of a routable protocol or dialup connection, which has strong ties back to CIP-002-2 and contains terms that compliant entities are already familiar with. Suggested Revised Definition for BES Cyber System Component - One or more programmable electronic devices utilizing a routable protocol or dialup connection (including software) which is used to monitor, control, or operate the BES. In addition to revising this definition, SDG&E also recommends that the drafting team release a document (perhaps a FAQ or Guideline) that steps through examples for various entities to show what devices / facilities would be in-scope with the requirements in CIP-010. We suggest this because we believe that the current Standard as proposed will bring an enormous amount of components and systems into scope that will require substantial resources to be compliant with the Standard. Will the reliability of the BES increase by the same substantial amount?
52.a	Regulatory Compliance	Disagree with	Some components such as the display of data may not impact real time operation. More

#	Organization	Yes or No	Question 1.a. Comment
		proposed definition	clarification is needed or strike the display of data from the definition.
53.a	IRC Standards Review Committee	Disagree with proposed definition	Some devices may meet the definition of BES Cyber System Component, particularly "enable control and operation" but have little to no impact to the BES if unavailable or compromised because operators may have alternative means to provide the same functionality. Is the intent of this phrase in the definition to expand the applicability of the term to components that are not related to BES condition or Disturbance? Or is it meant to apply only to those components that respond to BES condition or Disturbance?
54.a	Network & Security Technologies Inc	Disagree with proposed definition	Suggest striking "data" from the proposed definition. Cyber Systems and/or their components perform various operations with data (create it, store it, modify it, send or receive it, etc.), and data is of course fundamental to reliable, computer-aided or controlled operation of the BES, but it is not a "programmable electronic device."
55.a	Entergy	Disagree with proposed definition	Suggest: "or more" should be stricken; 'component' should be singular - a discrete unit. "Or more" is appropriate in the BES Cyber System definition below.
56.a	Allegheny Power	Disagree with proposed definition	Suggested alternative definition: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System

#	Organization	Yes or No	Question 1.a. Comment
			Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES. The terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed.
57.a	EEI	Disagree with proposed definition	Suggested alternative definition: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Alternatively, BES Cyber System could be defined before BES Cyber System Component. This would follow a top town approach. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES. The terms storage,

#	Organization	Yes or No	Question 1.a. Comment
			maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed. SUGGESTION: Reorder positions to place "BES Cyber System" prior to "BES Cyber System Component", this follows a top down approach. BES Cyber System - A system performing one or more BES functions identified in CIP-010 Attachment 1 and which if rendered unavailable, degraded, compromised, or misused would, within 15 minutes, adversely impact the real-time operational control of the BES.BES Cyber System Component - One or more programmable electronic devices that are a component of a BES Cyber System and which if rendered unavailable, degraded, compromised, or misused would adversely impact a BES Cyber System. Control Center - A location where one or more BES Cyber Systems are used to perform BA, RC, or TOP functions for generation Facilities or Transmission Facilities at multiple sites. Also consider removing the word communications. This would include any connection via leased lines or other third party data circuits.
58.a	Duke Energy	Disagree with proposed definition	Suggested clarifying change as follows: "One or more electronically programmable devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation."
59.a	Alberta Electric System Operator	Disagree with proposed definition	The AESO would like to see a more detailed definition of "enable control and operation" and a definition of "BES condition".
60.a	APPA Task Force	Disagree with proposed definition	The APPA Task force disagrees with the current definition and would like to point out areas where it can be improved. Foremost, we feel the whole standard revolves around the concept of routable protocol. Since this is a common theme of a number of the requirements we feel this should be included in the definition. Also we think the current definition tries to cover a laundry list of functions which complicates the definition. We provide the following edited version for the drafting team's

#	Organization	Yes or No	Question 1.a. Comment
			consideration: BES Cyber System Component -A programmable electronic device connected via routable protocol, which responds to a BES condition or Disturbance, or enables control and operation of the BES. If the drafting team does not use this version we at least request that adding “connected via routable protocol” be included in some manner in the definition that is used.
61.a	Wolverine Power	Disagree with proposed definition	The concepts of "BES" and "critical", as they relate to generation, need to be revisited and clarified -For example - A BES generator, that is used only occasionally, for peaking purposes, and is not black start capable, may logically be declared as "non critical" using the current NERC CIP guidelines - but under these proposed standards, as I read them, this example might be forced to be considered as "low impact".(low criticality vs. not critical)The existing CIP standards allow for a logical separation between "BES and Critical" (i.e. just because a generator is BES doesn't automatically mean it's critical to the BES - how it's used should be taken into consideration) Under these proposed standards, as I read them, any generation resource identified as BES, automatically must be characterized as "low impact" at a minimum. I believe there should be some language in the standard that 1) takes into account the regional entity's right to define what constitutes BES generation; and 2) Doesn't force a "low impact" by default on any and all "BES" generation, without due consideration of its actual use and true impact on the BES.
62.a	Cogeneration Association of California and Energy Producers & Users Coalition	Disagree with proposed definition	The current standard limits its applicability to those systems with routable protocols or dial-up access. That limits the applicability of the CIP standards to those systems that are accessible and therefore vulnerable. This proposed standard will impose the CIP requirements on all programmable equipment regardless of its accessibility to external forces. A cyber system inside a generator accessible only to generator staff is as critical to its function as any pump or valve. The security measures safeguarding the pump and the valve should also be sufficient for the cyber system. Only those cyber systems accessible to the outside world require additional, special security requirements. Similar comments were made by many parties in response to the definitions in the proposed

#	Organization	Yes or No	Question 1.a. Comment
			version 4 CIP standards.
63.a	Southwest Power Pool Regional Entity	Disagree with proposed definition	The definition as written could be read to imply that data is a BES Cyber System Component. Data is not a programmable electronic device; however data can reside on a programmable electronic device. The definition should be clarified to make it clear to the reader that the programmable electronic device includes any software and/or data residing on the hardware. Also, consider changing “or enable control and operation” to “or enable control, operation, and/or situational awareness.”
64.a	MWDSC	Disagree with proposed definition	The definition is confusing with disconnected phrases and will be subject to many interpretations. What’s the difference between a “condition” and a Disturbance? The NERC Glossary defines Disturbance as 3 events which should cover all relevant conditions. The proposed definition may be interpreted to include a condition on a local BES system which will not create a Disturbance to an interconnected system. For example, a relay for a transmission/distribution bank breaker may operate and drop the distribution voltage load connected to that BES substation, but not create any Disturbance to other systems. The term "control and operation" was changed from prior draft to "monitoring and control" -see Attachment I under CIP-010. Also, it is unclear who controls and operates the component. In the extreme, a smart grid meter on a distribution circuit could be a “programmable electronic device” which responds to or enables control of a BES condition by reducing or dropping load. Suggest changing definition as follows: "BES Cyber System Component - One or more programmable electronic devices connected to the BES (including hardware, software and data), organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data, and which respond to a BES Disturbance affecting an interconnected BES system or enable monitoring and control of the BES by a Transmission Operator, Generator Operator, or Balancing Authority."
65.a	USACE HQ	Disagree with proposed	The definition is still too broad. The definition includes “software and data” as devices, but when someone thinks of a device usually it is a physical component. I think the intended of the team is to state that the software and the data must be included as part

#	Organization	Yes or No	Question 1.a. Comment
		definition	of the device definition, therefore I suggest changing the definition from a "programmable electronic devices (including hardware, software and data)" to "programmable electronic devices (including its components such as hardware, software and data)". Also, the definition is broad enough that test environments and maintenance devices can be included in the definition. CIP-011-1, page 22, states that "devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System". I suggest that the exclusion of devices "not permanently connected to (the) BES Cyber Systems" be explicitly present in the definition of BES Cyber System Component. Lastly, I suggest that all the definitions, in both CIP-010-1 and CIP-011-1 be present together to make it easier for the reader to understand all the new language introduced to the standards
66.a	Kansas City Power & Light	Disagree with proposed definition	The definition is too broad regarding the application of the data used by programmable devices. The proposed definition would include devices used for system analysis or system maintenance with historical data (e.g. Disturbance Monitoring Equipment (DME)). The important considerations are for those devices for the processing and use of data in the real time control of the BES. Recommend modification of the current definition to: One or more programmable electronic devices (including hardware, software and data) organized for the processing and use of data for the purpose of control and operation of the BES.
67.a	US Bureau of Reclamation	Disagree with proposed definition	The definition needs to clarify that the phrase "or enable control and operations" applies only to Cyber System Components that enable the control or operation of BES Assets. It will also need to define the term BES Assets.
68.a	Exelon Corporation	Disagree with proposed definition	The definition should only contain elements that are directly associated with obtaining and using data in support of reliable real-time operations or a device that would automatically respond to an adverse condition on the BES. Specifically the elements in the proposed definition of storage, maintenance, sharing and disposition should not be included. The display of data is also not needed as the display of data would be covered

#	Organization	Yes or No	Question 1.a. Comment
			by the "use" element. The definition needs to be more definitive with the term "programmable electronic devices" and their potential to impact the BES. The definition should consider whether a device can be controlled or operated via remote communication. Disturbance (as defined in the Glossary of Terms Used in NERC Reliability Standards April 20, 2010) is too vague and casts too wide a net and is not in synch with EOP-004. The term "BES condition or disturbance" needs to be clarified. Exelon has a concern that this definition may be interpreted differently in each region.
69.a	Con Edison of New York	Disagree with proposed definition	The Drafting Team (DT) should not include collection, storage, maintenance, use; sharing, communication, disposition, and display of data in the definition because these components cannot respond to a BES condition and may add ambiguity to the definition. By including these words, the Standard is implying that company networks outside of the EMS (e.g. PI) may be included as BES Cyber Systems. Suggested alternative definition: "Any microprocessor-based programmable electronic device used to enable control and operation of a BES element."
70.a	Electricity Consumers Resource Council (ELCON)	Disagree with proposed definition	The existing standard applies to systems with routable protocols or dial-up access. That limits the application of the CIP standards to systems that are accessible and therefore vulnerable. The proposed new standard will impose the CIP requirements on all programmable equipment regardless of its accessibility by external threats. Only those cyber systems accessible to the outside world require special security requirements.
71.a	SCE&G	Disagree with proposed definition	The language "enable control and operation" needs to be better defined. What constitutes control?
72.a	Indeck Energy Services, Inc	Disagree with proposed	The phrase "which respond to a BES condition or Disturbance" doesn't differentiate a component that takes action directly because of the BES condition or Disturbance and one that takes action when told to do so following a BES condition or Disturbance. For example, an under-frequency relay will take action on its own (e.g. trip) upon measuring

#	Organization	Yes or No	Question 1.a. Comment
		definition	the frequency and time corresponding to its setpoint, whereas, a generating unit without a governor will increase generation when the ISO, RTO or TO requests it to do so following the BES condition or Disturbance. The second system shouldn't be categorized as a BES Cyber System Component based on its action following a BES condition or Disturbance. --------- [suggestion] "One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which independently respond to a BES condition or Disturbance."
73.a	Oncor Electric Delivery LLC	Disagree with proposed definition	The purpose of a "component" is to collect, store, process, etc DATA. Data should not be included in the specification of a "component". It should read, "One or more programmable electronic devices (including hardware and software) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation."
74.a	LADWP	Disagree with proposed definition	The term "organized" seems to broaden the scope of a BES Cyber System Component to any device that may not be utilized but could be utilized in the BES system. A clearer definition needs to be made.
75.a	American Electric Power	Disagree with proposed definition	The term "programmable electronic devices" is general and vague. For example, based on this definition it is not clear how it will align with transmitters and other microprocessor systems. AEP suggests that the drafting team develop a definition that provides more clarity as to what is to be considered in scope. AEP suggests using the wording of NIST SP800-82 sections 2.3.1 and 2.3.2 to clarify the control system components that need to be evaluated for security controls.
76.a	Public Service Enterprise Group companies	Disagree with proposed	The text in brackets "(including hardware, software and data)" is not clear. These items are not types of "programmable electronic devices". Does a specific piece "software" or "data" collection constitute a "BES Cyber System Components"? This text needs to be

#	Organization	Yes or No	Question 1.a. Comment
		definition	dropped or a clearer definition is required.
77.a	Minnesota Power	Disagree with proposed definition	This definition is generally acceptable, with clarification or correction regarding the following items: o What if the device is not programmable, rather defined to perform one function (i.e., coded in firmware)? These types of devices still could have security flaws. What is meant by "disposition" of data? Disposition of data is typically a maintenance function performed after-the-fact which would not have a real-time impact on the BES. There are corporate system which ultimately receive, display and/or act upon data pertaining to the BES. These are not for real-time operations, and should immediately be recognized as out of scope. This definition should reference "real-time operations" or "BES Reliability" to clarify the intended scope. Minnesota Power recommends the following revised definition:"One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, or display of data which, in real-time, respond to a BES condition or Disturbance or enable control and operation."
78.a	Ameren	Disagree with proposed definition	This definition is overbroad and potentially brings in an inappropriate number of devices that should be excluded from the scope of this definition, e.g. display terminals, personal cell phones, pagers etc. The last sentence "which respond to a BES condition" is too encompassing, and the term Disturbance is also. Also, if "communication" devices are going to be included in this definition, then communication devices need to be more precisely defined. The definition of BES Cyber System Component includes "disposition." This phrase should either be defined more precisely or removed.
79.a	Midwest ISO	Disagree with proposed definition	This definition is overly broad and seems to miss the point that the information technology is there to support the operation of the BES and not vice versa. For example, collection and storage of data does not impact the operation of the BES and should not even be considered unless the facility can be used to control or manipulate the operation. Furthermore, what does it mean to respond to a BES condition? Suggest modifying the definition to: One or more programmable electronic devices (including

#	Organization	Yes or No	Question 1.a. Comment
			hardware and software) organized to enable control, operation and protection of equipment.
80.a	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree with proposed definition	This is a vast improvement over "Bulk Electric System Subsystem," and agrees with the focus on the cyber system up front rather than round about. However, there is room for further improvement. The present proposed definition can include programmable relays with no network connection at all - serial or addressable - to cell phones used to receive SCADA alarms. The main focus of the Standard is to protect BES Cyber Systems that are vulnerable to network/Internet based attack, or infection from malicious software. Secondary is the need for physical protection; however, all critical facilities whether cyber or not in nature need physical protection. Therefore in light of this, restricting to components that are vulnerable to remote attack via a network, the Internet, or the inadvertent infection of malware is advised. It should be recognized that not all programmable electronic devises are subject to "cyber attack," and should be excluded. "including hardware" may fail to clarify what is included; does this include a network and supporting equipment connected to the BES Cyber System Component such as a printer, or does it imply only the programmable electronic device itself? The use of "respond to" implies automatic operations the BES Cyber System performs and the additional qualifiers "control and operation" implies programmable equipment that only supplies monitoring data of the BES is outside the CIP scope. This does not appear to cover the required need for BES operator situational awareness of the electrical condition of the BES, and partially negates the BES Cyber System definition below.CIP-011-1 R26 considers maintenance devices to not be part of a BES Cyber System. These devices should be excluded from the proposed definition to be consistent.CIP-011-1 R11 considers devices used to remotely access BES Cyber Systems to be external to those BES Cyber Systems. These devices should be excluded from the proposed definition to be consistent.
81.a	Pepco Holdings, Inc. - Affiliates	Disagree with proposed	We agree with EEI's comments including the position on software and data. In addition, there seems to be a potential for confusion by including "one or more" in the definition. Because there does not seem to be a clear distinction between BES Cyber System

#	Organization	Yes or No	Question 1.a. Comment
		definition	Component and a BES Cyber System, it would seem like a BES Cyber System Component could qualify as a BES Cyber System.
82.a	We Energies	Disagree with proposed definition	We Energies agrees with the EEI Suggested alternative definition and explanation: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: o Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES. The terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed.
83.a	Garland Power and Light	Disagree with proposed definition	We have concerns about data being included in the definition - Many of the CIP requirements are difficult to document or comply with for the data.

#	Organization	Yes or No	Question 1.a. Comment
84.a	Southern Company	Disagree with proposed definition	We recommend the following definition: One or more programmable electronic devices that are a component of a BES Cyber System and which if rendered unavailable, degraded, compromised, or misused would adversely impact a BES Cyber System. This definition should be moved to after the definition of BES Cyber System to reflect a top-down approach. If the list of functions is found to be necessary, communication should be removed or, at least, limited to communication outside the BES Cyber System.
85.a	Alliant Energy	Disagree with proposed definition	We think the existing definition is too broad and propose the following: One or more programmable electronic devices (including hardware and software) organized to enable control, operation and protection of BES equipment.
86.a	MRO's NERC Standards Review Subcommittee	Disagree with proposed definition	We think the existing definition is too broad and propose the following: One or more programmable electronic devices (including hardware and software) organized to enable control, operation and protection of BES equipment.
87.a	Constellation Power Source Generation	Disagree with proposed definition	What is the definition of the term “BES condition”? It is not a term in NERC’s Glossary of Terms. It needs a local definition much like other terms have been defined in these standards. Using the definition proposed for a BES Cyber System Component, is the intent to include electronic meters such as Nexus Meters? They do not respond to a BES condition, but they do display data. Constellation’s interpretation would be that they are out of scope, but that may not be the intent of the SDT.
88.a	Verizon Business	Disagree with proposed definition	The definition should be specific to the Bulk Electric System to ensure that it does not include generation facilities used on distribution systems or non-BES facilities. This change could be accomplished by adding to the end of the sentence "... on the Bulk Electric System (>100 kv)."

1.b. BES Cyber System — One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.

Summary Consideration:

Many conmmentors observed that the definition of the 15-minute window was too ambiguous. Others observed that a 30-minute window would be more in alignment with other reliability standards. Many commenters observed that the impact was too vaguely described in the definition, and the scope was too broad.

The SDT has carefully reviewed the 15-minute window and has concluded that 15 minutes was more representative of a real-time impact. Some reliability standards cite 30 minutes as recovery times, others cite 15 minutes. The SDT believes that a 30 minute window may include more systems that would not have a "real-time" effect on the reliability of the BES. The SDT has shifted the BES impact aspect of the definition of BES Cyber Systems to the definition of BES Cyber Assets, with clearer definitions of the impact, with respect to "BES Reliability Operating Services", and specific reference to BES "real-time" reliability operations.

The new definition of **BES Cyber System** is:

One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.

#	Organization	Yes or No	Question 1.b. Comment
1.b	BGE	Agree	1.a and 1.b should be reversed.
2.b	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the definition but believes that the definition can be improved significantly. FMPA offers the following simpler definition:"One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could cause a Disturbance to the BES, or restrict control and operation of the BES within 30 minutes."For the following reasons: (i) see comments to Question 2 for time considerations; and (ii) including that phrase loss of situational awareness is superfluous since it restricts control and operation of the BES and is therefore included in that term.

#	Organization	Yes or No	Question 1.b. Comment
3.b	Puget Sound Energy	Agree	Generally agree, however it is unclear how to use the 15 minutes very meaningfully and how that will be tested in an audit.
4.b	Dynegy Inc.	Agree	I agree but request additional detail examples be provided to determine specifically what these items are.
5.b	Green Country Energy	Agree	Please define "affect situational awareness"
6.b	Reliability & Compliance Group	Disagree	: There needs to be more clarification about what it means to “restrict control and operation.” If you lose backup control, does this restrict control and operation if you still have primary control? Also, provide a definition of situational awareness in the standard at this point and capitalize the term.
7.b	Oncor Electric Delivery LLC	Disagree	“Systems” are categorized as high, medium and low, entities will tend to identify “Cyber System” at the lowest level possible. We need more clarity (white paper) to assist in how utility equipment should be identified as components or systems.
8.b	Indeck Energy Services, Inc	Disagree	1) The phrase “if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause” is too broad with the word “could”. The proper standard should be “is highly likely to cause.” 2) Situational Awareness is defined as the state of the BES. If this means that it includes systems and data used in the State Estimator, then it should specify that. The more specific the definition, the more certainty that BES ALR will be assured. 3) In FERC Order 706, NERC was required to “provide sufficient guidelines to inform generation owners and operators on how to determine whether it should identify a facility as a critical asset.” The only guideline that this definition provides is that the Cyber System could cause a disturbance. Spread across the nine Functions in Attachment I, this is patently incomplete as guidelines. For each of the Functions, some basis for a risk assessment should be outlined. [suggestion] “As to function Controlling Voltage (Reactive Power), any BES facility (asset) capable of providing <100 MVARS is not a BES Cyber Asset as to this function.” 4) [suggested replacement language] "As determined through the application of the Registered

#	Organization	Yes or No	Question 1.b. Comment
			Entity's risk based assessment methodology, one or more BES Cyber System Components which, if rendered unavailable, degraded, compromised, or misused, is highly like to cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES."
9.b	Progress Energy (non-Nuclear)	Disagree	1. Need a better statement of what 'within 15 minutes' means. Is 15 minutes considered real time operation? Most disturbances will occur in milliseconds. Is there a basis for 15 minutes? A malicious code could lie dormant for extended periods of time, but if activated may have an immediate impact. The term misused is very subjective and may need clarification. The 15 minute window may be good in that it possibly excludes equipment such as circuit breaker hydraulic, pneumatic and gas systems which may cause a breaker to be removed from service but not within 15 minutes. 2. With the 15 minute definition and using organized subsystem concept from 1.a. we can design Cyber (sub)Systems' delineation to effectively minimize impact on BES (see question 7 below). Limit Medium, High impact to a select few subsystems with the rest Low impact. Alternatively the entire plant control system would be viewed as one large Cyber System (High Impact) with the resultant full CIP requirements.3. Rules regarding redundancy need to be clearly defined. The 15 minute window brings redundancy into the picture.4. Need clarification of the terms 'compromised' and 'misuse'.5. Need to know if this would include DCS networks that do "batch" (non-continuous) type control. Some examples would include coal/limestone/gypsum conveying, limestone slurry processing, etc. These processes have inherent storage capabilities that far exceed the 15 minute rule.
10.b	Consultant	Disagree	1. The term would appear to imply that the "one or more BES Cyber System Components" perform a function related to the BES, for example, voltage control, generation control, transmission control, etc. The definition does not appear to address a "Cyber System", it appears to address just a "pile of components". If the answer is just the impact as it applies to a "pile of components", then this term would seem unnecessary as the "pile of components" is covered by the BES Cyber System Components term. It would seem that this definition should distinguish between

#	Organization	Yes or No	Question 1.b. Comment
			components, such as multiple desktop computers and servers as individual devices and their installed software (BES Cyber System Components), and the collection of those components networked and programmed to function as an Energy Management System (BES Cyber System).2. This clarification then raises the question whether the threat ("degraded, compromised, or misused") is a threat to components or a threat to systems. If the component is threatened then the system is threatened, but is there a mechanism to threaten the system without threatening the components? 3. This clarification would have an impact on the methodology for identifying affected assets.
11.b	Entergy	Disagree	A) How is "restrict" defined? How will this be audited? Suggest: Consider deletion B) Many things can "affect" situational awareness of the BES? Suggest "could...adversely affect." C) How much loss of situational awareness does it take to adversely affect the BES? We lose it all the time and keep on running (e.g., temporarily using state estimators) Suggest: Consider deletion D) How much of the BES is at issue? Suggest: "...could, within 15 minutes, cause a Disturbance in that part of the BES falling under the aegis of the Responsible Entity."
12.b	Nuclear Energy Institute	Disagree	Agree with the exception that: The word "could" is ambiguous. Propose changing could to would. Additionally, this definition does not maintain alignment with the definition of "reliable operation" provided in Section 215 of the Federal Powers Act: "The term "reliable operation" means operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements." The definition of BES Cyber System should be revised. An acceptable definition would be:"One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused would, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements." Lastly, it should

#	Organization	Yes or No	Question 1.b. Comment
			also be clarified that a single facility may have BES Cyber Systems that have different impact categorizations. Upon initial read, it would seem that if the one system in a generating station has a power capability of 2,000MW, then every BES Cyber System at the station is High Impact, which is inappropriate.
13.b	GTC & GSOC	Disagree	Although we appreciate that it is extremely difficult to define this concept, the current definition is too expansive. The phrase "affect situational awareness of the BES" could be interpreted to include the loss of a single status point. Such a minor outage would "affect situational awareness of the BES" but only to a trivial extent. The same could be said with respect to control. We suggest an alternative below. In addition, CIP 010 creates the definition above and then qualifies it in R1 to include only the BES Cyber Systems that "enable one or more functions defined in CIP 010 -1 Attachment I". But CIP 011 has no such qualification (except in its purpose statement), so in theory CIP 011 could apply to a more expansive set of assets than CIP 010. We recommend that the qualifications in R1 be incorporated into the definition. The clarification regarding maintenance devices that is currently in the local definition for maintenance devices (R26) should be part of this definition. Finally, the term "owned" is too narrow; theoretically an entity could absolve itself of all CIP compliance responsibility by leasing its systems. As noted in response to question 10 below, perhaps the concept of "responsible for" would be more appropriate than "owns." We recommend the following definition: One or more BES Cyber System Components which: 1) Performs one of the following functions-Dynamic Response-Balancing Load and Generation-Controlling Frequency (Real Power-Controlling Voltage (Reactive Power)-Managing Constraints-Monitoring & Control-Restoration of BES-Situational Awareness-Inter-Entity Real-Time Coordination, and 2) if rendered unavailable, degraded, compromised, or misused, could, within 15 minutes: (a) cause a disturbance to the BES; (b) restrict control and operation of the BES to the extent an entity can no longer fulfill its obligations under Reliability Standards; or (c) degrade situational awareness to the extent that an entity can no longer maintain an accurate view of the operational status of the portion of the BES it is responsible for. 3) Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered

#	Organization	Yes or No	Question 1.b. Comment
			part of a BES Cyber System.
14.b	BCTC	Disagree	BCTC recommends the following aspects of this definition be revisited: Â reword "within 15 minutes" to "15 minutes or less" the 15 minute threshold is considered adequate for high impact systems but feel that the threshold would not be the same for medium and low impact systems; for low impact systems, for example, the threshold could be as high as 24 hours before any potential impact to the BES would be realized.
15.b	Network & Security Technologies Inc	Disagree	Believe the 15-minute threshold, while intended to distinguish systems required for and/or affecting real-time ops from others, could have a number of unintended consequences. Entities inclined to "game the system" could declare none of their cyber systems would impact the BES if lost or compromised for at least 20 minutes. How would such a claim be verified or disproven? Moreover, wouldn't a 15-minute threshold compel the establishment of cyber security incident response and/or recover plans with an often unrealistic time to complete of 15 minutes? That this is a difficult problem is understood - at a minimum the SDT might consider adding language to CIP-010 and 011 indicating this definition should not be interpreted as requiring a 15-minute recovery time interval for BES Cyber Systems.
16.b	Platte River Power Authority	Disagree	BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could cause a real-time deadline to be missed resulting in a Disturbance to the BES, or restricting control and operation of the BES, or affecting situational awareness of the BES.
17.b	Minnesota Power	Disagree	BES Cyber System should be defined as "physical or logical set of one or more BES Cyber System Components which if rendered unavailable, degraded or compromised, could, within an operational time horizon of 15 minutes, cause a Disturbance to the BES or restrict control and operation of the BES."
18.b	WECC	Disagree	Change "affect situational awareness" to "loss of situational awareness". Also is Situational Awareness defined? The 15-minute criterion seems arbitrary and unneeded.

#	Organization	Yes or No	Question 1.b. Comment
			The ability to negatively impact the BES is an attribute that either exists or does not regardless of time factors. The time element should be removed.Bulletizing the list of impacts would better format the definition.The following rewrite is proposed; BES Cyber System - One or more BES Cyber System Components deployed for: The control and operation of the BES; or Collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data used in control and operation decision making for the BES. These systems, if rendered unavailable, degraded, compromised, or misused could cause one or more of the following; A Disturbance to the BES; or Restrict control and operation of the BES; or o Affect situational awareness of the BES.
19.b	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
20.b	Cogeneration Association of California and Energy Producers & Users Coalition	Disagree	Comments to Question 1.a above apply here also. Additionally, this definition would be difficult to apply for many entities. For example, how would a GOP determine if a problem at a generation plant would, within 15 minutes, cause a Disturbance to the BES if a BES Cyber System is rendered unavailable, degraded, compromised, or misused? In most cases, our experience with plant trips, equipment malfunctions and forced shoutdowns has indicated no effect on the interconnected grid.Guidance will be needed on how entities who do not operate the BES and do not have access to BES studies can determine if their facility will cause a Disturbance to the BES within 15 minutes when a Cyber System is unavailable, degraded, compromised, or misused.
21.b	ERCOT ISO	Disagree	Comments: The 15 minute requirement does not align to the other reliability standards. Recommend changing to 30 minutes to align with the EOP standards.
22.b	Southwest Power Pool Regional Entity	Disagree	Consider changing “One or more BES Cyber System Components…” to “One or more logically related BES Cyber System Components…” Also, is the term “Disturbance” well understood? The three definitions found in the NERC Glossary of Terms (April 20, 2010) use vague terms that may be open to interpretation by the reader. Similarly, the term “affect situational awareness” is sufficiently vague to be unclear exactly what is meant.

#	Organization	Yes or No	Question 1.b. Comment
			Without precise definitions, the entity and auditor may have different interpretations of the terms.
23.b	Constellation Energy Commodities Group Inc.	Disagree	Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such a tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment.Suggest that the time horizon be changed to within 10 minutes to remain consistent with the Area Control Error requirements. As stated in NERC documentation: DCS measures if a control area is meeting its reserve requirements. These reserves include contingency reserve and regulating reserve. The control area must: 1) recover from the contingency and 2) regulate to load changes over the ten minutes, but the control area need not correct control error that existed before the contingency.If the control area or reserve sharing group recovers ACE to zero or to the level of ACE prior to the first contingency within ten minutes of the start of the second contingency then count two contingencies as recovered 100% within 10 minutes. BAL-001-0.1a - Real Power Balancing Control PerformanceIn order to ensure that the average ACE calculated for any ten-minute interval is representative of that ten-minute interval, it is necessary that at least half the ACE data samples are present for that interval.
24.b	Constellation Energy Control and Dispatch, LLC	Disagree	Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon

#	Organization	Yes or No	Question 1.b. Comment
			to directly operate equipment.
25.b	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes this definition is ambiguous. The NERC glossary definition of "Disturbance" is very broad and "affect situational awareness" is also ambiguous. In addition the word "could" as used in "...could, within 15 minutes, cause a Disturbance..." is problematic. "Could", under what circumstances or what system conditions? Further clarification is required.
26.b	Turlock Irrigation District	Disagree	Disagree because this definition would include communication systems which are currently exempt from the CIP Standards and would therefore represent a major expansion of the cope of the CIP Standards. Was this the intention of the SDT?
27.b	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Disturbance has no metrics in its definition: "1. An unplanned event that produces an abnormal system condition. 2. Any perturbation to the electric system. 3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load." Therefore any "unplanned event that produces an abnormal system condition" on the BES must be included. Coupled with the broad definition of BES Cyber System Component, almost all programmable electronic devices will be included. Consider the following: loss of a programmable relay and its redundant backup will create the loss of protection on the BES facilities it is assigned to; these relays are not networked with any other cyber systems. The loss, say from malicious physical tampering from a disgruntled employee within the substation, is the unplanned event; and the resulting loss of BES transmission protection is the abnormal system condition. Therefore, it appears that the programmable relays must be included as a BES Cyber System even though the only way to compromise these components is through direct physical contact.If the definition of BES Cyber System Component is expanded to include monitoring ability, "situational awareness of the BES" should be clarified to encompass the electrical status of the BES. Otherwise, situational awareness can include video surveillance and security equipment that is programmable. Security systems should not be considered except where they help protect Medium or High Impact BES Cyber System Components and BES facilities. The cell phone

#	Organization	Yes or No	Question 1.b. Comment
			mentioned in 1.a. above is a BES Cyber System if it displays BES alarms. CIP-011-1 R26 considers maintenance devices to not be part of a BES Cyber System. These devices should be excluded from the proposed definition to be consistent. CIP-011-1 R11 considers devices used to remotely access BES Cyber Systems to be external to those BES Cyber Systems. These devices should be excluded from the proposed definition to be consistent.
28.b	National Grid	Disagree	Do not have a clear understanding of the "within 15-minutes" interval to have an impact on the system. It appears that this clause applies only to control operations such as opening and closing of a breaker. In substations where protection and control are integrated it would be possible to make changes that will take longer than 15 minutes to impact the BES. What type of contingencies will be considered for the 15 minute time horizon? (n-1, n-2 or none). Also, many of the cyber systems are programmable devices. The cyber security could be compromised in real time and the detrimental effect can be achieved after a programmed time interval. This issue requires to be addressed in the definition. There is also no link between attachment I and definition of BES Cyber System. Suggest tying attachment I with definition of BES Cyber System. National Grid proposes the following definition: One or more BES Cyber System Components which execute(s) or enable(s) one or more functions essential to the reliable operation of the BES and which, if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness.
29.b	Dominion Resources Services, Inc.	Disagree	Dominion supports the inclusion of "within 15 minutes". It is important to establish a reasonable boundary condition for real-time or near real-time effects of the BES Cyber System and 15 minutes provides adequate time for the effects to be mitigated to prevent further harm to the BES. In addition, Dominion proposes to replace the phrase "or affect situational awareness of the BES" with "or affect BES situational awareness of one or more of the following: Balancing Authority, Transmission Operator, Reliability Coordinator." This modification is reflected in the revised definition below: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable,

#	Organization	Yes or No	Question 1.b. Comment
			degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES; or restrict control and operation of the BES; or affect BES situational awareness of one or more of the following: Balancing Authority, Transmission Operator, Reliability Coordinator.
30.b	E.ON U.S.	Disagree	E ON U.S. believes the term "affect situational awareness" is overbroad. E.ON U.S. suggests that this term should be rewritten as "degrade situational awareness." Also, "Unavailable" is not clearly defined. E.ON U.S. believes that it would be helpful if one could determine "no impact" assessments
31.b	Exelon Corporation	Disagree	Exelon suggests that the time period should not be stated in specific minutes. The standard should be revised to "One or more BES..., or misused could, without sufficient time to take mitigating action, cause a disturbance to the BES,..."
32.b	Progress Energy - Nuclear Generation	Disagree	For nuclear purposes the use of the word "component" conflicts with the definition in 1a. A system contains components rather than a component being a system.
33.b	USACE - Omaha Anchor	Disagree	Further clarify Disturbance to the BES - potentially consider "negative Disturbance"
34.b	USACE HQ	Disagree	Given that BES Cyber System is based on the definition of BES Cyber System Components, which I disagree with, I must also disagree with this one. Furthermore, the use of a time limit to represent real-time should not be present given that is lacking documentation support for the number. Either introduce a definition for real time for CIP purposes or provide support for the risk-informed dentition of using 15 minutes as the limit.
35.b	Southwestern Power Administration	Disagree	I disagree with the proposed definition and offer a simpler one that clearly identifies what is in scope.BES Cyber System - A collection of one or more BES Cyber System Components which control a BES Facility(s) and/or process data for the real time operation of the BES. To define the scope of applicability for the CIP standards, real time is considered to be the operational time horizon of approximately 15 minutes.

#	Organization	Yes or No	Question 1.b. Comment
36.b	The Empire District Electric Company	Disagree	I disagree with the proposed definition please consider the simpler one that clearly identifies what is in scope.BES Cyber System - A collection of one or more BES Cyber System Components and associated communication network(s), which control a BES Facility(s) and/or gather data for the real time operation of the BES.
37.b	Kansas City Power & Light	Disagree	Including "within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES" in the definition provides a difficult set of parameters that encourages issues with interpretation of what would constitute the situations under which "within 15 minutes" applies, as well as, what constitutes "restricted control or generation"? It is understood the Drafting Team is trying to capture the essence of those systems that have a real-time impact on the BES, however, it is recommended to limit the scope of the applicable "BES Cyber System" to those systems that support facilities that are identified as critical to the reliability of the transmission grid determined by regional system study. Recommend the following definition for consideration: One or more BES Cyber System Components that provide support for facilities that have been identified as critical to the reliability of the BES.
38.b	Ingleside Cogeneration, LP	Disagree	Ingleside Cogeneration, LP believes that this definition is still too vague to make a determination of whether a system meets the threshold of a BES Cyber System and can be assigned a "No-Impact" rating. This is in stark contrast with the "bright line" delineation between High Impact systems and Medium Impact systems provided in Attachment II of CIP-010-1. The components of the definition in question are "restrict control and operation of the BES" and "affect situational awareness of the BES". Both seem to be Control Center concepts and could be interpreted to mean that any system supporting multiple generation or transmission facilities at multiple locations would automatically carry at least a "Low-Impact" rating. However, this does not speak to the associated generation or transmission facilities that may be "No-Impact" if a cyber intrusion cannot cause a Disturbance - a term which is very well defined in EOP-004-1. Ingleside's concern is that recent rulings by FERC concerning the definition of the BES

#	Organization	Yes or No	Question 1.b. Comment
			and the applicability of PRC-023-1 to facilities under 200 kV, indicate they are pushing a stricter level of adherence to Reliability Standards across the board. If this continues, Functional Entities with “No-Impact” systems once considered compliant with CIP-010-1, may be considered non-compliant at a future date. This could lead to the assessment of violations and fines, even though the Standard has not changed.
39.b	Emerson Process Management	Disagree	It could be more appropriate to state that the unavailable component(s) can not be recovered within 15 miuntes.
40.b	Bonneville Power Administration	Disagree	It is not clear that this definition limits the scope and applicability of CIP-010-1 (and CIP-011-1) to real-time operations systems as indicated in Attachment I and Question #2 of this comment form. Situational Awareness is too broad and all the commas in the definition can lead to numerous interpretations of the sentence. Recommend changing the definition to the following: "One or more BES Cyber System Components which if rendered unavailable, degraded compromised, or misussed could, within 15 minutes: (1) cause a Disturbance to the BES; or (2) restrict real-time control and operation of the BES; that could cause a Disturbance in 15 minutes, or (3) affect situational awareness of the BES that would lead to a Disturbance required for real-time control of the BES. "What is real-time operations? To fully understand the definition of a BES Cyber System, the reader must pull out the NERC Glossary for the definition of Disturbance, BES, and ACE. Recommend an explicit definition that doesn't contain words from the NERC Glossary of Terms.NERC defines Disturbance as: 1. An unplanned event that produces an abnormal system condition. 2. Any perturbation to the electric system; or 3. The unexpected change to ACE (Area Control Error) that is caused by the sudden failure of generation or interruption of load.
41.b	CWLP Electric Transmission, Distribution and Operations Department	Disagree	It is unclear how the 15 minute time frame is to be construed for the purpose of defining a BES Cyber System. The 15 minute time frame appears arbitrary.

#	Organization	Yes or No	Question 1.b. Comment
42.b	FirstEnergy Corporation	Disagree	It is unclear if systems such as HP OpenView or a centralized logging system, which monitor alerts, are outside the scope of a BES Cyber System or if they are considered to affect situational awareness of a BES. As written, the definition could encourage entities to not install alerts so as not to have additional cyber systems. FE proposed change: "... or impact situational awareness that is deemed essential to the reliability of the BES". As an alternate, FE also supports EEI's suggested change to " ... materially disrupt situational awareness of the BES"The SDT should clarify how redundancy may impact the classification of BES Cyber Systems. For example, in a highly redundant architecture, there are many components whose loss would not impact or render essential systems as unavailable.The team should consider leveraging its work in developing the BES Cyber System and BES Cyber System Components to revise the existing Critical Cyber Asset.
43.b	Dairyland Power Cooperative	Disagree	It seems likely that a component could belong to multiple systems. How does this fit with the compliance regulations? Sentences are a little confusing with nested commas... It seems the intent is that 15 minutes applies to causing a disturbance, but it could be argued that it is ambiguous.
44.b	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
45.b	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggested alternative definition: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness of the BES.
46.b	US Army Corps of Engineers, Omaha Distirc	Disagree	Need definitions of "restrict control and operation" and "affect situational awareness. These are very broad. If the intent of the standard is to create groups of cyber system

#	Organization	Yes or No	Question 1.b. Comment
			components and evaluate them based on their impact to system reliability why not state the definition in terms of the impacts. Suggest alternative wording - A Cyber System Component or logical grouping of Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, negatively impact one of the functions essential to the operation of the BES (Dynamic Response, Balancing Load and Generation, Controlling Frequency, Controlling Voltage, Managing Constraints, Monitoring & Control, Restoration of BES, Situational Awareness, Inter-Entity Real-Time Coordination and Communication, other functions as needed).
47.b	Garland Power and Light	Disagree	Need to add "scoping filter" as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states "typically excludes business, market function systems, and non real-time systems", then it is a good definition and we would agree.
48.b	The United Illuminating Co	Disagree	Not clear if the rendering unavailable, degraded, compromised or misused applies to the Cyber System or to the individual components of the Cyber System.Suggest: BES Cyber System - Comprised of One or more BES Cyber System Components. If a BES Cyber System when rendered unavailable, degraded, compromised, or misused could, within 15 minutes of such act, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.
49.b	PacifiCorp	Disagree	PacifiCorp agrees with EEI's suggested alternative definition:BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness

#	Organization	Yes or No	Question 1.b. Comment
			of the BES. In addition, the phrase "situational awareness of the BES" needs some more clarity to derive determine what is intended.
50.b	Public Service Enterprise Group companies	Disagree	Please clarify that the 15 minute threshold means that if the cyber component would not cause a disturbance in the BES, or restrict control and operation, or affect situational awareness, within 15 minutes, the aggregation of BES Cyber System Components is not deemed to be a BES Cyber System and thus out of scope of Version 4.
51.b	Hydro One	Disagree	Recommend the following definition - A set of one or more programmable electronic device(s) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; and which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES for the support of real-time operations. The SDT should consider 30 minutes instead of 15 as this time is consistent with requirements of EOP-001 and IRO-001.
52.b	ISO New England Inc	Disagree	Recommend the following definition - A set of one or more programmable electronic device(s) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; and which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES for the support of real-time operations. - Recommend "30 minutes" to align with EOP standards - Please provide background for where the 15 minute recommendation came from.
53.b	Northeast Power Coordinating Council	Disagree	Recommend the following definition - A set of one or more programmable electronic device(s) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; and which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of

#	Organization	Yes or No	Question 1.b. Comment
			the BES for the support of real-time operations.
54.b	Con Edison of New York	Disagree	Regarding the BES Cyber System definition, specifically the qualification criteria “within 15 minutes could impact BES operation”, it is not clear how an entity will determine / distinguish which BES Cyber Systems could impact operation within 15 minutes versus which will not. This may be more challenging than distinguishing which Cyber Assets are essential to operation or not, as we do for version 2 of the CIPs. Our understanding is that the purpose of including the 15 minute period is to limit the application of CIP-010 to BES Cyber Systems impacting real time operations. An alternate way to address BES Cyber Systems impacting real time operations would be to look to the existing NERC Reliability Standards. The following definition language is recommended: “The following operating functions are essential to real-time reliable operation of the Bulk Electric System (BES). To define the scope of applicability of CIP Standards, the functions of relevance are only those that can have an effect on real-time operation of the BES within the time period established in the applicable Reliability Standard(s), or if no time period exists, within 15 minutes of the BES Cyber System failure.”The following are examples of Reliability Standard citations: Standard BAL-005-0.1b - Automatic Generation Control R6. ... If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator. Standard EOP-001-0 - Emergency Operations Planning R2. The Transmission Operator shall have an emergency load reduction plan for all identified IROLs. ... The load reduction plan must be capable of being implemented within 30 minutes.
55.b	MWDSC	Disagree	Same general comments as for BES Cyber System Component. Also, "situational awareness" is redundant with the "monitoring and control" function as specified in Attachment 1 - see comment to Question 3 and suggested combination of terms. Disturbance reporting is required under EOP-004 - to avoid confusion or a conflict, definition needs a cross reference. Suggest changing last part of definition as follows:"... within 15 minutes, cause a Disturbance to the BES that requires a report pursuant to EOP-004, or affect the monitoring and control of the BES by a Transmission Operator,

#	Organization	Yes or No	Question 1.b. Comment
			Generator Operator, or Balancing Authority.
56.b	San Diego Gas and Electric Co.	Disagree	SDG&E is supportive of the "15 minute" criteria to help focus CIP-010 attention on real-time BES Cyber Systems. SDG&E recommends clarifying the categorization levels in conjunction with the 15 minute criteria, if the architecture or design includes the concept of redundant BES Systems (per Attachment I & II). Example: If a given BES System is potentially classified as a High BES System; but where an Entity has designed and operates a redundant BES System to enhance reliability of the BES Systems; and one which is in place to mitigate or reduce negative impacts to the BES, then the combined redundant system would not meet the criteria of a High BES System. Suggestions include incorporating a third classification category or filter which identifies potential High BES Systems which are treated separately, but have security controls applied.In the definition for a Component, the language states how a cyber system component "responds" to a BES condition or Disturbance or "enables" control and operation, but when talking about the System, a Component is spoken of in terms of a "causing" a disturbance, or "restricting" operation. Why is the piece of the whole (the component) "responding or enabling" yet when used in the context of "the whole" (the system) the piece is now labeled as "causing or restricting"? It is a bit confusing and redundant that a cyber system may also be a cyber system component. SDG&E is not certain what the value is with this level of granularity, and we are not certain that a "system component" definition is necessary. In addition, SDG&E suggests additional clarification on what "affect situational awareness of the BES" means.
57.b	Electricity Consumers Resource Council (ELCON)	Disagree	See comment on 1.a above.
58.b	Wolverine Power	Disagree	See comments listed for 1a
59.b	NextEra Energy Corporate Compliance	Disagree	See comments to 1.a. Furthermore, NextEra questions why there needs to be qualifiers like Disturbance. The industry understands which components need to be protected to safeguard Control Centers, Transmission and Generation. There would be a minimum

#	Organization	Yes or No	Question 1.b. Comment
			list developed that must be protected without qualifiers that could be misunderstood. In this regard, it is recommended that the following approach be adopted: BES Cyber System - A BES Cyber System Control Center, Transmission or Generation as defined in Section XX.
60.b	EEI	Disagree	See EEI's suggested wording in 1.a. Alternatively, EEI suggests: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness of the BES.
61.b	Tenaska	Disagree	Should only say: A grouping of one or more BES Cyber System Components. All other qualifiers should be in tables for Medium and High requirements. Careful consideration should be given to the "within 15 minutes" phrase, this time period may be too long or too short depending on the severity of the event, type of cyber asset, or the type of BES entity.
62.b	Madison Gas and Electric Company	Disagree	Suggest replacing the phrase, "cause a Disturbance on the BES, or restrict control and operation of the BES, or affect situational awareness of the BES" with "cause an abnormal BES condition, degrade control and operation of the BES, or degrade situational awareness of the BES." The definition of Disturbance when used in this context is overly broad, for it includes "a perturbation to the electric system" or "the unexpected change in ACE that is caused by the sudden failure of generation or interruption of load." A perturbation to the electric system and a change is ACE are not qualified as to materiality. For example, a responsible entity's programmable device may be used in normal operation to curtail or interrupt relatively small amounts of load; such control of load (even simply for economic reasons) perturbs the electric system and affects ACE to some extent. Yet such effects are part of normal operation of the electric system. In addition, control and operation of the BES are always restricted to some extent; the concern is whether or not control and operation are degraded.

#	Organization	Yes or No	Question 1.b. Comment
			Likewise, the concern is whether or not situational awareness is degraded ("affect" could be in a way that is good or bad). New definition should read: One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause an abnormal BES condition, degrade control and operation of the BES, or degrade situational awareness of the BES.
63.b	ReliabilityFirst Staff	Disagree	Suggest thefollowing definition: "One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could impact realtime operation of the BES such as; cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES."
64.b	Allegheny Energy Supply	Disagree	Suggest: BES Cyber System - One or more BES Cyber System Components, performing one or more functions essential to the reliable operation of the BES, which if unable to perform its function, is misused, or operated by unauthorized personnel, could within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES that could lead to a BES Disturbance, or affect situational awareness of the BES that could lead to a BES disturbance.
65.b	Allegheny Power	Disagree	Suggested alternative definition: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness of the BES.
66.b	SCE&G	Disagree	The 15 minute timeframe should be eliminated. There are too many variables in determining whether a system will have a 15-minute impact.
67.b	APPA Task Force	Disagree	The APPA Task force disagrees with the current definition for similar reasons stated above in regard to 1a. We offer the following simpler definition: “One or more BES Cyber System Components connected via routable protocol, which if rendered unavailable, degraded, compromised, or misused could cause an Adverse Reliability

#	Organization	Yes or No	Question 1.b. Comment
			Impact to the BES, or restrict control and operation of the BES for 30 minutes."See comments to Question 2 for time considerations. If the drafting team does not use this version we at least request that adding "connected via routable protocol" be included in some manner in the definition that is used.
68.b	US Bureau of Reclamation	Disagree	The identification of a BES cyber system based on the 15 minute criteria established here could be difficult to ascertain by those entities that do not directly operate or control the BES. Most entities can determine if it could compromize their respective BES assets. Further, this definition, if it does not establish additional qualifying criteria, would generally establish all Components identified under part 1.a., as Cyber Systems. As an example, an isolated single function cyber-based protective relay would qualify as a BES Cyber System Component under 1.a., but it would also qualify under criteria identified here in 1.b., since it is one or more "components" which could cause a disturbance if compromised - irrespective of the fact that it is not tied to any other components. Was this the intent of the drafting team?
69.b	LADWP	Disagree	The relative nature of the 15 minute criteria. What is the definition of a "Disturbance"?
70.b	Manitoba Hydro	Disagree	The term "misuse" in this definition is inappropriate. The definition misuse n. Improper, unlawful, or incorrect use; misapplication. 1. To use incorrectly. 2. To mistreat or abuse. The misuse of an asset describes the type of human action leading an effect on an asset, while the other terms unavailable, degraded or compromise describe more appropriately the state of the asset. The term misuse might lead into the area where analysis of one asset might cause an effect on another asset which is part of the BES Cyber System Component - secondary effects. Rather than using this approach the drafting team should list the types cyber assets which need consideration. i.e. support systems, HVAC, security, etc.) There may be Cyber system components linked to monitoring and/or network control that may operate periodically that could affect BES with disturbances. If there are any Cyber components that are not continuously or periodically (within 15 minute intervals) monitored for operational status that could either create or incorrectly not mitigate a network disturbance when they are

#	Organization	Yes or No	Question 1.b. Comment
			unavailable, they would not fit into the proposed definition. The definition needs clarification to include reference to all normal modes of operation of the BES Cyber System. For example, a protective relay has normal modes of operation of trip and restrain to trip. The 15 minute "real-time" criterion applies to both the trip and restrain to trip modes of operation. If a digital relay which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes of its trip mode or within 15 minutes of its restrain to trip mode (within 15 minutes of any normal mode of operation), cause or fail to mitigate a Disturbance to the BES, or restrict control and operation of the BES, it is a BES Cyber System.
71.b	American Electric Power	Disagree	The terms "situational awareness" is ambiguous; systems that are not needed for operating the BES, but provide information would be in scope. This definition appears to include items such as all meters, instruments, and transducers.
72.b	Seattle City Light	Disagree	The terms BES condition or Disturbance need to be further defined and clarified.
73.b	LCEC	Disagree	The time frame reference of "Within 15 minutes" could cause a great deal of confusion in identifying BES Cyber Systems. What is the basis for 15 minutes? How will the 15 minute test be audited?
74.b	Ameren	Disagree	The words "A Responsible Entity's" should be added before the words "BES Cyber System Components" to make it clear that this only includes BES Cyber Systems components under the control of the Responsible Entity and specifically excludes entities such as Verizon. The last sentence the term Disturbance is too encompassing. Consider revising for more exact situations. The flow of the definition is difficult to read.
75.b	Matrikon Inc.	Disagree	This definition calls out those cyber systems that affect the BES in some way. During the application of CIP-010-1 there will be the need to classify and label those cyber systems that do not have any impact on the BES. That is the value of keeping the definition "Cyber Asset", because it does not care about the relationship to BES

#	Organization	Yes or No	Question 1.b. Comment
			reliability, only to define the types of electronic systems to be evaluated as part of CIP-010-1 R1. My suggestion is to provide a label/definition for those systems that have no affect on BES, and allow "cyber assets" to remain.My second challenge when trying to apply this definition is how a "component" becomes a "system". The security controls of CIP-011 will be applied to individual cyber assets, and evaluating their individual impact on the BES is of ultimate importance. The need to apply the Impact requirements of CIP-011 appropriately will be satisfied when cyber assets share the same boundary access point, and all will have to inherit/conform to the same, and uppermost security controls criteria.In our CIP-002 definitions, we have defined a "system" as a group of cyber assets performing similar and/or cooperative activities in order to support a function. A similar definition can be used to support BES Cyber System, and the difference from BES Cyber System Component.
76.b	Duke Energy	Disagree	This definition is too broad. The phrase "compromised, or misused" could render compliance an impossibility, since administrators must have access to, and could misuse their access. Also, the phrase "situational awareness" should be clarified to include only that awareness required by System Operators to perform their reliability-related functions. Suggested clarifying change as follows: "One or more BES Cyber System Components which if rendered unavailable or degraded, could, within 15 minutes,: cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES required by System Operators to perform their reliability-related functions." Also, It is not clear if there will be any guidance around how 15 minutes threshold should be measured to ensure that numbers of interpretations for this threshold are limited.
77.b	Midwest ISO	Disagree	We agree that the time frame should be limited to the present but question the use of 15 minutes. Real-Time is a term that is included in the NERC Glossary. Why not use this term?
78.b	Pepco Holdings, Inc. -	Disagree	We appreciate the desire of the SDT to narrow BES Cyber Systems to real-time operations and understand the purpose of including 15 minutes to make that

#	Organization	Yes or No	Question 1.b. Comment
	Affiliates		distinction. We are not sure what the appropriate time frame would be and/or if 15 minutes is the correct time. So a Digital Fault Recorder which is traditionally used for after the fact analysis would not fall within the 15 minute window while and EMS/SCADA system which provides alarms and allows control of the BES would fall within the 15 minute window. Would a system that is compromised with a Trojan months or years ago but no action has been taken yet to compromise the BES meet the 15 minute window. Another possible approach is to list the real-time systems that need to be in-scope or considered.Because there does not seem to be a clear distinction between a BES Cyber System and a BES Cyber System Component, it would seem like a BES Cyber System could qualify as a BES Cyber System Component
79.b	Alliant Energy	Disagree	We believe the definition should be revised to: "One or more BES Cyber System Components which if rendered unavailable, degraded, or compromised could, within an operational time horizon of 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES."
80.b	Independent Electricity System Operator	Disagree	We do not agree with the 15-minute qualifier. Any BES cyber system components that if tampered with can cause a disturbance to the BES or restrict control and operation of the BES, etc. should fall into this category since some components may have an impact on the BES if tampered with by more than 15 minutes before real time. To qualify the components to be only those that affect real time operation, we suggest wording such as "for the current hour and next hour operations" at the end of the sentence. Further, the term "misused" can be subject to a wide range of interpretation, and hence we suggest that it be replaced with "tampered with" or any term that the SDT thinks is more clear and appropriate.
81.b	We Energies	Disagree	We Energies agrees with the EEI Suggested alternative definition with minor modifications: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or

#	Organization	Yes or No	Question 1.b. Comment
			materially disrupt situational awareness of the BES.
82.b	MRO's NERC Standards Review Subcommittee	Disagree	We feel “affect situational awareness of the BES” should be removed, as this is already covered under “operation of the BES”. As written, situational awareness is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for operation of the BES. We also feel “misused” should be removed, as this is already covered under “compromised”.As currently worded, we also believe the intent of the 15 minute time frame is ambiguous. We would propose incorporating what we believe to be the drafting team’s true intent directly in to the definition, along with our other suggestions, as follows: One or more BES Cyber System Components which if rendered unavailable, degraded, or compromised could, within an operational time horizon of 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES.
83.b	IRC Standards Review Committee	Disagree	We question the technical basis for a 15 minute time frame applied to any component that may cause a “Disturbance” to the BES. Without careful understanding of how the failure of the component could impact the BES 15 minutes may be too long or too short a time frame to allow recovery of the component or enable a mitigation solution. Further, we disagree that the disabling or degradation of any BES Cyber System Component would cause a “Disturbance” that is of significance to the integrity of the interconnected BES. To qualify the components to be only those that affect real-time operation reliability, we suggest wording such as “for the current hour and next hour operations” at the end of the sentence.The term “misused” can be subject to a wide range of interpretation, and hence we suggest that it be replaced with "tampered with" or any term that the SDT thinks is more clear and appropriate.
84.b	Southern Company	Disagree	We recommend the following definition: A system performing one or more BES functions identified in CIP-010 Attachment 1 and which if rendered unavailable, degraded, compromised, or misused would, within 15 minutes, adversely impact the real-time operational control of the BES.

#	Organization	Yes or No	Question 1.b. Comment
85.b	Covanta Energy	Disagree	Without a clear understanding of why '15 minutes' is the defined measure, it is difficult to support the definition.
86.b	Verizon Business	Agree	The “15 minute” criterion should be expanded in writing by the drafting team to provide a better sense of when the time starts. This could be done in an associated guideline or “Frequently Asked Question”

1.c. Control Center — A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,
- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations,
- BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES),
- Alarm monitoring and processing specific to operation and restoration function, or
- Coordination of BES restoration activities.

Summary Consideration:

Many entities expressed concerns that the proposed definition of Control Center was too broad and could include various types of facilities not commonly considered control centers. Others questioned whether a Control Center should be defined as a collection of systems versus a physical facility housing such systems. Many entities indicated that the definition should be restricted to the functions of Reliability Coordinator, Balancing Authority, or Transmission Operator. Some expressed concerns about including situational awareness in the definition.

The SDT has modified the definition of Control Center to clarify that it is one or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more functions that support System Operators in the real-time operation of the BES. In consideration of the possible configurations where multiple locations may host such systems, the SDT used 'one or more' facilities. The SDT declined to limit the definition to of Control Center to facilities operated by RCs, BAs, or TOPs, since there are Control Centers operated by TOs and GOs/GOPs as well that must be protected.

The revised definition of **Control Center** is as follows:

One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations:

- *Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,*

- *Inter-utility exchange of BES reliability or operability data,*
- *Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES,*
- *Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function,*
- *Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES*
- *Coordination of BES restoration activities.*

#	Organization	Yes or No	Question 1.c. Comment
1.c	BCTC		BCTC recommends the following aspects of this definition be revisited:Â Recommend the first bullet point be broken into three:ï‚§ Supervisory Controlï‚§ AGCï‚§ Automatic Load SheddingÂ Recommend that the functions be categorized as "mandatory" for defining a facility as a control centre. These would include:ï‚§ Supervisory controlï‚§ BES and system status monitoringï‚§ Alarm monitoringï‚§ Coordination of BES restoration activitiesÂ To be considered a control centre the facility should have "two or more" of the functions listedÂ Remove "or" and replace with "and"Â For BES restoration a Utility may have workstations at an alternate site that by our everyday definition is not considered a control centre (i.e. alternate office building); how would these be classified within this definition? One of the questions we struggled with when looking as this definition was how to define a facility based on the number of RTUs present within them (i.e. one versus many) ... any advice?
2.c	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group		With no metrics defining anything upfront, it is possible to include applicability to very small entities. Control of two or more BES generation or Transmission Facilities with a combined historical demand of less than 500 MW should not be included in this definition. At some point, a defining line needs to be established to effectively define the bounds of the BES "castle" where defense of BES reliability is cost effective. Adding undue BES reliability compliance burdens on smaller DP/LSEs will ultimately add no BES reliability, and will hurt local distribution reliability efforts. If 500 MW is too large, then a conservative value can be agreed to and later revised as engineering studies become

#	Organization	Yes or No	Question 1.c. Comment
			available to justify a larger value.If that cell phone from 1.a. receives alarms from two or more locations and is used to make real time decisions it becomes a Control Center although it performs no control function and is not a center. Suggest that a Control Center be defined as a fixed server location.From the workshop, we realize that the lines separating the Component from the System and from the Center were intended to be flexible and up to the entity to consider system designs. The standard, however, does not read that way. We are concerned that based on the written standard the REs will not allow flexibility or even lines. All BES cyber devices, including every BES alarm displaying cell phone will be cast into all three buckets.
3.c	Dynegy Inc.	Agree with proposed definition	I agree but request additional detail examples be provided to determine specifically what these items are.
4.c	Southern California Edison Company	Agree with proposed definition	SCE requests clarification on systems and components that: (1) facilitate inter-utility exchange; and (2) devices that enable system status monitoring. Would devices such as email systems used for messaging and IP telephony systems in facilities be considered a "control center" or a BES Cyber System? The drafting team should issue guidelines on systems that directly perform BES reliability functions and systems/devices that are used by human operators for feedback prior to the manipulation of cyber components that directly impact the BES. It would also be beneficial for telecommunications equipment, which support a BES Critical Cyber system, be applicable only to COM-001 R2. If the intent of the drafting team is to limit the scope of cyber security controls to systems where real time BES impact is caused by direct human supervisory control over devices and systems, it should be clearly stated as such.
5.c	FEUS	Agree with proposed definition	What would it be considered if it only performed one function for a single BES facility at a single location? It would not be a control center.

#	Organization	Yes or No	Question 1.c. Comment
6.c	Minnesota Power	Agree with proposed definition	While Minnesota Power generally agrees with the proposed definition, it recommends that "(i.e., two or more)" be removed from the definition.
7.c	National Grid	Disagree with proposed definition	1. A control center is usually considered as a physical place with operators using various tools like EMS. The definition implies that a control center is a cyber asset. Isn't the Control Center much more than that? Maybe SDT is trying to define a "Control Center Cyber Asset". If so then SDT should use the term Control Center Cyber Asset. 2. National Grid seeks clarification on "Reliability" or Operability Data" since they can be subject to interpretation. 3. In bullet 3, the asset management piece should not be included. Also, if bullet 3 is indicating statuses like breaker status, then it is not required since it is covered in the preceding bullet. If not, then this should be better defined. 4. In bullet 4, there is no need to include "restoration function" as this is included in "operation" 5. In bullet 5, operators "coordinate" the BES restoration activities and not the cyber systems.
8.c	Progress Energy (non-Nuclear)	Disagree with proposed definition	1. From the definition, the ECC, DCC and the back-up control facilities would definitely be included. A substation that has a LAN connecting several cyber components would not be included. 2. Is a single generating facility the same as a single generating plant? Is a single generating plant a generating unit or a collection of generating units at 1 physical plant site? Clarify that a generating station control room is not a control center. 3. We need to be careful with definition of supervisory control as one possible interpretation of what the control room operator does is supervise the distributed control platforms that make up the plant control system. 4. These systems are independent only controlling one at a time. The key word here is "multiple". Control rooms at some generation plants house multiple DCS systems. But, by design, each DCS controls its respective unit independently and are considered separate entities. I do not think this example would qualify as a Control Center. We can agree with this concept if they are talking about large regional control like the PJM interconnect or an ECC which it sounds like and NOT plant level Control Rooms. 5. A Control Center would operate

#	Organization	Yes or No	Question 1.c. Comment
			multiple generating Units with one control system.
9.c	Consultant	Disagree with proposed definition	1. The definition should identify that the "set of one or more BES Cyber Systems capable of performing..." are at a single location. If there are multiple locations where this capability exists then each location should be identified as a Control Center. 2. As stated, the definition creates a Control Center at every location where the capability "exists", whether this is a normal operation for each of those locations or is an emergency capability of each of those locations. If that is not the intent of the definition, then the distinction between normal and emergency (backup, off-normal) operations should be included in the definiton.
10.c	Progress Energy - Nuclear Generation	Disagree with proposed definition	A control center at a nuclear facility is different than this definition. I do not belive it is intended to apply to nuclear generation facilities, but rather the energy control centers that supervise bulk power loading functions.
11.c	Dairyland Power Cooperative	Disagree with proposed definition	A control center sound intuitively like a type of facility, but here is used as a term for a system(s) affecting multiple facilities. This will be confusing terminology.
12.c	Indeck Energy Services, Inc	Disagree with proposed definition	A control system that monitors through read-only access should not be categorized as a Control Center under CIP-010. A load aggregator is not identified as a potential Control Center.
13.c	Nuclear Energy Institute	Disagree with proposed definition	Agree with the exception that: The term “multiple locations” should be clarified to “multiple geographically distinct locations” to preclude confusion with a single facility with multiple generating units from being inappropriately identified as a control center.

#	Organization	Yes or No	Question 1.c. Comment
14.c	Alliant Energy	Disagree with proposed definition	Alliant Energy agrees with the EEI comments.
15.c	Pacific Gas & Electric Company	Disagree with proposed definition	Appears that under this definition of Control Center, several BES Cyber Systems or Components would be considered Control Centers such as:Distributed EMS or SCADA front-end processors Transfer Trip Protection Systems located at a specific substation control house that control other subs and/or generationSpecial Protection Schemes that control devices at multiple substations.Don't disagree on the importance of the items above to BES, just that defining them as a Control Center likely will lead to confusion.
16.c	City Utilities of Springfield, Missouri	Disagree with proposed definition	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
17.c	Ameren	Disagree with proposed definition	Clarify the definition to explain if it covers Power Plant control rooms, or if this is limited to transmission dispatching. Please clarify if “locations” refers to physical or electrical locations. Does “generation plants” refer to a Power Plant or generation “Facility” as defined by NERC; there use of plant vs. Facility is inconsistent. The definition appears to automatically cover all plant control rooms for any generator that see’s or controls the switchyard, is this the intent? In the third bullet, the term “and asset management” needs to be removed. As currently written, the inclusion of this term improperly suggests that facilities used for commercial and market purposes are covered by this definition.The definition of Control Center should only include those facilities where NERC certified operators are required for its operation.
18.c	CenterPoint Energy	Disagree with	Disagree - Control Center is a common industry term that often refers to a physical location. It should not be redefined under the CIP standards and should be deleted.

#	Organization	Yes or No	Question 1.c. Comment
		proposed definition	However, if the SDT feels a strong need to include this definition CenterPoint Energy suggest the following: A set of one multiple (i.e. two or more) BES Cyber Systems, located together at the same physical location, capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations: o Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, o Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations, o BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES), o Alarm monitoring and processing specific to operation and restoration function, or o Coordination of BES restoration activities.
19.c	Tenaska	Disagree with proposed definition	Display and Inter-utility should be left out. Just display of will not hurt the reliability of the BES (PI data). Loss of inter-utility data need to have an N-11 type requirement with it. The loss of some percentage of data is tolerated in normal operation every day. The EMS/SCADA accounts for bad data. Consider using the definitions for Reliability Coordinator and Balancing Authority for clarity.
20.c	E.ON U.S.	Disagree with proposed definition	E.ON U.S. does not believe that the "display of BES reliability or operability data for the support of real-time operations" alone should qualify a locale as a control center. For example, view only information is often made available to plant operators Does "Alarm Monitoring" in the Control Center definition include sending alarms to remote ends of a transmission line from a substation? For example, carrier check-back and breaker failures. In addition how is transfer trip being addressed.?
21.c	Southern Company	Disagree with proposed	EOP-008, which is focused on control centers and control center functionality, does not contain or need a definition of the term. This implies that the CIP standards may not require a definition, either, and that any definition which is constructed must be done in light of the contents of EOP-008.If a definition is needed, we recommend the following

#	Organization	Yes or No	Question 1.c. Comment
		definition	definition:A location where one or more BES Cyber Systems are used to perform BA, RC, or TOP functions for generation Facilities or Transmission Facilities at multiple locations.If, for some reason, the existing definition must be modified, the following factors should be taken into consideration:Definition of Control Center - its our understanding that the Control Center definition is to be used to scope requirements based on 'environmental' factors and to differentiate it from generating plants and substations (field locations). So Control Center 'environment' is a 'data center' environment consisting of mostly traditional servers and workstations, Generation environment was a campus, plant type environment, and Transmission is an environment with unmanned field locations and mostly purpose built devices. These environments are then used to scope requirements appropriately based on the types of devices and the physical environment prevalent in that situation. The current definition of control center will pull in devices and systems from all the above environments and loses what we considered was the reason the environments were created and defined.For bullet 2...This clause pulls in far more facilities than are either intended or generally thought of as control centers. Things that would qualify: o An unattended remote data acquisition node o A standalone ICCP server feeding data to neighboring utilities o An RTU receiving data from multiple generating unitsThe definition should be modified to require multiple functions for a facility to qualify as a Control Center, and the second bullet, which includes many facilities which are not actually Control Centers and which does not add any additional facilities which should be considered as Control Centers, should be removed.In general, and in particular on bullet 4, processing is not a function of a control center; it's a function of the underlying cyber systems. The actual alarm monitoring, for example, is the key piece, and the wording about "processing" should be removed.For bullet 5...The fluid nature of disaster recovery makes this one worrisome. A makeshift command center set up in the wake of a natural disaster would qualify, even if all they had were laptops with no external network connection, creating some difficult access tracking issues. In general, the inclusion of BES restoration, if necessary, will need to be bounded carefully - one solution would be include the phrase "BES restoration specific to situational awareness".In addition, there are concerns about

#	Organization	Yes or No	Question 1.c. Comment
			small hydro units which can send control signals to other small hydro units being classified as control center locations.
22.c	Oncor Electric Delivery LLC	Disagree with proposed definition	Exclude "display" of data. Inclusion would allow an auditor to assess that the simple display of Responsive Reserve in an office constitutes a "control center".
23.c	Southwestern Power Administration	Disagree with proposed definition	For the purpose of this standard it would be clearer if the definition would just identify what NERC functions are performed in the control center environment. This will also lessen the chance for confusion going forward with non-CIP reliability standards usage of the term "Control Center". BES Control Center - A site where personnel can perform one or more of the following functions:Reliability CoordinatorBalancing AuthorityTransmission Operator
24.c	USACE HQ	Disagree with proposed definition	Given that Control Center is based on the definition of BES Cyber System Components and BES Cyber System, which I disagree with both, I must also disagree with this one.
25.c	Edison Mission Marketing and Trading	Disagree with proposed definition	I don't agree that status and alarm monitoring has anything to do with relaibility
26.c	San Diego Gas and Electric Co.	Disagree with proposed definition	If an asset to be evaluated for Control Center status is only one BES Cyber System, it does not seem to meet the definition of "a set". Therefore, SDG&E suggests that the first sentence of the definition should be changed to read "One or more BES Cyber Systems capable of ..."Is a control center appropriately defined as one or more "BES Cyber Systems capable of performing...", or would is it more appropriately defined as "A location where one or more BES Cyber Systems are monitored for proper performance

#	Organization	Yes or No	Question 1.c. Comment
			of one or more of the following functions (i.e., two or more)…"Why is control of two or more facilities required for this definition? How does a backup control center factor into this definition? In the past, the "two or more facilities" piece was part of the differentiation between a control room and a control center, but we don't see a definition of "control room" in this draft.
27.c	Dominion Resources Services, Inc.	Disagree with proposed definition	It is not clear whether the control center is the aggregate of the BES Cyber Systems or the physical space containing them. There is ambiguity as to whether the last phrase (at multiple…) belongs to the set of BES Cyber Systems or to the multiple facilities. Other definitions are of the form that "if it does this" then it is "this". It should be clarified that the presence of one or more of these functions does not make it a Control Center. For example, using a conference room or field office to direct BES restoration activities during an emergency does not make that conference room or field office a Control Center. The term should be limited to only those physical spaces used by a Balancing Authority, Reliability Coordinator and/or Transmission Operator in the performance of real-time functions, since these are the 3 entities charged with overall reliability functions for the BES. Dominion proposes the following definition of a Control Center: Control Center - The space where a Balancing Authority, Reliability Coordinator and/or Transmission Operator uses one or more BES Cyber Systems to perform one or more of the following functions for two or more geographically dispersed BES Generation or Transmission Facilities: o Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, o Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations, o BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES), o Alarm monitoring and processing specific to operation and restoration function, or o Coordination of BES restoration activities.

#	Organization	Yes or No	Question 1.c. Comment
28.c	Emerson Process Management	Disagree with proposed definition	It is very unclear how this term could be interpred for typical power generation plants. Very rarely, multiple generation facilities at different locations will be controlled under one physical control center. Control systems and control rooms are mostly located at the same place with the generation units.So, the term of Control Center in this standard may be totally inapplicable to BES generation facilities or entities.
29.c	Liberty Electric Power, LLC	Disagree with proposed definition	Many generation plants are not part of the current definition of BES. This standard is not the correct place to redefine BES, and any language which does so will force "No" votes on the standard, regardless of the merits of the rest of the document.
30.c	MidAmerican Energy Company	Disagree with proposed definition	MidAmerican Energy agrees with EEI's suggested modification to “Alarm monitoring” below:BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
31.c	Public Service Enterprise Group companies	Disagree with proposed definition	Mostly agree with the definition. However, the applicability of the first qualifier “(i.e., two or more)” is not clear. Does the qualifier apply to only “BES generation Facilities” or to “BES generation Facilities or Transmission Facilities”? Please clarify the language.
32.c	Regulatory Compliance	Disagree with proposed definition	Please clarify - for any control room at a generating facility that can remotely operate another site, whether or not it would be classified as a control center.
33.c	MWDSC	Disagree with proposed definition	Proposed definition conflicts with industry understanding and potentially with other standards. Attachment II assumes a Control Center is not just a collection of BES Cyber Systems gathering data, but rather a 24/7 facility staffed with certified power operators who take appropriate actions. Someone has to make decisions using the information being sent over cyber systems. Suggest changing definition as follows:"Control Center -

#	Organization	Yes or No	Question 1.c. Comment
			A facility staffed by a Transmission Operator, Generator Operator, or Balancing Authority who makes decisions based on information received from a set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations.
34.c	Con Edison of New York	Disagree with proposed definition	Regarding the definition of Control Center, as written, it appears that any facility can be deemed a Control Center. If a Transmission, Generation or other facility has a BES Cyber System that controls more than 1 generation or transmission facility it would be a Control Center. If so, this may be conflicting when addressing CIP-011-1 requirements that distinguish between Control Center and other facilities. This may also cause a transmission station that is connected to a generating station to be a Control Center if the station has an RTU cyber asset (with or maybe without an HMI) that can trip all station breakers (impacting the transmission station) and thereby trip the generator (impacting the generating station).
35.c	Wolverine Power	Disagree with proposed definition	See comments listed for 1.a
36.c	EEI	Disagree with proposed definition	See EEI's suggested wording in 1.a. Alternatively, EEI suggests:A modification to "Alarm monitoring":BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
37.c	WECC	Disagree with proposed definition	Seems to define the control center to try and exclude control rooms that only affect local facilities. Suggest rewriting to scope all bulleted functions performed inside a single location and EXCLUDING locations that only affect location facility operation.Based on the previously defined term "BES Cyber Systems" it is redundant to characterize a Control Center as a "set of one or more."The following rewrite is

#	Organization	Yes or No	Question 1.c. Comment
			proposed;Control Center - A facility used to implement a BES Cyber System(s) to perform one or more of the following functions for BES Generation Facilities, BES Transmission Facilities, and/or Distribution Facilities located at two or more locations: o Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, o Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations, o BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES), o Alarm monitoring and processing specific to operation and restoration function, or o Coordination of BES restoration activities.Distribution is included in this suggested rewrite based on its inclusion in the Applicability List as “Distribution Provider.”
38.c	Madison Gas and Electric Company	Disagree with proposed definition	Suggest removing the comma after "Transmission Facilities." With the comma, the subsequent phrase, "at multiple (i.e., two or more) locations," could be interpreted to apply to "one or more BES Cyber Systems" rather than BES Generation or Transmission Facilities.The term "location" is ambiguous in the context of the definition. For example, multiple generators at the same generating plant are placed in multiple locations (unless they impossibly occupy the same physical space). The intent of the qualification "at multiple locations" seems to be to exclude generating plant control systems, yet the definition could be read to potentially include generating plant control systems as Control Centers. Recommend modifying the definition to provide more specificity.Similar to the definition of BES Cyber System, the definition of Control Center does not provide criteria for aggregating BES Cyber Systems to define the "set of one or more BES Cyber Systems" that comprise a Control Center.New definition should read:Control Center - A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

#	Organization	Yes or No	Question 1.c. Comment
39.c	Entergy	Disagree with proposed definition	Suggest: A) Changing definition to speak specifically to "Functions" in Attachment I; and delete "for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations." B) Delete all bullets and rely on list of Functions as sole qualifiers. C) Note: close scrutiny of this definition is needed relative to EOP-008 (Project 2006-04: Backup Facilities; nearing final ballot) to avoid conclusion.
40.c	Green Country Energy	Disagree with proposed definition	Suggested definition:Control Center - A set of one or more BES Cyber Systems capable of performing one or more of the following functions at two or more BES generation Facilities, or Transmission Facilities at two or more locations:
41.c	Allegheny Power	Disagree with proposed definition	Suggested modification to "Alarm monitoring" o BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
42.c	Allegheny Energy Supply	Disagree with proposed definition	Suggested modification to "Alarm monitoring"- BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
43.c	Constellation Power Source Generation	Disagree with proposed definition	The "Acquisition, aggregation, processing..." function that a Generation Management System (GMS) or a marketing system would fall under scope of a "control center" though it would make more sense (in reliability terms) for it to be just a BES cyber system. A clarifying statement is needed to exclude marketing and GMS systems from this control center definition. The definition of control center is too broad in only requiring performance of one of the functions to meet the definition. A control center is commonly understood to be a location, not a system, where at least 4 of the 5 functions are performed, if not all 5 functions. This definition eliminated the concept of a control center as a defined space with operating systems and instead identifies a control center

#	Organization	Yes or No	Question 1.c. Comment
			as cyber systems which pull in work spaces that should not be in scope.
44.c	APPA Task Force	Disagree with proposed definition	The APPA Task force is concerned that under the proposed definition, a substation control room could be considered a "Control Center." Therefore, we offer the following clarification for your consideration:"A set of one or more BES Cyber Systems at centralized, primary or back-up locations that enable centralized operation of a Reliability Coordinator, Balancing Authority or Transmission Operator."
45.c	Xcel Energy	Disagree with proposed definition	The definition needs to clarify that it applies to interconnected control systems. For example, two independent control systems with no interdependency that operate generation units at separate locations should not be defined as a control center.
46.c	Constellation Energy Control and Dispatch, LLC	Disagree with proposed definition	The definition of Control Center is too broad in only requiring performance of one of the functions to meet the definition. A Control Center is commonly understood to be a location not a system, where at least four of the five functions are performed, if not all. This definition eliminates the concept of a control center as a defined space with operating systems and instead identifies a control center as systems which would pull in work spaces that should not be considered Control Centers. Remove AGC Systems from function 1. Automatic Generation Control is defined to be Equipment (not a system) that automatically adjusts generation in a Balancing Authority from a central location to maintain the BAs interchange schedule plus Frequency Bias. The Equipment that automatically adjust generation is located at the generation site not in the Control Center. The Control Center EMS has the ability to send a signal to a generator, but not to automatically adjust the generation. Rather the generator is set up to pick up the signal in a central control system at the site and use the signal to change its operating level with in established operating parameters in accordance with established capability. The definition of Control Center should focus on the systems in a Control Center that can actually automatically operate equipment, i.e. Supervisory control of BES assets at generating plants, transmission facilities and substations is a sufficient description of these type of Control Center functions.Remove asset management from function 3.

#	Organization	Yes or No	Question 1.c. Comment
			Unless this term is defined to narrow the scope as related to Control Center functions, this term is loosely used in the industry and would result in too broad of an application of this function.It may be worth including a data acquisition timing reference to appropriately narrow the scope as well. Control Centers are processing data in terms of cycles or seconds and many of the function described may be performed by systems using longer intervals and these longer interval systems should not be pulled into the definition.
47.c	Constellation Energy Commodities Group Inc.	Disagree with proposed definition	The definition of... "capable of performing one or more..." should be changed to "capable of performing four or more..."The definition of Control Center is too broad in only requiring performance of one of the functions to meet the definition. A Control Center is commonly understood to be a location not a system, where at least four of the five functions are performed, if not all. This definition eliminates the concept of a control center as a defined space with operating systems and instead identifies a control center as systems, which would pull in work spaces that should not be considered Control Centers. Remove AGC Systems from function 1. Automatic Generation Control is defined to be Equipment (not a system) that automatically adjusts generation in a Balancing Authority from a central location to maintain the BAs interchange schedule plus Frequency Bias. The Equipment that automatically adjusts generation is located at the generation site not in the Control Center. The Control Center EMS has the ability to send a signal to a generator, but not to automatically adjust the generation. Rather the generator is set up to pick up the signal in a central control system at the site and use the signal to change its operating level within established operating parameters in accordance with established capability. The definition of Control Center should focus on the systems in a Control Center that can actually automatically operate equipment, i.e. Supervisory control of BES assets at generating plants, transmission facilities and substations is a sufficient description of these types of Control Center functions.Remove asset management from function 3. Unless this term is defined to narrow the scope as related to Control Center functions, this term is loosely used in the industry and would result in too broad of an application of this function.It may be worth including a data acquisition timing reference to appropriately narrow the scope as well. Control Centers

#	Organization	Yes or No	Question 1.c. Comment
			are processing data in terms of cycles or seconds and many of the function described may be performed by systems using longer intervals and these longer interval systems should not be pulled into the definition.Typically, BES restoration processes are coordinated with manual processes, and are not Cyber System related.
48.c	Platte River Power Authority	Disagree with proposed definition	The function"BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES)," doesn't clearly represent the real-time nature of the function. "System" is already included in BES. Suggested revision:BES real-time status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES),
49.c	CWLP Electric Transmission, Distribution and Operations Department	Disagree with proposed definition	The last two bullet points should be removed. The first is redundant and the last muddies the concept of control center. Restoration activities could be coordinated from a bucket truck or a temporary command center. These functions are actually human interactions not cyber systems.
50.c	US Bureau of Reclamation	Disagree with proposed definition	The term "BES asset" is not defined. The requirement should either propose a definition or the language in the requirement should be modified to refer to "BES Facilities" both of which are defined in the NERC Glossary of Terms.
51.c	LCEC	Disagree with proposed definition	The term "locations" needs to be defined. Should the human/machine interface be considered in defining a control center? Ensure that control rooms are not considered as control centers per this definition.
52.c	Southwest Power Pool Regional Entity	Disagree with	The use of "multiple (i.e., two or more)" twice in the same sentence is confusing. Consider changing the definition to read "A set of one or more BES Cyber Systems

#	Organization	Yes or No	Question 1.c. Comment
		proposed definition	capable of performing one or more of the following functions for multiple (i.e., two or more) geographically disperse BES generation Facilities or Transmission Facilities:"
53.c	Hydro One	Disagree with proposed definition	There is a gap regarding centralized configuration of BES Cyber Systems. The current definition of control center does not include a centralized system used for maintaining or configuring remote equipment such as RTUs or relays.Based on the control centre proposed definition all hub sites would be deemed within the definition of control centers. We would like the clarification if the auxiliary systems (High pressure air systems, cable temperature monitoring, QFW sag monitoring, DC inverters, PLCs, substations WANs, teleprotections, synchrophasors etc.) would be considered as BES Cyber System Components. As proposed, this definition would have massive implications to Hydro One in terms of implementation, capital cost, OM&A expenses etc.
54.c	Northeast Power Coordinating Council	Disagree with proposed definition	There is a gap regarding centralized configuration of BES Cyber Systems. The current definition of control center does not include a centralized system used for maintaining or configuring remote equipment such as RTUs or relays.
55.c	Bonneville Power Administration	Disagree with proposed definition	Third bullet should make it more clear that only real-time management (control and operation) is relevant. The example is for real time control; changing "e.g." to "i.e" would be sufficient. In addition, the way the definition is written it is possible that a substation could end up being identified as a Control Center. The definition needs to be clear that these are facilities whose prime purpose is to be control centers, not just substations that happen to have information covering other substations, or even possibly the ability to exercise some control over another substation.
56.c	Exelon Corporation	Disagree with proposed	This definition does not align with the commonly understood definition of control center and could be interpreted to apply to multiple unmanned locations housing servers.

#	Organization	Yes or No	Question 1.c. Comment
		definition	
57.c	NextEra Energy Corporate Compliance	Disagree with proposed definition	This definition needs to be more specific. NextEra suggest removing "capable" in the first line and removing or better defining "coordination" and "restore BES activities." NextEra also recommends defining control center as having the "Primary function."NextEra also suggests being clear on whether remote Control Centers are included, and, if so, CIP-011 needs to be very clear on any differences in the protection of remote control centers versus primary control centers. NextEra will be providing additional comments in the future.
58.c	Reliability & Compliance Group	Disagree with proposed definition	This definition seems to include control room as a Control Center. Does this mean a control room can be considered as a control center? Normally a Control Center requires having real time operation functions. The way it is stated above if you meet one of the last two functions, it is qualifies as a control center
59.c	Duke Energy	Disagree with proposed definition	This definition should be revised to clarify that a Control Center only includes facilities required to be staffed by NERC-certified operators. The revised definition should explicitly clarify that the term Control Center does not include the control room for a multiple generating unit site. Also, the use of the capitalized term "Facilities" continually causes confusion during audits, because, as the term is defined, even a single generating unit site could contain multiple "Facilities" (e.g. a line, a generator, a shunt compensator, transformer, etc.)Also, the phrase "capable of" is open to interpretation, and should be replaced with the phrase "operationally responsible for". Also, the phrase "for the support of" in the second bullet is open to interpretation, and should be replaced with the phrase "essential to".
60.c	Old Dominion Electric Cooperative	Disagree with proposed definition	This seems to widen the definition of control center to the point of being overreaching.

#	Organization	Yes or No	Question 1.c. Comment
61.c	Pepco Holdings, Inc. - Affiliates	Disagree with proposed definition	We agree with EEI's comments. Do transmission facilities include substations or does it reference just the transmission line components?
62.c	FirstEnergy Corporation	Disagree with proposed definition	We are unclear why 'control center' is being redefined as a logical set of cyber systems rather than a physical site which accommodates the functions traditionally identified with control centers. This definition appears to align with legacy architectures, where the control center serves as a communications hub and data center, thus creating a single point of failure. Modern architectures that employ best practices for reliability, redundancy, and diversity do not employ that structure. Since this is a significant departure from the commonly understood definition of 'control center', it is unclear how this definition will impact compliance to the newly proposed standards.
63.c	GTC & GSOC	Disagree with proposed definition	We do not agree with this definition. We believe that it will capture a large number of systems that are not part of what is commonly understood to be a control center. For example, an RTU acting as a data concentrator acquires data from multiple locations and supports real-time operations, but is not itself a control center. In addition, the term "BES assets" is an artifact of the version 1, 2, and 3 CIP standards and should either be replaced or clarified. More basically, though, we question the need for this definition. Its primary function appears to be as a scoping criterion for CIP-011 in the same manner that generation [sic] Facility and Transmission Facility are. However, the SDT did not feel the need to define either of those terms. We recommend that this definition may be better suited for a guidance document.
64.c	We Energies	Disagree with proposed definition	We Energies agrees with EEI Suggested modification to "Alarm monitoring" with minor modifications: o BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or Suggested modification to "Acquisition" bullet o Acquisition, aggregation, processing, inter-utility exchange or display of BES reliability or operability data for the support of real-time BES operations.

#	Organization	Yes or No	Question 1.c. Comment
65.c	Independent Electricity System Operator	Disagree with proposed definition	We generally agree with the description in the definition, but do not agree with the term “control centre” as it confuses with the traditional control centre of BES operations. We suggest the term be changed, for example, to “BES Cyber Cluster”, or “BES Cyber Control Cluster”.
66.c	IRC Standards Review Committee	Disagree with proposed definition	We generally agree with the description in the definition, but do not agree with the term “control centre” as it confuses with the traditional control centre of BES operations. We suggest the term be changed, for example, to “BES Cyber Cluster”, or “BES Cyber Control Cluster” or “BES Control System”.
67.c	Midwest ISO	Disagree with proposed definition	What is really being described is a control system and not a control center. A control center implies physical attributes that are not described in this definition. We suggest to modify the definition to control system rather than control center.
68.c	Florida Municipal Power Agency	Disagree with proposed definition	With this definition, a substation control room can be a “Control Center”. A Control Center has other characteristics associated with it that make it a control center, i.e., “centralized operation”, the reverse of the term. FMPA suggests a simpler definition:”A set of one or more BES Cyber Systems at centralized, primary or back-up locations that enable centralized operation of a Reliability Coordinator, Balancing Authority or Transmission Operator.”

2. **The definition of BES Cyber System limits the scope of the definition and the applicability of CIP-010-1 (and CIP-011-1) to real-time operations systems with an operational time horizon of 15 minutes. Do you agree with this scope of applicability? If not, please explain why and provide specific suggestions for improvement.**

Summary Consideration:

While there was general agreement with scoping the applicability of the standards to "real-time" systems, many entities questioned the source of 15 minutes as the scoping time. Some commenters expressed concerns about the auditability of this qualification in defining the scope of applicability.

In selecting the 15-minutewindow, the SDT reviewed various reliability standards and identified two widely used time horizons: 30 minutes and 15 minutes. The intent of the SDT is to include those systems that impact "real-time" operation of the BES. The SDT used a 15-minute window to qualify the "real-time" nature of the impact and felt that a 30-minute window would include those systems that might not be considered as "real-time".

The proposed definition of a **BES Cyber System** has been revised as follows:

One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.

#	Organization	Yes or No	Question 2 Comment
2.1	USACE HQ		I disagree with the scope and disagree with expanding the scope. The use of a time limit to represent real-time should not be present given that is lacking documentation support for the number. Either introduce a definition for real time for CIP purposes or provide support for the risk-informed dentition of using 15 minutes as the limit
2.2	Arizona Public Service Company		The 15-minute criteria specified as part of the definition of a BES Cyber System may both lead to confusion and/or act as a loophole to exclude BES Cyber System Components from further consideration. Confusion may be caused by likely differing interpretations of "restrict control and operation of the BES, or affect situational awareness of the BES". Without more specific definitions, each Entity may utilize different criteria for determining whether control and operation has been 'restricted' or whether situational awareness has been 'affected'. Such potential ambiguity may also allow Entities to utilize

#	Organization	Yes or No	Question 2 Comment
			excess discretion in this determination in order to 'exclude' Cyber System Components from categorization. A suggestion would be to attempt to avoid such vague terms if a timeline is specified in the definition at all, or to avoid a timeline in the definition and add time windows to the Impact Categorizations. Examples of terminology changes include using the term 'impede' rather than 'restrict' (as some restriction may be tolerable, but impede strengthens the concept being conveyed) or using the phrase 'impact operational decision making' rather than 'affect situational awareness' (as such a phrase might be less likely to be misinterpreted outside of Power Operations expertise).
2.3	Nuclear Energy Institute	Agree with scope	A recommended change to BES Cyber System Component has been proposed to clarify that the intent is to protect real-time operations. NEI recommends examples of systems that would fall in and outside this scope.
2.4	US Army Corps of Engineers, Omaha Distirc	Agree with scope	Agree with limiting scope to real-time systems with an operational time horizon of 15 minutes. However the wording of the definition needs to be strengthened because the intended meaning of the definition as "real-time" systems with an operational time horizon of 15 minutes" was not clear until.
2.5	Entergy	Agree with scope	Agree with scope limitation to "real-time operations." Suggest: Rule 706 be carefully reviewed to assure this is not countervailing to FERC directives; their directives suggest a broader scope of applicability.
2.6	Allegheny Power	Agree with scope	Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.7	EEI	Agree with	Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be

#	Organization	Yes or No	Question 2 Comment
		scope	appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.8	MWDSC	Agree with scope	Also need to identify who makes the real-time operational decisions, i.e., Transmission or Generator Operator or Balancing Authority. See suggested changes in comments to question 1.b.
2.9	City Utilities of Springfield, Missouri	Agree with scope	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
2.10	Dominion Resources Services, Inc.	Agree with scope	Dominion supports the inclusion of "within 15 minutes". It is important to establish a reasonable boundary condition for the real-time or near real-time effects of the BES Cyber System and 15 minutes provides adequate time for the effects to be mitigated to prevent further harm to the BES.
2.11	Southwest Power Pool Regional Entity	Agree with scope	Entities today eliminate assets from the Critical Asset list because they assume a mitigation to a voltage instability or thermal overload is available and will always be successful. Consider modifying the definition to read "...could, if not mitigated within 15 minutes,..."
2.12	Southwestern Power Administration	Agree with scope	Fifteen minutes seems to be a reasonable operational horizon, but should the language be modified in such a way to allow for an operational time horizon of approximately 15 minutes in order to discourage "clock watching" by entities and/or auditors to reach a conclusion of either fourteen or sixteen minutes.
2.13	Platte River Power Authority	Agree with scope	I agree so long as the BES Cyber System definition is updated to more clearly explain the horizon. For example:BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within an

#	Organization	Yes or No	Question 2 Comment
			operational time horizon of 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.
2.14	MidAmerican Energy Company	Agree with scope	MidAmerican Energy agrees with EEI's affirmation below:Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.15	Progress Energy (non-Nuclear)	Agree with scope	See comment for question 1b.
2.16	APPA Task Force	Agree with scope	The APPA Task force agrees with the proposed definition, but offers the following suggestions:It seems that the 15 minute horizon is arbitrary. We suggest aligning the time to an already determined time limit in the standards. For instance, TOP-004-2, R4 allows 30 minutes for a Transmission Operator to restore the system to a known operating state within operational limits from an “unknown operating state”, which seems to be a good metric to use since loss of situational awareness at a Control Center results in an “unknown operating state”, which seems to correspond with the longest time frame of Attachment I to CIP-010. We understand that other commenters are submitting alternative language. We can support alternative options if they are based on existing NERC defined terms or already determined time limits.
2.17	Bonneville Power Administration	Agree with scope	The definition clearly ties the scope of the standard to real-time control. The time limit clearly separates real-time from long-term. The choice of 15 minutes versus some other duration is not as important as limiting the duration.While we agree with the scope, we don't believe the definition of BES Cyber System makes it clear that the scope is limited to real-time operation systems. The definition of BES Cyber System doesn't include the words real-time. For CIP-002, BPA identifies only control center systems used for real-

#	Organization	Yes or No	Question 2 Comment
			time controls as Critical Cyber Assets. This scope is consistent with what BPA does now for control center cyber systems.
2.18	Southern California Edison Company	Agree with scope	The drafting team should provide justification on the use of a 15 minute window for a BES cyber system to cause a Disturbance. Is the drafting team suggesting registered entities simulate disturbance events in 15 minute increments as a criterion in engineering studies to assess device capability that may be the justification for an impact based assessment methodology? If so, the drafting team needs to clarify this.SCE suggests removal of the 15 minute qualifier if no clear operational justification exists for the choice of such timeframe. While a three year timeframe for engineering studies is an acceptable, the constraints necessary for inclusion within the study, to look for specific disturbance conditions, may be difficult to implement.
2.19	Midwest ISO	Agree with scope	We agree in general. However, we do not necessarily agree with 15 minutes. Please see our response to Question 1.b.
2.20	Pepco Holdings, Inc. - Affiliates	Agree with scope	We agree with EEI's comments regarding the intended scope (i.e. limit to systems that impact the real-time real-time operations of the BES) and suggestions. Please also reference response to 1b.
2.21	We Energies	Agree with scope	We Energies agrees with EEI comments. Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.22	GTC & GSOC	Agree with scope	We understand the intent of the 15 minute aspect of the defined scope, but believe it will be difficult to implement and audit. Otherwise, we recommend the revised definition in 1b

#	Organization	Yes or No	Question 2 Comment
2.23	Duke Energy	Agree with scope	With the clarifications we've made above, we agree with the scope of applicability.
2.24	ISO New England Inc	Disagree with scope	- Recommend "30 minutes" to align with EOP standards- Please provide background for where the 15 minute recommendation came from
2.25	ReliabilityFirst Staff	Disagree with scope	Assuming the 15 minutes identified here is the same 15 minutes used in question 1.b above, we believe the scope should be 5 minutes.
2.26	Tenaska	Disagree with scope	Careful consideration should be given to the "within 15 minutes" phrase, this time period may be too long or too short depending on the severity of the event, type of cyber asset, or the type of BES entity. The Operational Time Horizon should be based on the potential severity of the event as well as the availability of other systems that can provide the same functionality.
2.27	Cogeneration Association of California and Energy Producers & Users Coalition	Disagree with scope	Comments to Questions 1.a and 1.b apply here also.
2.28	ERCOT ISO	Disagree with scope	Comments: The 15 minute requirement does not align to the other reliability standards. Recommend changing to 30 minutes to align with the EOP standards.
2.29	CenterPoint Energy	Disagree with scope	Disagree - CenterPoint Energy is concerned with the definition as stated above in response to 1.b. In addition, the SDT has offered no basis for the 15 minute time horizon.

#	Organization	Yes or No	Question 2 Comment
2.30	E.ON U.S.	Disagree with scope	E.ON U.S. seeks clarification of whether the 15 minutes captures the intent of the 'Restoration of BES" function identified in Attachment 1 of CIP-010
2.31	Exelon Corporation	Disagree with scope	Exelon suggests that the time period should not be stated in specific minutes. The standard should be revised to "One or more BES..., or misused could, without sufficient time to take mitigating action, cause a disturbance to the BES,..." The 15 minute timeframe is inconsistent with other standard language. Specifically, TOP-004-2 R.4. has a 30 minute response requirement.
2.32	LCEC	Disagree with scope	I am concerned that a time based definition will lead to confusion and create a difficult situation from an audit perspective. I agree that the standard should exclude "situational awareness" related functions that are not real-time in nature and do not provide the primary operational monitoring or control function of the BES.
2.33	Matrikon Inc.	Disagree with scope	I am trying to determine where to insert this operational time horizon into the evaluation criteria. Due to the room for interpretation, I don't yet support or reject the use of 15-minutes, or an appropriate duration. Fundamentally, there is no clear definition or instruction on how this can be used as criteria for determining Impact Level of cyber systems.I worry there is room for different interpretations, putting an entity trying to comply with the new CIP-01x standard at a competitive disadvantage to another entity that takes a different approach. I foresee 2-3 places where the time horizon could be inserted into a Responsible Entity's interpretation of BES Cyber Systems, I am hoping a tighter definition will address this issue.First Interpretation Scenario:1. The entity first determines the Impact Rating of each individual Cyber System using Attachment 2.2. Do they now evaluate the impact rating against the time horizon? Let us assume the Cyber System has High Impact. But if there is no effect in 15 minutes, does that mean: 2a. I automatically assign a Medium impact Rating? 2b. Or, I now evaluate it against the Medium impact criteria?3. If it continues to have no impact in 15 minutes to the Medium criteria, then is it a Low Impact BES Cyber System?Second

#	Organization	Yes or No	Question 2 Comment
			Interpretation Scenario:1. The entity first determines the Impact Rating of each individual Cyber System using Attachment 2. 1a. Let's now assume that the rating of High/Medium/Low is assigned to each BES Cyber Component and cannot be changed.2. Do they now go through the complete list of Cyber Systems looking for those which could affect any reliability function within 15 minutes? 2a. This may bring in other support systems like HVAC, UPS, CEMS opacity readings for generation, water supply and others that are not explicitly named in Attachment 1.Third Interpretation Scenario:1. An event has occurred at the facility that some action needs to be taken. There is the capability to notify the authority, and shutdown/bypass safely within 5-10 minutes.2. If the Responsibility Entity has the ability to exceed 15-minutes before taking action, then is this no longer an impact to the BES, and subsequently falls to the bottom and become Low Impact. 2a. For example, coal handling is down but we have some coal left on the conveyor, and the boiler is still hot so we have time to respond. 2b. For example, water supply is dropping but do not have to take action within 15 minutes. 2c. For example, vibration or emissions data is high, but we don't have to take action, within 15 minutes.Please provide additional information and guidance on how the 15-minute time horizon is to be applied to systems.
2.34	CWLP Electric Transmission, Distribution and Operations Department	Disagree with scope	It is unclear how the 15 minute time frame is to be applied.
2.35	Emerson Process Management	Disagree with scope	It really depends on how we view this issue. If I understand this intent correctly, the current language is trying to state that the BES reliability will be suffered if the BES cyber system is unavailable for more than 15 minutes. In another word, if the BES cyber system is failed for more than 15 minutes and the BES is not suffered, this system will be not categorized as BES Cyber System. This definition is very difficult in interpretation for power generation. If a plant has a 2000MW generation capacity and its water treatment cyber system is failed, the plant itself can sustain for a while, but not too long. After this grace period, the unit(s) will be shut down. The 2000MW will be lost. Does this affect

#	Organization	Yes or No	Question 2 Comment
			BES reliability? This is the confusion.
2.36	Florida Municipal Power Agency	Disagree with scope	It seems that the 15 minutes is arbitrary. FMPA suggests aligning the time to an already determined time limit in the standards. For instance, TOP 004 2, R4 allows 30 minutes for a Transmission Operator to restore the system to a known operating state within operational limits from an "unknown operating state", which seems to be a good metric to use since loss of situational awareness at a Control Center results in an "unknown operating state", which seems to correspond with the longest time frame of Attachment I to CIP-010.
2.37	Seattle City Light	Disagree with scope	It will be difficult to quantify the impact of systems within a window of time - this would be a qualitative assessment which invites a tremendous amount of subjectivity.
2.38	Garland Power and Light	Disagree with scope	Need to add "scoping filter" as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states "typically excludes business, market function systems, and non real-time systems", then it is a good scope and we would agree
2.39	Kansas City Power & Light	Disagree with scope	No. Including "within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES" in the definition provides a difficult set of parameters that encourages issues with interpretation of what would constitute the situations under which "within 15 minutes" applies, as well as, what constitutes "restricted control or generation"? It is understood the Drafting Team is trying to capture the essence of those systems that have a real-time impact on the BES, however, it is recommended to limit the scope of the applicable "BES Cyber

#	Organization	Yes or No	Question 2 Comment
			System" to those systems that support facilities that are identified as critical to the reliability of the transmission grid determined by regional system study.
2.40	Covanta Energy	Disagree with scope	Not clear as to why 15 minutes is the optimal number... would like more basis information prior to supporting.
2.41	IRC Standards Review Committee	Disagree with scope	Please see our comments under Q1b
2.42	Independent Electricity System Operator	Disagree with scope	Please see our comments under Q1b.
2.43	Public Service Enterprise Group companies	Disagree with scope	PSEG agrees that cyber protections should be mandated only for real-time operations systems.
2.44	National Grid	Disagree with scope	Real time operation of the system typically implies SCADA. If protection systems are part of the real time operations then as stated in 1b, the 15 minute time horizon may not be adequate. 15 minute time limitation also does not appear realistic. The vulnerability can exist beyond this timeline and can be equally catastrophic.
2.45	Electricity Consumers Resource Council (ELCON)	Disagree with scope	See comment on 1.a above.
2.46	NextEra Energy Corporate Compliance	Disagree with scope	See comments to 1a. NextEra believes if this approach is maintained despite these concerns, then this section needs clarity regarding 15 minute time horizon regarding recoverability. As written, the definition encompasses and overlaps normal operations

#	Organization	Yes or No	Question 2 Comment
			systems and recovery timeframes and does not address impacts to the BES beyond normal reliability operations.
2.47	Manitoba Hydro	Disagree with scope	See comments to Question 1.6
2.48	BCTC	Disagree with scope	See previous response
2.49	Network & Security Technologies Inc	Disagree with scope	See response to 1.b., previous
2.50	Puget Sound Energy	Disagree with scope	See response to question 1b. While it seems realistic, it is unclear how to prove something is within the 15 minute timeframe or not and unclear how this could be tested during an audit that something should have been included or not included. Some examples would be beneficial. Also PSE agrees with the scope of the definition, but is concerned with the vagueness of two of the terms used in the definition: "restrict" and "affect". PSE agrees with the definitive language of "cause a Disturbance", as that is a measurable level of compliance. The current standard has too many vague terms that are left open for interpretation.
2.51	WECC	Disagree with scope	Suggest SDT re-evaluate if reliability coordination systems such as Coordinated Outages, Historian, or Next Day Studies should be excluded from scope of these standards.Also, see response to 1c
2.52	Indeck Energy Services, Inc	Disagree with scope	The 15 minute time horizon needs to exclude events that the BES normally resolves within 15 minutes. Many events could take place in significantly less time. Normal operations work within the 10 minute horizon for measurements such as controlling

#	Organization	Yes or No	Question 2 Comment
			ACE. Not everything that happens within 15 minutes necessarily affects BES ALR. A single 15 minute time horizon appears to cast the net too widely. The time horizon needs to be specified for each of the Functions in Attachment I.
2.53	FirstEnergy Corporation	Disagree with scope	The 15 minute time limit causes confusion on how the definition will be applied in practice, since in most cases the loss of a component creates a probabilistic risk and not a certain risk.FE suggest that the SDT avoid the use of the 15 minute reference and consider incorporating the existing NERC glossary terms of "Real-time" and "Real-time Assessment". We offer the following definition for BES Cyber System:BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could cause a BES Disturbance or impact the Real-time Assessment capability, Real-time control and operation, or materially impact situational awareness of the BES.Situation awareness is somewhat vague and may mean different things to different people. The team should consider taking the description of situational awareness as shown in Attachment I - "Functions Essential to Reliable Operation of the Bulk Electric System" and making it a NERC Glossary of Terms definition.
2.54	LADWP	Disagree with scope	The 15 minute window is relative. The industry needs to define what is an acceptable time horizon.
2.55	Dairyland Power Cooperative	Disagree with scope	The 15-minute rule seems arbitrary and one dimensional. How does the availability of using a system for control relate to this time frame? I'm having trouble relating this to for instance a telemetry/control function. It would be possible that long periods of down time could pass without impact to the BES system... but under certain conditions it would be critical to have the monitoring and control functions.
2.56	Constellation Energy Commodities Group Inc.	Disagree with	The definition of a Disturbance includes a concept, as applied by Balancing Authorities of sudden failures of generation or interruption of load. The fifteen minute window is generally viewed as the length of time in which recovery should take place. The drafting

#	Organization	Yes or No	Question 2 Comment
		scope	team should look at narrowing the time horizon further to capture BES Cyber Systems that will directly control equipment and result in immediate system impacts. The definitions of Disturbance and Emergency reflect events that immediately impact the system; the fifteen minute window is viewed as the point in time by which the system should be recovered.
2.57	Constellation Energy Control and Dispatch, LLC	Disagree with scope	The definition of a Disturbance includes a concept, as applied by Balancing Authorities of sudden failures of generation or interruption of load. The fifteen minute window is generally viewed as the length of time in which recovery should take place. The drafting team should look at narrowing the time horizon further to capture BES Cyber Systems that will directly control equipment and result in immediate system impacts. The definitions of Disturbance and Emergency reflect events the immediately impact the system, the fifteen minute window is viewed as the point in time by which the system should be recovered.
2.58	San Diego Gas and Electric Co.	Disagree with scope	The phrase "real-time" doesn't have a definitive industry-wide connotation, although for collecting field data it usually means seconds instead of minutes. In general, SDG&E supports the inclusion of real-time operations systems being in-scope, but we support a shorter operational time horizon (such as 5 minutes) to make the definition more immediate, with more high value BES Cyber assets being part of the scope.
2.59	Minnesota Power	Disagree with scope	The scope of applicability and operational time horizon of 15 minutes appears arbitrary and Minnesota Power is unsure as to how the Standards Drafting Team envisions that a Registered Entity will be able to show and document (i.e., prove for audit purposes) that a particular Cyber System will or will not have an effect on the BES in a certain time period. If the intent is "real-time operations," then state that and drop "within 15 minutes."
2.60	Consultant	Disagree with	The scope statement should clarify the inclusion or exclusion (or alternative treatment) of backup systems, development systems and environments, quality assurance systems and environments, testing systems and environments.As stated the only systems that

#	Organization	Yes or No	Question 2 Comment
		scope	appear to be "in scope" are live production systems.
2.61	US Bureau of Reclamation	Disagree with scope	This requirement puts a premium on the definition of what the BES is. There are components of the power system that are not "BES" and therefore do not qualify under these Standards. This issue needs to be further addressed. Further, the term "operational time horizon" needs further definition. Is this 15 minute criterium to be applied under normal operation conditions, or only those that COULD be experienced if the Cyber System were to be compromised?
2.62	Ameren	Disagree with scope	We disagree with the scope; the 15 minutes should only apply if the disturbance is not recoverable.
2.63	Southern Company	Disagree with scope	While we understand the intent of the 15-minute scope, we feel that the inclusion of this factor causes too much vagueness in the interpretation of the definition. We recommend that the focus be limited to real-time operations only.
2.64	Verizon Business	Agree	The “15 minute” criterion needs to be expanded – perhaps in an associated guideline or “Frequently Asked Question”

3. **Requirement R1 of draft CIP-010-1 states, "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions defined in CIP-010 – 1 Attachment I – Functions Essential to the Reliable Operation of the BES to identify BES Cyber Systems for the application of security requirements." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.**

Summary Consideration:

Many entities expressed concerns on the broad implication associated with the phrase "execute or enable…". Entities generally agreed with the assignment of compliance responsibility to owners, but many others expressed concerns for jointly owned facilities or facilities that may be operated by other than owners. There were many concerns expressed about the Functions and their description and definition. Others expressed concerns about the differences between systems and their components.

CIP-010-1 Requirement R1 has been replaced by CIP-002-5, which reads:

Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems*. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

Additional guidance for jointly owned facilities has been provided in the Application Guidelines section of the standard. The reliability functions have been redefined as Reliability Operating Services to avoid any confusion with the use of the term Functions as used in the Functional model.

#	Organization	Yes or No	Question 3 Comment
3.2	WECC		Agree with the concept however, "…to execute or enable…" or "…which execute and/or enable." "to" can be construed as passive. It is redundant to utilize the phrasing "…to identify BES Cyber Systems for the application of security requirements."The following rewrite is proposed;R1. Each Responsible Entity shall identify and document each BES Cyber System(s) that it owns, which execute and/or enable one or more functions defined in CIP-010 - 1 Attachment I - Functions Essential to the Reliable Operation of the BES. (Violation Risk Factor: High)
3.3	Entergy	Agree	Agree that applicability should be strictly focused on "owned" assets.

#	Organization	Yes or No	Question 3 Comment
3.4	US Army Corps of Engineers, Omaha Distirc	Agree	Agree with R1 requirement - Find the measures for R1 - R3 troublesome. Measures are stated in terms of number of BES cyber systems. It is conceivable that plant SCADA systems could be considered a single system or a group of a few systems. How is a missed component handled? Is it another system or is a component. It appears like the violation measures are being handled as a count of BES cyber system components not BES cyber systems. Feel the measures should be revisited with the low number of systems likely to be identified in mind. Seems odd that any additional system is a sever violation if you have identified fewer than 6 systems.
3.5	Florida Municipal Power Agency	Agree	Although FMPA agrees with the requirements, FMPA suggests that naming Attachment I "Functions ...." will add confusion with the "Functional Model". FMPA suggests renaming Attachment I to "Activities Essential to the Reliable Operation of the BES", and of course modify R1 to reflect this change. Additional comments on Attachment I are included below in Question 6.
3.6	Garland Power and Light	Agree	Definitely agree with the words "it owns"
3.7	SCE&G	Agree	Guidelines should be provided to assist entities in determining how BES Cyber System Components should be grouped into BES Cyber Systems. Can a single component reside in two cyber systems?
3.8	Dynegy Inc.	Agree	I agree but request additional detail examples be provided to determine specifically what these items are.
3.9	Reliability & Compliance Group	Agree	Is the assumption that the initial list needs to contain both BES and non-BES Cyber Systems? It would be better if the standard was even more proscriptive here.
3.10	Con Edison of New York	Agree	Please note comments to question 6. It may be easier if the DT reference functions as detailed by FERC-approved NERC Reliability Standards. The definitions in Attachment I will ultimately lead to many requests for interpretation. R1 requires identification and documentation of BES Cyber Systems. There is no requirement to identify BES Cyber

#	Organization	Yes or No	Question 3 Comment
			System Components within CIP-010. However, CIP-011-1 R23 requires that you develop an inventory of these Components. Should this be a CIP-010 requirement? Then CIP-011 can expand on the Change Management Controls.
3.11	San Diego Gas and Electric Co.	Agree	SDG&E agrees with the wording in R1, but has additional comments and requests for clarification. Specifically, we request clarification regarding the "situational awareness" reference in Attachment I. In our case, as many other entities, we use Remote Terminal Units to gather data from BES substations and present that data to the operators to improve their Situational Awareness. Loss of a single RTU vs. loss of multiple RTUs affects the presentation of this data to operators to varying degrees (with associated effects on monitoring the BES), but the Standards don't address quantitative issues such as this.In a similar vein, SDG&E also requests clarification regarding the term "inter-entity real-time coordination and communication" in Attachment I. For example, are inter-entity telephone systems in-scope or is this referring to electronic data exchange between entities such as ICCP data links?Probably SDG&E's largest concern with CIP-010-1 R1 is the sheer amount of effort and resources it will take to build the lists of BES Cyber Systems and the impact categorizations. While there are some loose parallels with the current CIP-002 Standard, we won't be able to re-use the bulk of the work already done in our Risk-Based Assessment to identify Critical Cyber Assets. SDG&E's opinion is that CIP-010 doesn't leverage as much of CIP-002 as we'd like to see. We'd like to take advantage of what already has been produced to become Compliant with the existing Standards, and we see these new draft Standards as going in a new direction with many of the requirements. We would feel better about it if the new Standards were bringing substantial additional reliability and security to the BES, but that is not apparent.
3.12	Minnesota Power	Agree	With the previously stated recommendations regarding the definition of BES Cyber System (see Question 1.b.) and the changes indicated below, Minnesota Power generally agrees with the proposed Requirement R1. "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns which execute or enable one or more functions defined in CIP-010 - 1 Attachment I, Functions Essential to the Reliable

#	Organization	Yes or No	Question 3 Comment
			Operation of the BES, for the purpose of applying the security requirements."
3.13	BCTC	Disagree	- Recommend removal of the “Inter-Entity Real-Time Coordination and Communication” (Attachment 1) point as this is covered under the COM domain
3.14	Bonneville Power Administration	Disagree	"...that it owns to execute or enable..." is somewhat unclear. It appears the intent is the equivalent of "that it owns that is able to execute or enable...". As it is written, it can give the impression that the purpose of owning the system is to execute or enable the functions. That is too narrow. Another possible interpretation is that the "to execute or enable..." refers to the objective of the requirement. If that is so, then please break the objective out separately:"Objective: To execute or enable...Requirement: Each Responsible Entity..."Many of the other requirements include "to..." at the end of the requirement. These are clearly objective statements. They should be broken out separately, into an "Objective" and "Requirement", as stated above. The last phrase in Requirement 1 is “for the application of security requirements.” In Requirement 2 the last phrase is “for the application of Cyber Security requirements . . . .” Are these two phrases supposed to have the same meaning? If so, shouldn’t they use identical words? If not, what does “for the application of security requirements” mean? Is it referring to some or all of the requirements in CIP-011-1? If so, it should clearly state that and, if not the entire standard, which specific requirements it is referring to.It seems that it should read as follows: “for the application of the Requirements contained in Standard CIP-011-1.”
3.15	Consultant	Disagree	1. I think the standards should provide some distinction between ownership responsibility and operations responsibility, or provide a mechanism to identify the responsibility for the requirements based on each specific situation. (Technical Feasibility Exception for owner versus operator responsibility?) This may include split responsibility for different aspects of the requirements. (This comment probably applies to more than just this requirement in both CIP-010 and CIP-011.)2. Wording is confusing regarding systems for application of security requirements. Suggest ending the requirement statement after "...Reliable Operation of the BES."3. Suggest using the complete title of

#	Organization	Yes or No	Question 3 Comment
			Attachment I: "Bulk Electric System" not "BES".4. In all locations in both CIP-010 and CIP-011 suggest removing references to specific revisions (e.g. CIP-010-1). This requires all standards to be changed for a change in any one standard. The documentation of which revision was used at the time of implementation should be included in the Responsible Entity's documentation or compliance.
3.16	Dairyland Power Cooperative	Disagree	A Responsible Entity should be responsible for any systems used for their operation regardless of ownership. Basing responsibility based on the ownership of a system creates a big loophole. It is possible an interfacing utility or service provider could be involved. Basing responsibility on the ownership of the facility containing the systems make more sense.
3.17	Duke Energy	Disagree	Additional clarification is needed on the process for identifying and categorizing BES Cyber Systems. Requirement R2 should really come first, and require that Responsible Entities identify their BES Cyber Systems that meet the criteria in Attachment II (i.e., that can affect operations for the listed facilities/functions). Requirement R1 should come second, and require documentation of the functions affected for each BES Cyber system identified. Attachment I is not needed as part of the standard, but should be included in a guidance document.Much more clarification is needed to Attachment I. As described, the functions are far too broad. Specific language issues: o Monitoring & Control - Activities, actions and conditions that provide both monitoring and control of BES elements. o Situational Awareness - too broad as stated. Should be limited to situational awareness of the BES required by System Operators to perform their reliability-related functions o Inter-Entity Real-Time Coordination and Communication - too broad as stated; would seem to possibly include telephone lines
3.18	Arizona Public Service Company	Disagree	Additional verbiage needs to be included in order to clearly delineate which entity is responsible for an asset/system when it is jointly owned. Is it the majority owner? The operator? Where is the line?"

#	Organization	Yes or No	Question 3 Comment
3.19	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Again, no defining metrics. Small DP/LSEs will unnecessarily be required to comply with no BES reliability return.
3.20	IRC Standards Review Committee	Disagree	At the NERC CIP workshop in May 2010, there were so many examples brought forth where it could not be determined with exactness which components are part of a BES Cyber System or not because of the flexibility built into the requirements. "It depends" was often the response from the panels. So although the intent of CIP-010 is to provide more concrete guidance for registered entities to define BES Cyber Systems, in practice it may introduce just as many new questions about applicability as it may solve. It would be better to develop a performance based approach to define BES Cyber Systems rather than use bright line definitions to identify BES Cyber Systems. The proposed definitions of High and Medium include criteria that describe facilities, by KV level, MW size etc. But these are really proxies for an underlying intent of trying to describe a certain level of operational performance. For example, higher KV levels are assumed to reflect greater impacts on neighbors. And higher MW levels of generation are assumed to reflect greater risk of disturbance to load. Rather than use these proxies, the ratings High and Medium should instead employ descriptors related to a desired level of performance, for example, "...a loss of a facility that does not cause a IROL violation two systems away." Such an approach in defining the BES Cyber System would better focus the CIP-011 requirements and compliance efforts of both NERC and the registered entity on only those components that truly have a significant impact on the interconnected BES and not include facilities and components that although meet a bright line definition, really have minimal impact on the BES because of its particular location or configuration.
3.21	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
3.22	ERCOT ISO	Disagree	Comments: It should be stated that the Responsible Entity is allowed to perform R1 and R2 in the order they deem appropriate. Consider: "Each Responsible Entity shall

#	Organization	Yes or No	Question 3 Comment
			document each identified BES Cyber Systems that it owns which support the functions defined in CIP-010-1 Attachment I - Functions Essential to the Reliable Operation of the BES, for the application of security requirements."
3.23	LCEC	Disagree	Concerned with the word "owns". Recommend "owns or operates" or a statement referencing operational responsibility.With the current definition of BES Cyber System Components including "one or more" devices, a lot of guidance will be needed to determine what constitutes a system versus a number of components. Most of the standards currently reference the system versus the component which could leave a gap in applicability. Is it assumed that all components must be a system or part of a system? Modifying the BES Cyber System Component definition to exclude "one or more" will help but entities will still need clarification on the grouping of components to form systems. An implementation guideline will help address this.
3.24	Constellation Power Source Generation	Disagree	Constellation believes that this requirement is too broad in terms of auditability. The proposed verbiage of CIP-010 is flexible in terms of how to define cyber systems, but is it implying that a methodology is needed to identify cyber systems? Or is it implying that each Responsible Entity define cyber systems as they see fit, without an explanation? For a company such as Constellation, which owns a fleet of diverse generation facilities, this flexibility will cause each plant to have its own unique methodology for developing cyber systems, which vastly increases the procedural burden of this standard when compared to the current version of CIP-002. A suggestion would be to clarify this requirement in a guidance by stating whether or not a methodology is needed to define cyber systems, and if not, what type of evidence would be suggested for showing that a cyber system has been identified correctly.
3.25	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy does not agree with the direction of the SDT and believes it is pre-mature to discard the current CIP requirements with a completely new philosophy. Most entities are in the compliance phase of implementation of the current CIP requirements and have yet to be audited. To have a fundamental shift in approach before the current requirements have been evaluated as to effectiveness and

#	Organization	Yes or No	Question 3 Comment
			compliance is unwarranted. In addition, CenterPoint Energy does not agree with the expansion of the CIP requirements to facilities that do not have a high impact on the reliable operation of the Bulk Electric System. CIP-010-1 and CIP-011-1 would apply some cyber security requirements to facilities and systems that the draft Standard would identify as having a medium to low impact to the reliable operation of the Bulk Electric System. While CenterPoint Energy agrees that some set of minimal security criteria should be used to protect facilities from malicious behavior, vandalism, or simply the curious, CenterPoint Energy believes these efforts are more accurately characterized as Good Business Practice and as such should not be auditable under mandatory reliability standards. Stated another way; those facilities and systems that have been identified as medium to low impact, using the draft standard methodology, by the nature of having little or no impact to reliable operation of the Bulk Electric System, should not be protected under auditable, mandatory, requirements.
3.26	Constellation Energy Control and Dispatch, LLC	Disagree	Disagree based on concerns with Attachment 1 Propose definitions for Attachment 1:Dynamic Response functions: BES equipment that reacts automatically to a BES Disturbance.Balancing Load and Generation: BES equipment that directly controls generation or load.Controlling Frequency: BES equipment that directly controls frequency (Does control of generation already cover this function?)Controlling Voltage: BES equipment that directly controls reactive power resources.Managing Constraints: (Delete this function) - Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Monitoring & control: Delete Monitoring and limit the BES equipment that control actions such as open and closing switches or relays, motor starts/stops, etc. Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope

#	Organization	Yes or No	Question 3 Comment
			for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Restoration of BES: BES equipment required for system restoration.Situational Awareness: (Delete this function). Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Inter-Entity RT Coordination and Communication: (Delete this function) As written this function is too broad and should be limited data that drives operation of BES equipment . Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment.
3.27	Constellation Energy Commodities Group Inc.	Disagree	Disagree based on concerns with Attachment 1Propose definitions for Attachment 1:Dynamic Response functions: BES equipment that reacts automatically to a BES Disturbance.Balancing Load and Generation: BES equipment that directly controls generation or load.Controlling Frequency: BES equipment that directly controls frequency (Does control of generation already cover this function?)Controlling Voltage: BES equipment that directly controls reactive power resources.Managing Constraints:

#	Organization	Yes or No	Question 3 Comment
			(Delete this function) - Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Monitoring & Control: Delete Monitoring and limit the BES equipment that control actions such as open and closing switches or relays, motor starts/stops, etc. Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such a tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Restoration of BES: BES Cyber System or Components required for system restoration.Situational Awareness: (Delete this function). Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Inter-Entity RT Coordination and Communication: (Delete this function) As written this function is too broad and should be limited data that drives operation of BES equipment. Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to

#	Organization	Yes or No	Question 3 Comment
			directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such a tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment.Define the term Situation Awareness and how it applies to BES Cyber System or components required for system restoration.
3.28	Dominion Resources Services, Inc.	Disagree	Dominion agrees with R1, but is concerned with the functions listed in Attachment 1. Please see Dominion's response to Question 6.
3.29	E.ON U.S.	Disagree	E ON U.S. notes the absence of any study to assess whether identifying and categorizing all BES Cyber Systems as required by R.1 provides for material enhancement of BES reliability relative to the current Critical Asset identification methodologies allowed under CIP-002. E ON U.S. is also not aware of any effort to objectively quantify the costs that will result from R.1. Given the likely significant costs to consumers it would behoove the SDT and NERC to make an effort to understand the costs and incremental improvement to BES reliability associated with the sweeping changes proposed in CIP-010, R.1.The proposal does not allow for "no impact" assessments to be determined through engineering evaluation or other approved methods. E ON U.S. believes it would be an improvement to include language similar to that in existing CIP-002 R1.2.
3.30	EEI	Disagree	EEI generally agrees with R1, however, all owners of jointly owned facilities may not be responsible for protecting the BES Cyber Systems. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1. As a result, the drafting team should clarify what is meant by "owns" (i.e. how should GOs and GOPs collectively assess BES Cyber Systems).
3.31	ReliabilityFirst Staff	Disagree	For clarity, ReliabilityFirst suggests the following revision to the language of this requirement, "BES Cyber Systems that the entity owns, operates, or is otherwise

#	Organization	Yes or No	Question 3 Comment
			responsible for. . .”
3.32	American Municipal Power	Disagree	I agree with the intent, but I disagree with the structure of CIP-010. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
3.33	USACE HQ	Disagree	I disagree with the new approach the team is presenting of substituting the risk-based assessment methodology with a list of essential function without any support of why they are essential. Order 706, page 70 - 72, recognize the need for risk-based assessment methodology guidance, therefore recognizing that the use of a quantifiable methodology based on risk is the right way to assess criticality of assets or systems present in the community. To create a list of functions and stating that they are essential without having done some type of study looking into what are really essential functions supporting the BES are only limits the protection of each asset to what a small group of people think is critical without taking into consideration the individual circumstances each asset brings to the table. I suggest that either the team moves back to the original intent in CIP-002 versions 1 - 3 and re-institute the language of risk-based methodology to create the list of BES Cyber Systems OR the team does a risk-based study on the BES to establish the “functions essential to the reliable operation of the BES”.
3.34	Pepco Holdings, Inc. - Affiliates	Disagree	In general we agree with R1 when there is only one owner of a BES Cyber System. However we also agree with EEI’s comments that owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are

#	Organization	Yes or No	Question 3 Comment
			Transmission Lines and/or Substations that are owned by multiple parties but one party is responsible for the operation and maintenance. Suggest considering adding language to R1 to cover joint owned facilities (e.g. In cases of joint owned BES Cyber Systems, the assigned Responsible Entity or Entities shall...).
3.35	Southern California Edison Company	Disagree	It is not clear how this requirement differs from CIP-002, R3. While the description of CIP-011 states the intent to retire CIP-003 through CIP-009, CIP-002 would still be in place. It is also not clear how these CIP-010-1 and CIP-002 would work together.
3.36	SPS Consulting Group Inc.	Disagree	It is unclear how the list of Essential Functions in Attachment 1 correlates to the categorization in Attachment II, which does not mention essential functions. I believe that Attachment I can be deleted and that Attachment II is fully sufficient for the categorization exercise. The stated purpose of Attachment I to define the scope of the CIP standards is unnecessary because the CIP standards do not apply to functions, they apply to registered entities, which are quite clearly stated.
3.37	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
3.38	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's recommendation to change owner to the owner-operator that performs operations as described below:Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The owner-operator that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.39	Michigan Public Power Agency	Disagree	MPPA is one of many organization that are co-owners of facilities that do not maintain operational control of the facility. MPPA suggests that the word "owns" in "...Systems that it owns to execute..." be changed to "operates."
3.40	Tenaska	Disagree	No R1 should be to identify BES assets that cyber systems are a part of. Consider

#	Organization	Yes or No	Question 3 Comment
			replacing attachment 1 with better definitions in the body of the standard.
3.41	Progress Energy (non-Nuclear)	Disagree	One major issue is that we do not have a clear definition of the BES. How do we define the BES? Is it all lines over 100kV excluding transmission feeders? It appears that some reliability groups are presently trying to define the BES clearly. If the BES includes >100kV import/tie lines, nuclear off-site power path, cranking path, quite a few T/T substations with microprocessor relays on lines could be put in scope of identification. These might be excluded or classified low impact if no communication is provided. Will power line carrier, transfer trip, etc. be in scope? This could turn into a very large list to develop and maintain.
3.42	Allegheny Energy Supply	Disagree	Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.43	Allegheny Power	Disagree	Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.44	PacifiCorp	Disagree	PacifiCorp agrees with EEI's recommendation to change owner to entity that performs operations as described below:Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is should be identified as responsible for the requirements identified by CIP-010-1.
3.45	Regulatory Compliance	Disagree	Please clarify - Attachment I - The function identified for Inter-entity Real-time Coordination and Communication: Is the coodination between the Responsible Entities' associated System operators or between BAs? Also what specific equipment is brought

#	Organization	Yes or No	Question 3 Comment
			into scope? Is it only for data communcation or voice communication as well?
3.46	Puget Sound Energy	Disagree	Puget Sound Energy feels that, without clarity (as commented in question 2 above), the scope of BES Cyber Systems can not be uniformly agreed upon and, as such, defendable metrics to prove compliance will not be able to be establish. For example, corporate email can be used to provide efficient communications between operators of the BES. The loss of corporate email, which in no way could cause a disturbance to the BES (and is physically and logically separated from all BES Cyber Systems), could "restrict" or "affect" the real-time operations of the BES through degradation in efficient communications. As well in order to prove compliance the unintended consequence of this requirement is a massive work effort to evaluate all the BES Cyber Systems in order to then establish or demonstrate which enable or execute essential functions.
3.47	Alliant Energy	Disagree	R1 is ambiguous when referring to "Joint-Owned Units", and we believe that the word "owns" should be replaced with "owns and operates." In a joint-owned facility, the operator typically has responsibility for compliance with NERC standards.
3.48	Wolverine Power	Disagree	See comments listed for 1.a
3.49	NextEra Energy Corporate Compliance	Disagree	See comments to 1a. In addition, NextEra believes if the introduction of "functions" is another area that could lead to misunderstanding. If left, we recommend it only be for "informational purposes" and not controlling. As stated above, the specific list of components in BES Cyber Systems of Control Centers, Generators and Transmission should be what is controlling and protected. Also, as the drafting team will see throughout these comments, language that can be misunderstood will be proposed to be changed. The drafters often spoke of their intent, and while this term is widely used by the industry and it always means well, it is not a compliance/regulatory term the serves the industry, NERC or FERC well. The intent of the drafting team is not recognized as record evidence, nor is it controlling in an audit or before NERC or FERC. Thus, preambles should be clear. For example, "Purpose: To provide clear understanding of what BES Cyber System Components must be protected consistent with CIP-011-

#	Organization	Yes or No	Question 3 Comment
			1."Similarly, NextEra is not supportive of using technical guidance papers to supplement the Standards. NextEra believes the Standards are what NextEra will need to comply with and the guidance papers, unless approved by FERC, are not controlling from a compliance perspective. Moreover, guidance papers tend to be loosely written and subject to being misunderstood. NextEra would rather see the specifics in the Standards.
3.50	MWDSC	Disagree	Situational Awareness is a new term that will be confused with Monitoring and Control function in Attachment I. The term "Control and Operation" was changed from prior draft to "Monitoring and Control". Shouldn't situational awareness be performed by the same operator? Suggest deleting Situational Awareness and revising the Monitoring and Control function as follows:"Activities, actions and conditions that provide monitoring and control of BES elements, including the assessment of current, expected, and anticipated state of the BES.
3.51	Matrikon Inc.	Disagree	Still open for interpretation, in its most simple form the only action words are "execute" or "enable" that correspond the cyber system to each of the functions. Please provide further definition or guidance on its application.
3.52	Southwest Power Pool Regional Entity	Disagree	The ability of the entity to group its cyber assets into cyber systems as it sees fit potentially offers an opportunity to game the system by dissecting legitimate cyber systems into smaller groups of components with less span of control and thus lower impact. There needs to be some sort of sufficiency criteria to ensure proper logical grouping. Additionally, a concern to the auditor is the ability to ascertain that the entity has identified all of the pertinent cyber systems and that all of the necessary cyber system components have been accounted for. Lastly, consider modifying the phrase "...that it owns to execute or enable..." to read "...that it owns to execute, enable, or support..."
3.53	APPA Task Force	Disagree	The APPA Task force disagrees with the proposed requirement but we offer the following suggestions:We suggest that naming Attachment I "Functions ...." will create

#	Organization	Yes or No	Question 3 Comment
			confusion with the "Functional Model". We suggest renaming Attachment I "Activities Essential to the Reliable Operation of the BES", and of course modify R1 to reflect this change. Additional comments on Attachment I are included below in response to Question 6. There are many different business models in our industry, and "ownership" may not mean "owns and operates." Therefore we would propose replacing the word "owns" with "owns and operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has any control of the BES Cyber Systems installed, and/or the related day-to-day compliance with NERC standards.
3.54	Nuclear Energy Institute	Disagree	The current CIP-002 provides a risk-informed approach to the identification of assets critical to the reliability of the bulk-power system. The current practice is for a generator owner/operator to coordinate with the local transmission owner/operator to determine if the generator is critical to maintaining the reliable operation of the Bulk-Power system.The proposed CIP-010-1 eliminates this risk-informed approach, and would require all generators of any size to be required to comply with the CIP Standards even if the BES would not be adversely affected by the loss of the generating facility.NEI believes that the proposed methodology in CIP-010-1 is contrary to the intent of section 215 of the Federal Power Act (FPA) (16 U.S.C. 824o) which is to prevent instability, uncontrolled separation, or cascading failures as the result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.In order for CIP-010-1, R1 to be acceptable, reliance on an analysis by the transmission system owner/operator must be performed to determine if the generator operator/owner facilities are critical to the reliability of the bulk-power system.
3.55	GTC & GSOC	Disagree	The definition unnecessarily restates detail that should be in the definition of BES Cyber Systems. We recommend it be simplified to state the following "Each Responsible Entity shall identify and document each of its BES Cyber Systems in order to apply Cyber security requirements."

#	Organization	Yes or No	Question 3 Comment
3.56	FirstEnergy Corporation	Disagree	The definitional terms for Control Center, BES Cyber System and BES Cyber System Components in conjunction with the Requirement R2 "Impact Categorization (Attachment II)" should provide sufficient direction to the "programmable devices" that are within in scope and require protection under the proposed CIP standard. The R1 requirement places an unwarranted compliance documentation burden on the industry with questionable reliability payback. FE suggests that R1 and its corresponding Attachment I can be eliminated from the standard.Secondly, the requirement describes two unique actions - identify and document - BES Cyber Systems. "Documenting" the identified BES Cyber Systems is actually evidence of compliance that should be left to the Measures and not explicitly stated in the requirement. Failure to identify a BES Cyber System poses a real reliability risk to the BES, however, identifying and protecting a BES Cyber System but only neglecting to include it in a documented report is an administrative task with no reliability risk.
3.57	USACE - Omaha Anchor	Disagree	The owner may be a distant owner - I feel it should be operators - or the owner in conjunction with the operator.
3.58	Detroit Edison	Disagree	The phrase "to identify BES Cyber Systems for the application of security requirements" at the end of R1 is a restatement of the purpose of CIP-010 and should be removed. Consider changing R1 to: Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions defined in CIP-010-1 Attachment I - Functions Essential to the Reliable Operation of the BES.
3.59	Indeck Energy Services, Inc	Disagree	The R1 requirement ignores the risk based assessment methodology that is required by FERC-see Order 706. [suggested replacement language] "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions, defined in CIP-010 - 1 Attachment I - Functions Essential to the Reliable Operation of the BES, and perform a risk assessment according to its risk based assessment methodology of the impact on the reliability of the BES to identify a BES Cyber Systems for the application of security requirements."

#	Organization	Yes or No	Question 3 Comment
3.60	US Bureau of Reclamation	Disagree	The unclear definition for "could have an effect on real-time operation..." as used in the opening of Attachment I, needs to be clarified/quanitized or defined. Almost any of these functions (and many more), at any facility - no matter the size - could have an effect. The effect needs to be characterized as more than trivial to be deemed essential to reliable BES operation. Whether the changes are made to the Attachment or within this requirement is immaterial. The language in the requirement needs to be cleaned up as follows: "Each Responsible Entity shall catgorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachement II - Impact Categorization of BES Cyber Systems." The title of Attachment to is incorrect in the requirement.
3.61	Platte River Power Authority	Disagree	There can be some confusion regarding who is responsible for implementing and demonstrating compliance with the CIP standards under certain circumstances (e.g. joint ownership). It would be helpful if there was a mechanism to identify the “Responsible Entity” responsible for implementing and demonstrating compliance for various Assets. The “Responsible Entity” designation could also include operators and could vary based on standard\requirement. For example:The designated Responsible entity is the owner unless specified otherwise.For Assets where an owner is not the designated Responsible Entity:- The owner must document an agreement with the designated Responsible Entity including the Asset(s) and requirements the designated Responsible Entity is responsible for.- The designation must be to a NERC Registered Entity.- The designation must be reviewed and reaffirmed annually
3.62	Manitoba Hydro	Disagree	This is satisfactory if identifying the cyber system with a reasonably short descriptive overall functional summary is sufficient. It is unsatisfactory if each and every single component of the cyber system must be described in some detail. Since some of the requirements in CIP-011 are at the BES Cyber System Component level, the need to identify the components should be explicitly required in the standard. Requirement R1 is unclear as drafted. It is not clear if the phrase “to execute or enable one or more functions...” describes the purpose of identifying BES Cyber Systems, or if it describes a

#	Organization	Yes or No	Question 3 Comment
			necessary characteristic of the BES Cyber Systems. Note that in Measure M1, "to" is replaced with "that", creating an inconsistency between Requirement R1 and Measure M1. Measure M1 is not a complete sentence. What needs to be documented?.
3.63	Southwestern Power Administration	Disagree	Though identification of BES Cyber Systems may be beneficial, adding prescriptive categories such as those included in Attachment I only add another layer of administrative "check-listing" for compliance purposes and do not actually have a positive effect on reliability. If Attachment I is intended as guidance in understanding the functions essential to reliable operation of the BES, it would be more appropriately included in a guidance document.
3.64	Midwest ISO	Disagree	We do not believe that it is necessary to document what function its BES Cyber Systems perform in attachment I. We believe that it is only necessary to test them against the criteria established in Attachment II. Developing inventory lists of what BES Cyber Systems performs what functions in Attachment I would increase the risk of a coordinate attacks should the information get into the wrong hands.
3.65	We Energies	Disagree	We Energies agrees with EEI comments. Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.66	Madison Gas and Electric Company	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose replacing the word "owns" with "owns and operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has anything to do with the BES Cyber Systems installed, or the related day-to-day compliance with NERC standards. Attachment 1 requires clarification.Balancing Load and Generation, Controlling Frequency (Real Power) and Controlling Voltage (Reactive Power) are Functions Essential to Reliability Operation of

#	Organization	Yes or No	Question 3 Comment
			the Bulk Electric System but do not contain the modifier of BES as in Monitoring and Control does. Is it implied that the listed functions are only those functions Essential to Reliability Operation of the Bulk Electric System? Please clarify.
3.67	MRO's NERC Standards Review Subcommittee	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose replacing the word "owns" with "owns and operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has anything to do with the BES Cyber Systems installed, or the related day-to-day compliance with NERC standards.
3.68	The Empire District Electric Company	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose replacing the word "owns" with "operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has anything to do with the BES Cyber Systems installed, or the related day-to-day compliance with NERC standards.
3.69	Alberta Electric System Operator	Disagree	We find the current wording somewhat confusing. Consider rewording the sentence. As a suggestion, "...that it owns that executes or enables one of..."
3.70	Oncor Electric Delivery LLC	Disagree	We need more clarity (white paper) to assist in how utility equipment should be identified as components or systems. Is the relaying scheme at a single substation a "system" and all the individual relays are "components", or is the primary and backup relays for a single line terminal, bus, or transformer the "system" and the individual primary/backup relay is a "component". This is basic to the implementation of this standard and needs to more fully defined.

4. **Requirement R2 of draft CIP-010-1 states, "Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II – Impact Categorization of BES Cyber Systems to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.**

Summary Consideration:

The majority of the concerns raised in the comments were related to Appendix 2, the criteria used for categorization.

Specific concerns about categorization are addressed in the responses to Q7 and in the criteria which were approved by industry for Version 4 of CIP-002.

In CIP-002-5, this requirement has been consolidated with Requirement R1 of the previously posted CIP-010-1, to create CIP-002-5 Requirement R1 as follows:

Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems.* All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. *[Violation Risk Factor: High][Time Horizon: Operations Planning]*.

#	Organization	Yes or No	Question 4 Comment
4.1	WECC	Agree	Agree with the comment but it is unnecessary to utilize the phrasing "...for the application of Cyber Security requirements commensurate with the potential impact on the BES." The following rewrite is proposed;R2. Each Responsible Entity shall categorize and document such categorization for each BES Cyber System(s) identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems to categorize the BES Cyber Systems identified in Requirement R1. (Violation Risk Factor: High)
4.2	LCEC	Agree	Agree with the intent of the requirement but need to clarify the content of the attachment.

#	Organization	Yes or No	Question 4 Comment
4.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
4.4	FirstEnergy Corporation	Agree	FE supports R2 and the Impact Categorization achieved through Attachment II. Attachment II provides much needed clarity, compliance certainty but most importantly a consistent application of the critical infrastructure required to be secured within the context of the proposed CIP requirements.Suggested improvements to Attachment II are provided in our Question 7 response.As described in Question 3 above FE believes that R1 and Attachment I are not needed within the standard and that terminology for Control Center, BES Cyber System and BES Cyber System Components is sufficient. Therefore, conforming changes would be needed in R2 for a removal of R1/Attachment I. For example, "Each Responsible Entity shall document an impact categorization of its BES Cyber Systems consistent with CIP-010 Attachment ...."Requirement R2 and its corresponding Attachment II provides no guidance on whether digital relays colocated at a Transmission Facility need to be treated as individual BES Cyber Systems. FE recommends that the team clarify that a responsible entity could generically reference "Digital Relay Protection System" as a BES Cyber System located at a particular Transmission Facility (substation). There should be no need to identify/document each individual digital relay as a separate and unique BES Cyber System. Rather, the digital relay would be viewed as BES Cyber System Component of the Transmission Facility protection system. This will simplify compliance documentation, particularly for devices that may be associated with a Low Impact categorization.
4.5	Dynegy Inc.	Agree	I agree but request additional detail examples be provided to determine specifically what these items are.
4.6	NextEra Energy Corporate Compliance	Agree	In general, NextEra is supportive of the high, medium and low impact approach. However, in response to question 7, NextEra addresses concerns of the low impact approach.

#	Organization	Yes or No	Question 4 Comment
4.7	Minnesota Power	Agree	In order to increase clarity, Minnesota Power recommends the following changes to the language of Requirement R2: "Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II, Impact Categorization of BES Cyber Systems. Each BES Cyber System's impact category will require the application of specific Cyber Security requirements commensurate with their potential impact on the BES."Minnesota Power believes that if a Registered Entity can support the exclusion of specific criteria identified in Attachment II with study data, then the Registered Entity should be allowed to exclude such criteria from further analysis.
4.8	Puget Sound Energy	Agree	Puget Sound Energy agrees with the language in R2, provided the language in attachment II is addressed (comments provided in question 7).
4.9	Con Edison of New York	Agree	See comments on question 7.
4.10	Platte River Power Authority	Agree	Suggest Revising:Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems for the application of Cyber Security requirements commensurate with the potential impact on the BES.
4.11	Reliability & Compliance Group	Agree	The categorization seems pretty straight forward however, it appears that you will be now excluding lots of "BES Cyber Systems" that were identified as CCA's originally and now will be just medium impact BES cyber systems.
4.12	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	The Requirement is sound in and of its self.
4.13	Bonneville Power	Agree	There need to be definitions of "High", "Medium", and "Low" impact. Attachment II describes how to determine whether a system meets the criteria for one of the impacts,

#	Organization	Yes or No	Question 4 Comment
	Administration		but doesn't give an overall explanation of what they mean. The CIP-002-4 draft included level definitions and that was a good idea. That level of detailed definition is not required; that detail is in Attachment II. But, a general impact level definition is needed, for example:"High: Loss of availability of the system leads to an unacceptable risk to the BES. Medium: Loss of availability of the system has a direct impact on the BES.Low: Anything else"These definitions will be used in answering the various questions about the tables.The objective of this requirement ("to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action(s) that the Responsible Entity must take.In Requirement 2 the last phrase is "for the application of Cyber Security requirements . . . ." The last phrase in Requirement 1 is "for the application of security requirements." Are these two phrases supposed to have the same meaning? If so, shouldn't they use identical words? If not, what does "for the application of Cyber Security requirements . . . ." mean? Is it referring to some or all of the requirements in CIP-011-1? If so, it should clearly state that and, if not the entire standard, which specific requirements it is referring to.It seems that it should read as follows: "For the application of the Requirements contained in Standard CIP-011-1 . . . ."
4.14	Western Area Power Administration	Agree	Why is Cyber Security capitalized?
4.15	Independent Electricity System Operator	Disagree	(i) Medium impact categorization is based on an arbitrary generator nameplate rating of 1000 MVA, or voltage level of 200 kV and number of lines, with no regard to actual impact. The same is true of Special Protection Systems. Thresholds should be determined according to studies or other criteria determined by the Reliability Coordinator. As currently drafted, these criteria would significantly reduce the MW currently identified as 'Critical Assets' and protected within our Reliability Coordinator

#	Organization	Yes or No	Question 4 Comment
			area. (ii) The 3 impact levels (H, M, L) create additional layers of management complexity to implement and maintain security processes and monitor compliance, with no commensurate improvement to reliability. Based on the proposed applicability of CIP 11 for H,M & L categories, it seems likely that the number of BES assets afforded the maximum level of protection will decrease from the current standards.
4.16	E.ON U.S.	Disagree	: CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems currently lists 14 "High Impact Ratings" of the categorization of the BES Cyber Systems. E ON U.S. proposes that the Standard include only Control Centers and Backup Control Centers in the High Impact Rating category; all other points listed in the High Impact Rating category should be moved to the Medium Impact Rating category, and all points currently listed in the Medium Impact Rating category should be moved to the Low Impact Rating category.
4.17	BCTC	Disagree	Â Recommend sample BES Cyber Systems be provided for each impact categorization to help guide UtilitiesÂ (Attachment 2) Cost should not be a consideration as the focus is the reliable operation of the BES(Attachment 2) the impact categorizations are good for directing Utilities on how to categorize their BES Cyber Systems ... nice job!
4.18	USACE HQ	Disagree	As same as for question 3, I disagree with the new approach the team is presenting of substituting the risk-based assessment methodology with a list of thresholds to assign risk levels to assets. Again, Order 706, page 70 - 72, recognize the need for risk-based assessment methodology guidance, therefore recognizing that the use of a quantifiable methodology based on risk is the right way to assess criticality of assets or systems present in the community. I suggest that either the team moves back to the original intent in CIP-002 versions 1 - 3 and re-institute the language of risk-based methodology to create the list of BES Cyber Systems OR the team does a risk-based study on the BES to establish real threshold levels to assing risk to the different assets and/or systems in the community.

#	Organization	Yes or No	Question 4 Comment
4.19	Entergy	Disagree	Asset categorization in Attachment II may be valid for any number of purposes, but cyber security is not one of them. Size does not matter in terms of potential adverse impact to the BES as a functioning whole from cyber threats. Connectivity and network navigability are what matter in terms of the ability to adversely affect the bulk electric system through cyber means. Size matters for grid engineering and nominal-state operational grid management, physical security attacks (e.g. terrorist attack), and destruction by weather conditions (e.g. tornado). The cyber attack surface salient to integrity of the BES as a functioning system is primarily where routable protocols (e.g., TCP/IP) are used to connect operating sites, e.g., substations to control centers, regardless of size. The correlation between asset size and potential risk to the functioning BES as a whole is a misapplication of an electrical engineering frame of reference to what is fundamentally a networked-computing security engineering problem. The current approach brings great numbers of asset sites in-scope for required application of cyber defense countermeasures where the threat does not warrant it, e.g., substations of any size that are only connected back to a control/data center using legacy serial communications lines. If the paradigm of size-based impact categorization is to remain in the final Standard, specific requirements also should be established for each different type of network connectivity employed between sites, i.e., routed, legacy serial, dial-up, wired/wireless LAN, etc. One size fits all requirements such as that currently drafted will require overkill in far too many instances relative to genuine threat. As written, the standards are binary in terms of applicability across the spectrum of size-based impact categories, resulting in unnecessary requirements for some asset sites, generally medium impact sites with serial line communications only. This approach is not supported by any evidence in the administrative record. By bringing a large number of low-risk asset sites (i.e., substations using legacy serial communication lines only) into the scope of the requirements, they are imposing significant costs which do not address the real risks. Conversely, too little emphasis in the Requirements is placed upon “low impact” sites where routable protocols are used, which present a clear and present danger for which heightened security measures are certainly warranted.

#	Organization	Yes or No	Question 4 Comment
4.20	Madison Gas and Electric Company	Disagree	Attachment 2 requires clarification. Criteria Number 1.3, per the NERC Glossary, Wide Area is: The entire Reliability Coordinator Area as well as the critical flow and status information from adjacent Reliability Coordinator Areas as determined by detailed system studies to allow the calculation of Interconnected Reliability Operating Limits. Please give and state the reference of "must run" and how entities should interpret what "must run" is. Must run is a market issue, and could be designated as must run but for only a week. Criteria Number 1.11, is the intent that the automatic aggregate load shedding be under a common control system as is stated in the current CIP 002 Standard? If that is the case, adding a comment to clarify the criteria would provide clarity as in criteria 1.2 "(if using a shared BES Cyber System)"?
4.21	IRC Standards Review Committee	Disagree	Attachment II - Impact Categorization of BES Cyber Systems does not recognize that there is another dimension of risk or impact that must be considered. The availability of alternative tools that provide the same functionality should be considered when categorizing these components (e.g. a High Impact BES Cyber System with a viable substitute could reduce it to a Medium Impact).
4.22	Garland Power and Light	Disagree	Attachment II 1.4 Should state that it is the Primary Black Start Unit and does not include the Next Start Unit.1.5 Multiple circuits between two substations should count as a single transmission line.General CommentNeed to add "scoping filter" as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states "typically excludes business, market function systems, and non real-time systems", then it is a good scope and we would agree
4.23	Southern California Edison	Disagree	Attachment II defines the amount of generation under control as the rated capacity of

#	Organization	Yes or No	Question 4 Comment
	Company		the resource. This is not accurate for some systems which can only control the resource between certain points (e.g. minimum operational output [Pmin] and maximum operational output [Pmax]). This could drastically overstate the impact of the cyber system on the BES. For example, suppose that a cyber system controlled a generating resource with maximum capacity of 2,000 MW. According to attachment II, this would then categorize as "high impact rating". However, suppose further that the system can only control the unit between its Pmin and Pmax which are 1,500 and 2,000, respectively. This would place the system in a "low impact rating" according to the attachment. The Attachment II should be modified to account for only the capacity that can be controlled by the system.In addition, Attachment II designates as a high impact rating, "Each BES Cyber System that can affect operations for Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan." This should be clarified to show only BES Cyber Systems will be utilized during the period of time that the resource is providing actual Blackstart service. In SCE's case, if a Blackstart unit is on GMS during normal operating conditions, this should not make it a high impact rating in and of itself. If GMS will be used in the Blackstart plan to restore the system, then it should be included.
4.24	ERCOT ISO	Disagree	Comments: It should be stated that the Responsible Entity is allowed to perform R1 and R2 in the order they deem appropriate. Consider: "Each Responsible Entity shall document categorization of each BES Cyber System identified in Requirement R1. Categorization must address the criteria contained in CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems."
4.25	Tenaska	Disagree	Dependent on R1
4.26	Constellation Energy Control and Dispatch, LLC	Disagree	Disagree based on concerns with Attachment 2. Attachment 2, 1.1. As drafted BES Cyber Systems associated with generating facilities that have a Contingency Reserve obligation lower than their net Real Power capability would be forced to be in the High Impact Rating even though they may be only capable of producing 600 MW. I do not believe the drafting team is intending to capture generators at this capability level. I recommend

#	Organization	Yes or No	Question 4 Comment
			having a specific net real power generation threshold that could result in frequency decay to underfrequency load shedding levels and elimination of the term Contingency Reserve to ensure that a larger threshold is captured.Attachment 2, 1.8 1.8 Transmission Facilities and Generation Facilities are capitalized terms in parts of the draft but not defined terms in the NERC Glossary. Based on their use in the standard a definition should be established. For example, the debate on whether operation of generator interconnection facilities qualifies the operator for transmission operator status may lead to confusion as to who is responsible to categorize Transmission Facilities under this standard.Atachment 2, 1.12, 1.13, and 1.14 - delete and replace with the following: A Control Center that directly operate BES equipment to support the functions (as modified per suggestions) listed in Attachment 1, and whose operation could result in the loss of X MWs in the Eastern Interconnection, X MWs in the Western Interconnection or X MWs in the Texas and Quebec Interconnections. The Interconnection megawatt thresholds should be treated seperatly and not combined.
4.27	Constellation Energy Commodities Group Inc.	Disagree	Disagree based on concerns with Attachment 2. Attachment 2, 1.12, 1.13, and 1.14 - delete and replace with the following: A Control Center that directly operate BES equipment to support the functions (as modified per suggestions) listed in Attachment 1, and whose operation could result in the loss of X MWs in a balancing authorities' interconnection. The Balancing Authority megawatt thresholds should be treated separately and not combined.Request clarification and definition for the term Generation Aggregation and shared BES Cyber System.
4.28	Exelon Corporation	Disagree	Exelon does not agree with all of the specific criteria in Attachment II. Each of the criteria needs to either align with the other existing standard requirements, or have a technical basis or business risk mitigation basis to be defined as criteria. It would be very beneficial to the industry's understanding of each requirement if the basis for each was included in the Attachment or supporting documentation. One result of a deterministic criteria, in terms of a lost MW threshold and assuming all generators employing a common cyber system are lost "in combination" is that detailed studies of cyber impact on equipment are avoided. That is, it is no longer necessary to identify specifically which

#	Organization	Yes or No	Question 4 Comment
			critical assets are affected. With the change in paradigm, a simple identification that a cyber system is common to multiple generators will result in a determination of "High Impact".
4.29	Allegheny Energy Supply	Disagree	Generally agree with intent, however there should be a "None" category in addition to High, Medium, and Low. For example there are likely Cyber Systems on very small generators connected to low voltage transmission that could not have any adverse impact on the BES.
4.30	Oncor Electric Delivery LLC	Disagree	High, Medium, Low is not granular enough. An entity which operates a facility which has no IP based communication should not be required to comply with the cyber security requirements of this proposed standard.
4.31	American Municipal Power	Disagree	I disagree with the structure of CIP-010, but I agree with the intent. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
4.32	Progress Energy - Nuclear Generation	Disagree	If a plant system at a nuclear facility is in scope for NERC CIP Standards, additional categorization is not needed.
4.33	Public Service Enterprise Group companies	Disagree	In general there is agreement with the R2 text. However, in Attachment II, statement 1.4 entails categorizing all Blackstart Units with a "High Impact Rating", while statement 1.6 requires that only the "primary cranking path" transmission facilities need to be categorized with a "High Impact Rating". Statement 1.6 implies that some Blackstart

#	Organization	Yes or No	Question 4 Comment
			Units, although categorized with a "High Impact Rating" would not be afforded transmission facilities with the same risk categorization. We recommend changing statement 1.6 to include only Blackstart Units that are in the primary cranking path.
4.34	National Grid	Disagree	In lieu of the BES NOPR and the exemption process currently proposed, if facilities above 100 kV are exempted by NERC and FERC, will those facilities automatically be exempted from CIP standards? Currently, as per the standards, all the BES systems which are not categorized high impact or medium impact will be defaulted to LOW IMPACT category regardless of how the facility is impacting the Bulk power system. There are facilities >100kV having very localized impact and minimal impact to the reliability of the BES system for which entities will request for exemption. National Grid requests the SDT to clarify this issue.
4.35	Luminant	Disagree	Medium Impact: an item for TO, TOP, GO, GOP Functions performed at primary or backup control centers has been left off of attachment 2. This was in the previous posting as item 2.6"Control Centers and backup Control Centers controlling transmission ... This should be reinstated.
4.36	Matrikon Inc.	Disagree	My suggestion is that the term "system" is replaced with "component", as that is how the security controls of CIP-011 will be applied (to individual cyber components). A typical control system is built of multiple components, and some are more important than others (eg. operator stations versus controllers). As a whole, they work together to control generation or transmission, and identifying impact of each component will help with the application of CIP-011-1.
4.37	Seattle City Light	Disagree	NERC should first assess the effectiveness of the existing standards before proposing replacements. The current Requirements haven't yet had the chance to undergo a full assessment for effectiveness. The impact of adopting CIP Requirements was tremendous and forced utilities to develop and implement new operational processes at a great expense. The first round of CIP Spot Checks is just now underway and is providing the first validation point for interpretations of the standards (and our first

#	Organization	Yes or No	Question 4 Comment
			round of significant penalties.) Utilities are now at a pivotal point in maturing their CIP compliance programs. Drastically changing the requirements now is a common reaction to newly introduced regulatory compliance frameworks and NERC should learn from the mistakes of other regulatory bodies that now have mature compliance frameworks (i.e., PCI, HIPAA, SOX.) Opportunities to further mature and improve the effectiveness of our CIP compliance programs will not happen if the proposed methodology is adopted in the near future. The cost and resource expense will shift to adapting to the new standards which carries a significant opportunity cost from a risk perspective.
4.38	Duke Energy	Disagree	R1 and R2 should be reordered and reworded (see comment on Question #3 above). Also, the quantities identified on Attachment II appear arbitrary, and need an engineering basis. We suggest an approach based upon Violation Risk Factor language, such that for the High Impact Rating, the qualifier should be whether or not the BES Cyber System could directly cause or contribute to Bulk Power System instability, separation, or a cascading sequence of failures, or could place the Bulk Power System at an unacceptable risk of instability, separation, or cascading failures. For the Medium Impact Rating, the qualifier should be whether or not the BES Cyber System could directly affect the electrical state or the capability of the Bulk Power System, or the ability to effectively monitor and control the Bulk Power System, but is unlikely to lead to Bulk Power System instability, separation, or cascading failures.
4.39	San Diego Gas and Electric Co.	Disagree	SDG&E recommends aiming for a limitation of scope related to those assets that are truly high and medium impact categorizations. Some of the high and medium items could have “BES outage” implications but not necessarily result in instability of the BES. We recommend having consistency in the application of the assets included in the impact categories to the BES as a whole. Do the HIGH or MEDIUM impact categorizations consider redundancy and functionally equivalent back-ups? SDG&E recommends that this be taken into account during the categorization process.SDGE is concerned about the sheer number of assets that will be tagged “High impact” with the definitions presented in Attachment II, leading to a much larger compliance workload by entities with these new CIP Standards. Will all of these efforts bring significant additional

#	Organization	Yes or No	Question 4 Comment
			reliability to the BES?In paragraph 1.14, SDG&E has a concern about the last portion of the last sentence that reads "functionality that remotely controls a BES Cyber System with a High Impact Rating." That verbiage has the capability of causing many additional assets to fall in-scope that do not necessarily need to be. Suggest striking those words out of 1.14 since there are other protections in place within other requirements to protect the BES Cyber Systems with a High Impact rating.
4.40	Wolverine Power	Disagree	See comments listed for 1.a
4.41	Manitoba Hydro	Disagree	See comments to Question 3.
4.42	Indeck Energy Services, Inc	Disagree	The Impact Characterization of BES Cyber Systems is arbitrary and overly simplistic. It groups all facilities, regardless of the functions from Attachment I that they may or may not be able to perform and the significance of that type of facility to providing that function, in three arbitrary categories, LOW, MEDIUM and HIGH. The LOW category sweeps too broad a stroke. For generators, it arbitrarily includes, as a minimum, all generators less than 1,000 MW, regardless of type or capability to provide any or all of the functions from Attachment I. For example, one 150 MW generator providing "Controlling Voltage (Reactive Power)" has much less, probably a de minimis level, of support compared to a 999 MW generator. Wind generators are intermittent and non-dispatchable and, unlike dispatchable generators which are almost all running at high loads at high load times, when Controlling Voltage is a problem, are unlikely to be running near full load at those times. The categorization needs to be much more specific to the facility being categorized under CIP-010 and the function to be performed. Although the CIP-010 and CIP-011 are already voluminous, in order to positively affect BES ALR, they need to be restructured to reflect the complexity of the BES and not arbitrarily set LOW, MEDIUM and HIGH categories. [suggestion] There should be 5 categories: VERY HIGH, HIGH, MEDIUM, LOW and VERY LOW based upon the relative impact on the BES ALR, for each of the functions in Attachment I.

#	Organization	Yes or No	Question 4 Comment
4.43	PacifiCorp	Disagree	The initial wording “Each BES Cyber System that can affect operations for” should be clarified or additional clarification added to some of the following items. For example the wording above, together with the wording associated with 1.8 give fairly good guidance, but the wording applied to items 1.4 and 1.5 are not as clear. The wording “affect operations” can have many meanings ranging from minor operational issues to total loss of the facility. The phrase “singularlity or in combination” in Item 1.1 of Attachment II seems to be attempting to incorporate multiple units of an integrated plant, but the parenthetical does not effectively convey that concept. While item 1.1 ties back to the Contingency Reserve and the Reserve Sharing Group, it does not provide definitive guidance regarding which Facilities are meant to be incorporated into the requirement since this value is not easy to obtain and may by definition change year to year. Also, item 1.3 seems to be an “either/or” catch-all related to item 1.1, but there is no indication of who determines which units are “must-run” units. It is unclear how A BES Cyber System, if rendered unavailable, degraded, compromised, or misused, within 15 minutes, cause a disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES could fall into anything other than High or Medium impacts.
4.44	US Bureau of Reclamation	Disagree	The language in the requirement needs to be cleaned up as follows: "Each Responsible Entity shall catgorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachement II - Impact Categorization of BES Cyber Systems." The remaining parts of sentence should be deleted.
4.45	Detroit Edison	Disagree	The phrase “to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES” at the end of R2 is a restatement of the purpose of CIP-010 and should be removed. Consider changing R2 to:Each Responsible Entity shall categorize and document such categorization of each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II - Impact Categorization of

#	Organization	Yes or No	Question 4 Comment
			BES Cyber Systems.
4.46	Progress Energy (non-Nuclear)	Disagree	This is a good approach to apply protection based on an impact level vs. an all or nothing approach. The trigger levels (MW, MVar, etc) need to be reassessed - are these realistic / practical? This requirement is going to involve extensive effort and coordination between work groups. The DSCADA master that could control all T/D substation capacitor banks would be included. The term misused shows up a couple more times in Attachment II. It would appear that 1.11 includes the T/D Substation under frequency relaying. This is installed in almost every T/D substation which would require some level of access control.What is a generation facility versus a unit?Do we need to identify each cyber component of the BES Cyber System or just the (sub)system itself? Our interpretation of R1, R2, & R3 is that the requirements are driving us to identify Cyber subsystems. If we design small Cyber subsystem architectures we could get to Low impact categorization for each defined subsystems?Are the requirements aimed at subsystem level or overall system? An example would be to design a simple cycle Cyber system (Siemens T3000) architecture for combustion turbines alone and a second Cyber system (Ovation) for the balance of plant. We can make these independent systems at the process level and thereby minimize their respective impacts on the BES. Is that NERC's intent?
4.47	Southwestern Power Administration	Disagree	This requirement seems to be an excellent candidate for performance/results-based criteria rather than numerous bright line requirements that may or may not actually have a significant effect on the BES, depending on the surrounding topology, operating procedures, or configuration of a particular Responsible Entity.
4.48	MWDSC	Disagree	Unclear how much supporting documentation or explanation is required to demonstrate how your system applies or doesn't apply to each of the subcategories. For example, would a table with "yes", "no", or "not applicable" and certified by a SME be sufficient?
4.49	Turlock Irrigation District	Disagree	We agree with the principle of the Requirement, however, we disagree with some of the

#	Organization	Yes or No	Question 4 Comment
			High Impact Rating criteria in Attachment II, as explained in question 7 below.
4.50	Midwest ISO	Disagree	We do not believe the drafting team has developed a justification for moving away from the Critical Asset concept. We understand that the regulators have a concern about the level of Critical Assets identified but that could mean the criteria simply needs to be more stringent for selecting Critical Assets. If the categorization approach is maintained, at a minimum, a no or negligible impact category should be adopted. There are BES Cyber Systems that simply cannot have an impact on reliability and therefore the CIP standards should not apply to them.
4.51	Ameren	Disagree	We generally agree with the criteria used to identify "High" impact facilities, but believe that the item 1.5 criterion should be expanded to include EHV transformers, and not limited to 4 EHV lines. However, there are too many EHV facilities in item 2.6 that would be classified as "Medium" impact, but should be classified as "Low" impact. It is suggested that EHV facilities with three or less EHV lines and transformers should be considered as "Low" impact, as they likely have little impact on the BES.
4.52	Verizon Business	Disagree	In Attachment II, Item 1.1 regarding Generation Facilities, references to "Contingency Reserve" or "Reserve Sharing Group" should be removed. Specifically, any Generation Facility, singularly or in combination with aggregate higher than 2,000 MW, should be included as a High Impact Rating. Referring to the "Contingency Reserve" is confusing and could result in the incorrect or inconsistent declaration of a generation asset as a High or Medium impact.

5. **Requirement R3 of draft CIP-010-1 states, "To ensure the application of adequate requirements on its BES Cyber Systems, each Responsible Entity shall:**

   3.1 review the identification and categorization of its BES Cyber Systems within 36 months of the last identification and categorization

   3.2 review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it owns

   3.3 update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of such change to the BES."

   Do you agree with the proposed Requirement R3? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Many entities expressed concerns about the requirement to review the categorization following a planned change. Others expressed concerns again on the emphasis on ownership, but asked for the addition of "or operates".

In response to these comments, the requirement has been restructured, separating changes to the BES and categorization, and periodic reviews and approvals. More specificity has been added in the requirements as to when the categorization has to be updated upon a change. The SDT continues to believe that owners should be responsible for compliance and that the responsibility to operators should be the subject of agreements between the owners and operators.

#	Organization	Yes or No	Question 5 Comment
5.1	Progress Energy (non-Nuclear)		Agree that there needs to be a periodic review set cycle as well as a process to assess the impact for current projects. One concern could be how we deal with multi-phase projects that may extend over years.3.2 should not require that the whole identification and categorization process be redone for any 'planned changed'. Suggest changing the wording to 'review the identification and categorization of its affected BES Cyber Systems as a results of any planned change to the portion of the BES that it owns.'
5.2	MWDSC		Although R3 generally appears reasonable, cannot comment on specified times until all the requirements are finalized.

#	Organization	Yes or No	Question 5 Comment
5.3	National Rural Electric Cooperative Association (NRECA)		In R 3.3, please provide an explanation on "when applicable" -- explain this so that both the auditor and a registered entity can understand the "when applicable" circumstances.In R 3.3, what is meant by "such change" -- is it referring to actions related to R 3.1 and 3.2? If yes, ensure the standard is clear about this in order to minimize confusion about what is required.
5.4	Arizona Public Service Company		Potential confusion may exist without guidance or criteria that indicate how, specifically, a BES Cyber System Component should be identified. This is a problem of specificity in uniquely identifying a Component versus generically categorizing types of Components. This also relates to CIP-011 R23 and the inventory. Some potential options for specificity include manufacturer, model, serial number, assigned name or unique identifier, and location (logical and/or physical). Concerns with inventory management and uniquely identifying include how to better determine if a Cyber System Component has been modified or replaced with a different one, etc.
5.5	FEUS	Agree	3.2 is not clear when the entity is required to review the identification and categorization as a result of a planned change. 3.3 require documentation to be updated relative of changes from R1 and R2 within 45 calendar days. The drafting team should consider clarification for 3.2 either prior to implementation/completion of the planned change or within xx days.
5.6	Constellation Energy Commodities Group Inc.	Agree	Add a materiality component in 3.2.; review identification and categorization of BES Cyber Systems upon significant planned changes. Also recommend adding provisions for re-evaluating new systems prior to going live.
5.7	Constellation Energy Control and Dispatch, LLC	Agree	Add a materiality component in 3.2.; review identification and categorization of BES Cyber Systems upon significant planned changes.
5.8	WECC	Agree	Agree with the general requirements, but for clarity and auditability the following rewrite is suggested.R3 Perform a documented review the identification and categorization of its BES Cyber Systems within 36 months of the last identification and

#	Organization	Yes or No	Question 5 Comment
			categorization. R4 Perform a documented review the identification and categorization of its BES Cyber Systems as a result of any planned or unplanned change to the portion of the BES that it owns.R5 Update or reaffirm the documentation specified in Requirements R1 and R2 within 45 calendar days from the completion of reviews as required by R3 and R4.Also suggest that the SDT consider requiring documentation be updated PRIOR to completion of the change.
5.9	Florida Municipal Power Agency	Agree	Although FMPA agrees with the intent of this requirement, we believe that 3.2 and 3.3 are duplicative and confusing from a monitoring perspective. We also note that there seems to be a gap for significant changes to BES Cyber Systems. In addition, ownership of BES Facilities seems to be the incorrect determining factor, especially since the definition of BES Cyber Systems is focused on operations and it would seem that the focus ought to be on the BES Cyber Systems owned by the System Operator to operate the BES within its operational scope. FMPA recommends deleting 3.3 and replacing 3.2 with the following:"3.2 Review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it operates. The effective date of any changes to BES Cyber System identification or categorization shall be the in service date of such change."Such language would result in the need to plan ahead of time and ensure the documentation is developed, but not necessary implemented until the in- service date of the new equipment.FMPA also recommends adding a new 3.3 to address significant changes to BES Cyber Systems that may impact identification and categorization, such as:"3.3 Review the identification and categorization of its BES Cyber Systems as a result of change in BES Cyber System configuration or scope. The effective date of associated changes to BES Cyber System identification or categorization shall be the in service date of such change."
5.10	Minnesota Power	Agree	Minnesota Power recommends the following wording change to increase the clarity of Part 3.2, "...as a result of any planned and implemented change..."
5.11	PNGC-Cowtitz-Central Lincoln-Benton-Clallam	Agree	Need to clarify what is required for temporary situations, such as a normal open closed to allow maintenance. The closing of the open would be a "planned change," but only

#	Organization	Yes or No	Question 5 Comment
	Group		temporary. The Change in status of a BES Cyber System would be a wasted compliance effort for only a short duration.
5.12	US Army Corps of Engineers, Omaha Distirc	Disagree	"planned change" in 3.2 needs to be qualified. Suggest changing to "planned change likely to alter the impact of the associated BES cyber systems." Changes to BES Cyber Systems that could change their impact on the BES should also be considered.
5.13	Covanta Energy	Disagree	3.1 - If no changes have been made to any BES Cyber Systems, would suggest changing review period from 36 months to 60 months.... need to reduce administrative activities to allow more focus on reliability based activities.
5.14	Duke Energy	Disagree	3.1 is part of change control. Do we still need this review? Also, 3.2 implies that ALL BES Cyber Systems would need to be reviewed as a result of any planned change to the portion of the BES that it owns. Need to bound this review to only BES cyber systems that are affected by the change.
5.15	Southwest Power Pool Regional Entity	Disagree	3.2 assumes that the BES Cyber System owner is also the owner of the BES assets being changed. This is not always the case. There are, for example, numerous instances where the Balancing Authority, Transmission Operator, and / or Generation Operator is not the Transmission and / or Generation Owner. Some sort of mandatory coordination is required to avoid this important requirement from falling through the cracks. 3.3 only requires a documentation update to be completed upon a change to the BES. This requirement should be modified to also require a documentation update upon a change to the BES Cyber System configuration, including adjustments to the list of components and supporting networks.
5.16	LCEC	Disagree	3.2 Change "owns" to "owns or operates". "Any planned change" may not be signficant enough to justify a full review.
5.17	Hydro One	Disagree	A local definition of “planned change” is needed. Suggest this definition excludes planned outages or maintenance. “Modification to facilities” as used in FAC-009 should

#	Organization	Yes or No	Question 5 Comment
			be considered.
5.18	Northeast Power Coordinating Council	Disagree	A local definition of “planned change” is needed. Suggest this definition excludes planned outages or maintenance. “Modification to facilities” as used in FAC-009 should be considered.
5.19	BCTC	Disagree	Â Preference would be to retain the current process of an annual review BES Cyber Systems and impact categorizationsÂ Please consider that if a change occurs that results in a BES Cyber System’s impact categorization increasing (i.e. from medium to high) the resulting effort to bring this system into compliance could be substantial (i.e. 6 to 12 months); how are these types of scenarios covered under Version 4?
5.20	USACE - Omaha Anchor	Disagree	A) 3.2 - any planned changes to the “cyber-system” portion of the BES that it owns. Otherwise you would be continually reviewing the plansB) 3.1 - would prefer to strike 3.2 and change 3.1 to 12 months.
5.21	Ameren	Disagree	Ameren feels that 45 days is too short and is also an uneven boundary that is hard to track. We would recommend changing it to a more even boundary such as bi-monthly (60 days) or quarterly (90 days). In the case of a complex merger or acquisition between responsible entities there needs to be additional guidance, longer timelines established, etc. to allow sufficient time before and/or after the completion of the transaction for compliance to be achieved and implies a perfectly complied with Configuration Change Management Program. Suggest adding “or as a result of the periodic review” at the end of R3.3.
5.22	E.ON U.S.	Disagree	CIP-010-1, R3.2 creates arguments that parties must constantly assess and re-assess their Impact Ratings of facilities. This is particularly true given that changes to the BES occur on a daily basis. Parties should be permitted expressly to engage in an annual assessment and a reassessment should only be required for “any major planned change to the portion of the BES that it owns prior to implementation of such plan.”CIP-010-1, R3.3 should read, “Update, when applicable, the documentation specified in

#	Organization	Yes or No	Question 5 Comment
			Requirements R1 and R2 within 45 calendar days of the completion of such major changes to the BES."
5.23	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
5.24	PacifiCorp	Disagree	Comments: The term "Any any planned change" used in 3.2 is terribly open-endedshould be more specific to avoid including small planned changes that have a de minimis impact on the identification and categorization of BES Cyber Systems. There must be some operationally prudent, de-minimus changes that can be made without triggering the 45 day change reviewIn addition, PacifiCorp suggests the following:. Change Modify item 3.3 to state Update documentation specified in Requirements R1 and R2 within 45 calendar days of any categorization changes caused by modifications to the BES.
5.25	Black Hills Corporation	Disagree	Define "change" in terms of those alterations to BES Cyber Systems which may modify the functional identification or an impact categorization. There are numerous minor changes which clearly will not change either Attachment I or II assignments and would not need to be tracked. If they are not tracked, an entity will not be able to prove compliance.
5.26	Exelon Corporation	Disagree	Exelon is concerned that this Requirement implies that each BES Cyber System Component will need to be classified as High, Medium or Low Impact. If this is the case, this will result in a major change management initiative with field personnel and add unnecessary administrative burden and expense with no resulting benefit to the reliability of the BES. Given that concern, Exelon suggest that Requirement 3.2 be modified to read "review the identification and categorization of its applicable BES Cyber Systems as a result of any planned change to the portion of the BES that it owns." Exelon has several concerns as to how this Requirement would be audited. As written, Requirement 3.2 could be interpreted to mean that ANY change to the BES, whether it impacted a BES Cyber System or not, would necessitate a 45 day review and documentation. Furthermore, what is the definition of "planned"? Exelon is concerned

#	Organization	Yes or No	Question 5 Comment
			that like-for-like emergent equipment replacements would likewise necessitate a 45 day review and documentation.
5.27	Dominion Resources Services, Inc.	Disagree	Extending the window for periodic validation of the identification and categorization of BES Cyber Systems is an improvement given the additional requirement to review the impact of planned changes. The current language implies that all identified and categorized BES Cyber Systems must be reviewed each time a change occurs to any single system, although the intent is only to determine the impact of the change. How that determination is made should be at the discretion of the Responsible Entity. The wording for R3.2 should be changed to more accurately represent the intent as follows:"...determine whether planned changes to the portion of the BES it owns, requires the identification of additional BES Cyber Systems or changes or impacts the categorization of any existing BES Cyber System."
5.28	ReliabilityFirst Staff	Disagree	For clarity, ReliabilityFirst suggests the following revision to the language of these requirements, 3.2 ". . . of any planned change to the portion of the BES that it owns or operates", 3.3 "Update within 45 calendar days, the documentation specified in Requirements R1 and R2 when the review required in 3.1 or 3.2 indicates a change."
5.29	MRO's NERC Standards Review Subcommittee	Disagree	For item 3.2, we believe the word "planned" should be replaced with "incorporated". Otherwise, an entity could end up identifying and categorizing BES Cyber Systems that never actually end up getting installed.
5.30	Oncor Electric Delivery LLC	Disagree	High, Medium, Low is not granular enough. An entity which operates a facility which has no IP based communication should not be required to comply with the cyber security requirements of this proposed standard.
5.31	American Municipal Power	Disagree	I agree with the intent, but I disagree with the structure of CIP-010. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will

#	Organization	Yes or No	Question 5 Comment
			be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
5.32	Constellation Power Source Generation	Disagree	It seems the intent of R3.2 and R3.3 is to review and document any changes to a BES Cyber System that an entity owns, but instead it states "a change to the BES." An ownership change of a generation facility, or the change of an electromechanical overcurrent relay to a microprocessor overcurrent relay would change a BES Cyber System, but that doesn't change the BES. These requirements need to be rewritten to state BES Cyber Systems in place of BES.
5.33	Green Country Energy	Disagree	It would be nice to add a bit more definition to the timeframe. 3.1 within 36 months of last completed identification... 3.3 within 45 days of approved completion of such change...
5.34	Luminant	Disagree	Item 3.2 is unclear and very broad. Any planned change to the BES that it owns could simply be the changeout of an oil pump or boiler tubes. Luminant proposes two possible fixes. First, limit the review to changes that impact the BES Cyber Systems, or impact the High, Medium or Low rating. Even this is problematic in execution and enforcement. S
5.35	MidAmerican Energy Company	Disagree	Item 3.3 is not clear what does "update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of such change to the BES." mean. Change item 3.3 to state Update documentation specified in Requirements R1 and R2 within 45 calendar days of any categorization changes caused by modifications to the BES.
5.36	National Grid	Disagree	National Grid recommends a local definition of "planned change". Also, clarify if planned change refers to an "approved" change. There are scenarios when planned changes are

#	Organization	Yes or No	Question 5 Comment
			not approved by Senior Management for various reasons. Should the planned change still be “reviewed”? What about “unplanned changes”?
5.37	NextEra Energy Corporate Compliance	Disagree	NextEra suggests combining 3.2 & 3.3 as follows:3.2 For any planned change that results in a BES cyber system re-categorization (low, medium, high) the documentation specified in R1 & R2 will be updated within 45 days of the completion of such change.NextEra also suggest eliminating or specifically defining what constitutes a change that needs to be documented, such as a hardware modification, or change to network connectivity.
5.38	Progress Energy - Nuclear Generation	Disagree	Nuclear facilities are required by multiple the Code of Federal Regulation (CFR)requirements to maintain configuration control of components. Plant systems and components subject to Cyber Security regulation, either by FERC/NERC or other regulatory agencies are maintained under configuration control due to the CFR programs. Revisiting the classification of assets is not needed to enhance configuration control as on-going design control and configuration management processes are applied to meet the legal requirements implemented by CFR.
5.39	The United Illuminating Co	Disagree	Proposed R3.3 uses the term “such change to the BES” is not clear. The use of the phrase leads to the belief it applies only to 3.2, Did the SDT intends R3.3 to apply to both R3.1 and R.32?Suggest rewording 3.3 to: Update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of reviews required by R3.1 and R3.2.
5.40	Pacific Gas & Electric Company	Disagree	R 3.2 Understand the overall intent of 3.2, however "...any planned change to the portion of the BES..." essentially occurs on a daily basis so unclear on the overall feasibility of this requirement. Suggest 3.2 be more refined than "any planned change to the portion of the BES".
5.41	Reliability & Compliance Group	Disagree	R3.1 is unnecessary with a proscriptive program for identifying BES cyber systems. Therefore, you should only need to review the identification and categorization of your BES cyber systems if there is a planned change to the system or if there is a change to

#	Organization	Yes or No	Question 5 Comment
			the standard's definition of what is or is not a BES cyber system or system component.
5.42	American Electric Power	Disagree	R3.2 and R3.3 are triggered from changes to the BES. Depending upon what constitutes a change to the BES, there could be daily triggering events that would require the review and updates as stated in these two requirements. Will every BES Cyber System (including those not associated with the BES change) need to be reviewed and possibility updated for each and every change to the BES?Furthermore, it appears that it would be possible that a Responsible Entity could be in violation of R3 the Responsible Entity could also be in violation of R1 and/or R2 as well. It appears that R1 and R2 are one-time initial events and that R3 is the on-going requirement replacing those events; however, if that is the intent it is not clear in that regard.
5.43	Consultant	Disagree	R3.2 'any' planned change is probably too broad. Should include addition or removal of BES assets, whether by construction, retirement, purchase, or sale of assets. Some qualification of the changes BES assets that would require review of the identification and categorization of a BES asset would be better. Possible wording "changes to cyber systems or physical protection cyber systems associated with BES assets...", which would appear to be consistent with R23 in CIP-011.Possible "unintended consequence" - requirement R3.2 as stated, and in the suggested changes, requires change control for all BES cyber assets regardless of impact categorization.
5.44	SCE&G	Disagree	R3.2 needs to be clarified regarding "any planned change to the portion of the BES that it owns". What constitutes a change? Is this a Transmission/Generation factility change, operational change, or a cyber systems change, or all three? This has the potential to be interpreted by auditors as needing to be reviewed anytime equipment is replaced.
5.45	Madison Gas and Electric Company	Disagree	R3.2 states " review the identification and categorization of BES Cyber Systems of any planned change to a portion of the BES that it owns". It is unclear how an entity will accomplish a review of a "planned" change. Recommend the "planned" be removed and supplement with "incorporated". R3.2 should read as:"review the identification and categorization of its BES Cyber Systems as a result of any incorporated change to the

#	Organization	Yes or No	Question 5 Comment
			portion of the BES that it owns".
5.46	ERCOT ISO	Disagree	R3.2: Consider: review and document the identification and categorization of its BES Cyber Systems as a result of any planned change to its BES Cyber Systems or BES Cyber System ComponentsR3.3: Recommend that the 45 days be changed to 30 days to align with the changes recommended under FERC Order 706 (i.e., section 651).
5.47	BGE	Disagree	Recommend adding provisions for re-evaluating new systems prior to going live.
5.48	ISO New England Inc	Disagree	Recommend that a local definition of "planned change" is needed. Suggest this definition excludes planned outages or maintenance. Possibly use "modification to Facilitiies" per FAC-009 as a starting point.
5.49	Detroit Edison	Disagree	Remove the "planned change" verbiage in R3.2. Consider changing R3 subrequirement 3.2 to:Each Responsible Entity shall: 3.2 Review the identification and categorization of its BES Cyber Systems as a result of any change to the portion of the BES that it owns that affects the classification of a BES Cyber System or causes the addition or removal of BES Cyber Systems
5.50	Nuclear Energy Institute	Disagree	Requirement 3.2 implies that ALL BES Cyber Systems would need to be reviewed as a result of any planned change to the portion of the BES that it owns. Need to bound this review to only BES cyber systems that are affected by the change. Also, it would be helpful to clarify the term "change" to preclude the triggering of a review for something like a password change.Additionally, the phrase "adequate requirements" in the R3 introductory paragraph should be clarified to "adequate security requirements."
5.51	Southern California Edison Company	Disagree	SCE's concerns regarding Requirement 3.2 are three-fold: (1) Requirement 3.2 appears to require review of all BES cyber systems whenever any change in ownership of any portion of the BES occurs. SCE recommends the drafting team clarify that the review should only occur for systems that are impacted by the ownership change.(2) It is unclear whether Requirement 3.2 adds significant value to the reliability of BES because

#	Organization	Yes or No	Question 5 Comment
			planned changes may not be always approved or implemented as designed and actual changes made would, regardless, have to be documented by R3.3 within 45 calendar days.Finally, the drafting team should make the period after an unplanned change "time-bound" obligating RE's to develop plans to address compliance with CIP standards within a specific timeframe after which R3.2 would become applicable. This approach would be in agreement with the intent of Order 706 which places paramount importance on the reliability of the BES. It is also unclear from this requirement that the timeframe within which a system or component identified in R3 has to adhere to CIP-011. Such a timeframe should be clearly stated within the standard.
5.52	San Diego Gas and Electric Co.	Disagree	SDG&E doesn't necessarily have issues with the 36-month review requirement in R3.1. However, we do have a concern about the 45-day requirement in R3.3 due to the sheer number of BES Cyber Systems that could change. We suggest that this requirement be changed to 90 days so that entities will have adequate time to update appropriate documentation.
5.53	Network & Security Technologies Inc	Disagree	Suggest adding a requirement to review the identification and categorization of its BES Cyber Systems as a result of any planned changes to one or more of its BES Cyber Systems. "Planned changes" include but are not limited to hardware and/or software upgrades adding new functionality, addition of new BES Cyber Systems, retirement or redeployment of existing BES Cyber Systems.
5.54	Allegheny Energy Supply	Disagree	Suggested modification to 3.2:review the identification and categorization of its BES Cyber Systems as a result of changes to the portion of the BES that it operates.
5.55	Allegheny Power	Disagree	Suggested modification to 3.2:review the identification and categorization of its BES Cyber Systems as a result of changes to the portion of the BES that it operates.
5.56	Dynegy Inc.	Disagree	The 3.3 update should be extended to 6 months. This type of update could be detailed and require more than 45 days.

#	Organization	Yes or No	Question 5 Comment
5.57	APPA Task Force	Disagree	The APPA Task force agrees with some parts of the proposed requirement but we offer the following suggestions:We believe that 3.2 and 3.3 are duplicative and confusing from a monitoring perspective. We also note that there seems to be a gap that does not cover significant changes to BES Cyber Systems. In addition, "ownership" of BES Facilities seems to be the incorrect determining factor, especially since the definition of BES Cyber Systems is focused on operations. It would seem that the focus ought to be on the BES Cyber Systems owned by the System Operator that it uses to operate the BES within its operational scope. We recommend deleting 3.3 and replacing 3.2 with the following:"3.2 Review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it operates. The effective date of any changes to BES Cyber System identification or categorization shall be the in-service date of such change."Such language would result in the need to plan ahead of time and ensure the documentation is developed, but that it need not be implemented until the in- service date of the new equipment.We also recommend adding a new 3.3 to address significant changes to BES Cyber Systems that may impact identification and categorization, such as:"3.3 Review the identification and categorization of its BES Cyber Systems as a result of change in BES Cyber System configuration or scope. The effective date of associated changes to BES Cyber System identification or categorization shall be the in-service date of such change."
5.58	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The change management requirements of CIP-011 necessitate lengthening the time to document completed changes to 60 days or more.
5.59	ReymannGroup, Inc.	Disagree	The dynamic and real-time nature of cyber security threats requires a minimum review cycle for identifying and classifying new or changing BES Cyber Systems to 12 months or less as determined by planned or unplanned changes to the BES. Therefore, we recommend revising 3.1 to a 12-month cycle and revising 3.2 to include planned and unplanned changes.

#	Organization	Yes or No	Question 5 Comment
5.60	Bonneville Power Administration	Disagree	The objective of this requirement ("To ensure the application of adequate requirements on its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence. The Requirement should not include the objective. That would clearly separate the objective from the action(s) that the Responsible Entity must take.3.2 doesn't define the magnitude of "planned change". As defined, it includes routine maintenance such as replacing conductors on a line. A better definition would be "...planned change to the architecture of the portion...". In any event, there must be some way for entities to determine which change triggers a review.
5.61	Manitoba Hydro	Disagree	The requirement needs to include a review of the categorization of the BES Cyber System as a result of a change in the BES Cyber System. Is the intent of Requirement 3.2 to review the identification and categorization of ALL its BES Cyber Systems as a result of ANY planned change to the portion of the BES that it owns? If so, this is excessive and should be limited to BES Cyber Systems impacted by the planned change. If the intent is to limit the review in Requirement 3.2 to the BES Cyber Systems impacted by the change, then the 36 month review in Requirement 3.1 could be continually reset, and an overall review never completed. The period for an overall review should be a fixed interval of every 36 months. Requirement 3.3 language is vague when referring to "such change". If the intent is to update the documentation in when triggered by events in 3.1 and 3.2, then the language of 3.3 needs to be added to both 3.1 and 3.2. As a result, 3.3 can be deleted. Requirement R3.3 is incomplete or inconsistent as drafted. The first portion of Requirement R 3.3 refers to updating documentation specified in Requirements R1 and R2, which includes a 3 year review, yet the latter portion of Requirement 3.3 specifies that updating must be done within 45 days of a change. It is not clear when updates must be done after a three year review.
5.62	Alberta Electric System Operator	Disagree	The wording of R3.3 implies it is a sub-requirement of R3.2 because of the wording "such change." Consider revising to "... within 45 calendar days of the completion of such review."

#	Organization	Yes or No	Question 5 Comment
5.63	EEI	Disagree	There are no boundaries around what constitutes a change to the BES in R3.2 and R3.3. As written, every change to a breaker setting in a BES substation would cause the RE to have to perform a review. The requirement should be rewritten so that only changes which cause a reclassification under Attachment II should be included in this requirement. In addition, the review period should be specified as 45 days from deployment of the change. The change has to be material to the classification criterion in Attachment 2 in order to trigger a review.As noted in EEI's response to Question 3, a Responsible Entity may not need to characterize all the BES Cyber Systems it owns (for example, jointly owned units). EEI suggests the following modification to 3.2:"review the identification and categorization of its BES Cyber Systems as a result of material changes to the portion of the BES that it operates."
5.64	Southern Company	Disagree	There are no boundaries around what constitutes a change to the BES in R3.2 and R3.3. As written, every change to a breaker setting in a BES substation would cause the RE to have to perform a review. The requirement should be rewritten so that only changes which cause a reclassification under Attachment II should be included in this requirement. In addition, the review period should be specified as 45 days from deployment of the change.R.3.2 requires the review of identification and categorization for planned changes. R3.3 requires an update of documentation related to these changes within 45 days of completion. The requirements of R3.2 would be difficult to audit and are better covered under R3.3.
5.65	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
5.66	Independent Electricity System Operator	Disagree	We agree with R3 and its sub-requirements except R3.2. Specifically, we do not agree with the term "the portion of the BES that it owns" since some Responsible Entities do not own any BES facilities. We suggest replacing this term with "the portion of the BES that it owns or operates".

#	Organization	Yes or No	Question 5 Comment
5.67	IRC Standards Review Committee	Disagree	We agree with R3 and its sub-requirements except R3.2. Specifically, we do not agree with the term "the portion of the BES that it owns" since some Responsible Entities do not own any BES facilities but do own Cyber Systems with which they operate the BES. We suggest to replace this term with "the BES Cyber Systems or the portion of the BES that it owns".
5.68	GTC & GSOC	Disagree	We are concerned with requiring an update of all BES Cyber System categorizations whenever planned changes are made to the BES. First, there is a gap here with respect to capturing the changes to the BES Cyber Systems themselves that may affect categorization. Also, this will likely create a complicated compliance tracking scenario for the entity who will be required to track a number of activities to ensure they are completed "within 12 months" of the categorization. We recommend replacing "within 36 months" in R3.1 with "annually" and completely removing both R3.2 & R3.3. This will allow the tracking of compliance activities to occur more on a programmatic basis rather than necessarily on a device by device basis.
5.69	Xcel Energy	Disagree	We believe 60 days is a more appropriate time to allow updating of document under Requirement 3.3. During certain times of the year, (i.e. end of year holidays and financial close out activities) 45 days can be challenging.
5.70	Alliant Energy	Disagree	We believe Article 3.1 is unnecessary and should be deleted. If an entity does an initial assessment and identifies and categorizes its BES Cyber Systems, the only time there would be a change to the listing is if the BES Cyber Systems were modified, which is covered in Articles 3.2 and 3.3. If the SDT determines that Article 3.1 is required, the timeframe should be revised to 60 months to correspond to other summary reviews required by NERC (ie; 5-year analysis of Black-Start capabilities).In Article 3.2 the word "planned" should be replaced with "installed" or "incorporated". There are many modifications planned that never get installed, so it is not reasonable to require all "planned" items to be included.In Article 3.3 the update period should be 90 days not 45, to allow the Registered Entity time to make the necessary changes. 45 days is not

#	Organization	Yes or No	Question 5 Comment
			adequate time to do the updates at the end of a project.
5.71	FirstEnergy Corporation	Disagree	We do not agree with the VRF of High assigned to this requirement and believe a Medium VRF is more appropriate. Violating R3 does not pose the same risk to the BES as violating R1 and R2.As written, 3.2 implies that every change to the BES would trigger a documented review of the cyber system list and becomes a burdensome compliance task. As a compromise we propose that you simplify R3 such that a review/update is required every 18 months.
5.72	We Energies	Disagree	We Energies agrees with EEI suggested modification to 3.2:"review the identification and categorization of its BES Cyber Systems as a result of changes to the portion of the BES that it operates."
5.73	Midwest ISO	Disagree	We request that 3.3 be modified to 60 days rather than 45 days. We believe 45 days will be a challenge for most entities to meet as this effort will likely be incorporated into an entity's broader business continuity efforts.
5.74	Verizon Business	Agree	The requirement should provide guidance relating to when a utility needs to add a new BES system or component and what the timelines are for implementation of the CIP-010, R3 requirements.

6. CIP-010-1 Attachment I contains a listing and brief description of Functions Essential to Reliable Operation of the Bulk Electric System. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

Summary Consideration:

Many entities expressed concerns that Attachment I is part of the standard and includes the use of many undefined terms. Others expressed concerns about the vagueness of many of the terms.

In response to these comments, the SDT has changed the definition of the Reliability Functions to **BES Reliability Operating Services**, and has included these terms in the Glossary. Some modifications have been made to more precisely define the context in many sub-definitions.

#	Organization	Yes or No	Question 6 Comment
6.1	Madison Gas and Electric Company		Recommend eliminating the word "conditions" used in the descriptions of the functions. It's not clear what "conditions" means in the context in which it is used in Attachment I. A function is a set of activities and actions to accomplish an objective or purpose. Such activities and actions may be automatic or manual or a combination of the two and certain tools and infrastructure may be inherently needed to fully execute the functions. In contrast, conditions are states that result from the execution of functions and/or the effects of external, sometimes uncontrollable, factors.Recommend Function section to read:CIP-010-1 - Attachment I Functions Essential to Reliable Operation of the Bulk Electric System The following operating functions are essential to real-time reliable operation of the Bulk Electric System (BES). To define the scope of applicability of CIP Standards, the functions of relevance are only those that can have an effect on real-time operation of the BES within 15 minutes. Dynamic Response - Actions performed by BES elements or Facilities which are automatically triggered to initiate a response to a BES activity or action Balancing Load and Generation- Activities and actions for monitoring and controlling generation and load. Controlling Frequency (Real Power)- Activities and actions to control frequency within defined bounds. Controlling Voltage (Reactive Power) - Activities and actions to control voltage within defined bounds. Managing

#	Organization	Yes or No	Question 6 Comment
			Constraints- Activities and actions to maintain operation of BES elements within their design limits and constraints. Monitoring & Control - Activities and actions that provide monitoring and control of BES elements. Restoration of BES- Activities and actions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Situational Awareness - Activities and actions to assess the current, expected, and anticipated state of the BES. Inter-Entity Real-Time Coordination and Communication- Activities and actions for real-time coordination and communication between Responsible Entities' System Operators.
6.2	ISO New England Inc	No	- Recommend "30 minutes" to align with EOP standards- Please provide background for where the 15 minute recommendation came from
6.3	Progress Energy (non-Nuclear)	No	A concern is that depending on how we identify the BES, the 'monitoring & control' function may be associated with many transmission lines that utilize microprocessor relays. Based on the definitions of BES Cyber System Component and the monitoring and control function, this could be interpreted as to being in consideration regardless of whether or not we connect communications to the relay.CIP-010-1 Attachment I - More guidance needed - There needs to be guidance on the definition of 'can have an effect on real-time operation of the BES within 15 minutes'. This leaves too much ambiguity in defining the Cyber Systems that could potentially be covered by the standards and at which level. It could even be interpreted to include systems which may even be beyond the control of the Responsible Entity. The definition needs to provide a bright line of distinction so that systems which have the highest potential of presenting a risk receive the greatest attention to enhanced security - rather than requiring finite resources to be spent filling notebooks with information about low risk Systems/Components.
6.4	Duke Energy	No	Attachment I should not be part of the standard, but should be in a guidance document.
6.5	Kansas City Power & Light	No	Do not agree with the "Inter-Entity Real-Time Coordination and Communication" as the description appears directed toward the devices and systems utilized for verbal communications between Regional Entities and the coordination that occurs as a result

#	Organization	Yes or No	Question 6 Comment
			of those interactions and is outside of the scope of cyber control systems that monitor and control the BES.
6.6	Con Edison of New York	No	One general comment is that CIP-010 should avoid using undefined terms, and use NERC Glossary Terms and cross-references to other Reliability Standards wherever possible.Attachment I is a list of "Functions Essential to Reliable Operation of the BES". The DT has attempted to re-define functions that are already documented in Standards. The definitions should be enhanced to reference the applicable Reliability Standards. o Dynamic Response: The only actions automatically triggered on BES elements are protection systems (see PRC Standards), UFLS systems (see PRC Standards), AGC systems (see BAL Standards), Special Protection Systems and AVR's (see VAR Standards). Everything else is manual operation. It is recommended that the term "Dynamic Response" be removed and replaced with "Automatic Response" and reference the applicable Standards. o "Balancing Load and Generation" and "Controlling Frequency (Real Power)" are the same action. This activity should reference the BAL standards which require BA's to balance generation and tie lines. o "Controlling Voltages (Reactive Power)": This function is addressed by VAR, TOP, and IRO Standards. o "Managing Constraints": If included, this action falls within BAL, INT and TOP standards which should be referenced. o "Monitoring and Control": The definition of the "BES Cyber System" is monitoring and control. Remove this and use the term in the introduction to Attachment I. o "Restoration of BES": This function is addressed by the EOP standards. o "Situational Awareness": Eliminate the "Situational Awareness" function, as this category is too broad and general. o "Inter-Entity Real Time Coordination and Communication": Reference the applicable FERC approved Standards.Also the phrase: "activities, actions, and conditions" at the start of each items is not clear. For example, is an alarm panel an activity, action or condition? Is an HMI computer an activity, action or condition?
6.7	Regulatory Compliance	No	Please see response to question 3.

#	Organization	Yes or No	Question 6 Comment
6.8	Southwestern Power Administration	No	Requiring Responsible Entities to utilize categories which are intended for guidance in identifying BES Cyber Systems, within the reliability standard; and then requiring Entities to be measured by having evidence that those Cyber Systems tie to the functions listed in Attachment I does not further the goal of maintaining reliability and adds complexity and confusion to the process. Attachment I should be converted to a guidance document.
6.9	San Diego Gas and Electric Co.	No	SDG&E would like to request clarification on a definition of the "situational awareness" function. It is too broad for us to effectively determine what assets might be in scope for this requirement. Similarly, we'd also like to request a definition of the term "BES element" in the Monitoring and Control section.SDG&E would also like to request clarification on the "Inter-Entity Real-Time Coordination and Communication" function. Is this meant to cover voice communication between entities or would it also cover electronic data communication between entities such as ICCP data links? We'd suggest that the ICCP links be specifically excluded because it doesn't fit the wording of "real-time coordination or communication between System Operators"
6.10	IRC Standards Review Committee	No	The descriptions for most of the functions in Attachment I are too vague that they cannot serve as a guideline for identifying which components whose Cyber Systems should be included. For example, Dynamic Response" can cover a very wide range of facilities from generator excitation system, stabilizers, governors, AVRs, to SVCs, HVDC controls, switchable shunts, series compensation devices, even under-load tap changers and phase angle regulators, etc. Every one of them has an effect on real-time operations but not all of them, when tempered with, have significant adverse impacts on BES reliability. The list in Attachment I renders almost all facilities to qualify as essential to reliable operation of the BES, but not all of them have any significant impacts on reliability.Attachment II provides a list of facilities to be categorized under various impact levels. We believe this list is more useful in assisting Responsible Entities in identifying facilities whose Cyber Systems are subject to the security requirements. Further, we believe the establishment of this list already had the built-in assumption that

#	Organization	Yes or No	Question 6 Comment
			they perform one or more of the functions listed in Attachment I.
6.11	E.ON U.S.	No	The inclusion within the function "Situational Awareness" of current state of the BES creates an unnecessary overlap with the "Monitoring and Control" function. In addition, this inclusion appears to require tools such as a video wall fall within the scope of CIP standards despite it not being necessary to perform state estimation or operator monitoring of real-time events. E ON U.S. suggests the "Monitoring and Control" function explicitly include real-time monitoring of real-time or current state of the BES and "Situational Awareness" be limited to assessment of the expected and/or anticipated state of the BES. E ON U.S. also notes that in most cases "Restoration of BES" would be greater than 15 minutes The term "effect" in paragraph 1 of Attachment 1 should be defined.
6.12	Nuclear Energy Institute	No	The introductory paragraph should be revised to be more precise. First, "could" should be replaced with "would". Second, it is not clear what "within 15 minutes" constitutes. Leveraging the definition of BES Cyber System, an acceptable opening paragraph would be:The following operating functions are essential to real-time reliable operation of the Bulk Electric System (BES). To define the scope of applicability of CIP Standards, the functions of relevance are only those that would have an effect on real-time operation of the BES within 15 minutes of the BES Cyber Systems that implement them being rendered unavailable, degraded, compromised, or misused.
6.13	Manitoba Hydro	No	The second sentence of Attachment I is unclear. Within 15 minutes of what? Is the reference to "real-time" necessary given the requirement to have an effect on the BES within 15 minutes?
6.14	Midwest ISO	No	We do not believe Attachment I is needed for anything more than a starting point for identifying BES Cyber Systems per Attachment II. Thus, it is not necessary to expand this any further.
6.15	PacifiCorp	Yes	- PacifiCorp agrees with EEI's suggested improvements for Attachment I below:The

#	Organization	Yes or No	Question 6 Comment
			"Situational Awareness" description should be modified as shown below:Situational Awareness -Activities, actions and conditions to assess the current (real-time) state
6.16	Cogeneration Association of California and Energy Producers & Users Coalition	Yes	1. The first paragraph of Attachment 1 to CIP-010 states:". . . the functions of relevance are only those that can have an effect on real-time operation of the BES within 15 minutes." This is a vague statement. Every device connected to the BES will have an effect on real-time operation but some device's effects will be negligible. Clarification is needed on how entities can determine if their assets have a material, non-negligible effect on real-time operation of the BES within 15 minutes when a Cyber System is unavailable, degraded, compromised, or misused.2. In Attachment 1 of CIP-010, Dynamic Response is defined as:"Actions performed by BES elements or Facilities which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition." Examples or guidance on what is covered by Dynamic Response areneeded. For instance, would Automatic Generation Control be considered a Dynamic Response action?3. Attachment 1 of CIP-010 describes Controlling Frequency and Controlling Voltage as functions essential to reliable operation of the Bulk Electric System. Generators provide Real Power (Controlling Frequency) and Reactive Power (Controlling Voltage). However, we are aware of no disturbance to the BES due to loss of Real Power output or Reactive Power output from our generators. Further clarification is required regarding how impact on grid operations should be determined and measured when determining if a function is "essential" to reliable operation.
6.17	Florida Municipal Power Agency	Yes	Although FMPA agrees with the intent of Attachment I, we believe the definitions contained in the attachment can be significantly improved.As discussed in response to Question 3, FMPA recommends using the word "activities" (or other suitable synonym) for the word "function" to avoid confusion with the Functional Model.The description of situational awareness is too ambiguous and can be interpreted in multiple ways. For further clarification, FMPA suggests:"Information processing and presentation within a Control Center to enable operators to assess the current, expected, and anticipated

#	Organization	Yes or No	Question 6 Comment
			state of the BES."FMPA has other recommended changes to help simplify and clarify the definition of terms used:"Dynamic Response - Actions performed by Protection Systems, control systems, and/or BES Cyber Systems which automatically trigger to initiate a response to a BES Disturbance." (Facilities and Elements do not perform any action, protection, control and cyber systems perform the action)Balancing Supply and Load - Activities, actions and conditions for monitoring and controlling supply and Load. (supply is a more encompassing term that includes energy storage, such as batteries, that may not be included in the term "generation", and Load should be capitalized since it is in the Glossary)Managing Constraints - Activities, actions and conditions to maintain operation of the BES within SOLs and IROLs. (by definition, a BES Element is a Facility; hence, if this suggestion is not taken, then BES element ought to be eliminated from the bullet. Additionally, SOLs and IROLs ought to be discussed in this context and those terms subsume Facility design limits)Restoration of BES - Activities, actions and conditions necessary to go from a shutdown condition to an operating condition. (the phrase "delivering electric power without external assistance" adds no value and is not supported by EOP-005).
6.18	Tenaska	Yes	As long as these functions are applied to High and maybe medium BES assets then the cyber system attached to them. Clarification to "monitoring" should be considered to limit applicability.
6.19	FirstEnergy Corporation	Yes	As stated in our response to Question 3 FE believes that adequate critical infrastructure protection and BES reliability can be accomplished without a need for burdensome compliance documentation of functions described in Attachment I. We encourage the team to carefully review its need and consider removing this aspect from the standard. Please see our response to Question 3 for more details.
6.20	Progress Energy - Nuclear Generation	Yes	Attachment 1 needs to clarify that nuclear generating stations defer to the principles of nuclear security first before consideration is given to the bulk electric system.

#	Organization	Yes or No	Question 6 Comment
6.21	Southern Company	Yes	Broad use of Situational Awareness and System Restoration in the BES functions list and definitions cause the scope of the standards to be overly broad, well beyond the point where there is any reliability benefit. Because there are very few programmable devices in any BES facility that do not have some relevance to one of the listed BES functions, the number of devices included in the standard compliance effort will mushroom unmanageably. The large majority of these newly-included devices pose no significant threat to the BES, but the effort of bringing them into compliance will both distract from the efforts to improve security and will reduce reliability by slowing emergency restoration response time.The function list and other parts of the standards should be modified so that only systems which are used directly in regional or larger Situational Awareness efforts or are relevant to the Entity's System Restoration Plan are included.In addition, the definition of "Restoration of the BES" is vague - does "a shutdown condition" refer to the BES being shut down or a BES component is shut down. The wording should be changed to clarify that it is the BES that is in a shutdown condition."have an effect on real-time operation" should be replaced by "have an adverse effect on real-time operation".
6.22	City Utilities of Springfield, Missouri	Yes	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
6.23	LCEC	Yes	Concerned about the 15 minute threshold.All functions should state: Activities, actions OR conditionsSituational awareness: What is the difference between expected and anticipated? This function could reference real-time system operations of the BES instead of the proposed BES Cyber System definition.
6.24	Southwest Power Pool Regional Entity	Yes	Consider modifying the opening statement to read "...can have an effect on real-time operation of the BES within 15 minutes if not mitigated. Clarify that the expectation is to assume the mitigation is not available or fails for the purposes of the BES Cyber System identification."

#	Organization	Yes or No	Question 6 Comment
6.25	Idaho Power Company	Yes	Controlling voltage needs to reference the voltage on the BES, not just voltage in general which could include distribution level. Situational awareness would seem to include a time window beyond the 15 minute criteria especially as it relates to anticipated state of the BES. Inter-entity Real-Time Coordination and Communication is very broad and pulls in communication systems that are required by other reliability standards to be redundant with plans in place to deal with loss of the primary communication channels. Unless all of the redundant systems are compromised, communication can still be accomplished between entities.
6.26	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Yes	Defining metrics is needed somewhere. For instance, requiring Low Impact compliance over Monitoring & Control of a 20 MW cumulative BES system would be outrageous. If real-time operation is interpreted by the auditor as isolation of a faulted line and Dispatch awareness that the line needs to be fixed, what reliability objective is obtained for the BES? Only local level of service is affected.Concerning "without external assistance" for Restoration of BES is not clear. A boundary is not defined so as to know what external help would be. Would this be the Balancing Authority boundary, or the Reliability Coordinator boundary?
6.27	ReliabilityFirst Staff	Yes	Definition of "BES Elements", What does "external assistance" mean (restoration)?, Sit Awareness: what is "anticipated state", does communication include functions such as phones or email?
6.28	Puget Sound Energy	Yes	Dynamic Response: This is a poor title, as dynamic response has a specific meaning in Electrical Engineering. The definition is too vague and could be interpreted to include a breaker operation due to a line fault, as this is a "response to a BES condition". This definition would include the auto switching controls at nearly every distribution substation with a looped transmission line as a BES Cyber System.Controlling Frequency & Controlling Voltage: This definition would include Under Frequency Load Shedding (UFLS) and Under Voltage Load Shedding (UVLS) schemes, which in many cases only drop single distribution banks, effecting 15 MW of load, which has negligible impact on the

#	Organization	Yes or No	Question 6 Comment
			BES.Managing Constraints: This definition would include overcurrent relays, which may only trip a single 115 kV line that serves local load and has negligible impact on the BES.
6.29	EEI	Yes	EEI suggests that the term “Situation Awareness” be deleted because the term is vague and duplicative of the term “Monitoring & Control.” In the alternative, the “Situational Awareness” description should be modified as shown below:Situational Awareness - Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.
6.30	Exelon Corporation	Yes	Generation functions are not explicit in the Attachment I functions, but are embedded/inherent. As a generation owner/operator, Exelon could review the functions of Attachment I and conclude that generation is not a required function, a reasonable approach if considering loss of a single unit or station out of the entire BES. If adopting the proposed CIP-010 approach, we recommend explicit inclusion of generation as necessary to ensure the Adequate Level of Reliability of the BES.
6.31	The Empire District Electric Company	Yes	I disagree with keeping Attachment I in the standard. The conceptual discussion of functions only adds redundancy, complexity and confusion. The suggested changes to the definition of BES Cyber System and BES Control Center should be enough guidance to identify what is in scope. Therefore, I recommend that the SDT either eliminate Attachment I or convert it to a reference/guidance document supporting the standard
6.32	Consultant	Yes	I think the "15 minute" criteria needs additional clarification. As stated, "an effect on real-time operation of the BES within 15 minutes." is very broad. Suggest limiting to "adverse effect". Also could include some terminology about "adverse effect preventing or limiting the capability of BES assets to perform the listed functions."Suggest numbering the defined functions to allow easier cross-reference to this attachment.
6.33	Alliant Energy	Yes	In paragraph 1 the phrase “that can have an effect on real-time operation” needs to be

#	Organization	Yes or No	Question 6 Comment
			clarified. We believe it should be tied to and IROL, SOL, or degradation of the reliability of the BES. As written it is undefined and too ambiguous.In the item listed "Monitoring & Control" we do not believe monitoring should be included as listed it is too ambiguous and could be interpreted to include every meter, instrument transformer, etc, even if it is not needed for protection of the BES.
6.34	Luminant	Yes	Is it possible to have a real time impact (15 minute time horizon) related to Situational Awareness for Generation? If not it should be removed. At most it should be scoped to BA, RC,TOP and then only to a subset of data.The definitions in Attachment I are very broad. Could the SDT include examples or a reference document that provides more details for the functions in Attachment I?
6.35	Detroit Edison	Yes	It is not clear how the list in attachment 2 was created. Consider leveraging other NERC documents such as the Definition of Adequate Level of Reliability located at http://www.nerc.com/docs/pc/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf.
6.36	Reliability & Compliance Group	Yes	It needs to be more clearly defined what it means to have an effect on real-time operation of the BES. There are many things that can have an effect on the BES that occur even during normal operations. Recommend that the effect be defined as a reduction in the stability of the BES and that level of reduction needs to have a quantifiable measure.
6.37	US Army Corps of Engineers, Omaha Distirc	Yes	It seemes clear from the workshop that the committee intends for protective relay systems to be include for consideration. That was not clear prior to the workshop. They appear to fall under the category of Dynamic Response. Suggest strengthening the definition and include the term "protective relay."
6.38	US Bureau of Reclamation	Yes	It would be helpful to provide a example list of some of the elements which provide the related functions. Further, the unclear definition for "could have an effect on real-time operation..." as used in the opening of Attachment I, needs to be clarified/quanitized or defined. Almost any of these functions (and many more), at any facility - no matter the

#	Organization	Yes or No	Question 6 Comment
			size - could have an effect. The effect needs to be characterized as more than trivial to be deemed essential to reliable BES operation. Rather that attempt to define Restoration of the BES in the Attachment, would it be better to refer to other Standards?
6.39	Lincoln Electric System	Yes	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
6.40	MidAmerican Energy Company	Yes	MidAmerican Energy agrees with EEI's suggested improvements below:The "Situational Awareness" description should be modified as shown below:Situational Awareness - Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.Suggest the following addition for Attachment I:Plant cyber systems or cyber components that do not provide or support BES Cyber System (CIP-010 definition) functions (CIP-010, Attachment I) and which logically are external to the electronic boundary (ESP) protecting a BES Cyber System are excluded from the CIP-011 requirements. Examples of excluded components and systems are those that 1) support balance-of-plant functions and operations that cannot directly result in the loss of generating capacity within 15 minutes, and 2) are logically external to the electronic boundary (ESP) protecting a BES Cyber System.
6.41	Oncor Electric Delivery LLC	Yes	Need more clarity on the "15-minute" criteria. Is this ADVERSE effect? Is this RESTORATIVE effect?
6.42	USACE HQ	Yes	Please read answer to question 3.
6.43	BGE	Yes	Provide examples or definitions of actions, activities and automatically triggered.Add the words "to the BES" after "delivering electrical power" in the definition of Restoration of BES to clarify. Further define the Inter-Entity Real Time Coordination and Communication Function (currently implicates, phone system, harmony, email, PJM all

#	Organization	Yes or No	Question 6 Comment
			call system, 800 MHz devices used to communicate to field personnel and notifind)
6.44	SCE&G	Yes	Remove the 15 minute timeframe.
6.45	Southern California Edison Company	Yes	SCE's concerns with the proposed criteria are two-fold. First, it is unclear whether the term "effect" and "disturbance" refer to the same event. Thus, SCE asks the Standards Drafting Team to clarify. As the criterion is currently written, Attachment I states, "To define the scope of applicability of CIP Standards, the functions of relevance are only those that can have an effect on real-time operation of the BES within 15 minutes." However, the definition of BES cyber system in this standard states, "One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES." If "effect" means "disturbance to the BES, restricted control and operation of the BES, or affecting situational awareness of the BES", then the definitions are consistent. This being said, it is not clear that these have the same meaning. An extreme definition of "effect real-time operation" could be virtually anything whether the impact on operations will be significant or not.Additionally, SCE recommends treating control and monitoring as separate functions. Systems that are only capable of monitoring BES elements should be treated differently from systems that are able to perform control functions. SCE suggests the drafting team add an additional function that is based on "actual device capability" rather than "how it has been implemented" by a particular registered entity. For instance, HMI's providing electronic output have a different real-time impact on BES reliability than HMI's designed as I/O devices. The task of reviewing data on a "view only" capable system resulting in human action on another system that could potentially cause BES reliability issues is a distinctly different function than the task of initiating actions. In this case, the monitoring system and the control system are both "real-time" but with very different BES impact potential.
6.46	Constellation Energy	Yes	See answer to Question 3.

#	Organization	Yes or No	Question 6 Comment
	Control and Dispatch, LLC		
6.47	Constellation Energy Commodities Group Inc.	Yes	See answer to Question 3.Provide examples or definitions of “actions”, “activities” and “automatically triggered” as provided in Attachment I.Add the words “to the BES” after “delivering electrical power” in the definition of Restoration of BES to clarify. Further define the Inter-Entity Real Time Coordination and Communication Function (currently implicates, phone system, harmony, email, PJM all call system, 800 MHz devices used to communicate to field personnel and notifying).Please define the industry use for the term Generation Management System (“GMS”). We believe there are two categories of GMS, Regulated and non-Regulated Utilities since they could be use differently or have different functionality.
6.48	MWDSC	Yes	See comments for question 3 above.
6.49	Wolverine Power	Yes	See comments listed for 1.a
6.50	BCTC	Yes	See previous response 0n CIP-010-1-R1
6.51	Dynegy Inc.	Yes	Show examples of how the identification and categorization and tie-in to Attachment 1 would work.
6.52	Constellation Power Source Generation	Yes	Some of the terms are ambiguous. What is meant by monitoring and control? As written, it is an AND statement, meaning that a BES Cyber System would have to do both monitoring AND control to be labeled a BES Cyber System. What about electronic metering at a plant? That provides monitoring, but not control. So is it excluded?Situational Awareness should be clarified. A suggestion would have the following statement attached to the current definition: “and cause an action without further analysis.” This would exclude metering that, if rendered unavailable, would not be detrimental to the BES as phone communication would be used in the event of metering errors.

#	Organization	Yes or No	Question 6 Comment
6.53	Platte River Power Authority	Yes	Suggest removing “Inter-Entity Real-Time Coordination and Communication” until there is a mechanism to define a single BES Cyber System that includes BES Cyber System Components from multiple Entities. The mechanism should include documentation of coordination with implementing the CIP standards for the BES Cyber System.
6.54	SPS Consulting Group Inc.	Yes	Suggestion number one is to get rid of the list, as previously stated. Failing that my other question is about Dynamic Response. I assume this refers to things like UFLS, UVLS and runbacks initiated by SPS. Also assume this does not include things like AGC, AVR, and governor response from generators since these actions are not triggered by a single element or control device, or a combination of devices, but rather are initiated by operating condition fluctuations. Is that true?
6.55	Dairyland Power Cooperative	Yes	Systems used to communicate between entities are not mentioned, yet many of these are critical to the operation of the BES. Imagine the impact to the BES of an ISO/RTO without ICCP communications. How can these systems be ignored?
6.56	Allegheny Energy Supply	Yes	The “Situational Awareness” description should be modified as shown below:Situational Awareness -Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.Suggest that the definitions for "Dynamic Response" and "Balancing Load and Generation" be more specific.
6.57	Allegheny Power	Yes	The “Situational Awareness” description should be modified as shown below:Situational Awareness -Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.

#	Organization	Yes or No	Question 6 Comment
6.58	APPA Task Force	Yes	The APPA Task force agrees with the intent of Attachment I. We believe, however, the definitions contained in the attachment can be substantially refined and improved.As discussed in response to Question 3, we recommend using the word "activities" (or other suitable synonym) for the word "function" to avoid confusion with the Functional Model.The description of situational awareness is too ambiguous and can be interpreted in multiple ways. For further clarification, We suggest:Situational Awareness - Information processing and presentation within a Control Center to enable operators to assess the current, expected, and anticipated state of the BES.Other recommended changes to help simplify and clarify the definition of terms used:Facilities and Elements do not perform any action, protection, or control; rather cyber systems perform the action. Therefore we propose:Dynamic Response - Actions performed by Protection Systems, control systems, and/or BES Cyber Systems which automatically trigger to initiate a response to a BES Disturbance. Supply is a more encompassing term that includes energy storage, such as batteries, that may not be included in the term "generation." Therefore we propose:Balancing Supply and Load - Activities, actions and conditions for monitoring and controlling supply and load. SOLs and IROLs should be discussed in this context. If this suggestion is not taken, then "BES element" should be eliminated from the definition. Therefore we propose:Managing Constraints - Activities, actions and conditions to maintain operation of the BES within SOLs and IROLs. The phrase "delivering electric power without external assistance" is not supported by EOP-005 and should be removed from this definition. Therefore we propose:Restoration of BES - Activities, actions and conditions necessary to go from a shutdown condition to an operating condition. As written, the term "monitoring" is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for control of the BES and should therefore be removed from the Monitoring and Control function. Therefore we propose:Control - Activities, actions and conditions that provide control of BES elements.
6.59	Arizona Public Service Company	Yes	The APS review team had the following comment: The document heading is "Function Essential to Reliable Operation of the Bulk Electric System." Typically restoration of BES

#	Organization	Yes or No	Question 6 Comment
			is a completely different activity than the normal or emergency operation of the BES. The document includes restoration which is typically not essential to the reliable operation of the BES. This is not a contradiction but the operation is being defined more broadly than typical. This broad function description can create ambiguity.
6.60	Independent Electricity System Operator	Yes	The descriptions for most of the functions are too vague that they cannot serve as a guideline to identifying those components whose Cyber Systems should be included. For example, Dynamic Response" can cover a very wide range of facilities from generator excitation system, stabilizers, governors, AVRs, to SVCs, HVDC controls, switchable shunts, series compensation devices, even under-load tap changers and phase angle regulators, etc. Every one of them has an effect on real-time operations but not all of them, when tampered with, have significant adverse impacts on BES reliability. The list in Attachment I renders almost all facilities to qualify as essential to reliable operation of the BES, but not all of them have any significant impacts on reliability.Attachment II provides a list of facilities to be categorized under various impact levels. We believe this list is more useful in assisting Responsible Entities in identifying facilities whose Cyber Systems are subject to the security requirements. Further, we believe the establishment of this list already had the built-in assumption that they perform one or more of the functions listed in Attachment I.We suggest Attachment I be eliminated.
6.61	Entergy	Yes	The Functions as identified in Attachment I are far too general in nature and thereby leave too much latitude in interpretation in audit, i.e., creates a risk that if the Responsible Entity excludes a system(s) from scope and the auditor disagrees, this could be a very significant adverse finding. Entergy recommends that general Function descriptors be augmented with specific examples of applications that execute the stated functions 'essential to reliable operation of the BES', e.g., ACE, AGC, state estimator, etc., to help avoid as this dilemma to the extent foreseeable.
6.62	NextEra Energy Corporate Compliance	Yes	The standard should clarify those functions and provide examples specific to Generation, Transmission and Control Center Facilities. These clarifications, we believe, should be contained in the body of the standard as opposed to a reference attachment.

#	Organization	Yes or No	Question 6 Comment
			Attachments should be used to add specific examples or propose exclusions.With respect to the Inter-Entity real time coordination and communication function, the standard should specifically exclude voice communications systems due to the fact that they are covered under separate standards (i.e. COM Standards)
6.63	American Electric Power	Yes	The terms "Dynamic Response" appears to be a very broad function. Is it the intent that this would include all devices such as relays?The "monitoring" portion of function "Monitoring & Control" is too ambiguous. We would propose using the following: "Control - Activities, actions and conditions that provide control of BES elements."In addition, "Situational Awareness" is ambiguous; systems that are not needed for operating the BES, but provide information would be in scope. This definition appears to include items such as all meters, instruments, and transducers.
6.64	Dominion Resources Services, Inc.	Yes	There is overlap among the many functions listed. The list can be reduced to only Monitoring & Control with many of the others listed as examples of this function. As examples; Balancing Load and Generation and Controlling Frequency (Real Power) are essentially the same. Frequency is a direct result of the balance between supply (generation) and demand (load). It is redundant to list both, and doubly redundant since both are covered by Monitoring & Control. Monitoring & Control touches or covers most of the other listed functions. Any portion of Dynamic Response, Controlling Frequency (Real Power), Controlling Voltage (Reactive Power), and Managing Constraints not captured in the Monitoring & Control function should be identified and listed separately, but not those entire functions. Also, some of the definitions are too broad and encompass functions that are not required for the reliability of the BES.Facilities must have ratings per FAC-008 and must be operated within those ratings in other reliability standards. Please refer to “ratings” rather than “design limits and constraints.”Dominion requests that the functions be reduced to: Monitoring & Control - Activities, actions, or conditions that provide real-time operation and control to maintain BES elements within their ratings. Restoration of BES (as defined).Situational Awareness - Activities, actions, or conditions required by the BA, RC, or TOP for real-time operational decision-making associated with the BES.Inter-Entity Real-Time Coordination

#	Organization	Yes or No	Question 6 Comment
			and Communication (as defined).
6.65	Pepco Holdings, Inc. - Affiliates	Yes	We agree with EEI's comments.
6.66	We Energies	Yes	We Energies agrees with EEI comments. The "Situational Awareness" description should be modified as shown below:Situational Awareness -Activities, actions and conditions essential for to assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.We Energies agrees with EEI Suggest the following addition for Attachment I:Plant cyber systems or cyber components that do not provide or support BES Cyber System (CIP-010 definition) functions (CIP-010, Attachment I) and which logically are external to the electronic boundary (ESP) protecting a BES Cyber System are excluded from the CIP-011 requirements. Examples of excluded components and systems are those that 1) support balance-of-plant functions and operations that cannot directly result in the loss of generating capacity within 15 minutes, and 2) are logically external to the electronic boundary (ESP) protecting a BES Cyber System. Additionally, We Energies does not understand the inclusion of "Real "Power" and "Reactive Power" in the context of the functions "Controlling Frequency" and "Controlling Voltage" respectively. It is suggested that these qualifiers be eliminated.
6.67	Bonneville Power Administration	Yes	We find the guidance on Attachment I confusing. The statement "The following operation functions are essential to real-time reliable Operation of the Bulk Electric System" makes the explicit statement that all the functions listed below are essential to real-time operation; and the second sentence doesn't do a good job of clarifying that it is only those BES Cyber Systems for which the loss of the functions listed below (Dynamic Response, Balancing Load and Generation, Situational Awareness, etc.) can have an effect on real-time operations of the BES within 15 minutes.For example, the loss of a cyber system used for situation awareness of lightning strikes would not have an effect on real-time control and operations of the BES within 15 minutes. As such, it is NOT a

#	Organization	Yes or No	Question 6 Comment
			BES Cyber System.It would be helpful if this statement in Attachment I and the definition of BES Cyber System were more consistent with each other."Situational Awareness" is too broad. Refer to comments in Question 1.b.
6.68	American Transmission Company	Yes	We propose to remove “monitoring” from the Monitoring and Control function. As written, the term “monitoring” is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for control of the BES.We would propose using the following:Control - Activities, actions and conditions that provide control of BES elements.
6.69	MRO's NERC Standards Review Subcommittee	Yes	We propose to remove “monitoring” from the Monitoring and Control function. As written, the term “monitoring” is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for control of the BES.We would propose using the following:Control - Activities, actions and conditions that provide control of BES elements.
6.70	WECC	Yes	While scoping the CIP standards to only cover functions within a 15-minute event time frame is appropriate for generation, transmission, and other operations it is not appropriate for Reliability Coordination functions such as situational awareness. There are many cases of critical systems to support a reliability coordination function that do not fall within a 15 minute time horizon such as next day studies, coordinated outages, and contingency planning. Suggest that the SDT redefine functions for situational awareness and communication between entities to not be restricted to a 15 minute time period.The opening paragraph again refers to a 15-minute time period to be used in the identification of BES Cyber Systems. It appears that an effort is being made to restrict applicability of this standard to real-time systems. Section 215 of the Federal Power Act does not include such a restriction; therefore, this should be removed from the standard. Any cyber system that could affect the reliability of the bulk electric system, regardless of timeframe, should be in-scope.Dynamic ResponseThe second sentence is poorly worded and does not appear to add anything. This language should be clear and concise.Restoration of BESThere are a significant number of restoration plans at the

#	Organization	Yes or No	Question 6 Comment
			Balancing Area and Transmission Operator level that hinge on external assistance. In many cases these areas play a significant role in delivering power across the transmission system during restoration, but do require external assistance. As drafted, the functional characterization for restoration of the BES, may fail to identify systems critical to system restoration and is seemingly inconsistent with Attachment II, specifically Item 1.6.
6.71	Ameren	Yes	Would change the second sentence defining the scope to read "To define the scope of applicability of CIP Standards, the below functions are relevant only if they can have an effect on real-time operation of the BES within 15 minutes.Would suggest to impose limits on the definitions for example Controlling Voltage (Reactive Power) is partially dependent on hydrogen pressure for hydrogen cooled generators. We would also suggest adding the word "grid" in front of voltage.Change the first sentence of Dynamic Response to read "Actions performed by BES elements or Facilities which are automatically triggered to initiate a response to mitigate the impact to a BES condition". Is it the SDT intent to implement physical and cyber security of any tertiary systems for example, Controlling Frequency (Real Power) is also dependent upon coal mills providing enough fuel to the boiler, do these systems also need to be secured?The "Controlling Frequency" section needs some clarification. Governor controls on all generating units have built mechanisms whether mechnical or electronic that act to control or balance frequency during a disturbance. The current definition would lead to inclusion of all generating units regardless of any other factor. â€,The last section on communication needs to be clarified to explicitly address voice communication vs. data communication and the expectations of both.
6.72	Verizon Business	Yes	The criteria should include major systems needed for the essential operation of such systems as control centers. For example, Heating, Ventilation and Air Conditioning (HVAC) systems are essential to the operation of a control center. The failure of the HVAC could lead to shutdown of the control center within the 15 minute time frame.

7. **CIP-010-1 Attachment II contains criteria for categorization of BES Cyber Systems for High, Medium and Low impact categories. The criteria were originally developed in collaboration with representatives of the Operating and Planning Committees, some of whom continued to provide input during the drafting of Attachment II. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.**

Summary Consideration:

The summary of responses to Question 7 was previously posted on the NERC website prior to the posting of Version 4 of the CIP-002 through CIP-009 standards.

#	Organization	Yes or No	Question 7 Comment
7.1	Platte River Power Authority		1.1 is confusing. Consider revising: For the preceding 12 months did the Generation Facility's net Real Power capability (rated net) exceeds the largest value of either the Contingency Reserve or the Reserve Sharing Group's total reserve sharing obligation. In the case where no Contingency Reserve or total reserve sharing obligations have been established, Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW. 2.7. "switching stations operated at 200kV or above" should read "switching stations operated between 200kV and 299kV"
7.2	National Rural Electric Cooperative Association (NRECA)		In 1.1, "must run" must be more clearly defined and there needs to be language to make clear how Generation Facilities are labeled "must run" -- i.e., who determines the "must run" status? In 1.5 and other places in this document, the term Transmission lines is used. What does "lines" mean? One wire? One three-phase circuit? One single phase of a three phase circuit? Please make this clear so there is no confusion for registered entities when determining High, Medium or Low. In 1.10, please provide an explanation of what "impact" and "local area" means in the phrase "have impact beyond the local area." Add language to 1.10 as needed to make

#	Organization	Yes or No	Question 7 Comment
			this more clear.
7.3	Emerson Process Management		It is only uncertain how the criteria of 2000MW and 1000MW were chosen for generation facilities.
7.4	Arizona Public Service Company		These criteria are closely related to the definition of a BES Cyber System and the feedback for question #2. If the intent is to categorize the majority of BES Cyber Systems into the Low, Medium and High Impact Categories, with the current timeline specified in the definition of a BES Cyber System, it may lead Entities to exclude from Impact Categorization (by the Definition) Cyber System Components that the drafting team did not intend. A preferred approach may be to eliminate the time windows from the definition, causing all BES Cyber Systems to be inventoried, and enhancing the Impact Categories with additional time window criteria. For example, a High category may be further refined by specifying an impact window of 0-15 minutes, a Medium of 16-240 minutes, a Low of 241-1440 minutes (24 hours), etc. Additionally, a further Impact Category of 'None' may be beneficial if the 15-minute time windows is removed from the definition. This would allow a floor to be utilized in the Impact Categorization of 'Low' so that it would not result in unintended consequences of including undesired BES Cyber System Components in a category with Standard applicability. Further comments regarding the (as-of-yet undefined) implementation schedule include concerns that a long implementation schedule or different implementation schedules for High, Medium and Low both raise the risk of confusion as well as the risk or FERC disapproval. An alternate method, in conjunction with the definition and Impact Category adjustments mentioned, of creating a phased implementation schedule, by time period (12 months, 24 months, 36 months, for example) would allow the applicable standards to increase over time for the lower categories. This would also allow for some Standards to be applied earlier than other Standards in the same Impact Category.
7.5	ISO New England Inc	No	"Must run" in 1.3 and 2.3 is a phase should not be used, even if quotations are around it, because it is a regulatory mechanism, used in some areas of the country, to ensure generators receive adequate payments. Other generators - that are equally important

#	Organization	Yes or No	Question 7 Comment
			to grid operation - may not have reliability must-run agreements. In short, these agreements are established simply as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators are impactive on the bulk electric system. If the Standard Drafting Team insists on using the term, it must, at a minimum, define what it means by this phrase.
7.6	Madison Gas and Electric Company	No	1.3 and 2.3 utilize the words “must run”. Must run is used in many markets whereby a GO may designate a unit to be online outside the need for reliable operations of the BES. Since “must run” is not defined, it is recommend that the SDT remove the term “must run”.
7.7	Progress Energy (non-Nuclear)	No	All T/D substation capacitor banks that provide system reactive support are controlled through a capacitor bank control program residing on the substation gateway device. However the DSCADA master may be included in 1.2 (more than 1000 MVAR). 2.4 will bring many T/T substations into consideration with the four or more lines >200kV. Also see comment 4. Attachment II defines "Each Cyber System that can affect operations for..." as it relates to Impact Rating on BES. For new combined cycle facilities which will include diverter dampers to allow simple cycle operation can we designate separate Cyber systems for simple cycle operation (approximately 70% of total plant output) and combined cycle operation (approximately 30% of total plant output). Potentially that would define each system as a "Low " impact versus a combined Medium to High. The plants are being designed to go from combined cycle to simple cycle operation in less than 15 minutes. We will need to know whether this designation is allowed and then design the cyber system(s) architectures appropriately.
7.8	Consultant	No	Attachment II - Section 1.1 & 1.2 To avoid confusion, suggest consistent wording in the parenthetical phrases following the words "singularly or in combination" in these sections.

#	Organization	Yes or No	Question 7 Comment
			Section 1.2 - Similar to section 1.1, should there be a 12 month component to the Reactive Power criteria in addition to the 1,000 MVAR. Section 1.3 & 2.3 - The term "pre-designated" doesn't make sense. A facility is not in the "must run" status unless it is "designated". Additionally, the statement has "must run" units both "designated" and "assigned", and semantically these are two different conditions. Section 1.3 & 2.3 - Further, the reliability "must run" status is an economic and contractual condition rather than a BES operational condition. It would seem that the plants that would be designated as reliability "must run" should have a BES operational or reliability criteria, independent of their "must run" status, which should be the criteria used to include or exclude these facilities. Section 1.6 - suggest including the title of EOP-005 in the statement as a complete reference citation. Section 1.9 - suggest including the title of NUC-001 in the statement as a complete reference citation. Section 1.10 - suggest clarifying which entity makes the determination that a RAS has "impact beyond the local area." - RAS Owner, RAS Operator, or appropriate regional entity. Section 1.11 (& throughout CIP-011) - BES Elements, BES elements, and elements are used throughout this standard. It is not clear if all are intended to be the glossary definition of 'Elements', or if 'BES elements' or 'BES Elements' are new definitions or incorrect application of the glossary term 'Elements'. Please clarify the usage. Sections 1.8, 1.13, 2.5 - These sections include the words "singularly or in combination" without a subsequent parenthetical qualifier. Suggest consistency with sections 1.1 & 1.2 as discussed above. Section 2.1 - See comments on sections 1.1 and 1.2 regarding consistency of parenthetical statement.

#	Organization	Yes or No	Question 7 Comment
			Section 1.1, 1.3, 1.4, 1.5, 1.7, 2.1, etc. - Multiple sections use the terms Generation Facilities or Transmission Facilities with capitalization that should indicate a defined term, either by this standard or in the current glossary. These terms are not defined in the current glossary. Suggest consistency of using defined terms throughout the standard. Section 2.1 - The criteria in this section are not parallel to the criteria in section 1.1 with a 'downsized' value. The term "most current and prior to most current rated" is not defined, or included in the glossary. Suggest clarifying this section, and defining or referencing the terminology.
7.9	E.ON U.S.	No	CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems currently lists 14 “High Impact Ratings” of the categorization of the BES Cyber Systems. E ON U.S. proposes that only Control Centers and Backup Control Centers fall into the High Impact Rating category. All other points listed in the High Impact Rating category should be moved to the Medium Impact Rating category, and all points currently listed in the Medium Impact Rating category should be moved to the Low Impact Rating category. More generally, “reliable operation” of the interconnected BES is defined in Section 215(a)(4) as:” . . . operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cyber security incident, or unanticipated failure of system elements.” Attachment II’s low impact category appears completely untethered to the statutory definition of reliable operation of the bulk power system. Attachment II also appears to introduce an ill-defined set of multiple contingencies or sequence of events that needs more definition and boundaries to be of any practical use and to provide a reasonable means for compliance cost quantification.
7.10	Kansas City Power & Light	No	Do not agree with several of the items listed in Attachment II.

#	Organization	Yes or No	Question 7 Comment
			Items 1.7 & 1.8 are too broad. There are any number of combinations of transmission facilities that can be removed from service such that the undesirable effect of exceeding an IROL limit or the loss or reduction of generation would occur. Recommend their removal as the remaining items left in Attachment II are sufficient to capture the HIGH impact areas. Item 1.10 regarding SPS is too broad. SPS systems are in place for a number of different reasons, including the protection of facilities from damage. The SPS that should be considered here are only the SPS that are intended to prevent cascading, uncontrolled separation, or instability. Item 1.14 is too broad and would include facilities that are unnecessary. Recommend tying Control Centers in where facilities are identified in 1.5. Recommend the following language for consideration: Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations for transmission facilities identified by 1.5.
7.11	FirstEnergy Corporation	No	FE suggests that item 1.5 be removed such that it is effectively reclassified as a medium impact and covered by item 2.4. Within the High Impact category, items 1.6, 1.7 and 1.8 appropriately cover those situations where Transmission Facilities should rise to a High Impact level. Consider removing item 1.9. This delves into a nuclear plant safety concern that is covered by the NUC-001 standard and not directly associated with BES reliability. If in item 1.1 a 2000MW level adequately depicts a High Impact generation facility hurdle then transmission facilities associated with a 900MW nuclear plant should not be deemed High Impact for BES reliability. In item 1.10 the term “local area” is vague and open to interpretation. Its suggested to simplify such that all SPS and RAS systems would be treated as High Impact. If the intent is to exclude SPS or RAS associated with limiting generation output under contingency loss of certain Transmission Facilities then consider a separate Medium Impact SPS or RAS describing those instances and rewrite 1.10 to say “Special Protection Schemes,

#	Organization	Yes or No	Question 7 Comment
			Remedial Action Schemes (RAS) or automated switching of BES elements not include in Section 2, item 2.x" However, the preference is to keep it simple and just treat all SPS and RAS items as High Impact. Suggest adding thresholds below which no measures need to be taken. The low impact rating as written could require significant effort for negligible security and reliability improvement.
7.12	National Grid	No	In lieu of the BES NOPR and the exemption process currently proposed, if facilities above 100 kV are exempted by NERC and FERC, will those facilities automatically be exempted from CIP standards? Currently, as per the standards, all the BES systems which are not categorized high impact or medium impact will be defaulted to LOW IMPACT category regardless of how the facility is impacting the Bulk power system. There are facilities >100kV having very localized impact and minimal impact to the reliability of the BES system for which entities will request for exemption. National Grid requests the SDT to clarify this issue. National Grid recommends a tabular format similar to the tables in CIP-011-1 with various criteria listed under Low Impact, Medium Impact, and High Impact. This will help in understanding the key differences among the three categories efficiently."Must run" in 1.3 and 2.3 is a phase should not be used, even if quotations are around it, because it is a regulatory mechanism, used in some areas of the country, to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must-run agreements. In short, these agreements are established simply as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators are impactive on the bulk electric system. If the Standard Drafting Team insists on using the term, it must, at a minimum, define what it means by this phrase.
7.13	American Electric Power	No	Overall we like the concept of these gradients, but need more time to fully ascertain the validity of the breakpoints. It is uncertain what engineering analysis drove these specific categorization levels. We assume that there could be a significant difference from region

#	Organization	Yes or No	Question 7 Comment
			to region, and the SDT should consider regional impacts for the categorization.
7.14	Regulatory Compliance	No	Qualifier should include capacity factors averaged over the last five years - otherwise it will require some large plants that are only on-line several days a year to remediate to the "High Impact" category
7.15	Manitoba Hydro	No	Regarding criterion 1.1, the phrase “with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW” is difficult to understand. For some utilities, the required reserve obligations could be a small value which would not compare very well to the proposed 2000 MW limit for utilities with NO reserve obligations (such as small utilities). A related minimum value for utilities with reserve obligations should be provided, or the greater value of the required reserve obligations and 2000 MW should be used .Regarding criteria 1.5 and 2.4, clarify the requirements through the appropriate use of colons, semi-colons and numbers. It is not clear as drafted whether phrase “with four or more transmission lines” applies to Texas and Quebec.
7.16	Seattle City Light	No	see prior comments
7.17	Indeck Energy Services, Inc	No	The system of 3 categories oversimplifies the BES. 1) The grouping of, for example, all generators of capacity less than 1,000 MW (except for special cases like Must Run units) as LOW needs to be further subdivided. The categorization ignores the Functions in Attachment I. Not all generators have the same impact on the BES ALR for all functions. Different types of generators have different effects on the BES ALR. This isn’t to say that all generators should not be categorized, but not all require the same LOW level of requirements. Choosing only 3 categories was highly arbitrary. The LOW category should be subdivided into 3 or more groups reflecting the relative impact on BES ALR that was used to differentiate the HIGH and MEDIUM groups. 2) Additionally, the standards ignore the fact that access to BES cyber facilities can be

#	Organization	Yes or No	Question 7 Comment
			controlled at either end of a communications path. If it is adequately controlled at one end, then controlling the other end or the middle is less important, if not unimportant. For example, an RTU at a small generator that is a window to the BES cyber facilities at the control center is a bigger risk for BES ALR at the control center than it is at the generator. Any effect on the generator may be insignificant, whereas, access to the control center could be critical. Applying controls at the control center takes away the need to control all of the insignificant RTU's, but not the ones affecting other parts of the BES. 3) Nowhere in the categorization process is the potential impact on BES ALR assessed by Function. Attachment II makes arbitrary categories that may be appropriate for the HIGH and MEDIUM categories, but has not been done for the remainder that are lumped in the LOW category. The concept of impact to the BES ALR is missing from the categorization process. The impact on the BES ALR of, for example a 999 MW generator versus a 499 MW generator versus a 299 MW generator are very different and different by Function as well. The impact on the BES ALR should be assessed for all facilities in the LOW category to differentiate them. All of the facilities should be categorized as to the impact on the BES ALR by function. [suggestion] There should be 5 categories: VERY HIGH, HIGH, MEDIUM, LOW and VERY LOW based upon the relative impact on the BES ALR, with various combinations of facility types and functions from Attachment I.
7.18	Reliability & Compliance Group	No	These criteria do now however, exclude many systems that were previously identified as CCA's. However they also include many systems that registered entities eliminated using the RBAM.
7.19	BCTC	No	This looked very thorough. Great job!
7.20	Xcel Energy	No	While the draft provides guidance in Attachment II as to which BES elements are classified as High, Medium, and Low impact, no criteria is provided for why each element was assigned into the specific impact category. The decision to place each element into

#	Organization	Yes or No	Question 7 Comment
			a category is not based on any identified objective criteria. The SDT should publish the criteria used to place each item under the assigned category.
7.21	Independent Electricity System Operator	Yes	(1) We support explicitly including Restoration of BES as a critical function. However, in the proposed standard it is limited to blackstart generation and transmission subsystem cranking paths (impact level H, items 1.4 and 1.6 in Attachment II). The impact criteria do not include a requirement to protect sufficient generation capacity to allow restoration to proceed to a point of relative assurance of stability and resiliency (not necessarily all load served). With these criteria, in Ontario we would drop 6 generating stations (a total of over 3000 MW capacity) from a High impact (current Critical Assets) to a Low impact category. We suggest to add a requirement in the High category for generation essential to facilitate restoration as determined by the RC. (2) 1.3 "Generator pre-designated as must run": In some developed markets, must run generators change from time to time and often are not determined (designated) until week/day ahead of real time. We do not believe facilities of this dynamic nature should be included. If we want to include generators having a significant impact on reliability in this category, we need only to say: "Generation Facilities that have Wide Area reliability impacts when removed from service". (3) 1.7: Violating IROL does not result in instability, uncontrolled separation or cascading. In everyday operations, IROLs are exceeded from time to time due to changing system conditions and external impacts. For so long as such exceedances are corrected within Tv, the BES is deemed to be reliable. We suggest the first part of this category be removed. Keeping the second part "Transmission Facilities, including FACTS, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in instability, uncontrolled separation or Cascading would suffice. (4) 1.13: BA does not operates transmission facilities or generators; it only balances load/generation/interchange and maintain frequency by entering schedules onto the EMS. If the intent of R1.13 is to stipulate the primary and backup control centres of a BA that balances load and generation for a BA Area of the MW size as noted in 1.13, then

#	Organization	Yes or No	Question 7 Comment
			simply say so. (5) 2.3: See our comments on 1.3. We do not see the need for this category. (6) 2.8: See our comments on 1.13. The BA does not operate transmission facilities or generators. Suggest to reword it in a similar fashion.
7.22	IRC Standards Review Committee	Yes	(i) There are "bright-line" cutoffs for the range of violations for MW of generation (1.1, 2.1) and voltage levels (1.5, 2.4). Although these cutoffs are appropriate for most of the Interconnection(s), there may be local configurations that warrant that BES Cyber System to be rated other than what is defined with the "bright-line" cutoff. CIP-010-1 should either allow for a documented alternative rating or waivers be allowed to diverge from the cutoff limits. (ii) 1.3: "Generator pre-designated as must run": In some developed markets, must run generators change from time to time and often are not determined (designated) until week/day ahead of real time. We do not believe facilities of this dynamic nature should be included. If we want to include generators having a significant impact on reliability in this category, we need only to say: "Generation Facilities that have Wide Area reliability impacts when removed from service". (iii) 1.7: Violating IROL does not result in instability, uncontrolled separation or cascading. In everyday operations, IROLs are exceeded from time to time due to changing system conditions and external impacts. For so long as such exceedances are corrected within Tv, the BES is deemed to be reliable. We suggest the first part of this category be removed. Keeping the second part "Transmission Facilities, including FACTS, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in instability, uncontrolled separation or Cascading would suffice. (iv) 1.13: A BA does not operates transmission facilities or generators; it only balances load/generation/interchange and maintain frequency by entering schedules onto the EMS. If the intent of R1.13 is to stipulate the primary and backup control centres of a BA that balances load and generation for a BA Area of the MW size as noted in 1.13, then

#	Organization	Yes or No	Question 7 Comment
			simply say so. (v) 2.3: See our comments on 1.3. We do not see the need for this category. (vi) 2.8: See our comments on 1.13. The BA does not operate transmission facilities or generators. Suggest to reword it in a similar fashion.
7.23	FEUS	Yes	*1.1; clarify 'if the Generation Facilities capability exceeds the largest value of the Contingency Reserve or reserve sharing obligations for the Reserve Sharing Group' the Contingency Reserve is also relative to the Reserve Sharing Group. *1.10: The drafting team should consider allowing for voltage differentiations for High and Medium SPS, RAS, or automated switching stations similar to that used in 1.5 and 1.14
7.24	Hydro One	Yes	"Must run" in 1.3 and 2.3 is a phrase that we strongly disagree with, and should not be used, because it is a regulatory mechanism, and used in some areas of the country to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must run agreements. These agreements are established as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators impact the bulk electric system. If the Standard Drafting Team insists on using the term it must, at a minimum, define what it means by this phrase. We strongly suggest that a fourth category of NO IMPACT is included as follows: No Impact contains all other documented BES Cyber Systems that have no affect on operation and are not categorized as having either High, Medium or Low Impact rating.
7.25	Northeast Power Coordinating Council	Yes	"Must run" in 1.3 and 2.3 is a phrase that we strongly disagree with, and should not be used, because it is a regulatory mechanism, and used in some areas of the country to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must run agreements. These agreements are established as a function of market payments and current grid

#	Organization	Yes or No	Question 7 Comment
			operations, and are therefore inappropriate for establishing criteria around determining which generators impact the bulk electric system. If the Standard Drafting Team insists on using the term it must, at a minimum, define what it means by this phrase.
7.26	Florida Municipal Power Agency	Yes	1.1, 1.8, 1.11 and 1.13 ought to be combined into a single supply-demand mismatch metric. Also, in 1.1, 2000 MW is arbitrary and in 1.13 4000 MW is arbitrary. And in 1.11, 300 MW is arbitrary and seems to coincide with DOE reporting requirements associated with EOP-004 which has nothing to do with BES Reliability. FMPA suggests: "Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that if destroyed, degraded, misused, or otherwise rendered unavailable, can cause a supply-demand mismatch exceeding the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group. Net Winter Real Power capabilities of generators are to be used in determining the supply side of determining the mismatch. The greater of actual coincident peak load, or forecasted peak load for the next year, of the Reliability Coordinator is to be used for the demand side of the equation. In the case where no Contingency Reserve or total reserve sharing obligations have been established, the supply-demand mismatch metric shall be equal to the largest loss of source plus 50% of the next largest loss of source for the Reliability Coordinator area."Such language addresses situations where a DC tie line may be the largest loss of source contingency for a region that is left as a gap in the existing definition, clarifies whether winter or summer generator capabilities are to be used, and used reliability related metrics instead of arbitrary targets. Similarly, the 1000 MW of 2.1 is arbitrary. A more appropriate metric would be the lowest expected value for a single contingency loss of source in the Reliability Coordinator area. For instance, assuming a 7% average forced outage rate for generators, using a metric of the second largest loss of source contingency in the Reliability Coordinator area for a supply-demand mismatch metric would give a greater than 99% confidence that the largest loss of source contingency at any given time is greater than that metric. Since the system is always operated to the worst case single

#	Organization	Yes or No	Question 7 Comment
			contingency at any moment, then, we would be quite confident in using the metric of the second largest loss of source contingency for Medium Impact. Hence, FMPA suggests that 2.1, 2.5 and 2.8 be combined using similar language to that which FMPA suggests for 1.1 using the second largest loss of source contingency in place of the reserve sharing obligation used in 1.1. that is:"Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that can cause a supply-demand mismatch exceeding the second largest loss of source contingency in the Reliability Coordinator Area." In 1.2, the 1000 MVARs is arbitrary. Additionally 1.2, 1.3, 1.7 and 1.10 ought to be combined using the same concept of exceeding IROLs. FMPA suggests:"Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding an IROL and/or an Adverse Reliability Impact" Similarly, the 500 MVAR in 2.2 is arbitrary. FMPA suggests combining 2.2 with 2.3 and 2.5 in a similar fashion:"Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding a SOL."Radial Facilities serving only load should not be included in 1.5 or 2.4. The term "Facilities" in these bullets is misused; a substation is NOT a Facility, but rather an interconnection point for multiple Facilities. Large auto-transformers and GSUs should not be excluded from the count. And, the distinction between the Interconnects is arbitrary and meaningless. FMPA suggests:"1.5 Transmission substations or switching stations with four or more Transmission Facilities operated at 300 kV or higher (for transformers, both primary or secondary winding > 300 kV, or a GSU of a registered generator)."By using the term Facilities, which by definition is a "... single BES Element", we also exclude radial serving only load Elements since those Elements are not Facilities. 2.4 would then be identical except using the 200 kV metric instead of 300 kV.In 2.6, the

#	Organization	Yes or No	Question 7 Comment
			distinction between the Interconnects is arbitrary and meaningless. The 300 kV metric should be used for all Interconnects. Black start and cranking paths should not be High Impact at all. High impact would be the system going black, a delay in restoring the system is a Medium Impact since the damage has already been done. Hence, 1.4 and 1.6 should be combined and made a Medium Impact. 1.14 is ambiguous. Is a tapped substation included in the count? Or a station on the end of a radial line? FMPA suggests associated the count of substations with 2.4, i.e.:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations identified in 2.4, or functionality that remotely controls a BES Cyber System with a High Impact Rating."
7.27	Southwest Power Pool Regional Entity	Yes	1.1: The criteria to include as High only the generation that exceeds the Contingency Reserve or reserve sharing obligation effectively removes nearly all generation resources from this impact category. 1.3: "Wide Area reliability impacts" as defined by the NERC Glossary of Terms (April 20, 2010) may be far too broad. If the unit is designated as RMR, it should be High impact regardless of the wide area consideration. 1.10: Please define the term "local area." 1.12 and 1.13: The Reliability Coordinator, and in the instance of a consolidated Balancing Authority, the Balancing Authority functions afforded a High impact categorization are fed real-time operational data from smaller, lower impact BES Cyber Systems owned and operated by other entities. Because of the criticality of the Reliability Coordinator and Consolidated Balancing Authority's near total reliance upon external real-time data sources, those sources need to also be afforded a High impact category. In particular, these BES Cyber Systems would include the EMS/SCADA and ICCP subsystems found in an entity's control center. 2.1: The 1000 MW criteria defining a Medium Impact generation asset will likely place

#	Organization	Yes or No	Question 7 Comment
			most generation into a Low Impact category.
7.28	Oncor Electric Delivery LLC	Yes	1.10 needs to better define “local area” (eg. 3 busses) Need criteria for “Low” such that “None” is the lowest level of protection required. Also, there is a need to have categories for systems with no IP communication or dial-up only communications.
7.29	LCEC	Yes	2.4 Replace transmission facilities with “Substations and/or switching stations and two or more non-radial transmission lines”. or”Transmission Facilities with four or more non-radial transmission lines operated at 200 kV or above in the Eastern and Western Interconnections, or 100 kV or above in the Texas and Quebec Interconnections, not included in Section 1.” 2.7 change to "non-radial" Transmission substations or switching stations or”Primary or Backup Control Centers that remotely control two or more Transmission substations or switching stations, each with four or more non-radial transmission lines, operated at 200 kV or above in the Eastern and Western Interconnections and 100kV or above in the Texas and Quebec Interconnections, or functionality that remotely controls a BES Cyber System with a Medium Impact Rating, not included in Section 1.”
7.30	Turlock Irrigation District	Yes	Attachement II criterion #1.4 states that BES Cyber Systems that can affect operations for Blackstart Resources in the Transmission Operator's restoration plan shall be categorized as High Impact. This should be changed to include only the Blackstart Resources in a region's Blackstart Capability Plan because Transmission Operator's restoration plans typically include Blackstart Resources that are not material to the restoration of the BES. Blackstart Resources that are material to the restoration of the BES are designated by each Regional Entity in accordance with NERC Standard EOP-007-0 titled "Establish, Maintain, and Document a Regional Blackstart Capability Plan". We suggest that the wording of criterion #1.4 be changed to "Generation Facilities designated as Blackstart Resources in the Regional Blackstart Capability Plan". Making this change would maintain consistency between the Standards and would also be consistent with the Purpose section of CIP-010-1 which states that the categorization of

#	Organization	Yes or No	Question 7 Comment
			BES Cyber Systems should be "commensurate with the adverse impact... on the reliability of the BES. Attachment II criterion #1.6 uses the term "primary Cranking Path". What is the meaning of the word "primary" as used in this context? We suggest that the wording be changed to "Facilities required to support Cranking Path(s) that are material to the restoration of the BES as used in a Transmission Operator's restoration plan per EOP-005".
7.31	Garland Power and Light	Yes	Attachment II 1.4 Should state that it is the Primary Black Start Unit and does not include the Next Start Unit.1.5 Multiple circuits between two substations should count as a single transmission line. General Comment Need to add “scoping filter” as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states “typically excludes business, market function systems, and non real-time systems”, then it is a good scope and we would agree
7.32	Powersouth Energy Cooperative	Yes	CIP-010 Attachment II 1.1 As drafted, if reserve requirements have not been established for an entity, generation facilities are considered High Impact if singularly or in combination exceed 2,000 MW. It seems to be reasonable to apply the 2,000 MW limit to reserves as well with reserve requirements only greater than 2,000 MW being considered as High Impact. 1.4 Additional consideration should be given to categorizing blackstart units in all cases as High Impact. Some units, while identified in a TO’s restoration plan, are not part of

#	Organization	Yes or No	Question 7 Comment
			the Regional Entities Restoration Plan. Some generation that may be used in a restoration effort may be removed from the TO's restoration plan to avoid implementation of High Impact security requirements. Some "middle ground" should be found so that more units can remain available in a restoration plan without being subject to costly security requirements and subsequently an increase in exposure for a utility to be non-compliant. It is recognized that there must be a sufficient number of blackstart critical units that remain protected by High Impact status to ensure restoration following an event. 1.10 Is "local area" meant to be the Balancing area or can the entity define local area. 2.1 As drafted, if reserve requirements have not been established for an entity, generation facilities are considered Medium Impact if singularly or in combination exceed 1,000 MW. It seems to be reasonable to apply the 1,000 MW limit to reserves as well with reserve requirements only greater than 1,000 MW being considered as Medium Impact. 3. Some consideration should be given to providing exclusions to exempt assets that in reality have no material impact.
7.33	City Utilities of Springfield, Missouri	Yes	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
7.34	MidAmerican Energy Company	Yes	Clarification is needed for the term "primary Cranking Path" (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term; however, "primary Cranking Path" is not defined. Item 1.4 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Larger entities submit multiple plans with many blackstart units and cranking paths. Protecting all blackstart units will divert valuable renounces from (better) protecting more valuable facilities. Draft definition of "primary Cranking Path": "Cranking Path and facilities included in the Transmission Operator's restoration plan as the preferred path and facilities for restoring the BES system to a stable condition with sufficient generation capacity synchronized to complete the full restoration of native load". Subsequently, CIP-010-1 Attachment II item 1.4 should be updated to only designate

#	Organization	Yes or No	Question 7 Comment
			Generation Facilities associated with the “Primary Cranking Path”. ALSO Mr. Scott Mix indicated in the May workshop that there should not be any CIP-002 critical asset systems that map to the CIP-010 low category. Current MW ratings in Attachment II Items 1.1 and 2.1 are set too high and will cause critical generating plants to move to the low impact category. Four critical units at MEC would move to low. Simultaneous loss of the four MEC units would impact the reliability of the BES. Set the MW level in Attachment II Item 1.1 to 500MW and Item 2.1 to 300MW.
7.35	PacifiCorp	Yes	Comments: Clarification is needed for the term “primary Cranking Path” (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term; however, “primary Cranking Path” is not defined. Item 1.4 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Larger entities submit multiple plans with many blackstart units and cranking paths. Protecting all blackstart units will divert valuable renounces from (better) protecting more valuable facilities. Draft definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for restoring the BES system to a stable condition with sufficient generation capacity synchronized to complete the full restoration of native load”. ALSO "Wide Area" impacts need to be clarified in Item 1.3 for "Must Run" units. ALSO Mr. Scott Mix indicated in the May workshop that there should not be any CIP-002 critical assets that map to the CIP-010 low category. Current MW ratings in Attachment II Items 1.1 and 2.1 are set too high and will cause critical generating plants to move to the low impact category. Set the MW level in Attachment II Item 1.1 to 500MW and Item 2.1 to 300MW.

#	Organization	Yes or No	Question 7 Comment
7.36	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Yes	Concerning generation facility capability, "rated net Real Power" can produce fictitious numbers that will never be attained. This should be the historical or commissioning test maximum net Real Power continuous output, whichever is greater. Wide Area is a very large area for WECC, as WECC is the RC. We are not sure if there are any generation facilities in WECC that have an impact on the whole of WECC. We are also not sure if generation being "pre-designated as reliability 'must run'" is a practice in all areas. It is possible that some units may be designated using other terminology or have detailed contracts. It may be better to remove the quotes and define Must Run Generation in the Glossary. Not all generation that is designated by the Transmission Operator's restoration plan as Blackstart is critical to the plan. It may be listed as a possible resource, but not a primary first choice. Further, much of the restoration plans are out of date and due for revision; requiring generation owners and operators to upgrade for CIP compliance only to have their plant removed in the new restoration plan in the next year or so would be wasteful. The purpose of a Blackstart resource in an old (pre-mandatory reliability standard compliance) restoration plan may be for local level of service resource for the TOP's local distribution area rather than a resource for BES reliability, i.e. the old plans to not coordinate well with each other. Last of all, should there not be a rating qualifier?
7.37	Detroit Edison	Yes	Criteria 1.3 and 2.3 should be removed for the following reasons: 1. The term "reliability must run" is not defined. 2. There is no generator that is so essential to reliability that it would need to run 100% of the time. 3. A generator could be required to run on a given day to serve load in an area that cannot be otherwise served due to a transmission constraint. This would be a temporary condition and should not warrant a high or medium classification.
7.38	Cogeneration Association of California and Energy Producers & Users	Yes	Criteria 2.4 should be clarified. The criteria states "Transmission Facilities with four or more transmission lines operated at 200kV or above..." Do two transmission lines, each with two circuits that can operate independently for a total of four circuits, count as two

#	Organization	Yes or No	Question 7 Comment
	Coalition		transmission lines or four transmission lines?
7.39	Exelon Corporation	Yes	Each of the criteria needs to either align with the other existing standard requirements, or have a technical basis or business risk mitigation basis to be defined as criteria. It would be very beneficial to the industry's understanding of each requirement if the basis for each was included in the Attachment. A specific example is the 4 or more Transmission line requirement. The previous draft had a 3 or more Transmission line requirement, so what was the basis for the 3 or more and, moreover, what is the basis for now changing it to 4 or more? The technical basis for generation limits in Attachment II is not provided. That is, the basis for the 2000 MW and 1000 MW thresholds appear arbitrary. Combined losses of greater than these values have occurred without significant impact to the BES. No "reasonable bounds" are allowed. For example, if a common vendor provides a cyber product in multiple generating stations, it appears that the assumption is that this common product, no matter how local its impact, creates a common mode failure for all plants simultaneously, resulting in the determination before the fact that this product will be rated as High Impact. No allowance is made for geographical location. For example, if a common cyber system is used in several large generating stations in different regions of the country, their simultaneous loss may result in no significant impact to the BES. However the deterministic MWe thresholds and simple "in combination" wording will result in virtually all such cyber systems rated as high, deterring use of common vendors, standardization, and economies of scale. Although moving to a more deterministic approach can be seen as increasing consistency in application of the standard, it would appear that a deterministic approach will decrease the flexibility of operation now allowed and may in fact, reduce BES reliability. As a modification to the Attachment, Exelon suggests that the existing deterministic criteria could be used, unless an entity chooses to show by actual historical data or modeling that such losses do not result in significant impact on the BES. This performance-based criteria could be expanded to define high, medium, and low impacts on the BES in terms of stability, voltage swing, etc.

#	Organization	Yes or No	Question 7 Comment
7.40	American Transmission Company	Yes	For R1.4, we propose changing text from “designated as Blackstart Resources” to “designated as the primary Blackstart Resources” (similar to primary Cranking Path in 1.6). Add “restoration plan per EOP-005” (similar to 1.6). Note that Transmission Operators can only designate Blackstart Resources that have been volunteered to them by Generation Owners. All GO may choose not to volunteer any Blackstart Resources if they don’t want their associated cyber systems to be subject to this standard. For R1.10, we propose removing SPS from the criteria. SPSs cannot be approved by the Regional Entities unless they have been designed not to be critical to the BES (e.g., not critical if they operate when they should not or do not operate when they should).
7.41	SCE&G	Yes	How does the SDT see AGC coming into play in 1.1? Would every generator operated on AGC (if the aggregated total met the contigency reserve commitment) be considered high impact, or just the centralized AGC itself?" Must Run" units needs to be clarified. Who determines if a unit is "must run"? 1.4 This language needs to be clarified to identify resources designated as "Primary" Blackstart resources. 1.5 Transmission lines should be change to Transmission Lines to utilize the NERC Definition 1.8 Is this misusing/destroying one Transmission Facility at a time? SDT should consider defining "Transmission Facility" as a whole instead of utilizing separate NERC Definitions for "Transmission" and "Facility"
7.42	Entergy	Yes	If “size” of an electric facility remains the primary key differentiator for applicability of CIP requirements, which Entergy does not support, the following should be considered: 1. High Impact Rating (H)”Each BES Cyber System that can affect operations for: 1.1. Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation Facilities), whose aggregate rated net Real Power

#	Organization	Yes or No	Question 7 Comment
			capability exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group . In the case where no Contingency Reserve or total reserve sharing obligations have been established, Generation Facilities , singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW." Attachment II of CIP-010-1 qualifier 1.1 as stated above includes those generation facilities that have the capability to exceed the Contingency Reserve as High Impact to the BES. This is not truly indicative of the impact to the reliability to the BES. Entergy has multiple generation facilities with the capability to exceed the contingency reserve. However, their Service Hours (SH) are less than 900 hours and a Service Factor (SF) is less than 1.0, averaged over the past five years, where: - Definitions from GADS Data Reporting Instructions - January 2010- Service Hours - SH is the sum of all Unit Service Hours.- Period Hours - PH is the number of hours in the period being reported that the unit was in the active state.- Service Factor - SF = SH/PH x 100% Entergy proposes that a better representation for how much a generation plant runs, and therewith potential adverse impact on BES reliability, would be better determined by a measurement of the percent of SH, e.g., running at least 80% of the year; SH greater than 7008 hours per year, or, a SF of greater than 80% per year. Therefore, suggested alternative language for 1.1 is: "Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation facilities the unit with the highest Service Factor is used to determine applicability), whose Service Factor (Service Factor = Service Hours per Year / Hours per Year X 100%) is equal or greater than 80% for a five year average." Additionally, extending this logic to the Medium Impact BES Cyber Systems, Entergy suggests replacement of language concerning Medium Impact Rating (M) 2.1 from: "Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to most current rated net Real

#	Organization	Yes or No	Question 7 Comment
			Power capability of 1000 MW or more, not included in Section 1." To: "Generation Facilities, singularly or in combinations (if using a shared BES Cyber System that affects multiple generation facilities the unit with the highest Service Factor is used to determine applicability) with equal to or greater than 70% for a five year average."
7.43	Edison Mission Marketing and Trading	Yes	If we are going to use the High, Medium, and Low and there is not going to be a does not apply category, then there should be an engineering analysis or study performed by the BA's, RC's or an independent firm and it should include which sites/generators are critical and which are not and why. Once completed then and only then do we begin categorizing them into whatever scale the Standard Drafting Team and the included entities agree upon. As it is stands now we not only have to include nominal size generators, but wind sites as well.
7.44	Puget Sound Energy	Yes	In 1.6, the restoration plan is linked to EOP-005, shouldn't the restoration plan mentioned in 1.4 be linked to EOP-005 as well? It appears that all BES Cyber Systems must fall into one of three categories. Are there any other criteria that would all for something not to be categorized as one of these three (i.e., such as non-dispatchable wind generation)? Also Blackstart should only classify as high those needed for primary region wide restoration since some (such as ours) are more secondary paths and there should be some minimum level of generation to be classified low. There is no need to classify as low a 20 MW hydro generator that does not impact BES reliability. We would recommend 300 MW.
7.45	Alliant Energy	Yes	In Article 1.3 we believe including "must-run" as listed is problematic. This could fluctuate in response to maintenance outages on lines, etc. The must-run units have to be tied to a long-term study that shows the need for a reliability must-run unit, not short-term analyses to reflect changing conditions.

#	Organization	Yes or No	Question 7 Comment
			Article 1.4 - By including "All Black-Start Units" the standard is utilizing a "one-size-fits-all" strategy that the industry has recognized does not work for everything, and is working to address. All Black-Start units do not carry the same importance and this should be recognized in the standard. This philosophy may be counter-productive to system reliability as one classification may reduce the number of Black Start units that would be made available to a TOP's restoration plan due to the high initial security cost and the future possible financial risk of strict compliance guidelines with penalties. There should be a recognized hierarchy for the Black-Start resources, similar to the High, Medium, and Low for BES Cyber Systems. This methodology would assure Black Start units could be categorized by attributes in general to support the BES during a blackstart event. Each Balancing Authority Area (BAA) could be required to have a minimum number of high priority Black Start units depending on the BAA size to support the area during a black out. Lower priority units would be used for stabilizing power at generating stations, local area islanded load and used as a backup plan if all other contingency plans would fail. Article 1.6 - This item should reflect the same categorizing as is recommended in the comment to Article 1.4 above. Article 2.1 - Please clarify "with aggregate higher of the most current and prior to most current rated net Real Power capability." We believe it would be clearer if stated as below: "Generation Facilities, singularly or in combination (if using a shared BES Cyber System) with a rated Real Power capability of 1000 MW or more, not included in Section 1." Article 2.3 - we believe including "must-run" as listed is problematic. This could fluctuate in response to maintenance outages on lines, etc. The must-run units have to be tied to a long-term study that shows the need for a reliability must-run unit, not short-term analyses to reflect changing conditions.
7.46	Public Service Enterprise Group companies	Yes	In general there is agreement with the R2 text. However, in Attachment II, statement 1.4 entails categorizing all Blackstart Units with a "High Impact Rating", while statement 1.6

#	Organization	Yes or No	Question 7 Comment
			requires that only the “primary cranking path” transmission facilities need to be categorized with a “High Impact Rating”. Statement 1.6 implies that some Blackstart Units, although categorized with a “High Impact Rating” would not be afforded transmission facilities with the same risk categorization. We recommend changing statement 1.6 to include only Blackstart Units that are in the primary cranking path.
7.47	ReliabilityFirst Staff	Yes	In Part 1.1, the referent for “largest value” does not seem to be appropriate. Suggest changing the wording to “average value.” In Part 1.4, a “Blackstart Resource” is only the first resource that starts in a system restoration. Suggest changing the wording to “Generation Facilities required to support the Cranking Path(s) identified in Part 1.6.” In Part 1.6, a “primary” Cranking Path is not required to be identified in an entity’s restoration plan by EOP-005. Suggest changing the wording to “Facilities required to support at least one Cranking Path.” In Part 1.10 “local area” should be defined. As we are not certain what is meant by this term, we have no suggested wording.
7.48	RRI Energy	Yes	Include or add a "No impact category" that is determined by the RC.
7.49	MRO's NERC Standards Review Subcommittee	Yes	Item 1.3 We believe this item may be problematic in nature, as the designation of reliability “must run” units is something that could fluctuate. This would create administrative difficulties for an entity and their RTO as a unit moves between Impact Ratings. We believe this item needs further clarification to indicate its true intent, such as who stipulates the “must run” designation, what constitutes “reliability must run”, etc. Item 1.4 Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator’s restoration plan as having a High Impact Rating with regards to the Bulk Electric System. Albeit on a smaller scale, this appears to be the same “one size fits all” approach of the current standards that the SDT is working so diligently to address. In reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System.

#	Organization	Yes or No	Question 7 Comment
			Therefore, we believe there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact. To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. A 10 MW Blackstart Resource that directly supports restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, we would propose judging the relative importance of a Blackstart Resource by the relative importance of the facilities it directly supports. We would recommend rewording item 1.4 as follows, leveraging the existing language of Item 1.8: "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above." We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.5 We need to clarify the meaning of "Transmission lines". If a 300 kV substation has a terminal connected to a 345/115 kV transformer, which then feeds a 115 kV transmission line leaving the facility, does this constitute a 115 kV or 345 kV "Transmission line" within the context of this item? For this example, we would interpret this to be a 115 kV line, so it would not be included in the Transmission line count for the substation bright line. We also believe the bright line should take higher voltages in to consideration. A substation with three 765 kV lines would not be High Impact, but a substation with four 345 kV lines would be. We propose additional criteria of two or more 500 kV lines, or

#	Organization	Yes or No	Question 7 Comment
			simply adding to/changing the High Impact criteria along the lines of the Medium Impact criteria (item 2.6), calling out "Transmission Facilities operated at 500 kV or higher..." Item 1.6 We would recommend rewording item 1.6 as follows for consistency in approach with the proposed Item 1.4: "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 1.1 above."We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.14 We would recommend rewording item 1.14 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more BES Cyber Systems with a Medium Impact Rating, or one or more BES Cyber Systems with a High Impact Rating."We believe this approach should provide a better sense of a control center's true impact on the Bulk Electric System. Item 2.7 We would recommend rewording item 2.7 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control one or more BES Cyber Systems with a Medium Impact Rating, not included in Section 1."We believe this approach should provide a better sense of a control center's true impact on the Bulk Electric System. Section 2 Additions We would recommend adding the following items under section 2, Medium Impact Rating, for consistency in approach with the proposed Items 1.4 and 1.6: o "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility

#	Organization	Yes or No	Question 7 Comment
			with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1." o "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1." We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.
7.50	Minnesota Power	Yes	Item 1.4: Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator's restoration plan as having a High Impact Rating with regards to the Bulk Electric System. In theory, on a smaller scale, this appears to be a "one size fits all" approach, but in reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System. Therefore, Minnesota Power believes that there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact. To implement this approach, Minnesota Power believes it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just the fact that it has been included. For example, a 10 MW Blackstart Resource that directly supports restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, Minnesota Power proposes that the Standards Drafting Team allow Registered Entities to assess the relative importance of a Blackstart Resource based on the importance of the facilities it directly supports. Minnesota Power recommends rewording item 1.4 as follows utilizing the existing language of Item 1.8:

#	Organization	Yes or No	Question 7 Comment
			"Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above." Minnesota Power believes this approach will provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.14: Minnesota Power recommends rewording item 1.14 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more BES Cyber Systems with a Medium Impact Rating, or one or more BES Cyber Systems with a High Impact Rating."Minnesota Power believes that this approach will provide a better sense of a control center's true impact on the Bulk Electric System. Item 2.7: Minnesota Power recommends rewording item 2.7 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control one or more BES Cyber Systems with a Medium Impact Rating, which are not included in Section 1."Minnesota Power believes that this approach will provide a better sense of a control center's true impact on the Bulk Electric System. Section 2 Additions: Minnesota Power recommends adding the following items under section 2, Medium Impact Rating, for consistency with the proposed Item 1.4:"Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1."Minnesota Power believes that this approach will provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.

#	Organization	Yes or No	Question 7 Comment
7.51	The Empire District Electric Company	Yes	Item 1.4 Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator's restoration plan as having a High Impact Rating with regards to the Bulk Electric System. Albeit on a smaller scale, this appears to be the same "one size fits all" approach of the current standards that the SDT is working so diligently to address. In reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System. Therefore, we believe there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact. A regional study performed by the regional entities would be an excellent approach to determine this. To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. A 10 MW Blackstart Resource that directly supports restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, we would propose judging the relative importance of a Blackstart Resource by the relative importance of the facilities it directly supports. We would recommend rewording item #1.4 as follows, leveraging the existing language of Item #1.8: "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above." Since item #1.6 is also related to system restoration, we would recommend rewording it as follows for consistency in approach: "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as

#	Organization	Yes or No	Question 7 Comment
			described in Part 1.1 above." We would also recommend adding the following items under section 2, Medium Impact Rating: o "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above." o "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 2.1 above." We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.5 We need to clarify the meaning of "Transmission lines". If a 300 kV substation has a terminal connected to a 345/115 kV transformer, which then feeds a 115 kV transmission line leaving the facility, does this constitute a 115 kV or 345 kV "Transmission line" within the context of this item? For this example, we would interpret this to be a 115 kV line, so it would not be included in the Transmission line count for the substation bright line. We also believe the bright line should take higher voltages in to consideration. A substation with three 765 kV lines would not be High Impact, but a substation with four 345 kV lines would be. We propose additional criteria of two or more 500 kV lines, or simply changing the High Impact criteria to mirror that of the Medium Impact (item 2.6), calling out "Transmission Facilities operated at 500 kV or higher...".
7.52	Lincoln Electric System	Yes	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS), which address the current structure of Attachment II as proposed. However, LES believes a better overall approach would be applying

#	Organization	Yes or No	Question 7 Comment
			Engineering studies to truly determine a facility's impact on the Bulk Electric System. We realize an Engineering study is not as simple as a "bright line" based metric. Unfortunately, the Bulk Electric System is not a simple system - it is actually very complex. So in order to properly assess the importance of the various facilities that make it up, LES feels a complex Engineering study is required.
7.53	Luminant	Yes	Medium Impact: an item for TO, TOP, GO, GOP Functions performed at primary or backup control centers has been left off of attachment 2. This was in the previous posting as item 2.6"Control Centers and backup Control Centers controlling transmission ...
7.54	Nuclear Energy Institute	Yes	Need to clarify the expectations for a multi unit generation site. For example: Under what conditions would a site containing two separate 900 MW generators be considered "Medium Impact Rating" because the total site would now be greater than 1000 MW? Similarly, when would a site that had three separate 900 MW generators be considered "High Impact Rating" because the total site would now be greater than 2000 MW?
7.55	NextEra Energy Corporate Compliance	Yes	NextEra finds that a catch-all for Low impact is a fatal flaw. There should be some threshold that is justified for low. For example, a proper minimum criteria for LOW impact BES Cyber Systems could be:Cyber Systems that control BES level facilities that meet one of the following: 1) three or more transmission circuits operated at 100 kV or above not covered in Section 1 or 2, 2) two or more transmission circuits and two or more autotransformer with a secondary voltage 100kV or above,3) two or more transmission circuits and generation capacity at the site of greater than 1000MW Alternatively, a NO IMPACT category may be added which eliminates subjectivity in which BES Cyber components need to be reviewed. Single point buses representing looped load serving type stations cannot produce results worse than single contingency which must be operated to at all times. An additional item that should be specifically covered is the use of remote access for transmission and / or generation control locations and their applicability to the High, Medium, Low and/or No impact criteria.

#	Organization	Yes or No	Question 7 Comment
			The term "affect operations" can be subjective and can be open to interpretation. NextEra suggests changing the15 minute requirement to “in real time (instantaneous). For example, closed loop control, which does not allow time for human intervention.” NextEra also recommends adding the word “both” prior to monitor and control. NextEra would also like to know what does 1.1.1 of section D mean? This is unclear. A suggestion would be eliminating or providing a specific definition.
7.56	Pacific Gas & Electric Company	Yes	Not all blackstart resources should necessarily be considered high impact. Suggest revising 1.4 as follows: Generation Facilities designated as Blackstart Resources and explicitly listed as essential to the restoration of the BES in the Transmission Operator’s restoration plan.
7.57	Northeast Utilities	Yes	NU is concerned with some of the impact criteria in Attachment II related to generation facilities. To base impact on “bright line" Facility Rating thresholds, i.e., MW, kV, MVAR, etc., could lead to mis-categorization and ultimately unprotected cyber systems. These thresholds do not take into consideration regional differences in configuration and load flows. Therefore, it is our suggestion that categorization could be based on the results of a regional engineering study, similar to what is currently required in the TPL Standards. This study could be conducted by the regional Planning Authority(s) or an independent third party and approved by the Regional Entity. The results of the study would identify the contingencies that have the potential to cause levels of impact to the BES.
7.58	Matrikon Inc.	Yes	Please describe how the 15-minute time horizon would fit into Attachment 2. Is the intent for the 15-minute horizon to provide a level of realism to determination of impact? To bring in more BES Cyber systems that could have indirect impact, or an escape clause if effects don’t occur within 15 minutes?
7.59	USACE HQ	Yes	Please read answer to question 4.

#	Organization	Yes or No	Question 7 Comment
7.60	BGE	Yes	Provide additional clarification of "automatic aggregate". For instance, does automatic mean an application that is kicked off without human intervention or does automatic mean after an operator hits a button? Suggest adding the word "instantaneous" before load shedding to clarify. Additional clarification on 1.14 (What is meant by "functions")
7.61	Southwestern Power Administration	Yes	Rather than numerous bright line requirements that may or may not actually have a significant effect on the BES, depending on the surrounding topology, operating procedures, or configuration of a particular Responsible Entity, a better approach may be to include performance/results-based criteria in Attachment II. However, if the current approach is forwarded, I would suggest the following improvements: 1.4. Generation Facilities designated as Primary Blackstart Resources in the entity's restoration plan. 1.7 Transmission Facilities, including Flexible AC Transmission Systems (FACTS), that, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more Interconnection Reliability Operating Limits (IROLs). 1.10 Special Protection Systems (SPS), Remedial Action Schemes (RAS) or automated switching systems that operate BES Elements that if destroyed, degraded, or misused, would violate one or more Interconnection Reliability Operating Limits (IROLs). 1.11. Delete. Is this not a Control Center issue? 1.12. Control Centers that perform the Reliability Coordinator functions. 1.13. Control Centers that perform the Balancing Authority functions for 4,000 MW or more in Eastern and Western Interconnections and 2,000 MW or more in the Texas and Quebec Interconnections. 1.14. Control Centers that perform the Transmission Operator functions for a Facility

#	Organization	Yes or No	Question 7 Comment
			with a High Impact Rating. 2.4. Transmission Facilities that, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more System Operating Limits (SOLs) 2.7. Control Centers that perform the Transmission Operator for a Facility with a Medium Impact Rating, not included in Section 1. 2.8. Control Centers that perform the Balancing Authority functions for 2,000 MW or more in the Eastern and Western Interconnections and 1,000 MW or more in the Texas and Quebec Interconnections, not included in Section 1.
7.62	Southern California Edison Company	Yes	SCE believes Attachment II should be modified to account for only the capacity that can be controlled by qualifying systems. As currently written, Attachment II defines the amount of generation under control as the rated capacity of the resource. This is not accurate for some systems which can only control the resource between certain points (e.g. minimum operational output [Pmin] and maximum operational output [Pmax]). This could drastically overstate the impact of the cyber system on the BES. For example, suppose that a cyber system controlled a generating resource with maximum capacity of 2,000 MW. According to attachment II, this would then categorize as "high impact rating". However, suppose further that the system can only control the unit between its Pmin and Pmax which are 1,500 and 2,000 respectively. This would place the system in a "low impact rating" according to the attachment. For that reason, SCE believes that Attachment II should be modified to account for only the capacity that can be controlled by the system.
7.63	San Diego Gas and Electric Co.	Yes	SDG&E recommends aiming for a limitation of scope related to those assets that are truly high and medium impact categorizations. Some of the high and medium items could have "BES outage" or reliability implications but may not necessarily result in instability of the BES. We recommend having consistency in the application of the assets included in the impact categories to the BES as a whole.

#	Organization	Yes or No	Question 7 Comment
7.64	Constellation Energy Control and Dispatch, LLC	Yes	See answer to Question 4.
7.65	Constellation Energy Commodities Group Inc.	Yes	See answer to Question 4. Please clarify the intended treatment of a Generation Management System ("GMS"). Attachment II implies that capacity monitored by a GMS system would be aggregated to determine its impact categorization. However, to be consistent with the intention to protect connections that truly impact the BES net real power capability should only be aggregated within a balancing authority.
7.66	MWDSC	Yes	See comments for question 4 above.
7.67	Wolverine Power	Yes	See comments listed for 1.a
7.68	Dynegy Inc.	Yes	Show examples of how the identification and categorization and tie-in to Attachment II would work.Also, for 1.1, either increase the net MW rating or add an annual capacity factor to a generating unit to account for old units at a site that no longer run because no longer economical. These types of facilities should not have to meet High category requirements if they no longer run. Also, for 1.3 add more detail. Explain pre-designated. Assigned by who? Explain Wide Area reliability impacts.
7.69	WECC	Yes	Similar to our previous comment, if Attachment 1 is expanded to include in scope reliability coordination functions critical to reliable operation of the BES outside of 15 minutes the impact levels need to be updated. While many functions of a Reliability Coordinator are critical and should be an high impact, not all functions of reliability coordination should be made high impact. For instance, Coordinated Outage systems while important to the reliability of the BES and should be in scope, should best be classified as a low-impact BES Cyber System. The considerations for identification and categorization has been elevated to a high level such that BES Cyber Systems and not individual devices are identified based on their specific functionality. It is suggested that if BES Cyber Systems are to be indentified and

#	Organization	Yes or No	Question 7 Comment
			categorized there be some inclusion and development of a process to granulate these systems down to their individual component level. Further, the quantitative qualification bar has been set to level that precludes most BES Cyber Systems from reaching identification as a high or even medium level of impact. Taking into account. If a BES Cyber System can impact reliability a baseline set of security controls should be established that creates tracking for all assets, accountability for access to these assets, and physical and electronic protection for these assets. Specific Line Item Comments(1.1) The standard, as drafted, seemingly excludes all generation but large dams, large mine-based coal plant and nuclear plants?(1.1) The developed sentence structure lends itself to multiple interpretations and will prove to be difficult to audit consistently. (1.1) Is the term aggregated defined as geographically co-located, common substation, common communication paths, etc?(1.6) What about redundant paths? There is no requirement to identify and document multiple paths. (1.6) A reference to EOP-008 would also be appropriate.
7.70	Con Edison of New York	Yes	Specific comments on the Categorization: The impact categories should be linked to the reliability Standard functions in Attachment I. Therefore, the High, Medium and Low ratings should reference specific Standards whenever possible. o 1.1: This requirement should be broken down into two requirements. One should refer to BAL-002 and reserves needed to be compliant. The second should be any generation facility with a common BES Cyber System greater than 2,000 MW. o 1.2: This should be linked to the function of “controlling voltages”. Two other concerns; first - shunt reactors and capacitors are not included and second - there needs to be a technical basis for a Reactive Power capability limit. o 1.3: Suggest moving to “Low” category since reliability must run equipment is frequently a local congestion or voltage control situation. This would not qualify for a “High” impact rating.

#	Organization	Yes or No	Question 7 Comment
			o 1.4: Black start resources should only be designated as a High Impact Rating if they are the only resource in the TOP's restoration plan. If the TOP has multiple restoration resources and procedures, the resources should be a Medium Impact Rating. Reference this to EOP standards. o 1.5: OK o 1.6: This item should be included in item 1.4 o 1.7: FACTS devices are used to control voltage and power flow. o 1.8: This should be included in requirement 1.1 o 1.9: OK o 1.10: Refer to PRC standards o 1.11: A basis for the 300 MW or greater UFLS system should be provided. o 1.12, 1.13, and 1.14 address Control Centers and should be aggregated into one requirement based on RC functions, BA functions, TOP functions and TO functions. In addition, there may be a conflict between a Control Centers with a "Low Impact Rating" and a single substation with a "High Impact Rating". The DT should consider addressing this conflict where the "BES Cyber Security Components" on one side of a device (e.g. breakers) is a "high impact" while the command signal will be a "low impact" device. General comment on criteria for categorization: Overall, the high, medium, and low levels do not properly meet the needs of the BES. The DT should be looking at what the system does and determining its ability to impact the BES rating rather then the impacted equipment. For example, SCADA systems should be High whether they are on the 138 kV or 345 kV. Wide scale damage can be done with access to the SCADA system, however only local issues can occur with access into a single non-networked microprocessor relay. Alarm panels and other microprocessor that do not have direct impact should also be at lower level. Items that set levels should be a medium level. Basis for criteria for categorization is needed:

#	Organization	Yes or No	Question 7 Comment
			Attachment II to CIP-010 contains a number of what appear to be administratively determined "bright lines." Please provide both the detailed rational supporting each "bright line" and a specific quantification of the reliability benefits resulting from its implementation. In responding to this question, please focus more on the technical, reliability-related rational and improvements for each "bright line" selected, rather than on the source of any particular number. Reference any white papers, studies, expert opinion, or other documentation relied upon and supporting the "bright lines" selected. For example, in Attachment II category High Impact for item 1.11, please explain why 300 MW was selected. We are not so much interested in any reference to a 300 MW EOP-004 DOE reporting requirement, as we are in the specific criticality of the 300 MW level to BES reliability, e.g., 300 MW represents a large (>10%) percent of area load, or in the case of inadvertent actuation would cause an uncontrolled system instability(ies) and cascading, or in the event of a failure-to-actuate would cause the Interconnection UFLS program not to return frequency to nominal within the program required time period. What if for a given entity 300 MWs is not a significant percentage of local load, or inadvertent actuation would not cause uncontrolled instability and cascading, or failure-to-actuate would not prevent the return of frequency to normal within the required time period? Why rate such aggregate automatic load shedding "High" rather than "Medium" or "Low?" Are there any Interconnection-wide studies which would support this 300MW "bright line" value? Please provide any reference(s).
7.71	Allegheny Energy Supply	Yes	Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact.

#	Organization	Yes or No	Question 7 Comment
7.72	Allegheny Power	Yes	Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. Clarification is needed for the term “primary Cranking Path” (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term, however, “primary Cranking Path” is not defined. Item 1.3 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Most larger entities submit multiple plans with multiple blackstart units and cranking paths. Protecting all blackstart units may divert finite resources from (better) protecting more valuable facilities. Moreover, it is not appropriate to create a perverse incentive for system owners and operators to reduce the current flexibility and diversity of multiple blackstart units and cranking paths by requiring a level of protection that is not proportional to the level of impact to restoration of the BES. Draft definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for restoring the BES system to a stable condition with sufficient generation capacity synchronized to complete the full restoration of native load”. Regarding 1.7, we recommend striking “Flexible AC Transmission Systems (FACTS)” because it would be included within Transmission Facilities. Although capitalized, it does not appear in the NERC Glossary of terms The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact. Under Frequency Load Shed systems under a common control system.

#	Organization	Yes or No	Question 7 Comment
7.73	EEI	Yes	Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. Clarification is needed for the term “primary Cranking Path” (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term, however, “primary Cranking Path” is not defined. Item 1.4 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. As a result, the drafting team should consider whether to combine Items 1.4 and 1.6. Moreover, most larger entities submit multiple plans with multiple blackstart units and cranking paths. Protecting all blackstart units may divert finite resources from providing additional protections for more valuable facilities. Moreover, this may create incentives for system owners and operators to reduce the current flexibility and diversity of multiple blackstart units and cranking paths by requiring a level of protection that is not proportional to the level of impact to restoration of the BES. It is not appropriate to expand the definition of blackstart to include full restoration of native load, that would essentially include all or most of the BES. The objective here is to prioritize, and augment security for the elements needed to begin system restoration. EEI suggests the following definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for initial system restoration”. In addition, the drafting team should modify the wording to only include units designated on a seasonal or annual basis. Regarding 1.7, EEI recommends striking “Flexible AC Transmission Systems (FACTS)” because it would be included within Transmission Facilities. Although capitalized, it does

#	Organization	Yes or No	Question 7 Comment
			not appear in the NERC Glossary of terms Suggest Adding: 1.15 Control Centers including Generation Control Centers. Also, we suggest that the drafting team place the highest impact facilities earlier (e.g. 1.1) on the list. The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact. EEI suggests that 1.11 in Attachment II be revised as follows:"BES Elements that perform automatic aggregate load shedding of 300 MW or more under a common control system."]
7.74	APPA Task Force	Yes	The APPA Task Force commends the drafting team on their work on CIP-010-1. We appreciate the team's consideration of our Task Force comments from the previous informal comment period. We feel it is especially important for entities to have the option of categorizing the impact level based on the Contingency Reserve or total of reserve sharing obligations as stated in 1.1. However, we are concerned with the "bright line" Facility Rating thresholds, i.e., MW, kV, MVAR, etc. These thresholds do not have a basis from industry experience and could be challenged by entities or regulators. We are concerned that having chosen these numbers without empirical data supporting them, the numbers can easily be changed without the supporting empirical data. It is our recommendation that these numbers be evaluated more closely. At a minimum, the thresholds should be quantified to show what percentage of generation and transmission facilities would be designated under each Impact Rating. Florida Municipal Power Association (FMPA) provided some suggested alternative calculation methods for the Impact Categorization of Attachment II. We provide them here for the drafting team's discussion in evaluating the bright line thresholds. FMPA Comments:

#	Organization	Yes or No	Question 7 Comment
			Categorization could be based on the results of a regional engineering study, similar to what is currently required in the TPL Standards. This study could be conducted by the regional Planning Authority(s) or an independent third party and approved by the Regional Entity. The results of the study would identify the contingencies that have the potential to cause the following levels of impact to the BES: o High (has the potential to cause an Adverse Reliability Impact) o Medium (has the potential to require planned/controlled loss of load) o Low impact (has no potential to cause loss of load) Make changes to existing criteria: 1.1, 1.8, 1.11 and 1.13 ought to be combined into a single supply-demand mismatch metric. Also, in 1.1, 2000 MW is arbitrary and in 1.13 4000 MW is arbitrary. And in 1.11, 300 MW is arbitrary and seems to coincide with DOE reporting requirements associated with EOP-004 which has nothing to do with BES Reliability. FMPA suggests: "Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that if destroyed, degraded, misused, or otherwise rendered unavailable, can cause a supply-demand mismatch exceeding the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group. Such language addresses situations where a DC tie line may be the largest loss of source contingency for a region that is left as a gap in the existing definition, clarifies whether winter or summer generator capabilities are to be used, and used reliability related metrics instead of arbitrary targets. Similarly, the 1000 MW of 2.1 is arbitrary. A more appropriate metric would be the lowest expected value for a single contingency loss of source in the Reliability Coordinator area. For instance, assuming a 7% average forced outage rate for generators, using a metric of the second largest loss of source contingency in the Reliability Coordinator area for a supply-demand mismatch metric would give a greater than 99% confidence that the largest loss of source contingency at any given time is

#	Organization	Yes or No	Question 7 Comment
			greater than that metric. Since the system is always operated to the worst case single contingency at any moment, then, we would be quite confident in using the metric of the second largest loss of source contingency for Medium Impact. Hence, FMPA suggests that 2.1, 2.5 and 2.8 be combined using similar language to that which FMPA suggests for 1.1 using the second largest loss of source contingency in place of the reserve sharing obligation used in 1.1. that is: "Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that can cause a supply-demand mismatch exceeding the second largest loss of source contingency in the Reliability Coordinator Area." In 1.2, the 1000 MVARs is arbitrary. Additionally 1.2, 1.3, 1.7 and 1.10 ought to be combined using the same concept of exceeding IROLs. FMPA suggests: "Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding an IROL and/or an Adverse Reliability Impact." Similarly, the 500 MVAR in 2.2 is arbitrary. FMPA suggests combining 2.2 with 2.3 and 2.5 in a similar fashion: "Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding a SOL." Radial Facilities serving only load should not be included in 1.5 or 2.4. The term "Facilities" in these bullets is misused; a substation is NOT a Facility, but rather an interconnection point for multiple Facilities. Large auto-transformers and GSUs should not be excluded from the count. And, the distinction between the Interconnects is arbitrary and meaningless. We suggest:

#	Organization	Yes or No	Question 7 Comment
			”1.5 Transmission substations or switching stations with four or more Transmission Facilities operated at 300 kV or higher (for transformers, both primary or secondary winding > 300 kV, or a GSU of a registered generator).” By using the term Facilities, which by definition is a “… single BES Element”, we also exclude radial serving only load since that those Elements are not Facilities. 2.4 would then be identical except using the 200 kV metric instead of 300 kV. In 2.6, the distinction between the Interconnects is arbitrary and meaningless. The 300 kV metric should be used for all Interconnects. 1.14 is ambiguous. Is a tapped substation included in the count? Or a station on the end of a radial line? FMPA suggests associated the count of substations with 1.5, i.e.:”Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations identified in 1.5, or functionality that remotely controls a BES Cyber System with a High Impact Rating.” End of FMPA comments. The APPA Task Force also supports the proposal by the MRO-NERC Standards Review Subcommittee (MRO-NSRS) in their comments on Item 1.4 and 1.6 to assign the impact rating of blackstart units and cranking path relative to assigned impact rating of the generating facilities it directly supports. We feel that inclusion of all blackstart resources in the High Impact Rating will waste limited resources protecting facilities which are not in support of High Impact generation. MRO-NSRS proposal: High Impact:1.4 “Generation Facilities designated as Blackstart Resources in the Transmission Operator’s restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above.” 1.6 “Facilities required by the Transmission Operator’s restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated

#	Organization	Yes or No	Question 7 Comment
			capabilities as described in Part 1.1 above."Medium Impact:2.X "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1." 2.X "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1."
7.75	US Bureau of Reclamation	Yes	The criteria defined in this and several previous requirements are based around BES Cyber Systems, which under the definition of BES (per the WECC Glossary) does not include all power system assets. Therefore, there appears to be a category of Cyber Assets that do not presently require any protection measures (i.e., they might control a powerplant feeding a radial load or be associated with a system of less that 100kV. The classification "Low" will potentially include those systems which do not have an impact. It is counterintuitive to classify a system as low when it has No Impact. The Team should develop a description of "Low" similar to that which was provided for "High" and "Medium". Then the Drafting Team could issue a statement that systems not classified as "High", "Medium" , or "Low" would be classified as "No Impact".
7.76	Dominion Resources Services, Inc.	Yes	The criteria for categorization of Low Impact systems is too broad and uses the terminology "can affect" which the SDT has appropriately recognized is ambiguous. The following alternate wording is proposed:"All other BES Cyber Systems not categorized as having a High or Medium Impact rating that are required for the reliable operation of the BES."
7.77	Southern Company	Yes	The definition of "pre-designated as Reliability must run" in Attachment II, 1.3 is unclear and cannot be implemented with existing practices in some utilities. For utilities who designate units as must run on a day-ahead basis in some cases, a valuable practice, every unit in the fleet would have to be classified as high impact. The wording should be changed to only include units designated on a seasonal or annual basis. In addition, a

#	Organization	Yes or No	Question 7 Comment
			definition of “must run” should be provided or referenced from elsewhere in NERC documentation. The wording in 1.3 also creates a new requirement that all “must run” units be classified as to whether they have Wide Area impact, which is not currently required. Are there actually any “must run” units (or any units, for that matter) that have Wide Area impact? Because Blackstart Resources are included in Cranking Paths, 1.4 is redundant in light of 1.6 and should be removed. Alternatively, 1.4 should be limited to primary Blackstart Resources to match 1.6. In 1.4, consideration should be given to reducing the impact level for situations where multiple Blackstart Resources are available. Universally search for “effect” and replace with “adverse effect”. In 1.6, replace “support” with “is part of”.In 1.7, delete the phrase "including Flexible AC Transmission Systems (FACTS). This is redundant as it is referenced again in the following sentence.
7.78	Constellation Power Source Generation	Yes	The final sentence in 1.1 needs to be rewritten, as it’s extremely confusing. A suggestion would be to simply add the 2,000 MW bright-line at the end of the first sentence. It would read “Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation Facilities), whose aggregate rated net Real Power capability exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve, total of reserve sharing obligations for the Reserve Sharing Group, or 2000 MW (if no Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group is established).” Is it the intent of the SDT for the MOD10 data to be the data used in this criteria? If so, that data changes seasonally, so a seasonal review would be needed, especially for units who are on the thresholds of the high/medium/low criteria. A suggestion would be to use nameplate data as that is a fixed rating that will not change. 1.4 and 1.6 should be

#	Organization	Yes or No	Question 7 Comment
			combined together, as they are referring to similar items. The combined High Impact Rating should read "Generation, Transmission, and other Facilities required to support a primary Cranking Path used in a Transmission Operator's restoration plan per EOP-005." However, 1.4 and 1.6, either combined or separate, still penalize generation entities that own numerous black start facilities within a single Balancing Authority's footprint. Generation entities in the aforementioned situation have already invested a lot to ensure the reliability of the BES, but under CIP-010 they will be forced to invest even more. A suggestion would be for the TOP to designate a percentage of the black starts as High, and the rest as medium or low depending on their MW size. Another suggestion would be for the TOP to specifically designate certain black start units as high, and the rest are classified based on their MVA size, with the caveat that the TOP should not designate all black start units as high to avoid liability.
7.79	Dairyland Power Cooperative	Yes	The impact ranking for blackstart should be equivalent to the highest impact of all transmission and control center systems. If an entity has only low or medium impact systems other than blackstart, a high impact for blackstart is not appropriate. 1.2 and 2.2 specify 1000 MVAR and 500 MVAR, respectively for categorizing reactive power facilities. Since reactive power problems are localized in general, these numbers seem to be high. It is difficult to set global criteria on reactive power as it is network dependent. I would advise about 50% of the proposed level to be more conservative.
7.80	Duke Energy	Yes	The quantities identified on Attachment II appear arbitrary, and need an engineering basis. We suggest an approach based upon Violation Risk Factor language, such that for the High Impact Rating, the qualifier should be whether or not the BES Cyber System could directly cause or contribute to Bulk Power System instability, separation, or a cascading sequence of failures, or could place the Bulk Power System at an unacceptable risk of instability, separation, or cascading failures. For the Medium Impact Rating, the qualifier should be whether or not the BES Cyber System could directly affect the electrical state or the capability of the Bulk Power System, or the ability to effectively monitor and control the Bulk Power System, but is unlikely to lead to Bulk Power System

#	Organization	Yes or No	Question 7 Comment
			instability, separation, or cascading failures. Need to clarify the expectations for a multi unit generation site. For example: Under what conditions would a site containing two separate 900 MW generators be considered "Medium Impact Rating" because the total site would now be greater than 1000 MW? Similarly, when would a site that had three separate 900 MW generators be considered "High Impact Rating" because the total site would now be greater than 2000 MW? o CIP10-1.4: We have many small sites (hydro's) listed in our Blackstart plan because they are available. They are not essential to our plan, but because they are available, we list them. Under this guidance, we would be required to include them as "High Impact", when in reality they are 'Low'. The wording should be revised to reflect that only those sites "REQUIRED" for Blackstart be secured under 1.4 o CIP10-1.6: We need a defined and clear understanding of what is intended in the use of the term "Cranking Path" as it relates to CIP and EOP-005. What is being sought under this requirement? The term is loosely defined in the glossary, and how it is interpreted by the industry may vary greatly from how it is intended by regulators. o Under our current understanding of the term, we would see minimal increase in sites added to our "High" list. However if we impose a severe interpretation, we could see an exponential increase to our 'High' list. o CIP10-1.7 & 2.5: The word 'Misuse' should be removed or very strictly defined. It is too vague to have meaning. o CIP10-1.11: Need a clear and functional definition of 'Element' for the industry to understand the intent of the requirement. Current glossary definition is poor at best. Also, revise 2.6. as follows: Transmission Facilities operated at 300 kV or higher, which have 2 or more 300kV or above lines, in the Eastern and Western Interconnections or operated at 200 kV or higher in Texas and Quebec Interconnections not included in Section 1.
7.81	Bonneville Power Administration	Yes	The sixth line in 1.1 begins with the words "Generation Facilities." Generation Facilities is not a defined term in the April 20, 2010, Glossary of Terms Used in NERC Reliability

#	Organization	Yes or No	Question 7 Comment
			Standards. Since this phrase is not used at the beginning of a sentence, it should be "generation Facilities." There is the same problem at the beginning of the second line in 1.2. That should also be changed to be "generation Facilities."The first line in 1.7 contains the phrase "Flexible AC Transmission Systems (FACTS)." That phrase is not defined in the April 20, 2010, Glossary of Terms Used in NERC Reliability Standards. Aren't all capitalized terms used in Standards supposed to be defined? Or does FACTS have a generally accepted definition in the industry? CIP-010-1 - Attachment II Impact Categorization of BES Cyber Systems High Impact Rating (H)Each BES Cyber System that can affect operations for:1.1. Generation Facilities, etc."can affect operations" does not relate to impact. We suggest it be reworded: "If the BES systems can change operation by the following amounts they will be in the HIGH CATEGORY: - Generation - 4,000 MW- trip or reduce output of "MUST RUN" generators to below their MUST RUN amount. - Transmission - de-energize at least 4 lines above 300 kV - MVAR support - change MVAR by 1,000 MVAR
7.82	US Army Corps of Engineers, Omaha Distirc	Yes	The word "affect" in the first sentence is somewhat ambiguious and does not fit the intent of all of the subsequent paragraphs(1.4 & 1.6) Paragraph 1.3 define wide area impacts. Paragraph 1.4 should be limited to BES Cyber Systems that are required to energize a Blackstart Resource listed in the TO's system restoration plan per the GO's written restoration plan. As written it appears to apply to any BES Cyber System that merely affects the Blackstart asset and that all BES at such a facility would be High Impact which could have a chilling effect on an entities willingness to provide Blackstart resources. Paragraph 1.6 should be limited to BES Cyber Systems required to operate or support equipment in the primary cranking path. Again this would appear to apply to all BES Cyber Systems at such a facility merely because the facility was part of the cranking

#	Organization	Yes or No	Question 7 Comment
			path regardless of their impact on system restoration. Paragraph 1.10 define impact beyond the local area.
7.83	Midwest ISO	Yes	There is no documentation for the justification of the selection of the various thresholds. Justification of these thresholds should be documented and defended.
7.84	SRW Cogeneration Limited Partnership	Yes	There needs to be a category for "no impact". We are a small Cogen plant that does not even sell firm power to the grid. In essence, we are a steam plant that happens to generate electricity. We have no "Critical Assets" as defined by CIP-002. There needs to be an equivalent level for that in CIP-010. If there needs to be a system study performed by the RC to support a "no impact" rating, that's fine. And if a facility is found to be "no impact", then that facility should be exempt from the majority of further CIP requirements, just like today where CIP-004 thru CIP-009 do not apply to facilities with no Critical Assets/Cyber Assets and only R2 of CIP-003 applies.
7.85	Covanta Energy	Yes	There still needs to be some allowance to fewer mandatory requirements associated with smaller generators.... those in the 20-50 MW range (which are unmonitored) who typically have to notify their TOP/BA that they are on the system or off the system (or reduced load if applicable).
7.86	Pepco Holdings, Inc. - Affiliates	Yes	We agree with EEI's comments.
7.87	We Energies	Yes	We Energies agrees with EEI Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. We Energies agrees with EEI comments Clarification is needed for the term "primary Cranking Path" (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term,

#	Organization	Yes or No	Question 7 Comment
			however, “primary Cranking Path” is not defined. Item 1.3 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Most larger entities submit multiple plans with multiple blackstart units and cranking paths. Protecting all blackstart units may divert finite resources from (better) protecting more valuable facilities. Moreover, it is not appropriate to create a perverse incentive for system owners and operators to reduce the current flexibility and diversity of multiple blackstart units and cranking paths by requiring a level of protection that is not proportional to the level of impact to restoration of the BES. It is not appropriate to expand the definition of blackstart to include full restoration of native load, that would essentially include all or most of the BES. The objective here is to prioritize, and augment security for the elements needed to begin system restoration. Proposed definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for initial system restoration”. Regarding 1.7, we recommend striking “Flexible AC Transmission Systems (FACTS)” because it would be included within Transmission Facilities. Although capitalized, it does not appear in the NERC Glossary of terms. We Energies agrees with EEI. Suggest Adding:1.15 Control Centers including Generation Control Centers .Also, we suggest that the drafting team place the highest impact facilities earlier (e.g. 1.1) on the list. The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact. Under Frequency Load Shed systems under a common control system.
7.88	Ameren	Yes	We generally agree with the criteria used to identify “High” impact facilities, but believe that the item 1.5 criterion should be expanded to include EHV transformers, and not

#	Organization	Yes or No	Question 7 Comment
			limited to 4 EHV lines. However, there are too many EHV facilities in item 2.6 that would be classified as "Medium" impact, but should be classified as "Low" impact. It is suggested that EHV facilities with three or less EHV lines and transformers should be considered as "Low" impact, as they likely have little impact on the BES. The use of TPL performance standards would confirm that many of these facilities have a "Low" impact. For 1.1 the 4th sentence should be reworded to say "total obligations for the entire Reserve Sharing Group." 1.3 needs clarification of what a "reliability must run" unit is. Also, clarify 1.4 if it refers to the actual black start unit, or the entire plant in which the black start unit resides. Last, clarify 1.6 on what magnitude of support is required by the facility. Currently this could apply to any Transmission or Generation Sub-system in the path. Performance criteria, such as the loss of 300 MW of system load to qualify for "High" impact or 100 MW of system load to qualify for "Medium" impact, should also be applied to the EHV facilities identified in items 1.7 and 2.6.
7.89	GTC & GSOC	Yes	We recommend that Attachment II be organized to more clearly indicate which items apply to which type of assets. In the case of Control Centers, it appears the primary applicable item in the High Impact category are 1.12, 1.13 and 1.14, but several other items could be misconstrued to apply as well, which could lead to those control centers being inadvertently given a High designation.
7.90	CenterPoint Energy	Yes	While it appears the SDT put a lot of effort in the development of Attachment II, the criteria to be used is arbitrary, is too prescriptive, does not allow for studies or analysis to determine whether or not the loss, compromise, or mis-use of an identified facility would have an impact on the reliable operation of the BES and, in some cases, appears inconsistent. For example; 1.5 Transmission Facilities with four or more Transmission lines operated at 300kV of higher in the Eastern or Western Interconnections or operated at 200kV or higher in the Texas or Quebec Interconnections would require any and all facilities meeting this criteria to be categorized as High Impact without any basis for this rating. Determining a facility's impact to an electric transmission system involves

#	Organization	Yes or No	Question 7 Comment
			more analysis than counting the number of transmission lines operated at or above a threshold voltage level; 1.14 Transmission Operator functions is based on the number of substations a control center may be able to remotely control. The previous criterion, 1.13 Balancing Authority functions, is based on the mega-watt amount the Control Center operates. Neither offers a basis for either the number of substations or the mega-watt amount under the operation of the Control Center. While CenterPoint Energy would find Attachment II useful as a guide or systems to be considered it is apparent the SDT meant this to be a requirement and therefore CenterPoint Energy does not agree with Attachment II and suggests it be deleted.
7.91	Verizon Business	Yes	1) Attachment II, Item 1.1 regarding Generation Facilities – Suggest removing any reference to "Contingency Reserve" or "Reserve Sharing Group." Specifically, any Generation Facility, singularly or in combination with aggregate higher than 2,000 MW should be included as a High Impact Rating. Reference to the "Contingency Reserve" (etc.) comments can result in incorrect or inconsistent declaration of a generation asset being a High or Medium impact. 2. What is the status of OSI Layer 3 definition raised in the FAQs of March 2006? For the definition above and for CIP-002 earlier versions, OSI Layer 2 was not included; however, the inference above is that it now is included. This and any other questions from FAQ for CIP-002 should be addressed in the standard.

8. **Do you have any other comments to improve this version of draft standard CIP-010-1? If so, please explain and provide specific suggestions for improvement.**

Summary Consideration:

Many entities commented on the need to have the approach provided in the posted CIP-010 and CIP-011: it was pointed out that a substantial amount of work has been done in compliance with a Risk Based Methodology. Many entities commented on the the use of the systems approach, remarking that the flexibility allowed may not be appropriate. Other entities commented that the work done in the current CIP-002 through CIP-009 with Critical Assets should be preserved.

The SDT has reconsidered its approach to the structure of the standards and believes that Version 5 will provide an incremental approach while addressing the FERC directives.

#	Organization	Yes or No	Question 8 Comment
8.1	Constellation Power Source Generation		A guidance document is needed to add clarity, as some terms are still vague.
8.2	Allegheny Energy Supply		A lot of work went into the prepration of the existing CIP-002 standard. This new CIP-010 standard completely throws away that body of work in favor of this new approach. While there are many good things about the new approach, please consider the amount of work that entities have given to refine the CIP-002 drafts and to create and implement the current identification methodoligies and compliance plans. We suggest that you consider incorporating the new ideas as incremental changes to the existing standards. Suggest that the standard require controls that are commensurate with the amount of risk of compromise that a device presents. Not all BES Cyber System components present the same risk, or if compromised, have the same potential impact on the BES. For example: - Serially attached electronic components do not face or create the same risk as those that use routable protocols. - Devices that communicate to each other within a self-contained, isolated network

#	Organization	Yes or No	Question 8 Comment
			segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. - Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.3	Entergy		A) Giving each individual Responsible Entity the 'freedom' to define "a system" any which way each prefers will almost certainly create similar problems as those experienced with CIP-002-1/2/3 that allowed each Entity to chose a 'risk based assessment methodology' of its own preference to identify Critical Assets. In the abstract the notion of self-conceptualization of "a system" may be appealing, but in terms of the confusion factor relative to NERC's goals for consistent interpretation, application, and subsequent audit-ability across the industry this portends trouble. Entergy suggests that "BES Cyber Systems" should be defined as collections/groups of hardware and software employed cooperatively to execute a Reliability Function in Attachment I. It is not necessary to explicitly define what a "SCADA system" is, but most can agree that there are cooperative components that must work together to execute the functions associated with 'SCADA.' Tangibly, this will no doubt be different in each setting in terms of specific gear used to assemble and operate the systems functions, but taken together they are indeed "a" system. It would seem more appropriate to instruct identification of groups of cooperative components that work together to be treated as a system, and extraneous or stand alone or single-purpose equipment could be distinctly characterized as "unitary systems" when appropriate. There is practical value in logically treating several cooperative components as a system, and requirements for implementation documentation will be more straightforward and simpler if they can be treated as such. B) The fundamental flaw in the combined logic of CIP-010-1 (and transitively CIP-011-1) is the notion that risk to reliable operation of the BES posed by use of cyber assets correlates exclusively with the size of the electric operating site at issue. This single-minded orientation ignores other highly salient cyber security threat vectors in play,

#	Organization	Yes or No	Question 8 Comment
			most notably, concerning what type of data communications technology is used to network within and between sites comprising a BES Cyber System. The CIP V1 SDT correctly recognized the especial vulnerabilities posed by use of routable protocols, if the BES Cyber System is not secured with proper cyber security procedural controls and technical countermeasures. At the same time, less vulnerable - in terms of adverse impact on reliable operation of the bulk electric system as a whole - BES Cyber Systems or Components thereof that communicate using legacy serial, dial-up, or other Data Link Layer data transmission paths pose less of a practical risk in terms of overall BES attack surface due to their inherent lack of an Inter-Network Layer. Absent routable protocols, miscreant cyber navigation to and attack of other systems or components not directly attached to the individual serial link (dial-up or hard line) or Data Link Layer (sub-)network is simply not possible. Furthermore, the binary orientation of applicability of a requirement discussed above actually creates unsavory unintended consequences: in a number of ways a single requirement can mandate unnecessary and costly countermeasures for sites of a certain size regardless of the attack surface presented by the communications medium. That is, rigorous requirements appropriate for BES Cyber Systems/Components at sites that employ routable protocols are also imposed on other sites that do not, e.g., operating sites where only legacy serial lines are used. Finally, requirements for BES Cyber Systems/Components at work in purportedly small-impact grid operating sites where routable protocols are employed are in many cases simply deemed to be not applicable (not required). Summarily, the use of "electrical rating" (size) as the sole determinant of applicability of cyber security requirements will result in both excessive expenditures and undue regulatory risk concerning sites that pose minimal risk of cyber attack. This approach simultaneously fails to apply the Requirements to sites that, while not significant from an electric reliability standpoint, could afford a cyber entry point which could be used to access the larger network via routable protocols. Please see comments under Question 54 for a continuation of the above train of thought for explicit recommendations for improvements concerning both the structural organization and logical substance of CIP-010-1 and CIP-011-1 when taken together.

#	Organization	Yes or No	Question 8 Comment
8.4	Allegheny Power		Allegheny Power does not believe it is necessary to abandon the Critical Asset approach described in CIP-002. The new impact categorization structure proposed by CIP-010 introduces a completely new approach. All of the investment in procedures, training, documentation and other efforts to date to ensure compliance with the CIP standards will need to be redone. AP believes that the objectives of the Standard Drafting Team to provide further clarification and remove the uncertainty of the current CIP-002 are proper and necessary. However, AP believes that these same objectives can be accomplished by incrementally revising the current CIP-002 standard and not abandoning the approach entirely, which would essentially force all entities to start their CIP compliance efforts over from the beginning. Changing the terms, concepts and numbering schemes alone will disrupt continuity of CIP programs and have a major impact on each entity. Not all BES Cyber System components (as defined by CIP-010) face the same risk, or if compromised, have the same potential impact on the BES. o Serially attached electronic components do not face or create the same risk as those that use routable protocols. o Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. o Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.5	Green Country Energy		An overall guidance document would be very helpful to the large number of entities that will have to comply with this standard that previously were not critical. Nothing specific, some reference links, examples of expectations, a resource guide.
8.6	CWLP Electric Transmission, Distribution		Any terms used, such as Operational Time Horizon, should be included in the NERC Glossary of Terms.

#	Organization	Yes or No	Question 8 Comment
	and Operations Department		
8.7	Dominion Resources Services, Inc.		Attachment II contains some errors and should be revised in accordance with the following; CIP-010-1 1.3. The term Wide Area is applicable only to a RC area. GOs do not have access to information necessary to make such a designation. This requirement should state that a RC must inform a GO within a certain specified time frame if the RC determines that the GO owns a "must run" unit. Also. there must be some "implementation period" for the GO to become compliant. Compliance may require extensive engineering, procurement and the expenditure of significant resources that must be considered when determining the appropriate implementation period. CIP-010-1 2.3. It is not clear which entities (e.g., BA, RC, TOP, other) have the responsibility to make such designation. GOs do not have access to information necessary to make such designation. The entities that have access to the information include the RC, TOP and possibly the BA. The RC should make the designation, but with the input of the BA and TOP. If the RC makes such a designation, it is proposed that this requirement be revised to contain a statement that the RC must inform the GO within a certain specified time frame. Also, there must be some "implementation period" for GO to become compliant. Compliance may require extensive engineering, procurement and the expenditure of significant resources that must be considered when determining the appropriate implementation period. NOTE - Currently, in PJM, units so designated do not impact the entire RTO (equivalent of Wide Area) but are designated due to local import constraint limits (CETL). It appears likely that such generator would be designated as Medium impact. However, in smaller RC areas (e.g., NY), this could result in generators that appear to be equal in size (to a generator designated as medium in PJM) being designated as High because the impact to that RC area is based on size of the area as well as the generators within that area.

#	Organization	Yes or No	Question 8 Comment
8.8	Constellation Energy Commodities Group Inc.		Based on the current CMEP the audit cycle will always be longer than a full calendar year, would it be clearer to state that the data retention period is for 3 years.
8.9	Constellation Energy Control and Dispatch, LLC		Based on the current CMEP the audit cycle will always be longer than a full calendar year, would it be clearer to state that the data retention period is for 3 years.
8.10	ReliabilityFirst Staff		Because the acronym "BES" is not included in the NERC Glossary of Terms, we suggest that BES should be spelled out in the Introduction to this standard.
8.11	Reliability & Compliance Group		Being more specific with better definitions is a tremendous help with interpreting the requirements. Right now, there is still too much open to interpretation and as such, this will be very hard to make auditably compliant anywhere but to our own procedures.
8.12	City Utilities of Springfield, Missouri		City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
8.13	IRC Standards Review Committee		Comments: NERC should lead a discussion of whether the proposed CIP standards provide an appropriate level of protection from attacks. By level, we mean the granularity of the requirements - or how far down to individual components and personnel procedures. Attempting to put requirements to protect from nearly every possible attack scenario possible on every possible asset and or component that touches the BES is an extraordinary effort that will certainly provide a perception that NERC and the registered entities are doing what they can to protect from threats. There is no argument that if every registered entity protects every asset/component from threats to the nth level of granularity, the industry would be able to state that it has made every possible effort to thwart attempts to sabotage the interconnected grid. But NERC should begin a discussion on whether it is necessary to have such extensive requirements to be able to prevent a system-wide incident. The proposed CIP standards do not seem to align with NERC's approach in setting reliability requirements for more "traditional" system threats such as facility loading and system frequency. With these "traditional" standards, there is a distinction between requirements and procedures that are local in

#	Organization	Yes or No	Question 8 Comment
			nature and those that are needed on a wider interconnection level. For these "traditional" reliability threats, it is accepted by industry and regulators that this is an appropriate approach. For example, NERC does not establish requirements for relay maintenance crews to properly disengage trip coils when testing relays. But NERC does establish standards for registered entities to maintain those relays that impact BES reliability. The details of how the registered entity ensures that maintenance programs are carried out requires a local or individual procedure/requirement. NERC's focus should remain on setting standards to protect from wide area impacts - not on establishing standards that manage individual system components. NERC and the industry need to take a hard look at what exactly the CIP standards should protect from and write standards that can leverage compliance resources to reducing the wider interconnection level threats and leave setting measures or requirements that are local in nature up to the registered entities.
8.14	Southwest Power Pool Regional Entity		Consider combining the Medium and Low categories into a single category. A three tier categorization is not necessary.
8.15	Public Service Enterprise Group companies		Considerable effort was spent by industry stakeholders in classifying assets as Critical Assets (CAs) and as Critical Cyber Assets (CCAs) for CIP v1-v3. An official guide to map identified assets using the CIP v1-v3 CA and CCA terms and the new BES Cyber System Component and BES Cyber System terms is needed. Such will be an aid in ensuring a smooth transition.
8.16	Oncor Electric Delivery LLC		Control Centers and substation need to be considered separately. What is prudent cyber protection at a control center may be totally unnecessary at a substation.
8.17	E.ON U.S.		cyber systems used exclusively for local distribution of electric energy is contrary to FPA Section 215 (1) & (3). Other comments on specific areas of the proposed standards: CIP-010-1 B Requirements Section 3.2,3.3 What constitutes a "change" under these requirements.

#	Organization	Yes or No	Question 8 Comment
			CIP-010-1 C. Measures, M3 E.ON U.S. requests that the SDT clearly define in which requirements this measure applies. CIP-010-1, Violation Severity Levels There is very little difference in risk between failing to update documentation for 60 versus 80 calendar days, yet there are various gradations based on the 10-15 day window from the low-to-severe. CIP-010-1, section 3 "Low Impact Ratings" Maintaining an inventory of all low-impact rated BES cyber systems/ components will result in a significant administrative burden. Given the few prescribed protective measures that apply under CIP-011 to low impact facilities the inclusion of low impact facilities appears to provide little in the way of additional BES reliability.
8.18	San Diego Gas and Electric Co.		Draft Standard CIP-010-1 is a significant paradigm shift from the currently effective Standard CIP-002-2. SDG&E has spent significant resources to be compliant with the current version of the CIP Standards including becoming knowledgeable with the current terminology and applying it within the current CIP Standards. Draft Standard CIP-010-1 departs from the current CIP Standards but at the end of the process, it is unclear whether this change in approach will in fact result in a material enhancement to the reliability of the BES. SDG&E suggests that before continuing to move forward, the SDT needs to specifically understand and communicate to the industry what it is trying to accomplish. What is the target that we are all trying to hit with these proposed changes to the CIP Standards? In so doing, the industry can provide specific alternatives that accomplish the goal at hand. When evaluating the alternatives to meet the goal, it is critical that there is a quantifiable incremental reliability benefit to the BES before proceeding. SDG&E and many other entities have spent significant resources to comply with the current CIP Standards. At this point in time, the industry needs to know that additional resources to

#	Organization	Yes or No	Question 8 Comment
			comply with the proposed CIP Standards will result in an incremental benefit to the reliability of the BES. SDG&E strongly recommends that before moving any further, these questions be answered and that the SDT actually "test" the proposed draft CIP-010-1 Standard on a handful of companies or scenarios to gain some practical experience from the proposed changes. Are the in-scope assets easy to identify and categorize? How does the quantity of in-scope assets compare to that of the current Standards? Perhaps the SDT will find that there is a significant enhanced reliability impact to the BES. On the other hand, the SDT may find that the results do not accomplish the goal that it is trying to achieve and thus another approach would make more sense. SDG&E advocates leveraging the existing CIP Standards as much as possible moving forward, because we (like many others) have a lot of time and resources invested in our current compliance efforts and we'd really like to build from those efforts instead of essentially starting over with a new process.
8.19	BCTC		Emergency Situations - The provision for "emergency situations" should remain at the policy level. BCTC is of the opinion that it is feasible for emergency situations to be unforeseen and, as such, does not agree with the assigning of such contingencies to specific requirements.<See CIP-011-1-R3 below for an example> TFEs - TFEs will continue to be required due to the limitations of technology - i.e. older systems being unable to enforce strong passwords, etc. These limitations are beyond the Utilities control and, as such, it would be considered unfair to be found in non-compliance for such instances. What should be required in such situations is that the Utility implement controls to minimize the vulnerability that results from the TFE.
8.20	Exelon Corporation		Exelon companies have embraced the development of logical, clear and effective reliability standards as evidenced by its commitment of time and resources to various standard development initiatives (including participation on several NERC and Regional Committees, Sub-Committees and Standard Drafting Teams). As evidence of our

#	Organization	Yes or No	Question 8 Comment
			commitment, Exelon has devoted in excess of 4 years and $11 million for the implementation and integration of the NERC CIP-002 to CIP-009 Standards. We have concerns with several aspects of the CIP Version 4 Standards. The CIP Version 4 Standards represent a significant change in the scope of the standards in the equipment/systems that fall under the standards as well as the elimination of terms/categories of assets. Exelon is also not in favor of changing the current CIP-002-009 standards to the new CIP-010 and CIP-011 format. Each change in itself represents a significant "change management" issue that impact databases used for the tracking/storing of evidence of compliance, training requirements, safeguards, and systems that have been put into place to ensure Exelon's continued compliance to all NERC Standards. Exelon feels strongly that the proposed changes must be accompanied by a risk based analysis as justification for such dramatic and costly changes which to date have not been shared with the industry. Essentially we are most interested in understanding the incremental difference or benefit of moving away from the current Regulatory approved CIP-002 to CIP-009 standards to a different set of standards that will result in many of us "starting from square one" to implement. If this shift to CIP-010 and CIP-011 is approved, policies, procedures, contracts, training, drawings, methodologies, systems, data structures, and countless other documents will need to change to reflect the new language and concepts. The confusion that this will cause within organizations to retrain personnel and realign around the new standards cannot be underestimated. In fact, Exelon may even need to put some value-added compliance projects on-hold because the entire design will need to change with the implementation of the new standards. Specifically, Exelon would like to see the SDT: Discard the concept of a wholesale rewrite of the CIP standards -- but use the standards drafting team work as an input to the process. Incrementally change the existing CIP-002 through CIP-009 standards to clarify and improve upon the established approach. Retain the fundamental terms, concepts, and standards numbering scheme to enable

#	Organization	Yes or No	Question 8 Comment
			continuity. This approach would more effectively build upon the work that has already been accomplished, while allowing the industry to continue to improve on security and compliance related to critical infrastructure.
8.21	Duke Energy		Explicitly state that terms found in the NERC glossary apply here unless otherwise stated.
8.22	USACE - Omaha Anchor		General comment - committee referred to relays as being addressed in this standard. We are unsure what that interpretation is based in attachment 1.
8.23	Powersouth Energy Cooperative		General Comments: The approach to classify cyber systems according to their impact seems to be a better approach for the industry. Taken in conjunction with CIP-011 that establishes security requirements, it is logical to establish security levels based upon the impact of compromising these assets. The drafting team is commended for this approach. Consideration should be given however to recognizing that while technically some assets are BES assets, they do not materially affect the BES. For example, a small DP may own UFLS relaying however the magnitude of the load that is shed by their entire UFLS program would insignificantly affect the overall objective of the regional UFLS programs to protect the BES. While identifying those assets is reasonable, to require any security measures in CIP-011 is not warranted. Perhaps a "No Material Impact" category should be considered based on load. R1. There is a perception that every cyber system associated with the BES owned by an entity must be identified to determine if the cyber system executes or enables one of the functions in the attachments. It would seem appropriate to review all facilities (i.e. locations) to determine and document the functions that are performed at that location. However, if it is determine that no BES functions are performed documenting each system seems to provide little benefit. Example: A small distribution station is served from a transmission line greater than 100 kV. The station does have multiple cyber systems none of which perform identified BES function. The perception is each system must be documented. Since on a higher level,

#	Organization	Yes or No	Question 8 Comment
			a functional assessment indicated no BES functions are performed, is it necessary to document each cyber asset?
8.24	American Municipal Power		I agree with the intent, but I disagree with the structure of CIP-010. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
8.25	Matrikon Inc.		I offer to provide a workflow decision diagram I have prepared (Visio or JPG) to show how CIP-010 could be interpreted, but also to see how each of the statements in the requirement are supposed to fit into evaluation of BES Cyber Systems. I am a visual person, and my goal was to visualize the interpretation of CIP-010 for myself and colleagues to have a clearer understanding of its application. Diagram has been sent directly to Lauren.Koller@nerc.net as part of my comments. Use at your discretion, feel free to leverage/expand on my diagram, and share with SDT. My intent is to simply help reduce misinterpretation of the standards and debate on how they should be applied.
8.26	Cogeneration Association of California and Energy Producers & Users Coalition		Is it the intent of the Drafting Team that a cyber system will not be classified as a BES Cyber System if it does not cause a disturbance to the BES within 15 minutes or does not have an effect on real-time operation of the BES within 15 minutes of it becoming unavailable, degraded, compromised, or misused? If yes, guidance will be needed on

#	Organization	Yes or No	Question 8 Comment
			what proof of lack of disturbance is necessary to support an entity not classifying a cyber system as a BES Cyber System.
8.27	EEI		It would be helpful for the drafting team to develop in a separate guidance document more information about the threat basis that the standard is intended to provide protection against. The opportunity is to inform asset owners/operators of how and where to prioritize efforts to protect components of the BES. Over the last several years, a number of parties have expressed concern about the risk associated with multiple, simultaneous remote attacks against BES Cyber Systems, potentially impacting multiple generation, transmission and control center facilities. If in fact, the primary concern is the issue of multiple, simultaneous remote attacks, it is not appropriate to mandate excessive controls over physical elements such as the copper or fiber optics cable plant within a generating facility or a building housing a control center. Security requirements and controls should be developed that are proportional to the potential or probability of compromise as well as impact of compromise.EEI suggests that the drafting team recognize that not all BES Cyber System components face the same risk based on their connectivity. o Serially attached electronic components do not face or create the same risk as those that use routable protocols. o Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. o Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.28	ISO New England Inc		Modify the purpose statement to be more clear and understandable. Proposed Purpose: To identify and categorize BES Cyber Systems that execute or enable

#	Organization	Yes or No	Question 8 Comment
			functions essential to reliable operation of the BES. Apply appropriate cyber security requirements commensurate with the adverse impact that loss, compromise or misuse of those BES Cyber Systems could have on the reliability of the BES.
8.29	Hydro One		Most North American utilities spent significant capital and manpower resources in order to achieve compliance with current version of CIP standards. Version 4 brings a multitude of changes that appear to significantly broaden compliance requirements. Hydro One understands and supports the intent to improve the overall reliability of the BES through reduction of the vulnerability to cyber attacks. Based on the previous experience, in the development of the version 4 implementation plan, the SDT should consider the long time periods necessary to implements the changes required for this version.
8.30	Michigan Public Power Agency		MPPA is concerned with how these standards would impact its members who are registered entities but do not own or operate facilities that are, by NERC definition, a part of the BES. MPPA recommends clarification in the applicability section with the insertion of ", that operates BES facilities, " between "...Functional Entities..." and "...will be collectively...". This segment of the sentence would then read as: "...Functional Entities, that operates BES facilities, will be collectively..."
8.31	MidAmerican Energy Company		Need to ensure the VSLs are not written with zero-defect quality prescriptions. The proposed VSL levels in CIP-010 are too prescriptive. Replace zero-based quality prescriptions in the requirements, measures and violation severity levels with based performance targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: o program implemented o program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120) o correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity

#	Organization	Yes or No	Question 8 Comment
			levels should correspond, for example: VSL For Severe program not implemented High controls not implemented Moderate reviews not completed Lower corrections from reviews not completed These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
8.32	Progress Energy - Nuclear Generation		NERC should facilitate the Federal Energy Regulatory Commission (FERC) consideration to suspend implementation of Critical Infrastructure Protection (CIP) Reliability Standards CIP 002 through 009 for nuclear plants in favor of implementing CIP-010-1 and CIP-011-1. Originally, CIP-002 through 009, Version 4, were to be developed to address nuclear cyber requirements as a result of FERC Order 706-B. However, CIP-010-1 and CIP 011-1 are now being developed to address the nuclear cyber requirements. In the mean time, nuclear will be required to implement CIP-002 through 009, Version 3, which do not align with CIP-010-1 and CIP-011-1 to satisfy the FERC requirements. CIP-010-1 and CIP-011-1 could be implemented at the nuclear plants in the same time frame licensees committed to the Nuclear Regulatory Commission for the 10 CFR 73.54 required Cyber Security Plans. Using the current North American Electric Reliability Corporation (NERC) timeline approved by FERC, R+18 of CIP 002 through 009, Version 3, (~ August 2011), the timing of implementation of CIP-010-1 and CIP-011-1 will be well after CIP 002 through 009 and potentially 73.54. This will require multiple reiterations of nuclear licensee cyber security plans and implementing programs and procedures. These changing requirements create potential error opportunities.
8.33	NextEra Energy Corporate		NextEra suggests a re-write of the following provisions as set forth below to provide

#	Organization	Yes or No	Question 8 Comment
	Compliance		clarity: 4.2. Physical Facilities 4.2.1. All BES Facilities under NERC jurisdiction, including those nuclear generating plant facilities that as part of FERC Order 706-B (and other applicable FERC orders) processes are determined to be subject to this CIP Standard. B. Requirements R1. For each BSE Control Center, Generation Facility or Transmission Facility implicated by the Responsible Entity's application of High, Medium and Low Impact Risk in Attachment II to its BES, the Responsible Entity shall identify and document all BES Cyber System Components that it owns and indicate its association with a BES Cyber System. (Violation Risk Factor: High) R2. The Responsible Entity shall ensure that each BES Cyber System Component identified in R1 is in compliance with the applicable protections as required in CIP-011-1. (Violation Risk Factor: High) CIP-010-1 - Attachment I (For informational purposes only) Functions Essential to Reliable Operation of the Bulk Electric System The following provides an understanding of the operating functions which are essential to real-time reliable operation of the BES and are provided for informational purposes only.
8.34	Independent Electricity System Operator		No, but please see our comments under Q9.
8.35	USACE HQ		Please answer to questions 3 and 4.
8.36	FirstEnergy Corporation		Please see Question 1 for FE's Summary view on the CIP-010 and CIP-011 standard.

#	Organization	Yes or No	Question 8 Comment
8.37	BGE		Provide a definition for "Automatic Load Shedding".
8.38	Puget Sound Energy		Puget Sound Energy notes that the Violation Severity Levels put specific metrics (5%, 10%, etc...) to previously commented on vague terminology. In order for NERC to determine "5% or fewer BES Cyber Systems have not been identified", there has to be a total number of BES Cyber Systems at an entity. But, with vague, open to interpretation, terms like "restrict" or "affect", the total list of BES Cyber Systems is subjective to different opinions on what it means to restrict or affect the BES.
8.39	Liberty Electric Power, LLC		RE: VSLs. Smaller facilities with limited cyber assets will pay a much larger penalty for a single miscategorized asset than a large utility. Example: TOP miscategorizes 49 of its 1000 cyber assets, and gets hit with a single lower VSL. Small generator miscategorizes 1 of 8 cyber assets, gets hit with a severe violation. Some method of recognizing the disproportionate affect on smaller entities must be included in the standard.
8.40	LCEC		Recommend that the development and release of implementation guidelines takes place sooner rather than later to assist entities in complying with the new standards.
8.41	Minnesota Power		Regarding the Violation Severity Levels, how does the Standards Drafting Team envision these being applied? If systems are not identified, how will an auditor know how many are missing? For example, VSL R2 mentions "incorrectly categorized" BES Cyber Systems. How will an auditor determine that a Registered Entity has incorrectly categorized systems when they have documented their review and categorization process? Also, for VSL R3, it seems arbitrary that a difference of 20 days takes a violation from a "Lower" to a "Severe" VSL. How were those numbers determined?
8.42	Wolverine Power		See comments listed for 1.a
8.43	Nuclear Energy Institute		Several:

#	Organization	Yes or No	Question 8 Comment
			a) In the Introduction, Section 3 (A.3), the word "could" should be replaced with "would." b) In the Introduction, Section 5: Clarification should be made that upon approval by FERC, CIP 010-1 supersedes, in their entirety, all prior versions of the CIP standards, and that compliance with the requirements of CIP-010-1 must be in accordance with the implementation schedule for CIP-010-1.
8.44	APPA Task Force		The APPA Task Force commends the drafting team on their work on CIP-010-1. We thank the team for its hard work and appreciate the team's consideration of our comments from the previous informal comment period. We think the standard is moving in the right direction and with this next round of comments should hopefully result in a set of standards that will meaningfully improve the reliability of the BES and address the cyber security issue for the industry.
8.45	US Bureau of Reclamation		The changes in the Standards to focus on Cyber Systems is reasonable, but the definitions for Cyber System Components, Cyber Systems, and Control Centers may need further refinement (or application examples) to help implementation staff address fundamental questions. As an example: Is an isolated electronic relay providing generator protection for a single large generation resource a BES Cyber System? Under the present definitions it would appear to be (it certainly qualifies as a BES Cyber System Component). If it is a BES Cyber System, it is subject the requirements of CIP-011 based on the impact of the "System." Is this really the intent of the drafting team(s)? Would it not be better to establish select security criteria for isolated components (specifically components such as cyber-based relays and synchronizing equipment) that fit the nature of their deployment - rather than trying to fit them into a "system" category?
8.46	Southern California Edison Company		The CIP-010 and CIP-011 drafts should indicate how these standards will replace or supplement the current CIP-002 through CIP-009. If the intent is to retire CIP-002 through CIP-009 then it would make more sense to call these standards CIP-002-5 and CIP-003-5 with CIP-004 through CIP-009 being retired. A gap of unused numbers

#	Organization	Yes or No	Question 8 Comment
			between CIP-001 and CIP-010 will potentially cause future confusion.SCE also requests the Standards Drafting Team clearly define what should be included as Protective Systems. Additionally, a matrix mapping CIP Version 3 requirements to CIP Version 4 requirements would be very helpful.
8.47	LADWP		The CIPs should evolve in a manner that does not minimize the investment of resources already expended to meet compliance but should leverage the work done already. The draft version 4 is a drastic change and would require multiple years for a Responsible Entity to approach compliance. If CIP version 4 is implemented as currently drafted, there would be a huge resource drain to rewrite language and requirement references that are now part of numerous policy and procedures as well as contract packages.
8.48	Xcel Energy		The definition of BES Cyber System uses criteria that the element must be capable of causing a system disturbance or other impact within 15 minutes. We would like to know if or classification based on the 15 minutes must rely on analysis or if judgment/expert opinion is allowed. 1.5 Please clarify that the "Texas Interconnection" refers to ERCOT. 1.5 If a cyber system can only impact 1 transmission line within a substation containing 4 or more lines, it should not be classified as high. Suggest 1.5 wording be changed to Each BES Cyber system that can affect operations for: "Four or more Transmission lines operated at 300 kV or higher in the Eastern and Western Interconnections or operated at 200 kV or higher located at Transmission Facilities within the Texas and Quebec Interconnections 1.9 It is not clear why facilities serving a nuclear site under NUC-001 are high impact if the nuclear site itself is not High impact.
8.49	Dairyland Power Cooperative		The distinctions between systems and facilities are unclear. The Requirements in CIP-010 shift to a systems oriented identification. Yet the Attachment I/II definitions still rely

#	Organization	Yes or No	Question 8 Comment
			on the concept of facilities and almost seem to equate facilities with systems. These distinctions need to be clear.
8.50	Con Edison of New York		The Drafting Team needs to take into account the fact that the ability to work on any cyber systems in a substation will typically already require a detailed work permit process which includes getting a work permit from an operating authority with jurisdiction on the equipment. The employee working on the cyber system must typically be an approved employee to work on these systems.
8.51	FEUS		The drafting team should consider an alternative for the VSL categorization. By basing it on a percentage, it could potentially unfairly affect smaller entities with fewer BES Cyber Systems. A smaller entity will inherently have fewer BES Cyber Systems, so missing a single classification of a BES Cyber System could automatically merit a severe violation. For example, an entity with as few as 5 BES Cyber Systems that misses the identification of a single system would be in a severe category. A larger entity with inherently more BES Cyber Systems can fail to identify more BES Cyber Systems and have a lesser severity level. An entity with 50 BES Cyber Systems can fail to identify 8 before reaching a severe violation level. The risk of failing to identify 8 BES Cyber Systems puts the BES at a much higher risk than failing to identify 1 BES Cyber System.
8.52	Indeck Energy Services, Inc		The FERC directed guidelines to Registered Entities on the risk based assessment methodology are missing.
8.53	PacifiCorp		The low, moderate and high violation severity levels for R3 do not seem to measure the correct violation criteria. The number of days after a change is completed should not be the sole criteria. The number of days after a change is completed should not be the sole criteria for determining whether a violation was harmless or severe. This is especially true for a standard that currently has no meaningful qualifier to allow for routine or de - minimus changes to elements of the BES without triggering a full review. These criteria should track other violation criteria that consider whether the violator had an adequate

#	Organization	Yes or No	Question 8 Comment
			process in place for the types of changes that merit a re-evaluation. Need to ensure the VSLs are not written with zero-defect quality prescriptions. The proposed VSL levels in CIP-010 are too perscriptiveprescriptive. Replace zero-based quality prescriptions in the requirements, measures and violation severity levels with based performance targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: o program implemented o program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120) o correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity levels should correspond, for example: VSL For Severe program not implemented High controls not implemented Moderate reviews not completed Lower corrections from reviews not completed These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
8.54	National Rural Electric Cooperative Association (NRECA)		The Purpose section of CIP-010-1 and CIP-011-1 should be similar in regards to the facilities it refers to. Add the word in all CAPS to the CIP-010-1 Purpose to bring it in line with the Purpose in CIP-011-1:".... that execute or enable functions essential to reliable operation of the INTERCONNECTED BES..."
8.55	SCE&G		The SDT needs to consider how auditors may interpret the words of the standard

#	Organization	Yes or No	Question 8 Comment
			differently. The language needs to be written clearly and concisely enough so that a consistent interpretation of the standard will be applied by all auditors across all regions. Consideration of Nuclear Facilities: Definitions for BES Cyber System and BES Cyber System Component conflict with definitions that have been accepted by the Nuclear Regulatory Commission (NRC) in NEI 08-09 Revision 6 for Critical System and Critical Digital Asset; recommend for nuclear systems subject Federal Energy Regulatory Commission (FERC) 706-b definitions for FERC and NRC regulated systems are consistent. This will avoid regulatory uncertainty as well as human error at nuclear facilities. CIP-010-1 R2 and Attachment 1 - some of these functions are covered by NRC regulation. Will issuance of this document require re-submittal of systems for exemption after the Bright Line submittal of systems? The implementation schedule for CIP 10 - 11 versus CIPs 02-09 requires doing the same reviews twice and is an unnecessary burden on nuclear licensees as well as other FERC critical assets. The deterministic nature of the security controls in CIP 11 do not provide for acceptance of Common Controls as defined by NIST 800-53. In nuclear facilities with mature physical security programs, engineering control programs, and physical segregation of trusted industrial control system networks from un-trusted networks, CIP 11 should include provision for NIST 800-53 Common Control processes.
8.56	Consultant		There appears to be inconsistency in use of terminology throughout the standard as the terms apply to defined glossary terms, new definitions contained in this standard, and what appear to be 'common terminology' that is not defined. The terminology should be reviewed and applied consistently to avoid ambiguity and confusion. It is not clear that the implied process in the requirements (R1. Identify BES Cyber Systems, R2. Categorize Cyber Systems) is the best methodology. This seems to be missing the first step of the process: 1. Identify the BES assets (Facilities, Elements, &

#	Organization	Yes or No	Question 8 Comment
			Control Centers). The previous versions of CIP-002 started with the identification of BES assets followed by inclusion or exclusion as Critical Assets using the Risk-Based Methodology. As the current standard is written it seems to have lost the step to identify BES assets to which the CIP-010 R1 & R2 steps would be applied. Suggest adding the 'first step' to identify BES assets. This would probably require some restructuring of the current R1 & R2 statements to apply them to the identified BES assets.
8.57	Ameren		There are no system performance requirements as part of the determination of "High", "Medium", or "Low" impact to the BES other than item 1.7. The addition of performance requirements from the TPL standards (TPL-003 and 004) could further help to identify which facilities have the biggest impact on the BES and reduce the number of "High" and "Medium" impact facilities identified to provide significant cost savings to the industry.
8.58	WECC		Utilizing the prescriptive nature of CIP-010-1 Attachment II would be very useful as a rewrite of CIP-002-4. The CIP-002 through CIP-009 format lends itself very well to being audited. What is needed is clarification and explicit language. The current standard needs to be made better not replaced.
8.59	Kansas City Power & Light		Very concerned regarding the "lines" that have been drawn in Attachment II. What is the engineering basis for any of the "bright line" thresholds that have been expressed in Attachment II? Recommend thoughtful consideration regarding operating assumptions be developed an analysis be performed to establish the facilities that should be considered HIGH, MEDIUM and LOW reliability impact. Operating criteria should be established to determine what has HIGH, MEDIUM and LOW reliability impact. In addition, there are facilities that have NO IMPACT to reliability of the BES. Whatever criteria is established, a "smell test" should be done to see if the criteria works. There are numerous small Regional Entities that are obviously no impact to the reliability of the BES, and if any of these requirements and definitions draw any of the facilities of these small entities into the CIP Standards, something is wrong and adjustment to the criteria

#	Organization	Yes or No	Question 8 Comment
			needs to be considered.
8.60	ERCOT ISO		Violation Severity Levels: Recommend that VSLs address "identify" and "document" BES Cyber Systems. "Identify" and "document" are noted separately in the requirements. Attachment I: What is the originating source for this? Can it be referenced? What does "BES elements" mean?
8.61	Pepco Holdings, Inc. - Affiliates		We agree with EEI's comments regarding not all BES Cyber System components face the same risk, or if compromised, have the same potential impact on the BES (e.g. serially attached electronic components versus those that use routable protocols; devices that communicate to each other within a self-contained, isolated network segment versus devices that communicate via routable protocols across multiple geographic or logical boundaries, and devices that use dedicated (and non-routable) point-to-point communications channels versus devices that communicate via routable protocols across multiple geographic or logical boundaries). Would suggest that consideration be given up front in CIP-010 to the types of communication/risk when developing security requirements.
8.62	We Energies		We Energies agrees with EEI. It would be helpful for the drafting team to develop additional documentation providing more information about the threat basis that the standard is intended to provide protection against. The opportunity is to inform asset owners/operators of how and where to prioritize efforts to protect components of the BES. Over the last several years, a number of parties have expressed concern about the risk associated with multiple, simultaneous remote attacks against BES Cyber Systems, potentially impacting multiple generation, transmission and control center facilities. If in fact, the primary concern is the issue of multiple, simultaneous remote attacks, it is not appropriate to mandate excessive controls over physical elements such as the copper or fiber optics cable plant within a generating facility or a building housing a control center. Security requirements and controls should be developed that are proportional to the potential or probability of compromise as well as impact of

#	Organization	Yes or No	Question 8 Comment
			compromise. Not all BES Cyber System components face the same risk, or if compromised, have the same potential impact on the BES. o Serially attached electronic components do not face or create the same risk as those that use routable protocols. o Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. o Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.63	Progress Energy (non-Nuclear)		We need definition of when the CIP requirements "turn on" during new plant construction, commissioning, and/or start-up. Recent major projects with CIP CCA's have been add-ons to existing facilities. We have used the model that until we "logically" connect to the existing facility ESP the full CIP requirements were not required. The next projects will be new facilities with no ESP logical connection to the existing steam plants. We should recommend wording that states that the CIP ESP and PSP requirements do not turn on until the plant is turned over to Energy Supply for commercial operation and it becomes available to ECC. Argument being that during testing ECC manages other generation assets to allow for testing impact on BES. Standard malware protection rules (A/V, etc.) would still apply. Have the regional entities auditing & compliance groups made an initial assessment as to the relative impact when compared to existing standards? For example do they anticipate significant increase in compliance records and audit evidence required? Unofficial Comment Form - CIP-010-1 and CIP-011-1 Cyber Security Order 706 (Project 2008-06)

#	Organization	Yes or No	Question 8 Comment
			Is there expected to be a TFE process for these standards - based on current experience the TFE process is more onerous and adds considerable paperwork without effectively enhancing security of BES. Need consideration for redundancy, backups, alternate systems in relation to required levels of protection - CIP-010-1 R1 makes no provision for considering redundancy, backup systems, or alternate systems which may be in place to 'provide assurance in the resiliency of these functions.' But according to the NERC document Guidance for the Electric Sector: Categorizing Cyber Systems, providing for the 'assurance in the resiliency of these functions' is part of 'The Purpose of Categorizing BES Cyber Systems'. Failure to consider these additional systems as layered safeguards and thereby reducing the criticality of any one of them may mandate that each such BES Cyber System be considered equally essential and critical. The result would be to provide disincentives for the responsible Entities to implement these additional layers - reducing the assurance in the resiliency of these functions. This would be contrary to the stated purpose of 'reducing risk to the performance of functions.' Need better provision for standards tailored to various asset types - Although the new standards will bring even more 'single use' equipment into focus, the standards are designed to protect 'multi function' PC based equipment from the attack vectors that they present. The standards need to take into consideration equipment that doesn't require protection (or extra work such as a TFE) for vulnerabilities that do not exist. Example: A terminal server which is a 'single use' type platform that only does protocol conversion between serial and Ethernet communications presents very few attack vectors. The same functions could be performed by a fully functional PC but that device would present a much larger opportunity for a hacker. The current version of the standards will actually make it more advantageous for entities to implement this function using the larger target of a fully functional PC rather the 'single use' type device simply because of ease of compliance. Recommend implementation timeline:

#	Organization	Yes or No	Question 8 Comment
			High - 4 years Medium - 4 years Low - 4 years
8.64	US Army Corps of Engineers		Will there be official guidance documents, such as the DRAFT Guidance for the Electric Sector: Categorizing Cyber Systems?
8.65	Verizon Business		1. It is not clear whether electricity trading was considered in the draft standard. 2. Attachment III Section 1.11 discusses "BES Elements that perform automatic aggregate load shedding of 300 MW or more." This statement should be revised to specifically exclude Smart Grid Distribution. 3. This standard should be compared to the elements included in the NERC Frequently Asked Questions for CIP-002 to ensure that any new and different perspectives from the FAQs woven into the CIP-002-4 version are addressed completely. 4. The inclusion or exclusion of "non-routable protocols" under CIP-002-4 needs to be addressed. For instance, if the standard included all protocols, then a substantial number of communications systems (e.g., Serial, SONET, etc.) would now be included in the list of "BES Cyber Systems." This would be a substantial change to the Registered Entities, and compliance would be difficult. Overall, non-routable protocols should be included in the CIPs as well as routable protocols. 5. An explanation is required for the inclusion of Distribution Provider in Section 4, Applicability. The inclusion herein has caused confusion for Smart Grid implementation. The Distribution Provider should not be included. 6. In the BES Cyber System Component definition, the word "Disturbance" is capitalized. This word should be defined in the Glossary and could be included as a

#	Organization	Yes or No	Question 8 Comment
			Local Definition in CIP-010. To assist implementing utilities, it would be useful to do some mapping and case studies of the transformation of “Critical Assets” and “Critical Cyber Assets” to “BES Cyber Systems” and “BES Cyber System Components.”

9. Do you prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements? Do you prefer the alternate format, where the requirements are grouped in separate standards? Or do you have no preference?

Summary Consideration:

There was no clear preference from the compilation of responses received. Many entities liked the approach and structure provided by the posted CIP-010 and CIP-011, while a substantial number would prefer to keep the current CIP-002 – CIP-009 structure. Reasons provided by the latter centered around substantial compliance management frameworks implemented to support the CIP-002-CIP-009 structure. Others offered a hybrid approach, with some grouping.

The SDT has considered these comments and has opted to keep, in large part, the current structure of CIP-002 – CIP-009, with the addition of two new standards, CIP-010 and CIP-011. The two additional standards allow for some requirements from previous standards, where the subject matter did not quite fit, to be separated into the additional standards. In this manner, the SDT believes that each standard consists of a set of related requirements that support an identified purpose.

#	Organization	Yes or No	Question 9 Comment
9.1	WECC		This seems to be essentially a formatting issue. If the same requirements are included in either on single standard or multiple standards, the preference is with the individual reader. Keeping it as one single CIP-011-1 standard will ease discussions throughout organization when talking about CIP as there will only be one standard for all controls and it makes sense based on the previous versions repeated statement that the standards should be treated as one standard.Breaking CIP-011-1 into multiple standards lends itself very well to being audited. In either option, what is needed is clarification and explicit language. Regardless of the format, the standard (s) needs to be made stronger, more clear, more concise.
9.2	ISO New England Inc	Break CIP-011-1 up into multiple standards	- Disagree with the current structure- Establish new standards by functional areas- Ensure there is not a circular loop relating to other requirements/standards, each requirement/standard should be standalone

#	Organization	Yes or No	Question 9 Comment
9.3	IRC Standards Review Committee	Break CIP-011-1 up into multiple standards	(i) We disagree with the current structure. We'd suggest the SDT to establish new standards by functional areas and ensure there is not a circular loop relating to other standards. Each standard should be standalone(ii) We understand the need for this standard to take care of cyber security concern when there does not currently exist an across-the-board cyber protection standards that apply generically to all sectors that utilize cyber components and cyber access for control and data exchange. However, over time, we urge NERC and the electric industry to assess if indeed it needs to have its own cyber protection standards at all. Cyber protection is not unique to the electric industry. Other sectors - airline industry, national security/ defense, financial sector, banking system, etc. all employ a high level of cyber security to protect fraud and invasions. Wouldn't the electric industry be better served if owners of BES Cyber Systems be required to adopt similar practices of these other sectors as opposed to developing it own very detailed set of requirements which, for the most part, seem to replicate the other sectors' requirements?It will be desirable to have a generic set of Cyber protection standards that is applicable to all sectors that use Cyber Systems - may they be for BES control or access to airline reservation, air traffic control, e-banking, security trading, etc. NERC and the electric industry should take the lead to initiate a continent-wide effort to consolidate all such standards and practices to avoid redundant efforts.
9.4	Entergy	Break CIP-011-1 up into multiple standards	A) Compliance Enforcement Problems: From the point of view of both implementation and auditing of Requirements it makes little difference as to the granularity of Requirements contained per Standard. However, from an enforcement perspective, using a single Standard document consisting of many Requirements is highly problematic. Per the current codified NERC Standards Development Process any Standard can be assigned only a single Violation Risk Factor (VRF). Consequently, even if only one Requirement in the single document approach is considered a "High" Risk Factor, then the entire Standard must be designated as High. This is problematic first in that not all CIP Requirements contained in either CIP-003-3 through CIP-009-3 or CIP-011-1 are of equal salience in terms of security vulnerability/risk created in virtue of failure to comply - some are indeed High, but by no means all. [However, note that

#	Organization	Yes or No	Question 9 Comment
			determination of Violation Severity Level (VSL) is not especially problematic - it's still a measure of just 'how far out of compliance' the Entity is.] Second, it is hard to imagine any Responsible Entity being 100% compliant with every Requirement in a single large Standard in any calendar year; it could well be that all Responsible Entities in the industry are found to be out of compliance with some aspect of a single large multi-Requirement Standard every year. Statistically, this does not speak accurately as to the quality of the NERC Standard, its Reliability Standards Program, or the industry's attentiveness or sense of urgency concerning the need for proper cyber security. For the reasons above, Entergy submits that a larger number of Standards, with fewer, more finely focused Requirements in each will serve our collective purposes much better.B) Cost Impact: Moreover, the cost of revising all the existing procedures, database systems, and other compliance programs to comport with a new numbering system alone is prohibitive for any company with a large number of cyber assets. There is no support in the administrative record for the notion that the current numbering system is a problem, or that the proposed combined "all-in-one" standard would improve grid reliability, security, or companies' efforts to comply with the standards. The change to a single CIP-011-1 Standard is arbitrary and of no salient value to anyone. Summarily, Entergy proposes that the: i) Organization and naming/labeling of Version 4 of the CIP Standards remain intact, i.e., simply the fourth iteration of Version 1. ii) SDT should lay FERC Order 706 side by side with CIP-003-3 through CIP-009-3 and make changes specifically attendant to 706 FERC directives - no more, no less. iii) Topical subjects addressed in CIP-003-3 through CIP-009-3 Standards respectively should remain the same, i.e., subject matter organization should not be moved under from under one Standard to another;iv) Concepts already well established and understood throughout the industry created under CIP V1, e.g., CA, CCA, ESP, PSP, etc., should be preserved intact; and,v) Orientation in Version 4 toward protection of "data in motion" is applauded.
9.5	CenterPoint Energy	Break CIP-011-1 up into	As stated above, many entities are now in the compliance phase of the current CIP Standards and have spent a great deal of effort in developing documentation and evidence gathering processes base on the CIP-002 through CIP-009 Standards.

#	Organization	Yes or No	Question 9 Comment
		multiple standards	CenterPoint Energy is concerned about the upheaval required to alter processes and procedures, currently tied to multiple Standards, to match a single Standard. CenterPoint Energy recommends keeping the current format.
9.6	Northeast Power Coordinating Council	Break CIP-011-1 up into multiple standards	Because of the number of requirements involved, combining all into one document will make it more difficult for stakeholders to use, and make it more difficult to assess compliance.
9.7	FirstEnergy Corporation	Break CIP-011-1 up into multiple standards	Break CIP-011-1 up into multiple standards. Multiple standards allows for easier ownership assignment and referencing (indexing) within policies and programs. The new format still provides multiple reference for the same item in multiple locations (e.g. Access), therefore this supports keeping multiple standards.
9.8	City Utilities of Springfield, Missouri	Break CIP-011-1 up into multiple standards	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
9.9	Reliability & Compliance Group	Break CIP-011-1 up into multiple standards	Combining some of the standards may make sense but combining them all does not make it easier to comply, it instead creates an administrative mess by requiring everyone to change all their document references to conform to the new standards and requirements.Some standard combinations that do make sense are physical, electronic and information access (CIP-003 R4, CIP-005 R2-R3, and CIP-006 R2-R6). Also, combining incident response and recovery makes sense.Has a decision yet been made how this would be audited as a single standard? Would we now have compliance violations reported on a requirement level instead of a standard level?

#	Organization	Yes or No	Question 9 Comment
9.10	San Diego Gas and Electric Co.	Break CIP-011-1 up into multiple standards	Due to our previous CIP compliance efforts and all the documentation and Standard Operating Procedures currently in place, SDG&E recommends keeping (as much as possible) the existing CIP Standards and Requirements in place, and augmenting each of the existing Standards with new and modified Requirements. This strategy will allow participating entities to transition to the new version 4 requirements in an easier fashion, while making better use of existing documentation and procedures. We've put a lot of time into the organization, layout, and design of our process and materials and it appears to be a daunting task to revamp all of this to comport with almost completely new Standards. For example, most participating entities would now recognize CIP-004 as having to do with Personnel and Training, whereas combining all the CIP-003 through 009 requirements in CIP-011 just makes it that much more difficult to leverage existing compliance efforts and documentation without a major revamping effort.SDG&E recommends maintaining the current format of standards as CIP-002 to CIP-009, and enhancing the required individual standards as necessary. The existing standards are clear by function and controls - based on general cyber security and systems security practices and controls with the goal of protecting Confidentiality, Integrity and Availability. The implemented standards cover policy, access, change control, monitoring, DR, etc..., and are simple to review, document, communicate, audit and coordinate activities against. Transitioning to a comprehensive single document requires Entities to perform additional translation, communication, implementation and review across departments, organizational structures and systems owners, and increases the potential for communication and task errors, and the potential probability of introducing an operational or security concern.
9.11	E.ON U.S.	Break CIP-011-1 up into multiple standards	E.ON U.S. prefers that individual standards be used instead of the combined standards as outline in CIP-011.

#	Organization	Yes or No	Question 9 Comment
9.12	Matrikon Inc.	Break CIP-011-1 up into multiple standards	For Responsible Entities, their Compliance Teams, their Employees, and their Contractors have all been indoctrinated with the terminology, standards and requirement numbering of CIP 002-009. One reason for continuing a similar number standard is to reduce the confusion for all those involved with compliance, and migration from CIP-002/009 to CIP-010/011.The second reasoning for maintaining similar numbering is the mapping exercise of CIP 002-009 to CIP-010 and CIP-011. If the first priority is to perform the mapping between the two evolutions of the standard, then organically CIP-010/011 will be organized. This will help all affected parties identify the differences, perform gap analysis, and implications to their environment much easier. Unfortunately, all organization will have the exercise of re-authoring a lot of their own NERC CIP compliance procedures to catch up with the new terminology, numbering, and requirements. This will help to maintain compliance with CIP-002/009 while implementing CIP-010/011. Regardless if this is performed by the SDT, every Responsible Entity and Auditor is going to have to do this exercise anyways, with subtle differences.My suggestion is to consider skipping CIP-010, and name it CIP-012. Then take the content related to CIP-003, and organize it into CIP-013. Effectively, putting the next evolution of the standards into the next "decade", whereby the second-digit is incremented.
9.13	Exelon Corporation	Break CIP-011-1 up into multiple standards	Given the extensive work that has been done to establish monitoring and compliance tracking systems, the wholesale change in format will cause extensive rework to compliance programs (systems, procedures, governance models, etc...). One must ask how this re-work is intended to improve reliability. Unless there is a strong basis for making such a dramatic change to a set of standards that have not been in force for many years, Exelon sees neither need nor value in making such a dramatic change. This change will result in essentially starting from the beginning from a compliance program perspective. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.

#	Organization	Yes or No	Question 9 Comment
9.14	USACE HQ	Break CIP-011-1 up into multiple standards	I suggest to break up the standard into three (3) standards, one (1) for low impact BES Cyber System, one (1) for medium impact BES Cyber System, and one (1) for high impact BES Cyber System. This way it is more clear what is required for each impact level system.
9.15	Progress Energy (non-Nuclear)	Break CIP-011-1 up into multiple standards	If NERC separates into multiple standards, need to make sure the CIP standards are stand alone.
9.16	Indeck Energy Services, Inc	Break CIP-011-1 up into multiple standards	In addition to breaking up the standards by grouping, they should be broken up by facility type and/or function. Not all of these standards apply equally to all facility types or functions. Unmanned facilities with direct communications with a BES control facility need a different set of requirements from a continuously staffed facility without direct communications with a BES control facility. Requirements for a BA are different than for a GOP.
9.17	MWDSC	Break CIP-011-1 up into multiple standards	It is confusing that the tables for each major category only show those requirements with different impacts, while there are other requirements that apply to all impacts. Suggest adding a matrix of all the requirements by a major category showing all the requirements and impacts, not just the ones which differ. Having one standard would require the entire standard to be re-issued for any change. This may cause more confusion whether anything else changed and create more wasted paper. Suggest multiple standards or using a numbering scheme such as CIP-011-1.1, CIP-011-1.2, CIP-011-1.3, etc to separate the requirements by major categories. If there is a change to a major category, the numbering would be CIP-011-1.2a, CIP-011-1.3c, etc.
9.18	Platte River Power	Break CIP-	It would be clearer if the requirements were organized based on their objectives:

#	Organization	Yes or No	Question 9 Comment
	Authority	011-1 up into multiple standards	physical security, system security, boundary security, personnel management, access, etc. One document would be fine if the requirements matched up with the standards and the sub-requirements matched up with the requirements.
9.19	Allegheny Energy Supply	Break CIP-011-1 up into multiple standards	It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements
9.20	Allegheny Power	Break CIP-011-1 up into multiple standards	It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.
9.21	EEI	Break CIP-011-1 up into multiple standards	It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.
9.22	MidAmerican Energy	Break CIP-011-1 up	MidAmercian Energy does not prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements. The revolutionary approach proposed

#	Organization	Yes or No	Question 9 Comment
	Company	into multiple standards	will cause confusion, which may adversely affect the reliability of the BES. The version 4 standards should be built upon the existing standards to avoid the unnecessary confusion that will be introduced during the implementation of CIP-011. Rewrite CIP-011 and apply the requirements to existing CIP-003 thru CIP-009 standards.
9.23	CWLP Electric Transmission, Distribution and Operations Department	Break CIP-011-1 up into multiple standards	Monitoring changes to the requirements would be easier if they were separated into different standards.
9.24	Con Edison of New York	Break CIP-011-1 up into multiple standards	Most owners of BES equipment have multiple departments that manage different corporate functions. These departments include Information Resources, System Operations, Human Resources, Relay Protection, Engineering, etc. Organizing the CIP requirements into topic-specific standards (as was done for CIP-002 through CIP-009), will facilitate corporate management of compliance.
9.25	Michigan Public Power Agency	Break CIP-011-1 up into multiple standards	Multiple standards that are logically separated is preferred. However, if separated the standards still should be approved as a complete set.
9.26	PacifiCorp	Break CIP-011-1 up into multiple standards	PacifiCorp does not prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements. The revolutionary approach proposed will cause confusion, which may adversely affect the reliability of the BES. The version 4 standards should be built upon the existing standards to avoid the unnecessary confusion that will be introduced during the implementation of CIP-011. Rewrite CIP-011 and apply the requirements to existing CIP-003 thru CIP-009 standards.
9.27	Florida Municipal Power	Break CIP-	The addition of sub-headings into CIP-011 is illustrative of the need to separate them.

#	Organization	Yes or No	Question 9 Comment
	Agency	011-1 up into multiple standards	From a presentation perspective, e.g., most frequency violated standards, we would be faced with tough decision of either having one standard with a very large bar in a top 10 bar chart, or possibly having multiple CIP standards is the bar chart, until the Industry gets used to the new standards. Either way is politically difficult, so, the simpler approach is probably the preferable approach of multiple standards on different security topics.
9.28	APPA Task Force	Break CIP-011-1 up into multiple standards	The APPA Task Force believes the addition of sub-headings to CIP-011 is illustrative of the need to separate this standard into multiple standards. We also feel with multiple standards the revision process would be simplified. If only one section needs to be revised, then NERC could just post that particular section for industry comment.
9.29	Emerson Process Management	Break CIP-011-1 up into multiple standards	The original setup seems indicating some logic on how cyber security should be addressed. Also, it has been there for several years. Most people probably have become used to the titles and subjects.
9.30	Southern California Edison Company	Break CIP-011-1 up into multiple standards	The section of standards that deal with controls should be divided into components that are grouped thematically. For instance, management of personnel may contain all requirements pertaining to training, background checks, etc., as one standard. Another standard should be used for governance functions such as policy making and management, audit documents, change management, etc. A third standard for Access Management can be used to list in detail end-to-end access controls for interactive access that is electronic, escorted and unescorted physical access and access to information. Boundary protections, physical and electronic, can be addressed as a family of security controls along with system security requirements as a fourth standard. A section that describes priority of controls within each requirement, in addition to a VRF/VSL document, should be provided so that RE's can implement controls at a granular level even within the High-Medium-Low framework.SCE supports the

#	Organization	Yes or No	Question 9 Comment
			modification of the CIP standards from a family of eight controls in the current version, and the reduction of the number of sub-levels within requirements. But on the other hand, combining all controls into "one standard" is a cause for concern.
9.31	LCEC	Break CIP-011-1 up into multiple standards	The standard grouping in CIP11 will result in a negative perception as to the progress industry is making in improving cyber security of the BES. Consider individual standards or a new approach to metrics reporting that focuses on the security domain versus the standard.
9.32	Old Dominion Electric Cooperative	Break CIP-011-1 up into multiple standards	This draft is far too cumbersome. Breaking up the requirements will allow emphasis to be placed on categories that may be more critical to security. Breaking up the requirements will also allow for much easier application.
9.33	Pepco Holdings, Inc. - Affiliates	Break CIP-011-1 up into multiple standards	We agree with EEI's comments.
9.34	We Energies	Break CIP-011-1 up into multiple standards	We Energies agrees with EEI comments: It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.

#	Organization	Yes or No	Question 9 Comment
9.35	Luminant	Keep CIP-011-1 as one document	future changes that do not impact the compliance domentation numbering should be considered
9.36	FEUS	Keep CIP-011-1 as one document	Having CIP-011-1 as one document makes it more streamlined and is easier to follow. The concern FEUS has is how multiple violations of several different sub-requirements will be looked at by the compliance enforcement agencies. If an entity is found in violation of CIP-011-1 R4 for example and is later found in violation of CIP-011-1 R26 will this be considered a second violation? If so, FEUS would prefer CIP-011-1 to be grouped into separate standards.
9.37	Public Service Enterprise Group companies	Keep CIP-011-1 as one document	Having the requirements in a single standard significantly improves understanding and ease of reading.
9.38	Ameren	Keep CIP-011-1 as one document	It is much easier to find all the requirements when all contained is a single document and the chance of discrepancies between documents is greatly reduced. However, the CMEP should be updated to monitor and report violations by standard and requirement not just standard. Otherwise, CIP-011 will always be in the list of Top 10 most violated standards and create a misleading impression that utilities cannot figure out how protect the reliability of the BES.
9.39	Southwestern Power Administration	Keep CIP-011-1 as one document	Keeping the controls in one document as proposed is preferable; provided that the intent is not that ALL requirements in CIP-011-1 have to be audited as a family of requirements.
9.40	Dairyland Power	Keep CIP-011-1 as	One document is better.

#	Organization	Yes or No	Question 9 Comment
	Cooperative	one document	
9.41	Green Country Energy	Keep CIP-011-1 as one document	One document makes it a lot cleaner for a smaller entity to deal with.
9.42	Progress Energy - Nuclear Generation	Keep CIP-011-1 as one document	Security controls included in CIP-011-1 are similar to the Security Controls established by Nuclear Energy Institute (NEI) 08-09, Revision 6, Appendices D and E. These security controls are based on one or more National Institute of Standards and Technology (NIST) 800 series standards and have been accepted by the Nuclear Regulatory Commission (NRC) in a letter dated May 5, 2010. Alignment of CIP security controls with security controls based on NIST 800 series standards and implemented in NEI 08-09, Revision 6, for nuclear plant systems would prevent regulatory uncertainty and potential dual regulation of a single system.
9.43	Consultant	Keep CIP-011-1 as one document	Subject to the following:1. Requirement number should be consistent with the Requirement table numbering. For example, currently requirement 3.1 Cyber Security Training does not relate to Table item 3.1 Electronic Access. The result is two items that would be referenced as CIP-011 3.1 on completely different topics.2. Every requirement should have a related table. Currently R1 & R2 do not have related tables for applicability. It is 'bad practice' to assume the interpretation that those requirements without a table apply to everything.3. The 'local definitions' should be gathered in a separate definitions section and numbered. Lacking a definitions section there is no convenient mechanism to refer to local definitions.4. While I understand the expressed opinion makes the standard easier to use, I don't agree with that opinion. The defined terms related to this standard should be listed in a separate section. My opinion is that the current format of the local definitions is more confusing than clarifying.5. Based on the CIP Standards Workshop information, I would suggest the Requirement statment (R1, R2, R3, etc.) be a statement of the requirement objective, and the Table rows be

#	Organization	Yes or No	Question 9 Comment
			implementing requirements for that objective. This approach should also resolve items 1 & 2 above.
9.44	RRI Energy	Keep CIP-011-1 as one document	The previous CIP-003 through CIP-009 required cross-referencing between the standards and standard owners to get it right. CIP-011 is much easier to follow and understand.
9.45	Bonneville Power Administration	Keep CIP-011-1 as one document	The single document format clearly states the requirements unlike the current standards which link to one another but do not clearly link the requirements.Having CIP-011-1 as one document rather than multiple standards is great. All of the requirements are in one place and easy to find.
9.46	Detroit Edison	Keep CIP-011-1 as one document	The tables holding the sub-requirements are a good feature that enhances readability. CIP-011 R3 and R4 have some requirements outside of the table and some in the table. Please move all sub-requirements to table format so each requirement would become a paragraph followed by a table with subrequirements. This will help minimize confusion caused by having a requirement and a table entry with the same number.
9.47	Dominion Resources Services, Inc.	Keep CIP-011-1 as one document	Using a single standard for all requirements is preferred, however the format internal to the single standard appears to be inconsistent. For example, some requirements are in paragraph form while others are embedded in a requirements Table. All requirements should be contained within a requirements Table. Where possible, information preceding the table should be used only to state the context and establish the security objective or intent behind the requirements.
9.48	Manitoba Hydro	Keep CIP-011-1 as one document	We agree with the proposed approach which creates a clear list of security requirements within a single standard. This addresses some of the complexity with the existing cyber security standards. We are, however, concerned about the current compliance monitoring and enforcement structure where the magnitude of fines and sanctions are levied based on prior violations, and the violations are reported per standard. The

#	Organization	Yes or No	Question 9 Comment
			proposed standard contains over one hundred requirements and sub-requirements, which increases an entity's exposure to multiple violations for a single standard, and increases the exposure of the industry to a large number of violations to a single standard.
9.49	Hydro One	Keep CIP-011-1 as one document	We agree with the proposed format for simplicity purposes. However, by consolidating the current version 3 standards into one document, this new CIP-011 standard would become one of the NERC's standards with the largest number of requirements. This could potentially make it "the most violated" one as well consequently impact the amount of monetary sanctions. If the proposed format is adopted, special compliance consideration should be adopted when dealing with violations
9.50	Minnesota Power	Keep CIP-011-1 as one document	With the requirements in a single document, it seems that it will be easier to arrange and consolidate requirements to alleviate the duplications and contradictions which have plagued the preceding CIP standards.
9.51	Tenaska	No preference	A personnel training issue can cause a violation of the whole standard that will be looked at as the same as a Cyber System boundary problem (Outsider Scanning). Until violations reporting and sanctions are reported at the requirement level only, then this could have a disproportionate impact on the entity relates to potential impact on the BES.
9.52	Network & Security Technologies Inc	No preference	Believe the SDT's time and effort are better spent on defining well-understood and auditable requirements that will enhance BES security & reliability than on trying to force-fit new/updated requirements into existing document structures.
9.53	US Army Corps of Engineers, Omaha Distirc	No preference	Combined this standard covers a very large number of requirements. Note the drafting committee divided the standard into several logical groupings for the presentation of the standard.

#	Organization	Yes or No	Question 9 Comment
9.54	ERCOT ISO	No preference	Either option is acceptable. Having them in one document could prevent public documentation of specific areas of weakness for an organization as audit results are public information and published on the NERC website. It also eliminates the need for circular referencing that is in the current CIP-002 to CIP-009 (e.g., CIP-005 R1.5).
9.55	Southwest Power Pool Regional Entity	No preference	Having all of the requirements in one document as opposed to many makes no difference to the compliance monitoring and enforcement process as long as Violation Severity Levels and Violation Risk Factors do not roll up higher than the main-level enumerated requirements. The advantage of keeping everything in one document is simpler version management and reducing the need for cross-standard references. The disadvantage is that more of the requirements will potentially be exposed to comments whenever the standard is being updated. Additionally, multiple standards permit parallel modification efforts whereas a single standard may result in single-threaded modifications over a prolonged development and approval timeframe.
9.56	Pacific Gas & Electric Company	No preference	Keeping CIP-011 as one document reduces complexity and makes overall understanding easierBreaking CIP-011 into multiple documents facilitates certain compliance and accountability aspects
9.57	SCE&G	No preference	The SDT should consider the advantages of breaking the Standard into multiple standards, as far as implementation goes. Some requirements will require more time to implement than others. Having the standard broken apart may make distinguishing these timeframes easier.
9.58	Southern Company	No preference	The tabular format for the requirements section is an excellent vehicle to capture the individual requirements. This should be expanded to include all requirement items. The numbering in the tables should be made unique to match the associated requirements in the standards body. (i.e., R3.1 is related to security training while table entry 3.1 is related to electronic access.)Sections of the table which do not apply should be marked N/A.

#	Organization	Yes or No	Question 9 Comment
9.59	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	No preference	Violations are by requirement, so whether it is one standard or multiple standards makes no difference.
9.60	Independent Electricity System Operator	No preference	We understand the need for this standard to take care of cyber security concern when there does not currently exist an across-the-board cyber protection standard that applies generically to all sectors that utilize cyber components and cyber access for control and data exchange. However, over time, we urge NERC and the electric industry to assess if indeed it needs to have its own cyber protection standards at all. Cyber protection is not unique to the electric industry. Other sectors - airline industry, national security/ defense, financial sector, banking system, etc. all employ a high level of cyber security to protect fraud and invasions. Wouldn't the electric industry be better served if owners of BES Cyber Systems be required to adopt similar practices of these other sectors as opposed to developing it own very detailed set of requirements which, for the most part, seem to replicate the other sectors' requirements?It will be desirable to have a generic set of Cyber protection standards that is applicable to all sectors that use Cyber Systems - may they be for BES control or access to airline reservation, air traffic control, e-banking, security trading, etc. NERC and the electric industry should take the lead to initiate a continent-wide effort to consolidate all such standards and practices to avoid redundant efforts.These comments notwithstanding we still offer some comments on the remaining questions.
9.61	Verizon Business	Keep CIP-011-1 as one document	One document eliminates potential confusion about the use of the correct version. However, during the initial implementation phase, there may be multiple revisions for CIP-011 being issued each month/quarter.

10. The Purpose of draft CIP-011-1 states, "To ensure Functional Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems for which they are responsible and that execute or enable functions essential to reliable operation of the interconnected BES." Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Suggestions for the purpose statement for the draft CIP-011 standard included several suggestions for rewording as well as comments expressing confusion around the term BES Cyber Systems. Several commenters expressed that the owner of BES Cyber Systems should have responsibility for compliance with the Standards and the Purpose statement did not reflect this.

In response to the industry comments received for draft CIP-011, the CSO706 SDT decided to divide up the draft CIP-011 requirements and include them in the multiple Version 5 CIP Standards (CIP-003 through CIP-011). Therefore, the purpose statement included with the draft CIP-011 no longer applies.

#	Organization	Yes or No	Question 10 Comment
10.1	PacifiCorp	Agree	: PacifiCorp agrees with EEI's suggested revision:"To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES."
10.2	WECC	Agree	Agree with the genearal purpose however, The term "necessary cyber security protection" in the purpose statement has no meaning without a frame of reference. The purpose statement may be used to clarify intent where the standard language is ambiguous or vague, so it should explicitly state the objectives of the standard.The phrase "...that perform functions essential to reliable operations of the interconnected BES" in the purpose statement is redundant. BES Cyber Systems are defined elsewhere so this clause adds confusion at best, and contradicts at worse.
10.3	Southwest Power Pool Regional Entity	Agree	As an overall purpose, the statement is OK. Consider addressing the issue of "responsibility" as it pertains to multiple entity aspects, including joint ownership

#	Organization	Yes or No	Question 10 Comment
			agreements, different owners versus operators, and the like.
10.4	Old Dominion Electric Cooperative	Agree	I agree under the assumption that this is in line with the enabling legislation in the Energy Policy Act. I disagree that this is the best way to go about achieving this goal.
10.5	Green Country Energy	Agree	I agree with the concept, however as I will repeat through the remainder of the comments, A guidance document is needed to address key points desired to be accomplished by these policies. This will also reduce the subjectivity during audits of this and all the following requirements
10.6	Progress Energy (non-Nuclear)	Agree	It is still unclear if cyber security implies that an external communications capability is available. Definitions and references seem to indicate that we can have a BES cyber system component without external connectivity.
10.7	US Bureau of Reclamation	Agree	Recommend that the Drafting Team change "Functional" to "Registered" in the 1st line of the Purpose. Add "they" between "that" and "execute" in the 3rd line of the Purpose statement.
10.8	Minnesota Power	Agree	This purpose statement is generally acceptable, with clarification or correction to the following: o What is the definition of “responsible”? Minnesota Power recommends changing this to “own” as is stated in CIP-010-1, R1. o The reference to “Functional Entities” should be replaced with “Registered Entities.” “Functional Entities” is not a defined term.
10.9	San Diego Gas and Electric Co.	Agree	While SDG&E agrees with the purpose of CIP-011 as applied to the various requirements, we would like to see additional language that would help clarify the meaning of the phrase “responsible for”. What if an entity owns a particular asset but does not operate it?
10.10	ISO New England Inc	Disagree	- Please provide additional clarification. Especially with regard to “necessary cyber security protection”.- Suggest changes from “cyber security protection” to “cyber

#	Organization	Yes or No	Question 10 Comment
			security controls".
10.11	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Advise replacing "are responsible" with "operate." Where one Entity may own the BES Cyber System, and another Entity operates the same BES Cyber System, it must be clear who will be responsible for developing and implementing the policies. In many instances, the owner of a BES Cyber System only has monitoring capability, and no control or supervisory role in the BES Cyber System. Owners should not be responsible for creating policies for Systems they do not fully understand; owners should only be responsible for securing the BES Cyber System Components that they operate.
10.12	FirstEnergy Corporation	Disagree	As stated in our opening remarks, we fundamentally oppose the change in terminology. Additionally we disagree with the need for functional categorization as described in Attachment I. Therefore, we do not support the purpose statement of CIP-011.It is suggested that the proposed definitions for BES Cyber System and BES Cyber System Component could be combined to redefine the existing Critical Cyber Asset term allowing industry to better leverage its existing CIP implementation.Additionally, there is a concern, in going with the concept of "BES Cyber Systems" that it will expand beyond the systems that are directly responsible for the reliable/safety of the BES and into business systems.
10.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
10.14	ERCOT ISO	Disagree	Consider: "To ensure Responsible Entities develop cyber security programs to provide for appropriate protection of the BES Cyber Systems for which they are responsible that execute or enable functions essential to reliable operation of the interconnected BES."
10.15	Consultant	Disagree	Cyber security policies or cyber security protection do not 'execute' functions essential to reliable operation of the BES. Suggest removing the word 'execute'."interconnected BES" is not a defined term. Suggest removing the word 'interconnected'.

#	Organization	Yes or No	Question 10 Comment
10.16	US Army Corps of Engineers, Omaha Distirc	Disagree	Delete everything after "for which they are responsible." It reads awkward and is merely restating the meaning of BES Cyber System.
10.17	Kansas City Power & Light	Disagree	Do not agree with ensuring security policies in the purpose. The express purpose of these requirements should be to identify the cyber systems that require protection and the level of protection to achieve. There is no need to include a purpose of entering into the management of an organization and the levels an organization deems necessary to achieve compliance with the these CIP Standards or any other NERC Reliability Standard.
10.18	Dominion Resources Services, Inc.	Disagree	Dominion recommends changing the statement as follows: "To ensure Functional Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems."
10.19	American Municipal Power	Disagree	I feel the purpose is not based on reliability. The purpose should not restate the applicability section.
10.20	Wolverine Power	Disagree	I have a concern with how to detrmine hat constitutes a "BES Cyber Ssystem" I don't think the standards are clear.See comments listed for 1.a fro explanation and proposed solution
10.21	Turlock Irrigation District	Disagree	Is the use of the words "the BES Cyber Systems for which they are responsible" above meant to be the same as the words "the BES Cyber Systems that it owns" which are used in CIP-010-1 R1? The Purpose of CIP-011-1 focuses compliance responsibility on the entity that is responsible for the BES Cyber Systems while CIP-010-1 R1 focuses compliance responsibility on the owner of the BES Cyber Systems.
10.22	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggested revision:"To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES."

#	Organization	Yes or No	Question 10 Comment
10.23	NextEra Energy Corporate Compliance	Disagree	NextEra believes implementation responsibility of protection methods should tie back to facilities under the entities control and ownership.
10.24	Reliability & Compliance Group	Disagree	Recommend adding the words “and implement”. Also the phrase “execute or enable functions essential to reliable operation…” needs a more concise definition.
10.25	Independent Electricity System Operator	Disagree	See response to Q9.
10.26	Network & Security Technologies Inc	Disagree	Suggest replacing “enable functions essential to…” with “support functions essential to…”
10.27	Allegheny Energy Supply	Disagree	Suggested Revision:”To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES.”
10.28	Allegheny Power	Disagree	Suggested Revision:”To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES.”
10.29	EEI	Disagree	Suggested Revision:”To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES.”
10.30	Nuclear Energy Institute	Disagree	The phrase “and that execute or enable functions essential to reliable operation of the interconnected BES” should be struck as it is redundant to the definition of BES Cyber Systems.
10.31	APPA Task Force	Disagree	The purpose is not to “develop … policies” as the first item in the list currently indicates. The purpose is to protect cyber systems from attack, with policies, procedures, etc., to support that purpose. The APPA Taskforce suggests inserting the following “Purpose”

#	Organization	Yes or No	Question 10 Comment
			section:Purpose: To safeguard the reliability of the Bulk Electric System (BES) by protecting BES Cyber Systems from attack through the use of appropriate policies, procedures, tools and other resources.The APPA Task Force further recommends that each of the Requirements be reworded to separate out the stated objective to be accomplished from the text of the actual requirement and to state the objective prior the text of the Requirement. Auditors should not be placed in the position of having to evaluate if an entity has met the objective stated in the requirement, since this is essentially a subjective judgment. We feel this objective should not be part of the requirements. Here is one example of our proposed format illustrated with Requirement R5: Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R5 - Physical Security for BES Cyber Systems. The APPA Task Force recommends adding the following "Objectives" section after the Purpose in this standard:A. Introduction 1. Title: Cyber Security - BES Cyber System Protection 2. Number: CIP-011-1 3. Purpose: To ensure Responsible Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems for which they are responsible and that execute or enable functions essential to reliable operation of the interconnected BES. 4. Objectives:a. Personnel Training, Awareness, and Risk Assessment: To ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems. b. Physical Security for BES Cyber Systems: To prevent and/or detect unauthorized physical access to BES Cyber Systems.c. Personnel Risk Assessment: To ensure that personnel who have such access have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. d. etc...If the Objectives are not incorporated into the Introduction, we recommend they be removed from the requirement all together. If the team determines they are necessary, they must be in a separate sentence prior to the requirement. See comments on Question #12 and all other questions regarding the requirement title.
10.32	Florida Municipal Power Agency	Disagree	The purpose is not to "develop ... policies" as the first item in the list currently indicates. The purpose is to protect cyber systems from attack, with policies, procedures, etc., to support that purpose. FMPA suggests the following:np"To safeguard the reliability of the

#	Organization	Yes or No	Question 10 Comment
			Bulk Electric System (BES) by protecting BES Cyber Systems from attack through the use of appropriate policies, procedures, tools and other resources."
10.33	Indeck Energy Services, Inc	Disagree	The purpose of CIP-011, assumes that every facility registered with NERC is a cyber threat. It needs to differentiate functional entities to determine the impact on BES ALR. The functions identifies in Attachment I of draft CIP-010 are all important. Many of them are provided by hundreds or thousands of facilities. The cyber policies envisioned cannot ensure (that is guarantee) that there will be no blackouts due to cyber attack. [suggestion] "To require Functional Entities to develop, coordinate and apply adequate cyber security protection to the BES Cyber Systems for which they are responsible and that will achieve BES Adequate Level of Reliability." The coordination is to avoid unnecessary duplication of cyber security protection. This may require a different type of requirement that links connected parties, such as TO and GO, as to protecting particular facilities.
10.34	Manitoba Hydro	Disagree	The purpose statement appears to be missing words in the last line. Consider adding the words 'as outlined in this CIP-011-1' after the word 'responsible'.
10.35	Constellation Energy Control and Dispatch, LLC	Disagree	The purpose statement will need to be developed for each standard if CIP-011 is broken up into its major components.
10.36	Platte River Power Authority	Disagree	This comment is referring to an earlier comment suggesting a mechanism for identifying a "Responsible Entity" who is responsible for implementing and demonstrating compliance. With the "Responsible Entity mechanism in place I would suggest the following revision:To ensure the Responsible Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems that execute or enable functions essential to the reliable operation of the BES.
10.37	Entergy	Disagree	This Requirement uses the qualifier: "for which they are responsible." In Requirement 1 of CIP-010-1 (Question 3) the qualifier is "that it owns" - these two requirement statements must be consistent one way or the other.

#	Organization	Yes or No	Question 10 Comment
10.38	ReymannGroup, Inc.	Disagree	Vendor management and due diligence of 3rd party vendors is a growing area of risk across multiple industries, including the bulk power system. We believe the "Purpose" language should be enhanced to clearly cover the Functional Entities' internal practices and those of its 3rd party resources. This should include all 3rd party vendors that may have on-site or off-site access to the BES hardware, software, or data. For example, the information security risk associated with a growing use of data recovery service providers is not addressed in the NERC guidelines. Data Recovery is defined in Wikipedia as the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally. The definition of a BES includes programmable electronic devices such as hardware, software, and data. It makes sense that as the demand for such electronic storage devices continues to rise, more equipment will be damaged or will fail due to daily wear and tear, physical damage, data corruption, or natural disasters (e.g., flood, fire, etc.) If backup copies of lost data on the BES are not available, the need for data recovery services will increase to keep pace with the use of BES technology. It could be made more clear to emphasis that Cyber security protections are applicable while the BES is in operation and off-line. BES could be taken off-line for repair or other incidents such as a damaged hard drive and recovery of BES data, which will require a 3rd party vendor to recover sensitive data from the BES device.We recommend that NERC consider adding a new Requirement for Vendor Management as described in our comments to Security Governance and Policy (R1) and updating the R25 and R30 guidelines to address this 3rd party vendor data recovery risk. It is a very small aspect of day-to-day operations in the scheme of the Entity's priorities, which is why it has gone unnoticed - until now. As one regulator commented to us recently, "this is not a potential problem - it is a real problem." It can create a huge risk with a huge downside, if it is not controlled. Most organizations don't even realize that this "sleeper risk" exists, until it is too late. The good news is that with minor updates to proposed guidelines, NERC can educate entities and others about the risk associated with the use of data recovery service providers and provide meaningful tactical guidance on how to manage such risk. The current initiative to revise the CIP Cyber Security Reliability Standards is a timely opportunity to take the initial steps.

#	Organization	Yes or No	Question 10 Comment
			Perhaps some organizations have included data recovery security practices and protocols in incident response or recovery planning. The challenge here is that it usually requires a material event to activate the incident response or recovery plans. In such instances, these plans do not address the proper day-to-day use of data recovery service providers that would not be considered a material event. Frequently, the use of a data recovery service provider does not trigger a formal recovery plan or incident response plan. It is unlikely that most entities would execute a recovery or incident response plan to recover data from a failed BES device in the normal course of day-to-day activities. In the interim, it would be helpful to Functional Entities and others if NERC issued supplemental guidance specific to this topic. This will help establish an immediate awareness of the risk and share much needed guidance on appropriate due diligence and security protocols for data recovery service provider activities, selection, and use. Specifically, the data recovery risk exists from a lack of information security protocols and practices in the vetting, selecting, and use of data recovery service providers.Whether a breach of sensitive information occurs from a hacker, cyber threat, insider threat, or a data recovery service provider, the potential cost, fines, reputational damage, and loss of trust that an organization would experience is huge. In short, data recovery service provider risk can create as much damage as other risks that are addressed in existing NERC guidelines, if adequate controls are not defined and implemented. A typical security and compliance budget will allocate funds to protect people, information, and assets within the perimeter. Many entities are also focused on protecting data on the inside of their organization from outside attacks. Data recovery, however, frequently falls into a low priority category that does not pop-up on the CISO's radar or in an information security risk assessment. The need for data recovery is frequently associated with an immediate sense of urgency, e.g., the data contained on the damaged storage device must be recovered right away. o Help Desk personnel or office technicians are usually tasked with the responsibility of selecting an outside third party vendor to recover the data quickly. o Such third party vendors may or may not be listed on an approved vendor list. o Frequently, the due diligence and selection process of such a vendor is limited to its financial stability, the cost of its services, and a fast

#	Organization	Yes or No	Question 10 Comment
			"turnaround time."According to an independent national study - Security of Data Recovery Operations - published by the Ponemon Institute in December 2009 and conducted among IT security and IT support practitioners, there is a gap in security guidelines when selecting data recovery service providers. Specifically, o Sixty-four percent of the respondents decentralize the selection for data recovery vendors to the local level, e.g., Help Desk, while 24 percent are not sure how the vendor is selected. o Sixty-nine percent of the respondents do not have or are unsure if they have a policy for ensuring the protection of data during the recovery process. o Forty-nine percent say IT security is not involved in the selection process. o Only 20 percent believe data security is a major selection criterion. o Eighty-two percent say that it should be.A large percentage of respondents in this study (83 percent) reported at least one data breach in the past two years. Of the 83 percent who said the organization had a data breach, 19 percent said the breach occurred when a drive was in the possession of a third-party data recovery service provider. Forty-three percent of those respondents who said the breach occurred while at the vendor say it was due to a lack of data security protocols. Most organizations also have some additional backup and recovery procedures that overshadow the sense of urgency for more attention to data recovery practices on devices that were not backed up. In short, even with a strong backup recovery program, data recovery needs still arise. Seventy-nine percent of the respondents to the Ponemon study noted that their organizations have used or will continue to use a third-party data recovery service provider to recover lost data.Additional guidance is needed on how to extend current information system program practices to clearly address the protection of sensitive data, while it is in the possession of a third party service provider for data recovery. If the Entity has a strong vendor risk management program, it should include ALL vendors that have access to sensitive data, including data recovery vendors. Mandated vendor management practices apply to all stages of the information life cycle. Specific to data recovery vendors, this includes:â^š Pre-selection and negotiation of Master Service Agreements with appropriate vendors. These should be reviewed by a risk management committee and audited on an annual basis.â^š Due diligence of all third party vendors (e.g., financial stability, client references, information security

#	Organization	Yes or No	Question 10 Comment
			practices, etc.)â^š Verification of the vendor's security procedures to govern the transfer of devices and sensitive information.â^š Proof of internal information technology controls and data security safeguards, e.g., ISO 27001 certification, NIST SP 800-53 Audit Report, FFIEC Service Provider Examination Report, BITS Shared Assessment Report, or SAS 70 Type II Audit Report (especially if the data recovery involves financial information). The appropriate certification and audit report will vary depending on the service provider's client base.â^š Proof of current training and certifications of engineers in all leading encryption software products and platforms.â^š Adequate chain-of-custody documentation and network security.â^š Vetted and performed background checks of its employees.â^š Adequate procedures for the secure and permanent destruction of devices, when required.â^š Capabilities for encryption of data files in transit and storage.â^š Adequate clean room facilities, e.g., certified ISO 5 (Class 100).â^š A security procedure for the analysis of the information and device upon return to the organization to ensure malware and other malicious software has not been loaded.The lack of information security protocols and practices in the vetting, selecting, and use of data recovery service providers is not a potential problem - it is a real problem! NERC guidelines are a key resource that can help educate functional entities and others to this sleeper risk and identify prudent risk management practices and controls.
10.39	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
10.40	We Energies	Disagree	We Energies agrees with EEI: Suggested Revision:"To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES."
10.41	GTC & GSOC	Disagree	We recommend the language should be consistent with CIP-010 "owns" versus "responsible for." As indicated in comments on 1.b above, "owns" may be problematic.

#	Organization	Yes or No	Question 10 Comment
10.42	Xcel Energy	Disagree	We suggest the Purpose be revised to state "...and apply necessary cyber and physical security protection..."
10.43	Verizon Business	Agree	Any "carryover exceptions" from CIP-002 to CIP-009 need to be identified. Specifically, OSI Layer 2 Protocols need to be explicitly addressed.

11. Requirement R1 of draft CIP-011-1 states, "Each Responsible Entity shall develop, implement, and annually review formal, documented cyber security policies that address the following for its BES Cyber Systems:" and then provides a list of topics that must be addressed. Do you agree with this proposal and list? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Many commenters requested more clarity regarding the terms used (including the following: "formal," "annually," "boundary protection," "security roles and responsibilities," "personnel," etc…). Commenters requested to have the terms used throughout the standard defined in this section. Additional clarity was sought in terms of the policy expectations, purpose, and structure. Specifically, there were numerous questions about what is meant by "policy language," along with concerns about how to demonstrate compliance with a policy. Some commenters also noted that the policy requirements were too prescriptive. There were some comments that led the SDT to believe that there was some possible confusion surrounding general policy hierarchy.

The SDT agrees with the need for additional clarification and clearer expectations with regard to the policy. The drafting team has provided clarification through the addition of guidance material related to items that should be included in policy, and has implemented a style for the measures in each requirement that can be used as an aid in setting clear expectations for possible audit evidence.

Some commenters raised questions about the requirements with respect to the Senior Manager; specifically with concerns about delegation and the potential for conflict with R3, or claims of double jeopardy between R1 and other requirements.

The SDT appreciates the concerns about double-jeopardy issues and the prescriptive nature of the requirements. As such, the SDT has proposed moving the prescriptive elements of the requirement to guidance. This approach will allow the Responsible Entity greater flexibility to create a policy that is meaningful for its unique environment, while still providing the foundation necessary for an effective cyber security program.

#	Organization	Yes or No	Question 11 Comment
11.1	Entergy	Agree	"Annually" must be defined. At least once every twelve months? At least once per calendar year (this could extend past 12 months). Please clarify.
11.2	Green Country Energy	Agree	Agree with the list, however I really see the need for a reference document or footnotes pointing to sources for guidance on the expectations for these policies. Because the policies / requirements were designed not to be to prescriptive they in turn need references to give some expectations as to the points to be addressed within the

#	Organization	Yes or No	Question 11 Comment
			policies. This will allow flexability as to tailor the policy to each business, the policy will meet with the objectives of NERC / FERC and make the policies easier to audit. Is this what results based standards is all about...
11.3	Covanta Energy	Agree	Annually may be needed due to frequent challenges and changes to cyber hacking techniques.
11.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
11.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent, but believes the following improvements should be made:What does "formal" mean, does the drafting team intend a Company Policy?Terms used in later requirements ought to be defined here, such as unauthorized access, Cyber Security Incident(s), and electronic access controls.Terms that are ambiguous, such as "Boundary protection" and "media sanitization" ought to have definition boxes associated with them. In general, definition boxes should be adjacent to the term as it is first used in the standard. Alternatively, a definitions sections such as is used in typical contracts could be a new standard section for those definitions that are used only in this standard that are not included in the Glossary.It should be clear the "Personnel ..." used in 1.4 includes external contractors.1.7 seems to encompass 1.5, 1.6 and 1.8, consider making 1.5, 1.6 and 1.8 sub-bullets of 1.7
11.6	National Grid	Agree	In 1.2 please elaborate on "security roles and responsibilities". What is the SDT looking the entities to include as part of this document?
11.7	Minnesota Power	Agree	Minnesota Power would like to see more detail regarding each of the topics on the list to help clarify the expected content of these policies. For example, item 1.3 requires the naming of a single senior management official, with no mention of the ability to also name delegates. Yet, Requirement R3 includes the following language: "...that are approved by the single senior management official...or their delegate..."

#	Organization	Yes or No	Question 11 Comment
11.8	Bonneville Power Administration	Agree	NOTE: This following comment deals more with structure of the document than it does with content: NIST SP 800-53 lists 19 families of security controls for Government systems. Although the purposes of 800-53 and CIP-011 are not equivalent, there seem to be 800-53 families missing from CIP-011 that address areas that should be of interest in CIP-011. Even if the individual controls are addressed in CIP-011, listing the families would be useful. In particular, it is unclear why Audit and Accountability, Contingency Planning, Identification and Authentication, Personnel Security, System and Communications Protection, System and Information Integrity, and Program Management are not addressed. We believe that incorporating these would be an improvement to the document. In the CIP versions 1, 2 and 3 standards organizations have had numerous and almost endless discussions about what "annual," "annually review," etc. means. Hours have been spent trying to figure out what these terms mean. Some have said that "annual" means within 13 months. Annual meaning "within 13 months" makes absolutely no sense. It would be extremely helpful to the industry if clarity were provided in CIP-011-1. The debate needs to end. There appear to be four different phrases that could be used to provide more clarity:1. "at least once every 12 months" - let's assume that the organization reviews all of the various policies referenced in R1 on July 15, 2010, and again on March 15, 2011. Using this phrase and example, however, raises a couple of questions. When must the next review be completed? Is it no later than July 15, 2011, or no later than March 15, 2012? In other words, is there a window in which "annual" events must occur, "12 months +/- a month" or if you perform something early for efficiency's sake, does your annual date reset to the earlier date?2. "every 12 months" - the review would occur on the same date each year. This would be virtually impossible to manage. 3. "within 12 months of the last . . ." - in this case let's assume that a review is performed on March 15, 2010. The next review would have to occur no later than March 15, 2011, but could occur earlier (let's say it occurred on December 15, 2010). If it occurred on December 15, 2010, the subsequent review would have to occur no later than December 15, 2011.4. "anytime during the calendar year" - which would give the organization maximum flexibility in accomplishing the compliance activities.The Standards Drafting Team (SDT) should

#	Organization	Yes or No	Question 11 Comment
			provide more clarity as to what is intended and use an exact phrase rather than the word “annually” review. #3 - “within 12 months of the last . . . .” appears to be clearer than either of the others while #4 would provide a hard deadline that would not result in "date creep."
11.9	Dominion Resources Services, Inc.	Agree	Please see Dominion’s response to Question 9.
11.10	Reliability & Compliance Group	Agree	This could be better clarified. Some may interpret this to mean that procedures that address those topics will satisfy the requirement. A global definition of cyber security policy might help.
11.11	ISO New England Inc	Disagree	- Suggest changing the word “annually” to “a defined time frame” provided example at the end.- Suggest removing the “one or more formal” and add “documented and approved cyber security policies.”
11.12	Garland Power and Light	Disagree	* Please clarify the words "one or more" - does this require the review of all policies for the following functions
11.13	Consultant	Disagree	1. The list should include "Governance" as the first item. Suggest the first three items should be subheadings to the Governance item.2. Technically, R1 does not require designation of a CIP Senior Manager. As worded it requires a policy addressing the "Identification of a single senior management official...". Suggest an additional requirement statement requiring the Responsible Entities to designate a CIP Senior Manager, and document that designation.3. The mechanism for assigning responsibility is typically not a policy. Consider modifying the statement "Identification of a single senior management official with overall authority..." with "The senior management official's authority..." as an item to be addressed in the policy.
11.14	FEUS	Disagree	1.3 does not allow for delegation of authority for situations when the identified senior manager is unavailable. The Drafting Team should consider allowing a delegate or

#	Organization	Yes or No	Question 11 Comment
			alternative designated by the senior manager.
11.15	USACE HQ	Disagree	1.3 is missing the language that the single senior management official has the power to delegate some or all of the functions and/or actions to one or more named delegates. Also, double jeopardy is present since Requirements 6, 7, 11, 14, 15, 16, 17, 18, 20, 21, 23, 24, 25, 26, 27, 29, 30, and 32 cover part of or all of the policy documentation been required in 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11, 1.12, and 1.13.
11.16	Alliant Energy	Disagree	Alliant Energy agrees with EEI on verbiage suggestions and clarifications.
11.17	FirstEnergy Corporation	Disagree	As written the requirement and the list will require significant rework of existing policies for negligible benefit. In fact, the retraining that will be required will cause confusion and increase the challenge of achieving and maintaining compliance.Provide a standard that addresses all access issues (physical, logical, informational, etc.) instead of it being in multiple sections. Would also like to see emergencies being brought back into the main document, instead of having it part of each section.
11.18	Poplar Bluff Municipal Utilities	Disagree	Based on past experience, saying "Each Responsible Entity shall..." causes the Regional Entity to apply all CIP Standard requirements to all entities even if they own no Critical Cyber Assets. CIP-011 should clearly state that its requirements only apply to Entities that own BES Cyber Systems.
11.19	Con Edison of New York	Disagree	CIP-011-1 refers to timed requirements in various ways. The requirements should define the meaning and differences between annual, every year, within 3 calendar years, once every 12 months etc. There continues to be multiple interpretations of how within 365 days, within 12 months or in 2 calendar years, etc is defined.The term “annual” and “annually” should be defined. A suggested definition follows:Annual and Annually shall mean approximately every 12 months, but any period of no less than 9 and no more than 15 months.
11.20	E.ON U.S.	Disagree	CIP-011-1, R1.3 does not specify delegation by senior manager as currently permitted

#	Organization	Yes or No	Question 11 Comment
			under CIP-003-2. E ON U.S. proposes that delegation of authority by the senior manager be included as currently provided in CIP-003-2.
11.21	Dairyland Power Cooperative	Disagree	Communications between components/systems at different facilities or between different entities is an area lacking governance. Boundary protection is not sufficient.
11.22	ERCOT ISO	Disagree	Consider: "Each Responsible Entity shall develop, implement, approve, and annually review formally documented cyber security policies that address the following for its BES Cyber Systems:" Please clarify the meaning of "1.1. Applicability to organizational and third-party personnel".
11.23	Progress Energy - Nuclear Generation	Disagree	Existing nuclear document hierarchy programs require review of policies, procedures, programs, and directives. The periodicity of the reviews should be consistent for nuclear generating facilities.See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
11.24	Southern Company	Disagree	For R1, What does "Addresses" mean? For 1.1...These are not usually actual third parties; the correct term is probably "non-employees acting on behalf of the Entity".R1.3 and R3 create a requirement (a single responsible figure) that does not exist in any other NERC standard. Governance structures should be determined by the Entity and should not be regulated; the focus should be on the meeting of the other requirements and on the overall culture of compliance, so that the Entity can focus on creating the organizational structure that allows it to best meet the needs of CIP-011. This clause should be removed.Change the word "policy" in R1 to "policy or equivalent document"."Boundary protection" is undefined.
11.25	ReymannGroup, Inc.	Disagree	In many situations, outsourcing information technology tasks offers the Entity a cost effective alternative to in-house capabilities. Outsourcing, however, does not reduce the fundamental risks associated with information technology or the business lines or BES Systems that use it. Because the functions are performed by an organization outside the

#	Organization	Yes or No	Question 11 Comment
			Entity, the risks may be realized in a different manner than if the functions were inside the Entity resulting in the need for controls designed to monitor such risks. An additional security policy on 3rd Party Due Diligence and Vendor Management should be included. Functional Entities' should be required to establish a formal risk management processes to establish, manage, and monitor IT outsourcing relationships.
11.26	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	It is not clear what the Entity is responsible for if they do not own or operate any BES Cyber Systems. The assumption is not clear if the BES Cyber Systems list is null that Requirement R1 is then not applicable. Further, if a Low Impact BES Cyber System is the one and only System an Entity is responsible for, it is not clear whether a policy corresponding to an item (such as 1.5. Physical security) is required when the subsequent related Requirement pertaining to that item has a null listing for the Low Impact column in the following table (see Requirement R5). We advise the following change: "Each Responsible Entity who owns or operates one or more BES Cyber System shall develop, implement, and annually review formal, documented cyber security policies addressing applicability found in Requirements R2 through R32. The cyber security policies shall address each of the following categories, and include a statement of non-applicability for a category where appropriate:"
11.27	Western Area Power Administration	Disagree	It seems the requirement wants us to make the Physical Security Plan a part of the Cyber Security Policies? Is that what is intended?
11.28	Duke Energy	Disagree	List of topics need to be better defined. For example, 1.8. "boundary protection" may need to be changed to "electronic boundary protection". 1.9 should be changed to "Change Management" and "BES Cyber system maintenance" to "Configuration Management" for better alignment with NIST, COBIT and other control framework documents. Also, this policy is the only place where a Sr. Management official is mentioned. Does one or more imply a different policy per requirement or per business unit? If we have more than one policy, does the same Senior Manager need to manage and implement the requirements of the standard?

#	Organization	Yes or No	Question 11 Comment
11.29	NextEra Energy Corporate Compliance	Disagree	NextEra comments that during an emergency situation, a utility's primary objective is to end the emergency situations as soon as possible. For example, before, during and after the impact of a hurricane, the affected utility will mobilize much of its workforce to address system and customer restoration efforts. This may cause certain CIP requirements or deadlines to be missed for a short period of time. Moreover, there may be a need to relax CIP requirements, such as contractor qualification requirements for unescorted physical access into substations. Given the unforeseeable nature of emergencies, it is not possible to ensure all deadlines are met ahead of time, nor is it possible to pre-qualify all contractors, because it is not always known which contractors will be available or needed for emergency situations. A provision for emergency situations in the cyber security policy provides the utility and auditors alike with a framework and vehicle to ensure that any missed CIP deadlines or requirements that were relaxed are tracked, documented and that after the event, any missed or relaxed CIP requirements are addressed within a reasonable time after the emergency situation has ended. To implement emergency provisions and add clarity to other issues, NextEra proposes the following revisions:Each Responsible Entity shall have a documented cyber security policy related to the protection of BES Cyber System Components and BES Cyber Systems. The cyber security policy shall be reviewed every year during the month of March and updated, as necessary, no later than March 31st . The cyber security policy may also be updated as necessary. The cyber security policy shall include the following:B. The applicability of cyber security policy to employees and contractor personnel, including the manner in which the cyber security policy will be made available to employees and contractor personnel; C. The list of employees responsible for authorizing unescorted physical and/or cyber access to a BES Cyber System component consistent with R2-R4; D. The identification of a single senior management official with overall authority and responsibility for leading and managing implementation of requirements within this standard, including contact information; E. A provision that addresses the Responsibility Entity's response to emergency circumstances in the context of CIP compliance. This provision shall address how the Responsibility Entity will track and document any missed CIP deadlines or CIP requirements held in abeyance

#	Organization	Yes or No	Question 11 Comment
			because of the emergency, and documents how, after the emergency condition has ended, any missed CIP deadlines or CIP requirements held in abeyance were brought back into compliance. An overview of the Responsibly Entity's approach to compliance is indicated with the following:
11.30	Ameren	Disagree	Overall this Requirement is vague and it will be open for interpretation during an audit. Suggest adding references to the corresponding requirements for sub-requirements R1.1 through R1.13. Also, if corporate policies cover all these areas would that be sufficient to prove compliance? Does the Senior Manager still need to approve this policy? These questions need to be answered to provide necessary clarity.
11.31	Tenaska	Disagree	R2 Clarify Sound Security PracticeR3 If a CCA were to go DOWN (NOT running) and the only vender that is available at that time that can fix it is not trained and/or criminal background and identity verified, does the standard address how to utilize the vendor and not violate the standard?
11.32	Exelon Corporation	Disagree	Requirement 1.3 should be revised to state a "Single Senior Management Official as per the entity's registration". Exelon is concerned that as presently written, Requirement 1.3 could be interpreted that Exelon as a corporate entity would need to have one and only one "single senior management official with overall authority and responsibility for leading and managing implementation of requirements within this standard".
11.33	Manitoba Hydro	Disagree	Requirement R1 states that each Responsible Entity shall "... annually review one or more .... cyber security policies..." which implies that a entity could review a single policy in a year. If an entity developed a policy for each of the R1 sub-requirements, it would take 13 years to complete the policy review. Consider including cross references to each of the specific Requirement numbers in 1.1 to 1.13.
11.34	Southern California Edison Company	Disagree	SCE first makes the following specific comments in relation to this Requirement: (1) R1.1 "third-party personnel" is vague and needs to be more clearly defined; (2) CIP-001-1-R1 does not include provisions for emergency situations; and (3) R1 appears to exceed the

#	Organization	Yes or No	Question 11 Comment
			mandates of FERC Order 706, paragraph 355, in that a finite list of topics to include in the policy were not required by FERC.In addition to those specific comments, SCE also makes the following general comment: the contained list attempts to be too prescriptive but does not seem to be exhaustive at the level of detail that is chosen. For instance, R1.5 and R1.6 are essentially sub-components of R1.8. Policy objectives should be such that they are at a higher level and yet clearly state the desired cyber security control objective in a manner that can drive the development of procedures and tools. The drafting team should consider dividing the standards into thematic areas that require policy statements for each thematic area.
11.35	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that the Requirement R1 in CIP-011 be re-worded to change the text “annually review formal documented cyber security policies” to "annually review a formal documented cyber security policy framework that includes policies, standards, and guidelines." Not everything within the framework would be a policy.
11.36	Independent Electricity System Operator	Disagree	See response to Q9.
11.37	Allegheny Energy Supply	Disagree	Suggested Revision:”Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber Systems:”Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.38	Allegheny Power	Disagree	Suggested Revision:”Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber

#	Organization	Yes or No	Question 11 Comment
			Systems:"Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.39	EEI	Disagree	Suggested Revision:"Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber Systems:"Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. EEI suggests additional language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. EEI suggests additional language to bring clarity or removing R1 1.8.It is unclear as to the distinction between "1.9. Configuration change management;" and "1.11. BES Cyber System maintenance;" EEI suggests additional language to bring clarity or removing R1 1.11.
11.40	Alberta Electric System Operator	Disagree	The AESO suggests removing "formal, " from the proposal as it is subjective.
11.41	APPA Task Force	Disagree	The APPA Task Force agrees with the intent, but believes the following improvements should be made:What does "formal" mean? Does the drafting team intend a Company-wide Policy?Terms used in later requirements ought to be defined hereTerms that are ambiguous, such as "Boundary protection" and "media sanitization" ought to have definition boxes associated with them. In general, definition boxes should be adjacent to the term as it is first used in the standard. Alternatively, a definitions sections such as is used in typical contracts could be a new standard section for those definitions that are used only in this standard that are not included in the Glossary.It should be clarified that

#	Organization	Yes or No	Question 11 Comment
			"Personnel ..." as used in 1.4 includes external contractors.1.7 seems to encompass 1.5, 1.6 and 1.8. Consider making 1.5, 1.6 and 1.8 sub-bullets of 1.7The APPA Task Force believes that a number of the requirements listed in the tables throughout CIP-011 should be part of an overarching policy developed by each registered entity. While each utility's approach may be different, each registered entity should establish a coherent approach to cyber-security for its BES facilities. Requirement R1 should be viewed as the cornerstone of defining what is important to that utility. We believe the subsections of R1 are confusing and need clarification. Since revocation of access is common to many of the requirements The APPA Task Force believes the following Additional/Edited cyber security policies should be addressed in each entity's policy:1.2.1 Revocation of Access - Triggering Criteria
11.42	Southwestern Power Administration	Disagree	The phrase "leading and managing" is too restrictive, particularly for larger entities whose single Senior Management Official may have overall authority and responsibility, but his or her managers are the personnel who are responsible for leading and managing the details of the cyber program.1.3 Identification of a single senior management official with overall authority and responsibility for implementation of requirements within this standard;
11.43	Kansas City Power & Light	Disagree	The requirements here for a policy statement are much too prescriptive and are unnecessary. Policy statements should be global and encompassing and provide overall guidance. Recommend removal of a policy statement requirement from this proposed Standard. What purpose does this requirement serve or problem does this requirement solve? If this requirement is not included, what process or procedure will not be done in support of the remainder of the requirements? What is important are the processes and procedures that are in place to support the meat of the Standard. Mandatory and enforceable requirements are sufficient to stand alone. If a company feels they need a policy statement to support the CIP Standards, or any other Standard, let that be their decision.Do not agree with the need for requirement 1.3 regarding the need to appoint a single senior management official for overall authority and responsibility for leading and managing implementation of the CIP requirements. These requirements cover a broad

#	Organization	Yes or No	Question 11 Comment
			spectrum of systems and can engage many organizational parts of a company that one person may not be meaningful over all parts. NERC Reliability Standards compliance is sufficient weight to allow a company to determine the level of approval it needs to achieve and ensure compliance throughout an organization for CIP and any other NERC Reliability Standard.This Standard should focus on identification of cyber systems that need protection and an appropriate level of protection needed and move away from requirements that manage an organization such as R1.
11.44	LCEC	Disagree	The requirements of a formal policy should be defined.Boundary protection should be definedmedia sanitization should be definedCyber Security incident should be defined
11.45	Progress Energy (non-Nuclear)	Disagree	The term annual needs to be defined. Is it during a year, per 12 months, Jan 1 to Jan 1, 365 days, from what starting date, etc.R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.46	Michigan Public Power Agency	Disagree	The term annually is not consistently applied throughout the industry. For some organizations, this term means sometime in a calendar year, others apply it to their fiscal years. Some have applied it to mean a 12 month period based on the last event. The term either needs to be defined similarly to R3, where there is a local definitions box or the wording should be altered to remove the ambiguity.
11.47	US Bureau of Reclamation	Disagree	There are 6 "definitions" provided in CIP-011 which are needed to enforce the standards. Those 6 "definitions" need to be formally proposed as definitions in order to ensure enforceability of the standard.
11.48	Southwest Power Pool Regional Entity	Disagree	This requirement is not objectively auditable as written. Some level of explanation or direction needs to be defined to assist the entity and the auditor in a common

#	Organization	Yes or No	Question 11 Comment
			understanding of the expectation. While a simple regurgitation of the applicable enumerated (not "R") requirements is undesirable, the required polic(ies) need to state expectations in sufficient detail for the entity and its contract / vendor support personnel to understand the requirements of the policy as they pertain to implementing the standard(s).
11.49	American Municipal Power	Disagree	This requirement seems to be too prescriptive.
11.50	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
11.51	We Energies	Disagree	We Energies agrees with EEI: Suggested Revision:"Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber Systems:"We Energies agrees with EEI: Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.52	American Electric Power	Disagree	What burden of proof is needed for items 1.4-1.13 to demonstrate implementation? Would this be the same proof that would be required to prove R2-R32 have been met? Is this an instance of double jeopardy? Failure to meet an item in R2 would also mean failure to implement the cyber security policy in R1. Suggest removing "implement" and allowing the R2-R32 requirements stand as proof of implementation.To what level of detail must the cyber security policy address the items? Is it sufficient to outline how they will be addressed? Different auditors may have different levels of detail in mind. Is this meant to outline a Responsible Entities Cyber Security Policy? The majority of the

#	Organization	Yes or No	Question 11 Comment
			details for compliance will be found in the procedures, not in policy statements. Does this do anything more than demonstrate a Cyber Security culture for a Responsible Entity?
11.53	ReliabilityFirst Staff	Disagree	What does the term “addresses” in Requirement R1 mean? How does an entity “address” sub-requirements 1.1 through 1.13? Sub-requirement 1.3 needs clarification regarding the definition of the phrase “single senior management official”. Does this phrase mean one individual for an enterprise or one individual for each registered function, or either?
11.54	WECC	Disagree	While we agree with the general proposal and list, this requirement should be rewritten to more clearly indicate what is required. The word formal should be defined in this context. The level of detail required in the policies should be indicated. Suggest changing review annually to "review at least every 365 days" or to "once during the calendar year" depending on what SDT's intent is for the requirement.(1.1) The phrase,” Organizational and third-party”, is inconsistent with phrases used in other requirements. Consider utilizing the same language used to describe individuals with access to cyber systems, or simply state “everybody”. (1.3) No specific documentation is required.(1.4 through 1.13) These requirements are very vague and offer no guidance at all as to the level at which these topics must be addressed. As written this requirement provides no value whatsoever, and is essentially unauditable.
11.55	Verizon Business	Disagree	1) Revise 1.9 Configuration Change Management to two separate lines – one for “Change Management” (which would apply to procedure compliance, etc.) and one for “Configuration Management. 2) The list is too vague. The prior approach with CIP-003 identifying the specific policies needed is preferable. 3) Item 1.8, “Boundary Protection” should be defined. The requirement should state whether it is consistent with the definition in NIST 800-53. 4) Revise 1.5 to read “Physical Security of BES Cyber System Components.”

12. Requirements R2 to R4 of draft CIP-011-1 concern personnel training, awareness, and risk assessment, which were previously contained in CIP-004. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Note: CIP-011-1 R2 through R4 now resides in CIP-004-5 R1 through R3.

Several commenters suggested training related to networking, hardware, software, and electronic interconnectivity was either unnecessary or inappropriately targeted to individuals who have no working knowledge of the subject. The SDT agrees, and has made the training 'role-appropriate'; meaning only individuals whose roles necessitate such knowledge must receive the training.

Some commenters suggested the awareness requirements were not clear; specifically, use of the terms "proper use", "essential", and "sound security practice" were highly subjective. In response, the SDT has removed those terms and provided a requirement that can be audited more objectively.

In addition, some commenters suggested the quarterly reinforcement timeframe was too frequent. However, the SDT believes the requirement to update security awareness material is not overly burdensome and serves the reliability benefit of getting up-to-date threat information to a wide audience of individuals who can protect the BES Cyber Systems.

Some commenters suggested the annual timeframe for training individuals was inflexible and should allow for additional time to have individuals trained. The SDT agrees and has suggested the alternative use of the phrase "at least once every calendar year, but not to exceed 15 months between training."

Some commenters suggested the requirement for photographic identification was not necessary, since it adds the additional requirement for individuals to be on site for a personnel risk assessment. In response, the SDT acknowledges the requirement for photographic identification would necessitate individuals to be physically present. However, the requirement has been modified to require identity verification only for the initial personnel risk assessment performed for each individual.

Some commenters also suggested background checks were overly burdensome by requiring entities to cover all of the locations of residents within the past seven years. The SDT appreciates these comments but does not feel an adequate personnel risk assessment can be made without such information.

#	Organization	Yes or No	Question 12 Comment
12.1	Alliant Energy		Alliant Energy agrees with EEI to strike "sound" and "essential from R2. Also, additional

#	Organization	Yes or No	Question 12 Comment
			clarity around awareness training and the term “provide” and whether that requires completion tracking. Suggestion: Use the term “distribute” instead of “provide” to remove that implied obligation for awareness training.Additionally, R3.2 is not a practical requirement. Role based training is good; however, training should be specific to the responsibilities within the BES Cyber System and should not be prescribed by the standard. What is “specified” and why is training on networking hardware and connectivity required for users/operators of BES Cyber System Components who are not network administrators. What benefit is provided by providing technical training to personnel whose core competency and job duties do not require this level of expertise or understanding?R3.5 introduces a rolling creeping calendar. Recommend changing all 12 month timeframes to either 13 calendar months or 5 calendar quarters from the previous completion to allow entities to maintain a program with an annual training rollout with the appropriate amount of lead time to be successful in annual renewal. A 12 month timeframe will create a training program that becomes administered on a user by user, day by day basis without considerations for consistent annual content updates and bulk annual renewal.R4.1 is too prescriptive and does not take into consideration personnel with access and zero need for onsite presence.
12.2	National Rural Electric Cooperative Association (NRECA)		In R4, other than performing, documenting and updating personnel risk assessments, is there anything else that is required regarding personnel risk assessments? It does not appear there is, but wanted your confirmation on that.In R4.3, please specify what "at least once every seven years" means. This needs to be made clear so there are no misunderstandings. For example, if the last assessment was done on Jan. 15, 2001, does this provision mean the next one must be completed by Jan. 15, 2008?In R4.3, if a person never had an assessment completed and they already has access to BES Cyber Systems, when must the initial assessment be completed?
12.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.R2The phrase “to ensure that personnel maintain awareness ...” should be removed from the requirement as it adds ambiguity to the requirement. Is the auditor going to measure “quarterly reinforcement” or “personnel ... awareness” or both? It

#	Organization	Yes or No	Question 12 Comment
			seems like the drafting team is trying to add an objective for the requirement. If that is the case, then consider one of two other alternatives: (1) adopt International Standards Organization format where they have an objective for each requirement introducing each requirement; or (2) develop a longer Purpose section where the purpose of each of the requirements is further embellished. This comment should be carried on to all of the requirements.What does "reinforcement" mean?R3The term "granted authorized ... access" seems to be superfluous. Authorizing and granting are two different activities and the standard seems to prohibit granting access without first authorizing access (unless under certain specified exceptions). Consider just using the term "granted" in this requirement. The confusion between the terms "granted" and "authorized" is throughout the document and ought to be clarified.Consider correlating the training requirements in R3 with whether the person is a "user" or "administrator", and whether the training is "job training", a "refresher", or "awareness", with separate levels of training frequency and content for each of these categories.3.1 should not include "procedures" since these procedures are not identified elsewhere in the standard. The word "program" should be struck from "Visitor control program" since nowhere else in the standard is there a requirement for such a program. There should be no "back-door" requirements for procedures or programs such as these.3.5 should use the term "annually" instead of "at least once every twelve months" to give entities flexibility around various business needs on when during the calendar year to hold training flexible.R4The term "granted authorized" is superfluousConsider shortening "ensure a personnel risk assessment is performed" to "perform a personnel risk assessment"
12.4	Regulatory Compliance	Agree	R2 - Awareness - please clarify what are accetable forms of awareness.R3.2 - suggestion - STRIKE the reference to networking hardware and softwareR4 - Question: How do you propose to close the gap in regards to a criminal background check of an employee who has lived outside the country for a period of time in the past seven years that may not equal the 6 month period but long enough to be involved in supicious activities?
12.5	Emerson Process	Agree	R2 and R3 do not have tables for their applicability to three impact-types of BES cyber systems. Would it be better to include the tables for consistency with the rest of the

#	Organization	Yes or No	Question 12 Comment
	Management		standard?
12.6	Northeast Utilities	Agree	Recommend that R2 be clarified to indicate whether or not documentation must be provided that awareness material was received and understood by the CIP authorized personnel.Also, it is recommended that more guidance is provided on the level of training expected under R3.2 when stating "include training on networking hardware and software and other issues of electronic interconnectivity". The clarification is important to acknowledge that the intent is clearly not to have all personnel with electronic access to any BES Cyber System to become network engineers. For example: for operations personnel, what is the level of knowledge expected concerning networking hardware and software?
12.7	Green Country Energy	Agree	Will their be any guidance, footnotes or would ANY cyber security training be acceptable?
12.8	Independent Electricity System Operator	Disagree	- Suggest changing R3.2 so that it is only required based on personnel having a role in networks, etc. An operator and other personnel do not need to know how a firewall or switch works or its software. They may need to know how to use their token for t
12.9	Reliability & Compliance Group	Disagree	: "Sound security practices" is too vague of a term. How is this going to be audited? Who will determine what a sound security practice is? There needs to be an industry standard used. Is it going to be security practices listed under NIST 800-53? What about physical security practices? Without a benchmark, how can we measure adherence to the standard?R3 is way too cumbersome the way it is written. Keep the first part of the standard written the way it is. Then start a new sentence that says, "exceptions to this requirement must be specifically outlined in the responsible entities policies and are limited to emergency situations and acceptable alternative training." The part of the standard that reads, "impact the reliability of the BES or emergency response, to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems" is just confusing to read and understand. No matter what is done, try and make this requirement more than one sentence.R3 is better than the old

#	Organization	Yes or No	Question 12 Comment
			standard in how it defines how training should be handled for different roles and responsibilities. The 12 month timeframe needs to be tightened down even further. Is that 12 months +/- one month or is it every 365 days?
12.10	USACE - Omaha Anchor	Disagree	3.2 - should be worded closer to 3.3. or 3.4. You are giving training on network hardware and electronic connectivity to everyone with electronic access. This is counterintuitive - these folks for the most part do not have a need to know. They should only be given as much information as necessary to do their job.
12.11	Luminant	Disagree	3.5 We would prefer that training be conducted annually (completed within a calendar year) to avoid the confusion of tracking multiple comliance dates. How much documentation must be maintained? 12 months? 24 months, 36?
12.12	Platte River Power Authority	Disagree	Access to "any BES Cyber System" shouldn't automatically require training on networking hardware and software or other issues of electronic interconnectivity. The training should be tailored to the individual's job junction and not based on the BES Cyber System they have access to. For example, an operator doesn't need to know the brand, model, configuration, or connectivity of the networking hardware that they're using. They need only know the proper use of the asset they've been granted access to. I would like to avoid training individuals on the interworkings of our network when they have only been granted limited electronic access.
12.13	Liberty Electric Power, LLC	Disagree	CIP-011 R2 requires quarterly training for all plant personnel in cyber security. This is too frequent, and I would suggest changing to annual.CIP-011 R4.3 repeats the error of CIP-004 concerning the word "update". There were many comments about requiring entities to have their long-time employees provide government-issued ID every "update" in the RFI, and the recordkeeping and potential for violation over trivia continues by not addressing the issue. I suggest changing the wording to define update as doing the background check again, and not getting into the realm of potential violations over lost wallets.

#	Organization	Yes or No	Question 12 Comment
12.14	E.ON U.S.	Disagree	CIP-011-1, R3.5 unnecessarily inhibits an organization's flexibility by mandating training every 12 months. E ON U.S. proposes that the Standard state "annual training", as currently required.CIP-011-1, R4 contains requirement of the Personnel Risk Assessment that should be revised. When seeking information from foreign nations concerning someone having resided in those foreign nations, compliance with these literal requirements may not be possible or feasible. An exception should be included to address a failure to obtain this level of evidence following a good faith attempt to do so.CIP-011-1, R4.3 ignores practical problems with requiring background checks of contractors and/or service vendors. Privacy concerns have raised many questions as to whether literal compliance is possible (especially in the context of this Standard which eliminates some of the language from the former CIP-004). E ON U.S. proposes that the requirement provided by the Regional Compliance Implementation Group ("RCIG") in RCIG-A-002 be adopted conceptually in this Standard.
12.15	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
12.16	LADWP	Disagree	Consultants or employees who lived abroad for a time may not be able to meet the 4.1 requirement to cover all locations where subject has resided. This could prevent proper authorization to BES systems.
12.17	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes Personnel Training, Awareness, and Risk Assessment should only apply to personnel with access to high impact BES cyber systems and not include personnel with access to medium and low impact systems. CenterPoint Energy also suggests changing R3.2 to: "For personnel having job duties that require a role in BES Cyber System networking and electronic interconnectivity, this cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems."Numbering of sub-requirements for R3 and R4 conflicts with numbering of requirements in Tables R3 and R4 (there are two 3.1 and 3.2 and two 4.1 and 4.2).

#	Organization	Yes or No	Question 12 Comment
			CenterPoint Energy suggests moving all sub-requirements for R3 and R4 to tables to be consistent with other sections in CIP-011.
12.18	FEUS	Disagree	Disagree with Comments: 3.2 requires personnel with electronic access to have training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems. Extensive training on networking hardware and software should be limited to support staff or personnel with administrative privileges. It is not clear what 'other issues of electronic interconnectivity' is?3.5 requires training to be conducted every 12 months from the date of 'initial' training. The Drafting Team should consider revising the wording to allow for training more frequent to align with a regular training schedule for more personnel.4.1 requires a seven year criminal history check covering all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. How would the Responsible Entity verify 'all locations' were identified by the subject for the criminal history check? If a subject is attending an out-of-area school via online courses it is not logical to perform a criminal background check for the location of the school.
12.19	Southern Company	Disagree	For R2, This requires the Entity to either track which personnel have access to every low-impact system or to include all personnel company-wide, including vendors and contractors, in the awareness program. A table should be added excluding low-impact Cyber Systems to parallel R3 and R4.For R3, How does "granted authorized electronic access" interact with the situation where a network service on a system is available to anyone who can get a packet to it? For 3.5, A specified 12-month cycle makes the training program much more difficult to administer without any benefit to reliability. A 14-month cycle would allow a reasonable annual training program to work.3.2 does not actually address any security need for the large majority of personnel with access. While Order 706 requires that NERC address the issue, that FERC requirement could be considered to have been met by the standards comment process without the wording making it into the final standard.Suggested rewrite of R3: Each Responsible Entity shall ensure that all personnel who are granted authorized electronic access and/or

#	Organization	Yes or No	Question 12 Comment
			authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training, when specified in CIP-011-1 Table R3 - Cyber Security Training, prior to their being granted authorized access in order to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.Temporary authorized access may be granted for specified exceptional circumstances that are approved by the senior management official identified in Requirement R1.3 or their documented delegate; for circumstances that require temporary access for emergency response; or for circumstances that would otherwise negatively impact the reliability of the BES. Suggested rewrite of R4: Each Responsible Entity shall ensure that all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, undergo a personnel risk assessment, when specified in CIP-011-1 Table R4 - Personnel Risk Assessment, prior to their being granted authorized access in order to ensure that personnel have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.Temporary authorized access may be granted, without prior personnel risk assessment, for specified exceptional circumstances that are approved by the senior management official identified in Requirement R1.3 or their documented delegate; for circumstances that require temporary access for emergency response; or for circumstances that would otherwise negatively impact the reliability of the BES. R4 is difficult to implement for the case of vendor support through remote access and for vendor support staff who are not citizens of the US, Canada, or Mexico.
12.20	Progress Energy (non-Nuclear)	Disagree	For R3 - the definitions in the box should be included as formal definitions. It is confusing with these text boxes hanging with only certain R#s.R2 contains two very subjective words: “sound” and “essential.” Suggest striking these words.For 3.1 - cyber training included incorrectly here...last bullet. Move to 3.2.4.1 First bullet comments- this new requirement appears to be a duplication of the E-Verify/I-9 process in which employment eligibility is verified for all new hires. All employers are required to verify their employees’ employment authorization and confirm that the identification documents presented are legitimate, thus establishing an individual’s identity covering

#	Organization	Yes or No	Question 12 Comment
			both the employee and contractor population. Additional verification through the PRA or requiring completion of the PRA after completion of the employment eligibility requirements adds additional steps to the process with no added value.4.1 Second bullet comments - the current regulation requires a 7 year criminal check. It does not specify that the check needs to cover everywhere the person worked or went to school and lived for > 6 months. The new language appears to be taken from a response to the interpretation given to the Army Corp of Engineers by NERC regarding how a PRA should be performed, which PE disagrees with.The current wording requires companies to gather much more data on an individual from the individual (as that is the only source of the information). Not even Nuclear attempts to gather this kind of data (everywhere worked and went to school for > 6 months) when they perform their checks. Based on historical experience, for those who have had multiple employments the information provided by the individual with regard to employment will likely not be accurate.PE suggests running a 7 year criminal history on all addresses that show up on the application or in the credit databases and then running a nationwide search to cover any other areas. An alternate to that may be fingerprint checks if utilities can be given access to the data.Either of these approaches will streamline the process.CIP-011-1 R3.1 (Cyber Security Training) - It appears that R3.1 was written with the intention of providing a level of training appropriate to job functions (language which was explicitly in previous versions) in regard to those with only unescorted physical access (such as janitors, electricians, HVAC technicians, etc); however the last bullet point 'Identification and reporting of a Cyber Security Incident' could easily be misinterpreted to be requiring training of a cyber nature rather than those of a physical nature directed against cyber assets (which I believe is the training we should be providing an individual with the aforementioned responsibilities)
12.21	Alberta Electric System Operator	Disagree	For R3.1, consider removing "and storage media" from bullet "The proper handling of BES Cyber Systems information and storage media" because information handling should be implemented regardless of the media type.For R4.1, consider changing the seven year time horizon, and make time horizon dependent on BES Cyber System impact level. For example, Low Impact could be seven years, Medium Impact five years, and High Impact

#	Organization	Yes or No	Question 12 Comment
			three years.
12.22	American Municipal Power	Disagree	I agree with the intent, but I feel there is some redundancy between requirements for training, awareness, risk assessment, etc. that should be addressed more concisely (less requirements)
12.23	GE Energy	Disagree	i) R3.2 lists a requirement for training on networking hardware for all users having electronic access. Perhaps this should only be for users with administrative access to network hardware. If this requirement is really calling out the need for VPN or similar training, this should be more specific than "network hardware".ii) Is it possible for vendors' personnel risk assessment process and records to be ratified/certified by NERC, so that individual Responsible Entities do not have to duplicate the effort for those vendors who have teams providing services to multiple REs? This would be more efficient and secure.iii) Vendor privacy issues are a concern regarding the background screens. Some clarity on the expectation between the client and vendor and the paperwork required to validate a screen, and clarity on who should actually conduct the screens would be helpful (client versus vendor). The expectation should be for the vendor to maintain their own records.
12.24	Public Service Enterprise Group companies	Disagree	In CIP v1~v3 the requirement for refresher training was "Annual", where "Annual" was understood to mean sometime within a calendar year. The new requirement of "once every 12 months from the date of initial training" implies that a daily checks are required for each person that had previously been training on whether training has expired. This imposes undue administrative overheard on Registered Entities without significantly enhancing cyber security. More flexibility is needed to accommodate vacations, illness, etc. One possibility is that training is required annually, with an up to 90 day extension for good cause or administrative efficiency.
12.25	National Grid	Disagree	In R2, National Grid recommends an annual reinforcement.Recommend that R3.2, R3.3 and R3.4 change "training" to "role appropriate training"

#	Organization	Yes or No	Question 12 Comment
12.26	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
12.27	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggested revision:R2 contains two very subjective words: “sound” and “essential.” Suggest striking these words. Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site? Make requirement for photo ID apply to physical access only.
12.28	Minnesota Power	Disagree	Minnesota Power requests that the Standards Drafting Team consider replacing the phrase “provide all” with “make available to all,” in order to ensure clarity and avoid the potential that this phrase may be interpreted to include the requirement to document that the materials were actually received by all personnel. For example, it would be difficult to document that bulletin board postings were “provided” to each individual employee.Regarding Requirement R2, “...under their security awareness program to ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems” Minnesota Power has the following comments: o What security awareness program is being referenced? The Standard does not require the creation or implementation of a security awareness program. Minnesota Power recommends removing “under their security awareness program” from the Requirement. o What are “the cyber security practices that are essential?” The way this is stated infers that there is a known list of essential practices, which are particular to BES Cyber Systems (as opposed to general IT security practices), though none are referenced. Regarding Requirement R3, Minnesota Power recommends rewording the purpose statement as follows:"Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to access being authorized as specified in CIP-011-1 Table R3 - Cyber Security Training. This training is required except in exceptional circumstances that are approved by the single senior management official or their authorized delegate and

#	Organization	Yes or No	Question 12 Comment
			impact the reliability of the BES or emergency response." In addition, Minnesota Power has the following comments regarding Requirement R3: o R3 makes reference to a delegate for the senior management official, however R1 does not allow for the ability to assign a delegate for any purpose. o The box of definitions for R3 includes definitions for "routable protocol" and "non-routable protocol" however; these definitions are not used in R3 and therefore should be removed. o Sub-section 3.1 references a visitor control program which is not defined anywhere in this requirement. In light of the Standards Drafting Teams intentions to remove the "how-to" components of these Requirements, Minnesota Power recommends removing references such as this to a "program" and replacing with a statement such as "How visitor access is managed." o Regarding sub-sections 3.2, 3.3 and 3.4, as these sub-sections are currently written, it is not clear that this training is required for those individual's with a "need to know" only. o Regarding sub-section 3.2, what is the word "specified" in "specified electronic access" referring to? Minnesota Power recommends removing this term from the phrase as it doesn't add to the meaning of the sentence. o Regarding sub-section 3.2, "training on the networking hardware and software and other issues of electronic interconnectivity" is overly broad and could be interpreted as in-depth technical training, which would go beyond the intent of this Requirement. Minnesota Power recommends the following alternate wording, "training on the cyber security policies, access controls and procedures for the BES Cyber Systems to which they have electronic access." o For sub-sections 3.3 and 3.4, Minnesota Power recommends adding a comma following "...BES Cyber System recovery," for 3.3 and "...BES Cyber System incident response," for 3.4. o Regarding sub-section 3.5, the term "This" at the beginning of the sentence should be replaced with "Each" to be consistent with the other Requirements. o Minnesota Power recommends adding a statement to Requirement 3 that the training referenced in subsections 3.1 through 3.4 can be performed in a single training session or in multiple training sessions each covering one or more of the required topics. Regarding Requirement R4, Minnesota Power recommends rewording the purpose statement as follows:"Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems,

#	Organization	Yes or No	Question 12 Comment
			including contractors and service vendors, have undergone a personnel risk assessment prior to access being granted as specified in CIP-011-1 Table R4 - Personnel Risk Assessment. The completion of this assessment is required except in exceptional circumstances that are approved by the single senior management official or their authorized delegate and impact the reliability of the BES or emergency response. This is to ensure that personnel who have such access have been assessed for risk, subject to existing collective bargaining unit agreements, in accordance with federal, state, provincial, and local laws."In addition, Minnesota Power has the following comments regarding Requirement R4: o Regarding sub-section 4.1, the use of the phrase "personnel risk assessment program" seems inaccurate. Rather, 4.1 only defines what a personnel risk assessment itself shall, at a minimum, include. Minnesota Power recommends that the term "program" be removed from this sub-section as it's not required to demonstrate compliance. o The addition of "via photographic identification documentation issued by a government agency" to sub-section 4.1 could create an unnecessary burden on Registered Entities, especially for those vendors and contractors who do not come on-site. Minnesota Power recommends utilizing the language of the current CIP-004-2 Standard and requiring SSN verification for U.S. residents and photographic identification documentation for non-U.S. residents. o In the event that Standards Drafting Team chooses to leave the language of sub-section 4.1 as is, Minnesota Power recommends that photographic verification of identity be done at the time of initial access and that it is not necessary to renew this verification every 7 years. o Regarding sub-section 4.2, what does "document the results" mean? Under the current NERC CIP-002 - CIP-009 Standards there has been some confusion regarding what a Registered Entity needs to show compliance with this type of Requirement. Does this mean keep a redacted copy of the personnel risk assessment or would logging a summary of the results (e.g., "no findings"), including dates, source of background check, etc., be adequate? The Standards Drafting Team should consider clarifying what is meant by "document the results" so that consistency can be established.
12.29	NextEra Energy Corporate	Disagree	NextEra believes that the former standard provided valuable examples of awareness training methods which should be part of this revised standard. One question that arises

#	Organization	Yes or No	Question 12 Comment
	Compliance		is how will the delivery of this awareness training be measured? The standard should clarify the requirement. Also, the standard should provide examples of exceptional circumstances under which exception from training and PRA requirements may be documented.
12.30	Garland Power and Light	Disagree	o Disagree or need clarification with 3.1 - 1st bullet "The proper use of BES Cyber Systems" What does "use" mean - The EMS control system is operated by NERC certified operators and updated / maintained by qualified technical personnel. For CIP training, what is meant by train on the "use" of this system o Clarification on 3.2 should apply only to personnel having a role specific to support services for "networking hardware, and software and other issues of electronic interconnectivity supporting the operation and control of the BES cyber systems" and should be limited to security features. Training of all personnel in these areas will reduce cyber security.
12.31	PacifiCorp	Disagree	PacifiCorp agrees with EEI's suggested revision:R2 contains two very subjective words: "sound" and "essential." Suggest striking these words. Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site? Make requirement for photo ID apply to physical access only.
12.32	Kansas City Power & Light	Disagree	Quarterly reinforcement is excessive and places an unnecessary administrative burden on Regional Entities and a poor investment of time and effort distracting from the productive work of maintaining cyber system security and integrity. Annual training is sufficient for the FERC Standards of Conduct, for important reliability functions in the EOP Standards such as black start and energy capacity emergencies, and for CIP sabotage recognition and reporting. Annual training for the personnel with access to identified cyber systems is sufficient to ensure the importance of maintaining the security and operation of identified cyber systems.R3.2 requires training that is much too detailed for personnel with access to a cyber system. Would this make sense for someone whose task was to wire in a Remote Terminal Unit for acquisition of field data into an EMS? The training specified in requirement R3.1 is sufficient for these kinds of

#	Organization	Yes or No	Question 12 Comment
			personnel. Recommend removal of R3.2.R3.5: Requiring annual cyber security training 12 months "from the date of initial training" is an unnecessary burden on the Regional Entity. It is enough provide for an annual training within a calendar year for those personnel who have physical and electronic access to cyber systems. What issue is this addressing? It is more important to focus investments of time, energy, and finances toward the actual security and integrity of the cyber systems than to support an administrative system to ensure training is done at a specific time rather than the training itself.R4.1 is too prescriptive in specifying the actions that are required to achieve the background check objectives. There may be other regulatory restrictions that prevent adherence to the prescription described here. Recommend removal of such prescription and include the language from CIP-004-2 that states to perform such checks "as permitted by law and subject to existing collective bargaining unit agreements".
12.33	Con Edison of New York	Disagree	Quarterly training is excessive for the large number of people likely to be involved. This training should be annual or at maximum twice a year. This training will get very expensive given the large number of people to be added to the training pool.
12.34	Dominion Resources Services, Inc.	Disagree	R2 - Based on the SDT's comments at the workshop, the intention of the Awareness program is not to require documentation of security awareness at an individual level. This interpretation is evidenced by the differentiation between the intent of security awareness versus the intent of security training. As defined in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program", awareness is not training. The purpose of awareness is to focus attention on security. Many of the techniques commonly used to deliver security awareness topics (e.g., posters) do not lend themselves to tracking at an individual level. On one hand, awareness topics are intended to allow individuals to recognize IT security concerns and respond accordingly and, on the other hand, training strives to produce relevant and needed security skills and competencies. The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus attention on an issue or set

#	Organization	Yes or No	Question 12 Comment
			of issues. Consequently, the SDT's intentions are correct and consistent with industry best practices. Given that the intent of this requirement is to reinforce cyber security program expectations for those personnel with access to BES Cyber Systems and not to document evidence of individual training, the following alternate wording is proposed: "Each Responsible Entity shall establish a security awareness program. The program shall provide for reinforcement, at least quarterly, on selected topics of security expectations and practices required to ensure the protection of BES Cyber Systems." 3.2 - Requirement R3.2 proposes training personnel who have electronic access to a BES Cyber System "on the networking hardware and software and other issues of electronic connectivity supporting the operation and control of BES Cyber Systems." Dominion recognizes that networking and network transport mechanisms (i.e., connectivity) involve specialized skills requiring a high level of expertise and experience. Because of the specialized nature of networking, providing this training would provide only a very limited security benefit at best, and could encourage personnel without the full qualifications and experience necessary, to take actions affecting network connectivity that would adversely impact the reliability of the BES. Based on Paragraph 434 of the Directives in FERC's Order No. 706, the Commission's intent was only that training programs encompass this training, not that any individual who has electronic access to a BES Cyber System receive such training. This requirement should be removed.3.5 - The change from annual to 12 months appeared to cause some confusion at the workshop and does not provide for a grace period (e.g., 12 months plus or minus a month to allow for shift workers and emergencies). Dominion requests that the SDT consider returning to using "Annual" and define how annual is to be used for these standards. Dominion prefers that "Annual" be defined as "12 months plus or minus a month" since this provides some flexibility in completing the task and also allows the Responsible Entity to not be forced into 11 month cycles so as not to miss a 12 month deadline. For example, Dominion had a training session set up for certain field personnel. The night before the meeting, a storm came through the system and caused enough damage that the meeting had to be cancelled because everyone was needed for restoration activities. The logistics involved in setting up these training sessions are often complex and a grace

#	Organization	Yes or No	Question 12 Comment
			period would provide the flexibility for rescheduling without compromising the spirit or intent of the training objective. Dominion understands that the "12 months plus or minus a month" definition is being used throughout the nuclear industry. Dominion suggests the following alternate wording for R3.5:"Initial training shall be conducted prior to granting access to BES Cyber Systems. Re-training shall be conducted annually."R3.5 contains requirements that are not identified in Table R3. All requirements should be contained within the associated table. Please see Dominion's response to Question 9. 4.1 - With inclusion of the nuclear plants, time horizons for personnel risk assessments are shorter than currently required by the standard. For example, Nuclear does background checks for unescorted access authorization every 5 years. Since they are done every 5 years, they do not check history for the last 7 years. To accommodate this difference, which effectively exceeds the requirements of this standard, it is recommended that the language in the 2nd bullet of R4.1 be revised to read:R4.1 o A criminal history records check initially and at least every 7 years thereafter, covering all locations where, during the time from the last check to the current time, the subject has resided . . .
12.35	Southwestern Power Administration	Disagree	R2 - Replace "shall provide" with "shall make available to" to clarify that the Responsible Entity must make quarterly awareness available, and not document that all personnel have reviewed and understand the awareness material.R3 & R4 - what would be an exceptional circumstance that would warrant training exception and/or investigative exception from the senior manager for personnel who are granted authorized electronic access and/or authorized unescorted physical access? If this is where the SDT is attempting to replace the previous "Exception to Policy" requirement, the placement of that language in R2 and R4 may need to be revisited, as these requirements seem to focus only on managing controls for personnel that DO have authorized access rights - not emergency personnel or non-authorized personnel access in emergency situations.R3.2 - This requirement is ambiguous in its inclusion of the phrase "other issues of electronic interconnectivity" A better approach would be to list the minimum coverage or topics to be covered. R3.5 - The requirement can be interpreted to read that everyone with authorized access will have to be trained exactly 12 months from his or

#	Organization	Yes or No	Question 12 Comment
			her initial training date. This would cause the responsible entity to be continually training and tracking staggered dates and creates an overly burdensome documentation effort, leading to the opportunity for mistakes and missed course deadlines. It is much more efficient and advantageous to do annual training in a group format. A better approach would be to state: "The Responsible Entity shall maintain documentation that such cyber security training is provided or offered once every 12 months, and documentation that personnel having authorized electronic access and/or authorized physical access to BES Cyber Systems have completed such training within 60 calendar days of such training being offered."
12.36	Ameren	Disagree	R2 - Without examples of what minimally constitutes reinforcement, this requirement will be problematic to audit. Would oral reinforcement count and how would you document that? Give examples such as posters, emails, events, or meetings would at least give an indication of the need to document evidence of the reinforcement taking place. A quarterly review seems extensive and an administrative burden. Once or twice per year should be sufficient.â€,â€,The bullets under R3.1 and R4.1 should be numbered as sub-requirements so that they can be cross referenced for audit purposes, i.e. R3.1.1 or R4.1.1 etc. Using the same numbering in the tables and in the requirements is confusing. The tables should use letters or roman numerals so they would not be confused with the sub-requirements indexing.
12.37	EEI	Disagree	R2 contains two very subjective words: "sound" and "essential." EEI suggests striking these words.For R2, This requires the Entity to either track which personnel have access to every low-impact system or to include all personnel company-wide, including vendors and contractors, in the awareness program. A table should be added excluding low-impact Cyber Systems to parallel R3 and R4.
12.38	Allegheny Energy Supply	Disagree	R2 contains two very subjective words: "sound" and "essential." Suggest striking these words.

#	Organization	Yes or No	Question 12 Comment
12.39	Allegheny Power	Disagree	R2 contains two very subjective words: “sound” and “essential.” Suggest striking these words.
12.40	Constellation Power Source Generation	Disagree	R2 states quarterly reinforcement in sound security practices under their security awareness program. This may be training, but it does not have to be, as stated in the CIP V4 Workshop. However, this requirement as written does not seem to be auditable. How can an entity prove that an email/screensaver/poster/meeting meets the reinforcement stated in the requirement? Further clarity is needed, either within the requirement or in a guidance document.
12.41	Madison Gas and Electric Company	Disagree	R2, We would propose replacing the terms “provide all” with “make available to all”, as we are concerned the word “provide” could be interpreted to include documenting that the materials were actually received by all personnel. For example, it would be very difficult to document that bulletin board postings were “provided” to each individual employee.Within R3 and R4 there is an exception of “except for program specified exceptional circumstances “ that is modified with the phrase “and impact the reliability of the BES or emergency response” (R3 only), please clarify. Is this exception giving the single senior manager the ability to wave cyber security training in the event that a non trained person is required to accomplish a task that they alone have the skill set for completion of said task (ie, a software engineer associated with the company that designed your SCADA system)?R3.1, The first bullet states “The proper use of BES Cyber Systems” and should be deleted since that is assumed as stated within the actual requirements of R3.1. The intent should be that training should be focused on protection of the BES Cyber System not how the particular BES Cyber System works, Please clarify.R3.2, The word “specified” is used and is not understood. Please clarify. If this is to mean additional training outside of the training within R3, than please “specify” that the entity shall have additional training program (module) for “specified” training that is not covered by R3. Please clarify if this is the required training differences between users and system administrators?The following requirements do not include a table of Low Impact, Medium Impact and High Impact (where the word “required” is

#	Organization	Yes or No	Question 12 Comment
			used under each column):R2R3.3R3.4R3.5R4.3Is this to indicate that all Entities must comply with these requirements whether or not they have BES Cyber Systems? Please clarify?
12.42	LCEC	Disagree	R2. The reliability benefit statement should not be included within the requirement section. This would be better positioned under the purpose section of the standard where it does not add confusion to the specific requirements that are being audited. The ISO27001 standards include an "objective" statement for each set of security controls which adds clarity and serves as a good best practice example.What is meant by reinforcement? How will this be demonstrated to an auditor?What is meant by sound security best practices? How will this be demonstrated to an auditor?R3 Remove or rewrite all content in the first paragraph after Table R3 - Cyber Security Training. The intent of this is unclear and very confusing.Split performance and program requirements into separate requirements for ease of auditing. If there is a requirement to have a program it should reside in its own requirement. Ref bullet 3 3.1Personnel with electronic access need to have an understanding of the risk associated with interconnectivity not necessarily the specific hardware involved. Personnel with the ability to change hardware configurations should have an understanding of hardware, software and interconnectivity impact.Training requirements should be tailored to user versus administrator and job based versus.The table should include the full range of requirements, like Table R5, and if not applicable should explicitly state that, not through blank cells. This leads entities to interpret that no training is required for these systems.4.2 in the table R4 should read unescorted physical access.
12.43	US Army Corps of Engineers, Omaha Distirc	Disagree	R2. meaning of quarterly reinforcement is vauge seems like it could be difficult to maintain audit records. 3.2 All users with electronic access do not need to know or understand networking hardware and software. Such information is usualy limited to those who support the network/system and have a need to know.
12.44	CWLP Electric Transmission, Distribution	Disagree	R2. Quarterly reinforcement training of cyber security practices seems excessive. This could be reduced to an annual obligation consistent with the training obligation in

#	Organization	Yes or No	Question 12 Comment
	and Operations Department		requirement 3.5. R3.2. This appears to require training on all systems connected to the BES, not just the specific system a user may require access to. A user accessing a server, PC or relay should not require training on network devices such as switches, routers, etc. This should be limited to requiring training on the specific area of the BES Cyber system the user is utilizing. R3.3. Similar to R3.2 this requirement should provide wording specifying that the training obligation is limited to the specific role the user has in regards to the Cyber System. R4. Requires a definition of “Electronic Access”.
12.45	Consultant	Disagree	R2. Suggest deleting the word "all" as redundant.R2. Suggest deleting the words "practices under their security awareness program". The requirement should be for dissemination of security information, not to create a program.R2. Change the words "that are essential to" to "associated with". Essential is a subjective term.R2 - R3 This is an example of where the insertion of 'local definitions' makes reading the requirement text difficult. Also, "For the purpose of this standard" is unnecessary and essentially not true. If the term is defined in the standard it is expected to be included in the next update to the NERC glossary, as that is how terms get in the glossary.General Comment- the term "and/or" is bad grammar. The word "or" is all that is necessary.R3 - Suggest deleting the word "all" as it is not consistent with the requirements identified in Table R3.R3 - This is three requirements and an objective statement stuffed into one convoluted sentence.R3[-1] shall ensure personnel complete training prior to be being granted access as required in the Table.R3[-2] personnel under this requirement includes employees, contractors, and service vendors.R3[-3] Designated CIP Senior Manager shall approve instances where exceptional circumstances related to BES reliability or emergency situations may allow access without completed training.R3[-4] cyber security training objective is to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.-- Suggest rewriting as individual requirements for better clarity.R3.2 Suggest deleting "specified" as an unnecessary word.R3.2 Suggest deleting "any" as it is not consistent with the requirements in Table R3. Training is not required for "any" access, only for those systems identified.R3.2 Suggest specifying the training is for the security aspects of "networking hardware and software and other issues of electronic interconnectivity" not training on installation,

#	Organization	Yes or No	Question 12 Comment
			programming, or other aspects of these components.R4 - Suggest deleting the word "all" as it is not consistent with the requirements identified in Table R4.R4 - This is three requirements and an objective statement stuffed into one convoluted sentence.R4[-1] shall ensure a personnel risk assessment is performed prior to be being granted access as required in the Table.R4[-2] personnel under this requirement includes employees, contractors, and service vendors.R4[-3] Designated CIP Senior Manager shall approve instances where exceptional circumstances related to BES reliability or emergency situations may allow access without a completed personnel risk assessment.R4[-4] cyber security training objective is to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.Suggest rewriting as individual requirements for better clarity.R4 - "assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements." The personnel risk assessment is not performed in accordance with "federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements". It is performed in accordance with the Registered Entitie's policies and procedures, and should be in compliance with "federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements." Suggest modifying the wording of to clarify.Wording between R3 and R4 is inconsistent. R3 - completed security training & R4 - personnel risk assessment is performed. Suggest consistent wording as completed security training & completed personnel risk assessment. R4.1 suggest deleting the word "program" as unnecessary. It is the personnel risk assessment that has the specified identity check & background checkLogically, the topic in R3 should precede R2. It would seem to make more sense to grant access prior to providing security awareness on that access.Likewise, the topic R3.4 should precede R3.3. It would seem to make more sense to respond to an incident prior to recovery from an incident.Clarify annual for review of the policies, and for training. Suggest using the regulatory basis of over 30 years from the nuclear industry in dealing with periodicity for defining these periodic timelines. Should probably be a definition in both new standards to relate to periodic requirements.

#	Organization	Yes or No	Question 12 Comment
12.46	Western Area Power Administration	Disagree	R2: Please clarify whether "all personnel" includes "contractors and service vendors".R2: Please clarify what is meant by "reinforcement" required quarterly.R2: Needs some language clarifying intent. Does authorized electronic access = unescorted physical access? If so, this has major ramifications for support.R3: Requires the Responsible Entity to ensure that contractors and service vendors complete cyber security training - it does not specify that they must complete OUR training, just that they can provide proof of training that includes the specifics of R3.1. Is this the correct intent?R3.2: This requirement is too vague. What training on networking hardware and software are required? Is the intent to have training on the various forms of electronic access (VPN, dial-up, direct connection to equipment with a laptop or other diagnostic tool, etc.)? Is it directed at users like dispatchers who connect to the system via a console or workstation? All of the above? Each category of electronic access would have different training requirements.R3.3: Does this requirement specifically relate to disaster recovery/COOP/Business Resumption Plan? Would it also include training for field staff doing repairs on specific systems? Will we have to document all of the training they receive, including training on the maintenance and repair of all substation electronic equipment?R4: What is the definition of “program specified exceptional circumstances”? R4.1: Why are we changing to photographic versus finger printing? Photographic is easily fooled.R4.1: Would an entity be responsible for maintaining the results of a 7 year criminal check for outside entities having physical access (foreign utility workers, vendors, contractors, etc.)? If the other entity is also a NERC defined CIP applicable entity, is verification by that entity that the employee is properly vetted satisfactory? This is sensitive information that other entities may not be able to divulge due to local, state or national laws.
12.47	Southwest Power Pool Regional Entity	Disagree	R3 and its included requirements should be clarified to require training appropriate to the roles and responsibilities of the recipients. It is likely inappropriate to train a janitor or security guard with physical-only access on the proper use of BES Cyber Systems the same way a person with electronic access would be trained. Similarly, it is likely unnecessary to train a vendor support staff with only remote electronic access on the

#	Organization	Yes or No	Question 12 Comment
			physical access controls and visitor control program. 3.2 requires training for personnel having "specified" electronic access. What is "specified" electronic access? Additionally, it is likely not appropriate to train a dispatcher/operator on networking hardware, software, and connectivity issues, although they have electronic access. Greater granularity or assignment of responsibilities to roles may be necessary. 3.5: is the 12-month requirement a hard 12 months? Or is there some grace period permitted, such as +/- one month, to avoid calendar creep? And, does the 12-month timer reset with the completion of the latest training received or is the expectation that the training is actually performed approximately the same time every year regardless of any training that might be completed at a different time of the year? Additionally, rather than specifying the "date of training" shall be documented, consider using language similar to "[t]he responsible entity shall maintain documentation demonstrating that the required cyber security training is completed at least once every 12 months." Let the entity determine what is necessary to demonstrate compliance. R3 Overall, consider requiring a minimum expectation as to the quality of training. For example, should there be some sort of post-training assessment to determine if the recipient understands the course material? 4.3: Consider clarifying the requirement to "...update each personnel risk assessment within seven years of the previous personnel risk assessment" and make it clear that in this instance the requirement is from the actual date of the previous personnel risk assessment, not "in the same calendar year" or "+ / - some grace period."
12.48	The United Illuminating Co	Disagree	R3. Introduction is a run-on sentence with clauses nested within it. It is unduly confusing. I would reword for the SDT, but I can not understand the clausa relationships.R3.1 to R 3.4: There are employees who will require training in 3.1 thru 3.4. This amount of training could cover multiple days separated by periods of time. The requirement does not allow for General training on one day, Vyber incident response with the response team on another day, and training in backup restoration with a third team on a different day. R3.2: What specified electronic access triggers this requirement? Electronic access is not synonymous with remote electronic access, so what is being directed with this requirement. A user with a password does not require these topics. R 3.5 annual training from the initial date of training is too restrictive.

#	Organization	Yes or No	Question 12 Comment
			Union workforces are trained in groups and training schedules shift from year to year. Also a new union higher may receive an initial one-on-one training session and then be synchronized with the rest of the workforce by repeating the training in under 12 months.Suggest "once every 12 months from the date of the initial training, or the last completed training date" This will allow flexibility to reset the training date without going over the 12 months between training classes.Also request the SDT consider allowing a two month grace period in the requirement. UI suggests including a requirement for venors/contractors who provide support via remote access only (EMS/SCADA vendors). These vendors do not require training in physical access control procedures, or visitor control processes. Additionally, they often service multiple organizations and should not be required to view the same cyber security program as the BES cyner system owner employees. The suggested wording is:"For personnel requiring electronic access only training shall include at a minimum:- The proper use of BES Cyber Systems o The proper handling of BES Cyber Systems information o Identification and reporting of a Cyber Security Incident
12.49	Black Hills Corporation	Disagree	R3.1 & R3.2 does not allow for role-based training. Need to have unique numbering between sub-requirement and table references. (There should only be one 3.1 in R3)
12.50	Detroit Edison	Disagree	R3.2 requires "training on the networking hardware and software and other issues of electronic interconnectivity". Training system operators on network gear is beyond the scope of their job duties. At the Dallas workshop, the drafting team stated that this training was required by FERC order 706 paragraph 434. That paragraph also says "we clarify that our proposal discussion on this topic was not intended to suggest that personnel have training that is not appropriate for an employee's duties, functions, experience, or access level". We don't believe that FERC is requesting all personnel be trained on network gear, only that the training is appropriate to the person's job functions. System administrators and network engineers would need to have training on the network, operations personnel do not.R3.2 also requires training prior to access of any BES Cyber System which is inconsistent with table entry 3.1 which does not require training for Low Impact or Medium Impact with routable connectivity.R3.5 removes the

#	Organization	Yes or No	Question 12 Comment
			term “annual” that was used in CIP-004 and replaces it with once every 12 months. This is too restrictive. Consider an entity that has a window for training in the month of May. Requiring every 12 months would cause the calendar to creep earlier in the year so eventually the training would be moved to April. We prefer “at least once per calendar year, not to exceed 14 months between instances”. The identity verification via photographic identification required in R4.1 is too prescriptive. The standard should be the “what” not the “how”. Previous versions of CIP-004 required an identity verification with the example of SSN verification. Consider changing the first bullet to “Identity verification (e.g., Social Security Number verification in the U.S. or via photographic identification documentation issued by a government agency i.e. Federal, State or Provincial)”.Table 4.2 should only require a PRA for unescorted physical access.
12.51	SCE&G	Disagree	R3.5 12 months should be changed to annually to allow entities to utilize a "calendar year" to setup training pools to conduct the necessary CIP training. Otherwise provisions should be made to allow initial training to be conducted during the implementation period of the standard.R4 SDT should consider allowing entities to leverage PRA controls in place (i.e. Nuclear PRA process)SDT should develop requirements for entities to validate a vendor's/contractor's PRA process. This would impose the burden of conducting the administrative work for the PRAs on the contractors/vendors, while still maintaining the compliance burden with the entity.
12.52	Powersouth Energy Cooperative	Disagree	R3.5 Suggest additional consideration be given to the requirement “every 12 months from the date of initial training.” Suggest the following wording: “no later than the end of the calendar month that the 12 month anniversary of the individual’s initial or previous training falls in” or similar to extend the window to a reasonable time to allow training to be done in a schedule fashion to allow some leeway for unanticipated delays that could previously lead to non-compliance due to a hard deadline. R4. Request additional language be added to clarify the allowance of reciprocity of PRA’s between a contractor or vendor and the responsible entity. It is understood that PRA’s are an important component of proper security but due to the volume of contractors and vendors used at any given time, a mechanism for the third party to perform their own

#	Organization	Yes or No	Question 12 Comment
			PRA and provide assurance that the PRA meets the requirements of the registered entity in both substance and time requirements will reduce cost and complexity greatly.
12.53	American Electric Power	Disagree	R3: In regards to "are approved by the single senior management official identified in Requirement R1 or their delegate and...", does this statement add any benefit to security? Is a senior manager or delegate's approval needed each time an emergency situation is declared?3.2, 3.3, 3.4: This is an attempt at role based training. Would it be better to combine 3.2, 3.3, and 3.4 together into a single requirement? Suggested wording: "The cyber security training must be role based for personnel that are users, administrators, responsible for system recovery, and responsible for responding to or investigating cyber security incidents of BES Cyber Systems."3.5: Regarding "conducted at least once every 12 months from the date of initial training", will this result in a date backup? Does an entity need to keep the initial date of training for all users? Does it seem feasible to still have the initial training records 20 years down the road?If training is completed on 6/30/2011, would it need to be completed before 6/30/2012? If it was then completed on 4/15/2012 would the next date of training be before 6/30/2013 or before 4/15/2013?Suggested wording: "at least once every 12 months from the last completed training date".
12.54	ISO New England Inc	Disagree	Recommend rephrasing R3 so that is clear that the Entity does not need to list all potential emergency responseTraining should be on policy, procedures, standards, and process and how to conduct oneself. Training should not be on networking,hardware,software. Companies have personnel that have the background in each function that are subject matter experts. That is there job and should not need to be trained each year on it since that's what they do every day. For R3 there is a sub requirement 3.2 and then another requirement in table 3 numbered 3.2 this can confusing.R3.2 in table 3 please defined what is meant by external connectivity. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?For R4 there is a sub requirement 4.2 and then another requirement in table 4 numbered 4.2 this can confusing.R4.2 in table 4 please defined what is meant by external connectivity. External to BES Cyber

#	Organization	Yes or No	Question 12 Comment
			System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?The term "annual" should be replaced with the phrase: "no fewer than X (e.g. 9) months, but no greater than Y (e.g. 18) months". The time duration in "X" and "Y" should be clarified by the Standard Drafting Team, taking into consideration the appropriate level of exposure the time duration would provide. This phrase would provide Registered Entities with flexibility within any given calendar year to accomplish the prescribed action, but at the same time restrict companies from taking action in December of one calendar year, and then again in January of the next. This should be done to all the section that have 12 months. Scenario...In 2010, we roll out the training on June 1.Person A, who has access to CCAs, completes the training on June 15. In 2011, we roll the training out again on June 1.Person A, who has access to CCAs, completes the training on June 25. Under the new language, it could be interpreted that Person A has been out of compliance for 10 days if access was not revoked.The following are items we have in our training today, that will become requirements under the new standard: o Visitor control program (R3.3.1) o Identification and reporting of a Cyber Security Incident required(R3.3.1) o Recovery - note, this was required, but the language is more specific here (R3.3.3)The following are new requirements that will impact the training programs: o Training on networking hardware and software and other issues of electronic interconnectivity (R3.3.2) o BES Cyber System incident response action plans and procedures (R3.3.4)
12.55	Hydro One	Disagree	Recommend rephrasing R3 so that it is clear that the Entity does not need to list all potential emergency responses.We were wondering if the intent of R3.2 is to prevent access to a launch point for a multi location attack. (i.e. why limit the physical access to only sites with external connectivity?)
12.56	Northeast Power Coordinating Council	Disagree	Recommend rephrasing R3 so that it is clear that the Entity does not need to list all potential emergency responses.Recommend that R3.2, R3.3 and R3.4 change "training" to "role appropriate training".

#	Organization	Yes or No	Question 12 Comment
12.57	ERCOT ISO	Disagree	Recommend the following be more clearly stated as an exception: “except for program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response”. R3.1: Consider: This cyber security training shall cover these requirements as well as policies, access controls, and procedures developed for the BES Cyber Systems, and include, at a minimum, the following required items: R3.2. Please clarify the intent of “training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems”. Examples of curriculum would help. R3.5. The requirement does not address retaining records of completion of initial training. R4: Recommend that “except for program specified exceptional circumstances that impact the reliability of the BES or emergency response” be addressed more clearly as an exception.R4.2. Consider: “Each Responsible Entity shall document the results and review of each personnel risk assessment.”
12.58	ReliabilityFirst Staff	Disagree	ReliabilityFirst is not clear on the meaning of the phrase “. . . except for program specified exceptional circumstances that are approved by the single senior management official. . .” If this is intended to cover the language of CIP-003 Requirement R1.1 referring to, “. . . including provision for emergency situations.” we believe the proposed language needs more clarity. In Requirement R3.1, the use of the word “specified” is unclear as to the intent of this requirement. We believe the drafting team should add language to clearly express the intent of this requirement and, more importantly, the intent of the word “specified”. Regarding Requirement R3.5, please provide guidance on the phrase, “once every 12 months”. For example, if an individual is trained on December 1st one year, can the individual receive the training on December 12th the following year and still be in compliance? Regarding R2, there is no documentation of implementation required, making auditing of the requirement impossible. A requirement to document the quarterly reinforcement is needed. Also regarding R2, a “security awareness program” is mentioned, but not required here or elsewhere and should be added.

#	Organization	Yes or No	Question 12 Comment
12.59	Constellation Energy Control and Dispatch, LLC	Disagree	Remove the phrase "sound security practices" or identify and define what the phrase means, i.e. sound security practices as defined in the cyber security policies.
12.60	BGE	Disagree	Remove the verbiage “sound security practices” or identify and define what this means.
12.61	US Bureau of Reclamation	Disagree	Requirement 2: Agree, but requirement should emphasize Program first then quarterly awareness refreshers.Requirement 3: AgreeRequirement 3.1: Agree, but revise "at a minimum" to "in addition" in the introductory statement.Requirement 3.2: Disagree. The requirement for network training should not be applied to everyone with logical (electronic) access, only to those who administer network and/or system administration. As written, this requirement could be taken to apply to operations staff (operators) with access to operations consoles. They do not need network training. Further, what is "specified network access." Requirement 3.3: Agree. Role-based training is probably a good idea, but this might be handled with a general statement.Requirement 3.4: Agree, see above.Requirement 3.5: Agree, but there should be some tolerance so that there is no date creep.Requirement 3 (in Table): The requirements R3 and R4 include tables which are in themselves requirements. Since the numbering system is the same as other requirements, this could result in confusion with what the actual requirements are. It is suggested that Tables R3 and R4 be clarified.Requirement 4: This requirement needs to be simplified. It is wordy and confusing.Requirement 4.1: The requirement should not limit identification processes to photographic means. Fingerprints are and should be acceptable. Further, the criminal check requirement, with local information, is beyond what can normally be addressed. Suggest this check be limited to a national level only. The risk assessment process needs to specify that an adjudication process needs to be completed.Requirements 4.2 and 4.3: Agree.
12.62	Network & Security Technologies Inc	Disagree	Requirement 3.2 (training on networking hardware and software), as written, seems to require that ALL personnel with electronic access to BES Cyber Systems receive such training. This frankly makes no sense. Will SCADA/EMS operators be expected to understand the intricacies of Cisco IOS? Furthermore, it violates the principal of “need to

#	Organization	Yes or No	Question 12 Comment
			know." Suggest this requirement be reworded in a manner that makes it similar to 3.3 and 3.4 and limits its scope to personnel responsible for hardware and software.
12.63	Oncor Electric Delivery LLC	Disagree	Requirement 3.2 is not appropriately worded. Most users with electronic access to our Cyber Systems have no need to know anything about the networking hardware, software, or interconnectivity issues. The personnel responsible for maintaining this equipment may need additional training but most have required skill sets as specified by their job descriptions.Requirement R4.2 uses the term "results" of a Personnel Risk Assessment. Different auditors may interpret this term differently. We propose this to be a binary result, ie pass/fail and stated as such, for clarity.
12.64	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Requirement R2 has all BES Cyber System operators to have a security awareness program that will maintain cyber security practices. However Requirement R3, R5 and R6 exempt Low Impact BES Cyber Systems. How can an Entity begin a security awareness program where Initial training (R3) and physical security (R5 & R6) is not required? This is very confusing.
12.65	San Diego Gas and Electric Co.	Disagree	Requirements 3.2 - 3.4 in CIP-011-1 seem to imply that a Registered Entity must have a separate training program for these three subjects. Unless the requirement is intended to be that prescriptive, SDG&E recommends a single training requirement that addresses the requirements in R3.1 - 3.4. This will help make the training requirements more manageable.Attempting to split hairs between training requirements for physical and cyber access to BES Cyber Systems for Medium and High Impact systems seems to unnecessarily increase risk exposure for a Registered Entity and complicates the process and controls needed to meet R3 and R4 of CIP-011-1.
12.66	Southern California Edison Company	Disagree	SCE requests clarification on the scope of R3.1. This requirement requires people listed on Table 5 (those with physical or electronic access to "high impact BES system[s]" to receive training on the "proper use of the BES cyber system". This requirement as currently written is unclear whether the training requirement only applies to people who work with affected systems, or whether the requirement more broadly applies to

#	Organization	Yes or No	Question 12 Comment
			everyone who is permitted unescorted physical access to a PSP. If it is the former, then SCE believes that would be the correct application of this rule. However, if it is the latter case, then persons who are granted unescorted physical access rights to a PSP, but who do not themselves operate these systems (for example, CIP-cleared security guards), would have to receive training on the "proper use" of the protected system. Such training should only be required of individuals who actually work with protected systems, and not to everyone who has unescorted physical access rights to a PSP.SCE also seeks clarification on Requirement R2. As written, R2 requires quarterly "reinforcement". The drafting team should clarify the distinction they imply by using the term "reinforcement" rather than "training" as used in R3. Finally, SCE ask for clarity on Requirement R3. As written, Requirement R3 seems to allow for exceptions in the training requirement. The drafting team should clarify why an "organizational infeasibility" is being allowed while a structured method to seek technical feasibility exceptions is being eliminated. Both conditions create a situation where strict compliance with the standard is impossible to implement.
12.67	Progress Energy - Nuclear Generation	Disagree	See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
12.68	Idaho Power Company	Disagree	Sub requirement 3.2 is too broad. Dispatcher/operating personnel who have electronic access via an EMS application would not need training on networking hardware and software but it would be appropriate for EMS support staff. Cyber security incident identification and reporting would be sufficient for Dispatch/Operations personnel.
12.69	APPA Task Force	Disagree	The APPA Task Force agrees with the changes proposed by MRO-NSRS to replace "provide all" with "make available to all." We also believe the term "reinforcement" is not a defined term and should be replaced with "awareness material." As stated in our response to question 11 above, it is important to reference the required policies under requirement R1.If the drafting team does not follow Objective format suggested in response to Question 10, the APPA Task Force recommends the following format:R2.

#	Organization	Yes or No	Question 12 Comment
			Objective:Personnel Training, Awareness, and Risk Assessment: To ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems. R2. Requirement:Each Responsible Entity shall make available to all personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems at least quarterly awareness material in sound security practices under their security awareness program. The security awareness program will be part of the policy developed under requirement R1.The APPA Task Force cautions the drafting team on using the terms “grant” and “authorize” interchangeably. The following is our recommended revision to R3 with the Objective removed from the requirement:R3. Objective:To ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.R3. Requirement:Each Responsible Entity shall ensure all personnel who are granted electronic access and/or unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being authorized access when specified in CIP-011-1 Table R3 - Cyber Security Training, except for program specified exceptional circumstances that are approved authorized by the single senior management official identified in Requirement R1 or his/her delegateR4. Objective:To ensure that personnel who have such access have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. R4. Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted electronic access and/or unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being authorized access when called for in CIP-011-1 Table R4 - Personnel Risk Assessment, except for program specified exceptional circumstances that impact the reliability of the BES or emergency response,
12.70	Indeck Energy Services, Inc	Disagree	The definition of Cyber System is so broad that these requirements are applied on a one size fits all basis. A control center computer system requires a different level of requirement than a substation RTU. This lends itself to differentiating the standards by function and/or functional entity. R3.2 applies IT networking requirements on the operator who logs in to use the functionality, without any ability to program it. The term

#	Organization	Yes or No	Question 12 Comment
			"specified electronic access" is overly broad.
12.71	Manitoba Hydro	Disagree	The meaning of "quarterly reinforcement" is unclear. Consider whether Requirement R3.5 should refer to "Each Responsible Entity", rather than "This Responsible Entity". Requirement R4 appears to be missing the explicit requirement that access would be prohibited based on the negative or poor results of a personnel risk assessment; it just speaks of a personnel risk assessment being required. The structure of Requirement R3 and Requirement R4 is confusing and needs to be corrected. As written, the Table CIP-011-1 R3 applies to each of the sub-requirements, which may not meet the intent of the requirement - how does Table 3 item 3.2 for physical access relate to Requirement 3.2 for electronic access? What does "specified" mean in Requirement 3.2? The duplicate use of the same numbering of the requirements and the table items is very confusing. The format of requirements together with the use of tables for R2 to R4 should be consistent with the rest of the proposed standard. Manitoba Hydro agrees that cyber security training is not a standard requirement for all personnel who have unauthorized physical access to Low Impact BES Cyber Systems, and therefore is not auditable. We do not agree that training is not a requirement for personnel who have authorized electronic access to Low Impact BES Cyber Systems, and suggest that it be an auditable requirement.
12.72	WECC	Disagree	The new way these requirements are written is very confusing. Too many levels, sub-levels, bullets and tabled criteria. Please simplify. Consider replacing with a requirement for Training and Awareness program that addresses the criteria that the SDT feels is critical for security and reliable operation of BES Cyber Systems.Regarding the phrase, "all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors", consistent language should be used through the standards. It may be useful to create a term for this group of people, define it, and use it in place of this long phrase.The last half of the requirement sentence lacks clarity. It is difficult to understand what is being required. If the intent is to create an exception process for training, the text should be removed. Standards should not have exceptions written into

#	Organization	Yes or No	Question 12 Comment
			them; they should establish a high bar of excellence.(3.1) “Visitor control program” needs definition or explanation.(3.2) The training requirements in this sub requirement seem vague.(3.3) Regarding the reference to “Systems;” most controls apply at the device level, and therefore should be required at that level.(3.5) Time intervals need to be clearer and well defined.(Table R3) Why no training for low impact systems? Seems arbitrary.
12.73	Bonneville Power Administration	Disagree	The objectives of these requirements (“to ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems,” “to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems,” and “to ensure that personnel who have such access have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements”) should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action(s) that the Responsible Entity must take.R3: Exception is somewhat confusing. In particular, is "or emergency response" an alternative to "...are approved by..."? In other words, it could be read that exceptional circumstances require either approval or an emergency. However, it could also be that the "or emergency response" is an alternative to "impact the reliability..." It appears that the former is more likely, but the reader should not have to parse the sentence to get there. Some selected bulleting would help.Suggested rewrite of R3:Recommended Changes - Objective 3 - To ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems. R3. The Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, have completed cyber security training prior to their being granted authorized access when specified in CIP-011-1 Table R3 - Cyber Security Training, except for - Program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the

#	Organization	Yes or No	Question 12 Comment
			reliability of the BES, or - Emergency responseThis assumes the first interpretation of "or"3.1 is acceptable3.2 Needs clarification, as it is not clear what the intent is. In a non control center environment, persons who have electronic access to BES Cyber Systems often do not have nor require knowledge or training in networking hardware and software. They make electronic connections and use their electronic access to collect electrical system information such as fault data, monitor device functions or do electrical systems analysis. It is not their job to understand networking.R3.3 and R3.4 are acceptable.R3.5 requires that training be conducted, but does not specifically require that every individual complete it. Also, it addresses the first annual training, but doesn't clearly stated what to do afterwards. The intent seems to be that each person complete training within each year. In other words, if the initial training was on July 1 2010, then training would be needed sometime in 2011 (say September), some time in 2012 (January?) and so forth. As currently written, a separate 12-month clock would be needed for each person. Finally, it's not clear if the required documentation is for the initial training, the annual training, or both. The SDT should be very specific as to what it means for how frequently an individual must take cyber security training. Suggested rewrite: Rewrite 3.5 to address annual training only: "This Responsible Entity shall ensure that all such persons receive annual training at least once each calendar year, starting the calendar year after they are granted access. The Responsible Entity shall remove authorized access from any individual who fails to complete such training in a timely manner." This removes some flexibility from the entities, but produces an unambiguous and manageable annual training program.We believe that a new requirement, 3.6, is needed to address documentation: "This Responsible Entity shall maintain documentation of any cyber training addressed in R3 or its subrequirements, includinge the date the individual's training in completed."Header in Table R3: Doesn't address annual training: Suggest "Cyber Security Training is Required Prior to Obtaining and For Continued:"R4: Has the same issue with the intent of "or emergency response" that R3 has. We suggest the same solution.The way that R 3.5 is written, it appears that two things must be done: the Responsible Entity must maintain documentation and each individual who is required to take cyber security training must take it as specified.

#	Organization	Yes or No	Question 12 Comment
			Would a violation of R 3.5 be due to an organization not maintaining documentation or due to an individual not having taken the required cyber security training in a timely manner? Or could there be two violations of R 3.5 - one for an organization not having up-to-date documentation and one (or many) for an individual(s) not having taken the required cyber security training in a timely manner? There is no indication in R 3.5 what should happen if an individual does not take the cyber security training as and when required. Should that individual's electronic access and/or unescorted physical access be revoked until the cyber security training has been completed? Or is what is important here only that the documentation be maintained regardless of whether each individual takes the cyber security training as and when required?For large organizations with a thousand or more people that must take cyber security training, is it possible that R 3.5 could indicate those organizations can provide the cyber security training during specific times of the year (say within a 3-month window) without regard for each individual having to take the training at a specific time? In this case, there would be no violation in an individual did not take the training exactly 12 months apart (or whatever the time requirement is) if the individual took the training within the 3-month window in each of two years.
12.74	Exelon Corporation	Disagree	The quarterly reinforcement requirement as spelled out in CIP-004 R1 Versions 1 through 3 is more specific and should be continued into this version. Requirement 3.2 as currently stated could cause someone such as a control room operator using an EMS system to be required to receive training on networking hardware and software for which they have no business need to know. It also could impact job specific training that is focused on improving reliable operations, due to the loss of precious training time being used for training that is not required for their position. We would suggest including wording such as "....appropriate to personnel roles and responsibilities"Requirement 4.1 second bullet states that "a seven year criminal history check" be performed. It is not clear from the requirement as to what agencies would need to be contacted to accomplish such a check. If local Police agencies are envisioned to be part of this check, that does not seem to be a very practical approach. R4. The need to show a photo ID is unnecessary to ensure a valid Identity Verification. The methods currently used to cross

#	Organization	Yes or No	Question 12 Comment
			reference and verify identity are satisfactory. To now require photo identification provides no additional benefit but would make it extremely difficult for remote personnel since we would now need someone to personally view the original photographic document. This would eliminate the ability to electronically transmit the required information.
12.75	Duke Energy	Disagree	The reinforcement requirement in R2 is vague and is up for interpretation by auditors. The Responsible Entity should only have to prove that the reinforcement information is provided. Previously, various means to provide the information, including posters, etc. were acceptable. This should still be the case. If so, is should not be necessary to prove that all personnel read the poster. R2 is open to interpretation as to what kind of evidence is sufficient. Explicitly state that materials are sufficient. Explicitly state which levels of Impact apply to R2. Need clarification on the program exception in R3. Does this apply to electronic and physical access? Must every situation need to be accounted for in the program or may it be case-by-case? Also, Requirement R3 contains a run-on sentence that makes the requirement hard to understand. Please consider breaking this into 2 or more smaller sentences.Requirement R3.2: What is meant by "specified electronic access?" Also, the requirement is vague in that it can be interpreted that the user of a BES cyber system needs detailed networking hardware and software training, when this is not the case. The user typically needs to know that device A is connected to device B and needs to know how to use the software. Said user does not need to know that the network communication routes through a brand XYZ switch using Ethernet and that the software was written in C# and so on. Clarification needed for audits, etc.Requirement R3.3: This requirement also needs bounds. If Employee A has a role in the recovery of BES Cyber System 123 only, then Employee A needs training on action plans and procedures to cover only BES Cyber System 123.R3.4 seems to be incomplete.Requirement R3.5: Is there any grace period on the 12 months? If there were "exceptional circumstances" such as in R4? For example, what if Technician A was due for training in June and was called for emergency storm duty and missed the training as a result? For 4.1, who will keep track of photographic identification? What is BA/TOP doing for Areva evidence of photo IDs? Will we have to gather the photo ID every 7

#	Organization	Yes or No	Question 12 Comment
			years? Suggest changing 4.3 to only include the criminal history check.
12.76	Nuclear Energy Institute	Disagree	The use of the expression "authorized electronic access" should be clarified, in all requirements in this standard where used. The correct expression should be "authorized electronic administrative access." Users who have access but no authorization to perform administrative functions on a BES Cyber System Component are of greatly less concern than those individuals having administrative access. Performing, as required by R4.1 a seven year background check, on each individual with non-administrative access to a Component is inappropriate. The focus should be on individuals who would pose a direct challenge to the system's reliable operation. An alternate solution may be to define "authorized electronic access" in the "Definitions" section.
12.77	FirstEnergy Corporation	Disagree	Though role based training is appealing, this activity is difficult to manage and maintain. It becomes administratively difficult to develop, maintain and track different training programs. A better approach would be having training that is differentiated by access (e.g. logical vs. physical.)For R3.2 qualifications should be made for only those people responsible for supporting networking hardware and software. There is no valid reason to provide networking training to non-networking personnel.If 3.3 and for 3.4 remain: Replace '...having a role...' with '...responsible for...'. Training for recovery plans and incident response is fundamentally different than the general cyber security training and should not be rolled into a 'one size fits all' training requirement.More clarity is needed on identity verification, how often does it need to be checked, does a copy need to be retained.
12.78	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
12.79	We Energies	Disagree	We Energies agrees with EEI suggestion: R2 contains two very subjective words: "sound" and "essential." Suggest striking these words.
12.80	GTC & GSOC	Disagree	We recommend removing the word "all" in R2 to ensure that you do not have to track

#	Organization	Yes or No	Question 12 Comment
			and document reinforcement for each and every individual. We also recommend that R3.2 "For personnel having specified electronic access to any BES Cyber System" be clarified to identify to what "specified" access this is intended to apply.We recommend R2 through R4 should distinguish between the different types of users and administrators that have different responsibilities and access and therefore need different levels of training.R4 needs to be revised to better reflect the limitations of performing background checks on persons who have resided even briefly in foreign countries.
12.81	Xcel Energy	Disagree	We think R2 should be clarified to note that wide-distribution information such as company newsletters or e-mails satisfy the quarterly reinforcement requirement and that tracking on an individual basis is not required.
12.82	MRO's NERC Standards Review Subcommittee	Disagree	We would propose replacing the terms "provide all" with "make available to all", as we are concerned the word "provide" could be interpreted to include documenting that the materials were actually received by all personnel. For example, it would be very difficult to document that bulletin board postings were "provided" to each individual employee.
12.83	The Empire District Electric Company	Disagree	We would propose replacing the terms "provide all" with "make available to all", as we are concerned the word "provide" could be interpreted to include documenting that the materials were actually received by all personnel. For example, it would be very difficult to document that bulletin board postings were "provided" to each individual employee.
12.84	Entergy	Disagree	Wording in R2 is very awkward. Language needs to be written more concisely to show that awareness modules simply need to be disseminated. Current language allows for misinterpretation. It could be assumed that evidence to prove that modules have not only been disseminated but have also been received by appropriate personnel is required. The language incorporated into R3 for emergency provisions is similar to that found in CIP-003-3, R1.1, but seems to be restrictive to only cyber security training and personnel risk assessments in R4. These emergency provisions (which should be approved by the Senior Manager or Delegate) should continue to be allowed for all

#	Organization	Yes or No	Question 12 Comment
			standards/requirements, if a potential impact to emergency response or the BES subsists. Efforts to add newly created topics to the cyber security training module should be minimal. R3.5 adds clarity by replacing the word "annual" with "every 12 months". CIP-011, R4 is largely unchanged from CIP-004-3, R3. Criteria for an acceptable personnel risk assessment appears to be more lenient and allows for identity verification via a government-issued photo ID, as opposed to the social security check that was required for v3. Language is a little unclear as to which types of government-issued IDs are permissible. Are government-issued IDs from different countries (Mexico, Iran, etc.) acceptable? Additional specificity is needed.
12.85	Verizon Business	Agree	For section 3.1, "Escort Management:" should be a required item for the Cyber Security Training. In paragraph R4, the first sentence should be revised to read as follows (bolded is added text): "Each Responsible Entity shall ensure a personal risk assessment is performed and reviewed and approved by the Responsible Entity for all personnel…." 4.1, First Bullet – This could refer to the requirements of U.S. Form "I-9" for verification to work in the U.S. By passing the requirements of I-9, one satisfies this CIP-011 requirement. In paragraph 4.2, the requirement should be amended to read (bold is added text): "Each Responsible Entity shall document the results of each personnel risk assessment and they shall document that the results were reviewed and accepted or rejected as an acceptable risk for the Responsible Entity.

13. Do you agree with the proposed definitions for external connectivity, routable protocol, and non-routable protocol? Please explain and provide any suggestions for modification.

Summary Consideration:

While some commenters indicated support for local definitions, most commenters suggested moving the definitions to the NERC Glossary instead. In response, the SDT has moved all definitions to the NERC Glossary and discontinued the use of local definitions.

Several commenters expressed the need to bring back the concept of an Electronic Security Perimeter, because otherwise, the definition of "external connectivity" makes it difficult to determine at what point in the communication path a device is external. The SDT generally agrees with these comments and has reintroduced the definition of an "Electronic Security Perimeter" as a collection of Electronic Access Points.

Several commenters made suggestions about the use of the term "routable." The suggestions provided include more examples of routable versus non-routable protocols and the use of the OSI seven-layer network model. Others noted the term "routable external connectivity" is used, but "routable protocol" is never used. In response, the SDT has only defined the term "**External Routable Connectivity**" as follows: *"The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol."*

Commenters expressed confusion about the term BES Cyber System and requested additional guidance. In response, the SDT has added considerably more detail about the Reliability Operating Services a BES Cyber System performs along with the types of assets considered as part of the BES Cyber System.

#	Organization	Yes or No	Question 13 Comment
13.1	WECC		This should be defined at the top of the standard, dislike the definition box in the middle of a requirement.The use of external connectivity and/or enabled routable protocols to differentiate between required and non-required controls should be reconsidered. In most cases, the controls are still necessary to protect against insider threats.
13.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.

#	Organization	Yes or No	Question 13 Comment
13.3	ReliabilityFirst Staff	Agree	Does the drafting team intend to include these terms in the NERC Glossary of Terms?
13.4	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	However, this does not come up until well into the Standard. It is not clear how programmable electronic devises having no external connectivity, routable protocol, or non-routable protocol are treated. How shall programmable devises be treated when the only connectivity is on site connection to a laptop computer?
13.5	Puget Sound Energy	Agree	Puget Sound Energy would like to note that, with the widespread use of Internet Protocol (IP) as the communication protocol for the majority of Cyber Systems on the planet, if the standard is trying to be more inclusive of routable protocols than just IP, it should give some examples of others. "Routable Protocols" is an extremely technical concept, when talking about routable protocols other than IP, which could greatly impact scope, reliability, response, and overall compliance. If the standard is being specific to IP, then it should clarify that. If the standard is referencing other routable protocols than IP, then it should give some examples. (Ex: Routable protocols include, but are not limited to, IP, DecNet, MPLS, etc...).
13.6	Kansas City Power & Light	Agree	Recommend moving these definitions with R6 where routable protocol is first referenced.
13.7	Emerson Process Management	Agree	The current draft standard does away with the perimeter concept. It becomes slightly difficult in defining "internal" and "external."
13.8	LCEC	Agree	The definitions sound good but I do not agree with the use of "Required for external connectivity only" within the tables as they do not make sense most of the time.
13.9	SCE&G	Agree	The proposed definintions should be added to the "definitions table" at the front of the standard, rather than just in the boxes throughout the standard.
13.10	Allegheny Power	Agree	The proposed definitions are helpful, and should be used more extensively within the requirements to identify controls that are appropriate to devices based upon their

#	Organization	Yes or No	Question 13 Comment
			functionality/vulnerability.
13.11	EEI	Agree	The proposed definitions are helpful, and should be used more extensively within the requirements to identify controls that are appropriate to devices based upon their functionality/vulnerability.Suggested modification for R3:"Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access except for emergency circumstances that are approved by the senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response."Suggest elimination of Table R3.Suggested modification for Requirement 3.2:"For personnel that have a role in maintaining networking hardware and software supporting a BES Cyber System, this cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems" In general, the drafting team needs to account for a person's "need to know" within the training program.
13.12	Florida Municipal Power Agency	Agree	These definitions ought to be associated with the first requirement that uses the definitions. As it appears now, these definitions seem associated with R3 on training, which has nothing to do with these definitions.
13.13	Electricity Consumers Resource Council (ELCON)	Agree	We agree with the definitions but they should be applied to limit the applicability of all the requirements in the standard.
13.14	Cogeneration Association of California and Energy Producers & Users Coalition	Agree	We agree with the definitions; however, they should be applied to limit the applicability of all of the requirements in the standard.
13.15	We Energies	Agree	We Energies agrees with EEI comment: The proposed definitions are helpful, and should

#	Organization	Yes or No	Question 13 Comment
			be used more extensively within the requirements to identify controls that are appropriate to devices based upon their functionality/vulnerability.We Energies agrees with EEI: Suggested modification for R3:Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access except for emergency circumstances that are approved by the senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response.We Energies agrees with EEI: Suggest elimination of Table R3.Suggested modification for Requirement 3.2:For personnel having electronic access to any BES Cyber System, this cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems.
13.16	FirstEnergy Corporation	Agree	While in agreement with the definition of routable protocol, it does not provide enough clarity. Would like to see the definition expanded to include protocol encapsulation.
13.17	US Bureau of Reclamation	Agree	Yes, but the definitions appear in the wrong location within the Standard.
13.18	Independent Electricity System Operator	Disagree	- External connectivity needs to be defined. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?
13.19	Consultant	Disagree	1. Suggest deleting the words "for the purpose of this standard". These words are unnecessary and obfuscate the term being defined. Once the standard is approved these terms should be added to the NERC glossary as part of the next update process for that document.2. The term being defined should be capitalized, as it is now a defined term.3. Suggest listing these definitions in a section of the standard, and deleting these text boxes. Locating them in these text boxes makes the requirements difficult to read.4. If the definitions have to be injected like this, it is not clear why these definitions are located here. Nothing in these requirements discusses the terms being defined.5.

#	Organization	Yes or No	Question 13 Comment
			Suggest deleting "is defined as" as unnecessary. Suggest the format below:External Connectivity - Data communication across the protected electronic boundary. (Addressed in R20.) This definition also relates to the definition of Electronic Access Point in R20.Routable Protocol - a communications protocol that contains a network address as well as a device address thereby allowing packets to be forwarded from a device on one network to a device on another network. Non-Routable Protocol - a communications protocol that contains only a device address and not a network address that not incorporate an addressing scheme for sending data from a device on one network to a device on another network.
13.20	NextEra Energy Corporate Compliance	Disagree	Although on the surface these definitions are straight forward, NextEra believes there is a need to make a transition from the previous requirements for access points. There is not a strong tie between the definition for external connectivity (routable or not) to the requirements in the following sections. For example, Is a serial connection to a BES Cyber considered an Access Point to be protected? The definitions and requirements for protection need to be consistently applied across different levels of impact.
13.21	Garland Power and Light	Disagree	Comment - TOP definition needs to reword as follows:For the purpose of this standard, external connectivity is defined as a data communication path from a BES Cyber System Component to a device external to the BES Cyber System.Suggest better routable and non-routable protocols definitions - give examples of routable and non-routable protocols ie. tcp/ip, netbios, ipx, appletalk,
13.22	Network & Security Technologies Inc	Disagree	Current proposed definition of “external connectivity” is basically circular and could be interpreted in a number of ways. As written, it could even be applied to situations where two discrete BES Cyber Systems are connected to the same LAN segment, which we assume is not what the SDT intended. Suggestion: Unless the SDT really does intend for any network connection not entirely “within” a BES Cyber System to be considered “external,” rewrite the definition to provide a better point of reference than the BES Cyber System itself. Towards that end, the SDT might reconsider its decision to scrap the term, “Electronic Security Perimeter” (which, we note, still appears in CIP-011 in the

#	Organization	Yes or No	Question 13 Comment
			language of R20). We believe that in the context of current CIP Standard CIP-005, "external" connections are widely understood to be defined relative to the logical boundary of an ESP.
13.23	US Army Corps of Engineers, Omaha Distirc	Disagree	Definition of external connectivity is loose and problematic in the interplay with the loose definition of BES Cyber System. Does a communication path exist through a firewall? Does the term mean only intended paths?
13.24	Dominion Resources Services, Inc.	Disagree	Dominion has concerns about the definitions of external connection and electronic access point (Boundary Protection) as illustrated in the following example:A power station has 3 units with the same control system and a shared process I/O bus. Each unit has a control room with MMI, a dedicated server that is networked to the servers at the other 2 units, a front-end processor that is networked to multiple PLCs which are connected to smart I/O controllers. The servers are connected through a firewall to the central engineering office.Under this scenario, it is unclear where the BES Cyber System boundaries should be drawn. If the boundary is drawn around the station, everything is likely to be classified as High Impact and hundreds of I/O transmitters would be included that would normally be Low Impact. If an attempt is made to break the BES Cyber Systems down by unit, every interconnection between the units becomes an external connection and an electronic access point. Excluding a PLC from being part of the High Impact system is difficult because the PLC becomes the electronic access point and its data becomes an external connection. Boundary Protections with the PLC or its connection to the data bus cannot be met.The definition of a "communications path" needs to be clarified. Dominion proposes the following alternate wording to clarify the intent of the definition for external connectivity: ".....external connectivity is defined as any digital communication with a BES Cyber System component from a source external to the BES Cyber System."
13.25	E.ON U.S.	Disagree	E.ON U.S. believes that external connectivity should specify that it is going through an "access point" per the current definition of an access point. The definition of "external connectivity" references the existence of a "data communications path." Does this take

#	Organization	Yes or No	Question 13 Comment
			into consideration any protective measures that assist in the isolation or blocking of data communications? For instance, if a BES Cyber System or Component has a network connection, even an indirect one with multiple levels of firewalls and other security protective devices, to another "external" devices, does it have external connectivity? If so, virtually every system is externally connected; only those that are completely electronically/network-isolated would not be
13.26	USACE - Omaha Anchor	Disagree	External connectivity definition is incorrect. Would prefer a definition external to the facility or external to the electronic security perimeter (understanding that term doesn't exist in this standard.)
13.27	Black Hills Corporation	Disagree	External Connectivity is too open to interpretation; needs to distinguish between external and remote connectivity.
13.28	Luminant	Disagree	External connectivity should include any path and not just those that are considered part of the system functionality. Should also only include routable connectivity
13.29	Progress Energy (non-Nuclear)	Disagree	How are these terms applicable? Is this the key that will take many of our microprocessor relays in Transmission out of scope? If so, we need a clearer linkage to the definitions. It is still not clear if a non-routable protocol like VanCom is definitely excluded. If VanCom is not excluded as it was with previous standards, then every transmission RTU is pulled into consideration.Why have these definitions if the programmable electronic device definition is in play? Again is NERC's intent to manage at component, subsystem, or plant system level? Seems like impact would vary depending to what level of detail we need to get to.These terms are used very limited in CIP 11 and when used they are not used as individual terms. They are combined ie. "external routable connectivity".Do we have to use "routable protocols" term versus the ISO model...like layer 3 and greater?
13.30	Turlock Irrigation District	Disagree	In the definition of external connectivity the use of the words "data communications path" are confusing. Perhaps external connectivity could be defined as "Any electronic

#	Organization	Yes or No	Question 13 Comment
			access point that allows data to be transmitted and/or received between a defined BES Cyber System and a device that is not part of the defined BES Cyber System".
13.31	Southwest Power Pool Regional Entity	Disagree	It is unclear whether the definition of routable protocol includes Layer 2 devices in its scope, understanding that entities have had a difficult time distinguishing between a communications protocol and the networking infrastructure supporting the protocol's use. Additionally, given that the standard is now identifying BES Cyber Systems based upon the reliability functions they perform or support, is it even appropriate to continue to distinguish between routable and non-routable protocols? It is the function and the span of control of the Cyber Asset that determines the impact categorization and requirements applicability.
13.32	National Grid	Disagree	National Grid recommends changing from "from a device external to the BES Cyber System" to "from a device external to the BES Cyber System Boundary"
13.33	LADWP	Disagree	Needs brighter lines.
13.34	ISO New England Inc	Disagree	needs work - removable of ESP has implications. Needs better definition, use of routable protocol clouds issue. External connectivity needs to be defined. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?Recommend changing from "from a device external to the BES Cyber System " to "from a device external to the BES Cyber System Boundary"
13.35	Dairyland Power Cooperative	Disagree	Once the identification of external connectivity is made, why is it relevant to distinguish routable vs. non-routable? A serial cable connected to an unprotected facility may be much more risky than a routable protocol with strict limitations on routing. There may be distinctions to be made in system or communication related requirements, but for training, the external connectivity criteria alone would be the best criteria for the impact level distinctions.

#	Organization	Yes or No	Question 13 Comment
13.36	Public Service Enterprise Group companies	Disagree	Please define the meaning of "routable external connectivity". The terms "external connectivity", "routable protocol", and "non-routable protocol" were defined but not "routable external connectivity" is not. In particular, please clarify the language to provide that if an IP based protocol is in use for a BES Cyber System (e.g. at a substation) where the network address is not required and there is no "external connectivity" (i.e. the IP routing capabilities are disabled - there are no routers or devices capable of routing an IP datagram), this would result in the BES Cyber System being categorized as not having "routable external connectivity".
13.37	Hydro One	Disagree	Recommend changing from "from a device external to the BES Cyber System" to "from a device external to the BES Cyber System Boundary".
13.38	Northeast Power Coordinating Council	Disagree	Recommend changing from "from a device external to the BES Cyber System" to "from a device external to the BES Cyber System Boundary".
13.39	Con Edison of New York	Disagree	Routable Protocol is defined as a communications protocol that contains a single address which identifies both the network and a unique device on that network.
13.40	San Diego Gas and Electric Co.	Disagree	SDG&E recommends rewording and clarifying the definitions of an External and Internal BES Cyber System and Remote Access. Connectivity is defined as "a data communication path existing to a BES Cyber System Component from a device external to the BES Cyber System." 1) What are the standard elements, configuration items, or technology implementations which would distinguish an internal and external BES Cyber System? For example, using this definition, Cyber System A could be on the same LAN as Cyber System B, but considered "external" because the "data communication path" exists (and is switched and not routed) between the 2 Cyber Systems, and 3) does a "data communication path" include serial, USB, Wireless, Channel Attached, or other data communication types of transport? We feel that the access concepts and Remote Access definitions are unclear and difficult to decipher.

#	Organization	Yes or No	Question 13 Comment
13.41	Northeast Utilities	Disagree	Suggest revising the local definition for external connectivity to add “boundary” so the definition would read “… from a device external to the BES Cyber System Boundary”.
13.42	Allegheny Energy Supply	Disagree	Suggest that the External Access definition be revised to include the concept that external access is communcations path access outside of the electronic and physical protection boundaries of BES Cyber System or its connected networks.
13.43	Duke Energy	Disagree	Suggest using these definitions in CIP-010. For generation stations in particular, external connectivity and remote connectivity (R11) should be defined as remote/external to the protected network rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome with little value to cyber security. Same for R13.
13.44	Alberta Electric System Operator	Disagree	The AESO would like to see the terms “network address” and “device address” further defined, to limit possible ambiguity. Consider taking frames (e.g. Ethernet or 802.3) into account in the definition, in addition to packets.
13.45	Southern Company	Disagree	The definition of external connectivity should make it clear that a data communication path does not include human action as an intermediate step.
13.46	Matrikon Inc.	Disagree	The definition of routable protocol should be congruent with the OSI networking stack <http://en.wikipedia.org/wiki/OSI_model>. Routable protocols are those which provide capabilities to communicate at OSI "Network" Layer 3.External connectivity definition still has room for interpretation. If we continue the approach of following the OSI model, then external connectivity is: a communication data "session" using a routable protocol, to an external network requiring OSI Layer 3 "router" or "access point"in order to communicate to an extended network.

#	Organization	Yes or No	Question 13 Comment
13.47	Entergy	Disagree	The definitions for routable and non-routable protocol appear to be satisfactory. However, the definition of external connectivity could prove troublesome, depending upon one's interpretation of a BES Cyber System. For example, a backup site may be classified as a different BES Cyber System than that of a primary site, thus making each one external from the other. Utilizing this interpretation could cause complications from an external connectivity perspective. Conversely, if both sites were classified as a single BES Cyber System, then the issue for external connectivity would not exist.
13.48	US Army Corps of Engineers	Disagree	The proposed definition states that external connectivity is defined as a data communication path existing to a BES Cyber System Component from a device external to the BES Cyber System. Does the use of the word "existing" mean that the data communication path is permanent? If a plant allowed dial-up connectivity to their BES Cyber System, but would need to physically connect the modem for the outside person to dial-in everytime, and then disconnect the modem when completed, leaving an air-gap, would that count as "external connectivity" in this definition?
13.49	Indeck Energy Services, Inc	Disagree	The term “routable protocol” is used only once and the term “non-routable protocol” is never used except in the definition. “Routable connectivity” or “routable external connectivity” are used multiple times without definition.
13.50	Nuclear Energy Institute	Disagree	These definitions should appear in the “Definitions” section.Additionally, for generation stations in particular, external connectivity and remote connectivity (R11) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome with little value to cyber security. Same for R13.
13.51	MidAmerican Energy Company	Disagree	This definition depends on the definition of a BES Cyber System Component, deferring to the functionality of the connected device as the differentiating factor between internal

#	Organization	Yes or No	Question 13 Comment
			and external connectivity. By this definition, a device providing "control" of the BES is by definition a "BES Cyber System Component" and thus, is NOT qualified as external connectivity. For example, a personal home PC, using an Internet connection, could provide "control" of the BES, and thus be considered a BES Cyber System Component, and thus by definition, is not considered remote access.We propose that the definition of external connectivity somehow incorporate the concept of communication medium and endpoint/host control. If the entity does not have 'control' of the medium over which the communications occur, then the communication path must be deemed 'external connectivity'. Additionally, if the entity does not have 'control' over the endpoints/hosts on both ends of the communications path, then the communication path must also be deemed 'external connectivity'. In short, any communication path to a BES Cyber System Component for which the entity does not "control" the communication medium or does not have "control" over both communication endpoints and devices communicating through the endpoints, should be considered 'external connectivity'.Of course, the key consideration in this definition is what constitutes 'control'. The CIP standard for physical security perimeter protections for hosts and endpoints is a good place to start, with the understanding that logical controls such as encryption are viable alternatives for communication paths.If the definition of external connectivity is intended to include dial-up connectivity it should be expressly stated.
13.52	PacifiCorp	Disagree	This definition depends on the definition of a BES Cyber System Component, deferring to the functionality of the connected device as the differentiating factor between internal and external connectivity. By this definition, a device providing "control" of the BES is by definition a "BES Cyber System Component" and thus, is NOT qualified as external connectivity. For example, a personal home PC, using an Internet connection, could provide "control" of the BES, and thus be considered a BES Cyber System Component, and thus by definition, is not considered remote access.We propose that the definition of external connectivity somehow incorporate the concept of communication medium and endpoint/host control. If the entity does not have 'control' of the medium over which the communications occur, then the communication path must be deemed 'external connectivity'. Additionally, if the entity does not have 'control' over the

#	Organization	Yes or No	Question 13 Comment
			endpoints/hosts on both ends of the communications path, then the communication path must also be deemed 'external connectivity'. In short, any communication path to a BES Cyber System Component for which the entity does not "control" the communication medium or does not have "control" over both communication endpoints and devices communicating through the endpoints, should be considered 'external connectivity'.Of course, the key consideration in this definition is what constitutes 'control'. The CIP standard for physical security perimeter protections for hosts and endpoints is a good place to start, with the understanding that logical controls such as encryption are viable alternatives for communication paths.If the definition of external connectivity is intended to include dial-up connectivity it should be expressly stated.
13.53	GTC & GSOC	Disagree	We recommend that local definitions for a specific Reliability Standard be documented in a section prior to the requirements sections instead of interspersed throughout the requirements. While it may improve the initial readability of the requirements, it is problematic in the long term determining if and where a particular word is defined.We also recommend "external connectivity" should be limited to situations where an external device can initiate a connection to the BES System Component. If a firewall limits connections to only those initiated by the BES System Component itself (i.e., connections are only one-way: out), the component should not be considered to have external connectivity.We recommend deleting the portion referring to network and device addresses because not all protocols make a clear distinction between a network address and a device address. The functional packet-related distinction is sufficient. The second and third paragraphs of the definition would read: "For the purpose of this standard, a routable protocol is defined as a communications protocol that allows packets to be forwarded from one network to another.For the purpose of this standard, non-routable protocol is defined as a communications protocol that does not incorporate an addressing scheme for sending data from one network to another."
13.54	Bonneville Power Administration	Disagree	We understand the need to keep definitions close to where they're used, it is also important to have them centrally located. We understand that this leads to a document maintenance issue. However, most document creation tools have solutions. For

#	Organization	Yes or No	Question 13 Comment
			instance, in Microsoft Wordâ„¢, you can make the definition a bookmark, and then insert a cross-reference somewhere else. The definition of "External Connectivity" is too broad. Consider an example: A user in a Control Center is logged into a workstation that is part of a BES Cyber System. The user opens a connection from that workstation to another BES Cyber System in the same Control Center. The communications path is totally under the control of the Responsible Entity, and all systems and communication paths involved are under the physical and electronic protections of the Control Center. Yet, this would constitute and external connection to the second BES Cyber System, and thus constitute remote access to that system. This is an untenable situation, especially considering the tight controls justifiably required for connections from outside the control of the Responsible Entity.Recommendation: "...defined as a data communications path to a BES Cyber System that encompasses, in some or all portions, links outside the control of the Responsible Entity." The definition of "Routable Protocol" is acceptable.The definition of "Non-routable Protocol" is slightly broader than necessary. It excludes point-to-point protocols. For instance, RS232 is one of many serial communications protocols that contains no address of any kind. Recommend changing "...that contains only a device address and not a network address." to "...that contains at most a device address and no network address."
13.55	Verizon Business	Disagree	1) The definition should explicitly state that a “Routable Protocol” includes TCP/IP. Also, the definition should explicitly state that MPLS is considered a “Routable Protocol” because MPLS is considered OSI Layer “2 ½” and hence there may be disagreement whether it is routable. For a “Non-Routable Protocol,” an example like a protocol in the OSI Layer 2 should be provided. 2) The term “external connectivity” requires more explanation. It is unclear whether it would include two BES Cyber Components that are connected to each other, regardless of the length of separation.

14. Tables R3 and R4 provide direction concerning what impact level of BES Cyber Systems to which Requirements R3 and R4 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R3 and R4 have moved to CIP-004-5 R1 through R3.

Several commenters expressed confusion regarding the purpose of specifying routable connectivity in the applicability for training requirements. The SDT agrees and has modified the applicability to include all High and Medium BES Cyber Systems.

In addition, several commenters suggested the training and personnel risk assessment should apply across all impact levels. One commenter suggested the training and personnel risk assessment should only apply to the High Impact level of BES Cyber Systems, and another commenter suggested there should also be a “no-impact” level. The SDT has changed the requirements for training and personnel risk assessments to apply to High and Medium Impact BES Cyber Systems. These requirements do not apply to Low Impact BES Cyber Systems because of the significant effort required to track the Low Impact BES Cyber Systems and the persons who have authorization to access those systems.

#	Organization	Yes or No	Question 14 Comment
14.1	US Army Corps of Engineers		In Tables R3 and R4, the phrase "Physical access to BES Cyber Systems" is qualified with the words "with routable external connectivity" but these words are not referenced in any of the paragraphs R2-R4. Paragraphs R2-R4 state physical access as "authorized unescorted physical access to BES Cyber Systems." Should we assume that both terms are the same?
14.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
14.3	Northeast Utilities	Agree	Please change Table R4 to read “Personnel Risk Assessment”.
14.4	Madison Gas and Electric Company	Agree	Thank you for adding these helpful tables immediately after the requirement. This reduces the confusion of turning a page to an appendix.

#	Organization	Yes or No	Question 14 Comment
14.5	GTC & GSOC	Agree	We recommend making sure there is consistency with impact levels for authorizing physical and authorizing electronic access
14.6	Black Hills Corporation	Agree	Would like to know if an entity exceeded any NERC requirements as internal policy, and subsequently had an individual miss training who did not interact with a BES Cyber System, would this be considered a violation by NERC.
14.7	ERCOT ISO	Disagree	3.2 & 4.2: Please clarify why "with routable external connectivity" is addressed.
14.8	US Army Corps of Engineers, Omaha Distirc	Disagree	3.2 not clear as to purpose of this training or how external connectivity relates. Without electronic access the most they could do is damage hardware. Does this only apply to hardware providing external connectivity such as firewall etc?
14.9	Tenaska	Disagree	5.3 Consider leaving the word "uniquely" out or change it to say individually identify.
14.10	BCTC	Disagree	Â We are in strong disagreement with R3.2. We have various parties who have electronic access to our BES Cyber Systems but do not agree that training these individuals on networking hardware and connectivity would increase the security of the BES. Could you please clarify the objective of this requirement? - i.e. why would someone who simply accesses a console to view BES Cyber System data require network-related training? We recommend that the requirement be worded something like "... personnel will be supplied training on applicable NERC CIP devices that they are authorized to work on and the associated related security controls, as identified in the CIP Standards..." Above we have recommended above that "emergency situation" language remain at the security policy level. A potential scenario in this requirement is an emergency occurs (i.e. a critical piece of equipment breaks) whereby the closest service provider available to fix the problem is minutes away but has not completed CIP training or a PRA; from an operations (i.e. "keeping the lights on") perspective we would identify this as an emergency situation, seek approval from our Senior Manager or delegate to allow this person to access our facility, and allow the repair to occur. In this scenario we are assuming our 'regular' service technicians are unavailable or far way

#	Organization	Yes or No	Question 14 Comment
			from the facility.Â We have encountered an issue where some non-North American countries will not disclose criminal histories so it will be difficult to meet the requirement that states ... "A seven year criminal history records check covering all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration." We can have new employees from these countries start employment but lived in North America for less than 7 years. For such a scenario we recommend that the language be revised to indicate that the Utility requests a seven year criminal history check on a best efforts basis; i.e. we can ask for the information but there is no guarantee the originating country will provide us with the results - this is beyond our control. FYI, simply denying a person on these grounds in Canada violates out employment legislation.Â R4.2 We currently retain a "clear"/ "not clear" result with all PRAs for contractors and employees. Please confirm that this requirement does not require the Utility to retain detailed records (i.e. listing of criminal offenses, charges, etc.)
14.11	Hydro One	Disagree	Agree provided the external connectivity definition is revised per the response to question 13.Recommend changing Table R4 from "personal" to "personnel".Suggest changing to annually for consistency.Such classification will add additional unnecessary burden since specific training will need to be generated and tracked depending on the type of system access
14.12	Northeast Power Coordinating Council	Disagree	Agree provided the external connectivity definition is revised per the response to question 13.Recommend changing Table R4 from "personal" to "personnel".Clarify "12 months".
14.13	ISO New England Inc	Disagree	Agree provided the external connectivity definition is updated per answer #13 Table 4 title uses "personal" instead of personnel.
14.14	San Diego Gas and Electric	Disagree	Attempting to split hairs between PRA and Training requirements for physical and cyber access to BES Cyber Systems for Medium and High Impact systems seems to

#	Organization	Yes or No	Question 14 Comment
	Co.		unnecessarily increase risk exposure for an Entity and complicates the process and controls needed to meet R3 and 4 of CIP-011-1. SDG&E recommends that the requirements for both of these tables be required for High Impact BES Cyber Systems only
14.15	E.ON U.S.	Disagree	CIP-011, R3 states that contractors and service vendors with authorized electronic or unescorted physical access are to complete cyber security training before given this access. However, this begs the question of what constitutes satisfactory evidence of this training for these individuals? If vendor-provided training is adequate, what evidence is needed to maintain this training?a. (3.2) "...shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity..." For most users of these systems, training on the networking hardware and software provides little or no value. Unless these are systems administrators tasked with responsibilities for managing / monitoring these systems, users (and associated training) should be focused on the functions of the system to support operation, monitoring, and control for which they are responsible.CIP-011, R4 requires background checks for contractors and service vendors. The new requirements do not clarify the acceptable evidence required to be maintained by entities. Is it acceptable for a service provider to conduct the background checks? If so, what evidence of background checks does the registered entity need to maintain?Does the requirement apply for everyone that has access to the BES cyber system ? Would this include support personnel and janitorial staff? E.ON U.S. suggests that the requirement be tied to job function rather than a blanket requirement for all.E.ON U.S. requests clarification as to how personnel that only have remote access to the system should be verified. Photo IDs are neither practical nor required.
14.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
14.17	US Bureau of Reclamation	Disagree	Cyber access training and personnel risk assessment requirements should be applied to

#	Organization	Yes or No	Question 14 Comment
			all three impact levels.
14.18	BGE	Disagree	Define “electronic access” as noted in table R3 (3.1). 3.2 Should say “Physical access to BES Cyber Systems (remove routable external connectivity). Table R4 (4.2) should add “unescorted” physical access to BES.....
14.19	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes Personnel Training, Awareness, and Risk Assessment should only apply to personnel with access to high impact BES cyber systems and not include personnel with access to medium and low impact systems. This requirement as currently drafted is unduly burdensome for field personnel that have local access to programmable electronic devices. These personnel need not be aware of network considerations to securely perform their job duties.
14.20	Luminant	Disagree	Does R4, 4.1 need to be modified to address valid identification for foreign nationals with remote (overseas) access to BES Cyber Systems?
14.21	MRO's NERC Standards Review Subcommittee	Disagree	For item 3.1 and 3.2, we propose making the Low Impact criteria “Required”. Cyber Security Training is something that should probably be carried out across the BES.For item 3.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external connectivity only”.For item 4.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external connectivity only”.If an entity is required to restrict physical access, then they should also be required to provide training.
14.22	The Empire District Electric Company	Disagree	For item 3.1 and 3.2, we propose making the Low Impact criteria “Required”. Cyber Security Training is something that should probably be carried out across the BES.For item 3.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external connectivity only”.For item 4.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external

#	Organization	Yes or No	Question 14 Comment
			connectivity only".If an entity is required to restrict physical access, then they should also be required to provide training.
14.23	Platte River Power Authority	Disagree	Is the intent that prior training is not required for Physical access to BES Cyber Systems without routable external connectivity? In other words, the table says that prior training is only required if Physical access is granted to a BES Cyber Systems with external connectivity. Is that the intent?
14.24	Entergy	Disagree	It appears nonsensical to require cyber security training and personnel risk assessments for electronic access to BES Cyber Systems classified as Medium-impact, but not for physical access to Systems with external connectivity. Requiring these items for only one type of access and not the other merely increases the likelihood of misinterpretation of the requirements by the Entity. PRAs and training should be required for both types of access or neither.
14.25	FirstEnergy Corporation	Disagree	It would be very difficult to administer training and PRAs based on impact levels. It seems like it would be easier to just have one level for all. We suggest eliminating the tables/impact levels for R3 and R4.Training and PRAs should be required for all levels. It is easier to maintain, track and move employees around if they are all trained and background checked, especially with the need to continuously reassign employees.
14.26	Manitoba Hydro	Disagree	Manitoba Hydro agrees that cyber security training is not a standard requirement for all personnel who have unauthorized physical access to Low Impact BES Cyber Systems, and therefore should not be auditable. We do not agree that training is not a requirement for personnel who have authorized electronic access to Low Impact BES Cyber Systems, and suggest that it be an auditable requirement.
14.27	Progress Energy (non-Nuclear)	Disagree	May not be an issue since most our personnel that require access will very likely require access to all three impact levels and will require adherence to the highest security level anyway. It does not seem practical and reasonable to develop and maintain three different security programs based on the three impact levels.The question with most of

#	Organization	Yes or No	Question 14 Comment
			the impact level requirements is the difficulty and cost associated with developing and maintaining three different levels of security, monitoring and controls and making sure that the appropriate levels are applied with an increase in impact level.Again is NERC's intent to manage at component, subsystem, or plant system level? Impact will vary depending to what level of granularity we need to get to.Section R3.1 appropriately provides for a level of NERC CIP training consistent with physical only access. The last point 'Identification and reporting of a Cyber Security Incident' should be clarified to be the physical aspects of a cyber security incident. Since this is the type of training that we will be providing to janitors/HVAC repair technicians/electricians, there should not be a requirement to provide any type of cyber training. The full 'Identification and reporting of a Cyber Security Incident' can be included under R3.2 - which is intended for those with actual cyber access.
14.28	National Grid	Disagree	National Grid agrees provided the external connectivity definition is updated per answer 13.Recommend changing Table R4 from "personal" to "personnel".
14.29	LCEC	Disagree	No. These tables should include all standards and clearly indicate their intent.
14.30	American Municipal Power	Disagree	Please add a little or no impact category.
14.31	Puget Sound Energy	Disagree	Puget Sound Energy, as stated earlier in this document, would need to see more specific definition to "Low", "Medium", and "High" impact, as well more specific definition to subjective terms such as "restrict" and "affect". If specificity can be provided to the subjective areas of the definition to "Low Impact", "Medium Impact", "High Impact", "restrict control", and "affect situational awareness", Puget Sound Energy agrees with the tables.
14.32	ReliabilityFirst Staff	Disagree	Requirement R4.1; ReliabilityFirst is concerned that permitting documents other than Social Security Identification for identity verification could lead to questionable results. Requirement R4.3 only addresses updating a PRA every seven years but does not include

#	Organization	Yes or No	Question 14 Comment
			a requirement to update the PRA "for cause." Table R3 and R4, Medium Impact BES Cyber Systems should be required for rows 3.2 and 4.2 respectively.
14.33	Southwest Power Pool Regional Entity	Disagree	Some degree of physical and electronic access training is basic security training that should be applicable to all impact categories. The extent of the training could perhaps be adjusted to reflect the impact categorization. 4.2: See the discussion regarding the need for distinguishing between routable and non-routable protocols. The Personnel Risk Assessment should be required prior to access for at least High and Medium impact BES Cyber Systems, both physical and electronic, regardless of any communications protocol being used.
14.34	Network & Security Technologies Inc	Disagree	Suggest (1) dropping "routable external connectivity" qualifier for High Impact systems in 3.2 and 4.2 and adding Medium Impact systems to 3.2 and 4.2.
14.35	EEI	Disagree	Suggest elimination of Table R3. EEI suggests making training mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.Suggest elimination of Table R4. EEI suggests making personnel risk assessment mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site?
14.36	Emerson Process Management	Disagree	Table R3 implies that Cyber Security Training is not required for people who have physical access to a high impact BES Cyber System as long as this system does not have routable external connectivity.Per 3.1, the training shall cover the policies, access controls and procedures.This is unclear about the connection between the needed training and the lack of routable external connectivity.Same note applies to Tabe R4.
14.37	American Electric Power	Disagree	Table R3, 3.2: Regarding "Physical access to BES Cyber Systems with routable external connectivity", suggested wording: "Authorized, unescorted physical access".Current

#	Organization	Yes or No	Question 14 Comment
			wording seems to require training for all physical access. Would a group taking a walking tour of a generation control room, transmission substation, or control center need cyber security training?Table R4, 4.2: Regarding "Physical access to BES Cyber Systems with routable external connectivity", suggested wording: "Authorized unescorted physical access"Current wording seems to require personnel risk assessment checks for all physical access. Would a group taking a walking tour of a generation control room, transmission substation, or control center need personnel risk assessments?
14.38	Alberta Electric System Operator	Disagree	The AESO suggests that security training and PRA are required for all impact levels for 3.1, 3.2, 4.1, 4.2 in the tables. The SDT should consider devising a graduated implementation scheme, or let the RE determine how much and to what extent the training and PRA should include for each impact level.
14.39	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS proposal to require cyber security training in Table 3.1 and Table 3.2 for all impact levels. The training requirements for Table 3.1 and Table 3.2 Low Impact, should only be required to comply with R3 sub-requirement 3.1, at a frequency of every 2 years. These Low impact facilities should not be required to comply with the specific requirements detailed in R3, sub-requirements 3.2-3.5. We suggest the table state; “Applies to sub-requirement 3.1 only, Frequency: Every 2 years” for Low Impact facilities. We agree with the MRO-NSRS comments on item 3.2; MRO-NSRS proposes removing “with routable external connectivity.”The APPA Task Force feels there is confusion with blanks in the tables. For example, in Table 4.1 we have assumed that a blank under the Low Impact category means a Low Impact BES cyber system is not required to conduct any Personal Risk Assessments Prior to Obtaining Table 4.1 and 4.2 access. If this is the meaning of such blanks it is our recommendation that the drafting team make that clear and insert a N/A for Not Applicable in all blanks throughout the document and define N/A in the introduction.For R4 Table 4.2, the APPA Task Force agrees with the MRO-NSRS proposal to remove “with routable external connectivity”, and to add the following under Medium Impact: “Required for routable external connectivity only”.The APPA Task Force suggests the following text for the noted tables:R3 Table 3.1: Low Impact: Required (Applies to sub-requirement 3.1 only) at

#	Organization	Yes or No	Question 14 Comment
			least once every 24 monthsMedium Impact: RequiredHigh Impact: RequiredR3 Table 3.2: Low Impact: Required (Applies to sub-requirement 3.1 only) at least once every 24 monthsMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR4 Table 4.1: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR4 Table 4.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required
14.40	Duke Energy	Disagree	The format in these tables is confusing. The requirements tell “what” the requirement is, and the table tells “who” the requirement applies to.
14.41	Con Edison of New York	Disagree	The R3 Dialog box defines external connectivity. It is not clear whether external activity is between systems in all cases, or does it mean between systems that are within different electronic boundaries. The wording needs to make this clear.The requirement to check photographic ID’s seem appropriate initially, or during the hiring process. As written it will require checking photo ID’s every seven years for an employee that has been working in for the Company for the entire period and whose identity should no longer be in question. The recurring requirement should not apply. R3.2 - it is unrealistic to expect to train operators on network equipment, software, and protocols, which is a separate and distinct job function.R3.3 - Review of DR procedures is appropriate, but specific training on DR is not
14.42	Consultant	Disagree	The 'required' blocks for electronic access would seem to imply that there is no connectivity between low impact assets and medium or high impact assets. If this is the case, then the table seems adequate. Or there should be a 'highest impact rules the network access controls' qualifying statement.The 'required' block for physical access would seem to imply that there is no co-located assets of different impact levels. This seems less likely than electronic access segregation. There should be a 'highest impact rules the physical boundary access controls' qualifying statement.
14.43	Idaho Power Company	Disagree	The table does not address training requirements for personnel with access to sensitive information about BES cyber systems but do not otherwise have electronic or physical

#	Organization	Yes or No	Question 14 Comment
			access to the system itself. It would be difficult to be compliant with R24 if personnel are not trained to recognize sensitive information or trained on the proper labeling and handling procedures.
14.44	Florida Municipal Power Agency	Disagree	The tables are ambiguous. For instance, is the blank in the table for R3 for Low Impact supposed to mean that no training is required, as FMPA interprets? FMPA believes that some level of training ought to be provided for all levels of impact, correlated with the impact level (e.g., biennially instead of annually for Low Impact for instance). FMPA suggests embedding the bullets into the table in a similar manner as R5 and leaving no blanks in the table to make clear what is required for each impact level.
14.45	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The tables should clearly specify unescorted physical access.
14.46	Constellation Energy Control and Dispatch, LLC	Disagree	-There should be a row in the R3/R4 tables for each Requirement/Sub-Requirement-Define "electronic access" in table R3 (3.1).-Table R4 (4.2) should say "unescorted" physical access to BES Cyber Systems with routable external connectivity.
14.47	Bonneville Power Administration	Disagree	Training and especially a PRA should be required for physical access to any High or Medium impact system, regardless of whether it has routable external connectivity. A hammer to a RAS system could cause severe issues, whether or not the system connects to field units with a routable protocol. In addition, physical access to BES Cyber Systems is potentially far more dangerous that Electronic Access (especially at field sites) The requirements in the table should be at least the same for physical and electronic access. In both Tables R3 and R4, the word “unescorted” should be added at the beginning of Items 3.2 and 4.2.
14.48	WECC	Disagree	Training should be done for all employees with any level of access to a minimum level. Additional criteria for training should be done dependent on the level of access and their

#	Organization	Yes or No	Question 14 Comment
			role. See previous comments about suggestion to replace with a requirement for a training and awareness program with specific criteria.These requirements should apply to all impact levels. Awareness, training, overall education, and personnel risk assessment are the building blocks for a successful security program.
14.49	We Energies	Disagree	We Energies agrees with EEI: Suggest elimination of Table R3. Make training mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.We Energies agrees with EEI: Suggest elimination of Table R4. Make personnel risk assessment mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.We Energies agrees with EEI: Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site?
14.50	Minnesota Power	Disagree	While the impact levels seem reasonable, it is the inclusion of the term “external connectivity” as a qualifier in sections 3.2 and 4.2 of Tables 3 and 4 respectively that creates confusion. The relevance of connectivity to implementing appropriate physical security measures is not clear. Physical Access averts the need for electronic access, so this seems counterintuitive to include “external connectivity” as a provision. Minnesota Power recommends that sections 3.2 and 4.2 of Tables 3 and 4 respectively simply state “Physical access to BES Cyber Systems.”

15. Requirements R5 and R6 of draft CIP-011-1 concern procedures for physical security, which were previously contained in CIP-006. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Many of the commenters expressed concerns with the timing of the revocation requirements as being unrealistic, especially for authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access. Commenters stated that the time required for revocation should be extended to 72 hours or to the next business day, whichever is longer, to allow for communications of this circumstance. Timing issues regarding the termination of access for contractors and/or service vendors were also raised.

The SDT has clarified that the timely revocation of electronic access to cyber systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform the assigned functions, that access should be revoked. Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services). CIP-004-5 Requirement 7 enumerates the proposed requirements under a variety of conditions regarding revocation of access.

Some commenters expressed confusion regarding the use and meaning of the terms "grant" and "authorize" and their use in these requirements. Also, the term "Physical Access Control Systems" was requested to be defined, as the term will likely have different meanings for different entities and auditors and could lead to difficulties in implementation and auditing. The SDT has provided additional clarity in the requirements and has proposed the following definition for **Physical Access Control Systems**: *"Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers."*

Physical security at remote substation sites was also raised as not being cost effective in preventing or detecting cyber attacks, especially for remote substations with only dial-up communications. Commenters indicated that physical security should only be required at Control Centers and High Impact substations with IP-based communications. While some commenters generally liked having all the Physical Security requirements in one standard versus references to multiple standards and multiple requirements within standards, the commenters expressed concern that the clarity that was intended was not provided, as the language used is vague and confusing. Some restructuring of the requirements was suggested to improve the clarity of the standards.

While some restructuring of the requirements for physical security has been implemented by the SDT in the Version 5 standards, each Responsible Entity is required to ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. CIP-006-5 defines the requirements for physical protection for Low, Medium, and High Impact BES Cyber Systems. While the requirements place the

emphasis for physical protection on the High and Medium Impact BES Cyber Systems, each Responsible Entity's Physical Security Plan is required to address how it will protect Low Impact BES Cyber Systems.

#	Organization	Yes or No	Question 15 Comment
15.1	National Rural Electric Cooperative Association (NRECA)		In R5.5, the statement to "Authorize unescorted physical access....." makes it sound like the utility should provide blanket authorization for unescorted physical access. I don't believe that is the case. Please clarify R5.5 -- I believe what is intended here is to have policies and procedures in place to detemine who has authorization to have unescorted physical acess.
15.2	Idaho Power Company		R6 is confusing. The headings suggest the need for a physical security plan but the tables pertain to requirements to protect physical access control systems. 6.1 should read "Restricting physical access to physical access control systems that are protecting BES Cyber systems identified in Requirement R5 Part 5.1, 5.2 5.3." 6.2 should read similarly. The current wording suggests that a physical access control system would be identified in Requirement 5 but it is not a BES cyber system because it does not perform a function listed in the attachment 1.
15.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.In R5 and R6, "prevent" is an objective (or purpose) and should not be embedded in the requirement, e.g., if unauthorized physical access occurs such as someone driving a bull-dozer through a building, is the entity non-compliant? Objectives should not be mixed with the actual requirement.In the bullets to R5 and R6, the areas in and of themselves do not "protect" BES Cyber Systems, they "contain" them.R5The requirement to "apply criteria" is not a strong requirement. FMPA suggests: "Each Responsible Entity shall apply the security controls specified in CIP-011-1 Table 5 - Physical Security for BSE Cyber Systems."In the bullets, there is confusion among the terms "grant" and "authorize". "Authorize" is senior manager approval, "grant" is being given the key or card. The requirements should keep these two concepts clear. For instance, in 5.5, "authorize" should be changed to something like: "Grant unescorted physical access to areas containing BES Cyber Systems only to those who are authorized

#	Organization	Yes or No	Question 15 Comment
			such access". Also, in order for 5.8 and 5.9 to apply to Medium, then 5.5 needs to apply to Medium.5.7, 5.9 and 5.9 will be open to interpretation. If an employee was given key and card access, is revoking card access sufficient or both the key and the card?5.7 should apply to Medium5.8 and 5.9 should be combined and the time durations correlated with the impact level instead of Control Center vs. Facility.5.10 strike "access"R6The order of R5 and R6 seems backwards. It would seem development of the physical security plan (R6) should come before implementing the plan (R5)
15.4	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 12.
15.5	Independent Electricity System Operator	Disagree	- R5.1 in table 5 please define what is meant by external connectivity. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?- 5.3 and 5.4 should be consistent in
15.6	Reliability & Compliance Group	Disagree	: Putting data retention into a separate section of the standard is confusing without a reference. If you want to keep data retention separate, you should refer to the data retention rules in the standard. i.e. Retention rules for R5 can be found in section 1.4.1 and 1.4.3 of this standard.Also, visitor control should be included for medium impact systems as well. If not, why are we restricting access to those systems if we can routinely open the door for anyone to come in and wander around unescorted. One interpretation of this would be to have some employees given access rights and others would be daily guests who are not logged or monitored.
15.7	Regulatory Compliance	Disagree	5.7 - qualification should be made in regards to a service vendor that the 24 hour period should start once notice is received from their company.5.8 - prefer 7 day revocation deadline5.9 - prefer 7 day revocation deadline
15.8	USACE - Omaha Anchor	Disagree	A) Dislike that methods to achieve compliance were removed from standard and will be placed in a guidance document. Guidance documents aren't binding. B) 5.9 - how do

#	Organization	Yes or No	Question 15 Comment
			you revoke access when it was never formally granted in the first place?
15.9	Duke Energy	Disagree	a) We generally like having all the Physical Security requirements in one standard versus references to multiple standards and multiple requirements within standards. However, the clarity that was intended is not provided as the language is vague and confusing.b) The standard has eliminated terms like the Physical Security Perimeter, 6 wall boundary and Physical Security Plan but it appears that they will be expected in order to achieve compliance. In fact, R6 includes a reference to "...one or more physical security plans..." that is not mentioned in the R5 requirement which appears inconsistent since R5 is the Physical Security for the BES Cyber Systems. Provide clarity and make consistent. c) Requirements 5.1, 5.2 and 5.3 appear to be less prescriptive than previous CIP 006 versions. However, is it left up to the Responsible Entity to determine the requirements for controlling access, monitoring access and logging access? Are some of the expectations from previous CIP 006 Rev. 3 still expected, but not documented? d) General Comment: V4 is very vague and unclear as to what is required. We would suggest additional wording to provide clarity as to what is intended for the responsible entity to physically meet R5.1, R5.2 and R5.3Physical security will be extremely difficult to implement on components located throughout the plant.For 5.9, assuming a key is used to access a system, revoking access within 72 hours maybe impossible. Changing locks may not be able to happen that fast. Face to face terminations may not be the case. Costs associated with card readers to replace locks is extremely high ($5-7k per reader, average 6 readers per hydro station and about 5 hydro stations this will apply to is a minimum of $150,000). Some systems are in cabinets that must be left open to do work. Card readers will set off alarms before work can be completed.For 5.11, should be deleted, as this should be included in the incident response procedures.For 5.2, what does monitoring entail?For 5.8, should be 48 hours.6.3 states "implementing maintenance and testing program....function properly". "Properly" is a vague term open for interpretation.
15.10	SCE&G	Disagree	Again, SDT should allow provisions for entities to leverage existing controls (i.e. Nuclear Facility Physical Security). NPP's have one of the most effective Physical Security

#	Organization	Yes or No	Question 15 Comment
			Programs of all Critical Infrastructures. CIP-011 R5/R5 should acknowledge this progam.5.2 SDT needs to better define what constitues appropriate "Monitoring". 6.3 "physical access control systems" should be defined. Is there an expectation for entities to walk fences around substations/generation facilities every 3 years?
15.11	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comment.
15.12	Liberty Electric Power, LLC	Disagree	CIP-011 R5 has very short times to revoke access. If an entity gives a contractor a code to enter the a room so he can download data on a Friday night shutdown, the code will have to be changed prior to the next business day -even if he is physically incapable of entering the plant.
15.13	E.ON U.S.	Disagree	CIP-011-1, R5.7, R5.8 and R5.9 does not fairly address the termination of access of contractors and/or service vendors. These types of requirements have generated many self reports to the NERC regions, and it is clear that this will continue so long as registered entities are presumed to have immediate knowledge of a change in the status of each contractor's employees. E ON U.S. proposes the requirements read as follows:R5.7 - "Revoke authorized unescorted physical access to areas protecting BES Cyber Systems within 24 hours for employees terminated for cause. For contractors/service vendors, access shall be revoked within 24 hours from the time of notification from the contracting/service vendor company."R5.8 - "Revoke authorized unescorted physical access to areas protecting BES Cyber Systems for employees who no longer require such access within 36 hours. For contractors/service vendors, access shall be revoked within 36 hours from the time of notification from the contracting/service vendor company."R5.9 - "Revoke authorized unescorted physical access to areas protecting BES Cyber Systems for employees who no longer require such access within 72 hours. For contractors/service vendors, access shall be revoked within 72 hours from the time of notification from the contracting/service vendor company."Additionally, CIP-011-1, R5.11 is ambiguous. E ON U.S. requests that the SDT clarify "review" to address is expected.

#	Organization	Yes or No	Question 15 Comment
15.14	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
15.15	LADWP	Disagree	Commensurate security measures need to be defined. If 6 wall is no longer the standard, what is replacing it?
15.16	Public Service Enterprise Group companies	Disagree	Comments: R5.8 requires physical unescorted access be revoked within 36 hours. This is too short a period, especially if the event occurs over a weekend or holiday. The timeframe should be changed to 5 calendar days or 3 business days. At a minimum, 72 hours.Physical protection of assets that are located within a NRC mandated Security Boundary / Perimeter that complies with NRC security regulations for Nuclear plants should be deemed to satisfy NERC CIP physical security requirements. NRC background checks, training, etc. for unescorted access and the physical security provided at Nuclear plants is more than adequate to satisfy NERC reliability physical security needs. Registered entities should not be required to implement duplicative procedures and programs for physical security of BES cyber assets located inside the NERC security Boundary/Perimeter. The drafting team should develop appropriate language to this effect.
15.17	CenterPoint Energy	Disagree	Disagree - For R5.8 and R5.9, CenterPoint Energy recommends increasing the timeframe for revocation of authorized unescorted physical access for personnel who no longer require such access to seven days as is found in the current Standard. CenterPoint Energy also believes physical access methods employed at a control center should differ versus those at a remote substation environment and therefore recommends revisions allowing for such differences.
15.18	FEUS	Disagree	Disagree with comments: 5.5 and 5.6 require authorization and quarterly reviews of unescorted physical access. It is not clear what type of authorization process would be required or what is required to be reviewed.

#	Organization	Yes or No	Question 15 Comment
15.19	Black Hills Corporation	Disagree	In 5.1, do not understand the significance of external connectivity only. Also in 5.1, restrict physical access is not defined (what evidence would be required to prove if we are not required to monitor, log, authorize, etc?) In 5.6, quarterly is a good goal, but without a solid definition of the window associated with "quarterly", this will be an evidence gathering problem - suggest changing to semi-annual. 5.2 & 5.3, and 6.2 & 6.3 should have consistent impact applicability.
15.20	Constellation Power Source Generation	Disagree	In R5.2, what is meant by the term monitor? Is that continuous, automated monitoring, or can it be an inspection during an operator's round? A suggestion would be to include the phrase "automated or manual" to add clarity. R5.4 defines the action of logging as "manual or automated." This definition should also be used in R5.3 and R5.2. In R5.6, why is the review on a quarterly basis? Other requirements ensure that a terminated employee has access revoked extremely quickly, so the review in R5.6 can be extended out to an annual review without an adverse reliability impact on the BES. In R5.9, why is the term generation lowercase? Is this implying a different meaning? R6.3 is requiring testing and maintenance of all physical security mechanisms on a cycle no longer than 3 calendar years. However, some plants are on a 3 to 5 year maintenance schedule and are otherwise expected to be running. This will force a plant to take an outage it otherwise would not have just to comply with a physical security requirement.
15.21	Luminant	Disagree	It does not make sense to physically protect BES Cyber System for Meduim Impact systems that have external connectivity. The impact of physical access is no different that for systems not externally connected. 5.8 change to 48 hours (2 days) 5.9 1 week. Also remove 5.8 and 5.9 from the Medium impact requirements, as you cannot revoke access since it is not a requirement to restrict or grant unescorted access.
15.22	Emerson Process Management	Disagree	It is unclear about the relevance of physical access control and external connectivity.
15.23	WECC	Disagree	Low and Moderate impact assets must have some baseline physical security. It appears

#	Organization	Yes or No	Question 15 Comment
			that some requirements have differences between the levels for their own sake without the justification of security risk analysis. The standard should be adjusted to provide baseline physical security for all systems regardless of impact and/or method of communication.
15.24	Manitoba Hydro	Disagree	Manitoba Hydro does not agree with the drafting team approach to defer the FERC Order 706 directive for multiple physical security perimeters. Upgrading physical security at facilities is costly and time consuming and deferring the multiple perimeter requirement will require entities to later rework physical security at many facilities. The drafting team should either include the multiple physical security perimeters in version 4 or limit all physical security requirements to those already completed under CIP V1-V3. The reference in Requirement R5.11 to incident response procedures should be cross-referenced to Requirement R27, assuming that these are the procedures being referenced in Requirement R5. Requirement 5.7 could be interpreted as a subset of Requirement 5.8. Requirement 5.8 should explicitly exclude personnel terminated for cause. There are no specifics given with respect to 'restricting' access in Requirement 6.1 so it is assumed to be at the Responsible Entity's discretion in terms of to whom, by what means, etc. It is not clear if the "Required for routable access only" in the impact columns refers to routable BES Cyber Systems or routable physical access control systems.
15.25	Network & Security Technologies Inc	Disagree	Minimum retention period for logs should be specified. 5.11 does not specify a time frame for reviewing and handling unauthorized physical access attempts.
15.26	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R5, but recommends changes as follows: o Regarding Table R5, Minnesota Power recommends changing "areas protecting" to "areas containing BES Cyber Systems" to reduce ambiguity and confusion. o For Section 5.1 of Table 5, for Medium Impact Systems, the inclusion of the term "external connectivity" as a qualifier that creates confusion. The relevance of connectivity to implementing appropriate physical security measures is not clear. Physical Access averts the need for electronic access, so this seems

#	Organization	Yes or No	Question 15 Comment
			counterintuitive to include “external connectivity” as a provision. Minnesota Power recommends that the reference to “external connectivity” be removed from sections 3.2, 4.2, and 5.1 of Tables 3, 4, and 5 respectively. o As currently written, sections 5.3 and 5.4 seem to be similar and could be combined. If it is the Standards Drafting Teams intent that 5.3 apply to those individuals authorized for access, then Minnesota Power recommends the following revision to R5.3:"Log physical access to areas containing BES Cyber Systems for individuals with authorized cyber access and/or authorized physical access. Logging should..." o For sections 5.5, 5.6, 5.7 and 5.10 Minnesota Power recommends that the Medium Impact column match section 5.1. Since 5.1 requires restricted access, that implies that authorization needs to exist for access as well as access review, revocation, and visitor escorting procedures.Minnesota Power generally agrees with the proposed Requirements R6, but recommends changes as follows: o Requirement R6 discusses preventing and/or detecting unauthorized physical access to BES Cyber Systems while the sections of Table 6 discuss “physical access control systems.” This inconsistency creates confusion regarding what should be included in the physical security plan(s). o Regarding Table R6, Minnesota Power recommends changing “areas protecting” to “areas containing BES Cyber Systems” to reduce ambiguity and confusion. o Parts 6.1, 6.2, and 6.3 of Table 6 refer to the “physical access control systems” identified under Requirement R5, Part 5.1, 5.2, 5.3,” but R5 does not identify or use the term “physical access control systems.” Rather, it requires restricting, monitoring and logging physical access and does not require an access control system to do so. Certainly, as a result of its analysis and implementation of Parts 5.1, 5.2 and 5.3, a Registered Entity may implement an electronic system for access control, monitoring and logging, but it is not explicitly required. These parts should be reworded to state that if the Registered Entity has implemented an electronic physical access control system, then these requirements apply.
15.27	NextEra Energy Corporate Compliance	Disagree	NextEra believes it is not specifically clear what relations the different requirements have for the Medium Impact BES systems. For example, 5.1 requires that physical access be restricted, however, it would appear that this access does not need to be logged, authorized, or reviewed in 5.4 through 5.6. Similarly, 5.9 requires revocation of this

#	Organization	Yes or No	Question 15 Comment
			restricted access which may not have been authorized. We believe that R5 needs further clarification.Also, provide clarity regarding 5.1 "External connectivity only" requirement in Medium Impact column. For a site with Medium Impact BES Cyber systems, why would access not be restricted only if the BES Cyber Systems had no external connectivity. Granting access to the site may result in same impact once the individual is at the site as if they had remote connectivityRegarding R5 & R9 - 24 hour revocation requirement “for cause”, technical infrastructure does not support wide scale user administration to revoke cyber access within 24 hours. User administration for site cyber devices is not centralized. NextEra suggests providing specific definition of “revocation of access” to specify physical / cyber access. For example, if an individual has cyber access only and physical access and remote access to the systems is removed, this effectively revokes access. Regarding R5 & R9, what triggers “for cause” termination / no longer requires access?There needs to be consistency of administration in the industry. What starts the 24 hour clock?NextEra believes it should be at the point where the decision is officially entered into the system and/or communicated to the individual no longer requiring access.
15.28	Consultant	Disagree	NOTE: The format of these two requirements and tables is better than that for Requirements R1 through R4. For R5 & R6 the 'requirement' states the objective and the table specifies the required activities.R5 & R6 - The wording to implement the criteria in the tables is incorrect. The tables are specifying the requirements and application of requirements to the classes of assets resulting from the impact categorization process. The wording of the statement should be modified to reflect this distinction.R6. A physical security plan does not "prevent or detect unauthorized physical access..."It appears that R6 is misidentified as Physical Security Plans, when it seems to address protection for cyber systems providing physical protection to BES Cyber Systems.Based on the reconfiguration of the requirements in this standard a physical security plan is not necessary to meet the requirements.Suggest this requirement be restated to replace the term "Physical Security Plans" with "Protect Physical Access Control Systems" Table item 6.1 would require protection of cyber systems performing the functions identified in Table R5 items 5.1, 5.2, and 5.3 (See next comment regarding deleting 5.2).Table item

#	Organization	Yes or No	Question 15 Comment
			6.2 would require protection of cyber systems performing logging functions for physical access points.Table item 6.3 would require implementation of a maintenance & testing program for the assets identified in 6.1 & 6.2.A better option would be to include in Attachment 1 a function that relates to physical access control systems as part of the BES Cyber System identification. Such as:Physical Access Controls - activities, actions and conditions necessary to restrict and to log physical access to BES Cyber Systems. This would allow items 6.1 & 6.2 to be deleted, and the protections for "BES Cyber Systems" to apply to the physical access control cyber systems. Should the maintenance and testing requirements apply to BES Cyber Systems identified during the identfication and categorization proces, including those that are used to control physical access?
15.29	Garland Power and Light	Disagree	o Requirement 5.10 - clarify that continuous escort does not include entering bathroom facilities - some bathrooms are small non-partitioned one room facilities and it is inappropriate for escort in such areas.
15.30	PacifiCorp	Disagree	PacifiCorp generally agrees, except R5.9 should be expanded to control centers as well, and R5.8 should be removed. There is not a significant or compelling reason for different deadlines which add to the complexity of the standards and the administrative workload to parse the circumstances of each revocation.Define Physical Access Control Systems and ensure the controls in others requirements are suitably applied to those components.
15.31	Progress Energy (non-Nuclear)	Disagree	PE agrees with the 24 hour timeline for access revocation for employees terminated for cause, however it believes this will continue to pose a considerable challenge to many in the industry for its contractor population and would suggest “upon notification” be added to the beginning of the sentence. Thus, Section 5.7 would read, “Upon notification, revoke authorized unescorted physical access to areas protecting BES Cyber Systems within 24 hours for personnel terminated for cause.”PE disagrees with content set forth in R5.8 and R5.9 and believes it will be difficult for many entities to meet and likely result in significant violations throughout the industry. PE suggests language be added to include “upon notification” for both sections and change 36 hours to 48 hours

#	Organization	Yes or No	Question 15 Comment
			for Control Centers so that Section R5.8 reads: "Upon notification, revoke authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 48 hours," and Section R5.9 reads: "Upon notification, revoke authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 72 hours."5.1 implies that we could have a cyber component without external connectivity. 5.7 revocation of access within a 'hours' timeframe implies that the access would be controlled through a security group with 24/7 coverage. Other requirements appear to be in line with requirements of previous standards.CIP-011 R5.7 thru .9 what is the decision process to be used to determine "when job duties no longer require ... access"? What would be suitable compliance evidence that is to be collected that indicates "when job duties no longer require access" as this is critical in determining if revocation has been accomplished within the mandated 1 hour, 4 hours, 6 hours, 24 hours, 36 hours, 72 hours?Need clarification on period allowed for revocation of access due to expiration of training of background check - recommend that this be included with 5.8, 5.9 (no longer require access - or fail to meet necessary criteria).R5.7 - poor wording "handle...access attempts" Propose: "process such physical..."
15.32	Allegheny Energy Supply	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls.
15.33	Allegheny Power	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls.

#	Organization	Yes or No	Question 15 Comment
15.34	EEI	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls.
15.35	MidAmerican Energy Company	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls. Define Physical Access Control Systems and ensure the controls in others requirements are suitably applied to those components.
15.36	Oncor Electric Delivery LLC	Disagree	Physical security at remote substation sites is not cost effective in preventing/detecting cyber attacks. Remote substations with only dial-up communications cannot support the 24-hr time frame of Requirement 5.7 when systems are non-functional (phone line damage, etc). Five to seven days may be required, depending whether some communication system has been installed to the facility. Physical security should only be required at control centers and High impact substations with IP based communications.
15.37	American Electric Power	Disagree	Please see comments as provided in response to Question 15.
15.38	Puget Sound Energy	Disagree	Puget Sound Energy has the following suggested changes:Table 5:5.3 - Suggest changing to “Logging shall record sufficient information to uniquely identify known individuals, or assist in the identification of unknown individuals, and the time of access...”Table 6:6.1/6.2 - Puget Sound Energy would like clarity on how restricting physical access to areas protecting control or monitoring systems for physical access protects the BES Cyber Systems. Physical protection of the BES Cyber Systems (Table 5) is understandable to protect the BES. But, a malicious or inadvertent act solely against the Cyber Systems that provide physical security in no way impact the BES or the Cyber Systems that make

#	Organization	Yes or No	Question 15 Comment
			up the BES unless the physical location of both types of Cyber Systems is the same.6.3 - Puget Sound Energy requests clarity on "...of all physical security mechanisms...". Like many entities, Puget Sound Energy employs physical security measures that are made up of components that do not use routable protocols. Is 6.3 suggesting a full test of all mechanisms (routable protocol or not) involved in restricting, monitoring, and logging? (Ex: card key strikes at doors)
15.39	LCEC	Disagree	R5 - and/or should simply read or. "To prevent and/or detect unauthorized physical access" should read "limit access to authorized personnel through detection and prevention."Medium impact for "external connectivity only" doesn't make sense from a physical security perspective. Change to Control center only.Move 5.8 and 5.9 to 5.7 and base the timings on whether or not it is a control center. CC should be 36 hours and others should be 72 hours.5.5 should be required for Medium as well since there is a requirement to revoke access in 5.8 & 5.9The term "areas protecting" is confusing and should be replaced with "areas containing" BES Cyber Systems.Please consider identifying at what level of access granting must be removed to sufficiently mitigate the personnel risk.R6 Need to clarify "required for routable connectivity only" in regard to physical security controlsMost physical security systems do not require preventive maintenance which makes it difficult for an entity to provide a basis for maintenance performed. Testing is also a challenge because these systems either work or they do not work. What is the intent of the testing and maintenance requirement? Can this requirement be better served by reviewing the configuration of the system and comparison to approved access lists?
15.40	Southwest Power Pool Regional Entity	Disagree	R5 does not address the expectations of FERC Order 706 and subsequent orders. 5.3 needs to include both ingress and egress. 5.4 needs to include identification of the escort staff. 5.3 and 5.4 could be combined. 5.7: The time to revoke physical access can be much faster for control center environments; suggest 2 hours for the control center and 8 hours elsewhere. Ideally, the person's primary access credentials (badge, keys, etc.) should be lifted and access revoked concurrently with the person being notified of the termination for cause. 5.8 and 5.9 can be combined and the timeframe should be

#	Organization	Yes or No	Question 15 Comment
			expressed in business days. 5.10: define "continuous escort" somewhere. R5 overall: consider defining the concept of specifying an "effective date" of a transfer that reflects the reality that often a transferred employee will back fill or support the losing department for a period of time after the HR date of the transfer. 6.3 needs to be much more frequent in a control center environment where the inspection program can be readily performed; weekly is suggested. Additionally, the frequency needs to be commensurate with the impact category regardless of site characteristics.
15.41	ISO New England Inc	Disagree	R5.1 in table 5 please defined what is meant by external connectivity. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?R5.8 and 5.9 Is the 36 hours or 72 hours from the time the access is reviewed? Or is it that access should be reviewed within 36 hours of personnel that change job responsibilities, transfer, etc. Then require access be modified based on the review. Suggest changing the 36 hours to 72 hours. If a transfer were to occur on a Friday at 5 pm then access would need to be reviewed by Sunday.
15.42	Western Area Power Administration	Disagree	R5.2: What is the definition of "monitoring" physical access? Since the concept of the physical security perimeter has been dropped, what specifically is meant by "access to areas protecting BES cyber systems? What constitutes sufficiency in monitoring?R5.3: What constitutes sufficient logging? Is a self-written logbook sufficient? Does logging have to be performed electronically or by a third party if manually logged, or is self-logging sufficient?R5.5: How does 5.5 differ from the requirements of R4?R5.7: Can be very difficult if someone is terminated on a Friday afternoon. Communication is very critical and requires more people knowing in advance, which in itself may cause an additional risk. R5.8: 36 hours could be an issue on 3 day weekends. Suggest 48 hours. Then is will only be an issue at Thanksgiving.R6, 6.3: Needs more guidance on testing and maintenance program what they must cover besides a blanket statement of testing and maintenance of all physical security mechanisms. Shouldn't we follow the installers or manufacturers recommendation on this? Documentation of these tests and maintenance evidence should be kept for how long?R6: what is meant by "routable

#	Organization	Yes or No	Question 15 Comment
			connectivity only"?
15.43	Kansas City Power & Light	Disagree	R5.3: What does "sufficient information" mean? This may encourage too much interpretation and recommend some clarity in the Table R5.R5.10: How do you prove someone who requires an escort was escorted at all times? From an audit perspective this is "proving the negative". It is understood what is intended in this requirement, but this is not measurable or auditable.R6.1 through R6.3: qualification here of "routable connectivity only" is not clear with respect to physical access controls. Routable implies electronic security measures rather than physical.
15.44	Con Edison of New York	Disagree	R5.8 and R5.9 - Add the words "Required for" before "Control Center" or before "Generation or Transmission Facility".R5.1 Need clarification to this item. If I have an enclosure which secures and isolated my cyber system, do I need to restrict access into the enclosure or do I need to restrict access to the area around the enclosure?R5.6 - Quarterly reviews are excessive. Annual or bi-annual would be reasonable.R5.9. - Should be business days, for example 3 business days. Support staff may not be available 24/7 to do this work.R5.10 - Continuous escort access is not practical in the numerous substations. The requirement should be relaxed to say oversight or supervisor, or any other mean which will limit the total escort and allow the operator to perform tasks while people may come to the station.R5.1 Medium Impact; not sure what external connectivity means? R3 clarification may resolve this.R5.8 (and others) - 36 hour requirements for compliance criteria will be a challenge
15.45	San Diego Gas and Electric Co.	Disagree	R5.8 and R5.9 require revoking authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 36 hours for medium and high impact control centers and within 72 hours for medium and high impact generation or transmission facilities. CIP-006-2 R1.5, by reference to CIP-004-2 R4, currently requires such revocation within 7 days for all PSPs. Revocation within 36 or 72 hours will be much more difficult to capture, especially for internal personnel reassignments. SDG&E believes that the risk to BES Cyber Systems associated with reassignment of an employee does not justify the effort (and potential non-

#	Organization	Yes or No	Question 15 Comment
			compliance) associated with this change. These time-periods approach the 24-hour limit for personnel terminated for cause in CIP-006, which does carry genuine risk to BES cyber systems.R6.1 and R6.2 in CIP-011-1 concern restricting and monitoring physical access to "areas protecting physical access control systems". Does this mean areas equivalent to PSPs have to be set up around these physical access control systems? Currently, CIP-006-2 R2 and R2.2 concern protection of "cyber assets that authorize and/or log access" to PSPs. Thus, server racks and control panels are locked and monitored, but PSPs are not required around these systems.
15.46	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R5.8 and R5.9 should be extended to 72 hours or next business day, whichever is longer, to allow for communications for this circumstance. A late Friday occurrence could be addressed early Monday instead of over the weekend.
15.47	Dominion Resources Services, Inc.	Disagree	R5.8 and R5.9. To meet regulatory directives, if job duties are changed due to disciplinary actions or are "forced" on the user, then a shorter time frame to revoke access may be necessary. However, the current 24 hour time period is the least time period that can be reasonably accommodated through the business processes.Requirement R4 establishes the process for personnel risk assessments. This practice determines the loyalty, reliability and trustworthiness of an individual as a prerequisite to authorizing logical or physical access. This is a standard practice used throughout the physical and cyber security industry and accepted by other regulatory agencies and Federal programs. Similar to R4.3, personnel risk assessments typically must also re-validate this trustworthiness periodically - commonly within 7 years and in some cases more frequently depending on the nature of the access. The presumption is that, once trustworthiness is established, it is not invalidated unless there is cause to reconsider or an individual voluntarily terminates their employment or retires. Only in instances where the established trustworthiness is in question, is prompt access revocation appropriate and warranted. Consequently, for personnel who "no longer require access", but for which there is no cause to question their trustworthiness, there is no basis for immediate or prompt revocation of access within the time frames

#	Organization	Yes or No	Question 15 Comment
			specified in this standard. The DHS Catalog for Control System Security Controls, Sections 2.3.4 and 2.3.5 reflect this practice - requiring revocation of access for cause within 24 hours and revocation of access for personnel reassigned or transferred to another position within 7 days. In other regulatory programs, revocation of access, not involving a question of change in trustworthiness, is handled via a periodic (e.g., monthly) review of access only. The 7 day requirement in the current standards would meet or exceed standard practice in this case. The requirements should be clarified to state that if there is no triggering event indicating that access is no longer required, then that determination should be made at the quarterly review.
15.48	ERCOT ISO	Disagree	Recommend moving requirements 5.5 through 5.9 to a common access management section which addresses cyber access and information access. The remaining parts of Requirements R5 and R6 could be combined.
15.49	US Bureau of Reclamation	Disagree	Requirement R5: Physical security requirements are not adequately addressed in the present Standard. Much of the language from the previous version of the Standard should be re-established in version 4. In addition low and medium systems should include the equivalent of a 6-wall boundary around the cyber systems.Requirement R6: Physical security plans should be required for more than just electronic physical access control systems.
15.50	Progress Energy - Nuclear Generation	Disagree	See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
15.51	Xcel Energy	Disagree	The 36 and 72 hour timeframes to revoke unescorted physical access for individuals no longer requiring access under 5.8 and 5.9 are not justified. When the change is for a business reason such as a job change 7 days is sufficient for access removal. When the access change is unrelated to a termination for cause, the individual's trustworthiness and reliability are not in question and the short timeframes are not needed. "Restrict physical access" in Requirement 5.1 also needs further definition. Does this mean locks?

#	Organization	Yes or No	Question 15 Comment
			Fencing?There appears to be inconsistencies between R5 and R6. Specifically;1) Table R5, R5.1 applies to Medium impact systems with external connectivity, while Table R6 6.1 applies to Medium impact systems with routable connectivity. 2) Table R6 refers back to 5.1, 5.2, and 5.3 for Medium impact systems, however 5.2 and 5.3 do not apply to Medium impact systems.
15.52	GTC & GSOC	Disagree	The 36 hour requirement for a person who no longer needs access (R5.8) is too stringent. If a transfer or retirement occurs on a Friday there is no reason you cannot wait until Monday. We recommend changing this to "within 36 hours or the next business day, whichever is greater".
15.53	APPA Task Force	Disagree	The APPA Task Force recommends the following edits to R5-R6:R5. Objective:To prevent and/or detect unauthorized physical access to BES Cyber Systems.R5. Requirement:Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R5 - Physical Security for BES Cyber Systems." R6. Objective:To prevent and/or detect unauthorized physical access to BES Cyber Systems.R6. Requirement: Each Responsible Entity shall document and implement one or more physical security plans that apply the criteria specified in CIP-011-1 Table R6 - Physical Access Control Plans
15.54	Bonneville Power Administration	Disagree	The objective of these requirements ("to prevent and/or detect unauthorized physical access to BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action(s) that the Responsible Entity must take.The objective of R5 and R6 should be changed to read "to prevent and detect unauthorized physical access to BES Cyber Systems." They should not say "and/or". Isn't the objective to prevent unauthorized physical access to BES Cyber Systems and to detect unauthorized physical access to BES Cyber Systems?R6: The entries in Table R6 refer to "Part 5.1, 5.2, 5.3". It is unclear whether these refer to subrequirements R5.1, R5.2, and R5.3, which do not exist, or in Table R5, entries 5.1, 5.2, and 5.3.5.7-5.9 refer to timeliness of revocation. Twenty-four hours for terminations for

#	Organization	Yes or No	Question 15 Comment
			cause is reasonable, however having two additional categories complicates matters and could potentially lead to confusion and someone not revoked in the appropriate category. For 5.8-5.9 this should be the same and be reviewed to take place within 3-5 business days. 5.11 is good in that unauthorized physical access is a procedural violation and not necessarily an incident.
15.55	Exelon Corporation	Disagree	The requirement to revoke access (5.8 & 5.9) in 36/72 hours for personnel who no longer require access is far too severe and places unnecessary administrative burden on the entity without technical or risk analysis justification. This would imply that there is little differentiation between an employee terminated for cause and a person who we regard as a solid member of our organization and in turn, we deem as having integrity. This would also become an undue burden to the business as our employees require transition time to ensure there is reliable transfer of information to the new owner of a role or task. This requirement would make that transition period extraordinarily difficult. Also, the ability to capture and store the transfer data to the hour would be impossible with our current human resource data systems. Modifying this system would result in major expense with little to no stated benefit to BES reliability. Exelon's position is that the current 7 day requirement is reasonable from a technical and risk perspective. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
15.56	Ameren	Disagree	The short period of time to remove access for 5.8 does not extend well across weekends or through the 2nd business day in cases where access is no longer required at the end of the day. Suggest that this requirement be extended to a week to remain in line with current CIP standards. This will allow for proper hand off time in cases where job duties need to be transferred. Also, R6 should be a stand alone requirement, remove circular reference to R5.â€,
15.57	Pepco Holdings, Inc. -	Disagree	We agree with EEI's comments.

#	Organization	Yes or No	Question 15 Comment
	Affiliates		
15.58	Entergy	Disagree	We disagree with 5.1 "Restrict physical access to areas protecting BES Cyber Systems" for Medium Impact BES Cyber Systems with external connectivity only. What difference does it make if the physical security of Medium Impact BES Cyber Systems access is restricted to the Physical Security Perimeters if the access mode to be protected is external, but there is no other requirement to monitor, or log access into or out of the PSP for these cyber systems.How can access be revoked from a Medium Impact BES Cyber Systems if there is no requirement to monitor or log access in and out of the PSP? There seems to be conflict with these requirements. Remove the requirements 5.1, 5.7 and 5.8 for Medium Impact BES Cyber Systems.Instead of having different access revocation time frames for High Impact BES Cyber Systems based on the locations as described in requirements 5.7, 5.8 and 5.9 it would be easier to manage evidence for compliance if all locations was the same. During the Dallas CIP Workshop it was apparent that the SDT was struggling with the interval for access revocation. It is suggested that the revocation of physical access for employees terminated for cause be by the end of the business day the first normal business day after the employee is terminated i.e. if the entities normal business week is Monday - Friday 8:00 - 5:00 and an employee is terminated Friday to Sunday then revocation should be completed prior to 5:00 on Monday for all High Impact BES Cyber Systems regardless were the cyber systems is located, control center, transmission facility or generating station. This would provide a consistent method of tracking the access revocation across the entities facilities and reduce requirements and potential compliance shortcoming and reduce the vulnerability of not taking actions to terminate employees for cause if the 24 hour requirement cannot be achieved on the weekend and the termination be held off until the normal work week when the requirement can be met.
15.59	We Energies	Disagree	We Energies agrees with EEI comment: Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to

#	Organization	Yes or No	Question 15 Comment
			determine the components that may need additional controls.
15.60	PNM Resources, Inc.	Disagree	We would prefer that all accress granting and revocation, for physical and logical access, be identified in a single table. In the current draft, they are scattered through several unrelated requirements.

16. Tables R5 and R6 provide direction concerning what impact level of BES Cyber Systems to which Requirements R5 and R6 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Some commenters expressed concern that the electric industry already physically protects its cyber assets from the public for reliability, business, and safety reasons, and that making physical security a standard requirement for Low Impact BES Cyber Systems creates an additional compliance burden that does not contribute any additional reliability to the Bulk Electric System.

Each Responsible Entity is required to ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. The SDT has revised CIP-006-5 R1 to define the requirements for physical protection for Low, Medium, and High Impact BES Cyber Systems. While the requirements place the emphasis for physical protection on the High and Medium Impact BES Cyber Systems, each Responsible Entity's Physical Security Plan is required to address how it will protect Low Impact BES Cyber Systems.

Some commenters also expressed concern that there appears to be a discrepancy in the Medium Impact category, where there could be sites that are not required to restrict access because there is no external connectivity, but they are required to revoke access. The SDT has revised these requirements and has removed the consideration for external connectivity from the applicability portion of this requirement, such that all Medium Impact BES Cyber Systems are required to have a Physical Security Plan. The revocation of access requirements are enumerated in CIP-005-5 R7, and have eliminated the identified potential for conflict.

Some commenters expressed disagreement with the requirements for restricting, monitoring, and maintenance testing for systems that provide physical access control over Medium BES Cyber Systems, when there is no requirement to monitor or log access into a Medium BES Cyber System. This likely is a conflict with the requirements for Medium BES Cyber Systems. The tables need to document basic physical security requirements for all Low and Medium Impact BES Cyber Systems. The SDT has revised the requirements for physical and electronic access for Low, Medium, and High Impact BES Cyber Systems to address these concerns. These requirements are stated in CIP-005-5 and CIP-006-5.

#	Organization	Yes or No	Question 16 Comment
16.1	American Municipal Power		Please provide a little or no impact category.
16.2	Regulatory Compliance	Agree	BUT:5.1 Medium Impact - "Required" only.

#	Organization	Yes or No	Question 16 Comment
16.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Blanks are ambiguous. If Low Impact is “Not Applicable”, then the blanks should be replaced with “NA”FMPA recommends making more clarity to the terms “required for external connectivity only” or “required for routable connectivity only” with: “required for areas containing BES Cyber Systems with routable external connectivity”FMPA believes that even Low Impact BES Cyber Systems should have restricted physical access and believes 5.1 ought to be applicable to Lower Impact “for areas containing BES Cyber Systems with routable external connectivity”R6 assumes card access and a “physical access control system” where the physical access may be restricted through lock and key (especially in substation environments for Medium Impact) and monitored through an alarm signal of a substation control house door opening through a SCADA system. It is unreasonable to require testing of simple padlocks or door-locks in 6.3.Maintenance of such system in 6.3 is unreasonable. Such electronic systems are usually just tested on a periodic basis and maintained as necessary. And, we assume that use of the system is testing the system. If not, what type of testing would be required in 6.3?
16.4	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
16.5	Manitoba Hydro	Agree	Manitoba Hydro agrees that physical security is not a standard requirement for Low Impact BES Cyber Systems, and should not be auditable. The electric industry already physically protects its cyber assets from the public for reliability, business and safety reasons. Making physical security a standard requirement for Low Impact BES Cyber Systems creates an additional compliance burden which does not contribute any additional reliability to the Bulk Electric System.
16.6	San Diego Gas and Electric Co.	Agree	Most of the requirements in Tables R5 apply to “high impact” BES cyber systems. Table R6, dealing with physical access control systems, applies to medium impact systems with

#	Organization	Yes or No	Question 16 Comment
			routable connectivity and high impact systems. This seems reasonable, but the scope will depend on what SDG&E determines will fall into these impact levels. Except as noted in the comments for Question no. 15, there are no apparent increases in physical security requirements for covered systems.
16.7	NextEra Energy Corporate Compliance	Agree	NextEra agrees but would like clarification regarding "Required for routable connectivity only" on Medium Impact physical access control systems. Also, as written, the standard does not have consistency in application of the different requirements as noted above.Also, in 5.11, how is the "unathorized physical access attempt" defined? Should this apply to all attempted access card swipes for electronic access systems. We do not believe that application of the incident response plan should apply to attempts such as these at the physical boundary. We believe a tie to suspicious activity threshold or physical boundary damage may be a better definition.NextEra also questions table R6, do training and PRA requirements apply to individuals with access to Physical Access Control Systems for BES Cyber Systems?
16.8	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 12.
16.9	Northeast Utilities	Agree	Suggest merging 5.8 and 5.9 and using 72 hours for the allowable revocation period for all personnel terminated not for cause.
16.10	Minnesota Power	Agree	With the implementation of the changes and clarifications described in Question 15, the impact levels seem reasonable.
16.11	Independent Electricity System Operator	Disagree	- For R 5.8 and 5.9, if restricting physical access is not required for Medium impact assets (R5.1) then why does access need to be revoked?
16.12	PacifiCorp	Disagree	: PacifiCorp agrees with EEI's observations below:Table R5 Row 5.1 needs to document basic physical security requirements for all low and medium BES Cyber Systems.Table R5

#	Organization	Yes or No	Question 16 Comment
			Row 5.2: There should be additional language describing what “Monitoring” means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a particular item or location.Regarding Table 6, it is unclear what the benefit is for having requirement differentiation for Medium BES Cyber Systems with routable connectivity vs. those without.Table R6 Row 6.3, it is appropriate to validate those basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.13	Madison Gas and Electric Company	Disagree	: Recommend 5.3 to use the same wording as 5.4 concerning logging access. This would reduce any confusion and provide uniform outcome to each sub requirement. Recommend 5.3 to read:”Log (manual or automated) ...” 5.7 states “Revoke authorized unescorted physical access to areas protecting BES Cyber Systems within 24 hours for personnel terminated for cause”. It may be possible to turn off someone’s electronic access but if there are combination locks, key locks, etc, this may not be possible to accomplish within 24 hours. This also applies to 5.8 and 5.9..
16.14	National Grid	Disagree	1. 5.1 - for Medium Impact BES CS, is it external connectivity with both routable and non-routable protocols? Please specify.2. There appears to be a discrepancy between 5.1 vs 5.7 & 5.8 in the Medium impact category. There could be sites that are not required to restrict access per 5.1 because there is no external connectivity. But, they are required to revoke access per 5.7 & 5.8. Could this be clarified?3. Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9.4. In 5.11, is the SDT considering providing the timeline for reviewing any unauthorized physical access attempts?5. Should the “routable connectivity” be “external connectivity” or “external routable connectivity” for Requirements 6.1, 6.2 and 6.3?
16.15	Consultant	Disagree	5.1 Physical access "Required for External Connectivity Only" is not logical. Suggest rewording to clarify.It is not clear why the change from Physical Security Perimeter to

#	Organization	Yes or No	Question 16 Comment
			the words "areas protecting BES Cyber Systems" makes sense. The new wording is not as clear and removes what was a "bright line". Suggest retaining the Physical Security Perimeter term in this version of the standards. 5.3 As this is currently stated it would appear to require monitoring and logging of both ingress & egress from "areas protecting BES Cyber Systems". Based on the discussion at the workshop, this is not the intent of this requirement. If that is the case then the wording should be modified to reflect the intent. 5.2 and 5.3 The distinction between "logging physical access" and "monitoring physical access" is not clear. If access is logged, then by default it has been monitored. Suggest deleting 5.2, or clarifying the difference between monitoring and logging in this context.5.4 The parenthetical after the word visitors is a definition, and as such should be listed as a definition, rather than being embedded in the requirement statement.5.4 Suggest replacing "to and from" with "entry and exit" or "ingress & egress". A more logical sequence of the requirements list by topic flow would be 5.1, 5.5, 5.3,5.2(see above comment), 5.4, 5.10, 5.7, 5.8, 5.9, 5.6.5.7, 5.8, 5.9 - Personnel transactions are typically measured in days. Setting a requirement in hours for a transaction that is not recorded at that level will create compliance problems. Suggest checking with the nuclear industry about time frames for access revocation. The answers there would be based on over 30 years of regulatory scrutiny.5.8 & 5.9 - There is no difference for personnel transactions based on the facility type, so creating a differential time frame for revocation by facility type would seem to imply that some facilities have less impact than other facilities outside of the impact categorization criteria. Suggest the access revocation time frames should be consistent based on the impact categorization, or adjust the impact categorization criteria to be consistent with the listed revocation time frames. The current table would imply that control center are high impact, and generation and transmission facilities are medium impact.5.11 Suggest deleting the word "any" as the current wording is unnecessarily restrictive. For example, the current wording implies that a single "bad swipe" of an access card should be reviewed, while entities typically have defined 3 to 5 consecutive bad swipes as an adverse event.5.1, 6.1, 6.2 & 6.3 - These table items create another dimension to the impact categorization process. If an asset has been categorized as Medium Impact, it should be afforded the

#	Organization	Yes or No	Question 16 Comment
			same level of protection as any asset categorized as Medium Impact. If the asset does not require the same level of protection then the impact categorization criteria should be adjusted to have it excluded from that impact level.
16.16	US Army Corps of Engineers, Omaha Distirc	Disagree	5.1 unclear why medium impact for "required for external connectivity only." Does this only apply to external connectivity hardware or is it for systems with external connectivity only? 5.8 & 5.9 are inconsistent with 5.5 granting of access is not required for Medium impact BES Cyber Systems.
16.17	Reliability & Compliance Group	Disagree	5.1, 5.5 and 5.8 are contradictory. They make you restrict and revoke access to medium impact systems but how do you do that if you don't have to authorize access to medium impact systems?Also, table R6 contradicts table R5 with regard to medium impact systems.
16.18	ERCOT ISO	Disagree	5.1: Please clarify why "Required for external connectivity only" is specified for medium impact BES Cyber System. 5.2-5.7: Should apply to medium impact BES Cyber System.5.10-5.11: Should apply to medium impact BES Cyber System.6.1-6.3: Please clarify why "Required for external connectivity only" is specified for medium impact BES Cyber System.
16.19	Dairyland Power Cooperative	Disagree	5.11 seems to say that known physical security incidents can be ignored for low and medium impact systems. This seems wrong. If a non-routable protocol terminates at some other facility, it seems there potentially should be physical access controls for that other facility as well-perhaps this would be required for high impact systems.
16.20	LCEC	Disagree	5.5 should be required for Medium as well since there is a requirement to revoke access in 5.8 & 5.9R6 Need to clarify "required for routable connectivity only" in regard to physical security controls
16.21	Duke Energy	Disagree	a) CIP-011-1 Table R6 is identified as applying to "Physical Access Control Systems" but is very confusing to understand as written because the columns describe levels of impact

#	Organization	Yes or No	Question 16 Comment
			to the BES Cyber System but there are no impacts if the Physical Access Control System is operated on a network that is separate and distinct from the SCADA system. Is that the intended interpretation?b) Table R5 Physical Security for BES Cyber Systems state that requirement 5.1 applies only to Medium Impact BES Cyber Systems with "...External Connectivity Only". Does this mean that since 5.1 only requires restricting access to BES Cyber Systems; an acceptable method would be mechanical lock and key control?c) Table R6 Physical Access Control Systems state that Medium Impact BES Cyber Systems requirements R6.1, R6.2 and R6.3 for physical security are "Required for Routable Connectivity Only". Does this mean "Routable Connectivity" of the BES Cyber System or Physical Access Control System?d) Was the access control system intended to be included or intended to be excluded if it is on a separate network and not connected with any BES Cyber Systems? e) General Comment: V4 Tables R5 & R6 are very vague and unclear as to what is required. We would suggest additional wording to provide clarity as to what is intended for the responsible entity to physically meet R6.1, R6.2 and R6.3For Table R5, we propose the addition of "for external connectivity only" in the high impact column. Same for Table R6. Suggest changing "routable" in the table to "external" in Table R6Remove requirement for Medium impact in 5.1. Remove requirements for Medium Impact Systems in Table R6Requirement R6, Medium Impact: allowances should be included to exclude BES cyber systems which incorporate one way connectivity (e.g. outside the ESP via a one way hardware device), even if the protocol is routable. This would be in addition to the existing non-routable protocols.
16.22	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.5.8 - 5.10 is the first of many occurrences where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any

#	Organization	Yes or No	Question 16 Comment
			distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
16.23	Southwest Power Pool Regional Entity	Disagree	At a minimum, access revocation should extend to all impact categories. Access to a BES Cyber System is an available attack vector. 5.2: Restricting access without monitoring access is an ineffective control; 5.1 is not auditable in the absence of some sort of verification that the control is in place. 5.3 needs to consider that automated logging systems cannot guarantee 100% up time. Consider adding a requirement for recognizing the automated process has failed and responding to the failure (not the same as repairing the failure, which will be situation dependent. 5.11: There should be a clearly defined maximum timeframe for reviewing unauthorized access attempts. Simply leaving it to the discretion of an entity's incident response plan is not an effective control. R6: The Cyber security plan applicability will need to be updated to reflect any changes to the R5 applicability matrix.
16.24	US Bureau of Reclamation	Disagree	At a minimum, physical security controls should be required for low and medium systems, even if it is just a lock on the door.
16.25	FirstEnergy Corporation	Disagree	CIP -011-1 Table R5- Physical Security for BES Cyber SystemsItem 5.1: Should specify minimum expectations regarding how physical access should be restricted. There appears to be not difference in the level of security required for Medium and High impact facilities.Item 5.8, 5.9: Why two different revoke authorized unescorted physical access time periods to complete this task? It should be consistent for Control Centers, Generation and Transmission sites to revoke access in one time period to revoke access when no longer required. As stated this is open for confusion and separate corporate polices and procedures for personnel to train, track and manage. If desired to separate time frames it should be based on Low - Medium - High impacts which is not reflected.Additionally, we do not agree with the shortened time frame to revoke access to those who no longer require access -what justifies change? It should remain consistent with current CIP Ver 2 - Certain business processes and day to day operations will cause unrealistic burden in tracking from manual or automated process to revoke

#	Organization	Yes or No	Question 16 Comment
			access for no cause in shortened time frameItem 6.1 Should specify minimum expectations regarding how physical access should be restricted. There appears to be not difference in the level of security required for Medium and High impact facilities.
16.26	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
16.27	Ameren	Disagree	Due to the scope of the number of medium facilities it will be burdensome and labor intensive to maintain documentation of R5.1 physical security controls with no added protection to the BES. Suggest removing Medium Impact Systems from R5.1.
16.28	Entergy	Disagree	Entergy disagrees with the requirements 6.1, 6.2 and 6.3 to restricting, monitoring and maintenance testing to the systems and provide physical access control over Medium BES Cyber Systems when there is no requirement to monitor or log access into a Medium BES Cyber System, again there is a conflict with the requirements for Medium BES Cyber Systems. High BES Cyber Systems access for unescorted access and visitors alike logged and monitored for ingress and egress. If a systems is going to put in place to monitor egress for visitors then the same system could monitor unescorted personnel as well, this would reduced the maintenance of logs for visitors verses unescorted should be into and out unescorted and visitor alike for HIGH BES Systems should have a very high degree of control including the security systems providing access and monitoring.
16.29	Southern Company	Disagree	For 5.1, More specificity is probably called for here. What standard of care is called for? What does “protecting BES Cyber Systems” mean? Does it just mean “containing”?In 5.2, what are the boundaries of “monitoring”? Does this require real-time observation, alarm response, or after-the-fact review? What constitutes monitoring?5.5 “Authorize” should be replaced with “Control” or “Place limits on”.5.9 creates a responsibility for an Entity to monitor the employment status of all of its contracting companies; the requirement should be eliminated, changed to cover employees only, or changed to 72 hours from notification by contracting company.There is a need for greater differentiation based on connectivity and BES component types in R5 and R6. Having

#	Organization	Yes or No	Question 16 Comment
			one set of physical security standards for the differing types of BES components leads to trying to implement standards in an environment to which they are not suited - for example, several of the requirements do not make sense in a substation environment. The tables for R5 and R6 should be reviewed on a per-requirement basis to take these differences into account.
16.30	MRO's NERC Standards Review Subcommittee	Disagree	For item 5.1, we propose making the Low Impact and Medium Impact criteria "Required". Restricting physical access is something that should, and is probably already, being carried out almost everywhere in the BES. Physical security is one of the first lines of defense for all facilities, but the most important defense for those facilities without routable external connectivity.For item 5.2 through 5.11, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability. This approach builds consistency within R5 and R6.Item 5.3 requires entities to "log" access, and item 5.4 requires entities to "log (manual or automated)" access. Either item 5.3 should define the scope of "logging" access, or "manual or automated" should be deleted from item 5.4 because "log" by itself could already indicate either manual or automated processes.For item 5.7, since termination with cause could occur without warning, revoking access within 24 hours may not be practical at distributed locations without routable external connections, where changes may need to be implemented locally. We would propose including a longer timeline for areas without routable external connections. We also believe a two tiered approach would be practical, where personnel specific access devices (manual keys, key cards, etc.) are removed immediately, and then wide scale access changes (shared combination locks, etc.) are allowed more time to be addressed. We believe this approach is similar to that of the NRC.For items 6.1 - 6.3, we would propose all Medium Impact criteria to be changed to "Required for routable external connectivity only", to maintain consistency with existing wording within the standard.For items 6.1 - 6.3, the drafting team may want to consider how these requirements apply to areas without any

#	Organization	Yes or No	Question 16 Comment
			type of automated physical access control system. What if access is simply restricted by keys, manual logging, and door alarms transmitted by the local RTU to a Control Center? This approach would appear to meet the requirements of R5, but would not seem to be applicable to the requirements of R6.
16.31	The Empire District Electric Company	Disagree	For item 5.1, we propose making the Low Impact and Medium Impact criteria "Required". Restricting physical access is something that should, and is probably already, being carried out almost everywhere in the BES. Physical security is one of the first lines of defense for all facilities, but the most important defense for those facilities without routable external connectivity.For item 5.2 through 5.11, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability. This approach builds consistency within R5 and R6.Item 5.3 requires entities to "log" access, and item 5.4 requires entities to "log (manual or automated)" access. Either item 5.3 should define the scope of "logging" access, or "manual or automated" should be deleted from item 5.4 because "log" by itself could already indicate either manual or automated processes.For item 5.7, since termination with cause could occur without warning, revoking access within 24 hours may not be practical at distributed locations without routable external connections, where changes may need to be implemented locally. We would propose including a longer timeline for areas without routable external connections.For items 6.1 - 6.3, we would propose all Medium Impact criteria to be changed to "Required for routable external connectivity only", to maintain consistency with existing wording within the standard.For items 6.1 - 6.3, the drafting team may want to consider how these requirements apply to areas without any type of physical access control system. What if access is simply restricted by keys, manual logging, and door alarms transmitted by the local RTU to a Control Center? This approach would appear to meet the requirements of R5, but would not seem to be applicable to the requirements of R6.

#	Organization	Yes or No	Question 16 Comment
16.32	BGE	Disagree	General: What is an "area"? With the elimination of PSP this leaves "area" up for debate. Provide definition for "monitor" (is this manual, automated, 24x7??). 5.1 - Remove the requirement for medium impacted systems (currently says "required for external connectivity only, this requirement is pertaining to physical access). Combine 5.3 & 5.4 and reword to say "Log the entry and exit of all individuals with access to an area protecting BES Cyber Systems." 5.8 & 5.9 should not be restricted to removal from Control Center Only. This should be "areas protecting BES Cyber Systems" to maintain consistency. Define "Generation or Transmission Facility". Define "invalid access". To what extent does physical access mean, does it mean dispatching a guard for every single invalid access attempt? Under 5.8 access is revoked for Medium and High impacted systems but in 5.11 there is no requirement to review access for Medium impacted Systems.6.3 Physical access control systems were not defined in 5.1, 5.2 & 5.3. Should read "Implementing a maintenance and testing program for systems used to comply with 5.1, 5.2 & 5.3)." Define "physical security mechanism".
16.33	Constellation Energy Control and Dispatch, LLC	Disagree	-In 5.1 remove the requirement for medium impacted systems, which is not appropriate for a requirement pertaining to physical access.-Eliminate the timing differences for revoking access between Control Centers, generation or transmission facilities and use a single timing requirment for access to all BES cyber systems.
16.34	Bonneville Power Administration	Disagree	In general, Table R5 is acceptable, other than the items discussed below.We understand the impact of FERC requiring immediate revocation. However, it is difficult to see how to achieve that in every case. The standard should be based upon what is achievable and reasonable for both routine revocation and revocation for cause. The table should have a closer resemblance to R9.Section 5.8 and 5.9: 36 or 72 hours seems very short for revoking access for people who, presumably, are still trustworthy, but merely no longer need access or who have left the entity under routine circumstances. They simply no longer require access because of a job change. Such revocation should be a routine, normal business-day action. 72 hours does not allow for business-day action during a long weekend. In fact, for a large organization revocation for field assets in such a short

#	Organization	Yes or No	Question 16 Comment
			time period would often be impossible. Recommend changing this to five business days or five calendar days. We also recommend using the same criteria for all assets: Control Center, generation, or Transmission Facility.Section 5.11 is very good: it makes it clear that unauthorized access is an incident, not a violation.Table R6, 6.1-6.3 require the plans to address Part 5.1-5.3 if identified as "Medium". However, 5.2 and 5.3 do not require physical security under "Medium". How can a plan address elements that are not required?
16.35	Idaho Power Company	Disagree	In R5, if access authorization is not required for medium impact systems then why is there a requirement to revoke authorized access if it was never authorized in the first place.
16.36	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
16.37	Southern California Edison Company	Disagree	Local logical (electronic) access is and should be recognized as a type of role based access where one has to be physically present, near a device, to operate it. The boundary protection for this type of role is: (1) the physical security boundary; and (2) the device level electronic security boundary. The proposed standard as it is currently worded allows for the removal of at least one access mechanism at the time of revocation. In that case, removal of access through the physical boundary will ensure the immediate revocation of a component critical for this type of role. The drafting team should add additional revocation criteria to adequately address this type of revocation.While this control is easily implemented in a control center or data center environment, field devices that are often located over vast geographic areas pose compliance challenges. This requirement may result in the creation of substantial organization capabilities for compliance without a comparable improvement in reliability of the BES. SCE believes Requirement 5.1 should apply to low impact BES Cyber Systems and Requirement 5.5 should apply across all impact levels. For many field devices, where enforcement of cyber security controls in a timely fashion may be a challenge given the large geographic operational areas, limitation of physical access may be the most

#	Organization	Yes or No	Question 16 Comment
			effective control. Limiting unrestricted access, even to Low impact devices and the ability to control such access, could be a mitigating factor for the inability to perform device by device access revocation where no external access exists.
16.38	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's observations below:Table R5 Row 5.1 needs to document basic physical security requirements for all low and medium BES Cyber Systems.Table R5 Row 5.2: There should be additional language describing what "Monitoring" means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a particular item or location.Regarding Table 6, it is unclear what the benefit is for having requirement differentiation for Medium BES Cyber Systems with routable connectivity vs. those without.Table R6 Row 6.3, it is appropriate to validate those basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.39	Oncor Electric Delivery LLC	Disagree	Physical security should only be required at control centers and High impact substations with IP based communications.
16.40	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation 'Required for external connectivity only' in R5.1. This is an odd mix of physical and electronic access requirements. Please define the stipulations 'Required for external connectivity only' in R6.1, 6.2 and 6.3 for the same reasons.
16.41	WECC	Disagree	Recieved a uniform disagree from all but a vast range of responses to this question depending on the function of the entity reviewin the question.Low levels seem inappropriate as there is veryminimal requiremens for security based on the current tables.andShould apply to all impact levels.
16.42	Hydro One	Disagree	Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9. For consistency with Requirement 5.1, Requirements

#	Organization	Yes or No	Question 16 Comment
			5.5, 5.6, 5.7 and 5.11 should have a specification for BES Medium Impact Cyber System.Please clarify Requirements 6.1, 6.2 and 6.3. Is the routable connectivity on the BES Cyber System or the physical access control system?Should the "routable connectivity" be "external connectivity" for Requirements 6.1, 6.2 and 6.3?
16.43	ISO New England Inc	Disagree	Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9. For consistency with Requirement 5.1, Requirements 5.5, 5.6, 5.7 and 5.11 should specify something for BES Medium Impact Cyber System.Request clarification on Requirements 6.1, 6.2 and 6.3 is the routable connectivity on the BES Cyber System or the physical access control system?Should the "routable connectivity" be "external connectivity" for Requirements 6.1, 6.2 and 6.3?
16.44	Northeast Power Coordinating Council	Disagree	Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9. For consistency with Requirement 5.1, Requirements 5.5, 5.6, 5.7 and 5.11 should have a specification for BES Medium Impact Cyber System.Request clarification for Requirements 6.1, 6.2 and 6.3. Is the routable connectivity on the BES Cyber System or the physical access control system?Should the "routable connectivity" be "external connectivity" for Requirements 6.1, 6.2 and 6.3?
16.45	ReliabilityFirst Staff	Disagree	ReliabilityFirst believes the existing defined term "Physical Security Perimeter" should be retained and used in CIP-011. The current proposed language, "Restrict Physical access to areas protecting BES Cyber Systems", could lead to many questions for an auditor. Further, we believe that all rows of Table R5 (5.1 through 5.11) should be "required" for Medium Impact BES Cyber Systems. For Table R5, row 5.11; what constitutes an unauthorized physical access attempt? If unintended triggering of a magnetic card reader (such as simply walking too close to a reader and unintentionally activating it) indicates "failed attempts", are those to be considered unauthorized access attempts? Also in row 5.11, within what time frame must the review be conducted and we believe

#	Organization	Yes or No	Question 16 Comment
			there should be a requirement to document the review.
16.46	Luminant	Disagree	Remove the requirements for Medium Impact systems
16.47	Nuclear Energy Institute	Disagree	Requirement R6, Medium Impact: allowances should be included to exclude BES cyber systems which incorporate one way connectivity (e.g. outside the ESP via a one way hardware device), even if the protocol is routable. This would be in addition to the existing non-routable protocols.
16.48	Exelon Corporation	Disagree	Requirements 5.8 and 5.9 contain time parameters in hours. Exelon's tracking systems that would be used to demonstrate compliance are tracked in time increments of days, not hours. If an hourly timeframe is required, it will cause extensive modifications to numerous enterprise wide systems to allow tracking at an hourly level. One must ask how this improves reliability. What is the basis for time levels and having a different timeframe for a control center than other locations? It is difficult to understand how the impact levels were determined. The basis of the original CIP Standards addressed the critical sites and took into account the nature of the Critical Cyber Assets that could impact the BES, not the functional/operational parameters of the equipment that is connected to the BES. Exelon's position is that the access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.We are also concerned about the practicality of potentially applying these standards to multiple unmanned locations. Items 5.1, 5.2, 5.3: Requiring this level of physical security for any BES Cyber System that has no external connectivity should be reconsidered. No matter what level of impact, entities should not have to provide more physical security for a cyber based device or protective relay when it has no external connectivity and therefore would have no more impact to the BES than the other electromechanical devices, protective relays or control switches mounted in the same control panel.

#	Organization	Yes or No	Question 16 Comment
16.49	Progress Energy - Nuclear Generation	Disagree	See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
16.50	Xcel Energy	Disagree	See comments on question 15
16.51	Western Area Power Administration	Disagree	See previous comments
16.52	Emerson Process Management	Disagree	Since physical access restriction is not required for low and, maybe, medium impact BES Cyber Systems, according to R2 and R3, everyone in a generation plant will be subject to awareness and training requirements. Further, per R3.1, the training will cover the proper use of BES Cyber Systems, the proper handling of BES Cyber Systems information and storage media, and others. Why do plant's administrative staffs need to know how to use BES Cyber System?
16.53	Detroit Edison	Disagree	Table entries 5.8 and 5.9 require access revocation for Medium Impact access that is not required to be explicitly authorized.Table entries 5.8 and 5.9 should address the concept of expired PRA and/or training requirements. Propose changing 5.8 and 5.9 to read:"...who no longer require such access or no longer meet the training or PRA requirements as specified in R3 or R4..."Table entries 6.1, 6.2, and 6.3 Medium Impact states "Required for routable connectivity only". This term is not defined. We suggest replacing that language with "BES Cyber Systems that use a routable protocol".
16.54	EEI	Disagree	Table R5 Row 5.2: There should be additional language describing what "Monitoring" means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a particular item or location.Table R5 Row 5.9 creates a responsibility for an Entity to monitor the employment status of all of its contracting companies; the requirement should be eliminated, changed to cover

#	Organization	Yes or No	Question 16 Comment
			employees only, or changed to 72 hours from notification by contracting company.In general, there is a need for greater differentiation based on connectivity and BES component types in R5 and R6. Having one set of physical security standards for the differing types of BES components leads to trying to implement standards in an environment to which they are not suited - for example, several of the requirements do not make sense in a substation environment. The tables for R5 and R6 should be reviewed on a per-requirement basis to take these differences into account.
16.55	Allegheny Energy Supply	Disagree	Table R5 Row 5.3: This requirement should be consistent with Row 5.4 with respect to logging entry and exit.Table R6 Row 6.3, it is appropriate to validate that basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.56	Allegheny Power	Disagree	Table R5 Row 5.3: This requirement should be consistent with Row 5.4 with respect to logging entry and exit.Table R6 Row 6.3, it is appropriate to validate that basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.57	American Electric Power	Disagree	Table R5:5.1, Column "Medium Impact BES Cyber System", regarding "Required for external connectivity only", this should be stated "routable external connectivity"?5.8 & 5.9, Column "Medium Impact BES Cyber System", regarding "Control Center only" and "generation or Transmission Facility only". Authorized unescorted physical access is not required for medium impact facilities in row 5.5. If it is not required in 5.5, how can it be revoked in 5.8?5.11, regarding "...unauthorized physical access attempts". Suggested wording: "unauthorized physical access or physical access attempts".Table R6:6.1: Row 5.1 only requires access to areas protecting BES Cyber Systems be protected. It does not say that it needs to be done with a control system. A pad lock can used to restrict physical access. It also requires it for any external connectivity, not just routable.6.2: Monitoring of Medium Impact BES Cyber Systems is not required in section 5.26.3: A physical security control system is not needed to meet row 5.1 on Medium impact

#	Organization	Yes or No	Question 16 Comment
			Facilities since no other requirements from Table 5 are needed.
16.58	Alberta Electric System Operator	Disagree	Tables R5 and R6 do not log, monitor, or control physical security and access to Low Impact BES Cyber Systems. Consider making the requirements in tables R5 and R6 more restrictive. For example, restrict physical access for all impact levels, but make frequency and time horizon of reviews dependent on impact level - Low Impact review semi-annually, Medium Impact quarterly, and High Impact monthly.In table 5.4 - Change to "Log (manual or automated) visitor access (individuals not authorized..." to be consistent with Table 5.3.
16.59	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS proposal to include the Low and Medium Impact requirement in 5.1, but as stated in our response to Question 14, we believe the implementation of this requirement must be for a reasonable physical access policy, for example, as required for employee and public safety code compliance. Compliance with this requirement should be straight forward: locked gates, locked control house doors and/or locked fence around BES Cyber systems. Table R5 Item 5.1 should state for Low and Medium Impact; "Required".The APPA Task Force supports the MRO-NSRS proposal For items 5.2 through 5.6; we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We also suggest the following language for the tables noted:R5 Table 5.1: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR5 Table 5.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.3: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.4: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.5: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.6: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredThe APPA Task Force recommends removal of Table Items 5.7 - 5.9, dealing with "revoking authorized unescorted access," since this is covered in Table 9.2-9.5, Access Revocation. We believe there should not be a distinction between the two revocations and the timeframes for the revocation should be the same. There

#	Organization	Yes or No	Question 16 Comment
			should be only one set of revocation requirements.R5 Table 5.10: (renumber if 5.7-5.9 are removed)Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredR5 Table 5.11: (renumber if 5.7-5.9 are removed)Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredThe APPA Task Force supports the MRO-NSRS proposal for items 6.1 - 6.3; hence, we would propose all Medium Impact criteria to be changed to "Required for routable external connectivity only", to maintain consistency with existing wording within the standard. The tables would then read:R6 Table 6.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR6 Table 6.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR6 Table 6.3: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredThe APPA Task Force believes the 3 year maintenance and testing requirement on "all physical security mechanisms" in 6.3 is unreasonable. The term "all" should be replaced with "major" and the timeframe should be based on manufacturer recommendations, not an arbitrary 3 year timeframe.
16.60	Black Hills Corporation	Disagree	The concept makes sense, but 5.2 & 5.3, and 6.2 & 6.3 should have consistent impact applicability.
16.61	Network & Security Technologies Inc	Disagree	There are a number of inconsistencies in these and other tables related to grant and revocation of access (e.g., 5.1 requires restriction of physical access to areas protecting Medium Impact systems with external connectivity but 5.5 does not indicate such access must be authorized). Recommend a complete "scrub" of all requirements pertaining to authorization of, control of, and revocation of physical and electronic access.
16.62	We Energies	Disagree	We Energies agrees with EEI comment: Table R5 Row 5.1 needs to document basic physical security requirements for all low and medium BES Cyber Systems.We Energies agrees with EEI comment: Table R5 Row 5.2: There should be additional language describing what "Monitoring" means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? We Energies agrees with EEI: Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a

#	Organization	Yes or No	Question 16 Comment
			particular item or location.We Energies agrees with EEI comment: Regarding Table 6, it is unclear what the benefit is for having requirement differentiation for Medium BES Cyber Systems with routable connectivity vs. those without.We Energies agrees with EEI comment: Table R6 Row 6.3, it is appropriate to validate that basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.63	Progress Energy (non-Nuclear)	Disagree	Why does Table R6 require access control to systems identified in 5.1, 5.2, 5.3 medium impact with routable connectivity, but 5.1 does not reference routable and 5.2, 5.3 have no requirements for medium impact?See comment 14.

17. Requirement R7 of draft CIP-011-1 states "Each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in CIP-011-1 Table R7 – Account Management Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of electronic access control requirements that are included in Requirements table R7? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please Explain and provide any suggestions for modification.

Summary Consideration:

Comments concerning the requirement language in Requirement R7 with regard to "acceptable use" and the requests for clarity of the term "account types" indicated that these terms were misunderstood. The term "acceptable use" has been replaced with a requirement to authorize the use of account types, and the associated guidance document has been expanded to include descriptions of account types as used in this requirement.

Many commenters indicated that the format of Requirement R7 was causing confusion, suggesting that consistency in the use of columns and the format of the requirements and other information included in the tables would be helpful. The SDT agreed, and made consistency changes in the format and content of the columns in the tables, including the information required for High, Medium, and Low Impact BES Cyber Systems and BES Cyber Assets.

#	Organization	Yes or No	Question 17 Comment
17.1	ERCOT ISO	Agree	7.1: Please clarify "identification" and "group account".
17.2	Duke Energy	Agree	It's unclear how R7 tasks accomplish the purpose statement for low impact systems.
17.3	Minnesota Power	Agree	Minnesota Power generally agrees with the list of electronic access control requirements included in Table R7. However, it believes that some confusion exists regarding what distinguishes a "group" account from a "shared" account or a "system" account from an "administrative" account as described in Part 7.1.In addition, many types of equipment found in generating facilities or substations do not have typical "accounts," although they may have some type of access control (i.e., configuration password). To add further clarity, Minnesota Power recommends that the following be added to the end of purpose statement for Requirement 7:"...Required for only BES Cyber System

#	Organization	Yes or No	Question 17 Comment
			Components with account management capabilities."
17.4	Puget Sound Energy	Agree	Puget Sound Energy suggests that, because a BES Cyber System is made up of multiple components (hardware, operating system, application) that there should be a little clarity added. For example: "Identification of account types...and administrative accounts, in use for the BES Cyber Systems at the operating system, and applicable application(s) on the BES Cyber System Components."
17.5	Progress Energy - Nuclear Generation	Agree	R7 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
17.6	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 6.
17.7	Bonneville Power Administration	Agree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.
17.8	Entergy	Agree	This matches the guidance presented in the nuclear industry document NEI-08-09 Rev 6 Section 1.2.
17.9	Green Country Energy	Agree	Would it be possible throughout the standard to footnote sources for guidance such as DHS catalog of control systems or specific NIST documents? Hopefully this would remove some of the ambiguity and lead towards a more results based standard.

#	Organization	Yes or No	Question 17 Comment
17.10	Independent Electricity System Operator	Disagree	- Should R7.1 include anonymous to be consistent with R8.3.- R7.2 appears to be a policy statement vs something that can be audited. Some violations of acceptable use can't be detected or monitored so how can this be audited? If this is a policy stateme
17.11	Southwest Power Pool Regional Entity	Disagree	7.1 needs to include both local and domain user accounts. Elaborate a bit more on what is meant by "group" account. In many cases, a group account and a shared account are the same account. Very easy to overlook the group categorization the way the requirement is written as it is not defined in the current CIP standards.
17.12	US Army Corps of Engineers, Omaha Distirc	Disagree	7.2 implies that the user agreements would be so detailed as to differentiate the valid uses of individual systems and account types. It should be possible to have user agreements that allow them to work on authorized systems for authorized purposes (ie sysadmin account is authorized for sysadmin work) and restrict use for unlawful and non business purposes.
17.13	BCTC	Disagree	Please provide a definition of Acceptable Use. It is recommended that the term "acceptable use" be replaced (i.e. are we looking to define the roles within the BES Cyber System and define what actions each can take within the system?)
17.14	Idaho Power Company	Disagree	Acceptable use is a broad term when it comes to administrative accounts. As long as acceptable use can be defined in general terms and does not require a definitive list, this requirement will be OK. If it requires a definitive list, then there is risk in trying to define every situation or use of an administrative account.
17.15	Constellation Energy Control and Dispatch, LLC	Disagree	Account types should be defined.
17.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.

#	Organization	Yes or No	Question 17 Comment
17.17	The Empire District Electric Company	Disagree	Comments: Many types of equipment found in generating facilities or substations do not have typical “accounts”, although they may have some type of access control (configuration password). To alleviate this, we propose adding the following to the end of R7: “Required for only BES Cyber System Components with account management capabilities.”
17.18	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes a technical feasibility exception may be required based on the current wording of this requirement when considering local access to programmable electronic devices in a substation environment that do not support the ability to demonstrate acceptable use. Also for R7.2, CenterPoint Energy is not sure what is meant by "Acceptable use of each identified account types" and suggests adding specific examples.
17.19	Kansas City Power & Light	Disagree	Do all cyber systems and component that may be identified here have the capability to have an account? Recommend consideration of additional language such as “where equipment capabilities allow” for R7.
17.20	CWLP Electric Transmission, Distribution and Operations Department	Disagree	Documentation requirements would be burdensome without preventing malicious activity.
17.21	Dominion Resources Services, Inc.	Disagree	Dominion presumes that the word “acceptable” used in 7.2 will be defined by the Reliability Entity and will not be dictated by an outside group.
17.22	E.ON U.S.	Disagree	E.ON U.S, does not believe a compliance requirement is necessary for the low impact category.
17.23	Western Area Power Administration	Disagree	How is the responsible entity to meet this requirement for BES Cyber system components that do not have specific account types? For example...relays, comm equipment, other substation equipment that may now be part of the “affect situational

#	Organization	Yes or No	Question 17 Comment
			awareness of the BES" portion of the requirement.
17.24	Matrikon Inc.	Disagree	I would separate the requirements of creating an "inventory of user accounts" and its application to BES Cyber Systems, from the requirement of assigning "ownership and authorization of user accounts".The key separation is the "inventory" and the "authorization/use" of those accounts. A Cyber system may have 5 user accounts, of which some are disabled, some are shared, and some are actively used by specific individuals.
17.25	Florida Municipal Power Agency	Disagree	Is R7 needed since the real reliability goal is accomplished in R8? "Shall document" is not a strong requirement. The requirement is really account management. FMPA suggests: "Each Responsible Entity shall manage accounts and account permissions in the manner described in CIP-011-1 Table R7 - Account Management Specifications".Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration password). To alleviate this, if R7 is kept, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities." Without this addition, we believe this item sets the stage for numerous TFE's within the industry.
17.26	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
17.27	American Transmission Company	Disagree	Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration password). To alleviate this, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities."
17.28	MidAmerican Energy Company	Disagree	Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration

#	Organization	Yes or No	Question 17 Comment
			password). To alleviate this, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities." Without this addition, we believe this item sets the stage for numerous TFE's within the industry.
17.29	MRO's NERC Standards Review Subcommittee	Disagree	Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration password). To alleviate this, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities." Without this addition, we believe this item sets the stage for numerous TFE's within the industry.
17.30	NextEra Energy Corporate Compliance	Disagree	NextEra believes requirement 7.1 within table 7 should provide guidance to identify role based access controls for accounts on the BES Cyber System components. The current way the requirement reads, it is unclear if the specific account types listed are the only ones required for identification. Additionally, the BES Cyber Systems may not have the specific account types listed in requirement 7.1. Furthermore, NextEra believes requirement 7.2 should provide additional guidance related to acceptable use. It is unclear if the acceptable use requirement should be defined per account on each BES Cyber System Component. The requirement should require acceptable use based on role based access controls for categories of accounts. What is the criteria for 7.2 "Acceptable use" of each identified account types? Please add a local definition of "acceptable use" within the standard.Regarding R7, this table seems to apply the CIP electronic account standards to all units. Is this the intent?If so, then for 7.1 - the volume of research and account management, we suggest applying this to high impact only.As for R11.1 does the user restriction for wireless technologies include Blackberries and SmartPhones, NextEra believes this would impact on volume of devices and would be burdensome to manage.NextEra would like to see statement treating personal communication devices the same as company issued laptops since there are internal access controls designed to prevent misuse.

#	Organization	Yes or No	Question 17 Comment
17.31	Indeck Energy Services, Inc	Disagree	Not all Cyber Systems have logins and accounts. [suggestion] "For any Cyber System permitting login access, each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in CIP-011-1 Table R7 - Account Management Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems."
17.32	Network & Security Technologies Inc	Disagree	Purpose of R7.1 is unclear. Is it intended to require that every type of account a given individual has authorization to use be identified? If so, please clarify.Suggest "acceptable use" be addressed in R1 (policy) rather than here.
17.33	LCEC	Disagree	R7 - "access to its BES Cyber Systems " should read "Access to a BES Cyber System or its components "Roles should be identified during the creation of accounts.R8 - R7 and R8 should be combined into managing accounts.In CIP 10 there should be an air-gap exclusion for the thousands of relays connected to medium impact or lower systems that would require access revocation.
17.34	Consultant	Disagree	R7 - The wording to implement the criteria in the tables is incorrect. The tables are specifying the requirements and application of requirements to the classes of assets resulting from the impact categorization process. The wording of the statement should be modified to reflect this distinction.R7 & Table: In this section there is a change in terminology from the requirement to the table name to the column heading for the requirements. For this requirement:R7: document BES Cyber System accountsTable Name: Account Management Specificationscolumn Heading: Account Management DocumentationThis is confusing, as it is not clear what the topic is being addressed. Suggest consistent terminology for these locations. NOTE: There are multiple requirements where this condition exists and should be addressed.R7 - Account management would not seem to prevent malicious operation of BES Elements. It would seem to maintain control of access to BES Cyber Systems. The grouping of Electronic Access Controls would be more likely to be used to prevent malicious operation. R7 - Suggest deleting the word "maintaining" as account management controls access to BES

#	Organization	Yes or No	Question 17 Comment
			Cuber Systems, and the word maintaining control is unnecessary.7.1 Suggested rewording: For each BES Cyber System identify the account types in use on that system, including individual, group, shared, system, and administrative accounts.7.2 The intent is not clear. Does this mean document the acceptable use of each account type on each system, or document the acceptable use of the account types in use across all BES Cyber Systems? The resulting documentation is significantly different.
17.35	Southern Company	Disagree	R7 creates a workload requirement with very little benefit to overall reliability.
17.36	SCE&G	Disagree	R7 Is every BES Cyber Sytem required to have account types. Will there be provisions for equipment incapable of having an "account type"?R9 When does the timetable start for personnel terminated for cause? Once paperwork is completed?R10 SDT should consider the high volume of TFEs that may be generated for equipment with hardcoded passwords that cannot be changed. The TFE process should be evaluated and revised to make it less burdomesome on entities to document that a password is incapable of being changed every 12 months, or a provision should be added to the requirments. Overall provisions should be added to allow entities to utilize more secure methods of account access control, such as RSA tokens, without burdening the entity with additional adminsitrative work for choosing an access control method which is inherently more secure.R11: The box containing the definition for remote access: is this remote 2-way or 1-way?
17.37	Luminant	Disagree	R7.1 should not be required for low impact.
17.38	ISO New England Inc	Disagree	R7.2 appears to be a policy statement vs something that can be audited. Some violations of acceptable use can't be detected or monitored so how can this be audited? If this is a policy statement then it should be relocated to R1.
17.39	Ameren	Disagree	R7.2 does not list a monitoring frequency, it implies continual monitoring. Recommend that a monitoring frequency be added to this requirement.

#	Organization	Yes or No	Question 17 Comment
17.40	Powersouth Energy Cooperative	Disagree	R7-14. The required electronic security measures should be limited to the access or gateway point. Strong security measures at the gateway can effectively protect all the cyber assets that are accessed through the gateway. An argument can be made for example that the frequent changing of passwords on tens if not hundreds of devices inside a boundary that has very strong security measures lessens reliability should a qualified employee need to access the device but not be able to do so due to a recently changed password. Little is gained by requiring hundreds of devices inside a secure boundary to have the same level of protection that is provided through a secure gateway. Just because "it can be done" does not mean that "it should or must be done". The objective is to protect the assets. It should be recognized that protecting the assets can be done by focusing on the gateway that allows access to the devices. This allows entities to keenly focus on managing the security of those points of access rather than spending time, capital and other resources that provide limited if any added security. Prior to the workshop it was felt that strong gateway protection would meet the objectives of the standard. However, that is no longer clear. For example, it was felt that at a substation strong security measures at the gateway that allowed access to the cyber devices would meet the objective of standard with the cyber system (a collection of protective relays or other devices) being protected by the secure gateway. It appears that may not be the case. This results, for example, in the failure to change a password in a single device on a secured network being non-complaint with the standard for a situation where the BES reliability was never jeopardized. That type approach will likely result in numerous non-compliances that will on serve wasted resources even though the BES was never jeopardized. If it is intended that protecting only the gateway meets the objective that needs to be made clear.
17.41	BGE	Disagree	Replace the word "element" with "Cyber System Component" to maintain consistency with the defined terms. What is the difference between group and shared? What is the definition of "Acceptable use"?
17.42	San Diego Gas and Electric	Disagree	SDG&E recommends separating Wireless concepts from Access Concepts. Wireless is a

#	Organization	Yes or No	Question 17 Comment
	Co.		method of access, as is VPN, Citrix, dial-up, etc..., while Access implies a physical and logical service provided to a client.
17.43	Garland Power and Light	Disagree	Shared & group accounts should not be created or allowed because there is no accountability for these accounts
17.44	APPA Task Force	Disagree	The APPA Task Force does not believe the description of R7 follows the intent of the requirement. The following are recommended edits:R7. Objective:To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems.R7. Requirement:Each Responsible Entity shall document manage BES Cyber System accounts Components with account management capabilities by incorporating the criteria specified in CIP-011-1 Table R7- Account Management Specifications R8. Objective:To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems. R8. Requirement: Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R8 - Account Management Implementation R9. Objective: To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems. R9. Requirement: Each Responsible Entity shall revoke system access to its BES Cyber Systems as specified in CIP-011-1 Table R9 - Access Revocation R10. Objective: To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber SystemsR10. Requirement:Each Responsible Entity shall implement the account management access control actions specified in CIP-011-1 Table R10 - Account Access Control Specifications The drafting team uses the word "any" in the description in R11 and R12. This appears to require the all BES Cyber Systems be included in the requirement, even if the wireless functionality is disabled. The APPA Task Force believes the description should read: R11. Objective:To ensure that only authorized access is allowed to BES Cyber Systems that have remote or wireless electronic access.R11. Requirement: Each Responsible Entity that allows remote or wireless electronic access to a BES Cyber System shall apply the criteria specified in CIP-011-1 Table R11- Wireless and Remote Electronic Access Documentation for that specific BES Cyber System R12. Objective:To ensure that only authorized access is allowed to BES

#	Organization	Yes or No	Question 17 Comment
			Cyber Systems that have remote or wireless electronic access.R12. Requirement:Each Responsible Entity that allows wireless and remote electronic access to a BES Cyber System shall manage that electronic access in accordance with the criteria specified in CIP-011-1 Table R12 - Wireless and Remote Electronic Access Management for that specific BES Cyber System. R13. Objective:To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems.R13. Requirement:Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems [it owns and operates?] by implementing the criteria specified in CIP-011-1 Table R13 - Remote Access Revocation R14. Objective:To ensure that only authorized access is allowed to BES Cyber Systems that have remote or wireless electronic access.R14. Requirement:Each Responsible Entity shall document and implement its organizational processes, technical mechanisms, and procedures for control of wireless and remote access to electronic access points to the BES Cyber Systems including wireless and remote access if it is used, that incorporate the criteria specified in CIP-011-1 Table R14 - Wireless and Remote Electronic Access Controls.
17.45	Southern California Edison Company	Disagree	The drafting team should clarify mapping of controls, as identified in CIP-005 R1.5, and unbundle these requirements for access control devices. This would be in agreement with the drafting team's stated objective to leverage the financial and organizational capital invested by registered entities in providing cyber security through compliance with current versions of the CIP standards. SCE believes that all instances of electronic access, whether to the boundary or a system/device within the boundary, should be in one requirement. A new standard for access may include these account related controls in addition to others.The drafting team should provide guidance for R7.2. As written, R7.2 suggests that the acceptable use for each identified account type is required across all impact levels. It is not clear whether the intent here is to document business justification(s) for the acceptable use, the posting of signage describing acceptable use, or both. SCE recommends that the drafting team explicitly state the intent of this requirement.

#	Organization	Yes or No	Question 17 Comment
17.46	US Bureau of Reclamation	Disagree	The use of terminology is a problem in this standard. It is suggested that the term "electronic access" should be used instead of the term "account";or, a definition should be developed to clearly differentiate the difference, if there is one. The term electronic access is more precise.
17.47	Public Service Enterprise Group companies	Disagree	This is too short a period, especially if the event occurs over a weekend or holiday. The timeframe should be changed to 5 calendar days or 3 business days. At a minimum, 72 hours.
17.48	Pepco Holdings, Inc. - Affiliates	Disagree	What is a Cyber System account? Does this exclude Cyber System Component accounts? Would microprocessor relays passwords be in scope? Please reference comments on BES Cyber System Components and BES Cyber System definitions.
17.49	Manitoba Hydro	Disagree	What is the definition of “Acceptable use” for Requirement R7.1?

18. Table R7 provides direction concerning what impact level of BES Cyber Systems to which Requirement R7 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011 R7 was moved to CIP-007-5 R5.

Several commenters expressed concern that the documentation requirements for Low Impact BES Cyber Systems would be burdensome and would not prevent malicious activity. In response, most documentation and technical requirements applying to Low Impact BES Cyber Systems have been removed. However, the requirement for changing the default password remains, because this addresses a significant vulnerability and does not require periodic maintenance.

Some commenters suggested the standards need to be more explicit as to whether the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components. In response, the SDT provided additional clarity as to when a requirement applies to individual Cyber Assets. However, the requirements are written to allow flexibility in implementation.

In addition, commenters suggested adding "Required for routable connectivity only" to the applicability for Low and Medium Impact BES Cyber Systems. In response, the applicability for this requirement has been modified to High and Medium Impact BES Cyber Systems. For Medium Impact BES Cyber Systems, the SDT does not believe that the communication attributes of the BES Cyber System adequately mitigate the vulnerability this requirement addresses.

#	Organization	Yes or No	Question 18 Comment
18.1	Idaho Power Company	Agree	Account types will not vary by BES impact.
18.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
18.3	The Empire District Electric Company	Agree	Comments: We agree, assuming the suggested statement under question 17 is included.
18.4	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.

#	Organization	Yes or No	Question 18 Comment
18.5	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 6.
18.6	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels of R7 if the drafting team accepts our edits proposed in response to question 17.
18.7	Duke Energy	Agree	This is a lot of work to do for low impact systems. We suggest the requirement be removed from R7. Please provide insight as to how these tasks accomplish the purpose for low impact systems.
18.8	MRO's NERC Standards Review Subcommittee	Agree	We agree, assuming the suggested statement under question 17 is included.
18.9	BGE	Disagree	7.1 and 7.2 remove the requirement for low and medium since we do not need to log and monitor those systems per R8.
18.10	The United Illuminating Co	Disagree	7.1 and 7.2 should not apply to Low Impact devices.
18.11	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
18.12	LCEC	Disagree	Clarify if 7.1 & 7.2 are for account types only or if this includes specific accounts.
18.13	Indeck Energy Services, Inc	Disagree	Cyber Systems without login access need to be excluded.
18.14	CWLP Electric Transmission, Distribution and Operations Department	Disagree	Documentation requirements would be particularly burdensome for low impact BES cyber systems.

#	Organization	Yes or No	Question 18 Comment
18.15	E.ON U.S.	Disagree	E.ON U.S, does not believe a compliance requirement is necessary for the low impact category.
18.16	Minnesota Power	Disagree	It appears inconsistent with the other Requirements of CIP-011-1 to apply the criteria specified in Parts 7.1 and 7.2 to Low Impact BES Cyber Systems. If those using accounts on Low Impact Systems are not required to have Training, as required in R3, how are they to know the acceptable use of these accounts and therefore, why inventory and document it?
18.17	LADWP	Disagree	Low impact BES Cyber Systems should not be required.
18.18	National Grid	Disagree	National Grid suggests removing controls for Low Impact BES CS in table R8 to be consistent with table R7.7.2 - Elaborate on "acceptable use" and documentation required for acceptable use
18.19	NextEra Energy Corporate Compliance	Disagree	NextEra believes the requirement to identify and document acceptable use of accounts on Low Impact BES Cyber systems should not be required. The exercise of complying to that requirement for Low Impact BES Cyber systems will take considerable effort but will provide little if any security value or improve the reliability or security of the BES Infrastructure. It is recommended to have the requirement apply to both Medium and High Impact BES Cyber Systems.
18.20	American Municipal Power	Disagree	Please provide a little or no impact category.
18.21	Hydro One	Disagree	Presently, R7.1 specifies identification of account types. We suggest that the requirement R7.1 is modified to delete the word "types".
18.22	Puget Sound Energy	Disagree	Puget Sound Energy notes that physical security measures are only applicable to High Impact and some Medium Impact BES Cyber Systems. Puget Sound Energy suggests aligning Table 7 to Tables 5 and 6, or clarifying "Required for routable connectivity only"

#	Organization	Yes or No	Question 18 Comment
			for Low and Medium Impact BES Cyber Systems. At the very least, Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management.
18.23	Progress Energy (non-Nuclear)	Disagree	R7.1 - account management for "low" assets may be significant when you consider all of the intelligent programmable field instrumentation they will likely be categorized this way.Acceptable use is too broad a requirement. If someone is deemed competent to have access this requirement is not needed.Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.24	Constellation Energy Control and Dispatch, LLC	Disagree	Remove Required status for low and medium BES Cyber Systems, since R8 does not require logging or monitoring of those systems.
18.25	Garland Power and Light	Disagree	Requirement 7.1 & 7.2 should not be required for Low Impact BES Cyber Systems
18.26	Network & Security Technologies Inc	Disagree	See response to 17, previous.
18.27	Constellation Energy Commodities Group Inc.	Disagree	Should not be required for low impact systems.
18.28	Ameren	Disagree	Suggest removing R7.1 and R7.2 for Low Impact Systems. Creating and maintaining recordkeeping for all BES Systems will be a massive undertaking with no added protection to the BES.
18.29	Entergy	Disagree	The requirements should apply across the board for sites where routable protocols and dial-up communications are employed.

#	Organization	Yes or No	Question 18 Comment
18.30	Allegheny Energy Supply	Disagree	Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.31	Allegheny Power	Disagree	Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.32	EEI	Disagree	Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.33	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments. Please also reference comments on BES Cyber System Components and BES Cyber System definitions.
18.34	American Transmission Company	Disagree	We agree, assuming the suggested statement under question 17 is included.
18.35	We Energies	Disagree	We Energies agrees with EEI use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT

#	Organization	Yes or No	Question 18 Comment
			needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.36	FirstEnergy Corporation	Disagree	We feel there could be limited value in maintaining account type information for low impact BES Cyber Systems. Suggest removing 'required' for that column of table for R7.
18.37	Manitoba Hydro	Disagree	What is the purpose of Requirement 7.1 for Low Impact BES Cyber Systems? It is not clear that this information is needed for other requirements. Requirement 7.2 is inconsistent with Requirement R3, where no training is required for Low and Medium Impact BES Cyber Systems. Defining acceptable use of account types serves no purpose if it is not provided in training. The meaning of the references in Requirement R7.1 to "account types" and in Requirement R10.8 to "non-privileged accounts" is unclear. The reference in Requirement R7.2 to "Acceptable use of each identified account types" is incomplete. What is it that the Responsible Entity is required to do - develop criteria related to acceptable use, monitor for compliance with such criteria, etc? There are no specifics given with respect to "restrictions" in Requirement R11.1 or "allowed methods" in Requirement R11.2 1, so it is assumed to be at the Responsible Entity's discretion. It is unclear whether Requirement R11.3 requires a written policy to be in place - one would assume no written policy was required by the opening language of Requirement R11.

19. At the present time, the Access Control requirements for Physical Access have not been combined with the Access Control requirements related to Electronic Access. Do you agree with this method? Or would you prefer to have the Physical Access control requirements combined with the Electronic Access control requirements? Please explain and provide any suggestions for modification.

Summary Consideration:

Some commenters expressed concern that physical and electronic access controls may use the same terms, but they can actually mean different things, so there is a need to keep the requirements separate. In response, the terms physical and electric access control have been kept separate, but the controls for authorization, review, and revocation have been combined to ensure consistency across the requirements.

Some commenters expressed the need to combine requirements so that all "revoke" requirements are in one place. The SDT agrees with this suggestion, and the requirements to revoke access have been combined.

Some commenters expressed the need to combine the physical and electronic access control requirements based on the concern that being in separate requirements might lead to an entity missing something. The SDT agrees with this suggestion. The terms physical and electric access control have been kept separate, but the controls for authorization, review, and revocation have been combined to ensure consistency across the requirements.

Some commenters suggested continuing the use of ESP and PSP terminology, since it is now well understood. Upon further review, the SDT decided to continue use of the term Electronic Security Perimeter (ESP), but PSP has been modified to Defined Physical Boundary (DPB) to focus the requirements on controlling access rather than creating a perimeter.

#	Organization	Yes or No	Question 19 Comment
19.1	Duke Energy	Agree with proposed method	Access control for physical and electronic should continue to be separate.
19.2	Dairyland Power Cooperative	Agree with proposed method	Access to a physical area is different than access to an account that provides access to system(s) or application(s). Separate handling is appropriate.

#	Organization	Yes or No	Question 19 Comment
19.3	City Utilities of Springfield, Missouri	Agree with proposed method	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
19.4	Platte River Power Authority	Agree with proposed method	Electronic security and physical security are different disciplines and should be kept separate.
19.5	LCEC	Agree with proposed method	I agree that these should be separate but think that the retired terminology like Electronic Security Perimeter (ESP) and Physical Security Perimeter (PSP) are well understood and should not be retired for the sake of change. A lower level of controls does not make sense for physical access in some areas like data centers or control centers but may make sense in areas like substations.
19.6	Southwest Power Pool Regional Entity	Agree with proposed method	Physical access control includes certain requirements, such as escort, that are not applicable to electronic access. If combined, the standard will need to carefully make the appropriate distinction between physical and electronic access controls as necessary.
19.7	Bonneville Power Administration	Agree with proposed method	Physical and Electronic access controls may sometimes use the same terminology, and appear similar, but they are very different disciplines. Physical security may use electronic tools are part of its tool kit. However, it is still primarily a physical and geographical control methodology. Electronic access controls are more amorphous, with boundaries being at once more difficult to define, but more easily and absolutely controlled. Combining them would only lead to confusion and probably to failure in the end.
19.8	FirstEnergy Corporation	Agree with proposed method	Preference is to keep all electronic access requirements together, all physical access requirements together, and all informational access requirements together, but keep the three separate from each other.

#	Organization	Yes or No	Question 19 Comment
19.9	San Diego Gas and Electric Co.	Agree with proposed method	SDG&E recommends separation of the concepts of Logical (electronic) and Physical access.
19.10	APPA Task Force	Agree with proposed method	The APPA Task Force agrees with the SDT's proposal to separate requirements for Physical Access and Electronic Access. We do want to point out that both are interdependent. If a BES Facility has physical access control and does not have external routable connectivity, you do not need cyber system access control. This is covered in our comments for a number of the requirements where we recommend changing the impact level from "Required" to "Required for Routable External Connectivity Only."
19.11	Madison Gas and Electric Company	Agree with proposed method	The separation allows for clarity in these two distinct areas.
19.12	Progress Energy - Nuclear Generation	Agree with proposed method	To improve this Requirement, see attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
19.13	Xcel Energy	Agree with proposed method	We believe the separation is beneficial because it recognizes cases where physical access is needed but electronic access is not required, such as in the case for a mechanical maintenance vendor who performs no duties requiring electronic access.
19.14	Regulatory Compliance	Agree with proposed method	Would not want the controls for Physical Access and Electonic Access to be mixed.
19.15	US Bureau of Reclamation	Combine Access	Agree, but physical, logical, and information access control requirements should all be

#	Organization	Yes or No	Question 19 Comment
		Control requirements	included under a single set of requirements.
19.16	ERCOT ISO	Combine Access Control requirements	All access control areas should be combined (i.e., electronic access, physical access, information access). This will enable ease of use of the standard and a clearer understanding of the requirements. The current practice of having to go from standard to standard to find the requirements makes it more likely to miss a requirement and risk potential violations.
19.17	Puget Sound Energy	Combine Access Control requirements	As stated in the comments for question 18, Puget Sound Energy would prefer to see consistency (or an explanation of the differentiation of physical and logical controls).
19.18	Detroit Edison	Combine Access Control requirements	Combine all access control and revocation requirements into one requirement and one table.
19.19	Garland Power and Light	Combine Access Control requirements	Combine Tables R5, R9, R13, and R24.4 into one table so one can look at one table and see all the “revoke” requirements in one place - for most companies, the same people are going to be involved with “revoking” regardless of the Requirement #.
19.20	Consultant	Combine Access Control requirements	If the requirements for access control are the same, then combining them is better.Consideration should be given to combining information protection access and wireless access as well.It will also be clearer if there are any differences in access requirements for different types of access to have them combined so differences are obvious.
19.21	Idaho Power Company	Combine	It makes sense to combine some of them such as authorization, PRA and training,

#	Organization	Yes or No	Question 19 Comment
		Access Control requirements	revocation. Others are more specific to the type of access and may not lend themselves to combining.
19.22	USACE - Omaha Anchor	Combine Access Control requirements	Makes it easier to know which access must be terminated without looking through the entire document.
19.23	Southern California Edison Company	Combine Access Control requirements	The drafting team may not have adequately addressed the intent of Order 706 with respect to system security controls. Local logical (electronic) access is and should be recognized as a type of role based access where one has to be physically present near a device to operate it. The boundary protection for this type of role is (a) the physical security boundary and (b) the device level electronic security boundary. The proposed standard as it is currently worded allows for the removal of at least one access mechanism at the time of revocation. In that case, removal of access through the physical boundary will ensure the immediate revocation of a component critical for this type of role. The drafting team should add additional revocation criteria to adequately address this type of revocation.
19.24	Reliability & Compliance Group	Combine Access Control requirements	Tracking is easier if they are combined. We suggest that information access control be also included.
19.25	American Municipal Power	Combine Access Control requirements	Whenever possible, please eliminate redundancy in the requirements.
19.26	Progress Energy (non-	Combine	Will these be two distinct groups or will many have both accesses? Many people with

#	Organization	Yes or No	Question 19 Comment
	Nuclear)	Access Control requirements	physical access to transmission facilities will also need electronic access, suggesting that a single group/list may be easier to maintain.
19.27	Florida Municipal Power Agency	Combine Access Control requirements	Without a change in the definition of BES Cyber System to include an exclusion similar to the existing CIP-002-2 R3.1, R3.2 and R3.3, then there can be thousands of digital relays covered by this standard. A relay technical could have electronic access to thousands of such relays. It would be impossible to change all of those accounts within the time limits proposed in R9. We need to be careful in developing the standards that we do not cause unintended consequences of changing behavior that would reduce the reliability of the BES. This requirement R9 (and others within the standard) may have an unintended consequence of causing entities to revert to electro-mechanical relays to avoid onerous requirements in the standards. Reverting to electromechanical relays would likely increase costs as far as increased maintenance and testing requirements, but, would save costs of having to change accounts at numerous remote locations every time an employee changed positions.FMPA suggests combining physical and electronic (including wireless) access requirements to develop more reasonable requirements for situations such as these, e.g., revoking physical access to BES Cyber Systems with no external routable protocol should be enough. Thinking through these combinations is important to developing reasonable requirements.

20. Requirement R8 of draft CIP-011-1 states "Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R8 – Account Management Implementation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R8? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each criteria as represented in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R7 and R8 have been moved to CIP-004-5 and CIP-007-5.

Some commenters expressed confusion regarding the definition of "monitor" with respect to shared and guest account access privileges. In response, the specific term "monitor" has been removed from these account access requirements in favor of clearly defining the functions and actions associated with monitoring. Requirements to monitor access control have been moved to the Security Event Monitoring requirements in CIP-007-5.

Some commenters expressed a belief that the requirement for quarterly review of accounts and access privileges is excessive. The SDT notes that the quarterly review is required for Medium and High Impact BES Cyber Systems. The drafting team has clarified that it is not necessary to perform a detailed quarterly review of entitlements at the individual asset level.

Some commenters expressed a need to make the requirements for Account Management Specifications (CIP-011-1 R7) and for Account Management Implementation (CIP-011-1 R8) more consistent. In response, the drafting team has attempted to supply consistency as suggested by the commenters and has included these requirements in CIP-007-5.

Some commenters suggested removal of allowance of "guest" accounts. The drafting team believes there are reasons to retain "guest" accounts, and that complete removal would cause a hardship to some entities or may not be possible. Those using such accounts should be identified as required in the modified requirement.

Some commenters suggested combining Account Management Implementation (CIP-011-1 R8) with Access Revocation (CIP-011-1 R9). The drafting team has combined requirements in all cases where it seems feasible. However, what was formerly R9 concerned revocation, which carries a different VRF than most other access control requirements, and the subject matter concerns personnel actions. The Access Revocation requirements are now defined in CIP-004-5 R7.

Some commenters suggested changing R8.3 to "maintain a list of those who have access to guest/shared accounts." After review, the SDT determined that this part of the requirement was unnecessary and has removed it.

#	Organization	Yes or No	Question 20 Comment
20.1	National Rural Electric Cooperative Association (NRECA)		In R8.3, how do your demonstrate "monitor" to an auditor? This should be reworded such that both the auditor and the utility understand this the same way.
20.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
20.3	The Empire District Electric Company	Agree	Comments: Note impact level comments under question 21.
20.4	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made."Apply criteria" is not a strong requirement. The activity is account management, so, the requirement ought to be account management and R7 and R8 can be combined.Quarterly reviews of all accounts and privileges could be an onerous activity, and could actually decrease the reliability of the BES due to the higher rate of human error. FMPA suggests annual review of accounts and associated access privileges.
20.5	Puget Sound Energy	Agree	Puget Sound Energy suggests that R8.1 include wording regarding the removal of accounts. Example: "Establish and implement a process for authorizing the addition of account(s) and associated access. This process shall include necessary steps for the removal of accounts when no longer necessary."
20.6	Progress Energy - Nuclear Generation	Agree	R8 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
20.7	APPA Task Force	Agree	The APPA Task Force Agrees with the criteria. See our response to Question #21 for

#	Organization	Yes or No	Question 20 Comment
			the Impact Levels discussion.
20.8	FEUS	Agree	The drafting team should clarify 8.3 what is intended to 'monitor' the use of shared and guest accounts.
20.9	Bonneville Power Administration	Agree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Item 8.2 in Table R8 states "Conduct a quarterly review and verification of accounts and associated access privileges." It does not indicate what type of documentation is required to demonstrate compliance. Is an attestation sufficient documentation? Or is the Responsible Entity required to have specific documentation of its quarterly review by account types, etc?
20.10	Reliability & Compliance Group	Agree	The requirements in table 8 really should apply to medium impact systems as well.
20.11	Independent Electricity System Operator	Disagree	- R8.3 is anonymous synonymous with null sessions? If so then this will be difficult since anyone in the same network can connect with a null session.
20.12	Southwest Power Pool Regional Entity	Disagree	8.1: Authorization should be required for both the addition and the modification of a user account. 8.3: Define what is meant by "monitoring" the use of the shared and guest/anonymous accounts. Is it sufficient to know that someone used the account or must their activities with the account be monitored? Is monitoring required in real-time or after the fact? Is there a requirement to review account activity after the fact?
20.13	Con Edison of New York	Disagree	8.2 Quarterly reviews are excessive, suggest annual reviews and a documented

#	Organization	Yes or No	Question 20 Comment
			process for adding, removing or modifying access8.3 Need clarification on what monitoring means outside of annual review of if it is still required
20.14	Progress Energy (non-Nuclear)	Disagree	8.2 Quarterly seems to be too frequent - propose 6 months or longer. We are required in R9 to revoke access for those that are terminated or do not need access within 72 hours.
20.15	American Electric Power	Disagree	8.3, regarding "Monitor the use of shared and guest/anonymous accounts". This is not technically feasible on all systems. What level of detail is required to monitor the use? Does this need to be an automated electronic process? Is it even feasible to believe this can be done manually? How long must this monitoring data be kept?This should be removed.
20.16	Michigan Public Power Agency	Disagree	A quarterly review and verification of accounts would be overly burdensome and would not improve the electronic security of the system compared to a defined "annual" review.
20.17	BCTC	Disagree	Â Suggest removing “guest” from the language; guest accounts should not be permitted to be used in a secure systemÂ R 8.3 why single out monitoring of shared and guest accounts; should we not monitor all accounts?; unsure what the objective of this requirement is
20.18	Entergy	Disagree	Again, this is similar to NEI-08-09 Rev 6 Section 1.2. However, we question the advantage of having Account Management Implementation separate from Access Revocation. Please consider combining R9 with R8 by adding requirements 8.4 and 8.5 (below) and modifying the language in 8.1, as well as adding ‘required’ to low and medium impact BES Cyber Systems for 8.2 and 8.3.
20.19	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes a technical feasibility exception may be required base on the current wording of this requirement when considering local access to programmable electronic devices in a substation environment that do not

#	Organization	Yes or No	Question 20 Comment
			support the ability to demonstrate acceptable use.
20.20	Dominion Resources Services, Inc.	Disagree	Dominion recommends changing the wording of R8.3 to read:"Maintain a list of who has access to shared and guest/anonymous accounts."
20.21	US Bureau of Reclamation	Disagree	If the requirements of R7 are going to be implemented/established at all levels, an account management process should be required at the same levels.
20.22	LCEC	Disagree	In 8.1, changes to existing accounts that grant additional access should be authorized as well.
20.23	Black Hills Corporation	Disagree	In 8.2, quarterly is a good goal, but without a solid definition of the window associated with "quarterly", this will be an evidence gathering problem - suggest changing to semi-annual.
20.24	Minnesota Power	Disagree	In Part 8.3 of Table 8 the Standards Drafting Team needs to clarify what is meant by the term "monitor." Does this mean that Registered Entities need to be able to review who (named individual) accessed a shared account, and when this access occurred, or does this require logging their actions while utilizing the shared account? In addition, does this include system/admin accounts (as they are listed above as being different than shared accounts)? These measures seem to be appropriate, but implementation and providing auditable evidence could be difficult.
20.25	Idaho Power Company	Disagree	Monitor in 8.3 is vague. Would it require just that we know who used the account when or more detail about what the user did while using the account.
20.26	National Grid	Disagree	National Grid recommends changing Requirement 8.2 from "quarterly review" to "annual review" since the extra work is noticeably less than the benefit. Request clarification on 8.3 "monitor"
20.27	NextEra Energy	Disagree	NextEra believes the standard requirement 8.3 needs to be clarified regarding the

#	Organization	Yes or No	Question 20 Comment
	Corporate Compliance		ability to "Monitor" the use of shared and guest/anonymous accounts. What is the extent of this monitoring? If allowed by the standard, we do not believe effective monitoring of the use of these generic accounts is feasible due to their generic nature. This may be better stated as maintaining logging information and ensuring that quarterly reviews ensure access is documented to individuals with valid business need and credentials.The impact levels are appropriate for the requirement. However, for Requirement 8.2 it is unclear what an acceptable verification method is. Clarification regarding recommended methods for verifying accounts and privileges especially for legacy BES Cyber System components should be included in the requirement.Additionally, Requirement 8.3 is concerning because it is unclear what monitor means in the context of the requirement, the word should be clearly defined. Multiple users can use shared accounts at the same time and that would be something impossible to monitor. If monitor means who has approval to use shared accounts and who is has access to the password for shared accounts that should be defined in the requirement. Likewise, it is unclear how to monitor anonymous access. Clarification should be provided regarding the definition, intent, and appropriate evidence to demonstrate monitoring.
20.28	Oncor Electric Delivery LLC	Disagree	Not all BES Elements can monitor the use of shared and guest/anonymous accounts. TFE should be applicable. Requirement 8.3 should only apply to remote routable communications.
20.29	American Municipal Power	Disagree	Please provide a little or no impact level category
20.30	Pepco Holdings, Inc. - Affiliates	Disagree	Please reference to question 17.
20.31	Ameren	Disagree	R8.2 - Exhaustive review of all accounts quarterly will be time consuming with no added protection to the BES; this requirement should be changed to annually.

#	Organization	Yes or No	Question 20 Comment
20.32	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R8.2. Due to the requirements of R9 the review and verification time should be extended to an annual time frame.
20.33	Western Area Power Administration	Disagree	R8.3 - What constitutes "monitoring" of the use of shared and guest/anonymous accounts?
20.34	EEI	Disagree	R8.3 may create the possibility that an Entity would have to be able to show who used a shared account or password each time that it was used. This is an unimplementable requirement; the requirement should be clarified to make it clear that what must be tracked is the ability to use the shared account.
20.35	Southern Company	Disagree	R8.3 may create the possibility that an Entity would have to be able to show who used a shared account or password each time that it was used. This is an unimplementable requirement; the requirement should be clarified to make it clear that what must be tracked is the ability to use the shared account. In addition, . this requirement could require a large number of TFE's for systems which do not support multiple passwords.
20.36	Kansas City Power & Light	Disagree	R8.3: What does the "Monitor" represent?
20.37	Hydro One	Disagree	Recommend changing Requirement 8.2 from "quarterly review" to "annual review". There are no additional benefits to the shorter review period.Request clarification of the use of "monitor" in 8.3.
20.38	ISO New England Inc	Disagree	Recommend changing Requirement 8.2 from "quarterly review" to "annual review" since the extra work is noticeably less than the benefitR8.3 is anonymous synonymous with null sessions? If so then this will be difficult since anyone in the same network can connect with a null session. clarification on monitoring use of shared accounts.

#	Organization	Yes or No	Question 20 Comment
			"use" not provisioning. login/logout, all activity while logged in? commands used?
20.39	Northeast Power Coordinating Council	Disagree	Recommend changing Requirement 8.2 from “quarterly review” to “annual review”. There are no additional benefits to the shorter review period.Request clarification of the use of “monitor” in 8.3.
20.40	BGE	Disagree	Replace the word “elements” with Cyber System Component to maintain consistency with the defined terms. R7 & R8 requirements need to be synchronized. What is the definition of “monitor” (track actions, how much detail, will sudo suffice?)
20.41	Northeast Utilities	Disagree	Request clarification:- Are shared accounts included in 8.2 and required to be reviewed quarterly?- What does monitor mean in 8.3?
20.42	Garland Power and Light	Disagree	Requirement 8.3 - Do not believe that shared and guest/anonymous accounts should be allowed.
20.43	Network & Security Technologies Inc	Disagree	SDT should clarify intent of 8.3 (monitor use of shared and guest/anonymous accounts).
20.44	GE Energy	Disagree	Some type of account and privilege review should be required for Medium Impact systems, but not on a quarterly basis. These systems may well be used to validate software before promoting it to High Impact systems, and thus should have some account management due diligence.
20.45	Platte River Power Authority	Disagree	Suggested Revision:8.3 Track individuals that have been granted access to shared and guest/anonymous accounts.
20.46	Duke Energy	Disagree	Table 8: 8.2 quarterly reviews are too frequent. Suggest annually8.3 explain what is meant by “Monitor”What are the expectations for monitoring use of shared and guest/anonymous accounts? Is that up to the Responsible Entity? If the RE provides a procedure/policy and follows the policy, is that sufficient to pass audit?What is the

#	Organization	Yes or No	Question 20 Comment
			acceptable practice? 24/7?
20.47	ReliabilityFirst Staff	Disagree	Table R8; row 8.1 - suggest adding the word “document”, row 8.2 - what constitutes “review” and suggest the review should be documented, row 8.3 - what does “monitor” mean?
20.48	Constellation Energy Control and Dispatch, LLC	Disagree	The phrase "monitoring the use" of accounts is too vague.
20.49	ERCOT ISO	Disagree	The requirements of R7 and R8 can be combined. The purpose of each requirement is so similar that there appears to be no reason to separate them.
20.50	WECC	Disagree	The table lists three procedures for account management. Suggest this requirement be written to state: “Each Responsible Entity shall have implemented and documented procedures as described in Table...”The requirements should mandate additional rigor around access management, including the maintenance of access lists or automated provisioning systems. Additional specificity should be added to clarify the level of detail at which access must be tracked.
20.51	Consultant	Disagree	The word 'criteria' should be changed to requirements, as the table is listing requirements.Suggest replacing the words "to prevent malicious operation of BES Elements by maintaining..." with to maintain control..."Table R8-8.3 Not clear why this only applies to shared and guest accounts? And the difference between 'monitoring' and 'logging' is not clear.Suggest requirement is to "Log electronic access to BES Cyber Systems." and keep as required for High Impact Systems.
20.52	Dairyland Power Cooperative	Disagree	Validating whether users are assigned to appropriate roles or accounts should follow this timing. A detailed review to insure that the roles (or account groups) have proper permission settings can be a very time consuming and complex task depending on the complexity of a system. The detailed role definition review should be no more frequent than annually. The language used is not clear as to whether a distinction is

#	Organization	Yes or No	Question 20 Comment
			intended.
20.53	GTC & GSOC	Disagree	We recommend in R8.3 the term "Monitor" be replaced by "Review monthly". The term "monitor" could be taken to imply real time monitoring. Many entitities do not have the communication links required to meet such a real time requirement.
20.54	Alliant Energy	Disagree	We recommend retaining the annual requirement for 8.2 account review while retaining a quarterly requirement for personnel access review.8.3 needs more clarification regarding the activities included in the term “use” so as to provide specific guidance as to what constitutes a sufficient audit record.
20.55	The United Illuminating Co	Disagree	What is the intent of 8.3? It is difficult to discern what Monitor means in this requirement.
20.56	Manitoba Hydro	Disagree	word “Monitor” in Requirement 8.3 is unclear.

21. Table R8 provides direction concerning what impact level of BES Cyber Systems to which Requirement R8 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R8 has been moved to CIP-007-5 R5.

Some commenters expressed concern CIP-011-1 R8.1 (Account Authorization) should apply to all three impact levels. In response, the SDT notes that authorization also implicitly carries with it requirements for account review, revocation, and training. The SDT did not believe that the effort required to comply with these requirements for all three impact was appropriate given the risk posed to the Bulk Electric System.

Other commenters expressed concern that only Medium Impact BES Cyber Systems with routable external connectivity should be subject to the Table R8 requirements. The SDT disagrees and believes regardless of a BES Cyber System's communication characteristics, it is important to ensure that access to BES Cyber System is properly authorized and subject to periodic review.

Other commenters also expressed concern that the requirements in Table R8 should be aligned with those in Table R7. In response, the Table 7 and Table 8 requirements have been combined into CIP-007.

Some commenters expressed that the impact levels in R8.2 should have different review periods. The SDT believes a quarterly review period for access authorization and an annual review period for access privileges are appropriate for both High and Medium Impact BES Cyber Systems.

#	Organization	Yes or No	Question 21 Comment
21.1	Florida Municipal Power Agency	Agree	For item 8.1 through 8.3, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections.
21.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.

#	Organization	Yes or No	Question 21 Comment
21.3	Puget Sound Energy	Agree	Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management. If account management is not required for Low Impact BES Cyber Systems then it is unclear what benefit is there in identification of those accounts.
21.4	Progress Energy - Nuclear Generation	Agree	R8 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
21.5	Progress Energy (non-Nuclear)	Agree	See comment 14.
21.6	FirstEnergy Corporation	Agree	While the proposal provides flexibility based on Impact Categorization from a practicality viewpoint it will be easier to administer if all are treated equally. FE would likely take a conservative approach and treat all the same to simplify administration of this requirement.
21.7	ReliabilityFirst Staff	Disagree	8.1 should apply to all BES Cyber Systems. 8.2 should provide different periods of review for different levels of impact. Suggest making these annual for Low Impact, semi-annual for Medium Impact, and quarterly for High Impact.Suggest “required” Medium Impact for row 8.3.
21.8	ERCOT ISO	Disagree	8.1: Should be required for all. 8.2: Could be documented temporally. Low Impact required annually. Medium Impact required quarterly. High Impact required quarterly. 8.3: Please clarify meaning of “monitor”. Should be revised to address who has access to the accounts.
21.9	US Army Corps of Engineers, Omaha Distirc	Disagree	8.3 "monitor the use of" is somewhat vague. What would the measure be? Please define

#	Organization	Yes or No	Question 21 Comment
21.10	Southwest Power Pool Regional Entity	Disagree	Account authorization is a basic security control and should be applicable at all impact levels. Periodic review is also important and should be done for at least Medium impact systems as well, albeit more frequently for High impact than lesser impact.
21.11	Alliant Energy	Disagree	Alliant Energy agrees with EEI's comments relative to 8.3 and the consideration of capabilities and connectivity.
21.12	USACE HQ	Disagree	At a minimum, 8.2 should be required for all impact levels. Requirement 7 creates a document of every account type and its acceptable use, but for low and medium impact systems it is not required to update the same as per requirement 8.2.
21.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
21.14	The Empire District Electric Company	Disagree	Comments: For item 8.1 through 8.3, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
21.15	FEUS	Disagree	Disagree: The drafting team should consider 8.1 be applicable to LOW BES Cyber Systems for consistency with 7.1, 7.2, and 9.1. Without a process for authorizing new accounts it is difficult to review approved accounts and to revoke access that was not authorized.
21.16	WECC	Disagree	Even "Low Impact" systems have the capability of impacting operation of the BES within 15 minutes, thus these requirements should be required for all impact levels. Again, this requirement could then be rewritten without the table to provide more clarity.These requirements should apply to all impact levels

#	Organization	Yes or No	Question 21 Comment
21.17	San Diego Gas and Electric Co.	Disagree	For entities that own both Medium & High impact assets, they will likely perform all of the requirements contained in Table 8 for both classes of assets instead of maintaining separate procedures and mechanisms that will have a higher risk of compliance errors. SDG&E believes it just adds potential confusion to the process to have different requirements for Medium and High impact assets in this instance.
21.18	MRO's NERC Standards Review Subcommittee	Disagree	For item 8.1 through 8.3, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
21.19	American Transmission Company	Disagree	For R8.1 through R8.3 suggest adding "Required for routable external connectivity only." At the present there is no practical method to monitor the use of devices such as relays and IMUXs when accessed from inside a substation. They may be able to be front-ended, but as yet it has not proven viable.
21.20	Consultant	Disagree	If 8.1 requires authorizing accounts for Medium Impact Systems, then quarterly review of 8.2, and the logging access of 8.3 (see previous comment) should be required for those systems.Or, remove the requirement in 8.1 for Medium Impact Systems.
21.21	US Bureau of Reclamation	Disagree	If the requirements of R7 are going to be implemented/established at all levels, an account management process should be required at the same levels.
21.22	Black Hills Corporation	Disagree	In 8.3, do not understand why guest/anonymous accounts would be allowed. Should be limited to shared accounts only.
21.23	E.ON U.S.	Disagree	It is not clear what is meant by the term "monitor." Does monitor in 5.2 mean active

#	Organization	Yes or No	Question 21 Comment
			monitoring, e.g., video" Does it mean log?
21.24	Emerson Process Management	Disagree	It is prudent that account and privilage can only be created and granted with proper authorization. This principal should be applied to any BES Cyber System.
21.25	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
21.26	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's comments below:Regarding Table R8 Row 8.1:There can be a documented process even for low impact systems. It may not be as rigorous as for medium or high impact systems.Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.
21.27	Con Edison of New York	Disagree	Modified 8.2 should be required for medium (annual review)
21.28	American Municipal Power	Disagree	Please provide a little or no impact category
21.29	BGE	Disagree	R7 & R8 requirements are not synchronized.
21.30	Ameren	Disagree	R8.3 - should be required for Medium Impact Systems.
21.31	Allegheny Energy Supply	Disagree	Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.

#	Organization	Yes or No	Question 21 Comment
21.32	Allegheny Power	Disagree	Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.
21.33	EEI	Disagree	Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.
21.34	Southern California Edison Company	Disagree	SCE believes it may be possible to leverage the NERC PRC standards to effect compliance. In R8.2, an additional control with a timeframe longer than a quarter may be added for low and medium impact systems. It seems that access to low and medium impact systems never has to be verified. Although monitoring under R8.3 is not required for low and medium, which SCE is in agreement with, SCE believes that R8.2 should be modified where list of accounts and access privileges are tracked on a time bound basis.[MVL-HOW?] This may be an opportunity for the drafting team to review the appropriate NERC PRC standard on protection relay maintenance schedules and leverage the compliance requirements stated there.
21.35	GE Energy	Disagree	See question 20 comments
21.36	Entergy	Disagree	Suggest 8.2 apply to medium assets as 8.1 required a process for authorization. There is value in reviewing access lists from a security perspective.
21.37	Network & Security Technologies Inc	Disagree	Suggest adding a periodic review of access privileges to Medium Impact systems (8.2), perhaps every 12 months in lieu of quarterly.

#	Organization	Yes or No	Question 21 Comment
21.38	Alberta Electric System Operator	Disagree	The AESO believes that reviews should also be performed for Low and Medium Impact levels. Consider creating additional rows in the table to perform annual reviews for Low and Medium Impact BES Cyber Systems.For Table 8.1 - A process should be required for all impact levels.For Table 8.3 - Monitoring should be performed for all impact levels, however frequency of monitoring can be dependent on the impact level.
21.39	APPA Task Force	Disagree	The APPA Task Force supports the proposal by the MRO-NSRS to change 8.1 - 8.3 under Medium Impact to read "Required for routable external connectivity only." As stated in our response to Question #19, the physical security is covered in requirement R5 so only routable external connected devices are vulnerable. The tables should therefore read:R8 Table 8.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR8 Table 8.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR8 Table 8.3: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required
21.40	Constellation Power Source Generation	Disagree	The impact levels mapped out in R8 should be changed to mimic those in R7. Why identify all account types for every BES Cyber System, but then require processes for authorization and quarterly reviews of privileges for some of the impacts?
21.41	Reliability & Compliance Group	Disagree	The requirements in table 8 really should apply to medium impact systems as well.
21.42	Southern Company	Disagree	The scoping levels of R7-R14 are vastly expanded when compared to R5 and R6. Each requirement should be examined to determine the correct scope to best support overall reliability. The lack of differentiation based on connectivity and BES component type, in conjunction with the inclusion of requirements that have a per-low-system-component impact, mean that the vast majority of the effort involved in CIP compliance will have to be spent on low-impact, relatively unimportant assets,

#	Organization	Yes or No	Question 21 Comment
			often at the expense of overall reliability.
21.43	Oncor Electric Delivery LLC	Disagree	These requirements should only apply to systems with routable communications.
21.44	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments regarding Table R8 Row 8.3.
21.45	We Energies	Disagree	We Energies agrees with EEI regarding Table R8 Row 8.1:There can be a documented process even for low impact systems. It may not be as rigorous as for medium or high impact systems.We Energies agrees with EEI regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.

22. FERC has mandated immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset. Requirement R9 of draft CIP-011-1 states "Each Responsible Entity shall revoke system access to its BES Cyber Systems as specified in CIP-011-1 Table R9 – Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R9? Please explain and provide any suggestions for modification, including time proposals. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R9 has been moved to CIP-004-5 R6 and R7.

A number of commenters requested that the Standards make a distinction between "primary" access and "secondary" access, based on an understanding that an individual would need primary access to be able to use any secondary access (such as a database account). The SDT has revised the access revocation requirements (CIP-004 R7) to state that revocation of access includes remote, electronic, and physical access to the BES Cyber Systems. The requirements also address the revocation of "the ability to access" BES Cyber Systems and BES Cyber System Information as well as the resulting follow up actions related to additional assets (such as applications and databases). The SDT believes this best captures the concept of primary and secondary access.

Other commenters suggested revocation "with cause" should remain at 24 hours, and revocation "without cause" should remain at 7 days. This timing would keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer. In response, the SDT notes the FERC Order directs revocation of access to occur immediately in all cases where access is no longer needed. The requirement has been modified to simply revoke access when a person no longer needs it. Given that organizations usually have termination procedures to return company property and perform exit interviews, the SDT believes the processes for revoking access (both physical and remote electronic) can be incorporated into an organization's termination and transfer procedures.

Some commenters expressed concern that the revocation timeframe requirements based on combinations of BES Cyber System type and Impact Level are overly complex, and add confusion and undue administrative overhead in situations of job changes. To address this, commenters recommended more consistent timeframes. In response, the requirement has been modified to simply revoke access when a person no longer needs it. Evidence showing termination down to the hour is not practical in many cases. In the revised requirements, entities will show revocation of access as part of their termination procedures and demonstrate they follow these procedures (i.e., through dated sign-off records, system logs or actual system access control databases).

#	Organization	Yes or No	Question 22 Comment
22.1	Green Country Energy	Agree	Additionally addressing the transfer of responsibilities to another individual shpould be addressed if the terminated employee is a system administrator or such. If a "key" individual is terminated it may be quite a process to remove them from the system within 24 hours,leaving a system vulnerable or a backup plan unable to be executed. In summary termination with cause of a high security level employee could be very difficult to accomplish in 24 hours.
22.2	Oncor Electric Delivery LLC	Agree	One of the few examples where “Control Center” is separated from Transmission and Generation.
22.3	FEUS	Agree	The drafting team should consider revising the wording for revocation as ‘immediately but not to exceed XX hours’
22.4	Progress Energy - Nuclear Generation	Agree	To improve implementation of this requirement incorporate information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
22.5	Regulatory Compliance	Disagree	9.1 - clarify for service vendor that the clock should start upon notification to the entity.9.2-9.4 - 7 day revocation across the board
22.6	American Electric Power	Disagree	9.2 - 9.4: Recommend rewording 9.2-9.4 to match 5.7-5.9 or vice versa.Recommend removing physical access and external connectivity within a short-time window, and application rights later.
22.7	ISO New England Inc	Disagree	9.2, 9.3, 9.4 - all should be within the same time frame 72 hours. Same level of security issues or concerns across all (control center, trans, gen). Remove Requirements 9.3 and 9.4R9.2, R9.3 a d R9.4 suggest changing the requirement to “Review access to BES Cyber Systems for personnel that change job responsibilities as a result of reassignment, transferred to other positions within x hours of the

#	Organization	Yes or No	Question 22 Comment
			change."The purpose of the requirement is so that personnel have the least amount of access that is needed to do their jobs and so that they don't accumulate access as they move around. Also this is to limit possible segregation of duty violations and to require that authorized access permissions are the minimum necessary to perform work functions. (R10.6)
22.8	Dominion Resources Services, Inc.	Disagree	9.2, 9.3, and 9.4. To meet regulatory directives, if job duties are changed due to disciplinary actions or are "forced" on the user then a shorter time frame may be necessary. However, the current 24 hour time period is the least time period that can be reasonably accommodated through the business processes. And 24 hours is only possible if Revoking System Access is limited to controls that prevent the user from physically and electronically accessing the system. For example, if the user must either have physical access to the device or authenticate through a corporate system (e.g., active directory) before being allowed to access a BES Cyber System, then removal of physical access rights and of the ability to authenticate in the corporate system meets the Requirement for revoking system access, even though an account may still exist on the BES Cyber System. The account on the BES Cyber System would be removed within 7 days since many BES Cyber Systems are not administered 24x7.Requirement R4 establishes the process for personnel risk assessments. This practice determines the loyalty, reliability and trustworthiness of an individual as a prerequisite to authorizing logical or physical access. This is a standard practice used throughout the physical and cyber security industry and accepted by other regulatory agencies and Federal programs. Similar to R4.3, personnel risk assessments typically must also re-validate this trustworthiness periodically - commonly within 7 years and in some cases more frequently depending on the nature of the access. The presumption is that, once trustworthiness is established, it is not invalidated unless there is cause to reconsider or an individual voluntarily terminates their employment or retires. Only in instances where the established trustworthiness is in question, is prompt access revocation appropriate and warranted. Consequently, for personnel who "no longer require access", but for which there is no cause to question their trustworthiness, there is no basis for immediate or prompt revocation of access

#	Organization	Yes or No	Question 22 Comment
			within the time frames specified in this standard. The DHS Catalog for Control System Security Controls, Sections 2.3.4 and 2.3.5 reflect this practice - requiring revocation of access for cause within 24 hours and revocation of access for personnel reassigned or transferred to another position within 7 days. In other regulatory programs, revocation of access, not involving a question of change in trustworthiness, is handled via a periodic (e.g., monthly) review of access only. The 7 day requirement in the current standards would meet or exceed standard practice in this case. The requirements should be clarified to state that if there is no triggering event indicating that access is no longer required, then that determination can be made at the quarterly review.
22.9	Con Edison of New York	Disagree	9.2,3,4 - may be dependent on a company's existing HR/Payroll business system capabilities and introduce significant costs to remediate. Even though the individuals were trusted and the trust did not change as a result of cause. A week may be more realistic
22.10	US Bureau of Reclamation	Disagree	A requirement for revocation needs to be included for all impact levels. Suggest the timeframes for Requirements 9.2 through 9.4 be established on the basis of business days (for example 2 business days) or that the number of hours be increased cover long weekends.
22.11	MidAmerican Energy Company	Disagree	Access removal should be considered complete by removing physical and remote access. Removing physical and remote access effectively removes access to any BES Cyber Systems. Also see MidAmerican Energy's response to question 54.
22.12	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.Also, 9.2 - 9.4 is the second of many occurrences where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations

#	Organization	Yes or No	Question 22 Comment
			for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
22.13	Kansas City Power & Light	Disagree	Are these requirements applicable for electronic and physical access? 36 and 72 hours are too short a time frame for considering personnel who have changed access status other than that of termination when consideration of weekends and holidays. 5 to 7 business days would be an appropriate time frame. For personnel terminated for cause, 24 hours is acceptable.
22.14	Xcel Energy	Disagree	As noted in our response to a previous question, the 36 and 72 hour timeframes to revoke unescorted physical access for individuals no longer requiring access under 5.8 and 5.9 are not justified. When the change is for a business reason such as a job change 7 days is sufficient for access removal. When the access change is unrelated to a termination for cause, the individual's trustworthiness and reliability are not in question and the short timeframes are not warranted.
22.15	E.ON U.S.	Disagree	CIP-011-1, R9 references "system access." Does this mean physical or electronic access? For requirements 9.3 an d 9.4 it can be difficult to determine the exact time a person no longer needs access if, for example, the person has not required access for an extended period of time.E.ON U.S. does not believe compliance requirements are necessary for the low impact category.
22.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
22.17	The Empire District Electric Company	Disagree	Comments: If physical access is removed per R5, and remote access is removed per R13, this effectively removes all avenues to electronic access. Therefore, we propose

#	Organization	Yes or No	Question 22 Comment
			that the period for removing electronic access be lengthened.
22.18	BGE	Disagree	Define “immediate”. The table does not specify that the revocation is for personnel with electronic access. Combine 9.2, 9.3 & 9.4 revocation for any high impacted system should be consistent.
22.19	USACE HQ	Disagree	Does not make sense to create “for cause” requirement in any environment but a “no longer require” for only three (3) specific environment. I suggest to only have a two requirements, one (1) “for cause” and one (1) “no longer require”.
22.20	Duke Energy	Disagree	For 9.2, change 36 hours to 48 hours. Is the FERC mandate for ALL BES systems? Is there any room for loosening the requirement for low impact system?
22.21	Reliability & Compliance Group	Disagree	For personnel transferring to new positions where access is no longer available, 36 hours seems unduly burdensome. Recommend that this be changed to 72 hours for personnel no longer needing access to control center BES Cyber Systems.Also, this contradicts R5. Why do you need to revoke physical access at all for medium impact systems if you did not authorize it in the first place?
22.22	LCEC	Disagree	I agree with the intent of this requirement but need additional clarification to determine what is meant by revoking system access. Access may be granted at a system or component level. If system, network & wireless access is removed is this requirement satisfied? If audited at the component level, it may not be possible to make all of the necessary changes within the timeframes that are being dictated. The scope of this requirement should be clarified to indicate remote or wireless access only. Component level access will be mitigated by the physical security controls.
22.23	MRO's NERC Standards Review Subcommittee	Disagree	If physical access is removed per R5, and remote access is removed per R13, this effectively removes all avenues to electronic access. Therefore, we propose that the period for removing electronic access be lengthened.

#	Organization	Yes or No	Question 22 Comment
22.24	WECC	Disagree	If the goal is to revoke access at termination ("immediate") then the requirement should state simply, "The Responsible Entity will remove electronic and physical access at the time of termination." This should be possible for any entity that has use physical tokens for physical or electronic access (such as RSA SecurID, keys, RFID badges), however it would NOT be possible for entities that are still using access control systems with passwords, combination locks, or other access methods where revoking access requires reprogramming of devices. Note- this could indirectly require token based authentications for perimeter access which is not necessarily a bad requirement for medium and high impact systems.Terminations for cause should require immediate revocation of access - performed in conjunction with the termination notification to the employee. This is already standard practice at many entities. Additional criteria regarding employee suspensions should be added.
22.25	Consultant	Disagree	Immediate revocation is not achievable as indicated by the fact that there is a time frame for each identified revocation condition. Suggest using rules similar to the nuclear plants for access revocation, as those rules have over 30 years of regulatory basis for being adequate to control access revocation.R9. - Suggest deleting the words "...by maintaining control of access to its BES Cyber Systems," Revoking access does prevent malicious operation.9.1 - If access to Low Impact Systems does not require an authorization process(R8), then it is illogical to require the undocumented access to be revoked.9.1, 9.2, 9.3, & 9.4 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.9.2, 9.3, & 9.4 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.9.2, 9.3, & 9.4 - the word "such" in the statement is unnecessary. Suggest deleting the word "such".Similar to combining access requirements, the revocation requirements should be combined. This makes both

#	Organization	Yes or No	Question 22 Comment
			similarities and differences easier to understand.
22.26	Minnesota Power	Disagree	In extreme circumstances, it may not be possible to adhere to proposed the 24 and 36 hour revocation timeframes, especially in instances where BES Cyber System support is 8 hours a day, 5 days a week or where notification of termination comes from corporate systems that are also updated on an 8 hours a day, 5 days a week schedule.Are we to interpret "revoke system access" to mean access to individual accounts, or does it also include shared/group/system/admin accounts known by the person who no longer requires access?
22.27	LADWP	Disagree	It is infeasible to revoke access to Medium and High BES systems within the max 72-hour requirement. a. Revocation of Hard-Copy information should not be considered under the standard. b. The current 7 day window for revocation of access for individuals no longer needing access is reasonable and should remain a part of the standard.
22.28	Allegheny Energy Supply	Disagree	It may be appropriate to address revocation of access within the context of "Effective Access." For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System. Another example is if the BES Cyber System has no electronic communications outside of its physical boundary, then revoking physical access is effectively revoking access. Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.29	Allegheny Power	Disagree	It may be appropriate to address revocation of access within the context of "Effective Access." For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System.

#	Organization	Yes or No	Question 22 Comment
			Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.30	EEI	Disagree	It may be appropriate to address revocation of access within the context of "Effective Access." For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System. Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.31	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
22.32	Southwest Power Pool Regional Entity	Disagree	Make a distinction between "primary" access and "secondary" access. Primary access includes the domain user account, remote access (e.g., VPN, dial-up) credentials, and physical access (badge, keys) credentials. The idea is that the individual would need to gain access using the primary access in order to be able to use any secondary access such as a database account. Revoke primary access in much less than 24 hours for termination for cause, especially for control center systems access. Ideally, primary access should be revoked at the same time the individual is being terminated. Express revocation timeframes for terminations other than for cause in terms of business days. Provide for a negotiated "effective transfer date" other than the HR effective date; transferred personnel often back fill or otherwise continue to provide assistance to the losing department for some period of time.
22.33	National Grid	Disagree	National Grid recommends that Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems (transmission, generation, and control centers)

#	Organization	Yes or No	Question 22 Comment
			and remove Requirements 9.3 and 9.4.
22.34	Manitoba Hydro	Disagree	NERC should request from FERC a clarification on their meaning of “immediate”. “Remote access” in Requirements R11 - R14 could be considered a subset of “system access” in Requirement R9. Is the intent for Requirement R9 to refer to local, electronic access?
22.35	NextEra Energy Corporate Compliance	Disagree	NextEra believes the requirements for access revocation for personnel who are still employed by the responsible entity but no longer in a job function that requires access to BES Cyber Systems are too restrictive. The responsible entity should be able to develop timelines and processes to support the removal of access for a person who transfers, since a transfer is not an indication that the employee is a security risk or threat to the BES Cyber System.For personnel terminated for cause, the access should be removed before notification to the impacted personnel. The access that is revoked would be considered global access, as in the terminated personnel’s physical access to the BES Cyber Systems as well as network access. The responsible entities could then create a process, which gives them additional time up to two weeks, to remove individual system access to each BES Cyber system component. For personnel who separate from a responsible entity due to retirement or resignation should go thru a deprovisioning process based on the responsible entities internal processes. The risk posed by normal termination or transfer is extremely small and if malicious behavior or intent is planned, then the actions will happen before the scheduled termination. The recommendation is to revoke network and corporate cyber access and physical access, which would be considered global access within a 2-week timeframe. The responsible entities could then create a process, which gives them additional time up to thirty days, to remove individual system access to each BES Cyber system component. NextEra would also like to establish what is meant by revoking System Access? Is this revocation time frame applicable to removal of access rights at the Boundary Level, BES Cyber System level, or BES Cyber System Component Level?â€,Access is given to individuals on different levels beginning with access to entity networks and facilities, and flowing to access to individual BES Cyber System

#	Organization	Yes or No	Question 22 Comment
			components. The revocation of the individual's access to entity networks and facilities should be referenced or defined as accomplishing the desired result. This effectively removes the individual's ability to access any BES Cyber Systems and allows for the timely execution to approach the "immediate" completion as defined in Table R9.â€,This item should also reference upstream requirements to grant access at either the BES Cyber System level or the BES Cyber System Component level. What level of documentation is required for access rights?â€,Transmission Faciltities' IEDs (such as protective relays) utilitze shared passwords as the method of access control. What are the expectations regarding R9 - Access Revocations for those BES Cyber System Components? Are the expectations to change every IED shared password the user being revoked had access to in every High and Medium BES Transmission Facilities within 72hrs? This task of changing hundreds of protective relay passwords within 72hrs is currently not operationally feasible.R9 - indicates that NERC CIP password schemes will be applied to all units. Many systems with passwords have never had a password change.Large volume to manage. Control systems were not designed to have password changed regularly.When we implemented the NERC rules on the Load Control Computers in December, we found that they wouldn't run properly without the administrator password from when the software was originally installed. On one machine, we ended up having to reload the software to get it to work againThe OPC connections between the Toshiba ST and Ovation systems are the same way, they will only work with the logon credentials from the original software loading and configuration.NextEra suggests not requiring changes for legacy systems with embedded passwords.
22.36	PacifiCorp	Disagree	Per question 15 above, PacifiCorp believes revocation when access is no longer needed should be consistent among the different types of facilities. Specifically, R9.2 should be merged with both R9.3 and R9.4 resulting in a consistent 72-hour requirement.Access removal should be considered complete by removing physical and remote access. Removing physical and remote access effectively removes access to any BES Cyber Systems.

#	Organization	Yes or No	Question 22 Comment
22.37	American Transmission Company	Disagree	Propose maintaining time frame in 24 hour increments. Revocation for Medium impact should be revised from 36 hours to 48 hours.
22.38	Southern Company	Disagree	R9 should be modified to make it clear that the goal is effective removal of access - for example, that can be accomplished through revocation of physical access and revocation of network access without action at the individual BES Cyber System Component level.Removal of access within 24 hours for low-impact systems is unnecessarily burdensome.An unachievably short time limit for revocation due to dismissal for cause will actually result in damaging security as Entities are forced to delay dismissal until revocation can be accomplished in order to maintain compliance.Requiring that an Entity monitor the employment status of its contracting companies' employees creates an impossible burden. The requirement should be modified to require removal of access within a given number of hours after notification by the contracting company, combined with requirements that communication requirements are to be given to the contracting company.
22.39	Luminant	Disagree	R9 should not be required for low impact. 9.2 could 36 hours be changed to 48 (2 days) 9.3 and 9.4 1 week
22.40	Detroit Edison	Disagree	R9 uses the term "system access" while in other places the term is "authorized electronic access". Table entries 9.2, 9.3 and 9.4 should address the concept of expired PRA and/or training requirements. Propose changing to read:"...who no longer require such access or no longer meet the training or PRA requirements as specified in R3 or R4..."
22.41	Ameren	Disagree	R9.2, R9.3, and R9.4 - The short period of time to remove access does not extend well across weekends or through the 2nd business day in cases where access is no longer required at the end of the day. Suggest that these requirements be extended to a week to remain in line with current CIP standards. This will allow for proper hand off time in cases where job duties need to be transferred.

#	Organization	Yes or No	Question 22 Comment
22.42	Black Hills Corporation	Disagree	Recommend that in all cases, network/remote and physical access shall be revoked within 24 hours. All other access shall be revoked within 72 hours. This creates a balance of risk between immediately securing the BES systems and removing "all" access which can become quite intricate.
22.43	ERCOT ISO	Disagree	Recommend: "Each Responsible Entity shall revoke the ability to access its BES Cyber Systems as specified in CIP-011-1 Table R9 - Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Requirements should be revised to address primary and secondary access. Primary access being access to electronic and physical security perimeters (i.e., domain, remote access, badge access). Secondary access being access to assets within the protection of the primary access means (i.e., applications, databases, internal doors within facilities). The timelines listed in 9.1 - 9.4 are acceptable for primary access. Secondary access should allow a more reasonable timeframe. This also needs to address situations where a person may have access to a shared account that would require an outage to change the password. Doing this in a rushed manner would pose a risk to the BES Cyber System and to reliability. Access revocation should be consistent with R5. Recommend SDT consider language addressing access for system administrators and others with high risk access privileges.
22.44	Garland Power and Light	Disagree	Requirement 9.1 - For many companies, it is physically impossible to travel to all substations and change locks within the 24 hour deadline - don't put out a requirement that you know companies cannot comply with - especially for Low and Moderate Impact classified systems.Requirements for 9.1 should be 7 days for Low Impact, 48 hours for medium, and 24 hours high impact location.For requirements 9.3 and 9.4 should the medium impact time requirements should be 7 days.Removing physical access to non-external connected devices (or that only have data output ports connected, i.e. can not be reprogrammed or logged into from that port) should meet the requirements for revoking access for any terminated employee.

#	Organization	Yes or No	Question 22 Comment
22.45	Hydro One	Disagree	Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. We suggest removing requirements 9.3 and 9.4.Requirement 9.1 should be revised to include wording that "terminated for cause" should encompass employees terminated for not only cause, but for suspension or other reasons.
22.46	Northeast Power Coordinating Council	Disagree	Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.Requirement 9.1 should be revised to include wording that "terminated for cause" should encompass employees terminated for not only cause, but for suspension or other reasons.
22.47	Exelon Corporation	Disagree	Requirements 9.2, 9.3 and 9.4 contain time parameters in hours. Exelon's tracking systems that would be used to demonstrate compliance are tracked in time increments of days, not hours. If an hourly timeframe is required it will cause extensive modifications to numerous enterprise wide systems to allow tracking at an hourly level. One must ask how this improves reliability. What is the basis for time levels and having a different timeframe for a control center than other locations? Exelon's position is that the access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
22.48	Progress Energy (non-Nuclear)	Disagree	Revoking access within 24 hours will most likely require a special procedure. Revocation of access within a 'hours' timeframe implies that the access would be controlled through a security group with 24/7 coverage.Generation subsystems are much less sensitive than any of the control center subsystems. Leave this at 168 hours revocation other than for cause.
22.49	Southern California Edison Company	Disagree	SCE does not feel that reliability is served by imposing a 36 hour revocation for medium impact systems in a control center, and does not see any great distinction

#	Organization	Yes or No	Question 22 Comment
			between medium impact in transmission, generation, or a control center - these should all use a 72 hour timeframe. The timeframe for revocation of access to servers, applications, systems, sensitive information, relays, and equipment, etc. within a physically controlled area should be longer (e.g. 7 days). SCE also requests clarification on what devices must be revoked. The standard does not clarify what immediate revocation of access is - be it access to the "front gate" of an electronic and/or physical boundary versus the revocation of access to each "door" to every system and or component. As such, the potential scope of system access under R9.1 is unclear. SCE Recommends the drafting team revise this so that there is a single requirement for access revocation that and have it sub-divided into sections for physical, electronic, and information artifacts.
22.50	SCE&G	Disagree	SDT needs to consider utilizing the layers of access control leveraged by the exisiting standards here to meet the FERC mandate. Consider allowing entities to revoke access at the firewall level or password level within the timeframes suggested, and then give entites additional time to remove access at all of the other access control layers.
22.51	Florida Municipal Power Agency	Disagree	See comments to Question 19.In 9.2, 9.3 and 9.4 "who no longer require" is an ambiguous term separate from a more defined process of "granting" or "authorizing" access. FMPA suggests: "For personnel who have changed job responsibilities such that authorized access ... is no longer justified".9.3 and 9.4 can be combined into "non-Control Center BES Cyber Systems"
22.52	Liberty Electric Power, LLC	Disagree	See R5 comments on the short times to revoke access. It should be "next business day", not 24 hours in most cases. Further, it should be clear that revoking physical access to an entire facility would serve to revoke physical access to a secure are within the facility.
22.53	Constellation Power	Disagree	Some systems have a single username and password (shared), so when an employee is terminated, is the expectation that every component (such as a similar relay used

#	Organization	Yes or No	Question 22 Comment
	Source Generation		all over the system) have their shared passwords changed? A suggestion would be to allow physical revocation of access in these instances to trump cyber access. R9.4 should state "Generation" with a capital 'G' instead of "generation."
22.54	Entergy	Disagree	Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance point of view to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
22.55	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	The 24 hour requirement of 9.1 will be particularly burdensome for small entities that do not have 24/7 dispatch. While terminations can and should happen after hours when the situation calls for it, those who can revoke access may not necessarily be available. The unintended consequence may be a needed termination being delayed. Another fix would be to increase the number of those able to revoke access, but this may create more problems than it solves.
22.56	San Diego Gas and Electric Co.	Disagree	The access revocation timeframes listed for R9.2 - R9.4 should be consistent, since there is not a significant enough difference in risk between the three requirements warranting different time-periods. R9.4 is contradictory with R9.2 if, by the proposed definition of Control Center, a BES Cyber System controls two or more generation facilities or transmission facilities.SDG&E believes that the requirements in Table R9 should include language clarifying that contractors and service vendors that have access shall have that access revoked (within whatever time frame is appropriate) once the RE is notified by the contactor/service vendor of a contractor/service vendor's termination. The RE cannot and should not be held responsible for the lack of timely notifications of termination of contractor/service vendor personnel from a contractor/service vendor company. In other words if a contractor were to terminate someone on 1/1/XX and they do not notify the RE until 1/3/XX, the RE should not have to be held to a revocation time period that ends sometime on 1/2/XX.
22.57	Seattle City Light	Disagree	The most mature user provisioning systems with effective processes would unlikely meet the parameters in this requirement. As a result, utilities will modify their

#	Organization	Yes or No	Question 22 Comment
			organizational processes to redefine when "access is no longer needed." For example, rather than submitting a request to remove user access after termination, utilities will await completion of the revocation request before officially terminating employment. This would make the requirement ineffective in accomplishing it's intent.
22.58	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.The requirement should refer to electronic access, not just system access. The 36/72 hour requirement to remove access for routine changes is overly confining, as detailed in the answer to Question 16. Table 5 Part 5.7-5.9 also refer to timeliness of revocation. Twenty-four hours for terminations for cause is reasonable, however having two additional categories complicates matters and could potentially lead to confusion and someone not revoked in the appropriate category. For 5.8, 5.9, 9.2, 9.3 and 9.4, the 36/72 hour requirement to remove access for routine changes is overly confining. We suggest that routine revocation be accomplished within 5 business or 5 calendar days.
22.59	Northeast Utilities	Disagree	The table must be simplified; making a distinction by type of asset only increases risk of non-compliance. For personnel terminated not for cause why not make them all the same?
22.60	FirstEnergy Corporation	Disagree	There is much emphasis in properly categorizing facilities in Attachment II but that information seems to disregarded in information presented in Table 9 of CIP-011. If different timeframes for revoking access is warranted then it should be bases on Low-Medium-High impact - its unclear why a control center and generation/transmission facility is treated differently if each are deemed High Impact. This seems to be an issue in multiple tables dealing with revocation of access privileges - logical and

#	Organization	Yes or No	Question 22 Comment
			physical.Consider replacing 9.2, 9.3 and 9.4 with one row that say 'BES Cyber Systems' with appropriate timeframes for Low, Medium and High impact if needed. However, FE believes the R9.2, R9.3, R9.4, 36 and 72 hours is too restrictive and would like it to remain at the Version 2/3 timeframe of 7 days. To simplify, we recommend consistent revocation of all employees regardless of impact level. In practice most entities will likely implement consistently throughout their organization to the most restrictive requirement. Therefore, not sure the H/M/L levels has a practical use in this situation due to an administrative burden to implement and track differing time periods.
22.61	Powersouth Energy Cooperative	Disagree	This will be greatly affected by the ability to revoke access by account management at the gateway to the cyber system versus the changing of each component that makes up the system. Password/account management on systems such as relays that don't allow individual user accounts will be extremely complicated and time consuming. Consideration should be given to clarifying if managing access at the gateway and revoking physical access is sufficient, especially for low impact systems.
22.62	CWLP Electric Transmission, Distribution and Operations Department	Disagree	Time frames for 9.2 to 9.4 should be extended to 72 hours or next business day, whichever is longer.
22.63	USACE - Omaha Anchor	Disagree	Timelines are unreasonable for removal of electronic access - we do not have 24/7 coverage for revocation of electronic access. Revocation of physical access should be allowed for this section. If they don't have physical access - they can't access the electronic access. Electronic access removal should then be changed to two business days or next business day.
22.64	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.

#	Organization	Yes or No	Question 22 Comment
22.65	We Energies	Disagree	We Energies agrees with EEI. It may be appropriate to address revocation of access within the context of "Effective Access." For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System. Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.66	GTC & GSOC	Disagree	We recommend changing this to "36 hours or 1 business day, whichever is greater".
22.67	GE Energy	Disagree	Why introduce a time interval not based on a day? 36 hours may as well be 48 hours.Time periods should be specific to business days and take into account weekends.
22.68	APPA Task Force	Disagree	With physical access control as covered in R5 and remote access control as covered in R13, the greatest risk to the BES is presented by employees and contractors who have been terminated for cause. We therefore recommend the following conforming changes should be made to R9 Table 9.2 - 9.4: R9 Table 9.1: For personnel terminated for cause. Low, Medium and High Impact: "24 hours".APPA recommends elsewhere in these comments that (i) all impact levels have physical access controls in R5 Table 5.1, (ii) requirements in R5 Table 5.7-5.9 be removed, and (iii) requirement R10 Table 10.2 be edited to require passwords to be changed annually, If these comments to the drafting are accepted, the risk of malicious operations is minimal. We therefore recommend the following conforming changes be made to R9 Table 9.2-9.4:R9 Table 9.2: For personnel and others previously granted unescorted access who no longer require such access to Control Center BES Cyber Systems. R9 Table 9.3: For personnel and others previously granted unescorted access who no longer require such access to Transmission BES Cyber Systems. R9 Table 9.4: For personnel and others previously granted unescorted access who no longer require such access to Generation BES

#	Organization	Yes or No	Question 22 Comment
			Cyber Systems.

23. Table R9 provides direction concerning what impact level of BES Cyber Systems to which Requirement R9 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R9 has been moved to CIP-004-5 R6.

Commenters expressed concern that Table R9 is inconsistent with Table R8 for Low Impact BES Cyber Systems, as there should be no requirement to revoke access if there is no requirement to authorize it. In addition, many commenters raised concerns about entities being able to meet proposed revocation times, especially for Low Impact BES Cyber Systems due to the expected large numbers of such systems. The SDT agrees with these concerns, and the requirements for revocation of access for Low Impact BES Cyber Systems have been removed.

#	Organization	Yes or No	Question 23 Comment
23.1	BCTC		Â Recommend collapsing requirements 9.1 to 9.3 into one requirement.Â The time requirements for the one requirement are recommended to be:Â Medium Impact - within 72 hoursÂ High Impact - within 24 hours
23.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
23.3	Florida Municipal Power Agency	Agree	See comments to Questions 19 and 22. Also consider adding “Required for remote access or routable external connectivity only” to Medium and Lower Impact. Lower Impact should be not applicable for 9.1 to be consistent with 5.7. Also, for Medium Impact, 9.1 and 5.7 ought to be consistent.
23.4	Bonneville Power Administration	Agree	The table should refer to electronic access, not system access. The revocation time frames should be adjusted, as discussed above.
23.5	E.ON U.S.	Disagree	: CIP-011-1, R9 has stringent commitments for Low Impact and Medium Impact BES Cyber Systems. E ON U.S. proposes that these time requirements be extended. It is

#	Organization	Yes or No	Question 23 Comment
			not a hard and fast rule as to when employees no longer requires access to 9.4 cyber systems. This is particularly true when an employee is moving to another position within the Company and a certain amount of training is required to backfill their position. Three days does not allow time for that situation. A monthly or quarterly time frame would be adequate in most instances.
23.6	Network & Security Technologies Inc	Disagree	9.1 - Access to Low Impact systems needs to have been explicitly granted (8.1) or at least documented (7.1??) in order to be revoked (consistency issue - also see comments on Question 16).
23.7	Consultant	Disagree	9.1 - If access to Low Impact Systems does not require an authorization process(R8), then it is illogical to require the undocumented access to be revoked.9.1, 9.2, 9.3, & 9.4 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.9.2, 9.3, & 9.4 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.
23.8	Detroit Edison	Disagree	9.1 requires access revocation for Low Impact but there is no requirement to specifically authorize access for Low Impact.
23.9	American Electric Power	Disagree	9.1, Column "Low Impact BES Cyber System", regarding "Within 24 hours". There is no requirement to formally request, authorize, or review access to low impact BES Cyber Systems. How would it be possible to effectively remove that access?
23.10	Constellation Energy Commodities Group Inc.	Disagree	Align time requirement for 9.2 with the other 9.3 and 9.4 (all at 72 hours) to eliminate confusion.
23.11	Oncor Electric Delivery	Disagree	As stated earlier, depending on the type of communication to Cyber Systems, it may

#	Organization	Yes or No	Question 23 Comment
	LLC		not be possible to comply with these requirements due to communication failures. This requirement is particularly burdensome as it applies to contractors and service vendors. Many entities have resorted to weekly verification with their contractors/vendors to verify this requirement. A 24-36 hour requirement, other than "for cause", is not practical.
23.12	Northeast Power Coordinating Council	Disagree	Because the Low Impact levels do not have an access control requirement, Requirement 9.1 is not applicable. Remove the entry from the 9.1/Low Impact BES Cyber System box in the table. Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.
23.13	USACE - Omaha Anchor	Disagree	Believe revocation of physical access should be adequate for this standard - if that were so timelines and impact levels would be acceptable.
23.14	ReliabilityFirst Staff	Disagree	By not specifying a time for revocation of access for low impact assets, the requirement will not be enforceable for these assets. Suggest something like 30 or 90 calendar days for Low Impact BES Cyber System for 9.2, 9.3 and 9.4.
23.15	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
23.16	BGE	Disagree	Combine 9.2, 9.3 & 9.4 revocation for any high impacted system should be consistent. Can the drafting team declare why the time elements were changed from 1 week to 36 or 72 hours?
23.17	The Empire District Electric Company	Disagree	Comments: For item 9.1 through 9.4, we would propose adding the following under Medium Impact: "Required for remote access or routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.For item 9.1, we believe the Low Impact requirement

#	Organization	Yes or No	Question 23 Comment
			should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access).
23.18	Exelon Corporation	Disagree	Does this apply to protective relays, even if there is no external access? If so, entities should not have to provide more physical security for a cyber based device or protective relay when it has no external connectivity and therefore would have no more impact to the BES than the other electromechanical devices, protective relays or control switches mounted in the same control panel.Exelon's position is that the access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
23.19	Allegheny Energy Supply	Disagree	Effective Access to low impact systems should be removed within seven calendar days.
23.20	Allegheny Power	Disagree	Effective Access to low impact systems should be removed within seven calendar days.
23.21	San Diego Gas and Electric Co.	Disagree	Even though the compliance timeframes are reasonable in Table R9, two versus three timeframes are preferred. SDG&E believes that the control center timeframe (36 hours) should also be 72 hours, like R9.3 and R9.4.
23.22	USACE HQ	Disagree	First, requirements 9.1, 9.2, 9.3, and 9.4 should be required for every level of impact. Second, to avoid the "Friday 5PM termination with cause" scenario, the language should be change as follow: 9.1, from "within 24 hours" to "Close of Business Day (COB) of the following day after the termination", 9.2 from "within 36 hours" to "Close of Business Day (COB) of the second day after access is no longer required", and 9.3 and 9.4 from "within 72 hours" to "Close of Business Day (COB) of the third day after access is no longer required", OR if requirements 9.2 - 9.4 are collapsed into one requirement (please refer to my answer to previous question) from "within XX

#	Organization	Yes or No	Question 23 Comment
			hours" to "Close of Business Day (COB) of the third day after access is no longer required".
23.23	MRO's NERC Standards Review Subcommittee	Disagree	For item 9.1 through 9.4, we would propose adding the following under Medium Impact: "Required for remote access or routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.For item 9.1, we believe the Low Impact requirement should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access).
23.24	American Transmission Company	Disagree	For item 9.1, we believe the Low Impact requirement should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access).
23.25	LCEC	Disagree	I agree with the intent of this requirement but need additional clarification to determine what is meant by revoking system access. Access may be granted at a system or component level. If system, network & wireless access is removed is this requirement satisfied? If audited at the component level, it may not be possible to make all of the necessary changes within the timeframes that are being dictated. The scope of this requirement should be clarified to indicate remote or wireless access only. Component level access will be mitigated by the physical security controls.
23.26	APPA Task Force	Disagree	If our comments in response to Question #22 are accepted, we believe the Low Impact requirement should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access). We feel for remote and unmanned BES facilities ensuring and demonstrating compliance with this requirement will be difficult if not impossible to comply with from a logistical standpoint. We also recommend the drafting team allow more time to comply with 9.3 and 9.4. We know there are pressures to have access restricted as soon as

#	Organization	Yes or No	Question 23 Comment
			possible. But there are substantial difficulties in doing so, as many systems have multiple owners, are in remote locations and have numerous devices to access. The drafting team appears to be basing its timetable on a control center environment where the cyber systems are more IT focused and have controls that can be turned on and off easily. We therefore recommend the following changes be made to the impact levels: R9 Table 9.1: Low Impact: For remote access or routable external connectivity only, 24 hoursMedium Impact: For remote access or routable external connectivity only, 24 hoursHigh Impact: 24 hours.R9 Table 9.2: Low Impact: N/AMedium Impact: For remote access or routable external connectivity only, 36 hoursHigh Impact: 36 hoursR9 Table 9.3: Low Impact: N/AMedium Impact: For remote access or routable external connectivity only, 1 week.High Impact: Within 1 weekR9 Table 9.4: Low Impact: N/AMedium Impact: For remote access or routable external connectivity only, 1 week.High Impact: Within 1 week
23.27	US Bureau of Reclamation	Disagree	If the requirements of R7 are going to be implemented/established at all levels, the account revocation requirements should be required for the same levels
23.28	Manitoba Hydro	Disagree	Is 24 hours a reasonable and achievable time interval to revoke electronic access to Low Impact BES Cyber Systems? This is too short in consideration of the large number of Low Impact BES Cyber Systems.
23.29	Progress Energy (non-Nuclear)	Disagree	It seems reasonable that access for all impact levels, even low, should be revoked if and whenever it is no longer needed.The complexity and compliance risk of managing all of these requirements at different levels, for different functional areas will be very problematic to substantiate compliance.
23.30	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
23.31	MidAmerican Energy Company	Disagree	MidAmerican Energy does not agree with the timelines specified in Table R9. See the response to question 54.

#	Organization	Yes or No	Question 23 Comment
23.32	Tenaska	Disagree	Most of these are doable on SCADA and EMS hosts only and/or ingress/egress of perimeters/boundaries.10.1 Some DCSes will not allow this for some processes to work.10.2 Same as 10.110.3 must have a way of handling old equipment.10.4 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries .10.5 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.5 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.6 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.7 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.8 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.
23.33	National Grid	Disagree	o Since the Low Impact does not have an access control requirement, how can Low Impact have Requirement 9.1? National Grid recommends removal of this combination. o The text in 9.2/9.3/9.4 - "who no longer require such access" is vague and should be specific such as transfers, suspensions, or change in job duties.
23.34	American Municipal Power	Disagree	Please provide a little or no impact category
23.35	NextEra Energy Corporate Compliance	Disagree	Please see response to item 22. NextEra believes while it is appropriate to require access revocation requirements for Medium and High Impact BES Cyber Systems, the periods are too restrictive for personnel who transfer, or who separated from the responsible entity via normal means not for cause. NextEra does not believe that 9.1 should apply to Low Impact or No Impact BES Cyber System. In previous section, 8.1 (Authorizing Access) is not required for Low Impact BES Cyber System and the standards should be consistent.
23.36	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management and Table 9 Access Revocation. If account management is not

#	Organization	Yes or No	Question 23 Comment
			required for Low Impact BES Cyber Systems how can account access be revoked within 24 hours? Additionally, if physical security is not required for Low Impact BES Cyber Systems, then Puget Sound Energy suggests including wording similar to Table 5: "Required for routable connectivity only".
23.37	Luminant	Disagree	R9 should not be required for low impact. 9.2 could 36 hours be changed to 48 (2 days) 9.3 and 9.4 1 week
23.38	Ameren	Disagree	R9.1 - Without accounting for who has access this will be a difficult requirement to maintain documentation for Low Impact Systems.
23.39	Black Hills Corporation	Disagree	Recommend that in all cases, network/remote and physical access shall be revoked within 24 hours. All other access shall be revoked within 72 hours. This creates a balance of risk between immediately securing the BES systems and removing "all" access which can become quite intricate.
23.40	Minnesota Power	Disagree	Regarding Part 9.1, Low Impact BES Cyber Systems cannot require revocation, because creation of accounts for these was not tracked in Requirement R8.
23.41	EEI	Disagree	Regarding Table 9 Row 9.1, Effective Access to low impact systems should be removed within 24 hours for the "termination for cause" requirements See question 22 for definition of Effective Access.
23.42	Idaho Power Company	Disagree	Registered Entities will potentially have a large number of low impact systems. One individual may have access to many of the low impact systems. It may not be possible to remove the access from all of them individually within 24 hours.
23.43	Southern Company	Disagree	Removal of access within 24 hours for low-impact systems is unnecessarily burdensome.
23.44	Garland Power and Light	Disagree	Requirement 9.1 - For many companies, it is physically impossible to travel to all

#	Organization	Yes or No	Question 23 Comment
			substations and change locks within the 24 hour deadline - don't put out a requirement that you know companies cannot comply with - especially for Low and Moderate Impact classified systems.Requirements for 9.1 should be 7 days for Low Impact, 48 hours for medium, and 24 hours high impact location.For requirements 9.3 and 9.4 should the medium impact time requirements should be 7 days.Removing physical access to non-external connected devices (or that only have data output ports connected, i.e. can not be reprogrammed or logged into from that port) should meet the requirements for revoking access for any terminated employee.
23.45	Alberta Electric System Operator	Disagree	Revocation criteria should be specified for Low Impact BES Cyber Systems as well. The AESO suggests the following timelines in Table R9:9.1 Low, Medium, and High all Within 24 Hours9.2, 9.3 and 9.4 Low, Within 120 Hours, Medium and High, Within 72 Hours
23.46	Southern California Edison Company	Disagree	SCE does not agree with 36 hour revocation for medium impact systems in a control center, and does not see any great distinction between medium impact in transmission, generation, or a control center. These should all use 72 hour timeframe.Table R9 is that Requirements R9.3 and R9.4 are identical and can be combined. The time constraint for access revocation for low impact system as written is identical across impact levels. This does not reflect the intent of Order 706 where controls are commensurate with impact to BES reliability. The drafting team has selectively interpreted Order 706's directive for "immediate" revocation but has not given adequate consideration to the impact on BES reliability.
23.47	Alliant Energy	Disagree	See response for Question 22.
23.48	ISO New England Inc	Disagree	Since the Low Impact do not have an access control requirement, how can Low Impact have Requirement 9.1? Recommending removal of this combination.Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4

#	Organization	Yes or No	Question 23 Comment
23.49	Northeast Utilities	Disagree	Since the Low Impact does not have an access control requirement, how can Low Impact have Requirement 9.1? Recommend removal of this combination (i.e., Low Impact / For Cause).Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.
23.50	Entergy	Disagree	Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance point of view to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
23.51	Southwest Power Pool Regional Entity	Disagree	Termination of access, whether or not for cause, is a basic security control and needs to be applicable to all impact categories.
23.52	The United Illuminating Co	Disagree	The time frames should specify what T=0 is. For example, for termination for cause does the clock start with the termination, or with the notice from Human Resources.
23.53	Dairyland Power Cooperative	Disagree	There should be some time frame for revoking access to low impact systems. 30 days?
23.54	Reliability & Compliance Group	Disagree	They contradict R5.
23.55	FirstEnergy Corporation	Disagree	Timeframes should not be in 'hours' (i.e. less than a full day). Tracking by time rather than days would not be logistically possible on all systems and compliance could not be maintained.The new requirements now have too many different time frames to meet. Again, not logistically possible on all systems and compliance could not be maintained for larger utilities. In practice we would likely enforce the most restrictive. As stated in our response to Question 22 the revocation times for a high or medium impact facility should not be different for control centers and other facilities - otherwise why is it "high impact"?Why is Low Impact not covered? This implies a need for a "no impact" category which we believe is warranted.

#	Organization	Yes or No	Question 23 Comment
23.56	ERCOT ISO	Disagree	Timelines should be identified for low impact systems on 9.2, 9.3, and 9.4. The current timeline of 7 days would be appropriate.
23.57	Con Edison of New York	Disagree	Timeliness of access removal is important. This criteria can be interpreted to mean (R9.1 for example) as access needs to be revoked within 24 hours of the actual time of termination for cause. This can be unrealistic. The controlling department, for access, may not be notified by the individuals department of the termination within the time period. This is more likely when contract personnel are considered. The requirement should be clearly worded to provide 24 hours from notification of the termination for cause.
23.58	US Army Corps of Engineers, Omaha Distirc	Disagree	Times will be near impossible to meet for 9.1. Particularly when they cover high medium and low impact systems. Recommend that the emphasis be placed on removing remote electronic access and physical access to facilities. Time frames in terms of business days would be an improvement. 9.1 could be remove remote and physical access by next business day. 9.2 could be remove remote and physical assess within 2 business days. 9.3 & 9.4 within 3 business days. Also have concerns about meaning of "when no longer required" and how this would be tracked and audited. Example would be of an employee that leaves a job but retains system rights in order to train new person.
23.59	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
23.60	Hydro One	Disagree	We believe that changing passwords on non-routable devices isn't realistic and depending on final version of BES CSC list, this may even be unachievable. The standard should allow for other methods of revocation and permit appropriate implementation time.Because the Low Impact levels do not have an access control requirement, Requirement 9.1 is not applicable. Remove the entry from the 9.1/Low Impact BES Cyber System box in the table. Requirement 9.2 should use 72 hours for

#	Organization	Yes or No	Question 23 Comment
			all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.
23.61	We Energies	Disagree	We Energies agrees with EEI recommendation: Effective Access to low impact systems should be removed within seven calendar days.
23.62	PacifiCorp	Disagree	While we PacifiCorp agrees that terminations for cause require more immediate action to remove access than other terminations; we do not believe that normal terminations and transfers require such timeframes and believe that the current timeframes are more than adequate to ensure the safe operation of the BES. If these timeframes are unavoidable, business days should be considered as opposed to the currently proposed number of hours as this imposes significant risk to our ability todifficulty comply given the lack of available automated access removal solutions in the market place that can be realistically deployed across a wide-range of systems.

24. Requirement R10 of draft CIP-011-1 states "Each Responsible Entity shall implement the account management access control actions specified in CIP-011-1 Table R10 – Account Access Control Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R10? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R10 has been moved to CIP-007-5 R5.

Some commenters expressed concern that password criteria should be provided as guidance, and that entities can increase password strength and meet security requirements without meeting all criteria for password complexity. The drafting team believes that moving all password criteria to guidance would create a significant challenge in auditing this requirement, and would lead to the continued use of Technical Feasibility Exceptions, as entities and auditors may not agree on the most appropriate password policy. However, flexibility in the periodicity of changing passwords has been incorporated in the standards, and the requirement for password complexity was modified to allow more equally effective complexity requirements to be attainable.

Other commenters expressed that Table R10 focuses only on passwords, when there are other mechanisms for authentication (such as tokens). A more flexible requirement has been added to validate credentials before granting access to BES Cyber Systems. This requirement is intended to allow for other types of authenticators.

Some commenters expressed the need to have certain password changes occur during outages, and not necessarily be time based. In response, revisions were made to the password requirements to allow an entity to consider system characteristics when developing a password policy dealing with periodicity of change.

Some commenters suggested combining the requirements R10.6 to R10.8, and they also have concerns about having multiple IDs for different systems and permission levels. In response, the requirement for administrators to have an account for privileged functions was removed because it was too prescriptive. This requirement would not be reasonable to apply on all systems.

Some commenters expressed general concern about being able to enforce the Account Access Control requirements in R10.1 to R10.5. In response, the requirements have been modified to allow for procedural enforcement mechanisms. However, the measure makes clear the challenge in auditing procedural enforcement: entities may be required to divulge their passwords prior to immediately changing them to show compliance.

Some commenters expressed that in R10.7 "explicit authorization" is not defined, and questioned how this differs from R10.8. In response, the term "explicit authorization" has been removed from the requirement. Authorization requirements have been combined

into CIP-004-5, and CIP-003-5 now addresses the delegation of authorization responsibility.. Anywhere authorization is needed in the Standards, the requirement states the authorization occurs by the "CIP Senior Manager or Delegate".

Some commenters requested that the SDT define “privileged” and “other system functions” as used in R10.8. The SDT has removed these terms from the requirements.

#	Organization	Yes or No	Question 24 Comment
24.1	National Rural Electric Cooperative Association (NRECA)		In R10.1, the wording appears to permit changing vendor passwords "anytime" after installation. Do we mean prior to installation or within some specific time after installation. Please clarigy so there is not auditor confusion on what is required here.In R10.7, what what "explicit autorization" mean? Is this different from "authorization?" If yes, please ensure the requirement is clear on what is required.
24.2	WECC		SDT should reevaluate the password complexity requirements as many systems do not support special characters but could still have strong passwords by increasing lengths or changing more frequently. Consider replacing with a requirement that passwords have a minimum bit length (which is what requiring certain lengths, and character sets is prescribing).The password requirements are too weak to be effective. Strong password construction should be required at all levels.
24.3	FEUS	Agree	Agree with comments: The drafting team should clarify when default vendor passwords must be changed after installation (10.1)
24.4	RRI Energy	Agree	Could possibly need a TFE for field installed intelligent electronic devices - meters, monitors, plcs, rtus
24.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Passwords or equivalent should not be so prescriptive and such requirements can result in many TFEs. Also, by creating onerous password requirements, it is more likely to create reliability issues in the BES by having to keep track of complicated passwords; passwords should be both reasonable and functional.The focus of the requirement should be on user accounts. “System”

#	Organization	Yes or No	Question 24 Comment
			accounts should be excluded from many of these requirements (possibly considering new requirements concerning the security of system passwords) to avoid numerous TFEs while maintaining security.User accounts should focus on the password entropy, not on the specifics of number of characters and types of characters. Password entropy is the term used in the computer industry and a much better metric for defining password complexity vs. having to give a specific length or number of characters. For instance, there are 94 ASCII printable characters as described in 10.3, 10.4 and 10.5, so, a 6 character password can have about 36 bits of password entropy. An 8 character password consisting of non-case sensitive alpha-numeric characters (36 characters) has 40 bits of entropy; more than what is described in the standard. FMPA suggests using a metric of 36 bits of entropy for medium-impact password requirements. Such a step will avoid numerous TFEs for older equipment that cannot handle special characters, but can handle longer passwords for instance. FMPA suggests using the NIST's Electronic Authentication Guideline as a baseline for the standard. A copy can be found at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdfA password's information entropy can be expressed by the formula: where N is the number of possible symbols and L is the number of symbols in the password. The function log2 is the base-2 logarithm. H is measured in bits. (See Appendix A in NIST Electronic Authentication Guide referenced above for more detailed information).Even these simple requirements will not pose much of a threat to automated attack which is why these requirements must work together in order to best secure the BES. If securing the BES is the objective, passwords alone are not enough to secure devices; they must be accompanied by logging and alerting systems to ensure industry best practices. For example, a 56-bit password could be cracked in under a day with specialized hardware. A 72-bit password would take over 1,000 years to crack, while 128 bit passwords are currently considered uncrackable by brute force. A 22-character alpha-numeric password has entropy of 128 bits.Footnote 1 is unnecessarily onerous, e.g, if a device cannot support special characters or case sensitivity, but does support 32 character passwords, then the footnote would require use of all 32 characters with around 180 bits of entropy.Also, the focus on passwords

#	Organization	Yes or No	Question 24 Comment
			excludes other, even more secure tools, such as multifactor authentication, that ought to be accounted for.10.1 and 10.2 can be combined "Passwords much be changed upon installation and at least once every twelve months"On bullet 10.6 the wording "the minimum necessary to perform work functions." is subjective and difficult to measure. We propose this be replaced with "in accordance with the policy required in R1." In addition, 10.6 is account management and should be in R8, not R10.10.7 is duplicative of 8.1 and should be removed.10.8 is duplicative of requirements in R7 and R8 and should be removed or embedded within that requirement.
24.6	Green Country Energy	Agree	Guidance?
24.7	Emerson Process Management	Agree	In the popular Windows Active Directory, there is no enforcement of complying with password complexity policy. So, the policy can be set for password complexity, the user can still implement weak password without rejection.
24.8	Puget Sound Energy	Agree	Puget Sound Energy suggests including "Where Technically Feasible" to R10, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 10.
24.9	Progress Energy - Nuclear Generation	Agree	R10 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
24.10	National Grid	Agree	Requirements 10.3, 10.4, and 10.5 indicate the "how" which NERC wants to move away from. Suggest moving this to the guidance document.
24.11	US Bureau of Reclamation	Agree	Row 10.4 and 10.5 would be easily reworded into a specific requirement for password construction. Also refer to question #54, comment 2.
24.12	PNGC-Cowtitz-Central	Agree	See comment for question 6.

#	Organization	Yes or No	Question 24 Comment
	Lincoln-Benton-Clallam Group		
24.13	Network & Security Technologies Inc	Agree	Suggestion offered at recent workshop to substitute “ensure authenticity” for “use passwords” has merit and should be considered.
24.14	Alberta Electric System Operator	Agree	The AESO thinks that it is impossible to guarantee a RE can “prevent malicious operation,” however the RE can “mitigate malicious operation.”Please define the term "BES Elements".We agree with the list of criteria that are included in Requirements Table R10.
24.15	Independent Electricity System Operator	Disagree	- R10.2 broaden the scope of passwords and allow for certificates, keys, etc. Some vendors deliver default certificates. In addition, keys may be used for authentication and should be changed. If using two factor or multi factor authentication it techn
24.16	LADWP	Disagree	1. The footnote [1] for CIP-011-1 R10 appears to allow entities to assess TFEs for Account Access Control / Passwords within their own judgment. I would recommend that for 10.3, 10.4, and 10.5 be replaced by footnote [1]. a. The current FERC-Approved TFE process is inefficient; the incorporation of all TFEs into their appropriate requirements should suffice the standard.
24.17	Progress Energy (non-Nuclear)	Disagree	10.1 may be better to indicate ‘upon commissioning’10.7 and 10.8 are too broadly defined to effectively control.It needs to be clarified that it is not required that each device be capable of being configured to automatically enforce authentication requirements (forcing password change, password length, password sophistication, etc.).R10.6 - Recommend clarification of language to indicate that ‘access permission are the minimum necessary to perform work functions’ means normal work functions for each particular individual. There should be no intention to require a single individual to maintain multiple logins for each function for which they are responsible (beyond an administrative login and a ‘normal functions’ login).Consider combining 10.6 and 10.8. If you meet the intent of 10.6 then you should be meeting 10.8.

#	Organization	Yes or No	Question 24 Comment
24.18	LCEC	Disagree	10.1 should be changed passwords prior to production as opposed to after installation.10.1-10.5 lead back to TFE issues. Consider applying only to interactive users.Must address current compliance challenge of requiring technical enforcement of password policies. 10.2 is not auditable as a performance requirement.Footnote [1] is subject to major interpretation: complexity is ambiguous. May not be legally defensible. Maximum should be maximum comparable.We suggest removing 10.6 it is too subjective.
24.19	Idaho Power Company	Disagree	10.1 should specify a period of time after installation or require it before putting it in production. As long as default passwords are changed, low impact systems should have a longer password change cycle
24.20	American Electric Power	Disagree	10.1: Regarding "Change default vendor passwords after installation", suggest using "Default vendor password shall be changed before or during commissioning", or "Change default vendor passwords". The word "after" fails to establish a time frame for the change.10.3: Regarding "Implement a password scheme that has the following attributes:[1]Minimum of six characters", and its footnote. While the footnote potentially allows for some exceptions, this could still be subject to a Technical Feasibility Exception (TFE) process. The TFE process is very cumbersome and provides little value. Based on the direction of CIP-010, the number of TFEs could grow exponentially.10.7: Regarding "Require explicit authorization of access to system and security administrative functions within the BES Cyber System". This seems redundant to 10.6. Would these not be granted based on job function? If not, how is it different than 10.6?10.8: Regarding "Require users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions". What security benefit does this provide? This defeats any single sign-on functionality. To what level do you limit each account? Why are users required to have more than one account? Will they need more than 2 accounts? What is the limit?

#	Organization	Yes or No	Question 24 Comment
24.21	Dominion Resources Services, Inc.	Disagree	10.8. Some equipment does not support non-privileged accounts. A footnote similar to the one added for 10.3 to eliminate the need for a TFE should be added to 10.8.
24.22	BCTC	Disagree	Â BCTC can see the need for a TFE with requirement 10.2, 10.3, and 10.4Â Requirement 10.7 - we are uncertain as to the objective of this requirement. Does this simply require System Owner, or delegate, approval fro personnel assigned Admin accounts?Requirement 10.8 - we would appreciate some guidance on what type of evidence would be required to demonstrate compliance to this requirement. This seems very difficult to enforce.
24.23	Public Service Enterprise Group companies	Disagree	A rework of the language is needed to address the following questions to avoid confusion and misunderstanding. Please define for 10.7 what is meant by "security administrative functions" and for 10.8 what is meant by "other system functions". Does the Operating System need automatically to check a user account against a list of "security administrative functions" before allowing access? What needs to be done if the Operating System does not have this capability? Meeting this requirement may not be technically feasible.
24.24	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.Also 10.3 - 10.8 seem to suggest technical authentication enforcement capability for all systems. Suggest softening the language to allow for administrative controls to compensate where technical controls are not possible. Also recommend verbiage that provides consideration for said technical limitations to eliminate the requirement for TFEs.
24.25	FirstEnergy Corporation	Disagree	As written, it appears that this would eliminate many TFEs and we like this change.10.4, 10.5 - Make text in table more generic - 'implement a password scheme that utilizes as many of the four attributes as possible for the device to which the password applies'. As written, 10.5 would still mean TFE's for any Microsoft-based authentication systems.Need to provide guidance for 2nd factor authentication (which is typically all numeric) and non-password authentication sources (e.g. smart

#	Organization	Yes or No	Question 24 Comment
			cards)
24.26	Constellation Energy Commodities Group Inc.	Disagree	Choose a single standard for password complexity, rather than differentiating by risk level. Either choose a standard that is compatible with MS Windows, or explicitly state that implementing the maximum password complexity that the device supports is sufficient to meet the requirement without requiring documentation of an exception.
24.27	Liberty Electric Power, LLC	Disagree	CIP-011 R10 changing passwords every 12 months. This is a “feel good” requirement which does not advance security, but rather degrades is as the new passwords are more likely to be written down than the old passwords. The number one method of password theft is reading off a written document.The better method for password security is requiring changes "for cause".
24.28	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
24.29	GTC & GSOC	Disagree	Dictating password attributes requires a specific technology, one that is rapidly becoming obsolete. We recommend the standard should require adequate authentication measures to prevent unauthorized access to systems without specifying passwords as the method for doing so.
24.30	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy is concerned for entities without routable connectivity this requirement is overly burdensome and would require the manual resetting of passwords on thousands of remotely distributed programmable electronic devices. Emergency response would be hampered with the resulting manual password modification and management process. An unintended consequence of not excluding unconnected devices from this requirement may cause an entity to establish connectivity to meet this requirement. This potentially exposes BES cyber system to additional unnecessary security risks which should not be the intention of this requirement. Additionally, password protection may not be available on all BES Cyber

#	Organization	Yes or No	Question 24 Comment
			Systems since some may use other authentication schemes, such as digital certificates or encryption keys. TFEs may be necessary for this requirement.
24.31	Exelon Corporation	Disagree	Exelon is concerned that this will require unique identifiers and passwords for each BES Component despite the ambiguity resulting from the use of the term BES Element which could be read to mean group of components. Exelon suggests that this be limited to only those BES Components which can be remotely accessed via routable or dial-up protocol.
24.32	Constellation Power Source Generation	Disagree	For R10.1, instead of changing passwords "after installation," it should state "upon installation" in case the password is changed before physical installation. R10.2 requires passwords to be changed every 12 months, but in the case of relays for a base loaded generation facility that has planned outages every 3-5 years, this is not possible. The verbiage should add flexibility for planned outages. For R10.4, passwords are not the only way to authenticate, so requiring a password scheme is troublesome.
24.33	Southwest Power Pool Regional Entity	Disagree	Ideally, require user authentication before granting access without prescribing any particular technology. For the requirements specific to password management, add "if used" to the requirement. As written, R10 can be read to mandate the use of passwords. 10.3: Longer is better, especially for administratively privileged accounts. Require 10 or more characters for administratively privileged accounts and at least 8 characters for less-privileged accounts. Where the BES Cyber System Component cannot support the defined length, mandate the maximum password length supported. 10.4 and 10.5: Instead of defining the complexity characteristic, require complex passwords as enforced by the BES Cyber System Component's operating system. 10.7: Define what "explicit authorization" means and clarify if for all types of access or only interactive access. 10.8: Consider rewording the requirement to read "Require users of security administrative accounts to use non-privileged accounts when performing non-administrative functions on BES Cyber Systems."

#	Organization	Yes or No	Question 24 Comment
24.34	Detroit Edison	Disagree	In 10.1 the term “after installation” is vague. Change the sentence to “Change default vendor passwords prior to putting any BES Cyber System Component in service”.In 10.2 change 12 months to “at least once per calendar year, not to exceed 14 months between instances”
24.35	San Diego Gas and Electric Co.	Disagree	In Table R10, Requirement 10.5, SDG&E believes that passwords for high impact systems should be longer, not necessarily more complex. We recommend that high impact system passwords be a minimum of 10 characters. Complexity requirements should be the same for high and medium systems (SDG&E recommends 10.4).Certain legacy devices won’t be able to comply with these password requirements as listed (such as substation serially connected relays), so TFEs may be required for some of these Requirements in CIP-011.The drafting team also may want to consider changing R10 to include other technologies for controlling access besides passwords, such as special locks, biometric devices, etc.
24.36	Hydro One	Disagree	In the case of R10.2 we believe that the change of passwords every 12 months for all three categories would be very difficult to implement and would not provide increased benefit to the overall reliability of the BES. Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.The use of the “minimum” will make 10.6 difficult to audit (refer to the response to Question 54).
24.37	Minnesota Power	Disagree	Is it the Standards Drafting Teams intent that Part 10.7 of Table R10 requires explicit approval for every login to system or security administrative accounts? If yes, Minnesota Power believes that this is excessive and will inhibit proper administration of BES Cyber Systems. Minnesota Power believes that the intent of authorizing access privileges is adequately covered by Requirement R8, subject to the comments made in Question 20.
24.38	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).

#	Organization	Yes or No	Question 24 Comment
24.39	Pacific Gas & Electric Company	Disagree	Need to consider physical security interaction with “cyber” security. An example is a substation control panel (handles, etc, which you can physically operate various devices in a sub) that is physically co-located with electronic devices that perform the same functions. In this case “electronic access control” for local access to should not be required.
24.40	NextEra Energy Corporate Compliance	Disagree	NextEra comments that in reference to the footnote regarding the situation where the "device is not capable of meeting the password threshold, then implement the maximum password complexity that the device can support", isn’t this better presented for the Responsible Entitiy to have a mechanism to file for a TFE or any other exception process proscribed by the Standards?Regarding 10.8, what is the expected documentation and/or account management access control actions to demonstrate requiring users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions?Regarding R10.2, how are BES Cyber Systems not capable of technically enforcing password changes handled? Are procedural controls sufficient to meet this requirement?Additionally, how could one demonstrate compliance with R10.2 if the BES Cyber System Component is not capable of logging when the password was last changed (e.g. protective relays)?Requirement 10.2 time requirement for changing passwords at least once every 12 months does not take into account or include verbiage for legacy systems that do not have the functionality to change passwords, Is there an opportunity for an exception with evidence from the BES Cyber System component manufacturer? There should also be verbiage included in the requirement for exceptions related to BES Cyber system components that passwords cannot be changed due to operational and reliability impacts to the BES. For requirements 10.3 - 10.5, it is unclear how responsible entities document implementing the password scheme requirements. Does the responsible entity comply with having a policy that indicates the necessary requirements or is it necessary that these requirements are enforced technically by the BES Cyber System component? It is recommended that these requirements are satisfied by policies

#	Organization	Yes or No	Question 24 Comment
			instituted by the Responsible Entities and the verbiage indicates that the requirements do not have to be technically enforced. Another recommendation is that there are allowable exceptions to this requirement if a BES Cyber System component cannot technically enforce the requirements, since there are a number of legacy systems that cannot enforce this requirement.For requirement 10.6, there needs to be direction on documenting how access permissions are the minimum necessary to perform work functions. A recommended approach should indicate that the responsible entities administer policies requiring the concept of least privilege concerning their role-based access control administration. Lastly, it is unclear how requirements 10.7 and 10.8 differ from requirement 8.1, since authorization of adding account and subsequent access has to be included in a process based on the requirement. Requirements 10.7 and 10.8 should be moved to 8.X requirements section and clarification should be made as to what explicit authorization means. Is this authorization required each time a user has to access system and security administrative functions? In addition, how is the Responsible Entity supposed to demonstrate compliance to 10.7 and 10.8?
24.41	Southern Company	Disagree	Password requirements written to the level specified in R10.3 through R10.5 have proven unworkable in past versions of the standard. What should be included is only a requirement for strong authentication measures so that alternative, possibly superior, technology is not disallowed.
24.42	Platte River Power Authority	Disagree	Question:Require users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions What is meant by “other system functions”? What if the “other system functions” require a privileged account?
24.43	Consultant	Disagree	R10 (and others) Suggest the wording "to prevent malicious operation of BES Elements by maintaining control of access to its ES Cyber Systems." be modified to remove the phrase "to maintain control of access to its ES Cyber Systems." Account management and access control do not prevent malicious operation. The objective of

#	Organization	Yes or No	Question 24 Comment
			the standard is to prevent malicious operation, but the requirements control access (in this group), which is only one of the actions required by the standards "to prevent malicious operation."Table R10 - Items 10.3, 10.4, and 10.5 - These are statements of "How To" regarding technical implementation and should be changed to be a "What" requirement by using the words from the footnote: "implement the maximum password complexity that the device can support."Suggest items 10.6 & 10.7 be moved to the table R8, as these statements regard account management rather than access control.Item 10.8 This item should be removed. "Non-privileged account" is not an account type required by R7, and is a subjective term. "other system functions" is not defined and is also a subjective term. "security administrative accounts" is not a defined term. This statement uses multiple undefined and subjective terms and does not establish a requirement that can be implemented or audited.
24.44	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R10. System functionality and capabilities may not allow an entity to meet this requirement. Will there be language added to relieve this requirement if the system is not capable? R10.8 should contain language specifying that it applies to other system functions that do not require system level access.
24.45	Con Edison of New York	Disagree	R10.1 Changing passwords on equipment that are not networked, such as relays, is very labor intense. This activity and will be a year-long job because by the time you finish, you will need to go back to the first relays and start changing those again. The requirement to change these passwords on a yearly basis should be on systems that are networked. There must be a lower level requirement on the non-networked equipment.R10.6 Some system may not technically have the ability to perform this function.R10.8 The purpose of this requirement is not clear.R10.7 requires “explicit” authorization. This requirement should allow for specific personnel designation to be authorized for access and not require it be by name. For example LAN administrators by job definition should be able to be authorized for a specific level of access.R10.8 requires LAN administrators to log in differently if they do not need full access for the current task. This can be enforced procedurally although there should be no expectation that this can be documented to show that in each case the correct login

#	Organization	Yes or No	Question 24 Comment
			was used.R10.8 - Impossible to verify compliance or audit this, should be removed
24.46	Kansas City Power & Light	Disagree	R10.8 is unmanageable in the "windows" world. These requirements are too prescriptive and consideration should be given toward what needs to be accomplished and less on how to accomplish it.
24.47	Western Area Power Administration	Disagree	R10: Biometric and token-based factors not addressed. They need to be. R10.3 - Suggest combining 10.3 & 10.5 to number 10.3 with a 10.3.1 & 10.3.2. R10.4 - Delete 10.4 & just use 10.5 for both Medium & High.R10.4 - Are there exceptions for any equipment that doesn't handle special characters?R10.5 - Are there exceptions for any equipment that doesn't handle special characters?
24.48	ISO New England Inc	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1 and 10.8 repeats 7.2Concerned that 10.6 will be hard to audit, should be a policy statement and included in R1. There is no clear way to audit this requirement and is open to auditor interpretation. This can be easy to audit if an administrator has admin access everywhere or a dispatcher has admin access in the application as well as components. But really an auditor's opinion may differ from BES cyber system's owner.R10.8 Should be a policy statement and included in R1. There is no clear way to audit this requirement. How is this going to be audited? Whether a user has two accounts?R10.7 Please explain "explicit" authorization, versus authorization? They seem to be the same why the emphasis.
24.49	Northeast Power Coordinating Council	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.The use of the "minimum" will make 10.6 difficult to audit (refer to the response to Question 54).
24.50	Black Hills Corporation	Disagree	Recommend that 10.4 be eliminated and medium impact systems be subject to 10.5 (subject to the footnote). Implementing both adds training complexity that has little value.

#	Organization	Yes or No	Question 24 Comment
24.51	Northeast Utilities	Disagree	Regarding 10.4 and 10.5 - Most, if not all, security software can not make the distinction to this level of detail nor can it be effectively monitored manually. Recommend that the criteria MS Windows defines today for password complexity is used. Additionally, trying to make a distinction by BES impact can lead to unnecessary confusion when going to this level of granularity.
24.52	EEI	Disagree	Regarding Table R10 Row 10.1:Default vendor passwords should be changed before or during commissioning for use.Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o "special" characters (e.g. #, $, @, &)Regarding Table R10 Row 10.7:It is not clear what "security administrative functions" means. Moreover, it appears duplicative of requirement 10.6.
24.53	Allegheny Energy Supply	Disagree	Regarding Table R10 Row 10.1:Where possible, default vendor passwords should be changed before being commissioned for use.Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o "special" characters (e.g. #, $, @, &)This should also include the ability to provide alternatives such as 2 factor authentication where all the types of characters for a single password may not be possible.Regarding Table R10 Row 10.7:It is not clear what "security administrative functions" means. Moreover, it appears duplicative of requirement 10.6.
24.54	Allegheny Power	Disagree	Regarding Table R10 Row 10.1:Where possible, default vendor passwords should be changed before being commissioned for use.Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o "special" characters (e.g. #, $, @, &)Regarding Table R10 Row 10.7:It is not clear what "security administrative

#	Organization	Yes or No	Question 24 Comment
			functions" means. Moreover, it appears duplicative of requirement 10.6.
24.55	BGE	Disagree	Replace the word "element" with "Cyber System Component" to maintain consistency with the defined terms.
24.56	Duke Energy	Disagree	Requirement 10.1: Passwords should be changed BEFORE making the system operable as opposed to "after installation," as written currently.Requirement 10.2: change passwords once every 12 months. Nuclear plants are on an 18 month fuel cycle. Some are moving to a 24 months. Ideally, systems would be started up at the end of a refueling outage and not touched, save for required maintenance activities until the beginning of the next refueling outage. If the maintenance activity didn't require electronic access, then having each technician/engineer/operator go to the device and change their user specific password on a 12 month basis is actually adding more risk to the BES. Alternate controls can be just as effective with less risk - for instance, installing a stand-alone (e.g. not network/serial/wireless connected) device located in a locked/alarmed cabinet. Is there any allowance for such an alternate control? Also, can this requirement be lessened for low impact systems?10.3 State that multi factor token may be used in place of password.Requirement 10.6: Require that authorized access permissions are the minimum necessary to perform work functions. This applies to user permissions as opposed to administrator functions, correct? Administrator privileges typically include all permissions.
24.57	Nuclear Energy Institute	Disagree	Requirement 10.1: Passwords should be changed before making the system operable as opposed to "after installation," as written currently.Requirement 10.2: change passwords once every 12 months. Frequencies for all requirements should be defined by the Entity, and not defined in these Standards. If a time must be specified in the Standard, then a process must exist for the frequency to be tailored to meet operational requirements.
24.58	USACE HQ	Disagree	Requirement 10.3 should include the language in the footnote to make it clear that

#	Organization	Yes or No	Question 24 Comment
			that is an option under the standard.
24.59	Garland Power and Light	Disagree	Requirement R10 - Paragraph needs to state that a policy or procedure requiring password length, complexity, and password changes are adequate and do not need to be technically enforced by the device.
24.60	Oncor Electric Delivery LLC	Disagree	Requirements 10.5 and 10.7 cannot be applied to all legacy systems currently in-service as they do not support account management. These should allow for TFE. Mandated password change should only be on High impact systems with routable/dial-up communications.
24.61	Xcel Energy	Disagree	Since not all deices are capable of supporting these password requirements, this is an area where TFE need to be allowed. We are concerned with Requirement 10.2 to change passwords every 12 months. For substation devices this would a significant burden, especially for low and medium impact systems.
24.62	ERCOT ISO	Disagree	Since the purpose of this is basically the same as the previous requirements, these could all be combined into a single requirement. 10.1: Recommend specifying a time-frame for changing passwords. 10.2-10.5: Recommend that the requirements address the use of alternate authentication means, such as biometrics and RSA SecurID. TFEs should be allowed for the requirements under this section.
24.63	MidAmerican Energy Company	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
24.64	Ameren	Disagree	Suggest changing R10.1, R10.2, and R10.3 for Low Impact BES Cyber System requirement to “Required, unless system is behind a firewall or other protective measures.” Giving password strength criteria is too specific when entities may use

#	Organization	Yes or No	Question 24 Comment
			other ways to implement security that meet or exceed this requirement. The manpower necessity for changing passwords yearly and maintaining a protected/immediately accessible database to store passwords so that those who need to access relays can when needed for Low Impact Systems is not needed. If all the High Impact System relays have firewall protection that should be enough. The industry needs to be able to access relays to keep the BES system functional and respond to operational issues. Also, for R10.1 need to clarify how long after installation should a vendor password be changed.â€,â€,R10.4 and R10.5 - These requirements will be difficult to prove in an audit. Should be changed to provide a documented process should be sufficient and should be less trouble in dealing with an audit on these requirements. However, some systems may not be able to adhere to these policies, and TFE's may be required.R10.6 - Documentation of the permission check will be volumes of data that will have to be performed in the audit. This requirement needs a periodic review time associated with it.R10.7 - What is the intention of this requirement? If all access is already accounted for in R10.6 isn't this requirement duplicate effort?
24.65	Entergy	Disagree	Suggest simplifying requirements 10.4 and 10.5 by combining and rewriting into: “Implement a password scheme that cannot be found in the dictionary and has at least three of the following four attributes: Lower case alphabetic, upper case alphabetic, numeric, “special” characters (e.g. #, $, @, &)”Requirement 10.8 should be reviewed from a technology perspective. While use of a “normal” user account and gaining “root” access through “sudo” is robust in the UNIX variant operating systems, performing the same function in the Windows operating system can be problematic with logging in as a different user all together. Suggest possibly relaxing this requirement.
24.66	ReliabilityFirst Staff	Disagree	Table R10; row 10.2 - High Impact BES Cyber Systems should have the password changed at least every 6 months. Regarding footnote 1, for devices that are not capable of meeting the password threshold, the entity should be required to

#	Organization	Yes or No	Question 24 Comment
			document this situation, including compensating measures, for audit review.
24.67	Southern California Edison Company	Disagree	Technical capability is not a homogenous quantity in a system with diverse classes of devices and thus the ability to implement generic controls over a heterogeneous system does not always exist. A means to seek exception from the "word" of the standard, while still complying with the intent which is to clearly identify technical situations where a prescribed control, is not implementable while maintaining cyber security protections is needed. Requirements R10.4 and R10.5 are too prescriptive and do not allow registered entities to seek out alternative access authentication mechanisms. For instance, biometrics or 2-factor authentication based on numerical passwords generated by a key-based security architecture may not meet the word of the standard but go above and beyond the intent of the standard.
24.68	USACE - Omaha Anchor	Disagree	TFE will be required for this section if verbiage isn't added to address lower level machines where some items (10.7, 10.5) are not possible.
24.69	Manitoba Hydro	Disagree	The account access control requirements should be more generic and technology independent, allowing the entity to apply a variety of account access controls. If passwords are needed, Requirement R10.3 should also require some "special" characters, to the extent that the device is capable. The standard should also allow protection by layers of security, which may be provided by other methods or cyber systems.
24.70	APPA Task Force	Disagree	The APPA Task Force supports the proposal by MRO-NSRS to be more generic in the wording of the requirements in R10, to account for innovations such as biometric controls used in lieu or in conjunction with password controls.We propose the following edits to R10:R10 Table 10.1: Restrict electronic access to BES Cyber Systems through use of an electronic access control that does not use/rely on the vendor defaut password.R10 Table 10.2: Electronic access controls must be updated/modified at least once annually.Since numerous devices would be exempt from this requirement due to their inability to support password protection, the term

#	Organization	Yes or No	Question 24 Comment
			"Electronic Access Controls" should replace "Passwords". This is non-limiting and will not lock into the standard a current technology, for example, keyboard-based "password access."APPA proposes that items 10.3 - 10.5 be removed from this requirement and be submitted to the "guideline in support of the standard" drafting team to be included as a best practice for account access control. If 10.3-10.5 must remain in the requirement we recommend they be less technology-specific. We propose the following language:R10 Table 10.3: Implement a password scheme that has a minimum of six characters, or an electronic access control with an equivalent or superior technology option.R10 Table 10.4: Implement a password scheme that has at least two of the following four attributes: Lower case alphabetic, upper case alphabetic, numeric, "special" characters (e.g. #, $, @, &), or an electronic access control with an equivalent or superior technology option. R10 Table 10.5: Implement a password scheme that has at least three of the following four attributes: Lower case alphabetic, upper case alphabetic, numeric, "special" characters (e.g. #, $, @, &), or an electronic access control with an equivalent or superior technology option.In Table 10.6 the wording "the minimum necessary to perform work functions" is subjective and will be difficult to measure. We propose this be replaced with "Require that access permissions are in accordance with the entity access authorization policy required in R1."
24.71	Constellation Energy Control and Dispatch, LLC	Disagree	The appropraite account access control mechanisms should not be specifically defined in the Table R10.
24.72	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.In today's electronic world there are many methodologies for electronic access control. Many systems now make use of multi-factor passwords, and/or biometrics. They use passwords or

#	Organization	Yes or No	Question 24 Comment
			pass-codes are randomly generated, encrypted and time sensitive. Access codes or passwords may be one time, expiring after one use, and/or after a specified time (usually 60 seconds). The systems implemented may also provide checks to insure that the passwords are not captured and hijacked. These modern methodologies are far more effective and secure than the stated requirements. This requirement is prescriptive and too specific. The way it is written it would preclude the use of modern and stronger tools because they may technically not meet one or more of the specifications, even though they are bigger, better and stronger. If the requirements must remain this prescriptive, then the following changes should be made:- There should be a second footnote, "Stronger methods, such as multi-factor authentication of one-time passwords, may be used in lieu of username/password combinations."- 10.1: A time frame for "after installation" needs to be specified.- 10.3: Given the efficacy and availability of Rainbow Tables, a 6-character password is woefully inadequate. The minimum should be at least 10, and 14 would be better. - 10.6: There's a difference between "minimum necessary" and "minimum practical and necessary". Strict interpretation would require that access grants would change depending on the task being performed, which is probably not the intent. Suggest the wording be changed as described. An alternative would be to use the NIST definition of "Least Privileges - The security objective of granting users only those accesses they need to perform their official duties" (NIST IR 7298 - NIST Glossary of Key Information Security Terms) and then require the use of Least Privileges.Item 10.2 in Table R10 states that "/p/asswords must be changed at least once every 12 months". Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently passwords must be changed.
24.73	Reliability & Compliance Group	Disagree	This requirement does not consider the use of biometric access systems such as finger print readers that could be used in place of password verification.Also, it should include the word "electronic" when it talks about "maintaining control of access to its BES Cyber Systems."

#	Organization	Yes or No	Question 24 Comment
24.74	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments regarding footnote 1 and Table R10 Row 10.7.
24.75	American Transmission Company	Disagree	We believe the depth of detail in R10 needs to be better coordinated with the rest of the standard, where the entity is told what they need to do, not explicitly how to do it. R10 appears to be overly prescriptive, which could potentially box entities in if they want to exceed the requirements of the standard.We would propose replacing item 10.1 with something more generic, like "Restrict electronic access to BES Cyber Systems", similar to how physical access is handled under R5.1. Passwords may not apply in all cases, and some entities may wish to implement alternative methods of user authentication that are superior, but as currently worded they would be limited by the standard.We would also propose replacing item 10.2 with something more generic, like "Electronic access controls shall be reviewed at least once every 12 months". A requirement for changing the access controls every 12 months is not applicable for an entity using biometrics scanning as opposed to passwords.We would propose deleting items 10.3 - 10.5, as they would not apply under the approach proposed here. Finally, the standard should allow for other control methods such as front ending a device with a fully password protected access control device instead of the required password controls directly on the device.
24.76	MRO's NERC Standards Review Subcommittee	Disagree	We believe the depth of detail in R10 needs to be better coordinated with the rest of the standard, where the entity is told what they need to do, not explicitly how to do it. R10 appears to be overly prescriptive, which could potentially box entities in if they want to exceed the requirements of the standard.We would propose replacing item 10.1 with something more generic, like "Restrict electronic access to BES Cyber Systems", similar to how physical access is handled under R5.1. Passwords may not apply in all cases, and some entities may wish to implement alternative methods of user authentication that are superior, but as currently worded they would be limited by the standard.We would also propose replacing item 10.2 with something more generic, like "Electronic access controls shall be reviewed at least once every 12

#	Organization	Yes or No	Question 24 Comment
			months". A requirement for changing the access controls every 12 months is not applicable for an entity using biometrics scanning as opposed to passwords.Finally, we would propose deleting items 10.3 - 10.5, as they would not apply under the approach proposed here.
24.77	The Empire District Electric Company	Disagree	We believe the depth of detail in R10 needs to be better coordinated with the rest of the standard, where the entity is told what they need to do, not explicitly how to do it. R10 appears to be overly prescriptive, which could potentially box entities in if they want to exceed the requirements of the standard.We would propose replacing item 10.1 with something more generic, like "Restrict electronic access to BES Cyber Systems", similar to how physical access is handled under R5.1. Passwords may not apply in all cases, and some entities may wish to implement alternative methods of user authentication that are superior, but as currently worded they would be limited by the standard.We would also propose replacing item 10.2 with something more generic, like "Electronic access controls shall be reviewed at least once every 12 months". A requirement for changing the access controls every 12 months is not applicable for an entity using biometrics scanning as opposed to passwords.Finally, we would propose deleting items 10.3 - 10.5, as they would not apply under the approach proposed here.
24.78	We Energies	Disagree	We Energies agrees with EEI: Regarding Table R10 Row 10.1:Where possible, default vendor passwords should be changed before being commissioned for use.We Energies agrees with EEI: Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o "special" characters (e.g. #, $, @, &)We Energies agrees with EEI: Regarding Table R10 Row 10.7:It is not clear what "security administrative functions" means. Moreover, it appears duplicative of requirement 10.6.

#	Organization	Yes or No	Question 24 Comment
24.79	PacifiCorp	Disagree	While the criteria themselves are not onerous for the long term/future development of the systems, the fact is that current BES technology in place or available, will require technical feasibility exceptions as not all systems within the BES can support all criteria listed.The standard needs to allow for non-password based authentication systems or one time passwords. Modify 10.2 through 10.5 with "or equivalent or greater authentication methods"The current password requirements in table 10 are too burdensome and unnecessary. The requirements as written are also confusing. Passwords should not be the only acceptable way to authenticate a user prior to granting access.
24.80	Luminant	Disagree	Will require TFE for some systems

25. Table R10 provides direction concerning what impact level of BES Cyber Systems to which Requirement R10 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R10 moved to CIP-007-5 – Cyber Security - Systems Security Management - Requirement R5.

Commenters indicated that passwords on Low Impact BES Cyber Systems should not be subject to any periodic change as stated in Table R10 (10.2). In response, the SDT revised the password requirements, and they are not applicable for Low Impact BES Cyber Systems.

Commenters suggested a single criterion for password complexity. In other words, do not differentiate by risk level. The SDT agreed and reduced the password complexity requirement to be the same regardless of applicable risk or impact level.

#	Organization	Yes or No	Question 25 Comment
25.1	US Army Corps of Engineers	Agree	Agree with impact levels, but disagree on item Table R10, 10.8: "Require users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions." Add to the end of the statement, if the system function does not require the use of using a privileged account.
25.2	CWLP Electric Transmission, Distribution and Operations Department	Agree	As long as TFEs are available for systems that do not support the password requirements.
25.3	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
25.4	US Bureau of Reclamation	Agree	Recommend we establish Requirement 10.6 for all impact levels. Also, please refer to question #54, comment 2
25.5	Southern California	Agree	Requirement 10.7 may be interpreted that access need not be denied as a default

#	Organization	Yes or No	Question 25 Comment
	Edison Company		setting. If the intent of the drafting team is a different control, the team should consider rephrasing this requirement.
25.6	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
25.7	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels for R10 if it is understood that a blank in the table means N/A. The APPA Task Force agrees with the MRO-NSRS proposal:"If the standard were to remain as written, we would propose that the 10.1 - 10.3 requirements be removed for Low Impact systems, and be "Required for remote access or routable external connectivity only" for Medium Impact systems."
25.8	GTC & GSOC	Agree	We recommend 10.8 to be changed to: "Require persons to use non-privileged accounts when accessing system functions that do not require privileged accounts"
25.9	Exelon Corporation	Agree	We would suggest the password items begin with "Where passwords are utilized they must ...." These requirements should allow entities the flexibility to use other user authentication methods besides just passwords such as two factor tokens or other methods that provide even better protection than just passwords. Exelon appreciates the clarification provided in footnote #1 which has the potential to limit the number of TFEs that would be required.
25.10	Regulatory Compliance	Disagree	10.1 - 10.3 STRIKE "Required" for Low Impact10.6 - STRIKE "Required for medium impact - inconsistent with level.
25.11	LCEC	Disagree	10.2 is not auditable as a performance requirement.Footnote [1] is subject to major interpretation: complexity is ambiguous. May not be legally defensible. Maximum should be maximum comparable.We suggest removing 10.6 it is too subjective.
25.12	BGE	Disagree	10.2 maintain consistency for timeframes (i.e. use 12 months or annual). 10.3, 10.4

#	Organization	Yes or No	Question 25 Comment
			and 10.5 should be combined.10.6 needs a definition for "minimum". 10.8 needs clarification for the meaning of "other system functions".
25.13	Dominion Resources Services, Inc.	Disagree	10.2. It is anticipated that there will be thousands of Low Impact devices geographically spread across a utility's system. By definition these devices provide little risk to the BES. It is impractical from a resource perspective and unnecessary from a reliability perspective to change the passwords of low impact components every 12 months. The requirement should be removed from Low Impact.
25.14	ERCOT ISO	Disagree	10.7-10.8: Should apply to Medium Impact BES Cyber System.
25.15	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
25.16	Southern Company	Disagree	As long as there are requirements which include per-component action for each low-impact BES Cyber System, the effort needed to implement those actions will overwhelm the rest of the CIP compliance effort. For example, a reasonable estimate is that our Entity will have approximately 2,500 low-impact substations with an estimated 100 programmable devices in scope per substation. Without any other consideration of work required, that represents 250,000 password changes each year to be performed, tracked, and communicated. The majority of those devices have hardware override switches which disable password protection for anyone who has physical access to the device, so no reliability advantage is gained by performing the password change. This is just one example of the scope of work with little or no benefit to the BES that is required as long as there are per-component low-impact requirements.The standards should be modified so that requirements for low-impact cyber systems include only program-wide efforts such as policy, governance, incident response planning, and disaster recovery planning.If low-impact requirements cannot be eliminated completely, then at least the specific requirements for password changes for components with no external connectivity should be removed, as they provide no additional benefit when paired with physical security requirements.In addition, vendor contracts with sole suppliers of necessary equipment may conflict

#	Organization	Yes or No	Question 25 Comment
			with 10.1. At the least, this creates the necessity for a large, cumbersome TFE program.In 10.1, the phrase "after installation" should be replaced by "before, during, or immediately after installation".10.4 and 10.5 create a TFE burden without any substantial benefit and disallow advanced technology that provides stronger authentication but does not meet the literal wording. Instead, the requirement should be modified to require authentication.
25.17	Tenaska	Disagree	At the end of R11 just add "identify restrictions and uses for accesses". And remove table.
25.18	Constellation Energy Commodities Group Inc.	Disagree	Choose a single standard for password complexity, rather than differentiating by risk level.
25.19	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
25.20	The Empire District Electric Company	Disagree	Comments: With the changes proposed in question 24, we would propose that revised items 10.1 and 10.2 be "Required" for Low, Medium, and High Impacts.We would agree with the current impact levels for items 10.6 - 10.8.However, it the standard were to remain as written, we would propose that the 10.1 - 10.3 requirements be removed for Low Impact systems, and be "Required for remote access or routable external connectivity only" for Medium Impact systems. Once someone has gained physical access to a facility, the hurdle of a password does very little to limit the amount of physical damage or misuse that can be done. However, for remote access, the password becomes critical to preventing damage or misuse. We also believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
25.21	Southwest Power Pool	Disagree	Complex passwords and minimum password lengths are a basic security control and

#	Organization	Yes or No	Question 25 Comment
	Regional Entity		should be applicable to all impact categories.
25.22	E.ON U.S.	Disagree	E.ON U.S. does not believe a requirement is necessary for low impact items.
25.23	Consultant	Disagree	Item 10.2 - There is no requirement for account management for Low Impact assets, and it is illogical to require password controls where there are no account controls.
25.24	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
25.25	Progress Energy (non-Nuclear)	Disagree	Low impact BES systems should not have this requirement. By virtue of their definition they do not need this requirement.CIP-011 R10 - Would like to compliment the SDT for constructing a realistic and reasonable approach with regard to effective use of complex passwords. The SDT has recognized that there may be password complexity limitations with older existing electronic gear that is in operational service and rather than try to mandate a standard that is technically not feasible to implement, they have provided the footnote to require that practical password complexity should be set to the maximum that the device is capable of supporting.CIP-011 R10 - Account management access control & passwords is this meant to include BIOS or only interactive logins to devices?10.2 - "Passwords must be changed at least once every 12 months", If this is referring to cyber system components, this represents unreasonable costs to utilities. Password changes for relays with no remote capability will be cost prohibitive, and password changes for individual relays with remote capability will require excessive time.
25.26	NextEra Energy Corporate Compliance	Disagree	NextEra believes for Low Impact BES Cyber Systems, requiring passwords to be changed at least once every 12 months should be changed at least every 24 months; for Medium Impact BES Cyber Systems, we suggest changing passwordsat least every eighteen months.
25.27	Alberta Electric System	Disagree	Please consider the following changes to increase security and make the

#	Organization	Yes or No	Question 25 Comment
	Operator		requirements more restrictive:Table 10.2 - passwords changes at least once every three months.Table 10.3 - minimum eight character password (with same footnote)Table 10.4 - change to “three of the following five attributes” and include two-factor authentication as an additional attribute.Table 10.5 - change to “four of the following five attributes” and include two-factor authentication as an additional attribute.Table 10.6 - required for Low, Medium, and High impact levelsTable 10.7 - required for Medium and High impact levelsTable 10.8 - required for Medium and High impact levels
25.28	American Municipal Power	Disagree	Please provide a little or no impact category
25.29	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management, Table 9 Access Revocation, and Table 10 Account Access Controls. Additionally, if physical security is not required for Low Impact BES Cyber Systems, then Puget Sound Energy suggests including wording similar to Table 5: “Required for routable connectivity only”.
25.30	Con Edison of New York	Disagree	R10.6 should not be required for medium impact
25.31	Ameren	Disagree	R10.8 - Should be added for Medium Impact Systems.
25.32	ISO New England Inc	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1 and 10.8 repeats 7.2
25.33	Hydro One	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.We’d like to know the full meaning of “explicit authorization”. If possible please add the definition in the glossary.
25.34	Northeast Power Coordinating Council	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.

#	Organization	Yes or No	Question 25 Comment
25.35	Black Hills Corporation	Disagree	Recommend that 10.4 be eliminated and medium impact systems be subject to 10.5 (subject to the footnote). Implementing both adds training complexity that has little value. Similarly, 10.7 & 10.8 should also apply to medium impact systems.
25.36	Northeast Utilities	Disagree	Recommend that the 10.4 scheme (use 2 of 4) is used for both medium and high impact and that the 10.5 scheme (use 3 of 4) is eliminated. Trying to make a distinction by BES impact can lead to unnecessary confusion when going to this level of granularity.
25.37	Minnesota Power	Disagree	Regarding Part 10.2, Minnesota Power believes that the requirement to change passwords for Low Impact Systems at least once every 12 months is excessive. The requirement that a Registered Entity change passwords within this time frame for all BES Cyber Systems is unnecessarily cumbersome and time consuming. In addition, the coordination that would go into making these changes is infeasible and could result in an inability to access the system. In addition, Minnesota Power recommends that the Standards Drafting Team consider adding the following qualifier to Parts 10.1 through 10.5 of Table R10:"...where passwords are used for access control."
25.38	MidAmerican Energy Company	Disagree	Requirement 10.1 needs to state “Change default passwords prior to production operation” or words to that effect. It is imperative that vendor passwords are never placed into a production environment.
25.39	PacifiCorp	Disagree	Requirement 10.1 needs to state “Change default passwords prior to production operation” or words to that effect. It is imperative that vendor passwords are never placed into a production environment.
25.40	SCE&G	Disagree	SDT should consider not requiring Low Imapct systems to have passwords changed annually. This could potentially generate a high volume of TFEs for hardcoded passwords as previously described.

#	Organization	Yes or No	Question 25 Comment
25.41	Constellation Energy Control and Dispatch, LLC	Disagree	See comment provided to question 24
25.42	LADWP	Disagree	See previous
25.43	Western Area Power Administration	Disagree	See previous
25.44	WECC	Disagree	Several of the actions should be done for low impact assets, such as "Require that authorized access permissions are the minimum necessary to perform work functions". Consider relooking at the impact levels.The password requirements should apply to all impact levels.
25.45	Allegheny Energy Supply	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
25.46	Allegheny Power	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
25.47	EEI	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.If low-impact requirements cannot be eliminated completely, then at least the specific requirements for password changes for

#	Organization	Yes or No	Question 25 Comment
			components with no external connectivity should be removed, as they provide no additional benefit when paired with physical security requirements.
25.48	Duke Energy	Disagree	Table 10: o All of Table 10 will potentially require a TFE o 10.1 change 'after installation' to "prior to being placed in service" o Suggest all password verbiage be replaced with 'authentication method' and remove specified attributes. Otherwise TFEs will be required for 10.3-10.5. o For 10.2 change 'at least every 12 months' to 'when security conditions require' o Requirement 10.2: Can this requirement be lessened for low impact systems? o 10.8 requires multiple accounts for individuals with admin rights on individual accounts. Suggest making this applicable only for shared admin accounts or removing for Windows based systems.
25.49	ReliabilityFirst Staff	Disagree	Table R10; rows 10.7 and 10.8, should be "required" for medium Impact BES Cyber Systems.
25.50	Dairyland Power Cooperative	Disagree	The focus is entirely on passwords, but other forms of credentials can be used. For example there are certificate or key based authentication to many systems. Many vendors use default keys that need to be changed, just as default passwords. The password rules are very weak compared to common practices. This seems to be an attempt to encourage the strongest possible password on legacy components/systems, but the by-product is that this weakens the requirements for modern systems. There should be a better way to deal with legacy systems while requiring new systems to use stronger passwords.
25.51	FirstEnergy Corporation	Disagree	The impact levels are agreeable assuming the changes suggested in Q24.10.1 Vendor default passwords should be changed based upon a clear definition of "installation." Non-password authentication sources need to be addressed. Possibly combine 10.4 and 10.5, but keep the note on implementing the maximum password complexity.FE request that the "Required" shown in the Low Impact column of rows 10.2 and 10.3 be removed. Password changes to Low Impact items should not be a requirement in the standard but left as a "best practice" guideline. A requirement to annually change

#	Organization	Yes or No	Question 25 Comment
			passwords to multiple digital protection relays associated with Low Impact facilities would be extremely burdensome with little reliability improvement. Each relay would require individual attention as there is no method of globally changing all digital relay passwords. If retained, consider allowing entities to synch up the changing of passwords on these devices with their normal PRC-005 maintenance cycles.
25.52	Southwestern Power Administration	Disagree	The language in this requirement should be changed to include a broader scope of technology or to be technologically neutral so that new or emerging technology (such as biometrics) which may be more secure than passwords will still be considered as in compliance.
25.53	Entergy	Disagree	The requirement indicates that the drafting team believes protection of sensitive information associated with allegedly "low impact" BES Cyber Systems/Components that provide routable protocol attack vector access to control hosts, etc., is unnecessary. Suggest this be rethought.Suggest making password requirements for all assets meet the requirements for high assets and let foot note as written take care of the assets that are unable to meet the requirement.
25.54	American Transmission Company	Disagree	The standard should allow for other control methods such as front ending a device with a fully password protected access control device instead of the required password controls directly on the device.
25.55	Florida Municipal Power Agency	Disagree	The table should have different levels of password entropy required for the different impact areas. For example, medium impact systems should have 40-bits of required entropy, while high impact systems should require 64-bits of entropy. Low impact may be able to get by with 32-bits of entropy.
25.56	Oncor Electric Delivery LLC	Disagree	These requirements should only apply to Control Center Cyber Systems.
25.57	We Energies	Disagree	We Energies agrees with EEI: Sufficient Password security can be accomplished by

#	Organization	Yes or No	Question 25 Comment
			combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
25.58	MRO's NERC Standards Review Subcommittee	Disagree	With the changes proposed in question 24, we would propose that revised items 10.1 and 10.2 be "Required" for Low, Medium, and High Impacts.We would agree with the current impact levels for items 10.6 - 10.8.However, if the standard were to remain as written, we would propose that the 10.1 - 10.3 requirements be removed for Low Impact systems, and be "Required for remote access or routable external connectivity only" for Medium Impact systems. Once someone has gained physical access to a facility, the hurdle of a password does very little to limit the amount of physical damage or misuse that can be done. However, for remote access, the password becomes critical to preventing damage or misuse. We also believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
25.59	Emerson Process Management	Disagree	With the latest Windows OS, there is really no great difficulty of asking for complex password. This requirement can be easily applied. The only thing is enforcement. This enforcement may be retuired for high or medium impact BES Cyber Systems.

26. Requirement R11 of draft CIP-011-1 states "Each Responsible Entity that allows remote or wireless electronic access to any of its BES Cyber Systems shall apply the criteria specified in CIP-011-1 Table R11– Wireless and Remote Electronic Access Documentation to ensure that no unauthorized access is allowed to its BES Cyber Systems. Do you agree with the list of criteria that are included in Requirements Table R11? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

The remote access requirements from CIP-011-1 have been moved to CIP-005-5 - Cyber Security - Electrnic Security Perimeters – Requirement R2. The wireless requirements have been removed.

Commenters suggested more clarity was needed in the terms "remote access" and "external connections" and "wireless". The SDT proposed the following formal definitions for additional clarity on "remote access" and "external connectivity," and removed wireless access requirements from the revised Standard.

External Connectivity: *Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter*.

External Routable Connectivity: *The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.*

Interactive Remote Access: *Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.*

Commenters suggested that wireless and remote access be broken out into separate requirements. In response, the SDT notes that wireless access requirements have been removed from the Standard. There is a single requirement for Remote Access in CIP-005-5 R2.

Commenters stated that given the local definition of Remote Access, the requirements of Table 11 Row 11.2 are extremely unclear. In response, a new requirement for Remote Access Management (CIP-005-5 R2) was created based on the Urgent Action Revisions to CIP-005-3.

#	Organization	Yes or No	Question 26 Comment
26.1	Regulatory Compliance	Agree	BUT:11.1 Please clarify whether these are wireless technologies within the electronic boundary or wireless technologies originating outside the electronic boundary.
26.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
26.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made."shall implement the requirements ..." makes the bullets individual requirements, which FMPA does not believe what the intent of the drafting team. FMPA suggests "shall implement the security controls ..." as an alternative.Consider combining R7, R8, R11 and R12. FMPA believes the standard should be more clear as to if this is wireless connection that is under the complete control (end-to-end) of the Responsible Entity or not. There is no way an individual can ensure that their data path, once outside of their control, routes over a wireless device or not. For access that is not under the control of the RE, the standard should refer to it just as it might for any other remote access control, demanding that the data is encrypted and the end point is protected.
26.4	Progress Energy - Nuclear Generation	Agree	R11 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
26.5	BCTC	Agree	Suggest rewording from Wireless and Remote Electronic Access to Wireless or Remote Electronic Access
26.6	APPA Task Force	Agree	The APPA Task Force believes disabling the wireless functionality should be an option. If the description is not changed as proposed in Question #17 then we recommend that R11 Table 11.1 should include "and/or document that the wireless functionality is disabled."

#	Organization	Yes or No	Question 26 Comment
26.7	Bonneville Power Administration	Agree	The objective of this requirement ("to ensure that no unauthorized access is allowed to its BES Cyber System") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.It it not clear that wireless needs to be specifically addressed. It is one of many access methods that may be use. If it is to be specifically addressed, then it should be treated separately, but as a sub-class of remote access. (Even if wireless access is intended to be used for access by Entity personnel, its very nature means that access could be gained from other locations.)If it is addressed at all it should be limited to requiring adequate protection for Wireless Access Points, but not to the level of specifically prescribing the methods that need to be taken.Finally, "Wireless Access" needs to be defined. The most common usage refers to wireless local area networks under one of the 802.11 standards. But, technologies such as point-to-point communications using microwave or laser are also wireless technologies. We offer no suggestions for the definition, since we do not know the intent of the team.
26.8	Progress Energy (non-Nuclear)	Agree	We like the clarity provided by the use of the term "interactive" remote access.
26.9	Independent Electricity System Operator	Disagree	- R11 combines Wireless and Remote access. It is suggested that this be broken out in to separate requirements. Seems like an assumption that if you are connecting via wireless you are remote - not always the case.- R11.1 - Is this just a policy stat
26.10	BGE	Disagree	11.1 Define "wireless technology" (i.e. could implicate a cell phone). Throughout the table when "external connectivity only" is stated this can be interpreted as a connection from the DMZ or other company network.
26.11	Black Hills Corporation	Disagree	All BES systems should have should have access controls regardless of hard line /

#	Organization	Yes or No	Question 26 Comment
			remote / wireless connection.
26.12	Southern California Edison Company	Disagree	All forms of access documentation should be required along with the level of protction and type of access granted.
26.13	Southwest Power Pool Regional Entity	Disagree	An important aspect of wireless access was overlooked. Prescribe the use of available security features on all wireless access points. If possible word the requirement to not prescribe specific characteristics of configurations (WEP versus WPA, SSID broadcast, MAC address filtering, etc.) in order to not preclude next generation technology.
26.14	Southern Company	Disagree	Better specificity is needed as to what constitutes wireless access. Is the intent limited to 802.11x access or is the intent to include all communication done without wired connectivity?R11.1 This requirement could be interpreted to include all wireless, including voice. Insert “network” prior to “technologies”.
26.15	Luminant	Disagree	Combine 11 and 12? Does this apply to a remote user that may be connected via a wireless network connection at a remote location?
26.16	CenterPoint Energy	Disagree	Disagree - For R11.1, CenterPoint Energy is not clear as to what is meant by "use restrictions". Table R11 is titled "Wireless AND Remote Electronic Assess..." but R11 states "Each Responsible Entity that allows remote OR wireless electronic access..." CenterPoint Energy suggests separating remote and wireless access requirements. CenterPoint Energy also suggests adding clarification as to type of wireless protocols that should be included.
26.17	Exelon Corporation	Disagree	Exelon feels that definition of access needs clarity. Is this meant to include “view only” access or is it limited to administrative access that allows for maintenance, trouble shooting or modification of BES Cyber Systems?
26.18	Duke Energy	Disagree	For generation stations in particular, external connectivity (R3) and remote

#	Organization	Yes or No	Question 26 Comment
			connectivity (R11, R12, R13) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome. Same for R13.Distinction between "remote access" and "external connectivity" is not clear. More clear definitions may need to be provided. Such as, external connectivity allows for direct Internet access vs. remote connectivity allows for access from the enterprise WAN.Table 11: suggest removing 11.3 for low impact systems. No need to authorize remote access when physical or electronic access is not authorized.
26.19	Allegheny Energy Supply	Disagree	Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.20	Allegheny Power	Disagree	Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.21	EEI	Disagree	Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.22	Constellation Power Source Generation	Disagree	In general, Constellation Power Generation believes that wireless controls should be combined with network controls, as the same controls will be applied.
26.23	Minnesota Power	Disagree	In reading and applying the definitions of "remote access" and "external connectivity," remote access is a specific type of external connectivity. Therefore, any reference to criteria for remote access based on whether or not it is externally connected is redundant. In addition, by definition all wireless access is also remote access and this should be stated or otherwise clarified.Regarding Part 11.3 of Table

#	Organization	Yes or No	Question 26 Comment
			R11, does this require explicit approval for every remote login to BES Cyber System accounts? If yes, Minnesota Power believes that this is excessive and will inhibit proper administration of BES Cyber Systems. Minnesota Power recommends changing the language to clarify that Part 11.3 requires that a Registered Entity determine who has authorized remote access privileges.
26.24	Southwestern Power Administration	Disagree	Is a separate requirement for wireless access really necessary when a requirement already exists for protecting access to a BES Cyber System by any means of entry? If so, then suggest separating wireless from remote access.
26.25	Dairyland Power Cooperative	Disagree	It is unclear if the standard wants to make a distinction between wireless and remote access, or an equivalence.
26.26	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with SPP's observation below:We question the need for a specific requirement for wireless devices. We understand there have been inquiries about treatment of wireless devices. But a wireless access point has the same impact on a BES Cyber System as any other access point. A requirement to protect access to a Cyber System already includes any possible means of entry. The use of a wireless device to access a BES Cyber System can be determined with an audit of access logs and a further audit of control of that access would reveal whether appropriate protections were in place. There is not a need for a separate distinct requirement subject to records retention and audit for specific wireless devices. NERC must realize that the more requirements that are added, the more questions/interpretations of words that can result from the requirement. Registered entities become more subject to violations not because they have neglected to protect their BES Cyber Systems, but rather because of differences in understanding of the words of a requirement - all the while the intent of the requirement had never really been “violated”.
26.27	FirstEnergy Corporation	Disagree	Need clarification wireless technology (does it include Wi-Fi, Bluetooth, Routable Protocol).

#	Organization	Yes or No	Question 26 Comment
26.28	National Grid	Disagree	o National Grid recommends changing 11.1 to “Identify the use and security restrictions for wireless technologies”. Are smart phones which have wireless capabilities considered as wireless technologies? Suggest providing examples of wireless technologies in the guidance document. o For 11.2 and 11.3 National Grid recommends changing from “Required for external connectivity only” to “Required” since the criteria already limits the scope to “remote access”
26.29	PacifiCorp	Disagree	PacifiCorp agrees with EEI's observations below:Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.30	Puget Sound Energy	Disagree	Puget Sound Energy requests clarity to NERC’s definition of “wireless”. If NERC means the 802.1x protocol, then it should specify that so as not to confuse entities with radio telecommunication networks and other wireless technologies.
26.31	LCEC	Disagree	R11 - Any wireless portion of a control or administrative session should be included. Remove the term remote and replace with non-console.Many issues surrounding wireless including encryption and open transport, relay communication, PLCs. Need to clearly define scope and expectations.
26.32	ISO New England Inc	Disagree	R11.1 - Is this just a policy statement and belong in R1 or does it need to be enforced and detect violations of the restrictions? How can this be audited? If there are no restrictions is this a violation?For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”
26.33	Ameren	Disagree	R11.1 what is meant by "use Restrictions" does this apply to the type of device allowed to be used on wireless, of the type of use allowed on wireless technology. Please add more detail on this requirement.R11.2 and R11.3 - Does this include Serial communications such as RTU connectivity or other non-routable protocols? Please

#	Organization	Yes or No	Question 26 Comment
			add more description in these requirements.
26.34	Northeast Power Coordinating Council	Disagree	Recommend changing 11.1 to “Identify the use and security restrictions for wireless technologies”.For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
26.35	Detroit Edison	Disagree	Remove requirement 11.1. Wireless electronic access is not an access method; it is just the medium to obtain access. In an effort to remove reference to specific technology, wireless should not be identified anywhere in the standard. References to specific technologies should be addressed in the guidance documentation.R11, R12 and R14 use term “remote electronic access” and R13 uses the term “remote access”. Revise to maintain consistency.
26.36	WECC	Disagree	Requirements R11 and R12 could be combined into a requirement to produce and implement a Remote Access Plan.There are no specific requirements regarding use restrictions on wireless technologies. This criterion cannot be audited.”Wireless” and “remote electronic access” are two different things and should be addressed in separate requirements.There are no specific requirements regarding remote access. These criteria cannot be audited.
26.37	San Diego Gas and Electric Co.	Disagree	SDG&E recommends that the definition be reworded to say "...a device external to the BES Cyber System's network.”
26.38	Network & Security Technologies Inc	Disagree	Section is unclear. Is wireless an example of a technology that might be employed for remote access, or is the SDT positing other uses? Please clarify. In addition, beyond 11.3, section does not contain any explicit requirements for controlling remote access. 11.1 and, possibly, 11.2 as written would more appropriately be included in a policy (R1). Requirements in R11 should be more aimed towards enforcement of “use restrictions” and exclusion of access methods that are not explicitly allowed.

#	Organization	Yes or No	Question 26 Comment
26.39	American Electric Power	Disagree	Security controls for wireless access seem out of place in the remote access area. Wireless Access controls is a form of boundary protection for the network and should be moved to R20-R22.
26.40	Manitoba Hydro	Disagree	Since Requirement R11 refers to external access, the words “for external connectivity only” are unnecessary in the impact columns and should be removed. Requirement 11.3 is unclear if it refers to authorizing remote access as a design, or operational requirement, or does it refer to the authorization of user access and privileges? Please clarify.
26.41	Entergy	Disagree	Suggest breaking out wireless access from other remote access. These are two distinct technology types, and breaking out within this document the use restrictions and minimum security countermeasures (e.g., WPA, WPA2) for wireless technologies is appropriate.
26.42	Alberta Electric System Operator	Disagree	The AESO believes that wireless access and remote access should be two separate concepts.
26.43	E.ON U.S.	Disagree	The definition of remote access includes the criteria “...from a device external to the BES Cyber System . . . “ With the removal of the concepts of an electronic security perimeter, the boundaries to these systems are not clearly defined, and “external” becomes difficult to determine. It is unclear, for example, whether accessing a BES Cyber System from an internal workstation (though external to the BES Cyber System) constitutes remote access. The definitions for BES Cyber System and BES Cyber Component also do not address the concept of a perimeter.
26.44	Kansas City Power & Light	Disagree	The scope of “wireless” is not clear and can result in interpretation issues throughout these requirements.
26.45	Consultant	Disagree	There is no difference in "remote access" and "wireless electronic access" as remote access is defined in the standard. Suggest deleting reference to wireless electronic

#	Organization	Yes or No	Question 26 Comment
			access in requirement. But if you must have wireless addressed, include it in the definition of remote access.R11. This phrasing is awkward - "to ensure that no unauthorized access is allowed to its BES Cyber Systems" Suggest using wording comparable to R8 "to maintain control of access to its BES Cyber Systems." Table R11 - 11.1 Removing the wireless term from the requirement eliminates the need for this item. Suggest deleting this item.Item 11.3 - This is an account management requirement, and should be moved to R8, and deleted from R11.Item 11.2 - The terminology "Required for external connectivity only" is redundant in this requirement. This requirement is about allowing external connectivity via remote access. Suggest deleting "for external connectivity only"
26.46	Northeast Utilities	Disagree	There is not enough information provided - please specify minimum acceptable security standard allowed (i.e., two-factor, level of encryption, etc.) associated with the use of wireless technologies.
26.47	Emerson Process Management	Disagree	This is a very confusing requirement. Remote does not equal to wireless.The requirement states "allows remote OR wireless electronic access.." The table title is "Wireless AND Remote..."If a remote access is carried out through wired VPN, doesn't this table apply?Does this "remote access" only emphasize on "interactive user session?" If so, this requirement is not applicable to wireless I/O when only data are transmitted to and from BES Cyber System via wireless communications.
26.48	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
26.49	Hydro One	Disagree	We don't understand why the wireless communication is getting special attention. We believe that the protection should remain the same regardless of the type of access point (i.e if it is wired, Wi-Fi, ZigBee etc.). Please explain the rational behind the decision.Recommend changing 11.1 to "Identify the use and security restrictions for wireless technologies".For 11.2 and 11.3 recommend changing from "Required for external connectivity only" to "Required" since the criteria already limit the scope to

#	Organization	Yes or No	Question 26 Comment
			"remote access".
26.50	We Energies	Disagree	We Energies agrees with EEI: Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.We Energies agrees with EEI: The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.51	RRI Energy	Disagree	While the statement 'an interactive user session with a BES Cyber System" is clear to me, examples of "interactive non-user" should be clarified so that the users of this standard know when R11 does not apply. The most common non-user interaction, I would term as "interactive application session". One prevalent wireless "interactive application session" would be a GPS antenna to time synch a cyber asset. Another example would be a wireless serial data IO application. Since these are non-user sessions, R11 does not apply.
26.52	US Army Corps of Engineers, Omaha Distirc	Disagree	Wireless and remote access should be separated.
26.53	NextEra Energy Corporate Compliance	Disagree	Wireless and remote electronic access should be two distinct and separate categories of requirements. Wireless should be defined and it should be established that the term wireless in the context of the requirements is a technology based on 802.1X. As it stands right now, wireless could additionally be considered both blue tooth and radio technologies.Moreover, interactive user session needs to be defined and clarified. It should explain if interactive includes a user session where the user only has read capabilities or if an interactive user session is only applicable when the end user had modification capabilities to the BES Cyber System component. It is unclear how requirement 11.1 adds to the reliability or security of the BES Cyber system. Are the use restrictions per user or are these network restrictions? Moreover, if a Responsible Entity's documented use restrictions are overly broad and insecure, they still comply with the requirement as is. The recommended approach should provide guidelines on acceptable means of securing wireless access to BES Cyber System

#	Organization	Yes or No	Question 26 Comment
			components.Requirement 11.2 should be modified to include the requirement for strong technical and procedural controls for remote access. Requirement 11.3 is vague and unclear as it is currently stated. A responsible entity could misinterpret the requirement for establishing and implementing a defined process for authorizing the establishment of remote access and associated remote access privileges to approve the initial remote access infrastructure and not approving each individual that has remote access capabilities.Requirement 11.3 should be worded to state the following, “If remote access is used and/or implemented, establish, and implement a defined process for authorizing the establishment of remote access infrastructure”NextEra suggests an additional requirement be added and stated as follows:”If remote access is used and/or implemented, establish a defined process for authorizing users to utilize remote access for unescorted interactive cyber access to BES Cyber Systems.”There are not any requirements related to logging or monitoring of remote electronic access and the current requirements within Boundary Protection (R20-R22) requirements do not address this issue either.Finally in 11.2 and 11.3, why make the distinction for "for external connectivity only" rather than just stating that it is "required"? When remote access is used and/or implemented, does it imply "external" connectivity based on the local definition?
26.54	Platte River Power Authority	Disagree	Wireless technology shouldn’t be specifically called out in the standards. Security controls should be broad enough to cover all technologies including wireless and should be handled in their respective sections.

27. Do you agree with the definition of remote access as proposed for this standard? Please explain and provide any suggestions for modification.

Summary Consideration:

The remote access requirements from CIP-011-1 have been moved to CIP-005-5 - Cyber Security - Electronic Security Perimeters – Requirement R2.

Commenters expressed concern that the Standards need better definitions to clarify remote access vs. external access. In response, a new requirement for Remote Access Management (CIP-005-5 R2) for Interactive Remote Access was created based on the Urgent Action Revisions to CIP-005-3.

Commenters expressed that there should be some governance of automated data exchange with remote systems. In response, the SDT noted that automated data exchange (or data in motion) requirements are not considered within scope of this Standard.

The SDT has proposed three formal definitions to provide greater clarity around external connectivity and remote access as they apply to NERC's Reliability Standards:

External Connectivity: *Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.*

External Routable Connectivity: *The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.*

Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

#	Organization	Yes or No	Question 27 Comment
27.1	WECC		Consider renaming to Remote User Access since it is specific to user not other systems or machines. Move to the beginning of the standard. Don't like box in the middle of requirement.Additional language should be added to clarify what constitutes a remote interactive session.

#	Organization	Yes or No	Question 27 Comment
27.2	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	Definition is good, but please see comments for questions 1.a and 1.b.
27.3	Exelon Corporation	Agree	Exelon would like clarity on whether “view only” access would be included in the definition of “interactive user session”? If the answer is no, this should be explicitly stated in the definition of remote access.
27.4	Dairyland Power Cooperative	Agree	However, there should be some governance of automated data exchange with remote systems, perhaps in another section. Also, there is no governance as to how wireless technology can be used for non-interactive data communications.
27.5	Alliant Energy	Agree	However, we recommend consideration of adding clarity to the use of the term “external” in the definition or the replacement of the word “external” with “geographically or logically separate”.
27.6	Consultant	Agree	If "wireless access" has to be specifically stated it should be included in the definition as a method of remote access.
27.7	Southern California Edison Company	Agree	Remote Access is defined without reference to boundaries, logical or physical. For example, access from any device residing in the same local area network, but not part of the BES Cyber System, can be interpreted as Remote Access.
27.8	Florida Municipal Power Agency	Agree	The review periods of the access may need to change with the different levels (12 months for low, 6 for medium, and 4 for high). The standard should require end-to-end encryption between the BES Access Point and the endpoint. Wireless should require minimum standards for 802.11 access points, such as WPA/AES encryption.
27.9	Progress Energy (non-Nuclear)	Agree	This can imply a non routable protocol since a command to open a breaker does result in an operation and provides a subsequent indication that the breaker actually

#	Organization	Yes or No	Question 27 Comment
			did open.
27.10	FirstEnergy Corporation	Agree	We agree fundamentally with the definition, but are concerned about impact to areas outside the BES Cyber System (e.g. Remote access to corporate networks bordering the BES Cyber Systems). Need clarity of "interactive user session".
27.11	Xcel Energy	Agree	We feel it would be beneficial to define the remote access point. For example, a case where a user uses a desktop VPN access to dial-up access a substation relay.
27.12	Independent Electricity System Operator	Disagree	- For 11.2 and R11.3 is Required for external connectivity only. If you connect remotely, how is this not external connectivity to the BES Cyber system - shouldn't these entries just be "required"
27.13	PacifiCorp	Disagree	(See comments on #13) The problem is conflicting definitions. The BES Cyber System Component definition requires that any device providing "control" of the BES Cyber System is to be considered a component of the BES Cyber System. (pg 2, Standard CIP-010-1) Yet, remote access is defined as an "interactive user session with a BES Cyber System from a device external to the BES Cyber System". (pg 12, Standard CIP-011-1)In short, all devices providing 'control' must be considered "BES Cyber System Components", which corresponds to 'internal access'. This definition eliminates remote access that provides control, because the provided function of 'control' requires reclassification as 'internal'.
27.14	US Army Corps of Engineers, Omaha Distirc	Disagree	Agree with general concept of remote access referring to an interactive session from an external location. Definition of external to BES Cyber System is poorly defined. Requirement is too stringent. Breaking systems up into small groups to provide levels of control and protection appropriate to the group of components would be common good practice. This requirement would seem to restrict communication among BES Cyber Systems within a facility and make them cumbersome to manage and protect at appropriate levels. entities need more leeway in defining communication amongst systems and different levels would apply between different systems.

#	Organization	Yes or No	Question 27 Comment
27.15	MRO's NERC Standards Review Subcommittee	Disagree	As written, the definition could be interpreted to include simple data exchanges between an RTU and a SCADA master, although we do not believe this was the intent of the drafting team. We would propose adding the following to the end of the existing definition: "Automated data exchange systems would not be considered remote access".
27.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
27.17	The Empire District Electric Company	Disagree	Comments: As written, the definition could be interpreted to include simple data exchanges between an RTU and a SCADA master, although we do not believe this was the intent of the drafting team. We would propose adding the following to the end of the existing definition: "Automated data exchange systems would not be considered remote access".
27.18	Luminant	Disagree	Controls for Remote access should include only the machines that have direct acces.
27.19	Network & Security Technologies Inc	Disagree	Current definition suffers from inadequacy of the definition of "external connectivity." As suggested in our response to Question 13, we think the definition might be helped by recasting it as meaning interactive access to a BES Cyber System from "outside" an electronic boundary such as an ESP.
27.20	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy is concerned this definition would apply to laptop computers used to perform maintenance on programmable electronic devices and believes that a temporary laptop connection to perform maintenance on an on-site programmable electronic device does not involve the same process as a typical interactive user session through remote access. Therefore CenterPoint Energy believes this requirement should not apply to temporary laptop connections which are otherwise in compliance with section R26 and recommends an exception be included.

#	Organization	Yes or No	Question 27 Comment
27.21	E.ON U.S.	Disagree	E.ON U.S. suggests that the standard specify access is through an “access point”.
27.22	RRI Energy	Disagree	Give more clarity on non-user sessions so that it is well understood that application data sessions are not a part of the “remote access” terminology of R11.
27.23	San Diego Gas and Electric Co.	Disagree	If a device can establish an interactive user session with a BES Cyber System and thus either respond to a BES condition or disturbance or enable control and operation, this “external device” should be named a “BES Cyber System Component.SDG&E recommends that the definition be reworded to say "...a device external to the BES Cyber System's network.”
27.24	US Bureau of Reclamation	Disagree	In addition, however, a mechanism needs to needs to be established to deal with devices locally connected for the purpose of "testing" and "configuration" so that these devices can be periodically connected for a specified and limited purposes. Per discussions during the recent Grapevine, TX, meeting, the drafting teams indicated that they would address this issue during their revision process.
27.25	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
27.26	National Grid	Disagree	National Grid recommends this definition be consistent with the “external connectivity” definition -recommend changing from “from a device external to the BES Cyber System” to “from a device external to the BES Cyber System Boundary”.
27.27	Black Hills Corporation	Disagree	Need a better definition to clarify remote access vs. external access. This creates policy issues for entities with respect to their definitions of these terms.
27.28	Northeast Utilities	Disagree	Need to clarify external connectivity (i.e., from other security domains within the company’s internal network or directly from the public internet). Level of authentication required should differ.

#	Organization	Yes or No	Question 27 Comment
27.29	LADWP	Disagree	Needs more clarification
27.30	NextEra Energy Corporate Compliance	Disagree	NextEra suggests defining external connectivity should be defined and clarified. It is unclear if external connectivity means external to the network the BES Cyber System resides or if it means connectivity from any device to any BES Cyber System component whether it is on the same network. External connectivity should be defined as any remote connection established through the BES Cyber System network access point devices, which includes examples of access point devices, such as dial-up connections, firewalls, SSL VPN connections, etc to a BES Cyber System component. As a point of clarification, since remote access is defined as "an interactive user session with a BES Cyber System from a device external to the BES Cyber System", is the device external to the BES Cyber System now considered a BES Cyber System with the same BES Impact Level as the BES Cyber System in which the device is remotely connecting to? For example, if we have a High Impact BES Cyber System which is an Energy Management System (EMS) within a Control Center, a laptop is used to remotely connect to this EMS, is the laptop now considered a High Impact BES Cyber System?
27.31	Tenaska	Disagree	not needed
27.32	USACE - Omaha Anchor	Disagree	Per your definition one cyber system talking to another cyber system that are side by side would be considered remote access - there seems to be no way to mitigate this. Remote access would be better served defined as communication from outside of the “physical security perimeter” or outside the plant.
27.33	Con Edison of New York	Disagree	R11 dialog box refers to Remote access as an interactive session with a BES Cyber System from a device “external” to a BES Cyber System. It is expected that external means from outside the electronic boundary.
27.34	Hydro One	Disagree	Recommend this definition be consistent with the “external connectivity” definition - recommend changing from “from a device external to the BES Cyber System” to “from

#	Organization	Yes or No	Question 27 Comment
			a device external to the BES Cyber System Boundary".
27.35	ISO New England Inc	Disagree	Recommend this definition be consistent with the "external connectivity" definition - recommend changing from <<from a device external to the BES Cyber System >> to << from a device external to the BES Cyber System Boundary>>
27.36	Northeast Power Coordinating Council	Disagree	Recommend this definition be consistent with the "external connectivity" definition - recommend changing from "from a device external to the BES Cyber System" to "from a device external to the BES Cyber System Boundary".
27.37	American Electric Power	Disagree	Regarding "Remote access for the purpose of this standard means an interactive user session with a BES Cyber System from a device external to the BES Cyber System", should this be "Remote electronic access"? Table R11 refers to "Wireless and Remote Electronic Access Documentation". Adding "electronic" to the definition would maintain consistency.
27.38	Regulatory Compliance	Disagree	Remote access - access originating from outside the eletronic boundary.
27.39	Southwest Power Pool Regional Entity	Disagree	Remote access can be application-to-application and should not be limited to just interactive access. For example, an FTP file transfer works the same way whether invoked interactively by a human user or programmatically by an application. It makes no sense to establish requirements for interactive access only.
27.40	Duke Energy	Disagree	See above, external to station. For generation stations in particular, external connectivity (R3) and remote connectivity (R11, R12, R13) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome. Same for R13.The definition may need to state "a device external to the BES Cyber System and outside the BES Cyber System electronic boundary".

#	Organization	Yes or No	Question 27 Comment
27.41	MidAmerican Energy Company	Disagree	Specific requirements for wireless devices are not necessary.
27.42	Allegheny Energy Supply	Disagree	Suggest clarifying similar to the following: Remote access should be interactive access of a BES Cyber System from a device external to the electronic and physical protection boundaries of that BES Cyber system.
27.43	Platte River Power Authority	Disagree	Suggested Revision:Remote access for the purpose of this standard means an interactive user session with a BES Cyber System Component from a device external to the BES Cyber System.That would better match the definition of external connectivity.
27.44	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS proposal to add the following to the end of the existing definition: "Automated data exchange systems would not be considered remote access".
27.45	Minnesota Power	Disagree	The current definition of "remote access," along with definition of "external connectivity," leaves open to interpretation whether Requirement R11 applies to host-based controls, or if it mandates network-based controls even within isolated or protected networks. It would appear that any interactive network access to a BES Cyber System is by definition remote access unless a portion of the network is included in the definition of that particular BES Cyber System. If the latter approach is adopted then multiple, otherwise independent, BES Cyber Systems might be arbitrarily selected to be a single BES Cyber System in order for this requirement to be met and still allow for reasonable security management.
27.46	Detroit Edison	Disagree	The definition may be interpreted to include maintenance devices. Revise as follows "Remote access for the purpose of this standard means an interactive user session with a BES Cyber System from a device external to the Electronic Boundary of the BES Cyber System."

#	Organization	Yes or No	Question 27 Comment
27.47	Ameren	Disagree	The phrase "from a device external to the BES Cyber System," is open to interpret. Please clarify if this refers to a device physically external or electrically external.â€,â€,â€,
27.48	Alberta Electric System Operator	Disagree	The word “user” should be removed from “interactive user session” because it implies human interaction and does not consider automated malware.
27.49	Progress Energy - Nuclear Generation	Disagree	This definition is not clear to me. I recommend Remote Access be defined based on NIST 800-53 Appendix B slightly modified to accommodate industrial control systems. “Access to a BES Cyber Security System by a user or process communicating from an untrusted network”
27.50	Bonneville Power Administration	Disagree	This has the same issues as the definition of "External Connectivity". In fact, the definition could simply be "an externally connected interactive user session. Recommend that the definition be reworded to use the definition of External Connectivity, along with a suitable redefinition of that term, as described in question 13. If not, recommend - "Remote Access - For the purposes of this standard, remote access is defined as an electronic connection with control capabilities to a BES Cyber System, using a data communications path that encompasses, in some or all portions, links outside the control of the Responsible Entity. "Also add a definition of wireless access that makes it clear that such access is always an example of external connectivity. The definition should exclude such protocols as Bluetooth and infrared, which are intra-system, not inter-system methods. Note that even non-interactive wireless access should be controlled.Suggestion: Wireless electronic access for the purpose of this standard means access to or from a BES Cyber System to another cyber system using wireless communications. Even if both systems and any wireless access points are under the control of the Responsible Entity, the wireless communications path itself is not. For that reason, any wireless electronic access is considered to be external connectivity."

#	Organization	Yes or No	Question 27 Comment
27.51	Kansas City Power & Light	Disagree	This is too broad and could include devices such as Remote Terminal Units.

28. Table R11 provides direction concerning what impact level of BES Cyber Systems to which Requirement R11 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R11 has moved to CIP-005-5- Cyber Security - Electronic Security Perimeters, Requirement R2.

Commenters expressed concern that for items R11.2 and R11.3, given the definitions provided in the standard, how is remote access provided without external connectivity? The SDT agrees and notes that a new requirement for Remote Access was created based on the Urgent Action Revisions to CIP-005-3.

Commenters also expressed concern that there are inconsistent definitions for "external connectivity" and "remote access". The SDT has proposed three formal definitions to provide greater clarity around external connectivity and remote access as they apply to NERC's Reliability Standards:

External Connectivity: Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.

External Routable Connectivity: The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.

Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

#	Organization	Yes or No	Question 28 Comment
28.1	WECC		Again consider replacing with requirement for remote access plan that provides specific requirements and conditions for remote access.
28.2	Florida Municipal Power Agency	Agree	For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the

#	Organization	Yes or No	Question 28 Comment
			BES Cyber System.
28.3	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
28.4	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
28.5	Bonneville Power Administration	Agree	This agreement assumes that External Connectivity is suitably redefined. Also, consider the following changes:1 - Remove Wireless from the title and the requirements.2 . If wireless is to be addressed, add a new requirement item specifically for wireless, dealing with the requirements on wireless access that are in addition to those for remote access in general.
28.6	E.ON U.S.	Disagree	: E.ON U.S. does not believe that compliance requirements are necessary for low impact systems
28.7	Southwest Power Pool Regional Entity	Disagree	“Required for external connectivity only” does not make sense. A properly configured wireless access should never directly connect within the secured network, thus any access will be “external.”
28.8	Luminant	Disagree	11.2 and 11.3 should be for Routable External Connectivity only
28.9	American Electric Power	Disagree	11.2: Regarding "If remote access is used and/or implemented, document the allowed methods for remote access", does this mean the list of approved ports and services? If not, what is meant by "allowed methods"?
28.10	US Army Corps of Engineers, Omaha Distirc	Disagree	Agree with general concept of remote access referring to an interactive session from an external location. Definition of external to BES Cyber System is poorly defined.

#	Organization	Yes or No	Question 28 Comment
			Requirement is too stringent. Breaking systems up into small groups to provide levels of control and protection appropriate to the group of components would be common good practice. This requirement would seem to restrict communication among BES Cyber Systems within a facility and make them cumbersome to manage and protect at appropriate levels. entities need more leeway in defining communication amongst systems and different levels would apply between different systems.
28.11	Southern California Edison Company	Disagree	All forms of access documentation should be required along with the level of protction and type of access granted.
28.12	Black Hills Corporation	Disagree	Applicability needs to be consistent previous non-wireless requirements.
28.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
28.14	LCEC	Disagree	Clarify what is meant by external connectivity only. Is this referring to any access to a BES cyber system component as defined earlier in the standard?
28.15	The Empire District Electric Company	Disagree	Comments: For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
28.16	Platte River Power Authority	Disagree	Disagree with the inclusion of Wireless.
28.17	Hydro One	Disagree	For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
28.18	ISO New England Inc	Disagree	For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”

#	Organization	Yes or No	Question 28 Comment
28.19	Northeast Power Coordinating Council	Disagree	For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
28.20	American Transmission Company	Disagree	For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
28.21	MRO's NERC Standards Review Subcommittee	Disagree	For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
28.22	NextEra Energy Corporate Compliance	Disagree	For Low Impact BES Cyber Systems, (1) documenting the allowed methods for remote access per 11.2, and (2) establishing and implementing a defined process for authorizing the establishment of remote access and associated remote access privileges per 11.3 should not be required. The identification of use restrictions for wireless technologies per 11.1 should be a sufficient security management control for Low Impact BES Cyber Systems. 11.2 and 11.3 will be administratively burdensome if required for practically every BES Cyber System.
28.23	San Diego Gas and Electric Co.	Disagree	Instead of defining requirements by using the impact levels, SDG&E feels it would be more appropriate to factor in the level of risk associated with the BES Cyber Systems to define the requirements for wireless and remote access.
28.24	Dairyland Power Cooperative	Disagree	Is external connectivity considered to be from outside the entity’s premises, or is it considered to be from outside the protected BES system (including for instance a corporate LAN). If it means outside the premises, then it seems deficient to not document the access-especially when later enabling of external connectivity could occur without the involvement of the supporting the BES cyber system. If it means external to the BES cyber system, then “external connectivity” and “remote access”

#	Organization	Yes or No	Question 28 Comment
			are redundantly used in 11.2 and 11.3.
28.25	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
28.26	FirstEnergy Corporation	Disagree	Need clarification on "external connectivity", because the nature of remote is external.
28.27	National Grid	Disagree	o For 11.2 and 11.3 National Grid recommends changing from “Required for external connectivity only” to “Required” since the criteria already limits the scope to “remote access” o National Grid also suggests deleting the requirement 11.3 for Low Impact BES CS.
28.28	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation ‘Required for external connectivity only’. Without understanding the defined intent suggested specific changes may be vague. Remote access is defined but not external connectivity. Is there a distinction?
28.29	American Municipal Power	Disagree	Please provide a little or no impact category
28.30	BGE	Disagree	Remove the requirement for Low on 11.1, 11.2 and 11.3
28.31	Garland Power and Light	Disagree	Requirement 11.1, 11.2, 11.3 - remove Low Impact classification from all 3
28.32	Detroit Edison	Disagree	Requirements 11.2 and 11.3 specify “Required for external connectivity only”. This is redundant. It is not possible to have remote access without external connectivity by definition.
28.33	Emerson Process Management	Disagree	Since this standard is for remote access, is the "external connectivity" potentially redundant or extra? If there is no external connectivity, how can user establish an interactive session remotely?

#	Organization	Yes or No	Question 28 Comment
28.34	MidAmerican Energy Company	Disagree	Specific requirements for wireless devices are not necessary.
28.35	ERCOT ISO	Disagree	Table 11 should address remote and wireless access across all requirements in keeping with the title of the section.
28.36	Consultant	Disagree	Table R11 - 11.1 Removing the wireless term from the requirement eliminates the need for this item. Suggest deleting this item.Item 11.3 - This is an account management requirement, and should be moved to R8, and deleted from R11.Item 11.2 - The terminology "Required for external connectivity only" is redundant in this requirement. This requirement is about allowing external connectivity via remote access. Suggest deleting "for external connectivity only"There is an inconsistency between Table R11 and Table R12. If R11 requires all impact levels to have documented controls, then R12 should require account management controls for all impact levels. To be consistent with previous account management requirements, the account management controls should be applied to medium & high impact systems, and removed from low impact systems, and Table R11 items should not be required for low impact systems. Or all impact levels should be required in both R11 & R12.
28.37	Alberta Electric System Operator	Disagree	The AESO suggests moving row 11.1 in Table R11 to a separate section governing wireless as a standalone requirement.
28.38	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS comment that “for external connectivity only” is redundant and should be removed from R11 Table 11.2 and Table 11.3 impact levels.
28.39	Reliability & Compliance Group	Disagree	the external connectivity qualifier
28.40	Minnesota Power	Disagree	The impact levels seem well defined however inconsistencies in the definitions of “remote access” and “external connectivity,” (see response in Question 26) create

#	Organization	Yes or No	Question 28 Comment
			confusion regarding the applicability of the criteria for each impact level.
28.41	US Bureau of Reclamation	Disagree	The level for Low Impact is not consistent with Electronic Access Management requirement in R8.

29. Requirement R12 of draft CIP-011-1 states "Each Responsible Entity that allows wireless and remote electronic access to any of its BES Cyber Systems shall manage that electronic access in accordance with the criteria specified in CIP-011-1 Table R12 – Wireless and Remote Electronic Access Management to ensure that no unauthorized access is allowed to its BES Cyber System." Do you agree with the list of criteria that is included in Requirements Table R12? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each item as represented in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R12 has moved to CIP-005-5 – Cyber Security - Electronic Security Perimeters, Requirement R2

Commenters suggested the need to separate wireless and remote access, and Requirement R12.1 appears to be duplicative of R8.2 and has been removed. The SDT agrees and notes a new requirement for Remote Access was created based on the Urgent Action Revisions to CIP-005-3, and the wireless access requirements have been removed.

Several commenters suggested that R8 and R12 are duplicative as both require quarterly review and verification of accounts and associated access privileges. The SDT moved all requirements for verification of accounts and associated access privileges into the revised CIP-004-5.

Other commenters suggested this requirement should have increased applicability (Low, Medium, and High rather than High only). In response, the SDT notes that the applicability for remote access requirements extends to Medium Impact BES Cyber Systems. The SDT does not feel it necessary to extend this requirement to Low Impact BES Cyber Systems. The SDT does not feel that the risk reduction for reliability justifies the administrative overhead of applying this requirement to all Low Impact BES Cyber System.

#	Organization	Yes or No	Question 29 Comment
29.1	WECC		See comments for R10/R11 consider combining this into a requirement for a Wireless Plan and Remote Access PlanThis requirement could be rolled into R8.
29.2	Southern California Edison Company	Agree	Additional clarification may be provided on criteria for control systems. It seems that a control center is temporally viewed as a distributed control system; each node (footprint restricted to one facility but electronically extends scope of control to at least one other facility) can be treated as a "control center". The drafting team should

#	Organization	Yes or No	Question 29 Comment
			develop a guideline document that presents a discussion of the local definition of a control center as a facility or system that has the ability to control more than one BES asset, side by side, with definition of the electronic boundaries of a BES system. Remote access within a facility and from beyond a particular physical facility can have different risk profiles.
29.3	Southwest Power Pool Regional Entity	Agree	Agree with the wording as presented. See comments to question 30 about applicability.
29.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
29.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Consider combining R7, R8, R11 and R12.
29.6	MRO's NERC Standards Review Subcommittee	Agree	Note impact level comments under question 30.
29.7	Progress Energy - Nuclear Generation	Agree	R12 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
29.8	BCTC	Agree	Suggest rewording from Wireless and Remote Electronic Access to Wireless or Remote Electronic Access
29.9	Bonneville Power Administration	Agree	The objective of this requirement ("to ensure that no unauthorized access is allowed to its BES Cyber System") should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that

#	Organization	Yes or No	Question 29 Comment
			the Responsible Entity must take.Our agreement with this Requirement is contingent on the redefinition as discussed in Question 27 and the definition of wireless electronic access stated above.
29.10	GTC & GSOC	Agree	We generally agree but disagree with the inclusion of the term Wireless in the requirement and associated table. Neither have anything to do with wireless as distinguished from other remote access.
29.11	Independent Electricity System Operator	Disagree	- R12 combines Wireless and Remote access. It is suggested that this be broken out in to separate requirements. Seems like an assumption that if you are connecting via wireless you are remote - not always the case.
29.12	Luminant	Disagree	12.1 should be for Routable External Connectivity only
29.13	US Bureau of Reclamation	Disagree	Access management should be established for all impact lelvels. If the requirements of R11 are going to be established, R12 needs to be established to support enforcement. Further, what is meant by quarterly review.
29.14	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
29.15	Black Hills Corporation	Disagree	Do not understand why wireless has its own table. Even if the overall requirement is a little more difficult, consistency of approach will result in greater security.
29.16	Entergy	Disagree	Entergy agrees with the list of criteria, but believes it should apply equally to high, medium and low assets.We also suggest eliminating R12 and combine it with R8.2 (quarterly review and verification of accounts and associated access privileges), as these are part and parcel of account rights management.
29.17	Hydro One	Disagree	For consistency with 12.1, recommend removing “wireless” from R12.Recommend changing Requirement 12.1 from “quarterly review” to “annual review”. There are no additional benefits to the shorter review period.Similarly to our previous comment

#	Organization	Yes or No	Question 29 Comment
			to R11, we don't understand why the wireless communication is getting special attention. We believe that the protection should remain the same regardless of the type of access point (i.e. if it is wired, Wi-Fi, ZigBee etc.). Please explain the rational behind the decision.
29.18	ISO New England Inc	Disagree	For consistency with 12.1, recommend removing "wireless" from R12R12 combines Wireless and Remote access. It is suggested that this be broken out in to separate requirements. Seems like an assumption that if you are connecting via wireless you are remote - not always the case.
29.19	Northeast Power Coordinating Council	Disagree	For consistency with 12.1, recommend removing "wireless" from R12.Recommend changing Requirement 12.1 from "quarterly review" to "annual review". There are no additional benefits to the shorter review period.
29.20	Duke Energy	Disagree	For generation stations in particular, external connectivity (R3) and remote connectivity (R11) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome. Table 12 o redundant with Table 11 and Table 8. Suggest including this review as part of the review conducted in 8.2. o suggest removing 'and verification.' We don't understand the benefit to this and question if it is possible for remote access.
29.21	Constellation Power Source Generation	Disagree	In general, Constellation believes that wireless controls should be combined with network controls, as the same controls will be applied.
29.22	Southwestern Power Administration	Disagree	Is a separate requirement for wireless access really necessary when a requirement already exists for protecting access to a BES Cyber System by any means of entry? If so, then suggest separating wireless from remote access.

#	Organization	Yes or No	Question 29 Comment
29.23	Northeast Utilities	Disagree	It is our belief that the review of access privileges conducted under Requirement 8 would satisfy the intent of this requirement as well and that R12 should be eliminated.Hence, this requirement is not needed as long as it is clear that remote access will not be granted unless explicit specific rights are granted to some asset they connect with. Access should not be given access to a protected area unless there is a need to access a specific asset, i.e., there is no business need to just grant network only access.
29.24	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with SPP's observation below:We question the need for a specific requirement for wireless devices. We understand there have been inquiries about treatment of wireless devices. But a wireless access point has the same impact on a BES Cyber System as any other access point. A requirement to protect access to a Cyber System already includes any possible means of entry. The use of a wireless device to access a BES Cyber System can be determined with an audit of access logs and a further audit of control of that access would reveal whether appropriate protections were in place. There is not a need for a separate distinct requirement subject to records retention and audit for specific wireless devices. NERC must realize that the more requirements that are added, the more questions/interpretations of words that can result from the requirement. Registered entities become more subject to violations not because they have neglected to protect their BES Cyber Systems, but rather because of differences in understanding of the words of a requirement - all the while the intent of the requirement had never really been “violated”.
29.25	NextEra Energy Corporate Compliance	Disagree	NextEra believes that if remote access is used and/or implemented, document and implement a quarterly review and verification of the personnel with remote access and their associated access privileges, it is unclear how this access is supposed to be verified and what is accepted as part of the verification process. This is the same as the comments to address question #20 of this questionnaire. If remote access is used and/or implemented, documenting and implementing a quarterly review and verification of the personnel with remote access and their associated access privileges

#	Organization	Yes or No	Question 29 Comment
			may not be sufficient. This process needs to be tied in with personnel (1) gaining authorized remote access to a BES Cyber System, (2) modifying their access privileges to a BES Cyber System due to change of the user's access rights due to change in role or responsibility and, (3) loosing authorized remote access to a BES Cyber System due to a revocation of electronic access to a BES Cyber System.
29.26	National Grid	Disagree	o National Grid recommends an annual review for verification since quarterly review does not have much benefit. o National Grid recommends changing from “Required for external connectivity only” to “Required” under High Impact BES CS since the criteria already limits the scope to “remote access”
29.27	Progress Energy (non-Nuclear)	Disagree	Quarterly seems to be too frequent - propose 6 months or longer. We are required in R9 to revoke access for those that are terminated or do not need access within 72 hours.
29.28	LCEC	Disagree	R12 - 12.1 is covered in the account review requirements in R8. This should be changed to review the need for wireless as opposed to wired connectivity and reviewed annually.
29.29	Consultant	Disagree	R12 is an account management requirement. The requirement should be moved to R8 as an aspect of account management.There is no difference in "remote access" and "wireless electronic access" as remote access is defined in the standard. Suggest deleting reference to wireless electronic access in requirement. But if you must have wireless addressed, include it in the definition of remote access.R12. This phrasing is awkward - "to ensure that no unauthorized access is allowed to its BES Cyber Systems" Suggest using wording comparable to R8 "to maintain control of access to its BES Cyber Systems."
29.30	CWLP Electric Transmission, Distribution and	Disagree	R12. Due to the requirements access revocation in R9 this requirement should be extended to an annual review.

#	Organization	Yes or No	Question 29 Comment
	Operations Department		
29.31	Southern Company	Disagree	R12.1 addresses remote access only and does not include wireless, the table title and R12 includes wireless.
29.32	Allegheny Energy Supply	Disagree	Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.33	Allegheny Power	Disagree	Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.34	EEI	Disagree	Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.35	PNM Resources, Inc.	Disagree	Requirements for disabling access or user accounts in periods that are less than 6 hours are unrealistic, especially on weekends or during off-hours.
29.36	San Diego Gas and Electric Co.	Disagree	SDG&E recommends that the wireless and remote electronic access management apply to devices external to the BES Cyber System's network.
29.37	Manitoba Hydro	Disagree	Since Requirement R12 refers to external access, the words “for external connectivity only” are unnecessary in the impact columns and should be removed. Consider adding a requirement for securing the wireless access point.
29.38	ERCOT ISO	Disagree	Table 12 should address remote and wireless access across all requirements. 12.1: Should be combined with other access management requirements (physical, cyber, information).
29.39	BGE	Disagree	Tables 11 and 12 are out of synch.
29.40	Kansas City Power & Light	Disagree	The scope of “wireless” is not clear and can result in interpretation issues throughout these requirements.
29.41	FirstEnergy Corporation	Disagree	The Table is titled “Wireless and Remote ...”For consistency we suggest that 12.1 be

#	Organization	Yes or No	Question 29 Comment
			revised to state "... personnel with wireless and remote access ..."
29.42	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
29.43	We Energies	Disagree	We Energies agrees with EEI: Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.44	Alberta Electric System Operator	Disagree	Wireless access and remote access should be two separate concepts.
29.45	Detroit Edison	Disagree	Wireless electronic access is not an access method; it is just the medium to obtain access. In an effort to remove reference to specific technology, wireless should not be identified anywhere in the standard. References to specific technologies should be addressed in the guidance documentation.R11, R12 and R14 use term "remote electronic access" and R13 uses the term "remote access". Revise to maintain consistency.Requirement 12.1 specifies "Required for external connectivity only". This is redundant. It is not possible to have remote access without external connectivity by definition.

30. Table R12 provides direction concerning what impact level of BES Cyber Systems to which Requirement R12 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R12 has moved to CIP-005-5 – Cyber Security - Electronic Security Perimiters, Requirement R2.

Commenters suggested a reword of this item to remove "for external connectivity only", since remote access cannot be granted without external connectivity. The SDT agrees and has made this change.

Other commenters suggested this requirement should have increased applicability (Low, Medium, and High rather than High only). In response, the SDT notes that the applicability for remote access requirements extends to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems. The SDT does not feel it necessary to extend this requirement to Low Impact BES Cyber Systems. The SDT does not feel that the risk reduction for reliability justifies the administrative overhead of applying this requirement to all Low Impact BES Cyber System.

Several commenters suggested that R9 and R12 are duplicative. The SDT moved all requirements for revocation of access privileges into the revised CIP-004-5.

#	Organization	Yes or No	Question 30 Comment
30.1	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Consider combining R7, R8, R11 and R12. At minimum, R12 should be consistent with R8.
30.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
30.3	Progress Energy (non-Nuclear)	Agree	See Comment 14.Not needed. There already is another requirement for cyber access reviews.
30.4	Northeast Utilities	Agree	Suggest eliminating R12 - see response to Question 29.

#	Organization	Yes or No	Question 30 Comment
30.5	Independent Electricity System Operator	Disagree	- For R12.1 is Required for external connectivity only. If you connect remotely, how is this not external connectivity to the BES Cyber system - shouldn't these entries just be "required"
30.6	ERCOT ISO	Disagree	12.1: Should apply to Medium Impact BES Cyber System.
30.7	Southern California Edison Company	Disagree	All forms of access documentation should be required along with the level of protection and type of access granted. Wireless technology needs full security and encryption in regards to any level of BES Cyber System.
30.8	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
30.9	USACE HQ	Disagree	At a minimum, 12.1 should be required for all impact levels. Requirement 11 creates a document of remote access procedure and who has the right to use it, but for low and medium impact systems it is not required to update the same as per requirement 12.1.
30.10	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
30.11	Tenaska	Disagree	Combine 12 and 13
30.12	The Empire District Electric Company	Disagree	Comments: For item 12.1, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
30.13	Alberta Electric System Operator	Disagree	Create additional requirements in Table R12 for Medium and Low impact levels. Suggest semi-annual review for Medium Impact, and Annual review for Low impact.
30.14	Black Hills Corporation	Disagree	Do not understand why wireless has its own table. Even if the overall requirement is

#	Organization	Yes or No	Question 30 Comment
			a little more difficult, consistency of approach will result in greater security.
30.15	Entergy	Disagree	Entergy agrees with the list of criteria, but believes it should apply equally to high, medium and low assets.
30.16	Duke Energy	Disagree	For generation stations in particular, external connectivity (R3) and remote connectivity (R11) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station).
30.17	American Transmission Company	Disagree	For item 12.1, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
30.18	MRO's NERC Standards Review Subcommittee	Disagree	For item 12.1, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
30.19	Consultant	Disagree	Item 12.1 - The terminology "Required for external connectivity only" is redundant in this requirement. This requirement is about allowing external connectivity via remote access. Suggest deleting "for external connectivity only"There is an inconsistency between Table R11 and Table R12. If R11 requires all impact levels to have documented controls, then R12 should require account management controls for all impact levels. To be consistent with previous account management requirements, the account management controls should be applied to medium & high impact systems, and removed from low impact systems, and Table R11 items should not be required for low impact systems. Or all impact levels should be required in both R11 & R12.

#	Organization	Yes or No	Question 30 Comment
30.20	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
30.21	WECC	Disagree	Medium Impact should still have the requirement as well.This should apply to all impact levels.
30.22	National Grid	Disagree	National Grid recommends changing from “Required for external connectivity only” to “Required” under High Impact BES CS since the criteria already limits the scope to “remote access”.
30.23	FirstEnergy Corporation	Disagree	Need clarification on "external connectivity", because the nature of remote is external.
30.24	NextEra Energy Corporate Compliance	Disagree	NextEra believes that regarding 12.1, why make the distinction for "for external connectivity only" rather than just stating that it is "required"? When remote access is used and/or implemented, does it imply "external" connectivity based on the local definition?
30.25	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation ‘Required for external connectivity only’.
30.26	American Municipal Power	Disagree	Please provide a little or no impact category
30.27	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12. Specifically, if 11.2 and 11.3 require documenting allowed methods and processes for remote access, then table 12 should require quarterly review of the access granted via 11.2 and 11.3. Puget Sound Energy suggests including wording similar to Table 11: “Required for external connectivity only”.

#	Organization	Yes or No	Question 30 Comment
30.28	LCEC	Disagree	R12 - 12.1 is covered in the account review requirements in R8. This should be changed to review the need for wireless as opposed to wired connectivity and reviewed annually.
30.29	Hydro One	Disagree	Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.Recommend that Medium Impact BES Cyber System should be Required.
30.30	Northeast Power Coordinating Council	Disagree	Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.Recommend that Medium Impact BES Cyber System should be Required.
30.31	Southwest Power Pool Regional Entity	Disagree	Remote access should be periodically reviewed for all impact categories. Ideally, a more frequent review should be required for High impact systems.
30.32	Allegheny Energy Supply	Disagree	Requirement R12 appears to be duplicative of R8.2 and should be removed.
30.33	Allegheny Power	Disagree	Requirement R12 appears to be duplicative of R8.2 and should be removed.
30.34	EEI	Disagree	Requirement R12 appears to be duplicative of R8.2 and should be removed.
30.35	ISO New England Inc	Disagree	Should be across the board, and annually for allRecommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”
30.36	MidAmerican Energy Company	Disagree	Specific requirements for wireless devices are not necessary. Furthermore, requirement R12.1 is duplicative of R8.2.
30.37	ReliabilityFirst Staff	Disagree	Suggest “Required for external connectivity only” for Medium Impact in row 12.1.
30.38	Network & Security	Disagree	Suggest including Medium Impact systems with external connectivity.

#	Organization	Yes or No	Question 30 Comment
	Technologies Inc		
30.39	US Bureau of Reclamation	Disagree	Table R12 should be applied to all Impact levels in keeping with requirements established in R11.
30.40	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS that "for external connectivity only" is redundant and should be removed from R12 Table 12.1. The table should therefore read:R12 Table 12.1: Low Impact: N/AMedium Impact: N/AHigh Impact: Required
30.41	Minnesota Power	Disagree	The impact levels seem well defined however inconsistencies in the definitions of "remote access" and "external connectivity," (see response in Question 26) create confusion regarding the applicability of the criteria for each impact level.
30.42	PacifiCorp	Disagree	The term verification needs further definition. Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
30.43	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
30.44	We Energies	Disagree	We Energies agrees with EEI: Requirement R12 appears to be duplicative of R8.2 and should be removed.

31. Requirement R13 of draft CIP-011-1 states "Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 – Remote Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that is included in Requirements Table R13? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R13 has moved to CIP-004-5 – Cyber Security - Personnel and Training, Requirement R7.

Commenters suggested making the timeframes for revocation in R13 the same as R9. In response, the timeframes for revocation requirements have been simplified as follows:

- Revocation of access to BES Cyber Systems at the time of the termination or resignation and by by the end of the next calendar day for reassignments or transfers action,
- Revocation of access to BES Cyber System Information by by the end of the next calendar day for terminations or reassignments, and
- Additional requirements were added to address revocation of user accounts on BES Cyber Systems and shared accounts.

Commenters expressed concerns that persons who transfer are not automatically considered a threat to the system, and the timeframes for revocation should reflect this. In response, the requirement for transfers now states a review of access is required on the transfer date, and any unneeded access is revoked when it is no longer needed.

Commenters suggested keeping the revocation timeframes the same as defined in CIP Version 3. The SDT notes that FERC Order 706 directs revocation of access to occur immediately in all cases where access is no longer needed. The requirement has been modified to simply revoke access when a person no longer needs it. Organizations usually have termination procedures to return company property and perform exit interviews. Processes for revoking access (both physical and remote electronic) can be incorporated into an organization's termination and transfer procedures.

#	Organization	Yes or No	Question 31 Comment
31.1	WECC	Agree	Agree with criteria but recommend combining with R9 Revoking Access.This could be rolled into R9

#	Organization	Yes or No	Question 31 Comment
31.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
31.3	Florida Municipal Power Agency	Agree	Consider combining R9 with R13 and making the timing consistent. In 13.1, 13.2 and 13.3, "when job duties no longer require ..." is ambiguous and should be tied back to the policy of R1.
31.4	Progress Energy - Nuclear Generation	Agree	R13 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
31.5	Minnesota Power	Agree	These criteria are generally acceptable, except for the statement that "Each Registered Entity shall revoke remote access by disabling one or more of the multiple factors required..." The requirement to implement multi-factor authentication is not included in CIP-011-1.
31.6	Independent Electricity System Operator	Disagree	- There is no requirement for removing external access for cause. Does R9.1 cover this access? Should for cause be changed to involuntarily terminated to include those that are terminated unwillingly due to layoffs, job cuts, fired/performance, etc.- R1
31.7	PacifiCorp	Disagree	: The list of criteria is inconsistent with BES system access as outlined in Table 9. Remote access to BES should follow the same revocation criteria as system access.
31.8	USACE - Omaha Anchor	Disagree	13.1 - '... when job duties no longer require remote access' should either be changed 'when terminated for cause' or if the verbiage is deemed appropriate then the length of time to change the password needs to be greatly expanded. Just because an employee changes jobs does not mean they are a threat to the system, they still have the appropriate clearances and training.13.2 & 13.3 - since we are talking about a current employee who is just changing jobs the high impact numbers are crazy. The person is not a threat to the system, they have the necessary background.

#	Organization	Yes or No	Question 31 Comment
			Recommend times be the same as medium impact system.
31.9	Xcel Energy	Disagree	A 1 hour revocation time in R13.1 is completely unworkable. Examples where this is impossible include a termination by a vendor or joint access partner, or a termination during evening hours or weekends/holidays, when IT staff needed to terminate the access can not respond within 1 hour. The 4 and 6 hour revocation times for job duty changes are unjustified and unneeded. When the change is for a business reason such as a job change 7 days is sufficient for access removal. When the access change is unrelated to a termination for cause, the individual's trustworthiness and reliability are not in question and the short timeframes are not warranted.
31.10	BCTC	Disagree	Â Suggest collapsing Requirements 13.1 to 13.3 into one.Â Time targets would be the same as those suggested in Requirement 9 above
31.11	Alberta Electric System Operator	Disagree	Are the "multiple factors" referenced in R13 defined?
31.12	Tenaska	Disagree	Combine 12 and 13
31.13	BGE	Disagree	Combine 13.1, 13.2 and 13.3 into one requirement. Revocation for high impacted systems should be 24 hours to maintain consistency with other requirements with CIP-011.
31.14	Entergy	Disagree	Consider eliminating R13 altogether or combining it with R8.4 and R8.5.Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance perspective to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
31.15	E.ON U.S.	Disagree	E.ON U.S. believes that the proposed time requirements are not reasonable and require 24x7 support personnel with the privilege to revoke access. Revocation of remote access within one hour for Control Centers is unreasonable for high-impact

#	Organization	Yes or No	Question 31 Comment
			Systems when the revocation is unrelated to termination with cause. If revocation is the result of one's job duties no longer requiring access, then E ON U.S. suggests next-business day should be adequate. Likewise, six hours for Transmission substation systems, and four hours for Generation Systems is unreasonable. Next business-day revocation should be adequate for all of these situations and presents little, if any, additional risk. E.ON U.S. requests clarification as to what is included in the term "multiple factors" for remote access.
31.16	EEI	Disagree	EEI suggests the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems."
31.17	Constellation Energy Control and Dispatch, LLC	Disagree	-Eliminate the timing differences for revoking access when no longer required that exists between Control Centers, generation or transmission facilities and use a single timing requirment for access to all BES cyber systems.-The previous requirements have
31.18	FirstEnergy Corporation	Disagree	For 13.1, 13.2, 13.3 - Change text to '...when job responsibilities no longer requires BES Cyber System remote access'.This table should include a consideration when termination for cause. Should parallel Table 9 expectations.The recommended times are unreasonable for transfers/job reassignments.We have the same concerns with inconsistent application in regards to Impact Level as we previously identified in Table 9. See our comments to Questions 22 and 23.
31.19	Exelon Corporation	Disagree	Implementing revocation of access in as short a time as those proposed would require major changes to many enterprise wide systems in order to document compliance. Why do these time periods differ from those for physical and electronic access? Exelon feels these requirements are too restrictive and might necessitate moving to a 24/7 position to monitor the need for access revocation. Exelon's position is that the

#	Organization	Yes or No	Question 31 Comment
			access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
31.20	USACE HQ	Disagree	It does not make sense to create three (3) separate requirements for three specific environments only, I suggest to have only one requirement that reads “Revoke remote access when job duties no longer require BES Cyber System remote access”.
31.21	APPA Task Force	Disagree	New: R13 Table 13.1: For personnel terminated for cause on a preplanned basis. Low Impact: N/AMedium Impact: 8 hourHigh Impact: 8 hourThe Existing 13.1 - 13.3 will need to be renumbered if this new 13.1 is accepted.
31.22	National Grid	Disagree	o National Grid recommends changing from “Required for external connectivity only” to “Required” under High Impact BES CS since the criteria already limits the scope to “remote access” o Reword “remote access” as “Remote access (LAN and wireless) communication interface o 24 hours is the minimal practical time for revoking access. A 1 or 4 hour revocation of access is not reasonable. National Grid suggests keeping times same as in Table R9.
31.23	NextEra Energy Corporate Compliance	Disagree	Please refer to comments submitted for questions 22 and 23. Furthermore, NextEra believes the timeframes suggested will be burdensome to administer since personnel that have authorized remote access have by definition also authorized electronic access. With this current draft, it connotes that when revoking access to High Impact Control Center BES Cyber Systems when job duties no longer require BES Cyber System remote access; the Responsible Entity has 1 hour to revoke remote access per 13.1 and has 36 hours to revoke electronic access per 9.2. We suggest making the time requirements consistent and up date the timeframe to "as soon a practical but within 36 hours" for both 13.1 and 9.2
31.24	Dominion Resources	Disagree	Please see Dominion’s response to Questions 15 and 22. Dominion also requests that

#	Organization	Yes or No	Question 31 Comment
	Services, Inc.		the removal of authentication needed for remote access suffice to meet the intention of this requirement for "immediate" revocation.
31.25	American Electric Power	Disagree	Please see response to Question 32 for additional detail.
31.26	Puget Sound Energy	Disagree	Puget Sound Energy disagrees with the current wording of the criteria. "...when job duties no longer require BES Cyber System remote access" is an abstract concept that will be impossible to quantify in order to validate compliance with the requirement. Puget Sound Energy suggests rewording to "Revoke remote access to...BES Cyber Systems when notification by personnel that job duties no longer require BES Cyber System remote access. In light of the 4 hr to 72 hr clock to revoke access, Puget Sound Energy suggests some measurable trigger from which to start the countdown to required revocation timeframes.
31.27	Detroit Edison	Disagree	R11, R12 and R14 use term "remote electronic access" and R13 uses the term "remote access". Revise to maintain consistency.
31.28	LCEC	Disagree	R13 requirements should be moved to the account management section.
31.29	Southwest Power Pool Regional Entity	Disagree	R13: The objective states that access will be revoked by disabling one or more of the multiple factors required for such access, yet multiple factor access authentication has yet to be prescribed. 13.1, 13.2, and 13.3 simply states "revoke access." As stated, the requirement is unclear and inconsistent between the object statement (Requirement) and the criteria. It may be beneficial to swap Requirements 13 and 14, prescribing remote access authentication controls before prescribing revocation of such access.
31.30	Hydro One	Disagree	Recommend using the same thresholds as R9.Recommend changing from "Required for external connectivity only" to "Required" since the criteria already limit the scope to "remote access".Recommend moving this Requirement to the Boundary Protection Requirements.

#	Organization	Yes or No	Question 31 Comment
31.31	Northeast Power Coordinating Council	Disagree	Recommend using the same thresholds as R9.Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.Recommend moving this Requirement to the Boundary Protection Requirements.
31.32	ISO New England Inc	Disagree	Recommend using the same thresholds as R9Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”Recommend moving this Requirement to the Boundary Protection RequirementsR13.1, R13.2 and R13.3 Is the 36 hours or 72 hours from the time the access is reviewed? Or is it that access should be reviewed within 36 hours of personnel that change job responsibilities, transfer, etc. Then require access be modified based on the review. Suggest changing the 36 hours to 72 hours. If a transfer were to occur on a Friday at 5 pm then access would need to be reviewed by Sunday. R13.1, R13.2 and R13.3 suggest changing the requirement to “Review access to BES Cyber Systems for personnel that change job responsibilities as a result of reassignment, transferred to other positions within x hours of the change.”
31.33	Black Hills Corporation	Disagree	Remote access revocation should be no different that other types of access and the 24 hour should apply.
31.34	Regulatory Compliance	Disagree	Remove R13 altogether and treat revocation of remote access the same as system access.
31.35	Garland Power and Light	Disagree	Requirement 13.1 - Medium Impact should read 48 hours instead of 36 hours and High Impact should read 4 hours instead of 1 hour. To be as strict as written is not necessary for just a job duty change
31.36	Reliability & Compliance Group	Disagree	Revocation for employees terminated for cause needs to be included.

#	Organization	Yes or No	Question 31 Comment
31.37	Southern California Edison Company	Disagree	SCE recommends matching R13 with R9. The time limits for high-impact generation BES is less than transmission substation BES, whereas they are the same in R9. SCE also suggest that 13.2 and 13.3 be given the same time limit.Also, SCE requests clarification about the types of devices that must be revoked. Order 706 seeks immediate revocation to devices and facilities. While order 706 has been unequivocal in the requirement of this control, they do not specify that access to “each” device must be individually revoked. The drafting team should be asked to provide supplemental guidance with this requirement to state that immediate revocation in timeframes shorter than 24 hours to “boundaries” electronic and physical be instituted.
31.38	SCE&G	Disagree	SDT needs to account for transitional periods when incumbent needs to train a replacement for job tasks. In this case when would time period begin for "no longer requiring access". There would be no timestamped document to start the clock.
31.39	ERCOT ISO	Disagree	Should be combined with other access management requirements (physical, cyber, information).
31.40	Manitoba Hydro	Disagree	Since Requirement R13 refers to external access, the words “for external connectivity only” are unnecessary in the impact columns. Please clarify if the “one or more of the multiple factors required for such remote access...” refers to the electronic access controls in Requirement R14. Please clarify what “such access” means.
31.41	Alliant Energy	Disagree	Specifically 1 hour system access removal is not even possible in an environment that is largely automated and unreasonably creates an environment of non-compliance. More generally, Table 13 is another occurrence where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the

#	Organization	Yes or No	Question 31 Comment
			business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
31.42	Allegheny Energy Supply	Disagree	Suggest the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems."
31.43	Allegheny Power	Disagree	Suggest the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems."
31.44	Duke Energy	Disagree	Table 13: How will this apply in case of a death?13.1 change 36 hours to 48 hours
31.45	MidAmerican Energy Company	Disagree	The list of criteria is inconsistent with BES system access as outlined in Table 9. Remote access to BES should follow the same revocation criteria as system access.
31.46	Ameren	Disagree	The short period of time to remove access does not extend well across weekends or through the 2nd business day in cases where access is no longer required at the end of the day. Suggest that these requirements be extended to a week to remain in line with current CIP standards. This will allow for proper hand off time in cases where job duties need to be transferred.
31.47	Southern Company	Disagree	The time limits in 13.1 are needlessly short in the context of an employee who is not

#	Organization	Yes or No	Question 31 Comment
			being dismissed for cause but is simply having his job duties changed. In addition, it is not clear exactly what the trigger point is for the start of that time table.
31.48	Northeast Utilities	Disagree	The timeframe is extreme for routine personnel changes (1 - 6 hours). Suggest a "for cause" termination for these timeframes and make routine more reasonable (3 days to align with R9?) Also, it is not needed if you agree with comment to 29. Host/application and network access should be treated the same.
31.49	Dairyland Power Cooperative	Disagree	These rules seem redundant to table R9. Why are there redundant rules for remote access accounts vs regular accounts? Any rules here should be for something that is unique to remote access.
31.50	US Bureau of Reclamation	Disagree	This requirement appears to be in conflict with R9. In reading R9 it is not clear that it does not also include remote access. Just as in R11 remote needs to be defined especially since R9 does not indicate remote access is excluded as this standards implies. Further, requirements need to be established for all system impact levels and timeframes need to be realistic and achievable. Shorter timeframes, as established in the table, would appear to be more applicable to individuals terminated for cause.
31.51	Consultant	Disagree	This requirement is access revocation and should be included in R9 as it relates to account management and access revocation.13.1, 13.2, & 13.3 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.13.1, 13.2, & 13.3 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.Suggest deleting "for external connectivity only" as redundant & unnecessary. This requirement is for remote access and is by definition external access.

#	Organization	Yes or No	Question 31 Comment
31.52	Bonneville Power Administration	Disagree	This requirement is not necessary. It is already covered under R9. Revocation of electronic access applies to all electronic access regardless of whether it is local, remote or wireless. There is no difference.If the Requirement is retained, then the objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.
31.53	Progress Energy (non-Nuclear)	Disagree	This revocation is not based on termination for cause. It will be very difficult to meet the 1 - 6 hour revocations. If termination was for cause would an individual not need physical access to get remote access - we are required to physically secure areas around remote access? Shouldn't all access, system, physical, remove etc. have consistent revocation times?Revocation of access within a 'hours' timeframe implies that the access would be controlled through a security group with 24/7 coverage.This should be no different than the revocation of cyber access. This requirement is not needed. Also the time limits as proposed for High Impact are impractical and will only lead to unnecessary self-reports that provide no benefit to system security.CIP-011 R13.1 thru .3 What is the decision process to be used to determine "when job duties no longer require ... access"? What would be suitable compliance evidence that is to be collected that indicates "when job duties no longer require access" as this is critical in determining if revocation has been accomplished within the mandated 1 hour, 4 hours, 6 hours, 24 hours, 36 hours, 72 hours?The complexity and compliance risk of managing all of these requirements at different levels, for different functional areas will be very problematic to substantiate compliance.
31.54	CWLP Electric Transmission, Distribution and	Disagree	Time frames should be extended to 72 hours or next business day, whichever is longer.

#	Organization	Yes or No	Question 31 Comment
	Operations Department		
31.55	Con Edison of New York	Disagree	Timeliness of access removal is important. These criteria can be interpreted (R13.1 for example) to mean remote access needs to be revoked within 7 hours of the actual time of change of job duties. This can be unrealistic. The controlling department, for access, may not be notified by the individuals department of the change within the time period. This is more likely when contract personnel are considered. The requirement should be clearly worded to provide 7 hours from notification of the need for change.R13.2 and 13.3: it is not clear that the standard defines either a Transmission or Generation BES Cyber System.
31.56	We Energies	Disagree	We Energies agrees with EEI: Suggest the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems." We Energies agrees with EEI: Suggest adding requirements to address the removal of remote access for low impact systems.
31.57	GTC & GSOC	Disagree	We recommend this requirement include language that would allow personnel to retain access during a transition period while training their replacement. We recommend the language used in requirement 5, row 5.8: "personnel who no longer require such access."We also recommend that termination for cause should be handled seperately. All other time lines should be commensurate with the associated risk and consistent throughout all requirements.We recommend the language in Table 13 should be consistent with 5.8 and 5.9 in Table 5.We recommend requirements 13.1, 13.2, 13.3 should include the words "the entity determines the" between the words "when" and "job"; this would prevent an auditor from second guessing an entity's decision on required access. The requirement should also specifically state that this does not preclude a person from retaining access in order to assist his replacement with fulfilling his old job duties during a transition of

#	Organization	Yes or No	Question 31 Comment
			responsibilities.
31.58	Network & Security Technologies Inc	Disagree	Wording suggests multi-factor authentication is required for all systems subject of R13, but R14 only requires multiple factors for High Impact systems. Also suggest swapping order of requirements in R13 and R14.

32. Table R13 provides direction concerning what impact level of BES Cyber Systems to which Requirement R13 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R13 has moved to CIP-004-5 – Cyber Security - Personnel and Training, Requirement R5.

Commenters suggested aligning with R9 normal revocations. In response, the requirements for revocation have been consolidated to CIP-004-5 R7.

Commenters suggested including targets for Low Impact BES Cyber System revocation. The SDT notes the applicability to Low Impact BES Cyber Systems has been removed.

Commenters suggested times need to be stated in business days. In response, times have been changed to calendar days. The use of business days is not appropriate because this can be interpreted to include exclusions for weekends and holidays.

#	Organization	Yes or No	Question 32 Comment
32.1	Luminant	Agree	13.1 should be changed to 48 hours (2 days)
32.2	USACE - Omaha Anchor	Agree	Agree - just want to reiterate the times associated with removal for a job transfer are ridiculous. The person has been trusted and trained - it's not an emergency just because they changed jobs. (Due to lack of personnel - if this happened on a Friday - we would have to treat it as an emergency.)
32.3	Idaho Power Company	Agree	Need to make this consistent with revocation requirements for normal electronic access. Why would these timelines be shorter?
32.4	SCE&G	Agree	The timeframes, specifically for High Impact Control Center assets, are extreme.
32.5	US Army Corps of Engineers, Omaha Distirc	Disagree	"when job duties no longer require" will be very hard to account for. Time frames are unrealistic / impossible. Times should be stated in terms of business days. It would be more realistic for High Impact BES Cyber Systems to be Next Business Day and for Medium Impact Cyber Systems to be 2 and 3 business days.

#	Organization	Yes or No	Question 32 Comment
32.6	Florida Municipal Power Agency	Disagree	1 hour is not reasonable. Planned termination for cause can be 1 hour, but, otherwise the 1 hour is not reasonable. Consider aligning the times with R5 and R9. Access revocation alternatives/mitigation techniques should allow for deviation from the standard, or be recognized. For example, escorted supervision while restricting access to communication devices/computers should be a reasonable way to get around the 1-hour requirement if it can't be met for some particular reason.
32.7	American Electric Power	Disagree	13.1 - 13.3, regarding all information in column "High Impact BES Cyber System". These values are not feasible on a system unless it is managed with a domain controller or has only a few network components. Suggest using the 36/72/72 as required in the R9. There is no need to make this more restricted than the local access.There also does not appear to be a requirement to revoke access within 24 hours for a termination for cause. Is that the intent?
32.8	Con Edison of New York	Disagree	13.1,2,3- may be dependent on a company's existing HR/Payroll business system capabilities and introduce significant costs to remediate. Even though the individuals were trusted and the trust did not change as a result of cause. A week may be more realistic
32.9	ERCOT ISO	Disagree	13.1: 1 hour may not be possible. Especially in light of access granted to external organizations (ie: an RC or BA with access a TOP's systems).
32.10	Southern California Edison Company	Disagree	A longer time frame (range of <72 hours for high medium and low impact systems) should be instituted for each device. Revocation should not be treated as a monolithic requirement and should be such that it leverages controls instituted by boundary protections.
32.11	Constellation Energy Commodities Group Inc.	Disagree	Align all high and medium impact systems on the 72 hour standard to eliminate confusion and allow consistent administration.

#	Organization	Yes or No	Question 32 Comment
32.12	MidAmerican Energy Company	Disagree	As noted in question 31 we believe that the list of criteria should align with Table 9, the impact levels should begin with termination for cause and then address the criteria. In addition, the impact between transmission and generation is inconsistent and not understood why these would be different, again inconsistent with Table 9. With regards to the impact levels - time to revoke access - we disagree that this too would be different than as outlined in Table 9. All revocation requirements under 24 hours is concerning as this imposes significant risk to our ability to comply given the lack of available automated access removal solutions in the market place that can be realistically deployed across a wide-range of systems.
32.13	PacifiCorp	Disagree	As noted in question 31 we believe that the list of criteria should align with Table 9, the impact levels should begin with termination for cause and then address the criteria. In addition, the impact between transmission and generation is inconsistent and it is not understood clear why these would be different, again inconsistent with Table 9. With regards to the impact levels - time to revoke access - we disagree that this too would be different than as outlined in Table 9. All revocation requirements under 24 hours is concerning as this imposes significant risk difficulty to our ability to comply given the lack of available automated access removal solutions in the market place that can be realistically deployed across a wide-range of systems.
32.14	American Transmission Company	Disagree	As written, we believe the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access), but would be in agreement with terminology urging entities to expedite this process as much as possible with regards to remote access.
32.15	MRO's NERC Standards Review Subcommittee	Disagree	As written, we believe the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-

#	Organization	Yes or No	Question 32 Comment
			compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access), but would be in agreement with terminology urging entities to expedite this process as much as possible with regards to remote access.
32.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
32.17	Tenaska	Disagree	Combine 14 and 11
32.18	The Empire District Electric Company	Disagree	Comments: As written, we believe the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access), but would be in agreement with terminology urging entities to expedite this process as much as possible with regards to remote access.
32.19	Alberta Electric System Operator	Disagree	Consider adding “120 hours for external connectivity only” to all Low Impact BES Cyber System levels (13.1, 13.2, 13.3).
32.20	Entergy	Disagree	Consider eliminating R13 altogether or combining it with R8.4 and R8.5.Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance perspective to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
32.21	Duke Energy	Disagree	Drafting team, please explain the basis for the 1 hour, 6 hour, and 4 hour requirements for the High Impact column. These appear to be overly restrictive and arbitrary. Similar to the comment above, these items are much more achievable if "remote" and "external" are defined as external to the plant in a generation

#	Organization	Yes or No	Question 32 Comment
			environment. Also, as stated above (question 27), remote connectivity requires more unambiguous definition.
32.22	E.ON U.S.	Disagree	E.ON U.S. believes that the proposed time requirements are not reasonable and require 24x7 support personnel with the privilege to revoke access
32.23	USACE HQ	Disagree	First, requirements 13.1, 13.2, and 13.3 should be required for every level of impact. Second, to avoid the "Friday 5PM no longer required access" scenario, the language should be change as follow: for High Impact BES Cyber System in 13.1, 13.2, and 13.3, from "XX hours for external connectivity only" to "Close of Business Day (COB) of the following day after the no longer access required for external connectivity only", for Medium Impact BES Cyber System in 13.1, 13.2, and 13.3, from "XX hours for external connectivity only" to "Close of Business Day (COB) of the second day after the no longer access required for external connectivity only", and for Low Impact BES Cyber System in 13.1, 13.2, and 13.3 (please refered to my answer to question 31), from "----" to "Close of Business Day (COB) of the third day after the no longer access required for external connectivity only".
32.24	Network & Security Technologies Inc	Disagree	If authentication is required for remote access to Low Impact systems (R14), it should be covered by R13 revocation.
32.25	WECC	Disagree	If the employee can access the system remotely why can the entity not remotely disable the access? Please have another look at the hours for the medium impact level.This should apply to all impact levels and Medium and Low impact systems should require not more than 24 hour timelines for revocation.
32.26	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
32.27	BGE	Disagree	Low impacted systems should have a timeframe defined for revocation

#	Organization	Yes or No	Question 32 Comment
32.28	FirstEnergy Corporation	Disagree	Need clarity on '...for external connectivity...'. For example, does this mean consoled in (directly connected) as well as remote electronic logon?Timeframes should not be in 'hours' (i.e. less than a full day). Tracking by time rather than days would not be logistically possible on all systems and compliance could not be maintained.The new requirements now have too many different time frames to meet. Again, not logistically possible on all systems and compliance could not be maintained for larger utilities.Similar concerns as previously stated with Table 9. See Questions 22 and 23.
32.29	Detroit Edison	Disagree	Please explain the reason for different revocation times between High Impact on 13.2 and 13.3.
32.30	American Municipal Power	Disagree	Please provide a little or no impact category
32.31	NextEra Energy Corporate Compliance	Disagree	Please refer to comments submitted for questions 22 and 23.
32.32	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12 and Table 13. Puget Sound Energy suggests including wording similar to Table 11: "Required for external connectivity only".
32.33	Progress Energy - Nuclear Generation	Disagree	R13 durations should align with those described in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
32.34	LCEC	Disagree	R13 requirements should be moved to the account management section.
32.35	ISO New England Inc	Disagree	Recommend using the same thresholds as R9 Recommend changing from "Required for external connectivity only" to "Required" since the criteria already limit the scope

#	Organization	Yes or No	Question 32 Comment
			to “remote access”
32.36	Hydro One	Disagree	Recommend using the same thresholds as R9.Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
32.37	Northeast Power Coordinating Council	Disagree	Recommend using the same thresholds as R9.Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
32.38	Black Hills Corporation	Disagree	Remote access revocation should be no different that other types of access and the 24 hour should apply.
32.39	Public Service Enterprise Group companies	Disagree	Remote access should be governed by the same rules are normal access. The time frame in 13.1 for High Impact BES Cyber Systems is unreasonably short. Notifying and securing the appropriate personnel to disable access once the job duties no longer require access may not be possible in all circumstances to guarantee that access is always revoked within 1 hour. This may not be operationally feasible. The timeframe should be similar to access revocation for user with non-remote access as specified in Table R9 item 1.9 (i.e. within 24hrs).
32.40	Manitoba Hydro	Disagree	Remote electronic access to BES Cyber Systems should be revoked for Low Impact BES Cyber Systems, and not permitted indefinitely. The remote access revocation period for generation High Impact BES Cyber Systems should be 6 hours, the same as for the Transmission High Impact BES Cyber System.
32.41	Exelon Corporation	Disagree	Requirements 13.1, 13.2 and 13.3 contain time parameters in hours. Exelon’s tracking systems that would be used to demonstrate compliance are tracked in time increments of days, not hours. If an hourly timeframe is required it will cause extensive modifications to numerous enterprise wide systems to allow tracking at an hourly level. One must ask how this improves reliability. What is the basis for time

#	Organization	Yes or No	Question 32 Comment
			levels and having a different timeframe for a control center than other locations? With the exception of a termination for cause, what is the basis for requiring access removal for someone who was a trusted employee on such an aggressive timeframe? What is the risk that is being addressed by making a 1 hour timeframe requirement?
32.42	Southwest Power Pool Regional Entity	Disagree	Revocation timeframes should be expressed in business days.
32.43	National Grid	Disagree	Same as in Q. 31.
32.44	San Diego Gas and Electric Co.	Disagree	SDG&E feels that the key for this requirement is the definition of the phrase "when job duties no longer require remote access". This phrase can be interpreted in a couple of different ways. The more strict interpretation is that a person would no longer need access after their session is complete, or perhaps after taking a break or going to lunch. This could happen a few times per day, depending on the work. A second interpretation could mean that a person no longer needs access after a 6 month long project is completed or there is a reassignment to another part of the company after 3 years of working on the BES Cyber Systems, etc. In the former case, it becomes a large burden to revoke access within one hour several times per day, and could be a manual process on some systems. On the other hand, if you consider the second interpretation (6 month project or transfer after 3 years), SDG&E would ask why is it so important to revoke remote access with 1, 4, or 6 hours after such a long period of time that a person has had access? Sometimes it takes time for a person to get reassigned, change locations, change projects, etc. In this case, 4 hours would be the minimum that SDG&E feels is practical to be able to comply with.
32.45	Progress Energy (non-Nuclear)	Disagree	See comment 14.This should be no different than the revocation of cyber access revocation. This requirement is not needed.
32.46	GTC & GSOC	Disagree	See comments to question 31 above

#	Organization	Yes or No	Question 32 Comment
32.47	BCTC	Disagree	See our response for table 9 time targets
32.48	Constellation Energy Control and Dispatch, LLC	Disagree	See response to Question 31.
32.49	Regulatory Compliance	Disagree	STRIKE Table R13
32.50	EEI	Disagree	Suggest removal of the words "for external connectivity only" from the table 13 columns, as the requirement themselves discuss the issue of remote access, therefore the words "for external connectivity only" are unnecessary and redundant.EEI suggests using a uniform number of hours across various facility types for high and medium.EEI suggests using 7 calendar days for medium.EEI suggests using 8 hours for high impact.EEI suggests adding a footnote here to reference the definition put forth in R11: "Remote access for the purpose of this standard means an interactive user session with a BES Cyber System from a device external to the BES Cyber System."
32.51	Allegheny Energy Supply	Disagree	Suggest using a uniform number of hours across various facility types for high, medium and low.Suggest using 7 calendar days for medium and 14 calendar days for low impact.Suggest using 12 hours for high impact.
32.52	Allegheny Power	Disagree	Suggest using a uniform number of hours across various facility types for high, medium and low.Suggest using 7 calendar days for medium and 14 calendar days for low impact.Suggest using 12 hours for high impact.
32.53	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS comments noting that as written, the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access). However we feel the one area where an entity is vulnerable is when personnel are terminated for cause. We see this as the most extreme case when an

#	Organization	Yes or No	Question 32 Comment
			entity should be diligent in protecting remotely accessible BES cyber systems and act within the time of a normal shift. We suggest 8 hours for termination for cause, except when a termination is preplanned, in which case a shorter time period may be feasible. Similar to the comments we provided regarding R9: We know there are pressures to have access restricted as soon as possible but we are trying to be realistic given the time it will take to remove access from systems which have multiple owners, are in remote locations and which have numerous devices to access. It seems that the drafting team is basing their proposed timetable on a control center where the cyber systems are more IT focused and have controls that can be turned on and off easily.We propose the following changes to the Impact Levels of R13:R13 Table 13.1: (NEW) Low Impact: N/AMedium Impact: 8 hoursHigh Impact: 8 hoursR13 Table 13.2: (Old 13.1)Low Impact: N/AMedium Impact: 36 hoursHigh Impact: 36 hourR13 Table 13.3: (Old 13.2)Low Impact: N/AMedium Impact: 1 WeekHigh Impact: 1 WeekR13 Table 13.4: (Old 13.3)Low Impact: N/AMedium Impact: 1 WeekHigh Impact: 1 Week
32.54	Minnesota Power	Disagree	The impact levels seem well defined however inconsistencies in the definitions of “remote access” and “external connectivity,” (see response in Question 26) create confusion regarding the applicability of the criteria for each impact level.In certain circumstances, it may not be possible to adhere to the proposed timeframes, especially in instances where BES Cyber System support is 8 hours a day, 5 days a week or where notification of termination comes from corporate systems that are also updated on an 8 hours a day, 5 days a week schedule. The need for more immediate time constraints, when compared to electronic access as defined in Requirement R9 that is not remote is understood, but both the Requirements in R9 and R13 need to take into account reasonable business processes that impact notification of employee reassignment and separation.Minnesota Power recommends that the timelines for R13 be consistent with those established in R5 and R9, but would agree that terminology should be included urging Registered Entities to expedite this process as much as possible with regards to remote access.

#	Organization	Yes or No	Question 32 Comment
32.55	GE Energy	Disagree	The revocation targets for High Impact systems will be almost impossible to meet for revoking vendor personnel access (Table R13 HI BES remote access must be terminated within 1 hour of access no longer being required). It also seems to be in conflict with the revocation times in Table R9? These need to be linked together.
32.56	Northeast Utilities	Disagree	The timeframe is extreme for routine personnel changes (1 - 6 hours). Suggest a "for cause" termination for these timeframes and make routine more reasonable (3 days to align with R9?) Also, it is not needed if you agree with comment to 29. Host/application and network access should be treated the same.
32.57	US Bureau of Reclamation	Disagree	The timeframes for High Impact are not consistent with R9 and appear to be too stringent. Further, requirements need to be established for all system impact levels.
32.58	Oncor Electric Delivery LLC	Disagree	These proposed time frames are not practical as most HR systems are separate (and should be) from real-time operations of the BES. The time-frames for High Impact cannot be different from Medium, as they utilize the same back-office information systems.
32.59	Bonneville Power Administration	Disagree	These requirements are not necessary. They are already covered under R9. Revocation of electronic access applies to all electronic access regardless of whether it is local, remote or wireless. There is no difference. In addition, this requirement could force Cyber System administrative personnel to take action to revoke access even if it means not performing other actions needed to support real-time operations, or risk non-compliance. As an example, if a BES Cyber System has failed for some reason, the corrective actions should take precedence over revoking access. Under those circumstances, an entity could find itself in the position of deliberately allowing non-compliance in order to restore the integrity of the BES. The required time frames are impossibly short for high impact systems. It is difficult to justify dropping all other actions to revoke access for someone unless there is reason to believe that the individual poses a threat. In that case the requirements of R9 are in effect.This

#	Organization	Yes or No	Question 32 Comment
			requirement seems to conflict with R9 and Table R9. Table R9 allows 24 hours for access revocation due to termination for cause. Table requires revocation within 1 hour, even if termination for cause is not required.Recommendation: Remove this requirement entirely. Treat revocation of remote access as just another revocation of access under R9. Otherwise, increase the time frames to something achievable.
32.60	Consultant	Disagree	This requirement is access revocation and should be included in R9 as it relates to account management and access revocation.13.1, 13.2, & 13.3 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.13.1, 13.2, & 13.3 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.Suggest deleting "for external connectivity only" as redundant & unnecessary. This requirement is for remote access and is by definition external access.
32.61	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
32.62	We Energies	Disagree	We Energies agrees with EEI: Suggest removal of the words "for external connectivity only" from the table 13 columns, as the requirement themselves discuss the issue of remote access, therefore the words "for external connectivity only" are unnecessary and redundant.We Energies agrees with EEI: Suggest using a uniform number of hours across various facility types for high, medium and low.We Energies agrees with EEI: Suggest using 7 calendar days for medium and 14 calendar days for low impact.We Energies agrees with EEI: Suggest using 8 hours for high impact.We Energies agrees with EEI: Suggest adding a footnote here to reference the definition put forth in R11: "Remote access for the purpose of this standard means an interactive user session

#	Organization	Yes or No	Question 32 Comment
			with a BES Cyber System from a device external to the BES Cyber System."

33. Requirement R14 of draft CIP-011-1 states "Each Responsible Entity shall document and implement its organizational processes, technical mechanisms, and procedures for control of wireless and remote access to electronic access points to its BES Cyber Systems including wireless and remote access if it is used, that incorporate the criteria specified in CIP-011-1 Table R14 – Wireless and Remote Electronic Access Controls to ensure that no unauthorized access is allowed to its BES Cyber Systems." Do you agree with the list of criteria that is included in Requirements Table R14? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Requirements for remote access in CIP-011-1 R14 have moved to CIP-005-5 - Cyber Security — Electronic Security Perimeters.

Commenters expressed concern that the scope of the "Banner" requirement should be clarified and that having a banner is not a security control. The SDT agrees and notes that the requirement to have appropriate use banners was considered administrative and has been removed.

Several other commenters suggested splitting wireless and remote access requirements. The SDT notes that a new requirement for Remote Access Management (CIP-005-5 R2) was created based on the Urgent Action Revisions to CIP-005-3, and the wireless access requirements have been removed.

#	Organization	Yes or No	Question 33 Comment
33.1	WECC		Don't see the security value of requiring login banner as required in 14.4. This requirement seems to stem from the belief that in a legal prosecution the court would need to show that the system was misused or accessed inappropriately and that a login banner accomplishes this by notification. Since most attacks are done via automation today, and internal attackers are likely required to sign an acceptable use policy this requirement seems to only add operational cost. Additionally, one can prove that inappropriate use was done by the mere fact that the person is using the system without authorization. Also keeping this in for only high impact systems would let attackers easily know which systems are high impact/value. Recommend dropping criteria all together. The appropriate use banner criterion does not belong here. This is a legal protection, not a security control, and would be better placed in a policy type requirement. Consider replacing "multi-factor" with "strong", and offering

#	Organization	Yes or No	Question 33 Comment
			additional language to clarify the term. "Strong" auth should be required for all remote access. Provide distinction between remote access from untrusted locations, such as the internet, and remote access from trusted locations, such as a backup control center.
33.2	Duke Energy	Agree	14.4 requires a TFE
33.3	Regulatory Compliance	Agree	BUT14.2 - What is the risk protection versus cost, time and overhead to implement?
33.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
33.5	CWLP Electric Transmission, Distribution and Operations Department	Agree	Is multifactor access control limited to electronic methods only? Can the use of enabling or disabling a device such as a modem equal to a portion of multifactor controls?
33.6	Puget Sound Energy	Agree	Puget Sound Energy agrees with the criteria, but suggests NERC provide clarity in regards to 14.4. Is NERC requiring an "appropriate use banner" on the user screen for the initial attempt of remote access, or for all interactive attempts established after successfully authenticating remotely? Example: Is an appropriate use banner only needed for a 2-factor VPN connection screen, or at all systems accessed through a 2-factor VPN (operating system and application(s) on BES Cyber System Components?
33.7	Progress Energy - Nuclear Generation	Agree	R14 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
33.8	GTC & GSOC	Agree	We recommend references to wireless should be removed from R14 and the associated table. The actual requirements are not related to wireless as distinct from

#	Organization	Yes or No	Question 33 Comment
			other remote access
33.9	Green Country Energy	Agree	Will their be guidance? How about changing the statement to "reasonably ensure" that no unauthorized access is allowedExample: If my processes allow anyone to be authorized, I then can "ensure" no unauthorized access will occur.
33.10	Independent Electricity System Operator	Disagree	- R14.1 and R14.2 seem to be stating the same thing. R14.2 is covered by R14.2.- R14.4 - Shouldn't the use banner be required to be installed on the BES cyber components themselves prior to login. If port 22 is open on a firewall, the firewall will
33.11	American Electric Power	Disagree	14.1: Regarding "If remote access is used and/or implemented, include authentication controls". Suggest replacing "include" with "document".
33.12	FirstEnergy Corporation	Disagree	14.2 this could be difficult to implement depending on the definition of "interactive user session" within the definition of remote access.14.2 - add '...authentication controls for remote access mechanisms'14.3 - add 'remote access' somewhere in this sub-requirementWith R14.4, it requires an appropriate use banner; there is no allowance for equipment that can not support a banner.
33.13	Luminant	Disagree	14.4 - where technically feasible
33.14	Southwest Power Pool Regional Entity	Disagree	14.4 is overly prescriptive. Consider revising the requirement to simply state "Display an "appropriate use banner" upon an interactive attempt to access a BES Cyber System, stating that unauthorized use of the system is prohibited."
33.15	BCTC	Disagree	Â R 14.1: remove Required as the requirement is satisfied under R14.2R14.4: text "remote electronic access" devices; suggest that the language be rewritten/ simplified so the objective is clear - i.e. ensure appropriate CCAs display appropriate use banner when connecting to these assets remotely
33.16	Southern California	Disagree	As stated above, remote access should be thoroughly documented and full encryption

#	Organization	Yes or No	Question 33 Comment
	Edison Company		and authentication methods applied.Also, SCE requests that the drafting team review the intent of R14.4 and R7.2 and consider combining the requirements.
33.17	Tenaska	Disagree	Combine 14 and 11
33.18	Alliant Energy	Disagree	Consideration should be given to whether or not the access provides control capability or simply read only.
33.19	ISO New England Inc	Disagree	Did the SDT assume that wireless is a form of remote access for R11 - R14? If YES, please update the wording. If NO, the Requirements are confusing because we use wireless that is not remote access, plus wireless includes more than WiFi.Depending on that answer, R14 should move into R11 or into the Boundary Protection RequirementsR14.1 and R14.2 seem to be stating the same thing.14.2 should have requirement for medium. 14.4 appropriate use banner - is this required for legal steps in the event of an issue... this is not a security control.If the banner is need then the use banner should be required to be installed on the BES cyber components themselves prior to login. If port 22 is open on a firewall, the firewall will allow the traffic through without displaying a banner.
33.20	Northeast Power Coordinating Council	Disagree	Did the SDT assume that wireless is a form of remote access for R11 - R14? If YES, the wording should be revised. If NO, the Requirements are confusing. Wireless that is not remote access may be used, plus wireless includes more than WiFi.Depending on that answer, R14 should move into R11 or into the Boundary Protection Requirements.
33.21	Florida Municipal Power Agency	Disagree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Item 14.4 is very specific in requiring “appropriate use banner” this should be removed or reworded to cover various methods of notification. Also the standard should demand that no identifiable details be given about the system before authentication is complete.We believe items 14.3 and 14.4 are going to set the stage for numerous TFE’s within the industry. Many devices (e.g.,

#	Organization	Yes or No	Question 33 Comment
			protective relays) do not support explicit access permissions and appropriate use banners.
33.22	USACE - Omaha Anchor	Disagree	Have concerns about 14.2 “multifactor authentication.” Would prefer terms either “multi-authentication.” If we were to implement multifactor we would be removing levels of access to our system and potentially making it easier to hack if they can overcome the multifactor issue.
33.23	Black Hills Corporation	Disagree	If two cyber systems are on the same protected network, and within the same physical boundary, should two-factor authentication be required? We don’t think so, but according to the definition of remote access and this requirement it would be.
33.24	LCEC	Disagree	Is this for remote access and wireless network access or does it also apply to wireless communications between BES Cyber System Components?
33.25	NextEra Energy Corporate Compliance	Disagree	NextEra believes the multifactor controls required in section 14.2 is too specific. “Strong technical controls” is a preferred update to the requirement. There may be better controls from a security and reliability standpoint, but as the requirement stands, Responsible Entities are limited in the technological implementations to support compliance to the requirement.Requirement 14.3 specifying that responsible entities must “deny access by default; [specifying] explicit access permissions” is unclear. Since this is supposed to be related to remote electronic access, the requirement should clarify that the end user is explicitly denied access thru the access point(s) of the network containing the BES Cyber System unless explicitly allowed access into that network.Requirement 14.4 requires the displaying “of an ‘appropriate use banner’ on the user screen of remote electronic access control devices that, upon an interactive attempt to access a BES Cyber System, states that unauthorized use of the system is prohibited.” This appropriate use banner should be required upon every new connection and entry attempt to the BES Cyber System network, for example a firewall or SSL VPN connection that controls remote access. Also, allowance for TFE's in 14.2 through 14.4 should be included.Regarding 14.2, NextEra

#	Organization	Yes or No	Question 33 Comment
			would like clarifaction for the required multifactor authentication controls. Is it required for assets within the boundary or does it only apply to the control of wireless and remote access to electronic access points to BES Cyber Systems? or both?
33.26	Constellation Energy Commodities Group Inc.	Disagree	Provide clarification regarding acceptable use banner (14.4) - in some instances such banners cannot be added to system. Make clear that the requirement may be met by displaying a banner upon workstation sign-on or upon user entry to the remote access environment. What is the specific meaning of authentication controls in 14.1? Since this is called out separately from two-factor authentication, I interpret it to mean that remote access cannot be enabled via generic accounts, only via user specific accounts with authentication (password) known only to the individual. Is that the idea?
33.27	Detroit Edison	Disagree	R11, R12 and R14 use term “remote electronic access” and R13 uses the term “remote access”. Revise to maintain consistency.Wireless electronic access is not an access method; it is just the medium to obtain access. In an effort to remove reference to specific technology, wireless should not be identified anywhere in the standard. References to specific technologies should be addressed in the guidance documentation.
33.28	Ameren	Disagree	R14.1 - The complexity and scope of the documentation of the Low Impact Systems will be challenging to keep succinct for auditors.R14.3 - Deny access by default is not needed. Requiring authentication implies access is denied by default.R14.4 - Not all systems support user banners. This will be hard to keep from being a TFE on many “high” systems.
33.29	Southern Company	Disagree	R14.1-4 addresses remote access only and does not include wireless, the table title and R14 includes wireless.
33.30	Entergy	Disagree	R14.2 dictates multifactor authentication controls for only high impact BES Cyber Systems. Entergy recommends serious consideration of extending this to low and medium impact BES Cyber Systems where localized wireless technology is employed.

#	Organization	Yes or No	Question 33 Comment
			Eliminate 14.4. We understand the purpose of this requirement but do not believe that it adds to the protection of any cyber system. If it is to be added then it should be placed outside of the wireless and remote electronic access control section and placed elsewhere. Entergy believes some aspects of R11 and R14 are redundant and suggests combining them. We also believe criteria in R14 should apply to high, medium and low risk assets and provide a footnote indicating that where requirements are unable to be met explicitly that the strongest possible controls should be employed alternatively.
33.31	US Bureau of Reclamation	Disagree	R14.3: Add deny access by default requirement for low systems. Specific access permissions are not required, however.
33.32	San Diego Gas and Electric Co.	Disagree	SDG&E recommends that a definition of what is meant by "multifactor authentication controls" be included in a definition box near R14.
33.33	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS proposal. Criteria in 14.3 and 14.4 are very specific in application of technology that may not be supported by devices in the field. These criteria should be removed or reworded to cover various methods of operation. If the drafting team keeps these requirements the following is our recommended language: R14 Table 14.3: If a BES cyber system component supports explicit access permission capability, the device should deny access by default. R14 Table 14.4: If a BES cyber system component supports notification capability, remote electronic access control device users should be notified that unauthorized use of the system is prohibited.
33.34	MidAmerican Energy Company	Disagree	The new definition of BES Cyber System creates confusion over what technologies are intended to be in-scope. The core changes significantly changes how a responsible entity (RE) establishes and secures remote access to these systems. The REs will develop their own unique determination on how to deal with this situation. Which is likely not going to deliver the intended result the Standards drafters are looking for industry-wide? As this relates to R22 - firewalls, our CIP defined access points, are

#	Organization	Yes or No	Question 33 Comment
			defined as part of a given BES Cyber System. One likely scenario is that we will define a separate BES Cyber System that manages these firewalls that might include a client PC, a firewall manager, and some network infrastructure components. The remote access rules and even the other general protections of these cyber components to manage this type of communication become very ambiguous.Retain the existing ESP concept versus adopting the BES Cyber system concept and make some of the other operational improvements this draft makes.While the criteria themselves are not onerous for the long term/future development of the systems, the current BES technology in place or available, will require technical feasibility exceptions as not all systems within the BES can support all criteria listed.
33.35	PacifiCorp	Disagree	The new definition of BES Cyber System creates confusion over what technologies are intended to be in- scope. The core changes significantly changes how a responsible entity (RE) establishes and secures remote access to these systems. The REs will develop their own unique determination on how to deal with this situation. Which is likely not going to deliver the intended result the Standards drafters are looking for industry-wide? As this relates to R22 - firewalls, our CIP defined access points, are defined as part of a given BES Cyber System. One likely scenario is that we will define a separate BES Cyber System that manages these firewalls that might include a client PC, a firewall manager, and some network infrastructure components. The remote access rules and even the other general protections of these cyber components to manage this type of communication become very ambiguous.Retain the existing ESP concept versus adopting the BES Cyber system concept and make some of the other operational improvements this draft makes.While the criteria themselves are not onerous for the long term/future development of the systems, the current BES technology in place or available, will require technical feasibility exceptions as not all systems within the BES can support all criteria listed.
33.36	Bonneville Power Administration	Disagree	The objective of this requirement ('to ensure that no unauthorized access is allowed to its BES Cyber System") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than

#	Organization	Yes or No	Question 33 Comment
			appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.In addition: Table R14, Section 14.2 is excessive. Given the draft Standard's definition of external connectivity, remote access could also be a case of accessing a system from a nearby system over secured communications paths. An example would be a user on one BES Cyber System accessing another BES Cyber System in the same Control Center. It is not reasonable to justify multi-factor authentication in these circumstances. In addition, many existing systems do not have the capability of enforcing multi-factor authentication. Finally, there are other authentication controls stronger than username/password which are not multifactor: biometric, one time passwords, dial-back, and so forth. Recommendation: Delete the requirement. If not, change the definition of "external connectivity" as discussed in question 13, and change the requirement from "multifactor authentication controls" to "authentication controls stronger than username/password".Section 14.4. There are significant issues with this requirement. - The warning banner is a legal requirement, not a security requirement. Its only purpose is to provide support for legal recourse if someone violates what it says. - No unauthorized person should be accessing High Impact Cyber Systems. Any user with authorized electronic access will have completed security training, which includes proper use of BES Cyber Systems. Any unauthorized user will ignore the banner. - It does not prevent unauthorized access, and therefore does not support the purpose of the requirement. - The requirement has technical feasibility issues. To provide specific scenarios: 1. The user connects from a device controlled by the Responsible Entity, using networks owned by the RE. The user authenticates at the local device. When attempting to connect the the BES Cyber System, the firewall access point allows the traffic, based on the originating point within the trusted network. The user again authenticates at the BES CYber System. At no time does the user authenticate at the access point itself (nor does the rest of Table R14 require authentication at the access point.) In fact, under these circumstances firewalls generally do not have the capability to request authentication or present a banner. 2. The user connects via a

#	Organization	Yes or No	Question 33 Comment
			VPN. The VPN client authenticates the user, then uses a PKI certificate to authenticate to the access point. The user is then granted access to the network and can proceed to authenticate and connect to a BES Cyber System. At no point did the user authenticate to the access point, nor was there an opportunity to present a banner.Recommendation: The best solution is to eliminate the requirement. If the requirement cannot be removed:First, change the definition of remote access and/or external connectivity as discussed above. This would eliminate the requirement to present a banner to users attempting access from equipment belonging to the Responsible Entity. Second, allow the banner to be present at locations other than the access point. A possible revised requirement would be: "Display an "appropriate use banner" to the user that, upon an interactive attempt ..." Also, change "Required" to "Required for external connectivity only".
33.37	Consultant	Disagree	The terminology "wireless and remote access" is redundant. The definition of remote access (near requirement R11) includes wireless access implicitly. Suggest using the defined term "Remote Access" rather the redundant terminology.Table R14 - Item 14.1 It seems illogical to require authentication controls on Low Impact systems when there is no Account Management required for these systems. Suggest deleting the requirement for Low Impact BES Cyber Systems.Items 14.1 & 14.2 - The terminology "is used and/or implemented" seems redundant. It appears that being "implemented" creates the vulnerability, and the requirement for control. Suggest changing the words "is used and/or implemented" to "is implemented".Item 14.3 - This includes two different requirements: (1) Deny access by default & (2) specify explicit access permissions. The first requirement is a technical implementation and should remain here. The second is an account management requirement and should be moved to the account managment requirement R8.
33.38	Minnesota Power	Disagree	These criteria are generally acceptable; however, Minnesota Power requests that the Standards Drafting Team consider defining “authentication controls.”Also in Part 14.2, the requirement regarding the use of multifactor authentication controls sets a technology-specific direction that may not stand over time, including the possibility of

#	Organization	Yes or No	Question 33 Comment
			biometric authentication that, while not multifactor, is a stronger control.
33.39	Dominion Resources Services, Inc.	Disagree	To avoid the potential for TFE's associated with R14.4, a footnote similar to the one used for Table R10 on Page 11 of CIP-011 should be added. Also, access controls related to access points would be better addressed in the Boundary Controls Section of CIP-011.
33.40	Hydro One	Disagree	We don't understand the emphasis on wireless communication and believe that in the present form, it would be very complex to implement. It's our opinion that the protection should remain the same regardless of the type of access point.
33.41	Progress Energy (non-Nuclear)	Disagree	What conditions would dictate different authentication controls for different impact levels? Is it better for them to all be the same?R14.4 is unnecessary. The population of persons granted remote access rights is extremely limited and these people are highly trained and trustworthy. The appropriate use banner is used in situations where a general population was granted this type of access and that is not the case for remote access to any control systems.
33.42	National Grid	Disagree	What types of authentication controls are valid? (Authentication level such as a shared password or a user level control)
33.43	Alberta Electric System Operator	Disagree	Wireless access and remote access should be two separate concepts.
33.44	Network & Security Technologies Inc	Disagree	Wording of 14.4 gives the (doubtless unintended) impression a banner must be displayed on the user screen of electronic access control devices. Re-word to clarify banner must be displayed on the user screen of the accessing device.

34. Table R14 provides direction concerning what impact level of BES Cyber Systems to which Requirement R14 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R14 has moved to CIP-005-5 R1.

Commenters expressed that the 'deny by default' requirement should also apply to Low impact BES Cyber Systems. In response, the SDT agrees that some network access control should apply to all BES Cyber Systems, including the Low Impact BES Cyber Systems. CIP-005-5 R1 – Electronic Security Perimeter allows considerable flexibility for the entity to determine which security controls to apply, because of the significant number of Low Impact BES Cyber Systems.

Commenters suggested requiring a banner on Medium and Low Impact BES Cyber Systems. However, the SDT disagrees and felt the requirement to have "appropriate use banners" was administrative; therefore, it has been removed.

#	Organization	Yes or No	Question 34 Comment
34.1	CWLP Electric Transmission, Distribution and Operations Department	Agree	As long as TFEs are available for systems that do not support the password requirements.
34.2	Bonneville Power Administration	Agree	But see comments on R14.2, above. In addition, 14.4 is only acceptable if the definitions of remote access and external connectivity are changed, as discussed above. A banner is appropriate for someone accessing a BES Cyber System from completely outside the control of the entity.
34.3	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
34.4	FirstEnergy Corporation	Agree	With the exception of the concerns presented in the previous question.

#	Organization	Yes or No	Question 34 Comment
34.5	Oncor Electric Delivery LLC	Disagree	(R14.2)Multifactor authentication in legacy substation devices is extremely difficult and not needed. Appropriate logging and access controls will eliminate most threats. (R14.4)Appropriate Use Banners are not possible on many legacy dial-up devices used in substations. Appropriate logging and access control will eliminate most threats.
34.6	Southwest Power Pool Regional Entity	Disagree	14.2 and 14.4 should also apply to Medium impact BES Cyber Systems.
34.7	US Army Corps of Engineers, Omaha Distirc	Disagree	14.2 Multifactor authentication will be a major burden for small IT staffs. Standard should offer alternatives to mitigate - stronger passwords and or more frequent password changes.
34.8	WECC	Disagree	14.3 should be required for low impact.Remote access controls should apply to all impact levels.
34.9	Black Hills Corporation	Disagree	14.4 should be “Required” for all. Others are OK.
34.10	ERCOT ISO	Disagree	14.4: Should apply to Medium Impact BES Cyber System.
34.11	Tenaska	Disagree	18.1 all should be each.19.1 Validation of inbound data is more often done on the host application level and not at the boundary or host level.19.2 Is this RTU data? The protection is done at the applications level and I cannot examine data at my perimeter if it is encrypted at the host level.
34.12	Progress Energy (non-Nuclear)	Disagree	Believe it should be required for Low, Medium and High for R14.1, R14.2 and R14.2.
34.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
34.14	The Empire District	Disagree	Comments: We believe items 14.3 and 14.4 are going to set the stage for numerous

#	Organization	Yes or No	Question 34 Comment
	Electric Company		TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.15	E.ON U.S.	Disagree	E.ON U.S. believes that the proposed time requirements are not reasonable and require 24x7 support personnel with the privilege to revoke access.
34.16	Entergy	Disagree	Entergy believes some aspects of R11 and R14 are redundant and suggests combining them. We also believe criteria in R14 should apply to high, medium and low risk assets and provide a footnote indicating that where requirements are unable to be met explicitly that the strongest possible controls should be employed alternatively.
34.17	Dominion Resources Services, Inc.	Disagree	High Impact should be removed from 14.1 since it is covered by 14.2.
34.18	GE Energy	Disagree	If user accounts are audited on Medium Impact systems (see question 20), there should be an appropriate use banner.
34.19	LCEC	Disagree	Is this for remote access and wireless network access or does it also apply to wireless communications between BES Cyber System Components?
34.20	US Bureau of Reclamation	Disagree	It would seem that this criteria is in conflict with sound business practices. The concept of allowing access by default to Low Impact BES Cyber Systems does not make sense. Add deny access by default requirement for low systems. Specific access permissions are not required, however.
34.21	MidAmerican Energy Company	Disagree	Items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.Table R14 should be rewritten in a manner that minimizes TFEs. As an example, eliminate the word upon in 14.4 to eliminate TFE for systems that can only display banners immediately after access.

#	Organization	Yes or No	Question 34 Comment
34.22	National Grid	Disagree	National Grid suggests having 14.3 for Low Impact systems as well.
34.23	NextEra Energy Corporate Compliance	Disagree	NextEra believes Medium Impact BES Cyber Systems should have to comply with requirement 14.4. However, the rest of the impact levels are appropriate.
34.24	American Municipal Power	Disagree	Please provide a little or no impact category
34.25	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12. Table 13, and Table 14. Puget Sound Energy suggests including wording similar to Table 11: “Required for external connectivity only”.
34.26	Garland Power and Light	Disagree	Requirement 14.3 and 14.4 Should add "required" to all impact levels
34.27	USACE HQ	Disagree	Requirements 14.3 should be required for every level of impact.
34.28	San Diego Gas and Electric Co.	Disagree	SDG&E believes that Medium impact assets should also be required to have multifactor authentication controls (within the definition question mentioned in Question 33).
34.29	ISO New England Inc	Disagree	Should apply to all
34.30	ReliabilityFirst Staff	Disagree	Suggest “Required” for Medium Impact in row 14.2.
34.31	Consultant	Disagree	Table R14 - Item 14.1 It seems illogical to require authentication controls on Low Impact systems when there is no Account Management required for these systems. Suggest deleting the requirement for Low Impact BES Cyber Systems.
34.32	Alberta Electric System Operator	Disagree	The AESO suggests adding the following to Table R14: o 14.3 - Required for Low Impact. o 14.4 - Required for Low and Medium Impact.

#	Organization	Yes or No	Question 34 Comment
34.33	Southern California Edison Company	Disagree	The same authentication methods should be applied to all Levels.Also, SCE requests that the drafting team provide justification for the lack of a deny access by default for low impact system.
34.34	Minnesota Power	Disagree	These impact levels are generally acceptable, however to maintain consistency with Table R10, Parts 10.4 and 10.5, the High Impact cell in Part 14.1 should be blank since it is addressed in Part 14.2.
34.35	American Transmission Company	Disagree	We believe items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.36	Florida Municipal Power Agency	Disagree	We believe items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.37	MRO's NERC Standards Review Subcommittee	Disagree	We believe items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.38	Hydro One	Disagree	We don't understand the emphasis on wireless communication and believe that in the present form, it would be very complex to implement. It's our opinion that the protection should remain the same regardless of the type of access point.
34.39	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R14:R14 Table 14.1: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR14 Table 14.2: Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredR14 Table 14.3: (if this requirement is retained)Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredR14 Table 14.4: (if this requirement is retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required

35. Requirements R15 to R19 of draft CIP-011-1 concern procedures for system security protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R15 to R19? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R15 through R19 have moved to CIP-007-5 R1 through R4.

For physical ports and services, several commenters expressed confusion around the term "externally accessible." The SDT agrees, and "externally accessible physical ports" was removed and substituted with physical ports used for "network connectivity, console commands, or removable media."

In addition, for physical ports and services, commenters expressed concern that physical port protection seems unnecessary, since overall physical security and personnel vetting is required, and many devices do not allow for configurable disabling of ports. The SDT agrees the objective of disabling unnecessary physical ports is primarily to prevent accidental propagation of malicious code. In response, the requirement was modified to "restrict" access. A description of acceptable forms of restriction is included in the measures; for example, these could be physically disabling the port or including signage about the use of ports.

For security event monitoring, several commenters stated that there is no need for weekly log review/clarity or manual log review since continuous monitoring is required. The SDT disagrees and references paragraph 528 of the FERC Order 706 that provides context for a weekly log review. The requirement allows for a review to include a sampling or summarization of security event logs.

For security event monitoring, several commenters expressed concern that there is no definition of "cyber security event" (i.e., a normal good logon is a "security event"). The SDT agrees and has modified the requirement to ensure that audit events must be organizationally defined. An enumerated list of events in the Standard is of little value.

For security event monitoring, commenters expressed concern that the requirement can be interpreted to include monitoring and logging for systems that don't support this functionality. The SDT agrees, and in response, this requirement was modified to apply log generation to the BES Cyber System (rather than the component) and allow the entity to define the generated events to audit.

For patch management, commenters expressed concern that not every patch is applicable to a BES Cyber System. The SDT agrees with this observation and notes that this requirement should be covered through the patch evaluation process. The focus of the requirement should be a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner."

For patch management, commenters expressed concern that flexibility is needed for the installation of patches; these dates can be based on equipment outage schedules, which could change the frequently or grid conditions that may or may not allow patching. The SDT agrees that the date of installation needs to be flexible to take into account equipment outage situations or high risk system conditions that could present an undesirable time for installing patches. Requiring an install date for the patches does nothing to improve BES Cyber System reliability. The overall goal of security patching should be to decrease the latency between security patch release date, application vendor certification date, entity testing, and implementation date. The SDT has revised the patch management requirements to achieve this goal.

For patch management, some commenters posed the question of what starts the clock for patching (release vs. availability vs. OS vendor vs. control system vendor). The SDT agrees there should be a starting point, but requiring an install date for the patches does nothing to improve BES Cyber System reliability. In response, the requirement has been modified so that Responsible Entities are required to create or revise an implementation plan within 30 days of the patch release from the identified source of the patches.

For malicious code prevention, commenters posed the question of whether the standard requires testing against actual malicious code. In response, the SDT disagrees and feels the intent was strictly focused on insuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.. This has been clarified in the guidance for the standards.

For malicious code prevention, commenters expressed there is still nothing specifying that malicious code prevention does not apply to field or network equipment. The SDT agrees, and in response, the requirement was modified to include malware prevention processes. It is now much more a “what” and not a “how” level of requirement.

#	Organization	Yes or No	Question 35 Comment
35.1	Dairyland Power Cooperative		15. It is good that this section is not wrongly specific as CIP-007:R4 is. This should allow for solutions that are not specifically signature based. This should allow for a network-based solution rather than individual solutions on each component. BES systems should not be used like typical Internet user systems, and therefore it should not be enforced that Internet user solutions be applied.16.2 requires a fixed implementation schedule of patches. However there should be an allowance that not every little security patch needs application, and it should be acceptable to defer insignificant patches until a later date when a significant patch needs to be applied. Additional controls to compensate may not be needed other than the security already designed to isolate a BES cyber system.17.1 Focusing on documenting the process to

#	Organization	Yes or No	Question 35 Comment
			harden seems wrong-the focus should be on requiring/verifying that a system is hardened. 19.1/19.2 How is validating inbound data (19.1) different than determining if inbound data has been compromised (19.2)? Was the intent of 19.1 to validate/authenticate the remote host/application on inbound connection? There should be requirements to restrict inbound connections from known remotes only. Validation of data should be defined. Perhaps inbound need definition too. Is it inbound initiated connection vs. data transferred inbound regardless of initiation direction?
35.2	National Rural Electric Cooperative Association (NRECA)		In R17.1, what specifically is the mitigation plan required to address/accomplish? Please ensure this requirement is clarified to explain this better.
35.3	Progress Energy (non-Nuclear)		R16.2 fixed dates for generating stations that depend on outages for implementing this is impractical as outage dates frequently change. Also, the ambiguity from v1-v3 (resulting in so many TFEs) remains here and still needs to be addressed.R17.2 - do not understand the externally accessible port requirement, there are no externally accessible physical ports outside of the six-walled boundaries, requirement not needed.CIP-011 R15 - Require detecting and responding to introduction of malicious for Medium Impact Cyber Systems which could be an electronic relay, what if there isn't a commercial solution for installing malware detection for relays or any other electronic device that runs with only proprietary closed firmware? Would it be impractical to require this only for devices that run a general purpose programmable commercially available operating system such as Microsoft Windows Operating System variants/UNIX and LINUX variants/SUN SOLARIS variants/Apple OS variants, etc --- or Is there going to be TFE process for these such as for switches, etc.?We like that this requirement does not require the use of traditional virus protection software.CIP-011 R18.3 - Requirement to keep logs of system events for 1 year for each high impact device could be massive in terms of storage and archive and may not be technically feasible for electronic relays.CIP-011 - R19 table - Need additional clarification as to what data validation methods (data integrity checking) are to be

#	Organization	Yes or No	Question 35 Comment
			employed. Can this be satisfied solely by employing Secure FTP or Secure ICCP for all inbound data?Calibration ports on programmable relays must remain open for calibration but this requirement would require rendering them unusable. We want to ensure this use is interpreted as "normal" operations.CIP-011-1 R15.3 (System Security) - The statement 'Implement processes to test and update malicious code protections' should be clarified to specify that in no case should malicious code be purposefully exposed to operational BES Cyber Systems as a part of this testing.CIP-011-1 R16.2 (Security Patch Management) - Requiring a 'fixed date for either installation of the applicable patches or completion of mitigating measures that address the vulnerability' is too inflexible in a real world where such activities may need to be accomplished during the next plant outage.CIP-011-1 R19 (Communications and Data Integrity) - This sounds like a 'best practices' type of requirement, but depending on how BES Cyber Systems are defined, this could require redesign/implementation of front-end processors on all inbound traffic to all Control Center BES Cyber Systems. Such a requirement cannot be quickly implemented without significant potential impact on the BES. We would like to suggest that this be listed as a requirement for any new BES Cyber System implemented at a Control Center.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: "Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security."
35.4	FEUS	Agree	Agree with Comments: The drafting team should consider revising the wording of 17.1 from 'implement a mitigation plan' to 'implement mitigating measures' to reduce confusion with mitigation plans submitted to correct a violation.
35.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.R15.This is very poorly worded, and too open to interpretation on a number of areas.15.1 - how do you audit this item? FMPA suggests: "Document and implement procedures implemented to limit the

#	Organization	Yes or No	Question 35 Comment
			propagation of malicious code."15.3 - This could be interpreted to read that you need a full-scale development environment/copy of your production system to introduce malware to and guage the responsiveness of the mitigation techniques you put in place. If the intent of the standards is to protect the BES, by testing malicious code on systems that's not helping anyone. Time should be spent making sure it doesn't happen, not testing to see what happens when you introduce it. FMPA suggests "Review logs of malware detection systems within the following time periods: 30 calendar days for medium impact, 7 calendar days for high impact."R16.FMPA agrees with the intent of this standard; however there are some underlying issues that should be addressed before the standard is implemented. One such example might be a requirement to change out hardware to meet a new patch released by a vendor; before equipment is purchased it has to be tested - in some cases equipment shortages may make it impossible to comply with the 30-day requirement.R17.17.1 - How does "external connectivity" apply to network ports being shut down? Does that mean for devices that route data to other external networks?17.2 - What does "externally accessible physical ports" mean? Does this refer to ports that are connected via Ethernet cable to an area outside of the protected area? If so, the standard should explicitly say this.R18.18.1 - Requiring components that do not have logging capabilities to be monitored could be a real problem. While there are a number of technical ways to accomplish logging of systems, there is no clarity in the standard as to what is and is not acceptable levels of logging on a device - this needs to be better defined. FMPA suggests "Implement automated tools or organizational processes to monitor and log all available system events that are related to cyber security for all BES Cyber System components." This would give more flexibility in collecting data from other centralized devices (such as SCADA systems) and limit the data collection to what is available.18.2 - what is the definition of "Cyber Security"? How does one know what does or doesn't relate if there is no defining criteria?18.3 - what is the definition of "Cyber Security"? How does one know what does or doesn't relate if there is no defining criteria?18.4- what is the definition of "Cyber Security"? How does one know what does or doesn't relate if there is no defining

#	Organization	Yes or No	Question 35 Comment
			criteria?R19.This is a very difficult implementation. As a general comment, if the intent is to protect the BES, perhaps more effort spent on ensuring that no unauthorized machine can communicate with BES components is a better place to spend effort.
35.6	Emerson Process Management	Agree	For R16, keeping cyber systems current so that they can be supported with security patches is very essential in maintaining system security. This should be a requirement under R16 and provide a TFE opportunity if this can not be met immediately, but with a auditable mediation plan.
35.7	SCE&G	Agree	How does the SDT intend to account for equipment incapable of supporting certain requirement (e.g. malicious code)? Will the TFE process be utilized. If so, it would be helpful for entities to see where the SDT envisions initially allowing for TFEs.
35.8	Southern California Edison Company	Agree	SCE requests guidance on whether the list of requirements apply to each component or if they only apply at a system level. For instance, can testing and malicious code protection in R15.3 be performed at a system level or should each component demonstrate this capability?A separate standard with highly prescriptive methods to document situations where it is not technically possible to implement a certain control, controlled and auditable documentation of mitigation plans will enable registered entities to record instances of non-conformity.A prime example would be that R 17.1 may be impossible to implement because of the technical design for a particular device. While the standard allows or a mitigation plan, the draft does not indicate whether or not the lack of such capability is a case of strict compliance.
35.9	Nebraska Public Power District	Agree	Security protection for cyber components that cannot connect to an external network do not require the same level of protection as those cyber components with connectivity to an external network. I recommend adding an exclusion to R16 and R18 for cyber components that cannot be connected to an external network.
35.10	USACE - Omaha Anchor	Agree	This is a less strenuous requirement than previous version of CIP. Previously every

#	Organization	Yes or No	Question 35 Comment
			item in the ESP had to comply - requirement states every system must comply - implying not every item must comply as long as the system does.
35.11	Xcel Energy	Agree	While we agree overall, we do have some suggestions/requests for clarification1. R15 to R19 should allow for TFEs2. R18.4/R20.6 We do not agree with a need to review logs every 7 days.3. R19.1 Further definition is needed of the expectation to "Validate data". Our concern is if were to include RTU data that can not be validated. A TFE allowance may be needed in this case.
35.12	Independent Electricity System Operator	Disagree	- R15.1 define malicious code. For R15 and sub requirements, does malicious code mean AV or Spyware detection/prevention or does Malicious code require a code review when deploying code and patches to systems?- - R16.2 does not require that the mitigatio
35.13	National Grid	Disagree	1. Inconsistency in using "processes" versus "one or more processes" in all requirements. National Grid suggests using "one or more processes". 2. Recommend new wording for 15.2 similar to 26.2 -Respond to the detection of malicious code.3. Recommend new wording for 15.3 - Implement processes to test and update protections in place to respond to the detection of malicious code.4. Recommend using the controls for Low Impact BES CS too since once the code is propagated it spreads across network irrespective of low/medium/high BES CS.5. Recommend changing 16.1 from "release" to "availability". 6. Recommend removing "with a fixed date" from 16.2 because the cyber system may not be available for maintenance due to grid system conditions.7. Request a R17 local definition of "attack surface".8. 17.2 - recommend changing "externally accessible physical ports" to "externally accessible physical communication ports". Also please clarify external to what.9. Request a local definition of "security events".10. In 18.2, is the SDT considering providing the timeline for issuing alerts and also to respond to those alerts? 11. Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber Systems.12. Recommend that 18.4 be re-worded to be consistent with FERC Order P526 - "Some manual review of logs to improve automated detection settings, even if

#	Organization	Yes or No	Question 35 Comment
			alerts are employed on the logs."13. Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven days.14. Recommend that R19 should "insure the integrity of the data."15. Recommend that 19.1 should be "Entity should document process to insure the integrity of the data link between the BES Cyber System and the remote node." This new 19.1 should be "Required" for High Impact and Medium Impact BES Cyber Systems.16. Recommend that 19.2 should be "Where links cannot be secured, the Entity shall document the mitigation in use." This new 19.2 should be "Required" for High Impact and Medium Impact BES Cyber Systems.
35.14	Southwest Power Pool Regional Entity	Disagree	15.1: The criteria should "limit the introduction and propagation of malicious code." 15.3 should require such testing prior to implementation rather than assuming. The objective statements in R16 and R18 are prescribing a requirement through the use of the statement "to ensure." 16.1: Clarify who is "releasing" the security patch. For example, is it being released by the operating system vendor (e.g., Microsoft) or the third-party application vendor (e.g., the EMS/SCADA vendor) subsequently certifying the patch against the supported application? 16.2: Clarify that compensating measures must be implemented within a prescribed timeframe after determining a security patch to be applicable unless the patch is installed within that prescribed timeframe. If compensating measures are implemented as an interim measure, they must remain in place until the security patch is installed with the understanding that the compensating measures can be improved during the interim period. 17.1: The term "mitigation plan" has an enforcement connotation. Consider requiring the documentation and implementation of compensating measures instead. 17 overall: there are a number of additional system hardening techniques other than disabling logical and physical ports. Additional hardening should be required for High impact systems. See the baseline configurations found on the Center for Internet Security web site for additional information. 18.2: This requirement presumes 100 percent availability of the monitoring process, which is unreasonable for automated solutions. Additionally, prescribe a timeframe for issuing alerts for detected system events.

#	Organization	Yes or No	Question 35 Comment
			18.3: Consider rewording the criteria to read “Maintain logs of system events related to cyber security for the specified time period.” 18.4: The requirement to maintain records documenting the review of logs is a compliance evidence issue and should not be included in the requirement. 19.1: Questionable if this is an auditable requirement. Clarify what is intended by inbound data validation? 19.2: Encrypted data does not mean uncompromised / valid data. Is this requirement essentially the same as 19.1? Is this asking for the validation process to be external to the normal validation processes included in the application software running on the BES Cyber System? Is this an indirect requirement to implement “Secure ICCP?”
35.15	Regulatory Compliance	Disagree	15.3 - STRIKE "testing" from the criteria. There is very little bennefit to test signature. 16.1a - Need clarification on components not patchable.16.b for those devices that are patchable - assessment of patches within 30 days.16.2 - Clarification - assess whwther vulnerabilities exist for a device.17.2 - need definition of external connectivity - more guidance on physical switch ports18.4 - propose 30 days for 30 days for manual review of automated systems - it is redundantR19 - wait and see - need guidance
35.16	LADWP	Disagree	15.3 states to test and update malicious code protections. Testing the code protections should be removed.
35.17	Network & Security Technologies Inc	Disagree	16.1 - Please clarify meaning of “release” of security patches by specifying patch source (the corporation, organization, or individual that wrote it?). This matters because some application vendors combine O/S patches in “bundles” they release to customers with service contracts.17.2 - Given the restrictions on physical access and the requirements to train and background check personnel with unescorted physical access to BES Cyber Systems, this requirement seems unnecessary. Moreover, on any given day it may be very difficult to predict whether a given physical port might be of use in an emergency troubleshooting or restoration situation. Could be contentious during audits.R18 - Does the SDT intend that Responsible Entities be able to, if necessary, determine what user(s) was on what system and when? If so, this

#	Organization	Yes or No	Question 35 Comment
			requirement should be made explicit.19.1 - Please clarify types of “inbound” data this requirement applies to. Operational data only? Mirrored backup data received at a backup Control Center from a primary Control Center? An emergency “hot fix” from a SCADA/EMS vendor? Meaning of “validate” also needs to be clarified. SDT has solicited input on which proposed requirements should be “eligible” for TFEs - surely this is one. Depending on the intent of this requirement, “data validation” may be something that can only be done in a useful/meaningful way by application logic.19.2 - We consider this to be an unenforceable requirement and therefore suggest it be dropped unless compelling evidence exists that replay and/or MITM attacks are a real and growing problem. Investigating a single occurrence of invalid data could consume scores of person-hours, lengthy interactions with communication providers, other Responsible Entities (e.g., for a BA that operates a Control Center that receives all its data feeds from other companies), and even law enforcement with no guarantee of success. Cryptographic protection of in-transit data, even if achievable (probably not unless a Responsible Entity owns and/or controls both ends of the data feed), offers no protection against corruption of data at the source and could also cause latency issues.
35.18	ERCOT ISO	Disagree	16.1: Clarify “release” from whom--the product vendor (e.g., Microsoft) or other vendor that prohibits installation of a patch until certified with their applications?17.1: Compensating measures should be allowed in instances where a mitigation plan to achieve strict compliance is not possible. 18.2: Specify the timing for responding to alerts. 18.3: Should be removed to data retention section. 18.4: Should address the use of automated security event monitoring systems. TFEs should be allowed for R16. TFEs should be allowed for R17.TFEs should be allowed for R18.TFEs should be allowed for R19.
35.19	MidAmerican Energy Company	Disagree	16.2 - Define when the implementation schedule needs to be completed by and define how far in the future the installation can be scheduled. For example a patch is assessed within 30 days; the currently wording would allow me to develop an implementation schedule a year later and the schedule could call for the installation

#	Organization	Yes or No	Question 35 Comment
			to take place three years later. 17.2 Change to “Disable, render unusable or configure such that it has no access to a BES System” This would allow us to put ports into logical VLANS that do not have access to the BES Systems.19.1 What does “validate data” mean? This sounds like in would need to be an application level control. Is that what is intended?
35.20	PacifiCorp	Disagree	16.2 - Define when the implementation schedule needs to be completed by and define how far in the future the installation can be scheduled. For example a patch is assessed within 30 days; the currently wording would allow me to develop an implementation schedule a year later and the schedule could call for the installation to take place three years later. 17.2 Change to “Disable, render unusable or configure such that it has no access to a BES System” This would allow us to put ports into logical VLANS that do not have access to the BES Systems.19.1 What does “validate data” mean? This sounds like in would need to be an application level control. Is that what is intended?
35.21	ReliabilityFirst Staff	Disagree	16.2 - need a time frame (60 days), for row 17.1 does there need to be a time frame for implementation of a mitigation plan?
35.22	Luminant	Disagree	17.1 implement a mitigation plan or compensitory measures
35.23	Progress Energy - Nuclear Generation	Disagree	Agree with Table 15, R16.2, Table 17, 18.1 AND 18.2. R15-R19 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments. Durations for R16.1, R18.3, and R18.4 should align with comments in Attachment 1.
35.24	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.15.3 should include more clarification on what "testing" entails and whether that just refers to signature updates.Recommend replacement of the word "known" with "discovered" in R18. 18.4: more clarity

#	Organization	Yes or No	Question 35 Comment
			needed regarding the allowance of both automated and manual review of logs. R19 creates a potentially impossible level of obligation. Recommend striking.
35.25	American Transmission Company	Disagree	As written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings, requiring an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We believe this item should be deleted.As written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously.
35.26	MRO's NERC Standards Review Subcommittee	Disagree	As written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings, requiring an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We believe this item should be deleted.As written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously.
35.27	Western Area Power Administration	Disagree	Assuming one can detect and respond to the introduction of malicious code, how is it expected that we limit propagation of malicious code? By definition, malicious code is often not detected, and if it is detected (by virus prevention software, for instance), that software generally quarantines or deleted the malicious code automatically. This section seems to need a little thought as to what is really being required. This opens up technical interpretation of what "limits" malcode. This also assumes only a specific

#	Organization	Yes or No	Question 35 Comment
			vector (rootkit, malware, virus/worm) but doesn't address Denial of Service attacks which could be much more serious. Maybe they need to specify intent. R16: A plan for every patch as opposed to relying on the change control process? This seems excessive.R17: Seems to be an improvement. For 17.2, does this mean plug up physical ports like USB? This is unclear. If it does, cannot rely on physical perimeter for protection?R19: Since this applies only to external connectivity (ICCP connections or equivalent), how is it intended that we validate the actual data coming into the system? What level of validation? Ex: end-point validation (ipsec and certs) vs application endpoint (ssl), the way this is worded it goes WAY beyond this. This is not a communications validation issue. Are they wanting to get to MITM attacks? If so it isn't clear.
35.28	E.ON U.S.	Disagree	CIP-011, R15.1 Limiting propagation of malicious code is an integral part of any standard A/V protection. If this requirement is calling for something more than this then the requirement should be clarified to remove this ambiguity. If it is one and the same as R15.2, then E ON U.S. suggests combining these two sub-requirements.CIP-011, R17.2 The term "...externally accessible physical ports" is ambiguous. Does this refer any externally-facing port through which a party may attempt to gain unauthorized electronic access to a BES Cyber System Component? Or, does this refer to an externally-facing port directly on the BES CSC itself?CIP-011, R18.3 The requirement to maintain logs for one year is a significant burden. This can be a tremendous amount of data depending on the level of logging enabled.CIP-011, R18.4The expectations regarding review of logs should be more clearly defined. The whole point in having "continuous security monitoring for detected system events" is to avoid the extremely burdensome requirement of manually sifting through tremendous volumes of log data. Though some mechanism should be in place to ensure the automated logging and alert systems are not disabled, the requirement to manually review system logs is excessive and provides little if any security enhancement.CIP-011, R19.1The expectations for validation of data inbound to a BES Cyber System should be more clearly defined. How is this reasonable to be accomplished? Parameter checking is already a common mechanism within most

#	Organization	Yes or No	Question 35 Comment
			SCADA / DCS systems, but this does not protect against tampering or data manipulation within the prescribed bounds for a given data point.CIP-011, R19.2 Same comment as for R19.1...how is this to be accomplished?
35.29	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
35.30	The Empire District Electric Company	Disagree	Comments: As written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings, requiring an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We believe this item should be deleted.As written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously.
35.31	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy has the following concerns with requirements R15 - R19:R15 - A TFE may be required for programmable electronic devices within a substation environment where is not technically feasible to manage malicious code.R16.1 - The definition of a “release” needs to allow for vendor verification of the applicability of a patch to a given systems functionality before the thirty day clock begins.R17.2 - CenterPoint Energy recommends clarification as to what are considered "externally accessible physical ports" R18 - the phrase "related to cyber security" is ambiguous. R18.2 -implementing "continuous security monitoring that issue alerts for detected system events related to cyber security" would seem to require installation of external communications to remote substations increasing their vulnerability. R18.4 - A manual review every 7 calendar days is overly burdensome. Automated processes are already mandated to detect and alert personnel of cyber security events. CenterPoint Energy recommends a 30 day review.R19.1 - Concerned

#	Organization	Yes or No	Question 35 Comment
			with the method to "validate data inbound to a BES Cyber System". This requirement is intended to address data integrity issues associated with man-in-the-middle attacks, but it does not specifically address the issue. It leaves open the issue of data which was intentionally or unintentionally manipulated by responsible entities. The issue becomes something different if our Control Center must validate data from a Reliability Coordinator or Transmission Operator which has been intentionally or unintentionally modified by trusted personnel. Data integrity implies encryption. This requirement should state: “One or more of the following encryption standards are required to ensure data integrity inbound to the Control Center.R19.2 - Concerned with ability to provide evidence that we "evaluate invalid data inbound to a BES Cyber System" to determine whether the data has been compromised maliciously with current systems capability. As stated previously, this requirement does not address the issue of malicious entities entering malicious data from the endpoints. This requirement is an attempt to address issues associated with MITM attacks. Inherent in the various SCADA protocols is error detection and data delivery, but not data integrity. The ICCP protocol is encapsulated within TCP/IP. The TCP/IP protocol will ensure communication reliability and error detection, but it will not ensure data integrity.
35.32	Entergy	Disagree	Entergy suggests making requirements in general apply to high, medium, and low assets alike and provide a footnote to allow a TFE for assets which are not capable of meeting the requirements. 17.1 suggests that unused network ports only have to be disabled in the event there is external connectivity. This requirement appears to be extremely relaxed from version 1. The current language suggests that the perimeter firewall can be used to control port usage thus relieving the requirement to control at the asset itself. In 17.2 there is a reference to externally accessible physical network ports. Entergy suggests language change to just say “unused physical network ports.” In 18.2 there is a time requirement of maintaining logs for 1 year for high and 90 days for medium. Maintaining logs for 1 year can be problematic due to the amount of space required. Suggest making requirement for 90 days for high, medium and adding the same requirement for low assets. Also suggest adding a footnote to allow TFE for

#	Organization	Yes or No	Question 35 Comment
			assets that are unable to meet requirements. In R19 it appears the requirement is to encrypt all data coming into a BES Cyber System. The intent is to ensure data integrity. Most EMS systems have CRC checks, and reasonability checks, etc., embedded in the systems to validate the integrity of the data being received. Entergy does not believe that encryption is required for all digital data as it greatly increases overhead, operation and troubleshooting of the data networks. Entergy suggests that encryption should be required for remote access as remote access connectivity many times traverses the Internet or some non-private network links at some point. Entergy suggests providing alternate methods to validate inbound data rather than encryption.
35.33	Southern Company	Disagree	For 17.2, what does this mean? An externally accessible physical port would require a switch next to an open window or something.R15.3 requires testing of malicious code protections. This is an effort better left for malware protection suppliers. Often only the production system is available to the end user, the quantity and frequency of malware release prohibit an effective end user test program.R16.1 requires assessment of security patches within 30 days of release. This assessment is typically performed by control system supplier to assure that no adverse impact occurs to their product. Often only the production system is available to the end user. The end user has no control over vendor testing schedules. If this requirement is placed on the end user MS KB977165 type “blue screen” events may occur.R16.2 The requirement of a fixed date for patch installation may not be possible in all cases if a system restart is required for an operating unit.For R15 & R16, there is the potential that implementing malicious code detection and security patch management on substation devices could interfere with the primary function of these substation devices which is the reliable delivery of power.For R17.2, what will be considered acceptable for rendering physical ports unusable? We should not be required to permanently disable ports thereby making the ports unavailable for future use.For R18, not all BES Cyber System components in substations are capable of monitoring and logging system events.For R18, implementing security monitoring processes on substation devices may interfere with the primary function of these substations devices which is the reliable delivery of

#	Organization	Yes or No	Question 35 Comment
			power.R18.2 Clarify intention, is continuous monitoring with manual review of logged alerts acceptable? What is a "detected system event"? Is a single or double incorrect password attempt an alarmed event?R18.1 requires an automated log system R18.4 requires a review of log events. Is a manual review of all logs required in an automated system or just the alarms?
35.34	Detroit Edison	Disagree	In 15.2, "respond" is vague. Propose rephrase to read "Detect the introduction and mitigate the effects of malicious code."Remove table entry 19.1 since it is redundant to 19.2.The term "applicability" in 16.1 is vague. Consider introducing vulnerability severity classifications to patch management that determines the action and timetable required. Please note that this is submitted for consideration as a concept. The language and time tables will need further review and editing before this would be ready to add to the standard. o Level 4 - Intruders can easily gain control of a BES Cyber System Component, which can lead to the compromise of BES Cyber System security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the introduction of backdoors. High: patch within 7 days; Medium: patch within 14 days; Low: patch within 30 days. o Level 3 - Intruders can possibly gain control of a BES Cyber System Component, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host. High: patch within 14 days; Medium: patch within 30 days; Low: patch within 90 days. o Level 2 - Intruders may be able to gain access to specific information stored on a BES Cyber System Component, including security settings. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files, directory browsing, disclosure of filtering rules and security mechanisms, and unauthorized use of services. High: patch within 30 days; Medium: patch within 60 days; Low: patch during next system maintenance window. o Level 1 - Intruders may be able to collect sensitive information from a BES Cyber System Component, such as the precise version of software installed, open ports, services, etc. High: during next system maintenance window; Medium: during next

#	Organization	Yes or No	Question 35 Comment
			system maintenance window; Low: Patch during next system maintenance window.
35.35	RRI Energy	Disagree	In regards to 17.1, for clarification purposes, based on the definition of external connectivity written in the Standard, if a web server is actively listened on port 80 inside the BES boundary protection but is not accessible externally from the outside of the BES boundary protection, the Responsible Entity does not have to report and assess that port and service.In R17.2, what does externally accessible mean? Ex. Physical port is on a device that is in a cabinet, the cabinet is within a building, and the building is within a fence-lined property. Is the port non-accessible? What type of physical ports are we trying to protect? Is it only physical "network" ports? How about USB ports, PC (PCMCIA) Card slots, CD/DVD drives?Not all devices can be logged such as PLC's, meters, etc.; therefore 18.1 should allow for a TFE.In regards to R19, what defines an internal versus external boundary. Within a single facility, are all boundaries internal? If cables transverse hallways between "computer rooms" within a Control Center does an external connection exist? Can a back-up control center be an extension of a primary control center where all data connections between the control centers are considered "internal"?
35.36	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
35.37	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R16, but recommends changes as follows: o Regarding Part 16.2, this requirement contains no timeframe by which this schedule must be developed. If it was intended that the development of this schedule is to coincide with the activity described in Part 16.1, then that should be explicitly stated. Also, there is no limitation regarding how far in the future is reasonable to set the "fixed date." Minnesota Power recommends that if a timeframe for the "fixed date" is not established in the Standard then there should be a stipulation that if the date for installation of the patch is greater than a pre-determined amount (say 45 days), then mitigating measures need to be in place until the security patch is implemented.Minnesota Power generally agrees with the

#	Organization	Yes or No	Question 35 Comment
			proposed Requirements R17, but recommends changes as follows: o Regarding Part 17.1, the first sentence creates some confusion. Minnesota Power recommends that it be reworded as follows: “One or more processes to ensure that for each BES Cyber System Component, only those network accessible ports and services that are required for normal and emergency operations are enabled.” o For Part 17.2, is it the Standards Drafting Teams intent that a CD or DVD drive be considered an “externally accessible physical port?” If so, this should be explicitly defined. Logically, mounting a DVD is no different than plugging a memory stick into a USB port.Minnesota Power generally agrees with the proposed Requirements R18, but recommends changes as follows: o If it is the Standards Drafting Teams intent that Requirement R18 apply only to cyber security events, then Minnesota Power recommends that the term “security events,” which is used throughout this requirement, is reworded to state “cyber security events.” o Regarding Part 18.1, the Standards Drafting Team should consider clarifying the timeframe within which the monitoring of system events should occur (i.e., real-time, minutes, hours, days, etc.). If monitoring is done using a manual process, rather than an automated tool, real-time may not be possible, and guidelines should be established regarding how quickly events must be examined. o Is it the Standards Drafting Teams intent that Part 18.1 address the collection of security events into logs and Part 18.2 address the process to review and act upon the logs collected under Part 18.1? If so, the Standards Drafting Team should consider wording that would clarify the differences between these two Parts. o In Part 18.2, does the term “continuous” refer to “real-time?” If so, Minnesota Power recommends changing the term to real-time to avoid confusion. o Minnesota Power recommends rewording Part 18.3 as follows: "Retain logs of system events related to cyber security for the specified time period." o Minnesota Power recommends communicating all time frames in calendar days to eliminate confusion regarding what constitutes “1 year.” o Regarding Part 18.4, if 18.2 provides for “continuous” monitoring of system events for these same systems, why is it also required that a Registered Entity manually review these logs? In addition, can the Standards Drafting Team provide guidance regarding what should be included in this review? On an SEIM, for instance,

#	Organization	Yes or No	Question 35 Comment
			these logs can be enormous - to the point that manual review is not possible within reasonable time constraints.Minnesota Power generally agrees with the proposed Requirements R19, but recommends changes as follows: o Regarding Part 19.1, How, in real-time operation, can external data be validated (protocols already validate message structure)? For example, an LBA receives unit set-points from its ISO-BA via ICCP. If the data being received is within operating limits for that unit, it is "valid." The ISO may truly be requesting the unit to drop by xx MW. How is that differentiated from someone altering an inbound message to maliciously tell a unit to drop by the same xx MW value? The process for echoing values back to the external system does not solve this, since this, too, can be manipulated. o Part 19.2 appears to be a specific instance of Part 19.1 and given that this Part starts with the phrase "Where not cryptographically protected," it seems that Part 19.1 may be misstated. Is Part 19.1 supposed to discuss "protecting" inbound data, rather than "validating" it, via encryption, authentication, etc.? Also, in Part 19.2, what constitutes "invalid" data? Is this data which is outside of normal operating limits? Or maybe outside of reasonability limits? Again, maliciously inserting perfectly normal or valid data could have detrimental effects to the BES, whereas "invalid data" should, by default, be thrown out by normal processing.
35.38	Idaho Power Company	Disagree	Need to put a limit on how far out the fixed date should occur for implementation or mitigation of security patches. R18 refers to security events but the sub-requirements refer to system events related to cyber security. Need to make this clearer that the focus is on abnormal system events as a normal authorized log-in is a normal security event but not one that needs review or response.
35.39	NextEra Energy Corporate Compliance	Disagree	NextEra believes the current language did not provide clear guidance and is too lax which leaves room for interpretation. The following are the recommended updates for the requirements:15.1 - Implement technical, procedural and/or process controls to limit the impact of code which modifies or destroys data, steal data, allow unauthorized access Exploits or damage a system, and does something that user did not intend to do. o Implement technical controls, where technically feasible, to

#	Organization	Yes or No	Question 35 Comment
			detect and mitigate malicious code o Implement technical and/or procedural controls to limit the propagation of malicious code o Implement technical and/or process and procedural controls to respond to introduction of malicious code15.2 - Malicious code protections should be updated at least on a quarterly basis if applicable updates are available and technically feasible. Updates should be tested prior to implementation to ensure no adverse impact by the software updates.As far as the order of requirements, detection should come first and it should be a requirement by itself. Combined 15.1 and 15.2 and removed 15.3 from the initial version.NextEra believes the implementation of processes incorporating the criteria specified in CIP-011-1 Table R16 - Security Patch Management in order to ensure that security vulnerabilities in BES Cyber Systems are mitigated was not clearly identifiedThe current language did not provide clear guidance and left room for interpretation. The following are the recommended updates for the requirement: 16.1 - The Responsible Entity shall establish a security patch management assessment program to track, evaluate, and test cyber security patches within 30 calendar days of their release to validate their applicability to its BES Cyber Systems.16.2 - The Responsible Entity shall develop an implementation schedule with a fixed date for either installation of the applicable security patches or the completion of mitigating measures that address the vulnerability if application of the security patch is not technically feasible.It should be stated that there needs to be a program to track, evaluate, and test cyber security patches within the defined timeframe that are applicable to the BES Cyber System.It is also recommended that there is more in depth guidance on the implementation schedule.CIP-011-1/R17Did not account for technical feasibility for disabling of ports.The following are the recommended updates to the requirements:17.1 - Implementation of process (es) to ensure that only those network accessible ports and services required for normal and emergency operations are enabled. In cases where unused network accessible ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document and implement compensating measures to mitigate the risk of exposure.If it is not technically feasible, the entity must have documented compensating measures to mitigate the

#	Organization	Yes or No	Question 35 Comment
			risk of exposure. This requirement should be applied to Medium and High BES Cyber Systems.The CIP CIP-011-1 Table R18 - Security Event Monitoring to ensure that security events are known, logged, and responded to on BES Cyber Systems did not provide enough guidance.The current language did not provide clear guidance and left room for interpretation. The following are the recommended updates: 18.1 - Implement automated tools or organizational processes to monitor and log system events that are related to cyber security for all BES Cyber System components, where technical feasible. Instances, that are not technical feasible the Responsible Entity shall implement manual processes to mitigate risk exposure.18.2 - Implement and document security processes for continuous (24/7 365 days, except when conducting system maintenance of the monitoring devices) security monitoring that issue alerts for detected system events related to cyber security.18.3 - Maintain system logs of system events where technical feasible, related to cyber security within the specified time period. If not technically feasible, the Responsible Entity shall document and implement manual processes to mitigate risk exposure.18.4 - The Responsible Entity shall verify that the log and alerting system is working in the time intervals mentioned. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs within 90 daysAdded language provides more definition.The CIP-011-1 Table R19 - Communications and Data Integrity to protect the real-time operation of the BES from the use of maliciously modified data by BES Cyber Systems did not provide enough guidance.The current language did not provide clear guidance and left room for interpretation. The following are the recommended updates:19.1 - Validate data inbound in the Control Center for specific connections and verify if those are the correct connections. 19.2 - Where not cryptographically protected, develop and implement a process to evaluate invalid data inbound to the BES Cyber System in a Control center to determine whether the data has been compromised. All unauthorized access attempts to a control center must be identified and investigated.Added language provides more definition.Also, In 15.1, please clarify the term "limit propagation". How would a Responsibility Entitity demonstrate the compliance to 15.1? Is a documented

#	Organization	Yes or No	Question 35 Comment
			technical or procedural control to limit the propagartion of malicious code sufficient? Furthermore, NextEra asks that examples be provided on how to meet this requirement at BES Transmission Facilities where all BES Cyber System Components are not capable of running anti-virus software.In 16.1, is the assessment necessary when regular patch cycle or planned installation is under 30 calendar days?In 16.2, what is a reasonable "implementation schedule with a fixed date for either installation of the applicable security patches or completion of mitigating measures that address the vulnerability"In 16.2, is an implementation schedule necessary when regular patch cycle or planned installation is under 30 calendar days?In 16.2, if the "installation of the applicable security patches" would cause a risk on the availability and performance of BES Cyber System, is it sufficient to complete the mitigation measures that address the vulnerability? If so, we propose that the language of 16.2 be modified to have this as an option in lieu of the installation of the applicable security patchesIn 17.1, does this apply only to BES Cyber System Components that are accessible from the outside? If yes, does this apply only to the ports that are externally connected or for all ports if the BES Cyber system Component has external connectivity?In 18.4, please clarify the term "review logs of system events" -- how will compliance be demonstrated?In 19.1, how do we validate data inbound to a BES Cyber System in a Control Center? Please provide methods that could be employed by the Responsible Entity. Could 19.1 and 19.2 be simplifeid by jjust requiring cryptographic protection for High Impact BES Cyber System in a Control Center?Regarding R-18, the log review of assets is too short. (i.e. 30 / 7 days). With this constraint, there will be limited knowledgeable personnel available for review. Some systems do not provide data to allow for this type of analysis. Need support from external vendors, which may not be feasible on a weekly / monthly basis. Due to volume in the industry, it is anticipated that vendor resources will be limited to support us in this capacity. NextEra suggests at least quarterly for Medium / High.18.1 states logging events "related to cyber security". This is subject to broad interpretation and should be clarified. NextEra suggest providing specific examples, such as: Abnormal System Shutdown Account Lockouts Admin User Account Changes

#	Organization	Yes or No	Question 35 Comment
			All Domain Account Logon Failures All Group Account Changes All User Account Changes All Policy Changes Domain Admin Acct Logon Failures Domain Admins-Admin Group Acct ChgDomain Admins-Admin Group ChgDomain Trust Rel Policy ChangesEvent Log FullLogon Logoff SummaryNormal System Startup-ShutdownPassword Changes and ResetsSecurity Log ResetsSrv Wkst All Logon FailuresTerm Srv All Logon Logoff SuccessesTerm Srv All Session Discon-ReconUser Account Creation or DeletionUser Account Password ChangesUser Rights Policy Changes18.2 uses the term "issue alerts" which could imply alarming or otherwise performing a notification. If NextEra had to raise an alert for every system event we could potentially have a continuous alarm stream. If it is determined that event alarms are necessary, then the events have to be further defined and our systems have to be specifically tuned on site for the real running environment.NextEra recommends defining the term further to either include explicit alarm/notification or not. Would also push further for alert in the form of logging to be reviewed or alarmed for review.19.1 states validate data inbound to a control center. Data should be further classified as data directly related to real-time BES operation. If a Monitoring and Diagnostics Center is classified a control center they would potentially have to perform data validation on all historical data made available to that center, depending on interpretation. An alternative is to further classify or define "validate" to allow validation simply by verification of traffic from a reliable source, i.e. identifying the source historical data server.NextEra proposes considering validation of the originating source rather than validating the data itself.
35.40	Con Edison of New York	Disagree	o R16.2 requires a “fixed date” for apply security patches or mitigation. This requirement does not take into consideration that entities may require vendors to test the patches on their systems before they will be applied to operational systems. The release dates for these patches is not fixed by the vendor. The requirement should allow for the planned install date to be a fixed period after the patch is tested and available to the user. A fixed date may be a challenge when predicated on manufacturer certification which may introduce unnecessary risks to operations. o R17.1 “external connectivity” is expected to mean external to the (ESP) boundary. o

#	Organization	Yes or No	Question 35 Comment
			R17.2 It is not clear what externally accessible physical ports includes. External to the location or external to the device (i.e.: located on the front of the workstations) o R18.2 - need clarification on type of events that need continuous monitoring; security logs can be voluminous with excessive informational notifications o R18.4 - if automated tools are used this should not be required o R19 - need more info on ensuring data integrity. What does "external" mean? Does this require special checks of RTU inbound data? Unclear what will be considered validation. Is Encryption validation? If the RTU data is not encrypted is the EMS validation of data sufficient? If the systems (especially legacy equipment) do not support integrity checks the addition or development may not be possible or recommended. Will this require a TFE?
35.41	Puget Sound Energy	Disagree	Puget Sound Energy has the following comments:R15.1 - Puget Sound Energy feels that "Limit propagation..." is an abstract term and needs clarity to it in order for NERC to be able to consistently validate compliance.R15.3 - Puget Sound Energy suggests clarity to what type of testing is required of malicious code protections. Is NERC requiring functional testing that the malicious code protections are reliably functioning or security testing (penetration testing)?R17.1 - Puget Sound Energy would like clarity into the degree of documentation required to validate compliance with "...required for normal and emergency operations are enabled." Puget Sound Energy would also like clarity into NERC's definition of "enabled" and "disabled". For example, can network accessible ports be "enabled" and "disabled" through the use of host based firewalls?R17.2 - Puget Sound Energy suggests that the disabling of physical ports on BES Cyber System Components only be required where physical security protections are not required, as outlined in Table 5. If physical security is provided, per Table 5, then the disabling of physical ports seems unnecessarily redundant. Puget Sound Energy would like clarity on "externally accessible physical ports", in cases where the BES Cyber System Component is physically protected by measures outlined in Table 5.Table 18 - Puget Sound Energy suggests including "Where Technically Feasible" to R18, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 18. For example, entities may incorporate

#	Organization	Yes or No	Question 35 Comment
			dialup accessible devices that, by the nature of a connection that is built up and torn down as necessary, is incapable of providing “continuous security monitoring that issues alerts”.R19.1 - Puget Sound Energy requests clarity into what NERC means by “validate data inbound”. “Validate” is subjective and Puget Sound Energy would like clarity on how entities can prove compliance. Puget Sound Energy would also like clarity into the scope of the inbound data it must validate. For example, is NERC asking for validation of interconnections with other utilities and balancing authorities or validation of every RTU that provides an inbound data stream to a control center’s BES Cyber System?
35.42	BCTC	Disagree	R15 - Â Change title to “Prevent Malicious Code”Â 15.1 - suggest replacing the words “Limit propagation” to “Prevention”Â 15.3 - we do not agree with this requirement. Recommend removal of the words “to test”. It is not a good practice to introduce malicious code into a BES Cyber System - even in QA!Â Another potential area for TFEsR16 - Â R 16.2: if the patch results in a system upgrade it could take up to 6 months to implement the patches; if the patch does not result is a system upgrade then recommend allowing 30 days to implement said patchesR17 - Â The requirements needs to provide more guidance on how to provide evidence for open/ closed TCP (static) versus UDP (dynamic) ports Â R 17.1 Guideline would be appreciated on how to meet this requirement. We have struggled with this one in the past.Â Provide a definition of what is “system hardening” R 17.2 - what is the objective of this requirement? We feel that simply disabling a physical report does not provide much value from a security perspective (i.e. can unplug an active port and plug in an unapproved device); instead we recommend locking down devices’ MAC addresses as this would result in a more secure environmentR18 - Â R18.3. A year seems excessive to require an entity to retain ALL logs. What is the objective in requiring utilities to do this?R18.4. Suggest breaking this one in to two requirements - one for log review and the other for maintaining records - current wording can be interpreted as having to retain events for medium impact systems for a longer period than high impact? R19 - Â R19.1. We request a definition of what is meant by “validation” as well as guidance on how to perform this taskÂ Potential area for TFEsÂ

#	Organization	Yes or No	Question 35 Comment
			R19.2. We are struggling with how to comply with this requirement. We have an IDS implemented in our environment where users are alerted on suspect packets - is this what this is referring to? Intent not clear with the current wording.
35.43	WECC	Disagree	R15 - alright with all criteria, R16 - alright with all criteria, R17 - Item 17.1 should cover local ports and services not just network ports and services. Consider removing the words "network accessible" like text in previous standards and make required for Medium and High impact levels. Physical ports should be rendered unavailable on components of Medium impact systems as well as High. Item 18.2 needs to define "continuous" or remove it from the criteria. R17 - Consider adding more criteria for system hardening including system base-lining or move system base-lining from the change management section to here. Look for other overlap between R17 and change management. R19 - agree with criteria but would suggest adding the following after validate data "(eg. syntax checking, bounds checking, sanity checking, etc)"There needs to be more language specifying a definition of malicious code, what it means to limit its propagation, and to detect and respond to its introduction. As written, there is very little to audit against in this requirement.Additional language is needed to describe what it means for a patch to be released.System hardening should be required for all systems, not just those that are externally connected.Additional language is needed to clarify the requirements for security event monitoring, for example, what continuous monitoring means.Log review intervals are too long to be effective.The data integrity criteria are good additions but need additional language to clarify the intent. What does it mean to validate inbound data? Also, consideration should be given to the fact that cryptographic protection is not fully effective in all circumstances. More direction is needed as to when cryptography is an acceptable control. Also there are no requirements in the standard that define criteria for cryptographic controls.
35.44	Alberta Electric System Operator	Disagree	R15 - Change requirement to include confidentiality, to address potential MITM or MITB attacks. "...malicious software that could affect availability, integrity, or confidentiality of the..."Table R16 - include additional row similar to 16.1, but to

#	Organization	Yes or No	Question 35 Comment
			assess security patches within 60 days. Make this a requirement for Low Impact BES Cyber Systems. All BES Cyber Systems should be assessed, however High and Medium Impact systems should be assessed sooner.Table R19 - 19.1 states "Validate data inbound to a BES Cyber System in a Control Center." And the corresponding impact states "Required for external connectivity only." Based on the definitions, "inbound to a BES Cyber System" can only be from a device "external to the BES Cyber System" so the impact is redundant. Similar situation for 19.2. Suggest changing "Required for external connectivity only" to "Required". Table R19 - consider adding additional rows to Table R19 to address validating inbound data to BES Cyber Systems that are not in a control centre. 19.1 Validate data inbound to a BES Cyber System in a Control Center. Required for Medium and High 19.2 Validate data inbound to a BES Cyber System. Required for High19.3 Where not cryptographically protected, develop and implement a process to evaluate invalid data inbound to a BES Cyber System in a Control Center to determine whether the data has been compromised maliciously. Required for Medium and High19.4 Where not cryptographically protected, develop and implement a process to evaluate invalid data inbound to a BES Cyber System to determine whether the data has been compromised maliciously. Required for High.
35.45	LCEC	Disagree	R15 - Testing for malicious code protection is not auditable.R16 - Device end of life support issues need to be addressed. Release needs to be clarified to address the situation where a vendor may release a security patch for a BES Cyber System Component but it is not yet approved by the BES Cyber System vendor.R17 - o It is not often clear whether the standard is referring to logical and physical ports. Physical, logical or both should be specified any time the term port is used.R18 - What constitutes a security event?Is the 90 day requirement meant to be an absolute 90 days as opposed to 3 years and 90 days to be able to show compliance?R19 - How would one validate inbound data? Was this clearly meant to be data integrity as opposed to data protection? Why was this scope chosen?
35.46	Dominion Resources	Disagree	R15 - The stated intentions of the SDT at the May Workshop were to reduce TFEs and to distinguish between Control Centers vs. Substations and Power Stations. Neither

#	Organization	Yes or No	Question 35 Comment
	Services, Inc.		of these stated goals is presented in R15. TFEs will be required for 15.2 and 15.3 and there is nothing indicating that these should not apply to field equipment or network equipment (e.g., firewalls, routers, switches). Dominion agrees with the stated intentions of the SDT team.To avoid the potential for TFE's associated with R15.2 and R15.3, a footnote similar to the one used for Table R10 on Page 11 of CIP-011 should be added. Also, access controls related to access points would be better addressed in the Boundary Controls Section of CIP-011.R16.2. The word "fixed" should be replaced with "planned" to allow some flexibility for installing the patch. 17.2. It should be clarified that an alternative where the equipment does not provide a configurable method of disabling the port is that methods, such as using security tape, to indicate any tampering with the port may be used.18.2. This section will require a TFE since many devices do not have the capability of issuing alerts. A footnote to avoid need for a TFE should be added.18.3. One year is too long to maintain logs for network devices. Storage space is at a premium. There will be a substantial increase in cost to increase storage space for each high impact cyber system This should be changed back to 90 days for High Impact cyber systems. 18.4. Logs of system events should only be required to be reviewed every 90 days. Logs should be reviewed only when an alert is issued for a detected system event. Routine reviews would take an extraordinary amount of time with no expected substantial results. R19. Common methods for ensuring data integrity include physical protection of the asset, authentication and authorization of data sources/inputs, using data validation and error checking rules at the application or database level, and a variety of other technical, operational and management controls. Dominion recommends the wording used in R19.1 be modified as follows to state the objective without specifying how it should be accomplished since the methods vary depending on the nature of the system and the technology in use:"19.1 Implement methods to maintain the integrity of data inputs to a BES Cyber System in a Control Center. " 19.2. It is sometimes impossible to determine if data has been compromised. Dominion understands that the proposed re-wording for 19.1 will also suffice to meet the requirements for 19.2 and recommends that 19.2 be removed.

#	Organization	Yes or No	Question 35 Comment
35.47	FirstEnergy Corporation	Disagree	R15 - We prefer the new text over the old CIP standards and it would reduce TFEs. In R15/Table 15: need some type of exception for devices incapable of running anti-malware.R16 - We prefer the new text over the old CIP standards. R17 - We prefer the new text over the old CIP standards.R17/Table 17: Need clarity on "externally accessible and physical ports". Does that mean serial, parallel, USB, Fireware, etc. or ports that are capable of transmitting routable protocols (e.g. network interface cards).R18 - 18.4 - Need greater clarity around whether automated alarming can be used rather than manual review of system event logs. Also - should it be specified somewhere in R18 that these sub-requirements apply to electronic security only, not physical security events (which is spelled out in R6)? 18.2 - We question the use of the word 'continuous' in this sub-requirement as this would be difficult for those entities that use 'organizational processes' to monitor and log.R19 - Overall this requirement appears to be too broadly worded. 19.1 - The use of the word 'validate' seems vague. Is the intent of the SDT that entities provide the specifics on what 'validate' means - e.g. the appropriate data or a point-for-point comparison, how often, etc? 19.2 - Many existing systems do not provide a means to accomplish compliance with this sub-requirement - for example, legacy RTU protocols. R19/Table 19: Need clarity on "invalid data". How do you evaluate invalid data?
35.48	US Army Corps of Engineers, Omaha Distirc	Disagree	R15 needs to be limited to general processing equipment. Requirement for anti-virus type software on all systems will numerous TFE's. R18 logging of all BES Cyber System components will generate numerous TFE's. R19 concerned about what realistic measures are available to meet requirements.
35.49	US Bureau of Reclamation	Disagree	R15.3 - If it is truly intended that entities test malicious code protections (not just ensure signatures are up to date and that protection software is running, the Standard should provide some additional guidance. Few entities are going to be willing to introduce malicious code, even into a test system, to verify malicuious code protection. Further, there is not timeline for when the malicious code protection must be tested. It would not be unreasonable to require and annual test of the

#	Organization	Yes or No	Question 35 Comment
			malicous code protections. The malicious code protections should be an intelligent requirement. Some devices that are not addressable may not need malicious code protection. R16.2 - Suggest the phrase "if the patch will not be installed" be added to the end of the requirement. R17.2 - Is locking within an enclosure satifactory? R18.3 - Suggest medium impact requirement be "for at least 90 calendar days" and that high impact timeframe be considered for reduction, perhaps to at least 180 calendar days.R19.1 - Explain how this is to be accomplished within the Standard - based on some specific criteria. This requirement is too open-ended. Since the concept of BES Cyber Systems now includes such devices as programmable multifunction or solid state relays, the requirement to "validate data" inbound makes no sense. Many of these devices reside within a control center. The definition now includes those center which are used to control more than one BES generator. The data going into the relays is from transducers either inside or outside the physical security perimeter but within another physical security perimeter. This data may be digital or analog. How would it be validated, cryptographically progracted or analyzed for malicious compromise?It is not clear how an "interactive user" session would apply to "programmable" relays.
35.50	Ameren	Disagree	R16.1 - This requirement should address documenting the installation date of patches and that patches have been installed.R18 - should only apply to network based systems with external connections only; currently this required is not limited on what it applies to.R19.1 and R19.2 - There is no way to comply with this standard without requiring the vendors to write better code. Suggest removing these requirements.
35.51	Northeast Utilities	Disagree	R17 appears to be significantly weaker than the previous standards. It also does not appear to align with the draft change control standards. Ports and services are a strong control to ensure only services required for operation are allowed. At minimum the High Impact BES Cyber systems should be “Required”.R19 needs more explanation. What does validate data mean?

#	Organization	Yes or No	Question 35 Comment
35.52	Hydro One	Disagree	Recommend new wording for 15.2 - Respond to the detection of malicious code.Requirement 15.3 implies that testing ensures that the deployment will not adversely impact security. However, the existing words could be interpreted as testing the malicious code prevention by introducing malicious code.Recommend changing 16.1 from “release” to “availability”.Recommend removing “with a fixed date” from 16.2. The cyber system may not be available for maintenance due to grid system conditions.Request a R17 local definition of “attack surface”.Recommend changing 17.2 from “Disable, or render unusable, externally accessible physical ports” to “Disable or secure externally accessible physical communications ports”.Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber Systems.Requirement 18.4 seems to have one purpose and that is to prove 18.2. To us this seems redundant since R18.2 require alert for system events. Why do we need a review at some later point? We recommend removing the requirements R18.4 Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommend that R19 should “ensure the integrity of the data”.Recommend that 19.1 should read “Entity should document process to ensure the integrity of the data link between the BES Cyber System and the remote node.” This new 19.1 should be “Required” for High Impact and Medium Impact BES Cyber Systems.Recommend that 19.2 should read “Where links cannot be secured, the Entity shall document the mitigation in use.” This new 19.2 should be “Required” for High Impact and Medium Impact BES Cyber Systems.Please clarify the applicability of R19. Does this requirement apply only to code releases into the system or it applies only to external data streams (e.g. weather data from a service provider, data from RTUs etc)?
35.53	ISO New England Inc	Disagree	Recommend new wording for 15.2 - Respond to the detection of malicious codeBelieve the SDT meant that 15.3 testing insures that the deployment will not adversely impact security. However the existing words could be interpreted as testing the malicious code prevention by introducing malicious code.Recommend changing

#	Organization	Yes or No	Question 35 Comment
			16.1 from “release” to “availability”Recommend removing “with a fixed date” from 16.2 because the cyber system may not be available for maintenance due to grid system conditions, implement based on your documented patch process. Request a R17 local definition of “attack surface”Recommend changing 17.2 from <<Disable, or render unusable, externally accessible physical ports>> to <<Disable or secure externally accessible physical communications ports>>Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber SystemsR18.3 Some automated tools do not have separate log retention based on the asset. The log retention applies to all assets. It is unclear if the log retention is the actual log from each Cyber System component or the log that an automated tool keeps (ie parsed out info from syslog). Either way a years worth of logs will require terrabytes upon terrabytes of storage for useless information. Recommend that 18.4 be re-worded to be consistent with FERC Order P526 - <<Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs. >>Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven daysRecommend that R19 should “insure the integrity of the data.”Recommend that 19.1 should be “Entity should document process to insure the integrity of the data link between the BES Cyber System and the remote node.” This new 19.1 should be “Required” for High Impact and Medium Impact BES Cyber Systems.Recommend that 19.2 should be “Where links cannot be secured, the Entity shall document the mitigation in use.” This new 19.2 should be “Required” for High Impact and Medium Impact BES Cyber Systems.
35.54	Northeast Power Coordinating Council	Disagree	Recommend new wording for 15.2 - Respond to the detection of malicious code.Requirement 15.3 implies that testing ensures that the deployment will not adversely impact security. However, the existing words could be interpreted as testing the malicious code prevention by introducing malicious code.Recommend changing 16.1 from “release” to “availability”.Recommend removing “with a fixed date” from 16.2. The cyber system may not be available for maintenance due to grid system conditions.Request a R17 local definition of “attack surface”.Recommend changing

#	Organization	Yes or No	Question 35 Comment
			17.2 from “Disable, or render unusable, externally accessible physical ports” to “Disable or secure externally accessible physical communications ports”.Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber Systems.Recommend that 18.4 be re-worded to be consistent with FERC Order 706 paragraph 526 - “Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs.”Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommend that R19 should “ensure the integrity of the data”.Recommend that 19.1 should read “Entity should document process to ensure the integrity of the data link between the BES Cyber System and the remote node.” This new 19.1 should be “Required” for High Impact and Medium Impact BES Cyber Systems.Recommend that 19.2 should read “Where links cannot be secured, the Entity shall document the mitigation in use.” This new 19.2 should be “Required” for High Impact and Medium Impact BES Cyber Systems.
35.55	USACE HQ	Disagree	Requirement 15.1 should be deleted from the list. Limiting the propagation of malicious code is a logical step in the “respond to the introduction of malicious code” phase, process which is required in 15.2. Therefore 15.1 present a possible double jeopardy since it is logical to think that when responding to the introduction of malicious code in the environment the steps will include limiting the propagation of the same before removing it from the system. Also, requirement 15.1 language is to broad in the interpretation of it. “Limit propagation of malicious code” implies that the code has moved through some part of the system, therefore the question is, how much movement of the code is acceptable when creating a response process?. The acceptable answer to this question could depend on the auditor’s subjective views of what is acceptable safe propagation of the code inside the system.
35.56	Garland Power and Light	Disagree	Requirement 16.1 - Reword requirement to say assess within 60 days - reason is because we feel it is adequate to check the vendor web site every 30 days and allow 30 days for testing and determination of implementationRequirement 18 - Reword

#	Organization	Yes or No	Question 35 Comment
			requirement to allow for Responsible Entity to develop a definition of a "system security event". The words are used in the main requirement and each subrequirement. Requirement 19 - o Delete Requirement R19 - Control systems currently validates data for quality and limits and then tags the data with any issues so that downstream applications can handle appropriately. This is sufficient for the security and reliability of the BES. R19 is impractical for implementation in the field for large or small utilities. This will reduce reliability of the overall system.
35.57	Oncor Electric Delivery LLC	Disagree	Requirements 15.1 and 15.3 are not necessary. The use of antivirus and malware software is problematic on some systems, while "whitelisting" requires additional hardware which may contain its own vulnerabilities. Detection and response should be sufficient. Many programmable devices are not capable of propagating malicious code or running prevention software.Requirement 18.2 does not apply to many legacy cyber systems and should only be applicable to systems which utilize routable communications.
35.58	Manitoba Hydro	Disagree	Revise the wording of Requirement R15 to "... integrity of the BES Cyber Systems." Please clarify the intent of "test and update malicious code protections". Requirement R16.2 should be revised to indicate the development AND implementation of the schedule. The wording of Requirement 16.2 currently does not require the application of mitigating measures prior to the installation of the applicable patch, and may need to be revised. For Requirement R17, please what is the meaning of "network accessible ports", and "externally accessible physical ports". Are physical ports enclosed within an unlocked cabinet "externally accessible ports"? Are physical ports within a non-public space, "externally accessible ports"? Requirement R18 does not contain any requirement for response to security event alerts or monitoring. Remove the word "maliciously from Requirement R19.2. It may be very difficult to determine if the data compromise was malicious or not. There are no specifics given with respect to "limit" propagation in Requirement R15.1. It is assumed to be at the Responsible Entity's discretion in terms of criteria, means, etc. There are no specifics given with respect to "validate" data in Requirement R19.1 so it is assumed to be at the

#	Organization	Yes or No	Question 35 Comment
			Responsible Entity's discretion in terms of criteria, means, etc.
35.59	San Diego Gas and Electric Co.	Disagree	SDG&E thinks that R17.2 sounds good in theory (disabling external physical ports on assets), but in practice this can be difficult to achieve without damaging the port for future legitimate use. Many shops use epoxy or other glue-based products to physically disable / protect such ports, and these solutions tend to be permanent. If we are physically protecting the asset from access anyway with card readers and other physical means, why is it necessary to take this redundant step of sealing physical ports on assets when only people with authorized physical access (who have had training) can actually access the asset?SDG&E has concerns about the viability of complying with R19.1 (validating inbound data to a BES Cyber System in a control center) in a situation where the incoming data is encrypted. How does the SDT define "validate"? Where does the validation need to occur?SDG&E also has concerns about the viability of complying with R19.2 (evaluate invalid data for malicious compromise) without MUCH additional vendor support. How does the SDT define "evaluate invalid data"?
35.60	Platte River Power Authority	Disagree	Suggested Revision (clarify what to test):15.3 Implement processes to update malicious code protections including testing security controls
35.61	Duke Energy	Disagree	Table 15: will need a TFEWithin generation, we have differing opinions on the definition of code. Suggest clarifying that it does not include programming code.Requirement 16.1: Assessment of security patches within 30 calendar days of their release for applicability to its BES Cyber Systems. Release from whom? It makes a big difference if the patch is released from Microsoft, for example, or the patch is released from the control system vendor (e.g. Emerson, Invensys, Areva, etc.) as to how/if the patch is implemented to prevent risk to the BES cyber system.Table 17: for devices inside a locked cabinet, are the physical ports on that device externally accessible?Requirement 17.2: how does the definition of "externally" in "externally accessible physical ports" compare with the definition of external in "external connectivity" in R3? Also, this definition implies that there are physical ports that are

#	Organization	Yes or No	Question 35 Comment
			NOT “externally accessible”. Need to make definition more clear. Suggest taking out reference to “externally accessible”.Table 18: 18.1 - not all devices are capable of logging, need a TFE18.2 - it would be helpful to have a definition of ‘events related to cyber security’18.4 - remove for systems where automated tools are in place. Requirement 18.2: " one or more security processes for continuous security monitoring" - is there any interpretation of the expectation here so that we don't have disagreement at audit? Are alternate controls allowed for BES Cyber Components that don't support logging/monitoring (example: manual review of physical access logs for stand-alone equipment)?Table19:Item 19.1 & 19.2 Additional explanation is needed to explain acceptable threshold for “validation of inbound data.”Clarify validate in 19.1. Is encryption a form of validation?What is meant by Data in 19.1?Requirement 19.1: What types of data validation controls are acceptable to meet this requirement? For example, control totals, presence check etc. Requirement 19.2: Need to provide an example with what methods can invalid data be evaluated to conclude that the data has been compromised maliciously?
35.62	Consultant	Disagree	Table R15 - Item 15.3 The requirement to "Implement processes to test and update malicious code protections." is confusing. Is the intent to "test malicious code protections and update malicious code protections" or to "test updates to malicious code protections" Please clarify the intent. There is a need to distinguish between updates to the malicious code protection "software" and malicious code protection "signature files". The software should be implemented in accordance with change control processes. The "signature files" are a specific subset of update to malicious code protection where it is unlikely a registered entity would have the capability to test what are typically vendor proprietary file formats. The extent of the 'testing' necessary for these signature files should be clarified.Table R16 - Item 16.2 While the concept of a "fixed date" sounds good, the requirement should allow for reasonable scheduling, including rescheduling, of the installation of applicable security patches or completion of mitigating measures. An option could be to remove the words "with a fixed date" and add a new item that would require that "Events that delay a security patch implementation schedule greater than thirty days shall be documented."Table

#	Organization	Yes or No	Question 35 Comment
			R17 Item 17.1 The first sentence uses the terminology "network accessible ports and services" and the second sentence uses the terminology "network accessible services and communication methods". Suggest using consistent terminology to avoid confusion.Suggest defining the term "network accessible ports and services" (may be multiple terms) as they are intended for use in the standards. There does not appear to be a standardized definition for this term in the industry. The term "network accessible ports and services" appears to imply access across the protection boundary? If it does then the requirement statement of "Required for external connectivity only" is unnecessary and should be changed to "Required".Table R18 - Item 18.3 Suggest changing the word "within" to the word "for" for clarity of meaning.Item 18.4 - Weekly log review appears to create an excessive administrative burden without a corresponding decrease in risk to the High Impact assets. Items 18.1 and 18.2 require continuous monitoring of the same activity. Manual log review is redundant to these requirements. While there may be a reason for manual log review to confirm the continuous monitoring is occurring as expected a more reasonable periodicity of monthly or quarterly should be required for both Medium and High Impact assets.Table R19 - The limitation of these items to a Control Center is an added dimension of Impact that is not included in the impact categorization criteria. If data is an issue, then these requirement should apply to all assets based on impact categorization without addendum or modification by the requirement. Suggest modifying the impact categorization criteria to clearly identify those assets.Table R19 - "Inbound data" implies remote access, and the terminology "Required for external connectivity only" is redundant. Suggest changing the wording to "Required".Items 19.1 and 19.2 are inconsistent. Item 19.1 requires validation of inbound data, and item 19.2 provides an exception to validation for encrypted data. If you comply with item 19.1, then item 19.2 is irrelevant. If you comply with item 19.2, then you are in violation of item 19.1.R19 - Overall, this requirement should be removed in it's current form. Automatic system operation cannot exist if "inbound data" is required to be validated. Automatic system operation is dependent on responses to external data inputs. If the intent is to return the BES to manual operation, this requirement

#	Organization	Yes or No	Question 35 Comment
			will achieve that end.
35.63	American Electric Power	Disagree	Table R15: 15.1, regarding "Limit propagation of malicious code", suggest replacing "propagation of" with "propagation and introduction of".15.2, regarding "Detect and respond to the introduction of malicious code." Would this be covered in a traditional cyber security incident response program? This should already be covered in R27.Table R16:16.1: Regarding the word "release" within "Assessment of security patches within 30 calendar days of their release for applicability to its BES Cyber Systems." Release from who? For example, is it the release of a new patch by Microsoft, or is it the certification of the patch by the control system vendor that the patch does not negatively impact the control system? Further clarification is needed. Patches released by Microsoft are not typically tested for several days or weeks by Control System vendors to validate that the patch does not impact functionality. Industry cannot test software patches as thoroughly as the Control System vendors.16.2: Is it a violation if you do not meet the fixed date? Suggested wording: replace "fixed date" with "scheduled date". Add a provision to supply reasoning for not meeting scheduled dates. The rewording provides flexibility to the Responsible Entity to push installation of the patch to a later date without being in violation.17.2: Add a sentence similar to the last sentence in 17.1, "In the case where unused, externally accessible physical ports cannot be disabled, the Responsible Entity shall document and implement a mitigation plan." The disabling of physical ports is not supported by all network devices. To meet the literal wording an entity may need to physically damage equipment which would void warranties and prevent further vendor support.18.1: Regarding "organizational processes" and "system events that are related to cyber security". Is it reasonable to think this can be done without automated tools?18.2: Regarding "continuous security monitoring", is this redundant to 18.1? If you are implementing automated tools to monitor and log system events are you not providing continuous security monitoring? Suggest removing these words to eliminate double jeopardy.This requirement should be focused on issuing an alert.Regarding "system events related to cyber security", what constitutes a system event related to cyber security? What criteria should be used? Is there an accepted

#	Organization	Yes or No	Question 35 Comment
			standard that an entity will be held to in an audit? If the right system events are not classified in an auditors' eyes, is this a violation? Suggest rewording to reference an acceptable set of minimal system events to monitor. What if a BES Cyber System does not generate a sufficient amount of detail to determine if a cyber security event occurred? Suggest allowing a TFE in this instance.18.3: Regarding "Maintain logs of system events related to cyber security within the specified time period", what if a BES Cyber System cannot store events for the duration required? Is a responsible entity required to go out to a device repeatedly to export their logs if they cannot meet the 90 day or 1 year increment? Suggest rewording to take into account limitations of BES Cyber Systems. Possibly use as a TFE item, if TFE's are maintained.What benefit does this provide for reliability or security? 18.4 is the important element, not the data retention.R19: With real-time or near real-time control systems, these requirements could increase latency and pose a negative impact to reliability.19.1: Regarding "Validate data inbound to a BES Cyber System in a Control Center", validate against what? Is the source being validated? Is the data itself being validated? Is providing encryption on the data sufficient? Who determines the appropriate level of validation? Is it being left to an auditor?Reliability could be compromised if this induces extra latency on the systems sending and receiving real-time data. This should be included as a TFE; older systems may not be able to handle the latency.19.2: Would "bad quality" indicators in the EMS system be an example of this?
35.64	APPA Task Force	Disagree	The APPA Task Force believes that Requirement R15 as currently drafted will require numerous TFE's. Each entity will need to document that they are not following this requirement since a vast array of devices in substations and generation stations are BES Cyber System Components but are not capable of propagating malicious code. Therefore we recommend the following edits for R15:R15. Objective:To protect BES Cyber Systems from malicious software that could affect availability or integrity of the Reliability Functions.R15. Requirement:Each Responsible Entity shall document and implement one or more processes incorporating the criteria specified in CIP-011-1 Table R15 - Malicious Code Protection. This requirement applies only to BES Cyber

#	Organization	Yes or No	Question 35 Comment
			System Components that have the capability to propagate malicious code. Change the Table legend to “Malicous Code Protections”.The APPA Task Force is concerned that the criteria in R15 Table 15.3 do not constitute a reasonable requirement when looking at the transmission and generation environments that will be required to comply. The drafting team may not fully appreciate the full magnitude and implications of the phrase “test and update”. We recommend that the criteria in Table 15.3 be removed or only be required for control centers.R16 Objective:To ensure that security vulnerabilities in BES Cyber Systems are mitigated. R16. Requirement:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R16 - Security Patch Management R17. Objective:To reduce the available attack surface of the BES Cyber System.R17. Requirement:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R17 - System Hardening The APPA Task Force agrees with the MRO-NSRS proposal noting that as written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings. This would require an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We recommend that this item be deleted.R18. Objective:To ensure that security events are known, logged, and responded to on BES Cyber Systems.R18. Requirement:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring R19. Objective:To protect the real-time operation of the BES from the use of maliciously modified data by BES Cyber Systems.R19. Requirement:Each Responsible Entity shall implement processes incorporating the criteria specified in CIP-011-1 Table R19 - Communications and Data Integrity The APPA Task Force is extremely concerned with the actual ability of the industry to comply with the criteria in R19 as proposed. A discussion is necessary to understand if this requirement is actually feasible for all entities with High Impact facilities.

#	Organization	Yes or No	Question 35 Comment
			Utilities hire capable operators to make decisions on incomplete data all the time. If validating the data inbound means another electronic verification, this is impractical. If validating the data inbound means calling a lineworker in the field to check a setting in a substation when an operator is not comfortable with the data he is receiving, this is reasonable, but still not an auditable requirement. We agree with the MRO-NSRS evaluation of 19.2, which notes that as written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously. We recommend that this requirement be removed and placed in the guidance in support of the standard as a future technology.
35.65	Bonneville Power Administration	Disagree	The objectives of these requirements ("to protect its BES Cyber Systems from malicious software that could affect availability or integrity of the Reliability Functions," "to ensure that security vulnerabilities in BES Cyber Systems are mitigated," "to reduce the available attack surface of the BES Cyber System, "to ensure that security events are known, logged, and responded to on BES Cyber Systems," and "to protect the real-time operation of the BES from the use of maliciously modified data by BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirements rather than appearing at the end of the requirements (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.The phrase "Reliability Functions" at the end of R15 is not a defined term in the April 20, 2010, Glossary of Terms Used in NERC Reliability Standards. Does the drafting team mean CIP-01-01 - Attachment 1, Functions Essential to Reliable Operation of the Bulk Electric System? If so, that should clearly be stated. If not, there should be a definition in the Glossary. Table 16, Section 16.2. We applaud the new standard, which makes it clear that immediate mitigation or installation of patches is not required. However, there are still some issues:1. Security patches arrive weekly to daily to multiple times a day. Many may be applicable to systems, but of minimal

#	Organization	Yes or No	Question 35 Comment
			threat. Entities should be able to not only evaluation the applicability, but the threat and risk of the threat to their systems within their environment, and choose to escalate or deescalate patches as appropriate to them. Low impact, or low risk patches may be assigned to a regular patch or maintenance cycle, while high risk patches may be tested and implemented immediately. This should be up to the system owners, and not prescribed in the requirement.2. Mitigation plans are not necessarily applicable. Some patches, while technically applicable to specific equipment or operating systems, may have such a low risk or impact that they entity may choose not to apply the patch.3. There are instances where a patch may be applicable from a security perspective, but the risk it presents from a reliability perspective may outweigh it. 4. Where systems are isolated from external affects, even a patch that applies to a specific device may not be necessary.5. Meaning of "fixed date" is not clear. Does it mean "the same for every patch", or "the date can't be changed"? Both are bad choices. Different patches might require different schedules, depending on their impact and the availability of outage time on the system.R17: Rename this back to "Ports and Services" to avoid confusion. In the electrical industry "Hardened" systems are those that meet specific electrical requirements and interference requirements.Also, the use of the word surface implies something physical rather than electronic.Recommendation for R17: "Objective 17 - To reduce the available electronic attack points of the BES Cyber System.R17. Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R17 - Ports and Services"Table 17, Section 17.1. A mitigation plan might not be appropriate. In the context of NERC standards, a mitigation plan describes the actions that will be taken to achieve compliance. That is not the situation here. Recommendation: "cannot be disabled, the Responsible Entity shall document the reasons for the inability and compensating measures used."Section 17.2. We understand that FERC wishes the standard to address physical ports. However, this could have negative conquences:1. There are hundreds of thousands of devices in service that have physical ports that may not be used. The fact that they are not needed or used normally means that there is nothing connected

#	Organization	Yes or No	Question 35 Comment
			to them. If there is nothing connected to them, they are not vulnerable to any kind of external or remote attack.2 - Disabling physical ports on electrical system components may be: o Impossible o Degrade the operation of the equipment o Render the warranties on the equipment void thereby removing vendor service o Create such a huge national work load that it could never be accomplished.Recommended change - Eliminate 17.2Table R18:18.1 & 18.2 - The use of the term "all BES Cyber System Components" is not accomplishable:1. Many, if not most "components" in the field do not capture what would be considered cyber security related events. They only capture electrical system events. They don't even have the capability to capture access events.It is the access points to these devices that may have the ability to capture even the most rudimentary cyber security information (Access Attempt, Date, Time, Account, Source, Target)2. It may not be possible to place monitoring equipment within electronic monitoring proximity of these components. 3. The term "events that are cyber security related" is not defined. What exactly does it mean? Is this access events, Intrusion Detection systems, Antivirus, ??? Much of this cannot be implemented on or even for "all BES Cyber Components". Recommendation: 1. Remove "components", so that the requirement is at the BES Cyber System level.2. Change "...security for all..." to "...security, as defined by the Responsible Entity, for all..."18.3 has the same issue with the definition of "events related to cyber security". In addition, this time frame has caused some confusion from an audit perspective. - Some have read that to mean that there must be, on the originating system, at all times, at least 90 days worth of logs. While others (rightfully, we feel) are maintaining archives of their logs in alternate locations for 90 days or longer. Recommendation: replace with "Maintain captured log information within the specified time period on-line, in archives, or in some other readily accessible form."Section 18.4. Consistently accomplishing manual review of logs could be difficult for large entities with large numbers of devices, especially within the 7 days required for high impact systems. The obvious solution is the use of an automated log review tool. This should be explicitly addressed in the standard. Recommendation: "Review, either manually or by automated means, logs...." Entries in Table R19 are acceptable only if the

#	Organization	Yes or No	Question 35 Comment
			definition of external connectivity is changed, as discussed above. Otherwise, entities would be forced to validate data inbound from one BES Cyber System to another BES Cyber System, all within the same Control Center. This does not seem to be the intent: using the existing definition of external connectivity, any data inbound to a BES Cyber System uses external connectivity. In that case, why state it so? Clearly, the intent was to validate traffic inbound from outside the Control Center, at most.
35.66	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The requirements are to prescriptive for the range of systems that it will apply to.
35.67	Constellation Power Source Generation	Disagree	The term "release" in R16.1 needs to be further defined. The issue with it being vague is that some patches for a system may be released for all users, but if that system is tied to a distributed control system, the distributed control system vendor has to validate the patch before its implemented by a facility. Using this example, there are really 2 release dates. For auditing purposes, a suggestion would be to define release locally as "the date of which a security patch has been safely validated by a vendor. If another vendor must validate this release before implementation, than the date it has been released by the second vendor will be used as the release date." R16.2 is not worded correctly. A suggested change would be "Development of an implementation schedule with a fixed date for installation of the applicable security patches and a fixed date for completion of mitigating measures that address the vulnerability, until implementation of the patch." In R18.1, is the monitoring and logging continuous, or on a fixed schedule? The SDT should add clarity to this requirement. R18.2 discusses issuing alerts but does not give a timeframe for issuing them. A suggestion would be 90 days to ensure a proper review of an incident to determine if it was a cyber event. At the CIP V4 Workshop, the drafting team stated that R18.4 was not meant to be an exhaustive manual review of logs, but rather a check to ensure the automated log is functioning. This needs to be included in the verbiage of the requirement. R19.1 should be reworded to say "Implement a process to validate data received by a

#	Organization	Yes or No	Question 35 Comment
			Control Center's BES Cyber System." Doing so would clarify R19 as a whole, and R19.2 can be removed due to its redundancy with R19.1.
35.68	Public Service Enterprise Group companies	Disagree	There are several clarifications necessary to make the language understandable and ensure that entities know what is required. [1] Please clarify the distinction between requirements 15.1 and 15.2. Performance degradations and potentials for false positives from detection mechanisms that inspect each file when accessed, as possibly implied by 15.2, may not appropriate for real-time systems. [2] In requirement 18.2 please specify what is meant by "continuous"? Is a periodic check sufficient? [3] Please clarify the distinction between requirements 19.1 and 19.2. In requirement 19.1 please specify what is meant by "Validate"?
35.69	Constellation Energy Commodities Group Inc.	Disagree	There is no definition of malicious code provided. Clarify the scope of malicious code to include virus, malware and spyware protection, as currently generally commercially understood.Please define the stipulation 'Required for external connectivity only'.Are the tools and processes listed in R18 intended to provide automated detection, or manual\narrative logging of events detected under the heading of other controls? If automatic, what sorts of events are contemplated? What is intended by the term 'Validate' in 19.1? Does this mean the identification of a separate, independent source for the data, business rules, or something else? Without understanding the intent of the standards drafting team, I cannot suggest specific changes.
35.70	Allegheny Energy Supply	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. Requirement 15.3 is unclear as to what is meant by "Implement processes to test and update malicious code protections." Suggest "Implement processes to detect malicious software, and review annually".It may be appropriate to add language that is more precise regarding the attributes of

#	Organization	Yes or No	Question 35 Comment
			the BES cyber systems/BES cyber components to be protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.71	Allegheny Power	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. Requirement 15.3 is unclear as to what is meant by "Implement processes to test and update malicious code protections." Suggest "Implement processes to detect malicious software, and review annually".It may be appropriate to add language that is more precise regarding the attributes of the BES cyber systems/BES cyber components to be protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.72	EEI	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. Requirement 15.3 is unclear as to what is

#	Organization	Yes or No	Question 35 Comment
			meant by "Implement processes to test and update malicious code protections." Suggest "Implement processes to detect malicious software, and review annually".It may be appropriate to add language that is more precise regarding the attributes of the BES cyber systems/BES cyber components to be protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.73	Reliability & Compliance Group	Disagree	To help eliminate TFE's here, you need to add a qualifier such as "to protect its BES Cyber Systems from malicious software that could affect availability or integrity of the Reliability Functions if mechanisms exist that can protect the BES Cyber System Component."
35.74	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
35.75	We Energies	Disagree	We Energies agrees with EEI: There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. With respect to requirement 15.1, We Energies believes this may not be possible for non-windows based devices/systems.We Energies agrees with EEI: Requirement 15.3 is unclear as to what is meant by "Implement processes to test and update malicious code protections." Suggest "Implement processes to detect malicious software, and review annually".It may be appropriate to add language that is more precise regarding the attributes of the BES cyber systems/BES cyber components to be

#	Organization	Yes or No	Question 35 Comment
			protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. We Energies agrees with EEI: Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.76	GTC & GSOC	Disagree	We Recommend: 1. In R15.3: taking out the words "test and" or, alternatively, clarifying what is meant by "test"2. In R19.1: clarifying whether encryption is required or if CRC will be sufficient3. Completely removing R19.2 because of the following reasons referenced from the DHS Catalog of Control System Security: a. The use of cryptography within a control system will introduce latency to control system communication. The latency introduced from the use of cryptographic mechanisms must not degrade the operational performance of the control system or impact personnel safety. b. Failure of a cryptographic mechanism must not create a denial of service. Control systems generally support the objectives of availability, integrity, and confidentiality. Therefore, the use of cryptography should be determined after careful consideration.
35.77	Midwest ISO	Disagree	What does it mean to validate data in R19.1. What is the expectation if a piece of data has been changed/modified when the value received is within reasonable limits but is not the actual value sent? This could be particularly troubling for the Interregional Security Network and ICCP. For example, how can an RC validate that the SCADA system sent valid data to the ICCP server at a TOP if it is within an expected range? More details around the expectation of validating data would be helpful to ensure entities can be compliant.

36. Tables R15 to R19 provide direction concerning what impact level of BES Cyber Systems to which Requirements R15 to R16 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 Requirements R15 through R19 have moved to CIP-007-5 Requirements R1 through R4.

Many commenters disagreed with the proposed BES Cyber System impact levels and made suggestions for improving these requirements, including suggestions to revise or refine the impact levels based on the particular characteristics of the BES Cyber Systems involved. For example, some suggested that certain requirements should apply only to Medium Impact BES Cyber Systems with external connectivity. Others suggested that there were key requirements such as malware prevention that should apply at all BES Cyber System impact levels. In response, the SDT has made changes to include an applicability column in each table for each requirement. The applicability column further refines the set of BES Cyber Systems and assets to which each part of the requirement must be applied. The intent of this approach is to refine, as commenters suggested, the scope of requirements that apply to each type of BES Cyber System or device based on its characteristics. The drafting team recommends that commenters carefully review the proposed applicability column in the table for each requirement in CIP-003-5 through CIP-011-1.

#	Organization	Yes or No	Question 36 Comment
36.1	Northeast Utilities	Agree	Need TFE language added; not all CCAs or protecting assets require malicious code protection.
36.2	FirstEnergy Corporation	Agree	R17 - Does 'external connectivity only' mean only firewalls? If not, please provide intent of SDT.
36.3	BGE	Disagree	15.1, 15.2 and 15.3 should also apply to Low impacted systems. 16.2 implies that the patching can only occur on the same day every month.19.1 Define "validate".
36.4	ERCOT ISO	Disagree	15.1-15.3: Should apply to Low Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
36.5	American Electric Power	Disagree	17.1: Regarding "Required for external connectivity only" within the High and Medium

#	Organization	Yes or No	Question 36 Comment
			impact categories. Is this required for "routable external connectivity" only, or all connectivity?How will items in R18 and R19 be performed on systems with nonroutable connectivity? Will dedicated IT Security Operation staff need to be added to isolated networks to perform the security status monitoring?
36.6	US Bureau of Reclamation	Disagree	Add R15.1, R15.2 and either R18.1 or R18.2 to the requirements for a low impact system. Concept of REMOTE connectivity is not defined. Without that definition, it is hard to assess if a High Impact is appropriate or if no Medium Impact is reasonable..
36.7	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
36.8	Black Hills Corporation	Disagree	At least 15.2 and 16.1 should also apply to low impact BES Cyber Systems.
36.9	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
36.10	The Empire District Electric Company	Disagree	Comments: For items 15.1 - 15.3, 16.1 - 16.2, and 17.1 we would propose using the following under Medium Impact and High Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.We believe the time frames for item 18.4 may not be practical at distributed locations without routable external connections, where logs would need to be reviewed locally.
36.11	US Army Corps of Engineers, Omaha Distirc	Disagree	define terms "continuious security monitoring" and "detected system events."
36.12	CWLP Electric Transmission, Distribution and	Disagree	Due to the requirement for continuous monitoring and alerts defined in R18.2 the requirement for log reviews every 7 days should not be needed. A standard 30 day review as in the medium impact area should be appropriate for both high and

#	Organization	Yes or No	Question 36 Comment
	Operations Department		medium impact levels.Does the fact that the data has been successfully passed through a Firewall or Access List meet the obligation to validate data incoming to a Control Center in R19 or does this require the data be inspected all the way down to the packet level?
36.13	American Transmission Company	Disagree	For items 15.1 - 15.3, 16.1 - 16.2, and 17.1 we would propose using the following under Medium Impact and High Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
36.14	MRO's NERC Standards Review Subcommittee	Disagree	For items 15.1 - 15.3, 16.1 - 16.2, and 17.1 we would propose using the following under Medium Impact and High Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.We believe the time frames for item 18.4 may not be practical at distributed locations without routable external connections, where logs would need to be reviewed locally.
36.15	Southern California Edison Company	Disagree	In order to appreciate the impact based categorization and reflect the actual impact on BES reliability, an additional requirement can be added to R16 for medium and low impact system. The drafting team should look at NERC PRC standards on maintenance schedules and synchronize CIP patching and upgrades to a maintenance and inspection schedule that is already mandated by NERC.Requirement R18 requiring logs be reviewed manually every seven days, when controls to automatically monitor such logs are already in place, is a control that does not seem to add additional security value. If the intent of the drafting team is to manually ensure and certify that the logging capability is functioning adequately, the drafting should include such verbiage. The current draft language of the standard seeks only a manual review of

#	Organization	Yes or No	Question 36 Comment
			the log rather than the manual verification of the logging capability.
36.16	Progress Energy - Nuclear Generation	Disagree	Incorporate information contained in the matrix in Attachment 1 for durations to ensure consistency by aligning CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
36.17	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
36.18	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's observations below:There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: “Implement and document one or more security processes for security monitoring

#	Organization	Yes or No	Question 36 Comment
			that issue alerts for detected system events related to cyber security."Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it.
36.19	NextEra Energy Corporate Compliance	Disagree	NextEra believes requirement R17 should be applied to both high and medium BES Cyber Systems.
36.20	PacifiCorp	Disagree	PacifiCorp agrees with EEI's observations below:There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: "Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security."Requirement R19 creates a potentially impossible level of

#	Organization	Yes or No	Question 36 Comment
			obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is presented to it.
36.21	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation 'Required for external connectivity only'.
36.22	American Municipal Power	Disagree	Please provide a little or no impact category
36.23	The United Illuminating Co	Disagree	R15.2, introduction of malicious code, responding to the introduction of malicious code is a specific cyber security incident. Suggest 15.2 be limited to processes to detect malicious code. Response is already part of cyber incident response.
36.24	Southwest Power Pool Regional Entity	Disagree	R15: Malicious code prevention is a basic security control and should be applicable to all impact categories. R17 and R19 should not make a distinction between external and non-external connectivity. R17: Once access is gained into the network by any means to any cyber system on the network, external access is immaterial.
36.25	Southern Company	Disagree	R19 comes from the DHS catalog, requirement 2.8.8. In the DHS catalog, there are 4 requirement enhancements, two of which are warnings which could greatly affect reliability. The DHS catalog presumes this requirement would be implemented on a case by case basis after appropriate research and testing. It therefore has no place in a mandatory standard that will force its use everywhere without regard to the reliability impacts. This requirement should be removed from a reliability standard.
36.26	National Grid	Disagree	Refer to answers in Q. 35.
36.27	Manitoba Hydro	Disagree	Requirement 18.4 can be very onerous for the industry for legacy systems which don't support automated log consolidation or review. The requirements must allow more flexibility.

#	Organization	Yes or No	Question 36 Comment
36.28	Garland Power and Light	Disagree	Requirement 19, 19.1 and 19.2 should not be required for any level
36.29	San Diego Gas and Electric Co.	Disagree	SDG&E feels that if R17.1 is a requirement for Medium Impact systems, then R17.2 should be as well for Medium Impact systems. For R18.3 and R18.4, SDG&E recommends that consistency be applied to the requirements to help ease the compliance burden of companies that have both High and Medium Impact BES Cyber systems. SDG&E also feels that instead of using the word "impact" for these Requirements, apply a concept of "risk" for inclusion. We would want to identify the risks with associated systems security and protect accordingly.
36.30	Con Edison of New York	Disagree	Section 15 & 16 should be limited to networked systems. Isolated microprocessors not part of a network should not have the same requirement.
36.31	ISO New England Inc	Disagree	see answer to question 35
36.32	Progress Energy (non-Nuclear)	Disagree	See comment 14.
36.33	WECC	Disagree	See comments for Q35Criteria should aplpy to all impact levels
36.34	LCEC	Disagree	See previous comments
36.35	BCTC	Disagree	See response to Q35.
36.36	Hydro One	Disagree	see response to Question 35
36.37	Entergy	Disagree	See response to Question 35 immediately above.
36.38	Northeast Power Coordinating Council	Disagree	See response to Question 35.

#	Organization	Yes or No	Question 36 Comment
36.39	ReliabilityFirst Staff	Disagree	Suggest “Required” for Medium Impact in rows 15.1, 15.2, 15.3, and 17.2. Suggest “Required for external connectivity only” for Medium Impact in rows 19.1 & 19.2.
36.40	Duke Energy	Disagree	Table 18: Manual reviews every 7 days is not practical.
36.41	Consultant	Disagree	Table R15 - Item 15.3 The requirement to "Implement processes to test and update malicious code protections." is confusing. Is the intent to "test malicious code protections and update malicious code protections" or to "test updates to malicious code protections" Please clarify the intent. There is a need to distinguish between updates to the malicious code protection "software" and malicious code protection "signature files". The software should be implemented in accordance with change control processes. The "signature files" are a specific subset of update to malicious code protection where it is unlikely a registered entity would have the capability to test what are typically vendor proprietary file formats. The extent of the 'testing' necessary for these signature files should be clarified.Table R16 - Item 16.2 While the concept of a "fixed date" sounds good, the requirement should allow for reasonable scheduling, including rescheduling, of the installation of applicable security patches or completion of mitigating measures. An option could be to remove the words "with a fixed date" and add a new item that would require that "Events that delay a security patch implementation schedule greater than thirty days shall be documented."Table R17 Item 17.1 The first sentence uses the terminology "network accessible ports and services" and the second sentence uses the terminology "network accessible services and communication methods". Suggest using consistent terminology to avoid confusion.Suggest defining the term "network accessible ports and services" (may be multiple terms) as they are intended for use in the standards. There does not appear to be a standardized definition for this term in the industry. The term "network accessible ports and services" appears to imply access across the protection boundary? If it does then the requirement statement of "Required for external connectivity only" is unnecessary and should be changed to "Required".Table R18 - Item 18.3 Suggest changing the word "within" to the word "for" for clarity of

#	Organization	Yes or No	Question 36 Comment
			meaning.Item 18.4 - Weekly log review appears to create an excessive administrative burden without a corresponding decrease in risk to the High Impact assets. Items 18.1 and 18.2 require continuous monitoring of the same activity. Manual log review is redundant to these requirements. While there may be a reason for manual log review to confirm the continuous monitoring is occurring as expected a more reasonable periodicity of monthly or quarterly should be required for both Medium and High Impact assets.Table R19 - The limitation of these items to a Control Center is an added dimension of Impact that is not included in the impact categorization criteria. If data is an issue, then these requirement should apply to all assets based on impact categorization without addendum or modification by the requirement. Suggest modifying the impact categorization criteria to clearly identify those assets.Table R19 - "Inbound data" implies remote access, and the terminology "Required for external connectivity only" is redundant. Suggest changing the wording to "Required".Items 19.1 and 19.2 are inconsistent. Item 19.1 requires validation of inbound data, and item 19.2 provides an exception to validation for encrypted data. If you comply with item 19.1, then item 19.2 is irrelevant. If you comply with item 19.2, then you are in violation of item 19.1.R19 - Overall, this requirement should be removed in it's current form. Automatic system operation cannot exist if "inbound data" is required to be validated. Automatic system operation is dependent on responses to external data inputs. If the intent is to return the BES to manual operation, this requirement will achieve that end.
36.42	Alberta Electric System Operator	Disagree	Table R15 - make 15.1, 15.2, 15.3 required for Low Impact BES Cyber Systems, but possibly on a longer time horizon than for Medium and High Impact BES Cyber Systems.Table R16 - make 16.2 required for Low Impact BES Cyber Systems.Table R17 - make 17.1 “Required for external connectivity only” for Low, and “Required” for Medium and High. Make 17.2 required for Medium also.Table R18 - make 18.1 and 18.2 required for Low Impact systems. Make 18.3 90 calendar days for Low Impact systems. Make 18.4 30 calendar days for Low Impact systems.

#	Organization	Yes or No	Question 36 Comment
36.43	Idaho Power Company	Disagree	The review of logs every 7 days or even 30 days is extreme unless the logs are filtered for only abnormal events and only logs of abnormal events are reviewed.
36.44	Ameren	Disagree	The system hardening in Table for R17 is rendundant when other standards already restrict physical access to these systems.â€,â€,â€,R18.1, R18.2, R18.3, and R18.4 - Log file monitoring at Medium Impact Systems will be costly as there may not be bandwidth available to send the logs to a central location to be reviewed. Suggest removing these requirements for Medium Impact Systems.
36.45	Allegheny Energy Supply	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: “Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security.”Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it.

#	Organization	Yes or No	Question 36 Comment
36.46	Allegheny Power	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: "Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security."Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it.
36.47	EEI	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System

#	Organization	Yes or No	Question 36 Comment
			Components are already subject to physical protection requirements.Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: "Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security."EEI recommends deleting R19. As written, R19, fails to recognize the obligation to "Do no Harm." Concerning data communication. Entities attempting to implement some of these measures, may in fact introduce latency or unintended, self inflicted denial of service attacks. It should be noted that the source of this requirement (DHS Catalog of Controls) provides multiple warnings about implementation risks associated with this control. It is not appropriate to put forth requirements that may reduce the reliability of the BES.
36.48	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
36.49	We Energies	Disagree	We Energies agrees with EEI: There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.We Energies agrees with EEI: The creation of a mitigation plan should not be deemed an exception requiring a TFE.We Energies agrees with EEI:

#	Organization	Yes or No	Question 36 Comment
			Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.We Energies agrees with EEI: Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.We Energies agrees with EEI: Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.We Energies agrees with EEI: Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: "Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security."We Energies agrees with EEI: Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it. We Energies agrees with EEI: As written, R19, fails to recognize the obligation to "Do no Harm." Concerning data communication. Entities attempting to implement some of these measures, may in fact introduce latency or unintended, self inflicted denial of service attacks. It should be noted that the source of this requirement (DHS Catalog of Controls) provides multiple warnings about implementation risks associated with this control. It is not appropriate to put forth requirements that may reduce the reliability of the BES.
36.50	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R15 - R19:R15 Table 15.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR15 Table 15.2: Low

#	Organization	Yes or No	Question 36 Comment
			Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR15 Table 15.3: (If retained)Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR16 Table 16.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR16 Table 16.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR17 Table 17.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR17 Table 17.2: (If retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required for routable external connectivity onlyWe believe the "continuous security monitoring" as described in 18.2 is not practical for all BES Cyber System Components. We also believe the time frames for item 18.4 may not be practical at distributed locations without routable external connections, where logs would need to be reviewed locally. Therefore we propose that for Medium impact facilities 18.1-18.4 be "Required for Control Centers only."R18 Table 18.1: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: RequiredR18 Table 18.2: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: RequiredR18 Table 18.3: Low Impact: N/AMedium Impact: 90 calendar days for Control Centers OnlyHigh Impact: 1 yearR18 Table 18.4: Low Impact: N/AMedium Impact: 30 calendar days for Control Centers OnlyHigh Impact: 7 calendar daysR19 Table 19.1: (If retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required for external connectivity onlyR19 Table 19.2: (If retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required for external connectivity only

37. Requirements R20 to R22 of draft CIP-011-1 concern procedures for boundary protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R20 to R22? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1Requirements R20 through R22 have moved to CIP-005-5 Requirement R1.

Many commenters suggested phrases or aspects of the requirements that needed to be clarified. Several commenters questioned the need for weekly review of log entries, indicating that reviewing log entries at this interval would be burdensome with little or no positive impact on reliability.

Several commenters suggested reverting to the old name of Electronic Security Perimeter in place of Electronic Boundary Protection. In addition, several commenters suggested removing the system boundary protection requirement because it is overly prescriptive.

The drafting team agrees with commenters that some aspects of the requirement were too prescriptive, and has made significant changes to update the requirement both to clarify it and make it less prescriptive, while still addressing FERC Order 706 directives. The drafting team also agreed to revert to the Electronic Security Perimeter designation.

#	Organization	Yes or No	Question 37 Comment
37.1	WECC		Agree with concept, however, some work on the wording might make this more clear. R21 should have an additional item 21.3 - Cyber System components will not be shared with non-BES cyber systems or BES Cyber Systems of different impact levels.The former requirements for ESPs were better. The new language describing access points on communication paths may be an indirect way to get there, but it does not make things clearer or more auditable. This method of describing controls will make matters more complex and create additional work for entities.
37.2	GE Energy	Agree	"Logical Separation." Logical separation should be clarified. Logical separation could mean network access separation through an access point or it could be account separation by having separate user, system or service accounts that are different

#	Organization	Yes or No	Question 37 Comment
			amongst BES systems.
37.3	USACE - Omaha Anchor	Agree	Define 'unauthorized access attempts' is this a ping, or is this when a bad password is given to the system.
37.4	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.R20.20.2 - How does one implement a deny access by default for a dialup modem? That effectively either takes the modem out of service, or if you were to rely on the PSTN to do any kind of 'validation' of the incoming call, this is at best security through obscurity as it is trivial to spoof the callerid which is the only form of data validation that can be done over a dialup line.20.4 - What does "unauthorized access" mean? Does that mean an access attempt? Would a port scan of a firewall qualify as "unauthorized access"?20.5 - What does "unauthorized access" mean? If something as simple as a connection attempt qualifies, this requirement puts a tremendous burden on staff to track every little event that might happen on the firewall, and would not accomplish much in the end. If the intent of the standard is to keep unauthorized login attempts at bay, it should say that.R21.21.2 - Communication through an "electronic access point" for dial-up communications could prove difficult for some devices. Some devices are extremely sensitive to any sort of jitter introduced to a data stream, and having a security device in front of these kinds of devices may introduce enough jitter to make the communications unusable. R22.This seems duplicative of R14, R16, R18 and R23. FMPA suggest modifying those requirements to incorporate the protective cyber systems elements.22.2 - This should be consistent with R16; medium should be required to patch access control points. Also, low should have to patch at least quarterly. For access points, consider forcing high impact to asses 'critical' patches within 7 days.
37.5	Green Country Energy	Agree	Footnotes, guidance document?
37.6	Exelon Corporation	Agree	If systems are connected to a master station/location that is a BES Cyber system, do all the connected systems become BES Cyber systems? At what level do these

#	Organization	Yes or No	Question 37 Comment
			requirements apply - for example at the relay level where someone is logging into the relay? Exelon would like clarification on the definition of the electronic access point - is it at the component level or at the system level?
37.7	Progress Energy - Nuclear Generation	Agree	R20-22 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
37.8	Independent Electricity System Operator	Disagree	- R20.1 R20.4 20.5 and 20.6 External and External connectivity needs to be defined. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary? - - R20.5 Please define
37.9	National Grid	Disagree	1. National Grid requests clarification on “all communication paths” in 20.1 which can be every possible communication path between two end points. The entity should be required to document only external communication paths with dial up access or routable protocol. Recommend removing R20.1 and 20.2 from LOW impact category.2. National Grid recommends removing “within the following time period” from 20.5 and 20.6. Also, for dial ups it would be difficult to review the alerts in the given time period. Suggest 30 days for logging related to dial-ups. 3. National Grid recommends that 20.6 be re-worded to be consistent with FERC Order P526 - “Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs.”4. National Grid recommends that 20.6 High Impact BES CS should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven days. Also should it be included for Medium Impact BES CS?5. National Grid recommends removing 21.2 since it is covered in 20.26. National Grid recommends removing R22 since it is redundant and move it’s table into the respective Requirements o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23

#	Organization	Yes or No	Question 37 Comment
37.10	Dairyland Power Cooperative	Disagree	20. What are the boundary rules for serial connectivity vs. routable protocols. Serial connections can be external to different systems and they can be internal. How do we determine if there is a boundary to protect?21. The logical separation rule needs more detail "Logical Separation" should have a definition. What is the impact for an RTU field device than can be scanned by multiple systems or entities? Is the mere configuration of available data on each physical or logical port enough to satisfy logical separation? What about components used as system-to-system gateways?
37.11	Regulatory Compliance	Disagree	20.1 - clarify - are these communication paths external to the electronic boundary?20.2 - clarify - This implies a firewall for even low impact?20.3 - guidance on what required elements to document20.6 - Clarify if this is for firewall logs only21.1 - Major clrification needed - what about BES Sytems that rely on input and out from system to system in having the logical separations?
37.12	Dominion Resources Services, Inc.	Disagree	20.1. The language "Document all communication paths" is too vague and suggests a need to map out the entire LAN/WAN infrastructure. Based on the May workshop discussion, the intent of the requirement is to document inputs and outputs associated with the BES Cyber System. Dominion recommends the following alternate wording for R20.1:"Document all digital interfaces associated with each BES Cyber System."20.4. Dominion recommends revising the language of this requirement to read:"Document and implement one or more processes for logging all access attempts at each electronic access point."Firewall logs cannot identify all "actual unauthorized access." Someone using a trusted source to gain access to a BES Cyber System would be permitted through a firewall. That is "actual unauthorized traffic" but it is not detectable. Blocked access attempts are shown in firewall logs as a dropped or denied entry.20.5. As explained in the comment for requirement 20.4, firewall logs cannot identify all "unauthorized access attempts." Therefore, Dominion recommends rewording this requirement to read as follows: "Document and implement one or more processes for alerting and review of alerts by designated response personnel at each electronic access point within the following time period."

#	Organization	Yes or No	Question 37 Comment
			20.6. Compliance with this requirement is labor intensive and, therefore, not practical for a large number of BES Cyber Systems. Requiring a manual review every 7 days is excessive for the benefit received and does not make allowances for reviewer unavailability due to sickness, emergency work or vacation. At minimum Dominion recommends extending the review requirement to every 30 calendar days or revising the requirement to allow for selected BES Cyber Systems to be reviewed every 7 calendar days as follows: "Document and implement a process for manual review of a sampling of log entries or sorted or filtered logs for selected BES Cyber Systems within the following time period."21.1. The word "either" should be inserted after the word "provide." The phrase "or controlled access from one system to the other" should be added after "between each system." This modification is reflected in the revised language below: "Cyber System Components in Control Centers that are shared between BES Cyber Systems must provide either logical separation that prevents access between each system or controlled access from one system to the other."The issue is devices that provide a gateway between 2 systems. An example is the node that passes data between the EMS and ICCP networks.
37.13	Network & Security Technologies Inc	Disagree	20.2 - Current wording could be interpreted to mean an access point is required between a BES Cyber System and any other BES Cyber System the Responsible Entity may have defined, even if on a shared network. Could also be interpreted to mean access points are required on a per routable protocol basis. Assuming these interpretations were not intended, 20.2 should be rewritten for greater clarity.20.3 - Except for "document," this requirement seems to duplicate 20.2.20.6 - Wording suggests this requirement applies to all BES Cyber Systems. Is this what was intended, or is it to be applied to access point devices? Please clarify.21.1 - Please clarify intent and applicability of this requirement. Is it intended to apply to virtual machines? Disk arrays shared by multiple application servers? Both? Neither?21.2 - Redundant if all access points are properly identified. Suggest eliminating it or combining the statement with one of R20's sub-requirements.R22 - Seems to overlook physical protections for cyber systems that establish electronic boundaries.22.4 - Configuration changes such as updating access control settings on a firewall or

#	Organization	Yes or No	Question 37 Comment
			revising the physical access permissions associated with a card key should not be subject to this requirement, and it should so state.
37.14	American Electric Power	Disagree	20.2 & 20.3: Regarding "Document and implement access control at each electronic access point established in Part 20.2", is this redundant to R14 - lines 14.1 through 14.3? Suggest rewording or removing if it poses double jeopardy.20.6: Regarding "Document and implement a process for manual review of a sampling of log entries or sorted or filtered logs for each BES Cyber System within the following time period", does this provide any security benefit? If a system event for cyber security was missed by an automated tool, is it reasonable to expect it to be found in a manual review? What is an entity supposed to look for in this manual review?21.2: Regarding "Cyber system components that provide external communication to the BES Cyber System must only communicate externally through an electronic access point as specified in Requirement R20", it appears that this is a restatement of the elements of R20. If that is not a correct assumption, the SDT need to provide additional information.
37.15	ERCOT ISO	Disagree	20.2: Recommend using “ingress or egress point” instead of “access point”. 22.1-22.3: Please remove reference to other standard. Address the content in the appropriate standard only. The circular references in the existing standards are very difficult to navigate and provide opportunity to miss the requirement.
37.16	BGE	Disagree	20.5 timeframe should be consistent for medium and high.
37.17	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
37.18	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
37.19	Southwest Power Pool Regional Entity	Disagree	Clarify the requirement. A reader could interpret the criteria as requiring an access point between each defined BES Cyber System regardless of network segment placement. 20.4: More often than not, authentication is performed at the end host

#	Organization	Yes or No	Question 37 Comment
			system. Rather than prescribing logging of attempted or actual unauthorized access at the access point, simply require such logging at the point such unauthorized access is detected. 20.6: What are the minimum expectations for a log sampling program (e.g., how much, how often?). 21: Clarify that shared BES Cyber System Components (e.g., a networked storage device) must be afforded the highest impact categorization of all of the BES Cyber Systems sharing the component (similar to the sharing aspect of the electronic access point definition). 22: Include the requirement to protect the access control system from unauthorized physical access.
37.20	CenterPoint Energy	Disagree	Disagree - R20.2 CenterPoint Energy suggests striking the word dial-up. If dial-up is not stricken a TFE may be required to comply with this requirement for serial dial-up paths.CenterPoint Energy believes requirements, R20.3-R20.6, may require a TFE for compliance for non-routable protocols.R20.6 CenterPoint Energy believes the 7 day calendar requirement to review sampling of log entries is overly burdensome and unnecessary. Controls and alert processes to notify appropriate personnel of unauthorized access attempts are mandated in prior requirements. CenterPoint Energy recommends a 30 day review.
37.21	E.ON U.S.	Disagree	E.ON U.S. interprets R20.1 to require documentation of “all” communication paths which could include communication links to all RTUs, etc. This level of documentation is not necessary
37.22	Duke Energy	Disagree	Elimination of terms such as electronic security perimeter without a completely thought through substitute concept contributes to industry frustration. The industry, at least, had come to understand the concept of an ESP. How the “boundary” is identified does not seem well thought through. In the text box, information such as “...cyber systems sharing one or more common electronic access points ...will be treated at the highest BES Cyber system impact categorization level of the BES Cyber system...” seems to belong in CIP 010 where the actual categorization occurs. This information is NOT a technical control and does not seem to belong in CIP 011. Rather it provides additional information concerning the categorization. This standard

#	Organization	Yes or No	Question 37 Comment
			will cause entities to document a lot of confidential information, which then must be protected. R20 - electronic security perimeter is a retired term, suggest replacing with a different term.Table 20: 20.2 is confusing for initial setup processes. How can we explicitly authorize?Requirement 20.2: The electronic access point can therefore be shared between systems as defined in the text box beside R20. For generation stations in particular, there are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). Sharing such an access point is highly desirable. Requirement 20.2, as written, seems to contradict the definition in the text box in requiring that the Responsible Entity establish an electronic access point on EACH routable protocol or dialup communication path between BES Cyber Systems.Requirement 20.4: this requirement makes sense if remote/external access is defined by the "shared access point" as described here (which seems to be in agreement with comments made in sections R11, R12, R13, where the emphasis was on communication between the devices rather than "at the access point").Requirement 20.6: please consider including the words "related to electronic boundary protection" to make the sentence read as follows: Document and implement a process for manual review of a sampling of log entries or sorted or filtered logs relating to electronic boundary protection for each BES Cyber System within the following time period. Also, where logs are accumulated, there is no way to tell if the user was internal or external to the edge device.Table 2121.1 Suggest changing 'prevents' to 'limits' or remove 'that prevents access'. Within Generation, that access is required. Also, Does "logical separation" include "virtual separation"?21.2. Verify this is not just for control centers.
37.23	RRI Energy	Disagree	For 20.1, define communication path, eg., source and destination(s) only or everything in between?For 20.5, what does "all unauthorized access attempts" mean? If an operator fat-fingered login password, does the standard expect alert and follow up each time? "all unauthorized access attempts" needs to be redefined with some threshold before declaring it as unauthorized access attempt. Otherwise, Entities and operators will spend a lot of time documenting unauthorized access and instead of

#	Organization	Yes or No	Question 37 Comment
			securing their assets.
37.24	Northeast Utilities	Disagree	For 20.5, please provide clarification on the meaning of "all unauthorized access". Every password violation for example, is not an unauthorized access attempt but could be interpreted as such. Do we really need to follow-up on every invalid password attempt? Instead of every invalid password attempt, are password lockouts an appropriate trigger? Also, please consider addressing repeated lockouts in the criteria specified.R22 appears to be significantly weaker than the previous standards. One area that is specifically weaker is with regard to access control to Protective Cyber Systems. How can an entity not authorize, review and revoke a role as important as a firewall administrator?
37.25	Constellation Power Source Generation	Disagree	In R20.1 as well as the definition box, the term digital information needs to be defined further. R21 inherently forces entities to further segment their BES Cyber Systems, which is counter to the entire premise of allowing the entities to define their own BES Cyber Systems. Allowing the entities to define their own BES Cyber Systems would limit the scope of an attack, which the SDT stated in the CIP V4 Workshop as their goal in R21. Constellation suggests removing this requirement entirely. Likewise, R22 should be removed as it is completely redundant. Note that in each sub requirement it merely points to another requirement in the document. A suggestion would be to implement the verbiage found in Table R22 to each of the requirements it points to.
37.26	Alberta Electric System Operator	Disagree	In Table R21, was the intent of 21.1 only for Control Centers? The AESO would suggest removing the Control Center parameter and make 21.1 applicable to all High and Medium BES Cyber Systems.
37.27	Constellation Energy Commodities Group Inc.	Disagree	Is the intent to require use of hardware firewalls? If so, is it possible to state that clearly? If not, what is the intent?
37.28	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).

#	Organization	Yes or No	Question 37 Comment
37.29	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's observations below:Suggest using electronic security perimeter rather than "Boundary Protection."Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.For R 20.5: Document and implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.For R 20.6: Document and implement a process for manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.R21: Suggest using electronic security perimeter rather than "System Boundary Protection."Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.There may need to be additional requirements for "Protective Cyber Systems" to include remote access controls, patch management, security event alerting, change control and change management.
37.30	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R20, but recommends changes as follows: o Regarding Part 20.2, since Low Impact BES Cyber

#	Organization	Yes or No	Question 37 Comment
			Systems do not require any Physical Security as defined in previous requirements, it seems inconsistent to require electronic access point security for those systems. o Regarding Part 20.4, how does the Standards Drafting Team envision that a Registered Entity would log "actual unauthorized access?" Actual unauthorized access is not identifiable since it would appear to have been authorized (or the attempt would not have succeeded. o Regarding Part 20.4, in reading and applying the definitions of "remote access" and "external connectivity," remote access is a specific type of external connectivity. Therefore, any reference to criteria for remote access based on whether or not it is externally connected is redundant. o Is it the Standards Drafting Teams intent that Part 20.5 require an after the fact review of unauthorized access attempts? If so, it may not be possible to adhere to proposed timeframes, especially in instances where BES Cyber System support is 8 hours a day, 5 days a week. If it is the Standards Drafting Teams intent that Part 20.5 address responding and monitoring a potential malicious attack situation, then the time frames are not sufficient.Minnesota Power generally agrees with the proposed Requirements R22, but recommends changes as follows: o The language in Part 22.1 creates confusion. The requirement states that remote access is to be restricted as stated in R14 and that for Low Impact BES Cyber Systems this is required. However, in reviewing Requirement R14, only Part 14.1 is required for Low Impact BES Cyber Systems. As a result, does this mean that only Part 14.1 needs to be implemented for Low Impact Cyber Systems in 22.1 or do 14.1-14.4 need to be implemented? The same should be addressed for Medium Impact BES Cyber Systems. o The same type of confusion regarding the language in Part 22.1 exists in Parts 22.2, 22.3, and 22.4. The Standards Drafting Team should consider whether these cross-references are necessary. It does not appear that Parts 22.1-22.4 are identifying specific criteria, but rather are a reminder that these assets need to comply with R14, R16, R18, and R23.
37.31	NextEra Energy Corporate Compliance	Disagree	NextEra believes requirement 20.1 is unclear as written. Is the communication path expected to end at each and every end point that receives digital information to each BES Cyber System? If this communication path is to each end point, it would be difficult to demonstrate compliance. Does compliance to this requirement also

#	Organization	Yes or No	Question 37 Comment
			require all the communications paths within a WAN or ISP?Requirement 20.2 does not allow a responsible entity to put more than one BES Cyber System inside an access point since it requires access points between systems. This is highly inefficient and creates access points where not needed and could potentially impact the reliability a BES Cyber System. It is unclear why the requirements are moving away from the well established ESP concept. This concept is well established in 'defense in depth' and other security frame works. The requirements for boundary protection should follow the ESP model from V1 and V2 of the NERC CIP requirements. In addition the definition also (inadvertently) conflicts with the definition given at the start of this requirement related to access points and therefore is open to interpretation by auditors.Requirement 20.4 requires the documentation and implementation of one or more "processes for logging of all authorized remote access and all attempts at or actual unauthorized access at each electronic access point." Until the definition of remote access is clearly defined, it is unclear how responsible entities must comply and demonstrate compliance. In addition, it is unclear if remote access is considered any an access attempt from outside of the access point.Requirement 20.5 requires, "Document and implement one or more processes for alerting and review of alerts by designated response personnel on all unauthorized access attempts at each electronic access point within the following time period." The responsible entity should be able to determine the threshold for unauthorized access attempts. The way the requirement is written now, personnel would have to investigate every single denied access attempt including someone who accidentally fat fingered their credentials when trying to gain authorized access to a BES Cyber System component. The recommended approach would be to require a review of 4 or more failed attempts against a common UserID without a successful login within 1 hour. Also consider more than X total bad access attempts within one hour for User ID brute force attacks or reconnaissance. Also, in 20.1, please define what is meant by the word "paths" Is it logical or is it physical path?In 20.4, is a single failed login classified as an attempt? The wording states "all attempts at or actual unauthorized access at each electronic access point"In 21.1, does this mean that for example, a SAN

#	Organization	Yes or No	Question 37 Comment
			(Storage Area Network) can be shared by Cyber System Component and other devices as long as there is logical separation?In 21.1, if two BES Cyber Systems "share" a network switch, does this meet the requirement of "logical separation"?
37.32	PacifiCorp	Disagree	PacifiCorp agrees with EEI's observations below:Suggest using electronic security perimeter rather than “Boundary Protection.”Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.For R 20.5: Document and implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.For R 20.6: Document and implement a process for manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.R21: Suggest using electronic security perimeter rather than “System Boundary Protection.”Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.There may need to be additional requirements for “Protective Cyber Systems” to include remote access controls, patch management, security event

#	Organization	Yes or No	Question 37 Comment
			alerting, change control and change management.
37.33	Puget Sound Energy	Disagree	Puget Sound Energy has the following comments:R21.1 - Puget Sound Energy has concerns that Cyber System Components that are shared between BES Cyber Systems must provide logical separation. For example: For entities with Control Centers that utilize a Microsoft infrastructure, multiple BES Cyber Systems may centrally authenticate (or have logical security controls) facilitated by a single or clustered Microsoft Active Directory domain controller. As the requirement is currently written, Puget Sound Energy feels that those shared domain controllers would not be able to reside on the same local area network segment as the domain they participate in. Puget Sound Energy requests clarity be added in to this requirement.Table 22 - Puget Sound Energy suggests including "Where Technically Feasible" to R22, as some Protective Cyber Systems may be incapable of meeting all the requirements in Table 22.Puget Sound Energy suggests aligning Table 11 with Table 12. Table 13, Table 14, and Table 22. Puget Sound Energy suggests including wording similar to Table 11: "Required for external connectivity only".
37.34	LCEC	Disagree	R20 - 20.1 Must define what is included in communication paths. If needed specify physical interface. Digital information is actually digital data, control, or signals.20.3 is not auditable. What is access control. There is no defined scope.20.5 includes requirements for cyber incident response which is covered in a later requirement.Need to clearly identify what is considered an access point on multiple interface devices.20.6 what's the difference between this and 18.4?21.2 A BES Cyber System could include components at different physical locations that communicate with each other. This is not technically external to the system so does it apply here?
37.35	FirstEnergy Corporation	Disagree	R20 - 20.6 - Need greater clarity around whether automated alarming can be used rather than manual review of logs. This sub requirement is unnecessary with an automated system in place.R21 - We agree with the use of 'logical separation' in this requirementR22 - We do not like the way R22 refers back to other requirements. This

#	Organization	Yes or No	Question 37 Comment
			is redundant and the requirement should be eliminated.
37.36	Consultant	Disagree	R20 - The terminology appears to be incorrect. Electronic access points do not define an electronic security perimeter. It also seems odd to say the defined term Electronic Security Perimeter is going to be retired, and then use that same term to define a requirement. "Electronic Boundary Protection" is created by identifying an electronic security perimeter based on the logical network connections of cyber assets, which includes electronic access points for External Connectivity that provides Remote Access to the assets within the electronic security perimeter. Suggest retaining the term Electronic Security Perimeter as described here.Table R20 - Items 20.1 & 20.2 - This appears to be "Identifying the Electronic Security Perimeter" as describe in the comment above regarding the usage of the term Electronic Security Perimeter, but stated in more confusing language in both cases.Item 20.3 Suggest rewording as "Implement and document access control mechanisms for each electronic access point (to the Electronic Security Perimeter)."As a general comment you would "implement and document" rather than "document and implement"Item 20.4 Suggest rewording as "Implement and document access attempts and access authorizations at each access point." Item 20.4 - The terminology "Required for external connectivity only" is redundant as the access point is where external connectivity occurs. Suggest changing to "Required"Item 20.5 contains two requirements:1. Implement and document processes to identify unauthorized access attempts at each electronic access point.2. Responsible entities shall review unauthorized access attempts in the time frame specified.Item 20.4 - The terminology "Required for external connectivity only" is redundant as the access point is where external connectivity occurs. Suggest changing to "48 hours" & "12 hours".Item 20.4 - It would appear to create an excessive administrative burden without corresponding decrease in risk to require this review every 12 hours for High Impact Assets. Suggest changing required review time to "Daily".Item 20.6 - The requirement statement is subjective in regard to the degree of sampling, sorting, and filtering allowed, expected, or required. This is a requirement similar to event log review of Table R18 - Item 18.4 and the wording of these two requirements should be similar.Item 20.6 -

#	Organization	Yes or No	Question 37 Comment
			This requirement is regarding access through electronic access points and "7 calendar days for external connectivity only" is redundant. Suggest deleting "for external connectivity only"Item 20.6 - Weekly log review appears to create an excessive administrative burden without a corresponding decrease in risk to the High Impact assets. Items 20.4 and 20.5 (as commented) require continuous monitoring of the same activity. Manual log review is redundant to these requirements. While there may be a reason for manual log review to confirm the continuous monitoring is occurring as expected a more reasonable periodicity of monthly or quarterly should be required for both Medium and High Impact assets.Items 20.1, 20.4, & 20.5 - Delete the word "all" It is redundant and unnecessary to the requirement statement. (The word "all" should be removed from "all" requirement statements in the standard")Table R21 - Item 21.1 This requirement appears to create a mutually exclusive situation where shared cyber system components are separated. The wording needs to be clarified or, as it is worded it should be deleted.Item 21.1 The application of the requirement to control centers creates an added dimension to the impact categorization. The application of requirements is based on impact categorization. Modify the impact categorization criteria to capture the assets where this requirement should be applied.Item 21.2 This item appears to restate what is previously stated in the referenced R20. If some additional requirement is intended, then that requirement should be included in the reference R20 requirements list, rather than a 'hidden' requirement that is cross-referenced here.R22 - This requirement appears to be redundant. The requirements referenced in the Table R22 (R14, R126, R18, & R23) appear to include whatever is listed in this requirement. If there is some additional requirement that is intended, that requirement should be put in the respective referenced requirements. Each requirement statement and table should be contain everything related to that requirement, rather than having a separate requirement that 'adds' to other requirements.
37.37	Xcel Energy	Disagree	R20.1 - The definition and level of detail for “communication paths” is needed. For example, does this include a commercial telephone carrier used to communicate between relays?R20.2 - Clarifying language is needed for “Establish an electronic

#	Organization	Yes or No	Question 37 Comment
			access point". Does this mean in documents, drawings, etc?R20.5 - This requirement needs clarification. Are these intended to be automatically generated alerts, such as logs? The current language could be interpreted to require a 12 hour review of a login attempted that failed due to an incorrectly typed login ID, as automated software may interpret this as an authorized login attempt. Also, 12/48 hours to complete a review of a failed unauthorized login attempt is unreasonable and unnecessary. R21.1 - We would like additional information on what type of "logical separation" is expected.
37.38	Ameren	Disagree	R20.1 - This will require use of a firewall at all locations or similar devices. Simply documenting this information is not practical for non routable devices. Also, clarify if communication paths, refer to physical equipment or locical paths. R20.2 - What is the difference between R20.2 and R20.3? Suggest combining the two requirements.R20.5 - 12 hours does not allow for weekends or for events that occur outside business hours. This should be increased to 24 hours or lowered to 24x7 (continuous). Also, need to clarify whether the alerts need to be reviewed during the time frame given (48 hours, 12 hours, or 7 days) or that alerts need to be sent every 48 hours, 12 hours, or 7 days. Please clarify how often should alerts be sent and how often do they need to be reviewed. R21.2 - Where does an RTU or serial communication fit into this requirement? Need to add more clarification on this requirement of what devices are included. R22 - Need to add requirements at a minimum for account listings, approvals, and access controls. There are no considerations for risk assessment or training for users of these devices. Also, these devices should be included in the Vulnerability Assessment.
37.39	US Bureau of Reclamation	Disagree	R20.2 should be modified to read "Establish an electronic access point on each routable protocol or dialup communication path between BES Cyber Systems." Define the use of "other devices" in this context. R20.4 - add "where feasible" to this requirement.R21.2 - Please provide and example...

#	Organization	Yes or No	Question 37 Comment
37.40	Entergy	Disagree	R20.5 Entergy cannot understand the reasoning behind the criteria of 12 hours? Why not 6 or why not 24?R21.1 is unclear and must be reworded to better reflect exactly what the SDT had in mind. We cannot guess at what that might have been.R22 - Entergy suggests R22 apply equally for high, medium and low assets; and thatthe requirements for processes and procedures in this section should be placed back into each of the respective sections (R14, 16, R18 and R23).
37.41	Western Area Power Administration	Disagree	R20.6 - Is this a requirement to review, and document the review, of logs weekly?R21.2 - Unclear. Does it mean our "one-way" rule from internal to external? Or does it mean use a proxy located outside the ESP?
37.42	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R20.6. With the obligation of reviewing alerts designated in R20.5 the requirement for manual review of logs should be extended to a 30 day window.
37.43	BCTC	Disagree	R22. Suggest just removing this requirement as it just references previous requirements
37.44	Hydro One	Disagree	Request clarification on “all communication paths” in 20.1 which can be every possible communication path between two end points.Recommend removing R21 because: o 21.1 is prescriptive in requiring Entity’s to segment their BES Cyber System o 21.2 is covered in 20.2Recommend removing R22 and move its table into the respective Requirements: o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23
37.45	ISO New England Inc	Disagree	Request clarification on “all communication paths” in 20.1 which can be every possible communications between two end points20.3 should be part of 20.2 - denys and explicit allows might be better language. R20.5 Please define what is an unauthorized access attempt. A user may be authorized but may try to connect using telnet where telnet is disabled. Is this considered unauthorized? Recommend

#	Organization	Yes or No	Question 37 Comment
			removing R21 because: o 21.1 is prescriptive in requiring Entity's to segment their BES Cyber System o 21.2 is covered in 20.2Recommend removing R22 and move it's table into the respective Requirements o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23R21.1 = question on what is "logical separation" very vague
37.46	Northeast Power Coordinating Council	Disagree	Request clarification on "all communication paths" in 20.1 which can be every possible communication path between two end points.Recommend removing R21 because: o 21.1 is prescriptive in requiring Entity's to segment their BES Cyber System o 21.2 is covered in 20.2Recommend removing R22 and move its table into the respective Requirements: o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23
37.47	Oncor Electric Delivery LLC	Disagree	Requirement 20.4, 20.5 and 20.6 are not applicable to some legacy cyber systems. These requirements should only be required for systems which utilize routable communication.Requirement 22 references other requirements and should be eliminated because it is redundant.
37.48	Garland Power and Light	Disagree	Requirement 20.6 - What we really feel is that this is impractical and should be deleted. However, it was stated at the NERC CIP workshop that the intent was to verify that the automated system capturing various logs off cyber devices was actually capturing each log - intent needs to be added to the requirement or wording changed to better express the intent at a minimum. Requirement 22 - Keep life simple - add the words "and Protective Cyber Systems" after the words BES cyber systems in each of the referenced requirements (14, 16, 18, and 23) and DELETE Requirement 22 - that way, everything is covered by the referenced requirements that this R22 uses
37.49	San Diego Gas and Electric Co.	Disagree	SDG&E feels that R20.1 is not clear. What is the point of documenting paths that transmit or receive digital information external to each BES Cyber System if they may not interface with other BES Cyber Systems? In addition, another observation from SDG&E related to R20.1 has to do with non-routable protocols. If this requirement

#	Organization	Yes or No	Question 37 Comment
			includes the documentation of non-routable protocols, it can become VERY expensive to document "chatty" protocols that broadcast to lots of assets (DHCP and BOOTP, to name just two examples).In R20.2, SDG&E asks for a clarification of the term "explicitly".SDG&E recommends grammatical changes for R20.4. We feel it should read "Document and implement one or more processes for logging all authorized remote access sessions and all successful and unsuccessful attempts of unauthorized access at each access point within the following time period. SDG&E suggests the following changes to R20.5: "Document and implement one or more alert processes that includes review of alerts by designated response personnel..." SDG&E feels that R21.1 is a bit confusing and worthy of discussion. If affected cyber systems and components are on the same network anyway, then what are the benefits of logical separation?
37.50	Allegheny Energy Supply	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection." (In general, using the existing terms where possible will cause much less confusion.)
37.51	Allegheny Power	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection."
37.52	EEI	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection."Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.For R 20.5: Document and implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.For R 20.6: Document and implement a process for

#	Organization	Yes or No	Question 37 Comment
			manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.R21: Suggest using electronic security perimeter rather than "System Boundary Protection."Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.There may need to be additional requirements for "Protective Cyber Systems" to include remote access controls, patch management, security event alerting, change control and change management.
37.53	Progress Energy (non-Nuclear)	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection." Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.Is the relay communications port for local interface with a laptop considered as an electronic access point? If so, this complicates these requirements.R20.1 by external to each BES system do you mean outside individual six walled boundaries?R20.6 is not needed, as long as we do R20.5.For 20.5 - Don't see the need for more than one capability.For 20.6 - change to "document process to ensure automatic monitoring and alerting process is working properly"CIP-011 - R20 - Are communications between Control centers and field RTUs/IEDs which do not employ routable protocols considered remote external communications?R20.6 - Need additional guidance as to what constitutes a manual review and the minimum sampling required.CIP-011 - R21 - Need clarification with guidance as to what constitutes "Cyber systems components in control Centers that are shared between BES Cyber Systems"

#	Organization	Yes or No	Question 37 Comment
37.54	Detroit Edison	Disagree	Table entries 20.4, 20.5, and 20.6 specify external connectivity only. This text is not necessary since the requirement is boundary protection and that implies external connectivity is the scope.
37.55	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS comments on this question, but also provides the following drafting suggestions:R20. Objective:To define an electronic security perimeter thereby minimizing the risk of system intrusion.R20. Requirement:Each Responsible Entity shall document and implement processes that establish electronic access controls point that incorporate the criteria in CIP-011-1 Table R20 - Electronic Boundary Protection. In R20 Table 20.2 we are concerned about the term "explicitly authorized communication." It is our assumption that a password is sufficient to comply with this requirement. If the drafting team intended another meaning we believe this will not be reasonable and we could not support this definition. We propose the following revised language:Table 20.2: Establish electronic access control on each routable protocol or dialup communications path between BES Cyber Systems and other devices.We recommend that R20 Table 20.4 should specify "at each electronic access point established in Part 20.2", similar to item 20.3. We recommend that R20 Table 20.5 should specify "at each electronic access point established in Part 20.2", similar to item 20.3. We recommend that R20 Table 20.6 should specify "at each electronic access point established in Part 20.2", similar to item 20.3. R21. Objective:To protect each BES Cyber System from other cyber systems by establishing protected boundaries between each cyber system and any shared components. R21. Requirement:Each Responsible Entity shall document and implement processes that incorporate the criteria in CIP-011-1 Table R21 - System Boundary Protection. The APPA Task Force supports the MRO-NSRS proposal to delete criteria in R21 Table 21.2. This is a redundant requirement and would put an entity in noncompliance of 2 requirements for one violation. The APPA Task Force recommends removal of R22. All of the criteria in Table 22.1 - 22.4 refer to previous requirements and will put an entity in noncompliance of 2 requirements for one violation.

#	Organization	Yes or No	Question 37 Comment
37.56	Bonneville Power Administration	Disagree	The objectives of these requirements ("to define an electronic security perimeter thereby minimizing the risk of system intrusion," "to protect each BES Cyber System from other cyber systems by establishing protected boundaries between each cyber system and any shared components," and "to protect each cyber system that establishes physical or electronic boundaries of BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirements rather than appearing at the end of the requirements (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R20Section 20.1 This is unacceptable. The requirement does not limit the extent of the documentation. Conceivably, it could require documentation of the entire Internet, if the BES Cyber Asset had direct or even indirect access to the Internet. The requirement needs to be limited. Recommendation: Remove the requirement. It is difficult to see how to write it in a way that encompasses all possibilities without leading to results such as the one described above. Instead, document external interfaces as part of the configuration management process.20.2: Requiring an electronic access point between a BES Cyber System and any other system produces unacceptable complication, latency, and administrative burden for a facility with multiple BES Cyber Assets in close proximity. As an example: 20.2 would require that all traffic from one BES Cyber System within a Control Center to any other system within the Control Center to go through a firewall or some other access control device. It is unlikely that this was the intent of the entry. Recommendation: Replace "Required" with "Required for external connectivity only", using the redefinition of external connectivity described above.20.3 Similar issue to 20.2 Recommendation: Replace "Required" with "Required for external connectivity only" throughout the table.20.4 - 20.6. Remove, the are already covered under 18.3 and 18.4. R18 and Table R18 require monitoring of all cyber security events, whether at access points or at BES Cyber Systems themselves.20.6. First, the requirement is already covered more clearly in Table R18. Second, it is unclear why a Electronic Boundary Protection requirement should be addressing BES Cyber Systems. Third, The intent is unclear,

#	Organization	Yes or No	Question 37 Comment
			due to the plethora of "ors" in the requirement. It could be that a manual review is always required, using sampled, sorted or filtered logs. It could also be that a manual view of logs is required, using sorted or filtered logs. It could also be that either a manual review or {sorted or filtered logs} is required. Part of the confusion is that filtering is clearly a method to sample, and sorting may be, as well. It would probably be better not to use those terms at all. In addition, there should be a provision to allow automated review of log entries. Recommendation: Delete the entry.Table R21Section 21.1 is completely unacceptable. It is quite possible in a Control Center for a single Dispatch workstation to provid access to several BES Cyber Systems. The requirement in 21.1 would make this impossible. The alternate would be to provide a separate workstation for each such system, which is unacceptable.Section 21.2 is acceptable only with externally connected redefined as described above.R22 and Table R22: These are references to other requirements. It seems that rather than referring to the other standards from this one, it would be cleaner to simply include this requirement as part of those other standards. That is, put the necessary references in R14, R16, R18 and R23.
37.57	Constellation Energy Control and Dispatch, LLC	Disagree	The timeframe in 20.5 for medium and high should be the same.
37.58	ReliabilityFirst Staff	Disagree	To eliminate confusion, we believe the drafting team should develop a definition for “protective cyber system”. We also believe that Table R22 should include an additional requirement stating, “Implement processes as specified in Requirement R15 - System Security.” and make this new requirement TFE eligible. Further, this new requirement should be “Required” for medium and High Impact BES Cyber Systems.
37.59	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
37.60	American Transmission	Disagree	We believe item 20.2 is going to set the stage for numerous TFE’s within the industry. Many devices (i.e., protective relays) do not support explicitly authorized

#	Organization	Yes or No	Question 37 Comment
	Company		communication.We believe items 20.4 - 20.6 should specify "at each electronic access point established in Part 20.2", similar to item 20.3. These items do not appear to be applicable for non-routable connections, and adding this language would assure they are limited to routable and dialup connections only.Items 21.1 and 21.2 use the term Cyber System Components, which is undefined. This term either needs to be defined, or replaced with BES Cyber System Components.Item 21.2 requires that all external communications flow through an electronic access point as established in R20. However, R20.2 only establishes electronic access points for routable and dialup connections. If an entity employs non-routable connections, these would not be defined under R20.2, and thus R21.2 would not allow the entity to communicate through them. We believe item 21.2 should just be deleted, as it seems to add nothing to the standard.
37.61	MRO's NERC Standards Review Subcommittee	Disagree	We believe item 20.2 is going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicitly authorized communication.We believe item 20.4 should specify "at each electronic access point established in Part 20.2", similar to item 20.3. This item does not appear to be applicable for non-routable connections, and adding this language would assure it is limited to routable and dialup connections only.We believe item 20.5 should specify "at each electronic access point established in Part 20.2", similar to item 20.3. This item does not appear to be applicable for non-routable connections, and adding this language would assure it is limited to routable and dialup connections only.We believe the following should be added to the end of item 20.6: "at each electronic access point established in Part 20.2". This item does not appear to be applicable for non-routable connections, and adding this language would assure it is limited to routable and dialup connections only. It also makes for a consistent approach with item 20.3.Items 21.1 and 21.2 use the term Cyber System Components, which is undefined. This term either needs to be defined, or replaced with BES Cyber System Components.Item 21.2 requires that all external communications flow through an electronic access point as established in R20. However, R20.2 only establishes electronic access points for routable and dialup connections. If an entity employs

#	Organization	Yes or No	Question 37 Comment
			non-routable connections, these would not be defined under R20.2, and thus R21.2 would not allow the entity to communicate through them. We believe item 21.2 should just be deleted, as it seems to add nothing to the standard.
37.62	The Empire District Electric Company	Disagree	We believe item 20.2 is going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicitly authorized communication.We believe items 20.4 - 20.6 should specify "at each electronic access point established in Part 20.2", similar to item 20.3. These items do not appear to be applicable for non-routable connections, and adding this language would assure they are limited to routable and dialup connections only.Items 21.1 and 21.2 use the term Cyber System Components, which is undefined. This term either needs to be defined, or replaced with BES Cyber System Components.Item 21.2 requires that all external communications flow through an electronic access point as established in R20. However, R20.2 only establishes electronic access points for routable and dialup connections. If an entity employs non-routable connections, these would not be defined under R20.2, and thus R21.2 would not allow the entity to communicate through them. We believe item 21.2 should just be deleted, as it seems to add nothing to the standard.
37.63	We Energies	Disagree	We Energies agrees with EEI: Suggest using electronic security perimeter rather than "Boundary Protection."We Energies agrees with EEI: Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.We Energies agrees with EEI: There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.We Energies agrees with EEI: Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: We Energies agrees with EEI: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.We Energies agrees with EEI: For R 20.5: Document and

#	Organization	Yes or No	Question 37 Comment
			implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.We Energies agrees with EEI: For R 20.6: Document and implement a process for manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. We Energies agrees with EEI: Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.We Energies agrees with EEI: R21: Suggest using electronic security perimeter rather than "System Boundary Protection."We Energies agrees with EEI: Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. We Energies agrees with EEI: R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.We Energies agrees with EEI: Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.We Energies agrees with EEI: There may need to be additional requirements for "Protective Cyber Systems" to include remote access controls, patch management, security event alerting, change control and change management.
37.64	GTC & GSOC	Disagree	We recommend rewording R21.1 to provide clear direction on what is expected to comply with this requirement because the wording is ambiguous. We are unable to suggest alternative language because we are not certain of the intent. If this requirement would prevent, for example, the use of a shared backup system for two Cyber Systems we do not see the reliability based justification for the requirement and would recommend its elimination.
37.65	Emerson Process Management	Disagree	What is the difference between "Electronic Access" in R20-R22 and the "Remote and Wireless Electronic Access" in R11-R13?

#	Organization	Yes or No	Question 37 Comment
37.66	Manitoba Hydro	Disagree	What is the meaning of "dial-up"? The wording for Requirement R20.2 is unclear. The suggested wording for Requirement 20.2 is "Establish an electronic access point that denies access by default and allows explicitly authorized communications on each routable protocol or dial-up communication path between BES Cyber Systems and other devices. Requirement R20.2 is inconsistent with Requirement R20.3. It is unclear how explicitly authorized communication is allowed without the implementation of access controls for Low Impact BES Cyber Systems. Requirement R20 does not contain any requirement for response to alerts. The wording for Requirement 21.1 is unclear. The suggested wording for Requirement 21.1 is "Cyber System Components that are shared between BES Cyber Systems must provide logical separation that prevents access between each system." and change the wording in the impact columns to "Control Centre Only". The wording for Requirement R21.2 is unclear. The suggested wording for Requirement R21.2 is "All external communication to the BES Cyber System must occur through an electronic access point as specified in Requirement R20." Requirement R22 is missing the requirement for the physical protection of the cyber system that establishes the physical or electronic boundaries of the BES Cyber System. There are no specifics given with respect to 'logical' separation in Requirement R21.1 so it is assumed to be at the Responsible Entity's discretion to determine.

38. Do you agree with the proposed definition of electronic access point? Please explain and provide any suggestions for modification.

Summary Consideration:

Many commenters agreed with the definition of Electronic Access Point, but other commenters requested clarifications in the definition. A number of commenters recommended changes to language concerning systems sharing an electronic access point. Some commenters suggested removing the sharing of electronic access points from the definition.

In response, the SDT has modified the definition of an **Electronic Access Point** to: *"An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets"*.

The sharing of electronic access points is likely not an issue because High Impact BES Cyber Systems are Control Centers and would rarely share an Electronic Access Point with Medium Impact BES Cyber Systems.

#	Organization	Yes or No	Question 38 Comment
38.1	WECC		Move to definition to beginning of the standard; dislike the definition box in the middle of a requirement. Make clear that access points can be anything that meets the definition and not only firewalls or devices specifically created for this purpose that must be put "in line". Ie. an Access Point can be the actual device itself providing access control.The phrase "where electronic access can be controlled" will prove difficult to audit. Inherently it allows an exception. All communication paths should be in scope regardless of the ability to control electronic access. It is not foreseen that communication paths could not be controlled.
38.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
38.3	NextEra Energy Corporate Compliance	Agree	Is a serial connection to a BES Cyber System considered an electronic access point? Please clarify in requirements.
38.4	Minnesota Power	Agree	Minnesota Power agrees with the proposed definition of electronic access point, but recommends replacing "All cyber systems sharing..." with "All BES Cyber Systems

#	Organization	Yes or No	Question 38 Comment
			sharing..."
38.5	Duke Energy	Agree	The second sentence is a requirement, not part of a definition; consider moving. Specify that "All cyber systems" only applies to BES Cyber Systems. This definition, particularly the concept of "sharing one or more common electronic access points or components" is much more practical in a power plant environment. See previous comments on R11, R12, R13.
38.6	Public Service Enterprise Group companies	Agree	There is general agreement, but need for clarification in the language in one regard. Please clarify whether this requirement would necessitate classifying a Distribution cyber system at a High Impact level if both the Distribution cyber system a High Impact BES cyber system at substation are interconnected using a single router/firewall device to a communications provider. I.e., effectively an additional router/firewall would be required in this situation to not entail classification of the Distribution cyber system at a High Impact level.
38.7	Consultant	Disagree	According to this definition electronic access point where electronic access cannot be controlled for communication paths that transmit and/or receive digital information would not be considered an access point?An access point should defined as locations where information crosses the established protection boundary, or as the locations where external connectivity or remote access occurs. An access point is not dependent on the ability to control the communication path. The sentence "All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s)." is a requirement. It is not a definition nor part of a definition. The concept is sensible, but still not a definition. Suggest moving this to the requirements table.Suggest modifying this definition to be consistent with "External Connectivity" and "Remote Access" definitions.

#	Organization	Yes or No	Question 38 Comment
38.8	Northeast Utilities	Disagree	Agree in principle with the definition but disagree that all cyber assets sharing the access point will be treated at the highest BES Cyber System impact categorization. This will have a big impact on development and test systems as well as other related but not critical systems. How will this impact DMZ systems which by design are not trusted?
38.9	Alliant Energy	Disagree	Alliant Energy agrees with EEI in that it is appropriate to apply protective measures to the literal ingress points (interfaces) on the electronic access points, but not the requirement to apply protective measures to all of the components that connect to said ingress interfaces (to require this creates a house of mirrors.)
38.10	E.ON U.S.	Disagree	CIP-011, R20.1 See previous comments regarding the definition of "external".CIP-011, R20.1 "Document all communication paths that transmit and/or receive digital information external to each BES Cyber System." Does this include the WAN if the defined BES Cyber System is inclusive of multiple sites/locations? All equipment and communication paths such as a Sonet ring?CIP-011, R20.3 The term "access control" should be further clarified. Does implementation of firewall rules alone limiting access as defined in R20.2 meet this requirement, or does this require further mechanisms to provide "access control" on an individual user-basis?CIP-011, R20.4, R20.5, R20.6 See previous comments regarding the definition of "external."CIP-011, R21.1 How might the logical separation called for here be implemented?CIP-011, R21.2 See previous comments regarding the definition of "external."
38.11	Progress Energy (non-Nuclear)	Disagree	Communication paths may be better defined by including routable protocol and/or 'external to the BES Cyber System'.Assuming this is the same as external access point it does seem somewhat repetitious.
38.12	American Electric Power	Disagree	Electronic access point for the purpose of this standard is defined as a point where electronic access can be controlled for communication paths that transmit and receive; or only receive digital information. All cyber systems sharing one or more

#	Organization	Yes or No	Question 38 Comment
			common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).Rational: An electronic access point that provides a transmit and receive path or a receive only path to a BES Cyber System provides an access path into the system to be used for possible exploit. By limiting traffic to transmit only communications the risk to the protected BES Cyber System is reduced since an electronic access point is not provided.
38.13	Entergy	Disagree	Entergy suggests adding specific language to the definition that includes "uses routable protocol or is dial-up accessible"
38.14	APPA Task Force	Disagree	In the APPA Task Force comments for Question 37 we proposed changing electronic access point to electronic access control. We do not feel it is necessary to define an electronic access point. We do believe it is necessary for entities to have control of their boundaries. We have proposed using electronic access control in R10, Account Access Control Specifications, in the place of the term Password since we feel there are other methods of controlling access that are equivalent or superior to password protection. We recommend the drafting team use electronic access control rather than defining another High Impact BES Cyber System outside of CIP-010-1.
38.15	Dairyland Power Cooperative	Disagree	In trying to be general, it adds more question as to the intent. Is an access point one a device physically connecting multiple communications paths? What about a terminal server? Is an authentication server or policy managing server an access control point even if it is not in-line with the path?
38.16	Constellation Energy Commodities Group Inc.	Disagree	Is the intent to require use of hardware firewalls? If so, is it possible to state that clearly? If not, what is the intent?
38.17	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggestion below:Suggest removing the requirement: "All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact

#	Organization	Yes or No	Question 38 Comment
			categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s)." from the definition of electronic access point. In addition, the requirement fails to recognize that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.18	LCEC	Disagree	Need to clarify the specific access point from an interface perspective. What is meant by the term controlling access? Is this from a network protocol perspective? Is a radio link that extends serial communications considered to be an access point?
38.19	Progress Energy - Nuclear Generation	Disagree	Not all EAPs constitute the highest degree of risk especially is nuclear facilities which are highly secure.
38.20	PacifiCorp	Disagree	PacifiCorp agrees with EEI's suggestion below:Suggest removing the requirement: "All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s)." from the definition of electronic access point. In addition, the requirement fails to recognize that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.Further, PacifiCorp believes the proposed definition is too broad. The preference would be to and should be restricted it to communications supporting routable protocols and or dial-up communication. In 20.2 the standard refers to the use of an access point on routable protocol and or dial-up paths but the definition is currently proposed to be broader. In plant control systems, we have many devices which use an IP routable protocol and an industrial communication control protocol such as fieldbus or profibus in the same device. The new definition would require each of these devices to be defined as an access point.
38.21	American Municipal Power	Disagree	Please provide a little or no impact category

#	Organization	Yes or No	Question 38 Comment
38.22	FirstEnergy Corporation	Disagree	Please provide clarification and examples on definition. Propose changing the second sentence to "All BES cyber systems sharing one or more common electronic access points or components will be logically separated such that each logical system is treated at its own categorization level or, where not separated, electronic access points will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s)."
38.23	Dominion Resources Services, Inc.	Disagree	Please see Dominion's response to Question 13. The interface between systems contained wholly within an access controlled facility should not constitute an electronic access point or be subjected to the Boundary requirements.
38.24	Southern Company	Disagree	R20.5 Is a single or double access attempt on a single access point required to be reviewed?
38.25	San Diego Gas and Electric Co.	Disagree	SDG&E has concerns about the last half of the proposed definition for electronic access points. If two medium or one medium and one low BES Cyber System share an access point, this definition makes the shared access point High impact? Regardless of other controls that may be in place? We feel that this definition is not reasonable.SDG&E suggests the definition of electronic access points should include the words "...between networks." Otherwise, every device on the network becomes an access point.
38.26	BGE	Disagree	Should include wording to clearly define the communication paths that transmit and or receive digital information to a BES Cyber System.
38.27	Allegheny Energy Supply	Disagree	Suggest removing the requirement: "All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s)." from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security

#	Organization	Yes or No	Question 38 Comment
			requirements.
38.28	Allegheny Power	Disagree	Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.29	EEI	Disagree	Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.30	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The concept of sharing access points must be better defined. Does connectivity to an outside entity at a firewall constitute a shared access point?
38.31	Luminant	Disagree	The definition of access points infers that cyber systems and BES Cyber Systems can share an access point but 20.2 states that BES Cyber systems must be seperated from other devices. re. Cyber systems protected by same firewall but in different zone
38.32	US Bureau of Reclamation	Disagree	The definition proposed is that "ALL cyber system sharing one or more common electronic access point or components..." Components can mean many things and almost all devices share components which have not impact on the BES. It would be better to indicate that "ALL BES cyber systems sharing one or more common

#	Organization	Yes or No	Question 38 Comment
			electronic access point or BES CYBER SYSTEM components...."
38.33	Constellation Energy Control and Dispatch, LLC	Disagree	The definition should clearly establish that the access point is a place where digital information is transmitted or received.
38.34	US Army Corps of Engineers	Disagree	The definition states that an electronic access point is a point where electronic access can be controlled for communication paths that transmit and/or receive digital information. What does "controlled" mean? Would network switches fall under this definition because network switch ports can be electronically controlled with port security?Suggest definition be changed to: An electronic access point is an electronic security point where traffic flowing from different security areas are restricted, controlled, and monitored from entering or leaving a particular security area. This may be restricting traffic from a lower security area (devices external to the BES Cyber System) from entering a higher security area (BES Cyber System.) It may also be restricting sensitive traffic from leaving a higher security area to a lower security area.
38.35	Bonneville Power Administration	Disagree	The first sentence, "Electronic access point for...digital information.", is acceptable, but only because it says what an electronic access point is, not where one has to be located. Second sentence is completely unacceptable, more so than anything else in the standard, for numerous reasons:First, it leads to the equivalent of CIP-007's including every network device within the Electronic Security Perimeter. In retrospect, that inclusion caused additional workload and costs which far exceeded the gain in security. To repeat that error would be totally unacceptable. The requirement should apply only to BES Cyber Systems, and not all cyber systems.Second, it ignores the level of threat posed by the various systems. Just because a cyber system or even a BES Cyber System is behind the same access point as a High impact BES Cyber System does not mean that poses the same risk to the BES, or even any risk at all.Third, it ignores the possibility of nested access point. For instance, consider systems A and B residing within a highly protected network and sharing a single access point. Add system C residing with a less protected network with an access point to the internet. If A and B access the internet through the same

#	Organization	Yes or No	Question 38 Comment
			access point that C uses, then C has to be treated as stringently as the highest impact of A or B.Fourth, applying impact levels based on the highest level of the BES Cyber System is a problematic issue that has been discussed at length. The mere fact that a cyber component exists within a High Impact BES cyber system does not make that specific component a high impact component. There are levels of impact that should be applied within and to the Cyber System. Devices or equipment (Components) within a High impact BES cyber system, may actually have little or no impact on that cyber system regardless of what happens to them. The standard that applies to that device should not necessarily be tied to the Impact rating for the whole BES cyber system.Finally, the second sentence is a statement of a requirement, not a definition. To use an example, assume a Control Center that relies on nested networks, with the outermost controlling external access, and further firewalls controlling access to their nested layers. The outermost firewall would be a common access point, shared by all systems within the Control Center. In that case, all the cyber systems would have to be treated as BES Cyber Systems at the highest impact level of any BES Cyber Systems in the Control Center. Such a treatment ignores the threat a system might or might not pose to the BES. To provide a somewhat absurd but demonstrative limiting case, a minimally functional print server residing in the outermost layer, barely able to accept an IP address, and having no connectivity except Ethernet on one side and a printer interface on the other, would have to be treated the same as an AGC system within the innermost layer controlling thousands of megawatts of generation at sites scattered across multiple states.Recommendation: Delete the second sentence.
38.36	Southern California Edison Company	Disagree	The requirement does not adequately address the technical nuances of virtualization. The central point of virtualization capability can be interpreted as the “shared” access point. At the same time, the centrally located virtualization device may also be interpreted as a BES critical cyber system. In the first case, the controls for the virtualization system will be those afforded to an access point, which may be less stringent than those afforded to a BES critical cyber system. In the second case, where the virtualization device is a BES critical system, on the user end, end user computing devices such as mobile laptops can potentially be considered as BES cyber system

#	Organization	Yes or No	Question 38 Comment
			component, and on the SCADA end, automation devices would be considered as BES cyber system components. Requirement R21 does not make drawing such distinctions clear of subjective interpretation.
38.37	Oncor Electric Delivery LLC	Disagree	The term “public communication paths” should replace “communication paths”. Systems which are isolated from the internet are less susceptible to cyber attacks.
38.38	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
38.39	Xcel Energy	Disagree	We believe the second sentence places an unnecessary burden on lower impact systems if they are unable to communicate with the higher impact system, as is the case with dial-up based systems.
38.40	We Energies	Disagree	We Energies agrees with EEI Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.41	US Army Corps of Engineers, Omaha Distirc	Disagree	What does "controlled" mean? Definition also appears to contain a requirement "All cyber systems sharing one or more . . " The requirement doesn't appear to be in line with industry practice. A firewall can protect 2 or more networks from external connections and from each other. Both networks do not have to be at the same sensitivity level. suggest definition be changed to:An electronic access point is an electronic security point where traffic flowing from different security areas are restricted, controlled and monitored from entering or leaving a particular security area. This may be restricting traffic from a lower security area (devices external to the BES Cyber System) from entering a higher security area (BES Cyber System.) It may

#	Organization	Yes or No	Question 38 Comment
			also be restricting sensitive traffic from leaving a higher security area to a lower security area.

39. Tables R20 to R22 provide direction concerning what impact level of BES Cyber Systems to which Requirements R20 to R22 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Many commenters disagreed with the proposed BES Cyber System impact levels and made suggestions to clarify them, including suggestions to revise or refine the impact levels based on the particular characteristics of the BES Cyber Systems involved. In response, the SDT has made changes to include an applicability column in each table for each requirement. The applicability column further refines the set of BES Cyber Systems and assets to which each part of the requirement must be applied. For example, the SDT made changes to the applicability column to include the scoping filter of External Routable Connectivity where the use of a routable connection would be required to comply with the requirement, such as the requirement to have Electronic Access Points.

The intent of this approach is to refine the scope of requirements that apply to each type of BES Cyber System or device based on its characteristics. The drafting team recommends that commenters carefully review the proposed applicability column in the table for each requirement in the CIP Version 5 standards.

#	Organization	Yes or No	Question 39 Comment
39.1	US Army Corps of Engineers		The statement in Table R21, 22.1 "Cyber system components that provide external communication to the BES Cyber System must only communicate externally through an electronic access point as specified in Requirement R20.", is confusing. What is the standard trying to say here?
39.2	GE Energy	Agree	20.2: Low BES systems should be required to document and implement access controls.
39.3	Black Hills Corporation	Agree	21.1 requires further definition of logical separation requirements in a disaster recovery scenario. As stated, this does not allow for control centers to back-up each other in a fail-over mode for disaster recovery.
39.4	Duke Energy	Agree	Agree if the external connectivity is via a shared electronic access point as discussed in previous comments.Apply all requirements, where currently in place, only for external connectivity. 20.6: Review of logs every 7 days is not practical.21.2: Only

#	Organization	Yes or No	Question 39 Comment
			require for external connectivity
39.5	Progress Energy (non-Nuclear)	Agree	See comment 14.
39.6	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
39.7	GTC & GSOC	Agree	We recommend a slight rewording of R20.2 as follows "Establish an electronic access point that denies access by default and allows explicitly authorized communication on each path where a routable protocol or dialup communication exists between BES Cyber Systems and other devices."
39.8	E.ON U.S.	Disagree	: E.ON U.S. does not believe there is a need for compliance requirements for low impact systems. High Impact has such a short timeframe for revocation, that it would require employees be available to revoke privileges 24/7. The SDT should adopt a more reasonable time frame- at least 24 hours. E.ON U.S. believes that R22 is merely a repeat of other requirements and therefore should be deleted
39.9	NextEra Energy Corporate Compliance	Disagree	: NextEra believes it is unclear what the timeframes for Medium Impact and High Impact BEST Cyber Systems are supposed to mean. Do response personnel have to review security logs related to external connectivity every 48 hours or are the expectation for designated personnel supposed to respond to an alert within a 48 hour period? The recommendation is to document and establish one or more processes for automated alerting and response to alerts by designated response personnel for unauthorized access attempts at each electronic access point. This requirement would be applicable to both Medium and High Impact BES Cyber Systems. If automated alerting and notification is not technically feasible, Responsible Entities should be able to develop a process to manually review security logs to determine potential cyber security incidents.

#	Organization	Yes or No	Question 39 Comment
39.10	Regulatory Compliance	Disagree	20.1 STRIKE "Required for Low Impact20.5 Propose - 72 hours for Medium Impact Propose - 48 hours for High Impact21.1 - STRIKE "required" for Medium Impact
39.11	BGE	Disagree	20.5 timeframe should be consistent for medium and high.
39.12	Florida Municipal Power Agency	Disagree	22.2 - Add medium, require low to asses quarterly. Consider high impact to review 'critical' patches within 7 days.22.3 - This should be consistent with R18; medium should be required to monitor their systems. Low should review logs at least quarterly for events, or at least have an automated system in place to alert for specific threats.
39.13	ERCOT ISO	Disagree	22.2-22.3: Should apply to Medium Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
39.14	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
39.15	The Empire District Electric Company	Disagree	Comments: For items 20.4 - 20.6, we believe "for external connectivity only" should be removed from the impact levels to properly coordinate with the comments on these items made under question 37.
39.16	Progress Energy - Nuclear Generation	Disagree	Durations should align with information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
39.17	EEI	Disagree	EEI recommends deleting R21 because it is vague and the risks are addressed in R20. Introducing boundaries within engineered systems will result in decreased reliability.
39.18	Entergy	Disagree	Entergy suggests making R20.3 and R20.4 apply to low impact assets.

#	Organization	Yes or No	Question 39 Comment
39.19	MRO's NERC Standards Review Subcommittee	Disagree	For items 20.4 - 20.6, we believe “for external connectivity only” should be removed from the impact levels to properly coordinate with the comments on these items made under question 37.
39.20	US Army Corps of Engineers, Omaha Distirc	Disagree	Intent of 22.1 is unclear
39.21	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
39.22	Luminant	Disagree	Low impact BES Cyber Systems should be protected but not have to be seperated from all other cyber systems. re introduces the concept of cyber systems in "ESP". R21 How can cyber systems be shared and not be a BES Cyber System
39.23	LADWP	Disagree	Low impact requirements will become an administration issue.
39.24	Minnesota Power	Disagree	Per the discussion regarding these tables in Question 37, Minnesota Power recommends that for Parts 20.1, 20.2, 21.2 and 22.1 “Required” be removed for Low Impact BES Cyber Systems.
39.25	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation ‘Required for external connectivity only’. In 20.5, aligning the time requirement on 48 hours for clarity and consistency.
39.26	American Municipal Power	Disagree	Please provide a little or no impact category
39.27	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12. Table 13, Table 14, and Table 22. Puget Sound Energy suggests including wording similar to Table 11: “Required for external connectivity only”.
39.28	FirstEnergy Corporation	Disagree	R20 - Timeframes should not be in ‘hours’ (i.e. less than a full day). Tracking by time

#	Organization	Yes or No	Question 39 Comment
			rather than days would not be logistically possible on all systems and compliance could not be maintained.The new requirements now have too many different time frames to meet. Again, not logistically possible on all systems and compliance could not be maintained for larger utilities.R21 - R21.2 - Remove 'Required' for Low Impact Cyber Systems.R22 - Eliminate - see Q37 above.
39.29	Con Edison of New York	Disagree	R20 dialog box; speaks to inheritance of HIGH Impact BES requirements for all cyber systems with shared access points.o Does the inheritance only apply to R20 requirements or does this mean all requirements for these devices would be at the High Impact level?o If all cyber systems regardless of BES use that are within the same boundary require High, this may cause significant manpower or create the need to isolate the true BES systems. The isolation will take significant time to plan and implemento This standard must allow the use of 1 physical firewall, logically separated to isolate networks without inheritance of BES levelR21.1 does this require Cyber Components on the same isolated network be logically separated? Is that correct?o This should not apply to devices on the same network.o Should only be required for high.R20.6 - if automated review and alerting is used this should not be requiredR22 mentions established physical boundaries --- the draft CIP standards do not mention physical boundaries are the PSP requirements defined in this version?
39.30	Southwest Power Pool Regional Entity	Disagree	R20: Distinction between external and non-external connectivity is not appropriate. R22: Patch management should be applicable to all impact categories.
39.31	Hydro One	Disagree	Recommend that 20.4 and 20.5 should be Required instead of specifying "external connectivity" since the criteria limits the scope to remote access. Also recommend removing "within the following time period" from 20.5.Recommend that 20.6 be re-worded to be consistent with FERC Order 706 paragraph 526 - "Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs."Recommend that 20.6 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommended removing R21 in the response to

#	Organization	Yes or No	Question 39 Comment
			Question 37.Recommended moving the R22 criteria in the response to Question 37. The moved 22.2 and 22.3 should apply to Medium Impact BES Cyber Systems as well.
39.32	ISO New England Inc	Disagree	Recommend that 20.4 and 20.5 should be Required instead of specifing "external connectivity" since the criteria limits the scope to remote access. Also recommend removing "within the following time period" from 20.5Recommend that 20.6 be re-worded to be consistent with FERC Order P526 - <<Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs. >>Recommend that 20.6 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven daysRecommended removing R21 in the answer to question 38Recommend moving the R22 criteria in the answer to question 38. The moved 22.2 and 22.3 should apply to Medium Impact BES Cyber Systems as well.
39.33	Northeast Power Coordinating Council	Disagree	Recommend that 20.4 and 20.5 should be Required instead of specifying "external connectivity" since the criteria limits the scope to remote access. Also recommend removing "within the following time period" from 20.5.Recommend that 20.6 be re-worded to be consistent with FERC Order 706 paragraph 526 - "Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs."Recommend that 20.6 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommended removing R21 in the response to Question 37.Recommended moving the R22 criteria in the response to Question 37. The moved 22.2 and 22.3 should apply to Medium Impact BES Cyber Systems as well.
39.34	National Grid	Disagree	Refer to comments in Q. 37.
39.35	Oncor Electric Delivery LLC	Disagree	Requirement 20.6 should provide for a review every 30 days.
39.36	US Bureau of	Disagree	Requirement 22.1 conflicts with earlier requirements regarding controls on remote

#	Organization	Yes or No	Question 39 Comment
	Reclamation		and wireless access.
39.37	San Diego Gas and Electric Co.	Disagree	SDG&E feels that too many classifications make compliance more difficult and likely more risky. We would suggest making the time in R20.5 24 hours for both High and Medium impact systems.SDG&E also feels that instead of using the word “impact” for these Requirements, apply a concept of “risk” for inclusion. We would want to identify the risks with associated systems security and protect accordingly.
39.38	LCEC	Disagree	See previous comments
39.39	Bonneville Power Administration	Disagree	See Question 37, above.
39.40	Constellation Energy Control and Dispatch, LLC	Disagree	See response to question number 37.
39.41	ReliabilityFirst Staff	Disagree	Suggest “30 calendar days for external connectivity only” for Medium Impact in row 20.6. Suggest “Required” for Medium Impact in rows 22.2. and 22.3.
39.42	Ameren	Disagree	Suggest removing R21.2 from Low Impact Systems.
39.43	Alberta Electric System Operator	Disagree	Table R20 - For 20.5 set Low Impact to “120 hours for external connectivity only”; for 20.6, set Medium Impact to “30 calendar days for external connectivity only”Table R22 - Consider making 22.1, 22.2, 22.3, 22.4 Required for all Low, Medium, and High Impact BES Cyber Systems because they are protecting the boundary.
39.44	Consultant	Disagree	The impact levels would be impacted by previous comments on this group of requirements.The terminology "for external connectivity only" is redundant as the access point is where external connectivity occurs. Suggest removing these words from the table where they occur.

#	Organization	Yes or No	Question 39 Comment
39.45	Southern California Edison Company	Disagree	The standard should read such that the centralized/federated primary virtualization system and its back-up are afforded protections commensurate with the impact level of the automation devices that support a particular reliability function. The standard should comply with the intent of Order 706 to prevent intentional or accidental misuse of BES components and limit BES cyber system classification to the automation nodes and virtualization nodes. End-user computing devices in a virtualization system should be classified as conduits to the virtual system that is protected by an electronic border.
39.46	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The time frame for requirement 2.5 would be difficult to comply with for smaller entities.
39.47	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R20 - R22 if our changes proposed in Question 37 are accepted:R20 Table 20.1: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.2: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.3: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.4: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.5: Low Impact: N/AMedium Impact: 48 hoursHigh Impact: 12 hoursR20 Table 20.6: Low Impact: N/AMedium Impact: N/AHigh Impact: 7 calendar daysR21 Table 21.1: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR21 Table 21.2: (Removed)R22 Table 22.1 - 22.4: (Removed)
39.48	MidAmerican Energy Company	Disagree	While the concept of applying various levels of security controls to BES Cyber Systems based upon their impact level appears to be appealing, until the assessment of each BES Cyber System is made by a utility and the catalog of security controls that must be maintained for each BES Cyber System is understood, the impact level strategy cannot be accessed.

#	Organization	Yes or No	Question 39 Comment
39.49	PacifiCorp	Disagree	While the concept of applying various levels of security controls to BES Cyber Systems based upon their impact level appears to be appealing, until the assessment of each BES Cyber System is made by a utility and the catalog of security controls that must be maintained for each BES Cyber System is understood, the impact level strategy cannot be accessed.

40. The configuration change management requirement is centered on the identification of a component inventory and baseline configuration. Do you agree with the list of criteria that are included in the baseline configuration? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the baseline and managed through the configuration change management process? Do you agree with the list of criteria that are included in Requirements Table R23? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in Table R23? Please explain and provide any suggestions for modification.

Summary Consideration:

Commenters are concerned about a lack of clarity on what is expected for a baseline configuration, and if it should be applicable to an entire BES Cyber System or to individual components. Commenters also expressed a lack of understanding on how detailed inventories should be and to what category they should apply. Many comments addressed the requirements that include component-based actions for low-impact BES Cyber Systems. These are viewed as potentially overwhelming in the overall CIP compliance process. Also, identifying the physical location of a virtual component is identified in several comments as "confusing." Concerns were also identified about the definitions and clarification around terms. For example, what is meant by "Other documentation," "baseline configuration," and "virtual BES Cyber System component" were the primary terms mentioned. Also, more specific information on "security controls" was requested.

This requirement has been moved into a new standard, CIP-010-1 -- Cyber Security — Configuration Management and Vulnerability Assessments. In response to stakeholder comments, the drafting team has provided additional guidance in the 'Application Guidelines' section for the standard regarding the elements of a baseline configuration. The requirement to have an explicit inventory has been removed. This requirement is effectively inferred by the requirement to document a baseline configuration. The drafting team also agrees that maintaining an inventory for all Low Impact BES Cyber Assets within the current compliance framework in which the NERC CIP standards exist is problematic. As such, the drafting team has made an effort to prioritize controls for Low Impact BES Cyber Assets that don't require the documentation of every individual component and may be managed on a site-by-site basis, where feasible.

Several commenters suggested that inventories and monitoring should also apply to Medium and High Impact categories, since impact of the Low category to the BES Cyber System is minimal, and the effort appears to be greater than the benefit. In addition, there are questions on the timeframe and processes for monitoring. Does it need to be real time or can the Responsible Entity establish a tailored schedule for response to the detection of unauthorized changes? With regard to Requirement 23, Part 23.2, several commenters stated that it was written around typical IT equipment configurations and not the multitude of devices within generating or transmission facilities. They believe that because of this situation, the requirement should be limited to control centers similar to Requirement 23, Part 23.6. They further state that for generating facilities and substations, it would be adequate to require the entity to document and implement one or more processes for configuration change management, and that this would be applied to all Low Impact, Medium Impact, and High Impact BES Cyber Systems.

The drafting team intends for the monitoring and alerting capabilities to occur on a near real-time basis. The drafting team appreciates the concerns regarding substation and generation environments and believes that tools to perform these processes on a near real-time basis in these environments are either too immature to be included as part of a mandatory standard or simply do not exist, particularly since a large number of these cyber assets have no external communication method. Additionally, the drafting team believes that other NERC reliability standards, such as those regarding protective relay maintenance and testing, provide some level of mitigation for this lack in currently available technology.

The configuration management requirements state that an inventory must be developed of the physical or virtual BES cyber components "excluding software running on the component". Several commenters questioned why software should not be considered as constituting a "virtual" BES cyber component. Many comments were also submitted on what is perceived as a cumbersome process around inventory, monitoring, and responding to changes in the baseline configuration. They state that the criteria should be simplified, with items such as removing "physical location" from the requirement.

The drafting team has attempted to address these concerns by modifying the impact levels to which they apply. The drafting team, however, continues to believe that a rigorous configuration management program, including documented baseline configurations, is essential to an effective cyber security program.

#	Organization	Yes or No	Question 40 Comment
40.1	USACE - Omaha Anchor		23.2 - clarify "software" - is this all software on the machine or version of the OS?
40.2	US Army Corps of Engineers		Does requirement R23.7 "Monitor changes to the baseline configuration and respond to the detection of any unauthorized changes" imply or require automated monitoring?
40.3	WECC		Not sure that baseline is the right word to use as many entities define baselines only at specific times in implementation projects or as part of system hardening. Item 23.5 says to "assess potentially impacted security controls" then Item 23.6 says to test them. Is this the same requirement? The second bullet in 23.6 is very difficult to read. Consider having a separate requirement for 1) Change Management Criteria, 2) Testing Criteria, 3) Test Environment Criteria.Virtualization is mentioned in 23.1. This is good, but should probably be considered in other requirements as well. In 23.2 an inventory is required of components. Based on the current definition of component,

#	Organization	Yes or No	Question 40 Comment
			this would not need to be done down to the device level; however, management at the device level is needed for effective application of change management.In 23.6 there does not appear to be a provision for changes to the baseline configuration itself. Also, the requirement for established procedures was removed. This will lead to inconsistent testing and makes auditing much more difficult.
40.4	Exelon Corporation	Agree	Exelon seeks clarification on the following questions. Do Requirements 23.2 and 23.4 include relay and SCADA equipment settings and settings changes? Would documentation of an assessment be required in a test environment before each and every relay or SCADA setting change?
40.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.There is no process to identify when any changes made to the BES might affect the actual identification of the BES component(s) as a new impact rating.FMPA does not believe that a Responsible Entity will be able to fully comply with some of these standards as they are written. For example, to fully assess how a change might impact the BES Cyber System could be interpreted to mean the RE would need a fully functional replicated copy of the production environment. FMPA does not believe this is reasonable.
40.6	Progress Energy - Nuclear Generation	Agree	R23 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
40.7	CWLP Electric Transmission, Distribution and Operations Department	Agree	R23.5. What are the ramifications to the Responsible Entity if the assessment is inaccurate and a change does adversely affect the BES Cyber System? Conducting an assessment does not guarantee success as there are always unforeseen incidents that may impact upgrades and new installations.
40.8	Xcel Energy	Agree	We believe additional guidance is requires as to what type of monitoring is expected

#	Organization	Yes or No	Question 40 Comment
			in R23.7. Is active monitoring expected, or periodic review of logs sufficient?
40.9	Dairyland Power Cooperative	Disagree	23 Note that on many SCADA systems, the simple matter of summing two telemetered values may require the modification of software/scripts. For simple calculations such as these the overhead of change control and security track will serious slow the process of making adjustments during a field checkout. Are there any further criteria that can be used to minimize the overhead on changes that are not reasonably expected to impact security posture?
40.10	FirstEnergy Corporation	Disagree	23.1 - Should also exclude data.23.2 - Cyber System Components is used two different ways in 23.1 and in 23.2. And neither uses really match the definition provided in CIP 010. What is expected for a baseline configuration for an entire BES Cyber System as opposed to a configuration for an individual component?23.3 - Change 30 days to 90 days. Remove 'other documentation as necessary' or be more specific as to what that means.23.2 - 23.4: Is the standard requiring the Responsible Entity to update the baseline documentation every time a patch is applied?
40.11	Dominion Resources Services, Inc.	Disagree	23.1 & 2 & 3(inventory only). It should be clarified that the inventory is for in-service equipment and that location refers to an area or room and not to a rack or slot. 23.4. A definition of "Authorize" should be provided.23.5. At the May workshop, an entity said they were audited by 2 regions and each region had a different definition of what cyber security controls were. On this point Dominion recommends that the word "Assess" be changed to "Define cyber security controls and assess." 23.7 Dominion is unclear how this requirement can be met. For example, an alarm is received when a relay is placed into "configure" mode, but there is no ability to see what is being changed. Stated differently, Dominion can respond to a change, but cannot monitor what is being changed. If the relay is in a remote location, Dominion's response time will be impeded. This is the best case scenario. Much equipment does not alarm when its configuration has been changed (e.g., a computer does not generate an alarm when a new program is loaded.) Dominion requests that this requirement be

#	Organization	Yes or No	Question 40 Comment
			removed.
40.12	BGE	Disagree	23.2 custom software/scripts should not be part of the baseline inventory. Recommend having 1 inventory for Low, medium and High.
40.13	American Electric Power	Disagree	23.3: Regarding "Authorize and document changes to the BES Cyber System that deviate from the existing inventory and update the inventory and other documentation as necessary within 30 days of the change being completed", what changes must be authorized and documented? Is this targeting physical network changes or adding/deleting equipment? Is this targeting software changes?23.7: Regarding "Monitor changes to the baseline configuration and respond to the detection of any unauthorized changes", is this a continuous monitoring requirement? If not, what is the frequency that a comparison between the actual and latest approved baseline be conducted? Comparing baseline to existing configurations would be a manual process is most instances. Suggest rewording to specify that this will be conducted on the individual BES Cyber System components at some frequency, possibly quarterly.
40.14	Regulatory Compliance	Disagree	23.4 - propose adding - "Authorize and document changes that present a high risk to the BES....23.4a - additional criteria - Entity documents changes into categories of risk, based on the risk assessments determines if changes are in or out of scope.23.7 - unreasonable expectation based on the definition of baseline configuration. Instead propose the following: Do an annual review, recapturing the baseline configuration. Review for unauthorized changes during this process. If unauthorized changes are found remediate and document within 60 days of the documented annual review.
40.15	Southwest Power Pool Regional Entity	Disagree	23.5: Clarify what is meant by “deviation from the existing baseline configuration.” A new or replacement BES Cyber System Component needs to be validated before placing into service even if it uses an existing baseline configuration if for no other reason than to verify the configuration as built matches the baseline. Additionally, “potentially impacted cyber security controls” is highly subjective and open to

#	Organization	Yes or No	Question 40 Comment
			interpretation. Remove the "potentially impacted" language. 23.6: "included in the baseline configuration of the BES Cyber System" has a vendor baseline connotation. Consider clarifying to refer to the currently approved configuration of the production BES Cyber System. Additionally, the criteria need to clarify just what is meant by "baseline configuration." Does this mean the currently approved hardware and software, including versions or release levels? Or is it less granular, such as "a server running Linux and EMS/SCADA software." Without the clarification, the term is open to interpretation and the ability to audit will be affected.
40.16	MidAmerican Energy Company	Disagree	23.7 Most entities do not have the capability, resources or tools currently to live monitor configuration changes on all category A devices. There could be impacts to performance to run agents on equipment and some vendor supported devices may not allow live monitoring.
40.17	BCTC	Disagree	Â R23. Define in more explicit terms the definition of a "baseline configuration" - what comprises a baseline config - i.e. patch level, etc. R23.6. There are expected to be scenarios whereby a test environment may not exist for a high impact BES Cyber System. In such cases would a scenario like rolling out changes to a non-critical environment represent a test environment from a compliance perspective?
40.18	Southern Company	Disagree	As long as there are requirements which include per-component action for each low-impact BES Cyber System, the effort needed to implement those actions will overwhelm the rest of the CIP compliance effort. With 100's of low impact BES substations, there are 1000's of BES Cyber System components. These substation devices are being changed daily. The documentation requirements of R23 are overly burdensome with little benefit for low impact BES Cyber Systems. We recommend removing Low Impact BES Cyber Systems from all R23 controls.
40.19	E.ON U.S.	Disagree	CIP-011, R23.1 The requirement states that an inventory must be developed of physical or virtual BES CSC's excluding software running on the component. What

#	Organization	Yes or No	Question 40 Comment
			constitutes a "virtual" BES CSC if not software?
40.20	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
40.21	Constellation Energy Commodities Group Inc.	Disagree	Clarify R23 to not require tracking of routine changes within the container of existing software (example, add a point or change data type of a point), but to track code migrations and changes to the baseline of deployed components.
40.22	The Empire District Electric Company	Disagree	Comments: This requirement, especially evident in item 23.2, appears to be written around typical IT equipment, and not the multitude of electronic programmable devices an entity will encounter in the field at a generating facility or substation. Therefore, we believe the current intent of this requirement should only apply to control centers, similar to item 23.6, where typical IT equipment is becoming more of the standard.For generating facilities and substations, we believe it would be adequate to require the entity to document and implement one or more processes for configuration change management, and this would be applied to all Low Impact, Medium Impact, and High Impact systems.
40.23	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy disagrees with the list of criteria in the baseline configuration. Maintenance of such a list including, software versions, active ports and services, any patches and custom software/scripts will be burdensome and subject to unintended error as the list will contain a significant number of entries. CenterPoint Energy is unsure of the value of such a list regardless of R23 assertion that it is meant "...to prevent and detect unauthorized modifications to BES Cyber Systems." Unless such a list is reviewed on a daily basis, or perhaps even more often, there is no "detection" involved. As to "protection", CenterPoint Energy fails to see where that would occur from the development of and maintenance of such a list. CenterPoint Energy does understand the need to maintain current configuration data, however this criteria is too prescriptive.

#	Organization	Yes or No	Question 40 Comment
40.24	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Having a hard time with the idea of documenting the physical location of the cell phone described in question 1.a, and with documenting every change in its location within 30 days of every move.
40.25	Progress Energy (non-Nuclear)	Disagree	If the BES Cyber System Component is a microprocessor relay/device, this can get complicated. These devices have numerous 'configurations' based on an application. Also, firmware versions would need to be considered. Today, most utilities lock firmware on many relay models. Another issue may be when a cyber component is returned to a manufacturer for repair - how do we verify that a replaced operating system component is compliant.R23.2 need to be explicit that the baseline is the inventory in existence at compliance time for existing systems.R23.7 in most existing generating plant systems would not be able to meet this requirement and the value is questionable since the use of administrator accounts is highly restricted by multiple other requirements.CIP-011 - R23 - Need clarification as to what constitutes a "virtual BES Cyber System Component".
40.26	Midwest ISO	Disagree	It is not clear how R23 inventories differ from those inventories that must be identified in CIP-010 R2. To the extent that these are duplicate, the duplications should be eliminated.
40.27	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
40.28	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R23, but recommends changes as follows: o For Parts 23.1 and 23.2, Minnesota Power recommends that Standards Drafting team define what constitutes a "Virtual BES Cyber System Component." o Regarding Part 23.2, Minnesota Power recommends that the Standards Drafting Team further define the level of software versions are required for tracking purposes. For example, an EMS has hundreds of small programs that make up the system. Each of these individual programs is combined under an

#	Organization	Yes or No	Question 40 Comment
			overall version number. In addition, different Registered Entities, with the same EMS version, may have different internal applications with different levels of fixes. To what level should those be documented? o For Parts 23.5 and 23.6, Minnesota Power recommends that the Standards Drafting Team define the term “cyber security control.” o For Part 23.6, what constitutes a “deviation?” What level of baseline is required? o Regarding Part 23.7, Minnesota Power requests that the Standards Drafting Team consider defining the term “monitor” and identify the level of detail required for these changes. For example many EMS sub-programs constantly create/modify/remove files as a normal course of business. Would these changes need to constantly be reviewed and verified?In general, Minnesota Power believes that the list of items to be tracked/tested/monitored is vague and could cause Registered Entities to incorrectly implement processes to satisfy this Requirement.
40.29	NextEra Energy Corporate Compliance	Disagree	Nextera believes there is not an agreement for the list of criteria that should be included in the baseline configuration, the requirement is a big undertaken to manage the software on BES Cyber Systems and provides little improvement to the reliability of the BES Cyber Systems.The following is the recommended updates:23.2 - Develop a baseline configuration of the BES Cyber System, which shall include an inventory of its physical or virtual BES Cyber System Components (excluding software running on the component), physical location, active ports and services, any patches, and any custom software/scripts.Keeping inventory on running software on medium and high impact BES systems will be a big undertaken. With the other levels of controls to develop baseline configurations, software should be excluded.In 23.7, this implies implementation of automated tools to detect configuration changes. Not all systems will support these tools. If not possible to automate, are manual processes acceptable? If so, wording should specify "automatic or manual detection".
40.30	LCEC	Disagree	No. The baseline configuration is not specific enough and leaves much open to interpretation.

#	Organization	Yes or No	Question 40 Comment
40.31	National Grid	Disagree	o National Grid suggests rewording 23.5 - "Assess changes to baseline configuration to verify controls are not adversely affected ..." o 23.6 - Need more information on testing requirements. o23.7 - Expand on "monitor changes". Is the SDT considering a timeline to respond to detection of any unauthorized changes o National Grid recommends the SDT to check the new EOP Backup Facility Standard for testing in 23.6
40.32	PacifiCorp	Disagree	PacifiCorp seeks clarity on 23.2 as to the 'components'. In the case of a server, is this every component in the case (including fans?) or additionally all apparatus which are directly attached (Mouse, Keyboard etc) which would not normally be included in a change record.
40.33	RRI Energy	Disagree	Part 1: does "active ports and services" refer to the network accessible ports and services as mentioned in the above requirement 17.1?Part 2: Some application uses port ranges. Netstat command only reports actively listening port(s). The requirement explicitly states "active ports and services". Some ports in the port ranges may not be active when the netstat command runs. So when the inactive ports are not in use, depending on the vendor/program, entity could be out of compliance. Active could be replaced with "Active or documented system design ports and services".What does "closely models" mean?Is a "test environment" an actual thing or a state? Example: a generation unit is online generating x MWs - no test environment "state' exists due to the unit being online; a generation unit is in a 2 week maintenance outage, all cyber assets related to the unit are in a test environment "state".
40.34	Northeast Utilities	Disagree	Please clarify 23.7. Specifically, does this monitoring need to be automated? If not, how often will the monitoring need to be performed to meet the standard?
40.35	Network & Security Technologies Inc	Disagree	R23 - Sound configuration change management practices can minimize the risk of unauthorized modifications but cannot "prevent and detect" in all instances. Suggest

#	Organization	Yes or No	Question 40 Comment
			revising the overall goal here.23.6 - Suggest adding a provision allowing a Responsible Entity to suspend this requirement under emergency conditions (e.g., to apply an emergency hot fix needed to restore a disabled or impaired BES Cyber System).23.7 - Absent the use of automated tools, this may be a very hard requirement for Responsible Entities to meet. Suggest SDT consider reasonable approaches to how it might be done on a manual basis (e.g., periodic comparisons of running configurations and stored configuration profiles) without imposing an undue burden on Responsible Entities with large numbers of High Impact systems and no current investment in automated monitoring.
40.36	Consultant	Disagree	R23. The terminology "incorporate the criteria" seems incorrect. The table is actually listing the requirements. Suggest changing to "incorporate the requirements".Table R23 - Item 23.1 The terminology "virtual BES Cyber System Components (excluding software running on the component)" seems confusing. Software would seem to be the 'virtual' component, so if software is excluded then the 'virtual' aspect seems unnecessary. Please clarify the intent of this requirement. Item 23.1 The "physical location" of a "virtual component" does not appear to make sense. Suggest rewording to specify physical location of hardware. Item 23.1 & 23.2 Qualification of "physical or virtual" components should be unnecessary. The defined term 'BES Cyber System Component' should be the basis for the requirement. Adding these qualifiers implies that the definition is not adequate. Suggest removing the qualifiers physical or virtual.Item 23.2 Suggest changing "software (including version)" "installed software versions".Item 23.2 & 23.6 The terminology "any patches, and any custom software/scripts" is vague. Suggest changing to "installed patches, and installed custom software or custom scripts".Items 23.3, 23.4, & 23.6 - Suggest changing "that deviate from the existing" to "that modify the existing".Item 23.4 - The terminology "and other documentation" is vague and subjective. Suggest deleting that phrase from this item. While "other documentation" may require an update this requirement should stay focused on configuration status.Items 23.3, 23.4, & 23.5 - The terminology shifts from 'BES Cyber System Components' used in Items 23.1 & 23.2 to 'BES Cyber System' in the last three items. If the inventory & baseline configuration is on the

#	Organization	Yes or No	Question 40 Comment
			component level then these three items should address changes on the component level to be dealing at the same level of detail. Suggest using consistent terminology in this table, either 'systems' or 'components'.Item 23.6 - Suggest deleting "each" as an unnecessary word. "For changes that modify the..." is better phrasing.Item 23.6 - Suggest deleting "software versions, active ports and services, any patches, and any custom software/scripts included in the" as unnecessary wording. The statement that the test environment closely models the baseline configuration should be adequate.Item 23.6 - Suggest punctuation or reformatting the second bullet for clarity. Possibly a separate line item: "For testing changes that modify the document: (1) the results of the testing (2) the difference between the test environment and the baseline configuration..., and (3) a description of measures used to account for the differences in operation between the test environment and the baseline configuration...."Item 23.7. This requirement statement is vague. Does it mean an inventory of hardware to monitor if any additional hardware was added, or hardware was removed? It appears to relate to some type of software status monitoring, but is not clearly stated. The terminology "respond to the detection of any unauthorized changes" is not clear and is subjective. As it is written, suggest deleting this item, or clarify the wording so it is a viable requirement.
40.37	ISO New England Inc	Disagree	r23.2 - custom software/scripts? Maybe better language is those custom software scripts that are required for the function of the BES cyber system component would be more appropriate. Recommend that 23.2 should remove physical location since it is covered in the updated 23.1 (see answer to question 41)R23.5 A entity may define that it's only security control is password complexity while other may try to adopt a Security Controls from the Center for Internet Security. As an entity defines more security controls the higher the risk for violating a requirement. Can cyber security controls be defined or identify requirements within this standard?R23.5 looks like the wording of the requirement allows the change to be made to production then test (after the change is made) to determine if the security has been adversely affected? Appears to contradict R23.6.As written, 23.5 is confusing. Suggest using “Assess changes to baseline configuration to verify controls are not adversely affected

#	Organization	Yes or No	Question 40 Comment
			..."Recommend the SDT check the new EOP Backup Facility Standard for testing in 23.6R23.7 What is the timeframe for monitoring? R23.4 gives 30 days to document the difference so can you monitor 30 days after the change. Does monitoring need to be real-time or can a daily process be used (other than weekends and holidays) to detect changes and reconcile to change management requests?
40.38	Independent Electricity System Operator	Disagree	R23.2 - what is meant by "software". Is this requiring that the version of Notepad, Wordpad, WinZip be recorded or only software that is needed to operate the component?- R23.5 A entity may define that it's only security control is password complexity while other may try to adopt a Security Controls from the Center for Internet Security. As an entity defines more security controls the higher the risk for violating a requirement. Can cyber security controls be defined or identify requirements within this standard?- - R23.5 looks like the wording of the requirement allows the change to be made to production then test (after the change is made) to determine if the security has been adversely affected? Appears to contradict R23.6.- - R23.7 What is the timeframe for monitoring? R23.4 gives 30 days to document the difference so can you monitor 30 days after the change. Does monitoring need to be real-time or can a daily process be used (other than weekends and holidays) to detect changes and reconcile to change management requests?- R23.3: replace "existing inventory" with "existing baseline" since above the baseline configuration was defined to include an inventory...; replace "update the inventory" with "update the baseline"- R23.3: what is "other documentation"- R23.3: is 30 days calendar days or business days?- Not clear on the difference between 23.3 and 23.4- R23.5: define "cyber security controls"- R23.6: could the statement "test the changes to the BES Cyber System in a test environment..." be changed to replace the second "test" with another word-what if it is tested in an environment that is not "test" but meets the requirements as stated?
40.39	Ameren	Disagree	R23.3 - Does change only constitute replacing hardware as inventory and replacement of software is not a requirement for low systems? Need to clarify requirement.R23.4 - This requirement will be challenging to audit as there is no clear lower threshold for

#	Organization	Yes or No	Question 40 Comment
			changes to the baseline configuration. Suggest adding the term significant changes.R23.7 - Is this requiring the installation of additional software to perform this function? Some systems may not allow the addition of this type of software, this requirement will likely end up needing a TFE.
40.40	Allegheny Energy Supply	Disagree	R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.
40.41	Allegheny Power	Disagree	R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.
40.42	EEI	Disagree	R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high

#	Organization	Yes or No	Question 40 Comment
			impact cyber systems.
40.43	Constellation Power Source Generation	Disagree	R23.7 describes monitoring, but not how the monitoring should be implemented (automated, manual, etc). What is the timeline to respond to the detection of unauthorized changes? Yearly? Daily? Continuously? A suggestion would be a yearly manual monitoring system.
40.44	Hydro One	Disagree	Recommend that 23.2 should remove physical location since it is covered in the updated 23.1 (see response to Question 41).As written, 23.5 is confusing. Suggest rewording to "Assess changes to baseline configuration to verify controls are not adversely affected ..."Recommend the SDT check the new EOP Backup Facility Standard as it applies to testing in 23.6.Please explain the rational to limit 23.6 to Control Centers only.
40.45	Northeast Power Coordinating Council	Disagree	Recommend that 23.2 should remove physical location since it is covered in the updated 23.1 (see response to Question 41).As written, 23.5 is confusing. Suggest rewording to "Assess changes to baseline configuration to verify controls are not adversely affected ..."Recommend the SDT check the new EOP Backup Facility Standard as it applies to testing in 23.6.
40.46	Garland Power and Light	Disagree	Requirement 23.2 23.4, 23.6 and 23.7 - should not apply to database changes or display changes
40.47	Alliant Energy	Disagree	Requirement 23.7 forces entities to implement discovery tools where they may not already exist into environments that may incur negative impact from the very nature of these discovery mechanisms. Where the operational risk of discovery tool deployment precludes its introduction, this requirement would necessitate manual processes. These manual processes would tax the operational resources normally dedicated to increasing the reliability of the BES.
40.48	Public Service Enterprise	Disagree	Requirement 23.7 may not be technically feasible for certain types of BES Cyber

#	Organization	Yes or No	Question 40 Comment
	Group companies		System Components such as older generation or legacy Remote Terminal Unit (RTU) products. To implement this requirement, an Operating System level change to the component may be required, which may be infeasible or not available from the Original Equipment Manufacturer (OEM). This requirement needs to be qualified with the phrase “where technically feasible”.
40.49	San Diego Gas and Electric Co.	Disagree	SDG&E feels that unless there is a major change in the number of types of assets that fall into the low category, there is little reason to have these assets be subject to a different set of requirements than those in the medium and high impact areas. Also, if there is consistency in the application of medium and high impact assets for R23.2 and R23.4, then why is R23.5 only required for high impact assets? SDG&E also requests an example of a virtual BES Cyber System Component (excluding software running on the component).
40.50	Duke Energy	Disagree	Some software on a BES Cyber system may not be relevant to the system (ex. Microsoft calculator or other bundled software) we don’t want to include a version of that. Suggest removing software since the software itself may be the BES cyber systemRequirements 23.3, 23.4, 23.5 - authorization should be able to be made more than 30 days BEFORE the installation.Requirements 23.3, 23.4: documentation via "red-marked" drawings ("interim as built") should satisfy this requirement. Is that the case?Requirement 23.5: as written, it allows the assessment to occur AFTER the fact. Should this not occur BEFORE the change is made?Requirement 23.6: with the proposed definition, it is open for interpretation how closely test environment should model the production environment.Requirement 23.7: what is the expectation for implementing this control? Manual? Automatic? Suggest removing. We are unaware of any device capable of doing this.
40.51	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS comments to require the current drafted language of R23 Table 23.1 - 23.7 for Control Centers Only. We also offer the following recommendation to cover a Configuration Change Management process for the rest of the facilities:R23 Table 23.8 (NEW): Develop one or more processes for

#	Organization	Yes or No	Question 40 Comment
			configuration change management for BES Cyber System Components in generation and transmission facilities.R23 Table 23.8: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR23. Objective:To prevent and detect unauthorized modifications to BES Cyber Systems. R23. Requirement:Each Responsible Entity shall document and implement processes that incorporate the criteria in CIP-011-1 Table R23 - Configuration Change Management.
40.52	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent and detect unauthorized modifications to BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.In addition, Section 23.7 of Table R23 has issues.It is not clear what is meant by "monitor changes...." If this implies some form or ongoing or periodic "monitoring" consider the following:Depending upon the definition of "change" and because of the nature of devices located at substations and other BES equipment, any form of ongoing check or monitoring would be extremely difficult. Because there is the potential for each device to have specific configurations and settings depending up the conditions of the circuit it might be connected to, this would mean that each piece of equipment would have to be manually connected to and checked on a periodic basis. These are industrial controls that are not normally connected to unless service is required for some reason. The definition of a change should not include day to day work processes that are performed to keep the lights on such as settings changes, resetting relays, AV signature updates, or other services and settings kinds of activities. Nor should it necessarily include data changes that do not affect the executable code or configuration of the system. We would expect to be able to define what a change is within our environment.Recommendation: Delete 23.7. Modify R23 to read:Objective 23 - To prevent and detect unauthorized modifications to BES Cyber Systems.R23. Each Responsible Entity shall document and implement processes that incorporate the criteria in CIP-011-1 Table R23 - Configuration Change Management. Such processes shall include an Entity-specific

#	Organization	Yes or No	Question 40 Comment
			definition of what constitutes a system change.
40.53	US Bureau of Reclamation	Disagree	The table requires additional clarification, particularly for different sorts of devices (relays, etc.)
40.54	Con Edison of New York	Disagree	These systems are constantly be upgraded all year long with little impact on any security. The need to do this within 30 days is excessive and should be limited to an annual review.
40.55	MRO's NERC Standards Review Subcommittee	Disagree	This requirement, especially evident in item 23.2, appears to be written around typical IT equipment, and not the multitude of electronic programmable devices an entity will encounter in the field at a generating facility or substation. Therefore, we believe the current intent of this requirement should only apply to control centers, similar to item 23.6, where typical IT equipment is becoming more of the standard.For generating facilities and substations, we believe it would be adequate to require the entity to document and implement one or more processes for configuration change management, and this would be applied to all Low Impact, Medium Impact, and High Impact systems.
40.56	Western Area Power Administration	Disagree	This requires a near-identical test system and makes no adjustments for risk analysis, and does not allow testing on failover devices (maybe) as it says "test environment" specifically. Is that truly the intent?
40.57	We Energies	Disagree	We Energies agrees with EEI: R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.We Energies agrees with EEI: R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.

#	Organization	Yes or No	Question 40 Comment
40.58	Manitoba Hydro	Disagree	We support the baseline approach to change management. It is unclear as to what "other documentation" in Requirements R23.3 and R23.4 is being referenced.
40.59	Emerson Process Management	Disagree	What is the significance of excluding software from the inventory requirement in 23.1 for low-impact BES Cyber System? Cyber security is mostly related to software than hardware. This exclusion does not give any value to the low impact systems.

41. Table R23 provide direction concerning what impact level of BES Cyber Systems to which Requirement R23 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Configuration Change Management" is now addressed in CIP–010–1 — Cyber Security — Configuration Change Management

Commenters raised concerns about requirements that include component level actions for Low Impact BES Cyber Systems, such as inventories and development and maintenance of documentation. Commenters believed that the effort needed to implement those actions will detract from other, more critical actions on Medium and High Impact BES Cyber Systems and Components. Some recommendations are to remove Low Impact BES Cyber Systems from all Requirement R23 controls. In addition, because inventories are required in R23.1-2 for Low Impact components, commenters recommend that these should be limited to devices that have an external accessible connection with a potential direct impact on BES reliability. The drafting team appreciates the concern regarding the level of effort necessary for compliance on Low Impact assets. As such, the drafting team has attempted to implement a framework where the controls for Low Impact assets are those that can be implemented at a higher level of abstraction (such as on a site-by-site basis versus a component level basis) or are primarily programmatic or organizational in nature.

Commenters recommended that monitoring changes to the baseline configuration and responding to the detection of any unauthorized changes be limited to control centers only. The commenters submit that although the requirement may be appropriate for certain types of assets, the technology required to monitor many devices in generation and transmission facilities does not exist. As indicated in its response to Question 40, the drafting team appreciates these concerns and has modified the applicability for configuration monitoring to High Impact control centers.

Commenters noted that Requirement R23.2 adds a requirement for a detailed level of inventory including software versions. Commenters were not clear on the granularity required of this inventory. In addition they question how custom code is tracked for systems such as EMS and scripts that are routinely developed to streamline operational functions. In response, the specific language of the requirement regarding the necessary elements in a baseline configuration has been updated by the drafting team with the intent to provide additional clarity. (See Requirement R1, Part 1.1 in CIP-010-5)

Comments were submitted that recommend one inventory be required to cover all Low, Medium and High Impact BES Cyber Systems. It was also suggested that in Requirement R23.6, the requirements identified for Control Centers should only be extended to High Impact BES Cyber Systems as well as Control Centers. In response, the drafting team has adjusted the impact levels of the items that require an inventory to more suitably focus the effort of the Responsible Entity on items that are not as documentation-centric. None of the requirements in proposed CIP-010-5 apply to Low Impact BES Cyber Systems.

Regarding the testing of changes, commenters recommended testing of all High and Medium Impact BES Cyber Systems, not just those in Control Centers. They also recommended, however, that developing a test environment that models the production environment and documents differences should be applied only to High Impact BES Cyber Systems in Control Centers. In response, the drafting team has modified the standard to require testing of security controls for both High and Medium Impact BES Cyber Systems, but only requires testing in a test environment for those High Impact BES Cyber Systems in Control Centers. (See Requirement R3, Part 3.2 in the proposed CIP-010-5).

#	Organization	Yes or No	Question 41 Comment
41.1	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
41.2	Reliability & Compliance Group	Agree	You need to provide a definition of a virtual BES cyber system component.
41.3	LCEC	Disagree	23 What level does the software inventory include? Driver versions? What about devices with embedded OSes? Needs to include functionality testing.Is the requirement in 23.6 for control center only in reference to the cyber system components?
41.4	Black Hills Corporation	Disagree	23.5 should apply to Medium impact BES cyber systems.
41.5	ERCOT ISO	Disagree	23.5-23.7: Should apply to Medium Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
41.6	Regulatory Compliance	Disagree	23.7 - High Impact - "required for Control Center only"
41.7	US Bureau of Reclamation	Disagree	All impact levels should have some minimum level of requirement established.
41.8	Southwest Power Pool Regional Entity	Disagree	Although the language will work as written, it could be improved by separating the component inventory requirement defined in 23.1 from the more comprehensive

#	Organization	Yes or No	Question 41 Comment
			requirements in 23.2, making 23.1 applicable to all impact categories. Similar improvement is possible with 23.3 and 23.4. 23.6: Testing prior to implementation should apply to Medium category systems.
41.9	Southern Company	Disagree	As long as there are requirements which include per-component action for each low-impact BES Cyber System, the effort needed to implement those actions will overwhelm the rest of the CIP compliance effort. With 100's of low impact BES substations, there are 1000's of BES Cyber System components. These substation devices are being changed daily. The documentation requirements of R23 are overly burdensome with little benefit for low impact BES Cyber Systems. We recommend removing Low Impact BES Cyber Systems from all R23 controls. R23.1-2 requires an inventory of all Low Impact components, this is an intensive work load addition for the Low category components. Components as identified in the definition include all programmable devices. This includes most instrumentation in a generation unit. This should be limited to devices which have an external accessible connection with a potential direct impact on BES reliability.
41.10	WECC	Disagree	Change management and testing should be done for all medium and high impact level BES Cyber System Components not just control center or high.Criteria should apply to all impact levels.
41.11	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
41.12	The Empire District Electric Company	Disagree	Comments: See comments under question 40.
41.13	US Army Corps of Engineers, Omaha Distirc	Disagree	Define "changes" as used in 23.4. Does requirement R23.7 "Monitor changes to the baseline configuration and respond to the detection of any unauthorized changes" imply or require automated monitoring? If automated monitoring is required this could result in numerous TFE's for other than general processing equipment.

#	Organization	Yes or No	Question 41 Comment
41.14	Alberta Electric System Operator	Disagree	In 23.5 and 23.7, consider setting Medium Impact both to Required
41.15	Entergy	Disagree	Inventory and component baseline configuration management are basic care and feeding requirements generally accepted as best practice - 'systems management 101'; and should therefore apply for intelligent infrastructure employed throughout a control system. It is also clear from Order 706 that this is what FERC intends.
41.16	Consultant	Disagree	Item 23.6 - Stating that this is required for Control Centers only adds an additional dimension to the impact categorization. The impact categorization criteria should clearly identify the assets that go into a particular impact classification. The table should only state whether the requirement is required for that classification or not, it should not add an additional classification criteria.
41.17	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
41.18	Oncor Electric Delivery LLC	Disagree	Need an inventory for Medium and High systems(R23.1) and should document changes for Medium and High systems(R23.3) Requirement R23.7 should allow for manual processes to detect changes. It is also unclear how an entity would document a phased implementation - is it based on "in-service" designation?
41.19	Con Edison of New York	Disagree	o R23 changes and adds to Change Management Configuration requirements. This requirement mentions the need for an inventory of BES cyber components. This is not mentioned in CIP-010 o R23.2 This requirement adds a much more detailed level of inventory including software versions. This would be an extensive task, and does this require an inventory of all, such as any Microsoft Office on the workstations, non- MS app's etc? Shouldn't this be limited to knowing the release level you are on, without the line-by-line level information? How do you handle custom code for custom systems such as EMS?How do you manage scripts, they can be written to pull information from the database as shorthand; would that count? These are routinely

#	Organization	Yes or No	Question 41 Comment
			written by staff to get something quickly, and to address repetitive solutions/commands.
41.20	American Municipal Power	Disagree	Please provide a little or no impact category
41.21	Madison Gas and Electric Company	Disagree	R23.1 states: Develop an inventory of its physical or virtual BES Cyber System Components (excluding software running on the component), including its physical location.The BES Cyber System Component definition states: One or more programmable electronic devices (including hardware, software and data).... This requirement excludes software, but what about data?
41.22	BGE	Disagree	Recommend having 1 inventory for Low, medium and High.
41.23	Hydro One	Disagree	Recommend that 23.1 and 23.3 should be Required for High Impact, Medium Impact and Low Impact BES Cyber Systems.Recommend 23.6 High Impact BES Cyber Systems should be Required, not Required for Control Center Only.Recommend a clarification of "monitor" in 23.7.
41.24	ISO New England Inc	Disagree	Recommend that 23.1 and 23.3 should be Required for High Impact, Medium Impact and Low Impact BES Cyber SystemsRecommend 23.6 High Impact BES Cyber Systems should not be Requireed for Control Center Only
41.25	Northeast Power Coordinating Council	Disagree	Recommend that 23.1 and 23.3 should be Required for High Impact, Medium Impact and Low Impact BES Cyber Systems.Recommend 23.6 High Impact BES Cyber Systems should be Required, not Required for Control Center Only.Recommend a clarification of "monitor" in 23.7.
41.26	National Grid	Disagree	Refer to comments in Q. 40.
41.27	San Diego Gas and Electric	Disagree	SDG&E feels that unless there is a major change in the number of types of assets that

#	Organization	Yes or No	Question 41 Comment
	Co.		fall into the low category, there is little reason to have these assets be subject to a different set of requirements than those in the medium and high impact areas. Also, if there is consistency in the application of medium and high impact assets for R23.2 and R23.4, then why is R23.5 only required for high impact assets?
41.28	American Electric Power	Disagree	See comments under question 40.
41.29	MRO's NERC Standards Review Subcommittee	Disagree	See comments under question 40.
41.30	Southern California Edison Company	Disagree	Should be unilateral across all levels.
41.31	ReliabilityFirst Staff	Disagree	Suggest "Required" for Medium Impact in rows 23.5, 23.6, and 23.7.
41.32	Network & Security Technologies Inc	Disagree	Suggest requiring changes be tested for all High and Medium Impact Cyber Systems. Requirements to use a test environment that models production environment and to document differences could be applied only to High Impact systems in Control Centers.
41.33	Midwest ISO	Disagree	The requirement to document changes to the inventories in R23 is 30 days. The requirement to update inventories CIP-010 R2 is 45 days per CIP-010 R2. These should be consistent and we recommend it should be 60 days per our response in Q5.
41.34	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R23 if our changes proposed in Question 40 are accepted:R23 Table 23.1: Low Impact: Required for Control Centers OnlyMedium Impact: N/AHigh Impact: N/AR23 Table 23.2: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: Required for Control Centers OnlyR23 Table 23.3: Low Impact: Required for Control Centers OnlyMedium Impact: N/AHigh Impact: N/AR23 Table 23.4: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: Required for Control Centers

#	Organization	Yes or No	Question 41 Comment
			OnlyR23 Table 23.5: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyR23 Table 23.6: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyR23 Table 23.7: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyR23 Table 23.8: Low Impact: RequiredMedium Impact: RequiredHigh Impact: Required
41.35	GTC & GSOC	Disagree	We recommend that R23.7 be applicable for control centers only. This requirement is more appropriate for control centers and not for transmission and generations operations. While this requirement may be feasible for certain types of protective relays, this technology generally does not exist for a wide range of devices including certain RTUs and meters. In fact, some RTU's must be taken offline in order to retrieve their configuration. Thus, compliance with this requirement would have a negative reliability benefit.
41.36	Progress Energy (non-Nuclear)	Disagree	We see 23.5 as documented lab and field testing for any change to an existing relay/gateway/etc. configuration. Is this what was intended?Baseline configuration is not clear - does this start with the implementation date of the standard or the original production of the facility/element.Virtual BES is not clear. Please specify intention.

42. The definition of sensitive information was derived from the previous version of the CIP standards to minimize disruption to entity information protection programs that are already in place. Do you agree with the proposed definition? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

The definition of "sensitive information" that was originally posted as an informal definition adjacent to Requirement R24 in the draft CIP-011-1 was:

For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.

The primary issue identified with sensitive information was the term itself. Many commenters indicated that this term is already being used by organizations for other purposes, and its inclusion in the NERC CIP standards will cause much confusion. There were several suggestions of alternative terms to use including "CIP-sensitive information" and "protected information." In response to these comments, the drafting team has changed the term to "BES Cyber System Information." The commenters also included numerous suggestions for the improvement of the definition. One commenter indicated that this was not really a definition at all, but rather a list of examples. The drafting team did recognize this as a list of examples, and as such removed it from the requirement language and included the suggestions in the definition of the term BES Cyber System Information.

Several commenters indicated that "floor plans of computing centers" should be removed from the definition. The drafting team agrees that floor plans are problematic as they often are required to be submitted as part of work permits or other items. As such, the drafting team has clarified that only those floor plans that include impact designations of BES Cyber Systems should be identified as BES Cyber System Information, since it is the aggregate data that rises to the level of required protections and not just floor plans alone. This modification was also made to other elements of the definition such as equipment layouts.

A few commenters suggested that the scope of the definition was not broad enough and should be modified by saying "includes but not limited to" or changed entirely to include all data that affects the confidentiality, integrity, and availability of the BES. The drafting team appreciates this suggestion, but sees difficulty in the ability to measure such a broadly scoped definition. Additionally, the drafting team wanted to base the definition on the elements previously defined in CIP-003-3 R4.1 to leverage the investment that Responsible Entities have already made in their existing NERC CIP Information Protection Programs.

The proposed definition of "**BES Cyber System Information**" is:

"Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans."

#	Organization	Yes or No	Question 42 Comment
42.1	Florida Municipal Power Agency	Agree	24.4 - How can a RE "revoke access" from data which may have been copied by personnel?
42.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
42.3	CWLP Electric Transmission, Distribution and Operations Department	Agree	Does network topology or similar diagrams include in-house wiring or plant wiring that may include fiber and Ethernet facilities?
42.4	Exelon Corporation	Agree	Exelon seeks clarification on the following question. Is it the intention of the Standard Drafting Team to include blueprints (schematics and one lines diagrams) for relay and SCADA components in the definition of sensitive information? And, to the extent that such information described large generation facilities or combinations of facilities greater than 2000 MW, then would the electronic record system be considered a High BES Cyber System?
42.5	USACE - Omaha Anchor	Agree	Question - it's difficult to electronically distribute controlled information - however the incident response plan and the recovery plan are supposed to be easily available to all folks. Seems a bit of an oxymoron.

#	Organization	Yes or No	Question 42 Comment
42.6	Northeast Utilities	Agree	The prior version had a concern with user lists, logon-ids, etc. Was applicability to that type of information intentional removed? Also, please clarify whether a recipient of CIP sensitive information must be CIP cleared (PRA & trained).
42.7	Consultant	Disagree	"...network topology or similar diagrams..." should be modified to "network topology that includes BES Cyber Systems" Corporate network topology should not be included in the standards, but this wording would include such diagrams."...floor plans of computing centers that contain BES Cyber Systems..." should be removed, or clarified to specify "floor plans that indicate locations of BES Cbyer Systems". Building floor plans exist in many places that are beyond the control of the Responsible Entities, e.g. architects, landlords, building maintenance companies. A better option might be rewording to qualify the entire list of items as applying to BES Cyber Systems. "... includes (1) security operational procedures, (2) network topology or similar diagrams, (3) floor plans of computing centers, (4) equipment layouts, (5) disaster recovery plans, (6)incident response plans, and (7) security configuration information that contain BES Cyber System information.The definition should be written as a definition, i.e. Sensitive Information - (1) security operational procedures, (2) network topology or similar diagrams, (3) floor plans of computing centers, (4) equipment layouts, (5) disaster recovery plans, (6)incident response plans, and (7) security configuration information that contain BES Cyber System information.The definition is NOT 'For the purposes of this standard', it is expected to be included in the next Glossary update after approval of the standard, and the defined term is hidden somewhere in the statement.
42.8	Luminant	Disagree	"floor plans of computing centers that contain BES Cyber Systems" should be changed to "floor plans that specifically identify BES Cyber Systems or their locations". " BES Cyber System disaster recovery plans" should be “BES Cyber System recovery plans"
42.9	Tenaska	Disagree	24.1 should say: Identify sensitive information.24.2 should say: implement procedures protect sensitive information25.1 should say: render sensitive information unusable

#	Organization	Yes or No	Question 42 Comment
			when disposing of documents and equipment that may contain that information.
42.10	Alliant Energy	Disagree	Alliant Energy agrees with EEI on all points and timeframe consistency. Table 24 is another occurrence where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
42.11	Dairyland Power Cooperative	Disagree	BES systems actually contain information/data about the BES that is sensitive as well, but are ignored. Definitions for SCADA, electrical network topology, schematics, and other information can also be BES information related to critical infrastructure that requires protection.
42.12	E.ON U.S.	Disagree	CIP-011, R24 The definition of sensitive information should provide examples of what constitutes a “security operational procedure.”
42.13	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes the Responsible Entity should identify and classify data as sensitive information and therefore the definition is too restrictive. CenterPoint Energy recommends it be revised as follows: For the purpose of this standard, sensitive information includes but is not limited to, security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and

#	Organization	Yes or No	Question 42 Comment
			security configuration information.
42.14	Dominion Resources Services, Inc.	Disagree	Dominion recommends changing “contain” to “identify” and adding the phrase “that specifically identify Medium or High Impact components” after the phrase “equipment layout of BES Cyber Systems.” This modification is reflected in the revised definition below: For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that identify BES Cyber Systems, equipment layouts of BES Cyber Systems that specifically identify Medium or High Impact components, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.
42.15	Bonneville Power Administration	Disagree	FERC, NERC and the Regional Entities do not have the information necessary to determine what information is sensitive or not as it regards any Responsible Entity. This is conditional and depends on more that just the types of information involved. The determination of what is sensitive information, and what is not can only be done by the Responsible Entity and under the laws and regulations they must comply with. Floor Plans, network diagrams, equipment layouts and other information may or may not be sensitive depending upon what additional information is provided with it. In addition, legal contracts, Federal, state and municipal laws, regulations, and fiduciary requirements may also govern what information may be protected and what must be released.Recommended Change - For the purpose of this standard, sensitive information may include security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information as determined by the Responsible Entity.
42.16	NextEra Energy Corporate Compliance	Disagree	In R24, is it a requirement to map every user's access privileges to sensitive information?In R24, for every new document that contain security operational procedures, network topology or similar diagrams, floor plans of computing centers

#	Organization	Yes or No	Question 42 Comment
			that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information, do we need to record the explicit authorization of every personnel that has access privileges for each type of documents?In 24.2, does this mean that the handling procedures for hard copies of sensitive information include a documentation for chain-of-custody for High Impact BES Cyber Systems?
42.17	Regulatory Compliance	Disagree	Incident Response plans and Diaster and Recovery plans should not be included as sensitive information - these plans should be psuedo public as long as they have written without security configuration information in them.
42.18	Progress Energy (non-Nuclear)	Disagree	It is not clear if this includes relay device information such as electrical diagrams/schematics.Incident response plans typically do not contain any system specific information. The plans provide the actions that must be taken and must be freely available to many. Will that approach meet the intention of the new standard?
42.19	MidAmerican Energy Company	Disagree	Many entities including MEC use "Sensitive" information as one of the classifications for information that needs to be protected. Calling all information to be protected sensitive will cause confusion. Change the term "sensitive information" to "protected information" in CIP-011.
42.20	Con Edison of New York	Disagree	o R24.3 does the word explicitly mean we cannot say all EMS staff has access to information? Does it need to be by name?
42.21	Network & Security Technologies Inc	Disagree	R24 and/or its sub-requirements should be modified to make it clear they apply sensitive information regardless of media type (including paper copies).24.4 - Revocation of access can be hard to do, and even harder to verify, in cases where an individual has taken either electronic or paper copies of sensitive documents off the Responsible Entity premises (sometime for legitimate reasons). Suggest revising this requirement in a manner that acknowledges this reality - something like “best effort” to retrieve sensitive information the individual may have in his or her possession,

#	Organization	Yes or No	Question 42 Comment
			accompanied by warnings that subsequent unauthorized disclosure of any such information may result in prosecution.
42.22	Hydro One	Disagree	Recommend that the definition change “includes” to “includes but not limited to”.
42.23	ISO New England Inc	Disagree	Recommend that the definition change “includes” to “includes but not limited to”
42.24	Northeast Power Coordinating Council	Disagree	Recommend that the definition change “includes” to “includes but not limited to”.
42.25	US Army Corps of Engineers, Omaha Distirc	Disagree	Remove "floor plans of computing centers"
42.26	Allegheny Energy Supply	Disagree	Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram “similar” (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely available to responsible entity personnel. Acceptable Use Banners could be considered part of security

#	Organization	Yes or No	Question 42 Comment
			configuration information.The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part of this standard.
42.27	LCEC	Disagree	Sensitive is a classification that is specific to the CIP standards per this definition but is used in organizations as one of the levels of information classification. To differentiate, the term BES Sensitive might be considered.
42.28	Public Service Enterprise Group companies	Disagree	Sensitive should be changed to “protected Information”, the definition is fine.
42.29	Progress Energy - Nuclear Generation	Disagree	Sensitivity levels for information are established for nuclear generation facilities by CFR. This definition should be adjusted to acknowledge information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
42.30	Southwest Power Pool Regional Entity	Disagree	Should include more than “security” operational procedures. IT-specific operating procedures (“run books”) are very sensitive and could be used to exploit a system. Operations procedures may also be sensitive to some extent if they describe the use of the BES Cyber System.
42.31	San Diego Gas and Electric Co.	Disagree	The "definition" is only a list of examples, not a real definition. SDG&E suggests the following definition: "Sensitive information is defined as any information owned by

#	Organization	Yes or No	Question 42 Comment
			the Responsible Entity, or for which the Responsible Entity is the custodian of, that, if inappropriately disclosed, modified, or rendered unavailable, could adversely impact human safety or the reliability of the BES. Examples include...(their list)"
42.32	APPA Task Force	Disagree	The APPA Task Force would like to comment on the definition of sensitive information: As pointed out in Question 44, the following disclaimer needs to be added to that definition: "To the extent that state/local laws allow"
42.33	Entergy	Disagree	The definition of sensitive information is nearly identical to the one currently being used in version 3. R24.1 and R24.2 explicity allow the Entity to classify and protect "sensitive" information under its own auspice. As long as the classification guidelines are left for the Entity to decide, this definition should prove sufficient.The requirement indicates that the drafting team believes protection of sensitive information associated with allegedly "low impact" BES Cyber Systems/Components that provide routable protocol attack vector access to control hosts, etc., is unnecessary. Suggest this be rethought.Please define "Explicitly Authorize"? Does this mean that every individual with access to a particular piece of information needs some type of documented approval? Can this be done at a group level based on job function? Is approval documentation all that's required, or is a maintained list required as well?
42.34	Manitoba Hydro	Disagree	The definition should also reference control rooms.
42.35	Southern California Edison Company	Disagree	The definition should clearly distinguish BES operational information and cyber security related information. A smaller subset of the former and larger subset of the latter form potential candidates for "protected information".
42.36	Oncor Electric Delivery LLC	Disagree	The definition should not prescribe items as being "sensitive". The identification and classification process of Requirement 24.1 should do that. "For the purpose of this standard, sensitive information includes procedures, diagrams and any other document which provides proprietary information about BES Cyber Systems or BES

#	Organization	Yes or No	Question 42 Comment
			Cyber System Components."
42.37	Allegheny Power	Disagree	There is no reasoned basis to simply bring forward a historic definition then add significant additional requirements based on a legacy definition.Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram "similar" (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely available to responsible entity personnel. Acceptable Use Banners could be considered part of security configuration information.The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part

#	Organization	Yes or No	Question 42 Comment
			of this standard.
42.38	EEI	Disagree	There is no reasoned basis to simply bring forward a historic definition then add significant additional requirements based on a legacy definition.Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram "similar" (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely available to responsible entity personnel. Acceptable Use Banners could be considered part of security configuration information.The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part

#	Organization	Yes or No	Question 42 Comment
			of this standard.
42.39	ReymannGroup, Inc.	Disagree	This definition should be expanded to include the identification and classification of ALL data that affects the confidentiality, integrity, and availability (CIA) of the BES system commensurate with its sensitivity and consequence.
42.40	US Bureau of Reclamation	Disagree	This effort needs to be aligned with the Executive level CUI requirements.
42.41	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
42.42	We Energies	Disagree	We Energies agrees with EEI: There is no reasoned basis to simply bring forward a historic definition then add significant additional requirements based on a legacy definition.We Energies agrees with EEI: Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.We Energies agrees with EEI: The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. We Energies agrees with EEI: A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram "similar" (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely

#	Organization	Yes or No	Question 42 Comment
			available to responsible entity personnel. Acceptable Use Banners could be considered part of security configuration information.We Energies agrees with EEI: The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. We Energies agrees with EEI: For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part of this standard.
42.43	American Transmission Company	Disagree	We propose deleting "floor plans of computer centers" from the definition of sensitive information. Floor plans do not typically include information specific to devices, IP addresses, etc which could be used to compromise a BES Cyber System. Moreover, a computer center is an undefined term which could mean anywhere there was more than one computer.
42.44	LADWP	Disagree	Word sensitive needs to be changed as it can coincide with actual classification used by entities.
42.45	FirstEnergy Corporation	Disagree	Would like to see the definition even more narrow, to focus on information that truly can compromise the BES (e.g. Vulnerability assessments', mitigation strategies, passwords, and DR plans).

43. Do you agree with the proposed definition of Media? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

The definition of "media" that was originally posted as an informal definition adjacent to Requirement R25 in draft CIP-011-1 was:

Media for the purpose of this standard means any mass storage devices within a BES Cyber System Component including, but not limited to, magnetic tapes, optical disks, and magnetic disks onto which information is recorded and stored.

The proposed definition of "media" received significant agreement from those entities that chose to respond to this question. The majority of comments on the definition of media indicated that the definition should be expanded to include additional storage types as well as more traditional media types such as paper. The drafting team intends for Responsible Entities to protect media, such as paper, through the required handling procedures included in the Information Protection requirement.

One commenter indicated that USB drives, CDs, and floppy disks should be included in the definition of media. It was the intent of the drafting team that these device types would be considered devices used to perform maintenance and thus treated in accordance with the maintenance requirements. As the maintenance requirements evolved with the inclusion of additional remote access requirements, the drafting team considered expanding the scope of the media definition.

Another commenter made an interesting case regarding the media being "within" a BES Cyber System and suggested that once the media was removed that it no longer met the definition. The drafting team considered this comment and has modified the standard to require sanitization of BES Cyber System Information contained on media. The remaining comments focused primarily on the requirements themselves and not the definition. Specifically, commenters were concerned about the level of sanitization that would be required on the media. Several commenters noted that the level of sanitization should be commensurate with the potential threat to BES reliability, while others suggested that there be a defined minimum acceptable sanitization process, such as an NSA standard. The drafting team understands the need for a minimum acceptable sanitization process. However, the NERC Standards Development Process does not allow the drafting team to simply reference another standard. As such, we have modified the language in the revised standard to require that media be destroyed or other actions taken to prevent unauthorized retrieval.

Given the potential confusion with establishing a NERC Glossary definition for media, the drafting team has elected to define the term within the language of the standard itself.

#	Organization	Yes or No	Question 43 Comment
43.1	Florida Municipal Power Agency		How would one define the process used to render the media unrecoverable? What does unrecoverable mean? Unrecoverable by NSA standards or unrecoverable by means of something like phase transition?
43.2	Black Hills Corporation	Agree	Believe that solid-state mass-storage (flash drives, thumb drives, jump drives, etc,) should be included as examples in the definition.
43.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
43.4	Northeast Utilities	Agree	Suggest that a minimum acceptable sanitization process (i.e., NIST standard) is specified.
43.5	APPA Task Force	Agree	The APPA Task Force agrees with the definition.
43.6	Dairyland Power Cooperative	Agree	With the proliferation of flash memory solutions, the only way to sanitize some media is physical destruction. Many devices use flash memory in a way that is not removable. Is destruction of this equipment intended?
43.7	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
43.8	FirstEnergy Corporation	Disagree	Believe the definition should not include example because of the quickly changing storage technologies.
43.9	Xcel Energy	Disagree	Further clarification, similar to the definition of Maintenance in R26, is needed to make it clear that media such as hard drives on laptops used for maintenance do not need to be sanitized after temporary connection to BES Cyber Systems.

#	Organization	Yes or No	Question 43 Comment
43.10	LADWP	Disagree	Is portable storage included here?
43.11	Emerson Process Management	Disagree	It should include USB memory stick which is becoming very popular.
43.12	LCEC	Disagree	Media can be removed from the BES Cyber System and it should still be considered media per this requirement. Remove the word "within" and replace with "used by" or "written to by" a BES Cyber System.
43.13	Public Service Enterprise Group companies	Disagree	Media should also include persistent configuration data that is stored in solid state devices (e.g. flash memory, EEPROM (electrically-erasable programmable read-only memory), etc.)
43.14	Southwest Power Pool Regional Entity	Disagree	Portable media, including CD/DVD and USB devices should be included. Basically, anything that sensitive information can be written to.
43.15	Reliability & Compliance Group	Disagree	Recommend removing the word “mass” and instead use the term storage devices.
43.16	USACE - Omaha Anchor	Disagree	Sanitization should only apply to media internal to the devices.
43.17	San Diego Gas and Electric Co.	Disagree	SDG&E notes that the proposed definition does not appear to include "old school" media like paper that is often used to store sensitive information.
43.18	ERCOT ISO	Disagree	Should also specifically address CDs and USB storage devices in the definition.
43.19	Progress Energy (non-Nuclear)	Disagree	Should the definition also clearly state device hard drives?
43.20	Manitoba Hydro	Disagree	The current definition would also require the sanitization of other mass storage devices, such as flash memory, which could render the cyber component unfit for

#	Organization	Yes or No	Question 43 Comment
			reuse outside of the BES Cyber System. The strict sanitization requirement does not permit the return of a failed BES Cyber System or BES Cyber System Component to the vendor for failure analysis. The information protection requirements must provide more flexibility, which may also be achieved through processes and procedures.
43.21	ReliabilityFirst Staff	Disagree	The definition does not need to specify “mass storage devices” and, in fact, should include devices such as flash drives. Media should also be defined to include media types other than electronic such as paper.
43.22	Consultant	Disagree	The definition is technology limited by magnetic and optical technologies. While pervasive, there are and will be other technologies to retain information.Suggest: Media - computer components and recording media that retain digital data used for computing for some interval of time.Might also consider making the definition "Electronic Media" to eliminate books, notebooks, paper, etc. which are also 'information storage media'.
43.23	Entergy	Disagree	The definition of "media" includes the open-ended term "including, but not limited to", which could practically bring anything into scope. A more concise definition with specific examples would remove ambiguity and leave less room for interpretation. The examples of Media in the box should also include flash memory as well.An example of the type of sanitization required should be provided.
43.24	Alberta Electric System Operator	Disagree	The definition states “including, but not limited to,”. The AESO suggests modifiying the definition to explicitly include non-volatile storage to ensure coverage of memory cards and flash drives.
43.25	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
43.26	We Energies	Disagree	We Energies agrees with EEI: When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of

#	Organization	Yes or No	Question 43 Comment
			voltage or frequency does not pose a risk to the BES.
43.27	Allegheny Energy Supply	Disagree	When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of ambient air temperatures does not pose a risk to the BES.
43.28	Allegheny Power	Disagree	When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.
43.29	EEI	Disagree	When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.

44. Requirements R24 and R25 of draft CIP-011-1 concern procedures for information protection and media sanitization. Do you agree with the list of criteria that are included in each Requirements Table for R24 and R25? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

Concerns regarding the requirement for information protection centered around the revocation timeline and scope as well as differentiating access to information vs. access to systems. The drafting team is attempting to address the FERC directive that requires the revocation of access to BES Cyber System Information. The drafting team is proposing to address revocation of access to BES Cyber Systems and to BES Cyber System Information all in one place to ensure more consistency in the requirements and their implementation.

There were a number of commenters who raised concerns with the requirement for media sanitization regarding media failure conditions or disposal. The word "sanitization" appeared to cause confusion for a number of commenters and as such has been removed from the revised standard. Additionally, a couple of commenters raised concerns about the burden of proof, compliance requirements, legal issues, and ownership responsibilities.

As with other areas of this standard, there were a significant number of the comments asking for clarity of phraseology and terminology, including words such as consequence, annually, explicitly, acceptable, commensurate, etc. The drafting team eliminated the words, "explicitly, acceptable, commensurate, and annual" from the revised CIP-011-1 standard.

#	Organization	Yes or No	Question 44 Comment
44.1	ISO New England Inc		Recommend changing 24.4 to Revoke physical/logical access to sensitive information for personnel terminated for causeWhat about revoking access for other than cause?Recommend changing R25.1 to avoid the gap of High Impact to Low Impact to reuse outside of BES Cyber Systems. Suggest changing "reuse outside of BES Cyber Systems" to "reuse outside of the Entity's High Impact or Medium Impact BES Cyber Systems"
44.2	Northeast Utilities	Agree	Agree that this requirement covers the key cyber assets but how does this apply to

#	Organization	Yes or No	Question 44 Comment
			protective systems such as the physical access system, firewalls and logging devices?
44.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
44.4	Black Hills Corporation	Agree	Legally Required Release: There may be "legal" situations in which we may be required to share certain information with outside entities, both government and non-government. Examples could include OSHA or MSHA investigations, employee lawsuits (with the associated discovery). There does not appear to be any provision in the regulation to allow this sharing. We could be placed in the position of violating this regulation, or violating some other legal requirement (subpoena, etc)
44.5	Puget Sound Energy	Agree	Puget Sound Energy suggests modifying R24.4 to "Revoke access to media containing sensitive information within 24 hours..." to align with the NERC definition in R25 and to provide clarity around sensitive information in a hardcopy format.
44.6	GTC & GSOC	Agree	We recommend the verbiage and timelines for R24.4 be consistent with tables R5 and R13.
44.7	Independent Electricity System Operator	Disagree	- R24.4 define for cause. Should the wording be involuntarily terminated to include those that are terminated unwillingly due to layoffs, job cuts, fired/performance, etc.- R24.4 how do you remove access where personnel may have physical copies offsite o
44.8	ERCOT ISO	Disagree	24.2: Recommend: "Implement labeling and handling procedures for sensitive information according to its defined classification level." 24.3: It is unclear whether the requirement includes internal and external personnel. 24.4: Should be combined with other access management requirements (physical, cyber)24.5: Should also address "need to know". The requirement did not address the access control means for protecting information or the access to hard copies of information.
44.9	Duke Energy	Disagree	24.3 - We don't feel it is realistic to explicitly authorize access to paper copies of

#	Organization	Yes or No	Question 44 Comment
			information. Add 'repositories' at the end of the sentence.Include "repository" in 24.4 and 24.5 as well. Requirement 24.3 is particularly burdensome in a nuclear environment where there is already heavy physical security. There are thousands of drawings, for example, available for the plant. There are hundreds of personnel that have a business need to know certain things about the plant that are contained in these drawings. During outages that number often goes above 1000 personnel. Segregating all drawings/manuals/equipment layouts/floor plans/procedures and EXPLICITLY authorizing personnel for access is difficult at best. Certainly, protecting cyber specific information such as firewall rules, group policies, passwords, and other specific cyber information makes sense and is done already.
44.10	Regulatory Compliance	Disagree	24.4 - Strike altogether. Revocation should go back and be included in the scope of System revocation.25.1 - Propose : Sanitize only media containing sensitive information prior to disposal for reuse outside of BES Cyber Systems, using a method to render the data unrecoverable.
44.11	Southwest Power Pool Regional Entity	Disagree	24.4: Is this requirement prescribing Information Rights Management? There are many types of access, including access to information no longer under the direct control of the entity. 24.5 is poorly worded. Would be better to require that access is authorized, not that it reflects authorization. 25.1 should require either sanitization or physical destruction.
44.12	American Electric Power	Disagree	25.1: Regarding "Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a method to render the data unrecoverable", what evidence would be required from an audit perspective? If a USB harddrive is used to copy patches onto a system, would that USB harddrive need to be destroyed with documented evidence if it failed 2 weeks down the road?Suggested rewording:Media for the purpose of this standard means any mass storage devices within a BES Cyber System Component including, but not limited to, magnetic tapes, optical disks, and magnetic disks onto which sensitive information is recorded and stored.Rational: Adding sensitive to the "Media" definition will clarify that this is intended to be used

#	Organization	Yes or No	Question 44 Comment
			to protect the inadvertent distribution of protected information, not all media devices that are plugged into a BES Cyber System will need to be sanitized.
44.13	BCTC	Disagree	Â R24.4. We need clarification on revocation of access. We are assuming it is from the point the person departs their job - i.e. access to the BES Cyber System is revoked. Such personnel could have hard copies of information but how would you prove that such documentation was shredded? What about information they have retained within their brain? ï¿Š We need some clarity on what the parameters are herePlease provide a concise definition for 'sanitize'. We discussed scenarios such as patching the BES Cyber System via a CD - would compliance require that we 'sanitize' the CD? If yes, seems like overkill from our discussions on the subject. Please provide more concise language to define the scope.over real time to either. Yet, in reading the requirements we could potentially be found non-compliant based on the wording of the version 4 standards - this should not be! FYI, I raised this point at the recent 2 day workshop in Texas and the drafting team was in agreement that our current configuration is an example of excellence ... yet is a potentially non-compliant based on current wording ... this needs to be revisited.
44.14	Progress Energy - Nuclear Generation	Disagree	Agree with R24.1, R24.2 and R25.1. Disagree with R24.3, R24.4 and R24.5 which are governed for nuclear generating facilities by CFR. R24-24 should acknowledge information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
44.15	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
44.16	E.ON U.S.	Disagree	CIP-011-1, R24.4 is unnecessary and difficult to impossible to document. At this point, all authorized unescorted physical and electronic access would have been removed per other requirements. E ON U.S. proposes that this requirement be deleted.

#	Organization	Yes or No	Question 44 Comment
44.17	USACE - Omaha Anchor	Disagree	Definition would include external hard drives and other external media. It seems ridiculous if you are installing patches to sanitize the media before going to the next cyber system. You are treating the cyber system as a classified system. This is serious overkill. External media for the most part should be exempt from this requirement unless sensitive information is placed on the media in which case it should follow the rules of R24.
44.18	Dominion Resources Services, Inc.	Disagree	Dominion recommends revising Requirement R24.1 to read:"Identify and designate controls for protection of sensitive information commensurate with its importance to the security and reliable operation of the associated BES Cyber System."24.3. With the heavy industry reliance on vendors and contractors and the requirements throughout other NERC standards to share data with other entities, it is impractical to "Explicitly authorize personnel for access to sensitive information." For example, when information is sent outside Dominion, it is impossible to know every person who sees it. Moreover it is unlikely that whoever does see it would want to sign an agreement with every entity that can submit information. The controls specified above in the requested revision to 24.1 should cover the requirements for access to the information. Dominion requests that this requirement be removed.24.4. It is possible to revoke electronic access to company-controlled devices containing sensitive information and to revoke physical access to company-controlled areas containing sensitive information within 24 hours. It is not reasonable to identify and retrieve information within 24 hours that may have been taken by an authorized user prior to being terminated for cause and it may not be possible to ever retrieve this information if it has been hidden by the individual. Please restate this requirement to indicate that it covers physical and electronic access as follows:"24.4 Revoke electronic access to company-controlled devices containing sensitive information and physical access to company-controlled areas containing sensitive information within 24 hours."24.5. As stated in Dominion's comment to 24.3, it is impractical to authorize individuals. As applied to this requirement it is also impractical to track individuals. In the example given in the above response to 24.3, any non-company

#	Organization	Yes or No	Question 44 Comment
			personnel that might see sensitive data would need to be authorized by every Registered Entity and their companies would have to keep every RE appraised of every personnel change and provide annual lists of all personnel. Dominion requests that this requirement be removed.Note: At Dallas, the SDT requested input as to requiring training and a PRA for access to sensitive information. Dominion requests that training and a PRA NOT be required. Training and a PRA are not required by versions 1, 2, and 3 of the CIP standards and could be impossible to implement across vendors within the electric industry. In the example given in the above response to 24.3, every vendor or business partner would have to take the training from every Registered Entity or have their training approved by every entity (including annually providing the training program to each RE for approval) and ES-ISAC would have to keep every RE appraised of every personnel change and provide annual lists of all personnel. And then, PRAs would have to be addressed. Registered Entities should be required to have internal requirements for access to sensitive information.
44.19	ReymannGroup, Inc.	Disagree	Expand the list of procedures to include 3rd party data recovery services in accordance with an approved vendor management policy for all impact levels.
44.20	RRI Energy	Disagree	Explicitly define “access” as related to sensitive information. Data can be locally cached on web browsers, remote or personal pc’s, etc. These cannot easily be removed let alone 24 hrs removal.
44.21	Constellation Power Source Generation	Disagree	In R24.1, what classifications for sensitive information should be used? The SDT should develop classifications specifically for CIP. As written, this is not an auditable requirement.
44.22	ReliabilityFirst Staff	Disagree	In row 24.1, what is meant by “consequence”? In Table R24, row 24.5, we suggest the verification of access privileges be performed at least quarterly. To Table R24, add a new row 24.6 stating, “Revoke access to sensitive information within 72 hours for personnel terminated not for cause.” And assign this requirement an impact level of “Required” for both Medium and High Impact BES Cyber Systems. Table R25, row

#	Organization	Yes or No	Question 44 Comment
			25.1; we believe there should be a definition of "sanitize" to eliminate confusion regarding what actions must be taken to comply with this requirement.
44.23	MidAmerican Energy Company	Disagree	It was mentioned in the May workshop that the SDT would consider the necessity for Personnel risk assessments and training required prior to granting access to protected information.Personnel risk assessments and training should not be required prior to granting access to protected information. As an example, entities would have a nearly impossible task of completing personel risk assessments for international employees at global help desks that are allowed view only access to a BES Cyber System.
44.24	WECC	Disagree	Item 24.2 should be made clear that individual hard drives, servers, laptops, etc do not need to be labeled. Perhaps "labeling of media" was meant. Item 24.3 will have great impact on the ability to have technical support from large global vendors such as Cisco. Consider exception to this requirement for maintenance or add something to Maintenance requirement R26 to deal with it.Clarify how sensitivity and consequence are determined.Clarify the requirements for authorization for access to sensitive information (i.e. need to know).
44.25	LCEC	Disagree	Need to clarify the acceptable methods.
44.26	NextEra Energy Corporate Compliance	Disagree	NextEra believes that R24 did not take into consideration access privileges with sensitive information. It does not provide clear guidance and left room for interpretation. The following are the recommended updates:R24.5 Verify at least every 12 months that the access privileges to sensitive information reflect the appropriate need with the personnel roles and responsibilities. Access privileges to sensitive should correspond with the needs and appropriate personnel roles and responsibilities.Regarding CIP-011-1/R25, R25 did not provide a standard to sanitize media. The current language did not provide clear guidance and left room for interpretation. The following is the recommended updates:25.1 - Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using clearing

#	Organization	Yes or No	Question 44 Comment
			utility supporting the Department of Defense clearing and sanitation standard. R24.4 - Requirement covered by revocation of physical and cyber access.Revoking physical and cyber access would revoke access to protected information. Therefore, NextEra suggests removing 24.4
44.27	National Grid	Disagree	o Provide timelines for access revocation for reasons other than "terminated for cause" o Do laptops and devices that maintain the BES Cyber Systems need to be sanitized?
44.28	PacifiCorp	Disagree	PacifiCorp asks that the reference to "at least every 12 months" is modified to read "annuallyonce every calendar year." Allowing responsible entities the flexibility to require trying once every calendar year rather than at least every 12 months would relieve entities of the significant administrative burden of tracking specific training deadlines for each individual employee. At the same time, this change will still ensure that employees are trained at regular enough intervals to achieve the reliability goal of the training requirement.
44.29	Ameren	Disagree	R24.3 - Listing people who have access to information serves no purpose in protecting BES systems from Cyber attack. The list of people with this information is not the same as the list of people that have access to the systems. This requirement should be removed.R24.4 - This requirement is impossible to prove for printed documentation. Suggest removal.
44.30	Liberty Electric Power, LLC	Disagree	R25 appears to require the hard drives of laptops used in relay calibrations to be wiped before leaving site. This is a serious issue for smaller entities, due to almost all of the relay work being done by outside contractors. These contractors often need the data taken to write reports which are required by other NERC standards. This requirement needs to be removed.
44.31	Allegheny Energy Supply	Disagree	R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the responsible entity is unable to

#	Organization	Yes or No	Question 44 Comment
			perform sanitization on the media.Requirement 25.1 uses the word “Unrecoverable”. This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of ambient air temperature does not pose a risk to the BES.
44.32	Allegheny Power	Disagree	R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the responsible entity is unable to perform sanitization on the media.Requirement 25.1 uses the word “Unrecoverable”. This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.
44.33	EEI	Disagree	R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the responsible entity is unable to perform sanitization on the media.Requirement 25.1 uses the word “Unrecoverable”. This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.

#	Organization	Yes or No	Question 44 Comment
44.34	Hydro One	Disagree	Recommend changing 24.4 to Revoke physical/logical access to sensitive information for personnel terminated for cause.Revoking access for other than cause should be addressed.Recommend changing R25.1 to avoid the gap of High Impact to Low Impact to reuse outside of BES Cyber Systems. Suggest changing "reuse outside of BES Cyber Systems" to "reuse outside of the Entity's High Impact or Medium Impact BES Cyber Systems".
44.35	Northeast Power Coordinating Council	Disagree	Recommend changing 24.4 to Revoke physical/logical access to sensitive information for personnel terminated for cause.Revoking access for other than cause should be addressed.Recommend changing R25.1 to avoid the gap of High Impact to Low Impact to reuse outside of BES Cyber Systems. Suggest changing "reuse outside of BES Cyber Systems" to "reuse outside of the Entity's High Impact or Medium Impact BES Cyber Systems".
44.36	Idaho Power Company	Disagree	Revocation of access to sensitive information is virtually impossible if the person terminated has the information in their possession either hard copy or portable media. Access to additional information can be revoke. Consider rewording this requirement to accommodate this reality.
44.37	Southern California Edison Company	Disagree	SCE feels the standard, as written, may be operationally difficult to implement. As such SCE recommends allowing for the revocation of electronic access to sensitive information within 24 hours, or make a written demand (which may be followed up by legal process) for such information within a 24 hour timeframe. This distinction is crucial as not all sensitive information may reside within the physical confines of the registered entity. Business concerns may require registered entities to allow sensitive information (if adequately protected by contractual or employment terms) to leave the confines of the company. For example, employees may have CIP-protected information in company-issued laptops. In some scenarios, it may be impossible to recover those laptops if they were left offsite when the employee was terminated. However, it would be possible to issue a written demand, supported by law, for such

#	Organization	Yes or No	Question 44 Comment
			documents. The drafting team is requested to rephrase R24.4 with a view on implementability, enforceability and auditability.
44.38	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that R24.3 should read "Explicitly authorize role-based access to sensitive information."In R24.4, SDG&E asks how would we do this for hard-copy information?In R24.5, SDG&E suggests changing the wording to read "Verify at least every 12 months that the role-based access privileges to sensitive information reflect authorization."
44.39	Progress Energy (non-Nuclear)	Disagree	Should there be an item in table R25 to identify the media to be sanitized that may be overlooked, i.e. printers/plotters/scanners, relay test sets, etc.
44.40	Consultant	Disagree	Table R24 - Item 24.3 This is an access control requirement, and should be moved to access control requirement table. Access control should cover cyber access, physical access, and information access together, as the process for attaining each type of access is related.Item 24.4 is an access revocation requirement, and should be moved to the access revocation requirement table. Access revocation should cover cyber access, physical access, and information access together, as the process for revoking each type of access is related. The comments related to timeframes in those sections are applicable to information access revocation as well.Item 24.5 is an account management requirement, and should be moved to the account management requirement table. Account Management and reviews should cover cyber access, physical access, and information access together, as the process for reviewing and confirming each type of access is related. The comments related to timeframes in those sections are applicable to information access access review as well.Table R26 - Item 26.1 Replace the word "all" with "BES Cyber System" as a better statement.Item 26.1 If 'media' is a defined term it should be capitalized. (See comments on definition of Media.)
44.41	APPA Task Force	Disagree	The APPA Task Force cautions the drafting team on the information protection requirements in R24. Nearly every state in the United States has a public records law

#	Organization	Yes or No	Question 44 Comment
			that applies to public power systems as units of state or local government (These laws are often referred to as “Government in the Sunshine” laws.). We recommend that the drafting team consult with NERC legal counsel prior to revising this requirement. We do not want public power systems to have to choose between being in noncompliance with the proposed requirements or violating their state open records laws. Rebecca Michaels of NERC Staff is familiar with this issue. If this must move forward as proposed we recommend that the following be added to the requirement: “To the extent that state/local laws allow.”R24.Objective:To prevent unauthorized access to sensitive information associated with BES Cyber SystemsR24. Requirement:To the extent permissible under federal and state laws, each Responsible Entity shall document and implement one or more processes that incorporate the criteria in CIP-011-1 Table R24 - Information Protection.
44.42	Reliability & Compliance Group	Disagree	The method of sanitizing media should be done in an industry accepted manner to provide for auditability of the standard.
44.43	Bonneville Power Administration	Disagree	The objectives of these requirements (“to prevent unauthorized access to sensitive information associated with BES Cyber Systems” and “to prevent the unauthorized dissemination of BES Cyber System information”) should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R24, Section 24.1. Recommend replacing "classify" and "classification" with "categorize" and "category" and "categorization", . "Classify" and "classification" have very specific meanings to any Federal agency. Those meanings are restricted to the realm of National Security Information and are different from what is presented here. Such information requires storage in General Services Administration-approved safes, transmission using National Security Agency-approved encryption, and can be only be processed on computer systems if those systems are dedicated to such use, totally isolated from any publicly accessible network, and stored in secure facilities when not

#	Organization	Yes or No	Question 44 Comment
			in use. Furthermore, the Federal Agencies do not have the option of using a different definition. In fact, using Regional Entity standard forms marked "Confidential" is problematic for Federal agencies, as such a marking is reserved for a particular level of classified information. Given the large number of Federal organizations to which this standard applies, it would simplify matters to restrict the use of "classify" and similar terms to the realm of National Security Information.Recommend deletion of Table 24, Section 24.3. Requiring formal authorization is a process more stringent to that required to gain access to National Defensed Information at the Confidential and Secret level: A formal determination of trustworthiness, but no formal further formal authorization required for access once the clearance has been granted. For sensitive information other than National Defense Information, Federal agencies are required only to determine the the recipient needs the information to support the activities of the agency. Such a determination can be made informally, by any person with custody of the information. We realize that there seem to be conceptual difficulties about revoking access without formally authorizing it. But, they are resolved when we note that authorizing access is not the same as granting it. Authorizing access is a declaration that the person is allowed to have access. Granting access is giving them the info. It is not clear to which of these "revoke" is intended to apply. However, R24 is only concerned about revocation following termination for cause. In those cases, electronic and physical access to all Entity assets is generally revoked. That would effectively deny access to the information, as well. Thus, revocation can be accomplished even though a formal access authorization is not used.
44.44	US Bureau of Reclamation	Disagree	The use of the term classification is not appropriate, suggest "categoruize" to avoid conflict with other requirements in the federal sector.
44.45	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments regarding Requirement 25.1.
44.46	We Energies	Disagree	We Energies agrees with EEI: R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the

#	Organization	Yes or No	Question 44 Comment
			responsible entity is unable to perform sanitization on the media.We Energies agrees with EEI: Requirement 25.1 uses the word "Unrecoverable". This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.We Energies agrees with EEI: When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.
44.47	FirstEnergy Corporation	Disagree	We would like to have clearer definition on what is acceptable sanitation methods.
44.48	Entergy	Disagree	What exactly does "Explicitly Authorize" mean? Does this mean that every individual with access to a particular piece of information needs some type of documented approval? Can this be done at a group level based on job function? If so, it should be stated as such.Is approval documentation all that's required, or is a periodically maintained list required as well?What is the definition of "Revoking Access"? Does the individual need to be removed from every Cyber System he/she had access to?
44.49	Manitoba Hydro	Disagree	What is the meaning of "consequence" in Requirement R24.1? There is currently no requirement for revocation of access to sensitive information for any other reason than "for cause". There are no specifics given with respect to "classify" sensitive information in Requirement R24.1 so it is assumed to be at the Responsible Entity's discretion in terms of criteria, methodology, etc. There are no specifics given with respect to "method" in Requirement R25.1 so it is assumed to be at the Responsible Entity's discretion.

45. Tables R24 and R25 provide direction concerning what impact level of BES Cyber Systems to which Requirements R24 and R25 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

Concerns were raised by commenters regarding the applicability of the information protection and media sanitization requirements. The issues centered around the tables being too broad brushed. There was also concern surrounding the differentiation of information sensitivity vs. impact categorization. The drafting team modified the standard to only include information protection for High and Medium Impact BES Cyber Systems and associated Physical Access Control Systems, associated Electronic Access Control or Monitoring Systems, and associated Protected Cyber Assets.

#	Organization	Yes or No	Question 45 Comment
45.1	WECC		Criteria should apply to all impact levels
45.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
45.3	Consultant	Agree	Table R24 - Items 24.3, 24.4, & 24.5 should be moved to their respective subject areas as suggested in the comment on Question 44. (Cyber access, physical access, and information access requirements should be addressed together, as the requirements and processes for each type of access is related.)
45.4	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels proposed for R24-R25 if it is understood that a blank in the table means N/A.
45.5	PacifiCorp	Disagree	: Lines 24.1 and 24.2 imply that multiple classifications levels for "Sensitive Information" will be required. Need to allow for entities to use one classification for "Sensitive Information".24.4 The requirement to revoke access to sensitive information within 24 hours is impractical. The information may be offsite on paper hardcopy or electronically on media. 24.5 Entities should also be required to correct

#	Organization	Yes or No	Question 45 Comment
			access privileges found to be inaccurate once they have been verified.
45.6	Southwest Power Pool Regional Entity	Disagree	24.1, 24.2, and 25.1 should be applicable to all impact categories.
45.7	US Army Corps of Engineers, Omaha Distirc	Disagree	24.3 does a job description constitute "explicit authorization?" Restrictions on media use as written would preclude using media to transfer information to external systems using media. Should be reworded with the intent that the media be sanitized before disposed of or released outside the organization or allowances made for transfering information. Also could be interpreted to mean an update disk used to update BES Cyber System 1 would have to be wiped and could not be used to update system 2.
45.8	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
45.9	Allegheny Energy Supply	Disagree	As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.
45.10	Allegheny Power	Disagree	As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.
45.11	EEI	Disagree	As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.
45.12	MidAmerican Energy Company	Disagree	Lines 24.1 and 24.2 imply that multiple classifications levels for “Sensitive Information” will be required. Need to allow for entities to use one classification for “Sensitive Information”.24.4 The requirement to revoke access to sensitive information within 24 hours is impractical. The information may be offsite on paper hardcopy or electronically on media. 24.5 Entities should also be required to correct access privileges found to be inaccurate once they have been verified.

#	Organization	Yes or No	Question 45 Comment
45.13	American Municipal Power	Disagree	Please provide a little or no impact category
45.14	US Bureau of Reclamation	Disagree	Requirements should be applied to information sensitivity, not the impact level of the system(s).
45.15	Southern California Edison Company	Disagree	SCE feels that R24 and R25 apply regardless of the BES Control System impact level.
45.16	Progress Energy (non-Nuclear)	Disagree	See comment 14.
45.17	LCEC	Disagree	See previous comments
45.18	BCTC	Disagree	See Question 44 response
45.19	Bonneville Power Administration	Disagree	See the response to question 44.Item 24.5 in Table R24 states as follows: "Verify at least once every 12 months that the access privileges to sensitive information reflect authorization". Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently verifications must occur.
45.20	LADWP	Disagree	Should be restricted to high level only.
45.21	ReliabilityFirst Staff	Disagree	Suggest "Required" for Low Impact in row 25.1.
45.22	Entergy	Disagree	The requirement indicates that the drafting team believes that protection of sensitive information associated with allegedly "low impact" BES Cyber Systems/Components that provide routable protocol attack vector access to control hosts, etc., is unnecessary. Suggest this be rethought.
45.23	Pepco Holdings, Inc. -	Disagree	We agree with EEI's comments.

#	Organization	Yes or No	Question 45 Comment
	Affiliates		
45.24	We Energies	Disagree	We Energies agrees with EEI: As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.

46. The BES Cyber System Maintenance requirement is intended to cover the instances where it is necessary to directly connect a device to the BES Cyber System temporarily to perform a support function, provide appropriate controls on the maintenance device to protect the BES Cyber System. Do you agree with the definition of maintenance as provided?

Summary Consideration:

The definition of "maintenance" that was originally posted as an informal definition adjacent to Requirement R26 in draft CIP-011-1 was:

Maintenance for the purpose of this standard includes the activities associated with the support, testing and upkeep of a BES Cyber System. Examples of maintenance activities for BES Cyber Systems include configuration changes, vulnerability assessments, and software patches. Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System.

There were questions and concerns raised by commenters about what is included in the scope of maintenance activities. There were comments that the term "maintenance devices" needs to be defined. In addition, there was a question regarding whether remote access is included as maintenance. There were suggestions that the definition of maintenance should be focused on the temporary connections.

One commenter suggested the following definition: "Maintenance for the purpose of this standard includes any activity requiring the temporary connection of digital equipment (e.g., laptops) capable of altering the configuration of, or introducing malicious code, to the BES Cyber System." The drafting team considered this feedback, and removed the definition of maintenance from the revised standard, and instead focused on temporarily connecting to a BES Cyber System (such as for maintenance) rather than on the activity being performed. (See proposed CIP-007-5 – System Access Control.)

The requirement for Transient Cyber Assets and media in CIP-007-5 R3.4 is intended to ensure that devices used for temporary access to the BES Cyber System (such as for maintenance) do not accidently introduce malicious code into the BES Cyber System or introduce an unauthorized external access point to the BES Cyber System. This requirement also clarifies that these devices may be temporarily connected to the BES Cyber System, but do not become a part of the BES Cyber System, nor are they considered Protected Cyber Assets. The definition for **Transient Cyber Asset** is as follows:

A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset, 2) used for data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System.

#	Organization	Yes or No	Question 46 Comment
46.1	WECC		Provide a separate definition of maintenance device. The requirement does not state that maintenance devices “directly connect” to BES Cyber Systems. In practice, much maintenance is done via network connections. These criteria need to be reassessed if they are intended to apply to network or remote access.
46.2	SCE&G	Agree	Are maintenance devices also to be treated as remote access, as it is a device external to the BES cyber system?26.2: TFEs may be necessary for maintenance devices not capable of supporting malicious code prevention.
46.3	Regulatory Compliance	Agree	BUT -Please clarify definition of "not permanently connected"What if you have a device that might be connected for several months?
46.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
46.5	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	Definition is good, but please see comments for questions 1.a and 1.b.
46.6	NextEra Energy Corporate Compliance	Agree	NextEra comments that if a laptop is used to remotely connect to a High Impact Control Center BES Cyber System to debug a problem or view Operator issues by temporarily gaining alarm permissions that are assigned to the Operator, is this considered a maintenance activity?
46.7	Progress Energy - Nuclear Generation	Agree	Nuclear facilities have maintenance programs based on CFR. This definition can be improved by acknowledging 10CFR50.65.
46.8	APPA Task Force	Agree	The APPA Task Force agrees with the definition.

#	Organization	Yes or No	Question 46 Comment
46.9	GTC & GSOC	Agree	We recommend the last sentence in this definition ("Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System") be removed from R.26 and instead be included as part of the BES Cyber System definition, as suggested in our comment to 1.b. above.
46.10	Consultant	Disagree	"Examples of maintenance activities for BES Cyber Systems include configuration changes, vulnerability assessments, and software patches." NONE of these activities are maintenance activities.Configuration changes & software patches are changes covered by change control. Vulnerability assessments are tests covered by vulnerability assessments."Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System." This is not a definition of "Maintenance". This is (or should be) part of the definition of BES Cyber System Component. Suggest both of these statements be removed from the "definition".
46.11	Dairyland Power Cooperative	Disagree	26.2 A definition of a maintenance device seems needed here. I'm presuming this typically would be the computer used by the support staff to access the BES system for maintenance. What if maintenance is being directly performed on a BES system, is there no maintenance device involved in that case?
46.12	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
46.13	Network & Security Technologies Inc	Disagree	Definition is good overall but should address the question of whether a maintenance device is "external" and must therefore connect via an access point.
46.14	National Grid	Disagree	Does testing the capabilities of the relays part of the maintenance activities?
46.15	Dominion Resources Services, Inc.	Disagree	Dominion recommends revising the definition of Maintenance as follows:"Maintenance for the purpose of this standard includes any activity requiring the temporary connection of digital equipment (e.g., laptops) capable of altering the

#	Organization	Yes or No	Question 46 Comment
			configuration of, or introducing malicious code, to the BES Cyber System."
46.16	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's comment below:The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.17	Black Hills Corporation	Disagree	Middle sentence of Maintenance definition should add ... include but are not limited to configuration...
46.18	Minnesota Power	Disagree	Minnesota Power recommends that the following definitions be adopted by the Standards Drafting Team:Maintenance: Maintenance, for the purpose of this standard, is defined as activities associated with the support, testing and upkeep of a BES Cyber System. Maintenance Equipment: Maintenance Equipment, for the purpose of this standard, is defined as any programmable, electronic device used for maintenance activities that are not permanently connected to the BES Cyber System(s). These devices are not considered part of the BES Cyber System(s).
46.19	PacifiCorp	Disagree	PacifiCorp agrees with EEI's comment below:The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.20	Southwest Power Pool Regional Entity	Disagree	Programmable, general purpose devices connected temporarily are a potentially high risk to the BES Cyber System and should have some minimum set of applicable requirements to minimize that risk. An example is the "wandering laptop" that the support staff uses to connect to High impact BES Cyber Systems and also to surf the Internet from a home Internet connection.
46.21	Duke Energy	Disagree	Suggest replacing "Cyber System Maintenance" with "Cyber System Configuration Management". The definition (first sentence) states: "Maintenance for the purpose of this standard includes the activities associated with the support, testing and upkeep of a BES Cyber System." There are numerous activities that are associated

#	Organization	Yes or No	Question 46 Comment
			with support, testing, and upkeep of a BES Cyber System that are not related to cyber. This could be tuning, calibrating, etc. and could be done with a screwdriver and a meter. The second sentence includes configuration changes, vulnerability assessments, and software patches. These items are more applicable to the cyber related definition. The suggestion is to combine these sentences:"Maintenance for the purpose of this standard includes the cyber security related activities associated with the support, testing and upkeep of a BES Cyber System, including configuration changes, vulnerability assessments, and software patches."Also, please clarify if non-portable test systems that are connected to BES Cyber Systems thru an access point are included. Otherwise define “permanently connected.”
46.22	BGE	Disagree	Systems used for maintenance should be protected and sanitized per 25.1.
46.23	FirstEnergy Corporation	Disagree	The definition does not clearly specify that the intention is for temporary direct connections.
46.24	Allegheny Energy Supply	Disagree	The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.25	Allegheny Power	Disagree	The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.26	EEI	Disagree	The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.27	Southern California Edison Company	Disagree	The justification of separating end users of BES systems and those involved in maintenance is not consistent with the justification for systems that are used for maintenance. The drafting team has chosen to treat ancillary systems used to perform maintenance type activities on a BES system as equally critical. However, a distinct list of maintenance personnel is required to be maintained. The suggestion for the drafting team is to move this requirement to the section dealing with personnel.

#	Organization	Yes or No	Question 46 Comment
46.28	Progress Energy (non-Nuclear)	Disagree	Troubleshooting also needs to be explicitly included as an example.
46.29	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
46.30	We Energies	Disagree	We Energies agrees with EEI: The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.31	LADWP	Disagree	Will require multiple list management. Individual doing maintenance will already be on physical and electronic access list. Now another list is introduced which will also need to be maintained with the same revocation requirements. 26.1 is not necessary.

47. Requirement R26 of draft CIP-011-1 concerns procedures for BES Cyber System maintenance. Do you agree with the list of criteria that are included in Requirements Table R26? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Commenters raised concerns about the interaction between the list of personnel in draft CIP-011-1 R26.1 and the lists of those granting authorized electronic and physical access. In addition, commenters were concerned about the interaction with other user/account management requirements. Some commenters suggested that all maintenance devices should be documented in a list. In addition, there were comments regarding the allowance for emergency maintenance situations.

Some commenters suggested that Requirement R26.1 is duplicative of Requirement R8 and should be removed, and that Requirement R26.2 is duplicative of Requirement R23 and should also be removed. The drafting team considered this feedback and has attempted to address these concerns by incorporating the requirements associated with maintenance into the requirement in CIP-007-5 – System Access Control regarding preventing the introduction of malware into the BES Cyber System, as the objective of these two requirements is the same.

#	Organization	Yes or No	Question 47 Comment
47.1	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
47.2	National Grid	Agree	Please provide clarification on 26.2.
47.3	Puget Sound Energy	Agree	Puget Sound Energy suggests additional language to clarify if personnel referenced in R26.1 are required to be maintained on the lists associated with Table 5.
47.4	Southern California Edison Company	Agree	SCE requests the Standards Drafting Team combine Requirement R26.1 with other requirements for personnel management and rationalize compliance requirements across personnel.
47.5	APPA Task Force	Agree	The APPA Task Force has no comment on this question.

#	Organization	Yes or No	Question 47 Comment
47.6	Emerson Process Management	Agree	This seems to be a typical task for properly maintaining a cyber (or computer) system. The personnel for doing this task should be already identified in the personnel training, awareness, and risk assessment. This requirement seems to be extra.
47.7	Independent Electricity System Operator	Disagree	- R26.2 define malicious code. Does malicious code mean AV or Spyware detection/prevention or does Malicious code require a code review when deploying code and patches to systems?- R26.1: suggest using a word other than “personnel”
47.8	Network & Security Technologies Inc	Disagree	26.1 - Should be reworded to distinguish “maintenance” personnel from System Administrators, who in most instances also perform maintenance activities. If the SDT concludes there is really no distinction, this requirement becomes redundant and should be eliminated, as lists of users and the permissions they have (including “System Administrator”) are already required.26.2 - Many test devices are appliances and may not be capable of meeting other CIP-011 requirements, including malicious code protection. Thus, this requirement needs to be eligible for TFEs.
47.9	Dairyland Power Cooperative	Disagree	26.1 This overlaps with the requirement of limits access based on electronic accounts. How can this be blended with user/account management?
47.10	ERCOT ISO	Disagree	26.1: Recommend addressing emergency situations more clearly. How should an entity address listing authorized personnel where support companies use a call center and cannot provide dedicated resources for the entity? This is particularly relevant for after-hours issues.
47.11	Regulatory Compliance	Disagree	26.2 - Propose this phrasing:Insure maintenance devices are free and clear of malicious code prior to the intoduction to the BES System.
47.12	Luminant	Disagree	26.2 should read "Detect and respond to the introduction of malicious code."
47.13	Southwest Power Pool	Disagree	26.2: Requirement is not necessarily applicable to special purpose testing devices, such as Fluke meters. Need to revise to limit the requirement to general purpose

#	Organization	Yes or No	Question 47 Comment
	Regional Entity		devices for which malware prevention is possible.
47.14	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
47.15	Liberty Electric Power, LLC	Disagree	CIP-026 will penalize entities if malware gets on any device, even if we employ the best available technology and processes to prevent it. This requirement needs to be removed.
47.16	Alberta Electric System Operator	Disagree	Consider revising R26.1 (or creating a new sub-requirement) to include verifying and updating the list of authorized personnel.
47.17	PacifiCorp	Disagree	Devices used for maintenance should also meet the system hardening criteria of R16 and R17.
47.18	MidAmerican Energy Company	Disagree	Devices used for maintenance should meet the system hardening criteria of R16 and R17.
47.19	Dominion Resources Services, Inc.	Disagree	Dominion appreciates the SDT's thoughts in providing this section and its associated exclusions and is very much in favor of this type of requirement. Dominion agrees with the need to protect the BES Cyber System from harm during this process, but is concerned that these requirements are overly broad.26.1. Dominion recommends that this requirement be deleted. All of these actions are covered by other requirements - access controls, change management, training (roles and responsibilities). It adds another layer of administrative paperwork to track every action made by every authorized technician with no corresponding protection to the BES. 26.2. It appears that this requirement intends to allow technicians to connect their personal laptops to relays without having to reformat them afterwards. This requirement has the unintended consequence of including any device used for maintenance (e.g., fluke meters, etc.). A footnote to avoid the necessity of a potential TFE should be added.

#	Organization	Yes or No	Question 47 Comment
47.20	US Bureau of Reclamation	Disagree	Either individuals have access authorization or they don't. This would appear to be an unnecessary tracking requirement.
47.21	RRI Energy	Disagree	Even if a maintenance device is completely up-to-date on all security patches, and also has up-to date virus detection software with the most recently release virus pattern definitions, I can not 100% ensure that malicious code will not accidentally be introduced to a BES cyber system while connected. "Ensure" is a very absolute word that is hard to match in practice. It would be better to "require " that maintenance devices have the same level of virus protection and patch management as BES Cyber Assets which the maintenance devices are being used to maintain.
47.22	ReliabilityFirst Staff	Disagree	How do personnel get authorized for addition to the list in row 26.1 and how often does this list get reviewed and updated. Add requirements for the conduct of a vulnerability assessment and actions to be taken (i.e., mitigation plan) resulting from this vulnerability assessment.
47.23	Western Area Power Administration	Disagree	How do we differentiate between "maintenance" and "administration"? This seems like a new role? This should be worked into Table R10.
47.24	WECC	Disagree	Item 26.1 would have strong impact on the ability to get timely technical support from large global companies such as Cisco Systems. Perhaps there needs to be distinct definitions for "authorized access" vs "maintenance access"? Item 26.2 seems to be covered in previous R15.The requirement does not state that maintenance devices "directly connect" to BES Cyber Systems. In practice, much maintenance is done via network connections. These criteria need to be reassessed if they are intended to apply to network or remote access.
47.25	NextEra Energy Corporate Compliance	Disagree	NextEra believes that Requirement R26 does not provide anytime frame in which the list should be reviewed nor does it take into consideration vendors. The current language does not provide clear guidance and leaves room for interpretation. The following are the recommended updates:26.1 - NextEra suggests maintaining a list of

#	Organization	Yes or No	Question 47 Comment
			personnel authorized to perform maintenance on the BES Cyber System, allow authorized personnel to escort cyber and physical vendors, and allow only authorized personnel to perform maintenance on the BES Cyber System. The list of personnel authorized to perform maintenance of the BES Cyber System should be updated at least annually.Maintenance devices not permanently connected to BES Cyber Systems are not considered part of the BES Cyber System.
47.26	Allegheny Energy Supply	Disagree	R 26.1 is duplicative of Requirement 8 and should be removedR 26.2 is duplicative of Requirement 23 and should be removed.
47.27	Allegheny Power	Disagree	R 26.1 is duplicative of Requirement 8 and should be removedR 26.2 is duplicative of Requirement 23 and should be removed.
47.28	EEI	Disagree	R 26.1 is duplicative of Requirement 8 and should be removedR 26.2 is duplicative of Requirement 23 and should be removed.
47.29	Southern Company	Disagree	R.26.1 If personnel are required to have a PRA, are granted physical access, system usage is logged and the individual has access credentials for cyber systems, the additional list generation should not be required.Vendor personnel supporting systems would need to be added to the personnel listing, these personnel frequently change. The addition of a name to the list would become a common event.
47.30	Consultant	Disagree	R26 - Suggest changing wording to "implement and document"Suggest changing wording to: "Systems and to ensure that" for correct grammar.R26 - Delete the word "accidentally" from the statement. It would appear a better objective is to prevent the introduction of malicious code, "accidentally" or "intentionally" is not relevant to the objective.Table R26 - Item 26.1 This is a new account management requirement. There are account management activities for cyber access, physical access, information access, and now maintenance access. As such this requirement should be moved to the account management requirements table.Item 26.2 This is not a requirement statement, it is a statement of a desired objective. It is not clear what

#	Organization	Yes or No	Question 47 Comment
			requirement or requirements are intended to meet this objective. Please clarify the requirement.
47.31	FirstEnergy Corporation	Disagree	R26 text needs to be more specific that the intention is for temporary direct connections. Otherwise, R26 appears to be covering CIP 7R1 and 7R3.
47.32	Progress Energy (non-Nuclear)	Disagree	R26.1 - do not see need for this requirement. Changes can only be made with cyber access rights which is covered by other requirements.R26.2 - either eliminate this requirement or make additional provisions for the safe use of maintenance components. CIP standards shouldn't mandate malware protection on all test equipment. The BES Cyber Systems components should already be adequately protected from threats as a result of being compliant with the other requirements.We like the use of the footnote earlier in the standard that allowed the use of the highest level of protection the components can support maybe something like that could be used here too.
47.33	Public Service Enterprise Group companies	Disagree	R26.1 requires maintaining another list of personnel who perform maintenance on a BES Cyber System. These individuals are already tracked and documented under other access lists. Seems like a duplication of effort with no benefit and thus the requirement should be deleted.
47.34	Xcel Energy	Disagree	R26.2 - The requirement should be worded to require anti-malware protection on all maintenance devices. The current wording would make it an enforceable violation if, in spite of best efforts, malware was introduced in to a device.
47.35	Hydro One	Disagree	Recommend adding a Requirement for listing the devices used for maintenance activities.
47.36	Northeast Power Coordinating Council	Disagree	Recommend adding a Requirement for listing the devices used for maintenance activities.

#	Organization	Yes or No	Question 47 Comment
47.37	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that different sections with similar requirements be aligned to avoid confusion. In Table 26, with respect to R26.1, other sections contain similar requirements for Physical Security, Electronic Access, and System Security. We'd prefer to see them re-aligned in a fashion similar to the way the older version of the Standards have them. The new maintenance requirements can be added into those Standards. Similar comment for 26.2; SDG&E feels that this could have been added to the System Security/Protection area.
47.38	LADWP	Disagree	See previous
47.39	BGE	Disagree	Should not have a separate list for maintenance personnel. All personnel should be included on the access control lists created per R7 - R14.
47.40	Duke Energy	Disagree	Suggest replacing "Cyber System Maintenance" with "Cyber System Configuration Management".Requirement 26.1: Please consider adding the word "cyber security related" to make the definition read as follows:Maintain a list of personnel authorized to perform cyber security related maintenance on the BES Cyber System and allow only authorized personnel to perform maintenance on the BES Cyber System.Requirement 26.2: Please consider changing as highlighted below:Detect and prevent the introduction and propagation of malicious code on all computer based maintenance devices.Remove 'accidently' from R26. Suggest removing all of R26.26.1 Specify maintenance performed is done with the maintenance device. We interpret 26.1 to be that the maintenance personnel would not have to be background screened and trained. Suggest including screens and trains for these folks. Or remove the requirement with the understanding that these personnel will have electronic or unescorted physical access to the BES Cyber System. This is extra work for no added security.26.2 will need a TFE. Within generation, we have differing opinions on the definition of code. Suggest clarifying that it does not include programming code.
47.41	Detroit Edison	Disagree	Table R26.2 only addresses the introduction and propagation of malicious code into

#	Organization	Yes or No	Question 47 Comment
			the BES Cyber System. It is likely however, that a device may be modified not to introduce or propagate code but act as a bridge to another rogue network via wireless, cellular or other medium. This would be akin to introducing an unsecured access point into the boundary if this system is not subject to the same requirements equal to or greater than that of highest impact BES Cyber System component. A possible solution could be to require mitigation for multi-homed or bridged networks for all components used for BES Cyber System maintenance, and/or append R26 to read "...and ensure that systems used for maintenance do not introduce malicious code into the BES Cyber System or act as an unauthorized access point into an Electronic Security Perimeter."
47.42	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent unauthorized maintenance on BES Cyber Systems and ensure that systems used for maintenance do not accidentally introduce malicious code into the BES Cyber System") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R26, Section 26.2. It is impossible to prevent the introduction and propagation of malware. This is already addressed in Requirement 15. Recommendation: Delete Section 26.2.
47.43	Manitoba Hydro	Disagree	The personnel authorized to perform maintenance on the BES Cyber System should be identified by roles, not individual names. There are no specifics given with respect to "prevent" in Requirement R26.2 so it is assumed to be at the Responsible Entity's discretion in terms of means, criteria, etc.
47.44	Reliability & Compliance Group	Disagree	There is a possible issue that could occur with this requirement regarding collective bargaining unit rules. It may require that job classifications be created for individuals who work on these systems.

#	Organization	Yes or No	Question 47 Comment
47.45	Constellation Energy Commodities Group Inc.	Disagree	There is no definition of malicious code provided. Clarify the scope of malicious code to include virus, malware and spyware protection, as currently generally commercially understood.
47.46	Minnesota Power	Disagree	Using the definitions proposed in Question 46, Minnesota Power recommends that Requirement R26 state that "prior to connecting Maintenance Equipment or importing data, patches, code or other electronic files into the BES Cyber System, the device and/or files shall be scanned for malware and up-to-date on security patches."
47.47	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
47.48	We Energies	Disagree	We Energies agrees with EEI: R 26.1 is duplicative of Requirement 8 and should be removedWe Energies agrees with EEI: R 26.2 is duplicative of Requirement 23 and should be removed.
47.49	Florida Municipal Power Agency	Disagree	Why is malware mentioned in 26.2, when it already has been covered in R15? FMPA believes this should be removed.

48. Table R26 provides direction concerning what impact level of BES Cyber Systems to which Requirement R26 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Several commenters suggested that the types of connectivity used for temporary connections should be considered. In addition, several commenters suggested that the criteria should be applied to all impact levels. There was also a comment for a no impact category.

The drafting team considered this feedback and attempted to address these concerns by incorporating the requirements associated with maintenance activity into the requirement in CIP-007-5 – System Access Control regarding preventing the introduction of malware into the BES Cyber System, as the objective of these two requirements is the same.

#	Organization	Yes or No	Question 48 Comment
48.1	WECC		Criteria should apply to all impact levels
48.2	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels proposed for R26 if it is understood that a blank in the table means N/A.
48.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
48.4	Progress Energy - Nuclear Generation	Agree	R26 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
48.5	Allegheny Energy Supply	Disagree	R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extend an electronic security perimeter.

#	Organization	Yes or No	Question 48 Comment
48.6	Allegheny Power	Disagree	R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extend an electronic security perimeter.
48.7	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
48.8	American Municipal Power	Disagree	Please provide a little or no impact category
48.9	BGE	Disagree	Should not be separate requirements for maintenance of BES Cyber Systems.All personnel should be included on the access control lists created per R7 - R14.
48.10	Consultant	Disagree	The comments on Question 47 regarding moving item 26.1 elsewhere, and Item 26.2 not being a requirement statement preclude an evaluation of application to impact categories.
48.11	Duke Energy	Disagree	Require for low when the maintenance device also connects to medium or high systems.
48.12	EEI	Disagree	R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extent an electronic security perimeter.
48.13	Entergy	Disagree	Basic Maintenance requirements should apply equally for all components of a control system
48.14	FirstEnergy Corporation	Disagree	Until clarity is provided on the above comments (Q46 and Q47), we can not provide a

#	Organization	Yes or No	Question 48 Comment
			response to this question.
48.15	Florida Municipal Power Agency	Disagree	FMPA believes this standard should be removed entirely, as it is already addressed under account control, R7.
48.16	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
48.17	Progress Energy (non-Nuclear)	Disagree	See comment 14.
48.18	Public Service Enterprise Group companies	Disagree	General agreement, but Requirement 26.2 may not be technically feasible for certain types of maintenance devices. To implement this requirement, an Operating System level change to the component may be required, which may be infeasible or not available from the Original Equipment Manufacturer (OEM). This requirement needs to be qualified with the phrase "where technically feasible".
48.19	ReliabilityFirst Staff	Disagree	Suggest "Required" for Low Impact in rows 26.1 and 26.2.
48.20	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that different sections with similar requirements be aligned to avoid confusion. In Table 26, with respect to R26.1, other sections contain similar requirements for Physical Security, Electronic Access, and System Security. We'd prefer to see them re-aligned in a fashion similar to the way the older version of the Standards have them. The new maintenance requirements can be added into those Standards. Similar comment for 26.2; SDG&E feels that this could have been added to the System Security/Protection area.
48.21	Southern California Edison Company	Disagree	The drafting team has chosen to treat ancillary systems used to perform maintenance type activities on a BES system as equally critical. If this is not the intent of the team, the wording of the standard should be modified to reflect the difference in impact levels.

#	Organization	Yes or No	Question 48 Comment
48.22	Southwest Power Pool Regional Entity	Disagree	26.2 should be applicable to all impact categories.
48.23	US Army Corps of Engineers, Omaha Distirc	Disagree	There needs to be a provision for emergency work. Whether that means talking someone through a fix at 2am or hiring a vendor for additional expertise.
48.24	We Energies	Disagree	We Energies agrees with EEI: R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extent an electronic security perimeter.

49. Requirements R27 to R29 of draft CIP-011-1 concern procedures for Cyber Security Incident response. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R27 to R29? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Cyber Security Incident Response" is now addressed in CIP–008–5 — Cyber Security — Incident Reporting and Response Planning.

One of the primary focus areas of the comments concerned coordination with the reporting requirements in CIP 001 and EOP-004 for reporting to the ES-ISAC, and additional guidance in determining incident classifications. The SDT has attempted to coordinate with the drafting team working on revisions to CIP-001 and EOP-004 to ensure the two sets of requirements are coordinated. As the two teams are working in parallel, continued coordination will be necessary.

Several commenters asked for definitions for cyber security incidents and reportable cyber security incidents. The SDT developed a revised definition for "**BES Cyber Security Incident**" as follows:

A malicious act or suspicious event that:

- *Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or*
- *Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or*
- *Results in unauthorized physical access into a Defined Physical Boundary.*

The SDT also proposed a new definition of "**Reportable Cyber Security Incident**" as follows:

Any BES Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service.

Several requests were made to clarify the periodic timing requirements such as annual, calendar year, and 12 months. The drafting team reviewed the timing elements of all requirements and where there was a reference to "annual" the SDT replaced this with the following:

". . . at least once each calendar year, not to exceed 15 calendar months between. . ."

Some commenters recommended placing all requirements in the table, not in the objective or in the "pre-amble" for cyber incident reporting, and the drafting team has included all mandatory performance in the requirements.

Many commenters requested clarifications for plan testing requirements, operational exercises, test environment, as well as the number of tests required. The drafting team did attempt to add more clarity to plan testing requirements along with operational exercise, test environment, and number of tests required in the revised standard (CIP-008-5).

Guidance was requested regarding review of the results of incident response tests in less than 60 days. The revised standard now requires the review to take place within 30 calendar days and the update, based on lessons learned, to take place within 60 calendar days of the test.

Some commenters asked for clarity on the inclusion of physical breach aspects of cyber security incidents as reportable. The drafting team is coordinating its revisions with the revisions to CIP-001 and EOP-004 underway through Project 2009-01 – Disturbance and Sabotage Reporting.

There were concerns raised as neither logging nor monitoring are required for Low Impact BES Cyber Systems, there is no basis for requiring Cyber Security Incidents on these systems to be tracked or classified. The applicability section of the entire suite of CIP Version 5 standards has been revised to provide greater clarity on which BES Cyber Systems (High, Medium, and Low Impact) are applicable to specific requirements.

#	Organization	Yes or No	Question 49 Comment
49.1	National Rural Electric Cooperative Association (NRECA)		In R27.1 a "process" is required, but it is not clear as to how a utility is required to "classify" events. Please provide further clarification as to how one is required to "classify" these events.In R29.1 the requirement is to review the plan once every 12 months. Please provide specificity as to what "once every 12 months" means. If I review the plan on Jan. 15, 2001, am I in compliance if I review it again by Jan. 25, 2002? Please make sure that this is clear in the requirement and in all requirements of CIP-010-1 and CIP-011-1.
49.2	Tenaska		Consider combining 28 and 29
49.3	Black Hills Corporation	Agree	Request that the language in 27.3 be broadened to include contacting appropriate law enforcement authorities, similar to CIP-001.
49.4	FEUS	Agree	Agree with Comments: the drafting should clarify the reporting time requirement for

#	Organization	Yes or No	Question 49 Comment
			27.3, reporting to the ES-ISAC
49.5	Green Country Energy	Agree	I really see the need for a reference document or footnotes pointing to sources for guidance on the expectations for these requirements.
49.6	SCE&G	Agree	R29 is a good example of an instance where there are a lot of timing requirements embedded in the requirements. It would be helpful to entities if timing requirements were consistently put in the same location in the tables (under the low, medium, and/or high columns) rather than embedded in the text. The SDT should evaluate the number of timed requirements in relation to the low, medium, and high impact categories. Once the requirements are finalized it would be of benefit to entities to have a list of the timeframe type requirements which must be met for each low, med, and high impact system, as these often present some of the greatest administrative burden in documenting these timeframes were met.
49.7	Allegheny Energy Supply	Disagree	Suggested modification to R27.3: "Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC)."If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.
49.8	Allegheny Power	Disagree	Suggested modification to R27.3: "Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC)."If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.
49.9	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
49.10	Ameren	Disagree	R27 would be better suited in CIP-001, Sabotage Reporting.â€,â€,â€,

#	Organization	Yes or No	Question 49 Comment
49.11	American Electric Power	Disagree	27.1 - 27.3: Recommend requiring this for systems with routable external connectivity only. To properly monitor and alert on cyber security events, a trained IT Security Operations staff and dedicated set of monitoring tools are required. If there is no external connectivity, there is no access for the IT teams to monitor these cyber systems.
49.12	APPA Task Force	Disagree	The APPA Task Force supports the drafting team's efforts on incident response. We propose the following edits:The APPA Task Force believes that NERC, as the ES-ISAC, should have a standard process for entities to use in reporting Cyber Security Incidents. Therefore, we propose the following wording for R27 Table 27.3: 27.3: Use the reporting guidance developed by the ES-ISAC for reporting Cyber Security Incidents, either directly or through an intermediary, or develop a process equivalent or superior to that guidance.28.1, recommend changing "once every 12 months" to "Annually."29.1, recommend changing "once every 12 months" to "Annually."
49.13	Bonneville Power Administration	Disagree	The objectives of these requirements ("so that responses to Cyber Security Incidents involving BES Cyber Systems can occur" and "to verify its response plan's effectiveness in responding to a Cyber Security Incident impacting a BES Cyber System") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table 28, Section 28.1. It's not clear whether testing in January 2010 and June 2011 would satisfy the requirement, since February 2010 through January 2011 would be a 12-month period with no testing. Recommendation: Replace "every 12 months" with "each calendar year". Also, there are other ways to test, as well. Recommendation: "Test the execution of the incident response plan (by recovering from an actual incident, or with a test at least as comprehensive as a paper drill) at ... Table 29, Section 29.1. Same comment as 28.1

#	Organization	Yes or No	Question 49 Comment
49.14	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
49.15	Consultant	Disagree	R27 - "...so that responses to Cyber Security Incidents involving BES Cyber Systems can occur." should be reworded. Suggest "to identify responsibilities and actions in response to an incident associated with BES Cyber Systems."Table R27 - should specify in each statement that it applies to BES Cyber Systems."Cyber Security Incident" is defined in the Glossary using the terminology from CIP-002 through CIP-009. That definition should be revised by including a new definition in this standard using the terminology associated with CIP-010 and CIP-011.Item 27.3 Not all Cyber Security Incidents are reportable to ES-ISAC as indicated in The Security Guidelines for the Electricity Sector: Threat and Incident Reporting, version 2.0, dated April 1, 2008. Suggest clarifying the statement about reporting.Table R28 - Item 28.1 Clarify the periodicity to be consistent throughout the standard. Annual, 12 months, or other statement. Suggest getting information from the nuclear industry on stating and handling periodicity of requirements.Table R28 - Item 28.1 It is not clear from the table whether one test is required, or two tests (one for High Impact & one for Medium Impact) Suggest some clarification wording in the requirement statement.Table R29 - Item 29.1 Clarify the periodicity to be consistent throughout the standard. Annual, 12 months, or other statement. Suggest getting information from the nuclear industry on stating and handling periodicity of requirements.Item 29.2 - Suggest deleting the word "each" as an unnecessary word.Item 29.3 - Actions necessary to address documented plan deficiencies may not be completed within 30 days, so requiring an update to the plan with 30 days would appear to create a situation where compliance is not viable, or sensible. Suggest modifying to be based on completion of corrective actions.Item 29.5 Suggest deleting the word "all" as an unnecessary word.
49.16	Detroit Edison	Disagree	Table 28.1 and 29.1 refer to a period of "12 months". We prefer “at least once per calendar year, not to exceed 14 months between instances”.

#	Organization	Yes or No	Question 49 Comment
49.17	Dominion Resources Services, Inc.	Disagree	Per R18, neither logging or monitoring are required for Low Impact Systems, hence there is no basis for requiring Cyber Security Incidents on these systems to be tracked or classified.
49.18	Duke Energy	Disagree	Requirement 27: The requirements need a definition of a "Cyber Security Incident". This needs to differentiate between a cyber security attack and a mistake that a technician makes in the plant. We don't need to report every time a technician forgets their password.Requirement 28 only has one item and it is related to Requirement 29. Perhaps combine these two?Table 28: 28.1 assumes there is only one incident response plan when R27 allows for multiple plans. We would like to test AN incident response plan instead of all of them. Or allow for a different time frame (12 months per plan) to test all of them. Combine 28 with 29 if the VSL is the same.Table 29: 29.1 We would like to review AN incident response plan instead of all of them. Or allow for a different time frame (12 months per plan) to review all of them.
49.19	E.ON U.S.	Disagree	Comments: CIP-011, R27 The application of this standard to low-impact BES CS's seems inconsistent. There are not requirements for monitoring security events associated with these assets.CIP-011, R29.1 The application of this standard to low-impact BES CS's seems inconsistent with other requirements for monitoring security events associated with these assets.CIP-011, R30.2 Please clarify whether "...identification of the personnel responsible..." require naming individuals, or job functions?
49.20	EEI	Disagree	Suggested modification to R27.3: "Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC)."If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.

#	Organization	Yes or No	Question 49 Comment
49.21	Emerson Process Management	Disagree	Without being required to perform tasks in System Security, low impact BES Cyber systems may not be able to easily classify cyber security incidents.
49.22	Entergy	Disagree	The current definition of “Cyber Security Incident” will need to be changed as it references ESPs and PSPs. As such, it may be a good idea to define what this term means here.It is observed that as written there is no longer a requirement to keep documentation associated with a Cyber Security Incident (i.e., akin to CIP-008 R2). Is this the intent?
49.23	ERCOT ISO	Disagree	29.2: Should be 30 days rather than 60 days to align with FERC Order 706.
49.24	FirstEnergy Corporation	Disagree	27.1: From CIP-008 R1.1, what happened to the concept of "reportable"?
49.25	Independent Electricity System Operator	Disagree	- R27.1: note that the word “reportable” has been removed; CIP-008-2, R1.1 stated “Procedures to characterize and classify events as reportable Cyber Security Incidents”- R28.1: modify the sentence to state “Test the execution of the Cyber Sec
49.26	ISO New England Inc	Disagree	see recommendation for review in prior requirements use same for all annual/ 12 month review.
49.27	Manitoba Hydro	Disagree	The wording of Requirement R28.1 should be revised as the phrase “with a paper drill” could be misinterpreted. There are no specifics given with respect to ‘classifying’ events in 27.1 so it is assumed to be at the Responsible Entity’s discretion in terms of criteria, etc.
49.28	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R27, but recommends that the last phrase be changed from “so that responses to Cyber Security Incidents involving BES Cyber Systems can occur” to “so that responses to Cyber Security Incidents involving BES Cyber Systems follow a defined plan.” Responses can (and will) happen with or without a plan. The purpose of R27 is to define, ahead of time, a process to ensure an orderly response.Minnesota Power

#	Organization	Yes or No	Question 49 Comment
			generally agrees with the proposed Requirements R29, but recommends that this Requirement should be revised to ensure consistency with Requirement R32. For example, Part 29.1 should state "Review the incident response plan(s) at least once every 12 months or when BES Cyber System(s) have any system, organization or technological changes. Document any identified deficiencies, changes or improvements.") If this language was consistent with Requirement R32, the following issues could be resolved. In addition, the Standards Drafting Team should consider whether or not Parts 29.2 - 29.5 should also be required of Medium Impact Systems (since Part 28.1 requires testing for those systems) with a longer timeframe.
49.29	Network & Security Technologies Inc	Disagree	R27 - should clarify whether cyber security incidents of a physical nature are included and, if so, should tie back to 5.11.29.2 - Sixty days seems like a very long time to wait before evaluating the effectiveness of response actions, esp. if they were taken in response to an actual incident. Suggest revising to require a much more immediate "after action" review, at least for actual incidents. Should be a matter of days - perhaps 7 or less, not months. Even for tests, 60 days seems overly generous. Suggest revising to 30 days.
49.30	Nuclear Energy Institute	Disagree	Does the definition of cyber security incident, as used in this Standard, comport with the definition in Section 215 of the FPA? ("The term "cybersecurity incident" means a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system.")
49.31	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
49.32	Progress Energy - Nuclear Generation	Disagree	Incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security

#	Organization	Yes or No	Question 49 Comment
			Plans for comments for nuclear generating facilities.
49.33	Progress Energy (non-Nuclear)	Disagree	What makes 28.1 and 29.1 different that requires 2 different requirements? If you test the execution every 12 months then you have effectively done a review.
49.34	ReliabilityFirst Staff	Disagree	Problem with auditing the "effectiveness" of R28 without some clear guidelines that would lead to consistent application by all auditors. For R29.4, please clarify what is meant by system, organizational, and technology changes.
49.35	San Diego Gas and Electric Co.	Disagree	SDG&E believes that the Incident Response Plan requirements should only apply to Medium and High impact assets. Including Low impact assets in these requirements seems like overkill. For example, in R27.3, we don't feel that we would necessarily report a "Cyber security incident" on a Low impact item to ES-ISAC.
49.36	Southwest Power Pool Regional Entity	Disagree	27.1: Should be a "reportable" cyber incident. May be appropriate to add as a separate requirement to identify Cyber Security Incidents as "reportable." 27.2: "Communication plans" needs to be defined somewhere. 28.1: Consider changing "Test the execution of the incident response plan" to "Exercise the incident response plan." Clarify that the exercise scenario must involve a covered BES Cyber System and that the exercise must follow (actually exercise) the incident response plan steps. Also need to clarify whether each BES Cyber System, or at least one in each impact category represented, must be included in the exercise. Requiring the inclusion of each BES Cyber System is not recommended due the potential burden; this is a clarification issue to ensure the entities and the auditors have the same understanding. 29.1: Should the 12-month requirement be +/- one month? 29.2: Reviewing an exercise or actual response 60 days after the fact is too long. To keep it fresh in the minds of the responders, 30 days max is suggested, 15 days for High impacting systems is preferred.
49.37	US Bureau of Reclamation	Disagree	Why would we have incident reporting requirements related to systems that we have no processes to track them on...? This would appear to be in conflict with many of

#	Organization	Yes or No	Question 49 Comment
			the previous requirements that did not apply to low systems.
49.38	We Energies	Disagree	We Energies agrees with EEI: Suggested modification to R27.3: "Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC)."We Energies agrees with EEI: If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.

50. Tables R27 to R29 provide direction concerning what impact level of BES Cyber Systems to which Requirements R27 to R29 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Cyber Security Incident Response" is now addressed in CIP–008–5 — Cyber Security — Incident Reporting and Response Planning, and "Cyber Security Incident Response Plan Testing" is addressed in CIP-009-5 - Cyber Security — Recovery Plans for BES Cyber Assets and Systems."

The primary focus areas of the comments received was on impact levels and the concern for coordination with the reporting requirements in CIP 001. The SDT has coordinated with the drafting team working on revisions to CIP-001 to ensure the two sets of requirements are coordinated.

Many commenters requested that Incident Response requirements for Low Impact BES Cyber Assets or non-routable connections be removed along with providing improved consistency between requirements related to impact level. The revised requirements (now contained in CIP-008-5) do not apply to Low Impact BES Cyber Assets. The SDT updated the applicability section of all requirements in the entire suite of CIP Version 5 standards.

It was suggested that Requirement R28.1 should be modified to clarify that test plans should be exercised once each calendar year (vs. every 12 months), and that these tests will be conducted on an overall system basis and not on a per system or per component level basis. This requirement is defined in CIP-009-5 Requirement R2.1, Recovery Plan Implementation and Testing. There were suggestions regarding the clarification of the plan testing requirements, operational exercises, and test environment, and there were comments regarding the addition of guidance on Cyber Security Incident classification by adding glossary definitions of Cyber Security Incident and Reportable Cyber Security Incident. The testing requirements, operational exercises, and test environment are described in CIP-009-5, and a couple of terms were added to the NERC Glossary for completeness.

The SDT developed a revised definition for "**BES Cyber Security Incident**" as follows:

"*A malicious act or suspicious event that:*

- *Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or*
- *Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or*
- *Results in unauthorized physical access into a Defined Physical Boundary."*

The drafting team proposed a new definition of "**Reportable Cyber Security Incident**" as follows:

" Any BES Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service."

A few comments were directed at reviewing of results of Incident Response tests in less than 60 days, including the physical aspects of Cyber Security Incidents. The SDT modified this requirement and now requires that this review be performed within 30 days of the BES Cyber Security incident or test and to update the BES Cyber System Incident response plan based on lessons learned within 60 calendar days of the BES Cyber Security incident or test.

Issues identified in comments for the SDT to consider for modifications included additional guidance on performing Cyber Security Incident classification. This is now covered in the guidance documentation for CIP-008 and CIP-009..

With Version 5, the drafting team has worked to make the applicability for each requirement very clear.

#	Organization	Yes or No	Question 50 Comment
50.1	Hydro One		Recommend for consistency incident response plan for medium and high impact mirrors 31.1 and 31.2 time frames not to exceed 24 and 12 months respectively.
50.2	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels proposed for R27-R29 if it is understood that a blank in the table means N/A.
50.3	Bonneville Power Administration	Agree	Items 28.1 in Table R28 and 29.1 in Table R29 states that the incident response plan shall be tested "at least once every 12 months" and that the incident response plan should be reviewed at least once every 12 months." Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently testing or review must occur.
50.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
50.5	Florida Municipal Power	Agree	FMPA believes "12 months" should be changed to "annual"

#	Organization	Yes or No	Question 50 Comment
	Agency		
50.6	PacifiCorp	Agree	29.3 - Does the requirement to update each response plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency?29.4 - When does the clock start ticking? There could be a series of changes, whether technological or organizational, which is part of a project. What is considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is introduced or is modified. Modifications to the response strategy or response activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the response.
50.7	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
50.8	Southern California Edison Company	Agree	SCE recommends that the standards drafting team use the phrase “cyber security incident” or “physical security incident” to differentiate them from the occurrence of system events that may or may not result from the breach of a “cyber” or “physical” control. As the Requirements are currently written, there is no logging and monitoring requirements for low impact systems. It is inconceivable how a registered entity could implement an incident response plan at these facilities when per CIP standards access and use of these facilities is not required. If the drafting team intends for incident response, as it pertains to Sabotage Reporting under CIP 001, they should state it.
50.9	Alberta Electric System Operator	Disagree	In Table R29, for 29.2, consider revising to review results for High Impact systems to within 30 days, and Medium Impact systems to within 60 days.
50.10	Allegheny Energy Supply	Disagree	R 28.1 should be modified to be clear that testing of incident response plans need not

#	Organization	Yes or No	Question 50 Comment
			include every possible BES Cyber System.
50.11	Allegheny Power	Disagree	R 28.1 should be modified to be clear that testing of incident response plans need not include every possible BES Cyber System.
50.12	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
50.13	Ameren	Disagree	R28.1 - Based on the number of Medium Impact Systems this will be labor intensive with no added protection to the BES. Suggest that this requirement only remain for High Impact Systems.
50.14	American Electric Power	Disagree	Please see response to Question 49.
50.15	American Municipal Power	Disagree	Please provide a little or no impact category
50.16	American Transmission Company	Disagree	R27 requires a response to cyber security incident for all Low Impact BES Cyber Systems; however R18 does not require monitoring and/or logging of Low Impact BES Cyber Systems. How do you respond to an incident unless it is being monitored?
50.17	BGE	Disagree	R29 should apply to any BES Cyber System required in R28.
50.18	Black Hills Corporation	Disagree	28.1 and 29.2 should also be required for Low Impact BES Cyber Systems.
50.19	Consultant	Disagree	Table R27 to Table R29 - It doesn't appear to make sense that the Incident Response Plan applies to all impact level categorizations, while testing the plan applies to Medium Impact & High Impact assets, and actions related to updating the plan only apply to High Impact assets.It would seem logical that the columns in this table should indicate the requirements apply to the same impact level assets, which would be either only High Impact assets, or Medium & High Impact assets, but not a mix.
50.20	Dominion Resources	Disagree	29.2 - 29.5 should be required for Medium Impact to be consistent with R28. R29.2 thru R29.5 currently use text to convey numbers (e.g., sixty vs. 60). This is not

#	Organization	Yes or No	Question 50 Comment
	Services, Inc.		consistent with the convention used throughout CIP-011 and is more difficult to read. A single convention using numerical values should be used throughout.
50.21	Duke Energy	Disagree	Requirement 28.1: is this one test of the cyber incident response plan (global) once per 12 months or is this the test of test of the cyber incident response plan for EACH BES cyber system per 12 months? Once globally per 12 months should be plenty.Requirement 29.5: is the communication of updates a broadcast or is specific feedback from each person required? Remove these requirements for Low Impact.
50.22	EEI	Disagree	EEI suggest that R 28.1 should be modified to be clear that test plans should be exercised annually and not at a per system or per component level.
50.23	Entergy	Disagree	These Requirements should apply for all three BES Cyber System/Component Impact categories.
50.24	Garland Power and Light	Disagree	Requirement 27.1, 27.2, 27.3 and 29.1 - remove from “Low Impact” classification
50.25	ISO New England Inc	Disagree	If the Entity’s Incident Response Plan is tested (instead of testing each BES Cyber System), recommend that “Require” should apply for High Impact, Medium Impact, and Low Impact BES Cyber Systems
50.26	LADWP	Disagree	Table 27 - low impact should not be included.
50.27	Manitoba Hydro	Disagree	Cyber Security Incidents for Low Impact BES Cyber System should not require reporting to the ES-ISAC.
50.28	MidAmerican Energy Company	Disagree	29.3 - Does the requirement to update each response plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency? 29.4 - When does the clock start ticking? There could be a series of changes, whether technological or organizational, which is part of a project. What is

#	Organization	Yes or No	Question 50 Comment
			considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is introduced or is modified. Modifications to the response strategy or response activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the response.
50.29	Minnesota Power	Disagree	With the implementation of the changes discussed in Question 49, these impact levels are generally acceptable.
50.30	National Grid	Disagree	o National Grid recommends deleting 27.3 for Low Impact BES CS o National Grid recommends the timeframes for Medium and High Impact in R28 similar to Table R31 31.1 and 31.2 for consistency.
50.31	Network & Security Technologies Inc	Disagree	Table 27 includes Low Impact systems, but Table 18 (event monitoring) does not. Need to change one or the other.
50.32	Northeast Power Coordinating Council	Disagree	Recommend for consistency incident response plan for medium and high impact mirrors 31.1 and 31.2 time frames not to exceed 24 and 12 months respectively.
50.33	Oncor Electric Delivery LLC	Disagree	The Incident Response Plan should be required for the entity, not for every High Impact cyber system. Requirement 29.4, update of Incident Response Plan, we suggest these reviews be conducted quarterly.
50.34	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
50.35	Progress Energy (non-Nuclear)	Disagree	Need to clarify the annual/12 month/365 day issue.
50.36	ReliabilityFirst Staff	Disagree	For R29, each subrequirement should be "Required" for all the "Medium" impact BES Cyber Systems.

#	Organization	Yes or No	Question 50 Comment
50.37	San Diego Gas and Electric Co.	Disagree	SDG&E also feels that instead of using the word “impact” for these Requirements, apply a concept of “risk” for inclusion. We would want to identify the risks with associated systems security and protect accordingly
50.38	Southwest Power Pool Regional Entity	Disagree	28.1 should be applicable to all impact categories. An incident response plan should be tested to verify that it will work when needed. 29.2 through 29.5 should be applicable to all impact categories, perhaps with shorter time frame for higher impact systems.
50.39	US Bureau of Reclamation	Disagree	Why would we have incident reporting requirements related to systems that we have no processes to track them on…? This would appear to be in conflict with many of the previous requirements that did not apply to low systems.
50.40	We Energies	Disagree	We Energies agrees with EEI R 28.1 should be modified to be clear that testing of incident response plans need not include every possible BES Cyber System.
50.41	WECC	Disagree	All items should be required for medium impact levels in R29Criteria should apply to all impact levels.

51. Requirements R30 to R32 of draft CIP-011-1 concern procedures for BES Cyber System Recovery. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R30 to R32? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Recovery Plans" are now addressed in CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems

The primary focus areas of the comments were concerns with improving the clarity of the periodic timing requirements, the requirement to reinstall and configure any application and system software using its baseline configuration vs. functionality, and the recognition that a large amount of test equipment will be necessary to develop representative environments for numerous disparate facilities.

Some commenters noted the different terms used for references to annual activities. The SDT reviewed the use of annual, calendar year, 12 months, etc. and in the revised standards used the phrase, ". . .at least once each calendar year, not to exceed 15 calendar months between. . ." .

There were suggestions that the testing requirements should only apply to control centers. Additional guidance was requested for operational testing, the use of redundant sites as an acceptable means to address recovery, and for testing of information that is stored on backup media. The SDT added some information about testing in the Rational Box for the proposed CIP-009-5 R1. Testing is necessary to verify the Responsible Entity's Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

Recovery Testing – Operational Test every 36 months should count for the annual test. The SDT notes that there is a FERC directive to add a requirement to conduct a full operational test of the recovery plan once every three years – so the suggestion to count the full operational test as the annual test was adopted. Areas of opportunity suggested for modification of the standards by the SDT were to provide recovery plan testing clarifications, data retention plan clarification, identification requirements of "Personnel Responsible", and incident recovery plan reviews.

Commenters suggested changes and provided various requests/suggestions for re-wording/wordsmithing and improved coordination of backup and recovery with EOP-008. The SDT has coordinated its proposed requirements with the now FERC approved EOP-008-1 – Loss of Control Center Functionality. Commenters suggested that all requirements should be in the table, not in the objective or in the "pre-amble" to the requirements and that the SDT should consider providing a summary table for all periodic requirements and remove the "how to" statements from the requirements. The SDT has included all mandatory performance in the requirements of the revised

standards. The SDT did not adopt the suggestion to develop a summary table for periodic requirements as the format for Version 5 is considerably different from the format proposed when the requirements were all combined in CIP-011.

Several commenters suggested adding definitions for terms such as “initially stored,” and the SDT believes that these terms do not have a unique meaning when used in the standard and do not require a formal definition. The team has tried to limit its proposed definitions to those terms that either have a unique meaning when used in a NERC Reliability Standard, or when misunderstanding a word may have a material impact to reliability.

#	Organization	Yes or No	Question 51 Comment
51.1	Dairyland Power Cooperative		30.5 does the system test require a test of every element in the recovery plan? If a recovery plan covers multiple systems, must all systems be tested annually? Or is it sufficient to test some scenarios affecting some systems?
51.2	National Rural Electric Cooperative Association (NRECA)		In R31.1 and R31.2 there are references to "once every 24 months" and "once every 12 months." Please ensure these timeline requirements are clear similar to my comments in Question 49 regarding R29.1.
51.3	SCE&G		R31.3: What constitutes and operational exercise? What is the scope of the recovery and systems to be covered (all high impact cyber systems, or one sample system if the same recovery plan is used acroos all)?
51.4	WECC		Item 31.2 looks like it should be two separate items. Consider making a separate item for “Test any information used...” at the same required level for high impact.
51.5	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
51.6	Florida Municipal Power Agency	Agree	30.5 mentions restoring to the previous baseline configuration, without regard to the fact that the baseline may have been the source of the problem. FMPA suggests “prior”, giving the RE the flexibility to restore systems based on what they know to be a working system.

#	Organization	Yes or No	Question 51 Comment
51.7	Independent Electricity System Operator	Agree	- R30.1 Please define Recovery Plan. Some regions are not accepting a backup control center, with redundant systems and data as suffice for recovery and think it means building a component from scratch (ie install os, configuration, install application,
51.8	PacifiCorp	Agree	30.4 - Define "protection of information required to successfully restore".30.5 - The requirement to reinstall and configure any application and system software using its baseline configuration does not consider strategies, such as redundancy or high availability, making the reinstall of a system unlikely and impractical.Define "secure backups" and "functionality".31.2 - By including the testing of information used in the recovery of BES Cyber systems that is stored on backup media in 31.2 means that Low and Medium Impact BES Cyber Systems do not require testing of such information? If so, it should be a standalone requirement.Define "initially stored", "useable and current". This could be interpreted as a full restore to a system, one file being restored as verification that data is not corrupt and process to restore are in place to looking at a tape log and seeing that a backup was made of the data.32.4 and 32.6 - When does the clock start ticking. There could be a series of changes, whether technological or organizational, which is part of a project. What is considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is introduced or is modified. Modifications to the recovery strategy or recovery activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the recovery.31.5 - Does the requirement to update each recovery plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency?
51.9	Southern California Edison Company	Agree	The standard should clarify that the time line for the operational exercise that is required by R31.3 is not 36 months for every device is scope, but rather than every disaster recovery plan has to be tested on a scheduled basis.The operational impact of protecting backups at par with operational BES systems is substantial. The backup

#	Organization	Yes or No	Question 51 Comment
			does not support real time BES reliability and should be treated as an ancillary system (i.e. climate control, fire prevention etc.) or similar to systems such as access points and boundary protection devices.
51.10	Alberta Electric System Operator	Disagree	In Table R30, for 30.5, consider changing “known secure backups” to “known good backups” since availability and integrity are more important than confidentiality during system recovery.
51.11	Ameren	Disagree	R30.1 - If you miss listing all conditions or you fail to activate your plan if the certain condition is met makes this difficult to provide complete documentation for an audit. Suggest removal or changing the phrase to "List possible conditions that may activate the recovery plan, update these conditions within 30 days of an actual incident that was not included within the scope of the originally documented conditions."
51.12	American Electric Power	Disagree	31.2: Regarding "Test any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least every 12 months to ensure that the information is useable and current", should this be a separate line item? It seems out of place in 31.2.
51.13	APPA Task Force	Disagree	The APPA Task Force supports the drafting team’s efforts on System Recovery. We propose the following edits:31.2, recommend changing “once every 12 months” to “Annually.”32.1, recommend changing “once every 12 months” to “Annually.”32.4, recommend changing “once every 12 months” to “Annually.”
51.14	BGE	Disagree	Provide definition of “operational exercise”
51.15	Bonneville Power Administration	Disagree	The objectives of these requirements (“so that BES Cyber Systems can be restored to a defined state,” “to verify recovery plan readiness and effectiveness,” and “to ensure that the recovery plan(s) will function as intended and that personnel are aware of any relevant changes”) should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the requirement rather than

#	Organization	Yes or No	Question 51 Comment
			appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R30, Section 30.5 is too prescriptive. For example, one way to do backups is to take a complete image of the system. Restoration becomes merely an issue of restoring that image. There is no need to reinstall and reconfigure. Recommendation: Remove 30.5Table R31, Sections 31.1 and 31.2. There are other ways to test, as well. Testing methods should be devised by the RE, not the standard. The frequency may vary based on the Impact status of the system. However, standardization on the middle ground of at least once every 24 months would simplify compliance.
51.16	Con Edison of New York	Disagree	This criterion should be for control centers or SCADA system only. Many cyber systems which would need to comply with CIP-011 do not have back-ups. The BES can be operated effectively even if other cyber systems are down.
51.17	Constellation Energy Control and Dispatch, LLC	Disagree	Provide a definition of operational exercise.
51.18	Constellation Power Source Generation	Disagree	R31.3 uses the term “representative environment.” At the CIP V4 Workshop, the team stated they used this vague term to give entities flexibility in their operational exercises, but this is not auditable.
51.19	Consultant	Disagree	Table R30 Item 30.5 - First bullet - Suggest changing the word "defined" to "documented" or "identified" or "identified and documented". R23 does not define the baseline.Item 30.5 - Second Bullet - Suggest deleting the words "any" & "most" & "known" & "secure" New wording: "Load information from recent backups." Suggest deleting this bullet. Reloading backup date should be an operational decision made based on the conditions that exist at the time of recovery, and not "forced" by a requirement.Table R32 - Item 31.2 This is two requirements. Suggest separating each into it's own line item.Table R32 - The periodicity requirements of this table should be adjusted. The testing and operational exercise statements are not consistent with the

#	Organization	Yes or No	Question 51 Comment
			incident response plan requirements. Suggest making the requirements for incident response plans and recovery plans consistent.Item 32.2 & 32.3 Suggest changing the word "execution" to "occurrence".Item 32.5 - Actions necessary to address documented plan deficiencies may not be completed within 30 days, so requiring an update to the plan with 30 days would appear to create a situation where compliance is not viable, or sensible. Suggest modifying to be based on completion of corrective actions.Item 32.7 Suggest deleting the word "all" as an unnecessary word.
51.20	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R31.2 the term “current” is not valid if any data has changed since the backup. A backup completed 12 months earlier could never be considered current on an operational system. Consider removing this term.
51.21	Detroit Edison	Disagree	Table 31.2 and 32.1 refer to a period of "12 months". We prefer “at least once per calendar year, not to exceed 14 months between instances”.Table 32.4 should not be an annual update but should be triggered on the required review in 32.2. Consider revising to a sixty day window after the review.Table 32.6 The term "any" is too broad. Consider revising to read "...changes that impact the recovery plan."Table 32.7 Revise "recover" to "recovery"
51.22	Dominion Resources Services, Inc.	Disagree	30.2. The phrase “including identification of the personnel responsible” should be removed from this requirement. Roles and responsibilities should be adequate for the plan. There should not be a need to list 20 relay technicians that could be allowed to recover a substation system. 31.2. The second paragraph of this requirement should be revised to state “Verify BES system can be restored from backup initially and at least annually thereafter”.32.1. The phrase “or when BES Cyber Systems are replaced” should be changed to “or when impacted by BES Cyber System changes.”32.6. The phrase “technology changes” should be changed to “technology changes that impact the recovery plan.” (e.g., not all organizational changes affect the recovery plan.)32.7. The word “recover” should be changed to “recovery”.

#	Organization	Yes or No	Question 51 Comment
51.23	Duke Energy	Disagree	Table 30:30.2 remove “including identification of the personnel”30.3 change ‘personnel responsible’ to “responders”30.5 CIP should not prescribe HOW we restore the system. Suggest removing and adding ‘restoration’ to the list in 30.4Table 31:31.1 multiple plans may be required. Same comment as 28.1 above. Is this once per 12 months per the plan or once per 12 months for each BES cyber system? Suggest allowing 12 months per plan to test.31.2 specify that verifying backup media functionality is an acceptable test.31.3 operational exercises at some generation stations may be unrealistic (unrealistic for availability or costs)Table 32:32.6 this should be part of change managementSuggest allowing 12 months per plan for review.Remove ‘incident’ from 32.2 and 32.3
51.24	EEI	Disagree	Suggested revision for R30.2:Roles and responsibilities of responders, including identification of the personnel (using Job title or job function) responsible for recovery efforts.
51.25	Emerson Process Management	Disagree	It seems there is a conflict between 31.2 and 31.3. If the operational exercise needs to be donw every 36 months per 31.3, then, it should not be needed again every 12 months per 31.2.
51.26	Entergy	Disagree	Entergy agrees for High and Medium Impact Cyber Systems it is important to be able to recover and demonstrate that the recovery plan and backup media used in the process is sufficient to recover the BES Cyber System however, requirement 31.2 and 31.3 appear to be a little redundant although not completely. In requirement 31.3 the entity is required to demonstrate recovery in a representative environment where 31.2 only the backup media is required to be verified as useable and current. Both of these activities provide validation that data can be recovered from the backup media. Requirement 31.3 should be deleted - testing the plan every 12 months either via paper drill or full operational exercise or actual incident coupled with validating the backup media is readable is sufficient to the demonstrate recovery. Requirement 31.1 should be change to include: “Testing any information used in the recovery of

#	Organization	Yes or No	Question 51 Comment
			the BES systems that is stored on backup media when initially stored and at least every 24 months to ensure that the information is useable and current."
51.27	ERCOT ISO	Disagree	30: Request that the use of redundant sites is an acceptable means to address recovery.30.2: Recommend noting what information is necessary here. Are group notifications considered sufficient (e.g., on-call rotations)? 32.2: Should be 30 days rather than 60 days to align with FERC Order 706.
51.28	FirstEnergy Corporation	Disagree	R31 - 31.3 - Need clarity on what is meant by 'Operational' exercise. We believe the intent was business operations, not IT system operations and related DR plan recovery. A business operational exercise is a business continuity planning issue. (example: EMS Operation hot-site testing) Sub-requirement 31.3 would need to be answered by each business unit and not within an IT DR Team response as business operational (BCP) tests are not performed for DR Plans. DR Plans have physical and media type testing which it appears to be what the intent was for 31.1 and 31.2. Need clarity on ownership. It seems like 31.1 and 31.2 are owned by IT, and 31.3 is owned by business units. R32 - 32.6 - We do not agree with changing names in individual recovery plans except during the annual review. Normally organization changes affect the recovery plan approvers list and if changed, would require re-approval of the DR plan. Given the complexity of our critical DR plans, this requirement is not reasonable, and certainly not within a 30 day window - especially if the new name is for someone just starting in a position. We agree that interim organizational changes could be made for call trees of 'personnel expected to respond to/perform a recovery using the recovery plans', but call trees are not part of the individual recovery plans and are instead part of an overall recovery plan. R32 - 32.7 - Recovery is misspelled ('communicate all recover plan...')
51.29	Garland Power and Light	Disagree	Requirement R30 requires the implementation of the plan to be in compliance - Concern is that for some business reason (perhaps a certain business strategy or the economy) some system or facility might not need to be rebuilt. There should be a provision for the Responsible Entity to provide justification to Regional Entity for not

#	Organization	Yes or No	Question 51 Comment
			rebuilding and not be in violation for not implementing and actually rebuilding the "whatever" that failed.
51.30	GE Energy	Disagree	36 months is too long between operational recovery exercises. This should be at maximum 24 months, and should require re-validation if a large system configuration change is made, such as hardware changes, version upgrades, or 3rd party software upgrades.
51.31	GTC & GSOC	Disagree	We recommend R32.1 be changed to the following: "Review and update recovery plan(s) at least once every 12 months or when a Cyber Security Incident recovery of BES Cyber System(s) does not effectively proceed according to the documented plan."We recommend the word "incident" be replaced throughout R30 through R32 with the words "Cyber Security Incident"
51.32	Hydro One	Disagree	Recommend changing the bullets for 30.5 to start with "plans for". The first bullet should be "install" not "reinstall." The recovery plan does not need to include non-BES Cyber Systems. The third bullet should test the BES Cyber System Component(s).
51.33	ISO New England Inc	Disagree	31.2 - "Test any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least every 12 months to ensure that the information is useable and current. "impossible to test " - is this to test if your backup works and is usable? Realtime data is never restored - clarification on information and is this test your media for usability? "Test when initially stored"?? Not feasible. More appropriate Verify backup completed successfully, not verify data that was backed up. Control Centers utilize full functioning backup facilities for recovery from the main center being compromised and or rendered unavailable, so for control centers the recovery should be to run from the backup control center once a year. The media should be tested on an annual base to make sure that the data from the offline storage is still recoverable. For facilities that do not have a backup BES cyber systems then I would agree that they need to recover in the way stated. Recommend changing 30.5 bullets to start with "plans for". The first bullet should be "install" not

#	Organization	Yes or No	Question 51 Comment
			"reinstall." Recommend that the recovery plan does not need to include non-BES Cyber Systems. Recommend that the third bullet should test the BES Cyber System Component(s).
51.34	LADWP	Disagree	CIP-011-1 R30 Cyber System Recovery (CSR) should not require to document identification of the personnel responsible for recovery effort (R30.2) within the CSR. Identification of specific personnel will lead to revision of the document when personnel are reassigned.
51.35	Manitoba Hydro	Disagree	The wording of Requirement R31.1 should be revised as the phrase "with a paper drill" could be misinterpreted. There are no specifics given with respect to the Requirements of R30 (in terms of "conditions", "roles and responsibilities", etc., so it assumed to be at the Responsible Entity's discretion in terms of criteria, etc. Consider whether Requirement R31.2 should be two separate Requirements - R31.2 with respect to "Conduct a test..." and R31.3 with respect to "Test any information...". There are no specifics given with respect to "demonstrates readiness" in Requirement R31.3 so it assumed to be at the Responsible Entity's discretion as to whether the test has demonstrated readiness or not. The word "recover" in Requirement R32.7 should be "recovery".
51.36	MidAmerican Energy Company	Disagree	Define "protection of information required to successfully restore".30.5 - The requirement to reinstall and configure any application and system software using its baseline configuration does not consider strategies, such as redundancy or high availability, making the reinstall of a system unlikely and impractical.Define "secure backups" and "functionality".Define "initially stored", "useable and current". This could be interpreted as a full restore to a system, one file being restored as verification that data is not corrupt and process to restore are in place to looking at a tape log and seeing that a backup was made of the data.32.4 and 32.6 - When does the clock start ticking? There could be a series of changes, whether technological or organizational, which is part of a project. What is considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is

#	Organization	Yes or No	Question 51 Comment
			introduced or is modified. Modifications to the recovery strategy or recovery activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the recovery.31.5 - Does the requirement to update each recovery plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency?
51.37	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R30, but recommends that the Standards Drafting Team consider defining the term "known secure backups" as it is not currently defined in the Standard and is open to interpretation. Part 31.2 requires that data be "tested" at the time of backup and every 12 months to ensure that it is "useable and current" and to ensure consistency with that requirement, Minnesota Power recommends that the Standards Drafting Team replace "known secure" with "useable". Minnesota Power generally agrees with the proposed Requirements R31, but recommends that the Standards Drafting Team further define what is meant by "test" data stored on backup media to "ensure that the information is useable and current" in Part 31.2. While testing usability can be done by verifying one can read the tapes' contents, how does one test that data is current? This would require more of a manual verification or comparison function than a test, correct? In addition, is R31.3 requiring a full restoration, or is it requiring that each scenario documented in the Restoration Plan be fully tested every 36 months? Minnesota Power recommends that the Standards Drafting Team revise the wording of Part 31.3 to eliminate confusion regarding their intent.Minnesota Power generally agrees with the proposed Requirements R32, but to be consistent with the "update" portion R32, Minnesota Power recommends that Part 32.1 be modified to state "Review the recovery plan(s) at least once every 12 months, or when BES Cyber System(s) have any system, organization or technological changes. Document any identified deficiencies, changes or improvements."Minnesota Power generally agrees with the proposed Requirements R32, but recommends that the term "recover" be

#	Organization	Yes or No	Question 51 Comment
			changed to “recovery” for Part 32.7.
51.38	National Grid	Disagree	National Grid recommends changing 30.5 bullets to start with “plans for”. The first bullet should be “install” not “reinstall.” Also recommends that the recovery plan does not need to include non-BES Cyber Systems and that the third bullet should test the BES Cyber System Component(s).
51.39	Network & Security Technologies Inc	Disagree	30.5 - Suggest revising to require use of either baseline configuration or most recent known “good” configuration. Covers the possibility a (new) baseline configuration is causing problems (can and does happen - even if tests pass).30.5 - Need to define what “secure” backup means.31.2 - Requirement to test information “when initially stored” may be extremely burdensome in some environments, depending on backup mechanisms used. Some types of backup systems use on-the-fly techniques to verify a copy/write operation is “good” but SDT should use language that is less prescriptive. Should also drop the word, “current.” Certain types of operational data will cease to be “current” moments after it is copied. Only real-time mirroring can satisfy this requirement and entities should not be compelled to implement it.
51.40	NextEra Energy Corporate Compliance	Disagree	NextEra believes the CIP-011-1 Table R30 - Recovery Plan Specifications so that BES Cyber Systems can be restored to a defined state did not provide enough guidance and left room for interpretations.The following are the recommended updates:30.1 - The Responsible Entity shall define conditions for activation of the recovery plan(s).30.4 - Processes and procedures for the backup, storage and protection of information required to successfully restore a BES Cyber System30.5 - Implement a test plan to identify the processes and procedures for the restoration of BES Cyber Systems to include the following: o Reinstall and configure any application and system software using its baseline configuration defined in Requirement R23, o Load any information from the most recent, known secure backups, o Conduct a system test to verify functionalityModified the wording and additional guidance should be provided by NERC on the minimum conditions which would activate the plan.NextEra also believes that Table R31 - Recovery Plan Testing Specifications to verify recovery

#	Organization	Yes or No	Question 51 Comment
			plan readiness and effectiveness did not talk about documenting test resultsThere should be documentation of test results to validate that it was performed. The following are the recommended updates:31.1 - Conduct a test (by recovering from an actual incident, with a paper drill, or with a full operational exercise) of the recovery plan at least once every 24 months. All testing results shall be documented.31.2 - Conduct a test (by recovering from an actual incident, with a paper drill, or with a full operational exercise) of the recovery plan at least once every 12 months. Test any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least every 12 months to ensure that the information is useable and current. All testing results shall be documented.31.3 - Conduct an operational exercise at least once every thirty-six months that demonstrates recovery in a representative environment unless an actual incident response occurred within the thirty-six month timeframe that demonstrates readiness. All testing results shall be documented.In 30.5, the recovery plan expands the current backup and restore of any application and system software using its baseline configuration. Is the definition of baseline the current or previous version of an application and system software?In 31.2, does the testing of any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored to ensure that the information is useable and current require the Responsible Entity to "load back" the data that is stored on backup media to an operational system to prove usability? Is loading it back to a test environment sufficient?In 31.2, "Test any information used in the recovery of BES Cyber systems." Does the requirement imply that in the case of protective relays at a BES Transmission Facilities, the backup settings file for every protective relay at High Impact facilities should be tested every 12 months?
51.41	Northeast Power Coordinating Council	Disagree	Recommend changing the bullets for 30.5 to start with “plans for”. The first bullet should be “install” not “reinstall.” The recovery plan does not need to include non-BES Cyber Systems. The third bullet should test the BES Cyber System Component(s).
51.42	Oncor Electric Delivery LLC	Disagree	These requirements are unnecessarily burdensome. Entities have been recovering from man-made and natural disasters for many years without these requirements.

#	Organization	Yes or No	Question 51 Comment
			Entities should be able to leverage Business Continuity, High Availability architectures and Standardization to demonstrate their ability to recover from unforeseen events. Requirement 32.6, update of Recovery Plan, we suggest this review be conducted quarterly.
51.43	Progress Energy - Nuclear Generation	Disagree	Agree with R30 and R31. Disagree with R32. Incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments for consistency in regulation for R30-32.
51.44	Progress Energy (non-Nuclear)	Disagree	R30.5 the first bullet should not be a requirement based on the second bullet.
51.45	Regulatory Compliance	Disagree	30.5 - STTRKE all the bullet points. Recovery plan should be system wide. Test restoration annually - document processes.31.2 - Make the second item a separate criteria line item - it's too confusing the way it is currently written. "Required" for High Impact.32.2 - "Annually" review the results.....
51.46	ReliabilityFirst Staff	Disagree	For R30, change “or failure” to “failure, or destruction.” For 30.4, please clarify what is meant by “successfully restore”. For R30.5, please clarify what is meant by “known secure backups”. For R31.3, change “incident response” to “activation of the recovery plan”. For R32, delete “relevant” so all changes are communicated. For R32.7, change “recover” to “recovery”.
51.47	ReymannGroup, Inc.	Disagree	R30.4 should be expanded to include processes for the recovery, restoration, and protection of data from a damaged or failed BES Cyber System. R30.5 should be expanded to include a review to ensure that malicious code has not been installed on the recovered files or device.
51.48	RRI Energy	Disagree	What constitutes a representative environment?

#	Organization	Yes or No	Question 51 Comment
51.49	San Diego Gas and Electric Co.	Disagree	R30 - R32 were originally covered in CIP-009-3. Referencing Table R30 - SDG&E suggests that R30.4 and R30.5 be removed. The IT Disaster Recovery Plan covers this and it would not normally be part of our Business Continuity Recovery Plan. The Responsible Entity (RE) should not be required to develop Recovery Plans with detailed IT processes for storage, backup, protection and reinstallation of software, etc. Referencing Table R31 criteria 31.3, SDG&E suggests that this wording be changed. CIP-009-3 R2 provides the RE with more options for "exercising" the recovery plan and we prefer the way the Requirement is worded in CIP-009. Referencing Table R32, CIP-009-3 R3 provides the RE more options when developing plans and procedures to comply with the Requirements. The new table seems to hold the Entities (both Medium and High) to several compliance timetables that are extremely restrictive. SDG&E suggests that we utilize the same wording for this Requirement from CIP-009-3 R3.
51.50	Southwest Power Pool Regional Entity	Disagree	R30: Is a recovery plan required for each BS Cyber System or is a generic plan acceptable? Recovery plans need to range from device component failure to catastrophic failure (e.g. physical facility disaster). 30.2: Is the identification by individual name or by position title? 30.5: What is meant by "secure" backups? Encrypted? Securely stored? Something else? Also, the backup and restoration processes should be "as applicable." Not all recovered systems are restored from a "backup." 31.2: Does the requirement to test backup media when initially stored apply to every daily backup, or only after BES Cyber System updates? Does the test include a restoration to an offline environment to verify the backup is not only readable but also complete? 31.3: Clarify that the operational exercise is more than a system or site fail over (NERC Standard EOP-008 exercise) but must also include performing the necessary steps to recover from the failure and restore the failed systems to normal operation by following the steps of the plan. 32.1: Include BES Cyber Systems that are significantly updated / upgraded requiring an update to the recovery plan. 32.4: Require the update within a much shorter time following determination of the need through the methods defined in the criteria. Delayed

#	Organization	Yes or No	Question 51 Comment
			updates are at risk of being overlooked and out of date plans pose a risk to the entity's ability to quickly recover. 60 days is recommended.
51.51	USACE - Omaha Anchor	Disagree	A) 30.5 - how often must system test be conducted? B) 31.2 Clarify "initially stored" is this the first time the tape is used?C) 32.6 - this could be interpreted to require a change in the recovery plan every time a software change occurs. This is very extensive - and unrealistic. Potential verbiage could be 'whenever system, organizational, or technology changes effect the recovery plan.'
51.52	We Energies	Disagree	We Energies agrees with EEI: Suggested revision for R30.2:Roles and responsibilities of responders, including identification of the personnel (using Job title or job function) responsible for recovery efforts.
51.53	Xcel Energy	Disagree	Definition is needed as to what constitutes an "operational Exercise". Is this a table top drill, or something more.

52. Tables R30 to R32 provide direction concerning what impact level of BES Cyber Systems to which Requirements R30 to R32 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Recovery Plans" are now addressed in CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems

The primary focus areas of the comments were concerned improving the clarity of the periodic timing requirements and the large amount of test equipment it would take to develop representative environments for numerous disparate facilities.

Some commenters noted the different terms used for references to annual activities. The SDT reviewed the use of annual, calendar year, 12 months, etc. and in the revised standards used the phrase, ". . .at least once each calendar year, not to exceed 15 calendar months between. . ."

There were suggestions that the testing requirements should only apply to control centers as Recovery Plans apply to Medium & High Impact Level categorizations, while some aspects of the recovery plan may only apply to High Impact assets. Additional guidance was requested for operational testing and for testing of information that is stored on backup media. The SDT added some information about testing in the Rationale Box for Requirement R1 in the revised CIP-009-5. Testing is necessary to verify the Responsible Entities Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

Issues identified in comments for SDT consideration were Recovery Testing – Operational Test every 36 months should count for the annual test, recovery plan testing clarifications, data retention plan clarification, identification requirements of "Personnel Responsible", coordination of physical aspects of Cyber Security Incidents, and incident recovery plan reviews. The SDT notes that there are FERC directives (e.g., P686, P687, P725) to add a requirement to conduct a full operational test of the recovery plan once every three years – so the suggestion to count the full operational test as the annual test was not adopted. (CIP-009-5 R2)

Commenters suggested changes and provided various requests/suggestions for re-wording/wordsmithing and improved coordination of backup and recovery with EOP-008. The SDT has coordinated its proposed requirements with the now FERC approved EOP-008-1 – Loss of Control Center Functionality. Commenters suggested that all requirements should be in the table, not in the objective or in the "pre-amble" to the requirements and that the SDT consider providing a summary table for all periodic requirements and remove the "how to" statements from the requirements. The SDT has included all mandatory performance in the requirements of the revised standards. The SDT did not adopt the suggestion to develop a summary table for periodic requirements as the format for Version 5 is considerably different from the format proposed when the requirements were all combined in CIP-011.

	Organization	Yes or No	Question 52 Comment
52.1	Alberta Electric System Operator	Agree	There appears to be a typo in 32.7 - "Communicate all recover plan updates" - recover should be recovery.
52.2	Emerson Process Management	Agree	In reality, it would be a good practice to exercise recovery plan during or toward the end of each scheduled unit outage for generation.
52.3	Florida Municipal Power Agency	Agree	FMPA suggests changing “12 months” to “annual” and “24 months” to “biennial”
52.4	PacifiCorp	Agree	31.2 - By including the testing of information used in the recovery of BES Cyber systems that is stored on backup media in 31.2 means that Low and Medium Impact BES Cyber Systems do not require testing of such information? If so, it should be a standalone requirement.
52.5	American Municipal Power	Disagree	Please provide a little or no impact category
52.6	American Transmission Company	Disagree	Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.7	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS comments on impact levels and therefore proposes the following changes:R31 Table 31.3: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyThe APPA Task Force agrees with the impact levels for the rest of R30-R32 if it is understood that a blank in the table means N/A.
52.8	BGE	Disagree	R30 - R32 should synchronized with R29 to include both Low and medium impacted

	Organization	Yes or No	Question 52 Comment
			BES Cyber Systems.
52.9	Black Hills Corporation	Disagree	30.4 should also apply to Medium Impact systems. Without this basic information, recovery would have to start from scratch.
52.10	Bonneville Power Administration	Disagree	Table R32Sections 32.2 and 32.3. Both should allow 60 days for review.Section 32.4: 12 months is too long. No more than 6 months should be allowed. Items 31.1 through 31.3 in Table R31 and 32.1 and 32.4 in Table R32 states certain events must occur "at least once every 12, 24, or 36 months." Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently the events referenced above must occur.
52.11	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
52.12	Con Edison of New York	Disagree	See 51
52.13	Consultant	Disagree	Table R30 - It doesn't appear to make sense that the Recovery Plans applies to Medium & High impact level categorizations, while aspects of the recovery plan only applies to High Impact assets.Table R31 & R32 - How many test and exercises are required? The structure here will create an administrative burden to track what was done when that has no corresponding risk reduction.Mixed requirements would force multiple recovery plans based on categorization of assets, which could mean two recovery plans for the same asset type where the application of each asset has a different impact categorization. This does not appear to be a sensible approach to recovery plans.Suggest deciding on a consistent set of requirements that can be applied equally to High Impact and Medium Impact assets.
52.14	CWLP Electric Transmission, Distribution	Disagree	R32.6. In order to meet the required change management process in R23 this window should be extended to 60 days.

	Organization	Yes or No	Question 52 Comment
	and Operations Department		
52.15	ERCOT ISO	Disagree	All requirements should apply to Medium Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
52.16	FirstEnergy Corporation	Disagree	R32 - Combine R32.5 and R32.6 and eliminate the word 'organizational'.
52.17	Garland Power and Light	Disagree	Requirements 30.1 & 30.2 - remove Medium Impact classification
52.18	ISO New England Inc	Disagree	32.6 - clarification on scope of "any" technology and system change scope. (organizational change is fine). R32.7 spelling "recover" should be recovery? CIP Standard use of the term "annual": The term "annual" should be replaced with the phrase: "no fewer than X (e.g. 9) months, but no greater than Y (e.g. 18) months". The time duration in "X" and "Y" should be clarified by the Standard Drafting Team, taking into consideration the appropriate level of exposure the time duration would provide. This phrase would provide Registered Entities with flexibility within any given calendar year to accomplish the prescribed action, but at the same time restrict companies from taking action in December of one calendar year, and then again in January of the next.
52.19	LADWP	Disagree	Medium Impact should not be a factor.
52.20	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
52.21	Manitoba Hydro	Disagree	Medium Impact BES Cyber System should be included as "Required" in sections 30.3 to 30.5
52.22	MidAmerican Energy Company	Disagree	Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous

	Organization	Yes or No	Question 52 Comment
			disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.23	MRO's NERC Standards Review Subcommittee	Disagree	Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.24	Oncor Electric Delivery LLC	Disagree	Verification of the entity's Recovery Plan for High Cyber Systems every 12 months should cover Requirement 31.1. This should require only one test for the entity - remove low/medium/high)
52.25	Progress Energy (non-Nuclear)	Disagree	See comment 14.What is meant by an operational exercise in a representative environment? Does it mean individual components that can be easily tested for recovery plans?
52.26	ReliabilityFirst Staff	Disagree	For R30, each subrequirement should be "Required" for all the "Medium" impact BES Cyber Systems. For R32.6, should be "Required" for "Medium".
52.27	San Diego Gas and Electric Co.	Disagree	SDG&E would agree with Table R30 if item 30.5 were to be removed. Similarly, SDG&E would agree with Table R31 if item 31.3 were to be removed. Referencing Table R32 - SDG&E prefers the wording in CIP-009 R3 in this area because it provides more flexibility for the Entities while still covering the issues.
52.28	Southern California Edison Company	Disagree	The drafting team should state in CIP 010 that back-up systems should be treated at par with system key to real time BES reliability if the intent of this requirement is that CIP-011 be applied to all BES systems.
52.29	Southwest Power Pool	Disagree	30.3, 30.4, and 30.5 should be applicable to Medium impact systems. 32.6 should be

	Organization	Yes or No	Question 52 Comment
	Regional Entity		applicable to Medium impact systems with perhaps a 60-day update timeframe.
52.30	The Empire District Electric Company	Disagree	Comments: Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.31	WECC	Disagree	All items should be required for medium impact levels in R30Criteria should apply to all impact levels.

53. Which requirements in draft CIP-011-1 should allow for TFE submissions? Note that not all requirements will be considered as being applicable for TFE submissions. The drafting team has attempted to minimize the need for TFEs by modifying the language to allow for flexibility in meeting the requirements. Please provide suggestions on how the language of the standard may be modified to eliminate the need for TFEs. If TFEs are still needed, please provide specific examples to justify the inclusion of a requirement as being TFE eligible.

Summary Consideration:

Some commenters stated that the requirements should be written around the specific device types. The drafting team considered this option, but believes that it becomes problematic for entities and auditors to determine when a device is multi-purpose versus purpose-built. Some purpose-built devices can be considered multi-purpose depending on how the device was manufactured and implemented.

A variety of comments were received regarding the TFE process and its applicability to the specific CIP Cyber Security requirements. While the TFE process itself was outside the scope of the drafting team's work, commenters stated that TFEs should be allowed for passwords, malicious code monitoring, system hardening, system event monitoring, wireless and remote access, as well as for communications and data integrity. The drafting team considered these comments and revised the requirement text where necessary to allow entities more flexibility in implementing these requirements thereby reducing the need for TFEs. In some cases, the requirement was removed or written at a system level to prevent the need for TFEs.

#	Organization	Question 53 Comment
53.1	Detroit Edison	14.4, 17.1, 17.2, 16.2, 10.1-10.8 should retain TFE status.
53.2	Network & Security Technologies Inc	19.1 (see comments on Question 35), 26.2 (see comments on Question 47)
53.3	ISO New England Inc	Actual language on several requirements need to be clarified, many are still open to interpretation which may lead to TFE's.
53.4	EEI	Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.

#	Organization	Question 53 Comment
53.5	Progress Energy - Nuclear Generation	All CIP 011-1 Requirements should contain provisions similar to NIST 800-53, Regulatory Guide (RG) 5.71, and NEI 08-09, Revision 6, CIP standards should provide for nuclear facilities' use of alternative methods which implement security controls equivalent to those required by CIP. Nuclear programs, required by regulation, currently in place at nuclear facilities provide these alternate methods. Technical Feasibility Evaluations (TFE) should not be required with such documentation. One example is that nuclear facilities have one of the most effective Physical Security Programs of Critical Infrastructures. CIP-011-1 requirements R5 and R6 should acknowledge nuclear generating station physical security programs.
53.6	Ameren	All of the following requirements would need a TFE o R10 for passwords complexity o R14.4 for user banners o R15 for malicious code protection o R16 for installing patches o R18 for logging security events o R19 for validating data inbound o R23.7 for monitoring changes to a baseline configuration.
53.7	US Army Corps of Engineers, Omaha Distirc	All requirements that require existing hardware and software be capable of performing any function should allow for the possibility of TFE's. Sections R10, R15, R17, R18, R19, & R23 have requirements that are likely to require TFE's.
53.8	Southwest Power Pool Regional Entity	Any time a requirement specifies "continuous", "all", or prescribes a specific solution or characteristics of a technical solution, a TFE may be necessary. Try to avoid specific technology requirements as discussed elsewhere in these submitted comments.
53.9	The Empire District Electric Company	Comments: See comments under questions 34, 35, and 37.
53.10	RRI Energy	Cyber assets that are not on your standard IT equipment list are the most likely devices to need TFEs. This list could include meters, vibration monitors, PLCs, DCS, RTUs, cpu based test equipment.
53.11	E.ON U.S.	E.ON U.S. believes that many of the requirements remain ambiguous and additional clarity is needed. Absent such clarity it is difficult to ascertain where TFE ability can be eliminated. In fact, the proposal to provide greater compliance flexibility for responsible entities makes this determination even more difficult. As the requirements currently read, E.ON U.S. believes that more, not less, TFE requests will

#	Organization	Question 53 Comment
		result. Areas where responsible entities have requested additional clarity need to be addressed prior to issuance of a final industry draft. The informal comment period does not provide an adequate forum to identify all areas of concern and suggest specific replacement language.
53.12	Cogeneration Association of California and Energy Producers & Users Coalition	Entities should be able to use TFEs for any instance where unsupported technology is in place that may not be compliant with CIP-011 requirements due to age or vendor proprietary technology. Patches, updates, virus scanning, or firewalls may not be available for older, unsupported technology. An entity should not be required to upgrade or replace a system that currently satisfies the needs of the entity. The entity should be able to use other mitigation methods to protect a system if patches, updates, virus scanning, or firewalls cannot be applied.
53.13	Northeast Utilities	Equipment that never has security software patches or virus protection should be exempt. Also, those cyber assets that do not have user authentication capabilities should be exempt from password requirements.
53.14	ERCOT ISO	ERCOT ISO supports the proposed form of combining all requirements into a single reliability standard. The use of a single standard will eliminate the need for cross-referencing to other reliability standards. ERCOT ISO does request a realignment of some requirements. All requirements for access authorization, revocation, and review should be combined to eliminate confusion of how access should be managed.The timing of updates to documentation should be consistent throughout the requirements. Recommend the use of 30 days to be in compliance with the directives of FERC Order 706.
53.15	Bonneville Power Administration	If the standards present the overall security controls required, and do not attempt to dictate how those controls are accomplished, there should be no need for TFEs.If there is a need:First, the TFE process as presently constituted has shown to be cumbersome, not well understood, and inflexible. Neither NERC nor The Regional Entities have the detailed internal system knowledge or manpower to do make an intelligent judgment. At best, they can make a broad, industry best guess. The TFE approval process belongs within the Responsible Entity, at a technical level where there are people who know the environment, the systems, and their capabilities can evaluate them. They should be audited as part of the normal compliance audit.Second, if a system will not, or can not perform a

#	Organization	Question 53 Comment
		required function, it should be up to the RE to determine what steps should be taken to meet the standard. Third, because there are so many ways to accomplish the security of systems, the only time a TFE should be necessary is when all methods have been exhausted that could provide a level of protection required.That being said - Any time a situation arises where for technical reasons, or because implementation of security features may present BES reliability issues, or where application of one security measure would compromise others, the RE should have the authority to choose how to proceed. If this is called a TFE, the RE should approve it and document it as part of the overall security planEven if TFEs with approval required by the REs or NERC are used under CIP-010 and CIP-011, the process needs to be revised. As examples:1. There needs to be an opportunity for entities to appeal or request reconsideration of a rejection of the initial submission. Under the current, at best they can resubmit one time to correct errors.2. It should be possible to submit TFEs under multiple justifications.3. There are claims that the regional entities have been instructed to reject any TFEs other than those based on legacy equipment. If true, this violates the process, which allows TFEs for both new and legacy systems. It is also unreasonable: there are still systems today, and will be for the foreseeable future, that may be the best overall solution for reliable operation of the grid but which do not allow full compliance. Having said that:10.6 may not be possible for all systems. For overly simplistic example, routers intended for small office/home office use often allow either full access or no access. If all that is necessary is to review a log, full administrative access is overkill. To avoid the need for a TFE, recommend "To the extent possible for the particular device or system, require that authorized..."10.8. Same comment as 10.6.14.2. Unless the definitions of external connectivity and/or remote access or change, 14.2 may not be possible in every instance. For example, consider a legacy multi-user system in a Control Center that is not capable of multi-factor authentication. Any access from a system not part of the BES Cyber System containng the legacy system would constitute remote access and require multi-factor authentication for a High Impact system. It is not clear from R14 whether that multi-factor authentication is required at the BES Cyber System itself or at the access point. If it is required at the system itself, then a TFE would be required. Recommendation: Redefine external connectivity and remote access as described above. Multi-factor could then be required clearly at the external access point.14.4. It is not always possible to display an appropriate use banner under such circumstances. As an example, consider remote connection using a VPN. The access point in that case would the device at the endbound end of the encrypted tunnel. The user never sees a

#	Organization	Question 53 Comment
		screen on that access point, and therefore sees no such banner. Recommendation: See the suggested revisions to 14.4 R19. For both 19.1 and 19.2, validation might not be possible. In particular, commercial off the shelf software (COTS) may or may not provide such validation. If the COTS is the best solution otherwise, a TFE would be required.
53.16	Public Service Enterprise Group companies	Implementation of requirements 10 (Response to Question 24), 13(Response to Question 32), 23.7 (Response to Question 40) and 26.2 (Response to Question 48) may not be feasible in all situations. Please see comments in the questions that relate to these requirements for description of the potential infeasibility.
53.17	Idaho Power Company	In R19, data validation and encryption may in some control center applications, introduce a data latency that renders the application degraded or useless and may result in a more secure environment but less reliability. In R19.2, I am unaware of technology that can determine whether invalid data has been maliciously compromised. Most EMS/SCADA systems which would be the most common BES cyber system in a control center filter or ignore invalid data anyway and I do not see that the benefit of this requirement outweighs the technology investment needed to meet this requirement.The ability to alert on unauthorized access attempts may require a TFE depending on the boundary device that is protecting the system. Some boundary devices do not lend themselves to providing alerting and may require a TFE until they are replaced with a device that can meet this requirement.
53.18	Lincoln Electric System	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
53.19	MidAmerican Energy Company	MidAmerican Energy agrees with EEI's comment below:Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.
53.20	Minnesota Power	Minnesota Power recommends that the following requirements should still be eligible for Technical Feasibility Exceptions:Requirement 8, Part 8.3:Depending on the definition of “monitor the use,” it may be impossible to do this for many devices. For example, for Windows computers, how does one monitor the use of someone when much of the interaction involves mouse clicks? Will software be

#	Organization	Question 53 Comment
		required to log, not just keystrokes, but mouse clicks? Further, certain devices do not even maintain an audit trail of logins/logouts (e.g.: networked KVMs for remote console access to servers to allow for efficient system administration).Requirement 10, Part 10.2:While this is certainly good IT Security practice, implementing this on every BES Cyber System could very well put the reliability of the BES at greater risk. Since there is no way to change all passwords in all the various devices simultaneously, especially in a utility that is geographically distributed and remote, this will result in a continual need to change passwords. As a result, it could become commonplace for technicians and engineers to not know/remember what password to use on what device. Not only will this keep them from accessing devices at potentially critical times to perform needed maintenance, but EVERY failed login attempt will then have to be investigated in detail. This could be minimized by requiring this for only Medium and High Impact systems.Requirement 10, Parts 10.4 and 10.5:It is quite probable that devices exist that cannot meet these requirements.Requirement 10, Parts 10.8:It is quite probable that devices exist that do not allow for the creation of accounts, whereby all functions must be performed from the system/admin account(s).Requirement 15:For any BES Cyber Systems that are not on routable protocol networks, it is not possible to have network-based malware detection/prevention. Thus, if the device itself does not support the installation of malware-prevention software, Requirement R15 would be not technically feasible.Requirement 18:For any BES Cyber Systems that are not on routable protocol networks, it is not possible to have network-based malware detection/prevention. Thus, if the device itself does not support the security event logging, R18 would be not technically feasible.Requirement 19:The way this is written, the requirement is likely technically infeasible for most any system. To correct, Part 19.1 could be changed by replacing the word “Validate” with “Encrypt”.Requirement 23, Part 23.7:This implies detecting changes that have occurred outside of the approved methods of Parts 23.3-23.6. As such, not all devices may support the installation of software that would allow for such monitoring.
53.21	Progress Energy (non-Nuclear)	Need to include language that allows for procedural controls - example as for password requirements which cannot typically be enforced technologically.
53.22	WECC	No requirements should be so prescriptive to required a TFE. The SDT has done a good job in rewriting requirements to describe WHAT is required without describing HOW it must be achieved.It is impossible to draft standards language that anticipates all possible limitations for implementation.

#	Organization	Question 53 Comment
		The standards, or Rules of Procedure should allow for exceptions to any requirement if an entity could provide justifiable basis and acceptable alternative controls.
53.23	Nuclear Energy Institute	Older computer based equipment may not support all of the controls such as logging/monitoring and accounts/passwords. Alternate controls should be allowed in these cases.
53.24	PacifiCorp	PacifiCorp agrees with EEI's comment below:Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.R10 - equipment still exists in the field that cannot meet the requirement of a 6 character password. R14 - equipment still exists in the field that cannot meet the requirements.
53.25	Dominion Resources Services, Inc.	Please see Dominion's responses above suggesting the addition of footnotes to avoid required TFEs for requirements 10.8, 14.4, 15.2, 15.3, 18.2, 26.2.
53.26	Puget Sound Energy	Puget Sound Energy suggests Table 10, Table 18, and Table 22 as inclusive for TFE eligibility for the following reasons (also stated in those sections):Table 10 - Puget Sound Energy suggests including "Where Technically Feasible" to R10, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 10.Table 18 - Puget Sound Energy suggests including "Where Technically Feasible" to R18, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 18. For example, entities may incorporate dialup accessible devices that, by the nature of a connection that is built up and torn down as necessary, is incapable of providing "continuous security monitoring that issues alerts".Puget Sound Energy suggests including "Where Technically Feasible" to R22, as some Protective Cyber Systems may be incapable of meeting all the requirements in Table 22.
53.27	FEUS	R10: Access Controls; some legacy systems do not allow for default factory accounts to be changed; some legacy systems only allow for a single level of access.R14: For systems not connected to an external network that use Dial-Up access for remote support multifactor authentication may not be technically feasible. Keeping some systems/networks separate from an external cooperate network can reduce cyber vulnerabilities.

#	Organization	Question 53 Comment
53.28	Southern California Edison Company	R7.2: Enforcing this control may be limited by the technical capability of a SCADA device. A device such a PLC that has preset accounts forces the RE to develop acceptable use for a set of accounts retroactively rather than have the capability to limit the account types.R10.4 and R10.5: There are SCADA devices in service that are not at the end of their service life that do not offer this capability. R15.1, 15.2 and 15.3: While these capabilities may be possible at the electronic boundary, individual SCADA devices may not support this functionality. Strict compliance is restricted by technical limitation.R17.1: The mitigation plan that is suggested should be a part of a formal technical feasibility exception program.R28.1: The phrase "or a full operational exercise" is expected to result in technical feasibility exceptions since this will require test data/ setting to be loaded onto in-service SCADA systems.
53.29	Alliant Energy	Recommended changes for any TFE program implemented:Security patch TFEs should be programmatic and not based on individual patch releases.Cyber Asset counts should be stricken. Approved changes to the environment create an immediate ad-hoc obligation for TFE update to the RRO for what is already a burdensome process.Quarterly updates should be removed and replaced by re-approval on an annual basis by the Sr. Manager or delegate.NERC should create a standard Class-Type list as originally proposed.
53.30	USACE HQ	Requirements 10, 14.4, 15 and 17, among others, should have a TFE.
53.31	San Diego Gas and Electric Co.	SDG&E recommends that the TFE processes be changed and incorporated into the Vulnerability Management Process; where the Entity would identify, track, and mitigate any TFEs as a Vulnerability. This methodology will streamline and enhance the TFE process and thereby 1) allow Entities to manage their TFE's internally, 2) reduce Entity, NERC, Reliability Coordinators and Regional Reliability Organization resource requirements, 3) reduce paperwork, resources, and overhead, 4) reduce the potential for errors or leakage of secured information, 5) enhance the audit process and 6) standardize and clarify the process across all Entities.
53.32	BGE	See comments for R13 under Q31-31 and R23 comments under Q40-41.

#	Organization	Question 53 Comment
53.33	MRO's NERC Standards Review Subcommittee	See comments under questions 17, 34, 35, and 37.
53.34	American Transmission Company	See comments under questions 34, 35, and 37.
53.35	Florida Municipal Power Agency	See comments under R7, R14, R16, R23, R20
53.36	CenterPoint Energy	See references to possible TFE issues in comments above.
53.37	SCE&G	Similar to RG 5.71 and NEI 08-09, allowances should be provided for use of alternatives to the required security controls. Alternate controls would be justified and documented that the Threat Vector has been mitigated. TFEs are administartively burdomesome and currently require annual certification and ultimate elimination. The scope of equipment eligible for TFEs will drastically increase the number of filed TFEs, especially for eligble requirements with low impact categories. The SDT needs to consider the feasibility and practicality of implementing the current TFE process with these standards.
53.38	ReliabilityFirst Staff	Table R10, requirements 10.1 and 10.2, Table R14, requirement 14.4, requirement R15, Table R19, requirement 19.2.
53.39	Consultant	Technical Feasibility Exceptions should be allow for any requirement. There are about 2,000 registered entities. Trying to address every configuration of every asset across that spectrum would result in either the requirements being written in a convoluted and confusing manner to address the multiple configurations or being written with little detail to allow the multiple configurations, neither of which could even approach a "bright lines" concept of the requirements. The Technical Feasibility Exception should include a technical basis that shows implementing the specific requirement as stated would not achieve the requirement objective, or improve the security position as it relates to the requirement objective.The Technical Feasibility Exception process probably needs to be improved to deal with exceptions as described here.

#	Organization	Question 53 Comment
53.40	Kansas City Power & Light	TFE should continue to be allowed. Unsure of all the requirements that this may apply to at this point. Recommend the Drafting Team at least consider a direct translation from the CIP version 2 requirements to these CIP-011 requirements at a minimum since CIP-011 is intended to be a translation but less prescriptive.
53.41	USACE - Omaha Anchor	TFE's will still be required in several standards - I've addressed the requirement for TFE in applicable standards.
53.42	Allegheny Energy Supply	TFEs can be reduced by providing additional language in the standard that recognizes the limitations of certain BES Cyber Components.
53.43	Allegheny Power	TFEs can be reduced by providing additional language in the standard that recognizes the limitations of certain BES Cyber Components.
53.44	National Grid	TFEs related to Password and Appropriate Use Banner.
53.45	CWLP Electric Transmission, Distribution and Operations Department	TFEs should be allowed for requirements R10, R13, R14, R15, R16, R17, R18, R19, and R23.
53.46	Reliability & Compliance Group	The best thing that could be done for this Standard is to ensure that everything is well defined so that there is no ambiguity when it comes to identifying BES Cyber Systems and also categorizing their impact.
53.47	Manitoba Hydro	The language or the requirements should be written such that there should be no need for TFE submissions. The standards should allow for compensating measures. For all instances where it is not technically possible to meet strict compliance with a requirement, the Responsible Entity should apply compensating controls which are documented and approved by the senior manager or delegate, similar to the policy exception process in CIP-003-1. The current TFE process creates a enormous administrative burden on the electric industry which provides no additional value to the reliability of

#	Organization	Question 53 Comment
		the Bulk Electric System.
53.48	LADWP	The need for TFEs still exist as certain control systems are legacy systems that may not have current update or patch capability (e.g. SCADA systems). Removal of TFEs for these systems would result in non-compliance as replacement or upgrade of these systems must be done on a planned and scheduled manner.
53.49	Garland Power and Light	There are 2 requirements specifically listed below that need TFE's but there should be provision for any equipment that cannot be made strictly compliant with any requirement that either a TFE or a mitigation plan can be written and implemented such as is stated in 16.1 or 17.1.Requirement R10 - Unless the requirement is rewritten to allow for procedural controls to suffice for compliance or the language in the footnote is actually included in the requirement, a TFE is needed for this requirementRequirement R14 - A printed circuit board (with a network connection) in most cases will not allow for any process to be loaded onto it to protect against malicious software - need a TFE for this requirement
53.50	GE Energy	These changes should eliminate the need for the vast majority of TFEs. There may still be a requirement for TFEs on systems that cannot enforce the password complexity rules.
53.51	FirstEnergy Corporation	This question should be postponed until the Standards are in a more final state so that entities can better see how the new requirements would apply to specific devices, etc. It appears that R20 would necessitate new TFEs.
53.52	NextEra Energy Corporate Compliance	Though NextEra believes TFEs are very important part of the CIP process, given the number of changes proposed, NextEra will wait until the next draft to comment on TFEs.
53.53	Oncor Electric Delivery LLC	To eliminate the need for TFE's the standard will have to be more granular. Many legacy systems are immune to cyber attacks, yet cannot satisfy the requirements of this standard. R8.3 as an example, there is no system to monitor access at the physical port of relays. R10 - legacy devices do not support account management.

#	Organization	Question 53 Comment
53.54	American Electric Power	We encourage the SDT efforts in drafting requirements in such a manner that will eliminate the need for a TFE. The TFE process should be standardized between the Regional Entities. Currently, Responsible Entities are required to submit multiple forms and varying information for the TFE process depending on the Regional Entity. AEP suggests standardizing on a single submission form and process and have all TFE data submitted to a single source maintained by NERC that can be used by all Regional Entities. This will allow Responsible Entities to submit and/or modify TFE data once and have it available to all Regional Entities on a consistently.See comments under questions 24 and 35.
53.55	We Energies	We Energies agrees with EEI: Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.
53.56	Regulatory Compliance	We feel that TFE's should still be considered for the following tables:R10 - Account Access Control SpecificationsR14 - Wireless and Remote Access ControlsR16 - Security Patch ManagementR17 - System HardeningR18 - Security Event MonitoringR19 - Communications and Data IntegrityR20 - Electronic Boundary ProtectionR23 - Configuration Change Management
53.57	BCTC	We have embedded this information in our individual responses to previosu questions.
53.58	US Bureau of Reclamation	We have not had an opportunity to assess which requirements may require a TFE yet. We will evaluate the requirements during the next evaluation period.
53.59	Duke Energy	We prefer that all of the requirements allow for an exception. Older computer based equipment may not support all of the controls such as logging/monitoring and accounts/passwords. Alternate controls should be allowed in these cases.
53.60	GTC & GSOC	We recommend that TFEs should be considered for all requirements with the exception R1 because of the ability of the regional entity and NERC to review the appropriateness of the TFE. We recommend adding language to the requirements on acceptable use banners and passwords to clarify that they do not require TFEs.If our recommendation to allow TFEs for all requirements is not viable then the following requirements should allow an entity to request a TFE. (R5, R6, R8, R9, R10, R13, R14, R15,

#	Organization	Question 53 Comment
		R16, R17, R18, R19, R21, R22, R23, R26)Example justifications are as follows:R5: BES Cyber Systems where physical security cannot reasonably be provided such as devices that are physically hung on a transmission line such (i.e. transmission line fault detectors). R6: While physical protection of the physical security systems should be feasible in most instances, there may still be instances where mitigation measures need the oversight provided by the TFE process.R8: The majority of substation devices use the concept of "shared" accounts. While an entity can add a device to facilitate logging into substation devices, there is not a feasible way to "monitor" these accounts on the purpose built devices themselves such as protective relays. R9: Depending on the method chosen to physically protect the BES Cyber System, it may not be technically feasible to revoke physical access to every location within 24 hours for an individual terminated for cause if an individual does not return their key (physical key, electronic key, or otherwise).R10: There are numerous examples of legacy devices which cannot meet the requirement of a 6 character password, or a password with special characters, etc.R13: Depending on the method chosen to electronically protect remote access to the BES Cyber System, it may not be technically feasible to revoke remote access to every location within 1 hour for an individual terminated for cause if an individual does not return their key (physical key, electronic key, or otherwise).R14: There are rare instances where remote access may be needed without 2-factor authentication such as for the administration of the device that authenticates the remote access itself. There are also instances where a display of appropriate use banner is not technically feasible.R15: While this requirement should greatly reduce the number of TFE's submitted based on the existing CIP v3 malware requirement, there will still be existing legacy purpose built BES Cyber Systems that do not have the ability to detect and respond to the introduction of malicious code. Specifically, consider the case of a protective relay with no external connectivity.R16: The allowance for TFE's should carry over from the existing CIP-007-3 R3.R17: Based upon the existing TFE framework, the language "shall document and implement a mitigation plan" from row 17.1 would necessitate that a TFE be filed.R18: There exists no such tool or process to monitor for system events related to cyber security on protective relays with no external connectivity.R19: Not all data protocols include a checksum. Whereas most SCADA protocols do contain this data error detection functionality, this requirement (19.1) is not limited to those inbound SCADA connections. There are a number of reasons, supported by the DHS Catalog of Control System Security itself, where an entity may choose not to encrypt all data inbound to a BES Cyber System (19.2).R21: There may be shared

#	Organization	Question 53 Comment
		cyber system components between BES Cyber Systems that do not provide logical separation. Clarification of this requirement may resolve the need for a TFE allowance on R21.R22: The TFE allowance justification for R22 carries over from the justifications for R14, R16, R18, and R23.R23: There are a number of devices for which there exist no such tool to monitor changes to the baseline configuration (23.7). In addition, it will not be feasible to monitor and detect changes for those systems with no external connectivity.R26: There are maintenance devices for which there are no known methods to detect and prevent the introduction and propagation of malicious code. Examples include devices such as data analyzers, birdogs, etc.
53.61	Constellation Energy Commodities Group Inc.	We support the effort to reduce the need for TFEs; however, the complexity and variability of systems across industry make it difficult and inappropriate to expect one-size-fits-all requirements.The password complexity requirements should either be written so as to avoid the need for TFE's, or clarified to specify that the use of maximum complexity allowed by the device is sufficient.
53.62	Entergy	Where the need for TFE has been obvious to us we have noted as such in comment to the respective requirements. We will be more thorough during the formal comment period.
53.63	Con Edison of New York	Will Technical Feasibility Exceptions still be accepted, required or will this process no longer be enforced? The Password requirements would still drive the need for TFE's. TFE's may be avoidable if the standard allows for internal documentation and approval of exceptions. There will be many TFE required because the net has been cast on so many different unique type systems that are located on the power system. Many of these systems are 20 to 30 years old. The CIP is written to address concerns for new technology computer network systems. Much of the equipment used on the power system is uniquely built and not designs with a full wide area network design.It would be a much better approach to address the SCADA systems (remote control and indications) & EMS systems and pay less attention to trying to force all the other unique (less critical) equipment in the same square hole.

54. Do you have any other comments to improve this version of draft standard CIP-011-1?

Summary Consideration:

Many of the commenters stated that the Standards need additional clarity. Define what is meant by words like monitor and review and remove potential ambiguity. Make clear the intent or objective of each requirement. The timing requirements of the standards need to be clearly defined. In response to these comments, the drafting team has made several steps to improve the clarity of the standards. These steps include moving to a Results-Based Standard approach, where the reliability objective must be specified for each requirement. Also the Drafting Team reviewed these standards with regional CIP auditors, with FERC, and with industry representatives ahead of the NERC Quality Review process to gain additional clarity in the requirements. The Drafting Team agrees and has made efforts to eliminate inconsistent terms and phrases and to consistently and unambigouously use timing phrases throughout the standards.

Commenters stated that the Implementation Plan should address the significant amount of effort required to comply with the standards for the many new cyber systems that will be in scope. Significant time should be included in the Implementation Plan for the categorization of BES Cyber Assets and for the transition from previous versions of the CIP standards to the Version 5 standards. The Drafting Team is proposing to allow 2 years for the Responsible Entities become compliant with all of the CIP standards and to allow entities the option to become compliant earlier if they choose to bypass Version 4 compliance.

Many commenters expressed a common theme to remove or minimize requirements for Low Impact BES Cyber Systems. Since the overarching objective is to provide for some level of security for all BES Cyber Assets, the Drafting Team has kept the requirements for physical and electronic boundary protection as well as basic security program elements such as policy, awareness and incident response, for the Low Impact BES Cyber Systems.

#	Organization	Question 54 Comment
54.1	Independent Electricity System Operator	- Specify calendar or business days when referring to a time frame- Issue with the bundled approach-- if you violate more than 3 in the same standard, this affects the VSL? need to look at NERCs governing procedure on VSLs- Strongly suggest that standards
54.2	Consultant	1. Each requirement should have a unique title. Currently the requirements are grouped by the subject area, but the requirements typically are just a statement. This makes it difficult to reference requirements except by number. What will really happen is everyone will develop their own "short title" for each requirement number, and it will not be consistent across the industry, and will result in

#	Organization	Question 54 Comment
		confusion.2. There should be consistency for the requirement title, the associated table name, & the requirements column heading for each requirement. Currently these three items are not necessarily consistent, and in some cases there doesn't seem to be a connection or relationship in the terminology in these locations.3. If the Requirements Groups are going to stay in the standard then they should be numbered in order to facilitate cross referencing the groups.4. The word "criteria" in the requirement statement should be change to "requirements" where it occurs. The tables list requirements, not criteria. (Multiple instances throughout CIP-011)5. There is different sentence structure and grammatical structure throughout CIP-011. While it is a good idea to combine the requirements in a single standard, it still appears to be written by multiple authors. There are still access control and account management requirements scattered across multiple requirement groups, and each is a bit different. Another example, the incident response and the recovery plan requirements groups should be very similar, but are, in fact, very different in the requirement and the wording of the requirements, much like the differences noted in CIP-008 and CIP-009. The structure of the "local definitions" is different throughout.Suggest a "wide area" review to make the standard appear to be written by a single author rather than multiple authors.6. The definitions should be written as definitions. [Defined Term - Definition statement.] The wording "for the purpose of this standard" is not correct, and thus unnecessary. The glossary collects definitions from the standards when the glossary is updated. The next update should add the terms defined in these standards, and therefor they are not "for the purposes of this standard". Also, the words "is defined as" are redundant as it is a definition.7. Data retention requirements should be included as requirements. Moving data retention to Section D isn't logical. If there is no requirement for data retention, then it isn't a viable compliance activity. At the workshop it was stated that this was a NERC format. In this case NERC is wrong and needs to correct the format, both for these standards and for the other reliability standards. 8. Suggest dropping all requirements for assets categorized as Low Impact. They are after all, low impact on the BES. Based on the discussion at the workshop, looking at a 10 year implementation timeline for low impact assets is effectively the same as no implementation. Many things will change in 10 years, and expenditure of resources in the low impact is unlikely to have any increase in BES security. The Low Impact category needs to remain as part of the categorization process in order to include all BES assets in that process.9. There are multiple requirements that differentiate between types of facilities in the requirements tables. This is an indication that the categorization criteria is incomplete or incorrect, or

#	Organization	Question 54 Comment
		that the requirements are not properly stated. If a requirement currently indicates in the High Impact column that it applies to Control Centers only, then either (1) the transmission, generation, and special systems are not "High Impact", or (2) the requirement statement doesn't properly address all asset classes.The categorization criteria should properly place each asset in each asset class in the appropriate category with "bright lines" to eliminate adding categorization in the requirements.10. While this format for commenting and collecting comments seems good, there should be a mechanism to complete the form 'non-sequentially'. For example, as comments are made through the form's current sequence, if a 'general' comment arises, the only method to enter that comment is to page through to the end, save the comments, and then reopen and page back to the location where you started. This is not very user friendly.11.The commenting tool should have a "Save and Continue" option to allow saving work in progress without exiting and re-entering the tool.12. An improvement to the "status bar" of the commenting tool would be a table of the questions with an indication for each question if a response has been entered.
54.3	Con Edison of New York	A few general questions:Will there be an implementation plan? The document for comments indicates there will be an implementation schedule that will take into consideration existing BES Systems (CCA's) and newly defined BES Systems (CCA's). In order to be able to meet the requirements in CIP-011, the devices on secured networks that are not currently CCA's by definition but are "treated as" since they are on the same network need to be considered as part of the implementation plan. The inheritance rules may require newly defined CCA's in order to allow the time that we be needed to address these additions. If they are considered existing since they are "treated as" a short implementation period could be an issue.Is there a six-wall physical boundary requirement in this version of the standards? Suggested additional defined terms:"BES Cyber System Failure": should be defined to serve as shorthand for the long list of items currently used in the draft CIP-010/011 Reliability Standards.Current Wording: "disruption, compromise or failure of BES Cyber Systems""if destroyed, degraded, misused or otherwise rendered unavailable"Proposed Wording:The term 'failure' when used in conjunction with the terms BES Cyber Component and/or BES Cyber System shall encompass the meanings 'malfunction, disruption, compromise, failure, destruction, degradation, misuse or unavailability' of those.Suggest replacing term "affect" with already defined term "adverse reliability impact". The drafting team (DT) uses the terms "affect" and/or "affects" without providing any specific meaning, system impacts, or other bounding explanation to describe that term. Proposed

#	Organization	Question 54 Comment
		Alternative Wording:NERC Glossary of Terms - Substitute definition for BES Cyber System "affect" or "affects." [Causes] Adverse Reliability Impact - The impact of an event that results in o frequency-related instability; o unplanned tripping of load or generation; or o uncontrolled separation or cascading outages, that affects a widespread area of the Interconnection.
54.4	Allegheny Energy Supply	A lot of work went into the prepration of the existing CIP-002 through CIP-009 standards. This new CIP-011 standard completely throws away that body of work in favor of this new approach. While there are many good things about the new approach, please consider the amount of work that entities have given to helping to refine the CIP-003 through CIP-009 drafts and to create and implement the current compliance plans and related software systems. We suggest that you consider incorporating the new ideas as incremental changes to the existing standards. It would be helpful for the drafting team to develop additional documentation providing more information about the threat basis that the standard is intended to provide protection against. The opportunity is to inform asset owners/operators of how and where to prioritize efforts to protect components of the BES.Suggest that the standard require physical security controls for BES Cyber Systems that no more stringent than other requirements for the BES equipment that the BES Cyber System controls, protects, or monitors.Suggest that the standard require controls that are commensurate with the amount of risk of compromise that a device presents. Not all BES Cyber System components face the same risk, or if compromised, have the same potential impact on the BES. For example: - Serially attached electronic components do not face or create the same risk as those that use routable protocols. - Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.- Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
54.5	Allegheny Power	Allegheny Power does not understand the need to eliminate and combine CIP-003 thru CIP-009 into a new standard CIP-011. AP believes that the objectives of the Standard Drafting Team to provide further clarification and remove the uncertainty of the current CIP standards are proper and necessary. However, AP believes that these same objectives can be accomplished by incrementally revising the current CIP standards and not force changes in terms, concepts and numbering schemes

#	Organization	Question 54 Comment
		which would essentially force all entities to start their CIP compliance efforts over from the beginning. AP would like the SDT to abandon the concept of completely rewriting the CIP standards in favor of incrementally revising the existing standards to accomplish the same objectives.
54.6	Lincoln Electric System	Although much of the standard seems very practical, LES believes it was written with routable systems in mind. When applied to systems with only non-routable connections, or even no connections, many of the requirements are not very applicable, and would set the stage for numerous TFE's within the industry. LES believes this either needs to be addressed requirement-by-requirement, as in the approach taken by the MRO NERC Standards Review Subcommittee (MRO NSRS), or there should be a blanket statement that removes non-routable systems from the requirements that are not applicable. Either way, LES believes this differentiation is extremely important, since non-routable connections (or even better, no connections) are inherently more secure against, and limit potential damage from, remote attacks, and by default eliminate the threat of propagating localized attacks to other facilities.
54.7	Oncor Electric Delivery LLC	As the tables of CIP-011-1 specify certain requirements for "Control Center Only" or "External Connectivity", the additional requirement of "Routable Communication or Dial-up Only". Many requirements do not even make sense without integral communications being part of the cyber systems. If there isn't communication involved, the cyber system should be excluded from a requirement.
54.8	Garland Power and Light	At the CIP workshop, there were several comments that were made that were "depends" or "our intent was" o The "depends" requirements need to be reworded so that requirement is clear. o The "intents" need to be expressed clearly in the document because it is almost guaranteed that the will be many different interpretations if they are not expressed.
54.9	Constellation Power Source Generation	At the workshop, it was stated that an assumption of the SDT that High Impact BES Cyber Systems were most likely already Critical Cyber Assets per the older standard. This is false. Non routable protocols and other criteria used by Registered Entities have excluded certain assets at critical locations from being critical cyber assets. A 3 year timeframe should be implemented for High BES Cyber Systems to be fully compliant if it was previously not classified as a CCA. Another suggestion for implementation is to make the procedural requirements auditable first, and then implementing the

#	Organization	Question 54 Comment
		other requirements in stages. Furthermore, as stated in the workshop, allowing an entity to declare advanced implementation for audits would be of great benefit, as compliance with the new standard will take years to implement. The blank boxes found in the requirements tables of CIP-011 are implying that a high/medium/low BES Cyber System does not need to comply with that requirement's particular control, but that is not written anywhere. A blanket statement in the beginning of CIP-011 needs to state that the intent of an empty box to avoid confusion. An audit standardization or guidance document should be developed for use by auditors/reviewers of compliance to NERC CIP standards. Even though the formalization of cyber protection compliance programs are relatively new within the NERC standards body, there are mature examples of cyber protection and information security controls frameworks comprised of formalized cyber security standards, compliance management methodologies and auditing guidance such as defined in NIST 800-XX and ISO 2700X regimens . These regimens include guidance and standardization for auditing compliance (e.g., NIST SP800-53A). Other examples of formalized auditing guidance include guidance documents published by ISACA (Information System Audit and Control Association). These regimens include formal auditing guidance to ensure comprehensive coverage of compliance requirements, consistency in auditing approaches and better insight for auditees in ensuring auditability for their compliance audits. This improves the effectiveness as well as the business efficiency of companies' compliance programs. This rationale also applies to the NERC CIP program.
54.10	E.ON U.S.	Because Distribution Providers are for the first time made subject to CIP standards they may need additional time to come into compliance
54.11	ReliabilityFirst Staff	Because the acronym "BES" is not included in the NERC Glossary of Terms, we suggest that BES should be spelled out in the Introduction to this standard.
54.12	Reliability & Compliance Group	By dividing up the Standards and just revising CIP-002 through CIP-009, it makes it easier for the Registered Entities to update their existing documentation. It allows for the creation of a "crosswalk" document that helps examine the changes. While it may not be able to be done requirement by requirement and sub-requirement by sub-requirement, it can be done Standard by Standard. Where possible, it would be good to create a change crosswalk document that lists the version 3 requirements and the points to where they are now covered in the version 4 standards and note that

#	Organization	Question 54 Comment
		there is either a major change or a minor change.
54.13	LADWP	CIP-011-1 R16 The patch management does not specify a required time for installation of patch. The entity should be given the ability to determine the schedule as systems vary on when they can be brought down to install a patch. The language in R16.2 addresses the issue and no additional language to restrict the installation time needs to be included.
54.14	City Utilities of Springfield, Missouri	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
54.15	US Army Corps of Engineers	Definitions within the standard need to be improved so they are less ambiguous.Statements like those found in Table R21, 22.1 "Cyber system components that provide external communication to the BES Cyber System must only communicate externally through an electronic access point as specified in Requirement R20", are confusing. What is the standard trying to say here?
54.16	USACE HQ	Definitions within the standard need to be more direct and narrower scope. Also, the relocation of all of them to a separate attachment would help too.
54.17	Dominion Resources Services, Inc.	Dominion recommends placing all requirements into a requirements table. It is sometimes difficult to distinguish requirements mixed into the preambles.Using a single standard for all requirements is preferred; however the format internal to the single standard is inconsistent. For example, some requirements are in paragraph form while others are embedded in a requirements Table. All requirements should be contained within a requirements Table. Where possible, information preceding the table should be used only to state the context and establish the security objective or intent behind the requirements.
54.18	EEI	EEI would like to thank the members of the Drafting Team for their significant efforts on this important issue.
54.19	Black Hills Corporation	Emergency Response: Emergency Response provisions are limited to R3 & R4, and address training and risk assessment controls. There are many possible scenarios that could be identified which would

#	Organization	Question 54 Comment
		require emergency exceptions to most of the requirements of CIP-011. There should be a general emergency clause that allows appropriate response to many possible emergency situations.Outside Vendors: There is no mention in the rules how the use of outside vendors should be addressed. A common solution could be to have the responsible entity extend the necessary requirements of these regulations to the third party via contract. (Example from other regulatory efforts includes the HIPAA regulations and their business associate requirement). An example of this in action could be the requirement that a contractor conduct the personal risk assessment, according to the requirements specified in CIP regulations.
54.20	Exelon Corporation	Exelon companies have embraced the development of logical, clear and effective reliability standards as evidenced by its commitment of time and resources to various standard development initiatives (including participation on several NERC and Regional Committees, Sub-Committees and Standard Drafting Teams). As evidence of our commitment, Exelon has devoted in excess of 4 years and $11 million for the implementation and integration of the NERC CIP-002 to CIP-009 Standards. We have concerns with several aspects of the CIP Version 4 Standards. The CIP Version 4 Standards represent a significant change in the scope of the standards in the equipment/systems that fall under the standards as well as the elimination of terms/categories of assets. Exelon is also not in favor of changing the current CIP-002-009 standards to the new CIP-010 and CIP-011 format.. Each change in itself represents a significant "change management" issue that impact databases used for the tracking/storing of evidence of compliance, training requirements, safeguards, and systems that have been put into place to ensure Exelon's continued compliance to all NERC Standards. Exelon feels strongly that the proposed changes must be accompanied by a risk based analysis as justification for such dramatic and costly changes which to date have not shared with the industry. Essentially we are most interested in understanding the incremental difference or benefit of moving away from the current Regulatory approved CIP-002 to CIP-009 standards to a different set of standards that will result in many of us "starting from square one" to implement. Policies, procedures, contracts, training, drawings, methodologies, systems, data structures, and countless other documents will need to change to reflect the new language and concepts. The confusion that this will cause within organizations to retrain personnel and realign around the new standards cannot be underestimated. In fact, Exelon may even need to put some value-added compliance projects on-hold because the entire design will need to change with the implementation of the new standards.Specifically, Exelon

#	Organization	Question 54 Comment
		would like to see the SDT: Discard the concept of a wholesale rewrite of the CIP standards -- but use the standards drafting team work as an input to the process. Incrementally change the existing CIP-002 through CIP-009 standards to clarify and improve upon the established approach. Retain the fundamental terms, concepts, and standards numbering scheme to enable continuity.This approach would more effectively build upon the work that has already been accomplished, while allowing the industry to continue to improve on security and compliance related to critical infrastructure.Compliance with NERC cyber security standards should be re-scheduled for nuclear generation. That is, nuclear generation is currently in the process of compliance with Version 3 of CIP-002 thru -009 by September, 2011. However, it appears that compliance with Version 4 of the standards may be required by 2013. In terms of resource expenditures, ultimately borne by consumers of electricity, it seems wasteful to build a program for nuclear generators based on CIP-002 thru 009 that will be scrapped roughly two years later to be compliant with CIP-010 and CIP-011. Such scheduling will result in maintenance of a program based on CIP-002 thru -009, including audit support, and purchasing and installing equipment during refueling outages, at the same time a new program built on CIP-010 and -011 is being constructed. This new Version 4 program will include doing away with the concept of Critical Assets so that purchase and installation of the equipment previously installed may no longer be required. The existing cyber security programs and regulations in place or in process to protect nuclear generators, e.g., NEI-04-04 and 10CFR73.54, the limited contribution of nuclear generation to the BES (roughly 20%), and the limited time until Version 4 of the NERC Standards are expected to be in force all limit the cyber vulnerability of nuclear units. It is recommended that the implementation of Version 3 of CIP-002 thru -009 for nuclear units be deferred, and compliance with NERC cyber security standards for nuclear generation be re-scheduled for Version 4.
54.21	BGE	General - The wording was changed to “at least every 12 months” instead of “annually” in previous CIP versions. Can the exercise or test occur in the same month each year or must it be 11 months 29 days or less from the previous exercise/test?
54.22	Network & Security Technologies Inc	Good start! Strive for clarity. Ask both individuals responsible for compliance and auditors for their interpretation of every requirement. Be explicit about what’s required (e.g., documentation of, records to demonstrate compliance with, etc.). It’s okay to not be very prescriptive but try to avoid

#	Organization	Question 54 Comment
		implied requirements - they will be a source of endless debate.
54.23	CWLP Electric Transmission, Distribution and Operations Department	Guidance documents should be available before balloting these standards. All terms used should be defined in the NERC Glossary of Terms or in the standard.
54.24	Green Country Energy	I really like the way the standard is developing it is a huge improvement and hopefully with industry comments it will develop into a fine standard that meets everyones expectations.I would like to see a Guidance Document, footnotes, measures and VSLs etc to make compliance and auditability a lot clearer and less subjective.
54.25	US Bureau of Reclamation	It seems that the standards are applying a postage stamp level of security to Cyber elements involved in BES reliability. Multifunction relays or Solid State relays which are programmable must now have eletronic access attributes which are normally associated with BES computer control systems. The SDT should reexamine the true nature and scope of these types of systems before lumping these deviced together with traditional computer control systems. Lumping everything into one standard will make adminstration by the Responsible Entities and Reliability Entities difficult and may add to confusion with respect to individual table elements.While the tables applied to requirements in CIP-011 are an excellent way to establish security requirements for the 3 levels of system impact addressed, the empty fields should be avoided as they lead to confusion on the part of readers. All blocked fields should indicate something, even if it is an indication that the requirement is “Not Applicable,” “Not Required,” “Addressed under Requirement xx.x, above,” or “In accordance with entity policy.” Further, all requirements should include the 3-level requirement application table, even if the requirement applies equally to all three levels. This will further avoid confusion when reading the Standards.Appreciate the “blocked-out” area-specific definitions, but the drafting team must ensure that this feature is only used for area-specific needs and not global definitions. If the scope of the definition extends beyond a specific section there could be problems with sub-dividing the document to simplify what is handed over to organizational components with different functional responsibilities, particularly if the definitions do not also appear in the NERC glossary.The use of “objective statements” is very much appreciated, both as a guide to entities addressing

#	Organization	Question 54 Comment
		implementation and also (we would assume) to reviewers and audit staff addressing compliance. We encourage the drafting team(s) to continue this direction and to strengthen and refine the objective statements in order to provide clear direction for Standards users, including down to the sub-requirement level (as applicable).
54.26	Luminant	Measures need to be defined
54.27	Minnesota Power	Minnesota Power believes that, for all requirements which specify that something must be completed within X hours, the Standards Drafting Team consider using the following statement:"As soon as practical, but not exceed x business days from the date reported."This would preserve the spirit of the requirement, but also allow for more practical time frames.With so many auditable elements included in these Draft Standards, Minnesota Power believes that the VSL's cannot be written with the current zero-defect mentality. It would be more practical to allow for minor issues to be identified and scheduled for corrective action without representing immediate non-compliance which will result in extended investigations and settlement proceedings.Minnesota Power recommends that the Standards Drafting Team consider using a technical writer and/or solicit feedback from multiple proofreaders who have not been involved in the creation of this Standard to ensure that the following items are addressed: o any interpretable vocabulary is defined o grammar is correct o punctuation is correct o meaning is clear and does not require any guessing as to the intention of the Standards Drafting Team.This should be done prior to the official comment period, so that the Industry can concentrate on technical aspects of the review, rather than spending time on interpretation. The ability of Registered Entities to properly interpret the Requirements is highly dependant upon clear wording, good grammar and proper punctuation. This has been one of the greatest problems with the version 1 through 3 CIP standards. Minnesota Power requests that the Standards Drafting Team ensure that improper writing does not change or hide the intended meaning. The misuse of
54.28	Progress Energy (non-Nuclear)	More examples of requirement application to the real world would aid auditors and the industry.In CIP-011 If the record keeping and retention for compliance is similar to previous standards this standard significantly increases the record keeping administrative burden on utilities and compliance authorities due to the number of devices which are now to be declared without actually increasing security of BES.Implementation plan (when developed) needs to consider how it will overlap existing

#	Organization	Question 54 Comment
		standards compliance record-keeping and documentation, then establish a phased-in approach of the new standards to eliminate double record-keeping and double documentation across audit compliance periods.Implementation schedule needs to be developed that allowsHigh - 4 yearsMedium - 4 yearsLow - 4 yearsNeed clearer definitions of annual, quarterly, etc.Need to resolve issues/questions with current standards:How is communication/wiring covered by the standards? This becomes even more of a question when a BES Cyber System could be defined as a SCADA system including all of the RTU's which support it.Within ESPBetween ESP'sInto/Out of ESPPassword strength/management. Improvement has been made here, but it is still not clear if requirements must be enforced by the assets in question or if policies are sufficient. For instance, regarding the requirement to change passwords at least once every 12 months, must the device force this password change, or is it sufficient for an entity to have a policy requiring compliance along with documentation to attest that the policy was followed?Timeframe for revocation of access for expired training/background checks. NERC CIP Training is required at least every 12 months. It can be assumed that if the training is not completed in the allowed timeframe that access must be revoked; however, it isn't clear if this revocation must be done immediately, within 24 hours, 36 hours, 72 hours.There is currently no provision for moving cyber systems from one ESP to another (such as between a primary and backup ECC). Although this type of even will need to happen from time-to-time, it is left up to each entity to determine how that can be accomplished within the standards.There is no clear distinction between various types of Access control. It is obvious that the standards apply to network facing logins for BES Cyber System Components;however there are other types of access that are not clearly addressed or excluded such as-Access to configuration controls for something like a time standard which are only available to someone with physical access to the front of the device-Access to the BIOS on a typical PC-Access to various functions/programs on a machine - some of which may require special login - others which don't.How 7 year background checks are handled for someone under the age of 25 since juvenile records prior to the age of 18 may not be legally searched in many cases.Will the TFE process continue? What a TFE is, where it is/is not allowed, how it is to be handled (regarding documentation, approvals, submittals, periodic reviews, etc)
54.29	Michigan Public Power Agency	MPPA is concerned with how these standards would impact its members who are registered entities but do not own or operate facilities that are, by NERC definition, a part of the BES. MPPA recommends clarification in the applicability section with the insertion of ", that operates BES facilities,

#	Organization	Question 54 Comment
		" between "...Functional Entities..." and "...will be collectively...". This segment of the sentence would then read as: "...Functional Entities, that operates BES facilities, will be collectively..."
54.30	ISO New England Inc	Need more precise, well-defined language. Several requirements are measures, not standard requirements to measure against. Provide examples, FAQ, what is the actual risk/ driving requirement - what are we trying to protect against? Understanding the background to the requirement will help to define defenses to perceived threats that this standard is trying to protect. Clearer definitions of Cyber Systems, Cyber System Components, Control Center. Suggestion for an additional page that repeats all of the local definitions - this means the local definitions exist in the document as is plus this additional pageRequest that the tables and time constraints be consistentEliminate confusion caused by two 3.1's. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (see R5-R32)Request a cross-reference of CIP-011 Requirements that refer to another CIP-011 Requirement - especially the Access Control Requirements. Diagram might help.
54.31	WECC	Need to have consistency in spelling out time periods versus numerically showing them (ie thirty-six months vs 36 months). Also need consistency in use of the tables as some say "criteria" and others say "procedures" or "processes". In many cases when a requirement states that you should have a process or a procedure it might be easier for audit purposes to instead require a program that addresses many of the processes or procedures required. A single requirement for a program or plan that meets a table of criteria might reduce the number of requirements and ease audits. For instance "Wireless Security Program covering the following risks" "Remote Access Program addressing the risks in Table X" "Maintenance Program addressing the criteria in Table X" "Physical Security Program addressing the criteria in Table X"
54.32	US Army Corps of Engineers, Omaha Distirc	Next draft should include the measurement criteria. Standards are very computer center centric.
54.33	Regulatory Compliance	NRG Energy Inc. is concerned with some of the impact criteria in Attachment II related to transmission and generation Facilities. To base impact on "bright line" Facility Rating thresholds, i.e., MW, kV, MVAR, etc., could lead to mis-categorization and ultimately unprotected cyber systems. These thresholds do not take into consideration regional differences in configuration and load flows.

#	Organization	Question 54 Comment
		Therefore, it is our suggestion that categorization could be based on the results of a regional engineering study, similar to what is currently required in the TPL Standards. This study could be conducted by the regional Planning Authority(s) or an independent third party and approved by the Regional Entity. The results of the study would identify the contingencies that have the potential to cause the following levels of impact to the BES: Â· High Impact (has the potential to cause an Adverse Reliability Impact) Â· Medium Impact (has the potential to require planned/controlled loss of load) Â· Low impact (has no potential to cause loss of load)
54.34	National Grid	o There is inconsistency in using "processes" or "one or more processes" in several requirements. For example R25 states that Each Responsible Entity shall document and implement one or more processes..." while R26 states that Each Responsible Entity shall document and implement processes...". National Grid recommends using "one or more processes". o Request that the tables and time constraints be consistent o Eliminate confusion caused by two 3.1's. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (see R5-R32) o Request a cross-reference of CIP-011 Requirements that refer to another CIP-011 Requirement - especially the Access Control Requirements. Diagram might help.
54.35	Southwest Power Pool Regional Entity	Overall auditing issue: The requirements need to consider issues of sufficiency (adequacy of the entity solution) without being prescriptive in the solution. Where possible, clearly define the objective and do not prescribe technical solutions. Also, avoid the use of adjectives in defining the objective and / or specific requirement. Terms such as "adequate", "sufficient", and the like are very difficult to objectively audit. Overall observation: The implementation plan concept presented at the May 19-20 workshop in Dallas, coupled with the proposed applicability matrix for Medium and Low impact BES Cyber Systems will likely reduce, not improve the overall cyber security protection afforded the BES Cyber Systems today. A good number of existing Critical Cyber Assets will fall out of the High impact category, many becoming Low impact, with the resultant relaxation of protections. The applicability matrix as it appears today does not define a reasonable baseline of protections for Low and Medium impact systems. Re-categorization of BES Cyber Systems: While this will hopefully not happen very often, a BES Cyber System that sits on the cusp between two categories could find itself being re-categorized more than necessary unless some sort of a dead-band is introduced that would preclude re-categorization as a result of a small change. Implementation Plan: There needs to be a consistent

#	Organization	Question 54 Comment
		implementation plan for any BES Cyber Systems represented under today's standards as Critical Cyber Assets regardless of their ultimate categorization. Any existing Critical Cyber Asset should be afforded a very short timeframe to achieve compliance under the new standard(s) as it can be reasonably be expected to be already compliant. This is similar to the Table 1 entities concept for Version 1 of the existing standards where entities subject to the UA 1200 standard were given the shortest timeframe to comply. Consideration needs to be given to how an entity will migrate from compliance with the existing standards to the new standards. A piecemeal approach will be very difficult for the entity to maintain and for an auditor to evaluate compliance.
54.36	Alliant Energy	Per previous comments, all occurrences where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement. Per previous comments, all instances where 12 calendar months are used as the outside allowance for renewal a rolling creeping calendar is introduced. Recommend changing all 12 month timeframes to either 13 calendar months or 5 calendar quarters from the previous completion to allow entities to maintain a program with an annual training rollout with the appropriate amount of lead time to be successful in annual renewal. A 12 month timeframe will create a training program that becomes administered on a user by user, day by day basis without considerations for consistent annual content updates and bulk annual renewal.
54.37	FirstEnergy Corporation	Please see our response to Question 1 for the FE Summary view of the proposed CIP V4 standards.The new format, tables, information boxes is a good change o We question whether the new format (low-to-high impact, in particular) will encourage us to categorize more as high so we track things in a similar way. It seems like an administrative burden to try to track things at three levels. It is hard enough to track everything now with just one level. This 'administrative burden' issue crops up in

#	Organization	Question 54 Comment
		several places.
54.38	PacifiCorp	Procedural exceptions are onerous to manager operationally; the standards would be more effective if less differences in revocation of access were implemented across the BES system and criteria.The term "Annual" is not defined. "Annual" requirements were changed to 12 months in most cases (not consistently). The 12 month requirement causes "schedule creep". Define "Annual" in the NERC glossary to be 12 months not to exceed 15 months. Change all 12 month references back to "Annual" or, preferably, use the definition of annual defined for the NERC FERC Standards of Conduct (calendar year). The following FERC Directives need to be addressed with version of of CIP-010 and CIP-011: o 2 or more diverse security measures for defense in depth at the security boundaries o Active vulnerability assessments every 3 years o Incorporate forensic data collection and proceduresThe framework is in place to incorporate requirements in CIP-011 that address the directives. CIP-011 has a potentially long implementation time. FERC will likely not wait for the implementation of CIP-011-1 to be complete prior to making NERC address these directives. Incorporating these directives in the middle of the implementation of CIP-011-1 will be confusing and cause additional expense and effort. Don't wait. Address the following FERC Directives in version 1 of of CIP-010 and CIP-011.
54.39	Southern California Edison Company	SCE recommends revising the numbering of CIP-0011-1. Between CIP-010 and CIP-011 the drafts should indicate the intention of the intent is to retire CIP-002 through CIP-009 then it would make more sense to call these standards CIP-002-5 and CIP-003-5 with CIP-004 through CIP-009 being retired. Otherwise, the gap of unused numbers between CIP-001 and CIP-010 will potentially cause confusion. SCE also suggests rearranging the structure of these new requirements. for example, by breaking up CIP 011 into functional areas such as Governance & Personnel, System Security & Boundary Protection (with Incident response since “incidents” are cyber security incidents), Access Management (Physical, Electronic and Information), and Disaster Recovery Planning & Capability. From a policy formulation perspective, this would result in fewer policies than CIP 011 as it is currently structured. For example, combining physical access controls with electronic access controls provide the means of utilizing a combination of both to determine sufficient total security. Providing secure physical access controls and disconnecting routable communications such as gateways and/or modems.Finally, separate and apart from the recommendations made above, SCE also recommends allowing use of local definitions as in-line guidance at the requirement level. The use of local

#	Organization	Question 54 Comment
		definitions in addition to the NERC glossary is good approach. The text of each requirement objective should be such that it is only a objective and not a control statement. A control should reside within the impact level table. For instance, R11, R12, R18 contains control statements within the objective.
54.40	San Diego Gas and Electric Co.	SDG&E notes that it appears the drafting team took the approach of defining the details and then working up to the bigger picture items, i.e., BES Cyber Systems Component to BES Cyber System. SDG&E feels that there is risk associated with taking this "bottom up" approach to the standard setting process vs. the "top down" as used in the previous three versions of the standards. The risk is that components posing no significant risk to the BES system can get "swept up" into BES Cyber System definition and require protection commensurate with components that are correctly required to have strong security measures.SDG&E feels that part of the issue with Versions 1-3 of the CIP standards was that the "top down" approach to critical asset identification was not started high enough; it was started at the Responsible Entity level rather than at the Region / Reliability Coordinator level. If that level is deemed too high, even a sub-region level would be more appropriate. In SDG&E's case, it has a view of its assets in the context of its service territory that serves 1.4 million retail customers. Independent generators on the other hand don't have that regional view. In Southern California, for instance, congestion is high in some places and regulatory mandates for incorporating renewable energy are growing. Thus, the risk to the BES can only be fully evaluated when considering sources (generation - fossil and renewable) and uses of energy (load) in the region as well as the adequacy of transmission to balance and move power. In such a scenario, the assets critical to BES stability and/or restoration are much easier to identify and so too are the BES Cyber Systems that support them. For those entities that do not have a region or sub-region view, perhaps the Regional Entity, Reliability Coordinator or Balancing Authority could be responsible for identifying which assets are critical.
54.41	Manitoba Hydro	Section D Compliance: 1.4 Data Retention should include all documentation, inventories, logs, etc that are mentioned throughout the Requirements, or include a "catch all" requirement for data retention for all other documentation referenced by the Requirements.General Comments: The language in Requirement R1 indicates that each Responsible Party shall "develop, implement and annually review one or more formal, documented cyber security policies" addressing the listed Requirements. This should be clarified to confirm whether a formal written policy is required for each of the listed Requirements or only for selected Requirements. From the language of the specific Requirements one

#	Organization	Question 54 Comment
		could assume that those Requirements that indicate "document and implement" require the Responsible Entity to prepare a written policy/process of some kind, while those Requirements that indicate only "implement" do not. Then there are those Requirements that require the Responsible Entity to "create, document and implement" - it is not clear if this would require something different than "document and implement". There are also those Requirements that simply require that certain criteria be applied which would seem to indicate that no documentation is necessary. If the Responsible Entity is to assume that the Requirements that indicate "document and implement" require the Responsible Entity to prepare a written policy/process of some kind, it is assumed that there may be one master policy covering all elements of the Requirements that must be documented given the language in Requirement R1 "one of more formal documented cyber security policies" and that separate documented policies for each of the Requirements requiring documentation are not necessary. Certain references to "review" in the Requirements should be clarified to indicate on what basis the review is to be conducted, what criteria should be applied, what the Responsible Entity should do with the results, etc. i.e. Requirements R5-5.6, R12-12.1, R18 -18.4. The same comment applies for certain references to "monitor" (i.e. Requirements R8-R8.3) and "verify" (i.e. Requirements R24-R24.5). Where no review or monitoring of developed protections or processes is specified, is it to be assumed that no review or monitoring is required? (Requirements R15 and R16) Each of the Requirements seems to provide a reason or justification for their inclusion i.e. Requirement R2 "……to ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems." Consider whether it is necessary to state the justification for each Requirement, especially if it could be that the objectives achieved by the Requirement are not exactly as specified or if the Requirement does not necessarily meet the objective as set out. It would be preferable to just have the broad purpose statement in the introduction which is stated to apply to each of the Requirements that follow. What is the purpose of the Measures in these standards? If they are to re-state the wording of the Requirement, they provide no value and create opportunities for legal interpretation if the wording in the measure does not exactly match the wording in the specific requirement. Entities should be allowed to employ multiple layers and tailor their approaches to cyber security to meet the intent of the requirement, such as including the inherent security benefits provided by private entity owned and managed communication networks. Manitoba Hydro is also concerned that the multiple layers of physical and electronic security directed by FERC Order 706 are

#	Organization	Question 54 Comment
		not included in this proposed version of the CIP-010 and CIP-011. While we understand that these directives were not included at this time for the sake of expediency, there is a risk that the electric industry may expend considerable resources to meet the requirements these proposed standards, only to revisit the electronic and physical security issues and expend more resources in the near future. Implementing physical security changes for electric facilities is proving to be a monumental task. This standard does a disservice to the industry if it does not provide the complete scope of the physical security changes required. If the entire scope of the physical security requirements, including the directives in FERC Order 706, cannot be provided to the industry in this proposed version of the standard, then all the requirements for physical security should be removed at this time and submitted to the industry, in its entirety, at a later date.
54.42	Alberta Electric System Operator	Specifying the units of measure (e.g. business vs. calendar days) and exact ordinal amounts ("365 days from date of implementation" vs. "annually") might help resolve some ambiguity surrounding some of the criteria.
54.43	Northeast Power Coordinating Council	Suggestion for an additional page that repeats all of the local definitions - this means the local definitions exist in the document as is plus this additional page.Request that the tables and time constraints be consistent. Also where the document refers to processes in some cases it specifies one or more processes and in others just processes. Eliminate confusion caused by two 3.1's. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (refer to R5-R32).Request a cross-reference of CIP-011 Requirements that refers to another CIP-011 Requirement, with emphasis on the Access Control Requirements. A diagram might help.Remove adjectives such as substantial, adequate, minimum, etc., as these are difficult to measure and can lead to different interpretations.Situational awareness displays currently in use at the Regions and FERC should not be included in the applicability of these standards. No operational actions or decisions are being made based on the information on those displays.
54.44	Nuclear Energy Institute	Terms should be clearly defined and unambiguous. Examples of items covered by the term and not covered by the term should be given. CIP-011-1 is a vast change from the prior CIP-003 through CIP-009, and clear definitions with examples will be valuable.

#	Organization	Question 54 Comment
54.45	Puget Sound Energy	The amount of work relative to CIP-010 is almost as much as CIP-010 because of the broad application of BES Cyber Systems. It would be prefereable to be able to manage this scope better up front so that entities don't have to evaluate and record so much to then only focus possibly a much smaller pool of work as more defined by CIP-011. It still not clear how to evaluate a system for "misuse" effectively and defensibly. Further guidance would be appreciated. Lastly their should be some grace period and easier interpretation process when these versions become effective in order to more quickly flush out interpretations of concepts once implementation starts. To date the interpretation is a lengthy process or determined in an audit as a result of a violation when the entity may have been well intended.
54.46	APPA Task Force	The APPA Task Force commends the drafting team on the overall development of CIP-011-1. We believe this document is another step in the right direction of cyber system protection. We did, however, notice a theme throughout the requirements that caused us some concern. There is an IT focus to a number of the requirements. The drafting team seemed to be focusing on control centers when developing requirements to protect critical facilities. As a result, a number of the requirements are not practical for remote substations and generation stations, that may be owned by many entities and operated by only one of them, or another entity. What may be simple in a control center environment may be next to impossible for a transmission substation or a generator.
54.47	Constellation Energy Commodities Group Inc.	The blank boxes in CIP-011 tables need to be filled in. While the intent appears to be that if the box is blank the control is not required, by leaving it blank, liability questions could be raised. Compensatory measures should be allowed in the compliance structure. Entities may find that alternative, but comparable protection measures will better fit the circumstances of their system.An audit standardization or guidance document should be developed for use by auditors/reviewers of compliance to NERC CIP standards. Even though the formalization of cyber protection compliance programs are relatively new within the NERC standards body, there are mature examples of cyber protection and information security controls frameworks comprised of formalized cyber security standards, compliance management methodologies and auditing guidance such as defined in NIST 800-XX and ISO 2700X regimens . These regimens include guidance and standardization for auditing compliance (e.g., NIST SP800-53A). Other examples of formalized auditing guidance include guidance

#	Organization	Question 54 Comment
		documents published by ISACA (Information System Audit and Control Association). These regimens include formal auditing guidance to ensure comprehensive coverage of compliance requirements, consistency in auditing approaches and better insight for being audited in ensuring auditability for their compliance audits. This improves the effectiveness as well as the business efficiency of companies' compliance programs. This rationale also applies to the NERC CIP program.The Implementation Plan should allow for sufficient time to complete the comprehensive task of identifying and categorizing BES cyber systems.The R3 and R4 tables should address each requirement. All tables should be completed in full stating either not applicable or required.
54.48	Midwest ISO	The categorization approach in CIP-010 appears to require any BES Cyber System that touches the BES in any way to be included no matter how minimal the impact of the Cyber System on the BES, we are concerned that the Midwest ISO energy and ancillary services markets will be impacted. We believe that market portals could become High, Medium or Low Impact facilities and, thus, require application of the CIP standards or modification of the systems to isolate them so that CIP standards don't apply. Our conservative estimate is that we could easily spend in excess of $10 million dollars without anywhere close to this impact because our existing processes would prevent the market from negatively impacting reliability. We request that the drafting team make clear that market systems should not be included per NERC standard development tenets. In some cases, drawing in market systems could present impossible challenges. For instance, if a market portal becomes a High Impact BES Cyber System, CIP-011 R4 appears to require that we would have to conduct personnel risk assessments on all users which would include thousands of employees from market participants submitting bids and offers. State laws make this impossible. The drafting team could help solve this problem by making clear that personnel does not include market participants/customers who already have significant financial incentive to enter good bid and offer data. Opportunity costs do not appear to be considered in the development of these standards. All business resources are limited. Requiring registered entities to focus on these specific issues may divert attention away from other important cyber and physical security initiatives and work that offer greater improvements to reliability.We are also concerned that cyber and physical security could initially be compromised as entities focus on becoming compliant for Low and Medium impact cyber systems. Likely, High Impact Cyber systems will meet the new requirements because they were likely Critical Cyber Assets under the existing CIP standards. Thus, their reliability could degrade as entities may lose focus on the High Impact BES

#	Organization	Question 54 Comment
		Cyber Systems.
54.49	Florida Municipal Power Agency	The drafting team seems to have added an objective into the requirements which adds ambiguity to the requirement. For instance, R2 adds the phrase "to ensure that personnel maintain awareness ..." which adds ambiguity to the requirement. Is the auditor going to measure "quarterly reinforcement" or "personnel ... awareness" or both? If the drafting team wishes to add an objective to each of the requirements, then consider one of two other alternatives: (1) adopt International Standards Organization format where they have an objective for each requirement introducing each requirement; or (2) develop a longer Purpose section where the purpose of each of the requirements is further embellished.Throughout the standard, there is confusion among the terms "grant" and "authorize". "Authorize" is senior manager approval, "grant" is giving the person a key, keycard, or user account. The requirements should keep these two concepts clear. For instance, in 5.5, "authorize" should be changed to something like: "Grant unescorted physical access to areas containing BES Cyber Systems only to those who are authorized such access".Overall, added complexity to the cyber systems will reduce the reliability of the BES, so this needs to be kept in mind when drafting these standards.Almost all of the standards need to have stronger language in them to remove ambiguity and give specific guidelines as to what it expected.
54.50	NextEra Energy Corporate Compliance	The following are specific language changes for clarity:1. Title: Cyber Security - BES Cyber System Protection 2. Number: CIP-011-1 3. Purpose: To provide clear understanding of the protections that are to be applied to BES Cyber System Components identified as a result of the applicable of CIP-010-1 to the Responsible Entity's BES.Also, for clarity, this section should be re-written as follows:R2. Each Responsible Entity shall reinforce sound security practices to all employee and contractor personnel who have authorized cyber access and/or authorized unescorted physical access to a BES Cyber System Component reinforcements in sound security practices at the beginning of each quarter. The Responsible Entity also has the discretion to reinforce sound security practices at any time, it deems appropriate. The reinforcement may be delivered via e-mail, intranet, posters, classes or other educations methods. .R3. Prior to granting employee and contractor personnel who have authorized cyber access and/or authorized unescorted physical access, each Responsible Entity shall ensure the personnel requesting access completes cyber security training consistent with that required in. CIP-011-1 Table R3 - Cyber Security Training,.3.1. For employees and contractor personnel requesting

#	Organization	Question 54 Comment
		authorized cyber access, this cyber security training shall cover the following: o The proper use of BES Cyber Systems o Physical access controls to BES Cyber Systems o Visitor control program o The proper handling of BES Cyber Systems information and storage media o Identification and reporting of a Cyber Security Incident For employees and contractor personnel requesting only unescorted physical access, this cyber security training shall cover the following: Procedures for not intervening with a BES Cyber System ComponentVisitor control programIdentification and reporting of a Cyber Security Incident 3.2. For employees and contractors personnel who engage in the operation or control of the BES via authorized cyber access to a BES Cyber System Component, cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber System Components and BES Cyber Systems. 3.3. For employees and contractor personnel who have a role in BES Cyber System recovery this cyber security training shall additionally include those related action plans and procedures to recover or re-establish BES Cyber Systems. For employee and contractor personnel who have a role in BES Cyber System incident response this cyber security training shall additionally include those related action plans and procedures.3.4. For employee and contractor personnel who have a role in BES Cyber System incident response this cyber security training shall additionally include those related action plans and procedures. 3.5. Each Responsible Entity shall maintain document for each employee and contractor personnel required to take cyber security training as required in R3 and its sub-requirements that the training was conducted at least once every 12 months plus or minus one month. R4. Prior to granting employee and contractor personnel who have authorized cyber access and/or authorized unescorted physical access, each Responsible Entity shall perform or have performed a personnel risk assessment on the employee or contractor personnel requesting access consistent with CIP-011-1 Table R4 - Personnel Risk Assessment, expect as prohibited or limited by federal, state, provincial, and local laws, and existing collective bargaining unit agreements. 4.1. This personnel risk assessment program shall at a minimum include: o Identity verification via photographic identification documentation issued by a government agency (i.e., Federal, State or Provincial); and o A seven year criminal history screened against specific criteria developed and documented by the Responsible Entity. The seven year criminal history shall include a records check that covers all locations where, during the previous seven years up to date the check was performed, the subject has resided, been employed, and/or attended school for six months or more, including

#	Organization	Question 54 Comment
		current residence regardless of duration. 4.2. Each Responsible Entity shall document the results of each personnel risk assessment. 4.3. Each Responsible Entity shall update or have updated each personnel risk assessment at least once every seven years after the initial personnel risk assessment.
54.51	Entergy	The industry has now had experience grappling with a one-size-fits-all set of cyber security standards' requirements for its grid and generation control systems. At a high level of abstraction the problems with this approach are manifest in two major ways. The first concerns the age of the control system components we have at work relative to cyber vulnerabilities, threats, and hence risk. In brief, our control host systems and operator consoles by and large today use mainstream "IT" commercial off the shelf computer (COTS) hardware, operating systems, and application code bases. These are the very same networked-computing systems components that are widely hacked on the Internet and within mainstream commercial businesses around the world, and accordingly represent highest risk to reliable grid operation from cyber malfunction or nefarious attack. If hacked, they provide the ability for perpetrators to commandeer and use the systems against us - which represents the worst case scenario (e.g., a widespread unplanned "load shedding event" - trip all). On the other far extreme, we have often decades-old computing equipment still widely used "in the field" at substations, switching stations, hydro dams, etc. Increasingly these field sites are connected to control hosts over ("Internet") routable protocol communications networks, and increasingly emergent wireless communications transmission technologies. But there also remains very high dependency on "legacy serial" and "POTS" dial-up communications. So, we have both very old and very new networked-computing control systems technology woven together that requires some kind of cyber security protection. The second major distinction is the physical orientation of control host and generating plant sites on the one hand, and the far flung field assets on the other. The former are typically referred to in security circles as "bastion sites," in that they can be defended in much the same way as castles of old using concentric rings of physical defenses, complimented by armed guards. The field sites on the other hand have more in common with gas and oil pipelines, rail infrastructure, and the like that are characterized by long stretches of geographical separation between sites. These are hard to physically defend economically, and, through use of protocols that by design enable "network navigation" akin to being able to telephone-dial anyone in the country on demand, provide an attack vector path back to control hosts, and therewith also creating opportunities for "island hoping" from one organizational network to another. Given these two decidedly different continuums of variables that the industry needs to

#	Organization	Question 54 Comment
		defend, “one size fits all” standards’ requirements result in situations where the requirements are expensive overkill in one circumstance, and if watered-down to ease this burden do not provide robust enough protections for the circumstance at the other end of the spectrum. The only standards-writing approach that affords appropriate cost-effective security is to define granular sets of standards that are specific to the real vulnerabilities and threats incumbent to each scenario. From this perspective, specific recommendations for improving the current Version 4 draft CIP Standards are outlined below.The SDT was directed in Order 706 to consider adaptation of the NIST Security Risk Management Framework, especially noting SP800-53. This comment is neither about the individual requirements themselves nor the fact that most of the specific CIP-011-1 requirement language was drawn from the DHS Catalog of Controls. Rather, this comment focuses on the fact that the SDT has diverged from FERC directive in not employing a major foundational construct of SP800-53. Specifically, the SDT has developed a single set of requirements, and then through use of sub-requirement tables indicate in binary fashion whether or not each (sub)requirement of note is applicable or not, based strictly on the high-medium-low “impact categorization” based exclusively upon a facility’s size (electrical operating characteristics). Contrast this with the SP800-53 paradigm, where there are three graduated, hierarchical layers of cyber security control and countermeasure requirements. First, there is a baseline set of requirements, which applies for all cyber systems, and these are the only requirements applicable for low-impact-on-mission cyber systems. Then, there is a second and third set of requirements that apply cumulatively for medium and high mission-impact cyber systems respectively. The SP800-53 approach is responsive to the stated FERC preference that there be a baseline set of requirements that must apply for all grid BES Cyber Systems/Components. Draft CIP-010-1 is not responsive to FERC Order 706 - many requirements as stated in the Standards’ language simply do not apply for BES Cyber Systems/Components in use at low and medium-sized grid sites.Recommendation: A) Modify the categorization of grid assets (Attachment II) into two groups:i) “Bastion Installations” consisting of data centers, control centers, and generation sites. Rationale: At least the ‘data center’ part tends to employ mainstream IT COTS HW/OS/and to some degree appl code; and, physical security measures can be used to greater advantage as compensating measures where cyber security measures may be difficult to implement for a variety of reasonsii) “Grid Field Assets” consisting of any physical site that does not have a control host/control center within their physical perimeters, regardless of what protocols are in use. The distinction again revolves around

#	Organization	Question 54 Comment
		physical security, in this case the difficulty in physically securing far flung field sites.B) Create layers of requirements akin to the SP800-53 paradigm, labeled 'a-z': i) The lowest enumerations being baseline requirements; e.g., 'a' could be associated with bastion installations, and 'b' could pertain for field grid asset sites. Important distinctions at the baseline can pertain for each site type.ii) Similarly, create appropriate sets of succeeding requirements applicable specifically to each column (bastion/field) depending on the type of data networking communications employed. This way appropriate requirements - not more nor less than necessary - and be specified for the unique characteristics and attack surfaces posed by each technology. As technologies are retired, e.g., serial legacy, POTS dial-up, so can entire categories of requirements.C) Create a "Scoping Table" consisting of: i) Two columns: Bastion/Field - #1 above); and,ii) X number of rows: #2 above - list of different communications technologies, i.e., routed, legacy serial, dial-up, non-routed LAN, non-routed wireless, etc., as the SDT deems appropriate. D) Apply requirements sets (a-z) as appropriate within each box on the grid.2) Entergy submits that NERC's intention to address the following FERC Order 706 directives in action subsequent to adoption of CIP Version 4 will create undue hardship for the industry. The following Order 706 directives are central to implementation of any organizational cyber security program, and it is unreasonable, inefficient, and potentially financially wasteful to require the industry to implement one approach per Version 4 Requirements, and then be made to re-visit entire cyber security programs in order to comply with post Version 4 changes. Entergy submits that the entire puzzle should be addressed at once, i.e., including the following FERC Order 706 directives, at the same time while recasting the CIP Standards under Version 4:...develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter... a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process.... consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.... revise the Reliability Standard to require two or more defensive measures.... modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years... that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a

#	Organization	Question 54 Comment
		physical security perimeter around critical cyber assets.... consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.... provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan.... to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard.... to revise CIP-009-1 to require data collection, as provided in the Blackout Report.... proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years.Entergy recommends that NERC appeal to FERC for permission to extend the deadline for final Version 4 drafting a modest amount of time necessary for the entire puzzle to be grappled at once. The industry is now hardly complete in implementation of CIP V1-V3 Standards' Requirements. The prospect of having to endure adaptation to two more waves of fundamental change to the tenets of these standards is not only onerous, but also not responsive to the imperative to provide service at lowest reasonable cost to ratepayers. We didn't build our national electric infrastructure overnight, and apt response to relatively recent emergence of cyber security threats will not be accomplished overnight either.
54.52	IRC Standards Review Committee	The organization of the 32 requirements and all of the subrequirements is lesser of a concern to us, although separate standards that group similar requirements allows for better administration. The greater concern is the degree of specificity of many of these standards. As discussed in the response to Q #8, many of these requirements go into exacting detail specific to technology and may duplicate either other industry standards or practices already employed. Many of these requirements can be elevated to "higher level" requirements that requires certain types of protections, e.g. - require user access identification, rather than specific password practices. For examples, the list of criteria that are included in Requirements Table R9, the details in the Tables for R10 and R11, and the specific treatment of wireless access in R12, to name a few.
54.53	Public Service Enterprise	The requirements for wireless and remote access (R11 to R14) are not well integrated with other

#	Organization	Question 54 Comment
	Group companies	requirements for access to BES Cyber Security Systems (R7 to R10).
54.54	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	The table format is great, makes it very easy to see what applies.If we say “CIP-011-1 R3.1” do you know what we am referring to? There is a sub-requirement 3.1 as well as a line 3.1 in Table R3. This could lead to confusion. Suggest extending the table to cover all sub-requirements, or otherwise avoid repeating numbers. This occurs only in R3 and R4.Regarding R21, no definitions have been provided for “other cyber systems” and “Cyber System Components” (without “BES” in the phrase.) Note that “Cyber System Components” is capitalized as if it was defined, but no definition exists or is proposed. While “other cyber systems” is not capitalized, it should also be defined to avoid any ambiguity over what the SDT intends. We appreciate the objectives that the SDT has included in the requirements, since this will help us to see the SDT’s intent. There is the risk, however, that auditors will see this as more than guidance when placed in the requirement. For example, an auditor might read R5 and R6 as requiring the prevention and/or detection of all unauthorized physical access, and find an entity non-compliant for an undetected or un-prevented intrusion. We suggest the objectives (“to prevent..”, “to ensure..”, etc.) be placed in the guidance document, or otherwise be removed from the requirements. Note that some of these objectives when read as requirements are absolute, such as R14; “..to ensure no unauthorized access is allowed.
54.55	MidAmerican Energy Company	The term "Annual" is not defined. Define "Annual" in the NERC glossary to be 12 months not to exceed 15 months. Change all 12 month references back to "Annual".The following provides a summary of the reasons for using a definition of “12 months not to exceed 15 months.” o It does not force “creep.” A definition of 365 days or 12 months, without a “not to exceed” clause means that work must be planned to be done enough before the 365 days to allow time for unexpected situations. This can result in doing “annual” requirements every 10 months or less to ensure compliance is not jeopardized. o It does not jeopardize compliance for either delivery or supply due to current implementation plans. A calendar year definition could unintentionally jeopardize compliance if delivery did not complete a task between June 30 and Dec. 31, 2009. o There is no effect of leap years, which could be a problem with a definition of 365 days._____Requirements that are defined to be completed within x hours are impractical and unnecessary. Entities do not currently document the precise hour that (as an example) a termination takes place. Thus hourly requirements are impractical to measure or audit.

#	Organization	Question 54 Comment
		Convert all hourly requirement as follows: o Convert 1 Hour requirements to "As soon as possible not to exceed date reported". o Convert 4 Hour requirements to "As soon as possible not to exceed date reported". o Convert 6 Hour requirements to "As soon as possible not to exceed date reported". o Convert 12 Hour requirements to "As soon as possible not to exceed date reported". o Convert 24 Hour requirements to "As soon as possible not to exceed next day from date reported". o Convert 36 Hour requirements to "As soon as possible not to exceed next day from date reported". o Convert 48 Hour requirements to "As soon as possible not to exceed next day from date reported". o Convert 72 Hour requirements to "As soon as possible not to exceed second day from date reported"._____The following FERC Directives need to be addressed with version 1 of CIP-010 and CIP-011: o 2 or more diverse security measures for defense in depth at the security boundaries o Active vulnerability assessments every 3 years o Incorporate forensic data collection and proceduresThe framework is in place to incorporate requirements in CIP-011 that address the directives. CIP-011 has a potentially long implementation time. FERC will likely not wait for the implementation of CIP-011-1 to be complete prior to making NERC address these directives. Incorporating these directives in the middle of the implementation of CIP-011-1 will be confusing and cause additional expense and effort. Entities will be required to make additional expenditures at greater cost if these issues are resolved in later versions. NERC should ask FERC for more time to implement version 1 if necessary.
54.56	Dairyland Power Cooperative	There are very few requirements that apply to low impact systems and many that do not apply to medium impact systems. Considering that many high impact systems will connect with lower impact systems, how will data integrity be adequately implemented? Consider a large RTO/ISO connecting a shared communications system to all entities in a region, regardless of impact to the BES.The standard basically excludes serial communications from being governed. This not only does not address protecting serial systems, but it introduces oddities and ambiguities about routable connections in relation to serial connections. There are security questions, as well as questions as to how such connections will be viewed by an auditor. Serial communications should not be ignored.
54.57	Ameren	These standards will require a substantional amount of effort to implement for entities while also maintianing compliance with the previous versions of the CIP standards, how will the implementation schedule address this? Will their be a period were the entity does not have to comply with the old

#	Organization	Question 54 Comment
		standards while implementing the new standards, for examle 30 days to 90 days while the entity is updating systems or updating/revising procedures for the new standards. Also, the local definitions should be included in the NERC glossary of terms rather than by the standard to which they apply.
54.58	Bonneville Power Administration	This is far better than the current standards. The requirements are more straight forward by not cross referencing each other in separate standards. Much time is spent "mapping" out how the standards relate to each other and under what specific requirements. If misinterpreted it could lead to potential violations. This is a much better approach. Not directly relating to the newly proposed standards but still a concern is the time for implementation. Numerous resources have been extended and significant dollars spent to meet the current requirements. There needs to be sufficient time to review the new standards, identify Cyber Systems and allow for proper prior planning to physically protect these systems. Depending on the category, low-high, significantly more dollars could be spent. There needs to be sufficient time to address the new standards and implement in a manner that is cost effective. The overall approach is superb: target the standards only at systems that can actually affect the BES in near-real time, include other systems only to the minimum extent necessary, require outcomes rather than specify actions. However, this draft has some wording issues that apparently have inadvertently broadened the scope far beyond the intent of the SDT, or even practicality. As described above, correcting these errors will produce a set of standards that enforce security where it needs to be, but do not waste time, money, and people addressing tasks that do not improve the security of the BES. In particular, we find that the following questions address issues that must be corrected before the standards could be acceptable:- Q5, addressing CIP-010 Table R3 Section 3.2- Q12, addressing CIP-011 Table R3 Section 3.2- Q13, addressing the the definition of "External Connectivity". Note that several other questions rely upon changing this definition.- Q16, addressing CIP-011 Table R5, sections 5.8 and 5.9- Q22 and Q23, addressing revocation time limits- Q24, addressing authentication schemes- Q27, definition of "Remote Access"- Q32, addressing revocation of remote access- Q33, addressing Table R14 Sections 13.2 and 14.4- Q35, addressing Table R16, Section 16.2 and patch risk assessment- Q35, addressing Table R17, Section 17.2 and disabling of physical ports- Q35, addressing Table R18, Sections 18.1, 18.2, 18.3, and 18.4- Q37, addressing Table R20, Sections 20.1, 20.2, 20.3, 20.6- Q37, addressing Table R21, Section 21.1- Q38, addressing the second part of the definition of electronic access point. This is the most serious flaw in the standard. It must be corrected.- Q40, addressing Table R23 section 23.7- Q42, addressing the definition of

#	Organization	Question 54 Comment
		sensitive information- Q44, addressing Table R24, Section 24.1 and 24.3- Q47, addressing Table R26, section 26.2- Q51, addressing Table R30, Section 30.5- Q51, addressing Table R31, sections 31.1 and 31.2- Q53, addressing TFEs Overall, an excellent start. Here are some additional suggestions:1. In all cases - Write the standards to identify the outcome of the requirement. Never say how to do something, say what you intend for it to accomplish. Let the Responsible Entities figure out the "how".2. Use Industry Standard wording wherever possible. For example, the term "Hardened" means one thing in IT and another in a substation.3. Define any terms that may present confusion - Example - Ports and services. There is a common IT understanding when you hear that term. It is almost always assumed to mean logical ports 0 to 65535 and the networking services they support. However, it can also mean physical ports like Ethernet jacks, RJ45, Serial connectors, parallel connections etc. If there is a question, put it in the definitions.4. Wherever possible, include all the elements of a standard into one standard. Only break requirements apart where it makes real sense to do so. So If you get to R32 and find that something there seems to fit in 20, go back and put it there rather than making a reference back. 5. Keep paring this down in size. It is so much better.6. If any of your experts know that equipment used in the electrical generation and distribution industry cannot perform specific functions, don't write the standards to say they have to.7. There were questions in the May webinar about the meaning of "revocation". Our suggestion is this: revocation is the act of ensuring that a person can no longer gain access to a system, physical area, or information. It can be accomplished directly or indirectly. For instance, if a cyber asset is only accessible from within a physical facility, then denying physical access to the facility also denies cyber access to the cyber asset. If sensitive information on a system resides only in electronic form on particular servers, then denying cyber access to those servers denies access to the information. The emphasis should be on the denial of access, not how that denial is accomplished.Definition of "annual" or "annually": There are numerous occurrences of these terms in the Requirements. Also now, Requirements state that activities must occur "at least once every 12, 24, or 36 months." Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. "/A/t least once every 12 months" could lead to some confusion. Let's assume that the event occurred on July 15, 2010, and again on March 15, 2011. That is "at least once every 12 months." But it raises the question of when the next activity or compliance event must occur. Is it no later than July 15, 2011, or no later than March 15, 2012? The exact questions could be asked for events that are supposed to occur "at

#	Organization	Question 54 Comment
		least once every 24 or 36 months."Following on to comment 1 immediately above, there are two other phrases that could be used depending on what NERC intends. o "every 12 months" - in this case, the event would occur on the same date each year. This would be virtually impossible. Same concern with "every 24 or 36 months." o "within 12 months of" the event - in this case let's assume that the event occurred on March 15, 2010. The next event would have to occur no later than March 15, 2011, but could occur earlier (let's say it occurred on December 15, 2010). If it occurred on December 15, 2010, the next event would have to occur no later than December 15, 2011. The same example with different dates would work for "at least once every 24 or 36 months."The SDT should be very specific as to what it means for how frequently the events referenced above must occur. BPA appreciates the opportunity to provide comments. Thank you.
54.59	MRO's NERC Standards Review Subcommittee	We believe all of the requirements that specify something to be completed within X hours would be better suited to the following language: "As soon as practical, but not to exceed x business days from the date reported". This would maintain the spirit of the requirement, while also allowing for more practical time frames.With so many auditable elements included within the requirements, we believe the VSL's cannot be written with the current zero-defect mentality. We feel a practical approach is required, where minor issues are allowed to be addressed without representing immediate non-compliance and associated investigations and settlement proceedings, but instead are identified and scheduled for corrective action.We understand the burden on the drafting team to meet FERC's deadlines, but we would propose that all outstanding FERC directives be addressed as part of the current process, as opposed to leaving some items for a later date.
54.60	Idaho Power Company	We commend the SDT on its efforts to draft a standard that meets the FERC directives but is feasible for the industry to implement. That is an extremely difficult assignment. This version will greatly expand the number of cyber assets that are impacted by the CIP requirements and represents a major shift in the identification and classification of an entities BES cyber systems. We are certainly willing to implement the standards because we understand the impact of failure to do so. However, the standards must be accompanied by as much guidance documentation as possible along with realistic implementation plans that take into account the technology required, time required to realistically implement the controls, the fact that registered entities must first assess the financial impact and then

#	Organization	Question 54 Comment
		budget appropriately, and the massive volume of work that implementation represents.
54.61	Xcel Energy	We do not agree that Low impact systems should have mandatory, enforceable cyber security standards. By their very definition, Low impact systems have very little potential to impact the BES. As such, cyber security controls on these systems is best left to the business judgment of each individual entity. The terms defined throughout the standard have not followed the convention of being capitalized. They should be capitalized so that it is clear to the reader that they are defined terms when they are used later in the standard. The Standard would be enhanced if it were to differentiate between software based versus firmware based devices.The Standard would also be enhanced if it were to separately define requirements for Control Centers, Substations, and Generation Facilities. The cyber security issues between these different types of facilities are vastly different. Transmission Control Centers are typically fully digital control systems with the ability to have wide area impacts. On the other extreme, where Generation facilities typically have digital systems are for retrofits to older, analog systems controlling individual components within the facility, such as digital feedwater or digital turbine controls. These are much different that Transmission Control Centers as they have only limited, local impact. Additionally, they typically have mechanical controls that can override the digital systems providing limited, if any benefit from protecting the digital aspects of the system from malicious attacks.
54.62	We Energies	We Energies agrees with EEI: Please see the earlier discussion about identification of a rational and understandable threat basis that should be used when constructing security requirements. The requirements should focus on the highest probability risks that will have the most negative impact. The requirements should not treat all threats and impacts equally.
54.63	Duke Energy	We had previously gone a long way towards getting common understanding on terms such as “Critical Assets”, Critical Cyber Assets”, “Electronic Security Perimeter” and Physical Security Perimeter”. Moving away from these terms in the current Version 4 draft creates uncertainty.Tables and subrequirements should have different numbering schemes so that, for example, there are not two 3.1 listings.If the standard is broken into smaller standards, please provide separate measures for each standard.

#	Organization	Question 54 Comment
54.64	Hydro One	We noticed that combined CIP-011-4 standard excluded vulnerability management program. We'd like to know what the rationale was behind this decision and if this might be considered in the next draft.Suggestion for an additional page that repeats all of the local definitions - this means the local definitions exist in the document as is plus this additional page.Request that the tables and time constraints be consistent. Also where the document refers to processes in some cases it specifies one or more processes and in others just processes. Eliminate confusion caused by two 3.1's. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (refer to R5-R32).Request a cross-reference of CIP-011 Requirements that refers to another CIP-011 Requirement, with emphasis on the Access Control Requirements. A diagram might help.Remove adjectives such as substantial, adequate, minimum, etc., as these are difficult to measure and can lead to different interpretations.
54.65	GTC & GSOC	We recommend a local definition of "Implement" should be added to CIP 011: "Implement means to put into place and consistently utilize. An entity has implemented a policy, procedure, or plan when it has created such policy, procedure or plan and consistently uses it in appropriate circumstances."Throughout the standards the inclusion of the words "for external connectivity only" in the tables is redundant and confusing. If used at all, the qualifier should be on "access" in the text of the standard rather than in the table.We recommend Annual be defined as recurring at least once every Calendar year and at least once within any thirteen (13) consecutive calendar months. Otherwise, annual training will necessarily have to take place earlier each calendar year to ensure all personnel are trained within twelve (12) months.We appreciate the significant effort that the NERC Cyber Security Order 706 Standards Drafting Team has put into developing these proposed standards and communicating them to the industry, especially the CIP Workshop held in Grapevine, TX. We are in full support of the NERC standards development process for the development of reliability standards to secure and protect North America's critical electric infrastructure. In particular, we appreciate the multiple opportunities to guide the development of the CIP standards through both informal and formal comment periods. We are supportive of the proposed standards. We believe these standards are a significant step forward in terms of being able to clearly understand the expectations that are placed upon the entity as well as the security that they provide for the Bulk Electric System.

#	Organization	Question 54 Comment
54.66	PNM Resources, Inc.	We suggest not removing explicit examples from the language of the standards. The incorporation of examples provides clarity and brightline guidance that improves a Responsible Entity's opportunity to comply with the standard. The introduction of new and additional "flexibility" can lead to ambiguity and differences of opinion between the entities and auditors and creatr more opportunities for Regional Entities to allege violations.
54.67	MWDSC	When looking at logical tasks to mitigate risk, e.g., malicious code propagation, could a malicious code in one cyber component affect another component and result in a change in the impact categorization, e.g., low vs medium?
54.68	Progress Energy - Nuclear Generation	Yes, see comments a - f below.a. Comments: Attachment 1 included in responses above follows this question. To obtain full benefit of this review, see Attachment 1.b. The security controls in CIP-011-1 should provide for acceptance of Common Controls as defined by NIST 800-53. CIP-011-1 would offer a more consistent approach in cyber security regulation by considering the mature physical security programs, engineering control programs, emergency plans and physical segregation programs within the nuclear industry that offer alternative countermeasures. These countermeasures provide at least the same degree of cyber security protection as the corresponding cyber security control. c. NIST 800-53 establishes provision for tailoring security controls and states that the level of detail required in documenting tailoring decisions in the security control selection process is strictly at the discretion of the organization consistent with the impact level of the information system. CIP-010-1 and CIP-011-1 should allow use of this provision in the nuclear industry consistent with acceptance by nuclear regulators.d. Nuclear applicability is specified in CIP-010-1, Section 4.2.1. The following comments are based on applicability to nuclear generating facilities: o Definitions for Bulk Electrical System (BES) Cyber System and BES Cyber System Component conflict with definitions that have been accepted by the NRC in NEI 08-09, Revision 6, for Critical System and Critical Digital Asset. Recommend, that for nuclear systems subject to FERC Order 706-B, that definitions for FERC and NRC regulated systems be consistent. o CIP-010-1 requirement R2 and Attachment 1 - some of these functions are covered by NRC regulation. Will issuance of this document require re-submittal of systems for exemption after the Bright Line submittal of systems? o The implementation schedule for CIP-010-1 and CIP-011-1 versus CIPs 002 through 009 requires doing the same reviews twice and is an unnecessary burden on

#	Organization	Question 54 Comment
		nuclear licensees as well as other FERC critical assets.e. Several requirements include periodic review of controls (e.g., R8.2, R12.1). This CIP should contain a provision that permits nuclear facilities to use the periodicities in its NRC approved Cyber Security Program in lieu of those in the CIP standards. This allowance would minimize the administrative burden of having two sets of requirements for the same Cyber Security programmatic element so that plant digital systems that support safety, security, EP or BOP functions are not regulated differently. The following are used to establish frequency or periodicity for security controls with identified durations: o NRC Regulations, Orders o Operating License Requirements (e.g., Technical Specifications) o Site operating history o Industry operating experience o Experience with security control o Guidance in generally accepted standards (e.g., NIST, IEEE, ISO) o Audits and Assessments o Benchmarking o Availability of new technologies. f. R27.1 - The definition of "Cyber Security Incident" should be revisited in light of current definitions, especially NRC and NEI, and revised to align with the definition of "Cyber Attack." It is not on the list of terms to be defined. From NERC Glossary of Terms used in NERC Reliability Standards updated April 20, 2010, the "Cyber Security Incident" definition is: o Any malicious act or suspicious event that:o Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,o Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.o It is unclear what NERC does with cyber incident reports and whether these reports are consistent with those required by the NRC in the event of a "cyber attack." Progress Energy Nuclear Generation Group CommentsCIP- 011-1ATTACHMENT 1NIST Security Control Description NIST 800-53 NEI 08-09 NEI 08-09 Description CIP-011-1 CIP-011 Description NRC CommentsSecurity Planning Policy and Procedures PL-1 N/A N/A R1 Security Governance and Policy 50 App B 50 App E73.5473.5573.56 The development and implementation of cyber security policies that address the requirements identified in R1 are mandated for nuclear by one or more Code of Federal Regulations (CFR). This requirement duplicates and/or is not consistent with the CFR and could lead to regulatory uncertainty. Review of cyber security is mandated by 73.55(m) and R1 conflicts with its duration. This would result in conflicting requirements for BOP systems and would result in dual regulation for the nuclear plant.Security Awareness AT-2 E9.2 Awareness Training R2 Personnel Training, Awareness and Risk Assessment 73.5450 App B Training requirements for nuclear personnel are established by CFR. R 3.3.2 would result in personnel without a need to know becoming knowledgeable in technical aspects of digital equipment. R3.3.4 is not required for users to perform

#	Organization	Question 54 Comment
		their job. This conflicts with 73.54 requirements that personnel are trained to the extent necessary to perform their assigned duties. This would result in conflicting requirements for BOP systems and would result in dual regulation for the nuclear plant.Security Training AT-3 N/A N/A R3 Personnel Training, Awareness and Risk Assessment 73.5473.55 Physical and logical access to plant digital systems is governed by CFR. Personnel who are granted access to these systems are required to complete training that result in their receiving formal and documented Qualifications. Requalification is at established intervals required by plant procedures. Whether the plant system performs functions associated with safety, security, emergency preparedness or BOP, the requirements are the same. Additional training and duration not consistent with established mature training programs would result in conflicting requirements for BOP systems and would result in dual regulation for the nuclear plant. R4 Personnel Risk Assessment 73.56 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. Results are documented and stored in Records. The requirements in R4 conflict with the requirements in the CFR that nuclear personnel supporting plant system performs functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from requirement R4. R5.1 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. before being granted unescorted physical access to nuclear plants. The nuclear plant is protected by armed security officers and other protective strategy that restricts access. The requirements in R5.1-3 are covered by the CFR for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement. R5.2 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. before being granted physical access to nuclear plants. Results are documented and stored in Records. The requirements in R5.2 are covered by the CFR for restricting physical access for all plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement. R5.3 Physical Security for BES Cyber

#	Organization	Question 54 Comment
		Systems 73.55 Nuclear personnel must pass through security access points before being granted physical access to nuclear plants. Automated scanning records entry. The requirements in R5.3 are covered by the CFR for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement.Monitoring Physical Access PE-6 E5.8 Monitoring Physical Access R5.4 Physical Security for BES Cyber Systems 73.55 Visitors must receive approval prior to arriving at the security access points and are subject to search before being granted physical access to nuclear plants. Entry and exit are documented. The requirements in R5.4 are covered by the CFR for nuclear visitors supporting plant systems performing functions associated with safety, security, emergency preparedness, BOP or other. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement.Physical Access Authorizations PE-2 E5.4 Physical Access Authorizations R5.5 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. before being granted unescorted physical access to nuclear plants. Results are documented and stored in Records. The requirements in R5.5 are covered by the CFR for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement.Physical Access Control PE-3 E5.5 Physical Access Control R5.6 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to annual retraining in order to maintain unescorted physical access to nuclear plants. Results are documented and stored in Records. The requirements in R5.6 conflict with the CFR that cover access authorization for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement. R5.7 Physical Security for BES Cyber Systems Part 2673.56 Requirements for nuclear personnel terminated for cause are covered by the CFR. The requirements in R5.7 conflict with the CFR that direct termination for cause of nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting

#	Organization	Question 54 Comment
		nuclear facilities from this requirement. R5.8 Physical Security for BES Cyber Systems 73.55 N/A to nuclear - applicable to Control Center R5.9 Physical Security for BES Cyber Systems 73.55 Requirements for nuclear personnel who no longer require physical access are covered by CFR. The requirements in R5.9 conflict with the CFR that covers removing physical access for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement.Monitoring Physical Access PE-6 E5.8 Monitoring Physical Access R5.10 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are trained and qualified to provide continuous escort for visitors while they are granted physical access to nuclear plants. The requirements in R5.10 are covered by the CFR for nuclear personnel who escort visitors supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R5.11 Physical Security for BES Cyber Systems 73.55 Unauthorized physical access is handled by armed security officers in nuclear security. The requirements in R5.11 are covered by the CFR for unauthorized physical access to the plant where systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R6.1 Physical Access Control Systems 73.55 Physical access control systems are covered by CFR requirements. The requirements in R6.1 are covered by the CFR and this physical access control system is subject to nuclear cyber security regulation only. Consider exempting nuclear facilities from this requirement. R6.2 Physical Access Control Systems 73.55 Physical access control systems are covered by CFR requirements. The requirements in R6.2 are addressed in the CFR and this physical access control system is subject to nuclear cyber security regulation only. Consider exempting nuclear facilities from this requirement. R6.3 Physical Access Control Systems 73.55 Physical access control systems are maintained and tested per CFR requirements. The requirements in R6.3 are addressed in the CFR. Therefore, this physical access control system is subject to nuclear cyber security regulation only. Consider exempting nuclear facilities from this requirement.Account Management AC2 D1.2 Account Management R7 Account Management Specifications Consistent with nuclear cyber security plan.Least Privilege AC6 D1.6 Least Privilege R8.1 Account Management Implementation Consistent with nuclear cyber security plan.Account Management AC2 D1.2 Account Management R8.2 Account Management Implementation Duration is inconsistent with nuclear cyber security plan. Requirements should be the same for plant systems whether they support safety, security, EP or BOP.Account

#	Organization	Question 54 Comment
		Management AC2 D1.2 Account Management R8.3 Account Management Implementation Consistent with nuclear cyber security plan. R9.1 Personnel Terminated for Cause Part 2673.56 Duration is inconsistent with nuclear requirements.N/A N/A N/A N/A R9.2 Personnel Terminated for Cause (Control Center) N/A to nuclear - applicable to Control CenterN/A N/A N/A N/A R9.3 Personnel Terminated for Cause (Control Center) N/A to nuclear - applicable to Control CenterAccount Management AC2 D1.2 Account Management R9.4 Access Revocation Duration is inconsistent for removal of access for personnel who no longer require access with nuclear cyber security plan. Requirements should be the same for plant systems whether they support safety, security, EP or BOP. Identification and Authentication (Non-Organizational Users) IA-8 D4.2 Identification and Authentication (Non-Organizational Users) R10.1-5 Account Access Control Specifications The control of passwords contained in R10.1 - 8 is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should include the provision contained in note 1 for digital assets that are not technically capable of supporting some of the password requirements. CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Least Privilege AC6 D1.6 Least Privilege R10.6 Account Access Control Specifications The control of passwords contained in R10.6 is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should contain provision for digital assets that are not technically capable of supporting some of the password requirements such as Hierarchical permissions.CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Access Enforcement AC3 D1.3 Access Enforcement R10.7 Account Access Control Specifications The control of passwords contained in R10.7 is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should contain provision for digital assets that are not technically capable of supporting some of the password requirements such as system and security administrative accounts. CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by

#	Organization	Question 54 Comment
		nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Separation of Duties AC5 D1.5 Separation of Functions R10.8 Account Access Control Specifications The control of passwords, contained in R10.8, is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should contain provision for digital assets that are not technically capable of supporting some of the password requirements such as Hierarchical permissions.CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Wireless Access AC18 D1.17 Wireless Access Restrictions R11.1 Wireless and Remote Electronic Access Documentation Consistent with nuclear requirements.Remote Access AC17 D.1.1 Access Control Policy and Procedures R11.2 Wireless and Remote Electronic Access Documentation Consistent with nuclear requirements.Remote Access AC17 D.1.1 Access Control Policy and Procedures R11.3 Wireless and Remote Electronic Access Documentation Consistent with nuclear requirements.Remote Access AC17 D.1.1 Access Control Policy and Procedures R12 Wireless and Remote Electronic Access Management 73.5573.56 Duration is inconsistent with nuclear requirements for reviewing remote access. Other physical security and access authorization nuclear regulation ensures personnel who have remote access are trustworthy and reliable therefore this type of review is not justified.N/A N/A N/A N/A R13.1 Remote Access Revocation (Control Center) N/A to nuclear - applicable to Control CenterN/A N/A N/A N/A R13.2 Remote Access Revocation (Transmission) N/A to nuclear - applicable to TransmissionRemote Access AC17 D.1.1 Access Control Policy and Procedures R13.3 Remote Access Revocation Part 26 73.56 Duration is established in nuclear requirements for removal of access for personnel who no longer require remote access.Remote Access AC17 D.1.1 Access Control Policy and Procedures R14.1-3 Wireless and Remote Electronic Access Control Consistent with nuclear requirements.System Use Notification AC8 D.1.8 System Use Notification R14.4 Wireless and Remote Electronic Access Control Inconsistent with nuclear requirements. CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. Add provision for this requirement to be implemented if technically supported.Malicious Code Protection SI-3 E3.3 Malicious Code Protection R15 Malicious Code Consistent with nuclear regulation.N/A N/A

#	Organization	Question 54 Comment
		D5.5 Installing Operating Systems, Applications, and Third Party Software Updates R16.1 Security Patch Management Duration is inconsistent with nuclear regulation otherwise requirements are consistent. D5.5 Installing Operating Systems, Applications, and Third Party Software Updates R16.2 Security Patch Management Consistent with nuclear regulation.N/A N/A D5.4 Hardware Configuration R17 System Hardening Consistent with nuclear requirements.Information System Monitoring SI-4 E3.4 Monitoring Tools and Techniques R18.1 Security Event Monitoring Consistent with nuclear requirements.Information System Documentation SA-5 E6 Defense-In-Depth R18.2 Security Event Monitoring Consistent with nuclear requirements.Incident Monitoring IR-5 E7.5 Incident Monitoring R18.2 Security Event Monitoring Consistent with nuclear requirements.Baseline Configuration CM-2 E10.3 Baseline Configuration R18.4 Security Event Monitoring Duration for maintaining logs is inconsistent with nuclear requirements. The duration for maintaining logs for digital systems that support safety, security, EP or BOP functions should not be regulated differently.N/A N/A E6 Defense-In-Depth R18.4 Security Event Monitoring Duration for review of logs is inconsistent with nuclear requirements. The duration for reviewing logs for digital systems that support safety, security, EP or BOP functions should not be regulated differently.N/A N/A N/A N/A R19 Communication and Data Integrity in a Control Center N/A to nuclear - applicable to Control CenterBoundary Protection SC-7 E6 Defense-In-Depth R20 Electronic Boundary Protection Consistent with nuclear regulation other than duration. The duration for reviewing alerts and logs for digital systems that support safety, security, EP or BOP functions should not be regulated differently.N/A N/A N/A N/A R21.1 System Boundary Protection N/A to nuclear - applicable to Control CenterBoundary Protection SC-7 E6 Defense-In-Depth R21.2 System Boundary Protection 73.54 Consistent with nuclear requirements. R22 Protective Cyber Systems (duplicate of R14,16,18,23) Duplicate - (duplicate of R14,16,18,23); Remove not neededInformation System Component Inventory CM-8 E10.9 Component Inventory R23.1 Configuration Change Management 73.54 Consistent with nuclear regulation.Baseline Configuration CM-2 E10.3 Baseline Configuration R23.2 Configuration Change Management 73.5450 App B Consistent with nuclear regulation.Configuration Change Control CM-3 E10.4 Configuration Change Control R23.3 Configuration Change Management 73.5450 App B Duration is inconsistent with nuclear regulation. Nuclear configuration management programs are mature and are required by 10CFR50 Appendix B. They are implemented for plant digital systems that support safety, security, EP or BOP functions and duration for updating configuration records and documenting changes should not be

#	Organization	Question 54 Comment
		regulated differently.Baseline Configuration CM-2 E10.3 Baseline Configuration R23.4 Configuration Change Management 73.5450 App B Duration is inconsistent with nuclear regulation. Nuclear configuration management programs are mature and are required by 10CFR50 Appendix B. They are implemented for plant digital systems that support safety, security, EP or BOP functions and duration for updating configuration records and documenting changes should not be regulated differently.Configuration Change Control CM-3 E10.4 Configuration Change Control R23.4 Configuration Change Management 73.5450 App B Duration is inconsistent with nuclear regulation. Nuclear configuration management programs are mature and are required by 10CFR50 Appendix B. They are implemented for plant digital systems that support safety, security, EP or BOP functions and duration for updating configuration records and documenting changes should not be regulated differently.Configuration Change Control CM-3 E10.4 Configuration Change Control R23.5 Configuration Change Management 73.5450 App B Consistent with nuclear requirements.Baseline Configuration CM-2 E10.3 Baseline Configuration R23.6 Configuration Change Management 73.5450 App B Consistent with nuclear requirements.Information System Component Inventory CM-8 E10.9 Component Inventory R23.7 Configuration Change Management 73.54 Consistent with nuclear requirements.Media Protection Policy and Procedures MP-1 E 1.1 Media Protection Policy and Procedures (SGI, Non-SGI, 2.390) R24.1 Information Protection Consistent with nuclear requirements.Information Output Handling and Retention SI-12 E3.10 Information Output handling and Retention R24.2 Information Protection Consistent with nuclear requirements. R24.3 Information Protection 73.56 The requirements in R24.3 are covered by the CFR for authorization to view security sensitive information for plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R24.4 Information Protection 73.56 The requirements in R24.4 are covered by the CFR for unauthorized physical access to the plant where systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R24.5 Information Protection 73.56 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. to ensure their trustworthiness and reliability. This requirement is not necessary for nuclear personnel. Consider exempting nuclear facilities from this requirement.Media Sanitation MP-6 E 1.6 Media Sanitation and Disposal R25 Media Sanitation Consistent with nuclear requirements.Maintenance

#	Organization	Question 54 Comment
		Personnel MA-5 E4.3 Personnel Performing Maintenance and Testing Activities R26.1 Maintenance Consistent with nuclear requirements.Maintenance Tools MA-3 E4.2 Maintenance Tools R26.2 Maintenance 50 App B Consistent with nuclear requirements.Incident Handling IR-4 E7.1 Incident Handling R27.1 Cyber Security Incident Response Plan Specifications DG-501950 App B50 App E The requirements in R27.1 are covered by the CFR for classifying events as Cyber Incidents whether the plant systems performing functions associated with safety, security, EP or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently.Incident Handling IR-4 E7.4 Incident Handling R27.2 Cyber Security Incident Response Plan Specifications 73.54 Consistent with nuclear regulation.Incident Reporting IR-6 N/A N/A R27.3 Cyber Security Incident Response Plan Specifications 73.5473 Appendix GDG 5019 This requirement should be addressed by NRC and FERC/NERC to ensure consistency in reportability requirements.Incident Response Testing and Exercises IR-3 E7.3 Incident Response Testing and Drills R28 Cyber Security Incident Response Plan Testing Specifications 73.54 Nuclear testing of Incident response plans is regulated by site E-Plans. When appropriate, plant digital systems that support safety, security, EP or BOP functions are included and duration for testing these plans should not be regulated differently. Incident Response Policy and Procedures IR-1 E7.1 Incident Response Policy and Procedures R29 Cyber Security Incident Response Plan Review, Update and Communication Specifications 73.5450 App E Duration is inconsistent with nuclear regulation. Nuclear review and updating of Incident response plans is regulated by site E-Plans. When appropriate, plant digital systems that support safety, security, EP or BOP functions are included and duration for testing these plans should not be regulated differently.Incident Response Policy and Procedures IR-1 E7.1 Incident Response Policy and Procedures R30.1 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Contingency Plan CP-2 E8.1 Contingency Plan R30.2 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Information System Recovery and Reconstitution CP-10 E8.6 Recovery and Reconstitution R30.3 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Information System Backup CP-9 E8.5 CDA Backup R30.4 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Information System Backup CP-9 E8.5 CDA Backup R30.5 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Contingency Plan Testing and Exercises CP-4 E8.2 Contingency Plan Test R31 Recovery Plan Testing Specifications 73.54 Duration is inconsistent with nuclear regulation. Nuclear tests and exercises for recovery for plant digital systems that support safety, security, EP or BOP functions

#	Organization	Question 54 Comment
		should not be regulated differently. R32 Recovery Plan Review, Update, and Communications Specifications Neither nuclear regulation nor NIST 800-53 contain expectations reviews, updates and communication of recovery plans at the frequencies established by R32. The bases for R32 requirements are unclear and consideration should be given to removing it.

END OF REPORT

Project 2008-06 Cyber Security Order 706

Consideration of Issues and Directives — DRAFT

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 25 We direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework.	FERC Order 706	It is important to highlight differences between NERC's and NIST's approaches. At the root of these differences is the divergent responsibilities and goals. NIST is providing standards and guidance for U.S. Federal Agencies in managing risks to their information and systems in support of their unique missions. NERC, on the other hand, has the role of setting standards for managing risks to systems in support of a shared community mission to ensure the reliability of the BES. This difference is important because it enables the industry to develop better detail about the impacts that they need to avoid in order to achieve their mission. NIST does not enjoy this benefit, as they are providing standards to almost two hundred different organizations, each with vastly different missions. The advantage that the NERC Standards enjoy enables a focus on a relatively small number of reliability services that need to be protected.
		This ultimately means that the NERC Standards can be more tailored and appropriate to the industry than a wholesale adoption of the NIST Risk Management Framework. Four key

Project 2008-06 Cyber Security Order 706		
Issue or Directive	Source	Consideration of Issue or Directive
		features of the NIST Risk Management Framework were incorporated into version 5 NERC CIP Standards: (1) ensuring that all BES Cyber Systems associated with the Bulk-Power System, based on their function, receive some level of protection, (2) customizing protection to the mission of the cyber systems subject to protection, (3) a tiered approach to security controls which specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk-Power System, and (4) the concept of the BES Cyber System itself. Features 2 and 3 above are tightly coupled. In the NIST Risk Management Framework, there is a concept of tailoring and scoping which allows the organization to determine which controls are applicable to their specific environment. In the NERC compliance framework, all requirements are mandatory and enforceable and therefore this concept does not translate directly. As such, the customization of protections by mission is based upon the environment that the BES Cyber System supports (control center, transmission facility, generation facility) and utilizes the tiered model and the requirement applicability to provide this customization to the individual environments that together support a combined mission of Bulk Power System Reliability. The NIST security control catalogue in 800-53 revision 3 was also used as a reference in addressing many of the FERC directives in Order 706.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 and 252 "Para 258. As to Entergys suggestion that the ERO provide a DBT profile of potential adversaries, the ERO should consider this issue in the Reliability Standards development process. Para 252. Entergy suggests, as an alternative approach to critical asset identification, that the ERO provide a Design-Basis Threat (DBT) a profile of the type, composition, and capabilities of an adversary that would assist the industry as a technical baseline against which to establish the proper designs, controls and processes. Entergy claims that a DBT approach would address many of the Commission's concerns regarding the risk-based methodology. For example, a DBT would focus the appropriate emphasis on the potential consequences from an outage of a critical asset. In addition, a DBT would address the Commissions concern that responsible entities will not have enough guidance in developing a risk-based methodology and not know how to identify a critical asset. Entergy contends that a DBT approach would provide the industry with more certainty in implementing the CIP Reliability Standards."	FERC Order 706	CIP-002-5 classifies BES Cyber Systems through impact thresholds, and does not use risk-based assessments performed by individual entities. Risk-based approaches to applying cyber security requirements is a worthy objective and will continue to be explored, but the complexity and subjectivity it adds is beyond the scope of these revisions.
Para 282 The Commission directs the ERO to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets.	FERC Order 706	The definition of BES Cyber Asset as used in CIP-002-5 requires Responsible Entities to consider misuse of the Cyber Assets in identifying BES Cyber Systems.
Para 285 The Commission directs the ERO to consider the comment from	FERC Order 706	The exclusion of Cyber Assets based on non-routable protocols has been removed from CIP-002-5 and added as a

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
ISA99 Team [ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience].		scoping filter for requirements where: (i) the use of non-routable protocols is a mitigating factor for the vulnerabilities a requirement addresses and (ii) implementation of routable protocols would be required to comply with the requirement (e.g. malware updates, security event monitoring and alerting, etc.).
Para 321 "Para 321. SPP and ReliabilityFirst suggest modifying CIP-002-1 to allow an entity to rely upon the assessment of another entity with interest in the matter. We believe that this is a worthwhile suggestion for the ERO to pursue and the ERO should consider this proposal in the Reliability Standards development process. We note that, even without such a provision, an entity such as a small generator operator is not foreclosed from consulting with a balancing authority or other appropriate entity with a wide-area view of the transmission system."	FERC Order 706	The SDT considered this suggestion, and it believes that the change to “bright line” criteria for identifying BES Cyber Systems, along with refining the scope of certain requirements through applicability columns based on impact and connectivity characteristics, addresses this concern.
Para 376 “the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards.”	FERC Order 706	The SDT removed the CIP-003-4 requirement to document exceptions to the Cyber Security Policy. • The SDT considers this a general management issue that is not within the scope of a compliance requirement. • The SDT found no reliability basis in this requirement. • Removal of this requirement provides clarity that the

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		only exceptions to the requirements is through the defined Technical Feasibility Exception process, where specifically allowed.
Para 386 The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly.	FERC Order 706	To address this directive, in CIP-004-5, Requirement R7, Responsible Entities are required to revoke access to BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.
Para 397 and 398 "The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes."	FERC Order 706	Two new requirements were added to address this change CIP-010-1, Requirement R1 (item 1.4), requires additional testing prior to a configuration change in a test environment. CIP-010-1, Requirement R2 (item 2.1), requires monitoring of the configuration of the BES Cyber System. • The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System. • Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment prior to their implementation in the

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		production environment to aid in identifying any accidental consequences of the change.
Para 433 “we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard.”	FERC Order 706	The SDT addressed this by determining that identification of certain core training elements would be beneficial, and the identification of those core training elements that must be provided in the training program should be role based, as required in CIP-004-5, Requirement R2
Para 434 “The Commission adopts the CIP NOPR’s proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets.”	FERC Order 706	The SDT added this as a topic for role-specific training in CIP-004-5, Requirement R2 (item 2.10). Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems.
Para 435 “Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves.”	FERC Order 706	The SDT has considered the issue and has determined that no modifications are necessary. In practice, this training is often conducted as computer based training (CBT). As such, as long as the training material itself is adequate, which can be evaluated through the existing audit process, security trainers themselves do not need any particular or specialized training.
Para 446 "Para 446. APPA/LPPC seek clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees. SDG&E seeks	FERC Order 706	The SDT clarifies the discretion in reviewing personnel risk assessments in CIP-004-5, Requirement R4, by establishing criteria for personnel risk assessments.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees. The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."		
Para 460 "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."	FERC Order 706	In CIP-004-5, Requirement R7, the SDT has addressed this directive by requiring revocation of access concurrent with the termination or disciplinary action (item 7.1) or by the end of the calendar day in cases of transfers or reassignments (item 7.2). In reviewing how to modify the requirement relating to transfers or reassignments, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement (item 7.2) from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers. CIP-004-5, Requirement R7 (item 7.4) augments the requirements in items 7.1 and 7.2 that respond to the directive. In order to meet the immediate timeframe, Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		access revocation on individual Cyber Assets and applications without affecting reliability. This requirement (item 7.4) provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
Para 464 We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification.	FERC Order 706	CIP-004-5, Requirement R5 (item 5.1), requires a personnel risk assessment as a condition of being granted access, with exceptions only for specific CIP Exceptional Circumstances which are outlined in the proposed glossary definition of the aforementioned term.
Para 473 The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entitys obligations regarding vendors with access to critical cyber assets.	FERC Order 706	CIP-002-5, Requirement R1 makes clear that asset owners are responsible for complying with the Standards.
Para 476 We direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent with the Commissions	FERC Order 706	Guidance in CIP-002-5 advises the owning Responsible Entities determine who is responsible for complying with the CIP Cyber Security Standards.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
determinations above.		
Para 496 "The Commission adopts the CIP NOPRs proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter"	FERC Order 706	The proposed requirement requires a Responsible Entity to deploy methods to inspect communications and detect potential malicious communications for all External Connectivity (Intrusion Detection). The drafting team addresses this in CIP-005-5, Requirement R1 (item 1.4). Per FERC Order 706, p 496-503, ESP's need two distinct security measures such that the cyber assets do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear this is not simple redundancy of firewalls, thus the drafting team has decided to add the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs.
Para 502 "The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process."	FERC Order 706	The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs as a second security measure for High Impact BES Cyber Systems.
Para 503 "The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures."	FERC Order 706	The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs as a second security measure for High Impact BES Cyber Systems.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 511 The Commission adopts the CIP NOPRs proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies.	FERC Order 706	CIP-005-5, Requirement R2 has additional security requirements for remote access from the work started in the Urgent Action Revisions to CIP-005-3. One of these requirements is two-factor authentication and specific examples of two-factor authentication are provided in the referenced guideline.
Paras 525, 526, 528, and 628 Para 525. "The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily…" Para 526. "the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments. The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs." Para 528. "The Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples every two weeks. CIP-007-5, Requirement R4, combines CIP-005-4, Requirement R5 and CIP-007-4, Requirement R6, and addresses FERC's directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor". The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the system. In addition, this requirement sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order 706 acknowledges this reality when directing a manual log review. As a result, this

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
or filtered logs." Para 628. "Requirement R6 of CIP-007-1 does not address the frequency with which log should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly…"		requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC Order 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings.
Paras 541, 542, and 547 Para 541. we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments." Para 542. "the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems." Para 547. "we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"	FERC Order 706	In CIP-010-1, Requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires annual paper assessments in the intervening years.
Para 544 "the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification." "we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability	FERC Order 706	The SDT addresses this paragraph in CIP-010-1, Requirement R3. • The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new Cyber Asset undergoes an active vulnerability assessment. • An exception is made for specified CIP Exceptional

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
assessment”		Circumstances. • Additionally, the new requirement in CIP-010, Requirement R1 (item 1.5) requires testing of all changes for High Impact BES Cyber Systems that deviate from the baseline configuration in a test environment to ensure that required security controls are not adversely affected.
Para 572 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."	FERC Order 706	The SDT addressed this in CIP-006-5, Requirement R1 (item 1.3) for High Impact BES Cyber Assets
Para 581 “The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years.”	FERC Order 706	The SDT addressed this in CIP-006-5, Requirement R3 (item 3.1) by changing the frequency to a 24 month testing cycle; after deliberation and consideration, the SDT determined that a requirement of more frequent testing (e.g., 12 months), was too often.
Paras 609, 610, and 611 Para 609. “We therefore direct the ERO to develop requirements addressing what constitutes a “representative system” and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.” Para 610. “we direct the ERO to revise the Reliability Standard to	FERC Order 706	CIP-010-1, Requirement R1 (item 1.4), provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. • The SDT proposes to require a “representative system” or test system for those High Impact Control Centers to use for the purposes of testing proposed

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above." Para 611. "the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."		changes and performing active vulnerability assessments. • The SDT proposes using the defined baseline configuration of a BES Cyber System for the measuring stick as to whether a test system is truly representative of the production system. • To account for any additional differences between the two systems, the SDT proposes using the words directly from FERC Order 706 "Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments."
Paras 620 and 622 Para 620. "The Commission will not adopt Consumers' recommendation that every system in an electronic security perimeter does not need antivirus software. Critical cyber assets must be protected, regardless of the operating system being used. Consumers has not provided convincing evidence that any specific operating system is not directly vulnerable to virus attacks. Virus technology changes every day. Therefore we believe it is in the public interest to protect all cyber assets within an electronic security perimeter, regardless of the operating system being used…"	FERC Order 706	The drafting team addressed this in CIP-007-5, Requirement R3. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 622. "The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above.		• The SDT rewrote the requirement as a competency based requirement that does not prescribe technology. • The SDT added Maintenance to cover malware on removable media. The drafting team also created a new requirement, CIP-007-5, Requirement R3 (item 3.4), to protect against personnel introducing malicious code when temporarily connecting to a BES Cyber Asset for Maintenance purposes. When remote access is used to connect to a BES Cyber Asset, an intermediate device is required in CIP-005-5, Requirement R2 (item 2.1) and guidance is further included for the cyber security policy in CIP-003-5, Requirement R2 to maintain up-to-date anti-malware software and patch levels before initiating interactive remote access.
Para 628. The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples every two weeks.
Paras 633 and 635	FERC Order 706	The SDT addresses these directives in CIP-011-1,

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 633. "The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it." Para 635. "the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."		Requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from media. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal.
Para 643 "The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."	FERC Order 706	In CIP-010-1, R3 (item 3.4), the SDT added a requirement for an entity planned date of completion to the remediation action plan following a vulnerability assessment. In order to provide more direction on what "features, functionality, and vulnerabilities" should be addressed in a vulnerability assessment, the SDT included guidance on active and paper vulnerability assessment. The SDT further referenced NIST SP800-115 to provide entities additional guidance on how to conduct a vulnerability assessment.
Para 661 "the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."	FERC Order 706	CIP-008-5 addresses the four parts of this directive as follows: 1. Added: Reportable Cyber Security Incidents include as a minimum any Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service. 2. Retired CIP-008-4, R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in the draft EOP-004-2, Requirement 1, Part 1.3.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		3. See 1 above 4. Guidance and measurements have been developed to be auditable and enforceable.
Para 673 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order 706	Cyber Security - Incident Reporting and Response Planning: Retired CIP-008-4, R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in the draft EOP-004-2, Requirement 1, Part 1.3
Para 676 "The Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order 706	Cyber Security - Incident Reporting and Response Planning: Retired CIP-008-4, R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in the draft EOP-004-2, Requirement 1, Part 1.3.
Para 686 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.."	FERC Order 706	In CIP-008-5, R3 (items 3.3 and 3.4), the SDT includes additional specification on the update of response plan and modifies the response plan requirements to incorporate lessons learned. Maintenance of documentation of paper drills, full operational drills, and responses to actual incidents is part of the documentation required to demonstrate compliance with the security controls in CIP-008-5 and is already subject to the evidence retention requirements associated with all

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		NERC Reliability Standards.
Para 694 “For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard”	FERC Order 706	The SDT added in CIP-009-5, R1, a requirement to implement the recovery plan
Para 706 "The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard."	FERC Order 706	CIP-009-5, R1 (item 1.5) requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service. The SDT captured the objective of this control, but did not explicitly use the term “forensics” due to the legal interpretations associated with the term.
Para 710 and 706 "Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report."	FERC Order 706	CIP-009-5, R1 (item 1.5) requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service.
Para 725 "The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years."	FERC Order 706	CIP-009-5, R2 (item 2.3) requires an operational exercise at least once every three calendar years.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 739 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."	FERC Order 706	In CIP-009-5, R1 (item 1.4), the SDT added requirements related to restoration processes based on review of the DHS Controls, and requires verification initially after backup to ensure that the process completed successfully. In CIP-009-5, R2 (item 2.2), the SDT requires an initial and once every calendar year test of the data at High Impact BES Cyber Systems or Medium Impact BES Cyber Systems at Control Centers.
Para 748 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."	FERC Order 706 NERC Alert regarding remote access VPN vulnerabilities	In CIP-009-5, R1 (item 1.4), the SDT added requirements related to restoration processes based on review of the DHS Catalog of Control Systems Security: Recommendations for Standards Developers (a derivation of NIST SP800-53 for Control Systems), and requires verification initially after backup to ensure that the process completed successfully. Addressed in CIP-005-5 ▪ Creates basic requirements to protect critical systems from untrusted networks. ▪ Identifies protective measures that provide secure access to critical systems. ▪ Helps ensure secure practices by employees, contractors, and service vendors to minimize exploitation of vulnerabilities. ▪ Addresses questions regarding ability to audit or

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		enforce the requirement through the design of clear measures. ▪ Significant guidance provided to address implementation options for organizations of differing sizes, capabilities, and complexity. Additionally, remote access is specifically required to be included in an entity's cyber security policy. Guidance is included to assist the entity in determining what this topic in the cyber security policy should address.
Para 13. "The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."	Order Approving Interpretation of Reliability Standard CIP-007-2 in Docket No. RD10-3-000, March 18, 2010	The SDT addressed this issue in CIP-007-5, R1, by having a requirement to disable or restrict use of physical I/O ports. The SDT changed the 'needed for normal or emergency operations' to those ports that are documented with reasons why they are necessary. In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Twelve Initial Ballot Windows Now Open for Ten Standards, Implementation Plan and Definitions: Friday, December 16 – Friday, January 6, 2012

Now Available

Twelve initial ballot windows, for the following ten CIP standards, the associated implementation plan, and a set of new and revised NERC Glossary definitions, are open through 8 p.m. Eastern on Friday, January 6, 2011.

- CIP-002-5 Cyber Security — BES Cyber Asset and BES Cyber System Categorization
- CIP-003-5 Cyber Security — Security Management Controls
- CIP-004-5 Cyber Security — Personnel and Training
- CIP-005-5 Cyber Security — Electronic Security Perimeter(s)
- CIP-006-5 Cyber Security — Physical Security of BES Cyber Systems
- CIP-007-5 Cyber Security — Systems Security Management
- CIP-008-5 Cyber Security — Incident Reporting and Response Planning
- CIP-009-5 Cyber Security — Recovery Plans for BES Cyber Assets and Systems
- CIP-010-1 Cyber Security — Configuration Management and Vulnerability Assessments
- CIP-011-1 Cyber Security — Information Protection

In addition, the following documents were previously posted to assist stakeholders in their review of the standards:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standards based on comments on CIP-010-1 and CIP-011-1 submitted during an informal comment period that ended June 3, 2010. (Note that the previously posted CIP-010-1 and CIP-011-1 are not the same standards as those posted for this comment/ballot period. The version of CIP-010 posted May 4 – June 3, 2010 addressed requirements associated with an earlier version of CIP-002, and the version of CIP-011 posted May 4 – June 3, 2010 was a single standard that contained all the requirements associated with earlier versions of CIP-003 through CIP-009.)
- Mapping Document – Identifies each requirement in the already-approved Version 4 CIP standards and identifies how the requirement has been treated in the Version 5 CIP standards (which includes CIP-002-5 through CIP-009-5 and CIP-010-1 and CIP-011-1).

- Clean versions of the approved versions of CIP-002-4 through CIP-009-4 – these are posted because the extent of the changes to each of the standards makes a redline of the posted draft standards against the approved standards impractical.
- Unofficial comment form in Word format – This is for informal use when compiling responses – the final must be submitted electronically.

Note that the Standards Committee has authorized an extended formal comment period (60 days), along with an extended ballot window (20 days), in consideration of the large number of standards and substantive changes to the format and content of the Version 5 CIP standards. In addition, the Standards Committee has authorized a deferral of the nonbinding polls to allow stakeholders an opportunity to focus more closely on the requirements, definitions, and implementation plan during this posting period. The nonbinding polls will take place in parallel with the next ballot of these standards.

Instructions for Balloting CIP V5 Standards, Implementation Plan, and Definitions

Each of the ten standards (ten ballots), the associated implementation plan (one ballot), and the set of definitions (one ballot) are being balloted individually to provide stakeholders an opportunity to cast separate ballots for each item. The individual ballots will provide the drafting team better feedback on which standards require additional development to achieve stakeholder consensus, as well as allow the team to gauge stakeholder support for the proposed implementation plan and definitions. Stakeholders are encouraged to consider each standard on its own merits and cast individual ballots, rather than casting the same ballot for all ten standards, in order to assist the drafting team with evaluating which standards require additional development to achieve consensus.

Members of the ballot pool associated with this project may log in and submit their votes for both the definition and the Detailed Information to Support an Exception Request from the following page: https://standards.nerc.net/CurrentBallots.aspx.

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Friday, January 6, 2012**. Please use this electronic form to submit comments. Please note that comments submitted during the formal comment period and the ballots for the standards all use the same electronic form, and it is NOT necessary for ballot pool members to submit more than one set of comments. The drafting team requests that all stakeholders (ballot pool members as well as other stakeholders) submit all comments through the electronic comment form.

In addition, in consideration of the volume of comments the drafting team anticipates, the drafting team requests that for groups of entities that develop a common set of comments, one member of the group submit the complete set of comments with other members simply submitting a brief statement that they support the comments submitted by [name/affiliation of the member of the group that

submits the complete set of comments]. This is the most efficient way to provide the drafting team with an indication of the volume of support for a set of comments.

If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Next Steps

The drafting team will consider all comments received and determine whether to make revisions to each of the standards, implementation plan, and definitions.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90 days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related directives in FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Ballot Pool Now Open: November 7 – December 15, 2011
Formal Comment Period Now Open: November 7, 2011 – January 6, 2012
Twelve Initial Ballot Windows Open for Ten Standards, Implementation Plan and Definitions: Friday, December 16 – Friday, January 6, 2012

Now Available

Ten CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1), a set of new and revised NERC Glossary definitions, and a proposed implementation plan have been posted for a formal 60-day comment period through Friday, January 6, 2012.

CIP-002-5 requires the categorization of these BES Cyber Systems according to bright-line criteria that characterize their impact on the Reliability Operations Services according to "bright-line" criteria contained in Attachment 1 – Impact Categorization of BES Cyber Assets and BES Cyber Systems of the draft CIP-002-5 standard.

CIP-003-5 through CIP-009-5, CIP-010-1 and CIP-011-1 in the draft Version 5 CIP Cyber Security Standards define the cyber security requirements to be applied to the BES Cyber Systems according to the categorization performed in CIP-002-5.

CIP-003 through CIP-009 generally follow the organization of Versions 1-4 of CIP-003 through CIP-009. CIP-010-1 is a new standard that contains the Configuration Management and Vulnerability Assessment requirements previously defined across several CIP standards in Versions 1 through 4. CIP-011-1 is a new standard that defines Information Protection and Media Sanitization requirements previously defined across many standards in Versions 1 through 4.

In addition, the following documents have been posted to assist stakeholders in their review:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standards based on comments on CIP-010-1 and CIP-011-1 submitted during an informal comment period that ended June 3, 2010. (Note that the previously posted CIP-010-1 and CIP-011-1 are not the same standards as those posted for this comment period. The version of CIP-010 posted May 4 – June 3, 2010 addressed requirements associated with an earlier version of CIP-002, and the version of CIP-011 posted May 4 – June 3, 2010 was a single

standard that contained all the requirements associated with earlier versions of CIP-003 through CIP-009.)

- Mapping Document - Identifies each requirement in the already-approved Version 4 CIP standards and identifies how the requirement has been treated in the Version 5 CIP standards (which includes CIP-002-5 through CIP-009-5 and CIP-010-1 and CIP-011-1).
- Clean versions of the approved versions of CIP-002-4 through CIP-009-4 - these are posted because the extent of the changes to each of the standards makes a redline of the posted draft standards against the approved standards impractical.
- Unofficial comment form in Word format – This is for informal use when compiling responses – the final must be submitted electronically.

Note that the Standards Committee has authorized an extended formal comment period (60 days), along with an extended ballot window (20 days), in consideration of the large number of standards and substantive changes to the format and content of the Version 5 CIP standards. In addition, the Standards Committee has authorized a deferral of the non-binding polls to allow stakeholders an opportunity to focus more closely on the requirements, definitions, and implementation plan during this posting period. The non-binding polls will take place in parallel with the next ballot of these standards.

Instructions for Joining Ballot Pool for Version 5 CIP Standards

A single ballot pool is being formed for the balloting of all ten standards, the implementation plan, and the definitions associated with the ten standards. The ballot pool that is formed will be cloned to create twelve separate ballot pools (one for each of the ten standards, one for the implementation plan, and one for the definitions). All members of the original ballot pool will automatically be eligible to vote in the twelve individual ballots.

The standards, implementation plan, and set of definitions are being balloted individually to provide stakeholders an opportunity to cast separate ballots for each item. The individual ballots will provide the drafting team better feedback on which standards require additional development to achieve stakeholder consensus, as well as allow the team to gauge stakeholder support for the proposed implementation plan and definitions. Stakeholders are encouraged to consider each standard on its own merits and cast individual ballots, rather than casting the same ballot for all ten standards, in order to assist the drafting team with evaluating which standards require additional development to achieve consensus.

To join the ballot pool to be eligible to vote in the upcoming ballots, as well as future ballots and non-binding polls for the Version 5 CIP standards, go to: Join Ballot Pool

During the pre-ballot windows, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited

from using the ballot pool list servers.) One ballot pool list server has been set up and can be used for communication on each of the standards being balloted for this project. The list server is: bp-2008-06_CIP-002-5_in@nerc.com

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Friday, January 6, 2012**. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Special Instructions for Submitting Comments

Please note that comments submitted during the formal comment period and the ballot for the standard both use the same electronic form, and it is NOT necessary for ballot pool members to submit more than one set of comments. The drafting team requests that all stakeholders (ballot pool members as well as other stakeholders) submit all comments through the electronic comment form.

Next Steps

The drafting team will host a series of three webinars – two on the substance of the standards, and a third to address process questions. The webinars on the substance of the standards, which have already been announced, will be held on November 15, 2011, and November 29, 2011. A separate announcement for the webinar that will address process questions will be sent with registration information as soon as details have been finalized.

Twelve initial ballots (one for each of the ten standards, one for the definitions, and one for the implementation plan associated with these standards) will be conducted beginning on Friday, December 16, 2011 through 8 p.m. Eastern on Friday, January 6, 2011.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90-days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related issues of FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Ballot Pool Now Open: November 7 – December 15, 2011
Formal Comment Period Now Open: November 7, 2011 – January 6, 2012
Twelve Initial Ballot Windows Open for Ten Standards, Implementation Plan and Definitions: Friday, December 16 – Friday, January 6, 2012

Now Available

Ten CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1), a set of new and revised NERC Glossary definitions, and a proposed implementation plan have been posted for a formal 60-day comment period through Friday, January 6, 2012.

CIP-002-5 requires the categorization of these BES Cyber Systems according to bright-line criteria that characterize their impact on the Reliability Operations Services according to "bright-line" criteria contained in Attachment 1 – Impact Categorization of BES Cyber Assets and BES Cyber Systems of the draft CIP-002-5 standard.

CIP-003-5 through CIP-009-5, CIP-010-1 and CIP-011-1 in the draft Version 5 CIP Cyber Security Standards define the cyber security requirements to be applied to the BES Cyber Systems according to the categorization performed in CIP-002-5.

CIP-003 through CIP-009 generally follow the organization of Versions 1-4 of CIP-003 through CIP-009. CIP-010-1 is a new standard that contains the Configuration Management and Vulnerability Assessment requirements previously defined across several CIP standards in Versions 1 through 4. CIP-011-1 is a new standard that defines Information Protection and Media Sanitization requirements previously defined across many standards in Versions 1 through 4.

In addition, the following documents have been posted to assist stakeholders in their review:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standards based on comments on CIP-010-1 and CIP-011-1 submitted during an informal comment period that ended June 3, 2010. (Note that the previously posted CIP-010-1 and CIP-011-1 are not the same standards as those posted for this comment period. The version of CIP-010 posted May 4 – June 3, 2010 addressed requirements associated with an earlier version of CIP-002, and the version of CIP-011 posted May 4 – June 3, 2010 was a single

standard that contained all the requirements associated with earlier versions of CIP-003 through CIP-009.)

- Mapping Document - Identifies each requirement in the already-approved Version 4 CIP standards and identifies how the requirement has been treated in the Version 5 CIP standards (which includes CIP-002-5 through CIP-009-5 and CIP-010-1 and CIP-011-1).
- Clean versions of the approved versions of CIP-002-4 through CIP-009-4 - these are posted because the extent of the changes to each of the standards makes a redline of the posted draft standards against the approved standards impractical.
- Unofficial comment form in Word format – This is for informal use when compiling responses – the final must be submitted electronically.

Note that the Standards Committee has authorized an extended formal comment period (60 days), along with an extended ballot window (20 days), in consideration of the large number of standards and substantive changes to the format and content of the Version 5 CIP standards. In addition, the Standards Committee has authorized a deferral of the non-binding polls to allow stakeholders an opportunity to focus more closely on the requirements, definitions, and implementation plan during this posting period. The non-binding polls will take place in parallel with the next ballot of these standards.

Instructions for Joining Ballot Pool for Version 5 CIP Standards

A single ballot pool is being formed for the balloting of all ten standards, the implementation plan, and the definitions associated with the ten standards. The ballot pool that is formed will be cloned to create twelve separate ballot pools (one for each of the ten standards, one for the implementation plan, and one for the definitions). All members of the original ballot pool will automatically be eligible to vote in the twelve individual ballots.

The standards, implementation plan, and set of definitions are being balloted individually to provide stakeholders an opportunity to cast separate ballots for each item. The individual ballots will provide the drafting team better feedback on which standards require additional development to achieve stakeholder consensus, as well as allow the team to gauge stakeholder support for the proposed implementation plan and definitions. Stakeholders are encouraged to consider each standard on its own merits and cast individual ballots, rather than casting the same ballot for all ten standards, in order to assist the drafting team with evaluating which standards require additional development to achieve consensus.

To join the ballot pool to be eligible to vote in the upcoming ballots, as well as future ballots and non-binding polls for the Version 5 CIP standards, go to: Join Ballot Pool

During the pre-ballot windows, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited

from using the ballot pool list servers.) One ballot pool list server has been set up and can be used for communication on each of the standards being balloted for this project. The list server is: bp-2008-06_CIP-002-5_in@nerc.com

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Friday, January 6, 2012**. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Special Instructions for Submitting Comments

Please note that comments submitted during the formal comment period and the ballot for the standard both use the same electronic form, and it is NOT necessary for ballot pool members to submit more than one set of comments. The drafting team requests that all stakeholders (ballot pool members as well as other stakeholders) submit all comments through the electronic comment form.

Next Steps

The drafting team will host a series of three webinars – two on the substance of the standards, and a third to address process questions. The webinars on the substance of the standards, which have already been announced, will be held on November 15, 2011, and November 29, 2011. A separate announcement for the webinar that will address process questions will be sent with registration information as soon as details have been finalized.

Twelve initial ballots (one for each of the ten standards, one for the definitions, and one for the implementation plan associated with these standards) will be conducted beginning on Friday, December 16, 2011 through 8 p.m. Eastern on Friday, January 6, 2011.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90-days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related issues of FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 (CIP Version 5)

Initial Ballot Results

Now Available

Twelve initial ballot windows for the following ten CIP standards, one ballot for the associated implementation plan, and one ballot for a set of new and revised NERC Glossary definitions, closed on Friday, January 6, 2011. The drafting team thanks stakeholders for the careful consideration of such a large volume of documents, and for the substantive and constructive feedback received.

Voting statistics for each ballot are listed below, and the Ballot Results webpage provides a link to the detailed results.

Ballot	Results
CIP-002-5 Cyber Security — BES Cyber System Identification	Quorum: 93.62% Approval: 22.09%
CIP-003-5 Cyber Security — Security Management Controls	Quorum: 93.62% Approval: 33.49%
CIP-004-5 Cyber Security — Personnel and Training	Quorum: 93.62% Approval: 26.82%
CIP-005-5 Cyber Security — Electronic Security Perimeter(s)	Quorum: 93.62% Approval: 28.04%
CIP-006-5 Cyber Security — Physical Security	Quorum: 93.61% Approval: 29.60%
CIP-007-5 Cyber Security — Systems Security Management	Quorum: 93.61% Approval: 24.15%
CIP-008-5 Cyber Security — Incident Reporting and Response Planning	Quorum: 94.02% Approval: 34.30%
CIP-009-5 Cyber Security — Recovery Plans for BES Cyber Assets and Systems	Quorum: 93.61% Approval: 27.28%
CIP-010-1 Cyber Security — Configuration Change Management	Quorum: 93.61% Approval: 26.61%
CIP-011-1 Cyber Security — Information Protection	Quorum: 93.61% Approval: 29.88%
CIP V5 Implementation Plan	Quorum: 92.15% Approval: 42.06%

Ballot	Results
CIP V5 Definitions	Quorum: 92.56% Approval: 25.34%

Next Steps

The drafting team will consider all comments and determine what changes to make to each of the standards, the implementation plan, and the definitions. After the drafting team has revised the standards, they will be submitted, along with the team's Consideration of Comments, for quality review and subsequently posted for a successive ballot.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90 days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related issues of FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed. Additional information about the project is available on the project webpage.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Ballot Results

Ballot Name:	Project 2008-06 CIP-002-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	455
Total Ballot Pool:	486
Quorum:	**93.62 % The Quorum has been reached**
Weighted Segment Vote:	22.09 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	19	0.174	90	0.826	10	6
2 - Segment 2.	11	0.9	2	0.2	7	0.7	0	2
3 - Segment 3.	120	1	19	0.174	90	0.826	5	6
4 - Segment 4.	38	1	4	0.118	30	0.882	2	2
5 - Segment 5.	103	1	14	0.163	72	0.837	5	12
6 - Segment 6.	60	1	11	0.204	43	0.796	3	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	11	1	3	0.3	7	0.7	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	3	0.3	4	0.4	2	0
Totals	**486**	**8.3**	**77**	**1.833**	**348**	**6.467**	**30**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	View
1	ATCO Electric	Glen Sutton	Abstain	View
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Negative	View
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Negative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Negative	View
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Negative	View
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	View
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	View
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Negative	View
1	KAMO Electric Cooperative	Walter Kenyon	Negative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Negative	View
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Negative	View
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	View
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Negative	View
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Negative	View
1	Sierra Pacific Power Co.	Rich Salgo	Negative	View
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Negative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Negative	View
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Negative	View
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Negative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Negative	View
3	City of Redding	Bill Hughes	Negative	View
3	City Water, Light & Power of Springfield	Roger Powers	Negative	View
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Negative	View
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Negative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	View
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	View
3	Madison Gas and Electric Co.	Darl Shimko	Negative	View

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	View
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Negative	View
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Negative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	View
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	View
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Negative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Negative	View
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Negative	View
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	View
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Negative	View
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Negative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	View
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Negative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Negative	View
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Negative	View
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	View
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Negative	View
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Negative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Negative	View
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Negative	View
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Negative	View
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	View
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Negative	View
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Negative	View
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	View
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Negative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Negative	View
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	View
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Negative	View
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Negative	View
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	View
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		James A Maenner	Abstain	
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Negative	View
8	INTELLIBIND	Kevin Conway	Affirmative	

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Pacific Northwest Generating Cooperative	Margaret Ryan	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	View
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Ballot Results

Ballot Name:	Project 2008-06 CIP-003-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	455
Total Ballot Pool:	486
Quorum:	**93.62 % The Quorum has been reached**
Weighted Segment Vote:	33.49 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	36	0.333	72	0.667	11	6
2 - Segment 2.	11	0.8	2	0.2	6	0.6	1	2
3 - Segment 3.	120	1	38	0.352	70	0.648	6	6
4 - Segment 4.	38	1	10	0.303	23	0.697	3	2
5 - Segment 5.	103	1	28	0.337	55	0.663	8	12
6 - Segment 6.	60	1	17	0.321	36	0.679	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	11	1	4	0.4	6	0.6	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	3	0.3	4	0.4	2	0
Totals	**486**	**8.2**	**140**	**2.746**	**277**	**5.454**	**38**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Negative	View
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	View
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Affirmative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Negative	View
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Affirmative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Affirmative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Affirmative	View
4	Detroit Edison Company	Daniel Herring	Affirmative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	View
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Affirmative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	View
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	View
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		James A Maenner	Abstain	
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway	Affirmative	

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Pacific Northwest Generating Cooperative	Margaret Ryan	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Ballot Results

Ballot Name:	Project 2008-06 CIP-004-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	453
Total Ballot Pool:	484
Quorum:	**93.60 % The Quorum has been reached**
Weighted Segment Vote:	26.82 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	29	0.269	79	0.731	11	6
2 - Segment 2.	10	0.7	1	0.1	6	0.6	1	2
3 - Segment 3.	120	1	30	0.278	78	0.722	6	6
4 - Segment 4.	38	1	7	0.212	26	0.788	3	2
5 - Segment 5.	103	1	20	0.241	63	0.759	8	12
6 - Segment 6.	60	1	13	0.245	40	0.755	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	3	0.3	6	0.6	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	3	0.3	4	0.4	2	0
Totals	**484**	**8**	**108**	**2.145**	**307**	**5.855**	**38**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Negative	View
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Negative	View
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Negative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Negative	View
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Negative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View
3	Alabama Power Company	Richard J. Mandes	Negative	View

3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Negative	View
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	View
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Negative	View
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	
3	Manitoba Hydro	Greg C. Parent	Negative	View

3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Negative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	View
3	Turlock Irrigation District	John Souza	Negative	View
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View
4	Flathead Electric Cooperative	Russ Schneider	Negative	

4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	View
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Michael Korchynsky	Negative	View

5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Negative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	View
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Negative	View

6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Negative	View
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Negative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	View
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Negative	View
8	INTELLIBIND	Kevin Conway	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	

8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Ballot Results

Ballot Name:	Project 2008-06 CIP-005-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	453
Total Ballot Pool:	484
Quorum:	**93.60 % The Quorum has been reached**
Weighted Segment Vote:	28.04 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	30	0.286	75	0.714	14	6
2 - Segment 2.	10	0.7	1	0.1	6	0.6	1	2
3 - Segment 3.	120	1	35	0.327	72	0.673	7	6
4 - Segment 4.	38	1	6	0.182	27	0.818	3	2
5 - Segment 5.	103	1	22	0.265	61	0.735	8	12
6 - Segment 6.	60	1	15	0.283	38	0.717	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	3	0.3	6	0.6	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	3	0.3	4	0.4	2	0
Totals	**484**	**8**	**117**	**2.243**	**294**	**5.757**	**42**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	View
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Negative	View
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	View
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Negative	View
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Abstain	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Affirmative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Abstain	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Abstain	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View
3	Alabama Power Company	Richard J. Mandes	Negative	View

3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Negative	View
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	
3	Manitoba Hydro	Greg C. Parent	Negative	View

3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Abstain	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Affirmative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View
4	Flathead Electric Cooperative	Russ Schneider	Negative	

4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Negative	View
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Negative	View
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Michael Korchynsky	Negative	View

5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	View
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Negative	View

6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Negative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		James A Maenner	Abstain	
8		Roger C Zaklukiewicz	Negative	
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Negative	View
8	INTELLIBIND	Kevin Conway	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	

8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 CIP-006-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	454
Total Ballot Pool:	485
Quorum:	**93.61 % The Quorum has been reached**
Weighted Segment Vote:	29.60 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	33	0.306	75	0.694	11	6
2 - Segment 2.	11	0.8	1	0.1	7	0.7	1	2
3 - Segment 3.	120	1	33	0.306	75	0.694	6	6
4 - Segment 4.	38	1	7	0.212	26	0.788	3	2
5 - Segment 5.	103	1	19	0.229	64	0.771	8	12
6 - Segment 6.	60	1	13	0.245	40	0.755	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	4	0.4	5	0.5	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	4	0.4	3	0.3	2	0
Totals	**485**	**8.1**	**116**	**2.398**	**300**	**5.702**	**38**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Negative	View
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Negative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Affirmative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Negative	View
3	Clearwater Power Co.	Dave Hagen	Negative	
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	View
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Affirmative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	View
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Negative	View
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Negative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	View
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	View
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Negative	View
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Negative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	View
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		Edward C Stein	Affirmative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway	Affirmative	

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Ballot Results

Ballot Name:	Project 2008-06 CIP-007-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	454
Total Ballot Pool:	485
Quorum:	**93.61 % The Quorum has been reached**
Weighted Segment Vote:	24.15 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	26	0.245	80	0.755	13	6
2 - Segment 2.	11	0.8	1	0.1	7	0.7	1	2
3 - Segment 3.	120	1	28	0.259	80	0.741	6	6
4 - Segment 4.	38	1	5	0.156	27	0.844	4	2
5 - Segment 5.	103	1	17	0.207	65	0.793	9	12
6 - Segment 6.	60	1	10	0.189	43	0.811	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	3	0.3	6	0.6	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	3	0.3	4	0.4	2	0
Totals	**485**	**8.1**	**95**	**1.956**	**317**	**6.144**	**42**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Negative	View
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Abstain	
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	View
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Negative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Negative	View
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Abstain	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Negative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Negative	View
3	City Water, Light & Power of Springfield	Roger Powers	Negative	View
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	View
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Negative	View
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	View
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Negative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	View
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Negative	View
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Abstain	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	View
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Negative	View
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	View
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	View
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Negative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Abstain	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	View
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Negative	View
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Negative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Negative	View
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Negative	View
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	View
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	
6	Los Angeles Department of Water & Power	Brad Packer	Negative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Negative	View
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	View
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		James A Maenner	Abstain	
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Negative	View
8	INTELLIBIND	Kevin Conway	Affirmative	

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Ballot Results

Ballot Name:	Project 2008-06 CIP-008-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	456
Total Ballot Pool:	485
Quorum:	**94.02 % The Quorum has been reached**
Weighted Segment Vote:	34.30 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	34	0.318	73	0.682	12	6
2 - Segment 2.	11	0.8	2	0.2	6	0.6	1	2
3 - Segment 3.	120	1	36	0.33	73	0.67	6	5
4 - Segment 4.	38	1	7	0.212	26	0.788	4	1
5 - Segment 5.	103	1	26	0.317	56	0.683	9	12
6 - Segment 6.	60	1	16	0.302	37	0.698	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	4	0.4	5	0.5	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	5	0.5	2	0.2	2	0
Totals	**485**	**8.1**	**132**	**2.779**	**283**	**5.321**	**41**	**29**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Abstain	
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Negative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Negative	View
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Affirmative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Negative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Negative	View
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Affirmative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	View
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Affirmative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Negative	View
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Abstain	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Negative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Negative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Abstain	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	View
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Negative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Negative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Edward C Stein	Affirmative	
8		James A Maenner	Abstain	
8		Roger C Zaklukiewicz	Negative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway	Affirmative	

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
GO
Advanced Search

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 CIP-009-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	454
Total Ballot Pool:	485
Quorum:	**93.61 % The Quorum has been reached**
Weighted Segment Vote:	27.28 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	31	0.29	76	0.71	12	6
2 - Segment 2.	11	0.8	0	0	8	0.8	1	2
3 - Segment 3.	120	1	33	0.306	75	0.694	6	6
4 - Segment 4.	38	1	4	0.129	27	0.871	5	2
5 - Segment 5.	103	1	21	0.259	60	0.741	10	12
6 - Segment 6.	60	1	12	0.226	41	0.774	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	4	0.4	5	0.5	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	4	0.4	3	0.3	2	0
Totals	**485**	**8.1**	**111**	**2.21**	**300**	**5.89**	**43**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Negative	View
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Abstain	
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Negative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Negative	View
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Affirmative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Negative	View
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Negative	View
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Negative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	View
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Affirmative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	View
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Negative	View
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Abstain	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	View
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Negative	View
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Negative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Negative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Abstain	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	View
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Negative	View
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Negative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Negative	View
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Negative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	View
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Negative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Negative	View
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		Edward C Stein	Affirmative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway	Affirmative	

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
GO
Advanced Search

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 CIP-010-5_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	454
Total Ballot Pool:	485
Quorum:	**93.61 % The Quorum has been reached**
Weighted Segment Vote:	26.61 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	30	0.28	77	0.72	12	6
2 - Segment 2.	11	0.8	1	0.1	7	0.7	1	2
3 - Segment 3.	120	1	33	0.306	75	0.694	6	6
4 - Segment 4.	38	1	5	0.156	27	0.844	4	2
5 - Segment 5.	103	1	22	0.268	60	0.732	9	12
6 - Segment 6.	60	1	13	0.245	40	0.755	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	3	0.3	6	0.6	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	3	0.3	4	0.4	2	0
Totals	**485**	**8.1**	**112**	**2.155**	**301**	**5.945**	**41**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Abstain	
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Negative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	View
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Negative	View
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Negative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Negative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Negative	View
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Negative	View
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Negative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Negative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Negative	View
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Negative	View
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Negative	View
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Negative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	View
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Negative	View
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	View
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Negative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Negative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		James A Maenner	Abstain	
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8	APX	Michael Johnson	Negative	View
8	INTELLIBIND	Kevin Conway	Affirmative	

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	View
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	View
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
GO
Advanced Search

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 CIP-011-1_CSO706 Version 5 CIP Standards_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	454
Total Ballot Pool:	485
Quorum:	**93.61 % The Quorum has been reached**
Weighted Segment Vote:	29.88 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	34	0.318	73	0.682	12	6
2 - Segment 2.	11	0.8	1	0.1	7	0.7	1	2
3 - Segment 3.	120	1	36	0.333	72	0.667	6	6
4 - Segment 4.	38	1	6	0.188	26	0.813	4	2
5 - Segment 5.	103	1	23	0.28	59	0.72	9	12
6 - Segment 6.	60	1	16	0.302	37	0.698	4	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.9	3	0.3	6	0.6	1	0
9 - Segment 9.	9	0.7	2	0.2	5	0.5	2	0
10 - Segment 10.	9	0.7	4	0.4	3	0.3	2	0
Totals	**485**	**8.1**	**125**	**2.421**	**288**	**5.68**	**41**	**31**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Negative	View
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Negative	View
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Abstain	
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	View
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Affirmative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	View
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View

3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster	Negative	View
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	View
3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Negative	View
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Negative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Affirmative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Negative	View
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	View
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	View
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Negative	View
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Affirmative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Negative	View
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Negative	View
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	View
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Negative	View
6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle	Negative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		Edward C Stein	Affirmative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway	Negative	View

8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Negative	View
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Ballot Results

Ballot Name:	CIP V5 Implementation Project 2008-06 Dec 2011_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	446
Total Ballot Pool:	484
Quorum:	**92.15 % The Quorum has been reached**
Weighted Segment Vote:	42.06 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	30	0.297	71	0.703	16	8
2 - Segment 2.	10	0.6	3	0.3	3	0.3	1	3
3 - Segment 3.	120	1	40	0.388	63	0.612	8	9
4 - Segment 4.	38	1	14	0.438	18	0.563	4	2
5 - Segment 5.	103	1	25	0.321	53	0.679	12	13
6 - Segment 6.	60	1	17	0.327	35	0.673	5	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.7	4	0.4	3	0.3	3	0
9 - Segment 9.	9	0.6	3	0.3	3	0.3	3	0
10 - Segment 10.	9	0.4	3	0.3	1	0.1	5	0
Totals	**484**	**7.3**	**139**	**3.071**	**250**	**4.23**	**57**	**38**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Electric Power Cooperative	Michael B Bax	Negative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Affirmative	
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Abstain	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Negative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Negative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier		
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Negative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	View
1	M & A Electric Power Cooperative	William Price	Negative	View
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	
1	Northeast Utilities	David Boguslawski	Abstain	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Negative	View
1	Sierra Pacific Power Co.	Rich Salgo	Abstain	
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Negative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum		
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Abstain	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Affirmative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe		
2	Southwest Power Pool, Inc.	Charles Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	View
3	Alabama Power Company	Richard J. Mandes	Negative	View

3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	View
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Negative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Garland	Ronnie C Hoeinghaus	Affirmative	
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Negative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Affirmative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster		
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	View
3	Kansas City Power & Light Co.	Charles Locke	Negative	
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	View
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	View
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	
3	Manitoba Hydro	Greg C. Parent	Negative	View

3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Affirmative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Negative	
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	View
3	Rutherford EMC	Thomas M Haire	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	View
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Negative	View
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	View
3	Turlock Irrigation District	John Souza	Negative	View
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View
4	Flathead Electric Cooperative	Russ Schneider	Abstain	

4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Negative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Negative	View
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Negative	View
5	Dynegy Inc.	Dan Roethemeyer	Negative	View
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Michael Korchynsky	Negative	View

5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Abstain	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Abstain	
5	Tri-State G & T Association, Inc.	Barry Ingold	Negative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Abstain	View
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn		
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Negative	View

6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Negative	
6	Black Hills Power	andrew heinle	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	View
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Negative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	
6	Duke Energy Carolina	Walter Yeager	Negative	View
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	View
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Abstain	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	View
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		Edward C Stein	Affirmative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	

8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Abstain	
8	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Affirmative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Abstain	
10	Southwest Power Pool RE	Emily Pennel	Affirmative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Ballot Results

Ballot Name:	CIP V5 Definitions Project 2008-06 Dec 2011_in
Ballot Period:	12/16/2011 - 1/6/2012
Ballot Type:	Initial
Total # Votes:	448
Total Ballot Pool:	484
Quorum:	**92.56 % The Quorum has been reached**
Weighted Segment Vote:	25.34 %
Ballot Results:	**The standard will proceed to a successive ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	23	0.217	83	0.783	12	7
2 - Segment 2.	10	0.6	1	0.1	5	0.5	1	3
3 - Segment 3.	120	1	22	0.212	82	0.788	7	9
4 - Segment 4.	38	1	6	0.176	28	0.824	3	1
5 - Segment 5.	103	1	18	0.222	63	0.778	9	13
6 - Segment 6.	60	1	13	0.25	39	0.75	5	3
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	1	4	0.4	6	0.6	0	0
9 - Segment 9.	9	0.6	2	0.2	4	0.4	3	0
10 - Segment 10.	9	0.6	2	0.2	4	0.4	3	0
Totals	**484**	**7.8**	**91**	**1.977**	**314**	**5.823**	**43**	**36**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	View
1	Arizona Public Service Co.	Robert Smith	Negative	
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	View
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	View

1	Balancing Authority of Northern California	Kevin Smith	Negative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	View
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Negative	View
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs	Negative	View
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	View
1	City Water, Light & Power of Springfield	Shaun Anders	Negative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Negative	
1	Deseret Power	James Tucker	Negative	View
1	Dominion Virginia Power	Michael S Crowley	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Negative	View
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	View
1	Entergy Services, Inc.	Edward J Davis	Affirmative	View
1	FirstEnergy Corp.	William J Smith	Negative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	View
1	Gainesville Regional Utilities	Luther E. Fair	Abstain	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	View
1	JEA	Ted Hobson	Affirmative	View
1	KAMO Electric Cooperative	Walter Kenyon	Negative	View
1	Kansas City Power & Light Co.	Michael Gammon	Negative	View
1	Keys Energy Services	Stanley T Rzad		
1	Lakeland Electric	Larry E Watt		
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Negative	View
1	M & A Electric Power Cooperative	William Price	Negative	View
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	View
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	Muscatine Power & Water	Tim Reed	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	View
1	National Grid	Saurabh Saksena	Negative	View
1	Nebraska Public Power District	Cole C Brodine	Negative	View
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	View
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	
1	Northeast Utilities	David Boguslawski	Abstain	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	View
1	NorthWestern Energy	John Canavan	Negative	View
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	View
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Negative	View
1	Platte River Power Authority	John C. Collins	Negative	View
1	Portland General Electric Co.	John T Walker	Negative	View
1	Potomac Electric Power Co.	David Thorne	Abstain	View
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Brett A Koelsch	Negative	View
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey	Affirmative	
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	View
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	View
1	Sacramento Municipal Utility District	Tim Kelley	Negative	
1	Salmon River Electric Cooperative	Kathryn Spence	Negative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.	Negative	
1	Seattle City Light	Pawel Krupa	Negative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Negative	View
1	Sierra Pacific Power Co.	Rich Salgo	Negative	View
1	Snohomish County PUD No. 1	Long T Duong	Negative	View
1	South California Edison Company	Steven Mavis	Negative	View
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert Schaffeld	Negative	View
1	Southern Illinois Power Coop.	William Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	View
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	View
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	View
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Negative	View
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	
1	Tucson Electric Power Co.	John Tolo	Negative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Negative	View
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota		
2	California ISO	Rich Vine	Negative	View
2	Electric Reliability Council of Texas, Inc.	Charles B Manning		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Negative	View
2	New Brunswick System Operator	Alden Briggs	Negative	View
2	New York Independent System Operator	Gregory Campoli	Negative	View
2	PJM Interconnection, L.L.C.	Tom Bowe		
2	Southwest Power Pool, Inc.	Charles Yeung	Negative	View
3	AEP	Michael E Deloach	Negative	View
3	Alabama Power Company	Richard J. Mandes	Negative	View

3	Alameda Municipal Power	Douglas Draeger	Negative	View
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Affirmative	
3	APS	Steven Norris	Negative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	View
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	View
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Negative	
3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Alexandria	Michael Marcotte	Negative	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Negative	View
3	City of Garland	Ronnie C Hoeinghaus	Negative	View
3	City of Green Cove Springs	Gregg R Griffin		
3	City of Lodi, California	Elizabeth Kirkley	Negative	View
3	City of McMinnville	John C Dietz	Affirmative	
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Negative	View
3	City Water, Light & Power of Springfield	Roger Powers	Negative	View
3	Clearwater Power Co.	Dave Hagen	Negative	View
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	View
3	ComEd	Bruce Krawczyk	Negative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	View
3	Consumers Energy	Richard Blumenstock	Negative	View
3	Consumers Power Inc.	Roman Gillen	Negative	View
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	View
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	View
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	View
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	View
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	View
3	Florida Power Corporation	Lee Schuster		
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	View
3	Grays Harbor PUD	Wesley W Gray	Affirmative	
3	Great River Energy	Brian Glover	Negative	View
3	Gulf Power Company	Paul C Caldwell	Negative	View
3	Hydro One Networks, Inc.	David Kiguel	Negative	View
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	View
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	View
3	Kansas City Power & Light Co.	Charles Locke	Negative	View
3	Kissimmee Utility Authority	Gregory D Woessner		
3	Lakeland Electric	Norman D Harryhill	Negative	View
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	View
3	Lincoln Electric System	Jason Fortik	Negative	View
3	Los Angeles Department of Water & Power	Daniel D Kurowski		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	View
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	
3	Manitoba Hydro	Greg C. Parent	Negative	View

3	Manitowoc Public Utilities	Thomas E Reed	Negative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	View
3	Mississippi Power	Jeff Franklin	Negative	View
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	View
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	View
3	Northern Lights Inc.	Jon Shelby	Negative	View
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Abstain	
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	View
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Negative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	View
3	Pacific Gas and Electric Company	John H Hagen	Negative	View
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Negative	View
3	Platte River Power Authority	Terry L Baker	Affirmative	View
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	View
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 1 of Benton County	Gloria Bender		
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson	Negative	View
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	View
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	View
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young		
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher	Negative	View
3	Tacoma Public Utilities	Travis Metcalfe	Negative	View
3	Tampa Electric Co.	Ronald L Donahey	Negative	View
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	View
3	Turlock Irrigation District	John Souza	Negative	View
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	View
3	Westar Energy	Bo Jones	Negative	View
3	Wisconsin Electric Power Marketing	James R Keller	Negative	View
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	View
4	Blue Ridge Power Agency	Duane S Dahlquist	Abstain	
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Negative	View
4	City Utilities of Springfield, Missouri	John Allen	Negative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Negative	View
4	Flathead Electric Cooperative	Russ Schneider	Negative	View

4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	View
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	View
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Negative	View
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	View
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	
4	Seattle City Light	Hao Li	Negative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	View
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	WPPI Energy	Patrick Connors	Negative	View
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	AES Corporation	Leo Bernier	Negative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Negative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Negative	View
5	Avista Corp.	Edward F. Groce	Negative	View
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas		
5	Caithness Long Island, LLC	Jason M Moore	Negative	
5	Chelan County Public Utility District #1	John Yale		
5	City and County of San Francisco	Daniel Mason	Negative	View
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Negative	View
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	View
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	View
5	Consumers Energy Company	David C Greyerbiehl	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View
5	Duke Energy	Dale Q Goodwine	Negative	View
5	Dynegy Inc.	Dan Roethemeyer	Abstain	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Michael Korchynsky	Negative	View

5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Negative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Preston L Walsh	Negative	View
5	Green Country Energy	Greg Froehling	Affirmative	
5	Imperial Irrigation District	Marcela Y Caballero		
5	JEA	John J Babik	Affirmative	View
5	Kansas City Power & Light Co.	Brett Holland	Negative	View
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Negative	View
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Los Angeles Department of Water & Power	Kenneth Silver	Abstain	
5	Lower Colorado River Authority	Tom Foreman	Negative	View
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	View
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	View
5	Muscatine Power & Water	Mike Avesing	Negative	View
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	View
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	View
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle R DAntuono	Negative	View
5	Omaha Public Power District	Mahmood Z. Safi	Negative	View
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Negative	View
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Negative	View
5	Portland General Electric Co.	Gary L Tingley	Negative	View
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	View
5	PSEG Fossil LLC	Tim Kucey	Negative	View
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	View
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Negative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	View
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	View
5	Southern Company Generation	William D Shultz	Negative	View
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	View
5	Trans Canada Power	John Fish	Abstain	
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Negative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	View
5	Westar Energy	Bryan Taggart	Negative	
5	Wisconsin Electric Power Co.	Linda Horn		
5	WPPI Energy	Steven Leovy	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Negative	View

6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Negative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Negative	
6	Black Hills Power	andrew heinle	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	View
6	City of Redding	Marvin Briggs	Negative	View
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	View
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Negative	View
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Negative	View
6	FirstEnergy Solutions	Kevin Querry	Negative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	View
6	Lakeland Electric	Paul Shipps	Negative	View
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Los Angeles Department of Water & Power	Brad Packer	Abstain	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull	Negative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan Johnson	Abstain	
6	Omaha Public Power District	David Ried	Negative	View
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Negative	View
6	Portland General Electric Co.	John Jamieson	Negative	View
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	View
6	Progress Energy	John T Sturgeon	Negative	View
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Negative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	View
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	View
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Negative	
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	View
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	View
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		Edward C Stein	Affirmative	
8		James A Maenner	Affirmative	
8	APX	Michael Johnson	Negative	View
8	INTELLIBIND	Kevin Conway	Affirmative	
8	JDRJC Associates	Jim Cyrulewski	Affirmative	

8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	Power Energy Group LLC	Peggy Abbadini	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	View
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	View
9	California Energy Commission	William M Chamberlain	Abstain	
9	Central Lincoln PUD	Bruce Lovelin	Negative	View
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Negative	View
9	Maine Public Utilities Commission	Michael Simmons	Abstain	
9	National Association of Regulatory Utility Commissioners	Diane J Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky	Negative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain	
10	Midwest Reliability Organization	James D Burley	Negative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Negative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Abstain	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	View
10	Texas Reliability Entity, Inc.	Donald G Jones	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Individual or group. (131 Responses)
Name (86 Responses)
Organization (86 Responses)
Group Name (45 Responses)
Lead Contact (45 Responses)
Question 1 (119 Responses)
Question 1 Comments (131 Responses)
Question 2 (123 Responses)
Question 2 Comments (131 Responses)
Question 3 (120 Responses)
Question 3 Comments (131 Responses)
Question 4 (110 Responses)
Question 4 Comments (131 Responses)
Question 5 (93 Responses)
Question 5 Comments (131 Responses)
Question 6 (110 Responses)
Question 6 Comments (131 Responses)
Question 7 (114 Responses)
Question 7 Comments (131 Responses)
Question 8 (111 Responses)
Question 8 Comments (131 Responses)
Question 9 (114 Responses)
Question 9 Comments (131 Responses)
Question 10 (113 Responses)
Question 10 Comments (131 Responses)
Question 11 (115 Responses)
Question 11 Comments (131 Responses)
Question 12 (92 Responses)
Question 12 Comments (131 Responses)
Question 13 (115 Responses)
Question 12 Comments (131 Responses)
Question 14 (112 Responses)
Question 14 Comments (131 Responses)
Question 15 (110 Responses)
Question 15 Comments (131 Responses)
Question 16 (112 Responses)
Question 16 Comments (131 Responses)
Question 17 (109 Responses)
Question 17 Comments (131 Responses)
Question 18 (114 Responses)
Question 18 Comments (131 Responses)
Question 19 (120 Responses)
Question 19 Comments (131 Responses)
Question 20 (92 Responses)
Question 20 Comments (131 Responses)
Question 21 (109 Responses)
Question 21 Comments (131 Responses)
Question 22 (104 Responses)
Question 22 Comments (131 Responses)
Question 23 (84 Responses)
Question 23 Comments (131 Responses)
Question 24 (119 Responses)
Question 24 Comments (131 Responses)
Question 25 (105 Responses)
Question 25 Comments (131 Responses)
Question 26 (108 Responses)
Question 26 Comments (131 Responses)
Question 27 (90 Responses)

Question 27 Comments (131 Responses)
Question 28 (108 Responses)
Question 28 Comments (131 Responses)
Question 29 (110 Responses)
Question 29 Comments (131 Responses)
Question 30 (107 Responses)
Question 30 Comments (131 Responses)
Question 31 (109 Responses)
Question 31 Comments (131 Responses)
Question 32 (114 Responses)
Question 32 Comments (131 Responses)
Question 33 (89 Responses)
Question 33 Comments (131 Responses)
Question 34 (109 Responses)
Question 34 Comments (131 Responses)
Question 35 (110 Responses)
Question 35 Comments (131 Responses)
Question 36 (111 Responses)
Question 36 Comments (131 Responses)
Question 37 (88 Responses)
Question 37 Comments (131 Responses)
Question 38 (108 Responses)
Question 38 Comments (131 Responses)
Question 39 (108 Responses)
Question 39 Comments (131 Responses)
Question 40 (109 Responses)
Question 40 Comments (131 Responses)
Question 41 (86 Responses)
Question 41 Comments (131 Responses)
Question 42 (111 Responses)
Question 42 Comments (131 Responses)
Question 43 (101 Responses)
Question 43 Comments (131 Responses)
Question 44 (112 Responses)
Question 44 Comments (131 Responses)
Question 45 (86 Responses)
Question 45 Comments (131 Responses)
Question 46 (106 Responses)
Question 46 Comments (131 Responses)
Question 47 (101 Responses)
Question 47 Comments (131 Responses)
Question 48 (85 Responses)
Question 48 Comments (131 Responses)
Question 49 (104 Responses)
Question 49 Comments (131 Responses)

Individual
Doug Peterchuck
Omaha Public Power District
Yes
Definition Concerns: 1. BES Cyber Asset: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. Please define or clarify the term “adversely”. Requesting clarification or suggest just using impact. Term “adversely” is subject to interpretation. 2. BES Cyber Security Incident: The term “suspicious” is open to interpretation and very vague. Suggest rewording to “intentional malicious act”. 3. Control Center: As defined, control

centers are as follows: one or more facilities “Hosting” a set of one or more BES Cyber Assets OR BES Cyber Systems performing one or more of the following functions that supports real-time operations by System Operations for two or more BES Generation facilities or transmission facilities, at two or more locations. While the definition of entities control centers (e.g., control centers monitoring and controlling generation and transmission facilities) are being interpreted by this definition, the control room for generation facilities could be interpreted to adhere to the same CIP standard requirements. Requesting a clear interpretation of control center, with examples for CEA’s and entities or a clear definition of generation control rooms and the separation of the two definitions in relation to CIP v5 standards. 4. Cyber Assets: Programmable electronic devices, including the hardware, software, and data in those devices. Does programmable devices include legacy Remote Terminal Units (RTU's) with eeproms? Some may not consider them as Cyber Assets. Because not all industrial devices are IT based, suggest thorough research be performed within the industry before declaring specific devices.
Yes
CIP-002-5: Attachment 1: Medium Impact Rating; 2.13: Clarification needed within the definition of (2) Generation control centers that control 300MW or more of generation. As stated within question one of this document, the definition of control center and generation control room needs to be defined separately. Entities and Compliance Enforcement Authority (CEA’s) are interpreting no difference in control centers and generation control rooms.
Yes
Yes
No
While it’s completely understandable the VSL’s are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL’s for all requirements.
Yes
Yes
Yes
Yes
Yes
Yes
No
While it’s completely understandable the VSL’s are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL’s for all requirements.
Yes
No
CIP-004-5 R2: Requirement 2.10: Role based training on the BES Cyber System’s interconnectivity and interoperability with other cyber systems. The understanding of this requirement is to perform annual training to those entities interdepartmental personnel who are responsible for implementing, maintaining and securing the interconnectivity and interoperability BES impacted networks. Many mid-range to small entities that will be impacted by CIPv5 have small internal departments controlling the CIP networks. The reality of performing training on personnel whom maintain the systems is very confusing, time consuming and redundant. Establishing training for those individuals who are so involved with the infrastructure or protecting the asset seems ineffective in protecting the reliability of

a BES Cyber System.
Yes
Yes
Yes
Yes
No
While understanding the justification of minimizing the risk scope and implementing logic from NIST 800-53 version 3 segments, clarification is needed for all requirements within CIP-004-5.R7. For example, R7.1 – HIGH & MED asset designation- individuals who resign or are terminated must have revocation of unescorted physical access and interactive remote access to BES Cyber Systems at the time of the resignation or termination. Request a sufficient timeframe (e.g., xxxx hours to complete the access revocation of physical and remote access) as entities processes may adhere to the standard, however, the phrase “at the time of the resignation or termination” is subject to interpretation. CIP-004-5.R7.2 – HIGH & MED asset designation – For reassignments or transfers, revoke the individuals unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day. Request a longer timeframe to complete the task of having a full assessment for reassignments or transfers. Recommend seven days for reassignments and transfers as too many variables may inhibit next calendar day completion.
No
While it’s completely understandable the VSL’s are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL’s for all requirements.
No
CIP-005-3 Requirement 1.1: Define technical and procedural controls to restrict unauthorized electronic access. With entities identifying assets High, Medium and Low, anticipation of many BES Cyber system assets being categorized as low should be considered when establishing criteria which are enforced. Assets that are categorized as Low could be into the thousands for any registered entity. Resources could be allotted toward High and Medium BES Cyber Systems as opposed to Low categorized BES Cyber Systems. CIP-005-3 Requirement 1.5: A documented method for detecting malicious communications at each EAP. The implementation of IDS systems at each identified ESP (internal and external), along with current security methods of deterring malicious intent seems to be extensive and very costly to entities. Recommend a re-write of the requirements to “a documented method for deterring malicious communications at each EAP”. Otherwise, if IDS is absolutely required, please consider IDS implementation on external outbound EAP’s. Internally identified EAP’s located within DBP’s, already enforced with ACL’s and logging should not be subjected to IDS implementation.
No
CIP-005-5 Requirement 2.2: Require encryption for all interactive remote access sessions to protect the confidentiality and integrity of each interactive remote access session. One element that needs to be addressed is contracts with the various service vendors and contractors that maintain systems from remote locations. Current contracts from vendor to owner have established terms and conditions that could negate the contact and void the service agreements. Also, if entities are utilizing vendor support to maintain a deemed BES Cyber System, how can entities implement encryption into vendor network, all the way to vendor end point (console)? Clarification is needed on where encryption needs to start and stop accordingly.
No
While it’s completely understandable the VSL’s are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL’s for all requirements.
Yes

Yes
No
CIP-006-5 Requirement 3.2: Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year. Clarification on the term “outage” is needed. If outage is referring to downtime that was unwarranted or unscheduled; suggest “maintenance and /or unscheduled operational downtime”.
Yes
Commend SDT on developing VSL’s for all categories.
No
CIP-007-5 Requirement 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. Requirement itself is too vaguely written, subject to interpretation. Request clarifications on the following terms: “console commands” and “signage” used in the measures section. Entities may have difficulty disabling or restricting the use of unnecessary physical input/output ports used for console commands, as multiple operating systems are being utilized throughout the industry, not just Microsoft. Due to the Stuxnet vulnerability, entities must be proactive and protect themselves by disabling the removable media ports (USB), however, restricting and disabling physical ports for console commands (basically serial ports), is not exactly logical.
No
CIP-007-5 Requirement 2.3: A process of remediation, including any exceptions for CIP exceptional Circumstances. Recommend changing the term “remediation” to “mitigation” this change will cause less ambiguity and will be consistent with terminology currently established. Also, measurements for compliance seem to exceed the requirements. Entities are performing these tasks (measures) on a monthly basis in conjunction to their security patch management programs. The current list of measure to meet this specific requirement does not improve security or the reliability of the BES Cyber Systems or BES Cyber Assets. Recommend scaling down the measures.
No
CIP007-5 Requirement 3.1: Deploy method(s) to deter, detect or prevent malicious code. Recommend re-wording the requirement as it’s subject to interpretation. Entities and CAE’s alike, view this requirement as a “either or” statement. Recommend utilizing “where technically feasible” as not all BES Cyber Systems are designated as computers utilizing Microsoft technology, (e.g., relay’s, PLC’s, Controllers, etc.) CIP-007-5 Requirement 3.1 through 3.4: Unfortunately, the manufactures that have developed industry hardware and some software do not view malicious software to be a legit issue. Recommend adding “where technically feasible” to requirement. Substation relays, Programmable Logic Controllers (PLC’s), Printers, controllers, controller cards, etc. are a few examples that cannot adhere to the malicious software requirements. TFE’s will be abundant.
No
CIP-007-5 Requirement 4.1: Measures: Evidence may include, but not limited to, a paper or system generated listing of event classes for which the BES Cyber System is configured to generate logs. Recommend redefining measures as UNIX systems and other systems outside of Microsoft environment do not have “event classes”. CIP-007-5 Requirement 4.1.1: Any detected failed access attempts at Electronic Access Points. Request implementing this requirement within CIP-005-5; Separating EAP and BES Cyber System requirements is essential and adds clarity within the requirements. Previous NERC CIP revisions failed to separate requirements which led to more confusion. CIP-007-5 Requirement 4.3: Detect and activate a response to event logging failures before the end of the next calendar day. Clarification needed on this specific requirement; is it the expectation of automated detection? If so, from a technical standpoint, not all operating systems are capable of detection of failed logging. Entities would have a real hard time meeting compliance with this requirement. CIP-007-5 Requirement 4.5 – HIGH asset designation: Review a summarization of sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day. Clarification needed for the term ‘summarization of logs’.
No

CIP-007-5 Requirement 5.4: Procedural controls for initially changing default passwords. Recommend the enforcement of the requirement be established for designated high and medium BES Cyber systems as low assets will be in the thousands requiring maximum resources protecting assets (LOW) that do not affect BES as established High and Medium BES Cyber Assets.
No
While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL's for all requirements.
Yes
No
CIP-008-5 Requirement 2.1: The incident response plans must be used when incidents occur and include recordings of deviations taken from the plan during the incident or test. The requirement to record the "deviations" from the incident response plans offers no significant improvement in the reliability of the BES Cyber Assets or BES Cyber Systems. This can be documented within the entities internal processes as lessons learned. Deviations can be a subject to an interpretation by CEA's.
No
CIP-008-5 Requirement 3.2, 3.4, 3.5: Recommend adjusting the time frame from 30 days on 3.2, 3.4 and 3.5 to match Requirement 3.3, 60 days. Unified representation adds clarity.
No
While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL's for all requirements.
No
CIP-009-5 Requirement 1.4: Backup media shall be verified initially after backup to ensure that the backup process completed successfully. Recommend removing the term "initially" or adding a footnote establishing a realistic timeframe in which backup can be validated. Backups can take hours and last into late evenings. Not all entities have 24/7 coverage within their establishments. Requirement is subject to interpretation. CIP-009-5 Requirement 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. Recommend merging this requirement into CIP-008-5, Incident Response Plans. The theory of preserving data at the time of the incident as opposed during the recovery of a BES Cyber Asset seems to be logical. If needed, lessons learned from the incident can be used to update the BES Cyber System recovery plans.
No
CIP-009-5 Requirement 2.3: Test each recovery plan referenced in R1, initially upon effected date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. The requirement itself is extremely stringent in regards to performing an operational exercise on "each" recovery plan for BES Cyber assets and BES Cyber Systems. The definition of "operational exercise" is also subject to interpretation as every entity performs this function differently and CAE's may interpret differently. Request removing operational exercise or designating this requirement for High designated assets. Depending on the amount of Medium and High BES Cyber Systems are designated, entities could be performing operational exercises on a bi-weekly basis just to meet the 39 month requirement.
No
CIP-009-5 Requirements 3.2 through 3.5: Added time frame to current revision is 30 days. Suggest establishing 60 days to complete requirements 3.2 through 3.5. Entities impacted by CIPv5 may establish a substantial amount of High and Medium BES Cyber assets and BES Cyber Systems. Thirty days seems a bit strenuous and may produce a high failure rate. Also, recommend this requirement be enforced to only High and Medium BES Cyber Assets and Systems.
No
While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and

Severe VSL's for all requirements.
No
CIP-010-1 Requirement 1.1: Baseline configuration of BES Cyber Systems. With the understanding that this particular requirement was derived from the DHS catalog for control systems security, how does an establishing specific field within a baseline record and those records being auditable increase security and therefore the reliability of the BES Cyber system? Establishing a baseline on each BES Cyber System has been established for the prior requirements that pertain to CIP-007. Entities should have the freedom to create and maintain baseline configurations that impact their assets. With that said, sub-requirement 1.1.4 is very vague. These systems may contain thousands of scripts and the documentation of these to this level is not practical. Also, Requirement 1.1.6, "any patch levels", UNIX and other operating system outside of Microsoft do not have patch levels. Recommend updating the requirement without sub-requirements 1.1.1 through 1.1.6 and leaving the base requirement of Requirement 1.1. The specific requirements 1.1.1 through 1.1.6 provide no added security or reliability to BES Cyber Assets and BES Cyber Systems. CIP-010-1 Requirement 1.2: Measures: A record of each change performed along with the minutes of a "change Advisory board" meeting (that indicate authorization of the change) where an individual with the authority to authorize the change was in attendance. Establishing a "change advisory board" for changes to BES Cyber System baseline configurations and recording the minutes and attendance records is completely non-productive and brings no significant security or reliability to BES Cyber Systems. This requirement maybe needed within larger entities with separate divisions performing multiple functions, however, midrange to small entities have established effective processes through various methods of change control. This particular requirement establishes that NERC CIP requirements are not a "one size fits all" methodology.
No
CIP-010-1 Requirement 2.1: Where technically feasible, monitor for changes to the baseline configuration and document and investigate the detection of any unauthorized changes. This specific requirement seems to be redundant to the requirements set forth in CIP-007-5 R4.1 through 4.5. Why add more responsibility to monitoring BES Cyber Systems outside of the requirements in CIP-007?
No
CIP-010-1 Requirement 3.1: ...conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as design. The term "security controls" is subject to interpretation. Recommend clarifying the term or designating areas within security that need to be assessed.
No
While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL's for all requirements.
No
CIP-011-1 Requirement 1.1: Measures, bullet 2: Training materials that provide personnel with sufficient knowledge to recognize BES Cyber Security Information. Not sure if SDT meant BES Cyber System Information?
Yes
No
While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL's for all requirements.
No
CIPv5 implementation plan may need to be revised based on FERC's non-approval of CIP v4. OPPD would prefer FERC to approve CIPv4, which would allow entities to comply with the "bright-line" criteria, which is similar to CIP-002-5 Attachment 1. In the future, CIPv5 can be gradually implemented, while allowing entities to meet the "bright-line" criteria, which has been approved in CIPv4 by the NERC balloting body. We recommend CIPv5 be introduced in stages or establishing an implementation cycle as opposed to bypassing the CIPv4 and implementing directly into CIPv5.

Introducing CIPv5 in stages will allow entities who are not in scope to implement CIPv4 “bright-line” criteria and establish a sound level of protection to Critical Cyber Assets. Those entities that are currently in scope will continue to adhere to the CIPv4 standards while preparing internally, financially and structurally for the implementation cycle of CIPv5. Also, would like to note that while the intent of the CIPv5 is to increase security and reliability to the BES, meet FERC Cyber security order 706, and present entities with guidance to enhance their own assets, CIPv5 requirements will take a heavy financial toll on our medium sized utility. Additional resources and infrastructure modifications may cost millions to meet compliance requirements. Additionally, entities impacted by natural disasters (e.g., flooding, tornadoes) are currently recovering and rebuilding their establishments, which only add to ongoing operational cost. Please remember these elements when defining the CIPv5 implementation process.
Group
Dominion
Connie Lowe
Yes
General Comments: The following comments are general in nature and do not apply specifically to Definitions. 1. Dominion supports the approach outlined in Mid-American’s January 3, 2012 document titled “Recommended Change Priorities for CIP Version Five” and does not believe that approach would disrupt Drafting Team efforts and the development of CIP Version Five (V5). The Drafting Team should review Mid-American’s approach and incorporate the recommendations set forth therein. 2. As part of adopting V5, existing CANs must be retired by incorporating the associated requirements and measures into V5. A reconciliation is required to determine which CANs are expected to be retired as a result of the adoption of V5 or may still be applicable at the time V5 is adopted. This information should be incorporated in either the “Reference to Prior Version” of each applicable requirement or through the “Guidelines and Technical Basis” of each applicable Standard. The associated CANs are: a. CAN-0005 b. CAN-0007 c. CAN-0010 d. CAN-0012 e. CAN-0016 f. CAN-0017 g. CAN-0024 h. CAN-0030 i. CAN-0031 Definitions Related Comments: • Annual: The term “Annual” should be created and defined as “At least once per calendar year, not to exceed 15 calendar months between occurrences.” In the requirements listed below, the phrase “on an Annual basis” should replace the phrase “initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences”. This change applies to: o CIP-002-5: R2 o CIP-003-5: R3 o CIP-004-5: R3.2, R6.5, R6.6 o CIP-008-5: R2.2, R3.1 o CIP-009-5: R2.1, R2.2, R3.1 o CIP-010-5: R3.1 o CIP-011-5: R1.3 The definition of “Annual” tracks the language already set forth in Version 5. Implementation of the definition of “Annual” simplifies the language in 13 requirements and reflects the retirement of CAN-0010.
No
No comments.
No
It is not clear how the retirement of CAN-0005 is being addressed in V5.
No
Consistent with the previous response, R2 should be modified to read “The Responsible Entity shall have its CIP Senior Manager or delegates approve the identification and categorization required by R1 initially upon an Annual basis, even if it has not identified High or Medium BES Cyber Assets or BES Cyber Systems.”
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
No comments.
No
The numbering scheme of the sub-bullets does not match the numbering scheme used in the other standards. It is recommended that “1.x” subtopics listed under CIP-003 R2 be renumbered as follows: 2.1. Personnel Security 2.2. Electronic Security Perimeters 2.3. Remote Access 2.4. Physical Security

2.5. System Security 2.6. Incident Response 2.7. Recovery Plans 2.8. Configuration Change Management 2.9. Information Protection 2.10. Provisions for declaring and responding to CIP Exceptional Circumstances
No
No comments.
No
No comments.
No
No comments.
No
No comments.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
Yes
No comments.
No
No comments.
No
No comments.
No
• It is not clear how the retirement of CAN-0012 is being addressed in V5 or how it applies to Personnel Risk Assessments (PRAs). • The implementation plan for V5 should address how Personnel Risk Assessments are to be conducted during the implementation period. • PRAs completed prior to V5 should be acceptable until the next time a PRA is required in the 7 year cycle. The following paragraph should be added as the last paragraph to the “Guidelines and Technical Basis” section for CIP-004-5 R4: Personnel Risk Assessments which were completed prior to the effective date of Version 5 of the CIP Standards are acceptable as evidence of completion of a Personnel Risk Assessment even though all of the requirements of Version 5 may not have been met. All Personnel Risk Assessments started after the effective date of Version 5 of the CIP Standards must address all of the sub-requirements in Table “CIP-004-5 Table R4”. • PRAs conducted in support of other compliance programs, such as compliance with requirements for the Nuclear Regulatory Commission (NRC), should be considered acceptable when an individual transfers from one compliance program to another. • The “Guidelines and Technical Basis” section should include a paragraph about “locations” to ensure time and money isn’t wasted on criminal history checks. While the PRA should include details of where an individual resided as part of the seven year criminal history check, we have concerns over the requirement to capture the location of prior employment and school attendance for periods greater than 6 months without further qualification. An individual may attend an on-line school or perform temp work remotely. In these cases, the location of the school and employer are less important to the evaluation of the individual than the location in which the schooling was completed or the work was performed. Dominion is concerned that unnecessary time and costs could be incurred in conducting PRAs without a qualification that the primary physical location of where the individual resided while performing school and work related activities is what needs to be investigated as part of the criminal history check—not the physical location of school or employer. • The requirements for original investigations and reinvestigations should be addressed separately. Reinvestigations should only be relevant for the time period after the original investigation was conducted.
Yes
No comments.
No
No comments.
No

No comments.
Yes
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
No comments.
No
Dial-up is addressed in other requirements and should be explicitly excluded from this requirement.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
CAN-0031 should be retired as part of V5. The “Guidelines and Technical Basis” section contains requirements reflective of CAN-0031 that should be removed entirely.
No
No comments.
No
No comments.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
No comments.
No
No comments.
No
No comments.
No
No comments.
No
• CIP-007-5 R5.1 needs to be qualified as being applicable to individual accounts. Credentials cannot be validated with shared accounts. • CIP-007-5 R5.5.1 and R5.5.2 provide that password length and complexity could be the maximum supported by the BES Cyber System. A BES Cyber System is a collection of assets that make up the system. The maximum supported password length and complexity of the system would therefore be driven by the maximum password length and complexity of the device least able to comply with the minimum requirements. The language of the requirements should be modified to read: o 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the Cyber Asset within the BES Cyber System. o 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset within the BES cyber system. • CAN-0017 must to be incorporated into the standard or retired. CAN-0017 indicated that both technical and procedural controls are required; however, the language of V5 indicates that either technical or procedural controls are required to address password complexity.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No

No
No comments.
No
No comments.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
No comments.
No
No comments.
No
No comments.
Yes
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
No comments.
No
No comments.
No
No comments.
Yes
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
In contrast to previous versions of the requirement, the language in CIP-011-1 R1.1 is confusing and may unintentionally reduce the level of information protection afforded to BES Cyber Systems. CIP-011-1 R1 should more closely reflect the intent of the Version 3 and Version 4 versions of the CIP-003 R4 requirements. CIP-011-1 R1.1 states that “One or more methods to identify BES Cyber System Information”. This suggests the overt labeling of information associated with BES Cyber System information with a tag that identifies it as BES Cyber System information. The standard should not require the overt labeling of such information with a BES Cyber System tag; rather, it should allow the flexibility described in the Change Rationale associated with having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business. To this end, the language should be modified to read: “One or more methods to label BES Cyber System Information to ensure the information can be associated with an appropriate access control and handling procedure.”
No
• The standard does not specifically address backup or copies of media. If the standard is modified to address backup or copies of media, such modification should be placed in the “Guidelines and Technical Basis” section of the standard. • Application to “any media” known is too broad. Clarity on the intent and applicability of the requirement is necessary. • It is unclear how hardcopies of information are to be disposed of in the new version of the standard.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.

No
No comments.
Individual
Jennifer Wright
San Diego Gas & Electric
Yes
San Diego Gas & Electric's (SDG&E)'s proposed definition revisions are as follows: BES Cyber Security Incident- Any malicious act or suspicious event that: •Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or a BES Cyber System, or, • Disrupts, or was an attempt to disrupt, the operation of an Electronic Security Perimeter or BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. In general, the proposed definitions are too long, general or arbitrary. The changes to the definitions from Version 3 to Version 5 may greatly change the interpretations; and hence force changes to system design architectures which currently exceed CIP standards. For example, with respect to a BES Cyber Asset, Information Systems designs and architectures best practices include Availability and Reliability as a basis to eliminate risk and increase Availability. The proposed standard definition eliminates Redundancy as a form of risk reduction and renders useless a potential design implemented to increase Availability. Redundancy is implemented to retain availability and should be considered a security measure. Additionally, terms such as Electronic Access Point (EAP) are now greatly different from Access Point to the ESP/PSP. These terms now require major changes to documentation, procedures and evidence. It would be more efficient and cost effective to build upon the existing definitions.
Yes
In general, the criteria should continue to align with NIST standards. Section 2.1 identifies as Medium Impact Rating, generation equal to or exceeding 1500 MW. Yet, 2.13 identifies generation control centers that control 300 MW or more of generation. It's unclear why the first only considers those of 1500 MW or greater, yet drops down to control centers for much less generation (300 MW). It would seem that 2.13 should also be 1500 MW since the impact to the BES would be the same. Sections 2.8 and 2.9: Should there be a requirement that the RC, PA, or TP notify the TOP/TO that they have designated the facility as critical. It's done in Section 2.3 for the GOP/GO. Guidelines and technical basis section: It's unclear how one would interpret the use of "Operational directives" in regards to Reliability Operations Services. Could NERC provide more guidance as to their intent? Additionally, SDG&E has comments regarding the Applicability Section. In Section 4.2.2, NERC identified as an included facility, those systems or programs designed, installed, and operated for the protection and restoration of the BES to include "Its transmission Operator's restoration plan". It would seem that this should have greater details as to what that includes. For example, does it include all of distribution system assets that are used to restore system load. That effectively makes the standards applicable to all distribution, which seems unnecessary.
No
SDG&E recommends expanding the requirement to 60 days due to potential changes in project schedules and ordering or delivery of equipment.
No
SDG&E recommends that the Senior Manager could approve "prior to or initially upon". In general, with regard to the proposed CIP Version 5 Standards, it is unclear whether all the requirements have to have been completed at least once prior to the effective date? In some cases, the standard requires that the entity perform some function initially upon the effective date and then have a follow-up requirement (e.g. update cyber security incident plan within 30 days). NERC should provide further guidance in regards to implementation of CIP Version 5 in this regard.
No
SDG&E recommends that the SDT provide examples of how and when an entity would provide proof of such awareness.

No
It is unclear which “approvals” and “authorizations” are being referenced in the language “shall be responsible for all approvals and authorizations required in the CIP standards.”
No
The training program first needs to identify the roles and the training required by each role. It then requires that each person have training in each of the areas which doesn’t seem then to make a distinction in roles. Shouldn’t the training be able to be different for the different roles?
No
SDG&E recommends language for Part 6.5 which lists all “systems accounts/groups…”
No
Regarding CIP-004-5 R7.2, revoking access due to reassignment or transfers by the end of the next calendar day seems unreasonable. This doesn’t take into consideration the fact that personnel that are reassigned or transferred may have a need to provide support during the transition to new personnel. The original language in Version 3 seems more logical that when access is no longer required, it should be revoked within 7 days. However, determining the date of transfer should be dependent on the type of transfer. For example, where transfers occur outside the department, a 7-day window may be reasonable. Where a change of role occurs within an organization, a 30 to 90 day window may be reasonable due to the time needed to hand-off responsibilities.
No
SDG&E recommends in Part 1.3 to define access permissions and provide examples.
No
For R1.1, SDG&E seeks clarification from NERC regarding how one would restrict access to unnecessary logical network accessible ports that can’t be disabled?
No
SDG&E recommends rewording the language for Transient and Maintenance Cyber Asset. Logging each transient asset connection may not be possible when considering USB or serial connections. This type of activity is better employed using technologies or policies.
No
The term “log generated events” is incorrect. A log is a type of output of a system that is generated by the system. A log, unless scripted by a system sub-process, cannot generate a log, and therefore requires a system process to generate the log. A better term would be a system event log, or system log. Secondly, some legacy or specific machines may not issue a log which can be a) accessed or b) may not meet the parameters of the standard.
No
The proposed language in the standard is unclear and provides little inherent benefit to a security program. SDG&E suggests that the language in R5.5.2 be changed from “the maximum complexity supported by the BES Cyber System” to “the maximum complexity of the above that can be supported by the BES Cyber System”. In R5.5 and 5.6, process or procedural based controls provide

limited security, and to limit unsuccessful authentication attempts or alerts may only be achieved through additional technologies – not procedures. In a Generation environment, for example, small engine and generator cyber assets exist, which do not support authentication or alert for authentication failures.
No
With regard to CIP-007-5 generally, the term “where technically feasible has been removed in many cases where they existed in Version 3. Systems may still have those technical limitations. Is its NERC’s intent that entities can meet these requires with non-technical solutions (e.g. procedural)?
No
SDG&E suggests that the language in R2.2 be changed from “initially upon the effective date” to “prior to or initially upon the effective date”.
No
SDG&E suggests that the language in R3.1 be changed from “initially upon the effective date” to “prior to or initially upon the effective date”.
No
The term "security controls" may not be universally understood within a change management structure. SDG&E recommends including examples of "security controls" and the nature of potential changes impacts to security controls.
No
The issue with the existing language regarding Configuration Monitoring is one where, in a normal systems operating environment, certain changes may not require change processes, and hence change monitoring which is predicated on identifying unauthorized changes fails. An example of this is a change to a data set point, or password change. Each is a general operational change to a system, and affects the configuration of a BES Cyber Asset or System, however may be operationally infeasible - due to the amount and effort of process required to monitor, track and schedule this type of activity.
No
The Vulnerability Assessment tasks listed in the table include the assessment of a test BES cyber system and a comparison of the VMA results against the production environment. Creating a test BES cyber system which models a baseline configuration of the production environment may not be feasible, and in some cases broadly expensive. Some environments rely on older or newer technologies and equipment, and some on a variety of equipment. In addtion, a baseline of the production environment may not be accurate without a VMA against the production system. SDG&E's suggestion is to retain the Version 3 VMA process.
Yes
Group
PacifiCorp
Sandra Shaffer
Yes
As a general, overarching comment, PacifiCorp is concerned about the new direction and definitions prescribed by Version 5, particularly with respect to CIP-002-5. Rather than clarifying and building

upon the existing methodology for identifying critical assets and related critical cyber assets, CIP-002-5 attempts to create a new and unproven methodology for identifying in-scope devices that introduces several procedural and interpretation flaws, rendering the proposed methodology less straightforward than the existing standards. PacifiCorp believes the primary problem with the CIP-002-3 methodology was a failure to clearly identify critical asset facilities, and not a failure to identify related critical cyber assets. This flaw (arising from the discretionary nature of self-determined risk assessment) was corrected by the bright-line criteria introduced as the foundation of CIP-002-4 which was approved by the industry in 2010. PacifiCorp strongly recommends that CIP-002-4 be used as the basis for identifying in-scope cyber devices. This approach would provide consistency and reduce confusion, cost and administrative burdens which would accompany the new regime outlined under CIP-002-5, and adversely impact the registered entities that have already established robust NERC CIP compliance programs based on the CIP-002-3 methodology and defined terms. If CIP-002-4 is used as the basis for identifying in-scope cyber devices, Version 5 of CIP-003 through CIP-011 could be adopted with necessary changes to reflect the preservation of CIP-002-4. Rather than building upon existing definitions that have been implemented and revised by the industry for several years as part of the prior versions of the CIP standards, Version 5 introduces new and problematic definitions. PacifiCorp recommends that the SDT go back to the definitions used in Version 4, and modify those definitions to add clarity. As an example, the new Version 5 definition of BES Reliability Operating Services introduces more problems than it resolves and is not necessary for Version 5 to be effective. Instead, we propose that the terms BES Reliability Operating Service, BES Cyber Asset and BES Cyber System not be implemented and the use of existing terms such as Critical Asset, Cyber Asset and Critical Cyber Asset be retained and modified as needed. As an example, the existing definition of "Critical Cyber Asset" could be revised as follows: "A Critical Cyber Asset is a Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, adversely impact the reliability of the Critical Asset facility where it is located and used." In the alternative, if there is consensus that the term BES Reliability Operating Service adds clarity to which cyber assets should be regulated by the CIP Standards, the definition should be properly incorporated into the definition of Critical Cyber Assets as follows: "A Critical Cyber Asset is a Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, adversely impact the capability of the Critical Asset facility where it is located and used to perform a BES Reliability Operating Service."

Yes

One of the key problems with Version 5 is that the methodology does not follow a logical "general to specific" categorization process. To generate a list of "qualified" Cyber Assets/Systems, the first logical step is to distinguish between what elements in the universe of potential regulated Cyber Assets are relevant and which can be ignored. The current draft of CIP-002-5 begins with the entire universe of a regulated entity's Cyber Assets. The process then flips back and forth between applying general and specific filters or qualifiers (including bright line criteria that only make sense when applied to a facility and not an individual Cyber Asset associated with a facility) to finally derive a list of BES Cyber Assets. PacifiCorp recommends that the SDT return to the current CIP-002-4 process of first identifying a critical facility, and then identifying the Cyber Assets and Critical Cyber Assets that are relevant to the operation of that critical facility. In the event that the new Impact Categorization criteria outlined in Attachment I of the proposed CIP-002-5 are adopted, we propose the following modifications: 1. In Section 2.1, the Attachment I bright line criteria of 1500 MW is an appropriate threshold if one is assessing generation facilities, but is not an appropriate criteria to assess BES Cyber Assets. This is because a 2000 MW generating plant is likely to have two to four separate control rooms that run units at that plant. On the other hand, it is highly unlikely that there are many generating facilities for which a single BES Cyber Asset affects 1500 MW. Once again, we recommend that entities start with a determination of Critical Asset facilities which will reduce the universe of Cyber Assets to those that are potentially relevant to the functioning of those facilities. 2. In Section 2.7, the Weight Value per Line of 700 should be replaced with a value in the range of 500 – 600, which is more representative of typical rating of 230 kV lines. PacifiCorp operates over 3,000 miles of 230kV line and only a small percentage of them have a peak rating of over 700 MW. 3. In Sections 2.8, 2.9 and 2.11, the table titled "Major WECC Transfer Paths in the Bulk Electric System" is not actively maintained by WECC and there is no clear identified basis for why certain paths are included in this table. Rhetorically, it has been mentioned that many of the paths on the table were included for economic / marketing reasons rather than reliability impact. As an alternative, we suggest "transmission paths contained in the WECC Path Rating Catalog with a maximum path rating equal to

or greater than 1,500 MW." This catalog is actively maintained by WECC and the 1,500 MW value ties much better to other items in Table 1. 4. In Section 2.11, the table titled "Major WECC Remedial Action Schemes (RAS)" is not actively maintained by WECC and there is no clearly identified basis for why certain Special Protection Systems (SPS) are included in this table. As an alternative, we suggest "each SPS categorized as a 'Wide Area Protection System' by WECC. This is the newly created mechanism within WECC to identify SPS of significant importance. 5. The opening paragraph of the definition of Medium Impact Rating should be revised as shown below to correspond with the wording for High Impact Rating: "Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at the following Facilities:"
No
PacifiCorp strongly recommends the removal of any requirements for defining or otherwise addressing Low Impact BES Cyber Assets from the current draft standard. The volume of Low Impact assets is an order of magnitude greater than Medium and High assets for most entities and poses a tremendous compliance burden. While we recognize that there may be security issues that need to be addressed with these assets, we recommend that they be addressed in a separate standard than Medium and High Impact assets. This would allow the industry to initially focus on the more important assets and provide time for further discussion and clarification with respect to Low Impact assets. R 1.1 of CIP-002-5, which requires an update to the status of a BES Cyber Asset within 30 days of a change to that BES Cyber Asset that changes its impact, is a good illustration of the problem with the Cyber Asset-first approach described above in our response to Question 2. Since the most common changes and the changes that are most relevant to the standard's intent, will be to BES Cyber Assets in the Low Impact category, to ensure compliance with the requirement, a regulated entity will have to track all changes to BES Cyber Assets in the Low Impact category – this is despite the current draft's express acknowledgement that Low Impact Cyber Assets are not relevant to the BES. So, even if this requirement can be audited via a spot check of Cyber Assets, compliance likely cannot be achieved without monitoring changes to every Low Impact BES Cyber Asset. In reality, all that really matters are changes made to BES Cyber Assets within a critical facility identified via Attachment I. Again, the starting point should be changes to a critical facility, and then to related critical cyber assets, which follows the methodology of Version 4. As currently drafted, R 1.1 of CIP-002-5 could only be audited through a highly ineffective spot check process, consisting of an auditor pointing out a specific Cyber Asset and asking about the nature of any changes made to that device. In general, PacifiCorp believes that Version 5 will be extremely difficult to audit and will lead to a wide spectrum of audit approaches, rather than a clear and consistent audit approach. Since CIP-002 is the linchpin standard for the entire suite of the CIP Standards, this standard must be clear and concise, with compliance or non-compliance easily determined. It is unlikely that an auditor would point to a Cyber Asset at a generation plant to challenge a regulated entity's determination of whether the mis-operation or non-operation of that individual BES Cyber Asset would or would not adversely impact the plant. It is much more likely that the auditor would look at the generation facility first to determine what impact the loss or mis-operation of the facility would have, and then determine what potential impact the individual BES Cyber Assets have on the plant's performance. Again, since this is the logical process for the analysis, the standard should be changed to reflect this.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No

PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
Yes
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
Yes
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No comment.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.

No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No comment.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No comment.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
Individual
Roger Pan
Emerson Process Management
No
The 15-minute criterion in BES Cyber Asset definition should be eliminated. This criterion should be only used in the high or low impact rating in CIP-002-5 Attachment I. Rationale: Therer are many auxiliary control sytems in power plants that will not adversely impact one ore more BES Reliability Operating Services within 15 minutes after rendered unavailable, degraded or misused. Based on the current definitions, these sytems will be totally out of CIP requirements, and not even being considered Low Impact systems. However, their continue unavailability after 15 minuts without successful recovery will have a devastating effect on sustaining continuous power generation. Also, most of them are indeed interconnected with main boiler control systems which shall be BES Cyber Systems. Excluding those auxiliary control sytems from the minimum security erquirements may be proven fatal if and when they are compromised.
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Could Remote Access cause "aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES" as stated in the Change Rationale for Part 1.1? If this rationale is justified, R2 should also be applicable to Low Impact BES Cyber Systems.
Yes
Yes
Yes
Yes
Yes
Yes

No
This requirement does not address the situation when legacy systems are not supported by OEM, have no security patches, but are still vulnerable to malicious exploitaton. The guideline for this requirment only requires a note "in your source document." A more proactive mitigation should be mandated such as an upgrade plan so that the assset or system has on-going support from the OEM, industry and governments. The guideline for 2.2 suggests the "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control System" by DHS as a source. Instead of patching the BES Cyber Assets or Systems monthly, this new requirement essentially relaxes it to a quarterly basis. It does not seem properly addrssing increasing malicious attackes mostly exploiting zero-day vulnerabilities.
No
Part 3.3 significantly relaxs the signature or pattern update from weekly to monthly. Thie relaxation only puts BES Cyber Assets or Systems more vulnerable to malicious attacks if there is no proactive and preventive protection in place.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Part 3.1 requires "a paper or active assessment of the security controls..." Preseumably, it is on the actual BES Cyber Asset or system. Part 3.2 requires "an active vulnerability assessment in a test enviornment..." It seems that Part 3.1 should only require a paper assessment, while 3.2 required an active assessment.
Yes
No
BES Cyber System Information has been defined in the Definitions of Terms Used in Version 5 CIP Cyber Security Standard. Does Part 1.1 allow to identify more BES Cyber System information beyond what has been included in the official definition? Is the intent really for "marking" the identified BES

Cyber System Information?
Yes
Yes
Yes
Group
Tennessee Valley Authority
Brian Millard
Yes
1) BES Cyber Security Incident - be more specific regarding a “suspicious event” (list examples?) 2) BES Cyber System - be more specific regarding a “Maintenance Cyber Asset.” 3) It says that a Maintenance Cyber Asset is not part of a BES Cyber System. If a misused Maintenance Cyber Asset could adversely impact one or more BES Reliability Operating Services, would it still be considered a "BES Cyber Asset"? What takes precedence? 4) BES Reliability Operating Services - it says “Activities, actions and conditions necessary to assess the current condition of the BES...” What defines what is "necessary"? 5) CIP Exceptional Circumstance - would it be appropriate to also add situations that pose risks to the environment, significant damage to the system, or loss of crucial data/information? 6) CIP Exceptional Circumstance - be more specific regarding what “emergency services” are. 7) Control Center - the definition of "control center" seems to be too open, which may lead to unintended interpretations of the standard. Would any location with the ability to control more than one generation facility, regardless of size, be considered a “control center”?
Yes
Criterion 2.6 (Transmission Facilities operated at 500-kV or higher) should have an exception for radial Transmission Facilities used only to connect “Low Impact” generation to the transmission system. If the generation itself does not merit a Medium Impact designation, the associated transmission facilities should not be categorized as Medium Impact. Attachment I, 2.13 - "Generation control centers that control 300 MW or more of generation" are considered Medium Impact. The 300 MW figure seems very low, especially considering 2.1, which cites a 1500 MW figure for Real Power capability. Should these not be similar? That is, "Generation control centers that control 1500 MW or more of generation" for Medium Impact?
Yes
Yes
Yes
Yes
Yes

No
Yes
Yes
Yes
Yes
Yes
No
Table R3 - Malicious Code Prevention, Part 3.3 "Update malicious code protections within 30 calendar days of signature or pattern update availability..." Clarify that only those pattern updates that the entity chooses to apply (according to the entity-defined frequency) are within scope, rather than every single pattern update that a vendor might have available.
Yes
Yes
Yes
Yes
Yes
Yes

Group
Northeast Power Coordinating Council
Guy Zito
Yes
Refer to additional comments submitted for Question 49. “Suspicious” is not an auditable term, and should be removed. What is an “attempt”? What attempts are serious enough to justify having to be reported? The definition should be made to read: BES Cyber Security Incident A malicious act that: • Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. Under “BES Reliability Operating Services”: • “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet • Recommend that “Change management” under “Situational Awareness” be clarified to changes in the BES instead of IT change management • Recommend clarification that “Facility” is the NERC Glossary term--in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication”: • Request clarification of the scope of this “Operational Directives”. Does it include a company’s messaging system? Two-way radios? What is the relationship with the new COM-002? • Request clarification that these Coordination and Communications are limited to Reliability, not Market Systems. • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret.
Yes
Recommend that 2.8, 2.9 and 2.11 start with “Applies to all Regions except…” For 2.8, 2.9 and 2.11 request that the SDT clarify whether the exception is all, or not WECC. In 2.12, “system” and “Facility” are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal?
No
For clarity, request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days when a change to BES Elements and Facilities is placed into operation”. For clarity and consistency with the previous change, request changing M1 from “as required in R1 and list of changes to the BES (” to “as required in R1 and list of changes to the BES Elements and Facilities)”. The word “intended” should not be used in the requirement because it is not auditable. Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium, and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber

Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced throughout the Standards.
No
Regarding CIP-003-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
The last bullet for M4 on page 12 is inconsistent with R4 since M4 requires periodic training instead of R4’s making staff aware of cyber security policies. Request that M4 be updated to be consistent with R4.
Yes
No
The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
No
Regarding CIP-004-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement. Recommend removal of

R2.3 and R2.4 since they are redundant to R2.2, or explain the difference between R2.2 and R2.3, R2.4. Request removing “potential” from R2.7 since training should include how to determine whether a BES System Event occurred or not.
Yes
No
For all R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”.
No
For R6.1 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.3 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber System Information. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.6 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I” in Information.
No
Request that the footnote for 7.1 be moved into the requirement. Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend removing the "following the resignation or termination" since it is redundant and inconsistent with the sibling Requirements. Recommend changing 7.4 from "For resignations or terminations," to "For terminations, resignations, reassignments, or transfers,".
No
Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point or not? Request clarification on 1.5's "at each EAP". Is that inside or outside or both? Regarding CIP-005-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology. Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete.
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress". Request Requirement 1.2 be updated to allow "escorted physical access." Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.4 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. " to "issue real time alerts for detection of breach through an access point". For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6. Regarding CIP-006-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, ".
No
Request clarification on what the "Associated" "Applicability" (High/Medium/Low BES Impact) for 3.1 and 3.2 Request capitalization of "locally mounted hardware or devices" in Requirement 3.1 so that it refers back to the defined term "Locally Mounted Hardware or Devices" .
No
Request clarification on 1.1, is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on 1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Regarding CIP-007-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a

mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request clarification of "remediation" in 2.2 since it reads that the patch must be applied, which does not allow to have an exception when applying the patch is the worst scenario such as creating a denial of service. For 2.2, suggest wording like "create a remediation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied". What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to the patch or the overall process?
No
Request allowances in 3.3 for signatures/pattern updates that cause trouble. Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media". The Measure for 3.4 does not match the Requirement.
No
Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities. Request clarification on 4.3, does the failure need to be detected within a calendar day? Request the rationale of 4.5's "two weeks". Recommend one month as a compromise between the prior version's 90 days and the suggested one week. In 4.5 clarification is needed for the associated protected cyber assets. Are these protected cyber assets associated with only high impact BES cyber systems, or could they be associated with medium impact BES cyber systems?
No
For 5.2, does the CIP Senior Manager or delegate approval policy or procedure for each authorization of access? In 5.2, should the Requirement be interpreted as "each use" as in "The CIP Senior Manager or delegate must authorize the use of each administrator, shared, default, or other generic account types." Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
No
Regarding CIP-008-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
2.1 is a new Requirement. Request the rationale for this new Requirement. Recommend changing from "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." to "When a BES Cyber Security Incident is classified or identified, the Responsible Entity must follow its incident response plan." Recommend removing “initially upon the effective date of the standard” from 2.2 of Table R2 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered.
No

Recommend removing “initially upon the effective date of the standard” from 3.1 of Table R3 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend that 3.2 wording be consistent with the 2.2 wording. For 3.3, recommend changing 1) "Update" to "Update as necessary" and 2) "the completion of the review of that plan" to "the completion of the review performed in 3.2" .
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommend removing Requirement 1.5. Reliability's top priority is restoration of service. Forensics in a recovery mode may not support BES reliability and requiring such actions may negatively impact the BES Cyber System restoration process. Regarding CIP-009-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend that 2.1 be implemented 180 days from the effective date of the Standard. For 2.1, request clarification, is “full operational exercise” the same as “functional exercise” as described in the rationale? For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the Standard.
No
For 3.1 recommend 1) removing “or when BES Cyber Systems are replaced” as it addressed in CIP-009 R3.4 and 2) removing “and document any identified deficiencies or lessons learned” as they are addressed in CIP-009 R3.2 and R3.3. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Recommend that 3.4 be referenced by CIP-009 R3.1. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of

the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." For 1.1, 1.2, 1.3 and 1.4, recommend changing the Requirements to be consistent with their Applicability --- from "For a change to the BES Cyber System" to "For a change to the BES Cyber System or Associated Systems or Associated Assets". Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold. Regarding CIP-010-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend removing "where technically feasible" from 2.1 since the remaining words should not need an exception.
No
For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend changing 3.2 from "in a production environment" to "in a production environment, or a test environment" to allow Entities more flexibility in meeting this Requirement.
No
Request clarification on 1.1. Some interpret this Requirement as what is the Entity's process for identifying BES Cyber Systems Information. If correct, the Measure should be "show me the methodology (document)." Others interpret these Measures as labeling BES Cyber System Information. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Regarding CIP-011-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request that footnote 2 in 2.1 be moved into that Requirement.
The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If

true, the surrounding words should explicitly state so. Otherwise, this Scenario table is confusing because it repeatedly uses 12 months while the earlier text uses 18 months. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very "narrow" window. Since Version 4 is not FERC approved, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. A summary of comments applicable to more than one standard: . • Recommend removing "initially upon the effective date of the standard" from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • Request clarification of the capitalized term "Facilities." Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5. A fiftieth question should have been included in this comment form asking for general comments or concerns. A question asking general comments should be included as part of every comment form posted to the industry.

Group

Turlock Irrigation District

John Souza

Yes

The definition of a BES Cyber Asset leaves room for interpretation. The major problem is in the use of the words "adversely impact". These words are only slightly better than the words "would affect" which are used in the definition of Critical Assets in version 3. In effect, version 5 will reinstate one of the problems that version 3 has by using an undefined phrase open to interpretation. (Although Version 4 retains the definition of Critical Assets using the words "would affect", it does not leave these words open to interpretation because of its pure use of "bright line" criteria for determining Critical Assets. Likewise, Attachment 1 of CIP-002-5 uses the words "adversely impact"; however, it also uses "bright line" criteria including MW, MVAR and kV levels to determine the specific level of adverse impact.) Although "bright line" criteria have been included in CIP-002-5, such criteria are only used for determining Impact Levels (High, Medium and Low), and not for defining a BES Cyber Asset. Even the definition of BES Reliability Operating Services does not take the place of "bright line" criteria as long as the unqualified words "adversely impact" are retained in the definition of BES Cyber Asset. One suggestion is to create bright line criteria for determining what a BES Cyber Asset is. For example, there are different levels at which a Cyber Asset could "adversely impact" the BES Reliability Operation Services. These different levels could be translated to MW levels that could be used to create bright line criteria for defining BES Cyber Assets. The definitions of External Connectivity and External Routable Connectivity are also confusing. They are both defined as routable communications between a BES Cyber Asset and a Cyber Asset external to the ESP. The only difference we can see is that External Connectivity includes dial-up communications and, presumably, External Routable Connectivity does not?

Yes

Attachment 1, Part 1.2 criterion is based solely on the functional obligations of a Balancing Authority, whereas the criteria in the other Parts of Attachment 1 are based on the characteristics of a facility/system or on a combination of functional obligations and characteristics of a facility/system. This inconsistency in the criterion of Part 1.2 could result in a distortion of the proper placement of risk to the reliability of the BES. For example, based on these criteria, a relatively small Balancing Authority with less than 700 MW of generation and less than 700 MW of peak load would be required to categorize their BES Cyber Assets at their Control Center as High Impact. In contrast to this, a Generation Operator with twice as much generation (1400 MW) would be required to categorize their BES Cyber Assets at their Control Center as Medium Impact. This inconsistency could be remedied by adding "where the peak load or maximum generation capability within the Balancing Authority area exceeds 1500 MW" to the end of Attachment 1, Part 1.2. This modification would be consistent with the 1500 MW criterion placed on Generation capability in Attachment 1, Part 2.1. Then all Control Centers performing the functional obligations of a Balancing Authority below the 1500 MW level could

be included in the Medium Impact category under Attachment 1, Part 2.13 by adding “Balancing Authorities” to the list of functional obligations in Part 2.13.
No
CIP-002-5 Requirement 1 contains the word “owns” in the first and second sentences, there by limiting this requirement of indentifying and categorizing BES Cyber Assets to the actual owner of the BES cyber Asset. We would like confirmation that this was the intention of the SDT. If it was not intended, then the word “owns” should be changed to “operates”, “uses”, “maintains” or combinations of these words, depending on the actual intentions of the SDT. Actually, we believe that keeping the concept of ownership as the sole deciding factor in determining the Entity that is responsible for indentifying and categorizing BES Cyber Assets is the best concept to use. If multiple concepts such as “owns, operates, uses or maintains” are used then you could end up with more than one Entity responsible for applying security controls to a single BES Cyber Asset or System, which could cause a host of problems. The CIP-002-5 Application Guidelines, Attachment 1 section, Overall Application sub-section, last bullet item, gives some support for maintaining ownership as the sole deciding factor in determining the Entity that should be responsible for performing R1 of CIP-002-5. However, if the concept of ownership is used as the sole determining factor then clarification should be included in the Application Guidelines stating that “owns” includes concepts such as “leases, rents, or maintains ownership-like control”, in order to accommodate unusual cases where the actual “owner” of the BES Cyber Asset is not a registered entity. Another concept of CIP-002-5 that bothers us is the idea that you do not need to discretely identify BES Cyber Assets and Systems that fall into the Low Impact category, however, presumably, you do need to apply appropriate security controls to such assets. When a Cyber Asset or System drops into the Low impact level, it just gets that much more difficult to determine it the Cyber Asset or System is a BES Cyber Asset or System at all, there by exacerbating the problem of trying to determine if a Cyber Asset is a BES Cyber Asset that the entity neglected to apply the appropriate security controls to, or the Cyber Asset was not considered to be a BES Cyber Asset at all. The definition of BES Cyber Asset is not explicit enough to resolve this problem (see response to question 1). One solution is to create bright line criteria for the definition of a BES Cyber Asset based on the MW level that the BES Cyber Asset could “adversely effect” one or more of the BES Reliability Operating Services.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
No
Generally we agree with R5, however, since R5 is tied closely to R4, the Applicability column for Table R5 should be the same as the Applicability column for Table R4.
Yes
No
It appears that Requirement 7 has been written to satisfy FERC Order 706 at the expense of adopting sound security practices. The circumstances of an individual's termination or transfer should be taken into consideration when determining how long the Entity has to remove physical or electronic access. Versions 3 and 4 did a better job of addressing this by specifying different conditions such as "for cause" terminations.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
We agree with most of the implementation plan, however, leading up to the day that version 5 becomes effective, we assume that it will essentially be necessary for entities to be compliant with the current version (either version 3 or version 4) and version 5 at the same time. Is this a correct assumption in the opinion of the SDT? Has thought been given to any potential problems that this may cause? We suggest that during the implementation period, entities should be allowed to be compliant with either the current version or version 5 (on the basis of individual requirements and on the basis of individual BES Cyber Assets/Critical Cyber Assets), but not necessarily both versions at the same time. In other words, during the implementation period after regulatory approval, the entity should be deemed to be compliant if it meets the requirements of either the current version or version 5, and the entity should be able to make the selection of which version it is compliant with based on individual BES Cyber Assets/Critical Cyber Assets.
Individual
Jianmei Chai
Consumers Energy Company
Yes
We do not agree with the “Definitions”. The definition of “BES Cyber Asset” is not thoroughly defined. Using the word “adversely” makes the definition vague; i.e., how adverse? As a minimum, it should be replaced with “Adverse Reliability Impact”, from the NERC glossary, but even that may not remove all the uncertainty as to the extent a less than significant impact must be considered.
Yes
We have suggestions and do not agree with the criteria. The SDT is incorrect in stating that “most of these criteria are similar… as part of Version 4”. Version 4 provided the “bright line” criteria for defining “Critical Assets”, not cyber assets. Further tests (routable, dialup, etc.) were applied following that. The new criteria has the possibility to create substantially additional cyber assets requiring CIP compliance. Additionally, creation of the “Low Impact” category further blurs any “bright-line” concept in that nearly all other entity assets end up as “low” and under some CIP compliance. As such, the “similar” criteria is far from it.
No

We do not agree, as R1 invokes Att 1 for classification. Att 1 implies that all Blackstart resources identified in the TOs plan be categorized as medium impact. Previously, only those resources comprising the initial or primary cranking path were required. Rev 5 should reflect the same categorization philosophy. There is no justification for secondary and alternate sources to meet the compliance requirements and measures dictated by a “medium” categorization.
Yes
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-002-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
Yes
Yes
Yes
Yes
Yes
Yes
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-003-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
Yes
Yes
Yes
Yes
Yes
Yes
No

Confusing Access Revocation sub-requirements on resignations or terminations. Suggest combine all relevant sub-requirements into one with one defined access revocation period. Too short of a window for Access Revocation sub-requirement on reassignments or transfers. Suggest seven calendar days or at least three calendar days.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-004-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-005-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-006-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-007-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.

Yes
Yes
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-008-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-009-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-010-1, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-011-1, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.

Group
Idaho Falls Power
Richard Malloy
No
No
No
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
I can forsee a conflict with BES definition criteria, which excludes generation that is less that 75 MVA on an LN. What of the generation assets that fall between the 20 MVA registry criteria for GO / GOP registration and 75 MVA that lie on a Local Network? These assets would be responsible for the version 5 CIP standards yet are excluded in the BES definition? Would the generator be a cyber asset island? Perhaps threshold criteria for generation assts that match the BES exception criteria be

drafted into the low impact requirements.
Yes
Yes
No
Again a conflict with the BES exception criteria exists. Generation assets below 75 MVA are excluded on Local Networks, however no such provision is made in the CIP version 5 standards, thus a 20MVA generator must comply with the low impact criteria. A problem could arise where physical security is established around the generator but the transmission feeds, being a part of the excluded Local Network under the BES exception criteria are not, therefore rendering the physical security around the 20 - 75 MVA generator on an LN imaterial.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Group
PPL Corporation
Brent Ingbrigtson
Yes
The PPL Companies suggest the follow changes: • For the definition of Inter-Entity-Real-Time Coordination and Communication in the bullet points use the term Reliability Directive" in lieu of "Operational directives" (this should mirror the efforts of Project 2006-06, COM-002-3.) • Formal definitions should be provided for the terms Impact and Adverse as these are used throughout the other standards. See current and proposed change. Current: BES Cyber Asset A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. Proposed: BES Cyber Asset A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact the ability of a BES Element or Facility with which it is associated to perform one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the ability of the BES Element or Facility with which it is associated to perform the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. Rationale: Clarify that the BES Cyber Asset is associated with a BES Element or Facility.
Yes
Comments: See current and proposed change. Current: 2.1. Generation with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. Proposed: 2.1. Generation Facilities with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. Rationale: Editorial comment for consistency with similar language, e.g. generation Facilities, Transmission Facilities, etc. found elsewhere in Attachment 1, Part 2.
No
Current: "Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification." Further, part 1.1 of R1 states "Update

the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. Proposed: Change the current part number “1.1” to “1.2” and add part 1.1 as follows: “Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.” Further, part 1.1 of R1 states “Each Responsible Entity shall identify and categorize its BES Elements and Facilities in accordance with CIP-002-5 Attachment 1.” Part 1.2 states “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. Rationale: It is important to identify the applicable Elements and Facilities and their impact categorization for consistent auditing purposes. The PPL Companies request clarification of the apparent inconsistency in the standards where the requirement states that each Responsible Entity shall identify and categorized its High and Medium Impact BES Cyber Assets and Systems and state that Low Impact do not require discrete identification. However, in later standards (CIP-005-5 Requirement 1.1 for example) applicability applies to Low Impact BES Cyber Systems. This inconsistency occurs when other standard require specific identification of low impact facilities but the CIP-002 specifically states that there is no need to identify the Low Impact facilities This inconsistency needs to be addressed. PPL Companies suggest that Low Impact BES Cyber Systems not be subject to the requirements as they have already been defined as Low Impact.
Yes
No
The PPL Companies request clarification on the wording “…15 calendar months between reviews and approvals”. This apparently assumes that both a review and approval needs to be done, but if no changes are made would not a review of the policy suffice? The PPL Companies suggest that the standard language be changed to eliminate the need for approvals to be required when no changes have been made.
No
See response to question 3. The PPL Companies seek clarification on: Does the term “ALL” imply that people who only have access to Low Impact BES Cyber Systems be included?
No
The PPL Companies suggest that the term Storage Media be defined as discussed in the Rationale discussion.
No
See response to Question 3 The PPL Companies suggest the following changes to the standard. The

“bolded” words are the suggest changes. R1.1 requirement defines technical or procedural controls and the measure states to provide documentation of technical and procedural controls – suggest the two match. R1.2 should be all external routable and dial-up connectivity – add the word external The PPL Companies suggest that in R1.3, which requires a listing of inbound and outbound traffic be changed tip indicate that it would be appropriate to list outbound rule set and continue to the current deny all for inbound
No
The PPL Companies suggest the following changes be made: R1.1 uses operational or procedural controls, and the measure states operational and procedural controls, the two should match. R1.3 needs to be adjusted. The term ‘complementary and different” are both included, in the requirement but the measure only uses the term “different”.
No
The PPL Companies suggest removing the last sentence of the measure for R1.2 as it provides no benefit The PPL Companies also request clarification on the definition of “defined timeframe” in the last sentence of R2.2.
No
The PPL Companies request clarification on: R3.1 applies to BES Cyber Systems and not assets, does this allow for router and switches to not require TFE. R3.3 does not include testing for the installation of signature files, should this not be in the requirement R3.4 does this requirement reach all removable items, just as wireless mouse, keyboards, PKI devices, etc. Does an inventory of all transient cyber assets need to be maintained.
No
The PPL Companies suggest that in R3.2 adding additional wording so the 30 day clock starts after the actual incident has completed, instead of 30 days from when the incident is first reported. During those 30 days the process to return to normal operations should occur before the clock begins on the review and lessons learned activities.
No
The PPL Companies have the following concerns about the scope of the requirement: R1.3 is adding information protection to a requirement, keep information protection requirement all within CIP-011-5. R1.4 the verification of each backup upon completion seems to well exceed the order, consider that verification should be completed after major system changes or upgrades The PPL Companies suggest adding to R1.5 the following language “Preserve data, where technically feasible and critical to cause determination, for analysis…”
No
The PPL Companies observe that in requirement and measures for R2.2 the requirement and the measure are just the same wording. The PPL Companies recommend that the requirement be changed so that backup media is “…tested initially upon major system changes and at least once each calendar year…” The PPL Companies seek clarification on R2.3. Does a representative environment match what has been defined to the test environment as required in CIP-010-5 R1.5?
No
The PPL Companies suggest the following wording changes: In R3.1 suggest adding the wording

"…when BES Cyber Systems that have an effect on the recovery plan are replaced…" For R3.2 consider adding wording that 30 days after a recovery plan exercise, but 30 days after an incident is not enough time, so the wording should be after incident recovery as restoring operations should be the priority. R3.4 consider adding the following wording "…any organizational or technology changes that have an effect on the recovery plan within thirty days…"
Yes
No
The PPL Companies seek clarification on: In R1.4.1 should not all security controls be tested instead of "determining" what controls, how do you determine what controls might change with the change. R1.5.2 requires that entities document the test environment with every change that is tested. PPL suggests that only when the test environment changes should an entity be required t document the testing environment
No
The PPL Companies request clarification as to in R3.2 Can the testing be completed in a passive mode in production vs. an active test in the test environment?
No
The LSE should be removed from the Applicability Section (remove entire section 4.1.6 and 4.2.1) of all CIP Version 5 standards. With the NERC BOT approval of PRC-006-1 and subsequent FERC filing (Docket No. RM06-16-000), NERC has recognized that LSEs have no role in UFLS/UVLS programs. The Applicability Section for CIP Version 5 Standards includes LSEs with UFLS/UVLS equipment. This is inconsistent with NERC BOT's recognition that LSEs do not serve a role in such programs. Therefore it is unnecessary to include such a qualified LSE in the Applicability Section. NERC's reasoning was stated in their filing for FERC approval of PRC-006-1 and EOP-003-2: Some comments suggested potential confusion with existing programs or identifying responsibility for providing load shedding. The SDT believes these concerns are addressed in the continent-wide standard by assigning applicability to "Distribution Providers" and "Transmission Owners with end-use Load connected to their Facilities where such end use load is not part of a Distribution Provider's load." We [NERC] believe this covers all load and eliminates potential confusion regarding Load Serving Entities. See Petition of the North American Electric Reliability Corporation for Approval of Proposed New Reliability Standards and Implementation Plans Related to Underfrequency Load-Shedding, FERC Docket No. RM06-16-000, at p. 273. The SDT has revised the applicability [of PRC-006-1] to include both Distribution Providers and Transmission Owners as UFLS entities that may be designated by Planning Coordinators to implement a UFLS program. The interim changes to the NERC Statement of Compliance Registry were made to reflect concerns about the definition of the LSE as a "facility owning entity" as opposed to the Distribution Provider. As demonstrated in the NERC LSE workshop, currently approved Functional Model and the interim Registry Criteria changes, for standards purposes the DP is the "wires" connection to the electric system and owner of the UFLS tripping equipment. This may be inconsistent with previous usage of the same terms in some parts of the country. The Version 0 applicability for UFLS was set prior to the Registry and determined on the then general understanding of the Functional Model and industry usage. The current Functional Model is much clearer on this issue and designates the DP as the facility owner. Since NERC has stated that the Registry Criteria now has an interim step to correct the issue, it is expected that the Registry Criteria will change as the standards are re-evaluated for appropriateness. The SDT believes that this standard is in line with the direction taken by the interim changes and the approved Functional Model. See Petition of the North American Electric Reliability Corporation for Approval of Proposed New Reliability Standards and Implementation Plans Related to Underfrequency Load-Shedding, FERC Docket No. RM06-16-000, at p. 331. This position is consistent with NERC's reasoning throughout the development of PRC-006-1: The SDT recognizes that the Functional Model Version 5 and the Statement of Compliance Registry cause confusion regarding the involvement of the LSE in UFLS

programs but the SDT refers to the section covering the Roles in Load Curtailment in Version 5 of the Functional Model Technical Document; “For non-voluntary curtailment, such as automatic underfrequency and undervoltage load shedding and manual load shedding, the Load-Serving Entity identifies which critical customer loads should be excluded from curtailment for public health, safety and/or security reasons.” See Consideration of Comments on Initial Ballot — Project 2007-01 Underfrequency Load Shedding Date of Initial Ballot: July 7-17, 2010 at p. 4.
Individual
Tom Bowe
PJM
Yes
• An explicit and exact definition of what a BES Cyber System is and what components are included in a BES Cyber System would be helpful here. Some examples may aid in this understanding. • What is the starting point for CIP 002-5 . Do we start with ALL cyber systems and then group them into 3 categories based on impact? Or do we identify ONLY those cyber systems that are used in an entity’s mission (in other words exclude payroll etc) and then classify them based on impact.
Yes
In section 2.3--Define what BES Adverse Reliability Impacts means (Adverse). Section 2.8, define derivation in “critical to the derivation of IROLs.” Is this meant to be definition instead of derivation? In section 2.10, more information is needed on Nuclear Plan Interface Requirements.
No
• Following statement not needed “All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.” While PJM appreciates the attempt to lessen the paperwork around this requirement, entities will still need to maintain this list inherently when the listing of BES Cyber Systems is created and each system is classified. • Section 1.1 – “Update the identification and categorization within 30 calendar days”. Does this update require sign-off from Sr. Manager or delegate? • Section 1.1 ‘…categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category’ –What if the change is from higher impact to lower impact category – is that expected to be captured in the annual review ?
No
• In M2. Reference to CIP Senior Manager should include “and delegate”. • In section 1.2 (Evidence Retention) change for retaining evidence is to three years from previous plus current year. Three years can add significant amount of data retention, not necessarily for CIP-002 but for other standards. Our preference is to not change to 3 years. • Section 1.2 the word compliant is mis-spelt as complaint.
Yes
No
• Should include “document CIP Senior Manager” as noted in R6. • This should be a Low Violation Risk Factor, not a Medium. This requirement and rationale is administrative and does not pose a medium risk factor
No
• Following statement should include “minimum” “…protection of its BES Cyber Systems and addresses, at a minimum, the following topics”. • In the list in 1.1 – 1.10, what about these topics should be included in policy? Topics better suited might be common domains of security. • In M2—with a numbered listed the statement should read “Evidence must include…”. • In the second measure in M2 implemented should be replaced with documented.
Yes
• In the M2—with a numbered listed the statement should read “Evidence must include…”. • Dated signature in M2 should be updated to include, electronic approval and workflow evidence.
No
• “Elements of” in the requirement should be removed. “Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function”.

Yes
No
• In R6, formatting error in copy reviewed. “Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change2”. The “2” should be a super script. • In M6, any acceptable form of evidence in M5 should be acceptable in M6. • In Part C, section 1.2 (Evidence Retention) change for retaining evidence is to three years from previous plus current year. Three years can add significant amount of data retention, not necessarily for CIP-002 but for other standards. Preference is to not change to 3 years.
No
Violation Risk Factors for R1 should be Low—see comments in #6 above
Yes
No
• For R2, are all of the roles expected for training included in the table? Is an entity expected to have separate training for each of the items listed in the table, or can the training be all inclusive and given to everyone? • For R 2.5 Visitor Control Program – what are the requirements for such a program • In Part 2.10, is this referring to general networking concepts and the network layout of an entity? Is vendor training sufficient for this area (i.e. Cisco training)?
Yes
No
• Part 4.2 – This requirement appears to lessen the requirements for international individuals. While we appreciate the standards drafting team’s considerations, it seems that when dealing with security some restrictions need to be applied around using the exception process. • Part 4.3 –We believe that the term “criteria” should be left out of the requirement. Reviewing PRAs is a highly subjective process that is handled on a case by case basis, and we believe that only a process that helps drive decisions should be included here.
Yes
R 5.2 Update each personnel Risk Assessment at least once every seven calendar years. Is it OK if the repeat PRA is not within 7 years of the original PRA as long as it is within seven calendar years?
Yes
R 6.1 and R 6.2 - ‘CIP Senior manager or delegate shall authorize’ - Most organizations have defined processes for who can authorize this type of access. Adding the phrase above only increases administrative overhead to sign and maintain delegation letters. Can these requirements be reworded so that CIP Senior manager does not have to be involved in authorizing –either directly or through delegates? Measures for R 6.1 and R 6.2 have numbered list of acceptable evidence. The heading should read ‘Evidence must include’. Otherwise the list should be a bulleted list and entities can choose to maintain one more items from the list.
No
• Part 7.2 –In reassignments or transfers knowledge transfer can take extended period of time (some positions that are recently vacated also are not immediately filled when transfer/reassignment is completed). Stipulations should be present to allow for this knowledge transfer to ensure that access is not revoked before it is truly not needed any longer. • The change rationale does not match part 7.2. As stated above, the requirement in the table currently reflects the need to cut access immediately as of the transfer, rather than allowing for proper transition plans to be executed. • Measures for 7.2 contain numbered list. The opening line should read ‘Evidence must include’. Or the list should be changed to a bulleted list.
Yes
No
• Part 1.1 – Examples of topics to cover/address should be listed. Requirements state “define technical or procedural”, while the measures state “documented technical and procedural controls”.

For an application “either or” would be needed. • Part 1.5 – In measures section a grammar update for, “configuration files of an intrusion detection system(s)” • The measures section is a bulleted list – implying an entity can choose which evidence measures to maintain. It should actually be a numbered list – entities should have all items listed in this section. • There should be clarity on the location of intrusion detection systems. In the current version there is no consistency of interpretation among the CEAs.
No
• Part 2.1 – Source is not clear. In network terminology, defining the source would be helpful. Examples of User Interactive Remote Access would also be helpful for this requirement. Examples of acceptable ‘Intermediate Devices’ would be helpful too. • Part 2.3 - What is the SDT definition of multi-factor authentication? This would be helpful for the requirement.
No
All VSL’s are listed as severe. A defined range or breakdown of levels of non-compliance would be better suited for R1 and R2.
No
• Part 1.1 – Applicability: A list of what “Low Impact BES cyber systems “are, is needed. - Requirements: What is the difference between “operational and procedural controls”? “ Define operational or procedural” is listed as “ define operational and procedural” in measures column, should be consistent. - Measures: What type of evidence does the measure require? • Part 1.2 – Requirements: “ Defined Physical Boundaries”, terminology needs to be used in Measures, for consistency. • Part 1.3 – Should we have separate ESP access point for Low and High impact BES Cyber systems? • Part 1.5 – Why are the requirements between 1.4 and 1.5 separated?
No
• Part 2.1 – Requirements: Define “continuous” • Part 2.2 – Requirements: “Defined Physical Boundaries” should be added to “A process requiring manual or automated logging of the entry and exit”, in order to match the Measures.
No
• Part 3.1 – Requirements: What would be the requirements for systems already in place at time of commissioning? • Part 3.2 – Applicability: Clarify what is meant by “Physical Access”
Yes
No
• Part 1.1 – Requirements: Clarify what “restrict access” means. • Part 1.2 – Requirements: Clarify what restrict means in “restrict the use of unnecessary…” The change description and justification appears weak on the basis the SDT was encouraged to address unused physical ports. A better defined position would be helpful to understanding of 1.2.
No
• Part 2.1 – Requirements: This needs to be written in the form of a requirement. (not a statement) • Part 2.3 – Requirements: “Execute the remediation plan” should be added to this requirement. These requirements aren’t matching up with the “Change Rationale”. • Part 2.3 - Measures – Acceptable evidence should also include workflow evidence from the Change Management system.
Yes
Requirement: Clarify what type of “connection"
No
• Part 4.1 -Requirements: 4.1.1 – Clarify whether it’s just only for Electronic Access Point for 4.1.2 – 4.1.4. 4.1.4 – This is too broad. Defining potential malicious activity would be helpful to understanding of 4.1.4. Metrics around successful or failed attempts would benefit and provide clarity to requirement. • Part 4.3 - Doesn’t match up with 4.5. (Clarity to review summary of two weeks by next calendar day or next calendar day for reviews of failures). • Part 4.5 – Requirements: Clarify what “a summarization or sampling” means.
No
• Part 5.2 – Most organizations have a process for who can authorize use of shared, default, administrator or generic accounts. Adding the phrase ‘CIP Senior Manager or Delegate’ only adds

administrative overhead. Consider rewording this phrase. • Part 5.3 – Requirement does not match to change rationale. • Part 5.4 – Requirements: Move “BES Cyber Assets, Electronic Access Control or Monitoring…” to the “Applicability” section
Yes
Comments: Consider adding a sliding scale of percentage of assets where an entity failed to document ports, monitoring etc. rather than classifying everything into High or Severe VSL.
No
• Requirements: Generally 1.1 is not posed as a requirement. Similar wording of other requirements is needed. “Responsible entity shall have…” • Measures: the use of the word “targeting” implies pulling in other than CIP related impacts to the BES. Reference in measures section should only be for CIP. • Generally 1.2 is not posed as a requirement. Similar wording of other requirements is needed. “Responsible entity shall have • 1.1, 1.2, 1.3 Applicability section should list the types of assets to which this requirement applies. ‘All responsible entities’ seems to broad, and can be interpreted to include assets not in the high, medium or even low impact BES cyber systems
No
• 2.1 Clarify “deviations” (…”recording of deviations taken from the plan”…. • Also clarify if the deviations should be recorded in real time or can that be done after the incident is complete • 2.2 Clarification is requested regarding the statement of “initially upon the effective date.” Does this mean that the plan has to be effective on the effective date but not before, can the plan be effective prior to the standards effective date, etc.
No
• 3.2 – The following statement from R2.1 “recording deviations from the plan” appears to align in 3.2. Clarification on why it is in R2.1 would be helpful. • 3.4 - Organizational changes should be responsibility or role changes
Yes
No
• Part 1.1 – Requirements: Examples of conditions are needed. • Part 1.3 – Requirements: “backup, storage,..” what can be acceptable as documentation of storage? This can become cumbersome when dealing with virtual environments. • Part 1.4 – “Part” in the first, second and third column should be “Applicability”, “Requirement” and “Measures” respectively. Requirements: “initially after backup” terminology needs further clarification. This seems to give no window of failure. Typically, we would investigate if a successful backup has not occurred within 48 hours. • Part 1.5 – Requirements: More defined examples of preserved data are needed.
No
• Part 2.1 – Requirements: In the third bullet point, it is mentioned “operational exercises.” But in the Rationale “Functional exercises” is defined. Clarification is requested regarding the statement of “initially upon the effective date.” Does this mean that the plan has to be effective on the effective date but not before, can the plan be effective prior to the standards effective date, etc. • Part 2.2 – Clarification on configurations is needed (compared to baseline)? • Part 2.3 – If calendar year is defined not to exceed 15 months, how does 3 calendar years translate to 39 calendar months?
No
• Part 3.1 - Measures- ‘or when BES Cyber systems are replaced’ –This should be reworded to the effect that when there are updates to High or medium impact BES Cyber Systems or assets, the recovery plans should be updated within 30 days of update to the list. • Part 3.4 - “Part” in the first, second and third column should be “Applicability”, “Requirement” and “Measures” respectively. Organizational changes should be responsibility or role changes
Yes
No
• Part 1.1 – In requirements instead of “develop a baseline configuration” it should be read as “create and maintain a baseline configuration” ♣ 1.1.3. Non-commercial (open source) should also be tracked. ♣ 1.1.6. This is too broad. By “Any security-patch levels” does it mean security patch levels of the operating system or the version? • Part 1.2 – Requirements: Grammatical Error “Authorized”

should be “Authorize” • Part 1.3 – Requirements: “including identification and categorization of the BES Cyber Systems..” is not clear. How does this fit in with “updating baseline configuration”? Should this refer to specific assets as opposed to the system? Measures: Need examples of changes other than asset recovery plans. • Part 1.4 – Requirements: 1.4.1 – Define “cyber security controls”. • Part 1.5 - An entity may not have comparable test environment for every BES Cyber system of high , medium or even low impact. There should be room to use non-CIP assets (even if they are in production) for testing prior to implementing in a CIP environment.
No
• Part 2.1 – Requirements: add “to the baseline” at the end of the sentence. Measures: What is considered as “records of investigations..” (email chain, change record)?
No
In relation to the Compliance section Part 1.2 Evidence Retention, What does “since the last audit” refer to? Explanation is required (does audit refer to a regional entity)? Spelling error “complaint” should be “compliant” in last sentence of first paragraph Part 1.2 Evidence Retention.
Yes
No
• Part 1.1 – Requirements: Generally 1.1 is not posed as a requirement. Similar wording of other requirements is needed. “Responsible entity shall have …” ---“One of more methods..” is not suitable for a requirement. Need a clearer understanding of what identify refers to. Measures: These measures are weak. • Part 1.2 - Generally 1.2 is not posed as a requirement. Similar wording of other requirements is needed. “Responsible entity shall have…” --“Part” in the first, second and third column should be “Applicability”, “Requirements” and “Measures” respectively. - Requirements: “Access control..” is not suitable for a requirement - Measures: In the first bullet point for “the document process” there is no requirement specified. According to the second bullet point, it is read “Records from an…..need to know basis” should this be enforced in a need to know basis? There is no requirement on need to know basis Third bullet point—difficult to track authorized individuals to a locked file cabinet. • Part 1.3 – Again, in general 1.3 does not pose as a requirement. “Part” in the first, second and third column should be “Applicability”, “Requirements” and “Measures” respectively. - Requirements: Clarify the time frame on “Initially upon the effective date…” - “assess adherence to its BES Cyber System Information protection process” “its”, is vague in this wording, clearer meaning would be helpful. R 1.3 – ‘Initially upon the effective date’ – How far in advance can the assessment be completed ?
No
• Part 2.1 – Measures: The requirement for this measure needs to be clarified. • Part 2.2 – Measures: Update is needed to leave open to other ways to prevent unauthorized retrieval of Information (ie. Encrypting, locking in safe or other physical securing)
No
• R1 – Severe should be only if all three items identified are missed. If not all are missed, a lower VSL should be listed. • R2 – High VSL- severity should be based on number of occurrences. Severe VSL- there is no requirement to document. Only to take action or implement process should not be listed as severe.
No
Plan should be a rolling implementation.
Individual
Chris Higgins / BPA CIP Team
Bonneville Power Administration
Yes
1 - BES Cyber Asset A cyber asset that if rendered unavailable degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one of more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The time frame (15 minutes) is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive

instructions to operate, and the time in which the operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. Comment: BPA believes the definition for BES Cyber Asset is very difficult to understand. BPA believes the author is trying to say, regardless of when the Cyber Asset actually broke, the Cyber Asset would cause an adverse impact to the BES within 15 minutes of when it is needed. Recommended Change: A Cyber Asset that if rendered unavailable, degraded, or misused would, when required for real-time operation, adversely impact one or more BES Reliability Operating Services within 15 minutes. The 15 minutes does not start at the time of unavailability, degradation, or misuse of the Cyber Asset. It starts when the Cyber Asset is next required to support one or more of the BES Reliability Operating Services. Redundancy shall not be considered determining the availability of the Cyber Asset. A Transient Cyber Asset is not considered a BES Cyber Asset. 2 - BES Cyber Security Incident A malicious action or suspicious event that: • Compromises or was an attempt to compromise the Electronic Security Perimeter, or • Disrupts, or was an attempt to disrupt the operation of a BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary Comment: BPA believes that malicious attempts are Cyber Security Incidents, regardless of their success. In addition, BPA believes that compromise of BES Cyber System Information should also constitute a BES Cyber Security Incident. Recommended Change: A malicious action or suspicious event which through an investigation and escalation process has been identified that: • Compromises or was an attempt to compromise the Electronic Security Perimeter, or BE Cyber Security Information • Disrupts, or was an attempt to disrupt the operation of a BES Cyber Asset or BES Cyber System • Results in unauthorized physical access into a Defined Physical Boundary 3 - BES Cyber System One or more BES Cyber Assets that are typically grouped together, logically, or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System. Comment: BPA believes the CIP-002 Standard appears to allow the identification and categorization of BES Cyber Assets OR BES Cyber Systems. However, the definition BES Cyber Security Incident and most of the CIP Version 5 standards assume that every identified BES Cyber Asset is part of an identified BES Cyber System. There is no definition for Maintenance Cyber Asset. Can a BES Cyber System include Cyber Assets that are not BES Cyber Assets? One or two of BPA's current Critical Cyber Assets have non-critical Cyber Asset components. The Applicability section of the standards includes a definition for Associated Protected Cyber Assets that are associated with a corresponding High or Medium Impact BES Cyber System. BPA suggests that all BES Cyber Assets must be identified as a component of an identified BES Cyber System and whether a Cyber Asset that is not a BES Cyber Asset can be part of a BES Cyber System be added to the definition. Recommended change: One or more BES Cyber Assets that are typically grouped together, logically, or physically, to operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. 4 - BES Cyber System Information Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans. Comment: BPA infers that the large and chunky sentences are confusing and difficult to understand. BPA suggests bullet lists so the reader and implementer can wrap their arms around one or many of the concepts (requirements) in the standard or definition. Recommended change: BES Cyber System or BES Cyber Asset information that includes: • Security procedures developed by the responsible entity, including BES Cyber System disaster recovery plans and BES Cyber System incident response plans; • Network topology or similar diagrams; • BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); • Floor plans that contain BES Cyber System Impact designations; • Equipment layouts that contain BES Cyber System Impact designations. • BES Cyber System disaster recovery plans, or • BES Cyber System incident response plan 5 - BES Reliability Operating Services BES Reliability Operating Services are those services contributing to the real-time reliable operation of the Bulk Electric System (BES). They include the following Operating Services: Comment: The definition says '…those services contributing to the real-time…' The word contributing is too broad and may encompass cyber assets/systems that do not significantly impact the reliable operation of the BES. Most of the verbiage in this definition should be included as an attachment in CIP-002 if it is only used

for identification of BES Cyber Assets and BES Cyber Systems. Inter-Entity Coordination and Communication is not a service but is a communication method for other Reliability Operating Services. Recommended change: BES Reliability Operating Service (ROS) is a service that is directly essential to the real-time, reliable operation of the Bulk Electric System (BES). BPA also suggests moving the services to an attachment or guidance document as indicated above, make each ROS Service its own definition, or put the definition of the specific service only in its own standard, where used. Remove Inter-Entity Coordination and Communication as a sub-definition of ROS. At a minimum, limit this to real-time ICCP data, which equals facility operational data and status. 6 - CIP Exceptional Circumstances A situation that involves one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability. Comment: BPA asks, "Should this not also include the threat of the risks that are defined?" This definition does NOT cover all exceptional circumstances. A Cyber Security Incident is limited to "a malicious act or suspicious event". It is possible that a BES Cyber Asset would fail in such a way that outside experts were needed to fix it. In most cases there is a reaction to a threat that would invoke exceptional circumstances until such time as it has been determined whether or not the threat is real. Recommended change: A situation (which includes the immediate threat or real event) that involves one or more of the following conditions: a risk of injury or death, a natural disaster, to public safety, health, welfare civil unrest, damage or destruction to Bulk Electric System equipment, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or the impediment of large scale workforce availability. 7 - CIP Senior Manager A single senior management official with overall authority and responsibility for leading and managing implementation of the requirements within the NERC CIP Standards. BPA supports "7 – CIP Senior Manager" and has no comments or concerns at this time. 8 - Control Center One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations: • Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, • Inter-utility exchange of BES reliability or operability data, • Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES, • Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function, • Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES • Coordination of BES restoration activities. BPA supports "8-Control Center" and has no comments or concerns at this time. 9 - Cyber Assets Programmable electronic devices including the hardware, software, and data in those devices Comment: The term should be singular (Cyber Asset and device) not plural (Cyber Assets and devices). The word "programmable" is not definitive enough to clearly identify all the electronic devices subject to these Standards. Recommended Change: Cyber Asset - Electronic device including the hardware, software, and data in the device that is programmable or configurable. 10 - Defined Physical Boundary (DPB) The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside and for which access is controlled. Change Rationale: "Defined Physical Boundary (DPB)" replaces "Physical Security Perimeter." Previous versions of the CIP standard focused on the development of a completely enclosed Physical Security Perimeter (PSP) ("six-wall" border) and managing access though this boundary. This has proven difficult due to the nature of the operating environment for many electrical utilities, especially in field locations. The intent of this standard is to focus on the controls put in place to restrict access rather than solely focusing on the PSP and a boundary protection model for physical security. Comment: BPA believes the wording is inconsistent with other usage in the standards. BPA suggests ensuring that the rational statement remains with the definition, or find some way of combining the two. Recommended change: BPA suggests adding "Monitoring" to produce the following: The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems reside and for which access is controlled. 11- Electronic Access Control or Monitoring Systems Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems BPA supports "11-Electronic Access Control or Monitoring Systems" and has no comments or concerns at this time. 12 - Electronic Access Point ("EAP") An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets. Comment: Does this purposefully ignore serial communications in a continuation of the differentiation built into the original

CIP-002 R3. Recommended Change: Any interface to an ESP which provides access to BES Cyber Systems or BES Cyber Assets which control or restricts Electronic (routable or dial-up) communications to those assets. 13 - Electronic Security Perimeter ("ESP") A collection of Electronic Access Points that protect one or more BES Cyber Systems. BPA support "13 – Electronic Security Perimeter ("ESP")" and has no comments or concerns at this time. 14 - External Connectivity Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter. Recommended change: Routable or dial-up data communication through an Electronic Access Point into an Electronic Security Perimeter between a BES Cyber Asset and a device external to the Electronic Security Perimeter. 15 - External Routable Connectivity The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol. BPA supports "15 – External Routable Connectivity" and has no comments or concerns at this time. 16 - Interactive Remote Access Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors or consultants Recommended Change: Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and that is not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Interactive remote access can be initiated from: Cyber Assets used or owned by the Responsible Entity; Cyber Assets used or owned by employees; or Cyber Assets used or owned by vendors, contractors, or consultants. 17 - Intermediate Device A Cyber Asset that: 1) may be used to provide the required multi-factor authentication for the interactive remote access; 2) may be a termination point for required encrypted communication; and 3) may restrict the interactive remote access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside the Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network. Comment: INTERMEDIATE DEVICE: Again, BPA applauds the inclusion of this definition. However, as stated, BPA believes a Cyber Asset can fail all the conditions and still be considered an Intermediate Device. Recommended Change: A Cyber Asset that meets one or more of the following conditions: - Is used to provide the required multi-factor authentication for the interactive remote access; - Is a termination point for required encrypted communication; and/or - Restricts the interactive remote access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate devices may be located outside the Electronic Security Perimeter, as part of the Electronic Access point, or in a DMZ network. BPA also believes the last sentence could be deleted. If it is not deleted, it should be reworded to make it clear that the three locations listed are not the only possible locations. BPA suggests; The intermediate device locations may include: - Outside the Electronic Security Perimeter, or - As part of the Electronic Access Point, or - In a DMZ network 18 - Physical Access Control Systems Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers. BPA supports "18 – Physical Access Control Systems" and has no comments or concerns at this time. 19 - Protected Cyber Asset A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the BES Cyber System. A Transient Cyber Asset is not considered a Protected Cyber Asset. Comment: BPA believes this definition relies on the definition of "Electronic Security Perimeter". Given that definition, the definition of Protected Cyber Asset becomes "A Cyber Asset connected using a routable protocol within a collection of Electronic Access Points that protect one or more BES Cyber Systems that is not part of the BES Cyber System." This implies that a Protected Cyber Asset is an Electronic Access Point. Recommended change: A Cyber Asset located within an Electronic Security Perimeter, but which is not a part of an associated BES Cyber System but is routably connected to an associated BES Cyber System. A Transient Cyber Asset is not considered a Protected Cyber Asset. 20 - Reportable BES Cyber Security Incident Any BES Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service. Comment: BPA suggests rewording this definition for clarity. Recommended change: Any BES Cyber Security event that has been officially escalated to the level of a Cyber Security Incident which has compromised or disrupted a BES Reliability Operating Service. 21 - Transient Cyber Asset A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset 2) used for

data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System. Comment: BPA believes this should include devices such as sniffers and scanners on a temporary basis. In additions, the references to “Maintenance Cyber Assets” in the standards need to be replaced by “Transient Cyber Assets”. Recommended Change: A Cyber Asset that is: 1. Located on a network segment protected by one or more Electronic Access Points protecting BES Cyber Assets or directly connected to a BES Cyber Asset, and 2. Connected to such a network segment or BES Cyber Asset for 30 days or less. Transient Cyber Assets are not considered Protected Cyber Assets. Terms to be Retired Comment: BPA believes that a Cyber Security Incident should be included in the list since the BES Cyber Security Incident is being added. Additional Comments Definitions in general: BPA believes that if a term applies to more than one standard, then it should be a defined term; however, if a term is used exclusively with a specific standard, then leave it in that standard only. Effective dates: Suggest making the Effective Dates paragraphs easier to decipher. These paragraphs are in every standard. They are extremely confusing to read and require further explanation in footnotes. Recommendation: 18 Months Minimum – The Version 5 CIP Cyber Security Standards shall become effective on the later date: January 1, 2015; or the first calendar day of the seventh calendar quarter after the applicable regulatory approval date. However, if Version 4 CIP Cyber Security Standards do not become effective, Version 3 CIP Cyber Security Standards remain in effect until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.
Yes
BPA suggests the following recommendations to High Impact: • Modify sentence to say “Each BES Cyber Asset or BES Cyber System used by and located at:” as the definition would already address the 15 minute consideration and no need for duplication here. • BPA suggests applying this to the Medium Impact sentence as well, but include the “not included in Section 1 above” portion. BPA recommends that 2.7 should have increased values assigned to lines with power transformer installations above a predefined nameplate rating at those 200kV and above substations since they are extremely important to the BES, extremely expensive, and have a very long lead time. Or revert back to the version 4 bright line criteria statement addressing number of 300kV lines only. Under the Transmission portion of Medium Impact the total aggregated weighted value indicates “3 connected 345 kV lines and 5 connected 230kV lines”–should that say “or” rather than “and” since then the aggregated totals would be 7000 rather than 3000 which I believe is the threshold desired. BPA also requests that the drafting team provide direction on how this apparent inconsistency in time horizons should be addressed in the cyber system categorization process. In Attachment I of CIP 002-5, there appears to be a conflict in time horizons for applicability of the standard. There are several references to the 15 minute "adverse impact" criteria. However, in the first sentence under Balancing Load and Generation in the Guidelines and Technical Basis section, the language suggests the need to include systems involved in monitoring and controlling generation and load "in the operations planning horizon". In the Situational Awareness section, there is also mention of Current Day "and Next Day" planning systems. Moving from a 15 minute impact criteria to the operations planning and next day planning horizons would significantly increase the scope the standard for BPA and likely for many other entities as well.
No
BPA asks, “Does this mean that we only have to update the list within 30 days if both conditions are true?” BPA believes that R1 should be broken into more requirements, one to address identification of the BES Cyber Assets and BES Cyber Systems and one or more to address updates due to changes to BES Elements and Facilities. CIP-002-5 R1 reads, "Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment 1 - Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification." (Emphasis added) BPA interprets CIP-002-5 to limit responsibility for compliance with the CIP standards for any BES Cyber Asset or BES Cyber System to the owner of that asset or system. It follows that the inverse is also true: i.e. only the owner of a BES Cyber Asset or BES Cyber System can be responsible for CIP compliance. Responsibility for CIP compliance will always fall to the asset owner. BPA believes this adds much needed clarity and strongly supports this position. BPA also supports the position that only one Entity be responsible for any BES Cyber Asset or BES Cyber System, and that the responsible Entity must be the owner or co-owner of the asset or system. BPA

supports this language because it clarifies responsibility and avoids potentially expensive and inefficient duplication of compliance efforts. BPA requests that the drafting team clarify whether they contemplate that scheduling systems would adversely impact one or more BES Reliability Operating Services within fifteen minutes if rendered unavailable, degraded, or misused. For example, does the potential for cyber attack on e-tagging systems before tags are loaded into EMS prior to the ramp suggest that scheduling systems should have a High or Medium Impact Rating? BPA requests that the drafting team define or clarify the term "generation control center" listed as having a medium impact rating in CIP-002-5 Attachment 1, at 2.13. Specifically, BPA requests that the drafting team clarify the extent of control over generation present at a "generation control center."
No
BPA would vote yes if the words “Initially upon the effective date of the standard” were changed to “within 12 months prior to effective date of the standard.
Yes
Yes
No
BPA believes that each organization should be able to create and implement cyber security policies that are suitable to their environment. The CIP version 5 standards assume a one size fits all approach across the industry. R2 Guideline: 2.3. Remote Access • Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating interactive remote access This line implies that VPN access is the only an acceptable interactive remote access method. Don't be so restrictive. Allow for Secure Shell, and Secure Socket Layer, and any other secure method we have available to us now and in the future. The standard is mandating an entity’s policy be too prescriptive and does not allow the usage of other technologies.
No
Comment: BPA believes that requiring a review upon the effective date of this standard ignores the fact that Responsible Entities already have Cyber Security Policies under Version 3 and are already reviewing them annually. BPA believes the statement, "initially upon the effective date of the standard" should be removed from the requirement. Recommendation: BPA recommends the following change: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals.
Yes
BPA believes the requirement is presently being completed under the current effective standards.
Yes
BPA believes the requirement is presently being completed under the current effective standards.
Yes
BPA believes the requirement is presently being completed under the current effective standards.
No
BPA believes the proposed VRFs and VSLs, associated with R2, assume all entities have implemented all mandated cyber security policies listed in CIP-003 version 5. BPA believes this does not take into account some entities may not have the need to implement certain cyber security policies based on current business practices and technologies in use (or not in use). BPA considers the level of the VRFs and VSLs are appropriate for R1, R4, R5, and R6.
Yes
BPA believes the requirement is acceptable as written and has no comments or concerns at this time.
Yes
Yes
The CIP004 R3.2 requirement states that training must be provided prior to access being granted and that training must be completed on an annual basis. However, it does not define what actions must occur if training is not completed within the stated timeframe. BPA recommends the inclusion of a

requirement specifying the actions to be taken with regard to authorized electronic or unescorted physical access in the event of an individual exceeding the annual timeframe for annual training.
No
BPA believes the additional language within R4.4.2 regarding assessment of residence, schooling and employment falls outside the boundary of a criminal history check. Verification of schooling, employment and residence is typically a function of employment eligibility verification and should not be considered as part of the assessment processes for risks associated with access to sensitive areas. Such risk analysis is typically based on character, trustworthiness and any revealed patterns of adverse behavior, which are only able to be assessed in reviewing the criminal history check. It is the opinion of BPA that items and issues that fall outside the scope of a criminal background investigation are not relevant when contrasted against the risks to BES Cyber Systems. Further, it is imprudent to require entities to perform positive and negative personal risk assessments based on the location of an individual's school, residence, and employment history. BPA recommends making the following change to CIP-004 R4.4.2: • A criminal history check must be performed prior to granting authorized electronic access or authorized unescorted physical access to BES Cyber Systems. Assessment of the criminal history check must be conducted to assess character, trustworthiness and any revealed patters of adverse behavior.
Yes
No
BPA believes that R6.4 could be improved and suggests making the following change: • Verify at least once each calendar quarter that individuals currently provisioned for unescorted physical access or electronic access to BES Cyber Systems are authorized for such access. BPA believes that R6.6 could be improved and suggests making the following change: • Verify at least once per calendar year, but not to exceed 15 calendar months between verifications to confirm that access privileges to "BES Cyber System Information" are correct and the minimum necessary for performing assigned work functions
No
BPA believes that significant issues and problems are created by the proposed requirements throughout CIP-004 R7 and its sub-requirements. BPA believes that R7.1 should require Responsible Entities to establish documented timelines for access revocations. This presents a potential for violations due to ambiguity. BPA recommends making the following change to CIP-004 R7.1: • For resignations or terminations, the RE shall establish guidelines and processes that adequately protect Unescorted Physical and/or Interactive Remote access to BES Cyber Systems following the time of the resignation or termination • Remove section (ii) of R7.1, and section (ii) of R7.2 BPA recommends making the following change to CIP-004 R7.3: • Modify requirement R7.3 to read… For resignations revoke the individual's access to BES Cyber Systems Information within a timeframe defined by the Responsible Entity – not to exceed 30 days. For terminations, revoke the individual's access to BES Cyber Systems Information within a timeframe defined by the Responsible Entity – not to exceed 7 days. BPA recommends making the following change to CIP-004 R7.4 and 7.5 • Remove requirement R7.4 and R 7.5 altogether as it is impractical to implement. Given the number, type, geographical location, and the inability to centrally manage all the devices within scope of these requirements makes the enforcement of the requirement impractical to implement. Applying CIP-004 R7.4 and R.7.5 at the BES Cyber Asset level (i.e. relays) cannot be accomplished within the stated 30 day timeframe. To do so would require a series of approved outages for every relay designated as a BES Cyber Asset followed by individually changing the Access Level Codes to each relay. Bonneville and other region entities support each other which results in mutually shared access codes. This effectively means individuals may posses the ability to access BES Cyber Assets within several entities' operating areas. Therefore, if an individual moves out of a job that requires access to BES Cyber Assets, every relay in every operating area would require access codes to be changed, which would require a physical visit to every impacted relay.
No
As the Violation Risk Factors and Violation Severity Levels point to requirements and statements that are in question or require modification, BPA is unable to adequately answer this question until the standards are complete.
No

CIP-005 R1.2: No - BPA has concerns with the Applicability definitions. BPA requests clarification in the standard regarding the following questions: • If you can connect to a serial device through a device such as a terminal console that is connected to a routable network, does that cause the serial device to be in scope? • Would a serial device that is capable of "Reverse Telnet" be an included device? • Are EAPs required at points in the network where serial communications are bridged to Ethernet networks? CIP-005 R1.3: Yes - BPA supports CIP-005 R1.3 CIP-005 R1.5: Yes - BPA supports CIP-005 R1.5
No
CIP-005 R2.2: No - BPA also finds "Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session." to be too prescriptive. If the interactive session is only for the purpose of showing maintenance logs or locations of faults, confidentiality and integrity may not be a requirement. If only integrity is a requirement, this can be handled with a hash of the data, not necessarily full encryption. In this case, a blanket requirement for encryption is far too encompassing and would require limits and specifics on the types of remote sessions that should be protected before we would agree to this requirement. In the end, for this matter, BPA should be allowed to determine our confidentiality and integrity needs and apply the appropriate protections as necessary.
No
CIP Version 5 takes the important step of moving toward a risk-based assessment approach by requiring Entities to classify assets and systems as High, Medium and Low Impact to the BES. However, the VSLs and VRFs do not reflect this risk-based approach. For example, in CIP-005-5, all VSLs are classified as Severe, yet CIP-005-5 R1.1 applies only to Low Impact BES Assets and Systems. BPA believes that the VSLs and VRFs in all CIP Standards should be reassessed based on the impact classification of the Assets and Systems covered by each Requirement. As an example, the Severity Levels for CIP-005-5 R1 could be rewritten as shown below. Column Heading "Requirement" = R1 Column Heading "Lower VSL" = For Low Impact Systems, Responsible Entity failed to document procedural controls to restrict access to a specific System. Column Heading "Medium VSL" = For High and Medium Impact Systems, Responsible Entity failed to document method for detecting malicious communication at each EAP. Column Heading "High VSL" = N/A Column Heading "Sever VSL" = The Responsible Entity did not establish Electronic Access Points to control and secure access to its High and Medium Impact BES Cyber Systems
No
The guidelines cited in version 5 standards “CIP 006-5 Cyber Security – Physical Security of BES Cyber Systems” Dated November 7, 2011, Page 22 and 23 “Guidelines and Technical Basis” state, in part: “Typically any opening greater than 96 square inches with one side greater than 6 inches in length would be considered an access point into the Defined Physical Boundary.” Therefore, BPA votes no. In reference to the guidelines cited above which originated from CAN-0031 referring to “…96 square inches…” as an access point, this is an area of concern for BPA. In an effort to shore up each 96 square inch opening throughout BPA’s service area, with either a physical barrier or intrusion detection system, the cost would significantly outweigh the value added for physical security protection. The challenge to utilities should be to prevent physical access to the BES Assets and to not gauge that access opportunity on 96 square inches. Accordingly, this provision will be unnecessarily costly to the utilities without an actual security benefit. BPA believes the language in the guidelines on pages 22 and 23 referring to 96 square inch access points needs to be removed from the standard, or: The proposed CIP 006 guidelines need to reflect reasonable dimensions, alternatives and language similar to other CIP standards for example: “The Responsible Entity shall document and implement physical or alternative measures for monitoring openings to the physical security perimeter greater than 150 square inches with no dimension less than 12 inches. The Responsible Entity shall implement one of the following methods:” • Physical measures: Bars, Wire Mesh, etc. • Alternative measures: Motion Sensors, Vibration Sensors, Intrusion Detection etc.
No
The guidelines cited in version 5 standards “CIP 006-5 Cyber Security – Physical Security of BES Cyber Systems” Dated November 7, 2011, Page 22 and 23 “Guidelines and Technical Basis” state, in part: “Typically any opening greater than 96 square inches with one side greater than 6 inches in length would be considered an access point into the Defined Physical Boundary.” Therefore, BPA votes no. In reference to the guidelines cited above which originated from CAN-0031 referring to “…96

square inches…" as an access point, this is an area of concern for BPA. In an effort to shore up each 96 square inch opening throughout BPA's service area, with either a physical barrier or intrusion detection system, the cost would significantly outweigh the value added for physical security protection. The challenge to utilities should be to prevent physical access to the BES Assets and to not gauge that access opportunity on 96 square inches. Accordingly, this provision will be unnecessarily costly to the utilities without an actual security benefit. BPA believes the language in the guidelines on pages 22 and 23 referring to 96 square inch access points needs to be removed from the standard, or: The proposed CIP 006 guidelines need to reflect reasonable dimensions, alternatives and language similar to other CIP standards for example: "The Responsible Entity shall document and implement physical or alternative measures for monitoring openings to the physical security perimeter greater than 150 square inches with no dimension less than 12 inches. The Responsible Entity shall implement one of the following methods:" • Physical measures: Bars, Wire Mesh, etc. Alternative measures: Motion Sensors, Vibration Sensors, Intrusion Detection etc.

No

The guidelines cited in version 5 standards "CIP 006-5 Cyber Security – Physical Security of BES Cyber Systems" Dated November 7, 2011, Page 22 and 23 "Guidelines and Technical Basis" state, in part: "Typically any opening greater than 96 square inches with one side greater than 6 inches in length would be considered an access point into the Defined Physical Boundary." Therefore, BPA votes no. In reference to the guidelines cited above which originated from CAN-0031 referring to "…96 square inches…" as an access point, this is an area of concern for BPA. In an effort to shore up each 96 square inch opening throughout BPA's service area, with either a physical barrier or intrusion detection system, the cost would significantly outweigh the value added for physical security protection. The challenge to utilities should be to prevent physical access to the BES Assets and to not gauge that access opportunity on 96 square inches. Accordingly, this provision will be unnecessarily costly to the utilities without an actual security benefit. BPA believes the language in the guidelines on pages 22 and 23 referring to 96 square inch access points needs to be removed from the standard, or: The proposed CIP 006 guidelines need to reflect reasonable dimensions, alternatives and language similar to other CIP standards for example: "The Responsible Entity shall document and implement physical or alternative measures for monitoring openings to the physical security perimeter greater than 150 square inches with no dimension less than 12 inches. The Responsible Entity shall implement one of the following methods:" • Physical measures: Bars, Wire Mesh, etc. Alternative measures: Motion Sensors, Vibration Sensors, Intrusion Detection etc.

No

Regarding R2, BPA would agree with the following concept: Failing to capture a single required logging data field, would be no violation at all. This is simply a failure to follow procedures rather than a material defect in, or lack of defined process. As an example, all data fields completed except "time of exit" would be no violation. Complete failure to log a visitor would be considered a Moderate violation because insufficient information exists to uniquely identify the visitor.

No

R1.1: The Guidelines state that ports that cannot be disabled are, by definition, needed. Therefore, BPA suggests that R1.1 be reworded to include the bracketed text as follows: • Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. [If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed necessary]. R1.1 "Measures": CIP-010 R1.1.5 requires that all logical network accessible ports are documented as part of the baseline configuration. BPA is asking for clarification, "Is it expected that Responsible Entities would have different evidence for these two requirements, or would the same evidence suffice?" R1.2 "Measures": The phrase "and screen shots" implies that screen shots are required. BPA recognizes that screen shots are certainly useful, but may not apply to all systems. In addition, this does not follow the explanation in the third paragraph of the "Background" section. BPA suggests rewording the measure to include the bracketed text as: • Evidence may include, but is not limited to: o Documentation stating specific or types of physical input/output ports to restrict, or o [System-generated evidence] or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. R1.1 "Guidelines": The guidelines provide additional requirements. BPA believes these requirements should be in the standard, not in the guidelines. BPA believes that Guidelines should be exactly that: a guide to achieving compliance. BPA requests that all the guidelines for CIP-007 be

carefully examined to ensure that no requirements are inadvertently introduced. In addition, to be clear include the full sentence“… blocking ports at a perimeter does not satisfy this requirement” is unnecessary, as the “Applicability” column explicitly applies to devices beyond perimeter devices. BPA suggests replacing the sentence with: • Note that the requirement is applicable to BES Cyber Systems and therefore to the Cyber Assets within those systems. This control is another layer in the defense against network-based attacks, therefore it is the intent that the control be on the device itself.

No

R2.1 “Measures”: “The list could be sorted by BES Cyber System or source.” BPA believes this sentence is true; in fact the list could be sorted in any of a number of ways, depending on the needs of the entity. BPA believes the standard should not address the sorting of lists. BPA recommends removing the sentence. R2.3: The requirement defines a process, but does not require that the process be followed. The Guidelines for R2.3 establish addition requirements. BPA believes that the remediation process is most appropriately defined in the plans required by R2.2. BPA suggests rewording as follows: Completion of the steps in the remediation plan required in CIP-007 R2.2, including any exceptions for CIP Exceptional Circumstances. R2.2 Guidelines: BPA is concerned about the use of terms such as “…the remediation plan will include a timeframe.” This strongly implies a requirement rather than mere guidelines. “…the remediation plan should include a timeframe” is more appropriate. R2.3 Guidelines: BPA believes this guideline establishes numerous requirements: “… that plan must be implemented”, “… must be implemented by the timeframe the entity documented …” BPA believes that these requirements are appropriate, but they should be in R2.3 itself, not in the guidelines.

No

R3.1: BPA agrees with and applauds the decision not to require anti-malware tools on every Cyber Asset. However, “BES Cyber System” merely groups Cyber Assets for convenience. Therefore, R3.1 could be still be construed to apply to each Cyber Asset in the BES Cyber System. BPA believes that R3.1 needs to be very explicit. In addition, the Guidelines make it very clear that the Responsible Entity can determine that a particular Cyber Asset or group of Cyber Assets is not susceptible to malware and therefore needs little or no protection. BPA suggests rewording as follows: “For Cyber Assets within the scope of CIP-007 R4.1, and which the Responsible Entity has determined to be susceptible to malware intrusion, deploy method(s) to deter, detect, or prevent malicious code”. BPA believes that these need not be deployed on every applicable Cyber Asset, as long as each applicable Cyber Asset is protected. R3.1 “Measures”: BPA believes “Measures” should be reworded to incorporate the changes to R3.1. BPA suggests rewording to include the bracketed changes as follows: Evidence may include, but is not limited to: • [Documentation of any determinations that specific Cyber Assets or specific types of Cyber Assets are not susceptible to malware]. • Records of the Responsible Entity’s deployment of these methods (i.e. through traditional antivirus, system hardening, policies, etc.). R3.3, “Measures”: “Measures” starts “Evidence may include, but is not limited to, (i) current signature or pattern updates, and (ii)…” This does not follow the explanation in the third paragraph of the “Background” section. BPA suggests rewording to include the bracketed changes as follows: Evidence may include, but is not limited to: • Current signature or pattern updates, or • [System-generated evidence showing the configuration of signature], • Pattern updates for automated controls • Work logs showing the signature, or • Pattern updates for manual controls R3.4: Applicability includes Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, but excludes Low Impact BES Cyber Systems. Requirement includes all BES Cyber Assets, including Low Impact BES Cyber Assets, but excludes the associated access control systems. It also includes all Protected Cyber Assets, not just Associated Protected Cyber Assets. BPA cannot determine which is correct, but believes that the two lists must be consistent. R3.4: BPA believes the requirement makes no provisions for Transient Cyber Assets for which no anti-malware is available. BPA suspects there may be circumstances when the use of such Transient Cyber Assets is necessary for the reliability of the BES. BPA suggests adding the following to the end of the requirement: For circumstances where such methods are not possible, document (i) Compensating measures taken to reduce the risk to the BES, and (ii) Justification that the risk to the BES of not using the Transient Cyber Asset is greater than the risk of using it without anti-malware protection R3.4 “Measures”: Logging connections of Transient Cyber Assets is addressed in R3.5. In addition, it does not address whether adequate methods were deployed. BPA believes it should be removed from the “Measures” for R3.4. Reword measures to add “that show” as bracketed below: Evidence may include, but is not limited to, logs [that show] when Transient Cyber Assets and

removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. R3.5: BPA believes the requirement does not address how the connection is made. In particular, depending on the device, it is possible to use Ethernet or serial connections. Serial connections represent a much lower threat but also represent a much lower capability for things such as automated logging. BPA does not know the intent of the drafting team, so BPA cannot offer any suggestions other than to make it clear (either in CIP-007 or in the definitions) whether or not serial connections from a Transient Cyber Asset are within scope. R3.5 “Measures”: Applicability includes Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, but excludes Low Impact BES Cyber Systems. Measures section includes all BES Cyber Assets, including Low Impact BES Cyber Assets, but excludes the associated access control systems. It also includes all Protected Cyber Assets, not just Associated Protected Cyber Assets. BPA cannot determine which is correct, but believes that the two lists must be consistent. R3 Guidelines: BPA believes the guidelines require testing of signature updates, despite the lack of any mention of such testing in the requirements. BPA suggests removing the reference in the guidelines.
No
R4.1: BPA had difficulty determining the meaning of the first sentence. In addition, the requirement clearly states a minimum list of event types. BPA believes that there is no need to include “as a minimum”. With or without that phrase, the Responsibility Entity can choose to log additional types of events. Including it in similar situations in the current standards has led to confusion about what is required. BPA has no concerns with the list itself. However, the Guidelines for 4.1 state “It is not the intent that if a device cannot log a particular event that a TFE must be generated.” As presently stated, the requirement does not support this intent. BPA suggests replacing the initial paragraph with the following: Use technical or procedural means to log generated events for identification of, and after-the fact investigations of, BES Cyber Security Incidents. Log each of the types of events shown below that are applicable to and can be logged for the system or device. Document the reason for any event types not being logged. For the purpose of this requirement a Technical Feasibility Exception is not required for systems or devices that cannot log any or all the event types below. BPA believes the “Measures” should also be modified as follows: • Evidence may include, but is not limited to, a paper or system generated documentation of event classes for which the applicable system or asset is configured to generate logs, along with the justification for event types required in R4.1 not being logged. This documentation must address the required event types. R4.2 “Measures”: BPA believes that screen shots may not be applicable to all systems. BPA suggests replacing “Screen-shots” with “System-generated evidence”. In addition, the format conflicts with the explanation in the third paragraph of the “Background” section. BPA suggests rewording “Measures” with changes as bracketed below Evidence may include, but is not limited to, • Paper or system-generated listing of event classes and conditions which necessitate real-time alerts • Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert, or • [System-generated evidence showing] how real-time alerts are configured R4.3: BPA believes this requirement has a fundamental flaw: To satisfy it, Responsible Entities must have a technical or procedural control to monitor the status of the logging system. BPA asks, “What happens if that control itself fails? Must there be another system to monitor the system monitoring logging?” SP800-53 control AU-5, referred to in the Rationale, addresses this first by listing typical causes for logging failure, some of which can be detected easily, and second by allowing the organization to define which events require real-time alerts (Enhancement 2). In addition, despite the explanation in the rationale, the requirement itself does not prohibit a violation for a failure to log. BPA recommends rewording as follows: • Define event logging failures which require prompt notification and correction, either at a Cyber Asset level, Cyber System level, entity level, or in combination. • Detect and initiate a response to such event logging failures before the end of the next calendar day. Logging failures in and of themselves do not constitute violations of R4. R4.3 “Measures”: BPA believes that based on the requirement, the “Measures” should show that the event was detected, and that a response was activated. The proposed “Measures” section does not do that. In particular, (i) Configuration of real-time alerts is a means to detecting a failure, not evidence that a failure was detected. In addition, screen shots are not applicable to all systems. (ii) This requires one of two specific actions. Other actions may be appropriate. In addition, the format conflicts with the explanation in the third paragraph of the “Background” section. BPA suggests replacing (i) and (ii) with: • Documentation demonstrating how and when the failure was detected • Documentation showing when the response to the failure was activated. Examples may include, but are not limited

to, dated records that personnel were dispatched or a work ticket was opened to review and repair logging failures. R4.4: Applicability includes Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, but excludes Low Impact BES Cyber Systems. Requirement includes all BES Cyber Systems, including Low Impact BES Cyber Systems, but excludes the associated access control systems and Associated Protected Cyber Assets. BPA cannot determine which is correct, but believes that the two lists must be consistent. R4.4: Despite the rationale for R4.3, BPA believes R4.4 still does not prevent a violation for a failure of the logging system. In particular, a hardware failure of media used to store logs would be a violation. In addition, the phrase "where technically feasible" forces Technical Feasibility Exceptions even in the case of a failure of the logging system. Technical Feasibility Exception should only be needed in the very rare cases of a logging system that is unable to provide for long-term retention of logs. BPA suggests rewording as follows: Unless prevented by a failure of system(s) used for logging, retain BES Cyber System security related event logs identified in 4.1 for at least the last 90 consecutive calendar days. R4.4 "Measures": "Measures" introduces a requirement that entities record what was done to the logs at the end of the 90 days. In many cases logs are removed automatically by the system at the end of some specified retention period. In these cases, there would be no "records of disposition". Furthermore, retention of disposition records should be addressed in data retention, if at all, and not in the "Measures". Finally, BPA believes the format conflicts with the explanation in the third paragraph of the "Background" section. BPA suggests rewording as bracketed below: Evidence may include, but is not limited to: • Security-related event logs from the past ninety days, • [Documentation of the process used to dispose of logs, or] • [Records of disposition of security-related event logs] R4.5: As stated, the requirement does not accommodate reviews in intervals less than two weeks. BPA suggests changing the first sentence to read "…of logged events at intervals of no greater than two weeks to identify…" In addition, the phrasing "sampling of logged events" leaves the possibility of having to review every log, despite the clear indications in the Justification that it is not feasible to review all systems logs. Furthermore, it is not clear whether the Responsible Entity is required to correct the deficiency within one calendar day, or merely begin the response within one calendar day. Also, "any deficiency" implies some type of system failure, when the event types listed in R4.1 all refer to security events involving actual or potential malicious action. Finally, response to logging failures is addressed in R4.3 and should not be addressed here. BPA recommends that the response to a significant event discovered in the review be addressed under CIP-008, not CIP-007. BPA suggests rewording as follows: • Define, document, and implement a process for reviewing security event logs that ensures that (i) Logs are reviewed, either by summarization or by sampling log-by-log or event-by-event, at intervals of no less than two weeks, and (ii) The Responsible Entity's Incident Response Plan, as defined under CIP-008, is initiated before the end of the next calendar day (or within the time constraints of the Incident Response plan, if longer) for any discovery of a potential security event defined under R4.1 of this Standard Perform the actions defined in the process, as applicable. R4.5 "Measures": "Measures", as stated, requires documentation of each of four different actions. Some of the actions may or may not occur. In addition, it is not clear what "documentation describing the review" means. Finally, the format conflicts with the explanation in the third paragraph of the "Background" section. BPA suggests rewording as follows: Evidence may include, but is not limited to; • Documentation describing the review process, • Findings from reviews, or • Signed and dated documentation showing the review occurred R4.1 Guidelines: The paragraph on page 41 states: User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped. The last sentence defines four types of events that must be logged, at least three of which are clearly not within the list in R4.1. This is an extension of the requirements. BPA believes this conflicts with the purpose of guidelines. If the requirements are valid, BPA believes the requirements should be moved to the requirements section. In addition, an earlier paragraph in the Guidelines makes it clear that it is not practical for the Standard to enumerate all events. BPA agrees with that earlier paragraph, and suggests not adding additional events in the Guidelines. Even if the paragraph is left in place (to which BPA is strongly opposed), there are other concerns, as well: • BPA believes "Account management" is not defined. Typically, it includes creation, deletion or changing of accounts or of privileges associated with those accounts. If that is the intent here, it should be stated explicitly. • BPA believes that requiring logging of object access and processes started and stopped will generate voluminous logs, to no real purpose. As an example, an active database can easily generate hundreds

of file accesses per second. There is little utility in logging these, or any other routine object access. BPA believes it makes more sense to log only failed object access or failed process start/stop. R4.2 Guidelines: BPA believes that “Alerts can be configured…” and “The log analysis rules can exist…” appear to be stating additional requirements, in that each sentence provides a closed list of actions. BPA suggests “Typically, alerts are configured…” and “The log analysis rules often exist…” as possible solutions to the issue. R4.3 Guidelines: In order to eliminate the possibility of the Guidelines appearing to expand on the requirements, BPA suggests the second paragraph be rewritten as: • For centralized logging systems, it should noted that if communication goes down between the cyber asset and the logging system, there is no logging failure as long as the cyber asset can store the logs locally for a period of time until the communication comes back up. R4.5 Guidelines: BPA believes the first sentence is unnecessary, as it merely restates the requirement.

No

R5.1: Applicability includes Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems, but excludes Low Impact BES Cyber Systems. Requirement includes all BES Cyber Systems, but excludes Associated Protected Cyber Assets and the associated access control systems. BPA cannot determine which is correct, but believes that the two lists must be consistent. R5.1: Based on the measures, the Rationale and the Guidelines, the apparent intent of R5 is to address user access only. To clarify this, BPA suggests modifying R5.1 to read “…granting users electronic access…” R5.1 “Measures”: The format conflicts with the explanation in the third paragraph of the “Background” section. BPA suggests modifying “and” to “or” as bracketed below. Evidence may include, but is not limited to: • Documentation describing how users are authenticated before being granted access, [or] • Demonstrations showing authenticated access enforcement of internal and remote paths to the BES Cyber System R5.2: Again, it is not explicitly stated that only user access is relevant. BPA suggests modifying R5.2 and change bracketed text to read “…other generic [user] account types.” R5.4: BPA recognizes that this is the only requirement in the standard that levies requirements on Low Impact BES Cyber Assets. It is also unusual in that it lists Responsible Entities in the “Applicability” section but lists the covered Cyber Assets in the requirement. Furthermore, it will require Technical Feasibility Exceptions that could be avoided. Finally, BPA believes this requires a procedure, but does not require that the procedure be followed. BPA suggests the following: • Applicability: o High Impact BES Cyber Systems o Medium Impact BES Cyber Systems. o Associated Physical Access Control Systems o Associated Electronic Access Control or Monitoring Systems o Associated Protected Cyber Assets Requirement: Define, document, and implement procedural controls for initially changing default passwords, unless - The default password is unique to the device or instance of the application on Cyber Assets or Cyber Systems involved, or: - The device does not allow the passwords to be changed For the purposes of this requirement an inventory of Cyber Assets is not required R5.5.3: The intent of “…or an obligation to the password…” is unclear to BPA and since BPA does not understand the intent of the phrase, BPA cannot suggest a correction. R5.3 Guidelines: This appears to apply to R5.4, not R5.3. In addition, in the first paragraph, “… passwords must be changed …” states a requirement. R5.4 adequately states the requirement. R5.5 Guidelines Table Comments: BPA does not understand all the columns in this table. In particular, BPA is uncertain of the meaning of “Significance of passwords …” and “Existing Service Agreements”. BPA suggest that the table be prefaced with a narrative describing the purpose of each column. In addition: • BPA does not understand the third and fourth entries, third column, reading “Local access path. Individuals must authenticate at an upstream device prior to gaining access.” Several things are not clear to BPA and BPA asks: • Do the two sentences refer to two independent conditions, with either or both being true, or are they both true? • What is an “upstream device”? Why must users authenticate at one? Is this a requirement for proper use of the password, or a technical issue defining when this particular entry is pertinent? • Why are there no other instances of shared passwords? • Fifth entry, third column: Is this a: o Requirement that remote users must authenticate using a different account prior to using the local account o Statement of two alternatives for using passwords, or o Definition of when the entry is applicable?

No

In the last condition for R2, Severe VSL: “except for CIP Exceptional Circumstances” is redundant, in the implementing the remediation plan is not required under those circumstances.

No

BPA believes there is a conflict in statements regarding Applicability - targeted at "All Responsible Entities" for CIP-008 R1.1 thru R3.1. Also in R3.2 thru R3.5 references High and Medium Impact

Cyber Systems. BPA does not does not understand the difference in Applicability; BPA believes it should be one or the other. Various incident response plans will need to be created and maintained. BPA believes this is a good approach both from a cyber security point of view and good business practice. BPA supports R1.0 as written and has no comments or concerns at this time. Add 1.3.4. Definition of process for documentation of allowable deviations from the plan and the documentation of those deviations. BPA supports R1.1 as written and has no comments or concerns at this time. R1.1 Measure: BPA suggests rewording to eliminate redundancy: Suggested Rewording: Evidence may include, but is not limited to, dated copies of BES Cyber Security Incident response plan(s) that include how to identify, classify, and respond to BES Cyber Security Incidents which target the Electronic Security Perimeter or Defined Physical Boundary of a BES Cyber System and covers incidents and that impact the reliability of BES. BPA supports R1.2 as written and has no comments or concerns at this time.
No
While documenting an incident is good business practice, BPA believes the standard should not dictate what evidence needs to be captured during an incident response. The standard should restrict itself to requiring documentation be provided, but the content should be up to the Responsible Entity. Lessons learned documents are valuable for example, but some incidents may be minor and there are no "lessons learned" leaving a requirement to file a Null attestation for compliance. R2.1 BPA believes the requirement needs rewording and BPA suggests that it should be revised: Current wording: "When a BES Cyber Incident occurs the incident response plans must be used when incidents occur and include recording deviations taken from the plan during the incident or test." • Suggested wording: "The incident response plan(s) must be used when a BES Cyber Security Incident occurs or when the incident response plan is exercised. Deviations from the plan must be fully documented in accordance with the plan." Note: The current requirement uses the word "test"; BPA recommends changing "test" to "exercise". R2.1 Measures: BPA believes the wording of the measure should be changed: Current wording: "Evidence may include, but is not limited to, incident reports, logs, and notes that were kept during the incident response process, and documentation that lists and justifies deviations taken from the plan during the incident." • Suggested wording: "Evidence may include, but is not limited to, incident reports, logs, and notes that were kept during the incident response process. Documentation of any deviations taken from the plan during the incident." Note: BPA believes in the measures "…the incident." at the end of the paragraph should be changed to "…incident or exercise". R2.2 Comment: BPA believes the use of the term "implement" at the front of the requirement is unusual. The normal definition is the plan is implemented upon publication; the plan can be invoked through an actual incident or through an exercise. • Suggested wording: Implement the BES Cyber Security Incident Response Plan(s) initially upon the effective date of the standard or before and at least once each calendar year thereafter…"] • Additional wording suggestion to be added: Incident response plans must be used when responding to real incidents or exercises, and must include recording deviations taken from the plan during either a real incident or the exercise. R2.3 BPA believes rewording is needed and suggests that it should be revised: Current wording: "Retain relevant documentation related to reportable BES Cyber Security Incidents for three calendar years." • Suggested wording: "Retain documentation described in the Incident Response Plan related to reportable BES Cyber Security Incidents for three calendar years."
No
R3.1 The current wording requires the Incident Response Plan to be implemented upon the effective date of the standard. BPA believes that could cause some entities to fail compliance if they did not publish their documentation on that exact date. • Suggested wording: o "Review each BES Cyber Security Incident Response Plan for accuracy and completeness o Initially, 30 days prior to the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and update as necessary." R3.2 and R3.3: BPA believes these requirements are redundant and should be combined. The requirement assumes there will be a need for a revision which may not necessarily the case. BPA suggest that requirement R3.2 be rewritten as follows and that R3 be deleted: • Suggested wording: "Review the results of BES Security Incident response Plan(s) test or actual incident response within thirty calendar days of the execution. o Document any lessons learned within thirty days of the exercise or actual incident o Update the plan within sixty days based on the any changes suggested in the lessons learned document."
Yes
R1 High VSL for R1 states that the plan ".does not communicate the incident to appropriate

organizations." BPA suggests that the VLS be changed to read "…or does not define the internal staff or external organizations that should receive communication of an incident". R2 Replace "test" with "exercise" R1 Guidelines: Comment: The Guidelines establish a definition for "Reportable BES Cyber Security Incident". BPA has issues with that definition: 1. The definition should be identical to the one in the formal CIP V5 Definitions of Terms; the SDT should pick one or the other. 2. The guideline added a new term "response action" with a definition. It also should be cross referenced to the CIP V5 Definitions of Terms. The guidelines also state that a response action can either be "necessary or elective" without defining those terms. They also go on to use "precautionary" as a term that defines elective. BPA believes it is useful to have this guideline, although it may make more sense to move the definitions out of the guideline and into the definitions section while leaving the guidance as is.

No

BPA would vote yes if the words "Initially upon the effective date of the standard" were changed to "within 12 months prior to effective date of the standard. o 18 Months Minimum – The Version 5 CIP Cyber Security Standards shall become effective on the later date: January 1, 2015; or the first calendar day of the seventh calendar quarter after the applicable regulatory approval date. However, if Version 4 CIP Cyber Security Standards do not become effective, Version 3 CIP Cyber Security Standards remain in effect until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan. (Use this format Version # CIP Cyber Security Standards to refer to the complete set of standards rather than the harder to read, takes up more space: CIP-002-3 through CIP-009-3) • Many of the requirements include the words "upon the effective date of the standard". Many recovery plans are already on an annual cycle. Will all recovery plans have to be exercised again, if they have already been tested during the calendar year prior to the effective date of the standard. This wording doesn't really make sense for systems placed into operation after the effective date of the standard. Recommendation: o CIP-009 R2 should be "prior to the effective date of the recovery plan(s) The addition of this new requirement calls for the preservation of data for forensic analysis following all events that trigger the Recovery Plans. If this requirement is implemented as written, it may delay recovery of impacted systems, as our first priority will be data preservation. This may negatively impact system reliability. We can approve this requirement if it states explicitly that recovery cannot be hampered by attempts to preserve data.

No

BPA would vote yes if the words "Initially upon the effective date of the standard" were changed to "within 12 months prior to effective date of the standard.

No

BPA would vote yes if the words "Initially upon the effective date of the standard" were changed to "within 12 months prior to effective date of the standard. Based on forensics and analyses it may take longer than 30 days to determine the cause of a failure. Please clarify if the expectation is that the analyses and updates are required to occur within this 30 day period.

No

BPA would change its position for the VRFs and VSLs if they Included the applicability of the requirements as an element. BPA believes the VRF & VSL should incorporate the risk to the BES Cyber System. As an example, High Impact BES Cyber System violation would result in a higher VRF & VSL. Likewise, a lower impact for applicability would result in a lower VRF &VSL.

No

Concerning R1.1 BPA recognizes that it would be overly burdensome to have to document every piece of software installed on an ACMS server, not just the major applications. There is some latitude available based on "specified grouping", but this continues to be a concern regarding maintaining compliance. We will address this from the "grouping" perspective and thus approve R1.1. Grouping is a software "package" or group of files. It is good requiring the differences in test vs. production to be documented demonstrates awareness that not all entities have test environments that model their production systems. This allows significant latitude that will enable us to remain compliant in the interim while we are working to enhance our test environments.

No

For the majority of programmable electronic devices in the field, especially devices that don't support routable protocols, it will not be technically feasible to monitor for changes to the baseline configuration. BPA assumes we will have to spend a lot of time submitting and managing Technical Feasibility Exceptions (TFEs) for each of these devices which does not increase reliability or cyber

security. BPA would vote yes if this requirement was not required for Medium Impact BES Cyber Systems and Associated Protected Cyber Assets.
No
BPA would vote yes if the words “Initially upon the effective date of the standard” were changed to “within 12 months prior to the effective date of the standard.
No
BPA makes the following recommendation for R2: BPA believes a 30 day window should be established to investigate and resolve the unauthorized change. Require that the unauthorized change be resolved either by formal approval of the change or that the change was backed out. The severity increases to Severe if not resolved after 30 days
No
R1.3: BPA believes the requirement needs to accommodate an initial assessment prior to the effective date of the standard. BPA suggests “Initially upon or no more than 15 months prior to the effective date…” R1.3: BPA believes the standard does not indicate what is meant by “adherence to its BES Cyber System Information protection process.” Reasonable interpretations could include any or all of: 1. Review of all BES Cyber System information to ensure it is properly labeled. 2. Review of a sampling of documents to ensure they are properly labeled. 3. Review of user access authorizations to electronic media storing the information
No
BPA believes that it is correct and true that data may be recovered from some media after erasure. However, it is also true, that for some media, erasure is fully adequate. BPA recommends the following change: Reword the requirement to make allowances for media reuse within the same control zone. In such cases, where the media stays at the same security level, there should be no need to cleanse the media prior to re-use. R2.2: Yes R2.1: There have been varying usages of the term “redeploy” in CIP-007-3 R7. In particular, there have been violations found when a change in an ESP leaves Cyber Assets that were once within an ESP (and therefore subject to CIP-007-3) outside the ESP. BPA suggests the following be added to the end of CIP-011-1 R2.1: This requirement does not apply to instances where the media remains in the Cyber Asset, but the Cyber Asset undergoes a change in status such that CIP-007 R2.1 is no longer applicable. R2 Guidelines: The last paragraph allows for the removal of a BES Cyber System from service to allow analysis of the media. BPA believes it should also point out that it may be appropriate to remove the media from the Cyber Asset to allow off-line analysis, as that would be neither reuse nor disposal.
Yes
Yes
General Comment on the Standards Development Process and Direction: The SDT has done an excellent job in capturing the weaknesses and problems that were included in the previous standards. The move toward a more FISMA/NIST based approach is obvious and should be applauded. However, this raises the question of why we are attempting another intermediate step rather than simply adopting the NIST FIPS and SP documents as our methodology for applying security. NIST has done an exceedingly good job of addressing Cyber Security for Federal systems for decades, and has taken steps to address the world of Industrial Control Systems. These standards and guides are strong yet flexible, allowing for application in many different environments. And the terminology and definitions used are already well understood industry standards. It seems that the scope of this (Version 5) change is broad enough that it would be a small step to skip over it and simply adopt the NIST Cyber Security Standards for our industry.
Group
Pacific Gas and Electric Company
Robert Mathews
Yes
Strike or revise bullets 3, 4 & 6 in the Control Center Definition
No
Criteria 2.13 in Attachment 1 is not acceptable because under 1) the functional obligations of TOP and TO is too vague and 2) 300MW of in many cases does not qualify as significant impact. Also 300 MW

of generation should not be equated to 300 MW of UFLS/UVLS. Intent of these criteria is not clear so suggested language is not provided
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
R6.3 is unacceptable as it does not fit the stated rationale for R6. All requirements pertaining to Information Protection should be in CIP-011 not CIP-004.
No
R7.1 and R7.2 are potentially infeasible
Yes
Yes
No
R1.4 needs further specification (e.g. detecting unauthorized entry in real-time may not be feasible in certain situations)
Yes
Yes
Yes

Yes
Yes
No
R5.1 for local access (e.g. relays) is problematic
Yes
Yes
No
R3.4 and R3.5 are potentially infeasible
No
Comments: Revise R1.5 to “Preserve data, where technically feasible or operationally prudent….” to enable actions in the best interest of BES reliability.
No
R.2.2 What is “any information” defined as?
Yes
Yes
Yes
Yes
No
CIP-011 overall is unclear on the distinction of information about BES Cyber Assets and information residing on BES Cyber assets. Also the scope of CIP-011 to Low Impact Cyber Assets is unclear.
No
CIP-011 overall is unclear on the distinction of information about BES Cyber Assets and information residing on BES Cyber assets. Also the scope of CIP-011 to Low Impact Cyber Assets is unclear.
Yes
Group
SPP RTO and listed members
Lesley Bingham
Yes
he definition of BES Cyber Asset has caused confusion. On two recent presentations by the Standards Drafting Team, a clear definition was requested and could not be provided. Given that this is a fundamental definition used in defining other terms and is a core concept of the CIP standards, a clear definition is needed. The definition of BES Cyber Incident contains the word “suspicious”. Recommend a change to “intentional”. The definition of BES Cyber System contains the term Maintenance Cyber Asset, which is not a defined term. Should that be Transient Cyber Asset? The definition of BES

Reliability Operating Services is lengthy and confusing. There is concern that it will be difficult to audit to this definition and that it conflicts with the established bright line criteria. The definition of CIP Exceptional Circumstance should include the word “may” to read “A situation that may involve one or more….” The definition of Control Center does not explicitly include generator control rooms. Is it intended to cover these facilities? If not, does that term need to be defined for greater clarity?
No
No
No
Yes
Yes
No
The areas covered are certainly appropriate to protect BES Cyber Systems, but every entity may not have processes which would be covered by all topics. Should a policy be drafted or language included where a process does not exist?
Yes
Yes
Yes
Yes
Yes
No
Language around this requirement pertaining to which personnel need to be covered is confusing. Rationale discusses personnel who have electronic or unescorted access. Information in table does not specify who should participate in awareness activities. Table specifies that language was “Changed to remove the need to ensure everyone with authorized access receives this awareness”. If all personnel, as opposed to strictly those with authorized access, at a Responsible Entity are covered by this requirement, then that should be specified in the standard.
No
Comment is specific to Part 2.10 of Table R2. Language in the table seems to require training on network connectivity for anyone with access to High and Medium BESCS. For some categories of users (e.g., Operators) this will be both out of context and irrelevant. For some categories (e.g., Network administrators) this will be unnecessary. Recommendation is to strike item 2.10.
Yes
Yes
Yes
Yes
No
Terminations, resignations and transfers all have the same access removal requirement: one business

day. This does not appropriately gauge the level of risk with each. A termination, especially an involuntary one, can expose the Responsible Entity to much more risk than a transfer. Also, how should a Responsible Entity define when the “clock starts”? For a transfer, access may still be needed during the backfill/transition process or even for resource management after the transfer has formally been completed. Also, in the Change Rationale, there is a comment that “the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer” yet the requirement is to revoke access. Reviewing access is not mentioned in the table.
Yes
No
Part 1.1 Requirement is to define controls. Yet the measure requires evidence that the controls have been implemented. The requirement and the measure should be closer in language. Part 1.2 should include only High Impact BES Cyber Systems, not Medium Impact BES Cyber Systems as well. If Medium Impact BES Cyber Systems need more protection than a Low Impact BES Cyber Systems, that protection should be described more specifically. Medium Impact BES Cyber Systems and High Impact BES Cyber Systems seem to get same treatment on this provision. This section also impacts Registered Entities who haven’t had CIP requirements previously. Some of the requirements for Low Impact BES Cyber Systems will have a high paperwork factor and burden. Part 1.5: Measures are very technology-centric around one solution, Intrusion Detection Systems or IDS. Request clarification that IDS is not required and that specific technology isn’t sole means of compliance.
No
Part 2.1 Concept of “Associated Protected Assets” is not well-understood. Clarity needed here. If Associated Protected Assets need a significant level of protection, a more direct approach would be to classify them as Medium Impact BES Cyber Systems or High Impact BES Cyber Systems? Part 2.3: User ID as an authentication method is addressed in other NERC publications and should not be included in the measure for this standard.
No
All the VSLs for this standard are Severe. A Responsible Entity with incomplete documentation is at as much risk for penalty as one with no permissions at an EAP. There should be a level of gradation in the VSL to reflect differences in severity levels. The VSL for CIP-006-5 provides a good example of the appropriate level of VSLs to reflect different degrees of noncompliance.
No
Part 1.2 and Part 1.3 contains language in the Measure of each to track egress, but the language of the standard does not specify this as a requirement. Standard includes language to restrict access (i.e. ingress) to those authorized. Egress language expands the standard and should be removed from the Measure. Part 1.3 also seems to set the stage for an additional number of Technical Feasibility Exceptions (TFEs). One of the goals of CIP Version 5 was to reduce TFEs in place of better security measures. The language “two or more…controls…where technically feasible” will lead to increased TFEs.
Yes
Yes
Yes
The VSL for CIP-006-5 is a good example of defining the appropriate degree of severity for noncompliance with a standard.
No
Part 1.1 indicates that the requirement is applicable to “systems”, but measure focuses on “assets”. Need a system approach if this requirement is intended to be applied at a broader level. The term “BES Cyber Asset” should be removed from measure if the requirement can be applied to “system”.
No
Part 2.1 Addition of “identified source” which can be final approver of patch, such as application vendor, is very helpful to Responsible Entities. Part 2.2 and Part 2.3 use the term “remediation plan”. Need clarification on when a “remediation plan” is needed. Is it required in delay between OS patch

release and vendor approval? When vendor will not approve patch? When there is a vulnerability for which no patch has been released?
No
Part 3.3 requires an update within 30 days. What “starts the clock” on this requirement? Is there an allowance for an approval step from a 3rd party vendor after the OEM has released the signature or pattern update? In some instances, a 3rd party vendor may have to approve prior to a Responsible Entity implementing a release and their delay could cause timing concerns. Part 3.5 requires logging each Transient Cyber Asset connection, but this would be captured in the Configuration Change Management requirements of CIP-010-1. As it is covered elsewhere, it should be removed from this section of the standard.
No
Part 4.1 includes the use of “any” in the list of activities to log. Not all activities require follow up or investigation and that is the purview of CIP-008-5. Specifically, “any” failed login may not be an indication of a problem. Certainly there is a threshold that deserves attention, but the broad use of the term “any” makes this requirement too broad. Part 4.3 sets a timeframe of “before the end of the next calendar day”. This is a very short timeframe. Certainly, logging failure should be addressed, but more time may be needed. Part 4.5 inserts a manual review when automation and alerting, both mentioned previously in the standard are much more effective and reasonable controls. If a Responsible Entity is compliant with Parts 4.1-4.4, then a manual review is a redundant effort which provides no additional security. Recommend that this Part be removed.
No
Requirement 5.5.3 is confusing and unclear, especially the license and service agreement language. Also, the inclusion of “based on the impact level of the BES Cyber System” is not helpful. Recommend that the impact phrase be stricken.
No
The VSLs for this standard are primarily High or Severe. A Responsible Entity with incomplete documentation is at almost as much risk for penalty as one with no implemented controls. There should be a further level of gradation in the VSL to reflect differences in severity levels. The VSL for CIP-006-5 provides a good example of the appropriate level of VSLs to reflect different degrees of noncompliance.
No
Part 1.3, requirement 1.3.3 needs the addition of “BES Cyber Security Incident” to replace the undefined “incident”.
No
Part 2.1, the language regarding “deviations” is confusing. Plans should be written at a high enough level that a Responsible Entity has the flexibility to respond best to their situation. Documenting a deviation does not provide additional security control. Recommend that the deviation language be stricken. Part 2.2 requires a test of a Responsible Entity’s BES Cyber Security Incident Response Plan “initially upon the effective date of the standard”. Is it proposed that if a Responsible Entity has completed a test 5 months prior to the effective date (complying with the “annual not to exceed 15 months” definition) that the Responsible Entity should do an additional retest on or about the effective date of Version 5?
No
Part 3.1 requires a review of a Responsible Entity’s BES Cyber Security Incident Response Plan “initially upon the effective date of the standard”. Is it proposed that if a Responsible Entity has completed a review 5 months prior to the effective date (complying with the “annual not to exceed 15 months” definition) that the Responsible Entity should do an additional review on or about the effective date of Version 5? The timeframes within Requirement 3 vary from 30-60 days. A consistent 60 days for each item would be recommended. Requirement 3.4 does not specify that the technology changes referenced are ones the Responsible Entity has actually implemented. Recommend adding “implemented” prior to “technology changes”.
No
The VSLs for this standard are either High or Severe. A Responsible Entity with incomplete documentation is at as much risk for penalty as one with no implemented controls. There should be a further level of gradation in the VSL to reflect differences in severity levels. The VSL for CIP-006-5

provides a good example of the appropriate level of VSLs to reflect different degrees of noncompliance.
No
The purpose of CIP-009 in all versions has been to provide that a Responsible Entity had adequate recovery plans. However, some CEAs are interpreting this standard to require the full restoration of facilities, including blueprints to rebuild structures. The standard should include language to reinforce the concept of BES system recovery and to specifically exclude full facility restoration. To support the recommendation above, the word “restore” used in R1, Part 1.3 should be changed to “recover” in both Requirement and Measure. Part 1.5 should be stricken. While data preservation is relevant to incident response processes, it is not relevant to recovery efforts.
No
Part 2.1 requires a test of a Responsible Entity’s Recovery Plans “initially upon the effective date of the standard”. Is it proposed that if a Responsible Entity has completed a test 5 months prior to the effective date (complying with the “annual not to exceed 15 months” definition) that the Responsible Entity should do an additional retest on or about the effective date of Version 5? A full operational test of recovery plans as required in Part 2.3 will be burdensome and expensive for smaller entities.
No
A 60 day timeframe for items 3.2-3.4, to be consistent with the recommendation for CIP-008-5, is recommended.
The VSLs for this standard are either High or Severe. A Responsible Entity with incomplete documentation is at as much risk for penalty as one with no implemented controls. There should be a further level of gradation in the VSL to reflect differences in severity levels. The VSL for CIP-006-5 provides a good example of the appropriate level of VSLs to reflect different degrees of noncompliance.
No
Part 1.1 requires a level of detail which is too granular for a baseline. Specifically, scripts and the physical location of a device, while certainly important, are not appropriate for a Change Management baseline. Part 1.2 requires that the CIP Senior Manager approve all changes. However, management approval is what is more appropriate in this instance. Recommend changing language from CIP Senior Manager to simply “Management approval”. Part 1.4 requires that “availability” is tested subsequent to a change. This should be stricken as availability of a BES Cyber System is not under the purview of CIP. Current language of CIP-007-3 R1 is preferable. Part 1.5 is duplicative of Part 1.4. Are Control Centers expected to perform dual testing procedures? This does not add to the security of a Control Center and simply adds additional work. Recommend striking 1.5.
Yes
No
An active vulnerability assessment of test environments as required in Part 3.2 will be burdensome and expensive for smaller entities. Additionally, requiring smaller entities to purchase a vulnerability assessment tool or contract for this service for every install is also burdensome and expensive.
Yes
No
The Measure for Part 1.1 contains the phrase “BES Cyber Security Information” and should be “BES Cyber System Information”.
Yes
No
The VSLs for this standard are either High or Severe. A Responsible Entity with incomplete documentation is at as much risk for penalty as one with no implemented controls. There should be a further level of gradation in the VSL to reflect differences in severity levels. The VSL for CIP-006-5 provides a good example of the appropriate level of VSLs to reflect different degrees of noncompliance.

No
Page 4 contains the phrase “CIP compliance program” yet that term is not defined. Is it intended that a Responsible Entity have a document describing their “CIP compliance program” as a part of their CIP-009-5 recovery documentation?
Individual
Daniel Duff
Liberty Electric Power, LLC
No
No
No
The wording of 1.1 is quite tortured, to say the least. It needs to be rewritten so that the action and triggers are clear.
Yes
Yes
Yes
No
CIP-003 R2 requires tracking of both exit and entry, as opposed to (for example) CIP-006 R1.6, which only requires tracking entry. The purpose of exit tracking is unclear, as is the reliability necessity of exit tracking. I would suggest deleting all reference to "egress" in CIP-003.
Yes
Yes
Yes
No
This time period should be lengthened to account for delays in personnel changes. A job search to fill a vacant position, including required background checks, takes significantly longer than 30 days in most cases. Using a 60 or 90 day window would be more appropriate, and would prevent needless paperwork where delegations are changed and then changed again simply to meet a paperwork requirement.
No
VSLs are not logically consistent - not naming a delegate for one function is considered a moderate VSL, but not changing that person within 30 days is a high VSL.
No
As written, the standard would prevent reasonable cyber access by vendors who maintain generator turbine controls. The standard requires 'individuals' to have site-specific cyber training on all aspects of the site security program. Vendors often have many agents who are capable of working on controls, and requiring each individual technician to sit through dozens of training sessions is not practical, nor does it enhance reliability of the BES.
Yes
Yes
No
See response to Q14.

No
See response to Q14.
No
See response to Q14.
No
The wording of this part of the standard should be "the effective day of the termination or resignation". Many individuals give significant notice of resignation, but would be expected to continue in their job function during the time between the resignation and actually leaving the position.
No
If failure to do a criminal background check on a single individual every seven years is a high violation, then not having background checks in the program should not be a moderate violation. Suggest breaking out this requirement so that one individual not having a complete update every seven years is a moderate, two or more a high VSL.
Yes
No
This section is too prescriptive. Cyber communication is a rapidly changing process, and including static requirements threatens to obsolete a standard, given the length of time needed to make changes to standards. Suggest rewording to "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement processes to mitigate unauthorized access".
Yes
Yes
No
Do not see the reliability gain from requiring exit logging on a "24-hour basis". Note that an individual entered a security perimeter should be sufficient.
No
Use of the electronic devices should be sufficient to demonstrate they are functional without a "test". Standard should be written stating testing is needed only for those security devices not active for a two-year period.
Yes
Yes
Yes
No
Some transient assets will not be under the control of the RE - the equipment used for relay calibrations, for example. There will be problems documenting the history of these assets, and whether they are compliant with this standard.
Yes
No
Password requirements will actually increase the risk to cyber systems, due to human response to strong passwords. The passwords will often be written down, which is the most common way passwords are compromised. Weaker passwords with sufficient bits of entropy will be safer in the long run than requiring 3 character types.
Yes
Yes

No
The RE should have the option of providing training in lieu of a test of the system.
Yes
No
Failure to provide the updated plan to a single individual should not be more severe than not updating a plan when significant faults have been discovered in the plan.
Yes
Yes
Yes
No
Same objection as CIP-008 - failure to notify a single individual of updates is treated as more severe than not updating a plan when faults are discovered.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Puget Sound Energy
Ed Croft
Yes
As criteria 1.4 and 2.13 part 2 read, a Wind Generation Control Center that controls 1500 MW or 300 MW of wind facilities may have associated High or Medium Impact BES Cyber Systems, respectively. Criteria 2.1 and 2.13 should distinguish between controllable generation and intermittent generation sources (i.e. wind and solar), since the loss of intermittent generation facilities happens naturally and regularly and is not viewed as an extreme event. Therefore, if this Control Center or generation's associated BES Cyber Systems are unavailable, degraded, or misused, the impact on the generation should not necessarily be viewed as high or medium impact. There is an overemphasis on Control Center impact versus large generation facilities. For example, a 1400 MW generation facility would only have associated Low Impact BES Cyber Systems (see 2.1), whereas a Control Center that controls 300 MW of generation may have associated Medium Impact BES Cyber Systems (see 2.13 part 2). The only material difference between these two facilities is that the Control Center controls multiple locations of generation, and the generation facility controls one. Part 2 of the Medium Impact criteria (2.13) for Control Centers should either be removed or the MW threshold should be raised

significantly to better match the Medium Impact generation criteria (2.1). Also, the enumeration in 2.13 does not make sense: "Control centers not included in High Impact Rating (H), above, that perform (1) . . , or (2) generation control centers that control 300 MW or more of generation."). The High Impact Generation Operator Control Center criteria (1.4) should be rewritten to clarify whether it is intended to include Control Centers that control one or more generation sites that each generate 1500 MW (2.1), or Control Centers that control a total of more than 1500 MW of generation. The latter meaning is suggested by CIP-002 Version 4 Attachment 1, criteria 1.15.
No
While it is documented within the definition, as referenced in the Rationale for R1 the Senior Management, the requirement that the senior manager have “overall authority and responsibility for leading and managing implementation of the requirements within this set of standards” would benefit from repetition within the R1 requirement itself. Standing alone after the removal of the rationale removal the requirement does not communicate the responsibility adequately.
No
Requirement R2 states that “Each Responsible Entity shall implement one or more documented cyber security policies…" and Measure M2, item 2 states that evidence may include "[r]ecords that indicate the required ten topics were implemented." We would like to see additional clarification of the meaning of the term "implemented". What evidence would be needed to show that the ten topics were "implemented"?
No
There needs to be additional clarity around the timing associated with the reviews and approvals. We believe what is intended is the review by the Responsible Entity and approval by the CIP Senior Manager is a combined event that must be completed initially upon the effective date of the standard and at least once each calendar year thereafter. A proposed content change might be: “Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter. For each cyber security policy, the annual review and approval cycle is not to exceed 15 calendar months.”
No
Proposed content change: Each Responsible Entity shall make its cyber security policies readily available to all individuals who have access to BES Cyber Systems or BES Cyber System Information.
Yes
No
The requirement includes a footnote that should be included within the requirement. Proposed content change: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change. Delegations do not need to be reinstated with a change in the CIP Senior Manager position or other position with delegation authority.
No
R4 VSL This language cites a High VSL when ‘not all’ individuals have been made aware of elements of the cyber security policy. This seems to contradict the intent described in the R4 rationale in which ‘it is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.’
No
The Measures for item 1.1 indicates that "Evidence must include the documented security awareness program, and additional evidence to demonstrate that this program was implemented such as, but not limited to, the quarterly reinforcement material that has been distributed." The "must," "and" and "not limited to" (underlined above) could be read to imply that evidence above and beyond quarterly reinforcement material is required as evidence. We recommend the following wording change to clarify that, while the program documentation and some evidence of implementation are required as evidence, there is not a prescriptive requirement for what evidence of implementation must be

provided.. "Evidence must include the documented security awareness program, and additional evidence to demonstrate that this program was implemented. Evidence of implementation may include, but is not limited to, the quarterly reinforcement material that has been distributed and documentation of the mechanism used to communicate the awareness content."
No
The rationale for R2 should be reworded from "…contains the proper policies…" to "…covers the required policies…" R2.6 – Requirement – Proposed word change Original - Training on handling of BES Cyber System Information and storage media. Proposed Change - Training on handling of BES High and Medium Impact Cyber System Information and storage media. Rationale – Rewording supports the applicability section. Since Low Impact Cyber Systems are not applicable, information specific to Low Impact Cyber Systems should not be in scope. R2.2 – Should this specify both cyber and physical security controls or is that "just understood"? R2.3 & R2.4 – Should the wording of the requirement and the measure be the same for both sub-requirements, given that they are addressing the same thing for each type of access control system?
No
R3.2 – requirement wording is confusing. Draft "requires" training "at least once every calendar year but not to exceed 15 calendar months." If it can go to 15 calendar months, then it is NOT required at least every calendar year. Propose re-wording along the lines of, "Training should be completed every calendar year but is required at least every 15 calendar months."
No
4.2 – Retention requirements do not extend beyond 3 years, creating confusion regarding retention of 7-year cycle background checks. Comments: R4.2 – The draft wording allows for gaps in the information required from an individual, as they would not need to provide information on where they lived, worked, or went to school (other than currently) if the duration was less than 6 months. Therefore, if someone moved/changed jobs after less than six months, that information could be excluded from the criminal history check. R4.4 – It is not clear why contractors must be separated out, rather than just having R4 be applicable to all individuals needing the access, regardless of their employer.
Yes
No
R6.1-3,6.4-6 – Propose use of language where access is appropriate for the roles and responsibilities rather than 'minimum necessary'. Comments: R6.3 – The measure, which requires a list of authorized people for BCSI would be problematic, since a person on the list, who owns BCSI, could share that BCSI with someone not on the list but who met all the requirements of R4. "Need to know" can be determined on a dynamic basis, and it would seem to potentially hamper workflow, if someone had to run through a process to show a diagram to someone. [[SSB: this one is a stretch, but not much harm in trying]] R6.5 & R6.6 – Same comment about timeframes as listed in item #15 above.
No
7.1 - There are questions in instances where resignations and/or terminations may be retroactive, which would introduce a challenge with revocation 'at the time of' events. 7.2 – Transfers or reassignments should frame access changes when no longer needed rather than the date of the transfer (as cited in the Measure (i)). The requirement may better address this issue by changing the wording to something like "For reassignments or transfers, review the individual's electronic and physical access to BES Cyber Systems by the end of the next calendar day. Revoke access when it is determined to be no longer needed." 7.3 – Propose use of 'approved BES Medium and High Impact Cyber System Information repositories,' to frame an appropriate location in which information can be managed and controlled.
Yes
No

R1.1 – This appears to address LIBCS & associated PACS; however, R1.2, R1.3 & R1.4 appear to address MIBCS, associated EACMS, associated PCA, but not associated PACS? Is this the intent? R1.2 & R1.3 –These requirements appear to now require the deployment of exit card readers at Medium and High sites – is that the intent? R1.4 – This requirement appears to address only actual access and eliminates access "attempts" – is this the intent? Also, how does this requirement apply to AEACMS or APCA, unless it is because they are required to located within a DPB? R1.6 – The change would make log retention duration 3 years. This is a big issue for video log storage . Also, this would seem to be both for authorized personnel and visitors? Since visitors are addressed in R2, this should probably say something like “Log (…) of individuals authorized unescorted physical access into each DPB….” to maintain consistency with the full definition of an authorized person, since a visitor can be an “authorized” person, they just can’t be unescorted. Also, the requirement does not appear to require tracking the time of entry into a DPB—is this the intent?? R2.2 –Requirement wording change for consideration: “A process requiring manual or automated logging of access by visitors into a DPB, which includes the date and time of first entry and last exit, the visitor’s name, and individual point of contact.”
No
R3 – Is this for commissioning the PACS or the DPB? Also, this would seem to imply that if you performed maintenance on a card reader, it would not need to be part of a later full system test?
Individual
Joanna Luong-Tran
TransAlta Centralia Generation
Yes
1. The criterion 1.4. There is no explanation why a BES Cyber Asset (BES Cyber System) located at the Control Center would have higher impact than another BES Cyber Asset (BES Cyber System) located outside the Control Center. In the case that the above two BES Cyber Assets (BES Cyber Systems), that if rendered unavailable, degraded, or misused, would have impact on the same

facilities identified in the criteria 2.1, 2.3, 2.4, or 2.12 in the same location, then, the impact on the BES would be same no matter where the locations of BES Cyber Assets (BES Cyber Systems) are. For example, an operator console is used solely to control/operate the Blackstart Resources in one location. If it is in a Control Center, it would be categorized as High Impact (criterion 1.4), while if it is outside the Control Center, for example, in a room at the Blackstart Resource's location, it would be categorized as Medium Impact (criterion 2.4). But if this console were rendered unavailable, degraded, or misused, the impact would be the same, i.e. the Blackstart Resources at this location would not be available. This case is different from another case that, if an operator console, located in a Control Center, controls/operates two Blackstart Resources, and these two Blackstart Resources are at two different locations, then the impact would be higher, i.e. affecting two Blackstart Resouces in two different locations, wider area impact. Based on the above argument, it is recommended the following change of the criterion 1.4, "Each Control Center or backup Control Center used to perform the functional obligations of the Generation Operator that includes control of one two or more of the assets identified in criteria 2.1, 2.3, 2.4, or 2.12, below, and these assets are at two or more location." 2. The criterion 1.4 has a reference to 2.12. But the criterion 2.12 is about the UVLS and UFLS. All the UVLS and UFLS standards are not applicable to GO/GOP. Generator Operators do not perform any obligation with UVLS and UFLS. Thus, it is recommended removing 2.12 in the criterion 1.4. 3. The criterion 2.13 (2), generation control centers that control 300MW or more of generation. We do not agree the 300MW number and justification in the guideline and suggest removing this 2.13 (2). The rationales are, a. In the case of a generation control center to control 300 MW, BES Cyber Systems (BES Cyber Assets), if rendered unavailable, degraded, or misused, would have an impact to cause the 300MW generation change. For a single unit of 500MW, its associated BES Cyber Systems (BES Cyber Assets) locally located at the plant, if rendered unavailable, degraded, or misused, would have an impact to cause the 500MW generation change. In the view of generation change, the second one has higher impact than the first one. But according to the criteria, it is opposite. Can the drafting team look at this situation and provide some explanation? b. The guideline says "The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold." We do not agree this statement here. The UVLS and UFLS are the last ditch efforts to save the BES, but the loss of 300 MW generation does not automatically trigger the 300MW load shedding (last ditch efforts). The UVLS and UFSL are triggered by the voltage and frequency, not directly by the generation loss. So the using the 300 MW from UVLS and UFLS is inappropriate for the generation loss. c. For the generation loss, the criterion 2.1 uses 1500MW. This number has been agreed by the industry during the version 4 standard development. In the view of generation loss, the BES Cyber Systems (BES Cyber Assets) in the generation Control Center should be categorized according the criterion 2.1, irrelevant to the BES Cyber System (BES Cyber Assets) location. Thus, there is no need to add a separate criterion to categorize the BES Cyber Systems (BES Cyber Assets) in the generation Control Center.
No

No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No

Individual
Mario Lajoie
Hydro-Québec TransÉnergie
No
since there is no place for on general comments, see responses in the to the last question (49) Under "BES Reliability Operating Services" • “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet • Recommend that “Change management” under “Situational Awareness” be clarified to changes in the BES instead of IT change management • Recommend clarification that “Facility” is the NERC Glossary Term -- in “Facility operational data and status” under “Inter-Entity Real-Time Coordination and Communication” o Request clarification on the scope of this “Operational Directives”. Does it include company messaging system? Two way radios? What is the relationship with the new COM-002? o Request clarification that these Coordination and Communications are limited to Reliability not Market Systems • recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret
Yes
HQT recommends that CIP-002-5 allow the use of a risk-based methodology or the bright line criteria stated in Attachment 1to identify critical assets. To ensure consistency within the industry, the methodology used and the results should be subject to approval by a panel of expert (for example, the NPCC TFIST for the NPCC Region and equivalent Task Force for other Regions). HQT also note that inconsistencies may arise from V4 to V5 based on the fact that the concept of Critical assets no longer exist in CIP-002-5. So this is not true to state that “most of these criteria are similar to those approved in version 4” The 15 minutes windows is not a criteria that is repeatable as it may be influenced by system conditions. The following criteria will need to be improved: 2.2 “Net Reactive Power” should be read as “Absolute value of Reactive Power” to consider Static VAR compensator and synchronous condenser 2.3 What means this criteria? How will it apply? 2.7 How a weighted value of a line is related to reliability? The number or the operating voltage are not reliability criteria. IROL, system restoration, voltage control, frequency control, interchange, load/generation balance are reliability criteria to consider.
No
For clarity, request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days when a change to BES Elements and Facilities is placed into operation” For clarity and consistency with the previous change, request changing M1 from “as required in R1 and list of changes to the BES (” to “as required in R1 and list of changes to the BES Elements and Facilities (” R1 : All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. In CIP-005-5 R1.1 and CIP-006-5 R.1.1, how can we define operational or procedural controls to restrict unauthorized electronic access or physical access if we didn't previously identified those assets either globally or specifically in CIP002-5 R1? R1 should required at least identification of type (or any other logical grouping) of LI BES CA (e.g. RTU-remote terminal unit) R1.1. Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. Transient Cyber Asset definition indicates a connection limit of 30 calendar days and here, we allow something to be considered in a lower impact category if it is intended to be in service for 6 calendar months or less. It seems to have a gap between 30 calendars days and 6 calendar months for these BES Cyber Assets. If these are LI BES CA, they could then easily pass under the radar, possibly not being identified (see previous comment on R1). M1. Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls. Does it mean the controls in CIP-005-5 R1.1 and CIP-006-5 R.1.1 could be used as evidence for CIP-002-5 R1? Isn't it like a circular reference? R1 Should add to R1, identification of "transient cyber assets". TCA could be a major threat source and should be "controlled".

No
For clarity in R2 and M2, request 1) using the term “annual” instead of all these extra words and 2) making “annual” a Glossary term
Yes
No
R1 [Violation Risk Factor: Medium] [Time Horizon: Operations Planning] According to Order on Violation Risk Factors, 119 FERC 61, 145 (May 18, 1907) and Guidelines for Developing Violation Risk Factors and Violation Severity Levels NERC (August 10, 2009), this requirement is administrative in nature, is in a operation planning time frame and if violated, would not be expected to affect the electrical state or capability of the BES, or the ability to effectively monitor, control, or restore the BES, or under the emergency, abnormal, or restorative conditions anticipated by the preparations, would not be expected to affect the electrical state or capability of the BES, or the ability to effectively monitor, control, or restore the BES. So this VRF should be "Lower" as it is for R3 and R6.
Yes
R2 [Violation Risk Factor: Medium] [Time Horizon: Operations Planning] Efficiency of a policy is not evaluated here. A bad policy is often not better or could be even worse than no policy at all. Thus, violating this requirement should not have a medium factor risk. Should be "Lower" as previous comment on R1… and the same VRF as R3.
Yes
The term “annual” is not used consistently in the Rational, Requirement and Measure. Request a consistent use of “annual” throughout R3.
No
M4’s last bullet on page 12 is inconsistent with R4 since M4 requires periodic training instead of R4’s making staff aware of cyber security policies. Request that M4 be updated to be consistent with R4. M4. Evidence may include, but is not limited to: • Policies are accessible on the corporate Intranet site • Documented records that policies have been provided to contactors where access to BES Cyber Systems is authorized • Policies are posted on company bulletin boards Because policies would be accessible to everyone, particular attention should be taken to be those policies are exempt of BES Cyber System Information.
Yes
No
Requirement has a typo. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes? Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”
Yes
Yes
No
Request clarification of whether personnel with access to only protected information need training / awareness. SDT should include this as additional Requirement Should be able to exclude people using BES cyber system in consultation only and has no impact on the operability of it Recommend removal of R2.3 and R2.4 since they are redundant to R2.2, or explain the difference between R2.2 and (R2.3 and R2.4) Request removing “potential” from R2.7 since training should include how to determine whether a BES System Event occurred or not.
No
R3 Part 3.1 & 3.2 - Applicability High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets R3 Require completion of the training specified in CIP-004-5 R2… where applicability is limited to: - High Impact BES Cyber Systems - Medium Impact BES Cyber Systems So it is useless here to apply it larger. Should have the same "Applicability" for both

R2 and R3.
No
For all R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to "grandfather" previous seven-year criminal checks executed for the previous versions of CIP Standards. The additional language should spell out when this "grandfathering" expires, which is also when new check will be required R4 [Violation Risk Factor: Medium] [Time Horizon: Operations Planning] According to Order on Violation Risk Factors, 119 FERC 61, 145 (May 18, 1907) and Guidelines for Developing Violation Risk Factors and Violation Severity Levels NERC (August 10, 2009), this requirement is administrative in nature, is in a operation planning time frame and if violated, would not be expected to affect the electrical state or capability of the BES, or the ability to effectively monitor, control, or restore the BES, or under the emergency, abnormal, or restorative conditions anticipated by the preparations, would not be expected to affect the electrical state or capability of the BES, or the ability to effectively monitor, control, or restore the BES. Like it is for R6 "Access Management Program", this VRF should be "Lower"
No
For clarity, recommend changing 5.1 from "authorized electronic or unescorted physical" to "authorized electronic or authorized unescorted physical"
No
For R6.1 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.3 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber System Information. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.6 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I” in Information. Part 6.1 to part 6.6 – Applicability Associated Protected Cyber Assets Here the definition given in this CIP is too restrictive. Instead, we should used "Protected Cyber Assets" as given in CIP v5 Definition: meaning all cyber asset inside an ESP. R6 Part 6.5 – Requirements : Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions. Before requiring some verification, the Access Management Program should require specification/identification of such accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions. R6 Part 6.6 – Requirements : Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.Before requiring some verification, the Access Management Program should require specification/identification of such access privileges are correct and the minimum necessary for performing assigned work functions. R6 Access Management Program Like R4 Personnel Risk Assessment, Program and R5 Personnel Risk Assessment, may be the R6 Access Management Program should be broke in 2 different requirements: "Access Management Program" and Access Management"
No
Request that 7.1's footnote be moved into the Requirement Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend removing the "following the resignation or termination" since it is redundant and inconsistent with the sibling Requirements Recommend changing 7.4 from "For

resignations or terminations," to "For terminations, resignations, reassignments, or transfers," What about the individual's user accounts on Protected Cyber Asset? It's possible that user have only user accounts on Protected Cyber Asset and any on BEC Cyber Assets. Should be reworded to: For resignations or terminations, revoke the individual's user accounts on Cyber Assets… Recommend changing 7.5 : Here the definition given in this CIP is too restrictive. Instead, we should used "Protected Cyber Assets" as given in CIP v5 Definition: meaning all cyber asset inside an ESP.
Yes
No
Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point or not? Request clarification on 1.5's "at each EAP". Is that inside or outside or both? Part 1.2 Applicability : High Impact BES Cyber Systems, Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Protected Cyber Assets Should add: "Associated Electronic Access Control or Monitoring Systems Following basic security principles, those cyber assets should have at least the same protection level that the cyber asset that they control. Because proposed revised (see comment) definition of Electronic Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems exclusive of Electronic Access Point composing the Electronic Security Perimeter", there will have no problems for that cyber asset to be protected by one Electronic Security Perimeter: it is not a fence over the fence situation. We have to keep in mind that AEACMS include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems. 1.1 Change Rationale: Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones and… What is the meaning of less trusted network zones? Is it all other network zones outside an ESP? Does the corporate network a less trusted network zones?
No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete R2.2 ADD "if technical possible" meaning add the possibility to have a TFE for this requirement. When not possible to have log every day "Real time" systems R2 : hould add another part in R2 –Remote Access Management requiring the Intermediate Device should not be located within ESP. It is implied by definition of "protected cyber asset" are all those asset within the ESP that are not BES cyber asset and by R2.1 where it is specified that a Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset. If ID is implement within the ESP, it should be considered as a PCA and then not directly accessible. If it is not specifically required, then someone could implement the ID within the ESP and there is no violation of any requirement. Should add requirements, guidance or definition about Cyber Assets associated with communication networks and data communication links within Electronic Security Perimeters (like Ethernet switches and routers) because their misconfiguration or unavailability could have a direct impact to BES CA. Their management should be done thru an Associated Electronic Access Control or Monitoring Systems. Should add requirement to "issue real-time alerts (to individuals responsible for response) in response to detected malicious communication at any EAP of a Electronic Security Perimeter", as with CIP-006-5 R1.4, for physical counterpart This is included by CIP-007-5 R4.2, but is it the right place? Should add requirements for logging of electronic access thru EAP of a Electronic Security Perimeter", as with CIP-006-5, R1. 6 for physical counterpart. Partially included by CIP-007-5 R4.3 but is it the right place? Should add requirements for testing of the AEACMS at EAP of a Electronic Security Perimeter to ensure the required functionality is being provided, as with CIP-006-5 R3.1 for physical counterpart Should add requirements for logging dates, time, and duration for failures or outages of access control, logging, and alerting systems of the AEACMS at EAP of an Electronic Security Perimeter to ensure the required functionality is being provided, as with CIP-006-5 R3.2 for physical counterpart.

Yes
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress" Request Requirement 1.2 be updated to allow "escored physical access." Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.4 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. " to "issue real time alerts for detection of breach through an access point" For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6 R1.3 The verification of outbound traffic is considered overkill since must attacked are from inside. For companies that have strong unions it could be difficult to be compliant to this requirement. Part 1.2 Applicability Medium Impact BES Cyber Systems. Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets Should add: Associated Physical Access Control Systems Because definition of Physical Access Control Systems: "Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers." There are no problems for that cyber asset to be protected by one Defined Physical Boundaries: it is not a fence over the fence situation. Part 1.3 Applicability High Impact BES Cyber Systems. Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets Should add: Associated Physical Access Control Systems Because definition of Physical Access Control Systems: "Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers." There are no problems for that cyber asset to be protected by one Defined Physical Boundaries: it is not a fence over the fence situation.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1 Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, " Part 2.1 Applicability High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets Part 2.1 Requirements Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.Applicability column is wider than the requirement that limit the identification of source or sources that are monitored for the release of security related patches, or updates for all software and firmware only to those associated with BES Cyber System or BES Cyber Assets. Should be reworded to remove this limitation to be sure that is applicable to all cyber asset indicated in the column Applicability.
No
Request clarification on what the "Associated" "Applicability" (High/Medium/Low BES Impact) for 3.1 and 3.2 Request capitalization of "locally mounted hardware or devices" in Requirement 3.1 so that it refers back to the defined term "Locally Mounted Hardware or Devices" R3.1: Return to 36 months. Require clarification on maintenance, can a normal maintenance on an appliance can be considered as maintenance.
Yes
No
Request clarification on 1.1, is this at the BES Cyber System level or at the Asset level or can the Entity chose? Request clarification on 1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? R1 and R2: ADD “if technical possible” meaning add the possibility to have a TFE for this requirement
No

Request clarification of "remediation" in 2.2 since it reads that the patch must be applied,which does not allow to have an exception when applying the patch is the worse scenario such as creating a denial of service For 2.2, suggest wording like "create a remediation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied" What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to the patch or the overall process? R1 and R2: ADD “if technical possible” meaning add the possibility to have a TFE for this requirement
No
Request allowances in 3.3 for signatures/pattern updates that cause trouble Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media" The Measure for 3.4 does not match the Requirement R3.3: Signature that require “Engine restart may ne require for version. 30 days is short for “Real time systems” and a different delay (longer) for Medium since the High will go first. Part 3.3 – Requirement Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). As for R2 Security Patch Management, and demonstrated by event McAfee DAT 5958 (2010-04-22), applying an update of malicious code protection without prior verification of signatures or patterns file could jeopardize the availability or integrity of the control system. This requirement should be reworded to handles the situation where malicious code protections updates can come from an original source (such as an ant-virus vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. As again R2, timeframe should run from availability from this second source. R3.5: ADD “if technical possible” meaning add the possibility to have a TFE for this requirement. If we have a paper log it does not prove anything. Part 3.5 Requirements Log each Transient Cyber Asset connection. This requirement should be move to CIP-005-5 because it is more related to Electronic Security Perimeter than this CIP more oriented about "system". (see comment in CIP-005-5)
No
Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities Request clarification on 4.3, does the failure need to be detected within a calendar day? Request the rationale of 4.5's "two weeks". We recommend one month as a compromise between the prior version's 90 days and the suggested one week R4.1.4: Any detected malicious activity is too wide. Need to be clarified (double avec TFIST) R4.3: ADD “if technical possible” meaning add the possibility to have a TFE for this requirement. When not possible to have log every day “Real time” systems We consider it to be not required. 24hr delay is short and too many operational and temporary situation may arise which come back to normal shortly after(24 – 48hrs) R4.5: Every 2 weeks does not match with timeframe of R4.3.When we have automatic events correlation, the 4.5 should not be required every 2 weeks. We suggest 60 days. Part 4.1 Requirements Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: Cyber Security Incidents is capitalized here and not defined in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" but BES Cyber Security Incidents and it seems having some discrepancy between the meanings of these terms. Should be revised. Part 4.1 Requirements 4.1.1. Any detected failed access attempts at Electronic Access Points This requirement should be move to CIP-005-5 because it is more related to Electronic Security Perimeter than this CIP more oriented about "system". (see comment in CIP-005-5) Successful access thru an EAP should be logged too. In fact, it should be reworded to include all inbound and outbound successful or failed access thru an EAP.
No
For 5.2, does the CIP Senior Manager or delegate approval policy or procedure for each authorization of access? In 5.2, should the Requirement be interpreted as "each use" as in "The CIP Senior Manager or delegate must authorize the use of each administrator, shared, default, or other generic account types." Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses." R5.5: Why the TFE was removed? ADD “if technical possible” meaning add the possibility to have a TFE for this requirement. When not possible to have log every day “Real time” systems. Part 5.1 Applicability High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or

Monitoring Systems Associated Protected Cyber Assets Part 5.1 Requirements Validate credentials before granting electronic access to each BES Cyber System. Applicability column is wider than the requirement limiting to validate credentials before granting electronic access only to BES Cyber Systems. Should be reworded to remove this limitation to be sure that is applicable to all cyber asset indicated in the column Applicability Part 5.4 Requirements Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. This requirement should be reworded as "BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" be placed in "Applicability" instead of "All Responsible Entities"

Yes

No

Part 5.1 Applicability High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets Part 5.1 Requirements Validate credentials before granting electronic access to each BES Cyber System. Applicability column is wider than the requirement limiting to validate credentials before granting electronic access only to BES Cyber Systems. Should be reworded to remove this limitation to be sure that is applicable to all cyber asset indicated in the column Applicability Part 5.4 Requirements Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. This requirement should be reworded as "BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" be placed in "Applicability" instead of "All Responsible Entities"

No

2.1 is a new Requirement. Request the rationale for this new Requirement Recommend changing from "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." to "When a BES Cyber Security Incident is classified or identified, the Responsible Entity must follow its incident response plan." For 2.2, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard"

No

For 3.1, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard" Recommend that 3.2 wording be consistent with the 2.2 wording For 3.3, recommend changing 1) "Update" to "Update as necessary" and 2) "the completion of the review of that plan" to "the completion of the review performed in 3.2"

Yes

No

For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommend removing Requirement 1.5. Reliability's top priority is restoration of service. Forensics in a recovery mode may not support BES reliability and requiring such actions may negatively impact the BES Cyber System restoration process.

Recommend that 2.1 be implemented 180 days from the effective date of the Standard. For 2.1, request clarification , is “full operational exercise” the same as “functional exercise” as described in the rational? For 2.1 and 2.3, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard" For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative

environments". What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the Standard.
No
For 3.1 recommend 1) removing "or when BES Cyber Systems are replaced" as it addressed in CIP-009 R3.4 and 2) removing "and document any identified deficiencies or lessons learned" as they are addressed in CIP-009 R3.2 and R3.3. For 3.1, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard" Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Recommend that 3.4 be referenced by CIP-009 R3.1. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
Yes
No
Recommend changing 1.3 to avoid double jeopardy from "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." For 1.1, 1.2, 1.3 and 1.4, recommend changing the Requirements to be consistent with their Applicability --- from "For a change to the BES Cyber System" to "For a change to the BES Cyber System or Associated Systems or Associated Assets" Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold R1.1.4: We consider that baselines for "scripts" is a little extreme, need clarification on the type of script required R1.1.5: The requirement is redundant and is already documented in CIP-007-5 R1 R1.4.2: Add to this requirement the possibility to add the level of criticality. Not all changes require the verification. Have the possibility to classify the changes by type and level
No
Recommend removing "where technically feasible" from 2.1 since the remaining words should not need an exception
No
For 3.1 and 3.2, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard" Recommend changing 3.2 from "in a production environment." to "in a production environment, or a production environment." to allow Entities more flexibility in meeting this Requirement
Yes
No
Request clarification on 1.1. Some interpret this Requirement as what is the Entity's process for identifying BES Cyber Systems Information. If correct, the Measure should be "show me the methodology (document)." Others interpret these Measures as labeling BES Cyber System Information. For 1.3, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard"
No
Request that footnote 2 in 2.1 be moved into that Requirement R2.2: Suggestion of wording for the requirement " Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media". The objective of this requirement is to ensure that the data is not readable, the use of destroy is a little "over kill"
Yes
No
We understand that the table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Otherwise, this Scenario table is confusing because it repeatedly uses 12 months while the earlier text uses 18 months. Since Version 4 is not FERC approved, we are concerned about the possibility of version 4 being effective

while version 5 is in implementation, resulting in version 4 being effective for only a few months. Since there is no place for general comments, we provide them here • We understand that the auditors are not bound by the Measures. Request an explanation on the need for Measures if auditors are not bound by the provided Measures? What is the benefit to these Measures? Should the SDT's time be better invested elsewhere? • Recommend removing the "initial bookend" from the Requirements that specify period because eight activities (CIP-008 2.2, CIP-008 3.1, CIP-009 2.1, CIP-009 2.3, CIP-009 3.1, CIP-010 3.1, CIP-010 3.2, CIP-011 1.3) in these Standards that are unnecessarily burdensome to Entities. Another reason to remove these initial bookends is that the initial bookend's language forces the Entity to be compliant with two Versions of the Standards at the same time. We are not objecting to the initial bookend in other Requirements which are policy-oriented. The effective date should be the start of the period. Initial bookend typically says "Initially upon the effective date of the standard". • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different than other Standards. • Request clarification of the capitalized term "Facilities." Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5.
Individual
Annette Johnston
MidAmerican Energy Company
Yes
GENERAL DEFINITIONS COMMENTS: Version 5 proposes retiring three definitions and creating or revising 21 definitions. The NERC request form for development or revision of a definition for a term states the development of new definitions should be avoided unless absolutely necessary. The majority of these changes are not required to address FERC Order 706 directives or improve security and in a number of cases the changes introduce ambiguity instead of clarity. NERC's first annual report to FERC on TFEs was filed in September 2011 and noted that 241 entities had declared Critical Cyber Assets. These entities are complying with all of the CIP standards. Changes in terms require extensive resources to modify existing compliance programs. Proposed changes that are not for a directive and/or don't improve security should not be made. CRITICAL ASSETS and CRITICAL CYBER ASSETS COMMENT: Do not retire Critical Assets or Critical Cyber Assets. MidAmerican Energy supports retaining CIP-002-4, the legacy framework for identification of Critical Cyber Assets and adding impact categorization. Renaming the concept of Critical Cyber Asset serves no security purpose and only increases implementation costs and confusion for personnel trained in and operating CIP programs in place today. MidAmerican Energy supports a separate standard to identify which Critical Cyber Assets are designated as high impact and what additional controls they receive. As a result, Critical Cyber Assets would be either medium or high impact. MidAmerican Energy supports a separate standard to identify low impact Cyber Assets. The standard for lows would not use the term Critical Cyber Asset. PHYSICAL SECURITY PERIMETER COMMENT: Do not retire Physical Security Perimeter. Version 5 renames the term and revised the term's definition. Renaming the term serves no security purpose and is not a directive. It increases implementation costs. If it can be demonstrated that it will not reduce security, the definition for the term could be revised to drop "six-wall" in order to provide more flexibility (without changing the name for the term). BES CYBER ASSET COMMENT: Retain Critical Cyber Asset. Do not create this new definition. FERC Order 706 did not direct changes to Critical Cyber Asset. See Order 706 paragraph 284, where FERC "declined to direct that such a method" (for identifying Critical Cyber Assets) be incorporated in the standards. See also paragraph 285, where FERC "did not find sufficient justification to remove this provision" (Critical Cyber Asset must either have routable protocols or dial-up access). Industry produced a guidance document for identifying Critical Cyber Assets. The proposed definition has many ambiguous terms and references another new, ambiguous definition for BES Reliability Operating Services. Version 5 materials have not identified what delta (or difference in outcome) is intended by the proposed definition versus the existing framework. BES CYBER SECURITY INCIDENT COMMENT: Retain the current definition of Cyber Security Incident. Addition of "BES" in the term name is not a directive, adds no security and increases implementation costs. As commented elsewhere in this question, MidAmerican Energy supports retaining Critical Cyber Asset and Physical Security Perimeter, which are included in the existing definition, and does not support creating the new term of Defined Physical Boundary. BES CYBER SYSTEM COMMENT: MidAmerican Energy supports retaining CIP-002-4 and the legacy framework for identification of Critical Cyber Assets and does not support the CIP-002-5

framework for identification. However, MidAmerican supports the concept of grouping one or more Cyber Assets for flexibility so that some controls can be addressed at a “system” level. If a new definition is created, it should be based on grouping Cyber Assets for purposes of applying security controls at a system level. Do not use “BES.” Consider what Cyber Assets can be grouped. The draft definition only included 15 minute impact (BES Cyber Assets) and did not include the option of grouping “Protected Assets.” Why not? Aren’t there any controls that could be applied to those assets at a “system” level? The concept of excluding Transient Assets from the system is important to retain. BES CYBER SYSTEM INFORMATION COMMENT: The draft definition uses reworded content from CIP-003-4 R4.1 and adds “BES.” There is no directive, it does not increase security and does increase implementation costs. MidAmerican can support creating a definition from the CIP-003-4 R4.1 language unchanged. This language is: “The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.” BES RELIABILTY OPERATING SERVICES COMMENT: Drop this draft definition. It is 736 words full of ambiguity and lacking clarity. It creates multiple dependencies on other NERC Glossary terms and other NERC standards. It is not a directive. Version 5 materials have not identified what delta (or difference in outcome) is intended by the proposed definition versus the existing framework or if it improves security. Consideration could be given to comparing the content of the draft definition, the 2009 concept paper, ACTUAL identified Critical Cyber Assets and the NERC guideline to determine if there is a gap or lack of clarity, and the guideline could be revised. CIP EXCEPTIONAL CIRCUMSTANCE COMMENT: Version 4 requirements in CIP-004-4 R2 and R3 refer to specified circumstances such as an emergency. Start the definition with “One or more of the following circumstances, or other conditions of similar nature.” CIP SENIOR MANAGER COMMENT: No comment. CONTROL CENTER COMMENT: Delete the bullets for presentation and display of BES reliability or operability data and the bullet as too ambiguous. Delete the bullet for coordination of BES restoration activities as too ambiguous. Clarify the modifying phrases as follows: “two or more transmission facilities at two or more locations or for two or more BES generation facilities at two or more locations where the aggregated generation is 300 MW or more.” Ensure substations are not swept in as control centers just due to data concentrators. Revise BES Cyber Asset to Critical Cyber Asset to correspond to retaining CIP-002-4. CYBER ASSETS COMMENT: Keep Cyber Assets revision as it aligns with FERC Order 706 paragraph 285 where FERC “did not find sufficient justification to order the inclusion of communication links.” DEFINED PHYSICAL BOUNDARY (“DPB”) COMMENT: Do not adopt this definition. See comments on Physical Security Perimeter. ELECTRONIC ACCESS CONTROL OR MONITORING SYSTEMS COMMENT: The name for the term should be Electronic Access Control Systems and drop “monitoring” in the name to be consistent with Physical Access Control Systems. Drop the reference at the end of the definition to “or BES Cyber Systems.” In this definition, does monitoring mean alerting and logging? If so, say so in the definition sentence. In other places, version 5 is using “alert” instead of “monitor,” for example, in CIP-006 which says “control, alert or log.” ELECTRONIC ACCESS POINT (“EAP”) COMMENT: MidAmerican does not support the version 5 concept change away from the logical boundary or this definition as drafted. Also, as drafted, the definition lacks the concept of external connectivity and consequently could be applied to identify multiple access points between Cyber Assets within the ESP because some functionality on those Cyber Assets restricts communications between Cyber Assets. Retain the CIP-005-4 ESP logical border concept and electronic access point. If the existing definition is revised, it could be to specify the access point is an interface. It might also be revised to address CIP-005 interpretations. Changes were not, however, directed by 706. EXTERNAL CONNECTIVITY COMMENT: Revise to: “Routable or dial-up data communication through an Electronic Access Point between a Cyber Asset inside the Electronic Security Perimeter and a device external to the Electronic Security Perimeter.” EXTERNAL ROUTABLE CONNECTIVITY COMMENT: Revise to: “Routable data communication through an Electronic Access Point between a Cyber Asset inside the Electronic Security Perimeter and a device external to the Electronic Security Perimeter.” (Revised to be consistent with External Connectivity.) INTERACTIVE REMOTE ACCESS COMMENT: No comments. INTERMEDIATE DEVICE COMMENT: No comments. PHYSICAL ACCESS CONTROL SYSTEMS COMMENT: Drop Defined Physical Boundary and return to Physical Security Perimeter. PROTECTED CYBER ASSET COMMENT: In versions 1 through 4, these are noncritical. If a definition is created, it should use the existing term of noncritical. “Noncritical Cyber Asset - A Cyber Asset using routable protocol and connected within an Electronic Security Perimeter, excluding Critical Cyber Assets and Transient Cyber

Assets." REPORTABLE BES CYBER SECURITY INCIDENT COMMENT: Comments on this definition are not ready at this time, awaiting the next actions on the revisions to the EOP standard. TRANSIENT CYBER ASSET COMMENT: Refer to Critical Cyber Assets and Noncritical Cyber Assets. Might Transient Cyber Assets also be connected to Electronic Access Control Cyber Assets? "A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a Cyber Asset inside an Electronic Security Perimeter, 2) … and 3)…"
Yes
GENERAL CIP-002 COMMENTS: Retain CIP-002-4 and Attachment I as approved by industry and NERC BOT and recommended to FERC. Accomplish categorization in a separate standard for high impact Cyber Assets and in a separate standard for low impact Cyber Assets. The industry has met FERC Order 706 directives for CIP-002. GENERAL CIP-002-5 ATTACHMENT COMMENTS: The specific delta (or difference in outcome) of the proposed Attachment I changes has not been identified or supported in the version 5 materials.
No
R1 REQUIREMENT COMMENTS: Retain CIP-002-4 and Attachment I as approved by industry and NERC BOT and recommended to FERC. Accomplish categorization in a separate standard for high impact Cyber Assets and in a separate standard for low impact Cyber Assets. The industry has met FERC Order 706 directives for CIP-002.The specific delta (or difference in outcome) of the proposed framework changes has not been identified or supported in the version 5 materials. NERC's first annual report to FERC on TFEs was filed in September 2011 and noted that 241 entities had declared Critical Cyber Assets. These entities are complying with all of the CIP standards. Retaining the version 4 framework allows entities to preserve and leverage investments in versions 1 through 4 and evolve to version 5. There was significant industry opposition to the version 5 framework change in the 2009 concept paper. These concerns continue to be valid today: unclear where to start, too broad, abstract, too complex, does not provide any additional clarity or value versus the current process and does not provide detail as to why the proposed concept is an improvement or will improve reliability. It will increase implementation costs for entities with existing programs. It has the potential to impede timely progress in resolving remaining FERC directives and implementing security improvements in the other CIP standards.
No
R2 REQUIREMENT COMMENTS: Retain CIP-002-4 and Attachment I as approved by industry and NERC BOT and recommended to FERC.
No
This standard has a high VRF that applies to requirements for both high and medium impact asset categories. We recommend a medium VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with proposed revisions to CIP-002 and the VRFs.
No
GENERAL COMMENTS ON CIP-003-5 Most of the changes made to CIP-003 were not directed by FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for entities with existing programs. MidAmerican Energy suggests the FERC directives be addressed within a structure and language that is more in line with version 4. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these also need revisions to be more in line with our proposed changes to the requirements. See also comments on CIP-010-1 and CIP-011-1. MidAmerican Energy does not support moving CIP-003-4 R6 to the a new CIP-010-1 separate standard. MidAmerican Energy does not support moving CIP-003-4 information protection requirements to the new CIP-011-1 separate standard. This was not directed by FERC, does not improve security and increases implementation costs for entities with fully implemented CIP programs. These requirements could remain within CIP-003-4 and preserve the numbering of the requirements within this standard. We propose the following requirements for CIP-003-5: R1: Cyber Security Policy R2: Leadership R3: Exceptions R4: Information protection The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. EXCEPTION COMMENTS: The V4 to V5 mapping document states that CIP-003-4 R3 Exceptions was deleted because "the FERC Order 706 made clear that you could not take exceptions to the policy." MidAmerican disagrees with this statement. In paragraph 376, FERC directed the ERO to "clarify that

the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards." Further, in paragraph 377, FERC stated "We do not believe that an entity's decision to not follow its cyber security policy in a particular situation should trigger a penalty, as long as no Reliability Standard Requirement (other than Requirement R1 in CIP-003-1) is violated as a result." Paragraphs 372 through 378 include discussion on documentation of exceptions and oversight by the ERO and Regional Entities. While the new term "CIP Exceptional Circumstance" has been introduced in Version 5, its use is limited to three standards (CIP-004, CIP-007 and CIP-010). There are situations outside of these three standards that may require an exception to the cyber security policy. Therefore, MidAmerican suggests going back to the Version 4 language for exceptions and modifying it to meet the FERC directive. R1 REQUIREMENT COMMENT: MidAmerican Energy proposes going back to the language in CIP-003-4 R2 for leadership and making minor modifications to address FERC directives not already addressed.
No
R2 REQUIREMENT COMMENT: MidAmerican Energy proposes going back to the language in CIP-003-4 R1 on the cyber security policy. FERC directed the ERO to provide additional guidance for topics and processes that the cyber security policy should address, but FERC did not direct any changes to the requirement itself. R2 REQUIREMENT PROPOSED REVISED TEXT: "Document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following: * The cyber security policy addresses the CIP standards, including provision for emergency situations; The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets; * Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2."
No
R3 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be deleted, in conjunction with our suggestion to go back to the CIP-003-4 R1 language, which includes the annual review and approval by the senior manager.
No
R4 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be deleted, in conjunction with our suggestion to go back to the CIP-003-4 R1 language, which includes a requirement to make the policy readily available to personnel who have access to Critical Cyber Assets. There was no FERC directive to change this requirement.
No
R5 REQUIREMENT COMMENTS: MidAmerican Energy proposes this requirement be deleted, in conjunction with our suggestion to go back to the CIP-003-4 R2 language, which includes language on delegations. FERC Order 706 did not direct any changes to the requirement. The draft requirement would create an additional administrative burden that does not improve security of the Bulk Electric System and creates a disproportionate amount of bureaucratic work.
No
R6 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be deleted, in conjunction with our suggestion to go back to the CIP-003-4 R2 language, which includes language on changes to the senior manager. FERC Order 706 did not direct any changes to CIP-003-4 R2.2. Proposed changes do not increase security over the current requirement but do increase implementation costs. The current requirement already covers changes to the senior manager that must be documented within thirty calendar days of the effective date.
No
This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with the proposed revised VRFs and other revisions proposed to the requirements. FERC Order RR08-4-000, paragraph 27, states that "as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…" We think some of the CIP-003-5 requirements could have gradated VSLs particularly as most of these requirements have lower Violation Risk Factors.
No
GENERAL COMMENTS ON CIP-004-5 Many of the changes made to CIP-004 were not directed by

FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for entities with existing programs. MidAmerican Energy suggests the FERC directives be addressed within a structure and language that is more in line with version 4. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. Further, CIP-004-4 states the entity will keep all documentation and records from the previous full calendar year unless directed by the Compliance Enforcement Authority to retain specific evidence for a longer period as part of an investigation. Version 5 expands this to three calendar years without justification. CIP-004 requirements generate a tremendous amount of detail records. The "canned" C.1.2 Evidence Retention section in this standard should be revised to correspond to the current obligation. We propose the following requirements for CIP-004-5: R1: Awareness R2: Training R3: Personnel Risk Assessment R4: Access R1 REQUIREMENT COMMENT: There were no FERC directives to change the language of this requirement. MidAmerican Energy proposes going back to the version 4 language. We would not be opposed to moving the mechanism examples to guidelines. R1 REQUIREMENT PROPOSED REVISED TEXT: "Establish, document, implement and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive ongoing reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms, such as: direct communications (for example, e-mails, memos, computer-based training); indirect communications (for example, posters, intranet, brochures); management support and reinforcement (for example, presentations, meetings)." R1 APPLICABILITY COMMENTS: Revise to medium and high impact assets.

No

R2 REQUIREMENT COMMENTS: Many of the changes made to this requirement were not directed by FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for entities with existing programs. MidAmerican Energy suggests the FERC directives be addressed within a structure and language that is more in line with version 4. MidAmerican has provided an example of how FERC directives could be incorporated into the version 4 structure. The draft version 5 did not address FERC Order 706, paragraph 435, which directed determination if modifications should be made to assure security trainers are adequately trained themselves. While we do not believe modifications are needed, we think the directive must be addressed somewhere in the draft standard so that FERC is aware of the determination on this directive. R2 REQUIREMENT PROPOSED REVISED TEXT: "R2.1 Establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets so that personnel understand how their actions or inactions could, even inadvertently, affect cyber security of all Cyber Assets within an Electronic Security Perimeter. R2.2 Review the cyber security training program annually, at a minimum, and update whenever necessary. R2.3. Ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency. R2.4. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-5, and include, at a minimum, the following core training elements appropriate to personnel roles and responsibilities: R2.5.1. The proper use of Critical Cyber Assets; R2.5.2. Physical and electronic access controls to Critical Cyber Assets; R2.5.3. The proper handling of Critical Cyber Asset information; R2.5.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident. R2.5.5. Networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of Critical Cyber Assets. R2.6. Maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records."

No

MidAmerican Energy proposes deleting this requirement, in conjunction with the suggested restructuring of R2 back to the version 4 language, since it already is covered.

No

R4 REQUIREMENT COMMENT: FERC Order 706, paragraph 443, directed change to require completion of personnel risk assessments before granting access. This change was made in an earlier version of the standard. There were no other FERC directives for the personnel risk assessment program requirement. We recommend version 4 language and numbering for CIP-004, R3 be retained. This

would mean using one table rather than two. R4 REQUIREMENT PROPOSED REVISED TEXT: (Note: Numbering would become R3) “R3 Document a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. Conduct a personnel risk assessment pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include: R3.1. Ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position. R3.2. Update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause. R3.3. Document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-5.”
No
FERC Order 706, paragraph 446, states the ERO should consider the issue of reviewing results of personnel risk assessments (PRA). This was not a directive. MidAmerican Energy would support the addition of criteria or a process for reviewing results of PRAs, but we suggest it be incorporated into the requirement discussed in question #16 (that MidAmerican would renumber to the legacy R3).
No
R6 REQUIREMENT COMMENT: In FERC Order 706, paragraph 381, the Commission stated its intent is to ensure there is a clear line of authority. Order 706 did not direct making the senior manager responsible for everything. We do not support requiring the CIP senior manager or delegate to authorize access as drafted in R6.1, R6.2 and R6.2 or the addition of ambiguity with the phrase “minimum necessary.” The version 5 draft is an additional administrative burden that does not commensurately improve security of the Bulk Electric System and creates a disproportionate amount of bureaucratic work. As mentioned in our comments on CIP-003, we propose retaining the existing V4 language for the leadership requirement. We propose the FERC directive on revocation of access be incorporated into the structure and wording from CIP-004-4 R4. CIP-004-5 R4 REQUIREMENT PROPOSED REVISED TEXT: Note: Under our proposed structure, this would become R4. “R4: Maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets. R4.1. Review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. Ensure access list(s) for contractors and service vendors are properly maintained. R4.2. Revoke such access to Critical Cyber Assets: R4.2.1 at the time of termination for personnel terminated for cause R4.2.2 by the end of the next calendar day for personnel who no longer require such access to Critical Cyber Assets.” MidAmerican Energy does not support CIP-004-5 R6.4, R6.5 and R6.6, which change an annual requirement in CIP-007-4 and makes it a quarterly requirement in version 5. The additional administrative work created is not offset by a commensurate improvement in security.
No
R7 REQUIREMENT COMMENTS: MidAmerican Energy proposes deleting this requirement, in conjunction with the suggested restructuring back to the version CIP-004-4 R4 language, since revocation already is covered.
No
This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with the proposed revised VRFs and revisions proposed to the requirements. FERC Order RR08-4-000, paragraph 27, states that “as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…” We believe most of the CIP-004-5 requirements could have gradated VSLs.
No
GENERAL COMMENTS ON CIP-005-5 The “canned” C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4.

See also comments on CIP-010-1. MidAmerican Energy does support combining the vulnerability assessment requirement from CIP-005-4 with CIP-007-4's vulnerability assessment requirement. GENERAL COMMENTS ON CIP-005-5 R1 While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. R1.1 REQUIREMENT COMMENTS: With our proposal to create a standard for controls that are only applicable to low impact assets/systems, this requirement would be moved to the new low impact standard with the following suggested changes. R1.1 MEASURES COMMENTS: Change "…documented technical and procedural…" to "…documented technical or procedural…" to be consistent with the requirement. R1.2 APPLICABILITY COMMENTS: CIP-005-4 combined with CIP-006-4 R2.2 do not require ESPs for Cyber Assets that authorize and/or log access to the Physical Security Perimeter. MidAmerican Energy does not support expanding the scope to include Associated Physical Access Control Systems. Removing these from scope will also eliminate confusion over the applicability in R1.3-R1.5 R1.2 APPLICABILITY PROPOSED REVISED TEXT: Remove "Associated Physical Access Control Systems." R1.2 REQUIREMENT COMMENTS: As literally written, R1.2 would require traffic between two Cyber Assets inside the ESP to go through an Electronic Access Point. R1.2 does not distinguish that the traffic connecting into the ESP is to go through an Electronic Access Point. Version 5 introduces a concept change that focuses on discrete Electronic Access Points rather than the logical Electronic Security Perimeter in prior versions. This concept change adds confusion and is not an Order 706 directive. MidAmerican does not support the concept change. R1.2 REQUIREMENT PROPOSED REVISED TEXT Use version 4 CIP-005 concepts. Address R1 to ensure that every Critical Cyber Asset resides in an ESP and R1.4 to protect non-critical Cyber Assets in an ESP. R1.3 REQUIREMENT COMMENTS: This requirement appears to combine both R2.1 and R2.2 from legacy. This does not add clarity and is not a directive. Retain legacy concepts. R1.3 REQUIREMENT PROPOSED REVISED TEXT: "Processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified." "At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services." R1.4 REQUIREMENT COMMENTS: Not a directive. May not be increasing security. More prescriptive. Use legacy language. R1.4 REQUIREMENT PROPOSED REVISED TEXT: "The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s)." R1.5 REQUIREMENT COMMENTS: The requirement should be to implement. "At" is not the best preposition, "through" is better. R1.5 REQUIREMENT PROPOSED REVISED TEXT: "Implement a method for detecting malicious communications through Electronic Access Points."

No

CIP-005 R2 GENERAL COMMENTS: Overall, MidAmerican Energy does not believe the proposed Intermediate Device and encryption sub requirements provide enough security benefit to offset the impact on operations. The Intermediate Device and encryption requirements also prescribe "how," not "what," is to be accomplished and do not allow room for alternate controls that could be equally or more effective. Narrow prescriptions in a rapidly changing technology environment obsolesce faster than the standards revision process can update. External routable connectivity is a different attack vector and warrants different treatment from dial up. MidAmerican Energy does not support requirements for dial up in this table. Our comment on CIP-005-5 R1 addresses securing dial up access. R2.1 APPLICABILITY COMMENTS: Add qualifier of External Routable Connectivity. Do not require for dialup. R2.1 APPLICABILITY PROPOSED REVISED TEXT: "High Impact BES Cyber Systems with External Routable Connectivity; Medium Impact BES Cyber Systems with External Routable Connectivity; Associated Protected Cyber Assets with External Routable Connectivity" R2.1 REQUIREMENT COMMENTS: The draft definition of Intermediate Device refers to implementing the functions of an Intermediate Device and includes the very important concept of proxy systems. Revise the text of the requirement to "Implement the functions of an Intermediate Device."(Project 2010-15 CIP-005 also proposed the verb "implement.") This makes it clearer in the requirement that the desired results are the functions of an Intermediate Device, not a device itself. This also aligns with the definition better than "Require an Intermediate Device" since the definition recognizes the functions may be implemented on one or more devices. The Intermediate Device definition as posted excerpt follows for reference: "Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside the Electronic Security Perimeter, as part of the Electronic

Access Point, or in a DMZ network." R2.1 REQUIREMENT PROPOSED REVISED TEXT: "Implement the functions of an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." R2.2 APPLICABILITY COMMENTS: Add qualifier of External Routable Connectivity. Do not require for dialup. R2.2 APPLICABILITY PROPOSED REVISED TEXT: "High Impact BES Cyber Systems with External Routable Connectivity; Medium Impact BES Cyber Systems with External Routable Connectivity; Associated Protected Cyber Assets with External Routable Connectivity" R2.2 REQUIREMENT COMMENTS: R2.2 is ambiguous on where encryption is required to start and stop. The last version posted for Project 2010-15 CIP-005 R6.2 attempted to address this with the following language: "Implement interactive remote access such that communications between the Cyber Asset initiating interactive remote access and the intermediate device are encrypted … while using a network that is shared with users not associated with the Responsible Entity." Correct "Reference to prior version: CIP-007 R3.1" because that requirement is about ports, not encryption. R2.2 REQUIREMENT PROPOSED REVISED TEXT: "Implement encryption when interactive remote access uses a network that is not associated with the Responsible Entity. Encrypt communications between the Cyber Asset initiating interactive remote access and where the Intermediate Device functions are implemented." R2.3 APPLICABILITY COMMENTS: Add qualifier of External Routable Connectivity. Do not require for dialup. R2.3 APPLICABILITY PROPOSED REVISED TEXT: "High Impact BES Cyber Systems with External Routable Connectivity; Medium Impact BES Cyber Systems with External Routable Connectivity; Associated Protected Cyber Assets with External Routable Connectivity" R2.3 REQUIREMENT COMMENTS: Correct "Reference to prior version: CIP-007 R3.2" because that requirement is about ports. Multi-factor authentication correlates closer to CIP-005-4 R2.4 strong procedural or technical controls at access points to ensure authenticity for external interactive access. R2.3 REQUIREMENT PROPOSED REVISED TEXT: No changes.

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with the revisions proposed for the VRFs and to the requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that "as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…" MidAmerican Energy believes it is possible to have gradated VSLs for many of the CIP-005-5 requirements.

No

CIP-006-5 GENERAL COMMENTS: See also comments on Definitions where we recommend we retain the NERC glossary term Physical Security Perimeter. The change from Physical Security Perimeter to Defined Physical Boundaries creates the need to update numerous procedure documents and physical security drawings, etc. Changing the term does not improve security, but increases costs for 241 entities that have PSPs. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. R1.1 APPLICABILITY COMMENTS: Add Medium Impact BES Cyber Systems with no External Routable Connectivity. R1.1 MEASURES COMMENTS: Change operational "and" procedural to operational "or" procedural to be consistent with the R1.1 requirement. R1.2 APPLICABILITY COMMENTS: Change Medium Impact BES Cyber Systems to Medium Impact BES Cyber Systems with External Routable Connectivity. R1.2 REQUIREMENT COMMENTS: FERC Order 706 didn't direct changes. The proposed changes do not improve security. Delete "that restricts access to only those individuals that are authorized." Access is covered in CIP-004. R1.2 REQUIREMENT PROPOSED REVISED TEXT: "All applicable Critical Cyber Assets shall reside within an identified Physical Security Perimeter. Each Physical Security Perimeter utilizes one or more different physical access control(s), where technically feasible." (Note: Use of the term CCA is recommended in CIP-002 comments.) R1.2 MEASURES COMMENTS: FERC Order 706 didn't direct changes. Current standards do not include controlling egress. R1.2 MEASURES PROPOSED REVISED TEXT: "Evidence may include, but is not limited to, language in the physical security plan that describes how access is controlled." R1.3 APPLICABILITY COMMENTS: "Associated Electronic Access Control or Monitoring Systems" as well as "Associated Protected Cyber Assets" can be read to include devices used for electronic access to a

Medium Impact BES Cyber System or used within a Medium Impact BES Cyber System's Electronic Security Perimeter. This requirement only applies to High Impact BES Cyber Systems. R1.3 APPLICABILITY PROPOSED REVISED TEXT: “High Impact BES Cyber Systems; Electronic Access Control or Monitoring Systems associated with High Impact BES Cyber Systems; Protected Cyber Assets located within a High Impact BES Cyber System Electronic Security Perimeter” R1.3 REQUIREMENT COMMENTS: With our proposal to create a standard for controls that are only applicable to high impact assets/systems, this requirement would be moved to the new high impact standard with the following suggested changes. The phrase "different and complementary" is not clear. R1.3 REQUIREMENT PROPOSED REVISED TEXT: "All applicable Cyber Assets shall reside within an identified Physical Security Perimeter. Each Physical Security Perimeter must utilize two or more different physical access controls, where technically feasible. Physical access controls may be provided by single devices with multiple access control measures." R1.3 MEASURES COMMENTS: FERC Order 706 didn't direct changes. Current standards do not require controlling egress. R1.3 MEASURES PROPOSED REVISED TEXT: "Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * language in the physical security plan that describes how access is controlled, or * physical security perimeter drawings, or * list of physical security perimeters and access points into the PSPs” R1.4 APPLICABILITY COMMENTS: Change Medium Impact BES Cyber Systems to Medium Impact BES Cyber Systems with External Routable Connectivity. R1.4 REQUIREMENT COMMENTS: FERC Order 706 did not direct changes. The proposed changes do not improve security. Change from Physical Security Perimeter to Defined Physical Boundaries increases paperwork and related costs to update procedure documents with no security improvement. R1.4 MEASURES COMMENTS: Change from Physical Security Perimeter to Defined Physical Boundaries increases paperwork and related costs to update procedure documents with no security improvement. Add human observation from CIP-006-3 R5 as other possible alert evidence. R1.4 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * language in the physical security plan that describes the issuance of automated or human observation alerts in response to unauthorized physical access through any access point in a Physical Security Perimeter, or *additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that documents that these alerts were generated” R1.5 APPLICABILITY COMMENTS: Change Medium Impact BES Cyber Systems to Medium Impact BES Cyber Systems with External Routable Connectivity. R1.5 REQUIREMENT COMMENTS: FERC Order 706 didn't direct changes. The proposed changes do not improve security. R 1.5 REQUIREMENT PROPOSED REVISED TEXT: "Immediately alert personnel responsible for a response to unauthorized physical access to Physical Access Control Systems." R1.5 MEASURES COMMENTS: Add human observation from CIP-006-3 R5 as other possible alert evidence. R1.6 APPLICABILITY COMMENTS: Change Medium Impact BES Cyber Systems to Medium Impact BES Cyber Systems with External Routable Connectivity. R1.6 REQUIREMENT COMMENTS: FERC Order did not direct any changes. It is redundant to restate the applicability information. Suggest going back to legacy language. R1.6 REQUIREMENT PROPOSED REVISED TEXT: "Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: computer logging, video recording or manual logging. Retain physical access logs for at least ninety days." R1.6 MEASURES COMMENTS: FERC Order did not direct any changes. R1.6 MEASURES PROPOSED REVISED TEXT: "Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * language in the physical security plan that describes logging and recording of physical entry into Physical Security Perimeters, or * additional evidence to demonstrate that this logging and recording has been implemented, such as logs of physical access into Physical Security Perimeters that show the date of entry into Physical Security Perimeters."
No
R2.1 REQUIREMENT COMMENTS: FERC Order 706 did not direct changes. The change from Physical Security Perimeter to Defined Physical Boundaries increases paperwork and related costs to update procedure documents with no security improvement. R2.1 REQUIREMENT PROPOSED REVISED TEXT: "Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Physical Security Perimeter." R2.1 MEASURES COMMENTS: FERC Order 706 did not direct changes. The change from Physical Security Perimeter to Defined Physical Boundaries increases paperwork and related costs to update procedure documents with no security improvement.

R2.1 MEASURES PROPOSED REVISED TEXT: "Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters, or * additional evidence to demonstrate that the process was implemented"
No
R3.1 APPLICABILITY COMMENTS: Add language to clarify to which systems the physical access controls are referring. R3.1 APPLICABILITY PROPOSED REVISED TEXT: "Associated Physical Access Control Systems and locally mounted hardware or devices associated with Physical Security Perimeters for High Impact BES Cyber Systems; Medium Impact BES Cyber Systems; Associated Electronic Access Control and Monitoring Systems; and Associated Protected Cyber Assets" R3.1 MEASURES COMMENTS: Delete language that repeats the requirements. R3.1 MEASURES PROPOSED REVISED TEXT: "Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * dated maintenance records, or * other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months." R3.2 APPLICABILITY COMMENTS: Delete "or Monitoring" to match the defined term. R 3.2 APPLICABILITY PROPOSED REVISED TEXT: "Associated Physical Access Control Systems" R3.2 REQUIREMENT COMMENTS: FERC Order 706 did not direct changes to this requirement. Suggest going back to legacy language. R3.2 REQUIREMENT PROPOSED REVISED TEXT: “Retain outage records for a minimum of one calendar year.”
No
The Table of Compliance Elements cites references to sub requirements that appear to be incorrect: Lower – Part 1.7 should point to 1.6; High – Part 1.6 should point to 1.5. R1.4 VRF COMMENT: The VRF for R1 is "Medium." This is not appropriate with R1.5, which is Associated Physical Access Control Systems, or for R1.1, which is Low Impact and Associated Physical Access Control Systems. This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with revisions proposed to the VRFs and requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that “as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…” MidAmerican Energy believes it is possible to have gradated VSLs for many of the CIP-006-5 requirements.
No
CIP-007-5 GENERAL COMMENTS: While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. See also comments on CIP-010-1 and CIP-011-1. MidAmerican Energy does not support moving CIP-007-4 requirements to the new CIP-010-1 separate standard. This was not directed by FERC, does not improve security and increases implementation costs for entities with fully implemented CIP programs. These requirements could remain within CIP-007-4 and preserve the numbering of the requirements within this standard. One exception is that we support combining the vulnerability assessment requirement from CIP-005-4 with CIP-007-4’s vulnerability assessment requirement. The “canned” C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. R1.1 REQUIREMENT COMMENTS: FERC Order 706 didn't direct changes. Requiring documentation of the need for remaining logical network accessible ports is burdensome and does not improve security. "Services" is absent from this requirement. The table heading still shows "Ports and Services." R1.1 REQUIREMENT PROPOSED REVISED TEXT: "Disable or restrict access to unnecessary logical network accessible ports. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed necessary." R1.1 MEASURES COMMENTS: FERC Order 706 didn't direct changes. Requirement revisions require Measures revisions. R1.1 MEASURES PROPOSED REVISED TEXT: Evidence may include, but is not limited to, documentation of how unnecessary logical network accessible ports for Critical Cyber Assets have been disabled. R1.2 REQUIREMENT PROPOSED REVISED TEXT: “Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media by disabling, restricting or labeling with a sign.” R1.2 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to, documentation of how unnecessary

physical input/output ports have been disabled, restricted either logically through system configuration or physically using a port lock or labeled with a sign.”
No
R2.1 REQUIREMENT COMMENTS: FERC Order 706 did not direct any changes. Clarify monitoring is for "security related" updates to software and firmware, which is comparable to security related patches. 2.1 REQUIREMENT PROPOSED REVISED TEXT: “Identify a source or sources that are monitored for the release of security related patches, or security related updates for all software and firmware associated with BES Cyber System or Critical Cyber Assets.” 2.1 MEASURES COMMENTS: Delete the last sentence regarding list sorting. 2.1 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to, a list of sources that are monitored on an individual BES Cyber System or Critical Cyber Asset basis.” R2.2 REQUIREMENT COMMENTS: Recommend two separate requirements, one for identifying applicable security related updates within 30 days of release and one for creating a remediation plan within 60 days of release unless the security related update is installed within 60 days. If installed within 60 days, the remediation plan is not required. Also add “security-related” before “updates.” 2.2 REQUIREMENT PROPOSED REVISED TEXT: First New Requirement – “Identify applicable security-related patches or security-related updates within 30 days of release from the identified source.” Second New Requirement – “Create a remediation plan, or revise an existing remediation plan, within 60 days of release from the identified source for applicable security-related patches or security-related updates to address vulnerabilities. A remediation plan is not required for security patches or security upgrades installed within 60 days of release from the identified source.” R 2.2 MEASURES COMMENTS: Revised Requirements result in revised Measures. R2.2 MEASURES PROPOSED REVISED TEXT: First New Measure – “Evidence may include, but is not limited to, an assessment conducted by, referenced by, or on behalf of a Registered Entity of security-related patches or security-related updates released by the documented sources.” Second New Measure – “Evidence may include, but is not limited to, a dated remediation plan showing when the vulnerability will be addressed or documentation showing the security-related patches or security-related updates have been installed within 60 days.” R2.3 REQUIREMENT COMMENTS: Change rationale indicates this requirement is for implementation of the remediation plan, subject to exceptions. R2.3 REQUIREMENT PROPOSED REVISED TEXT: “Implement remediation plans, allowing for CIP Exceptional Circumstances.” R2.3 MEASURES COMMENTS: Although the "Background" section states bullets in Measures indicates any one of the bulleted items, not all of them, this needs to be clear in the Measures section to be enforceable. Replace semi-colons with "comma, or" at the end of each bullet.
No
R3.1 REQUIREMENT COMMENTS: The requirements need to be clear on the competency based approach. It is only in the summary of changes and application guidelines. It needs to be in the requirement that is enforceable. Methods do not have to be used on every single Cyber Asset. R3.1 REQUIREMENT PROPOSED REVISED TEXT: "Deploy method(s) to deter, detect, or prevent malicious code based on the Cyber Asset's susceptibility to malware. Methods do not have to be used on every single Cyber Asset." R3.2 REQUIREMENT COMMENTS: Malicious code can be mitigated in various ways depending on many variables. R3.2 REQUIREMENT PROPOSED REVISED TEXT: “Mitigate identified malicious code.” R3.2 MEASURES COMMENTS: Each listed item should be separated by “or”. R3.3 REQUIREMENT COMMENTS: Include testing prior to updating. R3.3 REQUIREMENT PROPOSED REVISED TEXT: “Test and update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).” R3.3 MEASURES COMMENTS: List of measures should be separated by “comma or.” Limit evidence retention period to 90 days because retaining it for three years becomes burdensome. R3.3 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to, current signature or pattern updates, or screen shots showing the configuration of signature, or pattern updates for automated controls, or work logs showing the signature, or pattern updates for manual controls. Evidence to be retained for 90 days.” R3.4 APPLICABILITY COMMENTS: Remove the Associated Physical Access Control Systems and Associated Electronic Access and Control Monitoring items from the list. Protection is for Transient Cyber Assets and removable media when connected to Medium or High Impact BES Cyber Systems or Protected Cyber Assets according to the proposed version 5 requirements. R3.4 REQUIREMENT COMMENTS: Insert “known” prior to malicious code. It is reasonable to expect entities to protect against known malicious code, which also may protect for some unknown malicious code. However, it is not possible to protect against all unknown malicious

code. Revise the labels to use version 4 descriptions and NERC glossary terms for Critical and noncritical Cyber Assets. There is no security benefit to changing the labels. Changing the labels will be costly for the 241 entities that already have programs and documentation with these terms. R3.4 REQUIREMENT PROPOSED REVISED TEXT: “Deploy method(s) to deter, detect, or prevent known malicious code on Transient Cyber Assets and removable media when connecting them to Medium or High Impact Critical Cyber Assets or Associated Noncritical Cyber Assets.” R3.4 MEASURES COMMENTS: Logs showing when Transient Cyber Assets were connected to Critical Cyber Assets or Noncritical Cyber Assets is in CIP-007-5 R3.5. Also, including it here creates double jeopardy. It should not be included here. R3.4 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent known malicious code on Transient Cyber Assets and removable media.” R3.5 APPLICABILITY COMMENTS: Delete Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems because they are not Transient Cyber Asset related. R3.5 REQUIREMENT PROPOSED REVISED TEXT: “Log each Transient Cyber Asset connection to Medium or High Impact Critical Cyber Assets or Associated Noncritical Cyber Assets.” R3.5 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to Medium or High Impact Critical Cyber Assets or Associated Noncritical Cyber Assets.”
No
R4.1 REQUIREMENT COMMENTS: FERC Order 706 did not direct changes. The enumerated list is too prescriptive for the requirement. Add to guidelines. See more general requirement for R4.2. R4.1 REQUIREMENT PROPOSED REVISED TEXT: “Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents. Devices that cannot log a particular event do not require a TFE to be generated.” R4.1 MEASURES PROPOSED REVISED TEXT “Evidence may include, but is not limited to, a paper or system generated listing of event classes for which the Cyber Asset is configured to generate logs.” R4.2 REQUIREMENT COMMENTS: FERC Order 706 did not require a change; therefore the addition of “real time” is not required. Some assets can log, but cannot alert. R4.2 REQUIREMENT PROPOSED REVISED TEXT: “Generate alerts, where technically feasible, for events that the Responsible Entity determines necessary.” R4.2 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to paper or system generated listing of event classes and conditions that necessitate alerts; assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate an alert; screenshots showing how alerts are configured.” R4.3 APPLICABILITY COMMENTS: Delete “with External Routable Connectivity” from Medium Impact BES Cyber Systems. R4.3 REQUIREMENT COMMENTS: FERC Order did not direct a change. Add clarification to timing, “after identification.” R4.3 REQUIREMENT PROPOSED REVISED TEXT: “Activate a response to event logging or alerting failures before the end of the next calendar day after identification.” R4.3 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to: dated event logging failures and screen-shots showing how alerts were configured, or dated records showing that personnel were dispatched or a work ticket was opened to review and repair logging failures.” R4.4 APPLICABILITY COMMENTS: Delete "at Control Centers" from Medium Impact BES Cyber Systems. If this is not deleted, this requirement would not apply to substations, which would decrease security. R4.4 MEASURES COMMENTS: FERC Order 706 did not direct retaining records of disposition of security-related event logs. Retaining records of disposition of security-related event logs beyond 90 days up to the evidence retention period would be burdensome. R4.5 REQUIREMENT COMMENTS: With our proposal to create a standard for controls that are only applicable to high impact assets/systems, this requirement would be moved to the new high impact standard with the following suggested changes. Delete last portion of requirement to activate a response because it is already included in R4.3. Including it in this requirement too would result in double jeopardy. The term “unanticipated” is not needed. R4.5 REQUIREMENT PROPOSED REVISED TEXT: “Review a summarization or sampling of logged events every two weeks to identify Cyber Security Incidents and potential event logging failures.” R4.5 MEASURES COMMENTS: Delete last portion of measure to show personnel were dispatched or a work ticket was opened because it is already included in R4.3. R4.5 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to, documentation describing the review, findings from the review (if any), signed and dated documentation showing the review occurred.”
No
R5.1 REQUIREMENT COMMENTS: Need to allow for where technically supported and this is more

specifically addressing electronic user access. R5.1 REQUIREMENT PROPOSED REVISED TEXT: “Validate credentials before granting electronic user access to each BES Cyber System where technically supported.” R5.2 REQUIREMENT COMMENTS: Delete because this replicates the CIP-004 access authorization requirements. 5.3 REQUIREMENT COMMENTS: Delete as this would already be included in the CIP-004 access authorization requirements. R5.4 APPLICABILITY COMMENTS: Move list of applicability from Requirements to Applicability. R5.4 APPLICABILITY PROPOSED REVISED TEXT: “High Impact Critical Cyber Assets, Medium Impact Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.” R5.4 REQUIREMENT COMMENTS: It is not necessary to list the applicability in the Requirements section. Provide additional options for controlling default accounts. R5.4 REQUIREMENT PROPOSED REVISED TEXT: “Control default accounts by initially changing default passwords, or removing or disabling the accounts, where technically feasible, unless the default password is unique to the device or instance of the application. For the purposes of this requirement an inventory of Cyber Assets is not required.” R5.5 REQUIREMENT COMMENTS: 5.5.1. FERC did not direct a change in password length. Although eight characters increases security over six characters, 10 characters would increase security more than eight characters and so on. Where does one stop? Retain requirement for six character passwords. Passwords would be applied at the asset level instead of system level. R5.5 REQUIREMENT PROPOSED REVISED TEXT: “For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least six characters or the maximum length supported by the Critical Cyber Asset; 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non- alphanumeric) or the maximum complexity supported by the Critical Cyber Asset; 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the Critical Cyber Asset, the significance of passwords in the set of controls used to prevent unauthorized access to the Critical Cyber Asset and existing service agreements, warranties or licenses.” R5.6 REQUIREMENT COMMENTS: This is a new requirement that is not directed by FERC Order 706 and would generate a lot of TFEs without commensurate improvements to security. It overlaps with the alerting requirement and should be deleted.

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with revisions proposed to the VRFs and requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that “as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…” MidAmerican Energy believes it is possible to have gradated VSLs for many of the CIP-007-5 requirements.

No

GENERAL COMMENTS ON CIP-008-5: Most of the changes made to CIP-008 were not directed by FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for entities with existing programs. We recommend returning to legacy language and structure for CIP-008-5. Suggested text is included below. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. The proposed applicability of “All Responsible Entities” greatly expands the scope CIP-008, which was not directed by FERC. MidAmerican Energy recommends changing the Applicability for all of the CIP-008-5 requirements to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems. The “canned” C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. R1.1 REQUIREMENT PROPOSED REVISED TEXT: “Develop, maintain and implement a Cyber Security Incident Response Plan that includes the following: 1.1.1 Procedures to characterize and classify events as Reportable Cyber Security Incidents. 1.1.2 Response actions 1.1.3 Roles and responsibilities of Cyber Security Incident response teams 1.1.4 Cyber Security Incident handling procedures 1.1.5 Communication plans” R1.1 REFERENCE: CIP-008-4 R1, R1.1, R1.2, R1.3 R1.1 RATIONALE: There were no FERC directives for revisions. Wording in version 4 is clear and does not need to be changed. R1.2 REQUIREMENT PROPOSED REVISED TEXT: “Follow requirements in EOP-004 to report Reportable Cyber Security

Incidents." R1.2 REFERENCE: CIP-008-4 R1.3 R1.2 RATIONALE: FERC Order 706, paragraphs 673-677, addresses reporting of Cyber Security Incidents, including coordination between CIP-008 and other standards. Most of these FERC directives are being handled by the EOP-004/CIP-001 project. While the reporting requirement is being moved to EOP-004, a reference in this standard is needed. R1.3 REQUIREMENT PROPOSED REVISED TEXT: "Review the Cyber Security Incident response plan at least annually." R1.3 REFERENCE: CIP-008-4 R1.5 R1.3 RATIONALE: There were no FERC directives for revisions. Wording in version 4 is clear and does not need to be changed. R1.4 REQUIREMENT PROPOSED REVISED TEXT: "Update the Cyber Security Incident response plan within thirty calendar days of any organizational or technology changes that impact the plan." R1.4 REFERENCE: CIP-008-4 R1.4 R1.4 RATIONALE: There were no FERC directives for revisions. Additional words were inserted from version 4 language to clarify what changes are included in the requirement.

No

GENERAL COMMENTS ON CIP-008-5 R2: As mentioned in CIP-008-5 R1 comments, most of the changes made to CIP-008 were not directed by FERC Order 706 and do not result in improvements to security. MidAmerican Energy recommends returning to legacy language and structure for CIP-008-5. Suggested text is included below. The proposed applicability of "All Responsible Entities" greatly expands the scope CIP-008, which was not directed by FERC. MidAmerican Energy recommends changing the Applicability for all of the CIP-008-5 requirements to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems. R2.1 REQUIREMENT PROPOSED REVISED TEXT: "Test the Cyber Security Incident response plan at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. The test should include verification of the list of entities that must be called pursuant to the plan and that the contact numbers are correct." R2.1 REFERENCE: CIP-008-4 R1.6 R2.1 RATIONALE: FERC Order 706, paragraph 687 states CIP-008 should include verification of the list of entities and contact numbers. R2.2 REQUIREMENT PROPOSED REVISED TEXT: "Review the results of the Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan." R2.2 REFERENCE: New requirement R2.2 RATIONALE: FERC Order 706, paragraph 686 directs changes to the requirement to include revisions to the plan to address lessons learned. R2.3 REQUIREMENT PROPOSED REVISED TEXT: "Update the Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan." R2.3 REFERENCE: New requirement R2.3 RATIONALE: FERC Order 706, paragraph 686 directs changes to the requirement to include revisions to the plan to address lessons learned.

No

R3 REQUIREMENT COMMENTS: Most of the changes made to CIP-008 were not directed by FERC Order 706 and do not result in improvements to security. MidAmerican Energy proposes returning to the version 4 language and structure for CIP-008-5, which incorporates the R3 requirements into R1 and R2. Therefore, R3 would be deleted under our proposal.

No

The proposed VRFs and VSLs should be revised commensurate with revisions proposed to the requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that "as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…" MidAmerican Energy believes it is possible to have gradated VSLs for CIP-008-5. As an example, the VSLs for R1 could include the following. Lower: The Cyber Security Incident response plan was updated more than 30 calendar days but less than 60 calendar days of organizational or technology changes that impacted the plan. Moderate: The Cyber Security Incident response plan was updated more than 60 calendar days but less than 90 calendar days of organizational or technology changes that impacted the plan. High: The Cyber Security Incident response plan was updated more than 90 calendar days but less than 120 calendar days of organizational or technology changes that impacted the plan. Severe: The Cyber Security Incident response plan was updated more 120 calendar days of organizational or technology changes that impacted the plan.

No

PURPOSE STATEMENT COMMENTS: MidAmerican suggests revising the purpose statement to the following: "Standard CIP-009-5 ensures recovery plan(s) are put in place for Critical Cyber Assets." GENERAL COMMENTS ON CIP-009-5: The revised version 5 structure splits backup media

requirements between R1 (recovery plan) and R2 (implementation and testing). We think the FERC directives for CIP-009 can be more effectively addressed within a structure that is closer to version 4. MidAmerican Energy proposes the following requirements: R1 recovery plan (which includes implement); R2 exercise of the recovery plan; R3 backup media; and R4 maintain the recovery plan. Our suggested text and structure are included below. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. The current draft does not include any guidance. We think it is important to include guidance regarding possible ramifications to other NERC standards. For example, event analysis requirements and IRO-001 R3 must be considered if there is a potential delay of restoration to collect forensic data. The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. Column headers above R1.4 and R3.4 are incorrect. The document currently shows "Part" for each column instead of only the first one. R1.1 REQUIREMENT PROPOSED REVISED TEXT: "Create and implement a recovery plan that addresses at a minimum: R1.1.1. Conditions for activation of the recovery plan, and R1.1.2 Roles and responsibilities of responders" R1.1 RATIONALE: There were no FERC directives for this requirement, except for adding implementation. We suggest V4 legacy language, and incorporate implementation as directed. R1.2 REQUIREMENT COMMENT: Delete since this has been incorporated into R1.1. R1.3 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be moved to R3 backup media, under the revised structure mentioned above. R1.4 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be moved to R3 backup media, under the revised structure mentioned above. R1.5 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be moved to R2 exercise of the recovery plan, under the revised structure mentioned above. See comments under R2.

No

R2 REQUIREMENT COMMENTS: This requirement is about exercises and actual incidents. The use of the term "implement" in this requirement is confusing. We suggest implementation be incorporated into R1 to meet the FERC directive, and change this requirement to be more in line with version 4. R2 REQUIREMENT PROPOSED REVISED TEXT: "Each Responsible Entity shall exercise its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Exercise [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]" R2.1 REQUIREMENT PROPOSED REVISED TEXT: "Exercise the recovery plan(s) annually. An exercise can range from a paper drill, to a full operational exercise, to recovery from an actual incident." R2.1 RATIONALE: Maintain the version 3 language. R2.2 REQUIREMENT COMMENT: We suggest moving the requirement for testing backup media to R3. R2.3 REQUIREMENT COMMENT This requirement would become R2.2 under our proposed structure. R2.3 REQUIREMENT PROPOSED REVISED TEXT: "Exercise the recovery plan(s) at least every 39 calendar months through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual response may substitute for an operational exercise." R2.3 (which becomes R2.2) RATIONALE: We removed text on "initially upon the effective date." This should be incorporated in the implementation plan. R2.3 (which becomes R2.2) APPLICABILITY: This requirement should apply to High Impact BES Cyber Systems only. Associated assets should not be included. PROPOSED R2.3 REQUIREMENT COMMENT: MidAmerican Energy proposes R1.5 be moved to R2.3, since it is associated with events that trigger the recovery plan. PROPOSED R2.3 PROPOSED REVISED TEXT: Preserve data, when it does not impede or restrict system restoration, if necessary to determine the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. PROPOSED R2.3 RATIONALE: We removed "technically feasible" because the TFE concept does not work with this requirement due to the 60 day safe harbor in the rules of procedure. We revised the requirement to eliminate any conflicts with other reliability standards and event analysis requirements. The focus should be getting the system back up and operational. See paragraph 708 of FERC Order 706, which states: "should not impede or restrict system restoration." We also incorporated the concept "necessary to determine the cause," which is based on FERC's directive, paragraph 710. In some situations, data preservation may not be needed to determine the cause of an event that triggers the recovery plan. PROPOSED R2.3 APPLICABILITY: This is a burdensome new requirement. Therefore, MidAmerican Energy proposes the applicability be limited to High Impact BES Cyber Systems. PROPOSED R2.3 MEASURES: Measures should be bulleted with "ors" and commas.

No

R3 AND R4 GENERAL COMMENTS: Under our proposed structure, all of the requirements in the draft R3 would be moved to a new requirement, R4. Please see R4 below for comments regarding the draft R3.1 to R3.5. R3 REQUIREMENT COMMENT: MidAmerican Energy proposes R3 be a separate requirement for backup storage. Version 3 had two requirements related to backup storage. These had been incorporated into other requirements in the draft V5. R3 REQUIREMENT PROPOSED TEXT: “Each Responsible Entity shall have one or more documented processes that collectively include each of the applicable items in CIP-009-5 R3 - Recovery Plan Backup Media.” R3.1 REQUIREMENT COMMENT: We have moved R1.3 to be R3.1. R3.1 REQUIREMENT PROPOSED REVISED TEXT: “Back up and store information required to successfully restore BES Cyber System functionality. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.” R3.1 RATIONALE: The revised text is based on V3 language. This removes the word "protection" since this is not a FERC directive. The sentence "For example…" from V3 could be moved to measures. R3.2 REQUIREMENT COMMENT: We have moved R2.2 to be R3.2. R3.2 REQUIREMENT PROPOSED REVISED TEXT: “Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.” R3.2 RATIONALE: We propose the version 4 language, since there were no FERC directives to change it. R3.3 REQUIREMENT COMMENT: We have moved R1.4 to be R3.3. R3.3 REQUIREMENT PROPOSED REVISED TEXT: “Verify after significant changes that the backup process for software, data and information required to successfully restore CCAs completed successfully.” R3.3 RATIONALE: Refer to FERC Order 706, paragraph 740, which refers to "significant changes." R3.3 APPLICABILITY COMMENTS: Limit to High Impact BES Cyber Systems due to the burdensome nature of this new requirement. R4 REQUIREMENT COMMENT: Under our proposed structure, R4 would be Recovery Plan Review, Update and Communication. We propose deleting the draft R3.2, since there were no FERC directives to add this as a requirement. We propose deleting the draft R3.4. This is covered in the suggested text from version 4 for R4.2. R4.1 REQUIREMENT COMMENT: We have moved R3.1 to be R4.1. R4.1 REQUIREMENT PROPOSED REVISED TEXT: “Review the recovery plan annually.” R4.1 RATIONALE: There were no FERC directives to change the requirement. Revert to version 4 language. R4.2 REQUIREMENT COMMENT: We have moved R3.3 to be R4.2 R4.2 REQUIREMENT PROPOSED REVISED TEXT: “Update the recovery plan(s) to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident.” R4.2 RATIONALE: There were no FERC directives to change the requirement. Revert to version 4 language. R4.3 REQUIREMENT COMMENT: We have moved R3.5 to be R4.3. R4.3 REQUIREMENT PROPOSED REVISED TEXT: “Communicate updates to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.” R4.3 RATIONALE: There were no FERC directives to change the requirement. Revert to version 4 language.

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with revisions proposed to the VRFs and requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that “as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…” We think some of the CIP-009-5 requirements could have gradated VSLs for CIP-009-5. As an example, the VSLs for R2 as proposed by MidAmerican Energy could include the following. Lower: The recovery plan was exercised more than 39 calendar months but less than 40 calendar months since the previous exercise. Moderate: The recovery plan was exercised more than 40 calendar months but less than 41 calendar months since the previous exercise. High: The recovery plan was exercised more than 41 calendar months but less than 42 calendar months since the previous exercise. Severe: The recovery plan was exercised more than 42 calendar months since the previous exercise.

No

GENERAL COMMENTS ON CIP-0010-5: CIP-010-5 R1 and R2 greatly expand the scope of change control and configuration management beyond what was directed in FERC Order 706. MidAmerican does not support this scope expansion. MidAmerican Energy does not support organizing these requirements into a separate standard. This was not directed by FERC, does not improve security and increases implementation costs for entities with fully implemented CIP programs. These requirements

could remain within their version 4 standard and preserve the numbering of the requirements within those standards. One exception is that we support removing the vulnerability assessment requirement from CIP-005-4 and combining it with CIP-007-4's vulnerability assessment requirement. The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. R1 RATIONALE COMMENTS: The rationale does not address paragraph 399 of FERC Order 706 – having processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. R1.1 REQUIREMENT COMMENT: The draft requirement is too prescriptive. CIP-003-4 R6 is closer to a results based requirement and provides more flexibility to achieve the desired results. CIP-010-1 R1.1 greatly expands the scope of change control and configuration management (CIP-003-4 R6) beyond what was directed in FERC Order 706. FERC Order 706 paragraphs 397 and 398 directed "modifications to CIP-003-1 R6 to provide an express acknowledgement of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." The concern was that some form of verification is performed to detect when authorized changes have been made. CIP-010-1 R2.1 addresses Order 706's concern for some form of verification to detect unauthorized changes. FERC also did "not believe the changes will have burdensome consequences." CIP-010-1 R1.1 requires extensive and burdensome details tracking. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1. R1.1 REQUIREMENT PROPOSED REVISED TEXT: "Establish and document a process of change control and configuration management for adding, modifying, replacing or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process." If industry consensus can be achieved, MidAmerican will support requiring authorization of changes, but without the additional bureaucracy as drafted of authorization by the senior manager or delegate. Entities should be able to use their existing corporate change control authorization processes without having to create a CIP-only variation on their standard processes. R1.1 MEASURES COMMENTS: Change the measure to match the revised requirement, such as documentation of the change control process. R1.2 REQUIREMENT COMMENT: FERC Order 706 did not direct authorization by the senior manager or delegate. It directed "express acknowledgement of the need for the change control," which we believe is achieved with the proposed text below. R1.2 REQUIREMENT PROPOSED REVISED TEXT: "Authorize changes to hardware and software components of Critical Cyber Assets." R1.3 REQUIREMENT COMMENT: This requirement should be deleted with our proposal to remove the burdensome requirement for baseline configurations in R1.1. R1.4 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be replaced with CIP-007-4 R1. R1.4 REQUIREMENT PROPOSED REVISED TEXT: Ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of this standard, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware. R1.4.1 Implement and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation. R1.4.2 Document that testing is performed in a manner that reflects the production environment. R1.4.3 Document test results. R1.5 REQUIREMENT COMMENT: With our proposal to create a standard for controls that are only applicable to high impact assets/systems, this requirement would be moved to the new high impact standard with the following suggested changes. Delete "results of the testing" from R1.5.2 because it overlaps with R1.4 for highs. Delete and put in guidance: "including a description of the measures used to account for any differences in operation between the test and production environments." R1.5.2 REQUIREMENT PROPOSED REVISED TEXT: "Document the differences between the test environment and the production environment."

No

R2.1 REQUIREMENT COMMENT: MidAmerican Energy is concerned that this requirement creates the possibility of "double jeopardy" for violations with multiple other requirements. As currently written, if an auditor finds a violation for CIP-010-5 R1, the same situation likely would result in a violation of CIP-010-5 R2. The current draft also overlaps with the alerting that is required in CIP-007-5 R4.2 and the investigation that is required by CIP-008. We have provided proposed revised text that addresses the possibility of double jeopardy. We also deleted the words "and document" since documentation is

not providing any improvements to reliability, but increases implementation costs for entities. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1. R2.1 REQUIREMENT PROPOSED REVISED TEXT: "Where technically feasible, detect unauthorized changes to the configuration that have not been alerted under other CIP standards."
No
CIP-010-5 R3 GENERAL COMMENTS: MidAmerican Energy proposes the draft R3 be replaced with combined legacy language from CIP-005-4 R4 and CIP-007 -4 R8, with the following FERC directed additions: • The addition of an entity imposed timeline for completing the already required action plan. • Active vulnerability assessments every three years. MidAmerican generally supports the inclusion of details in guidelines. However, in this case, the current draft of CIP-010-5 R3 has removed too many details from the standard, thus making it a vague standard that introduces the possibility of significant scope expansion that was not directed by FERC. MidAmerican agrees the FERC directed requirement for active vulnerability assessments should be limited to High Impact Critical Cyber Assets. With our proposal to create a standard for controls that are only applicable to high impact assets/systems, R3.2 would be moved to the new high impact standard. MidAmerican would suggest deleting R3.3 since this is covered by the implementation plan.
No
This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with revisions proposed to the VRFs and requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that "as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…" We think some of the CIP-0010-5 requirements could have gradated VSLs.
No
CIP-011 GENERAL COMMENTS: MidAmerican Energy does not support organizing these requirements into a separate standard. This was not directed by FERC, does not improve security and increases implementation costs for entities with fully implemented CIP programs. These requirements could remain within their version 4 standard and preserve the numbering of the requirements within those standards. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. R1 GENERAL COMMENTS: The only FERC directive for information protection was prompt revocation of access to protected information (paragraph 386), which is addressed in CIP-004. There was no FERC directive to move the information protection requirement to a separate standard or to make other changes that increase implementation costs for entities with implemented programs, without any improvements to security. MidAmerican proposes going back to version 4 language and structure for information protection, with two parts instead of three. Proposed text is listed below. R1 REQUIREMENT PROPOSED REVISED TEXT: "Each Responsible Entity shall have one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]" R1.1 APPLICABILITY COMMENTS: Remove Associated Protected Cyber Assets. This was not directed by FERC and is an expansion of scope that does not improve security. R1.1 REQUIREMENT COMMENT: MidAmerican Energy proposes going back to text that is more in line with version 4 language. The SDT is proposing to remove the explicit requirement for classification. The SDT states this does not prevent having multiple levels of classification. However, the legacy language does not require multiple levels of classification. R1.1 REQUIREMENT PROPOSED REVISED TEXT: "Implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets. R1.1.1 The information to be protected shall include the following: Critical Cyber Information operational procedures; lists as required in Standard CIP-002-5; Critical Cyber Information network topology or similar diagrams; floor plans of computing centers that contain Critical Cyber Assets; equipment layouts of Critical Cyber Assets; disaster recovery and incident response plans for Critical Cyber Assets; and Critical Cyber Asset security configuration information. R1.1.2 Information shall be classified based on the sensitivity of the Critical Cyber Asset information." R1.1 MEASURES

PROPOSED REVISED TEXT: “Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * evidence that physical media is stored in secured locations to prevent unauthorized access, or * evidence that technical measures are in place to prevent unauthorized access to electronic information, or *records of training on information handling procedures” R1.2 APPLICABILITY COMMENTS: Remove Associated Protected Cyber Assets. This was not directed by FERC and is an expansion of scope that does not improve security. R1.2 REQUIREMENT COMMENT: MidAmerican Energy proposes going back to text that is more in line with version 4 language for assessment of the program. R1.2 REQUIREMENT PROPOSED REVISED TEXT: “At least annually assess adherence to the Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.”

No

R2.1 REQUIREMENT COMMENTS: We suggest some minor wording changes to begin the requirement with a verb and clarify that information is being retrieved from the asset. R2.1 REQUIREMENT PROPOSED REVISED TEXT: “Prevent the unauthorized retrieval of Critical Cyber System Information from Critical Cyber Asset media prior to the release of Critical Cyber Asset media for reuse.” R2.2 REQUIREMENT COMMENTS: We suggest some minor wording changes to begin the requirement with a verb and clarify that information is being retrieved from the asset. We suggest incorporating footnote #2 into the requirement or a definition, since a footnote can easily get overlooked. R2.2 REQUIREMENT PROPOSED REVISED TEXT: “Destroy the Critical Cyber Asset media prior to disposal or prevent the unauthorized retrieval of Critical Cyber System Information from Critical Cyber Asset media prior to disposal.”

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with revisions proposed to the VRFs and requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that “as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…” We think some of the CIP-0011-5 requirements could have gradated VSLs.

No

MidAmerican Energy does not believe it is possible to complete the implementation plan in 18 months given the scope and depth of changes contained in the current draft version 5. MidAmerican Energy, like many other entities, has found it complicated and confusing to apply the changes proposed in CIP-002-5. It is not possible to commit to an implementation plan when not sure of the entire scope of proposed changes. The number of changes required for CIP-003 through CIP-011 also makes it difficult to achieve the proposed implementation timeline. About 80 percent of the changes are not directed by FERC Order 706. Several of these changes are administratively burdensome with limited, if any, security improvement. The proposed changes for existing definition terms, such as Physical Security Perimeter and Critical Cyber Assets, also extends the time it takes to implement the number of changes needed in procedure documents, training materials, facility diagrams, etc. MidAmerican Energy suggests an alternative approach to create the opportunity to achieve a quicker implementation, particularly for high and medium impact Critical Cyber Assets. The approach builds on the work completed by the drafting team and on the CIP-002-4 standard already approved by the industry. MidAmerican Energy recommends retaining CIP-002-4 as approved by the industry in 2010. This version is filed with FERC. Industry and NERC comments on the FERC NOPR recommend FERC approval. This will eliminate the confusing and complicated process to identify BES Cyber Systems proposed in version 5. Retaining CIP-002-4 will meet FERC Order 706 directives regarding CIP-002. FERC 706 directives for CIP-002 are met by using industry approved guidance documents for identifying Critical Assets and Critical Cyber Assets, see paragraphs 253-258 and 270-273. CIP-002-4 aligns with FERC’s affirmation that the applicable responsible entities are responsible for identifying Critical Assets, see paragraphs 319-321. Also, CIP-002-2 added senior manager approval of risk-based methodology, see paragraphs 294-297. Excerpts from paragraphs 284 and 285 indicate FERC is not looking for changes to CIP-002. Paragraph 284 states, “…there is no formally accepted method for identifying critical cyber assets before us at this time … we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time.” Paragraph 285 says, “CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial up access … We do not find

sufficient justification to remove this provision at this time." Building on the categorization concept, we recommend development of two new standards, one for those requirements applicable only to high impact assets and one for those requirements applicable only to low impact assets. The new standards would use CIP-002-4 to categorize Critical Assets and Critical Cyber Assets into the high and low impact levels. The new "high only" standard would group the eight extra protections for only high impact assets (not medium or low) identified in the current draft of version 5. This separate standard on requirements applicable only to high impact assets provides an opportunity for a separate implementation timeline for the additional controls that apply only to high impact assets. This new standard provides flexibility in adjusting controls on high impact assets. In the future, only one standard has to be modified for these extra requirements on high impact assets. Also, entities that do not have high impact assets will not have to sort through this new standard and reliability standard audit worksheet to assure compliance and security. CIP version 5 introduces several new controls for low impact assets not directed by FERC Order 706 or included in the standard authorization request. The resulting scope expansion is not supported by many in the industry and will likely slow down the process to approve the new CIP 5 standards. A new "low only" standard would group those requirements applicable only to low impact assets (not high or medium.) This new separate standard can be commented and voted on in parallel with the efforts listed above without impacting the schedule to meet FERC Order 706. The new standard provides full transparency in the stakeholder process. It allows separate discussion on the cost and compliance concerns with low impact assets. Also the standard allows for a separate implementation schedule for low impact assets so changes for high and medium impact assets can be completed first. The vast majority of the drafted requirements in CIP-003 through CIP-011 remain in place. However, they should be adjusted to meet the changes described in the requirements comments to: 1 - include any changes necessary to address all of the applicable FERC directives and 2 - include security improvements not directed by FERC that are known to have significant industry support. Retain version 4 language for requirements that do not meet one of these two criteria (not a directive or not an industry established security improvement). Additional implementation notes: When the time comes, MidAmerican would propose an implementation date different than Jan. 1 due to resource issues at year-end. There are 36 references to "initially upon the effective date of the standard and at least once each calendar year" (or similar language) throughout the draft standards. All of these references should be eliminated from within the standard and incorporated into the implementation plan. This ensures the effective dates of the requirements are clearly spelled out for the initial implementation of the standard, as well as for newly identified assets. The industry (not this drafting team) should consider a standard authorization request to create a NERC Glossary term for the definition of annual and retire CAN-010. There could be another opportunity to positively impact the timeframe. Any improvements to TFEs prior to implementing version 4 and version 5 would lessen the impact of these transitions. NERC's first annual TFE report to FERC was filed in September 2011. It identified 3,998 approved TFEs of which 2,814 or 71 percent were approved on the basis of "not technically possible." Industry (not an expectation for this drafting team) working with NERC and FERC should determine if a NERC Rules of Procedures revision for TFEs can be supported. Could a rules of procedure change be achieved in time to alleviate some implementation burden for both registered entities and regional entities for version 4? For example, could some administrative overhead be reduced for the 71 percent that are not technically possible?

Individual

Dan Roethemeyer

Dynegy

No

Yes

On an 11/15/2100 NERC webinar regarding V5, a presenter indicated Large Control Centers were those owned by an RC, BA, or TOP but not by a GO or GOP. Slides 18 and 29 seem to support this. However, Attachment 1, Section 1.4 seemingly contradicts the webinar information by indicating a GOP's Control Center can be a High Rating. Suggest deleting Section 1.4 and let GOP Control Centers get picked up in Section 2.13. Also, please clarify in Attachment 1, Section 1.4 (if not deleted) and 2.13 that a generating station's Control Room is not considered a Control Center in accordance with Version 5.

No
Recommend consistency with R2 and do it annually not-to-exceed 15 months.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

No
Recommend selecting either V4 or V5 as the next step. This issue is complicated enough without having to implement two different versions over time as well as show compliance and get audited (or do the auditing).
Individual
J. S, Stonecipher, PE
City of Jacksonville Beach dba/Beaches Energy Services
No
BES Cyber System – Maintenance Cyber Asset is not defined, suggest changing to Transient Cyber Asset. BES Cyber System Information – (1) Security procedures should not be on the list because it creates a conflict between CIP-011-1 that restricts access to the information and CIP-003-5 and CIP-004-5 that require general training and dissemination of those procedures. (2) BES Cyber System Impact is not defined. BES Reliability Operating Services – under Dynamic Response to BES Conditions, suggest adding Excitation Response. Under Balancing Load and Generation – suggest removing unit commitment since it will not meet the 15 minute window and it is an operations planning function and not a real-time operating service. CIP Exceptional Circumstance should include imminent danger to a BES Facility as a condition. CIP Senior Manager – the definition should exclude CIP-001, at least until it is retired with Project 2009-01 Control Center – (1) We assume that a Control Center is only a Control Center as used by a BA, TOP, GOP or RC. The definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” For clarity, we suggest adding this clarity to the definition. (2) The use of the word “facilities” in a fashion that does not mean “Facilities” will lead to confusion and ambiguity, especially since “facilities” is used later in the same sentence as meaning “Facilities”. I suggest: “One or more sites hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation Facilities or transmission Facilities, at two or more locations”. Facilities should also be capitalized in the first bullet. Defined Physical Border is ambiguous. Specifically, are all spacial dimensions, horizontal and vertical, to be established as part of the boundary? In other words, it seems like the “roof” may no longer be required, e.g., 5 walls instead of 6 walls, but, vertical dimension requirements of walls / fences are ambiguous.
No
I believe that a fourth category of risk impact be developed, a “De Minimus Impact” category that would consist of otherwise Low Impact BES Cyber Assets but that do not have routable protocol or dial-up access. I understand that there is concern about Low Impact BES Cyber Assets due to the risk of a coordinated attack. A coordinated attack is much more likely to BES Cyber Assets that have routable protocol or dial-up access than to those BES Cyber Assets with no connectivity. It is much more difficult and impractical to attempt a coordinated attack on BES Cyber Assets without connectivity. Recognizing this difference in both difficulty level and Low Impact (in other words, it wouldn’t be worth the effort because other attack vectors with similar levels of difficulty would have more impact), we propose adding a fourth impact category, De Minimus Impact. I would propose that these De Minimus Risk BES Cyber Assets would not need to comply with the CIP standards because the costs would be unjustified. Bullet 1.2, a Control Center for any BA, even very small ones, being High risk is inappropriate. For instance, the entire load or supply of a small BA would fit into the “noise” of a large BA for supply and demand mismatch. Suggest changing 1.2 to parallel 1.3, e.g., a BA Control Center that includes control of one or more of the assets identified in criteria 2.1, 2.3, 2.4 and 2.12. Bullet 2.13 could then be used to accommodate smaller BAs Bullet 1.3, Transmission

Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” Bullet 2.5, “Facilities” should be changed to “Elements”. The cranking path is not necessarily part of the BES. Bullet 2.6, is an autotransformer of 500 kV to 230 kV included? Bullet 2.7 is inconsistent in its terminology, switching between “Facility” and “Lines”. It seems that “Line” is intended. The focus also seems to be “at a single station or substation” where the focus ought to be a single BES Cyber Asset / System that controls multiple Lines. I suggest changing the first sentence of 2.7 to read: “Multiple Transmission Lines operating at 200 kV or higher, but less than 500 kV, where the total weighted value of all BES Transmission Lines whose Reliability Operating Services would be adversely impacted within 15 minutes if a single BES Cyber Asset / System is rendered unavailable, degraded or misused exceeds a value of 3,000.” Bullets 2.8 and 2.9, the phrase “at a single station or substation location” does not seem to add any value and can be a source of ambiguity. I suggest striking the phrase. Bullet 2.12, the 300 MW bright-line seems arbitrary (albeit carried over from prior versions). In general, the system is more tolerant to loss of load than loss of generation and the 300 MW seems out of proportion with 2.1 of 1500 MW. The reasoning applied in the Application Guideline is flawed. UVLS and UFLS are only last ditch efforts if other events have already caused the system to be on the edge. So, how is that different from 2.1 if the system is already on the edge? The focus should be on how a malicious user can cause an Adverse Reliability Impact; hence, I suggest 1500 MW instead of 300 MW. Bullet 2.13, (1) Transmission Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” (2) The term “control centers” should be capitalized in the phrase “generation control centers” to make it clear that it refers to the defined term “Control Center” In the application guidelines, when discussing the BES Reliability Operating Services, the bullets have associated with them the functional entity that typically provides those services. However, there are exceptions and the guidelines ought to reflect those exceptions; for instance, a TO may also provide UFLS. Also in the application guidelines, the word “facilities” is used in a fashion that does not mean “Facilities”, which creates ambiguity and confusion (e.g., Facilities by definition is part of the BES, whereas assets owned and operated by DPs and LSEs are typically not BES). Suggest using “elements”. The Application guideline discussion of bullet 2.13 of Attachment 1 is not consistent with the actual bullet.

Yes

I agree with the requirement but question whether the standards actually meet the stated goal of the requirement to “not require discrete identification” of Low Impact BES Cyber Assets / Systems. There are numerous examples which seem to contradict this stated goal as described later in these comments and specifically to this requirement. How does one distinguish between a BES Cyber System and a non-BES Cyber System? Does this mean that we need to inventory all of our cyber assets and develop a test to distinguish between “Low” and “non-BES”, even though R1 says that “Low” does not “require discrete identification”? How are entities to prove to auditors that the identification and categorization was done without having an inventory, i.e., discrete identification? The VSLs seem to seem to imply that “Low Impact” needs to be discretely identified, e.g., what happens if an entity categorizes a Medium Impact as a Low Impact? In order to review correct categorization, doesn’t the auditor need to review Low Impact to see if they should have been categorized Medium or High Impact?

Yes

Yes

The Evidence Retention section of the standard should not refer to Rules of Procedure language that is subject to change. The sentence that states: “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit” should instead reference the Rules of Procedure, Attachment 4C on the CMEP, Paragraph 3.1.4.2, e.g., “also refer to the Rules of Procedure, Attachment 4C … Paragraph 3.1.4.2”. In this way, it is possible to accommodate changes to the ROP language without needing the change to the standard.

Yes
No
“Implemented” is not the right word because it creates double jeopardy with the rest of the CIP standards, e.g., a violation of another standard could mean that the policy was not implemented. Suggest changing to use the phrase “in force”, meaning that the policy is in force and able to be enforced, but not requiring enforcement of the policies in this requirement (implement includes enforcement), but rather enforcement is contained in ensuing standards. I suggest rephrasing to: “Each Responsible Entity shall have in force one or more documented cyber security policies …” The standards are inconsistent in its use of BES Cyber Assets /Systems, e.g., R2, to be consistent with CIP-002-5, should use the phrase “BES Cyber Assets and BES Cyber Systems”. Alternatively, CIP-002-5 could just use BES Cyber Systems. The bullets are incorrectly numbered; they should be 2.1 through 2.10 and not 1.1 through 1.10
Yes
The grammar of the sentence is a bit off and it is not clear whether the CIP Senior Manager needs to approve each of the policies or not. Suggest moving the phrase “each of its cyber security policies” to after the word “Manager”, e.g., “Each Responsible Entity shall review and obtain the approval from its CIP Senior Manager for each of its cyber security policies …”
Yes
Yes
“Cyber Security Policy” should be “cyber security policies” to be consistent with R2 and R3.
Yes
There is an extra “2” at the end of the sentence within the standard.
Yes
See the discussion of Evidence Retention in response to Question 3 VSL to R5, should there be a time frame applied, e.g., failed to document … two delegations within the audit period, within a year? If three failures are spread over 30 years, e.g., one failure each 10 years, is that a severe violation?
Yes
“Implement” is ambiguous. If a process in “in force” but in one instance is not followed, is that a violation? The process has been implemented. Merriam-Webster’s has two definitions of “implement”, one of which is probably intended: 1: carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures 2: to provide instruments or means of expression for A process can meet both of these definitions. If enforced, a process can meet the first definition; if not enforced, the process can meet the second definition. I assume the SDT intends the first definition. I suggest adding a footnote to specifically identify which definition of “implement” is intended.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 2.1, the measure and the requirement do not match. The requirement is to “define the roles”, the measure includes “and the training needed for each role”. Suggest adding this phrase from the Measure to the Requirement.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The phrasing of requirements that refer to tables is ambiguous with ambiguous reference of prepositional phrases. For instance, in this requirement, it is unclear if an entity that only has Low Impact BES Cyber Systems needs to develop training or not, i.e., does the prepositional phrase “that includes …” refer to “training program” or to “Responsible Entity” or to both? I suggest rephrasing: “Each Responsible Entity that owns applicable systems described in the Applicability column of Table ___ shall ___ in accordance with the applicable terms of Table ___” Such rephrasing should be done to all requirements that refer to a table associated with that requirement. In addition, measures should not include the word “must”. Measures are not enforceable but are instead examples of evidence.

No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 4.2, the phrase “up to the current time” is problematic since it infers that 7 year criminal background checks need to be updated on at least a daily basis to cover “up to the current time”, This should be reworded to seven years prior to the last background check.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The flow of the bullets seems backwards and missing a job function analysis step. In addition, the word “minimum” implies an optimization that is impractical to achieve, e.g., do we want every individual account to be optimized to that individual, which is very difficult to administer and prone to error, or rather do we want to establish account groups based on job functional analysis with associated, appropriate levels of permission and assign individuals to these groups. The latter is easier to administer and less prone to errors, and follows established practices such as security clearance levels. I suggest the following “flow”: 1. Job function analysis 2. “Account group” establishment with appropriate levels of permissions based on job function analysis with associated permissions 3. Assignment of individuals to the appropriate “account group” based on their position
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 7.1 is impossible for resignations. How is it possible for an entity to revoke access at the same time they receive a resignation? Footnote 2 does not help because it only applies to termination. For termination, the entity should know about the termination before the employee; however, for a resignation the reverse is true. I propose we create a new bullet specific to resignation and require revocation of access by the end of the next calendar day. Bullet 7.2, the urgency is out of alignment with the risk. Next calendar day means that if a re-assignment occurs on a Friday, that weekend work is required when that level of urgency is not justified by the situation / risk. I suggest end of the next calendar week.
No
See the discussion of Evidence Retention in response to Question 3 The Severe VSL for R3 includes the phrase “The Responsible Entity did not fully implement its cyber security training program” which makes it a binary VSL and eliminates the High VSL described. For counts, e.g., R6, R7, should there be a time frame identified? E.g., 2 individuals within a year, within the audit period?
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The requirement does not describe the overall purpose of the processes required. Are these processes to deny unauthorized access? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define technical and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the procedural and technical controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. Bullet 1.2 is ambiguous and implies another requirement. First, one does not “use” EAPs to control and secure, rather, EAPs are controlled and secured through use of some other means. Second, the requirement is to secure only identified EAPs,, e.g., is it a non-compliance if an entity misses an EAP, e.g., did not identify it? Third, the Measures are all to support the identification of EAPs and not to “secure and control” EAPs as required by the Requirement. And fourth, the ensuing bullets (1.3, 1.4) seem to be requirements to secure and control EAPs; and hence, bullet 1.2 seems to create double jeopardy. I suggest rewording bullet

1.2 to require identification of EAPs and not “secure and control”.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See the discussion of Evidence Retention in response to Question 3 The VSLs are binary, so, it seems that if one EAP is missed, it is a severe violation. Is this appropriate? I encourage the SDT to develop non-binary VSLs.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 1.1 is ambiguous. How can physical access be restricted without a Defined Physical Boundary? Does this imply that Low Impact assets need to be enclosed in both horizontal and vertical dimensions? Does a fence of xx height suffice? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define operational and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. The application guidelines act to embed a de facto standard requirement of 96 square inches that, if desired to actually be a requirements, must be specified in the actual Requirements of the standard and not in an application guideline that is not enforceable. Alternatively, a definition of a Physical Access Point could be developed with established thresholds that may vary between High, Medium and Low Impact and then the defined term used in the standard. FMPA is aware of challenges made by auditors to entity compliance surrounding issues like how thick does dry-wall need to be to constitute a wall. To avoid disputes between auditors and entities over what constitutes a Defined Physical Boundary, and what constitutes access points, FMPA encourages the SDT to develop bright-line criteria. Such criteria could be different for different risk impacts, e.g., for illustration purposes only: • High Impact might require 6 wall enclosure with every access of 96 square inches or larger opening defined as an access point with wall material of metal, concrete, or drywall of xx inches • Medium Impact may not require a roof, but, requires a fence or wall height of xx inches topped with a climbing deterrent such as barbed wire. • Low Impact video surveillance is sufficient. The standard is very ambiguous as to what is a sufficient physical boundary and will be open to debate between compliance and entities if such bright line criteria are not developed.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The note to bullet 2.2 that says “there is no need to document the escort or handoff between escorts” is inconsistent with the requirement of bullet 1.1 which states that visitors need “continuous” escort. How would one prove that escort was continuous without documenting the hand-offs? On bullet 2.2, what does the phrase “on a per 24 hour basis” mean? Does this mean that a visitor must be logged in and out on the same day and that if a visitor is there at midnight, then the visitor must be logged out at midnight on the prior day and logged back in the following day, or does this mean that military time is to be used when annotating the log?
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 3.1 is not limited to Medium and High Impact with the term “Locally mounted hardware or devices associated with Defined Physical Boundaries since Defined Physical Boundaries is not limited to only Medium and High Impact assets through its definition. This implies that all physical access controls, even those to Low Impact, are to be tested. Presumably, this includes padlocks used to control gates to fences, non-electronic door locks that control access to substation control houses that contain Low Impact digital relays, etc. Such an interpretation would

then require an inventory of those access controls, and presumably, to ensure a complete set, an inventory of Low Impact assets and their Defined Physical Boundaries. I suggest adding to the end of the phrase “Defined Physical Boundaries associated with Medium or High Impact …”
Yes
See the discussion of Evidence Retention in response to Question 3 R1 has both a Long Term Planning and a Same Day Operations time frame listed because the separate bullets are different time frames. If a non-compliance occurs, wouldn’t Same Day Operations always trump Long Term Planning? If that is not the desired outcome, consider separating the bullets into separate requirements or apply the time frame on a bullet by bullet basis.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. On bullet 2.2. - (1) Suggest adding the phrase “addressed by the security related patches or updates” after the word “vulnerabilities” as clarification. (2) “Remediation” implies compensatory measures; the standard should not require compensatory measures because such measures may reduce reliability. Consider another term such as “palliative plan”, “alleviation plan”, or “assuagement plan”. On bullet 2.3, “A process for” is redundant with the parent Requirement and should be deleted and just start the sentence with “Remediate as identified in the plans of 2.2 …”
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 4.2 allows the entity to establish its own threshold criteria for what unauthorized electronic access or malware activity results in a real-time alert, is that a desired state? Bullet 4.3 implies redundancy, e.g., how will we know that event logging failed unless a redundant system tells us? Bullet 4.4 is a data retention requirement and does not belong as a requirement, but rather in the Evidence Retention section of the standard.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 5.4, if “implement” as used in R5 means to “carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures”, then, this bullet 5.4 would require a complete inventory of all Low Impact BES Cyber Assets to ensure that default passwords were changed …. To solve this, implement could be removed from the parent requirement and replaced with “have”, e.g., “have processes”, and then the bullets that require asset by asset / system by system implementation could re-insert the word implement. As such, what would likely need to happen is two bullets would need to be created for default passwords, one for High and Medium which would use the phrase “implement procedural controls” and another for Low Impact which would use the phrase “have procedural controls” to distinguish between a system by system approach for Medium and High and a programmatic approach for Low. Bullet 5.5.3 allows the entity to specify the amount of time between password changes, is this appropriate or should a bright-line be developed? For instance, High – 3 months, Medium – 6 months, Low – 12 months Bullet 5.6 allows the entity to specify the number of unsuccessful login attempts before an alert is issued, is this appropriate or should a bright-line be developed?
No
See the discussion of Evidence Retention in response to Question 3.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures

described in Question 15. This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect and respond to cyber security incidents. Otherwise, how is one to "identify, classify and respond to BES Cyber Security Incidents" on Low Impact systems? This "hidden" requirement is inappropriate. I recommend making R1 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, even for Low Impact systems.
No
See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15. See discussion of the ambiguity of the word "implement" discussed in response to Question 13. This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect and respond to cyber security incidents. Otherwise, how is one to know "when a BES Cyber Se4curity Incident occurs". This "hidden" requirement is inappropriate. I recommend making R2 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, and hence this is duplicative for Low Impact systems. Bullet 2.2, "implement" is not the correct term and is duplicative with the parent requirement. How would one "implement" the entire response for a table top drill since no IT systems would be involved? "Exercise" or equivalent term is more appropriate, e.g., "R2 … implement a process for … 2.2 an Exercise …" Bullet 2.3 is an Evidence Retention requirement and should not be a requirement.
No
First, the question does not match the posted Requirement. The Requirement actually states: "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication". See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15. See discussion of the ambiguity of the word "implement" discussed in response to Question 13. See comments to Questions 34 and 35. I believe that in order to make this requirement applicable to Low Impact systems, which implies that CIP-007 become applicable to Low Impact systems and this "hidden" requirement is inappropriate. Instead, standard CIP-008-5 should not be applicable to Low Impact systems, especially in consideration of the requirements of EOP-004-1 which require entities to analyze and report cyber security incidents.
Yes
See the discussion of Evidence Retention in response to Question 3.
No
See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15. Bullet 1.4, what does the word "verified" mean, than the data is "retrievable", or that all the data is verified? The intent seems to be that the data is retrievable, otherwise 2.2 seems duplicative.
No
See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15. See discussion of the ambiguity of the word "implement" discussed in response to Question 13. Bullet 2.1, "implement" is not the correct term and is duplicative with the parent requirement. How would one "implement" the entire recovery for a table top drill since no IT systems would be involved? "Exercise" or equivalent term is more appropriate, e.g., "R2 … implement a process for … 2.1 an Exercise …" Bullet 2.2 "current configuration" is not accurate. The back-up will not reflect the "current configuration" but the configuration at the time of the back-up.
Yes
See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15.
Yes
See the discussion of Evidence Retention in response to Question 3.
Yes
See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15. See discussion of the ambiguity of the word "implement" discussed in

response to Question 13. The CIP Senior Manager (or delegate) should approve the baseline (1.1). Presumably, the baseline would be “reset” periodically to reduce the number of changes that need to be tracked, and the CIP Senior Manager (or delegate) should approve the new baseline (1.3). Bullet 1.3, the phrase “as necessary” does not seem to add anything and creates ambiguity. Suggest deleting the phrase.
No
Having to monitor all the assets associated under the Applicability section of Table R2 is a huge TFE generator based on the requirement. If the intent is to make sure that there have been no modifications to the device, it would seem appropriate that one could monitor other items and not just the configurations in order to meet the requirements of FERC Order 706, paragraph 397. I suggest that there are methods, such as documented monitoring of logins, wherein if a device has not been logged into, the configurations need not be constantly monitored. Having a yearly requirement to verify configurations (via MD5 hash matching, for example) is an acceptable requirement, but having to constantly monitor the devices for any configuration change is going to be impossible for many devices, and create an unnecessary burden on entities. See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 3.2, what is an “active” vulnerability assessment? The term is ambiguous.
Yes
See the discussion of Evidence Retention in response to Question 3.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. There should be recognition of law, e,.g., unauthorized people are only granted access in cases where the law requires divulging that information, such as public records acts, or a discovery process order by a judge. It would seem that access to BES Cyber Security Information should be approved by the CIP Senior Manager as a separate bullet under R1.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
Yes
See the discussion of Evidence Retention in response to Question 3.
No
(No comment at this time.)
Group
Pacific Northwest Small Public Power Utility Comment Group
Steve Alexanderson P.E.
Yes
We continue to see problems with the definitions. We note that the definition of Control Center now applies to “facilities” with a lower case f and with five widely differing definitions in the online dictionary we consulted. Consider a System Operator’s smart phone. It is programmable, so it is a Cyber Asset per the definition. If set up to receive automatically generated emails or texts regarding BES status or alarms from two BES locations, it “facilitates” the System Operator in doing his job, meeting one of the five definitions of “facility”. If misused, the operator might act on the false information within the fifteen minute window causing a negative impact to the BES (using the list of BES Reliability Operating Services). Therefore it is a both a BES Cyber Asset and a Control Center per the proposed definitions. This phone will carry either a Medium or High Impact rating from CIP-002 making it subject to most of the CIP standard requirements. We continue to believe the SDT did not mean to capture tools such as a smart phone in the definitions, since they do not very easily fit into

the CIP requirements. But they do get caught as we have demonstrated, so the unintended consequence is these tools will be abandoned resulting in possible negative effects to the reliability of the BES. As a start, we suggest that “Control Center” should be limited to rooms or buildings dedicated to controlling BES assets. We also note that the definition of Control Center depends on the NERC term System Operator, the definition of which uses the phrase “control center”; creating a circular definition. The definition of Cyber Asset hinges on whether or not the electronic device in question is “programmable.” Again consulting our online dictionary we see that programmable means capable of receiving working instructions for automatic operation. Therefore a simple static electronic UF relay set only by way of dials and switches and with no communication of any kind will be considered a Cyber Asset and also a BES Cyber Asset because of the function it performs. A Q&A during the webinar confirmed this assessment. Even if low impact, numerous CIP requirements now apply to the device and the entity that owns it. The entity owning this device will need to: 1. document and implement cyber security policies including the 10 sub-requirement subjects, 2. annually review the cyber security policies, 3. ensure employee awareness of the cyber security policies, 4. implement a Security Awareness Program conveying security awareness concepts with quarterly reinforcement of the concepts for the relay in question, 5. define operational or procedural controls to restrict physical access to the relay in question, 6. go through the TFE process for CIP-007 R5 since the relay in question has no password capability, 7. create a Cyber Security Response Plan for the relay in question, 8. implement and perform drills of the Cyber Security Response Plan for the relay in question, 9. and annually review the Cyber Security Plan for the relay in question. All of the above is in addition to the five CIP-002 and CIP-003 requirements that would apply whether the relay was electronic or electro-mechanical. The nine additional requirements represent a huge burden on UFLS owning DP/LSEs with no corresponding improvement in reliability. We suggest that Cyber Asset be limited to electronic devices that are programmable via a communication medium such as RS232, USB, Ethernet, Bluetooth, removable media, etc. BES Cyber System uses Maintenance Cyber Asset in its definition, although this term remains undefined. We believe the SDT intended to use the defined term Transient Cyber Asset here.
No
Yes
Thank you for taking our recommendation to exclude temporary changes.
Yes
We agree with the changes.
No
We note that most of the subject topics align with other CIP standard titles. In particular, sub-requirements 1.7, 1.8, and 1.9 align with CIP-009, 010, and 011. These three standards have no requirements for Low Impact BES Cyber Assets. Likewise CIP-003 R1.7 through R1.9 should not apply to entities that have no Medium or High Impact BES Cyber Assets. All of the sub-requirements should be renumbered to 2.1, 2.2... etc. This would match the mapping document and the Guideline section of CIP-003.
No
We believe this training program would more properly be included in CIP-004. Since security awareness and policy should be closely related, we believe the two subjects should both be addressed by CIP-004 R1.1.
No
“...at least a quarterly basis” may be stated contrary to the SDT’s intent. Since a quarter (1/4) is the smallest interval allowed, more frequent reinforcement would be considered a violation while less frequent would not be, since no upper interval limit was established. And like other intervals, quarter

is subject to interpretation as to whether a calendar quarter is intended, or any random three month period measured to the day. We suggest: "… at least once every calendar quarter." Also, please see our comment under Question 9 above.

Yes

Thank you for removing low impact from this requirement.

No

5.4 contains the magic words "where technically feasible", which will require TFEs for items that cannot meet strict compliance. Contrary to the statement regarding inventory, the TFE process will require a detailed inventory of those items an entity is requesting an exception for. We suggest substituting "possible" for "technically feasible."

The comment form provided no room for comments not addressing particular requirements, so we are listing our more general comments here. From the webinar we understand that where the requirements refer to tables where none of the table entries applies to an entity, the requirement itself is not applicable. Since this is not the general case for the relationship between requirements and sub-requirements in NERC standards, we suggest explicitly stating that this is how it works in the CIP standards. We find the Applicability-Facilities Section (4.2) in CIP-003 to be confusing, since all the requirements of this standard appear to apply to the applicable entities and not to facilities.

Suggest removing the 4.2.1 through 4.2.3, or stating more clearly how the facilities affect the requirements. The background section of CIP-003 goes into great detail regarding the table format while CIP-003 itself does not follow this format. Please remove or rewrite this section. The very last statement of the guideline section of CIP-005 references a document we are not familiar with. Please provide a complete reference or link to its location.
Individual
Thomas Lyons
Owensboro Municipal Utilities
Yes
The definition of “Control Center” needs to be very clear. It should be explicitly stated that a Control Center must have control functions over 2 or more BES facilities and that these BES facilities must be located in 2 or more separate geographic locations. If this definition is not clear, smaller entities that might otherwise be considered low impact may be labeled inappropriately as medium impact. The SDT should consider the addition of voltage criteria so that Control Centers are more easily identified. For example, a Control Center could be defined as supporting the real time operation of 2 or more BES facilities operated at 200kv & above or 3 or more BES facilities operated at 100kv & above. In addition, wording should include the following: Control rooms located at generation facilities should be excluded unless they perform the functions of a System Operator as a TOP, BA, or RC and perform control for the above mentioned BES Facilities.
Yes
“Control Center” in section 2.13 should be capitalized.
No
The wording of R1.1 is confusing. It may be more effective if this is divided into two separate requirements. For example: R1.1. Responsible Entities shall update the identification and categorization within 30 calendar days of a modification to BES Elements or Facilities if the modification is intended to be in effect for more than 6 calendar months and causes a change in the identification or categorization of the associated BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. R1.2. Responsible Entities shall update the identification and categorization within 30 calendar days of a BES Element or Facility being placed into operation if it is intended that the BES Element or Facility will be in operation for more than 6 calendar months and causes a change in the identification or categorization of the associated BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.
Yes
No
“And” needs to be struck from moderate and high VSL in the phrase “High and Medium Impact and BES Cyber Assets”.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No

Quarterly reinforcement of security awareness concepts will be difficult to implement and burdensome to document in order to sufficiently demonstrate compliance. The periodicity of on-going reinforcement should be at the discretion of the responsible entities. Annual training on security awareness concepts may be more practically implemented and more easily documented.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Responsible Entities need to be allowed some discretion in evaluating the effectiveness of security-related patches or updates and in determining the potential threat posed by an identified vulnerability. There may be circumstances when unintended effects of a patch or update are more debilitating to a Responsible Entity's Cyber System than the vulnerability being addressed. This may be implied within the requirement since the remediation plan is to be created by the Responsible Entity, but probably needs to be more explicitly defined if the requirement is going to be similarly applied by Compliance Enforcement Authorities throughout the various regions.
Yes
Yes
Yes
Yes

No
If not read in conjunction with the rationale, it may not be understood that an incident is reportable per the terms established by the DOE and by NERC in EOP-004. Perhaps R1.2 should state: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident as defined in NERC Reliability Standard EOP-004 Attachment 2-EOP-004.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Randy Hahn
Ocala Utility Services
Yes
Control Center – (1) We assume that a Control Center is only a Control Center is used by an BA, TOP, GOP or RC. The definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” For clarity, we suggest adding this clarity (RC, BA, TOP, and GOP entities only) to the definition. (2) The use of the word “facilities” in a fashion that does not mean “Facilities” will lead to confusion and ambiguity, especially since “facilities” is used later in the same sentence as meaning “Facilities”. We suggest: “One or more sites hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation Facilities or transmission Facilities, at two or more locations”. Facilities should also be capitalized in the first bullet. (3) "support" needs to be better clarified, and limited to only control centers that provide electronic support (specifically exclude any control center that does not provide

continuos electronic data to System Operators, otherwise any control center that receives any verbal instructions or inquiries from a System Operator could be drawn into the Medium impact, as supporting operations by System Operators) BES Cyber System – Maintenance Cyber Asset is not defined, suggest changing to Transient Cyber Asset. BES Cyber System Information – (1) Security procedures should not be on the list because it creates a conflict between CIP-011-1 that restricts access to the information and CIP-003-5 and CIP-004-5 that require general training and dissemination of those procedures. (2) BES Cyber System Impact is not defined. CIP Exceptional Circumstance should include imminent danger to a BES Facility as a condition. CIP Senior Manager – the definition should exclude CIP-001, at least until it is retired with Project 2009-01
Yes
Attachment I - Bullet 1.3, Transmission Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” Attachment I - Bullet 2.13, (1) Transmission Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” (2) The term “control centers” should be capitalized in the phrase “generation control centers” to make it clear that it refers to the defined term “Control Center” In the application guidelines, when discussing the BES Reliability Operating Services, the bullets have associated with them the functional entity that typically provides those services. However, there are exceptions and the guidelines ought to reflect those exceptions; for instance, a TO may also provide UFLS. Also in the application guidelines, the word “facilities” is used in a fashion that does not mean “Facilities”, which creates ambiguity and confusion (e.g., Facilities by definition is part of the BES, whereas assets owned and operated by DPs and LSEs are typically not BES). Suggest using “elements”. The Application guideline discussion of bullet 2.13 of Attachment 1 is not consistent with the actual bullet. Attachment I - Bullet 2.7 is inconsistent in its terminology, switching between “Facility” and “Lines”. It seems that “Line” is intended. The focus also seems to be “at a single station or substation” where the focus ought to be a single BES Cyber Asset / System that controls multiple Lines. We suggest changing the first sentence of 2.7 to read: “Multiple Transmission Lines operating at 200 kV or higher, but less than 500 kV, where the total weighted value of all BES Transmission Lines whose Reliability Operating Services would be adversely impacted within 15 minutes if a single BES Cyber Asset / System is rendered unavailable, degraded or misused exceeds a value of 3000.”
Yes
OUS agrees with the requirement but questions whether the standards actually meet the stated goal of the requirement to “not require discrete identification” of Low Impact BES Cyber Assets / Systems. There are numerous examples which seem to contradict this stated goal as described later in these comments and specifically to this requirement. How does one distinguish between a BES Cyber System and a non-BES Cyber System? Does this mean that we need to inventory all of our cyber assets and develop a test to distinguish between “Low” and “non-BES”, even though R1 says that “Low” does not “require discrete identification”? How are entities to prove to auditors that the identification and categorization was done without having an inventory, i.e., discrete identification? The VSLs seem to imply that “Low Impact” needs to be discretely identified, e.g., what happens if an entity categorizes a Medium Impact as a Low Impact? In order to review correct categorization, doesn’t the auditor need to review Low Impact to see if they should have been categorized Medium or High Impact?
Yes
Yes
Yes
No
“Implemented” is not the right word because it creates double jeopardy with the rest of the CIP standards, e.g., a violation of another standard could mean that the policy was not implemented.

Suggest changing to use the phrase “in force”, meaning that the policy is in force and able to be enforced, but not requiring enforcement of the policies in this requirement (implement includes enforcement), but rather enforcement is contained in ensuing standards. OUS suggest rephrasing to: “Each Responsible Entity shall have in force one or more documented cyber security policies …” The standards are inconsistent in its use of BES Cyber Assets /Systems, e.g., R2, to be consistent with CIP-002-5, should use the phrase “BES Cyber Assets and BES Cyber Systems”. Alternatively, CIP-002-5 could just use BES Cyber Systems. The bullets are incorrectly numbered; they should be 2.1 through 2.10 and not 1.1 through 1.10
Yes
Yes
Yes
“Cyber Security Policy” should be “cyber security policies” to be consistent with R2 and R3.
Yes
Yes
Yes
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 2.1, the measure and the requirement do not match. The requirement is to “define the roles”, the measure includes “and the training needed for each role”. Suggest adding this phrase from the Measure to the Requirement.
Yes
The phrasing of requirements that refer to tables is ambiguous with ambiguous reference of prepositional phrases. For instance, in this requirement, it is unclear if an entity that only has Low Impact BES Cyber Systems needs to develop training or not, i.e., does the prepositional phrase “that includes …” refer to “training program” or to “Responsible Entity” or to both? We suggest rephrasing: “Each Responsible Entity that owns applicable systems described in the Applicability column of Table ___ shall ___ in accordance with the applicable terms of Table ___” Such rephrasing should be done to all requirements that refer to a table associated with that requirement. In addition, measures should not include the word “must”. Measures are not enforceable but are instead examples of evidence.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 4.2, the phrase “up to the current time” is problematic since it infers that 7 year criminal background checks need to be updated on at least a daily basis to cover “up to the current time”, This should be reworded to seven years prior to the last background check.
Yes
No
The flow of the bullets seems backwards and missing a job function analysis step. In addition, the word “minimum” implies an optimization that is impractical to achieve, e.g., do we want every individual account to be optimized to that individual, which is very difficult to administer and prone to error, or rather do we want to establish account groups based on job functional analysis with associated, appropriate levels of permission and assign individuals to these groups. The latter is easier to administer and less prone to errors, and follows established practices such as security clearance levels. FMPA suggests the following “flow”: 1. Job function analysis 2. “Account group” establishment with appropriate levels of permissions based on job function analysis with associated permissions 3. Assignment of individuals to the appropriate “account group” based on their position
No

Bullet 7.1 is impossible for resignations. How is it possible for an entity to revoke access at the same time they receive a resignation? Footnote 2 does not help because it only applies to termination. For termination, the entity should know about the termination before the employee; however, for a resignation the reverse is true. OUS proposes to create a new bullet specific to resignation and require revocation of access by the end of the next calendar day. Bullet 7.2, the urgency is out of alignment with the risk. Next calendar day means that if a re-assignment occurs on a Friday, that weekend work is required when that level of urgency is not justified by the situation / risk. OUS suggest end of the next calendar week.
No
The Severe VSL for R3 includes the phrase “The Responsible Entity did not fully implement its cyber security training program” which makes it a binary VSL and eliminates the High VSL described. For counts, e.g., R6, R7, should there be a time frame identified? E.g., 2 individuals within a year, within the audit period?
No
The requirement does not describe the overall purpose of the processes required. Are these processes to deny unauthorized access? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define technical and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the procedural and technical controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. Bullet 1.2 is ambiguous and implies another requirement. First, one does not “use” EAPs to control and secure, rather, EAPs are controlled and secured through use of some other means. Second, the requirement is to secure only identified EAPs, e.g., is it a non-compliance if an entity misses an EAP, e.g., did not identify it? Third, the Measures are all to support the identification of EAPs and not to “secure and control” EAPs as required by the Requirement. And fourth, the ensuing bullets (1.3, 1.4) seem to be requirements to secure and control EAPs; and hence, bullet 1.2 seems to create double jeopardy. OUS suggests rewording bullet 1.2 to require identification of EAPs and not “secure and control”.
Yes
No
The VSLs are binary, so, it seems that if one EAP is missed, it is a severe violation. Is this appropriate? OUS encourages the SDT to develop non-binary VSLs.
No
Bullet 1.1 is ambiguous. How can physical access be restricted without a Defined Physical Boundary? Does this imply that Low Impact assets need to be enclosed in both horizontal and vertical dimensions? Does a fence of xx height suffice? Does video surveillance suffice? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define operational and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. The application guidelines act to embed a de facto standard requirement of 96 square inches that, if desired to actually be a requirement, must be specified in the actual Requirements of the standard and not in an application guideline that is not enforceable. Alternatively, a definition of a Physical Access Point could be developed with established thresholds that may vary between High, Medium and Low Impact and then the defined term used in the standard. FMPA is aware of challenges made by auditors to entity compliance surrounding issues like how thick does dry-wall need to be to constitute a wall. To avoid disputes between auditors and entities over what constitutes a Defined Physical Boundary, and what constitutes physical access points, OUS encourages the SDT to develop bright-line criteria. Such criteria could be different for different risk impacts, e.g., for illustration purposes only: • High Impact might require 6 wall enclosure with every access of 96 square inches or larger opening defined as an access point with wall

material of metal, concrete, or drywall of xx inches • Medium Impact may not require a roof, but, requires a fence or wall height of xx inches topped with a climbing deterrent such as barbed wire. • Low Impact video surveillance is sufficient. The standard is very ambiguous as to what is a sufficient physical boundary and will be open to debate between compliance and entities if such bright line criteria are not developed.
No
The note to bullet 2.2 that says “there is no need to document the escort or handoff between escorts” is inconsistent with the requirement of bullet 1.1 which states that visitors need “continuous” escort. How would one prove that escort was continuous without documenting the hand-offs? On bullet 2.2, what does the phrase “on a per 24 hour basis” mean? Does this mean that a visitor must be logged in and out on the same day and that if a visitor is there at midnight, then the visitor must be logged out at midnight on the prior day and logged back in the following day, or does this mean that military time is to be used when annotating the log?
No
Bullet 3.1 is not limited to Medium and High Impact with the term “Locally mounted hardware or devices associated with Defined Physical Boundaries since Defined Physical Boundaries is not limited to only Medium and High Impact assets through its definition. This implies that all physical access controls, even those to Low Impact, are to be tested. Presumably, this includes padlocks used to control gates to fences, non-electronic door locks that control access to substation control houses that contain Low Impact digital relays, etc. Such an interpretation would then require an inventory of those access controls, and presumably, to ensure a complete set, an inventory of Low Impact assets and their Defined Physical Boundaries. OUS suggests adding to the end of the phrase “Defined Physical Boundaries associated with Medium or High Impact …”
Yes
Yes
No
On bullet 2.2. - (1) Suggest adding the phrase “addressed by the security related patches or updates” after the word “vulnerabilities” as clarification. (2) “Remediation” implies compensatory measures; the standard should not require compensatory measures because such measures may reduce reliability. Consider another term such as “palliative plan”, “alleviation plan”, or “assuagement plan”.
Yes
No
Bullet 4.3 implies redundancy, e.g., how will we know that event logging failed unless a redundant system tells us? Bullet 4.4 is a data retention requirement and does not belong as a requirement, but rather in the Evidence Retention section of the standard.
No
Bullet 5.4, if “implement” as used in R5 means to “carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures”, then, this bullet 5.4 would require a complete inventory of all Low Impact BES Cyber Assets to ensure that default passwords were changed …. To solve this, implement could be removed from the parent requirement and replaced with “have”, e.g., “have processes”, and then the bullets that require asset by asset / system by system implementation could re-insert the word implement. As such, what would likely need to happen is two bullets would need to be created for default passwords, one for High and Medium which would use the phrase “implement procedural controls” and another for Low Impact which would use the phrase “have procedural controls” to distinguish between a system by system approach for Medium and High and a programmatic approach for Low.
No
No
This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect

and respond to cyber security incidents. Otherwise, how is one to “identify, classify and respond to BES Cyber Security Incidents” on Low Impact systems? This “hidden” requirement is inappropriate. OUS recommends making R1 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, even for Low Impact systems.
No
This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect and respond to cyber security incidents. Otherwise, how is one to know “(w)hen a BES Cyber Se4curity Incident occurs”. This “hidden” requirement is inappropriate. OUS recommends making R2 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, and hence this is duplicative for Low Impact systems. Bullet 2.2, “implement” is not the correct term and is duplicative with the parent requirement. How would one “implement” the entire response for a table top drill since no IT systems would be involved? “Exercise” or equivalent term is more appropriate, e.g., “R2 … implement a process for … 2.2 (an) Exercise …” Bullet 2.3 is an Evidence Retention requirement and should not be a requirement.
No
See comments to Questions 34 and 35. OUS believes that in order to make this requirement applicable to Low Impact systems, which implies that CIP-007 become applicable to Low Impact systems and this “hidden” requirement is inappropriate. Instead, standard CIP-008-5 should not be applicable to Low Impact systems, especially in consideration of the requirements of EOP-004-1 which require entities to analyze and report cyber security incidents.
Yes
No
Bullet 1.4, what does the word “verified” mean, that the data is “retrievable”, or that all the data is verified? The intent seems to be that the data is retrievable, otherwise 2.2 seems duplicative.
No
Bullet 2.1, “implement” is not the correct term and is duplicative with the parent requirement. How would one “implement” the entire recovery for a table top drill since no IT systems would be involved? “Exercise” or equivalent term is more appropriate, e.g., “R2 … implement a process for … 2.1 (an) Exercise …” Bullet 2.2 “current configuration” is not accurate. The back-up will not reflect the “current configuration” but the configuration at the time of the back-up.
Yes
Yes
Yes
The CIP Senior Manager (or delegate) should approve the baseline (1.1). Presumably, the baseline would be “reset” periodically to reduce the number of changes that need to be tracked, and the CIP Senior Manager (or delegate) should approve the new baseline (1.3).
No
Having to monitor all the assets associated under the Applicability section of Table R2 is a huge TFE generator based on the requirement. If the intent is to make sure that there have been no modifications to the device, it would seem appropriate that one could monitor other items and not just the configurations in order to meet the requirements of FERC Order 706, paragraph 397. OUS suggests that there are methods, such as documented monitoring of logins, wherein if a device has not been logged into, the configurations need not be constantly monitored. Having a yearly requirement to verify configurations (via MD5 hash matching, for example) is an acceptable requirement, but having to constantly monitor the devices for any configuration change is going to be impossible for many devices, and create an unnecessary burden on entities.
No
Bullet 3.2, what is an “active” vulnerability assessment? The term is ambiguous.

Yes
No
There should be recognition of law, e,.g., unauthorized people are only granted access in cases where the law requires divulging that information, such as public records acts, or a discovery process order by a judge. It would seem that access to BES Cyber Security Information should be approved by the CIP Senior Manager as a separate bullet under R1.
Yes
Yes
Yes
Individual
Tracy Richardson
Springfield Utility Board
Yes
SUB suggests the addition of a definition for the term “BES Cyber System Impact”. SUB assumes that it is in reference to CIP-002—5 Attachment 1 “Impact Categorization of BES Cyber Assets and BES Cyber Systems,” but other entities may not have the same assumption(s). Based on information received during NERC’s November 11, 2011 Electronic Security Perimeter (ESP) webinar, SUB would recommend adding clarification similar to the following language to “BES Cyber Systems”: “If an entity has determined that it has no Critical Cyber Assets, then it is not possible to have an Electronic Security Perimeter, and no BES Cyber Systems.”
Yes
SUB is concerned with the inclusion of Distribution Providers (DPs) in the Version 5 CIP Standards, as well as with the qualifiers proposed for Load-Serving Entities in the Applicability section of CIP-002-5. This inclusion will draw in small entities with no operational capabilities and cause them to go through an administrative burden of proving they either do not provide BES Reliability Operating Services or they do not have cyber assets associated with this equipment. SUB recommends that a bright line criteria method for Registered Entities to demonstrate “no impact” and be given an outright exemption from CIP-003-5 through CIP-011-5.
No
CIP-002-5 Attachment 1 – Impact Categorization of BES Cyber Assets and Cyber Systems addresses Impact Categorization, but there appears to be no guidance in the actual identification of BES Cyber Assets and BES Cyber Systems. In the Background statement of each of the Version 5 CIP Standards, it is noted that, “Standard CIP-00X-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the Version 5 CIP Cyber Security Standards.” However, CIP-002-5 is titled BES Cyber Asset and BES Cyber System Categorization, with no mention of identification. Measure 1 for Requirement 1 of CIP-002-5 requires physical lists for High and Medium categorization; however there is no list requirement for Low Impact. The following Version 5 CIP (CIP-003 through CIP-011) Standard Requirements imply or assume that all Responsible Entities (regardless of impact) have created a list identifying BES Cyber Assets and BES Cyber Systems. SUB recommends either adding a Low Impact BES Cyber Assets and BES Cyber Systems list requirement, or altogether removing the Requirement for those with a Low-Impact (or no impact) categorization. SUB believes more guidance and clarity should be provided for the actual identification of BES Cyber Assets and BES Cyber Systems, and suggests general guidelines be provided on how Registered Entities would identify demarcation points where a BES Cyber Asset and/or BES Cyber System begin and end. It is also SUB’s recommendation that a bright-line criteria method for Registered Entities to demonstrate “no impact” and be given an outright exemption from Standards CIP-003-5 through CIP-011-5.

Yes
SUB agrees with Requirement 2, believing this is not a change from previous versions of the CIP Cyber Security Standards, and understands this to already be a part of an entity's annual Self-Certification process.
No
SUB is concerned that an entity will need to produce a list of Low-Impact BES Cyber Assets to demonstrate that they have correctly (or incorrectly) categorized BES Cyber Assets in the "Low-Impact" category. This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
Yes
SUB does not see this as a new requirement, based on previous versions of CIP-003.
Yes
SUB does not see CIP-003-5 R2 as a new requirement(s), but just as a consolidation of requirements spelled out in previous versions of the CIP-002 through CIP-009 Standards.
Yes
SUB does not view this as a new requirement, based on previous versions of the CIP-003 Standard.
Yes
SUB does not view this as a new requirement, based on previous versions of the CIP-003 Standard.
Yes
SUB does not view this as a new requirement, based on previous versions of the CIP-003 Standard.
Yes
No comment.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
No
SUB agrees with this programmatic approach to a culture of cyber security by requiring entities to have a Security Awareness Program. However, SUB sees a quarterly requirement as too severe, particularly for entities with Low Impact BES Cyber Systems. SUB proposes separating the applicability based on impact and providing different time basis for each.
Yes
SUB agrees with CIP-004-5 R2 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with CIP-004-5 R3 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with CIP-004-5 R4 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with CIP-004-5 R5 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with CIP-004-5 R6 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
In Part 7.2 Requirements for reassignments or transfers, "by the end of the next calendar day" does not take into consideration weekend days. SUB would recommend "by the end of the next business day" for High and Medium Impact. SUB agrees with CIP-004-5 R7 not being applicable to Low Impact BES Cyber Assets and Cyber Systems.

No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
No
Based on information received during NERC's November 11, 2011 Electronic Security Perimeter (ESP) webinar, SUB would see value in adding clarification similar to the following language: "If an entity has determined that it has no Critical Cyber Assets, or BES Cyber Systems, then it is not possible to have an Electronic Security Perimeter." Requirement 1 of CIP-005-5 again implies that a listing of BES Cyber Systems, including those for Low Impact BES Cyber Systems, has been or would need to be created. Many of the Requirements of the Version 5 CIP Standards can be interpreted to require a listing of BES Cyber Systems. SUB recommends either adding a Low Impact BES Cyber Systems Identification List requirement in CIP-002-5, or removing the Low Impact BES Cyber Systems Electronic Security Perimeter requirement from CIP-005-5. SUB believes this requirement or non-requirement for a listing should be addressed in CIP-002-5, and SUB's preference is the removal of the requirement.
Yes
SUB agrees with CIP-005-5 R2 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
Yes
There's a typo in M1. "Evidence must includes…" SUB suggests, "Evidence must include each of the documented physical security plan(s)…" SUB does not disagree with requiring operational and procedural controls to restrict physical access to be defined. However, as previously commented in CIP-002-5, SUB is concerned that an entity will need to produce a list of Low-Impact BES Cyber Assets to demonstrate that they have correctly (or incorrectly) categorized BES Cyber Assets in the "Low-Impact" category. As also noted in CIP-005-5 comments, the CIP-006-5, Part 1.1 Requirements apply to Low Impact BES Cyber Systems, which assumes that a list of these systems has been created. SUB recommends either adding a Low Impact BES Cyber Systems Identification List requirement to CIP-002-5, or removing the Low Impact BES Cyber Systems Physical Security Plan requirement from CIP-006-5. SUB's preference is the removal of the requirement.
Yes
SUB agrees with CIP-006-5 R2 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees CIP-006-5 R3 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
Yes
SUB agrees with CIP-007-5 R1 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB appreciates the extended time period to allow for documentation of implementation.
Yes
SUB agrees with CIP-007-5 R3 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes

SUB agrees with CIP-007-5 R4 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with APPA's comments that point out that when requirements are applicable to All Responsible Entities including Low Impact BES Cyber Systems, these requirements must address "programmatic protection controls". SUB agrees that this approach to a culture of cyber security requiring facilities with Low Impact BES Cyber Systems to be covered by programmatic plans or procedures will improve cyber security. However, Table R5, Part 5.4 calls for "Procedural controls for initially changing default passwords," in the Requirements, but in the Measures the first bullet says; "Demonstration showing default vendor passwords have been changed, sampled on a locational basis." SUB agrees with APPA's recommended language changes. Requirement 5 of CIP-007-5 again implies that a listing of BES Cyber Systems, including those for Low Impact BES Cyber Systems, has been or would need to be created. Many of the Requirements of the Version 5 CIP Standards can be interpreted to require a listing of BES Cyber Systems. SUB recommends either adding a Low Impact BES Cyber Systems Identification List requirement in CIP-002-5, or removing the Low Impact BES Cyber Systems Electronic Security Perimeter requirement from CIP-005-5. SUB believes this requirement or non-requirement for a listing should be addressed in CIP-002-5.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
No
SUB is concerned that the Requirements of CIP-008-5 create potential conflict with the Requirements of EOP-004-2. The development of the two Standards appears to be in parallel with one another, rather than working together. SUB recommends more coordination between the Version 5 CIP SDT and the EOP-004-2 SDT. SUB understands CIP-008-5 to be the "Incident Response Plan" and EOP-004-2 requires the development of an "Operating Plan for Event Reporting." However, CIP-008-5 Table R1, Part 1.1 requires a process to "identify, classify, and respond to BES Cyber Security Incidents" while EOP-004-2 R1.1 requires; "A process for identifying events listed in Attachment 1." SUB recommends the SDT revise the CIP-008-5 Requirement and Measure in Table R1, Part 1.1 to remove the terms "identify" and "classify." Table R1, Part 1.2 requirement of a process to determine if an incident is a "Reportable BES Cyber Security Incident" is in direct conflict with Event Reporting Reliability Standard EOP-004-2. SUB suggests Part 1.2 be removed and coordinated with the EOP-004-2 SDT. Table R1, Part 1.3.3 requires definition of "Internal staff and external organizations that should receive communications of the incident." EOP-004-2 R1.3 requires "A process for communicating events in Attachment 1 to the ERO, the RC… and other appropriate entities." APPA suggests Part 1.3.3 be removed and coordinated with the EOP-004-2 SDT.
Yes
No comment.
No
Table R3, Part 3.2, 3.3, and 3.4 requires different times for updates, both 30 and 60 calendar days. For consistency and clarity, SUB again recommends coordinating with the EOP-004-2 SDT, which allows 90 calendar days for update of the plan.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
Yes
SUB agrees with CIP-009-5 R1 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with CIP-009-5 R2 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes

SUB agrees with CIP-009-5 R3 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
No
The definition of the term “configuration” is unclear. Configuration is not clearly defined in the Glossary of Terms Used in NERC Reliability Standards, Definitions of Terms Used in Version 5 CIP Cyber Security Standards, nor in the CIP-010-1 Cyber Security – Configuration Management and Vulnerability Assessments Standard. Are “configuration management”, “configuration change management”, and “asset management” intended to be synonymous in the way they are used in the CIP-010-1 Standard? Configuration is only mentioned in terms of “security configurations”. SUB recommends that a specific definition be provided for Configuration, Configuration Management, Configuration Change Management, and/or Asset Management. Perhaps, based on the extensive changes to definitions in Version 5 of the CIP Standards, it would be appropriate to create a CIP-specific glossary of terms used in the CIP Standards. SUB agrees CIP-010-5 R1 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
SUB agrees with CIP-010-1 R2 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
SUB agrees with CIP-010-1 R3 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
Yes
No comment.
Yes
No comment.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
No
As previously stated, SUB believes that an entity must identify all BES Cyber Systems and Cyber Assets, push systems through the Medium / High impact filter, and come out at the end of the process with a “Low Impact” (or No Impact) list of systems and assets (which may be a “null” list). While there are no requirements to specifically identify Low Impact systems, this does not remove applicability for the Low Impact BES Cyber Systems from the Version 5 CIP Standards. In the Background statement of each of the Version 5 CIP Standards, it is noted that, “Standard CIP-00X-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the Version 5 CIP Cyber Security Standards.” However, CIP-002-5 is titled BES Cyber Asset and BES Cyber System Categorization, with no mention of identification. Measure 1 for Requirement 1 of CIP-002-5 requires physical lists for High and Medium categorization; however, there is no list requirement for Low Impact. The following Version 5 CIP (CIP-003 through CIP-011) Standard Requirements imply or assume that all Responsible Entities (regardless of impact) have created a list identifying BES Cyber Assets and BES Cyber Systems. SUB recommends either adding a Low Impact BES Cyber Assets and BES Cyber Systems list requirement, or altogether

removing the Requirement for those with a Low-Impact (or no impact) categorization. SUB would also recommend that a simple method for DPs and LSEs to demonstrate “no impact” and be given an outright exemption from Standards CIP-002-5 through CIP-011-5.
Individual
Kirit Shah
Ameren
Yes
Definition of BES Cyber Asset – The second line where it states “, when required,” is out of place and as used does not make sense; please remove, or remove the comma. Definition of BES Cyber System – The proposed definition of BES Cyber System contains a reference to a “Maintenance Cyber Asset.” This should be replaced with the term “Transient Cyber Asset.” Definition of BES Reliability Operating Services – Inclusion of Dynamic Response to BES Conditions, the inclusion of Governor response provides for a wide array of systems. Consider listing the systems that should be included. Definition of BES Reliability Operating Services – Inclusion of Controlling Voltage, the inclusion of AVR does not define if it is for voltage control from the generator terminals or from the high side of the GSU. This service can create some jurisdictional problems where part of the system is owned by transmission, and the other part is owned by generation. Definition of BES Reliability Operating Services – Inclusion of Restoration of BES in the list of BES Reliability Operating Services is too broad without clarifying language that only those systems absolutely necessary for the restoration of the BES must be considered as BES Cyber Systems. Definition of BES Reliability Operating Services – Inclusion of Situational Awareness in the list of BES Reliability Operating Services is too broad without clarifying language that only those systems absolutely necessary for the continuing operation of the BES must be included as BES Cyber Systems. For example, there are visualization tools used purely for market participation purposes which serve a situational awareness function but which do not enhance reliability operations in any way and which do not pose any threat to the BES if compromised; those should not be included as BES Cyber Systems. Definition of Control Center – As constructed, the inclusion of the bullet beginning with “Providing information” would cause a facility containing a communications processing node which received information from multiple BES facilities to be classified incorrectly as a control center. For example, a substation containing a MUX which received RTU readings from multiple other substations or a satellite data node in a distributed EMS system located in an unattended communications hub would qualify their locations as control centers. This would have a chilling effect; removing from consideration some otherwise preferable communication systems designs. This clause does not bring in any facilities which would not be covered by the other items in the bullet list; it should be removed. Definition of Cyber Assets - Need to retain "and communication networks". We believe that without keeping the communications as part of the definition, any programmable device at a location, for example, within a substation, is a cyber asset regardless of whether we communicate to it or is used for communications. Our understanding is that this does not follow the original intended purpose of the CIP standards which is to secure remote communications to devices used to control the system. Definition of Electronic Access Control or Monitoring Systems – Remove the words "or BES Cyber Systems" at the end of the sentence. This is related to our comments above. Unless the BES Cyber Systems is not removed, the existing definition of Cyber Assets may require a need to put physical security around each location, for example substation, depending on interpretation. Definition of Electronic Access Point – While the need for a broad definition which allows for the wide range of real-world situations is appreciated, this definition does not properly capture the nature of an access point. The use of “Cyber Assets”, rather than any inclusion of “BES Cyber Assets”, implies that any barrier device anywhere within an Entity is in scope. The use of “restricts” rather than “allows but restricts” logically implies that even an Asset which is not connected to a BES network could be considered as an access point. The use of “interface” adds nothing to the definition and will lead to unnecessary confusion. Proposed replacement definition: “A Cyber Asset which allows but restricts routable or dial-up communication between a BES Cyber Asset and another Cyber Asset.” Definition of Interactive Remote Access – The second sentence adds nothing to the definition and could leave some unintended gaps; it should be removed or it should be clarified that the three items are examples.
Yes
In the application guidelines on page 18 of 30, the table at the bottom of the page needs to include the LSE Function Registration type and LSE needs to be referenced throughout the application guidelines. In the first bullet under Overall Application, the verb tense for “support” and “supports”

switches back and forth. “Supports” is correct. Under High Impact in the 5th line, a word is missing from “it must be noted that there may "be" agreements”.
No
Requirement 1.1 as stated is confusing. Suggested replacement: “Update the identification and categorization within 30 calendar days of the date when a change to BES Elements and Facilities is placed into operation, if the change is intended to be in service for more than 6 calendar months and causes a change in the identification or categorization of any related BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.” M1: It is impossible to create a categorized list of High and Medium impact assets without a resultant Low Impact list. For version 3, auditors have pointed out that you cannot have a CCA list unless you have a list of all Cyber Assets at a location. A similar situation exists in version 5 here as the last sentence to R1 and M1 are in conflict with each other. In R1, the phrase "do not require discrete identification" implies that Low impact BES Cyber Systems do not require categorization at all; but, in M1 it asks for evidence of categorizing of Low Impact BES Cyber Assets and BES Cyber Systems. Thus, R1 and M1 are contradictory and we suggest the last line of M1 should be removed.
No
M2 – Need to change the words after CIP Senior Manager to "or delegate approve" after CIP Senior Manager on the 3rd line of the paragraph for M2 and remove the words "review and update".
Yes
No
R1 Requirement – Change R1 to R2 to match legacy numbering in previous CIP versions.
No
R2 Requirement – Change R2 to R1 to match legacy numbering in previous CIP versions. Also, update numbering of sub-requirements to match requirement number.
Yes
No
R4 Requirement – Add the words "Medium or High Impact" in front of the words "BES Cyber Systems" on the first line.
Yes
Yes
R6 Requirement - The description of this requirement [on page 14 of 22] appears to have a typo, in that a "2" is included at the end of the first sentence.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
R6.6 Requirement - This requirement contains a grammatical error in the form of an extraneous “of” at the end of line 3.
No

R7 Applicability – This section needs to be revised to: Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets, and Associated Physical Access Control Systems of: High Impact BES Cyber Systems or Medium Impact BES Cyber Systems. R7 Rationale - The third paragraph could be interpreted to mean that all authentication credentials must be revoked for personnel to be considered as having their access revoked, rather than revocation being accomplished by revoking only the credentials which can allow the terminated individual to gain access to the Asset in question. If revoking "all" is the intended interpretation, it should be clarified; but, we believe that it would require a substantial amount of resources for no additional security gain and would cause unnecessary enforcement actions. If "all" is not the intended interpretation, the paragraph should be re-drafted to better clarify the intent. Suggested replacement text: Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services), although revocation can be accomplished by revoking all permissions which could allow the terminated individual to gain access to a given Cyber Asset. R7.1 Requirement – The words “at the time of” is poorly-defined, and many possible interpretations of it cannot be technically enforced as there is no threshold. R7.2 and R7.3 Requirements – There is no security benefit to using a one-day requirement for revocation as opposed to a seven-day revocation. In the entire span of UA 1200 and CIP versions 1 through 3, there have been no known incidents where a shorter revocation requirement would have prevented an incident. Consider stating “by the end of the next business day” in circumstances where a transfer may take place on a weekend or holiday. Consider changing all “calendar day” statements to “business day” statements to account for weekends and holidays. Application Guideline - We hesitate to call for more stringent wording, but In the Application Guidelines it seems to indicate that no action is required to revoke access in the case of the death of an employee. Given that unused accounts represent a small but real security risk with no corresponding benefit, the table should be changed to require removal of access in a reasonable timeframe.
No
The VSLs for R1, R2, and R3 should be should be progressive instead of binary. Also, the VSL for R6 has too many “or” clauses. Consider labeling VSLs for sub requirements to eliminate the multiple or statements.
No
R1.1 Requirement - In the requirement “define” should be replaced with “define and implement” for clarity. R1.1 Measure - The requirement states “technical or procedural controls” while the measure states “documented technical and procedural controls.” Please match language of the Requirement and Measure to their intended purpose. R1.2 Requirement - In cases where only one connectivity method exists, please state in the requirement “routable and/or dial-up” R1.3 Applicability - Change applicability for High Impact BES Cyber systems by adding the wording "with External Routable Connectivity." R1.4 Applicability - Why are these controls in place for “non-Interactive” or read only remote access? Would suggest removing this language out of the Applicability section.
No
Application Guideline - Requirement R2, If the Secure Remote Access Reference Document is going to be referenced in the Application Guidelines, then it needs to be included in the ballot packet and voted on along with the rest of the package because auditors may use content of this referenced document for the audit which is not the intended purpose of the referenced document. R2.3 Requirement - Need to define "multi-factor authentication" by adding this term to the definitions document.
No
(1) All the VSLs should be progressive instead of binary. (2) VSL for R1 should be split out into sub-requirements because they do not match the BES Cyber System classification. For example, if a Responsible Entity did not define any technical or procedural controls to restrict unauthorized electronic access for a Low Impact BES Cyber System this should not be a Severe VSL.
No
The Application Guidelines do not sufficiently allow for the development of new types of technology which could provide improved controls. R1.4 and R1.5 Requirements – We have concerned about the term "real-time" as it is not defined. Irrespective of the definition, these requirements should have

the possibility of a Technical Feasibility Exception; to preclude that possibility may hinder mitigating an emergency to issue an alert. We further suggest that, the alert language should be changed from issuing real-time alerts to issuing alerts within 15 minutes along with an option for TFE. R1.6 Requirement - Remove “of” after “entry” on the second line of the paragraph.
No
R2.2 Requirement – Need to remove the words "on a 24-hour basis". This could become an issue if the visitor crosses the midnight time-line. Suggest inserting words to allow a visitor turnover process in cases where the visitor begins work on shift 1 but continues through shift 2. This way the escorts can change without the visitor having to log in and out of the system.
No
R3.1 Requirement – Wording needs to be added to this requirement to prevent systems that are in place prior to version 5 to be forced to perform pre-commissioning testing for version 5. We suggest adding clarification to the Application Guideline on the reasons for a 24 calendar month M&T period and also provide some examples of M&T programs used in the industry.
No
VSL for R1 should be split out into sub-requirements because they do not match the BES Cyber System classification. For example, if a Responsible Entity did not document operational and procedural controls to restrict physical access for a Low Impact BES Cyber System this should not be a Severe VSL.
No
R1 Applicability – This section needs to be revised to: Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets, and Associated Physical Access Control Systems of: High Impact BES Cyber Systems or Medium Impact BES Cyber Systems. Other tables should include similar clarity.
No
R2.1 Requirement – Add the words "security related" in front of the words "software and firmware". R2.1 Measure – Remove the last sentence of the measure as we do not see a reason for it in reference to meeting the requirement.
No
R3.1 Requirement – This requirement should allow for the possibility of an Asset which requires no action, such as a vendor-hardened security appliance. R3.3 Applicability – This requirement should be limited to High Impact BES Cyber Systems and to Medium Impact BES Cyber Systems with External Routable Connectivity. R3.4 and R3.5 Applicability – This requirement should be limited to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, and Associated Protected Cyber Assets. Transient Cyber Assets (stated in the Measure) do not include Physical Access Control Systems or Electronic Access Control or Monitoring Systems per the definition of a Transient Cyber Asset.
No
R4.1 Requirement – As a clarification, at the end of the requirement, add the words "Devices that cannot log a particular event do not require a TFE to be generated" to cover devices that cannot produce logs. R4.2 Requirement – Remove the words "necessitate a real-time alert" at the end of the requirement and replace with "be necessary". R4.2 Measure – Remove the end of the sentence starting with "necessitate a real-time alert" and replace with the word "necessary". R4.3 Requirement – Replace the words "calendar day" with "business day after notification". Suggest making High Impact the next business day and the remaining categories 7 calendar days. R4.4 Requirement – Remove the word "consecutive". R4.4 Measures – Remove the last part of the sentence starting with the words "and records of disposition". R4.5 Requirement – We do not see a reason to rectify deficiency before the end of the next calendar day in every case. We suggest to remove the last sentence or change rectification period to certain number of business days.
No
R5.4 Requirement - would require a massive effort to change passwords for devices already in place in Low Impact locations (for an average mid-sized utility, for example, 200 Low Impact substations with an average of 25 Assets per substation would represent at least 5000 password changes during the implementation phase) with no noticeable benefit to security, given the required physical protections and the unimportance of the Facilities involved. This represents the single point currently

at which the v5 standards treat Low Impact BES Cyber Systems on an individual basis rather than on a programmatic basis, and that substantially changes the nature of the work required to comply with the standards, that is removing resources from the much more important work of securing the High Impact Assets. Also, suggest restating the requirement to simply "Procedural controls for initially removing, disabling, or changing default passwords, where technically feasible. For the purpose of this requirement an inventory of Cyber Assets is not required". R5.5 Requirement – Since the passwords are changed at the Asset level not the System level, add the word "Assets" after the words BES Cyber System" in the requirement.
No
(1) VSL R1 through R5 – For Medium Impact Assets, the VSL level should be changed to Medium and High from High and Severe. For Low Impact Assets the VRF should be changed to Low and the VSL should be changed to Low. (2) The VSL for R1 and R2 should be progressive opposed to binary.
No
R1.1, R1.2, and R1.3 Applicability – Include removal of Low Impact BES Cyber Systems from the Applicability section because security incidents have to do with incidents to the Electronic Security Perimeters and the Defined Physical Boundaries that Low Impact BES Cyber Systems would not have.
No
R2.1 Requirement – Remove the words "or test" from the end of the sentence. R2.2 Requirement – The initial timing required by 2.2 is confusing. A literal interpretation would require that the Entity be conducting the test implementation of the plan on the day that the standard goes into effect. The boilerplate wording used here should be replaced with a statement that the plan be tested before the implementation date of the standard and then repeated within 15 months of the pre-implementation test. R2.3 Requirement – Propose deletion of this sub requirement as this sub requirement is only a documentation issue that is already stated in the compliance section (1.2) of the standard. R2.1, R2.2, and R2.3 Applicability – Include removal of Low Impact BES Cyber Systems from the applicability section because security incidents have to do with incidents to the Electronic Security Perimeters and the Defined Physical Boundaries that Low Impact BES Cyber Systems would not have.
No
R3.1 Applicability – Include removal of Low Impact BES Cyber Systems from the applicability section because security incidents have to do with incidents to the Electronic Security Perimeters and the Defined Physical Boundaries that Low Impact BES Cyber Systems would not have. R3.4 Requirement – Need to remove the comma in the requirement section of 3.4.
No
VSL - Make the VSL for R2 progressive opposed to binary.
No
The column headings above 1.4 are incorrect. Suggest adding an Application Guideline for all of CIP-009 as a guideline would be very helpful. R1.3 Requirement – This requirement needs to be reworded to "One of more processes for the backup, storage, and restoration of information required to restore BES Cyber System functionality". R1.4 Requirement – This requirement needs to be reworded to "Ensure that backup processes are completed successfully for Information essential to BES Cyber System recovery".
No
R2.1 Requirement - The initial timing required by R2.1 is confusing. A literal interpretation would require that the Entity be conducting the test implementation of the plan on the day that the standard goes into effect. The boilerplate wording used here should be replaced with a statement that the plan be tested before the implementation date of the standard and then repeated within 15 months of the pre-implementation test. R2.2 Requirement – On lines 3 and 4, remove the words "initially and". R2.3 Requirement – Change the words "39 months" to "3 years not to exceed 39 months" to match other requirements on a 39 month schedule.
No
R3.1 Requirement and Measure – Remove the phrase "when BES Cyber Systems are replaced". R3.2 Requirement and Measure – Add the words "or incident" after the word "exercise". R3.4 Requirement – Suggest the deletion of Requirement 3.4 as is a new requirement for the CIP standards with no security benefit and it does not align with FERC Order 706.

Yes
No
R1.1.4 Requirement – Add the words "installed on the BES Cyber Asset" to the end of the sentence. R1.1.5 Requirement – Reword requirement to "Any network accessible ports and services; and". R1.2 Requirement – Reword requirement to "Document approved changes to the BES Cyber System that deviate from the existing baseline configuration". R1.5.2 Requirement – Remove the end of the sentence after the words "production environment" as it is too burdensome and unnecessary to document all the insignificant differences between test and production environments.
Yes
No
Application Guideline – The Application Guidelines for R3 needs an editorial correction, “not” rather than “note”. Also, the phrase “Strongly encouraged” is vague and subject to different interpretations, so suggest removing it.
Yes
No
R1.1 Requirement– Add the word "implement" at the beginning of the requirement. R1.2 Requirement – Correct the column header labels. Add the word "Establish" at the beginning of the requirement.
Yes
Yes
No
The implementation schedule needs to be modified to allow different time frames for Low, Medium, and High BES Cyber Systems. Recommend an implementation schedule of 36 months for High and Medium Impact BES Cyber Systems and 48 months for Low Impact BES Cyber Systems.
Individual
Aliza Dewji P.Eng
ATCO Power Canada Ltd.
Yes
Section 2.13 of Attachment 1 contains a 300 MW threshold for generation control centers. The application guideline suggests that the 300 MW value was used because the same value is used for UVLS and UFLS. The rationale for this threshold is flawed as generation control centers have no control over load-shedding. In addition there is a significant difference between a loss in generation and the loss of load. If the intention is that shedding load and loss of generation are to be treated the same, then the 300 MW threshold should apply to all generating units over 300 MW. The 300 MW threshold for generation control centers is far below the 1500 MW threshold for generating units with common mode vulnerabilities set out in section 2.1. In addition, the 1500 MW was approved by industry in the Version 4 consultation. As 1500 MW was derived from the single largest contingency criteria, the principle behind that value is acceptable. ATCO Power suggests that the SDT consider removing generating control centers from section 2.13. If this is done, generation control centers that control 1500 MW or more of generation will be covered under section 2.1, and all generation will be handled consistently.

Individual
Alice Ireland
Xcel Energy
Yes
1) Control Center: We recommend the definition be modified as follows, in order to add clarity: A facility hosting BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for more than one BES generation facility or transmission facility, at more than one location: 2) Routable Protocol: We recommend that

a Routable Protocol definition be created and added using criteria in the "Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets" version 1.0, dated June 17, 2010. For example, this would maintain the listing of example non-routable protocols shown on page 27 of this NERC guidance document. 3) Electronic Security Perimeter (“ESP”): Please clarify what is meant by the phrase “collection of Electronic Access Points”. Discussions within a NERC webinar on 11/18/11, “Establishing an Electronic Security Perimeter”, indicated that the general meaning of network based controls would not be impacted.
Yes
1) There appears to be an error in category 1.4 where it references 2.12 (which is UFLS and UVLS). To match version 4 the cross-reference should be to 2.11 (Special Protection Systems). 2) The meaning of 'adversely impact' is unclear. We recommend that the preambles in Appendix I, for high and medium control level facilities, be modified to read: “Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes, cause one or more of the following BES Reliability Operating Services to malfunction, preventing operation within prescribed reliability limits.” It is well understood that 'prescribed reliability limits' are those routine or situational operating requirements for the listed services, and ‘malfunction’ means the inability to respond to reliability needs as expected.
Yes
Yes
Yes
Yes
Yes
No
1) We feel that the requirement should reference cyber security policies created to satisfy CIP-003-5 R2. The wording could be modified as follows: “Each Responsible Entity shall review each of its cyber security policies created to satisfy CIP-003-5 R2 and obtain the approval of its CIP Senior Manager . . . “
Yes
Yes
Yes
Yes
No
1) Table R1, Part 1.1: The quarterly awareness is too frequent, considering many other critical aspects of reliability task execution are successfully and consistently implemented with a longer reinforcement period. A suggested change: Table R1, Part 1.1: "A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on an established interval, not to exceed a calendar year." 2) Table R1, Part 6.4: The quarterly verification of accurate access provisioning requires more effort than needed if the initial provisioning event is properly executed. A too frequent interval allows for complacency and potential 'process escapes' between quarters. A better process would require continuous verification (lists updated at the time access is granted). This ensures day to day control. The periodic verification should be used to confirm proper execution of this process. Recommended change: "Verify at least once each calendar year that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access."

Yes
Yes
Yes
Yes
No
1) The requirement parts 6.1-6.3 states “Access permission shall be the minimum necessary for performing assigned work functions.” We would like to ask for clarification on the meaning of “the minimum necessary” and how this is to be measured. While someone may not access a CIP facility or BES Cyber System on a regular basis, their job description or the location of an asset/system may require access only infrequently. If access, electronic or physical, is only used occasionally will a violation be considered under the minimal verbiage? 2) We believe the approach of quarterly verification of physical or virtual access to listed BES Cyber assets is too frequent. It assumes the ongoing, as needed verification process for a personnel status change (requires access, now does not require access) may not be executed properly. We believe that a process that requires quarterly reconciliation to ensure secure physical and virtual access is broken. We propose instead that the process for day to day management of personnel status changes for access be reviewed at least annually, and then, based on the results of that review, the frequency modified commensurate with conditions found. For example, a good on-going process should show no 'process escapes' for the previous period, and not require quarterly reviews. A process that shows errors should then be reviewed quarterly until two consecutive error-free verification reviews are performed.
No
CIP-004 R7.1 states, “For resignations or terminations, revoke the individual’s unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.” R7.2 states, “For reassignments or transfers, revoke the individual’s unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.” Finally, R7.3 states, “For resignations or terminations, revoke the individual’s access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.” The “same day” and “next calendar day” requirements do not allow for normal business flow especially in the case of holidays, vacations or weekends. Most databases update nightly (or on a 24 hour schedule) so the notification to revoke access, unless done manually every time, would be behind the requirement. If done manually, this would require an unprecedented amount of labor from management, Human Resources and in the case of access, Security. Additionally, for transfers, “the next calendar day” does not allow for the review of new role descriptions and required access reviews. It is recommended that the verbiage for the revocation within 24 hours for “for cause” situations and 7 days for those who no longer require access be re-established for requirements R7.1, R7.2 and R7.3. If not 7 days, a period of time that would allow for notification to management and the necessary databases to be updated.
Yes
Yes
No

1) Part 2.2 from Table R2 requires encryption for all Interactive Remote Access sessions. Some entities still use dial-up access, for any number of reasons such as cost, lack of infrastructure, etc. and encryption is not an option with dial-up access. This section should be modified so as not to require entities to redesign their entire system. The modification could read something like “Require encryption for all Interactive Remote Access sessions, where supported by available technology, to protect the confidentiality and integrity of each Interactive Remote Access session.” 2) In addition, Part 2.3 from Table R2 requires multi-factor authentication, with the additional note that a UserID is not considered an authentication factor. Under many instances, this multi-factor authentication will be difficult to achieve, and by removing a UserID as an authentication factor, it becomes even more difficult. We recommend this be modified to allow for UserID as an authentication factor.
Yes
Yes
1) CIP-006 R1.4 states, “Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.” Please clarify if the standard of “real-time” allows for any system delay? While the time between the alarm and the notification is minimal, there may be a short delay. 2) In regards to the Application Guidelines for CIP-006-5 R1 which state, “Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.” Xcel Energy provided comments related to protective measures in CAN-0031. Our comments are, “While we appreciate NERC providing some flexibility in how compliance with the six-wall border requirement is met, we feel this is going beyond the scope of what can be discerned from the standard. Furthermore, the source documents seem to introduce even more ambiguity as to what type of materials might be acceptable for construction of your PSP. Instead, we propose that NERC provide clarification on what threat(s) an entity should be protecting against. Then an entity's chosen protective measures/materials could be tested against those threats. This method would be more effective in ensuring a secure environment, and would allow for the introduction of new materials and defense strategies as the industry and vendor products develop/mature.” While the language has been changed from PSP to Defined Physical Boundary the need for clarification on what the threat we are trying to protect from is still needed.
Yes
Yes
Yes
The Table of Compliance Elements, R1 under High VSL states, “The Responsible Entity has documented and implemented physical access controls, but does not initiate a response within 15 minutes of a detected unauthorized physical access into a Defined Physical Boundary.” Please clarify what constitutes an appropriate level of “initiation” of a response. For example, if a response is in motion, such as personnel on their way to the site, does that meet the intent of “initiation” of a response? Additionally, the lower VSL for R1 states, “The Responsible Entity has documented and implemented physical access controls, but logging of authorized physical entry through any Defined Physical Boundary does not provide sufficient information to uniquely identify the individual and date of entry”, while the secondary, Severe VSL (as indicated by the OR) states, “The Responsible Entity has documented and implemented physical access controls, but two or more different and complementary methods do not exist to restrict access to High Impact BES Cyber Systems.” These two VSLs seem to be reversed. Would it not be a greater risk to the BES to have unidentified individuals accessing an area at unknown times than to have a documented and functioning access control system without a secondary measure?
No
Part 1.1 of Table R1 requires that the entity disable or restrict access to unnecessary logical network accessible ports. From the wording of the proposed requirement, it is unclear what a necessary port would include; is it only ports used during normal operations, does it include ports used to access the asset during maintenance, etc. In addition, it is unclear what is meant by “disable or restrict access”. One could argue that location within a PSP and ESP would “restrict access”. This requirement should

be clarified to address this ambiguity.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Request clarification on R1.4; “Information essential . . . that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.” Does this mean that every time a backup is performed a verification needs to occur, or that when a backup system is initially configured and the first backup is performed, that the verification needs to occur?
Yes
No
Request clarification of what “Review the recovery plan(s) initially upon the effective date of the standard . . . “means in this context.
Yes
Yes
Yes
There will be significant impacts to available resources with this requirement.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Thomas M. Haire, P.E.

Rutherford EMC
No
No
No
CIP-002-5 makes great strides to remove ambiguity and categorize the potential impacts of Cyber Assets. However, the standard should be modified by one of the following: 1) plainly state those entities with no Bulk Electric System (BES) assets per the definition included in the NERC Project 2010-17, Definition of Bulk Electric System, are not required to comply with this standard or, alternatively, the Senior Manager must annually certify that the entity has no BES assets per the definition thus no BES Cyber Assets/Systems or; 2) create a fourth category of “No Impact”, thus no further action required which can be certified annually by the Senior Manager. As the standard is currently stated, smaller entities with non-critical assets of the BES appear not to be involved with this standard, but that is dependent on the interpretation of “Transmission Protection System”. Concurring with the thoughts implied in comment 27.b by PNGC (et al) and considering the recent interpretation of PRC-004 and PRC-005 regarding the interruption of electric current fed from the BES, electronic relays with no communication to the “world” could be considered a Cyber Asset even though the relay has no impact on the BES if it were to fail or was lost or compromised. But regardless, the relay would be forced into the Low category because a “No Impact” or “Non-Critical” category does not exist. The Standard, as written, tends to assume that an entity does have Cyber Assets that can impose a risk to the BES. This assumption should be removed. Furthermore, in the context of protective relays, a small entity may be required by their Transmission Provider to own and maintain Under Frequency Load Shedding (UFLS) relays or a relay system. In the standard, the UFLS threshold is established at 300MW. The small entity may not have 300 MW of total load on their electric system, but their relaying is included in an UFLS system that is much greater than 300 MW. Thus the Standard needs to clarify how the 300MW threshold applies. For example, this small entity’s relay may not be critical to the BES and if degraded or destroyed would not compromise the total capability of the Transmission Provider’s UFLS system as this system is sufficiently small to be encapsulated by the window of design of the parent system. In many cases, the two systems are not integrated and do not have communications across a wide are network. The breaker controlled from the relay in this example may be monitored by SCADA through the use of a dry contact, but the relay itself does not have any other connections to the “world” other than the leads to sense frequency, provide relay power, and to control breaker operation.. Therefore, does the small entity own a Cyber Asset due to the 300 MW level, or is it still exempt? The Standard Drafting Team should work to clearly identify the entities not included by the BES definition. As the standard is currently written, an assumption is implied that all entities own Cyber Assets and all entities’ assets impact the BES. Left to the determination of what would or would not degrade the BES, the Standard Drafting Team has created a series of interpretations and clarifications that will be required from NERC regarding smaller DPs and LSEs. The assumptions and resultant ambiguity of interpretations and clarifications should be removed.
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Tommy Drea
Dairyland Power Cooperative
Yes
Make certain all terms are formally and clearly defined so that it does not rely on any interpretation outside the version 5 documents. Also, where definitions have been altered, there should be a clear statement as to what former interpretation is no longer valid.
Yes
It is not directly clear if equipment providing operational communications between BES facilities is now in scope as being classified as subject to categorization under the standards. The previous standard clearly excluded this specifically. The version 5 standard does not directly state this positively or negatively. Does this lack of mention mean communications (whether private or commercial) between facilities are in scope if it can effect BES Reliability Operating Services? The standard should be clear on this point as it previously excluded such communications from the scope of the standards. It is common for regional entities to place communications equipment at member entity facilities and mandate connection terms and 3rd party management of equipment. This is typical for Inter-Entity Coordination and Control applications such as ICCP. This practice puts the member in the position of being physically responsible for infrastructure it cannot control. Is it valid for the member to exclude the regional infrastructure from its compliance program? Is it acceptable

for a region to place such potentially critical infrastructure beyond the bounds of their physical control (and CIP program)? If the regional WAN infrastructure is not treated as critical, how can a member/entity's Inter-Entity Coordination and Control system be presumed to be critical (as it is in Attachment 1)?
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
The Summary of Changes for R1 states in reference to in reference to R1.2 "The non-routable protocol exclusion no longer exists; therefore there is no need for this requirement." It appears that "no longer exists" means that routable/non-routable/dial-up is no longer a criteria for CIP-002 classification. It is presumed that this reference to R1.2 means CIP-005-3:R1.2 has been removed. It is confusing that CIP-005-5 also has a requirement R1.2 that specifically addresses routable and dial-up electronic access points, which excludes non-routable. In the Applicability section on page 8, Electronic Access Point has a description that excludes non-routable from its scope. Also, the "Definition of Terms used in Version5 CIP Security Standards" document defines Electronic Access Points are either routable or dial-up. In the Guidelines and Technical basis section on page 20, in

discussing applicability of trust zones and deny by default, it states “Direct serial, non-routable connections are not included.” Is the Summary of Changes in conflict with other sections of this standard? Does the standard intend that non-routable electronic access points will not be allowed? Does it intend that externally connected non-routable (serial, hard-wired I/O, etc) devices are allowed as cyber assets, but not classified as Electronic Access Points? This should be defined clearly in the standard.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Requirement 1.5 categorically requires all changes to be implemented first in a test environment. There should be a requirement to have a test system, but there should also be allowance that not all implemented changes can be effectively performed on a test system. Further, those entities with Legacy systems may have no practical means of providing test equipment to meet this requirement.

Does this make these entities non-compliant?
No
The idea of monitoring for unauthorized baseline changes is good. The implementation for many systems may be very difficult. Common modern operating systems put up a multitude of ephemeral logical ports—how to automate finding the difference between ephemeral and unauthorized? “Where technically feasible” keeps this from being a compliance issue, but seems to reduce this from a “requirement” to a “guideline”.
No
This requirement needs to me specific as to what controls are required to be tested. Does this mean all controls related to CIP-005 and CIP-007? Does it mean all standards (including personnel security or information protection)? This requirement should be clear.
Yes
Yes
Yes
No
A “Medium” VRF for R1 seems very high, when the details for this requirement seem so general/non-specific. If this item is this important, there should be more specificity as to what is required for information protection.
Yes
The implementation plan should also allow for entities who would like to transition their CIP program to version 5 at an earlier date.
Individual
Saurabh Saksena
National Grid
Yes
General comment: There has been a significant change in the framework from version 4 to version 5 regarding definitions and core concepts such as Critical Assets, Critical Cyber Assets, etc. These proposed changes are not a requirement of FERC Order 706, do not enhance cyber security controls and create administrative burdens when migrating to version 5. There should be a correlation between BES Cyber Systems and the facilities that these systems serve. The current version of the CIP standards provides the correlation and recognize that systems (CCAs) do not operate independently of facilities (CAs). Therefore, applying physical and electronic controls is more transparent. We propose maintaining the current Critical Asset and Critical Cyber Asset definitions and concepts. High, Medium and Low categorizations can still be utilized with the legacy CA and CCA concepts. Regarding the use of the term “annual” throughout the standards, we suggest that the registered entity be allowed to maintain it’s own definition of “annual” based on CAN-0010 guidelines. 1) For all definitions please include the old term that the new term is replacing, as applicable 2) The time periods included in the first and second sentence of the definition of “BES Cyber Asset” are confusing. The 15 minutes discussed in the first sentence and the “delay” discussed in the second sentence are unclear. Suggest re-wording as follows: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The 15-minute period begins to run when the asset is operated, mis-operated, or fails to operate when necessary, regardless of the time period between the asset was degraded or misused and the time the asset is then operated, mis-operated or fails to operate when necessary. 3) BES Cyber System Definition - Maintenance Cyber Asset needs to be defined or if appropriate changed to Transient Cyber Asset
No
Yes

Yes
Yes
Yes
Yes
Yes
No
We recommend eliminating this requirement and moving it into CIP-004 R2 and include policy as part of the training required. This way, all awareness and training would be in CIP-004.
No
We propose retaining the current language in CIP-003-3 R2.
Yes
There should not be a foot note in the standard – make this part of the requirement.
No
R.2 – we suggest a "Lower" VSL for "The Responsible Entity has implemented the required cyber security policy or policies but has failed to adequately document the policy or policies." R.4 – We suggest Lower to Severe VSLs be based on a failure to take action, rather than a specific number of employees who are aware. As drafted, it would be a "high" violation to miss one single employee. That seems overly strict and does not match well with the requirement and measures, particularly when measures suggested includes making an internet posting. We suggest the following: "Lower" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but has not adequately documented the measures"; "Moderate" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 30% -50% of individuals who have access"; "High" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 50% -70% of individuals who have access"; and "Severe" VSL = "Registered entity has taken no measures to make any individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function OR Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 70% or more of individuals who have access" R.5 - Why do the VSLs begin at medium for the failure of one delegation? We recommend "Lower" VSL = failure of one delegation; Moderate = failure of two delegations; High = failure of three, and Severe = failure of "four or more". R.6 – We suggest VSLs structured similarly to CIP-002 - Lower = Change to one delegation was not documented within 30 days, but was documented within 31-41 calendar days of the effect vive date ; Moderate = Change to two-three delegations was not documented within 30 days OR change to one delegation was not documented within 30 days, but was documented within 42-52 days of the effective date; High = Change to three-four delegations was not documented within 30 days OR Change to one delegation was not documented within 30 days, but was documented within 53-63 days of the effective date; Severe = Change to more than four delegations was documented within 30 days of the effective date OR Change to one delegation was not documented within 74 days of the effective date.
Yes
No
We do not believe that role based training is necessary. The personnel performing the job functions are familiar with the various controls due to their job requirements. General training on CIP, as required under current version, is all that should be required.

Yes
Yes
Yes
No
There is no added security by requiring the CIP Senior Manager or delegate to authorize access. We suggest using legacy wording that only requires access to be authorized.
Yes
No
R.1: It seems harsh to include the failure to document a security awareness program as a severe VSL. We recommend the following as a "Lower" VSL "The Responsible Entity implemented, but failed to document a security awareness program" and change the Severe VSL to "The Responsible Entity failed to implement and document a security awareness program." Additional comments around adding “Missed a quarter and/or target audience (authorized physical or authorized electronic)?” R.2: No comments. R.3: The annual training requirement assumes that the initial training was completed before access was granted, therefore, missing a small number of employees with the subsequent annual training does not necessarily indicate high risk to the bulk electric system because these employees presumably had received prior training when their access was granted. We recommend a tiered approach to the VSLs for missing the annual training requirement so that failing to meet the annual requirement for a low percentage of employees (like 10% or less) is a lower VSL, failing annual requirement for between 11-20% is moderate, failing the annual requirement for 21-30% is high, and failing to meet the annual requirement for over 30% OR failing to do the initial training is severe. R.4: No comment R.5: A documentation error should not be a "severe" VSL. Delete the "OR/documentation" part from the Severe VSL and make a Lower VSL that reads "The Responsible Entity implemented, but failed to document a process for personnel risk assessments." R.6: For most utilities, there could be 100s of employees with access, and it seems unrealistic to base the VSLs on one failure with regard to one or two employees. We recommend changing the values in the Moderate - Severe to percentages of employees 10%, 20%, 30%or more. R.7: Same comment as R.6 - change values of one to three employees to percentages.
Yes
No
Requirement 2.2 specifies encryption for all Interactive Remote Access sessions, but does not specify where the encryption is required. If the intent is to require encryption from the user to the Intermediate Device the requirement should specify that clearly. Not all assets currently support encryption, so requiring encryption from the Intermediate Device to the Asset is not practical nor necessary if encryption is being employed outside of the ESP.
No
R.1 and R.2: There should be lower VSL where the processes listed on the table are implemented but not documented.
Yes
Yes
Yes
No
R.1: There should be lower VSL where the processes listed on the tables are implemented but not documented. Add to the Lower VSL: "OR the Registered entity has implemented but failed to document the required physical access controls" R.2: There should be lower VSL where the processes

listed on the table are implemented but not documented.
Yes
Yes
No
Requirement 3.5 requires logging of each Transient Cyber Asset connection. This is not practical as many assets do not have the capability of logging when someone makes a direct physical connection to the asset. Many assets are not capable of logging to centralized logging systems. Also, in a typical day, and engineer in the field may connect a Transient Cyber Asset to many different assets and it would be impractical for one to log each connection.
No
4.1 - The intent of 4.1 as written in the Guidelines and Technical Basis section is inconsistent with the requirement. The guidance states that “It is not the intent that if a device cannot log a particular event that a TFE must be generated”. If the intent is to not be out of compliance when a device cannot log certain events, it should be stated as such in the requirement. 4.3 - The activity level of some devices is such that they may not generate a logged event every day. Therefore, responding to an event failure with a day may not be possible. 4.3 & 4.5 – there is a conflict between these two. 4.3 requires a response to logging failures before the end of the next day. But, 4.5 requires bi-weekly sampling of logged events which would uncover logging failures. If the logs are being reviewed bi-weekly then logging failures may not be detected and responded to within the next day.
No
Items 5.4 & 5.6 in Table R5 includes the phrase “where technically feasible”. Does that mean a TFE will be allowed? If so, we believe that phrase should be removed and replaced with “as supported by the BES Cyber System” to eliminate need for TFE.
No
R.1 We have the same comment here about percentages for open ports (similar theme from above). What is written in high should be in moderate. What’s in severe should be broken down by percentages/numbers. R.2 Consider severity of patch as recommended by the vendor and the percentage of assets that may not have had a remediation plan associated with that patch. R.3 Consider putting some wording in here around the percentage.
No
There is some concern that multiple plans would prevent one single entry point into the Cyber Security Incident Response Process. We’d like to make the argument that only one plan is necessary and supporting documentation can be created as necessary that supports that plan.
No
The Applicability section of the tables refers to “All responsible entities”. We suggest using the same wording that all the other standards use (High Impacts, Medium Impact, Associated, etc) In R 2.2 In the first sentence, we recommend replacing the word “implement” with “exercise.” This is really about exercising the plan on a regular basis as the plan is already implemented. In 2.3, the "measure" for "relevant documents" does not give adequate guidance to the industry regarding what documents may be acceptable to demonstrate compliance. The "measure" indicates any "dated documentation related to" the reportable incident may be accepted. Please give some additional examples of the specific types of dated materials could be considered acceptable.
No
3.1 The terms “accuracy” and “completeness” are referenced but in terms of completeness there’s not a specific benchmark to compare the document again what should be quantified as complete. The suggestion is again to define a minimum set of information that would be expected in an Incident Response Plan. 3.2 - We recommend that clarity be added to ensure that language represents that review occurs 30 days after closure of the incident rather than invocation; rationale is that you might still be remediating and won't have learnt all lessons. We recognize the importance of the requirements to review the lessons learned, update the Incidence Response plan, and communicate the updates. However under the current structure it creates a rolling compliance effort following each incident. That is, an auditor will require that after each incident one has recorded lessons learned

review, changes to the response plan or that none were necessary and updated communications or that none were necessary. It would be easier to update the plan on a quarterly basis based on the previous quarter's incidents and not have so many auditable events to track.
Yes
No
1.5 – The requirement to preserve data for analysis or diagnosis may slow down the recovery process. There are times when recovery is urgent and must be done in a timely fashion. Is your intent to include this when you say "where technically feasible"? If so, language should be added spelling it out.
No
2.2 – We recommend removal of the phrase "and reflects current configurations" from the requirement. It is acceptable to have backup information that is less than current configuration and still perform a successful recovery. If this phrase is not removed, it will require a backup to be taken and tested for even the most minor configuration changes which is unnecessary.
Yes
No
We recommend the following VSLs for number of days until plan is reviewed in R3: 31-41 days = Lower, 42-53 days = Moderate, 53 plus is High and Severe for never updating plan. We also recommend the following VSLs for number of responsible personnel that the plan updates have not been communicated to: 1 person missed = Moderate, 2-4 = high and 5 or more is severe. We like the VSLs in CIP-010 R3. These recommendations attempt to make CIP-009 R3 consistent to CIP-010 R3.
Yes
Yes
No
We recommend considering emergency equipment replacement (partial outage) as "Exceptional Circumstances" . Based on the nature of our typical outages we would consider this practice to hinder the restoration efforts and bringing systems back on-line in a timely manner. We would certainly be good with language that allowed us to bring systems back on-line, ensure they are stable and then run a scan.
No
We recommend the following VSLs for number of days until documentation is updated in R1: 31-41 days = Lower, 42-53 days = Moderate, 53 plus is High and Severe for never updating documentation. R3 We like this structure. We've suggested this approach a number of times We aren't talking about whether or not this is violation, but rather about the severity of the violation and then rating the severity. We think this is a really good approach.
Yes
No
The footnote here should be part of the requirement.
No
We recommend the following VSLs on R 2: If the process to prevent unauthorized retrieval wasn't done on 1 device that would be low 2-5 moderate, more than 5 is high.
No
Due to the current status of version 4 (not FERC approved), there is potential for overlap of implementation with version 5 that could create extensive rework in a short period of time. This will cause an unnecessary expense to entities while not providing any additional cyber security benefit.
Individual
MIchael Johnson

APX Power Markets
No
Comments: Page 3 – under the Balancing Load and Generation section, “Unit commitment” section the word “know” should be “known”. Page 5 – Monitoring & Control – recommend that you include “situational awareness” into the definition. There is a separate definition for it, but including it here ties the two together better. Example: “… provide monitoring, situational awareness, and control of….” Page 6 – Control Center – include “situational awareness” in the fourth item. Example: “Alarm monitoring, situational awareness and processing specific…” Page 8 – Transient Cyber Asset – I believe it would be good to have examples on what these can be. There will be too much guessing and possible CEA leeway here to make in-consistent application of the definition. This is my major issue with this document.
No
Page 9 – M1. The last sentence that starts with “Evidence of categorization of Low Impact BES…”. What does this mean – it did not may a sense to me. Examples would be a help here. Attachment I – for items 1.4 and 2.1 it would be good to include some reference or example that relates to a Registered Entity that does not own generation, but provides services to those who do. Our business model is a SCADA SaaS provider – we connect generators to the ISO, so the loss of our systems could have significant impact on a regions capability to see what their generation is (situation awareness) and impact the BES if conditions change and the ISO could not see those changes in sufficient time to react to them. I have asked the SDT about our situation and it is felt that 1.4 and 2.1 would cover us, but it would be helpful if it was clearer. For 1.4 suggested modification could be “that includes control or situational awareness of one or more….” For 2.1 suggested modification could be “Generation or Control Center with an ….” I believe the above ties together independent references to Control Centers and Situation Awareness to make it clearer on their importance and impact to the BES .
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
This will be very difficult to implement for Service Vendor where the individual executing the service will not necessarily be the same person. This happens with hardware issues and the dispatch of the first Technician who can respond to the ticket. Getting vendors to agree to training would be almost

impossible for large service vendors like DELL, HP, IBM. I would like to suggest that the Guidelines include examples for exceptions to having this type of training that does not include an “emergency”. We can get around this by declaring everything an “emergency”, but that is not the spirit of the requirement. If we have hardware in a remote data center a service Tech may be brought into the facility and then left with the hardware while the work is being performed. The personnel bring the person into the facility are not employees of our company and we are charged for each 25 minutes they can not do other tasks. Would like to see provisions for exceptions that are documented with some type of mitigation. I do not have a suggestion on what they could be, but would be will to help the SDT define what the mitigations are.
Yes
Yes
Yes
Yes
Yes
Yes
No
Encryption and multi-factor of internal communications to some type of devices could be a problem. Encryption can be expensive for devices to implement and vendors may not be willing to provide that. Agree with the External communications that are coming in-bound. Need to allow for exceptions related to internal communications.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Real-time alerting is error prone – daily log review should be allowed as an alternative for those items that can generate a high number of false-positives.
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Need to allow the Registered Entity (RE) to define what the baseline configuration items are and will be monitored. This is not specifically spelled out that I can see. If the baseline configuration is not cleared defined (or allowed to be defined by the RE), I can see the CEA defining their own set of items that the RE may not being watching for.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Scott Bos
Muscatine Power and Water
Yes
MPW is recommending that since CIP version 4 has been approved by the NERC BOT and is awaiting approval from FERC, that CIP-002-5 be placed on hold. Our industry has approved CIP-002-4 and the terms Critical Assets and Critical Cyber Assets are well known terms within our current cyber security plans. The following supporting information outlines a superior solution to the proposed version 5 standards that meets the main FERC goal of including more critical assets without requiring a reduction in reliability by forcing entities to retool their existing programs from scratch. The proposed solution below allows entities to start from a firm industry approved base (CIP-002 version 4) and modify its controls (CIP-003 through CIP-011). This approach also appropriately maintains an ultimate focus on protecting the BES elements, which is the fundamental reason all NERC standards exist. The proposed CIP version 5 approach inappropriately drifts towards an Information Technology based approach. While this is understandable, given the fact cyber security is involved, any solution must remain focused on protecting the BES from instability, uncontrolled separation, and cascading as a whole from a relatively large coordinated attack. If the SDT does not take this recommendation,

then the following comments are submitted concerning Version 5 CIP Standards. Significant work needs to be performed on the definitions. Many times new definitions are proposed in version 5 that aren't an absolute necessity. This would require entities to unnecessarily revise documentation and drawings just to meet new wording in a definition when the old definition or a change to the definition itself, rather than the term/phrase, would suffice. For example, instead of changing Critical Cyber Asset to BES Cyber Asset, retain the term Critical Cyber Asset and change the definition of Critical Cyber Asset to include "within 15 minutes". Definitions may also confuse and unnecessarily expand the scope of compliance. This will likely generate the need for Compliance Application Notices and Standard Interpretations. The CIP Rev 5 definitions and requirements are confusing in that they require entities to carefully align separate definitions and requirements to understand the full impact. They also unnecessarily expand the compliance scope into assets not currently covered by CIP Rev 4. This expansion will increase the burden on almost all entities. One example is, a BES Cyber Asset is defined as a "Cyber Asset that if rendered unavailable, degraded or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, adversely impact one or more BES Reliability Operating Services". The use of "adversely impact " is ambiguous and will lead to people applying their own interpretation to what "adversely impact" means. An entity may have generation connected at the distribution level that when unavailable may adversely impact any one of a number of items listed in the definition of BES Reliability Operating Services. MPW recommends the SDT update BES Cyber Asset to be: "A Cyber Asset that if rendered unavailable, degraded or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, would impact the reliable operation of the BES within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance". This recommend definition is based on and is aligned with Section 215, Electric Reliability, (a), (4) of the Federal Powers Act. The above recommended definition would also allow for the definition of BES Reliability Operating Services to be deleted, since BES Cyber Asset is clearly identified. The definition of BES Reliability Operating Services includes several items that a non-BES user or owner does in real-time. Other examples and opportunities for improvement: 1) BES Cyber Asset: Contains multiple references to other definitions. It is unclear as to the "within 15 minutes of its operation" inclusion. The redundancy of devices should be taken into consideration if there is a totally isolated redundant system providing the same functions or in a supervisory role. In protection schemes, there are primary and secondary relays which protect the same lines and a good practice recommends the relays have different logic/hardware to avoid common mode failures (totally independent of each other). 2) BES Cyber System: Need to correct reference to Maintenance Cyber Asset 3) BES Cyber System Information: This begs a definition of "BES Cyber System Impact" (is this based on section 215 of the Federal powers Act?). 4) Situational Awareness: Definition includes the term "Situation Awareness Operating Service" that is not defined. The Current day and Next Day Planning functions can normally be performed on a corporate PC. Does this bring the entire corporate network into scope? 5) Control Center: Based on this definition, a Control Center could be a building at a substation with 2 RTU's that monitor a 345 KV substation with multiple transmission facilities (lines) and a 115 KV substation with multiple transmission facilities (lines) in two different yards (locations) but geographically adjacent. Need to clarify that the two or more locations refers to some type of geographical separation. If not, the control building could meet the bulleted items under the Control Center definition. 6) Transient Cyber Asset: Break up the 3rd qualifier based on the intention of the SDT as such: "3) capable of altering the configuration, or (and) 4) capable of introducing malicious code to the BES Cyber System." A second example of where definitions may also confuse and unnecessarily expand the scope of compliance is shown just below: 1) CIP-002-4 requires cyber controls on: Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection. (Emphasis added) Whereas: 2) CIP-002-5 requires cyber controls on: Control Center One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations: • Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, • Inter-utility exchange of BES reliability or operability data, • Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES, • Alarm monitoring and processing specific to the reliable operation of the BES and BES

restoration function, • Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES • Coordination of BES restoration activities. 3) Medium Impact Rating (M) Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for: 4) 2.13. Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners; or (2) generation control centers that control 300 MW or more of generation (emphasis added) The concern here is that every Distributed Control System (DCS) that controls two or more generators or substations with a total output of more than 300 MW will now be subject to the CIP Standards. Even if the DCS is not externally connected by serial or routable protocols it will be subject to the CIP standards.
Yes
MPW is recommending that since CIP version 4 has been approved by the NERC BOT and is awaiting approval from FERC, that CIP-002-5 be placed on hold. Our industry has approved CIP-002-4 and the terms Critical Assets and Critical Cyber Assets are well known terms within our current cyber security plans. The following supporting information outlines a superior solution to the proposed version 5 standards that meets the main FERC goal of including more critical assets without requiring a reduction in reliability by forcing entities to retool their existing programs from scratch. The proposed solution below allows entities to start from a firm industry approved base (CIP-002 version 4) and modify its controls CIP-003 through CIP-011. This approach also appropriately maintains an ultimate focus on protecting the electric grid elements which is the fundamental reason all NERC standards exist. The proposed CIP version 5 approach inappropriately drifts towards an Information Technology based approach. While this is understandable, given the fact cyber security is involved, any solution must remain focused on protecting the Bulk Electric System from instability, uncontrolled separation, and cascading as a whole from a relatively large coordinated attack. Issue: As currently drafted Version 5 of the CIP standards: • Would significantly increase cost without a commensurate increase in the reliability, safety, or security of the BES. • Create significant complexity, confusion, and administrative burden regarding the identification of Critical Cyber Assets, the definition of terms, and implementation of Cyber Controls. • Does not consider that smaller Entities have a much lower impact on the BES • Greatly exceeds FERC's 706 order without justification. Proposed Solution: 1) Retain CIP-002-4 as approved by the industry in 2010. It is filed with FERC; industry and NERC comments on the FERC NOPR recommended FERC approval. This will: • Eliminate the confusing and complicated process developed to identify BES Cyber Systems proposed by the drafting team in Rev 5 • Meet FERC's 706 for CIP-002-1: o Industry approved guidance documents for identifying Critical Assets and for identifying Critical Cyber Assets. ¶253-258, 270-273 o CIP-002-4 replaces the Critical Asset guidance and aligns with FERC's affirmation that the applicable responsible entities are responsible for identifying Critical Assets. ¶319-321 o CIP-002-2 added senior manager approval of risk-based methodology. ¶294-297 • Not exceed FERC Order 706: • ¶284: "… there is no formally accepted method for identifying critical cyber assets before us at this time … we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time." • ¶285: "CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial up access … We do not find sufficient justification to remove this provision at this time." 2) Develop a new standard for High Impact Assets: • That identifies which assets in CIP-004-2 are High Impact and • Clearly states the extra protection required for High Impact Assets: o The Draft version 5 identifies eight extra protections, most are in response to FERC Order 706. o Provides opportunity for a separate implementation timeline for the additional controls that apply only to High Impact assets. o Provides flexibility in adjusting controls on High Impact assets. In the future only one standard has to be modified. o Entities that do not have High Impact assets will not have to sort through all the standards and RSAWs to assure compliance and security. 3) Develop a separate standard for the Low Impact assets or abandon this concept. • Lows were not directed by FERC Order 706 nor included in the SAR. o A separate standard provides full transparency in the stakeholder process. o This is a scope expansion not supported by many in the industry. o Cost and compliance concerns with lows include whether lows have to be listed. This is a derivative of which controls are selected and how they are designed and audited. 4) Revise CIP-003-5 through CIP-011-5 and Definitions to reflect changes described in this paper and meet FERC Directives in order 706 If the SDT does not take this recommendation of maintain CIP-002-4, then MPW submits the following comments. Keep the "bright-line" criteria thresholds defined in CIP-002-4 in the CIP-002-5 standard. There was much industry input into developing these thresholds and it does not seem appropriate to modify them

again. It is difficult for utilities to keep up with the changing thresholds in the changing CIP versions and associated implementation plans, with no BES reliability improvement Issue - 1 high Impact, bullet 1.2, states: Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority. MPW does not understand how this can be applied to every BA, regardless of size. Upon review bullet 1.2 has qualifiers for a TOP in order to be a High Impact category (notwithstanding that a TO should not be included since TO's are not required to have primary or backup control centers). We can easily see that there is some stratification afforded to TOP and GOP Control Centers, based on voltage levels, total MW, total MVAR, number of lines, Blackstart Resources, etc, for being considered High Impact or Medium Impact. While the SDT has acknowledged there are some distinct differences between larger and smaller TOP's and GOP's, we want to point out that not all Balancing Authorities are created equally. Does anyone think that the smallest BA in North America, serving 38 MW of load, has the same Reliability Impact as a BA serving 10,000 MW, or more, of load? Does it really improve the reliability of the BES to have ALL those smaller BA Control Centers carry the same High Impact Rating? Issue - Criterion 2.7 in Attachment I describes the "weight value" to be applied to transmission lines. There is no guidance given for transformers. Many entities may treat a facility that has multiple voltages as separate substations, with separate control houses, and may be assessing the independent Impact Level of each voltage as separate facilities. Therefore, there must be some guidance on how to deal with transformers. Furthermore, it is suggested that the weight value given a transformer (if transformers are to be included in the calculation) be the weight value of the secondary, not primary side. For example, a 345kV substation may have a single 345kV transmission line out of it, weighted at 1300. That same substation may then have two 345kV/230kV transformers. It is not obvious from criterion 2.7 what the total weight of the substation would be. It is suggested that the secondary voltage be used (if transformers are to receive a weighting value) making each of these transformers valued at 700, for a total of 2700 at this substation, making it Low Impact. However, if the primary voltage level was used to determine the weight, the transformers would each count for 1300, making the total weight value of this substation 3900, and a Medium Impact facility. It is suggested, if transformers are to be included, that the secondary voltage be used because, from the 345kV bus in this example, its two additional outlets (the transformers) are only capable of 230kV outlet flows, even though they are connected to the 345kV bus. Issue - Criterion 2.8 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLs and their associated contingencies' with wording of, '. . . as Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more IROL violations', like the wording using in Criterion 2.11. Issue - Criterion 2.11 in Attachment I states "Each SPS, RAS or automated switching scheme that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more IROL violations." It is unclear whether the phrase "that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more IROL violations" refers to the SPS itself or the BES elements that the SPS operates. It is possible (and likely) for an SPS to be a higher Impact Level than the BES elements that it operates. Assuming the phrase is meant to apply to the SPS, a suggested re-wording of this phrase is the following. "Each SPS, RAS or automated switching scheme that operates BES Elements and is capable of causing one or more IROL violations if the SPS is destroyed, degraded, misused or otherwise rendered unavailable. MPW proposes the following: Criterion 2.9 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLS and their associated contingencies' with wording of, '. . . as FACTS that if destroyed, degraded, misused, or otherwise rendered unavailable, could cause the violation of one or more IROLs', like the wording using in Criterion 2.11. Criterion 2.12 – (1) Replaced the word, 'system' with 'common control system' to clarify that this criterion applies to a system triggered by a single (common) control, rather than a program (system) of many independent relays set to trip at the same frequency

No

Issue - What is the NERC basis for 30 days? Many Utility reviews are performed annually. NERC has not provided any technical justification for a 30 day update. An annual update is sufficient based upon the low probability of a serious cyber or physical attack. Issue - The text "all other BES Cyber Assets and BES Cyber Systems … shall be deemed to be Low Impact." This text appears to include all BES Cyber Assets in CIP scope. This has NOT been directed by FERC Order 706.

No
Issue - With recent guidance on the term “annual” provided by NERC, it may be prudent to replace the phrase “and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals” with the word “annually”.
No
Issue – MPW believes the VSLs recognize the fact that entities of different sizes are taken into account in the severity levels and associated impacts to the BES.
Issue - Most of the changes made to CIP-003, in general, were not directed by FERC Order 706. These changes do not result in improvements to security, but do result in increased bureaucracy and implementation costs for 241 entities in North America with existing programs. MPW suggests the FERC directives be addressed within the structure and language of CIP version 4. MPW proposes the following requirements for CIP003-5: R1: Cyber Security R2: Leadership R3: Exceptions R4: Information Protection
No
Issue - This is an administrative task and once implemented does not add to BES security.
No
Issue - With recent guidance on the term “annual” provided by NERC, it may be prudent to replace the phrase “and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals” with the word “annually”. Issue – MPW suggests changing to annual “review” and NOT approval. Entities need not “approve” the same security policy if there are no changes or updates.
Yes
Yes
No
Issue: What is the justification for documentation within 30 days?
Yes
No
Issue - Many of the changes made to CIP-004, in general, were not directed by FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for the 241 entities in North America with existing programs. MPW suggests the FERC directives be addressed within a structure and language that is more in line with CIP version 4. We propose the following requirements for CIP-004-5: R1: Awareness R2: Training R3: Personnel Risk Assessment R4: Access
Yes
Yes
No
Issue – MPW recommends adding clarification to R4.4 in terms of vendor support from foreign companies. Also, please clarify when an Entity or contractor is initially in the CIP Standards then they are removed (for some reason) then they are brought back into CIP compliance responsibility. Is the risk assessment previously obtained still valid if obtained within 7 year period?
Yes
No
Issue – MPW wants to point out that in FERC Order 706, paragraph 381, the Commission stated its intent is to ensure there is a clear line of authority. Order 706 did not direct making the Senior Manager authorize every individual change down to the account level. The version 5 draft is an additional administrative burden that does not commensurately improve security of the BES and

creates a disproportionate amount of administrative bureaucratic work.
No
Issue - For reassignments requiring a different level of access, there may be the need for a large amount of work in setting up new user accounts, modifying user accounts, changing firewall and router rules, etc, that cannot be accomplished by the end of the next calendar day without jeopardizing reliability. This is also an issue for BES Cyber System information for entities which are using document management systems with individual accounts to restrict access to information. It is typically easier for most Entities to “remove” an account than it is to “modify” an account, yet the modification of these accounts is subject to a single calendar day while the removal of these accounts is allowed for 30 calendar days. Due to the amount of reconfiguration needed for these types of changes, MPW suggests to allow at least 7 calendar days for modifications in access levels. Issue - FERC Order 706 did not direct a change. MPW recommends retaining CIP-004-4 where revocation already is covered. Issue - The time requirements are exceedingly restrictive for Medium Impact BES Cyber Systems. Allowing 7 calendar days for R7.1 and R7.2 would be more acceptable and practical for systems that may not be controlled centrally. Issue - MPW values how the SDT tried to give treatment to the “immediate revocation” requirement of the FERC order in Part 7.1. However, MPW feels the current language is broad, vague and considerably open for interpretation. Even with the footnote qualification, an auditor could still interpret “at the time” to mean literally “to the minute”. Complicating matters is the fact that there is often no way to determine specifically when a person resigned or is terminated. MPW suggests for Part 7.1 to restate as: “Develop and implement a program to revoke an individual’s unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of resignation or termination”. This way, the Entity is measured for compliance to their own program and not struggling to provide time-stamped comparisons that may not exist. For Part 7.5, it is possible that Entities use shared accounts for remote access. Suggest adding “...if shared accounts are used for Interactive Remote Access to BES Cyber Systems, passwords must be changed at the time of resignation or termination per Part 7.1”.
Yes
No
Issue - R1.1. To MPW, this appears to require that Entities document Low Impact Cyber Systems. This requirement should not be required for Low Impact BES Cyber Systems; otherwise, Entities would have to prove to auditors that external routable connectivity is not used at EVERY Low Impact BES Cyber System.
No
Issue - This Requirement disregards the fact that some Entities have their own (unique) communication network from the Control Centers to the Substations. Adding encryption devices and additional devices adds additional points of failure without increasing security. Exceptions should be made for interactive remote access across company-owned and operated communication links.
Yes
No
Issue - In the “Measures” column of Table R1, Part 1.1, it states the need for documented “operational and procedures controls”, while the Requirement states “operational or procedural controls.” MPW highly recommends to correct the Measures column to be consistent. If the error was in the Requirements column, MPW disagrees that operational physical access control systems should be required for Low Impact BES Cyber Systems. Issue - The Requirement in Table R1, Part 1.2 and Part 1.3, should define whether or not these physical access controls are to be operational, procedural, either, or both for Medium Impact and high Impact Cyber Systems as was done in Part 1.1 for Low Impact Cyber Systems. If operational controls are required, is a separate operational physical access control system needed to monitor the primary physical access control system or is it allowed for a system to monitor access to itself? Issue - For CIP-006, in general, MPW disagrees with changing the definition name from Physical Security Perimeter to Defined Physical Boundaries because it unnecessarily creates the need to update numerous procedure documents and physical security drawings, etc. MPW wants to be clear that changing the term does not, in any way, improve security, but increases confusion and adds costs for the 241 entities in North America that have Physical Security Perimeters.

No
Issue - R2.2 does not seem applicable to Medium Impact Substations. The logging of entry and exit of visitors will be tedious without bringing much value. R2.2. should only be applicable to Medium Impact Control Centers.
No
Issue - R3.1 and R3.2 will be exceedingly troublesome for Low Impact Facilities that use procedural controls for Physical Access Control. MPW wants to know what hardware or devices would be included? R3.1 and R3.2 should only be for applicable electronic physical access control systems.
Yes
Yes
No
Issue – MPW suggests changing the term “remediation” to “mitigation.” R2.3 appears to require the installation of the patches, where some Entities may mitigate the vulnerability through procedural controls.
No
Issue - R3.1. Allows the Responsible Entity to choose which approach they want to take to “deter, detect, or prevent.” If a Responsible Entity chooses to deter or prevent malicious code by procedural controls on isolated control systems (i.e. non-routable serial links), MPW wants to point out that requirement R3.2 and R3.3 are impossible to achieve compliance. Furthermore, R3.3 requires modifying a tested and working control system at a substation with the possibility of inadvertently introducing malicious software with manual updates (e.g. using thumb drives to install signature updates on non-networked systems). MPW recommends excluding Medium Impact BES Cyber Systems that do not have external routable connectivity. (Most AV or malicious code software cannot recognize new malicious code such as Stuxnet until the signatures are discovered anyway.)
No
Issue - FERC Order 706 does NOT direct these changes. CIP-007-5 R4.1 - The enumerated list is too prescriptive for the requirement. Add to guidelines. CIP-007-5 R4.2 – Some assets can log, but not alert. Remove “real-time”. CIP-007-5 R4.3 – MPW requests a clarification on timing. MPW proposes revised text, “Activate a response to event logging or alerting failures before the end of the next calendar day after identification.” MPW appreciates that the SDT allowed entities to develop their own system events related to cyber security, but this leaves an open door for auditors to apply their own approach (and interpretations) to what the THEY believe is acceptable. MPW believes R4.1. will be troublesome for Entities to prove compliance with Medium Impact BES Cyber Systems with no external routable connectivity, unless the auditors accept the configuration files and not the actual logs. Issue - R4.2. This Requirement also leaves a large audit hole for the Entity determining what events necessitate a real-time alert and the auditors having differing opinions of what they feel the entity should include.
No
Issue – MPW recommends to delete R5.2 because it replicates the CIP-004 access authorization requirements and could create a double jeopardy situation. Issue - R5.5.1 – FERC Order 706 did NOT direct a change to password length. Although an increase in password length from six to eight characters improves security, an increase to ten would improve it more and so on. This begs the question “Where does one stop?” Not all assets have capability for longer passwords. MPW recommends retaining the six-character password. Issue – MPW recommends that R5.4. be limited to Entities having a policy in place that all default passwords should be changed. Proving compliance at a sampled location opens up the door in an audit to have Entities having to prove compliance on all their BES cyber systems if there is 1 finding. That 1 finding would require the Entity to have to inventory all Low Impact Cyber Systems and show that every system had the default password changed. The requirement also leaves open the auditor’s interpretation of what is considered a Low Impact Cyber System at a sampled location, since there is not an inventory required by the Standard.
Yes

No
Issue – MPW recommends the SDT to coordinate more closely with EOP-004-2, SDT
Yes
Yes
Yes
No
Issue - R1.5 states, “Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.” As FERC Order 706, paragraph 708 states, “should not impede or restrict system restoration”, MPW recommends this proposed revised text: “Preserve data, when it does not impede or restrict system restoration, if necessary to determine the cause of any event that triggers activation of the recovery plan(s) as required by Requirement R1.
No
Issue - The wording in the Requirement Column of Table R2, Part 2.2, implies that all backup media must be tested annually. If an Entity, for example, has 25 Windows Servers – that entity should be able to annually test a Windows backup without having to test the backup for each system, especially if the same backup system is being used for all Servers. This is even more extreme in the case of substation cyber assets, such as protective relays. MPW recommends changing the language from “Test any information used in the recovery …” to “Test information, for each type of Cyber Asset, used in the recovery …”
No
Issue - In Table R3, Part 3.4, the language “Update recovery plan(s) to address any organization or technology changes…” is exceedingly vague with regards to technology changes. MPW recommends wording as “Update recovery plan(s) to address any organization or implemented technology changes…” Issue - R3.1. Is not clear on how soon the recovery plan has to be updated “when BES Cyber Systems are replaced”. MPW suggests to include “or within 30 days of when BES Cyber Systems are replaced.” Additionally, MPW recommends that “Update recovery plan(s) to address any organization or implemented technology changes that would prevent a successful implementation of the recovery plan”
Yes
No
Issue - The draft requirement is excessively prescriptive, which was not directed by FERC. Move these details to guidelines. MPW recommends limiting the applicability to High Impact Critical Cyber Assets, which will allow Entities to focus security improvement efforts on the highest priorities. Issue - R1.1. Will be tedious and extremely time-consuming for Medium Impact BES Cyber Systems at substations/plants. The number of IED’s and programmable devices is quite large and some of these devices may have multiple modules or add-on boards with different software versions. Issue - R1.2. and R1.4. will create many problems when making emergency repairs in the field that require replacing a “card” or “module” with different software versions and obtaining CIP Senior Manager approval without any security benefits for the BES. MPW suggestion: Provide a separate requirement for Medium Impact Control Centers and Medium Impact Systems excluding Control Centers which allow more flexibility for the type of environments and equipment. For Medium Impact BES Cyber Systems excluding Control Centers could require documenting baseline configurations on only a subset of the cyber assets (e.g. HMI’s, EAP’s, etc.) not including meters, gauges, battery chargers, electronic programmable thermostats, relays, modules, PLC’s, etc
No
Issue - MPW recommends that the applicability of Table R2, Part 2.1 include only “Medium Impact BES Cyber Systems with Routable Connectivity."
No
Issue - Annual vulnerability assessments on Medium Impact Cyber Systems will prove to be very

costly and resource intensive for utilities with multiple substations in this category that are geographically dispersed. MPW recommends allowing Medium Impact Cyber Systems to have 2 years between vulnerability assessments. Issue - Though FERC directed guidance for Vulnerability Assessments, the rewritten Standard's general reference to "security controls" could result in varying interpretations and likely expansion of assessment scope. Issue - R3.1. Needs to be reworded to more clearly define if the assessment is a vulnerability assessment or only an "assessment of the security controls", such as the EAP and Physical Access Controls. Issue - R3.2. Should allow entities to perform an active vulnerability assessment on either the production system or the test environment to meet the requirement. This will allow entities to make the choice on which environment to use and not require the documentation of differences between the test environments and production environments that leave entities open for interpretation of differences by auditors. Issue - For Part 3.2, please clarify whether all cyber assets need to be included in the assessment, or a subset, or representative sampling, or entity defined. There are certain cyber asset categories where "test" systems just aren't economically feasible. What is the acceptable deviation between test and production the auditors will allow? As written, and without explicit language in the requirement, our entity fears this will be a topic of a CAN later. Issue - For Part 3.3, please clarify whether "new Cyber Asset" means literally that or, more reasonably, could mean "new Cyber Asset category" or a new make/model, or a new function. It would be reasonable to test something that brings net-new functionality to a BES Cyber System, but if when replacing an end-of-life or failed component, it wouldn't make sense.
Yes
No
Issue - R2.1. Needs to include additional clarification of devices that are included. Where do protective relays or devices that have flash memory or other on-board memory media fall? Does this apply when reusing the device from a Medium Impact BES Cyber System to a Low Impact BES Cyber System? The application guideline does not distinguish if there is a difference between impact levels and only refers to reuse outside of a BES Cyber System (e.g. could go from High-Medium-Low without being erased.)
Yes
No
Issue - It is imperative for the industry to know whether or not Version 5 will supersede Version 4 well in advance of any implementation plan. If Version 4 has a short implementation period before Version 5 is in effect, entities will view their efforts to comply with Version 4 as "wasted" in many cases because the infrastructure required for a Version 4 Critical Asset is more than that of a Version 5 Medium Impact facility. It would be irresponsible to ask entities to "over-protect" facilities that will not be High Impact with Version 5 right around the corner. In addition, this could also have a drastic impact on decreasing reliability as many entities may elect to remove all routable protocols and dialup access to cyber assets within Version 4 "Critical Assets", to bide them time until Version 5 becomes effective. During this time, engineers would not have access to troubleshoot protection systems, retrieve fault data, and perform multiple other duties without having to travel to a remote site – this could result in prolonged customer outages, and possible instability with known defects in design taking longer to correct. Entities realize that NERC has made an effort to do this, however, there is still risk associated with version 5 not passing in time to supersede version 4. This could be catastrophic to the standards development process.
Individual
Robin W. Blanton
Piedmont EMC
No
Yes
CIP-002-5 makes great strides to remove ambiguity and categorize the potential impacts of Cyber Assets. However, the standard should be changed in one of the following: 1) plainly state those entities with no BES assets per the definition are not required to adhere to this standard or,

alternatively, the Senior Manager must annually certify that the entity has no BES assets per the definition thus no Cyber Assets; or, 2) create a fourth category stating No Impact, thus no further action required which can be certified annually by the Senior Manager. As the standard is currently stated, smaller entities with non-critical assets of the BES appear not to be involved with this standard, but that is dependent on the interpretation of “Transmission Protection System”. Concurring with thought implied in comment 27.b by PNGC (et al) and considering the recent interpretation of PRC-004 and PRC-005 regarding the interruption of current fed from the BES, electronic relays with no communication to the “world” could be considered as a Cyber Asset even though the relay has no impact on the BES if lost, but the relay would be forced into the Low category because a “No Impact” or “Non-Critical” category does not exist. The Standard, as written, tends to assume that an entity does have Cyber Assets that can impose a risk to the BES. This assumption should be removed. Furthermore, in the context of relays, a small entity may be required to own and maintain UFLS relay or relay system by the Transmission Provider. In the standard, the UFLS threshold is at 300MW. The small entity may not have 300 MW of load, but their relaying is part of the design of an UFLS system that is much greater than 300 MW. This small entity’s relay is not critical to the BES and if degraded or destroyed would not compromise the capability of the Transmission Provider’s UFLS system as the two systems are not integrated and do not communicate. Therefore, does the small entity own a Cyber Asset due to the 300 MW level, or is it still exempt? The Standard Drafting Team should work to clearly define the entities not included by the definition. As the standard is currently written, an assumption is implied that all entities own Cyber Assets and all entities assets impact the BES. Left to the determination of what would or would not degrade the BES, the Standard Drafting Team has created a series of interpretations and clarifications that will be required from NERC regarding smaller DPs and LSEs. The assumptions and then the created ambiguity for interpretations and clarifications should be removed.
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, R1 will not apply to those utilities.
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, R2 will not apply to those utilities.
Yes
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, CIP-003-5 will not apply to those utilities.
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, CIP-003-5 R2 will not apply to those utilities.
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, CIP-003-5 R3 will not apply to those utilities.
Yes
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, CIP-003-5 R5 will not apply to those utilities.
Yes
Yes
Yes

Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Marc Child
Great River Energy
Yes
The word “any” in the definition of “External Routable Connectivity” can be a bit misleading, and could be mis-interpreted as being similar to the “any” rule commonly found on a firewall. Recommend the SDT change “any” to “a”. The definition of “Interactive Remote Access” seems to refer to a person having interactive access to the operating system of the cyber system, but what about at the application layer? How does an entity give CIP-005 treatment to an EMS/DMS system in a control center that is accessed via a fat-client application via “remote” employees? The SDT should strongly consider adding a definition for the word “Access” (from a cyber perspective), or specifically state that an entity can make their own definition of access such that different treatment can be given to high-risk access versus low-risk access. High-risk meaning the ability to interact with, operate, modify, or cause availability issues with a BES Reliability Operating Service. Other examples where “access”, if left undefined, could cause problems for an entity are: VMWare hypervisors, Oracle database clusters, or NAS systems that contain both BES and non-BES data/systems. Is the entity required to give CIP-004 treatment to an accounting clerk who has “access” to a receivables data table on an Oracle cluster that also hosts the backend database to a (BES) load control or EMS system? The definitions of “Physical Access Control System” and “Locally Mounted Hardware of Devices Associated with Defined Physical Boundaries” (the latter defined within the CIP-006-5 standard) do not specifically define workstations used by guards to monitor Defined Physical Boundaries, nor do they define physical security panels which control (usually many) door readers and alarms. Are these two types of assets in scope for CIP-006-5 or not? The definition of Electronic Access Control or Monitoring Systems is still too vague. For Access Control, specifically, does this mean every cyber system that might contribute to the authentication, authorization, and accounting (“AAA”) of a person crossing an EAP? If an entity uses Windows Active Directory for firewall authentication, for instance, this could be interpreted to mean every domain controller in the company is in scope. Extending that argument,

the Help Desk PC that is used to grant access to the Windows Active Directory could be interpreted as being part of the AAA process, and therefore an Electronic Access Control cyber asset. Likewise, a PC in the Security Operations Center that is used to monitor alerts from the EAP could be considered a Cyber Asset used for Monitoring. Recommend the SDT provide a comprehensive list of cyber asset examples or "bright-line" set of criteria for Electronic Access Control or Monitoring Systems. (The same concern applies to Physical Access Control Systems as well). Lastly, the definition of "Transient Cyber Asset" leads one to believe that this only applies to devices directly plugged into other Cyber Assets, as opposed to those temporarily plugged into the ESP network. We ask that the SDT review this definition against CIP-007-5-R3.5 to ensure this was the intention.
Yes
Blackstart plans for resources used for load restoration purposes may be inadvertently included in the existing definition, specifically criteria 2.4. The Cranking Path diagram on Page 26 implies that Blackstart resources are only included where used to start a unit. Suggest criteria 2.4 be modified to read "Each Blackstart Resource identified in its Transmission Operator's restoration plan used to provide power for remote start of another generation unit(s)". Criteria 2.11 contains the words "…if destroyed, degraded, misused". (Twice). This appears to be a carryover from version 4, but it now is redundant and perhaps conflicting with the "15 minutes" qualification as defined at the top of the Medium Impact Rating section. Criteria 2.12 refers to a "system" – as in "Each system or Facility…" – that implies something of a cyber nature. The rest of the bright-line criteria refer to or describe hard assets, not cyber assets. This seems like an odd exception. Recommend removing "Each system or". Lastly, page 30 of the draft standard contains an example methodology or process flow for categorizing BES Cyber Assets and BES Cyber Systems. We realize that this graphically illustrates the overall intent of the SDT for CIP-002-5, but in reality we still have a standard that an entity will interpret as: Step One – list all my High and Medium facilities ("critical assets"). Step Two – list all my High and Medium cyber assets ("critical cyber assets"). This point of view is further supported by the fact that when you boil down all the security controls in CIP-003-5 through CIP-011-5, there really isn't any appreciable difference between High and Medium requirements. Therefore, the additional paperwork burden of stratifying High and Medium facilities and High and Medium cyber assets doesn't seem to be worth the effort. We understand that there is pressure to expand the scope of CIP to more hard assets, but let's not hide behind this High/Medium smokescreen and instead be honest with industry. Modify items 1.1 through 2.13 on Attachment I to be "All these assets have a Critical Impact Rating". Requirement 1 should therefore be "For all cyber assets including associated physical and electronic access control and/or monitoring systems and associated protected cyber assets, that support one or more BES reliability operating services at a Critical facility, apply the controls as specified in CIP-003 through CIP-011". If there are cases (like CIP-010-5-R3.2) where specific "High Impact" systems are intended, then say so in the requirement: "For Control Centers, perform an active vulnerability assessment every 39 months…".
No
What constitutes a "change to BES Elements…" per part 1.1? Suggest modifying this language to simply state that new or retired assets be added or removed from the list within 30 days of commission or decommission. For M1, we believe the intention is that entities are not specifically required to list their Low Impact systems, therefore we would recommend the last sentence be changed to "Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems is not required, but instead may be demonstrated by the application of the required controls". (New words are "is not required, but").
No
Recommend that this requirement and all others that use the words "…initially upon the effective date of the standard…" have this phrase stricken. The implementation plan that accompanies the final approved draft should include the requirements for first time iteration of periodic activities. It's not reasonable to assume that every entity is capable of executing all procedures "upon the effective date". Minor point, but this is the first time "CIP Senior Manager" is used in the standards. Perhaps add a cross-reference to the appropriate requirement in CIP-003-5. In section "B. Compliance", under sub-section "1.2 Evidence Retention", there is a typo in the second to last line. Please change "complaint" to "compliant". I'm sure this was unintentional, even though it sort of fits either way.
Yes

Yes
Yes
Yes
Yes
No
Are the measures listed under M5 actually examples of compliance, meant to be prescriptive? These are very specific and imply requirements. On this point, throughout the standards, measurements are now tightly tied to requirements and are much more prominent. We feel this is rightly so. However, we need to be very (very) careful that examples are stated as examples, lest “measures” become “requirements” themselves. Please state (somewhere) the compliance applicability of Measures. In the second bullet under M5, CIP-002-5 R3 is mentioned. There is no R3 in CIP-002-5. In the last sentence in the last bullet under M5, the words “…of the plant managers…” is mentioned. I don’t think it was the intention of the SDT to be this specific. In fact, this entire bullet is one huge run-on sentence, confusing, and should be redrafted for clarity.
Yes
Yes
Yes
No
Parts 2.2 and 2.4 seem somewhat redundant. If there was a specific distinction intended by the SDT, please rewrite to make this more clear. Part 2.10 needs a bit more clarity to understand what was intended. Was this meant to be technical training on how systems talk to each other over a network? Or is it for general knowledge on risks and controls of routable networks? Please add more clarity here.
No
One potential oversight in all versions of the CIP-004 standard is guidance on the training requirements for “transient” workers. By transient, we mean persons whose access is either temporary, or perhaps is granted and revoked on a periodic basis due to project work. We request that the drafting team add some words to R3 (or Part 3.2) to make clear the requirements for this category of worker.
No
One potential oversight in all versions of the CIP-004 standard is guidance on the PRA requirements for “transient” workers. By transient, we mean persons whose access is either temporary, or perhaps is granted and revoked on a periodic basis due to project work. We request that the drafting team add some words to R4 to make clear the requirements for this category of worker. The Applicability sections of R4 and R5 are different. This appears to be an oversight by the SDT, as it doesn’t make sense to design a PRA process for one set of assets, but implement it for a different set.
No
The Applicability sections of R4 and R5 are different. This appears to be an oversight by the SDT, as it doesn’t make sense to design a PRA process for one set of assets, but implement it for a different set.
No
Parts 6.1, 6.2, and 6.3 seem to imply that the CIP Senior Manager must specifically delegate persons who have the authority to authorize electronic/physical access. If it was the intention of the SDT that a signed list of authorizers is required, then please make this a specific requirement – either in CIP-004-5 or CIP-003-5. Parts 6.1, 6.2, and 6.3 state that “access permissions shall be the minimum necessary…” We feel this to be an aspirational statement that entities will be hard-pressed to prove at audit time. Recommend this sentence be moved to the Rationale or Guidelines section. Part 6.3

should include a cross-reference to CIP-011-1-R1.2, as in "…as documented in the entities information protection access control procedures in CIP-011-1-R1.2." Parts 6.1, 6.2, and 6.3 include the qualifier "…except for CIP Exceptional Circumstances". For consistency, we feel this language should either be stricken, or amended to include a reference back to the entities CIP Exceptional Circumstances policy per CIP-003-5-R2. Please clarify whether Part 6.5 applies to cyber access or physical access, or both. The notion of "groups" can theoretically apply to physical access control systems as well as cyber. Part 6.6 appears to be redundant to the annual information protection review performed per CIP-011-1-R1.3. Per earlier comment, the "minimum necessary" language throughout R6 will be difficult for entities to prove to an auditor and should be moved to the Rationale or Guidelines section.
No
We appreciate how the SDT tried to give treatment to the "immediate revocation" requirement of the FERC order in Part 7.1. However, we feel the current language is too open for interpretation. Even with the footnote qualification, an auditor could still interpret "at the time" to mean literally "to the minute". Complicating matters is the fact that there is often no way to measure specifically when a person resigned or is terminated. Our suggestion for Part 7.1 is to restate as: "Develop and implement a program to revoke an individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of resignation or termination". This way, the entity is measured for compliance to their own program and not struggling to provide time-stamped comparisons that may not exist. For Part 7.5, it is possible that entities use shared accounts for remote access. Suggest adding "...if shared accounts are used for Interactive Remote Access to BES Cyber Systems, passwords must be changed at the time of resignation or termination per Part 7.1".
No
In the Guidelines section of CIP-004-5, the last sentence under Requirements R3 (and again under R4) states "…by the single senior management official identified in Requirement R1". This should be re-written to say "…by the CIP Senior Manager or delegate identified in CIP-003-5-R1". In the Requirement R4 section of the Guidelines the reference to CIP-011 is a typo and should state CIP-004 instead. In the Requirement R6 section of the Guidelines, the last sentence of the first paragraph should be modified to state "Best practice recommends that access authorization and provisioning should not be performed by the same individual". Some entities are too small for strict separation of duties to be feasible.
No
How does an entity demonstrate compliance to Part 1.1 if CIP-002-5 does not require that entities document their Low Impact cyber assets? Please revise the Measures section to provide clear guidance on recommended artifacts for compliance that do not pre-suppose lists of Low Impact cyber assets. Please provide a technical basis for the requirement that outbound access permissions are necessary per Part 1.3. If no technical basis can be defined that can be uniformly applicable to all BES entities, then please qualify "outbound" to be "…inbound and, where implemented by the entity, outbound access permissions". In Part 1.5, the term "malicious communications" is too vague. Recommend changing 1.5 to say "A documented method for malicious traffic inspection at each EAP". The Guidelines section provides good information and a technical basis for R1, and the SDT should be complimented on their well-reasoned analysis, but we have concerns about Guidelines and Technical Basis language being included within the Standards themselves. The third paragraph, for example, states "This requirement applies only to communications for which 'deny by default' type requirements can by universally applied…". This sort of language, while useful, should more properly be included in the requirements. The SDT should make very (very) clear the intent of the Guidelines and Technical Basis section of the standards, and the expectations of the entity - and of the compliance enforcement authority – on how this information should be used.
No
We recommend that "where technically feasible" qualifiers be added to Parts 2.1, 2.2, and 2.3.
Yes
No
How does an entity demonstrate compliance to Part 1.1 if CIP-002-5 does not require that entities document their Low Impact cyber assets? Please revise the Measures section to provide clear guidance on recommended artifacts for compliance that do not pre-suppose lists of Low Impact cyber assets. Retention requirements for Part 1.6 are not made clear. Perhaps it was intentionally left

undefined by the SDT? If this is true, should the entity therefore assume they will need to retain three years of Logs per the Evidence Retention portion of the standard?
No
Retention requirements for Part 2.2 are not made clear. Perhaps it was intentionally left undefined by the SDT? If this is true, should the entity therefore assume they will need to retain three years of Logs per the Evidence Retention portion of the standard?
Yes
Yes
No
For Part 1.1, SDT should acknowledge the use of dynamic ports/ranges used by a wide variety of cyber systems. The documentation requirement seems a bit redundant to the configuration management documentation requirements of CIP-010-1-R1.1.
No
For Part 2.1, suggest the language be rewritten as “Identify and implement a process to monitor for the release of security patches…” As it’s currently written, “identifying sources” might be interpreted as writing down a bunch of third-party URL’s that may change without warning. Recommend revising Part 2.2 to say “Identify applicable security-related patches or security-related updates…” As written, a person could interpret “updates” to mean security-related or not. The words “…that addresses the vulnerabilities within a defined timeframe” should be separated from the end of the sentence and rewritten as its own sentence for clarity. Part 2.3 is not clear on what is actually required. The requirement talks about a process, yet the Measures suggest evidence that the remediation took place. Should Part 2.3 say “Execute the remediation plan documented in Part 2.2”?
No
For Part 3.5, need to add “where technically feasible” qualifier here. If we serial-connect a laptop into a router or a relay, the device may not be capable of detecting and logging that connection. The Change Rationale for Parts 3.4 and 3.5 mention the term “ESP”. Beyond just that typo, the definition of Transient Cyber Asset implies that this requirement only applies when such devices are directly connected to other BES Cyber Assets, not the “ESP” itself. In the Guidelines section under Requirement R3, the second paragraph states “…the entity must specify how those updates are tested”. Yet, there is no specific requirement for malware signature testing in R3 of the standard.
No
Parts 4.1, 4.2, and 4.3 are concerning in that no accommodation for “where technically feasible” is mentioned. Yet, the last paragraph on Page 41 – the Guidelines section – states that the SDT does not intend for TFE’s to be required. Does the Guidelines section carry any weight when an entity is being held to the letter of the standard? Or are the Guidelines to be read as part of the Standard? For Part 4.4, please clarify the contradictory requirements for 90-day log retention versus the three-year evidence retention specified in Part C Section 1.2 of the Standard (page 32). The Measures for Part 4.4 are a good start, but “records of disposition” is too vague.
No
This is a bit nit-picky, but Part 5.1 could be wrongly interpreted as “Show me your driver’s license before I provision an account for you on the BES Cyber System”. Recommend using language similar to CIP-006-5-R1.2 “Utilize at least one electronic access control that restricts access to only those individuals that are authorized”. Part 5.2 implies, but does not state, that a signed and approved list of delegates is required. Please clarify. Also, this requirement talks about the “use of” shared accounts. This could be interpreted as either the initial creation of, or day to day use of, those ID’s. We believe the SDT meant the former, but we request that you please clarify. Parts 5.2 and 5.3 imply, but do not explicitly state, that there must be a procedure to authorize individuals having access to shared/administrative accounts. Please clarify. For Part 5.4, please simplify by stating “Procedural controls for initially changing default passwords, where technically feasible”. All the rest can be stricken, and the asset types moved to the Applicability column.
Yes

No
For Part 1.2, need to have a cross-reference to the applicable EOP standard and requirement.
No
Part 2.1 the words "…when incidents occur" is redundant. The requirement is a bit contradictory in that the incident response plans MUST be used, yet deviations allowed. (emphasis mine). Recommend rewording this requirement to say "When a suspected BES Cyber Security Incident occurs, the incident response plans shall be executed. Should deviations from the plan be necessary, those shall be documented for later review". Part 2.2 should state simply "Test the BES Cyber Security Incident Response Plan at least once every calendar year", and include the three bullets.
No
The Change Description field mentions "DHS Controls". What are these? Also, due to the complexity of the testing and review of the BES Cyber Security incident response plans, recommend including a timeline/graphic in the Guidelines section to visually demonstrate the lifecycle of the plan.
Yes
No
General question about the scope of CIP-009 that has never been addressed – is the intent of the standard the recovery of the function of an asset or system, or the recovery of the actual asset itself? This would be a good opportunity to clarify. For Part 1.4, what does "verified initially" mean? Each time the backup runs, or the first time after the asset was commissioned? (Could be years ago). If the latter, evidence retention might be an issue for long-life assets.
No
Part 2.1 should state simply "Test the Recovery Plans at least once every calendar year", and include the three bullets. It also needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. For Part 2.2, the same question on scope applies. The language needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. Need to also allow for the fact that not all cyber assets can be "backed up" in a traditional IT sense. For Part 2.3, it was commented earlier, but an operational exercise "initially upon the effective date of the standard" will make for an exciting day on the North American bulk power system. Please remove all instances of such language from all the standards, and make this part of the implementation plan and allow for staggered and entity defined rollouts.
Yes
Yes
No
For Part 1.1.4, the word "scripts" is too generic and thereby problematic. Scripts that are used for key functionality of the system would make sense to include in the baseline, but scripts for administration, backups, maintenance or troubleshooting, for instance, may be too dynamic by nature to be included in the baseline. Please either clarify, or strike, the words "and scripts". For Parts 1.1 and 1.2 there is a potential problem with dynamic port ranges. Perhaps sub-Part 1.1.5 could be written as "Any static logical network accessible ports". Part 1.2 seems to imply that the CIP Senior Manager must approve a list of delegates who have the authority to authorize changes. If this was the intent, please add a specific requirement.
No
Requirement R2 needs a lot of work and justification. Perhaps unintentionally, this requirement as written will result in another massive filing of TFE's, since I can't install Tripwire on my Router. While the purpose of the requirement is well-intentioned, with good reference to best practices, the application doesn't work outside traditional IT server-based cyber assets. This is a net-new requirement within CIP that, if retained, will require major initial and ongoing investment by entities for little reliability benefit. We recommend striking R2, or vastly limiting its scope (Server-type assets at Control Centers, for instance).
No

For Part 3.2, please clarify whether all cyber assets need to be included in the assessment, or a subset, or representative sampling, or entity defined. There are certain cyber asset categories where “test” systems just aren’t economically feasible. What is the acceptable deviation between test and production the auditors will allow? As written, and without explicit language in the requirement, our entity fears this will be a topic of a CAN later. For Part 3.3, please clarify whether “new Cyber Asset” means literally that or, more reasonably, could mean “new Cyber Asset category” or a new make/model, or a new function. It would be reasonable to test something that brings net-new functionality to a BES Cyber System, but if when replacing an end-of-life or failed component, it wouldn’t make sense.
Yes
Yes
No
For Part 2.1, please add language that allows for re-use or redeployment within a similar BES Cyber System.
Yes
No
The SDT should modify the Implementation plan to identify requirements that are net-new (like CIP-010-1-R2) and might require capital investment, and provide an additional 12 months to implement. The justification being the reality of capital/budgeting cycles within an organization. Depending on the timing of the regulatory approval, it may be twelve months before capital can be obtained, thus leaving three calendar quarters to design, test, and implement these technologies to meet the “seven calendar quarters” implementation date. Secondly, every instance in the standards where “initially upon the effective date of the standard” is written needs to be removed from the standard and added to the Implementation Plan. For each of those specific requirements, a staggered table should be developed that allows entities the flexibility to perform their first iterations of cyclical events in a phased manner.
Individual
Michael Falvo
Independent Electricity System Operator
Yes
We are concerned with the exclusion of the “Intermediate Device” from the definition of “Interactive Remote Access”. As specified in the definition of “Intermediate Device”, this “Intermediate Device” can be located outside the ESP, and by excluding the this device from the interactive remote access rules defined in CIP-005-5, part 2.1 through 2.3, we feel that this may be a weakness that may opens up the danger of opening up potential, unprotected path to BES Cyber Assets.
Yes
1. IROLs may be based on dynamic system phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response. We suggest an additional criterion that captures this important impact: ‘Generation Facilities at a single station that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies’ 2. Currently our risk-based methodology includes a criterion to protect transmission stations that act as data hubs critical for monitoring and control of the BES. There appears to be no criterion in CIP-002-5 that recognizes this critical role. We suggest an additional criterion (similar to CIP-002-3 R1.2.7) in the Medium category to capture these self-identified impacts: ‘Any additional facilities that support BES Reliability Operating Services that the Responsible Entity deems appropriate.’
Yes
Yes

Yes
Yes
We are agreeing with this proposal; however, we feel that defining NERC senior manager to a role rather than to an individual may be more practical, especially when personnel changes are more frequent.
Yes
We agree that organizations shall have security policies to cover all of those elements described from 1.1 to 1.10 under R2 of this standard. However, we want clarification on the term “policy” that does not necessarily have to be represented or tied up with a “policy” documents, but should also includes other type of governing documents, such as “security standard” type of enforcement document that an organization already accustomed to.
Yes
Yes
Yes
Yes
Yes
We agree to all VRFs, except for the “medium” VRF proposal for R2. We suggest this should be a “high” VRF, because the security policy is the main driver from and the means from top level authority of the organization to enforce overall security and without one the overall security posture will not follow through, including the NERC standard requirements outlined.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Part 2.2 specifies that “Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session”. We feel that for clarity, the encryption termination point must be specified with this rule. We suggest the following language for the rule: “Require encryption for all Interactive Remote Access sessions, terminated at the intermediary device, to protect the confidentiality and integrity of each Interactive Remote Access session”.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
"Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1." This could require TFEs in a very ad-hoq manner. For example if data could not be preserved due to the nature of the technical damage (level or nature of coruption) of the media, this requirement would force the entity to file for a TFE because it was not techincally feasable to preserve the data. We suggest that this would not be a practical or effective use of TFEs. We suggest that the wording "where technically feasible" be replaced with "to the extent possible". We believe this would allow for situations where it is not possible to preserve the data without having to invoke a TFE for every instance that this occurs.
Yes
R2.3 states in part: "Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard,". We suggest that this would be impossible to test each plan on the recovery date. We suggest that the wording be revised: "Test each of the recovery plans referenced in Requirement R1, initially within 12 calendar months of the effective date of the standard,"
Yes
Yes
Yes
Yes

We suggest that the wording of “technically feasible” should not be included in R2, part 2.1 as this term is contradicting with R1, part 1.1 as the baseline configuration should already been created as required by this requirement.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Rodney Luck
Los Angeles Department of Water and Power
Yes
In Section "1. High Impact Rating (H)" of Attachment 1, the phrase in the first paragraph "within 15 minutes adversly impact..." is vague. More guidance and clarity are needed on how to determine adverse impacts.
No
R3.2 defines "annual" training as being completed within 15 months. This is a change from the NERC current definition as described in CAN-0010. Entities need more leeway in being able to define "annual" training and other "annual" requirements. It is extremely difficult to track and manage training of thousands of employees based on a 15 month time frame. Entities need to be allowed to complete training over an entire calendar year.
No
The time limits for revoking access upon terminations and transfers being proposed for the next calendar day present extreme challenges. More time needs to be given - the next calendar day for terminations and 72 hours for transfers to make these processes manageable.

No
R1.1 defines operational or procedures controls to restrict physical access to Low Impact BES Cyber Systems. Need to remove applicability of this requirement for Low Impact BES Cyber Systems. Existing Standard Operating Procedures address and restrict physical access to Low Impact BES Cyber Systems. Demonstration of existing procedures should be sufficient to meet the intent of this requirement. R1.3 requires utilization of two or more different and complementary physical access controls. This presents technical challenges and may not create additional security. One control is preferred. Depth of defense already exits through gates, security personnel and card reader systems. The current requirement of one or more physical access methods has been implemented with little or no problems encountered. The increase to two or more physical access controls may bring about unintended consequences and complexity. NERC should provide compliance feedback to the industry demonstrating that the one or more physical access methods have been ineffective. Additionally, High Impact Control Center typically emply stringent physical security controls and monitoring. In addition, the language under Measures in R1.3 describes how ingress and egress are controlled by one or more different methods. The requirement for egress has not been explicitly defined as a requirement. Preference is for ingress only. Egress requirement has been alluded to in the language stated in the Measure. Access controls for egress present a number of safety issues and concerns. R1.6 does not address access log retention. Preferenece is to maintain a log retention of ninety calendar days. A log retention of ninety calendar days maintains status status quo as far as log retention.
No
R3.1 requires maintenance and testing every 24 months. We prefer a maintenance and testing cycle to be no longer than three years. Equipment failure rates do not support the need for maintenance and testing every two years. Manufacturer Mean time before failure rates are in excess of three years. We believe maintaining the three year cycle is reasonable and effective. Additionally, equipment is monitored and malfunctions are reported immediately thus negating the need for a two year maintenance and test cycle.
No
R1.2 requires to "disable" unused physical ports. Given the age of some equipment, this may not be technically feasible and there are no provisions for exceptions. There is a designation for "signage" being acceptable. What is meant by "signage"? There needs some exception for physical ports that can not be disabled.
No
R4.5 The requirement that the time frame of documenting a response to rectify before the end of the next calendar day presents a very short time frame to come up with a way to rectify an issue that may require extended investigation. 30 days is preferred.
No
In R5.1, it is not clear if alternatives to password authentication can be used. There are many new forms of technology for validating credentials before granting electronic access such as biometrics, IRS scans, finger print scans, etc.
No
R2.3 states "test each of the recovery plans... through an operational exercise." The requirement

needs to allow for recovery plans which are representative of similar or like Applicable Cyber Assets which would achieve the same goal as individually testing each recovery plan. Excessive operational exercises when numerious recovery plans are available may potentially disrupt operations.
No
R3.3 states that prior to adding a new Cyber Asset to a BES Cyber System, the entity is to perform an active vulnerability assessment of the cyber asset. It is problematic to perform an active vulnerability assessment prior to installing a new Cyber Asset. "Active vulnerability assessment" is not defined. There are sufficient controls in place that any "active vulnerability assessment" would be unnecessary.
Individual
Jack Stamper
Public Utility District No. 1 of Clark County
Yes
The SDT should consider the following changes to the defined terms. BES Cyber System - One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. BES Cyber System Impact – Need definition. CIP Senior Manager - A single senior management official with overall authority and responsibility for leading and managing implementation of the requirements within the NERC CIP-002 – CIP-011 Standards.
Yes
The impact rating of control centers needs to be tied in with the facilities controlled by the control center. CIP-002-5 -Attachment I attempts to classify all Transmission Owner, Transmission Operator, and Generator Operator control centers as either High Impact or Medium Impact. There is a slight exception offered for Generator Operator control centers only. The SDT has for the most part adopted the Version 4 criteria; however, Version 4 was intended to identify an entity's facilities as either "critical or not critical." It is unreasonable that a control center determined to be "not critical" under Version 4 is then determined to have a Medium Impact Rating in Version 5. Yet this is exactly what criteria 2.13 will do. The SDT has attempted to lessen the harshness for generator control centers by adding a limit of 300 MW but has not provided any such "ceiling" for transmission control centers. The STD needs to be made aware that there are some Transmission Operators and Transmission Owners that operate small systems that have no practical impact on the reliability of the BES. Some of these utilities operate systems from dispatch centers that meet the definition of Control Center in CIP-002-5. Many of these entities have no real-time balancing capabilities and no frequency or voltage control (other than notifying the Balancing Authority in the event of an alarm). Also with no blackstart generation or cranking paths, system restoration consists of clearing of loads from distribution busses and then the re-establishment of load upon the restoration of the transmission system voltage by the Balancing Authority. If a utility has only electric facilities that have a Low Impact Rating, it is reasonable to expect that the center used to control these facilities would also have a Low Impact Rating. A similar argument can be made for control centers that control Medium Impact Rating electric facilities and High Impact Rating electric facilities. The SDT should further develop the criterion so that a reasonable boundary exists between the High and Medium Impact Rating and between the Medium and Low Impact Rating. Control centers should be rated based on the facilities controlled.
No
The SDT uses a number of different calendar days for reporting throughout the CIP standards. Clark recommends one consistent time of 90 calendar days.

No

The SDT uses a number of different calendar days for reporting throughout the CIP standards. Clark recommends one consistent time of 90 calendar days.

Individual
Paul Crosby
Platte River Power Authority
No
Yes
Attachment I, Criterion 2.13 – It's not clear if the term "generation control centers" is referring to: • control centers local to generation, • centralized control centers controlling multiple geographically disparate generation resources, • or both
No
Please consider revising Requirement 1 as follows: R1. Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its BES Cyber Assets and BES Cyber Systems as High or Medium Impact according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems not categorized as High or Medium Impact shall be deemed to be Low Impact and do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning]
Yes
Yes
Yes
Yes
No
We feel that Requirement 4 is training and should be moved to CIP-004-5 Requirement 3.
Yes
Yes
Yes
No
We feel that the term "security controls" in R2, Part 2.2 is broad and overlaps with R2, Part 2.4 "electronic access controls". We suggest either combining Part 2.2 and 2.4 or separating them into specific types of access controls, such as: • Electronic access controls • Physical access controls • Remote electronic access controls • Etc.
No
Since R3, Part 3.1 and 3.2 both reference and are related to R2 we suggest combining Requirements 3 and 2. The way they're written it's odd that the role-based program does not address completing training prior to access authorization nor requiring training updates once a year.
No
As written the Requirements don't require that the personnel risk assessment include a seven year criminal history check. The Measures do but not the Requirement. Should it?
No
As written the Requirements don't require that the personnel risk assessment include a seven year criminal history check. The Measures do but not the Requirement. Should it? R5 references and relates to R4 we suggest combining Requirements 4 and 5. The way they're written it's odd that the personnel risk assessment (PRA) program does not address completing the PRA prior to access

authorization nor requiring updates every seven years.
Yes
Yes
No
Part 1.2 states “Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs)”. The Measures for 1.2 do not address the demonstration of “control and secure”, only the identification of EAPs. Perhaps 1.2 should only address the use and identification of EAPs while Parts 1.3 addresses “control and secure”. Additionally, the requirement doesn’t specifically require the protection of a BES Cyber System. “Control and secure all routable and dial-up connectivity” to…? We suggest revising the language for Part 1.1 as followings, “Identify Electronic Access Points (EAPs) used to control and secure all routable and dial-up connectivity to applicable BES Cyber Systems.” Part 1.3, the term “access permissions” is unclear. We suggest revising the term to match the language in Part 1.2 using “access controls” instead. Part 1.4 still uses the term “where technically feasible.” We were under the impression that the drafting team was going to do away with TFEs.
No
CIP-005-2 Table R2 is labeled “Remote Access Management”. All the Parts contained within deal specifically with “interactive” access. We suggest renaming the table to “Remote Interactive Access Management”.
No
Part 1.4 states “Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.” We don’t believe it’s possible to issue real-time alerts for successful but unauthorized physical access. The system cannot distinguish between an unauthorized person using valid credentials and an authorized person using valid credentials. We suggest revising the requirement as follows, “Issue real-time alerts (to individuals responsible for response) in response to failed physical access attempts at any access point in a Defined Physical Boundary or to physical access control system alarms. Part 1.5 - Please see previous comment.
Yes
Yes
No
Part 1.1 – We are assuming this applies to the Asset level although it’s not clear. The applicability is defined per “BES Cyber System”, “Access Control System”, or “Associated Protected Cyber Asset”. We suggest revising as follows: “Disable or restrict access to unnecessary BES Cyber Asset logical network accessible ports and document the need for any remaining logical network accessible ports.”
No
Part 2.2 – The requirement isn’t written clearly. We suggest revising as follows “Assess security-related patches or updates for applicability within 30 days of release from the identified source and create a remediation plan, or revise an existing remediation plan that addresses the vulnerabilities within a defined timeframe.”
No
Part 3.1 & 3.4 – We feel the word “or” makes the Requirement unclear. Are we to deter or detect or prevent malicious code? Or are we to deploy method to do all or a combination of the three. We suggest replacing “or” with “and” or “and/or”.
No
Part 4.1.4 states “Any detected potential malicious activity.” Is this code for “all activity”? Isn’t all

activity “potentially” malicious? We suggest removing the word “potential” from 4.1.4.
No
Part 5.1 – It’s unclear in the requirement whose credentials require validation. We suggest rewording as follows, “Validate user credentials before granting electronic access to each BES Cyber System. “ Part 5.2 and 5.3 deal with access authorization and identification. We suggest moving them to CIP-004-5 R6. Part 5.5.3 – Changing passwords based on an “entity-specified time frame” may lead to questions around time frame adequacy. We suggest specifying a minimum time frame and allowing the entity to shorten as needed. For example use “Change annually or more often as needed”.
Yes
No
Part 2.1 – Please consider revising as follows, “The incident response plans must be used when BES Cyber Security incidents occur and include recording of deviations taken from the plan during the incident or test.
Yes
Yes
No
Part 2.2 – We feel the phrase “reflects current configurations” is unrelated to testing if the information is usable. We think the test is valid and should be moved to Part 2.3.
Yes
Yes
Yes
No
Part 3.1 – We feel the reference to “security controls” is unclear. We ask that the drafting team list the minimum set of Requirements that require assessment.
Yes
Yes
Yes
Individual
Nathan Smith
Southern California Edison
Yes
-BES Cyber Security Incident An attempt to compromise an electronic access control system is not included in this definition and should be. -BES Cyber System Maintenance Cyber Asset should be rephrased to say Transient Cyber Asset. Also, as it is currently worded, the means by which the clustering of BES Cyber Assets into BES Cyber Systems is to be done is not clear. -BES Cyber System Information The definition does not address information artifacts where BES Cyber Systems or BES Cyber Assets are depicted but not marked as such. For instance a substation network diagram

showing relays not specially marked as BES CA or BES CS could be classified as not being a BES Cyber System Information artifact since an uninformed user of that information would not be able to distinguish them as such. -BES Reliability Operating Services The term is too broadly defined. There are many systems involved in distribution that would not degrade the BES if they malfunctioned, but none the less are programed to respond to changes on the BES. The suggested improvement is to specifically note that distribution assets are not in scope. -Should all of the BES services be in scope? Order 706 did not order controls on all BES services. -Control Center There is no verbiage to clarify geographically dispersed centers. -Electronic Access point ("EAP") Based on how this term is defined a Level 2 switch is not considered an access point. An EAP should be defined such that it is required only for devices that are accessible by dial-up or routable channels. -Cyber Systems Please provide a definition for Cyber Systems -Defined Physical Boundary This concept is an improvement over the current 'Physical Security Perimeter', is expected to increase security of the BES, and provides more flexibility for compliance. -Electronic Security Perimeter ("ESP") The definition should state that ESPs are valid only for dial up accessible or routable access points. For instance a fully serial HMI cannot be provided with an ESP because there is no access point other than the device itself. -Intermediate Device Does the word "and" just before (3) imply that an intermediate device has to meet all three of the noted criteria? -Reportable BES Cyber Security Incident Please clarify what the term "compromised" could mean, or elaborate on what a "compromised" system looks like. -Reportable BES Cyber Security Incident The compromise of an ESP without an appreciable loss in BES Reliability Operating Services capability would not be reportable based on this definition. It is not in line with the requirements of Order 706. For further suggestions regarding Definitions see comments provided by EEI
Yes
SCE provides these specifc comments for the SDT's consideration. For further suggestions regarding CIP 002 see comments provided by EEI. Attachment I Paragraph 2.5 Please clarify the requirements for the Cranking Path. The third graph on page 26 of 30 seems incorrect. Paragraph 2.12 What is the phrase "without human intervention" mean? The subject of the paragraph is automated load shedding. Could the intent of the paragraph be to identify automated load shedding systems that start load shedding without human intervention or could the intent of the paragraph be to identify automated load shedding systems to continue to shed load once initiated by a human? This requirement assumes that the entity already knows which Cyber assets are BES Cyber assets / BES Cyber systems and which are not based on the impact categorization prior to the application of the methodology. There is no requirement that entities first collect a candidate list that is then subject to the criteria listed in CIP 002. High Impact – A data acquisition node or protection relay that is essential to for monitoring or control functions performed by an EMS which are located at a BES facility that is not a control center would result in the BES facility housing such a node or relay being classified as a control center. Suggest including this sentence: A data acquisition node or protection relay that is essential for monitoring or control functions performed by an EMS which are located at a BES facility that is not a control center do not result in the BES facility housing such a node or relay being classified as a control center.
No
002-R1 Suggest adding this sentence to the end of R1: Justification of Low Impact BES Cyber Assets is not required. If a Low Impact BES Cyber Asset is not identified discretely is there a need to justify why it is not considered a High or Medium Impact BES Cyber Asset? R1.1 uses the word "intended to be in service". This does not account for scenarios where a system or facility is not intended to be in service for more than 6 months but due to planned or unplanned outage days, the total period where the system or facility is connected is greater than 6 months (although it was not actually in service for the entire period). For instance a pilot project that is intended for a 6 month test period is removed from service for 30 days for modifications, and the pilot project is run for 7 months to "make up" for the lost 30 days of testing would be considered in scope per this requirement.
No
002 R2 "Upon the effective date" should be restated to read "on or (within 30 days) prior to. A list of Low impact BES facilities is not required to be maintained, however, certain standards require controls to be enforced at these facilities. At the very minimum, the standard should require that the RE's approval of High and Medium lists should include a list of facilities and systems considered as potential candidates for the evaluation.
No

For suggestions regarding CIP 002-5 Violation Risk Factors and Violation Severity Levels see comments provided by EEI.
Yes
For suggestions regarding CIP 003 R1 see comments provided by EEI
Yes
For suggestions regarding CIP 003 R2 see comments provided by EEI
Yes
For suggestions regarding CIP 003 R3 see comments provided by EEI
Yes
CIP 003-5 R4 What does it mean for employees and contractors to “have access to BES Cyber Systems”? Is the intent here to indicate the employee or contractor has control over the asset? Suggest revising the sentence to say “Each responsible entity shall make individuals with control over BES Cyber Systems aware of elements…”
Yes
For suggestions regarding CIP 003-5 R5 see comments provided by EEI
Yes
For suggestions regarding CIP 003-5 R6 see comments provided by EEI.
Yes
For suggestions regarding CIP 003-5 Violation Risk Factors and Violation Severity Levels see comments provided by EEI.
No
For further suggestions regarding CIP-004-5 R1 see comments provided by EEI
No
For further suggestions regarding CIP-004-5 R2 see comments provided by EEI
No
For further suggestions regarding CIP-004-5 R3 see comments provided by EEI
No
SCE provides these specifc comments for the SDT’s consideration. For further suggestions regarding CIP 004-5 see comments provided by EEI R4.1 – Suggest current PRA’s already in place be grandfathered, such that those with a PRA need not meet the new requirements for the PRA until the initial one expires. R4.2 – Suggest providing flexibility not to cover the full scope of the PRA for those that are in states that impose limits on how much personal information can be assessed. Retention of records of 7 year background checks is not clearly stated. Also there is no consideration of existing background checks under NERC CIP standards that are currently in effect. Can a PRA under the current CIP requirements be used to validate R4.2 under Version 5? R4.3 The application guideline provides guidance where it is ‘not possible to perform a full seven year criminal history check.’ How is ‘not possible’ measured? Propose a clearer delineation to frame instances in which personal records are not readily available – vs. impossible to obtain.
No
For suggestions regarding CIP-004-5 R5 see comments provided by EEI
No
CIP 004-5 R6 Propose use of ‘legacy’ language where access is appropriate for the roles and responsibility over ‘minimum necessary’
No
CIP-004-5 R7 R7.1. Suggest requiring access be revoked within 24 hours, or “as soon as possible”. “At the time of termination or resignation” is vague and difficult to define. R7.5. Some Medium Impact assets that are programmable and have shared passwords are deployed in the field and have no network connectivity. Given these assets are distributed in a wide geographical area, many in difficult to reach places, it is not technically feasible to get to all the distributed assets and change their passwords within 30 calendar days; especially assets that are in or near hydro facilitates. Suggest modifying the standard to exclude medium impact assets in the Applicability section. R7.1 - There are questions in instances where resignations and/or terminations may be retroactive, which would

introduce a challenge with revocation 'at the time of' events. R7.3 – Propose use of 'approved BES Cyber System Information repositories,' to frame an appropriate location in which information can be managed and controlled. Access revocation to protected information repositories is enforceable but revocation to hardcopies is difficult to prove. A control that acknowledges the difficulty of proving that access to hardcopies (Especially those in the possession of the person, not just those documents that are located in a locked cabinet or other storage areas) has been revoked should be added. A sign off form is an acceptable measure but not within the timeframe suggested. An outside limit of what is considered "at time of" should be provided. Language such as "access revocation should be completed within 24 hours" can be used.
No
Violation Risk Factors and Violation Severity Levels for CIP-004-5 Across all VSLs there is no consideration for the impact level of a particular violation. The Lower and Moderate VSL's should be made applicable to Medium Impact BES Cyber systems and their associated Cyber assets. For instance if a role is such that access is provisioned only to associated cyber assets and not to High or Medium or those assets deployed for protection, the violation should be a Lower or Medium VSL. R1, R2, R6 – Scale VSLs appropriately. R3, R7 - <1% of individuals for Medium Impact and associated cyber assets should be Lower VSL, 1-5% for Medium Impact and associated cyber assets should be moderate, 5-10% of any applicable BES cyber asset should be high, and any number greater than 10% of any applicable BES Cyber asset can be treated as severe.
Yes
SCE provides these specific comments for the SDT's consideration. For further suggestions regarding CIP 005-5 see comments provided by EEI R1.1 Should the measures read "documented technical or procedural controls that exist…" in order to match the requirement? Please confirm the Low Impact assets do not have to be protected by an Electronic Access Point? R1.3 Although security wise this requirement adds protections, explicit outbound access permissions places a load on processors that slows down the computing capability, and therefore may make the grid operate slower. Please be aware of the trade-offs. R1.5 This requirement is dictating the need for an intrusion detection system at all High Impact and Medium Impact Electronic Access Points (with external routable connectivity at control centers). This is a high cost investment for industry to make in a short period of time,, and may not be accomplishable for field deployed programmable assets. Are the measures aligned with the requirement here, since the Requirement requires a method but the measures point to a system or systems? Please define "malicious communications"
Yes
For suggestions regarding CIP-005-5 R2 see comments provided by EEI
Yes
Violation Risk Factors and Violation Severity Levels for CIP-005-5 R1 – R1.1 A procedural or technical control for a low impact system should be scaled in and not bundled with violations for high of medium impact systems. Proposed change could state that a violation of R1.1 for <5% of low impact is moderate, greater than 5% is High and not a severe VSL for Low impact.
Yes
SCE provides these specific comments for the SDT's consideration. For further suggestions regarding CIP 006 see comments provided by EEI R1.1 Suggest stating whether or not there is a requirement to implement the operational or procedural controls. R1.4. Suggest clarifying that issuing real time alerts for events at Medium Impact assets does not include pole top devices.
Yes
For further suggestions regarding CIP-006-5 R2 see comments provided by EEI
Yes
For suggestions regarding CIP 006 -5 R3 see comments provided by EEI
Yes
For further suggestions regarding CIP 006 Violation Risk Factors and Violation Severity Levels see comments provided by EEI
No
SCE provides these specific comments for the SDT's consideration. For further suggestions regarding CIP 007 see comments provided by EEI R1.1 Suggest revising the requirement to provide an

exception related to dynamic ports and the inability to disable them. If a dynamic port is closed, the service that is needed by the BES system may not be available. Furthermore, it is not always known which ports and services vendors are using. R1.2 Restricting the use of physical USB ports may not be accomplishable. There are so many devices with physical ports it is impossible to monitor each one. In addition, because a USB port is in use by a mouse, and therefore not required to have access restricted to it, someone could easily remove the mouse from the USB port and install malicious software. This requirement creates a huge burden and is easily circumvented.
No
CIP 007-5 R2.1 Suggest revising the standard to say “security updates”, not just “updates”. R2.2 Suggest revising the requirement to allow for 30 days to identify applicable security updates or patches and 30 days to draft a remediation plan. R2.3 This requirement is not clear and does not match the measures. Please revise it. A TFE option for unsupported devices should be added. Also the standard does not specify a timeline within which a remediation should be completed or a scheduled review of the status of the remediation plan.
No
CIP 007-5 R3.2 Suggest revising the requirement to include quarantine of the malicious code. R3.4 Should this standard be applicable to Transient Cyber Assists? If so it should stated in the “Applicability Column” R3.1 and R3.2 Should allow for applicability at the system level or on a per asset level. Whitelisting of applications could be stated as a requirement rather than a measure. The requirement thus stated would add to the robustness of documenting BES Cyber Systems since the hardware of a “cyber system” cannot conceivably perform any functions without some onboard software. The standard language as currently stated seems to apply to the hardware and deviates from Order 706.
No
CIP 007-5 R4.1.4 Please define “Malicious Activity” R4.5 Reviewing logged events every two weeks is burdensome and can be expensive to automate, and there is little improvement in BES security from this activity. Please consider re-thinking this requirement. A TFE option should be provided within this requirement since devices that do not support functions as listed. The language of the standard assumes automated logging for each BES Cyber Asset.
No
CIP 007-5 R5.4 Should the applicability here be noted as High Impact and Medium Impact assets?
No
CIP 007-5 R1 – Moderate or High VSL for undocumented ports on Medium Impact Cyber assets. R2 – Moderate or High VSL for failure to identify source. Failure to identify source and failure to implement should not be treated the same way.
Yes
For suggestions regarding CIP 008-5 R1 see comments provided by EEI
Yes
SCE provides these specific comments for the SDT’s consideration. For further suggestions regarding CIP 008-5 see comments provided by EEI R2.1 Suggest removing consideration of a test from the requirement.
Yes
For suggestions regarding CIP 008-5 R3 see comments provided by EEI
Yes
CIP 008-5 R2 – Failure to annually test an IR plan should be a high VSL not severe. Failure to use a IR plan and failure to test an existing IR plan should be treated differently.
Yes
SCE provides these specific comments for the SDT’s consideration. For further suggestions regarding CIP 009 see comments provided by EEI R1.1 Should the standard note what conditions should apply to the recovery plans? If so what type of conditions should be planned for? R1.3 Suggest replacing the word “protection” with the word “handling” or please explain what is intended by the word “ protection”
Yes

CIP 009-5 R2.3 Are there suppose to be specific recovery plans that need to be in place and tested?
Yes
CIP 009-5 R3.2 Suggest adding “or recovery” after “exercise” R3.3 Suggest adding “completion of” before “review”
Yes
CIP 009-5 For suggestions regarding Violation Risk Factors and Violation Severity Levels for CIP-009-5 see comments provided by EEI
No
SCE provides these specific comments for the SDT’s consideration. For further suggestions regarding CIP 010 see comments provided by EEI R1. We recommend the CIP SDT consider removing physical location from Baseline Configuration in CIP010 R1, or replace it with logical location (logical placement within the control systems architecture.) • R1.1.1 requires Physical Location be part of a Baseline Configuration. In the Guidelines and Technical Basis, Physical Location is explained as follows: The physical location referred to in the baseline configuration is geographically where the BES Cyber Asset is located (e.g. Pine Valley Control Room, Generator X, Substation Y) and should be used to ensure that BES Cyber Systems receive the controls that are applicable to the environment in which the components are located (e.g. control center, transmission facility, generation facility). The underlined phrase seems to imply that controls are applicable to the environment in which the cyber assets are located, whereas Controls are required by CIP004, CIP005, and CIP006, by categorization of BES Cyber System, as required in CIP020. The Applicability Section of each requirement clearly requires the categorization of assets to be protected by the controls required by CIP040, CIP050, and CIP060, and not the Environment in which the assets reside. • CIP002 R1requires Responsible Entities to identify and categorize High and Medium Impact BES cyber asset and cyber system. Asset identification includes an asset inventory, or list(s) as described in CIP002 R1 M1. Asset Identification, per NIST SP800-128 titled "Guide for Security Focused Configuration Management of information Systems", includes an asset Inventory of systems and system components in which one of the data elements may include "phyiscal location (e.g., building/room number, see Page 27 of this document)". Both CIP002 M1 and NIST SP800-128 point to an asset inventory that should be kept, and includes Physical Location where the asset resides. • CIP002 R1.1 requires "Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities..." A change of physical location where the BES Elements resides would require an update to the Asset Inventory or list. If the physical location is changed such that the BES Elements and Facilities are now outside of the already established controls, these controls will need to be re-established to comply with CIP004, CIP005, and CIP006. • CIP010 1.1 Change Rationale includes the following text: The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. DHS Catalog for Control Systems Security Section 2.6.2.2 includes the following text: The baseline configuration provides information about a particular component’s makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component’s logical placement within the control system architecture. and The inventory of control system components includes information (e.g., manufacturer, type, serial number, version number, and location) that uniquely identifies each component. Section 2.6.2.2 makes a distinction between a Baseline Configuration and an (Asset) Inventory of control systems components, and location is part of the inventory. Given this distinction in DHS Catalog for Control Systems, location (physical) should not be required to be part of a baseline configuration in CIP010. R1.1 Developing a baseline configuration is a huge task and should probably only apply to High Impact assets. R1.2 Please re-word the requirement – the meaning is not clear.
No
CIP 010-1 R2.1 Detecting unauthorized changes is burdensome. If the process is automated then that puts another load on processors and slows down computing. Please consider re-thinking this requirement only making it applicable to High Impact assets, and exclude serial devices.
No
For suggestions regarding CIP 010-1 R3 see comments provided by EEI
No
For suggestions regarding CIP 010-1 Violation Risk Factors and Violation Severity Levels see comments provided by EEI

Yes
For further suggestions regarding CIP 011-1 R1 see comments provided by EEI
Yes
For further suggestions regarding CIP 011-1 R2 see comments provided by EEI
Yes
For further suggestions regarding CIP 011-1 Violation Risk Factors and Violation Severity Levels see comments provided by EEI
No
SCE provides these specific comments for the SDT's consideration. For further suggestions regarding Implementation Plan see comments provided by EEI Schedule should be revised from 18 months to 24 months given the breadth of the increase in scope under version 5.
Individual
Barry Lawson
National Rural Electric Cooperative Association (NRECA)
Yes
BES Cyber System Information Define "BES Cyber System Impact" as it is a capitalized term used in this definition and it is not currently defined. CIP Senior Manager Replace: "NERC CIP Standards" with "NERC CIP-002 – CIP-011 Standards." The CIP-001 Reliability Standard is not part of this set of standards and has not yet been approved for inclusion in EOP-004-2. This will give clarity to the limit of the definition. Control Center NRECA is concerned with the broadness of this definition. The SDT should consider the impact on small entities that will be drawn in by an overly broad definition of Control Center. In this definition the SDT uses the defined term: System Operators which from the NERC glossary is: "An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time." If the SDT's intent was to limit Control Centers to buildings that house a System Operator with 24/7 staffing and include BA, TOP, GOP and RC functions, then NRECA could support the definition (if other changes in our comments related to CIP-002-5 Appendix 1 are also satisfactorily addressed) and requests that the SDT make this limitation clear in the definition. If this is not the intent of the SDT then NRECA does not support the proposed definition of Control Center.
Yes
3. Purpose NRECA requests the SDT to use consistent language in this section. On line 2 the phrase "reliable operation of the BES" is used and on line 5 the phrase "reliability of the BES" is used. The same phrase should be used in both locations. 4. Applicability 4.1.2 Distribution Provider 4.1.6 Load-Serving Entity NRECA is concerned with the new inclusion of DPs in the version 5 standards and with the qualifiers proposed for LSE in the Applicability section. NRECA believes that inclusion of this broad group of DP entities will draw in many small entities with no BES operational capabilities or responsibilities and cause them to go through a paperwork drill of proving they either do not provide BES Reliability Operating Services or they do not have cyber assets associated with this equipment. NRECA recommends that the SDT develop a simple method for DPs and LSEs to prove "No Impact" and be clearly exempt from CIP-002-5 – CIP-011-5. Attachment 1 1. High Impact Rating On line 2 the word "adversely" is used. This term can mean many things to many parties. Please provide additional clarity so that auditors and responsible entities have a better understanding of its use. 1.2 Add the following text to the end of the current 1.2: "for generation equal or greater than an aggregate of 1500 MW in a single Interconnection." NRECA strongly recommends the SDT to make this revision in order to stay as close to the CIP-002-4 criteria and to minimize cost impacts on entities that do not have a significant impact on the BES. 1.3 NRECA strongly opposes including "Transmission Owner" in this provision. Inclusion of RC, BA and TOP are appropriate, but the TO function does not rise to this same level of responsibility. NRECA requests that the TO function be removed from this section. Including the TO function here will make it very difficult for NRECA to change its vote to "affirmative" in the next ballot. If this is not changed for the next ballot, NRECA will likely recommend that its members vote "negative" on CIP-002-5. 2. Medium Impact Rating On line 2 the word "adversely" is used. This term can mean many things to many parties. Please provide additional clarity so that auditors and responsible entities have a better understanding of its use. 2.13 NRECA recommends that the proposed 2.13 language be deleted and replaced with the following: "TOP and GOP Control Centers not included in High Impact Rating and controlling 1500 MW or greater

of load or generation." Making this change will appropriately assign these control centers to the "medium" level and others not captured in the "high" or "medium" levels will be captured in the "low" level. Add new 2.14 Add: "2.14. Control Centers, not previously included in High Impact Rating (H) or Medium Impact Rating (M), above, that perform the functional obligations of Balancing Authority, Transmission Operators or Transmission Owners, and that do not implement protected data connections with other Control Centers in a manner as to prevent themselves from being used as cyber-attack vectors into other Medium Impact or High Impact Rating Control Centers." Making this change will ensure that other appropriate Control centers will be categorized in either the Medium or Low level.
No
R1 Replace "30 calendar days" with "90 calendar days." The SDT uses a number of different calendar days for reporting throughout the CIP standards. NRECA recommends one consistent time of 90 calendar days.
No
R6 NRECA recommends changing "30 calendar days" to "90 calendar days" to be consistent throughout the CIP standards.
No
R4 On line 2 after "unescorted physical access" add "to BES Cyber Systems" to clarify what this requirement applies to. R4.2 Clarity is needed to understand if the phrase "six months or more" applies to the entire sentence or just to "attended school."
No
R5.2 The phrase "once every seven calendar years" may create confusion on exactly what it means. In order to minimize such confusion, please be more explicit on how often personnel risk assessments must be updated.
No
R6.4 The phrase "once each calendar quarter" could be interpreted to mean almost a 6 month time period. Please provide further clarification on what the phrase means so all parties understand its meaning. In addition, please provide clarification in this requirement on what the difference is between "provisioned" and "authorized."
No
R7.1 Footnote 2 does not help to clarify what "at the time" means. Please provide more explicit language in this requirement regarding what "at the time" means. It may be appropriate to treat resignations and termination differently. This requirement could allow access for a resignation to continue until the individual's employment ends. For terminations this requirement could require access to be disabled at the same time the individual is notified of termination. R7.2 Replace "by the end of the next calendar day" with "within 30 days." NRECA believes that this requirement is excessive when compared to the threat of cyber attack on the system by someone being transferred or reassigned for reasons other than disciplinary action. R7.5 In the second paragraph of this requirement the word "extenuating" is used and could be interpreted in many different ways. Please provide more explicit language so that all parties have a better understanding of what is meant here.
No

R1.1 and 1.2 In R1.1 the word “restrict” is used and in R1.2 the words “control and secure” are used in such a way that for auditing purposes these words could mean many different things to different parties. Please provide additional clarity in these requirements as to the meaning of these words to minimize confusion.
No
R2.2 The way this is currently written it leaves open interpretation concerning the extent of encryption required. NRECA believes that the data encryption requirement should only pertain to the portion of the data path that is transmitted over public networks. We are afraid if you have to provide data encryption from the specific cyber device on the critical network you would create overhead that could result in communications failures, software conflicts, and unnecessary latency. NRECA requests that this be clarified as requested to avoid auditor and registered entity confusion in demonstrating compliance.
No
R1 On line 1 after the words “physical security plans” insert “for BES Cyber Systems.” R1.4 and 1.5 More clarity is needed to better understand what is meant by the phrase “Issue real-time alerts.” Real-time related to what? The time of the unauthorized access? As currently written, this requirement appears to be unrealistic. Please modify this requirement to provide clarity regarding what is necessary to comply with this requirement. R1.6 The word “sufficient” in this requirement is very subjective. Please provide greater clarity as to what is required for compliance with this requirement.
No
R1.5.1. and 1.5.2. If an entity’s model includes differences between the test environment and the production environment, would that be a violation of R1.5.1.? NRECA requests clarification that this would not be a violation.
No
R3.2 If an entity’s model includes differences between the test environment and the production environment, would that be a violation of R3.2? NRECA requests clarification that this would not be a violation.
No
R1.3 NRECA requests clarification regarding whether “deficiencies identified during the assessment” are considered violations of the standard. NRECA believes these deficiencies should not be considered violations of the standard and asks the SDT to address this.

No
Implementation Plan: On page 1 in the “Compliance with Standards” section, the applicable functions are listed. NRECA requests that this be revised to match the “Applicability” sections of the CIP V5 standards which include qualifiers to a number of the functions.
Individual
William O Thompson
NIPSCO Northern Indiana Public Service Company
Yes
-BES Cyber Asset: NIPSCO requests that further clarification is needed for the phrase “unavailable, degraded, or misused.” Clarification is also requested in the phrase, “when required” in sentence one, because it is ambiguous and confusing and as it is applied to other CIP reliability standards proposed. In addition, NIPSCO does not know if there needs to be a 15 minute test to “verify” the impact of the BES? And if so, how would an entity show compliance? Furthermore, NIPSCO recommends removal of the second and third sentence, because they do not provide any clarity to the time frame stated above. In addition, the third sentence regarding redundancy appears to conflict with the first sentence, therefore it is recommended that the fourth sentence be removed. The last sentence regarding “transient cyber asset” be removed because it is considered not appropriate as a cyber asset. [NIPSCO recommends that these CIP reliability standards should not exist.] -BES Cyber Security Incident: NIPSCO requests further clarification on what is meant by an, “intent to disrupt” and an “intent to compromise” as it is applied to an event and how to show evidence of such intent. NIPSCO recommends to use either “compromises” or “confirmed attempt to disrupt,” to replace intent to disrupt and intent to compromise. In addition, NIPSCO requests that the word, “suspicious” be removed. If the phrase “suspicious” is not changed, NIPSCO requests the removal of the third bullet point be removed and how to show compliance. NIPSCO recommends that compromise and disrupt be included in the first and second bullet items and recommends removal of the third bullet point, because as it currently is written, this sentence creates a confilict with the visitor escort event, and recommends removal of the third bullet point. -BES Cyber System: “typically”? This doesn’t seem appropriate for a standard. NIPSCO recommends that this definition be eliminated, because the BES Cyber System definition is too similar to the BES Cyber Asset and creates further confusion between what is a System or an Asset. The classification of an item as a “system” or an “asset,” is a huge problem, because each entity could make up and classify whatever they want and be exempted from all. The entities should not be deciding what is required as a system as a whole and what is required for individuals. Furthermore the CIP is inconsistent of what is a BES Cyber System and what is a BES Cyber Asset throughout the proposed reliability standards. NIPSCO requests clarification and a definition of “Maintenance cyber” and how it is applied and show to show compliance or use “transient cyber” consistently throughout the CIP reliability standards. -BES Cyber System Information: NIPSCO requests further clarification on the phrases “security procedures” and “impact designations.” In addition, NIPSCO requests clarification that the listed items not be a complete list, but a partial list that is not exhaustive. The word “similar” is vague and request removal of the phrase “similar diagrams.” Furthermore, patch levels on the system needs to be defined and should not include “data in transit” and “data at rest.” In addition, further clarification needs to be made how it is applied and how to show compliance. Based on the scope of cyber assets included in CIP Version 5, the cyber information is over burdensome to the whole system. Since significantly more devices are identified in CIP Version 5, the information associated with those devices impose more items to meet CIP standards that are overly burdensome. -Is it BES Cyber System disaster or can it be BES Cyber System or Asset disaster…? -BES Reliability Operating Services: The use of the word “All”, is not appropriate within monitoring and control. The responsibilities listed in the operating services list are already defined in the NERC Glossary definition of terms and should not be included in the CIP reliability standards. The CIP committee does not have authority to create these definitions, because it incorrectly creates definitions, when the appropriate party to create these definitions is NERC. -CIP Exceptional Circumstance: It is unclear what is a “risk of injury or death,” and should be clarified. NIPSCO recommends to add the word “imminent” risk of injury or death. The term “exceptional circumstance” is provided as a NERC defined, however, this is inconsistent with the CIP standards, which allow entities to define what an exceptional circumstance is in their own policy. The CIP

standard should define what is an “emergency condition.” NIPSCO recommends to change the phrase from a “CIP Exceptional Circumstance” to a NERC standard to be used generally. -CIP Senior Manager – no comments -Control Center – NIPSCO requests clarification what is meant by a “BES facility” and a “control facility.” In addition, the definition of “control room” needs to be defined in order for the definition of “control center” can be better understood and defined. In addition, further clarification is requested as to what is meant by “two or more BES generation facilities or transmission facilities.” -Cyber Assets: NIPSCO requests what is the definition of “programmable” electronic device and what is included in such device. In addition, it is recommended that the word “data in those devices” be removed from the description. -Defined Physical Boundary (DPB): NIPSCO requests clarification of the phrase “physical border” and discuss what is appropriate to show DPB that meets compliance. It is also recommended that the change rationale be excluded from the DPB. -Electronic Access Control or Monitoring Systems: NIPSCO requests definitions of both “electronic access control” and “monitoring system,” because both of these terms seem to be the same thing and including both would be redundant. In the alternative, further explanation is requested as to how each of the control or monitoring systems are applied. Furthermore, the reference to the defined term, “Electronic access control” in CIP-006 appears to conflict with the Electronic Security definition here. Electronic Access Point (EAP): Could an internal switch be categorized as an electronic access point if it is restricting any type of traffic? NIPSCO requests further clarification as to what devices or items fall under restricted routable or dial-up data communications, therefore it is recommended to remove the word “restricts” from the description. As it currently is written, it assumes the routable or dial-up restricts access. Furthermore, NIPSCO requests whether the term interface on a cyber asset was meant to apply to local hosts. Finally, NIPSCO recommends that the language be changed to state, “a routable communication through an ESP.” -Electronic security perimeter (ESP): NIPSCO recommends that the description should not be scoped to BES cyber systems, but should apply to BES cyber assets. Would the ESP include the trusted and untrusted EAP’s? -External Connectivity: NIPSCO recommends that the description should not be scoped to just BES cyber assets, and should remove the word “BES,” from cyber asset. -External Routable Connectivity: NIPSCO requests that the term “cyber system” be changed to a “cyber asset,” and further clarification as to what is an external routable connectivity. As the statement currently reads, it appears to be more of a recommendation instead of a standard. In addition, the definition as it stands is unclear and provides little guidance as to its purpose in the CIP reliability standards and more explanation or discussion should be made to this definition. -Interactive Remote Access : NIPSCO requests elimination of “Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.” -Intermediate Device: Based on the external routable connectivity and external connectivity definitions, would this be sufficient if outside the ESP? NIPSCO requests clarification at “termination point” and whether it is meant to also include end points, such as a work station, and how and where it applies and how to show compliance. In addition, NIPSCO requests elimination of “Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more cyber assets. The intermediate device may be located outside the Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network.” -Physical Access Control System: NIPSCO requests further review of the description and recommends that the description should include a defined list of what is included in the defined physical boundary. -Protected Cyber Asset: No comment -Reportable BES Cyber Security Incident: No comment -Transient Cyber Asset: Is this 30 days consecutively or collective, need clarification. -Define directly connected (Is this meant to answer the roaming laptop scenario?) NIPSCO requests that the term “maintenance” be defined and explained. NIPSCO recommends to remove the phrase, “or introducing malicious code,” and change “cyber system” to “cyber assets.” It is also recommended to add, “Assets used in vulnerability assessment.” NIPSCO also requests clarification whether removable media is included as a transient cyber asset.

Yes

Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -How does an entity show that a System or Asset falls or does not fall with the 15 minute window? Would one need to show results that support that the asset/system can be down longer with no adverse effects to the BES? NIPSCO recommends that the CIP cyber assets clarify whether Attachment 1 applies to any BES that affects the BES or whether only a high risk or something that would critically affect the BES and classifies something as “high impact.” In addition, further clarification is requested whether Attachment 1 applies to high risk physical assets or high risk cyber assets. NIPSCO will have a better understanding of its position once the actual rules are

created.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -“Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.” What does that mean? R1 does not require discrete identification of Low Impact. Does this mean an entity does require a list of the low impact assets/systems? -In 1.1 define BES Elements and Facilities. NIPSCO states that generally that the CIP reliability standards should be made up of requirements and measures and should not be inclusive of application guidelines, rationale, and technical background.
No
Comments: -Should it not read delegate(s) instead of just delegate? There could be more than one delegate. -The measure makes no mention of the delegate(s) approval? Need consistency between the Requirement and the measure. -1.2 Evidence Retention: Please explain what “Other evidence” would be required.
No
Comments: NIPSCO recommends that the high VRFs and VSLs are extreme and the definition of what is high, medium, or low violations are unclear and need to be clearly defined in order to show how entities can fully comply. -No mention of BES Cyber Systems throughout the VRF/VSL, only mentions BES Cyber Assets. -R2: There is no mention of the delegate(s) completing the annual review. Delegate is called out in the requirement.
No
Comments: NIPSCO states that generally that the CIP reliability standards should be made up of requirements and measures and should not be inclusive of application guidelines, rationale, and technical background.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -The requirement states one may delegate by position, yet the measures make no reference to position as being the only thing being listed. Does the documentation need to be updated when personnel change but the title/position doesn’t?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Under the purpose, should it read, “...physical access to BES Cyber Assets OR BES Cyber Systems”, instead of “and”? -Rationale states all personnel, yet in the table R1.1 has applicability to “All Responsible Entities”.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Should this requirement include Cyber Assets as well as Cyber Systems?
No

Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Upon reading requirement 3.1 in the table, does it imply that all personnel who access the systems during a CIP Exceptional Circumstance require training after the fact? When reading the measures it appears that that is the case.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -With modifications to this standard, do current personnel with access have to undergo another background check, or will they be grandfathered in? -How are you going to audit to ensure it includes all the residency requirements? It will be difficult to be 100% sure of a “full seven year criminal check”. In addition, many schools are online now and how does an entity determine location from those? -Setting a hard line of when employee’s “fail” a PRA is difficult, as it may determine on what role the individual is performing. It might even be more difficult to have “fails” defined for each role within the organization. Could the registered entity have criteria that include HR using judgmental decision making? -Part 4.2 Requirements will need to negotiate with applicable unions and labor agreements.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. - 6.2, measure (i) introduces “sampling”, where is this defined and what would be acceptable “sampling”? -6.3 also includes the word “sampling”. -6.4 may be overly onerous on entities. Is a list of the exceptions sufficient to meet the measurement?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Provide more definition/clarification of “at the time of the resignation or termination” and what is the timeframe allowed in order to meet compliance. -The measures for Part 7.1 (i) measure seem unattainable. While terminated employees should be immediately removed from the system, or as the text suggestions, even “prior to”; this seems like a very high goal. For instance, if one is terminated and they walk off the site with their badge at 10:00pm on Saturday night. How is the evidence of removal going to be captured the date of the termination action? -R7.2 It seems unreasonable to revoke all unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day, next business day would be more appropriate. Most transfers usually involve employees having possible dual roles for numerous days/weeks, this could be problematic for those type of employees and employees transferred on Fridays/Saturdays. -R7.3 Calendar day instead of business day. Calendar day could pose problems for all sizes of entities. -R7.1, R7.2 and R7.3 Reasonable time is required to allow for inter-company communications. Recommendation for 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require access. -R7.5 Clarify “extenuating circumstances”. Is this something that can be critiqued by an auditor?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1 – Provide a more granular break out if you only forget one quarter. Maybe a moderate vsl? -R1.1- Why does R1.1 apply to low assets when R1 only applies to high risks. -R3 – Provide a more granular break out also, possibly by percentage of total employees. As listed an entity could get a high vsl for “one” individual missing their training or for “200” individuals missing it. -R7 – Companies may have 10,000 employees or 100. It seems unreasonable if you miss 1 employee it can move either way (moderate-high or high-moderate), should this not go by percentages?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1.5 Measure – when it asks for config files of an IDS deployed at an EAP, should it not read “for” an EAP. The Rationale mention IPS; however, the requirement only mentions IDS through-out. -Change rational for R1.5 states intrusion detection systems/intrusion protection systems. Does the “/” mean “and”, or “or”?
No

Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Verification that this does not include system to system communications in to the ESP. -R2.2 Clarification on where the encryption is required to start and stop? -R2.3 Where is the multi-factor authentication required?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1.2 addresses restricting access to only those individuals that are authorized; however, the measures address egress badging. The requirements do not mention egress badging, but the measures do. -Requirements 1.4 and 1.5 address issuing alerts, but there is nothing about the response. -R1.4 – What is the definition of access point? (Window, hatch, door or all)
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. - Clarification of the definition of continuous.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1 – High VSL lists a response within 15 minutes of a detected unauthorized physical access into a Defined Physical Boundary. There is no mention of a time requirement within the standard. -R2 – Moderate VSL – The vsl states “each” however the requirement does NOT have the word each included. Is it implied? -R2 – High VSL – What are the requirements of “continuous escort”? Continuous escort is not defined, but it’s listed here. -Why does it apply to low but issues severe penalties?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1 – Screenshots as evidence for large companies could be overly onerous.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R2.1 – Clarification that the “updates for all software and firmware…” only applies to security related patches/updates. -R2.2 – Doesn’t define when a patch MUST be deployed, only that it has to be within a defined timeframe. Request clarification on what is an appropriate timeframe. -Does each patch require a remediation plan? (Or can there be generalized… Windows Tuesday update, etc...) -R2.3 – No mention of the 30 day requirement. Is this an oversight? It is mentioned in the “Change Rationale.” This should provide for a TFE.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. - R3.3 Provide clarification of availability. In requirement 2, it asks when an entity gets notified. Should this not follow the same process? Provide clarification of, “Update malicious code protections within 30 calendar days of signature or pattern update availability”. -R3.5 Provide clarification on where these logs can be kept. Can this be manual?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R4.1 – No TFE’s are allowed on this requirement. Concerned that not all devices can satisfy this requirement. -R4.1.4 – Very general statement, how would an entity define this? NIPSCO recommends removal of the word “potential” from the description. -R4.5 – Two week window with sampling is very tedious and time consuming. It is unclear what is defined as sampling? Is that one log, two logs, etc…? Would once a month or quarter be more appropriate?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R5.1 Measures – Define internal and remote paths. -R5.5.3 – There is no mention of a

measure for this requirement. Request to provide further clarification on the appropriate timeframe to change the password.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Request clarification on why the word “dated” has been added to the measures used throughout this requirement. -Do the suggested modifications in CIP-008 take into consideration Project 2009-01?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1.5 –How does this address reliability or recovery of the BES? Even though you can TFE this requirement, this will be difficult to implement enterprise wide when individuals are concerned about recovery and not “mirroring drives”. How long do you keep this data (extra drives)? Protection of this additional drives/data could also become an issue.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R3.1 – Should this mean BES Cyber Assets or BES Cyber Systems? How many of the assets of the system?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1.1.4 – Scripts could be anything from a customized startup script to a detailed script required for operations. Script is very vague and needs to be either removed or further detailed. -R1.1.5 and R1.1.6 – Request removal of the word “any” from the description. -R1.2 – A change advisory board is too large for many organizations and they don’t have them implemented. Provide a different example so entities won’t read that they are required to have CAB’s. -R1.4 – Determining security controls that could be impacted, where is the measure for this requirement?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Why is wireless review and scanning mentioned in the Guidelines section, but it’s not mentioned in the requirements? -Requesting clarification of “on the effective date,” and how to show compliance. -Request clarification of “vulnerability assessment” in a test environment.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on

this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1.2 – Formatting issue at the Headers of columns CIP-011-1 Table R1, in which they all say “Part”
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R2.1 – This requirement appears vague and request to review the description for more clarification. The word “cleared” appears to be essentially the same as “destroyed,” and request clarification on the appropriate method of clearing media and destroyed media that shows compliance. -The last paragraph in the Guidelines section actually still refers to “erased” and not “cleared”.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on these standards, therefore NIPSCO cannot provide an affirmative vote on the implementation plan.
Group
CenterPoint Energy
John.Brockhan@CenterPointEnergy.com
Yes
CenterPoint Energy suggests the following changes to the definitions: Page 1 – 2 – BES Cyber System/BES Cyber Asset/ BES Reliability Operating Services CenterPoint Energy does not agree with the introduction of these new terms and prefers the existing and familiar terms, Critical Asset and Critical Cyber Assets. The Company believes that the new terms and approach to determine covered assets lacks clarity, will be difficult to apply and audit, and creates ambiguity as to where the process ends. This is especially a concern considering the exhaustive list of BES Reliability Operating Services. If the SDT insists on retaining the BES Reliability Operating Services, CenterPoint Energy also suggests that the term not be added to the NERC Glossary, but be kept local to the CIP-002 Standard. The definition for BES Cyber Asset states that “Redundancy shall not be considered when determining availability.” CenterPoint Energy requests clarification on whether this concept has been reasoned for application in a substation environment, specifically in the instance of primary/backup relays and identical redundant systems. In the definition of BES Cyber System, the term “Maintenance” should be replaced with “Transient” in the definition of BES Cyber System to reflect changes in the terms and new definitions made available. Page 2 – BES Cyber Security Incident CenterPoint Energy believes “was an attempt” is vague and seeks clarification on how such an attempt will be determined. An alternative would be to delete the phrases “or was an attempt to compromise” and “or was an attempt to disrupt”. CenterPoint Energy also recommends that the 3rd bullet be deleted as it does not fit the term BES (Cyber) Security Incident. Page 2 – BES Cyber System Information CenterPoint Energy suggests that “computer” be added in front of network topology for clarification. The Company also suggests that the word “disaster” be deleted to be consistent with the way that recovery plans have been labeled in the current version. Disaster adds a qualification to recovery plans that could be limited to such situations (disasters). Additionally, CenterPoint Energy recommends that “Impact” be changed to begin with a lowercase “i” since a definition of BES Cyber System Impact has not been proposed. Page 2 – BES Reliability Operating Services Under Dynamic Response to BES Conditions, should “systems” be capitalized like the other items in the series (Elements, Facilities)? Please clarify. The criteria “Under and Over Voltage relay protection (includes automatic load shedding) -Sensors, relays & breakers” should be deleted as it is duplicated. Under Inter-Entity Real-Time Coordination and Communication, CenterPoint Energy questions the use of the term “operational directive” and would like to ensure that the SDT has considered NERC’s efforts underway to define “reliability directive”. Page 6 – CenterPoint Energy recommends that “or other, similar incident” be added to the definition of CIP Exceptional Circumstance to add some flexibility and “BES” be added in front of “Cyber Security Incident”. Page 6 – The Company proposes that the definition of CIP Senior Manager is not needed as a glossary term,

but is acceptable in the requirement description. Page 7 – CenterPoint Energy views the change in term to Defined Physical is unnecessary. Could not the definition of Physical Security Perimeter be updated with the meaning given to Defined Physical Boundary as seen with other existing terms? Page 7 – CenterPoint Energy requests clarification on the relationship between the EAP and ESP. Page 7 – CenterPoint Energy requests that the SDT use the definition from CAN-0024 for this term, External Routable Connectivity. Page 8 – CenterPoint Energy proposes that "consecutive" be added in front of calendar days for clarification. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
Yes
CenterPoint Energy is concerned that the language (as stated in 2.7) will result in identifying substations as critical/medium impact when, in fact, they are not. Line count does not necessarily mean that issues at particular substation will have a significant impact on the BES. Such impact can only be determined by studies and risk-based analysis of an entity's assets. Thus, CenterPoint Energy is in support of language similar to that in CIP-002-3/CIP-002-4 for identifying substations that are critical to the reliable operation of the BES. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy suggests that the SDT consider continuing the concept of starting with assets as an alternative approach. CenterPoint Energy proposes that the approach be based on an identification of High, Medium, and Low assets and then proceed with identifying Critical Cyber Assets at those facilities. Page 19 - 21 - "Operations Service" should be "Operating Service". CenterPoint Energy would like to request the removal of the extra bullet under Managing Constraints as it appears that criteria may be missing. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
Yes
CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy proposes that documentation errors should rarely if ever be deemed high/severe. Only violations that could have an immediate impact on the reliability of the BES should be considered high/severe. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy supports the concept of assigning a senior manager as outlined in the existing standards/requirements. However, the rationale for changing the language and numbering of this requirement is not obvious as the changes are immaterial and appear to have no effect on the implementation of the requirement. There will be an impact on compliance and compliance tracking for no substantial benefit. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Similar to the previous comment on R1, CenterPoint Energy supports the concept of establishing a cyber security policy as outlined in the existing standards/requirements. However, the rationale for changing the language and numbering of this requirement is not obvious as the changes are immaterial and appear to have no effect on the implementation of the requirement. There will be an impact on compliance and compliance tracking for no substantial benefit. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
See comment for R2. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy recommends that the SDT revert to the CIP Version 3/Version 4 language for this requirement as the changes are immaterial in writing yet could prove moderate in interpretation and implementation. The change is also not supported by a FERC directive. The Company would also like to propose that this requirement should be limited to the applicability of High and Medium impact BES Cyber Systems as it pertains to the categories and formatting. CenterPoint Energy also suggests that "unescorted" be added in front of all references to "access". CenterPoint Energy recommends that the

last 3 bullets under Measures (M4) be deleted as bullet 1 or 2 should be sufficient to prove compliance. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy recommends that the SDT revert to the CIP Version 3/Version 4 language for this requirement as the changes are immaterial in writing yet could prove moderate in interpretation and implementation. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
Yes
The footnote reference should be reformatted. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy views the VRF/VSLs for R4 and R5 as unreasonable and proposes that they be lowered. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests clarification on who should receive the on-going reinforcements. Alternatively, the SDT should revert to the CIP Version 3/Version 4 language. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests clarification on role-based training and suggests that “and the training needed.” Be added to Requirement 2.1. CenterPoint Energy also suggests that 2.2 be deleted and 2.3 and 2.5 be combined for simplification and clarity. Additionally, Requirement 2.7 should also be deleted and its concepts combined with 2.9. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 14 and 15 - R3.1 and R3.2 - CenterPoint Energy requests that “Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems” be removed from the applicability as it is seen as an expansion in scope that is not supported by a FERC directive or rationale. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy recommends that the applicability for this requirement be set to match that of R5.
Yes
CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy does not agree with this requirement and proposes that the SDT refer to the CIP Version 3/Version 4 language. There are also concerns on the measures and the amount of evidence required to demonstrate compliance. The first measure should be adequate. Also, the description of evidence on the 3rd measure is unclear. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 29 - R7.1, CenterPoint Energy suggests that the SDT change "at the time" to "concurrent or prior to the date of" to minimize the issue of time alluded to in footnote #2. Page 30 - R7.2 – CenterPoint Energy believes that the time limit of “by the end of the next calendar day” is unreasonable for reassignments or transfers and proposes that the SDT consider extending the time limit. CenterPoint Energy understands that access of transferred individuals should be reviewed and updated; however, there is usually a period of transition and such personnel changes are within the same organization. “Accumulating unnecessary authorizations through transfers” usually happens over a time period that is longer than the 7 days which is the current requirement. Page 31 – R7.3 – CenterPoint Energy requests clarification on tracking access to BES Cyber System Information. It appears that removing access to the system and physical facilities would be satisfactory. Page 33 – R7.5 – CenterPoint Energy is concerned with the applicability of this requirement to Medium Impact BES Cyber Systems. Implementation would have a significant impact on substation operational procedures. CenterPoint Energy questions if the removal of physical access for Medium Impact BES

Cyber Systems sufficient. For entities that do not network assets, this is not technically feasible. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Most of the VRF/VSLs are High/Severe. CenterPoint Energy believes that such classifications are not reasonable for most requirements given that minor exceptions would not lead to an interruption to the BES. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy recommends that the words “and monitor” in the Rationale for R1 be deleted as it does not fit with the definition or concept of Electronic Security Perimeter. Under Summary of Changes, “points” should be capitalized. Page 11 - R1.1 – Under Measures, “technical and procedural” should be changed to “technical or procedural” to reflect the language in the requirement. Additionally, CenterPoint Energy proposes the following wording for the measures: Evidence may include, but is not limited to, existing documented technical or procedural controls. Page 11 – R1.2 - CenterPoint Energy requests that “Associated Physical Access Control Systems” be removed from the applicability as it is seen as an expansion in scope that is not supported by a FERC directive or rationale. CNP suggests that “with external routable and dial-up connectivity” be added to “Associated Protected Cyber Assets”. Also, proposed alternative wording for the requirement is as follows: Control and secure all instances of external connectivity through the use of identified Electronic Access Points (EAPs). Page 12 – R1.3 – CenterPoint Energy suggests replacing “granting or denying” with “denying access by default”. Page 13 – R1.5 – CenterPoint Energy seeks clarification on whether this requirement is for host-based or network based intrusion detection systems or is it optional. The Company also suggests that “at each EAP” be changed to “at each ESP”. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy seeks clarification on when encryption initiates and terminates. CNP also requests that the SDT consider splitting this table into specific requirements for dial-up and requirements for routable. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations instead of all being rated, “Severe.” CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 11-12 – R1.2 &1.3 - CenterPoint Energy is concerned that tracking for ingress and egress is not available for many physical access control systems and a TFE might be necessary. This is also a change in scope that is not supported by a FERC directive or rationale. Page 13 - R1.4 – CenterPoint Energy requests clarification or a description of a “real-time alert”. In reference to a “response to an unauthorized physical access”, please clarify if this means real or attempted as a pure population of real or especially attempted events would be hard to track. In the case of unauthorized badge swiped, yet the system does not open the door, is that an “attempt”? Page 14 – R1.6 - CenterPoint Energy requests clarification on the retention required. Will entities be required to have 90 days as in the current standard or 3 years? Storage for three years of logs that are not related to an event could prove costly and burdensome for no benefit. CenterPoint Energy also has concerns regarding implementing this requirement in the substation environment given the group work that occurs under the direction of a crew leader. Does each person have to be identified? CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
Yes
CenterPoint Energy supports the comments submitted by Edison Electric Institute (EEI).
No
Page 18 – R3.1 - CenterPoint Energy requests clarification on what the SDT expects to be done at a door/fence/gate. Page 18 – R3.2 – CenterPoint Energy suggests that “or Monitoring Systems” be deleted under applicability. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy supports the comments submitted by Edison Electric Institute (EEI).

No
Page 10 – R1.1 - CenterPoint Energy foresees a substantial impact given this revised wording and suggests that the SDT consider the CIP Version 3/Version 4 language. Specifically, the change in “documenting compensating measures” (CIP Version 3/Version 4) versus “documenting the need” (CIP Version 5) could prove difficult for dynamic ports with little benefit and may not be technically feasible for all systems. CNP believes that intention and results would be the same if the legacy language was retained. Page 10 R1.2 – This requirement is very broad. Alternate wording could be included as follows: “Protect against the use of unnecessary physical I/O ports”. CenterPoint Energy also requests that the SDT consider provisions for procedural controls. The inclusion of removable media on this requirement is also a concern. CNP suggest that the term, removable media be deleted. The Company also does not believe that signage provides solid security benefit. Logical restriction and placement in a Defined Physical Boundary appears adequate to meet the requirement. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 12 – R2.1 - CenterPoint Energy requests that the SDT clarify that a null list is acceptable or include provisions for a TFE for this requirement as implementation may not be possible for all substation systems or assets. Also, add “security related” in front of updates. CNP also requests that the last sentence of the measures be deleted: “The list could be sorted by BES Cyber System or source.” Page 13 – R2.2 – CenterPoint Energy suggests the following as alternative language: “Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 60 days of release from the identified source.” Page 14 – R2.3 – CenterPoint Energy believes that the measures go above and beyond the requirement which only calls for a process. Detailed records would depend on the contents of the process. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 17 – R3.1, 3.2 - CenterPoint Energy suggests that the applicability be updated to reflect application to “Medium Impact BES Cyber Systems with External Routable Connectivity”. R3.2 – The measures do not align with the requirement. CNP suggests deleted bullets, 2 and 3. Page 18 – R3.4 – CenterPoint Energy requests that references to Transient Cyber Assets be deleted. The measure regarding logs should be moved to R3.5. Page 19 – R3.5 – CenterPoint Energy requests clarification on the implementation of this requirement as the Company foresees it to be burdensome and unrealistic, especially in a substation environment. Is this intended to be a system or manual log? CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 21 – R4.1 – CenterPoint Energy requests that “BES” be added in front of “Cyber Security Incident” and provisions for a TFE are made. CenterPoint Energy also recommends that the applicability for this requirement be set to match that of R4.4. Page 22 – R4.2 - CenterPoint Energy requests that the SDT revert back to the CIP Version 3/Version 4 language or provide a description for “real-time alert”. Page 23 – R4.3 – Add "after failure is identified or made aware of" in the requirement. Page 23 – R4.4 – CenterPoint Energy requests that the SDT revert back to the CIP Version 3/Version 4 language as there is no substantive change or related FERC directive. CNP also suggest that the measures sentence end before “and”. Page 44 – R4.5 - CNP suggests that the requirement ends before “and”. CNP also suggest that the measures sentence end before “and dated evidence…”. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 27 – R5.1 - CenterPoint Energy recommends the following alternative language: “Authenticate individual and shared account access before granting electronic user access to each BES Cyber System where technically feasible.” Page 28 – 30 - R5.2, 5.3, and 5.5 – CenterPoint Energy recommends that the “Medium Impact BES Cyber Systems” applicability for these requirements be updated to “Medium Impact BES Cyber Systems with External Routable Connectivity”. Page 31 – R5.6 – In regards to the applicability, Medium Impact BES Cyber Systems at Control Centers, CNP requests clarity on the types of devices that fit this description. Consoles only? CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations. CenterPoint

Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 11 - R1.1 – CenterPoint Energy requests that the phrase “or Defined Physical Boundary of BES Cyber System and” be deleted as it should not be included with Cyber Security Incidents. Provisions for physical incidents are covered under CIP-001 and EOP-004. Page 12 – R1.3 – CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 13 – R2.1, 2.2, 2.3 – CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Generally, Page 15 - 17 – R3 – CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. Page 5 – In the Purpose statement, CenterPoint Energy requests that the sentence end before “and” since business continuity and disaster recovery is beyond the scope of this Standard. Page 16 – R3.2 – Thirty calendar days is not enough time. CNP proposes that the requirement be updated to state “within 30 days of determining actual cause”. Page 16 – R3.3 – Add “if necessary” to the end of the sentence. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations. CNP also recommends that the “Requirement R1” paragraph under Guidelines and Technical Basis be deleted as entities should be able to refer to the definitions. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Generally, CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. Page 10 – R1.3 - Delete "protection of information” as it is required in CIP-011. Page 11 – R1.4, R1.5 – Check Table R1 headings. R1.4 - CenterPoint Energy requests that the SDT clarity what “verified” means in the requirement. (ex. A log showing status – “Successful”) CNP also asks that “after significant changes to the system" be added to the end of the sentence. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI). R1.5 – CNP proposes the following alternative language: “Preserve data for analysis or diagnosis of the cause of an event that triggers activation of the recovery plan as required in Requirement R1 when it does not impede or restrict restoration.”
No
Generally, CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. Page 13 – R2.2 – CenterPoint Energy suggests replacing “Test any information” with “Test a sample of information”. Page 14 - R2.3 – Delete “Medium Impact BES Cyber Systems at Control Centers” from applicability. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 15 – R3.1 – Delete “or when BES Cyber Systems are replaced” from the requirement. Page 16 – R3.2 – Delete “incident” from the requirement and the measures. Thirty days is not enough time to perform the exercise and document lessoned learned. CenterPoint Energy suggests 60 days. Page 17 – R3.4 – CenterPoint Energy suggests the following as alternative language: “Update recovery plan(s) within thirty calendar days of any organizational or technology changes that impact that plan.” CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).

No
CenterPoint Energy believes that the R1 requirements would be burdensome, not realistic for every day operations and difficult to implement for every asset, especially in the substation environment. Implementation is complicated further by the details listed in the baseline configuration (R1.1). CNP suggests that this requirement be modified to accommodate general testing and significant changes. Additionally, R1.5 seems to imply that there must be a test environment. Some testing may have to be done in the production environment. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 15 - R2.1 - CenterPoint Energy believes this requirement would be overly burdensome especially in a substation environment that is not networked. CNP proposed that the applicability “Medium Impact BES Cyber Systems” be updated to “Medium Impact BES Cyber Systems with External Routable Connectivity. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy proposes that the description does match vulnerability assessment and requests that the SDT clarify or refer to CIP Version 3/Version 4 language. CNP also suggests that “cyber” be added in front of security controls. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Generally, CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. CNP also suggests that the applicability for Medium Impact be with the qualifier of “with External Routable Connectivity” or “at Control Centers” and “Associated Protected Cyber Assets” deleted. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy suggests that 2.1 and 2.2 be combined and Associated Protected Cyber Assets be removed from applicability. Additionally, the term media could refer to a long list of devices for which this requirement would be difficult to track and enforce. CNP also requests clarification on the term reuse. (ex. Can assets be reused/redeployed as long as they remain in the Defined Physical Boundary and for the purpose of BES Cyber Assets/Systems?) CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Given the scope expansion and anticipated impact of CIP Version 5, CenterPoint Energy suggests that 18 months is not sufficient time to implement. CNP also requests that the effective date not be set in the month of December or January considering various business processes conducted at the end of the year.
Group
LCEC CIP Team
Ed Nagy
Yes
BES Cyber Asset: This section of the definition is confusing and should be omitted: This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The reference to a “Cyber Asset” within the definition includes a number of devices that might need further clarification due to the word “programmable”. Would a relay that is “configured” be considered a Cyber Asset even if the configuration does not involve any kind of network, telecommunication or IP based network connectivity? BES Cyber System Information: Information about a BES Cyber System or Asset could

include vendor provided manuals and should not be included. Cyber Assets: Need to clarify what is meant by the term “Programmable” A Cyber Asset should imply that some form of connectivity is required to access the device otherwise it would simply be an Asset. Electronic Access Point & External Connectivity These definitions do not touch on serial interfaces that are not dial-up. Does this mean that serial communications will not be considered External Connectivity?
Yes
Attachment 1 criterion 2.13 categorizes all Transmission Operator (TOP) and Transmission Owner (TO) Control Centers as Medium impact to the BES. This criterion is too inclusive as it includes Control Centers of low impact Radial Transmission Owners and Operators unnecessarily. This results in the applicability of security controls that are not at all aligned with the risk that these Control Centers could have on the BES. To avoid this situation, Criterion 2.13 could be aligned with criterion 2.7 but instead of focusing on a single station or substation; consider all of the facilities that the Control Center controls. If the “total aggregate value” of all Transmission Facilities does not exceed a value of 3,000; the Control Centers should not be designated as Medium impact. For Example: 2.13. Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners with a “total weighted aggregate value” that exceeds 3,000 for all Transmission Facilities controlled by the Control Center per criterion 2.7; or (2) generation control centers that control 300 MW or more of generation. This modification is well aligned with the NIST risk management framework and the drafting team’s approach to focus on the impact to a shared resource like the BES. Criterion 2.7 must have been developed with an engineering basis that relates to the impact of Transmission Facilities on the BES. With this in mind, the same impact to the BES can only be realized if the sum of all facilities managed by a Control Center exceeds this same criterion. In the NOPR for CIP-002-4 and the subsequent response to the NOPR by NERC the NIST Risk Management Framework is discussed in section 5. In this section the stated goal is to “Categorize BES Cyber Systems based on their function and impact”. In addition, “A tiered approach to security controls which specifies the level of protection appropriate for systems based on their importance to the reliable operation of the Bulk-Power System” is discussed. The drafting team’s approach to categorization is in fact “Based on the “impact” or compromise or of the scope of control of the BES Cyber System”. In this example, it makes sense to modify the criterion to remain consistent with the categorization based on the impact and scope of control of these Low Impact Control Centers. In the NOPR for CIP-002-4 and the subsequent response to the NOPR by NERC, “Potentially unprotected Control Centers” are discussed in section 6. The FERC concern that many Control Centers are left with “No obligation to apply cybersecurity measures” under CIP-002-4 is legitimate. The response however should not be to include all remaining Control Centers as Medium Impact assets as is the current approach in CIP-002-5 criterion 2.13. The best approach is to continue to align security controls with the risk and impact to the BES. Many of the Control Centers that FERC is concerned with will be included as Medium Impact BES Cyber Systems if this change is made while others have cybersecurity measures required as is appropriate for Low Impact Assets.
No
R1.1 This requirement states that documentation needs to be updated within 30 days if BES/Facility changes result in a change to the categorization of BES Cyber Assets or Systems from a lower to a higher category if intended to be in service for more than 6 months. What is the expectation for compliance with the additional standards as a result of this change in categorization? It will be difficult to determine “intent” from an auditing perspective. What happens if there is “intent” but the six months is exceeded or the intent changes? In addition, this requirement doesn’t state what the expectation is for new Cyber Assets or Systems or Cyber Assets or Systems that may move from a High to Medium or Medium to Low Category. Is there any requirement to document these changes other than during the annual review process in R2? Table of Compliance Elements For both R1 & R2 Lower VSL, what is the VSL if less than 30 days for updates in R1 or Review and approval for R2? Is there such a thing as having NO VSL?
Yes
No
Table of Compliance Elements For both R1 & R2 Lower VSL, what is the VSL if less than 30 days for updates in R1 or Review and approval for R2? Is there such a thing as having NO VSL?
Yes

Yes
Yes
Yes
Yes
Yes
Yes
No
R2.1 The requirement does not call for the identification of training that is needed for each role but this is listed in the measures section of the table. Need to add this to the requirement.
Yes
Yes
Yes
Yes
No
R7.1, R7.3, R7.4, R7.5 Resignation and termination are very different and need to be treated as such. A resignation may take place weeks prior to the last day of service which is when access needs to be revoked.
No
R1.1 This requirement calls for technical or procedural controls for Low Impact BES Cyber Systems with External Routable Connectivity. Since there is no requirement to identify these assets or systems, it will be difficult to audit this.
Yes
Yes
No
R2.1 The requirement for continuous escorted access of visitors makes sense but it is difficult to prove compliance with this requirement. The measures include language in a visitor control program AND additional evidence to demonstrate compliance such as visitor logs. Visitor logs DO NOT demonstrate compliance with this requirement. Recommend removing the AND from the measures section of the table. R2.2 Need to clarify what meant by “point of contact” for the visitor. Cell phone? Office Phone? Email address?
No
3.1 and 3.2 The applicability section is unclear, are the “Associated Physical Access Control or Monitoring Systems” referring to security systems that protect Medium or High Impact Cyber Assets or Systems only?

Yes
Yes
No
R3.1 & R3.4 Need to clarify if this requirement is deter or detect or prevent Or deter and detect or prevent Or deter and detect and prevent The wording is highly subjective and should be clarified. R3.4 & R3.5 Need to clarify if manual logs are acceptable for audit proof or if all systems need to be able to generate a log to show when Transient Cyber Assets have been connected. (Auditors will likely ask for system logs) This may not always be technically feasible for removable media on all assets. In addition, the connection may be via a network connection as opposed to a physical connection.
No
R4.4 Retention of logs for 90 days will not meet the expectation of auditors that will demand to see logs to demonstrate compliance for the entire reporting period. This standard should clearly state that the entity is not required to maintain these logs beyond 90 days and that the auditor should audit the process and/or select a test sample from the population of available logs.
Yes
Yes
No
R1.1 and R1.2 In order to identify, classify and respond to BES Cyber Security Incidents the entity would need to identify all of the Assets or Cyber Systems. This is not a requirement for Low Impact BES Cyber Systems but it is implied by these requirements.
No
See Response to Question 34
No
See response to question 34
No
1.4 Need to clarify what is meant by “verified” initially after backup
No
R2.2 Need to clarify what is meant by “test initially” and at least once each calendar year. Does this imply that a full recovery must be performed for each backup? If so, the best practice of completing more frequent back-ups may be bypassed to achieve compliance. Suggest removing “test initially” from the requirement. Also need to clarify that back-ups will likely not contain the most current configuration unless they are performed frequently.
Yes
Yes
No
R2.1 The “where technically feasible” statement implies that monitoring should be automated in some fashion and that if this is not possible, that a TFE will be generated. This will result in significant TFE’s which do not add value from a security perspective. In addition, the baseline that is referenced in section 1.1 includes the physical location. How will this be monitored without performing a physical inventory and at what cycle?
No
R3.1 This requirement calls for a paper OR active assessment of the security controls to determine

the extent to which the controls are implemented correctly and operating as designed. The terms "implemented correctly" and "operating as designed" seem to imply technical controls which will be difficult to validate with a paper based assessment. The paper review is a good option for entities so I would recommend that the results section of the requirement be rewritten as follows "to determine the extent to which controls are implemented and/or operating as designed."
Yes
Yes
Yes
Individual
Curt Wilkins
Douglas County PUD No.1
No
No
No
The Rationale for R1 appears to imply a two-step process in the identification and categorization of BES Cyber Assets/Systems, i.e. "Once they have been identified, they must be categorized according to their impact…" However, in R1 as currently written, the word "identify" comes after the statement that the requirement applies to Entities that own BES Cyber Assets/Systems. This implies that the identification step has already occurred. So, does the word "identify" refer to identifying High and Medium Impact BES Cyber Assets/Systems," or does it refer to identifying which Cyber Assets/Systems are BES Cyber Assets/Systems? If the former, it seems that "identify" is redundant with "categorize" since, identifying which BES Cyber Assets/Systems have High or Medium Impact would be the categorization step. If the latter, then "identify" seems to be misplaced in the sentence since, in the introduction to R1, Responsible Entities have already determined that they own BES Cyber Assets or BES Cyber Systems. Suggest rewording R1 to clearly identify the two-step process or adding a new R1 for the identification step: New R1: "Each Responsible Entity shall identify its BES Cyber Assets or BES Cyber Systems by determining which of its Cyber Assets or Cyber Systems perform or support any BES Reliability Operating Service and could impact the reliable operation of the BES." Evidence could be a list of Cyber Assets or Cyber Systems with a determination of the BES Reliability Operating Service(s) they perform, if any. BES Cyber Assets or BES Cyber Systems would be those Cyber Assets/Systems on the list that could adversely impact the BES Reliability Operating Service, per definition. It seems that this would aid the Entity in audit preparation by having a complete audit trail of its BES Cyber Asset/System identification and categorization processes. New R2: "Each Responsible Entity that owns BES Cyber Assets or BES Cyber Systems shall categorize them according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. BES Cyber Assets and BES Cyber Systems that it owns that are not categorized as High or Medium Impact shall be deemed to be Low Impact and do not require discrete identification." Evidence would be the same as the currently written M1. The "BES Reliability Operating Services" paragraph, CIP-002-5 page 8, appears that it should be edited. Sentence 2 states "In order to identify them, Responsible Entities determine whether BES Cyber Assets perform or support any BES Reliability Operating Service." If it's a BES Cyber Asset, then it has already been identified and determined. Suggest removing "BES" prefix to Cyber Assets: "In order to identify them, Responsible Entities determine whether Cyber Assets or Cyber Systems perform or support any BES Reliability Operating Service." Also suggest truncating sentence 4 after BES Cyber Systems to avoid the redundancy of "that perform or support BES Reliability Operating Services," i.e. "This ensures that the initial scope for consideration includes only BES Cyber Assets and BES Cyber Systems."
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Typo in R6, should be "change" not "change2".
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
DOPD agrees with the intent of R2, but makes the following suggestions for Part 2.1: (1) “when incidents occur” seems redundant with “When a BES Cyber Security Incident occurs,” (2) “or test” appears to be tacked on to the end without being mentioned earlier in the requirement, and (3) suggest using the word “exercise” instead of “test” to correlate with Part 2.2. Suggested rewording “When a BES Cyber Security Incident occurs or the BES Cyber Security Incident Response Plan is exercised, the incident response plans must be used and include recording deviations taken from the plan during the incident or exercise.” In the Measure for 2.1, suggest adding “or exercise” at the end of the measure: “…deviations taken from the plan during the incident or exercise.”
Yes
Yes
Yes
The column headings for CIP-009-5 Table R1 for Part 1.4 and 1.5 need to be corrected to “Applicability,” “Requirements,” and “Measures,” rather than Part, Part, Part. DOPD agrees with the intent of Part 1.5 as it applies to preserving forensic data for analysis of potential cyber security incidents or cyber events. Many triggers of the recovery plan(s) could be for physical, non-cyber events such as damage or failure due to fire, water, earthquake, power failure, etc. Taking the time to preserve data for these non-cyber events may increase the time it takes to recover the cyber assets. Suggested wording: “Preserve data, where technically feasible, for analysis or diagnosis of the cause of any cyber event that triggers activation of the recovery plan(s) as required in Requirement R1.”
Yes
Yes
The column headings for CIP-009-5 Table R3 for Part 3.4 and 3.5 need to be corrected to “Applicability,” “Requirements,” and “Measures,” rather than Part, Part, Part.
Yes
Yes
Yes
Yes
Yes
Yes

The column headings for CIP-011-1 Table R1 for Part 1.2 and 1.3 need to be corrected to "Applicability," "Requirements," and "Measures," rather than Part, Part, Part.
Yes
Yes
Yes
Individual
Brenda Frazer
Edison Mission Marketing & Trading
No
No
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
We do not think it should be required to badge out and we think it could present a problem if there were an emergency. And if it is being said that you do not have to badge out to open the door to exit - then are we not opening ourselves up to multiple violations/self reports and possibly fines?
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Black Hills Corporation Registered Entities (NCR00089, NCR05030, NCR05031 & NCR11186)
Bob Case - NERC Compliance Manager (605) 721-2716
No
Yes
The reference to “Change Management” in Attachment 1 (looks more like a capital (i) in the standard) of CIP-002-5 under Situational Awareness carries multiple meanings in the industry… e.g. the human reaction to change, managing changes in resource and transmission capabilities, and the validation process of security and upgrade patches. In the context of Attachment 1, the “managing changes in resource and transmission capabilities“ example is preferred.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
If the expectation is that delegation of approvals is required down to BES cyber system gate keepers (asset owner), then this requirement is considered overly prescriptive.
Yes
No
For R2: Suggest that a Moderate VSL be added that reads as follows: “The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required parts 2.1 to 2.10”. Change the High VSL to read as follows: “The Responsible Entity has implemented at least one cyber security policy, but has failed to address more than one of the required parts 2.1 to 2.10”. Change the Severe VSL to read as follows: “The Responsible Entity has not implemented any cyber

security policy." For R4: Add a Moderate VSL: "The Responsible Entity has made some, but not all, individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function. Less than 5% of those individuals who have access to BES Cyber Systems were not made aware of the cyber security policies appropriate for their job function." Change the High VSL to read: "The Responsible Entity has made some, but not all, individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function. Greater than 5% but less than 50% of those individuals who have access to BES Cyber Systems were not made aware of the cyber security policies appropriate for their job function." Change the Severe VSL to read: "The Responsible Entity has made some, but not all, individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function. Greater than 50% of those individuals who have access to BES Cyber Systems were not made aware of the cyber security policies appropriate for their job function."
No
The Measures section in Table R1 is worded in a way that may cause confusion. The wording "…and additional evidence to demonstrate that this program was implemented such as, but not limited to, the quarterly reinforcement material that has been distributed." may be interpreted to mean that more than the quarterly reinforcement material was necessary. Suggest changing to: "…and additional evidence to demonstrate that this program was implemented and awareness materials were identified and delivered to meet timeframes specified in the regulations." Also, since security awareness may be general in nature and a key contributor to a good corporate security program, it makes sense to add the ability to encourage vendors to provide their own awareness materials to their employees and allow the RE to accept documentation of that vendor awareness as compliance for this requirement relative to contractors and/or vendors with access to BES systems. The specific addition to the Measures section could read: "Documented evidence of awareness for contractor and/or vendor employees with access the BES systems may include evidence of the vendor's documented security awareness program and additional evidence to demonstrate that the vendor's program was implemented and awareness information was identified and delivered to the vendor/contractor employees to meet the content and timeframes specified in the regulations."
No
Delivery of cyber security training to vendor support staff who, most often, are never physically on site at a Registered Entity's facility can be difficult to document. For Table R2 Measures section for sub-requirements R2.2 – 2.10, retain the first paragraph in each sub-requirement as written, but add a second paragraph as follows: "Evidence to support contractor/vendor training may include, but is not limited to, vendor's attestation/certification that Responsible Entity's role-specific training has been delivered to all contractor/vendor employees with access to Responsible Entity's BES Cyber Systems."
No
Delivery of cyber security training to vendor support staff who, most often, are never physically on site at a Covered Entity's facility can be difficult to document. For Table R3 Measures section for sub-requirement R3.1, retain the first paragraph in each sub-requirement as written, but add a second paragraph as follows: "Evidence to support contractor/vendor training may include, but is not limited to, vendor's attestation/certification that Responsible Entity's role-specific training has been delivered to all contractor/vendor employees with access to Responsible Entity's BES Cyber Systems."
Yes
Yes
No
This language appears to change the access granting process significantly by requiring the CIP Senior Manager or delegate to authorize all electronic access. We believe this responsibility is typically job role (specific asset owner) based, and is not based on an individual delegation. Recommend that the language remain as identified in CIP-004-3, with updates as follows to retain the consolidation of access requirements found in CIPs-003, 004, 006, and 007": R6.1: Recommend the following language: "The responsible entity shall authorize electronic access based on minimum necessary work requirements except for those situations meeting the definition of "CIP Exceptional Circumstances". R6.2: Recommend the following language: "The responsible entity shall authorize unescorted physical

access to BES Cyber Systems based on minimum necessary work requirements except for those situations meeting the definition of “CIP Exceptional Circumstances”. R6.3: Recommend the following language: “The responsible entity shall appropriately manage and grant access to BES Cyber System information based on minimum necessary work requirements except for those situations meeting the definition of “CIP Exceptional Circumstances”.
No
R7.2 and R7.3: The language used fails to address issues related to ongoing access requirements during ‘transition periods’ associated with employee transfers. Recommend the following addition to the Requirements Section of Table R7: “For retirements and reassignments, revoke the individual’s unescorted physical access and Interactive Remote Access to BES Cyber Systems by the end of the next calendar day after access is documented as no longer required.
No
There are many administrative requirements where zero tolerance is inappropriate. Missing a re-training date by a day or a week should not be considered a High or Severe violation level.
Yes
Yes
Yes
No
R1.3 needs to clarify the need for multiple access controls vs. multiple physical access layers.
No
Intentions of change are good, however, the change description and justification in table 2 (R2.2) do not seem to reflect the current wording of the requirement.
Yes
Yes
Yes
No
The statement at the bottom of CIP-007-5 Table R2 “This is the same concept as in the current CIP-007 R3.2 wording however a 30 day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used” confuses the expectation for the implementation vs. the implementation plan needing to be done within 30 days.
No
No definition of transient cyber assets or transient cyber asset connections is provided within the standard, but is needed. Realize that is defined in supporting documents, but terms should be defined in the NERC Glossary, or the standard directly.
Yes
Yes
Yes
Yes
Yes
Yes

Yes
No
CIP-009-5 Table R1 in Part 1.5 requires preserving data, where technically feasible. This suggests that a TFE will be required if preserving data is not technically feasible. Do not understand how a TFE can be completed in its current form (compensating factors) since this would occur post-incident, and if the data is gone, it's gone.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Request clarity in R1.3 as to whether discovering a document not properly handled during an assessment constitutes a violation, even though the process was in place.
Yes
Yes
Yes
Individual
David Kiguel
Hydro One Networks Inc.
Yes
Refer to additional comments submitted for Question 49. "Suspicious" is not an auditable term, and should be removed. What is an "attempt"? What attempts are serious enough to justify having to be reported? The definition should be made to read: BES Cyber Security Incident: • A malicious act that: Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. Under "BES Reliability Operating Services": • "Identify and monitor flow gates" under "Managing Constraints" appears to be missing its bullet. • Recommend that "Change management" under "Situational Awareness" be clarified to changes in the BES instead of IT change management. • Recommend clarification that "Facility" is the NERC Glossary term--in "facility operational data and status" under "Inter-Entity Real-Time Coordination and "Communication": • Request clarification of the scope of this "Operational Directives". Does it include a company's messaging system? Two-way radios? What is the relationship with the new COM-002? • Request clarification that these Coordination and Communications are limited to Reliability, not Market Systems. • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions." • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret.

Yes
Recommend that 2.8, 2.9 and 2.11 start with “Applies to all Regions except…” For 2.8, 2.9 and 2.11 request that the SDT clarify whether the exception is all regions, or not WECC. In 2.12, “system” and “Facility” are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOP, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appealing?
No
For clarity, request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days when a change to BES Elements and Facilities is placed into operation.” For clarity and consistency with the previous change, request changing M1 from “as required in R1 and list of changes to the BES (” to “as required in R1 and list of changes to the BES Elements and Facilities).” The word “intended” should not be used in the requirement because it is not auditable. Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard. The process to classify and categorize Cyber Assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced throughout the Standards.
No
The last bullet for M4 on page 12 is inconsistent with R4 since M4 requires periodic training instead of R4’s making staff aware of cyber security policies. Request that M4 be updated to be consistent with R4.
Yes
No

The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
No
The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
No
Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement. Recommend removal of R2.3 and R2.4 since they are redundant to R2.2, or explain the difference between R2.2 and R2.3, R2.4. Request removing “potential” from R2.7 since training should include how to determine whether a BES System Event occurred or not.
Yes
No
For all R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical.”
No
For R6.1 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “authorize electronic access, except…” to “authorize electronic access to BES Cyber Systems, except…” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary.” For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary.” For R6.3 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber System Information. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary.” For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary.” For R6.6 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I” in Information.
No
Request that the footnote for 7.1 be moved into the requirement. Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend removing the "following the resignation or termination" since it is redundant and inconsistent with the sibling Requirements. Recommend changing 7.4 from "For resignations or terminations," to "For terminations, resignations, reassignments, or transfers,".
No
Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point or not? Request clarification on 1.5's "at each EAP." Is that inside, outside or both? Regarding CIP-005-5, the

Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard. This would make the CIP standards consistent with the Results Based Standards concept.
No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." As written, the proposed Requirement is too prescriptive and does not allow new technology. Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete.
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress." Request that Requirement 1.2 be updated to allow "escorted physical access." Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls." Is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.4 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress." Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. to "issue real time alerts for detection of breach through an access point." For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6. Regarding CIP-006-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis."
No
Request clarification on what the "Associated" "Applicability" (High/Medium/Low BES Impact) for 3.1 and 3.2 Request capitalization of "locally mounted hardware or devices" in Requirement 3.1 so that it refers back to the defined term "Locally Mounted Hardware or Devices."

No
Request clarification on 1.1. Is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on 1.1. Why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Regarding CIP-007-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard. Screenshots seem to be excessive for this requirement. Documenting the need for each network-accessible port is sufficient.
No
Request clarification of "remediation" in 2.2 since it reads that the patch must be applied, which does not allow having an exception when applying the patch is the worst scenario such as creating a denial of service. For 2.2, suggest wording like "create a remediation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied." What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to the patch or the overall process? How do we address the risk of the patch affecting the potential reliability of the BES upon testing, prior to release? What is the recourse if not applied within the 30 days when potential issues have been identified?
No
Request allowances in 3.3 for signatures/pattern updates that cause trouble. Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media". The Measure for 3.4 does not match the Requirement.
No
Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities. Request clarification on 4.3. Does the failure need to be detected within a calendar day? Request the rationale of 4.5's "two weeks." We recommend one month as a compromise between the prior version's 90 days and the suggested one week. In 4.5 clarification is needed for the associated protected cyber assets. Are these protected cyber assets associated with only high impact BES cyber systems, or could they be associated with medium impact BES cyber systems?
No
For 5.2, does the CIP Senior Manager or delegate approval policy or procedure for each authorization of access? In 5.2, should the Requirement be interpreted as "each use" as in "The CIP Senior Manager or delegate must authorize the use of each administrator, shared, default, or other generic account types?" Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
No
Regarding CIP-008-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the

need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

2.1 is a new Requirement. Request the rationale for this new Requirement. Recommend changing from "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." to "When a BES Cyber Security Incident is classified or identified, the Responsible Entity must follow its incident response plan." Recommend removing “initially upon the effective date of the standard” from 2.2 of Table R2 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered.

No

Recommend removing “initially upon the effective date of the standard” from 3.1 of Table R3 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend that 3.2 wording be consistent with the 2.2 wording. For 3.3, recommend changing 1) "Update" to "Update as necessary" and 2) "the completion of the review of that plan" to "the completion of the review performed in 3.2".

No

For 1.3, request clarification of the “protection of information.” Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not, what is the intent? Recommend removing Requirement 1.5. Reliability's top priority is restoration of service. Forensics in a recovery mode may not support BES reliability and requiring such actions may negatively impact the BES Cyber System restoration process. Regarding CIP-009-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Recommend that 2.1 be implemented 180 days from the effective date of the Standard. For 2.1, request clarification, is “full operational exercise” the same as “functional exercise” as described in the rational? For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Do “backup media” include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments.” What is the scope? All network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the

Standard.
No
For 3.1 recommend 1) removing “or when BES Cyber Systems are replaced” as it addressed in CIP-009 R3.4 and 2) removing “and document any identified deficiencies or lessons learned” as they are addressed in CIP-009 R3.2 and R3.3. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Recommend that 3.4 be referenced by CIP-009 R3.1. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
Recommend changing 1.3 to avoid double jeopardy from "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." For 1.1, 1.2, 1.3 and 1.4, recommend changing the Requirements to be consistent with their Applicability --- from "For a change to the BES Cyber System" to "For a change to the BES Cyber System or Associated Systems or Associated Assets". Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold. Regarding CIP-010-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend removing "where technically feasible" from 2.1 since the remaining words should not need an exception.
No
For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend changing 3.2 from "in a production environment." to "in a production environment or a test environment." to allow Entities more flexibility in meeting this Requirement.
No
Request clarification on 1.1. Some interpret this Requirement as what is the Entity's process for identifying BES Cyber Systems Information. If correct, the Measure should be "show me the methodology (document)." Others interpret these Measures as labeling BES Cyber System Information. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Regarding CIP-011-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are

different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5.\ There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Request that footnote 2 in 2.1 be moved into that Requirement.

No

The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Otherwise, this Scenario table is confusing because it repeatedly uses 12 months while the earlier text uses 18 months. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Since Version 4 has not been yet approved by FERC, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. A summary of comments applicable to more than one standard: • Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • Request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5. A fiftieth question should have been included in this comment form asking for general comments or concerns. A question asking general comments should be included as part of every comment form posted to the industry. Regarding CIP-003-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

Individual

Michelle Denike

Wolverine Power Supply Cooperative, Inc.

Yes

Definition needed for BES Cyber System Impact.

Yes

High and Medium Impact Ratings use the term "adversely". This needs to be defined. This is too subjective of a term. Under 2.13 what is meant by the term "control" in (2) generation control centers

that "control" 300 MW or more of generation? Does this mean physical control only or does it include verbal commands? Also, does the 300 MW refer to name plate rating or some other method AND is that 300 MW only for BES generation or all generation that generation controls?
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
What is the difference between "provisioned" and "authorized"?
No
7.5 The term "extenuating" can be interpreted many different ways. Clarification is needed here.
Yes
No
R1.1 and R1.2 Clarity is needed for the terms "restrict" and "control and secure".
No
Yes
No
R1.6 The term "sufficient" is very subjective and needs to be clarified.
Yes

Yes
Yes
Yes

Individual
Ron Donahey
Tampa Electric Company
No
In general, Tampa Electric supports the Comments from EEI for CIP002 with the following additional clarifications and suggestions: Tampa Electric suggests that SDT provide examples of potential assets for control center, transmission substations, and power generation in each type (BES Cyber System, BES Cyber Assets, Associated Electronic Control & Monitoring, Associated Physical Access Control, Electronic Access Point, etc.) How far does the BES Cyber System extend? EMS is definitely a BES Cyber System; does it extend to the switches, routers, time & frequency devices, Digis, Front End Processors etc.? Tampa Electric recommends that the SDT improve the definition of the BES Cyber Asset related to "adversely impact" one or more BES Reliability Operating Services in order to provide clarity. The SDT may wish to consider the current definition of Adverse Reliability Impact in the NERC Glossary of Terms. Alternatively, adversely impact should be defined as an "impact greater than the Reserve Sharing Group"; otherwise the term is vague. Tampa Electric believes that the definition of Transient Cyber Assets is too broad and could include USB, CD, and external drives. It should be focused on equipment that includes a processor such as a laptop pc or mobile computing device.
No
Tampa Electric supports the Comments from EEI for CIP002 Attachment 1 with the following additional clarifications and suggestions: For Control Centers, substations and generation – Tampa Electric suggests that SDT provide examples of assets in each type of this new breakout/definition (BES Cyber System, BES Cyber Assets, Associated Electronic Control & Monitoring, Associated Physical Access Control, Electronic Access Point, etc.) Tampa Electric also requests that the SDT provide supporting documentation similar to Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets. Tampa Electric also notes that significant effort is required to classify BES CS as High, Medium or Low Impact with very little differentiation within the actual requirements of the standards themselves. At a minimum, all VSLs should be evaluated to determine if the levels of severity should mirror the impact categorization. Tampa Electric also suggests the following for consideration: 2.1. Generation with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. This language does not address the following: Under Guidelines and Technical Basis, on page 24, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of generation capability higher than 1500 MW are adequately protected. Tampa Electric recommends that the item 2.1 be re-worded to incorporate the concept of only generation systems with common mode vulnerabilities. 2.12: Tampa Electric recommends that the Standard Drafting Team review of the Application Guidelines related to 2.12. 2.12 define as Medium Impact the 300 MW UVLS or UFLS; there is a reference to 2.13 for UVLS/UFLS. We believe this is a typo and should be 2.12. 2.13: Tampa Electric recommends SDT review of the Application Guidelines related to 2.13. The criteria includes "generation control centers" (lower case); however, on page 30, the Application Guidelines specifies "Transmission Operators and Owners Control Centers" (upper case). Since Control Center (upper case) is a defined term, it is unclear if "generation control center" (lower case) is a newly introduced term and exactly what this is referring to. For example, is this referring to a single control room at a single generation facility that controls more than 300MW or is it referring to a control center for multiple generation facilities?
No
Tampa Electric agrees with the EEI comments with the exception of their suggestion to add the requirement to identify lows. Tampa Electric proposes the identification of Low Impact BES CS at a Facility level, not by listing all the Cyber Assets associated as this would add administrative burden and not provide additional BES CS security or BES reliability. 1.2. Evidence Retention - For instances where the evidence retention period specified below is shorter than the time since the last audit, Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer. Tampa Electric recommends that the document retention period should follow the requirement; as stated, the evidence retention period is open ended.
No
Tampa Electric agrees with the EEI comments.

No
Tampa Electric is concerned that the time based VSLs for updating documentation are too severe based on the potential risk to the BES. We propose that updating documentation should be categorized to allow a longer period of time before moving from low to moderate VSL.
No
Tampa Electric agrees with the comments submitted by EEI. Additionally we recommend that the following be added to the Measures: or, a corporate level policy naming the CIP Senior Manager.
No
Tampa Electric agrees with the comments submitted by EEI. Additionally Tampa Electric recommends changes to Guidelines and Technical related to Requirement R2: 2.2 3rd bullet: Identification of trusted and untrusted resources – Tampa Electric suggests a clarification of the definition of resources to indicate whether a resource is a person, a device, a system, or something else. 2.3: Are these bullets to be considered as requirements of the standard e.g. CIP005? 2.4: Monitoring and logging of egress will place undue burden upon the responsible entity. These bullets are not included in CIP-006 except for logging for visitor exit which is accomplished via the Visitor Control Program. Should they be including this guidance in CIP-003 or should this be included in the standard to which it is applicable? 2.9: Information Protection bullet 2 notification of unauthorized information disclosure. This does not appear to be a requirement of the standard.
No
Tampa Electric agrees with the comments submitted by EEI.
No
Tampa Electric agrees with the comments submitted by EEI. Additionally we note that the Measures—2nd bullet requires extensive recordkeeping with little security benefits.
No
Tampa Electric agrees with the comments submitted by EEI. Additionally we question whether this implies a signature form. Requiring a signed document for each change of an approver places an undue administrative burden. These updates should go through the Entity's normal approval process. Tampa Electric requests clarification of the first sentence of Requirement R5, specifically does this requirement apply only for those CIP requirements that have a "required approval"? For Measure M5 – 3rd bullet indicates that the CIP Senior Manager approves the delegations for physical security also. We recommend that this measure be re-stated to state that delegations be approved by a member of management or delegated by a member of management but not the CIP Senior Manager. For many organizations, personnel responsible for approvals will span many different departments, many of which may not be under the direct control of the CIP Senior Manager. This requirement places an undue burden on such organizations by requiring CIP Senior Manager's involvement in personnel changes for delegation throughout the organization.
No
Tampa Electric agrees with the comments submitted by EEI. Additionally we note a typo (from change2 to change 2) Please refer to comments in question 10 above related to undue burden.
No
Tampa Electric agrees with the comments submitted by EEI.
Yes
No
Tampa Electric agrees with the EEI comments. In addition, Tampa Electric considers that there will be an administrative burden (may have many versions of training programs tailored to individual roles). Maintaining such training programs, reporting, and compliance will be difficult with little additional security benefit to the Bulk Electric System.
No
Tampa Electric agrees with the EEI comments. Additionally, Tampa Electric is concerned over the statement in the Measures related to the identification of the date access was first granted, particularly for those individuals already in compliance with NERC CIP version 3 requirements since that was not previously tracked.

No
Tampa Electric recommends modification of this requirement to include the use of a National Criminal Research Database which would cover all of these requirements and show reasonable due diligence. Individual background verifications at all locations of residence, employment, and education is less thorough and creates more of an administrative burden for recordkeeping.
No
Tampa Electric recommends modification of this requirement to include the use of a National Criminal Research Database which would cover all of these requirements and show reasonable due diligence. Individual background verifications at all locations of residence, employment, and education is less thorough and creates more of an administrative burden for recordkeeping.
No
Tampa Electric agrees with the comments from EEI. In addition, Tampa Electric offers the following concern: The measures for 6.3 and 6.4 indicate that a Registered Entity needs to verify the list of who has access against a listing of those who have been authorized. The wording is unclear on what this means.
No
Tampa Electric agrees with the EEI Comments. Reassignments may also be processed retroactively, and the requirements should take this into account.
Yes
No
Tampa Electric agrees with the comments submitted by EEI. In addition, for Requirement 1.3 Tampa Electric requests that the SDT provide clarification on what is meant by “explicit access”. Rules can include group objects for cyber assets or port strings. Stating “explicit” could be construed to mean all objects or ports must be explicitly stated. Is it the SDT’s intent that an Entity must explain the specific criteria for each and every Cyber Asset granted access through the access point? Or is it sufficient to provide explanations for groupings of assets? Requirement 1.5 seems to indicate that an Entity would need IDS at each EAP (i.e., host IDS). The “Guidelines and Technical Basis” section has a very good statement concerning communications. The wording excludes serial, non-routable connections. This wording needs to be included in the actual requirement – similar to 1.2 and 1.3. Tampa Electric recommends that the requirement allow for technical feasibility exceptions or deployment of alternative measures of network based IDS where host based IDS may not be possible.
No
Tampa Electric agrees with the comments from EEI.
No
Tampa Electric agrees with the comments from EEI on VRF and VSLs.
No
The language requires significant clarification. Tampa Electric agrees with the EEI comments.
No
Tampa Electric agrees with the EEI comments. The version lacks clarity.
No
Tampa Electric agrees with the EEI comments.
No
Tampa Electric agrees with the comments from EEI.
No
Tampa Electric agrees with the changes proposed by EEI for Requirement 1.1. is a major clarification that greatly reduces the scope of ports that must be included for compliance.
No
Tampa Electric agrees with the comments from EEI for Requirement 2.1.
No
Tampa Electric considers that R3.4 introduces a cyber asset that Entities have not yet had to identify or account for. This will make it difficult to prove compliance. Please also refer to our concerns in the

definitions question 1 related to Transient Cyber Assets.
No
Tampa Electric agrees with the comments submitted by EEI for R4.3 and R4.4. In addition, Tampa Electric shares the following comments: 4.1 Tampa Electric is concerned that there are devices that do not produce the level of event logging that is required. Recommend adding “where technically feasible” to the requirement. 4.2 – Requires alerts for events, but fails to specify alerts for security. Recommend that the requirement state “Generate alerts for security events that…” 4.5-Requires a manual review of sample of logs every two weeks. This requirement provides no security benefit; it is unclear as to what an adequate sampling would be. The requirement is redundant, given the other requirements in R4, and should be removed entirely.
No
Tampa Electric agrees with the comments submitted by EEI. Requirement 5.2 could be interpreted that the CIP Senior Manager must authorize each individual use of administrator and shared default accounts rather than the individuals who have the authority to use those accounts. We suggest that the SDT delete this requirement.
No
Tampa Electric agrees with the comments from EEI.
No
Tampa Electric agrees with the comments from EEI. Additionally Tampa Electric proposes a format change on R 1.3 Measures as follows: Proposed format change o Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of; ♣ BES Cyber Security Incident response personnel, ♣ BES Cyber Security Incident handling processes or procedures, ♣ Communications processes or procedures.
No
Tampa Electric agrees with the comments from EEI. For Part 2.2 Tampa Electric recommends that the Standards Drafting Team consider adoption of the Homeland Security Exercise and Evaluation Program described below: Rationale: The homeland Security Exercise and Evaluation Program https://hseep.dhs.gov/pages/1001_About.aspx#TerminologySection1 “There are seven types of exercises defined within HSEEP, each of which is either discussions-based or operations-based. Discussion-based Exercises familiarize participants with current plans, policies, agreements, and procedures, or may be used to develop new plans, policies, agreements, and procedures. Types of Discussion-based Exercises include: Seminar. A seminar is an informal discussion, designed to orient participants to new or updated plans, policies, or procedures (e.g., a seminar to review a new Evacuation Standard Operating Procedure). Workshop. A workshop resembles a seminar but is employed to build specific products, such as a draft plan or policy (e.g., a Training and Exercise Plan Workshop is used to develop a Multi-Year Training and Exercise Plan). Tabletop Exercise (TTX). A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. TTXs can be used to assess plans, policies, and procedures. Games. A game is a simulation of operations that often involves two or more teams, usually in a competitive environment, using rules, data, and procedure designed to depict an actual or assumed real-life situation. Operations-based Exercises validate plans, policies, agreements and procedures; clarify roles and responsibilities; and identify resource gaps in an operational environment. Types of Operations-based Exercises include: Drill. A drill is a coordinated, supervised activity usually employed to test a single specific operation or function within a single entity (e.g., a fire department conducts a decontamination drill). Functional Exercise (FE). A functional exercise examines and/or validates the coordination, command, and control between various multi-agency coordination centers (e.g., emergency operation center, joint field office, etc.). A functional exercise does not involve any "boots on the ground" (i.e., first responders or emergency officials responding to an incident in real time). Full-Scale Exercises (FSE). A full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, emergency operation centers, etc.) and "boots on the ground" response (e.g., firefighters decontaminating mock victims). “
No
Tampa Electric agrees with the comments from EEI.
No
Tampa Electric agrees with the comments from EEI.

No
Tampa Electric is in support of the comments from EEI for CIP-009-5 R1.
No
Tampa Electric is in support of the comments from EEI for CIP-009-5 R2.
No
Tampa Electric is in support of the comments from EEI for CIP-009-5 R3.
Yes
No
Tampa Electric supports the comments from EEI. Additionally, Tampa Electric submits the following comments for consideration: R1.1.3 Recommended language to requirement: “Any commercially available application software (including version) intentionally installed on the BES Cyber Asset for normal and emergency operation.” Measures: Tampa Electric considers that the language is unclear as to what are “required items” – Does this mean based on ports & services or normal/emergency operation of the asset? Suggest the following wording change: “required items as identified in R1.1.1 through 1.1.6 of the baseline configuration” R1.2 Propose that the CIP Senior Manager delegation be addressed. Delegation process as stated in CIP-010 creates an administrative burden for the CIP Senior Manager. Tampa Electric recommends that this measure be re-stated such that delegations be approved by a member of management or delegated by a member of management but not the CIP Senior Manager.
No
Tampa Electric supports the comments from EEI.
No
Tampa Electric supports the comments from EEI.
No
No
Tampa Electric agrees with comments submitted by EEI. In addition, Tampa Electric recommends the following: Add phrase “information protection” as follows: “Each Responsible Entity shall implement one or more documented information protection processes that collectively include each of the applicable…” R1.1 – insert “readily”, e.g., “One or more methods to readily identify…” R1.2 – table headings have typos (Part, Part, Part). Measures – 1st bullet – change to “Records indicating information that is stored, transported, and disposed of in a secure manner, consistent with the documented processes.” 2nd bullet – Current language: Records from an information management system containing electronic copies of BES Cyber System Information with user access implemented on a need-to-know basis; Proposed language: Records demonstrating that access to systems containing protected BES Cyber System information is implemented on a need to know basis. 1.3 - table headings have typos (Part, Part, Part).
No
Tampa Electric agrees with the comments submitted by EEI. In addition, Tampa Electric suggests the following: Insert ‘storage media re-use and disposal’ in front of ‘processes’. Also in the guidelines for R2, an analysis of whether a BES Cyber System can be released is mentioned – does this analysis need to be documented and stored as evidence? R2.1 Insert ‘storage’ in front of ’media’ in the requirement. For Measures, add phrase to sentence: “, or that information residing on the storage media is encrypted.” Definition in footnote should be added to definitions document. 2.2 Insert ‘storage’ in front of ’media’ in the requirement. For Measures, add phrase to sentence: “, or that information residing on the storage media is encrypted.”
No
R2 – lower VSL could be if process not documented but we are performing. Moderate VSL could be if process not followed in certain situations. VSLs should take into account extent of condition, e.g., 1 tape not degaussed – that shouldn’t be high severity.
No
Tampa Electric recommends that any requirements that are to be performed prior to or on the

effective date of the standard (“initially upon the effective date of the standard) be included in the Implementation Plan rather than in the body of the standards/requirements.
Individual
Michael Schiavone
Niagara Mohawk (National Grid Company)
Yes
There has been a significant change in the framework from version 4 to version 5 regarding definitions and core concepts such as Critical Assets, Critical Cyber Assets, etc. These proposed changes are not a requirement of FERC Order 706, do not enhance cyber security controls and create administrative burdens when migrating to version 5. There should be a correlation between BES Cyber Systems and the facilities that these systems serve. The current version of the CIP standards provides the correlation and recognize that systems (CCAs) do not operate independently of facilities (CAs). Therefore, applying physical and electronic controls is more transparent. We propose maintaining the current Critical Asset and Critical Cyber Asset definitions and concepts. High, Medium and Low categorizations can still be utilized with the legacy CA and CCA concepts. Regarding the use of the term “annual” throughout the standards, we suggest that the registered entity be allowed to maintain it’s own definition of “annual” based on CAN-0010 guidelines. 1) For all definitions please include the old term that the new term is replacing, as applicable 2) The time periods included in the first and second sentence of the definition of “BES Cyber Asset” are confusing. The 15 minutes discussed in the first sentence and the “delay” discussed in the second sentence are unclear. Suggest re-wording as follows: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The 15-minute period begins to run when the asset is operated, mis-operated, or fails to operate when necessary, regardless of the time period between the asset was degraded or misused and the time the asset is then operated, mis-operated or fails to operate when necessary. 3) BES Cyber System Definition - Maintenance Cyber Asset needs to be defined or if appropriate changed to Transient Cyber Asset
No
Yes
Yes
Yes
Yes
Yes
Yes
No
We recommend eliminating this requirement and moving it into CIP-004 R2 and include policy as part of the training required. This way, all awareness and training would be in CIP-004.
No
We propose retaining the current language in CIP-003-3 R2
Yes
There should not be a foot note in the standard – make this part of the requirement.
No
R.2 – We suggest a "Lower" VSL for "The Responsible Entity has implemented the required cyber security policy or policies but has failed to adequately document the policy or policies." R.4 – We suggest Lower to Severe VSLs be based on a failure to take action, rather than a specific number of

employees who are aware. As drafted, it would be a "high" violation to miss one single employee. That seems overly strict and does not match well with the requirement and measures, particularly when measures suggested includes making an internet posting. We suggest the following: "Lower" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but has not adequately documented the measures"; "Moderate" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 30% -50% of individuals who have access"; "High" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 50% -70% of individuals who have access"; and "Severe" VSL = "Registered entity has taken no measures to make any individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function OR Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 70% or more of individuals who have access" R.5 - Why do the VSLs begin at medium for the failure of one delegation? We recommend "Lower" VSL = failure of one delegation; Moderate = failure of two delegations; High = failure of three, and Severe = failure of "four or more". R.6 – We suggest VSLs structured similarly to CIP-002 - Lower = Change to one delegation was not documented within 30 days, but was documented within 31-41 calendar days of the effect vive date ; Moderate = Change to two-three delegations was not documented within 30 days OR change to one delegation was not documented within 30 days, but was documented within 42-52 days of the effective date; High = Change to three-four delegations was not documented within 30 days OR Change to one delegation was not documented within 30 days, but was documented within 53-63 days of the effective date; Severe = Change to more than four delegations was documented within 30 days of the effective date OR Change to one delegation was not documented within 74 days of the effective date.
Yes
No
We do not believe that role based training is necessary. The personnel performing the job functions are familiar with the various controls due to their job requirements. General training on CIP, as required under current version, is all that should be required.
Yes
Yes
Yes
No
There is no added security by requiring the CIP Senior Manager or delegate to authorize access. We suggest using legacy wording that only requires access to be authorized.
Yes
No
It seems harsh to include the failure to document a security awareness program as a severe VSL. We recommend the following as a "Lower" VSL "The Responsible Entity implemented, but failed to document a security awareness program" and change the Severe VSL to "The Responsible Entity failed to implement and document a security awareness program." Additional comments around adding “Missed a quarter and/or target audience (authorized physical or authorized electronic)?” R.2: No comments. R.3: The annual training requirement assumes that the initial training was completed before access was granted, therefore, missing a small number of employees with the subsequent annual training does not necessarily indicate high risk to the bulk electric system because these employees presumably had received prior training when their access was granted. We recommend a tiered approach to the VSLs for missing the annual training requirement so that failing to meet the

annual requirement for a low percentage of employees (like 10% or less) is a lower VSL, failing annual requirement for between 11-20% is moderate, failing the annual requirement for 21-30% is high, and failing to meet the annual requirement for over 30% OR failing to do the initial training is severe. R.4: No comment R.5: A documentation error should not be a "severe" VSL. Delete the "OR/documentation" part from the Severe VSL and make a Lower VSL that reads "The Responsible Entity implemented, but failed to document a process for personnel risk assessments." R.6: For most utilities, there could be 100s of employees with access, and it seems unrealistic to base the VSLs on one failure with regard to one or two employees. We recommend changing the values in the Moderate - Severe to percentages of employees 10%, 20%, 30%or more. R.7: Same comment as R.6 - change values of one to three employees to percentages.
Yes
No
Requirement 2.2 specifies encryption for all Interactive Remote Access sessions, but does not specify where the encryption is required. If the intent is to require encryption from the user to the Intermediate Device the requirement should specify that clearly. Not all assets currently support encryption, so requiring encryption from the Intermediate Device to the Asset is not practical nor necessary if encryption is being employed outside of the ESP.
No
R.1 and R.2: There should be lower VSL where the processes listed on the table are implemented but not documented.
Yes
Yes
Yes
No
R.1: There should be lower VSL where the processes listed on the tables are implemented but not documented. Add to the Lower VSL: "OR the Registered entity has implemented but failed to document the required physical access controls" R.2: There should be lower VSL where the processes listed on the table are implemented but not documented.
Yes
Yes
No
Requirement 3.5 requires logging of each Transient Cyber Asset connection. This is not practical as many assets do not have the capability of logging when someone makes a direct physical connection to the asset. Many assets are not capable of logging to centralized logging systems. Also, in a typical day, and engineer in the field may connect a Transient Cyber Asset to many different assets and it would be impractical for one to log each connection.
No
4.1 - The intent of 4.1 as written in the Guidelines and Technical Basis section is inconsistent with the requirement. The guidance states that “It is not the intent that if a device cannot log a particular event that a TFE must be generated”. If the intent is to not be out of compliance when a device cannot log certain events, it should be stated as such in the requirement. 4.3 - The activity level of some devices is such that they may not generate a logged event every day. Therefore, responding to an event failure with a day may not be possible. 4.3 & 4.5 – there is a conflict between these two. 4.3 requires a response to logging failures before the end of the next day. But, 4.5 requires bi-weekly sampling of logged events which would uncover logging failures. If the logs are being reviewed bi-weekly then logging failures may not be detected and responded to within the next day.
No

Items 5.4 & 5.6 in Table R5 includes the phrase “where technically feasible”. Does that mean a TFE will be allowed? If so, we believe that phrase should be removed and replaced with “as supported by the BES Cyber System” to eliminate need for TFE
No
R.1 We have the same comment here about percentages for open ports (similar theme from above). What is written in high should be in moderate. What’s in severe should be broken down by percentages/numbers. R.2 Consider severity of patch as recommended by the vendor and the percentage of assets that may not have had a remediation plan associated with that patch. R.3 Consider putting some wording in here around the percentage.
No
There is some concern that multiple plans would prevent one single entry point into the Cyber Security Incident Response Process. We’d like to make the argument that only one plan is necessary and supporting documentation can be created as necessary that supports that plan
No
The Applicability section of the tables refers to “All responsible entities”. We suggest using the same wording that all the other standards use (High Impacts, Medium Impact, Associated, etc) In R 2.2 In the first sentence, we recommend replacing the word “implement” with “exercise.” This is really about exercising the plan on a regular basis as the plan is already implemented. In 2.3, the "measure" for "relevant documents" does not give adequate guidance to the industry regarding what documents may be acceptable to demonstrate compliance. The "measure" indicates any "dated documentation related to" the reportable incident may be accepted. Please give some additional examples of the specific types of dated materials could be considered acceptable.
No
3.1 The terms “accuracy” and “completeness” are referenced but in terms of completeness there’s not a specific benchmark to compare the document again what should be quantified as complete. The suggestion is again to define a minimum set of information that would be expected in an Incident Response Plan. 3.2 - We recommend that clarity be added to ensure that language represents that review occurs 30 days after closure of the incident rather than invocation; rationale is that you might still be remediating and won't have learnt all lessons. We recognize the importance of the requirements to review the lessons learned, update the Incidence Response plan, and communicate the updates. However under the current structure it creates a rolling compliance effort following each incident. That is, an auditor will require that after each incident one has recorded lessons learned review, changes to the response plan or that none were necessary and updated communications or that none were necessary. It would be easier to update the plan on a quarterly basis based on the previous quarter’s incidents and not have so many auditable events to track.
Yes
No
1.5 – The requirement to preserve data for analysis or diagnosis may slow down the recovery process. There are times when recovery is urgent and must be done in a timely fashion. Is your intent to include this when you say “where technically feasible”? If so, language should be added spelling it out.
No
2.2 – We recommend removal of the phrase “and reflects current configurations” from the requirement. It is acceptable to have backup information that is less than current configuration and still perform a successful recovery. If this phrase is not removed, it will require a backup to be taken and tested for even the most minor configuration changes which is unnecessary.
Yes
No
We recommend the following VSLs for number of days until plan is reviewed in R3: 31-41 days = Lower, 42-53 days = Moderate, 53 plus is High and Severe for never updating plan. We also recommend the following VSLs for number of responsible personnel that the plan updates have not been communicated to: 1 person missed = Moderate, 2-4 = high and 5 or more is severe. We like the

VSLs in CIP-010 R3. These recommendations attempt to make CIP-009 R3 consistent to CIP-010 R3
Yes
Yes
No
We recommend considering emergency equipment replacement (partial outage) as “Exceptional Circumstances” . Based on the nature of our typical outages we would consider this practice to hinder the restoration efforts and bringing systems back on-line in a timely manner. We would certainly be good with language that allowed us to bring systems back on-line, ensure they are stable and then run a scan.
No
We recommend the following VSLs for number of days until documentation is updated in R1: 31-41 days = Lower, 42-53 days = Moderate, 53 plus is High and Severe for never updating documentation. R3 We like this structure. We’ve suggested this approach a number of times We aren’t talking about whether or not this is violation, but rather about the severity of the violation and then rating the severity. We think this is a really good approach.
Yes
No
The footnote here should be part of the requirement
No
We recommend the following VSLs on R 2: If the process to prevent unauthorized retrieval wasn’t done on 1 device that would be low 2-5 moderate, more than 5 is high
No
Due to the current status of version 4 (not FERC approved), there is potential for overlap of implementation with version 5 that could create extensive rework in a short period of time. This will cause an unnecessary expense to entities while not providing any additional cyber security benefit.
Individual
Jonathan Appelbaum
United Illuminating Company
Yes
• BES Cyber Security Incident – Proposed Change o Original Text – A malicious act or suspicious event that: ♣ Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or ♣ Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or ♣ Results in unauthorized physical access into a Defined Physical Boundary. o Proposed Change – A malicious act or suspicious event that: ♣ Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or Defined Physical Boundary ♣ Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System. o Rationale – The revised definition leverages legacy language from NERC’s ‘Glossary of Terms Used in NERC Reliability Standards,’ combining Electronic Security Perimeter and Defined Physical Boundary into the single bullet. It also raises ‘physical attempts to compromise’ into the category of BES Cyber Security Incident. • BES Cyber Security Incident – Proposed Change o Original Text – A malicious act or suspicious event that: ♣ Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or ♣ Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or ♣ Results in unauthorized physical access into a Defined Physical Boundary. o Proposed Change – A malicious act or suspicious event that: ♣ Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or Defined Physical Boundary ♣ Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System. o Rationale – The revised definition leverages legacy language from NERC’s ‘Glossary of Terms Used in NERC Reliability Standards,’ combining Electronic Security Perimeter and Defined Physical Boundary into the single bullet. It also raises ‘physical attempts to compromise’ into the category of BES Cyber Security Incident. o Original Text - Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and

Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans. o Proposed Change – Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain Medium or High BES Cyber System Impact designations; equipment layouts that contain Medium or High BES Cyber System Impact designations; BES Cyber System recovery plans; and BES Cyber System incident response plans. o Rationale – Information for Medium and High impact Bes cyber Systems location should be protected. This is consistent with the notion of protecting those assets that have greater impact on the BES and also all BES Cyber systems per CIP-002-5 have at a minimum a Low impact. • BES Reliability Operating Services – The services should focus on real time and hour ahead horizons. This horizon presents risk to reliability that requires immediate reaction. A service that occurs in the Current Day horizon can be reacted to in a reasoned and controlled manner. Additionally, what is Change Management as a reliability service? • Other terms which would benefit from definitions • Adverse - The SDT is utilizing the concept of "adverse impact" to properly scope High to control center cyber assets but the term adverse is not defined. UI is concerned that the universe of cyber assets supporting a TOP/BA/RC SCADA or EMS is not limited to the assets supporting the application and may extend into the substation and field RTU and devices. o Annual – Propose use of definition within CAN-0010 o Impact o Security Plan o Associated • Existing definitions that would benefit from alternative wording o Electronic Access Point ♣ EAPs typically have two (or more) access points and control access into an ESP (logical network) from a less trusted network or communication interface. The current wording could be applied to any port on a network switch within an ESP and fails to focus on interfaces where traffic does flow from a less trusted network to a more restricted network within an ESP. o Electronic Security Perimeter ♣ Suggest retaining the concept of logical network. This provides an easier means to identify "Associated Protected Cyber Assets" as they could be any cyber assets on the same logical network which are not identified as a BES Cyber Asset or BES Cyber System.

Yes

• Control Centers should be capitalized at the end of section 2.13 on page 17. • There should also be a column for LSE in the table provided on page 18. • The services should focus on real time and hour ahead horizons. This horizon presents risk to reliability that requires immediate reaction. A service that occurs in the Current Day horizon can be reacted to in a reasoned and controlled manner. • Additionally, what is Change Management as a reliability service? • On page 20, under the category "Balancing Load and Generation," Non-spinning reserve, the use of 'ramp rates' is typically associated with modeling programs not typically used as real time operation information and should be removed. • Restoration of BES – 'coordination' all by itself lacks context and should include additional words to better frame the intent. • UI is concerned that the universe of cyber assets supporting a TOP/BA/RC SCADA or EMS is not limited to the assets supporting the application and may extend into the substation and field RTU and devices. The SDT is utilizing the concept of "adverse impact" to properly scope High to control center cyber assets but the term adverse is not defined.

No

1. Applicability – (4.2.1 and 4.2.2) reference to UFLS and UVLS is a point of concern. Current wording implies that every distribution feeder which is part of a UV or UF load shedding scheme is now in scope, with all distribution level devices now BES Cyber Assets. This may greatly expand the scope greatly into the distribution level. UI proposes Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) under a common control system as required by its regional load shedding program. 2. CIP-002-5 R1 – Propose content change a. Original Content – Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. b. Proposed change - Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and

Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. Low Impact BES cyber systems support Bulk Reliability Operating Services but are not mentioned in the bright line criteria as noted in Attachment 1. However, failure of these cyber systems may adversely impact (i.e. not remain in the NERC prescribed category ranges) the voltage and/or frequency of the connected Bulk Electric System. Low Impact BES Cyber Systems do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning] c. Rationale – The original definition, as worded, creates the impression that all other cyber assets qualify as Low Impact, and does not communicate the criteria within the definition of BES Cyber Asset as a cyber asset that "if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The proposed rewording contributes towards ensuring only assets which have an impact on the BES are the focus of the CIP Standards (and may ensure a more rapid adoption of the Version 5 Standards). 3. The "Rationale – R1" box uses the term "Cyber Systems," which is not a formal term. Suggest changing the case to avoid confusion. 4. The last sentences of R1 and M1 conflict with each other, providing mixed messages specific to Lower Impact BES Cyber Systems/Assets. While Requirement 1 implies there is no need for discrete identification, Measurement 1 discusses evidence for categorizing Low Impact BES Cyber Assets/Systems. 5. Requirement 1.1 a. There is a missing word – "…within 30 calendar days of <when> a change to BES Elements and Facilities is placed into operation. b. UI proposes that the phrase "BES Cyber Assets and BES Cyber Systems" used in this requirement be changed to "BES Cyber System". A single BES Cyber Asset may comprise a BES Cyber System. The Requirement should be to list the BES Cyber System and the impact categorization. This appears to match the diagram on page 7 that identified BES Cyber Systems. c. The phrase "placed in operation" requires clarification. Facilities (e.g. HVDC Converters, SVC, FACTs, Generators) are often initially tested and commissioned connected to the BES but are not in commercial operation. Being specific such as "placed in operation, post-commissioning testing". d. UI requests clarification on the composition of the list required by this Standard. A BES Cyber system may be composed of multiple BES Cyber Assets. Would this list only contain the single BES Cyber System , or the five BES Cyber assets, or the BES Cyber System with the five BES Cyber assets listed? For example a High impact Control Center has an EMS with 5 BES Cyber Assets in the Control Center (two servers and three workstations). For compliance to this Requirement is the EMS listed, or the 5 BES Cyber assets? e. UI requests on the requirement to update. If a single BES Cyber Asset is added to an existing BES Cyber System does that initiate the 30 day update process for the list? For example if a Control Center with a High Impact adds a single workstation to an existing EMS, does that require a 30 day update to the list? A workstation is not a BES Element or Facility, but is a BES Cyber Asset.

No

1. Rationale R2 – Propose a content change: a. Original Text - The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. b. Proposed Change - The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems have been properly identified and categorized. 2. R2 – Proposed Change a. Original Text – The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. b. Proposed Change – The Responsible Entity shall have its CIP Senior Manager or delegate annually approve the identification and categorization required by R1. c. Rationale –Instances in which tasks are required to be completed in advance of the effective date of the standard should be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame. 3. M2 – Proposed Change a. Original Text – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. (R2) b. Proposed Change – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate annually approve, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems. (R2) c. Rationale –

The requirement only asks for Senior Manager (or delegate) approval. Instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.
No
1 – The Violation Risk Factors do not intuitively align with Violation Severity Level (VSL). Requirement 1 assigns a 'High" VRF independent of the potential low or no risk associated with instances in which BES Cyber Assets or BES Cyber Systems are assigned risk levels higher than those required. 2 – For the Last Paragraph VSL's within R1 (failed to update its documentation), EEI proposes the following time periods: Lower – More than 30, but less than or equal to 60 calendar days Moderate – More than 60, but less than or equal to 70 calendar days High – More than 70, but less than or equal to 80 calendar days
Yes
Yes
UI supports the Guideline for what a Policy should contain. Sub-numbering (1.1 through 1.10) should be modified to 2.1 through 2.10.
No
Propose content Change 1. Original Content – Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 2. Proposed change –The cyber security policies require annual review and approval by the senior manager assigned pursuant to R1. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 3. Rationale – The proposed revision carries forward language from previous versions of the standard (CIP-003 R1.3) which captures the root intent while providing language which has already been vetted and approved within the industry. . Instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.
No
1. Draft 1 content – "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function." 2. Proposed revision – "The cyber security policy is readily available to all personnel who have electronic access or unescorted physical access to, or are responsible for Medium or High Impact BES Cyber Systems." 3. Rationale –The scope as written would include visitors. UI does not believe that a visitor should be made aware of the CIP Policy or portions appropriate to the visitor's purpose.. Additionally, making individuals who have access 'aware of elements' of the cyber security policy does not provide adequate guidance to ensure said individuals comply with the cyber security policy. An Entity should make the Policy available for viewing. The awareness of the meaning Policy should be conducted in the CIP-004 training.
No
Requirement 5 – propose use of legacy language: • The responsible entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, standards. Rationale – Overall responsibility and authority (from the legacy language) can accomplish "direct and comprehensive responsibility" and "clear authority" (from FERC Order 706) provides flexibility without the prescriptive requirement for the senior manager or delegate to be responsible for all individual detailed approvals and authorizations in the standards. Citing "all approvals and authorizations" as a Senior Manager was identified as a concern as it is open ended. There were concerns of the additional administrative burden which is not commensurate with the security benefits. Neither the Blackout Report Recommendation 43 nor FERC Order 706 identify the need to establish this administrative overhead. For Security and Reliability NERC should be concerned with the outcome of the approval process, that is, the proper authorizations are being granted by the Responsible Entity which is contained in the other CIP Standards.

No
Propose use of legacy language from CIP-003-3 R2.2: Changes to the senior manager must be documented within thirty calendar days of the effective date.
No
R4 VSL 1. This language cites a High VSL when 'not all' individuals have been made aware of elements of the cyber security policy. This seems to contradict the intent described in the R4 rationale in which 'it is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.' 2. Use a more gradual scale rather than a single instance of non-access subject to a High VSL, and total non-access (for all) being a Severe VSL.
No
From the Guidance "The security awareness program is intended to be an informational program, not a formal training program." But the Measure for R1 states "Evidence must include the documented security awareness program." UI observes that requiring a documented program as evidence conflicts with an informal compliance guidance. The Measure should state "Evidence may include a documented security awareness program, and additional evidence to demonstrate that this program was implemented such as, but not limited to, the quarterly reinforcement material that has been distributed."
No
1. The rationale for R2 should be reworded from "…contains the proper policies…" to "…covers the required policies…" 2. This extends beyond the guidance of FERC Order 706. Paragraph 435 of the order calls for identifying what "role and steps should be taken by the ERO to ensure quality and consistency of trainers." This requirement should identify what areas of the standards that the training program must include. 3. EEI members question whether this requirement satisfies paragraph 434 of Order 706 where "any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions could, even inadvertently, affect cyber security. 4. UI proposes the following change to R2 to conform to the rationale box. As written R2 may not be clear that not all topics listed in 2.1 through 2.10 is applicable to each role. Proposed change "Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems. For each role identified by the Responsibility Entity only include the topics in CIP-004-5 Table R2 – Cyber Security Training Program that are applicable to that role." 5. R2.6 – Requirement – Proposed word change a. Original - Training on handling of BES Cyber System Information and storage media. b. Proposed Change - Training on handling of BES High and Medium Impact Cyber System Information and storage media. c. Rationale – Rewording supports the applicability section. Since Low Impact Cyber Systems are not applicable, information specific to Low Impact Cyber Systems should not be in scope.
No
Measure 3.1 where it calls for the date access was first granted is a point of concern for both legacy employees (where it may be impossible) as well as new access since existing technology may not adequately capture and retain this information. Requirement 3.2 – Propose content change • Original content – Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months. • Proposed change – Require annual completion of the training specified in CIP-004-5, Requirement R2. • Rationale – The wording adopts the CAN-0010 approach for annual as defined within the registered entity.
No
1. R4.1 a. Version 5 standards should indicate whether previous PRA's would be valid for this requirement (especially within the context of 'initial'). b. Provide a clearer delineation to frame instances in which personal records are not readily available – vs. impossible to obtain 2. R4.2 – Retention requirements do not extend beyond 3 years, creating confusion regarding retention of 7 year cycle background checks. 3. R4.3 a. UI favors a process approach over a fixed pass/fail approach independent of the individual or circumstances involved, and propose that the SDT shift away from a criteria based approach. b. The application guideline provides guidance where it is 'not possible to perform a full seven year criminal history check.' 4. R4.4 – Provide language to cover contract employees where I9 verification can only be conducted by employers. Service providers also may have instances where certain individuals may be located in another country, and may access certain

BES Cyber Assets remotely.
No
Version 5 standards should indicate whether previous PRA's would be valid for this requirement
No
1. R6.1-3,6.4-6 – Propose use of language where access is appropriate for the roles and responsibilities rather than 'minimum necessary' a. 'Minimum necessary' as identified as difficult to prove within an audit context 2. 6.3 – Propose content change a. Original content – The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions. b. Proposed change – Access to BES Cyber System Information repositories must be authorized, except for CIP Exceptional Circumstances. c. Rationale – Senior Manager authorization (or management of delegations) provides additional resource and response impacts which do not provide enhanced security and may impact reliability efforts when recovery processes are activate. Ensuring access is authorized will satisfy security controls without adding unnecessary overhead.
No
1. R7.1 - There are questions in instances where resignations and/or terminations may be retroactive, which would introduce a challenge with revocation 'at the time of' events. 2. R7.2 – Transfers or reassignments should frame access changes when no longer needed rather than the date of the transfer (as cited in the Measure (i)). 3. R7.3 – a. Propose use of 'approved BES Medium and High Impact Cyber System Information repositories,' to frame an appropriate location in which information can be managed and controlled. b. Propose to include in Guidance that access to BES Cyber System Information is considered revoked for electronic storage is NOT dependent on revocation of user account to electronic files provided remote access has been revoked. Similarly if paper records or electronic access is contained in a controlled physical perimeter access to BES Cyber System Information is considered revoked once the credential to access the physical security perimeter is revoked".
Yes
No
The Version 5 approach (as described within the R1 rationale "Summary of Changes") of focusing on discrete Electronic Access points rather than a logical perimeter adds confusion when determining Associated Protected Cyber Assets. A discrete list fails to recognize the inherent controls and permissions within a logical network. Control of routable protocol should consider the inherent network/host identifiers embedded within the addressing scheme in which all devices with an identical network component of their address are peers within a logical network where access points do not serve as access control. Rationale for R1 – Propose content change • Original Text - The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks. • Proposed Change - The Electronic Security Perimeter serves to control traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic according to a specified rule set, and assists in containing any successful attacks • Rationale – Monitoring is not identified within any R1 requirements. Table R1 1. R 1.1 1. Applicability - Propose use of "External Connectivity" instead of "External Routable Connectivity (to include dial-up capability). 2. Propose removal of "and have been implemented" from the end of the measure statement to avoid tracking compliance on a 'per-device' basis, otherwise this would introduce the need for tracking this information for low impact BES Cyber Systems. 2. R 1.2 1. Applicability – modify to frame applicable Cyber Systems/Cyber Assets as those with External Connectivity. 2. Requirements – Propose content change 1. Original content – Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs). 2. Proposed change – Control and secure all External Connectivity through the use of identified Electronic Access Points. 3. Rationale – The focus within CIP-005 should be on EAP devices with External Connectivity. 3. R 1.3 1. Requirements – proposed change 1. Original Text - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions. 2. Proposed

Change - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting access, denying all other access requests by default. 4. R1.4 – There were various interpretations of 'non-Interactive Remote Access,' which implies this requirement may need some additional clarification. This seems to be the only requirement where documentation of authentication measures appears within this standard. Consider removing 1.4 and modifying 1.2 to cover both rows.
No
1. Table R2 1. R2.1 1. Requirements – Request rewording to support placement of an intermediary device that may not be part of an ESP. 2. R2.2 1. Requirements – Propose clarification on viable termination points for encrypted traffic to support unencrypted traffic through Electronic Access Points. 2. Rationale – The ability to filter traffic effectively becomes much more difficult if the traffic is encrypted. Supporting technical implementation where encrypted is decrypted prior to allow for further access controls would benefit security capabilities. 3. Overall – Propose breaking table R2 into a Routable and Dial-Up categories to more effectively frame routable controls and dial-up controls without introducing confusion for the alternate approach.
No
1. Classifying instances where no documentation of compliance exists as severe is appropriate; instances in which a minority of non-compliance controls were identified within a primarily compliant program should be assessed a VSL with respect to the finding (page 17, bottom Severe VSL). 2. VSLs addressing 'each identified EAP' and 'all Interactive Remote Access' should be assessed as a sliding scale to consider whether lower/moderate/high may be more applicable.
No
1. Table R1 a. R1.1 i. Measures – Proposed Rewrite 1. Original Text – Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented. 2. Proposed Change – Evidence may include, but is not limited to, documented operational or procedure controls that have been implemented. b. R1.2 i. Measures – Proposed Change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs. 2. Proposed Change – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how access is controlled. 3. Rationale – FERC Order 706 did not ask for egress access controls. The additional criteria at the end of the measure extend beyond what FERC has asked for, with minimal security benefit. c. R1.3 i. Requirement – 'different and complementary' may not provide adequate guidance. Measure R1.3 only references 'different.' 1. Propose adding language to support single devices which may provide multiple access control measures (i.e. physical access card with PIN) ii. Measure – only mentions 'different' access control methods with no reference to complementary (as included within the requirement). d. R1.4 i. Requirement – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 2. Proposed Change – Issue alerts within 15 minutes (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 3. Rationale – The 15 minute criteria (Referenced in the 'Table of Compliance Elements,' page 21, R1 – High) provides greater clarity to satisfy alerting requirements. ii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs, or other evidence that documents that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. e. R1.5 i. Applicability – Presently states Associated Physical Access Control Systems. Is it Physical Access Control Systems Associated with all Low, Med, and High Bes Cyber Systems? I understood that wherever the Applicability uses Associated that there would be a Low/medium or High BES cyber system designation also. ii. Requirements – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 2. Proposed Change – Issue alerts within 15 minutes (to individuals

responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 3. Rationale – The 15 minute criteria (referenced in the 'Table of Compliance Elements,' page 20, R1 – High) provides greater clarity to satisfy alerting requirements. iii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. f. R1.6 i. Requirements – Proposed Change 1. Original Text – Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry. 2. Proposed Change – Log (through automated means or by personnel who control entry) of authorized individual's physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the authorized individual and date of entry. 3. Rationale – The addition of authorized provides additional segmentation from R2 (Visitor Control) access requirements.

Yes

No

Table R3 1. R3.1 a. This sub requirement cites tasks to be conducted 'prior to commissioning.' Since many controls are expected to be in place prior to V5 adoption, there should be language within the implementation plan to capture devices in use at the time the standard becomes effective. 2. Compliance a. 1.5.2 – Evidence retention should keep the existing 90 day period for physical access logs as extending this to 3 years can create extensive commitment in storage media, particularly for video monitoring.

Yes

The Table of Compliance Elements cites references to sub requirements that appear to be incorrect: • Lower – Part 1.7 should point to 1.6 • High – Part 1.6 should point to 1.5

No

R1.1 – Requirements – Proposed Content Change 1. Original Content – Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. 2. Proposed Change – Enable only logical accessible ports needed, including port ranges where required. 3. Rationale – The proposed language incorporates much of the legacy (CIP-007-3 R2.1) language. The additional requirement to document the need for remaining logical ports extends beyond what FERC Order 706 requests without adding security benefits. R1.2 1. Requirements – Content Change a. Original Content - Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. b. Proposed Change – Protect against the use of unnecessary physical input/output ports that could be used for network connectivity, console commands, or removable media by disabling, restricting, or use of signage. 2. Measures – Content Change a. Original Content - Evidence may include, but is not limited to, documentation stating specific or types of physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. b. Proposed Change - Evidence may include, but is not limited to, documentation stating specific physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage.

No

R2.1 1. Requirements – Content Change a. Original Content - Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. b. Proposed Change – Identify a source or sources that are monitored for the release of security related patches, or security updates for all related software and firmware associated with BES Cyber System or BES Cyber Assets. c. Rationale - Only security updates to software and firmware should be sourced. It is possible that at some point

security updates for a product will be sourced from a separate repository from non-security updates. 2. Measures – Propose striking the last sentence “The list could be sorted by BES Cyber System or source.” It introduces additional requirements with no clear security benefit or alignment with FERC Order 706.
No
1. R3.2 – Although CIP-007 v3 currently requires mitigation, UI believes that the actions to respond to a Virus (disarm or remove) is part of the CIP-008 Response Plan. The SDT used this approach in proposed R4.5. 2. R3.3 a. Include testing within both the requirements and measures as alluded to within the Application Guidelines (page 41). b. Measures – Format (i) and (ii) to a bulleted list signifying ‘or’ criteria 3. R3.4 a. Applicability – Propose deletion of Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems as they do not appear to be Transient Cyber Asset related. b. Requirements – Content Change i. Original Content - Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change – Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to Medium or High Impact BES Cyber Assets or Protected Cyber Assets. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. ii. Proposed Change – Evidence may include, but is not limited to, an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. iii. Rationale – Excised content introduced prescriptive criteria that introduced additional resources without clearly addressing the requirement. 4. R3.5 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems and Associated and they do not appear to be Transient Cyber Asset related. b. Requirements – Append “to Medium or High Impact BES Cyber Assets or Associated Protected Cyber Assets” to the end of the requirement. c. Measures – Content Change i. Original Text – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change - Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to Medium or High Impact BES Cyber Assets or Protected Cyber Assets.
No
R4 1. R4.1 a. Requirements – Content Change i. Original Content - Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. ii. Proposed Change – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. Devices that cannot log a particular event do not require a TFE to be generated. iii. Rationale – Content from the application guidelines has been introduced to promote the guidance that TFE’s are not required in instances in which devices cannot log a particular event. 2. R4.2 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control Systems as they are out of scope for this requirement. b. Requirements – Content Change i. Original Content – Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert. ii. Proposed Change – Generate alerts for events that the Responsible Entity determines necessary. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate real-time alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert; Screenshots showing how real-time alerts are configured. ii. Proposed Change – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate an alert; Screenshots showing how alerts are configured. iii. Rationale – Removed the usage of ‘real-time’ as it presents concerns demonstrating compliance. 3. R4.3 a. Requirements – Content Change i.

Original Text – Detect and activate a response to event logging failures before the end of the next calendar day. ii. Proposed Change – Activate a response to failures of event logging before the end of the next calendar day after identification. iii. Rationale – Some devices generate logs so infrequently that identification of logging failure may extend beyond any calendar day. The spirit of this requirement remains intact as one day remediation is required once the log failure is identified. 4. R4.4 a. Requirements – Content Change i. Measures – Content Change 1. Original Text – Evidence may include, but is not limited to, security-related event logs from the past ninety days and records of disposition of security related event logs beyond ninety days up to the evidence retention period. 2. Proposed Change – Evidence must include, but is not limited to, security-related event logs from the past ninety days. 5. R4.5 a. Requirements – Content Change i. Original Content – Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day. ii. Proposed Change - Review a summarization or sampling of logged events every two weeks to identify BES Cyber Security Incidents and potential event logging failures. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008. b. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred, and dated evidence showing that personnel were dispatched or a work ticket was opened to rectify the deficiency. ii. Proposed Change – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), and signed and dated documentation showing the review occurred. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008.

No

R5 1. R5.1 a. General Comment – The act of being presented a Log-On screen means that a person has accessed the BES Cyber System. The requirement should allow access to a BES Cyber System to perform the log-on/access process. b. Requirements – Content Change i. Original Content – Validate credentials before granting electronic access to each BES Cyber System. ii. Proposed Change – Authenticate user account access before granting electronic to each Medium or High Impact BES Cyber System or Associated Protected Cyber Asset, where technically feasible. iii. Validating credentials was seen as vague specific to technical compliance so authentication is offered as an alternate approach to satisfy the root requirement (and mirrors the language in the change rationale). The addition of technically feasible was made as technical capabilities currently in place may not adequately demonstrate compliance with this. 2. R5.2 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 3. R5.3 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 4. R5.4 a. Requirements – Content Change i. Original Text – Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. ii. Proposed Change – Procedural controls for initially removing, disabling, or changing default passwords, where technically feasible. For the purposes of this requirement an inventory of Cyber Assets is not required. iii. Rationale – The additional wording identify the multiple methods which can be used to mitigate default passwords. 5. R5.5 a. Requirements i. Change BES Cyber Systems to BES Cyber Assets throughout as password limitations should be identified to the device level. ii. Add language to 5.5.3 to cover instance where accounts may not be able to support password change to permit the entity specified time frame to be equal to the life-time of the BES Cyber Asset where technically required. 6. Please be consistent with the use of Term BES Cyber System versus BES Cyber Asset.

No

Violation Severity Levels 1. R3 a. Propose switching High and Severe Columns as the High captures instance in which no methods were deployed, Severe captures instances in which incomplete methods were deployed. b. The initial paragraph in Severe is duplicated in High. 2. R4 a. Moderate – delete ‘identify and implement methods to’ b. High – delete ‘identify and’ 3. R5 a. High – The initial

paragraph doesn't align with a requirement, propose striking.
No
1. General – Guidance or definitions should be provided to illustrate the expectation of this Standard. An Response Plan may solely contain the organizational structure, roles and responsibilities, and process to respond to an incident; but not include the specific steps required to resolve a specific type of incident on a specific BES Cyber Asset. For example I can describe an incident response for removing malware on a windows machine without being any more specific then contact Information technology group to remove Malware. 2. R1.1 1. Applicability – Content Change 1. Original Applicability ♣ All Responsible Entities 2. Proposed Applicability ♣ High Impact BES Cyber Systems ♣ Medium Impact BES Cyber Systems ♣ Associated Physical Access Control Systems ♣ Associated Electronic Access Control and Monitoring Systems ♣ Associated Protected Cyber Assets 3. Rational – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 3. R1.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rational – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 2. R1.3 1. Requirements ♣ The initial 'define' should be expanded to provide a complete sentence (i.e. An entities BES Cyber Security Incident Response Plan should include). 2. Measures – Content Change ♣ Original • Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of BES Cyber Security Incident response personnel, BES Cyber Security Incident handling processes or procedures, and communications processes or procedures. ♣ Proposed Change • Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of; o BES Cyber Security Incident response personnel, o BES Cyber Security Incident handling processes or procedures, o Communications processes or procedures.
No
1. R2.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rational – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 2. Requirements – Content Change ♣ Original Content • When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test. ♣ Proposed Change • When a BES Cyber Security Incident occurs, the incident response plans must be used and include recording of deviations taken from the plan during the incident. 2. 2.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rational – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist.. 2. Requirements – Content Change ♣ Original Content • Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): o by responding to an actual incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Proposed Change • Test the incident response plan(s) annually. A test of the plan may include: o A response to an incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Rationale – References to requirements needed upon the effective date should be captured within the implementation plan, allowing the standard to identify requirements (only) in place once the standard is approved. 3. R2.3 – Propose deletion as this sub requirement merely identifies retention requirements already documented within Compliance (C.1.2).
No

1. R3.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rational – The formal definition of BES Cyber Security Incident includes attempts to compromise the ESP or DPB, requiring Medium or High Impact BES Cyber Systems/Assets. 2. R3.2 1. Requirements – Propose content change a. Original content – Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan. b. Proposed change – Use lessons learned from incident responses or incident response exercises to update the incident response plan, within sixty days of documenting lessons. c. Rationale – It takes 30 days from the time an exercise is executed to the review and completion of an after action report. The thirty day clock should start once the after action report is completed. This is in line with the proposed 60 day timeline in R3.3. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan. ♣ Proposed Change – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or incident response within thirty calendar days of the lessons learned associated with the response plan. 3. R3.3 1. Requirements – Content Change ♣ Original Content • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan. ♣ Proposed Change • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that test or incident. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan. ♣ Proposed Change – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan test or incidence response and the dated, revised plan.

No

No

• Overall 1. References to ‘implement’ should be changed to ‘exercise’ regarding recovery plans to better capture activation of the plan vs. ‘release and publish’ efforts. 2. Actions required in advance of the implementation date (2.1, 2.2) should be removed from the standard(s) and included within the implementation plan. Purpose – Proposed Content Change 1. Original Content – Standard CIP-009-5 ensures that recovery plan(s) related to the storing of backup information are put in place for BES Cyber Assets and BES Cyber Systems and that these plans support and follow established business continuity and disaster recovery techniques and practices. 2. Proposed Change – Standard CIP-009-5 ensures that recovery plan(s) are put in place for BES Cyber Assets and BES Cyber Systems. R1.3- Remove protection from requirement because protecting information is covered in CIP-011. Proposed language: One or more processes for the backup, storage, and restoration of information required to restore BES Cyber System functionality. For R1 Suggest additional content supporting mirroring and/or redundancy within the backup/recovery methods such as: Mirroring and/or redundancy can be considered as complementary measure in support of this requirement, but a process must be in place to ensure retrieval of previous versions should current version(s) require reverting to a previous instance R1.4 The current form does not adequately address FERC Order 706, paragraphs 739 and 748, and in fact contradicts the intent that ‘The Commission does not believe that every change will necessitate verification of the backup and restoration processes’ from paragraph 740. ♣ Propose ‘new’ sub requirement applicable to High Impact BES Cyber Systems to require: • Upon implementation of significant changes to High Impact BES Cyber Systems, verify that backups are operational before they are relied upon for recovery purposes. ♣ Propose rewrite • Original – Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully. • Proposed Change – Ensure that backup processes are completed successfully for Information essential to BES Cyber System recovery. • Rational – This focuses on successful completion of the backup process which can be done within the routine backup. Verification would be moved to its own requirement applicable to High Impact BES Cyber Systems and limited to significant change instances. R1.5 Original Content – Preserve data,

where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. ♣ Proposed Change – Document root cause for events that trigger activation of the recovery plan(s) as required in Requirement R1. ♣ Rationale – Root cause documentation should be the focus for this requirement. The current draft language requires potential impediments to restoration efforts and is too vague.

No

1. General Comment: Please provide Guidance: Does the Recovery Plan for each BES Cyber System require to be tested each year, or only one Plan. For example the EMS system will have a Recovery Plan, and the associated Physical Access Control System will have a recovery Plan, so do both plans get exercised each year or only one Plan. R2.1 1. Requirements Original – Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: by recovering from an actual incident, or with a paper drill or tabletop exercise, or with a full operational exercise Proposed Change – Implement the recovery plan(s) referenced in R1 annually: • by recovering from an actual incident, or • with a tabletop exercise, or • with a functional exercise Rationale – Use of the functional exercise aligns with the R2 rationale content citing NIST SP 800-84 exercise types. Requirements in advance of the effective date of the standard should be addressed within the implementation plan. 2. Measures – Content Change ♣ Original – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with a full operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a tabletop exercise, or with a functional exercise) of the recovery plan annually. For the table top or functional exercise, evidence may include meeting notices, minutes, or other records of exercise findings. R2.2 Requirements – Content Change ♣ Original Text – Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations. ♣ Proposed Change – Test information used in the recovery of BES Cyber systems that is stored on backup media annually, to ensure that the information is useable. R2.3 1. Overall ♣ This requirement (to be done every 39 calendar months) appears to overlap considerably with 2.1 (to be done every year). ♣ Every 39 calendar months exceeds the 3 year retention identified within the Compliance section. ♣ How does this differ from current EOP-008 requirements? R2.3 2. Requirements – Content Change ♣ Original – Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise. ♣ Proposed Change – Exercise the recovery plan(s) at least every 39 calendar months through an operational exercise in a representative environment. An actual recovery response may substitute for an operational exercise. ♣ Rationale – Actions required to take place prior to the effective date of the standard should be captured within the implementation plan.

No

1. R3.1 Requirements – Content Change ♣ Original – Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned. ♣ Proposed Change – Review the recovery plan(s) annually and document any identified deficiencies. ♣ Rationale – Requirements addressing tasks to be done prior to the effective date should be captured within the implementation plan. 2. R3.2 Requirements – Content Change ♣ Original – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned. ♣ Proposed Change – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of completion, documenting any identified deficiencies or lessons learned. R3.4 – Propose deletion as the requirement is too broad with no clear alignment with FERC Order 706 or security benefit.

Yes

No
1. R1.1- In General UI does not agree with the addition of the new requirement. The existing Change Management requirement in CIP-003-3 is sufficient. The proposal is too prescriptive. CIP-003-4 R6 is closer to a results based requirement and provides more flexibility to achieve the desired results. CIP-010-1 R1.1 greatly expands the scope of change control and configuration management (CIP-003-4 R6) beyond what was directed in FERC Order 706. FERC Order 706 paragraphs 397 and 398 directed "modifications to CIP-003-1 R6 to provide an express acknowledgement of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." The concern was that some form of verification is performed to detect when authorized changes have been made. CIP-010-1 R2.1 addresses Order 706's concern for some form of verification to detect unauthorized changes. (CIP-010-1 R2.1 should delete reference to the baseline defined in CIP-010-1 R1.1.) FERC also did "not believe the changes will have burdensome consequences." CIP-010-1 R1.1 requires extensive and burdensome details tracking. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1 And R1.1.4 – Propose content change ♣ Original Text – Any custom software and scripts developed for the entity; ♣ Proposed Change – Any custom software and scripts installed on the BES Cyber Asset that can affect the security posture. ♣ Rationale – The change focuses scope to eliminate software and scripts not in use. 2. R1.2 1. Requirement – Propose content change ♣ Original Text – Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Proposed Change – Document approved changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Rationale – As documented earlier in this comment form, requiring Senior Manager (or delegate) authorization introduces resource constraints that impede the effective documentation of changes without adding security benefits or alignment with FERC Order 706. 2. Measure ♣ First paragraph – Add 'or,' at the end of the first bulleted paragraph. ♣ Second paragraph – Propose content change • Original Text – A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) were an individual with the authority to authorize the change was in attendance. • Proposed Change – A record of the change with authorization of the change. • Rationale – Citing a "change advisory board" within the measure overly represents adequate evidence in support of the requirement. 3. R1.3 1. Requirements – Propose content change ♣ Original Text – Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change. ♣ Proposed Change – Update the documented baseline configuration as necessary within 30 calendar days of completing the change. ♣ Rationale – The proposed rewording provides more focus on the root requirements. 4. R1.4 What is the meaning and scope of cyber security controls 5. R1.5 1. Requirements – Propose content change ♣ Original Text • 1.5.1 – Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any difference in operation between the test and production environments. ♣ Proposed Change • 1.5.1 – Prior to implementing any change from the existing baseline configuration in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment. ♣ Rationale – Proposed rewording provide greater focus on the root requirements. 2. Measures – Propose content change ♣ Original Text – Evidence includes, but is not limited to, a list of security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test. ♣ Proposed Change – Evidence includes, but is not limited to, a list of security controls tested along with the date of the test, test results, and a list of differences between the production and test environments.
No
R2.1 1. Applicability – Propose removal of Medium Impact BES Cyber Systems. ♣ Rationale – The

technology required to monitor/detect for changes is relatively new and not aligned to BES Cyber Systems which would be in place within a Medium Impact facility (substations, etc.). 2. Requirements – Propose content change ♣ Original Text – Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010_ R1, Part 1.1) and document and investigate the detection of any unauthorized changes. ♣ Proposed change – Where technically feasible, detect and document unauthorized changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1).
No

R3.1 1. Requirements – Proposed content change ♣ Original Text – Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed. ♣ Proposed Change – On an annual basis, conduct a paper assessment of the cyber security controls to determine the extent to which the controls are implemented correctly and operating as designed. • Propose the addition (3.1.1) of minimum cyber security controls to be assessed that; o Are referenced within these standards; and o Are not already required to be assessed in other standards (removing double jeopardy implications) ♣ Rational • Annual (as defined within CIP-0010) should be the consistent approach to allow entities to standardize annual requirements on a consistent basis. • Active assessment is cited within Part 3.2 (to be done every 39 months) so we've removed it from this part to avoid overlap. 2. Measures – Propose content change ♣ Overall – There needs to be clear segmentation from ♣ Original Text – Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the output of the tools used to perform the assessment. ♣ Proposed Change – Evidence may include, but is not limited to: • A document listing the date of the assessment, the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the assessment results. ♣ Rational – Annual should align with CAN-0010 definition. Documentation of assessment results focus on the root information in support of vulnerability rather than potentially extensive data (from tools) that may require extensive resources to retain. R3.2 1. General observations ♣ While the application guidelines recognize production devices which may not be capable of modeling within a test environment (ICCP, etc.), this requirement does not provide clear guidance to follow where these instances occur. ♣ The 39 month cycle exceeds the 3 year retention requirements. 2. Requirements – Propose content change ♣ Original Text – Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments. ♣ Proposed Change – At least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production. 3. Measures – Propose content change ♣ Original Text – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment. ♣ Proposed Change – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments. R3.4 1. Requirements – Propose content change ♣ Original Text – Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Proposed Change – Document the results of the assessments (conducted within 3.1-3.3) and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Rationale – referencing parts 3.1 – 3.3 provides alignment with the previous parts of the standards.

Yes

No

R1.1 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed

Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. R1.2 Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. R1.3 Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. R1.3 Requirements – Proposed content change ♣ Original Text - Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. ♣ Proposed Change – Annually assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. R1.3 Measures – Proposed content change ♣ Original Text – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence to demonstrate that the action plan was implemented. ♣ Proposed Change – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence of the status of the action. ♣ Rationale – Rewording allows for action plans which may be 'in progress' towards implementation, capturing instance in which remediation may rely on deliverables (not yet received) by vendors.
No
R2.1 Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. R2.1 Requirements – Proposed Change ♣ Original Content – Prior to the release for reuse of

BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media. ♣ Proposed Change – Prevent the unauthorized retrieval of BES Cyber System Information from BES Cyber Asset media prior to the release of BES Cyber Asset media for reuse. ♣ Rationale – While not directly changing the intent of the requirement, this rewording has been suggested to provide greater clarity of the root requirement. R2.2 Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts.

No

No

References to requirements to be conducted in advance of the implementation date should be migrated over into the implementation plan. This ensures any pre-requisites are captured within the implementation plan, freeing this content from the standards to provide clearer guidance. Implementing version 5: The implementation period should be no less than 24 months however it is impossible to propose a likely implementation period until the final basket of requirements take shape. The reasoning to support the minimal 24 months is that certain changes will require a capital expenditures and equipment acquisition. The SDT should consider that new capital expenditures require inclusion with the next budget cycle and then the process to procure and implement/install new equipment. Actions cannot be started until FERC completes its rulemaking process to define the basket of actions to take. Second, the likely addition of numerous Low Impact BES Cyber Systems that may not have been considered in scope for previous versions will require some Entities to create solutions from clean slates. . In the event that Low Impact assets are a component of the enforceable requirements on day 1 it is likely that additional time would be required. Finally, Entities currently subject to CIP standards are managing a zero defect CIP program and possible preparing for audits while implementing version 5. Planned Changes: UI agrees that if when an Entity plans a change the impact on BES Cyber System designation should be considered and any required security upgrades and CIP items should be completed prior to the Change. In some requirements that require periodic activity it would not increase security to force the activity outside the Existing Entities Schedule. For example, many entities rely on a consultant to perform a cyber vulnerability assessment once per year. This implementation plan would require a separate cyber vulnerability assessment on the new asset prior to placement into operation which will result in the additional expense of multiple assessments per year. Unplanned Changes in Impact designation: UI is concerned with unplanned changes. Changes to impact designations may require significant investment in equipment, process documentation, and personnel to implement a cyber security program and the compliance obligations. Every circumstance and situation can not be anticipated in the implementation plan. UI proposes that additional guidance is provided to state that the obligation to be compliant begins 12 months after notification, and an Entity that can not fully meet its compliance obligation will file a single mitigation plan with it Regional Entity providing a plan and timeline to come into compliance with each of the requirements.

Individual

Joe Petaski

Manitoba Hydro

Yes

-BES Cyber Asset: Some devices, such as digital relays, may operate independently, and neither send nor receive "instructions". It is unclear that an output contact status change would be considered an "instruction". -BES Cyber System: Maintenance Cyber Asset is not defined. Should this be Transient Cyber Asset? -BES Cyber System Information: The same phrase that applies to floor plans and equipment layouts – “that contain BES Cyber System Impact designations” – should also be added after “network topology or similar diagrams”. It is difficult to know how prescriptive the three examples are within the parentheses. Use the same wording used extensively throughout the CIP

standards: “Examples may include, but are not limited to: network addresses, security patch levels, list of logical network accessible ports.” -Dynamic Response to BES Conditions Operating Service: This definition is complex and inconsistent in approach. Parts of the definition are too specific, such as Protection Systems - Current, frequency, and phase. These are input quantities to Protection Systems, and we suggest that this line be deleted. Parts of the definition are too broad - Monitoring and Control - All methods of operating breakers and switches. Does this include manual operation? For clarity and consistency, we suggest using the NERC definition of Protection System instead of the term relay protection, and also remove the bullets which detail "sensors, relays & breakers". We suggest replacing "x-former" with the word "transformer". -CIP Exceptional Circumstance: Please clarify the meaning and intent of the phrase "an impediment of large scale workforce availability". How would this be measured? -Electronic Access Control and Monitoring Systems: It’s unclear whether only the monitoring of access to ESPs and BES Cyber Systems is meant, or all monitoring of ESPs and BES Cyber Systems (including for example the monitoring for malware). Suggest rewording to “Cyber assets used in the control or monitoring of electronic access to Electronic Security Perimeter(s) or BES Cyber Systems.” -Electronic Access Point (EAP): This definition is too broad and it should focus on BES Cyber Asset Protection. Suggest change for “between Cyber Assets” to be “to BES Cyber Assets”. -External Connectivity: Since the term “external connectivity” is not used anywhere in the standards, delete this definition. -External Routable Connectivity: When determining whether external connectivity is routable, is the Responsible Entity required to check only the parts of the communication system that it administers, or is it also responsible to investigate whether a routable protocol is in use anywhere within the communication systems of its communication service providers, even though those communication systems have been exempted from the CIP standards? This definition is unclear. Suggest the following wording: “The use of a routable protocol through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.” -Interactive Remote Access: The sentence "Remote access can be initiated from: ... contractors and consultants." is guidance information, and restricts the definition to only applying to Responsible Entity Cyber Assets, employees, vendors, contractors, and consultants. By definition, this would exclude interactive remote access by anyone else (public, non-legitimate users) from scope. We suggest removing the last sentence and providing this information in a guidance document. -Intermediate Device: As currently written, an Intermediate Device may perform none of the functions listed. We suggest “A Cyber Asset that performs one or more of the following functions: provides the required multi-factor authentication for the interactive remote access; or provides a termination point for required encrypted communications; or restricts interactive remote access to only authorized users.” The sentences “Intermediate devices are sometimes called …. Or in a DMZ network…” are examples which should be moved to the guidance section. -Physical Access Control System: This definition should be consistent with Electronic Access Control or Monitoring Systems. Suggest to added “monitoring” into the title and the definition. -Protected Cyber Asset: Protected Cyber Asset: Please clarify to what the Cyber Asset is connected. The BES Cyber System? To a device outside the ESP? To any device in the ESP? -Reportable BES Cyber Security Incident: A BES Cyber Security Incident has already been defined. How BES Cyber Security Incidents should be handled, including whether they should be reported is better described within the standard than in a definition. -Transient Cyber Asset: Please clarify the meaning of "directly connected" is unclear.
Yes
-Attachment I 1: High Impact Rating (H): We suggest deleting " ... that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services ...", since the phrase is included in the definition of BES Cyber System. Repeating that phrase is redundant and does not capture all the details in the definition. We suggest removing the phrase to improve clarity and readability of High Impact Rating. Attachment I 1 requires the High Impact asset / system to be located at EACH (i.e. every) Control Center or Back-Up Center. Is this really what was intended? If not, “each” should be replaced with “a”. -Attachment I - 1.3 & 1.4: It is not reasonable that a control center is classified as (H) High Impact Rating asset if it controls one or more Medium Impact Rating assets as defined in Section 2. As written, if a utility Control Center only controls a single Medium Impact Rating generation asset and some Low Impact Rating generation assets, its Control Center becomes a (H) Control Center that has the same classification as a large Transmission Owner Control Center facility! We suggest changing from “includes control of one or more of the assets...” to “includes control of two or more of the assets…” in Section 1.3 and 1.4. -Attachment I 1.4: The reference to 2.12 should be deleted. Underfrequency load shedding and undervoltage load shedding is not applied at generation, and the underfrequency load shedding

standards and undervoltage load shedding standards (PRC-006 through PRC-011) are not applicable to Generator Operators. -Attachment I 2.1: To improve clarity and readability, we suggest the wording "Generation facilities ...” -Attachment I 2.2: To improve clarity and readability, we suggest the wording ... "Facilities with an aggregate ...” -Attachment I 2.5: It is unclear from this criterion and the accompanying diagrams as to what the “generation unit to be started” would be in the case of a generating station which has multiple units but only some are designated as blackstart. -Application Guidelines Transmission Part 2.6: If the guidance describing the categorization of the collector bus for a generating plant is an exception to the 500kV criteria, then this should be clearly stated in the actual requirement, not only indicated in the Guidelines. -Attachment 1 2.7: The intent of this criteria was based on considering average MVA ratings of lines and considered that loss of 3-1300 MVA 345 kV lines should be similar to 5-700 MVA 230 kV lines. Calculating the weighting factor for 5-230 kV lines (3500), 3-345 kV lines (3900), and presumably 2-500 kV lines (4000), it seems that an appropriate bright line criterion is 3500 MVA. Rather than use an arbitrary average MVA rating, it is suggested that the drafting team permit actual line ratings to be used and to have the Planning Authority or Transmission Planner calculate the total MVA of the substation. The responsible entity could draw a circle around the entire substation and add up the MVA of each transmission line between 200 and 499 kV. If the total MVA exceeds 3500 MVA then the substation has a medium impact. At Manitoba Hydro, our 230 kV lines have average MVA ratings around 300-400 MVA. Loss of substation with five 230 kV transmission lines does not have an Adverse Reliability Impact. However, using the proposed methodology, considering a 700 weighting factor, several substations in Manitoba would be classified as having a medium impact. In addition, it is unclear in this criterion as to whether the intention is to capture only station level cyber systems or whether it is also intended to capture cyber systems associated with the transmission lines which caused the impact assessment in the first place. The concern is that transmission line protection cyber systems may require the identification of assets located at facilities other than the originally identified facility and it will very quickly multiply the number of stations requiring compliance. -Attachment I 2.13: Should "generation control centre" be” generation Control Centre", as used in the Application Guidelines, or does " generation control centre" have a different meaning than "Control Centre"? The Application Guidelines indicates that the 300 MW threshold for generation control centres is the same value used for the UFLS and UVLS. This is not a valid equivalence. UFLS and UVLS programs "provide last resort system preservation measures" and "provide system preservation measures", as stated in the purpose of NERC standards PRC-006 through PRC-011. The reliability impact of 300MW during abnormal system conditions which require underfrequency or undervoltage load shedding is significantly different than the reliability impact of 300MW under normal system conditions. Even if 300MW is an appropriate CIP impact threshold for UFLS and UVLS systems, it is not automatically appropriate for generation control centres. It is also unclear what is the difference in reliability impact of a 300MW generation control centre, a 300MW generating station, or a 300MW generating unit. The generation control centre concept needs to be revised.

No

-R1: To improve clarity, we suggest expanding the language when referring to several levels of impact or assets and systems. As currently written, "High and Medium Impact" could be interpreted as meaning an asset or system which is both High and Medium Impact. The same interpretation could be applied to BES Cyber Assets and BES Cyber Systems. To clarify, we suggest the wording "... High Impact BES Cyber Assets, High Impact BES Cyber Systems, Medium Impact BES Cyber Assets and Medium Impact BES Cyber Systems ..." We suggest this change be adopted in all applicable CIP standards. -R 1.1: If this requirement was intended to apply to changes to BES Elements and to changes to BES facilities, then this sentence should be reworded to refer to “a change to BES Elements OR Facilities...”. As drafted, the change would have to be to both a BES Facility and Element before the requirement applies. From a grammatical perspective, the phrase “IS placed into operation” should be “BEING placed into operation”. -M1: There are no controls specified in CIP-002-5. It is unclear how categorization of Low Impact would be measured.

No

-R2: If R2 was intended to require the CIP Senior Manager or delegate to approve the identification and categorization changes as per R 1.1 within the 30 day period, then this section needs to be clarified. As drafted, the CIP senior manager or delegate is only required to approve the change within the calendar year. -R2: For clarity, we suggest changing " ... even if it ... “ to ”... even if the Responsible Entity ...". -M2: We suggest changing "... records to demonstrate ..." to "records which

demonstrate ...". -M2: For clarity, we suggest changing " ... even if it ... " to " ... even if the Responsible Entity ...".
Yes
No
-R2: This requirement is too vague. The phrase “represents the Responsible Entity’s commitment “is unclear. Is the policy intended to document the Responsible Entity’s procedures for implementing CIP standards related to the itemized topics, or is it intended to be broader than standards- related requirements? Can the policy state general policy goals, but not detail the procedures? We suggest incorporating the language in the current CIP-003-4 "The cyber security policy addresses the requirements in Standards CIP-002-5 through CIP-009-5, and CIP-010-1, and CIP-011-1." Also, for clarity, we suggest changing “remote access” to “Remote Electronic Access". -Guidelines R2: Bullet "Identification of possible disciplinary action for violating this policy", and any similar statements should be deleted. Internal disciplinary actions for policy violations are not NERC reliability compliance issues. -Guidelines R2 Item 2.4: We suggest changing "ingress and egress" to "access and exit (for visitors only)" since monitoring of exit is only required for visitors, as per CIP-006-5 R2 Part 2.2. Guidelines R2 Item 2.8: The term "break-fix processes" is unclear.
No
R3: It does not state the purpose of the review or any action to be taken as a result of the review, yet the stated Rationale refers to ensuring that the policy is kept up to date. If that is the intent, then the requirement should state that the policies must be updated, presumably to reflect changes that have occurred since the last year‘s review / adoption. However, MH notes that this implies that R2 would then be interpreted to mean that the policy being implemented need not be kept current. This requirement needs to be clarified as between R3 and R2.
No
R4: Awareness of the policies should also include individuals who have access to BES Cyber System Information, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.
Yes
Yes
No
Measures 1.1: The reference is no longer to ‘may include’ but to ‘must include’ and ‘acceptable evidence’ – are these references an intentional shift from the ‘may include’ language?
No
-Measures 2.1: The reference is no longer to ‘may include’ but to ‘must include’ and ‘acceptable evidence’ – are these references an intentional shift from the ‘may include’ language? -R2 - Applicability: The Applicability for the training program in R2 should match the implementation of the training program in R3. -R2.7: Please clarify "associated notifications". Do the "associated notifications" refer to CIP-008-5 R1 Part 1.3?
No
-R3: To provide consistency with the language in R2, please specify which assets are in the scope of Requirement R3. -R3.1: “Access” should be “electronic or unescorted physical access”. -R3.2: It seems to be missing the words ‘between training’ at the end of the requirement.
No
-R4 - Applicability: The Applicability for the personnel risk assessment program in R4 should match the implementation of the personnel risk assessment program in R5. -R4.1: It fails to specify what ‘initial’ means – is it upon hiring? Upon access being granted?
No
-R5 - Applicability: The Applicability for the personnel risk assessment program in R4 should match

the implementation of the personnel risk assessment program in R5.
No
-Rationale for R6: for clarity, we suggest "... perform such grants and is included in the delegation process referenced in CIP-003-5." In the second paragraph, we also suggest "... against records of individuals authorized to access the BES Cyber System...." -6.5 Requirement: It is unclear if "all accounts" refers to system level accounts or cyber asset accounts. -R6.6: For clarity, we suggest changing from "Verify ... of access privileges ..." to" Verify … access privileges"
No
-R7.1: The extenuating circumstance clause within R7.5 should be included for all parts of Requirement 7. An example of why this would be required would be where an employee resigns at the end of the day with no notice, this would make meeting R7.1 virtually impossible. -R7.2: We agree with a timely access review for reassignments and transfers. To provide more clarity, as well as consistency with the Measures, Rationale and Guidance, we suggest changing "revoke" to "review", and adding more text as follows: -For reassignments or transfers, review the individual's needs for electronic and physical access to BES Cyber Systems by the end of the next calendar day. Document and implement a revocation plan, including dates. -R7.3: For clarity, we suggest changing "access" to "electronic access or unescorted physical access". -R7.4: More than 30 days may be required for access revocation conducted through manual processes. We suggest an entity defined revocation schedule for manual revocation processes. -R7.5: More than 30 days may be required for access revocation conducted through manual processes. We suggest an entity defined revocation schedule for manual revocation processes. It is unclear if the password change is at a system or cyber asset level. Shared account password changes may not be technically feasible for all cyber assets.
No
-Rationale for R1: To improve clarity, we suggest changing " ... external boundary ..." to "... external electronic boundary ..." -R1: In R1 and R2, all requirements should refer to applicable "requirements" in a table, rather than "items" in a table. -R1.2: As written, R1.2 requires that ALL ROUTABLE connectivity for a BES Cyber System must be controlled through the use of EAPs, which would INCLUDE routable connectivity between BES Cyber Assets in the same BES Cyber System. If the intent is to address external connectivity outside of the ESP, we suggest changing "…routable and dial-up connectivity" to "…routable and dial-up External Connectivity." -Measures: The wording in the Measures is unclear. Regarding the bullet "A list of uniquely identifiable Cyber Assets within the BES Cyber System and associated EAPs ": is this a list of Cyber Assets which comprise the BES Cyber System and a list of the EAPs on those BES Cyber System, which does not include Protected Cyber Assets; or is it a list of Cyber Assets which comprise the BES Cyber System and a list of Cyber Assets within the EAPs, which includes the Protected Cyber Assets, but is not a list of EAPs? -R1.3: Corresponding with the EAP asset level approach for ALL routable and dial-up communications in Item 1.2, this requirement would apply explicit permissions at each communications interface (EAP) for each device in a BES Cyber System. This may not be necessary or possible for all devices within a BES Cyber System. If the intent is to address external connectivity outside of the ESP, we suggest changing "…using routable protocol" to "…using external routable connectivity". In addition, it seems more appropriate for "including" to be "and" as people would think of establishing criteria for granting permission as a separate requirement from requiring permission at EAPs. -R1.5: We disagree with the requirement prescribing malicious communication detection. Change Rationale: It is not apparent from FERC Order 706, p 496 - 503 that the two distinct measures "is not simple redundancy of firewalls". The Order in p 501 does state that "... The Commission is not mandating any specific mechanism to be the second security measure. We are also not requiring uniformity of security measures, only that each responsible entity has at least two security measures unless it is not technically feasible to do so. The revised CIP Reliability Standard should allow enough flexibility for a responsible entity to take into account each site's specific environment." Based on the direction in the Order, the Responsible Entity should have some flexibility in determining the appropriate second security measure, and should be allowed to claim a TFE if necessary. In addition, we suggest the wording "Document and implement a method ...." to provide consistency with the other requirements.
No
-R2: We suggest adding " ... and Associated Protected Cyber Assets, Electronic Access Control or Monitoring System, and Physical Access Control Systems ..." -R2.1: The meaning of "... directly

access ... " is unclear. Also, there are no requirements for remote access management for Electronic Access Control or Monitoring Systems, and Physical Access Control Systems. We suggest that remote access management be applied to these systems. -R2.1: As written, R2.1 requires that ALL ROUTABLE connectivity for a BES Cyber System include an Intermediate Device. If the intent is to address external connectivity outside of the ESP, we suggest changing the applicability to Cyber Systems with "…routable and dial-up External Connectivity." -R2.2: As written, R2.2 requires that ALL ROUTABLE connectivity for a BES Cyber System include encryption for all Interactive Remote sessions. If the intent is to address external connectivity outside of the ESP, we suggest changing the applicability to Cyber Systems with "…routable and dial-up External Connectivity." -R2.3: As written, R2.3 requires that ALL ROUTABLE connectivity for a BES Cyber System include multi-factor for all Interactive Remote sessions. If the intent is to address external connectivity outside of the ESP, we suggest changing the applicability to Cyber Systems with "…routable and dial-up External Connectivity."

No

-R1.1: Applicability and Requirement: Associated Physical Access Control Systems (for High and Medium BES Impact Cyber Systems) are not required to be located in a Defined Physical Security Boundary while the High and Medium Impact BES Cyber Systems must be in a Defined Physical Security Boundary. It is inappropriate to use the Associated Physical Access Control Systems in the applicability for R1.1. This approach is inconsistent with the other requirements and standards since the Associated Physical Access Control Systems do not have any identified High Impact BES Cyber Systems or Medium Impact BES Cyber Systems. High Impact BES Cyber Systems and Medium Impact BES Cyber Systems should be added to the Applicability. -R1.2 - Applicability: CIP-006 local definition of Associated Electronic Access Control or Monitoring Systems and Associated Protected Cyber Assets is for both High Impact BES Cyber Assets and Medium Impact BES Cyber Assets. This applicability will lead to confusion (especially considering how R1.3 is written) with respective High Impact BES Cyber Assets requiring protection under R2 & R3. We suggest changing from "Associated Electronic Access Control or Monitoring Systems" and "Associated Protected Cyber Assets" to "Associated Electronic Access Control or Monitoring Systems associated with a corresponding Medium Impact BES Cyber System" and "Associated Protected Cyber Assets associated with a corresponding Medium Impact BES Cyber System". -Associated Physical Access Control Systems should require equivalent access controls (as they do under the CIP-006-4c) to the Medium (or High under R1.3) Impact BES Cyber Systems. We suggest adding" Associated Physical Access Control Systems associated with a corresponding Medium Impact BES Cyber System" under the Applicability to make the Associated Physical Access Control Systems have the same measures as Electronic Access Control or Monitoring Systems. -R1.2 – Measures: The reference to egress should not be included in the measures. The requirement only refers to access. -R1.3 – Applicability: We suggest changing from "Associated Electronic Access Control or Monitoring Systems" and "Associated Protected Cyber Assets" to "Associated Electronic Access Control or Monitoring Systems associated with a corresponding High Impact BES Cyber System" and "Associated Protected Cyber Assets associated with a corresponding High Impact BES Cyber System". -Associated Physical Access Control Systems should require equivalent access controls (as they do under the CIP-006-4c) to the High Impact BES Cyber Systems. We suggest adding" Associated Physical Access Control Systems associated with a corresponding High Impact BES Cyber System" under the Applicability to make the Associated Physical Access Control Systems have the same measures as Electronic Access Control or Monitoring Systems. -R1.3: "Where technically feasible" should not be necessary for High Impact BES Cyber Systems as the requirement should be achievable for the High Impact BES Cyber Assets. -Secondly, if "where technically feasible" is deemed to be a necessary part of the requirement, then we suggest "... establish one or more Defined Physical Boundaries, where technically feasible, that restricts ..." so that "technically feasible" does not apply to the portion of the requirement associated with authorized users. -R1.3 – Measures: The reference to egress should not be included in the measures. The requirement only refers to access. -R1.3 – Change Description: For clarity, we suggest "FERC Order 706 p575 directives are addressed by providing the examples of physical security defense in depth via multi-factor authentication or layered defined physical security boundary(s) in the guidance document." -R1.4: We suggest changing "access through any access point" to "entry into each defined Physical Boundary protecting applicable BES Cyber Systems, Protected Cyber Systems, and Access Control and Monitoring Systems ...". The suggested change creates a more general statement which allows the

entity flexibility in implementation, and is consistent with the language in Part 1.6. -R1.6: We suggest changing "date" to "date and time", which would better support investigations.
No
-R2 Rationale: For clarity, we suggest "To provide access control when personnel without authorized unescorted physical access are in any Defined Physical boundaries as applicable in Table R2." -R2.2: For clarity, we suggest "... the first entry and the last exit ...", and "... the visitor's name, and the individual contact personnel's name."
No
-R3.1 - Applicability: Capitalize "Locally mounted hardware ... Boundaries" as indicated in the Background Applicability section. -R3.1: For clarity, we suggest “Prior to placing in service,”.
No
-Table of Compliance Elements, R1 – Lower VSL: R1.7 that is referred in this table doesn’t exist in CIP-006-5 Standards. -Table of Compliance Elements, R1 – High VSL: “15 minutes” timeline is referred from R1.6, but R1.6 doesn’t have such a timeline.
No
Introduction - Purpose: Does "unavailability" refer to the BES Reliability Operating Services, or to the BES Cyber System? We suggest changing "... availability ..." to "... availability and integrity ..."
No
-R2.1 - Measures: An entity should be allowed to group like BES Cyber Systems and BES Cyber Assets for patch monitoring. In general, the information provided in the measures is guidance, and should be moved to the Guideline section. -R2.2: “a defined timeframe” is not clear. Who defines the timeframe, the identified source or Responsible Entity?
No
-R3.1: We suggest changing "... prevent malicious code ..." to "... prevent addition of malicious code ...”. -R3.2: Suggest rewording to “Disable, quarantine, or remove identified malicious code. -R3.3: We suggest that the Responsible Entity be permitted to define a time interval for the signatures or patterns which are updated through manual processes. These BES Cyber Systems are typically isolated from any communication network, and therefore at lower risk. -R3.4: Suggest changing from “when connecting them to BES Cyber Assets or Protected Cyber Assets” to “when connecting them to applicable BES cyber Assets or Protected Cyber Assets”. -R3.5: The purpose and value of logging each Transient Cyber Asset connection is unclear. While R3.4 improves the security of BES Cyber Systems, R3.5 does not improve security, and as such R3.5 should be deleted. Note that the requirement for Acceptable Use banners has been removed for a similar reason.
No
-R4.1: Suggest changing from “Cyber Security Incident” to “BES Cyber Security Incident” to ensure that the glossary’s definition is being used. -R4.1 – Measures: We suggest changing "... paper ..." to a more generic term "... manual ..." -R4.3: Event logging should refer to R4.1, otherwise it is too broad. How and when is the event logging failure detected? Suggest wording: “Activate a response to event logging failures before the end of the next calendar day when detected.” -R4.5: We suggest improved clarity by removing the word "unanticipated". The term "event logging" is too broad and should refer to R4.1. For clarity, we suggest "Before the end of the next calendar day, activate a response to rectify any deficiency identified from the review."
No
-R5.1: We suggest adding "where technically feasible". For example, for some High Impact BES Cyber Assets, their user electronic access is only a front panel which does not require any credentials (e.g. frequency deviation meters used for AGC). It is unclear how grouping this cyber asset into a BES Cyber System could be considered to make it compliant with R5.1, so a Technical Feasibility Exception would be required. -R5.4 – Applicability: The use of "All Responsible Entities" in the Applicability column of the table is confusing. Are these the entities identified by Functional Entities in Section 4 Applicability, or are the "All Responsible Entities" defined by the bullets in Section 5 Background Applicability? To maintain consistency and clarity with all the other requirements, we suggest replacing "All Responsible Entities" with the specific Cyber Assets in scope, for example, BES Cyber Assets. -R5.6: The wording is unclear. We suggest "A process to limit the number of unsuccessful authentication attempts or generate alarms after a threshold of unsuccessful login attempts, where technically feasible.

No
-Rationale for R1: To create a complete sentence, we suggest "Incident reporting and response planning ensures consistent responses to BES Cyber Security Incidents involving BES Cyber Assets and BES Cyber Systems." We also suggest changing "exploited" to "discovered", since not all incidents involve exploits. The Summary of Changes has not been completed. -R1.1 – Measures: under Measures, the last portion of the sentence beginning 'targeting…' does not seem necessary. It overlaps with, and encompasses part of, the definition of Cyber Security Incident. -R1.2: A BES Cyber Security Incident has already been defined. How BES Cyber Security Incidents should be handled, including whether they should be reported is better described within the standard than in a definition. We suggest moving the Reportable BES Cyber Security Incident to here. -R1.2 – Measures: The word 'also' at the end of the sentence should be deleted. -R1.3: For clarity, we suggest "Incident communication plans which include internal staff and external organizations."
No
-R2: Specific responses to Cyber Security Incidents should not apply to Low Impact BES Cyber Systems due to the large number of systems included and their low impact. By the definition, entities are required to treat all malicious or suspicious events resulting in unauthorized physical access into a Defined Physical Security Boundary as a BES Cyber Security Incident. This imposes an unnecessary burden on the entities and provides little value. -R2.1: For clarity, we suggest rewording for R2.1: "When a Cyber Security Incident occurs, the incident response plans must be used and include recording deviations from the plan during the incident." -R2.2: The word "full" in the phrase "full operational exercise" is unclear. Since even tabletop exercises are allowed, it should also be allowable to run an operational exercise that is somewhat limited in scope. Suggest removing the word "full" from both the Requirement and the Measures. -R2.2 – Measures: The words 'between executions of the plan(s)' should be added after 'not to exceed 15 months'.
No
-R3.1: the words 'the plan' should be added after 'update' -R3.1 – Measures: The words 'between reviews' should be added after 'not to exceed 15 months'. -R3.2: Since the definition of a BES Cyber Security Incident is very broad (i.e. it includes all suspicious events, all attempts to compromise an ESP, all attempts to disrupt a BES Cyber System), it is likely that many of them will be detected (e.g. port scans at a firewall). Suggest adding language whereby a Responsible Entity may document for itself criteria of which types of BES Cyber Security Incidents it will review.
-Table of Compliance Elements, R1 – the language in this table does not seem to match the language of the requirements exactly which leads to lack of clarity. Under Severe VSL, second paragraph - the words 'include a process to identify' should replace the words 'identify'. -Table of Compliance Elements, R2 –There does not seem to be any violation for failing to test the response plan upon the effective date of the standard – is this intentional? If not, the words 'upon the effective date of the standard' should be added. Table of Compliance Elements, R3 – High VSL – the first paragraph references a 30 day timeline for updating the response plan, but the requirement itself references 60 days. Need clarification. -Table of Compliance Elements, R3 – Severe VSL – the last paragraph is missing the requirement that the communication occur with 30 days of the completion of the update of the plan – is this intentional? If not, the 30 day timeline should be added.
No
-Title: We suggest changing "Systems" to "BES Cyber Systems". -Purpose: The apparent purpose of CIP-009-5 addresses more than just the "... storing of backup information ...". We suggest that the Purpose be revised to more fully reflect the intent of the standard. -Rationale for R1: Not all incidents involve weaknesses that were exploited. We suggest changing "exploited" to "discovered". For added clarity to the Summary of Changes, we suggest the wording "Added data protection provisions to facilitate event investigation after activation of the recovery plan." -R1.4: We suggest the wording "Process for the identification of information essential to BES Cyber System recovery that is stored on backup media." The statement "shall be verified ... successfully..." should indicate that the process is included in the plan, since the act of verification is addressed in Table R2 Part 2.2. The measure for R1 Part 1.4 should be revised to agree with the information identification and verification process. -R1.5: For clarity, we suggest changing "Preserve data ..." to "Process for preserving data,". -R1.5 – Measures: the word 'important' is unnecessary.
No

-R2.1: The need for the word “full” in the phrase “full operational exercise” is unclear. Since even tabletop exercises are allowed, it should also be allowable to run an operational exercise that is somewhat limited in scope. Suggest removing the word “full” from both the Requirement and the Measures. Note that the wording for R2.3 already refers to “operational exercise”, not “full operational exercise”. -M2.1: The relevant timing (i.e. ‘upon the effective date of the standard’, and ‘between executions of the plan’) is missing from the Measures but included in the Requirements, should also be in the Measures -R2.2: We suggest removing the word "any" since it is too broad. For clarity and consistency with the Measure, we suggest changing "initially" to "initially stored". -R2.3: We suggest "... every 3 calendar years". We also suggest "... representative environment that reflects the production environment, where technically feasible..." to address potential issues with legacy systems. Under Requirements and Measures, seems to be some discrepancy between the language of the Requirement and the Change Rationale and VSL in referencing ‘every 3 years’ and referencing ‘every 39 calendar months’. Is the intention that the testing occur every 3 years, with not more than 39 months between tests?
No
-R3.1: Under Requirements and Measures, from reading the Change Justification, it appears as though the review is to occur after system replacement in addition to the regular testing each calendar year. However, the way the Requirements and Measures are drafted using the word ‘or’, it could be interpreted to mean the testing can occur either once a year or when systems are replaced. We suggest "or" to be replaced with an "and" in Requirements and Measures -R3.2: For clarity and consistency with the Measure, we suggest changing "... exercise,” to "exercise in 2.1 and 2.3...". Also, from the current wording “the completion of the exercise”, it appears that the review is supposed to take place after every annual exercise. However the wording “or actual incident recovery” seems to imply that a review would be required after every recovery incident throughout the year. Since large systems may have hundreds of disks there may be many disk failure recovery incidents a year, but it is difficult to see the value of a review after each of these. Suggest deleting the words “or actual incident recovery”. Alternatively, suggest adding language whereby a Responsible Entity may document for itself criteria of which types of recovery incidents it will review. -R3.4: The word "any" is too broad. We suggest "Update the recovery plan(s) within thirty calendar days of any organizational or technology changes that impact that plan." This change is consistent with similar language in CIP-008-5 Table R3 Part 3.4 Requirement. -R3.5: For clarity, we suggest changing "... responsible under ..." to "... identified in ...".
No
-Table of Compliance Elements, R1 – High VSL – the section does not include a violation of 1.1, only 1.2 through 1.5 – is this the intention? -Table of Compliance Elements, R2 – High VSL – The same comments as in R2, 2.2 and 2.3 above.
No
-R 1.1.3: We suggest changing "available" to "developed", since commercial application software may still be in use, but not currently available. -R1.1.4: we suggest that the "and" be changed to "or". -R1.2: For consistence of tenses, we suggest changing "Authorization" to "Authorize". "Delegate" should be "Delegate(s)". -R1.3: The requirements referenced from the other CIP standards must be explicitly listed in this requirement. The drafting team should also ensure that the 30 day window does not conflict with the referenced requirements. We also suggest that not all of the "documented required" needs to be updated within 30 days, and could be allowed a longer update period. -R1.4.2: The words seem to be missing here, we suggest “following the change, verify that the required cyber security controls….” -R1.5: We suggest deleting "... for Control Centres..." since High Impact BES Cyber Systems only includes control Centres, and therefore this wording is redundant.
No
R2.1: For clarity, we suggest "Monitor for changes to the baseline, where technically feasible, (as defined ....". The technical feasibility should apply to the monitoring, not to the entire requirement, including documentation and investigation.
No
-R3.1: The language for requirements with time intervals should have a consistent format, beginning with the action, and ending with the time interval. In addition, the “security controls” must be specified. Does this include background checks or training? Suggest wording “the technical security controls that are covered by CIP-007-5”. -R3.2: Suggest deleting “not to exceed 39 calendar months

between assessments" -R3.2 - Measures – language regarding timeline should match the language used in the requirement itself. -R3.3 – Applicability: The Associated Physical Access Control Systems should be included in the Applicability. -R3.3: For clarity, we suggest "... perform a vulnerability assessment of the new Cyber Asset."
No
-VSLs - R3, Lower VSL – reference is made to assessments on 'each' BES Cyber Systems, but the timeline talks about the time between assessments on 'one of' the BES Cyber Systems. For entities with multiple BES Cyber Systems we need clarification whether the timeline runs between assessments on a particular Cyber System basis, or whether it runs between assessments on any Cyber System. -VSLs - R3 – Active Vulnerability Assessments is capitalized in the VSLs but is not elsewhere
Yes
No
-R2.1: We suggest using local definition instead of the footnote.
No
-R1, High VSL: There is a reference to assessing 'periodically' while the requirement itself sets out a specific timeline. It needs to be changed to reflect requirement.
No
-Unplanned Changes Resulting in a Higher Categorization: If the intent is to address changes made outside of the Responsible Entity's electric system as unplanned, then we suggest wording "an action by an external entity is performed outside of that particular transmission substation ...", and "... power flows would have been performed by the external entity ...". Is the intent to only capture changes by a neighboring entity? -What is the notification process for Responsible Entities to become aware of unplanned changes? When is the start time for compliance implementation for Entity A when Entity B makes a change to the BES which causes a higher categorization of Entity A's BES Cyber System? -We suggest 18 months for all the scenarios for unplanned changes to correspond with time period allowed for the initial effective date of the CIP V5 standards, due to the scope of the work required. -For clarity, we suggest "12 months for requirements not applicable for Low Impact or Medium Impact".
Individual
John Bee
Exelon
Yes
We support the comments submitted by EEI with the following additions: BES Cyber Asset – Add a statement "Support systems such as voice communication (e.g., 900 MHz Radio system), ventilation, power supply systems, and similar supporting systems are not considered BES Cyber Assets." CIP Exceptional Circumstance – Change to read (modified text underlined or crossed out) "A situation that involves one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability, or an emergency support to restore operation of BES Cyber Asset or BES Cyber System by a supplemental vendor not already authorized for electronic access." Background: - This addresses emergency situations. Current wording seems to be biased towards physical assistance, but not electronic. - While electronic should be accounted for in BES Cyber asset Recovery plans, the current wording does not address large vendors such as Microsoft or Oracle that may be needed to restore the BES Cyber System or Asset.
Yes
We support the comments submitted by EEI with the following additions: Dynamic response – TOP is listed in the table but not on the list in the next section.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.

No
We support the comments submitted by EEI.
Yes
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI with the following addition: R3, M3 item 2 – Please Add wording to the end. “Electronic signature is acceptable.”
No
We support the comments submitted by EEI with this addition: We would instead prefer the existing wording of CIP-003-4 R1.2 “The cyber security policy is readily available to all personnel who have access to, or are responsible for…” If an “awareness” of policy requirement is needed we feel it would be better addressed in CIP-004-5 R1 or R2.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
Yes
No
We support the comments submitted by EEI.
Yes
No
We support the comments submitted by EEI.
Yes
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI with these additions: R7.2 Personnel reassignments must be processed and access revoked by end of day, yet terminations are by end of NEXT calendar day - seems backwards. Exelon has concerns that this revocation of access for internal transfers as proposed will significantly increase administrative burden and costs in an area with no commensurate reduction in risk to the reliability of the BES. In order to implement this requirement as proposed, Exelon would need to completely reprogram its HR systems which currently run in batch mode every night. This would be a major expense without a commensurate increase to BES reliability. The SDT has failed to provide a technical justification for this change. Additionally, it is unclear if the major software vendors for Human Resource systems can such a major process change. R7.3 – Change capitalization as shown in measures “BES Cyber System Information”. R7.5 – b. Need a definition of “extenuating circumstances”
Yes
No
We support the comments submitted by EEI with these additions: R1.1 a. Update wording in Measures per mark-ups: “Evidence may include, but is not limited to, documented technical and or procedural controls that exist and have been implemented.” The requirement has “or”. We would like the text of measures to match the text of the requirement. R1.2 Applicability wording should not

include the Physical Access Control Systems. Currently CIP-006-4 R2.2 does not require the protective measures of CIP-005-4 R1 Electronic Security Perimeter and sufficient protections exist in the other requirements. R1.3 Suggest using existing CIP-005-4 R2.2 wording for this item or at least removing the "or denying" wording since we should only have to specify access permissions, not all the things we deny access to. As proposed, this would add significant administrative burden without a commensurate reduction in risk to the reliability of the BES.

No

We support the comments submitted by EEI with this addition: R2.2 Please identify where encryption is required? Do we have to encrypt on entity trusted networks or between the Intermediate device and the Electronic Access Point (EAP)?

No

We support the comments submitted by EEI.

No

We support the comments submitted by EEI with these additions: Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. Table Item 1.1: “Medium Impact BES Cyber Assets with no External Connectivity” should be added to the applicability wording Table Item 1.2: applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity”. Table Item 1.4: applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity”. Table Item 1.6: applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity”. Suggest removing the "protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems" wording from the requirement since that is part of the Defined Physical Boundary definition.”

No

We support the comments submitted by EEI with these additions: Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. Table Item 2.1: applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity”. Table Item 2.2: applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity”.

No

We support the comments submitted by EEI.

No

We support the comments submitted by EEI.

No

We support the comments submitted by EEI with these additions: In cases where the intent of the drafting Committee was not to submit TFEs when an asset was not capable of meeting a requirement explicitly state “Devices that cannot … “ do not require a TFE to be generated.” (Similar to EEI comment on R4.1) Several requirements list BES Cyber Assets, but Applicability does not. Either delete BES Cyber Assets from requirement, or list them in Applicability.

No

We support the comments submitted by EEI with these additions: R2.3 – a. Provide more clarity for

this requirement – does “any exceptions for CIP Exceptional Circumstances “ mean that we temporary suspend normal patching activities when “CIP Exceptional Circumstances” occur, or does it address situations where certain BES Cyber Assets cannot be patched, and this would be documented as “CIP Exceptional Circumstances”. b. R2 no longer allows TFEs, so we need to account for the assets that cannot be patched. Provide clarity around this. c. Include in Measures document showing any exceptions for CIP Exceptional Circumstances related to remediation plan.
No
We support the comments submitted by EEI with these additions: Rationale for R3 - No definition of “Maintenance Cyber Assets”, it should reference Transient Cyber Assets R3.4 – a. Add Transient Assets to the Applicability column b. There will be a significant issue with vendor assets – may want to distinguish between companies’ corporate assets vs. vendor assets. We have external vendors coming to substations or accessing remotely, and no control over their assets. c. Delete from Measures “logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets”. 1) This measure is more applicable to 3.5, and 2) There is no requirement in 3.5 to log when removable media were connected. R3.5 – Add Transient Assets to the Applicability column
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI with these additions: R5.5 – a. Measures include personal attestations. This may be required from a large group people and these attestations would need to be managed. b. If we submit an exception to our internal policy, will this automatically be compliant? This addresses 5.5.3 “password change on entity-specified time frame …” we may still have accounts where passwords cannot be changed. No TFEs are allowed. Provide clarity. 5.6 – b. The requirement specifies “A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts. ” In cases where we cannot limit number of unsuccessful authentication attempts but we can generate alerts, will we still need a TFE? Add clarity around that to the requirement.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI with the following additions: R2.1 – add wording to 1st bullet of requirement “by recovering from an actual incident involving a BES Cyber System or an equivalent system in the test/lab or pre-production environment, or …” R2.2 – Add wording at the end of the requirement “Testing of information for every BES Cyber Asset is not required. Testing of information for a representative sample is sufficient.” R2.3 – Add wording at the end of the requirement “Testing of recovery plans for every BES Cyber Asset is not required. Testing for a representative sample is sufficient.”
No
We support the comments submitted by EEI.
Yes
No

We support the comments submitted by EEI with the following additions: R1.4 – Update wording “For a change to the BES Cyber System that deviates from the existing baseline configuration as required by R1.1: ” Add the term “Cyber Security Controls” to definitions, and include examples of what you consider cyber security controls.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
Yes
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI with this addition: Timing should be at least 24 months due to the large number of Low Impact BES Cyber Assets that need to be inventoried and security settings documented.
Individual
David Martorana
Tenaska, Inc.
Yes
1. In the definition of BES Reliability Operating Services clarification of which aspects of “Spinning Reserve” “AVR” and “AGC” as they relate to the NERC Functional Model are included. It is not clear which Aspects of the Balancing Load and Generation apply to the GO and GOP. Add a Definition of Multi Factor Authentication
No
2. Section 2.3 in Attachment I, may be problematic as it allows Planning Coordinators or Transmission Planners to “arbitrarily” move GO and GOP entities from Low to Medium. In order to maintain a competitive market place and not place a disproportionate regulatory burden on less vertically integrated entities, bright lines for this determination must be drafted. I am not sure how subjective TPL-003 and TPL-004 are.
No
3. 30 days may not be enough time to assess, identify, and categorize if a whole facility is brought from Low to Medium by a Planning Coordinator or Transmission Planner. Does this revision say how long we have to apply the security controls after a BES Cyber Asset or System reaches an elevated Impact Rating. Is it considered an unplanned change per the Implementation Plan?
Yes
No
5. R1 VSL should take into consideration comment 3.
Yes
Yes
Yes
No
9. This requirement appears to be redundant and should be removed as it is covered with CIP 004

Yes
Yes
11. This seems fine, but it might need to be stated that the delegated authority can be exercised prior to the documentation being completed.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
20. R7 individuals should not be plural
Yes
Yes
22. Provide diagrams showing examples, (i.e. SSL VPN, with firewall as Intermediate Device) providing secure Interactive Remote Access. Allow the definition of Multi Factor Authentication to include Credentials on Vendor Network, ESP Firewalls by Vendor IP, and Credentials on BES Cyber Asset.
No
23. Should a lower VSL category be created for an outage associated with the IDS, or is that covered elsewhere?
Yes
Yes
Yes
Yes
27. In R3 the High VSL description should be moved to Moderate, also it would be helpful to note what elements are included in an acceptable “outage record”
Yes
Yes
Yes
30. The use of the word connected in the definition of Transient Cyber Asset, should be more clearly defined.

No
31. Requiring an Entity to rectify a deficiency by the next calendar day will require capital outlay, and eliminate the economic benefits of shared spares.
No
No
No
No
Yes
36. It is not clear if a change in 3.4 includes devices that reach an elevated Impact Rating, i.e. from Low to Med, is this in reference to a planned and unplanned change in the Implementation Plan?
Yes
37. In R1, Which appropriate organizations must an entity have evidence of contacting during a drill to avoid a High VSL? A lower VSL should be associated with partially using the Incident Response Plan, or define “does not use”.
Yes
Yes
Yes
40. Consider the recovery efforts, and that more time might be needed for documentation (3.3) following an actual incident recovery. (3.4) may be hard to comply with if technology changes are made in response to an actual incident recovery. The CIP Exceptional Circumstance language used in CIP-004, or Disaster Recovery in the Implementation Plan could be used to ease this concern.
Yes
41. It is not clear if the Severe VSL would apply if 99% of all BES Cyber Assets were addressed, and one was missed, consider a lower VSL for this circumstance.
Yes
42. This requires for most entities currently complying with CIP, the creation, modification, or expansion of a configuration management system, and modifications and additions to the security status monitoring systems.
No
Yes
Yes
45. Provide additional time for documentation for CIP Exceptional Circumstances
46. It is not clear what labeling methods are acceptable for Electronic Information (File Name, Watermark, etc.)
Yes
Yes
Yes
Individual
Robert Solomon

Hoosier Energy
Yes
The first two sentences in the definition of “BES Cyber Asset” are difficult to interpret. After considerable discussion among our staff, our understanding is as follows: the definition makes the distinction between when an asset is “rendered unavailable, degraded, or misused” and its actual “operation, mis-operation, or non-operation” under such conditions. If the asset impacts the BES “within 15 minutes” of its actual “operation, mis-operation, or non-operation,” then it is a “BES Cyber Asset,” regardless of how long since it was “rendered unavailable, degraded, or misused.” We recommend editing this definition for clarity as it took a number of our staff numerous reads and discussion to arrive at this understanding that we are still not sure is what the drafting team intended. The distinction should be clarified. Also, we question the necessity of such a distinction and whether the value it adds is worth the confusion it produces. Additionally, it is unclear whether the “timeframe” referred to in sentence three applies to the “within 15 minutes” timeframe or the “regardless of the delay” timeframe. How does the responsible entity know if a BES Cyber Security Incident was malicious? Understanding if an act was malicious implies an understanding of intent. We do not believe that intent is something that can always be quickly and easily understood. Consider the recent case of the failure of the water pump at a Springfield, Illinois water utility that was initially attributed to hacking because it was accessed from a Russian IP address. It turned out it was accessed by a contractor on vacation in Russia at the request of the utility. Obviously, this example demonstrates intent takes time to determine. The Project 2009-01 Disturbance and Sabotage Reporting even stated this in their recent posting for the reason they decided not to define sabotage because intent is so difficult to determine. Thus, we recommend striking malicious from the definition. BES Cyber System includes the capitalized term Maintenance Cyber Asset. The capitalization is an indication that the term is defined in the NERC Glossary. Neither can we find such an existing definition nor is it the definition proposed in this standards project. Either the capitalization needs to be removed or the term needs to be defined. We recommend the latter. BES Reliability Operating Services should not be a NERC defined term. Many of these services are similar to the Policy 10 – Interconnected Operating Services that was never passed because industry could not agree on it. It is doubtful industry is going to agree on this broad definition that could apply outside the CIP standards. Furthermore, there are several issues with the definition. First, it is not clear what is intended by including contingency reserve in parentheses after spinning reserve. Contingency reserve can include spinning and non-spinning components as long as it can respond in 15 minutes to meet DCS. Spinning reserve does not necessarily relate to contingency reserve directly in that it can include unloaded on-line reserves that respond in more than 15 minutes. Furthermore, NERC has two conflicting definitions of spinning reserve: Spinning Reserve and Operating Reserve – Spinning. One definition limits the spinning reserve to what can respond in 15 minutes and the other does not. Second, it is not clear what is intended by including contingency reserve in parentheses after non-spinning reserve. Per NERC definition, non-spinning reserve is time limited but not necessarily limited to the 15 minute limit set in DCS and, thus, on contingency reserves. Thus, while some contingency reserves may be non-spinning, not all non-spinning reserves will be contingency reserves. Third, under the Managing Constraints section of the BES Reliability Operating Services definition, ATC is identified. It should be removed. ATC is not used to manage constraints but rather to sell transmission service. That transmission service may never be used. While ATC is calculated using reliability components, it is not a reliability service but a commercial service. FERC even acknowledged that the MOD (ATC) standards were designed primarily “to ensure non-discriminatory allocation of transmission capacity among transmission market participants” in paragraph 30 of the order approving FAC-013-2 (137 FERC ¶ 61,131 Docket No. RD11-3-000). Fourth, the Inter-Entity Real-Time Coordination and Communication section of the BES Reliability Operating Services definition should be struck as it is just a supporting activity for all the other services. CIP Exceptional Circumstance should be modified to include a clause that other circumstances of similar nature and/or impact could be included as a CIP Exceptional Circumstance. Otherwise responsible entities could be put in a position of having to choose to violate some the CIP requirements because the SDT did not think of a particular exceptional circumstance that should have been included. CIP Senior Manager should be struck along with all references to CIP Senior Manager in the CIP standards. This definition and associated requirements dictate a corporate governance structure for no apparent reliability reason. A responsible entity should be free to have two, three, or more personnel oversee various portions of the CIP program. The responsible entity will still be required to meeting the CIP requirements regardless. Furthermore, mandating a single CIP Senior Manager implies that potential

for sanctions up to $1,000,000 per day per violation are not enough to get senior management's attention. This implication is totally contrary to the purpose of making standards enforceable by such sanctions. No other standards require identification of single senior manager and no reliability justification has ever been provided for why one is needed for the CIP standards. It is not clear that Control Center needs to be defined. EOP-008-1 (Loss of Control Center Functionality) was written without defining control center. We are concerned that this definition could cause confusion with EOP-008-1 and believe the definition needs to be coordinated with that standard. Reconvening the SDT that worked on EOP-008-1 may be necessary to accomplish this. For Interactive Remote Access, how do Cyber Assets used by the Responsible Entity differ from those used by employees? It is not clear why Responsible Entity is delineated in such a way. Reportable BES Cyber Security Incident needs to be coordinated with the Disturbance and Sabotage Reporting standards drafting team.

Yes

In the Background section, the SDT describes that the responsible entity will have a choice to evaluate BES Cyber Assets individually or collectively in a BES Cyber System. The opening paragraphs for High Impact or Medium Impact criteria need to be modified to make this clear. As written they do appear to provide a choice by stating "Each BES Cyber Asset or BES Cyber System". However, it does not make clear whose choice that is. The auditor might decide the choice belongs to them. Thus, these paragraphs need to be modified to make clear the choice belongs to the responsible entity. While similar and conforming changes need to be made to the Low Impact Rating as well, one additional change needs to be made. "All other BES Cyber Assets and BES Cyber Systems" should be changed to "All other BES Cyber Assets or BES Cyber Systems". Otherwise, there is no choice because both have to be included. This change would also conform Low Impact Rating to the Medium and High Impact Rating sections. While there are limitations on the TOP Control Centers such that not all TOP Control Centers will be included with a High Impact, there is no such limitation on the BA Control Centers. We recommend a similar limitation be place on a BA Control Center such that if the BA is not controlling assets that meet certain criteria in the Medium Impact they should not be included. There many small BAs that simply won't have a broad impact on the Interconnection and, thus, should not be included. Criterion 1.4 which obligates certain GOP control centers to be rated High Impact includes criterion 2.12 as one of those reasons. 2.12 should be struck as it deals with UVLS and UFLS which are not GOP functions. Criterion 2.3 creates an implied obligation on the Planning Coordinator (PC) or Transmission Planner (TP) to designate generation that is necessary to avoid BES Adverse Reliability Impacts. It is implied because there are not any requirements in any standard including the TPL standards that require the TP or PC to designate generation necessary to avoid BES Adverse Reliability Impacts. In fact, BES Adverse Reliability Impact is not even used in any requirements that pertain to the PC or TP. The implied obligation creates a compliance conundrum. Since it is only an implied obligation and not an explicit requirement, the PC and TP will never be required to meet it. How then, does the GOP or GO insure they get the information they need from the PC or TP? They have no recourse. Use of BES as a descriptor of Adverse Reliability Impact in Criterion 2.3 is redundant with the definition of Adverse Reliability Impact and should be struck. Criterion 2.3 focuses on the long-term planning horizon which is contrary to the standard. The standard focuses on reliability impacts caused on the BES in a 15 minute timeframe from the misuse, degradation or unavailability of the BES Cyber Asset or BES Cyber System. It does not make sense to subject BES Cyber Assets and/or BES Cyber Systems within a generator plant or GOP control center to these standards if a generator is identified as needed for reliability four years out but is not identified from year 0-3. For Criterion 2.5 regarding Cranking Paths, the last two bullets are confusing and the wording should be clarified. The graphic provided on page 26 in the Application Guidelines help with that clarification and the drafting team should consider adding this as an attachment so that it will remain with the standard. It is premature to base criterion 2.7 on the "Integrated Risk Assessment Approach – Refinement to Severity Risk Index". It is still a work in progress. This document and approach is being developed under the purview of the Planning Committee's (PC) Reliability Metrics Working Group (RMWG). The PC has not approved any of the indexes. The only thing the PC approved was the approach and framework. At the December 2011 PC meeting, it was clear that the RMWG has additional work to do to finalize the indexes. Thus, it is premature to use any of these indexes in the "Integrated Risk Assessment Approach – Refinement to Severity Risk Index" in a standard. At the very least, use of them should be coordinated with the PC and RMWG. Criterion 2.9 is redundant to Criterion 2.8. FACTs devices are Transmission Facilities and are covered in 2.8. Criterion 2.11 presumes that failure of an SPS or RAS would cause an IROL violation. This is not likely. An SPS or RAS may be implemented for a specific contingency for example. As an example,

when that contingency happens, certain switching might need to occur or generation run back. These automated actions might enable a higher limit on an IROL associated with a transmission corridor. If the SPS was not available, the limit would likely be lowered but not necessarily violated. A violation would depend on actual system conditions at the time. Thus, the language should probably be change to something along the lines of impacts or enables higher IROL limits. Criterion 2.13 has control centers in lowercase. This would mean that the proposed NERC glossary definition does not apply. Is this the intent? If so, how would this meaning of control center be different?

No

We think Requirement 1 and associated Attachment 1 should focus on identifying the BES Facilities that are important and then the associated BES Cyber Systems and BES Cyber Assets. Otherwise, all BES Cyber System and BES Cyber Assets will have to be inventoried. While the Background section states "Requirement 1 only requires that discrete identification of BES Cyber Systems and BES Cyber Assets for those in High and Medium categories", we do not see how a responsible entity can demonstrate that it has correctly identified all High and Medium Impact BES Cyber Systems and BES Cyber Assets unless it has a complete inventory of all BES Cyber Assets and BES Cyber Systems. We can envision auditors asking for such an inventory. Part 1.1 needs to be further refined regarding what kinds of changes are included. By the NERC Glossary definition, Facility can include relay equipment associated with protecting a transmission line as part of the "set of electrical equipment that operates as a single Bulk Electric System Element". Thus, a change to a relay setting could be could be inadvertently included. It should not be. We suggest the changes be limited to topological changes, generator interconnections and generator uprates and equipment retirements. While other changes such as permanent derates may allow that responsibility entity to lower the categorization of BES Cyber Systems and/or BES Cyber Assets, the reduction in compliance burden will cause them to do this. Thus, we don't need to increase their compliance burden by requiring them to do it for permanent derates.

No

Because regional entities already expect evidence to be signed and dated by persons of authority, there is no reason to have a specific requirement to have the CIP Senior Manager or delegate do this. The requirement is unneeded and the compliance auditor likely won't accept evidence for Requirement 1 unless it has been approved anyway by a person of authority. Thus, this requirement actually creates a form of double jeopardy that an entity could be held in violation of Requirement R1 and R2 for failure of the CIP Senior Manager or delegate to approve the list of BES Cyber Asset and BES Cyber Systems categories. Because there is no question dealing with other sections of this standard, we are adding comments regarding those sections here. We disagree with all the specificity in the applicability and facilities section for Distribution Provider (DP) and Load Serving Entity (LSE). These sections are not consistent with the Compliance Registry Criteria and will only cause confusion. There is no specific compliance registry criterion for including a DP that has been included in the Transmission Operator's restoration plan. Because NERC clearly states in their Rules of Procedure Appendix 5B Statement of Compliance Registry (see the first paragraph on page 2) that they will not enforce the standards against entities that are not registered, the standard simply couldn't be enforced against such an entity included in the TOP's restoration plan unless they were already registered. Furthermore, the Compliance Registry Criteria already allow NERC to register a responsible entity as a DP and LSE if that entity "owns, controls, or operates facilities that are part" of a required UFLS or UVLS program, special protection system (SPS) or transmission protection system. Since the DP or LSE with a required UFLS or UVLS program, SPS or transmission protection system, is already registered, how does this applicability section provide any more clarity? The DP or LSE will know whether they own or operate these facilities and simply will provide the appropriate response in any required CMEP submissions such as audits and self-certifications. If the responsible entity is not registered as an LSE or DP even if they own these facilities, then again NERC can't enforce these proposed CIP standards against the entity per their Rules of Procedure Appendix 5B Statement of Compliance Registry (see the first paragraph on page 2). In the Facilities section, we are concerned that non-BES Facilities will be included in the standard. Non-BES Facilities should not be included at this juncture given that the Project 2010-17 Definition of Bulk Electric System drafting team is just beginning its work on the second phase of defining the BES. Until this work is completed, non-BES Facilities should not be included and, then, they should only be included with significant justification. There should be a high bar for deviating from the BES definition particularly since it will be recent and have considered all issues facing the industry at that time. The application guidelines have not clearly

identified all functional entities that might have some responsibility for the various BES Reliability Operating Services. For instance, in the Dynamic Response section, Special Protection Systems responsibilities are attributed to only TO but this could be a GO or even DP responsibility. UFLS and UVLS are only attributed the DPs but the TO could choose to implement these systems on the transmission system. Governor Response could also be a GOP responsibility. Another example would be the current and next day planning in the Situational Awareness section. It is only attributed to the TOP even though there are NERC standards that require the RC to perform next day planning. In the Managing Constraints section, the responsibility for interchange schedules is attributed to the TOP and RC. It should be attributed only to the Interchange Authority or Interchange Coordinator. In the Restoration of the BES section, the responsibility for off-site power for nuclear facilities is attributed to the TOP. In the NUC standard, it is actually attributed to the transmission entity which could be one of eleven functional entities. Since there many errors (we did not identify all of them) in attributing responsibility in this section, we suggest the drafting team completely review this section and update it or consider removing the responsibilities altogether as their purpose is not clear. We believe the statements beginning on page 23 and continuing on page 24 of the High Impact section of the applicability guidelines regarding TOP delegation to the TO should be removed. If the TOP has delegated some functions to the TO that would otherwise have been carried out in the TOP Control Center and might have resulted in additional TOP BES Cyber Assets and BES Cyber Systems being categorized as High Impact, this delegation should not have an impact on the TOs categorization of BES Cyber Systems and BES Cyber Assets. First, the TOP is still responsible and can't pass that responsibility on through a delegation agreement. Thus, the TOP and TO will have to address this in their delegation agreement. Second, the TOP likely does not own these BES Cyber Assets at the TO. The TO likely owns these BES Cyber Assets and BES Cyber Systems, and they should be classified according to the criteria established for TOs in Attachment 1. Use of the term asset in the definition requires ownership by the responsible entity. If is not owned by the TOP, it is not a TOP asset and, thus, not a TOP BES Cyber Asset. Third, control Centers for TOs are not addressed in Attachment 1. Fourth, this appears to address some concerns regarding some RTO/ISO's TOP registration models that have been expressed in various forums by regulators. These concerns should not be addressed in piecemeal fashion but holistically in a forum covering all concerns and issues with the registration model. Fifth, there is nothing in the requirements that requires these BES Cyber Assets and BES Cyber Systems to be categorized in this manner. The application guidelines are not requirements and cannot modify the requirements. They can only help explain the requirements. However, these statements are fundamentally altering the requirements and how the attachment 1 criteria are applied. In the first paragraph on page 25 in the application guidelines, there is statement that indicates there may not be a Planning Coordinator for a given area. This statement is contrary to the Section 501.1.4 of the NERC Rules of Procedure. This section states that the registration process shall ensure that "no areas are lacking any entities to perform the duties and tasks identified in and required by the reliability standards". In the third paragraph on page 25 in the application guidelines, Category D contingency should be removed. The TPL standards only require a Planning Coordinator or Transmission Planner to document the impacts of Category D contingencies. There are no performance requirements for Category D contingencies. Thus, it is highly unlikely that any Planning Coordinator or Transmission Planner could ever justify the costs for reliability must run unit through Category D contingencies to its regulator, and, thus, there likely will not be any. In several places in the application guidelines (occurs on pages 26, 27, and 29), exceeding an IROL is discussed when the SDT really means violating an IROL. An IROL by definition has two components. It has a limit and a time constant called Tv. This time constant can be up to thirty minutes and usually is. The time constant is set based on how long the IROL limit can be exceeded without exposing the BES to an unacceptable risk. Thus, an IROL is only violated once the limit has been exceeded for a time greater than Tv. An IROL is exceeded but not violated when the time of the exceedance has not reached Tv. We suggest the drafting team modify the application guidelines in this standard and any other standard with the appropriate use of exceed or violate for the IROL consistent with this explanation. In the third bullet on page 29, the term regional load shedding requirement needs to be made consistent with the new UFLS standard. The UFLS program will be developed by the Planning Coordinator and not the Regional Entity. The NERC adopted version of the standard does not even require a regional version of the standard as was originally proposed.

No

The VSLs for R2 are not consistent with the requirement. Requirement R2 allows the CIP Senior Manager or delegate to approve identification and categorization of High and Medium Impact BES

Cyber Assets or BES Cyber Systems. The VSLs drop the “or delegate” language which implies the CIP Senior Manager has to approve the categorization and identification. The “or delegate” language should be added back.
No
This requirement should be struck along with all references to CIP Senior Manager in the CIP standards. This requirement dictates a corporate governance structure for no reliability reason. An entity should be free to have two, three or more officers or personnel to oversee various portions of the CIP program. The responsible entity will still be required to meet the CIP requirements regardless. Furthermore, mandating a single CIP Senior Manager implies that potential for sanctions up to $1,000,000 per day per violation are not enough to get senior management’s attention. This implication is totally contrary to the purpose of making standards enforceable by such sanctions. No other standards require identification of single senior manager and no reliability justification has ever been provided for why one is needed for the CIP standards.
No
We agree there should be “one or more documented cyber security policies that represent the Responsible Entity’s commitment to the protection of its BES Cyber Systems and addresses” the required ten topics seem. However, the items that a “Responsible Entity should consider” for inclusion in its cyber security policy as stated in the Guidelines and Technical Basis section (application guidelines) of the standard appear to be written as requirements and the drafting team should consider moving them to R2 if auditors will ultimately treat them as requirements. This will reduce compliance risk by leaving no doubt as to the minimum amount of information that is to be included for each topic. Requirement R2 should also be modified to make it clear that an entity may write exceptions into their cyber security policies. FERC made it clear in Order 672 that only the requirements in a standard are enforceable and part of the standard. Thus, while the application guidelines make it clear the drafting team can write in exceptions to its cyber security policy, the application guidelines are not enforceable and there is no way of ensuring that auditors follow them. Furthermore, we believe the fourth bullet in section 2.3 Remote Access regarding including language in contracts with vendors, consultants and contractors requiring them to follow the responsibility entity’s cyber security policy should be modified. The bullet should apply to future contracts and not existing contracts to avoid the need to renegotiate all contracts which puts the responsible entity at a significant disadvantage particularly with some contracts such those with EMS vendors. In addition, M2 bullet 2 says “Records that indicate the required ten topics were implemented.” What exactly does “implemented” mean in this case? That the items the responsible entity should consider for each of the topics are included in the policy(ies)? This needs to be clarified.
No
What does “initially upon the effective date of the standard” mean? It could be interpreted that the cyber security policies would need to be reviewed and approved on the date the standard is effective which is not reasonable for a myriad of reasons. A couple of those reasons could include that the effective date could be a holiday or weekend or the CIP Senior Manager is not available (they could be incapacitated). Ultimately, we believe that the intent is for the cyber security policy to be in effect and approved by the effective date rather than on the effective date and to ensure that is has been reviewed recently particularly since the implementation plan is a minimum of 18 months. Then going forward subsequent reviews and approval would take place at least once per calendar year not to exceed 15 calendar months. If this intent of this requirement, there really is no way to ensure the review occurred recently without making the requirement retroactive which clearly cannot be done within a requirement. In addition, M3 bullet 1 implies that a Responsible Entity needs to have a “document management system.” The word “system” could mean an application to manage documents. It could also mean a process for managing documents. Rather than leave it open to interpretation, we recommend eliminating the phrase, “from a document management system.”
No
Awareness of a security program is covered in depth in CIP-004-5 and ensuring accessibility and availability of cyber security policies goes hand in hand with this. We recommend removing R4 from CIP-003-5.
No
Based on the assumption that there will be a CIP Senior Manager, we generally agree with the use of a delegate. We even believe it would be reasonable for a delegate to approve the cyber security

policy. However, we do not agree with the use of “CIP Senior Manager” in this requirement based on our comments for R1 in question 6.
No
Based on the assumption that there will be a CIP Senior Manager, we generally agree with the use of a delegate. We even believe it would be reasonable for a delegate to approve the cyber security policy. However, we do not agree with the use of “CIP Senior Manager” in this requirement based on our comments for R1 in question 6.
No
We disagree with the VSLs for R2. More gradations could be provided based on the number of parts missed. Since there are 10 parts, there is plenty of room for four VSLs. The VSLs for R6 should consider using the numbers of days that documentation of the change to the CIP Senior Manager documentation is late. Use of number of days late is a common way to write a VSL and allows more gradations.
No
For Part 1.1, the rationale box does not appear to agree with the requirement. It states the need to ensure everyone with authorized access receives this awareness was removed. Yet, the requirement applies to the responsible entity and does not appear to exclude anyone with authorized access. Which is it? Furthermore, the rationale box should be more specific and use the full names of both types of access which are: authorized electronic access and authorized unescorted physical access. Otherwise, generically referring to authorized access could mean one or the other but not both, or it could mean both.
No
We agree with the concept that training should be role based. As an example, a system operator who is an end user of an EMS does not need most of the training identified in the various parts of Requirement 2. The system operator certainly does not need training on recovery plans for BES Cyber Systems but might need training on the visitor control programs and how malicious actors might use social engineering to gain access to the EMS. The problem we see with the requirements and it parts is that it does not make clear anywhere the need to identify what training each role would receive. Rather it only states that roles must be identified and then identifies training in the various requirement parts that apply to the main requirement which could be construed as applying to the whole training program including all roles. The paragraph references in the rationale boxes for parts 2.6 and 2.7 are inaccurate. Paragraphs 632-634, 688, and 732-734 refer to CIP-007 and CIP-009. There are no references to issues in CIP-004. While paragraph 413 does discuss CIP-004, it only describes what is in the standard and not any changes directed to the standard. In regards to Part 2.6 and storage media, the only mention in Order 706 of storage media is in paragraph 635 and it directs NERC to determine what it means to prevent unauthorized retrieval of data using storage media.
No
This requirement needs to be clarified that it only is intended to require appropriate role-based training for each individual with authorized electronic access or authorized unescorted physical access based on their specific job responsibilities and not the entire cyber security training program identified in R2. Use of the word “needing” is problematic. An entity cannot grant authorized electronic access or authorized unescorted physical access unless it is needed per CIP-007-5 R5. We suggest changing “each individual needing authorized electronic…” to “each individual with authorized electronic…” For consistency across the standards and clarity, we suggest every use of “authorized electronic or unescorted physical access” be replaced with “authorized electronic access or authorized unescorted physical access”. This will help to avoid similar confusion that arose in previous versions of the standard in which it was not clear if “authorized” applied only to electronic access or unescorted physical access. It will further make it clear that authorized electronic describes one type of access. Regardless of how it is written, it needs to be consistently used across that standards and it is not.
No
Part 4.2 may not be possible to complete. While we agree with the need to conduct seven year criminal history checks, obtaining all addresses may not be possible. The responsible entity can verify the current address or a recent address from reviewing a driver’s license but after that the responsible entity cannot with certainty verify that it has all of the former work, home and school addresses of the employee. The employee may not provide the addresses and the background check may not provide these additional addresses. The requirement needs to be clear that the responsible

entity may request this information from both the vendor providing the background check and the employee but will not be held accountable for either party's failure to provide a complete list of addresses. Part 4.3 could be problematic for a responsible entity and needs to be clarified that the responsible entity does not need to establish hard and fast criteria that must always be followed. Finding qualified personnel to work in these highly specialized fields is challenging enough without adding this additional constraint. Background checks may certainly reveal problems with an otherwise qualified person. While some of these problems would be obvious reasons to disqualify a person, others may simply require further research and explanation from the individual for why it is not a problem.
No
In general, we agree with the requirement but believe the requirement should be further clarified, perhaps in the measurement, that in no circumstance should a responsible entity be asked or required to show the personnel risk assessment for an individual to auditor and enforcement personnel. There are a myriad of reasons not to show the actual personnel risk assessment including privacy concerns and other applicable laws may prevent this.
No
The application guidelines on page 44 state that access authorization and provisioning should not be performed by the same person. While this is a laudable goal, it should be clear that small entities may simply not have the staff to accommodate this guideline. We suggest adding "where possible" to this statement.
No
It is not clear why resignations are separated from terminations in Parts 7.1, 7.3, 7.4 and 7.5. Resignations are voluntary terminations. We are unsure what the drafting team intends to accomplish by splitting them out. Where do retirements and layoffs fit in? Since there does not appear to be any different requirements on resignations and terminations, we suggest to use only the generic termination to avoid this confusion. Part 7.2 does not address the situation for phased transfers. For many entities, a transferred employee could continue to need authorized electronic access and authorized unescorted physical access for a long period of time to provide support particularly if a new employee is being trained. This could occur long after the transfer date. While the application guidelines do address this issue, they are simply not requirements and NERC is not bound to follow them. Thus, we suggest making Part 7.2 more generically state that the authorized electronic access and authorized unescorted physical access should be terminated once management determines it is no longer needed. We are a little surprised that the application guidelines state in the scenario table that no action is required to revoke access in the event of a death. While we agree there would be no immediate additional risk for obvious reasons, access should still be revoked at some point.
No
VSLs for Requirements R2 and R3 should have more gradated levels. For R2, there could easily be several roles which would allow for more than two VSLs. Since there are 10 parts to the requirement, four VSLs could easily be written based on the number of parts missed. For R3, more VSLs could be written based on the percentage of individuals that were not trained. The Severe VSL for Requirement R5 incorrectly includes personnel risk assessments (PRA). PRAs are dealt with in Requirement R4.
No
The requirements of Parts 1.2 and 1.3 make no mention of egress while the associated measures specifically mention it. Does the drafting team intend for there to be procedural or physical access controls regarding egress? If so, that is not clear in these standards at all and could set up a responsible entity for a compliance violation. We do not believe that egress controls should be necessary. Only ingress controls are necessary to prevent access to unauthorized individuals. Egress really only helps in knowing who is currently within the Defined Physical Boundary which might provide some value but the expense of installing egress physical access controls would likely far outweigh any benefit. It is unclear how the "operational and procedural controls" required in R1.1 differ from the "physical access controls" required in R1.2 and R1.3. Suggested methods for restricting physical access are given in the "Guidelines and Technical Basis" (application guidelines)

section, but none are given for “operational and procedural controls.” Additional discussion in the application guidelines on these operational and procedural controls would be helpful in understanding them. Also, regarding the application guidelines, it would be helpful if the section labeled “Requirement R1,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
We believe that this proposed requirement improves upon the existing requirements. However, we believe that individual point of contact could be confusing. We recommend changing it to escort and making it clear in the application guidelines that this would be the main escort with responsibility for the visitor but not necessarily someone who is with the visitor the whole time. Others could also temporarily escort the visitor. Regarding the “Guidelines…” section, it would be helpful if the section labeled “Requirement 2,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
Regarding the “Guidelines…” section, it would be helpful if the section labeled “Requirement 3,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
A visitor control program is intended to identify and log visitors to the Defined Physical Boundary (DPB). They cannot gain access due to other requirement such as CIP-006-5 Requirement R1 that compels the responsible entity to establish physical access controls. Furthermore, the training requirements of CIP-004-5 compel a responsible entity’s personnel with authorized unescorted physical access to have been trained on who has access and that visitors must be escorted. Thus, the visitor control program can only be an administrative function that is truly intended to keep track of those visitors that have been to the DPB. By definition, administrative requirements should have a Lower VRF. Thus, CIP-006-5 Requirement R2 should have a Lower VRF.
No
Part 5.5.2 needs to be refined further. It needs to be clear that maximum complexity regarding character types in the password applies if the BES Cyber System cannot support at least three character types. We suggest appending “if less than three character types” to the end of the requirement for further clarity.
No
Because there are likely many ports for Requirement R1, the four VSLs could be written based on the percentage of ports missing from documentation. For Requirements R2-R4, there will likely be many BES Cyber Systems to which the requirements apply. Four VSLs could easily be written based on the number of BES Cyber Systems for which the requirement was missed.
No
EOP 4 in the Rationale box should be replaced with EOP-004. While Part 1.2 requires a process to identify Reportable BES Cyber Security Incidents, there is no indication of who is to receive these reports. There is only Part 1.3 that requires the responsible entity to identify internal and external staff to which to communicate the “incident”. Does that mean the list of recipients is totally up to the responsible entity and could be null? If not, then the drafting team needs to identify the minimum list of recipients. In Part 1.3, we assume the drafting team means Reportable BES Cyber Security Incidents by the use of the term “incident”. If this assumption is correct, please replace “incident” with “Reportable BES Cyber Security Incident”.
No
The requirement in part 2.1 appears to apply to actual BES Cyber Security Incidents. However, the requirement states that deviations from tests should be recorded. Thus, “or test” needs to be struck. R2 Part 2.2 uses the phrase “initially upon the effective date of the standard.” It is not clear as to the meaning of this phrase. It could be interpreted that the BES Cyber Security Incident response plan(s)

would need to be implemented either by responding to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise on the date the standard becomes effective. This is not reasonable. If the intent of this requirement is to do an initial implementation within some time period of the standard becoming effective, then the requirement should state a time period for this to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. No application guidelines were written for this requirement. The drafting team should consider either writing some or making a statement that they are purposely omitted.

No

R3 Part 3.1 uses the phrase “initially upon the effective date of the standard.” It could be interpreted that a review of each BES Cyber Security Incident response plan would need to take place on the date the standard becomes effective. Because Requirement R1 compels the development of the response plan, it does not make any sense to compel review of the response the same day the requirement of the response plan becomes effective. Rather the response plan review should be required the following calendar year after its initial approval. No application guidelines were written for this requirement. The drafting team should consider either writing some or making a statement that they are purposely omitted.

No

The stated rationale for Part 1.1 does not support the change and additional rationale needs to be provided. Paragraph 694 of Order 706 requires NERC to develop a specific requirement to implement the recovery plan. This requirement is not an implementation requirement but still a requirement for what to include in the plan. Thus, we do not see how the rationale supports the requirement. Part 1.2 should not require either names or titles. These are problematic in that the recovery plan has to change for every personnel move which includes transfers, terminations and promotions. A promotion of IT Analyst to Senior IT Analyst would necessitate an unnecessary change. A better approach would be to allow the use of generic roles such as analyst or even perhaps staff from department X. The requirement needs to allow some flexibility to avoid unnecessary paperwork that provides no reliability benefit. The drafting team should develop application guidelines for these requirements. At the very least, the reference to the FAQs and CIPC Guidelines should be more specific with links to each guideline and FAQ.

No

Part 2.1 uses the phrase “initially upon the effective date of the standard.” It could be interpreted that the recovery plan(s) would need to be implemented either by responding to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise on the date the standard becomes effective. This is not practical for many entities and especially for smaller entities. Part 2.2 of CIP-008-5 R2 already requires BES Cyber Security Incident response plans to be exercised on the effective date of the standard. Many of the same staff involved in the BES Cyber Security Incident response plans will likely be heavily involved in the recovery plans. The important part is that the recovery plan will be in place on the effective date per CIP-008-5 R1 and will likely have been tested prior to the effective date. Thus, the requirement should simply state a reasonable time period that can be met by limited staff for the actual implementation or exercise to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. Part 2.2 has potentially has a similar issue to Part 2.1 but is less clear. Rather than use the full term “initially upon the effective date of the standard” it just states that the test must be conducted initially. We assume the drafting team meant for this to be conducted on the effective date similar to Part 2.1. This makes completing this part and other parts mentioned in the previous paragraph even more impractical. The requirement should simply state a reasonable time period for the actual implementation or exercise to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. Since Part 2.3 requires a full exercise in representative environment every 39 months and is required to be included per FERC directive, we recommend that it be limited to High Impact BES Cyber Systems. Conducting this test in a representative environment could get very expensive because responsible entities may have to purchase the appropriate equipment to set up a parallel environment. This is simply not practical or cost effective to do for every BES Cyber System. Is it really practically to set up a representative environment for every 500 kV substation or special protection system for testing?

No
Part 3.1 should be modified to require the first review of the recovery plan in the subsequent calendar year to the approval of the requirement. To accomplish this, the drafting team should strike “initially upon the effective date of the standard and”. CIP-009-5 R1 already compels the responsible entity to have a recovery plan and becomes effective on the same day as Part 3.1. Thus, the plan will already have been reviewed when it was developed and approved. Thus, it does not make sense to have a separate review in Part 3.1 on the effective date. For consistency with Part 3.3, R1.2 in Part 3.5 should be written as Requirement R1, Part 1.2.
No
The VSLs for Requirement R1 should include more gradations than two levels based on the number of parts missed. For Requirement R2 and R3, four VSLs could be written based on the number of days late for completing the task. This is a common way to write VSLs.
No
Part 1.1.6 could be redundant with CIP-007-5 Part 2.2. While CIP-007-5 Part 2.2 does not explicitly require documentation of the security-patch levels, demonstrating compliance with it ultimately will require such documentation. Thus, it becomes redundant with Part 1.1.6 of CIP-010-1 R1. If not redundant, it certainly sets up a high probability for double jeopardy because each compliance violation of CIP-007-5 Part 2.2 will likely result in a violation of Part 1.1.6. Part 1.2 is unclear. Is this intended to require the CIP Senior Manager or delegate to authorize the process to develop a baseline configuration or is it intended to require the CIP Senior Manager or delegate to authorize deviations to the baseline? As a result, Part 1.2 needs to be clarified. As it is written now, the only clear requirement from Part 1.2 is the need to document baseline configuration deviations. Part 1.4.1 requires the responsible entity to identify the cyber security controls that could be impacted by the change. This appears to be the first use of cyber security controls in the library of CIP standards. As a result, the intent and meaning of the term needs to be further clarified.
No
Comments: Part 3.1 uses the phrase “initially upon the effective date of the standard.” It could be interpreted that the security controls for every applicable BES Cyber System and BES Cyber Asset need to be assessed on the date the standard becomes effective. This is not practical particularly for smaller entities. Several other requirements including Part 2.1 of CIP-009-5 and Part 2.2 of CIP-008-5 R2 already require significant action on the effective date of the standards. Part 2.1 of CIP-009-5 requires recovery plans to be implemented on the effective date and Part 2.2 of CIP-008-5 R2 requires the BES Cyber Security Incident response plans to be exercised on the effective date of the standard. Imagine the amount of personnel and effort necessary to complete all of these tasks on (not by) the effective date. Many of the same staff involved in the BES Cyber Security Incident response plans and recovery plans will likely be heavily involved in the vulnerability assessments. The requirement should simply state a reasonable time period for the vulnerability to be completed after the effective date of the standard or make it clear that the vulnerability assessment needs to be completed by the effective date and not on. Part 3.2 has a similar issue as Part 3.1 in that it appears to require a vulnerability assessment for all High Impact BES Cyber Systems on the effective date of the standard. We have the same issue with this requirement in that the same limited set of staff will likely be responsible for completing these assessments as the tasks compelled by several other requirements that must be complied with on the same effective date.
No
In general, the VSLs escalate violations to the higher end of the sanctions matrix too rapidly for minor violations. This could be fixed by writing VSLs for each level rather than just High and/or Severe VSLs in some cases. For example, if an entity fails to establish a single baseline on one applicable BES Cyber System or BES Cyber Asset per Requirement R1, it would be deemed a High VSL. If that is one out of one thousand BES Cyber Systems or BES Cyber Assets, this would seem excessive. Likewise, if an entity is one day late in updating their baseline configuration per Requirement R1, the violation would be deemed Moderate. This is not consistent with many other requirements in the CIP proposal which provide four VSL based on the number of days late.
No
The rationale for Requirement R1 indicates Requirement 4.1 was moved to the BES Cyber System Information definition. It does not reference which standards the requirement comes from. It needs to

for clarity. Part 1.1 needs to be clarified. We believe the requirement pertains to ensuring BES Cyber System Information is marked in some way to be clear it is BES Cyber System Information. However, we are concerned that requirement could be interpreted as needing to develop a method to ensure that all BES Cyber System Information has been found and there is no extraneous information. In other words, we are concerned the requirement could be interpreted as requiring the method to be some sort of search process. Use of the word identify is what causes us concern since it is what is used in CIP-002-5 regarding finding all of the BES Cyber Assets. We think this problem would be solved by changing "identify" to "mark" and providing some discussion of the intent of the requirement in the application guidelines. Part 1.3 needs to be modified. It requires the responsible entity to assess its adherence to its BES Cyber System Information protection process "upon the effective date of the standard". This does not make any sense since the responsible entity will have just then been required to utilize the BES Cyber System Information protection process. What will they assess? This requirement should not require this assessment until the process has been in use for a year. Part 1.3 uses a term "protection process" that was not used previously in the requirement. For consistency with other requirements and clarity, we suggest that either that term be used in Requirement R1 instead of just the term process or that "protection" be struck in Part 1.3 and replaced with a reference to the main requirement.

No

We agree with the implementation plan concept that essentially bypasses the effective dates of version 4 of the standards for version 5. This will significantly lessen the compliance burden for responsible entities to avoid two separate transitions and avoid the confusion of preparing for version 5 while still preparing for version 4. We believe that some requirements should have delayed implementations plans rather than become effective on the same date as the remaining requirements. Some requirements are dependent on the completion of other requirements and do not make sense to implement until the other requirements have been in effect for some time. Consider Part 1.3 of CIP-011-5. It requires the responsible entity to perform an assessment of its adherence to the BES Cyber System Information protection process. However, the protection process is only required to be in effect the same day. What sense does it make to assess adherence to a process that was just started? The drafting team should perform a complete review of all the requirements for dependencies and determine an appropriate staggered implementation for them. The first sentence in the "Proposed Effective Date for Version 5 CIP Cyber Security Standards" on page 2 should be modified. It states the responsible entities must comply with the definitions on the effective date. Definitions have no compliance obligations. They simply become effective and help explain the requirements.

Individual

Tracy Sliman

Tri-State G&T Inc.

Yes

BES Cyber System Definition – Change: "Maintenance Cyber Asset" To: "Transient Cyber Asset" Rationale: Consistency and no definition proposed for Maintenance Cyber Asset. BES Reliability Operating Services –AECI believes the following BES services should be removed from the BES Reliability Operating Services, because they fail to meet the "real-time reliable operation of the BES" 15-minute adverse-impact criteria: 1) Balancing Load and Generation, (other than ACE, nothing else in this category can have a 15-minutes or less impact, and ACE availability and integrity are addressed within the BAL Standard, so including here is double-jeopardy.) 2) Restoration of BES, remove, "but is not limited to", and list the aspects of the Restoration of BES Operating Service. 3) Situational Awareness – Frequency Monitoring – (While frequency monitoring is important, contrary to the underlying position within the CIP standards, redundancy of frequency monitors really does matter, and the standard should probably leave this one off, in order to avoid only a few instances of frequency-monitoring equipment being implemented. Also, the availability of a reliable Frequency Monitoring signal is subject to a strict BAL standard. Control Center Definition – Change: "BES generation facilities or transmission facilities", To: "BES generation facilities or BES transmission facilities", Rationale: Clarity of scope.

No

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
R7 - Change: “at time of resignation or termination” To: “within 24 hours of resignation or termination” Rationale: Consistency with hard time-frames asserted with other sub-requirements, with reasonable delay for uncontrollable circumstances surrounding some separation of employment.
Yes
No
Low impact Cyber Systems should not be required to adhere to part 1.1 in the table.
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
Measures required to show evidence of this requirement are unclear.
Yes
R4 part 4.5 – The requirement to review security event logs every two weeks is very onerous. Recommend the current practice of 90 day review or the ability to skip a manual review in favor of automated alerting on specific security events.
No
R5.5.1 Change: reword as “Minimum Password length of at least 8 characters, or maximum supported by the BES Cyber System if less than 8 characters is supported.” Rationale: Clarity R5.5.3 Change: “based on” To: “based upon” Rationale: grammatical
Yes
Yes
Yes
Yes
No
R1..R3 VSLs for Low Impact Assets - Change: High VSL To: Low VSL and Change: Severe VSL To: Moderate VSL. Rationale: align risk with severity. R3 VSL - Change: “30 calendar days” To: “60 calendar days” then Append: “within 60 calendar days” to last sentence. Rationale: Consistency and align timeframe with Severity. (Failure to review within 30 days might be considered High, and written into that column – see note on Low Impact Asset VSLs above.)
Yes
No
R2.3 Guidelines – Add: Guidelines! Rationale: Without some related guidelines, the phrase “in a representative environment that reflects the production environment” introduces too much ambiguity and opportunity for disagreement between Responsible Entities and Auditors. “SEE FAQS AND CIPC GUIDELINES” is inconsistent with the quality of product being produced in other CIP version 5 standards.
Yes
No
R3 VSL - Change: Severe VSL To: High VSL and Add: Severe VSL with 60 days violation. Rationale: align severity with risk.
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
Change: “18 months” To: “24 months”, including all other related wording Rationale: CIP Version 4 provides for 24 month implementation plan, yet CIP Version 5 is going to bring many more Responsible Entities into scope that have not formerly been acclimated to planning and accomplishing compliance with the NERC CIP Standards.
Individual
Bob Thomas
Illinois Municipal Electric Agency
Yes
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
Yes
Illinois Municipal Electric Agency (IMEA)appreciates the SDT's efforts to date. We emphasize that even though the comment (and balloting) period was longer than normal, it was stlll not enough time for small entities (in particular) to adequately review a proposed Reliability Standards development of this magnitude. IMEA's limited comments or lack of comments to questions in this comment form are due to this inadequate comment period. IMEA, therefore, would like to empahsize that it supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency; particularly those comments regarding the impact on small entities and the need for a fourth category of low impact without connectivity in order to accomplish a more realistic application of the CIP standards to small entities.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Recommend changing "upon" to by. Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
Yes
Yes
No
Recommend changing "upon" to by. Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.

Yes
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No comment.
Yes
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No comment.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
Yes
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments

submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
Individual
Rich Vine
California ISO
Yes
1. Introducing ideas such as 'attempt to disrupt' into a definition requires a widely accepted and understood metric to define an attempt to disrupt. Recommend plagiarizing from NIST/ISO-27001/2 definitions to avoid these problems. 2. “Suspicious event” seems open to different interpretations. 3. Electronic Security Perimeter being defined as a “collection of Electronic Access Points” is an odd definition; a perimeter is not a set of objects, it is a line or boundary. 4. “Interactive Remote Access” is defined, yet “interactive access” is not, it would be helpful to have a definition for “interactive access”.
No
• Although stated that you do not need to keep a list of Low Impact BES Cyber Assets, you would still need to do a comprehensive inventory, as some requirements still apply to those assets.
No
• Measure 2 should include "or delegate".
No
• Seems like if you incorrectly categorized or missed 5% or fewer of your assets, by default you are automatically put into the Severe VSL range as it most likely will have been more than 60 days since the BES Cyber System was identified or categorized. If it only covers major changes to facilities and elements and not cyber systems, it would not be a concern – but this would need to spelled out.
Yes

Yes
• Would like to see some assurance that the auditors would focus only on the standard requirements, and not auditing against what is submitted into evidence. I believe there is some fear in the industry that the higher standards some entities hold themselves to could be held against them during the audit. This would help get rid of maintaining 2 different policies – one for CIP, and one for the non-CIP assets.
Yes
• Re-word the sentence - as written it is unclear whether we need to approve the CIP Senior Manager, or ensure that the policies are approved by the CIP Senior Manager.
No
• It appears to preclude an awareness and training program that covers all aspects of CIP for individuals who have access to BES Cyber Systems. This would be a more comprehensive way of ensuring that individuals who may have a job scope change in the future are not missed by having to track them and make sure they take another subset of the training pertinent to the new job function. Training and awareness is one of the most violated standards, and I believe it is the overhead associated with slicing up the base by roles, job functions and partitioned training that is causing this.
Yes
Yes
• M6 acceptable evidence should be the same as M5.
No
• Seems like the R1 VRF should be low as this does not directly affect the BES reliability, and is more administrative.
Yes
No
1. R2 appears to preclude an awareness and training program that covers all aspects of CIP for individuals who have access to BES Cyber Systems. This would be a more comprehensive way of ensuring that individuals who may have a job scope change in the future are not missed by having to track them and make sure they take another subset of the training pertinent to the new job function. Training and awareness is one of the most violated standards, and I believe it is the overhead associated with slicing up the base by roles, job functions and partitioned training that is causing this.
No
R3 implies that the training programs would be documented at the individual level as opposed to the program level. This suggests that showing that an individual received training may not be considered equivalent to a “documented training program for each individual….”
No
R4 seems to require an entity to document the criteria for pass/fail. While some general criteria could be described, each situation is fact-specific and it’s important that an entity have the ability to make a determination based on the facts and their perception of risk.
No
Disagree with the proposed modifications due to: 1. R6 specifies that “Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. Recently updated CAN-0007 (revised Dec. 9th, 2011) provides a better specification on what constitutes electronic (or logical) and physical access which should be included in this requirement to avoid any misinterpretation of intended requirements. Additionally, it is implied that if during review, a clerical error is identified in which access was provisioned incorrectly, it would be a violation of this requirement. Explicitly calling this out, if intended, is required to reduce unintended inference. 2. R6, 6.1 requirements should read “Identified Authorizers shall authorize electronic access, except for CIP Exceptional Circumstances, to BES Cyber Systems or systems enabling access to BES Cyber Systems (if this is required)." Most organizations have defined

processes for who can authorize this type of access. Adding the “CIP Senior Manager or delegate” increases administrative overhead to sign and maintain delegation letters. Can these requirements be reworded so that CIP Senior manager does not have to be involved in authorizing –either directly or through delegates?
No
Disagree with the proposed modifications due to: 1. In R7, the last paragraph in “Rationale for R7” should directly reference in accordance with the “Guidelines and Technical Basis” provided for CIP 004-5. The information provided in the “Guidelines and Technical Basis” is what is needed to ensure compliance with the requirements, and it should be blatantly obvious to avoid confusion. 2. In R7, 7.1, the requirement should read “. . .to BES Cyber Systems at the time of resignation or termination with verification of access removal and system-generated listing of user accounts showing such persons no longer have access with a maximum of x time”. There needs to be a defined threshold for acceptable maximum timeframe to complete and provide evidence for (such as 1 day, based on the maximum time required for system-based updates). 3. R7, 7.2 again the “Guidelines and Technical Basis” provide critical information for complying with the requirement, and information should be incorporated into the requirement directly. Given that the majority of job transfers require the user to essentially perform the current and prior job functions for some time, a review of permissions should be conducted, however, if permissions are still required, further review should occur during the next quarterly review. 4. R7, 7.3, again the “Guidelines and Technical Basis” should be included to reference the similar requirement indicated for 7.1 to remove unescorted physical access and Interactive Remote Access, with 30 days to remove all other local access permissions. 5. The drafting team should make it clear for reassignments or transfers that continued access should be allowed for a previous role for a period of time determined by an entity to be "necessary" to complete turnover and previous duties.
No
How does one document a technical implementation purchased from a vendor? How does one measure if that document proves sufficiency in impmentation? Highly recommend plagiarizing from NIST / ISO-27001/2 for appropriate control statements.
No
Most modern attacks originate using 'non-interactive' channels 'interactively.' Highly recommend plagiarizing from NIST / ISO-27001/2 for appropriate control statements.
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with. Request Requirement 1.2 be updated to allow "escorted physical access." Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress". Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.3 be consistent (not add a Requirement) with Requirement 1.3, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary " to "Issue real time alerts (to individuals responsible for response) upon detection of a breach through an access point". Request similar changes to R1.5. For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, ".
No
Request clarification of 3.1 and 3.2on what the "Associated" under "Applicability" pertains to (i.e.: High, Medium, or Low BES Impact).

No
1. Need clarification on what disabling a physical port would entail. 2. A targeted audit of a static list in dynamic environment will almost always find a control failure.
Yes
No
3.4 Need clarification of the required/expected login and tracking process for a transient cyber asset.
No
• Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities. • Request clarification on 4.3, does the failure need to be detected within a calendar day? • Request the rationale of 4.5's "two weeks". Recommend one month as a compromise between the prior version's 90 days and the suggested two weeks.
Yes
Disagree with the proposed modifications due to: 1. In the “Guidelines and Technical Basis” section for R5, 5.3 should read “Where possible, any default accounts provided. . .”. This was simply missed. In 5.5, the sentence in the last paragraph on page 43 should read “Password complexity refers to . . . passwords to have the following types of characters:. . . “. If all four are required, as indicated by the “and” separating the four characteristics, then this sentence should be fixed to eliminate conflicting requirements. 2. For R5. 5.2, having a separate list or administrator, shared, default, and other generic accounts, signed by the CIP Senior Manager, creates more work. This requirement can be met during the quarterly access review of all BES Cyber System accounts reviewed by appropriate, designated Approvers. 3. Need clarification on 5.5.3 - not able to extract what is required under this standard.
Yes
Yes
Yes
Yes
• Applicability section in table seems to be mixed between All Responsible entities and High/Medium Impact BES Cyber Systems.
Yes
No
For 1.4, clarification is required. Is this a backup media verification process? If not what is the intent? Does this mean that for every backup (full/incremental) that a log is kept, and if so, for how long?
No
Request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current. What is the preferred sample size (all assets/system based) or a representative grouping (db/web/app)?
No
Does this mean a recovery test for each asset or a representative grouping of assets? Can I recover(drill or exercise) what is a full operational exercise in R2.1? Can I limit to an individual asset or sytem?
No
• Requirements – 1.1.6 – Clarify “security-patch” requirements. • Requirements – 1.2 - “Authorized” should be “Authorize”. • Requirements – 1.4.1 – Define “cyber security controls”. • Requirements - 1.5 – Some BES Cyber Systems may not have comparable test environments. Testing in non-CIP

production assets before implementing in CIP environment should be allowed.
Yes
2.1 – Measures – Clarify meaning of “records of investigation” (change record, incident record, e-mail).
No
Disagree with the proposed modifications due to: 1. R1 1.1 lacks specificity as to what is required. Verbiage should be clarified to express whether the sub requirement is requesting a documented process for identifying applicable BES Cyber System Information, or that there is an information classification process in place and being followed to label applicable BES Cyber System Information. 2. The evidence examples provided in 1.2 are nebulous, and in some cases difficult to provide (e.g “hardcopies of information stored in a locked file cabinet with keys provided to only authorized individuals”). It should be clearly stated, if required, that approvals must include attestation that user access to BES Cyber System Information was granted based on a “need to know” basis.
No
Disagree with the proposed modifications due to: 1. As currently stated, 2.1 speaks only to BES Cyber Asset media, however BES Cyber System Information may reside on devices that are not BES Cyber Asset media (such as in printer memory, email servers, etc.). Given that CIP-011-1 R1 assumptions directly references “Information handling procedures should detail access, sharing, copying, transmittal. . .”, clarification that specifies any system that contains BES Cyber System Information should have media cleared, purged or destroyed prior to reuse or disposal should be specified, if that is the intention of the requirement. 2. The Standard (applicability) is sufficient, but not wide spread enough as it should cover all computer processing and storage assets (Cyber Assets) within the BES. The data contained on servers in a well-constructed infrastructure is stored on secured disk arrays. Individual processing units or storage devices connecting to these resources or attain data through a secondary transfer can collect confidential data. If the asset falls outside the standard, the data contained on the device can move beyond the established security perimeter. Any asset that provides a data storage capability that is within the security perimeter or enters the security should fall within the standard. 3. Requirement R2 “Guidelines and Technical Basis” information requires clarification to state whether strong encryption used on media besides a SAN is considered acceptable. 4. The standard states “Media Reuse and Disposal” is a requirement, but does not provide guidance of what is required for reporting “Evidence”. This leaves the method of what information or actions required open for interpretation. Specific definitions and requirements would allow Vendors to the BES provide solutions to meet destruction requirements provided for reporting and improve internal processes to meet this standard.
Yes
Group
NRG Energy Inc.
Patricia Lynch
Yes
1) The control center definition is in conflict with the requirements in Medium Impact Rating of CIP-002 Attachment I as it does not fully address or delineate those generation facilities that control small remote units on a different footprint from the centralized control room. . These units collectively may be significantly under the 300 MW threshold as indicated in 2.13 and present no risk to the BES, yet can be defined as control centers at medium impact as they are physically located on a different footprint. 2) The definition of BES Reliability Operating Services does not address whether read-only operating data which is displayed for situational analysis and decision making through voice communication needs to be protected under the CIP standards (ex. PI, RIG displays, Historian)
Yes
1) Although the BES cyber systems have been explained in detail, the allocation of impact for various BES cyber systems is not written clearly that classification of these systems is based upon

categorization of devices based upon site characteristics per Attachment I. It is not clear if BES cyber systems at a facility can have numerous levels of impact. 2) For facilities that control blackstart resources, it is not clear in Attachment 1 if all BES cyber systems within the confines of the control room would be considered for inclusion in CIP security, and if so, if they are considered medium impact. 3) In Attachment I-2.1, there are two different resulting interpretations as to how the 1500 MW threshold is applied. One is that if BES cyber systems in a facility are tied together and control more than 1500 MWs collectively, they would be in scope. The other interpretation is that all BES cyber systems are in scope for a facility of multiple generators that collectively produces 1500 MWs, whether the BES Cyber systems are tied together or not. This ambiguity should be removed.3) Under Attachment I 2.6, Transmission facilities operating at 500 KV or higher are included. Would this address facilities that essentially are radial leads with no load flow through? 4) For generation facilities that require notification from the Planning Coordinator or Transmission Planner for inclusion under medium impact, this must be placed on a frequency for notification and provide ample time for remediation 5) Since the aspect of qualifying connectivity has been removed in this set of standards, is it assumed that all relevant requirements need to be included for the various impact levels regardless if the devices are isolated? This needs to be explicit.
Yes
No
This should be stated clearly that this initial and annual review applies to all BES Cyber assets impact levels, regardless if the entity has not identified High or Medium BES Cyber Assets or BES Cyber Systems.
Yes
Yes
Yes
Yes
No
This requirement should state that training on relevant policies associated with job function are required.
No
The authority for subsequent delegations may result in reduced oversight and control.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
In Table R6, the Senior manager or delegate may be too far removed from the actual access control

process to authorize individuals and provide access permissions.
No
In large organizations that cross many regions, revocation under R7.1 concurrent with termination may not be possible if there are numerous BES systems that require coordination of revocation at that time
Yes
No
R1.1 does not clearly explain that an electronic security perimeter or technical controls is required for all low impact BES Cyber systems
Yes
No
R1.3 requires use of two or more complementary physical access controls appears to be excessive whereas one robust physical control can avoid unauthorized access.
No
Under this requirement, there are less restrictions for visitors than required for employees.
Yes
Yes
Yes
No
1) Security patch management does not spell out the required level of patching requirements. Should third party application be included? And what about parsing programs or scripts written for data collection, DVD drives, etc. which do not impact the functionality of the BES system? Please delineate all levels of required patching. 2) Patching that cannot be supported by devices will still require TFEs at medium and high impact levels. 3) Assessments on Vulnerability notices may take more than 30 day period. 4) What is the CIP Exceptional Circumstance definition? It is not listed.
No
TFEs would still be required under the medium or high impact levels unless these systems are upgraded or replaced.
No
If an high or medium impact system is required to alert in real time for events that necessitate a real time event in R4.2, why is necessary to review a sampling every two weeks under R4.5?
No
1) Under R5.2, The senior manager or delegate may be too far removed from the actual access control process to authorize individuals and provide access permissions for various accounts. 2) CAN-0017 is in direct conflict with R5.5 which allows either technical or procedural controls for enforcement of password parameters. CAN-0017 forces TFEs unnecessarily.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
Authorization under R1.2 by the CIP Senior Manager or delegate to document changes to the BES system that deviate from the baseline configuration may be considerably out of scope for these individuals. This includes maintenance activities such as patching.
Yes
Yes
No
Labelling of all devices and associated information is excessive and at the level of nuclear grade security.
Yes
Yes
No
There is a direct conflict with Version 4 and version 5 of the standards concerning overlap of time for implementation, if version 4 is not immediately approved. Secondly, if this was to occur, there may be conflicting requirements-ie CIP-002 R2.13 does not exist in V4 for same level of impact and remediation
Group
Imperial Irrigation District (IID)
Jesus Sammy Alcaraz
No
No
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Depending on the criticality of the device in question the VRL & VSL should be classified. Not all assets are the same and the language does not provide any room for type of assets
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
No
Part 3.2; 3.3, 3.4, 3.5 Due to limited resource, IID would like to change the response with additional 60 calendar days to current propose.
No
IID suggested the VRFs and VSLs should be at lower risk or moderate risk.
Yes
Yes
Yes
Yes
Yes
Yes
No
IID'S position does not agree with the combining of these two vulnerability assessments. IID feels that they should be kept separate.
Yes
Yes
Yes
Yes
Yes
Group
Western Area Power Administration
Brandy A. Dunn
Yes
1) “Transient Cyber Assets” are defined as directly connected devices. However, external cyber assets used for transient remote access are not addressed and no security controls are required for such devices. Since CAN-0005 asks if system operator laptops are CCAs (or …”are system operator laptops parts of the BES system?”) and this CAN is still outstanding, we recommend revising this definition to address direct and remote transient devices in CIP version 5 so CAN-0005 will be retired. 2) Add clear definitions of “physical access revocation” and “cyber access revocation” so CAN-0007 – Revocation of Access may be retired.
Yes
a) General - Study based exceptions should be allowed. Given that a substation may fall into the

medium category under the bright line criteria, an entity should be able to show through study work that loss of the substation does not lead to voltage collapse or cascading outages, and thus exclude its inclusion in the medium category through studies. b) General - The method used to determine classification of facilities is too proscriptive. Use of Short Circuit MVA coupled with study work showing that loss of the bus(es) at a substation do not lead to cascading or voltage collapse should be sufficient to show that the facilities should be classified as low. c) General - CIP-002-4 changes the risk based assessments to a more proscriptive method. The industry does not have a good measure of what those changes will lead to, yet is expected to accept additional changes in this version 5. The industry should be allowed to gauge the changes from version 3 to version 4 and operate under the new version before being asked to vote on acceptance of version 5. d) General - The "Guidelines and Technical Basis" section of the standard is problematic. It basically states that any element or system of elements that has an adverse impact on BES services should be listed. This is an issue because elements incorporated into the BES will always have an impact, otherwise they would not exist. This section of the standard goes on to define conditions that will always skew the impact toward adverse, and the impact is not quantified, so the reader is left with the implication that any adverse impact requires listing of the asset. Perhaps this is the intent, and if so why have the pretense of the "bright line" criteria? Simply declare all BES transmission elements as Medium and be done with it. Otherwise, the level of impact needs to be defined such as "additional elements which, upon loss, will lead to voltage collapse or cascading outages" in addition to or instead of the specific "bright line" criteria defined in Attachment 1 of the standard. e) General - Attachment 1 is written in the context that Version 4 is in effect and the entity has already performed the "bright line criteria" assessment of its facilities and has a completed list of CAs and CCAs. But if Version 4 is skipped (as described in the Version 5 implementation plan) then the Attachment-1 assessment process will require revision. It is not logical to assess cyber asset and cyber system impact on ROS impact as the first step. This approach would require the assessment of every single asset at all facilities to determine high/medium/low rankings, versus assessing & ranking facilities first, then assessing devices only at the high and medium ranked facilities. As described in the Version 4 Attachment 1, facilities supporting ROSs should first be determined, and then the cyber assets supporting those facilities and services can be assessed. f) Attachment 1, 2.4 and 2.5: The fact that a facility is identified in the TO's restoration plan does not imply that the facility is crucial to the plan. Given that multiple Blackstart Resources are available, then using the logic applied in the Application Guidelines, all these resources should not be deemed critical, and in fact none should be for these criteria. g) Attachment 1, 2.7: The "weight value per line" used to determine total weighted aggregate value does not allow for variations in various owners' systems. Many owners have 230 kV lines that are not capable of carrying 700 MVA as detailed in the Application Guideline. Provisions should be made to exclude facilities that can be shown to not lead to cascading or voltage collapse upon their loss. h) Attachment 1, 2.8 and 2.9: The standard is placing a burden upon the TO for actions of others, that the TO has no control over, with no allowance for coordination or negotiations for potential changes in the determination of IROLs. Previously stated in this standard, the TO has 30 days to place the facility on the Critical list, yet nowhere in this standard is there a requirement for the outside entity to communicate its proposed inclusion of the impacted TO's facility as a potentially higher rated facility. This would be problematic for the TO because if a new IROL was unilaterally declared by the outside entity, the 30 day clock may start before the TO is aware of the issue, in which case the standard could be violated by the TO for actions outside the TO's control. i) Attachment 1, 2.11: Given that the SPS could have an impact on IROLs, this standard implies that all components of the SPS are designated as medium without regard to whether loss of those elements of the SPS system would lead to the referenced IROL violation. The SPS can be designed so that incorrect readings or misoperation of a given element of the system has either no impact or acts to run the SPS in the "safest" manner. If this is the case, the individual elements of the SPS should not require a medium designation, and should be allowed for in the standard. j) Attachment 1, 2.12: The standard and the Application Guidelines do not indicate whether the 300 MW limit is a system limit or an entity limit. Discussion in the application guidelines started to define the load shed discussion to a single location, but then fogged it up again when the discussion brought in the term "system", and thus spread out the load again. This area needs to be more clearly defined. This could be done by inserting "aggregate" if the net potential load shed is the trigger or "discrete" if only concerned about loads at specific sites over 300 MW. k) Attachment 1, 2.12: Given that a system results in load shedding over 300 MW, if the system is a set of relays set to work on observation of a system variable such as frequency or voltage, independent of the other elements of the load shedding system (ie relays at substations distributed across the TO's system, set

to trip for various under voltage or frequency levels, but not in communications with each other), it is not necessary to declare each of the relays and therefore each substation as medium assets. l) The discussion in the Application Guidelines under transmission part 2.7 (page 28): This section claims that the average MVA line loading used in a report used as a reference for quantifying risk is 700 MVA for 230 kV lines, and 1300 MVA for 345 kV lines. It is not clear where this averaging took place, but at least one TO is outside the norm, with emergency ratings of the highest rated line of each voltage class under 72% of those values, let alone the average line loading. This goes directly to the greatest weakness of this revision of CIP-002-5, and that is that the standard does not allow for systems that are different than the model system used to baseline the standard, nor does it allow study-based exceptions.
No
1) See above comments on Attachment-1 – if Version 4 is skipped, then CIP-002-5, R1 is out of context; it prescribes a required process backward to what would logically be done to determine BES-CAs and BES-CSs. 2) R1-1.1 requires the identification and categorization of changes from lower to higher within 30 days. Does requirement 1.1 refer to inclusion of the element or facility on the BES Cyber Assets and Cyber System list, or does this requirement include the entire scope of CIP-002 actions including the signature of the CIP senior officer?
Yes
No
Under the Table of Compliance Elements is included the phrase “Operations Planning” under the “time horizon” column. The industry cannot predict with certainty future upgrades and additions to the system, yet the standard appears to state that VSL apply to the planning time horizon under the “time horizon” column. It may be that the standard intends to apply to operations only, but this is not clear in the text since both “Operations” and “Planning” are capitalized. Please clarify.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
CAN-0048 is in development to clarify acceptable sources of ID verification. CIP-004-5 R4.1 requires identity verification but does not address what is acceptable. NIST Special Publication 800-63 has an acceptable description of Identity Proofing Requirements by Assurance Level, where assurance levels are Level 1 (low) through Level 4 (high). Please identify acceptable ID verification methods, for instance by identifying High Impact BES Cyber Systems as needing Level 4 Identity Proofing Requirements, and Medium Impact BES Cyber Systems as needing Level 3 Identity Proofing Requirements, as documented in NIST Special Publication 800-63.

Yes
No
Table R6, Part 6.3 includes the requirement that access to BES Cyber system Information be controlled to the degree that “Access permissions shall be the minimum necessary for performing assigned work functions.” This requirement will place undue, onerous, and unmanageable restrictions on drawings, diagrams, etc. This requirement could result in hundreds of information categories; feasibly one category for each employee. It is reasonable to protect this information from public release, but unreasonable to require that an entity classify information down to the “assigned work functions” level. We recommend removing the words “Access permissions shall be the minimum necessary for performing assigned work functions.” from CIP-004-5, Table R6, Part 6.3. Also please remove the words, “and the minimum necessary for performing assigned work functions” from CIP-004-5, Table R6, Part 6.6.
Yes
No
Too highly ranked VSL for information protection violations
Yes
No
Project 2009-26 is an interpretation asking whether indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access shall be considered supervision of electronic access. This has not been adequately addressed in CIP-005-5, or CIP-007-5. The drafting team should either require that entities have documented procedures for supervised electronic access or the drafting team should specifically state that no supervised electronic access is allowed.
No
CAN-0031 – Acceptable physical opening dimensions. The six-wall border is eliminated. Does that mean that opening dimensions are also immaterial? CAN-0031 is in response to a request to define the entry point metric definition of the access points on the perimeter. NERC also received a request for clarification for an acceptable entry point into a Physical Security Perimeter (PSP) as well as acceptable opening dimensions. Recommend including the wording from CAN-0031, “That any opening that does not have physical preventative measures in place is less than 96 square inches. That any opening greater than 96 square inches, with its shortest side greater than 6 inches in length, is protected against entry by the use of bars, wire mesh or other permanently installed barrier that leaves no opening greater than 6 inches on its shortest side.”
Yes
No
Testing of these systems every three years is sufficient. There will be too many systems to test on a two year schedule. Also – if monitoring of the access control systems is required and use of the system proves it is functioning, the two year cycle becomes highly redundant.
No
CAN-0019 is in development to answer the question, “What is the acceptable time to install a software patch before a TFE is required?” CIP-007-5 R2 states that a remediation plan must be developed within 30 days, but does not answer the question. Please identify an acceptable interval for completion of the remediation plan. Is one year too long? Can a remediation plan state that implementation will start after 6 years?
No
R3.5 requires the logging of “each transient cyber asset connection”. This is not only a large burden

for Maintenance staff performing daily operations, but difficult (or impossible) to audit accurately.
Yes
No
Project 2009-26 is an interpretation asking whether indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access shall be considered supervision of electronic access. This has not been adequately addressed in CIP-005, or CIP-007. The drafting team should either require that entities have documented procedures for supervised electronic access or the drafting team should specifically state that no supervised electronic access is allowed.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Version 4 must pass to get the 'bright-line criteria' in place first or Version 5 will be too large of a leap in the assessment process, cause confusion, and be very difficult to audit. Western recommends NOT skipping version 4.
Individual
Richard Salgo
NV Energy
Yes
BES Reliability Operating Services – Dynamic Response to BES Conditions: Please provide clarity as to the intent of the term "sensors" as used to describe SPS, UFLS, and UVLS. Does this refer to instrument transformers, and if so, isn't this overly expansive? Also the "breakers" included in these items are not cyber systems and should be deleted. BES Reliability Operating Services – Managing Constraints: The inclusion of ATC and unit re-dispatch/unit commitment appears to be outside the

realm of “real-time” (15 minute threshold). Rather, these considerations are most typically hour-ahead and day-ahead in nature. Suggest deletion of these two items or re-write to emphasize that the scope is limited to real-time functions in these areas. BES Reliability Operating Services – Situational Awareness: The inclusion of “Current Day and Next Day Planning” is outside the realm of the stated 15-minute threshold for real-time. This should be removed.
Yes
TO/TOP Control Centers in 1.3 are contingent on controlling one or more of the assets listed at the end of 1.3. This list includes 2.12, which is UVLS and UFLS. Suggest deletion of this item 2.12 from the list in 1.3, as Control Centers cannot and do not manipulate the operation of UVLS or UFLS. UVLS/UFLS are discrete relay systems typically located in distribution systems distributed throughout the BA or TOP area, and have no linkage to particular control centers. GOP Control Centers in 1.4 similarly are qualified by control of assets identified including 2.12 (UVLS/UFLS). Again, the inclusion of UVLS and UFLS for a control center, and more particularly, a GOP control center, is inappropriate. Transmission Facilities 500kV or higher, 2.6: This should be qualified as “networked” 500kV, so as to exclude radial 500kV facilities, which are performing a distribution function. Transmission Facilities 200-500kV, 2.7: This item should be changed to specifically exclude radial and local network (see Project 2010-17 BES Definition) facilities from consideration in the weighting calculation. UVLS/UFLS 2.12: As a matter of principle, UVLS and UFLS should not be included; this item should be deleted. UVLS and UFLS are deployed at the distribution level and are not controlled via any common control system. Inclusion of these sorts of distributed discrete relay elements is extremely expansive, and does not appear to offer any benefit to cyber security of the BES. Version 0-3 only included such schemes if they were under “common control” and shedding 300MW or greater. If deletion is not agreed to by the SDT, then it may be acceptable to add a qualifier of “under common control” to this item. Also, it is not clear whether the phrase “as required by its regional load shedding program” modifies both UVLS and UFLS or simply UFLS. Generator Control Centers, 2.13: It is unclear what is the definition of the generation control center as used in 2.13. If this item is retained, the SDT should clarify the definition of a generation control center and specify that the 300MW generation threshold is limited to BES generation only.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
From the structure of the table in R2, it appears that the Requirement calls for training on all ten aspects 2.1 through 2.10 for all individuals having access to medium or high impact BES cyber systems. This would not allow the appropriate degree of role-based training differentiation and will

therefore require unnecessary training for many individuals.
No
The statement of R3 indicates that the entity shall implement its documented training program for individuals needing access that includes each of the applicable items in Table R3, but Table R3 doesn't contain any "applicable items". Does this reference really belong to Table R2?
Yes
Yes
Yes
Please clarify in Part 6.5 whether the intent is that there be a review conducted on an individual by individual basis that their access is appropriate, or does this call for a review of the access rights for each type of "role"?
No
Concurrent revocation required in Part 7.1 will be virtually impossible to comply with. As with any task that requires human intervention and consideration, there will necessarily be a time lag between the action of termination and the steps that are taken to revoke certain elements of access.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Individual
John Martinsen
Public Utility District No. 1 of Snohomish County
Yes
Comments: Refer to additional comments submitted for Question 49. “Suspicious” is not an auditable term, and should be removed. What is an “attempt”? What attempts are serious enough to justify having to be reported? The definition should be made to read: BES Cyber Security Incident A malicious act that: • Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. Under “BES Reliability Operating Services”: • “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet • Recommend that “Change management” under “Situational Awareness” be clarified to changes in the BES instead of IT change management • Recommend clarification that “Facility” is the NERC Glossary term--in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication”: • Request clarification of the scope of this “Operational Directives”. Does it include a company’s messaging system? Two-way radios? What is the relationship with the new COM-002? • Request clarification that these Coordination and Communications are limited to Reliability, not Market Systems. • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret.
Yes
Comments: Recommend that 2.8, 2.9 and 2.11 start with “Applies to all Regions except…” For 2.8, 2.9 and 2.11 request that the SDT clarify whether the exception is all, or not WECC. In 2.12, “system” and “Facility” are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal?
No
Comments: For clarity, request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days when a change to BES Elements and Facilities is placed into operation”. For clarity and consistency with the previous change, request changing M1 from “as required in R1 and list of changes to the BES (” to “as required in R1 and list of changes to the BES Elements and Facilities)”. The word “intended” should not be used in the requirement because it is not auditable. Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards

Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium, and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced throughout the Standards.

No

Comments: Regarding CIP-003-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Comments: The last bullet for M4 on page 12 is inconsistent with R4 since M4 requires periodic training instead of R4’s making staff aware of cyber security policies. Request that M4 be updated to be consistent with R4.

Yes

No

Comments: The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.

No

Comments: Regarding CIP-004-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This

question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Comments: Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement. Recommend removal of R2.3 and R2.4 since they are redundant to R2.2, or explain the difference between R2.2 and R2.3, R2.4. Request removing “potential” from R2.7 since training should include how to determine whether a BES System Event occurred or not.
Yes
No
Comments: For all R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
Comments: For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”.
No
Comments: For R6.1 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.3 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber System Information. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.6 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I” in Information.
No
Comments: Request that the footnote for 7.1 be moved into the requirement. Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend removing the "following the resignation or termination" since it is redundant and inconsistent with the sibling Requirements. Recommend changing 7.4 from "For resignations or terminations," to "For terminations, resignations, reassignments, or transfers,".
No
Comments: Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point

or not? Request clarification on 1.5's "at each EAP". Is that inside or outside or both? Regarding CIP-005-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Comments: Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology. Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete.

No

Comments: Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress". Request Requirement 1.2 be updated to allow "escorted physical access." Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.4 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. " to "issue real time alerts for detection of breach through an access point". For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6. Regarding CIP-006-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Comments: Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, ".

No

Comments: Request clarification on what the "Associated" "Applicability" (High/Medium/Low BES Impact) for 3.1 and 3.2 Request capitalization of "locally mounted hardware or devices" in

Requirement 3.1 so that it refers back to the defined term "Locally Mounted Hardware or Devices" .
No
Comments: Request clarification on 1.1, is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on 1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Regarding CIP-007-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Comments: Request clarification of "remediation" in 2.2 since it reads that the patch must be applied, which does not allow to have an exception when applying the patch is the worst scenario such as creating a denial of service. For 2.2, suggest wording like "create a remediation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied". What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to the patch or the overall process?
No
Comments: Request allowances in 3.3 for signatures/pattern updates that cause trouble. Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media". The Measure for 3.4 does not match the Requirement.
No
Comments: Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities. Request clarification on 4.3, does the failure need to be detected within a calendar day? Request the rationale of 4.5's "two weeks". Recommend one month as a compromise between the prior version's 90 days and the suggested one week. In 4.5 clarification is needed for the associated protected cyber assets. Are these protected cyber assets associated with only high impact BES cyber systems, or could they be associated with medium impact BES cyber systems?
No
Comments: For 5.2, does the CIP Senior Manager or delegate approval policy or procedure for each authorization of access? In 5.2, should the Requirement be interpreted as "each use" as in "The CIP Senior Manager or delegate must authorize the use of each administrator, shared, default, or other generic account types." Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
No
No
Comments: Regarding CIP-008-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be

at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Comments: 2.1 is a new Requirement. Request the rationale for this new Requirement. Recommend changing from "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." to "When a BES Cyber Security Incident is classified or identified, the Responsible Entity must follow its incident response plan." Recommend removing “initially upon the effective date of the standard” from 2.2 of Table R2 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered.

No

Comments: Recommend removing “initially upon the effective date of the standard” from 3.1 of Table R3 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend that 3.2 wording be consistent with the 2.2 wording. For 3.3, recommend changing 1) "Update" to "Update as necessary" and 2) "the completion of the review of that plan" to "the completion of the review performed in 3.2" .

No

Comments: For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommend removing Requirement 1.5. Reliability's top priority is restoration of service. Forensics in a recovery mode may not support BES reliability and requiring such actions may negatively impact the BES Cyber System restoration process. Regarding CIP-009-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Comments: Recommend that 2.1 be implemented 180 days from the effective date of the Standard. For 2.1, request clarification, is “full operational exercise” the same as “functional exercise” as described in the rationale? For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new

requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the Standard.

No

Comments: For 3.1 recommend 1) removing “or when BES Cyber Systems are replaced” as it addressed in CIP-009 R3.4 and 2) removing “and document any identified deficiencies or lessons learned” as they are addressed in CIP-009 R3.2 and R3.3. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Recommend that 3.4 be referenced by CIP-009 R3.1. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.

No

Comments: Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." For 1.1, 1.2, 1.3 and 1.4, recommend changing the Requirements to be consistent with their Applicability --- from "For a change to the BES Cyber System" to "For a change to the BES Cyber System or Associated Systems or Associated Assets". Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold. Regarding CIP-010-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Comments: Recommend removing "where technically feasible" from 2.1 since the remaining words should not need an exception.

No

Comments: For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend changing 3.2 from "in a production environment" to "in a production environment, or a test environment" to allow Entities more flexibility in meeting this Requirement.

No

Comments: Request clarification on 1.1. Some interpret this Requirement as what is the Entity's process for identifying BES Cyber Systems Information. If correct, the Measure should be "show me the methodology (document)." Others interpret these Measures as labeling BES Cyber System Information. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Regarding CIP-011-1, the Applicability sections of CIP-

002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Comments: Request that footnote 2 in 2.1 be moved into that Requirement.

No

Comments: The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Otherwise, this Scenario table is confusing because it repeatedly uses 12 months while the earlier text uses 18 months. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Since Version 4 is not FERC approved, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. A summary of comments applicable to more than one standard: . • Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • Request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5. A fiftieth question should have been included in this comment form asking for general comments or concerns. A question asking general comments should be included as part of every comment form posted to the industry.

Group

NESCOR/NESCO

Annabelle Lee

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Definitions: Clarify definition of Electronic Access Point Electronic Security Perimeter – definition does not say clearly that this has to include ALL interfaces from outside the BES(s) being protected. Suggest change to: “The collection of all EAPs that permit communications to a BES system from a device not in that system.” Note that existing definition of EAP says “restricts” rather than "permits.” Unsure of the specific meaning of “restricts". As stated in the document, "...from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities." Redundancy is not an appropriate mitigation for all vulnerabilities, but it is a mitigation for some. NERC may want to consider revising the sentence and being more specific when redundancy is not appropriate. As stated in the Table of Compliance elements, "100 High and Medium Impact BES Cyber Assets." Why are only cyber assets listed and cyber systems excluded? As stated, "The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” The term element is not defined nor related to cyber assets/systems. NERC may want to consider adding a definition for element. NERC may want to consider adding iteration/feedback loops to the use case CIP process flow diagram. BES Cyber System mentions the phrase Maintenance Cyber Asset. This phrase has no

associated definition. There is no explicit reference to generator control rooms in the definition a Control Center. It should be made clear if a generator control room is included or not.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Attachment I, Medium Impact Rating (M): This is of particular concern given that there is a push from FERC and congress that more generation be inclusive in the application of cybersecurity controls. The wording of this measurement has had much debate over the last several months and there isconflicting understanding on what this actually entails. Based on the latest information, the SDT has stated that this would be 1500 MW attached to a single DCS (for example). As currently written, this means that a single facility with multiple generation units at 1499 MW or less that are attached to separate DCS' would not reach the category of medium. An aggregation of generation capacity per facility should be considered. Attachment 1: Text before 2.1, 2.2 does not read correctly in connection to those items. We are unsure how it should be corrected. Blackstart plans for resources used for load restoration purposes may be inadvertently included in the existing definition, specifically criteria 2.4. The Cranking Path diagram on Page 26 implies that Blackstart resources are only included where used to start a unit. The SDT may want to consider criteria 2.4 be modified to read “Each Blackstart Resource identified in its Transmission Operator’s restoration plan used to provide power for remote start of another generation unit(s)”. Attachment 1: Blackstart plans for resources used for load restoration purposes may be inadvertently included in the existing definition, specifically criteria 2.4. The Cranking Path diagram on Page 26 implies that Blackstart resources are only included where used to start a unit. The SDT may want to consider criteria 2.4 be modified to read “Each Blackstart Resource identified in its Transmission Operator’s restoration plan used to provide power for remote start of another generation unit(s)”. Attachment 1: Criteria 2.11 contains the words “…if destroyed, degraded, misused”. (Twice). This appears to be a carryover from version 4, but it now is redundant and perhaps conflicting with the “15 minutes” qualification as defined at the top of the Medium Impact Rating section. Attachment 1: Criteria 2.12 refers to a “system” – as in “Each system or Facility…” – that implies something of a cyber nature. The rest of the bright-line criteria refer to or describe hard assets, not cyber assets. This seems like an odd exception. The SDT may want to consider removing “Each system or”. Attachment 1: Page 30 of the draft standard contains an example methodology or process flow for categorizing BES Cyber Assets and BES Cyber Systems. This graphically illustrates the overall intent of the SDT for CIP-002-5. However, when you boil down all the security controls in CIP-003-5 through CIP-011-5, there really isn’t any appreciable difference between High and Medium requirements. The SDT may want to consider modifying items 1.1 through 2.13 on Attachment I to be “All these assets have a Critical Impact Rating”. Requirement 1 would therefore be “For all cyber assets including associated physical and electronic access control and/or monitoring systems and associated protected cyber assets, that support one or more BES reliability operating services at a Critical facility, apply the controls as specified in CIP-003 through CIP-011”. If there are cases (like CIP-010-5-R3.2) where specific “High Impact” systems are intended, then the SDT could consider stating so in the requirement; “For Control Centers, perform an active vulnerability assessment every 39 months…”. Although the addition of "within 15 minutes" does lend itself to a "bright-line" criteria, it may be arbitrary in the event that a BES Cyber Asset or BES Cyber System is unavailable, degraded or misused and one or more BES Reliability Operating Service becomes "adversely impacted" at the 16 minute mark or longer. Why is an adverse impact happening within 15 minutes any less important to the BES than one happening in 20 minutes? Attachment 1: The term "adversely impact" is not clearly defined. Attachment 1: A concern with the 15-minute time limit is that it is really related to the ability to make generation with the contingency reserve available within 10 minutes of a disturbance and then allow the Transmission Operator/Balancing Authority to restore firm load within 15 minutes of a disturbance. The methodolgy does not equate on the security side. The security side is that you are attempting to reduce the risk that you have to recover within 15 minutes. A possible approach is to prescribe protective measures by facility type, system type, and device type. Attachment 1 is a good start, but it could be rewritten to be specifically based on preventing the need to restore. Attachment 1: Suggest changing wording “would, within 15 minutes, adversely impact” to “could adversely impact.” There is a significant difference between would and could. A more specific definition of “adversely impact” would be useful, but it is unclear whether this is practical given the number of BES reliability operating services and the utility circumstances. Multifunctional devices as high impact assets: Attachment 1: Handling of multifunctional devices identified as high impact assets, for example, protection relays may be addressed through sets of restrictive non-functional requirements. Besides of its protection function, digital protective relays typically provide monitoring

and reporting functions. CIP may be too restrictive or lacking guidance on how to approach accessing the protective devices and other multifunctional devices to allow for data and report retrieval. This is considered a significant problem by power utilities and currently they are restricted on how to retrieve and use recorded data and reports remotely.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Clarify – is each cyber asset categorized EITHER alone OR as part of a BES system? Since the BES system concept is a major change for v5, a bit more explanation would be useful. What constitutes a “change to BES Elements…” per part 1.1? The SDT may want to consider modifying this language to simply state that new or retired assets be added or removed from the list within 30 days of commission or decommission. For M1, we believe the intention is that entities are not specifically required to list their Low Impact systems. Therefore, the SDT may want to consider modifying the last sentence to “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems is not required, but instead may be demonstrated by the application of the required controls”. (New words are “is not required, but”)
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. For all places where a requirement states "at least once every calendar year thereafter, not to exceed 15 months…”, this means that if the activity is performed every 15 months, then it would have only been performed 4 times in 5 calendar years. This contradicts the "at least once every calendar year..." Similarly for “every 39 months…”. To ensure that aircraft receive annual inspections once a year, Federal Aviation Regulation (FAR) 91.409(a) requires that" no person may operate an aircraft unless, within the preceding 12 calendar months, it has had (1) an annual inspection in accordance with part 43" etc. This wording precludes attempts to extendthe word "annual" to mean longer than one year, and we suggest that similar wording could be used in the CIPs. For example, "an entity is out of compliance with requirement Rxxx unless, within the preceding 12 calendar months, it has performed X Y Z". The SDT may want to consider that this requirement and all others that use the words “…initially upon the effective date of the standard…” have this phrase stricken. The implementation plan that accompanies the final approved draft should include the requirements for first time iteration of periodic activities. It’s not reasonable to assume that every entity is capable of executing all procedures “upon the effective date”. Minor point, but this is the first time “CIP Senior Manager” is used in the standards. Perhaps add a cross-reference to the appropriate requirement in CIP-003-5. In section “B. Compliance”, under sub-section “1.2 Evidence Retention”, there is a typo in the second to last line. Please change “complaint” to “compliant”.
Yes
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. The need for cyber security policies that address the BES Cyber Systems is prudent; however, it appears that the required topics to be addressed may not be holistic and/or fully appreciated without more description. For example, does Personnel Security include Training and Awareness policies? Would an entity know to include policies addressing Monitoring & Logging in the topic System Security? There does not appear to be specific policy requirements to address Application Security, provisioning, forensics or cryptography. The list of topics does not include such items as: access control, training and awareness, audit and accountability, I&A, planning, risk management, information system and information integrity, continuity of operations, information system development and maintenance. Please consider looking at the full list of families included in NISTIR 7628 and consider augmenting the topics list. As stated, "BES Cyber Systems." This does not include BES cyber assets or facilities. Please clarify. Application Guidelines for R2: There are a number of technical issues raised here that, in some cases, can be technically enforced, and not just required by policy. Consider moving and/or adding these to other CIPs where they are more appropriate. Also many of these issues go beyond the scope of the standards and are not required for compliance. This may cause confusion as to what is required for compliance. Organization stance on use of wireless networks (this would be optimally addressed in CIP005) Monitoring and logging of ingress and egress

at Electronic Access Points (this is in CIP007 R4.1.1) Maintaining up-to-date anti-malware software before initiating interactive remote access (is in CIP007 R3.4) Maintaining up-to-date patch levels for operating system and applications used to initiate the interactive remote access before initiating interactive remote access (this would be optimally addressed in CIP007 R2.x) Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating interactive remote access (this would be optimally addressed in CIP005) For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s interactive remote access controls (this would be optimally addressed in CIP011 R1.x) Monitoring and logging of physical ingress and egress (this would be optimally addressed in CIP006 R1.x, noting that egress logging / monitoring in not in the current CIP standards) Availability of spare components (this was in CIP v1-v4, but doesn’t appear to be in CIP v5) Break- fix processes (this would be optimally addressed in CIP010 R1.x)
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. This rule states "...individuals who have access to BES Cyber Systems..." This could be emphasized to state that the "access to BES Cyber Systems" means logical and/or physical access. Even techs without cyber access to equipment in substations, for instance, should nevertheless be aware of the cyber security policies governing that equipment, such as, for example, no use of thumb drives.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Are the measures listed under M5 meant to be prescriptive? These are very specific and imply requirements. Throughout the standards, measurements are now tightly tied to requirements and are much more prominent. However, examples should be stated as examples, so that “measures” do not become “requirements” . The SDT may want to consider stating (somewhere) the compliance applicability of Measures. In the second bullet under M5, CIP-002-5 R3 is mentioned. There is no R3 in CIP-002-5. In the last sentence in the last bullet under M5, the bullet is one huge run-on sentence, confusing, and should be redrafted for clarity.
Yes
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. R1.1: If awareness is provided only to personnel with authorized electronic access and/or authorized unescorted physical access, it could still be possible for personnel without appropriate awareness doing unrelated work on systems in other networks such as the enterprise network to infect systems in those networks. This malware might then be used to stage attacks against electronic security perimeters protecting BES cyber systems. The Rationale for R1 indicates that personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems are to maintain awareness of best security practices. Neither the R1 requirement language nor the R1.1 table requirement make mention of best security practices rather the requirement states security concepts. Also, It would seem that if the expectation is for those personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems are to be the recipients of such awareness then the requirement should be explicit in that regard. It was noted that the Change Rationale for R1.1 states "Changed to remove the need to ensure everyone with authorized access receives this awareness" which appears to be counter to the Rationale of R1. Responsible Entities does not appear to include operators, specifically, those who operate the BES cyber system and/or BEST cyber assets. Operators should also receive training.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Parts 2.2 and 2.4 seem somewhat redundant. If there was a specific distinction intended by the SDT, please consider rewriting to make this clearer. For example, 2.2 could be reworded to add the clause “including electronic access controls” OR 2.4 could be reworded to say “The training

required under 2.2 shall include training on electronic access controls."
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Users of low impact BES cyber systems/assets also need basic cyber security training. Consider revising the training requirement to include basic cyber security training for all individuals. One potential oversight in all versions of the CIP-004 standard is guidance on the training requirements for "transient" workers. By transient, we mean persons whose access is either temporary, or perhaps is granted and revoked on a periodic basis due to project work. The SDT may want to consider adding some words to R3 (or Part 3.2) to make clear the requirements for this category of worker.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. R4.1: Without requiring verification of credentials, e.g., government issued photo ID, how is the utility able to trust an employee's identity? R4.2: The requirement only states criminal record checks and not other checks, such as random drug and alcohol testing. When people are drugged and/or intoxicated with alcohol, they may do things unknowingly, such as disclosing confidential information, losing confidential documentation and critical systems, and/or making improper judgments when running BES systems. Furthermore, drug and alcohol testing is reasonably commonplace in other industries and reasonable for both cyber security and safety. There should be consideration in this requirement to include drug and alcohol testing within the constraints of state laws and collective bargaining agreements. R4.2: The criminal check record is private confidential information and, therefore, needs to be stored securely. R4.4: It may be difficult to find contractors or vendors who have performed all the criteria listed in R4 (Personnel Risk Assessment Program). In many cases, these contractors and/or vendors, have been working for utilities for many years without any background or criminal check. What if the utility cannot get all that information? What if a utility finds something from the criminal record of a contractor who has been with them for several years? In these cases, what should the utility do? R4.4: Additionally, must vendors be authorized to provide criminal background check information to the utility for their employees, which would require permission from the employee? Or can the vendor assert to the utility that it has obtained and verified this information in accordance with the CIPs? R4.4: Current practice is to have the vendor and/or contractor attest to the fact that background checks (in accordance to the requirement) have been completed. Leveraging the TWIC program or creating a similiar program specific to the electric sector would lead to a consistent approach to 3rd party background screening and potentially reduce industry work effort on this activity.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. One potential oversight in all versions of the CIP-004 standard is guidance on the PRA requirements for "transient" workers. By transient, we mean persons whose access is either temporary, or perhaps is granted and revoked on a periodic basis due to project work. The SDT may want to consider adding some words to R4 to make clear the requirements for this category of worker. The Applicability sections of R4 and R5 are different and it doesn't make sense to design a PRA process for one set of assets, but implement it for a different set.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Parts 6.1, 6.2, and 6.3 state that "access permissions shall be the minimum necessary…" This appears to be a goal and the SDT may want to consider moving this sentence to the Rationale or Guidelines section. Part 6.3 should include a cross-reference to CIP-011-1-R1.2, as in "…as documented in the entities information protection access control procedures in CIP-011-1-R1.2." Parts 6.1, 6.2, and 6.3 include the qualifier "…except for CIP Exceptional Circumstances". For consistency, this language could either be stricken, or amended to include a reference back to the entities CIP Exceptional Circumstances policy per CIP-003-5-R2. Please clarify whether Part 6.5 applies to cyber access or physical access, or both. The notion of "groups" can theoretically apply to physical access to control systems as well as cyber access. Part 6.6 appears to be redundant to the annual information protection review performed per CIP-011-1-R1.3. Per an earlier comment, the "minimum necessary" language throughout R6 may be difficult for entities to prove and the SDT should consider moving it to the Rationale or Guidelines section.

No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Extended leave situations - such as a sabbatical, employee behavior/performance suspensions or maternal/paternal leave - are not identified as a reason for revoking or suspending access. Given the criticality of the environment being protected, reducing the privileges to only those who have a need for access as a part of current job duties should be maintained. These specific role changes perhaps could follow the requirements for transferred or reassigned personnel; however, it should be made clear in the requirement or Guidelines and Technical Basis section how to manage these common personnel situations. In the Guidelines and Technical Basis, there is a table that identifies that no action is required for death. The SDT may want to reconsider this requirement. Revocation of access privileges for the deceased is an important action. Dormant accounts with privileges could be misused. By removing such privileges, the entity is reducing their overall attack surface as well.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. In the Guidelines section of CIP-004-5, the last sentence under Requirement R3 (and again under R4) states "…by the single senior management official identified in Requirement R1". This should be re-written to say "…by the CIP Senior Manager or delegate identified in CIP-003-5-R1". In the Requirement R4 section of the Guidelines, the reference to CIP-011 is a typo and should state CIP-004. In the Requirement R6 section of the Guidelines, the last sentence of the first paragraph could be modified to state "Best practice recommends that access authorization and provisioning should not be performed by the same individual". Some entities are too small for strict separation of duties to be feasible.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. There is no clear requirement that non-routable communications between two ESPs, such as between a substation and control center, be encrypted or have the integrity assured. Technical solutions exist to secure serial SCADA communications, both in the form of proprietary vendor products, as well as standards such as IEEE 1711 (developed from AGA12) and Secure DNP3. We suggest that all non-routable persistent communications links between ESPs be protected with strong encryption and integrity. Furthermore, the endpoint devices providing the encryption and authentication should be considered part of the ESPs and subject to all other CIP requirements for cyber assets belonging to an ESP. Cyber assets associated with data networks and data communications links between discrete ESPs, rather than being exempt from CIP requirements, could be specifically included, and exempt only when all communications between those ESPs are encrypted and have their integrity assured. IPSec VPNs have been a mature technology for many years, as are SSL VPNs. Given that these technologies are widely used in other industries, and that devices implementing them are available in industrial- and substation-grade form factors, we recommend that all routable communications, not just remote access connections, be protected with strong encryption and integrity (message authentication), using encryption technologies such as site-to-site secure VPNs. Secure VPNs should not be confused with technologies such as MPLS and GRE that can segregate traffic, but do not encrypt, and are therefore only secure if every intermediate device in the traffic path is secure. Furthermore, the endpoint devices providing the encryption and authentication should be considered part of the ESPs and subject to all other CIP requirements for cyber assets belonging to an ESP. If communications assets are exempt from the CIPs as the draft currently states and communications are not encrypted and integrity verified, then every radio, modem, hub, communications device, wire, and fiber can provide an attacker with access to and the ability to falsify critical control system communications. This particularly applies to most private WANs leased from communications service providers: if communications over private WANs are not encrypted, then compromise of the service provider via mis-configuration, vulnerabilities in equipment, or insider collusion by employees of the service provider, could lead to compromise of multiple utility communications networks. This particularly applies to communications across the public Internet. Fully addressing security of communications links may require more than just removal of the A 4.2.4.2 exception. This topic seems sufficiently important to merit its own CIP section covering appropriate requirements for end-to-end protection of communications (encryption, integrity verification, key management, etc.). A comment in the summary of changes for R1 states that "the non-routable protocol exclusion no longer exists". However, R1.1, R1.2, R1.3, and R1.5 all provide

exclusions for non-routable protocols. Of these, R1.5 is the only requirement for which there might be limited choices of technical solutions currently available on the market. There are also exclusions in CIP 007 R1 and R4. We recommend removing all non-routable protocol exclusions, as the summary of changes claims. R1.5: This requirements states that the entity needs to establish a documented method for detecting malicious communications at each EAP. There is no additional comments in the Guidelines and Technical Basis section to clarify this requirement; however, the responsible entity could infer expectations from the measures column. Perhaps a better phrasing would be: "At each EAP, the entity shall document and implement methods for detecting and addressing communications that have the characteristics of malicious or unexpected activity." How does an entity demonstrate compliance to Part 1.1 if CIP-002-5 does not require that entities document their Low Impact cyber assets? Please consider revising the Measures section to provide clear guidance on recommended artifacts for compliance that do not pre-suppose lists of Low Impact cyber assets. Please provide a technical basis for the requirement that outbound access permissions are necessary per Part 1.3. If no technical basis can be defined that can be uniformly applicable to all BES entities, then please consider qualifying “outbound” to be “…inbound and, where implemented by the entity, outbound access permissions”. In Part 1.5, the term “malicious communications” is too vague. The SDT could consider changing 1.5 to say “A documented method for malicious traffic inspection at each EAP”. The third paragraph states “This requirement applies only to communications for which ‘deny by default’ type requirements can by universally applied…”. This sort of language, while useful, should more properly be included in the requirements. The SDT could consider making clear the intent of the Guidelines and Technical Basis section of the standards, and the expectations of the entity - and of the compliance enforcement authority – on how this information should be used. As stated, "A documented method for detecting malicious communications at each EAP." Does this include both inbound and outbound communications? Malicious communications can also be sent from the BES through the EAP. R1 Guidelines: Regarding dialup connections to a specific BES Cyber Asset, the guidelines state "... examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use". Dial-back modems are easily defeated as revealed by a simple google search. Caller-id spoofing services make reliance on caller-id tags questionable. Remote enable or powerup leaves a window of vulnerability unless combined with other defenses, such as modem BES cyber asset passwords. Policy requiring disabling after use is error prone. R1 Guidelines: Problems with dialup modems and methods of securing them are discussed in some detail in"Securing Control Systems Modems" from Idaho National Lab: www.inl.gov/technicalpublications/Documents/3874574.pdf Products and technical solutions to secure dialup connections exist at reasonable cost, and NERC could consider requiring stronger measures to protect dialup connections. R1 Guidelines: Products and technical solutions to secure dialup connections exist at reasonable cost, and NERC could consider requiring stronger measures to protect dialup connections. R1 Guidelines: This sentence is unclear: "Since low impact BES Cyber Systems can impact BES Reliability Operating Services in real time, they should not be located directly on public networks or other networks of lesser trust." Does that mean networks of lesser trust to public networks and, if so, what are those networks? Or is this saying that one should not place low impact BES Cyber Systems on public networks or networks of lesser trust to a corporate network or a network behind an EAP? It is not clear that Security Event Monitoring as called out in CIP 007 is required of all EAPs. NERC could consider security event monitoring be required of all EAPs, regardless of impact level. This requirement could also apply to Associated Electronic Access Control Systems and perhaps also Associated Protected Cyber Assets, since where authentication servers are used separately from the EAP devices, they need to be at least as strongly secured as the EAP devices themselves.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. R2.2: As stated, “Requires encryption for all interactive Remote Access sessions to protect the confidentiality and integrity of each interactive Remote Access session.” However, this statement does not address end-to-end encryption. Sometimes vendors access SCADA systems remotely via a third party remote access service, such as "logmein". Such sites may establish a secure tunnel between the vendor and the remote access service, and then another secure tunnel between the utility and the remote access service. In such a case, the remote access service has access to all the remote access traffic; that is, the encryption between the utility and the vendor is not end-to-end. R2.2: Connections between initiating Cyber Asset and Intermediate Device can be encrypted most

times using 3rd party applications, however the connections between the Intermediate Device and Remote gateway or end device (IED) is often not technically feasible. R2.2: It does not state anything about "Authenticating based on certificates". R2.2: There have been a significant number of CAs compromised recently, and recent versions of Firefox trust approximately 50 CAs located at organizations all over the world. Secure authentication is necessary to ensure that encryption is useful. Relying on CAs outside of the US to authenticate remote access to critical national infrastructure may need to further assessment. As stated, "Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session." Please consider replacing "encryption" with cryptographic techniques. Cryptographic techniques includes encryption, integrity, and non-repudiation. As stated, "Require multi-factor authentication for all Interactive Remote Access sessions." Why would multi-factor authentication be required for device to device remote access? As technology evolves, there could be more interactive device to device remote access sessions. R2.3: There is a discrepancy on the usage of multi-factor authentication. In this rule, it states that for High and Medium Impact BES Cyber Systems, as well as the Associated Protected Cyber Assets "REQUIRES" multi-factor authentication. However, in CIP-007 R5.1, it states to "validate credentials before granting electronic access to each BES Cyber System" which does not state the need for multi-factor authentication. A reference for the definition for strong (two-factor) authentication in the RSA information security glossary at http://www.rsa.com/glossary/default.asp?id=1080 R2.3: Multi-factor authentication needs to be carefully defined. US banks have been required to use two-factor authentication since 2006, but while the meaning of the term is clear to security professionals, it has been interpreted in some cases by the banking industry to mean "mother's maiden name plus last 4 of social security number", which is far weaker than the generally acknowledged concept. Without clearly defining what is intended by multi-factor authentication, significantly weaker interpretations may be chosen. NERC could consider that the different factors involved in a multi-factor authentication be drawn from at least two different classes of authenticator, the classes being something you know (e.g., password, userid), something you have (e.g., badge, smartphone, token, physical key), or something about you (e.g., fingerprint, retina scan, voice print). Also some requirement for liveness should be included to prevent, for example, a physical key (as in a metal thing with notches) acting as one factor being left permanently installed/attached to a reader.

Yes

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. This CIP standard no longer has a statement related to "All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter." The language could guide physical security measures through a description of acceptable construction materials, construction practices, and based on facility type. Specification on vegetation management, lighting requirements, stand off distances, periodic patrol, etc., should be included. The key point is that we are drafting physical security standards for the electric industry. It is important to write down a "standard" that people know how to follow for the sake of consistency and achieving the goal of protecting the BES Cyber Assets and BES Cyber Systems. For example, tell them they need an 8ft tall mesh fence with shakers and motion detection if that is needed to establish physical security perimeter. This is also necessary to help in making this requirement auditable. Without more description and additional security control specific the plans generated by the responsible entities may only identify the minimum stated requirement which can leave gapping holes. ASIS physical security standards could be considered as one source of generally accepted good practices that could be leveraged to help make CIP-006-5 a more robust and adequate security standard. As stated, "Define operational or procedural controls to restrict physical access." How is this consistent with the little or no security requirements for low impact systems? Also, as stated, low impact systems do not have to be uniquely identified. As stated, "Utilize two or more different and complementary physical access controls to..." Examples are provided – but they are not mandatory. What if the associated protected cyber asset is a laptop? Requirement 1.6 references only systems. Early CIPs also reference assets and facilities. How does an entity demonstrate compliance to Part 1.1 if CIP-002-5 does not require that entities document their Low Impact cyber assets? The SDT may want to consider revising the Measures section to provide clear guidance on recommended artifacts for compliance that do not pre-suppose lists of Low Impact cyber assets. R1.2/R1.3: The requirement statements in R1.2 and R1.3

address ingress controls; however, the associated measures state egress and ingress. If egress controls are an expectation then the requirement should make it clear as to what the responsible entity is required to do. R1.5: The control as documented is to issue alerts for un-authorized physical access, however there is no control to document results of followup. We propose that events (from alerts) and findings are documented, or even that a summary of findings per period (daily / weekly, etc) are documented. For consideration: “Issue real-time / immediate alerts in response to unauthorized physical access attempts, and investigate and respond to alerts before the end of the next calendar day, and document outcome.”
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Continuous monitoring should be defined with a maximum time frame of escort, communication mechanisms, minimum communications capability during escort, required periodic communications, maximum distance between escort and visitor, visitor identification mechanisms, escort qualifications.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Testing could be at least daily operational checks by security staff using the equipment. This can be simple camera pans, alarm testing, etc. Physical maintenance could be performed based on the environment, e.g., Gen plants are dirty so the condition may warrant a high frequency of checks due to carbon and dust build up, control centers are typically well enclosed, so lower frequencies are needed. NERC could consider adding a requirement to retest if the system fails.
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Table R1 is referred to as Ports & Services, but the controls are all about Ports, and there are no controls about services. NERC could consider either removing the reference to services or introduce a control to require an analysis of which services are running, and to disable or remove any services that are not necessary. For Part 1.1, SDT could consider acknowledging the use of dynamic ports/ranges used by a wide variety of cyber systems. The documentation requirement seems a bit redundant to the configuration management documentation requirements of CIP-010-1-R1.1. Under the Guidelines and Technical Basis for Requirement R1, 1.1 the draft states “. . . therefore it is the intent that the control be on the device itself; blocking ports at the perimeter does not satisfy this requirement”. This seems to exclude the use of an intermediate device immediately preceding/inline with the device, thereby removing a valid security defense mechanism. Inline security mechanisms where no path around them exists enable security functionality to be placed in a manner to ensure they are engaged and also allow multiple solutions to be used where existing systems lack protection. An example would be a dedicated firewall and IPS system placed directly between a critical system and all connections, ensuring they are in the path of all traffic and allowing specialized security functions not available on some systems. A rewording of the quote above would add the option of providing non-bypassable security controls. “. . . therefore it is the intent that the control be on the device itself, or positioned inline in a non-bypassable manner; blocking ports at the perimeter does not satisfy this requirement”.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. The SDT may want to consider revising Part 2.2 to say “Identify applicable security-related patches or security-related updates…” As written, a person could interpret “updates” to mean security-related or not. The words “…that addresses the vulnerabilities within a defined timeframe” could be separated from the end of the sentence and rewritten as its own sentence for clarity. Part 2.3 is not clear on what is actually required. The requirement talks about a process, yet the Measures suggest evidence that the remediation took place. Should Part 2.3 say “Execute the remediation plan documented in Part 2.2”? Patch management could also be considered for low impact systems. If the same operating system or application is used on low and medium/high impact BES systems, the patch should be applied to all the systems to mitigate the vulnerability. As stated, "A process for remediation, including any exceptions for CIP Exceptional Circumstances." This is vague – and could be more specific. Also, this should be linked to configuration management requirements and incident

response requirements, as applicable. R2.1: This requirement states the need to identify the source or sources to be monitored for security patches, updates, etc. However, there is no mention of how frequent the responsible entity should be conducting this activity. It can be inferred from R2.2 that this activity must be conducted, at a minimum, every 29 days or less; however, as written, compliance is limited to identifying a source or sources and does not account for how often monitoring is to be conducted. If the intent is to have the responsible entity frequently monitor the identified sources so security patches, updates, etc. are discovered within 30 days of their release then the requirement should be more clear as to the monitoring expectations.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. As stated, "Deploy method(s) to deter, detect, or prevent malicious code." This does not address remediation if the malicious code impacts a BES system. How does this requirement specifically relate to separate boundary protections? This requirement appears to be mandatory for every system, rather than to different systems at the boundary. As such, the requirement drives a specific architecture. At what level of the system is this required? Does this include the boot code/kernel, the OS, the applications, etc.? How does this apply to embedded systems? As stated, "Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns)." This requirement is specific to profiles. There are other techniques that address anomaly-based behavior analysis and heuristics based analysis/detection. NERC could consider revising the requirement to address other types of malicious code detection. R3.3: 30 days is a lifetime when considering updating signatures/pattern files to malicious-code protection tools. Consider shortening this to a lesser period of time that is commensurate to the risk. R3.4: There does not appear to be any consideration for the possibility of the introduction of malicious code through a cyber asset or network-media device connected to the same network (within an ESP or behind the same EAP) as a BES Cyber Asset or BES Cyber System. The definition of a Transient Cyber Asset states that it is a: "A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset, 2) used for data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System." Consider changing the definition of a Transient Cyber Asset to include assets connecting to the same network where a BES Cyber Asset or BES Cyber System is connected.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. A comment in the summary of changes for CIP 005 R1 states that "the non-routable protocol exclusion no longer exists". However, R4.2 and 4.3 provide exclusions for non-routable protocols. We recommend removing these exclusions, as the summary of changes claims. There is a requirement to log events (4.1), a requirement to generate alerts for certain important events (4.2), and a requirement to detect and activate a response to event logging failures within one day (4.3). There is no requirement to activate a response to events important enough to raise an alert within any time period. Dealing with the actual alerts is at least as important as dealing with logging failure. As stated, "4.1.4. Any detected potential malicious activity." How will "a potential malicious activity" be determined? This can be wide open to interpretation as what is “potentially malicious.” Why log every successful logon? NERC could consider logging all events related to privileged accounts. As stated, "Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert." This is not specific to cyber security. Is that the intent? As stated, "(i) dated event logging failures and screen-shots showing how real-time alerts were configured." Configured real-time alerts are not directly related to event logging failures. These are different events. NERC could consider clarifying the requirement or developing two requirements. As stated, "potential event logging failures." Logging failures are typically due to a full log or other basic problem. How is a bi-weekly review going to address this problem? A summarization may miss certain events. As stated, "Activate a response to rectify any deficiency identified from the review before the end of the next calendar day." It is not always possible to rectify a deficiency within a short period of time. This requirement may need to be split into two requirements – one addressing logging failures and a second addressing security incidents. R4.2: The Measures and Change Description/Justification indicated that analysis is expected; however the requirement states that necessary alerts need to be established. Consider rewording the requirement to make analysis of the alert a clear objective. There is no requirement within the set of CIP standards 002-5 through 011-5 that make it clear that trained, knowledgeable

and aware people are essential to making a security logging system fully functional. CIP-004-5 training requirements mention role-based training but without specific descriptions a responsible entity could have the alert analysis (and the R4.5 summary review) accomplished by an administrator who has no training or skills to perform such activity. Effective security log management requires aware and skilled personnel watching the log systems and output. If an entity does not have expertise to understand what alerts are possible, and what the alerts may indicate, then the alert generation exercise called out in the Measures is not effective. Furthermore, a utility might simply decide that no alerts need a real-time alert. We recommend that unauthorized access attempts, at a minimum, be considered to require real-time alerts. R4.5: As written, R4.5 requires log review exactly every two weeks. Since the intent of this rule is to require a review at least every two weeks, we recommend adopting wording for this requirement that is similar to what was recommended earlier to fix the definition of the term "annual". Specifically, we recommend something like " an entity is out of compliance with R4.5 unless, within the preceding 14 calendar days, it has reviewed a summarization or sampling of logged events".
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. As stated, "The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types." How do you implement least privilege and other security controls if they are not defined in policy? This does not restrict the use of administrator, shared, etc. account types. These should be limited based on least privilege and need to know. As stated, "Identify individuals who have authorized access to shared accounts." Why only shared accounts? Consider identifying individuals with privileges – particularly those with access to administrator accounts. As stated, "Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required." Consider changing default passwords on devices. Because a default password is unique to a device does not imply that it is secure. As stated, "A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts." Consider adding an exception for emergency situations. Also, this is a potential method for launching a denial of service attack. The decision to limit the number of unsuccessful authentication attempts should be based on the potential risk. Consider adding more details in the requirement related to the potential risk. Part 5.2 implies, but does not state, that a signed and approved list of delegates is required. Please clarify. Also, this requirement talks about the “use of” shared accounts. This could be interpreted as either the initial creation of, or day to day use of, those ID’s. We believe the SDT meant the former, but we request that you please clarify. Parts 5.2 and 5.3 imply, but do not explicitly state, that there must be a procedure to authorize individuals having access to shared/administrative accounts. Please clarify. For Part 5.4, please simplify by stating “Procedural controls for initially changing default passwords, where technically feasible”. All the rest may be stricken, and the asset types moved to the Applicability column. R5.5: Long passwords are primarily required to defend against offline password attacks. Increasing the minimum password length from 6 to 8 characters is not adequate to address offline password cracking attacks, in the face of modern GPUs offering significant hardware parallelism and available on cloud computing services such as Amazon's EC2. All possible 6-character passwords can be tested on a supercomputer such as the Tianhe-1A in approximately 1 second, or on a distributed EC2 cluster in approximately 15 seconds at a cost of 50 cents. Raising the minimum length from 6 to 8 characters only requires an attacker to spend 96*96 times longer to try all passwords, which is still less than a day using cloud-based distributed computing. Furthermore, on Windows systems that store LM hashes, any password of any length is easily cracked in minutes on a conventional CPU. This applies to all Window systems prior to Windows Server 2008 and Windows 7. We recommend that NERC consider increasing the minimum password length to no fewer than 12 characters on Windows systems and no fewer than 10 characters on Unix-based systems that use SHA-512, salt, and key stretching. We recommend that NERC consider disabling LM hashes on all Windows servers, clients, and domain controllers. Third, we recommend that NERC consider guidance accompanying the CIPs that point out that using long passwords, even those that satisfy the complexity metrics of 5.5.2, does not automatically result in strong passwords. For a real-world example, The Tech Herald reports that of the 860,160 Stratfor passwords leaked late 2011, they were able to crack roughly 10% of them in a little over 4 hours using a CPU-based (ie. no GPU acceleration) cracking tool. Many of these were longer than 8

characters. There is supporting document "NESCO Common TFE Analysis: CIP-007 R5.3 Password Complexity".

Yes

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com/. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library R1.2: Even though the R1 rationale states that reportable incidents would follow the EOP 4 actions and timelines, the requirement language cow;d be more specific regarding that expectation. R1.3.1: What happens if there is a third-party IT company that handles the utility's cyber security incidents? Who should be doing what and who has the ultimate responsibility? For example, should the IT company handle everything from the beginning to the notification of the incident?

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com/. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library Part 2.1 the words "…when incidents occur" is redundant. The requirement is a bit contradictory in that the incident response plans MUST be used, yet deviations are allowed. Recommend rewording this requirement to say "When a suspected BES Cyber Security Incident occurs, the incident response plans shall be executed. Should deviations from the plan be necessary, those shall be documented for later review". As stated, "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." Consider making testing cyber security incident plans a separate requirement. Part 2.2 does not address new vulnerabilities or threats. Consider adding a requirement that the plan be revised based on new threats/vulnerabilities. As stated, "Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years." Is this sufficient for law enforcement, state, and federal requirements? Also, if the documentation is in electronic form, consider storing it in encrypted form and signed to ensure confidentiality, non-repudiation, and integrity.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com/. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library The Change Description field mentions "DHS Controls". What are these? Also, due to the complexity of the testing and review of the BES Cyber Security incident response plans, consider including a timeline/graphic in the Guidelines section to visually demonstrate the lifecycle of the plan. As stated, "Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary." Consider revising the plan if there are incidents, new vulnerabilities, new threats, and modified security configurations. As stated, "Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan." Consider modifying other relevant documentation, e.g., configuration management plan, access control policies, audit policies, etc. As stated, "Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan." Consider updating the plan based on new threats and vulnerabilities.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com/. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position

of DOE. For Part 1.4, what does “verified initially” mean? Each time the backup runs, or the first time after the asset was commissioned? (Could be years ago). If the latter, evidence retention might be an issue for long-life assets. As stated, "Conditions for activation of the recovery plan(s)." The terms “response plans” and “recovery plans” are not adequately defined. It is not clear what the differences are between the two types of plans. As stated, "Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts." The definition of roles and responsibilities and the names of specific individuals assuming those roles are two different areas. Roles and responsibilities may not change significantly over time, unless there is a new vulnerability or threat. The identity of individuals may change – based on people moving, terminating, etc. Consider having the list of specific individuals in a separate document. R1.3: Protection of backup media and backed up information is only lightly mentioned in this rule. Consider adding greater emphasis on the protection of backups, such as off-site storage and other physical protection, so that sensitive information in backup files (network configurations, device configurations, passwords, etc.) is protected. Is the intent of the standard the recovery of the function of an asset or system, or the recovery of the actual asset itself? This would be a good opportunity to clarify.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Consider revising part 2.1 to read “Test the Recovery Plans at least once every calendar year”, and include the three bullets. It also needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. For Part 2.2, the same question on scope applies. The language needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. Need to also allow for the fact that not all cyber assets can be “backed up” in a traditional IT sense. As stated, "...initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment." The other components are tested every 15 months – why is this 39 months? This assumes that a utility has a complete representative environment. This may not be realistic for all the BES associated systems. If there is a significant cyber security incident, the plan could be tested once the system is made operational. This will ensure the revised plan is accurate.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. As stated, "or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned." Consider revising the plan after a significant cyber security incident to ensure that it is accurate. As stated, "Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned." and "Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2." These plans may require changes to other applicable plans, procedures, and documentation, e.g., configuration management documentation, security configurations, access control policies and procedures. As stated, "Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change." As discussed earlier, the basic recovery plan should not be linked to specific individuals in an organization. The list of POCs should be kept separate from the plan and updated regularly – based on personnel changes. “Technology changes” is a vague term and could refer to software, hardware, firmware and may or may not be security relevant. Consider clarifying the definition to focus on security relevant changes. Due to the complexity of the testing and review of the BES Cyber Security incident response plans, NERC could consider including a timeline/graphic in the Guidelines section to visually demonstrate the lifecycle of the plan. For Part 2.2, the same question on scope applies. The language needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. Also, not all cyber assets can be “backed up” in a traditional IT sense. R3.2: For an actual incident recovery, consider requiring that the data produced in R1.5 be assessed in reviewing the recovery process. This might be included in the requirement, in the measures, or both. R3.3: Consider updating the Measures in Part 3.3 of CIP-009-5 Table R3 to include identification and documentation of the date of any event or lesson learned that results in an update to the recovery plan. R3.4: Table CIP-009-5 R3 parts 3.4 and 3.5 need the sub-headers titled Part Part Part

Part updated to Part Applicability Requirements Measures. R3.5: NERC could consider updating the Measures in Part 3.5 of CIP-009-5 Table R3 to ensure communication of update activities be conducted in a manner that requires an irrefutable acknowledgment on the part of the receiver of the communication.
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library For Part 1.1.4, the word “scripts” is generic and thereby difficult to address. Scripts that are used for key functionality of the system would make sense to include in the baseline, but scripts for administration, backups, maintenance or troubleshooting, for instance, may be too dynamic by nature to be included in the baseline. Please either clarify or revise the words “and scripts”. As stated, "Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels." This is not a comprehensive list of what could be included for each cyber asset. It is not clear how this list applies if the device is hardware only. Also consider adding communication protocols. R1.1: The baseline configuration requirements is missing "Network Topology" – "Network Topology" is suggested in NIST SP800-53 CM-2 "Configuration Management" ---> "Baseline Configuration". R1.1: NERC could consider adding a requirement to include in the baseline any non-standard configurations of the BIOS, operating system, services, etc. For example, BIOS version, BIOS boot disk order, BIOS password, changes to Windows registry entries, changes to service/task scheduling priorities, addition of periodic processes via modifications of tools like crontab, etc. R1.1: NERC could consider adding a requirement to explicitly include in the baseline any remote access services, eg. RDP, VNC, PCanywhere, etc. R1.1: NERC could consider adding firmware and programmable device load versioning to the list of items in the configuration baseline. This could include any executable or loadable image that can be modified without requiring physical access to BES Cyber System component internals.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. NERC could consider adding protections to the process for modifying cyber assets, in addition to monitoring for unexpected changes. Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Vulnerability analysis looks for any weaknesses - it is more than an audit of implementation against design. There are no requirements that an entity identify or document third party connections to BES Cyber Assets. Such connections are common and a high source of potential risk. NERC could consider developing requirements to identify and document third party connections, and authenticate and control access, both ephemeral (remote access) and persistent, from such connections. Furthermore, any and all requirements specified by the CIPs for the BES Cyber Assets accessed, including technical controls, policies, background checks, information handling, etc., should also apply to the third party systems. Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library. There are no requirements that an entity identify or document third party connections to BES Cyber Assets. Such connections are common and a high source of potential risk. NERC could consider developing requirements to identify and document third party connections, and authenticate and control access, both ephemeral (remote access) and persistent, from such connections. Furthermore, any and all

requirements specified by the CIPs for the BES Cyber Assets accessed, including technical controls, policies, background checks, information handling, etc., should also apply to the third party systems. R3.1: This requirement does not compel an entity to take any action based on the results of the assessment to correct vulnerabilities, and is weaker than the language in R8.4 of CIP-007-3 currently in force. R3.2 calls for vulnerability assessments every three years. CIP 007-3 R8 requires vulnerability assessments annually. No rationale is given for weakening this requirement. As of January 2 2012, the National Vulnerability Database contains 49053 CVE vulnerabilities, with 11 being added per day. Even without likely acceleration of this growth rate, this implies 4000 new vulnerabilities will be discovered each year. Even if only a small percentage of these apply to BES cyber assets, this could mean a significant number of KNOWN vulnerabilities in BES cyber assets by the time a vulnerability assessment comes due. Because of the constant change and introduction of new vulnerabilities, revising the time frame to three years seems inconsistent with this constantly changing vulnerability environment. Consider modifying the time frame to annually, or less. R3.2: For Part 3.2, please clarify whether all cyber assets need to be included in the assessment, or a subset, or representative sampling, or entity defined. There are certain cyber asset categories where “test” systems just aren’t economically feasible. What is the acceptable deviation between test and production? R3.3: For Part 3.3, please clarify whether “new Cyber Asset” means literally that or, more reasonably, could mean “new Cyber Asset category” or a new make/model, or a new function. It would be reasonable to test something that brings net-new functionality to a BES Cyber System, but if when replacing an end-of-life or failed component, it may not make sense. R3.2:
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. This CIP does not address how third parties (consultants, contractors, vendors, etc.) should handle BES Cyber System information. Where 3rd parties have persistent or ephemeral remote access to Cyber Assets, they have implicit access to BES Cyber Asset information. NERC could consider applying all information requirements of CIP 011 to any 3rd parties with such access. The measures column in R1.1 talks about "training materials that ... to recognize BES Cyber Security Information." but does not contain information about having training materials for handling BES Cyber System information. Table CIP-011-1 R1 parts 1.2 and 1.3 need the sub-headers titled Part Part Part Part updated to Part Applicability Requirements Measures.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. The statement, "...the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media." does not clearly address secure sanitization of media. It is recommended that NIST SP800-88 is followed by the utilities to safely sanitize the information in the media. Some examples of safe sanitization methods according to NIST SP800-88 are: Clearing information in a media using an overwriting software or hardware, Purging using degaussing tool for magnetic media, Destroying by shredding, Disintegration, Incineration, Pulverization, and Melting. Also, another reference for clearing and sanitization is: http://www.oregon.gov/DAS/OP/docs/policy/state/107-009-005_Exhibit_B.pdf?ga=t For Part 2.1, please consider adding language that allows for re-use or redeployment within a similar BES Cyber System.
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. The implementation plan calls for CIPv5 to come into effect January 1, 2015. Given that this draft has already been in the works for nearly two years, it is not clear why the effective date is three years in the future.
Individual
Bo Jones

Westar Energy
Yes
Westar Energy supports EEI comments as submitted.
Yes
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No

Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
The current practice is to restrict access to only those ports and services needed with a business justification for each.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
Yes
Information pertaining to Associated Protected Cyber Assets could potentially contain protected information. Associated Protected Cyber Assets likely reside on a protected network therefore the information should be protected similar to High Impact BES Cyber Systems, Medium, Impact BES Cyber Systems, Associated Physical Access Control Systems, and Associated Electronic Access Control

or Monitoring Systems.
Yes
Information pertaining to Associated Protected Cyber Assets could potentially contain protected information. Associated Protected Cyber Assets likely reside on a protected network therefore the information should be protected similar to High Impact BES Cyber Systems, Medium, Impact BES Cyber Systems, Associated Physical Access Control Systems, and Associated Electronic Access Control or Monitoring Systems.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Individual
Bruce Metruck
New York Power Authority
Yes
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: A definition for a 'Control Center' would be helpful. i.e. Change 'two or more locations' to 'two or more separate locations', not including the facility where the BES Cyber Systems are located. In certain situations the control of an adjacent BES facility may be provided at a generating plant – which should not classify that plant control room to be classified as a Control Center.
Yes
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: It would help if section 1.4 clearly defined what level of control of generation would require classification as a 'High' impact. In some case a control center may have limited 'base point' setting capability for assets under section 2.1.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: The word 'owns' is used in two places – this should be changed to operates or utilize – ownership may not be the determining factor based on outstanding operating agreements over time – also a single asset may be used by more than one entity.
No
NYPA concurs with the response provided by NPCC for this question.
Yes
NYPA does NOT concur with NPCC in leaving this question unanswered.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Last bullet of M4 should not be there – covered in CIP-004 (possible double jeopardy). Wording should be focused on 'Available' rather than 'Aware'. In general, we believe that all measures should be what the auditors will accept, or they should be removed (for all standards).
Yes
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: The footnote should be embedded in the actual requirement wording, re-word or move into a guidance.
No
NYPA concurs with the response provided by NPCC for this question.

No
NYPA concurs with the response provided by NPCC for this question.
Yes
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: In 1.1 “Applicability” add the ‘Medium Impact Cyber Assets with no external connectivity’ (see below for rationale)
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: In 1.2 “Applicability” replace the “Medium impact BES Cyber Systems’ to ‘Medium Impact Cyber Assets with external connectivity’. The rationale for this change is that stand alone devices such as protective relays cannot be controlled via defined electronic access points as defined in Part 1,2 without increasing their vulnerability by connecting them to such points.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Recommend changing the language in Section R2 Part 2.1, as set forth in the table, from “Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets” to “Identify any available, active source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.” Many older cyber assets may exist that may not have active vendor support or the vendor may have gone out of business. The requirement should provide for such situations. Recommend changing the language in Section R2 Part 2.2, as set forth in the table, from “Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe” to “Identify, document and initiate review procedures for patches, updates and vendor security notices within 30 days of release from the identified source. Procedures shall review for applicability to the entities BES Cyber Systems and Assets, identify a level of security/operational risk and provide a plan with defined responsibilities to address any identified vulnerabilities.” The majority of patches and updates provided by vendors are not necessarily security related but may include bug fixes, enhancements and upgrades. In many cases, patches are issued against an Operating System that may not be applicable to a system that has been hardened. In addition,

utilities may be dependent on third parties (e.g. system integration vendors) to review and test the impact of patches on operating software. The time frame for planning the implementation of the patches, or any alternate mitigating measures is highly variable.
Yes
NYPA does not agree with the NPCC response for this question, the original wording is sufficient.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Recommend changing the language in Section R4 Part 4.1, as set forth in the table, from “Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: …” to “Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, where available, each of the following types of events: …”. The intent is to provide leeway for additional log information. It should be noted that many “Medium Impact Cyber Assets” such as protective relays, metering, etc., may have minimal event log capability. Here the standard will require that whatever is available should be preserved. Recommend clarification of the terms “alert” and “real-time alert” in Section R4 Part 4.2, as set forth in the table.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Recommend changing the language in Section R5 Part 5.1, as set forth in the table, from “Validate credentials before granting electronic access to each BES Cyber System” to “Validate credentials before granting functional electronic access to each BES Cyber System.” Functional access is defined as capability to affect the operation of the BES System/Asset or of any of the BES Reliability Functions of the System. Many cyber devices, such as protective relays, meters or IED display terminals have some level of “Read Only” capability. It is not practical to provide individual log in capability to perform functions such as viewing equipment status while walking by or reading relay targets. Similarly some HMI systems are provided with auto-boot to non-privileged accounts from which users may only start up a BES Reliability Application that provides for or requires authentication. Note also that some level of control is provided for these non-privileged accounts in that they will need to be listed in Section 5.2.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Deletion of the second sentence in the NPCC comment - 'Is this integrity, availability or other information protection such as access controls, encryption?' - , the original wording is sufficient. In addition, this wording should clearly focus on ‘Loss Prevention’ or ‘availability’ rather than ‘protection of information’, and 1.4, should be verified ‘upon’ the actual backup to ensure backup success.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: It is unclear where the line occurs between the ‘Implementation’ covered by 2.1 and the ‘Testing’ covered by 2.3 – please clarify.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Should use wording ‘When technology changes’, and should refer to only ‘Applicable’ organizational change, and Technology Changes should be only BES Systems.

No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Change sub-requirement 1.1.4 from 'any custom software or script …' to 'any compiled software or script that affects system startup, external communication or application program operation'. Some scripts such as macros for a spreadsheet or an application script do not merit full change control.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Requirement 2.1 should be replaced – i.e. 'Implement technical or procedural controls to detect unauthorized changes to the baseline configuration'. The existing wording appears to require additional technical controls beyond those stipulated in CIP-007 R3.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question, including the additional general comments that NPCC added to the comment since there was no other place to indicate such.
Individual
Edward Bedder
Orange and Rockland Utilities Inc.
No
Comments: Minor correction should be made to list of topics under R2. They are listed as 1.1, 1.2, 1.3 etc. They should either be labeled as 1 through 10, or 2.1, 2.2 through 2.10.
No
Comments: 4.1 and 4.2 do not clearly indicated whether an entity current PRA policy covers full identify verification and documentation of any PRA that could not go back a full 7 years. It should be made clear whether either of these requirements is retroactive or whether any PRA prior to the effective date of the standard are grandfathered. It is recommended that the committee not require previously completed PRA to be updated.

No
1. R7.1 is unclear even with the footnote description of what the desired time frame is for “at the time” of resignation or termination. The phrase “at the time” needs to be defined as simply same day, before COB or end of day. The requirement also appears to apply to any reason for departure from the company. An individual leaving for retirement or termination due to unethical behavior would be treated the same. We feel there needs to be a differentiation between an individual being “fired” and an individual leaving for other reasons. It is recommended that same day revocation be required to termination for cause, and a two day revocation for any other departure. 2. The revocation periods for R 7.2 and 7.3 should be subsequently changed to match the recommended two day revocation mentioned above. 3. For environments that do not have external connections and maintain physical security access, such as individual non networked microprocessor relays, the risk to system reliability associated with frequently accessing the relay for purposes of changing the password outweighs the benefit achieved through this password change. It is recommended to alter this requirement to allow periodic (twice per year) password changes on these types of devices. (R7.5).
No
Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to alerts in 15 minutes. There is a disconnect between the requirement and the VSL table.
No
Comments: Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to alerts in 15 minutes. There is a disconnect between the requirement and the VSL table. Also reference to part 1.6 appears to be incorrect, should be 1.4.
No
The change to R2.2 goes beyond the stated rationale of requiring the current assessment to include the identification of what/who the source of the patch is so the time of availably can be determined. The new requirement now also requires a plan vs. assessment and requires including in the plan a defined timeframe; each of which is beyond the rationale. It is recommended that the word “plan” be replaced by “assessment” as is the current requirement, and that the additional requirement to include in the plan a defined time period be removed as it is in the current requirement. If a time frame is desired, we recommend that the timeframe be a planned timeframe and not a fixed timeframe. It is also recommend that a “plan” not be required as it implies a more extensive documentation of the patch reviews which will require additional paperwork that will not add value to the patch process.
No
R4.5 requires a manual review of a sampling of logged events every two weeks. The frequency is excessive, requiring 2-3 days per review, and will provide minimal value. We recommend once per month (R4.5). R4.3 – The requirement as written can be interpreted very broadly. It is not clear whether the intent is to detect a device has stopped sending log or the logs have stopped being accumulated by the receiving end (Syslog for example) is vague. If it requires detecting something is not sending logging within 24 hours this can be an issue, as some devices do not send logs every day. Some UPS devices , KVMs, and network switches only send a log if something occurs. There may several days without use and therefore no logs. Also, every time someone shuts down a workstation logs will not be sent. If action needs to be taken each of these times that would require documenting on a daily basis numerous events. This requirement should only address that action if the log repository has stopped recording incoming logs.

No
R5.4 is not clear as to whether unique default passwords applies to application level passwords only or includes default vendor user passwords also. The language needs to be clarified.
No
R3.2 requires active scanning in an environment that models baseline configuration. This may be impractical to replicate, the replication will need to be maintained and the some systems may have issues with active scans. Recommendation: A complete active scan should not be required (R3.2).
No
CIP-011-1 Requirement 1.1: The Measures associated with R1.1 indicate that evidence may include indications on information (e.g., labels) that identify it as BES Cyber System Information. It is suggested that the SDT expand on what types of repository would require labeling. For example, it may not be reasonable to label micrographic media, but rather label the cabinets or a room where the media is stored. Recommendation: We recommend allowing the entity appropriate discretion when applying labeling. CIP-011-1 Requirement 1.2: Measures associated with R1.2 indicate that evidence could be provided that shows user access is implemented on a “need to know basis”. The Measure should state that “need to know” personnel are determined by the registered entity. Similarly there is a suggested Measure that hardcopies of information be stored in a locked file cabinet with keys provided to only “authorized individuals”. Recommendation: The Measure should include language indicating that the registered entity identifies the “authorized individuals”.
CIP-011-1 Requirement 2.1: “Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was cleared prior to its reuse.” Recommendation: SDT should define what “cleared” means. The language in footnote #2 should be included in the wording of R2.1, to ensure it becomes part of the Requirement.
No
General Comments: 1. Applicability sections of CIP-002-5 through CIP-011-5: the Applicability sections should be consistent. Note that in CIP-005-5 and CIP-006-5 the Applicability sections 4.2.2 are different from the other CIP standards. We recommend that the drafting team adopt consistent Applicability language across all Version 5 CIPs. Alternatively, the drafting team should explain any Applicability variances between the various Version 5 CIPs. 2. CIP-006-5 Requirement 1, Guidance section on pp. 22 and 23 (Guidelines and Technical Basis): “While the focus is shifted from the definition and management of a completely enclosed “six-wall” boundary, it is expected in many instances this will remain a primary control for controlling, alerting and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems. … Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.” Comment: In reviewing CIP-006 – 5 we have seen that the “enclosed 6 wall” wording is removed, but it appears as though six walls are still required. The guidance section mentions that the Defined Physical Boundaries are allowed to have openings less than 96 square inches but does not exclude the need for 6 walls, only

that they are not required to be completely enclosed (excerpt above). Is this correct? Would a window be considered an “opening,” to be protected by a barrier as noted in the guidance? The CIP wording could be read as requiring a ‘ceiling’ over open air substations in order to preclude exceeding the 96 sq. in. and 6-inch limits. We do not believe that this was the drafting team’s intent. What was the drafting team’s intent? Recommendations: We suggest that this matter be clarified by the addition of wording specifically allowing an exception from this requirement for open air substations, such as, “This requirement does not apply to open air substations” or “This wording is not intended to require placement of a roof over open air substations.” Alternatively, if it was the drafting teams’ intend to apply this requirement to open air substations, then would surrounding all BES Cyber Systems in six-walled enclosures within an open air substations meet the objective of this requirement? Clearly, a roof should not be required for and physically cannot be installed over all open air substations. 3. The use of the “Measures” column for each requirement is beneficial as are the guidelines of each CIP standard. Providing these as part of the standards can imply that they are part of the requirements. By this one could see that by meeting the measures for each requirement that will be in compliance. Also the guidelines provide much more information than the requirements. The requirements tell you to perform an assessment without specifics while the guidelines provide specifics. Are the guidelines to be read as requirements? For example, A Defined Physical Boundary is required, but it is not until the user reads the guidelines is there mention to it needing to be enclosed completely with limitations on the openings. The requirements call for a active vulnerability assessment and it is not until the guidelines that what should be in an assessment is provided.

Individual

Thad Ness

American Electric Power

Yes

The definitions are inconsistent on the use of singular versus plural. For example, “Cyber Assets” versus “BES Cyber Asset” and “Protected Cyber Asset.” AEP recommends the use of singular. In “BES Cyber Asset” the second sentence appears to be somewhat at odds with the first and third sentences and does not add any further clarity. AEP recommends considering deletion of the second sentence. In “BES Cyber Asset” should “cyber security event or incident” actually be “BES Cyber Security Incident”? AEP recommends using the defined term “BES Cyber Security Incident” if possible. In “BES Cyber Asset” it says “Redundancy shall not be considered when determining availability.” Does that redundancy refer to BES redundancy, or Cyber Asset redundancy? Is BES redundancy sufficient to eliminate a Cyber Asset from consideration as a BES Cyber Asset? For example, if multiple path options exist from a generating facility, do all path options have to be considered? AEP recommends changing the definition to read “Cyber Asset redundancy shall not be considered when determining availability” if that was the drafting team’s intention. Are all BES Cyber Assets part of BES Cyber Systems? Can BES Cyber Assets reside “outside” of a BES Cyber System? Or do all BES Cyber Assets necessarily have an associated BES Cyber System? If a BES Cyber System is required for all BES Cyber Assets, AEP recommends clarifying that in the definition. “BES Cyber System” definition includes “typically” – which is not well defined. AEP suggests removing the term “typically.” “BES Cyber System” definition still includes “Maintenance Cyber Asset” which is not a defined term. Does “Transient Cyber Asset” replace “Maintenance Cyber Asset”? “BES Cyber System Information” definition is not crisp. AEP recommends the definition should use the following construct to identify BES Cyber System Information. The information must explicitly indicate *something* about 1) the BES Cyber Assets themselves (such as information to uniquely identify a BES Cyber Asset), and 2) their impact on the BES (information to indicate the significance of its role in the BES). If both tests aren’t met, it isn’t “BES Cyber System Information” itself. “BES Cyber System Information” contains a lot of detailed information. Why include specific requirements for types of information in the definition? Can’t the requirements be included in a “Requirements” section? These are not examples – these are requirements. AEP recommends they be moved to the requirements. “BES Cyber System Information” should say “recovery plans” not “disaster recovery plans.” “BES Cyber System Information” says “BES Cyber System incident” but “incident” should be capitalized. “BES Cyber System Information” says “network topology” – which is not a defined term. It doesn’t appear that “network topology” refers to anything to do with the electrical system network (but it could be confused that way). AEP recommends this be changed to “communications network topology.” “BES Cyber System Information” says “Electronic Access Control System” but should say “Electronic Access Control or Monitoring Systems" to be consistent with the rest of the standards. “BES Cyber System

Information" uses the term "BES Cyber System Impact" which is not defined. AEP recommends defining the term or removing it from the definition. "BES Reliability Operating Services" uses lots of abbreviations and colloquial, casual language: "x-former" "&" "etc" "auto" "Know generation status & capability & restrictions". AEP recommends using very formal language for this important definition. In "BES Reliability Operating Services" "Monitoring & Control" should "BES Elements" be a NERC-defined term? "BES Cyber System" combined with "Situational Awareness" from BES Reliability Operating Service is unbounded – it could include a wide variety of internal and external inputs that arrive via Cyber Asset (Internet access, CNN, AM radio, etc.). It would be difficult to demonstrate that a system does NOT impact situational awareness. In this instance, AEP recommends removing the "but are not limited to" phrase. In "BES Reliability Operating Services" "Inter-Entity Real-Time Coordination and Communication" appears unbounded. How do you limit the systems which are subject to this criterion? Could this include public telephone systems, public communications networks, satellite telephone systems, or even amateur radios? In this instance, AEP recommends removing the "but are not limited to" phrase. In "CIP Exceptional Circumstances" "Cyber Security Incident" should be changed to "BES Cyber Security Incident." "CIP Exceptional Circumstances" – could a reliability crisis be considered a CIP Exceptional Circumstances? AEP recommends that be added. In the definition of "Control Center" the bullet "Coordination of BES restoration activities" could be problematic. Could temporary facilities be considered a Control Center? Or would the absence of BES Cyber Assets prevent that? Or would phones, radios, laptops, etc. that might be considered BES Cyber Assets pull those Control Centers in to scope? AEP recommends dropping "Coordination of BES restoration activities" from this definition – the other functions should be adequate. Can the drafting team provide a definition of "Control Room" in addition to "Control Center"? AEP recommends the drafting team leverage the definitions posited in the Critical Asset identification guideline. The definition of "Cyber Assets" includes the term "programmable" – which is not well defined. Is a device with DIP switches considered programmable? Is a device that is loaded with a non-modifiable, non-configurable firmware (such as a USB drive) considered programmable? Is a differential pressure transmitter programmable if it can be "programmed" via a HART protocol handheld? AEP recommends the term "programmable" be defined, or an alternative term ("configurable"?) be chosen. "Defined Physical Boundary" seems to be a low-value name change. Awareness and training materials will have to be updated, documentation will have to be changed, programmed systems will have to be re-written, etc. Why not continue to use the term "PSP"? Or at least leave both defined? At a minimum, AEP recommends the SDT should keep the term PSP (6-wall perimeter?) defined, so that legacy documentation is still "correct." "Dee-Pee-Bee" seems to be an awkward combination of letters. It's difficult to distinguish the letters when said quickly. Is there another word or phrase to describe a physical limit that is not a complete, six-wall enclosure? AEP recommends the drafting team consider alternative terms with different abbreviations. In "Electronic Security Perimeter" is "protect" subject to the qualifiers ("routable or dial-up data communications") in the definition of "Electronic Access Point"? That is, do non-routable or non-dial-up connections need to pass through an Electronic Access Point? AEP recommends that the drafting team clarify that this is not required. "External Routable Connectivity" and "External Connectivity" definitions vary. And "External Connectivity" does not appear to be used in the standards. Should "External Connectivity" have been deleted? AEP recommends deleting "External Connectivity" unless it is used somewhere in the standards. "External Routable Connectivity" implies inbound only. Is that the intention? Why have requirements in CIP-005-5 for outbound access when it's not governed by "External Routable Connectivity"? BES Cyber Systems / BES Cyber Assets that have access outbound only are not addressed by the standards. AEP recommends "External Routable Connectivity" have "is accessible from" changed to "is accessible from or has access to" if that was the drafting team's intention. Alternatively, should "External Routable Connectivity" be replaced with "Remotely Accessible"? Is it correct that "Interactive Remote Access" does not include client-server or "process" based communications in to the ESP? AEP recommends clarifying that in the definition. In "Interactive Remote Access" the term "network-based" appears to replace "routable" – can "routable" be used for consistency? AEP recommends replacing "network-based" with "routable." In "Intermediate Device" the term "Interactive Remote Access" should be capitalized. AEP recommends the definition of "Physical Access Control Systems" be extended to exclude logging systems that are merely used as a replacement for paper log book. This definition should only refer to systems that "programmatically" participate in the logging transaction, rather than those that are used as "offline" logging systems. Does a "Reportable BES Cyber Security Incident" that compromises one part (but not all) of the BES Reliability Operating Service really qualify as a Reportable BES Cyber Security Incident? If so, AEP

recommends the drafting team add “any part” to “compromised or disrupted a BES Reliability Operating Service” in that definition. Does “Transient Cyber Asset” include removable media such as USB drives, CD-ROMs, etc.? AEP recommends that the drafting team clarify this type of removable media would not qualify as a “Transient Cyber Asset.” The definition of “Transient Cyber Asset” includes the term “directly connected” – which is not well defined. Does this infer “locally connected” or “physical attachment”? Does it include USB, serial and 2-wire signaling? Is wireless included in the phrase “directly connected”? AEP recommends the drafting team replace “directly connected” with something more descriptive. AEP would like to see the language from CAN-0005 appear somewhere in the definitions, so that CAN-0005 can be retired in favor of an appropriate definition. AEP recommends the drafting team address the issue in the definition of “Transient Cyber Asset” by clarifying that “system operator laptops with the capability and purpose of controlling BES Cyber Systems remotely (either in normal operations or in emergencies) are not Transient Cyber Assets and must be considered BES Cyber Assets.” Alternatively, the term “System Operator Laptop” could be defined separately using CAN-0005. AEP is concerned that the process for maintaining and revising the definitions proposed in this project is not clear. Obviously, changes to any one of these definitions could have cascading implications to a variety of requirements. AEP recommends that this process be explicitly stated – that the definitions can only be changed by a SAR authorized SDT.

Yes

Due to the wording changes, AEP believes it’s not accurate to say “Most of these criteria are similar to those already approved by the industry as part of Version 4” – there have been small but significant changes. AEP recommends any future questions or statements on this topic make this clear. Does an entity have to maintain evidence of 15 minute impact? Is a 15 minute “test” applied for Cyber Assets included as BES Cyber Assets, or just Cyber Assets NOT included as BES Cyber Assets? And for Cyber Assets NOT included, will there be an expectation of evidence demonstrating why (or “how long”) a system could be down without impacting the BES? AEP recommends the drafting team explicitly answer this question in the Requirement / Measures. AEP believes the Attachment 1 “bright line” criterion regarding load shedding systems (“300 MW”) should be included in the Section 4.1.2 Distribution Provider Applicability section. Otherwise, all distribution providers may be obligated to demonstrate that their UFLS / UVLS / SPS / RAS equipment was not responsible for IROL violation / 300 MW – where they may not even be aware of the full scope. Alternatively, could the Distribution Provider Applicability section (4.1.2) be clarified that it is subject to the criteria in Attachment 1? AEP observed that 1.10 in CIP-002-4 has been removed. While there may not be many Transmission facilities that meet this criterion, it seems like a logical (and essential) criterion for the Transmission connection of Generation meeting Criterion 2.1, etc. AEP recommends it be reinstated in Attachment 1. AEP encourages the drafting team to consider whether BES Cyber Assets without routable or dial-up connectivity really are Medium Impact BES Cyber Assets. Due to the isolation of these systems, they simply don’t have the risk to the BES that a non-isolated Cyber Asset would, and shouldn’t have to meet the requirements for Medium Impact BES Cyber Assets. AEP noted that applicability sections throughout the standards include references to “Medium Impact BES Cyber Systems with External Routable Connectivity” – could the drafting team simplify its work by treating these isolated BES Cyber Asses / BES Cyber Systems as Low Impact BES Cyber Assets? The heading of “Attachment I” appears to use a Roman numeral. Why not use “1” for “Attachment I”? Why use a Roman numeral? AEP recommends consistent use of the Arabic numeral “1”.

No

AEP could not find a good place to insert this comment in the question form as it applies to all of the requirements in all of the standards in this project. It has come to AEP’s attention that elements, such as measures, that are bulleted lists infer that any individual or multiple items can be considered; however, if it is a numerical list then every element is in scope and must be applied. If this assumption is correct, AEP recommends that each standard have that direction explicitly stated. Otherwise, it is extremely likely that some individuals and/or entities will overlook this important distinction. AEP further recommends that the use of “or” and “and” be used with these lists to be explicitly clear to the readers. AEP is concerned that the sentence “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls” is not clear. AEP understands this to mean that an entity does NOT have to maintain a list of Low Impact BES Cyber Assets, but must simply apply the controls outlined in CIP-003-5 through CIP-011-5 for Low Impact BES Cyber Assets. If that’s the drafting team’s intent, can that be said more clearly? AEP recommends simply explicitly stating that a list of Low Impact BES

Cyber Assets is not required, but that entities must meet applicable requirements for Low Impact BES Cyber Assets. AEP is concerned that an entity has to maintain a list of Cyber Assets not identified as BES Cyber Assets. Again, AEP recommends explicitly stating that this is not required. On page 7 the diagram uses the term “Associated Protected Cyber Assets.” Should the term “Associated” be removed? On page 7 the diagram uses the term “Associated Electronic and Physical Access Control and Monitoring Systems.” Should the term “Associated” be removed? On page 10, “Evidence Retention” states “until found compliant.” As far as AEP understands, regional entity auditors will not deem an entity compliant; they will merely report “No Finding.” AEP recommends re-writing or striking the second bullet. On page 18, in the “Guidelines and Technical Basis” the description of the BES Reliability Operating Services varies between this section and the glossary of terms. The examples provided between the two vary as well. If the BES Reliability Operating Functions are going to be referenced their description and examples should be consistent between CIP-002 and the glossary of terms. AEP recommends deferring to the glossary of terms. On page 21, in the “Guidelines and Technical Basis” the term “Substation automation” is used. This is a term with widely varying meaning throughout the industry, and is not defined in the NERC Glossary. AEP recommends the drafting team think carefully about whether to include this term, or whether to remove it altogether.
No
The requirement says “delegate” but should say “delegate(s).” The measure does not reference “delegate(s)” despite the requirement referencing “delegate.” AEP believes R2 should say “initially prior to or upon the effective date of the standard…” Without that, it would seem the CIP Senior Manager or delegate(s) would need to approve the lists precisely on the effective date.
No
The VSL table doesn’t appear to address BES Cyber Systems. The VSL table seems to favor small entities, since the “percentage” of BES Cyber Assets would be lower. AEP recommends using a percentage for everyone.
Yes
No feedback to SDT.
No
The Rationale for R2 should be restated to include the word “cyber” before security policy (“One or more cyber security policies”). AEP believes the inclusion of the word "implement" in Requirement R2 may open entities up to double jeopardy with CIP-004 – CIP-011. The security controls for 1.1 – 1.9 are implemented as part of CIP-004 – CIP-011. If the implementation of the cyber security policy is audited then would it not be an audit of the CIP-004 – CIP-011 requirements? AEP recommends removing the word “implement” in this instance. AEP is also concerned that a Registered Entity with only Low Impact BES Cyber Systems would be unable to “implement” their cyber security policy since some of these areas are not applicable to them. Are those entities expected to go beyond the standards requirements and provide evidence they have done so? Again, AEP recommends removing the word “implement” in this instance. In item 1.10 in Requirement R2, AEP noted that provisions for “responding to” CIP Exceptional Circumstances are identified here, but are not covered anywhere else in the CIP standards. This might bring into scope (for example) Business Continuity, Disaster Planning, and Emergency Medical Response plans that have no bearing on cyber security. At a minimum, AEP recommends removing the words “and responding to” from item 1.10 in R2. In Measure M2 the standard states “Records that indicate the required ten topics were implemented.” This measure should not be required, as the actual implementation of the policy is addressed in the implementation of the requirements of CIP-004 through CIP-011. If you have a non-compliance issue with a requirement in CIP-006 would the entity be non-compliant with the policy in CIP-003-5 R2? AEP recommends striking item #2 from Measure M2.
No
AEP recommends that “initially upon the effective date…” should be phrased as “initially on or before the effective date…” or something similar. In Measure M3, this should be restated as “A dated approval by the CIP Senior Manager for each cyber security policy that indicates annual approval.” Approvals can occur via a variety of methods including but not limited to “wet ink” signature.
No
AEP believes it would be beneficial to consolidate this requirement with the training requirement in CIP-004.

No
AEP understands the desire for a filter-down effect of the approvals and authorizations; however, for larger companies the documentation and updates as part of this requirement would be a significant burden without a corresponding increase in cyber security or reliability. AEP recommends that entities should be required to develop a program for approvals and authorizations that demonstrates engagement of the CIP Senior Manager, without requiring numerous explicit, documented layers of delegation. At a bare minimum, AEP strongly recommends striking the last sentence of Requirement R5. AEP suggests the wording like the current version be used "R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager." The requirement that all approvals and authorizations be performed by the CIP Senior Manager (or an explicit delegate) will require a tremendous amount of paperwork, with no commensurate increase in security or reliability. “Cyber Security Policy” is lower case in other sections of the standard, and is not defined in the definitions. AEP does not believe it should be treated as a proper noun in CIP-003-5 R5. AEP believes the reference to CIP-003-5 R3 in CIP-003-5 R5 should be to be CIP-003-5 R2. In Measure M5 the requirement allows delegation by position or name of delegate, but the measures reference individuals. This appears to be inconsistent and if this requirement is going to remain in CIP-003-5 largely “as-is” AEP strongly recommends the measure be modified to reflect that delegates can be named by position. AEP believes the last bullet in Measure M5 is too complex and recommends it be restated to be clearer if possible. AEP suggests that the use of sub-bullets or additional bullets may make this bullet point clearer.
No
Please see AEP’s comments relating to Requirement R5. The footnote indication “2” should be in superscript.
No
VRFs: AEP believes the VRF for Requirements R1 and R2 should be Lower. These requirements are documentation and administrative based requirements. VSLs: Requirement R2: The implementation of the policy is a function of implementing the remainder of the requirements in CIP-004 through CIP-011. There should not be a requirement to implement the elements of policy as an instance of non-compliance of a specific requirement will result in “double jeopardy.” As such, there should be no associated VSL. Requirements R5 and R6: The numbers in the VSL are arbitrary and do not account for the size of the company, the number of BES Cyber Assets/Systems, number of employees or number of individuals delegated for the approvals. These number stated in the VSL would be acceptable for a smaller organization, but for larger organizations this would not be appropriate. AEP suggests more Levels to be defined in the VSL to account for a wider range and urge the SDT to incorporate a percentage (in addition to an absolute number) as has been done in other standards.
No
R1.1 is applicable to “All Responsible Entities” but the section called “Rationale for R1” (not the “Change Rationale”) only discusses “personnel who have authorized…access.” AEP suggests updating the “Rationale for R1” to reflect the more general applicability of the requirement.
No
AEP is uncertain if all roles need to be trained on all items in R2.2 through R2.10, but believes that not all roles may need each of the different types of training. AEP recommends the drafting team explicitly state this R2.1. R2.2 – R2.10: AEP is concerned that a Registered Entity could create a training program with one level of detail but that an auditor will expect a greater level of detail, and deem the program insufficient. AEP recommends attempting to offer greater specificity about the minimum requirements for each of these topics. While AEP does not have a specific recommendation for the drafting team, ideas might include a minimum number of minutes, a minimum number of “quiz” questions, or a minimum number of “slides.” R2.10: AEP is concerned this topic is well beyond the scope for most users. The few personnel who have this knowledge do so because they are involved in the day to day operation, engineering, design, and maintenance of the BES Cyber Systems, not because they have received training on them. Depending on what detail is included in the training the training itself would need to be updated every time there is a change to a BES Cyber System – undoubtedly by the experts on those systems, who are likely the only people to ever receive the training. This seems like an extremely inefficient use of scarce resources. Furthermore,

AEP is concerned that all of this "interconnectivity" would need to be documented for each BES Cyber System to ensure it is covered in training. AEP recommends re-wording Requirement R2.10 to specifically address the topic of concern, or to set a minimum “level of depth” so that if this topic was covered at a cursory level in the training course, it would be deemed acceptable during a Regional Entity audit.
Yes
No comments for SDT recorded.
No
R4.1: AEP is uncertain if users with existing access to existing BES Cyber Systems are considered “grandfathered”? Or do they need to have a new initial personnel risk assessment? AEP recommends clarifying that existing personnel risk assessments are sufficient until their regular seven year expiration. Is “Social Security Number verification” still sufficient for compliance? Or is the requirement intended to require matching photo identification to name to Social Security Number? AEP suggests the drafting team clarify what is meant by “identity verification.” AEP recommends continuing to explicitly allow “Social Security Number verification” in the requirement. Again, if photo identification matching is required (in addition to SSN verification as per CIP-004-3), is it required for only new personnel? AEP recommends that the drafting team clarify that existing personnel risk assessments are sufficient until their regular seven-year update. Finally, if evidence of photo identification matching is required, it will put large, widely distributed entities like AEP at significant risk of inadvertent disclosure of Personally Identifiable Information (PII). Like many companies, AEP has worked very hard to strictly limit the collection and storage of this information – but if this evidence is required to be produced at the time of the audit, it will require personnel from outside of an entity’s HR department to have access to extremely sensitive PII. As per above, AEP strongly encourages the drafting team to explicitly allow “Social Security Number verification” in the requirement. R4.2: AEP is extremely concerned that the requirement to perform a personnel risk assessment for each location where a person has “…been employed, and / or attended school for six months or more” is very difficult to do programmatically. The location of an employer or a school is not necessarily available from the Social Security Administration or other on-line databases. It requires a subject to provide a truthful statement, and then manual processing of that statement to order the correct criminal history check. This can no longer be done programmatically, and will be enormously labor intensive. And it will still be totally dependent on a truthful and complete statement from a person who could easily “forget” certain locations. For example, many modern “schools” of higher education are virtual, and do not have a single geographic location. AEP believes this is another reason that demonstrating compliance with Requirement R4.2 as written is totally unachievable for a large entity. AEP strongly recommends narrowly on the location of residence, or returning to previous language in the requirement. R4.3: No comments for SDT recorded. R4.4: AEP believes that the combination of requirements R4.1, R4.2 and R4.4 discourages AEP from handling contractors like employees – which could weaken an entity’s program. Using an entity’s own internal “employee” program for contractor personnel risk assessments is the best possible option, but having to maintain evidence of photo id matching / identity verification for widely distributed contract personnel is an unreasonable distribution of Personally Identifiable Information (PII) – something that AEP (and other entities) must work very hard to protect. AEP believes that it is particularly difficult to validate the information provided by contractors for compliance with R4.2. Again, this combination of requirements has the effect of discouraging entities from subjecting contractors to internal programs for entity employees because the burden of collecting, validating, and protecting information for non-employees is so overwhelming.
Yes
No comments for SDT recorded.
No
R6.1: “Delegate” should be “delegate(s)”. R6.1: Somewhat duplicative of CIP-003-5, R5. R6.1: How is (i) in the “Measures” aligned with the Requirement? Why wouldn’t one of the measures be process documentation approved by the senior manager or delegate? R6.1: Aren’t (i) and (ii) and more closely aligned with R6.4? R6.1: The measures (especially (i) and (ii)) appear to expand the requirement, and add confusion about how to demonstrate evidence. R6.1: Is it reasonable to have the CIP Senior Manager or delegate(s) authorizing access in this fashion? Is that scalable? Can the CIP Senior Manager or delegate(s) authorize low level authorizers for access? AEP recommends both

re-writing the Measures, and reconsidering whether this type of authorization is scalable for a large responsible entity. (R6.2 and R6.3 are similar to R6.1, and the same comments apply) R6.2: AEP recommends “BES Cyber Systems” be replaced with “Defined Physical Boundary.” R6.4: “physical or electronic” should be “physical and/or electronic” R6.4: AEP recommends the use of “are authorized” instead of “were authorized”? As long as the workflow can be produced that authorized access (“were authorized”), they can keep the access forever. As written, this requirement appears to be more paperwork and produce less security than the current requirement to (essentially) re-authorize access quarterly. R6.5: Does this requirement require assessment of the connection of accounts to groups or privileges provided to a group? Measure (i) is the former, while measure (ii) is the latter. AEP recommends re-writing the Measure to specify one or the other. (R6.6 is similar to R6.5, and the same comment applies)
No
R7.1: AEP recommends the drafting team clarify that “time of the resignation” does not refer to when they’ve announced their resignation (“notice”), but refers to the time when their resignation is effective – which could be two weeks (or more!) later. R7.2: AEP recommends the drafting team change this to seven days. Or, at a minimum, the next business day (instead of the next calendar day). For large organizations, with a large number of transfers, it isn’t reasonable to revoke all unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day. AEP is unsure why the strict time limit is imposed on “reassignments or transfers.” These are “friendly” transactions with known personnel. AEP strongly recommends a more realistic time boundary on “reassignments or transfers.” R7.2: AEP suggests inserting “unescorted” in front of “physical access” to maintain consistency with other standards. R7.3: Can this be changed to seven days? Or, at a minimum, the next business day? Revoking information access on a Saturday or holiday could be very problematic.
Yes
VRFs / VSLs: Not yet reviewed by AEP.
No
R1.1: AEP observed that Requirement R1 states “shall implement” while Requirement R1.1 only requires entities to “define technical or procedural controls.” AEP recommends the drafting team make these consistent. R1.2: No feedback to the SDT. R1.3: What does “explicit” mean in this context? Does that mean that rules cannot be grouped together, or that systems cannot be grouped together in a single rule? AEP recommends that the drafting team clarify the use of “explicit.” R1.3: In the phrase “…including explicit criteria for…” AEP recommends replacing the word “criteria” with “justification”. The use of “criteria” implies that you need criteria to assess the quality of the justification – where the Measures seem to suggest the justification alone is sufficient. R1.3: Use of “Medium Impact BES Cyber Systems with External Routable Connectivity” in the Applicability section implies that BES Cyber Systems without External Routable Connectivity do not need explicit outbound permissions. AEP recommends the SDT should consider whether this was the intention – AEP believes all Medium Impact BES Cyber Systems should require outbound permissions. R1.4: No feedback to SDT. R1.5: AEP believes there may be other technical solutions that address FERC’s desire for “two distinct security measures.” For example, would two firewalls (in series, not in parallel) achieve FERC’s request? Or would the Intermediate Device (Requirement 2) be sufficient? There simply may be situations where IDS / IPS can’t be used, and that other solutions must be acceptable (or the requirement must be subject to TFE). AEP recommends the drafting team take another careful look at both FERC’s guidance, and this requirement. If this is to remain “as is” AEP strongly recommends permitting TFEs for this requirement.
No
R2: AEP recommends the drafting team consider making this requirement (and associated sub-requirements) eligible for TFE. While TFEs are undoubtedly cumbersome, requiring an Intermediate System may result in eliminating Interactive Remote Access to certain BES Cyber Systems – and may result in lower BES reliability. While these TFEs would have to be subject to scrutiny, AEP believes the drafting team should at least consider making the mechanism available to entities. R2.1: “Intermediate Device” is defined by the services it provides. If the services described in the “Intermediate Device” definition can be provided in an alternative device(s), why is an Intermediate Device required? Could this requirement simply articulate the services that must be provided, and the definition of “Intermediate Device” be removed? R2.2: Requirement R2.2 appears to conflict with R1.5

in certain instances due to the definition of Intermediate Device. Is there a point of having “IDS”-type systems at EAP if the traffic to the Intermediate Device is encrypted? The Intermediate Device is permitted to be inside the EAP – so the traffic crossing the EAP could be encrypted. Common sense would suggest that the Intermediate Device should go outside of the EAP or be part of the EAP itself, but that’s not required by the definition of Intermediate Device. In fact, the definition explicitly allows the opposite. R2.3: No feedback to SDT.
No
R1 VSLs: It seems like Lower / Moderate / High VSLs should be described for instances where an EAP fails, or is implemented incorrectly. “All or nothing” VSLs seem unreasonable, and different types of failure should be accounted for. R2 VSLs: It seems like Lower / Moderate / High VSLs should be described for instances where an Intermediate Device fails, or is implemented incorrectly. “All or nothing” VSLs seem unreasonable, and different types of failure should be accounted for.
No
R1: AEP has a general concern with the specific inclusion of “egress” in the measures for R1.2 and R1.3. If “access” is intended to mean both ingress and egress, the requirements themselves should be specific. R1.1 uses the term “access” yet the associated measures makes no mention of either ingress or egress. A reasonable person would assume that “access” refers to the common definition of access; “a means of approaching or entering a place. “ If access to the space within the Defined Physical Boundary is what is being protected, egress controls in this context simply do not make sense. AEP recommends the drafting team remove “egress” from the Measures. R1: If implementation is going to be included in R1 then a list of all Low BES Cyber Systems will be required to demonstrate to an Auditor that the defined technical or procedural controls have been implemented. R1: AEP had hoped to see accommodation in CIP-006-5 for entities to rely on other entities’ Defined Physical Boundary for their own BES Cyber Systems. With increasing numbers of jointly located BES Cyber Assets, AEP recommends a provision for allowing “shared” or “delegated” DPB’s somewhere in Requirement R1. This will avoid a situation where a DPB must be created within a DPB. R1.1: AEP is concerned that “Associated Physical Access Control Systems” do not need to be inside a DPB. Why not have those systems inside a DPB? With (apparently) less strenuous controls for a DPB then a PSP, why not require a DPB? R1.2: Is the implication that “access” includes both ingress and egress? Why is “egress” in the Measures? What is the requirement for controlling egress? Is that for visitors? Or for those with authorized access? R1.2: If FERC hasn’t mandated a change to controlling egress, why is it in the Measures? Again, to be clear, it doesn’t appear in the Requirements. R1.3: Same comment as R1.2 regarding egress. Is it a requirement? It’s especially concerning that this appears to require “…egress is controlled by two or more methods…” R1.3: “Requiring” (via the Measures) two methods (card / bio / PIN) for egress is not reasonable. R1.2 and R1.3: Both of these requirements use “Associated” in the Applicability. AEP believes this term should have been removed. AEP recommends the drafting team determine how to apply the term “Associated” consistently throughout CIP-002 through CIP-011. R1.4: “access point” is not defined. Would a window, hatch, etc. count as an access point? Can the term “Physical Access Point” (similar to “Electronic Access Point”) be defined? R1.4: Suggest rewording:"Issue real-time alerts to individuals responsible for responding to unauthorized physical access through access points in a Defined Physical Boundary." R1.5: Suggest rewording:"Issue real-time alerts to individuals responsible for responding to unauthorized physical access through access points in a Defined Physical Boundary."
No
R2.1: “Continuous escort” is still not defined. AEP would recommend the standards drafting team emphasize the need to prevent tampering with BES Cyber Assets. As long as the escort can prevent the escortee from tampering with BES Cyber Assets, that should be sufficient. R2.2: No comments back to SDT.
No
R3.1: Why not use the same approach for “annual” events here? AEP would recommend consistency. For example, “every other calendar year, not to exceed 27 months” or something similar. R3.2: Where did the term “Associated Physical Access Control or Monitoring Systems” come from? Is “or Monitoring” a typo? AEP recommends using the defined term where possible.
No
R1 (High): This includes a “15 minute” time limit for response – apparently a requirement. This both

requires 1) response, and 2) response within 15 minutes. Neither of which are explicitly required by R1.4. Should requirements like this be introduced in the VSLs? And how do you measure compliance? R2 (Moderate): Should this say “daily” or “per 24-hour basis” similar to the requirement? And the requirement does not say “each” – should that be removed from the VSL? R2 (High): “Continuous escort” is still not defined.

No

R1.1: AEP recommends the SDT explicitly state that only enabled “listening” ports be documented. It is not always technically feasible to collect the enabled ports on a system. Is it permissible to document enabled listening network ports as “unknown” or “under investigation”? R1.1: There is no longer a technical feasible exception process for ports and services. Previous versions of this requirement were eligible for a TFE, will that be permitted or required under this version? Two approaches to identifying enabled ports and services, as well as their drawbacks are described below: 1. Port scanning of listening ports. TCP and UDP port scanning can be technically performed to enumerate listening ports, but it doesn’t address “disabling” unused ports. This approach does not appear to be fully compliant. Port scanning is not always reliable nor feasible in every situation. 2. Positive control by reviewing / modifying device configuration which is not always technically feasible. AEP recommends the drafting team be as explicit as possible about the results (and approach) expected from entities. R1.1: the measure says “and” screen shots. Producing screen shots for a large number of BES Cyber Assets could be extremely difficult. R1.2: Again, apparently no TFE allowed for this sub-requirement. This will require the use of “administrative” controls such as signs. Should this be “Disable, restrict or discourage”? AEP recommends removing this sub-requirement as the effectiveness and quality of this control will vary wildly based on a variety of factors such as environment, device type, and usage.

No

R2.1: The comma should be removed. The word “Security” should refer to “patches”, “software” and “firmware”. Not all software and firmware updates are related to security. R2.2: Can a responsible entity develop a pro-forma remediation plan to “apply all future Windows patches” or something similar? Or does a responsible entity need a patch-by-patch remediation plan? What information is required to be included in a remediation plan? Without a minimum set of required data points, responsible entities and compliance enforcement staff may disagree on the quality of the plan. R2.2: Are there limitations to the management and execution of a remediation plan such that revisions to the plan are limited? R2.3: “A process for remediation”? Could that be clearer? Perhaps, something like “execute the remediation plan developed for R2.2” or “implement the remediation plan developed for R2.2.” Can the remediation plan be condition based, such as based on the timing of a planned outage? R2.3: The 30 day window was apparently removed from this requirement, and should be removed from the “Change Rationale” as well.

No

R3: TFEs not permitted for R3 or any of its sub-requirements. This implies that either controls may be external to the systems being protected or that each discrete device is required to have dedicated controls locally installed. R3.1: Will all systems be required to “deter, detect, or prevent malicious code” locally or can external network based controls be documented and employed? R3.2: The measure suggesting “white-listing applications” can “disarm or remove identified malicious code” is incorrect. Application white-listing technology is a preventative control, not a corrective control or measure. This measure should be moved to the measures for R3.1. R3.3: What is the appropriate means to document that a malicious code protection does not use “signatures”? R3.5: There is nothing in the “Measures” column addressing how to prove the negative. Is an attestation acceptable to prove the there were no Transient Cyber Assets attached? Is the expectation that the logs are electronically generated? If so, should this be a requirement subject to a TFE? R3.5: AEP encourages the drafting team to clarify the language in this requirement. Instead of “Log each Transient Cyber Asset connection” AEP suggests something like “Log each time a Transient Cyber Asset is connected to a BES Cyber Assets or Protected Cyber Assets.” As written, the Requirement could be interpreted to mean a log is required for each connection originated from the Transient Cyber Asset.

No

R4.1: Many devices cannot be configured to alert on these events. How should an entity demonstrate compliance for devices that cannot be compliant with this requirement? Can this be addressed in the Measures? For example, in the Measures state: “For BES Cyber Systems capable of generating logs of

events, a paper or system generated listing of event classes for which the BES Cyber System is configured to generate logs." R4.1.1, R4.1.2: AEP recommends striking the word "Any" in these two requirements. "Any" is unnecessary and unreasonable. R4.1.3: Appears to be duplicative with R3. AEP recommends striking this requirement. R4.1.4: This requirement is too general. AEP recommends striking this requirement. R4.3: If this Requirement is meant to address the failure of the security event monitoring and alerting system, should the Applicability be limited to "(Associated) Electronic Access Control or Monitoring Systems"? Or, conversely, if the "Applicability" is correct, can the Requirement be made more realistic? Demonstrating compliance for all BES Cyber Systems would be extremely difficult. R4.3: In the Requirements, AEP recommends this be "next business day" especially if the Applicability really is all referenced BES Cyber Systems. R4.3: In the Measures, how does "dated event logging failures and screen-shots showing how real-time alerts were configured" address event logging failures? This is ambiguous. Please clarify. Is it meant to refer to collecting before and after logs to demonstrate how long the system was out of service? R4.4: R4.4 specifies log retention periods for a subset of the Cyber Systems described in R4.1. Should the Applicability be the same for both requirements? If not, are undocumented retention period requirements to be decided by the Responsible Entity? R4.5: AEP recommends replacing "unanticipated BES Cyber Security Incidents" with "events that are not configured to alert, but should possibly be considered BES Cyber Security Incidents" if that was the intent of the standards drafting team. R4.5: "potential event logging failures" is addressed in R4.3, and should be removed from R4.5. R4.5: What guidelines or practices are acceptable for determining an acceptable summarization or sampling method?
No
R5.1: The "Measures" section says "internal and remote paths" but doesn't define those terms. R5.2: "delegate" should be "delegate(s)." R5.2: "administrator" is an attribute of a shared, default or user-specific account. It is not a generic account type. R5.2: The "Measures" section isn't well aligned with the "Requirements." Is a list of accounts required? It's in the "Measures" but not the "Requirements". Furthermore, the list of accounts should be adequately addressed by R5.3. Suggest deleting it from the "Measures." R5.4: The "Measures" section isn't well aligned with the "Requirements". The Requirements indicate that a procedure or TFE should be sufficient to demonstrate compliance. Why doesn't the "Measures" section say that? R5.5.3: Why not just go with calendar year within 15 months where technically feasible? R5.5.3: Who will determine if a time frame is acceptable?
Yes
"Medium" is appropriate as a VRF for each CIP-007-5 requirement.
No
R1.1: "…dated copies of…" seems unusual. Why is this phrase introduced here in the measures for CIP-008-5? R1.2: "…dated documentation of…" seems unusual. Why is this phrase introduced here in the measures for CIP-008-5? R1.3.3: Can "internal staff" include groups rather than individual names? Can "internal staff" be clarified to something like "internal groups or individuals"?
No
R2.1: The phrase "when incidents occur" appears twice in the Requirement. The second use should be struck. R2.2: AEP recommends changing "initially upon the effective date of the standard" to "prior to or on the effective date of the standard" if that's the standards drafting team's intention. R2.2: Should "implement" be "execute or exercise"? R2.3: No feedback to SDT.
No
R3.1: AEP recommends changing "initially upon the effective date of the standard" to "prior to or on the effective date of the standard" if that's the standards drafting team's intention. R3.2: No feedback to SDT. R3.3: No feedback to SDT. R3.4: Renaming organizations shouldn't count as "organizational…changes that impact that plan." For large organizations, updating an incident response plan within 30 calendar days of any organizational change (department name change, for example) is not reasonable. Recommend adding something like "organizational change or technology changes that would impede the execution of the plan." R3.5: AEP recommends that "each person" should be "each person or group" or "each person within a group" who could fill the defined role.
No
AEP recommends that the VRF should be higher than "Lower" – it seems this should be at least "Medium." R2: The VSLs should be more granular. Failing to follow a single part of the plan when an incident occurs is not a "Severe VSL." Perhaps this should be a "Medium VSL"?

No
R1.1: AEP recommends that the requirement make clear the plan itself can contain the conditions for activation (e.g., based upon an event classification). R1.2: AEP recommends that “individuals” should be “individuals or groups”. Titles might refer to a single person, where several people with similar (but unique) titles might be eligible for a particular role in the recovery plan. R1.3: “…and protection of information…” appears to create double jeopardy with CIP-011-1, R1. Can that clause be removed? R1.4: Compliance with R2 should be sufficient. It is very difficult to demonstrate initial verification of this information after the backup. Compliance with R2 should adequately test this process. AEP recommends merging this with R2. R1.4: Appears to create double jeopardy with R2.2. R1.5: This seems like a “nice to have” but could be an unnecessary distraction during a stressful time where SMEs should be focused on recovery. Worse still, this could cause double jeopardy with CIP-008. AEP recommends moving this to CIP-008, or making this a guideline. R1.5: AEP notes this requirement says “where technically feasible.” How would you create a TFE for this situation? Would it be created “retroactively”? Is this compliant with the NERC Rules of Procedure?
No
R2: FERC wanted to see Responsible Entities actually implement the recovery plans when conditions for activation actually occur. Not implement a “different” recovery plan when the “real life” situation occurs. Did the drafting team adequately address FERC’s comment? R2: Are exercises "Operational" or "Functional"? R2 uses both “Functional Exercises” and “Operational Exercises”. AEP suggests change to "Operational" for both the std/requirement and the Rationale. R2: What is the rationale for not requiring testing on Medium Impact BES Cyber Systems outside of the Control Centers? Perhaps these BES Cyber Systems should be excluded from R2.3, but not R2.1 and R2.2? R2.1: Use of “operational exercise” is confusing. As AEP understands it, this is not an “operational exercise” of BES operations. This is an “operational exercise” restore of a BES Cyber Asset / BES Cyber System. For example, rebuilding an actual PC – not moving BES operations to a backup site. Is there a different term that can be used for “operational exercise”? Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner. Is this a simulated event in a simulated environment or a simulated event in a fully operational environment? R2.1: Exercises in a simulated operational environment. AEP suggests change to "Exercises in a simulated or fully operational backup environment." R2.1: "Full operational exercise." Strike the word "full." (It appears to conflict with the language of the Rationale: "Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, system equipment setup)." R2.1: AEP disagrees that this is “essentially unchanged.” Permitting an “operational exercise” (depending on its meaning) is significantly different than what is permitted for CIP-009-3, R2 today. R2.2: Appears to duplicate CIP-009-5, R1.4. Can they be consolidated? R2.3: Use of “initially upon the effective date” is confusing. Does it have to be done prior to the effective date? Can that be clarified? R2.3: What does “representative environment” mean? Can you use “on-line” “secondary” “hot” system instead of requiring a “tertiary” system for recovery plan testing?
No
R3.1: Unless conducting an actual exercise, there’s little difference between R2.1 and R3.1. R3.1: This needs to exclude like-for-like replacement of BES Cyber Assets. Also, does vendor equipment replacement invoke this requirement? How many BES Cyber Assets within the BES Cyber System need to be replaced before this requirement is invoked? R3.2: No comments back to SDT. R3.3: No comments back to SDT. R3.4: For large organizations, updating a recovery plan within 30 calendar days of any organizational change (department name change, for example) is not reasonable. Recommend adding something like “organizational change or technology changes that would impede the execution of the plan”. R3.5: Could this say “individual or group”? In large organizations, several individuals might be included in an email distribution group, and the group would be notified – not the individuals. “Personnel” (old term) is preferred over “individual or group”.
Yes
VRFs / VSLs: Not yet reviewed by AEP.
No
R1: The applicability includes “or Monitoring” for Electronic Access Control Systems. Is this intentional? R1.1: Could recording software “hashes” be used as an alternative to recording version

levels to verify that no unauthorized changes have been made to software on the BES Cyber Asset? AEP recommends this be added to the requirement. R1.1.3: Need to figure out how to put boundaries on software installed on BES Cyber Assets. Are individual “applications” subject to this? Which “utility applications” are subject to this? Is the version “product level” or “executable level”? R1.1.4: “scripts” is problematic. Very small scripts may be used for a multitude of purposes, including one-time activities such as software installation. Can the word “scripts” be struck from this requirement? R1.1.5: Can you further define “logical network accessible ports”? R1.2: Suggest rewording: "Changes to the BES Cyber System that deviate from the existing baseline configuration must be authorized by the CIP Senior Manager or delegate(s) and documented." R1.3: Some of the changes for R1.2 may not be baseline changes for all BES Cyber Assets within a BES Cyber System. While the change in R1.2 may require a baseline change to an individual BES Cyber Asset – it would not necessarily require a baseline change to all BES Cyber Assets within a BES Cyber System. R1.3: There is not good alignment between Requirements and Measures. The Measures do not address the first part of the requirement: “updating the baseline configuration.” R1.4: There is no explicit measure for R1.4.1 (“determining the controls”). If compliance with R1.4.1 is going to be “measured”, a “Measure” should be created. Alternatively, the requirement to determine the controls prior to the change should be removed. R1.5: The applicability to Control Center BES Cyber Systems should be captured in the “Applicability” section rather than the “Requirements” section. R1.5: In the Measures, “descriptions of how any differences were accounted for” is (unreasonably) challenging. Unless this description is boring, uniform, useless boiler plate documentation, it simply isn’t possible to scale this to any large number of BES Cyber Assets. R1.5: In the Measures, it is unclear as to what “including of the date of the test” applies to. Is the measure simply stating the evidence must include the date of the test, or is it stating that any differences in the date of the test must be accounted for?
No
R2: The applicability includes “or Monitoring” for Electronic Access Control Systems. Is this intentional? R2.1: How frequently must changes to the baseline configuration be monitored for or must it be done continuously? There is no defined time frame for the detection. What is the acceptable detection window? If the change monitoring cannot be done in an automated manner, does it need to be done manually? R2.1: In the Change Rationale section, text “DHS Catalog & addresses FERC Order 706, paragraph 397” is duplicated.
No
R3.1: The applicability includes “or Monitoring” for Electronic Access Control Systems. Is this intentional? R3.2: Difficult to articulate (and account for) all of the differences in the test environment. While Responsible Entities can endeavor to make their test environment as similar as possible, creating the documentation required seems like burdensome busywork. R3.3: AEP recommends the measure say “of any tools used to perform the assessment” or something similar, since “tools” may not be used in this active vulnerability assessment. R3.3: Applicability does not include Medium Impact BES Cyber Systems, or Associated Protected Cyber Assets. Is the implication that a new, but non-essential (?) Cyber Asset becomes an Associated Protected Cyber Assets after being added to the BES Cyber System? AEP recommends that the applicability of R3.3 be extended to include at least Associated Protected Cyber Assets. R3.4: If security controls tested in the assessment are found to be deficient, would that not be a violation of the CIP standards requirement for that security control? That would require a self report. Could the self report mitigation plan be used as the action plan for 3.4? Guidelines and Technical Basis: Includes sections on “Wireless Review” and “Wireless Scanning” which seems unrelated to the requirements.
Yes
VRFs / VSLs: Not yet reviewed by AEP.
No
R1.1: Should “a documented program” be listed in the Measures? The existing Measures appear be the results of a documented program and it seems only logical that the documented program itself should be a measure of compliance. R1.2: “Part” / “Part” / “Part” should say “Applicability” / “Requirement” / “Measure” R1.2: Should “a documented program” be listed in the Measures? The existing Measures appear be the results of a documented program and it seems only logical that the documented program itself should be a measure of compliance. R1.2: How do you prove that “hardcopies of information stored in a locked file cabinet…” exists? Are you expected to show the cabinet itself? R1.2: Why isn’t a “PSP” or other access restricted boundary listed as a Measure for

controlling access to Information? “Locked file cabinet” seems needlessly specific. R1.2: Why isn’t a locked office listed as a Measure for controlling access to Information? “Locked file cabinet” seems needlessly specific. R1.3: “Process” should be listed as potentially plural; “process(es)” since the requirement permits more than one process.

No

R2: This still doesn’t address the issue that BES Cyber System Information is not typically contained on the BES Cyber Assets themselves. R2: Can this require a documented program for disposal and redeployment? And allow you to write your own program for disposal and redeployment? R2: Can this require the “assessment of adherence” that’s found in R1.3? It seems appropriate for this type of program. R2.1: Can this say “Prior to the…of media containing BES Cyber System Information…” rather than “Prior to the…of BES Cyber Asset media”? R2.1: “cleared” appears to just be a different word for “erase.” “Prevent the unauthorized retrieval” in the Requirement is much closer to the actual intent. Can that phrase be used in the Measure as well? R2.1: It does not always make sense to clear the entire media if the Cyber Asset is going to be reused, especially if it is to remain as a component of the same BES Cyber System. Simply clear the “BES Cyber System Information” from the media – not the entire media. R2.1: “Reuse” may not be the most appropriate term in the measure. “Release” may be more appropriate, or “release to non-Responsible Entity personnel” or something similar. R2.2: No feedback to SDT.

Yes

VRFs / VSLs: Not yet reviewed by AEP.

No

AEP is still concerned about the impact of version 4 on version 5. Implementing “version 4” on a “bright line” set of assets and then implementing “version 5” on those assets shortly afterwards is unnecessarily difficult. Could these new standards be accompanied by a series of “readiness” audits or something similar? There is concern that with an abrupt transition from Critical Assets / Critical Cyber Assets to BES Cyber Assets, etc. there will be uncertainty about whether the compliance program includes the “right” assets. This type of “break in” period would be essential to understanding how the standards are going to be interpreted “in real life.”

Group

MRO NSRF

Will Smith

Yes

The NSRF is recommending that since CIP version 4 has been approved by the NERC BOT and is awaiting approval from FERC, that CIP-002-5 be placed on hold. Our industry has approved CIP-002-4 and the terms Critical Assets and Critical Cyber Assets are well known terms within our current cyber security plans. The NSRF does agree that CIP-003-5 through CIP-011-5 be moved forward. The following supporting information outlines a superior solution to the proposed version 5 standards that meets the main FERC goal of including more critical assets without requiring a reduction in reliability by forcing entities to retool their existing programs from scratch. The proposed solution below allows entities to start from a firm industry approved base (CIP-002 version 4) and modify its controls CIP-003 through CIP-011. This approach also appropriately maintains an ultimate focus on protecting the electric grid elements which is the fundamental reason all NERC standards exist. The proposed CIP version 5 approach inappropriately drifts towards an Information Technology based approach. While this is understandable, given the fact cyber security is involved, any solution must remain focused on protecting the Bulk Electric System from instability, uncontrolled separation, and cascading as a whole from a relatively large coordinated attack. If the SDT does not take this recommendation then the following comments are submitted concerning Version 5 CIP Standards. Significant work needs to be performed on the definitions. Many times new definitions are proposed in version 5 that aren’t an absolute necessity. This would require entities to unnecessarily revise documentation and drawings just to meet new wording in a definition when the old definition or a change to the definition itself, rather than the term/phrase, would suffice. For example, instead of changing Critical Cyber Asset to BES Cyber Asset, retain the term Critical Cyber Asset and change the definition of Critical Cyber Asset to include “within 15 minutes”. Definitions may also confuse and unnecessarily expand the scope of compliance. This will likely generate the need for Compliance Application Notices and Standard Interpretations. The CIP Rev 5 definitions and requirements are confusing in that they require entities to carefully align separate definitions and requirements to understand the full impact. They also

unnecessarily expand the compliance scope into assets not currently covered by CIP Rev 4. This expansion will increase the burden on almost all entities. One example is, a BES Cyber Asset is defined as a “Cyber Asset that if rendered unavailable, degraded or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, adversely impact one or more BES Reliability Operating Services”. The use of adversely impact is ambiguous and will lead to people applying their own interpretation to what adversely impact means. An entity may have generation connected at the distribution level that when unavailable may adversely impact any one of a number of items listed in the definition of BES Reliability Operating Services. Recommend that the SDT update BES Cyber Asset to be: “A Cyber Asset that if rendered unavailable, degraded or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, would impact the reliable operation of the BES within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance”. This recommend definition is based Section 215, Electric Reliability, (a), (4) of the Federal Powers Act. The above recommended definition would also allow for the definition of BES Reliability Operating Services to be deleted, since BES Cyber Asset is clearly identified. The definition of BES Reliability Operating Services includes several items that a non BES user or owner does in real-time. Other examples of errors: BES Cyber Asset: Contains multiple references to other definitions. It is unclear as to the “within 15 minutes of its operation” inclusion. The redundancy of devices should be taken into consideration if there is a totally isolated redundant system providing the same functions or in a supervisory role. In protection schemes, there are primary and secondary relays which protect the same lines and a good practice recommends the relays have different logic/hardware to avoid common mode failures (totally independent of each other). BES Cyber System: Need to correct reference to Maintenance Cyber Asset BES Cyber System Information: Need to define “BES Cyber System Impact” (is this based on section 215 of the Federal powers Act?). Situational Awareness: Definition includes the term “Situation Awareness Operating Service” that is not defined. The Current day and Next Day Planning functions can typically be performed on a corporate PC, does this bring the entire corporate network into scope? Control Center: Based on this definition, a Control Center could be a building at a substation with 2 RTU’s that monitor a 345 KV substation with multiple transmission facilities (lines) and a 115 KV substation with multiple transmission facilities (lines) in two different yards (locations) but geographically adjacent. Need to clarify that the two or more locations refers to some type of geographical separation. Otherwise the control building could meet the bulleted items under the Control Center definition. Transient Cyber Asset: Need to break up the 3rd qualifier based on the intention of the SDT as such: “3) capable of altering the configuration, or (and) 4) capable of introducing malicious code to the BES Cyber System.” A second example of where definitions may also confuse and unnecessarily expand the scope of compliance is shown just below: CIP-002-4 requires cyber controls on: 1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection. (Emphasis added) Whereas: CIP-002-5 requires cyber controls on: Control Center One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations: • Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, • Inter-utility exchange of BES reliability or operability data, • Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES, • Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function, • Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES • Coordination of BES restoration activities. 2. Medium Impact Rating (M) Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for: 2.13. Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners; or (2) generation control centers that control 300 MW or more of generation (emphasis added) The concern here is that every Distributed Control System (DCS) that control two or more generators or substations with a total output of more than 300 MW will now be subject to the CIP standards. Even if the DCS is not externally connected by serial or routable protocols it will be subject to the CIP

standards.
Yes
The NSRF is recommending that since CIP version 4 has been approved by the NERC BOT and is awaiting approval from FERC, that CIP-002-5 be placed on hold. Our industry has approved CIP-002-4 and the terms Critical Assets and Critical Cyber Assets are well known terms within our current cyber security plans. The NSRF does agree that CIP-003-5 through CIP-011-5 be moved forward. The following supporting information outlines a superior solution to the proposed version 5 standards that meets the main FERC goal of including more critical assets without requiring a reduction in reliability by forcing entities to retool their existing programs from scratch. The proposed solution below allows entities to start from a firm industry approved base (CIP-002 version 4) and modify its controls CIP-003 through CIP-011. This approach also appropriately maintains an ultimate focus on protecting the electric grid elements which is the fundamental reason all NERC standards exist. The proposed CIP version 5 approach inappropriately drifts towards an Information Technology based approach. While this is understandable, given the fact cyber security is involved, any solution must remain focused on protecting the Bulk Electric System from instability, uncontrolled separation, and cascading as a whole from a relatively large coordinated attack. Issue: As currently drafted Version 5 of the CIP standards: • Would significantly increase cost without a commensurate increase in the reliability, safety, or security of the BES. • Create significant complexity, confusion, and administrative burden regarding the identification of Critical Cyber Assets, the definition of terms, and implementation of Cyber Controls. • Exceeds FERC's 706 order without justification. Proposed Solution: 1. Retain CIP-002-4 as approved by the industry in 2010. It is filed with FERC; industry and NERC comments on the FERC NOPR recommended FERC approval. This will: • Eliminate the confusing and complicated process developed to identify BES Cyber Systems proposed by the drafting team in Rev 5 • Meet FERC's 706 for CIP-002-1: o Industry approved guidance documents for identifying Critical Assets and for identifying Critical Cyber Assets. ¶253-258, 270-273 o CIP-002-4 replaces the Critical Asset guidance and aligns with FERC's affirmation that the applicable responsible entities are responsible for identifying Critical Assets. ¶319-321 o CIP-002-2 added senior manager approval of risk-based methodology. ¶294-297 • Not exceed FERC Order 706: o ¶284: "… there is no formally accepted method for identifying critical cyber assets before us at this time … we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time." o ¶285: "CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial up access … We do not find sufficient justification to remove this provision at this time." 2. Develop a new standard for High Impact Assets: • That identifies which assets in CIP-004-2 are High Impact and • Clearly states the extra protection required for High Impact Assets: o The Draft version 5 identifies eight extra protections, most are in response to FERC Order 706. o Provides opportunity for a separate implementation timeline for the additional controls that apply only to High Impact assets. o Provides flexibility in adjusting controls on High Impact assets. In the future only one standard has to be modified. o Entities that do not have High Impact assets will not have to sort through all the standards and RSAWs to assure compliance and security. 3. Develop a separate standard for the Low Impact assets or abandon this concept. • Lows were not directed by FERC Order 706 nor included in the SAR. o A separate standard provides full transparency in the stakeholder process. o This is a scope expansion not supported by many in the industry. o Cost and compliance concerns with lows include whether lows have to be listed. This is a derivative of which controls are selected and how they are designed and audited. 4. Revise CIP-003-5 through CIP-011-5 and Definitions to reflect changes described in this paper and meet FERC Directives in order 706. If the SDT does not take this recommendation of maintain CIP-002-4, then the following comments are submitted. Keep the "bright-line" criteria thresholds defined in CIP-002-4 in the CIP-002-5 standard. There was much industry input into developing these thresholds and it does not seem appropriate to modify them again. It is difficult for utilities to keep up with the changing thresholds in the changing CIP versions and associated implementation plans, with no BES reliability improvement Issue - 1 high Impact, bullet 1.2, states: Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority. The NSRF does not understand how this can be applied to every BA, regardless of size. Upon review bullet 1.2 has qualifiers for a TOP in order to be a High Impact category (notwithstanding that a TO should not be included since TO's are not required to have primary or backup control centers). Recommend the similar qualifiers contained bullets 2.1, 2.3, 2.4, and 2.12 be written for a BA to be in the High Impact category. We can easily see that there is some stratification afforded to TOP and GOP Control Centers, based on voltage levels, total MW, total MVAR, number of lines, Blackstart Resources, etc, for being considered High Impact or Medium

Impact. While the SDT has acknowledged there are some distinct differences between larger and smaller TOP's and GOP's, we want to point out that not all Balancing Authorities are created equally. Does anyone think that the smallest BA, serving 38 MW of load, has the same Reliability Impact as a BA serving 10,000 MW, or more, of load? Does it really improve the reliability of the BES to have ALL those smaller BA Control Centers carry the High Impact Rating? Issue - Criterion 2.7 in Attachment I describes the "weight value" to be applied to transmission lines. There is no guidance given for transformers. Many entities may treat a facility that has multiple voltages as separate substations, with separate control houses, and may be assessing the independent Impact Level of each voltage as separate facilities. Therefore, there must be some guidance on how to deal with transformers. Furthermore, it is suggested that the weight value given a transformer (if transformers are to be included in the calculation) be the weight value of the secondary, not primary side. For example, a 345kV substation may have a single 345kV transmission line out of it, weighted at 1300. That same substation may then have two 345kV/230kV transformers. It is not obvious from criterion 2.7 what the total weight of the substation would be. It is suggested that the secondary voltage be used (if transformers are to receive a weighting value) making each of these transformers valued at 700, for a total of 2700 at this substation, making it Low Impact. However, if the primary voltage level was used to determine the weight, the transformers would each count for 1300, making the total weight value of this substation 3900, and a Medium Impact facility. It is suggested, if transformers are to be included, that the secondary voltage be used because, from the 345kV bus in this example, its two additional outlets (the transformers) are only capable of 230kV outlet flows, even though they are connected to the 345kV bus. Issue - Criterion 2.8 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLs and their associated contingencies' with wording of, '. . . as Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more IROL violations', like the wording using in Criterion 2.11. Issue - Criterion 2.11 in Attachment I states "Each SPS, RAS or automated switching scheme that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more IROL violations." It is unclear whether the phrase "that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more IROL violations" refers to the SPS itself or the BES elements that the SPS operates. It is possible (and likely) for an SPS to be a higher Impact Level than the BES elements that it operates. Assuming the phrase is meant to apply to the SPS, a suggested re-wording of this phrase is the following. "Each SPS, RAS or automated switching scheme that operates BES Elements and is capable of causing one or more IROL violations if the SPS is destroyed, degraded, misused or otherwise rendered unavailable. We propose the following: Criterion 2.9 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLS and their associated contingencies' with wording of, '. . . as FACTS that if destroyed, degraded, misused, or otherwise rendered unavailable, could cause the violation of one or more IROLs', like the wording using in Criterion 2.11. Criterion 2.12 – (1) Replaced the word, 'system' with 'common control system' to clarify that this criterion applies to a system triggered by a single (common) control, rather than a program (system) of many independent relays set to trip at the same frequency.
No
Issue - What is the NERC basis for 30 days. Many reviews are performed annually. NERC has not provided any technical justification for a 30 day update. An annual update is sufficient based upon the low probability of a serious cyber or physical attack. Issue - The text "all other BES Cyber Assets and BES Cyber Systems … shall be deemed to be Low Impact." This text appears to include all BES Cyber Assets in CIP scope, which was not directed by FERC Order 706.
Yes
Issue - With recent guidance on the term "annual" provided by NERC, it may be prudent to replace the phrase "and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals" with the word "annually".
No
Issue – We believes that the VSLs recognize the fact that entities of different sizes are taken into account in the severity levels and associated impacts to the BES.
No

Issue - Most of the changes made to CIP-003, in general, were not directed by FERC Order 706. These changes do not result in improvements to security, but do result in increased bureaucracy and implementation costs for 241 entities with existing programs. We suggests the FERC directives be addressed within the structure and language of CIP version 4. We propose the following requirements for CIP003-5: R1: Cyber Security R2: Leadership R3: Exceptions R4: Information Protection
No
This is an administrative task and once written does not add to BES security.
Yes
Issue - With recent guidance on the term “annual” provided by NERC, it may be prudent to replace the phrase “and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals” with the word “annually”. Issue - suggest changing to annual “review” and NOT approval. Entities need not “approve” the same security policy if there are no changes or updates.
Yes
Yes
Yes
No
Issue - Many of the changes made to CIP-004, in general, were not directed by FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for 241 entities with existing programs. We suggests the FERC directives be addressed within a structure and language that is more in line with CIP version 4. We propose the following requirements for CIP-004-5: R1: Awareness R2: Training R3: Personnel Risk Assessment R4: Access
Yes
Yes
No
Issue - Add clarification to R4.4 in terms of vendor support from foreign companies. Please clarify when an Entity or contractor is initially in the CIP Standards then they are removed (for some reason) then they are brought back into CIP compliance. Is the risk assessment previously obtained in it is still within 7 years?
Yes
No
Issue - In FERC Order 706, paragraph 381, the Commission stated its intent is to ensure there is a clear line of authority. Order 706 did not direct making the senior manager authorize every individual change down to the account level. The version 5 draft is an additional administrative burden that does not commensurately improve security of the Bulk Electric System and creates a disproportionate amount of bureaucratic work.
No
Issue - For reassignments requiring a different level of access, there may be the need for a large amount of work in setting up new user accounts, modifying user accounts, changing firewall and router rules, etc… that cannot be accomplished by the end of the next calendar day without jeopardizing reliability. This is also an issue for BES Cyber System information for entities which are using document management systems with individual accounts to restrict access to information. It is usually easier to “remove” an account than it is to “modify” an account, yet the modification of these accounts is subject to a single calendar day while the removal of these accounts is allowed for 30 calendar days. Due to the amount of reconfiguration needed for these types of changes, it is suggested to allow at least 7 calendar days for modifications in access levels. Issue - FERC Order 706 did not direct a change. We recommend retaining CIP-004-4 where revocation already is covered.

Issue - The time requirements are too restrictive for Medium Impact BES Cyber Systems. Allowing 7 calendar days for R7.1 and R7.2 would be more acceptable and practical for systems that may not be controlled centrally. Issue - We appreciate how the SDT tried to give treatment to the “immediate revocation” requirement of the FERC order in Part 7.1. However, we feel the current language is too open for interpretation. Even with the footnote qualification, an auditor could still interpret “at the time” to mean literally “to the minute”. Complicating matters is the fact that there is often no way to measure specifically when a person resigned or is terminated. Our suggestion for Part 7.1 is to restate as: “Develop and implement a program to revoke an individual’s unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of resignation or termination”. This way, the entity is measured for compliance to their own program and not struggling to provide time-stamped comparisons that may not exist. For Part 7.5, it is possible that entities use shared accounts for remote access. Suggest adding “...if shared accounts are used for Interactive Remote Access to BES Cyber Systems, passwords must be changed at the time of resignation or termination per Part 7.1”.
Yes
No
Issue - R1.1. Appears to require that you document Low Impact Cyber Systems. This requirement should not be required for Low Impact BES Cyber Systems; otherwise we have to prove to auditors that external routable connectivity is not used at EVERY Low Impact BES Cyber System.
No
Issue - The requirements ignore the fact that some utilities have their own (unique) communication network from the Control Centers to the substations. Adding encryption devices and additional devices adds additional points of failure without increasing security. Exceptions should be made for interactive remote access across company owned and operated communication links.
Yes
No
Issue - In the “Measures” column of Table R1, Part 1.1, it states the need for documented “operational and procedures controls”, while the requirement is “operational or procedural controls”. Please correct the Measures column to be consistent. If the error was in the Requirements column, we disagree that operational physical access control systems should be required for Low Impact BES Cyber Systems. Issue - The Requirement in Table R1, Part 1.2 and Part 1.3, should define whether or not these physical access controls are to be operational, procedural, either, or both for Medium Impact and high Impact Cyber Systems as was done in Part 1.1 for Low Impact Cyber Systems. If operational controls are required, is a separate operational physical access control system needed to monitor the primary physical access control system or is it allowed for a system to monitor access to itself? Issue - For CIP-006, in general, we disagrees with changing the definition name from Physical Security Perimeter to Defined Physical Boundaries because it unnecessarily creates the need to update numerous procedure documents and physical security drawings, etc. Changing the term does not improve security, but increases confusion and costs for 241 entities that have Physical Security Perimeters.
No
Issue - R2.2 does not seem applicable to Medium Impact Substations. The logging of entry and exit of visitors will be tedious without much value. R2.2. should only be applicable to Medium Impact Control Centers.
No
Issue - R3.1 and R3.2 will be troublesome for Low Impact Facilities that may use procedural controls for Physical Access Control. What hardware or devices will be included? R3.1 and R3.2 should only be for applicable electronic physical access control systems
Yes
Yes

No
Issue - Suggest changing the term “remediation” to “mitigation”. R2.3 appears to require the installation of the patches, where some utilities may mitigate the vulnerability through procedural controls.
No
Issue - R3.1. Allows the Responsible Entity to choose which approach they want to take “deter, detect, or prevent”. If a Responsible Entity chooses to deter or prevent malicious code by procedural controls on isolated control systems (i.e. non-routable serial links), requirement R3.2 and R3.3 are impossible to achieve. Additionally, R3.3 requires modifying a tested and working control system at a substation with the possibility of inadvertently introducing malicious software with manual updates (e.g. using thumb drives to install signature updates on non-networked systems.) Recommend excluding Medium Impact BES Cyber Systems that do not have external routable connectivity. (Most AV or malicious code software cannot recognize new malicious code such as Stuxnet until the signatures are discovered anyway).
No
Issue - FERC Order 706 didn’t direct changes. CIP-007-5 R4.1 - The enumerated list is too prescriptive for the requirement. Add to guidelines. CIP-007-5 R4.2 – Some assets can log, but not alert. Remove “real-time”. CIP-007-5 R4.3 – Clarify timing. We propose revised text, “Activate a response to event logging or alerting failures before the end of the next calendar day after identification. Issue - It is great to see how the SDT allowed entities to develop their own system events related to cyber security, but this leaves an open door for auditors to apply their own approach (and interpretations) to what the auditors believe is acceptable. R4.1. will be troublesome for entities to prove compliance with Medium Impact BES Cyber Systems with no external routable connectivity, unless the auditors accept the configuration files and not the actual logs. Issue - R4.2. Also leaves a large audit hole for the entity determining what events necessitate a real-time alert and the auditors having differing opinions of what they feel the entity should include. Issue - R4.3. Additional information should be provided for the requirement on how it will be possible to detect an event logging failure for a failed physical contact/sensor before the end of the next calendar day (e.g. door alarm contacts). Suggestion: This should be rewritten to only include “the event logging system failure, not to include sensors).
No
Issue - Delete R5.2 because it replicates the CIP-004 access authorization requirements and could create double jeopardy. Issue - R5.5.1 – FERC Order 706 did not direct a change to password length. Although an increase in password length from six to eight characters improves security, an increase to ten would improve it more and so on. Where does one stop? Not all assets have capability for longer passwords. We recommend retaining the six-character password. Issue - R5.4. Should be limited to Entities having a policy in place that all default passwords should be changed. Proving compliance at a sampled location basis opens up the door in an audit to have entities having to prove compliance on all their BES cyber systems if there is 1 finding. The 1 finding would require the entity to have to inventory all Low Impact Cyber Systems and show that every system had the default password changed. The requirement also leaves open the auditor’s interpretation of what is considered a Low Impact Cyber System at a sampled location, since there is not an inventory required by the standard.
Yes
No
Issue – The SDT should coordinate more closely with EOP-004-2, SDT
Yes
Yes
Yes
No

Issue - R1.5 states, “Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.” As FERC Order 706, paragraph 708 states, “should not impede or restrict system restoration”, we recommend this proposed revised text: “Preserve data, when it does not impede or restrict system restoration, if necessary to determine the cause of any event that triggers activation of the recovery plan(s) as required by Requirement R1.
No
Issue - The wording in the Requirement Column of Table R2, Part 2.2, implies that all backup media must be tested annually. If an entity, for example, has 25 Windows Servers – that entity should be able to annually test a Windows backup without having to test the backup for each system, especially if the same backup system is being used for all Servers. This is even more extreme in the case of substation cyber assets, such as protective relays. Recommend changing the language “Test any information used in the recovery …” to “Test information, for each type of Cyber Asset, used in the recovery …”.
No
Issue - In Table R3, Part 3.4, the language “Update recovery plan(s) to address any organization or technology changes…” is too vague in regards to technology changes. Recommend wording as “Update recovery plan(s) to address any organization or implemented technology changes…” Issue - R3.1. Is not clear on how soon the recovery plan has to be updated “when BES Cyber Systems are replaced”. Suggestion: Include “or within 30 days of when BES Cyber Systems are replaced.” Recommend that “Update recovery plan(s) to address any organization or implemented technology changes that would prevent a successful implementation of the recovery plan”
Yes
No
Issue - The draft requirement is too prescriptive, which was not directed by FERC. Move the details to guidelines. Recommend limiting the applicability to High Impact Critical Cyber Assets, which will allow entities to focus security improvement efforts on the highest priorities. Issue - R1.1. Will be time-consuming for Medium Impact BES Cyber Systems at substations/plants. The number of IED’s and programmable devices are very large and some of these devices may have multiple modules or add-on boards with different software versions. Issue - R1.2. and R1.4. Will create problems when making emergency repairs in the field that require replacing a “card” or “module” with different software versions and obtaining CIP Senior Manager approval. Suggestion: Provide a separate requirement for Medium Impact Control Centers and Medium Impact Systems excluding Control Centers which allow more flexibility for the type of environments and equipment. For Medium Impact BES Cyber Systems excluding Control Centers could require documenting baseline configurations on only a subset of the cyber assets (e.g. HMI’s, EAP’s, etc.) not including meters, gauges, battery chargers, electronic programmable thermostats, relays, modules, PLC’s, etc
No
Issue - We recommend that the applicability of Table R2, Part 2.1 include only “Medium Impact BES Cyber Systems with Routable Connectivity”. By requiring baseline monitoring of a system, the existence of a routable connection would be required. If an entity feels that a Medium Impact BES Cyber System should not have routable connectivity out of the perimeter (for example, a substation), then it should not be required to automatically detect baseline configuration changes since the implementation of such a system would require a routable connection from the system server to the Cyber System. Furthermore, some entities may have Medium Impact Cyber Systems at locations where the only means of communication is a low-quality analog microwave system, which may not be able to accommodate the traffic of a baseline configuration system. Issue - FERC Order 706 did not direct authorization by the senior manager or delegate, but to “express acknowledgement of the need for change control.” We recommend this can be achieved with revised text, “Authorize changes to hardware and software components of Critical Cyber Assets.” Issue - R2 does not provide any benefits and any changes should already be covered under R1.3. of CIP-010. Recommend to remove this requirement. Issue - Requirement R2 needs a lot of work and justification. Perhaps unintentionally, this requirement as written will result in another massive filing of TFE’s, since we can’t install a “Tripwire” on my Router. While the purpose of the requirement is well-intentioned, with good reference to best practices, the application doesn’t work outside traditional IT server-based cyber

assets. This is a net-new requirement within CIP that, if retained, will require major initial and ongoing investment by entities for little reliability benefit. We recommend striking R2, or vastly limiting its scope (Server-type assets at Control Centers, for instance).
No
Issue - Annual vulnerability assessments on Medium Impact Cyber Systems will prove to be very costly and resource intensive for utilities with multiple substations in this category that are geographically dispersed. We recommend allowing Medium Impact Cyber Systems to have 2 years between vulnerability assessments. Issue - Though FERC directed guidance for Vulnerability Assessments, the rewritten standard's general reference to "security controls" could result in varying interpretations and likely expansion of assessment scope. Issue - R3.1. Needs to be reworded to more clearly define if the assessment is a vulnerability assessment or only an "assessment of the security controls", such as the EAP and Physical Access Controls. Issue - R3.2. Should allow entities to perform an active vulnerability assessment on either the production system or the test environment to meet the requirement. This will allow entities to make the choice on which environment to use and not require the documentation of differences between the test environments and production environments that leave entities open for interpretation of differences by auditors. Issue - For Part 3.2, please clarify whether all cyber assets need to be included in the assessment, or a subset, or representative sampling, or entity defined. There are certain cyber asset categories where "test" systems just aren't economically feasible. What is the acceptable deviation between test and production the auditors will allow? As written, and without explicit language in the requirement, our entity fears this will be a topic of a CAN later. Issue - For Part 3.3, please clarify whether "new Cyber Asset" means literally that or, more reasonably, could mean "new Cyber Asset category" or a new make/model, or a new function. It would be reasonable to test something that brings net-new functionality to a BES Cyber System, but if when replacing an end-of-life or failed component, it wouldn't make sense.
Yes
No
No
Issue - R2.1. Needs to include additional clarification of devices that are included. Where do protective relays or devices that have flash memory or other on-board memory media fall? Does this apply when reusing the device from a Medium Impact BES Cyber System to a Low Impact BES Cyber System? The application guideline does not distinguish if there is a difference between impact levels and only refers to reuse outside of a BES Cyber System (e.g. could go from High-Medium-Low without being erased).
Yes
No
Issue - It is imperative for the industry to know whether or not Version 5 will supersede Version 4 well in advance of any implementation plan. If Version 4 has a short implementation period before Version 5 is in effect, entities will view their efforts to comply with Version 4 as "wasted" in many cases because the infrastructure required for a Version 4 Critical Asset is more than that of a Version 5 Medium Impact facility. It would be irresponsible to ask entities to "over-protect" facilities that will not be High Impact with Version 5 right around the corner. In addition, this could also have a drastic impact on decreasing reliability as many entities may elect to remove all routable protocols and dialup access to cyber assets within Version 4 "Critical Assets", to bide them time until Version 5 becomes effective. During this time, engineers would not have access to troubleshoot protection systems, retrieve fault data, and perform multiple other duties without having to travel to a remote site – this could result in prolonged customer outages, and possible instability with known defects in design taking longer to correct. Entities realize that NERC has made an effort to do this, however, there is still risk associated with version 5 not passing in time to supersede version 4. This could be catastrophic to the standards development process.
Individual
Chris de Graffenried
Consolidated Edison Co. of NY, Inc.

No

Minor corrections should be made to list of topics under R2. They are listed as 1.1, 1.2, 1.3 etc. They should either be labeled as 1 through 10, or 2.1, 2.2 through 2.10.

No

4.1 and 4.2 do not clearly indicated whether an entity current PRA policy covers full identify verification and documentation of any PRA that could not go back a full 7 years. It should be made clear whether either of these requirements is retroactive or whether any PRA prior to the effective date of the standard are grandfathered. It is recommended that the committee not require previously completed PRA to be updated.

No

1. R7.1 is unclear even with the footnote description of what the desired time frame is for “at the time” of resignation or termination. The phrase “at the time” needs to be defined as simply same day, before COB or end of day. The requirement also appears to apply to any reason for departure from the company. An individual leaving for retirement or termination due to unethical behavior would be treated the same. We feel there needs to be a differentiation between an individual being “fired” and an individual leaving for other reasons. It is recommended that same day revocation be required to termination for cause, and a two day revocation for any other departure. 2. The revocation periods for R 7.2 and 7.3 should be subsequently changed to match the recommended two day revocation mentioned above. 3. For environments that do not have external connections and maintain physical security access, such as individual non networked microprocessor relays, the risk to system reliability associated with frequently accessing the relay for purposes of changing the password outweighs the benefit achieved through this password change. It is recommended to alter this requirement to allow periodic (twice per year) password changes on these types of devices (R7.5).

No

Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to alerts in 15 minutes. There is a disconnect between the requirement and the VSL table.

No

Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to

alerts in 15 minutes. There is a disconnect between the requirement and the VSL table. Also reference to part 1.6 appears to be incorrect, should be 1.4.
No
No
The change to R2.2 goes beyond the stated rationale of requiring the current assessment to include the identification of what/who the source of the patch is so the time of availably can be determined. The new requirement now also requires a plan vs. assessment and requires including in the plan a defined timeframe; each of which is beyond the rationale. It is recommended that the word “plan” be replaced by “assessment” as is the current requirement, and that the additional requirement to include in the plan a defined time period be removed as it is in the current requirement. If a time frame is desired, we recommend that the timeframe be a planned timeframe and not a fixed timeframe. It is also recommend that a “plan” not be required as it implies a more extensive documentation of the patch reviews which will require additional paperwork that will not add value to the patch process.
No
R4.5 requires a manual review of a sampling of logged events every two weeks. The frequency is excessive, requiring 2-3 days per review, and will provide minimal value. We recommend once per month (R4.5). R4.3 – The requirement as written can be interpreted very broadly. It is not clear whether the intent is to detect a device has stopped sending log or the logs have stopped being accumulated by the receiving end (Syslog for example) is vague. If it requires detecting something is not sending logging within 24 hours this can be an issue, as some devices do not send logs every day. Some UPS devices , KVMs, and network switches only send a log if something occurs. There may several days without use and therefore no logs. Also, every time someone shuts down a workstation logs will not be sent. If action needs to be taken each of these times that would require documenting on a daily basis numerous events. This requirement should only address that action if the log repository has stopped recording incoming logs.
No
R5.4 is not clear as to whether unique default passwords applies to application level passwords only or includes default vendor user passwords also. The language needs to be clarified.
No
R3.2 requires active scanning in an environment that models baseline configuration. This may be impractical to replicate, the replication will need to be maintained and the some systems may have issues with active scans. Recommendation: A complete active scan should not be required (R3.2).
CIP-011-1 Requirement 1.1: The Measures associated with R1.1 indicate that evidence may include indications on information (e.g., labels) that identify it as BES Cyber System Information. It is suggested that the SDT expand on what types of repository would require labeling. For example, it may not be reasonable to label micrographic media, but rather label the cabinets or a room where the media is stored. Recommendation: We recommend allowing the entity appropriate discretion when applying labeling. CIP-011-1 Requirement 1.2: Measures associated with R1.2 indicate that evidence

could be provided that shows user access is implemented on a “need to know basis”. The Measure should state that “need to know” personnel are determined by the registered entity. Similarly there is a suggested Measure that hardcopies of information be stored in a locked file cabinet with keys provided to only “authorized individuals”. Recommendation: The Measure should include language indicating that the registered entity identifies the “authorized individuals”.

No

CIP-011-1 Requirement 2.1: “Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was cleared prior to its reuse.” Recommendation: SDT should define what “cleared” means. The language in footnote #2 should be included in the wording of R2.1, to ensure it becomes part of the Requirement.

No

General Comments: 1. Applicability sections of CIP-002-5 through CIP-011-5: the Applicability sections should be consistent. Note that in CIP-005-5 and CIP-006-5 the Applicability sections 4.2.2 are different from the other CIP standards. We recommend that the drafting team adopt consistent Applicability language across all Version 5 CIPs. Alternatively, the drafting team should explain any Applicability variances between the various Version 5 CIPs. 2. CIP-006-5 Requirement 1, Guidance section on pp. 22 and 23 (Guidelines and Technical Basis): “While the focus is shifted from the definition and management of a completely enclosed “six-wall” boundary, it is expected in many instances this will remain a primary control for controlling, alerting and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems. … Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.” Comment: In reviewing CIP-006 – 5 we have seen that the “enclosed 6 wall” wording is removed, but it appears as though six walls are still required. The guidance section mentions that the Defined Physical Boundaries are allowed to have openings less than 96 square inches but does not exclude the need for 6 walls, only that they are not required to be completely enclosed (excerpt above). Is this correct? Would a window be considered an “opening,” to be protected by a barrier as noted in the guidance? The CIP wording could be read as requiring a ‘ceiling’ over open air substations in order to preclude exceeding the 96 sq. in. and 6-inch limits. We do not believe that this was the drafting team’s intent. What was the drafting team’s intent? Recommendations: We suggest that this matter be clarified by the addition of wording specifically allowing an exception from this requirement for open air substations, such as, “This requirement does not apply to open air substations” or “This wording is not intended to require placement of a roof over open air substations.” Alternatively, if it was the drafting teams’ intend to apply this requirement to open air substations, then would surrounding all BES Cyber Systems in six-walled enclosures within an open air substations meet the objective of this requirement? Clearly, a roof should not be required for and physically cannot be installed over all open air substations. 3. The use of the “Measures” column for each requirement is beneficial as are the guidelines of each CIP standard. Providing these as part of the standards can imply that they are part of the requirements. By this one could see that by meeting the measures for each requirement that will be in compliance. Also the guidelines provide much more information than the requirements. The requirements tell you to perform an assessment without specifics while the guidelines provide specifics. Are the guidelines to be read as requirements? For example, A Defined Physical Boundary is required, but it is not until the user reads the guidelines is there mention to it needing to be enclosed completely with limitations on the openings. The requirements call for a active vulnerability assessment and it is not until the guidelines that what should be in an assessment is provided.

Individual

David Burke

Orange and Rockland Utilities, Inc.

No

Comments: Minor correction should be made to list of topics under R2. They are listed as 1.1, 1.2, 1.3 etc. They should either be labeled as 1 through 10, or 2.1, 2.2 through 2.10.

No

Comments: 4.1 and 4.2 do not clearly indicated whether an entity current PRA policy covers full identify verification and documentation of any PRA that could not go back a full 7 years. It should be made clear whether either of these requirements is retroactive or whether any PRA prior to the effective date of the standard are grandfathered. It is recommended that the committee not require previously completed PRA to be updated.

No

1. R7.1 is unclear even with the footnote description of what the desired time frame is for “at the time” of resignation or termination. The phrase “at the time” needs to be defined as simply same day, before COB or end of day. The requirement also appears to apply to any reason for departure from the company. An individual leaving for retirement or termination due to unethical behavior would be treated the same. We feel there needs to be a differentiation between an individual being “fired” and an individual leaving for other reasons. It is recommended that same day revocation be required to termination for cause, and a two day revocation for any other departure. 2. The revocation periods for R 7.2 and 7.3 should be subsequently changed to match the recommended two day revocation mentioned above. 3. For environments that do not have external connections and maintain physical security access, such as individual non networked microprocessor relays, the risk to system reliability associated with frequently accessing the relay for purposes of changing the password outweighs the benefit achieved through this password change. It is recommended to alter this requirement to allow periodic (twice per year) password changes on these types of devices. (R7.5).

No

Comments: Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to alerts in 15 minutes. There is a disconnect between the requirement and the VSL table.

No

Comments: Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to alerts in 15 minutes. There is a disconnect between the requirement and the VSL table. Also reference to part 1.6 appears to be incorrect, should be 1.4.

No

Comments: The change to R2.2 goes beyond the stated rationale of requiring the current assessment to include the identification of what/who the source of the patch is so the time of availably can be determined. The new requirement now also requires a plan vs. assessment and requires including in the plan a defined timeframe; each of which is beyond the rationale. It is recommended that the word "plan" be replaced by "assessment" as is the current requirement, and that the additional requirement to include in the plan a defined time period be removed as it is in the current requirement. If a time frame is desired, we recommend that the timeframe be a planned timeframe and not a fixed timeframe. It is also recommend that a "plan" not be required as it implies a more extensive documentation of the patch reviews which will require additional paperwork that will not add value to the patch process.
No
Comments: R4.5 requires a manual review of a sampling of logged events every two weeks. The frequency is excessive, requiring 2-3 days per review, and will provide minimal value. We recommend once per month (R4.5). R4.3 – The requirement as written can be interpreted very broadly. It is not clear whether the intent is to detect a device has stopped sending log or the logs have stopped being accumulated by the receiving end (Syslog for example) is vague. If it requires detecting something is not sending logging within 24 hours this can be an issue, as some devices do not send logs every day. Some UPS devices , KVMs, and network switches only send a log if something occurs. There may several days without use and therefore no logs. Also, every time someone shuts down a workstation logs will not be sent. If action needs to be taken each of these times that would require documenting on a daily basis numerous events. This requirement should only address that action if the log repository has stopped recording incoming logs.
No
Comments: R5.4 is not clear as to whether unique default passwords applies to application level passwords only or includes default vendor user passwords also. The language needs to be clarified.
No
Comments: R3.2 requires active scanning in an environment that models baseline configuration. This may be impractical to replicate, the replication will need to be maintained and the some systems may have issues with active scans. Recommendation: A complete active scan should not be required (R3.2).
No
Comments: CIP-011-1 Requirement 1.1: The Measures associated with R1.1 indicate that evidence may include indications on information (e.g., labels) that identify it as BES Cyber System Information. It is suggested that the SDT expand on what types of repository would require labeling. For example, it may not be reasonable to label micrographic media, but rather label the cabinets or a room where the media is stored. Recommendation: We recommend allowing the entity appropriate discretion when applying labeling. CIP-011-1 Requirement 1.2: Measures associated with R1.2 indicate that evidence could be provided that shows user access is implemented on a "need to know basis". The Measure should state that "need to know" personnel are determined by the registered entity. Similarly there is a suggested Measure that hardcopies of information be stored in a locked file cabinet with keys provided to only "authorized individuals". Recommendation: The Measure should

include language indicating that the registered entity identifies the “authorized individuals”.
No
Comments: CIP-011-1 Requirement 2.1: “Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was cleared prior to its reuse.” Recommendation: SDT should define what “cleared” means. The language in footnote #2 should be included in the wording of R2.1, to ensure it becomes part of the Requirement.
No
General Comments: 1. Applicability sections of CIP-002-5 through CIP-011-5: the Applicability sections should be consistent. Note that in CIP-005-5 and CIP-006-5 the Applicability sections 4.2.2 are different from the other CIP standards. We recommend that the drafting team adopt consistent Applicability language across all Version 5 CIPs. Alternatively, the drafting team should explain any Applicability variances between the various Version 5 CIPs. 2. CIP-006-5 Requirement 1, Guidance section on pp. 22 and 23 (Guidelines and Technical Basis): “While the focus is shifted from the definition and management of a completely enclosed “six-wall” boundary, it is expected in many instances this will remain a primary control for controlling, alerting and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems. … Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.” Comment: In reviewing CIP-006 – 5 we have seen that the “enclosed 6 wall” wording is removed, but it appears as though six walls are still required. The guidance section mentions that the Defined Physical Boundaries are allowed to have openings less than 96 square inches but does not exclude the need for 6 walls, only that they are not required to be completely enclosed (excerpt above). Is this correct? Would a window be considered an “opening,” to be protected by a barrier as noted in the guidance? The CIP wording could be read as requiring a ‘ceiling’ over open air substations in order to preclude exceeding the 96 sq. in. and 6-inch limits. We do not believe that this was the drafting team’s intent. What was the drafting team’s intent? Recommendations: We suggest that this matter be clarified by the addition of wording specifically allowing an exception from this requirement for open air substations, such as, “This requirement does not apply to open air substations” or “This wording is not intended to require placement of a roof over open air substations.” Alternatively, if it was the drafting teams’ intend to apply this requirement to open air substations, then would surrounding all BES Cyber Systems in six-walled enclosures within an open air substations meet the objective of this requirement? Clearly, a roof should not be required for and physically cannot be installed over all open air substations. 3. The use of the “Measures” column for each requirement is beneficial as are the guidelines of each CIP standard. Providing these as part of the standards can imply that they are part of the requirements. By this one could see that by meeting the measures for each requirement that will be in compliance. Also the guidelines provide much more information than the requirements. The requirements tell you to perform an assessment without specifics while the guidelines provide specifics. Are the guidelines to be read as requirements? For example, A Defined Physical Boundary is required, but it is not until the user reads the guidelines is there mention to it needing to be enclosed completely with limitations on the openings. The requirements call for a active vulnerability assessment and it is not until the guidelines that what should be in an assessment is provided.
Group
Salt River Project
Cynthia Oder
Yes
No
SRP agrees with the proposed criteria.
Yes
Please specify implementation timeline for the compliance of the newly identified and categorized BES Cyber Asset(s) and/or BES Cyber System(s).

Yes
Yes
Yes
Yes
Yes
SRP suggest removing "between reviews and" tp be consistent with the language in CIP-002-5 R2 and clarify that the time requirement is lined to the approval only.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
A clear definition of where encryption is needed for Remote Access needs to be provided, in particular where encryption needs to take place; e.g. at the source, from the source and the network to the access point, from the source to the network to the ESP, from the source all the way to the end-point, etc.
Yes
Yes
Yes
Yes

Yes
No
SRP suggests including language to specify this requirement is applicable only when technically feasible, consistent with the language in CIP-005-5 R2.
Yes
No
SRP suggests modifying the requirement to clarify if running antivirus on the transient device itself satisfies the requirement of malware protection and to specify this is required only when technically feasible (similar to language in CIP-005-5 R2).
No
SRP suggest modifying the requirement to allow for automated alerts to replace manual reviews or at least for the use of automated alerts to lengthen the time between manual sampling of the logs.
No
SRP suggests modifying the requirement to indicate that the implementation of all numeric two-factor authentication is acceptable.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
SRP suggests modifying the requirement to include the signoff from the Asset Owner and allow the Asset Owner to delegate this authority to the appropriate Manager.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Group
Luminant
Rick Terrill
Yes
The BES Cyber Asset definition states that “Redundancy shall not be considered when determining availability. Recommend clarifying as follows “Redundancy shall not be considered when determining classification as a BES Cyber Asset”..
Yes
The current Version 5 draft of the NERC CIP Cyber Security Standards will have a significant negative impact on the reliability of the ERCOT Bulk Electric System (BES). In particular, the Version 5 CIP Cyber Security Standards would severely inhibit the ability to restore the ERCOT grid in the event of a complete or partial system blackout. While Blackstart Resources in ERCOT today may be classified as Critical Assets, many do not have external Routable Protocol or Dial-up connections. Thus, they are not required to implement the current CIP-003-3 through CIP-009-3 requirements. The Medium Impact ranking proposed in the Version 5 draft of CIP-002 for Blackstart Resources would require implementation of a majority of the CIP Version 5 requirements for all Blackstart Resources regardless of the external routable connectivity considerations, and represents a step change in CIP compliance activities and costs. Typically, Blackstart Resources in ERCOT are older, smaller units with very low capacity factors and limited revenues. The application of the Medium Level CIP requirements will result in significant CIP investment and increased on-going operational costs as well as increased compliance risks. This will result in Generator Owners/Generator Operators not offering units for Blackstart service in the competitive ERCOT market. It would also likely result in Blackstart Resources not being maintained in a manner appropriate to support Blackstart service because of the additional on-going cost, thus removing them as a future option for providing Blackstart services. With fewer units being offered for Blackstart service, ERCOT may not have enough Blackstart Resources to effectively restore the ERCOT BES after a complete or partial system blackout event. Luminant recommends one of the following options for changing CIP-002-5, Attachment 1, to ensure the continued reliability of the ERCOT portion of the BES: 1) “2.4. Each Blackstart Resource with External Connectivity identified in its Transmission Operator's restoration plan.” This is the preferred option. Blackstart Resources with External Connectivity would still be in the Medium Impact category; however, those Blackstart Resources without External Connectivity would have less cyber risk and move to the Low Impact category. The Blackstart Resources in the Low Impact category would have the appropriate physical and cyber protection controls as listed in the current CIP Version 5 draft standard. Our understanding of CIP Version 5 draft standards is that External Connectivity is defined as having Routable or Dial-up connections through the Electronic Access Point. Thus, many ERCOT Blackstart Resources would not fit in the Medium Impact category. 2) Include a Regional Variance for ERCOT in CIP-002-5 similar to option 1 described above. This would limit the variance only to ERCOT and not be a comprehensive application to the industry. Also Attachment 1, section 2.13, creates ambiguity regarding the type of control center to which the rating applies. Recommend capitalizing Control Center to clarifiy that this applies to centralized command centers rather than plant operation control rooms.
No
The timeframe for updating should be changed to 60 days to allow for entities to train their staff to ensure common understanding, validate the modifications including basis, obtain reviews and approvals of documentation changes, and coordinate changes with third party entities.
Yes
No
The VSL table should refer to BES Cyber Assets and BES Cyber Systems (not just BES Cyber Assets) as does Requirement R1 for consistency with terminologies used in R.1 & R.2.

Yes
Yes
Yes
Yes
No
The Requirement and Measure are inconsistent in that the Requirement states delegation can be documented “by position or name of the delegate”, but the Measure indicates that evidence includes a document that includes the name of the individual to whom an authority has been delegated. Recommend removal of reference to individual names as documentation to that level significantly increases the administrative burden associated with this Requirement. Additionally, it is currently unclear if every approval within CIP-002 and CIP-004 – COP-011, and its subsequent delegations, must be documented individually. Strongly recommend indicating that a global delegation is acceptable.
Yes
No
The VSLs for R5 and R6 are too severe. The VSLs for these two requirements should start at the lowest level and follow the 5%/10%/15% guidance since the integrity of the Cyber Asset/Cyber system is not compromised by this violation. This violation is for an administration non compliance and not a violation that has a direct impact on the security controls and integrity of the Cyber Asset. Also, the term “delegate” should be changed to “delegate(s)” throughout this standard and all other CIP standards where appropriate. Language should be added to the VSLs to allow for a procedure based Roles and Responsibilities approach, including delegations, that does not require documentation of each delegation e. The procedures would pre-define those positions and the evidence should be consistent with the procedure requirements. This will avoid a documentation nightmare for delegation by person or positions every time a Senior Manger is not available.
Yes
Yes
Yes
Yes
Yes
No
Change the term “delegate” to “delegate(s)”. The SDT should add language to R6 to allow for self-identified and corrected administrative and documentation findings during quarterly or annual assessments/reviews. These should not be counted towards automatic violation of the standard since the discrepancy or non-compliance was self-identified, corrected by the entity.
Yes
No
Change the term “delegate” to “delegate(s)”. The SDT should add language to R6 to allow for self-identified and corrected administrative and documentation findings during quarterly or annual assessments/reviews. These should not be counted towards automatic violation of the standard since the discrepancy or non-compliance was self-identified, corrected by the entity.

Yes
No
The statement “Note that a user ID is not considered an authentication factor.” Implies that user ID/password is not a method of authentication. Recommend clarifying as follows: “Note that the combination of a User ID and its association Password is considered as one authentication factor. A User ID alone is not considered an authentication factor.”
Yes
No
We recommend removing the word “egress” from the Measures of 1.2 for Medium Impact assets. The program established access controls which are designed to restrict access. This should be sufficient for the Medium Impact category. We recommend removing the word “complimentary” from 1.3 since the requirements requires two or more physical controls. The words “and complementary…” is misleading and can be construed as requiring additional physical controls. For R1 overall, the SDT needs to include language that allows for deviations from the controls during CIP Exceptional Circumstances because there may be circumstances that require providing physical access control to individuals not on the authorized list.
No
For R2 overall, the SDT needs to include language that allows for deviations from the controls during CIP Exceptional Circumstances
Yes
Yes
Yes
No
It is not necessary to install Security Patches in all cases. A Security Patch when released should be assessed for BES Cyber Asset/System impact based on the configuration and external connectivity and other implemented security controls. Where remediation was deemed unnecessary, a documented justification with basis must be provided. It should be explicit in 2.2 that the plan could include not implementing the patch.
No
In Part 3.3, 30 days is not a reasonable time frame to assess, test, document, analyze, and implement a patch in a control system. We recommend 60 days as an appropriate time frame.
No
For R4.1 – the SDT should include “BES” just prior to “Cyber Security Incident” to correct the definition. Requirement 4.1.4 should be removed, as it is too broad and undefined. Recommend defining “Malicious Activity” as being one that has a direct adverse impact on the core functions of the BES Cyber Assets/Systems
No
In R5.1, it is not clear what is meant by “validate credentials”. We suggest the following language, “ Validate that users are authorized before granting electronic access to each BES Cyber System.”
No
The VSLs for R1 and R2 are too severe since there are other security controls that complement this control such as portable media control, physical access control, Training, etc. All these controls collective provide the necessary defense –in-depth based protection. We recommend a graduated approach starting with the Low VSL level. The way it is written, a failure to disable one port or the failure to install one patch or update in a timely manner would be a Severe VSL, while the actual potential impact to the BES is very limited.
Yes

No
We recommend changing the wording of R2.1 as follows, " When a Cyber Security Incident occurs, the incident response plans must be used (except in CIP Exceptional Circumstances) and include identification of any deviations from the plan during the incident or test.", because there may be circumstances that require deviating from the plan. Also, the words "and justifies" should be removed from the Measure for R2.1. In R2.2 the term "initially upon" should be changed to "prior to". If the standard is effective on January 1, 2015, it would be difficult to be in compliance if the initial test of the plan is not until January 1.
No
In R3.5, we recommend changing the word "Communicate" to "Distribute" and make the corresponding changes to the measures for better clarity.
Yes
No
R1.5 needs to be clarified that the retention period for raw event logs is no more than 90 days.
No
CIP-008-5 and CIP-009-5 appear to have similar type requirements, but the language is inconsistent between the standards. Where applicable, similar type language should be utilized in these two standards. Recovery Planning is a component of the Incident Response Planning for recovery, thus SDT must ensure consistency and seamless transition between these two (2) standards.
No
Change "initially" to "Prior to" in 3.1 . Also, CIP-008-5 and CIP-009-5 appear to have similar type requirements, but the language is inconsistent between the standards. Where applicable, similar type language should be utilized in these two standards. R3.5 should use the word Distribute, instead of Communicate.
Yes
No
We recommend the following changes to R1 and its subparts: 1) Add the term "intentionally installed" to 1.1.4 for better clarity since scripts are intentionally installed based on client requests 2) Language in the Requirement 1.2 section needs to be corrected as follows: "Document changes to the BES Cyber System that deviate from the existing baseline configuration, including the authorization by the CIP Senior Manager or delegate(s)." for better readability 3) 1.4.2 language should read – "Following the change verify that the required cyber security controls are in place, and the BES Cyber System is available, and" for better readability 4) 1.5 Language should read - "Prior to implementing any change in the production environment, except in CIP Exceptional Circumstances, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System in enough detail to verify and validate the integrity of the required cyber security controls." This change is necessary since there can be exceptional circumstances that may require implementing changes in the production environment without going first thru a test environment. In addition, the revised write-up provides clarity on what needs to be done.
No
We recommend the language in R2.1 should be changed to read, "…(as defined per CIP-010 R1, 1.1, excluding physical location)."because physical location is not a monitored logical parameter within a Cyber Asset/system.
No
We recommend changing the word "Initially" to "Prior to" in 3.1 and 3.2 for purposes of clarity. In section 3.1, the terms "security controls" and "controls" should both be changed to "required security controls" for clarity. We recommend changing the language in section 3.4 to be consistent with the language in CIP-011 section 1.3, as the language in CIP-011 is more clear.
Yes

No
In section 1.3, we recommend changing “Initially upon” to “Prior to” for purposes of clarity.
We recommend changing the language in section 2.2 to read “..shall destroy the media or take action…” The current sentence is lacking clarity and specificity.
No
The VSL for R2 in the high category should be rewritten to focus on the failure to purge the media or destroy the media prior to disposal, not a failure to precisely follow the prescribed process as the failure to destroy or purge the data is the core of the security risk. We suggest the following language, “The Responsible Entity has documented or implemented one or more media disposal or reuse processes to prevent the unauthorized retrieval of BES Cyber System Information from the media, but the Responsible Entity failed to purge or destroy the media prior to disposal.”
No
The minimum implementation time frame of 18 months is not sufficient. The timeframe for implementation should be extended in order to allow time for assessment, planning, budgeting and approval thereof, physical or logical modifications, development of new programs and procedures, including related training and full implementation of the requirements. With the additional requirements that include some activities at all generating facilities, there may be limited resources (both internal to companies and external third party resources) available to implement the requirements in this short duration. We recommend a minimum implementation period for CIP-002-5 of 12 months, and implementation for the remaining version 5 CIP standards for High and Medium Impact BES Cyber Systems at 24 months. Low Impact systems would be compliant within 36 months.
Group
City of Garland
Ronnie Hoeinghaus
Yes
“Cyber Asset” – should not include any portable memory devices such as USB memory devices, CDs, etc. “BES Cyber Security Incident” should read as follows: A malicious act that: • Compromises a BES Cyber System or BES Cyber Asset, or • Disrupts the operation of a BES Cyber System or BES Cyber Asset, or • Results in unauthorized physical access into a Defined Physical Boundary. “BES Cyber System Information” should include only floor plans, diagrams, equipment layouts, etc. that clearly delineate the cyber assets in some way. In other words, if the diagram denotes a device as a “Schweitzer” relay (or even an “SEL 2030”), the information should not require special treatment. “BES Reliability Operating Services” should be clarified so that the CIP Auditor does not feel licensed or obligated to perform a “693” audit – there are many opportunities as written for the CIP Auditor to “branch out” into areas that have nothing to do with Cyber Security. There are ample 693 standards and 693 auditors for those standards.
Yes
The addition of a “Low Impact” rating for every generation facility that does not meet the High or Medium Impact thresholds constitutes a significant change in the CIP Standards. This change forces every registered GO and GOP to adhere to approximately 40 requirements in the remaining CIP standards when, currently, those generators are not listed as Critical Assets. It seems unlikely that the cost to adapt existing corporate cyber security policies, cyber security awareness and cyber asset access management to these NERC CIP requirements will lead to a corresponding reliability benefit.
No
The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is too complicated. In addition to the BES Cyber Assets classified as high, medium and low in CIP-002, the other standards introduce ten additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some appear in the standards

themselves and these categories may or may not be included in the definitions document. This approach is complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future interpretations, CANs, etc. The Standards should be revised so that CIP-002 defines all assets needing protection rather than being introduced throughout the Standards.
No
Consider rewording so that the initial identification and categorization required by R1 is no later than the effective date and updated once each calendar year.
No
This should not apply to visitors – should read “shall make individuals who have authorized unescorted access…”
No
Change 30 days to 90 days
No
Need lower and moderate VSLs
No
Table Part 1.1 - Strike the “Security Awareness Program” from Requirement and Measures. So long as the Registered Entity provides security awareness quarterly, the program adds no value and is merely another “compliance document” to maintain, review, update, etc.
No
Language in the table seems to require training on network connectivity for anyone with access to High and Medium BESCS. For some categories of users (e.g., Operators) this will be both out of context and irrelevant. For some categories (e.g., Network administrators) this will be unnecessary. Recommendation is to strike item 2.10. Providing training on “physical access controls” is not necessary. The physical access controls are – generally – pretty straightforward (e.g. card key readers). It does not seem necessary to provide “training” on how to use a card key. The same can be said for training on electronic access controls. Most of those access controls merely involve two-factor authentication or something similar. The need to provide “training” on how to log on to devices is unnecessary. Strike R2.3 and R2.4 because they appear redundant to R2.2; alternatively, some explanation of the difference between R2.2 and R2.3/R2.4 should be provided. With respect to R2.8, it seems unnecessary to require training on recovery plans except for those very few employees who must implement the recovery plan. As currently worded, it is not clear whether only those who implement recovery plans must receive training.
No
Table Part 4.2 - too prescriptive - residency and educational history is not revelant to a criminal history - current 7 year criminal check is sufficient - if language remains, add language to “grandfather” previous seven-year criminal checks executed for the previous version of the CIP Standards. The additional language should spell out when this “grandfathering” expires (which will be when a new check is required).
No
Table Part 5.2 Add language to “grandfather” previous seven-year criminal checks executed for the previous version of the CIP Standards. The additional language should spell out when this “grandfathering” expires (which will be when a new check is required). For clarity, recommend changing 5.1 from "authorized electronic or unescorted physical" to "authorized electronic or authorized unescorted physical"
No
The CIP Senior Manager should not be the person that authorizes access in Table Part 6.1, 6.2, 6.3 –

this should be up to the Responsible Entity's business process owner
No
Table Part 7.1 It is impossible to always revoke access upon the termination date or resignations in the cases where OEMs are involved. We cannot enforce this in 3rd party companies. Additionally, it is impossible to change locking mechanisms in remote substations that are spread across large geographical regions. Table Part 7.2 While this may work in a control center, it is not practical or reasonable in transmission substation settings, particularly for devices that are not remotely connected. Please Note: Promoting someone or transferring someone does not make that person a security risk and should not be treated as such.
No
need lower and moderate VSLs
No
Table Part 1.5 IDS should not be required - a firewall should be sufficient. Should clarify requirements for low, medium, high impact BES Cyber Systems
No
Table 2 Part 2.3 – remove this statement from measures "Note that a UserID is not considered an authentication factor." "Associated Protected Assets" needs to be defined
No
Should have lower and moderate VSLS – not just higher & severe
No
Table 1 – Strike "egress" from measures – egress is not stated in the requirement Table 1 Part 1.6 - vague and needs to be clarified
No
Table 2 Part 2..2 – logs should be kept for 1 year – for a 6 year audit cycle, 6 years is too long to be required to keep logs – requirement should clearly state that the logs may be destroyed after 1 year so that an auditor will not ask for 1 year's worth of logs on a date 6 years ago to prove that the entity was compliant with 1 year of logs on that date
No
Table 1 Part 1.1 – Need provision for TFE Table 1 Part 1.1 indicates that the requirement is applicable to "systems", but measure focuses on "assets". Need a system approach if this requirement is intended to be applied at a broader level. The term "BES Cyber Asset" should be removed from measure if the requirement can be applied to "system". Table 1 Part 1.2 – Need provision for TFE
No
Table 2 Part 2.1 – remove comma after the word "patches," - the comma in the sentence requires that all software patches be included whether they are security related or not. Additionally, it is not practical to include firmware as very few vendors post when firmware updates become available Table 2 Part 2.2 – requires a "remediation plan" – if the patch is applied, there is no reason to require a "remediation plan" – should be reworded or struck
No
Table 3 Part 3.3 – needs to define when the 30 days start – when the EMS vendor says it can be applied or when the virus definition manufacturer says it is available. Additionally, needs provision for TFE in case the virus definition kills the application. Table 3 Part 3.4 – measure is too prescriptive for the requirement Table 3 Part 3.5 – should not apply to USB memory devices – if it does, requirement should be struck as this would be extremely burdensome.
No
Table 4 Part 4.1 – Although this may be practical for PCs, many substation devices do not have any logging capability at all – needs provision for TFE Table 4 Part 4.1.1 – Electronic Access Points should be addressed under CIP-005 Table 4 Part 4.1.4 – use of the word "potential" is vague and is not auditable Table 4 Part 4.3 – strike "before the end of the next calendar day" – end sentence with "failures" Table 4 Part 4.5 – strike 4.5 completely – it is a duplication of 4.2 and 4.3
No

Part 5.2, the CIP Senior Manager or delegate should not have to authorize the use of administrator, shared, default, and other generic account types. The “owner” of the asset (e.g. the SCADA/EMS manager) should be able to authorize the use of such accounts. [We realize that, under the Standard, the CIP Sr. Mgr. can delegate the responsibility to someone else. However, doing so simply creates another document (the delegation) to maintain, review, revise, etc. It makes more sense to just let the asset owner authorize the use.]
No
should have lower and moderate VSLs
No
No
Table 2.1 – strike deviation language from requirement – “lessons learned” exercise after the incident will be sufficient. Additionally, allowances need to be made in the requirement for the entity to deviate from “the plan” if circumstances call for a deviation without being penalized by the auditors. “Emergencies” or “Disasters” exist because something in everyday business life did not go as planned – requirements should allow for responses to be flexible to handle the unforeseen
No
Table 3 Part 3.1 – Consider rewording so that the initial incident response plan implementation is no later than the effective date and updated once each calendar year. Table 3 Part 3.4 – change from 30 days to 60 days
No
should have lower and moderate VSLs
No
Should state that ‘reconstitution of site is not required’ Table 1 Part 1.5 – should be struck completely – preservation of forensic evidence should never take priority over the restoration of the BES
No
Consider rewording so that the recovery plan implementation is no later than the effective date and updated once each calendar year. Table 2 Part 2.2 – remove the word “any” from the requirement Table 2 Part 2.3 – should be struck as it is a duplication of 2.1 – problems with 2.3 as written are what constitutes a full operational test of the plan – is it sufficient to reload one server or one workstation or replace a card in a computer? Additionally, if there are 4 scenarios written in the plan, do you have to do an operational test of each scenario?
No
Consider rewording so that the recovery plan implementation is no later than the effective date and updated once each calendar year. Table 3 Part 3.4 – change from 30 days to 60 days
No
should have lower and moderate VSLs
No
Table 1 Part 1.1.4 – strike completely - entirely too prescriptive – base line should not go beyond information from what a standard vulnerability scan application can provide Table 1 Part 1.2 – strike CIP Senior Manager – this should be a business function covered by the change management process Table 1 Part 1.4.2 – strike “availability” – “availability” is a business function, not a security function – question – if you make 40 changes in a year and “availability” goes down 1% (if you can determine that), how do you verify Table 1 Part 1.5 – strike completely – it is a duplication of 1.4 regardless of whether the change involves a control center or not
No
Table 2 Part 2.1 – strike completely – CIP-007 requirements are sufficient
No
Consider rewording so that the implementation is no later than the effective date. Table 3 Part 3.2 – strike completely – 3.1 should be sufficient
No
should have lower and moderate VSLs

No
Consider rewording so that the implementation is no later than the effective date
No
should have lower and moderate VSLs
Yes
Group
Corporate Compliance
Summer C. Esquerre
Yes
a. BES Cyber Asset – The sentence, “This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services” makes the definition more confusing. This is a suggestion to improve the definition: BES Cyber Asset - A Cyber Asset that is currently in operation if rendered unavailable, degraded, or misused would impact one or more BES Reliability Operating Services within 15 minutes. The 15-minute timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. b. The effective dates says the following: "18 Months Minimum – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan." This seems to state that CIP 002 - 009 Version 4 is never going to be implemented, this is confusing. It would be better to state: " 18 Months Minimum – The Version 5 CIP Cyber Security Standards (including CIP 010-1 and 011-1) shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. In the event CIP-002-4 through CIP-009-4 do not become effective, CIP-002-3 through CIP-009-3 will remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan." c. In the definition for a BES Cyber Asset it states: "A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services." The term "adversely impact" needs to be further defined, this seems to basically result in the same lack of clarity that resulted in the need to have versions 4 and 5 to ensure assets where identified as critical.
Yes
Attachment 1 does not indicate if these rules apply to non-dispatchable units (i.e. wind, solar, etc.), this should be defined. For Items 1.4 – Control Centers, 2.1 – Generation greater than 1500 MW, 2.3 – Generators designated by the Planning Coordinator and 2.4 Blackstart units, the definition of BES Cyber System that can impact BES Reliability Operating Services would force the inclusion of RTU’s, Governors, Power System Stabilizers and Protective Relaying. Item 2.1 - Need to better define what the phrase “adversely impact” means, i.e. if you have to lose all 1500 MW as defined under item 2.1 to result in an adverse impact Item 2.11 addresses Special Protection Systems (SPS), need to define if this includes SPSs which are associated with Generation sites. Item 2.12 - Under Frequency Load Shedding of 300 MW or more required by the regional load shedding program. Currently NPCC and RFC are seeking approval for their UFLS programs which would require generators who trip above the regional UFLS curve to independently arrange with the local DP for the equivalent amount of UFLS MW’s. While we have not yet evaluated our plants in NPCC and RFC, if they cannot meet the proposed UFLS curves, they would be pushed up into a Medium Impact Rating. Item 2.2 the former version had BES in front of Reactive Resource. The BES should be restored to make clear that this is transmission level as stated in the application notes. Item 2.3 uses the phrase “long-term planning horizon” which is later defined as one-year or longer, it would be better if the time horizon was defined with a number of years, otherwise it would be hard to have it audited. Item 2.3 uses the phrase “long-term

planning horizon" which is later defined as one-year or longer, it would be better if the time horizon was defined with a number of years, otherwise it would be hard to have it audited. Item 3 does not provide a minimum site MWs or interconnection voltage, would recommend nameplate rating greater than 20 MVA or gross plant/facility aggregate nameplate rating greater than 75 MVA including the generator terminals through the high side of the step-up transformer(s) connected at a voltage of 100 kV or above. This is in line with the Bulk Electric System (BES) definition developed under NERC Project 2010-17 Definition of the Bulk Electric System. Overall, the new rules are ripe for confusion. If the need was to ensure that the definition for what assets fell under the requirements, changing the definitions on what Cyber Assets are to be protected has no relation to this goal. It would seem to make more sense to define the Physical assets in the Bulk Electrical System (BES) which have potential to negatively impact the BES, then define how to protect Cyber Assets that are potentially open to external access, protecting them from internal assault through physical and logical access controls. The proposed definitions should return to Critical Assets and the Critical Cyber Assets at these sites would then be defined as: Critical Cyber Asset Identification— Using the list of Critical Assets developed pursuant to Requirement R1; the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. Critical Cyber Assets are qualified to be those having at least one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.

No

a. CIP-002-5 R1.1 which states "Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category" implies that the process to identify or categorization of the BES Cyber Assets or BES Cyber Systems is constantly being performed by the Responsible Entity – as stated in the rationale for R1 "…configuration of the BES is subject to changes due to new demands and requirements for Bulk Power and to environmental changes and operational events. When changes to the BES are planned, the effect of these changes on the set of identified and categorized BES Cyber Assets and BES Cyber Systems must be analyzed to ensure that the adequate level of protection is still applied to them." To ensure that every configuration change of the BES is fully accounted for with regards to the identification or categorization of the BES Cyber Assets or BES Cyber Systems, CIP-002-5 R1.1 as drafted requires that the process to identify or categorization of the BES Cyber Assets or BES Cyber Systems is required to be performed with 30 calendar days of the configuration change of the BES. This is burdensome as every configuration change of the BES needs to be tracked, dated, and evidence of the process to identify or categorization of the BES Cyber Assets or BES Cyber Systems be documented. An alternative method should be considered – for example, when planning studies reveal that the configuration change of the BES is material, they it would trigger the process to identify or categorization of the BES Cyber Assets or BES Cyber Systems. This will then start the 30 day window as stated in CIP-002-5 R1.1. b. Need to add discrete identification of Low Impact BES Cyber Assets or BES Cyber Systems, you are going to have to review each based upon Attachment 1 criteria; this will be the way to demonstrate compliance in a manner that is auditable. General Comment: In the background section of CIP-002 (specifically CIP-002 page 7), there is reference to being able to group Cyber Assets. The example provided refers to applying requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets. So it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply. It is unclear what this means exactly and what the overall benefit. Overall Comment related to the Background and Application Guidelines included in each of the Standards, it is unclear what the applicability is related to these sections. From a compliance perspective will Registered Entities will potentially be penalized for not following the sections from the EROs since they are not included within the Standard and do not serve as the Standard's requirements, but is additional material for the EROs to use to determine compliance. Recommend either including specific language from the guidelines as applicable to address FERC Order 706 and cyber security or removing from future versions of the draft standards.

No

a. To add clarity to CIP-002-5 R2, any change in the identification or categorization of the BES Cyber

Assets or BES Cyber Systems in between the “once each calendar year” review/approval of the CIP Senior Manager or delegate does not require the CIP Senior Manager or delegate approval. b. It would be easier to ensure compliance if the requirement to review the list on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders
No
FPL disagrees with the fundamental requirement to perform a review upon a change to the BES and therefore disagrees with the associated VSL associated with this requirement. See response to question 3
No
To add clarity to CIP-003-5 R1, CIP Senior Manager delegate that has the ability to approve Cyber Security Policy required in CIP-003-5 R3 shall also be identified by name. This will ensure that there is clear delegation of authority and ownership for the CIP program within an organization.
No
May need to look at the topics stated as they seem to be redundant – need to look at the overall structure of the CIP V5 standards
No
a. The CIP Senior Manager delegate may also review each of its cyber security policies and provide the approval. This is a suggestion to improve CIP-003-5 R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager or delegate, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals. Also, any change in the Responsible Entity’s cyber security policies in between the “once each calendar year” review/approval of the CIP Senior Manager or delegate does not require the CIP Senior Manager or delegate approval. b.It would be easier to ensure compliance if the requirement to review the list on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders.
Yes
No
a. The CIP Senior Manager should also be able to delegate the authority for any approvals and authorizations required in the CIP standards including the approval of the Cyber Security Policy required in CIP-003-5 R3. This is a matter of efficiency and does not detract from the intent of “clear lines of authority and ownership for security matters.” b. This will be difficult to manage in a large organization and provides no value. Just have the Senior Manager appoint any delegates for his role, then identify a Compliance Manager who will sign the appropriate documentation in their area.
Yes
Yes
Yes
No
a. In Part 2.1 under “Requirements” change “Define the roles that require training” to “ dentify each role and specify training required for each role.” The statement “Define the roles that require training” implies that some roles do not require training. b. The “Applicability” stated in CIP-004-5 Table R2 – Cyber Security Training Program and CIP-004-5 Table R3 - Cyber Security Training are inconsistent. CIP-004-5 Table R2 – Cyber Security Training Program has High Impact BES Cyber Systems and Medium Impact BES Cyber Systems listed whereas CIP-004-5 Table R3 - Cyber Security Training has High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets listed. CIP-004-5 R2 and CIP-004-5 R3 need to be consistent.
No

a. The “Applicability” stated in CIP-004-5 Table R2 – Cyber Security Training Program and CIP-004-5 Table R3 - Cyber Security Training are inconsistent. CIP-004-5 Table R2 – Cyber Security Training Program has High Impact BES Cyber Systems and Medium Impact BES Cyber Systems listed whereas CIP-004-5 Table R3 - Cyber Security Training has High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets listed. CIP-004-5 R2 and CIP-004-5 R3 need to be consistent. CIP 005-5 R1.1 includes Low Impact BES Cyber Systems with External Routable Connectivity and requires restriction of unauthorized electronic access. CIP 006-5 includes Low Impact BES Cyber Systems requires that you need to restrict physical access. These two requirements mean you have to define who can have access and the requirements for authorized access; it would make sense to include training on cyber security as part of the requirements to have authorized access. b. In order to add clarity to the role-based nature of the cyber security training program, suggest rewording CIP-004-5 R3 to: Each Responsible Entity shall implement its documented role-based cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training. This is to emphasize that the training is geared towards the individual’s role when the individual requires authorized electronic or unescorted physical access to each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program. 3.2 states Cyber Security Training must be done at least once every calendar year, but not to exceed 15 calendar months. It would be easier to ensure compliance if the requirement to complete the training on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders. c. If the individual’s role is changed from one role to another as defined in CIP-004-5 R2 Part 2.1, the Responsible Entity needs to show evidence that the training was completed within 30 days of the change of role. This is not currently in CIP-004-5 R3 and needs to be explicitly required to ensure proper role-based cyber security training is provided to individuals requiring authorized electronic or unescorted physical access to each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program. d. If the role definition as documented in CIP-004-5 R2 Part 2.1 changed (i. e., a defined role has its specific training requirement changed), for every individual whose role definition changed the Responsible Entity needs to show evidence that the training was completed within 30 days of the change of role definition. This is not currently in CIP-004-5 R3 and needs to be explicitly required to ensure proper role-based cyber security training is provided to individuals requiring authorized electronic or unescorted physical access to each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.
No
a. The “Applicability” stated in CIP-004-5 Table R4 – Personnel Risk Assessment Program and CIP-004-5 Table R5 – Personnel Risk Assessment are inconsistent. CIP-004-5 Table R4 – Personnel Risk Assessment Program has High Impact BES Cyber Systems and Medium Impact BES Cyber Systems listed whereas CIP-004-5 Table R5 – Personnel Risk Assessment has High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets listed. CIP-004-5 R2 and CIP-004-5 R3 need to be consistent. b. CIP 005-5 R1.1 includes Low Impact BES Cyber Systems with External Routable Connectivity and requires restriction of unauthorized electronic access. CIP 006-5 includes Low Impact BES Cyber Systems requires that you need to restrict physical access. These two requirements mean you have to define who can have access and the requirements for authorized access; it would make sense to include a Personal Risk Assessment (PRA) as part of the requirements to have authorized access.
No
a. The “Applicability” stated in CIP-004-5 Table R4 – Personnel Risk Assessment Program and CIP-004-5 Table R5 – Personnel Risk Assessment are inconsistent. CIP-004-5 Table R4 – Personnel Risk Assessment Program has High Impact BES Cyber Systems and Medium Impact BES Cyber Systems listed whereas CIP-004-5 Table R5 – Personnel Risk Assessment has High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets listed. CIP-004-5 R2 and CIP-004-5 R3 need to be consistent. b. CIP 005-5 R1.1 includes Low Impact BES Cyber Systems with External Routable Connectivity and requires restriction of unauthorized electronic access. CIP 006-5 includes Low Impact BES Cyber Systems requires that you need to restrict physical access. These two requirements mean you have to define who can have access and the requirements

for authorized access; it would make sense to include a Personal Risk Assessment (PRA) as part of the requirements to have authorized access
No
a. The requirement states that it is only valid, including in its parts, for Medium and High Impact BES Cyber Systems, as well as Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets. CIP 005-5 R1.1 includes Low Impact BES Cyber Systems with External Routable Connectivity and requires restriction of unauthorized electronic access. CIP 006-5 includes Low Impact BES Cyber Systems requires that you need to restrict physical access. These two requirements mean you have to define who can have access and the requirements for authorized access; it would make sense to include them in the Access Management Program as part of the requirements to have authorized access. b. In Part 6.2 under “Requirements” the wording should be changed from “The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.” to “The CIP Senior Manager or delegate shall authorize unescorted physical access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.” The phrase “to BES Cyber Systems” is inconsistent the list of systems/assets listed in Part 6.2 under “Applicability” (High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets). c. In Part 6.4 under “Requirements” the wording should be changed from “Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.” to “The CIP Senior Manager or delegate shall verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access were authorized for such access.” The phrase “to BES Cyber Systems” is inconsistent the list of systems/assets listed in Part 6.4 under “Applicability” (High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets). Also specifying the CIP Senior Manager or delegate removes the vagueness of who is required to review and approve the quarterly review. d. In Part 6.5 under “Requirements” the wording should be changed from “Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.” to “The CIP Senior Manager or delegate shall verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.” Specifying the CIP Senior Manager or delegate removes the vagueness of who is required to review and approve the “once each calendar year” review. e. In Part 6.6 under “Requirements” the wording should be changed from “Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.” to “The CIP Senior Manager or delegate shall verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.” Specifying the CIP Senior Manager or delegate removes the vagueness of who is required to review and approve the “once each calendar year” review. f. This is the first requirement in CIP-004-5 R6 that mentions access to BES Cyber System Information to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.3) – access to BES Cyber System Information did not require any role-based cyber security training program (per CIP-004-5 R2 and CIP-004-5 R3) nor one or more documented personnel risk assessment programs (per CIP-004-5 R4 and CIP-004-5 R5) – is this the intent of CIP-004-5 R6? g. To clarify for Part 6.1, CIP Senior Manager delegates allowed to authorize electronic access to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.1) need not be identified by name. CIP Senior Manager delegates allowed to authorize electronic access to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring

Systems, and Associated Protected Cyber Assets (as stated in Part 6.1) need only be identified by their position and necessary description of their authority to grant such access as part of the Responsible Entity's BES Cyber Systems access provisioning program. h. To clarify for Part 6.2, CIP Senior Manager delegates allowed to authorize unescorted physical access to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.2) need not be identified by name. CIP Senior Manager delegates allowed to authorize unescorted physical access to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.2) need only be identified by their position and necessary description of their authority to grant such access as part of the Responsible Entity's BES Cyber Systems access provisioning program. i. To clarify for Part 6.3, CIP Senior Manager delegates allowed to authorize access to BES Cyber System Information to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.3) need not be identified by name. CIP Senior Manager delegates allowed to authorize access to BES Cyber System Information to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.3) need only be identified by their position and necessary description of their authority to grant such access as part of the Responsible Entity's BES Cyber Systems access provisioning program. j. 6.5 states verification that all accounts/account groups or role categories and their specific associated privileges are correct and the minimum necessary for performing assigned work functions must be done at least once every calendar year, but not to exceed 15 calendar months. It would be easier to ensure compliance if the requirement to complete the training on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders k. 6.6 states verification of access privileges to BES Cyber Systems Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions must be done at least once every calendar year, but not to exceed 15 calendar months. It would be easier to ensure compliance if the requirement to complete the training on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders.
No
a. The requirement states that it is only valid, including in its parts, for Medium and High Impact BES Cyber Systems, as well as Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets. CIP 005-5 R1.1 includes Low Impact BES Cyber Systems with External Routable Connectivity and requires restriction of unauthorized electronic access. CIP 006-5 includes Low Impact BES Cyber Systems requires that you need to restrict physical access. These two requirements mean you have to define who can have access and the requirements for authorized access; it would make sense to include them in the Access Management Program as part of the requirements to have authorized access. b. By not specifying the amount of time to revoke access in Part 7.1 and relying on the Responsible Entity's judgment and interpretation of what constitutes the time element or meaning of the phrase "at the time of the resignation or termination" would result in various interpretations by auditors during a CIP spot check. Does this mean good faith effort by the Responsible Entity? If the intent is for "immediate revocation", we suggest clarifying Part 7.1 to state "For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access at the time of the resignation or termination during the same calendar day of the individual's resignation or termination. In extenuating circumstances that the revocation is not possible during the same calendar day, document the extenuating circumstances and revoke access as soon as possible. The documentation of the extenuating circumstances shall be signed by the CIP Senior Manager or delegate." By specifying the "the same calendar day", it will clarify the expectation that the revocation of the individual's unescorted physical access and Interactive Remote Access is performed immediately (and at most, within same calendar day) as recorded by the Responsible Entity. A provision to allow for documentation for "extenuating circumstances" is also included but would require a signature from the CIP Senior Manager or delegate; an example of an extenuating circumstance is that the time of revocation is close to the end of the calendar day (e. g., 11:55 pm) and revocation could not be completed by the same calendar day – this instance could be deemed as a valid extenuating circumstance. Please take note that the proposed rewording removed the phrase "to BES Cyber

Systems” since it is consistent with the “Applicability” column. The phrase “to BES Cyber Systems” is inconsistent the list of systems/assets listed in Part 7.1 under “Applicability” (High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets) c. Since the individual may change roles or that roles may be modified but may still require some form of electronic access or unescorted physical access, we suggest rewording of Part 7.2 to “For reassignments, transfers, role changes, or role modifications, revoke the individual’s unneeded electronic and/or unneeded physical access by the end of the next calendar day. Please take note that the proposed rewording removed the phrase “to BES Cyber Systems” since it is consistent with the “Applicability” column. The phrase “to BES Cyber Systems” is inconsistent the list of systems/assets listed in Part 7.2 under “Applicability” (High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets). The “and/or” for unneeded electronic access and unneeded electronic access covers all possibilities/combinations of the individual’s current access. d. There should also be a table entry (i. e., an additional part in CIP-004-5 R7 in the CIP-004-5 Table R7 – Access Revocation table) “For reassignments, transfers, role changes, or role modifications, revoke the individual’s unneeded access to BES Cyber System Information by the end of the next calendar day.” An individual’s access to BES Cyber System Information due to reassignments, transfers, role changes, or role modifications may need to be modified.
Yes
No
a. The requirement R1.1 states "Define technical or procedural controls to restrict unauthorized electronic access," yet the measures for the requirement states "Evidence may include, but is not limited to, documented technical and procedural controls that exist and have been implemented." These two are mutually exclusive; the requirement being "technical or procedural controls" yet the measure indicates you have to have "technical and procedural controls." Recommend both say "technical or procedural controls." b. Part 1.1 We recommend rewording the requirement to better align with Applicability and Change in Rationale: Define technical or procedural controls to restrict unauthorized interactive remote access c. Part 1.2 (Page 11) Applies to Associated Physical Access Control Systems – Requirement says “control and secure all routable and dial up connectivity through the use of identified EAPs” – Does this mean we will need to consider the whitefloor firewalls as an EAP? Although that is not the definition of an EAP, how will this work with our current architecture (i.e., Picture Perfect being a PAC sitting on the whitefloor)? d. R1.3 Are comments and explanations besides the rules sufficient to satisfy the requirement, also can there be a definition of what “explicit criteria” means. e. Part 1.4 Definition of interactive / non-interactive access is not clear. Definition should be added to the Definition of Terms. f. Requirement R1.5 states "A documented method for detecting malicious communications at each EAP" yet the Change Rationale states "The Order makes clear this is not simple redundancy of firewalls, thus the drafting team has decided to add the security measure of malicious traffic inspection (intrusion detection systems / intrusion protection systems) a requirement for these ESPs." If that is the case, why not just have the requirement state so for clarity. g. R1.5: The wording is too vague, measures and rational don’t match, suggest breaking down the requirement to specify what needs to be done for detecting malicious communication, i.e using AV, IDS, etc. h. Part 1.5 does not define the term “malicious”. A definition is needed to avoid interpretation.
a. Part 1.2 (Page 11) Applies to Associated Physical Access Control Systems – Requirement says “control and secure all routable and dial up connectivity through the use of identified EAPs” – Does this mean we will need to consider the whitefloor firewalls as an EAP? Although that is not the definition of an EAP, how will this work with our current architecture (i.e., Picture Perfect being a PAC sitting on the whitefloor)? b. R1.3 Are comments and explanations besides the rules sufficient to satisfy the requirement, also can there be a definition of what “explicit criteria” means. c. Requirement R2.1 states "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." It would seem a firewall or router meets this requirement, but we do not believe that is what was discussed in "Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3" document. Recommend that requirement state directly that the Electronic Access Point (EAP) does not meet this requirement. d. Requirement R2.2 states "Require encryption for all Interactive Remote Access

sessions to protect the confidentiality and integrity of each Interactive Remote Access session." Does that mean encryption is required only between the Intermediate Device and the EAP to the BES Cyber System or Protected Cyber Assets, or does it include the connection between the Cyber Asset being used to conduct remote access and the Intermediate Device? Recommend that this requirement be clarified as to the above and recommend it does not include the connection between the Remote Cyber Access and the Intermediate Device. e. Part 2.2 – clarification is needed where encryption is required. Is encryption needed from the intermediate asset to the BES Cyber Systems or Protected Cyber assets? Since, in many applications, it may not be technically feasible to implement encryption between intermediate device and BES Cyber Asset, we propose rewording requirement to: f. Require encryption between remote Cyber Asset and intermediate device for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session. g. Part 2.3 – multi factor authentication is used interchangeably with two-factor, should standardize on one. Term not defined in the Definition of Terms.
No
Suggestion to propose a fine monetary estimation for each VSL and establish a guideline regarding the how fines are determined, as it correlates to the number of devices with the PV, the exposure, the mitigations, and risk factor to the BES.
No
a. Requirement R1.1 requirement states "Define operational or procedural controls to restrict physical access" yet the measures for the requirement states "Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented." Recommend this be clarified, using "operational or procedural controls." b. R1.1 not specific enough in regards to what kind of physical controls need to be limited to restrict access. CIP-006-5 R1.1 Entity based Operational or procedural controls to restrict physical access – To allow for programmatic protection controls as a baseline for Low Impact BES Cyber Assets and Physical Access Control Systems. This does not require detailed lists of individuals with access. c. Part 1.1, 1.2 – We recommend that Associated Physical Access Control Systems are moved from requirement 1.1 to 1.2 in order to better align with the remaining CIP standards; for instance, the access management requirements in CIP-004. d. Requirement R1.3 states "Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible." Clarify if the statement means that a Technical Feasibility Exception (TFE) can be filed for this (give scenarios in the guidance where it would apply). e. Part 1.6 - Does log entry only require date or is time also required. If time is required, then it should be added. Since the concept of a “visit” is used for visitors, is the same concept used for the personnel with access? (see Part 2.2) f. The requirement does not state if you must protect cabling between Defined Physical Boundaries, please clarify. g. Deletion of identification of physical access points h. “Appropriate” use of access controls is part of CIP-004-5 2.3 i. Defense in depth needs to be moved out of the guidance section and into the requirement j. Definition of an access point needs to be added to the requirement: “Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.”
No
a. Requirements R2.1 and R2.2 do not mention Associated Physical Access Control Systems under Applicability, does this mean that they cannot be accessed by visitors or that they can. Recommend that Associated Physical Access Control Systems be included under Applicability section for both. b. Part 2.1 continuous escort is not defined. Requirements of a continuous escort should be clearly stated.
No
Part 3.2 (Page 18) – If the intention is to have a process underneath this to mitigate the risks when outages occur, recommend explicitly stating this in the requirement. There is further guidance in the end of the CIP but this should be included and a measure developed.
Yes
No

a. R1.2 states under Applicability that it is only applicable to "High Impact BES Cyber Systems" and "Medium Impact BES Cyber Systems at Control Centers." Based on what you are trying to accomplish, it would make sense to include "Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, as well as any "Medium Impact BES Cyber Systems." b. R1.2: Applicability – Change “Medium Impact BES Cyber Systems at Control Centers” to “Medium Impact BES Cyber Systems” c. The requirement does not address services that are not required for operation, this will potentially allow a major vulnerability, recommend services be added to R1.1 d. Table R1 – Ports and Services e. R1.1 – Requirements – Content Change i. Original Content - Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. ii. Proposed Change – Enable only logical accessible ports needed for normal and emergency operation, including port ranges where required. f. Rationale – The proposed language incorporates much of the legacy (CIP-007-3 R2.1) language. The additional requirement to document the need for remaining logical ports extends beyond what FERC requests within order 706 without adding security benefits. g. We see this as being applicable and valid for logical ports and services however disabling connectivity to all physical ports on devices such as servers within the applicable compliance areas could be cost prohibitive. Additionally this is mitigated by physical security controls preventing access to the physical devices. h. CIP-007-5 Table R1 – Ports and Services Part 1.1 Measures: Required evidence includes “screen shots” showing accessible ports. Screen shots are only one method to show evidence and requirement should not be so prescriptive. Evidence could be a listing or a report created from a database of ports. Some systems are not capable of capturing screen shots. i. CIP-007-5 Table R1 – Ports and Services Part 1.2 Measures: Same comment as above.

No

a. Table R2 – Security Patch Management b. R2.1: Requirements – Content Change i.Original Content - Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. ii.Proposed Change - Identify a source or sources that are monitored for the release of security related patches, or security related updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. c. R2.2: Requirements – Content Change i.Original Content – Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe. ii.Proposed Change – Identify applicable security-related patches or security related updates from the identified source that addresses the vulnerabilities within a defined timeframe within 30 days of release and create a remediation plan, or revise an existing remediation plan, within 60 days of release, unless the patch has been installed within 60 days of release. d. Part 2.3 (Page 14) – How will we prove compliance with this in the event that after the assessment, we decide that a patch will not be implemented due to the existence of mitigating controls? There will not be a remediation plan if the mitigating controls are already in existence and there will be no implementation logs. e. Requirement 2.3 states "A process for remediation, including any exceptions for CIP Exceptional Circumstances" as a requirement. Recommend that the term CIP Exceptional Circumstances be defined in the requirement. f. Part 2.3 (Page 15) – In the change rationale, is this implying that we now have to assess and implement within 30 days of release date? What is the beginning point for this 30 day window g. Throughout CIP-007-5 Table R2 – Security Patch Management Part 2.1 and 2.2: FPL does not agree with phrase “hotfixes and/or updates. The intent is to monitor for security vulnerabilities and this implies that CIP-007-5 R2 must be applied for software fixes and enhancements. Hotfixes and/or updates should only apply to this standard when hotfixes and/or updates contain security patches. h. CIP-007-5 Table R2 – Security Patch Management Part 2.3 does not have a timeframe associated with the requirement, yet the “rationale” states that a 30 day window has been given to complete the documentation. We recommend modifying the requirement to read: i. A process for remediation, including any exceptions for CIP Exceptional Circumstances shall be documented within 30 calendar days from the actual implementation

No

a. CIP-007-5 Table R3 – Malicious Code Prevention Part 3.3: FPL does not agree with requirement to update signatures within 30 days of availability. This is not practical if the entity has a process to test the signatures before implementing. Suggest making the requirement consistent to implementing security patches b. Requirement R3.3 states "Update malicious code protections within 30 calendar

days of signature or pattern update availability (where the malicious code protections use signatures or patterns)." Recommend that you add the following statement to make consistent with Requirement CIP 007-5 R2.1: "Identify a source or sources that are monitored for the release of signature or pattern update availability (where the malicious code protections use signatures or patterns). c. Since some malware "engine or application" updates require rebooting, which is not compatible with BES Cyber System reliable operation, recommend you add two requirements, consistent with CIP 007-5 R2.2 and R2.3: "Identify applicable malware engine or application updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe" and "A process for remediation, including any exceptions for CIP Exceptional Circumstances." d. R3 – Malicious Code Prevention e. R3.4 Applicability – Propose deletion of Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems as they do not appear to be Transient Cyber Asset related. f. R3.5 Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems and they do not appear to be Transient Cyber Asset related. g. Requirements – Append “to Medium or High Impact BES Cyber Assets or Associated Protected Cyber Assets” to the end of the requirement. h. Measures – Content Change i. Original Text - Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets. ii.Proposed Change - Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to Medium or High Impact BES Cyber Assets or Protected Cyber Assets. i. R3.2: The measures for R3.2 only ask for configurations or a response, not the actual disarming or removal of identified malicious code. As such, these measures seem incomplete and the expectation is that an auditor would request to see evidence of malicious code disarmed or removed. Please include evidence of malicious code disarming or removal in the measures. j. Requirement 3.5 seems incomplete. Log each Transient Cyber Asset connection to what? The measure is clear, however, the requirement is not specific to what connections need to be logged.

No

a. 4.1 Requirements – Content Change i. Original Text – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: ii. 4.1.1. Any detected failed access attempts at Electronic Access Points iii.4.1.2. Any detected successful and failed login attempts iv. 4.1.3. Any detected malware v. 4.1.4. Any detected potential malicious activity. vi. Proposed Change – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: vii. 4.1.1. Any detected failed access attempts at Electronic Access Points viii. 4.1.2. Any detected successful and failed login attempts ix. 4.1.3. Any detected malware x. 4.1.4. Any detected potential malicious activity. xi. ADD: Devices that cannot log a particular event do not require a TFE to be generated. b. 4.2: Applicability – Proposed deletion of Associated Physical Access Control Systems and Associated Electronic Access Control Systems as they are out of scope for this requirement. c. R4.1 and 4.2: The measures should include actual system generated logs or alerts if auditors will request this information in an audit. d. R4.5: does not give guidance for a sample size. Please give guidance on what an acceptable sample size would be to meet compliance. e. Part 4.5 (Page 24) – Can we suggest that this is applicable only in cases where automated alerting is NOT available f. CIP-007-5 Table R4 – Security Event Monitoring i.Part 4.1: Requirement does not clearly reflect the Change Description and Justification: This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term “system events related to cyber security” from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. ii.We recommend rewording the requirement to include the word “define,” and better align with previous language in CIP-007 R3: iii. Define log generated events for the identification of, and after-the-fact investigations of, Cyber Security Incidents, as a minimum, each of the following types of events, even if such are null: 1. 4.1.1. Any detected failed access attempts at Electronic Access Points 2. 4.1.2. Any detected successful and failed login attempts 3. 4.1.3. Any detected "malicious code" 4. 4.1.4 Any detected "malicious activity" g. Since, according to the Guidelines and Technical Basis, “It is not the intent that if a device cannot log a particular event that TFE must be generated,” we recommend revising the Measure section to provide this clarification by revising its language to include: h. Evidence may include, but is not limited to, a paper or system generated listing of event classes for which the BES Cyber System is configured to generate logs. This listing must include the required event types "even

if such log generated event capabilities are not technically feasible" i. Part 4.2: We recommend rewording the requirement to align with implied requirement to perform and document an analysis to determine which events constitute a real-time alert described in Measures and Change Description and Justification sections: i. 4.2 Document alerts for events that the Responsible Entity determines to necessitate a real-time alert. ii. 4.2.1 Implement such real-time alerts j. Part 4.3: This is a tremendous undertaking to be able to monitor every cyber asset for logging failures within 1 day. It would even be a technical challenge to automate the detection. k. Part 4.3: The documentation of failures is also implied within requirement and Measures. We recommend revising such requirements to clearly outline this requirement, for example: l. 4.3 Detect and activate a response to event logging failures before the end of the next calendar day. i.4.3.1 Document event logging failures within 30 calendar days

No

a. R5.2 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. b. R5.2: is not feasible for large Registered Entities or entities where the CIP Senior Manager is a company executive. c. R5.3 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. d. R5.4 - How do you demonstrate 'unique' and does that introduce potential compliance concerns? e. Requirement R5.4 states "Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required." State if a TFE can be submitted for this requirement if it is not technically feasible. f. R5.4: how is compliance achieved / demonstrated when it is technically feasible to change a default password or the default password is blank but the vendor does not recommend changing the password due to system instability? g. R5.5- Add language to 5.5.3 to cover instances where accounts may not be able to support password change as follows to permit the entity specified time frame to be equal to the life-time of the BES Cyber Asset where technically required. h. Requirement R5.6 states "A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts." State if a TFE can be submitted for this requirement if it is not technically feasible. i. General: The suggested password change frequency is going to make managing these systems difficult, it will add significant workload to the personnel who have to do so, especially with all the documentation that will result.

Yes

No

a. Requirement 1.2, the term Reportable BES Cyber Security Incident only applies to BES Reliability Operating Services and those do not include EACMS or PACS. Is that the intention of this requirement? I believe the applicability section should state more clearly what systems are in scope for this throughout the standard. b. In the Guidelines and Technical Basis section, the definition of a Reportable BES Cyber Security Incident is not the same as the Version 5 Definitions. What is a "necessary response action?" An action is necessary with every Cyber Security Event in order to determine if it's reportable. c. What agencies are incidents reportable to? That should be defined within the requirements.

No

a. R2.1, where it says, "or test," is this a test of the CSIRP? If so, this is more applicable to requirement 3.2. This requirement also addresses all Cyber-Security Incidents. I recommend changing to Reportable BES Cyber Security Incidents. If left as written, this brings all non-reportable Cyber-Security Incidents into scope. b. R2.1 – The use of the word incident is repeated in requirement. We recommend rephrasing requirement: c. R2.2 reads funny, it appears to read as if we are to implement the CSIRP upon the effective date of the standard and then implement the CSIRP again thereafter. If the intent of the standard is to "exercise" the CSIRP, that is more clear than "implement." d. When a BES Cyber Security Incident occurs, the incident response plans must be used. Deviations taken from the plan during the incident or test shall be recorded.

No

a. A timeframe for updating the plan from lessons learn is restrictive. If there is a process change identified that has a major business impact, 60 days may not be enough time for implementation. Recommend a word change to state, "Update the BES Cyber Security Incident Response Plan upon

the implementation of any documented lessons learned within 60 calendar days of implementation." b. General comment: None of the measures mention actions plans from CSIRP exercises. If action plans will be requested as evidence, they should be listed as a measure c. R3.5 Roles and responsibilities may be assigned to a group, not a named individual. We recommend rewording/replacing "each person" with personnel. The use of each person implies superfluous, administrative burden to demonstrate compliance. d. Communicate each update to the BES Cyber Security Incident response plan to personnel with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.

Yes

No

a. R1.3 - We do not agree with the introduction of "protection" within the Recovery Plan requirements. We recommend that information protection requirements be fully addressed in CIP-011 standard b. Specific to Part 1.4 – our current process calls for backups to occur daily, including a mix of incremental and periodic full backups. A manual verification of media on a daily basis is not feasible. Is this intended to be a manual process or can it be supported by system generated notifications of successful backup notifications? Also, what actions should be taken if a backup is unsuccessful? c. It is not clear whether the exercise of the one or more documented recovery plans for Physical Access Control and / or Electronic Access Control or Monitoring systems must be addressed at the system or component level. If the exercise can be met either with a system exercise or for the loss of an access point to the PSP / ESP needs to be stated. d. R 1.5 - Does the data need to be kept for more than 30 days after the analysis or diagnosis of the cause of the event?

No

a. Testing on the effective date of the new standard should be within a year of the new standard being approved. An entity could have conducted the exercise of the plan a couple of months prior to the adoption of the new standard and now be in violation due the wordings in the standard. This comment applies to the other requirements in this standard. b. Allow for the flexibility to combine an operational exercise that addresses both High Impact and Medium Impact BES Cyber Systems. c. Operational Exercise need to be defined. It is not clear whether NIST SP 800-84 definition of a Functional Exercise, which could be met with a paper exercise with personnel simulating their roles and responsibilities, meets the requirement for R2.1 & R2.3 d. R2.1, the wording should be changed to "Exercise the recovery plan." It appears to read as if we are to implement the Recovery Plan upon the effective date of the standard and then implement the Recovery Plan again thereafter. If the intent of the standard is to "exercise" the Recovery Plan, which is more clear than "implement." e. R2.2, the measures should indicate what acceptable evidence is. Is an actual restore expected or proof that the information is available for restoration? In addition, does the word "initially" refer to the effective date of the standard? f. Pursuant to R2.3, is an operational exercise considered the actual recovery of a system? Also, should each asset defined within the scope of a plan be tested or will a recovery of one of the systems within the plan be acceptable? g. R2.2 - It is not clear if by the use of the word "any" the intent is that testing of the media to restore any one component of a BES Cyber System satisfies the requirement.

No

a. None of the measures mention actions plans from Recovery Plan exercises. If action plans will be requested as evidence, they should be listed as a measure. b. R3.1 R 3.4, the level at which an organizational level needs to be stated. For a recovery plan, it is more applicable for changes in the roles and responsibilities of the responders and / or organization. c. R3.3, the 30 day time frame is too restrictive and may not be possible based upon resource constraints. Recommend a word change to state, "Update the recovery plan(s) upon the implementation of any documented deficiencies or lessons learned within 30 calendar days." d. R3.5 Roles and responsibilities may be assigned to a group, not a named individual. We recommend rewording/replacing "each individual" with personnel. The use of each individual implies superfluous, administrative burden to demonstrate compliance: e. Communicate each update to the BES Cyber Security Incident response plan to personnel with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.

No

R2 - The standard needs to allow for a period not to exceed 15 months from the effective date of the

standard or notification that the standard will be effective for the responsible entity to conduct the initial test.
No
a. R1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset: -- This seems to exclude any software that may have been unintentially installed or installed automatically, such as automated installs. b. R1.1.4. Any custom software and scripts developed for the entity: --- To which extend do we document a baseline of the scripts, do the scripts have to be associated with the reliability of the BES Cyber System. c. R1.2: This seems to be an extensive task to the Senior Manager (SM) or Delegate (D), I believe that delegation is presumed here, as the measures allude to it by “where an individual with the authority to authorize the change was in attendance.” d. R 1.2 is problematic in that changes to the BES Cyber System baseline will require authorization from Senior Management. This requirement needs to be limited to major changes in the BES System and have “major” clearly defined. Another approach is to have the ability for proper delegation. e. There is concern about requirement 1.1.4 and the scope of software and scripts that this requirement applies to. f. Changes need to be defined as infrastructure changes and/or software changes that require Cyber Security Testing. Changes to a software function that only involves software modifications need to be excluded. What constitutes a requirement for Cyber Security testing for software changes must be explicitly determined. We suggest that Cyber Security Testing be carried out when a change to the baseline system include: (a) introduces communication to or from another system that is not within the ESP, (b) requires a new listening port and service, (c) requires a patch update to the operating system, (d) requires a new application or generic account, (e) requires a new third party application to be introduced to an existing or new cyber asset, or (f) requires a new cyber asset installation or replacement of an existing cyber asset.
No
a. R2.1 – To better address the basis described in Application Guideline section associated with technical infeasibility to implement automated technical monitoring controls for every BES Cyber System, we recommend rewording the requirement: b. 2.1 Define method(s) and associated periodicity(ies) implemented to monitor changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1). c. 2.1.1 Document and investigate the detection of any unauthorized changes.
No
R3.2: Elaboration on the requirement requested: “perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used” Additionally, what if the utility does not have a 1 to 1 test to production.
No
The High VSL severity appears to go beyond what’s in CIP-10 R1. It implies that even though no cyber security controls were deemed to be impacted, that a test still needs to be done to verify that none were affected, The conditions under which Cyber Security Testing must be done for a change in the base configuration from a software change must be explicitly included in the document by the committee.
No
a. For 1.2 and 1.3, the column heading for the second and third columns says “Part” instead of “Requirement” and “Measure.” Is that intentional or is that a typo? b. For 1.2, the measures do no give an indication of what is acceptable evidence. It is a given that documentation will be stored either in electronic or hard copy. However, how will the access control of this requirement be measured? For example, will user access on a need to know basis require an access request form to prove compliance or will the results of the assessment performed in R1.3 demonstrate compliance? c. R1.2 The requirements for this, based upon the evidence that is mentioned, seem to meet at least the level of SECRET classification management in DOD, see especially the following potential two evidence types: " Records indicating information that is stored, transported, and disposed in a manner consistent with the documented process"and " Hardcopies of information stored in a locked file cabinet with keys provided to only authorized individuals". This seems excessive, the evidence outlined as "Records from an information management system containing electronic copies of BES Cyber System Information with user access implemented on a need-to-know basis" indicates the level of document control to provide the protection that should be sufficient. d. For 1.3 if there are changes

made to an existing IPP as a result of this new version, assessing adherence upon the effective date of the standard is unreasonable. I suggest that a 60 window be provided to assess adherence to an IPP to allow for any possible changes to be made to any applicable documentation. e. R1.3 States " Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process". It would be easier to ensure compliance if the requirement to review was done on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders. f. In addition, the example evidence stated evidence that the records were disposed of - there should be clarification on this (i.e. are disposal logs or retirement notices enough?) This needs to be clarified better so there is not over-reaching interpretations of what is acceptable. g. Also, is there a required time frame for an action plan to be implemented? Suggestion would be < 90 days.

No

Although the Guidelines and Technical Basis will not be included in the standard, the strong encouragement to use NIST SP800-88 guidance for media sanitation could be interpreted as the framework that all Registered Entities will be judged by when their media sanitation processes are reviewed by the regions. Is NIST SP800-88 the expectation, recommend providing additional verbiage to remove ambiguity and confusion?

Yes

No

The effective dates says the following: "18 Months Minimum – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan." This seems to state that CIP 002 - 009 Version 4 is never going to be implemented, this is confusing. It would be better to state: " 18 Months Minimum – The Version 5 CIP Cyber Security Standards (including CIP 010-1 and 011-1) shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. In the event CIP-002-4 through CIP-009-4 do not become effective, CIP-002-3 through CIP-009-3 will remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan."

Individual

Martin Kaufman

ExxonMobil Research and Engineering

No

Yes

CIP-002-5 Requirement R1 requires classification of assets as High, Medium, or Low Impact. Per Attachment 1, all assets that are not High or Medium Impact are , by exception, classified as Low Impact. Classifying all non-High and non-Medium Impact assets as Low Impact assets creates a conflict and logic error with exemption 4.2.4.4 “Exemptions: 4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems” [Language from CIP-004-5, but similar language is in the NERC Reliability Standards CIP-003-5 through CIP-011-5]. This exemption is common to CIP standards CIP-003-5 through CIP-011-5 and is used by many small entities that possess no means for remote access. However, it requires the identification of no cyber systems rather than Low Impact assets. As NERC Reliability Standard CIP-002-5, does not allow for the identification of no Cyber Systems, the Standard Drafting Team should modify Attachment 1, CIP-002-5 Requirement R1, or the exemption sections of NERC Reliability Standards CIP-003-5 through CIP-011-5 to correct this logic error.

No

CIP-002-5 Requirement R1 requires classification of assets as High, Medium, or Low Impact. Per Attachment 1, all assets that are not High or Medium Impact are , by exception, classified as Low

Impact. Classifying all non-High and non-Medium Impact assets as Low Impact assets creates a conflict and logic error with exemption 4.2.4.4 “Exemptions: 4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems” [Language from CIP-004-5, but similar language is in the NERC Reliability Standards CIP-003-5 through CIP-011-5]. This exemption is common to CIP standards CIP-003-5 through CIP-011-5 and is used by many small entities that possess no means for remote access. However, it requires the identification of no cyber systems rather than Low Impact assets. As NERC Reliability Standard CIP-002-5, does not allow for the identification of no Cyber Systems, the Standard Drafting Team should modify Attachment 1, CIP-002-5 Requirement R1, or the exemption sections of NERC Reliability Standards CIP-003-5 through CIP-011-5 to correct this logic error.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
No
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
No

No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No

The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not

identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to

develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and

correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.

No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No

The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
Group
Members Representative Committee
Michael Quinn, Chair
Yes
Revise 2.4 to read “Each Blackstart Resource with External Connectivity identified in its Transmission Operator's restoration plan.” Blackstart Resources with External Connectivity would still be in the Medium Impact category; however, those Blackstart Resources without External Connectivity would have less cyber risk and move to the Low Impact category. The Blackstart Resources in the Low Impact category would have the appropriate physical and cyber protection controls as listed in the current CIP Version 5 draft standard. Our understanding of CIP Version 5 draft standards is that External Connectivity is defined as having Routable or Dial-up connections through the Electronic Access Point. Thus, many ERCOT Blackstart Resources would not fit in the Medium Impact category.

Individual
Mikhail Falkovich
PSEG
Yes
1. Capitalization: Only defined Glossary terms or terms in the definitions document (and the standards) should be capitalized when used. Several undefined terms are capitalized, such as Responsible Entities (sometimes not capitalized), Power System Stabilizers, Maintenance Cyber Asset, Automatic Voltage Regulation, Static VAR Compensators, Over and Under Frequency, and Demand Response. Other terms that are defined in the Glossary are not capitalized, such as spinning reserves, contingency reserves, and non-spinning reserves 2. BES Cyber Asset: a. The third sentence that describes the 15-minute time frame and relies on the asset being operational, yet the first sentence states that the asset may be rendered unavailable. This contradiction needs resolution. b. The third sentence should have the last word “BES” changed to “BES Reliability Operating Services.” c. BES Cyber Assets should be tied to a BES Facility. d. An asset rendered unavailable may take more than 15 minutes to impact a BES Reliability Operating Service. For example, if a coal conveyer supplying fuel to generator from a remote fuel storage area is rendered unavailable, the unit itself may not be adversely impacted for hours, depending on its on-site fuel storage capacity. e. What is meant by “adversely impact?” A threshold should be defined. f. Many of the BES Reliability Operating Services are an economic as well as a reliability service (e.g. unit commitment). If the economic aspect of the service is impacted, but not its reliability function, it would appear that the service is not “adversely impacted,” but this should be clarified. g. The definition should have a guideline developed for it that a registered entity could use to develop its BES Cyber Assets. h. The following definition is offered for consideration to the SDT: BES Cyber Asset A Cyber Asset that, when its operation is required, either failed to operate or misoperated, and as a result, an adverse impact would occur on one or more reliability-related functions of one or more BES Reliability Operating Services within 15 minutes. The 15-minute timeframe is measured from the time when the BES Cyber Asset should have operated correctly and the time when adverse impacts begin. A BES Cyber Asset shall be associated with one or more BES Facilities. Cyber Asset redundancy is not a valid reason for not classifying a Cyber Asset as a BES Cyber Asset. A Transient Cyber Asset is not considered a BES Cyber Asset. 3. BES Cyber Security Incident: a. Add “as predefined by the Responsible Entity” after “suspicious event.” [Note: If this is added to the definition, then the Responsible Entity must have a requirement to define this must be included in a CIP standard.] 4. BES Reliability Operating Services a. Dynamic Response to BES Conditions i. Third bullet – spell out “transformer.” ii. Third bullet – if “voltage” is added to the phrase “- Current, frequency, speed, phase” then the fifth and six bullets can be eliminated since they would be redundant to the third bullet. iii. Fourth bullet - why are “Sensors, relays & breakers, possibly software” mentioned? Sensors and relays are part of any Protection System. Circuit breakers are not, although the control circuitry that operates the trip coils is. “Possibly software” is

unacceptable – the SDT should describe the characteristics of the intended software. b. Balancing Load and Generation i. First bullet – “real time” should be “real-time.” ii. Third bullet – Change “&” to “and.” iii. Third bullet – What is meant by “load schedules?” Is it intended to mean “load forecasts?” c. Controlling Reactive Power i. Opening phrase, replace “bounds” with “limits.” ii. Fourth bullet – eliminate “transformer tap changers” since they are not an inductive source. Tap changers raise voltage on one side of a transformer, while lowering it on the other. They move VARS by this action. Any transformer is an inductive source, but reactors, not transformers, are used as a source of inductive capacity. The entire parenthetical should be replaced by “reactors.” d. Managing Constraints i. Fourth bullet – “SOL’s & IROL’s” should be “SOLs and IROLs.” ii. “Identify and monitor Flowgates” should have a bullet e. Restoration of the BES i. First sentence – delete “without external assistance” because it is untrue. ii. Second bullet – replace “planned” with “documented.” iii. Second bullet – “path” should be plural. f. Situation Awareness i. First sentence – delete “planned” ii. Second bullet – delete “Change management” because it is vague. If left in, a time frame should be defined. iii. Third bullet – delete “& Next Day” since Situational Awareness is “current.” 5. CIP Exceptional Circumstance: All of the conditions that define an “exceptional circumstance” may not have been considered in the proposed definition. Therefore, we suggest that the definition be more flexible in defining an exceptional circumstance. The wording should be changed to add the phrase “, including, but not limited to” after “conditions.” 6. Defined Physical Boundary: For clarity, suggest that the last phrase be modified to “for which physical access is controlled.”
Yes
• 1.3 & 1.4 - For Attachment1, Section 1.3 and 1.4 substitute the word "criteria" with the word "section" for clarity purposes. • 2.1 - For Attachment1, Section 2.1: Since the Interconnection is a defined term that is not applicable to this discussion, please remove the capitalization of the term "Interconnection" in this context, and change ".. in a single Interconnection" to "at a single interconnection". • 2.3 - For Attachment1, Section 2.3: We recommend deleting "or Transmission Planner.." to ensure that only one entity is responsible for designating appropriate generation. • 2.8 - For Attachment1, Section 2.8: We recommend changing "Transmission Facilities.." to "BES Transmission Facilities" for consistency purposes. • 2.9 - For Attachment1, Section2.9: Please provide a definition for ther term "Flexible AC Transmission Systems FACTS" for consistency purposes. • 2.13 - For Attachment1, Section2.13: We propose to change the wording "generation control center" to "generation Control Center" for consistency purposes. • 3 - For Attachment1, Section3: we propose to change the wording "..or Section 2 Medium.." to "..Section 2 as having a Medium.." for consistency purposes. • For Attachment1, Section 1 where the statement reads "Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at:" we propose a change to say "Each BES Cyber Asset within a BES Cyber System which is used and located at:" - This is to remove redundancy of the definition from the statement. • For Attachment1, Section 2 where the statement reads "Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for:" we propose a change to say "Each BES Cyber Asset within a BES Cyber System not included in Section 1, and which is used for:" - This is to remove redundancy of the definition from the statement. • We would like to include the following example in the guideline to clarify the categorization of Low Impact BES Cyber Assets and Systems. Due to the need to categorize the Low Impact BES Cyber Systems, an example of a methodology would be to: (1) Identify the physical plant locations (facilities). (2) Determine the possible adverse impact of those physical plant locations (facilities) on the BROS (BES Reliability Operating Services) (3) If low adverse impact to the BROS, then categorize all BES Cyber Systems within the physical plant locations (facilities) to be Low Impact without discretely identifying each system. (per R1.)
Yes
• CIP-002 R1: a. In the wording of the Rationale section, the language states "Cyber Assets and Cyber Systems..". We recommend the language be changed to "BES Cyber Assets and BES Cyber Systems.." instead. b. Please provide a definition of "application of the required controls (last sentence of M1)" Background section comments: • Please provide a clarification on the following statement - "So it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply (Page 7, 2nd paragraph, last sentence.)" - Does this mean that the entity can choose the devices that need to follow the malware protection within a given BES Cyber System and choose those devices that are excluded? •

Since "RE can use the well-developed concept of a security plan for EACH BES Cyber System to document the programs…(last sentence on page 7.)", does this imply the discrete identification of Low Impact Cyber Systems is required?
No
• CIP-002 R2: a. The following wording should be added to the Measure in CAPs,"BES Cyber Assets and BES Cyber Systems initially upon….." should become "High and Medium Impact BES Cyber Assets and BES Cyber Systems initially upon….." • Evidence Retention comment: a. 1.2 We recommend the deletion of the following sentence "For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit." as it contradicts the requirement to retain the data for three calendar years.
Yes
Yes
Yes
Yes
Yes
No
• CIP-003 R5: For the third bullet under M5 we would recommend breaking it out into a table to allow for easier readiblity.
Yes
Yes
Yes
No
• CIP-004 R2: a. For sub-requirement 2.5: We propose to change the wording "Training on the visitor control program." to say "Training on the visitor control program for both physical and electronic security." for completeness purposes. b. For requirement 2: Please provide a guideline (sample deck) of acceptable level of training.
No
• CIP-004 R3: a. For requirements 3.1,3.2,5.1, and 5.2, Applicability section of the table: To stay consistent with the other requirements' applicability we propose to remove the following items from the Applicability Section: Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets
No
• CIP-004 R4: a. For Requirement 4.1 rationale section - We propose to change the wording "Specified that identify.." to "Specified that identity.." to correct the typo. b. There are times when a web-conference or a shared screen scenario can occur with a vendor for support (or other) purposes. In such a case, we believe that the electronic access is in fact 'escorted'. We propose the following change in the wording in the Rationale for R4: To ensure that individuals who need authorized unescorted electronic or unescorted physical access to BES Cyber Systems have been assessed for risk. Additionally we propose that two defined terms be added to the glossary: Escorted Electronic Access and Unescorted Electronic Access. Thus all of the references which specify 'electronic access' within the standards would become Unescorted Electronic Access.
Yes

Yes
Yes
Yes
No
• CIP-005 R1: a. Applicability - Please provide guidance on what would constitute such systems. Similarly, if no discrete identification of such assets is specified by R1 in CIP-002, an entity would not necessarily be able to identify whether External Routable Connectivity exists or not. We propose to remove the language 'with External Routable Connectivity' from any Applicability sections within the standards. b. For Measures for requirement 1.1 we propose to change the following language: "Evidence may include, but is not limited to, documented technical and procedural controls that exist.." to "Evidence may include, but is not limited to, documented technical or procedural controls that exist.." for clarification purposes c. For Requirement 1.3 (Applicability section) we propose to change the following language: "Electronic Access Points at High Impact BES Cyber Systems" with "Electronic Access Points at High Impact BES Cyber Systems with External Routable Connectivity" for clarification purposes. d. For the change rationale in R1.5: There are times that a single device can provide multiple distinct security measures such as a firewall and an IDS in the same hardware. Please confirm that 'two distinct security measures' can exist on the same device as part of the guideline.
No
a. For requirements 2.1,2.2 and 2.3: We recommend adding the wording "where technically feasible" at the end for all requirement sections within the R2 table.
No
• There is no gradation within the VSLs for this standard. We recommend that Multiple levels of VSLs should be created.
No
• CIP-006 R1: a. For Requirement 1.3 Please provide an example within the guideline of two or more complimentary physical access controls. (Would a magnetic lock and an access card reader be sufficient?) b. The VSLs specify an action to be taken within a limited amount of time (15 minutes). The standard does not specify a time duration. This timed requirement either needs to be removed from the VSLs or added into the standard language. c. For Requirement 1.1: This requirement would force the entities to discretely identify Low Impact BES Cyber Systems. We propose that the wording the Applicability Section is changed to: "facilities containing Low Impact BES Cyber Systems" d. For the Measures in Requirement 1.1: We propose a change in wording - "Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented." to be changed to "Evidence may include, but is not limited to, documented operational or procedural controls exist and have been implemented." e. For the Measures in Requirements 1.2 and 1.3: Due to safety, operational concerns, and local fire codes we propose the wording be changed from "..plan that describes the physical boundaries and how ingress and egress is controlled by two or more different methods.." to "..plan that describes the physical boundaries and how ingress is controlled by one or more different methods…." f. For Requirements 1.4 and 1.5: We propose the following wording change "..in response to unauthorized physical access through any access point.." to be changed to "..in response to unauthorized individuals obtaining physical access through any physical access point.." We also propose that requirements 1.4 and 1.5 are combined. g. For the Measure in Requirement 1: We propose a change in wording "Measure must includes.." to be changed to "Measure must include.." h. For Requirement 1 - Change Description: This language would force the entities to discretely identify Low Impact BES Cyber Systems. We propose that the wording in the Change Description section is changed to: "...this includes how the entity plans to protect facilities containing Low Impact BES Cyber Systems and.." Evidence retention comments: • For Evidence Retention: Three year evidence retention seems excessive and places undue burden and costs for compliance. We recommend a shorter period of a year or 18 months.
Yes

Yes
No
• In the case of the Medium VSL an entity would be punished for an omission of a part of the log, but if an entry was missed wholesale, that event would not be identified and therefore no punishment meted out.
No
• CIP-007 R1: a. For Requirement 1.1: We propose the following language instead of the current version "Disable or restrict access to unnecessary listening logical network accessible ports and document the need for any remaining listening logical network accessible ports" b. For Requirement 1.2: We propose to change the requirement language as follows: "....console commands, or removable media." to "....console commands, or removable media, where technically feasible." c. For Requirement 1.2: Does this language duplicate the physical security requirements already covered under CIP-006-5 R1.3?
No
• CIP-007 R2: a. For requirement 2.1 – measure: We propose that clarification language be included in the guideline that specifies: If a given vendor provides a system with multiple components and multiple softwares, then it is acceptable for the Registered Entity to go to the single vendor as a valid source for the patches and/or updates for all software and firmware. b. For Requirement 2.3: We propose the following changes: "A process for remediation..." to be changed to "A process for the implementation of the remediation plan"
No
• CIP-007 R3: a. For requirement 3.2: Does this language duplicate the requirements in the incident response standard CIP-008-5 R1 and it's sub-requirement? We propose to remove this requirement and add appropriate language to the guideline document of CIP-008v5 so that malicious code removal is addressed. b. For requirement 3.5 - measure: Please provide clarification: Are manually kept logs sufficient for those systems that cannot identify the connection? c. For the Rationale section of R3: Please provide a definition of "Maintenance Cyber Asset". d. For Requirement 3.1: We propose to change the requirement language as follows: "Deploy method(s) to deter, detect, or prevent malicious code." to "Deploy method(s) to deter, detect, or prevent malicious code., where technically feasible." e. For requirement 3.2: We propose to change the requirement language as follows: "disarm or remove identified malicious code" to "disarm or remove identified malicious code, where technically feasible" f. If malicious code constitutes a BES Cyber Security Incident, the first and third bullet points have already been addressed in Part 1.1 and 1.3 of CIP-008v5 R1 respectively. g. For Requirement 3.4: We propose adding ",where technically feasible." at the end of the requirement. h. For Requirement 3.5: We propose adding ",where technically feasible." at the end of the requirement. i. We propose to separate this requirement into 3 sub-parts: 1. Part 1 of 3.3 - Identify signature or pattern update availability (where the malicious code protections use signatures or patterns) 2. Part 2 of 3.3 - Update malicioius code protections within 30 calendar days after the release of approval from the identified source/sources that address(es) the updates 3. Part 3 of 3.3 - the implementation of malicious code protections
No
• CIP-007 R4: a. for requirement 4.3: This language implies that all entities have a seven day a week operations staff in this area. It may be more prudent to change the requirement from next calendar day to next business day. b. For Requirement 4.1.3: We propose adding ",where technically feasible." at the end of the requirement. c. For Requirement 4.1.4: We propose adding ",where technically feasible." at the end of the requirement.
Yes
No
2. VSL: • R2: a. For the VSLs applicable to Requirement 2: We recommend adding the following breakdown of the severity levels instead of having a single Severe level applied: -Severe being no source identified and patches not reviewed within 30 days -High being not all patches reviewed within 30 days or no remediation plan implemented for reviewed patches -Medium being no source identified • R3: a. Similarly to the comment for R3.2, the language in the R3 VSL references the disarming and

removal of identified malicious code which may be a duplicate of the incident response VSLs in the standard standard CIP-008-5 R1 • R4: a. For the VSLs applicable to Requirement 4: Under the High VSL the language references the need for real-time alerting for logging failures which is not identified in the standard requirements. We recommend removing this language. Additionally, an entity may choose to designate a real time alert requirement for a piece of hardware/software that technically is not able to perform logging. Thus, a technical exception may be needed. b. We propose the following change to the Severe VSL applicable to Requirement 4: "The Responsible Entity failed to identify and implement methods to generate alerts for events that it determines to necessitate a real-time alert" to be changed to “The Responsible Entity failed to identify and implement methods to generate real-time alerts for events it determined necessary to have real-time alerts”
No
a. We recommend that the first sentence is changed to “R1 provides for consistent responses to BES Cyber Security Incidents involving BES Cyber Assets and BES Cyber Systems.”? The third sentence should be changed to: “Once the number and severity of events rises to the level of becoming a Reportable BES Cyber Security Incident the current version of EOP-004 directs..."
No
• CIP-008 R2: a. 2.2 - We propose adding "exercise" for the first bullet and "test" for the second and third bullets to provide a clear description of what actions need to be taken to implement the BES Cyber Security Incidence response plan. The suggested languages are as follow: -"exercise" by responding to an actual incident, or -"test" with a paper drill or table top exercise, or -"test" with a full operational exercise b. 2.3 - The term "documentation" is too vague. "records" would be more concise term for this requirement. c. 2.2- The language “initially upon the effective date of the standard” appears in this requirement is unreasonable because it would require each Registered Entity to perform an action that is not valid unless performed on the effective date, such as conduct a paper drill or table top exercise or a full operational exercise. d. We suggest deleting "when incident occurs" after” response plans must be used" to eliminate redundancy. The proposed language is as follow: “When a BES Cyber Security Incident occurs, the incident response plans must be used and include recording …..”
No
• CIP-008 R3: a. Requirement - 3.4 - We suggest breaking down this requirement into 2 parts: 30 days for technology changes and 60 days for organizational changes, which may take longer to address. The proposed language is as follow: Update the BES Cyber Security Incident response plan(s) within: -1.THIRTY calendar days of any TECHNOLOGY changes that impact the plan and -2. SIXTY calendar days of any ORGANIZATIONAL changes that impact the plan b. Requirement 3.1 - The language “initially upon the effective date of the standard” appears in this requirement is unreasonable because it would require each Registered Entity to review its BES Cyber Incident response plan on the effective date even though it’s not required to have its initial response plan until the effective date per R1.
Yes
No
• CIP-009 R1: a. For requirements 1.4 and 1.5, titles of second and third column should be "Requirements" and "Measures" respectively b. For Requirement 1.4, delete “initially after backup" from the requirement due to the fact that the back up process is self-checking by default. c. For requirement 1.4, please provide clarification on the frequency of backup verification. We agree that backup verification should be undertaken; however, we believe that verification after each backup is counterproductive. d. For requirement 1.5, we believe that this should be moved to CIP-008 standard
No
• CIP-009 R2: a. For rationale section of requirement 2, please provide a definition for "Operational Exercises" b. For rationale section of requirement 2, delete "28" in the beginning of the last sentence of the "Functional Exercises" section c. For requirement 2.1, we recommend replacing "upon the" with "within the first calendar year of the effective date of the standard" d. For requirement 2.1, we recommend adding: -"exercise" to the first bullet -"test" to the second bullet -"test" to the third bullet e. Requirement 2.1 and 2.3 - The language “initially upon the effective date of the standard” appears in this requirement is unreasonable because they would require each Registered Entity to perform an action that is not valid unless performed on the effective date, such as conduct a paper drill or table

top exercise or a full operational exercise.
No
• CIP-009 R3: a. For requirement 3.1, we recommend removing "or lessons learned" at the end of the sentence b. For requirement 3.4, we suggest to allow 60 days for updating organizational changes related to recovery plan(s) c. For requirement 3.5, we suggest to allow 60 days for communicating recovery plan updates. d. Requirement 3.1- The language “initially upon the effective date of the standard” appears in this requirement is unreasonable because it would require each Registered Entity to review recovery plans on the effective date even though it’s not required to have its initial recovery plan until the effective date per R1.
Yes
No
• CIP-010 R1: a. For requirement 1.1, please provide a clarification on how often the baseline should be updated. b. For requirement 1.1.3, we recommend changing it to “Any commercially available application software (including version) intentionally installed by or at the request of the Responsible Entity on the BES Cyber Asset" c. We propose the following modified language to requirement 1.4.1: Prior to the change, determine required cyber security controls that could be impacted by the change AND TEST THE NEW CONFIGURATION IN A TEST ENVIRONMENT d. We propose the following modified language to requirement 1.5.2: the measures used to account for any differences in operation between the test and production environments BEFORE THE CHANGE IS MADE.
No
• CIP-010 R2: a. For Requirement 2.1, we recommend that the guideline includes the following statement: "physical hardware changes that do not affect the functionality of the system to be excluded from the requirement" (example I/O port rewiring or power supply changes)
No
• CIP-010 R3: a. We feel that the language “initially upon the effective date of the standard” appears in requirement 3.1 and 3.2 is unreasonable because it would require each Registered Entity to perform assessments on the effective date of the standard. Please provide a guidance section that would detail alternative times (such as, prior to the standard going into effect) that would allow the Registered Entity to comply effectively. b. For requirement 3.2, we recommend that the standard mention that the active vulnerability assessment be performed in either a test OR production environment For the Guidance and Technical Basis section: • Within the guidance document section R3(first sentence), we propose to change "not" to "note" Compliance: • For the Compliance section (on page 20), we propose first bullet of sec 1.2 to be changed to "Each Responsible Entity shall retain data or evidence from the last completed audit…" from "Each Responsible Entity shall retain data or evidence for since the last completed audit…"
Yes
No
• CIP-011 R1: a. The language “initially upon the effective date of the standard” within this requirement is unreasonable because it would require each Registered Entity to perform an assessment on the effective date of the standard
Yes
No
• This VSL should be updated to include “…initially within the first calendar month or quarter after the effective of the standard…”
No
1. The example on p. 3 of the Implementation Plan document for unplanned changes, power flows are not a criterion for the impact level of any BES Cyber Assets, so the example needs to be revised. Nevertheless, for “planned” changes by one Responsible Entity that impacts another Responsible Entity, what is the timeline for compliance by the other Responsible Entity and would the causal Responsible Entity be responsible for the compliance cost for the other Responsible Entity? For other standards (e.g., TPL) an entity that whose planned changes result in another entity being out of

compliance is responsible for the entire cost of compliance associated with its actions, both for itself and other entities that it impacts. 2. Although this issue is addressed in particular standards and not in the Implementation Plan, it will cause significant implementation issues if not addressed. Common language that requires implementation of a requirement “initially upon the effective date of the standard” appears in numerous standards. These requirements are unreasonable because they require an action on the first day (and first day only) that the standard is effective. Here is a list of where this language appears in the v5 standards for requirements that are unreasonable when this language is used. a. CIP-008-5, R2.2 is unreasonable because it would require each Registered Entity to perform an action that is not valid unless performed on the effective date, such as conduct a paper drill or table top exercise or a full operational exercise. b. CIP-008-5, R3.1 is unreasonable because it would require each Registered Entity to review its BES Cyber Incident response plan on the effective date even though it’s not required to have its initial response plan until the effective date per R1. c. CIP-009-5, R2.1 and R2.3 are unreasonable in that they would require each Registered Entity to perform an action that is not valid unless performed on the effective date, such as conduct a paper drill or table top exercise or a full operational exercise. d. CIP-009-5, R3.1 is unreasonable because it would require each Registered Entity to review recovery plans on the effective date even though it’s not required to have its initial recovery plan until the effective date per R1. e. CIP-010-1, R3.1 and R3.2 are unreasonable because they would require each Registered Entity to perform assessments on the effective date of the standard. f. CIP-011-1, R1.3 is unreasonable because it would require each Registered Entity to perform an assessment on the effective date of the standard.
Group
PowerSouth CIP Review Team
Tim Hattaway
No
Yes
Yes
Yes
Yes
Yes
No
Would like to see this changed to 60 days.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
No
Further clarification is needed regarding what part of the communication path to the destination host must be encrypted or if the entire communication path is the intent of the regulation. The lack of clarity leaves this open for interpretation by an audit team.
No
Under the measures section, it states "…and how ingress and egress is controlled by two or more different methods…" implies that both ingress and egress must be controlled by two or more different methods (physical access controls). We feel that a single egress physical access control should be acceptable for authorized individuals exiting a restricted space.
No
Clarify or Remove: "and records of disposition of security related event logs beyond ninety day up to the evidence retention period." To what extent do you mean "records of disposition"? How do you prove log data for a Cyber Assets was deleted from a log server after a certain age? This needs to be clarified more to identify exactly what is required. If the standard states you need to keep logs for 90 days, you shouldn't have to keep them longer to prove to an auditor that you had the logs for every 90 day period since the last audit. If that is the intent, then the standard should state that.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Individual
David Dockery
Associated Electric Cooperative, Inc
Yes
BES Cyber Asset Definition CHANGE FROM: BES Cyber Asset - A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. CHANGE TO: BES Cyber Asset - A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Service, without regard to the initial time of asset compromise. A Transient Cyber Asset is not considered a BES Cyber Asset. RATIONALE: 1) Brevity, clarity, and less is better. 2) Deleted stuff belongs in guidelines. BES Cyber Security Incident Definition - Bullets #1 & #2, Change: “was an attempt” To: “was an apparent attempt" Rationale: we cannot judge intent BES Cyber System Definition Change: “Maintenance Cyber Asset” To: “Transient Cyber Asset” Rationale: Consistency and no definition proposed for Maintenance Cyber Asset. BES Cyber System Information Definition Move: the “(e.g., network addresses…)” parenthetical To: immediately follow “Electronic Access Control Systems” Rationale: group EAC Information examples immediately with the EACs clause. Associated Electric Cooperative also agrees with NRECA's comment BES Reliability Operating Services –AECI believes the following BES services should be removed from the BES Reliability Operating Services, because they fail to meet the “real-time reliable operation of the BES” 15-minute adverse-impact criteria: 1) Balancing Load and Generation, (other than ACE, nothing else in this category can have a 15-minutes or less impact, and ACE availability and integrity are addressed within the BAL Standard, so including here is double-jeopardy.) 2) Managing Constraints, 3) Restoration of BES, (actual control likely will be performed by hand with field personnel) 4) Situational Awareness – Frequency Monitoring – (While frequency monitoring is important, contrary to the underlying position within the CIP standards, redundancy of frequency monitors really does matter, and the standard should probably leave this one off, in order to avoid only a few instances of frequency-monitoring equipment being implemented. Also, the availability of a reliable Frequency Monitoring signal is subject to a strict BAL standard. CIP Senior Manager Associated Electric Cooperative agrees with NRECA's comment Control Center Definition Change: “BES generation facilities or transmission facilities” To: “BES generation facilities or BES transmission facilities” Rationale: Clarity of scope. Comment: AECI's understanding that this definition's use of the NERC glossary "System Operator", inherently limits the scope of this definition to only "manned" locations where BA, TOP, GOP, or RC functions are performed. Electronic Access Point (“EAP”) Definition Comment: There appears to be a loop-hole in this definition, with regard to dumb terminals utilizing dial-up or routed access from the other end. By definition here, old dumb terminals are not Cyber Assets because they are not programmable. (Ok, most of the “later” models had EPROMS). This definition dictates “between Cyber Assets”. (This potential flaw may carry over to “External Connectivity” and “Interactive Remote Access” definitions as well.)
Yes

Appendix 1, both Sections 1.3 and 1.4 APPEND: “, at two or more locations” RATIONALE: Clarity of intent and consistency with Control Center definition. Appendix 1, Section 2.4 CHANGE: “Each” TO: “At least one” RATIONALE: 1) Current wording will result in many black-start resources being removed from Transmission Operator’s black-start plans, thereby decreasing overall system reliability in case of a real system-restoration emergency, and 2) consistency with the way the drafting-team’s CIP-002-5 Guidelines addresses redundant assets within an entity’s SRP black-start unit’s cranking-path. Appendix 1, Section 2.5 CHANGE: “the Cranking Paths” TO: “the section 2.4 identified Resource’s Cranking Path” RATIONALE: consistency with AECI's proposed change to 2.4 above Please note that AECI encourages the CSO 706 SDT to consider the following set of proposed Appendix 1, Section 1.2, 2.13, and new 2.14 changes and corresponding guidelines as a package. ===Begin==== Appendix 1, Section 1.2 CHANGE TO: “Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection”. RATIONALE: 1) Consistency with the bright-line risk cited throughout CIP-002-5 Appendix 1, 2) smaller BAs are automatically caught by CIP-002-5 Appendix 1 Proposed Section 2.14 Medium Impact Rating, and 3) legitimate APPA and NRECA concern for cost versus quality and risk of additional High Impact Rating controls and measures, versus expected return on industry’s investment forced on these small entities. Appendix 1, Section 2.13 CHANGE TO: “Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners that directly or indirectly control 1500 MW of generation; or (2) generation control centers that control 1500 MW or more of generation.” RATIONALE: 1) Inconsistency in this draft’s proposed usage and citation of UVLS and UFLS 300 MW load-shed threshold. UVLS and UFLS concern is expected shedding of load amounts necessary to stabilize system voltage or frequency, whereas this scope of concern is sudden and unexpected loss of generation. 2) Consistency with impact of Appendix 1, Section 2.1, although the impact of loss in 1500 MW generation, diversified across several electrical network locations, is expected to be much less than for 1500 MW single plant loss concentrated at one location within a network. 3) Section 2.14 is proposed below to manage remaining scope of this previously worded section. 4) BAs below 1500 MW are not exempted as are TOs, TOPs, and GOPs, because the scope of their interconnectivity with other control centers poses a greater risk to the BES. 5) See corresponding Guidelines below. Appendix 1 - Section 2.14 ADD: “2.14 Control Centers, not previously included in High Impact Rating (H) or Medium Impact Rating (M), above, that perform the functional obligations of Balancing Authority, Transmission Operators or Transmission Owners, or Generation Operators, and that do not implement protected data connections with other Control Centers in a manner as to prevent themselves from being used as cyber-attack vectors into other Medium Impact or High Impact Rating Control Centers.” Rationale: In the CIP-002-5 Guidelines p.30 Bullet#1 (on that page), the SDT provided no explanation as to why all transmission control centers should be deemed Medium Impact, although they did provide some impact consideration for generation control centers. AECI strongly encourages the SDT to adopt this recommended change along with our proposed corresponding guidelines, in consideration of FERC requests for consideration of control center impacts and connectivity risks (FERC Order 706, paragraphs 280, 281, 282, and FERC NOPR Docket No.RM11-11-000, paragraphs 41, 43, 53), and to incent our industry toward deploying true mono-directional “routable” (data-diodes) and non-routable (hardened mailbox RTU) data-interface connectivity, where applicable, as mitigating measures that would lower these local-control-centers to their true Low Impact category, and to incent further innovation and deployment of hardened communication interfaces. Also, per Appendix Section 3, the Control Centers excluded from Medium Impact Rating (M), must necessarily exercise Low Impact Rating (L) controls specified within the standards, and be subject to audit, which would necessarily include assessment of all their “protected data connections” required within this section. See also companion changes to CIP-002-5 Appendix 1, Sections 1.2 and 2.13. Appendix 1 Guidelines, Section 2.13 ADD GUIDELINE: “2.13 The phrase - directly or indirectly control - encompasses the potential to open multiple breakers or otherwise issue automated command controls from a compromised Control Center, in such a manner as to cause separation of 1500 MW or greater net generation from an Interconnection. This standard selects 1500 MW for compatibility with Section 2.1.” ========End======== Appendix 1 Guidelines, Section 2.14 ADD GUIDELINE: “2.14 Beyond direct or indirect impact above the bright-line threshold for generation or load, there is legitimate concern that any interconnected Control Center may serve as a cyber-attack vector into neighboring Control Centers. The CIP Standards’ Physical and Electronic controls, specified for High and Medium impact Control Centers, function to mitigate those prolonged-exposure threats. This section recognizes that our industry’s cyber-security

will benefit from their installing hardened data-communication interfaces that practically function as “air-gaps” against opportunistic hacking, and it seeks to incent such deployment at all Control Centers where the real-time BES impact would otherwise be rated as Low Impact. At the time of this standard’s ratification, some data-diodes or hardened mailbox-RTUs can meet this need, but it is likely that future developments will provide even more secure, robust, and economically attractive solutions. For responsible entities that identify their control-centers as Low Impact, the CEA will verify that the installed communications protection device(s) and implementation(s) on every communication interface with other Medium or High Impact Control Centers, are such that the Low Impact control centers have a low probability of being used as a cyber-attack vector on other Control Centers. Evidence the CEA might look for could include but not be limited to device configuration information, file structures used for the exchange of data, and related procedural controls. These devices should be protected and managed in a manner similar to that which is applied to devices serving as electronic access points to protected networks. Specifically, the responsible entity must be prepared to show evidence to the CEA that these interfaces to High and Medium impact Control Centers, have been and are being actively maintained through a deliberate program of security-patch awareness, evaluation, and deployment based upon their evaluation.”
No
R1.1 CHANGE: “and Facilities is placed” TO: “and Facilities being placed” RATIONALE: Grammatical.
No
R2 Rationale CHANGE: “Manager’s approval” TO: Manager’s responsibility in approval” RATIONALE: the Senior Manager or delegate performs an approval, but the responsibility remains with the Senior Manager. R2 CHANGE: “initially upon the effective” TO: “initially prior to or upon the effective” RATIONALE: “it should be permissible for the Senior Manager to perform this duty before the effective date, rather than confining that action to the exact date this body of standards become effective. M2 CHANGE: “Manager review” TO: “Manager or delegate review” RATIONALE: Consistency with the requirement itself.
Yes
Yes
No
R2 CHANGE: Renumber bullets 2.1..2.10 rather than 1.1..1.10. RATIONALE: Consistency with the Requirement number. R2 CHANGE: Tighten scope of requirements, succinctly, to match scope identified within guidelines RATIONALE: Legal requirement scope could be interpreted too broadly, by either responsible entities or auditors. Is Physical Security related to Cyber Assets, personnel, cyber-related personel, or general building security? Is System Security for the Electrical Power System, the Cyber System, or the Alarm System, and how is it differentiated from Electornic Security and Physical Security. While page 20 and 21 of the guidelines are invaluable here, the legal scope of this requirement could and should be narrowed.
Yes
Yes
Yes
No
R6 CHANGE: “thirty” TO: “sixty” RATIONALE: Senior Managers are busy and so long as there were no underlying violations within a program, it was working. And corresponding R6 VSL CHANGE: “30” TO: “60” RATIONALE: Senior Manager change will encompass a lot of responsibilities for very busy people. Making 30 days SEVERE is unreasonable. ALTERNATIVE PROPOSAL R6: no change R6 VSL: Low: Senior Manager change undocumented greater than 30 days but less than 60 days. Moderate: Senior Manager undocumented or one delegate undocumented greater than 60 days but less than 60 days. High: Senior Manager remained undocumented 60 days but less than 90 days or two or more delegates undocumented 30 days but less than 60 days. SEVERE: Senior manager remained

undocumented 90 days or more, or three or more delegates undocumented 30 days or more. Rationale: More granularity where risk is already noted as LOW, where nothing else went wrong other than this formal documentation.
No
R5 VSL Change: Shift all columns left Rationale: If the program continues to operate properly and no additional violations were spotted, then this failure in documentation is just window-dressing. If not, then there will be plenty of additional requirements violated along with those penalties. R6 VSL: AECI proposed two alternative changes for R6 and corresponding R6 VSL, posted under R6.
Yes
Yes
Yes
Yes
Yes
Yes
No
R7 CHANGE: “at time of resignation or termination” TO: “within 24 hours of resignation or termination” RATIONALE: Consistency with hard time-frames asserted with other sub-requirements, with reasonable delay for uncontrollable circumstances surrounding some separation of employment.
No
R4 VSL CHANGE R4 Lower VSL: “Entity had no formal PRA program per R4, yet provided evidence of PRAs having been performed within the last 7 years for all personnel with access stated within R4, and otherwise conformant to the PRA requirements within R4." CHANGE R4 Severe VSL: altered to read “and has no evidence of PRAs having been performed for individuals granted … access” RATIONALE: better match severity to risk of circumstance R5 VSL CHANGE R5 Lower VSL: “The Responsible Entity did not have a documented process for personnel risk assessment yet performed PRAs conformant with NERC CIP Standards” CHANGE R5 Severe VSL: append “and has no evidence of PRAs having been performed conformant with the NERC CIP Standards”. RATIONALE: match severity to risk of circumstance R6 VSL CHANGE R6 Severe VSL: append “and Access Privileges were in effect that did not conform to NERC CIP Standards” RATIONALE : match severity to risk of circumstance R7 VSL changes: for cases of reassigned or transferred individuals, shift the failure numbers as follows CHANGE R7 Lower VSL: “1 or 2” CHANGE R7 Moderate VSL: “3 or 4” CHANGE R7 High VSL: “5 or 6” CHANGE R7 Severe VSL: “7 or more” APPEND to 7 Severe VSL: “and Access revocation was not performed conformant to the NERC CIP Standards.” To the Severe VSL. RATIONALE: match severity to risk of circumstance (personnel retained within the company are operating at a higher trust level and with greater corporate policy controls than those who have been removed from the workplace.)
No
R1.5 Requirements CHANGE: “malicious” TO: “potentially malicious” or “unanticipated” or “unnecessary” RATIONALE: align with CIP-007-5 R4.1.4 wording, which employs “potentially” or use other wording that frees entities from being required to establish intent
Yes
No
R1 VSL CHANGE: Create R# R1.1 row with... ADD R1.1 Lower VSL: “The responsible entity did not define any technical or procedural controls to restrict unauthorized electronic access , but all sampling produced evidence of proper restrictions having been applied to EAPs” ADD R1.1 Moderate VSL: “The responsible entity did not define any technical or procedural controls to restrict unauthorized electronic access, and sampling did produce evidence that proper restrictions were not applied to

some internal EAPs and yet external EAPs were appropriately controlled" ADD R1.1 High VSL: "The responsible entity did not define any technical or procedural controls to restrict unauthorized electronic access, and sampling did produce evidence that proper restrictions were not applied to internal or external EAPs" ADD R1.1 Severe VSL: "non-applicable". RATIONALE: match severity with risk of Low Impact Assets and Systems R1 VSL CHANGE R1 VSL R#: "R1" TO: R1.2..R1.5 VSL R#: "R1.2..R1.5" CHANGE R1.2..R1.5, all VSLs: delete the phrase "The Responsible Entity did not define technical or procedureal controls to restrict unauthorized electronic access." RATIONALE: This phrase applies only to Low Impact Cyber Assets, which are addressed in the suggested companion change above. R2 VSL CHANGE R2 Moderate VSL: add the phrase "Responsible Entity had Medium Impact Assets where: ("<body of text found in the Severe column>")" CHANGE R2 Severe VSL: "Responsible Entity had High Impact Assets where ("<body of text originally in the Severe column>")" RATIONALE: match severity with risk.

No

Page 10 "Requirements and Measures, Summary of Changes, 2nd line CHANGE: "was no specific" IS: "is no specific" RATIONALE: grammatical M1.1 CHANGE: "controls exist" TO: "controls that exist" RATIONALE: grammatical R1.1 Rationale CHANGE: "how the entity plans to" TO: "how the entity plans and acts to" RATIONALE: intent of requirement and measure?

Yes

Yes

No

R1 VSL INSERT row R# R1.1 ADD R1.1 VRF: "Low" ADD R1.1 Low VSL: "The Responsible Entity has documented procedural controls but 1 or 2 boundaries failed to meet or exceed those controls" ADD R1.1 Moderate VSL: "The Responsible Entity has documented procedural controls but 3 or 4 boundaries failed to meet or exceed those controls" ADD R1.1 High VSL: "The Responsible Entity has documented procedural controls but 5 or 6 boundaries failed to meet or exceed those controls" ADD R1.1 Severe VSL: "The Responsible Entity did not have documented procedural controls, or 7 or more boundaries failed to meet or exceed their documented controls." RATIONALE: Current VSLs do not match Low Impact requirement. AND CHANGE previous row R# "R1" to "R1.2..R1.6" CHANGE "R1.2..R1.6" High VSL: remove the phrase "OR The Responsible Entity has documented and implemented physical access controls, but does not initiate a response within 15 minutes of a detected unauthorized physical access into a Defined Physical Boundary. (Part 1.6)" RATIONALE: There is no corresponding 15-minute response requirement for initiating a response to unauthorized physical access alarms. R1.6 does not apply to the violation described, and although R1.5 does somewhat match, there is no time-limit on response for that sub-requirement.

Yes

No

R2.2 CHANGE: "identified source that addresses" TO: "identified source, that addresses" RATIONALE: Clarity from inserted comma ","

No

R3.5 CHANGE: append ", and disconnection." RATIONALE: Need to know the extent of time that Transient Cyber Asset was in contact with a BES Cyber System, in order to verify it met the definition of a Transient Cyber Asset. M3.5 CHANGE: append ", and when they were disconnected as well." RATIONALE: Corresponding change to recommendation for R3.5.

No

R4.3 CHANGE: "calendar" TO: "business" RATIONALE: This standard's requirement will include small control centers with meager (0.5 –to- 2) support-staff. There is no need for weekend call-outs where non-operational event-logging has failed. Staffing demand is unreasonable for risk. R4.4 Measures REMOVE: "and records of disposition of security related event logs beyond ninety days up to the evidence retention period." RATIONALE: If the concern here is guarding Protected Information, it is addressed within CIP-011-1. If the concern is proof of prior existence, solely for audit purposes, this measurement is too onerous for the risk being managed, and the current 90-day records are sufficient.

No
R5.5.1 CHANGE: reword as “Minimum Password length of at least 8 characters, or maximum supported by the BES Cyber System if less than 8 characters is supported.” RATIONALE: Clarity R5.5.3 CHANGE: “based on” TO: “based upon” RATIONALE: grammatical
No
CHANGE R1 through R5 VSL for Medium Impact Assets MOVE R1 through R5 Medium Impact Assets High VSL text to Medium VSL column MOVE R1 through R5 Medium Impact Assets Severe VSL text to High VSL column CHANGE R1 through R5 VSL for Low Impact Assets (R5.4) MOVE R1 through R5 Low Impact Assets High VSL text to Low VSL column MOVE R1 through R5 Low Impact Assets Severe VSL text to Medium VSL column RATIONALE: align severity with risk
Yes
No
R2.1 DELETE: “when incidents occur” RATIONALE: grammatical CHANGE: “recording” TO: “notation” RATIONALE: While important to keep post-mortem notes of steps followed or omitted, “recording” implies notation of time with steps taken or time and rationale when a step is omitted, with the focus upon making certain those actions/decisions were accurately recorded. While this is reasonable during planned tests, a facility under cyber-assault is less likely to have the same luxury of time and there is no risk to after-the-fact annotations being performed by the response team. R2.1 Measures CHANGE: “documentation” TO: “follow-up documentation” RATIONALE: See rationale for accompanying suggested R2.1 change above.
Yes
No
MOVE R1 through R3 Low Impact Assets High VSL text to Low VSL MOVE R1 through R3 Low Impact Assets Severe VSL text to Moderate VSL RATIONALE: Align risk with severity CHANGE R3 VSL Low Impact Assets VSL: "30 calendar days" TO R3 VSL Low Impact Assets VSL: "60 calendar days" APPEND R3 VSL Low Impact Assets VSL: to last sentence "within 60 calendar days" RATIONALE: Consistency and align timeframe with Severity. (Failure to review within 30 days might be considered High, and written into that column – see note on Low Impact Asset VSLs above.)
Yes
No
R2.3 Guidelines ADD: Better guidelines. RATIONALE: Without some related guidelines, the phrase “in a representative environment that reflects the production environment” introduces too much ambiguity and opportunity for disagreement between Responsible Entities and Auditors. “SEE FAQS AND CIPC GUIDELINES” seems inconsistent with the quality of product being produced in other CIP version 5 standards.
Yes
No
MOVE R3 Severe VSL text to High VSL ADD R3 Severe VSL: With 60 days violation. RATIONALE: align severity with risk.
Yes
Yes
No
R3.1 CHANGE: “Initially” TO: “Prior to or upon” RATIONALE: industry flexibility in timing R3.2 CHANGE: “Initially" TO: “Prior to or upon” RATIONALE: industry flexibility in timing R3 Guidelines (page 28) CHANGE: “should not that” TO: “should note that” RATIONALE: correction
No

R1 High VSL – Remove: “OR The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, and the execution status of the mitigation plans.” Rationale: remove double-jeopardy, where other standards and/or requirements were violated because something went wrong with planned changes to the baseline
No
R1.3 CHANGE: "Initially" TO: "Prior to or " RATIONALE: industry needs flexibility in timing
Yes
Yes
No
In all Implementation Plan occurances throughout these Standards and Implementation Plan CHANGE: “18 months” TO: “24 months”, including all other related wording RATIONALE: CIP Version 4 provides for 24 month implementation plan, yet CIP Version 5 is going to bring many more Responsible Entities into scope that have not formerly been acclimated to planning and accomplishing compliance with the NERC CIP Standards. It does not seem fair for those who already have acquired this level of expertise and experience, to impose an unreasonable timeframe on the uninitiated, just because we want Version 5 to eclipse Version 4. If our industry believes it best to move directly from version 3 to version 4 of the CIP standards, then we need to come up with a better mechanism than unfairly burdening these newcomers. <<<<OTHER CHANGES AECI SAW NO PLACE TO SUBMIT>>>> CIP-003-5 through CIP-011-x, A. Introduction, section 4.1.2, Bullet#1 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away. CIP-003-5 through CIP-011-x, A. Introduction, section 4.1.2, Bullet#2 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away. CIP-003-5 through CIP-011-x, Introduction section 4.1.2 Bullet#5 CHANGE: “Its Transmission Operator’s restoration plan” TO: “Its Transmission Operator’s formal restoration plan” RATIONALE: Avoid entities’ violating these standards, due to unforeseen restoration conditions that cause them to reasonably activate a restoration plan outside of their formal plan. CIP-003-5 through CIP-011-x, A. Introduction, section 4.1.6, Bullet#1 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away. CIP-003-5 through CIP-011-x, A. Introduction, section 4.1.6, Bullet#2 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away. CIP-003-5 through CIP-011-x, A. Introduction, section 4.2.2, Bullet#1 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away. CIP-003-5 through CIP-011-x, A. Introduction, section 4.2.2, Bullet#2 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away.
Group
CWLP
Roger Powers
Yes
"Large" Control Centers should not equate to functional responsibility rather impact on reliability. TOP can be an entity with less than 100 miles of 138 kV transmission. BA function can refer to small subset of BA role when entity participates in an organized market environment. There is a need to clarify how the LBA function in MISO fits with the definition. BES Cyber System uses the term "Maintenance Cyber Asset" which is not defined. Should it be "Transient Cyber Asset"? Does the 30 day reference in Transient Cyber Asset refer to consecutive days, days per year, days ever?
Yes
The Drafting Team has chosen not to define "generation control center" in item 2.13 and to distinguish control rooms from control centers. An approved definition is crucial to eliminate varying interpretations.

Yes
Yes
No
An entitiy should be allowed to designate more than one CIP Senior Manager as long as the division of responsibility is clearly defined.
Yes
No
In conjunction with the comment on the previous question, the approval should come from the appropriate Senior Manager where more than one is allowed.
Yes
No
An entitiy should be allowed to designate more than one CIP Senior Manager as long as the division of responsibility is clearly defined.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
The 30 day time frame for access privilege revocation is not sufficient for remotely located cyber assets.
No
The requirement for Low Impact BES Cyber Systems is too vague to be auditable.
Yes
Yes
Yes
No
It is unclear from the standard and associated definitions whether cameras are considered locally mounted hardware.

Yes
Yes
Allowing 45 days for remediation plan creation would facilitate compliance for smaller entities.
Yes
No
The timeframe for detection and response to event logging failure needs to be extended to the end of the next regular working day.
No
The timeframe for activating a response needs to be extended to the end of the next regular working day.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Southwest Power Pool Regional Entity
Emily Pennel
Yes
(1) The definition of BES Cyber Asset includes criteria where if it were unavailable, degraded, or misused, "would" adversely impact one or more BES Reliability Operating Services within 15 minutes. This criteria needs to be prospective and state "could" adversely impact. Without the criteria being anticipatory, entities could take the stance that the criteria calls for a 15-minute certainty and

therefore the Cyber Asset in question does not meet the criteria for BES Cyber Asset. The definition also includes a timeframe qualifier that references sending or receiving "instructions to operate." This qualifier is too narrow. Entities may take the stance that the BES Cyber Asset must be directly involved in a supervisory control function and would eliminate non-supervisory control systems, including those providing situational awareness, from designation as a BES Cyber Asset. The definition of BES Cyber Asset also includes a statement that redundancy shall not be considered when determining availability. This statement should be modified to state "redundancy shall not be considered when determining potential impact or availability." (2) The third bullet in the definition of BES Cyber Security Incident should be modified to state "Results in 'attempted or actual' unauthorized physical access..." (3) The definition of BES Cyber System includes a statement that a "Maintenance Cyber Asset" is not considered a part of a BES Cyber System. This term, which is also used within several CIP Version 5 Standards requirements, is not defined in the definitions document, and appears to be used interchangeably within the standards with the term Transient Cyber Asset. One term should be adopted and used consistently. (4) The BES Cyber System Information definition includes a reference to "floor plans that contain BES Cyber System Impact designations." The reference to impact designations is unnecessary and alters the wording of this example of information to be protected found in previous versions of CIP-003/R4.1. The reference should be modified to state "floor plans that include BES Cyber System or BES Cyber Asset details." Similar treatment should be given to the reference to equipment layouts. The definition would also be improved by modifying the opening statement to state "Information, about one or more BES Cyber Systems or BES Cyber Assets, that include 'but are not limited to' one or more of the following." (5) The definition of BES Reliability Operating Services includes a reference to "operations planning horizon." This and other timeframe terms are used throughout the Version 5 standards. These terms need to be defined, either in the NERC Glossary or by reference to a NERC published document containing the definition. (6) The definition of Cyber Assets has been modified to eliminate communication networks from the definition and to add the qualifier "in those devices" to the specification of "data" in the definition. This revision suffers from two shortcomings. First, the elimination of communication networks from the definition could be misconstrued by the entity to now exclude networking devices (switches, routers, etc.) from identification as a Cyber Asset requiring protection if within the Electronic Security Perimeter. Additionally, the exclusion eliminates the expectation to protect data in motion within the confines of the Electronic Security Perimeter. This is a step backwards from the current version of the CIP standards and does not incorporate a FERC approved interpretation of CIP-006-3/R1.1 into the new standards. (7) The definition of Defined Physical Boundary ("DPB") is sufficiently non-specific as to potentially afford no protection at all. The DPB definition should clarify that the DPB needs to be designed to deter and detect unauthorized access. As currently written, a climbable fence with a locked gate, possibly in concert with an unmonitored substation control house could be construed as meeting the definition. The climbable fence is not a deterrent regardless of the locked gate and the unmonitored control house, while possibly a deterrent, will not serve to detect unauthorized entry. (8) The definition of Electronic Access Point ("EAP") includes references to "routable or dial-up communications" that could be construed to eliminate non-routable (e.g., RS-232 serial communications) from consideration. The definition could also be construed as meaning every network interface on every Cyber Asset within a defined Electronic Security Perimeter because of the "between Cyber Assets" terminology. It may be preferable to modify the definition to define the EAP as "an interface on a Cyber Asset that restricts or controls the exchange of data between Cyber Assets within the Electronic Security Perimeter and external Cyber Assets or networks." The ultimate intent to eliminate the requirement for protective controls from certain boundary crossing points can be readily handled through the application of the requirement to "Electronic Access points with External Routable Connectivity", "Associated Electronic Access Control or Monitoring Systems", and the inclusion of dial-up in an applicability reference. (9) The definition of External Connectivity also eliminates the consideration of serial communications. As the use of serial connectivity does not necessarily impede malicious access to a Cyber Asset, it is not appropriate to exclude serial connectivity from the definition. (10) The definition of External Routable Connectivity takes an outside-in only view of network communications. This is overly limiting in that network communication is two-way. Any Cyber Asset that can reach out to an external network has external connectivity and once the outbound connection is made, the external cyber system being reached out to has external connectivity back to the BES Cyber System. If the intent is to eliminate Data Diode controlled (single direction) connectivity from the need for protective controls, clarify the definition accordingly to state that external connectivity is limited to two-way communication. (11) The

definition of Interactive Remote Access can be read to mean that the use of an Intermediate Device sitting outside of the ESP is not Interactive Remote Access and thus anyone going through the Intermediate Device is not subject to the applicable requirements of the Version 5 CIP standards. It would be better if Interactive Remote Access was defined more traditionally and then require the use of the Intermediate Device for any such access. (12) The definition of Intermediate Device states that the device "may be located …" The definition should be modified to clarify that the Intermediate Device must reside outside of the ESP, either as a part of an Electronic Access Point or in a DMZ network. In addition, the definition would be helped by a comment that the Intermediate Device is also subject to certain protective controls of the CIP Version 5 standards even though it resides outside of the ESP. (13) The definition of Protected Cyber Asset defines that Cyber Asset as being connected via a routable protocol. This qualification is not appropriate. It is common for relays and other devices in a substation or generating plant to be serially connected to a communications processor or a serial-to-Ethernet protocol converter module. These devices, if not designated as BES Cyber Systems or BES Cyber Assets, are still reachable and potentially configurable via this non-routable connectivity and need to be included in the definition of Protected Cyber Asset. The type of connectivity is immaterial. (14) The definition of Reportable BES Cyber Security Incident should be reworded to refer to any BES Cyber Security Incident that has "attempted to or successfully" compromised or disrupted a BES Reliability Operating Service. It is important for the ES-ISAC and appropriate governmental agencies to be aware of attempted cyber attacks as part of their intelligence gathering operations. Knowledge of unsuccessful attempts may be the key to preventing a successful attack. (15) The definition of Transient Cyber Asset specifies that the device may be connected for a period of 30 calendar days or less. This is an arbitrary length of time and could afford an entity an opportunity to misuse the definition to their advantage. The definition would be better served by stating that the Transient Cyber Asset is "temporarily connected to a BES Cyber Asset or Protected Cyber Asset for the specific purpose of data transfer, active maintenance, active troubleshooting, or vulnerability assessment, and is promptly disconnected when such activity is complete." The fact that the device is capable of altering a configuration or introducing malicious code is immaterial to the definition and should be removed. In addition, the definition would be helped by a comment that the Transient Cyber Asset is also subject to certain protective controls of the CIP Version 5 standards.

Yes

Comments: (1) A number of criteria qualify with the term "would" adversely impact one or more BES Reliability Operating Services. The criteria should be prospective in nature and should use the term "could" adversely impact. Without the criteria being anticipatory, entities could take the stance that the criteria calls for a 15-minute certainty and therefore the criteria in question is not met and the BES Cyber Asset or BES Cyber System is excluded. (2) Criterion 1 includes the phrase "and located at." Entities could seize upon this nuance and determine that, for example, a BES Cyber Asset or BES Cyber System housed in a centralized data center and used by a geographically separate control center is not "located" at the control center and therefore is excluded. Either the BES Cyber Asset or BES Cyber System is used to perform the specified BES Reliability Operating Service or it does not. If it does, where the asset is located is immaterial. (3) The High Impact Rating criteria does not consider the inter-connected nature of the BES Cyber Assets or BES Cyber Systems when defining threshold-based criteria. BES Cyber Assets and BES Cyber Systems that interconnect with similar systems in other Control Centers should be afforded a High Impact Rating regardless of the "span of control" of other BES Cyber Assets and BES Cyber Systems supporting that Control Center. (4) Criterion 1.4 does not consider an aggregate span of control. A generation control system could theoretically control 15,000 MW of generation without a single asset meeting the thresholds defined in the referenced criteria. The overall span of control of the BES Cyber Assets and BES Cyber Systems need to be considered by aggregating the field assets being controlled. (5) Criterion 2.5 is confusing and requires the examples found in the application guideline documentation to understand. The criteria might be improved by stating any part of the cranking path between the black start generation resource and the unit to be started where there is no diversity is designated a Medium Impacting Facility. Additionally, the fact that the black start resource may be used to start multiple units does not mean the "last mile" path to each of the units should be excluded. If the unit must be started as part of initial system restoration as defined in the TOP-005 system restoration plan, the path needs to be protected all the way to the unit. If the plan includes "if-then-else" options (e.g., start unit 1, if cannot start unit 1 then start unit 2, etc.), the first option should be the one protected. (6) Criterion 2.7 specifies a floor of 200 kV. In certain parts of the country, the 200 kV floor is too

high. Within the SPP Region, the transmission backbone is 161 kV. Setting the floor to 100 kV is more appropriate and reflects the current and new definition of the Bulk Electric System (refer to the definition of Bulk Electric System resulting from the work of Project 2010-17).
No
Due to a lack of a specific opportunity to comment on overall issues with the standard, please accept and consider the following comments in addition to comments specific to Requirement R1. (1) Previous versions of the CIP standards are applicable to Transmission Service Providers. CIP Version 5 is not applicable to the TSP function. It is not clear why the TSP function was dropped from the list of Responsible Entities. (2) Exemption 4.2.4.2 should specifically exclude communication end points from the exemption. Addition of this exclusion would be consistent with previous versions of the CIP standards. (3) In the background discussion, a comment is made that malware protection applies to a system as a whole and may not be necessary for every individual device to comply. While the intent to eliminate nonsensical requirements that ultimately require Technical Feasibility Exceptions is reasonable, how is compliance with this requirement determined? As written, an entity could theoretically install network-based malware protection at the network perimeter, ignoring the BES Cyber Assets, and be considered compliant (and protected) under this provision. In reality, network-based anti-malware is only one aspect of malware protection and is completely ineffective for malware not introduced over the network or introduced within a protected network where the configuration of the network allows traffic to pass between Cyber Assets without inspection. (4) Similarly, the grouping of BES Cyber Assets into a BES Cyber System seems to be permitted without any consideration criteria. How will differences of opinion between the entity and the auditor be resolved, or is the auditor obligated to accept any configuration, regardless of how nonsensical the configuration might be? (5) The term "would" adversely impact one or more BES Reliability Operating Services is used in the background discussion. The criteria should be prospective in nature and should use the term "could" adversely impact. Without the criteria being anticipatory, entities could take the stance that the criteria calls for a 15-minute certainty and therefore the criteria in question is not met and the BES Cyber Asset or BES Cyber System is excluded. (6) The Categorization Criteria states that Requirement R1 only requires the discrete identification of BES Cyber Systems and BES Cyber Assets for those in the High and Medium categories. Everything else is considered Low Impact. As discussed in the June 2011 SDT meeting with the regional CIP auditors, the entity will still need to enumerate all BES Cyber Systems and BES Cyber Assets in order to demonstrate the High and Medium BES Cyber Systems and BES Cyber Assets have been properly categorized. (7) The Rationale for R1 refers to "impact." It should refer to "potential impact." (8) R1 specifically states that Low Impact BES Cyber Assets and BES Cyber Systems do not have to be discretely identified. The accompanying Measure M1 states that evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls. This aspect of the requirement renders the overall requirement unauditable. If the entity only has to enumerate the High and Medium Impacting systems, the entity has insufficient evidence to demonstrate all High and Medium Impacting systems have been properly categorized. The entity must be able to demonstrate those systems that default to the Low Impact category are, themselves, properly categorized and should not have been categorized at a higher rating. It is not appropriate to advise the entity in the requirement and accompanying measurement that all assets and systems remaining after the High and Medium Impact categorization are assumed to be properly categorized as Low Impact systems. (9) Requirement R1.1 refers to the intention for the BES Element or Facility to be in service for more than six calendar months. The converse is an element or facility intended to be temporary in nature and in service for less than six months. The entity should be required to document the intent in that instance to allow the auditor the latitude to accept intent over actuality in the case where the BES Element or Facility was in service for more than six months due to unforeseen circumstances.
Yes
The requirement is agreeable with the understanding that "upon the effective date" used throughout the CIP Version 5 standards means "on or shortly before the effective date" and that the entity does not have to perform the initial activity on the precise effective date to be compliant. Read strictly, the use of the term "upon the effective date" could be misconstrued as requiring the action to be performed on that very date.
No
Percentages of non-compliance are difficult to determine; using discrete numbers of non-compliant assets would be preferable in determining the R1 VSL. This is particularly true where random

sampling of the entity's assets is performed and the number of failures is derived by extrapolation. Additionally, the R1 VSLs refer to entities with more than 100 High and Medium Impact BES Cyber Assets (or 100 or fewer such assets). Is this count determined by the entity's determinations prior to the audit or is the count determined by the auditor, adjusting the entity's initial determination upon finding a possible violation? Finally, the standard refers to BES Cyber Systems as well as BES Cyber Assets. It appears that the VSL requires the compliance monitoring and enforcement staff determining the VSL to break down each BES Cyber System into its BES Cyber Asset components in order to achieve the correct determination. As the bright line criteria remove any subjectivity from the categorization process, the R1 VSL should be binary. Either the entity got it right or the entity did not. There should be only one VSL, that being "Severe." Similarly, the R2 requirement is very straightforward and a binary VSL is appropriate in that instance.
No
Although the definition of CIP Senior Manager refers to a single person, this requirement should be clarified that a "single" CIP Senior Manager is to be appointed. The appointment documentation needs to be specific as to its intent to preclude instances where a policy document refers, for example, to the CEO of the company as the Senior Manager and a years-old set of minutes from a Board of Directors meeting naming the CEO serves to complete the "compliant" documentation of the appointment. Additionally, delegations should have the same level of documentation as the Senior Manager. As delegations can be by position or name, why not allow the CIP Senior Manager to be designated by position or name and not specify just the name of the individual. There is a greater likelihood of multiple staff in a large company with the same name and it is less likely that multiple senior staff will have the same company position at the same time.
No
To be auditable, the requirement should specify the minimum level of detail expected. Otherwise, an entity could simply state in the policy, for example, that "we will protect all BES Cyber Systems" and the auditor would have nothing to objectively base a compliance determination upon. The guidance documentation suggests a certain level is desired, however, the auditor must audit to the strict language of the requirement and not to the language in the guidance document.
No
The requirement should be clarified to explicitly require documents (company policies, procedures, etc.) referenced in the CIP cyber security policy(s) to be included in the review and approval actions. Additionally, the suggested evidence in Measure M3 (2) should include electronic approvals as well as a wet ink signatures.
No
This requirement is not auditable as written and is duplicative of CIP-004-5/R2. The suggested evidence in the Measurement section clearly shows the intent of the requirement is that the policy documentation be available to personnel with access to BES Cyber Systems. While it is possible to audit the measurement criteria, the requirement itself requires staff to be "aware" of the policies appropriate to their job responsibilities, not that the policy documents be published in electronic or hardcopy form or the staff be aware of where they might access the documents. The training/awareness issue is already addressed by another requirement. Auditing that the staff is "aware" in this context is not practical. Recognizing the intent is to no longer require a complete set of policies be made readily available to anyone with physical or electronic access, the requirement might be improved by requiring the policy documents be published and that personnel with electronic access to BES Cyber Systems or BES Cyber Assets be advised where they might access the policies if needed. For the small number of staff with physical-only access, the CIP-004-5/R2 training should be all that is required. Similar to current practice, providing a copy of the appropriate policies to contractors and vendors and deeming them to have been appropriately published with a presumption (or a required confirmation from the contractor/vendor company) that contractor/vendor personnel are then told where or how they can access the information should be acceptable. With respect to the Measures, all but the last bullet (training documentation) are appropriate. The measures can be improved by requiring the published documents be maintained up-to-date. There should be no expectation that the published policy documents be customized such that there is a "janitor" bulletin board and a different "SCADA support engineer" bulletin board or Intranet posting.
No
The requirement stipulates that the delegate may be identified by name or position. The first and

third example measures indicate a document listing personnel by title is acceptable evidence. This does not comport with the strict language of the requirement. A title may or may not be the same as the position.
No
Allowing 30 days to document a change to the CIP Senior Manager or a delegate is excessive and unnecessary. Typical practice as demonstrated in past audits is to announce the appointment via documentation with a same or future effective date and the standard should adopt that practice. Past experience has shown that it is difficult to impossible to verify a change was documented within 30 days of the actual appointment, making this aspect of the requirement unauditable. All the 30-day provision allows is for the entity to recover from an improper approval by quickly appointing the signing person as the CIP Senior Manager or delegate, similar to back dating a check.
No
The VRF for R5 (delegations of authority) should be "Medium", the same as the appointment of the CIP Senior Manager. The VRF for R6 (change in leadership or delegation) should also be "Medium" since the documentation of a change carries the same importance and impact as the original appointment. The binary VSL for R1 includes language ("single senior management official") not currently found in the requirement itself. The VSLs for R3 do not include the conditions where the policy documents were approved without any evidence of review and where some but not all of the policy documents were reviewed prior to approval.
No
Part 1.1 is vague and leaves the program entirely up to the entity with minimal guidance. As such, the auditor is left with only verifying that the entity did something each quarter, whether meaningful or not. The requirement now removes the expectation to reach the personnel with access to the protected systems, further weakening the requirement to the point of adding no value to the security program. Part 1.1 would be greatly improved if there was a requirement to reinforce the cyber security policy and to demonstrate that the awareness materials were accessible to personnel with access (e.g., placement of posters, means and locations of publishing electronic security awareness information).
No
The main requirement statement specifies that the entity will now have a role-based training program. This is a stronger statement than previous versions of the standard and could be construed as no longer permitting a common training program for all personnel. This will require entities to customize training to individuals or classes of personnel with access. For example, the operators will need different training from the software engineers who might, in turn, need different training from system administrators and supervisory personnel. Parts 2.1 through 2.10 should be applicable to Associated Physical and Electronic Access Control and Monitoring Systems and Associated Protected Cyber Assets. The reason for this recommendation is that Requirement R3, which implements the R2 training program, is applicable to the associated systems. The requirement to develop a training program should be applicable to the same Cyber Assets as the requirement to conduct such training. Part 2.1 should require the defined roles to be mapped to the training topic areas defined in Parts 2.2 through 2.10, otherwise, the accompanying measure stipulates evidence not required by the language of the requirement. Part 2.2 should stipulate whether the training on security controls is for physical controls, electronic controls, or both. Because of the requirement for role-based training, it may be necessary to split Part 2.2 into two parts, one for physical security controls and one for electronic security controls. Part 2.7 should emphasize that training should cover the identification of any potential BES Cyber Security Incident and not only those that would be deemed to be reportable.
Yes
No
Parts 4.1 through 4.4 should be applicable to Associated Physical and Electronic Access Control and Monitoring Systems and should be considered for Associated Protected Cyber Assets. The wording of Part 4.1 states an "initial" personnel risk assessment is required that includes identity verification. Part 4.2 does not include a similar reference to "initial" making it unclear whether both elements are required initially and then every seven years thereafter. Part 4.1 calls for identity verification but does not define any minimum expectations as to what identity verification entails. Would it be acceptable, for example, to accept a library card as proof of identity? The US Government has identified through

the use of the DHS I-9 form and instructions a number of identity artifacts that can be presented to confirm identity. The Canadian and presumably the Mexican governments have similar defined expectations that were used in the development of an interpretation request. Those government-accepted proof-of-identification documents should be stated as appropriate for the purposes of this requirement. Part 4.2 prescribes that the background check must be conducted for all locations where the individual has resided, been employed, and/or attended school for six months or more. This requirement should be clarified that "employed" or "resided" includes those locations where a long-term (six-month or longer) onsite contract engagement was performed. Part 4.3 requires criteria or a process to be used to evaluate the personnel risk assessment results to determine if access is to be denied. This requirement is vague and begs the question: would "to be determined on a case-by-case basis" be sufficient to demonstrate compliance? Part 4.4 is similarly vague. Is the entity now required to perform the personnel risk assessment on the contractor/vendor staff? Does the entity have to formally approve the contractor/vendor's program? Does the entity have to see the results of the personnel risk assessment performed by the contractor/vendor, which may be contrary to state laws and company policies? Does the verification process include evaluation of the contractor/vendor's disqualification criteria and that the criteria were properly applied in all instances?

No

The measures for Part 5.1 should include documentation of the CIP Exceptional Circumstances in the event access is granted before a personnel risk assessment is performed. Allowing the personnel risk assessment to be updated every seven "calendar" years could permit the entity to go as long as nearly eight years between assessments. There is no reason an entity cannot plan ahead and renew a personnel risk assessment on or before the seventh anniversary of the current assessment. The requirement should be modified to require the renewal on or before the seventh anniversary. Additionally, the Evidence Retention section should be modified to prescribe that personnel risk assessment documentation shall be retained at least until completion of the first compliance audit following the expiration or renewal of the personnel risk assessment.

No

The rationale for R6 states that the requirement of CIP-004-4/R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access. From an audit perspective, the entity still needs to be able to demonstrate that everyone with access is known and accounted for. During an audit, the entity will be required to produce a list of every individual with electronic and/or unescorted physical access for sampling purposes and will be required to demonstrate that list is complete in all respects, including that the access and associated access rights were properly authorized. How the entity maintains or creates the list is up to the entity. The rationale section should be updated to make that expectation clear to the reader. The second example evidence defined in the Measures for Part 6.1 prescribes a signed document, workflow or email showing such persons have authorization. Any such authorization documentation needs to include the specific access rights that were authorized. Part 6.4 states that the entity must verify each calendar quarter that individuals provisioned for access were authorized for such access. This can still be interpreted as requiring a review of access rights to ensure the granted access rights were properly authorized. This does not appear to comport with the rationale statement where the quarterly review appears to be simply a review of individuals with access without regard to the actual access rights granted. Similarly, Part 6.5 requires an annual verification that all accounts/account groups or role categories and their specific associated privileges are correct and the minimum necessary for performing work functions. It is not clear from this statement if there is a requirement to verify individual personnel are properly granted such access to those accounts/groups/roles as opposed to verifying the rights on those accounts/groups/roles are correct. The same confusion exists with Part 6.6. It is not clear if this part requires verification that individuals have the proper access rights versus the access rights are properly defined or configured. The Measures for Parts 6.4, 6.5, and 6.6 do not always align with the language of the respective part requirements. The various parts of R6 need to be clarified to explicitly state when individual grants to access rights are to be verified and when access rights are to be verified as properly defined or configured without regard to individuals holding such access.

No

Part 7.1 should specify that physical, domain, and remote access is to be revoked at the time of termination. Domain access is currently missing. Revoking domain access, especially within the control center environment, is not a difficult task and helps ensure that should the terminated staff

gain network access, the individual cannot log onto the network or system. Part 7.2 needs to explicitly allow for an overlap transition period for transferred personnel. The losing and gaining managers should collaboratively determine an effective or "agreed to" date whereby prior access will no longer be required and is to be revoked. In the absence of this agreed to date, the auditor can only rely upon the effective date of the transfer as recorded by an HR personnel transaction, putting the entity at risk of a possible violation for failure to revoke access timely. Part 7.4 needs to be clarified to explicitly include application and database accounts. As written, the reader could inadvertently assume the requirement only pertains to domain and local operating system-level user accounts. Part 7.5 requires shared account passwords to be changed within 30 calendar days. This is excessive for any account in a control center environment and especially excessive and risky for shared accounts that are highly privileged (e.g., system administration accounts). The recommendation is to change the shared user account within the same calendar day for highly privileged accounts and within seven calendar days for lesser-privileged and field asset accounts. There is already a provision for extenuating circumstances to be applied if a much shorter time frame cannot be complied with (e.g., access passwords on relays and other BES Cyber Assets in field environments). Should there be extenuating circumstances, a completion date certain should be included in the extenuating circumstances documentation and passwords should be changed on or before the documented date. Allowing an additional ten calendar days is not necessary and without a date certain when the passwords will be changed, the entity could unnecessarily prolong the required activity for convenience. Additionally, the application guideline for Requirement R7 states that no action is required in the instance of the death of the access holder. While "immediate" action might not be required, access still needs to be revoked sooner rather than later. Also, the application guideline for Requirement R7 states "For transferred or reassigned individuals, the requirement states a review of access privileges must be performed." Parts 7.2 and 7.5 of the requirement imply, but do not explicitly state such a review is required. Additionally, the requirement needs to address the revocation of access to BES Cyber Security Information associated with the transfer of reassignment of personnel. Part 7.3 only applies to resignations and terminations, and Part 7.5 (which applies to transfers) only addresses the need to change the passwords for shared user accounts.

No

Because of the risk in not promptly revoking access, the VRF for R6 should be Medium. The High VSL for R4 refers to "required documented results" and to Part 4.5. The documented results are a requirement of R5 and there is no Part 4.5. The Severe VSL for R6 refers to Part 6.7. There is no Part 6.7.

No

The requirement no longer requires the entity to discover previously unidentified electronic access points. This opens a potential risk point that needs to be addressed. It may be possible to accomplish this task as part of defining the system baseline configuration (CIP-010-1/R1), but the task needs to be explicitly required. Part 1.1 requires technical or procedural controls to "restrict" unauthorized electronic access. The intent of the term "restrict" needs to be explained. Part 1.1 and Part 1.2 potentially conflict if both types of systems are collocated on the same network. The requirement needs to assert Part 1.2 prevails in the instance of a mixed categorization environment. Part 1.4 is applicable to dial-up access for "non-interactive" Remote Access. The requirement to perform access authentication for non-interactive access and not also for interactive access appears to be nonsensical. It is not clear what the real intent of this requirement is. Part 1.5 requires a documented method for detecting malicious communications at each EAP. Malicious communications needs to be defined. Additionally, the requirement may be too narrowly focused. Detection of malicious communication can often be detected via Intrusion Detection/Prevention systems running outside of the EAP. The change rationale for Part 1.5 states that ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is mis-configured, and that Part 1.5 is an attempt to address that need. Part 1.5 fails in this endeavor in that Intrusion Detection Systems are detection systems and not protection systems. To achieve the expectations of the FERC Order paragraphs cited in the rationale, an Intrusion Protection System would be required.

No

Part 2.2 requires encryption for all Interactive Remote Access sessions. This is problematic if the terminus of the encrypted session is inside the ESP since packet inspection at the ESP border is not possible. It also makes little sense to require encrypted Remote Access sessions but not require encryption anywhere else, such as communications between systems in different ESPs (e.g., primary-

backup control centers, ICCP traffic between control centers).
No
The Severe VSL for Requirement R1 needs to be specific as to which systems are in focus of the first condition. Perhaps a Part number reference would be appropriate as has been used elsewhere in the VSLs for other standards.
No
Part 1.2 suffers from an insufficiently defined term "Defined Physical Boundary" (See the comments in response to Question 1, item 7). Part 1.3 requires the use of two or more "different and complementary physical access controls." This needs to be defined or at least the intent clarified. FERC's intent, as stated in Paragraphs 572 through 576, is to implement defense in depth such that the Cyber Systems and Cyber Assets continue to be protected in the event one of the control systems fails. The Application Guideline for Requirement R1 offers examples of compliant applications that include "card key and pin code" and "card key and biometric scanner." These examples fail if the two-factor authentication is managed by the same Physical Access Control System. The failure of that system would result in the simultaneous failure of both controls. A compliant application of this requirement might be a card key/magnetic lock or door strike system with a logged and alarmed key override system. The failure of the primary Physical Access Control System would keep the door locked and the key override system would provide access. The key override system, being alarmed and logged, continues to provide protection by providing immediate alerting in the event the key override is used. Part 1.6 is too restrictive in requiring logging by personnel who control entry when automated means are not used. This implies security personnel whose primary responsibility is to control physical access and would not necessarily include escorting personnel. It would be better to require manual or electronic logging of access without restricting the logging to security personnel. Additionally, the date and time of access should be recorded and not just the date of access in support of CIP-006-5/R2.
No
Part 2.1 should prescribe "Require 'and perform' continuous escorted access..." Part 2.2 is confusing and unnecessarily broad. Basing the requirement on a 24-hour basis could also lead to inadvertent logging failures. It would be better for the requirement to permit the logging of initial ingress and final egress and permit brief exit/reentry as long as the time between the exit and reentry does not exceed a prescribed time period. The intent would be for someone to be able to run out to their truck as discussed in the Application Guideline without having to log out and right back in. However, leaving for lunch, to pick up a part, or other prolonged period between the exit and reentry should be logged out and back in. The suggestion is to log the visitor out and back in if the visitor is out of the DPB for more than 15 or 30 minutes and to not consider a visitor to have exited a DPB when traversing through successively layered perimeters (e.g., having to go through the control room DPB to enter the computer room, a separate DPB.
No
Maintenance and testing of Physical Access Control Systems can and should be performed far more frequently than once every 24 calendar months within routinely occupied facilities such as the primary control center. The suggestion is to require monthly testing in routinely occupied facilities. Part 3.1 specifies that the Physical Access Control System must be tested prior to commissioning and at least once every calendar 24 months thereafter. The requirement also needs to require that testing of the controls needs to be performed on or before the effective date of the CIP Version 5 standards to avoid the "book marking" issues seen with previous versions of the CIP standards.
No
The second condition of the High VSL for Requirement R1 includes the failure to initiate a response within 15 minutes of a detected unauthorized physical access. The 15 minute criterion is not specified in the language of the requirement itself. This condition also references Part 1.6, which does not appear to be correct. Part 1.4 is more applicable to this condition.
No
Part 1.2 should also be applicable to Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems.
No
Part 2.1 permits the entity to choose one or more sources for monitoring the availability of security

patches. The Change Rationale indicates that this could include the SCADA system vendor that "certifies" a patch before the entity can install it. There is a difference between "availability/applicability" of a patch and the ability to "install" a patch. The risk begins when the vulnerability is identified and may or may not coincide with the initial availability of a patch from the source vendor. There are a number of patch consolidation sources in addition to original patch providers that can be monitored. Allowing the entity to rely upon the SCADA or other vendor to "certify" a patch before it is considered available is an unnecessary delay and increases the risk to the reliability of the BES. If the vendor, for example, does not certify a patch for several years (if at all), the entity under this process has no expectation of addressing the vulnerability at all. As demonstrated by past history, the majority of cyber systems infected with malware are compromised because an available security patch was not installed. The certification, accompanied by the entity's own testing, determines if the patch can be installed. Regardless, the patch is applicable and available and compensating measures need to be adopted to address the vulnerability in the event the patch cannot be installed. The current practice of some vendors is to only report out "certified" patches against the current baseline product, which means some available and applicable, perhaps not installable patches will be overlooked. The requirement would be better if the entity was required to monitor the availability of a patch from the original provider, either by monitoring that vendor's site or by use of a vendor-agnostic patch monitoring service. The entity should only rely upon the application vendor if that vendor customizes and re-releases the security patch originally provided by a different vendor. Once the patch has been identified as available and determined to be applicable, the entity can and should wait for their application system vendor to certify the patch as compatible with their system. Part 2.3 needs to specify a remediation time frame where the patch is implemented or compensating measures are implemented pending the installation of the patch. The vague wording of this requirement would allow, for example, an entity to define a remediation process whereby the security patches are only installed as part of a system replacement once every several years. The suggested remediation timeframe is 30 calendar days after a patch is determined to be applicable for BES Cyber Systems in a control center and the next scheduled outage for plants and substations, with a requirement to implement compensating measures in lieu of the patch within 30 days of the patch availability whenever possible in the plants and substations. The provision for CIP Exceptional Circumstances can address the outlier issues.

No

This requirement needs to adopt and use common terminology, either the already defined term "Transient Cyber Assets" or the currently undefined term "Maintenance Cyber Assets." The term "Maintenance Cyber Assets" is used in the Rationale for Requirement R3. The vagueness of Part 3.1 could result in either a very subjective audit or potentially ineffective "compliance." For example, is the deployed method appropriate for the system to be protected? Is a perimeter-based solution, such as a network-based anti-virus or Network Intrusion Detection/Prevention System sufficient? Part 3.2 needs to define a timeframe in which malicious code is to be disarmed or removed. As written, the entity could effectively ignore the malware, citing a future plan or process to perform the required disinfection. Part 3.3 specifies malicious code protections shall be updated within 30 calendar days of the signature or pattern update. This is excessive, especially in a control center environment, where such updates are frequently provided by the anti-malware vendor in response to emerging threats. The signature files can typically be downloaded, tested, and rolled out to production within a couple of days of the release of the update. This requirement also suffers from the elimination of the requirement to "test" the update before rolling it out into production, although the Application Guideline for R3 still refers to testing prior to implementation. Past experience has demonstrated that anti-malware updates occasionally return a false-positive and have crippled systems in the past as a result of the automated response of the anti-malware system to the "detected" problem. Part 3.4 needs to be modified to require methods to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media "prior" to connecting them to BES Cyber Assets or Protected Cyber Systems. The goal is to prevent plugging in a device already compromised with malware. Part 3.5 should be modified to log both the connection and the removal of the Transient Cyber Asset. Logging the removal demonstrates the transient nature of the connection.

No

Part 4.1 requires the entity to log generated events. The Measures should include evidence that the logs are being generated with the appropriate information. Having a listing of what is to be logged is not the same as demonstrating the logs are being generated. Part 4.2 implies an automated system is

required in order to generate "real-time alerts." Allowing the entity to determine what it feels are required real-time alerts, with no minimum set of expectations, is a meaningless requirement. The auditor will either perform a highly subjective audit, or the auditor will be obligated to accept whatever the entity has determined, even if the entity has determined that there is no need for any real-time alerting. The Measures accompanying Part 4.2 should also include examples of actual alerts demonstrating the monitoring system is properly configured and operating. Part 4.4 Measures suggest that records of disposition of security related event logs are required. The requirement is to maintain logs for the past 90 calendar days and the auditor will only seek evidence that the entity has at least 90 days worth of logs. Maintenance of disposition records does not directly support the language of the requirement. Part 4.5 permits sampling of logged events in lieu of a 100 percent manual or automated review. This is impractical for firewalls and other high-volume logging systems. The intent of the FERC order was to require a periodic manual review to confirm the automated Security Incident and Event Monitoring (SIEM) system was properly configured and not overlooking events of interest. A manual process where automation can be deployed increases the risk to the BES reliability. Additionally, should the sampling continue to be permitted as currently drafted, the requirement needs to define a minimum expectation as to sample size and procedure. Otherwise, the entity will have the latitude to devise a meaningless and insufficient review for convenience.

No

Part 5.4 permits a default password to not be changed if "the default password is unique to the device or instance of the application." This provision is nonsensical. Passwords need to be changed on a regular basis as mitigation from possible inadvertent disclosure or discovery. And, technically, whoever set the initial password has knowledge of that password and thus access. Unless that individual is approved for access, the password needs to be changed to revoke the unauthorized access. Additionally, disabling or renaming system default accounts such as Guest and Administrator is good security practice and should continue to be required where appropriate and applicable. Part 5.5 already requires passwords to be regularly changed. Unconditionally requiring a default password to be changed prior to placing a system into service is good security practice and also affords the entity the opportunity to clearly understand and document the necessary procedure for changing the password on the device. Part 5.5.3 has removed the requirement to change the password at least annually and now permits the entity to specify its own time frame. This is a very vague requirement and will result in either a highly subjective audit or an obligation of the auditor to accept whatever the entity has defined, regardless of how nonsensical that time frame might be. The "where technically feasible" language has been removed, yet there may be instances where a password cannot be changed for valid technical reasons. The drafting team should consider restoring the technical feasibility provision. The VSL for this requirement already includes TFE language. Additionally, the measures for Part 5.5 include attestations that procedurally enforced passwords meet the password parameters. This is problematic to auditors as GAGAS does not permit the acceptance of attestations as primary evidence. Part 5.6 requires a failed password lockout or alert notification after an undefined number of failed attempts. The requirement needs to specify what is reasonable, perhaps with options including number of consecutive failed attempts and elapsed time before automatic lockout expiration.

No

Because of the risk, Requirement R2 should have a High VRF. The High VSL for Requirement R3 is essentially the same as the first condition of the Severe VSL, with the exception of applicability to Transient Cyber Assets. The Moderate and High VSLs for Requirement R4 are run-on statements that lose the required context. The last condition of the Severe VSL for Requirement R4 should include the specific requirements stipulated in Part 4.1. The Severe VSL for Requirement R5 should include conditions for where the account use was not authorized by the CIP Senior Manager or delegate (Part 5.2).

No

Identifying criteria for reportable Cyber Security Incidents per CIP-008/R1.3 has been very inconsistent across entities to date. Part 1.2 does nothing to address this inconsistency because, like previous versions of the CIP standards, this requirement does not establish minimum expectations or criteria for reporting. Additionally, Part 1.2 has dropped the requirement to ensure reportable incidents are reported to the ES-ISAC. This requirement can be improved by restoring the requirement to report the incident and by providing minimum expectations for what is considered reportable.

No
The requirement statement in Part 2.1 is awkwardly worded and confusing. The requirement can be broken into two expectations: (1) follow the documented Incident Response Plan in the event of a BES Cyber Security Incident or plan test, and (2) Document the execution of the plan and any deviations from the plan during the response for future evaluation and possible plan update. Part 2.3 should require the entity to retain "all" relevant documentation. The accompanying Measure should provide examples of documentation, such as logs, police reports, e-mails, phone logs, voice recordings, response team member notes, response checklists, forensic analysis results, restoration records, and post-incident review notes.
No
Part 3.1 requires an update, if necessary, following the annual review of the BES Cyber Security Incident response plan. If the entity has properly complied with the requirements of Parts 3.3 and 3.4, the need for an update following the annual review should be negligible. To be compatible with the currently in effect CIP-008 and CIP-009 standards, Parts 3.2 through 3.5 should be applicable to Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems. Part 3.3 should be modified to require the update to be completed within 30 calendar days of completion of the annual review, test, or actual incident response. The current wording requires an update within 60 calendar days and only requires the update following the annual review. Part 3.5 allows 30 calendar days to distribute the updated BES Cyber Security Incident response plan to each person with a defined role in the response plan. Thirty calendar days is excessive. A seven calendar day period is suggested.
No
The High and Severe VSLs for R3 do not reflect relative significance of the documented failures. Failure to update a plan, whether or not reviewed, should be a Severe VSL. Updating the plan but not distributing the plan timely should be High, not Severe.
No
Part 1.1 only requires the conditions for activating the recovery plan(s) to be documented. In the absence of setting minimum expectations, an entity could define a recovery plan that is only activated in the event of a catastrophic destruction of all control centers (primary, backup, etc.) and be found compliant. The recovery plans need to address (1) single BES Cyber System/Asset failure, (2) combined failure of the primary and backup BES Cyber Systems/Assets at one location, (3) the combined failure of the primary and backup BES Cyber Systems/Assets at more than one location, (4) the loss of multiple BES Cyber Systems/Assets at one or more locations, and (5) the catastrophic loss of one or more facilities with accompanying loss of the BES Cyber Systems/Assets at those locations. Part 1.1 also does not require the entity to document the recovery plan steps themselves, which should be the most important requirement of any documented recovery plan. A documented recovery plan with recovery steps is required to perform the requirement specified in CIP-009-5/R2. Part 1.4 requires the backup media to be "verified." The requirement needs to specify what verification entails. Does verification simply entail looking at a log file to confirm the backup process did not fail? Does it involve performing the verification option step as part of the backup process? Does it require a separate step for cataloging the backup media to verify the media can be successfully read end-to-end? Or does it include steps to confirm all information required to successfully restore a system has been captured?
No
Part 2.2 requires the entity to initially and annually thereafter "test" any information used in recovery of BES Cyber Systems that is stored on backup media to ensure the information is usable and "reflects current configurations." Similar to the comments submitted against CIP-009-5, Requirement R1, Part 1.4, what does "test" mean? Does it simply require a step for cataloging the backup media to verify the media can be successfully read end-to-end? Does it include steps to confirm all information required to successfully restore a system has been captured? Or does it require a full restoration of the BES Cyber System from the media? What is meant by reflecting current configurations? And, most importantly, does each media set require testing (e.g., test after every backup cycle)? If not, what are the parameters for demonstrating compliance with this requirement? Part 2.2 needs to be significantly clarified before entities fully understand the requirement and auditors know how to evaluate compliance. Part 2.3 requires an operational exercise of each of the recovery plans initially and then every three years thereafter. Must every Cyber Asset or type of Cyber Asset be tested?

What if the recovery plan is generic and broadly stated? How many Cyber Assets need to be "restored" to adequately demonstrate the adequacy and completeness of the recovery plan?
No
Part 3.1 requires the recovery plan to be reviewed when BES Cyber Systems are replaced. In addition to replacement, the recovery plan should be reviewed following a major update of the BES Cyber System (e.g., hardware component addition or upgrade, network connection update, or major software revision level upgrade). A major update is less than a replacement, but could still change the system sufficiently to require modifications to the recovery plan. Part 3.3 requires recovery plans to be updated within 30 days of the review of the results from a recovery plan test required by Part 3.2. This requirement should also require recovery plans to be updated within 30 days of the plan review required by Part 3.1, if changes were identified.
No
The second condition of the High VSL for R2 (testing the recovery plan at least once every three years) should be a Severe VSL.
No
Part 1.1 should include an additional requirement (1.1.7) to document the cyber security (system hardening) controls. This is more than simply the configuration of ports and services already required. Part 1.2 needs to provide for both routine, planned changes where documentation and approvals can be obtained prior to implementing the change and for emergency (it is 2:00 AM and the system is down, must be fixed now) changes where documentation and approvals are taken care of after the fact. As currently written, the requirement could be interpreted as requiring documentation and approvals prior to any change implementation. Emergency changes as discussed in this comment do not fall into the CIP Exceptional Circumstances exemption. The prior version reference for Requirement R1 (all parts) should be CIP-007-4 to be consistent with the rest of the standards.
Yes
No
Parts 3.1, 3.2, and 3.3 need to define what a paper and an active vulnerability assessment is. The Application Guideline attempts to define these types of assessments; however the auditor cannot audit to the language of the guideline. The expectation needs to be clearly defined in the requirement itself. Part 3.3 should require an active vulnerability assessment prior to placing a new BES Cyber Asset, new BES Cyber System, new Physical Access Control System, or new Electronic Access Control or Monitoring System into service as well as adding a new BES Cyber Asset to an existing BES Cyber System or Electronic Access Control or Monitoring System as currently prescribed in the requirement. Part 3.4 requires an action plan to remediate or mitigate vulnerabilities identified in an assessment and the execution status of the action plan. To date, entities have struggled with understanding what this requirement entails. The requirement needs to clarify that the action plan needs to have measurable milestones similar to a mitigation plan associated with a compliance violation. The requirement should also require the execution status of the action plan to be updated/reported at least quarterly.
No
The VRFs for Requirements R1 and R2 should be Medium, not Lower. The third condition of the High VSL for R1 should be Severe, not High. The graduated VSL conditions (performance of the vulnerability assessment) should be combined and set as a High VSL. The failure to perform a required Part 3.1 or Part 3.2 vulnerability assessment prior to the effective date of the standard and the failure to perform a Part 3.3 vulnerability assessment prior to placing a new BES Cyber System or BES Cyber Asset into service should be Severe VSLs.
No
The requirement statement in Part 1.1 is too vague. To be auditable, the requirement needs to prescribe the definition of measurable criteria for identifying BES Cyber System Information. Additionally, the accompanying measures may demonstrate the outcome of the application of the prescribed identification methods, but the suggested measures do not directly support the requirement itself. Part 1.3 requires the entity to implement an action plan to remediate deficiencies identified during the assessment required by Part 1.3. The requirement needs to clarify that the action plan needs to have measurable milestones similar to a mitigation plan associated with a

compliance violation. The requirement should also require a quarterly update/report of the execution status of the mitigation plan.
No
Parts 2.1 and 2.2 need to require the documentation of the process steps comprising the action taken to destroy the media (required by Part 2.2) or to prevent the unauthorized retrieval of BES Cyber System Information from the media (required by Parts 2.1 and 2.2). To be consistent with the VSL conditions for Requirement R2, the requirement also needs to prescribe documentation of the media purge or destruction activity. Additionally, the requirement should prescribe that the media will be physically protected from unauthorized access until such time as the media is purged or destroyed, even if the media or the Cyber Asset housing the media has been taken out of service.
No
The High VSL for R2 covers the instance where the documented purge or destruction process was not followed. If the entity cannot demonstrate that the documented process was ever followed, the VSL should be Severe. High is only applicable if the procedures were followed for some, but not all purge or destruction actions.
No
In the Scenario of Unplanned Changes table, the last scenario (add 12 months to the above) should be simplified to state 24 months. The last paragraph of the Implementation Plan states "following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved." What is the time frame whereby the entity is expected to either demonstrate full compliance or file a self-report of non-compliance?
Individual
Shari Heino
Brazos Electric Power Cooperative, Inc.
Yes
Add a definition for Interactive Remote Access. Control Center should probably be defined just for CIP-002 or just for the CIP standards.
Yes
The standard should clearly identify who has authority to determine the level of granularity of systems identified. BEPC is concerned that the standard as drafted would allow an auditor to second guess its designation of systems and how they are protected. For Attachment 1, CIP-002: A GOP Control Center could end up being treated as High Impact after being run through the analysis of Section 2.1 and then 1.4 depending on how those sections are interpreted. A GOP Control Center should not be High Impact merely because it represents 1500MW or more. Section 2.13 wording problem first part of sentence does not grammatically fit with (2). Section 2.5, In ERCOT, black start units change every two years pursuant to a competitive selection process; therefore, black start cranking paths change every two years. This will lead to much expense and effort on the part of TOs for something that may only have a medium impact designation for two years (and, given the implementation plan, may only be compliant for one). Additionally, “initial switching requirements” is unclear.
No
See ACES Power Marking comments (joined by Brazos).
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No

See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
Role based training is acceptable; however, companies should not be prohibited from overtraining employees. It is sometimes simpler to train employees all together rather than create and schedule several different trainings.
No
See ACES comments.
No
See ACES comments.
No
Because of other legal requirements, it should be made clear that registered entities will not be required to hand over PRAs from third parties to auditors.
No
Segregation of duties might not be possible in smaller organizations.
No
See ACES comments. Also, under Measures #(ii), requiring a print of a system generated list every time there is a termination would be onerous. Next calendar day is not always reasonable because HR will often do terminations at 5pm on Friday; use next business day.
No
See ACES comments.
No
In the Measures for 1.1, change “and” to “or” (technical or procedural instead of technical and procedure).
No
See ACES comments.
No
See ACES comments. Also, the guidelines for R2 should be moved to the standard itself for clarity.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments. Also, provide an exception in 1.1 for software’s use of dynamic ports (e.g., any answering port).
No
For 2.1, clarify that sources that registered entity chose to use are acceptable. The entity is not required to use a source identified by auditor.

No
See ACES comments. Also, for 5.6, account lockout is a bad idea; alerting is a better option. Account lockout can be used to institute a denial of service to legitimate users.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments. Also: For 1.4: Define what is meant by “verified.” This could be an onerous process. For 1.5: This requirement should modified to only require data preservation where it does not cause additional system down time. Time limit of preservation of data should also be limited.
No
See ACES comments. Also, For 2.2: Remove the word “any” – this is overly broad. For 2.3: This requirement is too onerous. Testing in a test environment is very expensive. Generally, provide more clarification about the amount of testing to be performed (entire system?).
No
See ACES comments.
No
See ACES comments.
No
See ACES comments. Also: For 1.1.4 and 1.1.6: It is excessive to require a new baseline after every script or security patch. For 1.2: Change control already handles this process. It should not require CIP Senior Manager approval.
No
See ACES comments. Also, for 3.2, performing a vulnerability assessment in a test environment will provide little information of value. An assessment in the production environment should be allowed as well. Production environment assessments provide more useful information.
No
See ACES comments.
No
Clarify in the requirement itself that marking is not required for BES Cyber System Information information; only that the information is recognized as such. Some information is not in a format that allows easy marking of the information.
No
No
See ACES comments. ALSO, Brazos has some general concerns about the version 5 drafts as listed below: (1) Because guideline documents are not binding on auditors, guidelines should be part of standard if important. Guidance documents are also a hassle because they are one more place we have to look to find information. (2) Clarify that evidence lists in measures do not require an entity to have all types of evidence listed. (3) Where retention period is less than audit cycle, provide examples of alternative evidence other than actual logs, etc. that would demonstrate compliance for the entire

audit period. (4) Some requirements appeared to drop the 90 day logging requirements, possibly unintentionally. These time limits should be reinstated where appropriate.
Group
Progress Energy
James Eckelkamp
Yes
Agree with EEI comments for this question
Yes
Agree with EEI comments for this question and addition have this comment for section 2.4. The diverse and distributed nature of the Bulk Electric System necessitates a design that allows for multiple sources to restart the electric system in the event of a blackout. Due to the multiple combinations of restoration paths, selecting an initial path for system restoration from selected blackstart units would be more feasible in the development of a restoration plan with the flexibility of choosing other restoration paths in the absence of the initially designed restoration path. This does not preclude the need for additional blackstart capable units, but allows for reasonable protection of specific assets for system restoration without placing undue burden on protecting all blackstart assets. Proposed: We would recommend the critical asset definition as it pertains to blackstart units remain limited to those blackstart resources in the electrical path of transmission lines used for initial system restoration.
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
Yes
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
R4.2 Requirement should be effective on or after the effective date of the standard and not retroactive for personnel processed under previous revisions of the standard since this interpretation expands the scope of the PRA to include checks where the person was employed or attended school for six months or more.
Yes

No
Agree with EEI comments for this question with addition to: R6.4 –We had concern over the wording “calendar quarter”. Comment: define quarter; or + or – 30 days on quarterly measurement. R6.5 Original content: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions. Proposed content: The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity’s needs and appropriate personnel roles and responsibilities
No
Agree with EEI comments for this question
Yes
No
Agree with EEI comments for this question with the addition of the following change: Table 1.1 Change “and “ to “or” under Measures.
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question with these additional comments: Original content: Severe The Responsible Entity did not implement encryption to protect the confidentiality and integrity of all Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for all Interactive Remote Access sessions. Proposed content: Lower The Responsible Entity did not implement encryption to protect the confidentiality and integrity for 1-30% of Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for 1-30% of Interactive Remote Access sessions. Moderate The Responsible Entity did not implement encryption to protect the confidentiality and integrity for 31-60% of Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for 31-60% of Interactive Remote Access sessions. High The Responsible Entity did not implement encryption to protect the confidentiality and integrity for 61-90% of Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for 61-90% of Interactive Remote Access sessions. Severe The Responsible Entity did not implement encryption to protect the confidentiality and integrity of all Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for all Interactive Remote Access sessions.
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question 5.2 Evidence Retention Under CIP-006-5 Section C (Compliance) 5.2 it states that each entity shall retain data or evidence for three calendar years or the duration of any regional Compliance Enforcement Authority investigation; whichever is longer. Comment: Version 5 evidence retention criteria goes beyond retention requirements of the current standard. Propose that the legacy evidence retention requirements for CIP-006 remain intact. Extending retention requirements will significantly increase administrative burden and costs with no added value. • Access logs (manual and/or electronic) retained for a period of 90 days (unless related to a reportable cyber security incident) • Outage records regarding access controls, logging, and monitoring for a minimum of one year (unless related to a reportable cyber security incident)
No
Agree with EEI comments for this question with additional comment Table 3.1 Original Text: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided. Propose: After the effective date or prior to commissioning Physical Access Control System(s) used at a Defined Physical Boundary shall be tested at least once every 24 calendar months thereafter to ensure required alerting and control

functionality is provided. Entity shall provide maintenance as necessary to support Physical Access Control System(s) functionality. Rationale: This sub requirement cites maintenance and testing to be conducted “prior to commissioning.” In many instances controls may already be in place or will be expected to be in place prior to V5 adoption, therefore language is needed to capture existing devices in service at the time the standard becomes effective.
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question – but has this additional comment in the compliance section under 1.2 first bullet: Original content: Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer. Proposed content: Each Responsible Entity shall retain data or evidence for 1 year or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
Yes
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
Yes
No
Agree with EEI comments for this question

No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question with the additional sentences on the first paragraph in the comment section. The existing time frame of 18 months is seen as too short, given the extensive enhancements within the standards as a whole, and particularly specific to the likely addition of numerous Low Impact BES Cyber Systems that may not have been considered in scope for previous versions. In the event that Low Impact assets are a component of the enforceable requirements on day 1 it is likely that additional time would be required. We recommend a timeframe of no less than 24 months for high, medium, EACM's, PACM's systems or assets and more time required for low Impact BES Cyber Systems as scope in unclear at this point.
Individual
Joe Tarantino
Sacramento Municipal Utility District
No
• The term "BES Reliability Operating Services" in the definitions includes language that result in unintended over-reach in the standard. Specifically, the language "activities, actions, and conditions" is used in the definition of many services. This language may be interpreted to mean that the cyber assets used to control the climate control system of the control room in which the operator performs his or her duties is subject to regulatory compliance. Therefore, the language needs to be changed so that the reference is only to cyber assets that directly implement the services listed in "BES Reliability Operating Services".
No
• This requirement requires the responsible entity to identify and categorize its "BES Cyber Assets" and "BES Cyber Systems" by impact level according to the criteria defined in Attachment I. The criteria in Appendix I, in turn, refers to the impact based upon adverse impact to one or more "BES Reliability Operating Services". The term "BES Reliability Operating Services" is so broad that it essentially covers everything that a utility does. There is nothing left to not include. • The definition of "BES Cyber Asset" in the CIP Version 5 definitions qualifies "BES Cyber Assets" based upon the 15 minute criterion. In Attachment I, in the definition of the High and Medium impact levels, the term "BES Cyber Asset" is used in conjunction with the 15 minute criterion. This is logically inconsistent because the term "BES Cyber Asset" does not include assets that have already been excluded by the 15 minute criterion. • The 15 minute criterion does not apply to the vast majority of systems covered by the standard because power system apparatus and computer systems generally operate in the time frame of five seconds or less. • Throughout the Application Guidelines language includes the following statements "Activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions." For example in "Situational Awareness" this language may be interpreted to mean that the cyber assets used to control the climate control system of the control room in which the operator performs his or her duties is subject to regulatory compliance because it determines the environmental conditions in which the operator performs the function of awareness of system conditions. Therefore, the language "Activities, actions and conditions" needs to be changed so that the reference is only to cyber assets that directly implement the services listed in "BES Reliability Operating Services". • The Low Impact Rating (L) definition is much too broad because it includes "All other BES Cyber Assets and BES Cyber Systems not categorized in Section 1 as having a High Impact Rating (H), or Section 2 Medium Impact Rating (M)." The CIP Version 5 standard needs to be written in a way that clearly limits its scope to assets that have significant impact to Bulk Electric System operation. We propose a defined Low Impact Rating as having minimal impact and create a "No Impact Rating" for all remaining BES Cyber Assets and BES Cyber Systems.
No
• The BES Reliability Operating Services encompasses everything a utility does. If this definition were used, it would encompass all assets. • The term "BES" is not defined in CIP standard Version 5. Definition of this term is crucial because it defines the scope to which the standard reaches. NERC is

in the process of defining the BES term in its NERC Project titled “2010-17 Proposed Definition of Bulk Electric System and Related Rules of Procedure Team”. While it will be possible to reference this external definition in the CIP standard, entities would become instantly non-compliant in the event that the external definition changes.
No
• How will FERC / NERC help the Utility Industry to have the authority necessary to conduct a broader and a more comprehensive Criminal History Records Check (CHRC) such as through the Federal Bureau of Investigation (FBI) that is a National check to ensure that individuals do not circumvent the process?” These types of comprehensive FBI CHRC are being done for Nuclear Regulated Facilities employees through the Nuclear Regulatory Commission (NRC) for years and have been extremely effective.
No
• C4-Table R6 Part 4: The Measures list two options which both require verification of evidence that conflicts with explanations in the rationale: 1. That the focus of this requirement is on the integrity of provisioning access rather than individual accounts. 2. That an administrative or clerical error should not be considered a violation of the standard. To be consistent, the Measures should only include evidence that the verification was completed, but not the results of the verification.
No
• C4-Table R7 Part 1: Revocation wording “at the time of” is not clear. Language such as “at the time” and “immediate” in a requirement are vague and difficult to both enforce and defend. Further, these terms imply a requirement of human perfection, which is a faulty concept. Language in the Standard must take into account the possibility for human error and the potential inability to meet the requirement due to unforeseen circumstances. • C4-Table R7 Part 1: Commission Order 706 provides the additional possibility that the ERO may “define what circumstances justify an exception that is other than immediate and determine what is the fastest revocation possible”. The Standard needs to include language that allows the entity the ability to document what circumstances justify an exception to “immediate revocation”. • C4-Table R7 Part 2: The standard should include language to document when it was not possible to implement immediate revocation due to unexpected circumstances without the threat of a non-compliance finding. • C4-Table R7 Part 2: For reassignments and transfers the Standard requires that an individual’s unneeded electronic and physical access to BES Cyber Systems be revoked by the end of the next calendar day. The language should be changed to say “next business day”.

No
• C7-Table R1 Part 1.1: The Measures imply that screen shots that show the accessible ports of BES Cyber Assets will be required. A screen shot implies that only proof at the machine level is acceptable evidence. This is an administrative burden to supply snapshot each and every logical port implemented in each system. This means that entities will need to provide this proof for every system. The Measures should simply state that the entity provide a list of ports that it is using. This makes it possible to use one list to represent the configuration of many systems. • To sync this with the rationale the 1.1 requirement needs to add the following language: “and document the need for any remaining physical input/output ports.” • C7-Table R1 Part 1.2: All High and Medium impact devices are already within a physical security perimeter. There is no need for further physical protection within these facilities. Further, physical Control Ports is a good example of scope creep. This occurred because clarification was requested regarding the meaning of the word “port” in prior CIP revisions. FERC confirmed the original meaning was for software ports. In its response, FERC “encouraged” entities to address hardware ports. This requirement would be expensive, administratively burdensome to administer, and provide little, if any protection. This requirement is unnecessary and it is suggested that this requirement be dropped. • C7-Table R1 Part 1.2: The words “network connectivity” are not clear and needs further definition. The wording should be changed to say “ports used for routable protocols”.
No
• C7-Table R2 Part 2.2: There is no provision for simply using an existing remediation plan or a patch handling procedure – which is most often the case. Most patches are handled the same way – with a procedure that is used to handle all patches. The Measures imply that there is a different Remediation Plan for each patch (eg. a “dated” remediation plan). This could be improved by simplifying the language that allows for including the use of an existing Remediation Plan. • Referring to the identification of the security patches, the statement “that addresses the vulnerabilities within a defined timeframe” is confusing. Does this mean that provided our plan is documented within 30 days, that we have unlimited time to deploy the patch? • C7-Table R2 Part 2.3: The Requirements language is very confusing because the requirement that there is process for remediation has already been established in R2.2. The Measures don’t match the Requirements. In addition, the Measures imply that the entity must prove that the changes were actually made in the systems. The Measures imply that recorded employee confirmation that the patch has been installed (e.g. from a workflow) would not be acceptable evidence. At the time of audit, the state of any system cannot be relied upon at the time of audit to contain the evidence. The reason for this is that any time, the installation of a major software upgrade would eliminate all the evidence associated with the prior release in which the patch was installed. This means that the entity must insure that it captures evidence of every patch installation at the time that each patch is installed. It is sufficient to simply use a time stamped workflow specific to the subject patch to document confirmation by the employee that the installation for that patch was completed. This would relieve entities of the risk of violation due to human error for failure to collect physical evidence of a patch installation that no longer exists on its systems at the time of audit. Further, this approach would eliminate the costly administrative overhead needed to make that evidence available. • C7-Table R2 Part 2.3: The measures only allow for the installation of the patches. What if the patches cannot be installed? What measures will be permitted to document the CIP Exceptional Circumstances?
No
• C7-Table R3 Part 3.3: Entities would take on a huge administrative burden and exposure of potential violation due to human error to provide the detailed technical evidence shown in the Measures. Confirmation by an employee in a time-stamped workflow should be sufficient evidence to show that the signatures were updated. • C7-Table R3 Part 3.4: Is the intent of including “removable media” actually to ensure that the media itself has some malicious software prevention capability? The rationale states that the intent is to protect the BES Cyber System. The requirement already requires that there be malicious software prevention on the assets, what is the purpose of calling out removable media as a separate thing to protect.
No
• C7-Table R4 Part 4.3: The Rationale states that the intent was to make it clear that it would not be a violation if the event logging system fails. However, this requirement conflicts with that Rationale

because it requires a foolproof system for detecting and responding to logging failures. It would be better if the requirement said “Provide Mechanism(s) to Detect and Activate a response to event logging failures” and as part of this change address the measures. The requirement in R4.5 requires manual log reviews. One of the stated intents of that requirement is to identify potential event logging failures. Requirement 4.3 then duplicates R4.5. Also, a logging failure is not an emergency that justifies a call-out on a non-business day. Next calendar day response times will necessarily lead to weekend/holiday – call-outs, which are administrative burden. ‘Next business day’ is suggest to replace the ‘next calendar day’. • C7-Table R4 Part 4.4: The Measures do not line up with the Requirement because it implies that more must be done than the requirement says (90 day retention). The Measure needs to refer to the same time frame as the requirement.
No
• C7-Table R5 Part 5.5.3: This requirement appears to be missing the link between the impact of the BES Cyber Security System to the password significance, we suggest this be re-worded.
Yes
No
• The requirement is confusing. The measure is more clear that the intent is to document that backups were successful and that could simply be the backup job report. The requirement could be interpreted to mean that the “information” on the backup media needed to be verified to confirm the backup was successful. Suggest making wording more simply, “For media backups that are essential to the BES Cyber System recovery, verify the backup process completed successfully.” In the measure add copies of backup system job reports as another measure. • R1.4: The Measure listed requires dated evidence that the verification of the backup process completed successfully. With this wording, an auditor may not accept confirmation by an employee via a Workflow that the backup process was completed and verified even though the wording of the Measurement includes the words “Evidence may include, but is not limited to…”. Backup systems can easily be automated to verify that the backup process completed successfully. Requiring dated system generated evidence that demonstrates that the backup and verification process completed successfully results in unnecessary administrative burden to the entity because of the never ending need to collect and store evidence repeatedly for many systems. Employee verification that the backup and verification processes were completed via a time-stamped workflow should be sufficient.
No
• The performance of an operational exercise of the recovery plans can be very costly, both in hardware/software and in people resources. This would require that we either take devices out of commission to facilitate the operational exercise or we have spare devices to facilitate “representative environment that reflects the production environment.” While we understand the need to ensure that you can actually do what is in the plan, we need to recognize the impact of this requirement. • R2.2 This requirement regards testing of information stored on backup media. The wording currently includes language “to insure that the information is usable and reflects current configurations.” The integrity of the information stored on backup media is not related to whether or not that information reflects current configurations because the information stored on the backup media contains the configuration of the system at the time the backup was taken. It is suggested that the wording “and reflects current configurations” be removed from both the Requirement and the Measures. • R2.3 This requirement includes a provision the entities to “Test each of the recovery plans referenced in Requirement R1,” initially upon the effective date of the standard.” It will not be possible for entities to test all of their recovery plans on that one day. As this is a new requirement, it will take many months for entities to prepare for and execute these tests. At a minimum, entities should have at least 12 months to prepare for and execute these tests.
No
• • Why not combine with Part 3.1 so it syncs with Part 3.2, add “and document any identified deficiencies or lessons learned within thirty calendar days” so that the requirements match. • R3.4

requires that recovery plans are updated address organizational changes within thirty calendar days of such change. The term “organizational changes” is undefined. When entities change their organizational structure, the computer systems and the people that support them are typically very much the same the day after the change as before the change. The reason for this is that BES Cyber Systems evolve separately from organizational changes. Moreover, the people that have the expertise to support BES Cyber Systems and BES Cyber Assets before the change are the same people who have the expertise to provide the support after the organizational change. It is suggested that the wording for this requirement state that the Recovery plans be updated when the information referred to in R1.2 changes.
No
1. Part 1.1.3 includes the phrase, “Any commercially available application software (including version) intentionally installed on the BES Cyber Asset”. Commercial providers such as SCADA vendors commonly package releases of other commercial software “eg. Oracle” into their products. In instances in which a Commercial provider’s release includes bundled releases of other commercial products, then reference to the highest level Commercial provider’s release number should be sufficient to define the baseline. The language of the standard could be improved by allowing entities to rely on the highest level Commercial provider’s release number as the definition for all bundled commercial software. 2. Part 1.2 – The requirements statement is not clear because it does not say what the CIP Senior Manager or delegate is authorizing. It is understood that the requirement is to authorize changes, but this is not stated. 3. Part 1.1.4. considers “Any custom software and scripts developed for the entity” as part of the baseline. It is unclear what the words “for the entity” mean. Software used by utilities generally contains a high level of customization. Changes occur incrementally and very frequently. Inclusion of custom software and scripts in the baseline is OK, but entities need some flexibility to determine what custom software and scripts are included as part of the baseline. Language needs to be added to provide the entities the flexibility to determine what custom software and scripts are considered part of the baseline, and what custom software and scripts are considered changes from the baseline. This will allow the entities the ability to structure their baseline and changes to the baseline in a manner that takes advantage of their existing infrastructure and systems in order to meet the desired objective without unnecessary burden. 4. Part 1.4.2 requires the entity to verify that the “required controls and BES Cyber System availability” are not adversely affected. It doesn’t make sense to require the entity to verify BES Cyber System availability resulting from the change. Whenever there is an availability problem, it will be detected and acted upon when it occurs. A future availability problem cannot be verified before it occurs. It is suggested that phrase “BES Cyber System availability” be removed from this requirement. Part 1.5.2 places an excessive administrative burden on the entities.
No
Comments: Under 3.2 the Measures require how differences between the production and test environments were accounted for in conducting the vulnerability assessment. It may be impossible to do this because the test environment will likely only include a subset of the equipment that is present in production.
Group
Arizona Public Service Company
Scott Bordenkircher
Yes
AZPS believes the definition for “BES Cyber Incident” should read “A Malicious act” not “Any Malicious act” in the first sentence. AZPS recommends changing the first bullet to “Compromises, or was an attempt to compromise, an Electronic Security Perimeter or a Defined Physical Boundary” in order to remove the language of “Physical Security Perimeter and use the new definition for PSP. AZPS

recommends the removal of the words “Critical Cyber Asset” in the second bullet since the sentence refers to BES Cyber Systems which would include Critical Cyber assets. AZPS also recommends the deletion of the 3rd bullet; this bullet is redundant to the first bullet. AZPS believes the last sentence in the definition for “BES Cyber System” should have the word “Maintenance” changed to “Transient” in order to align with the new terminology. AZPS is unclear on the definition for “BES Cyber System Information”. There is no definition of the term “BES Cyber System Impact Designations”. It is unclear what floor plans and equipment layouts would be considered BES Cyber System Information. AZPS recommends that the definition for “Restoration of BES”, bullet one should read “Blackstart restoration including planned cranking path as identified in Entity’s EOP-005 R1 artifacts.” Bullet 2 should be struck based on it being on the NRC side of the Bright Line criteria for applicability of the CIP Standards (and therefore outside of NERC jurisdiction). AZPS believes that under the definition for “Situational Awareness”, bullets 2 and 3 (“Change Management” and “Current Day & Next Day Planning”, respectively) should be struck because these functions are too long term to be considered Situational Awareness and have minimal impact on real-time operations. AZPS has 2 concerns with the definition for “CIP Exceptional Circumstance” 1) This is not defined in relation to BES reliability risk (i.e. person has heart attack in parking lot – probably not a CIP Exceptional Circumstance); 2) definition leaves no room for Entity to identify other situations wherein BES reliability is in jeopardy and declare a CIP Exceptional Circumstance as appropriate. AZPS recommends in the definition for “Control Center” that every use of the word “facilities” in this section be capitalized since it is a NERC defined word. AZPS believes in the definition for “Electronic Access Control or Monitoring Systems” including the phrase “or BES Cyber Systems” is much broader than the usage of this term in the Standards and could imply controls on all LOW impact devices. AZPS recommends deleting “or BES Cyber Systems”. AZPS recommends in the definition for “Electronic Access Point (EAP)” the word “restricts” be changed to “facilitates”. AZPS recommends the definition for “Electronic Security Perimeter” be changed to read “A collection of Electronic Access Points that protect one or more BES Cyber Systems.” AZPS believes that the definition for “Intermediate Device” should be an Electronic Access Point by definition and should be protected as such. It should not be allowed to reside outside an ESP and in fact should be part of an ESP. This definition could be rewritten as “a device that proxies communication with a BES Cyber Asset and terminates encrypted communications.” AZPS believes that in the definition for “Transient Cyber Asset”, item #3 is unnecessary and adds no value to the definition. It would also cause audit issues (e.g. proving that this criteria was met).
Yes
AZPS disagrees with 4.2 on page six. It is unclear, with the addition of 4.2.1 and 4.2.2, if the Facilities are restricted, in scope, to BES Facilities or if the identification and analysis of BES Cyber Systems is intended to expand to UFLS, UVLS, RAS, etc. that may be in Distribution Facilities. The Standard should specifically indicate, if this was the intention, that these specific Facilities may or may not actually be identified as BES Facilities but are still in scope because of their ability to impact BES facilities. AZPS would like clarity added to item 2.5 in attachment one; does cranking path imply only the primary Cranking Path, or is the intention to include all (or some) alternate Cranking Paths that have been identified in the restoration plan? AZPS disagrees with the Guidelines and Technical basis section at the end of this standard. Definitive or directive statements should not be made in Guidelines, as this leads to audit issues where Guidelines tend to be treated as more directive than they may have been intended.
No
AZPS believes in R1 that the use of the word ‘owns’ is ambiguous; should this not be the responsibility of the Entity that Operates the BES Cyber Assets/Systems? Multi-party ownership is a common business arrangement and leads to much confusion. The requirement should specifically identify which party is responsible for this identification and subsequent protection. Also, the sentence “All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification,” is not really feasible. It would not be possible to identify High and Medium Assets/Systems without a full list, which would lead to the conclusion that a list of Low Impact Assets/Systems is a necessary outcome of the identification. Also, several Standards are applied to Low BES Cyber Systems, which would indicate having to know what they are. The Standard should indicate that a list of Low Impact Assets/Systems is required at least at a summary level. There is a grammatical error in the first sentence of R1.1, it reads “BES Elements and Facilities is placed into operation” and should read “BES Elements and Facilities placed into operation”.
No

AZPS recommends changing the language “initially upon” to “prior to”. In M2 of R2, the phrase “review and update, where applicable” should be replaced with “review and approve”.
Yes
Yes
No
AZPS believes R2 could be enhanced by including the expanded descriptions of each bulleted item from the guidelines. Additionally, AZPS believes topics from CIP-002-5 and CIP-003-5 should be included in the policies.
No
AZPS recommends changing the phrase in R3 “initially upon the effective date” to “prior to the effective date”.
No
AZPS recommends the statement in R4 “individuals who have access” be changed to “individuals who have authorized access”. AZPS recommends the word “contractors” used in the bulleted list for Measure 4 be changed to “third parties”. The word “contractors” is too narrow.
No
AZPS recommends clarifying the word “position” in R5. Does this mean title or generalized organizationally defined role?
Yes
Yes
Yes
No
AZPS recommends expanding the applicability column in the R2 table to all systems identified in the R3 table. AZPS recommends changing the wording in table 2.2 Requirements. The wording should be changed to “Develop role specific Training, where applicable on the security controls protecting the Responsible Entity’s BES Cyber Systems.” AZPS recommends changing the wording in table 2.2 Measures to “Evidence may include, but is not limited to, training material on the security controls to protect BES Cyber Systems.” AZPS recommends changing the wording in table 2.3 Requirements to “Develop role specific Training, where applicable on the proper use of physical access controls protecting the responsible Entity’s BES Cyber Systems.” AZPS recommends changing the wording in table 2.4 Requirements to “Develop role specific Training, where applicable on the electronic access controls protecting the Responsible Entity’s BES Cyber Systems.” AZPS recommends changing the wording in table 2.5 Requirements to “Develop role specific Training, where applicable on the visitor control program.” AZPS recommends changing the wording in table 2.6 Requirements to “Develop role specific Training, where applicable on handling of BES Cyber System Information including storage media.” AZPS recommends changing the wording in table 2.7 Requirements to “Develop role specific Training, where applicable on identification of a potential BES Cyber Security Incident and associated notifications.” AZPS recommends changing the wording in table 2.8 Requirements to “Develop role specific Training, where applicable on recovery plans for BES Cyber Systems.” AZPS recommends changing the wording in table 2.9 Requirements to “Develop role specific Training, where applicable on response to BES Cyber Security Incidents.” AZPS recommends changing the wording in table 2.10 Requirements to “Develop role specific Training, where applicable on BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets.”
Yes
No
AZPS recommends expanding the applicability column in the R4 table to all systems identified in the R5 table.

No
AZPS recommends changing the wording of table 5.1 Requirement to “Ensure a personnel risk assessment has been performed as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.”
Yes
No
AZPS disagrees with the wording in the table 7.1 Requirements column “For resignations or terminations, revoke the individual’s unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.” It is not possible to implement or prove an activity was performed simultaneously with another activity. Also it is not clear if time of resignation means notice of resignation or actual effective resignation. AZPS disagrees with the time frame in table 7.2 Requirements “For reassignments or transfers, revoke the individual’s unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.” This is not a reasonable time frame. Take the scenario where an HR system processes a transfer on a Saturday. Requiring an entity to call-out personnel on a Sunday to revoke access for a transfer provides very little security value and will add significant burden. Seven calendar days is a reasonable timeframe. AZPS disagrees with the time frame in table 7.4 Requirements “For resignations or terminations, revoke the individual’s user accounts on BES Cyber Assets (unless already revoked in accordance with (R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.” This poses a much larger security risk than R7.2 and should allow no more than seven calendar days. AZPS disagrees with the time frame in table 7.5 “For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user.” Based on this security risk, AZPS believes no more than seven (7) calendar days should be allowed. AZPS also believes the second paragraph in the original text should be deleted due to there already being allowances for CIP Exceptional Circumstances.
Yes
No
AZPS disagrees with the applicability section of R1.1 and would recommend removing the word “routable”. AZPS believes dial up should be included from a security standpoint. The Guidelines for R1 do not align with what is stated in the R1.1 Requirements column. The guideline for R1 specifies network segmentation for all BES cyber systems. The requirement text is extremely ambiguous and does not provide enough specifics for an entity to know if what they provision will be found auditably compliant. The Measures states “documented technical AND procedural controls” while the Requirement states “technical OR procedural controls”. These need to be aligned. AZPS recommends that in R1.3 in the applicability section, the words “with external routable connectivity” should be removed because, from a security perspective, this should include dial up. In the measure for R1.3, “each access rule has a documented reason” is stated yet the Requirements do not include the mandate for “a documented Reason”. AZPS recommends that in R1.4 applicability section, the wording for the phrase "Electronic Access Points that use dial-up access for non-Interactive Remote Access" should change to "Electronic Access Points that utilize dial-up for External Connectivity that is not used for Interactive Remote Access" in order to clarify the intention of the phrase “non-Interactive Remote Access”. In the Requirements section, AZPS recommends removing “where technically feasible”. There are devices readily available that can be implemented that make this technically feasible so no exception is required. AZPS would like specificity in the requirements of R1.5. If the intent is to require an IDS, make the Requirement “Implement an IDS that monitors, detects and alerts for malicious activity at each EAP.”
No
AZPS disagrees with having a “technically feasible exception” for R2. AZPS believes all aspects of the requirement are technically feasible. AZPS would like the Requirements portion of R2.2 clarified. It is not clear which endpoints we need to encrypt between. Is this between originating devices and the intermediate device or all the way to the BES Cyber System?
Yes

No
AZPS recommends changing the wording in table 1.1 Applicability. The word implement should be added to the Requirement so it matches the Measures. AZPS disagrees with the wording in table 1.1 Requirements. Move Associated Physical Access Control Systems to Applicability in R1.2 for stronger controls much like in CIP-005-5 R1.2. AZPS recommends changing the wording in table 1.2 Measures by removing the words “accompanied by card reader logs”. This could be something other than a card reader. AZPS recommends changing the wording in table 1.3 Requirements. Reword the Requirement to “Utilize two or more authentication factors to gain physical entry.” The way it is worded currently allows for two physical access controls to be identified but does not specify that they both must be used for a single entry. The Guideline implies that the intent was to require multifactor authentication. Also – remove the words “where technically feasible”, this unnecessary exemption weakens security. AZPS recommends changing the wording in table 1.3 Measures by removing the words “accompanied by card reader logs”. This could be something other than a card reader. AZPS disagrees with the wording in table 1.4 Requirements. The wording should include attempts at unauthorized physical access. AZPS disagrees with table 1.5. This should be merged with Requirement R1.4. There is no reason not to require that physical access control systems reside within a DPB. AZPS recommends adding Associated Physical Access Control Systems to table 1.6 Applicability. AZPS disagrees with the security posture in table 1.6 Requirements. This requirement should mandate logging of entry AND EXIT by authorized personnel.
No
AZPS recommends changing the wording in R2 to “…Entity shall document and implement a visitor control program…”. AZPS recommends adding Associated Physical Access Control Systems to table 2.1 Applicability. AZPS recommends adding Associated Physical Access Control Systems to table 2.2 Applicability. AZPS recommends changing the wording in table 2.2 Requirements. This Requirement should be rewritten to state “Implement a process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit and includes the visitor’s name, the name of the person conducting the escorting, and the responsible point of contact. Document all escort handoffs.” This is a far better security implementation than what this requirement has been proposed as. AZPS doesn’t believe there is any reasonable way for an Entity to research an incident if they are unable to track when visitors enter and exit and unless they are able to clearly identify WHO escorted the visitor. Mandating the tracking of a non-present Point of Contact holds absolutely zero security value. AZPS disagrees with the wording in table 2.2 Measures. Add “and the name of the person or persons conducting the escorting.”
No
AZPS recommends changing the wording in R3 to “…Entity shall document and implement maintenance and testing…”. AZPS recommends changing the wording in table 3.1 Requirement to state “…calendar months thereafter, conduct testing and perform necessary maintenance of the Physical…”. AZPS recommends changing the wording “logging and alerting systems” in table 3.2 Requirement to “Physical Access Control Systems”.
Yes
No
AZPS recommends changing R1 to read “Each Responsible Entity shall document and implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.” AZPS believes that the words “of BES Cyber Systems” should be removed from the measures in R1.1 since R1.1 applies to more than the BES Cyber System. AZPS recommends that the language in the requirement for R1.2 should be changed from “console command” to “console control” in order to clarify the type of physical port enabled.
No
AZPS recommends changing R2 to read “Each Responsible Entity shall document and implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management” AZPS believes the requirements section of R2.1 should state “Security related updates” and not just “updates”. R2.1 also mentions firmware, but the configuration requirement in CIP10 does not require the documentation of firmware levels. These requirements need to align. Under the measures section for R2.1 the words “BES Cyber Systems” should be

removed since R2.1 applies to more than the BES Cyber System. Also remove the words “The list could be sorted by BES Cyber System or Source”, these words are not necessary. AZPS recommends in the requirements and measures of R2.2 should state “Security related updates” and not just “updates”. In the measures it states “a dated implementation plan showing how the vulnerability will be addressed”; this part of the measure does not align with the guidelines, the guidelines identify the option of an event driven timeline whereas this measure dictates a DATED plan. AZPS recommends that in the measures section of 2.3 you add “Previously implemented controls” as acceptable evidence of remediation.

No

AZPS recommends changing R3 to read “Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.” AZPS disagrees with Requirement 3.4, and recommends including removable media under R3.1. This Requirement would then be focused on Transient Cyber Assets. Also, remove the words “BES Cyber Systems” since R3.4 applies to more than the BES Cyber System. AZPS also disagrees with the measures portion of 3.4; there is no logging requirement anywhere in the standards for logging the use of removable media. Also, no inventory is required for transient devices anywhere in the standards. AZPS recommends that in the requirements and measures for R3.5, logging the disconnection of the transient asset should also be required as a better security practice.

No

AZPS recommends changing R4 to read “Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring." AZPS recommends changing the wording in the Requirements of R4.1 to read “logging of generated events…” instead of “log generated events…”. AZPS disagrees with the timeframe requirement set forth in the Requirement section of R4.3 and would like the timeframe removed. Further, event logging failure needs to be clarified, from a technical perspective you can’t always detect a failure of event logging. AZPS wants more clarity and alignment between the Requirement and the Measure in R4.4. The Requirement states “for at least the last 90 consecutive calendar days” while the Measures state “logs from the past ninety days”. AZPS recommends striking the “at least” language in the Requirement and have it read “for the last 90 days”. Also, remove the words “BES Cyber Systems” since R4.4 applies to more than the BES Cyber System. AZPS believes in the Requirements for 4.5 the “potential logging failure” language should be removed since that is covered in 4.3. The language in the Requirement that states “Activate a response to rectify any deficiency identified from the review before the end of the next calendar day” should be simplified by being changed to “Activate your incident response plan”; this language accomplishes what is intended and is far clearer. In the Measures for 4.5 AZPS would like to have the “signed” language stricken, with the belief that documenting the name of the reviewer in the review proves the review was completed; implying that the review must be physically signed adds unnecessary burden. The language in the Measures that reads “showing that personnel were dispatched or a work ticket was opened to rectify the deficiency” should be changed to “showing the incident response plan was activated”; this language accomplishes what is intended and is far clearer.

No

AZPS recommends changing R5 to read “Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.” In R5.1 AZPS recommends adding the word “user” in front of “credentials” in the Requirement section to add clarity. Also, remove the words “to each BES Cyber Systems” since R5.1 applies to more than the BES Cyber System. In the Measures for R5.1 remove the words “to each BES Cyber Systems” since R5.1 applies to more than the BES Cyber System. AZPS recommends for the Requirements section of R5.2 the words “the use of” should be deleted due to the potential for this to confuse people into thinking that every individual usage of these accounts should be authorized every time. In the Measures forR5.2 remove the words “to each BES Cyber Systems” since R5.2 applies to more than the BES Cyber System. AZPS disagrees with the Requirements section of R5.4. All of the text following the word “application” should be deleted and added in the applicability section as defined assets that are covered. This would keep consistency across all of the standards. AZPS recommends for the Requirements section of R5.5.1 and R5.5.2 remove the words “by the BES Cyber Systems” since R5.5 applies to more than the BES Cyber System. For R5.5.3 the language “of the BES Cyber System, the significance of passwords in the set of controls used to prevent

unauthorized access to the BES Cyber System and" should be removed and the word "or" should be added in place. The words are unnecessary in this section. AZPS recommends that for the Applicability section of R5.6 instead of "at Control Centers" it should state "all Medium Impact BES Cyber Systems" in order to maintain consistency.

Yes

No

AZPS recommends changing the wording in R1 from "have" to "document". AZPS believes there may be misalignment between the wording in table 1.2 Requirements and the Guidelines. The Guidelines define what is reportable but the Requirement allows the utility the latitude to define it for themselves. The intent needs to be made clear and the two need to align.

No

AZPS recommends changing the word "When" in table 2.1 Requirements to "In the event of…" Change to state "Document the use of the Incident Response Plan." Insert "Document deviation from the plan during the incident." Delete the word test, testing is covered in R2.2. AZPS believes the Measures does not align with the Requirement in that it adds the requirement to justify deviations. AZPS recommends changing the word "Implement" in table 2.2 Requirements to "Perform an exercise". Change "Initially upon the effective date…" to "Prior to the effective date…". Delete the phrase "between executions of the plan(s)"; it is not necessary. AZPS recommends changing the word "implementing" in table 2.2 Measures to "exercising".

No

AZPS recommends changing the wording in R3 from "implement one or more documented" to "document and implement". AZPS recommends changing the wording in table 3.1 Requirements from "initially upon the effective date" to "Prior to the effective date". Delete the phrase "between reviews"; it is not necessary. Add clarification to update within thirty calendar days. AZPS recommends changing the word "test" in table 3.2 Requirements to "exercise". AZPS recommends changing the requirement in table 3.2 Requirements to mandate the update within thirty calendar days instead of sixty for better security practice.

Yes

No

AZPS would like clarity in the Requirements section of R1.3. It is unclear what the intent of the word "protection" means in this context. AZPS believes the requirement would be better served with the use of the word "recovery" rather than the word "protection". Remove the words "BES Cyber System functionality" form the Requirements section since R1.3 applies to more than the BES Cyber System. Remove the words "BES Cyber System" from the Measures section since R1.3 applies to more than the BES Cyber System. AZPS recommends replacing all of the language in the Requirements section of R1.4 with "Verify that backups of information essential to recovery complete successfully." AZPS recommends replacing all of the language in the Requirements section of R1.5 with "Procedures that attempt the preservation of data of any event that triggers the activation of any recovery plans including documentation of any failures in preserving data". The Measures section of R1.5 also should be rewritten to state "Evidence may include, but is not limited to, procedures that attempt the preservation of data of any event that triggers the activation of any recovery plans including documentation of any failures in preserving data".

No

AZPS recommends changing R2 to read "Each Responsible Entity shall document and implement one or more recovery plans that collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. AZPS believes that in the Requirements section of R2.1 the word "Implement" should be changed to "Exercise" to add clarity to what is really required. Also, in the Requirements section the language "initially upon the effective date…" should be changed to "prior to the effective date…". The Measurements part of R2.1 should also be rewritten to better align with the Requirements. AZPS believes the Requirements section of R2.2 needs to have the language "of BES Cyber Systems" removed since R2.2 refers to all assets. The word "initially" should be removed and the words "prior to the effective date of the standard" should be added. Also in the Requirements section the language "information is useable and reflects current configurations",

should be changed to “information is recoverable and current”. AZPS believes the Measures section of R2.2 needs to have the language “of BES Cyber Systems” removed since R2.2 refers to all assets. The words “when initially stored” should be removed and the words “prior to the effective date of the standard” should be added. Also in the Measures section the language “information is useable and reflects current configurations” should be changed to “information is recoverable and current”. AZPS recommends in the Requirements section of R2.3 the words “initially upon the effective date of the standard and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment…” be rewritten to “at least once every 39 calendar months following the effective date of the standard through an operational exercise of the recovery plans in an environment...”. In the measurements section of R2.3 removes the language “initially upon the effective date of the standard and”, since the initial exercise is covered under R2.1 and no initial should be required to recover the entire system.
No
AZPS recommends that in the Requirements section of R3.1 the language “initially upon the effective date…” should be changed to “prior to the effective date…”. Also in the Requirements section, change “BES Cyber Systems” to “Cyber Assets”. AZPS recommends that in the Measures section of R3.1 the language “initially upon the effective date…” should be changed to “prior to the effective date…”. AZPS recommends a rewrite of the Requirements portion of R3.4 to state “Review and update (if appropriate) recovery plans to address any organizational changes within thirty calendar days of such change.” This new language adds the review aspect of the standard and removes the change due to technology change since that is covered in CIP10-5 R1.3.
Yes
No
AZPS recommends changing R1 to read “Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.” AZPS recommends the following changes to the Requirements section of R1.1: • Remove the words “ of each BES Cyber Systems” and “for each BES Cyber Asset identified” since R1.1 applies to more than the BES Cyber System • R1.1.3 remove the words “intentionally” and “on the BES Cyber Asset” • R1.1.4 should read “developed and installed” since just simply developed does not mean it was installed. • R1.1.5 should be deleted, because this is covered in CIP-007-5 • R1.1.6 should read “All installed security patches” • Hardware components and firmware versions should be added for better security practice. AZPS recommends in the Measures section of R1.1 remove the words “of each BES Cyber Asset in the BES Cyber System” since R1.1 applies to more than the BES Cyber System. AZPS recommends changing the Requirements section of R1.2 to read “documentation of changes” instead of “and document changes”. Remove the words “of each BES Cyber Systems” and “for each BES Cyber Asset identified” since R1.2 applies to more than the BES Cyber System. In the Measurements section of R1.2 “Evidence may include” should be changed to “Evidence of the change and the authorization may include”, since the standard explicitly requires authorization the evidence should show the authorization. AZPS recommends the wording in R1.3 be changed from “…required by a NERC CIP Standard, including identification and categorization of BES Cyber Systems as necessary…” to “required by any NERC CIP Standard as necessary…”. AZPS believes R1.5 should merge with R1.4 and require all steps for all of the items listed in R1.4 Applicability. Suggested combination and order of requirements referenced by current numbering (which of course would be renumbered R1.4.1-R1.4.5): R1.4.1, R1.5.1, R1.5.2, R1.4.2, R1.4.3.
No
AZPS disagrees with the Requirements section of R2.1 and believes the Requirement should be rewritten to read “Detect for changes of the baseline configuration within 7 days. Document and investigate within 30 days”.
No
AZPS recommends changing R3 to read “Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-010-1 Table R3 – Vulnerability Assessments”. AZPS recommends that in the Requirements section of R3.1 the language “initially upon the effective date…” should be changed to “prior to the effective date…”. The words “security controls” should be specified, the language from the Guidelines should be added here. The requirements section also needs some simplification to the language. AZPS recommends changing

"…to determine the extent to which the controls are implemented correctly…." to "to determine if the controls are implemented and operating as designed…". AZPS recommends that in the Requirements section of R3.2 the language "initially upon the effective date…" should be changed to "prior to the effective date…". Also in this section, replace the word "test" with "production environment or an…", this will allow for a VA to occur against the production environment or a representative environment without specifying it must be a test environment. AZPS does not think the Requirements section of 3.4 makes sense the way it is written. AZPS recommends that instead of "…planned date of completing the action plan and the execution status of the action plan." This should read "planned date of completing the action plan." What would also make sense would be to mandate updates to the status of the action plan at some periodicity such as quarterly.
Yes
No
AZPS recommends changing the wording of R11 to "Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection…" AZPS recommends, in table 1.1 Applicability, deleting "Associated, protected cyber assets" because these are not included in the Definitions. AZPS recommends, in table 1.2 Applicability, deleting "Associated, protected cyber assets" because these are not included in the Definitions. AZPS recommends, in table 1.3 Applicability, deleting "Associated, protected cyber assets" because these are not included in the Definitions. AZPS recommends changing the wording of table 1.3 Requirements to "Prior to the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment."
No
AZPS recommends changing R2 to "Each Responsible Entity shall document and implement one or more processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal…." AZPS disagrees with separating tables 2.1 and 2.2. Tables 2.1 and 2.2 should be combined under one Requirement. The words "Associated Protected Cyber Assets" should be deleted from Applicability. The combined table 2.1 and 2.2 Requirements should be reworded as "Media containing BES Cyber Security Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media. Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media."
Yes
Yes
Group
ZGlobal on behalf of City of Lodi, City of Ukiah, Alameda Municipal Power, Salmon River Electric Coop, California Pacific Electric Company
Mary Jo Cooper
Yes
We thank the drafting team and compliment them on their work. It is very valuable and provides a good basis for appropriately allocating responsibilities according to the impact to the BES. We believe the definition of BES Cyber Asset is accurate however based on the definition we feel that the Functional Applicability for each Standard is incorrectly defined. As a result we have cast a negative vote on the Standards. Additional work is needed due to a discrepancy between the definition of BES Cyber Assets and the applicability to entities with UFLS or UVLS equipment. Definition of BES Cyber Asset: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to

operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. Applicability: Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: • A UFLS program required by a NERC or regional Reliability Standard • A UVLS program required by a NERC or regional Reliability Standard • A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard • A Transmission Protection System required by a NERC or regional Reliability Standard • Its Transmission Operator's restoration plan Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: • A UFLS program required by a NERC or regional Reliability Standard • A UVLS program required by a NERC or regional Reliability Standard The discrepancy exist because (1) The definition states “The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES.” (2) LSE’s and DP’s with UFLS equipment are required to comply with the proposed CIP Standards over BES Cyber Assets when these devices are not consider BES Cyber Asset per definition. (3) These devices sense a system condition and do not send or receive instructions. In fact in some regions a UFLS device is not required to be a cyber-equipment type. For example, in the NPCC region an electro-mechanical relay can be used to fulfill an organizations UFLS program requirement. Proposed recommendation: Modify the applicability. “Load Serving Entities and Distribution Providers with a load shedding program that is activated through receipt of an instruction to its cyber processor to operate.”
No
Yes
Yes
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.

No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic

signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.

No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
Yes
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
Individual
Linda Jacobson-Quinn
Farmington Electric Utility System
Yes
BES Cyber Asset: The drafting team should consider revising the definition to consider the facility the Cyber Asset is associated with, “A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact the ability of the facility with which it is associated with. (See comments on CIP-002-5) Additionally, the terms “adversely impact” are not well defined. BES Cyber System states, “A Maintenance Cyber Asset is not considered part of a BES Cyber System.” The drafting team should consider removing this statement (since the definition of a BES Cyber Asset excludes Transient Cyber

Assets), modifying the statement to exclude Transient Cyber Assets, or defining “Maintenance Cyber Asset.” BES Cyber System Information: The definition includes the term “BES Cyber System Impact” designations; this term is not defined and should be clarified by the drafting team. CIP Exceptional Circumstance: It is unclear the differentiation of, “A Cyber Security Incident requiring emergency assistance” and “a response by emergency services.” CIP Senior Manager: The definition should be clarified it is applicable to CIP-002 thru CIP-011, as CIP-001 is currently enforceable and does not require a CIP Senior Manager Control Center: The definition is broad and could impact small entities by including ‘control rooms.’ As proposed, “One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations” System Operator is currently defined as, “"System Operator: An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time." A vertically integrated utility can have a “Control Center” with certified system operators that support the real-time operations and have a control room located at a generation plant that can perform one or more of the functions listed in the definition of Control Center. The drafting team should clarify if it is the intent to only include the Control Center with the primary responsibility for maintaining reliability of the BES, performing one or more of the functions that support real-time operations by System Operations. Reportable BES Cyber Security Incident: The definition included in CIPv5 conflicts with EOP-004-2 for both Cyber Security Incidents and Forced Intrusions for BES facilities. The drafting team should consider coordinating with the EOP-004-2 drafting team to ensure there is no overlap or ‘double jeopardy.’
Yes
FEUS supports the comments submitted by APPA.
No
FEUS concurs with the comments submitted by APPA. In addition, FEUS shares the concern, as others in the industry, that CIP-002-5 as currently drafted will not be auditable by CEA’s. CIP-002-5 R1 requires entities that own BES Cyber Assets and BES Cyber Systems to categorize those assets using Attachment 1. The definition of BES Cyber Asset includes Cyber Assets that adversely impact one or more BES Reliability Services. In order to comply with CIP-002-5 R1, the entity will FIRST have to identify ALL BES Cyber Assets and BES Cyber Systems that adversely impact BES Reliability Operating Services, then categorize the BES Cyber Assets and BES Cyber Systems using Attachment 1. Attachment 1 describes facilities that if the BES Cyber Asset or BES Cyber System meets one of the criteria, it inherits the high or medium impact with all others classified as low. In order to identify ALL BES Cyber Assets and BES Cyber Systems requires knowledge of the entities system. An auditor, who is not familiar with the system, would not be able to validate the entities assessment without knowledge of the system or FIRST looking at the entities facilities. While the requirement does not require discrete identification of Low Impact BES Cyber Assets and BES Cyber Systems, sub requirement R1.1 requires documentation of a change in the classification of within 30 calendar days for assets going from a lower impact to a higher impact. Without documentation the asset was classified as low prior to the reclassification, this would be almost impossible to audit. Additionally, the VSL’s for R1 are based on the number or the percent of BES Cyber Assets incorrectly identified – in order to determine the correct number or percent of BES Cyber Assets incorrectly identified, the CEA would have to determine all BES Cyber Assets, including the assets with a Low Impact to determine the correct VSL; thus, requiring ALL Low BES Cyber Assets being identified. FEUS agrees with Honeywell, a revised three-step process could replace the process in the current draft as follows: 1. For each BES Facility that has associated cyber assets, determine the impact using Attachment 1. 2. Determine the BES Reliability Operating Service(s) the BES facility supports 3. Identify associated BES Cyber Assets and BES Cyber Systems This allows the first step to be determined by facility, much like previous versions and the classification of BES Cyber Assets and BES Cyber Systems to be determined subsequent and inherit the designation of the facility. Thus, Low Impact facilities would not require a list of Low Impact BES Cyber Assets or BES Cyber Systems.
No
R2 requires approval, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS

recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time following the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective date, not to exceed three months following, and at least each calendar year thereafter…”
No
The VSL’s for R1 are based on the number or the percent of BES Cyber Assets incorrectly identified – in order to determine the correct number or percent of BES Cyber Assets incorrectly identified, the CEA would have to determine all BES Cyber Assets, including the assets with a Low Impact to determine the correct VSL; thus, requiring ALL Low BES Cyber Assets being identified.
Yes
Yes
The topics included in the sub requirements are capitalized indicating they are defined terms. The drafting team should verify all capitalized terms are defined.
No
The drafting team should revise the statement “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time following the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective date, not to exceed three months following, and at least each calendar year thereafter…”
Yes
Yes
Yes
Yes
Yes
No
The rationale states some personnel may not require training on all topics based on their role; R2 should be revised to indicate the training is based on the roles defined in R2.1. An example of such wording could include, “Each Responsible Entity shall have a role-based cyber security training program for personnel who require authorized electronic or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items that includes each of the applicable items based on their role in CIP-004-5 Table R2”
No
R3.1 and R3.2 should clarify the required training is role-based as determined in R2.1. The drafting team should consider revising R3.1 as follows, “Require completion of the training specified in CIP-004-5 R2, based on the role defined in CIP-004-5 R2.1, prior to granting authorized access, except during CIP Exceptional Circumstances.” A similar clarification can be made to R3.2.
No
R4.2 requires the seven year criminal history check for all locations where a person has resided, been employed, or went to school for more than six months. FEUS SME’s believe it will be difficult to verify all the locations a person has resided, been employed, or went to school for more than six months without accepting an attestation of all the locations from the individual.
Yes

No
CIP-004-5 R6.1 Measure (i) requires a sampling of accounts to verify unauthorized users do not have access; FEUS recommends the drafting remove this measure from R6.1 as doesn't seem relevant to authorization of access and is more appropriate in 6.4. The same comment applies to the Measure (i) of R6.2 and Measure (i) of R6.3.
No
FEUS appreciates the change rationale stated by the drafting team. However, the drafting team should consider revising R7.2 to maintain access, based on need, following a transfer. A reassignment or transfer may be a promotion that requires the same access levels, for example, a System Operator promoted to a Senior System Operator. In addition, for small entities, with limited staff, it may be necessary to allow access for duration to allow the entity to fill the vacant position and allow for sufficient training time.
No
The drafting team should clarify the Electronic Access Points in 1.3 and 1.5 are the Electronic Access Points identified in 1.2.
No
R2.2, the purpose of encryption is to protect the confidentiality and integrity data being transferred; the drafting team should simply require, "Require encryption for all interactive remove sessions." R2.3 requires multi-factor authentication for Interactive Remote Access. FEUS agrees with requiring multi-factor authentication; however, the reference document "Guidance for Secure Interactive Remote Access" states: "Multi-Factor Authentication Multi-factor authentication technologies use authentication factors from at least two of three generally accepted categories: something known (e.g., a password or personal identification number or PIN), something possessed (e.g., a one-time password token or a smart-card), and something unique about the user (e.g., fingerprint or iris pattern).6 Systems that use two or more factors are described as using multi-factor authentication; systems that use only two factors are described as using two-factor authentication. User IDs are not considered factors in a multi-factor authentication system." The drafting team should revise R2.3 to either define multi-factor authentication, allow a minimum of two-factor, or explicitly state a minimum of two factors.
No
R1.2 requires at least one physical access control to establish a one or more Defined Physical Boundaries that restricts access. The Measures for R1.2 require a physical security plan that describes how ingress and egress is controlled by one or more methods, proof access is restricted to authorized personnel accompanied by "card reader logs." The Change justification states specific examples have been moved to the Guidelines. The guidelines allow for alternate methods to log access. FEUS recommends the drafting team clarify if control and logging of ingress AND egress is required by R1.2 and remove "card reader" from the measures to allow for other means of logging. R1.3 Measures include a plan that describes how ingress and egress is controlled by two or more methods. The drafting team should clarify if ingress AND egress is required to be controlled by two or more methods. In addition, the drafting team should remove "card readers" to allow alternate means of logging. R1.5 requires, "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems." FEUS believes this requirement is vague as to its applicability. R1.1 applies to "Associated Physical Access Control Systems", R1.2 does not apply to "Associated Physical Access Control Systems", nor does R1.3. With the exception of R1.1, which applies to Low Impact BES Cyber Systems, there is not a requirement to establish a Defined Physical Boundary for the Physical Access Control System. Additionally, the applicability section of CIP-006-5 defines Associated Physical Access Control Systems as "Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems." The drafting team should either include associated Physical Access Control Systems to the applicability of R1.2 and R1.3 or eliminate R1.5.
No
FEUS recommends the drafting team define "continuous" or remove it from R2.1 Requirements and

Measures. The term continuous is not auditable. FEUS appreciates the changes made in R2.2 to allow for intermediate ingress and egress during the visit. However, for consistency, the drafting team should revise the date and time from “entry and exit” to “ingress and egress to the Defined Physical Boundary.”
No
R3 inclusive of R3.1 and R3.2 - the drafting team should clarify what Associated Access Control Systems it is applicable to (High/Medium/Low) and capitalize Locally Mounted Hardware or Devices.
No
The VSL should take into consideration a violation of Part 1.1 vs Part 1.2 and 1.3. R2 should remove “continuous” and refer to the entities escort policy.
Yes
No
The drafting team should clarify the requirement for R2.3 is only when the “remediation” can be concluded (the measures all point to evidence of installation/updates are completed) – If testing of a security patch the entity identifies the EMS does not operate properly when applied, R2.3 should not be applied until the EMS vendor supplies an additional update that is compatible.
Yes
No
The drafting team should consider revising R4.1.4 to “Any detected malicious activity.” The drafting team should add language from the rationale to clarify R4.3, “Detect and activate a response for event logging failures before the end of the next calendar day.” Clarify if this is the failure of the event logging system (SIEM) or the individual systems sending events to the SIEM.
No
FEUS supports the comments submitted by APPA. R5.6, FEUS recommends removing “generating alerts after a threshold of unsuccessful login attempts” as this is addressed in R4.1.
No
FEUS supports the comments submitted by APPA. FEUS shares the concerns with possible conflicts with CIP-008-5 and EOP-004-2. In addition, there definition of BES Cyber Security Incident states, “A malicious act or suspicious event that: Compromises, or was an attempt to compromise, the ESP; or disrupts or was an attempt to disrupt, the operation of a BES Cyber System; or Results in unauthorized physical access into a Defined Physical Boundary.” The measures for R1.1 include in relevant portion, “BES Cyber Security Incidents targeting the Defined Physical Boundary of a BES Cyber System.” The drafting team should revise the measure to align with the definition and include, that results in unauthorized physical access.
No
The drafting team should remove the requirement to “justify” deviations taken from the plan to align with the requirement. R2.2 requires approval, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…”
No
FEUS supports the comments submitted by APPA. R3.1 requires approval, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to

complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…”

Yes

R1.4 states backup media shall be “verified initially after backup,” the terms verified initially are vague. Many automatic backup systems run a series of backups at different times and report if the backup was successful. FEUS recommends the drafting team revise R1.4 to state “verified the backup was successful by the end of the next business day.”

No

R2.1, R2.2, and R2.3 include the statement, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…” The drafting team should clarify in R2.2 what includes “any information.” In addition, “and reflects current configurations” is not achievable and should be removed.

No

R3.1 include the statement, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…” R3.1 requires the plan be reviewed when BES Cyber Systems are replaced; R3.4 requires the recovery plan be updated to address technology changes within thirty calendar days. FEUS recommends removing the requirement to review when BES Cyber Systems are replaced from R3.1 and including the statement in R3.4.

Yes

No

Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration within 30 calendar days of completing the change approved in 1.2."

FEUS supports comments submitted by APPA.

No

FEUS supports the comments submitted by APPA. R3.1 and 3.2 include the statement, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…”

Yes
No
See FEUS related comment on the definition of BES Cyber System Information. There is a minor typo for the headers in section 1.2. R1.3 includes the statement, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…”
No
The drafting team should clarify, as referenced in the guidelines, if the media is to be reused outside of the BES Cyber System it should be properly erased as required to allow for BES Cyber Systems to be temporarily removed and reused within the same environment.
Group
Edison Electric Insititute
David Batz
Yes
The Edison Electric Institute (“EEI”) submits this executive summary concerning the Project 2008-06 Cyber Security Order 706 Version 5 CIP Standards as published 11/7/2011. EEI is the association of the nation’s shareholder-owned electric utilities, international affiliates, and industry associates world-wide. EEI takes the subject of cyber security and infrastructure protection very seriously, and is committed to the reliability of the Bulk Electric System. This commitment includes timely completion of Version 5 and filing a comprehensive set of revisions to the CIP standards for approval with the Commission. EEI appreciates the significant level of effort on the part of the CS 706 Standards Drafting Team, NERC staff, and industry stakeholders in the development of revisions to the CIP standards. EEI has provided a considerable number of comments and suggestions for revisions and enhancements to the Draft of Version 5. These suggestions for revisions are intended to improve the clarity and quality of the Draft. We encourage members of the CS 706 Standards Drafting Team to have an open mind when considering stakeholder feedback, and be willing to closely review and potentially remove new mandatory security requirements that are not specifically required by FERC Order 706 or that fail to provide meaningful security enhancements at a cost that can be afforded by the consumers of electricity. Any proposed modifications to the CIP Standards should appropriately recognize the significant investment that the industry has already made in adopting CIP Version 1, 2 and 3. New or modified requirements should build upon and leverage existing security programs and investments. We observe that there are a significant number of stakeholders who have concerns about the proposed framework change in CIP-002-5 for identification of the cyber assets to be protected and concerns with extensive changes in definitions. We recommend that the SDT carefully evaluate alternative strategies offered by stakeholders to address these concerns. In addition, we observe that there are a significant number of stakeholders who have great concern about the new proposals regarding low-impact BES cyber assets, both as to appropriate identification, and concerning the new mandatory controls that have been identified for low impact BES cyber assets. Technical experts have broadly varying positions on whether these assets should be covered by the mandatory NERC standards, as well as the nature of the controls that should be applied. IT and security systems professionals also continue to struggle with the design of the NERC standards, a template that is not ideally suited to addressing IT systems issues. Rigid adherence to a set of static requirements may serve to bring “Compliance”, but “Compliance” in this sense is not necessarily equivalent to actual enhancements in the security posture, reduction of risk, or increasing the reliability of the Bulk Electric System. With regards to addition of new administrative requirements, many in the industry are concerned that the additional cost will bring little or no security benefit. The redefinition of annual, the added requirements for delegations, along with other new administrative

requirements will not enhance security and may divert finite resources to non-security related efforts. We recommend that the SDT continue to evaluate alternative strategies that would allow for addressing the outstanding FERC Order 706 directives in a manner that does not create a situation where the electric sector is expending disproportionate resources for compliance activities associated with low impact BES cyber assets in comparison to medium or high impact BES cyber assets. We recommend that any new mandatory security controls be closely scrutinized to ensure that they provide a meaningful increase in the security and reliability of the BES that is commensurate with the amount of resources that are required to establish and maintain them. In the event that new mandatory security controls are established for low impact BES cyber assets, we recommend that implementation deadlines for the low impact BES cyber assets, where appropriate, occur after implementation deadlines for medium or high impact BES cyber assets. • There have been significant changes in the basic terms and definitions which have been used since the inception of the CIP standards, including dropping core concepts such as Critical Assets, Critical Cyber Assets, Physical Security Perimeter, and substantial changes in definitions to remaining terms. These changes are not clearly required to support FERC Order 706, or to enhance the security controls within the Bulk Electric System. EEI proposes that approved definitions within the CIP Standard (pre-Version 5) are retained whenever possible. We understand any need to modify the definition to align with FERC Order 706 or enhance security, and would much prefer new definitions over any elimination or introduction of terms. EEI members are opposed to any instances of changes where there is no clear need as each modification requires extensive resources to modify existing compliance processes and evidence. The removal of Physical Security Perimeter as a term (replaced by Defined Physical Boundary) is the primary example where the definition could be modified while retaining use of Physical Security Perimeter. • The loss of Critical Assets removes facilities from consideration. This presents challenges in assessing BES Cyber Systems as they provide services to a facility which provides BES Reliability Operating Services – not the BES Cyber System independently. This also introduces the approach in which BES Cyber Systems are not independently assessed for impact with consideration to the specific service they support, but are assigned the impact of the BES Reliability Service (conducted within a facility). The methodology should recognize the facility within impact assessment, and allow for subsequent entity assessment of the impact of any supporting BES Cyber System, whether they reside within facility or in another location in support of the facility. • Requirements and/or Measures that use all-encompassing words like 'any,' and 'all' introduce compliance challenges, as satisfying these definitions potentially introduce extensive additional elements that would be out of scope should more concise language be used. • Extension of the default retention requirements within all the standards from the current 'previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation,' to 'three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation' is not identified within FERC Order 706 nor does it enhance security commensurate with resource expenditures. EEI members would prefer use of the current 'previous full calendar year' retention period. • BES Cyber Asset – Proposed Definition Change o Original Text – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. o Proposed Change – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact the capability of the facility with which it is associated to perform one or more BES Reliability Operating Services. Redundancy shall not be considered when determining adverse impact. A Transient Cyber Asset is not considered a BES Cyber Asset. o Rationale – Impact Ratings as defined within CIP-002-5 focus on the role of the facilities' function specific to BES Reliability Operating Services. The BES Cyber Assets support the facility in providing that service. • BES Cyber System – Proposed Content Change o Original Text – One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System. o Proposed Change – One or more BES Cyber Assets that are logically grouped together to operate one or more BES Reliability

Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. o Rationale – Absent logical grouping, there is no clear understanding of how a BES Cyber Asset qualifies as a component of a BES Cyber System. Physical grouping could infer devices within a common rack, though they may provide quite different services within the facility. • BES Cyber System Information o Original Text - Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans. o Proposed Change – Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain Medium or High BES Cyber System Impact Designations; equipment layouts that contain Medium or High BES Cyber System Impact Designations; BES Cyber System recovery plans; and BES Cyber System incident response plans. o Rationale – The rewording clarifies the applicability (within CIP-011) of BES Cyber Information controls. • Defined Physical Boundary – Propose reverting back to (retaining) Physical Security Perimeter. The definition can be modified to remove the 'six-wall perimeter' criteria but from a documentation stand-point, requiring renaming what may be unchanged perimeters/boundaries is an additional resource constraint with no security (or compliance) benefit. The concept of physical security provides an excellent complement to electronic security to demonstrate 'defense in depth.' o Rationale – Retaining 'Physical Security Perimeter' allows existing compliance documentation to be used for instances where PSPs are identified within drawings and equipment layouts. • Inter-Entity Real-Time Coordination and Communication – Propose renaming this to 'Inter-Entity Real-Time Coordination' to avoid overlapping existing communication requirements within the COM standards. o Original Text ♣ Activities, actions, and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. ♣ Aspects of the Inter-Entity Coordination and Communication Operating Service include, but are not limited to: • Schedule interchange • Facility operational data and status • Operational directives o Proposed Change ♣ Activities, actions, and conditions necessary for the coordination between Responsible Entities to ensure the reliability and operability of the BES. ♣ Aspects of the Inter-Entity Coordination Service include, but are not limited to: • Schedule Interchange • Facility operational data and status • Reliability directives o Rationale – COM-002 is in the process of defining Reliability directives. This term would provide a more concise scope once the COM-002 definition has been finalized. • Add the following definitions (from CAN-0007) o Electronic Access – Access which allows a user to manipulate software and database (setting) attributes of a CCA by direct (primary) or indirect (from outside the ESP) methods. o Physical Access – Access which allows a user to manipulate hardware settings, and may allow the direct connection of a terminal or a computer that can be used to allow electronic access. o Revocation – Action that results in the inability of an individual to access the CCA. • Other terms which would benefit from definitions o Adverse o Annual – Propose use of definition within CAN-0010 o Impact o Security Plan o Associated • Existing definitions that would benefit from alternative wording o Protected Cyber Assets ♣ This term loses meaning in the context of Version 5 draft 1 definitions, given the loss of logical network qualification or any other means to assess 'associated.' Only with consideration of the network portion of an address can an entity determine whether a cyber asset qualifies as being within an ESP (where network portions of address are identical). o Electronic Access Point ♣ EAPs typically have two (or more) access points and control access into an ESP (logical network) from a less trusted network or communication interface. The current wording could be applied to any port on a network switch within an ESP and fails to focus on interfaces where traffic does flow from a less trusted network to a more restricted network within an ESP. o Electronic Security Perimeter ♣ Suggest retaining the concept of logical network. This provides an easier means to identify "Associated Protected Cyber Assets" as they could be any cyber assets on the same logical network which are not identified as a BES Cyber Asset or BES Cyber System.
Yes
• Control Centers should be capitalized at the end of section 2.13 on page 17. • There should also be a column for LSE in the table provided on page 18. • On page 20, under the category "Balancing Load

and Generation," Non-spinning reserve, the use of 'ramp rates' is typically associated with modeling programs not typically used as real time operation information and should be removed. • Managing constraints (page 21) has an extra bullet that should be removed. • Restoration of BES – 'coordination' all by itself lacks context and should include additional words to better frame the intent, or be removed. • Inter-Entity Coordination and Communication – In additional to the recommend removal of 'communication' from the section, this should also include BA within the Operational Directives.
No
1. Applicability – (4.2.1 and 4.2.2) reference to UFLS and UVLS is a point of concern a. Current wording implies that every distribution feeder which is part of a UV or UF load shedding scheme is now in scope, with all distribution level devices now BES Cyber Assets. This may greatly expand the scope greatly into the distribution level. EEI Members propose the following applicability to identify a more targeted scope: i. Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) under a common control system as required by its regional load shedding program. 2. CIP-002-5 R1 – Propose content change a. Original Content – Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning] b. Proposed change - Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. Low Impact BES cyber systems support Bulk Reliability Operating Services but are not mentioned in the bright line criteria as noted in Attachment 1. However, failure of these cyber systems may adversely impact (i.e. not remain in the NERC prescribed category ranges) the voltage and/or frequency of the connected Bulk Electric System. Low Impact BES Cyber Systems do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning] c. Rationale – The original definition, as worded, creates the impression that all other cyber assets qualify as Low Impact, and does not communicate the criteria within the definition of BES Cyber Asset as a cyber asset that "if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The proposed rewording contributes towards ensuring only assets which have an impact on the BES are the focus of the CIP Standards (and may ensure a more rapid adoption of the Version 5 Standards). 3. The "Rationale – R1" box uses the term "Cyber Systems," which is not a formal term. Suggest changing the case to avoid confusion. 4. The last sentences of R1 and M1 conflict with each other, providing mixed messages specific to Lower Impact BES Cyber Systems/Assets. While Requirement 1 implies there is no need for discrete identification, Measurement 1 discusses evidence for categorizing Low Impact BES Cyber Assets/Systems. 5. Requirement 1.1 a. There is a missing word – "…within 30 calendar days of <when> a change to BES Elements and Facilities is placed into operation. b. The Term "BES Elements and Facilities" used only once within the standards. Suggest changing this phrase to "BES Cyber Assets or Systems." 6. Attachment I - a. High Impact Rating – Propose content change i. Original content – Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at: ii. Proposed change – Each BES Cyber Asset or component of a BES Cyber System located at the facilities listed below that if rendered unavailable, degraded or misused would, within 15 minutes adversely impact the reliable operation of any of the following: iii. Rationale – Some devices may not reside within a Control Center, this rewording provides clarity to focus on assets located within a Control Center in support of BES Reliability Operating Services b. Medium Impact Rating – Propose content change i. Original Content – Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for: ii. Proposed Change - Each BES Cyber Asset or component of a BES Cyber System located at the facilities listed below and not included in Section 1 above, that if rendered unavailable, degraded or misused would, within 15 minutes adversely impact the reliable operation of any of the following: iii. Rationale – The proposed edits more directly connect with the facility and its function within the BES

Bright Line criteria. c. 2.2 – Propose content change i. Original content – An aggregate net Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). ii. Proposed change – Each transmission facility containing reactive devices with an aggregate net Reactive Power nameplate rating of 1000 MVAR or greater. iii. Rationale – the rewording provides the filter (for transmission only facilities) at the front to better identify the applicable Facility. d. 2.7 (Table) – The “Weight Value per Line” for 700 should be replaced with a value in the range of 500-600, which is more representative of the typical rating of 230 kV lines. e. 2.8, 2.9, 2.11 – “Major WECC Transfer Paths in the Bulk Electric System” is not actively maintained by WECC and there is no clearly identified basis for why certain paths are included on this list. As an alternative, we suggest “transmission paths contained in the WECC Path Rating Catalog with a maximum path rating equal to or greater than 1,500 MW.” This catalog is actively maintained by WECC. f. 2.11 – The table titled “Major WECC Remedial Action Schemes (RAS)” is not actively maintained by WECC. As an alternative, we suggest “Each SPS categorized as a ‘Wide Area Protection System’ by WECC” which is the newly created mechanism within WECC to identify SPS systems of significant importance.
No
1. General Observation – Since categorization is based on the facilities role within the BES, independent of the specific BES Cyber Asset or BES Cyber System Role, appropriate categorization fails to require assessment based on the criticality of the BES Cyber Asset or Cyber System in support of applicable BES Reliability Operating Services. 2. Rationale R2 – Propose a content change: a. Original Text - The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. b. Proposed Change - The lists required by R1 are reviewed annually to ensure that all BES Cyber Systems have been properly identified and categorized. 3. R2 – Proposed Change a. Original Text – The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. b. Proposed Change – The Responsible Entity shall have its CIP Senior Manager or delegate annually approve the identification and categorization required by R1. c. Rationale – EEI members propose instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame. 4. M2 – Proposed Change a. Original Text – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. (R2) b. Proposed Change – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate annually approve, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems. (R2) c. Rationale – The requirement only asks for Senior Manager (or delegate) approval. EEI members propose instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.
No
1 – The Violation Risk Factors do not intuitively align with Violation Severity Level (VSL). Requirement 1 assigns a ‘High” VRF independent of the potential low or no risk associated with instances in which BES Cyber Assets or BES Cyber Systems are assigned risk levels higher than those required. EEI would like a more risk based approach in which the compliance assessment considers risk in any non-compliance finding. 2 – For the Last Paragraph VSL’s within R1 (failed to update its documentation), EEI proposes the following time periods: Lower – More than 30, but less than or equal to 60 calendar days Moderate – More than 60, but less than or equal to 70 calendar days High – More than 70, but less than or equal to 80 calendar days
No
While it is documented within the definition, as referenced in the Rationale for R1 the Senior Management, the requirement that the senior manager have “overall authority and responsibility for

leading and managing implementation of the requirements within this set of standards" would benefit from repetition within the R1 requirement itself. Reading 'solely' this standard post rationale removal does not communicate the responsibility adequately. Propose use of 'legacy' wording and numbering schemes within this standard where possible. In this context the cyber security policy requirements should be R1, with 'leadership' requirements being R2 – EEI proposes this be made R2.
No
EEI proposes that 'legacy' wording and numbering schemes be retained within this standard were possible with the change (within CIP-003-4 R1.1) from "addresses the requirements" to "addresses the topics." This requirement should be R1. Rationale – Pre-version 5 language already captures the requirement and has been successfully vetted within the industry. FERC Order 706 did not identify any specific need to change policy language, only to provide additional guidance. Use of the legacy language would minimize approval barriers by ensuring minimal change where appropriate as long as the 'addresses the requirement' language is removed. Sub-numbering (1.1 through 1.10) should be modified to 2.1 through 2.10.
No
This goes beyond the scope of FERC Order 706. In previous versions, this requirement was a sub-requirement within R1. EEI proposes renumbering/rewording this to capture the legacy context. Propose content Change 1. Original Content – Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 2. Proposed change –The cyber security policies require annual review and approval by the senior manager assigned pursuant to R1. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 3. Rationale – The proposed revision carries forward language from previous versions of the standard (CIP-003 R1.3) which captures the root intent while providing language which has already been vetted and approved within the industry.
No
Propose legacy language/numbering from (pre-version 5) R1 1. Draft 1 content – "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function." 2. Proposed revision – "The cyber security policy is readily available to all personnel who have electronic access or unescorted physical access to, or are responsible for Medium or High Impact BES Cyber Systems." 3. Rationale – EEI members indicated making individuals who have access 'aware of elements' of the cyber security policy does not provide adequate guidance to ensure said individuals comply with the cyber security policy.
No
Requirement 5 – propose use of legacy language: • The responsible entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, standards. Rationale – Overall responsibility and authority (from the legacy language) can accomplish "direct and comprehensive responsibility" and "clear authority" (from FERC Order 706), which provides flexibility without the prescriptive requirement for the senior manager or delegate to be responsible for all individual detailed approvals and authorizations in the standards. Citing "all approvals and authorizations" as a Senior Manager was identified as a concern as it is open ended. There were concerns of the additional administrative burden which is not commensurate with the security benefits. Neither the Blackout Report Recommendation 43 nor FERC Order 706 identify the need to establish this administrative overhead. For Security and Reliability NERC should be concerned with the outcome of the approval process, that is, the proper authorizations are being granted by the Responsible Entity which is contained in the other CIP Standards.
No
Propose use of legacy language from CIP-003-3 R2.2: Changes to the senior manager must be documented within thirty calendar days of the effective date.
No
R4 VSL 1. This language cites a High VSL when 'not all' individuals have been made aware of elements of the cyber security policy. This seems to contradict the intent described in the R4 rationale in which 'it is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.' 2. EEI proposes the use of a more gradual scale

rather than a single instance of non-access subject to a High VSL, and total non-access (for all) being a Severe VSL.
Yes
No
1. The rationale for R2 should be reworded from "…contains the proper policies…" to "…covers the required policies…" 2. This extends beyond the guidance of FERC Order 706. Paragraph 435 of the order calls for identifying what "role and steps should be taken by the ERO to ensure quality and consistency of trainers." This requirement should identify what areas of the standards that the training program must include. 3. EEI members question whether this requirement satisfies paragraph 434 of Order 706 where "any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions could, even inadvertently, affect cyber security. 4. R2.2-4 – Can possibly be merged into a single sub requirement a. 2.2 – training on the security controls b. 2.3 – training on the proper use of physical access controls c. 2.4 – training on the electronic access controls 5. R2.6 – Requirement – Proposed word change a. Original - Training on handling of BES Cyber System Information and storage media. b. Proposed Change - Training on handling of BES High and Medium Impact Cyber System Information and storage media. c. Rationale – Rewording supports the applicability section. Since Low Impact Cyber Systems are not applicable, information specific to Low Impact Cyber Systems should not be in scope. 6. Propose merging of R2.7 with R2.9 7. (R2.10) – What changes are required to existing approved training programs to satisfy this new requirement?
No
Measure 3.1 where it calls for the date that access was first granted is a point of concern for both legacy employees (where it may be impossible) as well as new access since existing technology may not adequately capture and retain this information. Requirement 3.2 – Propose content change • Original content – Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months. • Proposed change – Require annual completion of the training specified in CIP-004-5, Requirement R2. • Rationale – The wording adopts the CAN-0010 approach for annual as defined within the registered entity.
No
1. 4.1 a. Version 5 standards should indicate whether previous PRA's would be valid for this requirement (especially within the context of 'initial'). b. EEI proposes a clearer delineation to frame instances in which personal records are not readily available – vs. impossible to obtain 2. 4.2 – Retention requirements do not extend beyond 3 years, creating confusion regarding retention of 7 year cycle background checks. 3. 4.3 a. Most EEI Members favored a process approach over a fixed pass/fail approach independent of the individual or circumstances involved, and propose that the SDT shift away from a criteria based approach. b. The application guideline provides guidance where it is 'not possible to perform a full seven year criminal history check.' c. 4.4 – Provide language to cover contract employees where I9 verification can only be conducted by employers. Service providers also may have instances where certain individuals may be located in another country, and may access certain BES Cyber Assets remotely.
Yes
No
1. R6.1-3,6.4-6 – Propose use of language where access is appropriate for the roles and responsibilities rather than 'minimum necessary.' a. 'Minimum necessary' as identified as difficult to prove within an audit context. 2. 6.3 – Propose content change a. Original content – The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions. b. Proposed change – Access to BES Cyber System Information repositories must be authorized, except for CIP Exceptional Circumstances. c. Rationale – Senior Manager authorization (or management of delegations) provides additional resource and response impacts, which do not provide enhanced security and may impact reliability efforts when recovery processes are activated. Ensuring access is authorized will satisfy security controls without adding unnecessary overhead. 3. 6.4 – EEI proposes conducting this task on an annual basis as the quarterly requirement

will introduce extreme resource constraints in some instances.
No
1. 7.1 - There are questions in instances where resignations and/or terminations may be retroactive, which would introduce a challenge with revocation 'at the time of' events. 2. 7.2 – Transfers or reassignments should frame access changes when no longer needed rather than the date of the transfer (as cited in the Measure (i)). 3. 7.3 – Propose use of 'approved BES Medium and High Impact Cyber System Information repositories,' to frame an appropriate location in which information can be managed and controlled.
Yes
No
EEI believes the Version 5 approach (as described within the R1 rationale "Summary of Changes") of focusing on discrete Electronic Access points rather than a logical perimeter adds confusion when determining Associated Protected Cyber Assets. A discrete list fails to recognize the inherent controls and permissions within a logical network. Control of routable protocol should consider the inherent network/host identifiers embedded within the addressing scheme in which all devices with an identical network component of their address are peers within a logical network, where access points do not serve as access control. Rationale for R1 – Propose content change • Original Text - The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks. • Proposed Change - The Electronic Security Perimeter serves to control traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic according to a specified rule set, and assists in containing any successful attacks. • Rationale – Monitoring is not identified within any R1 requirements. Table R1 1. R 1.1 1. Applicability - Propose use of "External Connectivity" instead of "External Routable Connectivity" (to include dial-up capability). 2. Propose removal of "and have been implemented" from the end of the measure statement to avoid tracking compliance on a 'per-device' basis, otherwise this would introduce the need for tracking this information for low impact BES Cyber Systems. 2. R 1.2 1. Applicability – 1. Modify to frame applicable Cyber Systems/Cyber Assets as those with External Connectivity. 2. Propose elimination of Associated Physical Access Control Systems as their introduction indicates applicability to subsequent subrequirements which doesn't add to overall security and presents extensive resource requirements. 2. Requirements – Propose content change 1. Original content – Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs). 2. Proposed change – Control and secure all External Connectivity through the use of identified Electronic Access Points (EAPs). 3. Rationale – The focus within CIP-005 should be on EAP devices with External Connectivity. 3. R 1.3 1. Requirements – proposed change 1. Original Text - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions. 2. Proposed Change - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting access, denying all other access requests by default. 4. R1.4 – There were various interpretations of 'non-Interactive Remote Access,' which implies this requirement may need some additional clarification. This seems to be the only requirement where documentation of authentication measures appears within this standard. Consider removing 1.4 and modifying 1.2 to cover both rows.
No
1. Table R2 1. R2.1 1. Requirements – Request rewording to support placement of an intermediary device that may not be part of an ESP. 2. R2.2 1. Requirements – Propose clarification on viable termination points for encrypted traffic to support unencrypted traffic through Electronic Access Points. 2. Rationale – The ability to filter traffic effectively becomes much more difficult if the traffic is encrypted. Supporting technical implementation where encrypted traffic is decrypted prior reaching Electronic Access Points to allow for further access control would benefit security capabilities. 3. Overall – Propose breaking table R2 into a Routable and Dial-Up categories to more effectively frame routable controls and dial-up controls without introducing confusion for the alternate approach.
No
1. Classifying instances where no documentation of compliance exists as severe is appropriate;

instances in which a minority of non-compliance controls were identified within a primarily compliant program should be assessed a VSL with respect to the finding (page 17, bottom Severe VSL). 2. VSLs addressing 'each identified EAP' and 'all Interactive Remote Access' should be assessed as a sliding scale to consider whether lower/moderate/high may be more applicable.
No
1. Table R1 a. R1.1 i. Applicability – 'Medium Impact BES Cyber Assets with no External Connectivity' should be added 1. Rationale - Medium Impact BES Cyber Assets should only require fully Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Measures – Proposed Rewrite 1. Original Text – Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented. 2. Proposed Change – Evidence may include, but is not limited to, documented operational or procedure controls that have been implemented. b. R1.2 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Measures – Proposed Change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs. 2. Proposed Change – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how access is controlled. 3. Rationale – FERC Order 706 did not ask for egress access controls. The additional criteria at the end of the measure extend beyond what FERC has asked for, with minimal security benefit. c. R1.3 i. Requirement – Propose change 1. Original content – Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible. 2. Proposed change – Utilize two or more different physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible. 3. Rationale – 'different and complementary' does not provide adequate guidance. The Measure R1.3 only references 'different. ii. Measure – only mentions 'different' access control methods with no reference to complementary (as included within the requirement). d. R1.4 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Requirement – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 2. Proposed Change – Issue alerts within 15 minutes (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 3. Rationale – The 15 minute criteria (Referenced in the 'Table of Compliance Elements,' page 21, R1 – High) provides greater clarity to satisfy alerting requirements. iii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that

describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs, or other evidence that documents that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. e. R1.5 i. Requirements – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 2. Proposed Change – Issue alerts within 15 minutes (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 3. Rationale – The 15 minute criteria (referenced in the 'Table of Compliance Elements,' page 20, R1 – High) provides greater clarity to satisfy alerting requirements. ii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. f. R1.6 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Requirements – Proposed Change 1. Original Text – Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry. 2. Proposed Change – Log (through automated means or by personnel who control entry) of authorized individual's physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the authorized individual and date of entry. 3. Rationale – The addition of authorized provides additional segmentation from R2 (Visitor Control) access requirements.
No
Table R2 1. R2.1 a. Applicability – Applicability wording of "Medium Impact BES Cyber Assets should be changed to "Medium Impact BES Cyber Assets with External Connectivity." i. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. 2. R2.2 a. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." i. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. b. Requirements – Proposed Change i. Original Text – A process requiring manual or automated logging of the entry and

exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact. ii. Proposed Change - A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the first entry and last exit, the visitor's name, and individual point of contact. iii. Rationale – The proposed change capture the intent with (hopefully) clearer language. The 24 hour basis may introduce expectations that 'round-the-clock' logging needs to be in place. Some visitations may cross the midnight time-line, which shouldn't introduce additional requirements.
No
Table R3 1. R3.1 a. Overall observations – EEI members felt that the shift from (pre-V5) maintenance on 'mechanisms' to the Draft 1 'systems' expands this requirement beyond the intent. • This should be more focused on testing to ensure alerting and control mechanisms work as intended. • Use of controls should be considered 'tested' in situations where applicable devices are used every day (i.e. card readers). b. This sub requirement cites tasks to be conducted 'prior to commissioning.' Since many controls are expected to be in place prior to V5 adoption, there should be language within the implementation plan to capture devices in use at the time the standard becomes effective. 2. Compliance a. 1.5.2 – Evidence retention should keep the existing 90 day period for physical access logs as extending this to 3 years can create extensive commitment in storage media, particularly for video monitoring.
No
The Table of Compliance Elements cites references to sub requirements that appear to be incorrect: • Lower – Part 1.7 should point to 1.6 • High – Part 1.6 should point to 1.5
No
R1.1 – Requirements – Proposed Content Change 1. Original Content – Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. 2. Proposed Change – Enable only logical accessible ports needed, including port ranges where required. 3. Rationale – The proposed language incorporates much of the legacy (CIP-007-3 R2.1) language. The additional requirement to document the need for remaining logical ports extends beyond what FERC Order 706 requests without adding security benefits. R1.2 1. Requirements – Content Change a. Original Content - Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. b. Proposed Change – Protect against the use of unnecessary physical input/output ports that could be used for network connectivity, console commands, or removable media by disabling, restricting, or use of signage. 2. Measures – Content Change a. Original Content - Evidence may include, but is not limited to, documentation stating specific or types of physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. b. Proposed Change - Evidence may include, but is not limited to, documentation stating specific physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage.
No
2.1 1. Requirements – Content Change a. Original Content - Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. b. Proposed Change – Identify a source or sources that are monitored for the release of security related patches, or security updates for software and firmware associated with BES Cyber System or BES Cyber Assets. 2. Measures – Propose striking the last sentence "The list could be sorted by BES Cyber System or source." It introduces additional requirements with no clear security benefit or alignment with FERC Order 706. 3. 2.2 and 2.3 should be switched, as 2.3 requires the establishment of a process for remediation, and 2.2 addresses the creation or revision of the remediation plan. 4. 2.2 a. Requirement – Propose content change i. Original content - Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe. ii. Proposed change – Identify applicable security-related patches or updates within 30 days of release from the identified source that addresses the vulnerabilities, and create or revise a remediation plan that addresses the vulnerabilities within a defined timeframe. iii. Rationale – The rewording captures the chronological order of the elements within this requirement to provide clearer guidance. 5. 2.3 a. Requirement – As

currently worded, there is no allowance for changes in the remediation plan should outage coordination, or other resource constraints require modifications to the remediation plan. This is a point of concern that should be addressed.
No
1. 3.2 a. Requirement – Content Change i. Original content – Disarm or remove identified malicious code. ii. Proposed change – Mitigate the threat of identified malicious code. iii. Rationale – In some instances, the presence of malicious code may present a lesser risk to the reliability of the BES than disarming/removal processes, especially when the malicious code may not exploit a feature used within the Cyber System. b. Measure – Add a bullet to allow for evidence of manual removal. 2. 3.3 a. Requirement – Propose content change i. Original content – Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). ii. Proposed change – Update malicious code protections from the identified source within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). iii. Rationale – The addition of 'the identified source' provides a context for determination of availability. b. Include testing within both the requirements and measures as alluded to within the Application Guidelines (page 41). c. Measures – Format (i) and (ii) to a bulleted list signifying 'or' criteria 3. 3.4 a. Applicability – Propose deletion of Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems as they do not appear to be Transient Cyber Asset related. b. Requirements – Content Change i. Original Content - Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change – Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to Medium or High Impact BES Cyber Assets or Protected Cyber Assets. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. ii. Proposed Change – Evidence may include, but is not limited to, an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. iii. Rationale – Excised content introduced prescriptive criteria that introduced additional resources without clearly addressing the requirement. 4. 3.5 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems and Associated and they do not appear to be Transient Cyber Asset related. b. Requirements – Append "to Medium or High Impact BES Cyber Assets or Associated Protected Cyber Assets" to the end of the requirement. c. Measures – Content Change i. Original Text – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change - Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to Medium or High Impact BES Cyber Assets or Protected Cyber Assets.
No
R4 1. 4.1 a. Requirements – Content Change i. Original Content - Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. ii. Proposed Change – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. Devices that cannot log a particular event do not require a TFE to be generated. iii. Rationale – Content from the application guidelines has been introduced to promote the guidance that TFE's are not required in instances in which devices cannot log a particular event. 2. 4.2 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control Systems as they are out of scope for this requirement. b. Requirements – Content Change i. Original Content – Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert. ii. Proposed Change – Generate alerts for events that the Responsible Entity determines necessary. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate real-time alerts; Assessment documentation or report

showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert; Screenshots showing how real-time alerts are configured. ii. Proposed Change – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate an alert; Screenshots showing how alerts are configured. iii. Rationale – Removed the usage of 'real-time' as it presents concerns demonstrating compliance. 3. 4.3 a. Requirements – Content Change i. Original Text – Detect and activate a response to event logging failures before the end of the next calendar day. ii. Proposed Change – Activate a response to failures of event logging before the end of the next calendar day after identification. iii. Rationale – Some devices generate logs so infrequently that identification of logging failure may extend beyond any calendar day. The spirit of this requirement remains intact as one day remediation is required once the log failure is identified. 4. 4.4 a. Requirements – Content Change i. Measures – Content Change 1. Original Text – Evidence may include, but is not limited to, security-related event logs from the past ninety days and records of disposition of security related event logs beyond ninety days up to the evidence retention period. 2. Proposed Change – Evidence must include, but is not limited to, security-related event logs from the past ninety days. 5. 4.5 a. Requirements – Content Change i. Original Content – Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day. ii. Proposed Change - Review a summarization or sampling of logged events every two weeks to identify BES Cyber Security Incidents and potential event logging failures. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008. b. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred, and dated evidence showing that personnel were dispatched or a work ticket was opened to rectify the deficiency. ii. Proposed Change – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), and signed and dated documentation showing the review occurred. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008.
No
R5 1. 5.1 a. Overall – EEI and its members struggled with providing alternate wording for this subrequirement. In both the original content and proposed change there exists a instances where access is a component of validation and/or authentication. This presents a potential compliance challenge that should be addressed. b. Requirements – Content Change i. Original Content – Validate credentials before granting electronic access to each BES Cyber System. ii. Proposed Change – Authenticate user account access before granting electronic to each Medium or High Impact BES Cyber System or Associated Protected Cyber Asset, where technically feasible. iii. Validating credentials was seen as vague specific to technical compliance so authentication is offered as an alternate approach to satisfy the root requirement (and mirrors the language in the change rationale). The addition of 'where technically feasible' was to recognize technical capabilities currently in place may not adequately demonstrate compliance with this. 2. 5.2 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 3. 5.3 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 4. 5.4 a. Requirements – Content Change i. Original Text – Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. ii. Proposed Change – Procedural controls for initially removing, disabling, or changing default passwords, where technically feasible. For the purposes of this requirement an inventory of Cyber Assets is not required. iii. Rationale – The additional wording identifies the multiple methods which can be used to mitigate default passwords. 5. 5.5 a. Requirements i. Change Systems to Assets throughout as password limitations should be identified to the device level. ii. Add language to 5.5.3 to cover instance where accounts may not be able to support password change to permit the entity specified time frame to be equal to the life-time of the BES Cyber Asset where technically required.

No
Violation Severity Levels 1. R3 a. Propose switching High and Severe Columns as the High captures instance in which no methods were deployed, Severe captures instances in which incomplete methods were deployed. b. The initial paragraph in Severe is duplicated in High. 2. R4 a. Moderate – delete 'identify and implement methods to' b. High – delete 'identify and' 3. R5 a. High – The initial paragraph doesn't align with a requirement, propose striking.
No
1. Rationale R1 1. The initial sentence is fragmented, providing an incomplete framing for R1. Absent a complete sentence, proposing alternate language to better frame this rationale is difficult. Propose rewriting this sentence. 2. Regarding applicability to all registered entities – While EEI Members understand the need for all entities to have an effective process to respond to incidents within each organization, for the purposes of CIP-008 it would be best to establish applicability to entities with Medium and High Impact BES Cyber Assets/Systems, as those are the impact ratings in which Defined Physical Boundaries and Electronic Security Perimeters are required. 3. R1.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 4. R1.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 5. R1.3 1. Requirements ♣ The initial 'define' should be expanded to provide a complete sentence (i.e. An entities BES Cyber Security Incident Response Plan should include). 2. Measures – Content Change ♣ Original • Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of BES Cyber Security Incident response personnel, BES Cyber Security Incident handling processes or procedures, and communications processes or procedures. ♣ Proposed Change • Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of; o BES Cyber Security Incident response personnel, o BES Cyber Security Incident handling processes or procedures, o Communications processes or procedures.
No
R2 1. 2.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 2. Requirements – Content Change ♣ Original Content • When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test. ♣ Proposed Change • When a BES Cyber Security Incident occurs, the incident response plans must be used and include recording of deviations taken from the plan during the incident. 2. 2.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist.. 2. Requirements – Content Change ♣ Original Content • Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): o by responding to an actual incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Proposed Change • Test the incident response plan(s)

annually. A test of the plan may include: o A response to an incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Rationale – References to requirements needed upon the effective date should be captured within the implementation plan, allowing the standard to identify requirements (only) in place once the standard is approved. 3. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence showing annual testing of the BES Cyber Security Incident response plan(s). Types of exercises may include discussion or operations based exercises. Document lessons learned within 30 days of incident or exercise. Use lessons learned to update incident response plan(s). ♣ Rationale – The Homeland Security Exercise and Evaluation Program identifies seven types of exercises within HSEEP, each of which is discussions-based or operations-based. 3. R2.3 – Propose deletion as this sub requirement merely identifies retention requirements already documented within Compliance (C.1.2).
No
1. R3 1. 3.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – The formal definition of BES Cyber Security Incident includes attempts to compromise the ESP or DPB, requiring Medium or High Impact BES Cyber Systems/Assets. 2. 3.2 1. Requirements – Propose content change a. Original content – Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan. b. Proposed change – Use lessons learned from incident responses or incident response exercises to update the incident response plan, within sixty days of documenting lessons. c. Rationale – It takes 30 days from the time an exercise is executed to the review and completion of an after action report. The thirty day clock should start once the after action report is completed. This is in line with the proposed 60 day timeline in R3.3. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan. ♣ Proposed Change – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or incident response within thirty calendar days of the lessons learned associated with the response plan. 3. 3.3 1. Requirements – Content Change ♣ Original Content • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan. ♣ Proposed Change • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that test or incident. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan. ♣ Proposed Change – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan test or incidence response and the dated, revised plan.
No
1. R1 – Severe 1. 2nd paragraph, add 'types' to the end of the paragraph (…plan does not identify Reportable BES Cyber Security Incident types). 2. R2 – Severe 1. The second paragraph should be modified from "The Responsible Entity has not tested the execution of its BES Cyber Security Incident Response Plan" to "The Responsible Entity has not executed its BES Cyber Security Incident Response Plan" 2. Rationale – This paragraph aligns with R2.2 which requires activation or exercising the plan. The revised words better support requirement R2.2. 3. R3 1. High VSL (first paragraph) – Content change ♣ Original content • The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 30 calendar days of execution. ♣ Proposed Change • The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 60 calendar days of completion. ♣ Rationale – This VSL combines the review (3.2) with the update (3.3) requirement, the 60 days support the 3.3 requirement.

No
• Overall 1. Propose renaming this Standard to “Recovery Plans for BES Cyber Systems” 2. The revised structure of CIP-009-5 documents requirements for backup media in both R1 and R2. Creating a requirement in which backup media requirements are consolidated (in-line with version 3) would provide a more concise means to identify media requirements. The requirements (as proposed) would be as follows: 1. R1 – Recovery Plan 2. R2 – Exercise of the Recovery Plan 3. R3 – Backup Media 4. R4 – Maintaining the Recovery Plan 3. References to ‘implement’ should be changed to ‘exercise’ regarding recovery plans to better capture activation of the plan vs. ‘release and publish’ efforts. 4. Actions required in advance of the implementation date (2.1, 2.2) should be removed from the standard(s) and included within the implementation plan. • Introduction 1. Purpose – Proposed Content Change 1. Original Content – Standard CIP-009-5 ensures that recovery plan(s) related to the storing of backup information are put in place for BES Cyber Assets and BES Cyber Systems and that these plans support and follow established business continuity and disaster recovery techniques and practices. 2. Proposed Change – Standard CIP-009-5 ensures that recovery plan(s) are put in place for BES Cyber Assets and BES Cyber Systems. 2. Applicability 3. Background • Requirements and Measures 1. R1 1. 1.1 – Propose alternate language (carried forward from previous versions) 1. Create and implement a recovery plan that at a minimum includes: ♣ Conditions for activation of the recovery plan ♣ Roles and responsibilities of the responders 2. 1.2 – Propose deletion as this sub requirement has migrated to R1.1 proposed R1.1 rewrite. 3. 1.3 1. Requirement – Content Change ♣ Original – One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality ♣ Proposed Change – One or more processes for the backup, storage, and restoration of information required to restore BES Cyber System functionality ♣ Suggest additional content supporting mirroring and/or redundancy within the backup/recovery methods such as: • Mirroring and/or redundancy can be considered as complementary measure in support of this requirement, but a process must be in place to ensure retrieval of previous versions should current version(s) require reverting to a previous instance. ♣ Rationale – Protection of BES Cyber System Information is addressed within CIP-011. 2. Measure – Content Change ♣ Original – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and protection of information required to successfully restore a BES Cyber System. ♣ Proposed Change – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and restoration of information required to successfully restore a BES Cyber System. ♣ Rationale – Protection of BES Cyber System Information is addressed within CIP-011. 4. 1.4 – Correct headers from ‘part’ to ‘Applicability,’ ‘Requirements,’ and ‘Measures’ 1. 1.4 ♣ The current form does not adequately address FERC Order 706, paragraphs 739 and 748, and in fact contradicts the intent that ‘The Commission does not believe that every change will necessitate verification of the backup and restoration processes’ from paragraph 740. ♣ Propose ‘new’ sub requirement applicable to High Impact BES Cyber Systems to require: • Upon implementation of significant changes to High Impact BES Cyber Systems, verify that backups are operational before they are relied upon for recovery purposes. ♣ Propose rewrite • Original – Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully. • Proposed Change – Ensure that backup processes are completed successfully for Information essential to BES Cyber System recovery. • Rationale – This focuses on successful completion of the backup process which can be done within the routine backup. Verification would be moved to its own requirement applicable to High Impact BES Cyber Systems and limited to significant change instances. 5. 1.5 1. Requirement – Content Change ♣ Original Content – Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. ♣ Proposed Change – Document root cause for events that trigger activation of the recovery plan(s) as required in Requirement R1. ♣ Rationale – Root cause documentation should be the focus for this requirement. The current draft language requires potential impediments to restoration efforts and is too vague.
No
1. 2.1 1. Requirements – Content Change ♣ Original – Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: by recovering from an actual incident, or with a paper drill or tabletop exercise, or with a full operational exercise ♣ Proposed Change – Implement the recovery plan(s) referenced in R1 annually: • by recovering from an actual incident, or • with a tabletop exercise, or • with a functional exercise ♣ Rationale – Use of the

functional exercise aligns with the R2 rationale content citing NIST SP 800-84 exercise types. Requirements in advance of the effective date of the standard should be addressed within the implementation plan. 2. Measures – Content Change ♣ Original – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with a full operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a tabletop exercise, or with a functional exercise) of the recovery plan annually. For the table top or functional exercise, evidence may include meeting notices, minutes, or other records of exercise findings. 2. 2.2 1. Requirements – Content Change ♣ Original Text – Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations. ♣ Proposed Change – Test information used in the recovery of BES Cyber systems that is stored on backup media annually, to ensure that the information is useable. 3. 2.3 1. Overall ♣ This requirement (to be done every 39 calendar months) appears to overlap considerably with 2.1 (to be done every year). ♣ Every 39 calendar months exceeds the 3 year retention identified within the Compliance section. ♣ How does this differ from current EOP-008 requirements? 2. Requirements – Content Change ♣ Original – Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise. ♣ Proposed Change – Exercise the recovery plan(s) at least every 39 calendar months through an operational exercise in a representative environment. An actual recovery response may substitute for an operational exercise. ♣ Rationale – Actions required to take place prior to the effective date of the standard should be captured within the implementation plan.
No
1. 3.1 1. Requirements – Content Change ♣ Original – Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned. ♣ Proposed Change – Review the recovery plan(s) annually and document any identified deficiencies. ♣ Rationale – Requirements addressing tasks to be done prior to the effective date should be captured within the implementation plan. 2. 3.2 1. Requirements – Content Change ♣ Original – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned. ♣ Proposed Change – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of completion, documenting any identified deficiencies or lessons learned. 3. 3.3 4. 3.4 – Propose deletion as the requirement is too broad with no clear alignment with FERC Order 706 or security benefit. 5. 3.5 2. Requirements – Content Change ♣ Original – Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed. ♣ Proposed Change – Updates to the recovery plan(s) shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of being completed. ♣ Rationale – The proposed change leverages ‘pre-version 5’ language which satisfies the intent of the requirement.
Yes
No
1. R1 1. Rationale – The current wording doesn’t capture the intent of FERC Order 706, paragraph 399: 1. We do not seek absolute assurances but rather are concerned that there be processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. 2. Suggest referencing this directive within the rationale, and ensure configuration management focus more on the spirit of the FERC Order rather than the currently framed “prevent unauthorized modifications to BES Cyber Systems.” 2. R1.1 a. CIP-010-1 R1.1 should be replaced with CIP-003-4 R6 i. Rationale – CIP-010-1 R1.1 is too prescriptive. CIP-003-4 R6 is closer to a results based requirement and provides more flexibility to achieve the desired results. CIP-010-1 R1.1

greatly expands the scope of change control and configuration management (CIP-003-4 R6) beyond what was directed in FERC Order 706. FERC Order 706 paragraphs 397 and 398 directed "modifications to CIP-003-1 R6 to provide an express acknowledgement of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." The concern was that some form of verification is performed to detect when authorized changes have been made. CIP-010-1 R2.1 addresses Order 706's concern for some form of verification to detect unauthorized changes. (CIP-010-1 R2.1 should delete reference to the baseline defined in CIP-010-1 R1.1.) FERC also did "not believe the changes will have burdensome consequences." CIP-010-1 R1.1 requires extensive and burdensome details tracking. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1. 1. 1.1.4 – Propose content change ♣ Original Text – Any custom software and scripts developed for the entity; ♣ Proposed Change – Any custom software and scripts installed on the BES Cyber Asset that can affect the security posture. ♣ Rationale – The change focuses scope to eliminate software and scripts not in use. 2. 1.1.5 – Propose content change ♣ Original Text – Any logical network accessible ports; and ♣ Proposed Change – Any network accessible ports or services; and ♣ Rationale – This clarifies the requirement to focus on 'active ports and services' rather than Ethernet jacks. 3. R1.2 1. Requirement – Propose content change ♣ Original Text – Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Proposed Change – Document approved changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Rationale – As documented earlier in this comment form, requiring Senior Manager (or delegate) authorization introduces resource constraints that impede the effective documentation of changes without adding security benefits or alignment with FERC Order 706. 2. Measure ♣ First paragraph – Add 'or,' at the end of the first bulleted paragraph. ♣ Second paragraph – Propose content change • Original Text – A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) were an individual with the authority to authorize the change was in attendance. • Proposed Change – A record of the change with authorization of the change. • Rationale – Citing a "change advisory board" within the measure overly represents adequate evidence in support of the requirement. 4. R1.3 1. Requirements – Propose content change ♣ Original Text – Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change. ♣ Proposed Change – Update the documented baseline configuration as necessary within 30 calendar days of completing the change. ♣ Rationale – The proposed rewording provides more focus on the root requirements. 5. R1.5 1. Requirements – Propose content change ♣ Original Text • 1.5.1 – Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any difference in operation between the test and production environments. ♣ Proposed Change • 1.5.1 – Prior to implementing any change from the existing baseline configuration in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment. ♣ Rationale – Proposed rewording provide greater focus on the root requirements. 2. Measures – Propose content change ♣ Original Text – Evidence includes, but is not limited to, a list of security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test. ♣ Proposed Change – Evidence includes, but is not limited to, a list of security controls tested along with the date of the test, test results, and a list of differences between the production and test environments.
No
1. R2 1. 2.1 1. Applicability – Propose removal of Medium Impact BES Cyber Systems. ♣ Rationale – The technology required to monitor/detect for changes is relatively new and not aligned to BES Cyber Systems which would be in place within a Medium Impact facility (substations, etc.). 2. Requirements – Propose content change ♣ Original Text – Where technically feasible, monitor for changes to the

baseline configuration (as defined per CIP-010_ R1, Part 1.1) and document and investigate the detection of any unauthorized changes. ♣ Proposed change – Where technically feasible, detect and document unauthorized changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1).
No
1. 3.1 1. Requirements – Proposed content change ♣ Original Text – Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed. ♣ Proposed Change – On an annual basis, conduct a paper assessment of the cyber security controls to determine the extent to which the controls are implemented correctly and operating as designed. • Propose the addition (3.1.1) of minimum cyber security controls to be assessed that; o Are referenced within these standards; and o Are not already required to be assessed in other standards (removing double jeopardy implications) ♣ Rationale • Annual (as defined within CIP-0010) should be the consistent approach to allow entities to standardize annual requirements on a consistent basis. • Active assessment is cited within Part 3.2 (to be done every 39 months) so we've removed it from this part to avoid overlap. 2. Measures – Propose content change ♣ Overall – There needs to be clear segmentation from ♣ Original Text – Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the output of the tools used to perform the assessment. ♣ Proposed Change – Evidence may include, but is not limited to: • A document listing the date of the assessment, the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the assessment results. ♣ Rationale – Annual should align with CAN-0010 definition. Documentation of assessment results focus on the root information in support of vulnerability rather than potentially extensive data (from tools) that may require extensive resources to retain. 2. 3.2 1. General observations ♣ While the application guidelines recognize production devices which may not be capable of modeling within a test environment (ICCP, etc.), this requirement does not provide clear guidance to follow where these instances occur. ♣ The 39 month cycle exceeds the 3 year retention requirements. 2. Requirements – Propose content change ♣ Original Text – Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments. ♣ Proposed Change – At least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production. 3. Measures – Propose content change ♣ Original Text – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment. ♣ Proposed Change – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments. 3. 3.3 4. 3.4 1. Requirements – Propose content change ♣ Original Text – Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Proposed Change – Document the results of the assessments (conducted within 3.1-3.3) and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Rationale – referencing parts 3.1 – 3.3 provides alignment with the previous parts of the standards.
Yes

No
1. 1.1 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed content change ♣ Original Text – One or more methods to identify BES Cyber System Information. ♣ Proposed Change – Implement one or more methods to identify BES Cyber System Information. ♣ Rationale – Additional wording frames this in a more complete manner. 2. 1.2 1. Overall – Correct column header labels within the table. 2. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 3. Requirements – Propose content change ♣ Original Text – Access control and handling procedures for BES Cyber System Information. ♣ Proposed Change – Demonstration of access control for BES Cyber System Information. ♣ Rationale – Additional wording frames this in a more complete manner. 3. 1.3 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed content change ♣ Original Text - Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. ♣ Proposed Change – Annually assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. 3. Measures – Proposed content change ♣ Original Text – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence to demonstrate that the action plan was implemented. ♣ Proposed Change – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence of the status of the action. ♣ Rationale – Rewording allows for action plans which may be 'in progress' towards implementation, capturing instance in which remediation may rely on deliverables (not yet received) by vendors.

No
1. 2.1 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed Change ♣ Original Content – Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media. ♣ Proposed Change – Prevent the unauthorized retrieval of BES Cyber System Information from BES Cyber Asset media prior to the release of BES Cyber Asset media for reuse. ♣ Rationale – While not directly changing the intent of the requirement, this rewording has been suggested to provide greater clarity of the root requirement. 2. 2.2 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts.
No
R1 (Severe) – Propose removal of the first paragraph as it is mirrored within the subsequent paragraphs that better frame the violation.
No
The Edison Electric Institute (“EEI”) submits this executive summary concerning the Project 2008-06 Cyber Security Order 706 Version 5 CIP Standards as published 11/7/2011. EEI is the association of the nation’s shareholder-owned electric utilities, international affiliates, and industry associates world-wide. EEI takes the subject of cyber security and infrastructure protection very seriously, and is committed to the reliability of the Bulk Electric System. This commitment includes timely completion of Version 5 and filing a comprehensive set of revisions to the CIP standards for approval with the Commission. EEI appreciates the significant level of effort on the part of the CS 706 Standards Drafting Team, NERC staff, and industry stakeholders in the development of revisions to the CIP standards. EEI has provided a considerable number of comments and suggestions for revisions and enhancements to the Draft of Version 5. These suggestions for revisions are intended to improve the clarity and quality of the Draft. We encourage members of the CS 706 Standards Drafting Team to have an open mind when considering stakeholder feedback, and be willing to closely review and potentially remove new mandatory security requirements that are not specifically required by FERC Order 706 or that fail to provide meaningful security enhancements at a cost that can be afforded by the consumers of electricity. Any proposed modifications to the CIP Standards should appropriately recognize the significant investment that the industry has already made in adopting CIP Version 1, 2 and 3. New or modified requirements should build upon and leverage existing security programs and investments. We observe that there are a significant number of stakeholders who have concerns about the proposed framework change in CIP-002-5 for identification of the cyber assets to be protected and concerns with extensive changes in definitions. We recommend that the SDT carefully evaluate alternative strategies offered by stakeholders to address these concerns. In addition, we observe that there are a significant number of stakeholders who have great concern about the new proposals regarding low-impact BES cyber assets, both as to appropriate identification, and concerning the new mandatory controls that have been identified for low impact BES cyber assets. Technical experts have broadly varying positions on whether these assets should be covered by the mandatory NERC standards, as well as the nature of the controls that should be applied. IT and security systems professionals also continue to struggle with the design of the NERC standards, a template that is not ideally suited to addressing IT systems issues. Rigid adherence to a set of static requirements may serve to bring “Compliance”, but “Compliance” in this sense is not necessarily equivalent to actual enhancements in the security posture, reduction of risk, or increasing the

reliability of the Bulk Electric System. With regards to addition of new administrative requirements, many in the industry are concerned that the additional cost will bring little or no security benefit. The redefinition of annual, the added requirements for delegations, along with other new administrative requirements will not enhance security and may divert finite resources to non-security related efforts. We recommend that the SDT continue to evaluate alternative strategies that would allow for addressing the outstanding FERC Order 706 directives in a manner that does not create a situation where the electric sector is expending disproportionate resources for compliance activities associated with low impact BES cyber assets in comparison to medium or high impact BES cyber assets. We recommend that any new mandatory security controls be closely scrutinized to ensure that they provide a meaningful increase in the security and reliability of the BES that is commensurate with the amount of resources that are required to establish and maintain them. In the event that new mandatory security controls are established for low impact BES cyber assets, we recommend that implementation deadlines for the low impact BES cyber assets, where appropriate, occur after implementation deadlines for medium or high impact BES cyber assets.

Group

PNM Resources (Includes Public Service Co. of New Mexico and Texas New Mexico Power

Michael Mertz

Yes

• The proposed definition of BES Cyber Asset has not addressed the interpretations that have clarified "Cyber Asset" in previous versions of the standard. Without clarifying the term "Cyber Asset" it will continue to result in inconsistent application of the standards. • The term BES Cyber System may include cyber assets and communication equipment and networks that are not owned and or operated by a NERC registered entity. Furthermore these assets and networks are beyond the statutory authority of FERC or NERC, and are regulated by other regulatory bodies. The terms in this document cannot be used to expand regulatory authority. The definition should be revised to exclude WAN communication systems utilized by the BES Cyber Systems similar to the exclusion in existing versions of the standard. • BES Cyber System-the term is ambiguous and will result in inconsistent application of the standards. It will be difficult for entities to determine where one "system" ends and another "system" begins. For example, where does an Energy Management "System" end, at the front end processors, the RTU's, the I/O? Where does the substation automation system begin? These are both presumably examples of BES Cyber Systems. • The definition of BES Cyber System contains the term "Maintenance Cyber Asset", which is not a defined term. It appears as though it should be "Transient Cyber Asset". • The definition of BES Reliability Operating Services is lengthy and confusing. There is concern that it will be difficult to audit to this definition and that it conflicts with the established bright line criteria. • The definition of CIP Exceptional Circumstance should include the word "may" to read "A situation that may involve one or more…." • There have been significant changes in the basic terms and definitions which have been used since the inception of the CIP standards, including dropping core concepts such as Critical Assets, Critical Cyber Assets, Physical Security Perimeter, and substantial changes in definitions to remaining terms. These changes are not clearly required to support FERC Order 706, or to enhance the security controls within the Bulk Electric System. EEI proposes that approved definitions within the CIP Standard (pre-Version 5) are retained whenever possible. We understand any need to modify the definition to align with FERC Order 706 or enhance security, and would much prefer new definitions over any elimination or introduction of terms. EEI members are opposed to any instances of changes where there is no clear need as each modification requires extensive resources to modify existing compliance processes and evidence. The removal of Physical Security Perimeter as a term (replaced by Defined Physical Boundary) is the primary example where the definition could be modified while retaining use of Physical Security Perimeter. • The loss of Critical Assets removes facilities from consideration. This presents challenges in assessing BES Cyber Systems as they provide services to a facility which provides BES Reliability Operating Services – not the BES Cyber System independently. This also introduces the approach in which BES Cyber Systems are not independently assessed for impact with consideration to the specific service they support, but are assigned the impact of the BES Reliability Service (conducted within a facility). The methodology should recognize the facility within impact assessment, and allow for subsequent entity assessment of the impact of any supporting BES Cyber System, whether they reside within facility or in another location in support of the facility. • Requirements and/or Measures that use all-encompassing words like 'any,' and 'all' introduce compliance challenges, as satisfying these definitions potentially introduce extensive additional

elements that would be out of scope should more concise language be used. • Extension of the default retention requirements within all the standards from the current 'previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation,' to 'three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation' is not identified within FERC Order 706 nor does it enhance security commensurate with resource expenditures. EEI members would prefer use of the current 'previous full calendar year' retention period. • BES Cyber Asset – Proposed Definition Change o Original Text – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. o Proposed Change – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact the capability of the facility with which it is associated to perform one or more BES Reliability Operating Services. Redundancy shall not be considered when determining adverse impact. A Transient Cyber Asset is not considered a BES Cyber Asset. o Rationale – Impact Ratings as defined within CIP-002-5 focus on the role of the facilities' function specific to BES Reliability Operating Services. The BES Cyber Assets support the facility in providing that service. • BES Cyber System – Proposed Content Change o Original Text – One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System. o Proposed Change – One or more BES Cyber Assets that are logically grouped together to operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. o Rationale – Absent logical grouping, there is no clear understanding of how a BES Cyber Asset qualifies as a component of a BES Cyber System. Physical grouping could infer devices within a common rack, though they may provide quite different services within the facility. • BES Cyber System Information o Original Text - Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans. o Proposed Change – Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain Medium or High BES Cyber System Impact Designations; equipment layouts that contain Medium or High BES Cyber System Impact Designations; BES Cyber System recovery plans; and BES Cyber System incident response plans. o Rationale – The rewording clarifies the applicability (within CIP-011) of BES Cyber Information controls. • Defined Physical Boundary – Propose reverting back to (retaining) Physical Security Perimeter. The definition can be modified to remove the 'six-wall perimeter' criteria but from a documentation stand-point, requiring renaming what may be unchanged perimeters/boundaries is an additional resource constraint with no security (or compliance) benefit. The concept of physical security provides an excellent complement to electronic security to demonstrate 'defense in depth.' o Rationale – Retaining 'Physical Security Perimeter' allows existing compliance documentation to be used for instances where PSPs are identified within drawings and equipment layouts. • Inter-Entity Real-Time Coordination and Communication – Propose renaming this to 'Inter-Entity Real-Time Coordination' to avoid overlapping existing communication requirements within the COM standards. o Original Text ♣ Activities, actions, and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. ♣ Aspects of the Inter-Entity Coordination and Communication Operating Service include, but are not limited to: • Schedule interchange • Facility operational data and status • Operational directives o Proposed

Change ♣ Activities, actions, and conditions necessary for the coordination between Responsible Entities to ensure the reliability and operability of the BES. ♣ Aspects of the Inter-Entity Coordination Service include, but are not limited to: • Schedule Interchange • Facility operational data and status • Reliability directives o Rationale – COM-002 is in the process of defining Reliability directives. This term would provide a more concise scope once the COM-002 definition has been finalized. • Add the following definitions (from CAN-0007) o Electronic Access – Access which allows a user to manipulate software and database (setting) attributes of a CCA by direct (primary) or indirect (from outside the ESP) methods. o Physical Access – Access which allows a user to manipulate hardware settings, and may allow the direct connection of a terminal or a computer that can be used to allow electronic access. o Revocation – Action that results in the inability of an individual to access the CCA. • Other terms which would benefit from definitions o Adverse o Annual – Propose use of definition within CAN-0010 o Impact o Security Plan o Associated • Existing definitions that would benefit from alternative wording o Protected Cyber Assets This term loses meaning in the context of Version 5 draft 1 definitions, given the loss of logical network qualification or any other means to assess 'associated.' Only with consideration of the network portion of an address can an entity determine whether a cyber asset qualifies as being within an ESP (where network portions of address are identical). o Electronic Access Point ♣ EAPs typically have two (or more) access points and control access into an ESP (logical network) from a less trusted network or communication interface. The current wording could be applied to any port on a network switch within an ESP and fails to focus on interfaces where traffic does flow from a less trusted network to a more restricted network within an ESP. o Electronic Security Perimeter Suggest retaining the concept of logical network. This provides an easier means to identify "Associated Protected Cyber Assets" as they could be any cyber assets on the same logical network which are not identified as a BES Cyber Asset or BES Cyber System.

Yes

• Control Centers should be capitalized at the end of section 2.13 on page 17. • There should also be a column for LSE in the table provided on page 18. • On page 20, under the category "Balancing Load and Generation," Non-spinning reserve, the use of 'ramp rates' is typically associated with modeling programs not typically used as real time operation information and should be removed. • Managing constraints (page 21) has an extra bullet that should be removed. • Restoration of BES – 'coordination' all by itself lacks context and should include additional words to better frame the intent, or be removed. • Inter-Entity Coordination and Communication – In additional to the recommend removal of 'communication' from the section, this should also include BA within the Operational Directives.

No

1. Applicability – (4.2.1 and 4.2.2) reference to UFLS and UVLS is a point of concern a. Current wording implies that every distribution feeder which is part of a UV or UF load shedding scheme is now in scope, with all distribution level devices now BES Cyber Assets. This may greatly expand the scope greatly into the distribution level. EEI Members propose the following applicability to identify a more targeted scope: i. Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) under a common control system as required by its regional load shedding program. 2. CIP-002-5 R1 – Propose content change a. Original Content – Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning] b. Proposed change - Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. Low Impact BES cyber systems support Bulk Reliability Operating Services but are not mentioned in the bright line criteria as noted in Attachment 1. However, failure of these cyber systems may adversely impact (i.e. not remain in the NERC prescribed category ranges) the voltage and/or frequency of the connected Bulk Electric System. Low Impact BES Cyber Systems do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning] c. Rationale – The original definition, as worded, creates the impression that all other cyber assets qualify as Low Impact, and does not communicate the

criteria within the definition of BES Cyber Asset as a cyber asset that "if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The proposed rewording contributes towards ensuring only assets which have an impact on the BES are the focus of the CIP Standards (and may ensure a more rapid adoption of the Version 5 Standards). 3. The "Rationale – R1" box uses the term "Cyber Systems," which is not a formal term. Suggest changing the case to avoid confusion. 4. The last sentences of R1 and M1 conflict with each other, providing mixed messages specific to Lower Impact BES Cyber Systems/Assets. While Requirement 1 implies there is no need for discrete identification, Measurement 1 discusses evidence for categorizing Low Impact BES Cyber Assets/Systems. 5. Requirement 1.1 a. There is a missing word – "…within 30 calendar days of <when> a change to BES Elements and Facilities is placed into operation. b. The Term "BES Elements and Facilities" used only once within the standards. Suggest changing this phrase to "BES Cyber Assets or Systems." 6. Attachment I - a. High Impact Rating – Propose content change i. Original content – Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at: ii. Proposed change – Each BES Cyber Asset or component of a BES Cyber System located at the facilities listed below that if rendered unavailable, degraded or misused would, within 15 minutes adversely impact the reliable operation of any of the following: iii. Rationale – Some devices may not reside within a Control Center, this rewording provides clarity to focus on assets located within a Control Center in support of BES Reliability Operating Services b. Medium Impact Rating – Propose content change i. Original Content – Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for: ii. Proposed Change - Each BES Cyber Asset or component of a BES Cyber System located at the facilities listed below and not included in Section 1 above, that if rendered unavailable, degraded or misused would, within 15 minutes adversely impact the reliable operation of any of the following: iii. Rationale – The proposed edits more directly connect with the facility and its function within the BES Bright Line criteria. c. 2.2 – Propose content change i. Original content – An aggregate net Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). ii. Proposed change – Each transmission facility containing reactive devices with an aggregate net Reactive Power nameplate rating of 1000 MVAR or greater. iii. Rationale – the rewording provides the filter (for transmission only facilities) at the front to better identify the applicable Facility. d. 2.7 (Table) – The "Weight Value per Line" for 700 should be replaced with a value in the range of 500-600, which is more representative of the typical rating of 230 kV lines. e. 2.8, 2.9, 2.11 – "Major WECC Transfer Paths in the Bulk Electric System" is not actively maintained by WECC and there is no clearly identified basis for why certain paths are included on this list. As an alternative, we suggest "transmission paths contained in the WECC Path Rating Catalog with a maximum path rating equal to or greater than 1,500 MW." This catalog is actively maintained by WECC. f. 2.11 – The table titled "Major WECC Remedial Action Schemes (RAS)" is not actively maintained by WECC. As an alternative, we suggest "Each SPS categorized as a 'Wide Area Protection System' by WECC" which is the newly created mechanism within WECC to identify SPS systems of significant importance.

No

1. General Observation – Since categorization is based on the facilities role within the BES, independent of the specific BES Cyber Asset or BES Cyber System Role, appropriate categorization fails to require assessment based on the criticality of the BES Cyber Asset or Cyber System in support of applicable BES Reliability Operating Services. 2. Rationale R2 – Propose a content change: a. Original Text - The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. b. Proposed Change - The lists required by R1 are reviewed annually to ensure that all BES Cyber Systems have been properly identified and categorized. 3. R2 – Proposed Change a. Original Text – The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. b. Proposed Change – The Responsible Entity shall have its CIP Senior Manager or delegate annually approve the identification and categorization required by R1. c. Rationale – EEI members propose instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is

conducted in an entity standardized time-frame. 4. M2 – Proposed Change a. Original Text – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. (R2) b. Proposed Change – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate annually approve, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems. (R2) c. Rationale – The requirement only asks for Senior Manager (or delegate) approval. EEI members propose instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.
No
For the Last Paragraph VSL's within R1 (failed to update its documentation), EEI proposes the following time periods: Lower – More than 30, but less than or equal to 60 calendar days Moderate – More than 60, but less than or equal to 70 calendar days High – More than 70, but less than or equal to 80 calendar days
No
While it is documented within the definition, as referenced in the Rationale for R1 the Senior Management, the requirement that the senior manager have "overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" would benefit from repetition within the R1 requirement itself. Reading 'solely' this standard post rationale removal does not communicate the responsibility adequately. Propose use of 'legacy' wording and numbering schemes within this standard where possible. In this context the cyber security policy requirements should be R1, with 'leadership' requirements being R2 – EEI proposes this be made R2.
No
EEI proposes that 'legacy' wording and numbering schemes be retained within this standard were possible with the change (within CIP-003-4 R1.1) from "addresses the requirements" to "addresses the topics." This requirements should be R1. Rationale – Pre-version 5 language already captures the requirement and has been successfully vetted within the industry. FERC Order 706 did not identify any specific need to change policy language, only to provide additional guidance. Use of the legacy language would minimize approval barriers by ensuring minimal change where appropriate as long as the 'addresses the requirement' language is removed. Sub-numbering (1.1 through 1.10) should be modified to 2.1 through 2.10.
No
This goes beyond the scope of FERC Order 706. In previous versions, this requirement was a sub-requirement within R1. EEI proposes renumbering/rewording this to capture the legacy context. Propose content Change 1. Original Content – Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 2. Proposed change –The cyber security policies require annual review and approval by the senior manager assigned pursuant to R1. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 3. Rationale – The proposed revision carries forward language from previous versions of the standard (CIP-003 R1.3) which captures the root intent while providing language which has already been vetted and approved within the industry.
No
Propose legacy language/numbering from (pre-version 5) R1 1. Draft 1 content – "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function." 2. Proposed revision – "The cyber security policy is readily available to all personnel who have electronic access or unescorted physical access to, or are responsible for Medium or High Impact BES Cyber Systems." 3. Rationale – EEI members indicated making individuals who have access 'aware of elements' of the cyber security policy does not provide adequate guidance to ensure said individuals comply with the cyber security policy.

No
Requirement 5 – propose use of legacy language: • The responsible entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, standards. Rationale – Overall responsibility and authority (from the legacy language) can accomplish "direct and comprehensive responsibility" and "clear authority" (from FERC Order 706), which provides flexibility without the prescriptive requirement for the senior manager or delegate to be responsible for all individual detailed approvals and authorizations in the standards. Citing "all approvals and authorizations" as a Senior Manager was identified as a concern as it is open ended. There were concerns of the additional administrative burden which is not commensurate with the security benefits. Neither the Blackout Report Recommendation 43 nor FERC Order 706 identify the need to establish this administrative overhead. For Security and Reliability NERC should be concerned with the outcome of the approval process, that is, the proper authorizations are being granted by the Responsible Entity which is contained in the other CIP Standards.
No
Propose use of legacy language from CIP-003-3 R2.2: Changes to the senior manager must be documented within thirty calendar days of the effective date.
No
R4 VSL 1. This language cites a High VSL when 'not all' individuals have been made aware of elements of the cyber security policy. This seems to contradict the intent described in the R4 rationale in which 'it is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.' 2. EEI proposes the use of a more gradual scale rather than a single instance of non-access subject to a High VSL, and total non-access (for all) being a Severe VSL.
Yes
No
1. The rationale for R2 should be reworded from "…contains the proper policies…" to "…covers the required policies…" 2. This extends beyond the guidance of FERC Order 706. Paragraph 435 of the order calls for identifying what "role and steps should be taken by the ERO to ensure quality and consistency of trainers." This requirement should identify what areas of the standards that the training program must include. 3. EEI members question whether this requirement satisfies paragraph 434 of Order 706 where "any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions could, even inadvertently, affect cyber security. 4. R2.2-4 – Can possibly be merged into a single sub requirement a. 2.2 – training on the security controls b. 2.3 – training on the proper use of physical access controls c. 2.4 – training on the electronic access controls 5. R2.6 – Requirement – Proposed word change a. Original - Training on handling of BES Cyber System Information and storage media. b. Proposed Change - Training on handling of BES High and Medium Impact Cyber System Information and storage media. c. Rationale – Rewording supports the applicability section. Since Low Impact Cyber Systems are not applicable, information specific to Low Impact Cyber Systems should not be in scope. 6. Propose merging of R2.7 with R2.9 7. (R2.10) – What changes are required to existing approved training programs to satisfy this new requirement?
No
Measure 3.1 where it calls for the date that access was first granted is a point of concern for both legacy employees (where it may be impossible) as well as new access since existing technology may not adequately capture and retain this information. Requirement 3.2 – Propose content change • Original content – Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months. • Proposed change – Require annual completion of the training specified in CIP-004-5, Requirement R2. • Rationale – The wording adopts the CAN-0010 approach for annual as defined within the registered entity.
No
1. 4.1 a. Version 5 standards should indicate whether previous PRA's would be valid for this requirement (especially within the context of 'initial'). b. EEI proposes a clearer delineation to frame

instances in which personal records are not readily available – vs. impossible to obtain 2. 4.2 – Retention requirements do not extend beyond 3 years, creating confusion regarding retention of 7 year cycle background checks. 3. 4.3 a. Most EEI Members favored a process approach over a fixed pass/fail approach independent of the individual or circumstances involved, and propose that the SDT shift away from a criteria based approach. b. The application guideline provides guidance where it is 'not possible to perform a full seven year criminal history check.' c. 4.4 – Provide language to cover contract employees where I9 verification can only be conducted by employers. Service providers also may have instances where certain individuals may be located in another country, and may access certain BES Cyber Assets remotely.

Yes

No

1. R6.1-3,6.4-6 – Propose use of language where access is appropriate for the roles and responsibilities rather than 'minimum necessary.' a. 'Minimum necessary' as identified as difficult to prove within an audit context. 2. 6.3 – Propose content change a. Original content – The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions. b. Proposed change – Access to BES Cyber System Information repositories must be authorized, except for CIP Exceptional Circumstances. c. Rationale – Senior Manager authorization (or management of delegations) provides additional resource and response impacts, which do not provide enhanced security and may impact reliability efforts when recovery processes are activated. Ensuring access is authorized will satisfy security controls without adding unnecessary overhead. 3. 6.4 – EEI proposes conducting this task on an annual basis as the quarterly requirement will introduce extreme resource constraints in some instances.

No

1. 7.1 - There are questions in instances where resignations and/or terminations may be retroactive, which would introduce a challenge with revocation 'at the time of' events. 2. 7.2 – Transfers or reassignments should frame access changes when no longer needed rather than the date of the transfer (as cited in the Measure (i)). 3. 7.3 – Propose use of 'approved BES Medium and High Impact Cyber System Information repositories,' to frame an appropriate location in which information can be managed and controlled.

Yes

No

The Version 5 approach (as described within the R1 rationale "Summary of Changes") of focusing on discrete Electronic Access points rather than a logical perimeter adds confusion when determining Associated Protected Cyber Assets. A discrete list fails to recognize the inherent controls and permissions within a logical network. Control of routable protocol should consider the inherent network/host identifiers embedded within the addressing scheme in which all devices with an identical network component of their address are peers within a logical network, where access points do not serve as access control. Rationale for R1 – Propose content change • Original Text - The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks. • Proposed Change - The Electronic Security Perimeter serves to control traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic according to a specified rule set, and assists in containing any successful attacks. • Rationale – Monitoring is not identified within any R1 requirements. Table R1 1. R 1.1 1. Applicability - Propose use of "External Connectivity" instead of "External Routable Connectivity" (to include dial-up capability). 2. Propose removal of "and have been implemented" from the end of the measure statement to avoid tracking compliance on a 'per-device' basis, otherwise this would introduce the need for tracking this information for low impact BES Cyber Systems. 2. R 1.2 1. Applicability – 1. Modify to frame applicable Cyber Systems/Cyber Assets as those with External Connectivity. 2. Propose elimination of Associated Physical Access Control Systems as their introduction indicates applicability to subsequent subrequirements which doesn't add to overall security and presents extensive resource requirements. 2. Requirements – Propose content

change 1. Original content – Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs). 2. Proposed change – Control and secure all External Connectivity through the use of identified Electronic Access Points (EAPs). 3. Rationale – The focus within CIP-005 should be on EAP devices with External Connectivity. 3. R 1.3 1. Requirements – proposed change 1. Original Text - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions. 2. Proposed Change - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting access, denying all other access requests by default. 4. R1.4 – There were various interpretations of 'non-Interactive Remote Access,' which implies this requirement may need some additional clarification. This seems to be the only requirement where documentation of authentication measures appears within this standard. Consider removing 1.4 and modifying 1.2 to cover both rows.

No

1. R2.1 1. Requirements – Request rewording to support placement of an intermediary device that may not be part of an ESP. 2. R2.2 1. Requirements – Propose clarification on viable termination points for encrypted traffic to support unencrypted traffic through Electronic Access Points. 2. Rationale – The ability to filter traffic effectively becomes much more difficult if the traffic is encrypted. Supporting technical implementation where encrypted traffic is decrypted prior reaching Electronic Access Points to allow for further access control would benefit security capabilities. 3. Overall – Propose breaking table R2 into a Routable and Dial-Up categories to more effectively frame routable controls and dial-up controls without introducing confusion for the alternate approach.

No

1. Classifying instances where no documentation of compliance exists as severe is appropriate; instances in which a minority of non-compliance controls were identified within a primarily compliant program should be assessed a VSL with respect to the finding (page 17, bottom Severe VSL). 2. VSLs addressing 'each identified EAP' and 'all Interactive Remote Access' should be assessed as a sliding scale to consider whether lower/moderate/high may be more applicable.

No

1. Table R1 a. R1.1 i. Applicability – 'Medium Impact BES Cyber Assets with no External Connectivity' should be added 1. Rationale - Medium Impact BES Cyber Assets should only require fully Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Measures – Proposed Rewrite 1. Original Text – Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented. 2. Proposed Change – Evidence may include, but is not limited to, documented operational or procedure controls that have been implemented. b. R1.2 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Measures – Proposed Change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs. 2. Proposed Change – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how access is controlled. 3. Rationale – FERC Order 706 did not ask for egress access controls. The additional criteria at the end of the measure extend beyond what FERC has asked for, with minimal security benefit. c. R1.3 i. Requirement – Propose

change 1. Original content – Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible. 2. Proposed change – Utilize two or more different physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible. 3. Rationale – 'different and complementary' does not provide adequate guidance. The Measure R1.3 only references 'different. ii. Measure – only mentions 'different' access control methods with no reference to complementary (as included within the requirement). d. R1.4 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Requirement – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 2. Proposed Change – Issue alerts within 15 minutes (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 3. Rationale – The 15 minute criteria (Referenced in the 'Table of Compliance Elements,' page 21, R1 – High) provides greater clarity to satisfy alerting requirements. iii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs, or other evidence that documents that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. e. R1.5 i. Requirements – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 2. Proposed Change – Issue alerts within 15 minutes (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 3. Rationale – The 15 minute criteria (referenced in the 'Table of Compliance Elements,' page 20, R1 – High) provides greater clarity to satisfy alerting requirements. ii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. f. R1.6 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Requirements – Proposed Change 1. Original Text – Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry. 2. Proposed Change – Log (through automated means or by personnel who control entry) of authorized individual's physical entry into each Defined Physical Boundary protecting applicable BES Cyber

Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the authorized individual and date of entry. 3. Rationale – The addition of authorized provides additional segmentation from R2 (Visitor Control) access requirements.
No
Table R2 1. R2.1 a. Applicability – Applicability wording of “Medium Impact BES Cyber Assets should be changed to “Medium Impact BES Cyber Assets with External Connectivity.” i. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. 2. R2.2 a. Applicability – Applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity.” i. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. b. Requirements – Proposed Change i. Original Text – A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor’s name, and individual point of contact. ii. Proposed Change - A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the first entry and last exit, the visitor’s name, and individual point of contact. iii. Rationale – The proposed change capture the intent with (hopefully) clearer language. The 24 hour basis may introduce expectations that ‘round-the-clock’ logging needs to be in place. Some visitations may cross the midnight time-line, which shouldn’t introduce additional requirements.
No
Table R3 1. R3.1 a. Overall observations – EEI members felt that the shift from (pre-V5) maintenance on ‘mechanisms’ to the Draft 1 ‘systems’ expands this requirement beyond the intent. • This should be more focused on testing to ensure alerting and control mechanisms work as intended. • Use of controls should be considered ‘tested’ in situations where applicable devices are used every day (i.e. card readers). b. This sub requirement cites tasks to be conducted ‘prior to commissioning.’ Since many controls are expected to be in place prior to V5 adoption, there should be language within the implementation plan to capture devices in use at the time the standard becomes effective. 2. Compliance a. 1.5.2 – Evidence retention should keep the existing 90 day period for physical access logs as extending this to 3 years can create extensive commitment in storage media, particularly for video monitoring.
No
The Table of Compliance Elements cites references to sub requirements that appear to be incorrect: • Lower – Part 1.7 should point to 1.6 • High – Part 1.6 should point to 1.5
No
R1.1 – Requirements – Proposed Content Change 1. Original Content – Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. 2. Proposed Change – Enable only logical accessible ports needed, including port ranges where required. 3. Rationale – The proposed language incorporates much of the legacy (CIP-007-3 R2.1) language. The additional requirement to document the need for remaining logical ports extends beyond what FERC Order 706 requests without adding security benefits. R1.2 1. Requirements – Content Change a. Original Content - Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. b. Proposed Change – Protect against the use of unnecessary physical input/output ports that could be used for network connectivity, console commands, or removable media by disabling, restricting, or

use of signage. 2. Measures – Content Change a. Original Content - Evidence may include, but is not limited to, documentation stating specific or types of physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. b. Proposed Change - Evidence may include, but is not limited to, documentation stating specific physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage.

No

2.1 1. Requirements – Content Change a. Original Content - Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. b. Proposed Change – Identify a source or sources that are monitored for the release of security related patches, or security updates for software and firmware associated with BES Cyber System or BES Cyber Assets. 2. Measures – Propose striking the last sentence "The list could be sorted by BES Cyber System or source." It introduces additional requirements with no clear security benefit or alignment with FERC Order 706. 3. 2.2 and 2.3 should be switched, as 2.3 requires the establishment of a process for remediation, and 2.2 addresses the creation or revision of the remediation plan. 4. 2.2 a. Requirement – Propose content change i. Original content - Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe. ii. Proposed change – Identify applicable security-related patches or updates within 30 days of release from the identified source that addresses the vulnerabilities, and create or revise a remediation plan that addresses the vulnerabilities within a defined timeframe. iii. Rationale – The rewording captures the chronological order of the elements within this requirement to provide clearer guidance. 5. 2.3 a. Requirement – As currently worded, there is no allowance for changes in the remediation plan should outage coordination, or other resource constraints require modifications to the remediation plan. This is a point of concern that should be addressed.

No

1. 3.2 a. Requirement – Content Change i. Original content – Disarm or remove identified malicious code. ii. Proposed change – Mitigate the threat of identified malicious code. iii. Rationale – In some instances, the presence of malicious code may present a lesser risk to the reliability of the BES than disarming/removal processes, especially when the malicious code may not exploit a feature used within the Cyber System. b. Measure – Add a bullet to allow for evidence of manual removal. 2. 3.3 a. Requirement – Propose content change i. Original content – Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). ii. Proposed change – Update malicious code protections from the identified source within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). iii. Rationale – The addition of 'the identified source' provides a context for determination of availability. b. Include testing within both the requirements and measures as alluded to within the Application Guidelines (page 41). c. Measures – Format (i) and (ii) to a bulleted list signifying 'or' criteria 3. 3.4 a. Applicability – Propose deletion of Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems as they do not appear to be Transient Cyber Asset related. b. Requirements – Content Change i. Original Content - Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change – Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to Medium or High Impact BES Cyber Assets or Protected Cyber Assets. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. ii. Proposed Change – Evidence may include, but is not limited to, an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. iii. Rationale – Excised content introduced prescriptive criteria that introduced additional resources without clearly addressing the requirement. 4. 3.5 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems and Associated and they do not appear to be Transient Cyber Asset related. b. Requirements – Append "to Medium or High Impact BES Cyber Assets or Associated

Protected Cyber Assets" to the end of the requirement. c. Measures – Content Change i. Original Text – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change - Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to Medium or High Impact BES Cyber Assets or Protected Cyber Assets.
No
R4 1. 4.1 a. Requirements – Content Change i. Original Content - Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. ii. Proposed Change – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. Devices that cannot log a particular event do not require a TFE to be generated. iii. Rationale – Content from the application guidelines has been introduced to promote the guidance that TFE's are not required in instances in which devices cannot log a particular event. 2. 4.2 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control Systems as they are out of scope for this requirement. b. Requirements – Content Change i. Original Content – Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert. ii. Proposed Change – Generate alerts for events that the Responsible Entity determines necessary. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate real-time alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert; Screenshots showing how real-time alerts are configured. ii. Proposed Change – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate an alert; Screenshots showing how alerts are configured. iii. Rationale – Removed the usage of 'real-time' as it presents concerns demonstrating compliance. 3. 4.3 a. Requirements – Content Change i. Original Text – Detect and activate a response to event logging failures before the end of the next calendar day. ii. Proposed Change – Activate a response to failures of event logging before the end of the next calendar day after identification. iii. Rationale – Some devices generate logs so infrequently that identification of logging failure may extend beyond any calendar day. The spirit of this requirement remains intact as one day remediation is required once the log failure is identified. 4. 4.4 a. Requirements – Content Change i. Measures – Content Change 1. Original Text – Evidence may include, but is not limited to, security-related event logs from the past ninety days and records of disposition of security related event logs beyond ninety days up to the evidence retention period. 2. Proposed Change – Evidence must include, but is not limited to, security-related event logs from the past ninety days. 5. 4.5 a. Requirements – Content Change i. Original Content – Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day. ii. Proposed Change - Review a summarization or sampling of logged events every two weeks to identify BES Cyber Security Incidents and potential event logging failures. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008. b. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred, and dated evidence showing that personnel were dispatched or a work ticket was opened to rectify the deficiency. ii. Proposed Change – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), and signed and dated documentation showing the review occurred. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008.

No
a. Overall – EEI and its members struggled with providing alternate wording for this subrequirement. In both the original content and proposed change there exists a instances where access is a component of validation and/or authentication. This presents a potential compliance challenge that should be addressed. b. Requirements – Content Change i. Original Content – Validate credentials before granting electronic access to each BES Cyber System. ii. Proposed Change – Authenticate user account access before granting electronic to each Medium or High Impact BES Cyber System or Associated Protected Cyber Asset, where technically feasible. iii. Validating credentials was seen as vague specific to technical compliance so authentication is offered as an alternate approach to satisfy the root requirement (and mirrors the language in the change rationale). The addition of 'where technically feasible' was to recognize technical capabilities currently in place may not adequately demonstrate compliance with this. 2. 5.2 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 3. 5.3 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 4. 5.4 a. Requirements – Content Change i. Original Text – Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. ii. Proposed Change – Procedural controls for initially removing, disabling, or changing default passwords, where technically feasible. For the purposes of this requirement an inventory of Cyber Assets is not required. iii. Rationale – The additional wording identifies the multiple methods which can be used to mitigate default passwords. 5. 5.5 a. Requirements i. Change Systems to Assets throughout as password limitations should be identified to the device level. ii. Add language to 5.5.3 to cover instance where accounts may not be able to support password change to permit the entity specified time frame to be equal to the life-time of the BES Cyber Asset where technically required.
No
1. R3 a. Propose switching High and Severe Columns as the High captures instance in which no methods were deployed, Severe captures instances in which incomplete methods were deployed. b. The initial paragraph in Severe is duplicated in High. 2. R4 a. Moderate – delete 'identify and implement methods to' b. High – delete 'identify and' 3. R5 a. High – The initial paragraph doesn't align with a requirement, propose striking.
No
1. Rationale R1 1. The initial sentence is fragmented, providing an incomplete framing for R1. Absent a complete sentence, proposing alternate language to better frame this rationale is difficult. Propose rewriting this sentence. 2. Regarding applicability to all registered entities – While EEI Members understand the need for all entities to have an effective process to respond to incidents within each organization, for the purposes of CIP-008 it would be best to establish applicability to entities with Medium and High Impact BES Cyber Assets/Systems, as those are the impact ratings in which Defined Physical Boundaries and Electronic Security Perimeters are required. 3. R1.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 4. R1.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 5. R1.3 1. Requirements ♣ The initial 'define' should be expanded to provide a complete sentence (i.e. An entities BES Cyber Security Incident Response Plan should include). 2. Measures – Content Change ♣ Original • Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of BES Cyber Security Incident response personnel, BES Cyber Security Incident handling processes or procedures, and communications processes or procedures. ♣ Proposed Change • Evidence may include, but is not

limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of; o BES Cyber Security Incident response personnel, o BES Cyber Security Incident handling processes or procedures, o Communications processes or procedures.
No
R2 1. 2.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 2. Requirements – Content Change ♣ Original Content • When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test. ♣ Proposed Change • When a BES Cyber Security Incident occurs, the incident response plans must be used and include recording of deviations taken from the plan during the incident. 2. 2.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist.. 2. Requirements – Content Change ♣ Original Content • Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): o by responding to an actual incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Proposed Change • Test the incident response plan(s) annually. A test of the plan may include: o A response to an incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Rationale – References to requirements needed upon the effective date should be captured within the implementation plan, allowing the standard to identify requirements (only) in place once the standard is approved. 3. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence showing annual testing of the BES Cyber Security Incident response plan(s). Types of exercises may include discussion or operations based exercises. Document lessons learned within 30 days of incident or exercise. Use lessons learned to update incident response plan(s). ♣ Rationale – The Homeland Security Exercise and Evaluation Program identifies seven types of exercises within HSEEP, each of which is discussions-based or operations-based. 3. R2.3 – Propose deletion as this sub requirement merely identifies retention requirements already documented within Compliance (C.1.2).
No
1. R3 1. 3.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – The formal definition of BES Cyber Security Incident includes attempts to compromise the ESP or DPB, requiring Medium or High Impact BES Cyber Systems/Assets. 2. 3.2 1. Requirements – Propose content change a. Original content – Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan. b. Proposed change – Use lessons learned from incident responses or incident response exercises to update the incident response plan, within sixty days of documenting lessons. c. Rationale – It takes 30 days from the time an exercise is executed to the review and completion of an after action report. The thirty day clock should start once the after action report is completed. This is in line with the proposed 60 day timeline in R3.3. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan. ♣

Proposed Change – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or incident response within thirty calendar days of the lessons learned associated with the response plan. 3. 3.3 1. Requirements – Content Change ♣ Original Content • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan. ♣ Proposed Change • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that test or incident. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan. ♣ Proposed Change – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan test or incidence response and the dated, revised plan.
No
1. R1 – Severe 1. 2nd paragraph, add 'types' to the end of the paragraph (…plan does not identify Reportable BES Cyber Security Incident types). 2. R2 – Severe 1. The second paragraph should be modified from "The Responsible Entity has not tested the execution of its BES Cyber Security Incident Response Plan" to "The Responsible Entity has not executed its BES Cyber Security Incident Response Plan" 2. Rationale – This paragraph aligns with R2.2 which requires activation or exercising the plan. The revised words better support requirement R2.2. 3. R3 1. High VSL (first paragraph) – Content change ♣ Original content • The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 30 calendar days of execution. ♣ Proposed Change • The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 60 calendar days of completion. ♣ Rationale – This VSL combines the review (3.2) with the update (3.3) requirement, the 60 days support the 3.3 requirement.
No
• Overall 1. Propose renaming this Standard to "Recovery Plans for BES Cyber Systems" 2. The revised structure of CIP-009-5 documents requirements for backup media in both R1 and R2. Creating a requirement in which backup media requirements are consolidated (in-line with version 3) would provide a more concise means to identify media requirements. The requirements (as proposed) would be as follows: 1. R1 – Recovery Plan 2. R2 – Exercise of the Recovery Plan 3. R3 – Backup Media 4. R4 – Maintaining the Recovery Plan 3. References to 'implement' should be changed to 'exercise' regarding recovery plans to better capture activation of the plan vs. 'release and publish' efforts. 4. Actions required in advance of the implementation date (2.1, 2.2) should be removed from the standard(s) and included within the implementation plan. • Introduction 1. Purpose – Proposed Content Change 1. Original Content – Standard CIP-009-5 ensures that recovery plan(s) related to the storing of backup information are put in place for BES Cyber Assets and BES Cyber Systems and that these plans support and follow established business continuity and disaster recovery techniques and practices. 2. Proposed Change – Standard CIP-009-5 ensures that recovery plan(s) are put in place for BES Cyber Assets and BES Cyber Systems. 2. Applicability 3. Background • Requirements and Measures 1. R1 1. 1.1 – Propose alternate language (carried forward from previous versions) 1. Create and implement a recovery plan that at a minimum includes: ♣ Conditions for activation of the recovery plan ♣ Roles and responsibilities of the responders 2. 1.2 – Propose deletion as this sub requirement has migrated to R1.1 proposed R1.1 rewrite. 3. 1.3 1. Requirement – Content Change ♣ Original – One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality ♣ Proposed Change – One or more processes for the backup, storage, and restoration of information required to restore BES Cyber System functionality ♣ Suggest additional content supporting mirroring and/or redundancy within the backup/recovery methods such as: • Mirroring and/or redundancy can be considered as complementary measure in support of this requirement, but a process must be in place to ensure retrieval of previous versions should current version(s) require reverting to a previous instance. ♣ Rationale – Protection of BES Cyber System Information is addressed within CIP-011. 2. Measure – Content Change ♣ Original – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and protection of information required to successfully restore a BES Cyber System. ♣ Proposed Change – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and restoration of information required to successfully restore a BES Cyber System. ♣ Rationale – Protection of BES Cyber System Information is addressed within CIP-011. 4. 1.4 – Correct

headers from ‘part’ to ‘Applicability,’ ‘Requirements,’ and ‘Measures’ 1. 1.4 ♣ The current form does not adequately address FERC Order 706, paragraphs 739 and 748, and in fact contradicts the intent that ‘The Commission does not believe that every change will necessitate verification of the backup and restoration processes’ from paragraph 740. ♣ Propose ‘new’ sub requirement applicable to High Impact BES Cyber Systems to require: • Upon implementation of significant changes to High Impact BES Cyber Systems, verify that backups are operational before they are relied upon for recovery purposes. ♣ Propose rewrite • Original – Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully. • Proposed Change – Ensure that backup processes are completed successfully for Information essential to BES Cyber System recovery. • Rationale – This focuses on successful completion of the backup process which can be done within the routine backup. Verification would be moved to its own requirement applicable to High Impact BES Cyber Systems and limited to significant change instances. 5. 1.5 1. Requirement – Content Change ♣ Original Content – Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. ♣ Proposed Change – Document root cause for events that trigger activation of the recovery plan(s) as required in Requirement R1. ♣ Rationale – Root cause documentation should be the focus for this requirement. The current draft language requires potential impediments to restoration efforts and is too vague.
No
1. 2.1 1. Requirements – Content Change ♣ Original – Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: by recovering from an actual incident, or with a paper drill or tabletop exercise, or with a full operational exercise ♣ Proposed Change – Implement the recovery plan(s) referenced in R1 annually: • by recovering from an actual incident, or • with a tabletop exercise, or • with a functional exercise ♣ Rationale – Use of the functional exercise aligns with the R2 rationale content citing NIST SP 800-84 exercise types. Requirements in advance of the effective date of the standard should be addressed within the implementation plan. 2. Measures – Content Change ♣ Original – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with a full operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a tabletop exercise, or with a functional exercise) of the recovery plan annually. For the table top or functional exercise, evidence may include meeting notices, minutes, or other records of exercise findings. 2. 2.2 1. Requirements – Content Change ♣ Original Text – Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations. ♣ Proposed Change – Test information used in the recovery of BES Cyber systems that is stored on backup media annually, to ensure that the information is useable. 3. 2.3 1. Overall ♣ This requirement (to be done every 39 calendar months) appears to overlap considerably with 2.1 (to be done every year). ♣ Every 39 calendar months exceeds the 3 year retention identified within the Compliance section. ♣ How does this differ from current EOP-008 requirements? 2. Requirements – Content Change ♣ Original – Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise. ♣ Proposed Change – Exercise the recovery plan(s) at least every 39 calendar months through an operational exercise in a representative environment. An actual recovery response may substitute for an operational exercise. ♣ Rationale – Actions required to take place prior to the effective date of the standard should be captured within the implementation plan.
No
1. 3.1 1. Requirements – Content Change ♣ Original – Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned. ♣ Proposed Change – Review the recovery plan(s) annually and

document any identified deficiencies. ♣ Rationale – Requirements addressing tasks to be done prior to the effective date should be captured within the implementation plan. 2. 3.2 1. Requirements – Content Change ♣ Original – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned. ♣ Proposed Change – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of completion, documenting any identified deficiencies or lessons learned. 3. 3.3 4. 3.4 – Propose deletion as the requirement is too broad with no clear alignment with FERC Order 706 or security benefit. 5. 3.5 2. Requirements – Content Change ♣ Original – Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed. ♣ Proposed Change – Updates to the recovery plan(s) shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of being completed. ♣ Rationale – The proposed change leverages 'pre-version 5' language which satisfies the intent of the requirement.

Yes

No

1. R1 1. Rationale – The current wording doesn't capture the intent of FERC Order 706, paragraph 399: 1. We do not seek absolute assurances but rather are concerned that there be processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. 2. Suggest referencing this directive within the rationale, and ensure configuration management focus more on the spirit of the FERC Order rather than the currently framed "prevent unauthorized modifications to BES Cyber Systems." 2. R1.1 a. CIP-010-1 R1.1 should be replaced with CIP-003-4 R6 i. Rationale – CIP-010-1 R1.1 is too prescriptive. CIP-003-4 R6 is closer to a results based requirement and provides more flexibility to achieve the desired results. CIP-010-1 R1.1 greatly expands the scope of change control and configuration management (CIP-003-4 R6) beyond what was directed in FERC Order 706. FERC Order 706 paragraphs 397 and 398 directed "modifications to CIP-003-1 R6 to provide an express acknowledgement of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." The concern was that some form of verification is performed to detect when authorized changes have been made. CIP-010-1 R2.1 addresses Order 706's concern for some form of verification to detect unauthorized changes. (CIP-010-1 R2.1 should delete reference to the baseline defined in CIP-010-1 R1.1.) FERC also did "not believe the changes will have burdensome consequences." CIP-010-1 R1.1 requires extensive and burdensome details tracking. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1. 1. 1.1.4 – Propose content change ♣ Original Text – Any custom software and scripts developed for the entity; ♣ Proposed Change – Any custom software and scripts installed on the BES Cyber Asset that can affect the security posture. ♣ Rationale – The change focuses scope to eliminate software and scripts not in use. 2. 1.1.5 – Propose content change ♣ Original Text – Any logical network accessible ports; and ♣ Proposed Change – Any network accessible ports or services; and ♣ Rationale – This clarifies the requirement to focus on 'active ports and services' rather than Ethernet jacks. 3. R1.2 1. Requirement – Propose content change ♣ Original Text – Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Proposed Change – Document approved changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Rationale – As documented earlier in this comment form, requiring Senior Manager (or delegate) authorization introduces resource constraints that impede the effective documentation of changes without adding security benefits or alignment with FERC Order 706. 2. Measure ♣ First paragraph – Add 'or,' at the end of the first bulleted paragraph. ♣ Second paragraph – Propose content change • Original Text – A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) were an individual with the authority to authorize the change was in attendance. • Proposed Change – A record of the change with authorization of the change. • Rationale – Citing a "change advisory board" within the measure overly represents adequate evidence in support of the requirement. 4. R1.3 1. Requirements – Propose content change ♣ Original Text – Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar

days of completing the change. ♣ Proposed Change – Update the documented baseline configuration as necessary within 30 calendar days of completing the change. ♣ Rationale – The proposed rewording provides more focus on the root requirements. 5. R1.5 1. Requirements – Propose content change ♣ Original Text • 1.5.1 – Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any difference in operation between the test and production environments. ♣ Proposed Change • 1.5.1 – Prior to implementing any change from the existing baseline configuration in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment. ♣ Rationale – Proposed rewording provide greater focus on the root requirements. 2. Measures – Propose content change ♣ Original Text – Evidence includes, but is not limited to, a list of security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test. ♣ Proposed Change – Evidence includes, but is not limited to, a list of security controls tested along with the date of the test, test results, and a list of differences between the production and test environments.

No

1. R1 1. Rationale – The current wording doesn't capture the intent of FERC Order 706, paragraph 399: 1. We do not seek absolute assurances but rather are concerned that there be processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. 2. Suggest referencing this directive within the rationale, and ensure configuration management focus more on the spirit of the FERC Order rather than the currently framed "prevent unauthorized modifications to BES Cyber Systems." 2. R1.1 a. CIP-010-1 R1.1 should be replaced with CIP-003-4 R6 i. Rationale – CIP-010-1 R1.1 is too prescriptive. CIP-003-4 R6 is closer to a results based requirement and provides more flexibility to achieve the desired results. CIP-010-1 R1.1 greatly expands the scope of change control and configuration management (CIP-003-4 R6) beyond what was directed in FERC Order 706. FERC Order 706 paragraphs 397 and 398 directed "modifications to CIP-003-1 R6 to provide an express acknowledgement of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." The concern was that some form of verification is performed to detect when authorized changes have been made. CIP-010-1 R2.1 addresses Order 706's concern for some form of verification to detect unauthorized changes. (CIP-010-1 R2.1 should delete reference to the baseline defined in CIP-010-1 R1.1.) FERC also did "not believe the changes will have burdensome consequences." CIP-010-1 R1.1 requires extensive and burdensome details tracking. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1. 1. 1.1.4 – Propose content change ♣ Original Text – Any custom software and scripts developed for the entity; ♣ Proposed Change – Any custom software and scripts installed on the BES Cyber Asset that can affect the security posture. ♣ Rationale – The change focuses scope to eliminate software and scripts not in use. 2. 1.1.5 – Propose content change ♣ Original Text – Any logical network accessible ports; and ♣ Proposed Change – Any network accessible ports or services; and ♣ Rationale – This clarifies the requirement to focus on 'active ports and services' rather than Ethernet jacks. 3. R1.2 1. Requirement – Propose content change ♣ Original Text – Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Proposed Change – Document approved changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Rationale – As documented earlier in this comment form, requiring Senior Manager (or delegate) authorization introduces resource constraints that impede the effective documentation of changes without adding security benefits or alignment with FERC Order 706. 2. Measure ♣ First paragraph – Add 'or,' at the end of the first bulleted paragraph. ♣ Second paragraph – Propose content change • Original Text – A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) were an individual with the authority to authorize the change was in attendance. • Proposed Change – A record of the change with authorization of the change. • Rationale

– Citing a “change advisory board” within the measure overly represents adequate evidence in support of the requirement. 4. R1.3 1. Requirements – Propose content change ♣ Original Text – Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change. ♣ Proposed Change – Update the documented baseline configuration as necessary within 30 calendar days of completing the change. ♣ Rationale – The proposed rewording provides more focus on the root requirements. 5. R1.5 1. Requirements – Propose content change ♣ Original Text • 1.5.1 – Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any difference in operation between the test and production environments. ♣ Proposed Change • 1.5.1 – Prior to implementing any change from the existing baseline configuration in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment. ♣ Rationale – Proposed rewording provide greater focus on the root requirements. 2. Measures – Propose content change ♣ Original Text – Evidence includes, but is not limited to, a list of security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test. ♣ Proposed Change – Evidence includes, but is not limited to, a list of security controls tested along with the date of the test, test results, and a list of differences between the production and test environments.

No

1. 3.1 1. Requirements – Proposed content change ♣ Original Text – Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed. ♣ Proposed Change – On an annual basis, conduct a paper assessment of the cyber security controls to determine the extent to which the controls are implemented correctly and operating as designed. • Propose the addition (3.1.1) of minimum cyber security controls to be assessed that; o Are referenced within these standards; and o Are not already required to be assessed in other standards (removing double jeopardy implications) ♣ Rationale • Annual (as defined within CIP-0010) should be the consistent approach to allow entities to standardize annual requirements on a consistent basis. • Active assessment is cited within Part 3.2 (to be done every 39 months) so we’ve removed it from this part to avoid overlap. 2. Measures – Propose content change ♣ Overall – There needs to be clear segmentation from ♣ Original Text – Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the output of the tools used to perform the assessment. ♣ Proposed Change – Evidence may include, but is not limited to: • A document listing the date of the assessment, the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the assessment results. ♣ Rationale – Annual should align with CAN-0010 definition. Documentation of assessment results focus on the root information in support of vulnerability rather than potentially extensive data (from tools) that may require extensive resources to retain. 2. 3.2 1. General observations ♣ While the application guidelines recognize production devices which may not be capable of modeling within a test environment (ICCP, etc.), this requirement does not provide clear guidance to follow where these instances occur. ♣ The 39 month cycle exceeds the 3 year retention requirements. 2. Requirements – Propose content change ♣ Original Text – Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production

environments. ♣ Proposed Change – At least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production. 3. Measures – Propose content change ♣ Original Text – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment. ♣ Proposed Change – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments. 3. 3.3 4. 3.4 1. Requirements – Propose content change ♣ Original Text – Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Proposed Change – Document the results of the assessments (conducted within 3.1-3.3) and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Rationale – referencing parts 3.1 – 3.3 provides alignment with the previous parts of the standards.

Yes

No

1. 1.1 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed content change ♣ Original Text – One or more methods to identify BES Cyber System Information. ♣ Proposed Change – Implement one or more methods to identify BES Cyber System Information. ♣ Rationale – Additional wording frames this in a more complete manner. 2. 1.2 1. Overall – Correct column header labels within the table. 2. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 3. Requirements – Propose content change ♣ Original Text – Access control and handling procedures for BES Cyber System Information. ♣ Proposed Change – Demonstration of access control for BES Cyber System Information. ♣ Rationale – Additional wording frames this in a more complete manner. 3. 1.3 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems •

Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed content change ♣ Original Text - Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. ♣ Proposed Change – Annually assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. 3. Measures – Proposed content change ♣ Original Text – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence to demonstrate that the action plan was implemented. ♣ Proposed Change – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence of the status of the action. ♣ Rationale – Rewording allows for action plans which may be 'in progress' towards implementation, capturing instance in which remediation may rely on deliverables (not yet received) by vendors.

No

1. 2.1 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed Change ♣ Original Content – Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media. ♣ Proposed Change – Prevent the unauthorized retrieval of BES Cyber System Information from BES Cyber Asset media prior to the release of BES Cyber Asset media for reuse. ♣ Rationale – While not directly changing the intent of the requirement, this rewording has been suggested to provide greater clarity of the root requirement. 2. 2.2 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts.

No

R1 (Severe) – Propose removal of the first paragraph as it is mirrored within the subsequent paragraphs that better frame the violation.

No

The existing time frame of 18 months is too short, given the extensive enhancements within the standards as a whole, and particularly specific to the likely addition of numerous Low Impact BES Cyber Systems that may not have been considered in scope for previous versions. In the event that Low Impact assets are a component of the enforceable requirements on day 1, there is little doubt the implementation time would extend considerable beyond 18 months. References to requirements to be conducted in advance of the implementation date should be migrated over into the implementation plan. This ensures any pre-requisites are captured within the implementation plan, freeing this content from the standards to provide clearer guidance. This occurs in the following

sections: 1. CIP-002 a. R2 b. M2 2. CIP-003 a. R3 3. CIP-008 a. R2.2 b. M2.2 c. R3.1 4. CIP-009 a. R2.1 b. R2.3 c. M2.3 d. R3.1 e. M3.1 f. VSL (High-R2) g. VSL (Severe-R2) h. VSL (Severe-R3) 5. CIP-010 a. R3.1 b. R3.2 6. CIP-011 a. R1.3 b. VSL (High-R1)
Individual
Andrew Z. Pusztai
American Transmission company, LLC
Yes
American Transmission Company (ATC) endorses EEI's comments on the proposed Definitions.
Yes
American Transmission Company (ATC) endorses EEI's comments on CIP-002-5 Standards. In addition, ATC is submitting comments for CIP-002-5 Attachment 1. Criterion 2.8 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLs and their associated contingencies' with wording of, '. . . as Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more IROL violations', like the wording using in Criterion 2.11. Criterion 2.9 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLS and their associated contingencies' with wording of, '. . . as FACTS that if destroyed, degraded, misused, or otherwise rendered unavailable, could cause the violation of one or more IROLs', like the wording using in Criterion 2.11. Criterion 2.12 – (1) Replaced the word, 'system' with 'common control system' to clarify that this criterion applies to a system triggered by a single (common) control, rather than a program (system) of many independent relays set to trip at the same frequency.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-002-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-002-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments regarding the VRFs and VSLs.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R4 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R5 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R6 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on VRFs and VSLs of CIP-003-5 Standard.
Yes
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-004-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-004-5 Standard.
No

American Transmission Company (ATC) endorses EEI's comments on R4 of CIP-004-5 Standard.
Yes
No
American Transmission Company (ATC) endorses EEI's comments on R6 of CIP-004-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R7 of CIP-004-5 Standard.
Yes
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-005-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-005-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on VRFs and VSLs of CIP-005-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-006-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-006-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-006-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on VRFs and VSLs of CIP-006-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R4 of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R5 of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on VRFs and VSLs of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-008-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-008-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-008-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on VRFs and VSLs of CIP-008-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-009-5 Standard.

No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-009-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-009-5 Standard.
Yes
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-010-1 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-010-1 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-010-1 Standard.
Yes
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-011-1 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-011-1 Standard.
No
American Transmission Company (ATC) endorses EEI's comments VRFs and VSLs of CIP-011-1 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on the proposed Implementation Plan for the CIP Standards.
Individual
David S. Revill
Georgia Transmission Corporation
Yes
In the definition of BES Cyber System, it should refer to "Transient Cyber Asset" instead of "Maintenance Cyber Asset." GTC also recommends that the definition include the phrase "at the discretion of the Responsible Entity" as follows: One or more BES Cyber Assets that are typically grouped together at the discretion of the Responsible Entity, logically or physically, to operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. In the definition of BES Reliability Operating Services, GTC is concerned that this definition is overly complex and would be better served in a guidance document. GTC recommends the definition consist of the first sentence and move the remaining information to guidance as follows: BES Reliability Operating Services: BES Reliability Operating Services are those services contributing to the real-time reliable operation of the Bulk Electric System (BES). GTC is concerned that the definition of BES Cyber System Information is too broad and overreaching. GTC recommends that the drafting team research other information frameworks such as PII. Specifically, GTC recommends that the definition look at information in aggregate (such as multiple elements of a security configuration) rather than information minutia (such as a single IP address). GTC recommends that the drafting team consider revising the definition for Control Center. GTC is concerned that a single RTU that also operates a remote line switch does in fact "support real-time operations by a System Operator for two or more…transmission facilities, at two or more locations." In the definition of Defined Physical Boundary, the term "Electronic Access Control Systems" should be "Electronic Access Control or Monitoring Systems." In the definition of Electronic Access Point, GTC recommends the definition be as follows: "An interface on a Cyber Asset that controls routable or dial-up data communications between Cyber Assets" In the definition of Physical Access Control Systems, GTC disagrees with the need to change the definition as it existed in version 3. GTC recommends that the previous wording be used as follows: "Cyber Assets that authorize or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers." GTC also believes cameras should

be added to the list of excluded devices and those devices should be excluded if they are at or outside of the Defined Physical Boundary, not just AT the boundary. The definition of Electronic Access Control or Monitoring Systems is substantially the same as under CIP version 3. It has been interpreted by at least some regions to include the systems of Managed Security vendors, even if they only perform monitoring and alerting functions (no access control) and if they are a backup to the entity's own systems. This discourages entities from utilizing these services because it is extremely difficult to monitor and enforce a third party's compliance with the standards. The end result is a reduced use of these services which increases risk and reduces reliability. Consider specifically excluding vendor systems as long as they do not perform access control or at least if they both do not perform access control and are a backup to and entity's primary logging and alerting system. As written, the definition of External Connectivity would include communication between two of an entity's BES Cyber Assets if they are within different ESPs. This should not be included in the definition. The definition of Interactive Remote Access does not address how the word "Interactive" should be interpreted. This is an important element of the term because there is dispute about whether or not read-only access should be included in the definition. The definition should specifically include or exclude read-only access so that the industry has the opportunity to weigh in on the issue. In the definition of "Intermediate Device" the words "may" and "may be" should be changed to "is". Otherwise a device might be included if it is capable of providing those services even if it is not intended to do so and is not configured to do so. The sentence "Intermediate devices are sometimes called proxy systems is inappropriate". Certainly a proxy system could serve as an Intermediate device, but not all proxy systems would qualify. Conversely there are other devices (such as VPN termination devices) that are not generally thought of as proxy systems that could serve as an Intermediate device. Accordingly the sentence adds confusion instead of clarity to the definition. In the definition of Transient Cyber Asset item 2 should be expanded by adding Vulnerability Assessment. Devices used for a VA are perfect examples of the type of systems that should be included in this definition but do not clearly fall under any of the other categories.

Yes

We disagree with the need to modify the criteria from those already approved by industry in version 4 of CIP-002. We recommend the drafting team revert the criteria to those previously approved. Additionally, we are concerned that some of these criteria may in fact extend beyond the definition of BES that is in the process of being developed. This would create a situation where a NERC defined “BES Cyber Asset” may in fact not be part of the BES. GTC disagrees with the inclusion of “Transmission Owner” in criteria 1.3 and 2.13. The functional model indicates that the Transmission Owner has no real time obligations. As such, a control center used to perform the functional obligations of the Transmission Owner cannot, by definition, have a real-time impact on the reliable operation of the BES. Additionally, none of the functional obligations of the Transmission Owner, as described in the NERC Reliability Functional Model, could be performed by a control center. We do agree, however, that a Transmission Owner may, in fact, have a control center that is performing obligations of a Transmission Operator without being registered as such. We believe this case should be clarified in a footnote to the criteria and Transmission Owner be stricken. GTC is concerned that thresholds are being used inconsistently in Attachment I. Specifically, generation is only included as a Medium Impact if it is above 1500MW. However, generation control centers are included at a much lower threshold: 300MW. 300MW is used in regards to UFLS and UVLS schemes. However, we believe the importance of these schemes to the BES to be fundamentally different than simply the loss of a specific amount of load or generation. As such, we suggest the drafting team modify criteria 2.13 to only include generation control centers greater than 1500MW as a medium impact. Also, in section 1.2 of the Compliance Section, the word compliant is spelled incorrectly.

Yes

No

GTC is concerned with the manner in which the drafting team has chosen to handle the bookending of requirements throughout the standard. The phrase “initially upon the effective date” may lead to confusion in the industry as to exactly what is expected. Dictionary.com defines “upon” as “immediately or very soon after.” This could lead one to believe that everywhere this phrase is used, the approval must be made precisely on the effective date and that an approval obtained prior to the effective date would be considered non-compliant.

Yes
No
GTC is concerned that this requirement requires the implementation by policy of security controls for Low Impact BES Cyber Assets that are not required elsewhere in CIP-004 though CIP-011 (e.g. Configuration Change Management and Information Protection).
No
See response to question #4.
No
GTC believes that this requirement should be removed from CIP-003 and included as an element of the required training program in CIP-004. This would have the effect of eliminating a previously approved requirement, but GTC believes this is justified as the objective of the requirement is being met through including it in the required training program.
Yes
Yes
GTC is not sure that there is a strong reliability objective to this requirement as it stands and suggests that this language be combined with R1 and R5, eliminating R6.
Yes
No
The requirement should clarify that some roles may not include all requirement parts in their training program.
GTC notes that the guidance material appears to be out of sync with the requirement.
No
GTC disagrees with requirement parts 7.4 and 7.5 as they relate to Medium Impact BES Cyber Systems. The vast majority of Medium Impact BES Cyber Systems are field IEDs such as RTUs and Relays. The passwords on these devices are typically designed with safety of operations in mind and not security. As such, revocation of physical and remote access provides the only reliability benefit in the majority of cases and the revoking of individual credentials or shared account passwords provides no reliability benefit and may in fact harm reliability. Many of these devices require that the entire configuration be redeployed on the device (which typically requires a device restart) in order to modify the password. This has the unfortunate side effect of temporarily impacting situational awareness and increases risk to the BES. As such, GTC suggests that Medium Impact BES Cyber Systems be eliminated from the applicability on 7.4 and 7.5.
The applicability for the “Associated Physical Access Control Systems” is unclear. Are these PACS associated with the Low Impact BES Cyber Assets or those of Medium and High Impact BES Cyber Assets?
In requirement part 3.2, are “access control, logging, and alerting systems” the same as or something different than Physical Access Control Systems? If they are the same, GTC recommends consistent language. If they are different, please clarify.

In 1.2, "document" should be "documentation of" Requirement 1.4.1 should be more focused; more detail on what types of “security controls” are included is needed. Security controls are a key element of other parts of this standard as well and therefore need to be very clearly defined. Requirement 1.4.3 should be deleted. Documenting the test results is something you do to provide evidence of compliance; it does not promote reliability. If you do not document the test results you will not be able to show compliance with 1.4.2, but it is not fair for the same act to also constitute violation of 1.4.3.
How would an entity monitor for changes in physical location; does this require RFID of each asset? This requirement should allow flexibility between monitoring or annual validation, perhaps as part of the VA process.
Individual
Steve Karolek
Wisconsin Electric Power Company
Yes
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In the definition of "CIP Exceptional Circumstances", consider providing examples of impediment of large scale workforce availability such as a work slowdown, strike or pandemic.
Yes
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In High Impact Rating criteria 1.4 on page 15, the phrase "...that includes control of one or more of the assets..." should be changed to match the definition of Control Center, which requires the control of two or more assets. • Control Centers should be capitalized at the end of section 2.13 on page 17. • There should also be a column for LSE in the table provided on page 18. • On page 20, under the category "Balancing Load and Generation," Non-spinning reserve, the use of 'ramp rates' is typically associated with modeling programs not typically used as real time operation information and should be removed. • Managing constraints (page 21) has an extra bullet that should be removed. • Restoration of BES – 'coordination' all by itself lacks context and should include additional words to better frame the intent. • Inter-Entity Coordination and Communication – In additional to the recommend removal of 'communication' from the section, this should also include BA within the Operational Directives.
No

Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 1.1 discusses changes that are "...intended to be in service for more than 6 calendar months..." It may be extremely difficult to document such intention to the satisfaction of an audit team. Wisconsin Electric Power Company requests that the Standards Drafting Team revisit this requirement and reword it to ensure it is actually auditable.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 2 and Measure 2 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. If the Guidelines and Technical Basis section will remain in the final published version of the standard, the table on page 18 should be updated to include the Entity Registration of Load Serving Entities with consideration of an "X" in the functional rows of "Dynamic Response", "Balancing Load and Generation" and "Controlling Voltage".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Measure 1, the bulleted items should be separated by ", or,". The requirement for designation to be made by a "high level official" is too vague. Designation of the CIP Senior Manager should be made by an officer of the company.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): If this requirement and measures are retained, the second measure should be further defined to identify acceptable (auditable) evidence that the ten topics were implemented. In the Guidelines and Technical Basis for Requirement 2, review the third bullet of section 2.4 and consider changing the phrase "ingress and egress" to the word "access" since monitoring and logging egress is not intended.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 2 and Measure 2 contain the phrase "…initially upon the effective date…". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. The wording of Requirement 3 could be interpreted to mean that there are two annual events to track, a review event and an approval event. Wisconsin Electric Power Company requests that the Standard Drafting Team consider wording changes to clarify that the annual review and approval is considered to be a single event.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): The bulleted list in Measure 4 should be separated by ", or," between each bulleted item. The last bulleted item should define the periodicity of training as annual. Consider whether the word "contactors" in the second bulleted item should be changed to "contractors".
No

Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Requirement 6, review the use of the word "change2" and consider changing this to "change". Also, in Rationale 6, review the use of the word "authoritv" and consider changing this to "authority".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
Yes
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Table R4, part 4.2 on page 17, delete the phrase "regardless of duration". It adds nothing to the meaning since there is a six month exception for certain addresses. Suggested new wording for this requirement would be: "Seven year criminal history records check in each county of residence, including any temporary residences where the individual lived away from a permanent residence while attending school for at least six months or while working for at least six months. A permanent residence is one which would be used when filing a state or federal income tax return. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed." Our rationale for this wording is that it clarifies that the county criminal court is the level of jurisdiction at which the inquiry must be made. This is distinct from the local municipal level, the state level or the federal level. It recognizes that some individuals travel to pursue education or employment and that they establish temporary residences in dormitories, apartments and motel rooms while away from a permanent residence. It allows individuals to seek, and employers to send personnel to, training or temporary work for up to six months without invoking a need to expand the scope of the PRA.
Yes
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): The lists in Measures 6.1, 6.2, 6.3, 6.5 and 6.6 do not follow the conventions for either numbered lists or bulleted lists. Based on the context, Wisconsin Electric Power Company recommends that these be formatted as bulleted lists, with the bullet items separated by ", or,". The bulleted list in Measure 6.4 should have the bullet items separated by ", or,". In the measures for Requirement 6.4, we would appreciate clarification to explain the difference between the two bullet items, which are extremely similar.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): The lists in Measures 7.1, and 7.2 do not follow the conventions for either numbered lists or bulleted lists. Based on the context, Wisconsin Electric Power Company recommends that these be formatted as bulleted lists, with the bullet items separated by ", or,". The bulleted list in Measure 7.5 should have the bulleted items separated by ", or,". The items in Measures 7.3 and 7.4 should be formatted as

bulleted lists, with the bullet items separated by ", or,".
No
Wisconsin Electric Power Company agrees that the requirement to revoke access when access is no longer needed is essential to the safe and reliable operation of the BES. We accept that we must establish effective and reliable systems to achieve that result and that we must be able to demonstrate our compliance with the requirement. We commit to establishment of an environment of a culture of compliance that strives for error-free results. However, in-service transfers and reassignments and out-of-service transitions are an area where many organizations have difficulty implementing effective and reliable controls. Not every such transaction begins with an individual informing their employer that they will be leaving service in 30 days. We can provide many examples if needed. We assert that planned, orchestrated out-of-service, reassignment and transfer events are less common than FERC suggests in Order 706, paragraph 461. And even fewer occur under the direct scrutiny and awareness of the security organizations responsible for compliance. In any larger organization, there is no single person or work group with complete situational awareness of every potential HR event. Because we are aware of this risk, we establish controls that deal with the planned, orchestrated events. We insert ourselves into existing automated information flows. We issue periodic awareness messages. We create tracking systems to time stamp events. We train supervisors and HR staff. We even add personnel to our organizations dedicated to NERC CIP compliance. However, this is an area of compliance that relies on habits and human memory, not automated systems that generate alerts and exception reports. It asks HR personnel and broadly dispersed supervisors to have high situational awareness of the impact of each personnel decision on authorization for access to NERC assets. Due to these compliance risks, we believe that the expectations established in the VSL for R7 are unreasonably high. In support of this position, we cite the Commission's own language in paragraph 461 which states in part, "...MOST organizations will know in advance..." (emphasis added), and "We understand that outlying elements may require some brief lag before denial of access is effective...". We believe this demonstrates the Commission’s knowledge and understanding that error-free compliance is unlikely and that exceptions will occur. It is unfair to demand that reasonably anticipated exceptions should lead to sanctioned violations. We suggest instead that "Severe VSL" should read: "The Responsible Entity did not have a documented process for access revocation." And that "High VSL" should read: "The Registered Entity had a documented process for access revocation but failed to follow it for more than (some number of) personnel." And that the "Moderate VSL" should read: "The Registered Entity had a documented process for access revocation but failed to follow it for more than (some smaller number of) personnel." The measures for R7 should then include documents sufficient to demonstrate that the process was documented and followed, but achievement of the time threshold was delayed and why.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Measures 1.2 and 1.3, the words "and egress" should be removed. The current standard does not require logging exit transactions and no significant benefit accrues from establishing such a requirement. In Measure 1.6, the time of entry should be shown in addition to the date.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments

submitted by Edison Electric Institute for this question (with the following exceptions/additions): If these requirements are to remain in the standard, the requirement in Table R3 part 3.1 on page 18 would be better if split into two requirements, one for maintenance and one for testing. In Table R3 part 3.2 on page 18, in the applicability column, "Associated Physical Access Control or Monitoring Systems" should be changed to "Associated Physical Access Control Systems".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Requirement 2.3, the bullet items in the measures column should be separated by ", or,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In requirement 3.2, the bullet list items in the measures column should be separated by ", or,". In requirement 3.3, the measures should be a bullet list, not a numbered list, and the bullet list items should be separated by ", or,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Requirement 4.3, the numbered list items should be separated by ", and,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 5.6 has the potential to generate many TFEs and should include language stating that a TFE is not required for those devices where this is not technically feasible.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): The measures for Requirement 1.3 should be written as a bulleted list with bullet items separated by ", or,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 2.3 and Measure 2.2 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. The measures for requirement 2.2 should be written as a bullet list with bullet items separated by ", or,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 3.1 contains the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would

not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. The measures for requirement 3.1 should be written as a numbered list with ", and," between each bullet item. The measures for requirement 3.3 should be written as a numbered list with ", and," between each bullet item.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirements 2.1 and 2.3, and Measure 2.3 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 3.1 and Measure 3.1 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year.
No
The severity levels for Requirement 2 and Requirement 3 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): The requirements in Table R1, Part 1.1 on page 10, as a numbered list, should be separated by ", and,". The measures in Table R1, Part 1.1 on page 10, as a bulleted list, should be separated by ", or,". The measures in Table R1, Part 1.2 on page 11, as a bulleted list, should be separated by ", or,". The measures in Table R1, Part 1.3 on page 12, as a bulleted list, should be separated by ", or,". The requirements in Table R1, Part 1.4 on page 13, as a numbered list, should be separated by ", and,". The requirements in Table R1, Part 1.5 on page 14, as a numbered list, should be separated by ", and,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No

Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirements 3.1 and 3.2 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. The measures in Table R3, Part 3.1 on page 29, as a bulleted list, should be separated by ", or,".
Yes
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 1.3 contains the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. The measures in Table R1, Part 1.1 on page 10, as a bulleted list, should be separated by ", or,". The measures in Table R1, Part 1.2 on page 11, as a bulleted list, should be separated by ", or,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): VSLs for Requirement 1 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
Group
Seattle City Light
Kevin Cyr
Yes
"EAP" should be dropped from the Standards. EAP actually stands for "Extensible Authentication Protocol" which was officially coined by RFC 3748 back in 2004. Cyber security standards should use standard terminology and certainly should not make up terms that conflict with existing cyber security terms.
Yes
A bright-line approach does not contain hypothetical conditions. The approach outlined by CIP-002-5 Attachment 1 does not provide a “bright-line” procedure for categorizing cyber assets or systems. “15 minutes” is arbitrary to cyber security and is an invalid measure for categorization. To illustrate this, apply the CIP-002-5’s proposed guideline to different scenario. The card payment industry (PCI) doesn’t ask “If the misuse of a system can result in stolen credit card numbers within 15 minutes…” and the health care industry doesn’t ask the same question about the disclosure of personal healthcare information. The arbitrary nature of the proposed approach simply shifts the “voluntary

compliance" problem from asset categorization to cyber asset categorization. "Most of these criteria are similar to those already approved by the industry as part of Version 4" suggests that the criteria are fine because they were previously approved. The approvals of CIP v1, v2, and v3 show the flaw of this logic. Additionally, Version 4 has not been tested.
No
This requirement contradicts basic regulatory compliance principles and will lead to conflict between regulators and entities. During audit, the regulators will ask for evidence that all cyber assets and systems were identified and categorized. The entity cannot prove this if identification records aren't maintained for low impact cyber assets.
Yes
No
The severity levels are determined by, among other things, the number of low impact cyber assets that are categorized improperly. The entity is not required to keep records of low impact cyber assets. This approach will not work.
Yes
Yes
Yes
This requirement implies that to be compliant entities will need to maintain an inventory of job functions and the track the roles of all personnel at all times. This will add significant administrative overhead to entity operations without significantly adding to cyber security.
No
The measures imply that a hard-copy signature is necessary to demonstrate approval. Corporate emails, digital signatures, and other formats should be included. The CIP requirements should not dictate how an entity conducts internal approvals.
No
SCL seconds APPA's comment.
Yes
Yes
No
In addition to the new tracking implicitly required by CIP-003-5 R4, the entities will also need to track the access roles for all personnel. This adds an additional facet to track without adding value to the current awareness and training requirements. Eliminate the overlaps between CIP-003-5 R4 and CIP-004-5 R2 and simplify the approach.
Yes
No
This requirement is not effective from a regulatory perspective because it lacks decision criteria for evaluation. As long as the entities have discretion in how they evaluate the PRA results, they should also have discretion in determining what information the PRA should include.
Yes
No
The CIP requirements should not specify that the CIP Senior Manager has the ultimate authority over the access approvals for an organization's assets. This contradicts the segregation of duties concept and should be removed. A single person should not have authority over monitoring a critical business process while also having an operational role in the same process. Also, the CIP requirements should

not dictate how an entity chooses to set up its management structure and the associated authority related to internal business operations.
No
Regarding rapid removal of access, FERC Order 706 Paragraph 460 and 461 also states, “outlying elements may require some brief lag before denial of access is effective, in which case, the circumstances justifying such lag must be documented for audit purposes.” The proposed requirement does not address delays in access revocation and is not reasonable. Additionally, compliance with the proposed short revocation timelines will require highly matured access management programs and systems. Such programs don’t grow and mature overnight. A medium sized organization would require 3-5 years to implement access management processes and systems to meet this obligation.
Yes
No
Regarding R1.2, this requirement states that each cyber system or asset must have an EAP between itself and all its neighbors. If this is not the intent of the requirement, then it needs to include the term “externally routable.” Additionally, the language needs to be clear enough to allow for an isolated network to have multiple subnets or networks without an EAP at each hop. This point will become increasingly relevant with the growing popularity of virtualization. Regarding R1.3, this requirement obviously refers to firewall functionality and should use the proper terminology. According to Wikipedia, a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass is called a “Firewall.” Permissions on a firewall typically refer to console access, and Access Control Lists (ACL) are the rules that govern ingress and egress traffic. "Require explicit...permissions" and "including explicit criteria" hints that a stateful and/or application firewall is required. Network traffic cannot be allowed or denied based on “explicit” anything without inspecting the traffic. This requirement is technically inaccurate and vague. Regarding R1.5, this requirement is not aligned with the rest of the Standard regarding remote access and provides opportunities for worthless monitoring. The requirement should not dictate where the monitoring points should be installed for several reasons. First, encryption is required for remote access but this Standard allows for the encryption termination point to be located anywhere (this issue is further addressed under the relevant requirement.) For example, if the termination point is behind the firewall then you’ll be monitoring encrypted traffic (this is impossible.) Second, if the outside interface of the firewall is on a public network (or even a poorly governed private network) and the monitoring point is also on the outside interface then there won’t be any monitoring value without a corresponding internal monitoring agent. Placement of monitoring agents should be determined by a security practitioner that is knowledgeable about their unique network. Even with expertly selected placement locations of monitoring, successful implementations usually require tuning and experimenting with different monitoring locations. There is not a valid cookie-cutter approach to monitoring design, especially given the restraints of the other vague requirements of this Standard.
No
This requirement appears to be incomplete. The addition of encryption to the Standards is more than overdue but is unfortunately missing the mark. Encryption is of little to no value with a poorly designed implementation. First, allowing the encryption termination to occur outside of the firewall while disallowing direct connections to the target cyber asset means that unencrypted authentication traffic is allowed from outside the firewall (potentially on a public or poorly managed private network.) The requirement does not mention anything about encryption types or strengths. Additionally, the requirement does not address key management which is equally important as the encryption itself. Also, reference to a guideline published separately from the requirements is up until now, not a good idea as the regulators are very quick to point out that “NERC guidelines are guidelines, not requirements.” All applicable and allowable configurations need to be included in the requirement or provide entities with full discretion for their remote access implementations.
Yes
No
SCL seconds APPA’s comments.

Yes
Yes
Yes
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
Yes
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
Yes
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
Yes
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
Yes
Yes
Yes
Yes

No
SCL seconds APPA's comments.
Individual
John Tolo
Tucson Electric Power
No
TEP is concerned that there is not adequate definition of a "facility", and how this differs from a Critical Asset in prior versions.
No
It is TEP's opinion that the changes to the bright-line criteria from Version 4 to Version 5, particularly #2.7 requiring the aggregate of all lines would have a large impact .
No
It is TEP's opinion that the asset identification and categorization process defined in the Attachment and the Guidance is not clear. It appears to go from specific cyber assets to general systems or facilities to determine level. This would appear to result in an inventory of every asset at every facility rather than just those determined to have an impact level of high or medium. It is our opinion that this approach should be reversed. In addition, the guidance does not clearly define the steps required for the process of asset identification, resulting in a great deal of confusion.
No
Senior Manager approval should only be necessary for identified BES Systems or BES Cyber assets.
Yes
Yes
Yes
Agree with requirement, comment is regarding Guidance. Concern with Guidance on having a policy regarding Remote Access, specifically "Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating remote access."
Yes
Yes
Yes
Yes
Yes
Yes
No
Concern is with 2.10 – "Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets", which is based on the FERC Order 706 paragraph 434: "clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets. CIP-004-1 should leave no doubt that cyber security training concerning a critical cyber asset should encompass the electronic environment in which the asset is situated and the attendant vulnerabilities. Any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions or inactions could, even inadvertently, affect cyber security. TEPC does not feel that 2.10 adequately conveys the order. Suggested wording:

“Training on BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets to the extent a person with access could put critical assets at risk through their actions, whether intentionally or accidental.”
Yes
Yes
TEP would like to see additional guidance on denial criteria.
Yes
Yes
Rationale for R6 is confusing. Paragraph 4 addressing the quarter reviews states “individuals actually provisioned to a BES Cyber System”. Then it states that “focus is on the integrity of provisioning access rather than individual accounts on all BES Systems”. Please provide clarification on which method of review is intended.
Yes
TEP suggests using the term “access revocation” instead of “access removal” in the measures section of 7.1, 7.3, 7.4. We do not feel the definitions are the same and the intent is revocation.
Yes
No
Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request that the intention expressed in the Rationale statement for R1.1 be clearly included in the Requirement which is vague as written. Suggest: “Define technical or procedural controls to restrict unauthorized electronic access so as Low Impact BES Cyber Systems are segregated from public or less trusted network zones.” Additionally, the concept of aggregation that is included in the Rationale is not defined elsewhere in the CIP Standards, which seems inconsistent. If this concept is to be considered here, it should be introduced in CIP-002. Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? For Requirement for R1.3, it is unclear why the Applicability for High Impact BES Cyber Systems does not include the reference to “with External Routable Connectivity” but it does for Medium Impact. What is the intended difference? Does this imply impacts to serial connectivity? If so, should the requirement clearly state that? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point or not? Request clarification on 1.5's "at each EAP". Is that inside or outside or both? The Rationale includes reference that the IDS must be separate from the Firewalls (2 distinct). If so, the Requirement should state that. From another point of view, if the intention is real time response detection, that could be stated without requiring that the method be IDS.
No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology. Recommend removing from M2.3 the statement "Note that a UserID is not considered an authentication factor." If needed, add to definitions.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
TEP requests a clarification as to whether the 30 day window is in reference to the “Change Rationale for Requirement R2.3.
Yes
No
TEP feels that, for Requirement R4.5, a 2 week window for sampling of logged events is too burdensome due to the number of unique logging systems. A monthly process would be reasonable.
No
For Requirement R5.4, TEP is concerned that this applies to Low Impact BES Cyber Systems. In addition, the requirement contains the statement, “For the purposes of this requirement an inventory of Cyber Assets is not required.” How would the TFE be managed without a list of assets impacted? Has the impact of requiring TFEs for every device within every BES critical asset been determined?
Yes
Yes
Yes
No
For Requirement R3.4, TEP feels an update within 30 calendar days for “any organizational” change is unreasonable. The standard does not clarify whether these include both external and internal organizations as are referenced in R1.3.3. Additionally, it is often impossible to guarantee notifications of such types of changes.
Yes
No
For Requirement R1.4, TEP requests clarification of the statement “verified initially after backup”. Does this imply every backup, or when a new backup method is used? For Requirement R1.5, TEP does not feel a TFE process is warranted and suggests changing the wording to “Preserve data, to the extent reasonably possible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.
Yes
No
For Requirement R3.4, TEP feels an update within 30 calendar days for “any organizational” change is unreasonable. The standard does not clarify whether these include both external and internal organizations as are referenced in R1.3.3. Additionally, it is often impossible to guarantee notifications of such types of changes.
Yes
Yes
No
TEP feels Requirement R2.1 would be particularly burdensome in the substation areas, and that the applicability to Medium Impact BES Cyber Sytems should be removed. Additionally , if this applicability remains, it is TEP’s opinion that the TFE requirement does not work. Monitoring changes to a baseline configuration for a device generally takes place on a system (monitoring system) outside

the device (monitored device). Would the TFE apply to the monitoring system or the monitored device? Would the RE be required to have multiple monitoring devices if one did not work with a particular monitored device?
Yes
Yes
No
TEP is concerned with the apparent overlap of access controls for protected information between CIP-004 and CIP-011. Access controls stated in Requirement R1.2 seem to apply to the physical controls as well as electronic, but CIP-004 R6.3 and 6.6 also cover access control (authorization and handling as part of that).
Yes
Yes
Yes
Individual
Tony Eddleman
Nebraska Public Power District
Yes
Distribution Provider is not listed in the definitions, but it is modified from its current use in each of the CIP standards under the Facilities section. Distribution Provider should not be defined in these definitions – the impact is too broad and reaches beyond the cyber security standards. If you want to change the definition of a Distribution Provider, it should be done in a separate project not associated with the cyber security standards. Specifically, the last two bullets should be deleted on including a Transmission Protection System and a TO's restoration plan. These bullets are too broad and include systems which don't materially affect the reliability of the Bulk Electric System. In general, we understand why you are trying to move away from critical assets (CA) and critical cyber assets (CCA), but the change is too significant and doesn't provide a reliability benefit. We have invested significant effort and cost in our current documentation of CAs and CCAs. We understand how to identify CA and CCAs under our current standards, but we don't understand how to identify Cyber Assets and Cyber Systems as defined in the version 5. Recommend the drafting team follow the recommendations of the MRO NSRF (comments submitted separately) and retain the current CIP-002-4 bright line criteria in place of the proposed CIP-002-5. BES Reliability Operating Services introduces confusion and sets up a compliance trap. At a high level, it sounds reasonable, but trying to implement the concept is problematic. We will need a document to address each and every item identified in this definition to prove we are compliant and prove we have reviewed our systems in accordance with this list. The current bright line criterion in CIP-002-4 adequately addresses how to identify Cyber Assets and Cyber Systems and is significantly easier to implement. As an example, if a dynamic map board is used for situational awareness for the operators, is it a cyber system requiring protection? It appears it is a Cyber System. But, the operators still have screens on their computers for situational awareness. If a problem occurs with the map board and reduces their situation awareness, at what point is it a compliance issue? If a light bulb on the map board fails to light, do we have 15 minutes to change the light bulb before we have to report noncompliance to our Regional Entity? How do we know if the light bulb blew when it attempted to light or failed earlier – maybe we have already exceeded the 15 minutes? In a mitigation plan to prevent the light bulb from failing again, how do I prevent the light bulb from failing in the future? Will I be required to set up an identical map board for a test system? The cost is significant. It appears the only compliance solution is to remove the map board and reduce reliability by denying operators this additional tool due to these new compliance requirements and associated risk of a potential violation. This is only one example of many compliance traps introduced by the BES Reliability Operating Services definition. Each of the individual categories, while there are many identified, are still too broad and will require significant

documentation to an auditor why our system is or isn't included. We can't go down this path, because it opens up too many undefined situations.
Yes
As discussed in item one above, we recommend retaining CIP-002-4 and not implementing CIP-002-5. CIP-002-5 is confusing and will be difficult to implement.
No
We disagree with the SDT's comments during conference calls & webinars that entities will not have to have a "list" of LOW cyber assets. Audit teams will, especially early in the process, want to assess that how we evaluated each asset was correct with the intent of the standard. They will want to see how we checked each asset against the BES Reliability Operating Services to see that we didn't make a mistake. The audit teams will be checking for 100% compliance without any room for errors. We don't understand how we prove compliance without a list of LOW Cyber Assets. The shear scope of evaluating all cyber assets is daunting. Keeping these lists current seems like an enormous paperwork exercise. We question how this improves reliability when we will spend more time chasing paper than keeping up with current security issues & practices. The requirement to be 100% compliant and have documentation to prove 100% compliance at all times is unrealistic and drives registered entities to focus more on documentation and spend our customers dollars on trivial items instead of equipment improvements that will increase reliability. If a registered entity has a program implemented and misses minor documentation issues, the registered entity should be allowed to address the minor issues in a Corrective Action Program (CAP) and not be required to self-report the issues as potential compliance violations. The registered entity should document the minor issues in their own CAP and provide them upon request to the audit team during an audit. As an example, if you have several hundred individuals on an access list and have successfully added and removed the majority of them in the time periods specified, but missed a few of the removal dates by a few days, it's evident you have a program in place and implemented. The CAP would address how to correct the remaining items and further identify any repetitive or systematic issues.
No
Delete the "not to exceed 15 calendar months between approvals" in CIP-002-5, R2 and M2 and throughout version five of CIP-002-5 through CIP-011-5. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
We are confused on which Cyber Assets and Cyber Systems the requirements in CIP-003-5 apply. In section 5. Background, under the Applicability section, the document refers to a table row to define the scope to which a specific requirement row applies. The only table provided in CIP-003-5 references VRFs and VSLs (i.e., an applicability table doesn't exist). The applicability section goes into detail on high, medium, low, and other Cyber Assets and Cyber Systems, but it isn't clear which requirements apply to which assets. General Comment affecting all the Version 5 CIP-002 through CIP-011 standards: Any requirement for "Low Impact Ratings" should be pulled from the various standards and collected in a stand alone standard specifically addressing low impact BES Cyber Assets and BES Cyber Systems. The current method of weaving the low impact requirements in with all the other requirements is confusing - this is a compliance trap.
No

We are confused on which Cyber Assets and Cyber Systems the requirements in CIP-003-5 apply. In section 5. Background, under the Applicability section, the document refers to a table row to define the scope to which a specific requirement row applies. The only table provided in CIP-003-5 references VRFs and VSLs (i.e., an applicability table doesn't exist). The applicability section goes into detail on high, medium, low, and other Cyber Assets and Cyber Systems, but it isn't clear which requirements apply to which assets. General Comment affecting all the Version 5 CIP-002 through CIP-011 standards: Any requirement for "Low Impact Ratings" should be pulled from the various standards and collected in a stand alone standard specifically addressing low impact BES Cyber Assets and BES Cyber Systems. The current method of weaving the low impact requirements in with all the other requirements is confusing - this is a compliance trap.
No
Delete the "not to exceed 15 calendar months between reviews and between approvals". This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience! Also, please refer to item 6 above.
No
We are confused on which Cyber Assets and Cyber Systems the requirements in CIP-003-5 apply. In section 5. Background, under the Applicability section, the document refers to a table row to define the scope to which a specific requirement row applies. The only table provided in CIP-003-5 references VRFs and VSLs (i.e., an applicability table doesn't exist). The applicability section goes into detail on high, medium, low, and other Cyber Assets and Cyber Systems, but it isn't clear which requirements apply to which assets. General Comment affecting all the Version 5 CIP-002 through CIP-011 standards: Any requirement for "Low Impact Ratings" should be pulled from the various standards and collected in a stand alone standard specifically addressing low impact BES Cyber Assets and BES Cyber Systems. The current method of weaving the low impact requirements in with all the other requirements is confusing - this is a compliance trap.
No
We are confused on which Cyber Assets and Cyber Systems the requirements in CIP-003-5 apply. In section 5. Background, under the Applicability section, the document refers to a table row to define the scope to which a specific requirement row applies. The only table provided in CIP-003-5 references VRFs and VSLs (i.e., an applicability table doesn't exist). The applicability section goes into detail on high, medium, low, and other Cyber Assets and Cyber Systems, but it isn't clear which requirements apply to which assets. General Comment affecting all the Version 5 CIP-002 through CIP-011 standards: Any requirement for "Low Impact Ratings" should be pulled from the various standards and collected in a stand alone standard specifically addressing low impact BES Cyber Assets and BES Cyber Systems. The current method of weaving the low impact requirements in with all the other requirements is confusing - this is a compliance trap.
No
We are confused on which Cyber Assets and Cyber Systems the requirements in CIP-003-5 apply. In section 5. Background, under the Applicability section, the document refers to a table row to define the scope to which a specific requirement row applies. The only table provided in CIP-003-5 references VRFs and VSLs (i.e., an applicability table doesn't exist). The applicability section goes into detail on high, medium, low, and other Cyber Assets and Cyber Systems, but it isn't clear which requirements apply to which assets. General Comment affecting all the Version 5 CIP-002 through CIP-011 standards: Any requirement for "Low Impact Ratings" should be pulled from the various standards and collected in a stand alone standard specifically addressing low impact BES Cyber Assets and BES Cyber Systems. The current method of weaving the low impact requirements in with all the

other requirements is confusing - this is a compliance trap.
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
The requirement for Quarterly Security Awareness is excessive. There is a “yearly” training requirement, so why do quarterly awareness. Even nuclear does not require that level of awareness. Our teams are already required to read and be aware of so much information that this additional awareness requirement provides minimal if any value. Recommend a bi-annual requirement, and reduce the burden on entities. Having a blanket statement that must include vendors in our security awareness is excessive for them. This requirement forces us to track each vendor with access reviews of quarterly data, and requires the vendor who supports many customers to review each of those independently. We propose a change to include only vendors “on-site” be included in the quarterly awareness (or biannual as proposed above), with off-site/remote only being required to do the yearly training. This is consistent with nuclear practice, and is consistent with any associated risk.
No
We understand the point of defining specific roles that the SDT believes require training. However, we believe that there are too many categories that require training listed. It is conceivable that individuals could have responsibilities in all nine (9) of the areas listed in R2. This would require completion of nine (9) different training modules every year. This seems excessive, not to mention the burden on the individual responsible for upkeep of the training material to ensure its correctness and applicability.
No
In Table R4, delete, “including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more”. It’s impossible to prove we reviewed all locations where an individual has lived over the past seven years. We can threaten to fire the individual if they prove false or misleading evidence on where they have lived, but we have no control over the information they provide. Also, there isn’t a nation-wide system that can check an individual’s previous residences and confirm they have provided reliable information. If an individual does lie to us in attempting to obtain a job by covering up residence information, and we find out later, now we have to self report a compliance issue. This requirement goes too far by requiring all locations.
No
Delete the “not to exceed 15 calendar months between verifications” in Table R6 Part 6.5 and Part 6.6. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
The draft standard currently requires revocation of unneeded access by the end of the next calendar day. For most instances, when people change jobs, they continue to support their old position for at least 30-60 days, while the position is re-staffed or retraining of someone new can be completed. The guidelines state that “a review of access privileges must be performed”. The standard wording does

not state that at all, it states revoke, with evidence showing it was done. This wording in the standard must be changed to allow us to continue using the individual that was reassigned or transferred, as we deem appropriate.
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
Requirement 1.3 requires two factor authentications for physical access to HIGH Impact areas. In the measures, it states to provide evidence for how “ingress and egress is controlled by two or more different methods”. Two methods are not required for egress and this requirement for documentation must be changed.
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
The Measures section for Table R1, Part 1.1 references screenshots showing accessible ports of BES Cyber Assets as evidence, and this is infeasible. Obtaining the data into text files is fine, but to attempt to get screenshots of all these ports is an enormous amount of work. We understand the measures indicate this evidence “may include”, but an auditor will point to the measure and indicate for us to prove our compliance, we have to provide the screen shots. Please change the screen shots to text files.
No
In Table R2, Part 2.1, requires monitoring patches and updates for “all” software and firmware associated with BES Cyber System or BES Cyber Assets. This is a compliance trap. In a large Cyber System, the risk is great of missing a small piece of software embedded in a vendor’s product. What if a product is no longer supported or the vendor that developed the software/firmware is no longer in business? How do you comply with this requirement?
No
Table R3, Part 3.2 requires us to, “Disarm or remove identified malicious code.” Of course we want to do this, but what happens if we don’t get it all – are we in violation? Once a system is infected, it’s extremely difficult to clean; and, as we learned with STUXNET, we may not realize the total extent of the infection until later. We understand this requirement and agree it’s the right thing to do, but implementation will be difficult and then to wrap the compliance piece around the event will be almost impossible to prove compliance. Table R3, Part 3.3 requires signature or pattern updates within 30 days of availability of the updates. For remote locations, this is not realistic. A real-time system operating in the BES is difficult to update that quickly. The update process has inherent risks of inadvertently tripping an on-line device or piece of equipment. A generation unit may have a cyber system isolated from any external connectivity and the cyber system may only be available for updates during a planned outage. Please leave some operational flexibility for a registered entity to install the updates at a frequency consistent with the risks for the system. A suggested wording for the requirement is, “within 30 days or other time period documented as appropriate by the registered entity”.
No
Table R4, Item 4.3 is a compliance trap. At a minimum, please change, “next calendar day” to “next

calendar business day". Please provide more information on what this requirement is requiring. Table R4, Item 4.4 – why should we have to maintain records of disposition of event logs? If we can show 90 days of logs, providing records of disposition is unneeded documentation. By adding this into the Measures area, an auditor can require either this or something similar from us to prove we are compliant. Table R4, Item 4.5 – we don't understand this requirement. It appears to be requiring us to review a log that we are reviewing logs. Recommend this requirement be deleted in its entirety. This is unnecessary documentation.
Yes
We appreciate the wording change to include "the maximum complexity supported by the BES Cyber System". Thank you!
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
In Table R1, Part 1.1, please remove "identify, classify" from the requirement. In Table R1, Item 1.2, please remove this requirement in its entirety. In Table R1, Part 1.3, please remove section 1.3.3.
No
Delete the "not to exceed 15 calendar months between executions of the plan(s)" in Table R2 Part 2.2. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
Delete the "not to exceed 15 calendar months between reviews" in Table R3 Part 3.1. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience! Table R3, Parts 3.2, 3.3, and 3.4 – Recommend combining these three parts in one and allow 90 days to update and communicate the changes. The current 30/60/30 time periods are confusing.
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
In Table R1, Part 1.5, our first and highest priority is to restore the real-time system to operations. While preserving data is desirable, it should not be the focus during a restoration. The requirement should plainly state restoring the BES Cyber System or BES Cyber Asset is the priority function and

preserving data is desirable, but not required at the expense or getting the system restored. As currently written, this is a threat to reliability, not an enhancement.
No
Delete the “not to exceed 15 calendar months” in Table R2 Parts 2.1 and 2.2. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
Delete the “not to exceed 15 calendar months” in Table R3 Part 3.1. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
Table R1, Part 1.5 is not clear. If we add a disconnect to a one-line drawing in the Energy Management System (or other database change), is this change required to be tested prior to implementation? This requirement will significantly hinder any operational changes to support field crews real-time. This requirement will also add documentation requirements for changes to the Cyber Asset that don’t adversely affect the security controls. The additional testing requirements aren’t security related and should be removed from the standard.
No
Table 2, Part 2.1 has the potential to add significant TFE’s without a corresponding increase in security. This requirement will also reduce the reliability of the BES Cyber Systems by increasing the complexity/administration due to unnecessary software monitoring each system.
No
Delete the “not to exceed 15 calendar months” in Table R3 Part 3.1. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!

No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
Delete the “not to exceed 15 calendar months” in Table R1 Part 1.3. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
The implementation period should be phased for high, medium and low impact assets. Since the cyber security standards have changed significantly, registered entities need to make significant changes to existing programs, while maintaining compliance to existing standards. High impact Cyber Systems should be implemented first, followed by medium, followed by low. Our task of bringing in low impact Cyber Systems is significant and should not be attempted while trying to address high and medium Cyber Systems.
Individual
Mark B Thompson
Alberta Electric System Operator
Yes
The definition for Intermediate Device doesn’t specify where the device should be located, i.e., limit to secure networks.
Yes
The AESO agrees, but we may need to write a requirement in the Alberta version of the standard to designate the work required specifically of the ISO.
Yes
Wording changes may be required in Alberta to align with our concept of “annual”. Alberta Reliability Standards do not use the word “calendar” to imply a consecutive time frame.
Yes
Yes
Yes
Wording changes may be required in Alberta to align with our concept of “annual”. Alberta Reliability Standards do not use the word “calendar” to imply a consecutive time frame.
Yes

The use of the term “appropriate” makes it difficult to define which individuals need to have access to the policies.
Yes
Yes
Wording may have to be changed in Alberta to align with our concept of “days”, and we don’t use the word “calendar” to imply a consecutive time frame.
Yes
The AESO agrees with need for security awareness training. The Change Rationale states that the requirement to “ensure everyone with authorized access receives this awareness” differs from the R1 Rationale, which states that R1 “ensures that personnel who have authorized [access] maintain awareness of best security practices.”
Yes
No
Part 3.1 may be onerous because training will be required for every new hire in the applicability section, and the training program outlined in R2 and its parts will be quite extensive. Training groups of new hires within a certain timeline would be more practical.
Yes
The AESO will need to change the wording and/or requirements in parts 4.1, 4,2, and 4.4, to meet applicable Federal and Provincial laws in the Albert Reliability Standards version.
Yes
The AESO will need to change the wording and/or requirements in parts 4.1, 4,2, and 4.4, to meet applicable Federal and Provincial laws in the Albert Reliability Standards version.
No
The AESO suggests that the requirement for part 6.4 should read “…that individuals provisioned for unescorted physical access or authorized electronic access to BES Cyber Systems…” The original wording implies “unescorted electronic access”, which is not a valid concept.
Yes
Parts 7.2. and 7.3 state “end of next calendar day” which implies these requirements could take place on a weekend or holiday. This will cause additional expense for some companies as they will have to have IT and Facilities staff on-call 24/7 to handle any revocations.
No
Can there be a Low Impact BCA/BCS within the same ESP as a High or Medium Impact BCS? The Applicability in Parts 2.1, 2.2, and 2.3 all reference High, Medium, and Associated, but not Low. Is it then possible to require a VPN into an ESP for High & Medium, but have a direct interactive connection for a Low within the same ESP?
Yes
Neither should be checked, as the AESO does not comment on the VRFs and VSLs.
No
The applicability is confusing between Parts 1.2 and 1.3. Both have “Associated Electronic Access Control or Monitoring Systems” and “Associated Protected Cyber Assets” listed as applicable, however the requirements in 1.3 are more comprehensive than in 1.2.
Yes
Yes

No
The AESO believes that Part 1.2 will not stop something like Stuxnet from propagating through a network.
No
The Version 5 Implementation Plan refers to R1.1 in CIP-002 for planned changes - which reads; " 1.1. Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category." The Implementation plan then stipulates a 12 month time period for entities to become compliant with all applicable requirements within CIPs v5 in cases where unplanned changes have occurred, but there is no requirement addressing unplanned changes within the CIP-002 standard.
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
Yes
MMWEC agrees with the comments submitted by APPA and NPCC.
Yes
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, MMWEC suggests for CIP-002 Attachment I - In 2.13, Change "(2) generation control centers" to "(2) generation Control Centers" (capitalize Control Center.) Indicate that Control Center is a defined term to avoid confusion with generation control rooms.
No
MMWEC agrees with the comments submitted by NPCC.
Yes
No
MMWEC agrees with the comments submitted by NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, –

Append: “ other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
Yes
Yes
No
MMWEC agrees with the comments submitted by APPA and NPCC.
Yes
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: “ other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by NPCC.
Yes
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: “ other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by NPCC.

No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by NPCC. Also, please clarify whether logged events must be reviewed for Medium Impact BES Cyber Systems.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in

frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by APPA.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
Individual
Andrew Gallo
City of Austin dba Austin Energy
Yes
The definition of "BES Cyber System Information" should include only floor plans, diagrams, equipment layouts, etc. that clearly delineate the cyber assets in some way. In other words, if the diagram denotes a device as a "Schweitzer" relay (or even an "SEL 2030"), the information should not require special treatment. Refer to additional comments submitted for Question 49. The SDT should also re-think including data in the definition of Cyber Assets. Additionally, "suspicious" is not an auditable term and ought to be removed. The same is true for "attempt." It is not clear which "attempts" justify reporting. Reportable BES Cyber Security Incident: Request that the drafting team keep this definition consistent with the efforts of the 2009-01 project team. The current definition does not align to the requirements listed in the new version of EOP-004. BES Cyber Security Incident: A malicious act that: • Compromises a BES Cyber System or BES Cyber Asset, or • Disrupts the operation of a BES Cyber System or BES Cyber Asset, or • Results in unauthorized physical access into a Defined Physical Boundary. BES Reliability Operating Services: we note the following: • "Identify and monitor flow gates" under "Managing Constraints" seems to be missing its bullet • We

recommend clarifying that the use of the word “Facility” means the NERC Glossary definition -- in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication” • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret. CIP Exceptional Circumstance: We request revision to “A situation that may involve one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance (internal or external), a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.” The definition needs some flexibility for entities to take appropriate measures without risking reliability of the BES that may not fit neatly into the conditions listed. CIP Senior Manager: Replace “NERC CIP Standards” with “NERC CIP-002 – CIP-011 Standards” because CIP-001 is not part of this set of standards. Control Center: We are concerned with the broadness of this definition. The SDT should consider the impact on small entities that will be affected by a broad definition of Control Center. In the proposed definition, the SDT uses the defined term “System Operator” which is “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” If the SDT’s intent was to limit Control Centers to BA, TOP, GOP and RC functions, we support the definition and request that the SDT make this limitation clear in the definition or in guidance. Intermediate Device: Recommended changes: “A Cyber Asset that 1) may be used to provide the required multi-factor authentication for the Interactive Remote Access; 2) may be a termination point for required encrypted communication; and 3) may restrict the Interactive Remote Access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside an Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network.” Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity’s Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access may be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

Yes

Attachment 1, Section 2.13 assigns a Medium Impact to "generation control centers that control 300 MW or more of generation." Control Center is a NERC-defined term; however, because "control center" is not capitalized in 2.13, it creates confusion because it could be interpreted that a typical control room of a combined cycle unit could be construed as a "control center” by the Regional Entity. The SDT should capitalize the term in 2.13 to make it clearer. We recommend adding a threshold for BAs similar to CIP-002-4. Change to “Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority that includes control of two or more of the assets identified in criteria 2.1, 2.3, 2.4, 2.12.” We do not agree with the inclusion of all Transmission Owner (TO) control centers. These may include local distribution "dispatch rooms" with visualization capability and minimal control of BES Facilities. We recommend removing “TO” from Attachment 1, 1.4 and 2.13. Alternatively, if TOs must be included, we recommend using the qualifier similar to what the SDT drafted in the guidance: "agreements where some of the functional obligations of a Transmission Operator [are] delegated to a Transmission Owner (TO)" (i.e. Replace “Transmission Owner” with “Transmission Owner, assigned by agreement, the functional obligation of a Transmission Operator”). The addition of a “Low Impact” rating for every generation facility that does not meet the High or Medium Impact thresholds constitutes a significant change in the CIP Standards. This change forces every registered GO and GOP to adhere to approximately 40 requirements in the remaining CIP standards when, currently, those generators are not listed as Critical Assets. It seems unlikely that the cost to adapt existing corporate cyber security policies, cyber security awareness and cyber asset access management to these NERC CIP requirements will lead to a corresponding reliability benefit. In addition, Regional Entity audit resources would be better served if allowed to focus on more critical locations. We recommend this category be eliminated. Criterion 2.7 seems to have been modified to include some transmission substations operating at 200kV to 300kV. The present Version 4 bright-line criterion includes only those operating above 300kV. Because this includes substations interconnected to generators, it seems likely that 200kV substations newly identified as “Medium Impact” could include some generation facilities as well. This would require a

whole new level of regulatory compliance to facilities not included under the Version 4 Standards. There is no reason to believe the Version 5 criterion better identifies critical substations than the Version 4 criterion. This criterion should be changed back to the one approved by the industry in CIP-002-4. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal? In 2.12, “system” and “Facility” are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned.
No
For clarity, we request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days of when a change to BES Elements and Facilities is placed into operation.” For clarity and consistency with the previous suggested change, request changing M1 from “as required in R1 and list of changes to the BES)” to “as required in R1 and list of changes to the BES Elements and Facilities)”. The word “intended” should not be used in the requirement because it is not auditable. Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Part 4 needs clarification. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementing CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion framework. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. The SDT should consider an approach that would have documentation “requirements” in a guidance document rather than in the requirements in the standard. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is too complicated. In addition to the BES Cyber Assets classified as high, medium and low in CIP-002, the other standards introduce ten additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some appear in the standards themselves and these categories may or may not be included in the definitions document. This approach is complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future interpretations, CANs, etc. The Standards should be revised so that CIP-002 defines all assets needing protection rather than being introduced throughout the Standards. We recommend replacing “30 calendar days” with “90 calendar days.”
Yes
Recommend adding the following: “…has had its CIP Senior Manager or delegate review and update…”
No comment.
No
The SDT should re-think the use of a “CIP Senior Manager.” In many organizations, there will not be one senior manager responsible for implementing the CIP Standards. For example, in some organizations, SCADA/EMS and Relay personnel report to one senior manager, but I.T., Security and H.R. personnel report to a difference senior manager (or managers). Yet, the SCADA/EMS, Relay, I.T., Security and H.R. all have roles in CIP compliance. A better approach would be for the Standards to require that a Senior Manager be designated for each Standard (or requirement), but it need not necessarily be the same Senior Manager for each Standard (or requirement).
Yes
Request clarification of the meaning of “implement” M2.2.
Yes

Suggested change: “Each Responsible Entity shall review each of its cyber security policies and obtain approval of the policies by its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.” As written, the requirement appears to require approval of the CIP Senior Manager rather than of the policies.
Yes
No
Please see our comments in response to Question 6, above.
Yes
We recommend changing “30 calendar days” to “90 calendar days.” The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
No comment.
Yes
Providing Security Awareness is useful and should remain in the Standard. However, the SDT should re-think the need to have a Security Awareness Program. So long as the Registered Entity provides security awareness quarterly, the program adds no value and is merely another “compliance document” to maintain, review, update, etc.
Yes
Comments: Most of the requirements in R2 make sense. However, providing training on “physical access controls” is not necessary. The physical access controls are – generally – pretty straightforward (e.g. card key readers). It does not seem necessary to provide “training” on how to use a card key. The same can be said for training on electronic access controls. Most of those access controls merely involve two-factor authentication or something similar. The need to provide “training” on how to log on to devices is unnecessary. We recommend removal of R2.3 and R2.4 because they appear redundant to R2.2; alternatively, some explanation of the difference between R2.2 and R2.3/R2.4 should be provided. With respect to R2.8, it seems unnecessary to require training on recovery plans except for those very few employees who must implement the recovery plan. As currently worded, it is not clear whether only those who implement recovery plans must receive training. With respect to R2.10, it seems unnecessary to require training on the systems’ electronic interconnectivity and interoperability with other cyber assets. Generally, the personnel doing the “care and feeding” of those assets already know how they work and how they interconnect and interoperate. The personnel using those devices have no need to know about the interconnectivity and interoperability of the assets. Request clarification of whether personnel with access to only protected information need training/awareness.
Yes
Yes
For all R4 table entries, we recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2, we recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of the CIP Standards. The additional language should spell out when this “grandfathering” expires (which will be when a new check is required).
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”. For R5.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
The CIP Senior Manager should not necessarily have a role in R6.1, R6.2 and R6.3. There should, instead, be a particular person designated as the “gate keeper” for each cyber asset and physical

security area. For example, the SCADA/EMS manager is the logical person to grant access to the SCADA/EMS system, not necessarily the “CIP Senior Manager.” [We realize that, under the Standard, the CIP Sr. Mgr. can delegate the responsibility to a “gate keeper.” However, doing so simply creates another document (the delegation) to maintain, review, revise, etc. It makes more sense to just create the “gate keeper” concept.] The Registered Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. In R6.1, we recommend changing “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except.” Also, change “minimum necessary” to “minimum the responsible entity considers necessary.” In R6.2, 6.3, 6.5 and 6.6, change “minimum necessary” to “minimum the responsible entity considers necessary.” For 6.4, request clarification of whether variances noted in the verification would be required to be a self report. For 6.6, we request clarification of whether variances noted in the verification would be required to be a self report. In the measure for R6.6, change “BES Cyber System information” to “BES Cyber System Information.”
No
In Part 7.1, the use of “at the time” of the resignation or termination is vague and ambiguous. For example, if a person informs the utility that his/her resignation is effective in three weeks, must the utility revoke access when informed of the resignation or when the resignation becomes effective? We recommend making the requirement seven days. We recommend moving the text in the footnote for 7.1 into the requirement. For Part 7.2, we recommend requiring only that the revocation occur as part of the next quarterly review. Those personnel have merely been reassigned or transferred. They do not pose a risk to the BES (as opposed to, for example, an involuntarily terminated employee). It makes sense that people deemed to be a risk (i.e. those terminated for cause) should have a very short timeframe for revocation. However, for people in good standing who are transferred or reassigned, the time frame has gone down from a seven-day permissible time frame to a single day. This seems an unnecessary burden that will cause utilities to incur costs needlessly (i.e., overtime pay to do revocations on Saturdays, as most people who resign or get reassigned or transferred would likely do so effective end of business Friday). Again, these costs and obligations seem reasonable for terminations for cause, but hard to justify for employees in good standing. Recommend changing 7.3 to “For resignations or terminations, revoke the individual’s access to BES Cyber System Information by the end of the calendar quarter in which the resignation/termination occurs.” For Part 7.4, revoking a person’s overall access to cyber systems should suffice. In other words, if a person must be on your corporate network in order to gain access to critical cyber systems, revoking overall network access should suffice to meet the Standard (as opposed to revoking the person’s access to the various individual systems). If this language remains, we believe it should be revised as follows: “For resignations or terminations, revoke the individual’s user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within ninety (90) calendar days of the date of initial access revocation.”
No
There should be a “lower” and “moderate” VSL for R1 through R3 (e.g. For R1, a “lower” VSL could be if awareness reinforcement was done only two times in a year; a “moderate” VSL could be if awareness reinforcement was done only three times in a year). For R5, we recommend the following language: “Personnel risk assessments are not updated at least once every seven years. (5.2)” Also for R5, the “severe” VSL contains the following language: “The Responsible Entity did not have a documented process for personnel risk assessments.” Failure to have a documented process for PRAs should not involve a severe VSL. The important question is whether PRAs are being performed; not if there’s a documented process for performing them. In other words, if a utility can demonstrate it is performing PRAs (correctly and timely), it should not matter whether the utility has a documented process to perform PRAs.
Yes
For R1 there is an issue of auditability regarding Low Impact BES Cyber Assets. If an entity need not create a list under CIP-002, there is no way to ensure the technical and procedural controls have been applied. Request clarification for when Low Impact BES Cyber Systems are in the ESP with High/Medium BES Cyber Systems. Are such Low Impact BES Cyber Systems subject to 1.1 or 1.2? There is also some disagreement over the VRFs for this Standard. Currently, the VRF is set at Medium. For part 1.1, that VRF should not be Medium but should instead have its own VRF of “Low.” We propose the following wording change to Table R1, Part 1.1: Requirement: An Electronic Security Perimeter Procedure that defines operational or procedural controls to restrict unauthorized access.

Measure: Evidence may include, but is not limited to, an Electronic Security Perimeter Procedure that describes the operational or procedural controls and additional evidence to demonstrate that this procedure was implemented such as, but not limited to, the signature of the CIP Senior Manger on the procedure. The Measures language proposed is similar to CIP-004-5 R1. We believe the use of the word “implemented” without further description may be interpreted to mean a Responsible Entity will need to provide a listing of Low Impact BES Cyber Systems and proof of protection on each individual device. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. Request clarification that the 1.3 and 1.5 Electronic Access Points are the Electronic Access Points identified in R1.2.
No
We recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset" to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset" because, as written, the requirement does not allow for the development of new technology. We recommend changing the Measure for R2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors."
No comment
Yes
We request clarification of Part 1.1’s Applicability because it does not identify which of High/Medium/Low BES Impact the Physical Access Control Systems are "Associated" with. We request Requirement 1.2 be updated to allow "escorted physical access." We propose the following wording change to Table R1 Part 1.1: Requirement: A Physical Security Plan that defines operational or procedural controls to restrict physical access. Measure: Evidence may include, but is not limited to, a Physical Security Plan that describes the operational or procedural controls and additional evidence to demonstrate that this plan was implemented such as, but not limited to, the signature of the CIP Senior Manger on the plan. The Measure language proposed is similar to CIP-004-5 R1. We feel the use of the term “implemented” without further description may be interpreted to mean a Responsible Entity will need to show how each Low Impact BES Cyber Asset is physically protected. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.3 be consistent (not add a Requirement) with Requirement 1.3, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary " to "Issue real time alerts (to individuals responsible for response) upon detection of a breach through an access point". Request similar changes to R1.5. For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6.
Yes
Requirement 2.2 requires clarification. If the intent is to require that visitors sign-in once each day, the draft language does not clearly set forth that requirement. As currently written, the language could be interpreted to require entry/exit logs “on a per 24-hour basis.” Such an interpretation would mean a Registered Entity would have to retain a great deal of paper (where logs are maintained on paper). This is especially true for an entity on a six-year audit cycle (which will have to maintain 2,190 individual daily logs for each facility). Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis,"
No
Request clarification of 3.1 and 3.2on what the "Associated" under "Applicability" pertains to (i.e.: High, Medium, or Low BES Impact).
No comment.
No
Request clarification on R1.1, is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on M1.1, why does the Measure refer to BES Cyber Asset while

the Applicability refers to Systems? Recommend that “of BES Cyber Assets” be removed.
Yes
We request clarification of Part 2.2 because it requires creation of a “remediation plan.” However, if the entity applies the patch, no remediation plan should be necessary. We suggest wording similar to the following: "create a remediation plan or a plan to mitigate the vulnerability if the Responsible Entity opts to not apply a patch or update." What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to each patch or the overall process? Recommend removing “CIP Exception Circumstances” since the conditions in the definition do not align with the circumstances that may prevent the implementation of the patch. Suggest wording like "process for completion of the defined implementation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied".
Yes
The Standard should make an allowance in Part 3.3 for signature/pattern updates that create system problems/issues. In the Requirement for Part 3.4, the words, “…Transient Cyber Assets and removable media….” should read, “…Transient Cyber Assets or removable media….”
No
Suggested wording: “Upon detection, activate a response to event logging failures before the end of the next calendar day. Please clarify the Requirement for Part 4.3. Does it require that the failure be detected within a calendar day or that a response be implemented within a calendar day of a failure being detected? The Requirement in Part 4.5 for log reviews every two weeks is too frequent. We recommend monthly reviews (which is still more frequent than the 90-day reviews in the previous version of the Standards).
Yes
In Part 5.2, the CIP Senior Manager or delegate should not have to authorize the use of administrator, shared, default, and other generic account types. The “owner” of the asset (e.g. the SCADA/EMS manager) should be able to authorize the use of such accounts. [We realize that, under the Standard, the CIP Sr. Mgr. can delegate the responsibility to someone else. However, doing so simply creates another document (the delegation) to maintain, review, revise, etc. It makes more sense to just let the asset owner authorize the use.] Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
No comment.
Yes
Yes
For 2.1, recommended wording changes; "When a BES Cyber Security Incident is identified or tested, the incident response plans must be used and include recording of deviations taken from the plan." Please ensure that R2.3 aligns with the Evidence Retention section of the standard. Due to audit schedules, the entity may be required to retain the information for more than 3 years.
Yes
In Table R3, Part 3.2, 3.3, and 3.4 require different times for updates; 30 and 60 calendar days. We believe these times should coordinate with the plan in EOP-004-2 which allows 90 calendar days for update of the plan. For 3.3, recommend changing "Update" to "Where necessary, update”. Recommend changing "the completion of the review of that plan" to "the completion of the review performed in 3.2".
No
The VSLs need to align with the requested changes in questions 34-36.
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommended change: “When backing up Information essential to BES Cyber System recovery, verify the media to ensure that the backup process was successful.”

No
For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 2.1, request change to “functional exercise” rather than “full operational exercise”. This is consistent with the information provided in the rationale. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported.
No
For Part 3.1, we recommend “and document any identified deficiencies or lessons learned” as that topic is addressed in CIP-009 R3.2. In Table R3, Part 3.2, 3.3, and 3.4 require updates within 30 calendar days. We believe these times should be consistent with CIP-008-5 updates and, as stated in our response to Question 36, should be changed to 90 calendar days for update of the plan. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
The VSLs need to align with the requested changes in questions 38-40.
No
Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold.
No
This requirement will be very difficult to meet and will require many technical feasibility exceptions. We suggest the SDT remove this requirement and address the FERC Order 706 directive in a cost benefit analysis that the cost of putting these controls on all High and Medium Impact BES Cyber systems outweigh the cyber security benefit.
No
For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 3.1, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend change for 3.2 “…perform an active vulnerability assessment in a test environment which models the baseline configuration of the BES Cyber System in the production environment.”
No comments
No
For 1.3, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered.

Yes
Footnote 2 in 2.1 should be moved into the body of the Requirement.
No comments.
No
The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Because Version 4 is not FERC approved, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. We also have the following overall comments: I. Black Start Issues There are several black start-related issues. First, in the current version of the Standards, a Registered Entity can have Critical Assets with no Critical Cyber Assets (CCAs). So, for example, a company may have black start units (i.e. Critical Assets) which have no associated cyber assets that use a routable protocol. As such, those black start units can be Critical Assets with no CCAs. As a result, the Registered Entity would not have to meet the NERC CIP requirements for the black start units. The same concept does not exist in the Version 5 Standards. In the Version 5 Standards, black start units will require CIP protections. That fact could have a chilling effect on entities. In other words, some entities may not bid their units into black start service because, by doing so, they would have to incur the expense of becoming NERC CIP compliant. In the ERCOT Region, black start service is not very lucrative and, therefore, some companies may refrain from bidding into black start service due to the expenses associated with being NERC CIP compliant (plus the fear of potential fines down the road). Additionally, many Blackstart units in the ERCOT Region are older, smaller units with very low capacity factors and limited revenue. Applying the “Medium Impact” CIP requirements on those units will result in the need for significant CIP investment and increased on-going operational costs as well as increased compliance risks. This may result in Generator Owners/Generator Operators not offering units for Blackstart service. It would also likely result in Blackstart units not being maintained in a manner appropriate to support Blackstart service because of the additional on-going cost, thus removing them as a future option for providing Blackstart service. With fewer units offered for Blackstart service, ERCOT may not have enough Blackstart Resources to effectively restore the ERCOT BES after a complete or partial system blackout event. We believe a Blackstart unit with no External Connectivity poses little or no risk to the BES and should be classified as Low Impact. We recommend the following modification to CIP-002-5, Attachment 1, to ensure the continued reliability of the ERCOT portion of the BES: “2.4. Each Blackstart Resource with External Connectivity identified in its Transmission Operator's restoration plan.” Blackstart Resources with External Connectivity would remain in the “Medium Impact” category; however, Blackstart Resources without External Connectivity would move to the “Low Impact” category. The Blackstart Resources in the Low Impact category would have the appropriate physical and cyber protection controls as listed in the current CIP Version 5 draft standard. Our understanding of CIP Version 5 draft standards is that External Connectivity is defined as having Routable or Dial-up connections through an Electronic Access Point. Another concern focuses on facilities downstream of the black start unit. For example, one company could be chosen to provide black start service from a generator, but a different company owns/operates the facilities along the cranking path. If that were the case, the transmission company would now have to incur the cost of becoming CIP compliant even though it is not compensated for those expenses. The same is true for facilities associated with the next-start unit. If the switch yard for the next-start unit is owned/operated by a company other than the one that won the black start bid, that next-start company may have to incur the cost of becoming CIP compliant even though it is not compensated for those expenses. Another question involves whether units that are black start capable must be NERC CIP compliant regardless of whether they are in the black start restoration plan. The reliability of the ERCOT system may be adversely impacted because units that have been updated to meet the NERC CIP Standards but not selected for Black Start service could be forced into mothball or retirement due to economics associated with maintaining NERC CIP compliance. Many such units are small, have small staffs and low capacity factors, do not run much during the year and may be running on the margin. If companies are reluctant to bid into the black start market due to the costs associated with being NERC CIP compliant, it could result in inadequate black start capability due to Generation Owners not bidding units into the black start market. Finally, we request clarity on

the inclusion of “next start units” in the black start path. As CIP-002 currently reads, it could be interpreted that they are not included in the black start path; consequently, clarification is in order. II. Other Issues • We recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • We request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • We request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5.

Group

Florida Municipal Power Agency

Frank Gaffney

No

First of all, we thank the Standard Drafting Team for all of the hard work on what we believe is a very significant step forward on Cyber Security Standards. We believe that this is heading in the right direction. Having said that, this is the first draft and as such we have a significant number of comments that we hope will help improve the standards. Now, our comment to Question #1 is as follows: BES Cyber System – Maintenance Cyber Asset is not defined, suggest changing to Transient Cyber Asset. BES Cyber System Information – (1) Security procedures should not be on the list because it creates a conflict between CIP-011-1 that restricts access to the information and CIP-003-5 and CIP-004-5 that require general training and dissemination of those procedures. (2) BES Cyber System Impact is not defined. BES Reliability Operating Services – under Dynamic Response to BES Conditions, suggest adding Excitation Response. Under Balancing Load and Generation – suggest removing unit commitment since it will not meet the 15 minute window and it is an operations planning function and not a real-time operating service. CIP Exceptional Circumstance should include imminent danger to a BES Facility as a condition. CIP Senior Manager – the definition should exclude CIP-001, at least until it is retired with Project 2009-01 Control Center – (1) We assume that a Control Center is only a Control Center is used by an BA, TOP, GOP or RC. The definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” For clarity, we suggest adding this clarity to the definition. (2) The use of the word “facilities” in a fashion that does not mean “Facilities” will lead to confusion and ambiguity, especially since “facilities” is used later in the same sentence as meaning “Facilities”. FMPA suggests: “One or more sites hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation Facilities or transmission Facilities, at two or more locations”. Facilities should also be capitalized in the first bullet. Defined Physical Border is ambiguous. Specifically, are all spacial dimensions, horizontal and vertical, to be established as part of the boundary? In other words, it seems like the “roof” may no longer be required, e.g., 5 walls instead of 6 walls, but, vertical dimension requirements of walls / fences are ambiguous.

No

FMPA believes that a fourth category of risk impact be developed, a “De Minimus Impact” category that would consist of otherwise Low Impact BES Cyber Assets but that do not have routable protocol or dial-up access. We understand that there is concern about Low Impact BES Cyber Assets due to the risk of a coordinated attack. A coordinated attack is much more likely to BES Cyber Assets that have routable protocol or dial-up access than to those BES Cyber Assets with no connectivity. It is much more difficult and impractical to attempt a coordinated attack on BES Cyber Assets without connectivity. Recognizing this difference in both difficulty level and Low Impact (in other words, it wouldn’t be worth the effort because other attack vectors with similar levels of difficulty would have more impact), we propose adding a fourth impact category, De Minimus Impact. FMPA would propose that these De Minimus Risk BES Cyber Assets would not need to comply with the CIP standards because the costs would be unjustified. Bullet 1.2, a Control Center for any BA, even very small ones, being High risk is inappropriate. For instance, the entire load or supply of a small BA would fit into the “noise” of a large BA for supply and demand mismatch. Suggest changing 1.2 to parallel 1.3, e.g., a BA Control Center that includes control of one or more of the assets identified in criteria 2.1, 2.3, 2.4

and 2.12. Bullet 2.13 could then be used to accommodate smaller Bas Bullet 1.3, Transmission Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” Bullet 2.5, “Facilities” should be changed to “Elements”. The cranking path is not necessarily part of the BES. Bullet 2.6, is an autotransformer of 500 kV to 230 kV included? Bullet 2.7 is inconsistent in its terminology, switching between “Facility” and “Lines”. It seems that “Line” is intended. The focus also seems to be “at a single station or substation” where the focus ought to be a single BES Cyber Asset / System that controls multiple Lines. FMPA suggest changing the first sentence of 2.7 to read: “Multiple Transmission Lines operating at 200 kV or higher, but less than 500 kV, where the total weighted value of all BES Transmission Lines whose Reliability Operating Services would be adversely impacted within 15 minutes if a single BES Cyber Asset / System is rendered unavailable, degraded or misused exceeds a value of 3000.” Bullets 2.8 and 2.9, the phrase “at a single station or substation location” does not seem to add any value and can be a source of ambiguity. FMPA suggests striking the phrase. Bullet 2.12, the 300 MW bright-line seems arbitrary (albeit carried over from prior versions). In general, the system is more tolerant to loss of load than loss of generation and the 300 MW seems out of proportion with 2.1 of 1500 MW. The reasoning applied in the Application Guideline is flawed. UVLS and UFLS are only last ditch efforts if other events have already caused the system to be on the edge. So, how is that different from 2.1 if the system is already on the edge? The focus should be on how a malicious user can cause an Adverse Reliability Impact; hence, we suggest 1500 MW instead of 300 MW. Bullet 2.13, (1) Transmission Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” (2) The term “control centers” should be capitalized in the phrase “generation control centers” to make it clear that it refers to the defined term “Control Center” In the application guidelines, when discussing the BES Reliability Operating Services, the bullets have associated with them the functional entity that typically provides those services. However, there are exceptions and the guidelines ought to reflect those exceptions; for instance, a TO may also provide UFLS. Also in the application guidelines, the word “facilities” is used in a fashion that does not mean “Facilities”, which creates ambiguity and confusion (e.g., Facilities by definition is part of the BES, whereas assets owned and operated by DPs and LSEs are typically not BES). Suggest using “elements”. The Application guideline discussion of bullet 2.13 of Attachment 1 is not consistent with the actual bullet.
Yes
FMPA agrees with the requirement but questions whether the standards actually meet the stated goal of the requirement to “not require discrete identification” of Low Impact BES Cyber Assets / Systems. There are numerous examples which seem to contradict this stated goal as described later in these comments and specifically to this requirement. How does one distinguish between a BES Cyber System and a non-BES Cyber System? Does this mean that we need to inventory all of our cyber assets and develop a test to distinguish between “Low” and “non-BES”, even though R1 says that “Low” does not “require discrete identification”? How are entities to prove to auditors that the identification and categorization was done without having an inventory, i.e., discrete identification? The VSLs seem to seem to imply that “Low Impact” needs to be discretely identified, e.g., what happens if an entity categorizes a Medium Impact as a Low Impact? In order to review correct categorization, doesn’t the auditor need to review Low Impact to see if they should have been categorized Medium or High Impact?
Yes
Yes
The Evidence Retention section of the standard should not refer to Rules of Procedure language that is subject to change. The sentence that states: “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit” should instead reference the Rules of Procedure, Attachment 4C on the CMEP, Paragraph 3.1.4.2, e.g., “also refer to the Rules of Procedure, Attachment 4C … Paragraph 3.1.4.2”. In this way, it is possible to accommodate changes to the ROP language without needing the change

the standard.
Yes
No
“Implemented” is not the right word because it creates double jeopardy with the rest of the CIP standards, e.g., a violation of another standard could mean that the policy was not implemented. Suggest changing to use the phrase “in force”, meaning that the policy is in force and able to be enforced, but not requiring enforcement of the policies in this requirement (implement includes enforcement), but rather enforcement is contained in ensuing standards. FMPA suggest rephrasing to: “Each Responsible Entity shall have in force one or more documented cyber security policies …” The standards are inconsistent in its use of BES Cyber Assets /Systems, e.g., R2, to be consistent with CIP-002-5, should use the phrase “BES Cyber Assets and BES Cyber Systems”. Alternatively, CIP-002-5 could just use BES Cyber Systems. The bullets are incorrectly numbered; they should be 2.1 through 2.10 and not 1.1 through 1.10
Yes
The grammar of the sentence is a bit off and it is not clear whether the CIP Senior Manager needs to approve each of the policies or not. Suggest moving the phrase “each of its cyber security policies” to after the word “Manager”, e.g., “Each Responsible Entity shall review and obtain the approval from its CIP Senior Manager for each of its cyber security policies …”
Yes
Yes
“Cyber Security Policy” should be “cyber security policies” to be consistent with R2 and R3.
Yes
There is an extra “2” at the end of the sentence within the standard.
Yes
See the discussion of Evidence Retention in response to Question 3 VSL to R5, should there be a time frame applied, e.g., failed to document … two delegations within the audit period, within a year? If three failures are spread over 30 years, e.g., one failure each 10 years, is that a severe violation?
Yes
“Implement” is ambiguous. If a process in “in force” but in one instance is not followed, is that a violation? The process has been implemented. Merriam-Webster’s has two definitions of “implement”, one of which is probably intended: 1: carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures 2: to provide instruments or means of expression for A process can meet both of these definitions. If enforced, a process can meet the first definition; if not enforced, the process can meet the second definition. FMPA assumes the SDT intends the first definition. FMPA suggests adding a footnote to specifically identify which definition of “implement” is intended.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 2.1, the measure and the requirement do not match. The requirement is to “define the roles”, the measure includes “and the training needed for each role”. Suggest adding this phrase from the Measure to the Requirement.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The phrasing of requirements that refer to tables is ambiguous with ambiguous reference of prepositional phrases. For instance, in this requirement, it is unclear if an entity that only has Low Impact BES Cyber Systems needs to develop training or not, i.e., does the prepositional phrase “that includes …” refer to “training program” or to “Responsible Entity” or to both? We suggest rephrasing: “Each Responsible Entity that owns applicable systems described in the Applicability column of Table ___ shall ___ in accordance with the applicable terms of Table ___” Such rephrasing should be done to all requirements that refer to a table associated with that requirement. In addition, measures should not include the word “must”. Measures are not enforceable

but are instead examples of evidence.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 4.2, the phrase “up to the current time” is problematic since it infers that 7 year criminal background checks need to be updated on at least a daily basis to cover “up to the current time”, This should be reworded to seven years prior to the last background check.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The flow of the bullets seems backwards and missing a job function analysis step. In addition, the word “minimum” implies an optimization that is impractical to achieve, e.g., do we want every individual account to be optimized to that individual, which is very difficult to administer and prone to error, or rather do we want to establish account groups based on job functional analysis with associated, appropriate levels of permission and assign individuals to these groups. The latter is easier to administer and less prone to errors, and follows established practices such as security clearance levels. FMPA suggests the following “flow”: 1. Job function analysis 2. “Account group” establishment with appropriate levels of permissions based on job function analysis with associated permissions 3. Assignment of individuals to the appropriate “account group” based on their position
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 7.1 is impossible for resignations. How is it possible for an entity to revoke access at the same time they receive a resignation? Footnote 2 does not help because it only applies to termination. For termination, the entity should know about the termination before the employee; however, for a resignation the reverse is true. FMPA proposes to create a new bullet specific to resignation and require revocation of access by the end of the next calendar day. Bullet 7.2, the urgency is out of alignment with the risk. Next calendar day means that if a re-assignment occurs on a Friday, that weekend work is required when that level of urgency is not justified by the situation / risk. FMPA suggest end of the next calendar week.
No
See the discussion of Evidence Retention in response to Question 3 The Severe VSL for R3 includes the phrase “The Responsible Entity did not fully implement its cyber security training program” which makes it a binary VSL and eliminates the High VSL described. For counts, e.g., R6, R7, should there be a time frame identified? E.g., 2 individuals within a year, within the audit period?
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The requirement does not describe the overall purpose of the processes required. Are these processes to deny unauthorized access? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define technical and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the procedural and technical controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. Bullet 1.2 is ambiguous and implies another requirement. First, one does not “use” EAPs to control and secure, rather, EAPs are controlled and secured through use of some other means. Second, the requirement is to secure only identified EAPs,, e.g., is it a non-compliance if an entity misses an EAP, e.g., did not identify it? Third, the Measures are all to support the identification of EAPs and not to “secure and control” EAPs as required by the Requirement. And fourth, the ensuing bullets (1.3, 1.4) seem to be requirements to secure

and control EAPs; and hence, bullet 1.2 seems to create double jeopardy. FMPA suggests rewording bullet 1.2 to require identification of EAPs and not “secure and control”.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See the discussion of Evidence Retention in response to Question 3 The VSLs are binary, so, it seems that if one EAP is missed, it is a severe violation. Is this appropriate? FMPA encourages the SDT to develop non-binary VSLs.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 1.1 is ambiguous. How can physical access be restricted without a Defined Physical Boundary? Does this imply that Low Impact assets need to be enclosed in both horizontal and vertical dimensions? Does a fence of xx height suffice? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define operational and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. The application guidelines act to embed a de facto standard requirement of 96 square inches that, if desired to actually be a requirements, must be specified in the actual Requirements of the standard and not in an application guideline that is not enforceable. Alternatively, a definition of a Physical Access Point could be developed with established thresholds that may vary between High, Medium and Low Impact and then the defined term used in the standard. FMPA is aware of challenges made by auditors to entity compliance surrounding issues like how thick does dry-wall need to be to constitute a wall. To avoid disputes between auditors and entities over what constitutes a Defined Physical Boundary, and what constitutes access points, FMPA encourages the SDT to develop bright-line criteria. Such criteria could be different for different risk impacts, e.g., for illustration purposes only: • High Impact might require 6 wall enclosure with every access of 96 square inches or larger opening defined as an access point with wall material of metal, concrete, or drywall of xx inches • Medium Impact may not require a roof, but, requires a fence or wall height of xx inches topped with a climbing deterrent such as barbed wire. • Low Impact video surveillance is sufficient. The standard is very ambiguous as to what is a sufficient physical boundary and will be open to debate between compliance and entities if such bright line criteria are not developed.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The note to bullet 2.2 that says “there is no need to document the escort or handoff between escorts” is inconsistent with the requirement of bullet 1.1 which states that visitors need “continuous” escort. How would one prove that escort was continuous without documenting the hand-offs? On bullet 2.2, what does the phrase “on a per 24 hour basis” mean? Does this mean that a visitor must be logged in and out on the same day and that if a visitor is there at midnight, then the visitor must be logged out at midnight on the prior day and logged back in the following day, or does this mean that military time is to be used when annotating the log?
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 3.1 is not limited to Medium and High Impact with the term “Locally mounted hardware or devices associated with Defined Physical Boundaries since Defined Physical Boundaries is not limited to only Medium and High Impact assets through its definition. This implies that all physical access controls, even those to Low Impact, are to be tested. Presumably, this includes padlocks used to control gates to fences, non-electronic door locks that control access to

substation control houses that contain Low Impact digital relays, etc. Such an interpretation would then require an inventory of those access controls, and presumably, to ensure a complete set, an inventory of Low Impact assets and their Defined Physical Boundaries. FMPA suggests adding to the end of the phrase “Defined Physical Boundaries associated with Medium or High Impact …”
Yes
See the discussion of Evidence Retention in response to Question 3 R1 has both a Long Term Planning and a Same Day Operations time frame listed because the separate bullets are different time frames. If a non-compliance occurs, wouldn’t Same Day Operations always trump Long Term Planning? If that is not the desired outcome, consider separating the bullets into separate requirements or apply the time frame on a bullet by bullet basis.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. On bullet 2.2. - (1) Suggest adding the phrase “addressed by the security related patches or updates” after the word “vulnerabilities” as clarification. (2) “Remediation” implies compensatory measures; the standard should not require compensatory measures because such measures may reduce reliability. Consider another term such as “palliative plan”, “alleviation plan”, or “assuagement plan”. On bullet 2.3, “A process for” is redundant with the parent Requirement and should be deleted and just start the sentence with “Remediate as identified in the plans of 2.2 …”
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 4.2 allows the entity to establish its own threshold criteria for what unauthorized electronic access or malware activity results in a real-time alert, is that a desired state? Bullet 4.3 implies redundancy, e.g., how will we know that event logging failed unless a redundant system tells us? Bullet 4.4 is a data retention requirement and does not belong as a requirement, but rather in the Evidence Retention section of the standard.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 5.4, if “implement” as used in R5 means to “carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures”, then, this bullet 5.4 would require a complete inventory of all Low Impact BES Cyber Assets to ensure that default passwords were changed …. To solve this, implement could be removed from the parent requirement and replaced with “have”, e.g., “have processes”, and then the bullets that require asset by asset / system by system implementation could re-insert the word implement. As such, what would likely need to happen is two bullets would need to be created for default passwords, one for High and Medium which would use the phrase “implement procedural controls” and another for Low Impact which would use the phrase “have procedural controls” to distinguish between a system by system approach for Medium and High and a programmatic approach for Low. Bullet 5.5.3 allows the entity to specify the amount of time between password changes, is this appropriate or should a bright-line be developed? For instance, High – 3 months, Medium – 6 months, Low – 12 months Bullet 5.6 allows the entity to specify the number of unsuccessful login attempts before an alert is issued, is this appropriate or should a bright-line be developed?
No
See the discussion of Evidence Retention in response to Question 3
No

See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect and respond to cyber security incidents. Otherwise, how is one to “identify, classify and respond to BES Cyber Security Incidents” on Low Impact systems? This “hidden” requirement is inappropriate. FMPA recommends making R1 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, even for Low Impact systems.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect and respond to cyber security incidents. Otherwise, how is one to know “(w)hen a BES Cyber Se4curity Incident occurs”. This “hidden” requirement is inappropriate. FMPA recommends making R2 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, and hence this is duplicative for Low Impact systems. Bullet 2.2, “implement” is not the correct term and is duplicative with the parent requirement. How would one “implement” the entire response for a table top drill since no IT systems would be involved? “Exercise” or equivalent term is more appropriate, e.g., “R2 … implement a process for … 2.2 (an) Exercise …” Bullet 2.3 is an Evidence Retention requirement and should not be a requirement.
No
First, the question does not match the posted Requirement. The Requirement actually states: “Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication”. See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. See comments to Questions 34 and 35. FMPA believes that in order to make this requirement applicable to Low Impact systems, which implies that CIP-007 become applicable to Low Impact systems and this “hidden” requirement is inappropriate. Instead, standard CIP-008-5 should not be applicable to Low Impact systems, especially in consideration of the requirements of EOP-004-1 which require entities to analyze and report cyber security incidents.
Yes
See the discussion of Evidence Retention in response to Question 3
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 1.4, what does the word “verified” mean, than the data is “retrievable”, or that all the data is verified? The intent seems to be that the data is retrievable, otherwise 2.2 seems duplicative.
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 2.1, “implement” is not the correct term and is duplicative with the parent requirement. How would one “implement” the entire recovery for a table top drill since no IT systems would be involved? “Exercise” or equivalent term is more appropriate, e.g., “R2 … implement a process for … 2.1 (an) Exercise …” Bullet 2.2 “current configuration” is not accurate. The back-up will not reflect the “current configuration” but the configuration at the time of the back-up.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15.
Yes
See the discussion of Evidence Retention in response to Question 3
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures

described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The CIP Senior Manager (or delegate) should approve the baseline (1.1). Presumably, the baseline would be “reset” periodically to reduce the number of changes that need to be tracked, and the CIP Senior Manager (or delegate) should approve the new baseline (1.3). Bullet 1.3, the phrase “as necessary” does not seem to add anything and creates ambiguity. Suggest deleting the phrase.
No
Having to monitor all the assets associated under the Applicability section of Table R2 is a huge TFE generator based on the requirement. If the intent is to make sure that there have been no modifications to the device, it would seem appropriate that one could monitor other items and not just the configurations in order to meet the requirements of FERC Order 706, paragraph 397. FMPA suggests that there are methods, such as documented monitoring of logins, wherein if a device has not been logged into, the configurations need not be constantly monitored. Having a yearly requirement to verify configurations (via MD5 hash matching, for example) is an acceptable requirement, but having to constantly monitor the devices for any configuration change is going to be impossible for many devices, and create an unnecessary burden on entities while adding no value to the protection of the BES. Also, this requirement appears to add additional technical controls such as “white listing” above what is already called for in CIP-007 R3. We believe the intent should be to ensure that as part of change control, system configurations are checked to determine if any changes from the approved baseline configuration have occurred since the last authorized change. If detected, these changes should be investigated as per procedures covered under CIP 007-R3. See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 3.2, what is an “active” vulnerability assessment? The term is ambiguous.
Yes
See the discussion of Evidence Retention in response to Question 3
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. There should be recognition of law, e,.g., unauthorized people are only granted access in cases where the law requires divulging that information, such as public records acts, or a discovery process order by a judge. It would seem that access to BES Cyber Security Information should be approved by the CIP Senior Manager as a separate bullet under R1.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
Yes
See the discussion of Evidence Retention in response to Question 3
Group
Western Electricity Coordinating Council
Steve Rueckert
Yes
BES Cyber Asset. From an enforcement perspective WECC urges the SDT to revise the proposed “BES Cyber Asset” definition to exclude the criterion that limits BES Cyber Assets to those that would impact BES Reliability Operating Services within a “15 minute window.” The “15 minute window” is not in the interest of reliability. Misuse of a BES Cyber Asset may pose significant risks to the BES within 16 minutes, 15 hours or 15 days. Further, entities and regulators will be forced to speculate as

to which Cyber Assets would impact BES operations within 15 minutes. There are hundreds of scenarios under which the same Cyber Asset may impact the BES over and under 15 minutes. The proposed Standard does not point to any study nor provide a rational basis to support the “15 minute window” exclusion. To ignore BES Cyber Assets that are presumed to not pose impact to BES operations within 15 minutes, is contrary to FERC Order 706, and the Federal Power Act §215. The 15 minute window restricts entity discretion and disregards the FERC Order 706 which states that “implementing [CIP] Reliability Standards must be done on the basis of the specific facts and circumstances applicable in the individual case at hand.” To limit BES Cyber Assets to Cyber Assets that would impact BES Reliability Operations within 15 minutes is, therefore, over prescriptive. WECC also recommends eliminating the exception that excludes “Transient Cyber Assets” from the definition of a BES Cyber Asset. If any Cyber Asset satisfies the criteria put forward in the definition there is no rational basis to exclude that Cyber Asset from identification as a Cyber Asset. The SDT should provide clarification regarding the definition of “adverse impacts to BES Reliability Operating Services” in the context of identifying BES Cyber Assets. What is an “adverse impact”? Are “adverse impacts” included in the definition related to “High” and “Medium” impacts described in CIP-002-5 “Attachment 1, page 23”? BES Cyber System A BES Cyber System is defined as “one or more BES Cyber Assets that are typically grouped together, logically or physically to operate one or more BES Reliability Operating Services.” The SDT should provide clarification as to how to determine if Cyber Assets are “typically grouped together.” Specifically, in the context Cyber Security, the technology is rapidly evolving. Including the term “typically” excludes the integration of new technology within an existing BES Cyber System. Secondly, the proposed definition of a BES Cyber System may exclude Cyber Systems that directly impact BES Operations. The proposed definition of a BES Cyber System presumes that BES Cyber Systems are comprised of Cyber Assets that individually impact BES Reliability operations within 15 minutes. The proposed definition, therefore, does not consider Control Systems critical to BES Operations apart from the impact of individual devices comprising that system. Consequently, a Cyber System comprised of Cyber Assets that collectively impact BES Operations would not be identified unless individuals devices within that system are first determined to have separate impacts on BES operations independent of that systems The definitions of Version 5 CIP Security Standards does not include a definition for a device identified as a “Maintenance Cyber Asset.” The exclusion of “Maintenance Cyber Assets” from BES Cyber System contradicts the definition of a BES Cyber Asset. If a “maintenance cyber asset” qualifies as a BES Cyber Asset there is no rational basis to exclude that device from being identified as part of a “BES Cyber System.” Control Center The definition of a “Control Center” in the “definitions” is inconsistent with criteria proposed in CIP-002-5, “Attachment 1”. The proposed definition “Attachment 1” Section 1.4 requires the Generator Operator to identify BES Cyber Assets that impact Reliability Operating Services at a black start resource. WECC recommends that the definition of “Control Center” to include one or more BES generation or transmission facilities at a single location. Transient Cyber Asset The definition of a “Transient Cyber Asset” should be revised to include more specific criteria. Any Cyber Asset connected to a BES Cyber Asset or Protected Cyber Asset for 30 days or less may pose a significant risk to the BES. Any Cyber Asset capable of altering the configuration of or introducing malicious code to the BES Cyber System should be considered a BES Cyber Asset regardless of the duration of its connectivity. Electronic Security Perimeter Definition does not say clearly that this has to include ALL interfaces from outside the BES(s) being protected. Suggest change to: “The collection of all EAPs that permit communications to a BES system from a device not in that system.” Note that existing definition of EAP says “restricts” rather than "permits.” Unsure of the specific meaning of “restricts."

Yes

From an enforcement perspective WECC is concerned that the proposed categorization of BES Cyber Assets does not resolve ambiguity in previous CIP-002 versions, and does not address directives issued by FERC in Order 706. More importantly, however, WECC is concerned that proposed categorization will not serve BES reliability. In Enforcement’s experience with CIP-002 Versions 1, 2, and 3, entity identification of BES impacts has been a significant hurdle that entities fail to clear. Given the current uncertainty regarding the definition of “BES”, many entities have had difficulty identifying BES facilities that impact BES operations. The proposed Standard not only requires that entities identify impacts of individual cyber assets, but also qualifies BES Cyber Asset impacts as those that result in an impact to BES Reliability Operations within 15 minutes. This added criterion creates more ambiguity and does not provide clarification mandated by the Commission in Order 706. Based on Enforcement’s experience with the CIP reliability Standards currently in effect, there is no evidence that “categorization” will facilitate Cyber Security implementation. Presently, effective

Reliability Standards categorize Cyber Assets into three groups: Critical Cyber Assets, Cyber Assets in an ESP, and ACM devices. And, similar to proposed CIP-002-5 R1, current versions of CIP Reliability Standards assign a specific set of compliance obligations for each of these categories. In many cases, however, Entities have opted to afford the same protections to all three categories of Cyber Assets rather than develop separate compliance crosswalks for each category of Cyber Assets. In cases where entities have opted to treat each category of asset separately, Enforcement has observed increased instances of noncompliance, and less effective mitigation. Categorization appears to lead to inconsistent implementation of Security Standards. Even with a single CIP compliance manager, segregation of Cyber Assets tends to lead to a lack of coordination between business groups within the same organization. Consequently, it is difficult to detect and effectively mitigate violations that may implicate multiple categories of cyber assets. Mitigation of a CIP-006-1 R1 violation for Critical Cyber Assets, will not extend to ACM Cyber Assets under CIP-006-1 R1.8. WECC recommends that an entity identify Cyber Assets based on “use” or “operation” rather than ownership. A Cyber Asset owned by one entity, may be used by another. Consequently, if only the “owner” is required to assess that cyber asset’s impact, the owner will determine that it is not essential to its BES Reliability Operations. Further, the “owner” of a cyber asset may have physical access to the device, but the same “owner” may not have logical access to a device that is logically sited within another entity’s network. Consequently the “owner” will be unable to implement logical protections required under CIP-005, CIP-007, and CIP-010. If categorization of BES Cyber Assets is preserved, WECC recommends that the Requirement also require identification of “lower” or other BES Cyber Assets as some CIP Reliability Standards contained in proposed Version 5 apply to all BES Cyber Assets including those identified as “lower risk.” The first sentence in 2.7 may be ambiguous due to the Boolean property of the word "and": A clarification is requested to ensure proper understanding of this criterion. Is the second phrase, "and where the 'total weighted aggregate value' of all BES Transmission Lines at a single station or substation operated at 200 KV or higher connected to other transmission stations or substations, including incoming and outgoing lines, exceeds a value of 3,000" a qualifier for the first phrase, "Transmission Facilities operating at 200 kV or higher, but at less than 500 kV, at a single station or substation that is connected to three or more transmission stations or substations" or is it a standalone criterion. In other words, if the second phrase is a standalone criterion, the phrase "and where the 'total…" should be replaced by the phrase "or where the 'total…" which would retain the original intent of the SDT. On the other hand, if the second phrase was intended as a qualifier for the first phrase, the language should be amended to read "…connected to three or more transmission stations or substations, where the "total weighted aggregate value' of all BES Transmission Lines …" Either change that meets the original intent of the SDT would clarify this criterion and eliminate ambiguity that might later call for an interpretation. This is of particular concern given that there is a push from FERC and congress that more generation be inclusive in the application of cyber security controls. The wording of this measurement has had much debate and there is conflicting understanding on what this actually entails. The SDT has stated that this would be 1500 MW attached to a single DCS (for example). As currently written, this means that a single facility with multiple generation units at 1499 MW or less that are attached to separate DCS' would not reach the category of medium. An aggregation of generation capacity per facility should be considered. From a reliability perspective we suggest that the threshold in the Medium Impact category for generation should be 1,000 MW instead of 1500 MW and 300 kV instead of 500 kV for substations. Although the addition of "within 15 minutes" does lend itself to a "bright-line" criteria, it may be arbitrary in the event that a BES Cyber Asset or BES Cyber System is unavailable, degraded or misused and one or more BES Reliability Operating Service becomes "adversely impacted" at the 16 minute mark or longer. Why is an adverse impact happening within 15 minutes any less important to the BES than one happening in 20 minutes?

No

From an enforcement perspective WECC Recommends that the SDT create two Requirements: one for identification of BES Cyber Assets; the other for categorization of BES Cyber Assets. As written, the proposed standard would result in multiple repeat violations of the same standard. Multiple repeats of a standard tend to suggest a culture of noncompliance. Multiple violations of this requirement, however, may stem from different causes. Thus multiple instances of noncompliance with this Requirement may mischaracterize an entity’s compliance record and have consequences that impact the scope of subsequent audits and compliance investigations. From an enforcement perspective WECC disagrees with limiting an entity’s identification of BES Cyber Assets on “ownership” thereof. To date, there has been a great deal of controversy regarding “ownership” of individual devices. Entity

“use” or “operation” of a Cyber Asset, however, is easier to identify and is consistent with the purpose of CIP-002- requiring entities to identify Cyber Assets that are critical to their BES Operations. Further, to refocus BES Cyber Asset identification to emphasize “use,” responsibility at joint use facilities or jointly owned facilities is immediately identifiable. WECC recommends that the entity that operates or uses a Cyber Asset, is responsible for assessing that asset’s impact to its BES operations, and, if appropriate, identifying the Cyber Asset as a BES Cyber Asset based the role the asset plays in its BES operations. WECC disagrees with the provision that requires entities to categorize and identify BES Cyber Assets that have been “updated” or deployed within 30 days. Consistent with current implementation guidance approved by FERC, WECC recommends that the entity assess and identify BES Cyber Assets before implementation of a change or deployment. Deployment or reconfiguration of a BES Cyber Asset may pose a significant risk to the BES. A thirty day gap will not only delay identification of a BES Cyber Asset, but will also delay implementation of Cyber Security measures prescribed under CIP-003 through CIP-010. WECC strongly disagrees with the provision limiting “updates” to include only those Cyber Assets “that are intended to be in service for 6 months.” Regardless of intent, a device that satisfies the definition of a BES Cyber Asset or BES Cyber System must be identified and protected as such. A BES Cyber Asset connected for one month poses the same risk to the BES during that time as does the BES Cyber Assets connected for more than one year. Further, this language would preclude enforcement of CIP-002-5 R1 in cases where a device initially intended to connect a BES Cyber Asset for less than six months, remains connected, for a period of seven months. Because that entity “intended” a six month period of connectivity would Enforcement be able to Enforce CIP-002-5 R1? WECC recommends that the SDT removes any reference to an entity’s “intent” from proposed CIP-002-5 language. There appears to be a discrepancy between the Low Impact language of R1 "All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification" and the "evidence of categorization" of Low Impact devices in M1. This discrepancy is derived from a strict interpretation of the R1 langauge: the entity must first prepare a comprehensive list of ALL Cyber Assets, then categorize appropriate BES Cyber Assets or BES Cyber Systems as High or Medium Impact according to the criteria in Attachment I, which then takes the BES ROS into account. Anything left over after the analysis process could be assumed as a Low Impact device, but it would still have been discretely identified by virtue of its position on the initial list. A more logical identification process indicates the entities should first identify any applicable BES Reliability Operating Services (ROS - as identified in the Guidelines and Technical Basis section, p. 18) relative to the entity's Registered Function(s), then identify and classify BES Cyber Assets and/or BES Cyber Systems associated with that BES ROS according to the criteria in Attachment I. As a practical matter, it seems that entities will follow the logical process as described above, but that approach does not address the "letter of the law" as stated in R1. The term “adversely impact” is not clearly defined. Please clairfy – is each cyber asset categorized EITHER alone OR as part of a BES system? Since the BES system concept is a major change for V5, more explanation wold be helpful.
No
WECC does not disagree with the requirement for the CIP Senior Manager or delegate approval There are clear definitions of the necessary bookends. However, we are concerned that given the recent NERC CAN on “annual” requirements, a separate definition of annual specific only to CIP-002-5 R2 will create confusion in the industry.
Yes
Yes
Yes
The need for cyber security policies that address the BES Cyber Systems is prudent; however, it appears that the required topics to be addressed may not be holistic and/or fully appreciated without more description. For example, does Personnel Security include Training & Awareness policies? Would an entity know to include policies addressing Monitoring & Logging in the topic System Security? There does not appear to be specific policy requirements to address Application Security, provisioning, forensics or cryptography & encryption.
Yes
We agree with the proposed requirement. However, as noted in question 4, given the recent NERC

CAN on “annual” requirements, does this create a separate definition of annual for this requirement? If so, this may create confusion in the industry.

No

Individuals with access to BES Cyber Systems AND BES Cyber Assets should be made aware of elements of its cyber security policies appropriate for their job function AND degree of access. Additionally, The Requirement is unclear for the following reasons: 1. Rationale – R4 states: “The intent of the SDT is to ensure that the responsible entity takes sufficient measures to make its cyber security policy available and accessible to personnel. It is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.” However, the Requirement states: “… shall make individuals who have access to BES Cyber Systems …” It is unclear from the language of CIP-003-5 R4 whether then responsible entity must make some, most, or all individuals with access to BES Cyber Systems aware. 2. “… access to BES Cyber Systems …” will lead to confusion. Which type of access? To solve the above two concerns, R4 language should be “Each Responsible Entity shall make all individuals who have authorized cyber or authorized unescorted physical access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.”

No

M5 refers to documents, signed by the CIP Senior Manager, as possible measurements but not required documents. Documents, signed by an authorized person, should be required in R5 as follows: “The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, approved (via signature), and shall specify the authority that is being delegated.”

Yes

Yes

Yes

WECC agrees with the apparent intent of the requirement. However, there is potential for registered entities confusion based on the current wording of this requirement. The rational states that the requirement "Ensures that personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems maintain awareness of best security practices." yet neither the R1 requirement language nor the R1.1 table requirement make mention of this expectation. Furthermore, the change rationale for R1.1 states that such language was removed from the requirement. It would seem that if the expectation is to ensure that personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems were aware of best practices then this would be explicitly stated in the requirement section. Additionally, if awareness is provided only to personnel with authorized electronic access and/or authorized unescorted physical access, it could still be possible for personnel without appropriate awareness doing unrelated work on systems in other networks such as the enterprise network to infect systems in those networks, that might then be used to stage attacks against electronic security perimeters protecting BES cyber systems.

Yes

Yes

WECC agrees with the intent of R4. However, there are several concerns that could be addressed through modification of R4. Without requiring verification of credentials, eg. Government issued photo ID, how is the utility able to trust an employee's identity? It only states criminal record check and not other checks, such as random drug and alcohol testing. When people are drugged and/or intoxicated with alcohol, they may do things unknowingly, such as disclosing confidential information, losing confidential documentation and critical systems, and/or making improper judgments when running BES systems. Furthermore, drug and alcohol testing is reasonably commonplace in other industries

and reasonable for both cyber security and safety. The criminal check record is private confidential information and this needs to be stored securely. It may be difficult to find contractors or vendors who have performed all the criteria listed in R4 (Personnel Risk Assessment Program). Contractors may not have 7 year history of criminal record, and also, in many cases, these contractors and/or vendors, have been working for them for many years. What if the utility cannot get all that info? What if the utility finds something from the criminal record of the contractor that has been with them for several years? In these cases, what should the utility do? Additionally, must vendors be authorized to provide criminal background check information to the utility for their employees, which would require this permission from the employee? Or can the vendor assert to the utility that it has obtained and verified this information in accordance with the CIP Standards? Current practice is to have the vendor and/or contractor attest to the fact that background checks (in accordance to the requirement) have been completed. Leveraging the TWIC program or creating a similar program specific to the electric sector would lead to a consistent approach to 3rd party background screening and potentially reduce industry work effort on this activity. Extended leave situations - such as a sabbatical, employee behavior/performance suspensions or maternal/paternal leave - are not identified as a reason for revoking or suspending access. Given the criticality of the environment being protected, reducing the privileges to only those who have a need for access as a part of current job duties should be maintained. These specific role changes perhaps could follow the requirements for transferred or reassigned personnel; however, it should be made clear in the requirement or Guidelines and Technical Basis section how to manage these common personnel situations. In the Guidelines and Technical Basis, there is a table that identifies that no action is required for death. WECC disagrees that no action should be taken. Revocation of access privileges for the deceased is an important action. Dormant accounts with privileges could be misused. By removing such privileges, the entity is reducing their overall attack surface as well.
Yes
No
WECC does not disagree with the purpose of the proposed Requirement. However, as noted in response to other questions WECC is concerned that given recent NERC CAN on “annual” requirements, a separate definition of annual specific only to CIP-002-5 R2 will create confusion in the industry. WECC also is concerned that escalating all access requests to the CIP Senior manager will not ensure reliability. The CIP senior manager may not be in a position to determine if the access rights granted are proportionate to an individual’s job function. Further, WECC Enforcement has observed that when asset owners are unable to remove access rights themselves, individuals maintain access rights beyond the point in time access to BES Cyber Assets is needed. Additionally, Part 6.1 doesn’t explicitly say “access to BES Cyber Systems” like it does in 6.2. Part 6.1 should be revised to: “The CIP Senior Manager or delegate shall authorize electronic access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.”
Yes
Yes
No
Part 1.5 states that the entity needs to establish a documented method for detecting malicious communications at each EAP. There is no additional comments in the Guidelines and Technical Basis section to clarify this requirement; however, the responsible entity could infer expectations from the measures column. Perhaps a better phrasing would be: "At each EAP, the entity shall document and implement methods for detecting and addressing communications that have the characteristics of malicious or unexpected activity." Part 1.5 Measures include intrusion detection systems as a limit, which only alert on a signature firing; however, permit the packet to pass through the EAP. It is suggested to change Measures to be a minimum of intrusion prevention systems. An IPS alerts and denies a packet from passing through the EAP, which caused a signature to fire.
No
Part 2.2 “Requires encryption for all interactive Remote Access sessions to protect the confidentiality and integrity of each interactive Remote Access session.”, but this statement does not address end-

to-end encryption. Sometimes vendors access SCADA systems remotely via a third party remote access service, such as "logmein". Such sites may establish a secure tunnel between the vendor and the remote access service, and then another secure tunnel between the utility and the remote access service. In such a case, the remote access service has access to all the remote access traffic; that is, the encryption between the utility and the vendor is not end-to-end. It does not state anything about "Authenticating based on certificates". There have been a significant number of CAs compromised recently, and recent versions of Firefox trust approximately 50 CAs located at organizations all over the world. Secure authentication is necessary to ensure that encryption is useful. Relying on CAs outside of the US to authenticate remote access to critical national infrastructure is risky. In Part 2.3 there is discrepancy on the usage of multi-factor authentication. It states that for High and Medium Impact BES Cyber Systems, as well as the Associated Protected Cyber Assets “REQUIRES” multi-factor authentication. However, in CIP-007 R5.1, it simply states to “validate credentials before granting electronic access to each BES Cyber System” which does not state the need for multi-factor authentication. Multi-factor authentication needs to be carefully defined. US banks have been required to use two-factor authentication since 2006. While the meaning of the term is clear to security professionals, it has been interpreted in some cases by the banking industry to mean "mother's maiden name plus last 4 of social security number". Without clearly defining what is intended by multi-factor authentication, significantly weaker interpretations may be chosen. Regarding dialup connections to a specific BES Cyber Asset, the guidelines state "... examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use". Dial-back modems are easily defeated as revealed by a simple Google search. Remote enable or power up leaves a window of vulnerability unless combined with other defenses, such as modem BES cyber asset passwords. Policy requiring disabling after use is error prone.
Yes
Yes
Yes
Yes
Yes
No
The requirement states that the entity shall “Disable or restrict access to unnecessary logical network accessible ports”. The “restrict access” option insinuates that access to any unnecessary ports must be restricted at the host and not at an access point to the network to which the host is connected (i.e. firewall). The wording does not explicitly eliminate an entity from assuming that perimeter firewalls restricting ports to an ESP network meets the R1 requirement. The addition of “from any network device, either local or remote to the cyber asset” would clarify the intent to require all networked hosts within an ESP to restrict access from any network device, regardless of location (i.e. end-point protection) to any unnecessary logical port.
No
The Security Patch Management requirements do NOT include any specific maximum timelines for vendor approved and recommended security patches/updates to be implemented. Requirement 2.2 requires a “timeframe” to be defined for a mitigation plan to address the vulnerability but again does not provide any specific timeframes. This type of vague language allows entities to keep delaying the implementation of vendor approved security patches/updates, creating significant risk to the network to which the device is connected, as well as the BES. Unpatched systems can create a situation where malware/Trojans can rapidly spread once any one system has been compromised (dominos or house of cards comes to mind). A requirement to test and implement relevant and approved patches on a regular basis (at least annually) would significantly reduce the exposure and risk to the BES. The requirements are acceptable and auditable except for the lack of required timeframe to address vulnerabilities.

No
The SDT should address the following to facilitate entity implementation: 1. How soon must the malicious code be removed under R3.2? 2. Who is responsible for identifying malicious code, malicious code prevention tool or any other source under R3.2? 3. Can the STD provide examples of “transient cyber assets”? Is the R3.4 referring to laptops, thumb drives, or any other media? 4. Enforcement recommends that R3.5 logging also require the identity of the person or entity connecting and using the transient device.
No
Part 4.2 - Currently CIP-007 version requires immediate notification or alerting. If immediate alerting is not required, please specify an acceptable timeframe in which staff must be alerted.
WECC supports the purpose of the requirement but notes that long passwords are primarily required to defend against offline password attacks. Increasing minimum password length from 6 to 8 characters is inadequate to address offline password cracking attacks, in the face of modern GPUs offering significant hardware parallelism and available on cloud computing services such as Amazon's EC2. Furthermore, without disabling LM hashes on Windows systems, any password of any length is easily cracked. This applies to all Window systems prior to Windows Server 2008.
Yes
Yes
WECC supports CIP-008-5, but suggests that the following questions need to be addressed. What happens if there is a third-party IT company that handles the utility’s cyber security incidents? Who should be doing what and who has the ultimate responsibility? For example, should the IT company handle everything from the beginning to the notification of the incident?
Yes
Yes
Yes
Yes
Yes
No
WECC agrees with the intent of R1, but offers the following improvements. Part 1.1 - This appears to be an asset inventory and not a true configuration baseline requirement. If a configuration baseline is to actually be achieved for the sake of assuring that the BES Cyber Asset can be monitoring for changes then this requirement should also include a system level baseline configuration action that can be achieved using tools like Tripwire. Of course, that would be where technically feasible. It is also noted that other than security patch level and available network ports there is no specific requirement to document the security controls. Although, it could be inferred that would be required as part of 1.1.3 and 1.1.4. Part 1.2 - Part 1.2 requires authorization of changes by the CIP Senior Manager or delegate but does not specify when. Unfortunately, some applicable entities may take this to the extreme, authorizing the change months after it occurs. Recommend Part 1.2 Requirement read: “Authorization prior to the change, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.”
No
WECC agrees with the purpose of CIP-010-1, but from an enforcement perspective, WECC recommends that in addition to R2.1, the SDT revise the requirement to require entities to document and implement an action plan to address current unauthorized changes and prevent unauthorized changes going forward. Part 2.1 – Similar to our comments above, we offer the following for Part 2.1.

Part 2.1 requires monitoring, documenting, and investigating the detection of any unauthorized changes but does not say when. Unfortunately, some applicable entities may take this to the extreme, documenting and investigating the change months after it occurs. Recommend Part 2.1 Requirement to read: “Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1). Document and investigate the detection of any unauthorized changes within thirty (30) calendar days.” Suggest adding protections to the process for modifying cyber assets, in addition to monitoring for unexpected changes.
No
Impacts cannot be prescribed by the Standards, but must be assessed and determined by Enforcement pursuant to FERC Order 672. In some instances a “medium impact” or “minimal” impact may be appropriate. Regional enforcement staff does not have the authority to disregard FERC mandates that require it to assess impacts of noncompliance based on facts and circumstances of each case. WECC agrees with the language of Requirement R3, but offers the following improvements to Table R3 – Vulnerability Assessments. Part 3.1, Requirements, requires a paper or active vulnerability assessment but does not adequately define what is required in the assessment. WECC recognizes FERC Order 706 paragraph 644, which leaves details to guidance. However, some applicable entities may take this to the extreme by doing very little in the assessment. Recommend the language be “Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed. The assessment must include, at a minimum, all of the following: 3.1.1: Enumeration (by name and cyber address) of all Cyber Assets of each BES Cyber System. 3.1.2: Enumeration of all enabled software ports and associated services for all Cyber Assets of each BES Cyber System. 3.1.3: Statement of which software ports and associated services of all Cyber Assets of each BES Cyber System are and are not required for normal and emergency operation. 3.1.4: Enumeration of community strings of all Cyber Assets of each BES Cyber System.” Part 3.2, Requirements, requires an active vulnerability assessment but does not adequately define what must be required in the assessment. WECC recognizes FERC Order 706 paragraph 644, which leaves details to guidance. However, some applicable entities may take this to the extreme by doing very little in the assessment. Recommend the language be “Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. The assessment shall include all elements defined in CIP-010 R3, Part 3.1.1 through 3.1.4. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.” Part 3.3, Requirements, requires an active vulnerability assessment but does not adequately define what must be required in the assessment. WECC recognizes FERC Order 706 paragraph 644, which leaves details to guidance. However, some applicable entities may take this to the extreme by doing very little in the assessment. Recommend the language be “Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset. The assessment shall include all elements defined in CIP-010 R3, Part 3.1.1 through 3.1.4.” Part 3.4, Requirements, requires an action plan with planned date of completion but does not actually require completion. Furthermore, it doesn’t set a time limit to complete the action plan. Unfortunately, some applicable entities may take this to the extreme by setting the planned date of completion to an unreasonable date or not actually completing the plan by a reasonable date. Recommend the language be “Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. The action plan shall be completed no later than ninety (90) calendar days from the date of the assessment. Certain vulnerabilities identified in the assessment do not have to be remediated or mitigated if a subject matter expert determines the action will degrade availability, integrity, or confidentiality to an unacceptable level. In such cases, the responsible entity shall document why vulnerabilities were not remediated or mitigated within ninety (90) calendar days.” Without this type of clarity how are the auditors supposed to audit this requirement?. Without defined timeframe criteria the entity can keep rolling the same vulnerabilities from one year to the next without addressing the vulnerability. To effectively audit this requirement the auditors need timeframes. General - Vulnerability analysis looks for any weaknesses - it is more

than an audit of implementation against design.
Yes
No
WECC agrees with the language of Requirement R1 and CIP-011-1 Table R1 – Information Protection, Parts 1.1 and 1.2. However, we suggest the following for Part 1.3. Part 1.3, Requirements, requires an action plan but does not set a time limit for the date of completion. Unfortunately, some applicable entities may take this to the extreme by not implementing the action plan by a reasonable date. Recommend that the language to be "Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. The action plan shall be implemented within ninety (90) calendar days from the date of assessment."
No
WECC agrees with the language of Requirement R2 but not with CIP-011-1 Table R2 – Media Reuse and Disposal. The phrase "release for reuse" in Part 2.1 (Requirements) will lead to confusion and inconsistencies among entities. Furthermore, the language of Part 2.1 (Measures) and Part 2.2 (Measures) allows but does not require an applicable entity to generate and maintain records, without which applicable entity management and auditors will not be able to assess the performance of the requirements. Furthermore, the two Parts could be reduced to one with the following: "Prior to the physical removal of BES Cyber Asset media from a Defined Physical Boundary, the Responsible Entity shall implement a 7-pass media overwrite, degauss, or physically destroy BES Cyber Asset media. Each instance shall be documented within thirty (30) calendar days of occurrence."
Yes
WECC recognizes the issues related to the implementation of Versions 4 and 5 of the CIP standards and urges NERC to work towards a resolution that provide reliability to the BES while not forcing registered entities to undertake unnecessary expense and effort.
Individual
Don Jones
Texas Reliability Entity
No
No
In R1, we disagree with the statement that Low Impact BES Cyber Assets/Systems "do not require discrete identification." By definition, all BES Cyber Assets/Systems have the ability to impact BES Reliability Operating Services in a short period of time, including Low Impact BES Cyber Assets/Systems. There are relatively few Requirements that apply to Low Impact BES Cyber Assets/Systems, but in order to ensure compliance (and to audit compliance) with those requirements it will be necessary for those assets and systems to be identified by the applicable entity. What are the "required controls" referred to in M1?
Yes
Yes
Yes
Yes
No

In R4, we feel that if cyber security policy awareness is implemented through periodic training, there should be a periodicity requirement (e.g., annual).
Yes
Yes
No
In Part 1.1, it is not clear what “security awareness concepts” are intended to be included in the program. We suggest listing some concepts that should be included to provide a standard against which the program can be assessed.
No
In Part 2.1, consider requiring the role definitions to be reviewed on an annual basis. We are concerned that these definitions will become neglected and stale if there is no requirement to revisit them periodically.
No
In Part 3.2, we suggest modifying the requirement to read: “Require completion and documentation of the training specified . . ..”
Yes
Yes
No
In Parts 6.1 and 6.2, the Measure should not allow only a “sampling of accounts” regarding people with electronic access or automated physical access to BES Cyber Assets/Systems. The entity should maintain a complete register of this information, even though an auditor may only want to review a sample.
Yes
No
In Part 1.1, if there is no requirement for an entity to discretely identify Low Impact Cyber Systems, there is not any basis from which to determine what assets and systems this requirement applies to, or to audit this requirement. We believe that all BES Cyber Assets/Systems should be discretely identified in order to ensure that they are designed and operated in compliance with applicable requirements, and to facilitate assessment of compliance. In Part 1.4, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement. Part 1.5 should say “Detecting and recording malicious communications at each EAP.” The focus of this requirement should be on detecting and recording malicious communications, not on producing a “documented method.”
Yes
No
In part 1.3, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement.
Yes

No
In part 3.1, consider reducing the testing and maintenance interval to 12 months. (What is the basis for 24 month interval?)
Yes
Yes
Yes
No
In Part 4.4, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement.
No
In part 5.3, we suggest adding a requirement to annually review the individuals who have access to shared accounts, to ensure that access authorizations are periodically reviewed and updated. In Part 5.4, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement. In Part 5.5.3, the required password change periodicity should be specified as at least annually. The entity should not be allowed to specify a time frame longer than 12 months. In Part 5.6, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement.
Yes
Yes
Yes
No
In Part 1.5, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement.
Yes
No
In Part 3.3, the requirement should refer to Part 3.1 as well as Part 3.2 (regarding updating the recovery plan based on deficiencies or lessons learned).
No
In Part 1.1, consider adding that the “baseline configuration” includes any databases (including

version information) that support or interact with BES Cyber Assets/Systems.
No
In Part 2.1, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement.
No
In part 3.1, we feel that there should be some specification of a minimum set of security controls that must be implemented and tested, to provide a basis for assessment of compliance with this requirement. In Part 3.2, we feel that the 36-month interval between vulnerability assessments is too long and presents a reliability gap. Vulnerability assessments should be conducted annually on High Impact systems. Also, vulnerability assessments should generally be conducted on the primary or mirrored backup BES Cyber Systems, not on “test systems.”
Yes
Yes
Individual
Roger Fradenburgh
Network & Security Technologies Inc
Yes
Definition of “CIP Exceptional Circumstance” is, perhaps unintentionally, limiting by virtue of its “one or more of the following conditions” language. As written, conditions such as the threat of potential large-scale, cyber-related disruptions of the BES would fall outside of this definition. Suggest rewording using language such as, “Situations that involve actual or potential harm to life, property, or BES operations that require temporary suspension of one or more CIP operating procedures.” Replacement of defined term, “Physical Security Perimeter” with new term, “Defined Physical Boundary” will compel many Entities to undertake an extensive, time-consuming and, in our opinion, pointless project to replace all instances of the current term with the new one in policy and procedure documents, drawings, training material, etc. “Physical Security Perimeter” with new term, “Defined Physical Boundary” Rather than replace “Physical Security Perimeter,” the SDT should consider amending the current definition in a manner similar to how it has amended the term, “Electronic Security Perimeter.” Recommend revising definition of “Transient Cyber Asset” as follows: - Clarify what is meant by “directly connected.” Absent such clarification, there will be arguments about what it means. - Consider deleting third characteristic (“capable of altering the configuration of or introducing malicious code to the BES Cyber System”). It makes a “Transient Cyber Asset” sound like something to be feared and avoided if possible. We note that ANY cyber asset has the potential capability of changing a BES Cyber System’s configuration and/or of introducing malicious code to it. Change definition of “Electronic Access Point.” As written (“An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets”) the definition can be interpreted to mean an EAP’s function is to limit or hinder data communications. Recommend modifying to indicate an EAP’s function is to restrict routable or dial-up data communications to only those that are required for normal or emergency operations. “BES Cyber Asset:” Recommend deleting the second sentence (“This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services.”). It is confusing and seems to contradict the first sentence (“A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services.”). “Electronic Access Point:” Proposed definition (“An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets”) has several shortcomings the SDT should address. It is not clear whether or not the “Cyber Asset” can be a BES Cyber Asset or part of a BES Cyber System. CIP-

005-5 provides no help here, as it does not specify whether or not BES Cyber Assets and BES Cyber Systems must be within an Electronic Security Perimeter. The definition does not say what restrictions an EAP should place on dial-up or data communications, nor does it specify what “between Cyber Assets” means. We recommend the SDT consider basing its definition on the language in CIP-005-3 R1.1. We also recommend an explicit requirement that Medium and High BES Cyber Assets and Systems must reside within an ESP.
Yes
We believe that this new version of CIP-002 should include an analog of criterion 1.10 from CIP-002-4 Attachment 1 (Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.).
No
That the CIP Senior Manager must have “the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards” should be in the R1 requirement statement, not just the accompanying “Rationale” statement.
No
The policy topic list includes items an Entity with only Low Impact systems would (or should) not be required to have (e.g., Incident Response and Recovery plans). This should be corrected. In the mapping document, the SDT states security policy exceptions have been dropped from CIP-003 requirements because “The FERC Order 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the Standards.” This is incorrect. In paragraphs 376 and 377 (among others) FERC states that policy exceptions may not be used to except responsible entities from compliance with CIP Standard requirements, but the Order does not state policy exceptions are unallowable.
Yes
No
Four of the five of the “Evidence” examples in M4 would NOT demonstrate compliance with R4’s requirement that the Entity “make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.” Should either change R4 using words conveying that policies must be made available to such individuals –or– change the “Evidence” list to examples that would actually demonstrate compliance.
No
Suggest dropping the 1st sentence, “The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards.” It conflicts with the 2nd, which states he or she may delegate much of the required authority for approvals and authorizations. What is meant by the statement, “The authority for subsequent delegations may also be delegated?” “Subsequent” means “coming after (something) in time,” or “later” and doesn’t seem to fit here. Is it the SDT’s intention that delegates appointed by the CIP Senior Manager may also delegate some the authority they have been granted, and that such “2nd tier” delegates may themselves delegate some of THEIR authority to “3rd tier” delegates, and so on? If so, this statement needs to be reworded to make that clear.
Yes
Yes
No
R2 and its included requirements should also be applicable to Associated Physical Access Control

Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets.
Yes
No
R4.2: We believe the requirement to perform a criminal check for any and all places of residence for the previous seven years has the potential to add considerable time and expense to the PRA process with little or no incremental benefit as compared to the existing Standard's seven-year criminal check requirement. We recommend dropping the "per place of residence" condition.
No
Grant of interactive remote access to Med and High BES Cyber Systems should be an explicit requirement. How can there be an explicit requirement in R7 to revoke this access if there is no corresponding requirement to authorize it?
No
R7.1: The SDT should clarify whether "at the time of the resignation or termination" means at the time the action is announced or at the time it becomes effective. R7.2: Suggested changing to, "For reassignments or transfers, revoke any and all unnecessary electronic and/or physical access to BES Cyber Systems within 30 calendar days of the date access is no longer needed." R7.3: The SDT should clarify whether the time limit (end of next calendar day) is meant to be tied to the date the resignation or termination action is announced or at the date it becomes effective. R7.5 The SDT should clarify whether the time limit (within 30 calendar days) is meant to be tied to the date the termination, resignation, reassignment, or transfer is announced or the date it becomes effective.
No
It is our understanding that SDT goals included making each Version 5 CIP Standard as "standalone" as possible. That being the case, we believe monitoring and logging requirements for Electronic Security Perimeters should continue to be addressed in CIP-005-5. When we first read the current proposed draft, we thought they were simply missing. R1.1: The word, "restrict" in, "Define technical or procedural controls to restrict unauthorized electronic access" is inappropriate, as it can be interpreted to mean, "put a limit on" or "hinder" where the presumed intention of the SDT is to prevent unauthorized access. Suggest replacing "restrict" with "prevent." Also suggest replacing "Define technical or procedural controls" with "Define and implement technical AND/OR procedural controls…" R1.1: The Application Guideline notes for Requirement R1 state that Entities should have "perimeter type security controls" that "segment low impact BES Cyber Systems from public or other less trusted network zones." However, since neither the Requirement statement nor the Measures statement contains such language, we believe there is a risk some Entities will feel they is no regulatory obligation to implement "perimeter type security controls" for low impact systems. The SDT should address this. R1.2: What is required for compliance with this requirement cannot, in our opinion, be clearly stated given the current definition of EAP. R1.2: It is not clear what's required for High and Medium systems that have neither external routable or dial-up connectivity. Recommend the SDT address this. R1.2: The phrase, "all routable" in the requirement statement, "Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs)," is overly broad. Suppose two BES Cyber Systems (or two or more BES Cyber Assets) at a single facility (e.g. a transmission substation) communicate with each other using routable protocols but do not communicate with any "off-site" systems using routable protocols. What is the Entity required to do under that condition? Recommend the SDT address this. R1.5: We believe the requirement ("A documented method for detecting malicious communications at each EAP") is overly prescriptive and that the requirement should be written in a manner that allows the Entity to decide how to address Order 706's directive that Entities must use "two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter." (p 496). The use of and IDS or of similar measures could be suggested in the guidance section of the Standard.
No
Suggest changing, "Interactive Remote Access" to "Interactive Remote Access using routable or dial-up connectivity"

No
R1.1's requirement statement, "Define operational or procedural controls to restrict physical access" begs the question, "Restrict physical access to what or to whom?" Also, as noted for CIP-005-5 R1.1, we presume the SDT's intention is to require Entities to prevent unauthorized physical access. Suggest replacing with "Define and implement technical and/or procedural controls to prevent unauthorized physical access." NOTE: Use of "restrict" in R1.2, "Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized" is okay, as the sentence includes information about what "restrict" is applied to ("to individuals that are authorized"). R1.2 and R1.3: Replace "restricts" with "restrict." R1.2 and R1.3: We note the Measures for these two requirements state that acceptable evidence includes descriptions of how both ingress and egress is controlled. However the requirements are, we believe, likely to be interpreted as requiring only that ingress be controlled. The SDT should resolve this apparent conflict. R1.6: Requirement should be to record time and date of entry, not just date (as in current CIP-006-3). In the "Guidelines and Technical Basis" section for R1, we believe the assertion that "two-factor authentication could be implemented using a single Physical Access Control System" violates the spirit, if not the letter, of FERC Order 706 p572. FERC Order 706 p562 states, "(the CIP NOPR) stated that use of a minimum of two different security procedures would, for example, enable continuous security protection when one of the security protection measures is undergoing maintenance and provides redundant security protection in the event that one of the measures is breached." Both "factors" in a two-factor authentication system that used a single Physical Access Control System would be rendered inoperable if the control system itself was inoperable.
No
R1.1: Should apply to all Medium Impact Systems R1.1: Change, "Disable or restrict access,…" to "Disable or prevent access,…" R1.2: Change, "Disable or restrict the use of,…" to "Disable or prevent the use of,…"
No
R2.2: Wording ("Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe") is very hard to follow. Suggest changing to: "Identify applicable security-related patches or updates within 30 days of their release from an identified source. Within that same 30 day period, create or revise an existing plan either to install the patch or update, or to otherwise remediate the vulnerability(ies) addressed by the patch or update. The plan shall include a defined time frame for its implementation." R2.3: We assume the requirement ("A process for remediation, including any exceptions for CIP Exceptional Circumstances") is meant to instruct Responsible Entities to implement the patch installation or remediation plan(s) required under R2.2. If this is true, R2.3 should so state in plain terms.
No
There should be a requirement, as there is in the current version of CIP-007, to test anti-malware signature or pattern update files prior to implementation. We note that in the "Application Guidelines" section, the SDT makes it clear this is their intent; however unless it is part of an "R" statement it will not be mandatory. R3.2: Should be subject to technical feasibility R3.5: As written ("Log each Transient Cyber Asset connection") the requirement may cause confusion as to what is meant by "each connection." The SDT should clarify whether it means each time a Transient Cyber Asset is physically or wirelessly connected to a BES Cyber Asset or to a subnetwork shared by BES Cyber Assets or each time a Transient Cyber Asset initiates a new logical connection (e.g., TCP) to a BES Cyber Asset.
No
R4.2 and 4.3 should apply to all Medium Impact BES Cyber Systems, not just those with external routable connectivity. R4.3: The SDT should clarify whether this requirement is meant to apply to individual BES Cyber Assets, to Cyber Assets that collect and analyze logs from many other Cyber

Assets, or both. R4.3: As written ("Detect and activate a response to event logging failures before the end of the next calendar day."), requirement would allow an event logging failure to last for nearly 48 hours (12:02 AM Tuesday to 11:59 PM Wednesday, for example). Suggest changing this to something more stringent, such as "24 hours or less."
No
R5.6: Suggest rewording as follows: "A process to limit, where technically feasible, the number of unsuccessful authentication attempts or to generate alerts after a predefined threshold of unsuccessful login attempts has bee reached."
No
Should apply only to Medium and High Impact systems, along with any "associated" BES Cyber Systems plus associated electronic and/or physical access control and/or monitoring systems. Why should a Responsible Entity with only Low Impact BES Cyber Systems be expected to define, implement, review, and test a Cyber Security Incident response plan when there are no corresponding requirements for monitoring, alerting, logging, etc. There's not even a requirement to maintain an inventory of "Low Impact" systems.
No
Should apply only to Medium and High Impact systems, along with any "associated" BES Cyber Systems plus associated electronic and/or physical access control and/or monitoring systems (as per our comments for R1, above). R2.1: Suggest rewording as follows: "When a BES Cyber Security Incident occurs, the incident response plans must be followed. Any deviations taken from the plan during the response must be recorded."
No
Should apply only to Medium and High Impact systems, along with any "associated" BES Cyber Systems plus associated electronic and/or physical access control and/or monitoring systems (as per our comments for R1, above). R3.3: Recommend time limit on updates be changed from 60 to 30 days for consistency with R3.4. R3.5: We can think of no reasonable justification for allowing up to 30 days to provide response team members with already completed response plan updates. Recommend the allowed time be shortened to five (5) days.
No
R1.5: Preservation of what FERC Order 706 refers to as "forensic data" should by all means be subject to "if possible" conditions but should NOT be subject to "technical feasibility." As written, it could compel an Entity whose control center burned to the ground to file a TFE. Suggest revising the requirement to preserve data for post-recovery analysis or to document why it was not possible to do so.
No
R2.1 and R2.3 are in conflict regarding what must be done on the effective date of the Standards: R2.1 directs Entities to "implement" recovery plans upon the effective date of the Standard by recovering from an actual incident, or with a paper drill or tabletop exercise, or with a full operational exercise. R2.3 directs Entities to "test" recovery plans upon the effective date of the Standard through an operational exercise or an actual recovery response. The SDT should decide whether Entities should have the option of performing a tabletop exercise to implement/test their plans upon the effective date of the Standard and revise either R2.1 or R2.3 accordingly.
No
R3.1: Recommend removing "when BES Cyber Systems are replaced" as a condition requiring review of recovery plan(s). This condition is covered by R3.4. R3.3: Updating of recovery plan(s) should be triggered by any findings of deficiencies resulting from R3.1 plan reviews in addition to any findings of deficiencies or lessons learned from R3.2 test result reviews. R3.5: We can think of no reasonable justification for allowing up to 30 days to provide response team members with already completed recovery plan updates. Recommend the allowed time be shortened to five (5) days.
No
It is our view that R1.4, as written, represents a considerable weakening of existing CIP-007 R1

("Test Procedures"), which is generally interpreted to mean changes to the baseline configurations of Critical Cyber Assets should be tested prior to implementation, using production systems if necessary. We recommend modifying R1.4 to require an explicit test of a change's impact on security controls on one or more "test systems" that may, if no other option exists, be "production" systems. The "verification" step that follows implementation of the change on all systems to which the change is applied should in fact be performed on all of those systems.

Group

ACES Power Marketing Member Collaborators

Jason Marshall

Yes

The first two sentences in the definition of "BES Cyber Asset" are difficult to interpret. After considerable discussion among our staff, our understanding is as follows: the definition makes the distinction between when an asset is "rendered unavailable, degraded, or misused" and its actual "operation, mis-operation, or non-operation" under such conditions. If the asset impacts the BES "within 15 minutes" of its actual "operation, mis-operation, or non-operation," then it is a "BES Cyber Asset," regardless of how long since it was "rendered unavailable, degraded, or misused." We recommend editing this definition for clarity as it took a number of our staff numerous reads and discussion to arrive at this understanding that we are still not sure is what the drafting team intended. The distinction should be clarified. Also, we question the necessity of such a distinction and whether the value it adds is worth the confusion it produces. Additionally, it is unclear whether the "timeframe" referred to in sentence three applies to the "within 15 minutes" timeframe or the "regardless of the delay" timeframe. How does the responsible entity know if a BES Cyber Security Incident was malicious? Understanding if an act was malicious implies an understanding of intent. We do not believe that intent is something that can always be quickly and easily understood. Consider the recent case of the failure of the water pump at a Springfield, Illinois water utility that was initially attributed to hacking because it was accessed from a Russian IP address. It turned out it was accessed by a contractor on vacation in Russia at the request of the utility. Obviously, this example demonstrates intent takes time to determine. The Project 2009-01 Disturbance and Sabotage Reporting even stated this in their recent posting for the reason they decided not to define sabotage because intent is so difficult to determine. Thus, we recommend striking malicious from the definition. BES Cyber System includes the capitalized term Maintenance Cyber Asset. The capitalization is an indication that the term is defined in the NERC Glossary. Neither can we find such an existing definition nor is it the definition proposed in this standards project. Either the capitalization needs to be removed or the term needs to be defined. We recommend the latter. BES Reliability Operating Services should not be a NERC defined term. Many of these services are similar to the Policy 10 – Interconnected Operating Services that was never passed because industry could not agree on it. It is doubtful industry is going to agree on this broad definition that could apply outside the CIP standards. Furthermore, there are several issues with the definition. First, it is not clear what is intended by including contingency reserve in parentheses after spinning reserve. Contingency reserve can include spinning and non-spinning components as long as it can respond in 15 minutes to meet DCS. Spinning reserve does not necessarily relate to contingency reserve directly in that it can include unloaded on-line reserves that respond in more than 15 minutes. Furthermore, NERC has two conflicting definitions of spinning reserve: Spinning Reserve and Operating Reserve – Spinning. One definition limits the spinning reserve to what can respond in 15 minutes and the other does not. Second, it is not clear what is intended by including contingency reserve in parentheses after non-spinning reserve. Per NERC definition, non-spinning reserve is time limited but not necessarily limited to the 15 minute limit set in DCS and, thus, on contingency reserves. Thus, while some contingency reserves may be non-spinning, not all non-spinning reserves will be contingency reserves. Third, under the Managing Constraints section of the BES Reliability Operating Services definition, ATC is

identified. It should be removed. ATC is not used to manage constraints but rather to sell transmission service. That transmission service may never be used. While ATC is calculated using reliability components, it is not a reliability service but a commercial service. FERC even acknowledged that the MOD (ATC) standards were designed primarily "to ensure non-discriminatory allocation of transmission capacity among transmission market participants" in paragraph 30 of the order approving FAC-013-2 (137 FERC ¶ 61,131 Docket No. RD11-3-000). Fourth, the Inter-Entity Real-Time Coordination and Communication section of the BES Reliability Operating Services definition should be struck as it is just a supporting activity for all the other services. CIP Exceptional Circumstance should be modified to include a clause that other circumstances of similar nature and/or impact could be included as a CIP Exceptional Circumstance. Otherwise responsible entities could be put in a position of having to choose to violate some the CIP requirements because the SDT did not think of a particular exceptional circumstance that should have been included. CIP Senior Manager should be struck along with all references to CIP Senior Manager in the CIP standards. This definition and associated requirements dictate a corporate governance structure for no apparent reliability reason. A responsible entity should be free to have two, three, or more personnel oversee various portions of the CIP program. The responsible entity will still be required to meeting the CIP requirements regardless. Furthermore, mandating a single CIP Senior Manager implies that potential for sanctions up to $1,000,000 per day per violation are not enough to get senior management's attention. This implication is totally contrary to the purpose of making standards enforceable by such sanctions. No other standards require identification of single senior manager and no reliability justification has ever been provided for why one is needed for the CIP standards. It is not clear that Control Center needs to be defined. EOP-008-1 (Loss of Control Center Functionality) was written without defining control center. We are concerned that this definition could cause confusion with EOP-008-1 and believe the definition needs to be coordinated with that standard. Reconvening the SDT that worked on EOP-008-1 may be necessary to accomplish this. For Interactive Remote Access, how do Cyber Assets used by the Responsible Entity differ from those used by employees? It is not clear why Responsible Entity is delineated in such a way. Reportable BES Cyber Security Incident needs to be coordinated with the Disturbance and Sabotage Reporting standards drafting team.

Yes

In the Background section, the SDT describes that the responsible entity will have a choice to evaluate BES Cyber Assets individually or collectively in a BES Cyber System. The opening paragraphs for High Impact or Medium Impact criteria need to be modified to make this clear. As written they do appear to provide a choice by stating "Each BES Cyber Asset or BES Cyber System". However, it does not make clear whose choice that is. The auditor might decide the choice belongs to them. Thus, these paragraphs need to be modified to make clear the choice belongs to the responsible entity. While similar and conforming changes need to be made to the Low Impact Rating as well, one additional change needs to be made. "All other BES Cyber Assets and BES Cyber Systems" should be changed to "All other BES Cyber Assets or BES Cyber Systems". Otherwise, there is no choice because both have to be included. This change would also conform Low Impact Rating to the Medium and High Impact Rating sections. While there are limitations on the TOP Control Centers such that not all TOP Control Centers will be included with a High Impact, there is no such limitation on the BA Control Centers. We recommend a similar limitation be place on a BA Control Center such that if the BA is not controlling assets that meet certain criteria in the Medium Impact they should not be included. There many small BAs that simply won't have a broad impact on the Interconnection and, thus, should not be included. Transmission Owner should be struck from Criterion 1.3. The Criterion states that it applies to Control Centers that are use to perform the functional obligations of the Transmission Owner and Transmission Operator. Per version 5 of NERC Functional Model, there are no functional obligations of a Transmission Owner that would be performed at a Control Center. Including Transmission Owner appears to be an attempt to address concerns regarding some RTO/ISO's Transmission Operator registration models that have been expressed in various forums by regulators. These concerns should not be addressed here in piecemeal fashion but holistically in a forum covering all concerns and issues with the registration model. If the drafting team chooses not to strike Transmission Owner, we suggest splitting out Criterion 1.3 into two Criteria for clarity: one criterion for the Transmission Owner and one for the Transmission Operator. As Criterion 1.3 is written now, it could be interpreted as though the control of assets identified in criteria 2.2 and 2.5 – 2.12 only applies to the Transmission Owner. We believe the drafting team intended to apply these criteria limitations to the Transmission Operator as well. If indeed that is the intention, splitting them out would clarify the intent. Criterion 1.4 which obligates certain GOP control centers to be rated High

Impact includes criterion 2.12 as one of those reasons. 2.12 should be struck as it deals with UVLS and UFLS which are not GOP functions. We request that the drafting team clarify Attachment I or the associated requirements that BES Cyber Assets and BES Cyber Systems are not intended to be classified at more than one impact level even if they meet a criterion in multiple impact levels. We further ask the drafting team to clarify that the BES Cyber Assets and BES Cyber Systems that are part of a Control Center are not to be evaluated against other non-Control Center criteria. For example, if a GOP Control Center is used to control more than 1500 MW of generation, it would not be evaluated under criterion 2.1 but rather under criteria 1.4 and 2.13. As the criteria are written now, it is possible to interpret that the Control Center's BES Cyber Systems and BES Cyber Assets could qualify as both a Medium Impact under criterion 2.1 and, then, a High Impact under criterion 1.4. Criterion 2.3 creates an implied obligation on the Planning Coordinator (PC) or Transmission Planner (TP) to designate generation that is necessary to avoid BES Adverse Reliability Impacts. It is implied because there are not any requirements in any standard including the TPL standards that require the TP or PC to designate generation necessary to avoid BES Adverse Reliability Impacts. In fact, BES Adverse Reliability Impact is not even used in any requirements that pertain to the PC or TP. The implied obligation creates a compliance conundrum. Since it is only an implied obligation and not an explicit requirement, the PC and TP will never be required to meet it. How then, does the GOP or GO insure they get the information they need from the PC or TP? They have no recourse. Use of BES as a descriptor of Adverse Reliability Impact in Criterion 2.3 is redundant with the definition of Adverse Reliability Impact and should be struck. Criterion 2.3 focuses on the long-term planning horizon which is contrary to the standard. The standard focuses on reliability impacts caused on the BES in a 15 minute timeframe from the misuse, degradation or unavailability of the BES Cyber Asset or BES Cyber System. It does not make sense to subject BES Cyber Assets and/or BES Cyber Systems within a generator plant or GOP control center to these standards if a generator is identified as needed for reliability four years out but is not identified from year 0-3. For Criterion 2.5 regarding Cranking Paths, the last two bullets are confusing and the wording should be clarified. The graphic provided on page 26 in the Application Guidelines help with that clarification and the drafting team should consider adding this as an attachment so that it will remain with the standard. It is premature to base criterion 2.7 on the "Integrated Risk Assessment Approach – Refinement to Severity Risk Index". It is still a work in progress. This document and approach is being developed under the purview of the Planning Committee's (PC) Reliability Metrics Working Group (RMWG). The PC has not approved any of the indexes. The only thing the PC approved was the approach and framework. At the December 2011 PC meeting, it was clear that the RMWG has additional work to do to finalize the indexes. Thus, it is premature to use any of these indexes in the "Integrated Risk Assessment Approach – Refinement to Severity Risk Index" in a standard. At the very least, use of them should be coordinated with the PC and RMWG. Criterion 2.9 is redundant to Criterion 2.8. FACTs devices are Transmission Facilities and are covered in 2.8. Criterion 2.11 presumes that failure of an SPS or RAS would cause an IROL violation. This is not likely. An SPS or RAS may be implemented for a specific contingency for example. As an example, when that contingency happens, certain switching might need to occur or generation run back. These automated actions might enable a higher limit on an IROL associated with a transmission corridor. If the SPS was not available, the limit would likely be lowered but not necessarily violated. A violation would depend on actual system conditions at the time. Thus, the language should probably be change to something along the lines of impacts or enables higher IROL limits. Criterion 2.13 has control centers in lowercase. This would mean that the proposed NERC glossary definition does not apply. Is this the intent? If so, how would this meaning of control center be different?

No

We think Requirement 1 and associated Attachment 1 should focus on identifying the BES Facilities that are important and then the associated BES Cyber Systems and BES Cyber Assets. Otherwise, all BES Cyber System and BES Cyber Assets will have to be inventoried. While the Background section states "Requirement 1 only requires that discrete identification of BES Cyber Systems and BES Cyber Assets for those in High and Medium categories", we do not see how a responsible entity can demonstrate that it has correctly identified all High and Medium Impact BES Cyber Systems and BES Cyber Assets unless it has a complete inventory of all BES Cyber Assets and BES Cyber Systems. We can envision auditors asking for such an inventory. Part 1.1 needs to be further refined regarding what kinds of changes are included. By the NERC Glossary definition, Facility can include relay equipment associated with protecting a transmission line as part of the "set of electrical equipment that operates as a single Bulk Electric System Element". Thus, a change to a relay setting could be

could be inadvertently included. It should not be. We suggest the changes be limited to topological changes, generator interconnections and generator uprates and equipment retirements. While other changes such as permanent derates may allow that responsibility entity to lower the categorization of BES Cyber Systems and/or BES Cyber Assets, the reduction in compliance burden will cause them to do this. Thus, we don't need to increase their compliance burden by requiring them to do it for permanent derates.

No

Because regional entities already expect evidence to be signed and dated by persons of authority, there is no reason to have a specific requirement to have the CIP Senior Manager or delegate do this. The requirement is unneeded and the compliance auditor likely won't accept evidence for Requirement 1 unless it has been approved anyway by a person of authority. Thus, this requirement actually creates a form of double jeopardy that an entity could be held in violation of Requirement R1 and R2 for failure of the CIP Senior Manager or delegate to approve the list of BES Cyber Asset and BES Cyber Systems categories. Because there is no question dealing with other sections of this standard, we are adding comments regarding those sections here. We disagree with all the specificity in the applicability and facilities section for Distribution Provider (DP) and Load Serving Entity (LSE). These sections are not consistent with the Compliance Registry Criteria and will only cause confusion. There is no specific compliance registry criterion for including a DP that has been included in the Transmission Operator's restoration plan. Because NERC clearly states in their Rules of Procedure Appendix 5B Statement of Compliance Registry (see the first paragraph on page 2) that they will not enforce the standards against entities that are not registered, the standard simply couldn't be enforced against such an entity included in the TOP's restoration plan unless they were already registered. Furthermore, the Compliance Registry Criteria already allow NERC to register a responsible entity as a DP and LSE if that entity "owns, controls, or operates facilities that are part" of a required UFLS or UVLS program, special protection system (SPS) or transmission protection system. Since the DP or LSE with a required UFLS or UVLS program, SPS or transmission protection system, is already registered, how does this applicability section provide any more clarity? The DP or LSE will know whether they own or operate these facilities and simply will provide the appropriate response in any required CMEP submissions such as audits and self-certifications. If the responsible entity is not registered as an LSE or DP even if they own these facilities, then again NERC can't enforce these proposed CIP standards against the entity per their Rules of Procedure Appendix 5B Statement of Compliance Registry (see the first paragraph on page 2). In the Facilities section, we are concerned that non-BES Facilities will be included in the standard. Non-BES Facilities should not be included at this juncture given that the Project 2010-17 Definition of Bulk Electric System drafting team is just beginning its work on the second phase of defining the BES. Until this work is completed, non-BES Facilities should not be included and, then, they should only be included with significant justification. There should be a high bar for deviating from the BES definition particularly since it will be recent and have considered all issues facing the industry at that time. The application guidelines have not clearly identified all functional entities that might have some responsibility for the various BES Reliability Operating Services. For instance, in the Dynamic Response section, Special Protection Systems responsibilities are attributed to only TO but this could be a GO or even DP responsibility. UFLS and UVLS are only attributed the DPs but the TO could choose to implement these systems on the transmission system. Governor Response could also be a GOP responsibility. Another example would be the current and next day planning in the Situational Awareness section. It is only attributed to the TOP even though there are NERC standards that require the RC to perform next day planning. In the Managing Constraints section, the responsibility for interchange schedules is attributed to the TOP and RC. It should be attributed only to the Interchange Authority or Interchange Coordinator. In the Restoration of the BES section, the responsibility for off-site power for nuclear facilities is attributed to the TOP. In the NUC standard, it is actually attributed to the transmission entity which could be one of eleven functional entities. Since there many errors (we did not identify all of them) in attributing responsibility in this section, we suggest the drafting team completely review this section and update it or consider removing the responsibilities altogether as their purpose is not clear. We believe the statements beginning on page 23 and continuing on page 24 of the High Impact section of the applicability guidelines regarding TOP delegation to the TO should be removed. If the TOP has delegated some functions to the TO that would otherwise have been carried out in the TOP Control Center and might have resulted in additional TOP BES Cyber Assets and BES Cyber Systems being categorized as High Impact, this delegation should not have an impact on the TOs categorization of BES Cyber Systems and BES Cyber Assets. First, the TOP is still responsible and can't pass that

responsibility on through a delegation agreement. Thus, the TOP and TO will have to address this in their delegation agreement. Second, the TOP likely does not own these BES Cyber Assets at the TO. The TO likely owns these BES Cyber Assets and BES Cyber Systems, and they should be classified according to the criteria established for TOs in Attachment 1. Use of the term asset in the definition requires ownership by the responsible entity. If is not owned by the TOP, it is not a TOP asset and, thus, not a TOP BES Cyber Asset. Third, control Centers for TOs are not addressed in Attachment 1. Fourth, this appears to address some concerns regarding some RTO/ISO's TOP registration models that have been expressed in various forums by regulators. These concerns should not be addressed in piecemeal fashion but holistically in a forum covering all concerns and issues with the registration model. Fifth, there is nothing in the requirements that requires these BES Cyber Assets and BES Cyber Systems to be categorized in this manner. The application guidelines are not requirements and cannot modify the requirements. They can only help explain the requirements. However, these statements are fundamentally altering the requirements and how the attachment 1 criteria are applied. In the first paragraph on page 25 in the application guidelines, there is statement that indicates there may not be a Planning Coordinator for a given area. This statement is contrary to the Section 501.1.4 of the NERC Rules of Procedure. This section states that the registration process shall ensure that "no areas are lacking any entities to perform the duties and tasks identified in and required by the reliability standards". In the third paragraph on page 25 in the application guidelines, Category D contingency should be removed. The TPL standards only require a Planning Coordinator or Transmission Planner to document the impacts of Category D contingencies. There are no performance requirements for Category D contingencies. Thus, it is highly unlikely that any Planning Coordinator or Transmission Planner could ever justify the costs for reliability must run unit through Category D contingencies to its regulator, and, thus, there likely will not be any. In several places in the application guidelines (occurs on pages 26, 27, and 29), exceeding an IROL is discussed when the SDT really means violating an IROL. An IROL by definition has two components. It has a limit and a time constant called Tv. This time constant can be up to thirty minutes and usually is. The time constant is set based on how long the IROL limit can be exceeded without exposing the BES to an unacceptable risk. Thus, an IROL is only violated once the limit has been exceeded for a time greater than Tv. An IROL is exceeded but not violated when the time of the exceedance has not reached Tv. We suggest the drafting team modify the application guidelines in this standard and any other standard with the appropriate use of exceed or violate for the IROL consistent with this explanation. In the third bullet on page 29, the term regional load shedding requirement needs to be made consistent with the new UFLS standard. The UFLS program will be developed by the Planning Coordinator and not the Regional Entity. The NERC adopted version of the standard does not even require a regional version of the standard as was originally proposed.

No

The VSLs for R2 are not consistent with the requirement. Requirement R2 allows the CIP Senior Manager or delegate to approve identification and categorization of High and Medium Impact BES Cyber Assets or BES Cyber Systems. The VSLs drop the "or delegate" language which implies the CIP Senior Manager has to approve the categorization and identification. The "or delegate" language should be added back.

This requirement should be struck along with all references to CIP Senior Manager in the CIP standards. This requirement dictates a corporate governance structure for no reliability reason. An entity should be free to have two, three or more officers or personnel to oversee various portions of the CIP program. The responsible entity will still be required to meet the CIP requirements regardless. Furthermore, mandating a single CIP Senior Manager implies that potential for sanctions up to $1,000,000 per day per violation are not enough to get senior management's attention. This implication is totally contrary to the purpose of making standards enforceable by such sanctions. No other standards require identification of single senior manager and no reliability justification has ever been provided for why one is needed for the CIP standards.

No

We agree there should be "one or more documented cyber security policies that represent the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses" the required ten topics seem reasonable. However, the items that a "Responsible Entity should consider" for inclusion in its cyber security policy as stated in the Guidelines and Technical Basis section (application guidelines) of the standard appear to be written as requirements and the drafting team should consider moving them to R2 if auditors will ultimately treat them as requirements. This will

reduce compliance risk by leaving no doubt as to the minimum amount of information that is to be included for each topic. Requirement R2 should also be modified to make it clear that an entity may write exceptions into their cyber security policies. FERC made it clear in Order 672 that only the requirements in a standard are enforceable and part of the standard. Thus, while the application guidelines make it clear the responsible entity can write in exceptions to its cyber security policy, the application guidelines are not enforceable and there is no way of ensuring that auditors follow them. Furthermore, we believe the fourth bullet in section 2.3 Remote Access regarding including language in contracts with vendors, consultants and contractors requiring them to follow the responsibility entity's cyber security policy should be modified. The bullet should apply to future contracts and not existing contracts to avoid the need to renegotiate all contracts which puts the responsible entity at a significant disadvantage particularly with some contracts such those with EMS vendors. In addition, M2 bullet 2 says "Records that indicate the required ten topics were implemented." What exactly does "implemented" mean in this case? That the items the responsible entity should consider for each of the topics are included in the policy(ies)? This needs to be clarified.
No
What does "initially upon the effective date of the standard" mean? It could be interpreted that the cyber security policies would need to be reviewed and approved on the date the standard is effective which is not reasonable for a myriad of reasons. A couple of those reasons could include that the effective date could be a holiday or weekend or the CIP Senior Manager is not available (they could be incapacitated). Ultimately, we believe that the intent is for the cyber security policy to be in effect and approved by the effective date rather than on the effective date and to ensure that is has been reviewed recently particularly since the implementation plan is a minimum of 18 months. Then going forward subsequent reviews and approval would take place at least once per calendar year not to exceed 15 calendar months. If this intent of this requirement, there really is no way to ensure the review occurred recently without making the requirement retroactive which clearly cannot be done within a requirement. In addition, M3 bullet 1 implies that a Responsible Entity needs to have a "document management system." The word "system" could mean an application to manage documents. It could also mean a process for managing documents. Rather than leave it open to interpretation, we recommend eliminating the phrase, "from a document management system."
No
Awareness of a security program is covered in depth in CIP-004-5 and ensuring accessibility and availability of cyber security policies goes hand in hand with this. We recommend removing R4 from CIP-003-5.
No
Based on the assumption that there will be a CIP Senior Manager, we generally agree with the use of a delegate. We even believe it would be reasonable for a delegate to approve the cyber security policy. However, we do not agree with the use of "CIP Senior Manager" in this requirement based on our comments for R1 in question 6.
No
Based on the assumption that there will be a CIP Senior Manager, we agree with this requirement. However, we do not agree with the use of "CIP Senior Manager" in this requirement based on our comments for R1 in question 6. There is an extraneous number 2 at the end of the requirement.
No
We disagree with the VSLs for R2. More gradations could be provided based on the number of parts missed. Since there are 10 parts, there is plenty of room for four VSLs. The VSLs for R6 should consider using the numbers of days that documentation of the change to the CIP Senior Manager documentation is late. Use of number of days late is a common way to write a VSL and allows more gradations.
No
For Part 1.1, the rationale box does not appear to agree with the requirement. It states the need to ensure everyone with authorized access receives this awareness was removed. Yet, the requirement applies to the responsible entity and does not appear to exclude anyone with authorized access. Which is it? Furthermore, the rationale box should be more specific and use the full names of both types of access which are: authorized electronic access and authorized unescorted physical access. Otherwise, generically referring to authorized access could mean one or the other but not both, or it could mean both.

No
We agree with the concept that training should be role based. As an example, a system operator who is an end user of an EMS does not need most of the training identified in the various parts of Requirement 2. The system operator certainly does not need training on recovery plans for BES Cyber Systems but might need training on the visitor control programs and how malicious actors might use social engineering to gain access to the EMS. The problem we see with the requirements and it parts is that it does not make clear anywhere the need to identify what training each role would receive. Rather it only states that roles must be identified and then identifies training in the various requirement parts that apply to the main requirement which could be construed as applying to the whole training program including all roles. The paragraph references in the rationale boxes for parts 2.6 and 2.7 are inaccurate. Paragraphs 632-634, 688, and 732-734 refer to CIP-007 and CIP-009. There are no references to issues in CIP-004. While paragraph 413 does discuss CIP-004, it only describes what is in the standard and not any changes directed to the standard. In regards to Part 2.6 and storage media, the only mention in Order 706 of storage media is in paragraph 635 and it directs NERC to determine what it means to prevent unauthorized retrieval of data using storage media.
No
This requirement needs to be clarified that it only is intended to require appropriate role-based training for each individual with authorized electronic access or authorized unescorted physical access based on their specific job responsibilities and not the entire cyber security training program identified in R2. Use of the word “needing” is problematic. An entity cannot grant authorized electronic access or authorized unescorted physical access unless it is needed per CIP-007-5 R5. We suggest changing “each individual needing authorized electronic…” to “each individual with authorized electronic…” For consistency across the standards and clarity, we suggest every use of “authorized electronic or unescorted physical access” be replaced with “authorized electronic access or authorized unescorted physical access”. This will help to avoid similar confusion that arose in previous versions of the standard in which it was not clear if “authorized” applied only to electronic access or unescorted physical access. It will further make it clear that authorized electronic describes one type of access. Regardless of how it is written, it needs to be consistently used across that standards and it is not.
No
Part 4.2 may not be possible to complete. While we agree with the need to conduct seven year criminal history checks, obtaining all addresses may not be possible. The responsible entity can verify the current address or a recent address from reviewing a driver’s license but after that the responsible entity cannot with certainty verify that it has all of the former work, home and school addresses of the employee. The employee may not provide the addresses and the background check may not provide these additional addresses. The requirement needs to be clear that the responsible entity may request this information from both the vendor providing the background check and the employee but will not be held accountable for either party’s failure to provide a complete list of addresses. Part 4.3 could be problematic for a responsible entity and needs to be clarified that the responsible entity does not need to establish hard and fast criteria that must always be followed. Finding qualified personnel to work in these highly specialized fields is challenging enough without adding this additional constraint. Background checks may certainly reveal problems with an otherwise qualified person. While some of these problems would be obvious reasons to disqualify a person, others may simply require further research and explanation from the individual for why it is not a problem.
No
In general, we agree with the requirement but believe the requirement should be further clarified, perhaps in the measurement, that in no circumstance should a responsible entity be asked or required to show the personnel risk assessment for an individual to auditor and enforcement personnel. There are a myriad of reasons not to show the actual personnel risk assessment including privacy concerns and other applicable laws may prevent this.
No
The application guidelines on page 44 state that access authorization and provisioning should not be performed by the same person. While this is a laudable goal, it should be clear that small entities may simply not have the staff to accommodate this guideline. We suggest adding “where possible” to this statement.
No

It is not clear why resignations are separated from terminations in Parts 7.1, 7.3, 7.4 and 7.5. Resignations are voluntary terminations. We are unsure what the drafting team intends to accomplish by splitting them out. Where do retirements and layoffs fit in? Since there does not appear to be any different requirements on resignations and terminations, we suggest to use only the generic termination to avoid this confusion. Part 7.2 does not address the situation for phased transfers. For many entities, a transferred employee could continue to need authorized electronic access and authorized unescorted physical access for a long period of time to provide support particularly if a new employee is being trained. This could occur long after the transfer date. While the application guidelines do address this issue, they are simply not requirements and NERC is not bound to follow them. Thus, we suggest making Part 7.2 more generically state that the authorized electronic access and authorized unescorted physical access should be terminated once management determines it is no longer needed. We are a little surprised that the application guidelines state in the scenario table that no action is required to revoke access in the event of a death. While we agree there would be no immediate additional risk for obvious reasons, access should still be revoked at some point.
No
VSLs for Requirements R2 and R3 should have more gradated levels. For R2, there could easily be several roles which would allow for more than two VSLs. Since there are 10 parts to the requirement, four VSLs could easily be written based on the number of parts missed. For R3, more VSLs could be written based on the percentage of individuals that were not trained. The Severe VSL for Requirement R5 incorrectly includes personnel risk assessments (PRA). PRAs are dealt with in Requirement R4.
No
The requirements of Parts 1.2 and 1.3 make no mention of egress while the associated measures specifically mention it. Does the drafting team intend for there to be procedural or physical access controls regarding egress? If so, that is not clear in these standards at all and could set up a responsible entity for a compliance violation. We do not believe that egress controls should be necessary. Only ingress controls are necessary to prevent access to unauthorized individuals. Egress really only helps in knowing who is currently within the Defined Physical Boundary which might provide some value but the expense of installing egress physical access controls would likely far outweigh any benefit. It is unclear how the “operational and procedural controls” required in R1.1 differ from the “physical access controls” required in R1.2 and R1.3. Suggested methods for restricting physical access are given in the “Guidelines and Technical Basis” (application guidelines) section, but none are given for “operational and procedural controls.” Additional discussion in the application guidelines on these operational and procedural controls would be helpful in understanding them. Also, regarding the application guidelines, it would be helpful if the section labeled “Requirement R1,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
We believe that this proposed requirement improves upon the existing requirements. However, we believe that individual point of contact could be confusing. We recommend changing it to escort and making it clear in the application guidelines that this would be the main escort with responsibility for the visitor but not necessarily someone who is with the visitor the whole time. Others could also temporarily escort the visitor. Regarding the “Guidelines…” section, it would be helpful if the section labeled “Requirement 2,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
Regarding the “Guidelines…” section, it would be helpful if the section labeled “Requirement 3,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
A visitor control program is intended to identify and log visitors to the Defined Physical Boundary (DPB). They cannot gain access due to other requirement such as CIP-006-5 Requirement R1 that compels the responsible entity to establish physical access controls. Furthermore, the training

requirements of CIP-004-5 compel a responsible entity's personnel with authorized unescorted physical access to have been trained on who has access and that visitors must be escorted. Thus, the visitor control program can only be an administrative function that is truly intended to keep track of those visitors that have been to the DPB. By definition, administrative requirements should have a Lower VRF. Thus, CIP-006-5 Requirement R2 should have a Lower VRF.
No
On page 39 of the application guidelines in section 1.2, Component should be made lower case.
No
Part 5.5.2 needs to be refined further. It needs to be clear that maximum complexity regarding character types in the password applies if the BES Cyber System cannot support at least three character types. We suggest appending "if less than three character types" to the end of the requirement for further clarity.
No
Because there are likely many ports for Requirement R1, the four VSLs could be written based on the percentage of ports missing from documentation. For Requirements R2-R4, there will likely be many BES Cyber Systems to which the requirements apply. Four VSLs could easily be written based on the number of BES Cyber Systems for which the requirement was missed.
No
EOP 4 in the Rationale box should be replaced with EOP-004. While Part 1.2 requires a process to identify Reportable BES Cyber Security Incidents, there is no indication of who is to receive these reports. There is only Part 1.3 that requires the responsible entity to identify internal and external staff to which to communicate the "incident". Does that mean the list of recipients is totally up to the responsible entity and could be null? If not, then the drafting team needs to identify the minimum list of recipients. In Part 1.3, we assume the drafting team means Reportable BES Cyber Security Incidents by the use of the term "incident". If this assumption is correct, please replace "incident" with "Reportable BES Cyber Security Incident".
No
The requirement in part 2.1 appears to apply to actual BES Cyber Security Incidents. However, the requirement states that deviations from tests should be recorded. Thus, "or test" needs to be struck. R2 Part 2.2 uses the phrase "initially upon the effective date of the standard." It is not clear as to the meaning of this phrase. It could be interpreted that the BES Cyber Security Incident response plan(s) would need to be implemented either by responding to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise on the date the standard becomes effective. This is not reasonable. If the intent of this requirement is to do an initial implementation within some time period of the standard becoming effective, then the requirement should state a time period for this to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. No application guidelines were written for this requirement. The drafting team should consider either writing some or making a statement that they are purposely omitted.
No
R3 Part 3.1 uses the phrase "initially upon the effective date of the standard." It could be interpreted that a review of each BES Cyber Security Incident response plan would need to take place on the date the standard becomes effective. Because Requirement R1 compels the development of the response plan, it does not make any sense to compel review of the response the same day the requirement of the response plan becomes effective. Rather the response plan review should be required the following calendar year after its initial approval. No application guidelines were written for this requirement. The drafting team should consider either writing some or making a statement that they are purposely omitted.
No
For Requirement R2 and R3, four VSLs could be written based on the number of days late for completing the task. This is a common way to write VSLs.

No
The stated rationale for Part 1.1 does not support the change and additional rationale needs to be provided. Paragraph 694 of Order 706 requires NERC to develop a specific requirement to implement the recovery plan. This requirement is not an implementation requirement but still a requirement for what to include in the plan. Thus, we do not see how the rationale supports the requirement. Part 1.2 should not require either names or titles. These are problematic in that the recovery plan has to change for every personnel move which includes transfers, terminations and promotions. A promotion of IT Analyst to Senior IT Analyst would necessitate an unnecessary change. A better approach would be to allow the use of generic roles such as analyst or even perhaps staff from department X. The requirement needs to allow some flexibility to avoid unnecessary paperwork that provides no reliability benefit. The drafting team should develop application guidelines for these requirements. At the very least, the reference to the FAQs and CIPC Guidelines should be more specific with links to each guideline and FAQ.
No
Part 2.1 uses the phrase “initially upon the effective date of the standard.” It could be interpreted that the recovery plan(s) would need to be implemented either by responding to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise on the date the standard becomes effective. This is not practical for many entities and especially for smaller entities. Part 2.2 of CIP-008-5 R2 already requires BES Cyber Security Incident response plans to be exercised on the effective date of the standard. Many of the same staff involved in the BES Cyber Security Incident response plans will likely be heavily involved in the recovery plans. The important part is that the recovery plan will be in place on the effective date per CIP-008-5 R1 and will likely have been tested prior to the effective date. Thus, the requirement should simply state a reasonable time period that can be met by limited staff for the actual implementation or exercise to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. Part 2.2 has potentially has a similar issue to Part 2.1 but is less clear. Rather than use the full term “initially upon the effective date of the standard” it just states that the test must be conducted initially. We assume the drafting team meant for this to be conducted on the effective date similar to Part 2.1. This makes completing this part and other parts mentioned in the previous paragraph even more impractical. The requirement should simply state a reasonable time period for the actual implementation or exercise to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. Since Part 2.3 requires a full exercise in representative environment every 39 months and is required to be included per FERC directive, we recommend that it be limited to High Impact BES Cyber Systems. Conducting this test in a representative environment could get very expensive because responsible entities may have to purchase the appropriate equipment to set up a parallel environment. This is simply not practical or cost effective to do for every BES Cyber System. Is it really practically to set up a representative environment for every 500 kV substation or special protection system for testing?
No
Part 3.1 should be modified to require the first review of the recovery plan in the subsequent calendar year to the approval of the requirement. To accomplish this, the drafting team should strike “initially upon the effective date of the standard and”. CIP-009-5 R1 already compels the responsible entity to have a recovery plan and becomes effective on the same day as Part 3.1. Thus, the plan will already have been reviewed when it was developed and approved. Thus, it does not make sense to have a separate review in Part 3.1 on the effective date. For consistency with Part 3.3, R1.2 in Part 3.5 should be written as Requirement R1, Part 1.2.
No
The VSLs for Requirement R1 should include more gradations than two levels based on the number of parts missed. For Requirement R2 and R3, four VSLs could be written based on the number of days late for completing the task. This is a common way to write VSLs.
No
Part 1.1.6 could be redundant with CIP-007-5 Part 2.2. While CIP-007-5 Part 2.2 does not explicitly require documentation of the security-patch levels, demonstrating compliance with it ultimately will require such documentation. Thus, it becomes redundant with Part 1.1.6 of CIP-010-1 R1. If not redundant, it certainly sets up a high probability for double jeopardy because each compliance

violation of CIP-007-5 Part 2.2 will likely result in a violation of Part 1.1.6. Part 1.2 is unclear. Is this intended to require the CIP Senior Manager or delegate to authorize the process to develop a baseline configuration or is it intended to require the CIP Senior Manager or delegate to authorize deviations to the baseline? As a result, Part 1.2 needs to be clarified. As it is written now, the only clear requirement from Part 1.2 is the need to document baseline configuration deviations. Part 1.4.1 requires the responsible entity to identify the cyber security controls that could be impacted by the change. This appears to be the first use of cyber security controls in the library of CIP standards. As a result, the intent and meaning of the term needs to be further clarified.

No

Part 3.1 uses the phrase “initially upon the effective date of the standard.” It could be interpreted that the security controls for every applicable BES Cyber System and BES Cyber Asset need to be assessed on the date the standard becomes effective. This is not practical particularly for smaller entities. Several other requirements including Part 2.1 of CIP-009-5 and Part 2.2 of CIP-008-5 R2 already require significant action on the effective date of the standards. Part 2.1 of CIP-009-5 requires recovery plans to be implemented on the effective date and Part 2.2 of CIP-008-5 R2 requires the BES Cyber Security Incident response plans to be exercised on the effective date of the standard. Imagine the amount of personnel and effort necessary to complete all of these tasks on (not by) the effective date. Many of the same staff involved in the BES Cyber Security Incident response plans and recovery plans will likely be heavily involved in the vulnerability assessments. The requirement should simply state a reasonable time period for the vulnerability to be completed after the effective date of the standard or make it clear that the vulnerability assessment needs to be completed by the effective date and not on. Part 3.2 has a similar issue as Part 3.1 in that it appears to require a vulnerability assessment for all High Impact BES Cyber Systems on the effective date of the standard. We have the same issue with this requirement in that the same limited set of staff will likely be responsible for completing these assessments as the tasks compelled by several other requirements that must be complied with on the same effective date.

No

In general, the VSLs escalate violations to the higher end of the sanctions matrix too rapidly for minor violations. This could be fixed by writing VSLs for each level rather than just High and/or Severe VSLs in some cases. For example, if an entity fails to establish a single baseline on one applicable BES Cyber System or BES Cyber Asset per Requirement R1, it would be deemed a High VSL. If that is one out of one thousand BES Cyber Systems or BES Cyber Assets, this would seem excessive. Likewise, if an entity is one day late in updating their baseline configuration per Requirement R1, the violation would be deemed Moderate. This is not consistent with many other requirements in the CIP proposal which provide four VSL based on the number of days late.

No

The rationale for Requirement R1 indicates Requirement 4.1 was moved to the BES Cyber System Information definition. It does not reference which standards the requirement comes from. It needs to for clarity. Part 1.1 needs to be clarified. We believe the requirement pertains to ensuring BES Cyber System Information is either marked in some way to be clear it is BES Cyber System Information or recognized as such by the responsible entity’s personnel. However, we are concerned that requirement could be interpreted as needing to develop a method to ensure that all BES Cyber System Information has been found and there is no extraneous information. In other words, we are concerned the requirement could be interpreted as requiring the method to be some sort of search process. We think this problem would be solved providing some discussion of the intent of the requirement in the application guidelines. Part 1.3 needs to be modified. It requires the responsible entity to assess its adherence to its BES Cyber System Information protection process “upon the effective date of the standard”. This does not make any sense since the responsible entity will have just then been required to utilize the BES Cyber System Information protection process. What will they assess? This requirement should not require this assessment until the process has been in use for a year. Part 1.3 uses a term “protection process” that was not used previously in the requirement. For consistency with other requirements and clarity, we suggest that either that term be used in Requirement R1 instead of just the term process or that “protection” be struck in Part 1.3 and replaced with a reference to the main requirement.

No
We agree with the implementation plan concept that essentially bypasses the effective dates of version 4 of the standards for version 5. This will significantly lessen the compliance burden for responsible entities to avoid two separate transitions and avoid the confusion of preparing for version 5 while still preparing for version 4. We believe that some requirements should have delayed implementations plans rather than become effective on the same date as the remaining requirements. Some requirements are dependent on the completion of other requirements and do not make sense to implement until the other requirements have been in effect for some time. Consider Part 1.3 of CIP-011-5. It requires the responsible entity to perform an assessment of its adherence to the BES Cyber System Information protection process. However, the protection process is only required to be in effect the same day. What sense does it make to assess adherence to a process that was just started? The drafting team should perform a complete review of all the requirements for dependencies and determine an appropriate staggered implementation for them. The first sentence in the “Proposed Effective Date for Version 5 CIP Cyber Security Standards” on page 2 should be modified. It states the responsible entities must comply with the definitions on the effective date. Definitions have no compliance obligations. They simply become effective and help explain the requirements. We suggest 18 Months Minimum should be modified. Please change the “date of the order” to “effective date of the order” for clarity. FERC typically issues an effective date of their orders that is dependent on publication in the federal register and is different from the date the order is published. This will help provide clarity that the effective date of the order is the appropriate date to reference rather than the publication date. This will need to be changed across all the standards and the definitions.
Individual
Kevin Koloini
AMP
Yes
AMP agrees with the APPA trade association comments for the definitions.
Yes
Distribution Providers have not been applicable in the past to CIP-002. Adding Distribution Providers to the full gamut of CIP is a significant increase in the requirements for smaller organizations. Smaller organizations that may not currently have the resources for implementing many of the requirements, especially those that are recurring, time consuming and that require multiple policies and procedures. We need to draw the line somewhere. Adding these requirements to organizations that do not have in-house expertise or resources seems excessive when done on a recurring basis (once a year for many requirements as drafted). A NERC Alert for Distribution Providers may serve that function and the industry in a more economic fashion by reducing the time commitment and the required policies and procedures. Distribution Providers will still increase awareness, improve core competencies in security, and protect their equipment, but would not be required to perform the "paperwork" or "exercises" associated with the CIP standards as drafted. Please remove Distribution Providers.
No
The requirement is good. I believe it would be better if the language "within 30 calendar days" was removed. I believe there is a small percentage of changes that would occur for most organizations and for those that do have changes 30 days may not be enough time.
No
Why does this need to be a recurring requirement? Upon identification and categorization, there are typically no changes and those that do change are typically addends. All I am saying is that this requirement asks for every Responsible Entity to do an exercise even if a large majority of the entities will have a similar or identical result as the previous year. I don't see the point. Suggest: "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and upon Cyber Asset or Cyber System changes."
No
Yes

No
Proving implementation is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for implementation.
No
Extend the requirement's review period or make it event-based. I suggest 2-5 years for the review period.
No
I agree with the intent of the requirement. I believe that individuals should be aware. However, I feel that the auditing process will require training logs. Why not just make the requirement fit the implementation to make it easy for everyone. "Each Responsible Entity shall train staff that have access to BES Cyber Systems, maintain a log of awareness training and material, and maintain a list of staff who have access to BES Cyber Systems." Despite my suggestion, I feel this requirement is not needed.
No
Once the CIP Senior Manager has been given authority and responsibility, the CIP Senior Manager should be able to delegate without having to have a paper trail for each delegation, otherwise I feel the CIP Senior Manager is delegating authority and responsibility by naming another person. What is the result this requirement is going to achieve?
No
Remove the 30 day requirement and remove the delegations. Consider a simpler requirement where the CIP Senior Manager status changes. I believe this requirement can be eliminated and the rest of the requirements will still achieve a reliable result.
No
No
Proving the implementation happened is difficult without clear and simple expectations. I suggest removing implement from the requirements or explicitly describing the expectations for compliance beyond documenting the processes.
No
Eliminate the requirement or revise with the results in mind. As written, this is a requirement that has the potential to be highly violated and that may or may not prevent a physical or cyber event in whole or in part.
No
Eliminate the requirement.
No
Eliminate the requirement.
No
Eliminate the requirement.
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the programs.
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the programs.
No

Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the plans.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the programs.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the programs.
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Yes
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the plans.
No
Replace "and" with "or".
No
Yes

No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
Yes
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Yes
Group
FirstEnergy
Doug Hohlbaugh
Yes
SUMMARY COMMENTS: FirstEnergy (FE) recognizes the dedicated work of the CIP Standards Drafting Team (SDT) in developing the proposed version 5 CIP standards. FE supports much of the SDT's work and changes offered by CIP V5. While we are balloting against the version 5 standards at this time, our voting position should not be viewed as a fundamental disagreement with the SDT's approach. However, we believe there is value in building on the version 4 CIP standards retaining certain key aspects of the standards which have already been implemented by hundreds of registered entities within industry. FE strongly supports further enhancements to the cyber security standards that improve reliability while providing compliance clarity and alleviating burdensome administrative tasks that do not improve reliability. As further described below, we propose the SDT: 1. retain the CIP-002-4 standard with slight modifications 2. continue to build upon its work for CIP-003-5 through CIP-011-5 3. develop a new standard for low impact critical cyber assets This proposal offers greater opportunity for the industry to deliver timely improvements needed in controls for medium and high impact cyber assets while further vetting any potential obligations for low impact cyber assets. Many

of the changes offered through CIP V5 are well received by FE. We appreciate that the SDT has tried to alleviate the need for TFEs where possible within the standards. As an example, CIP-007-5 R3 is a much needed improvement regarding malware prevention and no longer prescribes a specific technical method (anti-virus) as found in the existing CIP-007-3 R4 (which has historically generated a number of TFEs). We support the proposed table format which clearly shows the requirements and measures together and the additional insight and guidance offered by the Application Guidelines located in the back of each standard. The ability to classify BES Cyber Systems is also a welcomed change that helps simplify the maintenance of cyber asset lists subject to the CIP standards. Additionally, the proposal of new CIP-010-5 and CIP-011-5 standards more efficiently present obligations for configuration management, vulnerability assessments and information protection than the current CIP version standards. However, we encourage the SDT to retain certain existing terminology such as Critical Cyber Assets, Physical Security Perimeter over their proposed counterpart BES Cyber Asset and Defined Physical Boundary even if actual definition changes are warranted. FE is opposed to any instances of terminology name changes where no clear need is justified as the modifications will require significant industry resources to unnecessarily modify compliance procedures and processes. A significant departure from existing standards is moving away from determining cyber assets as “essential” to the Critical Asset that if “destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.” The introduction of BES Reliability Operating Services which if “misused” significantly increases the scope of cyber assets that could be subjected to the CIP standards. The NERC CIP standards should specifically define "Impact" as "The effect on the Bulk Electric System reliability if the essential asset is destroyed, degraded, or otherwise rendered unavailable." This is significantly different from whether an asset is "misused." If an asset has no external connectivity (i.e. not routable or dial-up), the assumption is that it cannot be misused by a remote attacker. However, it could be rendered unavailable -- which is why the assessment of "essential" is so important. As an example, an RTU -- if misused -- could have high impact on the BES. However, that same RTU -- if rendered unavailable (e.g. from a buffer overflow, loss of a communications circuit, or an ax to the chassis!) -- may have absolutely zero impact on the BES reliability. The term "misused" is therefore inappropriate in this context and should be removed from the language of the standards altogether. If that stays in the language, we'll have hundreds of new assets to manage under CIP that have little to no reliability impact if lost. We also suggest the SDT retain the concept of first identifying Critical Assets and then associated Critical Cyber Assets since the Attachment 1 Criteria listed in CIP-002-5 still refer to physical facility locations in most cases and are very similar to the NERC BoT approved “bright line” CIP-002-4 standard. In summary, we would like to see CA, CCA and PSP be retained terms with the definitions applied as suggested below. Therefore, we suggest retaining the CIP-002-4 standard with relatively minor adjustments to bring in some aspects of the SDT’s proposed CIP-002-5 standard. For instance, CIP-002-4 Attachment 1 could easily be adjusted to identify which criteria would qualify as high impact and medium impact in a similar manner as shown in attachment 1 of version 5. We are also supportive of other changes such as modifying version 4 Attachment 1 criterion item 1.7 to better match its version 5 counter-part criterion item 2.7 which lowers a threshold substation voltage level from 300kV to 200kV for qualification as medium impact facilities. The expansion of cyber protection to low impact devices, while warranting consideration, brings into scope many registered entities that have no CIP obligations today. The low impact requirements proposed by the SDT seem relatively benign on the surface and describe reasonable practices. However, they bring into question the ability to produce auditable evidence. For example, while it is indicated CIP-002-5 requirement R1 that BES Cyber Systems deemed to be low impact do not require discrete identification, yet it is unclear how the Compliance Enforcement Authority would be able to randomly sample whether or not an entity removed manufacture default passwords without an entity having a complete and thorough list of the devices. Producing such a list would not be insignificant and the reliability benefit requires further vetting in the proposed separate low impact standard. FE believes the low impact categorization is missing an important aspect regarding the connectivity of the cyber asset. Scope expansion beyond cyber assets with External Connectivity (routable and dial-up) greatly increases industry burden with questionable reliability improvement. Additionally, the FERC in Order 706 paragraph 285 states “CIP-002-1 provides that a critical cyber asset must have routable protocols or dial-up access … We do not find sufficient justification to remove this provision at this time. ” It is clear that, FERC did not explicitly direct NERC in its role as the ERO to expand coverage of cyber assets beyond those with external connectivity. However the Commission did direct the ERO to “consider the comment” made by an industry stakeholder that “argues that devices that use non-

routable protocols should also be considered as possible critical cyber assets." Therefore, FE believes that this subject requires further vetting in a separate standard focused on the controls required for low impact cyber assets. We would support a categorization as follows: 1. High Impact – CIP-002-5 Att. 1 High cyber assets regardless of connectivity. a. Essentially all the Control Centers described and regardless of connectivity. 2. Medium Impact – CIP-002-5 Medium cyber assets with External Connectivity 3. Low Impact – CIP-002 Att. 1 Medium cyber assets without External Connectivity and other BES (not captured in 1 or 2) cyber assets with external connectivity. The SDT spent a significant amount of effort describing the BES Reliability Operating Services to be evaluated in determining whether or not a cyber asset qualifies as a BES Cyber Asset. FE suggests that the BES Reliability Operating Services information be used solely as useful guidance in the Application Guideline section of CIP-002-5 that an entity could use to better assess if a cyber asset is "essential" to BES reliability and therefore subject to CIP standards and not be incorporated as an official NERC Glossary of Terms definition. In FERC Order 706 paragraph 284 the Commission in commenting about a stakeholder concern of too few critical cyber assets being identified indicates they share the concern but state: "However, there is no evidence that will be the case, and there is no formally accepted method for identifying critical cyber assets before us at this time. Therefore, we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time." Based on FERC's comments, we do not see a need for the drastic departure from the existing definition of Critical Cyber Asset and believe that the references to BES Reliability Operating Services within the proposed CIP-002-5 standard only further confuses compliance expectations. GENERAL COMMENTS FOR ALL STANDARDS: Since the Comment Form does not offer opportunity to address miscellaneous items outside of the specific questions raised by the Standard Drafting Team (SDT), prior to addressing this Definitions question, we offer comments that apply to all the standards. In a similar manner, if we have feedback related to a particular standard that is not addressed by one of the SDT's questions, we include our feedback in the 1st question related to the subject standard. ♣ We ask that the team add clarity around the term "routable" because there could be misinterpretations in the industry. The industry standard seven-layer OSI reference model defines "routable" as "Layer 3 and above". We believe this should be clear in all definitions, requirements, and in any guidance that discusses the term "routable" throughout the CIP standards. ♣ Use of the term "real-time" – in several locations within the standard requirements, "real-time" is used. If the intent is to use the NERC Defined term, then this term should be capitalized within the requirements. ♣ Section B (Compliance), item 1.2 (Evidence Retention). The following statement causes confusion and should be deleted or clarified - "For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit." The section later implies that an entity need only keep evidence for three years, however, the preceding statement quoted above causes confusion; particularly in regard to a GO and GOP where scheduled audits are anticipated every six years. The standard should be clear on expectations. ♣ In many areas of the standards, requirement language contains the text "Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between …" Any expectations of what needs to be accomplished to initially meet requirements should be clearly articulated in a standard's Implementation Plan and presents unnecessary requirement text. Although CAN-0012 "Completion of Periodic Activity Requirements During Implementation Plan" has already set expectations in this regard, we believe a clear Implementation Plan should address this matter within the CIP V5 standards. We offer proposed edits throughout the standards in regards to this topic. ♣ We suggest adding a definition in the NERC glossary for Annual defined as "A periodic activity occurring once each calendar year, not to exceed 15 calendar months between recurrences." This would alleviate the wordiness in each of these requirements, establish improved consistency across all standards having annual obligations and eliminate the need for CAN-0010. While both CAN-0010 and CAN-0012 indicate that an "annual" activity is met by performing the activity at least once per calendar year, each also refers to the not to exceed 15 months as the preferred approach. ♣ Section 4 (Applicability) and subsection 4.1 (Function Entity for Distribution Provider (4.1.2) and Load Serving Entity (4.1.6) contain redundant text with their counterpart Facilities (4.2) sections. We suggest streamlining the Functional Entity sections for DP and LSE to simply reference the information presented in the Facilities area. For example, rewrite item 4.1.2 to say "Distribution Provider that owns Facilities as described in section 4.2." ♣ The SDT implies that text from rational boxes will be moved to the guideline and technical basis section of the standard. We encourage the SDT to integrate this information into the existing guideline and technical basis information upon the second posting of the

standard so that we can see the complete guidance for each requirement. ♣ Violation Severity Levels – While we offer some comments on VSLs, in most instances we have not commented as it seems premature to comment in detail on VSLs until the requirement text is near final. As a general suggestion, it is useful when the requirement sub-parts are referenced within the VSLs listed in the VSL table. See standard CIP-004-5 as a good example of this practice. The SDT has not consistently used this format throughout the various VSL tables in other standards. Including the sub-requirement reference improves readability and ensures all parts of a given requirement are covered in the VSL table. ♣ The SDT should carefully review the table headings listed within each standard. In some cases each column says "Part" in each of the four columns instead of "Part, Applicability, Requirements, Measures". COMMENTS RELATED TO DEFINITIONS (Q1): 1. BES Cyber Asset – FE proposes the SDT abandon this definition and revert back to the existing Critical Cyber Asset term and its definition. 2. BES Cyber System – Change "Maintenance" to "Transient". We propose the definition be "One or more Critical Cyber Assets that are typically grouped together, logically or physically, and deemed essential to operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. 3. BES Cyber System Information – a. Break into bullet point for ease of reading as follows: "Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: ♣ security procedures developed by the responsible entity; ♣ network topology or similar diagrams; ♣ Security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports) of a BES Cyber System, Electronic Access Control System, and Physical Access Control System; ♣ BES Cyber System Impact designations; ♣ equipment layouts that contain BES Cyber System ; ♣ BES Cyber System disaster recovery plans; and BES Cyber System incident response plans." b. In the 4th bullet, we have removed of the phrase "floor plans that contain" since it is just one example of items that may contain BES Cyber System impact designations c. In the 5th bullet, we have removed the phrase "Impact designations" as protecting impact designations is now generally covered in our revised 4th bullet. 4. BES Reliability Operating Services – While we do not disagree with the details stated for each of the BES Reliability Operating Services, we do question the need for these items to be included in the NERC Glossary of Terms. Much of the same information is repeated in the CIP-002-5 Application Guidelines section. Since the only reference and use of the BES Reliability Operating Services is within CIP-002-5 we propose an alternate approach. FE proposes that the SDT 1) remove as an official defined term and 2) simply introduce the umbrella term (BES Reliability Operating Services) and the subcategories terms (Dynamic Response, Balancing Load and Generation, Controlling Frequency, etc.) in the Background section of the CIP-002-5 standard and refer to the CIP-002-5 Application Guide for more detailed information. This approach is analogous to how the terms "Associated Physical Access Control Systems, Associated Protected Cyber Assets and others are presented in the Background section of other CIP V5 standards. The BES Reliability Operating Services should only be viewed as guidance as how an entity may determine that a Cyber Asset is in fact a BES Cyber Asset (CCA). 5. Control Center – The definition, while similar to the version stated in the CCA Guideline Document (http://www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf) is not as succinctly written with the multiple "one or more" statements. We propose the following for the leading paragraph which is a hybrid of the two versions. "One or more facilities hosting BES Cyber Assets or BES Cyber Systems relied upon for performing any of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants and transmission substations. Functions that support Real-time operations of a Control Center include one or more of the following:" 6. Defined Physical Boundary – As stated above we propose that the PSP term be retained over DPB, however, the DPB definition should now be used. Also please add "or Monitoring Systems" after Electronic Access Control Systems. The definition should now read "The physical border surrounding locations in which Critical Cyber Assets, BES Cyber Systems, or Electronic Access or Monitoring Control Systems reside and for which access is controlled." 7. Electronic Access Points – We ask that the team add clarity around "routable" because there could be misinterpretations in the industry. The industry standard seven-layer OSI reference model defines "routable" as "Layer 3 and above". We believe this should be clear in this definition and in any guidance that discusses the term "routable". 8. Protected Cyber Asset – There is still some confusion as to how routable is defined? Please describe how "routable" should be interpreted. 9. Reportable BES Cyber Security Incident – change "Any" to "A" 10. General – Access management for vendors is a challenging area since there are occasions when immediate assistance is needed remotely from a vendor to get a malfunctioning system back to functionality. We assume that these cases are covered in the subrequirement language that includes exceptions for CIP

Exceptional Circumstances. We believe that immediate and emergency vendor support should be explicitly included in the definition for CIP Exceptional Circumstances.
Yes
General comments for CIP-002-5: 1) Purpose Statement: The purpose statement has a grammatical error and missing the word “the” in the second line between “to reliable”. We also suggest breaking the Purpose Statement into two sentences for ease of reading by adding a period after BES in the second line. 2) Applicability: 4.2.4.2 – Why is this needed? Since communication networks are now out of scope within the definition of Cyber Assets is this exemption still required? 3) Background: pg. 8 Real Time Ops: add wording to direct reader to BES Cyber Asset definition Evidence retention: 2nd sentence in opening par. should be reworded for clarity Evidence retention: How does 1st bullet fit in with entities on 6-year cycle? Attachment 1 Comments: Criteria 1.4 – We suggest adding 2.5 (a generation obligation) and removing 2.12 (not a generation obligation) Criteria 2.7 – This criteria has two embedded concepts separated by an “or” statement. During the Q&A session of the 1st NERC webinar conducted on 11/15, it appeared that the “or” is really intended to be an “and”. We suggest breaking these criteria into two bullet points for ease of reading. We propose: “Transmission Facilities operating at 200 kV or higher, but at less than 500 kV, at a single station or substation: ♣ connected to three or more transmission stations or substations; and ♣ with “total weighted aggregate value” of all BES Transmission Lines at a single station or substation operated at 200 KV or higher connected to other transmission stations or substations, including incoming and outgoing lines, exceeds a value of 3,000. The following “weight value per line” operated at the associated voltage value of a line will be used for the determination of the total weighted aggregate value.” Criteria 2.13 – The second reference to “control centers” should be capitalized to be clear it is intended to be proposed definition of Control Room (i.e. operating generation at two or more geographic locations) to avoid confusion with a control room(s) located at a single geographic generation plant location.
No
General – For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format. R1: Rational – Cyber Systems should be BES Cyber Systems 1.1 – what is meant by “intended”? for instance, what if you intended less than 6 months but it ended up being longer? We suggest replacing “intended” with “scheduled” 1.1 - also, we suggest that 30 days be extended to 60 days due to possible time needed to update the categorization
Yes
General – For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
No
R2 VSL - We do not believe that being late by 30 to 40 days is adequate since this a mere review of the list each year. We suggest changing the LOWER to “30 to 60 days”, then have 10 day increments for the rest of the VSL such as “60 to 70 days” for MEDIUM, “70 to 80 days” for High, and “80 to 90 days” for SEVERE.
Yes
General - For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format. We suggest removing the Applicability definitions on pages 7 and 8 since they are not used in CIP-003-5.
No
In M2, we do not agree with the 2nd example of evidence. How do you show the implementation of a policy? We suggest #2 be struck and reword the measure to “One or more documented cyber security policies that cover the ten topics specified in R2”. Also, in the guideline section in the first paragraph of page 20, the mandatory statement that says “must cover in sufficient detail” should not be in a guideline. If the team’s intent is to have certain minimum details covered in the cyber security policy, we suggest the team consider adding these minimum requirements within R2. For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
Yes
For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
No

1. We believe this requirement should only apply to High and Medium Impact BES Cyber Systems. Including all personnel who interface with Lower Impact BES Cyber Systems is unnecessarily burdensome with no significant reliability improvement. 2. R4 – The term “aware” is vague and our proposed revision to the requirement removes the ambiguity. We suggest a revision such that this requirement is clear that cyber security policies are made available to individuals given authorized electronic access or authorized unescorted physical access; and we suggest removal of “appropriate for their job function” since this gets into role-based training covered in CIP-004-5. We suggest that the requirement be rewritten to state - “Each Responsible Entity shall make available and accessible their CIP Cyber Security policy to individuals who have authorized electronic access or authorized unescorted physical access to BES Cyber Systems.” 3. M4 – We suggest removing the 2nd, 4th, and 5th bullets since they reference training which is outside the scope of the standard and requirement 4. We suggest that the Application Guideline include guidance for R4 since this is a challenging requirement to implement. 5. For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
No
We suggest removing “The authority for subsequent delegations may also be delegated” since this just creates an endless loop. Also remove the 3rd bullet of M5, which is in regards to our suggested change. For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
Yes
In regards to R6, the reference to footnote #2 needs to be reformatted as a superscript. For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
No
We propose that the VRF for Requirement R1 be modified to reflect a “Lower” VRF. The NERC VRF guideline document (http://www.nerc.com/files/Violation_Risk_Factors.pdf) indicates that a Lower VRF is “a requirement that is administrative in nature” and we believe this applies to R1 of CIP-003-5.
No
General CIP-004-5 comment: We suggest an addition in the applicability exception a new section: “4.2.4.5 Personnel associated with regulatory (e.g., Regional Entity, NERC or FERC) audit teams or investigations requiring access to BES Cyber System Information.”
No
2.2 - Should be eliminated. There is no way to talk about physical access controls and electronic access controls without talking about the security controls in place. This would be redundant with 2.3 and 2.4. 2.5 – We ask that the team clarify whether training on the visitor control program includes both electronic and physical access. Additional wording may be necessary in the requirement to make this explicit. 2.7 and 2.9 – We suggest switching 2.9 and 2.8 so that the requirements flow better since 2.7 and 2.9 deal with Cyber Security Incidents. 2.10 – The intended objective for item 2.10 is a bit unclear and what level of detail is required in regard to interconnectivity and interoperability. If the intent is a general “layman” understanding to the general population we can support, however, detailed training of IT staff that are knowledgeable and experienced in this area should not be the intent. FE requests that the SDT clarify this requirement.
No
R3 – The applicability includes other associated systems but R4 does not have these in the applicability. We ask the SDT to consider the need for consistency in applicability between the two. M3.1 – Measure 3.1 indicates that the date access was first granted would be evidence that may be needed for requirement 3.1. We ask that the SDT clarify in its guidance or compliance evidence retention section 1.2 as to the number of years the entity is required to retain this evidence. It should be clear that evidence is only needed for the last three years or since the last audit as stated in the evidence retention section.
No
4.4 – Add “Parts 4.1 through 4.3” at the end of the requirement 4.4 – measure should be consistent with the R5 Part 5.1 measure which allows the use of attestations from vendors and contractors
No
R5 – The applicability includes other associated systems but R4 does not have these in the

applicability 5.2 – In the measure, it is not clear the intent of “former” risk assessments. We suggest removing “former” since current assessments meets the intent of the requirement.
No
General – Access management for vendors is a challenging area since there are occasions when immediate assistance is needed remotely from a vendor to get a malfunctioning system back to functionality. We assume that these cases are covered in the subrequirement language that includes exceptions for CIP Exceptional Circumstances. We believe that immediate and emergency vendor support should be explicitly included in the definition for CIP Exceptional Circumstances. 6.1, 6.2, 6.3, 6.5, and 6.6 – the use of the term “minimum” is subjective and cannot be consistently defined across entities. We suggest replacing “the minimum” with “commensurate with what”. 6.2 and 6.3 – Remove “to verify unauthorized users do not have access” as this is not necessary for the entity to meet the requirement and it is up to the CEA to verify that the appropriate users have access. 6.1, 6.2, 6.3 - change from 'delegate' to 'delegate(s)' since it is likely that there will be more than one delegate to authorize all access.
No
7.1 - There may be times where access revocation may not be possible right away. In response to FE’s NOPR response suggesting that immediate be qualified as “as soon as possible” but not later than 24-hours, the FERC in paragraph 462 of Order 706 indicated that “the ERO may define what circumstances justify an exception that is other than immediate and determine what is the fastest revocation possible”. We encourage the SDT to revise requirement R7.1 to incorporate a “CIP Exceptional Circumstance” and revise the definition of CIP Exceptional Circumstance for “on the spot” terminations or resignations where the revocation may be forced to lag. Alternatively, allow for documentation of an “extenuating circumstance”, similar to 7.5, that required a lag not to exceed 24 hours for the revocation of access. The footnote should include resignations in addition to terminations consistent with 7.1. Also, footnote should be renumbered to #1. 7.2 and 7.3 – we suggest changing “next calendar day” to “next business day” due to weekends and holidays. 7.5 – We would find it very helpful if the team added some examples of “extenuating circumstances” in the guideline section of the standard.
No
R7 VSL – We believe the threshold violations are too low - it does not take into account the size of an entity and favors small entities. We believe that a percentage would be better such as up to 5% for LOWER, 10% for MEDIUM, 15% for HIGH, and 20% for SEVERE.
No
1.1 – Add “used” between “controls” and “to”. Measure 1.1 – Change “technical and procedural” to “technical or procedural”. Also, remove the last phrase “that exist and have been implemented since implementation should not be required for 1.1 since it only asks to define the controls. 1.3 – There are certain components that do not have the traditional "default Deny" platform. On these devices, an entity basically adds “deny or permit” statements as needed and their ability to get very granular for all in-bound and out-bound port specification is limited. We feel that as written this requirement would preclude existing technology from being used and cause unnecessary additional costs to replace them. We ask that the team remove the phrases “explicit inbound and outbound” from the requirements and have it worded as: “Require access permissions at each identified Electronic Access Point using routable protocols, including criteria for granting or denying those access permissions.” We believe that this change would meet the intent of the requirement. Also, to match the rewording of the requirement, we ask that the term “explicit” also be removed from the measure for 1.3. 1.4 – in general regarding TFE, will the NERC RoP’s TFE process in App. 4D be revised to be consistent with CIP V5 standards?
No
2.1 - The terms "Intermediate Device" and "directly access" are unclear. There are devices on the network between the Cyber Asset initiating Interactive Remote Access (e.g. corporate workstation) and a device within the ESP - are switches, routers, or firewalls sufficient as Intermediate Devices? In another scenario, if a proxy server authenticates the user and then grants Interactive Remote Access, is that proxy server sufficient as an Intermediate Device?. Is this considered direct access? We would appreciate it if the team clarified this language in the standard. The guideline and technical basis for R2 should include a link to the document referenced: “Guidance for Secure Interactive Remote Access”

No
The definition for Physical Access Control Systems explicitly excludes locally mounted hardware devices such as motion sensors, electronic lock control mechanisms and badge readers. However, its unclear if local panels containing programmable circuit boards would be considered part of the locally mounted hardware. Please clarify. General CIP-006-5 comments: Measure M1 statement preceding table: (grammar change) revise “Evidence must includes” to read “Evidence must include”. Table R1, Part 1.1 revise the Measure column to read “operational or procedural controls” for consistency with requirement language. Table R1, Part 1.1 revise the Measure column to strike the phrase “and have been implemented”. During the meeting it was raised that the statement is redundant with implementation wording in the M1 statement, however, it appears it may not be as the M1 statement reads “demonstrate implementation as described in the Measures column of the table.” Some were concerned that the statement “and have been implemented” raises concerns with the level of evidence required to show “implementation” of physical access controls related Low Impact BES Cyber Systems. Table R1, Part 1.2, replace “Utilize” with “Define and implement”. Table R1, Part 1.2 in the Measure column strike “and egress”. The requirement is to “restrict access” and there is no requirement expectation to track/control the egress of personnel who have unescorted physical access to Medium Impact BES Cyber Systems. Table R1, Part 1.3 in the Measure column strike “and egress”. The requirement is to “restrict access” and there is no requirement expectation to track/control the egress of personnel who have unescorted physical access to High Impact BES Cyber Systems. Table R1, Part 1.6 add the text “except during CIP Exceptional Circumstances” to the end of the requirement. FE believes a suspension of logs is warranted for the situations defined.
No
R2, part 2.1 revise the requirement to describe “visitors” as “known individuals or guests of the Responsible Entity” rather than just “individuals not authorized for unescorted physical access”. The reason for the suggested change is to alleviate any perception that a responsible entity may need to self report for this requirement in situations involving criminal theft or break-in within a Defined Physical Boundary protecting a BES Cyber System. FE suggests that the text with the parenthesis be revised to state “(individuals who are known or guests and not authorized for unescorted physical access)”
Yes
No
R1 Lower VSL, refers to Part 1.7, however, there is no part 1.7 in the requirements Table for R1. FE believes the 1.7 reference should be revised to Part 1.6. R1 High VSL, FE requests the drafting team remove the second item described in the High VSL text. The VSL describes an entity who failed to “initiate a response within 15 minutes” upon being alerted of unauthorized physical access into a Defined Physical Boundary. FE believes this VLS violates FERC Guideline 3 as stated in FERC’s June 19, 2008 Order on VLS. FERC’s Guideline 3 indicates VSLs should be consistent with the corresponding requirement and that the VSL should not expand upon requirement expectations. This portion of the High VSL refers to Part 1.6 which is related to logging physical entry into a Defined Physical Boundary. However, the VSL text does not appear to fit with any of the various rows of the requirements described in Table R1 (parts 1.1 through 1.6).
No
We suggest a change to the title of Table R1 to “Physical and Logical Ports” since “Services” is not included in requirements (part 1.1 and part 1.2) listed in the table. If “services” is brought back into the requirement for R1, we request the SDT to clarify its intent for “services”. 1.2 – We suggest a change to the requirement as follows: “Through technical or procedural controls, disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.
No
2.2 - It should be clear from the requirement that a remediation plan is not required if an entity planned on never installing a particular patch due to operational risk. If the remediation plan can state that the entity will 'have other layers of defense in place' then this should be explicitly clear and allowable in the requirement and measure. 2.3 – The requirement sentence is incomplete and we suggest the following wording: “Implement and document a process for remediation, including any

exceptions for CIP Exceptional Circumstances".
No
3.3 – We believe it should be clear in the requirement that the entity can evaluate malicious code protections for applicability and only implement the ones that apply to their specific environment. Activating every signature that gets released for an IPS device can impact the performance of the IPS and adversely impact the reliability of the BES. Furthermore, we believe that 30 days is too short of a timeframe for some entities. We suggest the following wording for 3.3: "Evaluate malicious code protections for applicability and potential adverse impact to the BES. Based on that evaluation, update applicable malicious code protections that are not expected to adversely impact the BES within 60 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns."
No
4.1 – For clarification, we suggest replacing the wording "Log generated events" with "For devices that can generate logs, log generated events…" 4.1.4 – We ask that the team add guidance and examples in the guideline and technical basis section regarding the phrase "potential malicious activity". 4.4 – In the applicability, we suggest changing "Medium Impact BES Cyber Systems at Control Systems" to "Medium Impact BES Cyber Systems with External Routable Connectivity" for consistency with the other subrequirements of R4. 4.5 – We are not sure of the justification for performing these reviews every two weeks. We suggest this time period be changed to "every calendar month".
No
5.1 – We propose deletion of this requirement as it appears to be redundant with CIP-005-5 R2.3 5.1 (Measure) – We ask the team for clarity around the use of the phrase "internal and remote paths". Is internal someone who is on the corporate network and getting into a CIP ESP and remote someone who is outside the corporate network (say on VPN)? Or is internal someone in the CIP ESP and remote is anyone on the corporate side connected into the CIP ESP via terminal servers and firewalls? 5.4 – For clarification, we suggest changing the Applicability and Requirements components of this part of R5. We suggest changing Applicability from "All Responsible Entities" to: "BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" We suggest changing the Requirements language to: "Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application. For the purposes of this requirement an inventory of Cyber Assets is not required." Without this change, it is unclear if the Requirements language may mean that such procedural controls are not needed when the cyber asset in question is, for example, a BES Cyber Asset. 5.5.2 – We suggest replacing "BES cyber system" with "BES cyber asset".
No
R2 SEVERE VSL - 1st section – We suggest changing "...did not identify a source or sources.." to "...did not identify sources...". In the 2nd section we suggest splitting these into two to make it clear; one should focus on the 30 day limit and one on not identifying. R3 HIGH VSL – The first section appears to duplicate what is stated in HIGH and suggest it be removed.
No
1.3 – We suggest removing 1.3.3 since this is covered in the proposed EOP-004-2 Event Reporting standard.
No
We suggest that 2.1 and 2.2 be switched so that the implementation comes before the incident response. 2.1 – We suggest rewording this requirement as follows: "For actual or simulated BES Cyber Security Incidents, the incident response plan(s) must be used and include recording of any deviations taken during the implementation of the plan." 2.3 – We suggest removing this subrequirement because this is dealing with retention of evidence already covered in the compliance section of the standard.
No
We believe that the Applicability of this whole standard should be to "All Responsible Entities" since it is requiring the development, implementation, and review of BES Cyber Security Incident plans. Therefore, the applicability of 3.2, 3.3, 3.4, and 3.5 should be "All Responsible Entities". 3.2 and 3.3 – We suggest the team consider moving these subrequirements under the umbrella of requirement 2

since they relate to testing and would seem to flow better in that requirement. 3.4 – We suggest changing the last phrase “that impact that plan” to “that impact the ability to execute that plan” to alleviate the burden of minor changes. Also, in many cases for large entities it may take longer than 30 days to update the plan and ask the team to consider 60 days.
No
1.3 – We suggest removing “protection” from the requirement and measure since protection of information is covered in new standard CIP-011-1. 1.4 – We suggest removal of the phrase “initially after backup” in the requirement since “ensuring the backup process completed successfully” already covers the intent. 1.5 – We suggest adding after “Preserve data” the following: “without impacting recovery efforts” to make it clear that recovery of critical information is of utmost importance and that if preserving data is possible after the recovery efforts, then 1.5 would apply. We therefore also ask that “where technically feasible” be removed. Lastly, we suggest the removal of “before proceeding with recovery” in the measure. Our suggestions align with FERC Order 706 Par. 708 in which FERC said in part “…recovery of critical cyber assets and the Bulk-Power System is of immediate critical importance, and information collection efforts should not impede or restrict system restoration.” General comments not specific to R1: ♣ We question why some of the subparts of the requirements in CIP-009-5 include “at Control Centers” in the applicability while others do not. For example, what would be the purpose of having a recovery plan per R1 for all Medium impact assets, but not require it to be implemented in R2. We ask the team to assure the applicabilities in CIP-009-5 are appropriate and consistent with the requirements. ♣ We suggest the removal of the phrase “initially upon the effective date of the standard and” because if the team intends for certain activities and requirements be completed by some date, then this should be clearly stated in the CIP Version 5 implementation plan and is not appropriate in the requirements. ♣ Purpose statement – we suggest the removal of the phrase “related to the storing of backup information” from the purpose. We believe this constrains the purpose of this standard since some information is not necessarily stored but continually changed and recovered. ♣ The headings in the columns on page 11 of 23 need to be adjusted as they all say “Part”. ♣ We ask that the guideline and technical basis section include the text of the referenced FAQs and CIPC guideline. ♣ We suggest the “Purpose” statement of the standard be changed. We suggest replacing '…plans(s) related to the storing of backup information are put in place for BES Cyber assets…' with '… plan(s) are in place for BES Cyber Assets…' ♣ We ask that the team attempt to make it clear in the standard on the use of the terms “recovery” versus “restoration”. In the “Disaster Recovery” world those have very different meanings and are not interchangeable.
No
2.1 – In the third bullet of the requirement, we suggest removing the term “full” and just use the phrase “with an operational exercise” in both the requirement and the measure. Incidents that occur usually only affect a portion of the system and only a portion of the recovery plan will be implemented. For example, testing 'failover' or 'restore-from-backup' of a small number of key EMS servers would be examples of partial exercises compared to a full test of all 100+ EMS servers all at one time (which is not possible for an entity without affecting the BES). 2.2 – We suggest removing the second word “any” and re-wording the phrase “backup media initially”. We suggest a rewording of the requirement as follows: “Test information used in the recovery of BES Cyber Systems that is stored on backup media (1) to ensure it is operational before use and (2) at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is still useable and reflects current configurations.” 2.3 – For consistency with other requirements and measures that mention periodic activities, we suggest changing the phrase “at least once every 39 calendar months” to “every 3 calendar years not to exceed 42 calendar months” in both the requirement and measure.
No
3.2 and 3.3 – We suggest combining these subrequirements into one subrequirement and allow 60 days for the review and update of the plan. We suggest the following wording for the new combined requirement: “Within 60 days of a test or actual incident, review the results of the recovery, document any deficiencies or lessons learned, and update the recovery plan based on any documented deficiencies or lessons learned.” 3.5 – The use of 'each' implies that we must prove that each person actually reviewed the updates. Suggest removing 'all' and 'each'.
No

General – Correct typo in first sentence of guideline and technical bases for R3; “note” instead of “not”. 1.1 – In 1.1.4, we suggest adding the word “installed” between “Any custom”. 1.1 (Applicability) – We suggest the removal of “Associated Protected Cyber Assets”. These are non-critical devices that happen to be in the ESP and believe the need to track the baseline configuration for these devices does not add any reliability benefit. 1.1.2 – In the guideline and technical basis section, we ask the team to add clarification with regard to “version” and the level of detail needed. And what is the expectation of applicability for appliances (e.g. HMCs) or for application ports (e.g. TCP/IP ports) where OS is not clearly defined like a Windows server? 1.1.3 – We are not clear as to the reason for the term “intentionally” and suggest it be removed. 1.2 – We suggest replacing the first phrase of the requirement “Authorization, by a CIP Senior Manager or delegate, and document” with “Document approved”. We believe it would be cumbersome and do not believe it is necessary to have the CIP manager or delegate in this requirement. From an overall policy standpoint per CIP-003-5 R5, this authorization and delegation is already covered in the “Configuration Change Management” portion of the cyber security policy. 1.3 – We suggest the removal of the phrase “and other documentation required by a NERC CIP Standard, including identification and categorization”. This phrase should be removed because this is adequately covered in other standards and may cause double jeopardy as a result. For example, identification and categorization of BES Cyber Systems changes is covered by CIP-002-5 R1 part 1.1. 1.4 – In 1.4.2, we suggest replacing the phrase “these required controls” with “the required cyber security controls” for consistency with the rest of the requirements in 1.4. 1.5 – We suggest striking the phrase “for Control Centers”. This is already captured in the High Impact BES Cyber System applicability since all High Impact systems are at control centers per Att. 1 of CIP-002-5.
No
2.1 – We suggest replacing “monitor for” with the phrase “utilize automated monitoring of”. This will align with the intent of the requirement as stated in the guideline section of the standard which says “the intent of R2 is to require automated monitoring of the BES Cyber System.”
No
3.1 and 3.2 - We suggest the removal of the phrase “initially upon the effective date of the standard and” because if the team intends for certain activities and requirements be completed by some date, then this should be clearly stated in the CIP Version 5 implementation plan and is not appropriate in the requirements. 3.3 – We suggest this requirement be made more specific as to when a modification requires an assessment. A broad requirement for an assessment for each and every modification is burdensome with no added reliability benefit for many of the modifications. FERC, in par. 547 of Order 706 made this clear and provided examples as follows: “…we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment. For example, we would anticipate that updating an attack signature file on the electronic access point would not require an active vulnerability assessment, but replacing the devices that comprise the electronic access point would require an active vulnerability assessment.” 3.3 – If our suggestion above for completely removing requirement 3.3 is not accepted, we suggest removing “Associated Electronic Access Control and Monitoring Systems” from the applicability for consistency with 3.2. Otherwise we would like clarification on the reasons for the difference.
We suggest adding references to the subrequirements for each VSL explanation in the Table of Compliance Elements.
No
Part 1.1 of Table R1, we suggest adding the words “evaluate and” between “to identify” so that the requirement reads “One or more methods to evaluate and identify BES cyber system information.” The proposed change is to better clarify the intent of the requirement. Part 1.1 of Table R1. The second bullet in the measure should not be included in this standard. The referenced training materials are covered in CIP-004, R2 Part 2.6 and not pertinent as a measure to this CIP-011 requirement. Heading of page 11 and 12 should be Part, Applicability, Requirements and Measures from left to right. Part 1.2 of Table R1, strike “procedures for” and replace with “of” in requirement to read, “Access control and handling of BES Cyber System Information”. The change is proposed to avoid any potential inadvertent interpretation that the requirement is merely assessing a documented procedure. The introductory R1 statement sufficiently covers implementation of a documented process. Part 1.2 of Table R1, add in Measures bullet 1 “BES Cyber System” and strike “in a manner” to read “Records indicating BES Cyber System Information that is stored, transported, and disposed

consistent with the documented process; Part 1.2 of Table R1, strike from Measures bullet 2 “with user access implemented on a need to know basis” to read “Records from an information management system containing electronic copies of BES Cyber System Information”. The text proposed for removal is not pertinent as a measure to this CIP-011 requirement and covered in CIP-004, R6. Part 1.2 of Table R1, add in Measures bullet 3 “BES Cyber System” and strike “with keys provided to only authorized individuals” to read “Hardcopies of BES Cyber System Information stored in a locked file cabinet”. The text proposed for removal is not pertinent as a measure to this CIP-011 requirement and covered in CIP-004, R6.Part 1.3 of Table R1, Strike the phrase “Initially upon the effective date” and the word “thereafter” so the revised requirement reads “At least once every calendar year, not to exceed 15 months between assessments …”. 1.3 – We suggest replacing “implement an action plan” with “initiate an action plan”. An action plan may take more than a year to complete and the requirement could be interpreted as requiring it to be completed annually. 1.3 - We suggest the removal of the phrase “initially upon the effective date of the standard and” because if the team intends for certain activities and requirements be completed by some date, then this should be clearly stated in the CIP Version 5 implementation plan and is not appropriate in the requirements.

No

General – We believe it would be helpful if the team added guidance or explicit language in the requirements with respect to media that is still in use but then the location becomes it is used in becomes “CIP-declassified”. Footnote “2” – We suggest that it would be more enforceable and mandatory if BES Cyber Asset Media was defined as stated in the footnote and be added to the NERC glossary of terms. 2.1 – We suggest changing the first part of the requirement “Prior to the release for reuse of BES Cyber Asset media…” to “Prior to redeployment of BES Cyber Asset Media outside the Electronic Access Perimeter…”. The ESP concept exists in the current wording of this requirement in CIP-007-3 R7.2 and therefore should be carried over into the proposed 2.1.

No

R1 VSL – The use of the term “periodically” in the HIGH VSL is not used within requirement R1 and should be removed. R2 VSL – We ask that the drafting team write the severity levels to be more granular with respect to the type of device being disposed. For example, it seems that not properly wiping a flash drive is not the same severity as not wiping a firewall.

No

We support the proposal to retain V3 while transitioning to V5 if the collective industry (Entities, NERC and FERC) achieve a timely approval of V5 prior to V4 becoming effective. However, the 18 month timeframe does not allow sufficient time to complete capital budget cycles and we suggest a 24 month implementation. Lastly, the SDT should consider a staggered implementation plan that would allow for focus on the high impact and medium impact items first, and then followed by the low impact items. This would ensure proper focus and attention is given to the more important items for BES reliability without distraction and attention being diverted to lower cyber asset issues. Lastly, references within periodic requirements that indicate “initially upon the effective date of the standard” should be moved into the Implementation Plan and removed from requirement language. This ensures clear prerequisite expectations upon the initial effective date of the standards and allows for more concise and clear requirement language.

Group

NERC Standards Review Subcommittee - ERCOT Region

Andrew Gallo, Chair

Yes

The definition of “BES Cyber System Information” should include only floor plans, diagrams, equipment layouts, etc. that clearly delineate the cyber assets in some way. In other words, if the diagram denotes a device as a “Schweitzer” relay (or even an “SEL 2030”), the information should not require special treatment. Refer to additional comments submitted for Question 49. The SDT should also re-think including data in the definition of Cyber Assets. Additionally, “suspicious” is not an auditable term and ought to be removed. The same is true for “attempt.” It is not clear which “attempts” justify reporting. Reportable BES Cyber Security Incident: Request that the drafting team keep this definition consistent with the efforts of the 2009-01 project team. The current definition does not align to the requirements listed in the new version of EOP-004. BES Cyber Security Incident: A malicious act that: •Compromises a BES Cyber System or BES Cyber Asset, or •Disrupts the operation of a BES Cyber System or BES Cyber Asset, or •Results in unauthorized physical access into

a Defined Physical Boundary. BES Reliability Operating Services: we note the following: •“Identify and monitor flow gates” under “Managing Constraints” seems to be missing its bullet •We recommend clarifying that the use of the word “Facility” means the NERC Glossary definition -- in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication” •Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" •For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret. CIP Exceptional Circumstance: We request revision to “A situation that may involve one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance (internal or external), a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.” The definition needs some flexibility for entities to take appropriate measures without risking reliability of the BES that may not fit neatly into the conditions listed. CIP Senior Manager: Replace “NERC CIP Standards” with “NERC CIP-002 – CIP-011 Standards” because CIP-001 is not part of this set of standards. Control Center: We are concerned with the broadness of this definition. The SDT should consider the impact on small entities that will be affected by a broad definition of Control Center. In the proposed definition, the SDT uses the defined term “System Operator” which is “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” If the SDT’s intent was to limit Control Centers to BA, TOP, GOP and RC functions, we support the definition and request that the SDT make this limitation clear in the definition or in guidance. Intermediate Device: Recommended changes: “A Cyber Asset that 1) may be used to provide the required multi-factor authentication for the Interactive Remote Access; 2) may be a termination point for required encrypted communication; and 3) may restrict the Interactive Remote Access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside an Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network.” Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity’s Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access may be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

Yes

Attachment 1, Section 2.13 assigns a Medium Impact to "generation control centers that control 300 MW or more of generation." Control Center is a NERC-defined term; however, because "control center" is not capitalized in 2.13, it creates confusion because it could be interpreted that a typical control room of a combined cycle unit could be construed as a "control center” by the Regional Entity. The SDT should capitalize the term in 2.13 to make it clearer. We recommend adding a threshold for BAs similar to CIP-002-4. Change to “Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority that includes control of two or more of the assets identified in criteria 2.1, 2.3, 2.4, 2.12.” We do not agree with the inclusion of all Transmission Owner (TO) control centers. These may include local distribution "dispatch rooms" with visualization capability and minimal control of BES Facilities. We recommend removing “TO” from Attachment 1, 1.4 and 2.13. Alternatively, if TOs must be included, we recommend using the qualifier similar to what the SDT drafted in the guidance: "agreements where some of the functional obligations of a Transmission Operator [are] delegated to a Transmission Owner (TO)" (i.e. Replace “Transmission Owner” with “Transmission Owner, assigned by agreement, the functional obligation of a Transmission Operator”). The addition of a “Low Impact” rating for every generation facility that does not meet the High or Medium Impact thresholds constitutes a significant change in the CIP Standards. This change forces every registered GO and GOP to adhere to approximately 40 requirements in the remaining CIP standards when, currently, those generators are not listed as Critical Assets. It seems unlikely that the cost to adapt existing corporate cyber security policies, cyber security awareness and cyber asset access management to these NERC CIP requirements will lead to a corresponding reliability benefit. In addition, Regional Entity audit resources would be better served if allowed to focus on more critical locations. We recommend this category be eliminated. Criterion 2.7 seems to have been modified to include some transmission substations operating at 200kV to 300kV. The present Version 4 bright-line criterion includes only those operating above 300kV. Because this includes substations interconnected to generators, it seems likely that 200kV substations newly

identified as “Medium Impact” could include some generation facilities as well. This would require a whole new level of regulatory compliance to facilities not included under the Version 4 Standards. There is no reason to believe the Version 5 criterion better identifies critical substations than the Version 4 criterion. This criterion should be changed back to the one approved by the industry in CIP-002-4. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal? In 2.12, “system” and “Facility” are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned.

No

For clarity, we request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days of when a change to BES Elements and Facilities is placed into operation.” For clarity and consistency with the previous suggested change, request changing M1 from “as required in R1 and list of changes to the BES)” to “as required in R1 and list of changes to the BES Elements and Facilities)”. The word “intended” should not be used in the requirement because it is not auditable. Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Part 4 needs clarification. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementing CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion framework. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. The SDT should consider an approach that would have documentation “requirements” in a guidance document rather than in the requirements in the standard. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is too complicated. In addition to the BES Cyber Assets classified as high, medium and low in CIP-002, the other standards introduce ten additional categories of assets to protect in various ways: •Associated Physical Access Control Systems •Associated Protected Cyber Assets •Associated Electronic Access Control or Monitoring Systems •Electronic Access Points (with External Routable Connectivity) •Electronic Access Points (with dial-up connectivity) •Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries •Transient Cyber Assets •Medium Impact BES Cyber Systems with External Routable Connectivity •Medium Impact BES Cyber Systems at Control Centers •Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some appear in the standards themselves and these categories may or may not be included in the definitions document. This approach is complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future interpretations, CANs, etc. The Standards should be revised so that CIP-002 defines all assets needing protection rather than being introduced throughout the Standards. We recommend replacing “30 calendar days” with “90 calendar days.”

Yes

Recommend adding the following: “…has had its CIP Senior Manager or delegate review and update…”

No

The SDT should re-think the use of a “CIP Senior Manager.” In many organizations, there will not be one senior manager responsible for implementing the CIP Standards. For example, in some organizations, SCADA/EMS and Relay personnel report to one senior manager, but I.T., Security and H.R. personnel report to a difference senior manager (or managers). Yet, the SCADA/EMS, Relay, I.T., Security and H.R. all have roles in CIP compliance. A better approach would be for the Standards to require that a Senior Manager be designated for each Standard (or requirement), but it need not necessarily be the same Senior Manager for each Standard (or requirement).

Yes

Request clarification of the meaning of “implement” M2.2.

Yes
"Each Responsible Entity shall review each of its cyber security policies and obtain approval of the policies by its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals." As written, the requirement appears to require approval of the CIP Senior Manager rather than of the policies.
Yes
No
Please see our comments in response to Question 6, above.
Yes
We recommend changing "30 calendar days" to "90 calendar days." The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from "Changes to the CIP Senior Manager and" to "Changes to the CIP Senior Manager or".
Yes
Providing Security Awareness is useful and should remain in the Standard. However, the SDT should re-think the need to have a Security Awareness Program. So long as the Registered Entity provides security awareness quarterly, the program adds no value and is merely another "compliance document" to maintain, review, update, etc.
Yes
Most of the requirements in R2 make sense. However, providing training on "physical access controls" is not necessary. The physical access controls are – generally – pretty straightforward (e.g. card key readers). It does not seem necessary to provide "training" on how to use a card key. The same can be said for training on electronic access controls. Most of those access controls merely involve two-factor authentication or something similar. The need to provide "training" on how to log on to devices is unnecessary. We recommend removal of R2.3 and R2.4 because they appear redundant to R2.2; alternatively, some explanation of the difference between R2.2 and R2.3/R2.4 should be provided. With respect to R2.8, it seems unnecessary to require training on recovery plans except for those very few employees who must implement the recovery plan. As currently worded, it is not clear whether only those who implement recovery plans must receive training. With respect to R2.10, it seems unnecessary to require training on the systems' electronic interconnectivity and interoperability with other cyber assets. Generally, the personnel doing the "care and feeding" of those assets already know how they work and how they interconnect and interoperate. The personnel using those devices have no need to know about the interconnectivity and interoperability of the assets. Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement.
Yes
Yes
For all R4 table entries, we recommend changing "documented risk assessment program" to "documented personnel risk assessment program" to avoid confusion with a corporate risk assessment program. For R4.2, we recommend adding language to "grandfather" previous seven-year criminal checks executed for the previous version of the CIP Standards. The additional language should spell out when this "grandfathering" expires (which will be when a new check is required).
No
For clarity, recommend changing 5.1 from "authorized electronic or unescorted physical" to "authorized electronic or authorized unescorted physical". For R5.2 recommend adding language to "grandfather" previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this "grandfathering" expires, which is also when a new check will be required.
No
The CIP Senior Manager should not necessarily have a role in R6.1, R6.2 and R6.3. There should,

instead, be a particular person designated as the “gate keeper” for each cyber asset and physical security area. For example, the SCADA/EMS manager is the logical person to grant access to the SCADA/EMS system, not necessarily the “CIP Senior Manager.” [We realize that, under the Standard, the CIP Sr. Mgr. can delegate the responsibility to a “gate keeper.” However, doing so simply creates another document (the delegation) to maintain, review, revise, etc. It makes more sense to just create the “gate keeper” concept.] The Registered Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. In R6.1, we recommend changing “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except.” Also, change “minimum necessary” to “minimum the responsible entity considers necessary.” In R6.2, 6.3, 6.5 and 6.6, change “minimum necessary” to “minimum the responsible entity considers necessary.” For 6.4, request clarification of whether variances noted in the verification would be required to be a self report. For 6.6, we request clarification of whether variances noted in the verification would be required to be a self report. In the measure for R6.6, change “BES Cyber System information” to “BES Cyber System Information.”

No

In Part 7.1, the use of “at the time” of the resignation or termination is vague and ambiguous. For example, if a person informs the utility that his/her resignation is effective in three weeks, must the utility revoke access when informed of the resignation or when the resignation becomes effective? We recommend making the requirement seven days. We recommend moving the text in the footnote for 7.1 into the requirement. For Part 7.2, we recommend requiring only that the revocation occur as part of the next quarterly review. Those personnel have merely been reassigned or transferred. They do not pose a risk to the BES (as opposed to, for example, an involuntarily terminated employee). It makes sense that people deemed to be a risk (i.e. those terminated for cause) should have a very short timeframe for revocation. However, for people in good standing who are transferred or reassigned, the time frame has gone down from a seven-day permissible time frame to a single day. This seems an unnecessary burden that will cause utilities to incur costs needlessly (i.e., overtime pay to do revocations on Saturdays, as most people who resign or get reassigned or transferred would likely do so effective end of business Friday). Again, these costs and obligations seem reasonable for terminations for cause, but hard to justify for employees in good standing. Recommend changing 7.3 to “For resignations or terminations, revoke the individual’s access to BES Cyber System Information by the end of the calendar quarter in which the resignation/termination occurs.” For Part 7.4, revoking a person’s overall access to cyber systems should suffice. In other words, if a person must be on your corporate network in order to gain access to critical cyber systems, revoking overall network access should suffice to meet the Standard (as opposed to revoking the person’s access to the various individual systems). If this language remains, we believe it should be revised as follows: “For resignations or terminations, revoke the individual’s user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within ninety (90) calendar days of the date of initial access revocation.”

No

There should be a “lower” and “moderate” VSL for R1 through R3 (e.g. For R1, a “lower” VSL could be if awareness reinforcement was done only two times in a year; a “moderate” VSL could be if awareness reinforcement was done only three times in a year). For R5, we recommend the following language: “Personnel risk assessments are not updated at least once every seven years. (5.2)” Also for R5, the “severe” VSL contains the following language: “The Responsible Entity did not have a documented process for personnel risk assessments.” Failure to have a documented process for PRAs should not involve a severe VSL. The important question is whether PRAs are being performed; not if there’s a documented process for performing them. In other words, if a utility can demonstrate it is performing PRAs (correctly and timely), it should not matter whether the utility has a documented process to perform PRAs.

Yes

For R1 there is an issue of auditability regarding Low Impact BES Cyber Assets. If an entity need not create a list under CIP-002, there is no way to ensure the technical and procedural controls have been applied. Request clarification for when Low Impact BES Cyber Systems are in the ESP with High/Medium BES Cyber Systems. Are such Low Impact BES Cyber Systems subject to 1.1 or 1.2? There is also some disagreement over the VRFs for this Standard. Currently, the VRF is set at Medium. For part 1.1, that VRF should not be Medium but should instead have its own VRF of “Low.” We propose the following wording change to Table R1, Part 1.1: Requirement: An Electronic Security

Perimeter Procedure that defines operational or procedural controls to restrict unauthorized access. Measure: Evidence may include, but is not limited to, an Electronic Security Perimeter Procedure that describes the operational or procedural controls and additional evidence to demonstrate that this procedure was implemented such as, but not limited to, the signature of the CIP Senior Manger on the procedure. The Measures language proposed is similar to CIP-004-5 R1. We believe the use of the word “implemented” without further description may be interpreted to mean a Responsible Entity will need to provide a listing of Low Impact BES Cyber Systems and proof of protection on each individual device. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. Request clarification that the 1.3 and 1.5 Electronic Access Points are the Electronic Access Points identified in R1.2.

No

We recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset" to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset" because, as written, the requirement does not allow for the development of new technology. We recommend changing the Measure for R2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors."

Yes

We request clarification of Part 1.1’s Applicability because it does not identify which of High/Medium/Low BES Impact the Physical Access Control Systems are "Associated" with. We request Requirement 1.2 be updated to allow "escorted physical access." We propose the following wording change to Table R1 Part 1.1: Requirement: A Physical Security Plan that defines operational or procedural controls to restrict physical access. Measure: Evidence may include, but is not limited to, a Physical Security Plan that describes the operational or procedural controls and additional evidence to demonstrate that this plan was implemented such as, but not limited to, the signature of the CIP Senior Manger on the plan. The Measure language proposed is similar to CIP-004-5 R1. We feel the use of the term “implemented” without further description may be interpreted to mean a Responsible Entity will need to show how each Low Impact BES Cyber Asset is physically protected. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.3 be consistent (not add a Requirement) with Requirement 1.3, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary " to "Issue real time alerts (to individuals responsible for response) upon detection of a breach through an access point". Request similar changes to R1.5. For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6.

Yes

Requirement 2.2 requires clarification. If the intent is to require that visitors sign-in once each day, the draft language does not clearly set forth that requirement. As currently written, the language could be interpreted to require entry/exit logs “on a per 24-hour basis.” Such an interpretation would mean a Registered Entity would have to retain a great deal of paper (where logs are maintained on paper). This is especially true for an entity on a six-year audit cycle (which will have to maintain 2,190 individual daily logs for each facility). Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis,”.

No

Request clarification of 3.1 and 3.2on what the "Associated" under "Applicability" pertains to (i.e.: High, Medium, or Low BES Impact).

No

Request clarification on R1.1, is this at the BES Cyber System level or at the Asset level or can the

Entity choose? Request clarification on M1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Recommend that “of BES Cyber Assets” be removed.
Yes
We request clarification of Part 2.2 because it requires creation of a “remediation plan.” However, if the entity applies the patch, no remediation plan should be necessary. We suggest wording similar to the following: "create a remediation plan or a plan to mitigate the vulnerability if the Responsible Entity opts to not apply a patch or update." What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to each patch or the overall process? Recommend removing “CIP Exception Circumstances” since the conditions in the definition do not align with the circumstances that may prevent the implementation of the patch. Suggest wording like "process for completion of the defined implementation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied".
Yes
The Standard should make an allowance in Part 3.3 for signature/pattern updates that create system problems/issues. In the Requirement for Part 3.4, the words, “…Transient Cyber Assets and removable media….” should read, “…Transient Cyber Assets or removable media….”
No
Suggested wording: “Upon detection, activate a response to event logging failures before the end of the next calendar day. Please clarify the Requirement for Part 4.3. Does it require that the failure be detected within a calendar day or that a response be implemented within a calendar day of a failure being detected? The Requirement in Part 4.5 for log reviews every two weeks is too frequent. We recommend monthly reviews (which is still more frequent than the 90-day reviews in the previous version of the Standards).
Yes
In Part 5.2, the CIP Senior Manager or delegate should not have to authorize the use of administrator, shared, default, and other generic account types. The “owner” of the asset (e.g. the SCADA/EMS manager) should be able to authorize the use of such accounts. [We realize that, under the Standard, the CIP Sr. Mgr. can delegate the responsibility to someone else. However, doing so simply creates another document (the delegation) to maintain, review, revise, etc. It makes more sense to just let the asset owner authorize the use.] Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
Yes
Yes
For 2.1, recommended wording changes; "When a BES Cyber Security Incident is identified or tested, the incident response plans must be used and include recording of deviations taken from the plan." Please ensure that R2.3 aligns with the Evidence Retention section of the standard. Due to audit schedules, the entity may be required to retain the information for more than 3 years.
Yes
In Table R3, Part 3.2, 3.3, and 3.4 require different times for updates; 30 and 60 calendar days. We believe these times should coordinate with the plan in EOP-004-2 which allows 90 calendar days for update of the plan. For 3.3, recommend changing "Update" to "Where necessary, update”. Recommend changing "the completion of the review of that plan" to "the completion of the review performed in 3.2".
No
The VSLs need to align with the requested changes in questions 34-36.
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommended change: “When backing up Information essential to BES Cyber System recovery, verify the media to ensure that the backup

process was successful.”
No
For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 2.1, request change to “functional exercise” rather than “full operational exercise”. This is consistent with the information provided in the rationale. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported.
No
For Part 3.1, we recommend “and document any identified deficiencies or lessons learned” as that topic is addressed in CIP-009 R3.2. In Table R3, Part 3.2, 3.3, and 3.4 require updates within 30 calendar days. We believe these times should be consistent with CIP-008-5 updates and, as stated in our response to Question 36, should be changed to 90 calendar days for update of the plan. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
The VSLs need to align with the requested changes in questions 38-40.
No
Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold.
No
This requirement will be very difficult to meet and will require many technical feasibility exceptions. We suggest the SDT remove this requirement and address the FERC Order 706 directive in a cost benefit analysis that the cost of putting these controls on all High and Medium Impact BES Cyber systems outweigh the cyber security benefit.
No
For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 3.1, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend change for 3.2 “…perform an active vulnerability assessment in a test environment which models the baseline configuration of the BES Cyber System in the production environment.”
Yes
No
For 1.3, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it

very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered.

Yes

Footnote 2 in 2.1 should be moved into the body of the Requirement.

No

Overall comment to all proposed Standards: I.Black Start Issues There are several black start-related issues. First, in the current version of the Standards, a Registered Entity can have Critical Assets with no Critical Cyber Assets (CCAs). So, for example, a company may have black start units (i.e. Critical Assets) which have no associated cyber assets that use a routable protocol. As such, those black start units can be Critical Assets with no CCAs. As a result, the Registered Entity would not have to meet the NERC CIP requirements for the black start units. The same concept does not exist in the Version 5 Standards. In the Version 5 Standards, black start units will require CIP protections. That fact could have a chilling effect on entities. In other words, some entities may not bid their units into black start service because, by doing so, they would have to incur the expense of becoming NERC CIP compliant. In the ERCOT Region, black start service is not very lucrative and, therefore, some companies may refrain from bidding into black start service due to the expenses associated with being NERC CIP compliant (plus the fear of potential fines down the road). Additionally, many Blackstart units in the ERCOT Region are older, smaller units with very low capacity factors and limited revenue. Applying the “Medium Impact” CIP requirements on those units will result in the need for significant CIP investment and increased on-going operational costs as well as increased compliance risks. This may result in Generator Owners/Generator Operators not offering units for Blackstart service. It would also likely result in Blackstart units not being maintained in a manner appropriate to support Blackstart service because of the additional on-going cost, thus removing them as a future option for providing Blackstart service. With fewer units offered for Blackstart service, ERCOT may not have enough Blackstart Resources to effectively restore the ERCOT BES after a complete or partial system blackout event. We believe a Blackstart unit with no External Connectivity poses little or no risk to the BES and should be classified as Low Impact. We recommend the following modification to CIP-002-5, Attachment 1, to ensure the continued reliability of the ERCOT portion of the BES: “2.4. Each Blackstart Resource with External Connectivity identified in its Transmission Operator's restoration plan.” Blackstart Resources with External Connectivity would remain in the “Medium Impact” category; however, Blackstart Resources without External Connectivity would move to the “Low Impact” category. The Blackstart Resources in the Low Impact category would have the appropriate physical and cyber protection controls as listed in the current CIP Version 5 draft standard. Our understanding of CIP Version 5 draft standards is that External Connectivity is defined as having Routable or Dial-up connections through an Electronic Access Point. Another concern focuses on facilities downstream of the black start unit. For example, one company could be chosen to provide black start service from a generator, but a different company owns/operates the facilities along the cranking path. If that were the case, the transmission company would now have to incur the cost of becoming CIP compliant even though it is not compensated for those expenses. The same is true for facilities associated with the next-start unit. If the switch yard for the next-start unit is owned/operated by a company other than the one that won the black start bid, that next-start company may have to incur the cost of becoming CIP compliant even though it is not compensated for those expenses. Another question involves whether units that are black start capable must be NERC CIP compliant regardless of whether they are in the black start restoration plan. The reliability of the ERCOT system may be adversely impacted because units that have been updated to meet the NERC CIP Standards but not selected for Black Start service could be forced into mothball or retirement due to economics associated with maintaining NERC CIP compliance. Many such units are small, have small staffs and low capacity factors, do not run much during the year and may be running on the margin. If companies are reluctant to bid into the black start market due to the costs associated with being NERC CIP compliant, it could result in inadequate black start capability due to Generation Owners not bidding units into the black start market. Finally, we request clarity on the inclusion of “next start units” in the black start path. As CIP-002 currently reads, it could be interpreted that they are not included in the black start path; consequently, clarification is in order. II.Other Issues •We recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will

make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. •We request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. •We request clarification of the capitalized term "Facilities." Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5.
Individual
Nathan Mitchell
American Public Power Association
Yes
BES Cyber System Change: Replace Maintenance Cyber Asset with Transient Cyber Asset Justification: Maintenance Cyber Asset is not defined. BES Cyber System Information Change: Define "BES Cyber System Impact" Justification: It is assumed when the SDT uses the capitalized BES Cyber System Impact it is referring to CIP-002—5 Attachment 1 "Impact Categorization of BES Cyber Assets and BES Cyber Systems." The SDT needs to make this clear in a BES Cyber System Impact definition. CIP Senior Manager Change: Replace: "NERC CIP Standards" with "NERC CIP-002 – CIP-011 Standards" Justification: CIP-001 Reliability Standard is not part of this set of standards and has not been approved for inclusion in EOP-004-2. This will give clarity to the limit of the definition. Control Center Proposed Definition:"One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations:" Comment: APPA is concerned with the broadness of this definition. The SDT should consider the impact on small entities. Many dispatch centers or control rooms will be drawn into compliance by an overly broad definition of Control Center. In this definition the SDT uses the defined term: System Operators which from the glossary is: "An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time." If the SDT's intent was to limit Control Centers to buildings that house a System Operator with 24/7 staffing and include BA, TOP, GOP and RC functions, then APPA supports the definition and requests that the SDT make this limitation clear in the definition or in guidance. If this is not the intent of the SDT then APPA does not support the broader definition of Control Center. APPA points the SDT to our comments in Question 2 on CIP-002-5 Attachment 1 which conflicts with this limited scope of Control Center where 1.3 and 2.13 of Attachment 1 include TO control centers in the High and Medium Impact Rating. APPA is also concerned with the use of the term "facility" in the definition due to the fact that a generator control room may control multiple generators on the same site. This control room could be interpreted to be a Control Center if the current definition is approved. Therefore, APPA supports the comments of the Florida Municipal Power Agency (FMPA) on replacing the term "facility" with the term "site" to provide clarity that a Control Center controls generators or transmission substations at multiple locations. APPA recommended definition: "Control Center: One or more sites used for real-time operations by System Operators on a 24/7 basis to perform the Functional obligations of the RC, BA, TOP or GOP. These sites also host a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions for two or more BES generation facilities or transmission facilities, at two or more locations: (Continue with bullets in proposed definition) Reportable BES Cyber Security Incident Comment: APPA is concerned with the conflict between CIP V5 Reportable BES Cyber Security Incident and EOP-004-2 Reporting of Cyber Security Incidents. The SDT should coordinate with EOP-004-2 SDT to make sure there is no overlap of standards.
Yes
4. Applicability 4.1.2 Distribution Provider 4.1.6 Load-Serving Entity Comment: APPA is concerned with the new inclusion of DPs in the version 5 standards and with the qualifiers proposed for LSE in the Applicability section. APPA believes that this inclusion of this broad group of entities will draw in small entities with no operational capabilities and cause them to go through a paperwork drill of proving they either do not provide BES Reliability Operating Services or they do not have cyber assets associated with this equipment. APPA recommends that the SDT develop a simple method for DPs and LSEs to prove "No Impact – owning no BES Cyber Assets or BES Cyber Systems" therefore are clearly exempt from CIP-002-5 – CIP-009-5 and CIP-010-1 – CIP-011-1. APPA points to the comments of the Florida Municipal Power Agency (FMPA) which describes a "De Minimus Impact" category as an exclusion alternative. The SDT should discuss these alternatives as a way to address the burden on

small entities. Attachment 1 1. High Impact Rating 1.2 BA Control Centers Change: Add Threshold for BAs similar to CIP-002-4. Change to “Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority that includes control of two or more of the assets identified in criteria 2.1, 2.3, 2.4, 2.12” Justification: Some small BAs do not control multiple assets and designating all BAs would be burdensome to small entities. 1.3 TO/TOP Control Centers Change: Removal of Transmission Owner or Replace “Transmission Owner” with “Transmission Owner, assigned by agreement, the functional obligation of a Transmission Operator” Justification: APPA members are in strong opposition to the inclusion of "ALL" Transmission Owners (TO) control centers. These may include local distribution "dispatch rooms" that have visualization capability and minimal control of BES Facilities. APPA recommends the removal of TO from Attachment 1, 1.3 and 2.13 If TOs must be included APPA recommends using the qualifier similar to what the SDT drafted in the guidance: "agreements where some of the functional obligations of a Transmission Operator [are] delegated to a Transmission Owner (TO)." 2.13 TO/TOP Control Centers not included in High Impact Rating Change: Removal of Transmission Owner, or Replace “Transmission Owner” with “Transmission Owner, assigned by agreement, the functional obligation of a Transmission Operator” Justification: APPA members are in strong opposition to the inclusion of "ALL" Transmission Owners (TO) control centers. These may include local distribution "dispatch rooms" that have visualization capability and minimal control of BES Facilities. APPA recommends the removal of TO from Attachment 1, 1.3 and 2.13 If TOs must be included APPA recommends the qualifier given in the guidance: "agreements where some of the functional obligations of a Transmission Operator [are] delegated to a Transmission Owner (TO)" Change: Add to 2.13: (3) Balancing Authority control centers that control 300 MW or more of generation. Justification: If the SDT accepts the change proposed by APPA in 1.2 above, limiting the High Impact BA control centers then those not included in the High Impact Rating, but control more than 300 MW of generation should be included in 2.13. This will limit the burden on small BAs that do not control major flows in an interconnect. APPA points to the comments submitted by AECI and NRECA, which propose an additional criteria that will include Control Centers that “do not use protected data connections.” This proposed approach should be discussed by the SDT as an option for addressing the 706 directives, and reducing the burden on small BAs.

No

Requirement R1, 1.1 of CIP-002-5 Change: Replace “30 calendar days” with “90 calendar days” Justification: The SDT uses a number of different calendar days for reporting throughout the CIP standards. APPA recommends one consistent time of 90 calendar days.

Yes

No

R1 VRF/VSL Comment: APPA is concerned that a Responsible Entity will need to produce a list of Low Impact BES Cyber Assets to prove they have not “incorrectly categorized BES Cyber Assets at a lower category.”

Yes

Yes

Yes

No

Change: In Measure M4 second bullet: Replace: “Documented records that policies have been provided to contractors where access to BES Cyber Systems is authorized” with: “Policies are accessible to contractors when access to BES Cyber Systems is authorized.” Justification: This Measurement imposes a documentation and records retention burden, which is above and beyond the cyber security benefits to compliance. APPA suggests the above change so contractors have the same access to the policies, but the responsible entity does not have to prove they have given each contractor (individual) a copy of the policy. Change: In Measure M4 fifth bullet: Add: “Training is not required in R4, but would be acceptable evidence of compliance” Justification: APPA suggests the above qualifier to M4 fifth bullet since the measure implies the need for training, when the requirement specifies only awareness.

Yes
No
Comment: APPA recommends changing “30 calendar days” to “90 calendar days” to be consistent throughout the CIP standards.
Yes
Yes
Comment: APPA agrees with this programmatic approach to a culture of cyber security requiring all Responsible Entities to have a Security Awareness Program.
Yes
Yes
Yes
Yes
Yes
No
R7 Access Revocation Change: Replace “by the end of the next calendar day” with “within 30 days.” Justification: APPA believes that the Requirement in Table7 Part 7.2 for “reassignments or transfers” is extreme compared to the threat of cyber attack on the system by someone being transferred or reassigned for reasons other than disciplinary action. Even the SDT in their Change Rationale stated an objective; “to prevent a person from accumulating unnecessary authorizations through transfers.” This is not a threat to BES reliability it is only a cleanup activity and Responsible Entities should be allowed more than one calendar day to complete and show compliance. APPA suggests 30 days which is consistent with Part 7.5.
Yes
No
Electronic Security Perimeter Comment: APPA agrees with the SDT comments in their Change Description and Justification calling for “Entities are to document perimeter type security controls”. We feel this approach to a culture of cyber security requiring facilities with Low Impact BES Cyber Systems to be covered by an Electronic Security Perimeter Procedure will improve cyber security. However, APPA does not see this same programmatic approach in the Requirement and Measures in Table R1 Part 1.1. Therefore, APPA proposes the following wording change to Table R1 Part 1.1: Requirements: An Electronic Security Perimeter Procedure that defines operational or procedural controls to restrict unauthorized access. Measures: Evidence may include, but is not limited to, an Electronic Security Perimeter Procedure that describes the operational or procedural controls and additional evidence to demonstrate that this procedure was implemented such as, but not limited to, the signature of the CIP Senior Manger on the procedure. APPA points out to the SDT that the Measures language proposed is similar to CIP-004-5 R1. We feel the use of the term “implemented” without further description may be interpreted to mean a Responsible Entity will need to provide a listing of Low Impact BES Cyber Systems and proof of protection on each individual device. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets.
Yes
Yes

No
R1. Physical Security Plan Comment: APPA agrees with the SDT comments in their Change Description and Justification calling for “programmatic protection controls as a baseline”. We feel this approach to a culture of cyber security requiring facilities with Low Impact BES Cyber Systems to be covered by a Physical Security Plan will improve cyber security. However, APPA does not see this same programmatic approach in the Requirement and Measures in Table R1 Part 1.1. Therefore, APPA proposes the following wording change to Table R1 Part 1.1: Requirements: A Physical Security Plan that defines operational or procedural controls to restrict physical access. Measures: Evidence may include, but is not limited to, a Physical Security Plan that describes the operational or procedural controls and additional evidence to demonstrate that this plan was implemented such as, but not limited to, the signature of the CIP Senior Manger on the plan. APPA points out to the SDT that the Measures language proposed is similar to CIP-004-5 R1. We feel the use of the term “implemented” without further description may be interpreted to mean a Responsible Entity will need to show how each Low Impact BES Cyber Asset is physically protected. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. Comment: Table R1 Part 1.2, In the Requirement it specifically states that a Responsible Entity should “restrict access.” APPA interprets this as meaning to allow only authorized individuals into (ingress) the restricted areas. However, the Measures states both “ingress and egress is controlled.” Cyber security is not enhanced by logging out (egress) authorized personnel. APPA recommends removal of the word “egress” from the Measures and the SDT should give guidance that ingress logging is all that is required for compliance. Additional Requirement: APPA recommends the addition of a requirement in R1 that addresses the issue of Physical Access logs similar to the requirement in CIP-007 R4.4 for Cyber System event logs. APPA Proposed Requirement: Retain BES Physical Access Ingress logs identified in R1.6 for at least the last 90 consecutive calendar days. Justification: APPA is concerned with the need to retain 3 years of logs as proof of compliance, when current standard language and audit practice is for entities to show a process requiring retention of logs and showing the auditor that entities have the current 90 days of logs at a minimum.
Yes
Yes
Yes
Yes
No
R2: Security Patch Management Comment: In Table R2, Part 2.2 the Requirements state “create a remediation plan or revise an existing remediation plan.” APPA believes the term "remediation" should be changed to "mitigation or compensatory measures", since remediation implies that a patch or update is required to be applied. In some cases it may be known through testing that a particular patch interferes with the operation of the system. Applying a patch in these cases may reduce reliability.
Yes
R4: Security Event Monitoring Comment: In Table R, Part 4.2 the Requirement states; “Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.” APPA feels this is a fill in the blank requirement that Registered Entities will need guidance on developing a threshold for generating alerts. Question: In Table R4, Part 4.3 was it the intent of the SDT to require duplicate logging capability with the statement; “Detect and activate a response to event logging failures?”
No
R5: System Access Controls Comment: APPA points out to the SDT when requirements are applicable to All Responsible Entities including Low Impact BES Cyber Systems these requirements must address “programmatic protection controls” as commented previously. We feel this approach to a culture of cyber security requiring facilities with Low Impact BES Cyber Systems to be covered by programmatic

plans or procedures will improve cyber security. However, Table R5, Part 5.4 calls for “Procedural controls for initially changing default passwords,” in the Requirements, but in the Measures the first bullet says; “Demonstration showing default vendor passwords have been changed, sampled on a locational basis.” APPA recommends the following changes to the Requirement and Measures: Requirement: System Access Control Procedure for initially changing default passwords…” Measures: Evidence may include, but is not limited to, a System Access Control Procedure that describes the process for initially changing default passwords when new devices are deployed and additional evidence to demonstrate that this procedure was implemented such as, but not limited to, the signature of the CIP Senior Manger on the procedure. APPA points out to the SDT that the Measures language proposed is similar to CIP-004-5 R1. We feel showing default vendor passwords have been changed will require a Responsible Entity to identify all Low Impact BES Cyber Assets. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. APPA understands that High Impact BES Cyber Systems may need to undergo more stringent compliance requirements. If the SDT feels it is necessary to conduct sampling of changed vendor passwords, Requirement R5 Part 5.4 should be split into two Parts; one for Low / Medium Impact BES Cyber Systems and one for High.
Yes
No
R1: BES Cyber Security Incident Response Plan Specifications Comments: APPA is concerned with the possibility of violations of Requirements in CIP-008-5 conflicting with Requirements in EOP-004-2. APPA understands that CIP-008-5 is the “Incident Response Plan” and EOP-004-2 requires the development of an “Operating Plan for Event Reporting.” However, CIP-008-5 Table R1, Part 1.1 requires a process to “identify, classify, and respond to BES Cyber Security Incidents” while EOP-004-2 R1.1 requires; “A process for identifying events listed in Attachment 1.” APPA recommends the SDT revise the Requirement and Measure in Table R1, Part 1.1 to remove the terms “identify” and “classify.” Table R1, Part 1.2 requirement of a process to determine if an incident is a “Reportable BES Cyber Security Incident” is in direct conflict with Event Reporting Reliability Standard EOP-004-2. APPA suggests Part 1.2 be removed and coordinated with the EOP004-2 SDT. Table R1, Part 1.3.3 requires definition of “Internal staff and external organizations that should receive communications of the incident.” EOP-004-2 R1.3 requires “A process for communicating events in Attachment 1 to the ERO, the RC… and other appropriate entities.” APPA suggests Part 1.3.3 be removed and coordinated with the EOP004-2 SDT.
No
R2: BES Cyber Security Incident Response Plan Implementation and Testing Comments: In Table R2 Part 2.2 the Requirement states “initially upon the effective date” which implies that date is the only time this plan can be implemented. APPA suggest replacing the term “upon” with the term “by.” This will allow Responsible Entities to implement the plan prior to the effective date and be in compliance. APPA recommends that Table R2, Part 2.3 be removed or clarified. If the intent of the SDT was to require records retention for compliance that is covered in Section C1.2 Evidence retention and Part 2.3 should be removed from the standard. If it was the intent of the SDT to require Responsible Entities to have a “Procedure” for retaining Reportable BES cyber Security Incidents then the Requirements and Measures need to be reworded. APPA offers the following revision for Part 2.3 Requirement: Procedure for retaining relevant documents related to Reportable BES cyber Security Incidents for three calendar years. Measures: Evidence may include, but is not limited to, a records retention procedure that describes retention of Reportable BES cyber Security Incidents for three calendar years and additional evidence to demonstrate that this plan was implemented such as, but not limited to, the signature of the CIP Senior Manger on the procedure. APPA points out to the SDT that the Measures language proposed is similar to CIP-004-5 R1. We feel showing records retention of all documentation for Reportable BES cyber Security Incidents will be a major burden to Responsible Entities.
No
R3: BES Cyber Security Incident Response Plan Review, Update, and Communication Comment: In Table R3, Part 3.2, 3.3, and 3.4 require different times for updates; 30 and 60 calendar days. APPA believes these times should coordinate with the plan update requirement in EOP-004-2 which allows 90 calendar days.

Yes
No
R1: Recovery Plan Specifications Comment: Table R1, Part 1.5 - The requirement to "Preserve data where technically feasible" may impede the timely restoration of a BES cyber asset that is required for the reliable operation of the BES. For example, if an entity is required to create an image of an affected hard drive for forensic analysis or to send the device to a laboratory for analysis, this may interfere with the restoration of the system. Suggest changing the wording to "Actions to preserve data where such actions do not interfere with the restoration of the function of a BES Cyber System."
No
R2: Recovery Plan Implementation and Testing Comment: Table R2, Part 2.2 the Requirement states; “to ensure that the information is useable and reflects current configuration.” APPA believes the statement should read “to ensure that the information is useable and reflects currently approved configuration based on the CIP-010-5 Part 1.1 or 1.2 as appropriate.”
No
R3: Recovery Plan Review, Update, and Communication Comment: In Table R3, Part 3.2, 3.3, and 3.4 require updates within 30 calendar days. APPA believes these times should consistent with CIP-008-5 updates and as stated in Question 36 should be changed to 90 calendar days for update of the plan.
Yes
No
R1: Configuration Change Management: Comments: In Table R1, Part 1.3 the Requirement states; “identification and categorization of the BES Cyber System, as necessary.” APPA believes the statement “as necessary” gives the Responsible Entity the option to self identify those BES Cyber Systems that apply to this requirement. Therefore, APPA recommends the removal of “as necessary” from this sentence. In Table R1, Part 1.4.2 and 1.4.3 use the term “verify” and “verification” where the version 3 CIP-007 R1 uses “test.” APPA would like clarification from the SDT why this change was made and why the Requirement does not match up with the Measure which uses the term “test.”
No
R2: Configuration Monitoring Comment: APPA recommends the SDT go back to the drawing board on this requirement. This requirement is next to impossible to do physically and it will be a compliance nightmare with constant technical feasibility exceptions. Even the first words of the requirement are “Where technically feasible.” APPA strongly suggests that the SDT remove this requirement and address the FERC Order 706 directive in a cost benefit analysis that the cost of putting these controls on all High and Medium Impact BES Cyber systems far outweigh the cyber security benefit. APPA cannot recommend to its members an affirmative vote on the CIP standards if this requirement remains as written.
No
Comments: In Table R3, Part 3.2 the Requirement states; “perform an active vulnerability assessment in a test environment.” APPA requests the SDT define at a minimum a “vulnerability assessment.” Also, what is the difference between an “active” and “passive” vulnerability assessment.” The SDT needs to clarify what a “test environment” is compared to a “production environment.” APPA suggest the following change to the Measurements that may clarify the intent of the SDT:”Each entity must define the test environment reflective of the requirements as laid out in CIP-010 R1.4.” In Table R1, Part 3.4 the Requirement states; “action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of the action plan.” This requirement will be hard to prepare for audit since it will require a continuous update of the execution status in case of a spot check. APPA recommends removal of the statement;” including the planned date of completing the action plan and the execution status of the action plan.” from the requirement.
Yes
Yes

Yes
Yes
No
Implementation Plan: Change: Remove: “18 Months Minimum” Add: “24 Months Minimum” Rationale: CIP Version 5 will impact an increased number of Responsible Entities who are not included in the Applicability of the CIP Version 3 or Version 4 standards. Twenty-four months is needed to allow for sufficient operational planning and budgeting activities to successfully implement Version 5. In most cases, twenty-four months will allow for two budgeting cycles to deal with the organizational and financial considerations of Version 5 for those Registered Entities (many of which are small) who have not previously dealt with the myriad of CIP asset issues. We understand that 18 months was proposed to facilitate the potential avoidance of implementing Version 4 however, Registered Entities may need the option of using this additional six months to successfully implement Version 5 to avoid non-compliance issues. Again, many of these entities are small and have not previously needed to deal with cyber asset issues to the degree Version 5 will likely require.
Individual
Greg Rowland
Duke energy
Yes
• Overall comments o There are many capitalized terms in this document that aren’t defined terms, and aren’t proposed to be defined terms, so their capitalization should be removed. (These definitions (as well as the ones on NERC’s website) need a thorough review and revision.) o Throughout—Terms and especially acronyms used but not defined in this document are not all defined in the NERC Glossary of terms. (CIP, NERC, BES, EMS, SVC, and DMZ (see more on DMZ below)). Also, inconsistent use of acronyms--SVC, ATC and AVR are defined upon use in the document most of the other acronyms used are not. The NERC Glossary of Terms is now outdated with terms like Critical Cyber Asset. o Throughout—some definitions include parenthetically noted acronyms, such as Electronic Security Perimeter (”ESP”). Others, such as Protected Cyber Asset (PCA??) are not. Be consistent, with a preference from this entity to publish acceptable (industry-wide) acronyms to assist in communications between entities, regulators, auditors, etc. o Page 8 “Intermediate Device”: The definition of “Intermediate Device” uses the acronym “DMZ” to describe a “DMZ” network. Both the acronym and the term “DMZ network” should also be defined. (Please do NOT use the common, but incorrect term “Demilitarized Zone” (a physical area where military activity is banned, usually between two opposing forces), but rather the more accurate and effective “Demarcation Zone” (A line defining the boundary of a buffer zone or area of limitation) to define the acronym DMZ!) • BES Cyber Asset – More guidance should be provided on how the 15-minute time criteria is to be be applied. Need to define or better clarify the meaning of the phrase “adverse impact” so that the threshold is understood. “Adverse impact” could mean many different things. For example, the NERC-defined term “Adverse Reliability Impact” means “The impact of an event that results in Bulk Electric System instability or Cascading”. • BES Cyber Security Incident – Third bullet should be reworded to include attempts to gain physical access into a Defined Physical Boundary. • BES Cyber System – “Maintenance Cyber Asset” should be “Transient Cyber Asset”. • BES Cyber System Information – The phrase “BES Cyber System Impact Designations” should use a lower case “I” on the word “impact”. • BES Reliability Operating Services o Lead-in paragraph – “Operating Services” is not a defined term and should not be capitalized. o Balancing Load and Generation – Unit Commitment is not a real-time activity and should be deleted. Also under Load management, Demand Response, and Manually Initiated Load Shedding, the “Ability to identify load change need” is not a real-time activity and should be deleted. o Managing Constraints – ATC is a forward-looking business concern and shouldn’t be on this list. Also, “Interchange schedules” raises many questions. For example the IDC is a NERC tool; so what entity (or entities) are responsible for its protection? “Identify and Monitor Flowgates” is planning horizon work and shouldn’t be on this list. o Restoration of BES – Blackstart restoration bullet should be reworded as follows: “Blackstart Resources and Cranking Paths as identified in the Transmission Operator’s restoration plan.” o Situational Awareness – “Situational Awareness” is not a defined term. It’s unclear what is meant by the phrases “unplanned changes” and “Change management”. “Next Day planning” is not real-time and should be struck from this list. o Inter-Entity

Real-Time Coordination and Communication – The ISN is a virtual NERC tool that they manage. Who is responsible for identifying and protection? Also RCIS? • CIP Exceptional Circumstance – Strike the phrase “Cyber Security” in order to make this more broad. • Transient Cyber Asset – How does the 30-day clock work? What does “directly connected” mean? Does it matter if the device is shut down every night? What if it’s physically disconnected for one minute and then reconnected?
Yes
• Under 1.4, 2.12 should be 2.13 • 2.5 needs to be replaced with the language of 1.5 from CIP-002-4 Attachment 1, as follows: “The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.”
Yes
It is important to retain, and if possible, more clearly delineate the provisions for dealing with Low Impact BES Cyber Assets and BES Cyber Systems (i.e. “do not require discrete identification” and “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.”).
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
1. The rationale for R2 should be reworded from “...contains the proper policies...” to “...covers the required policies...” 2. Consider whether the role-based training approach adequately addresses Order 706 paragraph 435, where “any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions could, even inadvertently, affect cyber security.”
No
Measure 3.1 - Delete the phrase “the date access was first granted”, since this may not be available for all individuals currently having access.
No
4.1 – should the word “initial” be retained? The word “Initial” here could indicate that this new requirement must be done for existing individuals who already have access prior to V5 becoming enforceable. Consider rewording or a grandfather clause. 4.2 - “Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more.” Does six months apply to just the school

requirement or “resided and been employed” “Been employed” can be construed many different ways especially if a company covers many areas and locations. Clarify this to ensure it will be clear that it covers where the person actually worked… not where the corporate office is.
Yes
No
R6.1, 6.2, 6.3, 6.5, 6.6 – These requirements introduce the phrase “minimum necessary” regarding access permissions. Demonstrating compliance could become controversial and overly burdensome. Consider using Version 4 language phrases such as “need-to-know” and “confirm that access privileges are correct and that they correspond with the Responsible Entity’s needs and appropriate personnel roles and responsibilities.”
No
R7.1 - Need further clarification to allow for situations where people are out for a period of time (suspension, sickness, etc.) and then determine while that person is still out that they are being terminated or not returning. Access should be allowed until the determination is made they are not coming back – not as of the last day worked.
Yes
No
R1.1 - Measures should be “technical OR procedural controls” to match language of requirement. Propose removal of “and have been implemented” from the end of the measure statement to avoid tracking compliance on a ‘per-device’ basis, otherwise this would support the need for tracking this information for low impact BES Cyber Systems. R1.2 - Modify the applicability column to frame applicable Cyber Systems/Cyber Assets as those with External Routable Connectivity or dial-up connectivity. Also modify the requirements column to exclude ‘all routable and dial-up connectivity’ as the focus should be ‘external routable or dial-up’ connectivity (as covered within the proposed Applicability change). R1.3 - Although 'Deny by Default" is included in the Guidelines and technical basis it should be put back in the language of the requirement and only have criteria for granting access. R1.4 - There were various interpretations of ‘non-Interactive Remote Access,’ which implies this requirement may need some additional clarification, may look to merge R1.4 with R1.2. “where technically feasible” – Make clear that this is a TFE-able section?
No
R2 - Not all requirements make sense for both routable and dial-up connectivity - perhaps split out requirements? Have one set for expectations for routable connectivity and another set of requirements for dial-up? R2.1 - Applicability should include External Routable or dial-up connectivity as a filter. Suggest rewording to support placement of an intermediary device that may not be part of an ESP. R2.2 - Where does encryption supposed to start/stop - suggestion is to specify that encryption doesn’t need to extend past the intermediate device…otherwise it renders the IDS unable to evaluate the potential for malicious traffic.
No
Classifying instances where no documentation of compliance exists as severe is appropriate; instances in which a minority of non-compliance controls were identified within a primarily compliant program should be assessed a VSL with respect to the finding. VSLs addressing ‘each identified EAP’ and ‘all Interactive Remote Access’ should be assessed as a sliding scale to consider whether lower/moderate/high may be more applicable.
No
Conceptually we are good with this section with only editorial comments noted below: 1. Page 11, Part 1.2 “Measures” states “the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.” a. This measure implies a requirement to log egress from Defined Physical Boundaries (DFBs) for “Medium Impact” BES Cyber Systems. The registered entity feels that this requirement goes above and beyond existing systems and installations to restrict access to cyber assets by controlling and logging ingress only. The additional system complexities and costs to add additional hardware and system capacity to log egress to a number of facilities across service areas by all NERC members

is considered onerous and does not address any perceived or real risks where individuals vacate a protected area. 2. Page 12, Part 1.3 Measures a. Entity has the same comment on egress logging as above. Particularly, when access is now restricted for High Impact based on multi-factor access controls. 3. Page 13, Parts 1.4 and 1.5 Requirement statements require real-time alerts to be issued to individuals responsible for responding to unauthorized physical access. a. The intent of the drafting committee regarding required responses is not clear and could range from each entity defining the parameters of the actual responses, or that there is some undocumented implication that CIP-008 requirements should be used, based on prior versions of the standards. 4. Page 14, Part 1.6 Requirement statement "Log (through automated means or by personnel who control entry) of physical entry into each DPB…" a. This statement implies that self-logging cannot be done by personnel entering the DPB. In the case of an authorized individual accessing a DPB by two different physical locks and keys (providing the 2 different access controls to a High Impact DPB) there is implication that this access point must be manned by a second party to conduct the logging. If this is the intention of the drafting team, the registered entity feels this is not operationally or cost effective to implement by the industry. If this is not the intent of the drafting team, the registered entity requests clarification of the written requirement.

Yes

No

Page 18, Part 3.2 Requirement states the entity must "Log dates, time, and duration for failures or outages of access control, logging, and alerting systems." • Suggest for clarity that this statement be changed to use the defined term "Physical Access Control Systems" in place of "access control, logging, and alerting systems", words which are contained in the definition of "Physical Access Control Systems".

Yes

No

• Table R1 o R1.1 Requirement – Suggest changing language to "Disable or restrict access to unnecessary logical network accessible ports". This removes the need to document the justification for all enabled ports while still requiring the need to demonstrate that ports have been reviewed and limited. o R1.1 Measures – Suggest changing language to "Evidence may include, but is not limited to, documentation that only necessary ports remain enabled". o R1.2 Requirement – Suggest adding the following sentence to the end: "Restriction of physical ports can be achieved technically or procedurally via policy".

No

• Table R2 o R2.1 Requirement – Agree with EEI recommendations. o R2.2 Requirement – Agree with EEI recommendations. o R2.3 Measures – Agree with EEI recommendations.

No

• Table R3 o R3.3 Measures – Agree with EEI recommendations. o R3.4 Requirement – Suggest changing language to "Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to any Cyber Asset listed in the Applicability section". o R3.4 Measures – Suggest changing language to "Evidence may include, but is not limited to, an inventory of Transient Cyber Assets or removable media and the methods used to detect, deter, or prevent malicious code." o R3.5 All – Suggest deletion of this Requirement in full. Logging, especially that without any form of review, provides no assistance in the protection of BES Cyber Systems and is not explicitly required in Order 706.

No

• Table R4 o R4.1 Requirement – Agree with EEI recommendations. o R4.2 Requirement – Agree with EEI recommendations. o R4.2 Measures – Agree with EEI recommendations. o R4.3 Requirement - Agree with EEI recommendations. o R4.3 Measures - Agree with EEI recommendations. o R4.4 Measures - Agree with EEI recommendations. o R4.5 Requirement - Agree with EEI recommendations. o R4.5 Measures - Agree with EEI recommendations.

No

• Table R5 o R5.1 Requirement – Suggest changing language to "Authenticate user account access before granting electronic access to each Cyber Asset within the Applicability section, where

technically feasible." o R5.2 All - Agree with EEI recommendations. o R5.3 All - Agree with EEI recommendations. o R5.5 Requirement - Agree with EEI recommendations.
No
Agree with EEI recommendations.
No
We are good with this standard in general. Suggest the following improvement: Page 11 Part 1.2 Requirements statement a. This requirement does not provide guidance to a Registered Entity in terms of the reporting process for an incident that has been determined to be a "Reportable BES Cyber Security Incident". Suggest that language be added to point to current or drafted standards and requirements such as CIP-001-1a R4 or EOP-004.
Yes
Yes
Yes
No
1. Requirement 1, Part 1.3 (page 10) stating "One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality". Comment is that the "protection" requirement could be construed as being redundant with CIP-011 and put responsibility entities in double jeopardy regarding compliance to two standards rather than just one. I believe the intent of protecting the information is also reflected in Part 1.4 of this same standard (page 11). 2. Requirement 1, Part 1.5 (page 11) is not a good requirement. It states "Preserve data, where technically feasible, or analysis or diagnosis of the cause of events that triggers activation of the recovery plans(s) as required in Requirement R1." This requirement is much too specific and I believe misses FERC Order Section 739's and 740's stated intent "give responsible entities a high confidence level that their backups will actually restore the system as needed". These FERC Order Sections should be and in my opinion are covered in Part 1.4, not in this new requirement. If anything, this new requirement should state that the responsible entity should conduct and document a root-cause analysis to attempt to identify the reason a system had to be recovered. There is real value in that, but not in a requirement to preserve data (but with no requirement to do anything with it!) As well, some system failures are obviously not data related and this practice again would be of no real value to preventing future impacts to the BES.
Yes
Yes
Yes
No
• General Comment – Still poorly written and difficult to understand. Needs a Technical Writer to correct tense, language use, match grammar to intent, etc. • Page 8/bullets 2&3: What is the difference here between these two? • Page 10/middle column-1.1.4: Should the last word be 'Asset' instead of 'Entity'? Seems confusing… • Page 11/middle column: Why Sr. Mgr. for baseline deviation approval? Too far removed from the daily working details. Should be line mgr/supv. • Requirement asks for physical location to be part of the baseline. Recommend to replace with "unique identifier". • Recommend to allow using minimum security baseline documents/templates as a baseline configuration vs actual point in time view of configuration on actual asset being a baseline • Not clear if such baseline needs to be changed every time an update is performed (e.g. every time new patch levels are released). Recommend instead to allow baseline that states "patch levels need to be up to date (no older than XYZ) days" that would allow for more consistent process.
No
Recommend to specify how frequently the changes to the baseline need to be monitored. Also,

recommend to add criteria for distinguishing between different levels of deviation (high risk vs. low risk change/deviation) and appropriate response based on the level.
No
• Page 18/3.3/middle column: What is “CIP Exceptional Circumstance”? This is undefined and new. Why is this being introduced, and what is the intent? • Recommend to replace wording “…the controls are implemented correctly and operating as designed” with less subjective language, such as “verify against minimum baseline”. • Need definition on “CIP Exceptional circumstances” under requirement 3.3
Yes
No
Agree in full with EEI recommendations.
No
Agree in full with EEI recommendations.
No
Agree in full with EEI recommendations.
No
We believe that due to the extensive changes in Version 5, more than 18 months will be required. We propose 24 months, and the effective date should not be on January 1, due to the added degree of difficulty with a year-end roll-out.
Individual
RoLynda Shumpert
South Carolina Electric and Gas
Yes
BES Cyber System Definition: Is the drafting team going to provide more guidance on how a "system" is to be determined by registered entities? Do all assets included in a system have to reside in the same physical location? BES Cyber Asset Definition: Is this definition intended to replace the definition of Cyber Asset? Drafting team needs to provide clarification on the statement "The timeframe is not in respect to any cyber security event or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES". How does this statement apply to assets that don't necessarily operate the BES, but produce real-time information that could affect real-time BES operational decisions (e.g. ATC/AFC calculation engines)? Also, is it the drafting teams intent that this definition include auxillary assets related to facilities where the assets reside (e.g. Fire systems, HVAC, Halon system, etc.)? BES Reliability Operating Services Definition: Related to Balancing Load and Generation [Manually Initiated Load Shedding], is it the drafting teams intent that this include load shedding resulting from opening non-BES circuits? Related to Monitioring and Control [SCADA], is it the drafting teams intent that the SCADA system be categorized into an impact category as a whole, or broken up into seperate BES Cyber Systems? Related to Inter-Entity Coordination and Communication [Scheduled Interchange], how does the drafting team expect registered entities to handle third-party BES Cyber Assets associated with scheduling interchange transactions (e.g. OATi). What is the drafting team's expectation for securing BES Cyber Assets that are used by multiple entities and maintained and operated by a common external vendor or service provider?
No
No
Drafting team needs to address change in categorization from higher to lower impact, if registered entities portion of BES is modified or changes.
Yes
Yes
Yes

Yes
Yes
No
This is an ambiguous requirement. Drafting team needs to expand on expectations for making individuals aware. Does this require distribution, training, posting on company website etc.?
Yes
Yes
Yes
Yes
No
If training is role-based then why is the applicability to High and Medium BES Cyber Systems. This implies that anyone with access to these assets needs all of the training specified in 2.2 thru 2.10 and takes away the basis of a role-based training program.
Yes
Yes
No
The applicability is confusing here and does not align with applicability for the PRA program.
No
How does the drafting team expect registered entities to prove that "Access permissions are the minimum necessary to perform assigned work functions?" This introduces an entirely new concept for revoking access when an employee's work functions change and could become overly burdensome?
Yes
Yes
No
Part 1.3 has an applicability which considers routable connectivity for Medium Impact assets, but not for High Impact assets. Part 1.5 includes this consideration for both classifications. Is there a reason for this inconsistency?
Yes
Yes
Yes
Yes
No
Drafting team needs to clarify whether an outage of a Physical Access Control System is a violation of the standard. R3 seems to allow for this type of occurrence; however it is unclear.
Yes

Yes
Yes
Yes
No
Drafting team needs to clarify whether part 4.1.2 applies locally at the device level. This is unclear. R4.2 is too generic. There will be inconsistency across the regions in how this requirement is implemented.
No
The applicability is inconsistent on part 5.4. Is "All Responsible Entities" meant to represent all asset classifications?
Yes
No
Is "All Responsible Entities" meant to represent all asset classifications? Is it the drafting teams' expectation that separate incident response plans be developed for different asset classifications?
Yes
No
Why does the applicability change from all Responsible Entities to High and Medium Impact?
Yes
No
Is it the drafting team's intent that a separate recovery plan be developed for each BES Cyber System and/or BES Cyber Asset?
Yes
Yes
Yes
No
If the baseline configuration includes security-patch levels, does the CIP Senior Manager have to approve every security patch that is implemented on every applicable asset?
Yes
No
What is the intent of the term "active" vulnerability assessment? This needs to be clarified by the drafting team?
Yes
Yes
Yes
Yes

Yes
Individual
Richard Powell
JEA
Yes
BES Cyber Assets – Need to clarify that the definition applies to physical devices. BES Cyber Security Incident – “suspicious event” is subjective and the word “compromised” is ambiguous. Either define them or remove them. BES Cyber System Information – See APPA comments (define BES Cyber System Impact). CIP Senior Manager – JEA supports APPA comments (change CIP to CIP-002 – CIP-011). Reportable BES Cyber Security Incident – The word “compromised” is ambiguous. Delete or define the word.
Yes
The main issue for JEA is that a new broad-brush approach, attempting to associate reliability of the BES to arbitrary counts of lines, substation MVA, and generation MW is not effective. It will both over-identify and under-identify critical BES elements. Instead, NERC and the industry would be best served and the reliability of the BES best ensured by CIP carefully specifying a new reliability-based methodology for use by the industry. As an alternative, NERC could use the current version 4 bright line criteria modified by the version 5 classification scheme to determine High and Medium Level assets. For the currently proposed criteria: 2.1 – The value of 1500 MW should be defined as either the nameplate or the continuous “rated” capability (where the equipment has been de-rated by the Responsible Entity for age/reliability). 2.7 – 2.7 – The IROL designation (criteria 2.8) correctly identifies transmission facilities that are critical to the reliability of the BES and makes criteria 2.7 unnecessary. The voltage or MVA capacity of a transmission line does not represent the criticality of the line to BES reliability. However, if the criterion 2.7 remains, JEA believes the voltage criteria adopted in version 4, criteria 1.7 is more appropriate than the newly proposed 200kv. 2.8 – Need clarification of what “single station or substation location” is (or is not). If the intent is any facility listed on an IROL, the criteria should state such. 2.13 – Under BAL-002, NERC has established a requirement to address loss of generation. This should eliminate the need for the generator control center portion of criteria 2.13 (part 2). Should the drafting team choose to maintain the second part of criteria 2.13, the 300 MW rating identified is too low and should be revised to be 1500MW in alignment with criteria 2.1.
No
See APPA comment (90 days instead of 30).
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No

JEA supports FMPA comments (VSL to R5 time frame of “within the audit period”).
Yes
Yes
No
2. The phrase “associated with” is used as a “catchall” phrase that leaves three definitions open ended and potentially confusing. The definitions are found in the “Definitions of Terms Used in Standard” for CIP-003 through 010. The definitions are recommended to read: • Associated Electronic Access Control or Monitoring Systems – Applies to Cyber Systems that provide Electronic Access Control or Monitoring for a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems • Associated Physical Access Control Systems – Applies to Cyber Systems that provide Physical Access Control for a corresponding High or Medium Impact BES Cyber Systems. • Associated Protected Cyber Assets –Protected Cyber Assets within a High or Medium Impact BES Cyber Systems.
Yes
No
See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
Yes
No
See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
Yes
No
JEA supports APPA comments (retain event logs for 90 days, like CIP-007 R4.4). See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
Yes
No
See “Associated…” comment in question 15.
No
JEA supports APPA comments (change “remediation” to “mitigation”). See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
No
JEA supports APPA comments (clarify retain event logs of R4.4) See “Associated…” comment in question 15.

No
JEA supports APPA comments (initial change of default passwords R5.4) See “Associated…” comment in question 15.
Yes
No
JEA supports APPA comments (remove communication of incident R1.3.3 and coordinate with EOP-004-2)
No
JEA supports APPA comment (in R2.2, implement “by” the effective date)
Yes
Yes
No
JEA supports APPA comments (Part 1.5 preserving corrupted drive could reduce reliability). See “Associated…” comment in question 15.
No
JEA supports APPA comment (Clarify Part R2.2 – that information is useable) See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
Yes
No
JEA supports APPA comments (Part 1.3 – delete “as necessary”) See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
No
R3.3 - Should PACS (Physical Access Control Systems) be included with EACM (Electronic Access Control and Monitoring) of CIP 007? See “Associated…” comment in question 15.
Yes
No
Access Control of information should be consolidated into CIP-004. See “Associated…” comment in question 15.
No
2. The phrase “associated with” is used as a “catchall” phrase that leaves three definitions open ended and potentially confusing. The definitions are found in the “Definitions of Terms Used in Standard” for CIP-003 through 010. The definitions are recommended to read: • Associated Electronic Access Control or Monitoring Systems – Applies to Cyber Systems that provide Electronic Access Control or Monitoring for a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems • Associated Physical Access Control Systems – Applies to Cyber Systems that provide Physical Access Control for a corresponding High or Medium Impact BES Cyber Systems. • Associated Protected Cyber Assets –Protected Cyber Assets within a High or Medium Impact BES Cyber Systems.
Yes
Yes

Group
Kansas City Power & Light
Scott Harris
Yes
Proposed definitions that include defined terms introduces additional confusion and the opportunity for misunderstandings. We recommend review of these definitions to address the identified issue. As a general comment, the proposed definitions lack clarity and are far too complex. It is difficult to comment on these definitions as there is uncertainty as to what the SDT was targeting. In general, KCP&L subscribes to the EEI comments regarding the definitions. If changing nomenclature is not specific to a directive or does not enhance security / reliability, the terms should stand as they currently exist with proposed adjustments to definitions if necessary. The BES Reliability Operating Services definition is a set of criteria and not a definition. The criteria specified are overly detailed. We recommend serious consideration is given to simplification. In addition, the criteria should be limited to the functions that support the real-time reliability of the BES. The current criteria include planning systems and tools that should not be included for consideration.
Yes
The purpose of the bright line criteria in CIP-002-4 was to establish clear and unambiguous criteria for determination and identification of critical assets applied to all facilities. That purpose was basically achieved. The proposed set of “definitions” and criteria in version 5 has completely reversed those efforts reintroducing ambiguity. Once again, it has become unclear with the current proposed “bright line” criteria what cyber equipment and systems are to be protected. Version 5 as proposed has reintroduced Registered Entity judgment in the determination. In addition, specifically for item 2.7, there is no engineering basis for the method to determine what transmission facilities should be included in CIP considerations. Utilizing the proposed “weighting” technique, despite the effort to defend such in the “Guidelines and Technical Basis” section, complicates the process further and does not provide sound rationale for application of this criteria. The phrase “adversely impact” leaves too much room for interpretation and will lead to additional confusion and misunderstandings. KCP&L strongly recommends the removal of this proposed CIP-002-5 Attachment 1 and replace with CIP-002-4 Attachment 1. This will likely need modification to include Medium and Low criteria to align with the other efforts in CIP version 5.
No
The following are general comments that permeate throughout CIP Version 5: 1. There is no need or purpose for the section “4.2 Facilities” under the applicability section. The criteria already established by Attachment 1 satisfy the direction for facilities under consideration. This section promotes confusion and is not helpful. We recommend removal. 2. Section 4.1.8 identifies the Regional Entity as an applicable entity. The Regional Entity has been defined by NERC in the Rules of Procedure as the Compliance and Enforcement Authority (CEA). The CEA has no operating obligations or operating authority. We recommend removal. This also applies to Section 4.1.7 concerning the NERC obligation for operations or operating authority. We recommend removal. In requirement 1 it says; “All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low impact and do not require discrete identification.” However, in M1 it says “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.” We recommend this inconsistency is corrected with an adjustment to either the Requirement or the Measure. Requirement 1.1 says; “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation…”. This is unclear and the underlined portion doesn’t make sense. KCP&L recommends modification to, “when a change to BES Elements is completed and / or the facility is placed into operation”.
No
The Standards Development Process should not produce standards or requirements that dictate how an entity is to accomplish meeting a requirement. The requirement should direct an entity to develop their Cyber Asset lists. Furthermore, the entity is directed to perform a review and approval process. The level of review and approval should be determined by the entities governance model, organizational structure, compliance culture, etc. It is inappropriate for the CIP Standards to dictate how the organization manages cyber security requirements or compliance with regulations.
No
The Violation Risk Factors (VSL’s) appear overly weighted to the HIGH and SEVERE severity levels.

The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an enity.
No
The Standards Development Process should not produce standards or requirements that dictate how an entity is to accomplish meeting a requirement. We recommend removal of this from the Standard. The level of review and approval should be determined by the entities organization and governance structure. It is inappropriate for the CIP Standards to dictate how an organization should manage security and protection of the Bulk Power System. Further, the Internal Compliance Program principles endorsed by NERC recommend that a strong compliance program is one that is supported by executive management. Registered entities implementing this type of program recognized by NERC. This action is sufficient and does not require the need for the Standard to dictate the appointment of a Senior Manager by name.
No
The SDT should not use specific examples under each topical area as it does in the Guidelines and Technical Basis section unless the list is all inclusive. Providing a general overview or definition of each topical area within the Requirements and Measures section under each sub-requirement (2.1-2.10) is preferable to listing a few examples under each topical area in a separate section of the Standard.
No
Reference to the CIP Senior Manager should be removed for the reasons stated earlier. Suggest the following content change: "Each Responsible Entity shall review each of its cyber security policies and obtain organizational approval initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals."
No
The phrase "make aware" is only a slight improvement over the phrase "readily available" used in the previous versions of this Requirement. Both leave room for interpretation. If you read the R4 Rationale and R4 Measures with the R4 Requirement, this Requirement is relatively clear. However, when the Rationale is removed upon final approval, the intent of the SDT will be lost. KCP&L recommends incorporating the clearly stated direction to communicate the intent of the SDT, stated in the Rationale, in the Requirement.
No
We recommend removal of the Senior Manager reference within the requirement for reasons stated previously.
No
We recommend removal of the Senior Manager reference within the requirement for reasons stated previously.
No
1. This language cites a High VSL when 'not all' individuals have been made aware of elements of the cyber security policy. This seems to contradict the intent described in the R4 rationale in which 'it is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.' 2. The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
Yes
No
Comment is specific to Part 2.10 of Table R2. Language in the table seems to require training on network connectivity for anyone with access to High and Medium BESCS. For some categories of users (e.g., Operators) this will be both out of context and irrelevant. For some categories (e.g., Network administrators) this will be unnecessary for job functions that require network connectivity knowledge. Recommendation is to strike item 2.10.

No
Measure 3.1 where it calls for the date access was first granted is a point of concern for both legacy employees (where it may be impossible). Requirement 3.2 – Propose content change • Original content – Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months. • Proposed change – Require annual completion of the training specified in CIP-004-5, Requirement R2. • Rationale – The wording adopts the CAN-0010 approach for annual as defined within the registered entity.
No
KCP&L recommends removal of the second sentence in Requirement 4.2. Requiring the reason a 7 year background check was unable to be fully completed will add additional cost contributing little or no value to the personnel risk assessment program. KCP&L recommends removal of Requirement 4.4 as it is not practical or cost effective for an entity to validate contractors or service providers are following the stipulations of CIP-004-5 R4. This stipulation would require entities to audit contractors and service providers which is not practical. We recognize the risk associated with contract personnel that do not have appropriate screening and clearance for the access as discussed. We recommend additional discussion around options for closing the gap, such as a registration function applicable to vendors and service providers operating in the space granting compliance enforcement authority for the regulator to review the CIP-004-5 R4 compliance of said entity.
Yes
No
Requirements 6.1, 6.2 and 6.3: These requirements should remove the Senior Manager reference for reasons stated previously. In addition, we recommend the content be changed to: Establish criteria for job functions that require electronic access, physical access, and/or cyber information maintaining a current list of personnel granted such access.
No
Requirements 7.1 through 7.5 and industry HR processes and practices are out of synch regarding HR practices and processes in the determination of dates for resignations, terminations, and transfers. These requirements are in desperate need of additional thoughtfulness in consideration of HR processes that can include adjustment of dates for resignations, terminations, and transfers to meet HR needs. In addition, these requirements do not consider the potential need for personnel to have a transition time as they transfer from one job function into another job function within an organization.
No
The proposed VSL's do not consider sufficient thoughtfulness to give Registered Entities credit for efforts to achieve compliance with requirements. Requirements R1 through R4 do not have Low or Moderate severity levels. There is room to recognize efforts to meet compliance.
No
Requirement 1.3: Outbound is of little security value and will come at additional expense to entities. Following the stipulations of the CIP Standards helps to ensure the integrity of the cyber assets physically and electronically. Inbound is definitely necessary. KCP&L recommends removal of the "outbound" language in the requirement and the measure. Requirement 1.5: It is not possible to detect "malicious communications" for some Electronic Access Point (EAP) equipment. We recommend replacing "at" to "for" in the requirement to recognize that some EAP equipment may not have such detection capability.
No
Requirement 2.2: this requirement lacks clarity to understand the scope and boundary for which remote session encryption is required. We recommend the SDT clarify the boundary for this requirement.
No
The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
No

Requirement R1.2: The measure includes additional requirements regarding egress controls. This is not included in the requirement and contributes minimal improvements to the physical security of cyber assets. The CIP Standards require control of personnel who can physically access cyber assets and stipulates escorting of non-authorized personnel. Ingress controls and monitoring are sufficient to protect cyber assets. Requirement 1.3: This requirement does not recognize defense in depth implementations nor does the requirement recognize alternative actions and measures that can be implemented in the temporary absence of a control. Failure to include these as alternative measures and limiting entities the current proposed requirement can result in substantial unwarranted costs. Recommend the SDT modify this requirement to include defense in depth implementations and alternative actions. Requirement 1.4: This requirement limits physical access alerts to only go "to personnel who are responsible for response". What is important is that alerts go to personnel regardless if the personnel can respond to the alert or to personnel who can notify other personnel to respond to the alert. Restricting this to personnel responsible for a response is shortsighted and does not recognize organizational structure. In addition, the requirement is too broad in alerts issued for "any access point in a Defined Physical Boundary." Recommend changing this to "any access at a Defined Physical Boundary."
No
Requirement R2.2: a. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." i. Rational - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attach vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. b. Requirements – Proposed Change i. Original Text – A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact. ii. Proposed Change - A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the first entry and last exit, the visitor's name, and individual point of contact. iii. Rationale – The proposed change capture the intent with (hopefully) clearer language. The 24 hour basis may introduce expectations that 'round-the-clock' logging needs to be in place. Some visitations may cross the midnight time-line, which shouldn't introduce additional requirements.
No
Requirement R3: 1. R3.1 a. Overall observations – the shift from (pre-V5) maintenance on 'mechanisms' to the Draft 1 'systems' expands this requirement beyond the intent. • This should be more focused on testing to ensure alerting and control mechanisms work as intended. • Use of controls should be considered 'tested' in situations where applicable devices are used every day (i.e. card readers). b. This sub requirement cites tasks to be conducted 'prior to commissioning.' Since many controls are expected to be in place prior to V5 adoption, there should be language within the implementation plan to capture devices in use at the time the standard becomes effective.
No
The Table of Compliance Elements cites references to sub requirements that appear to be incorrect: • Lower – Part 1.7 should point to 1.6 • High – Part 1.6 should point to 1.5
No
Requirement R1.1 – Requirements – Proposed Content Change 1. Original Content – Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. 2. Proposed Change – Enable only logical accessible ports needed, including port ranges where required. 3. Rationale – The proposed language incorporates much of the legacy (CIP-007-3 R2.1) language. The additional requirement to document the need for remaining logical ports extends beyond what FERC Order 706 requests without adding security benefits. 4. There is no direction or explanation about what an "unnecessary" port is nor does it address who the ultimate authority to make such a decision. This requirement leaves far too many components open for interpretation by the auditors and leaves entities in a precarious position of

possible non-compliance based on the opinions of the individual auditors. 5. The requirement language states that access to an “unnecessary” port can be disabled or access to the port can be restricted. It does not require any documentation detailing how access to the port is to be restricted nor does it require any documentation of these “unnecessary restricted” ports. It only requires documentation about the need for any “remaining” logical network accessible ports. This oddly worded requirement leaves too many components open for interpretation by the auditors and leaves the entities in a precarious position of possible non-compliance based on the opinions of the individual auditors. Requirement R1.2 1. Requirements – Content Change a. Original Content - Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. b. Proposed Change – Protect against the use of unnecessary physical input/output ports that could be used for network connectivity, console commands, or removable media by disabling, restricting, or use of signage. 2. Measures – Content Change a. Original Content - Evidence may include, but is not limited to, documentation stating specific or types of physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. b. Proposed Change - Evidence may include, but is not limited to, documentation stating specific physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. 3. The measure for this requirement indicates there needs to be a physical or software restriction on the physical input/output ports, but the requirement is not clear about the specific intent to physically, either through hardware or software, disable or restrict the use of physical input/output ports.
No
Requirement 2.1 1. Requirements – Content Change a. Original Content - Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. b. Proposed Change – Identify a source or sources that are monitored for the release of security related patches, or security updates for software and firmware associated with BES Cyber System or BES Cyber Assets. 2. Measures – Propose striking the last sentence “The list could be sorted by BES Cyber System or source.” It introduces additional requirements with no clear security benefit or alignment with FERC Order 706. 3. Need clarification on when a “remediation plan” is needed. Is it required in delay between OS patch release and vendor approval? When vendor will not approve patch? When there is a vulnerability for which no patch has been released? Requirement 2.3 – Clarification Needed KCP&L uses multiple sources to identify the release of security patches. For example, Microsoft may release an alert that a patch is available on date X but, we don’t receive a vendor alert that the patch is safe to put on until date Y. The wording does not state which date takes priority. Is it the earliest? Is it the latest? Is it up to each entity to decide? Need clarification added. Requirements 2.2 and 2.3 should be switched, as 2.3 requires the establishment of a process for remediation, and 2.2 addresses the creation or revision of the remediation plan. Requirement 2.2 a. Requirement – Propose content change i. Original content - Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe. ii. Proposed change – Identify applicable security-related patches or updates within 30 days of release from the identified source that addresses the vulnerabilities, and create or revise a remediation plan that addresses the vulnerabilities within a defined timeframe. iii. Rationale – The rewording captures the chronological order of the elements within this requirement to provide clearer guidance. Requirement 2.3 b. Requirement – As currently worded, there is no allowance for changes in the remediation plan should outage coordination, or other resource constraints require modifications to the remediation plan. This is a point of concern that should be addressed. c. Measures - Example measures for this requirement include items, such as, Exports from automated patch management tools that provide the installation date, verification screen captures that show Component software revision, registry exports that show software has been installed, etc. Using our current system for vulnerability management, a patch that isn’t relevant produces no evidence. The system only shows security patches that need to be installed. Using this system, KCP&L will not have installation dates, registry exports, etc. to provide as evidence. It is the lack of an applicable security patch being listed on reports that indicates compliance in our program. Need clarification that this is acceptable.
No
1. Requirement 3.2 a. Requirement – Content Change i. Original content – Disarm or remove

identified malicious code. ii. Proposed change – Mitigate the threat of identified malicious code. iii. Rationale – In some instances, the presence of malicious code may present a lesser risk to the reliability of the BES than disarming/removal processes, especially when the malicious code may not exploit a feature used within the Cyber System. b. Measure – Add a bullet to allow for evidence of manual removal. 2. Requirement 3.3 c. Requirement – Propose content change i. Original content – Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). ii. Proposed change – Update malicious code protections from the identified source within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). iii. Rationale – The addition of 'the identified source' provides a context for determination of availability. d. Include testing within both the requirements and measures as alluded to within the Application Guidelines (page 41). e. Measures – Format (i) and (ii) to a bulleted list signifying 'or' criteria f. Part 3.3 requires an update within 30 days. What "starts the clock" on this requirement? Is there an allowance for an approval step from a 3rd party vendor after the OEM has released the signature or pattern update? In some instances, a 3rd party vendor may have to approve prior to a Responsible Entity implementing a release and their delay could cause timing concerns. 3. Requirement 3.4 g. Applicability – Propose deletion of Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems as they do not appear to be Transient Cyber Asset related. h. Requirements – Content Change i. Original Content - Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change – Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to Medium or High Impact BES Cyber Assets or Protected Cyber Assets. i. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. ii. Proposed Change – Evidence may include, but is not limited to, an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. iii. Rationale – Excised content introduced prescriptive criteria that introduced additional resources without clearly addressing the requirement. 4. Requirement 3.5 j) Part 3.5 requires logging each Transient Cyber Asset connection, but this would be captured in the Configuration Change Management requirements of CIP-010-1. As it is covered elsewhere, recommend this requirement be removed from this section of the standard.

No

1. Requirement 4.1 a. Requirements – Content Change i. Original Content - Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. ii. Proposed Change – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. Devices that cannot log a particular event do not require a TFE to be generated. iii. Rationale – Content from the application guidelines has been introduced to promote the guidance that TFE's are not required in instances in which devices cannot log a particular event. iv. Requirement 4.1 includes the use of "any" in the list of activities to log. Not all activities require follow up or investigation and that is the purview of CIP-008-5. Specifically, "any" failed login may not be an indication of a problem. Certainly there is a threshold that deserves attention, but the broad use of the term "any" makes this requirement too broad. v. Requirement 4.1.4 is far too broad of a statement. Even if an entity uses an intrusion detection system, each IDS vendor has their own set of signatures. Who will be the authority on what is considered "potential malicious activity"? 2. Requirement 4.2 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control Systems as they are out of scope for this requirement. b. Requirements – Content Change i. Original Content – Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert. ii. Proposed Change – Generate alerts for events that the Responsible Entity determines necessary. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate real-time alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity

determines necessitate a real-time alert; Screenshots showing how real-time alerts are configured. ii. Proposed Change – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate an alert; Screenshots showing how alerts are configured. iii. Rationale – Removed the usage of 'real-time' as it presents concerns demonstrating compliance. 3. Requirement 4.3 d. Requirements – Content Change i. Original Text – Detect and activate a response to event logging failures before the end of the next calendar day. ii. Proposed Change – Activate a response to failures of event logging before the end of the next calendar day after identification. iii. Rationale – Some devices generate logs so infrequently that identification of logging failure may extend beyond any calendar day. The spirit of this requirement remains intact as one day remediation is required once the log failure is identified. iv. Requirement 4.3 sets a timeframe of "before the end of the next calendar day". This is a very short timeframe. Certainly, logging failure should be addressed. Recommend a longer time frame is needed. 4. Requirement 4.4 e. Requirements – Content Change i. Measures – Content Change 1. Original Text – Evidence may include, but is not limited to, security-related event logs from the past ninety days and records of disposition of security related event logs beyond ninety days up to the evidence retention period. 2. Proposed Change – Evidence must include, but is not limited to, security-related event logs from the past ninety days. 5. Requirement 4.5 Requirement 4.5 inserts a manual review when automation and alerting, both mentioned previously in the standard are much more effective and reasonable controls. If a Responsible Entity is compliant with Requirements 4.1-4.4, then a manual review is a redundant effort which provides no additional security. Recommend requirement 4.5 be removed.
No
1. Requirement 5.1 a. Overall – In both the original content and proposed change there exists instances where access is a component of validation and/or authentication. This presents a potential compliance challenge that should be addressed. b. Requirements – Content Change i. Original Content – Validate credentials before granting electronic access to each BES Cyber System. ii. Proposed Change – Authenticate user account access before granting electronic to each Medium or High Impact BES Cyber System or Associated Protected Cyber Asset, where technically feasible. iii. Validating credentials was seen as vague specific to technical compliance so authentication is offered as an alternate approach to satisfy the root requirement (and mirrors the language in the change rationale). The addition of 'where technically feasible' was to recognize technical capabilities currently in place may not adequately demonstrate compliance with this. 2. Requirement 5.2 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 3. Requirement 5.3 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 4. Requirement 5.4 a. Requirements – Content Change i. Original Text – Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. ii. Proposed Change – Procedural controls for initially removing, disabling, or changing default passwords, where technically feasible. For the purposes of this requirement an inventory of Cyber Assets is not required. iii. Rationale – The additional wording identifies the multiple methods which can be used to mitigate default passwords. 5. Requirement 5.5 a. Requirements i. Change Systems to Assets throughout as password limitations should be identified to the device level. ii. Add language to 5.5.3 to cover instance where accounts may not be able to support password change to permit the entity specified time frame to be equal to the life-time of the BES Cyber Asset where technically required. iii. Requirement 5.5.3 is confusing and unclear, especially the license and service agreement language. Also, the inclusion of "based on the impact level of the BES Cyber System" is not helpful. Recommend that the impact phrase be stricken.
No
The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
Yes
No

Requirement R2.1 states, "…and include recording of deviations taken from the plan during the incident or test". The measures require that we justify any deviations taken. No two incidents are ever the same and they will seldom follow a strict plan. The purpose of a sound incident response plan is to provide a framework to detect, contain, eradicate and recover allowing the freedom to assess and analyze a circumstances and conditions and take appropriate actions. Recommend this be removed from the requirement and the measure. 1. Requirement 2.2 a. Content Change ♣ Original Content • Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): o by responding to an actual incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Proposed Change • Test the incident response plan(s) annually. A test of the plan may include: o A response to an incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Rationale – References to requirements needed upon the effective date should be captured within the implementation plan, allowing the standard to identify requirements (only) in place once the standard is approved. b. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence showing annual testing of the BES Cyber Security Incident response plan(s). Types of exercises may include discussion or operations based exercises. Document lessons learned within 30 days of incident or exercise. Use lessons learned to update incident response plan(s). ♣ Rationale – The Homeland Security Exercise and Evaluation Program identifies seven types of exercises within HSEEP, each of which is discussions-based or operations-based. 2. Requirement 2.3 Propose deletion as this sub requirement merely identifies retention requirements already documented within Compliance (C.1.2).
No
1. Requirement 3.2 1. Requirements – Propose content change a. Original content – Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan. b. Proposed change – Use lessons learned from incident responses or incident response exercises to update the incident response plan, within sixty days of documenting lessons. c. Rationale – It takes 30 days from the time an exercise is executed to the review and completion of an after action report. The thirty day clock should start once the after action report is completed. This is in line with the proposed 60 day timeline in R3.3. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan. ♣ Proposed Change – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or incident response within thirty calendar days of the lessons learned associated with the response plan. 2. Requirement 3.3 1. Requirements – Content Change ♣ Original Content • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan. ♣ Proposed Change • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that test or incident. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan. ♣ Proposed Change – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan test or incidence response and the dated, revised plan.
No
The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
No
1. Requirement R1 • 1.1 – Propose alternate language (carried forward from previous versions) 1. Create and implement a recovery plan that at a minimum includes: 1. Conditions for activation of the

recovery plan 2. Roles and responsibilities of the responders • 1.2 – Propose deletion as this sub requirement has migrated to R1.1 proposed R1.1 rewrite. • 1.3 1. Requirement – Content Change 1. Original – One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality 2. Proposed Change – One or more processes for the backup, storage, and restoration of information required to restore BES Cyber System functionality 3. Suggest additional content supporting mirroring and/or redundancy within the backup/recovery methods such as: 1. Mirroring and/or redundancy can be considered as complementary measure in support of this requirement, but a process must be in place to ensure retrieval of previous versions should current version(s) require reverting to a previous instance. 2. Measure – Content Change 1. Original – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and protection of information required to successfully restore a BES Cyber System. 2. Proposed Change – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and restoration of information required to successfully restore a BES Cyber System. • 1.4 – Correct headers from 'part' to 'Applicability,' 'Requirements,' and 'Measures' 1. 1.4 1. The current form does not adequately address FERC Order 706, paragraphs 739 and 748, and in fact contradicts the intent that 'The Commission does not believe that every change will necessitate verification of the backup and restoration processes' from paragraph 740. 2. Propose 'new' sub requirement applicable to High Impact BES Cyber Systems to require: 1. Upon implementation of significant changes to High Impact BES Cyber Systems, verify that backups are operational before they are relied upon for recovery purposes. 3. Propose rewrite 1. Original – Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully. 2. Proposed Change – Ensure that backup processes are completed successfully for Information essential to BES Cyber System recovery. 3. Rational – This focuses on successful completion of the backup process which can be done within the routine backup. Verification would be moved to its own requirement applicable to High Impact BES Cyber Systems and limited to significant change instances. • 1.5 1. Requirement – Content Change 1. Original Content – Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. 2. Proposed Change – Document root cause for events that trigger activation of the recovery plan(s) as required in Requirement R1. 3. Rationale – Root cause documentation should be the focus for this requirement. The current draft language requires potential impediments to restoration efforts and is too vague.

No

1. Requirement 2.1 1. Requirements – Content Change ♣ Original – Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: by recovering from an actual incident, or with a paper drill or tabletop exercise, or with a full operational exercise ♣ Proposed Change – Implement the recovery plan(s) referenced in R1 annually: • by recovering from an actual incident, or • with a tabletop exercise, or • with a functional exercise ♣ Rationale – Use of the functional exercise aligns with the R2 rationale content citing NIST SP 800-84 exercise types. Requirements in advance of the effective date of the standard should be addressed within the implementation plan. 2. Measures – Content Change ♣ Original – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with a full operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a tabletop exercise, or with a functional exercise) of the recovery plan annually. For the table top or functional exercise, evidence may include meeting notices, minutes, or other records of exercise findings. 2. Requirement 2.2 1. Requirements – Content Change ♣ Original Text – Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations. ♣ Proposed Change – Test information used in the recovery of BES Cyber systems that is stored on backup media annually, to ensure that the information is useable. 3. Requirement 2.3 1. Overall ♣ This requirement (to be done every 39 calendar months) appears to overlap considerably with 2.1 (to be done every year). ♣ Every 39 calendar months exceeds the 3 year retention identified within the Compliance section. ♣ How does

this differ from current EOP-008 requirements? 2. Requirements – Content Change ♣ Original – Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise. ♣ Proposed Change – Exercise the recovery plan(s) at least every 39 calendar months through an operational exercise in a representative environment. An actual recovery response may substitute for an operational exercise. ♣ Rationale – Actions required to take place prior to the effective date of the standard should be captured within the implementation plan.
No
Requirement 3.1 1. Requirements – Content Change ♣ Original – Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned. ♣ Proposed Change – Review the recovery plan(s) annually and document any identified deficiencies. ♣ Rationale – Requirements addressing tasks to be done prior to the effective date should be captured within the implementation plan. Requirements 3.2 – 3.3 Recommend a 60 day timeframe for requirements 3.2-3.4, to be consistent with the recommendation for CIP-008-5. Requirement 3.4 Propose deletion as the requirement is too broad with no clear alignment with FERC Order 706 or security benefit.
No
The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
No
1. Requirement R1.1 1. 1.1.4 – Propose content change ♣ Original Text – Any custom software and scripts developed for the entity; ♣ Proposed Change – Any custom software and scripts installed on the BES Cyber Asset that can affect the security posture. ♣ Rationale – The change focuses scope to eliminate software and scripts not in use. 2. 1.1.5 – Propose content change ♣ Original Text – Any logical network accessible ports; and ♣ Proposed Change – Any network accessible ports or services; and ♣ Rationale – This clarifies the requirement to focus on 'active ports and services' rather than Ethernet jacks. 2. Requirement R1.2 1. Requirement – Propose content change ♣ Original Text – Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Proposed Change – Document approved changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Rationale – As documented earlier in this comment form, requiring Senior Manager (or delegate) authorization introduces resource constraints that impede the effective documentation of changes without adding security benefits or alignment with FERC Order 706. 2. Measure ♣ First paragraph – Add 'or,' at the end of the first bulleted paragraph. ♣ Second paragraph – Propose content change • Original Text – A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) were an individual with the authority to authorize the change was in attendance. • Proposed Change – A record of the change with authorization of the change. • Rationale – Citing a "change advisory board" within the measure overly represents adequate evidence in support of the requirement. 3. Requirement R1.3 1. Requirements – Propose content change ♣ Original Text – Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change. ♣ Proposed Change – Update the documented baseline configuration as necessary within 30 calendar days of completing the change. ♣ Rationale – The proposed rewording provides more focus on the root requirements. 4. Requirement 1.5 Requirement 1.5 is duplicative of Requirement 1.4. Are Control Centers expected to perform dual testing procedures? This does not add to the security of a Control Center and simply adds additional work. Recommend removal of Requirement 1.5.
Yes
No
Requirement 3.2: An active vulnerability assessment of test environments as required in Requirement

3.2 will be burdensome and expensive for smaller entities. Additionally, requiring smaller entities to purchase a vulnerability assessment tool or contract for this service for every install is also burdensome and expensive.
Yes
Yes
Yes
No
The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
No
References to requirements to be conducted in advance of the implementation date should be migrated over into the implementation plan. This ensures any pre-requisites are captured within the implementation plan, freeing this content from the standards to provide clearer guidance. This occurs in the following sections: 1. CIP-002 a. R2 b. M2 2. CIP-003 a. R3 3. CIP-008 a. R2.2 b. M2.2 c. R3.1 4. CIP-009 a. R2.1 b. R2.3 c. M2.3 d. R3.1 e. M3.1 f. VSL (High-R2) g. VSL (Severe-R2) h. VSL (Severe-R3) 5. CIP-010 a. R3.1 b. R3.2 6. CIP-011 a. R1.3 b. VSL (High-R1)
Individual
Rebecca Moore Darrah
MISO
In its comments on Version 4 of the CIP standards in Docket No. RM11-11, MISO raised a number of concerns arising out of the identification of Critical Cyber Assets through the application of the bright line criteria in Attachment I of CIP-002-4. In its comments, MISO stated: MISO is concerned that application of the "bright line" criteria proposed in the NOPR, some of which require identification of Critical Assets based on determinations made by Reliability Coordinators, Planning Authorities/Coordinators, and Transmission Planners, will create significant new burdens on Reliability Coordinators, Planning Authorities/Coordinators, and Transmission Planners – without the benefit of promoting the additional consistency and clarity that the Commission and NERC are seeking in approval of the NOPR. This concern is furthered by certain ambiguities in the "bright line" criteria that MISO has identified, particularly with regard to the treatment of data centers that support control centers. Finally, MISO is concerned that the requirement that Reliability Coordinators identify must-run units as Critical Assets may cause certain Generator Owners to preemptively take their units offline prior to identification of them as must-run. Although Attachment I of Version 4 is used to identify Critical Assets while Attachment I of Version 5 is used to identify BES Cyber Assets and Systems, MISO remains concerned about these issues in the Version 5 Standards, arising out of items 2.3, 2.8 and 2.9 of Attachment I of CIP-002-5. Because MISO has fully expressed these concerns in its comments on Version 4, MISO will not repeat the concerns here; rather, MISO hereby incorporates its comments on Version 4 of the CIP standards, which were filed on Nov. 21, 2011, Docket No. RM11-11
In the "Background" section of CIP-002-5, the SDT writes that one "of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems." The "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" defines the term BES Cyber System as "[o]ne or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services." The SDT goes on to state that the use of the term BES Cyber System is intended "to provide a higher level for referencing the object of a requirement." MISO requests clarification from the SDT on two issues associated with this language. First, the "Background" section provides the example of a BES Cyber System that is subject to a malware protection requirement and states that by using the concept of a BES Cyber System, "it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual

device to comply." However, neither the definition of BES Cyber System nor the malware requirements in CIP-007-5 indicate, on their own, that compliance with the requirement does not require every BES Cyber Asset that comprises a BES Cyber System to have malware protection. MISO is therefore concerned that the Regional Entities will continue to enforce the CIP standards on an individual BES Cyber Asset basis, per a literal interpretation of the text of the Version 5 Standards. As such, MISO requests more explicit confirmation of the holistic approach of the Version 5 Standards as indicated by the "Background" section of CIP-002-5. In addition, MISO requests additional examples similar to the malware example already provided. Second, MISO requests clarification regarding a Responsible Entity's ability to "determine the level of granularity at which to identify a BES Cyber System[,]" as stated in the "Background" section of CIP-002-5. In the same paragraph, the SDT states that the level of granularity is "left up to the Responsible Entity," but also that "defining the boundary too broadly could make the secure operation of the BES difficult to monitor and assess." While this language implies that Responsible Entities will be able to define the borders of BES Cyber Systems without oversight, MISO questions whether the Regional Entities would defer to the judgment of Responsible Entities with regard to the "proper" level of granularity of BES Cyber Systems, particularly since the SDT states that overly broad boundaries could make the secure operation of the BES "difficult to monitor and assess." As a result, MISO requests clarification that the Regional Entities would not play a role in the definition of boundaries of BES Cyber Systems, and suggests that the SDT provide a series of examples of the definition of the boundaries of BES Cyber Systems of varying types and sizes.
CIP-003-5, Requirement R2: Requirement R2 requires Responsible Entities to implement one or more cyber security policies that address each of ten listed topics listed. The "Guidelines and Technical Basis" section of this Standard state that the "cyber security policy must cover in sufficient detail the ten topical areas required by CIP-003-5 R2" and proceeds to list a number of sub-topics associated with each of the ten required topics that the "Responsible Entity should consider for each of the required topics." MISO requests confirmation that a cyber security policy that addresses each of the sub-topics identified in the "Guidelines and Technical Basis" section of CIP-003-5 will be considered to cover the ten topical areas identified in Requirement R2 "in sufficient detail."
CIP-004-5, Requirement R3: Requirement R2 requires Responsible Entities to have a role-based cyber security training program for personnel who need authorized electronic or unescorted physical access to BES Cyber Systems. The applicability for Requirement R2 is "High Impact BES Cyber Systems" and "Medium Impact BES Cyber Systems." Requirement R3 requires the implementation of this cyber security training program for each individual needing authorized electronic or unescorted physical access, however the applicability of Requirement R3 is "High Impact BES Cyber Systems," "Medium Impact BES Cyber Systems," "Associated Physical Access Control Systems," "Associated Electronic Access Control or Monitoring Systems," and "Associated Protected Cyber Assets." The difference in applicability between Requirements R2 and R3 is ambiguous and is likely to create confusion among Responsible Entities. If documentation of a training program is required only for Responsible Entities with "High Impact BES Cyber Systems" and "Medium Impact BES Cyber Systems," implementation of that training program should have the same applicability. MISO requests clarification of this issue.
CIP-004-5, Requirement R7: Requirement R7, Part 7.1 states that for "resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber

Systems at the time of the resignation or termination." The "Change Rationale" section states that this modification was made due to statements by the Federal Energy Regulatory Commission in Order No. 706 that access should be revoked immediately for any person no longer needing access. However, a footnote in Part 7.1 states that "[s]ince termination is often recorded without consideration to the time of day, 'at the time' does not require a to-the-minute or to-the-hour time-stamped comparison of access logs and the termination action." This footnote is ambiguous and will create confusion among Responsible Entities regarding the maximum allowable amount of time for revoking unescorted physical access and Interactive Remote Access to BES Cyber Systems. For instance, if a Responsible Entity were to revoke access on the same date that an employee with such access was terminated, would the Responsible Entity be in compliance? MISO therefore recommends that the SDT clarify or provide a safe harbor provision in Part 7.1.
CIP-005-5, Requirement R1, Part 1.3 requires Responsible Entities to "[r]equire explicit inbound and outbound access permissions at each identified [EAP] using routable protocols, including granting or denying access permissions." Requiring both inbound and outbound access permissions is redundant, and the added expense and effort required to implement such a framework would not be commensurate with the security benefit created by doing so. Electronic communication between devices requires both devices to acknowledge such communication in order for the communication to succeed. Such acknowledgment requires a signal to be sent from the initiating device to the other, and a response is then sent back to the initiating device. Until this initiation of communication is complete, no other communication can occur. If communication is disabled in one direction, the initialization of communication, i.e., the handshake, cannot occur, and further communication is not possible. Requiring only inbound access permissions should therefore suffice. Moreover, implementation of outbound access requirements in addition to inbound ones would be costly and resource intensive. As such, MISO recommends that outbound access permissions not be required in addition to inbound ones.
CIP-009-5, Requirement 1, Part 1.4 requires information "essential to BES Cyber System recovery that is stored on backup media" to be "verified initially after backup to ensure that the backup process completed successfully." This requirement places a significant burden on Responsible Entities with a large number of BES Cyber Systems or BES Cyber Assets comprising BES Cyber Systems. Such Responsible Entities may perform thousands of backups on a daily basis; as such, initial verification after each backup would require an extraordinary amount of resources while providing only a minimal benefit to the security of BES Cyber Systems over that attained by performing random sample verifications or sample verifications based on the type of Cyber Asset backed-up. MISO therefore requests that the SDT modify this requirement to provide for sample verifications, or to clarify that the current language of Part 1.4 is not intended to require initial verification following every backup.

Individual

Michelle D'Antuono

Ingleside Cogeneration LP

Yes

Overall, Ingleside Cogeneration LP agrees that expanding the number of cyber security definitions in the NERC glossary helps us gain a common understanding of a complex topic. There are a couple of terms that could be improved: First, the definition of “BES Cyber System” includes a statement that a “Maintenance Cyber Asset is not considered part of a BES Cyber System.” We believe this should be a “Transient Cyber Asset”, which will then be consistent with the definition of “BES Cyber Asset.” Second, the definition of “BES Reliability Operating Services” is close, but not exactly identical with the write-up in the “Guidelines and Technical Basis” section of CIP-002-5. Since this is essentially replacing the concept of a “Critical Asset” under the Version 4 standards, it is important to have a consistent description in both places. Furthermore the Functional Entity mapping to each operating service (Page 18 of CIP-002-5) is very helpful. The SDT should consider including it in the definition as well.

Yes

The most major change made to the CIP categorization criteria from Ingleside Cogeneration LP’s perspective is the addition of a Low Impact rating for every generation facility that does not meet the High or Medium Impact thresholds. This will force every registered GO and GOP to adhere to about 40 requirements in the remaining CIP standards. We are not convinced that the cost to “NERC-adapt” our existing cyber security policies, encourage cyber security awareness, and that cyber asset access management will lead to a corresponding reliability benefit. In addition, Regional audit resources would be better utilized to focus on truly critical locations – each hour spent on validating Low Impact facilities is one better spent on high or medium impact facilities. We recommend this category be eliminated. Secondly, Criterion 2.13 calls for “control centers that control 300 MW or more of generation” that are not already rated as High Impact, must be considered Medium Impact. The term “control center” is not capitalized – and it must be for consistency. Otherwise, it is possible that an auditor will declare all 300+ MW generation facilities to be at least Medium Impact, not just those that support two or more geographically separate locations. Lastly, Criterion 2.7 seems to have been modified to include some transmission substations operating at 200 kV to 300 kV. The present Version 4 bright-line criterion only includes those operating above 300 kV. Since this includes substations that are interconnected to generators, it seems likely that 200 kV substations newly identified as Medium Impact will require cyber hardening of the generation facilities as well. Again, there is no evidence provided by the SDT that a weighted assessment of the transmission facilities better identifies critical substations than the Version 4 criterion. This criterion should be changed back to the one approved by the industry in CIP-002-4.

No

There should not be a Low Impact rating for every facility that does not meet the High or Medium Impact thresholds. Our resources and Regional audit resources would be better served if allowed to focus on truly critical locations – each hour spent on validating Low Impact facilities is one better spent elsewhere.

Yes

Yes

Yes
No
We are not convinced that the cost to adapt our existing cyber security policies to specifically include the content proposed under CIP-003-5 R2 will lead to a corresponding reliability benefit. Similar to the manner in which they handle other NERC requirements, Compliance Enforcement Authorities will look for language that matches that in each of the ten listed items – whether clearly applicable to Ingleside Cogeneration LP or not. This usually means that if key words are not identical, a violation is assessed. The alignment of cyber security policies to the NERC format seems to be a paperwork exercise only, and makes little sense in the case of Low Impact facilities. Our resources, and our Regional Entity audit resources, would be better spent elsewhere. We recommend this requirement be made applicable to High and Medium Impact facilities only. In addition, it is likely that many of the low impact facilities, such as cogeneration facilities located within an industrial complex, currently have procedures in place. These are corporate wide procedures, and have been put in place for various agencies, i.e Department of Homeland Security, and this requirement would result in multiple procedures for a facility, causing confusion and would add no reliability value.
Yes
No
The rationale statement for CIP-003-5 R4 correctly captures the SDT's intent that the cyber security policy is available and accessible to personnel – not to prove that each and every individual can access the document. However the language of the requirement does not read that way. In fact, it seems to require that the Responsible Entity must track each individual's awareness of the appropriate elements of its cyber security policy. Ingleside Cogeneration LP believes that the requirement should include language that it is sufficient to post the policy on the corporate Intranet site or posted on bulletin boards that are accessible to all employees. These statements are presently captured in measure M4 and can be used as is. This provides accessibility to our personnel and on-site contractors. The education of cyber vendors is a much larger problem. Typically, their maintenance pools diagnose our systems remotely – and are not willing to distribute customer-specific cyber policies to their staff. We believe that an industry-specific policy needs to be developed and made publically available that will serve this need. It would seem likely to us that a NERC-driven initiative would catch the attention of such vendors – and could be written in a way that would be universally applicable to all industry stakeholders.
Yes
Yes
Yes
No
The "Guidance and Technical Basis" section addressing CIP-004-5 R1 correctly captures the SDT's intent that the cyber security awareness program is informational only – not to prove that each and every individual was made aware (i.e.; formal training.) However the language of the requirement does not read that way. In fact, it seems to require that the Responsible Entity must track each individual's awareness of the cyber security on a quarterly basis. Ingleside Cogeneration LP believes that the requirement should include language that it is sufficient to distribute quarterly reminders through email, on posters, or at meetings. These statements are presently captured in the "Guidance and Technical Basis" section and can be used as is. This will cover our personnel and on-site contractors. Maintaining the awareness of cyber vendors is a much larger problem. Typically, their maintenance pools diagnose our systems remotely – and are not willing to distribute customer-specific awareness materials to their staff. We believe that an industry-specific awareness program needs to be developed and made publically available that will serve this need. It would seem likely to us that a NERC-driven initiative would catch the attention of such vendors – and could be written in a way that would be universally applicable to all industry stakeholders.

No

Ingleside Cogeneration LP believes that CIP-005-5 R1.1 is unnecessary. The requirement applies to Low Impact facilities only and calls for technical or procedural controls to be defined that restrict electronic access. Its intent, as stated in the “Change Rationale” box, is to demonstrate that sufficient protections exist that prevent inappropriate access from public and other non-trusted networks. The SDT further infers that if enough Low Impact facilities are compromised by a cyber attacker, it may lead to higher level impacts to the BES. We are not convinced that such a risk exists – nor does the SDT provide any evidence that it does. This means that the cost to adapt our existing cyber security policies to specifically include the content proposed under CIP-005-5 R1.1 will not lead to a corresponding reliability benefit. The alignment of electronic access controls to the NERC format seems to be a documentation exercise only, and makes little sense in the case of Low Impact facilities.

No

Ingleside Cogeneration LP believes that the physical security requirements for Low Impact facilities (CIP-006-5 R1.1) are unnecessary. The requirement calls for operational or procedural controls to be defined that restrict physical access. Its intent, as stated in the “Change Rationale” box, is to “allow for programmatic protection controls as a baseline.” This appears to us to be a confirmation that no true reliability benefit is served by R1.1. From our viewpoint, the alignment of physical security controls to the NERC format seems to be a documentation exercise only, and makes little sense in the case of Low Impact facilities.

No

While Ingleside Cogeneration LP agrees with the intent and need for procedural controls which eliminate default passwords from BES Cyber Assets, we believe that CIP-007-5 R5.4 should not apply to Low Impact facilities. We are not convinced that the cost to adapt our existing password procedural controls to specifically include the content proposed under CIP-007-5 R5.4 will lead to a corresponding reliability benefit. From our perspective, the alignment of cyber security policies to the NERC format seems to be a paperwork exercise only, and makes little sense in the case of Low Impact facilities. Our resources, and our Regional Entity audit resources, would be better spent elsewhere.

No

The requirements for a cyber security incident response plan are similar, if not redundant with, those being developed under EOP-004-2 (Project 2009-02). If there are key items missing in EOP-004-2 that do not satisfactorily address a cyber attack, they should be corrected there. Otherwise Ingleside Cogeneration LP believes that we would be placed in a double-jeopardy situation for any gaps in the cyber security incident response plan.

No

The requirements for the execution of the cyber security incident response plan during an actual

intrusion attempt and the regular testing of the procedure are similar, if not redundant with, those being developed under EOP-004-2 (Project 2009-02). If there are key items missing in EOP-004-2 that do not satisfactorily address a cyber attack, they should be corrected there. Otherwise Ingleside Cogeneration LP believes that we would be place in a double-jeopardy situation for any failures to execute in accordance with CIP-008-5 R2.1 and R2.2. In the case of R2.3, the SDT calls for Responsible Entities to retain documents related to reportable cyber incidents for three years. However, item 1.2 under the "Compliance" section of CIP-008-5 states that the Compliance Enforcement Authority can request evidence dating back to the previous audit – which could be up to six years. In theory, the language in the requirement should predominate, but it is not clear to Ingleside Cogeneration that it would. Therefore, we recommend that a statement be included in the requirement which clearly shows its supremacy.
Yes
Individual
Scott Berry
Indiana Municipal Power Agency
Yes
BES Cyber System – Maintenance Cyber Asset is not a defined term. IMPA suggests using the term Transient Cyber Asset or defining Maintenance Cyber Asset. BES Cyber System Information – BES Cyber System Impact is not a defined term. CIP Manager – The definition should exclude CIP-001. Cyber Asset – definition is way too broad and could include devices such as a thermostat. Needs to be more tightly defined and be more applicable to the operation of the BES and should also relate somehow to how the device is accessed or connected – e.g utilizes/is connected via routable protocol and/or dial-up modem. There are numerous assets that are programmable that utilities use that have very minimal impact on the reliable operation of the BES (such as a programmable thermostat). BES Cyber Asset – need better definition on "if rendered unavailable, degraded, or misused…". This could be as simple as someone removing the trip output wiring – which could just as easily happen on a electro-mechanical relay with the same results. A BES Cyber Asset should be narrowed down to include if it is connected via routable protocol or dial-up modem and by use of this connection it is rendered unavailable, degraded, or misused would …….. BES Cyber Security Incident – the last statement could be interpreted to include someone cutting a substation chain link fence. This needs to be more narrowly defined or removed from the definition. BES Reliability Operating Services – again very broad in scope. In addition these Services, as defined, are confusing and vague and could lead to numerous interpretations by auditors.
Yes
IMPA would like to see the addition of another category called "Low Impact without Connectivity". This category would be made up of Low Impact BES Cyber Assets that do not have routable protocol or dial-up access. It would be impractical to attempt a coordinated cyber attack on BES Cyber Assets without connectivity. Since it would be impractical or very difficult to coordinate a cyber attack and in taking into account that we are talking about Low Impact Cyber Assets, IMPA believes these assets

would not need to comply with the CIP standards because the costs would be unjustified. In addition there should be additional bright line criteria used to delineate a Control Center that meets the requirements for Medium Impact. For example use a weighted value as is done in 2.7 but for transmission facilities operating at 100 kV and above.
Yes
IMPA agrees with the requirement and not requiring discrete identification of Low Impact BES Cyber Assets or Systems. However, IMPA does not understand how entities are going to prove to auditors that the identification and categorization was done without having to produce an inventory or listing of assets to the auditors. The VSLs seem to imply that Low Impact BES cyber Assets or Systems need to be discretely identified. M1 states in part that “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.” The only way to completely satisfy M1 would be to inventory and identify each and every Low Impact BES Cyber Asset and BES Cyber System. R1.1 provides a timetable to note a change to BES elements and Facilities that requires an entity to change the classification from a lower to a higher impact category but doesn’t provide a timetable for the phase-in for the entity to meet the potential additional Standard(s) Requirements caused by this change.
Yes
Yes
Yes
No
The bullets are incorrectly numbered. R2 should apply only to those entities that have High Impact or Medium Impact BES Cyber Systems. R2 would be overwhelming and costly for a small entity to comply with if that entity has a single facility that may have only 1 Low Impact BES Cyber System. This should align with the Applicability for CIP-004-5 R1 through R7.
No
This should apply only to High Impact and Medium Impact BES Cyber Systems (see R2). In addition, it is not clear if each individual cyber security policy needs to be improved or if the approval of the CIP Senior Manager (one signature) covers all of the cyber security policies.
No
This Requirement should apply only to those entities that have High Impact or Medium Impact BES Cyber Systems. See Applicability for CIP-004-5 R1 through R7.
Yes
Cyber Security Policy should not be capitalized (it is not capitalized in R2 and R3).
Yes
no comment
No
This Requirement should apply only to those entities that have High Impact or Medium Impact BES Cyber Systems. See Applicability for CIP-004-5 R1 through R7. In addition there may only be a single person that this would apply to at a smaller entity that has a single Low Impact BES Cyber System. Quarterly reinforcement would carry little value. IMPA recommends a semi-annual or annual reinforcement frequency.
No
IMPA does not agree with the use of “must” in M2. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M3. Measures are not requirements but are examples of evidence.
No

IMPA does not agree with the use of “must” in M4. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M5. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M6. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M7. Measures are not requirements but are examples of evidence. Part 7.1. IMPA finds it very difficult and maybe impossible to revoke access at the same time that a resignation is received. Footnote 2 does not address resignations, only termination. In addition, IMPA understands what the SDT is stating in the application guidelines for a voluntary termination under R7, but the requirement 7.1 does not make the same statement as in the guidelines. Auditors follow the requirements during an audit and not the SDT application guidelines.
No
The Severe VSL for R3 is either a yes or no answer which eliminates the high VSL.
No
IMPA does not agree with the use of “must” in M1. Measures are not requirements but are examples of evidence. IMPA also believes that R1 will force entities with Low Impact systems to inventory them in order to provide evidence that it has performed or satisfied this requirement.
Yes
IMPA does not agree with the use of “must” in M2. Measures are not requirements but are examples of evidence.
No
The way the VSLs are written just one missed EAP is a severe violation. The VSLs should be written in a manner to not make just one missed EAP a severe violation.
No
IMPA does not agree with the use of “must” in M1. Measures are not requirements but are examples of evidence. Part 1.1 is very ambiguous and is very open to interpretation by entities and auditors which can lead to many violations of this requirement. For example, an entity may see that a fence and a gate with a padlock are sufficient. An auditor may deem this to be insufficient and cite a possible violation. Do both horizontal and vertical dimensions need to be enclosed? IMPA recommends the use of bright line criteria to ensure entities and auditors are on the same page for what constitutes a sufficient physical boundary. In the Requirements column “Define operational or procedural controls to restrict physical access” whereas in the Measures column “documented operational AND procedural controls exist”. This needs to be consistent.
No
IMPA does not agree with the use of “must” in M2. Measures are not requirements but are examples of evidence. Part 2.2 The use of “on a per 24 hour basis” needs to be clarified. Do visitors need to be logged out at the end of 24 hours and then logged back? Does it mean use military time?
No
IMPA does not agree with the use of “must” in M3. Measures are not requirements but are examples of evidence. It is not clear if Part 3.1 applies to High, Medium, and/or Low Impacts.
no comment
No
IMPA does not agree with the use of “must” in M1. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M2. Measures are not requirements but are examples of evidence.
No

IMPA does not agree with the use of “must” in M3. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M4. Measures are not requirements but are examples of evidence. Part 4.3 In order for this requirement to be met, an entity must use a redundant system to recognize an event logging failure. Therefore, this requirement seems to imply the use of redundancy. Part 4.4 This requirement covers data retention and should be moved to the data retention section.
No
IMPA does not agree with the use of “must” in M5. Measures are not requirements but are examples of evidence.
no comment
No
IMPA does not understand how entities are to “identify, classify, and respond to BES Cyber Security Incidents” on Low Impact systems. In order to “identify” BES Cyber Security Incidents on Low Impact systems, it seem like these entities will need to use a system to monitor potential cyber incidents. Entities with High and Medium Impact systems are required to use systems to “identify” BES Cyber Security Incidents, however, IMPA does not believe that entities with Low Impact systems should be forced through an “unwritten” requirement to use a system to monitor potential cyber incidents. This requirement should only apply to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, even for Low Impact systems. CIP-008-5 R1 – Applicability should be restricted to High Impact and Medium Impact BES Cyber Systems. This would better dovetail with Applicability Requirements of CIP-004-5, 005-5, 006-5, and 007-5. IMPA does not agree with the use of “must” in M1. Measures are not requirements but are examples of evidence.
No
CIP-008-5 R2 – Applicability should be restricted to High Impact and Medium Impact BES Cyber Systems. This would better dovetail with Applicability Requirements of CIP-004-5, 005-5, 006-5, and 007-5. See answer to question 34. IMPA does not agree with the use of “must” in M2. Measures are not requirements but are examples of evidence. Part 2.3 This requirement covers data retention and should be moved to the data retention section.
No
The question does not match the requirement. CIP-008-5 R3 – Applicability should be restricted to High Impact and Medium Impact BES Cyber Systems. This would better dovetail with Applicability Requirements of CIP-004-5, 005-5, 006-5, and 007-5. See answer to question 34. IMPA does not agree with the use of “must” in M3. Measures are not requirements but are examples of evidence.
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
No
For unplanned scenerios, IMPA recommends 18 months and not 12 months. If an entity experiences an unplanned scenerio in Jan of a year and needs to budget for the equipment or software, then the entity needs time to purchase and then perform the work.
Group

Paul Skare, et al
Paul M. Skare
Yes
With NERC CIP v5, we believe a graded security approach with low, medium and high impact on the BES is a sound approach, but have found it mostly focused on medium and high impact systems, and mostly the medium and high impact systems are bundled as a pair. For example, some password requirements are given for medium and high impact systems, but the draft is completely silent about what should be done for low impact systems. There is no reason not to mandate a no default password policy for *all* systems within the BES. Yes, there might be a few cases where legacy systems do not support anything but hard-coded defaults, but these could be documented en masse as exceptions (with associated compensating controls) rather than let these exceptions be used as an excuse to allow a poor password policy. In an effort to reduce the burden to industry we recommend including a grandfather clause that provides certain exceptions for legacy low-impact systems (such as those that do not have external computing interfaces or capabilities). As noted, the systems are graded into low, medium, and high, but the requirements/controls are not applied in a graded three-tier approach. Most requirements lump high and medium into one category and ignore low. Ideally we should have requirements that get successively stronger as we migrate from low to medium to high. There are a number of concerns that either exist in multiple places throughout the CIP standards or are applicable to the standard as a whole they include: * Consistency of the capitalization of terms * Consistency in the use of the terms Cyber Asset and Cyber System * Consistency in the use of the terms Cyber access and electronic access * Section 4.2.4.2 of many of the requirements use the term Electronic Security Perimeters. Has this been deprecated? * We disagree with Section 4.2.4.2 as an exemption - Communication links should be protected between ESPs * As defined, CIP Exception circumstances are not that exceptional. Scaling back requirements within an exceptional circumstance is acceptable, but completely suspending requirements is not. * Include a definition of terms section to the standards. The applicability section of each standard defines how the term applies to that standard but does not fully define the meaning of the term. Note: This and other comments submitted by our team represent our collective judgment as subject matter experts—they are not the official position of the Department of Energy nor of the Pacific Northwest National Laboratory.
No
Section 4.1.2 How are smart grid devices being operated by Distribution Providers? * Battery Storage is another question that is not addressed * Other smart grid assets (100KV+) Section 4.2.4.x Cyber Assets should be prefaced by BES Should the last paragraph on page 7 say “cyber security plan”?
No
Section 4.2.4.4 What is the definition of Cyber System vs. Cyber Asset? There is a need for consistency in use – especially in the tables. Section 5. Background – It seems this entire section is predicated upon a table which is missing. There is no table [Table Reference] pg 7 and under Applicability there is no table to aid in understanding of all the different “Applicability Columns” R2 Should include a Procurement Policy requirement R2 Should include a Resiliency Policy requirement R2 1.5 System Security: Should include third-party, outsourcing, and availability or be considered as separate topics. Guidelines R2 2.1 Personnel Security: Should explicitly include subcontractors and outsourced services R2 2.3 Remote Access should be moved into System Security Include language in contracts that requires vendors, contractors, or consultants adhere to the Responsible Entity’s policies and controls. R2 2.7 Recovery Plans should include a prioritized recovery strategy
No

CIP-004-5 should also include the case where one organization has equipment in another organizations facility (i.e. substations)
No
The wording of the requirement is confusing. The measure for 3.1 does a better job defining the requirement than the requirement.
No
1.2 The requirements column should state “Control and secure all connectivity through the use of identified Electronic Access Points (EAPs). “ 1.4 Eliminate the “where technically feasible” loophole. The statement should simply be “Perform authentication when establishing dial-up connectivity with the BES Cyber System.” 1.4 Dial-up access for either non-interactive or interactive sessions should be authenticated. As written, 1.4 only protects non-interactive sessions.
No
Eliminate the “where technically feasible” loophole. The statement should simply be “Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items.” NEW: As written, low impact systems do not have to be protected with passwords, nor are the users required to be authenticated. Requirements for low impact systems should be added.
No
M1. Typo: - As stated “Evidence must includes…” should be “Evidence must include…” 1.5 Clarification needed with respect to the applicability column as to what impact level the associated physical access control systems apply. Explicitly state that this applies to all systems.
No
3.1 High and medium impact systems should have their associated physical access control systems monitored (and tested) more frequently that once every 24 calendar months. Testing frequency should be dependent upon the impact level (i.e. annual testing of a control center is not too frequent).
No
The requirement for all of CIP-007-05 should follow a graded approach to match the impact level of the various systems where the lower the impact level the more time or leniency is afforded to meet the requirement.
No
Patch management is optional for low impact systems. Even these systems should have patches applied, but perhaps in a less timely manner than is required for medium and high impact assets.
No
Malicious code protection is not required for low impact systems. Even these systems should be monitored/protected.
No
Once again, low impact systems are not included. Security event monitoring should also apply to low impact systems. R4 4.5 Two week lag before logs from high impact systems have to be reviewed. The reviews should be more timely, especially if only one calendar day is given to rectify issues discovered. We saw in GridEx how timeliness is important in this area.
No
Password management is not specified for low impact systems. No guidance is given regarding

sharing/reusing passwords between systems. R5 5.4 Eliminate the “where technically feasible” loophole. The statement should read “Procedural controls for initially changing default passwords unless the default password is unique to the device or instance of the application…” R5 5.6 Eliminate the “where technically feasible” loophole.
No
Seems OK. However, the definition of a reportable incident seems a bit vague.
No
1.2 Worded poorly. (Currently: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.) Should more clearly state that (pre) approval is needed for configuration management changes.
No
2.1 Caveat of “where technically feasible” applies to both medium and high impact systems. Compensating controls should be applied to high impact systems when built-in monitoring of baseline changes is not technically feasible.
No
3.3 Change in phrase order makes the requirement easier to understand “Perform an active vulnerability assessment prior to adding a new Cyber Asset to a Cyber System or Electronic Access Control or Monitoring System, except for CIP Exceptional Circumstances.
No
No uniform requirements for how BES Cyber System Information is to be handled. Is it business sensitive, official use only, etc? Furthermore, does the level of protection vary based upon whether the information is about high impact or medium impact systems? Missing a statement about how one is authorized to view BES Cyber System Information. How does one get added to the list of those with a “need to know” the information? The aspects of trust and the needed controls for trusted parties would be useful, especially regarding external entities such as vendors, contractors, DOE, NERC, etc.
Individual
Christine Hasha
Electric Reliability Council of Texas, Inc.
Yes
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
Yes

Yes
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT also offers these additional comments. Regarding 7.1, request definition of when the clock starts for revoking access upon termination or resignation. This is of particular concern with relying on notification from external parties such as Regional Entities, vendors, contractors, etc. Regarding 7.2, request definition of when the clock starts for revoking access upon reassignment or transfer. Is there an allowance for training or support of the prior position? Regarding 7.3, request definition of when the clock starts for revoking access upon termination or resignation. This is of particular concern with relying on notification from external parties such as Regional Entities, vendors, contractors, etc.
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes

No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT also submits these additional comments. Regarding 2.1, remove the comma from the requirement. The comma changes the requirement to address all updates and firmware regardless of security impact.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT also offers these additional comments. Request allowances in 3.3 for signatures/pattern updates that cause trouble. Suggest adding “Create a plan to mitigate the vulnerability where it is determined that the signature or pattern update cannot be safely applied.” Also, request similar language to R2 in identifying the source for updates. Regarding 3.5, request reasoning for this requirement. How does this requirement address the rationale listed? This will be of particular difficulty when dealing with CDs as well as assets that have no capability of logging event.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT also offers these additional comments. Regarding 1.5, request clarification of retention of the preserved data. Also, needs to be noted that these activities must be secondary to recovery and not impede recovery.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT offers these additional comments. Regarding 2.2, request clarification of what information is necessary. Does this include the operating system information from vendors? Does this mean testing every backup or every tape ever made? Does it have to be restored or just perform verification at the end of the backup? Regarding 2.3, is testing of each scenario in the plans required?
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT offers these additional comments. Regarding 3.1, it is not practical to perform a review of all documents on the specific date of the effective date of the Standard.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT offers these additional comments. Request flexibility to have appropriate management structures utilized in automated change management processes.
Yes

No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT offers these additional comments. Regarding 2.2, request clarification of the requirement. Does this mean destruction of data on the identified BES Cyber Assets only?
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Individual
Gregory Campoli
New York Independent System Operator
Yes
The Definition for External Routable Connection states that “The BES Cyber System is accessible from any Cyber Asset…” This should say “a” Cyber Asset rather than “any” Cyber Asset. The word “associated” (Associated Electronic Access Control or Monitoring Systems, Associated Physical Access Control Systems, Associated Protected Cyber Assets) is used throughout the Standards, but Associated is never defined. The terms Electronic Access Control or Monitoring System, Physical Access Control System, and Protected Cyber Asset are defined, but how is a Protected Cyber Asset different from an Associated Protected Cyber Asset? Description of an Associated Protected (or Physical Access or Electronic Access Control Systems) in the Applicability Section of the Standards states they are …”System associated with a corresponding High or Medium Impact BES Cyber System”. The Definitions document lists Protected Systems, but not Associated Protected Systems. What is a System associated with a corresponding System? Do not understand what these words mean. The Definition of a BES Cyber Asset refers to assets that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The definition also states: “This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Service”. The key information appears to be that a problem with an asset can adversely impact a BES Reliability Operating Service within 15 minutes. However, it also appears that the occurrence of the initial event has no bearing on this evaluation. Definition would be clearer if it emphasized the impact to one of the BES Reliability Operating Services rather than being rendered unavailable, degraded, etc. “Suspicious” is not an auditable term, and should be removed. What is an “attempt”? What attempts are serious enough to justify having to be reported? The definition should be made to read: BES Cyber Security Incident A malicious act that: • Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. Under “BES Reliability Operating Services”: • “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet • Recommend that “Change management” under “Situational Awareness” be clarified to changes in the BES instead of IT change management • Recommend clarification that “Facility” is the NERC Glossary term--in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication”: • Request clarification of the scope of this “Operational Directives”. Does it include a company’s messaging system? Two-way radios? What is the relationship with the new COM-002? • Request clarification that these Coordination and Communications are limited to Reliability, not Market Systems. • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret.

Yes
The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium, and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways. Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly-complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced through-out the Standards. One of the BES Reliability Services identified in Att. 1 is Balancing Load and Generation and one of the bullets under it is Demand Response. However the description of Demand Response includes the Ability to identify load change need and the Ability to implement load changes. These criteria are the same as the Manually Initiated Load Shedding bullet and are not criteria we would typically associated with Demand Response. Need a clarification on what Demand Response means in Att. 1 One of the BES Reliability Services identified in Att. 1 is Situational Awareness. Att. 1 seems to define Situational Awareness as what is going on in one's own system whereas Situational Awareness is typically used to describe system-wide awareness. Need clarification on what Situational Awareness means in Att. 1. Need clarification on the role/responsibility of PC, TP, GO, GOP, RC, PA in CIP-002-5, Att. 1, 2.3, 2.8, and 2.9 Comments: Recommend that 2.8, 2.9 and 2.11 start with "Applies to all Regions except…" For 2.8, 2.9 and 2.11 request that the SDT clarify whether the exception is all, or not WECC. In 2.12, "system" and "Facility" are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal?
No
CIP-002 requires update to Cyber Asset listing within 30 days of a change "…intended to be in service for more than 6 calendar months…". This is not auditable and we should delete the phrase regarding intentions. Transient Cyber Assets (assets directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset) are a poor security practice. Cyber Assets should not be connected to the protected systems without proper security and controls, whether it be temporary or permanent. For clarity and consistency with the previous change, request changing M1 from "as required in R1 and list of changes to the BES (" to "as required in R1 and list of changes to the BES Elements and Facilities)". Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term "Facilities" in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be "compliant" with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation "requirements" in a guidance document rather than in the requirements in the standard. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium, and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are

introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced throughout the Standards.
Yes
No
Regarding CIP-003-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
Yes
Yes
No
The last bullet for M4 on page 12 is inconsistent with R4 since M4 requires periodic training instead of R4’s making staff aware of cyber security policies. Request that M4 be updated to be consistent with R4.
Yes
No
The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
No
Comments: Regarding CIP-004-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement. Recommend removal of

R2.3 and R2.4 since they are redundant to R2.2, or explain the difference between R2.2 and R2.3, R2.4. Request removing “potential” from R2.7 since training should include how to determine whether a BES System Event occurred or not.
Yes
No
For all R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”.
No
For R6.1 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.3 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber System Information. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.6 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I” in Information.
No
Request that the footnote for 7.1 be moved into the requirement. Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend removing the "following the resignation or termination" since it is redundant and inconsistent with the sibling Requirements. Recommend changing 7.4 from "For resignations or terminations," to "For terminations, resignations, reassignments, or transfers,".
No
The Standards allow systems used for access control or monitoring to be located outside an ESP. It is a poor security practice to locate Associated Cyber Assets/Systems outside an ESP and these assets, if they are protecting BES Cyber Assets and are important enough to protect, should also be located in an ESP Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point or not? Request clarification on 1.5's "at each EAP". Is that inside or outside or both? Regarding CIP-005-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with

requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology. Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete.
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress". Request Requirement 1.2 be updated to allow "escorted physical access." Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.4 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. " to "issue real time alerts for detection of breach through an access point". For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6. Regarding CIP-006-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, ".
No
Request clarification on what the "Associated" "Applicability" (High/Medium/Low BES Impact) for 3.1 and 3.2 Request capitalization of "locally mounted hardware or devices" in Requirement 3.1 so that it refers back to the defined term "Locally Mounted Hardware or Devices" .
No
Request clarification on 1.1, is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on 1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Regarding CIP-007-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have

some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Request clarification of "remediation" in 2.2 since it reads that the patch must be applied, which does not allow to have an exception when applying the patch is the worst scenario such as creating a denial of service. For 2.2, suggest wording like "create a remediation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied". What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to the patch or the overall process?

No

Request allowances in 3.3 for signatures/pattern updates that cause trouble. Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media". The Measure for 3.4 does not match the Requirement.

No

CIP-007, R4.5 requires summarization/sampling of logged events for Associated Systems (access control, monitoring, physical access, protected asset associated with a corresponding High or Medium Impact System), but does not require such protection for a Medium Impact BES Cyber System. How can more stringent controls be required for a system associated with another system than required for the system itself? Or is it just a type that excluded it from R4.5? Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities. Request clarification on 4.3, does the failure need to be detected within a calendar day? Request the rationale of 4.5's "two weeks". Recommend one month as a compromise between the prior version's 90 days and the suggested one week. In 4.5 clarification is needed for the associated protected cyber assets. Are these protected cyber assets associated with only high impact BES cyber systems, or could they be associated with medium impact BES cyber systems?

No

For 5.2, does the CIP Senior Manager or delegate approval policy or procedure for each authorization of access? In 5.2, should the Requirement be interpreted as "each use" as in "The CIP Senior Manager or delegate must authorize the use of each administrator, shared, default, or other generic account types." Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."

No

Regarding CIP-008-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

: 2.1 is a new Requirement. Request the rationale for this new Requirement. Recommend changing

from "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." to "When a BES Cyber Security Incident is classified or identified, the Responsible Entity must follow its incident response plan." Recommend removing “initially upon the effective date of the standard” from 2.2 of Table R2 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered.

No

Recommend removing “initially upon the effective date of the standard” from 3.1 of Table R3 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend that 3.2 wording be consistent with the 2.2 wording. For 3.3, recommend changing 1) "Update" to "Update as necessary" and 2) "the completion of the review of that plan" to "the completion of the review performed in 3.2" .

No

For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommend removing Requirement 1.5. Reliability's top priority is restoration of service. Forensics in a recovery mode may not support BES reliability and requiring such actions may negatively impact the BES Cyber System restoration process. Regarding CIP-009-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Recommend that 2.1 be implemented 180 days from the effective date of the Standard. For 2.1, request clarification, is “full operational exercise” the same as “functional exercise” as described in the rationale? For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the Standard.

No

For 3.1 recommend 1) removing “or when BES Cyber Systems are replaced” as it is addressed in CIP-009 R3.4 and 2) removing “and document any identified deficiencies or lessons learned” as they are addressed in CIP-009 R3.2 and R3.3. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two

Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Recommend that 3.4 be referenced by CIP-009 R3.1. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.

No

Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." For 1.1, 1.2, 1.3 and 1.4, recommend changing the Requirements to be consistent with their Applicability --- from "For a change to the BES Cyber System" to "For a change to the BES Cyber System or Associated Systems or Associated Assets". Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold. Regarding CIP-010-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Recommend removing "where technically feasible" from 2.1 since the remaining words should not need an exception.

No

For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend changing 3.2 from "in a production environment" to "in a production environment, or a test environment" to allow Entities more flexibility in meeting this Requirement.

No

Request clarification on 1.1. Some interpret this Requirement as what is the Entity's process for identifying BES Cyber Systems Information. If correct, the Measure should be "show me the methodology (document)." Others interpret these Measures as labeling BES Cyber System Information. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Regarding CIP-011-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards

Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Request that footnote 2 in 2.1 be moved into that Requirement.

No

The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Otherwise, this Scenario table is confusing because it repeatedly uses 12 months while the earlier text uses 18 months. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Since Version 4 is not FERC approved, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. A summary of comments applicable to more than one standard: . • Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • Request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5. A fiftieth question should have been included in this comment form asking for general comments or concerns. A question asking general comments should be included as part of every comment form posted to the industry.

Group

Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG)

Marianne Swanson

No

Yes

The Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) has developed a mapping between NERC CIP v5 requirements and the high-level security requirements in the National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628, Guidelines for Smart Grid Cyber Security. The NISTIR 7628 is available at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf This mapping identifies any gaps between CIP v5 and the NISTIR 7628 high-level security requirements and recommendations to the CIP drafting team to consider. The complete mapping (Excel file) will be submitted to the CIP drafting separately as a reference document. Some sections of the comment form have been left blank because no gaps or recommendations were identified. The CIP-002-5 criteria provide a sound approach for identifying low, medium, and high impact systems within the BES. This three level approach aligns well with the three level approach (i.e., low, moderate, and high) used within the NISTIR. Most requirements in the current CIP drafts are applicable to both medium and high impact systems as a bundled pair and they are silent on their applicability to low impact systems. In contrast, the NISTIR uses a graded requirement approach that specifies baseline controls that apply at low impact levels and then specifies strengthened controls for moderate impact and even stronger controls for high impact levels. The CIP version 5 standards will be significantly strengthened if they were to incorporate a similar graded approach when applying requirements.

No

To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R1, 1.1, to include the concept of “continuous improvement” and best practices (to align to NISTIR 7628, SG.CA-

3, Continuous Improvement).
Yes
Yes
Yes
No
To align with the NISTIR 7628 high-level requirements, CIP should elaborate requirement: R2, 1.3, to include following - 1) Responsible Entity should document document allowed methods of access to the BES Cyber Systems (to align with NISTIR 7628, SG.AC-2, Remote Access Policy and Procedures); 2) Responsible Entity should incorporate in their policies the usage restrictions and criteria for allowing each remote access (to align with NISTIR 7628, SG.AC-2, Remote Access Policy and Procedures); 3) Responsible Entity should setup authorization procedures prior to granting remote access; 4) Responsible Entity should enforce requirement criteria for providing remote access to the BES Cyber systems (to align with NISTIR 7628, SG.AC-2, Remote Access Policy and Procedures); 5) Responsible Entities shall implement policies and procedures for managing remote sessions in their BES Cyber Systems access control policies and procedures (to align with NISTIR 7628, SG.AC-13, Remote Session Termination); 6) Responsible Entities shall include in procedures and criteria of granting Remote access encryption, authentication of all communication media through limited number of manageable access control points (to align with NISTIR 7628, SG.AC-15, Remote Access). R2, 1.5 to include following - Responsible Entities shall include in their policies and procedures to grant access privileges to their BES information Systems based on minimum privilege justified by the business requirement for access requests (to align with NISTIR 7628, SG.AC-19, Control System Access Restrictions). R2, 1.6 to include details on what the policy should address including objectives, roles and responsibilities, and the the scope of the incident response program, and require the identification and classification of potential interruptions (to align with NISTIR 7628, SG.IR-1, Incident Response Policy and Procedures). R2, 1.7 to specify required elements of the recovery plan (to align with NISTIR 7628, SG.CP-1, Continuity of Operations Policy and Procedures and SG.CP-2, Continuity of Operations Plan). R2, 1.9 to include following - 1) Responsible entities shall restrict access to external information systems or restrict processing, storing or transmitting controlled information through External Information systems over which the Responsible Entities have no control (to align with NISTIR 7628, SG.AC-18, Use of External Information Control Systems); 2) Responsible entities shall have a documented media protection security policy that addresses the objectives, roles, and responsibilities fo r the media protection security program as it relates to protecting the organization's personnel and assets; the scope of the media protection security program as it applies to all of the organizational staff, contractors, and third parties; and procedures to address the implementation of the media protection security policy and associated media protection requirements (to align with NISTIR 7628, SG.MP-1, Media Protection Policy and Procedures); and 3) Requirement that data communications be addressed in the information protection policy (to align with NISTIR 7628, SG.SC-1, System and Communication Protection Policy and Procedures).
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R4, 4.1, to include detailed personnel screening requirement detailed in NISTIR 7628, SG.PS-3, Personnel Screening, as follows: Basic screening requirements should include - a. Employment history; b. Verification of the highest education degree received; c. Residency; d. References; and e. Law enforcement records.
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R6, 6.1, 6.2, 6.3, and 6.4 to include security authorization for granting escorted/ unescorted access permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management (to align with NISTIR 7628, SG.PS-7, Contractor and Third-Party Personnel Security). R6, 6.5 and 6.6, to include security authorization for periodic review of permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management (to align with NISTIR 7628, SG.PS-7, Contractor and Third-Party Personnel Security).
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R7, 7.1, to include requirement of exit interview to convey the constraints imposed on the individuals/ contractors/ Third Party Service Providers, due to revocation of privileges caused by change in assignments or termination of job (to align with NISTIR 7628, SG.PS-4, Personnel Termination).
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R1, 1.2, to identify - 1) specific authentication credential management requirements (initial authentication credential content; administrative procedures for initial authentication credential distribution/lost credentials/lost, compromised, or damaged authentication credentials/revoking authentication credentials; changing/refreshing authentication credentials on an organization-defined frequency; and specifying measures to safeguard authentication credentials) (to align with NISTIR 7628, SG.IA-3, Authenticator Management); and 2) devices to be identified and authenticated prior to establishing a connection (to align with NISTIR 7628, SG.IA-5, Device Identification and Authentication). R1, 1.3 to identify devices to be identified and authenticated prior to establishing a connection (to align with NISTIR 7628, SG.IA-5, Device Identification and Authentication).
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R2, 2.1, to include - 1) The organization employs virtualization techniques to deploy a diversity of operating systems environments and applications; 2) The organization changes the diversity of operating systems and applications on an organization-defined frequency; and 3) The organization employs randomness in the implementation of the virtualization (to align with NISTIR 7628, SG.SC-28, Virtualization Technique). R2, 2.2, to include - 1) cryptographic key establishment and management (to align with NISTIR 7628, SG.SC-11, Cryptographic Key Establishment and Management); and 2) use of FIPS-140-2 approved or allowed cryptography and other security functions (to align with NISTIR 7628, SG.SC-12, Use of Validated Cryptography).
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R4, 4.2, to specify - 1) the use of an automated mechanism to necessitate a real-time alert (to align with NISTIR 7628, SG.IR-6, Incident Monitoring); and 2) receiving security alerts, advisories, and directives from external organizations (to align with NISTIR 7628, SG.SI-5, Security Alerts and Advisories). R4, 4.3, to specify some events that alerts should be generated (to align with NISTIR 7628, SG.AU-5, Response to Audit Processing Failures).
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R5, 5.1 to specify devices to be identified/authenticated prior to establishing a connection (to align with NISTIR 7628, SG.IA-5, Device Identification and Authentication). R5, 5.3 to specify requirements for managing authentication credentials for users/devices, including supplemental guidance to safeguard credentials by not loaning/sharing credentials (each individual must be identified for any shared account as opposed to sharing credentials) (to align with NISTIR 7628, SG.IA-3, Authenticator Management).
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R1, 1.3, to specify - 1) data is reported in compliance with applicable laws and regulations (to align with NISTIR 7628, SG.IR-7, Incident Reporting); 2) external entities that should be considered for not only communication but coordinated effort related to cyber security incidents (to align with NISTIR 7628, SG.IR-11, Coordination of Emergency Response).
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R2, 2.1, to specify the use of an automated mechanism in response to an incident (to align with NISTIR 7628, SG.IR-6, Incident Monitoring).
Yes
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R1, 1.3, to specify information to be backed up (to align with NISTIR 7628, SG.IR-10, Smart Grid Information System Backup). Information to be backed up includes user-level information, system-level information and system documentation including security related documentation. The confidentiality and integrity of the backup information shall be maintained. R1, 1.3, 1.4, and 1.5 to specify alternate storage sites (to align with NISTIR 7628, SG.CP-7, Alternate Storage Sites) and requirements to recover/reconstitute Smart Grid systems to a secure state (to align with NISTIR 7628, SG.CP-10,

Smart Grid Information System Recovery and Reconstitution).
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R2, 2.1, 2.2, and 2.3, to specify requirements to recover/reconstitute systems to a secure state (to align with NISTIR 7628, SG.CP-10, Smart Grid Information System Recovery and Reconstitution).
Yes
Yes
Yes
Yes
Yes
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R1, 1.1 to specify - 1) requirements to partition the communications for telemetry/data acquisition services and management functionality. The information system management communications path needs to be physically or logically separated from the telemetry/data acquisition services communications path (to align with NISTIR 7628, SG.SC-2, Communications Partitioning); and 2) requirements to employ underlying hardware separation mechanisms to facilitate security function isolation; and isolate security functions (e.g., functions enforcing access and information flow control) from both non-security functions and from other security functions (to align with NISTIR 7628, SG.SC-3, Security Function Isolation). R1, 1.2 to specify more granular retention requirements as applicable to law/regulations (to align with NISTIR 7628, SG.IA-2, Identifier Management).
Yes
Yes
Yes
Group
Southern Company Services, Inc.
Antonio Grayson
Yes
“BES Cyber Asset” could be improved by reinstating the phrase “and causes a Disturbance to the BES” that was in earlier drafts approved by the SDT. This would also help clarify what the phrase “adversely impacts” means by giving the industry a more concrete basis on which to determine what does/does not fall into this definition. “Situational Awareness” is a major concern because as currently defined its scope is so ambiguous and overly broad that it will inhibit meaningful implementation. Southern suggests adding clarifying phrases such as “wide area” and “for operational purposes.” The bullet point for “Change Management” should be deleted or further refined because this is a very generic term that means many different things to many different people and disciplines. “Control Center’’ has a major flaw in that it includes any facility that houses any BES Cyber Asset that is doing anything for more than one location. As such, the term “Control Center” is ambiguous and overly broad. For example, a master radio located on a pole-top that is aggregating data from more than one substation could be interpreted to be a control center according to this definition. Southern suggests including a more explicit definition that specifically references facilities where system operators are performing the BA/RC/TOP functions and any associated data centers. Southern also

suggests explicitly excluding field locations that aggregate data for use by the control center. “BES Cyber System Information” should add the words “BES Cyber System” in front of the phrase “network topology diagrams” for consistency purposes and to better clarify what types of diagrams are included. Southern also suggests deleting the phrase “or similar” in this definition and throughout the standard to avoid unnecessary ambiguity and confusion. “BES Cyber System” should have the word “Maintenance” changed to “Transient” to match the other definitions in the standard. “CIP Exceptional Circumstance” should have the word “BES” in front of “Cyber Security Incident” to match the proposed glossary term. “External Routable Connectivity” – spell out “ESP” (i.e., Electronic Security Perimeter) in the definition or be consistent with the External Connectivity definition. “Intermediate Device” – spell out “DMZ” (i.e., Demilitarized Zone).

Yes

As an overall comment in CIP-002-5, Southern has three primary concerns centered on (i) the inclusion of distribution assets in the applicability of the standards, (ii) the inclusion of low impact assets, and (iii) the extensive shift in methodology from previous versions of the standards. In addition, Southern suggests the following changes to the bright line criteria and guidance that help clarify the language. Inclusion of distribution assets Southern strongly suggests that the CIP standards remain focused directly on BES reliability. The inclusion of distribution assets in the applicability sections 4.2.1 and 4.2.2 of each of the reliability standards needs to be struck. Low impact assets Low impact assets are problematic in that they are high in volume creating extensive resource needs to comply with the CIP-002-5 requirements and creating a potential distraction from the primary focus of adequately protecting the High and Medium Impact assets. In order to move forward with expedient progress on Version 5, and to not let Low Impact assets distract the industry from adequately protecting High and Medium Impact assets, Southern proposes that Low Impact assets and their requirements be moved to another standard separate from High and Medium Impact assets and requirements. Southern also suggests that inventory and auditability issues with Low Impact systems could be better addressed by removing the Low Impact category and modifying the corresponding programmatic requirements to apply to the Responsible Entities themselves rather than to particular assets. Extensive shift in methodology CIP-002-5 as drafted contains an extensive shift in methodology when compared to previous versions of the CIP-002 standards. The new methodology is generating a significant amount of confusion in the industry. While the proposed approach is different, it is not clear that this change produces a significant difference from what would be protected using the industry approved methodology found in previous versions of the standards. The terms introduced as reliability services are often ambiguous and do not help focus application of the standards. For example, situational awareness is a broadly applicable term and if interpreted broadly has few limits. Therefore, Southern suggests that the SDT build from the Version 4 methodology with appropriate categorization and refinements to address remaining FERC directives and removing the reliability operating services approach. Enhancements to bright line criteria In criteria 1.4, the reference to 2.12 should be 2.13 to correctly include control centers. In criteria 1.3 and 1.4, the “that includes” should be changed to “is limited to” in order to not leave these criteria completely unbounded. Criteria 2.1 with its historical nature needs to account for decommissioned generating units. A unit that would have historically met this criteria but has been decommissioned should not be subject to this standard. Southern suggests adding “commissioned” or “active” to the beginning of the criteria. Criteria 2.5, first bullet should read “Up to and including the first interconnection point of the starting station service of the generation unit(s) to be started”. For criteria 2.7, Southern suggests returning to the industry balloted and approved language that is in CIP-002-4 regarding 345kV with 3 or more lines. Criteria 2.10 needs to be limited to the plant switchyard, otherwise the entire grid could be included. Southern suggests using the phrase “on site facilities”. Additionally, criteria 2.10 needs to include logic similar to R2.5 to determine if there are equivalent independent transmission alternative paths. Suggested changes to the guidance On pg. 25, the Medium Impact Generation bullet that begins Part 2.5 – As worded, this could be interpreted to cover both Generation and Transmission. The Transmission part picks up with the sentence that begins with “The drafting team further …”. Consider moving some of this material to the Transmission section that starts on pg. 27 and refer to it from pg. 25. Also consider moving the cranking path diagrams to the Transmission section that starts on pg. 27 into Part 2.5. On pg. 28, Part 2.7 paragraph – It is not clear how autotransformers in a station should be factored into this calculation. Do autotransformers count as a connection to another station? Does it matter if the autotransformer (including generator step-up transformers) is connecting to a higher voltage level such as 500kV versus a lower level such as 115kV? Please provide guidance on how to treat autotransformers and

GSUs in the calculation. On pg. 29, third bullet, in the 1st sentence in the guidance section for criteria 2.12, Southern suggests changing “are capable of performing” to “perform” which makes it match the actual criteria without adding ambiguity. Additionally, the reference to 2.13 in the second sentence should be 2.12. On pg. 29, the word “Systems” in UFLS and UVLS should be consistently capitalized.
No
Southern is very concerned with R1.1 as it centers on every “change to BES Elements and Facilities”. Southern believes that as currently drafted this requirement will be subject to varying interpretations and will be essentially impossible to implement and audit. For example, it will require some form of master list of every BES change, some determination of whether each change affected any cyber asset and to what degree, and the expected duration of every change to the BES. Southern believes this is an onerous burden and an incorrect approach to place on the industry. Some BES Elements and Facilities are integrated into critical cyber systems. Southern suggests making this impact change determination dependent upon BES Cyber Asset changes which is a much more manageable burden. Otherwise, Southern suggests returning to an annual review or alternatively the addition of a very specific list of BES changes for which the analysis must occur. Southern believes more clarity is needed in R1 on the concept of “its” and “owns”. Cyber Assets could be leased from entities outside the industry who are the “owners” and are not subject to the CIP standards. This may be as simple as changing it to “owns or leases”. R1.1 describes what to do when Facilities are placed “into” service but provides no guidance on what to do when Facilities are “out-of-service”. The SDT should consider a companion R1.2 for when Facilities are “out-of-service” which minimizes administrative overhead and compliance risks and maximizes potential for restoration of service with sound security.
Yes
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement. For instance, the VRF should be used to differentiate between violating the Disturbance Control Standard (BAL-002), and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRF’s should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRF’s are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRF’s can be applied.
Yes
No
Southern suggests that all measures should have bullet points rather than sequential numbers. As the measures are examples that “may include”, then the format of the individual items should not suggest that they must all be present. R2 and Measure #2 includes the verb “shall implement” and “and records that indicate the required ten topics were implemented.” This is quite open-ended as anything the entity decides to include in their policy that is above and beyond the CIP requirements could be the source of a violation of this requirement. Proving the implementation of all these policies on all BES cyber assets is overly burdensome on the industry.
Yes
No
The measure suggests the intent of the requirement is to make the policies widely accessible to those who have access to BES Cyber Systems. The requirement as worded, with the phrase “make individuals who have access to BES Cyber Systems aware”, would require tracking to the individual level for every BES Cyber System. With this wording, the provided measures do not meet the requirement. Southern suggests not using the word “individuals” and focusing the requirement on making the policies available rather than making individuals aware.
No

Southern strongly suggests refocusing R5 and R6 requirements on naming the CIP Senior Manager and the activities he's responsible for without the administrative overhead of tracking delegates and delegate authorities in paperwork. Updating the CIP Senior Manager within 30 calendar days of a change is reasonable. R5 and R6 as worded create unnecessary paperwork and administratively burdensome tasks that provide no enhancement to BES security. No other reliability standard requires explicit documentation and tracking of delegation. Delegation is an ordinary business activity. How a company organizes and delegates internally should not be a matter of reliability standards. Alternatively, sufficient language would be any industry approved version of the CIP-003 R2 language.
No
See response to question 10.
No
Southern has a general concern that Violation Severity Levels are routinely biased towards High and Severe. Lower degrees of severity are often needed within the VSLs. For example, in R3, as written, the VSL is High for a policy that covers all CIP requirements and is also High for a policy that covers one CIP requirement. Therefore, R3 potentially unfairly penalizes entities who have implemented multiple policy documents. Southern suggests (i) basing the R3 VSL on R2 and the number of parts not approved within the required timeframe and (ii) adding additional granularity, rather than the current wording of "not all". Consistent with Southern's response to question 9 above, in R4 Southern suggests not using the word "individuals" and focusing on making the policies available rather than making individuals aware. Consistent with Southern's response to question 10 above, R5 and R6 needs to be re-focused on the CIP Senior Manager and their responsibilities and away from creating and maintaining delegation paperwork. In general, regarding VRFs in each of the CIP standards, it is Southern's understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form "Do X" to all of "these systems" and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRF's can be applied.
Yes
No
CIP-004-5 Table R2 is highly repetitive, seems to provide an incomplete start to a role-based training program, and appears to misinterpret FERC Order 706 – paragraph 434. The FERC order does not mandate role-based training, but that "any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions or inactions could, even inadvertently, affect cyber security." This can be accomplished in numerous ways. Southern suggests a return to approved language in CIP-004-3 or CIP-004-4 with the directed FERC clarification that "training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity," not just CCAs. This can be accomplished with adding one or more bulleted items to R2.2 in CIP-004-3.
No
In previous versions of the standard, 'Protected Cyber Assets' were only subject to CIP-007 requirements. Version 5 expands on that with requirements such as the CIP-004 R3 training requirement, which also implies that access is tracked to the individual level on these types of Cyber Assets. Southern suggests that the requirements to which Protected Cyber Assets are subject be matched with current practice in current standards.
Yes
No

See reply to CIP-004 R3 (Question #15). In addition, applying this to EACMS without further qualification is problematic. The phrase “authorized electronic access” to an EACM would mean anyone with an ID on that system; essentially anyone who just has a record in the database. There is negligible risk from a person who is just authenticated out of a common ID store if they have no access to the actual BES Cyber Systems and entities should not be required to do PRA’s on every individual in a common ID store. Southern suggests separating this requirement such that administrators of the EACMs require PRAs, but not every person represented by a record in the EACM. If an entity has a directory service or a token authentication service that has CIP and non-CIP user IDs in it, the standard would not apply to people with no BES Cyber System access.

No

In Parts 6.1 and 6.3 the requirement for the CIP Senior Manager or delegates of the CIP Senior Manager to authorize access should be eliminated. Consistent with answers on questions 10 and 11, Southern strongly suggests focusing requirements on security requirements and results without the administrative overhead of the CIP Senior Manager or his delegates approving all access in paperwork. R6, Parts 6.1 and 6.3 as worded creates unnecessary paperwork and administratively burdensome tasks that provide no enhancement to BES security. Alternative language would be any industry approved version of the CIP approval language. It is strongly suggested that access review requirements use the model of R1.3 in CIP-011-1 rather than the ‘zero defect’ model they currently employ. Southern believes the desired behavior is to “find, fix, repeat” rather than having compliance violations levied for finding and fixing errors. The requirements should require entities to “self-audit” on a periodic basis, complete with remediation plans and deadlines for mitigation of issues found. If the above approach is not taken, then an issue arises in 6.4 – 6.6 where any access that was provisioned in error but never used is a violation. There is a paragraph in the included guidance that says this should not be considered a violation, but guidance does not override what the requirement plainly states. Southern suggests changing the language to be based on “users who used their access” to more closely match the intent. Throughout this requirement, it uses the phrase “Access permissions shall be the minimum necessary for performing assigned work functions.” Southern believes this to be overly onerous to audit (if not essentially unauditable to prove every access right on every cyber asset for every individual is necessary for some work function). Southern believes this phrase is unnecessary as the point of the authorization is to insure that there is a need for the requested permissions. Auditing to the authorization we feel is sufficient and the phrase should be deleted. More explanation is needed on the difference between R6.4 and R6.5. R6.5 appears to be a superset of R6.4 and both are performed on the same timetable. Measure (iv) in R6.5 appears to cover R6.4. Southern suggests deleting R6.4.

No

The standard addresses numerous forms of employee status changes, but does not address employee retirements. The included guidance suggests that access revocation for retirement should occur “day of”, but the requirement itself does not seem to allow this. R7.2 is problematic in that most in-company job transfers in some large organizations occur on the weekend (Saturday). If the person is remaining a trusted employee and is just transferring jobs, is there sufficient risk to require that all the access be revoked on Sunday? Southern suggests changing the timeframe to allow for weekend transfers. R7.3 is problematic for audits. How does an entity prove that access to every piece of BES Cyber System information, including paper prints, has been revoked? Southern suggests changing the language to “revoking access to areas designated for BES Cyber System Information”. This is still problematic, but much less so, and is language already contained within the change rationale in the requirement.

No

Southern has a general concern that Violation Severity Levels are routinely biased towards High and Severe and as worded may work against desired behavior. For example, R3 needs to be written to promote the desired behavior of “find, fix, repeat” rather than having compliance violations levied for finding and fixing errors. The R3 VSL should be reworded to account for evidence of periodic review and promptness in fixing errors, if any, once detected. In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take

into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRF's are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
No
R1.1 needs to be made explicit that the Low Impact systems can have their electronic access controls documented as a group or at a site level. Southern suggests changing the Applicability to "Responsible Entities" rather than Low Impact systems as that requires an audit at a system or device level. R1.3 should make it explicit that the responsible entity determines the "explicit criteria". Leaving this unaddressed leaves the requirement open to audit interpretation.
Yes
No
Southern has a general concern that Violation Severity Levels are routinely biased towards High and Severe. For example, as currently drafted CIP-005-5 has only Severe violations meaning any violation of a requirement is a Severe VSL. Additional thought needs go into what would really constitute a Severe violation and what should be lower severity levels or no violation. For example, in R2, configuration errors or necessary temporary conditions should be a lower severity level or no violation than not implementing an Intermediate Device at all.
No
In previous versions of the standard, "Protected Cyber Assets" were only subject to CIP-007 requirements. Version 5 expands on that with several requirements in CIP-006. The requirements assume that all PCAs are within the same Defined Physical Boundary with their associated BES Cyber Systems. Southern suggests that the requirements to which Protected Cyber Assets are subject be matched with current practice in current standards.
No
In Table R2, Part 2.2, Southern suggests deleting "a per 24-hour basis" which may be confused with continuous logging of an individual within a perimeter. Additionally, consider modifying the language to logging date and time of "initial" entry and "work completed or final" exit to reduce administrative burden if someone has to repeatedly move into and out of a perimeter to get the work done. Continuous escort of visitors within the perimeter is already required. Examples include pulling cabling, working on an access point itself, or moving volumes of equipment into a perimeter.
No
In Table R3 Part 3.2, due to the redundancy and/or robust design present in physical access control and monitoring systems the term "failure" and "systems" creates ambiguity and confusion. One component of an access control system can fail, but access control at the access point continues to operate as designed. Southern suggests striking "failure" as outage reflected in the current approved standards is sufficient. Additionally, logging date and time of an outage implies duration is a calculated and redundant (stop time - start time). Southern suggests the following wording: "Log dates and times of outages of Physical Access Control or Monitoring Systems." The term "outage" should specifically exclude routine maintenance activities such as replacing a battery or a badge reader.
No
Southern has a general concern that Violation Severity Levels are routinely biased towards High and Severe. A review of the violations of CIP standards could shed additional light on those types of activities that companies are being sighted for at audits, and that the VSLs can and appropriately account for those violations. In general, regarding VRF's in each of the CIP standards, it is Southern's understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form "Do X" to all of "these systems" and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be

accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
Yes
Yes
The Change Rationale needs to be updated to more closely reflect the requirement.
Yes
No
The “at a minimum” is problematic and Southern suggests deleting it. The requirement has a defined list of what must be included so the “at a minimum” phrase adds nothing to the requirement. R4.1.1 needs clarification on the issue of dropped packets at an EAP. Is a dropped packet that did not meet an explicit access rule a “‘failed access attempt”? This and R4.1.4 are problematic for Internet-facing systems as maintaining such logs (of “noise”) is overly onerous. The requirement does not allow for differentiation in environments where mostly noise is expected vs. environments where no noise is expected.
No
In R5.1, change the word “granting” to “permitting” to more closely match the intent. In the remainder of the standard, authorizers grant authorized access. R5.4 is very problematic from an audit perspective for Low Impact BES Cyber Systems. Southern strongly suggests that this be required only on High and Medium Impact systems. R5.5.3 is problematic from an implementation and an audit standpoint. Version 5 requires strong physical security and greatly enhances the electronic remote access security. Southern believes with these enhancements in perimeter security on remote devices (some of which may be pole mounted or have an easily accessible password bypass jumper) that the password change interval requirement should be removed until technology allows for more central management of such devices. As more and more field devices are pulled into scope, this requirement becomes onerous quickly with little reduction in risk.
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
Yes
Yes
No
Southern believes R3.4 goes well beyond the changes required from paragraph 686 of Order 706 and would be overly onerous to prove in an audit. This would require a list of all organizational or technological changes with an analysis of which impacted any cyber security incident response plan and then prove those plans were updated in response to those changes.
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and

violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.

No

R1.4 needs clarification as to whether the backup media must be verified (what the requirement states) or if it requires verification that the backup process completed successfully (what the measure says). If it is the former, then verifying multi-terabyte backups is prohibitive. Also, as a “system” level requirement, backup and verification of every individual component (a network hub for instance) is not feasible.

No

R2.2 is problematic in that it requires the entity to verify current configuration against a year old backup. Testing all backup media (multiple tera- if not petabytes) is onerous. It is also overly onerous to test every backup from every system annually. Is the standard actually requiring testing 365 backups per system if it has daily backups? The entities will spend an order of magnitude more time verifying backups than it takes to perform the back ups.

No

R3.4 would be onerous to prove in an audit. This would require a list of all organizational or technological changes with an analysis of which impacted any recovery plan from any cyber system and then prove those plans were updated in response to those changes.

No

In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.

No

In general, CIP-010 should be re-focused towards defining, approving, maintaining, and verifying cyber security controls for the various BES Cyber Systems. The CIP standards themselves suggest that items included as a part of the security controls baseline (R1.1) would include an assessment of the OS and security related patch levels, of application software and security related patch levels, of logging enabled, of anti-virus enabled and definitions updated, of default accounts and passwords appropriately configured, and ports and services reflecting the baseline for the BES Cyber System as appropriate. Without re-working the entire proposed CIP-010 standard, which the SDT may need to consider, Southern recommends certain enhancements to the requirements below. Southern believes that the SDT has over-interpreted FERC directives and overly constrained needed flexibility in implementing the standards, particularly in Table R3. Southern suggests that the SDT review FERC directives again before making any significant changes from the industry approved CIP version 4 language. The Rationale – R1 should be re-worded to exclusively prevent unauthorized “security controls related” modifications to BES Cyber Systems. Changes not impacting security controls should be beyond the scope of the CIP standards. In Table R1, Requirements column, the requirement should be re-worded to focus on a baseline “security controls” configuration. In Table R1, R1.1.1. Physical location is not a configuration item for most if not all cyber devices. Few cyber devices know or contain a parameter to configure location. Additionally, we are already required to secure devices within a Defined Boundary according to CIP-006-5 R1 which creates double jeopardy by including this item here. Physical location should be removed from the listing. In Table R1, R1.1.3. Southern

suggests the removal of the term “commercially available” and then R1.1.4 could be deleted as R1.1.3 will cover both. R1.2 needs to clarify the SDT’s intent as to temporary changes. For example, temporary scripts may be used on a cyber asset to help troubleshoot issues. Southern would strongly suggest deleting R1.1.4. If 1.1.4 must be included then it should be scoped to those scripts which impact the security controls, not all scripts. R1.2 generates a lot of confusion in that in R1.1, we define a security controls baseline on paper, then in R1.2 we jump to changes to devices without a clear linkage between the two. Southern suggests bridging the issue by rewording R1.2 to approve changes to the documented security controls baseline in R1.1 within 30 days of a change to the BES Cyber System or to the baseline and staying away from device level change management at this point in the standard. As previously noted, authorization by the CIP Senior Manager or delegate is unnecessary, burdensome, and should be removed. Southern strongly suggests refocusing CIP-004 Version 5 R5 on naming the CIP Senior Manager and the activities he’s responsible for without the administrative overhead of tracking delegates and delegate authorities in paperwork. CIP-004 version 5 R5 and CIP-010 R1.2 creates unnecessary paperwork and administratively burdensome tasks that provide no enhancement to BES security. No other reliability standard requires explicit documentation and tracking of delegation. Delegation is an ordinary business activity. How a company organizes and delegates internally should not be a matter of reliability standards. Alternatively, sufficient language would be any industry approved version of the CIP-003 R2 and R6 language. R1.4 is acceptable as written assuming suggestions in 1.1-1.3 above are adopted. This is where changes impacting security controls come into play. Since changes impacting security controls must also be approved, Southern suggests adding a requirement 1.4.4 “changes to BES Cyber Systems which cause a deviation from the existing baseline security controls configuration must be approved.” R1.5 change rationale is misguided in that FERC directives do not mandate security controls testing in a test environment but allow for it. This requirement should and can be deleted. Security controls testing can be effectively and safely performed in a production or test environment and the utility is best able to determine which environment is suitable best on their own tools, capabilities, and knowledge of their systems. Requirement 2.1 should be re-written as to not create technical feasibility exceptions. Consider, “Indicate in your baseline security controls configuration which items are actively (through alarming or active automated monitoring) or periodically (through a manual check) monitored. Security controls BES Cyber Systems must be monitored prior to or in conjunction with implementation, and at least once within a calendar year, unless retired.” Consider adding a requirement 2.2, “Identify deviations from the authorized security controls baseline (through requirement 2.1) and document how the deviation was resolved.” The rationale for this change is that the requirements are clear and measurable, meet the intent of FERC directives, and model the correct behavior for fixing security control related issues.
No
Southern suggests that R2.1 would be more appropriately limited to High Impact BES Cyber Systems only. Applying this requirement to Medium Impact, which incorporates an order of magnitude more field assets, will generate numerous TFEs. Requirement 2.1 should be re-written as to not create technical feasibility exceptions. Consider, “Indicate in your baseline security controls configuration which items are actively (through alarming or active automated monitoring) or periodically (through a manual check) monitored. Security controls BES Cyber Systems must be monitored prior to or in conjunction with implementation, and at least once within a calendar year, unless retired.” Consider adding a requirement 2.2, “Identify deviations from the authorized security controls baseline (though requirement 2.1) and document how the deviation was resolved.” The rationale for this change is that the requirements are clear and measurable, meet the intent of the FERC order, and model the correct behavior for fixing security control related issues.
No
R3.2 should allow for the active vulnerability assessment to occur in production environments where the entity has determined it is safe to do so. It should not be limited to test environments only. Is the intent of R3.3 that a new cyber asset would have a vulnerability scan run against it or that somehow the cyber security controls would be tested? With the proposed changes above in questions 43 and 44, Table R3 is no longer needed and can be deleted. As written, it is confusing, wordy, and appears to misinterpret the FERC directives. However, the intent of 3.4 can be preserved as a part of the proposed 2.2 above in question 43.
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF

is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
No
Overall, Southern suggests that the BES Cyber System Information related access requirements in CIP-004 be placed in CIP-011 so that the entire Information Protection program requirements are in one standard.
Yes
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
No
It’s not clear what an 18-month implementation timeframe is based on. And, depending on the final language of Version 5, it may not be possible to fully implement Version 5 in the allotted timeframe. Parallel implementation paths or overlapping implementation timeframes with CIP Version 4 or the just the significant change in methodology from CIP-002-3 to the drafted CIP-002-5, will probably create a situation where some or most but not all can reach full compliance with this aggressive implementation plan. Therefore, Southern suggests that the SDT consider creating an exception process, as reviewed and agreed to by the regional entity, to establish the compliance deadline for some assets for good business reasons. As stated in question 2 and reiterated here, Southern suggests that the SDT re-consider making significant changes to the CIP-002-4 asset identification methodology which will also help speed implementation of Version 5 by building on previous versions of the standards and our existing experiences. The notion of planned and unplanned change needs to be better explored. In addition, unplanned change needs to be better defined. It is difficult to envision an unplanned change to the BES except during exceptional circumstances. At the same time, it is easy to envision unplanned changes to cyber systems to address real-time issues. The implementation plan is not fully clear on how to determine if a change is planned or unplanned and creates incentive for change to be categorized as “unplanned.” Southern suggests that the correct position is for cyber assets to be treated as if they are in-scope during commissioning and be fully compliant in parallel with commissioning whenever possible. However, Southern also suggests that the SDT consider creating an exception process, as reviewed and agreed to by the regional entity, to establish effective compliance deadlines for some assets for good business reasons. Alternatively, consider a defined at least 24 month period to reach full compliance for existing and new assets. Additionally, consider 12 months for all changes.
Individual
David Grubbs
City of Garland
Yes

Under the definition of BES Reliability Operating Services under the section titled "Balancing Load and Generation" in the first sentence the words "in the operating planning horizon" should be deleted. This time horizon is well beyond the 15 minute effect as described in the Standards.
Yes
Under Section 4.1.2 Applicability on page 5, and again in section 4.2.2 on page 6, for DPs it states "Transmission Operator's restoration plans" that is very broad. Should be limited to paths used in the TOP Black Start Cranking Paths and facilities identified under Attachment 1, item 2.5 except for the voltage such as substations operated at 69 kV.. Under Section 4.2.4 Exemptions, page 6, should specifically exclude telephone systems and other voice communications systems that are not located within an ESP On the Figure on Page 7 The word Protected needs to be included (ie "Version 4 Protected Cyber Assets") in the title above both halves of the of the figure. Under Attachment 1, Item 1.3 and 1.4, the criteria for determining which control centers should be under the high category the 2.4 Black Start Resources should be under Transmission Operator Control Centers not under Generator Operators since under the EOP standards during Restoration such units are under the control of the TOP not the GOP/BA. Any cyber control by the GOP is minimal. On page 8, under Real Time Operations, do not agree with the last sentence that- says that "redundancy does not mitigate cyber security vulnerabilities." There is some level of redundancy with multiple technologies that could mitigate any vulnerability.
No
Under R1.1 believe that the 30 days should be extended to 60 days and that the 6 calendar months should be extended to 12 calendar months due to delivery times of replacement equipment. Temporary connections frequently last 9 to 11 months during construction activities.
No
Should state "not later than the effective date" not specify "upon the effective date". Approval should not be on a specific single date. This applies throughout all of the standards where this phrasing is used.
Yes
Yes
Yes
No
Should state "not later than the effective date" not specify "upon the effective date". Approval should not be on a specific single date. This applies throughout all of the standards where it is used.
No
This should not apply to visitors – should read “shall make individuals who have authorized unescorted access…”. Visitors, although potentially have physical access to BES Protected Systems, should not need to be trained prior to entry, only their escorts need to be trained.
Yes
Yes
Note the typo. There is an extra "2" at the end of the sentence.
No
A general comment for many of the CIP Standards. It appears that most of the VSL are of the High and Severe Category. Many of these violations should be in the LOwer or Moderate VSL, particularly those dealing with paperwork.
Yes
Yes
No

Under R3.1 should require training only for "unescorted" access.
Yes
Yes
Yes
No
Table Part 7.1 It is impossible to always revoke access upon the termination date or resignations in the cases where multiple companies are involved. We cannot enforce this in 3rd party companies. Additionally, it is impossible to immediately change locking mechanisms in remote substations that are spread across large geographical regions. Many substations have multiple utilities utilizing the same control house. Keeping track of every employee in every support company is not practical and will reduce reliability. For High Impact Facilities terminations the next business day is practical. For resignations seven or days is reasonable. For Medium Impact facilities which may require driving to the remote site several days may be needed to get to all facilities. Table Part 7.2 While this may work in a control center, it is not practical or reasonable in transmission substation settings, particularly for devices that are not remotely connected. Please Note: Promoting someone or transferring someone does not make that person a security risk and should not be treated as such. Believe Medium Impact systems should have 30 days or more to complete since may require onsite trips to reprogram every device at the remote locations. Reprogramming and testing may take several days at each location. The better solution would be to use the same wording as in part 7.1 and only require "removing unescorted physical and Interactive Remote Access to BES Cyber Systems." This is possible by the following day. If this is adequate for terminated employees why shouldn't this be adequate for transferred employees.
No
Not all violations are High or Severe
No
Comments: Table Part 1.5 IDS should not be required - a firewall should be sufficient.
Yes
No
No
Table 1 – Strike “egress” from measures – egress is not stated in the requirement Clarify if this means that a substion employee working all day in a control house can just swipe a card once and then go in and out without reswiping the card as a visitor is allowed or does this require swiping a card every time he crosses the Defined Physical Boundary
Yes
Yes
No
No
Table 1 Part 1.1 – Need provision for TFE Table 1 Part 1.2 – Need provision for TFE A general comment that many of these requirements throughoout all of the proposed CIP standards, while practical in a PC or Control Center environments are not practical in substation and generation environments. Need to have the ability to request a TFE for many requirements.
No
Table 2 Part 2.1 – remove comma after the word “patches,” - the comma in the sentence requires that all software patches be included whether they are security related or not. Additionally, it is not

practical to include firmware as very few vendors post when firmware updates become available
No
Table 3 Part 3.3 – needs to define when the 30 days start – when the EMS vendor says it can be applied or when the virus definition manufacturer says it is available. Additionally, needs provision for TFE in case the virus definition kills the application. Table 3 Part 3.5 – should not apply to USB memory devices, CDs, test equipment in the substation, etc – if it does, requirement should be struck as this would be extremely burdensome. Logging connections does not prevent any introduction of malware.
No
Table 4 Part 4.1 – Although this may be practical for PCs, many substation devices do not have any logging capability at all – need ability to file TFE Table 4 Part 4.1.1 – Electronic Access Points should be addressed under CIP-005 Table 4 Part 4.1.4 – use of the word “potential” is vague and is not auditable The Application Guidelines indicate this is not required for devices that do not support logging. This is not what the requirement states. If this is what is meant then the requirement needs to state it. Table 4 Part 4.3 – strike “before the end of the next calendar day” – end sentence with “failures” Table 4 Part 4.5 – strike 4.5 completely – it is a duplication of 4.2 and 4..3
No
Requirement 5.6 would make a denial if service attack on an asset much more successful if someone could go down the list of accounts and access the account until locked out on all accounts. Would be better to alert for event rather than lock out.
No
should have lower and moderate VSLs
Yes
No
A Cyber Security Event may be totally different than anticipated in the plan. Flexibility needs to be allowed to respond to the event regardless of what is in the plan.
No
Table 3 Part 3.1 – Consider rewording so that the initial incident response plan implementation is no later than the effective date and the review and update is conducted during the initial calendar year. Table 3 Part 3.4 – change from 30 days to 60 days
No
No
Table 1 Part 1.5 – should be struck completely – preservation of forensic evidence should never take priority over the restoration of the BES. At most should state that "to preserve evidence if it does not adversely affect the restoration of the system"
No
Comments: Consider rewording so that the recovery plan implementation is no later than the effective date and updated once each calendar year. Table 2 Part 2.2 – remove the word “any” from the requirement. That could require reloading EVERY piece of information stored. Every daily backup tape, etc. Table 2 Part 2.3 – should be struck as it is a duplication of 2.1 – problems with 2.3 as written are what constitutes a full operational test of the plan – is it sufficient to reload one server or one workstation or replace a card in a computer? Additionally, if there are 4 scenarios written in the plan, do you have to do an operational test of each scenario?
No
Consider rewording so that the recovery plan implementation is no later than the effective date and updated once each calendar year. Table 3 Part 3.4 – change from 30 days to 60 days
No
No
Do not believe physical location is required. Table 1 Part 1.4.2 – strike “availability” – “availability” is a business function, not a security function – question – if you make 40 changes in a year and

“availability” goes down 1% (if you can determine that), how do you verify
No
Table 2 Part 2.1 – Should not be applicable to Medium Impact BES Cyber Systems unless they are remotely connected. For non-networked equipment this is an unreasonable requirement. Although it is Technically Feasible to have someone continually log on to the device every hour or every day to see if a change has been made this is impractical.
No
Consider rewording so that the implementation is no later than the effective date. Table 3 Part 3.2 – strike completely – 3.1 should be sufficient
No
No
COnsider rewording to no later than the effective date.
No
The requirement needs to be further clarified.
No
Many of the application guidelines interpret the requirement significantly different than I read the requirement. I request that the application guidelines be made a part of the standard and allowed to be used as a defence. I am afraid that auditors will use the requirement without the explanation or exemptions that are included in the Guidelines and audit to the language of the requirement. Where they can be interpreted differently the language in the Application Guideline needs to be included in the requirement or at least made equal in enforcement with the requirement.
Yes
I do not have any problem with the implementation plan but believe that those without entities that do not have a regulatory body would. Regulatory approval generally takes 6 to 15 month or longer. I believe that the effective date for non-regulated entities should be at least 6 to 12 months longer after BOT approval than after regulatory approval for regulated entities.
Group
ISO/RTO Council Standards Review Committee
Christine Hasha
Yes
Refer to additional comments submitted for Question 49. CIP Exceptional Circumstance: Request revision to “A situation that may involve one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance (internal or external), a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.” The definition needs some flexibility for entities to take appropriate measures without risking reliability of the BES that may not fit neatly into the conditions listed. Reportable BES Cyber Security Incident: Request that the drafting team keep this definition consistent with the efforts of the 2009-01 project team. The current definition does not align to the requirements listed in the new version of EOP-004. Intermediate Device: Recommended changes: “A Cyber Asset that 1) may be used to provide the required multi-factor authentication for the Interactive Remote Access; 2) may be a termination point for required encrypted communication; and 3) may restrict the Interactive Remote Access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside an Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network.” Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity’s Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access may be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants. BES Cyber Security Incident: “Suspicious” is not an auditable term, and should be removed. What is an “attempt”? What attempts are serious enough to justify having to be reported? The definition should be made to read: BES Cyber Security Incident A malicious act that: • Compromises the Electronic Security Perimeter or

Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. BES Reliability Operating Services: “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet • Recommend clarification that “Facility” is the NERC Glossary term--in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication”: • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret.
Yes
• For 2.12, request that “system” be capitalized as it appears to align properly with the NERC definition. Also, recommend removing “as required by is regional load shedding program”. • For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal?
No
Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. Regarding 1.1, suggest a grammatical fix: “Update the identification and categorization within 30 calendar days of when a change to BES Elements and Facilities is placed into operation…” The word “intended” should not be used in the requirement because it is not auditable. Request it be replaced with “planned”. M1: This sentence needs to be clarified. It appears to require documentation of the low impact assets though this is not required. “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.” Request changing M1 from “as required in R1 and list of changes to the BES” to “as required in R1 and list of changes to the BES Elements and Facilities”. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium, and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced throughout the Standards.
Yes
Recommend adding the following: “…has had its CIP Senior Manager or delegate review and update…”. Request that “initially upon the effective date…” be revised to not require all approvals on the effective date of the standards. It is not practical to expect all documentation to be approved precisely on the effective date.
Yes
Yes
Yes
Request clarification of the meaning of “implement” M2.2.

No
Suggested change: “Each Responsible Entity shall review each of its cyber security policies and obtain approval of the policies by its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.” As written, the requirement appears to require approval of the CIP Senior Manager rather than of the policies.
Yes
No
Suggested change: “The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved by the CIP Senior Manager and shall specify the authority that is being delegated.”
Yes
The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
Yes
Yes
No
Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement. Request that the differences between R2.2, R2.3, and R2.4 be detailed.
Yes
No
For all measures related to R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”. For R5.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
For R6.1 2. Change “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.3 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For 6.4, request clarification of whether variances noted in the verification would be required to be a self report. For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary”. Request clarification of whether variances noted in the verification would be required to be a self report. For R6.6 Request clarification of whether variances noted in the verification would be required to be a self report. 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I”

in Information.
No
Request that the footnote for 7.1 be moved into the requirement. Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend changing 7.3 to “For resignations or terminations, revoke the individual’s access to BES Cyber System Information by the end of the next calendar day following the date of termination.”
Yes
No
Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 and 1.5 Electronic Access Points are the Electronic Access Points identified in R1.2.
No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology. Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete.
Yes
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with. Request Requirement 1.2 be updated to allow "escorted physical access." Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress". Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.3 be consistent (not add a Requirement) with Requirement 1.3, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary " to "Issue real time alerts (to individuals responsible for response) upon detection of a breach through an access point". Request similar changes to R1.5. For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, ".
No
Request clarification of 3.1 and 3.2on what the "Associated" under "Applicability" pertains to (i.e.: High, Medium, or Low BES Impact).
Yes
No
Request clarification on R1.1, is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on M1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Recommend that “of BES Cyber Assets” be removed.
No

Request clarification of "remediation plan" in 2.2. Suggest wording like "create an implementation plan or a plan to mitigate the vulnerability where it is determined that the patch cannot be safely applied". What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to each patch or the overall process? Recommend removing “CIP Exception Circumstances” since the conditions in the definition do not align with the circumstances that may prevent the implementation of the patch. Suggest wording like "process for completion of the defined implementation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied".
No
Request allowances in 3.3 for signatures/pattern updates that cause trouble. Suggest adding “Create a plan to mitigate the vulnerability where it is determined that the signature or pattern update cannot be safely applied.” Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media".
No
Suggested wording: “Upon detection, activate a response to event logging failures before the end of the next calendar day. Request the rationale of 4.5's "two weeks". Recommend one month as a compromise between the prior version's 90 days and the suggested one week. Request clarification for inclusion of associated protected cyber assets. Are these protected cyber assets associated with only high impact BES cyber systems, or could they be associated with medium impact BES cyber systems? Request clarification of whether variances noted in the review would be required to be a self report.
No
For 5.2, does the CIP Senior Manager or delegate approve policy/procedure for each authorization of access or each actual use/login of the account? Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
Yes
Yes
No
For 2.1, recommended wording changes; "When a BES Cyber Security Incident is identified or tested, the incident response plans must be used and include recording of deviations taken from the plan." Recommend removing “initially upon the effective date of the standard” from R2.2 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. Please ensure that R2.3 aligns with the Evidence Retention section of the standard. Due to audit schedules, the entity may be required to retain the information for more than 3 years.
No
Recommend removing “initially upon the effective date of the standard” from 3.1 of Table R3 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. For 3.3, recommend changing "Update" to "Where necessary, update”. Recommend changing "the completion of the review of that plan" to "the completion of the review performed in 3.2".
No
The VSLs need to align with the requested changes in questions 34-36.
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommended change: “When backing

up Information essential to BES Cyber System recovery, verify the media to ensure that the backup process was successful.”
No
For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 2.1, request change to “functional exercise” rather than “full operational exercise”. This is consistent with the information provided in the rationale. Recommend that 2.1 and be implemented 180 days from the effective date of the Standard. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the Standard.
No
For 3.1, recommend removing “or when BES Cyber Systems are replaced” as it addressed in CIP-009 R3.4. Recommend removing “and document any identified deficiencies or lessons learned” as they are addressed in CIP-009 R3.2 and R3.3. Recommend that 3.4 be referenced by CIP-009 R3.1. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
The VSLs need to align with the requested changes in questions 38-40.
No
Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold.
Yes
No
For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 3.1, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend change for 3.2 “…perform an active vulnerability assessment in a test environment which models the baseline configuration of the BES Cyber System in the production environment.”
Yes
No
For 1.3, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames

specified. Grandfathering should be considered.
Yes
Yes
The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very "narrow" window. Since Version 4 is not FERC approved, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. A summary of comments applicable to more than one standard: . • Recommend removing "initially upon the effective date of the standard" from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • Request clarification of the capitalized term "Facilities." Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5. The SRC appreciates the efforts of the drafting team in producing the published standards. We look forward to responses to the comments and subsequent revisions to the standards. A fiftieth question should have been included in this comment form asking for general comments or concerns. A question asking general comments should be included as part of every comment form posted to the industry.
Individual
Darryl Curtis
Oncor Electric Delivery Company LLC
Yes
CIP Exceptional Circumstance: Request revision to "A situation that may involve one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance (internal or external to an entity), a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability." Reportable BES Cyber Security Incident: Request that the drafting team consider the efforts of the 2009-01 project team and assure consistency between the definition as proposed under the new version of EOP-004 (Version 2).
Yes
Every two years within the ERCOT interconnect, the ERCOT ISO facilitates the bidding and selection of Black Start generation resources. Oncor Electric Delivery Company, as a Distribution Provider, Transmission Owner, Transmission Operator, and Load Serving Entity (and as further defined within the constraints of the Texas retail market) is not part of this selection process. Likewise, Oncor may not be able to sufficiently implement CIP Compliance on impacted facilities (substations) in a timely manner as there is typically a two month time span between selection and implementation of newly selected generation units as Black Start resources . Oncor will be significantly time-constrained on achieving strict compliance on any of its own, newly identified BES Cyber Systems and/or BES Cyber Assets once any applicable generation units are selected. Consideration should be given to provide a doable CIP implementation schedule for Distribution Providers, Transmission Owners, Transmission Operators and Load Serving Entities within the standard to accommodate newly acquired applicable Black Start resources.
Yes
Grammatical Correction: "Update the identification and categorization within 30 calendar days of when a change to BES Elements and Facilities is placed into operation…" M1 States: "Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls." – According to R1, Entities that own BES Cyber Assets and BES

Cyber Systems shall identify and categorize only its High and Medium Impact BES Cyber Assets and BES Cyber Systems. All remaining are deemed “Low Impact”. Oncor Electric Delivery suggest that some clarification in the language is needed for M1:
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Jose H Escamilla

CPS Energy
Yes
BES Cyber Asset definition should take into consideration redundant system in determining availability. A system with high availability typically involves multiple levels of redundancy. A high availability multi-site system will not likely experience an interruption that would impact the BES Reliability Operating Services. It is recommended that the SDT adopt a definition that takes into account the availability BES Cyber Assets to the end-user (i.e. system operators).

Individual
Adam Menendez
Portland General Electric
Yes
General Comments: Portland General Electric Company (PGE) takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because PGE believes that the definitions require additional clarity and that certain terms, including “dial up accessible” must be defined. PGE is opposed to any instances of changes where there is no clear need as each modification requires extensive resources to modify existing compliance processes, documentation, and evidence. Requirements and/or Measures that use all-encompassing or absolute words like “any” and “all” introduce compliance challenges, as satisfying these definitions potentially introduce extensive additional elements that would be out of scope and increase risk of non-compliance. PGE requests the standards drafting team (SDT) to clarify, ‘locations’ as it relates to facilities. The term is vague and does not provide a clear understanding for how entities’ can identify and categorize its BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. If the SDT did enhance the term ‘location’ with geographical parameters (IE: How is a wind facility considered? What is an acceptable distance between generating units?) this would enhance entities’ classification processes. • BES Cyber Asset – PGE agrees with EEIs proposed change • BES Cyber Security Incident – PGE agrees with EEIs proposed change • BES Cyber System – PGE agrees with EEIs proposed change • BES Cyber System Information - PGE agrees with EEIs proposed change • Defined Physical Boundary – PGE agrees with EEIs proposed change • Inter-Entity Real-Time Coordination and Communication – PGE agrees with EEIs proposed change • Add the following definitions (from CAN-0007) - PGE agrees with EEIs proposed change • Other terms which would benefit from definitions o Adverse o Annual – Propose use of definition within CAN-0010 o Impact o Security Plan o Associated o Dial up-Accessible • Existing definitions that would benefit from alternative wording - PGE agrees with EEIs proposed change
Yes
PGE agrees with EEIs proposed suggestions
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO for the following specific reasons: 1. PGE believes that applying the BES Reliability Operating Services approach as set out in CIP-002-5 is confusing and therefore will be exceptionally difficult to implement. Additionally, the BES Reliability Operating Services approach expands the scope of the standards beyond what is necessary for security or reliability of the BES. This expanded scope will significantly increase demands on labor and capital and will not deliver a markedly more secure system. Further, it will make auditing the standards difficult which may slow the industry’s ability to correct misconceptions in application of the standards. 2. CIP-002-4, on the other hand, establishes a bright-line approach which is well understood by the industry and has already been approved by stakeholders. Retaining the structure set out in CIP-002-4 will encourage compliance and make auditing of the standards and corrections to application much simpler, thereby protecting the security and reliability of the BES. In addition, PGE believes that CIP-002-4 could be compatible with a tiered high-medium-low approach as is contemplated by the

Standards Drafting Team in Version 5. 3. Applicability – PGE agrees with EEIs concerns in reference to UFLS and UVLS is a point of concern and agrees with the proposed. 4. CIP-002-5 R1 – PGE agrees with EEIs proposed changes 5. CIP-002-5 R1.1 - PGE agrees with EEIs proposed changes 6. Because PGE believes that a compliance structure that is easy to understand, apply and enforce increases security and reliability, PGE votes “no” on CIP-002-5 and encourages the Standards Drafting Team to retain CIP-002-4.
No
PGE agrees with EEIs comments and proposed changes
No
PGE agrees with EEIs comments and proposed changes
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO for the following reasons: PGE also agrees with EEIs comments and proposed changes
No
PGE agrees with EEIs comments and proposed changes
No
PGE agrees with EEIs comments and proposed changes. This goes beyond the scope of FERC Order 706.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO for the following specific reason because the standard is worded in a way that PGE believes could create confusion regarding the timing of the requirements.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
Yes
No
PGE agrees with EEIs comments and proposed changes. Additionally, PGE proposes clarity for how these requirements are applied with regard to shared administrative accounts? The shared administrative accounts standard (CIP-007 R5.2) has been removed, in favor of this requirement, but it is not explicit here that this applies to shared administrative accounts. The conflict between these requirements in previous versions has caused some confusion.

No
PGE agrees with EEIs comments and proposed changes.
Yes
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard is worded in a way that PGE believes could create confusion. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard creates confusion around what evidence is required to prove compliance. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO for the following specific reasons: 1. The standard as written is vague when applied to the Electronic Security Perimeter and does not account for the technical capabilities of virtual environments. 2. Additionally, as server virtualization is more fully deployed in CIP-compliant environments, there will be a need to think differently about where security products are deployed. In the below statement from page 39 of the CIP-007-5 document, please take note of this section: "This control is another layer in the defense against network-based attacks, therefore it is the intent that the control be on the device itself; blocking ports at a perimeter does not satisfy this requirement. "The issue with this type of thinking is that applications are starting to move off of the virtual servers to virtual appliances running on the hypervisor. It could be very important that the wording of requirements related to servers not assume that products like firewalls, anti-virus, intrusion detection, etc actually resides on the server itself. 3. When server virtualization is being used, does every virtual server residing on a physical host, have to be treated at the same “impact” level? For example, can a physical host have a “high impact” virtual server used by the Control Center, and also contain other virtual servers with a “low impact” rating. 4. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.

No
PGE agrees with EEIs comments and proposed changes. R4.2 Consideration- The real time alerting required by R4.2 may not be technically feasible in all situations and the requirement does not provide adequate guidance on what to do in such situations. Additionally, it is not clear how to treat shared administrative accounts for purposes of compliance with R5. R4.3 Consideration- This sub-requirement seems to conflict with 4.5. If the purpose of 4.5 is to “identify… potential event logging failures” and occurs every two weeks, what about the 4.3 requirement to “detect and respond to event logging failures before the end of the next calendar day”? Please clarify.
No
PGE agrees with EEIs comments and proposed changes. R5 Consideration - How shall this requirement be applied with regard to shared administrative accounts? The shared administrative accounts standard (CIP-007 R5.2) has been removed, in favor of this requirement, but it is not explicit here that this applies to shared administrative accounts. R5.1 Consideration - If PLCs are included in the definition of BES Cyber System they may not be technically capable of meeting this requirement.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard is worded in a way that PGE believes could create confusion regarding applicability and evidence measures. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO for the following specific reasons: 1. As written, the standard is overly broad and vague. It is not clear what exactly “information used in the recovery of BES Cyber Systems that is stored on back up media” relates to and because of this confusion, the standard could apply to hundreds of thousands of files. The lack of clarity in what the standard requires owners to test means that PGE cannot determine if compliance with this standard is technically feasible or, if it is possible, what the resulting burden would be. 2. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
Yes
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have

assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard does not effectively capture the intent of FERC Order No. 706. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
Yes
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard is worded in a way that PGE believes overly broad and confusing regarding applicability. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because PGE believes the implementation plan is incomplete because it does not capture all of the milestones laid out in the standards themselves necessary to achieve compliance. PGE also agrees with EEIs comments and proposed changes.
Group
EPUC, CAC and NCA
Donald Brookhyser
No
No
Yes
Yes
No
The following comments address the approach of Version 5 generally. They are provided here as the first available opportunity in this comment form: These comments are submitted by the Energy Producers and Users Coalition, the Cogeneration Association of California, and Nevada Cogeneration Associates #1 and #2 (collectively “the Cogeneration Parties”). As drafted, the Version 5 CIP standards impose significant new requirements on Responsible Entities, arguably without any material change in real protections related to access to, or vulnerability of, cyber systems. These additional administrative burdens are being imposed on entities that are already registered and compliant with the existing version of the standards, although their susceptibility to threat has not increased. The new standards will not impose any new limitations on access to cyber assets, and only create

additional, burdensome administrative support for the existing limitations. The Cogeneration Parties recommend that Responsible Entities that identify only Low Impact Cyber Systems in complying with CIP-002 be excused from compliance with any other CIP standard. Discussion All of the facilities operated by the Cogeneration Parties are generating facilities that are small enough that their assets qualify under the Version 5 definition as Low Impact BES Cyber Systems. This exclusion due to size probably applies to most of the generators in the Western Interconnection. As such, all of the substantive requirements that actually limit access or address vulnerabilities do not apply. This includes Standards CIP-004, Requirements 2-7; CIP-005, R2; CIP-007, R1-4; and CIP-009 through CIP-011. What will apply to these generators are the requirements for more detailed plans (Standard CIP-003 and CIP-006, R1), more training and awareness (CIP-004, Requirement 1), and a Cyber Security Incident response plan (Standard CIP-008). The CIP standards have up until this point been limited in their applicability based on access. The standards only required compliance from generators with cyber equipment that had either a routable protocol or dial-up access. That limitation excused from compliance with the CIP standards many of the generators that had registered. The early descriptions of Version 5 of the standards suggested that this same limitation on compliance based on access would be continued. But to the contrary, the draft has added many new requirements that are not so limited. The only requirement so limited by access is CIP-005, R1. To provide some rational limitation on the administrative burdens imposed by these proposed standards, the Cogeneration Parties suggest that where a Responsible Entity has only Low Impact Cyber Systems, it must perform the identification of cyber systems required by CIP-002 and then be excused from compliance with any of the other CIP standards.
No
See answer to Question 7

Group
Tacoma Power
Travis Metcalfe
Yes
Under the “BES Cyber Asset” definition there should be a different category for assets that can be misused versus those can only be rendered inoperable. For example, the loss of a RS232/RS484 to fiber optic converter on a 500 kV transformer temperature gauge would result in a minor loss of situational awareness, thus becoming a medium impact cyber asset. The focus should be on assets that could potentially be misused. BES Cyber Asset-“Adversely Impact” should also be a defined term. It should be defined as: An effect that results in a violation of any BAL, INT, IRO, or TOP standard or makes unavailable or significantly reduces operational ability.” BES Cyber System Information—The current definition uses the phrase “security procedures”. “Security procedures” covers a wide variety of possible procedures rendering the definition vague and overbroad. Provide clarification as to what security procedures need to be protected. BES Reliability Operating Services- This definition is overly broad because impacts to some of the specific bulleted items do not directly impact BES reliability. Furthermore, some of these functions are typically performed or stored outside of a control center with no electronic link to real time control systems. Recommend removing the following sections: 1. “Know generation status & capability & restrictions (must runs, minimum run times, ramp, heat rates, etc).” Some of this data is calculated, stored or communicated outside of a real-time control system. 2. “Know generation status, capability, ramp rate, start time “Some of this data is calculated, stored or communicated outside of a real-time control system. 3.”Monitoring and alerting (such as EMS alarms)” Not all EMS alarms are critical to BES reliability. 4. “Change management - Current Day & Next Day planning - Contingency Analysis” These functions are typically performed by engineers in an office environment instead of a real-time control center. These functions are not needed with a 15 minute time frame, but the current definitions could lead to categorizing the computers to do these functions as cyber assets. Control Center-This definition is overly broad because it includes many locations not traditionally thought of as control centers. The definition should include that the site is regularly staffed by System Operators and a separate definition should be created for data centers and other facilities that perform some of the same functions. Examples of unmanned locations that would become control centers per the current definition include: Substations that present the status of remote breakers or equipment, each communication facility that has more than one utility present, and the terminals of a transmission line that use tele-protection. Cyber Assets devices that are not programmable via communications should be excluded from a list of BES Cyber devices. There are many substation devices programmed via DIP switches or just an HMI such as temperature monitors and serial communications media converters that represent a very low possibility of misuse, but could currently be classified as medium impact assets. Tacoma Power also supports the comments submitted by APPA. Tacoma also supports the comments submitted by the Edison Electric Institute with the exception of the changes proposed for BES Cyber Security Incident.
Yes
Attachment 1 criteria for a High Impact rating should be more specific than “any” for a Control Center or Backup Control Center performing the functional obligations of a Balancing Authority Tacoma Power supports APPA’s comments regarding BA’s designated as High Impact for the following reason.

• There are 107 Balancing Authorities subject to NERC regulation but not all have the same level of impact to the BES. For example the States of New York and Texas have one Balancing Authority each, while Arkansas and Arizona each have eight and Florida has eleven. Some BA's in States with multiple BAs are operated by relatively small municipal utilities and control less than 1,000 MW. CIP-002-5 needs to set a threshold limit to determine which BA's should be categorized as High Impact and which should be categorized at a lesser impact level. CIP-002-5 states that BES Cyber Assets are those cyber assets that, if rendered unavailable, degraded, or misused, would impact the BES Reliability Operating Services within 15 minutes of the activation or exercise of the compromise. Both High Impact and Medium Impact categories contain the time element in their definition but Low Impact does not. The standard needs to be clear on whether the time quantifier applies to Low Impact assets. CIP-002-5, R1 states that "All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification". Subsequently some of the CIP-003-5 through CIP-011-5 standards identify specific requirements and measures that apply to "Low Impact" systems. Therefore, the standards are unclear as to how an entity may demonstrate compliance with requirements that apply to "Low Impact" systems without providing "discrete identification" of these systems. For example, CIP-005-5, R1.1 requires entities to "define technical or procedural controls to restrict unauthorized electronic access" with a measurable to include "documented technical and procedural controls that exist and have been implemented". The standards appear to be self-contradictory in that they require documentation for implementation of controls on "Low Impact" systems but state that "Low Impact" systems do not require discrete identification. This will become problematic both for auditing compliance and ensuring all Low Impact systems have been identified and properly protected. Recommend requiring a list of Low Impact Assets. CIP-002-5, Attachment I, criteria 2.13 sets a threshold of 300 MW or more of generation for generation control centers to become "Medium Impact". Unlike the "1500 MW in a single interconnection" value in criteria 2.1 for "Medium Impact" systems, which is derived from the most significant Contingency Reserves operated in BAs in all regions, the 300 MW threshold is not clearly justified in the application guidelines. There is a statement in the Transmission section of the CIP-002 Application Guidelines stating "the drafting team understands that the real-time impact to the Bulk Electric System of a loss of load, or the equivalent amount of generation, will be similar, with….loss of generation resulting in a frequency low condition." This statement appears to directly contradict the 1500 MW limit in 2.1 in regards to generation. The standard and application guidelines fail to justify or articulate how the UFLS and UVLS 300 MW "bright line" for transmission load shedding is applicable to Generation. Recommend that the SDT provide justification for this requirement Regarding the NERC definition of "Control Center" and the use of the definition in CIP-002-5 Attachment I, the definition is not clear on whether two or more process control systems at two or more generation plants, whose combined outputs exceed the 300 MW threshold, that are interconnected to provide maintenance staff with real-time data but are not directly used by the System or Generator Operator for supervisory control of the generator would be considered "Control Centers". As an example, consider two hydroelectric generation facilities separated by a mile of river each with a process control system for the generators. These two local control systems are interconnected for use by roving local maintenance staff but data from these systems is independently sent from each generation facility via telemetry to the System and Generator Operator's SCADA system for use in controlling and monitoring the generators. It is not clear from the definition whether the process control systems at the facilities would be considered "Control Centers" due to the interconnection or whether, because these systems are not the same as the System Operator's SCADA system, they would be excluded. Recommend that the SDT provide clarification. Please refer to comments on the definitions for BES Reliability operating services and Adversely Impact. As currently written, this would categorize almost every cyber asset in EHV substations as medium impact. In context with the PSP access and logging requirements, this effectively eliminates having any electronic devices mounted directly on Substation equipment as it would be impractical to meet those requirements. Recommend further refining the definition. The description of redundancy in the background information should be expanded to clarify whether different systems without common mode failure points are allowed. For example, if load and generation forecasts can be manually entered by a System Operator but are usually entered using an automated forecasting tool, is the automated tool considered redundant or superfluous cyber asset? Tacoma Power recommends expanding/clarifying the definition.

No

Tacoma Power supports the comments of the Edison Electric Institute.

No
Tacoma Power supports the comments of the Edison Electric Institute.
No
Updating documentation required by R1.1 should not go from lower to severe just by doubling the time. Periods of 60, 90, 120 and 120+ days would be more appropriate based on the time requirements than the proposed 40, 50, 60 and 60+ days.
Yes
No
Recommend that for clarity under R2 1.5 the policy currently named System Security be renamed to Cyber System Security. Recommend making a distinction of how 1.10 - Provisions for declaring and responding to CIP Exceptional Circumstances differs from 1..6 – Incident Response and 1.7 – Recovery Plans.
Yes
Yes
Yes
Yes
Yes
Yes
No
Tacoma Power supports the comments of the Edison Electric Institute.
No
The application of the standard is inconsistent. If the requirements of CIP-004-5 R2 are not applicable to Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Assets, why are they included in CIP-004-5 R3? We suggest including the Associated PACS system in CIP-004-5 R2 or deleting it from CIP-004 R3.
No
Tacoma Power supports the comments made by NPCC and the Edison Electric Institute.
No
The application of the standard is inconsistent. If the requirements of CIP-004-5 R4 are not applicable to Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Assets, why are they included in CIP-004-5 R5? We suggest including the Associated PACS system in CIP-004-5 R4 or deleting it from CIP-004 R5.
No
Tacoma supports the comments made by Edison Electric Institute with the exception of changing the quarterly review to an annual review.
Yes
Yes
No
Tacoma Power supports the comments submitted by APPA and the Edison Electric Institute.
No
Tacoma Power supports the comments submitted by APPA and the Edison Electric Institute.

Yes
No
R1.1 According to CIP-006-5 R1.1, Associated Physical Access Control Systems must have controlled access on par with a Low Impact BES Cyber System. According to Part 1.1 of the table, this does not require the protection of a Defined Physical Boundary that restricts access to only authorized individuals, nor does it require logging of access events. Furthermore, it specifically states that it does not require a detailed list of individuals with access. This appears to be inconsistent with the requirements of CIP-004-5 R3, R5, R6, and R7 which include completion of role-based training, a personnel risk assessment, and approval of access rights prior to granting access, review of access rights, and timely revocation of access rights. These requirements would seem to require listing individuals with authorized access and tracking access events. R1.2 and 1.3 Measures of evidence for CIP-006-5 R1.2 and R1.3 include the statement: "…ingress and egress is controlled by one or more of the following methods…" Controlled egress is currently not required. Recommend changing "ingress and egress" to "access." R1.5 It appears inconsistent that unauthorized access alerts and response are required on par with the monitoring and response requirements for the Defined Physical Boundaries that protect High and Medium Impact BES Cyber Systems if a Defined Physical Boundary that restricts physical access to only those that are authorized is not required per CIP-006 R1.1. Recommend rewriting the requirement to clarify this issue. Tacoma Power also supports the comments submitted by APPA. Tacoma Power also supports the Edison Electric Institute comments with the exception of the change to requirement. 1.4.
Yes
Yes
Yes
Yes
No
Tacoma Power supports the comments submitted by the Edison Electric Institute.
No
Tacoma Power supports the comments submitted by the Edison Electric Institute.
No
Tacoma Power supports the comments submitted by the Edison Electric Institute.
No
Tacoma Power supports the comments submitted by APPA and the Edison Electric Institute.
Yes
No
Tacoma Power supports the comments submitted by APPA and Edison Electric Institute.
No
Tacoma Power supports the comments submitted by APPA and Edison Electric Institute.
No
Tacoma Power supports the comments submitted by APPA and Edison Electric Institute.
Yes
No
Tacoma Power supports the comments submitted by Edison Electric Institute.
No
Tacoma Power supports the comments submitted by Edison Electric Institute.

No
Tacoma Power supports the comments submitted by Edison Electric Institute.
Yes
No
Tacoma Power supports the comments submitted by APPA and Edison Electric Institute.
No
Tacoma Power supports the comments submitted by Edison electric Institute.
No
Tacoma Power supports the comments submitted by Edison Electric Institute as modified below. 1. 3.1 1. Requirements – Proposed content change ♣ Original Text – Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed. ♣ Proposed Change – On an annual basis, conduct a paper or active assessment of the cyber security controls to determine the extent to which the controls are implemented correctly and operating as designed. • Propose the addition (3.1.1) of minimum cyber security controls to be assessed that; o Are referenced within these standards; and o Are not already required to be assessed in other standards (removing double jeopardy implications) ♣ Rational • Annual (as defined within CIP-0010) should be the consistent approach to allow entities to standardize annual requirements on a consistent basis. • Active assessment is cited within Part 3.2 (to be done every 39 months) so we've removed it from this part to avoid overlap. 2. Measures – Propose content change ♣ Original Text – Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the output of the tools used to perform the assessment. ♣ Proposed Change – Evidence may include, but is not limited to: • A document listing the date of the assessment, the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the assessment results. ♣ Rational – Annual should align with CAN-0010 definition. Documentation of assessment results focus on the root information in support of vulnerability rather than potentially extensive data (from tools) that may require extensive resources to retain. 2. 3.2 1. General observations ♣ While the application guidelines recognize production devices which may not be capable of modeling within a test environment (ICCP, etc.), this requirement does not provide clear guidance to follow where these instances occur. ♣ The 39 month cycle exceeds the 3 year retention requirements. 2. Requirements – Propose content change ♣ Original Text – Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments. ♣ Proposed Change – At least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production. 3. Measures – Propose content change ♣ Original Text – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment. ♣ Proposed Change – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments. 3. 3.4 1. Requirements – Propose content change ♣ Original Text – Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.

♣ Proposed Change – Document the results of the assessments (conducted within 3.1-3.3) and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Rationale – referencing parts 3.1 – 3.3 provides alignment with the previous parts of the standards.
Yes
No
Tacoma Power supports the comments submitted by Edison Electric Institute.
Yes
Yes
Yes
Individual
Scott Miller
MEAG Power
Yes
MEAG Power supports the comments submitted by APPA.
Yes
MEAG Power supports the comments submitted by AECI.
No
MEAG Power supports the comments submitted by APPA.
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
Yes
Yes
Yes
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
Yes
Yes
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
Yes
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
Yes
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.

Yes
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
Yes
Yes
Yes
Yes
No
MEAG Power supports the comments submitted by APPA.
Individual
Maggy Powell
Constellation Energy on behalf of Baltimore Gas and Electric, Constellation Power Generation, Constellation Commodities Group and Constellation Energy Control and Dispatch
Yes
Because the definitions underpin the suite of CIP standards, it is key that they are clear and understood by all stakeholders. Constellation offers the following comments and suggestions on the proposed definitions: BES Cyber Asset – The definition needs to better focus on the cyber asset rather than the 15 minute time qualification. The 15 minute description should be removed whenever "BES Cyber Asset" is used in a standard as it will be duplicative to the definition. Also, "when required" does not seem necessary in the definition. Proposed Revision: BES Cyber Asset – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation adversely impact one or more BES Reliability Operating Services. This is regardless of any delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. Redundancy shall not be considered when determining adverse impact. A Transient Cyber Asset is not considered a BES Cyber Asset. BES Cyber Security Incident – The definition should clarify that the terms "malicious" and "suspicious" are to be determined at the discretion of the Registered Entity and not by an auditor. In addition, in accordance with a request to return to using the term Physical Security Perimeter instead of Defined Physical Boundary (below), replace DPB with PSP. Proposed Revisions: BES Cyber Security Incident – A malicious act or suspicious event (as determined by the Registered Entity) that: • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or, • Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or • Results in unauthorized physical access into a Physical Security Perimeter. BES Cyber System – The word "typically" in the definition is too vague and lessens the clarity of the definition or its use in other standard language. “Typically” should be removed from the definition and the body of proposed standards. “Maintenance Cyber Asset” should be replaced with “Transient Cyber Asset.” Proposed Revision: BES Cyber System – A BES Cyber Asset or group of BES Cyber Assets (logically or physically) that operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. BES Cyber System Information – The term: "BES Cyber System Impact" is stated in all capitals, but “impact” should be in lower case since it is not defined. BES Reliability Operating Services – In general, further consolidation of the operating services is needed. Assets such as governors, automatic voltage regulators, and power system stabilizers fall into a number of the different BES Operating Services; therefore, a reordered definition will be more cohesive. For example, combining "controlling frequency," "controlling voltage," and "monitoring and control" are all related to ensuring

the BES is operating within its bounds. In addition, further clarity on who/what provides these services needs to be added (e.g. "Aspects of BES Dynamic Response, Spinning reserve - Providing actual reserves" it is not clear who provides the reserves). The Application Guidelines language in CIP-002 offers a good example for revision (see pages 19-22). The Operating Services definitions should include the parenthetical reference to describe who/what provides the service. Specifically under the section on Dynamic Response, Special Protection Systems or Remedial Action Schemes, the word “possibly” is too vague and should be removed. As well, further clarification is needed on what “software” is intended for inclusion. Unless “software” is specifically clarified, it should be removed. Proposed Revision: BES Real-Time Reliability Operating Services – BES Real-Time Reliability Operating Services are those real-time services or functions contributing to the real-time reliable operation of the Bulk Electric System (BES). They include the following Operating Services: Dynamic Response to BES conditions - Operation, monitoring or control of BES Elements, Facilities or systems that automatically respond to a BES condition. The operation, monitoring or control of BES Elements, Facilities or systems designed to perform an action or respond to a condition precedent. Aspects of BES Dynamic Response include, but are not limited to: • Spinning reserve (contingency reserves) – Deploying reserves (GOP) – Monitoring reserve levels (BA) • Governor Response – Control system used to actuate governor response (GO) •Protection Systems (transmission and generation) – Line, bus, transformer, generator (TO, GO) – Zone protection (TO, GO) – Breaker protection (TO, GO) – Current, frequency, speed, phase (TO, GO) - Under and Over Frequency relay protection (includes automatic load shedding) and their sensors, relays and breakers (DP) - Under and Over Voltage relay protection (includes automatic load shedding) and their sensors, relays & breakers (DP) • Power System Stabilizers (GO) • Controlling Frequency (Real Power) Generation Control (such as AGC (Automatic Generation Control)) – ACE (Area Control Error), current generator output, ramp rate, unit characteristics (BA, GOP) – Software to calculate unit adjustments (BA) – Data Transmittal to individual units (BA) – Unit controls responding to data transmittals (GOP) • Regulation Deployment (regulating reserves) – Frequency data (BA) – Governor control system (GOP) • Controlling Voltage (Reactive Power) - AVR (Automatic Voltage Regulation) – Sensors, stator control system, feedback (GOP) -Capacitive resources – Status, control (auto), feedback (TOP, TO, DP) -Inductive resources (transformer tap changer, or inductors) – Status, control (auto), feedback (TOP, TO, DP) -SVC (Static VAR Compensators) – Status, computations, control (auto), feedback (TOP, TO, DP) Balancing Load and Generation - Operation, monitoring or control of BES Elements, Facilities or systems necessary for provide awareness of or respond to load and generation balancing conditions in real-time. Aspects of the Balancing Load and Generation Operating Service include, but are not limited to: • Calculation of ACE – Field data (real time tie flows, frequency sources, time error, etc) (TO, TOP) – Software used to perform calculation (BA, RC) • Unit commitment information and communication – Know generation status, capability and load schedules (TOP, BA) • Controllable Load management/Demand Response – Ability to identify load change need (BA) – Ability to implement load changes (TOP, DP) • Remote Manual Initiated Load shedding – Ability to identify load change need (BA) – Ability to implement load changes (TOP, DP) • Remote Operation of Non-spinning reserve (contingency reserve) (GOP) Managing Constraints - Operation, monitoring or control of BES Elements, Facilities or systems that are necessary to ensure that the BES is operated in real-time within design limits. Aspects of the Managing Constraints include, but are not limited to: • Available Transfer Capability (ATC) Calculation (TOP) • Interchange schedules [Impact Analysis or Curtailment] (TOP, RC) • Identify and monitor SOL’s & IROL’s (TOP, RC) • Identify and monitor Flowgates (TOP, RC) SCADA and Substation Automation - Real-Time remote operation or control of breakers and switches and situational awareness. (TOP, GOP, RC, BA) Restoration of BES - Operation, monitoring or control of BES Elements, Facilities or systems that are necessary to reinstate reliable operation of the BES from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES Operating Service include, but are not limited to: • Blackstart unit and planned cranking paths (TOP, GOP) • Off-site power for nuclear facilities. (TOP) Situational Awareness - Operation, monitoring or control of BES Elements, Facilities or systems necessary to (i) assess the real-time condition of the BES or (ii) anticipate effects of planned and unplanned changes to BES conditions. Aspects of the Situation Awareness Operating Service include, but are not limited to: • Monitoring and alerting systems (such as EMS (Energy Management System) alarms) (TOP, GOP, RC, BA) • Change management [Change Management seems to vague compared to the other services listed. We request that the drafting team provide, more information to clarify. (TOP, GOP, RC, BA) • Current Day planning (TOP) • Contingency Analysis (RC) • Frequency monitoring (BA, RC) Inter-Entity Real-Time Coordination and Communication - Operation, monitoring or control of BES

Elements, Facilities or systems necessary for the coordination and communication of BES condition data between Registered Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication Operating Service include, but are not limited to: • Scheduled interchange (BA, TOP, RC) • BES Element, Facility or system operational data and status (TO, TOP, GO, GOP, RC, BA) • Operational directives (TOP, RC) [We request that the Drafting Team provide an example of the type of directive that is covered in relation to cyber assets/systems. Perhaps one example is the operation of a breaker/relay using a BES Cyber System (Asset)] CIP Senior Manager – Greater clarity needed on what is meant by "official" and does it mean that the CIP Senior Manager must be a company "officer"? Control Center – Control Center should not be defined in CIP Version 5. The term attempts to concisely define a complex and varied setting and risks creating more complications to applying the CIP measures. The team should remove the Control Center definition and allow the boundaries established in Attachment 1 to define the various control centers intended to deploy controls. If “Control Center” must be defined, it should be done by a separate, focused drafting team to tackle the complexities inherent in such a definition. This definition could be the stumbling block to achieving stakeholder support for the suite of Version 5 standards if not properly composed. Defined Physical Boundary (“DPB”) – The term “Physical Security Perimeter (PSP)” is more widely understood as a security term than is Defined Physical Boundary (“DPB”). However, the inclusion of the 6-wall perimeter requirement in the previous PSP definition was problematic. Now that the 6-wall requirement is removed, PSP is a better term than defining DPB. In addition, we propose two other refinements. Replacement of the DPB with PSP, if approved, will require replacement of the terms throughout the standard language. Proposed Revision: Physical Security Perimeter (PSP) - The physical boundary securing locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside and for which access is controlled. Electronic Access Point (“EAP”) – The cyber asset serving as an EAP both "restricts" and allows communication. Further evaluation of this term may be warranted as it may be understood differently as a definition versus in the context of the standard language. We continue to evaluate the proposed definition and may have additional comments. Proposed Revision: Electronic Access Point (“EAP”) - An interface on a Cyber Asset controls routable or dial-up data communications between Cyber Assets. External Connectivity and External Routable Connectivity – “External Connectivity” does not appear to be used in Version 5, though the definition makes more sense as a definition of “External Routable Connectivity.” We propose removing the term “External Connectivity”, but retain the definition language for “External Routable Connectivity.” Proposed Revision: External Routable Connectivity – Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter. Physical Access Control Systems – Revise in accordance with a request to return to using the term Physical Security Perimeter instead of Defined Physical Boundary. Proposed Revision: Physical Access Control Systems - Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s) exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. Reportable Cyber Security Incident – This definition must be consistent with the language in EOP-004 and the Events Analysis Process. (Please see additional comments to Question 36 regarding the relationship between CIP-008 and EOP-004). Transient Cyber Asset – Greater clarity is needed to confirm that “connected for 30 days” means a continuous connection for 30 days. As well, the criteria should require condition 1 along with condition 2 or condition 3, but not necessarily both. Proposed Revision: Transient Cyber Asset – A Cyber Asset that is directly and continuously connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset and 1) used for data transfer, maintenance, or troubleshooting purposes, or 2) capable of altering the configuration of or introducing malicious code to the BES Cyber System.

Yes

Repeating the definition language in Attachment 1 (for both the High and Medium Impact language) is redundant and, at present, the language does not match the proposed definition. Proposed Revision: “High Impact Rating: Each BES Cyber Asset or BES Cyber System used by and located at:” “Medium Impact Rating: Each BES Cyber Asset or BES Cyber System for:” In addition, per our proposal regarding the definition of Control Center, the term should be made lower case in Attachment 1. CIP-002-5 1.3: It's not clear what functional obligations are targeted by including TO. TO should be deleted. CIP-002-5 2.13: Generation control centers of 300 MW or more is too low of a threshold. Considering that drafting team states that a loss of generation of 1500 MW or more would have a medium impact to the BES, it is only logical that a control center capable of losing that much generation should then be medium as well.

No
It seems odd that CIP-002-5 R1.1 would require updates only when the impact category increased. As well, it is not clear whether “within 30 days” means before, after or either and it is not clear what defines the “change.” Proposed Revision: CIP-002-5 R1.1. Update the identification and categorization when a change is made to the BES Cyber Systems or BES Cyber Assets that is intended to be in service for more than 6 calendar months. The update shall be made within 30 days following when the changed BES Cyber System or BES Cyber Asset performs a Reliability Operating Service. It is also important that changes track with the language of the implementation plan. Constellation proposes changes to the Implementation Plan to address coordination with CIP-002-5 R1.1 and other concerns with the Implementation Plan. (Please see our response to Question 49). CIP-002-5 M1: Guidance to auditors should clarify the "includes, but not limited to" means that other forms of evidence other than those listed are acceptable to demonstrate compliance and it does not mean that other evidence is to be collected in additions to the types listed.
No
CIP-002-5 R.2: More clarity is needed on whether the team intends for the CIP Senior Manager or delegate approve required changes in identification and categorization. CIP-002-5 M2: For consistency with the requirement, the measure should read: "CIP Senior Manager or delegate". Proposed Revision: CIP-002-5 M2. Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate to review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.
No
In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.
No
CIP-003-5 R1. To accommodate the fact that a parent or affiliated company, not the Responsible Entity, may be the entity that identifies the CIP Senior Manager, this requirement should allow sufficient flexibility to accommodate varying corporate structures. Proposed Revision: CIP-003-5 R1. Each Responsible Entity shall have an identified CIP Senior Manager by name. CIP-003-5 M1. Further consideration should be given to how the qualification as a “high level official” can be audited. Does this mean that an officer of the company shall designate the CIP Senior Manager?
No
CIP-003-5 Requirement R2 does not require implementation of the ten topics, it requires implementation of the policies. Either remove the second bullet point or revise to clarify. Proposed Revision: Evidence may include, but is not limited to: 1. One or more documented cyber security policies, and 2. Records that indicate the policies address the ten topics enumerated in R2.
No
Constellation requests that “or delegate” be added to follow “CIP Senior Manager.” Given that the Senior Manager can delegate certain responsibilities, there may be instances in which the delegate is the more appropriate approver for a certain topic area that is to be covered by the policy documents.
No
CIP-003-5 M4: Further clarification is needed on the expectations of what is required to demonstrate awareness. We recognize that the measure correctly states that “Evidence may include” the listed items. Yet, we paused to consider what an effective demonstration of awareness is. Does the team feel that more than one of these listed items is required to demonstrate awareness? Further complicating the consideration is that training is not required as part of the requirement; however, dated training records are listed as an acceptable form of evidence. Listing things in measures that are not in the requirement is touchy for the audit context and auditors must be advised that training is not required. That said, it is understandable that an entity could deploy a robust awareness training program that would sufficiently demonstrate compliance on its own. Further guidance is requested.
No

CIP-003-5 R5: Constellation recommends removal of “with the exception of the approval of the Cyber Security Policy.” Note that the reference to the Cyber Security Policy as a single document in R5 is inconsistent with R2 and R3, where one or more cyber security policies are discussed. What does the SDT envision? A series of policy documents that address the 10 cyber security topics required under R2 or a single all encompassing cyber security policy document that addresses all 10 topics therein? Care should be given to avoid creating an overly cumbersome approval requirement and requirements need sufficient flexibility to accommodate varying corporate structures. CIP-003-5 M5: Change first sample bullet to RC control center instead of substation. The example may imply that all substations will be subject to this control and that may not be the case.

Yes

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

CIP-004-5 R1: The removal of the need to ensure that “everyone” received awareness is a positive improvement. CIP-004-5 Table R1, 1.1 adds a new term: “concepts.” The use of terms becomes problematic if accompanied by an assumed definition. Even though many terms – practice, program, procedures, are at times used interchangeably, entities now have experience in which auditors expected the title of the document to match exactly what is stated in the requirement even though functionally the terms were the same. Are entities to define what is meant by “concepts.” In addition, it is unclear what is meant by "reinforcement" in the R1.1 requirement. CIP-004-5 M1: Greater clarity is needed regarding the CIP-004-5 Table R1, 1.1 measures to understand what "material" qualifies as "reinforcement of such concepts." CIP-004-5 M1: Why did the command change from “may” to “must”? CIP-004-5 M2 states “must,” but only the measures in CIP-004-5 Table R2.1 state “must,” the rest state “may.”

No

CIP-004-5 R2: The term “role-based” is correctly lower case to allow the entity to define the roles and the associated training; however it should be emphasized to auditors that this is an entity determination and should be judged in the context of the entity program. Further discussion in the Application Guidelines may also be helpful. CIP-004-5 R2.3: Unlike the other requirements in R2, R2.3 discussed “proper use” of physical access controls. It is more consistent to remove the “proper use” reference or perhaps “implementation” is a more accurate and consistent word. CIP-004-5 Table R2 applies to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets.

No

CIP-004-5 Tables in R3 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In addition, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-004-5 M3 states “must,” but the measures in Table R3 state “may.” M3 should be revised to say “may.”

No

CIP-004-5 R4: Further clarification is required on expectations regarding personnel who have a valid personnel risk assessment (PRA) in place under Version 3 or 4. Those PRAs should remain valid and entities should not be required to conduct new PRAs for the sake of the standard revision to Version 5. CIP-004-5 M4.2 in Table R4 needs additional clarity on treatment if a seven year record is "not possible" keeping in mind that background checks go back to age 18 and not before. Background checks will be needed for individuals under the age of 25. In addition, the measures do not consider whether an FBI background check qualifies as acceptable. FBI checks are considered thorough and

reliable; however, the FBI is not obligated to follow the NERC requirements. Confirmation of an FBI background check should be acceptable evidence. CIP-004-5 Tables in R4 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. CIP-004-5 M4 states “must,” but the measures in Table R4 state “may.” M4 should be revised to say “may.”

No

CIP-004-5 Tables in R5 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In addition, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-004-5 M5 states “must,” but the measures in Table R5 state “may.” M5 should be revised to say “may.”

No

On the CIP-004-5 R6.1, 6.2 and 6.3 requirements, further clarification needed on how "minimum necessary" is to be judged. As well, “delegate" should be plural, "delegate(s)" as authorization of access for a corporation may be made by more than one delegate. CIP-004-5 M6.1: The discussion of sampling is inappropriate for the measure because it is an auditing method rather than a form of evidence. In addition, “workflow” is too general a term here. In addition, the format of the evidence options should be bulleted to be consistent with other table formats and to make the items options for evidence, not a required package of evidence. Proposed Revisions: CIP-004-5 M6.1 Acceptable forms of evidence include, but are not limited to: • a system-generated list of people with electronic access • a signed document, authorization workflow or email showing such persons have authorization • similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization. CIP-004-5 M6.2 Acceptable forms of evidence include, but are not limited to: • a system generated list of people with unescorted physical access through the Defined Security Boundary and a sampling of accounts (for automated physical access control) to verify unauthorized users do not have access • a signed document, workflow or email showing such persons have authorization • similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization. CIP-004-5 M6.3 Acceptable forms of evidence include, but are not limited to: • a list of people with access to BES Cyber System Information and a sampling of accounts (on electronic document systems) to verify unauthorized users do not have access • a signed document, workflow or email showing such persons have authorization • similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization. CIP-004-5 M6.5 Acceptable forms of evidence include, but are not limited to, documentation of the review including • a listing of all accounts/account groups or roles within the system • a summary description of privileges associated with each group or role • accounts assigned to the group or role and (iv) evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account. CIP-004-5 M6.6 Acceptable forms of evidence include, but are not limited to documentation of the review including: • a listing of authorizations for BES Cyber System information • any privileges associated with the authorizations • evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions. CIP-004-5 Tables in R6 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In addition, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-004-5 M6 states “must,” but the measures in Table R6 state “may.” M6 should be revised to say “may.”

No

CIP-004-5 R7: Generally speaking, please provide greater information and justification on the newly proposed “at the time of” and “by the end of the next calendar day” timing requirements. Also note that workflow should be deleted from the evidence options as the term is not widely or consistently understood. CIP-004-5 R7.2 The “end of next calendar day” is problematic. The time frame should be at least 7 days and preferably 30 days. CIP-004 R7.1: Under current CIP-004 R4.2, the Responsible Entity is required to revoke authorized cyber or authorized unescorted physical access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for all other personnel who no longer require such access. As it currently exists, this requirement has proven to be a compliance challenge for many in the industry, and has required significant time and resources to implement automated and procedural controls in order to meet the proscribed 24-hour and 7 calendar day thresholds. Nonetheless, proposed CIP-004 R7 further constricts the time period in which revocations must take place. For terminations and resignations, the act of revocation has been unreasonably accelerated from 24-hours and 7-days (respectively) to “at the time” of the termination or resignation. Not only is this a drastic change, but “at the time” is an incredibly vague measure to be held to and to audit as well. Accordingly, Constellation supports keeping the existing, concrete 24-hour and 7 calendar day requirements for CCA access revocation. With regard to the proposed “at the time” requirements, Constellation requests the following additional clarifications: • The justification behind changing the existing revocation time requirements. • Definition of and/or expectations around what “at the time” means. • What is meant by “workflow” as a form of evidence? • Is evidence of “at the time” revocation expected to be time stamped? If so, how is one to show a time stamp when a badge is revoked at the time of termination or resignation? CIP-004 R7.2: With regard to reassignments and transfers, clarification is also needed as to what revocation “by the end of the next calendar day” means. Under the current standard, reassignments and transfers fall under the 7 calendar day revocation requirement. As stated above, further constricting the time in which such revocations are required to take place and replacing a firm time requirement with a vague measure is contrary to what is in the industry’s best interest and what is clearly and objectively auditable. CIP-004 R7.3: The above comments similarly applies to proposed CIP-004 R7.3, which requires the individual access to BES Cyber System information by the end of the next calendar day for resignations and terminations. CIP-004-5 Table R7: The format of the evidence options should be bulleted to be consistent with other table formats and to make the items options for evidence, not a required package of evidence. Proposed Revisions: M7.1 Acceptable forms of evidence include, but are not limited to: • a sampling of terminations • workflow or sign-off form verifying access removal associated with the terminations and dated concurrent or prior to the date of the termination action • a system-generated listing of user accounts or other demonstration showing such persons no longer have access. CIP-004-5 M7.2 Acceptable forms of evidence include, but are not limited to: ♣ a sampling of individuals transferred or reassigned ♣ workflow or sign-off form showing the review of logical and physical authorizations dated on the same calendar day as the transfer or reassignment ♣ a system-generated listing of user accounts or other demonstration showing such persons no longer have access where the review determined it was no longer needed. CIP-004-5 Tables in R7 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In addition, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-004-5 M7 states “must,” but the measures in Table R7 state “may.” M7 should be revised to say “may.”

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

CIP-005-5 R1: While the rationale of CIP-005 is to focus on Electronic Access Points rather than the logical perimeter, the current approach in R1 makes it a requirement that physical and electronic monitoring systems be within an ESP because there must be defined access points. Requirement 1.3, in particular, may present an issue since explicit traffic access is to be specified along with why access

is needed. Some software makes this requirement difficult to define. CIP-005-5 R1.1: Please offer justification for the requirement to restrict unauthorized electronic access to Low Impact BES Cyber Systems when the CIP-004 program does not require declaring Low Impact BES Cyber Systems. Low Impact systems by virtue of their classification present a low impact risk; however the requirement poses a significant compliance burden. Additional consideration is needed to include this requirement and if retained, guidance needed on how to comply. Further, the applicability of CIP-005-5 R1.1 is Low Impact BES Cyber Systems with External Routable Connectivity. The definition of External Routable Connectivity is "The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol". While Constellation proposed a revision to the definition, additional insight from the drafting team will be helpful in assessing the language. Is your intent for Low Impact BES Cyber Systems to reside in an ESP? If so, does this imply implementation of additional controls or is it merely asking for documentation of how the Low Impact System is protected from access from a public network, i.e. existing controls to protect the corporate data network? In CIP-005-5 R1.2, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-005-5 M1 states "must," but the measures in Table R1 state "may." M1 should be revised to say "may." Measures in Table R1: Network diagrams, architecture diagrams, lists of access control rules and other documents are high risk security documents. Perhaps the standard language should include commitments to proper handling by NERC, Regions, auditors and any other potential external reviewers to ensure protection.

No

CIP-005-5 M2 states "must," but the measures in Table R2 state "may." M2 should be revised to say "may." CIP-005-5 Measures in Table R2: Network diagrams, architecture diagrams, and other documents are high risk security documents. Perhaps the standard language should include commitments to proper handling by NERC, Regions, auditors and any other potential external reviewers to ensure protection.

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

CIP-006-5 R1.3: Greater consideration is needed when imposing the requirement to "utilize two or more different and complementary physical access controls …" in order to balance security with practical operations. CIP-006-5 R1.3 stands to impose significant cost without clear commensurate improvements to security. This requirement needs further vetting and a more full justification of net gains associated with such measures. CIP-006-5 M1.2 and 1.3: The Table R1 Measures for 1.2 and 1.3 include evidence on egress, while the requirements say "access." The requirements should be clear and the measures should be consistent. The requirement language should perhaps state ingress and egress if that is the expectation of the requirement. CIP-006-5 R1.4 and 1.5 – These requirements state: "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access …" Please confirm that the entity is to define the "individual responsible for response" or clarify an alternate intent. If entity determined, it should be emphasized to auditors that this is an entity determination and should be judged in the context of the entity program. Further discussion in the Application Guidelines may also be helpful. CIP-006-5 R1.6 should be revised to as follows: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual visitor and the date of their entry. CIP-006-5 Table R1, 1.1 Applicability: It's unclear to what the "associated" systems are intended to align. Should the order of listing be reversed to read: Low Impact BES Cyber Systems - Associated Physical Access Control Systems Please reorder within CIP-006-5 Table R1 as follows: CIP-006-5 Table R1, 1.2: Medium Impact BES Cyber Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-006-5 Table R1, 1.3: High Impact BES Cyber Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-006-5 Table R1, 1.4: High Impact BES Cyber Systems -

Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-006-5 Table R1, 1.5 Applicability: It's unclear to what the "associated" systems are intended to align. CIP-006-5, M1 states "must," but the measures in CIP-006-5 Table R1 state "may." M1 should be revised to say "may."
No
CIP-006-5 R2: As written, this requirement limits entities to only having one visitor control program. The latitude to have more than one visitor control program is important to accommodate varying location configurations and potential technical limitations. Proposed Revision: "Each Responsible Entity shall implement one or more documented visitor control programs..." CIP-006-5 R2: The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Defined Physical Boundary to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit. It is also felt a Point of Contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort but there is no need to document everyone that acted as an escort for the visitor. The sentence, "It is also felt a Point of Contact should be documented who can provide additional details about the visit if questions arise in the future" is problematic. This sentence is ambiguous. Use of the words "should" and "if" may be interpreted several ways, potentially requiring management and documentation showing that each escort can speak to the details of every visit that occurs. Further clarification is needed to focus on a reasonable intent and to reduce uncertainty within the audit setting. The CIP-006-5 R2 Tables apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In addition, the order of the "associated" systems is confusing. Please reorder CIP-006-5 Table R2 for R2.1 and R2.2 as follows: High Impact BES Cyber Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-006-5 M2 states "must," but the measures in Table R2 state "may." M2 should be revised to say "may."
No
CIP-006-5 R3.1: Further clarification is needed on the intent/understanding behind the "prior to commissioning" for systems already in place. Prior to commissioning should be pointed at new Physical Access Control Systems commissioned after FERC approval of the CIP Version 5 standards. Proposed Revision: Prior to commissioning a new Physical Access Control System1, and at least once every 24 months after commissioning of a new Physical Access Control System, maintenance …" (Footnote 1 = A new Physical Access Control System is one that is commissioned by the Entity on a date following Version 5 CIP Cyber Security Standards approval by the applicable regulatory authority) CIP-006-5 R3.2 – Provide more insight on expectations around providing log records when the logging fails. CIP-006-5 Table R3, 3.1 and 3.2 Applicability: It's unclear to what the "associated" systems are intended to align. CIP-006-5 M3 states "must," but the measures in Table R3 state "may." M3 should be revised to say "may."
No
In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.
No
In CIP-007-5 R1.1, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 M1 states "must," but the measures in Table R1 state "may." M1 should be revised to say "may."
No
CIP-007-5 R2.2: For clarity, R2.2 should replace "of" with "after" to read "…within 30 days after release." CIP-007-5 Tables in R2 apply to only High and Medium impact assets. If possible to clarify

this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-007-5 R2.1, R2.2 and R2.3, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 M2 states “must,” but the measures in Table R2 state “may.” M2 should be revised to say “may.”

No

CIP-007-5 Tables R3, M3.3: The format of the evidence options should be bulleted to be consistent with other table formats and to make the items options for evidence, not a required package of evidence. Proposed Revision: M3.3 Evidence may include, but is not limited to: • current signature or pattern updates • either screen shots showing the configuration of signature, or pattern updates for automated controls, or work logs showing the signature, or pattern updates for manual controls. CIP-007-5 Tables in R3 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-007-5 R3.1, R3.2, R3.3, R3.4 and R3.5: The order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 M3 states “must,” but the measures in Table R3 state “may.” M3 should be revised to say “may.”

No

CIP-007-5 R4 appears to go beyond a focused effort to account for events of concern to encompass logging of all events whether or not it is a Cyber Security Incident. Further R4.5 creates a new obligation to the CIP standards (and added paperwork burden) to summarize logged events (not incidents) to identify "unanticipated BES Cyber Security Incidents". The potentially onerous and administrative nature of this requirement could overwhelm the desired benefit of on-going assessment and improvement to practices. Please reassess whether the requirements and the compliance tasks achieve the desired goals and are commensurate with improvements to reliability and security. CIP-007-5 M4.1 identifies "event classes" which is not part of the requirement and may not be clearly understood in practice. Please clarify the intent of the term “event classes.” CIP-007-5 R4.3: It is unclear how R4.3 will be enforced. It may be difficult to detect logging failures of a specific event. If gross logging stops then you may be able to see it due to lack of events. CIP-007-5 Tables R4, M4.3: The format of the evidence options should be bulleted to be consistent with other table formats and to make the items options for evidence, not a required package of evidence. Proposed Revision: CIP-007-5 M4.3 Evidence may include, but is not limited to: • dated event logging failures and screen-shots showing how real-time alerts were configured • dated records showing that personnel were dispatched or a work ticket was opened to review and repair logging failures. CIP-007-5, Table R4: The order of the “associated” systems is confusing. Please reorder as follows: R4.1 - High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 R4.2 and R4.3 High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems with External Routable Connectivity - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 R4.4- High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems at control centers - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 R4.5- High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 M4 states “must,” but the measures in Table R4 state “may.” M4 should be revised to say “may.” As a minor note, in CIP-007-5 R4.1, “includes” should be singular. In rationale for CIP-007-5 R4 - remove 'of' after comprises.

No
CIP-007-5 R5.1 – may be clearer to replace “validate” with “authenticate” to match the measures. CIP-007-5 R5.2 is not practical. IT departments use administrative, shared, and other passwords in day to day operations. Requiring the Senior Manager or even a delegate to be involved in an approval process at that level could present operational barriers. This requirement should be removed. In CIP-007-5 R5.1, R5.2, R5.3, R5.5 and R5.6, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 M5 states “must,” but the measures in Table R5 state “may.” M5 should be revised to say “may.”
No
In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.
No
CIP-008-5 R1: Proposed revision to clarify: “Each Responsible Entity shall document one or more BES Cyber Security Incident response plan(s)…” CIP-008-5 M1.2 appropriately states that the entity shall document the guidelines or thresholds for determining if a BES Cyber Security Incident is also a Reportable BES Cyber Security Incident. It should be emphasized to auditors that this is an entity determination and should be judged in the context of the entity program. Further discussion in the Application Guidelines may also be helpful. CIP-008-5 R1.3: Proposed revision to clarify: 1.3 Requirement “Define, within the Incident Response Plan: …” CIP-008-5 M1 states “must,” but the measures in Table R1 state “may.” M1 should be revised to say “may.”
No
CIP-008-5 R2.1: The working of R2.1 is awkward. Proposed Revision: When a BES Cyber Security Incident occurs, follow the Incident Response Plan(s) and record any deviations from the plan. CIP-008-5 R2.2: Further clarification is needed on the intent of implementing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that a test-type implementation is required on the day the standard becomes effective. The implications of such an imposition are significant since Day 1 is the same day for all entities. The requirement includes two activities – implementing on the effective date and testing the plan(s) each calendar year. The two requirements should be delineated and potentially put in two separate requirements. Proposed Revision: CIP-008-5 Rx: Implement the BES Cyber Security Incident response plan(s) so that they are in place upon the effective date of the standard. CIP-008-5 Mx: Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) on or before the effective date of the standard. CIP-008-5 Rx: Test the BES Cyber Security Incident response plan(s) at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise. CIP-008-5 Mx: Evidence may include, but is not limited to, dated evidence of testing of the BES Cyber Security Incident response plan(s) at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise. CIP-008-5 M2 states “must,” but the measures in Table R2 state “may.” M2 should be revised to say “may.”
No
CIP-008-5 R3: Additional information is needed regarding the timeframes. While the discussion finds the time frames to be “feasible” if the entity program is clearly defined, it does depend on the incident envisioned. For instance, incidents concerning a protection system could meet the timeframe; however, an intrusion into an Energy Management System could be more involved and struggle to meet the timeframe. Please offer more insight. CIP-008-5 R3.1: Further clarification is needed on the intent of reviewing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that evidence of a review is required on the day the standard becomes effective. This poses a paperwork obligation of questionable value. The requirement should accept that the development of the plan that was implemented per R2 fulfilled the review for accuracy and completeness and remove the obligation to show evidence for an initial review. Proposed Revision:

CIP-008-5 R3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness each calendar year following the effective date of the standard, not to exceed 15 calendar months between reviews, and update if necessary. CIP-008-5 M3.1: Evidence may include, but is not limited to, dated documentation of a review of each BES Cyber Security Incident response plan(s) at least once every each calendar year, not to exceed 15 calendar months, and an updated BES Cyber Security Incident response plan if necessary. CIP-008-5 M3 states "must," but the measures in Table R3 state "may." M3 should be revised to say "may." In reviewing CIP-008-5 in totality, Constellation is concerned that the requirements standards within CIP-008 and with EOP-004 may conflict or duplicate compliance obligations for cyber incidents. Constellation recognizes that both the EOP-004 and the CSO 706 drafting teams attempted to coordinate their efforts in order to streamline event reporting as a whole; however, the fact remains that there will be two standards governing reporting of cyber incidents. A possible solution would be to remove the cyber reporting requirements in EOP-004-2 and place them in CIP-008-5, thus requiring entities to have distinct incident reporting and response plans for cyber events and non cyber events.

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

R1: Proposed revision to clarify: "Each Responsible Entity shall document one or more recovery plans…" CIP009 R1.4 – It is unclear from the Requirement if the intent is to require initial verification of the backup and restore processes when significant changes are made to the BES Cyber System (FERC Order 739) as the associated M1.4 seems to address FERC Order 748 to ensure verification that backups are successful and backup failures are addressed. R1.4 and M1.4 need clarification as to whether the requirement is for initial verification of backup processes upon significant system change or ongoing verification that backup operations completed successfully, or both. In addition, it's not clear how R1.4 and R2.2 differ. Clarification as to how the R1.4 requirement differs from R2.2 with regard to testing of information stored on backup media initially. CIP009 R1.5: Please clarify how "technically feasible" is defined in R1.5 and what actions are required if data is unable to be salvaged. For some devices, pulling a disk out to salvage it and replace would be acceptable. Other devices, such as network switches, do not have removal parts and when failed switch replacement is required. Anticipation of a TFE process is unsettling given the burdensome nature of the TFE process currently in place. Further consideration is needed to successful fulfill the security intent of these measures without undue burden. CIP-009-5 Tables in R1 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-009-5 R1.1, R1.2, R1.3 and R1.5: The order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems Please reorder CIP-009-5 R1.4: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems Medium Impact BES Cyber Systems at control centers - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems CIP-009-5 Table R1, 1.4 and 1.5 – The column headings are incorrect. All columns are titled "Part." CIP-009-5 M1 states "must," but the measures in Table R1 state "may." M1 should be revised to say "may."

No

CIP009 R2.3: Please clarify what "representative environment" means. Our plans and tests are conducted in similar systems. This requirement depending on interpretation suggests that duplicate physical access control, monitoring systems and Energy Control System environment to allow to fully exercise recovery. Further, what does full operational exercise mean? Do you have to assume a complete loss of the environment scenario? A redundant environment allows more flexibility for recovery plans. CIP-009-5 R2.1, R2.2 and R2.3: Further clarification is needed on the intent of implementing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that a test-type implementation is required on the day the standard becomes effective. The implications of such an imposition are significant since Day 1 is the same day for all

entities. The requirement includes two activities – implementing on the effective date and testing the plan(s) each calendar year. The two requirements should be delineated and potentially put in two separate requirements. Proposed Revision for CIP-009-5 R2.1: CIP-009-5 R: Implement the recovery plan(s) referenced in R1 so that they are in place upon the effective date of the standard. CIP-009-5 M: Evidence may include, but is not limited to, dated evidence of implementing the BES recovery plan(s) on or before the effective date of the standard. CIP-009-5 R: Test the recovery plan(s) at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise. CIP-009-5 M: Evidence may include, but is not limited to, dated evidence of testing of the recovery plan(s) at least once every calendar year thereafter, not to exceed 15 months, by recovery from an actual incident, or with a paper drill or table top exercise, or with a full operational exercise. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. Clarify in the same way for CIP-009-5 R2.2 and R2.3 CIP-009-5 Tables in R2 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-009-5 R2.1, R2.2, and R2.3: The order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems Medium Impact BES Cyber Systems at control centers - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems In addition, the requirements in the Tables should be stated as nouns rather than action items to follow the direction of CIP-009-5 R2. CIP-009-5 M2 states “must,” but the measures in Table R2 state “may.” M2 should be revised to say “may.”
No
CIP009-5, R3: While deadlines for reviews and updates are useful, they should not trump operational priorities, workforce burden, cost implications and the reality of the review task. Thirty days in R3.2 is aggressive. With the complexity of these systems and the amount of documentation, the review process by all parties can take longer than 30 days and in some cases should in order to glean the relevant benefit from the review. Constellation proposes to increase the timing in CIP-009-5 R3.2 to 60 days. This change would also align with the time periods specified in CIP-008-5 R3.2 and 3.3 for the Incident Response drill and subsequent updates to the procedure. CIP-009-5 R3.1: Further clarification is needed on the intent of reviewing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that evidence of a review is required on the day the standard becomes effective. This poses a paperwork obligation of questionable value. The requirement should accept that the development of the plan that was implemented per CIP-009-5 R2 fulfilled the review for accuracy and completeness and remove the obligation to show evidence for an initial review. Proposed Revision: CIP-009-5 R3.1: Review the recovery plan for accuracy and completeness each calendar year following the effective date of the standard, not to exceed 15 calendar months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned. CIP-009-5 M3.1: Evidence may include, but is not limited to, dated documentation of a review of the recovery plan(s) each calendar year, not to exceed 15 calendar months, or when BES Cyber Systems are replaced, including documentation of any identified deficiencies. CIP-009-5Tables in R2 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-009-5 R3.1, R3.2, R3.3, R3.4 and R3.5: The order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems Medium Impact BES Cyber Systems at control centers - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems CIP-009-5 Table R3, 3.4 and 3.5 – The column headings are incorrect. All columns are titled “Part.” Typo in CIP-009-5 M3.2: "of the" is stated twice in a row.
No
In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.
No

CIP010 R1.4 and R1.5 – The requirements in R1.4 and R1.5 for verification that cyber security controls are not adversely affected appear to be redundant. Please clarify the differences between the requirement in R1.4.2 ("…verify these required controls and the BES Cyber System availability are not adversely affected") and the requirement in R1.5.2 ("…ensure that required cyber security controls are not adversely affected…"). CIP010 R1 - As currently written, this requirement will most likely require manual tracking of changes to the system rather than encouraging use of automated systems to discover configuration and detect unauthorized changes. Additional refinement to the language is needed to accommodate and encourage progress in change management mechanisms. Tables in CIP-010-1 R1 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-010-1 R1.1, R1.2, R1.3 and R1.4, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-010-1 M1 states "must," but the measures in Table R1 state "may." M1 should be revised to say "may."
No
CIP-010-1 R3.1 and R3.2: Further clarification is needed on the intent of implementing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that an assessment implementation is required on the day the standard becomes effective. The implications of such an imposition are significant since Day 1 is the same day for all entities. The requirement includes two activities – implementing on the effective date and assessing the plan(s) each calendar year. The two requirements should be delineated and potentially put in two separate requirements. CIP-010-1 Tables in R2 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-010-1 R2.1, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-010-1 M2 states "must," but the measures in Table R2 state "may." M2 should be revised to say "may."
No
CIP-010-1 Tables in R3 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-010-1 R3.1 and R3.4, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-010-1 M3 states "must," but the measures in Table R3 state "may." M3 should be revised to say "may."
No
In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.
No
CIP-011-1 R1.3: Further clarification is needed on the intent of implementing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that an assessment implementation is required on the day the standard becomes effective. The implications of such an imposition are significant since Day 1 is the same day for all entities. The requirement includes two activities – implementing on the effective date and assessing the plan(s) each calendar year. The two requirements should be delineated and potentially put in two separate requirements. CIP-010-1 Tables in R1 apply to only High and Medium impact assets. If possible to clarify this aspect in the

requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-010-1 R1.1, R1.2 and R1.3, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-011-1 M1 states "must," but the measures in Table R1 state "may." M1 should be revised to say "may." CIP-011-1 Table R1, 1.2 and 1.3 – The column headings are incorrect. All columns are titled "Part."

No

CIP-010-1 Tables in R2 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-010-1 R2.1 and R2.2, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-011-1 M2 states "must," but the measures in Table R2 state "may." M2 should be revised to say "may."

No

Comments: In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

The implementation plan is confusing and does not address certain situations. Constellation proposes revisions to simplify some aspect, address voids and remove references to language in other standards: Proposed Effective Date for Version 5 CIP Cyber Security Standards Responsible Entities shall comply with requirements in CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1, and the Definitions of Terms Used in Version 5 CIP Cyber Security Standards as follows: 1. 18 Months Minimum – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.2 2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities. 3. Newly Registered Entities3 – Version 5 CIP Cyber Security Standards shall become effective 18 months from the Entity's registration date. (Footnotes: 2= In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4. 3= A newly Registered Entity is one that has registered with NERC on the date that Version 5 CIP Cyber Security Standards receive applicable regulatory approval or thereafter) Changes Resulting in a Higher Categorization and Newly Commissioned Assets Scenario Compliance Implementation New High Impact BES Cyber System Upon Commissioning New Medium Impact BES Cyber System Upon Commissioning Newly categorized High Impact BES Cyber System from Medium Impact BES Cyber System 12 months for new requirements Newly categorized Medium Impact BES Cyber System from Low Impact BES Cyber System 12 months for new requirements Responsible Entity Identifies first Medium or High Impact BES Cyber System Add 12 months from time above Additional Guidance and Implementation Time Periods for Disaster Recovery A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003-5 R2. The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full

implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed. However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Additional Comments Submitted:

Organization	Yes or No	Additional Comments Received
Midwest Reliability Organization	Affirmative	The standards drafting team has achieved great strides in fulfilling the industries obligation to FERC Order 706. CIP Reliability Standards V5 adequately address the security control of access points to the control systems used to secure the reliable operation of the electric grid.
NorthWestern Energy	Negative	NorthWestern Energy supports the proposed Issue/Solution below: Issue: As currently drafted Version 5 of the CIP standards: o Would significantly increase cost without a commensurate increase in the reliability, safety, or security of the BES. o Create significant complexity, confusion, and administrative burden regarding the identification of Critical Cyber Assets, the definition of terms, and implementation of Cyber Controls. o Exceeds FERC's 706 order without justification or improving the security of the BES. o Many of the draft requirements add significant bureaucracy without adding security. The industry needs focus on improving security of the BES and not the security of individual assets or the appearance of security through the addition of administrative requirements. Proposed Solution: 1. Retain CIP-002-4 as approved by the industry in 2010. It is filed with FERC; industry and NERC comments on the FERC NOPR recommended FERC approval. This will: o Eliminate the confusing and complicated process developed to identify BES Cyber Systems proposed in Version 5 o Meet FERC's 706 for CIP-002-1: o Industry approved guidance documents for identifying Critical Assets and for identifying Critical Cyber Assets. Â¶253-258, 270-27 o CIP-002-4 replaces the Critical Asset guidance and aligns with FERC's affirmation that the applicable responsible entities are responsible for identifying Critical Assets. Â¶319-321 o CIP-002-2 added senior manager approval of risk-based methodology. Â¶294-297 o Not exceed FERC Order 706: o Â¶284: "... there is no formally accepted method for identifying critical cyber assets before us at this time ... we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time." o Â¶285: "CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial up access ... We do not find sufficient justification to remove this provision at this time." 2. Develop a new standard for High Impact Assets: o That identifies which assets in CIP-002-4 are High Impact and o Clearly states the extra protection required for High Impact Assets: o The Draft version 5 identifies eight extra protections, most are in response to FERC Order 706. o

Organization	Yes or No	Additional Comments Received
		Provides opportunity for a separate implementation timeline for the additional controls that apply only to High Impact assets. o Provides flexibility in adjusting controls on High Impact assets. In the future only one standard has to be modified. o Entities that do not have High Impact assets will not have to sort through all the standards and RSAWs to assure compliance and security. 3. Develop a separate standard for the Low Impact assets or abandon this concept. o Lows were not directed by FERC Order 706 nor included in the SAR. o A separate standard provides full transparency in the stakeholder process. o This is a scope expansion not supported by many in the industry. o Cost and compliance concerns with lows include whether lows have to be listed. This is a derivative of which controls are selected and how they are designed and audited. 4. Revise CIP-003-5 through CIP-011-5 and Definitions to reflect changes described suggested above and meet FERC Directives in order 706.
Volkmann Consulting, Inc.	Negative	The industry has already approved Version 4 and has gauged its impact and has started to prepare for implementation. Version 4 meets the FERC 706 order and should be given an opportunity to be implemented and evaluated before rushing to implement a comprehensive change to the industry. Version 5 standards go beyond FERC Order 706. The focus of the change to Version 5 should be to meeting the rest of the 706 order, not expanding it. More definition is need around 15 minute failure period and impact. Many small entities' performance of a particular BES Reliability Operating Services has little or no impact to the operation of the BES. Yet failure of a BES Cyber asset may impact their ability to perform the BES Reliability Operating Services and hence subject to the CIP standards. Low Impact category is discriminatory towards smaller entities because it will capture facilities that when similarly situated in a larger entity would not be included in the low category because it does not impede the larger entity's ability to performance the service. The Low category was not prescribed by the FERC 706 Order. For that reason and the above discussion, Low Impact should be eliminated in this round of standard drafting and be part of a larger FERC NOPR process. Much of the fear and possible negative votes is the uncertainty of meeting a very complicated set of standard. The SDT should consider recommending to FERC that enforcement of the standard coincide with completing and mitigating an initial Compliance Audit.
Lakeland Electric	Negative	Transmission Owners do not have Control Centers (TOPs-have Control Centers).
Muscatine Power & Water	Negative	Understanding that CIP version 4 has been approved by the NERC BOT and awaiting approval from FERC, MPW recommends that CIP-002-5 be placed on hold at this time. Our industry has approved CIP-002 Version 4 and the terms "Critical Assets" and "Critical Cyber Assets" are well known terms within our current Cyber Security plans. This proposal meets the main FERC goal of including more Critical Assets without requiring a reduction in reliability by forcing entities to retool their existing programs from scratch. As currently drafted, Version 5

Organization	Yes or No	Additional Comments Received
		of the CIP standards: Â· Would significantly increase cost without a commensurate increase in the reliability, safety, or security of the BES Â· Create significant complexity, confusion, and administrative burden regarding the identification of Critical Cyber Assets, the definition of terms, and implementation of Cyber Controls Â· Does not consider that smaller Entities have a much lower impact on the BES Â· Greatly exceeds FERC's 706 order without justification Concerning CIP-002-5 Attachment 1, MPW can easily see that there is some stratification afforded to TOP and GOP Control Centers, based on voltage levels, total MW, total MVAR, number of Transmission lines, Blackstart Resources, etc, for being considered High Impact, Medium Impact, or Low Impact. While the SDT has acknowledged there are some distinct differences between larger and smaller TOP's and GOP's, MPW wants to point out that not all Balancing Authorities are created equally. Does anyone think that the smallest BA in North America, serving 38 MW of load, has the same Reliability Impact as a BA serving 10,000 MW, or more, of load? Does it really improve the reliability of the BES to have ALL those smaller BA Control Centers carry the same High Impact Rating? In addition, MPW agrees with all the comments submitted by the MRO NSRF.
Salmon River Electric Cooperative, Alameda Municipal Power, City of Lodi, California	Negative	We believe the drafting teams work is very valuable and provides a good basis for appropriately allocating responsibilities according to the impact to the BES. However we feel additional work is needed due to a discrepancy between the definition of BES Cyber Assets and the applicability to entities with UFLS or UVLS equipment. Definition of BES Cyber Asset: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. Applicability: Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: o A UFLS program required by a NERC or regional Reliability Standard o A UVLS program required by a NERC or regional Reliability Standard o A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard o A Transmission Protection System required by a NERC or regional Reliability Standard o Its Transmission Operator's restoration plan Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: o A UFLS program required by a NERC or regional Reliability Standard o A UVLS program required by a NERC or regional Reliability Standard The discrepancy exist because (1) The definition states "The timeframe is not in respect to any cyber security events or incidents,

Organization	Yes or No	Additional Comments Received
		but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES." (2) LSE's and DP's with UFLS equipment are required to comply with the proposed CIP Standards over BES Cyber Assets when these devices are not consider BES Cyber Asset per definition. (3) These devices sense a system condition and do not send or receive instructions. In fact in some regions a UFLS device is not required to be a cyber-equipment type. For example, in the NPCC region an electro-mechanical relay can be used to fulfill an organizations UFLS program requirement. Proposed recommendation: Modify the applicability. "Load Serving Entities and Distribution Providers with a load shedding program that is activated through receipt of an instruction to its cyber processor to operate."
Liberty Electric Power LLC	Negative	In addition to the survey comments, the inclusion of the following sentence in the compliance measures section needs to be removed to make the standard acceptable: For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit. There is no BES reliability benefit for six years of documentation on many of these requirements. In those cases where there is such a benefit, the standard should be written with a six-year retention requirement.
Liberty Electric Power LLC	Negative	In addition to the survey comments, the inclusion of the following sentence in the compliance measures section needs to be removed to make the standard acceptable: For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit. There is no BES reliability benefit for six years of documentation on many of these requirements. In those cases where there is such a benefit, the standard should be written with a six-year retention requirement.
NorthWestern Energy	Negative	NorthWestern Energy supports the proposed Issue/Solution below: Issue: As currently drafted Version 5 of the CIP standards: o Would significantly increase cost without a commensurate increase in the reliability, safety, or security of the BES. o Create significant complexity, confusion, and administrative burden regarding the identification of Critical Cyber Assets, the definition of terms, and implementation of Cyber Controls. o Exceeds FERC's 706 order without justification or improving the security of the BES. o Many of the draft requirements add significant bureaucracy without adding security. The industry needs focus on improving security of the BES and not the security of individual assets or the appearance of security through the addition of administrative requirements. Proposed Solution: 1. Retain CIP-002-4 as approved by the industry in 2010. It is filed with FERC; industry and NERC comments on the FERC NOPR recommended FERC approval. This will: o

Organization	Yes or No	Additional Comments Received
		Eliminate the confusing and complicated process developed to identify BES Cyber Systems proposed in Version 5 o Meet FERC's 706 for CIP-002-1: o Industry approved guidance documents for identifying Critical Assets and for identifying Critical Cyber Assets. Â¶253-258, 270-27 o CIP-002-4 replaces the Critical Asset guidance and aligns with FERC's affirmation that the applicable responsible entities are responsible for identifying Critical Assets. Â¶319-321 o CIP-002-2 added senior manager approval of risk-based methodology. Â¶294-297 o Not exceed FERC Order 706: o Â¶284: "... there is no formally accepted method for identifying critical cyber assets before us at this time ... we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time." o Â¶285: "CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial up access ... We do not find sufficient justification to remove this provision at this time." 2. Develop a new standard for High Impact Assets: o That identifies which assets in CIP-002-4 are High Impact and o Clearly states the extra protection required for High Impact Assets: o The Draft version 5 identifies eight extra protections, most are in response to FERC Order 706. o Provides opportunity for a separate implementation timeline for the additional controls that apply only to High Impact assets. o Provides flexibility in adjusting controls on High Impact assets. In the future only one standard has to be modified. o Entities that do not have High Impact assets will not have to sort through all the standards and RSAWs to assure compliance and security. 3. Develop a separate standard for the Low Impact assets or abandon this concept. o Lows were not directed by FERC Order 706 nor included in the SAR. o A separate standard provides full transparency in the stakeholder process. o This is a scope expansion not supported by many in the industry. o Cost and compliance concerns with lows include whether lows have to be listed. This is a derivative of which controls are selected and how they are designed and audited. 4. Revise CIP-003-5 through CIP-011-5 and Definitions to reflect changes described suggested above and meet FERC Directives in order 706.
Manitoba Hydro	Negative	Please see comments submitted in electronic commenting form. In addition, Manitoba Hydro has the following general comments on CIP Version 5: -The Application Guidelines section provides no indication of how binding this section is. In fact, including it within the standard carries the impression that the Guidelines are more binding than before. In order to clarify that the Guidelines have not become more mandatory than today, this section should reinstate a Preamble with the following words: "Guidelines provide suggested guidance on a particular topic for use by BPS users, owners, and operators according to each entity's facts and circumstances and do not provide binding norms, establish mandatory reliability standards, or create parameters by which compliance to standards is monitored or enforced." -"Initially upon the effective date "in all Standards means beginning on the effective date. As written, action required "initially upon effective date" must be performed ON the effective date. This may be an unintended consequence of the wording. Was the intent "on or before" the effective date? If "on or before the effective date" is not the intent, then the statement "initially upon the effective date" is unnecessary since all requirements

Organization	Yes or No	Additional Comments Received
		for all standards must be implemented upon the effective date. -"All Responsible Entities" used in the Applicability column of the requirement table is confusing. Are these the entities identified by Functional Entities in Section 4 Applicability, or are the "All Responsible Entities" defined by the bullets in Section 5 Background Applicability? To maintain consistency and clarity with all the other requirements, we suggest replacing "All Responsible Entities" with the specific Cyber Assets in scope, for example, BES Cyber Assets. -Measures in the Requirement Table are supposed to indicate the body of evidence for the requirements, but as currently written, “may include” allows that the evidence may not include any of the items in the list. If there are some characteristics or criteria which are expected as part of the body of evidence, such as descriptions, signatures or dates, which are independent of the evidence types, such as paper records, electronic files or computerized systems, then these characteristics or criteria should be indicated in the measures as “Evidence shall include, ...”, instead of “Evidence may include, ...”. If the body of evidence is expected to include the listed items, we suggest changing the word “may” to be “shall”. -Introduction - Applicability Section: The phrase “designed, installed and operated for the protection or restoration of the BES” is used in Sections 4.1.2, 4.1.6, 4.2.1 and 4.2.2. Is this phrase necessary? Are some of the facilities not designed, installed and operated for such purposes? If the phrase is retained, is it clear which facilities are applicable? In 4.1.2, 4.2.2 a restoration plan is referenced, but is a restoration plan a “system or program”. Also, can a facility be “part of” a restoration plan? -4.1.2: We suggest adding clarity by changing "Its Transmission Operator's" to "The Distribution Provider's Transmission Operator's". -4.2.2: We suggest adding clarity by changing "Its Transmission Operator's" to "The Distribution Provider's Transmission Operator's". -Background: the meaning of three terms is explained, but it is not clear why these are not simply added to the list of defined terms. Are these meanings binding on NERC? Also, the distinction between “processes”, “plans” and “programs” is unclear. If programs and plans are types of documented processes, this should be stated. Background - Applicability Section: -High Impact BES Cyber Systems (for CIP-003-5 through CIP-011-1): We suggest changing "... each BES Cyber Systems ..." to "... each BES Cyber System ..." We suggest moving the sentence "Responsible Entities can implement ... across multiple BES Cyber Systems." to the Applicability section, just before the sub-bullets. This sentence is more general guidance, since it applies to not only High Impact BES Cyber Systems, but also Medium Impact BES Cyber Systems. This also adds consistency to the wording of the local definitions in Standards CIP 003 5 through CIP-011-1. -Medium Impact BES Cyber Systems: We suggest changing "Systems" to "System". -Medium Impact BES Cyber Systems with External Routable Connectivity: The meaning of "... directly accessed through External Routable Connectivity" is unclear. If this is an exclusion, does it only apply to Medium Impact BES Cyber Systems with External Routable Connectivity? -Low Impact BES Cyber Systems with External Routable Connectivity: We suggest changing "... each Low Impact BES Cyber Systems ..." to "... each Low Impact BES Cyber System ...". For clarity, we suggest changing” ... High or Medium" to” ... High Impact or Medium Impact". -Associated Electronic Access

Organization	Yes or No	Additional Comments Received
		Control or Monitoring Systems: We suggest changing "... BES Cyber Systems." to " ... BES Cyber System." -Associated Physical Access Control Systems: We suggest changing "... BES Cyber Systems." to “... BES Cyber System." -Associated Protected Cyber Assets: We suggest changing "... BES Cyber Systems." to “... BES Cyber System." -Electronic Access Points: This local definition is different than the proposed NERC Glossary of Terms definition. If the intent is to address associated Electronic Access Points, then to provide clarity and consistency with the other local definitions, we suggest changing this local definition title to "Associated Electronic Access Points". If “associated” was not intended, then this definition should not differ from the proposed NERC Glossary of Terms definition. -Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries: This local definition is only referenced in CIP-006-5 and should not be included as a local definition in any standards where it is not used. Only local definitions which are used in a specific standard should be included as a local definition of that specific standard. Compliance -1.1 - Compliance Enforcement Authority: should read “Compliance Enforcement Authority shall be the Regional Entity, or’ and then go on to list the 3 other options in the bullets. The second bullet - the words ‘to be responsible for compliance enforcement’ could be replaced with ‘to serve as the Compliance Enforcement Authority’. -1.2 - Evidence Retention: It is not clear how a Responsible Entity can retain data “for the duration of a regional or CEA investigation”. The term “investigation” can include a compliance audit, a spot check or compliance investigation. The latter 2 monitoring tools can be initiated at any time by the CEA. -Requirement Section: all requirements should refer to applicable “requirements” in a table, rather than “items” in a table.
Baltimore Gas & Electric Company	Negative	Baltimore Gas and Electric Company would like to thank the Standard Drafting Team for their tremendous effort in developing the CIP standards. This is a complex and challenging endeavor. While BGE is voting negative at this time, BGE remains optimistic that the ongoing stakeholder process can refine the language into an approvable set of standards. The items of concern behind the negative vote are spelled out in the comments submitted by Constellation Energy on our behalf. Extensive input is provided on the definitions. Because the definitions apply to the suite of CIP standards, they must be acceptable in order for the standards to be acceptable. Further input is provided on the specific standards in the comment form as well. Where possible, Baltimore Gas and Electric proposed revisions. It is critical that the standard language include clear and objective measures that minimize potential differences in perspective when judged for compliance. We support the pursuit of quality security measures that ensure BES reliability, but are sensitive to overly burdensome compliance obligations. Thanks again to the drafting team.
Liberty Electric Power	Negative	In addition to the survey comments, the inclusion of the following sentence in the compliance measures section needs to be removed to make the standard acceptable: For instances where the evidence retention period specified below is shorter than the time since

Organization	Yes or No	Additional Comments Received
LLC		the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit. There is no BES reliability benefit for six years of documentation on many of these requirements. In those cases where there is such a benefit, the standard should be written with a six-year retention requirement.
Power Energy Group LLC, Volkmann Consulting, Inc.	Negative	The industry has already approved Version 4 and has gauged its impact and has started to prepare for implementation. Version 4 meets the FERC 706 order and should be given an opportunity to be implemented and evaluated before rushing to implement a comprehensive change to the industry. Version 5 standards go beyond FERC Order 706. The focus of the change to Version 5 should be to meeting the rest of the 706 order, not expanding it. By mixing High, Medium and Low Impact requirements with the context of each standard creates a very complicated set of standards to administrate and to evaluate, especially in an audit environment. Reaching consensus and implementation of important High and Medium requirements may be impeded by failure to reach agreement on the Low Impact. It is recommended to segregate the requirements into High, Medium and Low standards, so that standard is only applicable to a particular level of Impact. More definition is need around 15 minute failure period and impact. Many small entities' performance of a particular BES Reliability Operating Services has little or no impact to the operation of the BES. Yet failure of a BES Cyber asset may impact their ability to perform the BES Reliability Operating Services and hence subject to the CIP standards. Low Impact category is discriminatory towards smaller entities because it will capture facilities that when similarly situated in a larger entity would not be included in the low category because it does not impede the larger entity's ability to performance the service. The Low category was not prescribed by the FERC 706 Order. For that reason and the above discussion, Low Impact should be eliminated in this round of standard drafting and be part of a larger FERC NOPR process. Much of the fear and possible negative votes is the uncertainty of meeting a very complicated set of standard. The SDT should consider recommending to FERC that enforcement of the standard coincide with completing and mitigating an initial Compliance Audit.
Liberty Electric Power LLC	Negative	In addition to the survey comments, the inclusion of the following sentence in the compliance measures section needs to be removed to make the standard acceptable: For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit. There is no BES reliability benefit for six years of documentation on many of these requirements. In those cases where there is such a benefit, the standard should be written with a six-year retention requirement.
Portland	Negative	PGE takes cyber security very seriously, especially as it relates to the critical infrastructure

Organization	Yes or No	Additional Comments Received
General Electric Co.		necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard is worded in a way that PGE believes could create confusion and goes beyond the scope of what FERC required in Order No. 706. For additional information, please see PGE's separately submitted comments.
Liberty Electric Power LLC	Negative	In addition to the survey comments, the inclusion of the following sentence in the compliance measures section needs to be removed to make the standard acceptable: For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit. There is no BES reliability benefit for six years of documentation on many of these requirements. In those cases where there is such a benefit, the standard should be written with a six-year retention requirement.
NRG Energy, Inc.	Negative	3) Under R3 TFEs would still be required under the medium or high impact levels unless these systems are upgraded or replaced.4) If a high or medium impact system is required to alert in real time for events that necessitate a real time event in R4.2, why is necessary to review a sampling every two weeks under R4.5? 5) Under R5.2, the senior manager or delegate may be too removed from the actual access control process to authorize individuals and provide access permissions for various accounts. 6) CAN-0017 is in direct conflict with R5.5 which allows either technical or procedural controls for enforcement of password parameters. CAN-0017 forces TFEs unnecessarily. 7) Under R2, Assessments on Vulnerability notices may take more than 30 day period. 8) What is the CIP Exceptional Circumstance definition? It is not listed
Southwest Transmission Cooperative, Inc.	Negative	On page 39 of the application guidelines in section 1.2, Component should be made lower case. Part 5.5.2 needs to be refined further. It needs to be clear that maximum complexity regarding character types in the password applies if the BES Cyber System cannot support at least three character types. We suggest appending "if less than three character types" to the end of the requirement for further clarity. Because there are likely many ports for Requirement R1, the four VSLs could be written based on the percentage of ports missing from documentation. For Requirements R2-R4, there will likely be many BES Cyber Systems to which the requirements apply. Four VSLs could easily be written based on the number of BES Cyber Systems for which the requirement was missed.
Kansas City Power & Light	Negative	Proposed standard introduces additional uncertainty, confusion and misunderstanding.

Organization	Yes or No	Additional Comments Received
Co.		
Hydro-Québec TransÉnergie	No	since there is no place for on general comments, see responses in the to the last question (49)Under "BES Reliability Operating Services" o “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet o Recommend that “Change management” under “Situational Awareness” be clarified to changes in the BES instead of IT change management o Recommend clarification that “Facility” is the NERC Glossary Term -- in “Facility operational data and status” under “Inter-Entity Real-Time Coordination and Communication”o Request clarification on the scope of this “Operational Directives”. Does it include company messaging system? Two way radios? What is the relationship with the new COM-002?o Request clarification that these Coordination and Communications are limited to Reliability not Market Systems o recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" o For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret
Pacific Northwest Small Public Power Utility Comment Group		The comment form provided no room for comments not addressing particular requirements, so we are listing our more general comments here.From the webinar we understand that where the requirements refer to tables where none of the table entries applies to an entity, the requirement itself is not applicable. Since this is not the general case for the relationship between requirements and sub-requirements in NERC standards, we suggest explicitly stating that this is how it works in the CIP standards.We find the Applicability-Facilities Section (4.2) in CIP-003 to be confusing, since all the requirements of this standard appear to apply to the applicable entities and not to facilities. Suggest removing the 4.2.1 through 4.2.3, or stating more clearly how the facilities affect the requirements.The background section of CIP-003 goes into great detail regarding the table format while CIP-003 itself does not follow this format. Please remove or rewrite this section.The very last statement of the guideline section of CIP-005 references a document we are not familiar with. Please provide a complete reference or link to its location.

Additional Comments Submitted:

Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG)
Corresponding additional information provided:

In addition to the background mapping matrix, the CSWG is also providing a narrative introduction to the methodology used to develop the mapping and prepare our "Official Comments:"

The Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) has developed a mapping between NERC CIP v5 requirements and the high-level security requirements (HLRs) in the National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628, *Guidelines for Smart Grid Cyber Security*. The NISTIR 7628 is available at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

This mapping identifies any gaps between CIP v5 and the NISTIR 7628 HLRs and recommendations to the CIP drafting team to consider. The complete mapping (Excel file) will be submitted to the CIP drafting separately as a reference document. Some sections of the comment form have been left blank because no gaps or recommendations were identified.

The CIP-002-5 criteria provide a sound approach for identifying low, medium, and high impact systems within the BES. This three level approach aligns well with the three level approach (i.e., low, moderate, and high) used within the NISTIR. Most requirements in the current CIP drafts are applicable to both medium and high impact systems as a bundled pair and they are silent on their applicability to low impact systems. In contrast, the NISTIR uses a graded requirement approach that specifies baseline controls that apply at low impact levels and then specifies strengthened controls for moderate impact and even stronger controls for high impact levels. The CIP version 5 standards will be significantly strengthened if they were to incorporate a similar graded approach when applying requirements.

Please see the Excel Spreadsheet attached to this document for review.

Xcel Energy
Alice Ireland
Question 16

16. CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Comments: Under the proposed CIP-004-5, attestations from contractors or service vendors for personnel risk assessments (PRAs) are explicitly permitted as proof that a PRA was completed prior to granting a contractor or vendor employee access to the various systems and assets covered by the Standard. We would like to request consideration for also including as acceptable evidence attestations from entities who share access to covered assets within a shared facility, such as a substation. We request the addition of language to Part 5.1, which describes the acceptable evidence of compliance with this obligation, to state that "evidence may include, but is not limited to . . . Dated documentation or attestations from *contractors, service vendors or entities with shared access at a facility* verifying that personnel risk assessments were conducted pursuant to CIP-004-5 R4 before access was authorized."

Pacific Northwest National Laboratory
David McKinnon, Sam Clements and Paul Skare

See attachment

END OF REPORT

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Tel: (509) 372-4210
Fax: (509) 372-4353
MSIN: K1-85
paul.skare@pnnl.gov

January 3, 2012

Laura Hussey
Standards Process Manager
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA

Dear Laura,

I wish you a successful 2012! During GridEx, you invited me to provide comments on NERC CIP v5. We had a parallel request from DOE, so we are able to provide you both with the comments.

David McKinnon, Sam Clements and Paul Skare from PNNL all contributed to this review. We realize that there is an electronic response form as well as a document form that are being used to collect comments on this draft standard. As we attempted to use these tools we felt that our comments did not fit well with the confines of the provided forms and thus decided to provide our comments as follows. You will find our responses in two categories 1) general comments that apply to the standards as a whole, and 2) specific comments for each of the individual standards. We did not spend the time to wordsmith or format to great lengths, so please excuse any vagaries. Our spirit in the review was to genuinely have impact to improve the final product NERC puts out. We hope that you find them useful and are happy to discuss further if you have questions.

General Comments

With NERC CIP v5, we believe a graded security approach with low, medium and high impact on the BES is a sound approach, but have found it mostly focused on medium and high impact systems, and mostly the medium and high impact systems are bundled as a pair. For example, some password requirements are given for medium and high impact systems, but the draft is completely silent about what should be done for low impact systems. There is no reason not to mandate a no default password policy for *__all__* systems within the BES. Yes, there might be a few cases where legacy systems

do not support anything but hard-coded defaults, but these could be documented en masse as exceptions (with associated compensating controls) rather than let these exceptions be used as an excuse to allow a poor password policy.

In an effort to reduce the burden to industry we recommend including a grandfather clause that provides certain exceptions for legacy low-impact systems (such as those that do not have external computing interfaces or capabilities).

As noted, the systems are graded into low, medium, and high, but the requirements/controls are not applied in a graded three-tier approach. Most requirements lump high and medium into one category and ignore low. Ideally we should have requirements that get successively stronger as we migrate from low to medium to high.

There are a number of concerns that either exist in multiple places throughout the CIP standards or are applicable to the standard as a whole they include:

- Consistency of the capitalization of terms
- Consistency in the use of the terms Cyber Asset and Cyber System
- Consistency in the use of the terms Cyber access and electronic access
- Section 4.2.4.2 of many of the requirements use the term Electronic Security Perimeters. Has this been deprecated?
- We disagree with Section 4.2.4.2 as an exemption - Communication links should be protected between ESPs
- As defined, CIP Exception circumstances are not that exceptional. Scaling back requirements within an exceptional circumstance is acceptable, but completely suspending requirements is not.
- Include a definition of terms section to the standards. The applicability section of each standard defines how the term applies to that standard but does not fully define the meaning of the term.

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

CIP-002-5

4.1.2 How are smart grid devices being operated by Distribution Providers?

- Battery Storage is another question that is not addressed
- Other smart grid assets (100KV+)

4.2.4.x Cyber Assets should be prefaced by BES
Should the last paragraph on page 7 say "cyber security plan"?

CIP-003-5

4.2.4.4 What is the definition of Cyber System vs. Cyber Asset? There is a need for consistency in use – especially in the tables.

5. Background – It seems this entire section is predicated upon a table which is missing. There is no table [Table Reference] pg 7 and under Applicability there is no table to aid in understanding of all the different "Applicability Columns"

R2 Should include a Procurement Policy requirement

R2 Should include a Resiliency Policy requirement

R2 1.5 System Security: Should include third-party, outsourcing, and availability or be considered as separate topics.

Guidelines
R2 2.1 Personnel Security: Should explicitly include subcontractors and outsourced services

R2 2.3 Remote Access should be moved into System Security

Include language in contracts that requires vendors, contractors, or consultants adhere to the Responsible Entity's policies and controls.

R2 2.7 Recovery Plans should include a prioritized recovery strategy

CIP 004-5

Purpose: Should also include the case where one organization has equipment in another organizations facility (i.e. Substation)

R3 The wording of the requirement is confusing. The measure for 3.1 does a better job defining the requirement than the requirement.

CIP 005-5

R1 1.2 The requirements column should state "Control and secure all connectivity through the use of identified Electronic Access Points (EAPs). "

R1 1.4 Eliminate the "where technically feasible" loophole. The statement should simply be "Perform authentication when establishing dial-up connectivity with the BES Cyber System."

R1 1.4 Dial-up access for either non-interactive or interactive sessions should be authenticated. As written, 1.4 only protects non-interactive sessions.

R2 Eliminate the "where technically feasible" loophole. The statement should simply be "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items."

NEW: As written, low impact systems do not have to be protected with passwords, nor are the users required to be authenticated. Requirements for low impact systems should be added.

CIP 006-5

M1. Typo: - As stated "Evidence must includes…" should be "Evidence must include…"

R1 1.5 Clarification needed with respect to the applicability column as to what impact level the associated physical access control systems apply. Explicitly state that this applies to all systems.

R3 3.1 High and medium impact systems should have their associated physical access control systems monitored (and tested) more frequently that once every 24 calendar months. Testing frequency should be dependent upon the impact level (i.e. annual testing of a control center is not too frequent).

CIP 007-5

The requirements in this section should follow a graded approach to match the impact level of the various systems where the lower the impact level the more time or leniency is afforded to meet the requirement.

R2 Patch management is optional for low impact systems. Even these systems should have patches applied, but perhaps in a less timely manner than is required for medium and high impact assets.

R3 Malicious code protection is not required for low impact systems. Even these systems should be monitored/protected.

R4 Once again, low impact systems are not included. Security event monitoring should also apply to low impact systems.

R4 4.5 Two week lag before logs from high impact systems have to be reviewed. The reviews should be more timely, especially if only one calendar day is given to rectify issues discovered. We saw in GridEx how timeliness is important in this area.

R5 Password management is not specified for low impact systems. No guidance is given regarding sharing/reusing passwords between systems.

R5 5.4 Eliminate the “where technically feasible” loophole. The statement should read “Procedural controls for initially changing default passwords unless the default password is unique to the device or instance of the application…”

R5 5.6 Eliminate the “where technically feasible” loophole.

CIP 008-5

Seem OK. However, the definition of a reportable incident seems a bit vague.

CIP 009-5

No comments.

CIP 010-5

R1 1.2 Worded poorly. (Currently: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.) Should more clearly state that (pre) approval is needed for configuration management changes.

R2 2.1 Caveat of "where technically feasible" applies to both medium and high impact systems. Compensating controls should be applied to high impact systems when built-in monitoring of baseline changes is not technically feasible.

R3 3.3 Change in phrase order makes the requirement easier to understand "Perform an active vulnerability assessment prior to adding a new Cyber Asset to a Cyber System or Electronic Access Control or Monitoring System, except for CIP Exceptional Circumstances.

CIP 011-5

No uniform requirements for how BES Cyber System Information is to be handled. Is it business sensitive, official use only, etc? Furthermore, does the level of protection vary based upon whether the information is about high impact or medium impact systems?

Missing a statement about how one is authorized to view BES Cyber System Information. How does one get added to the list of those with a "need to know" the information? Especially regarding external entities such as vendors, contractors, DOE, NERC, etc. the aspect of trust and the needed controls for trusted parties would be useful.

Sincerely,

Mark Morgan
Advanced Power and Energy Systems
Pacific Northwest National Laboratory

NISTIR Requirement		SG.SI-1
NERC CIP		System and Information Integrity Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.SI NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.SI NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.SI NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.SI NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.SI NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.SI NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.SI NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.SI NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.SI NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.SI NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.SI NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.SI NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.SI NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.SI NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.SI NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.SI NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.SI NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.SI NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.SI NISTIR MAPPING**	

R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.SI NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.SI NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.SI NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.SI NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.SI NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.SI NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.SI NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.SI NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.SI NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.SI NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.SI NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.SI NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.SI NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.SI NISTIR MAPPING**	

R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.SI NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.SI NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.SI NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.SI NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.SI NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.SI NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.SI NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.SI NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.SI NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.SI NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.SI NISTIR MAPPING**	

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.SI NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.SI NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.SI NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.SI NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.SI NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.SI NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.SI NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.SI NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.SI NISTIR MAPPING**	

R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.SI NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.SI NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.		2. The CIP requirement is specific to malicious communications. The NISTIR requirement addresses system and information integrity for the organization's personnel and assets
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.SI NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.		
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.SI NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.SI NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.SI NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.SI NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.SI NISTIR MAPPING**	

R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.		
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.		
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.SI NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.SI NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.SI NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.SI NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.SI NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.SI NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.SI NISTIR MAPPING**	

R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.SI NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.SI NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.		
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.		
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.		2. The CIP requirement is specific to remediation. The NISTIR requirement addresses system and information integrity for the organization's personnel and assets
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.SI NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.		

R3, 3.2: Disarm or remove identified malicious code.		
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).		
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.		
R3, 3.5: Log each Transient Cyber Asset connection.		2. The CIP requirement is specific to logging each transient cyber asset connection. The NISTIR requirement addresses system and information integrity for the organization's personnel and assets
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.SI NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.SI NISTIR MAPPING**	

R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.		
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.SI NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.SI NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.SI NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.SI NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.		2. The CIP requirement is specific to validating credentials. The NISTIR requirement addresses system and information integrity for the organization's personnel and assets
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.SI NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.SI NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.SI NISTIR MAPPING**	

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.SI NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.SI NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.SI NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.SI NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.SI NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.SI NISTIR MAPPING**	

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.SI NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.SI NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.SI NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.SI NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.SI NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.SI NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.SI NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.SI NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.SI NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.SI NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.SI NISTIR MAPPING**	

R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.SI NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.SI NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.SI NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.SI NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.SI NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.SI NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.SI NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.SI NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.SI NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.SI NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.SI NISTIR MAPPING**	

CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.SI NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.SI NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.SI NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.SI NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.SI NISTIR MAPPING**	

R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.SI NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.		
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.SI NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.SI NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.SI NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.SI NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.SI NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.SI NISTIR MAPPING**	

R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.SI NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.SI NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.SI NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.SI NISTIR MAPPING**	

SG.SI-2	SG.SI-3	SG.SI-4	SG.SI-5
Flaw Remediation	Malicious Code and Spam Protection	Smart Grid Information System Monitoring Tools and Techniques	Security Alerts and Advisories

		Originally marked with an "X" but not sure they map. The CIP requirement addresses controls to restrict unauthorized access. The NISTIR requirement addresses monitoring capabilities	

		2. The CIP requirement specifies a specific method, i.e. an intermediate device, to isolate the system or asset.	

Originally marked with an "X" but don't think they relate. CIP requirement addresses alerts in response to unauthorized physical access. The NISTIR requirement addresses flaw remediation.		1. Near match between CIP requirement and A5 of NISTIR requirement. NISTIR requirement contains additional requirements.	
			3. CIP requirement does not address receiving security alerts, advisories, and directives from external organizations

2. The CIP requirement requires the identification of sources to monitor for security patches, etc. The NISTIR requirement does not specify that the sources be identified.	2. The CIP requirement requires the identification of sources to monitor for security patches, etc. The NISTIR requirement does not specify that the sources be identified.	2. The CIP requirement requires the identification of sources to monitor for security patches, etc. The NISTIR requirement does not specify that the sources be identified.	
4. The CIP requirement identifies specific time frames. The NISTIR requirement does not identify specific time frames.	4. The CIP requirement identifies specific time frames. The NISTIR requirement does not identify specific time frames.	4. The CIP requirement identifies specific time frames. The NISTIR requirement does not identify specific time frames.	
4. Though the wording is different, the intent of these requirements are similar.			
2. The CIP requirement is specific to malicious code. The NISTIR requirement addresses flaw remediation in general.	3. The CIP requirement does not address preventing users from circumventing malicious code protection capabilities.	2. The CIP requirement is specific to malicious code. The NISTIR requirement addresses tools and techniques in general.	

	4. Though the wording is different, the intent of these requirements are similar.	2. The CIP requirement is specific to malicious code. The NISTIR requirement addresses tools and techniques in general.	
2. The CIP requirement is specific to malicious code. The NISTIR requirement addresses flaw remediation in general.	4. The CIP requirement identifies specific time frames for the updates. The NISTIR requirement states "whenever new releases are available in accordance with organizational configuration management policy and procedures"	2. The CIP requirement is specific to malicious code. The NISTIR requirement addresses tools and techniques in general.	
2. The CIP requirement is specific to malicious code. The NISTIR requirement addresses flaw remediation in general.	2. The CIP requirement is specific to transient cyber assets and removable media.	2. The CIP requirement is specific to transient cyber assets and removable media.	
		2. The CIP requirement is specific to logging each transient cyber asset connection. The NISTIR requirement addresses tools and techniques in general.	

			3. CIP requirement does not address receiving security alerts, advisories, and directives from external organizations

SG.SI-6	SG.SI-7	SG.SI-8	SG.SI-9
Security Functionality Verification	Software and Information Integrity	Information Input Validation	Error Handling
		NO NERC CIP MAPPING	**NO NERC CIP MAPPING**

	Originally not labeled with an "X" Suggest 1, but the CIP requirement states where technically feasible.		
Originally not labeled with an "X" Suggest 3. CIP requirement requires verification at least once a calendar year. NISTIR requirement requires verification at startup, restart, and command by user with appropriate privilege at an organization-defined frequency			

HLR Team - Please review the HLR families you've signed up for (including any rows that are hidden) to ensure that nothing was missed (or checked in error). Please make any/all edits in directly into this Google Document to ensure we are all working off the latest version.

Replace any "X"s in the current mapping with the following:

1 - Exact match in requirement between NISTIR and NERC CIP v5
2 - CIP requirement is more granular
3 - NISTIR requirement is more granular
4 - CIP is more specific, but there is no conflict between CIP and NISTIR. For example, in the area of physical security NISTIR requires a policy, while CIP's Visitor Control Program stipulates additional details that NERC requires in such a policy. No recommendation to CIP or NISTIR except identification of the mapping is necessary.

If the requirements are very similar, provide specific comments/recommendations in the mapping. Also, please make notes of any relevant gaps you notice in either the NISTIR or the CIP as you complete the review.

The end goal is to finalize a detailed mapping of the NISTIR reqs to the CIPs (v5), develop a Venn diagram showing requirement areas unique and common to both the NISTIR and CIP, and provide input to the CIP

NISTIR Requirement		SG.AC-1
NERC CIP		Access Control Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.AC NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.AC NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.AC NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.		SGIP should include following in SG.AC-1: Organization shall incorporate a policy of appointing a Senior Manager at sufficient position to ensure that cyber security security requirements get adequate priorities and effectiveness in policy implementation. The policy shall allow appointment of senior manager and delegation of his/her authority in the organization.

R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.AC NISTIR MAPPING**	
R2, 1.1: Personnel Security		SGIP should include following in SG.AC-1: Each organization shall document personnel Security assessment and back ground check policies and procedures for protecting BES Cyber Systems from internal and external Cyber threats.
R2, 1.2: Electronic Security Perimeters		SGIP should include following in SG.AC-1: Each organization shall document requirements to identify Critical Cyber Assets and identify Electronic Security Perimeter to define access control to the access points on the perimeter.

R2, 1.3: Remote Access		
R2, 1.4: Physical Security		SGIP should include following in SG.AC-1: Organization shall include policy and procedures for granting Physical access to the BES Cyber Systems. 2. Organization shall implement criteria for restricting or granting physical access to the BES Cyber Systems.

R2, 1.5: System Security		
R2, 1.6: Incident Response	**NO SG.AC NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.AC NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.AC NISTIR MAPPING**	
R2, 1.9: Information Protection		
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.AC NISTIR MAPPING**	

R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.		SGIP shall include following Requirement in SG.AC-1:Organizations shall review their Cyber Security Standards and obtain their Senior Manager's approval initially on the standards' effective date and subsequently once in each calendar year and the gap between approvals and reviews shall not exceed 15 calendar months.
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.AC NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.AC NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.AC NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.AC NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.AC NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.AC NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.		
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.AC NISTIR MAPPING**	

R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.AC NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.AC NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.AC NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.AC NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.AC NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.AC NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.AC NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.AC NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.AC NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.AC NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.AC NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.AC NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.AC NISTIR MAPPING**	
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.AC NISTIR MAPPING**	

R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.AC NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.AC NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.AC NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.AC NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.		2 - CIP requirement is more granular - CIP further specifies who is responsible for what type of access control.
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		2 - CIP requirement is more granular - CIP further specifies who is responsible for what type of access control.
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		2 - CIP requirement is more granular - CIP further specifies who is responsible for what type of access control.
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		2 - CIP requirement is more granular - CIP further specifies who is responsible for what type of access control.
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.		2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.		2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.		2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.AC NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.AC NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.AC NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.AC NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.AC NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.AC NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.AC NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.		3 - NISTIR requirement is more granular - NISTIR further specifies that policies should comply with applicable federal, state, and local regulations

R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).		
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.		
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.		
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.AC NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.		
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.		
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.		

R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.		
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.AC NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.		3 - NISTIR requirement is more granular - NISTIR further specifies that policies should comply with applicable federal, state, and local regulations
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.AC NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.AC NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.AC NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.AC NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.AC NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.AC NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.AC NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.AC NISTIR MAPPING**	

R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.AC NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.AC NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.AC NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.AC NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.		
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.AC NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.AC NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.AC NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.AC NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.AC NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.AC NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.AC NISTIR MAPPING**	

R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.AC NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.AC NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.AC NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.AC NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.AC NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.AC NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.AC NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.AC NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.AC NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.		2(SGIP should include each of the applicable items in CIP-007-5 Table R5 – System Access Controls)
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.		

R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.		
R5, 5.3: Identify individuals who have authorized access to shared accounts.		
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.		2 - CIP requirement is more granular - CIP specifies more detail with respect to default passwords.
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.		
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.		
CIP-011-1: Cyber Security-Information Protection		

R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.AC NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.AC NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.		3 - NISTIR requirement is more granular - NISTIR further specifies that policies should comply with applicable federal, state, and local regulations
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.AC NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.AC NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.AC NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.AC NISTIR MAPPING**	

SC.AC-2	SG.AC-3	SG.AC-4	SG.AC-5
Remote Access Policy and Procedures	Account Management	Access Enforcement	Information Flow Enforcement
			NO CIP MAPPING

CIP should elaborate requirement R2.13, to include following: 1. Responsible Entity should document allowed methods of access to the BES Cyber Systems 2. Responsible Entity should incorporate in their policies the usage restrictions and criteria for allowing each remote access 3. Responsible Entity should setup authorization procedure prior to actually granting remote access 4. Responsible Entity should enforce requirement criteria for providing remote access to the BES Cyber systems			

	2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.	2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.	
	2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.	2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.	

	2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.	2 - CIP requirement is more granular - CIP further specifies time frequency for specific type of access control management.	
3 - NISTIR requirement is more granular - NISTIR further specifies issue of authorization.			

3 - NISTIR requirement is more granular - NISTIR further specifies issues of usage restrictions and authorization.			
2 - CIP requirement is more granular - CIP specifies requirement for intermediate device.			

		2 - CIP requirement is more granular - CIP specifies controls to restrict physical access.	

		2 - CIP requirement is more granular - CIP specifies validating credentials.	

		2 - CIP requirement is more granular - CIP identifies different access account types (e.g. administrator, shared, default).	
	2 - CIP requirement is more granular - CIP discusses individuals for shared accounts.	2 - CIP requirement is more granular - CIP discusses individuals for shared accounts.	
	3(CIP should include SGIP requirement details)		

SG.AC-6	SG.AC-7	SG.AC-8	SG.AC-9
Separation of Duties	Least Privilege	Unsuccessful Login Attempts	Smart Grid Information System Use Notification
NO CIP MAPPING			

	2 - CIP requirement is more granular - CIP further specifies for electronic access.		
	2 - CIP requirement is more granular - CIP further specifies for unescorted BES Cyber Systems' physical access.		
	2 - CIP requirement is (slightly) more granular - CIP further specifies BES Cyber System Info.		
	2 - CIP requirement is more granular - minimum necessary access permissions stated in 6.1 and 6.2 in CIP. CIP further specifies time frequency for access control management.		
	3 - NISTIR requirement is more granular - NISTIR specifies using most restrictive privileges.		

	2 - CIP requirement is more granular - minimum necessary access permissions stated in 6.3 in CIP. CIP further specifies time frequency for access control management.		
		3 - NISTIR requirement is more granular - NISTIR specifies limiting number of unsuccessful logins with T time.	3 - NISTIR requirement is more granular - NISTIR discusses displaying banners before granting access that provide notices consistent with laws, directives, policies, etc.

	2 - CIP requirement is more granular - CIP specifies restricting for logical network ports.		
	2 - CIP requirement is more granular - CIP specifies restricting for physical network ports.		

		3- CIP-007-5-R5.6 shall include following requirement: a. Real-time logging and recording of unsuccessful login attempts; and b. Real-time alerting of a management authority for the Smart Grid information system when the number of defined consecutive invalid access attempts is exceeded.	

SG.AC-10	SG.AC-11	SG.AC-12	SG.AC-13
Previous Logon Notification	Concurrent Session Control	Session Lock	Remote Session Termination
NO CIP MAPPING		**NO CIP MAPPING**	

			CIP should elaborate requirement R2.13, to include following: 1. Responsible Entities shall implement policies and procedures for managing remote sessions in their BES Cyber Systems access control policies and procedures.

	3 - NISTIR requirement is more granular - NISTIR specifies limiting number of concurrent users.		3 - NISTIR requirement is more granular - NISTIR specifies to terminate remote activity after org-defined period of time.

SG.AC-14	SG.AC-15	SG.AC-16	SG.AC-17
Permitted Actions without Identification or Authentication	Remote Access	Wireless Access Restrictions	Access Control for Portable and Mobile Devices
			NO CIP MAPPING

	CIP should elaborate requirement R2.13, to include following: 1.Responsible Entities shall include in procedures and criteria of granting Remote access encryption, authentication of all communication media through limited number of manageable access control points.		

3 - NISTIR requirement is more granular - NISTIR specifies special cases for not requiring identification or authorization access controls.		3 - NISTIR requirement is more granular - CIP does not discuss wireless access. NISTIR specifies authentication and encryption and scanning for unauthorized wireless access points.	

	(SGIP should include protection of routable and dialup networks)		
	(SGIP should include accesss points using routable protocols and include criteria for granting or denying access privilege)		
	(SGIP should include authentication on dialup connectivity on BES networks)		
	3 - NISTIR requirement is more granular - NISTIR specifies additional processes for remote access (e.g. routes RA through limited number of managed access points, discusses constraints for wireless access, monitoring for unauthorized access).		
	2 - CIP requirement is more granular - CIP requires intermediate device for asset initiating remote access so asset does not directly access BES cyber system.		
	(SGIP should include requirement of encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session)		

	(SGIP should include requirement of multi-factor authentication for all Interactive Remote Access sessions)		

SG.AC-18	SG.AC-19	SG.AC-20
Use of External Information Control Systems	Control System Access Restrictions	Publicly Accessible Content
		NO CIP MAPPING

	CIP should elaborate Requirement R2.15 to include following: Responsible Entities shall include in their policies and procedures to grant access privileges to their BES information Systems based on minimum privilege justified by the business requirement for access requests.	
CIP should elaborate Requirement R2.19 to include following: Responsible entities shall restrict access to external information systems or restrict processing, storing or transmitting controlled information through External Information systems over which the Responsible Entities have no control.		

	3 - NISTIR requirement is more granular - NISTIR specifies restricting access to smart grid from organization's enterprise network.	

	3 - NISTIR requirement is more granular - NISTIR specifies restricting access to smart grid from organization's enterprise network.	

SG.AC-21
Passwords

2- SGIP shall implement the requirement as follows: Implement :Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.
2- SGIP shall implement the requirement as follows: IR5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.
2(SGIP should include this requirement)

NISTIR Requirement		SG.AT-1
NERC CIP		Awareness and Training Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.AT NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.AT NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.AT NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.AT NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.AT NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.AT NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.AT NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.AT NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.AT NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.AT NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.AT NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.AT NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.AT NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.AT NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.AT NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.AT NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.AT NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.AT NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.AT NISTIR MAPPING**	

R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.		2 - CIP requirement is more granular. - NISTIR requirement does not specify time periods.
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.		2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.
R2, 2.1: Define the roles that require training.		2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.		
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.		2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.		2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.
R2, 2.5: Training on the visitor control program.		2 - CIP requirement is more granular. - NISTIR does not describe a visitor control program.

R2, 2.6: Training on handling of BES Cyber System Information and storage media.		2 - CIP requirement is more granular. - NISTIR does not describe handling of storage media.
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.		2 - CIP requirement is more granular. - NISTIR does not address notifications.
R2, 2.8: Training on recovery plans for BES Cyber Systems.		2 - CIP requirement is more granular. - NISTIR does not address recovery plans.
R2, 2.9: Training on response to BES Cyber Security Incidents.		2 - CIP requirement is more granular. - NISTIR does not address incident response.
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.		2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.		2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.		2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.		2 - CIP requirement is more granular. - NISTIR requirement does not specify time periods.
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.AT NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.AT NISTIR MAPPING**	

R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.AT NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.AT NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.AT NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.AT NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.AT NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.AT NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.AT NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.AT NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.AT NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.AT NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.AT NISTIR MAPPING**	

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.AT NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.AT NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.AT NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.AT NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.AT NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.AT NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.AT NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.AT NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.AT NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.AT NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.AT NISTIR MAPPING**	

R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.AT NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.AT NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.AT NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.AT NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.AT NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.AT NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.AT NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.AT NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.AT NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.AT NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.AT NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.AT NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.AT NISTIR MAPPING**	

R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.AT NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.AT NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.AT NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.AT NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.AT NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.AT NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.AT NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.AT NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.AT NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.AT NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.AT NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.AT NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.AT NISTIR MAPPING**	

R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.AT NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.AT NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.AT NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.AT NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.AT NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.AT NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.AT NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.AT NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.AT NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.AT NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.AT NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.AT NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.AT NISTIR MAPPING**	

R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.AT NISTIR MAPPING**	
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.AT NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.AT NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.AT NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.AT NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.AT NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.AT NISTIR MAPPING**	

R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.AT NISTIR MAPPING**	
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.AT NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.AT NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.AT NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.AT NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.AT NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.AT NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.AT NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.AT NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.AT NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.AT NISTIR MAPPING**	

R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.AT NISTIR MAPPING**	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.AT NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.AT NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.AT NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.AT NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.AT NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.AT NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.AT NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.AT NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.AT NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.AT NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.AT NISTIR MAPPING**	

R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.AT NISTIR MAPPING**	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.AT NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.AT NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.AT NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.AT NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.AT NISTIR MAPPING**	

R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.AT NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.AT NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.AT NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.AT NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.AT NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.AT NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.AT NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.AT NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.AT NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.AT NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.AT NISTIR MAPPING**	

R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.AT NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.AT NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.AT NISTIR MAPPING**	

SG.AT-2	SG.AT-3	SG.AT-4	SG.AT-5
Security Awareness	Security Training	Security Awareness and Training Records	Contact with Security Groups and Associations
			NO CIP MAPPING

These are similar but not identical requirements. CIP specifies security awareness reinforcement on at least a quarterly basis. NISTIR specifies that cyber security awareness sessions with practical exercises be held at a recurring organization-defined frequency.	These are similar but not identical requirements. CIP specifies security awareness reinforcement on at least a quarterly basis. NISTIR specifies that authorized users of a system must undergo cyber security training prior to being granted access.		
2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.		
	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.		
	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.		
	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.	
	2 - CIP requirement is more granular. - NISTIR does not describe a visitor control program.		

	2 - CIP requirement is more granular. - NISTIR does not address notifications.		
	2 - CIP requirement is more granular. - NISTIR does not address recovery plans.		
	2 - CIP requirement is more granular. - NISTIR does not address incident response.		
	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.		
	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.		
	2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.		
	2 - CIP requirement is more granular. - NISTIR requirement does not specify time periods.		

SG.AT-6	SG.AT-7
Security Responsibility Training	Planning Process Training
	NO CIP MAPPING

2 - CIP requirement is more granular. - CIP describes more specific training program requirements than NISTIR.	

NISTIR Requirement		SG.AU-1
NERC CIP		Audit and Accountability
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.AU NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.AU NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.AU NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.AU NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.AU NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.AU NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.AU NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.AU NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.AU NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.AU NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.AU NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.AU NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.AU NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.AU NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.AU NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.AU NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.AU NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.AU NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.AU NISTIR MAPPING**	

R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.AU NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.AU NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.AU NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.AU NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.AU NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.AU NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.AU NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.AU NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.AU NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.AU NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.AU NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.AU NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.AU NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.AU NISTIR MAPPING**	

R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.AU NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.AU NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.AU NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.AU NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.AU NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.AU NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.AU NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.AU NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.AU NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.AU NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.AU NISTIR MAPPING**	

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.AU NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.AU NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.AU NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.AU NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.AU NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.AU NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.AU NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.AU NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.AU NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.AU NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.AU NISTIR MAPPING**	

R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.AU NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.AU NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.AU NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.AU NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.AU NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.AU NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.AU NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.AU NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.AU NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.		
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.AU NISTIR MAPPING**	

R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.AU NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.AU NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.AU NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.AU NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.		2 - CIP requirement is more granular. - NISTIR requirement describes a high level policy.
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.AU NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.AU NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.AU NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.AU NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.AU NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.AU NISTIR MAPPING**	

R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.AU NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.AU NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.AU NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.AU NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.AU NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.AU NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.		
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.		
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.		
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.		
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.		
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.AU NISTIR MAPPING**	

R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.AU NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.AU NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.AU NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.AU NISTIR MAPPING**	
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.AU NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.AU NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.AU NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.AU NISTIR MAPPING**	

R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.AU NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.AU NISTIR MAPPING**	
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.AU NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.AU NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.AU NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.AU NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.AU NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.AU NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.AU NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.AU NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		

R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.AU NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.AU NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.AU NISTIR MAPPING**	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.AU NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.AU NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.AU NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.AU NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.AU NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.AU NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.AU NISTIR MAPPING**	

R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.AU NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.AU NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.AU NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.AU NISTIR MAPPING**	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.AU NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.AU NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.AU NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.AU NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.AU NISTIR MAPPING**	

R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.AU NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.AU NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.AU NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.AU NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.AU NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.AU NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.AU NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.AU NISTIR MAPPING**	

R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.AU NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.AU NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.AU NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.AU NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.AU NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.AU NISTIR MAPPING**	

SG.AU-2	SG.AU-3	SG.AU-4	SG.AU-5
Auditable Events	Content of Audit Records	Audit Storage Capacity	Response to Audit Processing Failures
		NO CIP MAPPING	

2 - CIP requirement is more granular. - CIP requirement only refers to physical events. NISTIR requirement does not specify only physical events.			

2 - CIP requirement is more granular. - NISTIR requirement does not discuss failure of access control.	2 - CIP requirement is more granular. - NISTIR requirement does not discuss failure of access control.		

2 - CIP requirement is more granular. - CIP requirement defines some events to be audited, while NISTIR states that events must be defined.			
			3 - NISTIR requirement is more granular. - NISTIR specifies some events that alerts should be generated.
			2 - CIP requirement is more granular. - NISTIR does not specify end of next calendar day.

SG.AU-6	SG.AU-7	SG.AU-8	SG.AU-9
Audit Monitoring, Analysis, and Reporting	Audit Reduction and Report Generation	Time Stamps	Protection of Audit Information
	NO CIP MAPPING	**NO CIP MAPPING**	**NO CIP MAPPING**

2 - CIP requirement is more granular. - NISTIR requirement does not specify time periods.			

SG.AU-10	SG.AU-11	SG.AU-12	SG.AU-13
Audit Record Retention	Conduct and Frequency of Audits	Auditor Qualification	Audit Tools
	NO CIP MAPPING	**NO CIP MAPPING**	**NO CIP MAPPING**

2 - CIP requirement is more granular. - NISTIR requirement does not specify time periods.			

SG.AU-14	SG.AU-15	SG.AU-16
Security Policy Compliance	Audit Generation	Non-Repudiation
NO CIP MAPPING		**NO CIP MAPPING**

	2 - CIP requirement is more granular. - NISTIR requirement does not discuss failure of access control.	

NISTIR Requirement		SG.CA-1
NERC CIP		Security Assessment and Authorization Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.		4. The CIP requirement specifies that entities must categorize their cyber assets and systems. These categorizations are identified at the interface level in the NISTIR and explained in Section 2.3
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.		
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.		
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.		4. The CIP requirement is specific to the Senior Manager. The NISTIR requirement states that security assessment and authorization policies and procedures for the personnel and assets

R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.CA NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.CA NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.CA NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.CA NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.CA NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.CA NISTIR MAPPING**	
R2, 1.6: Incident Response	**NO SG.CA NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.CA NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.CA NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.CA NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.CA NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.		
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.CA NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.		

R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.		
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.CA NISTIR MAPPING**	
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.CA NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.CA NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.CA NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.CA NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.CA NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.CA NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.CA NISTIR MAPPING**	

R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.CA NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.CA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.CA NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.CA NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.CA NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.CA NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.CA NISTIR MAPPING**	
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.CA NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.CA NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.CA NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.CA NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.CA NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.CA NISTIR MAPPING**	

R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.CA NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.CA NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.CA NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.CA NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.CA NISTIR MAPPING**	
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.CA NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.CA NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.CA NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.CA NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.CA NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.CA NISTIR MAPPING**	

R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.CA NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.CA NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.CA NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.CA NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.CA NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.CA NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.CA NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.CA NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.CA NISTIR MAPPING**	

R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.CA NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.CA NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.CA NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.CA NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.CA NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.CA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.CA NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.CA NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.CA NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.CA NISTIR MAPPING**	

R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.CA NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.		
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.CA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.CA NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.CA NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.CA NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).		
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.CA NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.CA NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.CA NISTIR MAPPING**	

R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.CA NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.CA NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.CA NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.CA NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.CA NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.CA NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.CA NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.CA NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.CA NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.CA NISTIR MAPPING**	

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.CA NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.CA NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.CA NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.CA NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.CA NISTIR MAPPING**	

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.CA NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.CA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.CA NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.CA NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.CA NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.		
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.		
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.CA NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.CA NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.CA NISTIR MAPPING**	

R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.CA NISTIR MAPPING**	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.CA NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.CA NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.CA NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.CA NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.CA NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.CA NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.		

R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.		
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.		
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.		
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.CA NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.CA NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.		

R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.CA NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.CA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.CA NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.CA NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.CA NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.CA NISTIR MAPPING**	

R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.CA NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.CA NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.CA NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.CA NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.CA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.CA NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.CA NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.CA NISTIR MAPPING**	

SG.CA-2	SG.CA-3	SG.CA-4	SG.CA-5
Security Assessments	Continuous Improvement	Information System Connections	Security Authorization to Operate
		NO CIP MAPPING	
			This was labeled with an "X" as a match, but not sure it really does. The CIP requirement deals with asset and system categorization and the NISTIR requirement deals with authorization to operate.
4. The CIP requirement identifies specific time frames for updates. The NISTIR requirement states "organization-defined frequency"	3. The CIP requirement identifies specific time frames for updates. The NISTIR requirement states "continuous improvement." The NISTIR requirement is also specific to best practices.		4. The CIP requirement identifies specific time frames for updates. The NISTIR requirement states "organization-defined frequency or when a significant change occurs to the Smart Grid information system"
			4. The CIP requirement identifies specific time frames. The NISTIR requirement states "organization-defined frequency"

			4. The CIP requirement identifies specific time frames. The NISTIR requirement states "organization-defined frequency"
			4. The CIP requirement states that the Senior Manager or their delegate may authorize the system. The NISTIR requirement states "a management authority"

			2. The CIP requirement addresses changes to the Senior Manager or their delegate. The NISTIR requirement states "a management authority" and does not address changes to the management authority.

SG.CA-6

Continuous Monitoring

Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies review frequency

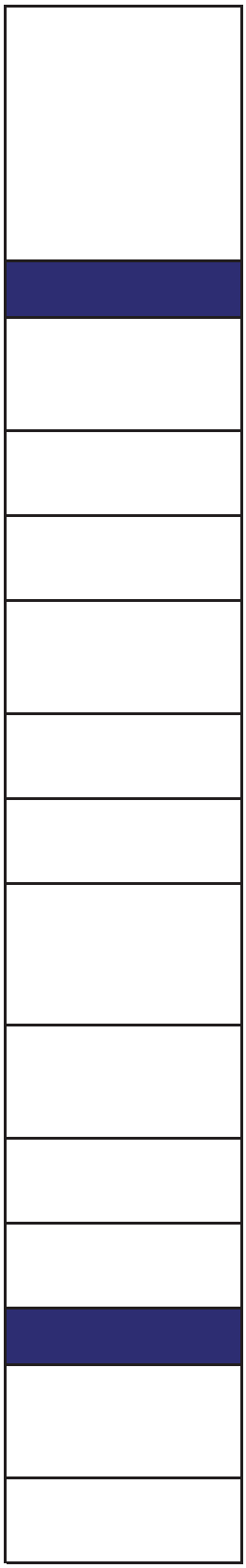

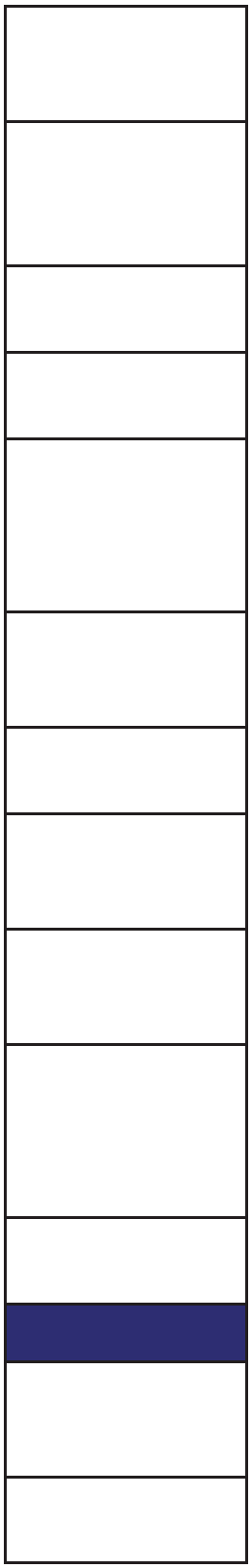

Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies update frequency
Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies update frequency

Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies update frequency
Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies update frequency
Originally not labeled with an "X"

Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies review frequency

Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies update frequency
Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies update frequency
Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies reporting time frame
Originally not labeled with an "X" Suggested label is 4 since the CIP requirement specifies update frequency

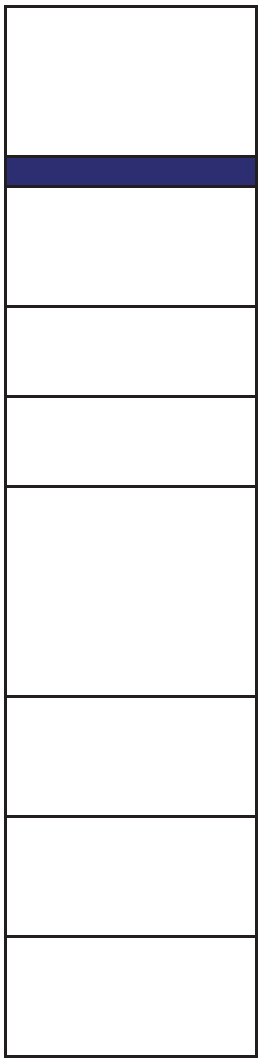

NISTIR Requirement		SG.CM-1
NERC CIP		Configuration Management Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.		
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.		
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.		
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.		
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:		
R2, 1.1: Personnel Security		
R2, 1.2: Electronic Security Parameters		
R2, 1.3: Remote Access		
R2, 1.4: Physical Security		
R2, 1.5: System Security		
R2, 1.6: Incident Response		
R2, 1.7: Recovery Plans		
R2, 1.8: Configuration Change Management		3 - CIP provides more information about the specifics of what a change management process should include in section 2.8.
R2, 1.9: Information Protection		

R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances		
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.		(this is related to all of the -1 SG high level requirements.
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.		
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.		
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.		
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.		
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.		
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.		
R2, 2.1: Define the roles that require training.		
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.		
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.		
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.		
R2, 2.5: Training on the visitor control program.		
R2, 2.6: Training on handling of BES Cyber System Information and storage media.		
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.		

R2, 2.8: Training on recovery plans for BES Cyber Systems.		
R2, 2.9: Training on response to BES Cyber Security Incidents.		
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.		
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.		
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.		
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.		
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.		
R4, 4.1: An initial personnel risk assessment that includes identity verification.		
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.		
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.		
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.		
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.		
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.		
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.		

R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.		
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.		
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.		
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.		
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.		
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.		
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.		
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.		

R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.		
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.		
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.		
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).		
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.		
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.		
R1, 1.5: A documented method for detecting malicious communications at each EAP.		
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.		
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.		
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.		
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.		
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.		
R1, 1.1: Define operational or procedural controls to restrict physical access.		
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.		

R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.		
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.		
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.		
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.		
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.		
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.		
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.		
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.		
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.		
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.		
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.		
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.		
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.		

R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.		X
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.		X
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.		
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.		
R3, 3.2: Disarm or remove identified malicious code.		
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).		
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.		
R3, 3.5: Log each Transient Cyber Asset connection.		
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.		
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.		
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.		
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.		
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.		
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.		

R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.		
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.		
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.		
R5, 5.3: Identify individuals who have authorized access to shared accounts.		
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.		
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.		
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.		
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.		
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.		
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.		

R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.		
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.		
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.		
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.		
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.		
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.		
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.		
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.		
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.		
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.		
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		

R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.		
R1, 1.1: Conditions for activation of the recovery plan(s).		
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.		
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.		
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.		
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.		
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.		
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.		
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.		
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.		
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.		
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.		
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.		

R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.		
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.		
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.		
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.		
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.		2 - CIP identifies specific information used to describe the baseline configuration including physical location, OS, applications, network ports and security patch levels.
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.		
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.		
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.		

R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.		X
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.		
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.		X
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.		
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.		
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.		
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.		
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.		
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.		

R1, 1.1: One or more methods to identify BES Cyber System Information.		
R1, 1.2: Access control and handling procedures for BES Cyber System Information.		
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.		
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		

SG.CM-2	SG.CM-3	SG.CM-4	SG.CM-5
Baseline Configuration	Configuration Change Control	Monitoring Configuration Changes	Access Restrictions for Configuration Change
	3 - CIP provides more information about the specifics of what a change management process should include in section 2.8.	3 - CIP provides more information about the specifics of what a change management process should include in section 2.8.	

			x-related
			x-related
			x-related

	X	X	
	X	X	

2 - CIP identifies specific information used to describe the baseline configuration including physical location, OS, applications, network ports and security patch levels.			
	2 - CIP is more explicit about how changes are authorized.	3 - CIP only requires monitoring changes "where technically feasible".	
2 - CIP requires a time limit for updating the configuration.			
x	X	X	

X	X	X	
X	X	X	

			x-related

SG.CM-6	SG.CM-7	SG.CM-8	SG.CM-9
Configuration Settings	Configuration for Least Functionality	Component Inventory	Addition, Removal, and Disposal of Equipment
Combines CM1,2,3,4			

X	X		
X	X		

X			
X			
X			

X			
X			

			x-related
			x-related
			x-related

SG.CM-10	SG.CM-11
Factory Default Settings Management	Configuration Management Plan
	Combines CM.1,3,4

X-NERC	

NISTIR Requirement	
NERC CIP	
Note that only the language from the requirement section of CIPv5 is included in this table.	
GENERAL NOTES	
Notes: CIP 9 compliance not required for LOW impact systems, whereas NISTIR has CP requirements for LOW systems	
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization	
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.CP NISTIR MAPPING**
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.CP NISTIR MAPPING**
CIP-003-5: Cyber Security — Security Management Controls	
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.CP NISTIR MAPPING**
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.CP NISTIR MAPPING**
R2, 1.1: Personnel Security	**NO SG.CP NISTIR MAPPING**
R2, 1.2: Electronic Security Parameters	**NO SG.CP NISTIR MAPPING**
R2, 1.3: Remote Access	**NO SG.CP NISTIR MAPPING**
R2, 1.4: Physical Security	**NO SG.CP NISTIR MAPPING**
R2, 1.5: System Security	**NO SG.CP NISTIR MAPPING**

R2, 1.6: Incident Response	**NO SG.CP NISTIR MAPPING**
R2, 1.7: Recovery Plans	
R2, 1.8: Configuration Change Management	**NO SG.CP NISTIR MAPPING**
R2, 1.9: Information Protection	**NO SG.CP NISTIR MAPPING**
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.CP NISTIR MAPPING**
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.CP NISTIR MAPPING**
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.CP NISTIR MAPPING**
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.CP NISTIR MAPPING**
CIP 004-5: Cyber Security – Personnel and Training	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.CP NISTIR MAPPING**
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.CP NISTIR MAPPING**
R2, 2.1: Define the roles that require training.	**NO SG.CP NISTIR MAPPING**

R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.CP NISTIR MAPPING**
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.CP NISTIR MAPPING**
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.CP NISTIR MAPPING**
R2, 2.5: Training on the visitor control program.	**NO SG.CP NISTIR MAPPING**
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.CP NISTIR MAPPING**
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.CP NISTIR MAPPING**
R2, 2.8: Training on recovery plans for BES Cyber Systems.	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.CP NISTIR MAPPING**
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.CP NISTIR MAPPING**
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.CP NISTIR MAPPING**
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.CP NISTIR MAPPING**
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.CP NISTIR MAPPING**
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.CP NISTIR MAPPING**
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.CP NISTIR MAPPING**

R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.CP NISTIR MAPPING**
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.CP NISTIR MAPPING**
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.CP NISTIR MAPPING**
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.CP NISTIR MAPPING**
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.CP NISTIR MAPPING**
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.CP NISTIR MAPPING**
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.CP NISTIR MAPPING**
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.CP NISTIR MAPPING**
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.CP NISTIR MAPPING**
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.CP NISTIR MAPPING**
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.CP NISTIR MAPPING**

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.CP NISTIR MAPPING**
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.CP NISTIR MAPPING**
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.CP NISTIR MAPPING**
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.CP NISTIR MAPPING**
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.CP NISTIR MAPPING**
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.CP NISTIR MAPPING**
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.CP NISTIR MAPPING**
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.CP NISTIR MAPPING**
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.CP NISTIR MAPPING**
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.CP NISTIR MAPPING**
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.CP NISTIR MAPPING**
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.CP NISTIR MAPPING**

R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.CP NISTIR MAPPING**
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.CP NISTIR MAPPING**
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.CP NISTIR MAPPING**
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.CP NISTIR MAPPING**
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems	
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.CP NISTIR MAPPING**
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.CP NISTIR MAPPING**
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.CP NISTIR MAPPING**
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.CP NISTIR MAPPING**
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.CP NISTIR MAPPING**
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.CP NISTIR MAPPING**
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.CP NISTIR MAPPING**
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.CP NISTIR MAPPING**
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.CP NISTIR MAPPING**

R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.CP NISTIR MAPPING**
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.CP NISTIR MAPPING**
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.CP NISTIR MAPPING**
CIP-007-5: Cyber Security-Systems Security Management	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.CP NISTIR MAPPING**
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.CP NISTIR MAPPING**
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.CP NISTIR MAPPING**
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.CP NISTIR MAPPING**
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.CP NISTIR MAPPING**
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.CP NISTIR MAPPING**
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.CP NISTIR MAPPING**
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.CP NISTIR MAPPING**
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.CP NISTIR MAPPING**
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.CP NISTIR MAPPING**
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.CP NISTIR MAPPING**

R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.CP NISTIR MAPPING**
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.CP NISTIR MAPPING**
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.CP NISTIR MAPPING**
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.CP NISTIR MAPPING**
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.CP NISTIR MAPPING**
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.CP NISTIR MAPPING**
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.CP NISTIR MAPPING**
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.CP NISTIR MAPPING**
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.CP NISTIR MAPPING**
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.CP NISTIR MAPPING**
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.CP NISTIR MAPPING**
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.CP NISTIR MAPPING**

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.CP NISTIR MAPPING**
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.CP NISTIR MAPPING**
CIP-008-5: Cyber Security-Incident Reporting and Response Planning	
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.CP NISTIR MAPPING**
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.CP NISTIR MAPPING**
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.CP NISTIR MAPPING**
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.CP NISTIR MAPPING**
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.CP NISTIR MAPPING**

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.CP NISTIR MAPPING**
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.CP NISTIR MAPPING**
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.CP NISTIR MAPPING**
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.CP NISTIR MAPPING**
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.CP NISTIR MAPPING**
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.CP NISTIR MAPPING**
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.CP NISTIR MAPPING**
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems	
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: Conditions for activation of the recovery plan(s).	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	

R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	

R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.CP NISTIR MAPPING**

R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.CP NISTIR MAPPING**
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.CP NISTIR MAPPING**
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.CP NISTIR MAPPING**
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.CP NISTIR MAPPING**
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.CP NISTIR MAPPING**
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.CP NISTIR MAPPING**
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.CP NISTIR MAPPING**
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.CP NISTIR MAPPING**

R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.CP NISTIR MAPPING**
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.CP NISTIR MAPPING**
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.CP NISTIR MAPPING**
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.CP NISTIR MAPPING**
CIP-011-1: Cyber Security-Information Protection	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.CP NISTIR MAPPING**
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.CP NISTIR MAPPING**
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.CP NISTIR MAPPING**
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.CP NISTIR MAPPING**
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.CP NISTIR MAPPING**
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.CP NISTIR MAPPING**
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.CP NISTIR MAPPING**

SG.CP-1	SG.CP-2	SG.CP-3	SG.CP-4
Continuity of Operations Policy and Procedures	Continuity of Operations Plan	Continuity of Operations Roles and Responsibilities	Continuity of Operations Training

3 - NISTIR requirement is more granular. - CIP requirement does not specify required elements of recovery plan (in CIP-003-5)	3 - NISTIR requirement is more granular. - CIP requirement does not specify required elements of recovery plan (in CIP-003-5)		

			2 - CIP requirement is more granular with training requirement and frequency for all individuals authorized for access to critical cyber assets - NISTIR does not specify personnel required and leaves frequency as "organization-defined"

2 - CIP requirement is more granular with requiring specific conditions	2 - CIP requirement is more granular with requiring specific conditions		
2 - CIP requirement is more granular with specific information on roles and responsibilities required	2 - CIP requirement is more granular with specific information on roles and responsibilities required	1 - Exact match in requirement between NISTIR and NERC CIP v5	

2 - CIP requirement is more granular with requirements for backup, storage and protection	2 - CIP requirement is more granular with requirements for backup, storage and protection		
2 - CIP requirement is more granular with requirements to preserve data of event that required continuity plan execution			
2 - CIP requirement is more granular with specific time requirements - NISTIR states frequency as an "organization-defined frequency"			
			2 - CIP requirement is more granular with specific time requirements for tabletop "testing" or "training" - NISTIR states frequency as an "organization-defined frequency"

	2 - CIP requirement is more granular with specific time requirements - NISTIR does not have review frequency in CP-2		
	2 - CIP requirement is more granular with specific time requirements - NISTIR does not have review frequency in CP-2		
	2 - CIP requirement is more granular with specific time requirements - NISTIR does not have review frequency in CP-2		
	2 - CIP requirement is more granular with specific time requirements - NISTIR does not have review frequency in CP-2		
	2 - CIP requirement is more granular with specific time requirements - NISTIR does not have review frequency in CP-2	2 - CIP requirement is more granular with responsibility to communicate changes to all responsible individuals	2 - CIP requirement is more granular with responsibility to communicate changes to plan (indirect training requirement) to appropriate personnel

SG.CP-5	SG.CP-6	SG.CP-7	SG.CP-8
Continuity of Operations Plan Testing	Continuity of Operations Plan Update	Alternate Storage Sites	Alternate Telecommunication Services
			NO DIRECT MAPPING

	2 - CIP requirement is more granular with specific update requirements and approvals - NISTIR uses an "organization-defined frequency"		

2 - CIP requirement is more granular with specific time requirements - NISTIR states testing frequency as an "organization-defined frequency"			

		3 - NISTIR requirement is more granular - CIP requirement does not specify alternate storage sites	
2 - CIP requirement is more granular with backup verification requirements		3 - NISTIR requirement is more granular - CIP requirement does not specify alternate storage sites	
		3 - NISTIR requirement is more granular - CIP requirement does not specify alternate storage sites	
2 - CIP requirement is more granular with specific time requirements - NISTIR states testing frequency as an "organization-defined frequency"			
2 - CIP requirement is more granular with specific time requirements - NISTIR states testing frequency as an "organization-defined frequency"			
2 - CIP requirement is more granular with specific time requirements - NISTIR states testing frequency as an "organization-defined frequency"			

2 - CIP requirement is more granular with specific review requirements with lessons learned - NISTIR states corrective actions should be initiated if necessary	2 - CIP requirement is more granular with specific review requirements with lessons learned - NISTIR uses an "organization-defined frequency"		
2 - CIP requirement is more granular with specific review requirements with lessons learned - NISTIR states corrective actions should be initiated if necessary			
2 - CIP requirement is more granular with specific review requirements with lessons learned - NISTIR states corrective actions should be initiated if necessary	2 - CIP requirement is more granular with specific update requirements with lessons learned - NISTIR uses an "organization-defined frequency"		
	2 - CIP requirement is more granular with specific update requirements		
2 - CIP requirement is more granular with responsibility to communicate changes to plan to appropriate personnel	2 - CIP requirement is more granular with responsibility to communicate changes to plan to appropriate personnel - NISTIR includes this in supplemental guidance		

SG.CP-9	SG.CP-10	SG.CP-11
Alternate Control Center	Smart Grid Information System Recovery and Reconstitution	Fail-Safe Response
NO DIRECT MAPPING		**NO DIRECT MAPPING**

	3 - NISTIR requirement is more granular with requirements to recover/reconstitute SG systems to secure state	
	3 - NISTIR requirement is more granular with requirements to recover/reconstitute SG systems to secure state	
	3 - NISTIR requirement is more granular with requirements to recover/reconstitute SG systems to secure state	
	3 - NISTIR requirement is more granular with requirements to recover/reconstitute SG systems to secure state	
	3 - NISTIR requirement is more granular with requirements to recover/reconstitute SG systems to secure state	
	3 - NISTIR requirement is more granular with requirements to recover/reconstitute SG systems to secure state	

NISTIR Requirement		SG.IA-1
NERC CIP		Identification and Authentication Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.IA NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.IA NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.IA NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.IA NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.IA NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.IA NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.IA NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.IA NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.IA NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.IA NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.IA NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.IA NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.IA NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.IA NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.IA NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.IA NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.IA NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.IA NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.IA NISTIR MAPPING**	

R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.IA NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.IA NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.IA NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.IA NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.IA NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.IA NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.IA NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.IA NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.IA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.IA NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.IA NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.IA NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.IA NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.IA NISTIR MAPPING**	

R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.IA NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.IA NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.IA NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.IA NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.IA NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.IA NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.IA NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.IA NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.IA NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.IA NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.IA NISTIR MAPPING**	

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.IA NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.IA NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.IA NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.IA NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.IA NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.IA NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.IA NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.IA NISTIR MAPPING**	

R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.		2 - CIP requirement is more granular to direct definition of controls to restrict unauthorized access to critical cyber assets - NISTIR only states to address the implementation of the identification and authentication security policy and associated identification and authentication protection requirements.
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).		2 - CIP requirement is more granular to direct definition of controls through electronic access points - NISTIR only states to address the implementation of the identification and authentication security policy and associated identification and authentication protection requirements.

R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.		2 - CIP requirement is more granular to require explicit inbound/outbound access permissions at each point
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.		2 - CIP requirement is more granular to address dial-up access - NISTIR does not specifically mention dial-up access
R1, 1.5: A documented method for detecting malicious communications at each EAP.		
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.		2 - CIP requirement is more granular with remote access requirements - NISTIR does not specifically discuss remote access

R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.		
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.IA NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.IA NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.IA NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.IA NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.IA NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.IA NISTIR MAPPING**	

R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.IA NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.IA NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.IA NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.IA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.IA NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.IA NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.IA NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.IA NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.IA NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.IA NISTIR MAPPING**	

R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.IA NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.IA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.IA NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.IA NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.IA NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.IA NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.IA NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.IA NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.IA NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.IA NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.IA NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.IA NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.IA NISTIR MAPPING**	

R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.IA NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.IA NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.		
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.IA NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.		
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.IA NISTIR MAPPING**	

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.IA NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.		
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.IA NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.IA NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.IA NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.IA NISTIR MAPPING**	

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.IA NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.IA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.IA NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.IA NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.IA NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.IA NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.IA NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.IA NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.IA NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.IA NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.IA NISTIR MAPPING**	

R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.IA NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.IA NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.IA NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.IA NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.IA NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.IA NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.IA NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.IA NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.IA NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.IA NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.IA NISTIR MAPPING**	

CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.IA NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.IA NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.IA NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.IA NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.IA NISTIR MAPPING**	

R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.IA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.IA NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.IA NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.IA NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.IA NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.IA NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.IA NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.IA NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.IA NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.IA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.IA NISTIR MAPPING**	

R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.IA NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.IA NISTIR MAPPING**	

SG.IA-2	SG.IA-3	SG.IA-4	SG.IA-5
Identifier Management	Authenticator Management	User Identification and Authentication	Device Identification and Authentication
NO CIP MAPPING			

	3 - NISTIR is more granular through specific authentication credential management requirements (initial authentication credential content; administrative procedures for initial authentication credential distribution/lost credentials/lost, compromised, or damaged authentication credentials/revoking authentication credentials; changing/refreshing authentication credentials on an organization-defined frequency; and specifying measures to safeguard authentication credentials).	2 - CIP requirement is more granular for access requirements at electronic access points	3 - NISTIR is specific for all devices to be identified and authenticated before establishing a connection - whereas the CIP requirement identifies and controls established access points/critical cyber assets but does not specifically all devices to be identified/authenticated (only "users")

		2 - CIP requirement is more granular for specific inbound/outbound access	3 - NISTIR is specific for all devices to be identified and authenticated before establishing a connection - whereas the CIP requirement identifies and controls established access points/critical cyber assets but does not specify all devices to be identified/authenticated (only "users")
		1 - CIP and NISTIR both require authentication, but NISTIR does not specifically mention dial-up connectivity	1 - CIP and NISTIR both require authentication, but NISTIR does not specifically mention dial-up connectivity
	2 - CIP requirement is more granular to document potential malicious communications - NISTIR only provides additional consideration to employ automated tools to determine if credentials can resist attack (malicious communications)		
			2 - CIP is more granular to require multi-factor authentication for remote access

			2 - CIP is more granular to require multi-factor authentication for remote access
			1 - Both CIP and NISTIR require encryption for remote access connections (both require this for MED and HIGH systems)
		2 - CIP is more granular to require multi-factor authentication for remote access, whereas NISTIR recommends multi-factor authentication for remote access to non-privileged and privileged accounts as additional considerations.	

		1	3 - NISTIR is specific for all devices to be identified and authenticated before establishing a connection - whereas the CIP requirement validates credentials but does not specify all devices to be identified/authenticated (only "users")
	3- NISTIR is more specific on requirements for managing authentication credentials for users/devices, including supplemental guidance to safeguard credentials by not loaning/sharing credentials (each individual must be identified for any shared account as opposed to sharing credentials)	1 - CIP and NISTIR are similar, although NISTIR does not specifically address "shared accounts" in IA set (stating that all users or processes are uniquely identified and authenticated)	

SG.IA-6
Authenticator Feedback
NO CIP MAPPING

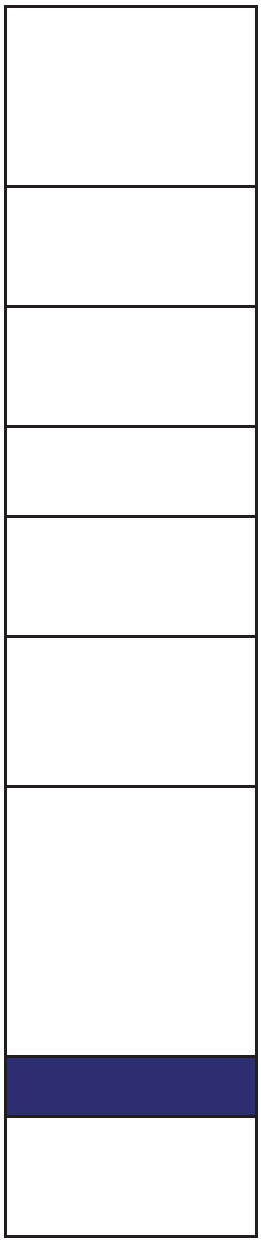

(NOTE: some similarity to NISTIR IA-6 which requires authentication mechanism to "obscure feedback of authentication information" to help protect information. CIP-005 requires an intermediate device to protect assets)

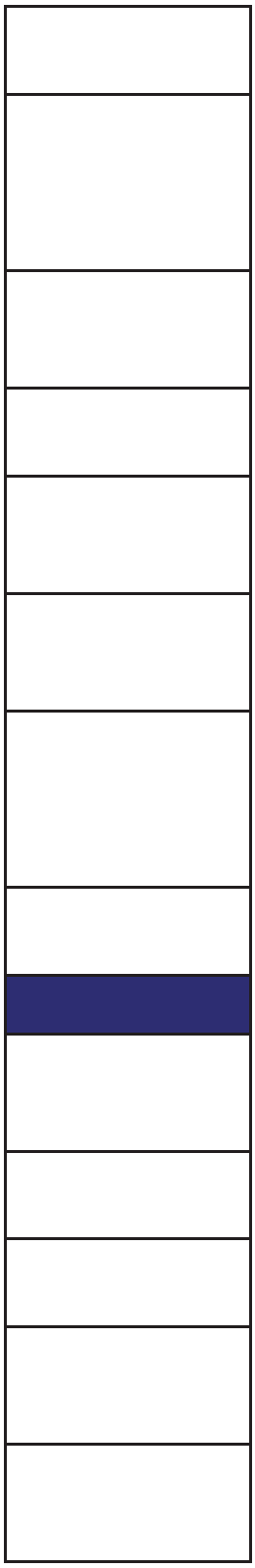

difficult to map – different detailed aspects of issue addressed

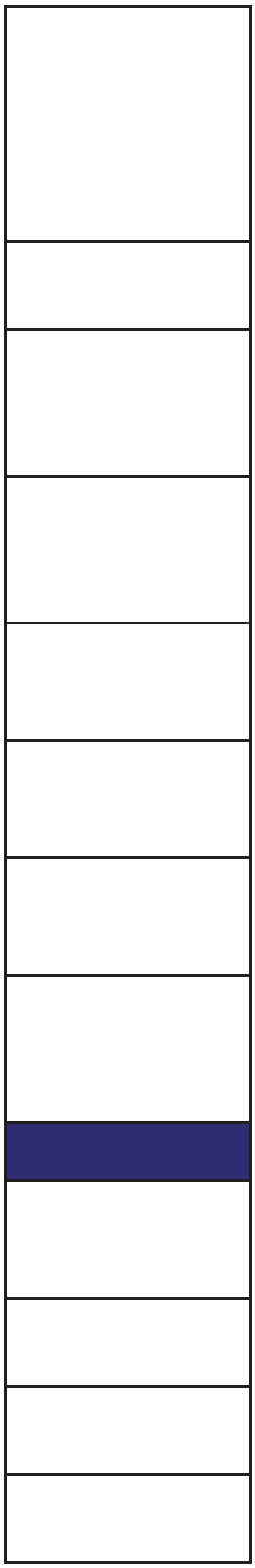

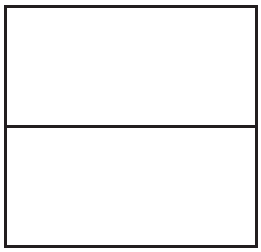

NISTIR Requirement		SG.ID-1
NERC CIP		Information and Document Management Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
GENERAL NOTES		
Notes: none of CIP-11 is applicable to LOW impact systems under CIP standards, whereas NISTIR recommends measures for LOW		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.ID NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.ID NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.ID NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.ID NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.ID NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.ID NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.ID NISTIR MAPPING**	

R2, 1.4: Physical Security	**NO SG.ID NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.ID NISTIR MAPPING**	
R2, 1.6: Incident Response	**NO SG.ID NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.ID NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.ID NISTIR MAPPING**	
R2, 1.9: Information Protection		3 - NISTIR requirement is more granular - CIP requirement does not specify required elements of information protection in CIP-003-5, but does in CIP-11
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.ID NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.ID NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.ID NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.ID NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.ID NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.ID NISTIR MAPPING**	

R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.ID NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.ID NISTIR MAPPING**	
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.ID NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.ID NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.ID NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.ID NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.ID NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.ID NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.ID NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.ID NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.ID NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.ID NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.ID NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.ID NISTIR MAPPING**	

R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.ID NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.ID NISTIR MAPPING**	
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.ID NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.ID NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.ID NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.ID NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.ID NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.ID NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.ID NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.ID NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.ID NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.ID NISTIR MAPPING**	

R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.ID NISTIR MAPPING**	
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.ID NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.ID NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.ID NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.ID NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.ID NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.ID NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.ID NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.ID NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.ID NISTIR MAPPING**	

R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.ID NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.ID NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.ID NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.ID NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.ID NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.ID NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.ID NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.ID NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.ID NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.ID NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.ID NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.ID NISTIR MAPPING**	

R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.ID NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.ID NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.ID NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.ID NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.ID NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.ID NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.ID NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.ID NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.ID NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.ID NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.ID NISTIR MAPPING**	

R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.ID NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.ID NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.ID NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.ID NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.ID NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.ID NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.ID NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.ID NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.ID NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.ID NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.ID NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.ID NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.ID NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.ID NISTIR MAPPING**	

R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.ID NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.ID NISTIR MAPPING**	
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.ID NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.ID NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.ID NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.ID NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.ID NISTIR MAPPING**	

R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.ID NISTIR MAPPING**	
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.ID NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.ID NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.ID NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.ID NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.ID NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.ID NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.ID NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.ID NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.ID NISTIR MAPPING**	

R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.ID NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.ID NISTIR MAPPING**	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.ID NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.ID NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.ID NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.ID NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.ID NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.ID NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.ID NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.ID NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.ID NISTIR MAPPING**	

R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.ID NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.ID NISTIR MAPPING**	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.ID NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.ID NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.ID NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.ID NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.ID NISTIR MAPPING**	

R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.ID NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.ID NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.ID NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.ID NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.ID NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.ID NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.ID NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.		

R1, 1.2: Access control and handling procedures for BES Cyber System Information.		
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.ID NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.ID NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.ID NISTIR MAPPING**	

SG.ID-2	SG.ID-3	SG.ID-4	SG.ID-5
Information and Document Retention	Information Handling	Information Exchange	Automated Labeling
		NO DIRECT MAPPING	**CIP standards do not require "automatic" labeling**

	2 - CIP requirement is more granular with handling requirements		3 - NISTIR requirement is more granular and requires "automatic" labeling - CIP requirement including labeling as evidence of indications on information (automatic labeling is not a requirement)

3 - NISTIR requirement is more granular with retention requirements as applicable to law/regulations - CIP requirement focuses only on controlling access to retained documents (no specific retention requirements)	2 - CIP requirement is more granular with handling requirements		3 - NISTIR requirement is more granular and requires "automatic" labeling - CIP requirement including labeling as evidence of indications on information (automatic labeling is not a requirement)
	2 - CIP requirement is more granular with specific time requirements - NISTIR states review frequency as an "organization-defined frequency"		

NISTIR Requirement		SG.IR-1
NERC CIP		Incident Response Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.IR NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.IR NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.IR NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.IR NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.IR NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.IR NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.IR NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.IR NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.IR NISTIR MAPPING**	

R2, 1.6: Incident Response		3 - NISTIR requirement is more granular - NISTIR specifies details on what the policy should address including objectives, roles and responsibilities, and the scope of the incident response program. The NISTIR also requires the identification and classifications of potential interruptions.
R2, 1.7: Recovery Plans	**NO SG.IR NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.IR NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.IR NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.IR NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.IR NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.IR NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.IR NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.IR NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.IR NISTIR MAPPING**	

R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.IR NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.IR NISTIR MAPPING**	
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.IR NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.IR NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.IR NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.IR NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.IR NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.		
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.IR NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.		
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.IR NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.IR NISTIR MAPPING**	

R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.IR NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.IR NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.IR NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.IR NISTIR MAPPING**	
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.IR NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.IR NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.IR NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.IR NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.IR NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.IR NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.IR NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.IR NISTIR MAPPING**	

R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.IR NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.IR NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.IR NISTIR MAPPING**	
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.IR NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.IR NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.IR NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.IR NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.IR NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.IR NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.IR NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.IR NISTIR MAPPING**	

R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.IR NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.IR NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.IR NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.IR NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.IR NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.IR NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.IR NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.IR NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.IR NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.IR NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.IR NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.IR NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.IR NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.IR NISTIR MAPPING**	

R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.IR NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.IR NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.IR NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.IR NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.IR NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.IR NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.IR NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.IR NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.IR NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.IR NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.IR NISTIR MAPPING**	

R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.IR NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.IR NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.IR NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.IR NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.IR NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.IR NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.IR NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.IR NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.		
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.		
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.IR NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.IR NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.IR NISTIR MAPPING**	

R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.IR NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.IR NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.IR NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.IR NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.IR NISTIR MAPPING**	
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.IR NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.IR NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.IR NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.		1 - NISTIR and CIP requirements have similar granularity.
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.		1 - NISTIR and CIP requirements have similar granularity.

R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.		
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.IR NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.		1 - NISTIR and CIP requirements have similar granularity.
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.		
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.IR NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.		2 - CIP requirement is more granular - CIP specifies time frame for review of the IR plan for accuracy and completeness.

R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.		
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.		
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.IR NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.		2 - CIP requirement is more granular - CIP specifies a time frame for communicating IR plan updates to each person with a defined role in the plan.
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.		
R1, 1.1: Conditions for activation of the recovery plan(s).		
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.		
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.		
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.		
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.IR NISTIR MAPPING**	

R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.IR NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.IR NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.IR NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.IR NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.IR NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.IR NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.IR NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.IR NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.IR NISTIR MAPPING**	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.IR NISTIR MAPPING**	

R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.IR NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.IR NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.IR NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.IR NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.IR NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.IR NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.IR NISTIR MAPPING**	

R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.IR NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.IR NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.IR NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.IR NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.IR NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.IR NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.IR NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.IR NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.IR NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.IR NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.IR NISTIR MAPPING**	

SG.IR-2	SG.IR-3	SG.IR-4	SG.IR-5
Incident Response Roles and Responsibilities	Incident Response Training	Incident Response Testing and Exercises	Incident Handling

	3 - NISTIR requirement is more granular - NISTIR specifies that refresher training should be received on an organization-defined basis.		
	3 - NISTIR requirement is more granular - NISTIR specifies training on roles and responsibilities.		

			1 - NISTIR and CIP requirements have similar granularity.

1 - NISTIR and CIP requirements have similar granularity.			1 - NISTIR and CIP requirements have similar granularity.
			2 - CIP requirement is more granular - CIP specifies that deviations taken from the plan during the incident or test are recorded.
		2 - CIP requirement is more granular - CIP specifies testing frequency requirements and the types of testing that are acceptable.	
			2 - CIP requirement is more granular - CIP specifies document retention time.

		2 - CIP requirement is more granular - CIP specifies time frame for documenting lessons learned from exercise of the response plan.	2 - CIP requirement is more granular - CIP specifies time frame for review and documentation of any exercise of the IR plan.
			2 - CIP requirement is more granular - CIP specifies time frame for updating IR plan after completion of a review.

SG.IR-6	SG.IR-7	SG.IR-8	SG.IR-9
Incident Monitoring	Incident Reporting	Incident Response Investigation and Analysis	Corrective Action
			NO CIP MAPPING

2 - CIP requirement is more granular - CIP specifies the activities that must be logged and tracked.			
3 - NISTIR requirement is more granular - NISTIR specifies that an automated mechanisms be used.			

	1 - NISTIR and CIP requirements have similar granularity.		

	3 - NISTIR requirement is more granular - NISTIR specifies that data is reported in compliance with applicable laws and regulations.		
3 - NISTIR requirement is more granular - NISTIR specifies that an automated mechanisms be used.			
	2 - CIP requirement is more granular - CIP specifies retention (including retention time) for reportable incident documentation.	3 - NISTIR requirement is more granular - NISTIR outlines specific steps to be taken to analyze an incident response investigation.	

SG.IR-10	SG.IR-11
Smart Grid Information System Backup	Coordination of Emergency Response

	3 - NISTIR requirement is more granular - NISTIR specifies (but does not limit) external entities that should be considered for not only communication but coordinated effort related to cyber security incidents.

3 - NISTIR requirement is more granular - NISTIR provides specifics on the information to be backed up.	
2 - CIP requirement is more granular - CIP specifies the frequency of verification	

NISTIR Requirement		SG.MA-1
NERC CIP		Smart Grid Information System Maintenance Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.MA NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.MA NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.MA NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.MA NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.MA NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.MA NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.MA NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.MA NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.MA NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.MA NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.MA NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.MA NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.MA NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.MA NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.MA NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.MA NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.MA NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.MA NISTIR MAPPING**	

R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.MA NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.MA NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.MA NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.MA NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.MA NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.MA NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.MA NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.MA NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.MA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.MA NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.MA NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.MA NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.MA NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.MA NISTIR MAPPING**	

R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.MA NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.MA NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.MA NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.MA NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.MA NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.MA NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.MA NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.MA NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.MA NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.MA NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.MA NISTIR MAPPING**	

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.MA NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.MA NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.MA NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.MA NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.MA NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.MA NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.MA NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.MA NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.MA NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.MA NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.MA NISTIR MAPPING**	

R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.MA NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.MA NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.MA NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.MA NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.MA NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.MA NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.MA NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.MA NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.MA NISTIR MAPPING**	

R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.MA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.MA NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.MA NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.MA NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.MA NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.		4 - CIP defines the specific need for patching policy while NISTIR is a universal policy
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.		

R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.		4 - CIP defines the specific need for patching policy while NISTIR is a universal policy
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.MA NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.MA NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.MA NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.MA NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.MA NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.MA NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.MA NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.MA NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.MA NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.MA NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.MA NISTIR MAPPING**	

R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.MA NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.MA NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.MA NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.MA NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.MA NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.MA NISTIR MAPPING**	
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.MA NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.MA NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.MA NISTIR MAPPING**	

R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.MA NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.MA NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.MA NISTIR MAPPING**	
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.MA NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.MA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.MA NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.MA NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.MA NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.MA NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.MA NISTIR MAPPING**	

R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.MA NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.MA NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.MA NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.MA NISTIR MAPPING**	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.MA NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.MA NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.MA NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.MA NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.MA NISTIR MAPPING**	

R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.MA NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.MA NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.MA NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.MA NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.MA NISTIR MAPPING**	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.MA NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.MA NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.MA NISTIR MAPPING**	

R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.MA NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.MA NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.MA NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.MA NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.MA NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.MA NISTIR MAPPING**	

R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.MA NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.MA NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.MA NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.MA NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.MA NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.MA NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.MA NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.MA NISTIR MAPPING**	

SG.MA-2	SG.MA-3	SG.MA-4	SG.MA-5
Legacy Smart Grid Information System Updates	Smart Grid Information System Maintenance	Maintenance Tools	Maintenance Personnel
		NO NERC CIP MAPPING	**NO NERC CIP MAPPING**

4 - CIP is more specific on Patching while NISTIR is general about all updates.	X- NISTIR is more detailed but includes all maintenance not just patching also includes testing and backups before maintenance is preformed.		
4 - CIP is more specific on Patching while NISTIR is general about all updates.	X- NISTIR is more detailed but includes all maintenance not just patching also includes testing and backups before maintenance is preformed.		

4 - CIP is more specific on Patching while NISTIR is general about all updates.	X- NISTIR is more detailed but includes all maintenance not just patching also includes testing and backups before maintenance is preformed.		

SG.MA-6	SG.MA-7
Remote Maintenance	Timely Maintenance
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**

NISTIR Requirement		SG.MP-1
NERC CIP		Media Protection Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.MP NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.MP NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.MP NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.MP NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.MP NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.MP NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.MP NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.MP NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.MP NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.MP NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.MP NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.MP NISTIR MAPPING**	
R2, 1.9: Information Protection		3 - NISTIR is more detailed including what to address under media protection policy.
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.MP NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.MP NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.MP NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.MP NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.MP NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.MP NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.MP NISTIR MAPPING**	

R2, 2.1: Define the roles that require training.	**NO SG.MP NISTIR MAPPING**	
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.MP NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.MP NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.MP NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.MP NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.MP NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.MP NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.MP NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.MP NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.MP NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.MP NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.MP NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.MP NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.MP NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.MP NISTIR MAPPING**	

R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.MP NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.MP NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.MP NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.MP NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.MP NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.MP NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.MP NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.MP NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.MP NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.MP NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.MP NISTIR MAPPING**	

R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.MP NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.MP NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.MP NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.MP NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.MP NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.MP NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.MP NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.MP NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.MP NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.MP NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.MP NISTIR MAPPING**	

R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.MP NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.MP NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.MP NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.MP NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.MP NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.MP NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.MP NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.MP NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.MP NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.MP NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.MP NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.MP NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.MP NISTIR MAPPING**	

R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.MP NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.MP NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.MP NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.MP NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.MP NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.MP NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.MP NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.MP NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.MP NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.MP NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.MP NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.MP NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.MP NISTIR MAPPING**	

R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.MP NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.MP NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.MP NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.MP NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.MP NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.MP NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.MP NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.MP NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.MP NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.MP NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.MP NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.MP NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.MP NISTIR MAPPING**	

R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.MP NISTIR MAPPING**	
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.MP NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.MP NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.MP NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.MP NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.MP NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.MP NISTIR MAPPING**	

R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.MP NISTIR MAPPING**	
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.MP NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.MP NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.MP NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.MP NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.MP NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.MP NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.MP NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.MP NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.MP NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.MP NISTIR MAPPING**	

R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.MP NISTIR MAPPING**	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.MP NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.MP NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.MP NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.MP NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.MP NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.MP NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.MP NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.MP NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.MP NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.MP NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.MP NISTIR MAPPING**	

R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.MP NISTIR MAPPING**	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.MP NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.MP NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.MP NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.MP NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.MP NISTIR MAPPING**	

R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.MP NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.MP NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.MP NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.MP NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.MP NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.MP NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.MP NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.MP NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.MP NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.MP NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.MP NISTIR MAPPING**	

R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.MP NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		4 - CIP specifies that all media must follow a process so that the media can not be retrieved by unauthorized users, NISTIR is a general policy that can but may not include this.
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		4 - CIP specifies that all media must follow a process so that the media can not be retrieved by unauthorized users, NISTIR is a general policy that can but may not include this.

SG.MP-2	SG.MP-3	SG.MP-4	SG.MP-5
Media Sensitivity Level	Media Marketing	Media Storage	Media Transport
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**

SG.MP-6
Media Sanitization and Disposal

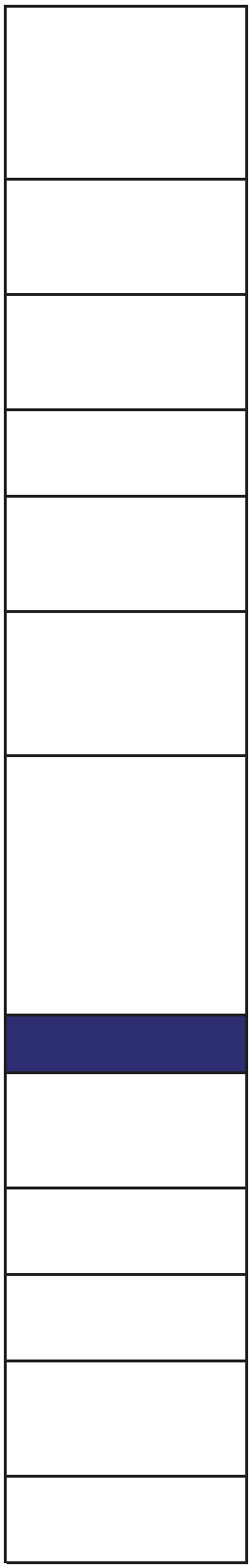

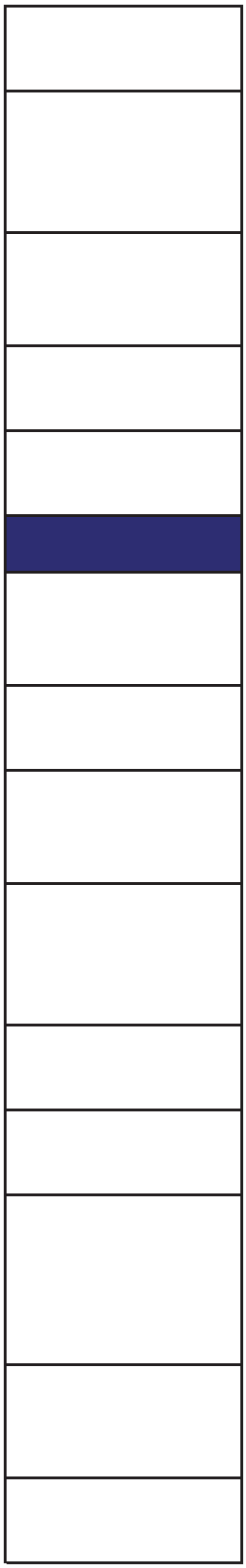

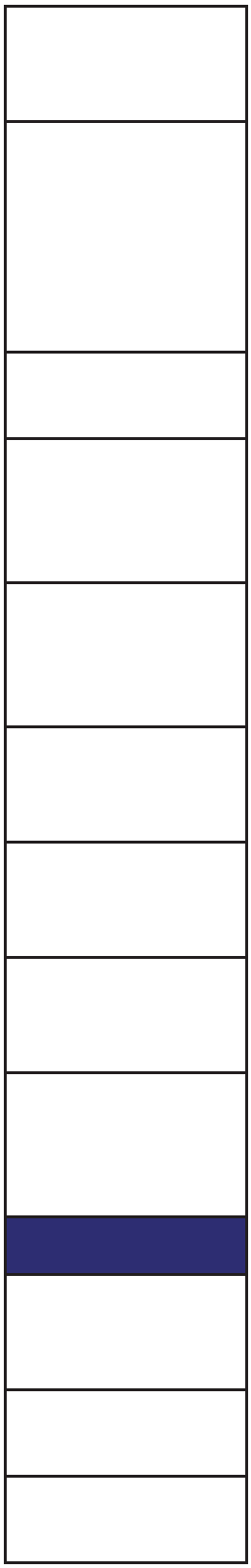

3 - NISTIR requires that no retrieval is possible even authorized before resuse or disposal. Also NISTIR requires the sanitization equipment be tested on a defined frequency
3 - NISTIR requires that no retrieval is possible even authorized before resuse or disposal. Also NISTIR requires the sanitization equipment be tested on a defined frequency

NISTIR Requirement		SG.PE-1
NERC CIP		Physical and Environmental Security Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.		4 - BES Cyber System Identification includes physical access control security configuration, floor plans, equipment layouts, disaster recovery and incident response plans. This satisfies the requirement for a "physical and environmental security policy" from the SG.PE-1
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.PE NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.PE NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.PE NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.PE NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.PE NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.PE NISTIR MAPPING**	

R2, 1.3: Remote Access	**NO SG.PE NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.PE NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.PE NISTIR MAPPING**	
R2, 1.6: Incident Response	**NO SG.PE NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.PE NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.PE NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.PE NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.PE NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.PE NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.PE NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.PE NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.PE NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.PE NISTIR MAPPING**	

R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.PE NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.PE NISTIR MAPPING**	
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PE NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PE NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.PE NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.PE NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.PE NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.PE NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.PE NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.PE NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.PE NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.PE NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.PE NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.PE NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.PE NISTIR MAPPING**	

R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.PE NISTIR MAPPING**	
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.PE NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.PE NISTIR MAPPING**	
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.PE NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.PE NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.PE NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.PE NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PE NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PE NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PE NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.PE NISTIR MAPPING**	

R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.		
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.		
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.PE NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.PE NISTIR MAPPING**	
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.PE NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.PE NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.PE NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.PE NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.PE NISTIR MAPPING**	

R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.PE NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.PE NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.PE NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.PE NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.PE NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.PE NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.PE NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.PE NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.		1 - Basically a direct match, though SG.PE-1 is more verbose about definitions.
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.		4 - This requirement provides details of the required physical and environmental security policy and procedures.
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.		4 - This requirement provides details of the required physical and environmental security policy and procedures.

R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.		
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.		
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.		
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.		4 - CIP specifies details of a physical access security system, as an instance of the type of policy required by the NISTIR.
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.		4 - CIP specifies details of a physical access security system, as an instance of the type of policy required by the NISTIR.
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.		
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.PE NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.PE NISTIR MAPPING**	

R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.PE NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.PE NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.PE NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.PE NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.PE NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.PE NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.PE NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.PE NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.PE NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.PE NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.PE NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.PE NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.PE NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.PE NISTIR MAPPING**	

R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.PE NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.PE NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.PE NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.PE NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.PE NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.PE NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.PE NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.PE NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.PE NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.PE NISTIR MAPPING**	

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.PE NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.PE NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.PE NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.PE NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.PE NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.PE NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.PE NISTIR MAPPING**	

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.PE NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.PE NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.PE NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.PE NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.PE NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.PE NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.PE NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.PE NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.PE NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.PE NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.PE NISTIR MAPPING**	

R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.PE NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.PE NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.PE NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.PE NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.PE NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.PE NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.PE NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.PE NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.PE NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.PE NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.PE NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.PE NISTIR MAPPING**	

CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.PE NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.PE NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.PE NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.PE NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PE NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.PE NISTIR MAPPING**	

R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.PE NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.PE NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.PE NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PE NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.PE NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.PE NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.PE NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.PE NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.PE NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.PE NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.PE NISTIR MAPPING**	

R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PE NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PE NISTIR MAPPING**	

SG.PE-2	SG.PE-3	SG.PE-4	SG.PE-5
Physical Access Authorizations	Physical Access	Monitoring Physical Access	Visitor Control
	NO NERC CIP MAPPING		

3 - CIP should be clear this includes physical access privileges. Also recommend NISTIR include an explicit section on access revocations.			
3 - CIP should be clear this includes physical access privileges. Also recommend NISTIR include an explicit section on access revocations.			

X	X		
	X		
	X		

		NISTIR is more detailed in what is required to be monitored, but CIP is more specific in requiring a real-time alert. Recommend NISTIR adopt the "unauthorized physical access" rather than "physical security incident".	
		NISTIR is more detailed in what is required to be monitored, but CIP is more specific in requiring a real-time alert.	
		2 - NIST simply says "monitor physical access" while CIP specifies that identity and time of entry are required fields.	
			4 - CIP specifies details of a physical access security system, as an instance of the type of policy required by the NISTIR.
			2 - CIP requires escort, while NISTIR considers that a requirements enhancement.

SG.PE-6	SG.PE-7	SG.PE-8	SG.PE-9
Visitor Records	Physical Access Log Retention	Emergency Shutoff Protection	Emergency Power
	NO NERC CIP MAPPING	**NO NERC CIP MAPPING**	

4 - CIP specifies details of a physical access security system, as an instance of the type of policy required by the NISTIR.			
2 - CIP provides further detail of what should be captured during visitor logging			

SG.PE-10	SG.PE-11	SG.PE-12
Delivery and Removal	Alternate Work Site	Location of Smart Grid Information System Assets
		4 - BES Cyber Asset Identification is defined to include physical location of logical assets.

		X

NISTIR Requirement		SG.PL-1
NERC CIP		Strategic Planning Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		**NO NERC CIP MAPPING**
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.PL NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.PL NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.PL NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.		
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:		
R2, 1.1: Personnel Security		
R2, 1.2: Electronic Security Parameters		
R2, 1.3: Remote Access		
R2, 1.4: Physical Security		

R2, 1.5: System Security		
R2, 1.6: Incident Response		
R2, 1.7: Recovery Plans		
R2, 1.8: Configuration Change Management		
R2, 1.9: Information Protection		
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances		
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.PL NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.		
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.PL NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.PL NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.PL NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.		
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.		
R2, 2.1: Define the roles that require training.	**NO SG.PL NISTIR MAPPING**	
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PL NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PL NISTIR MAPPING**	

R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.PL NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.PL NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.PL NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.PL NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.PL NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.PL NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.PL NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.PL NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.PL NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.PL NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.		
R4, 4.1: An initial personnel risk assessment that includes identity verification.		
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.		
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.		

R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.		
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.		
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.		
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.PL NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PL NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PL NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PL NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.PL NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.PL NISTIR MAPPING**	
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.PL NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.PL NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.		

R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.PL NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.		
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.		
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.		
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.PL NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.PL NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.PL NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.PL NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.PL NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.PL NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.PL NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.PL NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.PL NISTIR MAPPING**	

R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.PL NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.PL NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.PL NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.PL NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.PL NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.PL NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.PL NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.PL NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.PL NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.PL NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.PL NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.PL NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.PL NISTIR MAPPING**	

R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.PL NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.PL NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.PL NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.PL NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.PL NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.PL NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.PL NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.PL NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.PL NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.PL NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.PL NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.PL NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.PL NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.PL NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.PL NISTIR MAPPING**	

R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.PL NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.PL NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.PL NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.PL NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.PL NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.PL NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.PL NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.PL NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.PL NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.PL NISTIR MAPPING**	

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.PL NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.PL NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.		
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.PL NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.PL NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.PL NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.PL NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.PL NISTIR MAPPING**	

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.PL NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.PL NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.PL NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.PL NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.PL NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.PL NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.PL NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.PL NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.		
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.PL NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.PL NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.PL NISTIR MAPPING**	

R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.PL NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.PL NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.PL NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.PL NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.PL NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.PL NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.PL NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.PL NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.PL NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.PL NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.PL NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.PL NISTIR MAPPING**	

CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.PL NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.PL NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.PL NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.PL NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.PL NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PL NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.PL NISTIR MAPPING**	

R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.PL NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.PL NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.PL NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PL NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.PL NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.PL NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.PL NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.PL NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.PL NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.PL NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.PL NISTIR MAPPING**	

R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PL NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PL NISTIR MAPPING**	

SG.PL-2	SG.PL-3	SG.PL-4	SG.PL-5
Smart Grid Information System Security Plan	Rules of Behavior	Privacy Impact Assessment	Security-Related Activity Planning
			NO NERC CIP MAPPING
2 - CIP's Senior Manager has much more explicit responsibilities than the vague "management" and "the organization" in NERC			
2 - CIP's cyber security policy is an example of an information system security plan, and includes a number of specific topics, especially in the guidelines and technical basis section.			
2			
2			
2			
2			

2			
2			
2			
2			
2			
2			
	1(approx) (gap in initial mapping)		
	uncertain if this is a gap		
	uncertain if this is a gap		

		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	

		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	

		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	
		Privacy implications unaddressed in other CIP requirements	

			uncertain if this is a gap

			uncertain if this is a gap

NISTIR Requirement		SG.PM-1
NERC CIP		Security Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.		SGIP should include following Requirement from CIP-002-5R1:Organizations shall identify and categorize High and Medium impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.

R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.		SGIP shall include following requirement from CIP-002-5 R1.1 to Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.PM NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.PM NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.PM NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.PM NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.PM NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.PM NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.PM NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.PM NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.PM NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.PM NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.PM NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.PM NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.PM NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.		
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.PM NISTIR MAPPING**	

R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.		
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.PM NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.PM NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.PM NISTIR MAPPING**	
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PM NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PM NISTIR MAPPING**	

R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.PM NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.PM NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.PM NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.PM NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.PM NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.PM NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.PM NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.PM NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.PM NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.PM NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.PM NISTIR MAPPING**	
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.PM NISTIR MAPPING**	
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.PM NISTIR MAPPING**	
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.PM NISTIR MAPPING**	

R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.PM NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.PM NISTIR MAPPING**	
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.PM NISTIR MAPPING**	
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.PM NISTIR MAPPING**	
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PM NISTIR MAPPING**	
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PM NISTIR MAPPING**	
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.PM NISTIR MAPPING**	
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.PM NISTIR MAPPING**	
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.PM NISTIR MAPPING**	
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.PM NISTIR MAPPING**	
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.PM NISTIR MAPPING**	
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.PM NISTIR MAPPING**	

R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.PM NISTIR MAPPING**	
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.PM NISTIR MAPPING**	
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.PM NISTIR MAPPING**	
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.PM NISTIR MAPPING**	
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.PM NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.PM NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.PM NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.PM NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.PM NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.PM NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.PM NISTIR MAPPING**	

R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.PM NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.PM NISTIR MAPPING**	
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.PM NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.PM NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.PM NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.PM NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.PM NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.PM NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.PM NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.PM NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.PM NISTIR MAPPING**	

R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.PM NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.PM NISTIR MAPPING**	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.PM NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.PM NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.PM NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.PM NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.PM NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.PM NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.PM NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.PM NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.PM NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.PM NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.PM NISTIR MAPPING**	

R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.PM NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.PM NISTIR MAPPING**	
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.PM NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.PM NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.PM NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.PM NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.PM NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.PM NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.PM NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.PM NISTIR MAPPING**	

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.PM NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.PM NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.PM NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.PM NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.PM NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.PM NISTIR MAPPING**	

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.PM NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.PM NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.PM NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.PM NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.PM NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.PM NISTIR MAPPING**	
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.PM NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.PM NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.PM NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.PM NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.PM NISTIR MAPPING**	

R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.PM NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.PM NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.PM NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.PM NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.PM NISTIR MAPPING**	
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.PM NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.PM NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.PM NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.PM NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.PM NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.PM NISTIR MAPPING**	

CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.		
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.PM NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.PM NISTIR MAPPING**	
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.PM NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PM NISTIR MAPPING**	

R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.PM NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.PM NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.PM NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PM NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.PM NISTIR MAPPING**	
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.PM NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.PM NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.		
R1, 1.2: Access control and handling procedures for BES Cyber System Information.		

R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.PM NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PM NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PM NISTIR MAPPING**	

SG.PM-2	SG.PM-3	SG.PM-4
Security Program Plan	Senior Management Authority	Security Architecture

SGIP shall include following requirement from NERC CIP-003-5 R3 to review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.		

	SGIP shall include following requirement from NERC CIP-003-5 R3 to incorporate delegation of Senior Manager authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	

		SGIP should include CIP-010-1 R1.1.1 to develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.

		SGIP shall include following Requirement: Organizations shall implement document process and criteria to identify BES Cyber System Information.
		SGIP shall include following Requirement: Organizations shall implement Access control and handling procedures for BES Cyber System Information.

SG.PM-5	SG.PM-6	SG.PM-7	SG.PM-8
Risk Management Strategy	Security Authorization to Operate Process	Mission/Business Process Definition	Management Accountability
NO NERC CIP MAPPING		**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**

	SGIP shall include following Requirement: Organizations shall implement Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.		

NISTIR Requirement		SG.PS-1
NERC CIP		Personnel Security Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.PS NISTIR MAPPING**	
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.PS NISTIR MAPPING**	
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.PS NISTIR MAPPING**	
R2, 1.1: Personnel Security	**NO SG.PS NISTIR MAPPING**	
R2, 1.2: Electronic Security Parameters	**NO SG.PS NISTIR MAPPING**	
R2, 1.3: Remote Access	**NO SG.PS NISTIR MAPPING**	
R2, 1.4: Physical Security	**NO SG.PS NISTIR MAPPING**	
R2, 1.5: System Security	**NO SG.PS NISTIR MAPPING**	

R2, 1.6: Incident Response	**NO SG.PS NISTIR MAPPING**	
R2, 1.7: Recovery Plans	**NO SG.PS NISTIR MAPPING**	
R2, 1.8: Configuration Change Management	**NO SG.PS NISTIR MAPPING**	
R2, 1.9: Information Protection	**NO SG.PS NISTIR MAPPING**	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.PS NISTIR MAPPING**	
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.PS NISTIR MAPPING**	
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.PS NISTIR MAPPING**	
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.PS NISTIR MAPPING**	
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.PS NISTIR MAPPING**	
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: Define the roles that require training.	**NO SG.PS NISTIR MAPPING**	

R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PS NISTIR MAPPING**	
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.PS NISTIR MAPPING**	
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.PS NISTIR MAPPING**	
R2, 2.5: Training on the visitor control program.	**NO SG.PS NISTIR MAPPING**	
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.PS NISTIR MAPPING**	
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.PS NISTIR MAPPING**	
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.PS NISTIR MAPPING**	
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.PS NISTIR MAPPING**	
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.PS NISTIR MAPPING**	
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.PS NISTIR MAPPING**	
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.PS NISTIR MAPPING**	
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.PS NISTIR MAPPING**	
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.		2(SGIP should include CIP-004-5 Table R4 – Personnel Risk Assessment Program)

R4, 4.1: An initial personnel risk assessment that includes identity verification.		2- SGIP should include CIP-004-5 R4.4.1 as follows: Organizations shall implement initial personnel risk assessment that includes identity verification.
R4.4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.		
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.		
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.		
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.		
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.		
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.PS NISTIR MAPPING**	

R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.		

R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.		
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.		
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.		
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.		
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.		
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.		
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.		

R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.		
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.PS NISTIR MAPPING**	
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	**NO SG.PS NISTIR MAPPING**	
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	**NO SG.PS NISTIR MAPPING**	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	**NO SG.PS NISTIR MAPPING**	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	**NO SG.PS NISTIR MAPPING**	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	**NO SG.PS NISTIR MAPPING**	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.PS NISTIR MAPPING**	
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.PS NISTIR MAPPING**	

R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.PS NISTIR MAPPING**	
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.PS NISTIR MAPPING**	
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.PS NISTIR MAPPING**	
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.PS NISTIR MAPPING**	
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.PS NISTIR MAPPING**	
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.PS NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.PS NISTIR MAPPING**	
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.PS NISTIR MAPPING**	
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.PS NISTIR MAPPING**	
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	**NO SG.PS NISTIR MAPPING**	

R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.PS NISTIR MAPPING**	
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.PS NISTIR MAPPING**	
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.PS NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.PS NISTIR MAPPING**	
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.PS NISTIR MAPPING**	
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.PS NISTIR MAPPING**	
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.PS NISTIR MAPPING**	
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.PS NISTIR MAPPING**	
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.PS NISTIR MAPPING**	
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.PS NISTIR MAPPING**	
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.PS NISTIR MAPPING**	
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.PS NISTIR MAPPING**	

R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.PS NISTIR MAPPING**	
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.PS NISTIR MAPPING**	
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.PS NISTIR MAPPING**	
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.PS NISTIR MAPPING**	
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	**NO SG.PS NISTIR MAPPING**	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.PS NISTIR MAPPING**	
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.PS NISTIR MAPPING**	
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.PS NISTIR MAPPING**	
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.PS NISTIR MAPPING**	
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.PS NISTIR MAPPING**	
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		

R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.PS NISTIR MAPPING**	
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.PS NISTIR MAPPING**	
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.PS NISTIR MAPPING**	
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.PS NISTIR MAPPING**	
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.PS NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.PS NISTIR MAPPING**	
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.PS NISTIR MAPPING**	
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.PS NISTIR MAPPING**	
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.PS NISTIR MAPPING**	

R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.PS NISTIR MAPPING**	
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.PS NISTIR MAPPING**	
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.PS NISTIR MAPPING**	
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.PS NISTIR MAPPING**	
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.PS NISTIR MAPPING**	
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.PS NISTIR MAPPING**	
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.PS NISTIR MAPPING**	
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.PS NISTIR MAPPING**	
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.PS NISTIR MAPPING**	

R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.PS NISTIR MAPPING**	
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.PS NISTIR MAPPING**	
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.PS NISTIR MAPPING**	
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.PS NISTIR MAPPING**	
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.PS NISTIR MAPPING**	
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.PS NISTIR MAPPING**	
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.PS NISTIR MAPPING**	
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.PS NISTIR MAPPING**	
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.PS NISTIR MAPPING**	

R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.PS NISTIR MAPPING**	
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.PS NISTIR MAPPING**	
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.PS NISTIR MAPPING**	
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.PS NISTIR MAPPING**	
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.PS NISTIR MAPPING**	
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.PS NISTIR MAPPING**	

R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.PS NISTIR MAPPING**	
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.PS NISTIR MAPPING**	
R1, 1.1: One or more methods to identify BES Cyber System Information.	**NO SG.PS NISTIR MAPPING**	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.PS NISTIR MAPPING**	
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.PS NISTIR MAPPING**	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.PS NISTIR MAPPING**	
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PS NISTIR MAPPING**	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	**NO SG.PS NISTIR MAPPING**	

SG.PS-2	SG.PS-3	SG.PS-4
Position Categorization	Personnel Screening	Personnel Termination
NO NERC CIP MAPPING		

	3- NERC CIP-004-5 R4.4.1 should include detailed personnel screening requirement detailed in SG.PS-3 as follows: Basic screening requirements should include: 1. Employment history; 2. Verification of the highest education degree received; 3. Residency; 4. References; and 5. Law enforcement records.	
	2- SGIP should include CIP requirement for seven years history records as follows: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
	2(SGIP should include CIP-004-5 Table R4 – Personnel Risk Assessment Program to determine when to deny authorized access.)	
	2(SGAP should include CIP-004-5 Table R5)	
	2(SGAP should include personnel risk assessment for CIP exceptional Circumstances to include following: 1. Processes to invoke special procedures in the event of a CIP Exceptional Circumstance 2. Processes to allow for exceptions to policy that do not violate CIP requirements)	

		2(SGIP should include table CIP-004-5 Table R7 – Access Revocation)
		3(CIP-004-5-R7.1 shall include requirement of exit interview to convey the constraints imposed on the individuals/ contractors/ Third Party Service Providers, due to revocation of privileges caused by change in assignments or termination of job .)
		2(SGIP should include calendar day criteria)
		2(SGIP should include calendar day criteria)
		2(SGIP should include 30 calendar day criteria)

		2(SGIP should include 30 calendar day criteria and change of password for group passwords)

SG.PS-5	SG.PS-6	SG.PS-7	SG.PS-8
Personnel Transfer	Access Agreements	Contractor and Third-Party Personnel Security	Personnel Accountability
	NO NERC CIP MAPPING		**NO NERC CIP MAPPING**

		X	

		2(SGIP should include CIP-004-5 Table R4 – Personnel Risk Assessment Program)	

		3(CIP-004-5 R6.1 shall include security authorization for granting escorted/ unescorted access permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management.	
		3(CIP-004-5 R6.2 shall include security authorization for granting escorted/ unescorted access permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management.	
		3(CIP-004-5 R6.3 shall include security authorization for granting escorted/ unescorted access permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management.	
		3(CIP-004-5 R6.4 shall include security authorization for granting escorted/ unescorted access permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management.	

		3(CIP-004-5 R6.5 shall include security authorization for periodic review of permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management.	
		3(CIP-004-5 R6.6 shall include security authorization for periodic review of permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management).	
2(SGIP should include calendar day criteria)			

SG.PS-9
Personnel Roles
NO NERC CIP MAPPING

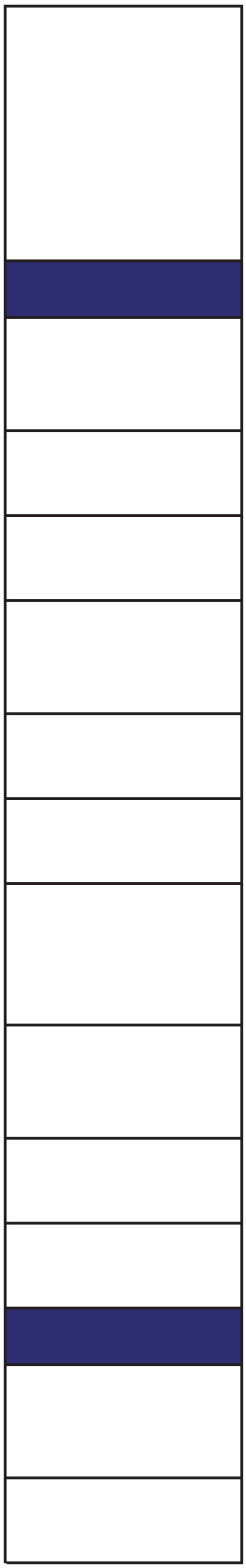

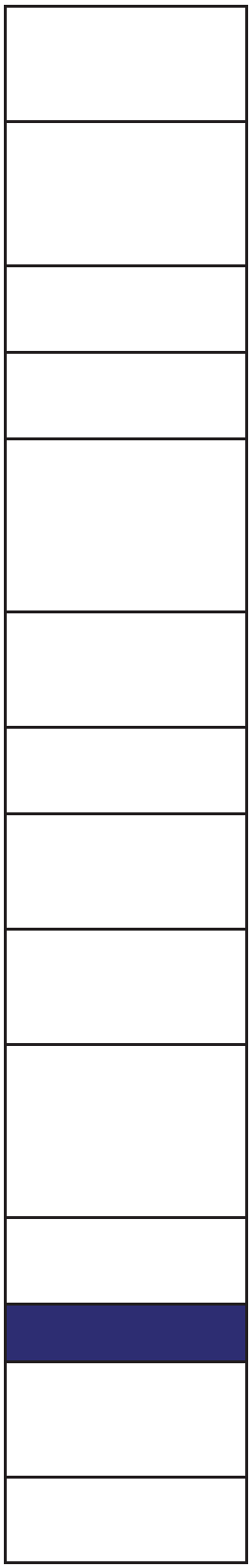

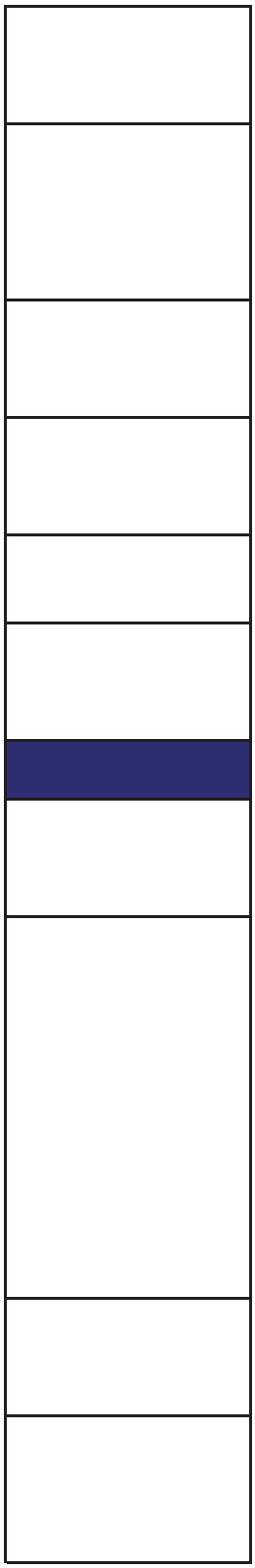

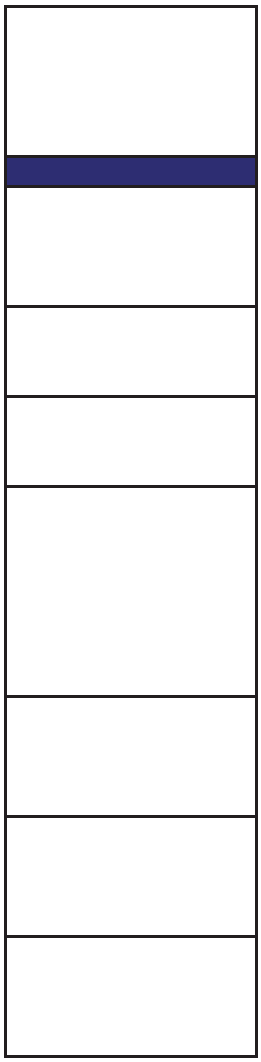

NISTIR Requirement		SG.RA-1
NERC CIP		Risk Assessment Policy and Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.		
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.		
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.		
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.		
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:		
R2, 1.1: Personnel Security		
R2, 1.2: Electronic Security Parameters		
R2, 1.3: Remote Access		
R2, 1.4: Physical Security		
R2, 1.5: System Security		
R2, 1.6: Incident Response		
R2, 1.7: Recovery Plans		
R2, 1.8: Configuration Change Management		
R2, 1.9: Information Protection		
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances		
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.		

R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.		
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.		
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.		
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.		
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.		
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.		
R2, 2.1: Define the roles that require training.		
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.		
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.		
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.		
R2, 2.5: Training on the visitor control program.		
R2, 2.6: Training on handling of BES Cyber System Information and storage media.		
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.		
R2, 2.8: Training on recovery plans for BES Cyber Systems.		
R2, 2.9: Training on response to BES Cyber Security Incidents.		
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.		

R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.		
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.		
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.		
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.		
R4, 4.1: An initial personnel risk assessment that includes identity verification.		
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.		
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.		
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.		
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.		
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.		
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.		
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		

R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.		
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.		
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.		
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.		
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.		
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.		
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.		
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.		
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.		

CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.		
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.		
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).		
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.		
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.		
R1, 1.5: A documented method for detecting malicious communications at each EAP.		
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.		
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.		
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.		
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.		
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.		
R1, 1.1: Define operational or procedural controls to restrict physical access.		
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.		
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.		
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.		

R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.		
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.		
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.		
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.		
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.		
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.		
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.		
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.		
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.		
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.		
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.		
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.		

R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.		
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.		
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.		
R3, 3.2: Disarm or remove identified malicious code.		
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).		
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.		
R3, 3.5: Log each Transient Cyber Asset connection.		
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.		
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.		
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.		
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.		
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.		
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.		
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.		
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.		

R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.		
R5, 5.3: Identify individuals who have authorized access to shared accounts.		
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.		
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.		
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.		
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.		
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.		
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.		
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.		

R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.		
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.		
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.		
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.		
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.		
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.		
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.		
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.		
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.		
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.		
R1, 1.1: Conditions for activation of the recovery plan(s).		

R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.		
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.		
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.		
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.		
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.		
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.		
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.		
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.		
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.		
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.		
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.		
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.		

R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.		
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.		
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.		
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.		
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.		
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.		
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.		
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.		

R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.		
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.		
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.		
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.		
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.		
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.		
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.		
R1, 1.1: One or more methods to identify BES Cyber System Information.		
R1, 1.2: Access control and handling procedures for BES Cyber System Information.		
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.		

R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.		
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		

SG.RA-2	SG.RA-3	SG.RA-4	SG.RA-5
Risk Management Plan	Security Impact Level	Risk Assessment	Risk Assessment Update
	2		
	2		

2			

SG.RA-6
Vulnerability Assessment and Awareness

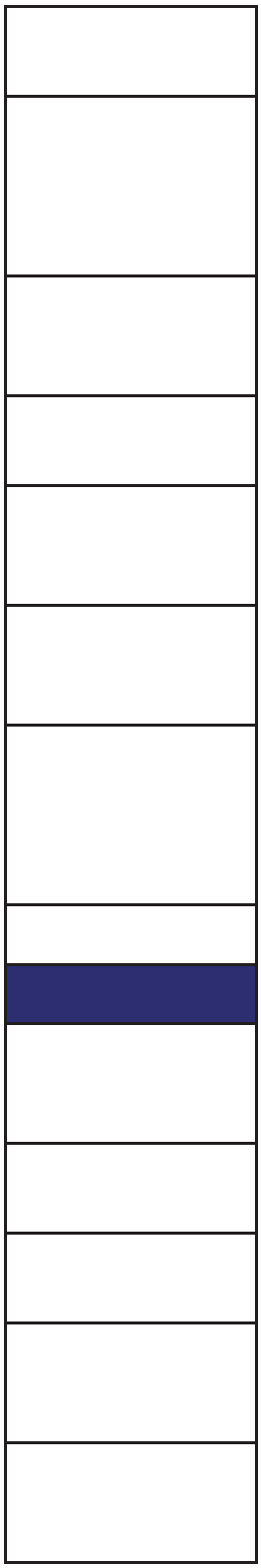

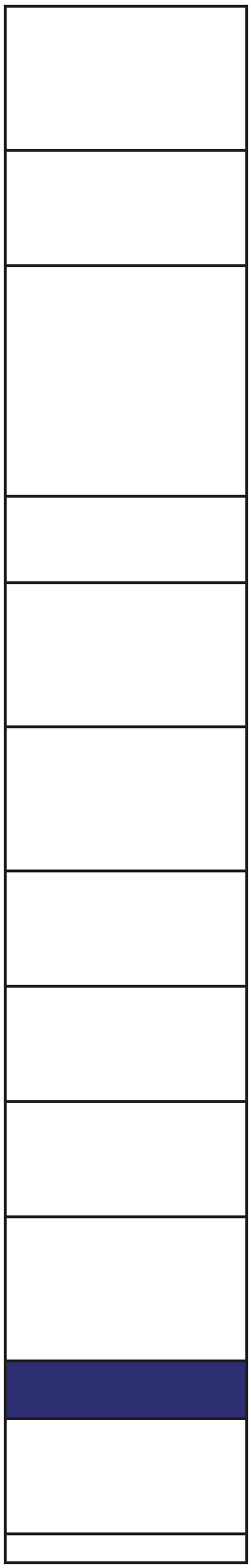

2
2
2
2
2

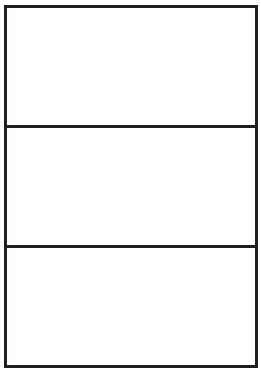

NISTIR Requirement		SG.SA-1
NERC CIP		Smart Grid Information System & Services Acquisition Policy & Procedures
Note that only the language from the requirement section of CIPv5 is included in this table.		
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization		
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.		
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.		
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.		
CIP-003-5: Cyber Security — Security Management Controls		
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.		
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:		
R2, 1.1: Personnel Security		
R2, 1.2: Electronic Security Parameters		
R2, 1.3: Remote Access		
R2, 1.4: Physical Security		
R2, 1.5: System Security		
R2, 1.6: Incident Response		
R2, 1.7: Recovery Plans		
R2, 1.8: Configuration Change Management		
R2, 1.9: Information Protection		
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances		

R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.		
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.		
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.		
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.		
CIP 004-5: Cyber Security – Personnel and Training		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.		
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.		
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.		
R2, 2.1: Define the roles that require training.		
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.		
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.		
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.		
R2, 2.5: Training on the visitor control program.		
R2, 2.6: Training on handling of BES Cyber System Information and storage media.		
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.		
R2, 2.8: Training on recovery plans for BES Cyber Systems.		

R2, 2.9: Training on response to BES Cyber Security Incidents.		
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.		
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.		
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.		
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.		
R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.		
R4, 4.1: An initial personnel risk assessment that includes identity verification.		
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.		
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.		
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.		
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.		
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.		
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.		

R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.		
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.		
R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.		
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.		
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.		
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.		
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.		
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.		
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.		

R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.		
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.		
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.		
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).		
R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.		
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.		
R1, 1.5: A documented method for detecting malicious communications at each EAP.		
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.		
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.		
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.		
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.		
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems		
R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.		
R1, 1.1: Define operational or procedural controls to restrict physical access.		
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.		

R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.		
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.		
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.		
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.		
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.		
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.		
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.		
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.		
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.		
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.		
CIP-007-5: Cyber Security-Systems Security Management		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.		
R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.		
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.		

R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.		
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.		
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.		
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.		
R3, 3.2: Disarm or remove identified malicious code.		
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).		
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.		
R3, 3.5: Log each Transient Cyber Asset connection.		
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.		
R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.		
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.		
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.		
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.		
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.		

R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.		
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.		
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.		
R5, 5.3: Identify individuals who have authorized access to shared accounts.		
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.		
R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.		
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.		
CIP-008-5: Cyber Security-Incident Reporting and Response Planning		
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.		
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.		
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.		

R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.		
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.		
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.		
R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.		
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.		
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.		
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.		
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.		
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.		
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.		
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems		

R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.		
R1, 1.1: Conditions for activation of the recovery plan(s).		
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.		
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.		
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.		
R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.		
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.		
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.		
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.		
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.		
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.		
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.		
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.		

R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.		
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.		
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.		
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.		
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.		
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.		
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.		
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.		

R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.		
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.		
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.		
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.		
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.		
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.		
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.		
CIP-011-1: Cyber Security-Information Protection		
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.		

R1, 1.1: One or more methods to identify BES Cyber System Information.		
R1, 1.2: Access control and handling procedures for BES Cyber System Information.		
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.		
R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.		
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.		

SG.SA-2	SG.SA-3	SG.SA-4	SG.SA-5
Security Policies for Contractors and Third Parties	Life-Cycle Support	Acquisitions	Smart Grid Information System Documentation

2			
2			
2			
2			
2			
2			
2			
2			

2			
2			
2			
2			
2			
2			
2			
2			
2			
2			
2			

2			
			2
			2
			2
			2
			2
			2
			2
			2
			2
			2

			2
			2
			2

			2
			2
			2
			2
			2
			2
			2
			2
			2
			2
			2

			2
			2
			2
			2
			2
			2

SG.SA-6	SG.SA-7	SG.SA-8	SG.SA-9
Software License Usage Restrictions	User-Installed Software	Security Engineering Principles	Developer Configuration Management
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	

		2	

		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	

		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	
		2	

		2	
		2	
		2	
			2
			2
			2
			2
			2

			2
			2
			2
		2	2
		2	2
		2	2
		2	2
		2	2

SG.SA-10	SG.SA-11
Developer Security Testing	Supply Chain Protection

2	
2	
2	
2	
2	

NISTIR Requirement	
NERC CIP	
Note that only the language from the requirement section of CIPv5 is included in this table.	
CIP-002-5: Cyber Security — BES Cyber Asset and BES Cyber System Categorization	
R1: Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.	**NO SG.SC NISTIR MAPPING**
R2: The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.	**NO SG.SC NISTIR MAPPING**
CIP-003-5: Cyber Security — Security Management Controls	
R1: Each Responsible Entity shall identify, by name, a CIP Senior Manager.	**NO SG.SC NISTIR MAPPING**
R2: Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:	**NO SG.SC NISTIR MAPPING**
R2, 1.1: Personnel Security	**NO SG.SC NISTIR MAPPING**
R2, 1.2: Electronic Security Parameters	**NO SG.SC NISTIR MAPPING**
R2, 1.3: Remote Access	**NO SG.SC NISTIR MAPPING**
R2, 1.4: Physical Security	**NO SG.SC NISTIR MAPPING**
R2, 1.5: System Security	**NO SG.SC NISTIR MAPPING**
R2, 1.6: Incident Response	**NO SG.SC NISTIR MAPPING**
R2, 1.7: Recovery Plans	**NO SG.SC NISTIR MAPPING**
R2, 1.8: Configuration Change Management	**NO SG.SC NISTIR MAPPING**

R2, 1.9: Information Protection	
R2, 1.10: Provisions for declaring and responding to CIP Exceptional Circumstances	**NO SG.SC NISTIR MAPPING**
R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.	**NO SG.SC NISTIR MAPPING**
R4: Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.	**NO SG.SC NISTIR MAPPING**
R5: The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.	**NO SG.SC NISTIR MAPPING**
R6: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.	**NO SG.SC NISTIR MAPPING**

CIP 004-5: Cyber Security – Personnel and Training	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on at least a quarterly basis.	**NO SG.SC NISTIR MAPPING**
R2: Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: Define the roles that require training.	**NO SG.SC NISTIR MAPPING**
R2, 2.2: Training on the security controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.SC NISTIR MAPPING**
R2, 2.3: Training on the proper use of physical access controls protecting the Responsible Entity's BES Cyber Systems.	**NO SG.SC NISTIR MAPPING**
R2, 2.4: Training on the electronic access controls protecting the Responsible Entity's BES Cyber Systems. Evidence may include, but is not limited to, training material on the electronic access controls to protect BES Cyber Systems.	**NO SG.SC NISTIR MAPPING**
R2, 2.5: Training on the visitor control program.	**NO SG.SC NISTIR MAPPING**
R2, 2.6: Training on handling of BES Cyber System Information and storage media.	**NO SG.SC NISTIR MAPPING**
R2, 2.7: Training on identification of a potential BES Cyber Security Incident and associated notifications.	**NO SG.SC NISTIR MAPPING**
R2, 2.8: Training on recovery plans for BES Cyber Systems.	**NO SG.SC NISTIR MAPPING**
R2, 2.9: Training on response to BES Cyber Security Incidents.	**NO SG.SC NISTIR MAPPING**
R2, 2.10: Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	**NO SG.SC NISTIR MAPPING**
R3: Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training.	**NO SG.SC NISTIR MAPPING**
R3, 3.1: Require completion of the training specified in CIP-004-5 R2 prior to granting authorized access, except during CIP Exceptional Circumstances.	**NO SG.SC NISTIR MAPPING**
R3, 3.2: Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	**NO SG.SC NISTIR MAPPING**

R4: Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program.	**NO SG.SC NISTIR MAPPING**
R4, 4.1: An initial personnel risk assessment that includes identity verification.	**NO SG.SC NISTIR MAPPING**
R4,4.2: Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**NO SG.SC NISTIR MAPPING**
R4, 4.3: Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.	**NO SG.SC NISTIR MAPPING**
R4, 4.4: Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4.	**NO SG.SC NISTIR MAPPING**
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment.	**NO SG.SC NISTIR MAPPING**
R5, 5.1: Perform a personnel risk assessment as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.	**NO SG.SC NISTIR MAPPING**
R6: Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program.	**NO SG.SC NISTIR MAPPING**
R6, 6.1: The CIP Senior Manager or delegate shall authorize electronic access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.SC NISTIR MAPPING**
R6, 6.2: The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.SC NISTIR MAPPING**
R6, 6.3: The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.	**NO SG.SC NISTIR MAPPING**
R6, 6.4: Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access.	**NO SG.SC NISTIR MAPPING**

R6, 6.5: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.SC NISTIR MAPPING**
R6, 6.6: Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.	**NO SG.SC NISTIR MAPPING**
R7: Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation.	**NO SG.SC NISTIR MAPPING**
R7, 7.1: For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.	**NO SG.SC NISTIR MAPPING**
R7, 7.2: For reassignments or transfers, revoke the individual's unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.	**NO SG.SC NISTIR MAPPING**
R7, 7.3: For resignations or terminations, revoke the individual's access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.	**NO SG.SC NISTIR MAPPING**
R7, 7.4: For resignations or terminations, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.	**NO SG.SC NISTIR MAPPING**
R7, 7.5: For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user. In extenuating circumstances that require a longer time period, document the extenuating circumstances and change the password(s) within ten calendar days following the end of the extenuating circumstances.	**NO SG.SC NISTIR MAPPING**
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: Define technical or procedural controls to restrict unauthorized electronic access.	**NO SG.SC NISTIR MAPPING**
R1, 1.2: Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	

R1, 1.3: Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions.	
R1, 1.4: Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	
R1, 1.5: A documented method for detecting malicious communications at each EAP.	**NO SG.SC NISTIR MAPPING**
R2: Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	
R2, 2.2: Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session.	
R2, 2.3: Require multi-factor authentication for all Interactive Remote Access sessions.	**NO SG.SC NISTIR MAPPING**
CIP-006-5: Cyber Security - Physical Security of BES Cyber Systems	

R1: Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: Define operational or procedural controls to restrict physical access.	**NO SG.SC NISTIR MAPPING**
R1, 1.2: Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized.	**NO SG.SC NISTIR MAPPING**
R1, 1.3: Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible.	**NO SG.SC NISTIR MAPPING**
R1, 1.4: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.	**NO SG.SC NISTIR MAPPING**
R1, 1.5: Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems.	**NO SG.SC NISTIR MAPPING**
R1, 1.6: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry.	**NO SG.SC NISTIR MAPPING**
R2: Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Defined Physical Boundary.	**NO SG.SC NISTIR MAPPING**
R2, 2.2: A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact.	**NO SG.SC NISTIR MAPPING**
R3: Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program.	**NO SG.SC NISTIR MAPPING**
R3, 3.1: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided.	**NO SG.SC NISTIR MAPPING**
R3, 3.2: Log dates, time, and duration for failures or outages of access control, logging, and alerting systems.	**NO SG.SC NISTIR MAPPING**
CIP-007-5: Cyber Security-Systems Security Management	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.	**NO SG.SC NISTIR MAPPING**

R1, 1.1: Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.	
R1, 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.	**NO SG.SC NISTIR MAPPING**
R2, 2.2: Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe.	**NO SG.SC NISTIR MAPPING**
R2, 2.3: A process for remediation, including any exceptions for CIP Exceptional Circumstances.	**NO SG.SC NISTIR MAPPING**
R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.	**NO SG.SC NISTIR MAPPING**
R3, 3.1: Deploy method(s) to deter, detect, or prevent malicious code.	**NO SG.SC NISTIR MAPPING**
R3, 3.2: Disarm or remove identified malicious code.	**NO SG.SC NISTIR MAPPING**
R3, 3.3: Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).	**NO SG.SC NISTIR MAPPING**
R3, 3.4: Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.	**NO SG.SC NISTIR MAPPING**
R3, 3.5: Log each Transient Cyber Asset connection.	**NO SG.SC NISTIR MAPPING**
R4: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring.	**NO SG.SC NISTIR MAPPING**

R4, 4.1: Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity.	**NO SG.SC NISTIR MAPPING**
R4, 4.2: Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.	**NO SG.SC NISTIR MAPPING**
R4, 4.3: Detect and activate a response to event logging failures before the end of the next calendar day.	**NO SG.SC NISTIR MAPPING**
R4, 4.4: Retain BES Cyber System security-related event logs identified in 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	**NO SG.SC NISTIR MAPPING**
R4, 4.5: Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.	**NO SG.SC NISTIR MAPPING**
R5: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.	**NO SG.SC NISTIR MAPPING**
R5, 5.1 : Validate credentials before granting electronic access to each BES Cyber System.	
R5, 5.2: The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types.	**NO SG.SC NISTIR MAPPING**
R5, 5.3: Identify individuals who have authorized access to shared accounts.	**NO SG.SC NISTIR MAPPING**
R5, 5.4: Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.	**NO SG.SC NISTIR MAPPING**

R5, 5.5: For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	**NO SG.SC NISTIR MAPPING**
R5, 5.6: A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.	**NO SG.SC NISTIR MAPPING**
CIP-008-5: Cyber Security-Incident Reporting and Response Planning	
R1: Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: Processes to identify, classify, and respond to BES Cyber Security Incidents.	**NO SG.SC NISTIR MAPPING**
R1, 1.2: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	**NO SG.SC NISTIR MAPPING**
R1, 1.3: Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	**NO SG.SC NISTIR MAPPING**
R2: Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	**NO SG.SC NISTIR MAPPING**

R2, 2.2: Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	**NO SG.SC NISTIR MAPPING**
R2, 2.3: Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	**NO SG.SC NISTIR MAPPING**
R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication.	**NO SG.SC NISTIR MAPPING**
R3, 3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	**NO SG.SC NISTIR MAPPING**
R3, 3.2: Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	**NO SG.SC NISTIR MAPPING**
R3, 3.3: Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	**NO SG.SC NISTIR MAPPING**
R3, 3.4: Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	**NO SG.SC NISTIR MAPPING**
R3, 3.5: Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	**NO SG.SC NISTIR MAPPING**
CIP-009-5: Cyber Security-Recovery Plans for BES Cyber Assets and Systems	
R1: Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: Conditions for activation of the recovery plan(s).	**NO SG.SC NISTIR MAPPING**
R1, 1.2: Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts.	**NO SG.SC NISTIR MAPPING**
R1, 1.3: One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality.	**NO SG.SC NISTIR MAPPING**
R1, 1.4: Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	**NO SG.SC NISTIR MAPPING**

R1, 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.	**NO SG.SC NISTIR MAPPING**
R2: Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: • by recovering from an actual incident, or • with a paper drill or tabletop exercise, or • with a full operational exercise.	**NO SG.SC NISTIR MAPPING**
R2, 2.2: Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations.	**NO SG.SC NISTIR MAPPING**
R2, 2.3: Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise.	**NO SG.SC NISTIR MAPPING**
R3: Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	**NO SG.SC NISTIR MAPPING**
R3, 3.1: Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned.	**NO SG.SC NISTIR MAPPING**
R3, 3.2: Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.	**NO SG.SC NISTIR MAPPING**
R3, 3.3: Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.	**NO SG.SC NISTIR MAPPING**
R3, 3.4: Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.	**NO SG.SC NISTIR MAPPING**
R3, 3.5: Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed.	**NO SG.SC NISTIR MAPPING**
CIP-010-1: Cyber Security-Configuration Management and Vulnerability Assessments	

R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	**NO SG.SC NISTIR MAPPING**
R1, 1.2: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	**NO SG.SC NISTIR MAPPING**
R1, 1.3: Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	**NO SG.SC NISTIR MAPPING**
R1, 1.4: For a change to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	**NO SG.SC NISTIR MAPPING**
R1, 1.5: For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.SC NISTIR MAPPING**
R2: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.	**NO SG.SC NISTIR MAPPING**

R3: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.	**NO SG.SC NISTIR MAPPING**
R3, 3.1: Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	**NO SG.SC NISTIR MAPPING**
R3, 3.2: Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	**NO SG.SC NISTIR MAPPING**
R3, 3.3: Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset.	**NO SG.SC NISTIR MAPPING**
R3, 3.4: Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.	**NO SG.SC NISTIR MAPPING**
CIP-011-1: Cyber Security-Information Protection	
R1: Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection.	**NO SG.SC NISTIR MAPPING**
R1, 1.1: One or more methods to identify BES Cyber System Information.	
R1, 1.2: Access control and handling procedures for BES Cyber System Information.	**NO SG.SC NISTIR MAPPING**
R1, 1.3: Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	**NO SG.SC NISTIR MAPPING**

R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal.	**NO SG.SC NISTIR MAPPING**
R2, 2.1: Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	
R2, 2.2: Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.	

SG.SC-1	SG.SC-2
System and Communication Protection Policy and Procedures	Communications Partitioning

the CIP standards listed here, you must also consider CIP-004 R6 related to Access Management which requires the following: 004 R6.1 - Requires all electronic access to be properly authorized and limited based on need 004 R6.2 - Requires all unescorted physical access to be properly authorized and limited based on need 004 R6.3 - Requires all access to CIP Information (in any form) to be properly authorized and limited based on need. 004 R 6.4 - Requires quarterly review to verify all electronic and physical access is authorized 004 R 6.5 - Requires annual review of individual access rights to ensure that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions 004 R 6.6 - Requires annual review of all access to CIP information to ensure privileges are correct and the minimum necessary for performing assigned work functions The CIP Standards do not, however specifically require data communications to be addressed in the information	

	3- CIP-011-1-R1.1 should include this requirement to partition the communications for telemetry/data acquisition services and management functionality. The information system management communications path needs to be physically or logically separated from the telemetry/data acquisition services communications path

SG.SC-3	SG.SC-4
Security Function Isolation	Information Remnants

3- CIP-011-1-R1.1 should include this requirement to information system employs underlying hardware separation mechanisms to facilitate security function isolation; and isolate security functions (e.g., functions enforcing access and information flow control) from both non-security functions and from other security functions.	

	2- SGIP should include this requirement to take action to prevent the unauthorized retrieval of BES Cyber System Information from the media, Prior to the release for reuse of BES Cyber Asset media.
	2- SGIP should include this requirement to destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media, Prior to the disposal of BES Cyber Asset media.

SG.SC-5	SG.SC-6	SG.SC-7	SG.SC-8
Denial-of-Service Protection	Resource Priority	Boundary Protection	Communication Integrity
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**		**NO NERC CIP MAPPING**

		2- SGIP should include this requirement to Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs).	

		2- SGIP should include this requirement to Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions..	
		2- SGIP should include this requirement to Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	

		2(SGIP shall include CIP-007-5-R1.1 to disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports.)	
		2(SGIP shall include CIP-007-5-R1.2 to disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media)	

		3(CIP-007-5 R5.1 shall include following requirement: Responsible Entity shall prevent public access into the information system networks except as appropriately mediated.	

SG.SC-9	SG.SC-10	SG.SC-11	SG.SC-12
Communication Confidentiality	Trusted Path	Cryptographic Key Establishment and Management	Use of Validated Cryptography
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**		

		3 - NISTIR specifies cryptographic key controls which must be in place. CIP only requires encryption, but the type of key controls required by NISTIR are typically not applicable due to the use of two-factor authentication which is required to establish an encrypted tunnel into an ESP.	3 - CIP does not specify any encryption standards which must be used.

SG.SC-13	SG.SC-14	SG.SC-15	SG.SC-16
Collaborative Computing	Transmission of Security Parameters	Public Key Infrastructure Certificates	Mobile Code
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**

SG.SC-17	SG.SC-18	SG.SC-19	SG.SC-20
Voice-Over Internet Protocol	System Connections	Security Roles	Message Authenticity
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**

SG.SC-21	SG.SC-22	SG.SC-23	SG.SC-24
Secure Name/Address Resolution Service	Fail in Known State	Thin Nodes	Honeypots
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**

SG.SC-25	SG.SC-26	SG.SC-27
Operating System-Independent Applications	Confidentiality of Information at Rest	Heterogeneity
NO NERC CIP MAPPING	**NO NERC CIP MAPPING**	**NO NERC CIP MAPPING**

SG.SC-28	SG.SC-29	SG.SC-30
Virtualization Technique	Application Partitioning	Information System Partitioning
	NO NERC CIP MAPPING	**NO NERC CIP MAPPING**

3- CIP-005-5-R2.1 should include the requirement's follows: A1. The organization employs virtualization techniques to deploy a diversity of operating systems environments and applications; A2. The organization changes the diversity of operating systems and applications on an organization-defined frequency; and A3. The organization employs randomness in the implementation of the virtualization.		

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft CIP Standards Version 5

Project 2008-06 Cyber Security Order 706 Standards Drafting Team
April 10, 2012

RELIABILITY | ACCOUNTABILITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda

- Opening Remarks – John Lim, Consolidated Edison, Chair
- Version 5 Overview – Philip Huff, AECC, Vice Chair
- Version 5, Highlights of Draft 2 – John Lim, Consolidated Edison; David Revill, Georgia Transmission Corporation; and Jay Cribb, Southern Company
- Comment and Ballot Process – Steven Noess, NERC and Jay Cribb, Southern Company
- Questions and Answers – Moderated by Steven Noess, NERC

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP Version 5 Overview

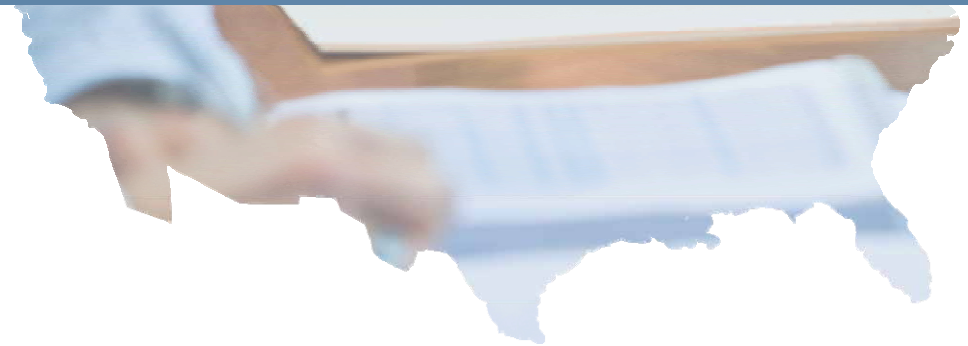

Comparative Table

Version 4	Version 5
42 requirements; 113 parts	37 requirements; 148 Parts
No contextual information	Includes background, rationale, and guidelines and Technical Basis
Measures on high level requirement only	Measures for each requirement, including parts
14 requirements with Technical Feasibility Exception (TFE) triggering language	12 requirements with TFE triggering language
Undefined periodic terms	Clear periodic requirements: initial requirements in Implementation Plan
Many binary Violation Severity Levels (VSLs)	More gradated VSLs

Advantages of Version 5

- Flexibility
- Builds on Experience
- Systems Approach
- Results-based Standards

Closes FERC Order 706

- Addresses the remainder of 60 directives in FERC Order No. 706
- Closes the continuous development cycle for CIP standards
- Allows industry to better implement long-term security solutions and audit programs

Results-based Standards

- Focuses on the reliability and security result
- Eliminates unnecessary documentation requirements
- Identifies examples of evidence
- Provides guidance and context alongside each requirement

Systems Approach

- Cyber Assets function together as a complex system
- Identify the system and apply requirements to the whole rather than the part

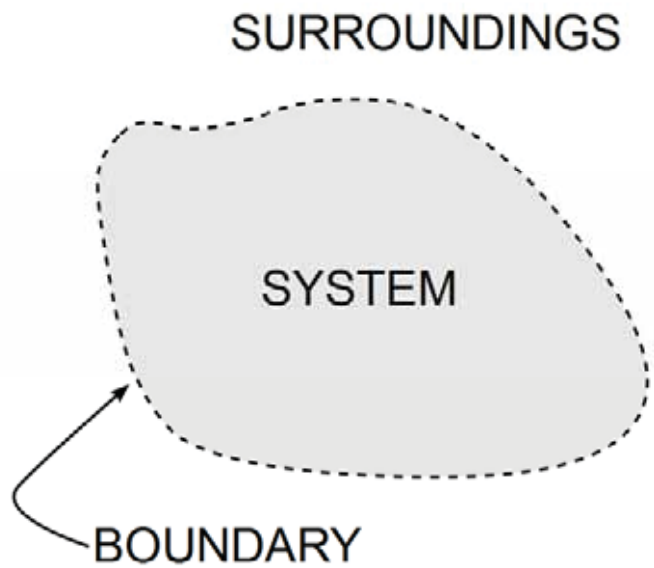

Risk-based Requirements

- Systems performing a Bulk Electric System (BES) function receive an appropriate level of protection
  - Systems are no longer “in or out”
- Impact and connectivity inform applicability
- Non-technology specific
- More appropriate use of TFE process
- Framework for establishing a culture of security

Building on Experience

- Informed by and responsive to implementation and audit lessons from Versions 1 through 3
- Industry has progressed with better, alternative ways to meet a requirement objective
- Cyber risk and the tools to mitigate risk have changed

Balanced Flexibility

- Demonstrates clear accountability for CIP, yet…
- Balances the need to be both:
  - **Specific** enough to objectively demonstrate compliance and
  - **Broad** enough to allow effective risk mitigation
- **Specific** in *when* and *what* to achieve but **broad** in *how* to get there

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP Version 5 – Highlights of Draft 2 Changes

Applicability – Section 4

- Applicability – Section 4
  - Distribution Provider/LSE
    - UVLS/UFLS
  - Distribution Provider
    - Cranking Path Elements

CIP-002-5

- Facilities-based approach
  - Identify High Impact and Medium Impact Facilities, Systems, and Equipment
  - Identify and categorize associated BES Cyber Systems and BES Cyber Assets
  - Attachment 1 criteria closer to Version 4 language
- BES Reliability Operating Services – No longer used
- Sixty days for update due to BES change

CIP-002-5 Restoration Assets

- Restoration Facilities, Systems, and equipment
  - Blackstart Resources
  - Cranking Paths
- Concerns on overall effect on BES restoration resources
  - NERC Operating Committee/Planning Committee discussion (March meetings)
- No longer in Medium Impact criteria
  - In scope
  - Default to Low Impact

CIP-002-5 Related Definitions

- BES Cyber Asset

  "A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, Systems, or equipment; which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, Systems and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)"

CIP-002-5 Related Definitions

- BES Cyber System
  - "One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity."
- BES Reliability Operating Services
  - Removed as a NERC Glossary Term and from references in the requirements or other definitions
  - Moved as guidance to Guidelines and Technical Basis

Definitions

- Control Center
  - "One or more facilities hosting operating personnel that monitor and control the BES in real-time to perform the reliability functional tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generation Operator for generation Facilities at two or more locations."

Low Impact Requirements

- Dispersed requirements were hard to find and identify
  - "All Responsible Entity" requirements also applied to Low Impact
- Removed all Low Impact requirements from CIP-004 though CIP-011
- Now only a single requirement (CIP-003 R2) – Low Impact Policy
  - 2.1 Cyber security awareness;
  - 2.2 Physical access control;
  - 2.3 Electronic access control; and
  - 2.4 Incident response to a BES Cyber Security Incident.
  - An inventory, list, or discrete identification of BES Cyber Systems is not required.

Initial Performance – Periodic Requirements

- Modified timing language in the standards
  - "~~initially upon the effective date of the standard and~~ at least once each calendar year ~~thereafter~~, not to exceed 15 calendar months"
- Initial performance clarified in Implementation Plan
  - On or before the Effective Date
  - Within X calendar days/months/years of the Effective Date

Implementation Plan

Proposed Implementation Plan for Version 5 of CIP Cyber Security Standards
(Graphic for illustrative purposes only; dates are estimates only and based on assumptions. There is no way to know or anticipate when FERC may take action on pending matters.)

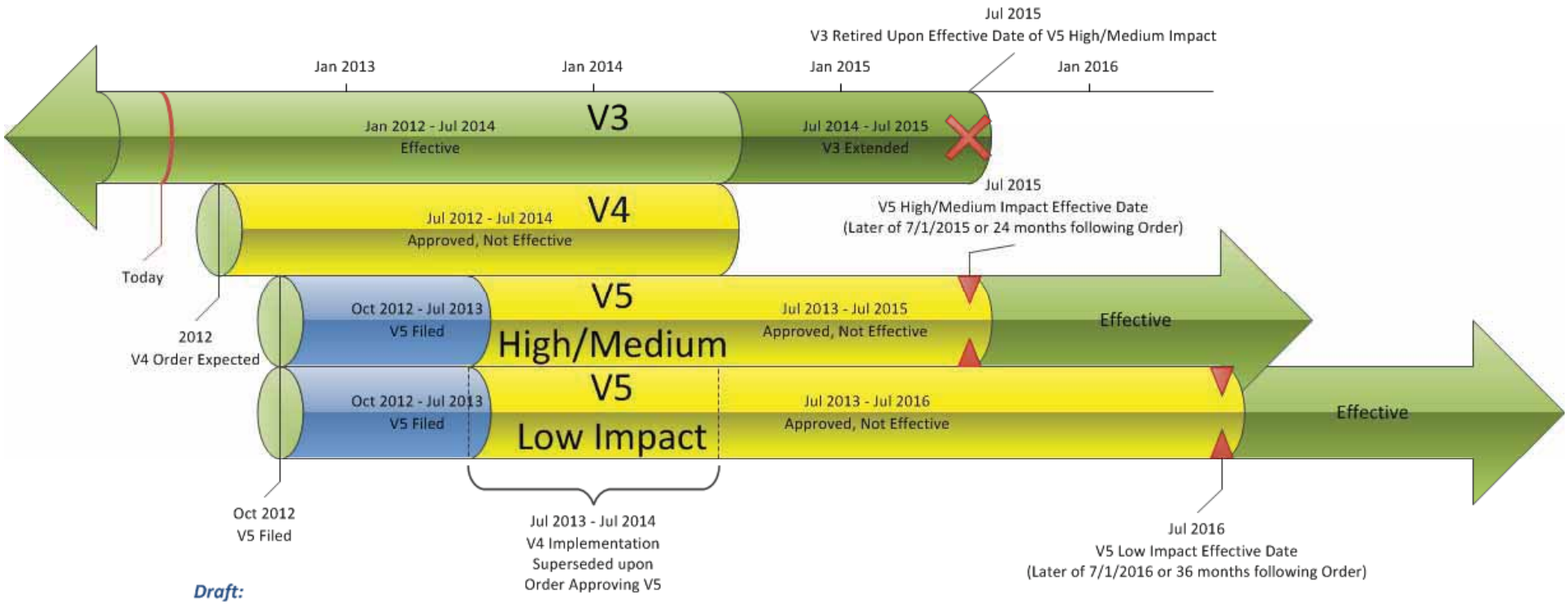

Draft:
April 10, 2012

ESPs - High Watermarking

- Electronic Security Perimeter (ESP)
  - "The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol."
- Protected Cyber Asset (PCA)
  - "A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same ESP (a Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset within an ESP or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes)."

ESPs - High Watermarking

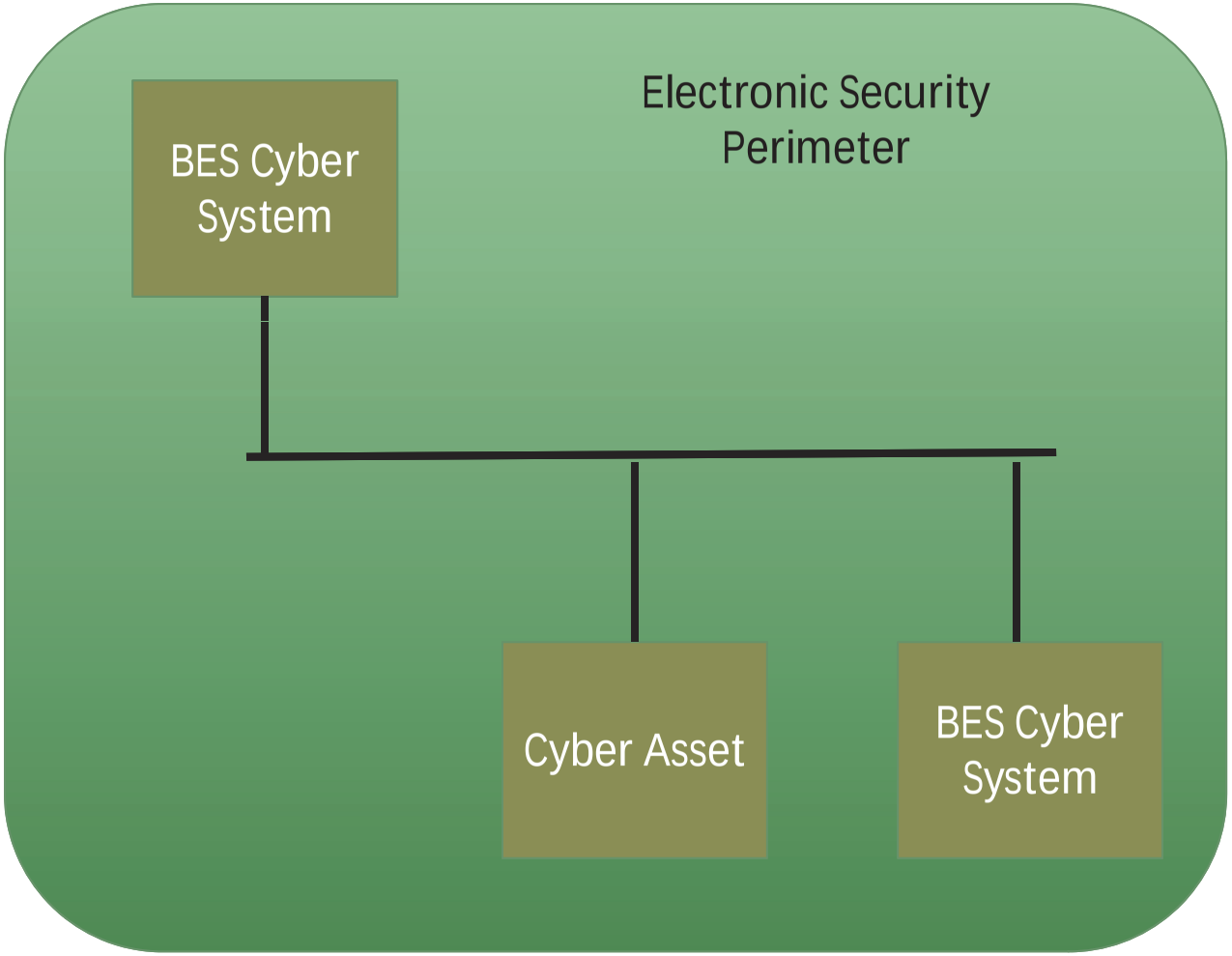

No External Routable Connectivity

ESPs - High Watermarking

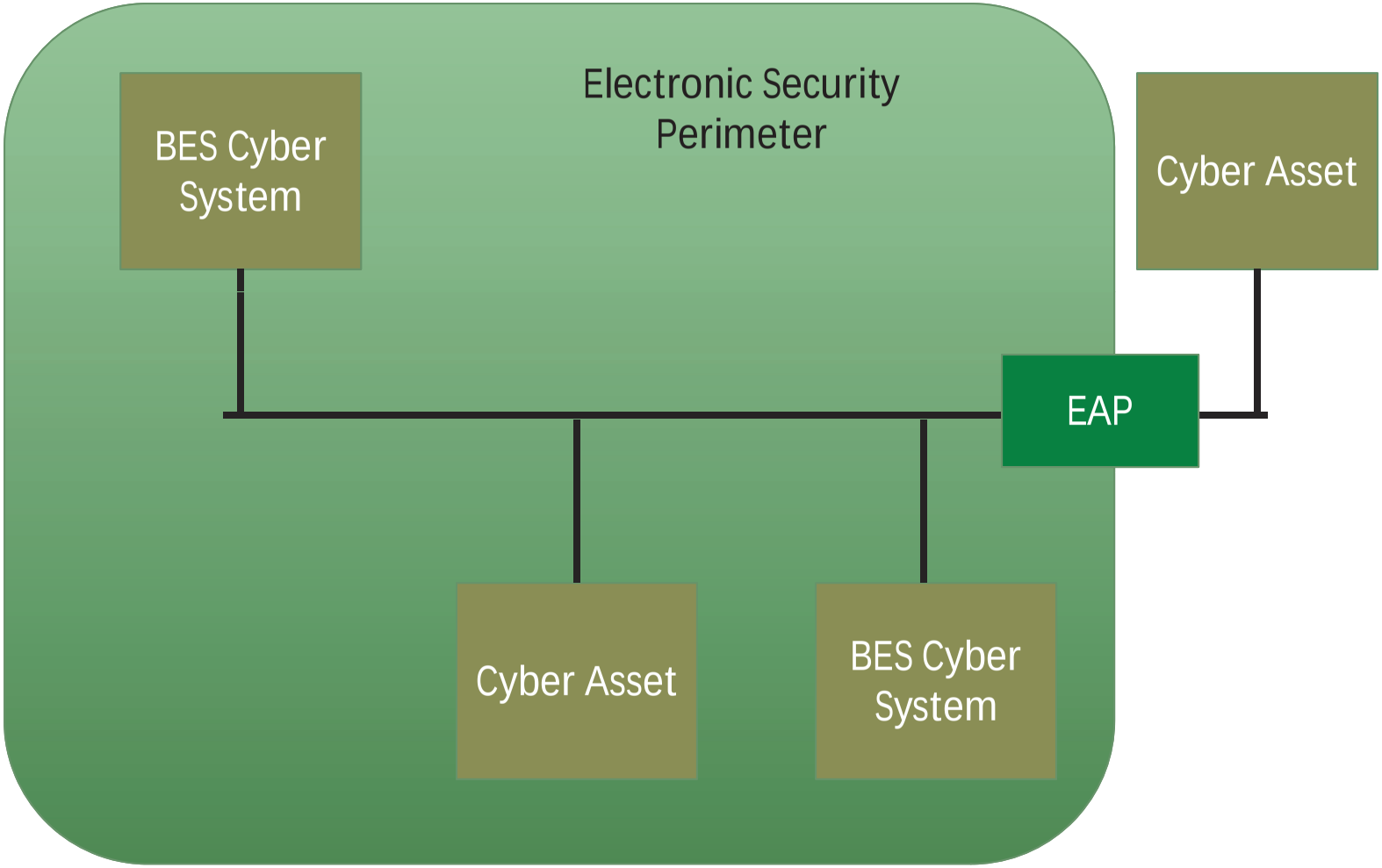

ESPs - High Watermarking

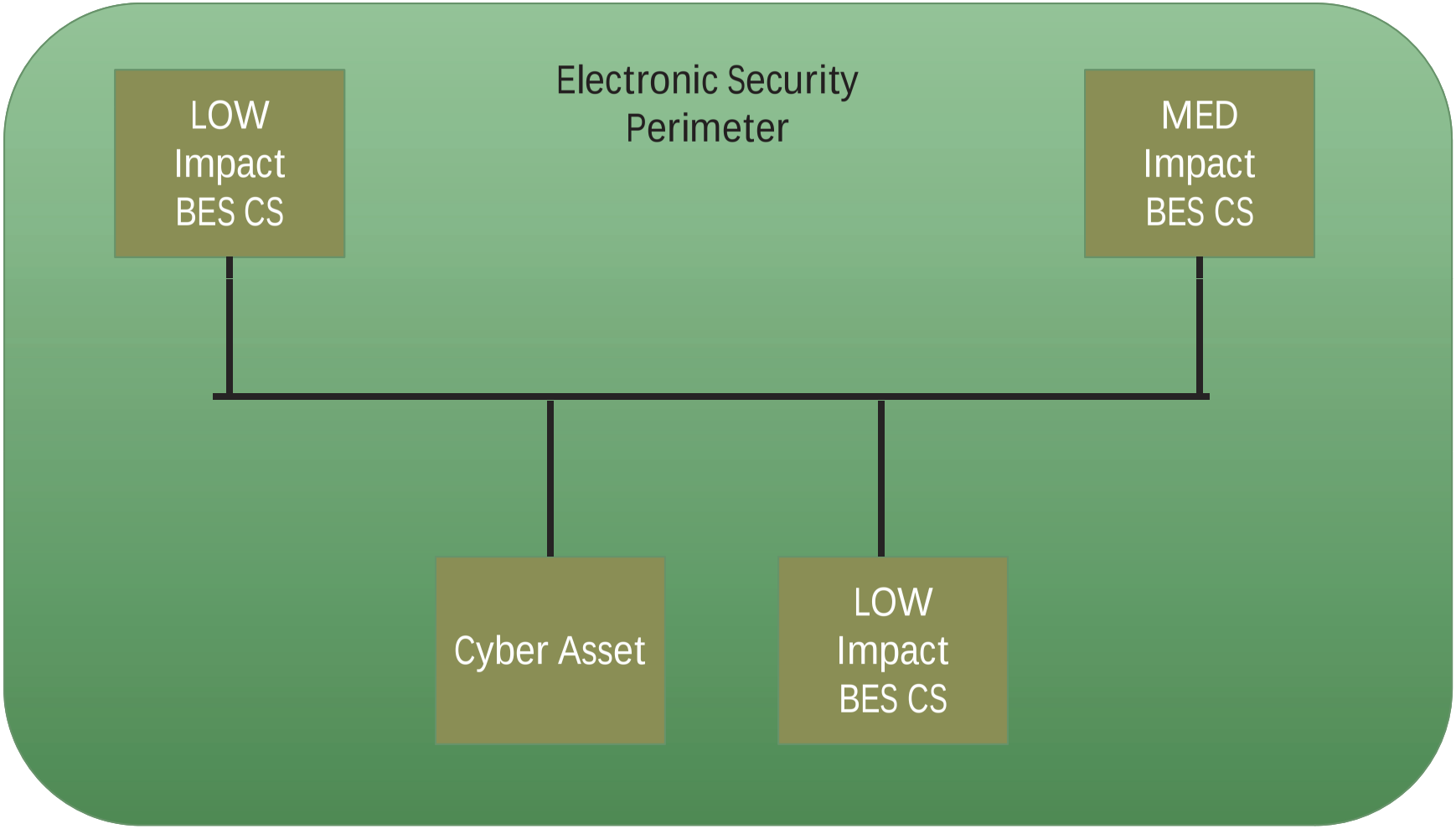

ESPs - High Watermarking

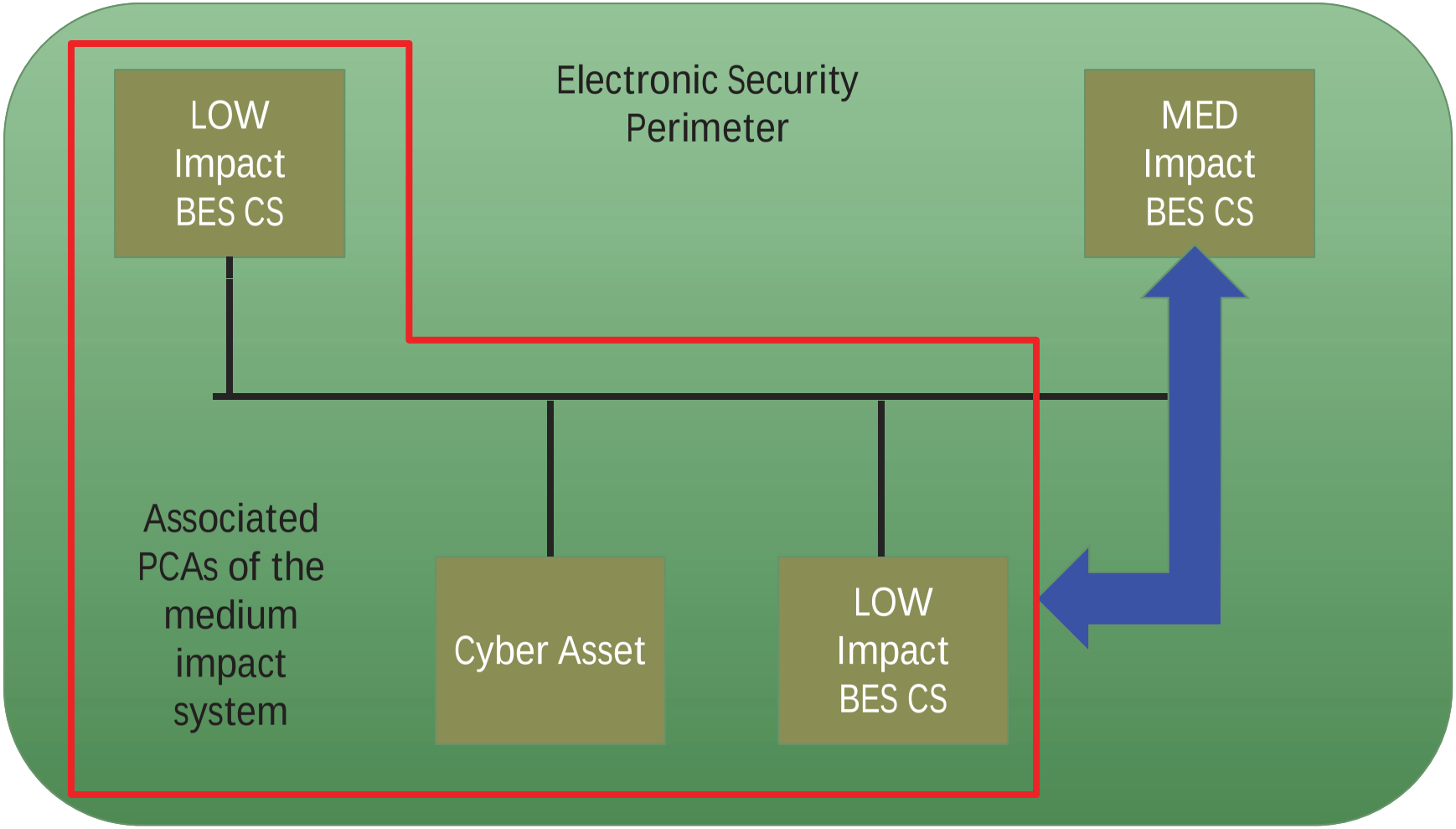

Physical Security and External Connectivity

- All High and Medium Impact BES Cyber Systems
  - "Define operational or procedural controls to restrict physical access"
  - This includes standalone and serial connected BES Cyber Assets
- Additional items for Medium Impact BES Cyber Systems with External Routable Connectivity and High Impact BES Cyber Systems
  - Control, monitor, and log access to Physical Security Perimeters
  - Allow access to only individuals who have authorized unescorted physical access
  - Visitor control program, maintenance, and testing

More Definitions

- "Physical Security Perimeter" term replaces "Defined Physical Boundary"
- "Transient Cyber Asset" deleted
- "External Connectivity" deleted

VSLs

- VSLs modified to include more granularity and gradation
  - Reduction in binary/severe nature
  - Gradated timeframes
  - Gradated percent of assets in violation

Comment and Ballot Process

Stakeholder Consensus Process

CIP Version 5 posted for 40-day formal comment and simultaneous 10-day successive ballot period

New/Successive Ballot:
At this step, the standard is either "new" or significantly changed from the last version posted for comment/ ballot. The ballot record starts with no votes and no comments.

Recirculation Ballot:
At this step, there have been no significant changes to the standard from the last ballot. The ballot record starts with all votes and comments from the previous ballot.

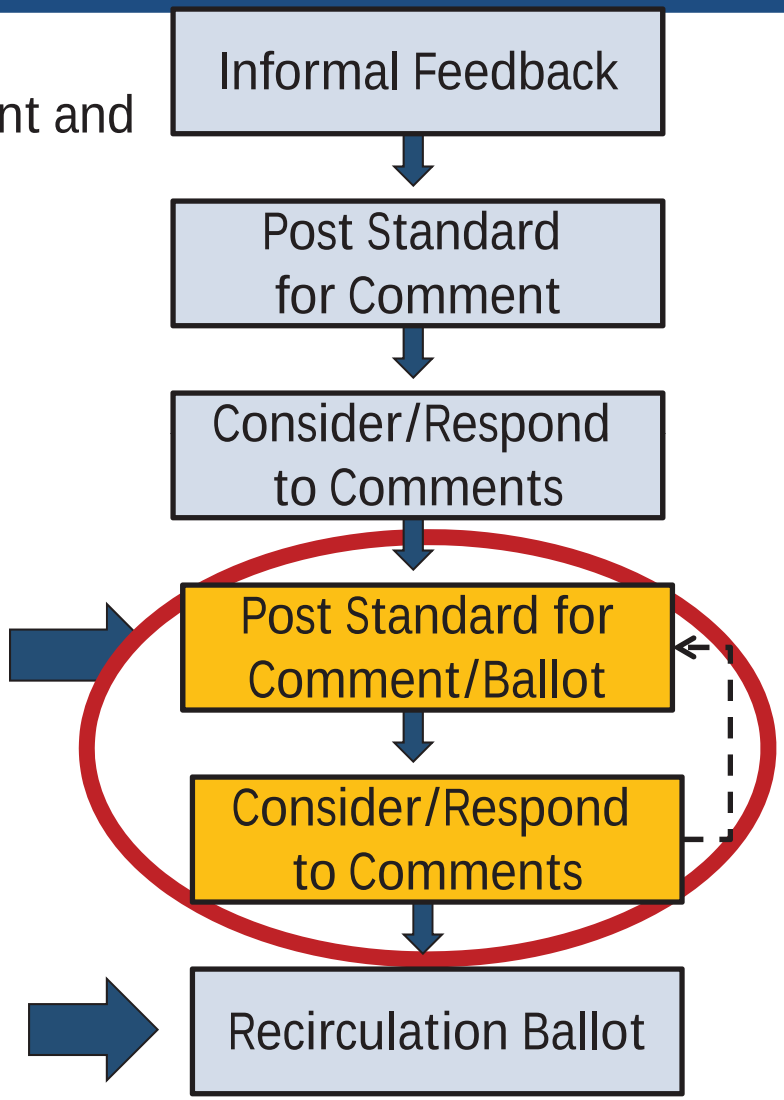

Comment and Ballot Period

- April 12, 2012 through May 21, 2012
  - Formal 40-day comment period
- May 11, 2012 through May 21, 2012
  - Twelve Successive Ballots open
    - Ten Standards
    - Definitions
    - Implementation Plan

Navigating Stakeholder Input Toward Consensus

- Stakeholder feedback is essential
- Almost 2000 pages of comments
- Very constructive comments during last posting
- Drafting team considered all viewpoints

Submitting Comments

- Ballot Comments
  - Submit through "checkbox form" – not within ballot
  - No need to submit same comment more than once
- Comments on proposed standards
  - Submit through electronic form
  - Be brief
  - Focus on question asked
  - Indicating agreement with others is preferred over copying the comments (e.g., "ABC agrees with XYZ's comments")

Comment Form

- Unofficial comment form
  - Provided to assist comment development
  - Divided into four forms (A through D)
  - Formatting will not transfer from unofficial form to official form (web-based)
- Warning included on comment form:

VERY IMPORTANT:
Please note that **the official comment form *does not* retain formatting** (even if it appears to transfer formatting when you copy from the unofficial Word version of the form into the official electronic comment form). If you enter extra carriage returns, bullets, automated numbering, symbols, bolding, italics, or any other formatting, that formatting will not be retained when you submit your comments. Therefore, if you would like to separate portions of your comment by idea, e.g., the drafting team requests that each distinct idea in the same comment block be prefaced with (1), (2), etc., instead of using formatting such as extra carriage returns, bullets, automated numbering, bolding, or italics.

Comment Form

5. CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

- ☐ Yes
- ☐ No

6. CIP-009-5 R2 states "Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

- ☐ Yes
- ☐ No

7. CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

- ☐ Yes
- ☐ No

8. CIP-009-5: If you disagree with the changes made to CIP-009-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments:

Standard Drafting Team Response Process

- Issues and responses for each individual requirement
- Effective feedback
  - Specific to question
  - Provided proposed change/rationale
- Less effective feedback
  - Repeating comment multiple times/responses to entire standard in every question
  - No reference to where suggested change should occur
  - Non-technology agnostic requirements that can't be applied to all Cyber Assets in a mandatory and enforceable environment.

Questions?

- Please submit your questions via the ReadyTalk chat window
- Moderator and point of contact – Steven Noess, NERC
  - steven.noess@nerc.net
- Key dates:
  - April 12, 2012 through May 21, 2012 – Formal Comment Period
  - May 11, 2012 through May 21, 2012 – Ballots Open
- Slides and recording of this webinar will be posted to the NERC website (usually within three business days)

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards, with some changes, and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-5

3. **Purpose:** To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities described in 4.2.2

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   4.1.7 Reliability Coordinator

   4.1.8 Transmission Operator

   4.1.9 Transmission Owner

   4.2. Facilities:

   4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

   4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

This standard provides “bright-line” criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, Systems, and equipment; which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team’s review of the NIST Risk Management Framework and the use of an analogous term “information system” as the target for categorizing and applying security controls.

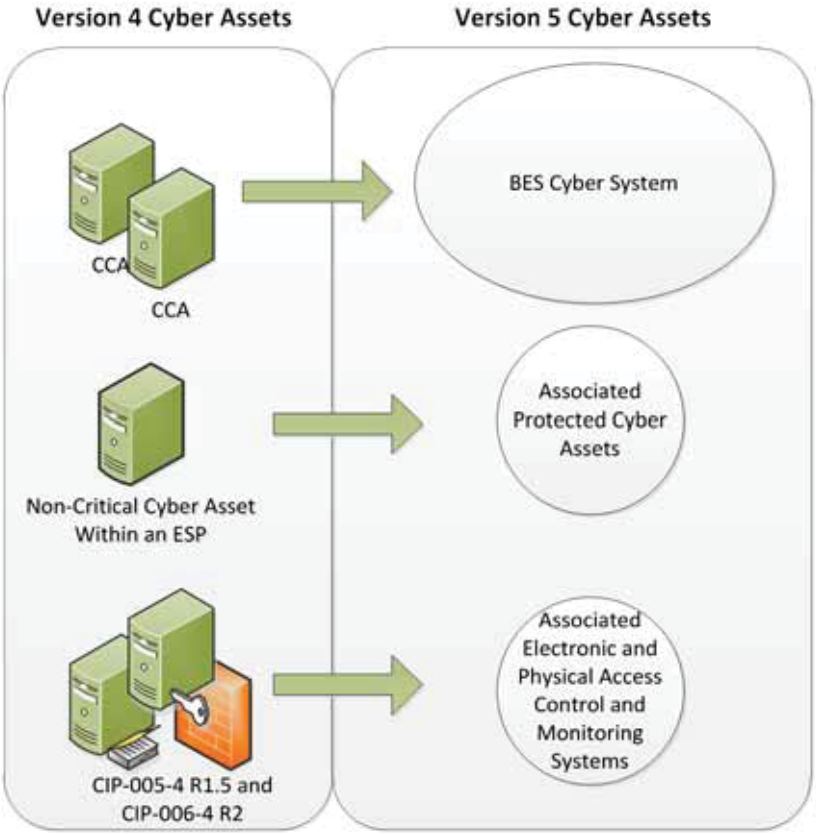

In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets. So it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to

maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify them, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems and their associated BES Cyber Assets for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Parts 1.1 to 1.4 and Parts 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the rest of Version 5 Cyber Security Standards.

Associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their proximity within the Electronic

Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems – Examples include: Electronic Access Points, Intermediate Devices, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems – Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

Rationale – R1:

BES Cyber Systems and their associated BES Cyber Assets have varying impact on the reliable operation of the BES. Once they have been identified, they must be categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to categorize these BES Cyber Systems in accordance with their impact on the BES. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

The configuration of the BES is subject to changes due to new demands and requirements for Bulk Power and to environmental changes and operational events. When changes to the BES are planned, the effect of these changes on the set of identified and categorized BES Cyber Systems must be analyzed to ensure that the adequate level of protection is still applied to them.

R1. Each Responsible Entity shall: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

1.1. Identify Facilities, Systems, or equipment that meet the criteria specified in CIP-002-5, Attachment 1 – Impact Rating Criteria Parts 1.1 to 1.4 and Parts 2.1 to 2.11;

1.2. Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;

1.3. Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;

- BES Cyber Systems which are not included in high impact or medium impact shall default to the category of low impact and do not require discrete identification; and

1.4. Review (and update as needed) the identification in Requirement R1, Parts 1.1, 1.2, and 1.3 within 60 calendar days of when a change to BES Elements or Facilities is placed into operation, which is planned to be in service for more than six calendar months and causes a change in the identification or

categorization of the BES Cyber Systems from a lower to a higher impact category.

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, Parts 1.1, 1.2 and 1.3, and a list of changes to the BES (with a date for each change) that cause a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.

Rationale – R2

The lists required by Requirement R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

R2. The Responsible Entity shall have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once each calendar year, not to exceed 15 calendar months between approvals, even if it has no identified items in Requirement R1, Parts 1.1, 1.2, or 1.3. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate review and update, where applicable, the identification and categorization of Facilities, Systems, and equipment, and their associated BES Cyber Systems and BES Cyber Assets, at least once each calendar year, not to exceed 15 calendar months between occurrences, even if it has none identified in Requirement R1, Parts 1.1, 1.2, or 1.3, as required by requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, five percent or fewer Facilities have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, 2 or fewer Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1; Or	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than five percent but less than or equal to 10 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, more than two, but fewer than four Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than 10 percent but less than or equal to 15 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, more than four, but fewer than six Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than 15 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, more than six Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1;

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer of high and medium impact BES Cyber Systems have not been identified or categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Assets, five or fewer high and medium impact BES Cyber Assets have not been identified or categorized or have been incorrectly categorized at a lower	identified according to Requirement R1, Part 1.1; Or For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Assets, more than five percent but less than or equal to 10 percent of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Assets, more than five but less than or equal to 10	identified according to Requirement R1, Part 1.1; For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Assets, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber Assets, more than 10 but less than or equal to 15	Or For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category;

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			category; Or The Responsible Entity failed to update its documentation of high and medium impact BES Cyber Assets in accordance with Requirement R1, Part 1.4 for more than 60, but less than or equal to 70 calendar days following the completion of the change.	identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with Requirement R1, Part 1.4 for more than 70, but less than or equal to 80 calendar days following the completion of the change.	identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with Requirement R1, Part 1.4 for more than 90, but less than or equal to 100 calendar days following the completion of the change.	Or The Responsible Entity failed to update its documentation of BES Cyber Systems in accordance with Requirement R1, Part 1.4 for more than 100 calendar days following the completion of the change.
R2	**Operations Planning**	**Lower**	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to Requirement R2 for	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to Requirement R2 for	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to Requirement R2 for	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to Requirement R2 for

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more than 30, but less than or equal to 40 calendar days of the latest required date.	more than 40, but less than or equal to 50 calendar days of the latest required date.	more than 50, but less than or equal to 60 calendar days of the latest required date.	more than 60 calendar days of the latest required date.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5 - Attachment 1

Impact Rating Criteria

1. High Impact Rating (H)

Each BES Cyber System used by and located at:

1.1. Each Control Center, backup Control Center, and associated data centers used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center, backup Control Center, and associated data centers used to perform the functional obligations of the Balancing Authority 1) for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection or 2) that includes control of one or more of the generation assets that meet criteria 2.3, 2.6, and 2.9.

1.3. Each Control Center, backup Control Center, and associated data centers used to perform the functional obligations of the Transmission Operator, that includes control of one or more of the assets that meet criteria 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center, backup Control Center, and associated data centers used to perform the functional obligations of the Generation Operator that includes control 1) for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection or 2) that includes control of one or more of the generation assets that meet criteria 2.3, 2.6, and 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1, above, associated with the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator, as necessary, to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher.

2.5. Transmission Facilities at a single station or substation that are operating between 200 kV and 499 kV, are connected to three or more other Transmission stations or substations, and which possess "aggregate weighted values" exceeding 3000. The "aggregate weighted value" for a Transmission Facility is determined by summing the "weight value per line" shown in the table below for each incoming or outgoing BES Transmission Line that is connected to another Transmission station or substation.

Voltage Value of a Line	Weight Value per Line
100kV to 199 kV	0 (not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, Parts 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching Systems that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each System or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS), as required by its regional load shedding program.

2.11. Control Centers and associated data centers not included in High Impact Rating (H), above, that: (1) perform the functional obligations of Balancing Authority or Transmission Operator, or (2) control an aggregate highest rated net Real Power

capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.

3. Low Impact Rating (L)

Each BES Cyber System associated with:

3.1. BES Facilities not categorized in Section 1 as having a High Impact Rating (H) or Section 2 as having a Medium Impact Rating (M).

3.2. Blackstart Resources.

3.3. Elements in the Cranking Path and initial switching requirements.

BES Cyber Systems that are not included in high impact and medium impact shall default to the category of low impact and do not require discrete identification.

Guidelines and Technical Basis

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-5. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	LSE	GOP	GO
Dynamic Response		X	X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X	X
Controlling Frequency		X					X	X
Controlling Voltage			X	X	X	X		X
Managing Constraints	X		X				X	
Monitoring and Control			X				X	
Restoration			X				X	
Situation Awareness	X	X	X				X	
Inter-Entity coordination	X	X	X	X			X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, x-formers, generators (TO, TOP, GO, GOP)
  - Zone protection for breaker failure (TO, TOP)
  - Breaker protection (TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays & breakers, possibly software (TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP,LSE)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP,LSE)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA) (RC)

- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP,LSE)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP,LSE)
- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)

- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP)
- Coordination

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day & Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers and Load Serving Entities

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Similarly, it is expected that only Load-Serving Entities that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. These qualifications are based on the requirements for registration as a Load Serving Entity. Additional qualifications for thresholds in Attachment 1, as specified in Section 4 of CIP-002, also apply.

Requirement R1:

R1 implements the methodology for the categorization of BES Cyber Systems and their associated BES Cyber Assets according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact that the Facilities, Systems and equipment that these BES Cyber Systems support, on the reliable operation of the BES.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for Facilities, Systems and equipment not specified in Parts 1.1 – 1.4 and Parts 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1. While the criteria are based on the scope of the BES Facilities, Systems and equipment, this is used here as a measure of the impact of the BES Cyber System for the purpose of categorization.

- When the drafting team uses the term "Facilities", it leaves some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities

should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers and associated data centers, that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generation Operator (GOP), as defined in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Parts 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named Functional Entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are parts 2.1, 2.3, 2.6, 2.9, and 2.11.

- Part 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of generation at a single plant for a unit or group of units with capability higher than 1500 MW are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In Part 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator as necessary to avoid BES Adverse Reliability Impacts in the long term planning horizon are categorized as medium impact. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  In the specification of the "long-term planning horizon," in this criterion, the drafting team sought to ensure that such BES Facilities would be designated in the time horizon described in the NERC document "Time Horizons," which defines long-term planning horizon as "a planning horizon of one year or longer."

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, or a Category D contingency as defined in TPL-004, then BES Cyber Systems for that unit are categorized as medium impact.

- Part 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Part 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for Generation Owners and Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- Part 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Transmission Operator or Balancing Authority, and Generation Operator for an aggregate generation of 300 MW or higher, and which have not already included in Part 1. The value of 300 MW is the same value used for UFLS and UVLS. This ensures that Control Centers for significant impact are included. Smaller Control Centers that qualify for the definition of generation Control Centers, but which are really controlling local generation for small downstream generation facilities and do not meet the 300 MW threshold are categorized as low impact.

Transmission

- Parts 2.2, 2.4-2.11 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Part 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- Part 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

  It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Part 1.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it doesn't significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Part 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.

- Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

- 230 kV –> 700 MVA
- 345 kV –> 1,300 MVA
- 500 kV –> 2,000 MVA
- 765 kV –> 3,000 MVA

In the case of autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers would not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Part 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

- Part 2.7 is sourced from the NUC-001 NERC standard for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Part 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Parts 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon).

- Part 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Part 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Part 2.12, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those Under Frequency Load Shedding (UFLS) facilities and Systems and Under Voltage Load Shedding (UVLS) Systems and Elements that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. These include automated Under Frequency Load Shedding Systems or Under Voltage Load Shedding Systems that are capable of load shedding 300 MW or more. It should be noted that those qualifying Systems which require a human operator to arm the System, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW rating for the preceding 12 months to account for seasonal fluctuations.

  Within an operational environment, the drafting team understands that the real-time impact to the Bulk Electric System of a loss of load, or the equivalent amount of generation, will be similar, with loss of load resulting in a frequency high condition and a loss of generation resulting in a frequency low condition. This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold.

  In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market.

- Part 2.11 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of Balancing Authorities or Transmission Operators not already categorized as high impact and at generation Control Centers that control generation of 300 MW or more. These include Control Centers for Transmission Owners which perform the function obligation of a Transmission Operator.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that these BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

  Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

  BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.

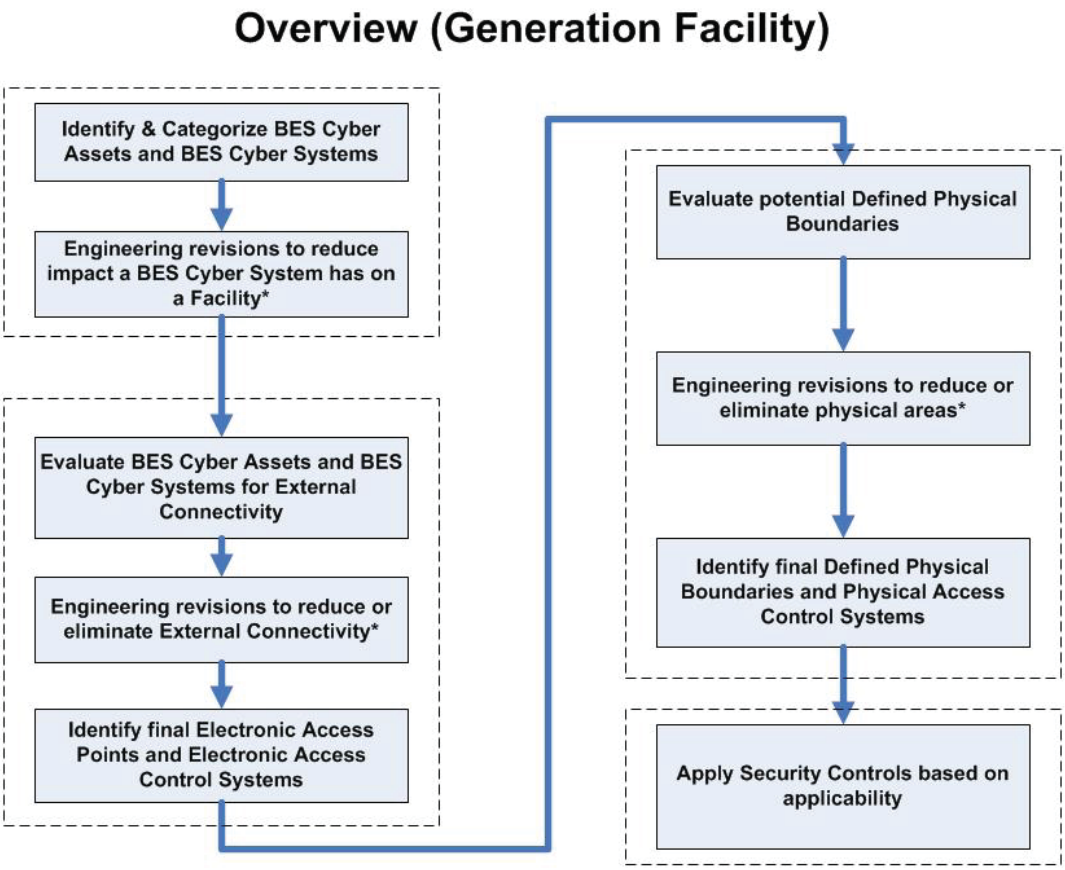

*** - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.**

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (~~A first posting of Version 5~~)~~ was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards, with some changes, and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center~~"~~."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a ~~responsible entity~~ Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification~~-~~.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — BES Cyber ~~Asset and BES Cyber~~ System Categorization

2. **Number:** CIP-002-5

3. **Purpose:** To identify and categorize BES Cyber ~~Assets and BES Cyber~~ Systems ~~that execute or enable functions essential to reliable operation of the BES,~~and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber ~~Assets~~Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems ~~could have on the reliability of~~support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities ~~that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~ **described in 4.2.2**

   - ~~A UFLS program required by a NERC or Regional Reliability Standard~~
   - ~~A UVLS program required by a NERC or Regional Reliability Standard~~
   - ~~A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard~~
   - ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
   - ~~Its Transmission Operator's restoration plan~~

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities ~~that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~ **described in 4.2.1**

   - ~~A UFLS program required by a NERC or Regional Reliability Standard~~

- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.94.1.7 Reliability Coordinator

4.1.104.1.8 Transmission Operator

4.1.114.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilitiesof the UFLS or UVLS Systems that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- **4.2.1** A UFLSa Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution ProvidersProvider: One or more Facilities that are part of any of the following systemsof the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLSor UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission where the Special Protection System required by a NERC or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan
- All other A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities~~:~~ listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

5. Background:

This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems ~~and BES Cyber Assets~~ based on ~~their~~the impact ~~on the real-time~~of their associated Facilities, Systems, and equipment; which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System ~~(BES)~~. Several concepts provide the basis for the approach to the standard.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.

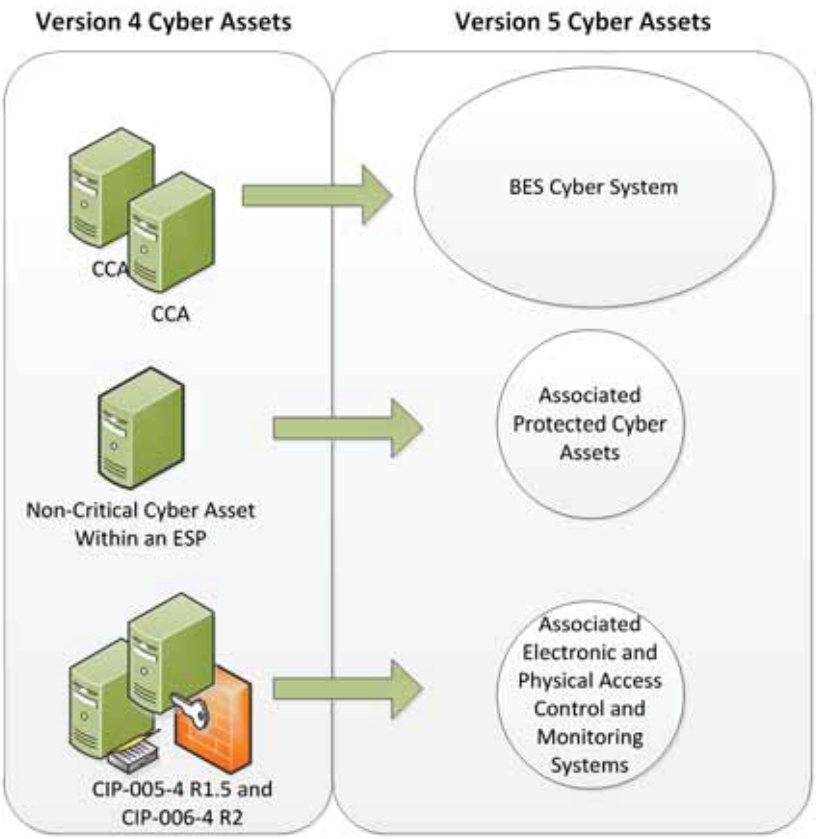

In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets~~.~~ (as that term is used in Version 4). The CIP Cyber Security Standards use ~~this~~the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets. So it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or ~~they~~it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System

boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

~~**BES Reliability Operating Services**~~

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber ~~Assets and BES Cyber~~ Systems that would impact the reliable operation of the BES. In order to identify them, Responsible Entities determine whether the BES Cyber ~~Assets~~Systems perform or support any BES ~~Reliability Operating Service. These services are functions that provide services~~reliability function according to those reliability tasks identified for ~~the reliable operation of the BES and are based on the functions defined~~functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber ~~Assets~~Systems and their associated BES Cyber ~~Systems~~Assets that perform or support ~~BES Reliability Operating Services.~~the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the ~~reliability and operability~~reliable operation of the BES. To provide a better defined time horizon than "~~real~~Real-time~~",~~," BES Cyber Assets are those ~~cyber assets~~Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the ~~BES Reliability Operating Services~~reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES ~~cyber assets~~Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems ~~and their BES Cyber Assets~~ into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems and their associated BES Cyber Assets for those in the ~~High~~high impact and ~~Medium~~medium impact categories. All ~~other~~ BES Cyber Systems ~~are deemed~~for Facilities not included in Attachment 1 – Impact Rating Criteria, Parts 1.1 to 1.4 and Parts 2.1 to 2.11 default to be ~~Low Impact~~low impact.

This general process of categorization of BES Cyber Systems ~~and BES Cyber Assets~~ based on impact on the ~~BES Reliability Operating Services~~reliable operation of the BES is consistent with risk management approaches for the purpose of application of

cyber security ~~controls~~requirements in the rest of Version 5 ~~cyber~~ Cyber Security Standards.

Associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their proximity within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security ~~standards.~~control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems – Examples include: Electronic Access Points, Intermediate Devices, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems – Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

~~Rationale – R1:~~

~~Cyber Assets and Cyber Systems have varying impact on the reliability and operability of the BES. Once they have been identified, they must be categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. Attachment I provides a set of "bright-line" criteria that the Responsible Entity must use to categorize these BES Cyber Assets and BES Cyber Systems in accordance with their impact on the BES. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.~~

~~The configuration of the BES is subject to changes due to new demands and requirements for Bulk Power and to environmental changes and operational events. When changes to the BES are planned, the effect of these changes on the set of identified and categorized BES Cyber Assets and BES Cyber Systems must be analyzed to ensure that the adequate level of protection is still applied to them.~~

B. Requirements and Measures

Rationale – R1:

BES Cyber Systems and their associated BES Cyber Assets have varying impact on the reliable operation of the BES. Once they have been identified, they must be categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to categorize these BES Cyber Systems in accordance with their impact on the BES. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

The configuration of the BES is subject to changes due to new demands and requirements for Bulk Power and to environmental changes and operational events. When changes to the BES are planned, the effect of these changes on the set of identified and categorized BES Cyber Systems must be analyzed to ensure that the adequate level of protection is still applied to them.

R1. Each Responsible Entity ~~that owns BES Cyber Assets and BES Cyber Systems~~ shall ~~identify and categorize its High and Medium~~: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

1.1. Identify Facilities, Systems, or equipment that meet the criteria specified in CIP-002-5, Attachment 1 – Impact Rating Criteria Parts 1.1 to 1.4 and Parts 2.1 to 2.11;

1.2. Identify each high impact BES Cyber ~~Assets~~System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment ~~1~~1 – Impact ~~*Categorization of*~~Rating Criteria;

1.3. Identify each medium impact BES Cyber ~~*Assets*~~System and its associated BES Cyber Asset(s) used for the Facilities, Systems~~. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed~~, or equipment identified in Requirement R1 Part 1.1 according to ~~be Low~~the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;

~~**R1.**~~• BES Cyber Systems which are not included in high impact or medium impact shall default to the category of low impact and do not require discrete identification~~. *[Violation Risk Factor: High][Time Horizon: Operations Planning]*~~; and

~~Rationale – R2~~

~~The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The mis-categorization or non-categorization of a BES Cyber System or BES Cyber Asset can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.~~

Rationale – R2

The lists required by Requirement R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

~~1.1.~~1.4. ~~Update~~Review (and update as needed) the identification in Requirement R1, Parts 1.1, 1.2, and ~~categorization~~1.3 within ~~30~~60 calendar days of when a change to BES Elements ~~and~~or Facilities is placed into operation, ~~that~~which is ~~intended~~planned to be in service for more than ~~6~~six calendar months and ~~that~~ causes a change in the identification or categorization of the BES Cyber ~~Assets or BES Cyber~~ Systems from a lower to a higher impact category.

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists ~~identifying the categorization of each of its BES Cyber Assets and BES Cyber Systems in the High and Medium categories as~~ required ~~in R1~~ by Requirement R1, Parts 1.1, 1.2 and 1.3, and a list of changes to the BES (with a date for each change) that cause a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.~~ Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.~~

R2. The Responsible Entity shall have its CIP Senior Manager or delegate approve the ~~identification and categorization~~identifications required by Requirement R1 ~~initially upon the effective date of the standard and~~ at least once each calendar year ~~thereafter~~, not to exceed 15 calendar months between approvals, even if it has no

identified ~~High~~items in Requirement R1, Parts 1.1, 1.2, or ~~Medium BES Cyber Assets or BES Cyber Systems~~1.3. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning~~]~~].*

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate review and update, where applicable, the identification and categorization of ~~BES Cyber Assets~~Facilities, Systems, and equipment, and their associated BES Cyber Systems and BES Cyber ~~Systems initially upon the effective date of the standard and~~ Assets, at least once each ~~subsequent~~ calendar year, not to exceed 15 calendar months between occurrences, even if it has ~~no~~none identified ~~High or Medium BES Cyber Assets~~in Requirement R1, Parts 1.1, 1.2, or ~~BES Cyber Systems. (~~1.3, as required by requirement R2~~)~~.

~~B.~~C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity~~; or~~
- ~~If the Responsible Entity works for~~ shall serve as the Compliance Enforcement Authority ("CEA") unless the ~~Regional Entity, then the~~ applicable entity is owned, operated, or controlled by the Regional Entity ~~will establish an agreement with~~. In such cases the ERO or ~~another~~a Regional entity approved by ~~the ERO and FERC (i.e., another Regional Entity) to be responsible for compliance enforcement.~~
- ~~If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and~~ FERC or other applicable governmental ~~authorities shall serve as the Compliance Enforcement Authority.~~
- ~~If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC~~authority shall serve as the ~~Compliance Enforcement Authority~~CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was ~~complaint~~compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until ~~found compliant~~mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R 1	Operations Planning	High	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, five percent or fewer Facilities have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, 2 or fewer Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1; Or For Responsible Entities	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than five percent but less than or equal to 10 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, more than two, but fewer than four Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than 10 percent but less than or equal to 15 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, more than four, but fewer than six Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part	For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than 15 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1; Or For Responsible Entities with a total of 40 or fewer Facilities, more than six Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1; Or For Responsible Entities

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			with more than a total of 100 ~~High~~high and ~~Medium Impact~~medium impact BES Cyber Systems, five percent or fewer of high and medium impact BES Cyber Systems have not been identified or categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Assets, ~~5%~~five or fewer ~~of High~~high and ~~Medium Impact~~medium impact BES Cyber Assets have not been identified or categorized or have been incorrectly categorized at a lower	1.1; Or For Responsible Entities with more than a total of 100 ~~High~~high and ~~Medium Impact~~medium impact BES Cyber Assets, more than ~~5%~~five percent but less than or equal to 10~~%~~ percent of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer ~~High~~high and ~~Medium Impact~~medium impact and BES Cyber Assets, more than ~~5~~five but less than or equal to 10 identified BES Cyber Assets have not been	1.1; For Responsible Entities with more than a total of 100 ~~High~~high or ~~Medium Impact~~medium impact BES Cyber Assets, more than 10~~%~~ percent but less than or equal to 15~~%~~ percent of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer ~~High~~high or ~~Medium Impact~~medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been	with more than a total of 100 ~~High~~high and ~~Medium Impact~~medium impact BES Cyber ~~Assets~~Systems, more than 15~~%~~ percent of identified BES Cyber ~~Assets~~Systems have not been categorized or have been incorrectly categorized at a lower category; Or For Responsible Entities with a total of 100 or fewer ~~High~~high and ~~Medium Impact~~medium impact BES Cyber ~~Assets~~Systems, more than 15 identified BES Cyber ~~Assets~~Systems have not been categorized or have been incorrectly categorized at a lower category;

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			category; ~~Or~~ ~~For Responsible Entities with a total of 100 or fewer High and Medium Impact BES Cyber Assets, 5 or fewer High and Medium Impact BES Cyber Assets have not been identified or categorized or have been incorrectly categorized at a lower category;~~ Or The Responsible Entity failed to update its documentation of ~~High~~high and ~~Medium Impact~~medium impact BES Cyber Assets in accordance with ~~part~~Requirement R1, Part 1.~~1~~4 for more than ~~30~~60, but less than or equal to ~~40~~70 calendar	categorized or have been incorrectly categorized at a lower category; Or The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with ~~part~~Requirement R1, Part 1.~~1~~4 for more than ~~40~~70, but less than or equal to ~~50~~80 calendar days following the completion of the change.	categorized or have been incorrectly categorized at a lower category; Or The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with ~~part~~Requirement R1, Part 1.~~1~~4 for more than ~~50~~90, but less than or equal to ~~60~~100 calendar days following the completion of the change.	Or The Responsible Entity failed to update its documentation of BES Cyber ~~Assets~~Systems in accordance with ~~part~~Requirement R1, Part 1.~~1~~4 for more than ~~60~~100 calendar days following the completion of the change.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			days following the completion of the change.			
R 2	Operations Planning	Lower	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to ~~requirement~~Requirement R2 for more than 30, but less than or equal to 40 calendar days of the latest required date.	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to ~~requirement~~Requirement R2 for more than 40, but less than or equal to 50 calendar days of the latest required date.	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to ~~requirement~~Requirement R2 for more than 50, but less than or equal to 60 calendar days of the latest required date.	The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager according to ~~requirement~~Requirement R2 for more than 60 calendar days of the latest required date.

~~C.~~D. Regional Variances

None.

~~D.~~E. Interpretations

None.

~~E.~~F. Associated Documents

None.

CIP-002-5 - Attachment ~~1~~1

~~**Impact Categorization of BES Cyber Assets and BES Cyber Systems**~~

Impact Rating Criteria

1. High Impact Rating (H)

Each BES Cyber ~~Asset or BES Cyber~~ System ~~that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services~~ used by and located at:

1.1. Each Control Center ~~or~~, backup Control Center, and associated data centers used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center ~~or~~, backup Control Center, and associated data centers used to perform the functional obligations of the Balancing Authority 1) for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection or 2) that includes control of one or more of the generation assets that meet criteria 2.3, 2.6, and 2.9.

1.3. Each Control Center ~~or~~, backup Control Center, and associated data centers used to perform the functional obligations of the Transmission Operator ~~or Transmission Owner~~, that includes control of one or more of the assets ~~identified in~~ that meet criteria 2.2, 2.4, 2.5, 2.~~6, 2.~~7, 2.8, 2.9, or 2.10~~, 2.11 or 2.12 below~~.

1.4 Each Control Center ~~or~~, backup Control Center, and associated data centers used to perform the functional obligations of the Generation Operator that includes control 1) for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection or 2) that includes control of one or more of the generation assets ~~identified in~~that meet criteria 2.~~1, 2.~~3, 2.~~4, or~~6, and 2.~~12, below~~9.

2. Medium Impact Rating (M)

Each BES Cyber ~~Asset or BES Cyber~~ System, not included in Section 1, above, ~~that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for~~associated with the following:

2.1. ~~**2.1.** Generation~~Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. ~~**2.2.** An~~Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate ~~net~~ Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. ~~**2.3.**~~ Each generation Facility that its Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator, as necessary, to avoid ~~BES~~an Adverse Reliability ~~Impacts~~Impact in the ~~long-term~~ planning horizon~~.~~ of more than one year.

~~**2.4.** Each Blackstart Resource identified in its Transmission Operator's restoration plan.~~

~~**2.5.** The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource~~

- ~~Up to and including the first interconnection point of the generation unit(s) to be started, or~~
- ~~up to the point on the Cranking Path where two or more path options exist and including any single failure points in the Cranking Path to and including the first interconnection point of the generation unit(s) to be started, or~~
- ~~up to and including the point on the Cranking Path where two or more path options exist to two or more independent generation unit(s) to be started as identified in its Transmission Operator's restoration plan.~~

2.4. ~~**2.6.**~~ Transmission Facilities operated at 500 kV or higher.

2.5. ~~**2.7.**~~ Transmission Facilities ~~operating at 200 kV or higher, but at less than 500 kV,~~ at a single station or substation that ~~is~~ are operating between 200 kV and 499 kV, are connected to three or more ~~transmission~~ other Transmission stations or substations ~~and where the "total weighted aggregate value" of all~~, and which possess "aggregate weighted values" exceeding 3000. The "aggregate weighted value" for a Transmission Facility is determined by summing the "weight value per line" shown in the table below for each incoming or outgoing BES Transmission ~~Lines at a single~~Line that is connected to another Transmission station or substation ~~operated at 200 KV or higher connected to other transmission stations or substations, including incoming and outgoing lines, exceeds a value of 3,000. The following "weight value per line" operated at the associated voltage value of a line will be used for the determination of the total weighted aggregate value~~.

Voltage Value of a Line	Weight Value per Line
100kV to 199 kV	0 (not applicable)
200 kV to 299 kV	700

300 kV to 499 kV	1300

~~2.8.~~

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning ~~Authority~~Coordinator or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

~~In the WECC Region, Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of SOLs and their contingencies for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System".~~

~~2.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs), and their associated contingencies.~~

~~In the WECC Region, Flexible AC Transmission Systems (FACTS), at a single station or substation location that are identified by its Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of SOLs and their contingencies for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System."~~

2.7. ~~2.10.~~ Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. ~~2.11.~~ Transmission Facilities providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, Parts 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching ~~system~~Systems that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations~~.~~ for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

~~In the WECC Region, each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed,~~

~~degraded, misused or otherwise rendered unavailable, would cause one or more System Operating Limits (SOLs) violations for transmission paths listed in the most current Table titled "Major WECC Transfer Paths in the Bulk Electric System" and each RAS listed in the most current table titled " Major WECC Remedial Action Schemes (RAS)."~~

2.10. ~~**2.12.** Each system or Facility that performs automatic load shedding~~Each System or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS~~)~~), as required by its regional load shedding program.

2.11. ~~**2.13.**~~ Control Centers and associated data centers not included in High Impact Rating (H), above, that: (1) perform ~~(1)~~ the functional obligations of ~~Transmission Operators~~Balancing Authority or Transmission ~~Owners;~~Operator, or (2) ~~generation~~ control ~~centers that control~~an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.

3. Low Impact Rating (L)

~~All other~~Each BES Cyber ~~Assets and~~ System associated with:

3.1. BES ~~Cyber Systems~~ Facilities not categorized in Section 1 as having a High Impact Rating (H) or Section 2 as having a Medium Impact Rating (M).

3.2. Blackstart Resources.

3.3. Elements in the Cranking Path and initial switching requirements.

BES Cyber Systems that are not included in high impact and medium impact shall default to the category of low impact and do not require discrete identification.

Guidelines and Technical Basis

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact ~~one or more~~the reliable operation of the BES ~~**Reliability Operating Services**." The new term BES Reliability Operating Service is a defined NERC Glossary term that in turn includes a number of defined named BES Reliability Operating Services. These named, defined services include:~~."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-5. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration performs which reliability ~~operations~~operating service, ~~which determines what each entity needs~~as a process to ~~address with their CIP program.~~identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable ~~Reliability Operations Services~~reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	LSE	GOP	GO
Dynamic Response		X	X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X	X
Controlling Frequency		X					X	X
Controlling Voltage			X	X	X	X		X

Managing Constraints	X		X				X	
Monitoring and Control			X				X	
Restoration			X				X	
Situation Awareness	X	X	X				X	
Inter-Entity coordination	X	X	X	X			X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES ~~elements~~Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that ~~should~~may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, x-formers, generators (TO, TOP, GO, GOP)
  - Zone protection for breaker failure (TO, TOP)
  - Breaker protection (TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays & breakers, possibly software (TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP,LSE)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP,LSE)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA) (RC)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP,LSE)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP,LSE)
- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor ~~Flowgates~~Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES ~~elements~~Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP)
- Coordination

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include~~, but are not limited to~~:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day & Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination ~~and Communication~~

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include~~, but are not limited to~~:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers and Load Serving Entities

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution

Provider and on the requirements applicable to Distribution Providers in NERC ~~standard~~Standard EOP-005.

Similarly, it is expected that only Load~~-~~-Serving Entities that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. These qualifications are based on the requirements for registration as a Load Serving Entity. Additional qualifications for thresholds in Attachment 1, as specified in Section 4 of CIP-002, also apply.

Requirement R1:

R1 implements the methodology for the categorization of BES Cyber Systems and their associated BES Cyber Assets according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the ~~systems~~Systems are assumed to be vulnerable) and a probability of threat of 1 (100~~%).~~ percent). The criteria in ~~attachment~~Attachment 1 provide a measure of the impact that the Facilities, Systems and equipment that these BES Cyber Systems support, on the ~~reliability and operability~~reliable operation of the BES.

Responsible Entities are required to identify and categorize those ~~systems~~ BES Cyber Systems that have high and medium impact. ~~Other BES~~ BES Cyber Systems for Facilities, Systems and ~~BES Cyber Assets are deemed~~equipment not specified in Parts 1.1 – 1.4 and Parts 2.1 – 2.11 default to ~~be~~ low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System~~.~~ as measured by the bright-line criteria defined in Attachment 1. While the criteria are based on the scope of the BES ~~asset~~Facilities, Systems and equipment, this is used here as a measure of the impact of the BES Cyber System for the purpose of categorization.

- When the drafting team uses the term "Facilities", it leaves some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that ~~support~~supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that

supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that ~~support~~supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems~~-~~. Generation Facilities are separately discussed in the Generation section below.

- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- ~~A~~It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers and associated data centers, that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), ~~Transmission Owner (TO)~~ or Generation Operator (GOP), as defined in the NERC Functional Model~~.~~, and as scoped by the qualification in Attachment 1, Parts 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above~~-~~-named Functional Entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations ~~must~~would be subject to categorization as ~~High Impact.~~high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment ~~1, Medium Impact~~1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are parts 2.1, 2.3, 2.~~4~~6, 2.~~5, 2.11~~9, and 2.~~13~~11.

- Part 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance~~".~~." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency

Reserve to cover the most severe single contingency.” The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of generation at a single plant for a unit or group of units with capability higher than 1500 MW are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In ~~part~~Part 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator as necessary to avoid BES Adverse Reliability Impacts in the long term planning horizon are categorized as ~~Medium Impact.~~medium impact. These Facilities may be designated as “Reliability Must Run~~”~~,” and this designation is distinct from those generation Facilities designated as “must run” for market stabilization purposes. Because the use of the term “must run” creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  In the specification of the “long-term planning horizon~~”~~,” in this criterion, the drafting team sought to ensure that such BES ~~facilities~~Facilities would be designated in the time horizon described in the NERC document “Time Horizons~~”~~,” which defines long-term planning horizon as “a planning horizon of one year or longer~~”~~.”

  If it is determined through ~~system~~System studies that a unit must run in order to preserve the reliability of the BES, such as due to a ~~category~~Category C3 contingency as defined in TPL-003, or a ~~category~~Category D contingency as defined in TPL-004, then BES Cyber Systems for that unit ~~must be~~are categorized as ~~Medium Impact~~medium impact.

  ~~In part 2.4, BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan are categorized as Medium Impact. NERC standard EOP-005-2 requires the Transmission Operator to have~~

~~a Restoration Plan and to list its Blackstart Resources in its plan as well as requirements to test these Resources.~~

- Part 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- ~~This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired. While the definition of Blackstart Resource includes the fact that it is in a Transmission Operator's Restoration Plan, the drafting team included the term in the criterion for clarity.~~

  ~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."~~

- ~~Part 2.5 categorizes BES Cyber Systems for Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, with the qualifications stated in the requirement part. This criterion is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started. The drafting team further qualified the Facilities to be designated as subject to BES Cyber System categorization as only those in the Cranking Path up to the point where two or more paths exist to the units to be started and subject to the qualifications in the requirement part.~~

  ~~Distribution Providers should note that they may have BES Cyber Systems that must be categorized as Medium Impact if they have facilities listed in the Transmission Operator's Restoration Plan.~~

  ~~The following illustrates the parts of the Cranking Path that are subject to CIP Cranking Path criterion.~~

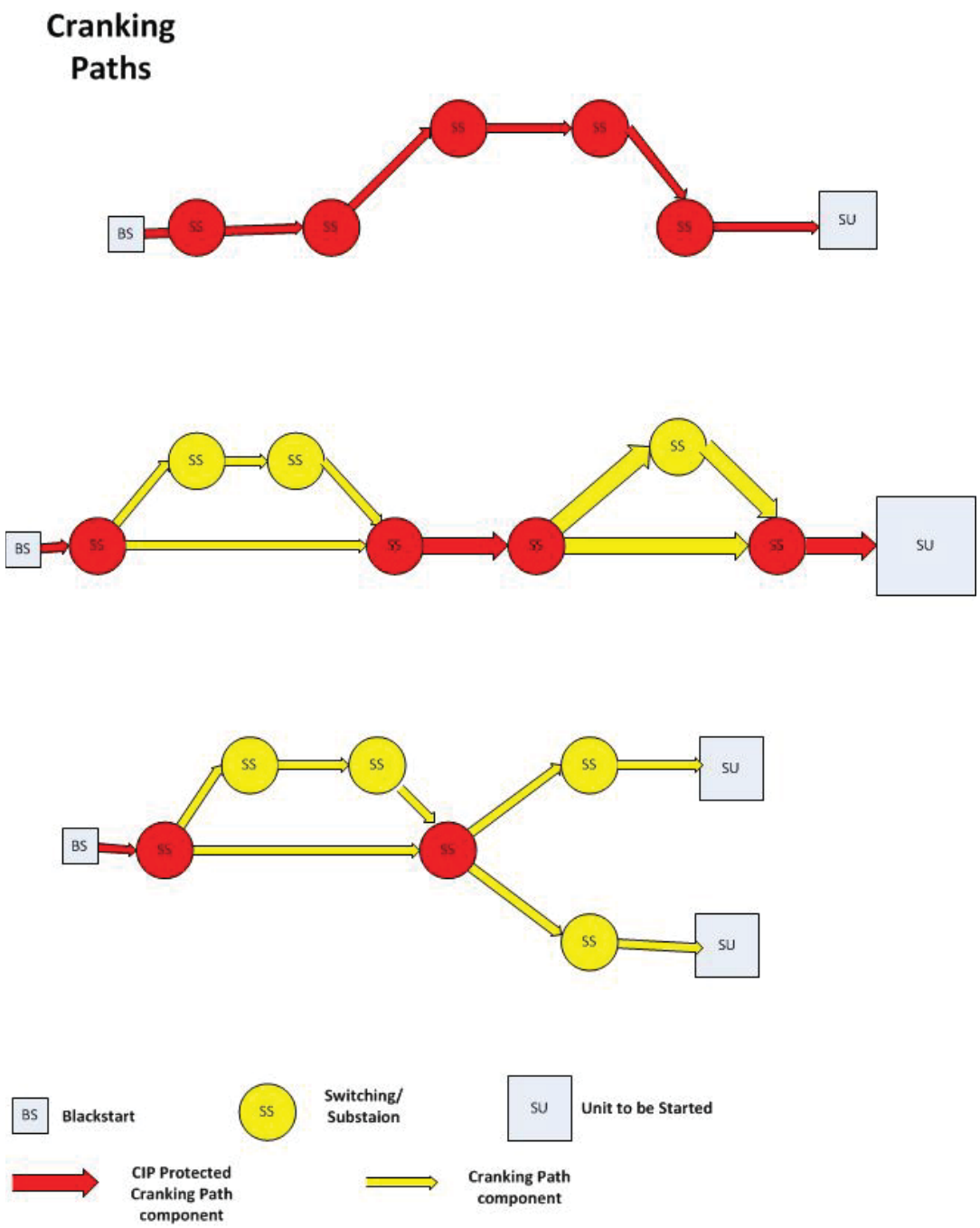

- Part 2.~~11~~9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as ~~Medium Impact.~~medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for~~.~~ Generation Owners and Operators which own BES Cyber Systems for such ~~systems~~Systems and schemes ~~must~~ designate them as ~~Medium Impact~~medium impact.

- Part 2.~~13~~11 categorizes as ~~Medium Impact~~medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Transmission Operator or Balancing Authority, and Generation Operator for an aggregate generation of 300 MW or higher~~.~~, and which have not already included in Part 1. The value of 300 MW is the same value used for UFLS and UVLS. This ensures that Control Centers for significant impact are included. Smaller Control Centers that qualify for the definition of generation Control Centers, but which are really controlling local generation for small downstream generation facilities and do not meet the 300 MW threshold are categorized as ~~Low~~low impact.

Transmission

Parts 2.~~1, 2.~~, 2~~,~~ .4-2.~~5-2.13~~11 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a ~~system~~System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). ~~For the WECC region where IROLs are not defined, alternative criteria are defined.~~

- ~~Part 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. In the case of BES Cyber Systems and BES Cyber Assets owned by Transmission Owners and Operators, this part identifies as Medium Impact those BES Cyber Systems for Transmission Facilities that provide the generation interconnection for Generation of 1500 MW or more to the Transmission system. The intent is to ensure the availability of Facilities necessary to support those generation facilities.~~

- Part 2.2 includes BES Cyber Systems for those Facilities in Transmission ~~systems~~Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- ~~In Part 2.5, the intent is to ensure that BES Cyber Systems for the Cranking Paths and other BES Transmission Facilities required to support the Transmission Operator's restoration plan required by EOP-005-2 receive consideration for protection from cyber threats. Transmission Owners and Operators own and operate a large number of these Facilities. EOP-005-2 specifies Facilities that comprise the "Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started".~~

  ~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."~~

- ~~Part 2.6~~Part 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the ~~Medium Impact~~medium impact category.

  It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Part 1.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface~~".~~." This collector bus would not be a facility for a ~~Medium Impact~~medium impact BES Cyber System because it doesn't significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Part 2.~~7~~5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

  - 230 kV –> 700 MVA
  - 345 kV –> 1,300 MVA
  - 500 kV –> 2,000 MVA
  - 765 kV –> 3,000 MVA

  ~~Parts 2.8 and 2.9~~In the case of autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location. In most cases, Responsible Entities would probably

consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers would not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Part 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

~~Alternate thresholds are used for WECC, where IROLs are not used.~~

- Part 2.~~10~~7 is sourced from the NUC-001 NERC standard for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown~~".~~." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Part 2.~~11~~8 designates as ~~Medium Impact~~medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Parts 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon).

- Part 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching ~~systems~~Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

~~For the WECC region, alternative thresholds are defined because IROLs are not defined for the region.~~

- Part 2.~~12~~10 designates as ~~Medium Impact~~medium impact those BES Cyber Systems for ~~systems~~Systems or ~~Facilities~~Elements that ~~are capable of performing~~perform automatic ~~load~~Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of ~~criterion~~Part 2.~~13~~12, and chose the term "Each" to represent that the criterion applied to a discrete ~~system~~System or Facility. In the drafting of this criterion, the drafting team sought to include only those ~~systems~~Systems that did not require human operator initiation, and targeted in particular those Under Frequency Load Shedding (UFLS) facilities and ~~systems~~Systems and Under Voltage Load

Shedding (UVLS) ~~facilities~~Systems and ~~systems~~Elements that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. These include automated Under Frequency Load Shedding ~~systems~~Systems or Under Voltage Load Shedding Systems that are capable of load shedding 300 MW or more. It should be noted that those qualifying ~~systems~~Systems which require a human operator to arm the ~~system~~System, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as ~~Medium Impact.~~ medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW rating for the preceding 12 months to account for seasonal fluctuations.

Within an operational environment, the drafting team understands that the real-time impact to the Bulk Electric System of a loss of load, or the equivalent amount of generation, will be similar, with loss of load resulting in a frequency high condition and a loss of generation resulting in a frequency low condition. This particular threshold (300 MW) was provided in CIP ~~version~~, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market.

- Part 2.~~13~~11 categorizes as ~~Medium Impact~~ medium impact those ~~cyber systems~~ BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of Balancing Authorities or Transmission Operators ~~and Owners Control Centers~~ not already categorized as ~~High Impact~~high impact and at generation Control Centers that control generation of 300 MW or more. These include Control Centers for Transmission Owners which perform the function obligation of a Transmission Operator.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that these BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in

Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.

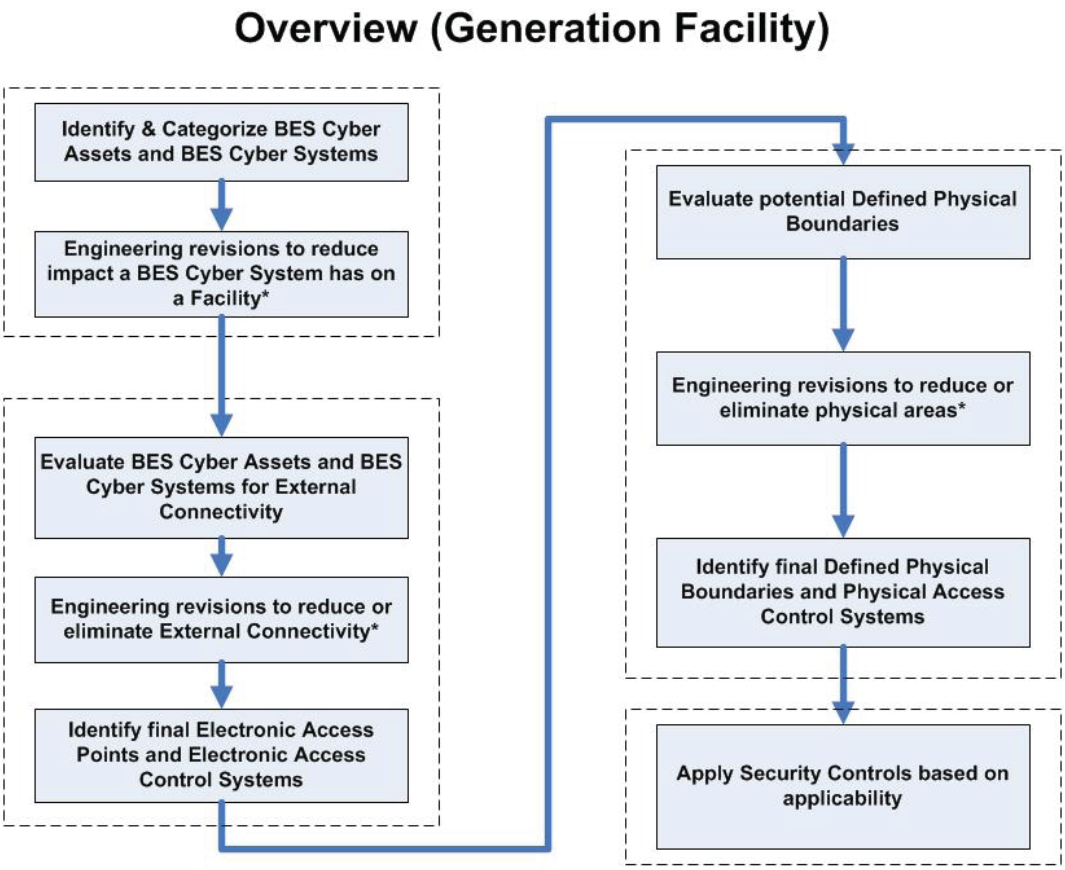

* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Update version from "3" to "4". Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

4.1.7 Reliability Coordinator

4.1.8 Transmission Operator

4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Measures provide examples of evidence to show documentation and implementation of the requirement. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

B. Requirements and Measures

Rationale – R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

R1. Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall implement one or more documented cyber security policies that address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel security;
- **1.2** Electronic Security Perimeters;
- **1.3** Interactive Remote Access;
- **1.4** Physical security;
- **1.5** System security;
- **1.6** Incident response;
- **1.7** Recovery plans;
- **1.8** Configuration change management;
- **1.9** Information protection; and
- **1.10** Provisions for declaring and responding to CIP Exceptional Circumstances.

M1. Evidence must include one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics.

Rationale – R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

R2. For BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics: *[Violation Risk Factor: Low] [Time Horizon: Operations Planning]*

- **2.1** Cyber security awareness;
- **2.2** Physical access control;
- **2.3** Electronic access control; and
- **2.4** Incident response to a BES Cyber Security Incident.

An inventory, list, or discrete identification of BES Cyber Systems is not required.

M2. Evidence must include one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics.

Rationale – R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests that the SDT consider whether the single senior manager should be a corporate officer or equivalent. The SDT believes that the requirement that the senior manager have "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence may include, but is not limited to:

- A dated and signed document from a high level official designating the name of the individual identified as the CIP Senior Manager; or
- A dated organizational chart designating the name of the individual identified as the CIP Senior Manager.

Rationale – R4:

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R4. Each Responsible Entity shall review and obtain CIP Senior Manager approval for cyber security policies identified in Requirements R1 and R2, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. Evidence may include, but is not limited to:

1. Revision history, records of review, or workflow evidence from a document management system that indicate annual review of each cyber security policy; and
2. A dated signature by the CIP Senior Manager for each cyber security policy that indicates annual approval.

Rationale – R5:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R5. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate and the date of the delegation, and approved by the CIP Senior Manager. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M5. Evidence may include, but is not limited to, a dated document, signed by the CIP Senior Manager, listing named personnel (by name or title) who are delegated the authority to approve or authorize specifically identified items.

Rationale – R6:

The intent of the requirement is to ensure that delegations are kept up-to-date and that individuals do not assume undocumented authority.

R6. Each Responsible Entity shall document any changes to the CIP Senior Manager or any delegations within thirty calendar days of the change. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M6. Evidence may include, but is not limited to, dated documentation that includes the name of the CIP Senior Manager or documentation that includes the names or titles of any delegations, that is current to within 30 days with the name or title of anyone who performed a required approval or authorization.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required Parts 1.1 to 1.10.	The Responsible Entity has not implemented any cyber security policy, Or The Responsible Entity has implemented at least one policy but has failed to address two or more of the required Parts 1.1 to 1.10.
R2	**Operations Planning**	**Medium**	**N/A**	**N/A**	The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required Parts 2.1 to 2.4.	The Responsible Entity has not implemented any cyber security policy, Or The Responsible Entity has implemented at least one policy but has failed to address two or more of the required Parts 2.1 to 2.4.
R3	**Operations**	**Medium**	**N/A**	**N/A**	**N/A**	The Responsible Entity has not identified, by

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning					name, a single senior management official ("the CIP Senior Manager") with overall authority and responsibility for leading and managing implementation of the requirements within the CIP group of standards.
R4	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity has reviewed its cyber security policy or policies, but not all of them have been approved by the CIP Senior Manager within the required time period.	The Responsible Entity has not reviewed the cyber security policy or policies and the CIP Senior Manager has not approved all of them within the required time period.
R5	**Operations Planning**	**Lower**	N/A	The Responsible Entity failed to document the approval and authorization of one delegation (by title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of two delegations (by title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of three or more delegations (by title or name of the delegate) as required.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	**Operations Planning**	**Lower**	N/A	NA	Change to one delegation was not documented within 30 calendar days of the effective date.	A change to the CIP Senior Manager, Or more than one delegation was not documented within 30 calendar days of the effective date.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the 10 topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel Security

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account Management

1.2 Electronic Security Perimeters

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points

1.3. Remote Access

- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating system and applications used to initiate the Interactive Remote Access before initiating Interactive Remote Access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s Interactive Remote Access controls

1.4 Physical Security

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress and egress

1.5 System Security

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.6 Incident Response

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.7 Recovery Plans

- Availability of spare components
- Availability of system backups

1.8 Configuration Change Management

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.9 Information Protection

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.10 Provisions for CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The SDT has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a compliance requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as

components of specific programs. The cyber security policy must cover in sufficient detail the 4 topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not necessary. The SDT also notes that in topics 2.2 and 2.3, the SDT uses the term "access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R5:

As indicated in the rationale for CIP-003-5, Requirement R5, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the Standard Drafting Team was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. As detailed in the examples provided in the Measure, a Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

Requirement R6:

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation

Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

~~**Note**: On November 21, 2011, NERC was alerted that the text contained in some of the Rationale boxes for the requirements of CIP-003-5 appeared to be incomplete.~~

~~This revised draft corrects the text box size to display all of the text (none of the text was changed).~~

~~No other changes were made to this standard or any of the other CIP V5 standards currently posted.~~

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **~~18~~24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center~~"~~."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Update version from "3" to "4". Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: ~~Standard CIP-003-5 requires that Responsible Entities have minimum~~To specify consistent and sustainable security management controls ~~in place~~that establish responsibility and accountability to protect BES Cyber ~~Assets and BES Cyber~~ Systems~~.~~ against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities ~~that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~ **described in 4.2.2**

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~
- ~~A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard~~
- ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities ~~that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~ **described in 4.2.1**

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~**4.1.7 NERC**~~

~~**4.1.8 Regional Entity**~~

~~4.1.9~~4.1.7 Reliability Coordinator

~~4.1.10~~4.1.8 Transmission Operator

~~4.1.11~~4.1.9 Transmission Owner

4.2. Facilities:

~~4.2.1~~ Load Serving Entity: One or more ~~Facilities~~of the UFLS or UVLS Systems that are part of ~~any of the following systems or programs designed, installed, and operated for the protection of the BES:~~

- **4.2.1** ~~A UFLS~~a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.
  - ~~A UVLS program required by a NERC or Regional Reliability Standard~~

4.2.2 Distribution ~~Providers~~Provider: One or more ~~Facilities that are part of any of the following systems~~of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS~~or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- ~~A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard~~
- ~~A Transmission~~ where the Special Protection System ~~required by a NERC~~ or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- ~~Its Transmission Operator's restoration plan~~
- ~~**All other**~~ A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities~~:~~ listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-~~003~~002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~**4.2.4.4** Except for R1, R5 and R6, Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems~~

5. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.~~

Measures ~~for the initial requirement are simply the documented processes themselves. Measures in the table rows~~ provide examples of evidence to show documentation and implementation of ~~specific elements required in the documented processes.~~the requirement. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e~~.~~., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards~~standards.

~~**Applicability**~~

~~Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.~~

- ~~**All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~
- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes.~~

Responsible Entities can implement common controls that meet requirements for multiple ~~High~~high and ~~Medium Impact~~medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.~~
- ~~**Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding~~

~~High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems~~

- ~~**Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.~~
- ~~**Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.~~
- ~~**Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.~~
- ~~**Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~
- ~~**Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

~~Rationale – R1:~~

~~The identification and documentation of the single CIP Senior Manager and any delegations ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43.~~

~~In FERC Order 706, paragraph 296, it requests that the SDT consider whether the single senior manager should be a corporate officer or equivalent. The SDT believes that the requirement that the senior manager have "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" ensures that the senior manager is of the sufficient position in the responsible entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.~~

B. Requirements and Measures

Rationale – R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

R1. Each Responsible Entity ~~shall identify, by name, a CIP Senior Manager. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*~~

~~**M1.** Evidence may include, but is not limited to:~~

- ~~A dated and signed document from a~~ for its high ~~level official designating the name of the individual identified as the CIP Senior Manager~~
- ~~A dated organizational chart designating the name of the individual identified as the CIP Senior Manager.~~

Rationale – R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

R2 Each Responsible Entity impact and medium impact BES Cyber Systems shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addressesaddress the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1.1.1 Personnel Securitysecurity;

1.2.1.2 Electronic Security Perimeters;

1.3.1.3 Interactive Remote Access;

1.4.1.4 Physical Securitysecurity;

1.5.1.5 System Securitysecurity;

1.6.1.6 Incident Responseresponse;

1.7.1.7 Recovery Plansplans;

1.8.1.8 Configuration Change Managementchange management;

1.9.1.9 Information Protectionprotection; and

1.10.1.10 Provisions for declaring and responding to CIP Exceptional Circumstances.

M2M1. Evidence maymust include, but is not limited to:

- One one or more documented cyber security policies, and

2.Records and evidence of processes, procedures, or plans that indicatedemonstrate the implementation of the required ten topics were implemented.

~~Rationale – R3:~~

~~Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.~~

~~R3.~~ ~~Each Responsible Entity shall review~~

Rationale – R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

R2. For BES Cyber Systems not identified as high impact or medium impact, each ~~of its~~Responsible Entity shall implement one or more documented cyber security policies ~~and obtain the approval of its CIP Senior Manager, initially upon~~that address the ~~effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.~~following topics: *[Violation Risk Factor: ~~Lower~~Low] [Time Horizon: Operations Planning]*

2.1 Cyber security awareness;

2.2 Physical access control;

2.3 Electronic access control; and

2.4 Incident response to a BES Cyber Security Incident.

An inventory, list, or discrete identification of BES Cyber Systems is not required.

M2. Evidence must include one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics.

Rationale – R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests that the SDT consider whether the single senior manager should be a corporate officer or equivalent. The SDT believes that the requirement that the senior manager have "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence may include, but is not limited to:

- A dated and signed document from a high level official designating the name of the individual identified as the CIP Senior Manager; or
- A dated organizational chart designating the name of the individual identified as the CIP Senior Manager.

Rationale – R4:

The intent of the SDT is to ensure that the responsible entity takes sufficient measures to make its cyber security policy available and accessible to personnel. It is not the intent of the SDT for the responsible entity to have the burden of proving

R4. Each Responsible Entity shall review and obtain CIP Senior Manager approval for cyber security policies identified in Requirements R1 and R2, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. Evidence may include, but is not limited to:

1. Revision history, records of review, or workflow evidence from a document management system that indicate annual review of each cyber security policy~~,~~; and
2. A dated signature by the CIP Senior Manager for each cyber security policy that indicates annual approval.

~~**Rationale – R4:**~~

~~The intent of the SDT is to ensure that the responsible entity takes sufficient measures to make its cyber security policy available and accessible to personnel. It is not the intent of the SDT for the responsible entity to have the burden of proving~~

~~**R4.** Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*~~

~~**M4.** Evidence may include, but is not limited to:~~

- ~~Policies are accessible on the corporate Intranet site~~
- ~~Documented records that policies have been provided to contactors where access to BES Cyber Systems is authorized~~
- ~~Policies are posted on company bulletin boards~~
- ~~Policies are accessible to individuals with all types of job functions that have access to BES Cyber Systems~~
- ~~Dated training records to show that individuals have received periodic training on necessary elements of the cyber security policy~~

Rationale – R5:

In FERC Order 706, paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations in order that this line of authority is clear and apparent from the documented delegations.

Rationale – R5:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R5 The . Where allowed by the CIP Senior Manager shall be responsible for all approvals and authorizations required inStandards, the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegatedspecific actions to a delegate or delegates. These delegations shall be documented (by position or , including the name or title of the delegate), dated and the date of the delegation, and approved and shall specify the authority that is being delegated.by the CIP Senior Manager. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M5. Evidence may include, but is not limited to:, a dated document, signed by the CIP Senior Manager, listing named personnel (by name or title) who are delegated the authority to approve or authorize specifically identified items.

A dated

Rationale – R6:

The intent of the requirement is to ensure that delegations are kept up-to-date and that individuals do not assume undocumented authority.

- **R6.** Each Responsible Entity shall document, signed by any changes to the CIP Senior Manager listing personnel (by title) who are delegated the authority to approve or authorize specifically identified items (i.e. substation maintenance manager may authorize unescorted physical access to substation control houses), or
- A dated document, signed by the CIP Senior Manager listing individuals who are delegated the authority to approve or authorize specific actions by requirement (i.e., 'name of individual' who may approve CIP-002-5 R3), or
- A dated document, signed by the CIP Senior Manager delegating to a named individual the authority for all approvals in CIP-002-5 and CIP-004-5 through CIP-011-1 as well as the authority to approve subsequentany delegations; a dated document, signed by the previous named individual delegating to a 3rd named individual the authority for all approvals in CIP-004-5 through CIP-011-1 as well as the authority to approve subsequent delegations; and a dated document, signed by the 3rd named individual delegating to each of the plant managers (by title) the authority for all approvals and authorizations required in CIP-004-5 through CIP-011-1 for each of the their plants, respectively.

Rationale – R6:

The intent of the SDT is to ensure that delegations are kept up-to-date and that individuals do not assume undocumented authority.

R6. Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change2. Delegation changes do not need to be reinstated

[2] Delegations do not need to be reinstated with a change in the CIP Senior Manager position or other position with delegation authority.

with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M6. Evidence may include, but is not limited to, dated documentation that includes the name of the CIP Senior Manager or documentation that includes the names or ~~positions~~titles of any delegations, that is current to within 30 days with the name or ~~position~~title of anyone who performed a required approval or authorization.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

- The Regional Entity.
- If the Responsible Entity works for shall serve as the Compliance Enforcement Authority ("CEA") unless the Regional Entity, then the applicable entity is owned, operated, or controlled by the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- For Responsible Entities that are also Regional Entities,. In such cases the ERO or a Regional Entityentity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For NERC, a third-party monitor without vested interest in the outcome for NERCauthority shall serve as the Compliance Enforcement AuthorityCEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaintcompliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliantmitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting

- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	~~N/A~~The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required Parts 1.1 to 1.10.	The Responsible Entity has not ~~identified, by name, a single senior management official ("the CIP Senior Manager") with overall authority and responsibility for leading and managing implementation~~implemented any cyber security policy, Or The Responsible Entity has implemented at least one policy but has failed to address two or more of the ~~requirements within the CIP group of standards~~required Parts 1.1 to 1.10.
R2	**Operations Planning**	**Medium**	**N/A**	**N/A**	The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the	The Responsible Entity has not implemented any cyber security policy, Or The Responsible Entity has implemented at least one

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					required ~~parts~~Parts 2.1 to 2.~~10~~4.	policy but has failed to address two or more of the required ~~parts~~Parts 2.1 to 2.~~10~~4.
R3	**Operations Planning**	~~Lower~~**Medium**	**N/A**	**N/A**	~~The Responsible Entity has reviewed its cyber security policy or policies, but not all of them have been approved by the CIP Senior Manager within the required time period.~~**N/A**	The Responsible Entity has not ~~reviewed the cyber security policy or policies and~~ identified, by name, a single senior management official (“the CIP Senior Manager~~ has not approved all~~”) with overall authority and responsibility for leading and managing implementation of ~~them~~the requirements within the ~~required time period~~ CIP group of standards.
R4	**Operations Planning**	**Lower**	N/A	N/A	The Responsible Entity has ~~made some~~reviewed its cyber security policy or	The Responsible Entity has not ~~made any individuals who have access to BES Cyber Systems aware of elements of~~reviewed the cyber security policy or

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					policies, but not all ~~individuals who~~of them have ~~access to BES Cyber Systems aware of elements of~~been approved by the ~~cyber security policies appropriate for their job function~~CIP Senior Manager within the required time period.	policies ~~appropriate for their job function.~~ and the CIP Senior Manager has not approved all of them within the required time period.
R5	**Operations Planning**	**Lower**	N/A	The Responsible Entity failed to document the approval and authorization of one delegation (by ~~position~~ title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of two delegations (by ~~position~~ title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of three or more delegations (by ~~position~~ title or name of the delegate) as required.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	**Operations Planning**	**Lower**	N/A	NA	Change to one delegation was not documented within 30 calendar days of the effective date.	A change to the CIP Senior Manager, Or more than one delegation was not documented within 30 calendar days of the effective date.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement ~~R2~~R1:

The number of policies and their specific language ~~would be~~are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the ~~ten~~10 topical areas required by CIP-003-5~~ R2~~, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In ~~this~~the case of a high-level umbrella policy, ~~it~~the Responsible Entity would be expected ~~that the entity~~to provide the high-level policy as well as the additional documentation in order to ~~prove~~demonstrate compliance with CIP-003-5~~ R2~~, Requirement R1. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

~~2~~1.1 Personnel Security

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account Management

~~2.2~~1.2 Electronic Security Perimeters

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points

~~2~~1.3. Remote Access

- Maintaining up-to-date anti-malware software before initiating ~~interactive remote access~~Interactive Remote Access
- Maintaining up-to-date patch levels for operating system and applications used to initiate the ~~interactive remote access~~Interactive Remote Access before initiating ~~interactive remote access~~Interactive Remote Access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating ~~interactive remote access~~Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s ~~interactive remote access~~Interactive Remote Access controls

~~2.4~~1.4 Physical Security

- Strategy for protecting ~~cyber assets~~Cyber Assets from unauthorized physical access

- Acceptable physical access control methods
- Monitoring and logging of physical ingress and egress

~~2.5~~1.5 System Security

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

~~2.6~~1.6 Incident Response

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

~~2~~1.7 Recovery Plans

- Availability of spare components
- Availability of system backups

~~2~~1.8 Configuration Change Management

- Initiation of change requests
- Approval of changes
- Break-fix processes

~~2~~1.9 Information Protection

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

~~2~~1.10 Provisions for CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The SDT has removed requirements relating to exceptions to a Responsible Entity's security policies since it ~~considers this~~is a general management issue that is not within the scope of a compliance requirement. The SDT considers ~~this~~it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the 4 topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not necessary. The SDT also notes that in topics 2.2 and 2.3, the SDT uses the term "access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R5:

As indicated in the rationale for CIP-003-5, Requirement R5, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the Standard Drafting Team was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. As detailed in the examples provided in the Measure, a Responsible Entity may satisfy this requirement ~~may be met~~ through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to ~~their~~its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

Requirement R6:

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated

the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-5

3. **Purpose:** To minimize the risk from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities described in 4.2.2

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   4.1.7 Reliability Coordinator

   4.1.8 Transmission Operator

   4.1.9 Transmission Owner

   4.2. Facilities:

   4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

   4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability

column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.

B. Requirements and Measures

Rationale for R1: Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R1 – Security Awareness Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	A security awareness program that, at least once each calendar quarter, conveys ongoing reinforcement of cyber security practices for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	Evidence must include the documented security awareness program, and additional evidence to demonstrate that this program was implemented. Evidence of implementation may include, but not limited to, documentation that the quarterly reinforcement has been provided. Evidence of reinforcement may include dated copies of information used to reinforce security awareness, as well as evidence of distribution such as: direct communications (for example, e-mails, memos, computer-based training); indirect communications (for example, posters, intranet, or brochures); management support and reinforcement (for example, presentations or meetings).
Reference to prior version: *CIP-004-4, R1*		**Change Rationale:** *Changed to remove the need to ensure everyone with authorized* electronic or authorized unescorted physical *access "received" ongoing reinforcement – to state that the program conveys awareness and measures that reinforcement "has been provided."* *Moved example mechanisms to guidance.* *Changed to record delivery.*	

Rationale for R2: To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:
   - The visitor control program
   - Electronic interconnectivity supporting the operation and control of BES Cyber Systems
   - Storage media as part of the handling of BES Cyber Systems information
2. Change references from Critical Cyber Assets to BES Cyber Systems

R2. Each Responsible Entity shall have a role-based cyber security training program to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*.

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Identification of each role and training required for each role.	Acceptable evidence must include a list of roles and what training is needed for each role.
Reference to prior version: NEW		**Change Rationale:** *The first thing needed in a role-based training program is to understand what roles individuals have so that the Responsible Entity can plan what training modules it needs to provide.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the cyber security policies protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material on the security controls that have been implemented to protect BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.1*		**Change Rationale:** *Removed to address cyber security issues, not the business function. The previous version was focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the physical access controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the proper use of physical access controls for BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.1 and R2.2.2*		**Change Rationale:** *Minor wording changes.*	
2.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the electronic access controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the electronic access controls to protect BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.1 and R2.2.2*		**Change Rationale:** *Minor wording changes.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the visitor control program.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the visitor control program.
Reference to prior version: *NEW*		**Change Rationale:** *No significant change from previous versions.*	
2.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on handling of BES Cyber System Information and its storage.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the handling of BES Cyber System Information, including its storage.
Reference to prior version: *CIP004-4, R2.2.3*		**Change Rationale:** *Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage media; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on identification of a potential BES Cyber Security Incident and initial notifications in accordance with the entity's incident response plan	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the identification of a potential BES Cyber Security Incident and associated notifications.
Reference to prior version: *CIP-004-4, R2.2.4 (new; implied but not stated in CIP-004-4 or CIP-008-4)*		**Change Rationale:** *Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting.*	
2.8	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on recovery plans for BES Cyber Systems.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on recovery plans for BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.4*		**Change Rationale:** *Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.9	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on response to BES Cyber Security Incidents.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the response to a BES Cyber Security Incident.
Reference to prior version: *CIP004-4, R2.2.4*		**Change Rationale:** *Minor wording changes.*	
2.10	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the electronic interconnectivity and interoperability with other Cyber Assets.
Reference to prior version: *NEW*		**Change Rationale:** *Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.*	

Rationale for R3: To ensure that personnel with authorized electronic access or authorized unescorted physical access are trained in the policies, access controls, and procedures to protect the BES Cyber Systems.

Summary of Changes: Re-organization of the training requirements into the respective requirements for "program" and "implementation" of the training.

R3. Each Responsible Entity shall implement its documented role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R3 - Cyber Security Training. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include, but is not limited to, documentation that the training was provided as defined in *CIP-004-5 Table R3 - Cyber Security Training*.

CIP-004-5 Table R3 – Cyber Security Training			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Require completion and documentation of the training specified in CIP-004-5, Requirement R2 prior to granting authorized electronic access and authorized unescorted physical access to BES Cyber Systems, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, for each individual requiring authorized electronic or authorized unescorted physical access, dated individual training records, the date authorized electronic or authorized unescorted physical access was first granted, or a dated log or documentation of when CIP Exceptional Circumstances were invoked and revoked.
Reference to prior version: *CIP004-4, R2.1*		**Change Rationale:** *Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.*	

CIP-004-5 Table R3 – Cyber Security Training			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Require completion and documentation of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	Evidence may include, but is not limited to, dated individual training records.
Reference to prior version: *CIP004-4, R2.3*		**Change Rationale:** *Updated to further define what "Annual" training means.*	

Rationale for R4: To ensure that individuals who need authorized electronic or unescorted physical access to BES Cyber Systems have been assessed for risk.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.

R4. Each Responsible Entity shall have one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M4. Evidence must include the documented personnel risk assessment program that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program.*

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	An initial personnel risk assessment ("PRA") that includes identity verification.	Acceptable evidence must include the documented personnel risk assessment program with a requirement for an initial personnel risk assessment that includes identity verification.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Addressed interpretation request in guidance. Specified that identity verification is only required for each individual's initial assessment. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.*	

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six months or more: 4.2.1. resided; 4.2.2. been employed (if applicable); and 4.2.3. attended school (if applicable). If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	Acceptable evidence must include the documented personnel risk assessment program with a requirement for a seven-year criminal history record check in accordance with this part.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.*	

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Process or criteria used to evaluate personnel risk assessments to determine when to deny authorized access.	Acceptable evidence must include the documented personnel risk assessment program with the process or criteria identified.
Reference to prior version: *NEW*		Change Rationale: *There should be documented criteria or a process used to evaluate personnel risk assessments.*	
4.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4, Parts 4.1 through 4.3.	Acceptable evidence must include the documented personnel risk assessment program with the criteria or process identified.
Reference to prior version: *CIP-004-4, R3.3*		Change Rationale: *Separated into its own table item.*	

Rationale for R5: To ensure that individuals who have authorized access to BES Cyber Systems have been assessed for risk.

R5. Each Responsible Entity shall implement one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable elements in *CIP-004-5 Table R5 – Personnel Risk Assessment. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R5 – Personnel Risk Assessment* and additional evidence to demonstrate that these processes were implemented as described in the Measures column of the table.

CIP-004-5 Table R5 – Personnel Risk Assessment			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
5.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Have a personnel risk assessment performed as specified in CIP-004-5, Requirement R4 prior to being granted authorized electronic or authorized unescorted physical access, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to: • Dated records showing that personnel risk assessments were completed before authorized electronic or authorized unescorted physical access was authorized; or • Dated records showing that, before authorized electronic or authorized unescorted access was authorized, the Responsible Entity received dated documentation or attestations from contractors or service vendors verifying that personnel risk assessments were conducted pursuant to CIP-004-5, Requirement R4.
Reference to prior version: *CIP-004-3, R3, R3.3*		**Change Rationale**: *Minor wording changes and added the ability to accept attestations from contractors or vendors.*	

CIP-004-5 Table R5 – Personnel Risk Assessment			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update each personnel risk assessment at least once every seven calendar years after the initial or previous personnel risk assessment such that the current PRA is no older than seven years.	Evidence may include, but is not limited to, current and previous personnel risk assessment records.
Reference to prior version: *CIP-004-4, R3.2*		**Change Rationale:** *Eliminated the "for cause" renewal.*	

Rationale for R6: To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to all Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 6.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R6 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

R6. Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in *CIP-004-5 Table R6 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

M6. Evidence must include the documented processes that collectively include each of the applicable items in *CIP-004-5 Table R6 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Designate one or more individual(s) to authorize: 6.1.1. electronic access; 6.1.2. unescorted physical access; and 6.1.3. access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity.	Evidence may include, but is not limited dated documentation designating one or more individual(s) to authorize electronic access, unescorted physical access, and access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity.
Reference to prior version: *CIP 003-4, R5.1; CIP-007-4, R5.1.1*		**Change Rationale:** Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent.	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to, a signed document, automated workflow approval, or email showing persons with electronic access have authorization, and similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP 007-4 R5.1, CIP 004-4 R4*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	The individual(s) designated in Part 6.1 shall authorize unescorted physical access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to, a system generated list of people with unescorted physical access, a signed document, automated workflow approval, or email showing persons with unescorted physical access have authorization, and similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP-006-4 R1.5*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	The individual(s) designated in Part 6.1 shall authorize access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determines are necessary for performing assigned work functions, except for CIP Exceptional Circumstances.	A signed document, automated workflow approval or email showing persons with access to BES Cyber System Information have authorization, and similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP-003-4, R5.2*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003 and CIP-007 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Verify at least once each calendar quarter that individuals provisioned for authorized electronic access or authorized unescorted physical access have associated authorization records.	Evidence may include, but is not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Documentation of the dated verification between a list of individuals who have been authorized for access (i.e. authorization forms) and a list of individuals provisioned for access (i.e. provisioning forms or shared account listing).
Reference to prior version: *CIP 004-4, R4.1*		**Change Rationale:** *Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	For electronic access, verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines necessary for performing assigned work functions.	Evidence may include, but is not limited to, documentation of the review including: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.
Reference to prior version: *CIP 007-4, R5.1.3*		**Change Rationale:** *Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, that access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity are correct and those that the Responsible Entity determines necessary for performing assigned work functions.	Evidence may include, but is not limited to, the following documentation of the review: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.
Reference to prior version: *CIP-003-4, R5.1.2*		**Change Rationale:** *Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.*	

Rationale for R7: The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (i.e., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to all Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate.

R7. Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning].*

M7. Evidence must include each of the applicable documented programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	For all termination actions, initiate the process to revoke the individual's unescorted physical access and Interactive Remote Access upon the effective date and time of the termination action, and complete the revocation within 24 hours after the effective date and time of the termination action.	Evidence may include, but is not limited to: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
77Reference to prior version: *CIP 004-4, R4.2*		**Change Rationale:** *The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards* ***to require immediate revocation*** *for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the reassignment or transfer.	Evidence may include, but is not limited to: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
Reference to prior version: *CIP-004-4, R4.2*		**Change Rationale:** *FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	For termination actions, revoke the individual's access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity by the end of the next calendar day following the effective date and time of the termination action.	Evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.
Reference to prior version: *NEW*		**Change Rationale:** *FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.4	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	For termination actions, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with Requirements R7.1 or R7.3) within 30 calendar days of the effective date of the termination action.	Evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
Reference to prior version: *NEW*		**Change Rationale:** *FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.5	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	For termination actions, reassignments, or transfers, change passwords for shared account(s) known to the user within 30 calendar days of the termination action, reassignment, or transfer of the user. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Evidence may include, but is not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; or • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers.
Reference to prior version: *CIP-007-4, R5.2.3*		**Change Rationale:** *To provide clarification of expected actions in managing the passwords.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so beyond 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not document a security awareness program. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 1 of the required training content as detailed in 2.2 through 2.10.	The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 2 of the required training content as detailed in 2.2 through 2.10.	The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 4 or more of the training content as detailed in 2.2 through 2.10.	The Responsible Entity did not have the required role-based training. (R2)
R3	**Operations Planning.**	**Medium**	With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not	With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not	With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not	With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			train 1 individual prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 1 individual authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)	train 2 individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 2 individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)	train 3 individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 3 individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)	train 4 or more individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 4 or more individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2) OR The Responsible Entity did not implement at all its cyber security training program. (R3)
R4	**Operations Planning**	**Medium**	N/A	The Responsible Entity has a personnel risk assessment program, as stated in	The Responsible Entity has a personnel risk assessment program, as stated in	The Responsible Entity did not have a personnel risk assessment program,

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R4, for individuals having authorized cyber or authorized unescorted physical access, but the program does not include identity verification or a criminal history records check. (4.1) (4.2)	Requirement R4, for individuals having authorized cyber or authorized unescorted physical access, but the program did not include the required documented results or the program did not include criteria or process to determine when authorized access shall not be granted. (4.3)(4.5)	as stated in Requirement R4, for individuals having authorized cyber or authorized unescorted physical access. (R4)
R5	**Same Day Operations**	**Medium**	Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 1 individual prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1) OR	Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 2 individuals prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1) OR The Responsible Entity did not update	Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 3 individuals prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1) OR	The Responsible Entity did not have a documented process for personnel risk assessments. (R5) OR Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 4 or more individuals

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity did not update personnel risk assessments every seven years for 1 individual within seven years after the initial performance or last update of the personnel risk assessment. (5.2)	personnel risk assessments every seven years for 2 individuals within seven years after the initial performance or last update of the personnel risk assessment. (5.2)	The Responsible Entity did not update personnel risk assessments every seven years for 3 or more individuals within seven years after the initial performance or last update of the personnel risk assessment. (5.2)	prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1)
R6	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity	The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity	The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity	The Responsible Entity did not have a documented process for access management. (R6) OR The Responsible Entity did not designate one or more individual(s) to authorize electronic access, unescorted physical access, or access to the physical and electronic

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			determined was necessary for performing assigned work functions. (6.2) (6.3) (6.4) OR The Responsible Entity did verify within 17 calendar months but not within 15 calendar months that: (6.6) (6.7) • all user accounts, user account groups, and user role categories were correct, or • their specific, associated privileges were correct or that they were those that that the Responsible	determined was necessary for performing assigned work functions and one user was granted access without authorization by the individual(s) designated in 6.1. (6.2) (6.3) (6.4) OR The Responsible Entity did not verify within the calendar quarter that individuals provisioned for unescorted physical access and electronic access had associated authorization records. (6.5) OR The Responsible Entity did verify within 19 calendar months but not within 17 calendar months that: (6.6)	determined was necessary for performing assigned work functions and two users were granted access without authorization by the individual(s) designated in 6.1. (6.2) (6.3) (6.4) OR The Responsible Entity did verify within 21 calendar months but not within 19 calendar months that: (6.6) (6.7) • all user accounts, user account groups, and user role categories are correct, or • their specific, associated privileges were	locations where BES Cyber System Information is stored by the Responsible Entity. (6.1) OR The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, and access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determined was necessary for performing assigned work functions and three or more users were granted access without authorization

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity determined necessary for performing assigned work functions. • access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing assigned work functions.	(6.7) • all user accounts, user account groups, and user role categories were correct, or • their specific, associated privileges were correct or that they were those that the Responsible Entity determined necessary for performing assigned work functions. • access to the physical and electronic locations where BES Cyber System	correct or that they were those that that the Responsible Entity determined necessary for performing assigned work functions. • access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for	by the individual(s) designated in 6.1. (6.2) (6.3) (6.4) OR The Responsible Entity did not verify within 24 calendar months that: (6.6) (6.7) • all user accounts, user account groups, and user role categories were correct, or • their specific, associated privileges were correct or that they were the those that that the Responsible Entity determined necessary for

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing assigned work functions.	performing assigned work functions.	performing assigned work functions, or • access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing assigned work functions.
R7	**Same Day Operations and Operations Planning**	**Medium**	Revocation of access to BES Cyber Information was not accomplished for 1 or more individuals	The Responsible Entity did not revoke unneeded unescorted physical or electronic access within the	The Responsible Entity did not revoke unneeded unescorted physical or electronic access according to	The Responsible Entity did not have a documented process for initiating the unescorted physical or

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			within the specified time frame (7.3); OR User accounts on BES Cyber Assets were not revoked for one or more individuals within the specified time frame (7.4); OR User passwords on BES Cyber Asset shared accounts were not changed for one or more individuals within the specified time frame; (7.5) OR Following the determination and documentation of extenuating operating circumstances, passwords for shared accounts were not changed for one or	specified times in CIP-004-5 R7 for one individual who was terminated, resigned, was reassigned, or transferred. (7.1 and 7.2)	the specified times in CIP-004-5 R7 for two individuals who were terminated, resigned, reassigned or transferred.(7.1 and 7.2)	electronic access revocation process; OR The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for three or more individuals who were terminated, resigned, reassigned, or transferred. (7.1 and 7.2)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more individuals within 10 days following the end of the extenuating operating circumstances. (7.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reference sound security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Guidance: Describe example mechanisms used to demonstrate the availability of this information

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The training may consist of multiple modules and multiple delivery mechanisms.

Note: Provide guidance or a local definition of "role appropriate" as it is used in this standard.

Requirement R3:

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response.

NOTE: Program specified exceptional circumstances can include a specified individual to declare an emergency.

Requirement R4 and R5:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access when called for in CIP-004-1 Table R4 – Personnel Risk Assessment, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response, to ensure that personnel who have such access have had their identity verified, then

been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, or individuals who may have resided in locations from where it is not possible to obtain a criminal history records check.

Requirement R6:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly and annual reviews. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The annual privilege review is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R6 is included below.

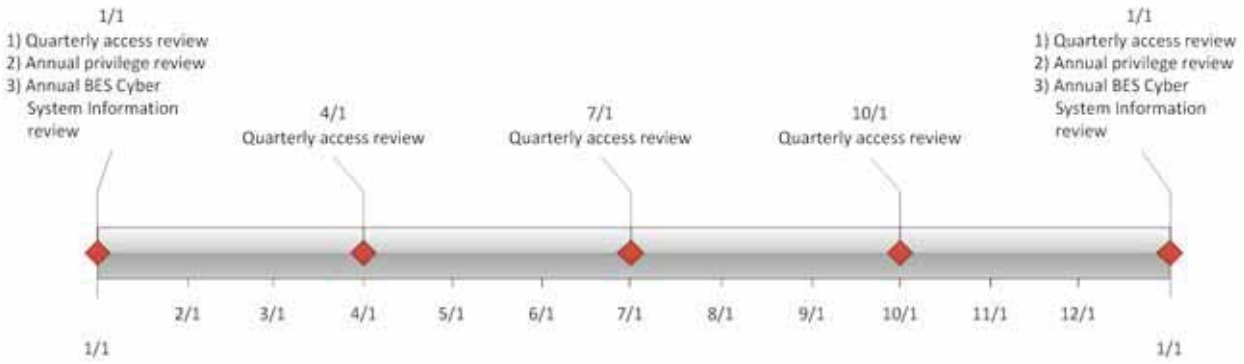

Separation of duties should be considered when performing the reviews in Requirement R6. The person reviewing should be different than the person provisioning access.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R6 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R7:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common examples and possible processes on when the termination action occurs are provided in the following table.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Termination prior to notification	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to

or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R7.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, the requirement states a review of access privileges must be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the ~~first~~second posting of ~~the~~ Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center~~"~~."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-5

3. **Purpose:** ~~Standard CIP-004-5 requires that personnel having authorized cyber or authorized unescorted physical access to BES Cyber Assets and BES Cyber Systems, including contractors and service vendors, have~~To minimize the risk from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities ~~that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~ **described in 4.2.2**

   - ~~A UFLS program required by a NERC or regional Reliability Standard~~
   - ~~A UVLS program required by a NERC or regional Reliability Standard~~
   - ~~A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard~~
   - ~~A Transmission Protection System required by a NERC or regional Reliability Standard~~
   - ~~Its Transmission Operator's restoration plan~~

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   ~~4.1.6~~4.1.7 Reliability Coordinator

   4.1.8 ~~that are part of any of the following systems~~**Transmission Operator**

   4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

4.1.74.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or regionalRegional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- A UVLS programA Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or regionalRegional Reliability Standard

4.1.8 NERC

4.1.9 Regional Entity

4.1.104.2.3 A Protection System that applies to **Reliability Coordinator**

4.1.11 Transmission **Operator**

4.1.12 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated forwhere the protection of the BES:

- A UFLS programProtection System is required by a NERC or regionalRegional Reliability Standard
- A UVLS program required by a NERC or regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or regional Reliability Standard
- A UVLS program required by a NERC or regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard

- ~~A Transmission Protection System required by a NERC or regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~
- ~~**All other**~~ Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~**4.2.3**~~**4.2.4 Responsible Entities**~~:~~ **listed in 4.1 other than Distribution Providers and Load-Serving Entities**: All BES Facilities.

~~**4.2.4**~~**4.2.5 Exemptions:** The following are exempt from Standard CIP-~~004~~002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~**4.2.4.4** Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.~~

5. Background:

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter~~ as applicable~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of ~~specific elements required~~applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance

to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e~~.~~., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and categorization processes. ~~Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example,~~

~~a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.

- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.~~

- **Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity** – Only applies to ~~Medium Impact~~medium impact BES Cyber Systems with External Routable Connectivity~~. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity~~ or dial-up connectivity.

- ~~**Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.~~

- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding ~~High or Medium Impact BES Cyber Systems.~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

- ~~**Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding ~~High~~high impact BES Cyber System or ~~Medium Impact BES Cyber Systems.~~

- ~~**Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact~~medium impact BES Cyber ~~Systems.~~

- ~~**Electronic Access Points** – Applies at Electronic Access Points (with~~ System with External Routable Connectivity ~~or dial-up connectivity) associated with a referenced BES Cyber System.~~

- ~~**Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~

- ~~**Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded~~ in the ~~definition of Physical Access Control Systems.~~

- applicability column.

B. Requirements and Measures

Rationale for R1: Ensures that Responsible Entities with personnel who have authorized electronic ~~access and/~~or authorized unescorted physical access to BES Cyber ~~Systems~~ Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of ~~best~~the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R1 – Security Awareness Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	A security awareness program that, at least once each calendar quarter, conveys ~~security awareness concepts and provides on-going~~ongoing reinforcement of ~~such concepts on at least a quarterly basis.~~cyber security practices for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	Evidence must include the documented security awareness program, and additional evidence to demonstrate that this program was implemented ~~such as, but not limited to, the quarterly reinforcement material that has been distributed.~~ . Evidence of implementation may include, but not limited to, documentation that the quarterly reinforcement has been provided. Evidence of reinforcement may include dated copies of information used to reinforce security awareness, as well as evidence of distribution such as: direct communications (for example, e-mails, memos, computer-based training); indirect communications (for example, posters, intranet, or brochures); management support and reinforcement (for example, presentations or meetings).
Reference to prior version: *CIP-004-4, R1*		**Change Rationale:** *Changed to remove the need to ensure everyone with authorized electronic or authorized unescorted physical access ~~receives this~~"received" ongoing reinforcement – to state that the program conveys awareness~~.~~ and measures that reinforcement "has been provided."* *Moved example mechanisms to guidance.*	

CIP-004-5 Table R1 – Security Awareness Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
		Changed to record delivery.	

Rationale for R2: To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems ~~contains~~ covers the proper policies, access controls, and procedures to protect BES Cyber Systems.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:
   - ~~the~~The visitor control program~~;~~
   - ~~electronic~~Electronic interconnectivity supporting the operation and control of BES Cyber Systems
   - ~~storage~~Storage media as part of the handling of BES Cyber Systems information
2. Change references from Critical Cyber Assets to BES Cyber Systems

R2. Each Responsible Entity shall have a role-based cyber security training program ~~for personnel who need~~to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5, Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable items in *CIP-004-5, Table R2 – Cyber Security Training Program*.

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~Define the roles that require~~Identification of each role and training required for each role.	Acceptable evidence must include a list of roles and what training is needed for each role.
Reference to prior version: NEW		**Change Rationale:** *The first thing needed in a role-~~-~~based training program is to understand what roles ~~your people~~individuals have ~~to help~~so that the Responsible Entity can plan what training modules ~~you need~~it needs to provide.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the cyber security ~~controls~~policies protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material on the security controls that have been implemented to protect BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.1*		**Change Rationale:** *~~Minor wording changes. Changed~~Removed to address cyber security issues, not the business function. The previous version was focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security.*	
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the ~~proper use of~~ physical access controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the proper use of physical access controls for BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.1 and R2.2.2*		**Change Rationale:** *Minor wording changes.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the electronic access controls protecting the Responsible Entity's BES Cyber Systems.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the electronic access controls to protect BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.1 and R2.2.2*		**Change Rationale:** *Minor wording changes.*	
2.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on the visitor control program.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the visitor control program.
Reference to prior version: *NEW*		~~**Change Rationale:** *Personnel administering the visitor control program and/or providing escort should be part of the core training; FERC Order 706 - paragraph 432.*~~ **Change Rationale:** *No significant change from previous versions.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on handling of BES Cyber System Information and its storage~~ media.~~.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the handling of BES Cyber System Information, including its storage ~~media~~.
Reference to prior version: *CIP004-4, R2.2.3*		**Change Rationale:** *Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage media; FERC Order No. 706~~ –~~, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16~~)~~.*	
2.7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on identification of a potential BES Cyber Security Incident and ~~associated~~initial notifications~~.~~ in accordance with the entity's incident response plan	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the identification of a potential BES Cyber Security Incident and associated notifications.
Reference to prior version: *~~CIP004~~CIP-004-4, R2.2.4 (new; implied but not stated in CIP-004-4 or CIP-008-4)*		**Change Rationale:** *Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706~~ - paragraph~~, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.8	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on recovery plans for BES Cyber Systems.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on recovery plans for BES Cyber Systems.
Reference to prior version: *CIP004-4, R2.2.4*		**Change Rationale:** *Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706~~ - paragraph~~, Paragraph 413.*	
2.9	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training content on response to BES Cyber Security Incidents.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the response to a BES Cyber Security Incident.
Reference to prior version: *CIP004-4, R2.2.4*		**Change Rationale:** *Minor wording changes.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.10	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Training ~~on~~content on risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the electronic interconnectivity and interoperability with other Cyber Assets.
Reference to prior version: *NEW*		**Change Rationale:** *Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706~~ - paragraph~~, Paragraph 434.*	

Rationale for R3: To ensure that personnel with authorized electronic access or authorized unescorted physical access are trained in the policies, access controls, and procedures to protect the BES Cyber Systems.

Summary of Changes: Re-organization of the training requirements into the respective requirements for "program" and "implementation" of the training.

R3. Each Responsible Entity shall implement its documented role-based cyber security training program ~~for each individual needing~~to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R3 - Cyber Security Training. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations~~]~~].*

M3. Evidence must include, but is not limited to, documentation that the training was provided as defined in *CIP-004-5 Table R3 - Cyber Security Training*.

CIP-004-5 Table R3 – Cyber Security Training			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	Require completion and documentation of the training specified in CIP-004-5, Requirement R2 prior to granting authorized electronic access and authorized unescorted physical access to BES Cyber Systems, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, for each individual requiring authorized electronic or authorized unescorted physical access, dated individual training records, the date authorized electronic or authorized unescorted physical access was first granted, or a dated log or documentation of when CIP Exceptional Circumstances were invoked and revoked.
Reference to prior version: *CIP004-4, R2.1*		**Change Rationale:** *Addition of exceptional circumstances parameters as directed in FERC Order No. 706~~, paragraph~~, Paragraph 431 is detailed in CIP-003-5~~.~~.*	

CIP-004-5 Table R3 – Cyber Security Training			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	Require completion and documentation of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.	Evidence may include, but is not limited to, dated individual training records.
Reference to prior version: *CIP004-4, R2.3*		**Change Rationale:** *Updated to further define what "Annual" training means.*	

~~**Rationale for R4:** To ensure that individuals who need authorized electronic or unescorted physical access to BES Cyber Systems have been assessed for risk.~~

~~**Summary of Changes:** Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.~~

R4. Each Responsible Entity shall have one or more documented personnel risk assessment programs ~~for individuals needing~~to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning~~]~~].*

M4. Evidence must include the documented personnel risk assessment program that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program.*

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	An initial personnel risk assessment ("PRA") that includes identity verification.	Acceptable evidence must include the documented personnel risk assessment program with a requirement for an initial personnel risk assessment that includes identity verification.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Addressed interpretation request in guidance. Specified that ~~identify~~identity verification is only required for each individual's initial assessment. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.*	

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six months or more: 4.2.1. resided; 4.2.2. been employed (if applicable); and 4.2.3. attended school (if applicable). If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	Acceptable evidence must include the documented personnel risk assessment program with a requirement for a seven-year criminal history record check in accordance with this part.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.*	

Reference to prior version: *CIP004-4 R3.1*	**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven year check cannot be performed.*

CIP-004-5 Table R4 – Personnel Risk Assessment Program			
Part	**Applicability Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.23	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.Process or criteria used to evaluate personnel risk assessments to determine when to deny authorized access.	Acceptable evidence must include the documented personnel risk assessment program with a requirement for a seven year criminal history record check in accordance with Requirement R4, Part 4.2. the process or criteria identified.

~~CIP-004-5 Table R4 – Personnel Risk Assessment Program~~			
~~Part~~	~~Applicability~~	~~Requirements~~	~~Measures~~
~~4.3~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems~~	~~Criteria or process used to evaluate personnel risk assessments to determine when to deny authorized access.~~	~~Acceptable evidence must include the documented risk assessment program with the criteria or process identified in Requirement R4, Part 4.3.~~

Reference to prior version: *NEW*		Change Rationale: *There should be documented criteria or a process used to evaluate personnel risk assessments.*	
4.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4~~.~~, Parts 4.1 through 4.3.	Acceptable evidence must include the documented personnel risk assessment program with the criteria or process identified ~~in Requirement R4, Part 4.4.~~ .
Reference to prior version: *CIP-004-4, R3.3*		Change Rationale: *Separated into its own table item.*	

Rationale for R5: To ensure that individuals who have authorized access to BES Cyber Systems have been assessed for risk.

R5. Each Responsible Entity shall implement one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable elements in *CIP-004-5 Table R5 – Personnel Risk Assessment*. [. [*Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R5 – Personnel Risk Assessment* and additional evidence to demonstrate that these processes were implemented as described in the Measures column of the table.

CIP-004-5 Table R5 – Personnel Risk Assessment			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
5.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	~~Perform~~Have a personnel risk assessment performed as specified in CIP-004-5, Requirement R4 prior to being granted authorized electronic or authorized unescorted physical access, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to: • Dated records showing that personnel risk assessments were completed before authorized electronic or authorized unescorted physical access was authorized; or • ~~Dated~~Dated records showing that, before authorized electronic or authorized unescorted access was authorized, the Responsible Entity received dated documentation or attestations from contractors or service vendors verifying that personnel risk assessments were conducted pursuant to CIP-004-5, Requirement R4 ~~before access was authorized~~.
Reference to prior version: *CIP-004-3, R3, R3.3*		**Change Rationale**: *Minor wording changes and added the ability to accept attestations from contractors or vendors.*	

CIP-004-5 Table R5 – Personnel Risk Assessment			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	Update each personnel risk assessment at least once every seven calendar years after the initial or previous personnel risk assessment such that the current PRA is no older than seven years.	Evidence may include, but is not limited to, current and ~~former~~previous personnel risk assessment records.
Reference to prior version: *CIP-004-4, R3.2*		**Change Rationale:** *Eliminated the "for cause" renewal.*	

~~**Rationale for R6:** To ensure that individuals with access to BES Cyber Systems have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and part of the delegations referenced in CIP-003-5.~~

~~Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services).~~

~~CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.~~

~~Quarterly reviews in 6.4 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.~~

~~If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement.~~

~~For BES Cyber Systems that do not have user accounts defined, the controls listed in R6 are not applicable. However, the Responsible Entity should document such configurations.~~

~~**Summary of Changes:** The primary change here involves pulling the access management requirements from CIP-003-4, CIP-004-4 and CIP-007-4 into a single requirement. The requirements from version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.~~

Rationale for R6: To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to all Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 6.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R6 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

R6. Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in *CIP-004-5 Table R6 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations]].*

M6. Evidence must include the documented processes that collectively include each of the applicable items in *CIP-004-5 Table R6 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Designate one or more individual(s) to authorize: 6.1.1. electronic access; 6.1.2. unescorted physical access; and 6.1.3. access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity.	Evidence may include, but is not limited dated documentation designating one or more individual(s) to authorize electronic access, unescorted physical access, and access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity.

Reference to prior version: *CIP 003-4, R5.1; CIP-007-4, R5.1.1*	**Change Rationale:** Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent.

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.~~1~~2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	The ~~CIP Senior Manager or delegate~~individual(s) designated in Part 6.1 shall authorize electronic access~~,~~ ~~except for CIP Exceptional Circumstances. Access permissions shall be~~ that the ~~minimum~~Responsible Entity determines is necessary for performing assigned work functions~~.~~, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to~~:~~ ~~(i) a system-generated list of people with electronic access and a sampling of accounts to verify unauthorized users do not have access,~~ ~~(ii)~~, a signed document, automated workflow approval, or email showing ~~such~~ persons with electronic access have authorization, and ~~(iii)~~ similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.

Reference to prior version: *CIP 007-4 R5.1, CIP 004-4 R4*	**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.~~2~~3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	The ~~CIP Senior Manager or delegate~~individual(s) designated in Part 6.1 shall authorize unescorted physical access ~~to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be~~that the ~~minimum~~Responsible Entity determines is necessary for performing assigned work functions~~.~~, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to~~:~~ ~~(i)~~, a system generated list of people with unescorted physical access ~~through the Defined Physical Boundary and a sampling of accounts (for automated physical access control) to verify unauthorized users do not have access,~~ ~~(ii)~~, a signed document, automated workflow approval, or email showing ~~such~~ persons with unescorted physical access have authorization, and ~~(iii)~~ similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP-006-4 R1.5*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.~~3~~4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	The ~~CIP Senior Manager or delegate~~individual(s) designated in Part 6.1 shall authorize access to the physical and electronic locations where BES Cyber System Information~~, except for CIP Exceptional Circumstances. Access permissions shall be the minimum~~ is stored by the Responsible Entity that the Responsible Entity determines are necessary for performing assigned work functions, except for CIP Exceptional Circumstances.	~~Evidence may include, but is not limited to:~~ ~~(i) a list of people with access to BES Cyber System Information and a sampling of accounts (on electronic document systems) to verify unauthorized users do not have access,~~ ~~(ii) a~~A signed document, automated workflow approval or email showing ~~such~~ persons with access to BES Cyber System Information have authorization, and ~~(iii)~~ similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.
Reference to prior version: *CIP-003-4, R5.2*		**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003 and CIP-007 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.~~4~~5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	Verify at least once each calendar quarter that individuals provisioned for authorized electronic access or authorized unescorted physical ~~or electronic access to BES Cyber Systems were authorized for such~~ access have associated authorization records.	Evidence may include, but is not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Documentation of the dated verification between a list of individuals who have been authorized for access (i.e. authorization forms) and a list of individuals provisioned for access~~.~~ (i.e. provisioning forms or shared account listing).
Reference to prior version: *CIP 004-4, R4.1*		**Change Rationale:** *Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.~~5~~6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	~~Verify~~For electronic access, verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all user accounts~~/~~, user account groups, or user role categories, and their specific, associated privileges are correct and ~~the minimum~~are those that the Responsible Entity determines necessary for performing assigned work functions.	Evidence may include, but is not limited to, documentation of the review including: 1. ~~(i) a~~A dated listing of all accounts/account groups or roles within the system~~,~~; 2. ~~(ii) a~~A summary description of privileges associated with each group or role~~,~~; 3. ~~(iii) accounts~~Accounts assigned to the group or role; and ~~(iv) dated~~ 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.
Reference to prior version: *CIP 007-4, R5.1.3*		**Change Rationale:** *Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.*	

CIP-004-5 Table R6 – Access Management Program			
Part	**Applicability**	**Requirements**	**Measures**
6.~~6~~7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, ~~of~~that access ~~privileges~~ to the physical and electronic locations where BES Cyber System Information ~~to confirm that access privileges~~is stored by the Responsible Entity are correct and ~~the minimum~~those that the Responsible Entity determines necessary for performing assigned work functions.	Evidence may include, but is not limited to, the following documentation of the review ~~including~~ : 1. ~~(i) a~~A dated listing of authorizations for BES Cyber System information~~,~~; 2. ~~(ii) any~~Any privileges associated with the authorizations~~,~~; and 3. ~~(iii) dated~~Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.
Reference to prior version: *CIP-003-4, R5.1.2*		**Change Rationale:** *Moved requirement to ensure consistency among access reviews. Clarified precise meaning ~~in the term~~of annual. Clarified what was necessary in performing a verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.*	

Rationale for R7: The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (i.e., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to all Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate.

R7. Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning]*.

~~**Rationale for R7:** The timely revocation of electronic access to cyber systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.~~

~~In considering how to address the FERC Order directing immediate revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (i.e. revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.~~

~~Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services).~~

~~**Summary of Changes:** Paragraphs 460 and 461 of FERC Order 706 state the following: The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).~~

~~As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate.~~

M7. Evidence must include~~–~~ each of the applicable documented programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

~~CIP-004-5 Table R7 – Access Revocation~~			
~~Part~~	~~Applicability~~	~~Requirements~~	~~Measures~~
~~7.1~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems.~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ ~~Associated Protected Cyber Assets~~	~~For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time[2] of the resignation or termination.~~	~~Evidence may include, but is not limited to~~ ~~(i) workflow or sign-off form verifying access removal associated with the terminations and dated concurrent or prior to the date of the termination action, and~~ ~~(ii) a system-generated listing of user accounts or other demonstration showing such persons no longer have access.~~
~~**Reference to prior version:**~~ ~~*CIP 004-4 R4.2*~~		~~**Change Rationale:** *The FERC Order 706 Paragraph 460 and 461 directs modifications to the Standards to require immediate revocation for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*~~	

~~[2] Since a termination action is often recorded without consideration to the time of day, "at the time" does not require a to-the-minute or to-the-hour time-stamped comparison of access logs and the termination action.~~

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.~~2~~1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	For ~~reassignments or transfers,~~ all termination actions, initiate the process to revoke the individual's ~~unneeded electronic and~~ unescorted physical access ~~to BES Cyber Systems by the end~~and Interactive Remote Access upon the effective date and time of the ~~next calendar day.~~ termination action, and complete the revocation within 24 hours after the effective date and time of the termination action.	Evidence may include, but is not limited to~~,~~: 1. ~~(i)~~Dated workflow or sign-off form ~~showing~~verifying access removal associated with the ~~review of logical~~termination action; and ~~physical authorizations dated on the same calendar day as the transfer or reassignment and~~ 2. ~~(ii) a system-generated listing of user accounts~~Logs or other demonstration showing such persons no longer have access ~~where the review determined it was no longer needed.~~.
~~**Reference**~~**77Reference to prior version:** *CIP~~-~~ 004-4, R4.2*		**Change Rationale:** *The FERC Order No. 706 ~~Paragraph~~, Paragraphs 460 and 461, directs modifications to the Standards* ***to require immediate revocation*** *for any person no longer needing access~~, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.~~. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**

7.~~3~~2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	For ~~resignations~~reassignments or ~~terminations~~transfers, revoke the individual's electronic and physical access ~~to BES Cyber System Information~~that the Responsible Entity determines is not necessary by the end of the next calendar day following the ~~resignation~~reassignment or ~~termination.~~transfer.	Evidence may include, but is ~~-~~not limited to~~,~~: 1. Dated workflow or sign-off form ~~verifying access removal to designated~~ showing a review of logical and physical ~~areas~~access; and Logs or ~~cyber systems containing BES Cyber System information associated with~~other demonstration showing such persons no longer have access that the ~~terminations and dated within the next calendar day of the termination action.~~ 2. Responsible Entity determines is not necessary.
Reference to prior version: ~~*NEW*~~*CIP-004-4, R4.2*		**Change Rationale:** ~~*The*~~ *FERC Order No. 706, Paragraph ~~386 directs~~460 and 461, direct modifications to the Standards to require ~~prompt~~immediate revocation ~~of~~ for any person no longer needing access, including transferred employees. In reviewing how to ~~protected information. To address~~modify this ~~directive, Responsible Entities are required to revoke~~requirement, the SDT determined the date a person no longer needs access ~~to areas designated for BES Cyber System Information. This could include records closets, substation~~after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control ~~houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.~~ in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.~~4~~3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity or dial-up connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	For ~~resignations or terminations~~termination actions, revoke the individual's ~~user accounts on~~access to the physical and electronic locations where BES Cyber ~~Assets (unless already revoked in accordance with R7.1 or 7.3) within thirty (30)~~System Information is stored by the Responsible Entity by the end of the next calendar ~~days of~~day following the effective date and time of ~~initial access revocation.~~ the termination action.	Evidence may include, but is not limited to, workflow or sign-off form ~~showing~~verifying access removal ~~for any individual~~to designated physical areas or cyber systems containing BES Cyber ~~Assets and software applications as determined necessary to completing~~System Information associated with the ~~revoking of access~~terminations and dated within ~~thirty~~the next calendar ~~days~~day of the termination~~.~~ action.
Reference to prior version: *NEW*		**Change Rationale:** ~~*The*~~ *FERC Order No. 706, Paragraph ~~460 and 461~~386, directs modifications to the ~~Standards~~standards to require ~~immediate~~prompt revocation ~~for any person no longer needing~~of access~~. In order~~ to ~~meet the immediate timeframe,~~protected information. To address this directive, Responsible Entities ~~will likely have initial revocation procedures~~are required to ~~prevent remote and physical~~ revoke access to ~~the~~ areas designated for BES Cyber System~~. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability.~~ Information. This ~~requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.~~could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.4	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	For termination actions, revoke the individual's user accounts on BES Cyber Assets (unless already revoked in accordance with Requirements R7.1 or R7.3) within 30 calendar days of the effective date of the termination action.	Evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
Reference to prior version: *NEW*		**Change Rationale:** *FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.*	

CIP-004-5 Table R7 – Access Revocation			
Part	**Applicability**	**Requirements**	**Measures**
7.5	High Impact BES Cyber Systems ~~Medium Impact BES Cyber Systems.~~ Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	For ~~terminations, resignations~~termination actions, reassignments, or transfers, change passwords for shared account(s) known to the user within ~~thirty (~~30~~)~~ calendar days of the termination~~, resignation~~ action, reassignment, or transfer of the user. ~~In~~ If the Responsible Entity determines and documents that extenuating operating circumstances ~~that~~ require a longer time period, ~~document the extenuating circumstances and~~ change the password(s) within ~~ten~~10 calendar days following the end of the ~~extenuating~~operating circumstances.	Evidence may include, but is not limited to: • Workflow or sign-off form showing password reset within ~~thirty~~30 calendar days of the termination; or • Workflow or sign-off form showing password reset within ~~thirty~~30 calendar days of the reassignments or transfers.
Reference to prior version: *CIP-007-4, R5.2.3*		**Change Rationale:** *To provide clarification of expected actions in managing the passwords.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity; or
- If the Responsible Entity works for shall serve as the Compliance Enforcement Authority ("CEA") unless the Regional Entity, then the applicable entity is owned, operated, or controlled by the Regional Entity will establish an agreement with. In such cases the ERO or another a Regional entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERCauthority shall serve as the Compliance Enforcement AuthorityCEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliantmitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	~~N/A~~The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	~~N/A~~The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not ~~provide~~convey on-going security awareness reinforcement ~~on~~ at least once for a ~~quarterly basis~~calendar quarter and did so beyond 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not document ~~or implement~~ a security awareness program. (R1)
R2	**Operations Planning**	**Lower**	~~N/A~~The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 1 of the required training content as detailed in 2.2 through 2.10.	~~N/A~~The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 2 of the required training content as detailed in 2.2 through 2.10.	The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include ~~training for one~~4 or more of the ~~roles~~training content as detailed in 2.2 through 2.10.	The Responsible Entity did not have the required role-based training. (R2)
R3	**Operations Planning.**	**Medium**	~~N/A~~With the exception of policy-identified CIP	~~N/A~~With the exception of policy-identified CIP Exceptional	With the exception of policy-identified CIP Exceptional	~~The Responsible Entity trained some, but not all individuals~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Exceptional Circumstances, the Responsible did not train 1 individual prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 1 individual authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)	Circumstances, the Responsible did not train 2 individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not train 2 individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)	Circumstances, the Responsible did not train 3 individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity ~~trained some but~~did not ~~all~~train 3 individuals authorized for electronic ~~or~~and unescorted physical access ~~at least once every~~in a calendar year~~, but~~ not ~~to exceed~~exceeding 15 months between training. (3.2)	~~authorized for electronic or unescorted physical access prior to their being granted such access, except in~~With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not train 4 or more individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1) OR The Responsible Entity did not ~~fully~~ train 4 or more individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						training. (3.2) OR The Responsible Entity did not implement at all its cyber security training program. (R3)
R4	**Operations Planning**	**Medium**	N/A	The Responsible Entity has a personnel risk assessment program, as stated in Requirement R4, for individuals having authorized cyber or authorized unescorted physical access, but the program does not include identity verification or a criminal history records check. (4.1) (4.2)	The Responsible Entity has a personnel risk assessment program, as stated in Requirement R4, for individuals having authorized cyber or authorized unescorted physical access, but the program did not include the required documented results or the program did not include criteria or process to determine when authorized access shall not be granted. (4.3)(4.5)	The Responsible Entity did not have a personnel risk assessment program, as stated in Requirement R4, for individuals having authorized cyber or authorized unescorted physical access. (R4)
R5	**Same Day Operations**	**Medium**	~~N/A~~Except for CIP Exceptional	~~N/A~~Except for CIP Exceptional	~~The~~Except for CIP Exceptional	~~The~~The Responsible Entity did not have a

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Circumstances, the Responsible Entity did not perform personnel risk assessments for 1 individual prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1) OR The Responsible Entity did not update personnel risk assessments every seven years for 1 individual within seven years after the initial performance or last update of the personnel risk assessment. (5.2)	Circumstances, the Responsible Entity did not perform personnel risk assessments for 2 individuals prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1) OR The Responsible Entity did not update personnel risk assessments every seven years for 2 individuals within seven years after the initial performance or last update of the personnel risk assessment. (5.2)	Circumstances, the Responsible Entity did not perform personnel risk assessments for 3 individuals prior to granting authorized electronic ~~or~~and unescorted physical access~~, except for CIP Exceptional Circumstances, but the~~ in a calendar year. (5.1) OR The Responsible Entity did not update personnel risk assessments ~~are not updated at least once~~ every seven years~~.~~ for 3 or more individuals within seven years after the initial performance or last update of the personnel risk assessment. (5.2)	documented process for personnel risk assessments. (R5) OR Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 4 or more individuals prior to granting authorized electronic ~~or~~and unescorted physical access~~, except for CIP Exceptional Circumstances.~~ in a calendar year. (5.1) ~~OR~~ ~~The Responsible Entity did not have a documented process for personnel risk assessments.~~
R6	**Operations**	**Lower**	The Responsible Entity did not	The Responsible Entity	The Responsible Entity	The Responsible Entity did not have ~~its~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning and Same Day Operations		authorize or have ~~its CIP Senior Manager or delegate~~the individual(s) designated in 6.1 authorize electronic ~~or~~access, unescorted physical access, or access to ~~BES Cyber Systems with the minimum~~the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determined was necessary ~~permissions~~ for ~~users to perform their~~ performing assigned work functions. (6.~~1~~2) (6.~~2~~3) (6.4) OR The Responsible Entity did verify	did not authorize or have ~~its CIP Senior Manager or delegate~~the individual(s) designated in 6.1 authorize electronic ~~or~~access, unescorted physical access ~~to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work functions and 1 user was granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2)~~ ~~OR~~ ~~The Responsible Entity did not have its CIP Senior Manager or delegate authorize~~ , or access to the physical and electronic locations where BES Cyber System Information~~,~~	did not authorize or have ~~its CIP Senior Manager or delegate~~the individual(s) designated in 6.1 authorize electronic ~~or~~access, unescorted physical access ~~to BES Cyber Systems with the minimum necessary permissions for users to perform their assigned work functions and 2 users were granted access without CIP Senior Manger or delegate authorization. (6.1) (6.2)~~ ~~OR~~ ~~The Responsible Entity did not have its CIP Senior Manager or delegate authorize~~ , or access to the physical and electronic locations where BES Cyber System Information~~,~~	~~CIP Senior Manager~~a documented process for access management. (R6) OR The Responsible Entity did not designate one or ~~delegate~~more individual(s) to authorize electronic ~~or~~access, unescorted physical access, or access to ~~BES Cyber Systems with~~ the ~~minimum necessary permissions for users to perform their~~physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity. (6.1) OR The Responsible

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			within 17 calendar months but not ~~have its CIP Senior Manager~~within 15 calendar months that: (6.6) (6.7) • all user accounts, user account groups, and user role categories were correct, or ~~delegate authorize access to BES Cyber System Information, with the minimum permissions~~ • their specific, associated privileges were correct or that they were those that that the	~~with~~ is stored by the ~~minimum permissions~~Responsible Entity that the Responsible Entity determined was necessary for ~~users to perform their~~performing assigned work functions and ~~1~~one user was granted access without ~~CIP Senior Manger or delegate~~ authorization~~.~~ by the individual(s) designated in 6.1. (6.2) (6.3) (6.4) OR The Responsible Entity did not verify within the calendar quarter that individuals provisioned for unescorted physical access and electronic access had associated authorization records.	~~with~~ is stored by the ~~minimum permissions~~Responsible Entity that the Responsible Entity determined was necessary for ~~users to perform their~~performing assigned work functions and ~~2~~two users were granted access without ~~CIP Senior Manger or delegate~~ authorization by the individual(s) designated in 6.1. (6.2) (6.3) (6.4) OR The Responsible Entity did verify within 21 calendar months but not within 19 calendar months that: (6.6) (6.7) • all user accounts, user account groups,	Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, and access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determined was necessary for performing assigned work functions and ~~3~~three or more users were granted access without ~~CIP Senior Manger or delegate~~ authorization~~.~~ (by the individual(s) designated in 6.1~~)~~. (6.2) (6.3) (6.4) ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Responsible Entity determined necessary for ~~users to perform their~~performing assigned work functions.~~ (6.3)~~ • access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing	(6.5) OR The Responsible Entity did verify within 19 calendar months but not within 17 calendar months that: (6.6) (6.7) • all user accounts, user account groups, and user role categories were correct, or • their specific, associated privileges were correct or that they were those that the Responsible Entity determined necessary for performing assigned work functions. • access to the	and user role categories are correct, or • their specific, associated privileges were correct or that they were those that that the Responsible Entity determined necessary for performing assigned work functions. • access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was	~~The Responsible Entity did not have its CIP Senior Manager or delegate authorize access to BES Cyber System Information, with the minimum permissions necessary for users to perform their assigned work functions and 3 or more users were granted access without CIP Senior Manger or delegate authorization. (6.3)~~ ~~OR~~ ~~The Responsible Entity did not perform a quarterly verification of individuals with authorized access against one or more lists of individuals provisioned for unescorted physical~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			assigned work functions.	physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing assigned work functions.	what the Responsible Entity determined necessary for performing assigned work functions.	or electronic access to BES Cyber Systems. (6.4) OR The Responsible Entity did not verify provisionedwithin 24 calendar months that: (6.6) (6.7) • all user accounts/, user account groups or, and user role categories and were correct, or • their specific, associated privileges according to the timeframe in CIP-004-5 6.5 to confirm that access privileges were correct and the

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~minimum~~were correct or that they were the those that that the Responsible Entity determined necessary for performing assigned work functions, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary ~~to perform the~~ for performing assigned work functions. ~~(6.5)~~ ~~OR~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~The Responsible Entity did not verify the access privileges to BES Cyber System Information according to the timeframe in CIP-004-5 6.6 to confirm that access privileges were correct and the minimum necessary to perform the assigned work functions. (6.6)~~ ~~OR~~ ~~The Responsible Entity did not identify when CIP Exceptional Circumstances were invoked and/or revoked (6.7)~~ ~~OR~~ • ~~The Responsible Entity did not have a documented~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						process for access management.
R7	Same Day Operations and Operations Planning	Medium	N/ARevocation of access to BES Cyber Information was not accomplished for 1 or more individuals within the specified time frame (7.3); OR User accounts on BES Cyber Assets were not revoked for one or more individuals within the specified time frame (7.4); OR User passwords on BES Cyber Asset shared accounts were not changed for one or more individuals within the specified time frame; (7.5) OR	The Responsible Entity did not revoke unneeded unescorted physical or electronic access according to within the specified times in CIP-004-5 R7 for one individualsindividual who was terminated, resigned, was reassigned, or transferred. (7.1 and 7.2)	The Responsible Entity did not revoke unneeded unescorted physical or electronic access according to the specified times in CIP-004-5 R7 for two individuals who were terminated, resigned, reassigned or transferred. (.(7.1 and 7.2)	The Responsible Entity did not have a documented process for initiating the unescorted physical or electronic access revocation process; OR The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for three or more individuals who were terminated, resigned, reassigned, or transferred. (7.1 and 7.2) OR The Responsible Entity did not have a documented process for access revocation.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Following the determination and documentation of extenuating operating circumstances, passwords for shared accounts were not changed for one or more individuals within 10 days following the end of the extenuating operating circumstances. (7.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reference sound security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Guidance: Describe example mechanisms used to demonstrate the availability of this information

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the ~~following~~ required items appropriate to personnel roles and responsibilities from Table ~~R4.~~R2. The training may consist of multiple modules and multiple delivery mechanisms.

Note: Provide guidance or a local definition of "role appropriate" as it is used in this standard.

Requirement R3:

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official ~~identified in Requirement R1~~ or their delegate and impact the reliability of the BES or emergency response.

NOTE: Program specified exceptional circumstances can include a specified individual to declare an emergency.

Requirement R4 and R5:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access when called for in CIP-~~011~~004-1 Table R4 – Personnel Risk Assessment, except for program specified exceptional circumstances that are approved by the single senior management official ~~identified in Requirement R1~~ or their delegate and impact the reliability of the BES or emergency response, to ensure that personnel who have such access have had their

identity verified, then been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, or individuals who may have resided in locations from where it is not possible to obtain a criminal history records check.

Requirement R6:

Authorization for electronic and unescorted physical access and access to BES Cyber System ~~information~~Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly and annual reviews. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The annual privilege review is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e~~.~~., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g~~.~~., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R6 is included

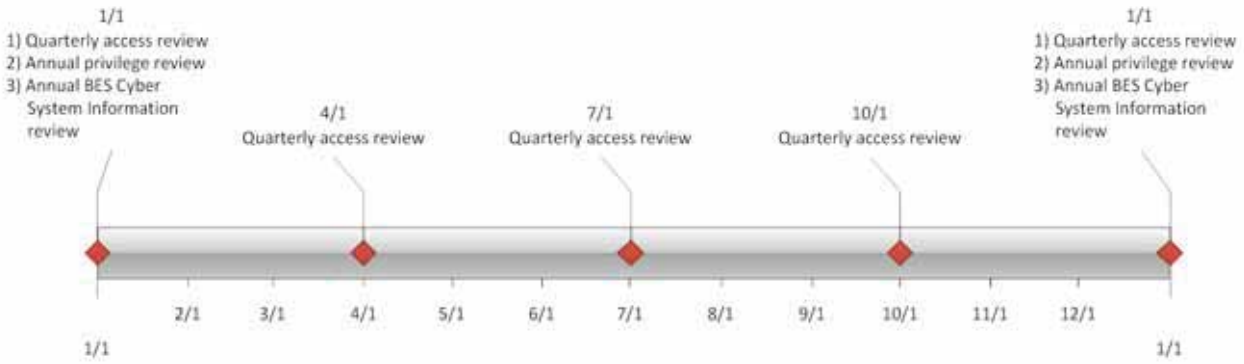

below.

Separation of duties should be considered when performing the reviews in Requirement R6. The person reviewing should be different than the person provisioning access.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R6 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R7:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common examples and possible processes on when the termination action occurs are provided in the following table.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human ~~resource~~resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Termination prior to notification	Human ~~resource~~resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human ~~resource~~resources personnel are notified of the termination and ~~works~~work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human ~~resource~~resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	~~No action is required.~~Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in ~~7~~Requirement R7.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents ~~an~~a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, the requirement states a review of access privileges must be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-5

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities described in 4.2.2

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   4.1.7 Reliability Coordinator

   4.1.8 Transmission Operator

   4.1.9 Transmission Owner

   4.2. Facilities:

   4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

   4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **High Impact BES Cyber Systems with dial-up connectivity** – Only applies to high impact BES Cyber Systems with dial-up connectivity.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems with dial-up connectivity** – Only applies to medium impact BES Cyber Systems with dial-up connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column.
- **Electronic Access Points** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column.

B. Requirements and Measures

Rationale for R1: The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter".

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	All BES Cyber Assets and associated Protected Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	Evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable Cyber Assets within each ESP.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*	
1.2	High Impact BES Cyber Systems with External Routable Connectivity Medium Impact BES Cyber Systems with External Routable Connectivity Associated Protected Cyber Assets	All External Routable Connectivity through the ESP must be through an identified Electronic Access Point (EAP).	Evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and BES Cyber System.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the rationale for granting access, and deny all other access by default.	Evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
Reference to prior version: *CIP-005-4, R2.1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.*	
1.4	High Impact BES Cyber Systems with dial-up connectivity Medium Impact BES Cyber Systems with dial-up connectivity	Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	Evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
Reference to prior version: *CIP-005-4, R2.3*		**Change Rationale:** *Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have a method for detecting malicious communications.	Evidence may include, but is not limited to: 1. Evidence that intrusion detection systems are functioning: • Configuration files of intrusion detection systems deployed to monitor an EAP; or • Logs that were generated by an intrusion detection system; and 2. Documentation showing where intrusion detection systems were deployed.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.*	

Rationale for R2: Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements or guidance documents are available to either require or recommend how secure remote access to BES Cyber Systems can or should be accomplished. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

Additional information is provided in *Guidance for Secure Interactive Remote Access* published by NERC in July 2011.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable items in *CIP-005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Protected Cyber Assets	Utilize an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	Evidence may include, but is not limited to, network diagrams or architecture documents.
Reference to prior version: *New*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Protected Cyber Assets	Utilize encryption for all Interactive Remote Access sessions that terminate at an Intermediate Device in order to protect the confidentiality and integrity of each Interactive Remote Access session.	Evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.
Reference to prior version: *CIP-007-5, R3.1*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Protected Cyber Assets	Require multi-factor authentication for all Interactive Remote Access sessions. Factors must be at least two of the three following categories: • Something the individual knows (including, but not limited to, passwords or PINs. User ID is not an authentication factor); • Something the individual has (including, but not limited to, tokens, digital certificates, or smart cards); or • Something the individual is (including, but not limited to, fingerprints, iris scans, or other biometric characteristic).	Evidence may include, but is not limited to, architecture documents detailing the authentication factors used.
Reference to prior version: *CIP-007-5, R3.2*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity failed to document one or more processes for *CIP-005-5 Table R1 – Electronic Security Perimeter* according to Requirement R1. OR The Responsible Entity failed to document 5% or less of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document 5% or less of inbound and outbound access permissions, including	The Responsible Entity failed to document more than 5% but less than or equal to 10% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document more than 5% but less than or equal to 10% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part 1.3.	The Responsible Entity failed to document more than 10% but less than or equal to 15% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document more than 10% but less than or equal to 15% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part 1.3.	The Responsible Entity failed to document more than 15% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document more than 15% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part 1.3. OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the rationale for granting access according to Requirement R1, part 1.3.			did not have all BES Cyber Assets and associated Protected Cyber Assets connected to a network via a routable protocol within a defined ESP according to Requirement R1, part 1.1. OR External Routable Connectivity through the ESP was not through an identified EAP according to Requirement R1, part 1.2. OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default according to

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Requirement R1, part 1.3. OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible according to Requirement R1, part 1.4. OR The Responsible Entity did not have a method for detecting malicious communications according to Requirement R1, part 1.5.
R2	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity failed to document one or more processes for *CIP-005-5 Table R2 – Interactive Remote*	The Responsible Entity failed to implement the required multi-factor authentication according to	The Responsible Entity failed to implement one of the following: • Intermediate	The Responsible Entity failed to implement two or more of the following:

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Access according to Requirement R2.	Requirement R2, Part 2.3.	Device according to Requirement R2, Part 2.1; OR • Encryption according to Requirement R2, Part 2.2.	• Intermediate Device according to Requirement R2, Part 2.1 (2.1); • Encryption according to Requirement R2, Part 2.2; OR • Multi-factor authentication according to Requirement R2, Part 2.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The standard does not require segmenting of BES Cyber Systems by impact classification, and many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and systems within the ESP will be elevated to the level of the highest impact BES Cyber System present in the ESP. The standard handles this by defining all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, the each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large

ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable, connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the SDT's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then the Requirement R2 requirements also apply.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear that this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the ~~first~~second posting of ~~the~~ Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center~~".~~."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-5

3. **Purpose:** ~~Standard CIP-005-5 requires the identification of all Electronic Access Points on the~~To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter~~(s), the protection of the communication through those points, and specific protections for interactive user remote access.~~ in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities described in 4.2.2

   ~~4.1.2~~4.1.3 Generator Operator

   ~~4.1.3~~4.1.4 Generator Owner

   ~~4.1.4~~4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   ~~4.1.5~~4.1.7 Reliability Coordinator

   ~~4.1.6~~4.1.8 Transmission Operator

   ~~4.1.7~~4.1.9 Transmission Owner

   4.2. Facilities:

   4.2.1 ~~that are part of any of the following systems~~**Load Serving Entity:** One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

   ~~4.2.1~~4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS ~~program required by a NERC~~ or ~~Regional Reliability Standard~~

- ~~A UVLS~~UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional ~~reliability standard~~Reliability Standard
- ~~A~~A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- ~~Its Transmission Operator's restoration plan~~
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~4.2.2~~4.2.3 Responsible Entities listed in 4.1 other than ~~Generator Operator~~

~~4.2.3~~4.2.4 ~~Generator Owner~~

~~4.2.4~~4.2.5 ~~Interchange Coordinator~~

~~4.2.5 Load-Serving Entity~~ ~~that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or regional Reliability Standard~~

~~4.2.6 NERC~~

~~4.2.7 Regional Entity~~

~~4.2.8~~4.2.6 ~~Reliability Coordinator~~

~~4.2.9~~4.2.7 ~~Transmission Operator~~

~~4.2.10~~4.2.8 ~~Transmission Owner~~

4.3. ~~Facilities:~~

~~4.3.1 Load Serving Entity:~~ ~~One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~4.3.2~~ **Distribution Providers**~~: One or more Facilities that are part of any of the following systems or programs designed, installed,~~ **and** ~~operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~
- ~~A Special Protection System or Remedial Action Scheme~~
- ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~

~~4.3.3~~4.3.1 **Load-Serving Entities**: All ~~**other Responsible Entities: All**~~ BES Facilities.

~~4.3.4~~4.3.2 **Exemptions:** The following are exempt from Standard CIP-~~005~~002-5:

~~4.3.4.1~~4.3.2.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.3.4.2~~4.3.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.3.4.3~~4.3.2.3 In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~4.3.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.~~

5. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter ~~as applicable~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show

documentation and implementation of ~~specific elements required~~applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e~~.~~., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards. Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~
- **High Impact BES Cyber Systems** – Applies to ~~each~~ BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and

categorization processes. ~~Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact~~

- **High Impact BES Cyber Systems with dial-up connectivity** – Only applies to high impact BES Cyber Systems~~. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems~~ with dial-up connectivity.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with dial-up connectivity** – Only applies to medium impact BES Cyber Systems with dial-up connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to ~~Medium Impact~~medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- ~~**Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.~~
- ~~**Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.~~
- ~~**Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.~~
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column.
- **Electronic Access Points** – Applies at Electronic Access Points ~~(with External Routable Connectivity or dial-up connectivity)~~ associated with a referenced high impact BES Cyber System~~.~~

- ~~**Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~
- ~~**Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact~~ or medium impact BES Cyber ~~Systems. These hardware and devices are excluded~~System in the ~~definition of Physical Access Control Systems.~~ applicability column.

B. Requirements and Measures

~~**Rationale for R1:** The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.~~

~~**Summary of Changes:** CIP-005 R1 has taken more of a focus on the discrete Electronic Access points rather than the logical "perimeter".~~

~~CIP-005 R1.2 has been deleted. This requirement was definitional in nature and used to bring dialup modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists, therefore there is no need for this requirement.~~

~~CIP-005 R1.1 and 1.3 were also definitional in nature and have been deleted as separate requirements but the concepts were integrated into the definitions of ESP and EAP.~~

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations~~]~~].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	~~Low~~High Impact BES Cyber Systems ~~with External Routable Connectivity~~ Medium Impact BES Cyber Systems	~~Define technical or procedural controls to restrict unauthorized electronic access.~~All BES Cyber Assets and associated Protected Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	Evidence may include, but is not limited to, ~~documented technical and procedural controls that exist and have been implemented~~a list of all ESPs with all uniquely identifiable Cyber Assets within each ESP.
Reference to prior version: *CIP-005-4, R1*		~~**Change Rationale:** *Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones and to prevent access to an aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES.*~~**Change Rationale:** *Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*	
1.2	High Impact BES Cyber Systems with External Routable Connectivity Medium Impact BES Cyber Systems~~.~~ ~~Associated Physical Access Control Systems~~ with External Routable Connectivity Associated Protected Cyber Assets	~~Control and secure all routable and dial-up connectivity~~All External Routable Connectivity through the ~~use of~~ESP must be through an identified Electronic Access ~~Points (EAPs~~Point (EAP).	Evidence may include, but is not limited to~~:~~ ~~• Network~~, network diagrams showing ~~EAP identification or~~ ~~• A list of uniquely identifiable Cyber Assets within the BES Cyber System~~all external routable communication paths and ~~associated~~the identified EAPs.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and BES Cyber System.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.3	Electronic Access Points ~~at~~ for High Impact BES Cyber Systems Electronic Access Points ~~at~~for Medium Impact BES Cyber Systems ~~with External Routable Connectivity.~~	Require ~~explicit~~ inbound and outbound access permissions ~~at each identified Electronic Access Point using routable protocols~~, including ~~explicit criteria~~the rationale for granting ~~or denying~~ access ~~permissions~~, and deny all other access by default.	Evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only ~~explicit~~permitted access is allowed and that each access rule has a documented reason.
Reference to prior version: *CIP-005-4, R2.1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having ~~justification~~a reason for what it allows through the EAP in both inbound and outbound directions.*	
1.4	~~Electronic Access Points that use dial-up access for non-Interactive Remote Access at~~ High Impact BES Cyber Systems with dial-up connectivity ~~Electronic Access Points that use dial-up access for non-Interactive Remote Access at~~ Medium Impact BES Cyber Systems~~.~~ with dial-up connectivity	Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	Evidence may include, but is not limited to, a documented process ~~identified in Requirement R1, Part 1.4~~ that describes how the Responsible Entity is providing authenticated access through each dial~~-~~-up ~~Electronic Access Point~~connection.
Reference to prior version: *CIP-005-4, R2.3*		**Change Rationale:** *~~Changed to refer to the defined term Electronic Access Point.~~ Added clarification ~~as to the goal of "secure", which is~~ that dial-up connectivity should perform authentication so that the BES Cyber System ~~should~~is not ~~be~~ directly accessible with a phone number only.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.5	Electronic Access Points ~~with External Routable Connectivity at~~for High Impact BES Cyber Systems Electronic Access Points ~~with External Routable Connectivity at~~for Medium Impact BES Cyber Systems at Control Centers~~.~~	~~A documented~~Have a method for detecting malicious communications ~~at each EAP~~.	Evidence may include, but is not limited to: 1. Evidence that intrusion detection systems are functioning: ~~1.~~• Configuration files of ~~an~~ intrusion detection systems deployed ~~at~~to monitor an EAP; or ~~2.~~• Logs that were generated by an intrusion detection system; and ~~3.~~2. Documentation showing where intrusion detection systems were deployed.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Per FERC Order No. 706, ~~p~~Paragraphs 496-503, ~~ESP's~~ESPs need two distinct security measures such that the ~~cyber assets~~Cyber Assets do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear this is not simple redundancy of firewalls, thus the ~~drafting team~~SDT has decided to add the security measure of malicious traffic inspection ~~(intrusion detection systems / intrusion protection systems)~~as a requirement for these ESPs.*	

Rationale for R2: Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of ~~large~~ electric sector entities, necessitate changes to industry security control standards. Currently, no requirements or guidance documents are available to either require or recommend how secure remote access to BES Cyber Systems can or should be accomplished. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

Additional information is provided in *Guidance for Secure Interactive Remote Access* published by NERC in July 2011.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations~~]~~].*

M2. Evidence must include the documented processes that collectively address each of the applicable items in *CIP-005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Protected Cyber Assets	~~Require~~Utilize an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	Evidence may include, but is not limited to, network diagrams or architecture documents.
Reference to prior version: *New*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Protected Cyber Assets	~~Require~~Utilize encryption for all Interactive Remote Access sessions that terminate at an Intermediate Device in order to protect the confidentiality and integrity of each Interactive Remote Access session.	Evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.
Reference to prior version: *CIP-007-5, R3.1*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Protected Cyber Assets	Require multi-factor authentication for all Interactive Remote Access sessions. Factors must be at least two of the three following categories: • Something the individual knows (including, but not limited to, passwords or PINs. User ID is not an authentication factor); • Something the individual has (including, but not limited to, tokens, digital certificates, or smart cards); or • Something the individual is (including, but not limited to, fingerprints, iris scans, or other biometric characteristic).	Evidence may include, but is not limited to, architecture documents detailing the authentication factors used.~~ Note that a UserID is not considered an authentication factor.~~
Reference to prior version: *CIP-007-5, R3.2*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity~~; or~~
- ~~If the Responsible Entity works for~~ shall serve as the Compliance Enforcement Authority ("CEA") unless the ~~Regional Entity, then the~~ applicable entity is owned, operated, or controlled by the Regional Entity ~~will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.~~
- ~~For Responsible Entities that are also Regional Entities,~~. In such cases the ERO or a Regional ~~Entity~~entity approved by ~~the ERO and~~ FERC or other applicable governmental ~~authorities shall serve as the Compliance Enforcement Authority.~~
- ~~For NERC, a third-party monitor without vested interest in the outcome for NERC~~authority shall serve as the ~~Compliance Enforcement Authority~~CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until ~~found compliant~~mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning and Same Day Operations**	**Medium**	~~N/A~~The Responsible Entity failed to document one or more processes for *CIP-005-5 Table R1 – Electronic Security Perimeter* according to Requirement R1. OR The Responsible Entity failed to document 5% or less of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document 5% or less of inbound and outbound access	~~N/A~~The Responsible Entity failed to document more than 5% but less than or equal to 10% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document more than 5% but less than or equal to 10% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part	~~N/A~~The Responsible Entity failed to document more than 10% but less than or equal to 15% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document more than 10% but less than or equal to 15% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part	~~The Responsible Entity did not define any technical or procedural controls to restrict unauthorized electronic access~~ The Responsible Entity failed to document more than 15% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity ~~did not establish Electronic Access Points to control and secure~~failed to document more than 15% of inbound and

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			permissions, including the rationale for granting access according to Requirement R1, part 1.3.	1.3.	1.3.	outbound access permissions, including the rationale for granting access ~~to its~~according to Requirement R1, part 1.3. OR The Responsible Entity did not have all BES Cyber ~~Systems~~Assets and associated Protected Cyber Assets connected to a network via a routable protocol within a defined ESP according to Requirement R1, part 1.1. OR External Routable Connectivity through the ESP was not through an identified EAP according to Requirement R1, part

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						1.2. OR The Responsible Entity did not ~~establish explicit~~require inbound and outbound access permissions ~~at each identified EAP that utilizes routable protocols~~and deny all other access by default according to Requirement R1, part 1.3. OR The Responsible Entity did not perform authentication ~~before~~when establishing dial-up connectivity with the BES Cyber System~~ for an EAP that uses dial-up access~~, where technically feasible according to

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Requirement R1, part 1.4. OR The Responsible Entity did not ~~deploy methods to detect~~have a method for detecting malicious communications~~.~~ according to Requirement R1, part 1.5.
R2	**Operations Planning and Same Day Operations**	**Medium**	~~N/A~~The Responsible Entity failed to document one or more processes for *CIP-005-5 Table R2 – Interactive Remote Access* according to Requirement R2.	~~N/A~~The Responsible Entity failed to implement the required multi-factor authentication according to Requirement R2, Part 2.3.	~~N/A~~The Responsible Entity failed to implement one of the following: • Intermediate Device according to Requirement R2, Part 2.1; OR • Encryption according to Requirement R2, Part 2.2.	-The Responsible Entity ~~did not~~failed to implement ~~an~~ two or more of the following: • Intermediate Device ~~between the Interactive Remote Access cyber asset and the BES Cyber System or Protected Cyber Asset~~according to Requirement R2,

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Part 2.1 (2.1); • Encryption according to Requirement R2, Part 2.2; OR ~~The Responsible Entity did not implement encryption to protect the confidentiality and integrity of all Interactive Remote Access sessions~~ ~~OR~~ • ~~The Responsible Entity did not implement multifactor~~Multi-factor authentication ~~for all Interactive Remote Access sessions~~according to Requirement R2, Part 2.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

CIP-005-5, Requirement R1 requires ~~that~~ segmenting of BES Cyber Systems ~~must be segmented~~ from other systems of differing trust levels by requiring controlled ~~electronic access points~~Electronic Access Points between the different trust zones. ~~ESP's~~ Electronic Security Perimeters are also ~~are~~ used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication ~~capabilities~~capability.

All BES Cyber Systems that are connected to ~~be protected~~a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The standard does not require segmenting of BES Cyber Systems by impact classification, and many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and systems within the ESP will be elevated to the level of the highest impact BES Cyber System present in the ESP. The standard handles this by defining all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, the each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access ~~Points (EAP's) that~~ Point (EAP) must control traffic into and out of the ~~BES Cyber System.~~ESP. Responsible Entities ~~(RE's)~~ should know what traffic needs to cross an EAP and document those ~~justifications and insure~~reasons to ensure the ~~EAP's~~EAPs limit the traffic to only those known~~, justified~~ communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from

controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols~~ and dialup modems. Direct serial, non-routable connections are not included.~~ . Direct serial, non-routable, connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

~~The intent of securing dialup~~As for dial-up connectivity, the SDT's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity ~~is established directly~~ to the BES Cyber Asset~~ with only a phone number.~~. If a ~~dialup~~dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is ~~not functioning as an Electronic Access Point.~~a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party ~~when connectivity is granted~~before completing the connection to the BES Cyber ~~Asset~~System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then the Requirement R2 requirements also apply.

~~Since low impact BES Cyber Systems can impact BES Reliability Operating Services in real time, they should not be located directly on public networks or other networks of lesser trust. The intent is to prevent access to an aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES. Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones.~~

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection

if one measure fails or is mis-configured. The Order makes clear that this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems
2. **Number:** CIP-006-5
3. **Purpose:** To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities described in 4.2.2

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   4.1.7 Reliability Coordinator

   4.1.8 Transmission Operator

   4.1.9 Transmission Owner

   4.2. Facilities:

   4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

   4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column.
- **Locally mounted hardware or devices at the Physical Security Perimeter** – Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale: Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed.

Summary of Changes: The entire contents of CIP-006-5 are intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

Added details to address FERC Order No. 706, Paragraph 572, directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.

R1. Each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that collectively include all of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plan or plans that collectively include all of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems	Define operational or procedural controls to restrict physical access.	Evidence may include, but is not limited to, documentation that operational or procedural controls exist and have been implemented.
Reference to prior version: *CIP-006-4c, R2.1 for Physical Access Control Systems* *New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity*		**Change Description and Justification:** *Change Description and Justification: To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected by a Physical Access Control System.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Utilize at least one physical access control to allow physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	Evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how access is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.
Reference to prior version: *CIP006-4c, R3 & R4*		**Change Description and Justification:** *This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Where technically feasible, utilize two or more different physical access controls to collectively allow physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	Evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how access is controlled by two or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.
Reference to prior version: CIP006-4c, R3 & R4		**Change Description and Justification:** *The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.* *Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.* *FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized circumvention of a physical access control into a Physical Security Perimeter.	Evidence may include, but is not limited to, documentation of controls that monitor the Physical Security Perimeter for unauthorized circumvention of a physical access control into a Physical Security Perimeter.
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*	
1.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Issue an alarm or alert in response to detected unauthorized circumvention of a physical access control into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection.	Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized circumvention of a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.6	Physical Access Control Systems Associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	Have controls that monitor each Physical Access Control System twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized physical access to a Physical Access Control System.	Evidence may include, but is not limited to, documentation of controls that monitor the Physical Security Perimeter for unauthorized circumvention of a physical access control into a Physical Security Perimeter.
Reference to prior version: CIP006-4c, R5		**Change Description and Justification:** *Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	
1.7	Physical Access Control Systems Associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the unauthorized physical access.	Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.
Reference to prior version: CIP006-4c, R5		**Change Description and Justification:** *Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	Evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.
Reference to prior version: CIP-006-4c, R6		**Change Description and Justification:** *CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.* *Examples of logging methods have been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	Evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change.*	

Rationale: To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

R2. Each Responsible Entity shall implement one or more documented visitor control programs that include each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require continuous escorted access of visitors (individuals who are known or guests, and not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.
Reference to prior version: *CIP-006-4c, R1.6.2*		**Change Description and Justification:** *Added the ability to not do this during CIP Exceptional Circumstances.*	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require manual or automated logging of the entry and exit of visitors into the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
Reference to prior version: *CIP-006-4c R1.6.1*		**Change Description and Justification:** *Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.*	
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain visitor logs for at least ninety calendar days.	Evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change*	

Rationale: To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable items in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each applicable item in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
3.1	Physical Access Control Systems associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	Evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.
Reference to prior version: *CIP-006-4c, R8.1 and R8.2*		**Change Description and Justification:** *Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.*	

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
3.2	Physical Access Control Systems associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	Document outages for physical access control, logging, and alerting systems and retain the outage records for at least 12 calendar months.	Evidence may include, but is not limited to, the outage records and availability of outage records for the preceding 12 calendar months.
Reference to prior version: *CIP-006-4c, R8.3*		**Change Description and Justification:** *No change.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has documented and implemented physical access controls, but logging of authorized physical entry through any Physical Security Perimeter does not provide sufficient information to uniquely identify the individual and date of entry. (1.8) OR The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days. (1.9)	The Responsible Entity has documented and implemented physical access controls, but it does not alert for unauthorized physical access to Physical Access Control Systems or does not communicate such alerts within 15 minutes to identified personnel(1.7) OR The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days. (1.9)	The Responsible Entity has documented and implemented physical access controls, but does not alert for unauthorized circumvention of a physical access control into a Physical security Perimeter or does not communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity has does not have controls that monitor each Physical Access Control System twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized physical access to a Physical	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access to only those individuals who are authorized. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one method does not exist to restrict access to Medium Impact BES Cyber Systems with External Routable Connectivity or External Dial-up Connectivity. (1.2) OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Access Control Systems. (1.6) OR The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days. (1.9)	The Responsible Entity has documented and implemented physical access controls, but two or more different methods do not exist to restrict access to High Impact BES Cyber Systems. (1.3) OR The Responsible Entity has does not have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized circumvention of a physical access control into a Physical Security Perimeter. (1.4) OR The Responsible Entity retained physical

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						access logs for less than 45 calendar days. (1.9)
R2	**Same-Day Operations**	**Medium**	N/A	The Responsible Entity included a visitor control program in its physical security plan, but did not log each of the initial entry and last exit dates and times of the visitor on a daily basis, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity included a visitor control program in its physical security plan, but failed to retain visitor logs for at least ninety days. (2.3)	The Responsible Entity included a visitor control program in its physical security plan, but it did not meet the requirements for continuous escort. (2.1)	The Responsible Entity has failed to include or implement a visitor control program to provide required escorted access of visitors within any Physical Security Perimeter. (2.1)
R3	**Long Term Planning**	**Lower**		The Responsible Entity has documented and	The Responsible Entity did not document	The Responsible Entity has not documented

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity did not retain outage records for at least 12 months of outages for physical access control, logging, and alerting systems. (3.2)	implemented a maintenance and testing program for Physical Access Control Systems, but the testing was not performed on a cycle of not more than 24 calendar months. (3.1)	outages for physical access control, logging, and alerting systems for Physical Access Control Systems as required. (3.2)	and implemented a maintenance and testing program for Physical Access Control Systems. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods to restrict physical access include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in

combination with a guard-monitored remote camera and door release, where the “guard” has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (i.e., key or card key) would provide access through both.

Typically any opening greater than 96 square inches, with one side greater than six inches in length, would be considered an access point into the Physical Security Perimeter. Protective measures such as bars, wire mesh, or other permanently installed metal barrier could be used to reduce the opening size, as long as it is leaves no opening greater than 96 square inches, or no more than six inches on its shortest side.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a Point of Contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Outage records should address when the installed control, monitor, and logging systems or hardware at access points are broken or unavailable.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. ~~CSO706 SDT appointed (August 7, 2008)~~
4. ~~Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)~~
5. ~~Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)~~
6. ~~Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)~~
7. ~~Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)~~
8. ~~Version 5 of CIP-002 to CIP-011 posted~~First posting for 60-day formal comment period and concurrent ballot (~~mm-dd-yy)~~November 2011).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012

Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]

~~1.~~2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center~~"~~."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated ~~version number~~Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees~~-~~.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-5

3. Purpose: ~~Standard CIP-006-5 requires the implementation of~~ To manage physical access to BES Cyber Systems by specifying a physical security plan ~~for the protection~~in support of protecting BES Cyber Systems~~.~~ against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities ~~that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~ **described in 4.2.2**

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~
- ~~A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard~~
- ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

~~4.1.6~~4.1.7 Reliability Coordinator

4.1.8 ~~that are part of any of the following systems~~Transmission Operator

4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

4.1.74.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- A UVLS programA Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard

4.1.8 NERC

4.1.9 Regional Entity

4.1.104.2.3 A Protection System that applies to **Reliability Coordinator**

4.1.11 Transmission **Operator**

4.1.12 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated forwhere the protection of the BES:

- A UFLS programProtection System is required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

- **All other** Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.34.2.4 **Responsible Entities**: **listed in 4.1 other than Distribution Providers and Load-Serving Entities**: All BES Facilities.

4.2.44.2.5 **Exemptions:** The following are exempt from Standard CIP-006002-5:

4.2.4.14.2.5.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.24.2.5.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systemsSystems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.-R. Section 73.54.

4.2.4.44.2.5.3 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opensMost requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the requiredapplicable items in [Table Reference].*" The referenced table requires the specific elementsapplicable items in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required.applicable items in the documented processes.. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e~~.~~., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and categorization processes.~~ Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to ~~Medium Impact~~medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.~~
- ~~**Low Impact BES Cyber Systems** – Applies to BES Cyber Systems not categorized as High Impact or Medium Impact according to the CIP-002-5 identification and categorization processes.~~
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding ~~High or Medium Impact BES Cyber Systems.~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column.
- ~~**Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.~~
- ~~**Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~
- **Locally ~~Mounted Hardware or Devices Associated with Defined~~ mounted hardware or devices at the Physical ~~Boundaries~~Security Perimeter** – Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) ~~associated with~~at a ~~Defined~~ Physical ~~Boundary for High~~Security Perimeter associated with a corresponding high impact BES Cyber System or ~~Medium Impact~~medium impact BES Cyber ~~Systems.~~System with External Routable Connectivity in the applicability column, and that does not

contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale: Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed.

Summary of Changes: The entire contents of CIP-006-5 ~~were~~are intended to constitute a physical security program~~, though~~. This represents a change from previous versions, since there was no specific requirement ~~dictating the need for such a~~ to have a physical security program in previous versions of the standards, only requirements for physical security plans.

Added details to address FERC Order No. 706, ~~paragraph~~Paragraph 572, directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706 ~~p575 directive~~, Paragraph 575.

R1. Each Responsible Entity shall implement one or more documented physical security plans ~~that include each~~for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that collectively include all of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations~~]~~].*

M1. Evidence must include~~s~~ each of the documented physical security plan or plans that collectively include ~~each~~all of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems ~~Low Impact BES Cyber Systems.~~	Define operational or procedural controls to restrict physical access.	Evidence may include, but is not limited to, ~~documented~~documentation that operational ~~and~~or procedural controls exist and have been implemented.
Reference to prior version: *CIP-006-4c, R2.1 for Physical Access Control Systems* *New Requirement for ~~Low~~Medium Impact BES Cyber Systems not having External Routable Connectivity*		**Change Description and Justification:** *Change Description and Justification: To allow for programmatic protection controls as a baseline~~, this~~ (which also includes how the entity plans to protect ~~Low~~Medium Impact BES Cyber Systems ~~and~~that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access~~–~~). Physical Access Control Systems do not themselves need to be protected by a Physical Access Control System.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Utilize at least one physical access control to ~~establish one or more Defined~~allow physical access into each applicable Physical ~~Boundaries that restricts access~~ Security Perimeter to only those individuals ~~that are~~who have authorized~~.~~ unescorted physical access.	Evidence may include, but is not limited to, language in the physical security plan that describes ~~the physical boundaries~~each Physical Security Perimeter and how ~~ingress and egress~~access is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.
Reference to prior version: *CIP006-4c, R3 & R4*		**Change Description and Justification:** *This requirement has been made more general to allow for alternate measures of restricting physical access ~~to reflect the change from Physical Security Perimeter to Defined Physical Boundary. The specific examples that specify~~. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section~~.~~.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Utilize~~Where technically feasible, utilize two or more different ~~and complementary~~ physical access controls to ~~establish one or more Defined Physical Boundaries that restricts~~collectively allow physical access into Physical Security Perimeters to only those ~~users that are~~individuals who have authorized~~,~~ ~~where technically feasible.~~ unescorted physical access.	Evidence may include, but is not limited to, language in the physical security plan that describes the ~~physical boundaries~~Physical Security Perimeters and how ~~ingress and egress~~access is controlled by two or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.
Reference to prior version: CIP006-4c, R3 & R4		**Change Description and Justification:** *The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.* *Added to address FERC Order No. 706 ~~p572~~, Paragraph 572, related directives for physical security defense in depth.* *FERC Order No. 706 ~~p575~~, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via ~~multifactor~~multi-factor authentication or layered ~~defined physical boundary~~Physical Security Perimeter(s).*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized circumvention of a physical access control into a Physical Security Perimeter.	Evidence may include, but is not limited to, documentation of controls that monitor the Physical Security Perimeter for unauthorized circumvention of a physical access control into a Physical Security Perimeter.
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*	
1.~~4~~5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Issue ~~real-time alerts (to individuals responsible for response)~~an alarm or alert in response to detected unauthorized circumvention of a physical access ~~through any access point in a Defined~~control into a Physical ~~Boundary.~~Security Perimeter to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection.	Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of ~~alerts~~ an alarm or alert in response to unauthorized circumvention of a physical access ~~through any access point in a Defined~~control into a Physical ~~Boundary~~Security Perimeter and additional evidence that ~~these alerts were~~the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that ~~these alerts were~~the alarm or alert was generated and communicated.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section~~.~~.*	
1.6	Physical Access Control Systems Associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	Have controls that monitor each Physical Access Control System twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized physical access to a Physical Access Control System.	Evidence may include, but is not limited to, documentation of controls that monitor the Physical Security Perimeter for unauthorized circumvention of a physical access control into a Physical Security Perimeter.
Reference to prior version: CIP006-4c, R5		**Change Description and Justification:** *Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	
1.~~5~~7	~~Associated~~ Physical Access Control Systems Associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue ~~real-time alerts (to individuals responsible for response)~~an alarm or alert in response to detected unauthorized physical access to a Physical Access Control ~~Systems.~~ System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the unauthorized physical access.	Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of ~~alerts~~an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that ~~these~~the alarm or alerts ~~were~~was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that ~~these alerts were~~the alarm or alert was generated and

CIP-006-5 Table R1 – Physical Security Plan			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
			communicated.
Reference to prior version: CIP006-4c ~~R2.2~~, R5		**Change Description and Justification:** *Addresses the ~~old~~prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.~~6~~8	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical ~~entry~~access into each ~~Defined~~ Physical ~~Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient~~Security Perimeter, with information to ~~uniquely~~ identify the individual and date and time of entry.	Evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into ~~Defined~~each Physical ~~Boundaries~~Security Perimeter and additional evidence to demonstrate that this logging ~~and recording~~ has been implemented, such as logs of physical access into ~~Defined~~ Physical ~~Boundaries~~Security Perimeters that show the individual and the date and time of entry into ~~Defined~~ Physical ~~Boundaries~~Security Perimeter.
Reference to prior version: CIP-006-4c, R6		**Change Description and Justification:** *CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the ~~Defined~~ Physical ~~Boundary~~Security Perimeter.* *Examples of logging methods have been moved to the Guidelines and Technical Basis section~~-~~.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	Evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change.*	

Rationale: To control when personnel without authorized unescorted physical access can be in any ~~Defined~~ Physical ~~Boundaries~~Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in ~~table~~Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

R2. Each Responsible Entity shall implement ~~its~~one or more documented visitor control ~~program~~programs that ~~includes~~include each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations~~]~~.]*

M2. Evidence must include ~~the~~one or more documented visitor control ~~program~~programs that collectively ~~includes~~include each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Require continuous escorted access of visitors (individuals who are known or guests, and not authorized for unescorted physical access) within ~~any Defined~~each Physical ~~Boundary~~Security Perimeter, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within ~~Defined~~ Physical ~~Boundaries~~Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.
Reference to prior version: *CIP-006-4c, R1.6.2*		**Change Description and Justification:** ~~*No change*~~*Added the ability to not do this during CIP Exceptional Circumstances*.	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~A process requiring~~Require manual or automated logging of the entry and exit of visitors into the Physical Security Perimeter that includes date and time of the initial entry and last exit ~~on a per 24-hour basis~~, the visitor's name, and the name of an individual point of contact~~.~~ responsible for the visitor, except during CIP Exceptional Circumstances.	Evidence may include, but is not limited to, language in a visitor control program that ~~provides logging of the entry and exit~~requires continuous escorted access of visitors ~~including date, time, and visitor name along with the individual point of contact;~~within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs ~~for each Defined Physical Boundary that~~ that include the ~~same~~ required information.
Reference to prior version: *CIP-006-4c R1.6.1*		**Change Description and Justification:** *~~Addressed~~Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-~~-~~entry ~~requirements~~scenarios of the same person in a day (log first entry and ~~added the point of contact which is~~ last exit), and name of the person who ~~can be considered the~~ is responsible or sponsor for the visitor. There is no ~~need~~requirement to document the escort or handoffs between escorts.*	

CIP-006-5 Table R2 – Visitor Control Program			
Part	~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain visitor logs for at least ninety calendar days.	Evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change*	

Rationale: To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, ~~paragraph~~Paragraph 581, directives ~~for~~to test more frequently than every three

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable items in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning~~]~~].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each applicable item in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
3.1	~~Associated~~ Physical Access Control Systems associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices ~~associated with Defined~~at the Physical ~~Boundaries~~Security Perimeter associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	~~Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance~~Maintenance and testing of ~~the~~each Physical Access Control ~~Systems~~System and locally mounted hardware or devices at the ~~Defined~~ Physical ~~Boundary~~ Security Perimeter at least once every 24 calendar months to ensure ~~the required functionality is being provided~~they function properly.	Evidence may include, but is not limited to~~-~~, a maintenance and testing program that provides for testing ~~the~~each Physical Access Control ~~Systems~~System and locally mounted hardware or devices associated with ~~Defined~~each applicable Physical ~~Boundaries prior to commissioning and~~Security Perimeter at least once every 24 calendar months ~~thereafter,~~ and ~~provides~~ additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed ~~at least once~~ on each applicable device or system at least once every 24 calendar months.
Reference to prior version: *CIP-006-4c, R8.1 and R8.2*		**Change Description and Justification:** *Added details to address FERC Order No. 706 ~~p581~~, Paragraph 581 directives to test more frequently than every three years. ~~It was felt annually~~The SDT determined that annual testing was too often and agreed on two years.*	

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measures**
3.2	~~Associated~~ Physical Access Control ~~or Monitoring~~ Systems associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity	~~Log dates, time, and duration for failures or~~Document outages ~~of~~for physical access control, logging, and alerting systems~~.~~ and retain the outage records for at least 12 calendar months.	Evidence may include, but is not limited to, ~~availability of~~ the outage records and availability of outage records for the preceding 12 calendar months.
Reference to prior version: *CIP-006-4c, R8.3*		**Change Description and Justification:** ~~*Outage records shall be generated but the retention period is addressed in the retention section*~~*No change*.	

C. Compliance

1. Compliance Monitoring Process:

5.1.1.1. Compliance Enforcement Authority-:

- The Regional Entity; or
- If the Responsible Entity works for shall serve as the Compliance Enforcement Authority ("CEA") unless the Regional Entity, then the applicable entity is owned, operated, or controlled by the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- For responsible entities that are also Regional Entities,. In such cases the ERO or a Regional Entityentity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For NERC, a third-party monitor without vested interest in the outcome for NERCauthority shall serve as the Compliance Enforcement AuthorityCEA.

5.2.1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliantmitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

5.3.1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting

- Complaint

5.4.1.4. Additional Compliance Information:

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has documented and implemented physical access controls, but logging of authorized physical entry through any ~~Defined~~ Physical ~~Boundary~~Security Perimeter does not provide sufficient information to uniquely identify the individual and date of entry. (~~Part~~ 1.~~7~~8) OR The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days. (1.9)	The Responsible Entity has documented and implemented physical access controls, but it does not alert for unauthorized physical access to Physical Access Control Systems ~~(Part 1.5~~or does not communicate such alerts within 15 minutes to identified personnel(1.7) OR The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days. (1.9)	The Responsible Entity has documented and implemented physical access controls, but does not alert for unauthorized ~~access through any access point in a Defined Physical Boundary. (Part 1.4~~circumvention of a physical access control into a Physical security Perimeter or does not communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity has ~~documented and implemented physical access~~does not have controls~~, but does not initiate a response within 15 minutes of a~~	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access to only those individuals who are authorized. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one method does not exist to restrict access to Medium Impact BES Cyber Systems with External Routable Connectivity or External Dial-up Connectivity. (1.2) OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~detected~~ that monitor each Physical Access Control System twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized physical access ~~into~~to a ~~Defined~~ Physical ~~Boundary. (Part~~ Access Control Systems. (1.6) OR The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days. (1.9)	The Responsible Entity has documented and implemented physical access controls, but two or more different ~~and complementary~~ methods do not exist to restrict access to High Impact BES Cyber Systems. (~~Part~~ 1.3) OR The Responsible Entity has does not have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized circumvention of a physical access control into a Physical Security Perimeter. (1.4) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						retained physical access logs for less than 45 calendar days. (1.9)
R2	**Same-Day Operations**	**Medium**	N/A	The Responsible Entity included a visitor control program in its physical security plan, but did not log each of the initial entry and last exit dates and times of the visitor on a daily basis, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity included a visitor control program in its physical security plan, but failed to retain visitor logs for at least ninety days. (2.3)	The Responsible Entity included a visitor control program in its physical security plan, but it ~~does~~did not meet the requirements ~~of~~for continuous escort. (2.1)	The Responsible Entity has failed to include or implement a visitor control program to provide required escorted access of visitors within any ~~Defined~~ Physical ~~Boundary protecting BES Cyber Systems.~~ Security Perimeter. (2.1)
R3	**Long Term**	**Lower**	~~N/A~~	The Responsible Entity	The Responsible Entity	The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning		The Responsible Entity did not retain outage records for at least 12 months of outages for physical access control, logging, and alerting systems. (3.2)	has documented and implemented a maintenance and testing program for Physical Access Control Systems, but the testing ~~is~~ was not performed on a cycle of not more than 24 calendar months. (3.1)	~~has documented and implemented a maintenance and testing program, but~~did not ~~all outage records regarding~~document outages for physical access ~~controls~~control, logging, and alerting ~~are generated~~systems for Physical Access Control Systems as required. (3.2)	has not documented and implemented a maintenance and testing ~~programs.~~ program for Physical Access Control Systems. (3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary ~~control~~mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods to restrict physical access include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the ~~Defined~~ Physical ~~Boundary~~Security Perimeter.

Methods to ~~alert on~~monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706~~ p572~~, Paragraph 572, directive~~, directed the intent of~~ discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more ~~Defined~~ Physical ~~Boundaries~~Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin~~-~~ code (something you know and something you have), or a card key and biometric scanner (something you have

and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (i.e~~.~~., key or card key) would provide access through both.

Typically any opening greater than 96 square inches, with one side greater than six inches in length, would be considered an access point into the ~~Defined~~ Physical ~~Boundary.~~Security Perimeter. Protective measures such as bars, wire mesh, or other permanently installed metal barrier could be used to reduce the opening size, as long as it is leaves no opening greater than 96 square inches, or no more than six inches on its shortest side.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the ~~Defined~~ Physical ~~Boundary~~Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

~~It is~~The SDT also ~~felt~~determined that a Point of Contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the ~~Defined~~ Physical ~~Boundary.~~Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Outage records should address when the installed control, monitor, and logging systems or hardware at access points are broken or unavailable.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-5

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities described in 4.2.2

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   4.1.7 Reliability Coordinator

   4.1.8 Transmission Operator

   4.1.9 Transmission Owner

   4.2. Facilities:

   4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

   4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:
Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column.

B. Requirements and Measures

Rationale for R1: The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are needed.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable items in *CIP-007-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For applicable Cyber Assets and where technically feasible, enable only logical network accessible ports needed, including port ranges or services where needed to handle dynamic ports.	Evidence may include, but is not limited to: • Listings of the needed ports by Cyber Asset or class of Cyber Assets; • Listings of the listening ports on the Cyber Assets from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.
Reference to prior version: *CIP-007-4, R2.1 and R2.2*		**Change Description and Justification:** *The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.*	

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	Evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
Reference to prior version: *NEW*		**Change Description and Justification:** *In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.*	

Rationale for R2: Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" there has been confusion as to what constitutes the availability. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-007-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	A patch management program for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	Evidence must include documentation of a patch management program and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.
Reference to prior version: *CIP-007, R3*		**Change Rationale:** *The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches. Documenting the source is used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Evaluate the security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified in Part 2.1.	Evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources within 30 calendar days of availability.
Reference to prior version: *CIP-007, R3.1*		**Change Rationale:** *Similar to the current wording but added "from the source or sources identified in 2.1" to clarify the 30-day time frame.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For applicable patches identified in Part 2.2, create a dated plan or revise an existing plan within 30 calendar days of the evaluation completion. The plan shall include the Responsible Entity's planned actions to mitigate the vulnerabilities exposed by each security patch and a timeframe to complete these mitigations.	Evidence may include, but is not limited to, a dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities exposed by the security patch and a timeframe for the completion of these mitigations.
Reference to prior version: *CIP-007, R3.2*		**Change Rationale:** *The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For each plan created or revised in Part 2.3, implement the plan as created or revised within the timeframe specified in the plan, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to: • Records of the installation of the patch; • Records of implementation of vendor recommended mitigations; • Exports from automated patch management tools that provide installation date; • Verification of BES Cyber System Component software revision; • Registry exports that show software has been installed; or • Evidence that affected services have been disabled.
Reference to prior version: *CIP-007, R3.2*		**Change Rationale:** *Similar to the current wording but added "from the source or sources identified in Part 2.1" to clarify the 30-day time frame.*	

Rationale for R3: Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.

Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"

In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R3 – Malicious Code Prevention. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable items in *CIP-007-5 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Deploy method(s) to deter, detect, or prevent malicious code.	Evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
Reference to prior version: *CIP-007-4, R4; CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.*	
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Mitigate the threat of identified malicious code.	Evidence may include, but is not limited to: • Predetermined response actions for malicious code detection; • Configuration of anti-virus response actions (e.g., quarantine, alert, etc.) to detected malicious code; or • Configuration of white-listing application to notify appropriate personnel of unauthorized applications.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-4, R4* *CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Update malicious code protections that use signatures or patterns at least once within 35 calendar days of each available signature or pattern release (this does not require use of every available release, but that for every release that is available, at least one update has occurred within 35 calendar days from that release), except for signature or pattern releases that the Responsible Entity documents as negatively affecting the Cyber Asset or BES Cyber System.	Evidence may include, but is not limited to: • Documentation showing the configuration of signature, or pattern updates for automated controls; or • Work logs showing the signature, or pattern updates for manual controls.
Reference to prior version: *CIP-007-4, R4; CIP-007-4, R4.2*		**Change Rationale:** *See the Summary of Changes. This part is written to ensure that signatures or patterns are updated within 35 days of release, but does not require installation of all releases so long as any given update occurs within 35 calendar days of each release. The part does not require update within 35 days of a particular release in cases where the Responsible Entity documents that the signature or pattern release negatively affects the Cyber Asset or BES Cyber System. Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.*	

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the immediate detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor and respond to audit processing failures.

Summary of Changes: Beginning in Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor."

The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the System.

In addition, this requirement sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

R4. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable items in *CIP-007-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. detected and logged failed access attempts at Electronic Access Points; 4.1.2. detected and logged successful and failed login attempts; 4.1.3. detected and logged malicious software; and 4.1.4. detected and logged malicious activity.	Evidence may include, but is not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required event types.
Reference to prior version: *CIP-005-4, R3; CIP-007-4, R5, R5.1.2, R6.1, andR6.3*		**Change Description and Justification:** *This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Generate alerts for security events that the Responsible Entity determines necessitate a real-time alert, that includes, as a minimum, each of the following types of events where technically feasible: 4.2.1. detected malicious activity; and 4.2.2. detected failure of 4.1 event logging.	Evidence may include, but is not limited to paper or system-generated listing of security events which the Responsible Entity determined necessitate real-time alerts and paper or system generated list showing how real-time alerts are configured.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.2*		**Change Description and Justification:** *This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Activate a response to detected event logging failures before the end of the next calendar day.	Evidence may include, but is not limited to, documentation describing the response and its timing, or an attestation indicating that no such events occurred.
Reference to prior version: *New Requirement*		**Change Rationale:** *This requirement was derived from NIST 800-53 version 3 AU-5, which addresses response to audit processing failures. Misunderstandings with previous versions considered the failure of the security event monitoring and alerting system itself to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain BES Cyber System security-related event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	Evidence may include, but is not limited to: 1. security-related event logs from the past 90 days; 2. records of disposition of security-related event logs beyond 90 days up to the evidence retention period; and 3. paper or system generated reports showing log retention configuration set at 90 days or greater.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.4*		**Change Rationale:** *No substantive change.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.5	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Review a summarization or sampling of logged events at a minimum every two weeks to identify undetected Cyber Security Incidents.	Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.5*		**Change Description and Justification:** *Beginning in Paragraph 525 and also 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.*	

Rationale for R5: To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Changing default passwords closes an easily exploitable vulnerability in many systems and applications.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Summary of Changes (From R5): CIP-007-4, Requirements R5.2.2 and R5.2.3 requiring the identification and management of shared account access have been removed. These requirements already exist in the authorization, security event monitoring and revocation of access, and guidance for these requirements makes clear the consideration of shared accounts. The requirement to identify and determine acceptable use for these accounts remains and the standard includes additional guidance on types of accounts to identify and appropriate use of these account types.

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT feels these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

R5. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R5 – System Access Controls. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-007-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Enforce authentication of all user access, where technically feasible.	Evidence may include, but is not limited to, documentation describing how access is authenticated.
Reference to prior version: *CIP-007-4, R5*		**Change Rationale:** *The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate must authorize enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Evidence may include, but is not limited to, a listing of accounts by account types and signed documentation or workflow by a CIP Senior Manager or delegate showing the approval of enabled or generic account types in use for the BES Cyber System.
Reference to prior version: *CIP-007-4, R5.2 and R5.2.1*		**Change Rationale:** *CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*	
5.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Identify individuals who have authorized access to shared accounts.	Evidence may include, but is not limited to, listing of shared accounts and the individuals who have access to each shared account.
Reference to prior version: *CIP-007-4, R5.2.2*		**Change Rationale:** *No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Change default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on Cyber Assets.	Evidence may include, but is not limited to: • Records of a procedure that passwords are changed when new devices are deployed; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
Reference to prior version: *CIP-007-4, R5.2.1*		**Change Rationale:** *The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Evidence may include, but is not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations by individuals that the procedurally enforced passwords meet the password parameters.

Reference to prior version: *CIP-007-4, R5.3*	**Change Rationale:** *CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.*

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For password-based user authentication, either technically or procedurally enforce password changes or an obligation to change the password at least once each calendar year, not to exceed 15 calendar months between changes.	Evidence may include, but is not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations by individuals that the procedurally enforced passwords meet the password parameters.
Reference to prior version: *CIP-007-4, R5.3.3*		**Change Rationale:** **This was originally Requirement R5.5.3, but moved to add "external routable connectivity" to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Limit, where technically feasible, the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful login attempts.	Evidence may include, but is not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.
Reference to prior version: *New Requirement*		**Change Rationale:** *Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	N/A		The Responsible Entity did not have a documented process that included the applicable items in *CIP-007-5 Table R1*. (R1) OR The Responsible Entity had unneeded logical network accessible ports enabled. OR The Responsible Entity had no methods to protect unnecessary physical input/output ports used for network connectivity, console commands, or removable media.
R2	**Operations Planning**	**Medium**	The Responsible Entity did not evaluate the	The Responsible Entity did not evaluate the	The Responsible Entity did not evaluate the	The Responsible Entity did not have a

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified. OR The Responsible Entity did not create a plan or revise and existing plan within 30 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.	security patches for applicability within 45 calendar days of availability of the patch from the source or sources identified. OR The Responsible Entity did not create a plan or revise and existing plan within 45 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.	security patches for applicability within 60 calendar days of availability of the patch from the source or sources identified. OR The Responsible Entity did not create a plan or revise and existing plan within 60 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.	documented process that included the applicable items in *CIP-007-5 Table R2*. (R2) OR The Responsible Entity did not have a patch management program for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets or did not track for the release cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists. OR The Responsible Entity did not implement the plan as created or

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						revised within the timeframe specified in the plan.
R3	**Same Day Operations**	**Medium**	Where signatures or patterns are used, the Responsible Entity did update malicious code protections that use signatures or patterns at least once within 45 calendar days of each available signature or pattern release, but not within 35 calendar days. (3.3)	Where signatures or patterns are used, the Responsible Entity did update malicious code protections that use signatures or patterns at least once within 55 calendar days of each available signature or pattern release, but not within 45 calendar days. (3.3).	Where signatures or patterns are used, the Responsible Entity did not update malicious code protections that use signatures or patterns at least once within 55 calendar days of each available signature or pattern release. (3.3).	The Responsible Entity did not have a documented process that included the applicable items in *CIP-007-5 Table R3*. (R3) OR The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. OR The Responsible Entity did not mitigate the threat of identified malicious code.
R4	**Same Day Operations and**	**Medium**	N/A	The Responsible Entity failed to identify and implement methods to	The Responsible Entity failed to activate a response to rectify the	The Responsible Entity did not have a documented process

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations Assessment			review a summarization of logged events every two weeks.	event logging failure before the end of the next calendar day. OR The Responsible Entity failed to identify and implement methods to retain BES Cyber System security-related events for at least the last 90 consecutive days, where technically feasible.	that included the applicable items in *CIP-007-5 Table R4*. (R4) OR The Responsible Entity failed to implement methods to generate alerts for events that it determines to necessitate a real-time alert. OR The Responsible Entity failed to log detected events necessary for the identification and after-the-fact investigation of Cyber Security Incidents.
R5	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity failed to implement procedures to authorize the use of administrative, shared,	The Responsible Entity did not have a documented process that included the applicable items in

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					default, and other generic account types. OR The Responsible Entity failed to implement procedures to identify the individuals with authorized access to shared accounts.	*CIP-007-5 Table R5*. (R5) OR The Responsible Entity failed to implement methods to validate credentials before granting electronic access to BES Cyber Systems. OR The Responsible Entity failed to implement procedures for password-based user authentication. OR The Responsible Entity failed to implement procedures to change or have unique default passwords, where technically feasible.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

Requirement 1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border is a requirement in CIP-005, Requirement R1 to protect the network and does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with a low tier documents establishing the more detailed process followed for individual systems. Low tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware, or those Cyber Assets that have no existing source of patches such as vendors that no longer exist.

2.2. Responsible Entities are to perform an assessment of security related patches within 30 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. The security patches, hotfixes, and/or updates or compensating measures may reduce the reliability of the system. The Responsible Entity must be allowed to evaluate their individual risk exposure and determine if actions must be taken to secure the system. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. For those security related patches that are determined to be applicable, the Responsible Entity must create a dated plan within 30 days which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities exposed by the security patch. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration". If the entity is going to install the patch, the plan can consist of a a simple record that normal patch installation process from 2.1 will be followed and designate the date of the patch installation.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code and should not require a TFE.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor

the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The requirement is written to handle two update frequency situations.

1) For those technologies that are providing very frequent updates (at most monthly but often daily or sometimes hourly), the updates applied to the applicable Cyber Assets should be no more than 35 calendar days old. In these instances, this is a 'maximum staleness' requirement. It does not require that every update within a 35 day period be applied, but that the currently installed update be no more than 35 days old.

2) For those technologies that provide less frequent updates that are more than 35 days, the requirements should be applied within 35 days of the last available update.

Testing of signature or pattern updates is not required. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times. Other Cyber Assets should have any updates tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device, but the entity disables or neglects to enable that logging, it is a violation. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3. Event logging failures occur when the components of the BES Cyber System cannot log events the Responsible Entity designated in 4.1. The most common reason for event logging failures is the event log being filled up beyond its configured storage threshold. However, there may be any number of other reasons for event logging failures.

For centralized logging systems, it should not be considered a failure if communication goes down between the Cyber Asset and the logging system if the Cyber Asset can store the logs locally for a period of time until the communication comes back up.

4.5. Reviewing logs every two weeks can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.

5.4. Where possible, any accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber

Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.

The requirement to change passwords permits the Responsible Entity to determine the periodicity of the password change in their policies and procedures based on a number of factors. The following table suggests appropriate periodicity requirements for passwords based on these factors.

Account Type	Impact Level	Significance of passwords in preventing unauthorized access	Existing Service Agreements	Suggested Periodicity of Password Change
User account password	High	Primary access path	None.	90 days
User account password	Medium	Primary access path	None.	180 days
Shared account Password for a microprocessor relay, PLC, RTU, etc.	Medium	Local access path. Individuals must authenticate at an upstream device prior to gaining access.	None.	During regularly scheduled maintenance
Shared account password for a generation control system	Medium	Local access path. Individuals must authenticate at an upstream device prior to gaining access.	None.	During scheduled plant outages
Administrative account passphrase with 15+ characters	High or Medium	Local access path. Remote user must be authenticated using a different account	None.	One year
System account password with 25+ pseudo-random characters	High or Medium	Local access path	None.	Two years or more

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the ~~first~~second posting of ~~the~~ Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center~~".~~."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-5

3. **Purpose:** ~~Standard CIP-007-5 requires the implementation of~~ To manage system security by specifying select technical ~~mechanisms for reducing the risk of loss of availability due to degradation~~, operational, and ~~misuse of~~procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities described in 4.2.2

   ~~4.1.2~~4.1.3 Generator Operator

   ~~4.1.3~~4.1.4 Generator Owner

   ~~4.1.4~~4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   ~~4.1.5~~4.1.7 Reliability Coordinator

   ~~4.1.6~~4.1.8 Transmission Operator

   ~~4.1.7~~4.1.9 Transmission Owner

   4.2. Facilities:

   4.2.1 ~~that are part of any of the following systems~~**Load Serving Entity:** One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

   ~~4.2.1~~4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS ~~program required by a NERC~~ or ~~Regional Reliability Standard~~

- ~~A UVLS~~UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- A Special Protection System or Remedial Action Scheme ~~required by a NERC or Regional Reliability Standard~~
- ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~

~~4.2.2~~4.2.3 where the~~**Generator Operator**~~

~~4.2.3~~4.2.4 ~~**Generator Owner**~~

~~4.2.4~~4.2.5 ~~**Interchange Coordinator**~~

~~**4.2.5 Load-Serving Entity** that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~**4.2.6 NERC**~~

~~**4.2.7 Regional Entity**~~

~~4.2.8~~4.2.6 ~~**Reliability Coordinator**~~

~~4.2.9~~4.2.7 ~~**Transmission Operator**~~

~~4.2.10~~4.2.8 ~~**Transmission Owner**~~

4.3. ~~**Facilities:**~~

~~**4.3.1 Load Serving Entity:** One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~**4.3.2 Distribution Providers**: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~
- ~~A~~ Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard

- A ~~Transmission~~ Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- ~~Its Transmission Operator's restoration plan~~
- ~~**All other**~~ Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~**4.3.3**~~**4.3.1 Responsible Entities**~~:~~ **listed in 4.1 other than Distribution Providers and Load-Serving Entities**: All BES Facilities.

~~**4.3.4**~~**4.3.2 Exemptions:** The following are exempt from Standard CIP-~~007~~002-5:

~~**4.3.4.1**~~**4.3.2.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~**4.3.4.2**~~**4.3.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~**4.3.4.3**~~**4.3.2.3** In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~**4.3.4.4** Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.~~

5. Background:

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter~~ as applicable~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of ~~specific elements required~~applicable items in

the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e~~.~~., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards. Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and categorization processes. ~~Responsible Entities can implement common controls~~

that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impactmedium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impactmedium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impactmedium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems.high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systemshigh impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systemshigh impact BES Cyber System or medium impact BES Cyber System in the applicability column.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion

~~sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

B. Requirements and Measures

Rationale for R1: The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and ~~physical I/O ports~~services.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are ~~documented with reasons why they are necessary. In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.~~needed.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations~~]~~.]*

M1. Evidence must include the documented processes that collectively include each of the applicable items in *CIP-007-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Disable or restrict access to unnecessary~~For applicable Cyber Assets and where technically feasible, enable only logical network accessible ports ~~and document the need for any remaining logical network accessible~~needed, including port ranges or services where needed to handle dynamic ports.	Evidence may include, but is not limited to~~, documentation~~: • Listings of the ~~need for each network-accessible port and screen shots showing the accessible~~needed ports ~~of BES~~by Cyber Asset or class of Cyber Assets~~.~~; • Listings of the listening ports on the Cyber Assets from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.
Reference to prior version: *CIP-007-4, R2.1 and R2.2*		**Change Description and Justification:** *The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.*	

CIP-007-5 Table R1– Ports and Services			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	~~Disable or restrict~~Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	Evidence may include, but is not limited to, documentation ~~stating specific or~~ showing types of protection of physical input/output ports ~~to restrict and screen shots or pictures showing the ports restricted~~, either logically through system configuration or physically using a port lock or signage.
Reference to prior version: *NEW*		**Change Description and Justification:** *In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.*	

Rationale for R2: Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source-(s) to monitor for release of security related patches, ~~hotfixes~~hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" there has been confusion as to what constitutes the availability. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning~~]~~].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-007-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.~~ A patch management program for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	Evidence ~~may~~must include~~, but is not limited to,~~ documentation of a ~~list~~patch management program and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or ~~BES~~ Cyber Asset basis. ~~The list could be sorted by BES Cyber System or source.~~
Reference to prior version: ~~*New*~~*CIP-007, R3*		**Change Rationale:** ~~*Defining*~~*The requirement is brought forward from previous CIP versions with the addition of defining* *the source(s) that a Responsible Entity monitors for the release of security related patches~~*, hotfixes, and/or updates will provide a starting point for assessing the effectiveness of the patch management program.*~~*.* *Documenting the source is~~ *also* *used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Evaluate the security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified in Part 2.1.	Evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources within 30 calendar days of availability.
Reference to prior version: *CIP-007, R3.1*		**Change Rationale:** *Similar to the current wording but added "from the source or sources identified in 2.1" to clarify the 30-day time frame.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.~~2~~3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Identify~~For applicable ~~security-related~~ patches ~~or updates and~~ identified in Part 2.2, create a ~~remediation~~dated plan~~,~~ or revise an existing ~~remediation~~ plan~~,~~ within 30 calendar days of ~~release from~~ the ~~identified source that addresses~~evaluation completion. The plan shall include the Responsible Entity's planned actions to mitigate the vulnerabilities ~~within~~ exposed by each security patch and a ~~defined~~ timeframe~~.~~ to complete these mitigations.	Evidence may include, but is not limited to, ~~an assessment conducted by, referenced by, or on behalf of a Registered Entity of security-related patches or updates released by the documented sources, and a~~ a dated ~~remediation~~ plan showing when and how the vulnerability will be addressed~~.~~ , to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities exposed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-5 Table R2 – Security Patch Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-007, R3.~~1~~2*		***~~Change Rationale:~~*** *~~Similar to the current wording but added "from the identified source" to establish where the release is from. The current wording: "The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" has led to varying opinions as to what constitutes "availability" of the patches or upgrades. The addition attempts to clarify where the release is from.~~* ***Change Rationale:*** *The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.~~3~~4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~A process for remediation, including any exceptions~~For each plan created or revised in Part 2.3, implement the plan as created or revised within the timeframe specified in the plan, except for CIP Exceptional Circumstances.	Evidence may include, but is not limited to: • Records of the installation of the patch; • Records of implementation of vendor recommended mitigations; • Exports from automated patch management tools that provide installation date; • Verification ~~screen captures that show~~of BES Cyber System Component software revision; • Registry exports that show software has been installed; or • Evidence that affected services have been disabled~~;~~. ~~• Implementation evidence of software configuration changes recommended by the operating system or Control System vendors.~~

CIP-007-5 Table R2 – Security Patch Management			
Part	~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets	**Requirements**	**Measures**
Reference to prior version: *CIP-007, R3.2*		~~**Change Rationale:** This is the same concept as in the current CIP-007 R3.2 wording however a 30 day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used. Splitting the implementation of security related patches, hotfixes, and/or updates into a separate item from compensating measures will provide granularity. Automated processes allow the implementation to be documented and confirmed electronically in a short time period. Manual processes may take an extended period of time to complete documentation of the installation. Priority should be given to the implementation rather than the documentation.~~**Change Rationale:** *Similar to the current wording but added "from the source or sources identified in Part 2.1" to clarify the 30-day time frame.*	

Rationale for R3: Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable ~~components~~Cyber Assets of a BES Cyber ~~system~~System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

~~The requirement for Maintenance Cyber Assets or media in 3.4 is intended to ensure that devices used for maintenance do not accidently introduce malicious code into the BES Cyber System or introduce an unauthorized external access point to the BES Cyber System.~~

~~This requirement also clarifies that these devices may be temporarily connected to the BES Cyber System, but do not become a part of the BES Cyber System, nor are they considered Protected Cyber Assets. These devices may be temporarily connected locally to the BES Cyber System for maintenance, but must be protected from introducing malicious code.~~

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of ~~TFE's~~TFEs as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of ~~cyber assets~~Cyber Assets in scope of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every ~~component~~Cyber Asset. The BES Cyber System is the object of protection.

Beginning in ~~paragraph~~Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"

In ~~paragraph~~Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5, Table R3 – Malicious Code Prevention. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations~~]~~].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable items in *CIP-007-5, Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Deploy method(s) to deter, detect, or prevent malicious code.	Evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (~~i.~~e.g., through traditional antivirus, system hardening, policies, etc.).
Reference to prior version: *CIP-007-4, R4* *; CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.*	
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Disarm or remove~~Mitigate the threat of identified malicious code.	Evidence may include, but is not limited to: • Predetermined response actions for malicious code detection; • Configuration of anti-virus response actions (~~i.~~e.g., quarantine, alert, etc.) to detected malicious code; or • Configuration of white-listing application to notify appropriate personnel of unauthorized applications.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets	**Requirements**	**Measures**
Reference to prior version: *CIP-007-4, R4* *CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Update malicious code protections that use signatures or patterns at least once within ~~30~~35 calendar days of each available signature or pattern release (this does not require use of every available release, but that for every release that is available, at least one update ~~availability (where~~has occurred within 35 calendar days from that release), except for signature or pattern releases that the ~~malicious code protections use signatures or patterns).~~ Responsible Entity documents as negatively affecting the Cyber Asset or BES Cyber System.	Evidence may include, but is not limited to~~, (i) current signature or pattern updates, and (ii) either screen shots~~: • Documentation showing the configuration of signature, or pattern updates for automated controls~~,~~; or ~~work~~ • Work logs showing the signature, or pattern updates for manual controls.

~~**Reference to prior version:**~~ ~~*CIP-007-4 R4*~~ ~~*CIP-007-4 R4.2*~~	~~**Change Rationale:** *See the Summary of Changes.*~~

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
~~3.4~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ ~~Associated Protected Cyber Assets~~	~~Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets.~~	~~Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code.~~

Reference to prior version: ~~*New*~~*CIP-007-4, R4; CIP-007-4, R4.2*	~~**Change Rationale:** *FERC Order 706 paragraph 621 states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software. In addition, a common interpretation of the current standards is that any device connecting inside the ESP must at that point be in compliance with the full set of Standards. This requirement makes clear that the device performing maintenance is not considered a part of the BES Cyber System.*~~**Change Rationale:** *See the Summary of Changes. This part is written to ensure that signatures or patterns are updated within 35 days of release, but does not require installation of all releases so long as any given update occurs within 35 calendar days of each release. The part does not require update within 35 days of a particular release in cases where the Responsible Entity documents that the signature or pattern release negatively affects the Cyber Asset or BES Cyber System. Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.*

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
~~3.5~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ ~~Associated Protected Cyber Assets~~	~~Log each Transient Cyber Asset connection.~~	~~Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets.~~
~~**Reference to prior version:**~~ ~~*New*~~		~~**Change Rationale:** *FERC Order 706 paragraph 621 states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software. In addition, a common interpretation of the current standards is that any device connecting inside the ESP must at that point be in compliance with the full set of Standards. This requirement makes clear that the device performing maintenance is not considered a part of the BES Cyber System.*~~	

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the immediate detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor and respond to audit processing failures.

Summary of Changes: Beginning in ~~paragraph~~Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the ~~commission~~Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor~~".~~."

The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the ~~system~~System.

In addition, this requirement sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

R4. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment*~~]~~*.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable items in *CIP-007-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Log~~-generated~~ events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. ~~Any~~ detected and logged failed access attempts at Electronic Access Points; 4.1.2. ~~Any~~ detected and logged successful and failed login attempts; 4.1.3. ~~Any~~ detected ~~malware~~ and logged malicious software; and 4.1.4. ~~Any~~ detected ~~potential~~and logged malicious activity.	Evidence may include, but is not limited to, a paper or system generated listing of event ~~classes~~types for which the BES Cyber System is capable of detecting and, for generated events, is configured to ~~generate logs.~~log. This listing must include the required event types.
Reference to prior version: *CIP-005-4, R3~~,~~; CIP-007-4, R5, R5.1.2, R6.1, ~~R6~~andR6.3*		**Change Description and Justification:** *This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. ~~Changes made here clarify this term by allowing entities to first define these security events.~~ Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Generate alerts for security events that the Responsible Entity determines ~~to~~ necessitate a real-time alert, that includes, as a minimum, each of the following types of events where technically feasible: 4.2.1. detected malicious activity; and 4.2.2. detected failure of 4.1 event logging.	Evidence may include, but is not limited to paper or system-generated listing of ~~event classes and conditions~~ security events which the Responsible Entity determined necessitate real-time alerts~~; Assessment documentation~~ and paper or ~~report showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert; Screen-shots~~system generated list showing how real-time alerts are configured.
Reference to prior version: *CIP-005-4, R3.2~~,~~; CIP-007-4, R6.2*		**Change Description and Justification:** *This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Detect and activate~~Activate a response to detected event logging failures before the end of the next calendar day.	Evidence may include, but is not limited to, ~~(i) dated event logging failures~~documentation describing the response and ~~screen-shots showing how real-time alerts were configured~~ ~~(ii) dated records showing~~its timing, or an attestation indicating that ~~personnel were dispatched or a work ticket was opened to review and repair logging failures.~~no such events occurred.
Reference to prior version: *New Requirement*		**Change Rationale:** *This requirement was derived from NIST 800-53 version 3 AU-5, which addresses response to audit processing failures. ~~Some interpretations of version 4 CIP Cyber Security Standards~~Misunderstandings with previous versions considered the failure of the security event monitoring and alerting system itself to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Retain BES Cyber System security-related event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, where technically feasible.	Evidence may include, but is not limited to~~,~~: 1. security-related event logs from the past ~~ninety~~90 days~~ and~~ ; 2. records of disposition of security-related event logs beyond ~~ninety~~90 days up to the evidence retention period; and 3. paper or system generated reports showing log retention configuration set at 90 days or greater.
Reference to prior version: *CIP-005-4, R3.2~~,~~; CIP-007-4, R6.4*		**Change Rationale:** *No substantive change.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
4.5	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Review a summarization or sampling of logged events at a minimum every two weeks to identify ~~unanticipated BES~~undetected Cyber Security Incidents~~ and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day.~~.	Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred~~, and dated evidence showing that personnel were dispatched or a work ticket was opened to rectify the deficiency.~~.
Reference to prior version: *CIP-005-4, R3.2~~,~~; CIP-007-4, R6.5*		**Change Description and Justification:** *Beginning in ~~paragraph~~Paragraph 525 and also 628 of the FERC Order No. 706, the ~~commission~~Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.*	

Rationale for R5: To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Changing default passwords closes an easily exploitable vulnerability in many systems and applications.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Summary of Changes (From R5): CIP-007-4, Requirements R5.2.2 and R5.2.3 requiring the identification and management of shared account access have been removed. These requirements already exist in the authorization, security event monitoring and revocation of access, and guidance for these requirements makes clear the consideration of shared accounts. The requirement to identify and determine acceptable use for these accounts remains and the ~~Standard~~standard includes additional guidance on types of accounts to identify and appropriate use of these account types.

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of ~~6~~six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT feels these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

R5. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning~~]~~].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-007-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Validate credentials before granting electronic access to each BES Cyber System.~~ Enforce authentication of all user access, where technically feasible.	Evidence may include, but is not limited to, documentation describing how ~~users are~~access is authenticated ~~before being granted access and demonstrations showing authenticated access enforcement of internal and remote paths to the BES Cyber System~~.
Reference to prior version: *CIP-007-4, R5*		**Change Rationale:** *The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	The CIP Senior Manager or delegate must authorize enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Evidence may include, but is not limited to, a listing of accounts by account types and signed documentation or workflow by a CIP Senior Manager or delegate showing the approval of enabled or generic account types in use for the BES Cyber System.
Reference to prior version: *CIP-007-4, R5.2 and R5.2.1*		**Change Rationale:** *CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*	
5.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems with External Routable Connectivity. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Identify individuals who have authorized access to shared accounts.	Evidence may include, but is not limited to, listing of shared accounts and the individuals who have access to each shared account.
Reference to prior version: *CIP-007-4, R5.2.2*		**Change Rationale:** *No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Change default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on Cyber Assets.	Evidence may include, but is not limited to: • Records of a procedure that passwords are changed when new devices are deployed; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
Reference to prior version: *CIP-007-4, R5.2.1*		**Change Rationale:** *The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.*	

CIP-007-5 Table R5 – System Access Control			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.~~2~~5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~The CIP Senior Manager~~For password-based user authentication, either technically or ~~delegate must authorize~~procedurally enforce the ~~use~~following password parameters: 5.5.1. Password length that is, at least, the lesser of ~~administrator, shared, default,~~eight characters or the maximum length supported by the Cyber Asset; and ~~other generic account~~ Minimum password complexity that is the lesser of three or more different types~~.~~ 5.5.2. of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Evidence may include, but is not limited to~~, a listing~~: • System-generated reports or screen-shots of ~~accounts by account types~~the system-enforced password parameters, including length and ~~signed documentation or workflow by a CIP Senior Manager or delegate showing the approval of account types in use for~~complexity; or • Attestations by individuals that the ~~BES Cyber System.~~ procedurally enforced passwords meet the password parameters.

Reference to prior version: *CIP-007-4, R5.~~2, R5.2.1~~3*	**Change Rationale:** *CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this.* ~~**Change Rationale:** *CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*~~ *The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.*

~~5.3~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems.~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ ~~Associated Protected Cyber Assets~~	~~Identify individuals who have authorized access to shared accounts.~~	~~Evidence may include, but is not limited to, listing of shared accounts and the individuals who have access to each shared account.~~
~~**Reference to prior version:**~~ ~~*CIP-007-4 R5.2.2*~~		~~**Change Rationale:** *No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.*~~	

~~CIP-007-5 Table R5 – System Access Control~~			
~~Part~~	~~Applicability~~	~~Requirements~~	~~Measures~~
~~5.4~~	~~All Responsible Entities~~	~~Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required.~~	~~Evidence may include, but is not limited to:~~ ~~• Demonstration showing default vendor passwords have been changed, sampled on a locational basis.~~ ~~• Records of a procedure that passwords are changed when new devices are deployed.~~ ~~• Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.~~
~~**Reference to prior version:**~~ ~~*CIP-007-4 R5.2.1*~~		~~**Change Rationale:** *The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.*~~	

Part	Applicability	Requirements	Measures
5.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the BES Cyber System. 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the BES Cyber System. 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the BES Cyber System, the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses.	Evidence may include, but is not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length, complexity and periodicity of changing passwords. • Attestations by individuals that the procedurally enforced passwords meet the password parameters.

~~**Reference to prior version:**~~ ~~*CIP-007-4 R5.3*~~		~~**Change Rationale:** *CIP-007-4 R5.3 requires the use of passwords and specifies a specific policy of 6 characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process..~~	
5.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems ~~at Control Centers~~with External Routable Connectivity Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.~~For password-based user authentication, either technically or procedurally enforce password changes or an obligation to change the password at least once each calendar year, not to exceed 15 calendar months between changes.	Evidence may include, but is not limited to: • ~~Screen~~System-generated reports or screen-shots of the ~~account-lockout parameters~~ • ~~Rules in the alerting configuration showing how the~~ system~~-notified~~-enforced periodicity of changing passwords; or • Attestations by individuals ~~after a determined number of unsuccessful login attempts~~that the procedurally enforced passwords meet the password parameters.

Reference to prior version: ~~*New Requirement*~~*CIP-007-4, R5.3.3*	~~**Change Rationale:** *Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.*~~**Change Rationale:** **This was originally Requirement R5.5.3, but moved to add "external routable connectivity" to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.*

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Limit, where technically feasible, the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful login attempts.	Evidence may include, but is not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.
Reference to prior version: *New Requirement*		**Change Rationale:** *Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity~~; or~~
- ~~If the Responsible Entity works for~~ shall serve as the Compliance Enforcement Authority ("CEA") unless the ~~Regional Entity, then the~~ applicable entity is owned, operated, or controlled by the Regional Entity ~~will establish an agreement with~~. In such cases the ERO or ~~another~~a Regional entity approved by ~~the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.~~
- ~~If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and~~ FERC or other applicable governmental ~~authorities shall serve as the Compliance Enforcement Authority.~~
- ~~If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC~~authority shall serve as the ~~Compliance Enforcement Authority~~CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was ~~complaint~~compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until ~~found compliant~~mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	N/A	~~The Responsible Entity did not document the logical network accessible ports and include why the ports are necessary.~~	The Responsible Entity did not ~~disable or restrict access to unnecessary~~have a documented process that included the applicable items in *CIP-007-5 Table R1*. (R1) OR The Responsible Entity had unneeded logical network accessible ports enabled. OR The Responsible Entity ~~did not disable or restrict the use of~~had no methods to protect unnecessary physical input/output ports used for network connectivity, console commands, or

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						removable media.
R2	**Operations Planning**	**Medium**	~~N/A~~The Responsible Entity did not evaluate the security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified. OR The Responsible Entity did not create a plan or revise and existing plan within 30 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.	~~N/A~~The Responsible Entity did not evaluate the security patches for applicability within 45 calendar days of availability of the patch from the source or sources identified. OR The Responsible Entity did not create a plan or revise and existing plan within 45 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.	~~N/A~~The Responsible Entity did not evaluate the security patches for applicability within 60 calendar days of availability of the patch from the source or sources identified. OR The Responsible Entity did not create a plan or revise and existing plan within 60 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.	The Responsible Entity did not ~~identify~~have a ~~source or sources~~documented process that ~~are monitored for~~included the ~~release of security related patches, hotfixes, and/or updates for all software and firmware associated with the BES Cyber System or BES Cyber Assets.~~applicable items in *CIP-007-5 Table R2*. (R2) OR The Responsible Entity did not ~~identify applicable~~ have a patch management program for tracking, evaluating, and installing cyber

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						security patches for applicable Cyber Assets or did not track for the release cyber security ~~related~~ patches~~, hotfixes, and/or updates and create a remediation plan, or revise an existing remediation plan within 30 days of release from the identified source~~ for applicable Cyber Assets that are updateable and for which a patching source exists. OR The Responsible Entity did not implement the ~~remediation plan as required, except for CIP Exceptional Circumstances.~~ plan as created or

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						revised within the timeframe specified in the plan.
R3	**Same Day Operations**	**Medium**	~~N/A~~Where signatures or patterns are used, the Responsible Entity did update malicious code protections that use signatures or patterns at least once within 45 calendar days of each available signature or pattern release, but not within 35 calendar days. (3.3)	~~N/A~~Where signatures or patterns are used, the Responsible Entity did update malicious code protections that use signatures or patterns at least once within 55 calendar days of each available signature or pattern release, but not within 45 calendar days. (3.3).	~~The~~Where signatures or patterns are used, the Responsible Entity did not ~~deploy method(s) to deter, detect, or prevent~~update malicious code ~~on all Cyber Assets, Transient Cyber Assets and removable media.~~protections that use signatures or patterns at least once within 55 calendar days of each available signature or pattern release. (3.3).	The Responsible Entity did not have a documented process that included the applicable items in *CIP-007-5 Table R3.* (R3) OR The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. OR The Responsible Entity did not ~~disarm or remove~~ mitigate the threat of identified malicious code. ~~OR~~ ~~Where signatures or~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~patterns are used, the Responsible Entity did not deploy method(s) to update malicious code protections within 30 days of signature or pattern update availability.~~
R4	**Same Day Operations and Operations Assessment**	**Medium**	N/A	The Responsible Entity failed to identify and implement methods to review a summarization of logged events every two weeks ~~to identify unanticipated Cyber Security Incidents and potential event logging failures, and activate a response before the end of the next calendar day.~~	The Responsible Entity failed to ~~identify and implement methods to generate real-time alerts for event logging failures, and~~ activate a response to rectify the event logging failure before the end of the next calendar day. OR The Responsible Entity failed to identify and implement methods to retain BES Cyber System ~~generated~~ security-related events for at least the last 90	The Responsible Entity did not have a documented process that included the applicable items in *CIP-007-5 Table R4.* (R4) OR The Responsible Entity failed to ~~identify and~~ implement methods to generate alerts for events that it determines to necessitate a real-time alert. OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					consecutive days, where technically feasible.	The Responsible Entity failed to ~~identify and implement methods to~~ log ~~generated~~detected events ~~that it determines~~ necessary for the identification and after-the-fact investigation of Cyber Security Incidents.
R5	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity failed to implement procedures to authorize the use of administrative, shared, default, and other generic account types. OR The Responsible Entity failed to implement procedures to identify the individuals with authorized access to shared accounts.	The Responsible Entity did not have a documented process that included the applicable items in *CIP-007-5 Table R5.* (R5) OR The Responsible Entity failed to implement methods to validate credentials before granting electronic access to BES Cyber Systems.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity failed to implement procedures for password-based user authentication. OR The Responsible Entity failed to implement procedures to change or have unique default passwords, where technically feasible.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

Requirement 1 exists to reduce the attack surface of ~~BES~~ Cyber Assets by requiring entities to disable known unnecessary ports. The ~~intent is~~SDT intends for the entity to know what ~~is~~ network accessible ("listening") ports and associated services are accessible on their assets and systems, ~~why~~whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. ~~For the logical network ports this~~This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port~~.~~ or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP Wrappers, or other means on the ~~device~~Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore ~~it is~~ the ~~intent~~SDT intends that the control be on the device itself~~; blocking~~, or positioned inline in a non-bypassable manner. Blocking ports at ~~a perimeter~~the ESP border is a requirement in CIP-005, Requirement R1 to protect the network and does not ~~satisfy~~substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed ~~necessary.~~'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a ~~Defined~~Physical Security ~~Boundary~~Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive ~~with auto-run capability. In cases where the Component cannot logically restrict physical~~. The protection of these ports~~, entities should have clear signs or obstructions indicating the unnecessary ports are~~ can be accomplished in several ways including, but not limited to ~~be used.~~:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; ~~its~~the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional

measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with a low tier documents establishing the more detailed process followed for individual systems. Low tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

~~**2.1.** *Documenting the source*~~**2.1.** The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. ~~In the event~~A patch source is not required for Cyber Assets that have no updateable software or firmware~~ is~~, or those Cyber Assets that have no existing source of patches such as vendors that no longer ~~supported by~~exist.

2.2. Responsible Entities are to perform an assessment of security related patches within 30 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a ~~software or firmware vendor~~determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or ~~Control System vendor it can be noted in your source document.~~ will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. The security patches, hotfixes, and/or updates or compensating measures may reduce the reliability of the system. The Responsible Entity must be allowed to evaluate their individual risk exposure and determine if actions must be taken to secure the system.

~~**2.2.** The intent is for Responsible Entities to perform an assessment of security related patches as they are released from their monitored source and create a remediation plan for applicable patches as to how the vulnerability will or has already been remediated. An assessment should consist of determination of the applicability of the entity's specific environment and systems. IF the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, and the~~

steps the entity has previously taken or will take. If the entity has to take steps to mitigate this new vulnerability, the remediation plan will include a timeframe. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration". The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.32.3. For those security related patches that are determined to be applicable, the Responsible Entity must create a dated plan within 30 days which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities exposed by the security patch. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration". If the entity is going to install the patch, the plan can consist of a a simple record that normal patch installation process from 2.1 will be followed and designate the date of the patch installation.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

Common malware introduction methods include web browsing, email attachments, and portable storage media. **3.1.** Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware, it is not practical within the standard to prescribe how malware is to be addressed on each componentCyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis

which ~~components~~Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional ~~anti-virus~~antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or ~~components~~Cyber Assets that are of identical architecture, they may provide one process that describes how all the ~~components~~like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code and should not require a TFE.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies ~~that are updated in response to evolving threats or~~ depend on signatures or patterns of known attacks, the ~~entity must specify how~~effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The requirement is written to handle two update frequency situations.

1) For those technologies that are providing very frequent updates ~~are~~ (at most monthly but often daily or sometimes hourly), the updates applied to the applicable Cyber Assets should be no more than 35 calendar days old. In these instances, this is a 'maximum staleness' requirement. It does not require that every update within a 35 day period be applied, but that the currently installed update be no more than 35 days old.

2) For those technologies that provide less frequent updates that are more than 35 days, the requirements should be applied within 35 days of the last available update.

Testing of signature or pattern updates is not required. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times. Other Cyber Assets should have any updates tested before implementation where the result of a 'false positive' could

harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing ~~is~~should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. ~~The testing~~Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ~~insuring~~ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production. ~~This includes the instance where the update may provide a "false positive."~~

Requirement R4:

Refer to NIST 800-92 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the ~~Standard~~standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in ~~version~~Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device, but the entity disables or neglects to enable that logging, it is a violation. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to

know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3. Event logging failures occur when the components of the BES Cyber System cannot log events the Responsible Entity designated in 4.1. The most common reason for event logging failures is the event log being filled up beyond its configured storage threshold. However, there may be any number of other reasons for event logging failures.

For centralized logging systems, it should not be considered a failure if communication goes down between the ~~cyber asset~~Cyber Asset and the logging system if the ~~cyber asset~~Cyber Asset can store the logs locally for a period of time until the communication comes back up.

4.5. Reviewing logs every two weeks can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a ~~Data Base~~Database.

- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.

5.~~3~~4. Where possible, any accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

The requirement to change passwords permits the Responsible Entity to determine the periodicity of the password change in their policies and procedures based on a number of factors. The following table suggests appropriate periodicity requirements for passwords based on these factors.

Account Type	Impact Level	Significance of passwords in preventing unauthorized access	Existing Service Agreements	Suggested Periodicity of Password Change
User account password	High	Primary access path	None.	90 days
User account password	Medium	Primary access path	None.	180 days
Shared account	Medium	Local access path.	None.	During regularly

Account Type	Impact Level	Significance of passwords in preventing unauthorized access	Existing Service Agreements	Suggested Periodicity of Password Change
Password for a microprocessor relay, PLC, RTU, etc.		Individuals must authenticate at an upstream device prior to gaining access.		scheduled maintenance
Shared account password for a generation control system	Medium	Local access path. Individuals must authenticate at an upstream device prior to gaining access.	None.	During scheduled plant outages
Administrative account passphrase with 15+ characters	High or Medium	Local access path. Remote user must be authenticated using a different account	None.	~~1~~One year
System account password with 25+ pseudo-random characters	High or Medium	Local access path	None.	~~2~~Two years or more

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes, and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-5

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities described in 4.2.2

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   4.1.7 Reliability Coordinator

   4.1.8 Transmission Operator

   4.1.9 Transmission Owner

   4.2. Facilities:

   4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

   4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:
Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

B. Requirements and Measures

Rationale for R1: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Once the severity of an event or events rises to the level of becoming a Reportable Cyber Security Incident, NERC EOP-004 directs further external reporting actions and timing requirements. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: The requirement to report the incident has been removed and incorporated in the draft EOP-004-2 Standard. Other wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions. These are described below each Requirement Part.

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Processes to identify, classify, and respond to Cyber Security Incidents.	Evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	A process to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident.	Evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents.
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *EOP-004-2 will address the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents.*	

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.*	
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	Evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery, post-incident analysis).
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Conforming change to reference new defined term Cyber Security Incidents.*	

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Internal groups or individuals and external organizations that should receive communication of the Cyber Security Incidents.	Evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that list internal groups or individuals (e.g., other departments, monitoring staff) and external organizations (e.g., law enforcement, ES-ISAC, software vendors, other affected entities) that should receive communication.
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Clarified the term "communication plan" by specifying the elements that need to be included.*	

Rationale for R2: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

R2. Each Responsible Entity shall implement its documented Cyber Security Incident response plan(s) to collectively include each of the applicable items in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable items in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test the BES Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 months between executions of the plan(s): • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise; or • With a full operational exercise.	Evidence may include, but is not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the incident response plan under Requirement R1 when responding to or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan during the response to the incident or exercise.	Evidence may include, but is not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** *Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.*	

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain relevant records related to Reportable Cyber Security Incidents.	Evidence may include, but is not limited to, dated documentation; such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.
Reference to prior version: *CIP-008, R2*		**Change Description and Justification:** *Removed references to the retention period because the Standard addresses data retention in the Compliance Section.*	

Rationale for R3: Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include each of the applicable documented processes that include each of the applicable items in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update and Communication* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Review and update each Cyber Security Incident response plan for accuracy and completeness at least once each calendar year, not to exceed 15 calendar months between reviews.	Evidence may include, but is not limited to, dated documentation of a review of each Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 calendar months between reviews, and an updated Cyber Security Incident response plan if necessary.
Reference to prior version: *CIP-008, R1.5*		**Change Description and Justification:** *Specified what the annual review entails.*	

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Document any lessons learned associated with a Cyber Security Incident test or actual incident response to a Reportable Cyber Security Incident within 30 calendar days after completion of the test or actual incident response.	Evidence may include, but is not limited to, dated documentation of lessons learned, if any, associated with the Cyber Security Incident Response Plan(s) test or actual incident response within 30 calendar days after completion of the test or actual incident response.
Reference to prior version: *CIP-008, R1.5*		**Change Description and Justification:** *Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the Cyber Security Incident response plan based on any documented lessons learned within 30 calendar days after the documentation required by Part 3.2.	Evidence may include, but is not limited to: • Dated, documented lessons learned from the Cyber Security Incident documentation required by Part 3.2 and the dated, revised Cyber Security Incident response plan showing any changes based on that documentation; or • A dated action plan from the documentation required by Part 3.2 showing the resolved action item for Cyber Security Incident response plan updates.

Reference to prior version: *CIP-008, R1.4*	**Change Description and Justification:** *Included additional specification on update of response plan addresses FERC Order No. 706, Paragraph 686, to modify on lessons learned.*		
CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the Cyber Security Incident response plan(s) within 30 calendar days of any of the following changes that the Responsible Entity determines would impact the ability to execute the plan: • Roles or responsibilities; • Cyber Security Incident response groups or individuals; or • Technology changes.	Evidence may include, but is not limited to, dated documentation reflecting changes made to the Cyber Security Incident response plan within 30 calendar days from and in response to the following changes that the Responsible Entity determined would impact the ability to execute the plan: • Roles or responsibilities; • Cyber Security Incident response groups or individuals; or • Technology changes.
Reference to prior version: *CIP-008, R1.4*	**Change Description and Justification:** *Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.*		

3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Distribute updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 30 calendar days of the update being completed.	Evidence of distribution of updates may include, but is not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Specifies activities required to maintain the plan.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but	The Responsible Entity has not developed a Cyber Security Incident response plan to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include processes to identify Reportable Cyber Security Incidents. (1.2)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					the plan does not include internal groups or individuals or external organizations that should receive communication of the Cyber Security Incident. (1.5)	
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity does not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	(2.1) The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. OR The Responsible Entity does not use its Cyber Security Incident response plan during a test or when a Reportable Cyber Security Incident occurs. (2.2) OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not retain relevant records related to Reportable Cyber Security Incidents. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not distributed updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 30 and less than 60 calendar days of the update being completed. (3.4)	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 30 and less than 60 calendar days after the documentation required by 3.1. (3.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) within 30 and less than 60 calendar days of any of the following changes that the responsible entity	The Responsible Entity has not documented any lessons learned within 30 and less than 60 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 60 calendar days after the documentation required by 3.1. (3.2) OR	The Responsible Entity has not documented any lessons learned within 60 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				determines would impact the ability to execute the plan: (3.3) • roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • technology changes. OR The Responsible Entity has not distributed updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 60 calendar days of the update being completed. (3.4)	The Responsible Entity has not updated the Cyber Security Incident response plan(s) within 60 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.3) • roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The following guidelines are available to assist in addressing the required components of an incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents are found in EOP-004-2. This standard only requires the entity to identify such incidents. However, an entity may include identification and reporting procedures in the same plan to comply with both standards.

Requirement R2:

Requirement R2 ensures entities periodically test the incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. TTXs can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.2 and (2) organizational or technology changes from Part 3.4.

The documentation of lessons learned from Part 3.2 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a BES Reportable Cyber Security Incident without any documented lessons learned.

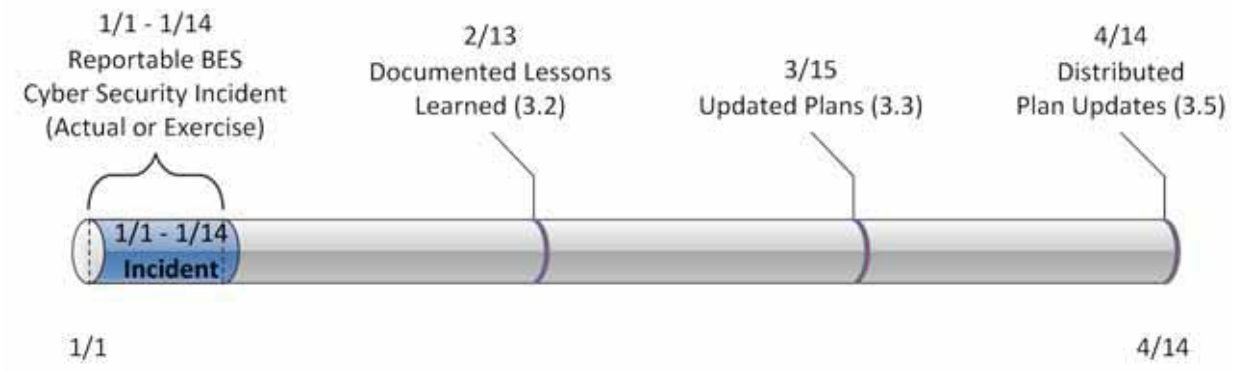

Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

Part 3.3 requires an entity to update the plan within 30 days of the documented lessons learned. This recognizes the time it may take to propose solutions to the lessons learned and complete the review and approval process.

Part 3.5 requires an entity to distribute the plan within 30 calendar days of the plan update. The measure specifies this can be accomplished through email, USPS, electronic distribution system (e.g., workflow software), or training records.

The plan change requirement in Part 3.4 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or

contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

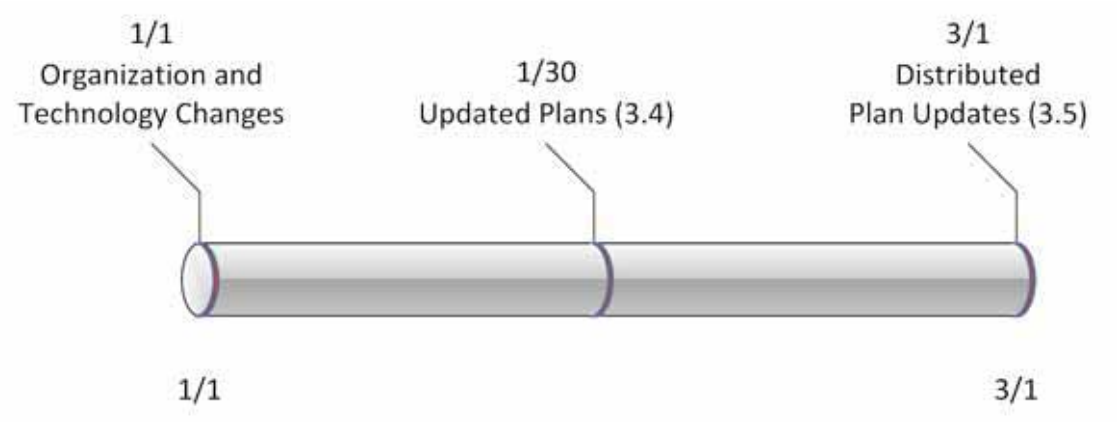

Figure 2: Timeline for Plan Changes in 3.4

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008~~)~~).
2. SC authorized moving the SAR forward to standard development (July 10, 2008~~)~~).
3. ~~CSO706 SDT appointed (August 7, 2008)~~
4. ~~Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)~~
5. ~~Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)~~
6. ~~Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)~~
7. ~~Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)~~
8. ~~8.~~3. ~~Version 5 of CIP-002 to CIP-011 posted~~First posting for 60-day formal comment period and concurrent ballot (~~mm-dd-yy)~~November 2011).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (~~A first posting of Version 5~~)~~ was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes, and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012

BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]

~~1.~~2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center~~".~~."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a ~~responsible entity.~~Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-5

3. **Purpose:** ~~Standard CIP-008-5 requires~~To mitigate the ~~identification, classification, response, and reporting~~risk to the reliable operation of the BES as the result of a Cyber Security ~~Incidents related to BES Cyber Assets and BES Cyber Systems.~~ Incident by specifying incident response requirements.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities described in 4.2.2

   ~~4.1.2~~4.1.3 Generator Operator

   ~~4.1.3~~4.1.4 Generator Owner

   ~~4.1.4~~4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   ~~4.1.5~~4.1.7 Reliability Coordinator

   ~~4.1.6~~4.1.8 Transmission Operator

   ~~4.1.7~~4.1.9 Transmission Owner

   4.2. Facilities:

   4.2.1 ~~that are part of any of the following systems~~**Load Serving Entity:** One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

   ~~4.2.1~~4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - ~~A UFLS program required by a NERC or Regional Reliability Standard~~
   - ~~A UVLS~~UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs

automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme ~~required by a NERC or Regional Reliability Standard~~
- ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~

~~4.2.2~~4.2.3 where the~~Generator Operator~~

~~4.2.3~~4.2.4 ~~Generator Owner~~

~~4.2.4~~4.2.5 ~~Interchange Coordinator~~

~~4.2.5 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~4.2.6 NERC~~

~~4.2.7 Regional Entity~~

~~4.2.8~~4.2.6 ~~Reliability Coordinator~~

~~4.2.9~~4.2.7 ~~Transmission Operator~~

~~4.2.10~~4.2.8 ~~Transmission Owner~~

4.3. ~~Facilities:~~

~~4.3.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~4.3.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~
- ~~A~~ Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A ~~Transmission~~ Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard

- ~~Its Transmission Operator's restoration plan~~
- ~~**All other**~~ Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~**4.3.3**~~**4.3.1** **Responsible Entities**~~:~~ **listed in 4.1 other than Distribution Providers and Load-Serving Entities**: All BES Facilities.

~~**4.3.4**~~**4.3.2** **Exemptions:** The following are exempt from Standard CIP-~~008~~002-5:

~~**4.3.4.1**~~**4.3.2.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~**4.3.4.2**~~**4.3.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~**4.3.4.3**~~ In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~**4.3.4.4**~~**4.3.2.3** ~~Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.~~

5. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter ~~as applicable~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of ~~specific elements required~~applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e~~.~~., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards. Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~
- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and categorization processes. ~~Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.

- ~~**Medium Impact BES Cyber Systems at Control Centers –** Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity –** Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.~~
- ~~**Associated Electronic Access Control or Monitoring Systems –** Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems~~
- ~~**Associated Physical Access Control Systems –** Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.~~
- ~~**Associated Protected Cyber Assets –** Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.~~
- ~~**Plans associated with High Impact BES Cyber Systems or Medium Impact BES Cyber Systems -a**pplies to any plan associated with a corresponding High or Medium Impact BES Cyber Systems.~~
- ~~**Electronic Access Points –** Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.~~
- ~~**Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~
- ~~**Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

~~**Rationale for R1:** So that consistent responses to BES Cyber Security Incidents involving BES Cyber Assets and BES Cyber Systems occur. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanne incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigatin the weaknesses that were exploited, and restoring computing services. Once the number and severity of events rises to the level of becoming a reportable incident NERC EOP-4 directs further external reporting actions and timing requirements. Whe a requirement applies to All Responsible Entities, the drafting team proposes that an enterprise or single incident response plan for all BES Cyber Systems may be submitted. An organization may have a common plan for multiple registered entities i owns.~~

~~**Summary of Changes:** (FERC directives, most significant items, summary of smaller items)~~

B. Requirements and Measures

Rationale for R1: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Once the severity of an event or events rises to the level of becoming a Reportable Cyber Security Incident, NERC EOP-004 directs further external reporting actions and timing requirements. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: The requirement to report the incident has been removed and incorporated in the draft EOP-004-2 Standard. Other wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions. These are described below each Requirement Part.

R1. Each Responsible Entity shall ~~have~~document one or more ~~BES~~ Cyber Security Incident response plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – ~~BES~~ Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning~~]~~].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – ~~BES~~ Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – ~~BES~~ Cyber Security Incident Response Plan Specifications			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Processes to identify, classify, and respond to ~~BES~~ Cyber Security Incidents.	Evidence may include, but is not limited to, dated ~~copies~~documentation of ~~BES~~ Cyber Security Incident response plan(s) that include ~~how~~the process to identify, classify, and respond to ~~BES~~ Cyber Security Incidents ~~targeting the Electronic Security Perimeter or Defined Physical Boundary of a BES Cyber System and covers incidents that impact the reliability of BES~~.
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *~~Minor wording changes; essentially unchanged~~"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.*	
1.2	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	A process to determine if an identified ~~BES~~ Cyber Security Incident is a Reportable ~~BES~~ Cyber Security Incident.	Evidence may include, but is not limited to, dated documentation of ~~process(es~~Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which ~~BES~~ Cyber Security Incidents are also Reportable ~~BES~~ Cyber Security Incidents.

CIP-008-5 Table R1 – ~~BES~~ Cyber Security Incident Response Plan Specifications			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *~~Minor wording changes; essentially unchanged~~EOP-004-2 will address the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents.*	
1.3	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	~~Define:~~ ~~1.3.1.~~ The roles and responsibilities of ~~BES~~ Cyber Security Incident response ~~personnel;~~ ~~1.3.2. The BES Cyber Security Incident handling procedures;~~ ~~1.3.3. Internal staff and external organizations that should receive communication of the incident~~groups or individuals.	Evidence may include, but is not limited to, dated ~~BES~~ Cyber Security Incident response process(es) or procedure(s) that ~~addresses~~define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of ~~BES~~ Cyber Security Incident response ~~personnel, BES Cyber Security Incident handling processes~~groups or ~~procedures, and communication processes or procedures~~individuals.
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *~~Minor wording changes; essentially unchanged~~Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.*	
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	Evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery, post-incident analysis).

CIP-008-5 Table R1 – ~~BES~~ Cyber Security Incident Response Plan Specifications			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Conforming change to reference new defined term Cyber Security Incidents.*	
1.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Internal groups or individuals and external organizations that should receive communication of the Cyber Security Incidents.	Evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that list internal groups or individuals (e.g., other departments, monitoring staff) and external organizations (e.g., law enforcement, ES-ISAC, software vendors, other affected entities) that should receive communication.
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Clarified the term "communication plan" by specifying the elements that need to be included.*	

~~**Rationale for R2:** Added testing requirements to verify the REs response plan's effectiveness and consistent application in responding to a BES Cyber Security Incident(s) impacting a BES Cyber System.~~

Rationale for R2: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

R2. Each Responsible Entity shall implement its documented ~~BES~~ Cyber Security Incident response plan(s) to collectively include each of the applicable items in *CIP-008-5 Table R2 – ~~BES~~ Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations~~]~~].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable items in *CIP-008-5 Table R2 – ~~BES~~ Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – ~~BES~~ Cyber Security Incident Response Plan Implementation and Testing			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	~~When a~~Test the BES Cyber Security Incident ~~occurs, the incident~~ response ~~plans must be used when incidents occur and include recording~~plan(s) at least once every calendar year, not to exceed 15 months between executions of ~~deviations taken from~~ the plan ~~during the incident~~(s): • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or ~~test~~tabletop exercise; or • With a full operational exercise.	Evidence may include, but is not limited to, ~~incident reports~~dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and ~~notes that were kept during the incident response process, and documentation that lists and justifies deviations taken~~communication resulting from the ~~plan during the incident.~~ test. Types of exercises may include discussion or operations based exercises.
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.* ~~*Allows deviation from plan during actual events or testing if deviations are recorded for review.*~~	

CIP-008-5 Table R2 – ~~BES~~ Cyber Security Incident Response Plan Implementation and Testing			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	~~Implement~~Use the ~~BES Cyber Security Incident~~incident response plan~~(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s):~~ • ~~by~~ under Requirement R1 when responding to or performing an ~~actual incident, or~~ • ~~with a paper drill or table top~~ exercise~~, or~~ • ~~with a full operational~~ of a Reportable Cyber Security Incident. Document deviations from the plan during the response to the incident or exercise.	Evidence may include, but is not limited to, ~~dated evidence of implementing~~incident reports, logs, and notes that were kept during the ~~BES Cyber Security Incident~~incident response ~~plan(s) initially upon~~ process, and follow-up documentation that describes deviations taken from the ~~effective date of~~plan during the ~~standard and at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident,~~incident or ~~with a paper drill or table top~~ exercise~~, or with a full operational exercise.~~ .
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** ~~*Minor wording changes; essentially unchanged*~~ *Allows deviation from plan(s) during actual events or testing if deviations are recorded for review*.	

CIP-008-5 Table R2 – ~~BES~~ Cyber Security Incident Response Plan Implementation and Testing			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.3	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain relevant ~~documentation~~records related to Reportable ~~BES~~ Cyber Security Incidents ~~for three calendar years.~~.	Evidence may include, but is not limited to, dated documentation; such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable ~~BES~~ Cyber Security Incidents.
Reference to prior version: *CIP-008, R2*		**Change Description and Justification:** *~~Minor wording changes; essentially unchanged~~Removed references to the retention period because the Standard addresses data retention in the Compliance Section.*	

~~**Rationale for R3:** Conduct sufficient reviews, updates and communications to verify the REs response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.~~

~~**Summary of Changes:** Addressed BES Cyber Security Incident response plan review, update, and communication specifications to ensure that BES Cyber Security Incident response plans remain updated and individuals are aware of the updates.~~

Rationale for R3: Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-008-5 Table R3 – ~~BES~~ Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment~~and Real-Time Operations]~~].*

M3. Evidence must include each of the applicable documented processes that include each of the applicable items in *CIP-008-5 Table R3 – ~~BES~~ Cyber Security Incident Response Plan Review, Update and Communication* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-008-5 Table R3 – ~~BES~~ Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	~~All Responsible Entities~~High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Review and update each ~~BES~~ Cyber Security Incident response plan for accuracy and completeness ~~initially upon the effective date of the standard and~~ at least once each calendar year ~~thereafter~~, not to exceed 15 calendar months between reviews~~, and update if necessary~~.	Evidence may include, but is not limited to, dated documentation of a review of each ~~BES~~ Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 calendar months between reviews, and an updated ~~BES~~ Cyber Security Incident response plan if necessary.
Reference to prior version: *CIP-008, R1.5*		**Change Description and Justification:** *~~Minor wording changes; essentially unchanged~~Specified what the annual review entails*.	

CIP-008-5 Table R3 – ~~BES~~ Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	~~Review the results of BES~~Document any lessons learned associated with a Cyber Security Incident ~~Response Plan(s)~~ test or actual incident response to a Reportable Cyber Security Incident within ~~thirty~~30 calendar days ~~of the execution, documenting any lessons learned associated with the~~after completion of the test or actual incident response ~~plan~~.	Evidence may include, but is not limited to, dated documentation of ~~a review of the BES~~ lessons learned, if any, associated with the Cyber Security Incident Response Plan(s) test or actual incident response within ~~thirty~~30 calendar days after completion of the ~~execution, including dated documentation of any lessons learned associated with the~~ test or actual incident response ~~plan~~.
Reference to prior version: *CIP-008, R1.5*		**Change Description and Justification:** *Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.*	

3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the Cyber Security Incident response plan based on any documented lessons learned within 30 calendar days after the documentation required by Part 3.2.	Evidence may include, but is not limited to: • Dated, documented lessons learned from the Cyber Security Incident documentation required by Part 3.2 and the dated, revised Cyber Security Incident response plan showing any changes based on that documentation; or • A dated action plan from the documentation required by Part 3.2 showing the resolved action item for Cyber Security Incident response plan updates.
Reference to prior version: *CIP-008, R1.~~5~~4*		**Change Description and Justification:** *Included ~~requirement for review after testing or actual~~ additional specification on update of* response *~~based on review of DHS controls~~plan addresses FERC Order No. 706, Paragraph 686, to modify on lessons learned.*	

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**

3.~~3~~4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the ~~BES~~ Cyber Security Incident response plan ~~based on any documented lessons learned~~(s) within ~~sixty~~30 calendar days of ~~the completion~~ any of the ~~review of~~following changes that the Responsible Entity determines would impact the ability to execute the plan: • Roles or responsibilities; • Cyber Security Incident response groups or individuals; or • Technology changes.	Evidence may include, but is not limited to, dated~~, documented lessons learned from~~ documentation reflecting changes made to the ~~results of the BES~~ Cyber Security Incident response plan within 30 calendar days from and in response to the following changes that the ~~dated, revised~~Responsible Entity determined would impact the ability to execute the plan: • Roles or responsibilities; • Cyber Security Incident response groups or individuals; or • Technology changes.
Reference to prior version: *CIP-008, R1.4*		**Change Description and Justification:** ~~*Included additional specification on*~~*Specifies the activities required to maintain the plan. The previous version required entities to update ~~of~~the plan in response ~~plan. Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls~~to any changes. The modifications make clear the changes that would require an update.*	
3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Distribute updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 30 calendar days of the update being completed.	Evidence of distribution of updates may include, but is not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Specifies activities required to maintain the plan.*	

~~CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication~~			
~~Part~~	~~Part~~	~~Part~~	~~Part~~
~~3.4~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems~~	~~Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.~~	~~Acceptable evidence may include, but is not limited to, updated documentation reflecting changes made to the BES Cyber Security Incident response plan in response to organizational or technology changes.~~
~~**Reference to prior version:**~~ ~~*CIP-008 R1.4*~~		~~**Change Description and Justification:** *Included additional specification on update of response plan. Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls*~~	
~~3.5~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems~~	~~Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.~~	~~Evidence of communication of updates may include, but is not limited to:~~ ~~• Emails~~ ~~• USPS or other mail service~~ ~~• Electronic distribution system~~ ~~• Training sign-in sheets.~~
~~**Reference to prior version:**~~ ~~*New Requirement*~~		~~**Change Description and Justification:** *Added specific timing requirement on communication of plan changes based on review of the DHS Controls*~~	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity
- If the Responsible Entity works for shall serve as the Compliance Enforcement Authority ("CEA") unless the Regional Entity, then the applicable entity is owned, operated, or controlled by the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity,. In such cases the ERO or a Regional Entityentity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERCauthority shall serve as the Compliance Enforcement AuthorityCEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaintcompliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliantmitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed ~~a BES~~the Cyber Security Incident response plan~~,~~(s), but the plan does not ~~define~~include the roles and responsibilities of Cyber Security Incident response ~~personnel,~~groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not ~~define~~include incident handling procedures~~,~~ ~~or~~ for Cyber Security Incidents. (1.4) OR The Responsible Entity has developed the	The Responsible Entity has not developed a ~~BES~~ Cyber Security Incident response plan to identify, classify, and respond to ~~BES~~ Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a ~~BES~~ Cyber Security Incident response plan, but the plan does not include processes to identify Reportable ~~BES~~ Cyber Security Incidents. (1.2)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Cyber Security Incident response plan(s), but the plan does not ~~communicate the incident to appropriate~~include internal groups or individuals or external organizations~~.~~ that should receive communication of the Cyber Security Incident. (1.5)	
R2	**Operations Planning** **Real-time Operations**	**Lower**	~~N/A~~The Responsible Entity has not tested the Cyber Security Incident response plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	~~N/A~~The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	~~N/A~~The Responsible Entity has not tested the Cyber Security Incident response plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity does not document	(2.1) The Responsible Entity ~~does~~has not ~~use its BES~~tested the Cyber Security Incident response plan ~~when an incident occurs.~~ (s) within 19 calendar months between tests of the plan. OR The Responsible Entity ~~has~~does not ~~tested the execution of~~use its ~~BES~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	Cyber Security Incident response plan once each calendar year,during a test or when a Reportable Cyber Security Incident occurs. (2.2) OR The Responsible Entity does not retain relevant records related to exceed 15 calendar months between executions of the plan.Reportable Cyber Security Incidents. (2.3)
R3	**Operations Assessment** **Real-time Operations**	**Lower**	N/AThe Responsible Entity has not distributed updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident	N/AThe Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 30 and less than 60 calendar days after the	The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on documented any lessons learned within 30 and less than 60	The Responsible Entity has not reviewed the results of each of its BES Cyber Security Incident response plan(s),documented any lessons learned within 60 calendar days of a test or actual

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			response plan within 30 and less than 60 calendar days of the update being completed. (3.4)	documentation required by 3.1. (3.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) within 30 and less than 60 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.3) • roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • technology changes. OR	calendar days of ~~execution.~~a test or actual incident response to a Reportable Cyber Security Incident. (3.1) OR The Responsible Entity has ~~reviewed but~~ not updated ~~each of its BES~~the Cyber Security Incident response ~~plans~~plan based on any documented lessons learned within ~~30~~60 calendar days ~~of any system, organizational, or~~ after the documentation required by 3.1. (3.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) within 60 calendar	incident response~~, within 30 calendar days of execution.~~ ~~OR~~ ~~The Responsible Entity has reviewed and updated each of its BES Cyber Security Incident response plans but has not communicated all updates~~ to ~~all responsible personnel.~~a Reportable Cyber Security Incident. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not distributed updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 60 calendar days of the update being completed. (3.4)	days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.3) • roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • technology ~~change that impacts one of the response plans~~changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

~~FAQ, SP99, ISA, US-CERT, NIST Guidelines, etc. as a source of materials~~

Requirement R1:

~~A Reportable BES~~The following guidelines are available to assist in addressing the required components of an incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems* *Cyber Security Incident* *Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a ~~BES~~ Cyber Security Incident that ~~results~~has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: ~~necessary~~ Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents are found in EOP-004-2. This standard only requires the entity to identify such incidents. However, an entity may include identification and reporting procedures in the same plan to comply with both standards.

Requirement R2:

Requirement R2 ensures entities periodically test the incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. TTXs can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency

operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.2 and (2) organizational or technology changes from Part 3.4.

The documentation of lessons learned from Part 3.2 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a BES Reportable Cyber Security Incident without any documented lessons learned.

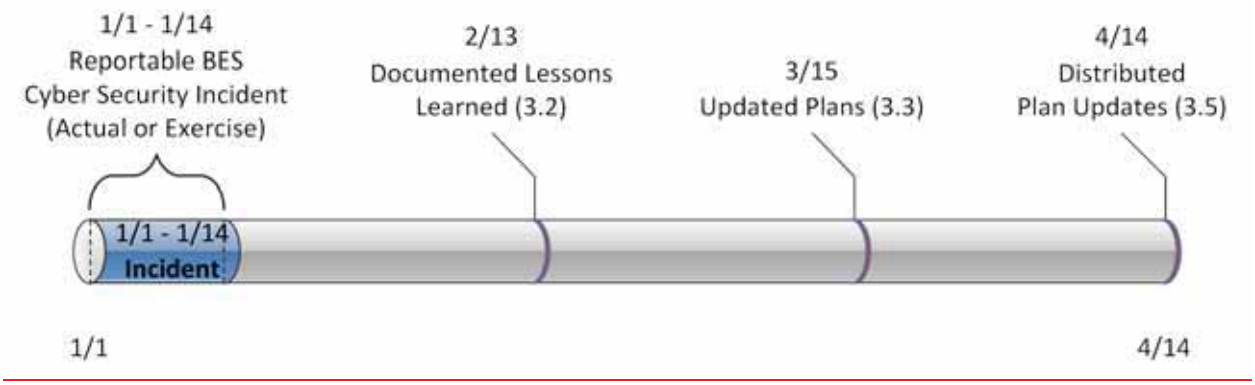

Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

Part 3.3 requires an entity to update the plan within 30 days of the documented lessons learned. This recognizes the time it may take to propose solutions to the lessons learned and complete the review and approval process.

Part 3.5 requires an entity to distribute the plan within 30 calendar days of the plan update. The measure specifies this can be accomplished through email, USPS, electronic distribution system (e.g., workflow software), or training records.

The plan change requirement in Part 3.4 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

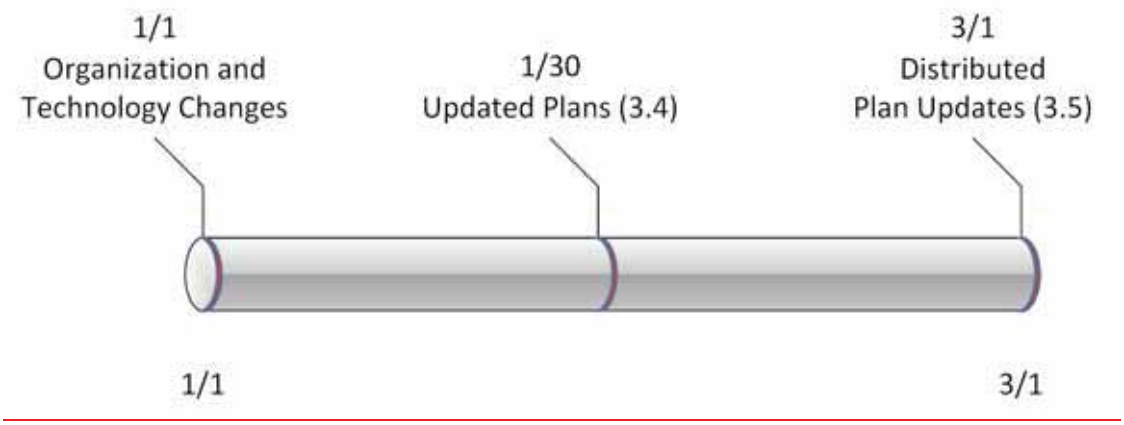

Figure 2: Timeline for Plan Changes in 3.4

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this Implementation Plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their Implementation Plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the Implementation Plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-5

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

4.1.7 Reliability Coordinator

4.1.8 Transmission Operator

4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:
Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.

B. Requirements and Measures

Rationale for R1: Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber Assets and BES Cyber Systems occurs.

Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Conditions for activation of the recovery plan(s).	Evidence may include, but is not limited to, one or more plans that include language identifying specific conditions for activation of the recovery plan(s).
Reference to prior version: *CIP-009, R1.1*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Roles and responsibilities of responders.	Evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
Reference to prior version: *CIP-009, R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, of information required to successfully recover BES Cyber System functionality.
Reference to prior version: *CIP-009, R4*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	Evidence may include, but is not limited to, dated evidence or logs confirming that the backup process completed successfully.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Addresses FERC Order Section 739 and 748.*	
1.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Processes to preserve data, except for CIP Exceptional Circumstances, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s).	Evidence may include, but is not limited to, procedures to preserve data; such as preserving a corrupted drive, making a data mirror of the system before proceeding with recovery, or taking the important assessment steps necessary to avoid reintroducing the precipitating or corrupted data.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added requirement to address FERC Order No. 706, Paragraph 706.*	

Rationale for R2: To verify the Responsible Entities Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

NIST SP 800-84 identifies the following types of exercises widely used in information system programs by single organizations:

Tabletop Exercises. Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an Emergency and their responses to a particular Emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.

Functional Exercises. Functional exercises allow personnel to validate their operational readiness for Emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, Emergency notifications, System equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual Emergency situation, but in a simulated manner.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Test the recovery plan(s) referenced in Requirement R1 at least once each calendar year, not to exceed 15 calendar months between tests of the plan: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Minor wording change; essentially unchanged.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Test information used in the recovery of BES Cyber Systems that is stored on backup media at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and is compatible with current system configurations.	Evidence may include, but is not limited to, dated evidence of a test of information used in the recovery of BES Cyber Systems that is stored on backup media when initially stored and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and is compatible with current system configurations.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-009, R5*		**Change Description and Justification:** *Combined Requirement from CIP-009 R5 included requirement to test when initially stored. Addresses FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups.*	
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Evidence may include, but is not limited to Dated evidence of: • An operational exercise prior to the effective date of the standard and at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual incident response which occurred within the 36 calendar month timeframe that exercised the recovery plans.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.*	

Rationale for R3: To enable the continued effectiveness of the Responsible Entities response plan's for planned and consistent restoration of BES Cyber System(s).

Summary of Changes: Addressed recovery plan review, update, and communication specifications to ensure that recovery plans remain updated and individuals are aware of the updates.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Document any identified deficiencies or lessons learned associated with each recovery plan test or actual incident recovery within 30 calendar days after completion of the test or recovery.	Evidence may include, but is not limited to, dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery within 30 calendar days after completion of the test or recovery.
Reference to prior version: *CIP-009, R1 and R3*		**Change Description and Justification:** *Added the time frame for update.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update the recovery plan(s) based on any documented deficiencies or lessons learned within 30 calendar days after the documentation required by Part 3.1.	Evidence may include, but is not limited to, dated, documented deficiencies or lessons learned required by Part 3.1 and the dated, revised recovery plan(s) based on that documentation.
Reference to prior version: *CIP-009, R3*		**Change Description and Justification:** *Added the timeframe for update.*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update recovery plan(s) within 30 calendar days of any of the following changes that the Responsible Entity determines would impact the plan or the ability to execute the plan: • Roles or responsibilities; or • Technology changes.	Evidence may include, but is not limited to, dated documentation reflecting changes made to the recovery plan(s) in response to the following changes that the responsible entity determined would impact the plan or the ability to execute the plan: • Roles or responsibilities; or • Technology changes.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery plans stay updated.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Distribute recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within 30 calendar days of the update being completed.	Evidence of distribution of updates may include, but is not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery personnel are aware of any changes to recovery plans.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address all of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.
R2	**Operations Planning** **Real-time**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months,	The Responsible Entity has not tested the recovery plan(s) according to R2 Part	The Responsible Entity has not tested the recovery plan(s) according to R2 Part

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations		2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	not exceeding 17 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (2.3)	2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 19 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not distributed updates of the recovery plan to each person or group with a defined role in the recovery plan(s) within 30 and less than 60 calendar days of the update being completed. (3.4)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 30 and less than 60 calendar days after the documentation required by R3 Part 3.1. (3.1) OR The Responsible Entity has not updated the Recovery plan(s)(s) within 30 and less than 60 calendar days of any of the changes listed in R3 Part 3.3 that the responsible entity determines would impact the ability to execute the plan (3.3)	The Responsible Entity has not documented any lessons learned within 30 and less than 60 calendar days of each recovery plan test or actual incident recovery. (3.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 60 calendar days after the documentation required by R3 Part 3.2. (3.2) OR The Responsible Entity has not updated the recovery plan(s)(s) within 60 calendar	The Responsible Entity has not documented any lessons learned within 60 calendar days of each recovery plan test or actual incident recovery. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity has not distributed updates of the recovery plan(s) to each person or group with a defined role in the recovery plan(s) within 60 calendar days of the update being completed. (3.4)	days of any of the changes listed in R3 Part 3.3 that the responsible entity determines would impact the ability to execute the plan. (3.3)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

(SEE FAQs AND CIPC GUIDELINES AS A BASIS.)

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. ~~CSO706 SDT appointed (August 7, 2008)~~
4. ~~Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)~~
5. ~~Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)~~
6. ~~Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)~~
7. ~~Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)~~
8. ~~3.~~ ~~Version 5 of CIP-002 to CIP-011 posted~~First posting for 60-day formal comment period and concurrent ballot (~~mm-dd-yy)~~November 2011).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012

BOT adoption	June 2012

Effective Dates

1. **~~18~~24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this ~~implementation plan~~Implementation Plan.[1]

~~1.~~2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their ~~implementation plan~~Implementation Plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the ~~implementation plan~~Implementation Plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a ~~responsible entity.~~Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification-.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber ~~Assets and~~ Systems

2. Number: CIP-009-5

~~**3. Purpose:** Standard CIP-009-5 ensures that recovery plan(s) related to the storing of backup information are put in place for BES Cyber Assets and BES Cyber Systems and that these plans support and follow established business continuity and disaster recovery techniques and practices.~~

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

~~4.1.2~~4.1.3 Generator Operator

~~4.1.3~~4.1.4 Generator Owner

~~4.1.4~~4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

~~4.1.5~~4.1.7 Reliability Coordinator

~~4.1.6~~4.1.8 Transmission Operator

~~4.1.7~~4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 ~~that are part of any of the following systems~~**Load Serving Entity:** One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

~~4.2.1~~4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLSUVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.24.2.3 where theGenerator Operator

4.2.34.2.4 Generator Owner

4.2.44.2.5 Interchange Coordinator

4.2.5 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.6 NERC

4.2.7 Regional Entity

4.2.84.2.6 Reliability Coordinator

4.2.94.2.7 Transmission Operator

4.2.104.2.8 Transmission Owner

4.3. Facilities:

4.3.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.3.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard

- A ~~Transmission~~ Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard

- ~~Its Transmission Operator's restoration plan~~
- ~~**All other**~~ Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~**4.3.3**~~**4.3.1 Responsible Entities~~:~~ listed in 4.1 other than Distribution Providers and Load-Serving Entities**: All BES Facilities.

~~**4.3.4**~~**4.3.2 Exemptions:** The following are exempt from Standard CIP-~~009~~002-5:

~~**4.3.4.1**~~**4.3.2.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~**4.3.4.2**~~**4.3.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~**4.3.4.3**~~**4.3.2.3** In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~**4.3.4.4** Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.~~

5. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter~~ as applicable~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of ~~specific elements required~~applicable items in the documented processes. A numbered list in the measure means the evidence

example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e~~.~~., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards. Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and categorization processes. ~~Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems.~~

~~For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.~~
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding ~~High or Medium Impact BES Cyber Systems.~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- ~~**Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.~~
- ~~**Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.~~
- ~~**Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~
- ~~**Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These~~

~~hardware and devices are excluded in the definition of Physical Access Control Systems.~~

B. Requirements and Measures

~~**Rationale for R1:** Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is therefore necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber Assets and BES Cyber Systems occurs.~~

~~**Summary of Changes:**~~

~~Added provisions to protect data that would be useful in the investigation of an event that results in the need for a cyber system recovery plan to be utilized.~~

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning~~]~~].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Conditions for activation of the recovery plan(s).	Evidence may include, but ~~-~~is ~~-~~not limited to, one or more plans that include language identifying specific conditions for activation of the recovery plan(s).
Reference to prior version: *CIP-009, R1.1*		**Change Description and Justification:** *~~Reworded to address FERC Order 706 P694 and simplify the~~Minor wording~~.~~ changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Roles and responsibilities of responders~~, including identification of the individuals, either by name or by title, responsible for recovery efforts~~.	Evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders~~, including identification of the individuals responsible for recovery efforts.~~.
Reference to prior version: *CIP-009, R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	One or more processes for the backup~~,~~ and storage~~, and protection~~ of information required to ~~restore~~recover BES Cyber System functionality.	Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, ~~and protection~~ of information required to successfully ~~restore a~~recover BES Cyber System functionality.
Reference to prior version: *CIP-009, R4*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**~~Part~~Applicable BES Cyber Systems and associated Cyber Assets**	**~~Part~~Requirements**	**~~Part~~Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.	Evidence may include, but is not limited to, dated evidence ~~of the verification~~or logs confirming that the backup process completed successfully.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Addresses FERC Order Section 739 and 748.*	
1.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~Preserve data, where technically feasible~~Processes to preserve data, except for CIP Exceptional Circumstances, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s~~) as required in Requirement R1.~~).	Evidence may include, but is not limited to, procedures to preserve data~~,~~; such as preserving a corrupted drive, making a data mirror of the system before proceeding with recovery, or taking the important assessment steps necessary to avoid reintroducing the precipitating or corrupted data.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added requirement to address FERC Order No. 706, ~~paragraph~~Paragraph 706.*	

Rationale for R2: To verify the Responsible Entities Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

NIST SP 800-84 identifies the following types of exercises widely used in information system programs by single organizations:

Tabletop Exercises. Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an ~~emergency~~Emergency and their responses to a particular ~~emergency~~Emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.

Functional Exercises. Functional exercises allow personnel to validate their operational readiness for ~~emergencies~~Emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, ~~emergency~~Emergency notifications, ~~system~~System equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements.~~28~~ Functional exercises allow staff to execute their roles and responsibilities as they would in an actual ~~emergency~~Emergency situation, but in a simulated manner.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing*. *[Violation Risk Factor: Lower] [Time Horizon: ~~Long Term~~Operations Planning~~]~~ and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~Implement~~Test the recovery plan(s) referenced in Requirement R1 ~~initially upon the effective date of the standard and~~ at least once each calendar year~~ thereafter~~, not to exceed 15 calendar months between ~~executions~~tests of the plan: • ~~by~~By recovering from an actual incident~~, or~~; • ~~with~~With a paper drill or tabletop exercise~~,~~; or • ~~with a full~~With an operational exercise.	Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with ~~a full~~an operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Minor wording change; essentially unchanged.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Test ~~any~~ information used in the recovery of BES Cyber ~~systems~~Systems that is stored on backup media ~~initially and~~ at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and ~~reflects~~is compatible with current system configurations.	Evidence may include, but is not limited to, dated evidence of a test of ~~any~~ information used in the recovery of BES Cyber ~~systems~~Systems that is stored on backup media when initially stored and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and ~~reflects~~is compatible with current system configurations.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets	**Requirements**	**Measures**
Reference to prior version: *CIP-009, R5*		**Change Description and Justification:** *Combined Requirement from CIP-009 R5 included requirement to test when initially stored. Addresses FERC ~~Requirements (~~Order No. 706, Paragraphs 739~~,~~ and 748~~)~~ related to testing of backups.*	
2.3	High Impact BES Cyber Systems ~~Medium Impact BES Cyber Systems at Control Centers.~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	Test each of the recovery plans referenced in Requirement R1~~, initially upon the effective date of the standard, and~~ at least once every ~~39~~36 calendar months ~~thereafter~~ through an operational exercise of the recovery plans in ~~a~~ an environment representative ~~environment that reflects~~of the production environment. An actual recovery response may substitute for an operational exercise.	Evidence may include, but is not limited to~~:~~ Dated evidence of ~~an~~: • An operational exercise ~~initially upon~~prior to the effective date of the standard and at least once every ~~39~~36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual incident response which occurred within the ~~39~~36 calendar month timeframe that ~~implemented~~exercised the recovery plans.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Addresses FERC ~~Requirement (~~Order No. 706, Paragraph 725~~)~~ to add the requirement that the recovery plan test be a full operational test once every 3 years.*	

Rationale for R3: To enable the continued effectiveness of the Responsible Entities response plan's for planned and consistent restoration of BES Cyber System(s).

Summary of Changes:

Addressed recovery plan review, update, and communication specifications to ensure that recovery plans remain updated and individuals are aware of the updates.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication. [Violation Risk Factor: Lower] [Time Horizon: ~~Long Term Planning]~~Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document~~Document any identified deficiencies or lessons learned~~.~~ associated with each recovery plan test or actual incident recovery within 30 calendar days after completion of the test or recovery.	Evidence may include, but is not limited to, dated ~~evidence of a review of the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, including~~ documentation of ~~any~~ identified deficiencies or lessons learned for each recovery plan test or actual incident recovery within 30 calendar days after completion of the test or recovery.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-009, R1 and R3*		**Change Description and Justification:** *Added the time frame for update.*	
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	Update the recovery plan(s) based on any documented deficiencies or lessons learned within 30 calendar days after the documentation required by Part 3.1.	Evidence may include, but is not limited to, dated, documented deficiencies or lessons learned required by Part 3.1 and the dated, revised recovery plan(s) based on that documentation.
Reference to prior version: *CIP-009, R3*		**Change Description and Justification:** *Added the timeframe for update.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	**~~Reference to prior version:~~** ~~*CIP-009-R1*~~Update recovery plan(s) within 30 calendar days of any of the following changes that the Responsible Entity determines would impact the plan or the ability to execute the plan: • Roles or responsibilities; or • Technology changes.	**~~Change Description and Justification:~~** ~~*Added the requirements to additionally review plans after system replacement. Also added requirement for documentation of any identified deficiencies or lessons learned.*~~ Evidence may include, but is not limited to, dated documentation reflecting changes made to the recovery plan(s) in response to the following changes that the responsible entity determined would impact the plan or the ability to execute the plan: • Roles or responsibilities; or • Technology changes.

~~CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication~~			
~~Part~~	~~Applicability~~	~~Requirements~~	~~Measures~~
~~3.2~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems at Control Centers.~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned.~~	~~Evidence may include, but is not limited to, dated evidence of a review of the results of each recovery plan test or actual incident recovery within thirty calendar days of the of the completion of the exercise, documenting any identified deficiencies or lessons learned.~~
~~**Reference to prior version:**~~ ~~*CIP-009 R3*~~		~~**Change Description and Justification:** *Added the timeframe for update.*~~	
~~3.3~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems at Control Centers.~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2.~~	~~Evidence may include, but is not limited to, dated documentation of updates to the recovery plan(s).~~
~~**Reference to prior version:**~~ ~~*CIP-009 R3*~~		~~**Change Description and Justification:** *Added the timeframe for update.*~~	

~~CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication~~			
~~Part~~	~~Part~~	~~Part~~	~~Part~~
~~3.4~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems at Control Centers.~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change.~~	~~Evidence may include, but is not limited to, dated documentation of organizational or technology changes, and dated documentation updates to the recovery plan(s).~~

Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery plans stay updated.*	
3.~~5~~4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	~~Communicate all~~Distribute recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within ~~thirty~~30 calendar days of the update being completed.	Evidence of ~~communication~~ distribution of updates may include, but is not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Ensures that recovery personnel are aware of any changes to recovery plans.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity~~; or~~
- ~~If the Responsible Entity works for~~ shall serve as the Compliance Enforcement Authority ("CEA") unless the ~~Regional Entity, then the~~ applicable entity is owned, operated, or controlled by the Regional Entity ~~will establish an agreement with~~. In such cases the ERO or ~~another~~a Regional entity approved by ~~the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.~~
- ~~If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and~~ FERC or other applicable governmental ~~authorities shall serve as the Compliance Enforcement Authority.~~
- ~~If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC~~authority shall serve as the ~~Compliance Enforcement Authority~~CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was ~~complaint~~compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until ~~found compliant~~mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-~~Term~~-term Planning**	**Medium**	N/A	~~N/A.~~The Responsible Entity has developed recovery plan(s), but the plan(s) do not address all of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery ~~plans,~~plan(s), but the ~~plans~~plan(s) do not address ~~all~~two of the requirements included in ~~Items~~Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber ~~Assets and~~ Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems ~~that~~, but the plan(s) does not address the conditions for activation~~,~~ ~~including roles and responsibility of responders; processes for backup, storage, and protection of information; storage of essential information to~~ in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						System recovery; and preservation of BES Cyber System Information for analysis and diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating ServiceSystems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.
R2	Long TermOperations Planning Real-time Operations	Lower	N/AThe Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1) OR	N/AThe Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1) OR The Responsible	The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems that is stored on backup media initially and at least once each calendar yearplan(s) according to R2 Part 2.1 within 17 calendar months, not to exceed	The Responsible Entity has failed to conduct a not tested the recovery plan test initially upon the effective date(s) according to R2 Part 2.1 within 18 calendar months between tests of the standard and at least once each calendar year

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	15exceeding 18 calendar months between tests. of the plan. (2.1) OR The Responsible Entity has not tested the recovery plan initially upon the effective date of the standard and at least once each 3 yearsinformation used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 17 calendar months, not to exceedexceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part	thereafter, not plan. (2.1) OR The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to exceed 15R2 Part 2.2 within 19 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					2.3 within 38 calendar months, not exceeding 39 calendar months between tests~~, that is an operational exercise in a representative environment to demonstrate readiness.~~. (2.3)	
R3	~~Long Term Planning~~Operations Assessment	Lower	~~N/A~~The Responsible Entity has not distributed updates of the recovery plan to each person or group with a defined role in the recovery plan(s) within 30 and less than 60 calendar days of the update being completed. (3.4)	~~N/A~~The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 30 and less than 60 calendar days after the documentation required by R3 Part 3.1. (3.1) OR The Responsible	The Responsible Entity has not ~~reviewed and~~ documented ~~the results of its~~any lessons learned within 30 and less than 60 calendar days of each recovery plan test or actual incident recovery~~ within 30 calendar days of its execution.~~ . (3.1)	The Responsible Entity has not ~~reviewed its recovery plan(s) initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, or when BES Cyber Systems are replaced.~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Entity has not updated the Recovery plan(s)(s) within 30 and less than 60 calendar days of any of the changes listed in R3 Part 3.3 that the responsible entity determines would impact the ability to execute the plan (3.3) OR The Responsible Entity has not distributed updates of the recovery plan(s) to each person or group with a defined role in the recovery plan(s) within 60 calendar days of the update being completed. (3.4)	OR The Responsible Entity has not updated ~~its~~the recovery plan(s) based on any documented ~~deficiencies or~~ lessons learned within ~~30~~60 calendar days after the documentation required by R3 Part 3.2. (3.2) OR The Responsible Entity has not updated the recovery plan(s)(s) within 60 calendar days of any of ~~its execution.~~the changes listed in R3 Part 3.3 that the responsible entity determines would impact the ability to	~~OR~~ ~~The Responsible Entity has reviewed and updated all of its recovery plans but has not communicated all updates to all responsible personnel~~documented any lessons learned within ~~30~~60 calendar days of ~~completing the updates.~~each recovery plan test or actual incident recovery. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					execute the plan. (3.3)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

(SEE FAQs AND CIPC GUIDELINES AS A BASIS~~)~~.)

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the configuration management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Configuration Management and Vulnerability Assessments

2. **Number:** CIP-010-1

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities described in 4.2.2

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   4.1.7 Reliability Coordinator

   4.1.8 Transmission Operator

   4.1.9 Transmission Owner

   4.2. Facilities:

   4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

   4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that

performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-010-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence.

These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column.

B. Requirements and Measures

Rationale – R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Develop a baseline configuration, which shall include the following for each Cyber Asset identified, individually or by group: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed on the BES Cyber Asset; 1.1.3. Any custom software developed for the entity; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches.	Evidence may include, but is not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset.
Reference to prior version: *New Requirement*		**Change Rationale:** *The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Authorize and document changes that deviate from the existing baseline configuration.	Evidence may include, but is not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.
Reference to prior version: *CIP-007-3, R9; CIP-003-3, R6*		**Change Rationale:** *The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3, Requirement R6.*	
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For a change that deviates from the existing baseline configuration, update the baseline configuration and other documentation required by CIP-005 and CIP-007 as necessary within 30 calendar days of completing the change.	Evidence may include, but is not limited to, updated baseline documentation for changes that impacted CIP-005 or CIP-007 documentation, and relevant CIP-005 or CIP-007 documentation, with a date that is within 30 days of the date of the completion of the change.
Reference to prior version: *CIP-007-3, R9; CIP-005-3, R5*		**Change Rationale:** *Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls identified in CIP-005, CIP-006, and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify these required controls determined in 1.4.1 and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	Evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.5	High Impact BES Cyber System	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline configuration to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	Evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.* *This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.*	

Rationale – R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R2 – Configuration Monitoring			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Where technically feasible, monitor continuously or periodically, not to exceed once every 35 calendar days, for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate detected unauthorized changes.	Evidence may include, but is not limited to, logs from a system that is monitoring the configuration of the BES Cyber System along with records of investigation for any unauthorized changes that were detected by the system.
Reference to prior version: *New Requirement*		**Change Rationale:** *The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.* *This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397.* *Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.*	

Rationale – R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	At least once every calendar year, not to exceed 15 calendar months between assessments, conduct a paper or active vulnerability assessment to determine the extent to which the cyber security controls identified in CIP-005, CIP-006, and CIP-007 are implemented correctly and operating as designed.	Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least once every calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; or • A document listing the date of the assessment and the output of the tools used to perform the assessment.
Reference to prior version: *CIP-005-4, R4; CIP-007-4, R8*		**Change Rationale:** *As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months between assessments, perform an active vulnerability assessment in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline configuration of the BES Cyber System in a production environment. If a test environment was used, document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months between assessments), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.* *As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Except for CIP Exceptional Circumstances and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset), prior to adding a new Cyber Asset perform an active vulnerability assessment of the new Cyber Asset.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of the tools used to perform the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.*	
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).
Reference to prior version: *CIP-005-3, R4.5; CIP-007-3, R8.4*		**Change Rationale:** *Added a requirement for an entity planned date of completion as per the directive in FERC Order No. 706, Paragraph 643.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity has established a configuration management program, but failed to authorize any changes to the baseline configuration and to document those changes. OR The Responsible Entity updated the baseline configuration, but failed to update the required documentation within 30-days of the change being completed.	The Responsible Entity has not established any configuration management programs. OR The Responsible Entity did not implement a configuration management program OR The Responsible Entity has established a configuration management program, but failed to establish a documented baseline OR The Responsible Entity has established a configuration management program, but with respect to the

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						changes in the baseline configuration, did not determine the required cyber security controls identified in CIP-005, CIP-006, and CIP-007 that could be impacted by the changes; or did not verify that the controls were not adversely affected when the change was implemented.
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not established a configuration monitoring process for changes to the baseline. OR The Responsible Entity has not investigated a detected unauthorized change to the baseline configuration.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity has established a configuration monitoring process for changes to the baseline but failed to document a detected unauthorized change.
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems.	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not performed an active vulnerability assessment on a new Cyber Asset prior to adding it to an applicable BES Cyber System. OR	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems.	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems.		The Responsible Entity has not established any vulnerability assessment processes for one of its applicable BES Cyber Systems. OR The Responsible Entity has established and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but failed to perform an active vulnerability assessment in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						configuration of its applicable BES Cyber Systems. OR The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, and the execution status of the mitigation plans.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their Vulnerability Assessment processes, Responsible Entities are strongly encouraged to include at least the following elements:

Paper Vulnerability Assessment

1. Network Discovery - A review of all Electronic Access Points to the Electronic Security Perimeter
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications

Active Vulnerability Assessment

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **~~18~~24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the configuration management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Configuration Management and Vulnerability Assessments

2. **Number:** CIP-010-1

3. **Purpose:** ~~Standard CIP-010-1 requires that Responsible Entities have minimum~~To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration management and vulnerability assessment ~~controls~~requirements in ~~place to protect BES Cyber Assets and~~support of protecting BES Cyber Systems~~.~~ from compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities:~~-~~ For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities described in 4.2.2

   ~~4.1.2~~4.1.3 Generator Operator

   ~~4.1.3~~4.1.4 Generator Owner

   ~~4.1.4~~4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   ~~4.1.5~~4.1.7 Reliability Coordinator

   ~~4.1.6~~4.1.8 Transmission Operator

   ~~4.1.7~~4.1.9 Transmission Owner

   4.2. Facilities:

   4.2.1 ~~that are part of any of the following systems~~**Load Serving Entity:** One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

   ~~4.2.1~~4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLSUVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.24.2.3 where theGenerator Operator

4.2.34.2.4 Generator Owner

4.2.44.2.5 Interchange Coordinator

4.2.5 **Load-Serving Entity** that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.6 NERC

4.2.7 Regional Entity

4.2.84.2.6 Reliability Coordinator

4.2.94.2.7 Transmission Operator

4.2.104.2.8 Transmission Owner

4.3. Facilities:

4.3.1 **Load Serving Entity:** One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.3.2 **Distribution Providers**: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard

- A ~~Transmission~~ Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard

- ~~Its Transmission Operator's restoration plan~~

- ~~**All other**~~ Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~**4.3.3**~~**4.3.1 Responsible Entities**~~:~~ **listed in 4.1 other than Distribution Providers and Load-Serving Entities**: All BES Facilities.

~~**4.3.4**~~**4.3.2 Exemptions:** The following are exempt from Standard CIP-~~010-1~~002-5:

~~**4.3.4.1**~~**4.3.2.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~**4.3.4.2**~~**4.3.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~**4.3.4.3**~~**4.3.2.3** In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~**4.3.4.4** Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.~~

5. Background:

Standard CIP-010-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter ~~as applicable~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of ~~specific elements required~~applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of

the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e~~.~~., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards. Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and categorization processes. ~~Responsible Entities can implement common controls that meet requirements for multiple High and~~
- **Medium Impact BES Cyber Systems**~~. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems~~ –

Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.~~
- ~~**Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.~~
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding ~~High or Medium Impact BES Cyber Systems.~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column.
- ~~**Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.~~
- ~~**Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~
- ~~**Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

~~Rationale – R1:~~

~~The configuration change management processes are intended to prevent unauthorized modifications~~
~~Systems.~~

B. Requirements and Measures

Rationale – R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*.

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Develop a baseline configuration~~ of the BES Cyber System~~, which shall include the following for each ~~BES~~ Cyber Asset identified, individually or by ~~specified grouping~~group: ~~1.1.1. Physical location;~~ ~~1.1.2.~~1.1.1. Operating system(s) (including version~~);~~) or firmware where no independent operating system exists; ~~1.1.3.~~1.1.2. Any commercially available or open-source application software (including version) intentionally installed on the BES Cyber Asset; ~~1.1.4.~~1.1.3. Any custom software ~~and scripts~~ developed for the entity; ~~1.1.5.~~1.1.4. Any logical network accessible ports; and ~~1.1.6.~~1.1.5. Any security~~ patch levels~~ patches.	Evidence may include, but is not limited to: • A spreadsheet identifying the required items of the baseline configuration for each ~~BES~~ Cyber Asset~~ in the BES Cyber System;~~; or • A record in an asset management system that identifies the required items of the baseline configuration for each ~~BES~~ Cyber Asset~~ in the BES Cyber System~~.

CIP-010-1 Table R1 – Configuration Change Management			
Part	~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets	**Requirements**	**Measures**
Reference to prior version: *New Requirement*		**Change Rationale:** *The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Authorization, by the CIP Senior Manager or delegate,~~Authorize and document changes ~~to the BES Cyber System~~ that deviate from the existing baseline configuration.	Evidence may include, but is not limited to: • A change request record and associated electronic ~~approval~~ authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • ~~A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) where an individual with the authority to authorize the change was in attendance.~~Documentation that the change was performed in accordance with the requirement.
Reference to prior version: *CIP-007-3, R9* *; CIP-003-3, R6*		**Change Rationale:** *The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3, Requirement R6.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Update~~For a change that deviates from the existing baseline configuration, update the baseline configuration and other documentation required by ~~a NERC CIP Standard, including identification~~CIP-005 and ~~categorization of the BES Cyber Systems,~~CIP-007 as necessary within 30 calendar days of completing the change.	Evidence may include, but is not limited to~~:~~ • ~~For~~, updated baseline documentation for changes that impacted ~~the categorization of a BES Cyber System, dated categorization documents, with a date that is within 30 days of the date of the completion of the change;~~ • ~~For changes that impacted the~~ CIP-~~009 required recovery plan of a BES Cyber System, a dated recovery plan~~005 or CIP-007 documentation, and relevant CIP-005 or CIP-007 documentation, with a date that is within 30 days of the date of the completion of the change.
Reference to prior version: *CIP-007-3, R9; CIP-005-3, R5*		**Change Rationale:** *Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For a change~~ to the BES Cyber System~~ that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls identified in CIP-005, CIP-006, and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify these required controls determined in 1.4.1 and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	Evidence ~~includes~~may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.5	High Impact BES Cyber System	~~For~~Where technically feasible, for each change that deviates from the existing baseline configuration~~ for Control Centers~~: 1.5.1. Prior to implementing any change in the production environment, test the changes ~~to the BES Cyber System~~ in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline configuration~~ of the BES Cyber System~~ to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	Evidence ~~includes~~may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

~~**Rationale – R2:**~~

~~The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.~~

CIP-010-1 Table R1 – Configuration Change Management			
Part	~~**Applicability**~~**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.* *This change addresses FERC Order ~~,paragraphs~~No. 706, Paragraphs 397, 609, 610, and 611.*	

R2. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning~~]~~].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Rationale – R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

~~2.1~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems.~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ ~~Associated Protected Cyber Assets~~	~~Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any unauthorized changes.~~	~~Evidence may include, but is not limited to, logs from a system that is monitoring the configuration of the BES Cyber System along with records of investigation for any unauthorized changes that were detected by the system.~~
~~**Reference to prior version:**~~ ~~*New Requirement*~~		~~**Change Rationale:** *The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.*~~ ~~*This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order 706, paragraph 397.DHS Catalog & addresses FERC Order 706, paragraph 397.*~~	

~~Rationale – R3:~~

~~The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of security controls as well as to continually improve the security posture of BES Cyber Systems.~~

CIP-010-1 Table R2 – Configuration Monitoring			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
2.1	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Where technically feasible, monitor continuously or periodically, not to exceed once every 35 calendar days, for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate detected unauthorized changes.	Evidence may include, but is not limited to, logs from a system that is monitoring the configuration of the BES Cyber System along with records of investigation for any unauthorized changes that were detected by the system.
Reference to prior version: *New Requirement*		**Change Rationale:** *The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.* *This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397.* *Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.*	

Rationale – R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	~~Initially upon the effective date of the standard and at~~At least once every calendar year~~ thereafter~~, not to exceed 15 calendar months between assessments, conduct a paper or active vulnerability assessment ~~of the security controls~~ to determine the extent to which the ~~controls~~cyber security controls identified in CIP-005, CIP-006, and CIP-007 are implemented correctly and operating as designed.	Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least ~~each~~once every calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; or • A document listing the date of the assessment and the output of the tools used to perform the assessment.
Reference to prior version: *CIP-005-4, R4~~ and~~; CIP-007-4, R8*		**Change Rationale:** *As suggested in FERC Order No. 706~~ paragraph~~, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	~~Initially upon the effective date of the standard and~~Where technically feasible, at least once every ~~3 calendar years thereafter, not to exceed 39~~36 calendar months between assessments, perform an active vulnerability assessment in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline configuration of the BES Cyber System in a production environment. ~~Document~~ If a test environment was used, document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed ~~within 39~~at least once every 36 calendar months ~~of the previous assessment~~between assessments), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706~~ p.~~, Paragraphs 541, 542, 543, 544, 545, and 547.* *As suggested in FERC Order No. 706~~ paragraph~~, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Except for CIP Exceptional Circumstances~~,~~ and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset), prior to adding a new Cyber Asset ~~to a BES Cyber System or Electronic Access Control or Monitoring System,~~ perform an active vulnerability assessment of the new Cyber Asset.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new ~~BES~~ Cyber Asset) and the output of the tools used to perform the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706~~ p.~~, Paragraphs 541, 542, 543, 544, 545, and 547.*	
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of ~~that~~any remediation or mitigation action ~~plan~~items.	Evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items~~ with~~, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).
Reference to prior version: *CIP-005-3, R4.5* *; CIP-007-3, R8.4*		**Change Rationale:** *Added a requirement for an entity planned date of completion as per the ~~FERC~~ directive in FERC Order No. 706, ~~paragraph~~Paragraph 643.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity~~; or~~
- ~~If the Responsible Entity works for~~ shall serve as the Compliance Enforcement Authority ("CEA") unless the ~~Regional Entity, then the~~ applicable entity is owned, operated, or controlled by the Regional Entity ~~will establish an agreement with~~. In such cases the ERO or ~~another~~a Regional entity approved by ~~the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.~~
- ~~If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and~~ FERC or other applicable governmental ~~authorities shall serve as the Compliance Enforcement Authority.~~
- ~~If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC~~authority shall serve as the ~~Compliance Enforcement Authority~~CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was ~~complaint~~compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for ~~since the last completed audit~~each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a ~~Registered~~Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until ~~found compliant~~mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit

- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	~~Lower~~Medium	N/A	~~The Responsible Entity updated the baseline configuration, but failed to update the required documentation within 30-days of the change being completed.~~ N/A	The Responsible Entity has established a configuration management program, but failed to ~~establish a documented baseline.~~ ~~OR~~ ~~The Responsible Entity has established a configuration management program, but failed to have the CIP Senior Manager or delegate~~ authorize any changes to the baseline configuration and to document those changes. OR The Responsible Entity ~~has established a configuration management~~	The Responsible Entity has not established any configuration management programs. OR ~~Did~~The Responsible Entity did not implement a configuration management program OR The Responsible Entity has established a configuration management program, but failed to establish a documented baseline OR The Responsible Entity has established

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~program, but with respect to the changes in~~updated the baseline configuration, ~~did not determine~~but failed to update the required ~~cyber security controls that could be impacted by the changes; or did not verify that the controls were not adversely affected when~~documentation within 30-days of the change ~~was implemented.~~being completed.	a configuration management program, but with respect to the changes in the baseline configuration, did not determine the required cyber security controls identified in CIP-005, CIP-006, and CIP-007 that could be impacted by the changes; or did not verify that the controls were not adversely affected when the change was implemented.
R2	**Operations Planning**	~~Lower~~**Medium**	N/A	N/A	N/A~~The Responsible Entity has established a configuration monitoring process for changes to the baseline but failed to document a detected~~	The Responsible Entity has not established a configuration monitoring process for changes to the

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~unauthorized change.~~	baseline. OR The Responsible Entity has not investigated a detected unauthorized change to the baseline configuration. OR The Responsible Entity has established a configuration monitoring process for changes to the baseline but failed to document a detected unauthorized change.
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has established one or more documented vulnerability assessment	The Responsible Entity has established one or more documented vulnerability assessment	The Responsible Entity has established one or more documented vulnerability assessment processes	The Responsible Entity has established one or more documented vulnerability assessment processes

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems.	processes for each of its applicable BES Cyber Systems, but has not performed an ~~Active Vulnerability Assessment~~active vulnerability assessment on a new ~~BES~~ Cyber Asset prior to adding it to an applicable BES Cyber System. OR The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a	for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems.	for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. OR The Responsible Entity has not established any vulnerability assessment processes for one of its applicable BES Cyber Systems. OR The Responsible Entity has established and documented one

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems.		or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but failed to perform an ~~Active Vulnerability Assessment in a test environment~~active vulnerability assessment in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline configuration of its applicable BES Cyber Systems. OR The Responsible Entity has established one or more

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, and the execution status of the mitigation plans.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

~~The physical location referred to in the baseline configuration is geographically where the BES Cyber Asset is located (e.g. Pine Valley Control Room, Generator X, Substation Y) and should be used to ensure that BES Cyber Systems receive the controls that are applicable to the environment in which the components are located (e.g. control center, transmission facility, generation facility). The physical location is not intended to be a specific floor plan location (e.g., panel A, rack B). As such, the physical location of virtual component should identify where the virtual components are being executed (e.g. Pine Valley Control Room, Generator X, Substation Y).~~

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, ~~patch level~~security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the ~~entity~~Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a ~~control center~~ BES Cyber System ~~which~~at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other ~~control centers~~Control Centers (such as by ICCP).

Requirement R2:

~~It should be understood that the~~The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the ~~Standards Drafting Team~~SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). ~~It is for this~~ For that reason ~~that~~, automated technical monitoring was not explicitly required, and ~~an entity~~a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should ~~not~~note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in ~~the initial NOPR from FERC as well as~~ FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their Vulnerability Assessment processes, Responsible Entities are strongly encouraged to include at least the following elements:

Paper Vulnerability Assessment

1. Network Discovery - A review of all Electronic Access Points to the Electronic Security Perimeter
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications

Active Vulnerability Assessment

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: On May 8, 2012, NERC was alerted that the text contained in the Rationale box for Requirement R1 of CIP-011-1 appeared to be incomplete.

This revised draft corrects the text box size to display all of the text (none of the text was changed).

No other changes were made to this standard or any of the other CIP V5 standards currently posted.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, *Categorizing Cyber Systems — An Approach Based on BES Reliability Functions*, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706, approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2, shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-1

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns Facilities described in 4.2.2

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   4.1.7 Reliability Coordinator

   4.1.8 Transmission Operator

   4.1.9 Transmission Owner

   4.2. Facilities:

   4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

   4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that

performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. Background:

Standard CIP-011-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items

in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:
Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column.

Rationale – R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Summary of Changes: CIP 003-4 R4, R4.2, and R 4.3 have been moved to CIP 011 R1. CIP-003-4, Requirement R4.1 was moved to the definition of BES Cyber System Information.

B. Requirements and Measures

R1. Each Responsible Entity shall implement an information protection program that includes each of the applicable items in *CIP-011-1 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning.]*

M1. Evidence for the information protection program must include the applicable items in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	One or more documented and implemented methods to identify BES Cyber System Information.	Evidence may include, but is not limited to, • Indications on information (e.g., labels) that identify it as BES Cyber System Information; • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or designated electronic and physical location.
Reference to prior version: *CIP-003-3, R4; CIP-003-3, R4.2*		**Change Rationale:** *The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection (*e.g., confidential, public, internal use only, etc.) *This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.*	

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	One or more documented and implemented procedures for handling BES Cyber System Information, including storage, transit, and use.	Evidence may include, but is not limited to: • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure; or • Procedures for handling, which include topics such as the storage, transit, and use of BES Cyber System Information.
Reference to prior version: *CIP-003-3, R4; CIP-003-3 R5.3*		**Change Rationale:** *The SDT removed the language to "protect" information and replaced it with "handling" to clarify the protection that is required.*	

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirement**	**Measure**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems	At least once every calendar year, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	Evidence may include, but is not limited to, once every calendar year, not to exceed 15 months between assessments, the documented review of adherence to its BES Cyber System Information protection program, assessment results, action plan, and evidence to demonstrate that the action plan was implemented.
Reference to prior version: *CIP-003-3, R4.3*		**Change Rationale:** *No significant changes.*	

Rationale – R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except in other high impact or medium impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Asset), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset. If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information, the responsible entity shall maintain chain of custody, which identifies who has possession of the device while it is outside of a Physical Security Perimeter.	Evidence may include, but is not limited to: • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information; or • If removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval of information, a chain of custody record that was maintained.
Reference to prior version: *CIP-007-3, R7.2*		**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*	

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media. If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity shall maintain chain of custody, which identifies who has possession of the device while it is outside of a Physical Security Perimeter.	Evidence may include, but is not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of a an applicable Cyber Asset; • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of a an applicable Cyber Asset; • Other records showing actions taken to prevent unauthorized retrieval such as encrypting, retaining in the Physical Security Perimeter; or • If removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval of information, chain of custody record that was maintained.

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R7.1*		**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.* *The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	The Responsible Entity has implemented a BES Cyber System Information protection program that includes one or more methods to identify BES Cyber System Information, one or more handling procedures for BES Cyber System Information, and has assessed adherence periodically as stated in Part 1.3, but has failed to implement an action plan to remediate deficiencies identified during the assessment.	The Responsible Entity has implemented a BES Cyber System Information protection program that includes one or more methods to identify BES Cyber System Information and one or more handling procedures for BES Cyber System Information, but has failed to assess adherence periodically as stated in Part 1.3, to its BES Cyber System Information protection program.	The Responsible Entity has not implemented a BES Cyber System Information protection program. OR The Responsible Entity has implemented a BES Cyber System Information protection program, but has not implemented one or more methods to identify BES Cyber System Information OR The Responsible Entity has implemented a BES Cyber System Information

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						protection program, but has not implemented one or more procedures for handling BES Cyber System Information.
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity failed to maintain chain of custody for Cyber Assets that contain BES Cyber System Information that have been removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval or destroying the data storage media.	The Responsible Entity has documented one or more processes, including both reuse and disposal, to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Assets, but the Responsible Entity either failed to take action to prevent the unauthorized retrieval of BES Cyber System Information from a Cyber Asset that contained BES Cyber System Information or failed to destroy the	The Responsible Entity has not documented or implemented any disposal or reuse processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					data storage media.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

Assumptions: Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. For example, the Responsible Entity may decide to mark or label the documents. The Responsible Entity may retain all of the information about BES Cyber Systems in a separate repository or physical or electronic location with access control implemented for both the repository and the BES Cyber Assets. Additional methods for implementing the requirement are suggested in the measures section.

While separating BES Cyber System Information into separate classifications is not required as it was in version 4, a Responsible Entity maintains that flexibility if desired. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. Topics that are appropriate for information handling procedures include access, sharing, copying, transmittal, distribution, and disposal or destruction of BES Cyber System Information.

Requirement R2:

Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it must be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Standard Development Timeline

Note: On May 8, 2012, NERC was alerted that the text contained in the Rationale box for Requirement R1 of CIP-011-1 appeared to be incomplete.

This revised draft corrects the text box size to display all of the text (none of the text was changed).

No other changes were made to this standard or any of the other CIP V5 standards currently posted.

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the ~~first~~second posting of Version 5 of the CIP Cyber Security Standards for a ~~45~~40-day formal comment period. An initial concept paper, *Categorizing Cyber Systems — An Approach Based on BES Reliability Functions*, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. ~~This version (Version 5)~~A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706, approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
~~45-day Formal Comment Period with Parallel Initial Ballot~~	~~11/03/2011~~
~~30~~40-day Formal Comment Period with Parallel Successive Ballot	~~March~~April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. ~~18~~24 **Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, ~~the standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5, Requirement R2, shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the ~~Application~~ "Guidelines ~~Section~~and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-1

3. Purpose: ~~Standard CIP-011-1 requires that Responsible Entities have protection controls in place~~To prevent unauthorized access to ~~protect~~ BES Cyber System Information~~.~~ by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities described in 4.2.2

~~4.1.2~~4.1.3 Generator Operator

~~4.1.3~~4.1.4 Generator Owner

~~4.1.4~~4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

~~4.1.5~~4.1.7 Reliability Coordinator

~~4.1.6~~4.1.8 Transmission Operator

~~4.1.7~~4.1.9 Transmission Owner

4.2. Facilities:

4.2.1 ~~that are part of any of the following systems~~**Load Serving Entity:** One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

~~4.2.1~~4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS ~~program required by a NERC~~ or ~~Regional Reliability Standard~~

- ~~A UVLS~~UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme ~~required by a NERC or Regional Reliability Standard~~
- ~~A Transmission Protection System required by a NERC or Regional Reliability Standard~~
- ~~Its Transmission Operator's restoration plan~~

~~4.2.2~~4.2.3 where the~~**Generator Operator**~~

~~4.2.3~~4.2.4 ~~**Generator Owner**~~

~~4.2.4~~4.2.5 ~~**Interchange Coordinator**~~

~~**4.2.5 Load-Serving Entity** that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~**4.2.6 NERC**~~

~~**4.2.7 Regional Entity**~~

~~4.2.8~~4.2.6 ~~**Reliability Coordinator**~~

~~4.2.9~~4.2.7 ~~**Transmission Operator**~~

~~4.2.10~~4.2.8 ~~**Transmission Owner**~~

4.3. ~~**Facilities:**~~

~~**4.3.1 Load Serving Entity:** One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~

~~**4.3.2 Distribution Providers**: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:~~

- ~~A UFLS program required by a NERC or Regional Reliability Standard~~
- ~~A UVLS program required by a NERC or Regional Reliability Standard~~
- ~~A~~ Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard

- A ~~Transmission~~ Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard

- ~~Its Transmission Operator's restoration plan~~
- ~~**All other**~~ Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~**4.3.3**~~**4.3.1 Responsible Entities~~:~~ listed in 4.1 other than Distribution Providers and Load-Serving Entities**: All BES Facilities.

~~**4.3.4**~~**4.3.2 Exemptions:** The following are exempt from Standard CIP-~~011-1~~002-5:

~~**4.3.4.1**~~**4.3.2.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~**4.3.4.2**~~**4.3.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~**4.3.4.3**~~**4.3.2.3** In nuclear plants, the ~~systems~~Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.~~-~~R. Section 73.54.

~~**4.3.4.4** Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.~~

5. Background:

Standard CIP-011-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Each requirement opens~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the ~~required~~applicable items in [Table Reference].*" The referenced table requires the ~~specific elements~~applicable items in the procedures for a common subject matter~~ as applicable~~.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of ~~specific elements required~~applicable items in

the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not ~~infer~~imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e~~.~~., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the ~~Standards~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the ~~Standards.~~standards. Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies~~.~~ to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- ~~**All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.~~
- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~High Impact~~high impact according to the CIP-002-5 identification and categorization processes. ~~Responsible Entities can implement common controls~~

~~that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as ~~Medium Impact~~medium impact according to the CIP-002-5 identification and categorization processes.
- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.~~
- ~~**Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.~~
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding ~~High or Medium Impact BES Cyber Systems.~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding ~~High or Medium Impact BES Cyber Systems~~high impact BES Cyber System or medium impact BES Cyber System in the applicability column.
- ~~**Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.~~
- ~~**Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.~~
- ~~**Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

~~**Rationale – R1:**~~

~~The intent of the information protection processes is to prevent unauthorized access to BES Cyber Syste~~

~~**Summary of Changes:**~~

~~Requirement R4.1 was moved to the definition of BES Cyber System Information.~~

Rationale – R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Summary of Changes: CIP 003-4 R4, R4.2, and R 4.3 have been moved to CIP 011 R1. CIP-003-4, Requirement R4.1 was

B. Requirements and Measures

R1. Each Responsible Entity shall implement ~~one or more documented processes~~an information protection program that ~~collectively include~~includes each of the applicable items in *CIP-011-1 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]~~]~~.]*

M1. Evidence ~~must include each of~~for the ~~applicable documented processes that collectively~~information protection program must include the applicable items in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R1 – Information Protection			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	One or more documented and implemented methods to identify BES Cyber System Information.	Evidence may include, but is not limited to, • Indications on information (e.g., labels) that identify it as BES Cyber System Information; • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber ~~Security~~System Information; or • Repository or designated electronic and physical location.
Reference to prior version: *CIP-003-3, R4* *; CIP-003-3, R4.2*		**Change Rationale:** *The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection~~.~~ (e.g., confidential, public, internal use only, etc.) This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.*	

CIP-011-1 Table R1 – Information Protection			
Part	**~~Part~~Applicable BES Cyber Systems and associated Cyber Assets**	**~~Part~~Requirement**	**~~Part~~Measure**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	~~Access control~~One or more documented and ~~handling~~implemented procedures for handling BES Cyber System Information~~.~~, including storage, transit, and use.	Evidence may include, but is not limited to: • Records indicating ~~information~~ that BES Cyber System Information is ~~stored, transported, and disposed~~handled in a manner consistent with the entity's documented ~~process;~~ procedure; or • ~~Records from an information management system containing electronic copies~~Procedures for handling, which include topics such as the storage, transit, and use of BES Cyber System Information ~~with user access implemented on a need-to-know basis;~~. ~~• Hardcopies of information stored in a locked file cabinet with keys provided to only authorized individuals.~~
Reference to prior version: *CIP-003-3, R4* *; CIP-003-3 R5.3*		**Change Rationale:** *The SDT removed the language to "protect" information and replaced it with "~~Implement~~ handling ~~and access control~~" to clarify the protection that is required.*	

CIP-011-1 Table R1 – Information Protection			
Part	**~~Part~~Applicable BES Cyber Systems and associated Cyber Assets**	**~~Part~~Requirement**	**~~Part~~Measure**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems ~~Associated Protected Cyber Assets~~	~~Initially upon the effective date of the standard and at~~At least once every calendar year~~ thereafter~~, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection ~~process~~program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	Evidence may include, but is not limited to, once every calendar year, not to exceed 15 months between assessments, the documented review of adherence to its BES Cyber System Information protection program, assessment results, action plan, and evidence to demonstrate that the action plan was implemented.
Reference to prior version: *CIP-003-3, R4.3*		**Change Rationale:** *No significant changes.*	

Rationale – R2:

The intent of the ~~media~~BES Cyber Asset reuse and disposal ~~processes~~process is to prevent the unauthorized dissemination of BES Cyber System Information upon ~~media~~ reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-011-1 Table R2 – ~~Media~~BES Cyber Asset Reuse and Disposal. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning~~]~~].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-011-1 Table R2 – ~~Media~~BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R2 – ~~Media~~BES Cyber Asset Reuse and Disposal			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except in other high impact or medium impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Asset ~~media[2]~~,), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the ~~media.~~Cyber Asset. If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information, the responsible entity shall maintain chain of custody, which identifies who has possession of the device while it is outside of a Physical Security Perimeter.	Evidence may include, but is not limited to~~, records that indicate that~~: • Records of actions taken to prevent unauthorized retrieval of BES Cyber ~~Asset media was cleared~~System Information; or • If removed from the Physical Security Perimeter prior to ~~its reuse.~~ action taken to prevent unauthorized retrieval of information, a chain of custody record that was maintained.

~~[2] For the purposes of this Standard, media should be considered to be any mass storage device onto which information from a BES Cyber Asset is recorded and stored electronically, including, but not limited to, magnetic tapes, optical disks, solid-state drives, and magnetic disks.~~

CIP-011-1 Table R2 – ~~Media~~BES Cyber Asset Reuse and Disposal			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R7.2*		**Change Rationale:** *~~(FERC Order 706 - p. 631)~~ Consistent with FERC Order No. 706, ~~paragraph~~Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*	

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems~~.~~ Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Prior to the disposal of ~~BES~~applicable Cyber ~~Asset media~~Assets that contain BES Cyber System Information, the Responsible Entity shall ~~destroy or~~ take action to prevent the unauthorized retrieval of BES Cyber System Information from the ~~media.~~Cyber Asset or destroy the data storage media. If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity shall maintain chain of custody, which identifies who has possession of the device while it is outside of a Physical Security Perimeter.	Evidence may include, but is not limited to~~, records~~: • Records that indicate that ~~BES Cyber Asset~~data storage media was ~~purged or~~ destroyed prior to ~~its~~the disposal~~.~~ of a an applicable Cyber Asset; • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of a an applicable Cyber Asset; • Other records showing actions taken to prevent unauthorized retrieval such as encrypting, retaining in the Physical Security Perimeter; or • If removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval of information, chain of custody record that was maintained.

CIP-011-1 Table R2 – Media Reuse and Disposal			
Part	**~~Applicability~~Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R7.1*		**Change Rationale:** *Consistent with FERC Order No. 706, ~~paragraph~~Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.* *The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

- The Regional Entity; or
- If the Responsible Entity works for shall serve as the Compliance Enforcement Authority ("CEA") unless the Regional Entity, then the applicable entity is owned, operated, or controlled by the Regional Entity will establish an agreement with. In such cases the ERO or another a Regional entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERCauthority shall serve as the Compliance Enforcement AuthorityCEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliantmitigation is complete and approved or for the duration specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	~~N/A~~The Responsible Entity has implemented a BES Cyber System Information protection program that includes one or more methods to identify BES Cyber System Information, one or more handling procedures for BES Cyber System Information, and has assessed adherence periodically as stated in Part 1.3, but has failed to implement an action plan to remediate deficiencies identified during the assessment.	The Responsible Entity has implemented ~~one or more~~a BES Cyber System Information protection ~~processes~~program that ~~include~~includes one or more methods to identify BES Cyber System Information and one or more ~~access control and~~ handling procedures for BES Cyber System Information, but has failed to assess adherence~~, either initially upon the effective date of the standard or~~ periodically as stated in Part 1.3, to its BES Cyber System Information protection ~~processes~~program.	The Responsible Entity has not implemented ~~one or more~~a BES Cyber System Information protection ~~processes~~program. OR The Responsible Entity has implemented ~~one or more~~a BES Cyber System Information protection ~~processes~~program, but has not ~~included~~implemented one or more methods to identify BES Cyber System Information OR The Responsible Entity has

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						implemented ~~one or more~~a BES Cyber System Information protection ~~processes~~program, but has not ~~included~~implemented one or more ~~access control and handling~~ procedures for handling BES Cyber System Information.
R2	**Operations Planning**	**Lower**	N/A	~~N/A~~ The Responsible Entity failed to maintain chain of custody for Cyber Assets that contain BES Cyber System Information that have been removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval or destroying the data storage media.	The Responsible Entity has documented ~~or implemented~~ one or more ~~media~~processes, including both reuse and disposal ~~or reuse processes~~, to prevent the unauthorized retrieval of BES Cyber System Information from the ~~media~~BES Cyber Assets, but the ~~media disposal or~~	The Responsible Entity has not documented or implemented any ~~media~~ disposal or reuse ~~process~~processes to prevent the unauthorized retrieval of BES Cyber System Information from the ~~media~~BES Cyber Asset.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~reuse processes, including~~ Responsible Entity either failed to take action to prevent the ~~recording~~unauthorized retrieval of BES Cyber System Information from a Cyber Asset that contained BES Cyber System Information or failed to destroy the ~~media purge or destruction, were not followed~~data storage media.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

Assumptions: Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within ~~these~~those systems must be evaluated, as the information protection requirements still apply.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. For example, the Responsible Entity may decide to mark or label the documents. The Responsible Entity may retain all of the information about BES Cyber Systems in a separate repository or physical or electronic location with access control implemented for both the repository and the BES Cyber Assets. Additional methods for implementing the requirement are suggested in the measures section.

While separating BES Cyber System Information into separate classifications is not required as it was in version 4, ~~responsible entities still have the~~a Responsible Entity maintains that flexibility ~~to do this~~ if ~~they so desire.~~desired. As long as the ~~entity's~~Responsible Entity's information protection program includes all ~~required elements~~applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements.

~~This~~The SDT does not intend that this requirement ~~is not intended to~~ cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. ~~Information~~Topics that are appropriate for information handling procedures ~~should detail~~include access, sharing, copying, transmittal, distribution, and disposal or destruction of BES Cyber System Information.

Requirement R2:

Media sanitization is generally classified into ~~4~~four categories: ~~disposal~~Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media ~~which~~that is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as ~~this~~that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it ~~should~~must be properly ~~erased~~cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Exhibit F

Record of Development of Proposed CIP Version 5 Reliability Standards

(Part 2 of 2)

Implementation Plan for Version 5 CIP Cyber Security Standards

April 10, 2012

Prerequisite Approvals
All Version 5 CIP Cyber Security Standards and the proposed additions, modifications, and retirements of terms to the *Glossary of Terms* used in *NERC Reliability Standards* must be approved before these standards can become effective.

Applicable Standards
The following standards and definitions, collectively referred to as "Version 5 CIP Cyber Security Standards,"[1] are covered by this Implementation Plan:
CIP–002–5 — Cyber Security —BES Cyber System Categorization
CIP–003–5 — Cyber Security — Security Management Controls
CIP–004–5 — Cyber Security — Personnel and Training
CIP–005–5 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–5 — Cyber Security — Physical Security
CIP–007–5 — Cyber Security — Systems Security Management
CIP–008–5 — Cyber Security — Incident Reporting and Response Planning
CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems
CIP–010–1 — Cyber Security — Configuration Change Management
CIP–011–1 — Cyber Security — Information Protection

"Definitions of Terms used in Version 5 CIP Cyber Security Standards" document, which includes proposed additions, modifications, and retirements of terms to the *Glossary of Terms used in NERC Reliability Standards*.

These standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

When these standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards become effective, all prior versions of these standards are retired.

Compliance with Standards
Once these standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards become effective, the responsible entities identified in the Applicability Section of the standard must comply with the requirements.

[1] Although CIP-010-1 and CIP-011-1 are proposed as first versions, any reference to "Version 5 CIP Cyber Security Standards" includes CIP-010-1 and CIP-011-1, in addition to CIP-002-5 through CIP-009-5, because CIP-010-1 and CIP-011-1 were developed as part of the "Version 5 CIP Cyber Security Standards" development process.

Proposed Effective Date for Version 5 CIP Cyber Security Standards

Responsible entities shall comply with all requirements in CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 as follows:

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5 R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[2]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5 R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Initial Performance of Certain Periodic Requirements

Specific Version 5 CIP Cyber Security Standards have periodic requirements that contain time parameters for subsequent and recurring iterations of the requirement; such as, but not limited to, ". . . once each calendar year . . ." and responsible entities shall comply initially with those periodic requirements, as follows:

1. On or before the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-002-5 R2
   - CIP-003-5 R4
2. Within 14 calendar days after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-007-5 R4 Part 4.5
3. Within 35 calendar days after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-007-5 R3 Part 3.3
   - CIP-010-1 R2 Part 2.1

[2] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

4. Within three calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5 R6, Part 6.5
5. Within 12 calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5 R3, Part 3.2
   - CIP-004-5 R6, Parts 6.6 and 6.7
   - CIP-006-5 R3, Part 3.1
   - CIP-008-5 R2, Part 2.1
   - CIP-008-5 R3, Part 3.1
   - CIP-009-5 R2, Parts 2.1 and 2.2
   - CIP-009-5 R3, Part 3.1
   - CIP-010-5 R3, Parts 3.1 and 3.2
   - CIP-011-5 R1, Part 1.3
6. Within 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment for the following requirement:
   - CIP-004-5 R5 Part 5.2.

Previous Identity Verification

A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be reperformed under CIP-004-5 R4, Part 4.1.

Unplanned Changes Resulting in a Higher Categorization

Planned changes refer to any changes of the electric system or BES Cyber System, as described in CIP-002-5, R1.1, which were planned and implemented by the responsible entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the Version 5 CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System as described in CIP-002-5, R1.1, which were not planned by the responsible entity. Consider the scenario

where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-5, Attachment 1, criteria.

For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System, as required in CIP-002-5, R1.1

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System, as required in CIP-002-5, R1.4:

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies first medium impact or high impact BES Cyber System	24 months

Additional Guidance and Implementation Time Periods for Disaster Recovery

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003-5, R1.

The rationale for this is that the primary task following a disaster is the restoration of the power system and the ability to serve customer Load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full compliance with the Version 5 CIP Cyber Security Standards, restoration could be hampered and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to comply with the Version 5 CIP Cyber Security Standards at the restored Facilities, and be able to demonstrate full compliance in a spotcheck or audit; or file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

The following security requirements in CIP-003 through CIP-011 apply to these Associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-004-5 R2	Cyber Security Training Program	X	X	
CIP-004-5 R3	Cyber Security Training	X	X	
CIP-004-5 R4	Personnel Risk Assessment Program	X	X	
CIP-004-5 R5	Personnel Risk Assessment	X	X	
CIP-004-5 R6	Access Management Program	X	X	
CIP-004-5 R7	Access Revocation	X	X	
CIP-005-5 R2	Remote Access Management			X
CIP-006-5 R1	Physical Security Plan	X	X	X
CIP-006-5 R2	Visitor Control Program	X		X
CIP-006-5 R3	Maintenance and Testing Program		X	
CIP-007-5 R1	Ports and Services	X	X	X
CIP-007-5 R2	Security Patch Management	X	X	X
CIP-007-5 R3	Malicious Code	X	X	X

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
	Prevention			
CIP-007-5 R4	Security Event Monitoring	X	X	X
CIP-007-5 R5	System Access Control	X	X	X
CIP-010-1 R1	Configuration Change Management	X	X	X
CIP-010-1 R2	Configuration Monitoring	X	X	X
CIP-010-1 R3	Vulnerability Assessments	X	X	X
CIP-011-1 R1	Information Protection	X	X	
CIP-011-1 R2	BES Cyber Asset Reuse and Disposal	X	X	X

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan ~~For~~for Version 5 CIP Cyber Security Standards

~~November 7, 2011~~

April 10, 2012

Prerequisite Approvals

All Version 5 CIP Cyber Security Standards and the proposed additions, modifications, and retirements of terms to the *Glossary of Terms* ~~*Used*~~used in *NERC Reliability Standards* must be approved before these standards can become effective.

Applicable Standards

The following standards and definitions, collectively referred to as "Version 5 CIP Cyber Security Standards[1]," "[2] are covered by this Implementation Plan:

CIP–002–5 — Cyber Security — BES Cyber System ~~Identification~~Categorization
CIP–003–5 — Cyber Security — Security Management Controls
CIP–004–5 — Cyber Security — Personnel and Training
CIP–005–5 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–5 — Cyber Security — Physical Security
CIP–007–5 — Cyber Security — Systems Security Management
CIP–008–5 — Cyber Security — Incident Reporting and Response Planning
CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems
CIP–010–1 — Cyber Security — Configuration Change Management
CIP–011–1 — Cyber Security — Information Protection

"Definitions of Terms ~~Used~~used in Version 5 CIP Cyber Security Standards" document, which includes proposed additions, modifications, and retirements of terms to the *Glossary of Terms* ~~*Used*~~*used in NERC Reliability Standards*.

These standards and Definitions of Terms ~~Used~~used in Version 5 CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

When these standards and Definitions of Terms ~~Used~~used in Version 5 CIP Cyber Security Standards become effective, all prior versions of these standards are retired.

~~[1] Although CIP-010-1 and CIP-011-1 are proposed as first versions, any reference to "Version 5 CIP Cyber Security Standards" includes CIP-010-1 and CIP-011-1 in addition to CIP-002-5 through CIP-009-5 because CIP-010-1 and CIP-011-1 were developed as part of the "Version 5 CIP Cyber Security Standards" development process.~~

[2] Although CIP-010-1 and CIP-011-1 are proposed as first versions, any reference to "Version 5 CIP Cyber Security Standards" includes CIP-010-1 and CIP-011-1, in addition to CIP-002-5 through CIP-009-5, because CIP-010-1 and CIP-011-1 were developed as part of the "Version 5 CIP Cyber Security Standards" development process.

Compliance with Standards

Once these standards and Definitions of Terms ~~Used~~used in Version 5 CIP Cyber Security Standards become effective, the ~~Responsible Entities~~responsible entities identified in the Applicability ~~section~~Section of the standard must comply with the requirements.~~ These Responsible Entities include:~~

~~• Reliability Coordinator~~
~~• Balancing Authority~~
~~• Interchange Authority~~
~~• Transmission Owner~~
~~• Transmission Operator~~
~~• Generator Owner~~
~~• Generator Operator~~
~~• Load Serving Entity~~
~~• Distribution Provider~~
~~• NERC~~
~~• Regional Entity~~

Proposed Effective Date for Version 5 CIP Cyber Security Standards

Responsible ~~Entities~~entities shall comply with all requirements in CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1~~, and the Definitions of Terms Used in Version 5 CIP Cyber Security Standards~~ as follows:

1. **~~18~~24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the later of ~~January~~July 1, 2015, or the first calendar day of the ~~seventh~~ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5 R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[3]
2. In those jurisdictions where no regulatory approval is required, the ~~standards~~Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the first day of the ~~seventh~~ninth calendar quarter following Board of ~~Trustees~~Trustees' approval, and CIP-003-5 R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[3] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Initial Performance of Certain Periodic Requirements

Specific Version 5 CIP Cyber Security Standards have periodic requirements that contain time parameters for subsequent and recurring iterations of the requirement; such as, but not limited to, ". . . once each calendar year . . ." and responsible entities shall comply initially with those periodic requirements, as follows:

1. On or before the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-002-5 R2
   - CIP-003-5 R4
2. Within 14 calendar days after the Effective Date of the Version 5 CIP Cyber Secuirty Standards for the following requirements:
   - CIP-007-5 R4 Part 4.5
3. Within 35 calendar days after the Effective Date of the Version 5 CIP Cyber Secuirty Standards for the following requirements:
   - CIP-007-5 R3 Part 3.3
   - CIP-010-1 R2 Part 2.1
4. Within three calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5 R6, Part 6.5
5. Within 12 calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5 R3, Part 3.2
   - CIP-004-5 R6, Parts 6.6 and 6.7
   - CIP-006-5 R3, Part 3.1
   - CIP-008-5 R2, Part 2.1
   - CIP-008-5 R3, Part 3.1
   - CIP-009-5 R2, Parts 2.1 and 2.2
   - CIP-009-5 R3, Part 3.1
   - CIP-010-5 R3, Parts 3.1 and 3.2
   - CIP-011-5 R1, Part 1.3

6. Within 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment for the following requirement:
   - CIP-004-5 R5 Part 5.2.

Previous Identity Verification

A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be reperformed under CIP-004-5 R4, Part 4.1.

Unplanned Changes Resulting in a Higher Categorization

Planned changes refer to any changes of the electric system or BES Cyber System, as described in CIP-002-5, R1.1, which were planned and implemented by the ~~Responsible Entity~~responsible entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in ~~Compliance~~compliance with the Version 5 CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System as described in CIP-002-5, R1.1, which were not planned by the ~~Responsible Entity.~~responsible entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5, Attachment 1~~. Then~~, then, later, an action is performed outside of that particular transmission substation~~,~~; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, ~~or load patterns shift resulting in corresponding transmission flow changes through that transmission substation,~~ and that unchanged BES Cyber System may become a ~~Medium Impact~~ medium impact BES Cyber System based on the CIP-002-5, Attachment 1, criteria~~. The actions that cause the change in power flows would have been performed by a neighboring entity and would result in a change in impact level the of the affected BES Cyber System~~.

For *planned* changes resulting in a higher categorization, the ~~Responsible Entity~~responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System, as required in CIP-002-5, R1.1

For *unplanned* changes resulting in a higher categorization, the ~~Responsible Entity~~responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System, as required in CIP-002-5, R1.~~1~~4:

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New ~~High Impact~~high impact BES Cyber System	12 months
New ~~Medium Impact~~medium impact BES Cyber System	12 months
Newly categorized ~~High Impact~~high impact BES Cyber System from ~~Medium Impact~~medium impact BES Cyber System	12 months for ~~new~~ requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized ~~Medium Impact~~medium impact BES Cyber System	12 months
Responsible ~~Entity Identifies~~entity identifies first ~~Medium~~medium impact or ~~High Impact~~high impact BES Cyber System	~~Add 12~~24 months ~~from time above~~

Additional Guidance and Implementation Time Periods for Disaster Recovery

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003-5~~ R2~~, R1.

The rationale for this is that the primary task following a disaster is the restoration of the power system~~,~~ and the ability to serve customer ~~load~~Load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full ~~implementation of the CIP~~ compliance ~~implementation program~~with the Version 5 CIP Cyber Security Standards, restoration could be hampered~~,~~ and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to ~~implement~~comply with the Version 5 CIP ~~compliance implementation program~~Cyber Security Standards at the restored ~~facilities~~Facilities, and be able to demonstrate full compliance in a ~~spot-check~~spotcheck or audit; or~~,~~ file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

The following security requirements in CIP-003 through CIP-011 apply to these Associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-004-5 R2	Cyber Security Training Program	X	X	
CIP-004-5 R3	Cyber Security Training	X	X	
CIP-004-5 R4	Personnel Risk Assessment Program	X	X	
CIP-004-5 R5	Personnel Risk Assessment	X	X	
CIP-004-5 R6	Access Management Program	X	X	
CIP-004-5 R7	Access Revocation	X	X	
CIP-005-5 R2	Remote Access Management			X
CIP-006-5 R1	Physical Security Plan	X	X	X
CIP-006-5 R2	Visitor Control Program	X		X
CIP-006-5 R3	Maintenance and Testing Program		X	
CIP-007-5 R1	Ports and Services	X	X	X
CIP-007-5 R2	Security Patch Management	X	X	X
CIP-007-5 R3	Malicious Code Prevention	X	X	X
CIP-007-5 R4	Security Event Monitoring	X	X	X
CIP-007-5 R5	System Access Control	X	X	X
CIP-010-1 R1	Configuration Change Management	X	X	X
CIP-010-1 R2	Configuration Monitoring	X	X	X

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-010-1 R3	Vulnerability Assessments	X	X	X
CIP-011-1 R1	Information Protection	X	X	
CIP-011-1 R2	BES Cyber Asset Reuse and Disposal	X	X	X

Definitions of Terms Used in Version 5 CIP Cyber Security Standards

This section includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards and proposes terms for retirement. Terms already defined in the Glossary of Terms used in NERC Reliability Standards are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary. New defined terms are underscored. For existing glossary terms, new language is shown as underscored, while deleted language is shown as stricken. The list of terms proposed for retirement is at the end of the document.

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, Systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, Systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

Cyber Security Incident

~~Any~~ A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter~~ of a Critical Cyber Asset~~, or~~,~~
- Disrupts, or was an attempt to disrupt, the operation of a ~~Critical Cyber Asset~~ BES Cyber System.

BES Cyber System

One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

BES Cyber System Information

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. Examples of BES Cyber System Information may include, but are not limited to, security procedures developed by the responsible entity and security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology

of the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements.

CIP Exceptional Circumstance

A situation that involves one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of the requirements within the NERC CIP Standards.

Control Center

One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability functional tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generation Operator for generation Facilities at two or more locations.

Cyber Assets

Programmable electronic devices, ~~and communication networks~~ including the hardware, software, and data in those devices.

Electronic Access Control or Monitoring Systems

Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems.

Electronic Access Point ("EAP")

A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Electronic Security Perimeter ("ESP")

The logical border surrounding a network to which ~~Critical Cyber Assets~~ BES Cyber Systems are connected using a routable protocol ~~and for which access is controlled~~.

External Routable Connectivity

A BES Cyber System that is accessible from a Cyber Asset that is outside its associated Electronic Security Perimeter via a bi-directional routable protocol connection.

Interactive Remote Access

All user-initiated access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether routable or dial-up access, using a client or remote access technology. Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Intermediate Device

A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate Device must not be located inside the Electronic Security Perimeter.

Physical Access Control Systems

Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Physical Security Perimeter ("PSP")

~~The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.~~

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside, and for which access is controlled.

Protected Cyber Asset

A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter (a Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset within an ESP or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes).

Reportable Cyber Security Incident

Any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.

Terms to be retired from the *Glossary of Terms used in NERC Reliability Standards* **once the standards that use those terms are replaced:**

Critical Assets

Critical Cyber Assets

Definitions of Terms Used in Version 5 CIP Cyber Security Standards

This section includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards and proposes terms for retirement. Terms already defined in the Glossary of Terms used in NERC Reliability Standards are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary. New defined terms are underscored. For existing glossary terms, new language is shown as underscored, while deleted language is shown as stricken. The list of terms proposed for retirement is at the end of the document.

~~**Effective Dates**~~

~~1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]~~

~~1. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, ~~when required,~~ adversely impact one or more ~~BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in~~Facilities, Systems, or equipment, which ~~that~~, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation ~~occurs and impacts~~of the ~~BES~~Bulk Electric System.

~~[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.~~

Redundancy of affected Facilities, Systems, and equipment shall not be considered when determining ~~availability.~~ adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A ~~Transient~~Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset ~~is not considered~~ within an ESP, or to a BES Cyber Asset~~.~~, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

~~BES~~ Cyber Security Incident

~~Any~~ A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter~~ of a Critical Cyber Asset~~, or~~,~~
- Disrupts, or was an attempt to disrupt, the operation of a ~~Critical Cyber Asset~~ BES Cyber System~~, or~~.
- ~~Results in unauthorized physical access into a Defined Physical Boundary~~.

BES Cyber System

One or more BES Cyber Assets ~~that are typically grouped together,~~ logically ~~or physically,~~grouped by a responsible entity to ~~operate~~perform one or more ~~BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System~~reliability tasks for a functional entity.

BES Cyber System Information

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. Examples of BES Cyber System Information may include, but are not limited to, security procedures developed by the responsible entity and security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements.~~Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations;~~

equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans.

BES Reliability Operating Services

BES Reliability Operating Services are those services contributing to the real-time reliable operation of the Bulk Electric System (BES). They include the following Operating Services:

Dynamic Response to BES conditions

Actions performed by BES Elements, Facilities or systems automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition.

Aspects of BES Dynamic Response include, but are not limited to:

- Spinning reserve (contingency reserves)
  - Providing actual reserves
  - Monitoring that reserves are sufficient
- Governor Response
  - Control system used to actuate governor response
- Protection Systems (transmission & generation)
  - Line, bus, x-former, generator
  - Zone protection
  - Breaker protection
  - Current, frequency, speed, phase
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays & breakers, possibly software
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers
- Power System Stabilizers

Balancing Load and Generation

~~Activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time.~~

~~Aspects of the Balancing Load and Generation Operating Service include, but are not limited to:~~

- ~~Calculation of ACE~~
  - ~~Field data sources (real time tie flows, frequency sources, time error, etc)~~
  - ~~Software used to perform calculation~~
- ~~Unit commitment~~
  - ~~Know generation status & capability & restrictions (must runs, minimum run times, ramp, heat rates, etc), load schedules~~
- ~~Load management~~
  - ~~Ability to identify load change need~~
  - ~~Ability to implement load changes~~
- ~~Demand Response~~
  - ~~Ability to identify load change need~~
  - ~~Ability to implement load changes~~
- ~~Manually Initiated Load shedding~~
  - ~~Ability to identify load change need~~
  - ~~Ability to implement load changes~~
- ~~Non-spinning reserve (contingency reserve)~~
  - ~~Know generation status, capability, ramp rate, start time~~
  - ~~Start units and provide energy~~

~~Controlling Frequency (Real Power)~~

~~Activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES.~~

~~Aspects of the Controlling Frequency Operating Service include, but are not limited to:~~

- ~~Generation Control (such as AGC)~~
  - ~~ACE, current generator output, ramp rate, unit characteristics~~
  - ~~Software to calculate unit adjustments~~
  - ~~Transmit adjustments to individual units~~

- Unit controls implementing adjustments
- Regulation (regulating reserves)
  - Frequency source, schedule
  - Governor control system

Controlling Voltage (Reactive Power)

Activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES.

Aspects of the Controlling Voltage Operating Service include, but are not limited to:

- AVR (Automatic Voltage Regulation)
  - Sensors, stator control system, feedback
- Capacitive resources
  - Status, control (manual or auto), feedback
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback
- SVC (Static VAR Compensators)
  - Status, computations, control (manual or auto), feedback

Managing Constraints

Activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES.

Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC)
- Interchange schedules
- Generation re-dispatch and unit commit
- Identify and monitor SOL's & IROL's

Identify and monitor Flowgates

Monitoring & Control

Activities, actions, and conditions that provide monitoring and control of BES elements.

An example aspect of the Monitoring and Control Service is, but is not limited to:

- ~~All methods of operating breakers and switches (such as SCADA)~~

~~Restoration of BES~~

~~Activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance.~~

~~Aspects of the Restoration of BES Operating Service include, but are not limited to:~~

- ~~Blackstart restoration including planned cranking path~~
- ~~Off-site power for nuclear facilities.~~

~~Situational Awareness~~

~~Activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions.~~

~~Aspects of the Situation Awareness Operating Service include, but are not limited to:~~

- ~~Monitoring and alerting (such as EMS alarms)~~
- ~~Change management~~
- ~~Current Day & Next Day planning~~
- ~~Contingency Analysis~~
- ~~Frequency monitoring~~

~~Inter-Entity Real-Time Coordination and Communication~~

~~Activities, actions, and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES.~~

~~Aspects of the Inter-Entity Coordination and Communication Operating Service include, but are not limited to:~~

- ~~Scheduled interchange~~
- ~~Facility operational data and status~~
- ~~Operational directives~~

CIP Exceptional Circumstance

A situation that involves one or more of the following, or similar, conditions~~:~~ that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of the requirements within the NERC CIP Standards.

Control Center

One or more facilities hosting ~~a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions~~operating personnel that ~~support~~monitor and control the Bulk Electric System (BES) in real-time ~~operations by System Operators~~to perform the reliability functional tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more ~~BES~~locations, or 4) a Generation Operator for generation ~~facilities or transmission facilities,~~Facilities at two or more locations~~:~~

- ~~Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,~~
- ~~Inter-utility exchange of BES reliability or operability data,~~
- ~~Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES,~~
- ~~Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function,~~
- ~~Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES~~
- ~~Coordination of BES restoration activities~~.

Cyber Assets

Programmable electronic devices, ~~and communication networks~~ including the hardware, software, and data in those devices.

~~**Defined Physical Boundary ("DPB")**~~

~~The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside and for which access is controlled.~~

> ~~***Change Rationale: "Defined Physical Boundary (DPB)" replaces "Physical Security Perimeter."*** *Previous versions of the CIP standard focused on the development of a completely enclosed Physical Security Perimeter (PSP) ("six-wall" border) and managing access though this boundary. This has proven difficult due to the nature of the operating environment for many electrical utilities, especially in field locations. The intent of this standard is to focus on the controls put in place to restrict access rather than solely focusing on the PSP and a boundary protection model for physical security.*~~

Electronic Access Control or Monitoring Systems

Cyber Assets ~~used in the~~that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems.

Electronic Access Point ("EAP")

~~An~~ A Cyber Asset interface on ~~a Cyber Asset~~ an Electronic Security Perimeter that ~~restricts~~allows routable ~~or dial-up data communications~~communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Electronic Security Perimeter ("ESP")

The logical border surrounding a network to which ~~Critical Cyber Assets~~ BES Cyber Systems are connected using a routable protocol ~~and for which access is controlled~~. ~~A collection of Electronic Access Points that protect one or more BES Cyber Systems.~~

~~**External Connectivity**~~

~~Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.~~

External Routable Connectivity

~~The~~A BES Cyber System that is accessible from ~~any~~a Cyber Asset that is outside its associated ~~ESP~~Electronic Security Perimeter via a bi-directional routable protocol connection.

Interactive Remote Access

~~Any~~All user ~~interactive~~-initiated access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether ~~network-based~~routable or dial-up access~~.~~, using a client or remote access technology. Remote access ~~can~~may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Intermediate Device

A Cyber Asset ~~that 1) may be used to provide the required multi-factor authentication for the interactive remote~~or collection of Cyber Assets performing access~~; 2) may be a termination point for required encrypted communication; and 3) may~~ control to restrict ~~the interactive remote access~~ Interactive Remote Access to only authorized users. The Intermediate ~~devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may~~Device must not be located ~~outside~~inside the Electronic Security Perimeter~~, as part of the Electronic Access Point, or in a DMZ network.~~.

Physical Access Control Systems

Cyber Assets that control, alert, or log access to the ~~Defined~~ Physical ~~Boundary~~Security Perimeter(s), exclusive of locally mounted hardware or devices at the ~~Defined~~ Physical ~~Boundary~~Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Physical Security Perimeter ("PSP")

~~The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.~~

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside, and for which access is controlled.

Protected Cyber Asset

A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System~~. A Transient~~ within the same Electronic Security Perimeter (a Cyber Asset is not ~~considered~~ a Protected Cyber Asset~~.~~ if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset within an ESP or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes).

Reportable ~~BES~~ Cyber Security Incident

Any ~~BES~~ Cyber Security Incident that has compromised or disrupted ~~a BES Reliability Operating Service.~~ one or more reliability tasks of a functional entity.

~~**Transient Cyber Asset**~~

~~A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset, 2) used for data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System.~~

Terms to be retired from the *Glossary of Terms used in NERC Reliability Standards* **once the standards that use those terms are replaced:**

Critical Assets

Critical Cyber Assets

~~**Physical Security Perimeter**~~

Unofficial Comment Form

Request for Comments Regarding the Draft of CIP Cyber Security Standards Version 5

Comment Form A
CIP-002 and CIP-003 Questions

Please **DO NOT** use this form to submit comments. Please use the electronic comment form to submit comments on the second formal posting of Project 2008-06 – CSO706 Version 5 CIP Standards. The electronic comment form must be completed by **May 21, 2012.**

2008-06 Project Page

If you have questions please contact Steven Noess at steven.noess@nerc.net or 404-446-9691.

Background

The Project 2008-06 Standard Drafting Team (SDT) is seeking industry feedback and suggestions on this Version 5 of the CIP Cyber Security Standards and its Implementation Plan. The industry feedback will be considered by the SDT in revising and refining Version 5 and related documents.

The SDT thanks stakeholders and other commenters for the extensive and thoughtful comments received during the previous posting period. The volume and quality of the comments provided significant input into many of the changes the team made in response. The SDT also thanks the many observers who attended several comment resolution and discussion sessions—both electronically and face-to-face—that the SDT conducted to prepare the drafts that are currently posted.

The SDT expended considerable work in reviewing, discussing, and responding to all of these inputs, and it believes that the major issues from these inputs have been addressed responsively in this posted draft CIP Version 5 package. As a result, the changes have been significant and substantive in all of the draft CIP Version 5 standards and Implementation Plan.

- Many entities expressed concern over the expanded scope of these standards. The SDT has drafted these standards in response to directives from FERC Order No. 706, and believes that the changes in CIP Version 5 are necessary to address all of those directives responsively. The number of requirements in Version 5 is not substantively higher than previous versions.

- There are many substantive changes in the Applicability section of the standards in response to concerns regarding Distribution Providers and Load Serving Entities. The changes ensure that only those systems owned by those functional entities that are material to BES reliability are within the scope of these standards.

- The SDT also made several substantive changes in CIP-002-5 to address stakeholders' preference for a facilities-based approach to the identification and categorization process for BES Cyber Systems and BES Cyber Assets. In addition, in response to concerns to overall reliability in the restoration facilities area, the SDT made substantive changes to the categorization of those facilities. The SDT made several changes in response to comments in the "bright-line" criteria in Attachment 1 as well.

- In standards CIP-003-5 through CIP-011-1, the SDT made substantive changes in the applicability of requirements to the medium impact category in response to concerns of practical application in field assets. The SDT also addressed many of concerns on requirement clarity and language in the standards. In addition, the SDT moved all low impact requirements and grouped them as policy/program requirements in CIP-003 (Security Management). Requirements in CIP-004-CIP-011 only apply to high and medium impact systems.

- In response to comments, the SDT extended the Implementation Plan's effective date to 24 months after approval in most cases, with up to 36 months for implementation for low impact systems. In addition, the initial required performance of those requirements with periodicity is moved into the Implementation Plan and removed from the requirements in the standards, since the initial performances are one-time requirements tied to the effective date.

In summary, the SDT believes this posting package addresses all of the substantive issues received from the comments and various other inputs.

The Project 2008-06 – Cyber Security Order 706 SDT was appointed by the NERC Standards Committee on August 7, 2008 to review each of the CIP reliability standards and develop the modifications necessary to address the directives in the FERC Order No. 706. Please see the Project 2008-06 background document that accompanies the other posted material.

Instructions:

The SDT is providing this form for industry participants to offer their comments on draft 2 of Version 5 of the CIP Cyber Security Standards.

Questions that ask for a "yes" or "no" response are separated from questions that ask for a narrative response. The drafting team considers each comment received irrespective of whether that comment accompanies a "yes" or "no" response to a particular question or is associated with an "affirmative" or "negative" ballot.

For each question that you provide a comment, please provide specific suggestions that would eliminate or minimize any concerns you have with the item in question. A comment or response to every question is not required.

VERY IMPORTANT:
Please note that the official comment form *does not* retain formatting (even if it appears to transfer formatting when you copy from the unofficial Word version of the form into the official electronic comment form). If you enter extra carriage returns, bullets, automated numbering, symbols, bolding, italics, or any other formatting, that formatting will not be retained when you submit your comments. Therefore, if you would like to separate portions of your comment by idea, e.g., the drafting team requests that each distinct idea in the same comment block be prefaced with (1), (2), etc., instead of using formatting such as extra carriage returns, bullets, automated numbering, bolding, or italics.

A. CIP-002 and CIP-003 Questions:

1. Requirement R1 of draft CIP-002-5 requires the identification of high and medium impact BES Cyber Systems as described in Attachment 1. Further, it requires a Responsible Entity to review (and update as needed), the required identification within 60 calendar days of when a change to BES Elements or Facilities is placed into operation, which is planned to be in service for more than 6 calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category. Do you agree with the proposed Requirement R1?

   ☐ Yes

   ☐ No

2. Requirement R2 of draft CIP-002-5 states, "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once each calendar year, not to exceed 15 calendar months between approvals, even if it has no identified items in Requirement R1, Parts 1.1, 1.2, or 1.3." Do you agree with the proposed Requirement R2?

   ☐ Yes

   ☐ No

3. CIP-002-5: If you disagree with the changes made to CIP-002-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

   Comments:

4. CIP-003-5 R1 states "Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall implement one or more documented cyber security policies that address the

following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R1?

- ☐ Yes
- ☐ No

5. CIP-003-5 R2 states "Each Responsible Entity for its BES Cyber Systems not identified as high impact or medium impact shall implement one or more documented cyber security policies to address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2?

   - ☐ Yes
   - ☐ No

6. CIP-003-5 R3 states "Each Responsible Entity shall identify a CIP Senior Manager by name." Do you agree with the proposed Requirement R3?

   - ☐ Yes
   - ☐ No

7. CIP-003-5 R4 states "Each Responsible Entity shall review and obtain CIP Senior Manager approval for cyber security policies identified in Requirements R1 and R2, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals." Do you agree with the proposed Requirement R4?

   - ☐ Yes
   - ☐ No

8. CIP-003-5 R5 states "Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate and the date of the delegation, and approved by the CIP Senior Manager." Do you agree with the proposed Requirement R5?

   - ☐ Yes
   - ☐ No

9. CIP-003-5 R6 states "Each Responsible Entity shall document any changes to the CIP Senior Manager or any delegations within thirty calendar days of the change. Delegation changes do not

need to be reinstated with a change to the delegator." Do you agree with the proposed Requirement R5?

- ☐ Yes
- ☐ No

10. CIP-003-5: If you disagree with the changes made to CIP-003-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

    Comments:

Unofficial Comment Form

Request for Comments Regarding the Draft of CIP Cyber Security Standards Version 5

Comment Form B
CIP-004, CIP-005, CIP-006 and CIP-007

Please **DO NOT** use this form to submit comments. Please use the electronic comment form to submit comments on the second formal posting of Project 2008-06 – CSO706 Version 5 CIP Standards. The electronic comment form must be completed by **May 21, 2012.**

2008-06 Project Page

If you have questions please contact Steven Noess at steven.noess@nerc.net or 404-446-9691.

Background

The Project 2008-06 Standard Drafting Team (SDT) is seeking industry feedback and suggestions on this Version 5 of the CIP Cyber Security Standards and its Implementation Plan. The industry feedback will be considered by the SDT in revising and refining Version 5 and related documents.

The SDT thanks stakeholders and other commenters for the extensive and thoughtful comments received during the previous posting period. The volume and quality of the comments provided significant input into many of the changes the team made in response. The SDT also thanks the many observers who attended several comment resolution and discussion sessions—both electronically and face-to-face—that the SDT conducted to prepare the drafts that are currently posted.

The SDT expended considerable work in reviewing, discussing, and responding to all of these inputs, and it believes that the major issues from these inputs have been addressed responsively in this posted draft CIP Version 5 package. As a result, the changes have been significant and substantive in all of the draft CIP Version 5 standards and Implementation Plan.

- Many entities expressed concern over the expanded scope of these standards. The SDT has drafted these standards in response to directives from FERC Order No. 706, and believes that the changes in CIP Version 5 are necessary to address all of those directives responsively. The number of requirements in Version 5 is not substantively higher than previous versions.

- There are many substantive changes in the Applicability section of the standards in response to concerns regarding Distribution Providers and Load Serving Entities. The changes ensure that only those systems owned by those functional entities that are material to BES reliability are within the scope of these standards.

- The SDT also made several substantive changes in CIP-002-5 to address stakeholders' preference for a facilities-based approach to the identification and categorization process for BES Cyber Systems and BES Cyber Assets. In addition, in response to concerns to overall reliability in the restoration facilities area, the SDT made substantive changes to the categorization of those facilities. The SDT made several changes in response to comments in the "bright-line" criteria in Attachment 1 as well.

- In standards CIP-003-5 through CIP-011-1, the SDT made substantive changes in the applicability of requirements to the medium impact category in response to concerns of practical application in field assets. The SDT also addressed many of concerns on requirement clarity and language in the standards. In addition, the SDT moved all low impact requirements and grouped them as policy/program requirements in CIP-003 (Security Management). Requirements in CIP-004-CIP-011 only apply to high and medium impact systems.

- In response to comments, the SDT extended the Implementation Plan's effective date to 24 months after approval in most cases, with up to 36 months for implementation for low impact systems. In addition, the initial required performance of those requirements with periodicity is moved into the Implementation Plan and removed from the requirements in the standards, since the initial performances are one-time requirements tied to the effective date.

In summary, the SDT believes this posting package addresses all of the substantive issues received from the comments and various other inputs.

The Project 2008-06 – Cyber Security Order 706 SDT was appointed by the NERC Standards Committee on August 7, 2008 to review each of the CIP reliability standards and develop the modifications necessary to address the directives in the FERC Order No. 706. Please see the Project 2008-06 background document that accompanies the other posted material.

Instructions:

The SDT is providing this form for industry participants to offer their comments on draft 2 of Version 5 of the CIP Cyber Security Standards.

Questions that ask for a "yes" or "no" response are separated from questions that ask for a narrative response. The drafting team considers each comment received irrespective of whether that comment accompanies a "yes" or "no" response to a particular question or is associated with an "affirmative" or "negative" ballot.

For each question that you provide a comment, please provide specific suggestions that would eliminate or minimize any concerns you have with the item in question. A comment or response to every question is not required.

VERY IMPORTANT:
Please note that the official comment form *does not* retain formatting (even if it appears to transfer formatting when you copy from the unofficial Word version of the form into the official electronic comment form). If you enter extra carriage returns, bullets, automated numbering, symbols, bolding, italics, or any other formatting, that formatting will not be retained when you submit your comments. Therefore, if you would like to separate portions of your comment by idea, e.g., the drafting team requests that each distinct idea in the same comment block be prefaced with (1), (2), etc., instead of using formatting such as extra carriage returns, bullets, automated numbering, bolding, or italics.

B. CIP-004, CIP-005, CIP-006 and CIP-007 Questions:

1. CIP-004-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

☐ Yes

☐ No

2. CIP-004-5 R2 states "Each Responsible Entity shall have a role-based cyber security training program to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

☐ Yes

☐ No

3. CIP-004-5 R3 states "Each Responsible Entity shall implement its documented role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R3 - Cyber Security Training.*" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

☐ Yes

☐ No

4. CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively includes each of the applicable items in *CIP-004-5 Table*

R4 – Personnel Risk Assessment Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4?

☐ Yes

☐ No

5. CIP-004-5 R5 states "Each Responsible Entity shall implement one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable elements in *CIP-004-5 Table R5 – Personnel Risk Assessment.*" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5?

☐ Yes

☐ No

6. CIP-004-5 R6 states "Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in *CIP-004-5 Table R6 – Access Management Program.*" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R6?

☐ Yes

☐ No

7. CIP-004-5 R7 states "Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R7?

☐ Yes

☐ No

8. CIP-004-5, **Requirement R1, R2, R3, R4 or R5** (NOTE: Requirements 6 and 7 are covered by next question): If you disagree with the changes made to CIP-004-5, Requirements R1, R2, R3, R4, or R5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments:

9. CIP-004-5, **Requirement R6 or R7**: If you disagree with the changes made to CIP-004-5, Requirements R6 or R7 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments:

10. CIP-005-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

- ☐ Yes
- ☐ No

11. CIP-005-5 R2 states "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

- ☐ Yes
- ☐ No

12. CIP-005-5, **Requirement R1** (NOTE: Requirement 2 is covered by the next question): If you disagree with the changes made to CIP-005-5, Requirement R1 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments:

13. CIP-005-5, **Requirement R2**: If you disagree with the changes made to CIP-005-5, Requirement R2 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments:

14. CIP-006-5 R1 states "Each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that collectively include all of

the applicable items in *CIP-006-5 Table R1 – Physical Security Plan*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

☐ Yes

☐ No

15. CIP-006-5 R2 states "Each Responsible Entity shall implement one or more documented visitor control programs that include each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program.*" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

☐ Yes

☐ No

16. CIP-006-5 R3 states "Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable items in *CIP-006-5 Table R3 – Maintenance and Testing Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

☐ Yes

☐ No

17. CIP-006-5: If you disagree with the changes made to CIP-006-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments:

18. CIP-007-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R1 – Ports and Services*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

☐ Yes

☐ No

19. CIP-007-5 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R2 – Security Patch*

Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

☐ Yes

☐ No

20. CIP-007-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R3 – Malicious Code Prevention*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

☐ Yes

☐ No

21. CIP-007-5 R4 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R4 – Security Event Monitoring*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4?

☐ Yes

☐ No

22. CIP-007-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R5 – System Access Controls*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5?

☐ Yes

☐ No

23.CIP-007-5, **Requirement R1, R2, R3, or R4** (NOTE: Requirement 5 is covered by the next question): If you disagree with the changes made to CIP-007-5, Requirement R1, R2, R3, or R4 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments:

24. CIP-007-5, **Requirement R5**: If you disagree with the changes made to CIP-007-5, Requirement R5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments:

Unofficial Comment Form

Request for Comments Regarding the Draft of CIP Cyber Security Standards Version 5

Comment Form C
CIP-008, CIP-009, CIP-010 and CIP-011

Please **DO NOT** use this form to submit comments. Please use the electronic comment form to submit comments on the second formal posting of Project 2008-06 – CSO706 Version 5 CIP Standards. The electronic comment form must be completed by **May 21, 2012.**

2008-06 Project Page

If you have questions please contact Steven Noess at steven.noess@nerc.net or 404-446-9691.

Background

The Project 2008-06 Standard Drafting Team (SDT) is seeking industry feedback and suggestions on this Version 5 of the CIP Cyber Security Standards and its Implementation Plan. The industry feedback will be considered by the SDT in revising and refining Version 5 and related documents.

The SDT thanks stakeholders and other commenters for the extensive and thoughtful comments received during the previous posting period. The volume and quality of the comments provided significant input into many of the changes the team made in response. The SDT also thanks the many observers who attended several comment resolution and discussion sessions—both electronically and face-to-face—that the SDT conducted to prepare the drafts that are currently posted.

The SDT expended considerable work in reviewing, discussing, and responding to all of these inputs, and it believes that the major issues from these inputs have been addressed responsively in this posted draft CIP Version 5 package. As a result, the changes have been significant and substantive in all of the draft CIP Version 5 standards and Implementation Plan.

- Many entities expressed concern over the expanded scope of these standards. The SDT has drafted these standards in response to directives from FERC Order No. 706, and believes that the changes in CIP Version 5 are necessary to address all of those directives responsively. The number of requirements in Version 5 is not substantively higher than previous versions.

- There are many substantive changes in the Applicability section of the standards in response to concerns regarding Distribution Providers and Load Serving Entities. The changes ensure that only those systems owned by those functional entities that are material to BES reliability are within the scope of these standards.

- The SDT also made several substantive changes in CIP-002-5 to address stakeholders' preference for a facilities-based approach to the identification and categorization process for BES Cyber Systems and BES Cyber Assets. In addition, in response to concerns to overall reliability in the restoration facilities area, the SDT made substantive changes to the categorization of those facilities. The SDT made several changes in response to comments in the "bright-line" criteria in Attachment 1 as well.

- In standards CIP-003-5 through CIP-011-1, the SDT made substantive changes in the applicability of requirements to the medium impact category in response to concerns of practical application in field assets. The SDT also addressed many of concerns on requirement clarity and language in the standards. In addition, the SDT moved all low impact requirements and grouped them as policy/program requirements in CIP-003 (Security Management). Requirements in CIP-004-CIP-011 only apply to high and medium impact systems.

- In response to comments, the SDT extended the Implementation Plan's effective date to 24 months after approval in most cases, with up to 36 months for implementation for low impact systems. In addition, the initial required performance of those requirements with periodicity is moved into the Implementation Plan and removed from the requirements in the standards, since the initial performances are one-time requirements tied to the effective date.

In summary, the SDT believes this posting package addresses all of the substantive issues received from the comments and various other inputs.

The Project 2008-06 – Cyber Security Order 706 SDT was appointed by the NERC Standards Committee on August 7, 2008 to review each of the CIP reliability standards and develop the modifications necessary to address the directives in the FERC Order No. 706. Please see the Project 2008-06 background document that accompanies the other posted material.

Instructions:

The SDT is providing this form for industry participants to offer their comments on draft 2 of Version 5 of the CIP Cyber Security Standards.

Questions that ask for a "yes" or "no" response are separated from questions that ask for a narrative response. The drafting team considers each comment received irrespective of whether that comment accompanies a "yes" or "no" response to a particular question or is associated with an "affirmative" or "negative" ballot.

For each question that you provide a comment, please provide specific suggestions that would eliminate or minimize any concerns you have with the item in question. A comment or response to every question is not required.

VERY IMPORTANT:
Please note that the official comment form *does not* retain formatting (even if it appears to transfer formatting when you copy from the unofficial Word version of the form into the official electronic comment form). If you enter extra carriage returns, bullets, automated numbering, symbols, bolding, italics, or any other formatting, that formatting will not be retained when you submit your comments. Therefore, if you would like to separate portions of your comment by idea, e.g., the drafting team requests that each distinct idea in the same comment block be prefaced with (1), (2), etc., instead of using formatting such as extra carriage returns, bullets, automated numbering, bolding, or italics.

C. CIP-008, CIP-009, CIP-010 and CIP-011 Questions:

1. CIP-008-5 R1 states "Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

☐ Yes

☐ No

2. CIP-008-5 R2 states "Each Responsible Entity shall implement its documented Cyber Security Incident response plan(s) to collectively include each of the applicable items in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.*" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

☐ Yes

☐ No

3. CIP-008-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

☐ Yes

☐ No

4. CIP-008-5: If you disagree with the changes made to CIP-008-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments:

5. CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

- ☐ Yes
- ☐ No

6. CIP-009-5 R2 states "Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

- ☐ Yes
- ☐ No

7. CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

- ☐ Yes
- ☐ No

8. CIP-009-5: If you disagree with the changes made to CIP-009-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments:

9. CIP-010-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

- ☐ Yes
- ☐ No

10. CIP-010-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring.*" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

- ☐ Yes
- ☐ No

11. CIP-010-1 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3– Vulnerability Assessments*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

- ☐ Yes
- ☐ No

12. CIP-010-1: If you disagree with the changes made to CIP-010-1 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments:

13. CIP-011-1 R1 states "Each Responsible Entity shall implement an information protection program that includes each of the applicable items in *CIP-011-1 Table R1 – Information Protection.*" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

- ☐ Yes
- ☐ No

14. CIP-011-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

- ☐ Yes
- ☐ No

15. CIP-011-1: If you disagree with the changes made to CIP-011-1 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments:

Unofficial Comment Form

Request for Comments Regarding the Draft of CIP Cyber Security Standards Version 5

Comment Form D
Definitions and Implementation Plans

Please **DO NOT** use this form to submit comments. Please use the electronic comment form to submit comments on the second formal posting of Project 2008-06 – CSO706 Version 5 CIP Standards. The electronic comment form must be completed by **May 21, 2012.**

2008-06 Project Page

If you have questions please contact Steven Noess at steven.noess@nerc.net or 404-446-9691.

Background

The Project 2008-06 Standard Drafting Team (SDT) is seeking industry feedback and suggestions on this Version 5 of the CIP Cyber Security Standards and its Implementation Plan. The industry feedback will be considered by the SDT in revising and refining Version 5 and related documents.

The SDT thanks stakeholders and other commenters for the extensive and thoughtful comments received during the previous posting period. The volume and quality of the comments provided significant input into many of the changes the team made in response. The SDT also thanks the many observers who attended several comment resolution and discussion sessions—both electronically and face-to-face—that the SDT conducted to prepare the drafts that are currently posted.

The SDT expended considerable work in reviewing, discussing, and responding to all of these inputs, and it believes that the major issues from these inputs have been addressed responsively in this posted draft CIP Version 5 package. As a result, the changes have been significant and substantive in all of the draft CIP Version 5 standards and Implementation Plan.

- Many entities expressed concern over the expanded scope of these standards. The SDT has drafted these standards in response to directives from FERC Order No. 706, and believes that the changes in CIP Version 5 are necessary to address all of those directives responsively. The number of requirements in Version 5 is not substantively higher than previous versions.

- There are many substantive changes in the Applicability section of the standards in response to concerns regarding Distribution Providers and Load Serving Entities. The changes ensure that only those systems owned by those functional entities that are material to BES reliability are within the scope of these standards.

- The SDT also made several substantive changes in CIP-002-5 to address stakeholders' preference for a facilities-based approach to the identification and categorization process for BES Cyber Systems and BES Cyber Assets. In addition, in response to concerns to overall reliability in the restoration facilities area, the SDT made substantive changes to the categorization of those facilities. The SDT made several changes in response to comments in the "bright-line" criteria in Attachment 1 as well.

- In standards CIP-003-5 through CIP-011-1, the SDT made substantive changes in the applicability of requirements to the medium impact category in response to concerns of practical application in field assets. The SDT also addressed many of concerns on requirement clarity and language in the standards. In addition, the SDT moved all low impact requirements and grouped them as policy/program requirements in CIP-003 (Security Management). Requirements in CIP-004-CIP-011 only apply to high and medium impact systems.

- In response to comments, the SDT extended the Implementation Plan's effective date to 24 months after approval in most cases, with up to 36 months for implementation for low impact systems. In addition, the initial required performance of those requirements with periodicity is moved into the Implementation Plan and removed from the requirements in the standards, since the initial performances are one-time requirements tied to the effective date.

In summary, the SDT believes this posting package addresses all of the substantive issues received from the comments and various other inputs.

The Project 2008-06 – Cyber Security Order 706 SDT was appointed by the NERC Standards Committee on August 7, 2008 to review each of the CIP reliability standards and develop the modifications necessary to address the directives in the FERC Order No. 706. Please see the Project 2008-06 background document that accompanies the other posted material.

Instructions:

The SDT is providing this form for industry participants to offer their comments on draft 2 of Version 5 of the CIP Cyber Security Standards.

Questions that ask for a "yes" or "no" response are separated from questions that ask for a narrative response. The drafting team considers each comment received irrespective of whether that comment accompanies a "yes" or "no" response to a particular question or is associated with an "affirmative" or "negative" ballot.

For each question that you provide a comment, please provide specific suggestions that would eliminate or minimize any concerns you have with the item in question. A comment or response to every question is not required.

VERY IMPORTANT:
Please note that the official comment form *does not* retain formatting (even if it appears to transfer formatting when you copy from the unofficial Word version of the form into the official electronic comment form). If you enter extra carriage returns, bullets, automated numbering, symbols, bolding, italics, or any other formatting, that formatting will not be retained when you submit your comments. Therefore, if you would like to separate portions of your comment by idea, e.g., the drafting team requests that each distinct idea in the same comment block be prefaced with (1), (2), etc., instead of using formatting such as extra carriage returns, bullets, automated numbering, bolding, or italics.

D. Definitions and Implementation Plan Questions:

1. Do you agree with the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset?

   ☐ Yes

   ☐ No

2. Do you agree with the proposed definition of Control Center?

   ☐ Yes

   ☐ No

3. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager?

   ☐ Yes

   ☐ No

4. Do you agree with the proposed definitions of Physical Access Control Systems and Physical Security Perimeter?

   ☐ Yes

   ☐ No

5. Do you agree with the proposed definitions of Electronic Access Control or Monitoring Systems, Interactive Remote Access, and Intermediate Device?

   ☐ Yes

   ☐ No

6. Do you agree with the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset?

☐ Yes

☐ No

7. Do you agree with the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident?

☐ Yes

☐ No

8. Definitions: Do you have any comments on the changes to the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

Comments:

9. Definitions: Do you have any comments on the changes to the proposed definition of Control Center? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

Comments:

10. Definitions: Do you have any comments on the changes to the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

Comments:

11. Definitions: Do you have any comments on the changes to the proposed definitions of Physical Access Control Systems and Physical Security Perimeter? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

Comments:

12. Definitions: Do you have any comments on the changes to the proposed definitions of Electronic Access Control and Monitoring Systems, Interactive Remote Access, and Intermediate Device? If you

voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

Comments:

13. Definitions: Do you have any comments on the changes to the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

Comments:

14. Definitions: Do you have any comments on the changes to the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

Comments:

15. Do you agree with the changes made to the proposed implementation plan since the last formal comment period?

- ☐ Yes
- ☐ No

16. Implementation Plan: If you disagree with the changes made to the Implementation Plan since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments:

17. If you have comments or specific suggestions **that you have not been able to provide in response to the previous questions**, please provide those comments here. Please provide specific suggestions or proposals for any alternative language.

Comments:

Project 2008-06 - Cyber Security Order 706 - Version 5

Working Draft (April 10, 2012) of Mapping Document Showing Translation of CIP-002-4 to CIP-009-4 into CIP-002-5 to CIP-009-5, CIP-010-1, and CIP-011-1.

Standard: CIP-002-4 – Cyber Security—Critical Asset Identification		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-002-4 R1.	CIP-002-5 R1.1	Critical Asset Identification – Instead of identifying Critical Assets as in previous versions, the Responsible Entity must Identify Facilities, Systems, or equipment that meet the criteria specified in CIP-002-5, Attachment 1.
CIP-002-4 R2.	CIP-002-5 R1.2, R1.3	Critical Cyber Asset Identification – Using the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 Impact Rating Criteria, the Responsible Entity must identify and categorize its BES Cyber Systems as high impact or medium impact. BES Cyber Systems not identified as high impact or medium impact default to low impact. New Standard identifies BES Cyber Systems as a grouping of BES Cyber Assets because it allows entities to apply some requirements at a system rather than asset level.
CIP-002-4 R2.	DELETED	Routable protocol exemption – A complete exemption of Cyber Assets based on communication characteristics no longer applies. This is because the vulnerability some security requirements address is not mitigated by the lack of routable protocols (e.g., training, response, recovery, etc.) Where the lack of routable protocols itself meets the requirement objective, the exemption is applied at the requirement level.

Standard: CIP-002-4 – Cyber Security—Critical Asset Identification		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-002-4 R3.	CIP-002-5 R2	Annual Approval – No significant changes to the approval. However, the CIP Sr. Manager now approves identifications required in CIP-002-5 R1 as noted above.
NEW	CIP-002-5 1.4	Update and re-categorize for changes to BES – Specifies time frame for complying with all re-categorization of items identified in CIP 002-5 R1 following a change, which is planned to be in service for more than six calendar months.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R1.	CIP-003-5 R1, 1.1 through 1.9	Cyber Security Policy – Includes high impact and medium impact BES Cyber Systems. A separate requirement applies to low impact BES Cyber Systems. Clarified that the cyber security policy needs to only reference the subject matter topics at a high level rather than each individual requirement in the CIP Cyber Security Standards.
CIP-003-4 R1.1.	CIP-003-5 R1, 1.10	Provision for emergency situations – Identified the specific exceptional circumstances in which emergency exceptions can be taken in response to the directive in FERC Order No. 706, Paragraph 443.
NEW	CIP-003-5 R2	Cyber Security Policy for BES Cyber Systems not identified as high or medium impact (low impact). Clarified programmatic controls that apply to low impact BES Cyber Systems and that discrete identification of such systems is not required.
CIP-003-4 R1.2.	DELETED	The Cyber Security Policy is readily available –This was in response to general confusion around the term “readily available.” Training requirements in CIP-004-5 provide for knowledge of policy.
CIP-003-4 R1.3.	CIP-003-5 R4	Annual review and approval – No significant change.
CIP-003-4 R2.	CIP-003-5 R3	Single senior manager – Created a definition of CIP Senior Manager to facilitate references across standards.
CIP-003-4 R2.1.	CIP-003-5 R3	The CIP Senior Manager shall be identified by name, title, and date of designation – The CIP Senior Manager only needs to be identified by name. The other details were considered unnecessary, administrative requirements.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R2.2.	CIP-003-5 R6	Changes to the CIP Senior Manager and any delegations must be documented within 30 calendar days of the change.
CIP-003-4 R2.3.	CIP-003-5 R5	Delegate authority – Made clear that where allowed by the standards, the CIP Senior Manager may delegate authority and such delegations must be documented.
CIP-003-4 R2.4.	DELETED	Authorize and document any exception – The FERC Order No. 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the standards.
CIP-003-4 R3.	DELETED	Exceptions – The FERC Order No. 706 made clear that you could not take exceptions to areas of your Cyber Security Policy that were also required as part of other NERC CIP requirements. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the standards.
CIP-003-4 R3.1.	DELETED	Exceptions - Requirement R3 is deleted.
CIP-003-4 R3.2.	DELETED	Exceptions - Requirement R3 is deleted.
CIP-003-4 R3.3.	DELETED	Exceptions - Requirement R3 is deleted.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R4.	CIP-011-1 R1, 1.1, 1.2	Information Protection - Removed language to "protect" information, and replaced with requirements for methods to identify BES Cyber System Information and procedures for handling BES Cyber System Information, including storage, transit, and use to clarify the protection that is required.
CIP-003-4 R4.1.	Definition	Identification – Replaced this requirement with the defined term BES Cyber System Information.
CIP-003-4 R4.2.	CIP-011-5 R1.1	Classification – Removed the explicit requirement for classification, as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.
CIP-003-4 R4.3.	CIP-011-5 R1.3	Assessment – No significant changes.
CIP-003-4 R5.	CIP-004-5 R6.4,	Authorize personnel for access to protected information – Clarified: "Program for managing access" included the authorization of access, as well as handling and access control procedures. Grouped requirements for electronic access, physical access, and access to BES Cyber System Information in CIP 004-5 R6.
CIP-003-4 R5.1.	CIP-004-5 R6.1	Authorizing personnel.
CIP-003-4 R5.1.1.	CIP-004-5 R6.1	Personnel shall be identified.
CIP-003-4 R5.1.2.	CIP-004-5 R6.7	Verification.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R5.2.	CIP-004-5 R6.7	Verify access privileges annually – Moved requirement to ensure consistency among access reviews. Clarified precise meaning in the term "annual". Clarified what was necessary in performing verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.
CIP-003-4 R5.3.	CIP-011-1 1.3	Annual Review – No significant changes.
CIP-003-4 R6.	CIP-010-1 R1, R2	Change Control and Configuration Management – Moved configuration change management to a separate standard because of the additional requirements necessary for satisfying FERC directives, and the subject matter in CIP version 4 is spread across CIP-003-4 and CIP-007-4. The baseline requirement is incorporated from the *DHS Catalog for Control Systems Security*. The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed. Added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-4 R6.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R1.	CIP-004-5 R1, 1.1	Security awareness program and quarterly reinforcement - Changed to remove the need to ensure everyone with authorized access receive this material, and moved example mechanisms to Guidance.
CIP-004-4 R2.	CIP-004-5 R2, R3	Training - Addition of identifying the roles that require training. Adding specific role-based training for the visitor control program and storage media as part of the handling of BES Cyber Systems information. Also added the FERC Order No. 706, directed electronic interconnectivity supporting the operation and control of BES Cyber Systems. This requirement is also reorganized into the respective requirements for "program" and "implementation" of the training.
CIP-004-4 R2.1.	CIP-004-5 R3.1	Training prior to authorized access – No significant changes.
CIP-004-4 R2.2.	CIP-004-5 R2.1-2.10	Training subject matter – This requirement is reorganized into the respective requirements for "program" and "implementation" of the training.
CIP-004-4 R2.2.1.	CIP-004-5 R2.2	Proper use of CCAs – Changed to refer to BES Cyber Systems. Requirement now addresses cyber security issues, not the business or functional use of the BES Cyber System.
CIP-004-4 R2.2.2.	CIP-004-5 R2.3,2.4	Physical and electronic access controls training – No significant changes. Refers to BES Cyber Systems.
CIP-004-4 R2.2.3.	CIP-004-5 R2.6	Information handling training – Core training added for the handling of BES Cyber System Information, with the addition of storage media.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R2.2.4.	CIP-004-5 R2.7,2.8,2.9	Incident identification and notification, incident handling and CCA recovery training – Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for individuals having a role in the recovery to address FERC Order No. 706, Paragraph 413.
CIP-004-4 R2.3.	CIP-004-5 R3.2	Annual training – Replaced "Annually" with "calendar year, not to exceed 15 months."
CIP-004-4 R3.	CIP-004-5 R4, R5, 5.1	Personnel Risk Assessment – Split into two requirements, R4 to define the PRA program, and R5 to implement the program for individuals prior to obtaining authorized access.
CIP-004-4 R3.1.	CIP-004-5 4R.1, 4.2	Identification and 7-year criminal check – Addressed interpretation request in Guidance. Specified that identity verification is only required for each individual's initial assessment. Specified that the 7-year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for 6 months or more, including current residence, regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full 7-year check cannot be performed.
CIP-004-4 R3.2.	CIP-004-5 R5.2	Perform the PRA every 7 years– Removed the "for cause" part of the requirement.
CIP-004-4 R3.3.	CIP-004-5 R4.4	Addresses the contractor or vendor performed PRA.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R4.	CIP-004-5 R6.2, 6.3	Authorize access - CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need-to-know" basis, or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.
CIP-004-4 R4.1.	CIP-004-5 R6.5	Quarterly review of access – Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4 R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.
CIP-004-4 R4.2.	CIP-004-5 R7	Prevent further access - The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the standards to require immediate revocation for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination, instead of within 24 hours. For transfers, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53, Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.
NEW	CIP-004-5 R2.1	Added to help facilitate understanding what roles the entity has to support the role-based training program.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-004-5 R2.5	Visitor control program training – Personnel administering the visitor control program and/or providing escort should be part of the core training per FERC Order No. 706, Paragraph 432.
NEW	CIP-004-5 R2.10	Electronic interconnectivity training – Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems per FERC Order No. 706 - Paragraph 434.
NEW	CIP-004-5 R4.3	PRA failure criteria – Requires process or criteria to evaluate personnel risk assessments to determine when to deny authorized access.
NEW	CIP-004-5 R7.2	Transfers – The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53, Version 3, to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-004-5 R7.4	Completion of revocation – The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the standards to require immediate revocation for any person no longer needing access. In order to meet the immediate time frame, entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
NEW	CIP-004-5 R7.5	Completion of revocation (shared accounts) – To provide clarification of expected actions in managing the passwords

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R1.	CIP-005-5 R1.1	Electronic Security Perimeter identification – Changes include referencing the defined terms Electronic Access Point and BES Cyber System.
CIP-005-4a R1.1.	Definition	Access Points – This was moved to the definition of Electronic Access Points.
CIP-005-4a R1.2.	Guidance	Dial-up accessible CCA – This is a clarifying statement that was moved to Guidance.
CIP-005-4a R1.3.	Guidance	Communication links between ESPs – This is a clarifying statement that was moved to Guidance.
CIP-005-4a R1.4.	Applicability	Applicability for Non-Critical Cyber Asset – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.5.	Applicability	Access control and monitoring Cyber Assets – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.6.	Measures	Maintain Documentation – This is a measure for the requirement to have ESP documentation.
CIP-005-4a R2.	CIP-005-5 R1	Electronic Access Controls – No significant changes.
CIP-005-4a R2.1.	CIP-005-5 R1.2, 1.3	Deny access by default - Changes include referring to the defined term Electronic Access Point, and to focus on the entity knowing and having justification for what it allows through the EAP. R1.3 explicitly states the network admission control includes both inbound and outbound connections.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R2.2.	CIP-007-5 R1.1, 1.2	Enable specific ports/services – Consolidated port hardening requirements to CIP-007.
CIP-005-4a R2.3.	CIP-005-5 R1.4	Secure dial-up – Changed to refer to the defined term Electronic Access Point. Added clarification as to the goal of "secure," which is that the BES Cyber System should not be directly accessible with a phone number only.
CIP-005-4a R2.4.	CIP-005-5 R2,2.3	Strong access control – Added a new requirement for remote access in response to increased vulnerabilities in VPN technology. This requirement also clarified strong access control meant two-factor (or more) authentication.
CIP-005-4a R2.5.	Measures	Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.1.	CIP-004-5 R6	The processes for access request and authorization – Consolidated with other similar requirements to CIP-004-5 R6.
CIP-005-4a R2.5.2.	Measures	The authentication methods - Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.3.	Measures	The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4. Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.4.	Measures	The controls used to secure dial-up accessible connections. Evidence requirements are considered as part of the measure.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R2.6.	DELETED	Appropriate Use Banner – The drafting team considered this requirement administrative. The objective of having an appropriate use banner is to prevent accidental use of the system and help allow prosecution of unauthorized individuals accessing the system. The drafting team did not consider either of these rising to the level of meeting a reliability objective.
CIP-005-4a R3.	CIP-007-5 R4, 4.1	Monitoring Electronic Access – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the standards.
CIP-005-4a R3.1.	CIP-007-5 R4, 4.1	Dial-up Accessible – Removed specific references to dial-up devices. Incorporated into logging/monitoring requirements. The drafting team did not feel further referencing this technology was necessary.
CIP-005-4a R3.2.	CIP-007-5, R4, 4.2	Alerts – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the standards.
CIP-005-4a R4.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements.
CIP-005-4a R4.1.	Measures	A document identifying the vulnerability assessment process - Evidence requirements are considered as part of the measure.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R4.2.	CIP-010-1 R3.1, 3.2	A review to verify that only ports and services required for operations at these access points are enabled - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to Guidance.
CIP-005-4a R4.3.	CIP-010-1 R3.1, 3.2	The discovery of all access points to the Electronic Security Perimeter - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to Guidance.
CIP-005-4a R4.4.	CIP-010-1 R3.1, 3.2	A review of controls for default accounts, passwords, and network management community strings - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to Guidance.
CIP-005-4a R4.5.	CIP-010-1 R3.4	Mitigation plan - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. Added element to have an entity defined date of completion of the mitigation plan per FERC Order No. 706, Paragraph 643.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R5.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.1.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.2.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.3.	CIP-007-5 R4.4	Retain relevant log information – Log retention requirements are consolidated to CIP-007-5 R4.
NEW	CIP-005-5 R1.5	Inspect and detect potential malicious communications – Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The order makes clear this is not simple redundancy of firewalls; thus the drafting team has decided to add the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs.
NEW	CIP-005-5 R2.1,2.2	Remote Access: intermediate device and encryption – This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R1.	CIP-006-5 R1	Physical Security Plan – Removed the requirement for senior management approval of the physical security plan because there is already approval of the physical security policy and delegation of the task in complying for this program. Additional approval is not considered necessary to meeting the reliability objective of physical security for the BES Cyber System.
CIP-006-4c R1.1.	CIP-006-5 R1.2, 1.3	Physical Security Perimeter – For high impact BES Cyber Systems clarified that two or more different physical access controls must be used to collectively allow physical access into Physical Security Perimeters.
CIP-006-4c R1.2.	DELETED	No longer requires identification of all physical access points.
CIP-006-4c R1.3.	CIP-006-5 R1.4, 1.5	Monitor physical access – A documented plan is required as part of CIP-006-5 R1 that references the new alerting term in Table Row 1.5. Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.
CIP-006-4c R1.4.	CIP-004-5 R2.3	Appropriate use of access controls – The term “appropriate” used in prior versions is subject to a high degree of subjectivity. The training requirement specifies role-based training on physical access controls.
CIP-006-4c R1.5.	CIP-004-5 R6 and R7	Review of access authorization requests and revocation of access authorization requirements were consolidated to CIP-004-5.
CIP-006-4c R1.6.	CIP-006-5 R2	Visitor control program - A documented program is required as part of CIP-006-5 R2. Otherwise, no significant change.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R1.6.1.	CIP-006-5 R2.2	Log entry and exit of visitors - Addressed multi entry requirements and added the point of contact of who can be considered the sponsor for the person to enter the DPB. There is no need to document the escort or handoffs between escorts.
CIP-006-4c R1.6.2.	CIP-006-5 R2.1	Continuous escorted access of visitors – No significant change.
CIP-006-4c R1.7.	DELETED	Update of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R1.8.	DELETED	Annual review of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R2.	Applicability	Protection of Physical Access Control Systems – Applicability to Physical Access Control and Monitoring Systems were moved to the Applicability section of each security requirement, and added this as a defined term in the glossary.
CIP-006-4c R2.1.	Applicability, CIP-006-5 R1.1	Physical Access Control Systems be protected from unauthorized physical access - Applicability to Physical Access Control Systems were moved to the Applicability section of each security requirement. For this particular requirement, see CIP-006-5, Item 1.1, which applies to Physical Access Control Systems.
CIP-006-4c R2.2.	CIP-006-5 R1.6, 1.7	Protection of Physical Access Control Systems - Applicability to Physical Access Control Systems were moved to the Applicability section of each security requirement throughout CP version 5.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R3.	Applicability	Protection of Electronic Access Control Systems - Applicability to what protections Electronic Access Control and Monitoring Systems need were moved to the Applicability section of each security requirement.
CIP-006-4c R4.	CIP-006-5 R1.2, 1.3	Physical Access Controls – R1.3 addresses FERC Order No. 706 Paragraph 572 related directives for physical security defense in depth by providing the examples in the guidance document of physical security defense in depth via multifactor authentication or layered Physical Security Perimeter(s).
CIP-006-4c R5.	CIP-006-5 R1.4, 1.5, 1.6, 1.7	Monitor physical access – Changed the term to alert for unauthorized access and clarified the actions taken for review of unauthorized physical access alerts. Examples of methods to implement have been moved to the Guidance section of this requirement.
CIP-006-4c R6.	CIP-006-5 R1.8,	Log physical access – CIP-006-4 R6 was specific to the logging of access at identified access points. This now more generally requires logging of physical access into the defined physical boundary. Examples of methods to implement have been moved to the Guidance section of this requirement.
CIP-006-4c R7.	CIP-006-5 R1.9 and CIP-008-5 Evidence Retention	Access log retention - Retain relevant incident related log information is addressed in CIP-008-5.
CIP-006-4c R8.	CIP-006-5 R3	Maintenance and Testing.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R8.1.	CIP-006-5 R3.1	Physical access control system three-year testing and maintenance – Shortened periodicity of testing to 2 years to address FERC Order No. 706, Paragraph 581 directives. Added testing of locally mounted security hardware devices.
CIP-006-4c R8.2.	REMOVED	Testing and maintenance records are considered the measurement of Item 3.1.
CIP-006-4c R8.3.	CIP-006-5 R3.2	Retain outage records – No significant changes.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R1.	CIP-010-1 R1.4	Assess security controls following changes - Provides clarity on when testing must occur, and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.
CIP-007-4 R1.1.	CIP-010-1 R1.5	Test procedures – This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.
CIP-007-4 R1.2.	CIP-010-1 R1.5	Testing reflects production environment - This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.
CIP-007-4 R1.3.	CIP-010-1 R1.4, 1.5	The Responsible Entity shall document test results. The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.
CIP-007-4 R2.	CIP-007-5 R1	Ports and Services – The requirement focuses on the entity knowing, and only allowing those ports that are necessary. The additional classification of “normal” or “emergency” added no value and has been removed.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R2.1.	CIP-007-5 R1.1	Enable only those ports and services required for normal and emergency operations – See description and justification for CIP-007-4 R2.
CIP-007-4 R2.2.	CIP-007-5 R1.1, 1.2	Disable other ports/services – See description and justification for CIP-007-4 R2.
CIP-007-4 R2.3.	DELETED	Compensating measures – See description and justification for CIP-007-4 R2.
CIP-007-4 R3.	CIP-007-5 R2	Security Patch Management – The existing wording, or CIP-007-4 R3, R3.1 and R3.2 was separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "Document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades." There has been confusion as to what constitutes the availability. Due to issues that may occur regarding control system vendor license and service agreements flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R3.1.	CIP-007-5 R2.2	Assess patches – Similar to the current wording, but added reference to "identification of a source or sources that the Responsible Entity tracks" to establish where the release is from. The word in previous versions: "The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades," has led to varying opinions as to what constitutes "availability" of the patches or upgrades. The addition attempts to clarify where the release is from.
CIP-007-4 R3.2.	CIP-007-5 R2.3, 2.4	Implement patches - This is the same concept as in the current CIP-007 R3.2 wording; however, a 30-day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used. Splitting the implementation of security related patches, hot fixes, and/or updates into a separate item from compensating measures will provide granularity. Automated processes allow the implementation to be documented and confirmed electronically in a short time period. Manual processes may take an extended period of time to complete documentation of the installation. Priority should be given to the implementation rather than the documentation.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R4.	CIP-007-5 R3, 3.1, 3.2, 3.3	Malicious Software Prevention – In prior versions, this requirement has arguably been the single greatest generator of TFE's as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method, nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a Responsible Entity does this should be detailed in its Cyber Security Policy so that it can be audited for compliance…" In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level, and regardless of technology, along with the enhanced change management requirements, meets this directive.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R4.1.	CIP-007-5 R3.1	Malware prevention tools – See description and justification for CIP-007-4 R3.
CIP-007-4 R4.2.	CIP-007-5 R3.2, 3.3	Update malicious code detections – See description and justification for CIP-007-4 R3.
CIP-007-4 R5.	CIP-007-5 R5.1	Use at least one authentication method – The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase, "that minimize the risk of unauthorized access," was removed and more appropriately captured in the Rationale Statement.
CIP-007-4 R5.1.	CIP-004-5 R6.1, 6.2	Access authorization – CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need-to-know" basis, or with respect to work functions performed. These were consolidated in CIP-004-5 R6.1 and 6.2 to ensure consistency in the requirement language.
CIP-007-4 R5.1.1.	CIP-003-5 R5.2	Access authorization – CIP-003-5 R5.2 requires CIP Senior Manager or delegate approval for all requirements for authorization in the CIP Cyber Security Standards.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R5.1.2.	CIP-007-5 R4.1	Identify security events for after-the-fact investigation – This requirement is derived from NIST 800-53, Version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the phrase, "system events related to cyber security," from informal comments received. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP, as required in CIP-005-4 R3, and user access and activity logs, as required in CIP-007-5 R5, are also included here.
CIP-007-4 R5.1.3.	CIP-004-5 R6.6	Annual account privilege verification – Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.
CIP-007-4 R5.2.	CIP-007-5 R5.2	Identify account types and determine acceptable use – CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure, at best.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R5.2.1.	CIP-007-5 R5.4	Change default vendor passwords – The requirement for the "removal, disabling, or renaming of such accounts where possible," has been removed and incorporated into Guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded, uniquely generated default password was manufactured with the BES Cyber System.
CIP-007-4 R5.2.2.	CIP-007-5 R5.3	Identify those individuals with access to shared accounts - No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.
CIP-007-4 R5.2.3.	CIP-007-5 R5.2, 5.3	Identify account types and determine acceptable use – No significant changes.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R5.3.	CIP-007-5 R5.5	Implement a password policy – CIP-007-4 R5.3 requires the use of passwords, and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials, while recognizing password parameters alone do not achieve this. The drafting team believes allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.
CIP-007-4 R5.3.1.	CIP-007-5 R5.5	Password length – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.2.	CIP-007-5 R5.5	Password complexity – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.3.	CIP-007-5 R5.5, 5.6	Password change frequency – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R6.	CIP-007-5 R4	Security Status Monitoring – Consolidated requirements for monitoring electronic events into CIP-007-5 R4.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R6.1.	CIP-007-5 R4.1	Identify security events – This requirement is derived from NIST 800-53, Version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the phrase, "system events related to cyber security" from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP, as required in CIP-005-4 R3, and user access and activity logs, as required in CIP-007-5 R5, are also included here.
CIP-007-4 R6.2.	CIP-007-5 R4.2	Identify security events for Real-time alerting – This requirement is derived from alerting requirements in CIP-005-4 R3.2 and CIP-007-4 R6.2, in addition to NIST 800-53, Version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.
CIP-007-4 R6.3.	CIP-007-5 R4.1	Identify security events for after-the-fact investigation – See description and justification for CIP-007-4 R6.1.
CIP-007-4 R6.4.	CIP-007-5 R4.4	Retain relevant log information – No significant changes.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R6.5.	CIP-007-5 R4.5	Review logs – Beginning in Paragraph 525, and also Paragraph 628 of the FERC Order No. 706, the commission directs a manual review of security event logs on a more periodic basis, and suggests a weekly review. The order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.
CIP-007-4 R7.	CIP-011-1 R2.1	Disposal or Redeployment – Consistent with FERC Order No. 706, Paragraph 631, clarified that the goal was to prevent the unauthorized retrieval of information from the asset, removing the word “erase” as, depending on the media itself, erasure may not be sufficient to meet this goal. Moved requirement explicitly requiring records of destruction/redeployment to a measure of compliance. Added requirement for chain of custody if the device is taken outside the Physical Security Perimeter.
CIP-007-4 R7.1.	CIP-011-1 R2.2	Disposal - Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the asset, removing the word “erase” since, depending on the media itself, erasure may not be sufficient to meet this goal. Moved requirement explicitly requiring records of destruction/redeployment, to a measure of compliance. Added requirement for chain of custody if the device is taken outside the Physical Security Perimeter.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R7.2.	CIP-011-1 R2.1	Redeployment – See description and justification for CIP-007-4 R7.
CIP-007-4 R7.3.	Measures	See description and justification for CIP-007-4 R7.
CIP-007-4 R8.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated requirements for vulnerability assessments from CIP-005-4 and CIP-007-4.
CIP-007-4 R8.1.	Measures	A document identifying the vulnerability assessment process – This is example evidence required for compliance.
CIP-007-4 R8.2.	CIP-010-1 R3.1, 3.2	Ports and services review – As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are included in Guidance.
CIP-007-4 R8.3.	CIP-010-1 R3.1, 3.2	A review of controls for default accounts – As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are included in Guidance.
CIP-007-4 R8.4.	CIP-010-1 R3.4	Mitigation plan – Added a requirement for an entity planned date of completion as per the FERC directive in Order No. 706, Paragraph 643.
CIP-007-4 R9.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
NEW	CIP-007-5 R1.2	Restrict physical I/O ports – In March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g., TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-007-5 R2.1	Identify patch sources – Defining the source(s) that a Responsible Entity monitors for the release of security related patches, hot fixes, and/or updates will provide a starting point for assessing the effectiveness of the patch management program. Documenting the source is also used to determine when the assessment time frame clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.
NEW	CIP-007-5 R4.3	Generate Real-time alerts and respond to audit-processing failures – This requirement was derived from NIST 800-53, Version 3 AU-5, which addresses response to audit processing failures. Some interpretations of version 4 CIP Cyber Security Standards considered the failure of the security event monitoring and alerting system to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.
NEW	CIP-007-5 R5.7	Limits or alerts on exceeding unsuccessful log in attempts threshold – Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-008-4 R1.	CIP-008-5 R1	Cyber Security Incident Response Plan – Separated requirement into multiple requirements in a comparable manner as CIP-009-4, where individual aspects of maintaining the plan are listed as separate requirements.
CIP-008-4 R1.1.	CIP-008-5 R1.1, 1.2	Identify reportable cyber security events – Defined the term Reportable Cyber Security Incident and further described the meaning in relation to CIP-008-5. "Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity. EOP-004-2 will address the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents.
CIP-008-4 R1.2.	CIP-008-5 R1.3, 1.4, 1.5	Roles and responsibilities of incident response teams –Replaced "incident response teams" with "incident response groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams. Conforming change to reference new defined term Cyber Security Incidents. Clarified the term "communication plan" by specifying the elements that need to be included.
CIP-008-4 R1.3.	DELETED	Reporting cyber security incidents – Coordinated with EOP-004-2 drafting team to ensure EOP-004-2 becomes the single standard for reporting incidents, and ensure EOP-004-2 references the defined term Reportable Cyber Security Incidents.

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-008-4 R1.4.	CIP-008-5 R3.3, 3.4	Update incident response plan following review – Included additional specification on update of response plan. Addresses FERC Order No. 706, Paragraph 686 directive to modify on lessons learned. Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.
CIP-008-4 R1.5.	CIP-008-5 R3.1, 3.3	Review incident response plans annually – Specified what the annual review entails. Addresses FERC Order No. 706, Paragraph 686 to document test, or actual incidents and lessons learned.
CIP-008-4 R1.6.	CIP-008-5 R2.1, 2.2	Test incident response plans annually – Allows deviation from plan(s) during actual events or testing if deviations are recorded for review, and specifies activities required to maintain the plan.
CIP-008-4 R2.	CIP-008-5 R2.3	Cyber Security Incident Documentation –Removed references to the retention period because the standard addresses data retention in the Compliance section.
NEW	CIP-008-5 R3.2	Document any lessons learned - Addresses FERC Order No. 706, Paragraph 686 to document test or actual incidents and lessons learned.
NEW	CIP-008-5 R3.5	Communicate incident response plan updates – Added specific timing requirement on communication of plan changes based on review of the DHS Controls and NIST 800-53 guideline.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-4 R1.	CIP-009-5 R1, 3.1, 3.3	Recovery Plan – Added requirement for documentation of any identified deficiencies or lessons learned. Added the requirement to additionally review plans after technology changes.
CIP-009-4 R1.1.	CIP-009-5 R1.1	Conditions for activation of recovery plan – Minor wording changes, essentially unchanged.
CIP-009-4 R1.2.	CIP-009-5 R1.2	Roles and responsibilities of recovery plan responders – No significant changes.
CIP-009-4 R2.	CIP-009-5 R2.1	Test recovery plan annually – No significant changes.
CIP-009-4 R3.	CIP-009-5 R3.2	Review results of recovery plan activities (tests, events) – Added the time frame for update.
CIP-009-4 R4.	CIP-009-5 R1.3	Backup processes – No significant changes.
CIP-009-4 R5.	CIP-009-5 R2.2	Test information used for recovery – Combined requirement from CIP-009-4 R5 and included requirement to test when initially stored. Addresses FERC Order No. 706, Directives 739 and 748 related to testing of backups.
NEW	CIP-009-5 R1.4	Testing of backup media – Addresses FERC Order No. 706, Paragraph 739 and 748 directives regarding the testing of backup media.
NEW	CIP-009-5 R1.5	Process to preserve data for analysis – Added requirement to address FERC Order No. 706, Paragraph 706, regarding the necessity to have procedures in place to retain Cyber Asset evidence as part of the recovery planning.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-009-5 R2.3	Test each of the recovery plans for high impact BES Cyber Systems at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. Addresses FERC Order No. 706, Paragraph 725, to add the requirement that the recovery plan test be a full operational test once every 3 years.
NEW	CIP-009-5 R3.4	Communicate recovery plan updates – This change ensures that recovery personnel are aware of any changes to recovery plans.
Standard: New Requirements in CIP-010-1 and CIP-011-1		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-1 R1.1	Baseline configuration – Baseline requirement incorporated from the DHS Catalog for Control Systems Security (also NIST 800-53). The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-1 R2.1	The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes. This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397. DHS Catalog & addresses FERC Order No. 706, Paragraph 397. Thirty-five calendar days allows for a “once-a-month” frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.
NEW	CIP-010-1 R3.2	Live Vulnerability Assessment for high impact BES Cyber Systems – Addresses FERC Order No. 706, Paragraph 541, 542, 544, and 547 directives regarding the performance of a live vulnerability assessment.
NEW	CIP-010-1 R3.3	Perform active VA on new BES Cyber Assets for high impact - Addresses FERC Order No. 706, Paragraph 541, 542, 544, and 547 directives regarding the performance of a vulnerability assessment prior to placing a new Cyber Asset into production.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2008-06 - Cyber Security Order 706 - Version 5

Working Draft (April 10, 2012) of Mapping Document Showing Translation of CIP-002-4 to CIP-009-4 into CIP-002-5 to CIP-009-5, CIP-010-1, and CIP-011-1.

Standard: CIP-002-4 – Cyber Security—Critical Asset Identification		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-002-4 R1.	~~DELETED~~ CIP-002-5 R1.1	Critical Asset Identification – ~~Removed this requirement because new Standard identifies and categorizes BES Cyber~~Instead of identifying Critical Assets as in previous versions, the Responsible Entity must Identify Facilities, Systems ~~directly without declaring assets as critical~~, or equipment that meet the criteria specified in CIP-002-5, Attachment 1.
CIP-002-4 R2.	CIP-002-5 R1.2, R1.3	Critical Cyber Asset Identification – Using the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 Impact Rating Criteria, the Responsible Entity must identify and categorize its BES Cyber Systems as high impact or medium impact. BES Cyber Systems not identified as high impact or medium impact default to low impact. New Standard identifies BES Cyber Systems as a grouping of ~~Critical~~BES Cyber Assets because it allows entities to apply some requirements at a system rather than asset level. ~~BES Cyber Systems are also identified using BES Reliability Operating Services, which provides more detail on what it means for a Cyber Asset to be critical to reliable operation.~~

Standard: CIP-002-4 – Cyber Security—Critical Asset Identification		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-002-4 R2.	DELETED	Routable protocol exemption – A complete exemption ~~or cyber assets~~of Cyber Assets based on communication characteristics no longer applies. This is because the vulnerability some security requirements address is not mitigated by the lack of routable protocols (e.g~~.~~., training, response, recovery, etc~~.).~~.) Where the lack of routable protocols itself meets the requirement objective, the exemption is applied at the requirement level.
~~CIP-002-4 R2.~~	~~DELETED~~	~~Control Center – No longer applicable since R2 has been deleted.~~
~~CIP-002-4 R2.~~	~~DELETED~~	~~Dial-up Accessible – No longer applicable since R2 has been deleted.~~
CIP-002-4 R3.	CIP-002-5 R2	Annual Approval – No significant changes to the approval. However, the CIP Sr. Manager now approves identifications required in CIP-002-5 R1 as noted above.
NEW	CIP-002-5 1.~~1~~4	Update and re-categorize for changes to BES – Specifies ~~timeframe~~time frame for complying with all re-categorization ~~and associated security requirements~~of items identified in CIP 002-5 R1 following a change, which is planned ~~change.~~to be in service for more than six calendar months.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R1.	CIP-003-5 ~~R2~~R1, 1.1 through 1.9	Cyber Security Policy – Includes high impact and medium impact BES Cyber Systems. A separate requirement applies to low impact BES Cyber Systems. Clarified that the cyber security policy needs to only reference the subject matter topics at a high level rather than each individual requirement in the CIP Cyber Security Standards.
CIP-003-4 R1.1.	CIP-003-5 ~~R2, 2~~R1, 1.10	Provision for emergency situations – Identified the specific exceptional circumstances in which emergency exceptions can be taken in response to the directive in FERC Order No. 706~~ paragraph~~, Paragraph 443.
NEW	CIP-003-5 R2	Cyber Security Policy for BES Cyber Systems not identified as high or medium impact (low impact). Clarified programmatic controls that apply to low impact BES Cyber Systems and that discrete identification of such systems is not required.
CIP-003-4 R1.2.	~~CIP-003-5 R4~~DELETED	The ~~cyber security policy~~Cyber Security Policy is readily available – ~~The Responsible Entity only needs to make individuals aware of elements of the cyber security policy related to their job function.~~ This was in response to general confusion around the term "readily available~~". Examples of how to make individuals aware are listed~~." Training requirements in ~~the Measures~~CIP-004-5 provide for knowledge of policy.
CIP-003-4 R1.3.	CIP-003-5 ~~R3~~R4	Annual review and approval – No significant change.
CIP-003-4 R2.	CIP-003-5 ~~R1~~R3	Single senior manager – Created a definition of CIP Senior Manager to ~~prevent cross referencing~~facilitate references across ~~Standards~~standards.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R2.1.	CIP-003-5 R1R3	The CIP Senior Manager shall be identified by name, title, and date of designation – The CIP Senior Manager only needs to be identified by name. The other details were considered unnecessary, administrative requirements.
CIP-003-4 R2.2.	CIP-003-5 R6	Changes to the CIP Senior Manager and any delegations must be documented within thirty30 calendar days of the change.
CIP-003-4 R2.3.	CIP-003-5 R5	Delegate authority – Made clear that where allowed by the standards, the CIP Senior Manager canmay delegate the ability to delegate. For example, a senior manager can delegate the ability to further delegate responsibility for a plant control system to a plant manager.authority and such delegations must be documented.
CIP-003-4 R2.4.	DELETED	Authorize and document any exception – The FERC Order No. 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the Standardsstandards.
CIP-003-4 R3.	DELETED	Exceptions – The FERC Order No. 706 made clear that you could not take exceptions to the policy.areas of your Cyber Security Policy that were also required as part of other NERC CIP requirements. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the Standardsstandards.
CIP-003-4 R3.1.	DELETED	Exceptions - Requirement R3 is deleted.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R3.2.	DELETED	Exceptions - Requirement R3 is deleted.
CIP-003-4 R3.3.	DELETED	Exceptions - Requirement R3 is deleted.
CIP-003-4 R4.	CIP-011-1 R1, 1.1, 1.2	Information Protection - Removed ~~the explicit requirement for classification as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business. Removed~~ language to "protect" information, and replaced with ~~"Implement~~requirements for methods to identify BES Cyber System Information and procedures for handling ~~and access control"~~BES Cyber System Information, including storage, transit, and use to clarify the protection that is required.
CIP-003-4 R4.1.	Definition	Identification – ~~Replace~~Replaced this requirement with the defined term BES Cyber System Information.
CIP-003-4 R4.2.	CIP-011-~~1 1~~5 R1.1	Classification – Removed the explicit requirement for classification, as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.
CIP-003-4 R4.3.	CIP-011-~~1 1~~5 R1.3	Assessment – No significant changes.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R5.	CIP-004-5 ~~6.3, CIP-011-1 1.2~~R6.4,	Authorize personnel for access to protected information – Clarified ~~the "program~~: "Program for managing access" included the authorization of access, as well as handling and access control procedures. Grouped requirements for electronic access, physical access, and access to BES Cyber System Information in CIP 004-5 R6.
CIP-003-4 R5.1.	~~DELETED~~CIP-004-5 R6.1	~~Authorizing personnel – Personnel are still required to have authorization, and the CIP Senior Manager authorizes or delegates this responsibility. So the additional requirement to have and maintain a list is considered duplicative and unnecessary.~~Authorizing personnel.
CIP-003-4 R5.1.1.	~~DELETED~~CIP-004-5 R6.1	Personnel shall be identified~~— 5.1 is deleted~~.
CIP-003-4 R5.1.2.	~~DELETED~~CIP-004-5 R6.7	Verification~~— 5.1 is deleted.~~.
CIP-003-4 R5.2.	CIP-004-5 ~~6.6~~R6.7	Verify access privileges annually – Moved requirement to ensure consistency among access reviews. Clarified precise meaning in the term "annual~~.~~". Clarified what was necessary in performing verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.
CIP-003-4 R5.3.	CIP-011-1 1.3	Annual Review – No significant changes.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R6.	CIP-010-1 R1, R2	Change Control and Configuration Management – Moved configuration change management to a separate ~~Standard~~standard because of the additional requirements necessary for satisfying FERC directives, and the subject matter in CIP version 4 is ~~currently~~ spread across CIP-003-4 and CIP-007-4. The baseline requirement is incorporated from the *DHS Catalog for Control Systems Security*. The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed. Added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-4 R6.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R1.	CIP-004-5 R1, 1.1	Security awareness program and quarterly reinforcement - Changed to remove the need to ensure everyone with authorized access receive this material, and moved example mechanisms to ~~guidance.~~Guidance.
CIP-004-4 R2.	CIP-004-5 R2, R3	Training - Addition of identifying the roles that require training. Adding specific role-based training for the visitor control program and storage media as part of the handling of BES Cyber Systems information. Also added the FERC Order No. 706~~-~~, directed electronic interconnectivity supporting the operation and control of BES Cyber Systems. This requirement is also reorganized into the respective requirements for "program" and "implementation" of the training.
CIP-004-4 R2.1.	CIP-004-5 ~~3~~R3.1	Training prior to authorized access – No significant changes.
CIP-004-4 R2.2.	CIP-004-5 ~~2~~R2.1-2.10	Training subject matter – This requirement is reorganized into the respective requirements for "program" and "implementation" of the training.
CIP-004-4 R2.2.1.	CIP-004-5 ~~2~~R2.2	Proper use of CCAs – ~~Minor wording changes.~~ Changed to ~~address~~refer to BES Cyber Systems. Requirement now addresses cyber security issues, not the business or functional use of the BES Cyber System.
CIP-004-4 R2.2.2.	CIP-004-5 ~~2~~R2.3,2.4	Physical and electronic access controls training – No significant changes. Refers to BES Cyber Systems.
CIP-004-4 R2.2.3.	CIP-004-5 ~~2~~R2.6	Information handling training – Core training added for the handling of BES Cyber System Information, with the addition of storage media.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R2.2.4.	CIP-004-5 ~~2~~R2.7,2.8,2.9	Incident identification and notification, incident handling and CCA recovery training – Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for individuals having a role in the recovery to address FERC Order No. 706~~ paragraph~~, Paragraph 413.
CIP-004-4 R2.3.	CIP-004-5 ~~3~~R3.2	Annual training – Replaced "Annually" with "calendar year, not to exceed 15 months~~. ~~."
CIP-004-4 R3.	CIP-004-5 R4, R5, 5.1	Personnel Risk Assessment – Split into two requirements, R4 to define the PRA program, and R5 to implement the program for individuals prior to obtaining authorized access.
CIP-004-4 R3.1.	CIP-004-5 ~~4~~4R.1, 4.2	Identification and 7~~-~~-year criminal check – Addressed interpretation request in ~~guidance.~~Guidance. Specified that ~~identify~~identity verification is only required for each individual's initial assessment. ~~Specify~~ Specified that the ~~seven~~ 7-year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for ~~six~~6 months or more, including current residence, regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full ~~seven~~ 7-year check cannot be performed.
CIP-004-4 R3.2.	CIP-004-5 ~~5~~R5.2	Perform the PRA every 7 years~~. ~~. Removed the "for cause" part of the requirement.
CIP-004-4 R3.3.	CIP-004-5 ~~4~~R4.4	Addresses the contractor or vendor performed PRA.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R4.	CIP-004-5 R6.2, 6.~~1, 6.2~~3	Authorize access - CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need~~-~~-to~~-~~-know" basis, or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.
CIP-004-4 R4.1.	CIP-004-5 ~~6.4~~R6.5	Quarterly review of access – Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4 R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.
CIP-004-4 R4.2.	CIP-004-5 R7	Prevent further access - The FERC Order No. 706~~ Paragraph,~~ Paragraphs 460 and 461, directs modifications to the ~~Standards~~standards to require immediate revocation for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination, instead of within 24 hours. For transfers, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53~~ version,~~ Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-004-5 ~~2~~R2.1	Added to help facilitate understanding what roles the entity has to support the role~~-~~-based training program.
NEW	CIP-004-5 ~~2~~R2.5	Visitor control program training – Personnel administering the visitor control program and/or providing escort should ~~have~~ be part of the core training per FERC Order No. 706~~– paragraph~~, Paragraph 432.
NEW	CIP-004-5 ~~2~~R2.10	Electronic interconnectivity training – Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems per FERC Order No. 706 - ~~paragraph~~Paragraph 434.
NEW	CIP-004-5 ~~4~~R4.3	PRA failure criteria – ~~There should be documented~~ Requires process or criteria ~~or a process used~~ to evaluate personnel risk assessments~~.~~ to determine when to deny authorized access.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-004-5 ~~7~~R7.2	Transfers – The FERC Order No. 706~~ Paragraph~~, Paragraphs 460 and 461, directs modifications to the ~~Standards~~standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53~~ version~~, Version 3, to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.
NEW	CIP-004-5 ~~7.3~~R7.4	Completion of revocation – The FERC Order No. 706~~ Paragraph~~, Paragraphs 460 and 461, directs modifications to the ~~Standards~~standards to require immediate revocation for any person no longer needing access. In order to meet the immediate ~~timeframe, Entities~~time frame, entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	Translation to New Standard or Other Action	Description and Change Justification
NEW	CIP-004-5 ~~7.4~~R7.5	Completion of revocation (shared accounts) – To provide clarification of expected actions in managing the passwords

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R1.	CIP-005-5 R1.1	Electronic Security Perimeter identification – Changes include referencing ~~-~~the defined terms Electronic Access Point and BES Cyber System.
CIP-005-4a R1.1.	Definition	Access Points – This was moved to the definition of Electronic Access Points.
CIP-005-4a R1.2.	Guidance	Dial-up accessible CCA – This is a clarifying statement that was moved to ~~guidance~~Guidance.
CIP-005-4a R1.3.	Guidance	Communication links between ESPs – This is a clarifying statement that was moved to ~~guidance~~Guidance.
CIP-005-4a R1.4.	Applicability	Applicability for Non-Critical Cyber Asset – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.5.	Applicability	Access control and monitoring ~~cyber assets~~Cyber Assets – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.6.	Measures	Maintain Documentation – This is a measure for the requirement to have ~~an~~ ESP documentation.
CIP-005-4a R2.	CIP-005-5 R1	Electronic Access Controls – No significant changes.
CIP-005-4a R2.1.	CIP-005-5 R1.2, 1.~~2~~3	Deny access by default - Changes include referring to the defined term Electronic Access Point, and to focus on the entity knowing and having justification for what it allows through the EAP. ~~The requirement~~ R1.3 explicitly states the network admission control includes both inbound and outbound connections.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R2.2.	CIP-007-5 R1.1~~.~~, 1.2	Enable specific ports/services – Consolidated port hardening requirements to CIP-007.
CIP-005-4a R2.3.	CIP-005-5 ~~1.3~~R1.4	Secure dial-up – Changed to refer to the defined term Electronic Access Point. Added clarification as to the goal of "secure~~",~~," which is that the BES Cyber System should not be directly accessible with a phone number only.
CIP-005-4a R2.4.	CIP-005-5 R2,2.3	Strong access control – Added a new requirement for remote access in response to increased vulnerabilities in VPN technology. This requirement also clarified strong access control meant two-factor (or more) authentication.
CIP-005-4a R2.5.	Measures	Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.1.	CIP-004-5 R6	The processes for access request and authorization – Consolidated with other similar requirements to CIP-004-5 R6.
CIP-005-4a R2.5.2.	Measures	The authentication methods - Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.3.	Measures	The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.~~–~~ Evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.4.	Measures	The controls used to secure dial-up accessible connections.~~–~~ Evidence requirements are considered as part of the measure.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R2.6.	DELETED	Appropriate Use Banner – The drafting team considered this requirement administrative. The objective of having an appropriate use banner is to prevent accidental use of the system and help allow prosecution of unauthorized individuals accessing the system. The drafting team did not consider either of these rising to the level of meeting a reliability objective.
CIP-005-4a R3.	CIP-007-5 R4, 4.1	Monitoring Electronic Access – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the ~~Standards~~standards.
CIP-005-4a R3.1.	CIP-007-5 R4, 4.1	Dial-up Accessible – Removed specific references to dial-up devices. Incorporated into logging/monitoring requirements. The drafting team did not feel further referencing this technology was necessary.
CIP-005-4a R3.2.	CIP-007-5, R4, 4.2	Alerts – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the ~~Standards~~standards.
CIP-005-4a R4.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements.
CIP-005-4a R4.1.	Measures	A document identifying the vulnerability assessment process - Evidence requirements are considered as part of the measure.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R4.2.	CIP-010-1 ~~3~~R3.1, 3.2	A review to verify that only ports and services required for operations at these access points are enabled - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order No. 706~~ paragraph~~, Paragraph 644, the details for what should be included in the assessment are left to ~~guidance~~Guidance.
CIP-005-4a R4.3.	CIP-010-1 ~~3~~R3.1, 3.2	The discovery of all access points to the Electronic Security Perimeter - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order No. 706~~ paragraph~~, Paragraph 644, the details for what should be included in the assessment are left to ~~guidance~~Guidance.
CIP-005-4a R4.4.	CIP-010-1 ~~3~~R3.1, 3.2	A review of controls for default accounts, passwords, and network management community strings - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order No. 706~~ paragraph~~, Paragraph 644, the details for what should be included in the assessment are left to ~~guidance~~Guidance.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R4.5.	CIP-010-1 ~~3~~R3.4	Mitigation plan - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. Added element to have an entity defined date of completion of the mitigation plan per FERC Order No. 706~~ para~~, Paragraph 643.
CIP-005-4a R5.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.1.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.2.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.3.	CIP-007-5 R4.4~~.5~~	Retain relevant log information – Log retention requirements are consolidated to CIP-007-5 R4.
NEW	CIP-005-5 ~~1.6~~R1.5	Inspect ~~&~~and detect potential malicious communications – Per FERC Order No. 706, ~~paragraph~~Paragraphs 496-503, ~~ESP's~~ESPs need two distinct security measures such that the ~~cyber assets~~Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The ~~Order~~order makes clear this is not simple redundancy of firewalls~~,~~; thus the drafting team has decided to add the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-005-5 ~~2~~R2.1,2.2	Remote Access: intermediate device and encryption – This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R1.	CIP-006-5 R1	Physical Security Plan – Removed the requirement for ~~Senior Management~~senior management approval of the physical security plan because there is already approval of the physical security policy and delegation of the task in complying for this program. Additional approval is not considered necessary to meeting the reliability objective of ~~physically~~physical security for the BES Cyber System.
CIP-006-4c R1.1.	CIP-006-5 ~~1~~R1.2, 1.3	Physical Security Perimeter ~~– Reworded~~ – For high impact BES Cyber Systems clarified that two or more different physical access controls must be used to ~~reflect the change from~~collectively allow physical access into Physical Security ~~Perimeter to Defined Physical Boundary.~~Perimeters.
CIP-006-4c R1.2.	DELETED	No longer requires ~~identifing~~identification of all physical access points ~~and controls at them to reflect the change from Physical Security Perimeter to Defined Physical Boundary~~.
CIP-006-4c R1.3.	CIP-006-5 R1.4, 1.~~4~~5	Monitor physical access – A documented plan is required as part of CIP-006-5 R1 that references the new alerting term in ~~table row 1.4, which replaces the monitoring term. Otherwise, no significant change.~~Table Row 1.5. Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.
CIP-006-4c R1.4.	CIP-004-5 ~~2~~R2.3	Appropriate use of access controls – The term "~~appropriate'~~appropriate" used in prior versions is subject to a high degree of subjectivity. The training requirement specifies role-based training on physical access controls.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R1.5.	CIP-004-5 R6 and R7	Review of access authorization requests and revocation of access authorization requirements were consolidated to CIP-004-5.
CIP-006-4c R1.6.	CIP-006-5 R2	Visitor control program - A documented program is required as part of CIP-006-5 R2. Otherwise, no significant change.
CIP-006-4c R1.6.1.	CIP-006-5 ~~2~~R2.2	Log entry and exit of visitors - Addressed multi entry requirements and added the point of contact of who can be considered the sponsor for the person to enter the DPB. There is no need to document the escort or handoffs between escorts.
CIP-006-4c R1.6.2.	CIP-006-5 ~~2~~R2.1	Continuous escorted access of visitors – No significant change.
CIP-006-4c R1.7.	DELETED	Update of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R1.8.	DELETED	Annual review of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R2.	Applicability	Protection of Physical Access Control Systems – Applicability to Physical Access Control and Monitoring Systems were moved to the ~~applicability~~Applicability section of each security requirement, and added this as a defined term in the glossary.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R2.1.	Applicability, CIP-006-5 R1.1	Physical Access Control Systems be protected from unauthorized physical access - Applicability to Physical Access Control Systems were moved to the ~~applicability~~Applicability section of each security requirement. For this particular requirement, see CIP-006-5 ~~item~~, Item 1.1, which applies to Physical Access Control Systems.
CIP-006-4c R2.2.	~~Applicability~~CIP-006-5 R1.6, 1.7	Protection of Physical Access Control Systems - Applicability to Physical Access Control Systems were moved to the ~~applicability~~Applicability section of each security requirement throughout CP version 5.
CIP-006-4c R3.	Applicability	Protection of Electronic Access Control Systems - Applicability to what protections Electronic Access Control and Monitoring Systems need were moved to the ~~applicability~~Applicability section of each security requirement.
CIP-006-4c R4.	CIP-006-5 ~~1~~R1.2, 1.3	Physical Access Controls ~~– Reworded to reflect the change from Physical Security Perimeter to Defined Physical Boundary. Also addressed~~ – R1.3 addresses FERC Order No. 706 Paragraph 572 related directives for physical security defense in depth~~. Examples of methods to implement have been moved to~~ by providing the examples in the guidance ~~section of this requirement.~~document of physical security defense in depth via multifactor authentication or layered Physical Security Perimeter(s).
CIP-006-4c R5.	CIP-006-5 ~~1~~ R1.4, 1.5, 1.6, 1.7	Monitor physical access – Changed the term to alert for unauthorized access and clarified the actions taken for review of unauthorized physical access alerts. Examples of methods to implement have been moved to the ~~guidance~~Guidance section of this requirement.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R6.	CIP-006-5 ~~1.7~~R1.8,	Log physical access – CIP-006-4 R6 was specific to the logging of access at identified access points. This now more generally requires logging of physical access into the ~~Defined Physical Boundary.~~defined physical boundary. Examples of methods to implement have been moved to the ~~guidance~~Guidance section of this requirement.
CIP-006-4c R7.	CIP-006-5 R1.9 and CIP-008-5 Evidence Retention	Access log retention - Retain relevant incident related log information is addressed in CIP-008-5.
CIP-006-4c R8.	CIP-006-5 R3	Maintenance and Testing.
CIP-006-4c R8.1.	CIP-006-5 ~~3~~R3.1	Physical access control system ~~3 yr.~~three-year testing and maintenance – Shortened periodicity of testing to 2 years to address FERC Order No. 706~~ paragraph~~, Paragraph 581 directives. Added testing of locally mounted security hardware devices.
CIP-006-4c R8.2.	REMOVED	Testing and maintenance records are considered the measurement of ~~item~~Item 3.1.
CIP-006-4c R8.3.	CIP-006-5 ~~3~~R3.2	Retain outage records – No significant changes.
~~NEW~~	~~CIP-006-5 1.1~~	~~Entity based Operational or procedural controls to restrict physical access – To allow for programmatic protection controls as a baseline for Low Impact BES Cyber Assets and Physical Access Control Systems. This does not require detailed lists of individuals with access.~~

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R1.	CIP-010-1 ~~1~~R1.4	Assess security controls following changes - Provides clarity on when testing must occur, and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order ~~,paragraphs~~No. 706, Paragraphs 397, 609, 610, and 611.
CIP-007-4 R1.1.	CIP-010-1 ~~1.4~~R1.5	~~Test procedures – See description and justification for CIP-007-4 R1.~~Test procedures – This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.
CIP-007-4 R1.2.	CIP-010-1 ~~1.4~~R1.5	Testing reflects production environment - ~~See description~~This requirement provides clarity on when testing must occur and ~~justification for CIP-007-4 R1~~requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.
CIP-007-4 R1.3.	CIP-010-1 R1.4, 1.~~4~~5	The Responsible Entity shall document test results. ~~– See description~~ The SDT attempted to provide clarity on when testing must occur and ~~justification~~removed requirement for ~~CIP-007-4 R1.~~specific test procedures because it is implicit in the performance of the requirement.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R2.	CIP-007-5 R1	Ports and Services – The requirement focuses on the entity knowing, and only allowing those ports that are necessary. The additional classification of ~~-~~"normal" or ~~emergency'~~"emergency" added no value and has been removed.
CIP-007-4 R2.1.	CIP-007-5 ~~1~~R1.1	Enable only those ports and services required for normal and emergency operations – See description and justification for CIP-007-4 R2.
CIP-007-4 R2.2.	CIP-007-5 ~~1~~R1.1, 1.2	Disable other ports/services – See description and justification for CIP-007-4 R2.
CIP-007-4 R2.3.	DELETED	Compensating measures – See description and justification for CIP-007-4 R2.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R3.	CIP-007-5 R2	Security Patch Management – The existing wording, or CIP-007-4 R3, R3.1~~,~~ and R3.2 was separated into individual line items to provide more granularity. The documentation of a source~~-~~(s) to monitor for release of security related patches, ~~hotfixes~~hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "~~document~~Document the assessment of security patches and security upgrades for applicability within ~~thirty~~30 calendar days of availability of the patches or upgrades~~" there~~." There has been confusion as to what constitutes the availability. Due to issues that may occur regarding ~~Control System~~control system vendor license and service agreements flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.
CIP-007-4 R3.1.	CIP-007-5 ~~2~~R2.2	Assess patches – Similar to the current wording, but added ~~"from the identified~~reference to "identification of a source or sources that the Responsible Entity tracks" to establish where the release is from. The ~~current wording~~word in previous versions: "The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within ~~thirty~~30 calendar days of availability of the patches or upgrades~~"~~," has led to varying opinions as to what constitutes "availability" of the patches or upgrades. The addition attempts to clarify where the release is from.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R3.2.	CIP-007-5 R2.3, 2.~~3~~4	Implement patches - This is the same concept as in the current CIP-007 R3.2 wording; however, a 30~~-~~-day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used. Splitting the implementation of security related patches, ~~hotfixes~~hot fixes, and/or updates into a separate item from compensating measures will provide granularity. Automated processes allow the implementation to be documented and confirmed electronically in a short time period. Manual processes may take an extended period of time to complete documentation of the installation. Priority should be given to the implementation rather than the documentation.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R4.	CIP-007-5 R3, 3.1, 3.2, 3.3~~, 3.4, 3.5~~	Malicious Software Prevention – In prior versions, this requirement has arguably been the single greatest generator of TFE's as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of ~~cyber assets in scope~~Cyber Assets of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method, nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. Beginning in ~~paragraph~~Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a ~~responsible entity~~Responsible Entity does this should be detailed in its ~~cyber security policy~~Cyber Security Policy so that it can be audited for compliance…" In ~~paragraph~~Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level, and regardless of technology, along with the enhanced change management requirements, meets this directive.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R4.1.	CIP-007-5 R3~~,~~ ~~3~~.1~~, 3.2, 3.3~~	Malware prevention tools – See description and justification for CIP-007-4 ~~R4~~R3.
CIP-007-4 R4.2.	CIP-007-5 R3.2, 3.~~4~~3	Update malicious code detections – See description and justification for CIP-007-4 ~~R4~~R3.
CIP-007-4 R5.	CIP-007-5 ~~5~~R5.1	Use at least one authentication method – The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase, "that minimize the risk of unauthorized access~~"~~," was removed and more appropriately captured in the ~~rationale statement~~Rationale Statement.
CIP-007-4 R5.1.	CIP-004-5 R6.1, 6.~~1~~2	Access authorization – CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need~~-~~-to~~-~~-know" basis, or with respect to work functions performed. These were consolidated in CIP-004-5 R6.1 and 6.2 to ensure consistency in the requirement language.
CIP-007-4 R5.1.1.	CIP-003-5 R5.2	Access authorization – CIP-003-5 R5.2 requires CIP Senior Manager or delegate approval for all requirements for authorization in the CIP Cyber Security Standards.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R5.1.2.	CIP-007-5 ~~4~~R4.1	Identify security events for after-the-fact investigation – This requirement is derived from NIST 800-53~~ version~~, Version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the ~~term~~phrase, "system events related to cyber security~~"~~," from informal comments received~~ on CIP-011.~~. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP, as required in CIP-005-4 R3, and user access and activity logs, as required in CIP-007-5 R5, are also included here.
CIP-007-4 R5.1.3.	CIP-004-5 R6.6~~.5~~	Annual account privilege verification – Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.
CIP-007-4 R5.2.	CIP-007-5 ~~5~~R5.2	Identify account types and determine acceptable use – CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure, at best.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R5.2.1.	CIP-007-5 ~~5~~R5.4	Change default vendor passwords – The requirement for the "removal, disabling, or renaming of such accounts where possible", has been removed and incorporated into ~~guidance~~Guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded, uniquely generated default password was manufactured with the BES Cyber System.
CIP-007-4 R5.2.2.	CIP-007-5 ~~5.2~~R5.3	~~Identify account types and determine acceptable use~~Identify those individuals with access to shared accounts - No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.
CIP-007-4 R5.2.3.	CIP-007-5 R5.2, 5.3	Identify account types and determine acceptable use – No significant changes. ~~Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.~~

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R5.3.	CIP-007-5 ~~5~~R5.5	Implement a password policy – CIP-007-4 R5.3 requires the use of passwords, and specifies a specific policy of ~~6~~six characters or more with a combination of alpha-numeric and special characters~~.~~. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials, while recognizing password parameters alone do not achieve this. The drafting team ~~felt~~believes allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.
CIP-007-4 R5.3.1.	CIP-007-5 ~~5~~R5.5	Password length – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.2.	CIP-007-5 ~~5~~R5.5	Password complexity – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.3.	CIP-007-5 R5.5~~.~~, 5.6	Password change frequency – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R6.	CIP-007-5 R4	Security Status Monitoring – Consolidated requirements for monitoring electronic events into CIP-007-5 R4.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R6.1.	CIP-007-5 ~~4~~R4.1	Identify security events – This requirement is derived from NIST 800-53~~ version~~, Version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the ~~term~~phrase, "system events related to cyber security" from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP, as required in CIP-005-4 R3, and user access and activity logs, as required in CIP-007-5 R5, are also included here.
CIP-007-4 R6.2.	CIP-007-5 ~~4~~R4.2	Identify security events for ~~real~~Real-time alerting – This requirement is derived from alerting requirements in CIP-005-4 R3.2 and CIP-007-4 R6.2, in addition to NIST 800-53~~ version~~, Version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.
CIP-007-4 R6.3.	CIP-007-5 ~~4~~R4.1	Identify security events for after-the-fact investigation – See description and justification for CIP-007-4 R6.1.
CIP-007-4 R6.4.	CIP-007-5 ~~4~~R4.4	Retain relevant log information – No significant changes.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R6.5.	CIP-007-5 ~~4.3~~R4.5	Review logs – Beginning in ~~paragraph~~Paragraph 525, and also Paragraph 628 of the FERC Order No. 706, the commission directs a manual review of security event logs on a more periodic basis, and suggests a weekly review. The ~~Order~~order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.
CIP-007-4 R7.	CIP-011-1 ~~2~~R2.1	~~Erase media no longer needed to store protected information~~Disposal or Redeployment – Consistent with FERC Order No. 706, ~~paragraph~~Paragraph 631, clarified that the goal was to prevent the unauthorized retrieval of information from the ~~media~~asset, removing the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal. ~~Removed~~ Moved requirement explicitly requiring records of destruction/redeployment ~~because this was implied as~~to a measure of compliance. Added requirement for chain of custody if the device is taken outside the Physical Security Perimeter.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R7.1.	CIP-011-1 ~~2~~R2.2	~~Disposal – See description and justification for CIP-007-4 R7.~~Disposal - Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the asset, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal. Moved requirement explicitly requiring records of destruction/redeployment, to a measure of compliance. Added requirement for chain of custody if the device is taken outside the Physical Security Perimeter.
CIP-007-4 R7.2.	CIP-011-1 ~~2~~R2.1	Redeployment – See description and justification for CIP-007-4 R7.
CIP-007-4 R7.3.	Measures	See description and justification for CIP-007-4 R7.
CIP-007-4 R8.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated requirements for vulnerability assessments from CIP-005-4 and CIP-007-4.
CIP-007-4 R8.1.	Measures	A document identifying the vulnerability assessment process – This is example evidence required for compliance.
CIP-007-4 R8.2.	CIP-010-1 ~~3~~R3.1, 3.2	Ports and services review – As suggested in FERC Order No. 706 ~~paragraph~~, Paragraph 644, the details for what should be included in the assessment are ~~left to guidance~~included in Guidance.
CIP-007-4 R8.3.	CIP-010-1 ~~3~~R3.1, 3.2	A review of controls for default accounts – As suggested in FERC Order No. 706 ~~paragraph~~, Paragraph 644, the details for what should be included in the assessment are ~~left to guidance~~included in Guidance.
CIP-007-4 R8.4.	CIP-010-1 ~~3~~R3.4	Mitigation plan – Added a requirement for an entity planned date of completion as per the FERC directive in Order No. 706, ~~paragraph~~Paragraph 643.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R9.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
NEW	CIP-007-5 ~~1~~R1.2	Restrict physical I/O ports – In ~~the~~ March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g~~.~~., TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.
NEW	CIP-007-5 ~~2~~R2.1	Identify patch sources – Defining the source(s) that a Responsible Entity monitors for the release of security related patches, ~~hotfixes~~hot fixes, and/or updates will provide a starting point for assessing the effectiveness of the patch management program. Documenting the source is also used to determine when the assessment ~~timeframe~~time frame clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-007-5 ~~4~~R4.3	Generate ~~real~~Real-time alerts and respond to audit-processing failures – This requirement was derived from NIST 800-53 ~~version~~, Version 3 AU-5, which addresses response to audit processing failures. Some interpretations of version 4 CIP Cyber Security Standards considered the failure of the security event monitoring and alerting system to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.
NEW	CIP-007-5 ~~5.6~~R5.7	Limits or alerts on exceeding unsuccessful log in attempts threshold – Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.
~~NEW~~	~~CIP-007-5 R6~~	~~Limit malicious code on maintenance devices – This is a new requirement to address the FERC Order 706 paragraph 621 directive to protect against personnel introducing malicious code into the BES Cyber System. This requirement also clarifies that these devices may be temporarily connected to the BES Cyber System, but do not become a part of the BES Cyber System, nor are they considered Protective (Protected??) Cyber Assets. These devices may be temporarily connected locally to the BES Cyber System for maintenance, but must be protected from introducing malicious code or creating an additional electronic access point.~~

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-008-4 R1.	CIP-008-5 R1	Cyber Security Incident Response Plan – Separated requirement into multiple requirements in a comparable manner as CIP-009-4, where individual aspects of maintaining the plan are listed as separate requirements. ~~The requirement to have an Incident Response Plan now applies to all Responsible Entities as a foundational element of a cyber security program for BES Cyber Systems.~~
CIP-008-4 R1.1.	CIP-008-5 R1.1~~.~~, 1.2	Identify reportable cyber security events – Defined the term Reportable Cyber Security Incident and further described the meaning in relation to CIP-008-5. "Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity. EOP-004-2 will address the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents.
CIP-008-4 R1.2.	CIP-008-5 R1.3, 1.~~2~~4, 1.5	~~Roles and responsibilities of incident response teams – No significant changes.~~Roles and responsibilities of incident response teams – Replaced "incident response teams" with "incident response groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams. Conforming change to reference new defined term Cyber Security Incidents. Clarified the term "communication plan" by specifying the elements that need to be included.

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-008-4 R1.3.	DELETED	Reporting cyber security incidents – ~~Coordinating~~Coordinated with EOP-004-2 drafting team to ensure EOP-004-2 becomes the single ~~Standard~~standard for reporting incidents, and ensure EOP-004-2 references the defined term Reportable Cyber Security Incidents.
CIP-008-4 R1.4.	CIP-008-5 R3.3~~.~~, 3.4	Update incident response plan following review – Included additional specification on update of response plan~~-~~. Addresses FERC Order No. 706, Paragraph 686 directive to modify on lessons learned~~ and aspects of~~. Specifies the ~~DHS Controls~~activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.
CIP-008-4 R1.5.	CIP-008-5 R3.1, 3.~~1~~3	Review incident response plans annually – ~~No significant changes~~Specified what the annual review entails. Addresses FERC Order No. 706, Paragraph 686 to document test, or actual incidents and lessons learned.
CIP-008-4 R1.6.	CIP-008-5 R2.1, 2.~~1~~2	Test incident response plans annually – ~~No significant changes~~Allows deviation from plan(s) during actual events or testing if deviations are recorded for review, and specifies activities required to maintain the plan.

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-008-4 R2.	~~DELETED~~CIP-008-5 R2.3	Cyber Security Incident Documentation – ~~The drafting team considered this requirement fully administrative and as part of~~ Removed references to the ~~internal program to maintain compliance evidence~~retention period because the standard addresses data retention in the Compliance section.
NEW	CIP-008-5 R3.2	Document any lessons learned - Addresses FERC Order No. 706, Paragraph 686 to document test or actual incidents and lessons learned.
NEW	CIP-008-5 ~~3~~R3.5	Communicate incident response plan updates – Added specific timing requirement on communication of plan changes based on review of the DHS Controls and NIST 800-53 guideline.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-4 R1.	CIP-009-5 R1, 3.1, 3.3	Recovery Plan – Added ~~the requirements to additionally review plans after system replacement. Also added~~ requirement for documentation of any identified deficiencies or lessons learned. Added the requirement to additionally review plans after technology changes.
CIP-009-4 R1.1.	CIP-009-5 ~~1~~R1.1	Conditions for activation of recovery plan – ~~Reworded to address FERC Order 706 paragraph 694 directive and simplified the requirement~~Minor wording changes, essentially unchanged.
CIP-009-4 R1.2.	CIP-009-5 ~~1~~R1.2	Roles and responsibilities of recovery plan responders – No significant changes.
CIP-009-4 R2.	CIP-009-5 ~~2~~R2.1	Test recovery plan annually – No significant changes.
CIP-009-4 R3.	CIP-009-5 ~~3~~R3.2	Review results of recovery plan activities (tests, events) – Added the ~~timeframe~~time frame for update.
CIP-009-4 R4.	CIP-009-5 ~~1~~R1.3	Backup processes – No significant changes.
CIP-009-4 R5.	CIP-009-5 ~~2~~R2.2	Test information used for recovery – Combined ~~Requirement~~requirement from CIP-009-4 R5 and included requirement to test when initially stored. Addresses FERC Order No. 706~~ directives~~, Directives 739 and 748 related to testing of backups.
NEW	CIP-009-5 ~~1~~R1.4	Testing of backup media – Addresses FERC Order No. 706~~ paragraph~~, Paragraph 739 and 748 directives regarding the testing of backup media.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-009-5 ~~1.6~~R1.5	Process to preserve data for analysis – Added requirement to address FERC Order No. 706, ~~paragraph~~Paragraph 706, regarding the necessity to have procedures in place to retain ~~cyber asset~~Cyber Asset evidence as part of the recovery planning.
NEW	CIP-009-5 R2.3	Test each of the recovery plans for high impact BES Cyber Systems at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. Addresses FERC Order No. 706, Paragraph 725, to add the requirement that the recovery plan test be a full operational test once every 3 years.
NEW	CIP-009-5 ~~3.5~~R3.4	Communicate recovery plan updates – This change ensures that recovery personnel are aware of any changes to recovery plans.
Standard: New Requirements in CIP-010-1 and CIP-011-1		

~~Standard: New Requirements in CIP-010-1 and CIP-011-1~~		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-1 ~~1~~R1.1	Baseline configuration – Baseline requirement incorporated from the DHS Catalog for Control Systems Security (also NIST 800-53). The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed.

~~Standard: New Requirements in CIP-010-1 and CIP-011-1~~		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-1 ~~2~~R2.1	~~Monitor for changes to the baseline configuration – Monitoring~~The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes. This ~~change addresses FERC Order 706, paragraph 397 directive and is based on a~~ requirement was added after review of the DHS Catalog of Control System Security ~~Controls (~~and to address FERC Order No. 706, Paragraph 397. DHS Catalog & addresses FERC Order No. 706, Paragraph 397. Thirty-five calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or ~~NIST 800-53).~~for beginning or endings of months on weekends.
NEW	CIP-010-1 ~~3~~R3.2	Live Vulnerability Assessment for high impact BES Cyber Systems – Addresses FERC Order No. 706~~ paragraph~~, Paragraph 541, 542, 544, and 547 directives regarding the performance of a live vulnerability assessment~~ in a test environment~~.
NEW	CIP-010-1 ~~3~~R3.3	Perform active VA on new BES Cyber Assets for high impact - Addresses FERC Order No. 706~~ paragraph~~, Paragraph 541, 542, 544, and 547 directives regarding the performance of a vulnerability assessment prior to placing a new Cyber Asset into production.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-4

3. Purpose: NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its records of approvals as specified in Requirement R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 The Regional Entity shall serve as the Compliance Enforcement Authority with the following exceptions:

- For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.2. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change “Control Center” to “control center”	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-4

3. Purpose: Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-003-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-4 Requirement R2.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance	

		Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-4

3. Purpose: Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-004-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-004-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);

- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program. Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-4a

3. Purpose: Standard CIP-005-4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4a should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-005-4a, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-4a:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4a.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.1 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.1 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.2 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-4a from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Developed separately.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2	Approved by NERC Board of	Modifications to clarify the requirements and to bring the compliance elements into	Revised.

	Trustees 5/6/09	conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Changed CIP-005-2 to CIP-005-3. Changed all references to CIP Version "2" standards to CIP Version "3" standards. For Violation Severity Levels, changed, "To be developed later" to "Developed separately."	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010	Addition
4a	01/24/11	Adopted by the NERC Board of Trustees	Update to conform to changes to CIP-002-4 (Project 2008-06) Update version number from "3" to "4a"

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-4c

3. Purpose: Standard CIP-006-4 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-4c should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-006-4c, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-006-4c:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the

Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-4c for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	May 2, 2006	Adopted by NERC Board of Trustees	
1	January 18, 2008	FERC Order issued approving CIP-006-1	
	February 12, 2008	Interpretation of R1 and Additional Compliance Information Section 1.4.4 adopted by NERC Board of Trustees	Project 2007-27
2		Updated version number from -1 to -2 Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	Project 2008-06
2	May 6, 2009	Adopted by NERC Board of Trustees	
	August 5, 2009	Interpretation of R4 adopted by NERC Board of Trustees	Project 2008-15
2	September 30, 2009	FERC Order issued approving CIP-006-2	
3	November 18, 2009	Updated version number from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized. Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	Project 2009-21
3	December 16, 2009	Adopted by NERC Board of Trustees	
	February 16, 2010	Interpretation of R1 and R1.1 adopted by NERC Board of Trustees	Project 2009-13
3	March 31, 2010	FERC Order issued approving CIP-006-3	
2a/3a	July 15, 2010	FERC Order issued approving the Interpretation of R1 and R1.1. Updated version numbers from -2/-3 to -2a/-3a.	
4	January 24,	Adopted by NERC Board of Trustees	

	2011		
3c/4c	May 19, 2011	FERC Order issued approving two interpretations: 1) Interpretation of R1 and Additional Compliance Information Section 1.4.4; and 2) Interpretation of R4. Updated version number from -3/-4 to -3c/-4c.	

Appendix 1

Requirement Number and Text of Requirement
R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following: R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
Question
If a completely enclosed border cannot be created, what does the phrase, "to control physical access" require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption? Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?
Response
For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are "physical in nature." The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

Appendix 2

Interpretation of Requirement R1.1.

Request: *Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*

Interpretation:

Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border.

CIP-006-1 — Requirement 1.1 requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

CIP-006-1 — Additional Compliance Information 1.4.4 identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.

1.4. Additional Compliance Information

1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.

Appendix 3

The following interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R4 was developed by the standard drafting team assigned to Project 2008-14 (Cyber Security Violation Severity Levels) on October 23, 2008.

Request:

1. *For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*
2. *Does the term, "time of access" mean logging when the person entered the facility or does it mean logging the entry/exit time and "length" of time the person had access to the critical asset?*

Interpretation:

No, monitoring and logging of access are only required for ingress at this time. The term "time of access" refers to the time an authorized individual enters the physical security perimeter.

Requirement Number and Text of Requirement

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-4

3. Purpose: Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-007-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-4 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	

		Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-4

3. Purpose: Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-008-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-4 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated Version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-4

3. Purpose: Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-009-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-009-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards

The Cyber Security Order 706 Version 5 CIP Drafting Team thanks all commenters who submitted comments on the first formal posting of Project 2008-06 - CSO706 Version 5 CIP Standards. These standards were posted for a 60-day public comment period from November 7, 2011 through January 6, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 131 sets of comments, including comments from approximately 294 different people from approximately 191 companies representing all 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_Version_5_CIP_Standards_.html

Note: In March 2012, in consideration of the extremely large volume of comments received during the formal comment period and initial ballots that ended January 6, 2012, the Standards Committee authorized the following:

Waive the requirement that the Cyber 706 SDT provide individual responses and direct the team to focus on providing detailed summary responses to each question subject to the following conditions:

- *Each summary response should address the comments submitted, in aggregate, such that the summary response clearly addresses all of the comments submitted.*
- *As part of the Consideration of Comments report, add a paragraph that clarifies that the drafting team developed summary responses rather than individual responses with the approval of the Standards Committee and invite any stakeholder who believes his or her comment was not adequately addressed to submit a written request for additional clarity within 15 calendar days [of the posting date] to the team's advisor with a commitment that the team will provide a written response within 15 calendar days. (The standards staff will post any requests for additional clarity and associated responses on the project's web page.)*
- *When the standards staff posts the revised standards for stakeholder comment, staff will include in the announcement the same offer to provide stakeholders with a more detailed response and commitment to publicly post these requests and associated responses.*

If you feel that your comment has been overlooked, please let us know immediately. Special instructions for submitting a request for additional clarification were provided in the announcement of this posting, which is posted on the project page. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President of Standards and Training, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

1. Many definitions in the Definitions document contain modified definitions from existing terms and new definitions for terms used in these standards. Do you have any suggestions that would improve the proposed definitions? If so, please explain and provide specific suggestions for improvement. 31

2. CIP-002-5 Attachment 1 contains criteria that provide the basis for the categorization of BES Cyber Systems and BES Cyber Assets. Most of these criteria are similar to those already approved by the industry as part of Version 4. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement. 47

3. Requirement R1 of draft CIP-002-5 states, "Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification." Further, part 1.1 of R1 states "Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement. 62

4. Requirement R2 of draft CIP-002-5 states, "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement. 75

5. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-002-5? If not, please provide suggested improvements on the proposed VRFs and VSLs 82

6. CIP-003-5 R1 states "Each Responsible Entity shall identify, by name, a CIP Senior Manager." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement. 89

7. CIP-003-5 R2 states "Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement. 90

8. CIP-003-5 R3 states "Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and

at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals." Do you agree with the proposed Requirement R3? If not, please explain why and provide specific suggestions for improvement. 92

9. CIP-003-5 R4 states "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function." Do you agree with the proposed Requirement R4? If not, please explain why and provide specific suggestions for improvement. 93

10. CIP-003-5 R5 states "The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated." Do you agree with the proposed Requirement R5? If not, please explain why and provide specific suggestions for improvement. 94

11. CIP-003-5 R6 states "Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement. 96

12. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-003-5? If not, please provide suggested improvements on the proposed VRFs and VSLs. 97

13. CIP-004-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 98

14. CIP-004-5 R2 states "Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 100

15. CIP-004-5 R3 states "Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific

suggestions for improvement with reference to the appropriate main requirement or part number. 103

16. CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 105
17. CIP-004-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 110
18. CIP-004-5 R6 states "Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R6 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 111
19. CIP-004-5 R7 states "Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R7 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 114
20. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-004-5? If not, please provide suggested improvements on the proposed VRFs and VSLs. 117
21. CIP-005-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 119
22. CIP-005-5 R2 states "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Remote Access Management." The requirement then proceeds to define the requirement parts in the table. Do

you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 120

23. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-005-5? If not, please provide suggested improvements on the proposed VRFs and VSLs. 122

24. CIP-006-5 R1 states "Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in CIP-006-5 Table R1 – Physical Security Plan." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 122

25. CIP-006-5 R2 states "Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 127

26. CIP-006-5 R3 states "Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 129

27. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-006-5? If not, please provide suggested improvements on the proposed VRFs and VSLs. 130

28. CIP-007-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 131

29. CIP-007-5 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 133

30. CIP-007-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 137

31. CIP-007-5 R4 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 140

32. CIP-007-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 144

33. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-007-5? If not, please provide suggested improvements on the proposed VRFs and VSLs..... 146

34. CIP-008-5 R1 states "Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 147

35. CIP-008-5 R2 states "Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 –BES Cyber Security Incident Response Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 149

36. CIP-008-5 R3 states "Conduct sufficient reviews, updates and communications to verify the REs response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 151

37. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-008-5? If not, please provide suggested improvements on the proposed VRFs and VSLs. 153

38. CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 154

39. CIP-009-5 R2 states "Each Responsible Entity shall implement one or more processes that collectively address the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 155

40. CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 156

41. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-009-5? If not, please provide suggested improvements on the proposed VRFs and VSLs. 158

42. CIP-010-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 160

43. CIP010-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 165

44. CIP-010-1 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide

specific suggestions for improvement with reference to the appropriate main requirement or part number. 169

45. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-010-1? If not, please provide suggested improvements on the proposed VRFs and VSLs. 172

46. CIP-011-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-011-5 Table R1 – Information Protection." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 173

47. CIP-011-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-5 Table R2 – Media Reuse and Disposal." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number. 175

48. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-011-1? If not, please provide suggested improvements on the proposed VRFs and VSLs. 178

49. Do you agree with the proposed implementation plan? If so, please explain and provide specific suggestions for improvement. 180

50. Other Comments 183

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		SERC	1, 3, 5, 6
2.	Mike Garton		NPCC	3
3.	Michael Gildea		MRO	3
4.	Louis Slade		RFC	3, 5, 6

2.	Group	Brian Millard	Tennessee Valley Authority	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Larry Akens			1
2.	Ian Grant			3
3.	David Thompson			5

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
4. Marjorie Parsons		6										
3. Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
5.	Brian Evans-Mongeon	Utility Services	NPCC	8
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	Chantel Haswell	FPL Group, Inc.	NPCC	5
9.	David Kiguel	Hydro One Networks Inc.	NPCC	1
10.	Michael Lombardi	Northeast Utilities	NPCC	1
11.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9
12.	Bruce Metruck	New York Power Authority	NPCC	6
13.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
14.	Rogert Pellegrini	The United Illuminating Company	NPCC	1
15.	Si-Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
16.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
17.	Saurabh Saksena	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Donald Weaver	New Brunswick System Operator	NPCC	2

4. Group	Brent Ingbrigtson	PPL Corporation	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Brenda Truhe	PPL Electric Utilities Corp.	RFC	1
2.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	WECC	5
3.	Mark Heimbach	PPL EnergyPlus	MRO	6
4.	Annette Bannon	PPL Generation, LLC on behalf of its NERC Registered Entities	RFC	5
5.	Mark Heinbach	PPL EnergyPlus, LLC	NPCC	6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Mark Heinbach	PPL EnergyPlus, LLC	SERC 6										
7.	Mark Heinbach	PPL EnergyPlus, LLC	SPP 6										
8.	Mark Heinbach	PPL EnergyPlus, LLC	RFC 6										
9.	Mark Heinbach	PPL EnergyPlus, LLC	WECC 6										
5.	Group	Lesley Bingham	SPP RTO and listed members		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.		Sunflower Electric Power Company	SPP	
2.		Nebraska Public Power District	SPP	
3.		Grand River Dam Authority	SPP	

6.	Group	Steve Alexanderson P.E.	Pacific Northwest Small Public Power Utility Comment Group			X	X					X	

	Additional Member	Additional Organization	Region	Segment Selection
1.	Dave Proebstel	Clallam County PUD No.1	WECC	3
2.	Russell A. Noble	Cowlitz County PUD No. 1	WECC	3, 4, 5
3.	Ronald Sporseen	Lincoln Electric Cooperative	WECC	3
4.	Ronald Sporseen	Blachly-Lane Electric Cooperative	WECC	3
5.	Ronald Sporseen	Central Electric Cooperative	WECC	3
6.	Ronald Sporseen	Consumers Power	WECC	1, 3
7.	Ronald Sporseen	Clearwater Power Company	WECC	3
8.	Ronald Sporseen	Douglas Electric Cooperative	WECC	3
9.	Ronald Sporseen	Fall River Rural Electric Cooperative	WECC	3
10.	Ronald Sporseen	Northern Lights	WECC	3
11.	Ronald Sporseen	Lane Electric Cooperative	WECC	3
12.	Ronald Sporseen	Raft River Rural Electric Cooperative	WECC	3
13.	Ronald Sporseen	Lost River Electric Cooperative	WECC	3
14.	Ronald Sporseen	Salmon River Electric Cooperative	WECC	3
15.	Ronald Sporseen	Umatilla Electric Cooperative	WECC	3
16.	Ronald Sporseen	Coos-Curry Electric Cooperative	WECC	3
17.	Ronald Sporseen	West Oregon Electric Cooperative	WECC	3
18.	Ronald Sporseen	Pacific Northwest Generating Cooperative	WECC	3, 4, 8
19.	Ronald Sporseen	Power Resources Cooperative	WECC	5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
7.	Group	Bob Case - NERC Compliance Manager (605) 721-2716	Black Hills Corporation Registered Entities (NCR00089, NCR05030, NCR05031 & NCR11186)	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	NCR00089 (BHCE)		WECC	1, 3, 4, 5, 6
2.	NCR05030 (BHP)		WECC	1, 3, 4, 5, 6
3.	NCR05031 (BHW)		WECC	5
4.	NCR11186 (BHCI)		WECC	5

8.	Group	Jesus Sammy Alcaraz	Imperial Irrigation District (IID)	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Tino Zaragoza	IID	WECC	1
2.	Jesus Sammy Alcaraz	IID	WECC	3
3.	Diana Torres	IID	WECC	4
4.	Marcela Caballero	IID	WECC	5
5.	Cathy Bretz	IID	WECC	6

9.	Group	Annabelle Lee	NESCOR/NESCO										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Glen Chason	EPRI		
2.	Scott Sternfeld	EPRI		
3.	Andrew Wright	N-Dimension Security		
4.	Chan Park	N-Dimension Security		
5.	Dan Widger	N-Dimension Security		
6.	Stacy Bresler	NESCO		
7.	Carol Muehrcke	Adventium Enterprises		
8.	Josh Axelrod	AlertEnterprise!		
9.	Mladen Kezunovic	TLI		
10.	Tomo Popovic	TLI		
11.	Art Conklin	University of Houston		
12.	Elizabeth Sisley	Calm Sunrise Consulting		
13.	Annabelle Lee	EPRI		
14.	Marc Child	Great River Energy		

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
15. Scott Hughes	Great River Energy											
10. Group	Will Smith	MRO NSRF										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mahmood Safi	OPPD	MRO	1, 3, 5, 6
2.	Chuck Lawrence	ATC	MRO	1
3.	Tom Webb	WPS	MRO	3, 4, 5, 6
4.	Jodi Jenson	WAPA	MRO	1, 6
5.	Ken Goldsmith	ALTW	MRO	4
6.	Alice Ireland	XCEL	MRO	1, 3, 5, 6
7.	Dave Rudolph	BEPC	MRO	1, 3, 5, 6
8.	Eric Ruskamp	LES	MRO	1, 3, 5, 6
9.	Joe Deporter	MGE	MRO	3, 4, 5, 6
10.	Scott Nickels	RPU	MRO	4
11.	Terry Harbour	MEC	MRO	1, 3, 5, 6
12.	Marie Knox	MISO	MRO	2
13.	Lee Kittelson	OTP	MRO	1, 3, 4, 5
14.	Tony Eddleman	NPPD	MRO	1, 3, 5
15.	Mike Brytowski	GRE	MRO	1, 3, 5, 6
16.	Richard Burt	MPC	MRO	1, 3, 5, 6

11. Group	Rick Terrill	Luminant					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Brad Jones	Luminant Energy	ERCOT	6
2.	Mike Laney	Luminant Generation		5

12. Group	Ronnie Hoeinghaus	City of Garland			X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Billy Lee		ERCOT	3
2.	Heather Siemens		ERCOT	3

13. Group	Michael Quinn, Chair	Members Representative Committee	X	X	X		X		X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Tim Soles	Occidental Power Services	ERCOT	5
2.	Bruce Wertz	Wertz & Associates, Inc.	ERCOT	5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3. Pam Zdenek		Sweetwater Wind 2 LLC	ERCOT 5										
4. Jose Escamillia		CPS Energy	ERCOT 9										
14.	Group	Tim Hattaway	PowerSouth CIP Review Team				X	X					
Additional Member		Additional Organization	Region Segment Selection										
1. Craig Kilpatrick			SERC										
2. Mark Dayton			SERC										
3. Brian Fleming			SERC										
4. Jon Harrison			SERC										
5. Greg Hataway			SERC										
15.	Group	Roger Powers	CWLP	X		X		X					
Additional Member		Additional Organization	Region Segment Selection										
1. Steve Rose			SERC 5										
2. Shaun Anders			SERC 1										
16.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X
ditional Member		Additional Organization	Region Segment Selection										
1.			Sunflower Electric Power Company SPP										
2.			Nebraska Public Power District SPP										
3.			Grand River Dam Authority SPP										
17.	Group	Mary Jo Cooper	ZGlobal on behalf of City of Lodi, City of Ukiah, Alameda Municipal Power, Salmon River Electric Coop, California Pacific Electric Company			X							
Additional Member		Additional Organization	Region Segment Selection										
1. Katie Spence		Salmon River Electric Coop	WECC 3										
2. Colin Murphey		City of Ukiah	WECC 3										
3. Douglas Draeger		Alameda Municipal Power	WECC 3										
4. Sam Rohn		California Pacific Electric Coop	WECC 3										
5. Elizabeth Kirkley		City of Lodi	WECC 3										
18.	Group	David Batz	Edison Electric Insititute	X				X					
http://www.eei.org													

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
19.	Group	Michael Mertz	PNM Resources (Includes Public Service Co. of New Mexico and Texas New Mexico Power	X		X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Laurie Williams	Public Service Co. of New Mexico	WECC	1
2.	Roger Dickens	Texas New Mexico Power	ERCOT	1
3.	Michael Mertz	PNM Resources	WECC	3

20.	Group	Kevin Cyr	Seattle City Light	X		X	X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Dana Wheelock	Seattle City Light	WECC	3
2.	Pawel Krupa	Seattle City Light	WECC	1
3.	Hao Li	Seattle City Light	WECC	4
4.	Dennis Sismaet	Seattle City Light	WECC	6
5.	Mike Haynes	Seattle City Light	WECC	5

21.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Timothy Beyrle	City of New Smyrna Beach	FRCC	4
2.	Greg Woessner	Kissimmee Utility Authority	FRCC	3
3.	Jim Howard	Lakeland Electric	FRCC	3
4.	Lynne Mila	City of Clewiston	FRCC	3
5.	Joe Stonecipher	Beaches Energy Services	FRCC	1
6.	Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4
7.	Randy Hahn	Ocala Utility Services	FRCC	3

22.	Group	Steve Rueckert	Western Electricity Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Brent Castagnetto	WECC	WECC	10
2.	Liz Brereton	WECC	WECC	10
3.	Don Pape	WECC	WECC	10

23.	Group	Jason Marshall	ACES Power Marketing Member Collaborators						X				

Additional Member	Additional Organization	Region	Segment Selection

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
1. Bill Hutchison	Southern Illinois Power Cooperative	SERC 1, 3, 5, 6										
2. James Jones	AEPCO/SWTC	WECC 1, 5, 6										
3. Bob Solomon	Hoosier Energy	RFC 1, 3, 5, 6										
4. Mark Ringhausen	Old Dominion Electric Cooperative	RFC 3, 4, 5, 6										
5. Patrick Woods	East Kentucky Power Cooperative	SERC 1, 3, 5, 6										
6. Lindsay Shepard	Sunflower Electric Power Corporation	SPP 1, 3, 5, 6										
7. Mohan Sachdeva	Buckey Power	RFC 4, 5, 6										
8. Shari Heino	Brazos Electric Power Cooperative	ERCOT 1, 3, 5										
24. Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Steve Osvath	FE	RFC	
2.	Cindy Sheehan	FE	RFC	
3.	Tim Sheerer	FE	RFC	
4.	Mary Jane Linn	FE	RFC	
5.	Dan Irwin	FE	RFC	
6.	Mark Koziel	FE	RFC	
7.	Troy Rhoades	FE	RFC	
8.	Betsy Hostert	FE	RFC	
9.	Peter Buerling	FE	RFC	
10.	Nathaniel Maier	FE	RFC	
11.	Larry Raczkowski	FE	RFC	
12.	John Olszewski	FE	RFC	
13.	Nathan Sterritt	FE	RFC	
14.	Don Miller	FE	RFC	
15.	David Griffin	FE	RFC	
16.	Ken Dresner	FE	RFC	
17.	Jim Simpson	FE	RFC	
18.	Robert Loy	FE	RFC	
19.	Ron Ross	FE	RFC	
20.	Phil Bowers	FE	RFC	
21.	Heather Herling	FE	RFC	
22.	Vicki Magni	FE	RFC	

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
25.	Group	Andrew Gallo, Chair	NERC Standards Review Subcommittee - ERCOT Region			X		X				X	

	Additional Member	Additional Organization	Region	Segment Selection
1.	Tim Soles	Occidental Power Services	ERCOT	5
2.	Bruce Wertz	Wertz & Associates, Inc.	ERCOT	5
3.	Pam Zdenek	Sweetwater Wind 2 LLC	ERCOT	5
4.	Jose Escamillia	CPS Energy	ERCOT	9

26.	Group	Scott Harris	Kansas City Power & Light	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Jennifer Flandermeyer	Kansas City Power & Light	SPP	1, 3, 5, 6
2.	Michael Gammon	Kansas City Power & Light	SPP	1, 3, 5, 6
3.	Alan Kloster	Kansas City Power & Light	SPP	1, 3, 5, 6
4.	Dean Larson	Kansas City Power & Light	SPP	1, 3, 5, 6
5.	Tony Mann	Kansas City Power & Light	SPP	1, 3, 5, 6
6.	Monica Strain	Kansas City Power & Light	SPP	1, 3, 5, 6
7.	Paul Schiemege	Kansas City Power & Light	SPP	1, 3, 5, 6
8.	John Breckenridge	Kansas City Power & Light	SPP	1, 3, 5, 6

27.	Group	Paul M. Skare	Paul Skare, et al									X	

	Additional Member	Additional Organization	Region	Segment Selection
1.	A. David McKinnon	Pacific Northwest National Laboratory	NA - Not Applicable	9
2.	Samuel L. Clements	Pacific Northwest National Laboratory	NA - Not Applicable	9

28.	Group	Marianne Swanson	Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG)									X	

	Additional Member	Additional Organization	Region	Segment Selection
1.	Victoria Yan Pillitteri	Booz Allen Hamilton	NA - Not Applicable	NA
2.	David Dalva	Booz Allen Hamilton	NA - Not Applicable	NA

29.	Group	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				

No additional members listed.

30.	Group	Christine Hasha	ISO/RTO Council Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Charles Yeung	SPP	SPP	2										
2. Al DiCaprio	PJM	RFC	2										
3. Marie Knox	MISO	RFC	2										
4. Ben Li	IESO	NPCC	2										
31.	Group	Donald Brookhyser	EPUC, CAC and NCA										
No additional members listed.													
32.	Group	Travis Metcalfe	Tacoma Power			X							
Additional Member	Additional Organization	Region	Segment Selection										
1. Chang Choi	Tacoma Power	WECC	1										
2. Keith Morisette	Tacoma Power	WECC	4										
3. Mike Hill	Tacoma Power	WECC	6										
4. Max Emrick	Tacoma Power	WECC	5										
33.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
34.	Individual	John Souza	Turlock Irrigation District			X							
35.	Individual	Richard Malloy	Idaho Falls Power			X		X					
36.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
37.	Individual	Ed Croft	Puget Sound Energy	X		X		X					
38.	Individual	John.Brockhan@CenterPointEnergy.com	CenterPoint Energy	X									
39.	Individual	Ed Nagy	LCEC CIP Team	X		X							
40.	Individual	Patricia Lynch	NRG Energy Inc.	X				X					
41.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
42.	Individual	Cynthia Oder	Salt River Project	X		X		X	X				
43.	Individual	Summer C. Esquerre	Corporate Compliance	X		X		X	X				
44.	Individual	James Eckelkamp	Progress Energy	X		X		X	X				
45.	Individual	Scott Bordenkircher	Arizona Public Service Company	X		X		X	X				
46.	Individual	Doug Peterchuck	Omaha Public Power District	X		X		X	X				
47.	Individual	Jennifer Wright	San Diego Gas & Electric	X		X		X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
48.	Individual	Roger Pan	Emerson Process Management										
49.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
50.	Individual	Tom Bowe	PJM		X								
51.	Individual	Chris Higgins / BPA CIP Team	Bonneville Power Administration	X		X		X	X				
52.	Individual	Daniel Duff	Liberty Electric Power, LLC					X					
53.	Individual	Joanna Luong-Tran	TransAlta Centralia Generation					X					
54.	Individual	Mario Lajoie	Hydro-QuÃ©bec TransÃ‰nergie	X									
55.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
56.	Individual	Dan Roethemeyer	Dynegy					X					
57.	Individual	J. S, Stonecipher, PE	City of Jacksonville Beach dba/Beaches Energy Services	X									
58.	Individual	Thomas Lyons	Owensboro Municipal Utilities			X							
59.	Individual	Randy Hahn	Ocala Utility Services	X									
60.	Individual	Tracy Richardson	Springfield Utility Board			X							
61.	Individual	Kirit Shah	Ameren	X		X		X	X				
62.	Individual	Aliza Dewji P.Eng	ATCO Power Canada Ltd.										
63.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
64.	Individual	Thomas M. Haire, P.E.	Rutherford EMC			X	X						
65.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
66.	Individual	Saurabh Saksena	National Grid	X		X							
67.	Individual	MIchael Johnson	APX Power Markets								X		
68.	Individual	Scott Bos	Muscatine Power and Water	X		X		X	X				
69.	Individual	Robin W. Blanton	Piedmont EMC			X							
70.	Individual	Marc Child	Great River Energy	X		X		X	X				
71.	Individual	Michael Falvo	Independent Electricity System Operator		X								

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
72.	Individual	Rodney Luck	Los Angeles Department of Water and Power	X		X		X	X				
73.	Individual	Jack Stamper	Public Utility District No. 1 of Clark County	X									
74.	Individual	Paul Crosby	Platte River Power Authority	X		X		X	X				
75.	Individual	Nathan Smith	Southern California Edison	X		X		X	X				
76.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)										
77.	Individual	William O Thompson	NIPSCO Northern Indiana Public Service Company	X		X		X	X				
78.	Individual	Curt Wilkins	Douglas County PUD No.1				X	X					
79.	Individual	Brenda Frazer	Edison Mission Marketing & Trading	X				X					
80.	Individual	David Kiguel	Hydro One Networks Inc.	X		X							
81.	Individual	Michelle Denike	Wolverine Power Supply Cooperative, Inc.	X									
82.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
83.	Individual	Michael Schiavone	Niagara Mohawk (National Grid Company)			X							
84.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
85.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
86.	Individual	John Bee	Exelon	X		X		X					
87.	Individual	David Martorana	Tenaska, Inc.					X					
88.	Individual	Robert Solomon	Hoosier Energy	X		X		X					
89.	Individual	Tracy Sliman	Tri-State G&T Inc.	X									
90.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
91.	Individual	Rich Vine	California ISO		X								
92.	Individual	Richard Salgo	NV Energy	X		X		X	X				
93.	Individual	John Martinsen	Public Utility District No. 1 of Snohomish County	X		X	X	X	X				
94.	Individual	Bo Jones	Westar Energy	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
95.	Individual	Bruce Metruck	New York Power Authority	X		X		X	X				
96.	Individual	Edward Bedder	Orange and Rockland Utilities Inc.	X		X							
97.	Individual	Thad Ness	American Electric Power	X		X		X	X				
98.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				
99.	Individual	David Burke	Orange and Rockland Utilities, Inc.	X		X							
100.	Individual	Martin Kaufman	ExxonMobil Research and Engineering	X				X					
101.	Individual	Mikhail Falkovich	PSEG	X		X		X	X				
102.	Individual	David Dockery	Associated Electric Cooperative, Inc	X		X		X	X				
103.	Individual	Shari Heino	Brazos Electric Power Cooperative, Inc.	X				X					
104.	Individual	Joe Tarantino	Sacramento Municipal Utility District	X		X	X	X	X				
105.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
106.	Individual	Andrew Z. Pusztai	American Transmission company, LLC	X									
107.	Individual	David S. Revill	Georgia Transmission Corporation	X									
108.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
109.	Individual	John Tolo	Tucson Electric Power	X									
110.	Individual	Tony Eddleman	Nebraska Public Power District	X		X		X					
111.	Individual	Mark B Thompson	Alberta Electric System Operator		X								
112.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric Company					X					
113.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
114.	Individual	Don Jones	Texas Reliability Entity										X
115.	Individual	Roger Fradenburgh	Network & Security Technologies Inc								X		
116.	Individual	Kevin Koloini	AMP				X						
117.	Individual	Nathan Mitchell	American Public Power Association			X							
118.	Individual	Greg Rowland	Duke energy	X		X		X	X				
119.	Individual	RoLynda Shumpert	South Carolina Electric and Gas	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
120.	Individual	Richard Powell	JEA	X		X		X					
121.	Individual	Rebecca Moore Darrah	MISO		X								
122.	Individual	Michelle D'Antuono	Ingleside Cogeneration LP					X					
123.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
124.	Individual	Christine Hasha	Electric Reliability Council of Texas, Inc.		X								
125.	Individual	Gregory Campoli	New York Independent System Operator		X								
126.	Individual	David Grubbs	City of Garland	X									
127.	Individual	Darryl Curtis	Oncor Electric Delivery Company LLC	X									
128.	Individual	Jose H Escamilla	CPS Energy	X		X		X					
129.	Individual	Adam Menendez	Portland General Electric	X		X		X	X				
130.	Individual	Scott Miller	MEAG Power	X		X		X					
131.	Individual	Maggy Powell	Constellation Energy on behalf of Baltimore Gas and Electric, Constellation Power Generation, Constellation Commodities Group and Constellation Energy Control and Dispatch	X		X		X	X				

Summary Consideration and Common Responses to Issues and Comments Frequently Repeated in Q1-Q49

There were several comments the SDT considered that were repeated across multiple questions, sometimes submitted by the same entity to each or to many of the questions. Rather than responding separately in each question, the SDT addresses many of those general comments here, while noting that submission of a comment only once by an entity, or repeated multiple times by that same entity in response to several questions, did not influence the manner in which the SDT considered the issue.

Measures

Some commenters had questions about the measures in the Version 5 standards, particularly regarding the use of "must" versus "may," and why there were differences of use in certain instances. The SDT tried to make a distinction by using the word, "must" for instances where the Responsible Entity "must" have something as evidence – variations are not expected to be acceptable. This would be the case for a requirement that says the Responsible Entity "shall" have a documented procedure – the entity must have that procedure to demonstrate compliance. Where the requirement says the Responsible Entity shall implement a documented procedure, then that entity must have the procedure. Since there are typically many ways of demonstrating "how" an entity has implemented a procedure, the word "may" has been used ahead of samples of performance that may be acceptable.

Furthermore, some commenters noted that some measures appeared technology specific, or specified that something must be "dated." The SDT tried to craft requirement language that speaks to results or to particular capabilities, without being technology specific; yet, the SDT fully realizes that certain technologies exist that serve to meet the requirements. The intent of any specific type of technology listed in the measures, which is generally limited, is to provide a non-inclusive example of high-quality evidence. The SDT contemplates that technology will change, and it did not want to specify certain technologies in the requirement language. Similarly, the word "dated" in the measure reflects a characteristic of high-quality evidence, but its use in the measure does not imply any additional obligation to the Registered Entity.

Initial occurrence of periodically required performance

In several instances in the Version 5 requirements, the SDT indicated certain periodic performance requirements, and they specified in the first posted draft's requirement language that the first iteration must be performed "initially upon

the effective date." Several commenters raised concerns with this language, and they suggested that not all initial performances should occur upon or before the effective date. The SDT agrees, and it has evaluated each periodic performance requirement. Furthermore, it has removed "initially upon the effective date" throughout the standards, and references to the initial performance in the requirements have been moved to the Implementation Plan as a separate section.

Technical Feasibility Exceptions

Some commenters asked whether the Technical Feasibility Exception ("TFE") process in the NERC Rules of Procedure, Appendix 4D, will be revised upon changes made to these standards. The SDT notes that requirements that require the submission of a TFE are identified in the NERC Rules of Procedure, and changes to that document are outside of the scope of this SDT. Historically, phrases such as "where/when technically feasible" have been considered trigger language for requirements necessitating a TFE when alternative measures are implemented. It is expected that the NERC TFE process will be modified to specify which requirements of Version 5's standards will require TFE submissions once the standards are finalized and submitted to the Commission.

Other commenters were concerned that "where technically feasible" suggests that an entity may unilaterally decide that a requirement does not apply, without filing a TFE. The SDT respectfully notes that entities are required to be compliant with all NERC reliability standards applicable to their function and Facilities. In some cases compliance is demonstrated by showing that the entity has no applicable assets; in other cases compliance is demonstrated through the TFE process. In no case does any language in a NERC reliability standard grant an exemption from compliance to applicable Responsible Entities.

Confidentiality of evidence used to demonstrate compliance

Some commenters questioned how they could demonstrate compliance when the subject matter may be high risk or confidential; inquiring how the SDT ensures that data will be protected. While outside the scope of this SDT, the SDT notes that the audit process requires strict adherence by auditors to confidentiality, which is part of the compliance process.

"As a minimum" and similar phrases

There were comments that suggested that phrases similar to "as a minimum" are not necessary; however, the SDT uses "as a minimum," e.g., in certain cases to distinguish from the concept of "exactly and no more," which the SDT does not intend. The SDT notes that most input to the drafting process by observers and through informal comment on this topic suggests that such a distinction is necessary for audit purposes.

Applicability

Some commenters asked for clarification on whether the rest of the Version 5 requirements applied if there was no determination of classification under CIP-002-5. The SDT intends that if a Responsible Entity determines that it does not have any BES Cyber Systems that meet CIP-002-5, Attachment 1 criteria, most of CIP-003-5 through CIP-011-1 would not apply to them (*but see* CIP-003-5, Requirement 2, as modified for the next formal comment period). Furthermore, applicability throughout CIP-004-5 through CIP-011-1 varies depending on BES Cyber System categorization under CIP-002-5, Attachment 1. Note, however, that BES Cyber Systems not categorized as 'high' or 'medium' impact are 'low' impact under CIP-002-5, Attachment 1. Responsive to FERC Order No. 706's directives concerning the NIST model, the Version 5 CIP standards require that all levels, including 'low' impact, receive some level of cyber security protection. Those are now programmatically covered under CIP-003-5, Requirement 2, in the next draft; so the SDT encourages each entity to evaluate carefully whether the standards apply to its own facts and circumstances.

Many commenters raised concerns over how the first draft of the Version 5 standards addressed low impact BES Cyber Systems. As discussed in the immediately preceding paragraph, the SDT agrees and notes that in the next posting of the CIP Version 5 standards, the 'low' impact requirements will be grouped together as one policy requirement, CIP 003-5, Requirement 2. The requirement specifies that Responsible Entities must address 'low' impact BES Systems at the policy/program level. Furthermore, and in recognition of the very significant volume of assets anticipated to be classified as "low impact," that requirement will be handled separately via the Implementation Plan, allowing approximately three years (one year longer than the rest of the requirements) for implementation.

The SDT notes that moving the 'low' impact requirements to one standard, along with extending the implementation period, mitigates some of the concern regarding costs to implement Version 5, particularly for smaller entities. The SDT has attempted to tailor requirements focused on results and a culture of security in support of reliability, and it believes that the system-level scoping throughout the requirements helps to accomplish that.

As to applicability, in response to several commenters' concerns, the SDT has modified the applicability sections of all of the CIP Version 5 standards so that they are consistent.

One entity repeated in almost all questions concern over the lack of an exemption in the Version 5 standards for smaller entities. With respect, the SDT emphasizes that there has never been an "exemption" specifically for small entities. In some cases, compliance can be achieved by taking an "exception" (e.g., non-routably connected assets) to the CIP standards, or by falling below compliance registry thresholds. However, Section 215 of the Federal Power Act does not allow exemptions from any reliability standards by anyone who qualifies as a "user, owner, or operator" of the "bulk power system." The proposal by the drafting team includes all BES Cyber Assets as in scope, but provides for

programmatic requirements for 'low' impact BES Cyber Systems, and accounts for gradated rigor or reach of the requirements for 'medium' impact assets, particularly between those with a routable connection and those without. Furthermore, the SDT has modified the standards so that CIP-004 through CIP-011 only applies to Responsible Entities having 'high' or 'medium' impact BES Cyber Systems. The policy-level requirements in CIP-003-5 still apply to all Responsible Entities. This, in part, addresses the directive in the FERC Order No. 706, Paragraph 25, to consider applicable features of the NIST Risk Management Framework, where it is fundamental that all BES Cyber Systems receive some level of protection.

Requirements for Documentation

Some commenters suggested that the Version 5 standards should not have any documentation requirements. In general, the SDT has endeavored to remove or minimize requirements that exist solely for purposes of creating documentation. However, there are other factors that support the use of requiring documentation in certain instances. The SDT has attempted to strike the appropriate balance. The SDT notes that many NERC standards require some level of procedure documentation to support the pre-thought responses to known conditions, or to ensure consistent responses when known events happen. Furthermore, certain documentation is essential to measure what needs to be secured. The SDT has sought to minimize such documentation requirements, and it has tried to provide detailed guidance. However, guidance alone is not a sufficient place for such documentation needs, as guidance is not mandatory nor enforceable.

Evidence Retention

Some commenters raised concerns about the evidence retention periods in the standards; to include concern that they are not the same as those in Version 4, that they increase the period from one to three years, or that they have a general misunderstanding over retention when the period between compliance audits may exceed the frequency stated. The evidence retention periods in the compliance section of the standards have been modified to make clear the expectation from the CMEP that entities have compliance evidence for the entire audit period. Furthermore, in some cases, compliance retention is different than records retention for the purpose of security analysis. The "requirement" level retention, where applicable, relates to maintaining records long enough to analyze them for security purposes, anomalous behavior, etc. The "compliance" retention, as specified in the Compliance section of the standard, deals with demonstrating that the requirement has been met (e.g., to demonstrate that the entity has maintained a "rolling" 90-day set of logs throughout the entire compliance audit period where the requirement specifies logging for 90 days). With respect to increases in the evidence retention periods from one to three years, the SDT notes that the initial evidence retention language pre-dates the establishment of the compliance program and its associated documented procedures. The NERC Rules of Procedure require that entities must "demonstrate compliance" for the entire compliance period (not that they must maintain all records for the entire compliance period). Note the distinction between demonstrating

compliance and maintaining all records noted in the requirements (e.g., again, to maintain records for 90 days for security analysis vs. demonstrating that records have been kept for a rolling 90-day period for an entire compliance period, whether three or six years).

'Annual' vs. 15 months

The SDT believes that some entities misunderstood the SDT's approach with respect to the SDT's attempt to provide flexibility to the industry on requirements that generally must be completed approximately every 12 months. Rather than specify exactly 12 months (or 365 days, etc.), which would create a very inflexible rolling period that would not allow for exception because of operational concerns, and which would not necessarily allow the use of a calendar reminder on the same day each year (e.g., because of weekends on the first or last day of the period), the SDT uses a convention of once per calendar year, not to exceed 15 months between occurrences. The SDT created this convention particularly because it appreciates the reality in implementing periodic requirements, and it believes that a short grace period beyond a strict 12 months makes the most sense. Nevertheless, some entities expressed concern that it would be difficult to implement a requirement on a 15-month period, that merely "annual" was preferred, or that the SDT should allow the convention explained in the CAN on the topic to govern.

The SDT believes that it has created a time convention that is practical and flexible. First, with respect to CANs, the CAN addressing "annual," CAN-0010, should not be necessary for Version 5, and the standards always supersede a CAN if different. As a general rule, a drafting team should always seek to provide sufficient clarity, such that using a CAN is not necessary. Thus, the SDT anticipates that CAN-0010's guidance on "annual" will not be applicable for these standards.

Next, the actual performance specified in the requirement language allows for the required performance to be performed generally on a 12-month cycle, which is not inconsistent with using a calendar reminder on the same date each year. The SDT included the 15-month time reference, however, specifically for the purpose of providing flexibility to Responsible Entities so that something that is generally accomplished on a 12-month schedule will not be in non-compliance if operating conditions, holidays, etc., cause the next period to occur slightly more than 12 months since the previous iteration. The alternative is an approach that does not contain such flexibility. In contrast, merely once per calendar year, or just "annually," allows for bookending that the SDT believes is contrary to reliability, as intervals that are too long affect the ability of the activity to protect reliability. Consider this example → Year 1 performance: January 1; Year 2 performance: December 31; Year 3 performance: January 1; Year 4 performance: December 31. In that example, the strict "once per calendar year" has been accomplished, and one might argue that the activity occurred "annually;" but in practice, almost 2 years elapse before immediate, quick succession performance in Years 2 and 3, and so on. The intent of the SDT is to accomplish these "annual" type performances on a schedule that approximates once every 12 months, while allowing some semblance of flexibility so that the requirement does not strictly require 365 days

between performances. There is absolutely and emphatically no preclusion in the standards for a Responsible Entity to harmonize its performance of these requirements to once every 12 months in a manner that makes the most sense to it (for example, every March 1), as long as the performance is accomplished once per calendar year, but not more than 15 months between occurrences. In this manner, the SDT has created a time parameter so that an entity can do precisely what some commenters suggest: automate a calendar reminder at the same time each year. But that same calendar reminder will not result in noncompliance if, for example, it falls on a Saturday and the Responsible Entity does not complete the performance until the next Monday; or during operational conditions for which conducting the performance risks instability, etc., the Responsible Entity waits until the operational condition has passed.

Definitions

Some commenters expressed a desire to maintain all legacy definitions in Version 5 on the basis that new terms require entities to dedicate resources in modifying existing policies, procedures, and evidence. The SDT appreciates this concern, and it has reevaluated changes to terms and reverted to previous terms in some cases. For example, the SDT has eliminated the "Defined Physical Boundary" term used in the initially-posted draft, and it reverted to the currently in-use "Physical Security Perimeter" term, albeit with a new definition for that term. However, the significant changes in response to addressing fully all of the remaining FERC Order No. 706 directives, along with adopting key features of the NIST risk management framework, do result in a paradigm shift in Version 5. To that end, and, for example, in the case of "Critical Cyber Asset" used in Versions 1 through 4, the conceptual changes in moving to "BES Cyber Assets" and "BES Cyber Systems" enable a more granular and appropriate scoping in Version 5 that render the use of the "Critical Cyber Asset" model inapplicable.

Consideration of NERC Quality Review Feedback

In addition to reviewing stakeholder-provided comments and modifying the standards in response to that consideration, the SDT submitted the ten standards and associated documents for a NERC Quality Review ("QR") in preparation for posting the draft Version 5 standards for formal comment and successive ballot. As a result of QR feedback, the SDT made substantive changes to improve the standards as described in the following paragraphs. The SDT also made several QR-suggested clarifying changes to conform grammar, style, and consistency throughout the standards, which are not individually described (e.g., rewording, consistency or terms, synchronization of Measures to Requirements, synchronizing listed rationales to Requirements and Requirement parts, hyphenation of certain words, numbering corrections to numbered lists, minimizing passive language, usage of commas in table references, confirming correct time horizons, typographical and grammatical corrections, updated Guidelines and Technical Basis sections of the standards, and other suggestions that are not as substantive in nature as the topics in the paragraphs that follow).

The QR noted that the mapping to previous versions, the VRF/VSL justifications, and the Version 5 Consideration of Issues and Directives documents were not complete. In response, the SDT revised those documents for accuracy and to match the revisions that accompany this posting.

The QR identified that the evidence retention sections of the standards varied and were not consistent with the suggested language in the Quality Review Background Document. In response, the SDT clarified the evidence retention periods and made that section consistent in all ten standards. In particular, the SDT clarified that for non-compliance, a Responsible Entity shall keep information related to the non-compliance "until mitigation is complete and approved . . ." as opposed to "until found compliant." The SDT also clarified that the evidence retention periods apply "for each requirement in the standard" for each standard.

The QR inquired about the CIP Cyber Security Standards' applicability to NERC and the Regional Entities. Specifically, NERC and the Regional Entities will not have any Facilities identified in CIP-002-5, attachment 1. Even though applicability to NERC and the Regional Entities would presumably be for purposes of protecting information submitted by the industry, because NERC or the Regional Entities are not users, owners, or operators of the bulk power system, that protection is not accomplished through application of the CIP standards. Rather, that protection is found in NERC's Rules of Procedure, Section 1500, and such protection applies regardless of applicability of the CIP standards to NERC or the Regional Entities. Since the Rules of Procedure provide for the protection that the SDT intended in originally proposing applicability to NERC and the Regional Entities, the SDT modified the standards' applicability sections to remove NERC and the Regional Entities.

The QR also identified language in the applicability section that referenced "required by a NERC or Regional Reliability Standard," where it was unclear whether the phrase applied to a protection system or to Transmission. The SDT clarified that the "required by . . ." language is in reference to a protection system.

The applicability qualifiers for Distribution Providers ("DPs") and Load-Serving Entities ("LSEs") were the same as those qualifiers in the Facilities section of the applicability sections. For clarity and brevity, the applicability qualifier for DPs and LSEs now reference the appropriate and corresponding Facilities reference rather than duplicating it. There are also many substantive changes in the Applicability section of the standards in response to concerns regarding Distribution Providers and Load Serving Entities. The changes clarify and ensure that only those systems owned by those functional entities that are material to BES reliability are within the scope of these standards.

In response to QR and industry comments, the SDT also reworked most of the VSLs in the standards. In general, and as described in the VSL question summaries, the SDT explains that it tried significantly to align the VSL language with the requirement language, and it also thoroughly reviewed binary VSLs to make them graduated where possible.

QR identified that the portions of the Background section of the standards explaining the applicability of the table items could be improved. Specifically, reference to mere "applicability" was potentially confusing, as there is an "Applicability" section of the standards. The SDT clarified in each instance that it means the "Applicability Columns in Tables," distinct from "applicability" of each standard as a whole. The SDT reviewed usage of applicability terms in the tables, and the SDT lists in the "Applicability Columns in Tables" section only those BES Cyber Systems and associated Cyber Assets for which a particular standard's tables apply. The SDT also moved the phrase relating to implementing common controls for multiple high and medium impact BES Cyber Systems from the "High Impact BES Cyber System" explanation into the more general background narrative.

The SDT clarified the purpose statements in all ten of the CIP standards in response to QR to clarify the reliability purpose of each standard. The SDT used the feedback from QR to reevaluate each standard in order to make each purpose statement conform to the correct style and form while specifying each standard's reliability-related benefit and tie to reliability principles.

In CIP-003-5, the QR identified several phrases that were unnecessary and unenforceable (e.g., "represents the Responsible Entity's commitment to the protection of . . ."). The SDT agreed and removed those phrases.

Removal of Restoration Facilities from CIP-002-5, Attachment 1's Medium Impact Rating (M)

The SDT notes that it has removed restoration facilities from CIP-002-5, Attachment 1's "Medium Impact Rating (M)" category. The SDT made this decision after receiving input from commenters, from industry, and following discussions about the issue as presented to NERC's Operating and Planning Committees. The SDT learned that Blackstart Resources face reduction because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool. Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed. The SDT explains this change in more detail in the Guidelines and Technical Basis section of the posted draft CIP-002-5.

QUESTION 1 - Definitions:

Many definitions in the Definitions document contain modified definitions from existing terms and new definitions for terms used in these standards. Do you have any suggestions that would improve the proposed definitions? If so, please explain and provide specific suggestions for improvement.

SUMMARY:

The SDT modified all of the definitions based on stakeholder comments. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity. Please see the redlined version of the definitions for a complete set of revisions to each definition.

BES Cyber Asset

Commenters requested that the drafting team consider revising the definition of BES Cyber Asset to consider the Facility the Cyber Asset is associated with, and the SDT has made changes to the definition to clarify that point.

Commenters noted concern that the term "adversely impact" is not well defined, and in response the SDT has made changes to the definition to further qualify this term with impact on the reliable operation of the BES.

Some commenters noted that the drafting team should consider removing the statement, "A Maintenance Cyber Asset is not considered part of a BES Cyber System," from the definition of BES Cyber System, since the definition of a BES Cyber Asset excludes Transient Cyber Assets, and modify the statement to exclude Transient Cyber Assets or to define "Maintenance Cyber Asset." In response, the SDT has removed undefined terms from the definition, and it has included the description of these devices as part of the definition itself. (Note that the SDT also removed "Transient Cyber Asset" as a defined term).

Commenters asked about the phrase "unavailable, degraded, or misused." These describe states of a BES Cyber Asset which could result from a Cyber Security Incident. Unavailable means that the BES Cyber Asset is unable to perform the service it is providing to the BES Facility, System, or equipment. Degraded means that it is able to provide the service, but in a degraded way (below specified capabilities). Misused means that it is being used for a purpose other than its designed use.

Commenters also asked about the phrase “when required.” The phrase “when required” is used in the context of a BES Cyber Asset: It is meant to distinguish between the time of the cyber security compromise, which could be earlier than the actual operation, misoperation, or nonoperation. The phrase means the time of the actual operation, misoperation, or non-operation when it is required to perform its designed operation. The drafting team has made changes to the definition which no longer uses this term, but uses “when needed” instead.

With respect to the 15-minute threshold, some commenters asked whether there is a need for a 15-minute test to “verify” the impact of the BES, and, if so, how an entity would demonstrate compliance. Furthermore, some commenters requested removal of the criterion. The SDT notes that, in using 15 minutes, it is attempting to articulate a time boundary for “Real-time” impact. The term “Real-time” in the Glossary of Terms used in NERC Reliability Standards did not provide enough specificity in the definition for this purpose. The SDT scoped the CIP standards to those Cyber Assets that would have an effect on Real-time operations. Misoperation or non-operation of systems that do not have a Real-time impact provide enough time for operators of the BES to perform mitigating, compensating, or corrective action to counteract the compromise. Some commented on the use of “could” versus “would” too, and the drafting team has discussed the use of both terms and has determined that the term “would” is the more appropriate term.

Some commenters requested removal of the second and third sentence in the previously posted definition of BES Cyber Asset because they do not provide clarity to the time frame stated above. The SDT has clarified and simplified the definition.

Some commenters noted concern with the applicability as applied to UFLS devices when those devices would not be BES Cyber Assets. The SDT notes that Section 4 specifies Facilities, Systems, and equipment. In the case of UFLS/UVLS, they include Elements (equipment) that provide the reliability tasks that are necessary to perform the functions of a Distribution Provider or Load Serving Entity, all tasks necessary for the reliability of the BES. The BES Cyber Assets are those Cyber Assets that support these elements for this function.

Commenters noted that the definition included a time frame qualifier that references sending or receiving "instructions to operate," and that such qualifier is too narrow (entities may take the stance that the BES Cyber Asset must be directly involved in a supervisory control function and would eliminate non-supervisory control systems, including those providing situational awareness, from designation as a BES Cyber Asset). The time frame qualifying term is no longer used in the amended definition.

Some commenters asked for changes from a perceived conflict that the third sentence that describes the 15-minute time frame relies on the asset being operational, yet the first sentence states that the asset may be rendered unavailable. The 15 minutes describes the time from the non-operation or Misoperation and the resulting impact on the BES. The

definition has been amended to clarify the distinction.

Some commenters noted concern with the definition's absence of "BES" relative to Reliability Operating Services, and the SDT notes that the term has been removed from the definition. BES Reliability Operating Services is no longer a defined term and has been moved to the Guidelines and Technical Basis section.

Some commenters asked for "BES Cyber Asset" to reinstate the phrase, "and causes a Disturbance to the BES" that was in earlier drafts approved by the SDT to clarify the phrase "adversely impacts." In response, the SDT reviewed the definition of Disturbance in the NERC Glossary and determined that the term was too broad for use in this context.

Commenters noted that the definition of BES Cyber Asset also includes a statement that redundancy shall not be considered when determining availability, and that the statement should be modified. The definition has been amended to use impact.

Commenters asked that the BES Cyber Asset definition take into consideration redundant systems in determining availability. The clause has been clarified to specify that redundancy is not used to determine impact. The purpose of the clause is to determine whether these systems are scoped in because of their "Real-time" impact. The Guideline and Technical Basis section discusses why redundancy is not considered for the purpose of cyber security vulnerability; and, therefore, the need for cyber security protection.
Some commenters asked for clarification on whether the drafting team's intent is for the definition to include auxiliary assets related to Facilities where the assets reside (e.g., Fire systems, HVAC, Halon system, etc.). In response: No, these do not directly support (BES) Facilities, Systems, and equipment that perform a BES reliability function. They may be included, however, if they meet qualification for other types of Systems that must be protected under CIP (e.g., in the same ESP).

Some commenters asked for a different category for assets that can be misused versus those that can only be rendered inoperable. The SDT notes that, from the impact determination standpoint, it does not make a difference whether they are unavailable or misused: Each has a potential and different impact that determines its categorization with the high watermark principle (worst impact).

Many commenters proposed the SDT abandon this definition and revert back to the existing Critical Cyber Asset term and its definition. The term Critical Cyber Asset was used in Versions 1, 2, 3, and 4 in an "in or out" paradigm. Version 5 uses a multilevel categorization where the use of this legacy term is inappropriate.

In various other capacities, some commenters indicated difficulty understanding certain aspects of the definition. The SDT notes that the definition has been amended since the last formal comment period in response to comments, and the

SDT believes that it is now simpler and clearer.

Some commenters asked the SDT to add the statement, "Support Systems, such as voice communication (e.g., 900 MHz radio System), ventilation, power supply systems, and similar supporting systems are not considered BES Cyber Assets." However, these do not directly support (BES) Facilities, Systems, and equipment that perform a BES reliability function. They may be included if they meet qualification for other types of Systems that must be protected under CIP (e.g., in the same ESP).

Based on these comments, the SDT has revised the definition as follows:

> A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation~~, when required~~, adversely impact one or more ~~BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in~~Facilities, Systems, or equipment, which~~ that~~, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation ~~occurs and impacts~~of the ~~BES~~Bulk Electric System. Redundancy of affected Facilities, Systems, and equipment shall not be considered when determining ~~availability.~~ adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A ~~Transient~~Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset ~~is not considered~~ within an ESP, or to a BES Cyber Asset~~.~~, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

BES Cyber Security Incident

For BES Cyber Security Incident, most individuals or organizations that commented indicated an overall vagueness of the definition because of the terms "attempt to disrupt" and "suspicious event." They commented that these terms are too subjective. In response, we note the proposed definition does not significantly modify the glossary definition. In addition, we are reverting to the previous term "Cyber Security Incident" based on other commenter feedback and to align with the EOP-004-2 drafting effort. There is not at this time a compelling need to significantly modify or introduce new terminology in the existing definition. The triggering langue, "disrupt or attempt to disrupt," must also be read in context with the qualifying phrase of "a malicious act or suspicious event." While this does not provide absolute certainty in the compliance evidence to demonstrate whether or not an act or event was a Cyber Security Incident, there must always be a degree of subjectivity in the entity's understanding of what constitutes a BES Cyber Security Incident.

Based on these comments, the SDT has revised the definition as follows:

~~BES~~ Cyber Security Incident

~~Any~~A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter ~~of a Critical Cyber Asset,~~ or~~,~~
- Disrupts, or was an attempt to disrupt, the operation of a ~~Critical Cyber Asset~~ BES Cyber System~~, or~~.
- ~~Results in unauthorized physical access into a Defined Physical Boundary .~~

BES Cyber System

Commenters noted concern with the distinction between BES Cyber Asset and BES Cyber System, and that the similarities created confusion between what is a "System" and what is an "asset." Furthermore, there was confusion over whether each BES Cyber Asset must be part of a BES Cyber System, or if BES Cyber System can include other assets or communications equipment. The SDT has thoroughly reviewed all comments on the issue, and it amended both definitions to make them clearer. The SDT has also made the relationship between BES Cyber Assets and BES Cyber Systems clearer. Additionally, it is now clear that every BES Cyber Asset must be part of a BES Cyber System. Whether the BES Cyber System includes Cyber Assets and communication equipment depends on how the BES Cyber System is defined. The Responsible Entity has discretion on how BES Cyber Assets are grouped, as long as they meet the definition of a BES Cyber System; including the option of defining BES Cyber Systems that only include a single BES Cyber Asset.

Some commenters noted that the loss of Critical Assets removes Facilities from consideration, presenting challenges in assessing BES Cyber Systems as they provide services to a Facility which provides BES Reliability Operating Services - not the BES Cyber System independently. The SDT notes that BES Reliability Operating Services is no longer a defined term, and the SDT has removed it (referencing functional tasks of the functional entity instead). Furthermore, for clarity, the definition of BES Cyber Asset now includes Facilities, Systems, and equipment as part of the definition.

Finally, some commenters noted concern with how one determines if Cyber Assets are "typically grouped together," particularly in the rapidly evolving security field, and they noted the absence of logical groupings in the definition. The definitions of both BES Cyber Assets and BES Cyber Systems have been modified for better clarity and include the concept of logical grouping to support a reliability functional task by a functional entity.

Based on these comments, the SDT has revised the definition as follows:

One or more BES Cyber Assets ~~that are typically grouped together,~~ logically ~~or physically,~~grouped by a responsible

entity to ~~operate~~perform one or more ~~BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System~~reliability tasks for a functional entity.

BES Cyber System Information

The SDT received several comments about the definition of BES Cyber System Information, and a primary concern was that "BES Cyber System Impact" was not a defined term. The SDT agrees and modified "impact" to be lower case. Additionally, the SDT received numerous concerns about specific items included in the list of items that defined BES Cyber System Information. A few comments, however, pointed out that there was not, in fact, a definition, but only a list of examples. The SDT agreed and modified the definition clarifying that BES Cyber System Information includes information "…that could be used to gain unauthorized access or pose a security threat to the BES Cyber System."

Based on these comments, the SDT has revised the definition as follows:

> Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. Examples of BES Cyber System Information may include, but are not limited to, security procedures developed by the responsible entity and security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements.~~Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans.~~

BES Reliability Operating Services

Several commenters commented that BES Reliability Operating Service needs more information for clarity as a defined term; that it is too broad, or that it uses language that many unintentionally result in overreach of the standards. Several commenters also asked for clarification of several components, whether the time horizons (which are in the NERC document "Time Horizons") or with particulars of several of the specifically listed services. Commenters also noted that

there needed to be clarity in the relationship to its use of terms with the functional model. In response, BES Reliability Operating Services is no longer a defined term, and has been moved to the Guidelines and Technical Basis section as guidance for Responsible Entities. The SDT has included in the definitions of BES Cyber Assets and BES Cyber Systems the concept that each BES Cyber Asset must be part of a BES Cyber System, and the relationship of the BES Cyber System with reliability functional tasks for functional entities. Situational analysis and decision making would be initially scoped as components necessary for the functional tasks and will be further scoped by the "Real-time" operations filter in the definition of BES Cyber Assets.

CIP Exceptional Circumstance

The SDT received a small number of comments regarding the definition of CIP Exceptional Circumstances. These comments consisted of requests for additional circumstances to be added to the definition. The SDT appreciates that it cannot be sure of all situations that may arise. As such, it has modified the definition to more closely tie it to safety and BES reliability. Additionally, it has added the case of "an imminent or existing hardware, software, or equipment failure" in consideration of the comments from industry that equipment may fail in ways that are not planned.

Based on these comments, the SDT has revised the definition as follows:

> A situation that involves one or more of the following, or similar, conditions~~:~~ that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.

CIP Senior Manager

The SDT received a number of comments indicating that the definition of CIP Senior Manager should reference the specific standards for which it is applicable. The SDT notes that the term is only applicable where it is specifically used in the standards. Additionally, the concern appeared to specifically reference CIP-001, which is currently planned for retirement.

Control Center

Commenters were concerned that the definition was too broad, either generally, with respect to location, or by the inclusion of "by System Operators," and that the drafting team should clarify if it is the intent to only include the Control Center with the primary responsibility for maintaining reliability of the BES and performing one or more of the functions that support Real-time operations by System Operations. Other commenters were concerned about whether it only applies to BA, TOP, GOP, or RC, and that without specifying, it could unintentionally include certain field assets. The SDT

has modified and clarified the definition in response to these concerns by specifying, ". . . operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability functional tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generation Operator for generation Facilities at two or more locations."

Some commenters also expressed concern about use of "facilities" in lowercase. The SDT uses facility in the generic sense (not the NERC Glossary term) of a location or site, and then specifies the capitalized term "Facilities" with respect to Transmission Facilities or generation Facilities (as noted in the preceding paragraph.)

Some commenters were concerned about generation Facilities that control small remote units at different footprints being part of the definition (that the units collectively may be significantly under the 300 MW threshold, as indicated in 2.13, and present no risk to the BES). The SDT notes that generation Control Centers are only categorized as medium if they control an aggregate of more than 300 MW.

Some commenters noted that Transmission Owners do not have Control Centers (and that TOPs-have Control Centers). The SDT has modified the definition of Control Center to address this comment. The new definition does not include Transmission Owner, but does specify that it includes Control Centers performing the reliability functional tasks of a Transmission Owner: Transmission Owner Control Centers may be delegated certain tasks through agreements with Transmission Operators. (See Guideline and Technical Basis section.)

Some commenters asked the SDT to include "situational awareness" in the fourth item. Instead of adopting that specific suggestion, note that the SDT has made other modifications to the definition of Control Center that address this comment. The new definition now refers to the reliability functional tasks of BAs, RCs, TOPs, and GOPs.

Some commenters questioned whether Control Center needs to be defined, and were concerned about confusion with use of lowercase "control center" in other standards (e.g., EOP-008-1). Control Centers is used throughout all CIP standards. These terms are capitalized in the standards to refer to the proposed NERC Glossary defined term. Other standards use the generic term "control center," which does not refer to the (proposed) NERC Glossary defined term. Other standards can use the current proposed term in their future versions, or may make modifications subject to stakeholder vetting. The SDT expects that the defined term will not apply to standards that already use "control center" (lowercase) without this stakeholder vetting.

Based on these comments, the SDT has revised the definition as follows:

> One or more facilities hosting ~~a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions~~operating personnel that ~~support~~monitor and control the Bulk Electric System (BES) in real-time ~~operations by System Operators~~to perform the reliability functional tasks of: 1) a Reliability

Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more ~~BES~~locations, or 4) a Generation Operator for generation ~~facilities or transmission facilities,~~Facilities at two or more locations~~:~~

~~• Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,~~

~~• Inter-utility exchange of BES reliability or operability data,~~

~~• Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES,~~

~~• Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function,~~

~~• Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES~~

~~• Coordination of BES restoration activities~~.

Cyber Assets

Some commenters requested the term be singular, but the SDT notes that the term is already in the Glossary of Term used in NERC Reliability Standards.

Some commenters asked about "programmable" with respect to electronic device. The SDT notes that it is an electronic device which can execute a sequence of instructions loaded to it through software or firmware, and configuration of an electronic device is included in "programmable." Depending on the scheme used, these instructions may include data, or data that must be processed to execute these instructions.

Some comments expressed concern that the removal of "communication networks" from the definition might cause some to not include communication devices, or that the removal eliminates a protection of data in motion. There is no exclusion of communication devices in the definition. As long as the electronic device meets the definition, they are Cyber Assets. Furthermore, there is no specific requirement to protect data in motion within the Electronic Security Perimeter, hence no expectation of compliance to a requirement that does not exist. A FERC-approved interpretation addressed the specific case of separate physical security perimeters within an Electronic Security Perimeter, and it addresses the alternate physical protection measures required in CIP-006-3. Physical access requirements now apply to BES Cyber Systems.

Other commenters asked to retain "and communication networks" because of concern that any programmable device at

a location (e.g., within a substation) is a Cyber Asset regardless of whether they communicate to it or is used for communications, and that Cyber Asset devices that are not programmable via communications should be excluded. The SDT notes that any device that meets the definition is a Cyber Asset. The intent of the SDT is to include all such devices: Communication and connectivity considerations are included in the Applicability column of requirements and their parts, not the definition. Communications is not a pre-requisite for compromise of a Cyber Asset. However, note that BES Cyber Systems that do not have External Routable Connectivity are excluded from certain requirements.

Some commenters indicated that "Cyber Asset" should not include any portable memory devices such as USB memory devices, CDs, etc. The SDT notes that those are not specifically included unless they meet the definition of "Cyber Asset," including that they are programmable (i.e., capable of executing a set of instructions). Furthermore, commenters asked about legacy Remote Terminal Units (RTU's) with eproms, and they are typically considered programmable devices (programs/data are typically loaded into memory for execution).

Based on these comments, the SDT has revised the definition as follows:

> Programmable electronic devices, ~~and communication networks~~ including the hardware, software, and data in those devices.

Defined Physical Boundary ("DPB")

The preponderance of the comments received on the term Defined Physical Boundary (DPB), indicated a preference to return to the more familiar industry term of Physical Security Perimeter (PSP). Although the drafting team initially chose DPB to help entities recognize the changes from the original PSP definition, the standards have been modified to use the original PSP term with a revised definition, and the proposed definition of DPB has been deleted. Even with the reversion to PSP, the drafting team wants to address the challenges with the completely enclosed "six-wall" border, especially in field locations, and the definition no longer retains the "six-wall" border concept. The intent of this definition change is to focus on the controls put in place to restrict access, rather than solely focusing on the PSP and a boundary protection model for physical security.

Based on these comments, the SDT has revised the definition of Physical Security Perimeter as follows:

> **Physical Security Perimeter ("PSP")**
> The physical ~~, completely enclosed ("six-wall")~~ border surrounding ~~computer rooms, telecommunications rooms, operations centers, and other~~ locations in which ~~Critical Cyber Assets are housed and~~ BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside, and for which access is controlled.

Electronic Access Control or Monitoring Systems

Some commenters asked the SDT to split the definition to define electronic access control and electronic monitoring systems separately. Others commented to drop the "or monitoring" from the term. The SDT considered that approach but disagrees, as these Systems are grouped together for the purpose of requirement applicability. There are no requirements that would apply to one but not the other, therefore the SDT maintains the definition as one for simplicity. In all previous versions of the standards, these systems were called "Cyber Assets used in access control and monitoring." The SDT is simply taking this otherwise 'on the fly' definition of a class of assets within a requirement in Versions 1 through Versions 4 and making it a defined term for Version 5.

Some commenters asked the SDT to delete or remove the "or BES Cyber Systems" from the definition, as it is broader than the usage of the term in the standards and could imply applicability to low impact BES Cyber Systems. The SDT disagrees because a definition is just that: It is defining what an EACMS is, not providing the scope of requirements applied to the defined object. The scope of applicability of requirements is handled in each standard itself, not in the definition of the object. As previous versions had monitoring requirements in CIP-007 at the Cyber Asset level that continue in this version, we cannot remove this from the definition without reducing the scope of today's standards.

A few commenters thought the definition was too vague as to its scope and that it needs a comprehensive list or bright-line criteria. The SDT has taken this definition out of the requirements that have been in CIP-005 since Version 1. The SDT agrees that the term is broad, but reflective of its overall approach in Version 5, it is opposed to creating comprehensive lists of current technology items, as they can quickly become outdated. The SDT prefers to stick with a definition based on the function of the technology. The SDT addressed vagueness by changing the word 'used' to 'that performs,' and it added clarification that it is 'electronic access control' and 'electronic access monitoring' to clearly denote that the scope does not include all types of monitoring.

Based on these comments, the SDT has revised the definition as follows:

> Cyber Assets ~~used in the~~that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems.

Electronic Access Point ("EAP")

Commenters noted concern with EAPs being an interface that restricts communication, and several comments suggested that the definition become more focused on 'crossing an ESP.' Many rightly pointed out that an EAP could be required for communications even between systems within an ESP, which was not the SDT's intent. The SDT agreed and has

rewritten the definition to focus on the fact that EAPs are Cyber Assets that reside on an ESP and allow communications across the ESP.

The SDT has not included serial, non-routable communications within the definition of EAP (other than with respect to dialup in CIP-005 R1.4). Dedicated serial communications are intentionally left out of scope, as the SDT believes it would be inappropriate for the standards to mandate a universal perimeter or firewall type security across all entities and all serial communication situations. There is no 'firewall' capability for a RS232 cable run between two cyber assets. Without a clear security control that can be applied in most every circumstance, such a requirement would just generate TFEs.

Several comments pointed out that the definition did not require ALL external communication interfaces to be included. It would be inappropriate to add this to the definition, as requiring EAPs and ESPs and specifying what they must do is in CIP-005-5, not in the definition of each term.

Based on these comments, the SDT has revised the definition as follows:

> ~~An~~ A Cyber Asset interface on ~~a Cyber Asset~~ an Electronic Security Perimeter that ~~restricts~~allows routable ~~or dial-up data communications~~communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Electronic Security Perimeter ("ESP")

Most comments concerned the change to a 'collection of points' based definition for a 'perimeter' and asked for additional clarity. The SDT agreed and has rewritten the definition based on the legacy definition of a logical border. Several comments pointed out that the definition did not require ALL external communication interfaces to be included. It would be inappropriate to add this to the definition, as requiring EAPs and ESPs and specifying what they must do is in CIP-005-5, not in the definition of each term.

Based on these comments, the SDT has revised the definition as follows:

> The logical border surrounding a network to which ~~Critical Cyber Assets~~ BES Cyber Systems are connected using a routable protocol ~~and for which access is controlled.~~
>
> ~~A collection of Electronic Access Points that protect one or more BES Cyber Systems~~.

External Connectivity

The comments indicated that there was confusion about the scope and use of External Connectivity, uncertainty surrounding whether the term included serial communication, and commenters concerns about the relationship between

External Connectivity and External Routable Connectivity. All uses of this term have been eliminated within the standards, and the proposed glossary term has been deleted completely.

External Routable Connectivity

Commenters noted concern that the definition took an "outside-in" only view of communications. The SDT has added the term 'bi-directional' to the proposed definition to clarify that any bi-directional communications path is included, regardless of the initiating side.

Commenters suggested that the SDT define 'routable protocol' and maintain a list of non-routable protocols, as per some of the NERC Guidelines. The SDT disagrees, as a guideline outside of the standards development process is the proper place to maintain such types of ever-changing information.

Based on these comments, the SDT has revised the definition as follows:

> ~~The~~A BES Cyber System that is accessible from ~~any~~a Cyber Asset that is outside its associated ~~ESP~~Electronic Security Perimeter via a bi-directional routable protocol connection.

Interactive Remote Access

Commenters' primary concerns regarding Interactive Remote Access were: 1) clarification of "interactive" access; 2) read-only remote access; and 3) ownership of Cyber Assets performing remote access.

Commenters noted concerns with the concept of asset ownership being included in the definition of Interactive Remote Access. The concept of asset ownership was included in the definition to provide an understanding that remote access is to have the appropriate protections applied, regardless of who owns or uses the system initiating the Interactive Remote Access session. Changes were made to the definition to add "use" along with owned. This is to assist those entities that lease equipment.

Comments were provided requesting a definition of "interactive" access. The definition of Interactive Remote Access has been updated to clarify that access is user-initiated access by a person. Interactive Remote Access has been clarified that this does not include system-to-system process communications. Additionally, the SDT updated the definition to use the term "routable" in the place of "network-based" to be more consistent with other requirements and definitions.

Commenters requested that read-only access to BES Cyber Systems be excluded from Interactive Remote Access. Because of the open channels that are needed, read-only access cannot be excluded.

Based on these comments, the SDT has revised the definition as follows:

~~Any~~All user ~~interactive~~-initiated access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether ~~network-based~~routable or dial-up access~~.~~, using a client or remote access technology. Remote access ~~can~~may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Intermediate Device

Commenters noted concern over the location of the device. To clarify, the definition has been modified to require that the device must not be located inside the Electronic Security Perimeter. This allows for the appropriate termination of the required encryption and authentication prior to allowing access into the Electronic Security Perimeter.

Commenters also noted concern with the required protections of the Intermediate Device. The definition has been updated to specify that the Intermediate Device performs access control.

Additionally, comments were provided regarding the use of the terms DMZ and proxy. These terms have been removed.

Based on these comments, the SDT has revised the definition as follows:

A Cyber Asset ~~that 1) may be used to provide the required multi-factor authentication for the interactive remote~~or collection of Cyber Assets performing access~~; 2) may be a termination point for required encrypted communication; and 3) may~~ control to restrict ~~the interactive remote access~~ Interactive Remote Access to only authorized users. The Intermediate ~~devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may~~Device must not be located ~~outside~~inside the Electronic Security Perimeter~~, as part of the Electronic Access Point, or in a DMZ network.~~.

Physical Access Control Systems

There were not many comments received on this definition. Of those received, several were actually related to the use of the term "Defined Physical Boundary" in the definition, and that term has been changed back to Physical Security Perimeter. One comment indicated the definition was acceptable as written. Another comment asked for the inclusion of cameras in locally mounted exclusion list, but the drafting team believes this is not necessary since the list is not all-inclusive. However, the drafting team has further clarified the exclusion of locally mounted devices to only those that do not contain or store access control information or independently perform access authentication.

Based on these comments, the SDT has revised the definition as follows:

> Cyber Assets that control, alert, or log access to the ~~Defined~~ Physical ~~Boundary~~Security Perimeter(s), exclusive of locally mounted hardware or devices at the ~~Defined~~ Physical ~~Boundary~~Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Protected Cyber Asset

In limiting the definition to routable protocol connectivity, commenters suggested that relays and other devices in a substation or generating plant that are serially connected would not fall under this definition. The SDT agrees they would not be PCAs under this definition; however, such devices would be part of a BES Cyber System in and of themselves and not out of scope.

Some comments requested that this be defined as 'non-critical cyber assets'. The SDT believes this term is not descriptive enough, as every other Cyber Asset in existence could be considered a non-critical cyber asset. The SDT has chosen the term Protected Cyber Asset as a more descriptive term, as these are the Cyber Assets within an ESP, and by their proximity and direct connectivity to BES Cyber Systems, they must be protected in much the same way as the BES Cyber System itself.

The definition was also changed in response to comments concerning how to handle a mixture of varying impact BES Cyber Systems within a single ESP. The definition now considers all Cyber Assets connected with a routable protocol within an ESP that are not a part of the highest impact BES Cyber System to be PCAs of that BES Cyber System.

Based on these comments, the SDT has revised the definition as follows:

> A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System~~. A Transient~~ within the same Electronic Security Perimeter (a Cyber Asset is not ~~considered~~ a Protected Cyber Asset~~.~~ if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset within an ESP or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes).

Reportable BES Cyber Security Incident

For Reportable BES Cyber Security Incidents, many commenters did not agree with the referenced BES Reliability Operating Services definition. In response, we have replaced the term with "reliability tasks of a functional entity."

Based on these comments, the SDT has revised the definition as follows:

Reportable ~~BES~~ Cyber Security Incident

Any ~~BES~~ Cyber Security Incident that has compromised or disrupted ~~a BES Reliability Operating Service.~~ one or more reliability tasks of a functional entity.

Transient Cyber Asset

The SDT has removed this definition as a standalone term from the proposed glossary terms, and has included it as an aspect of the definition of BES Cyber Asset.

The intent was to take Cyber Assets that are temporarily connected to BES Cyber Systems and exclude them from becoming part of the BES Cyber System. The SDT agrees that TCAs pose some level of risk. However, the SDT believes that considering them as BES Cyber Assets is not the solution. These are normally portable maintenance and diagnostic tools, which by their very nature cannot meet all the requirements mandated for BES Cyber Assets, such as a fulltime physical security perimeter, or wiping all information when it is 'redeployed' to another location when the purpose for its existence may be to bring back field data for analysis. The SDT does not intend for the CIP requirements to make impossible or impractical normal practices that increase reliability of the BES, such as being able to use Cyber Asset based tools for diagnostics and maintenance, especially among numerous field assets.

The SDT, in an attempt to define 'temporarily connected,' has replaced that concept with 'less than 30 days' to give some measurable boundary to the term. The SDT acknowledges that there is no perfect definition that will cover every conceivable circumstance, such as the "one minute disconnect."

The SDT agrees that the 30-day time frame should be clarified; that it is 30 'consecutive' days, and has made the change. The SDT has also incorporated suggestions that the connections could be made not only to another Cyber Asset, but also to the network within the ESP.

The SDT believes external (not directly connected) Cyber Assets are addressed through CIP-005-5' EAP and Interactive Remote Access requirements. The SDT is focusing on those primarily maintenance and diagnostics devices that are indeed 'directly' connected to the system within the ESP.

Some commenters wanted more examples within the definitions. The SDT disagrees, as confusion regarding examples within definitions or requirements tend to be interpreted as prescriptive lists.

QUESTION 2 – CIP-002 Attachment 1:

CIP-002-5 Attachment 1 contains criteria that provide the basis for the categorization of BES Cyber Systems and BES Cyber Assets. Most of these criteria are similar to those already approved by the industry as part of Version 4. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Attachment 1. The explanations below describe the responses the drafting team provided to commenters, along with the modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity. The last section of this question's summary provides general comments for Question 2 along with the drafting team responses.

Criteria 1.1 to 1.4 (Control Centers)

One comment was that the Impact Rating of a control center should be linked to the Impact Rating of the facilities that the control center controls. If a control center only controls Low Impact facilities, it makes no sense for the control center to be rated at a Medium Impact Rating. The drafting team responded that, by definition, the Control Center controls more than one facility. For Transmission Control Centers, if the Control Center performs the functional obligations of a Transmission Operator, then it does so for more than a single facility and its impact is therefore more than a single Low Impact facility. The SDT believes that these Control Centers should be subject to the requirements for Medium Impact systems.

One commenter stated that it would be good to include some reference or example that relates to a Registered Entity that does not own generation, but provides services to those who do. The drafting team agreed and modified the definition of the Control Center to refer to real-time reliability tasks for applicable functional entities from the functional model, which includes those necessary for situational awareness.

Another suggestion was to delete " ... that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services ..." in the introduction of High Impact Rating, since the phrase is included in the definition. The drafting team responded that it agreed and included this suggested change in the new draft.

Another comment was that there is no explanation why a BES Cyber Asset (BES Cyber System) located at the Control Center would have higher impact than another BES Cyber Asset (BES Cyber System) located outside the Control Center.

The drafting team responded that a Control Center controls assets at more than one location. A compromise of the Control Center has the potential to impact multiple assets simultaneously, which means they have a higher potential impact on the BES.

Another comment was that a Control Center for very small BAs being High Impact is inappropriate. The drafting team agreed and included this suggested change in the new draft.

Another comment was that Transmission Owners do not have Control Centers and should be struck from Criterion 1.3. The drafting team agreed and included this suggested change in the new draft.

Another suggestion was to substitute the word "criteria" with the word "section" in Criterion 1.3 and 1.4 for clarity purposes. The drafting team agreed that clarity was needed and changed the language to use “parts” instead of “criteria”.

Another suggestion was that in criteria 1.3 and 1.4, the phrase “that includes” should be changed to “is limited to” in order to not leave these criteria completely unbounded. The drafting team responded that it believes that the language correctly conveys that the “functional obligations” must include the items specified for the criterion to apply. The proposed language implies that the functional obligations are limited to the items specified.

Another commenter noted that there appeared to be an error in category 1.4 where it references 2.12 (UFLS and UVLS). To match version 4 the cross-reference should be to 2.11 (Special Protection Systems). The drafting team agreed and included this suggested change in the new draft.

Another comment was to change the phrase "...that includes control of one or more of the assets..." in criterion 1.4 to match the definition of Control Center, which requires the control of two or more assets. The drafting team responded that the definition of the Control Center requires control of 2 or more assets irrespective of their impact rating. An additional qualifying criterion for a MW threshold of 1500 has been included as well. Criterion 1.4 will result in the categorization of High if at least one of those assets meets the qualifications specified.

Another commenter stated that the definition of BES Cyber System that can impact BES Reliability Operating Services would force the inclusion of RTU’s, Governors, Power System Stabilizers and Protective Relaying. The drafting team responded that it agreed that it is intended that these types of devices (RTUs, relays, etc.) are included if they meet the definition of BES Cyber Assets.

Another commenter stated that the High Impact Rating criteria do not consider the inter-connected nature of the BES Cyber Assets or BES Cyber Systems when defining threshold-based criteria. BES Cyber Assets and BES Cyber Systems that interconnect with similar systems in other Control Centers should be afforded a High Impact Rating regardless of the

"span of control" of other BES Cyber Assets and BES Cyber Systems supporting that Control Center. The drafting team responded that using inter-connections as an impact criterion ultimately scopes in all interconnected systems in a single impact level. The concept of mutual distrust and security zones and perimeters implements cyber security boundaries that allow the selection and implementation of cyber security controls commensurate with the level of impact within a security boundary.

Another commenter noted that Criterion 1.4 does not consider an aggregate span of control. A generation control system could theoretically control 15,000 MW of generation without a single asset meeting the thresholds defined in the referenced criteria. The overall span of control of the BES Cyber Assets and BES Cyber Systems need to be considered by aggregating the field assets being controlled. The drafting team responded that it agreed and included this suggested change in the new draft.

Another suggestion was that it would help if section 1.4 clearly defined what level of control of generation would require classification as a 'High' impact. In some case a control center may have limited 'base point' setting capability for assets under section 2.1. The drafting team responded that the criterion has been modified to address the concern.

Another commenter stated that for Attachment 1, Item 1.3 and 1.4, the criteria for determining which control centers should be under the high category, the 2.4 Black Start Resources should be under Transmission Operator Control Centers not under Generator Operators since, under the EOP standards during Restoration, such units are under the control of the TOP, not the GOP/BA. The drafting team responded that it has eliminated the Blackstart Resources from these criteria, which is explained under Criterion 2.4 and 2.5's response.

Criterion 2.1 (Generation Plant)

Some commenters stated that although it is not delineated as such, it is implied that BES systems that are shared and control more than 1500 MWs collectively would be in scope. This should be clearly stated. If the intent is to include all BES systems for a facility that collectively produces 1500 MWs, then this should be clearly stated as such. The drafting team responded that it changed the criterion to clarify the situation.

Another commenter stated that since Interconnection is a defined term that is not applicable to this discussion, please remove the capitalization of the term "Interconnection" in this context, and change "in a single Interconnection" to "at a single interconnection". The drafting team responded that the use of the glossary term is correct: the 1500 MW threshold applies to generation in a single Interconnection. A generation plant may service multiple Interconnections.

Another suggestion was that Criterion 2.1, with its historical nature, needs to account for decommissioned generating units by adding "commissioned" or "active" to the beginning of the criteria. The drafting team responded that it agreed

and included this suggested change in the new draft.

Another commenter suggested that the threshold in the Medium Impact category for generation should be 1,000 MW instead of 1500 MW. The drafting team responded that the determination of the thresholds are derived in large part from version 4, which has been vetted by the industry, and was drafted with assistance from subject matter experts in the relevant operating areas.

Another commenter stated that the value of 1500 MW should be defined as either the nameplate or the continuous "rated" capability (where the equipment has been de-rated by the Responsible Entity for age/reliability). The drafting team responded that the criterion's MW value is based on a required rating measurement that must be submitted to the Regional Entity.

Another commenter stated that Criteria 2.1 and 2.13 should distinguish between controllable generation and intermittent generation sources (i.e., wind and solar), since the loss of intermittent generation facilities happens naturally and regularly and is not viewed as an extreme event. The drafting team responded that, while the unavailability of intermittent generation (vs. controllable generation) may not be considered an extreme event, the impact of misuse of the associated BES Cyber Systems due to a cyber security compromise can result in BES disturbances. The impact criteria provide a measure of this impact.

Criterion 2.2 (Reactive Resource)

One suggestion was that "Net Reactive Power" should be read as "Absolute value of Reactive Power" to consider Static VAR compensator and synchronous condenser. The drafting team responded that the word "net" has been removed, since the nameplate value is specified as the value to be used for aggregation.

Another commenter stated that the former version had BES in front of Reactive Resource. The term BES should be restored to make clear that this is transmission level as stated in the application notes. The drafting team responded that it agreed and included this suggested change in the new draft.

Criterion 2.3 (Adverse Reliability Impact)

One commenter asked: What is meant by this criterion? How will it apply? The drafting team responded that this criterion is intended to include generation facilities that are designated as "must run" for reliability reasons, not market reasons.

Section 2.3 in Attachment I, may be problematic as it potentially allows Planning Coordinators or Transmission Planners to "arbitrarily" move GO and GOP entities from Low to Medium should the unit be identified as reliability must-run unit. The drafting responded that is has clarified the language to "to avoid BES Adverse Reliability Impacts in the planning

horizon of more than one year." The drafting team believes that this change addresses the concern.

Another commenter recommended deleting "or Transmission Planner" to ensure that only one entity is responsible for designating appropriate generation. The drafting team responded that this standard does not determine who does the designation. Designations may be issued by either of these entities, depending on the region's practice.

Another commenter expressed concern that there is a need to clarify the role and responsibility of PC, TP, GO, GOP, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal? The drafting team responded that other NERC Reliability standards already define the obligations of these entities with respect to these criteria. Once identified, the Responsible Entity owning these Facilities, Systems and equipment is responsible for compliance to the CIP standards of the associated BES Cyber Systems.

Another expressed concern was that Criterion 2.3 uses the phrase "long-term planning horizon" which is later defined as one-year or longer. It would be better if the time horizon was defined with a number of years, otherwise it would be hard to have it audited. The drafting responded that is has clarified the language to "to avoid BES Adverse Reliability Impacts in the planning horizon of more than one year." The drafting team believes that this change addresses the concern.

Another commenter asked for the definition of BES Adverse Reliability Impact. The drafting team responded that Adverse Reliability Impact is a NERC Glossary defined term. The most recent BOT approved definition is "The impact of an event that results in Bulk Electric System instability or Cascading." The currently approved FERC definition is "The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection."

Another commenter stated that Criterion 2.3 creates an implied obligation on the Planning Coordinator (PC) or Transmission Planner (TP) to designate generation that is necessary to avoid BES Adverse Reliability Impacts. The drafting team replied that there is no implied requirement for PCs or TPs to designate "must run" generation to avoid Adverse Reliability Impact. The criterion is merely stating that when such a TP or PC does designate such generation, the BES Cyber Systems for that generation is subject to the CIP requirements.

Another commenter stated that the use of BES as a descriptor of Adverse Reliability Impact in Criterion 2.3 is redundant with the definition of Adverse Reliability Impact and should be struck. The drafting team responded that it agreed and included this suggested change in the new draft.

Another concern expressed was that Criterion 2.3 focuses on the long-term planning horizon which is contrary to the standard. The standard focuses on reliability impacts caused on the BES in a 15 minute timeframe from the misuse, degradation or unavailability of the BES Cyber Asset or BES Cyber System. The drafting team responded that the designation of generation as "must run" for reliability purposes as a result of "long term planning" has nothing to do with

the "real-timeliness" nature of the impact of its BES Cyber Systems on the function of "must run" generation asset to mitigate Adverse Reliability Impact. These time parameters are applied in different contexts. The intent is to ensure that the generation assets under these criteria are not transient assets run to mitigate short term market or operational conditions, but rather as long term mitigations for infrastructure deficiencies, whether permanent or temporary until long term remediation is engineered and put in service. In any case, the drafting team made minor modifications to avoid confusion with new Transmission Planning Horizon definitions in the glossary.

Criteria 2.4 (Blackstart Resources) and 2.5 (Cranking Path)

Many commenters expressed concern with this criterion. The SDT notes that it has removed restoration facilities from CIP-002-5, Attachment 1's "Medium Impact Rating (M)" category. The SDT made this decision after receiving input from commenters, from industry, and following discussions about the issue as presented to NERC's Operating and Planning Committees. The SDT learned that Blackstart Resources face reduction because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool. Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed. The SDT explains this change in more detail in the Guidelines and Technical Basis section of the posted draft CIP-002-5.

Criterion 2.6 (500kV Transmission)

One commenter asked if this criterion address facilities that essentially are radial leads and no load flow through. The drafting team responded that if they meet the definition of the BES, they are in scope. The use of the glossary term Facilities implies BES assets.

Another commenter asked if an autotransformer of 500 kV to 230 kV included. The drafting team responded that an autotransformer of 500 kV to 230 kV may be included depending on how the Responsible Entity defines its group of Facilities.

Criterion 2.7 (Other Transmission Facilities)

One commenter asked how a weighted value of a line is related to reliability. The drafting team responded that the weights used are based on average MVA ratings. These weights are used to normalize impact to a value for sites operating with different or multiple voltage levels.

Another suggestion was to change the first sentence of 2.7 to read: "Multiple Transmission Lines operating at 200 kV or higher, but less than 500 kV, where the total weighted value of all BES Transmission Lines whose Reliability Operating Services would be adversely impacted within 15 minutes if a single BES Cyber Asset / System is rendered unavailable, degraded or misused exceeds a value of 3000." The drafting team responded that the intent was to include BES Cyber Systems that could impact the reliable operation of the BES for any Facility within the single station or substation, not just Transmission Lines.

Another concern expressed was that the "weight value per line" used to determine total weighted aggregate value does not allow for variations in various owners' systems. Provisions should be made to exclude facilities that can be shown to not lead to cascading or voltage collapse upon their loss. The drafting team responded that the MVA values used are those used from a NERC reliability report, as pointed out in the Guidelines and Technical Basis section. The drafting team believes that this is an objective way of determining the level of impact that is sufficient for categorizing BES Cyber Assets.

Another commenter stated that line count does not necessarily mean that issues at particular substation will have a significant impact on the BES. Such impact can only be determined by studies and risk-based analysis of an entity's assets. The drafting team responded that they identified some gaps in the previous Version 4 criterion. The SDT believes that the current approach provides a more comprehensive approach to the impact of Transmission Facilities.

Another commenter suggested returning to the industry balloted and approved language that is in CIP-002-4 regarding 345kV with 3 or more lines. The drafting team responded that they made modifications to the transmission voltage threshold to remediate coverage gaps uncovered from the FERC data request following the Version 4 filing and to account for impact in situations with mixed voltage levels.

Another commenter stated that Criterion 2.7 specifies a floor of 200 kV. In certain parts of the country, the 200 kV floor is too high. The drafting team responded that the purpose of Criterion 2.7 is not to require all transmission Facilities in the transmission backbone (Bulk Electric System) be protected, only those that are determined to be critical. Criterion 2.7 establishes thresholds that would qualify such Facilities as Medium impact. Other Facilities are protected under the requirements for Low impact.

Another commenter noted that Criterion 2.7 in Attachment I describes the "weight value" to be applied to transmission lines. However, there is no guidance given for transformers. The drafting team responded that guidance has been added for transformers in the Guidelines and Technical Basis section.

Criterion 2.8 and 2.9 (IROL for generation and FACTS devices)

One commenter stated that the phrase "at a single station or substation location" does not seem to add any value and

can be a source of ambiguity. The drafting team responded that with the amended focus of the categorization criteria on Facilities, systems and equipment and their associated BES Cyber Systems, the drafting team believes that the phrase is now appropriate.

One commenter suggested adding an additional criterion that captures the fact that IROLs may be based on dynamic system phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response. The drafting team agreed and included language to this effect in the IROL criterion in Section 2 (Medium Impact).

Another commenter noted that the standard is placing a burden upon the TO for actions of others, that the TO has no control over, with no allowance for coordination or negotiations for potential changes in the determination of IROLs. The drafting team responded that FAC-014 requires the communication of the SOLs and IROLs to the asset owners who operate the affected Facilities.

Another suggestion recommended changing "Transmission Facilities" to "BES Transmission Facilities" for consistency purposes. The drafting team responded that the use of the NERC Glossary term “Facilities” includes the BES qualification.

Another commenter asked the drafting team to provide a definition for the term "Flexible AC Transmission Systems FACTS". The drafting team responded that the criterion specific to FACTS has been removed since it is included in Transmission Facilities.

Another commenter recommended that the term ‘Planning Coordinator’ be used rather than ‘Planning Authority” to be consistent with the rest of the standard and current NERC practice. The drafting team responded that they agreed and have changed the term to conform to the functional entity in the functional model.

Another commenter suggested that the phrase ‘. . . as critical to the derivation of IROLs and their associated contingencies’ be changed to, ‘. . . as Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more IROL violations’, like the wording using in Criterion 2.11. The drafting team responded that the current wording of this phrase is taken from the wording in FAC-014-2.

Another commenter expressed concern that there is a need to clarify the role and responsibility of PC, TP, GO, GOP, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal? The drafting team responded that other NERC Reliability standards already define the obligations of these entities with respect to these criteria. Once identified, the Responsible Entity owning these Facilities, Systems and equipment is responsible for compliance to the CIP standards of the associated BES Cyber Systems.

Another commenter stated that in sections 2.8, 2.9 and 2.11, the table titled “Major WECC Transfer Paths in the Bulk

Electric System" is not actively maintained by WECC and there is no clear identified basis for why certain paths are included in this table. The drafting team responded that upon further consultation with WECC, the specific language in question has been removed.

Criterion 2.10 (Nuclear Plant Interface Requirements)

One commenter stated that Criterion 2.10 needs to be limited to the plant switchyard, otherwise the entire grid could be included. The drafting team responded that the current language is the language used in NUC-001.

Criterion 2.11 (SPS)

One comment was that Criteria 2.11 twice contains the phrase "...if destroyed, degraded, misused". This appears to be a carryover from version 4, but it now is redundant and perhaps conflicting with the "15 minutes" qualification as defined at the top of the Medium Impact Rating section. The drafting team responded that the 15 minute term is meant to provide some boundaries to the term "real-time". It is intended to indicate the amount of time of when the effect of the triggered action resulting from the compromise of the BES Cyber Asset on the affected BES Asset (not BES), notwithstanding any other recovery mechanisms from contingency actions or redundancy. The drafting team has reviewed the definition of BES Cyber Assets and has removed the redundant terms from the Attachment 1 pre-ambles.

Another commenter observed that this criterion implies that all components of the SPS are designated as medium without regard to whether loss of those elements of the SPS system would lead to the referenced IROL violation. The SPS can be designed so that incorrect readings or misoperation of a given element of the system has either no impact or acts to run the SPS in the "safest" manner. If this is the case, the individual elements of the SPS should not require a medium designation, and should be allowed for in the standard. The drafting team responded that all the Elements of the SPS will inherit the "high water mark" of the SPS, and as a "system" that could cause excursions beyond the IROLs, should be categorized as Medium.

Another commenter questioned if this includes SPSs which are associated with Generation sites. The drafting team responded that these are included by referring the commenter to the Guideline and Technical Basis.

Another commenter stated that in sections 2.8, 2.9 and 2.11, the table titled "Major WECC Transfer Paths in the Bulk Electric System" is not actively maintained by WECC and there is no clear identified basis for why certain paths are included in this table. The drafting team responded that upon further consultation with WECC, the specific language in question has been removed.

Another commenter stated that Criterion 2.11 presumes that failure of an SPS or RAS would cause an IROL violation. An SPS or RAS may be implemented for a specific contingency for example. As an example, when that contingency happens,

certain switching might need to occur or generation run back. These automated actions might enable a higher limit on an IROL associated with a transmission corridor. If the SPS was not available, the limit would likely be lowered but not necessarily violated. A violation would depend on actual system conditions at the time. Thus, the language should probably be change to something along the lines of impacts or enables higher IROL limits. The drafting team responded that the drafting team responded that they agreed and have changed the criterion to address the comment.

Criterion 2.12 (UFLS/UVLS)

One commenter asked for clarification as to whether a UFLS or UVLS program of less than 300 MW is a Low Impact Rated Cyber Asset or is not subject to the CIP standards at all. The drafting team responded that changes have been made to the DP and LSE sections of Section 4 of CIP-002-5. Sections 4.2.1 and 4.2.2 state that only UVLS or UFLS Facilities that are in a UVLS or UFLS program required by a NERC or Regional Reliability Standard and meet the qualifications for Medium Impact are in scope for registered LSEs and DPs. No other UVLS or UFLS Facility is in scope for these CIP standards. The BES Cyber Systems that impact those automated UVLS and UFLS Facilities for more than 300 MW are categorized as Medium. Other BES Cyber Systems that only impact other UVLS or UFLS are not in scope.

Another commenter observed that the 300 MW bright-line seemed arbitrary (albeit carried over from prior versions). In general, the system is more tolerant to loss of load than loss of generation and the 300 MW seems out of proportion with criterion 2.1 of 1500 MW. The focus should be on how a malicious user can cause an Adverse Reliability Impact. The drafting team responded that UVLS and UFLS systems are last ditch efforts to recover from a BES event, when all other contingencies have been exercised to address the reliability issue. In fact, it could probably be argued that any UVLS or UFLS system that is part of a regional load shedding program designed to provide last ditch relief should be considered Medium Impact. The drafting team carried over the 300 MW from the current effective version, and version 4, which was industry approved in December of 2010.

One commenter expressed concern that Criteria 2.12 refers to a “system” - as in “Each system or Facility...” - which implies something of a cyber nature. The rest of the bright-line criteria refer to or describe hard assets, not cyber assets. The SDT may want to consider removing “Each system or”. The drafting team responded that the term BES Cyber System” or BES Cyber Asset” was used when referring to those BES Cyber Systems or BES Cyber Assets subject to the CIP standards. The term “systems” when used stand-alone is used in its broader sense to include Facilities, cyber assets or a combination of both when they directly perform a BES reliability function.

Another observation was that the standard and the Application Guidelines do not indicate whether the 300 MW limit is a system limit or an entity limit. The drafting team responded that it added the phrase “Each System or group of Elements that performs automatic Load shedding under a common control system” to clarify the criterion.

Another commenter suggested that the SDT replace the word, 'system' with 'common control system' to clarify that this criterion applies to a system triggered by a single (common) control, rather than a program (system) of many independent relays set to trip at the same frequency. The drafting team responded that it added the phrase "Each System or group of Elements that performs automatic Load shedding under a common control system" to clarify the criterion.

Another commenter requested that "system" be capitalized as it appears to align properly with the NERC definition. The drafting team responded that it agreed and included this suggested change in the new draft.

Another commenter observed that a small entity may be required to own and maintain UFLS relay or relay system by the Transmission Provider. In the standard, the UFLS threshold is at 300MW. The small entity may not have 300 MW of load, but their relaying is part of the design of an UFLS system that is much greater than 300 MW. This small entity's relay is not critical to the BES and if degraded or destroyed would not compromise the capability of the Transmission Provider's UFLS system as the two systems are not integrated and do not communicate. The drafting team responded that changes were made in the applicability section of the standard and in this criterion to address the concern.

Criterion 2.13 (Other Control Centers)

One commenter stated that Criteria 2.13 in Attachment 1 is not acceptable because under 1) the functional obligations of TOP and TO is too vague and 2) 300MW of in many cases does not qualify as significant impact. Also 300 MW of generation should not be equated to 300 MW of UFLS/UVLS. The drafting team responded that the functional obligations of the Transmission Operator and the Transmission Owner are listed in the NERC Functional Model. In many cases, where the Transmission Operator and the Transmission Owner are separate entities, there are agreements between the TOP and the TO on which functions of the TOP have been delegated to the TO. Registered Transmission Operators may have some of their functions performed by another entity through agreements. In addition, the application of the 300-MW threshold in this case is for Generation Control Centers. By definition, this criterion is applicable only to generation Control Centers that control more than one generation facility in more than one location. Generation Control Rooms that control generation in a single generation facility fall under the 1500 MW threshold. The intent is discussed in the Guidance and Technical Basis section.

Another comment was that Transmission Owners do not have Control Centers and should be struck from this criterion. The drafting team agreed and included this suggested change in the new draft.

Another comment was that the term "control centers" should be capitalized in the phrase "generation control centers" to make it clear that it refers to the defined term "Control Center." The drafting team agreed and included this suggested change in the new draft.

Another commenter recommended that the proposed 2.13 language be deleted and replaced with the following: "TOP and GOP Control Centers not included in High Impact Rating and controlling 1500 MW or greater of load or generation."

Add: "2.14. Control Centers, not previously included in High Impact Rating (H) or Medium Impact Rating (M), above, that perform the functional obligations of Balancing Authority, Transmission Operators or Transmission Owners, and that do not implement protected data connections with other Control Centers in a manner as to prevent themselves from being used as cyber-attack vectors into other Medium Impact or High Impact Rating Control Centers." Making this change will ensure that other appropriate Control centers will be categorized in either the Medium or Low level. The drafting team responded that for criterion 2.13, the proposed language would not adequately reflect the level of impact of generation and TOP Control Centers. The drafting team believes that all Control Centers not categorized as High Impact should be categorized at least as a Medium because of the functions they perform and their interaction with other Control Centers. The intent of the 300 MW threshold in the case of generation is an attempt to consider a specific type of configuration in generation Facilities, as explained in the Guideline and Technical Basis section. Regarding the addition of 2.14, criteria for Control Centers are precisely drafted so that adequate cyber security protections are applied. If these protections have been applied, then the Responsible Entity already complies. These ensure that all Control Centers have the protection implemented all the time. These protections implement a defense in depth posture represented by the requirements in these standards. Network connectivity is but one aspect of the total protection that is required for Medium Impact assets.

Another observation was that it is not clear if the term "generation control centers" is referring to: 1) control centers local to generation, 2) centralized control centers controlling multiple geographically disparate generation resources, 3) or both. The drafting team responded that the term Control Center is now capitalized: the assets covered under this criterion must meet the definition of Control Centers, not control rooms local to the generation location.

Another commenter asked for clarification on what is meant by the term "control" in (2) generation control centers that "control" 300 MW or more of generation. Does this mean physical control only or does it include verbal commands? Also, does the 300 MW refer to name plate rating or some other method AND is that 300 MW only for BES generation or all generation that generation controls? The drafting team responded that the term "control" means perform the functions of a Control Center. Verbal commands that have a real-time effect are included. The 300 MW is net Real Power for BES generation. The criterion has been amended to clarify these parameters.

Another commenter stated that Criteria 2.1 and 2.13 should distinguish between controllable generation and intermittent generation sources (i.e. wind and solar), since the loss of intermittent generation facilities happens naturally and regularly and is not viewed as an extreme event. The drafting team responded that, while the unavailability of intermittent generation (vs. controllable generation) may not be considered an extreme event, the impact of misuse of

the associated BES Cyber Systems due to a cyber security compromise can result in BES disturbances. The impact criteria provide a measure of this impact.

Section 3 – Low Impact Rating

One commenter proposed to change the phrase "...or Section 2 Medium..." to "...Section 2 as having a Medium..." for consistency purposes. The drafting team agreed and included this suggested change in the new draft.

Another observation was that Section 3 does not provide a minimum site MWs or interconnection voltage and recommended a nameplate rating greater than 20 MVA or gross plant/facility aggregate nameplate rating greater than 75 MVA including the generator terminals through the high side of the step-up transformer(s) connected at a voltage of 100 kV or above. This was proposed in line with the Bulk Electric System (BES) definition developed under NERC Project 2010-17 Definition of the Bulk Electric System. The drafting team responded that it specifically chose the defined term Facilities to limit the applicability to the BES. The SDT addressed the concern in Section 4 (Applicability) of the standard itself. Section 4 clearly stipulates under Facilities 4.2.3: "Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities." (Underline added). Only those Facilities that are deemed to be BES Facilities are in scope for the standard. If these Generation facilities are excepted from the BES definition, then they are also excepted from the applicability of these CIP Cyber Security standards.

General Comments

A general comment was that it is unclear if BES systems at a facility can have numerous levels of impact. The drafting team responded that at a given physical facility, there may be a BES Cyber System that may adversely impact a BES Facility classified as Medium and there may also be a BES Cyber System that may adversely impact a BES Facility classified as Low.

Another concern was that there is little justification provided for why the criteria for the various categories were selected and why three categories were selected. The drafting team responded that the Background, Rationale and Guidelines and Technical Basis sections of the posted CIP-002-5 provide the justification for both the criteria and the "bright lines" defined.

Several commenters wanted an impact level of "No Impact Rating". The drafting team responded that Cyber Assets that have "No Impact" are by definition not in scope.

Other commenters wanted a fourth category of risk impact, "De Minimis Impact", that would consist of otherwise Low Impact BES Cyber Assets but that do not have routable protocol or dial-up access. The drafting team responded that the

electronic connectivity of the BES Cyber Systems does not have a bearing on the impact of the specific BES Cyber Systems or BES Cyber Assets on the reliable operation of the BES. The drafting team has included consideration of the connectivity in the applicability column of various requirements.

Another concern was that there is no appreciable difference between the requirements for High and Medium impact levels. The SDT may want to consider modifying items 1.1 through 2.13 on Attachment I to be "All these assets have a Critical Impact Rating". The drafting team responded that there are significant differences in the functional impact of the High Impact assets and those in the Medium Impact. The Facilities, systems and equipment in the High Impact category typically provide reliability functions for a wide area and have control and therefore impact for a large number of Facilities with significant impact, especially with the additional qualifications in the revised draft. While the actual number of additional controls may not be significant in number, these few additional controls (or differences in controls) are significantly stronger in these environments. They are also more practically implementable in these environments.

Another commenter proposed that Low Impact assets and their requirements be moved to another standard separate from High and Medium Impact assets and requirements. In addition, it was felt that the scope for Low Impact generation would bring a considerable number of new assets into the CIP standards. The drafting team responded that they moved all the requirements for Low impact systems to CIP-003 as management controls, further indicating the programmatic nature of the requirements as well as substantive changes in the requirement language.

Another concern was that generation facilities that require notification from the Planning Coordinator or Transmission Planner (e.g. Criteria 2.3 and 2.6) must be placed on a transition plan that would allow those facilities that are notified of change in status adequate time for remediation. The drafting team responded that the implementation plan for newly identified BES Cyber Systems or BES Cyber Assets provides adequate time for the Responsible Entities to come into compliance.

Another concern was that the 15 minute criterion does not apply to the vast majority of systems covered by the standard because power system apparatus and computer systems generally operate in the time frame of five seconds or less. The drafting team responded that the combination of impact on reliable operation of BES Assets and the 15 minute "real-time" impact was used to limit the scope to those Cyber Assets that would impact the reliable operation of BES Assets within a 15 minute window, and excludes those Cyber Assets that do not have an impact within 15 minutes.

Another comment was that the term "adversely impact" should be defined. The drafting team responded that the term adequately conveys the meaning of an impact that has a negative effect on the reliable operation of the BES and therefore does not need to be added to the NERC Glossary of Terms.

Another comment was the suggestion to change the phrase "would, within 15 minutes, adversely impact" to "could

adversely impact." There is a significant difference between would and could. The drafting team debated the use of both terms and decided that the use of the term "would" provides a more accurate direction on the evaluation of the impact of the BES Cyber System or BES Cyber Asset on the BES Facilities, systems and equipment, and that the term "could" was too open- ended.

Another comment suggested an additional criterion (similar to CIP-002-3 R1.2.7) in the Medium category to capture these self-identified impacts: 'Any additional facilities that support BES Reliability Operating Services that the Responsible Entity deems appropriate.' The drafting team responded that they considered inclusion of such a criterion in Version 4 but withdrew it in consideration of the complexities for the Responsible Entities demonstrating compliance to such an open ended criterion.

Other comments were that study based exceptions should be allowed. The drafting team responded that the bright-line criteria ensure that these standards are uniformly applied across regions and entities. The use of exceptions based on engineering studies is contrary to that objective and reintroduces the non-uniformity and inconsistencies that bright-lines address.

Another concern was that the universe of cyber assets supporting a TOP/BA/RC SCADA or EMS may extend into the substation and field RTU and devices. The drafting team responded that the proposed definition of Control Center provides adequate scoping qualifications. The definition has been amended to refer to reliability tasks defined in the functional model for real-time operations for applicable functional entities. The scope of included BES Cyber Systems will depend on many factors, including how Responsible Entities define their systems and ESPs.

Another commenter stated that the Attachment 1 "bright line" criterion regarding load shedding systems ("300 MW") should be included in the Section 4.1.2 Distribution Provider Applicability section. Otherwise, all distribution providers may be obligated to demonstrate that their UFLS / UVLS / SPS / RAS equipment was not responsible for IROL violation / 300 MW - where they may not even be aware of the full scope. The drafting team changed the Applicability section in the updated draft to address this comment.

Another commenter observed that Criterion 1.10 in CIP-002-4 was removed and recommended that it be reinstated in Attachment 1. The drafting team agreed and included this suggested change in the new draft.

Another comment stated that the opening paragraph of the definition of Medium Impact Rating should be revised to correspond with the wording for High Impact Rating. The drafting team modified the heading as suggested.

Another concern expressed was that application of the "bright line" criteria proposed, some of which require identification of Critical Assets based on determinations made by Reliability Coordinators, Planning Authorities/Coordinators, and Transmission Planners, will create significant new burdens on Reliability Coordinators,

Planning Authorities/Coordinators, and Transmission Planners. The drafting team responded that the criteria in Attachment 1 provides no new requirement that the RC, TOP, PC, or TP are not already doing or being required to do by other NERC reliability standards.

QUESTION 3 – CIP-002 R1:

Requirement R1 of draft CIP-002-5 states, "Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems.* **All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification." Further, part 1.1 of R1 states "Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.**

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R1 and Parts 1.1 through 1.4 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Most of the comments submitted in response to this question centered around the following themes:

- Confusion about the order of categorization
- Disagreement with the use of the word, "intended" in Part 1.1
- Concerns about having 30 days to update categorizations in Part 1.1
- Concerns about the scope of change prompting the need to update asset categorizations
- Questions about identification of low impact assets
- Questions about responsibility for the requirement
- Minor wording recommendations
- Comments about the Informational sections of the standard
- Comments on Attachment 1
- Other comments

Each of these themes is discussed in more detail below.

Confusion about the Order of Categorization

Several stakeholders noted that the sequence of actions associated with complying with Requirement R1 was confusing and the process of classifying and categorizing cyber assets and then identifying other assets which must be protected (CIP-005 and CIP-007) is excessively complicated.

One commenter recommended the following three-step process for identification and categorization, and indicated that this process would result in only needing to identify high and medium impact facilities:

1. For each BES facility that has cyber assets associated with it, go to CIP-002-5 Attachment 1 to find out if the facility is low-, medium-, or high-impact.

2. Determine the BES Reliability Operating Services that the BES facility supports.

3. Just as was the case in CIP Versions 1-4, the last step is to identify the cyber assets associated with the facility that are in scope for the remaining CIP standards

Other commenters suggested starting by first identifying high, medium , and low assets and then proceed with identifying Critical Cyber Assets at those facilities. Still other commenters proposed identification of low impact BES Cyber System at a Facility level, rather than by listing all the Cyber Assets associated, as this would add administrative burden and not provide additional BES security or reliability.

Other commenters recommended creating two Requirements - one for identification of BES Cyber Assets and another for categorization of BES Cyber Assets to eliminate multiple repeat violations of the same requirement, noting that

multiple violations of this requirement may stem from different causes and may unintentionally lead to mischaracterize an entity's compliance record and have consequences that impact the scope of subsequent audits and compliance investigations. Another stakeholder recommended an identification process that starts with identifying any applicable BES Reliability Operating Services relative to the entity's Registered Function(s), then identifying and classifying BES Cyber Assets and/or BES Cyber Systems associated with that BES Reliability Operating Service according to the criteria in Attachment I.

As noted above, and in response to the above, the SDT offers that there are many different ways of approaching the organization of the actions in this requirement. After much deliberation, the SDT modified the Requirement R1 so that the order of activities in identifying and classifying assets is clearer. Requirement R1 now includes several "Parts" to step entities through the process of categorizing their BES Cyber Systems:

- Part 1.1 addresses the first step of identifying which of the entity's Facilities, Systems, and equipment meet the bright-line criteria in Attachment 1
- Part 1.2 uses the output of Part 1.1 and for each Facility, System and equipment with a high impact rating, requires the responsible entity to identify the BES Cyber Systems and associated BES Cyber Assets used for that Facility, System or equipment
- Part 1.3 uses the output of Part 1.1 and for each Facility, System and equipment with a medium impact rating, requires the responsible entity to identify the BES Cyber Systems and associated BES Cyber Assets used for that Facility, System or equipment
- The entity's Facilities, Systems and equipment not identified as high or medium impact is, by default, categorized as low impact

Some commenters expressed concern about the grouping of BES Cyber Assets into a BES Cyber System without any consideration criteria. One commenter asked if each cyber asset is categorized EITHER alone OR as part of a BES system. The SDT made significant changes to the Criteria in Attachment 1 in an attempt to make the criteria as objective as possible to eliminate questions about groupings. These changes clarify that a BES Cyber System is one or more BES Cyber Assets, and that all BES Cyber Assets are part of a BES Cyber System.

Disagreement with the Use of the Word, "Intended" In Part 1.1

Several commenters noted that Requirement R1.1 (Requirement R1.4 in draft 2) refers to the "intention" for the BES Element or Facility to be in service for more than six calendar months and observed that the word "intended" is not auditable. The SDT agrees and has changed "intended" to "planned". One stakeholder proposed that entities be

required to document the intent in that instance to allow the auditor the latitude to accept intent over actuality in the case where the BES Element or Facility was in service for more than six months due to unforeseen circumstances. With the change in wording from "intended" to "planned", the SDT believes that the dated electronic or physical lists showing changes to the BES (with a date for each change) accomplish the documentation of evidence required to demonstrate the planned nature of changes to the BES.

Concerns about Having 30 Days to Update Categorizations In Part 1.1

Several commenters had questions about the 30 days proposed for updating categorizations following a change to the BES in what was Requirement R1, Part 1.1 (now Part 1.4 in the revised standard). Some questions arose around the number of days, with some commenters proposing a longer period (60 days or 90 days or annual update). One commenter asked the SDT to provide its justification for the selection of the day time period, and implied that an annual review would be preferable to the 30 days. CIP-002 is the foundational standard for the entire set of CIP standards. If an entity adds a new piece of equipment to the BES and it is not accounted for under CIP-002, then that piece of equipment could be unprotected for an extended period of time (a year or more if the proposal to change the 30 days to "annual" were adopted.)

Some commenters questioned whether updates should be required for all changes to the BES and the SDT does not believe this is necessary. Under the revised standard, Responsible Entities are not required to implement protections to assets that have changed only in response to a temporary emergency situation and where the protective controls will not be implemented before the asset is returned to its original configuration.

Some commenters noted that updating this categorization, especially for low impact Elements and Facilities is burdensome as every configuration change of the BES would need to be tracked, dated, and evidence of the process to identify or categorize the BES Cyber Assets or BES Cyber Systems documented. An alternative method should be considered - for example, when planning studies reveal that the configuration change of the BES is material, this could trigger the process of identifying or categorizing the associated BES Cyber Assets or BES Cyber Systems.

One commenter proposed requiring the update before the equipment was placed into service cautioning that deployment or reconfiguration of a BES Cyber Asset may pose a significant risk to the BES. A thirty day gap would delay identification of a BES Cyber Asset, and also delay implementation of Cyber Security measures prescribed under CIP-003 through CIP-010, thus also disagreeing with the provision limiting "updates" to include only those Cyber Assets "that are intended to be in service for 6 months."

The SDT considered the different proposals provided and changed the 30 days to 60 days to provide entities more time to make needed updates – however the SDT cannot justify extending the period for longer than 60 days. Annual updates

would allow some Facilities, Systems, or equipment to go unprotected for longer than justified given the high or medium risk to the BES of leaving that Facility, System, or equipment unprotected. The SDT did not adopt the suggestion that changes to categorization be completed before deploying or reconfiguring a BES Cyber Asset. The SDT recognizes the risk to the BES that may occur if some equipment is not protected, however the SDT tried to maintain a balance of reasonable security awareness while also moderating audit impact and the impact to real-time operations. There may be many scenarios in which an entity is faced with the need to change a piece of equipment in 'real-time,' and waiting to do so while the asset is categorized may jeopardize reliability.

Concerns about the Scope of Changes Prompting the Need to Update Asset Categorizations

Some commenters asked if Part 1.1 refers to inclusion of the element or facility on the BES Cyber Assets and BES Cyber System list, or inclusion in the entire scope of CIP-002 actions including the signature of the CIP senior officer. As specified in Requirement R1, the requirement only requires an update to the identification of the Facilities, Systems, or equipment and the high and medium impact BES Cyber Systems and their associated BES Cyber Assets. Approval by the Senior Manager or delegate is specified in R2.

Several commenters expressed concern with the open-ended use of the word, "change" in reference to a change to the BES that prompts the responsible entity to update its categorization and indicated that leaving this open-ended leaves the requirement subject to varying interpretations and challenging to audit. One stakeholder suggested making the impact change determination dependent upon BES Cyber Asset changes; returning to an annual review; or alternatively adding a very specific list of BES changes for which the analysis must occur. Another commenter proposed that a change to a relay setting could be could be considered, using the strict definitions of Elements and Facilities, as a change to a BES Element and proposed that such a change is too granular for inclusion in the scope of changes warranting a revision to the categorizations required under Part 1.1 (now Part 1.4). The commenter proposed establishing boundaries for changes that would warrant updating the categorization including topological changes, generator interconnections and generator uprates and equipment retirements but not for derates since derates may lower the categorization of BES Cyber Systems and/or BES Cyber Assets and the reduction in compliance burden will cause them to do this.

One set of commenters recommended changing to, "when a change to BES Elements is completed and / or the facility is placed into operation".

Another set of commenters recommended adding a word between "calendar days of" and "a change to BES…"

In response to the concerns and suggestions offered above, the SDT notes that it elected to leave this open-ended as any list the SDT might develop would likely not meet all reasonable circumstances. The revised sentence says: "Review (and update as needed) the identification in Requirement R1, Parts 1.1, 1.2, and 1.3 within 60 calendar days of when a change

to BES Elements or Facilities is placed into operation, which is planned to be in service for more than six calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category."

One commenter expressed a concern that the requirement doesn't explicitly address "Transient Cyber Assets," noting that a transient cyber asset could fall "under the radar" and result in a major threat to the BES. The SDT deleted the proposed definition of "Transient Cyber Asset." These transient assets are normally portable maintenance and diagnostic tools, which by their very nature cannot meet all the requirements mandated for BES Cyber Assets, such as a fulltime physical security perimeter, or wiping all information when it is 'redeployed' to another location when the purpose for its existence may be to bring back field data for analysis. The SDT does not intend for the CIP requirements to make impossible or impractical normal practices that increase reliability of the BES, such as being able to use Cyber Asset based tools for diagnostics and maintenance, especially among numerous field assets. As such, the SDT does not believe it is necessary to include these in the scope of R1.

Another commenter recommended adding a companion requirement to address updating categorization when Facilities are "out-of-service." Regarding "out-of-service" cyber assets, these cease to be BES Cyber Assets by definition the moment their impact cease on the BES (i.e. within the 15 minute). The SDT offers that it is the Responsible Entity's option to ensure they do remain compliant if and when they are brought back in service.

One commenter noted that Part 1.1 doesn't provide a timetable for the phase-in for the entity to meet the potential additional Standard(s) Requirements caused by this change. The SDT notes that phase in of requirements is addressed in the Implementation Plan for the set of CIP standards.

One commenter asked for more clarity when categorization of the BES Cyber Assets or BES Cyber Systems shifts from a higher to a lower impact category. The SDT responds that if the change is from a higher to a lower category, the Responsible Entity is not required to update the lists, but if not doing so, it will be required to be compliant to the requirements for BES Cyber Systems at that level.

Questions about Identification of low impact Assets

One commenter asked the team to provide its justification for the criteria for the various categories selected, and specifically why three categories were selected, and expressed concern about the inclusion of "low impact" assets, proposing that the low impact assets be excluded from the standards. The SDT tried to provide its justification for the criteria and the categories in the Background section of the standard and the Application Guidelines at the end of the standard. Together these explain how the drafting team developed its justification for the criteria selected with this risk-based approach to cyber security.

Several commenters proposed revisions to the following sentence: "All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be low impact and do not require discrete identification" and identified that entities will still need to maintain this list when the listing of BES Cyber Systems is created and each system is classified. Several stakeholders indicated a concern that auditors will demand the list even if it is not explicitly required. The SDT believes that an explicit statement to the effect that no list is required is required to provide the required clarity in compliance requirements.

Several stakeholders proposed elimination of all requirements associated with low impact BES Cyber Systems from CIP-002 and proposed moving all the low impact requirements into a separate standard with a longer implementation plan. The SDT adopted the suggestion to move all the requirements associated with protection of low impact Systems into a single standard – and moved those requirements into CIP-003. The SDT did not remove the low impact language from CIP-002, as this is the standard where low impact systems are identified by default. Note that the SDT also adopted the suggestion to give entities more time to become compliant with protection for low impact assets in support of this suggestion. The Implementation Plan now specifies an implementation timeline of at least three years for the low impact requirement. This should allow entities more time to focus on protection of the more critical assets.

One stakeholder asked how entities could comply with CIP-005-5 R1.1 and CIP-006-5 R.1.1, (defining operational or procedural controls to restrict unauthorized electronic access or physical access) without previously identifying those assets either globally or specifically in CIP-002-5 R1? The SDT agrees that each responsible entity will need to identify and categorize its assets in CIP-002 as a prerequisite for meeting compliance with other CIP standards. Please see the revisions the SDT made to CIP-002 to clarify the process for identifying and categorizing assets.

Some commenters had questions about the low impact category and indicated that this resulted in having all BES Cyber Assets in the CIP standard scope, which was not directed by FERC Order 706. The SDT notes that FERC order 706 includes a directive to consider the National Institute of Standards and Technology (NIST) approach, which includes baseline protection for all applicable systems.

Several commenters indicated that the Measure M1 appeared to require documentation of the low impact assets even though the associated requirement included the phrase, "…and do not require discrete identification." In response, the SDT removed the following sentence from M1: "Evidence of categorization of low impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls."

Questions about Responsibility for the Requirement

Several commenters made suggestions about what functional entity should be required to comply with Requirement R1. Stakeholders raised issues about joint ownership, about responsibility for protection of facilities that are leased.

Regarding ownership, the SDT believes that the responsibility for compliance should rely on the owner of the asset, and that it is the responsibility of the owner, through contractual arrangements or otherwise, to ensure compliance by the operator if such operators are different from the asset owner.

One commenter noted that the word 'owns' is used in two places in R1 and recommended changing the word "owns" to 'operates' or 'utilizes' and cautioned that ownership may not be the determining factor based on outstanding operating agreements over time – and also noting that a single asset may be used by more than one entity. The SDT notes that the standard was revised so the word, "owns" is no longer used in Requirement R1, but removal of the word "owns" does not mean that the "Responsible Entity" is no longer the owner.

Some stakeholders asked the SDT to modify the standard to clearly state that those entities with no Bulk Electric System (BES) assets per the definition included in the NERC Project 2010-17, Definition of Bulk Electric System, are not required to comply with this standard or, alternatively, the Senior Manager must annually certify that the entity has no BES assets per the definition thus no BES Cyber Assets/Systems or to create a fourth category of "No Impact", thus no further action required which can be certified annually by the Senior Manager. In response, the SDT notes that if an asset has "no impact" this is not a cyber asset and is outside the scope of this standard by definition.

Some stakeholders asked for confirmation that entities without any BES will not have any Critical Cyber Assets or Systems and therefore, R1 will not apply to them. In response the SDT notes that registered entities that own assets necessary for the reliable operation of the BES must be included. That is the reason these entities are required to register as NERC Registered Entities.

Other Minor Wording Changes for Clarity

One stakeholder recommended changing "of" to "when" in the statement, "…when a change to BES Elements…" and the SDT adopted the intent of this suggestion by adding the word, "when" so that the revised phrase now reads, "…of when a change to BES Elements…"

One stakeholder indicated the term "would" adversely impact one or more BES Reliability Operating Services is used in the background discussion and recommended using the word, "could" instead. The commenter's concern was that without the criteria being anticipatory, entities could take the stance that the criteria calls for a 15-minute certainty and therefore the criteria in question is not met and the BES Cyber Asset or BES Cyber System is excluded. The SDT believes the word, "would" is more definitive and more clearly conveys the intended meaning, thus the SDT did not adopt this suggestion.

One commenter noted that the Rationale for R1 used the terms, "Cyber Assets and Cyber Systems.." and recommend the language be changed to "BES Cyber Assets and BES Cyber Systems.." and this change was adopted and is reflected in the

revised standard.

One commenter noted that the Rationale for R1 refers to "impact" and proposed that this should be changed to "potential impact." In response, the SDT modified Attachment 1 so that it no longer includes the phrase, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services…" and instead relies solely on defining Impact categorization based on bright line criteria. Thus the SDT believes the word, "impact" is the correct word.

One commenter noted that the "Rationale - R1" box uses the term "Cyber Systems," which is not a formal term and suggested changing the case to avoid confusion. The commenter was correct that "Cyber System" is not a defined term – however the SDT did propose a definition of "BES Cyber Systems" – and in the revised standard the SDT was careful to use the defined term, "BES Cyber Systems" in its updated rationale for Requirement R1.

One commenter suggested expanding the language when referring to several levels of impact or assets and systems and indicated that as originally drafted, "high and medium impact" could be interpreted as meaning an asset or system which is both high and medium . The SDT revised the standard so it does not include the phrase, "high and medium impact."

One commenter proposed changing the wording in Part 1.1 (now Part 1.4 in the revised standard) from "…and change to BES Elements and Facilities is placed…" to "…and change to BES Elements and Facilities being placed…" The phrase was changed based on several suggestions from different commenters to: "… of when a change to BES Elements or Facilities is placed…"

One commenter recommended changing "security plan" to "Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes and plans in place to comply with security requirements. Should the last paragraph on page 7 say "cyber security plan"? In response, the drafting team notes that, in the context of these standards, the term "security plan" includes any plan required by the standards (e.g. physical security plan, incident response plan, and recovery plan).

The Term "BES Elements and Facilities" used only once within the standards. Suggest changing this phrase to "BES Cyber Assets or Systems." The SDT changed this to "BES Elements <u>or</u> Facilities" in R1.4 to clarify the SDT's intent. (Underlining added).

Another stakeholder proposed modifying M1 to change the language, "…as required in R1 and list of changes to the BES…" to "…(as required in R1 and list of changes to the BES Elements and Facilities)…". Measure M1 was not modified in response to the proposed language modification. The requirement doesn't tie the update to changes in "Elements and Facilities" – the requirement ties the update to changes to the "BES."

Comments about the Informational Sections of the Standard

Some stakeholders asked about the enforceability of the Background and Application Guidelines sections of the standard. The SDT clarifies that the Background and Application Guidelines and Technical Basis are provided for guidance but is not enforceable - compliance monitoring is to requirements, not to any of the background, rationale or other contextual information presented in the posted standards. NERC has adopted the results-based format and process for standards and all results-based standards will include these sections.

Several commenters noted that in the background section of the standard, there is a statement that malware protection applies to a system as a whole and may not be necessary for every individual device to comply. These commenters noted that network-based anti-malware is only one aspect of malware protection and expressed the view that it is completely ineffective for malware not introduced over the network or introduced within a protected network where the configuration of the network allows traffic to pass between Cyber Assets without inspection. In response the SDT notes that there is a requirement in CIP-007-5 to protect the "BES Cyber System" not the asset. The entity has to be able to demonstrate compliance with protection of the BES Cyber System. See CIP-007 Requirement R3 and the associated information in the Rationale for R3 which includes the following: "The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection."

Other comments noted the phrase one "of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems." The "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" defines the term BES Cyber System as "[o]ne or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services." The SDT goes on to state that the use of the term BES Cyber System is intended "to provide a higher level for referencing the object of a requirement." The commenter suggested that neither the definition of BES Cyber System nor the malware requirements in CIP-007-5 indicate, on their own, that compliance with the requirement does not require every BES Cyber Asset that comprises a BES Cyber System to have malware protection. The commenter is therefore concerned that the Regional Entities will continue to enforce the CIP standards on an individual BES Cyber Asset basis, per a literal interpretation of the text of the Version 5 Standards. As such, the commenter requests more explicit confirmation of the holistic approach of the Version 5 Standards as indicated by the "Background" section of CIP-002-5 and additional examples similar to the malware example already provided.

In response, the SDT notes that it has made several significant changes to all of the standards and to the definitions of BES Cyber System and BES Cyber Asset to more clearly explain the BES Cyber System-level approach. The standards

themselves are applicable on a BES Cyber System-level (and certain associated Cyber Assets). The SDT also clarified the background section of each standard to more clearly explain the applicability section in the tables. Additionally, since the BES Cyber System definition was modified to strengthen the SDT's intent that they are one or more BES Cyber Assets logically grouped by the responsible entity, it underscores the holistic approach of the Version 5 standards. The SDT has also expanded the guidelines and technical basis section of CIP-007.

Some stakeholders questioned the Responsible Entity's ability to "determine the level of granularity at which to identify a BES Cyber System[,]" as stated in the "Background" section of CIP-002-5 and asked for clarification that the Regional Entities would **not** play a role in the definition of boundaries of BES Cyber Systems. The SDT cannot make promises for what a Regional Entity will and will not do. However, in addition to the changes made in the definitions and standards themselves, the SDT notes that the flexibility remains with the responsible entity. These are results-based standards, and the requirements indicate the required result aimed at the applicable BES Cyber System. By stating that "defining the boundary too broadly could make the secure operation of the BES difficult to monitor and assess," the SDT is cautioning that a determination to classify a system too broadly may introduce unnecessary challenges in meeting the requirements. In general, the SDT has attempted to explain that Version 5 is responsive to lessons learned from implementing previous versions by recognizing that Cyber Assets function together as a complex system. Entities now have an opportunity to identify those collective BES Cyber Assets as BES Cyber Systems and apply requirements to them on a system level.

In the Guidelines and Technical Basis section of the standard, commenters recommended that the team consider omitting the reference to "Substation automation" as it may have different meanings in the industry and is not defined in the NERC Glossary. Another comment identified a difference in the description of BES Reliability Operating Services in this part of the standard and in the proposed definition. The SDT has retained the reference to "Substation automation" since this is a term that may not be familiar to all, is likely to be familiar to substation owners – and those are the entities we are trying to reach. The SDT removed the proposed definition of "BES Reliability Operating Services" from the list of proposed definitions – so there is no conflict.

Comments on Attachment 1

One commenter indicated that Versions 1 and 3 of the CIP standards only required protection of the Blackstart initial or primary cranking paths and proposed retention of this approach.

The SDT modified the criteria in Attachment 1 so that Blackstart Resources and associated Cranking Paths are no longer included in the Attachment.

A commenter requested that the drafting team clarify whether the SDT contemplates that scheduling systems would adversely impact one or more BES Reliability Operating Services within fifteen minutes if rendered unavailable, degraded,

or misused (for example, does the potential for cyber attack on e-tagging systems before tags are loaded into EMS prior to the ramp suggest that scheduling systems should have a high or medium impact Rating?). In response, the drafting team has made changes to the approach that no longer uses the BES Reliability Operating Services. Rather, the approach is based on BES Cyber Systems that affect real-time functional tasks of the asset (in this case the Control Center). Scheduling and e-tagging is not generally considered a "real-time" operation.

Some commenters proposed that BES Reliability Operating Services encompass everything a utility does and use of this definition, by itself, would encompass all assets and expressed concern that the term, "BES" is under refinement, leaving entities in a position where they could potentially become instantly non-compliant in the event that the definition of BES changes. The SDT notes that the reliability functions provide the first step in a multi-layered filter intended to focus the most protection on those BES Cyber Systems that are most critical to reliability. The term, "Bulk Electric System" is a defined term today – and when the BES Definition team proposes revisions to this term those proposed revisions must be posted for stakeholder comment.

Other Comments

For consistency with the format of the other CIP standards being proposed, one stakeholder suggested putting the requirements into a table format and the SDT declined. The table format was developed for other standards where the requirements were subject to varying applicability. CIP-002 doesn't have the same variation with respect to applicability – Requirement R1 applies to all Responsible Entities.

Some commenters asked for confirmation of the distinction between lists that are bulleted and lists that are numbered. When a list in a requirement is bulleted, that is an indication that the responsible entity is required to meet the performance in at least one, but not all of the listed items. When a list in a requirement is numbered, that is an indication that under the specified condition, the responsible entity is required to meet the performance in each numbered item.

The SDT believes that the wording in each of the requirements clearly identifies the distinction between these cases.

One commenter proposed that the SDT revise the standard to align with the NISTIR 7628 SG.CA-3, Continuous Improvement High-level requirements by adding the concepts of "continuous improvement" and best practices. It is not the intent of the standards' requirements to specify best practices, but to clearly specify minimum requirements that must be made to provide the protection commensurate with the impact level. Certain requirements will include processes to ensure a specific action in response to changes, the concept of "continuous improvement" is hard to implement as an enforceable requirement sanctioned by penalties other than through clear and specific process actions.

Some commenters expressed a desire to include exemptions for smaller entities and proposed that the following be included: "Exemptions: 4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have

no BES Cyber Systems" noting that the similar language was found in other CIP standards. The commenters noted that use of this exemption would require the identification of "no cyber systems" rather than "low impact assets" and proposed modifying the standards for greater consistency. In response the SDT notes that the exemption is for entities that have no BES Cyber Systems – the CIP standards apply to BES Cyber Systems, not cyber assets.

One stakeholder asked the team to define BES Elements and Facilities, however these terms are already defined in the NERC Glossary of Terms Used in Reliability Standards.

One stakeholder noted the use of the terms, "Associated Protected Cyber Asset" and "Associated Electronic and Physical Control and Monitoring Systems in the diagram used to explain "BES Cyber Systems" and questioned the use of these terms. On page 7 the diagram uses the term "Associated Protected Cyber Assets." The SDT has added more information on these terms in the revised standard's Background section and these terms are used in other CIP standards to help narrow the applicability for specific requirements.

Several entities asked for more clarity on the use of the phrase, "application of the required controls (last sentence of M1). Here the SDT uses the word, "controls" in reference to the procedures, processes, etc that are required for protection of the BES Cyber Systems in the other CIP standards.

One commenter asked what VSL would be associated with an update that was less than 30 days late. The SDT notes that VSLs are only referenced after a finding of noncompliance. If the actual performance of the responsible entity meets or exceeds the required performance there is no associated VSL. Another commenter noted that the VSLs for R1 are based on the number or the percent of BES Cyber Assets incorrectly identified and identified that in order to determine the correct number or percent of BES Cyber Assets incorrectly identified, the CEA would have to determine all BES Cyber Assets, including the assets with a low impact to determine the correct VSL; thus, requiring ALL low BES Cyber Assets being identified. The SDT revised the VSLs to remove this conflict. The revised VSLs in R1 are linked more specifically to failure to assign a Facility to the high or medium impact categories.

One commenter recommended modifying the "BES Reliability Operating Services" paragraph, by removing "BES" prefix to Cyber Assets and by eliminating a phrase that seemed redundant in the paragraph and the SDT did not accept these suggestions. Based on other comments and SDT discussions, the SDT revised the informational sections of the standard (as well as R1) to better distinguish between BES Cyber Assets and BES Cyber Systems.

Some commenters noted that the "Evidence Retention" section of the standard used the phrase "until found compliant" in the following: "If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer." The SDT has updated this sentence to reflect the latest language from the enforcement program "until mitigation is complete and approved".

One commenter indicated support for the approach of categorizing systems based on their impact on the Bulk Electric System and proposed having FERC or NERC define which Country Assets are critical for defense and stability of the nation and to define better that for which we are trying to stabilize and provide reliability, thus defining those "BES" components that should be high, medium, or low impact. The SDT applauds this idea, but it is beyond the scope of work assigned to the SDT. The work of the BES Definition team and the work of the Adequate Level of Reliability Task Force may provide more clarity on the issues associated with classifying "Country Assets" in the future.

One commenter asked for a specific implementation timeline for the compliance of the newly identified and categorized BES Cyber Asset(s) and/or BES Cyber System(s) and the SDT notes that this information is contained in the Implementation Plan.

A commenter asked about Section 4.1.2 in relation to smart grid devices being operated by Distribution Providers, or for smart grid assets 100 KV+. The SDT notes that there is no special consideration of "smart grid" devices. The CIP standards specify certain types of Facilities, Systems, and equipment that are included as in scope for applicability of the CIP standards. If the BES Cyber Systems for these Distribution Providers perform that function for the BES, they are in scope. Similarly, for assets at 100KV+, if the BES Cyber Systems for those assets perform the function for the BES, they are also in scope (e.g. PMUs when they affect real-time operations).

A commenter also suggested that battery storage is is not addressed by the standards. The SDT notes that the omission is intentional, since these may include other types of Cyber Assets (e.g., Electronic Access Control and Monitoring Systems).

QUESTION 4 – CIP-002 R2:

Requirement R2 of draft CIP-002-5 states, "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the rationale, requirement, measure, and VSLs associated with Requirement R2 of CIP-002-5. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Please see the redlined version of the standard for a complete set of revisions.

R2 should be modified to read “The Responsible Entity shall have its CIP Senior Manager or delegates approve the identification and categorization required by R1 initially upon an Annual basis, even if it has not identified High or Medium BES Cyber Assets or BES Cyber Systems.”

Response: The SDT has defined the specific time requirement.

For all places where a requirement states "at least once every calendar year thereafter, not to exceed 15 months...”, this means that if the activity is performed every 15 months, then it would have only been performed 4 times in 5 calendar years. This contradicts the "at least once every calendar year..." Similarly for “every 39 months...”.

To ensure that aircraft receive annual inspections once a year, Federal Aviation Regulation (FAR) 91.409(a) requires that" no person may operate an aircraft unless, within the preceding 12 calendar months, it has had (1) an annual inspection in accordance with part 43" etc.

This wording precludes attempts to extend the word "annual" to mean longer than one year, and we suggest that similar wording could be used in the CIPs. For example, "an entity is out of compliance with requirement Rxxx unless, within the preceding 12 calendar months, it has performed X Y Z".

The SDT may want to consider that this requirement and all others that use the words “...initially upon the effective date of the standard...” have this phrase stricken. The implementation plan that accompanies the final approved draft should include the requirements for first time iteration of periodic activities. It’s not reasonable to assume that every entity is capable of executing all procedures “upon the effective date”.

Minor point, but this is the first time “CIP Senior Manager” is used in the standards. Perhaps add a cross-reference to the appropriate requirement in CIP-003-5.

In section “B. Compliance”, under sub-section “1.2 Evidence Retention”, there is a typo in the second to last line. Please change “complaint” to “compliant”.

Response: Changes were made to CIP-002-5 requirement R2 and Attachment 1 to address your comments.

Rationale R2 - Propose a content change:

a. Original Text - The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized.

b. Proposed Change - The lists required by R1 are reviewed annually to ensure that all BES Cyber Systems have been

properly identified and categorized.

R2 - Proposed Change

a. Original Text - The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.

b. Proposed Change - The Responsible Entity shall have its CIP Senior Manager or delegate annually approve the identification and categorization required by R1.

c. Rationale – We note instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.

M2 - Proposed Change

a. Original Text - Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. (R2)

b. Proposed Change - Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate annually approve, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems. (R2)

c. Rationale - The requirement only asks for Senior Manager (or delegate) approval. We note instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.

Response: Changes were made to CIP-002-5 requirement R1 and Attachment 1 to address your comments. Regarding R2 and the replacement of the language with the CAN-010 definition of annual, the suggestion was considered and rejected since the CAN is not meant to be a standard, but simply guidance for compliance enforcement authorities. The SDT has defined exactly what the requirement is.

Requirement 2 and Measure 2 contain the phrase "...initially upon the effective date..." We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year.

If the Guidelines and Technical Basis section will remain in the final published version of the standard, the table on page 18 should be updated to include the Entity Registration of Load Serving Entities with consideration of an "X" in the functional rows of "Dynamic Response", "Balancing Load and Generation" and "Controlling Voltage".

Response: The drafting team agrees with your comment and will remove the "upon the effective date of the standard" from the text.

We do not disagree with the requirement for the CIP Senior Manager or delegate approval. There are clear definitions of the necessary bookends. However, we are concerned that given the recent NERC CAN on "annual" requirements, a separate definition of annual specific only to CIP-002-5 R2 will create confusion in the industry.

Response: Regarding R2 and the replacement of the language with the CAN-010 definition of annual, the suggestion was considered and rejected since the CAN is not meant to be a standard, but simply guidance for compliance enforcement authorities.

Because regional entities already expect evidence to be signed and dated by persons of authority, there is no reason to have a specific requirement to have the CIP Senior Manager or delegate do this. The requirement is unneeded and the compliance auditor likely won't accept evidence for Requirement 1 unless it has been approved anyway by a person of authority. Thus, this requirement actually creates a form of double jeopardy that an entity could be held in violation of Requirement R1 and R2 for failure of the CIP Senior Manager or delegate to approve the list of BES Cyber Asset and BES Cyber Systems categories.

Response: Approval of the lists of Critical Assets and Critical Cyber Assets has been a requirement of CIP-002 in all versions. The SDT believes that an explicit approval of the lists by the Senior Manager or delegate is important as these lists are the foundation for the scope of applicability of the rest of the CIP standards.

The Standards Development Process should not produce standards or requirements that dictate how an entity is to accomplish meeting a requirement. The requirement should direct an entity to develop their Cyber Asset lists. Furthermore, the entity is directed to perform a review and approval process. The level of review and approval should be determined by the entities governance model, organizational structure, compliance culture, etc. It is inappropriate for

the CIP Standards to dictate how the organization manages cyber security requirements or compliance with regulations.

Response: Version 5 is scoped to complete changes responsive to FERC Order 706.

This should be stated clearly that this initial and annual review applies to all BES Cyber assets impact levels, regardless if the entity has not identified High or Medium BES Cyber Assets or BES Cyber Systems.

Response: The requirement for review and approval applies to list required in R1.

a. To add clarity to CIP-002-5 R2, any change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems in between the "once each calendar year" review/approval of the CIP Senior Manager or delegate does not require the CIP Senior Manager or delegate approval.

b. It would be easier to ensure compliance if the requirement to review the list on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders.

Response: There is no requirement to have the CIP Senior Manager or delegate approval of the identification and categorization other than that specified in R2, which is once every year. The requirement language "at least once each calendar year, not to exceed 15 calendar months between approvals" allows sufficient flexibility for the Responsible Entity to manage this periodic compliance.

AZPS recommends changing the language "initially upon" to "prior to". In M2 of R2, the phrase "review and update, where applicable" should be replaced with "review and approve".

Response: Initial requirements are now in the Implementation Plan. The standards language only specifies the periodic requirement.

We recommend that the Senior Manager could approve "prior to or initially upon".

In general, with regard to the proposed CIP Version 5 Standards, it is unclear whether all the requirements have to have been completed at least once prior to the effective date? In some cases, the standard requires that the entity perform some function initially upon the effective date and then have a follow-up requirement (e.g. update cyber security incident plan within 30 days). NERC should provide further guidance in regards to implementation of CIP Version 5 in this regard.

Response: The SDT will take the proposal into consideration. The drafting team agrees with your comment and will remove the "upon the effective date of the standard" from the text.

In M2. Reference to CIP Senior Manager should include "and delegate".

Response: Initial requirements are now in the Implementation Plan. The standards language only specifies the periodic requirement.

We would vote yes if the words "Initially upon the effective date of the standard" were changed to "within 12 months prior to effective date of the standard."

Response: The drafting team agrees with your comment has removed the "upon the effective date of the standard" from the text. Initial requirements are now in the Implementation Plan. The standards language only specifies the periodic requirement.

For clarity in R2 and M2, request 1) using the term "annual" instead of all these extra words and 2) making "annual" a Glossary term

Response: The term "annual" is used in many other NERC standards. The SDT opted to include the specific periodic language in the requirement itself to avoid repercussions in other NERC standards.

The assumption is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, R2 will not apply to those utilities.

Response: Responsible Entities that own assets qualified under the registration criteria are included in section 4.

"Upon the effective date" should be restated to read "on or (within 30 days) prior to. A list of Low impact BES facilities is not required to be maintained, however, certain standards require controls to be enforced at these facilities. At the very minimum, the standard should require that the RE's approval of High and Medium lists should include a list of facilities and systems considered as potential candidates for the evaluation.

Response: The SDT will take the proposal into consideration. The drafting team agrees with your comment and will remove the "upon the effective date of the standard" from the text.

Should it not read delegate(s) instead of just delegate? There could be more than one delegate.

The measure makes no mention of the delegate(s) approval? Need consistency between the Requirement and the measure.

1.2 Evidence Retention: Please explain what "Other evidence" would be required.

Response: As an example, if the requirement is to keep 90 days of event log entries, the Responsible Entity is not required to keep the event logs for the full compliance period between audits, but to be able to produce evidence that these logs have been retained for 90 days on a rolling basis during that period. Evidence could be logs of the process that

ran to implement the 90 day rolling event log.

We believe R2 should say “initially prior to or upon the effective date of the standard...” Without that, it would seem the CIP Senior Manager or delegate(s) would need to approve the lists precisely on the effective date.

Response: The drafting team agrees with your comment and has removed the “upon the effective date of the standard” from the text. Initial requirements are now in the Implementation Plan. The standards language only specifies the periodic requirement.

CIP-002 R2: a. The following wording should be added to the Measure in CAPs,"

BES Cyber Assets and BES Cyber Systems initially upon....." should become "High and Medium Impact BES Cyber Assets and BES Cyber Systems initially upon....."

Evidence Retention comment:

1.2 We recommend the deletion of the following sentence "For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit." as it contradicts the requirement to retain the data for three calendar years.

Response: The SDT will take the proposal into consideration.

R2 Rationale CHANGE: “Manager’s approval” TO: Manager’s responsibility in approval”

RATIONALE: the Senior Manager or delegate performs an approval, but the responsibility remains with the Senior Manager.

Response: The SDT will take the proposal into consideration.

Why does this need to be a recurring requirement? Upon identification and categorization, there are typically no changes and those that do change are typically addends. All I am saying is that this requirement asks for every Responsible Entity to do an exercise even if a large majority of the entities will have a similar or identical result as the previous year. I don't see the point.

Suggest: "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and upon Cyber Asset or Cyber System changes."

Response: The SDT will take the proposal into consideration.

General - For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.

Response: The SDT will take the proposal into consideration.

CIP-002-5 makes great strides to remove ambiguity and categorize the potential impacts of Cyber Assets. However, the standard should be changed in one of the following:

1) plainly state those entities with no BES assets per the definition are not required to adhere to this standard or, alternatively, the Senior Manager must annually certify that the entity has no BES assets per the definition thus no Cyber Assets; or,

2) create a fourth category stating No Impact, thus no further action required which can be certified annually by the Senior Manager.

Response: The SDT is aware of the DP and LSE issues and will consider your response.

QUESTION 5 – CIP-002 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-002-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

All comments not directly related to VRFs/VSLs for CIP-002-5 are addressed in Question 2.
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.

Response: The drafting team debated and developed the Table of Compliance Elements along with VRFs and VSLs to simplify and account for risk and severity measures with respect to the reliability of the BES.

Issue - We believe that the VSLs recognize the fact that entities of different sizes are taken into account in the severity levels and associated impacts to the BES.

Response: Violation Severity Levels are a measure of performance towards a standard independent of the size of the registered entity, and the drafting team developed the VSLs for the cyber security standards to account for the wide range of entity configurations and systems. The drafting team included both percentages and fix numbers of BES Cyber Systems and BES Cyber Assets in the VSLs to account for the wide range of entities with an objective toward reaching a

more equitable effect of the requirements on all entities.

The VSL table should refer to BES Cyber Assets and BES Cyber Systems (not just BES Cyber Assets) as does Requirement R1 for consistency with terminologies used in R.1 & R.2.

Response: The language of the VSLs will be revised.

Percentages of non-compliance are difficult to determine; using discrete numbers of non-compliant assets would be preferable in determining the R1 VSL. This is particularly true where random sampling of the entity's assets is performed and the number of failures is derived by extrapolation.

Response: The VSLs were developed to account for the wide range of entity configurations and systems. The drafting team included both percentages and fixed numbers of BES Assets in the VSLs to account for the larger and smaller entities with an objective toward reaching a more equitable effect of the requirements on all entities.

Additionally, the R1 VSLs refer to entities with more than 100 High and Medium Impact BES Cyber Assets (or 100 or fewer such assets). Is this count determined by the entity's determinations prior to the audit or is the count determined by the auditor, adjusting the entity's initial determination upon finding a possible violation?

Response: The methods and processes used to determine compliance with the requirements is a compliance process question and should be addressed to NERC's Compliance Department to achieve a consistent approach and determination.

The standard refers to BES Cyber Systems as well as BES Cyber Assets. It appears that the VSL requires the compliance monitoring and enforcement staff determining the VSL to break down each BES Cyber System into its BES Cyber Asset components in order to achieve the correct determination. As the bright line criteria remove any subjectivity from the categorization process, the R1 VSL should be binary. Either the entity got it right or the entity did not. There should be only one VSL, that being "Severe." Similarly, the R2 requirement is very straightforward and a binary VSL is appropriate in that instance.

Response: The language of the VSLs will be revised to include both BES Cyber Systems and BES Cyber Assets. The methodology and process used to determine compliance with the requirement is a compliance process question and should be addressed to NERC's Compliance Department to achieve a consistent approach and determination.

The Violation Risk Factors do not intuitively align with Violation Severity Level (VSL). Requirement 1 assigns a 'High" VRF independent of the potential low or no risk associated with instances in which BES Cyber Assets or BES Cyber Systems are assigned risk levels higher than those required. EEI would like a more risk based approach in which the compliance assessment considers risk in any non-compliance finding.

Response: The drafting team debated and developed the Table of Compliance Elements along with VRFs and VSLs to simplify and account for risk and severity measures with respect to the reliability of the BES. Violation Severity Levels are a measure of performance towards a standard independent of the size of the registered entity, and the drafting team developed the VSLs for the cyber security standards to account for the wide range of entity configurations and systems. The drafting team included both percentages and fix numbers of BES Cyber Systems and BES Cyber Assets in the VSLs to account for the wide range of entities with an objective toward reaching a more equitable effect of the requirements on all entities. The Violation Risk Factors are designed to assess the impact to reliability of violating a specific requirement, and to determine an appropriate sanction when the associated requirement is violated (refer to the ERO Sanctions Guidelines document). When a single requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, following the FERC Order of May 18, 2007, the VRF assignment must not be watered down to reflect the lesser risk level. The drafting team defined the VRFs for the cyber security standards in accordance with these guidelines.

For the Last Paragraph VSL's within R1 (failed to update its documentation), we propose the following time periods:

Lower - More than 30, but less than or equal to 60 calendar days

Moderate - More than 60, but less than or equal to 70 calendar days

High - More than 70, but less than or equal to 80 calendar days

Response: The portion of the VSL for R1 that refers to the number of calendar days taken to update its documentation following the completion of a change to the BES Asset or BES System categorization will be revised by the Drafting Team.

We propose that documentation errors should rarely if ever be deemed high/severe. Only violations that could have an immediate impact on the reliability of the BES should be considered high/severe.

Response: The omission of a BES Cyber Asset in the documentation required in CIP 002 may not always be a documentation error. The omission could be a result an incorrect application CIP-002 resulting in a BES Cyber Asset being incorrectly classified and protected under the requirements stated in CIP-003 to CIP-011. While the drafting team agrees that the updating of documentation as an isolated incident is not severe, the updating of documentation associated with the identification and categorization of its BES Cyber Systems and BES Cyber Assets is critical to the reliability of the BES, since it could lead to inadequate security measures or erroneous operations.

The severity levels are determined by, among other things, the number of low impact cyber assets that are categorized improperly. The entity is not required to keep records of low impact cyber assets. This approach will not work.

Response: The severity levels are determined by the impact of the BES Cyber System or BES Cyber Asset on the reliable operation of the BES if the BES Cyber System or BES Cyber Asset is destroyed, degraded, or otherwise rendered

unavailable. The Low Impact BES Cyber Systems or BES Cyber Assets are not required to have discrete identification.

The VSLs for R2 are not consistent with the requirement. Requirement R2 allows the CIP Senior Manager or delegate to approve identification and categorization of High and Medium Impact BES Cyber Assets or BES Cyber Systems. The VSLs drop the "or delegate" language which implies the CIP Senior Manager has to approve the categorization and identification. The "or delegate" language should be added back.

Response: The drafting team agrees with your comment and will insert the "or delegate" language as indicated in the VSLs for R2.

R2 VSL - We do not believe that being late by 30 to 40 days is adequate since this a mere review of the list each year. We suggest changing the LOWER to "30 to 60 days", then have 10 day increments for the rest of the VSL such as "60 to 70 days" for MEDIUM, "70 to 80 days" for High, and "80 to 90 days" for SEVERE.

Response: The drafting team believes that the current range of days for review and approval of the required categorization of BES Cyber Systems and BES Cyber Assets is appropriate and commensurate with the due diligence that is required by CIP 002.

The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.

Response: CIP 002, which is the scoping standard, is the foundation for CIP Version 5 Cyber Security standards. The CIP-002 standard is designed to identify and categorize the BES Cyber Systems and BES Cyber Assets that if destroyed, degraded, or otherwise rendered unavailable can potentially impact the reliable operation of the BES. An error in addressing the requirements of this CIP standard could result in the incorrect or inappropriate application of controls listed in standards CIP 003 to CIP011. Hence, the drafting team believes that the VSL severity levels for this standard are appropriate.

In general, regarding VRFs in each of the CIP standards, it is our understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement. For instance, the VRF should be used to differentiate between violating the Disturbance Control Standard (BAL-002), and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form "Do X" to all of "these systems" and the VRF is very dependent on the system involved. VRF's should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRF's are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on

VRF determination, or the SDT should split the requirements so that appropriate VRF's can be applied.

Response: The Violation Risk Factors are designed to assess the impact to reliability of violating a specific requirement, and to determine an appropriate sanction when the associated requirement is violated (refer to the ERO Sanctions Guidelines document). The VRF is not meant to compare the severity of the reliability impact of one requirement with another. When a single requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, following the FERC Order of May 18, 2007, the VRF assignment must not be watered down to reflect the lesser risk level. The drafting team defined the VRFs for the cyber security standards in accordance with these guidelines. The drafting team recognizes the possible extraordinary level of effort required to protect the numerous Low Impact BES Cyber Systems and BES Cyber Assets, and therefore strived to minimize the potential workload of protecting the Low Impact BES Cyber Assets and BES Cyber Systems by limiting the specific requirements that are applicable to those BES Assets. The drafting team believes that the VRFs for this requirement are appropriate.

Under the Table of Compliance Elements is included the phrase "Operations Planning" under the "time horizon" column. The industry cannot predict with certainty future upgrades and additions to the system, yet the standard appears to state that VSL apply to the planning time horizon under the "time horizon" column. It may be that the standard intends to apply to operations only, but this is not clear in the text since both "Operations" and "Planning" are capitalized. Please clarify.

Response: The meaning of the entries in the "time horizon" column in the Table of Compliance Elements is defined by NERC. The "Operations Planning" timeframe is defined as "operating and resource plans from day-ahead up to and including seasonal", and "Real-time Operations" is defined as "actions required within one hour or less to preserve the reliability of the bulk electric system". Please refer to the NERC Time Horizons document at http://www.nerc.com/files/Time_Horizons.pdf.

While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies.

Recommend Low, Medium, High and Severe VSL's for all requirements.

Response: The VSLs were developed to account for the wide range of entity configurations and systems, as well as the specific requirements. Some of the requirements are "binary" in nature (either the entity meets it or it doesn't), and a partial compliance is not possible. Following FERC's June 19, 2008 Order on Violation Severity Levels, these binary VSLs are by definition Severe.

This standard has a high VRF that applies to requirements for both high and medium impact asset categories. We

recommend a medium VRF for the medium impact assets to recognize the difference between asset impact categories.

Response: CIP 002 R1 includes the classification of all BES Cyber Assets into appropriate impact categories. An error or omission on the part of an entity in the performance of the tasks required by the standard or in the upkeep of documentation that is proof of performance of these tasks could result in an asset being incorrectly classified or completely omitted from classification. The result of such an error would cascade to the application of the controls stated in CIP 003-CIP011 and hence jeopardizing the reliability of the BES due to the incorrect application of cyber security controls. The Higher VRF associated with this requirement is due to these reasons. The VRF does not apply just to the classification of assets as Low Impact but rather to the entire process by which such a determination is made. Requirement R2 carries a lower VRF since the task associated with this requirement is a demonstration of senior management involvement and approval of the entity's BES Cyber System and BES Cyber Asset identification and categorization. The drafting team believes that the VRFs for this requirement are appropriate.

"And" needs to be struck from moderate and high VSL in the phrase "High and Medium Impact and BES Cyber Assets".

The drafting team agrees with your comment and will remove the extra "and" from the Moderate and High VSL language for R1.

We are concerned that an entity will need to produce a list of Low-Impact BES Cyber Assets to demonstrate that they have correctly (or incorrectly) categorized BES Cyber Assets in the "Low-Impact" category. This overall proposal is not substantive enough to objectively assess VSRs and VSLs. We recommend that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.

Response: The drafting team is keenly aware of the possibility to inadvertently require entities to produce a list of Low Impact BES Cyber Assets, and included language in the standard to avoid the generation of the list of Low Impact BES Assets. The wording states that "discrete identification" of Low Impact Assets is not required.

We recommend that the high VRFs and VSLs are extreme and the definition of what is high, medium, or low violations are unclear and need to be clearly defined in order to show how entities can fully comply.

-No mention of BES Cyber Systems throughout the VRF/VSL, only mentions BES Cyber Assets.

-R2: There is no mention of the delegate(s) completing the annual review. Delegate is called out in the requirement.

Response: The VSLs were developed to account for the wide range of entity configurations and systems, as well as the specific requirements. Some of the requirements are "binary" in nature (either the entity meets it or it doesn't), and a partial compliance is not possible. Following FERC's June 19, 2008 Order on Violation Severity Levels, these binary VSLs are by definition Severe. The Violation Risk Factors are designed to assess the impact to reliability of violating a specific

requirement, and to determine an appropriate sanction when the associated requirement is violated (refer to the ERO Sanctions Guidelines document). When a single requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, following the FERC Order of May 18, 2007, the VRF assignment must not be watered down to reflect the lesser risk level. The drafting team defined the VRFs for the cyber security standards in accordance with these guidelines.

The language of the VSL requirements will be revised to include "BES Cyber Systems" in R1 and "or delegate" in R2.

Seems like if you incorrectly categorized or missed 5% or fewer of your assets, by default you are automatically put into the Severe VSL range as it most likely will have been more than 60 days since the BES Cyber System was identified or categorized. If it only covers major changes to facilities and elements and not cyber systems, it would not be a concern - but this would need to be spelled out.

Response: Please note that there are multiple parts to the VSL definition for R1. One part requires an entity to correctly identify and categorize its BES Cyber Assets and BES Systems, and the second part refers to the number of calendar days taken by the entity to update its documentation following the completion of a change to its BES Cyber Systems or BES Cyber Assets. The first part of the VSL is in relation to the identification and categorization of BES Cyber Systems and BES Cyber Assets that have a High or Medium Impact on the reliable operation of the BES. If an entity incorrectly identifies or categorizes 5% or fewer of these assets at a lower category, then the entity will be in violation of the CIP-002-5 standard.

If an entity implements a change to the BES that is planned to be in service for more than 6 calendar months and it causes a change in the identification or categorization of its BES Cyber Assets or BES Cyber Systems from a lower to higher impact category, then the change needs to be documented within 30 calendar days of its implementation.

The type of change (major, minor, or other) is not addressed since the drafting team is concerned about the reliability of the BES and the impact of any change to the BES Elements that results in a change to the identification and categorization of the BES Cyber Systems or BES Cyber Assets.

VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.

Response: The comment requires changes to the compliance methodology and processes that must be addressed by the NERC Compliance Department and is out of scope of the drafting team for this standard.

In general, the VSL should relate to reliability and not administrative errors.

Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation

management VSL model may offer an alternative model to follow.

Response: An "administrative error" resulting in the failure to identify a High or Medium Impact BES Cyber Asset or BES Cyber System could potentially result in the BES Asset not being afforded the protections mandated by the NERC CIP Standards. The drafting team strived to define VSLs that are related to the reliable operation of the BES and to limit the effect due to administrative errors. However, administrative errors also need to be recognized and corrected in a timely manner. The SDT will examine the VSLs for FAC-003 for consideration.

QUESTION 6 – CIP-003 R1:

CIP-003-5 R1 states "Each Responsible Entity shall identify, by name, a CIP Senior Manager." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R1 and Part 1.1 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Industry comments raised a number of valid issues with CIP-003-5 R1. Many commenters were concerned with the reordering of the requirements. The opinion of the SDT in developing the first draft of version 5 was that the designation of the CIP Senior Manager should come prior to the requirement for Cyber Security Policy. However, the SDT was persuaded by industry comments and restored R1 as the Cyber Security Policy and moved the requirement to identify a CIP Senior Manager to Requirement R3. Other requirement ordering in CIP-003-5 may still impact existing compliance

documentation, however.

For instance, some commenters requested that requirements for low impact assets be collected and presented in a single location. The SDT agreed with this approach and modified the standards to include a single policy requirement for low impact BES Cyber Systems and included it as R2. This will displace the existing numbering for CIP-003-4, but compliance documentation impacts were unavoidable as several requirements from CIP-003-4 were either removed entirely or relocated to other standards.

Several entities raised concerns about the requirement to have a single senior manager. This was a key point of FERC Order 706 and as such is still included in the requirement. However, it should be noted that it is not the intent of the SDT or this requirement to dictate a particular organizational structure. Some comments were raised concerning repeating the phrase which defines the CIP Senior Manager in the language of the requirement itself. In drafting the CIP Standards, the SDT attempted to remove all cases which required an explicit cross reference to a requirement in another standard. As such, the SDT proposed a definition of CIP Senior Manager to be included in the NERC Glossary. This definition adequately clarifies the authority and responsibility of the CIP Senior Manager.

Additionally, commenters raised concerns, in this requirement and others, about specific examples included in the measures. To be clear, the measures are not mandatory or enforceable. In some cases, it is true that in the measures the SDT mentions items not specifically included in the language of the requirement. The SDT is attempting to use the measures as a tool to provide guidance about what may be considered high quality evidence, not to indicate any particular required performance, and encourages the industry to read them in the context in which they were intended.

QUESTION 7 – CIP-003 R2:

CIP-003-5 R2 states "Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R2 and its associated rationale and measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address

the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Many comments raised valid concerns that some topics that were required to be included in the policy for low impact BES Cyber Systems were not addressed elsewhere in the CIP Standards. The SDT appreciates this concern and in response has drafted a separate policy requirement specific to BES Cyber Systems not identified as high impact or medium impact - see Requirement R2 in the revised standard. (Policies for high and medium impact BES Cyber Systems were moved to Requirement R1 in the revised standard.)

Some commenters requested additional specificity to be included as to the nature of the cyber security policy. The SDT believes that in order to have effective policies, organizations need the flexibility to write policy in a manner in which is compatible with their corporate culture. As such, the SDT has allowed for flexibility to have higher level policies as well as very detailed policies.

A number of commenters raised concerns that the requirement to "implement" the cyber security policy may raise double jeopardy concerns with other CIP Standards. The SDT is very concerned about possibilities of double jeopardy, but disagrees that there is a double jeopardy issue here. The policy does not have the same level of granularity as the other requirements and the SDT does not believe that a violation of another CIP requirement would constitute a violation of the policy requirement. The "implement" language was added to the policy requirement as a result of FERC Order 706 paragraph 75 and the intent is for the Responsible Entity to demonstrate that it has not written a policy and put it on a shelf somewhere but is actively using it and abiding by its statements.

> Order 706, Paragraph 75: Consistent with that proposal, the Commission concludes that, where the CIP Reliability Standards obligate a responsible entity to develop and maintain a plan, policy or procedure, there should be a corresponding obligation to implement the plan, policy or procedure. However, while the CIP NOPR proposed to interpret the CIP Reliability

Standards as including an implicit obligation to implement plans, policies and procedures, we are persuaded by the commenters that a better approach is for the ERO to develop modifications to the CIP Reliability Standards that contain appropriate implementation language. Accordingly, we direct the ERO to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards.

Also, of concern to the SDT were comments that suggested that the policy requirement was administrative in nature or simply a documentation burden. The SDT disagrees that security policies are administrative in nature because they require documentation. The SDT believes that security policies are essential for an organization to ensure an effective security posture. Security policies were a concern identified in both the FERC Order No. 706 as well as the 2003 Blackout Report.

In addition, a number of commenters expressed a preference for all modifications to the language to return to the previously vetted and approved language of version 4. The SDT appreciates the concern about the use of previously approved and vetted language and has attempted to retain this language wherever possible. Some of the changes in language are a result of directives from FERC Order 706 while others are made based upon industry feedback.

Additionally, the SDT has attempted to bring the CIP standards in line with the NERC Results Based Standards format. As such, there were a number of language changes made based upon the requirements structure identified in the NERC Results Based Standards format. While the drafting team agrees that there is value in utilizing previously vetted language where possible, it believes that the migration to the NERC Results Based Standards format is the best approach for the future evolution and maturation of the standards.

QUESTION 8 – CIP-003 R3:

CIP-003-5 R3 states "Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals." Do you agree with the proposed Requirement R3? If not, please explain why and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R3 and its associated rationale and measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address

the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Several commenters noted that the language of the proposed CIP-003-5 R3 was unclear. The SDT has attempted to reword the requirement to provide clarity as to the intent. The SDT removed the phrase, "initially upon the effective date of the standard," and rearranged the sequence of information in the requirement but did not otherwise change the scope or intent.

Additional comments questioned the need for annual approval of the policy, particularly in situations where updates to the policy are not needed. The SDT believes that the periodic approval reaffirms management's commitment to the protection of its BES Cyber Systems. A few commenters also suggested an allowance for the policy to be approved by a delegate of the CIP Senior Manager. While the SDT appreciates this desire, the SDT believes that this is one area that must be approved by the CIP Senior Manager and not a delegate. This is consistent with previous versions of the CIP Standards.

QUESTION 9 – CIP-003 R4:

CIP-003-5 R4 states "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function." Do you agree with the proposed Requirement R4? If not, please explain why and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R4 and its associated rationale and measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address

the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Industry highlighted a number of concerns around the clarity of the proposed language of CIP-003-5 R4 and the potential overlap with the existing training and awareness program in CIP-004-5. The SDT was persuaded by these comments and has proposed the deletion of R4 with a corresponding addition in CIP-004-5 to explicitly require annual training on the cyber security policy (see CIP-004-5, Requirement R2, Part 2.2 and Requirement R3, Part 3.2).

Several commenters also requested that the list of acceptable types of evidence to support compliance in Measure M4 be either removed or clarified. The Standard Drafting Team responded that it did not intend the measure to be an exhaustive list of acceptable forms of evidence, but rather a list of possible examples.

Commenters also argued that this requirement should apply to onto those entities that have High Impact or Medium Impact BES Cyber Security Systems. The SDT responded that to ensure the overall culture of security for the industry, these are minimum areas that should be implemented by all owners of BES Cyber Security Systems.

QUESTION 10 – CIP-003 R5:

CIP-003-5 R5 states "The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated." Do you agree with the proposed Requirement R5? If not, please explain why and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R5 and its associated rationale and

measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Many commenters raised concerns about the significant overhead that may be required to track multiple levels of delegations. The SDT is persuaded that the documentation required to maintain documentation of multiple levels of delegations may be burdensome to some organizations. As such, the SDT has proposed language closer to the existing approved language of version 4 which did not explicitly allow for sub-delegations.

Additionally, the SDT believes that the additional flexibility allowed with the ability to delegate by title will make this proposed standard less burdensome, without any decrease in effectiveness, over previously approved versions of the standard.

A number of commenters noted the discrepancy between the written R5 Requirement and the measure that according to the requirement, delegates can be documented "by position or name of the delegate" yet the measure states that the document must include an actual name. The requirement and measure have both been rewritten to clarify that the document may include either the name or the title of the designee.

A number of commenters also raised questions about the consistency of the use of the term position vs. title. The SDT has revised the standard with consistent language using "title".

QUESTION 11 – CIP-003 R6:

CIP-003-5 R6 states "Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R6 and its associated rationale and measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

There were 3 primary issues raised by commenters concerning CIP-003-5 R6. First, commenters rightfully pointed out that the reference to the footnote was not properly superscripted. The SDT determined that the footnote should instead be included in the language of the requirement itself and the superscript "2" was deleted.

Several commenters made reference to revert the language back to the previously approved language of version 4. The SDT interpreted this to mean that the commenters preferred that the requirements to update the CIP Senior Manager and delegate should be included as separate sub-requirements. The SDT appreciates the desire to use the previously vetted and approved language. However, the change to explicitly call out updates to the CIP Senior Manager and the delegation in a single requirement (instead of sub-requirements of other requirements) allows for consistency with respect to the VRF and VSL for the requirement to have up-to-date documentation. As it exists in the version 3 standards, an update to a delegation outside of the 30 day window would constitute a violation of CIP-003-3 R2.3 instead

of CIP-003-3 R2.2 where the proper VSL is aligned with the activity.

Additionally, a few commenters requested that the SDT allow additional time to update documentation beyond 30 days. The SDT has chosen to keep the currently approved time window of 30 days in an effort against creating a situation where we are lessening the current level of compliance, which is not allowable without significant justification to the Commission and other governmental authorities.

QUESTION 12 – CIP-003 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-003-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the VSLs for R1, R3, and R4, and only minor or no changes to the VSLs for R2, R5 and R6. The SDT also changed the VRF for M3 from "Lower" to "Medium".

Please see the redlined version of the standard for the complete set of revisions.

A number of good concerns were raised by commenters regarding the VSLs and VRFs. Overall, commenters expressed a desire for additional granularity and reduction of severity with regards to VSLs. The SDT agrees with many of the comments that additional justification for VSLs and VRFs is needed. The VRFs and VSLs are based upon guidelines developed by NERC and FERC, and the SDT has provided an analysis of the VSLs and VRFs based upon these guidelines. One item of note was concern that the VSL for R4 was inconsistent with the stated SDT intent that awareness of the policy did not imply that this awareness should be investigated on an individual by individual basis. This issue has been resolved by the deletion of R4 and the introduction of cyber security policy as an explicitly required element of the training program in CIP-004-5.

Additionally, the core of several comments for additional granularity appeared to center around the severity as it may relate to multiple violations. The NERC and FERC guidelines make clear that VSLs should be written to account for single violations and not cumulative violations. As such, in many cases, additional granularity is not warranted.

Several commenters also expressed concern about the VRF level for the identification of the CIP Senior Manager. The SDT notes that this VRF is based on the VRF in previously approved version of the CIP-003.

QUESTION 13 – CIP-004 R1:

CIP-004-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made no changes to Requirement R1 but did make significant changes to Part 1.1 and its associated rationale and measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The SDT has reassessed the overall scope and applicability during the comment review period, and has concluded that CIP-004-5, R1 represents an approach which is a reasonable effort to advance the cyber security of the Bulk Electric System and critical infrastructure overall.

After review of the comments, the SDT updated the requirements with a goal toward improved clarity, while trying to maintain a balance of reasonable security awareness and to moderate audit impact. The changes to Requirement R1 include the following:

• Table R1: In response to several commenters asking for clarification as to who at the Responsible Entity should receive

security awareness information, the SDT has added the term "personnel" to the requirement.

• In response to comments that quarterly awareness is too frequent, the SDT made no changes because the team believes the current requirement of quarterly security awareness is appropriate for Version 5. Note that the measure for this requirement provides several ways an entity may demonstrate that it has implemented a security awareness program. In addition, the SDT narrowed the scope of entities that must comply to just the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to High and Medium Impact BES Cyber Systems.

• In response to concerns that R1 indicates that each of the applicable items in Table 1 are to be implemented, the SDT notes that even though there is only one Part, using "applicable items" is consistent with the rest of the standard, and the "applicable items" references the required elements of the requirement part language that a security awareness program must convey ongoing cyber security awareness of both authorized electronic and authorized unescorted physical access.
• In response to comments that the requirement in the table uses unmeasureable terms; such as a program that "conveys" security awareness, and the term "on-going" reinforcement, the team made no changes. The intent of R1 is to require all Responsible Entities who have High and Medium Impact BES Cyber Systems to have a security awareness program that communicates ("conveys") information to personnel that supports and informs effective security practices. The use of the term "access" covers both authorized unescorted physical access and authorized electronic access. The term "on-going" is used in the current standards and repeated in Version 5 to help with consistency.

• In response to comments that the capitalized term "Facilities" needs to be clarified in the Applicability section of the standard, the team has reviewed the Applicability sections of each standard to address the consistency issue. The capitalized term "Facilities" refers to the definition in the NERC Glossary of Terms.

• In response to comments that clarity and consistency is needed between the requirement and the Implementation Plan, the team has revised the Implementation Plan to clarify compliance on the Effective Date.

•In response to concerns to be "compliant" with requirements that simply rely on documentation, the drafting team believes documentation is appropriate for demonstrating compliance with the standards.

In addition, several commenters provided comments specific to Requirements other than Requirement R1, and those comments are addressed in the summary responses for the appropriate questions.

QUESTION 14 – CIP-004 R2:

CIP-004-5 R2 states "Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R10 and to each of its Parts (2.1 through 2.10) and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The SDT has reassessed the overall scope and applicability during the comment review period.

After review of the comments, the SDT updated the requirements with a goal toward improved clarity. The changes to Requirement R2 include the following:

•In response to comments that Requirement R2 precludes an awareness and training program that covers all aspects of CIP for individuals who have access to BES Cyber Systems, it is not the intent of the team to preclude a single, comprehensive cyber security awareness and training program; however, all requirements of Requirement 1 and

Requirement 2 must be met.

•In response to comments that Requirement R2 should be reworded from "…contains the proper policies…" the SDT agrees, and has made the proposed change in the Rationale for Requirement R2 by adopting the phrase, "…covers the proper policies…".

•In response to comments as to whether the role-based training approach adequately addresses Order 706, Paragraph 435, the team believes the awareness and training programs adequately address FERC Order 706, Paragraph 435.

> Order 706, Paragraph 435: Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves.

• In response to comments that FERC Order 706, Paragraph 435, calls for identifying what "…role and steps should be taken by the ERO to ensure quality and consistency of trainers," that Requirement R2 should identify what areas of the standards that the training program must include, the SDT discussed the issue of adequate training for the trainer and agreed that trainers do not need any special certification beyond the CIP training provided to personnel. The SDT believes the awareness and training programs adequately address FERC Order 706, Paragraph 435.

•In response to several comments suggesting Requirement R2 Part 2.2 should be eliminated, the SDT has removed Part 2.2 from Table R2. Requirements R2 Part 2.3 2.4 adequately capture the requirement.

•In response to several comments suggesting Requirement R2 Part 2.6 word change from "Original - Training on handling of BES Cyber System Information and storage media." The SDT agrees that the result of the requirement should provide training and handling on BES Cyber System Information and its storage (without specifying "media" and has modified the language to remove the word "media."

•In response to clarify wording in the requirement to make explicit Parts 2.7 and 2.9, the SDT believes Parts 2.7 and 2.9 in Table Requirement R2 should remain separate entries. The training requirement on connectivity has been modified to clarify the content should focus on the risks of a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets. The SDT has clarified the Applicability for the training on the visitor control program to include both physical and electronic access.

•In response to comments that the statement, "Define the roles that require training," implies that some roles do not require training, the SDT agrees and has modified the language in Requirement R2 Part 2.1 of Table R2 to use "identification" instead of "define".

•In response to concerns that CIP-004-5 R2 and CIP-004-5 R3 need to be consistent, the SDT has modified the

Applicability column in Table R2 to be consistent with Table R3.

•In response for clarification as to whether training on the visitor control program includes both electronic and physical access, the SDT has clarified the Applicability for the training on the visitor control program to include both physical and electronic access. The training for a visitor control program should focus on the responsibilities for each role designated by the entity that participates in the program; e.g., it is important to train individuals who serve as escorts on their roles.

•Requirement R2 Part 2.10: In response to comments concerning role-based training on the BES Cyber System's interconnectivity and interoperability with other cyber systems, the team has modified the requirement for clarification that the content should focus on the risks of a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets. The team has modified Requirement R2 Parts 2.3 through 2.10 to require "training content," and added examples in the Measures.

•In response to requests for clarification on role-based training, comments that Parts 2.3 and 2.5 be combined, and that Part 2.7 should also be deleted and its concepts combined with Part 2.9, the team has added "and training required for each role" to Part 2.1 of Table R2. However, the SDT disagrees with the combination of Parts 2.7 and 2.9, as these address different activities.

•Requirement R2 Part 2.3: In response to comments that the phrase "proper use" of physical access controls is not consistent, the SDT agrees and has removed "proper use" from Part 2.3 of Table R2.

•In response to comments that the requirement should include Cyber Assets as well as Cyber Systems, the SDT has modified the Applicability section to include associated Physical Access Control Systems and associated Electronic Access Control or Monitoring Systems for High and Medium Impact BES Cyber Systems.

•In response to comment that the "Delivery of cyber security training to vendor support staff on site at a Registered Entity's facility can be difficult to document," the SDT would request specificity regarding the challenge of documenting training to vendor support staff. The Responsible Entity may allow vendor attestations in accordance with its policies, practices, and procedures.

•In response to concerns that the requirement has the potential to be highly violated and that may or may not prevent a physical or cyber event, the SDT disagrees. The team believes that this requirement is necessary, it provides the requirements to be met for an entity's training program.

•Measure M2: In response to comments to change the word "must" in M2, the team was attempting to make a distinction by using the word, "must" for instances where the Responsible Entity "must" have something as evidence. Since there are many ways of demonstrating "how" an entity has implemented a procedure, the word, "may" has been

used ahead of samples of performance that may be acceptable.

•Requirement R2 Part 2.1: In response to suggestions that Part 2.1 require the role definitions to be reviewed on an annual basis, the SDT notes that Requirement R2 specifies what must be included in the training, and Requirement R3 requires when and how frequently the training required in Requirement R2 must be conducted.

•In response to suggestion that the term "Storage Media" be defined, the drafting team has removed the term "media" from Requirement R2 Part 2.6 and the associated measure.

QUESTION 15 – CIP-004 R3:

CIP-004-5 R3 states "Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in *CIP-004-5 Table R3 - Cyber Security Training."* **The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.**

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R3 and Parts 3.1 and 3.2 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

After review of the comments, the SDT updated the requirements with a goal toward improved clarity. The changes to

Requirement R3 include the following:

•In response to suggestions of changing "each individual needing authorized electronic" to "each individual with authorized electronic," the SDT modified the language to "to attain and retain" authorized electronic or unescorted physical access.

•In response to suggestion of changing the phrase "associated with," the SDT has revised the Applicability sections to help clarify the meaning of the term "Associated" as it is used with Physical Access Control Systems, Electronic Access Control or Monitoring Systems, or Protected Cyber Assets.

•In response to several comments that Tables in Requirement R3 apply to only High and Medium impact assets, the SDT notes that it has moved the requirements for Low Impact BES Cyber Assets into CIP-003-5 to emphasize the programmatic nature of these controls, which further clarifies that the requirements do not apply to "Low Impact"

•In response to suggestions that Requirement R3 Parts 3.1 and 3.2 should clarify the required training is role-based, the SDT agrees and has modified Requirement R3 to include a reference to "role-based."

•In response to requests for clarification of Requirement R3 Part 3.2, "annual" training as being completed within 15 months, the team reviewed the requirement, and believes inclusion of 15 months to complete training in Part 3.2, Table R3, does not preclude an entity from using only the once every calendar year timeframe. When an individual is assigned a new role, the training should be completed prior to granting new access, not within 30 days.

•In response to request to clarification of Requirement 3.1 on whether all personnel who access the systems during a CIP Exceptional Circumstance require training after the fact, the team notes that the requirement requires training before access is granted, and the CIP Exceptional Circumstance exception clarifies that such training is indeed not required before granting access in those instances (e.g., in emergency situation that is a CIP Exceptional Circumstance, such training is not required of responding emergency personnel before they are granted access).

•In response to the suggestion to eliminate Requirement R3, the SDT made no changes. The requirement is necessary, as it requires completion of the training in R2 before access is granted.

•In response to the suggestion to modify the requirement to read, "Require completion and documentation of the training specified . . .." the SDT agrees and has made the suggested addition to Part 3.2.

•Measure M3.1: In response to comment to delete the phrase, "the date access was first granted," the team made no changes, as although the requirement does not include documenting the date access was first granted, the entity must demonstrate that it provided the training before access was granted – and this is hard to do without the dates involved.

The Measure uses "may" so that date is not required to be tracked.

•In response to comments that a potential oversight in all versions of the CIP-004 standard is guidance on the training requirements for "transient" workers, the SDT reviewed the requirement and transient workers still need the applicable training before authorized electronic or unescorted physical access is granted. Additional training would not be needed if access was removed and then reinstituted for the same individual, with the same role, within the same calendar year as the training occurred.

•In response to comments that "Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems" be removed from the Applicability, the team believes protection of the Physical Access Control Systems and Electronic Access Control or Monitoring Systems Associated with High and Medium Impact BES Cyber Systems is a security enhancement that is appropriately included in these requirements.

•Requirement R3 Part 3.1: In response to comments that Part 3.1 may be onerous because training will be required for every new hire in the Applicability section, the SDT reviewed the requirement and believes the training must occur before authorized electronic or unescorted physical access is granted, except during CIP Exceptional Circumstances. In response to the comments that Applicability includes other associated Systems, but R4 does not have these in the Applicability, the SDT agrees there needs to be consistency between the Applicability section in R3 and R4, and has made those changes.

•In response to the comment that Table R3 doesn't contain any "applicable items," the SDT responds that the reference to applicable items in the Table is standard language to indicate that the Responsible Entity should implement the applicable requirements listed in the Table.

QUESTION 16 – CIP-004 R4:

CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*.**" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.**

SUMMARY:

Based on stakeholder comments, the SDT made clarifying changes to Requirement R4, Part 4.1 and Part 4.4 but made significant changes to Part 4.2 and Part 4.3 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for

improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

•After review of the comments, the SDT updated the requirements with a goal toward improved clarity, while trying to maintain a balance of reasonable security awareness and to moderate audit impact. The changes to Requirement R4 include the following:

•In response to comments to add the phrase, "to BES Cyber Systems," to clarify what this requirement applies to, the SDT added the language "to BES Cyber Systems, as suggested.

•Requirement R4 Part 4.2: In response to requested clarification to understand the phrase "six months or more," the team has modified the language in Requirement R4 Part 4.2 to clarify that "six months or more" applies to resided, employed, and attended school.

•In response to concern for consistency in CIP-004-05, Table R4, the team has edited the language in Requirement R4 to clarify the purpose of the risk assessment programs are to attain and retain authorized electronic or authorized unescorted physical access.

•Requirement R4 Parts 4.1 and 4.2: In response to comments asking whether either of these requirements is retroactive, the SDT states that the revised requirements for the criminal history check could necessitate a new assessment if the entity's previous program does not meet the new requirements.

•In response to several comments that it will be difficult to be 100% sure of a "full seven year criminal check," the team recognizes there may be challenges conducting a full seven-year criminal history check, and has included language in Part

4.2 to cover that possibility.

•In response to comments regarding online schools and how an entity determines location, after review of the comments, the SDT believes the expectation is that the student's physical location is considered when taking on-line classes.

•In response to several comments of being difficult to have "fails" defined for each role within the organization, the team agrees that all the criteria for determining what causes an individual to "fail" the PRA are difficult to document, and has modified the order of words in Part 4.3 to ensure Entities are clear that a assessment "process" is acceptable.

•In response to comments of difficulty in setting a hard line of when an employee "fails" a PRA is difficult, as it may be determined based on what role the individual is performing, after review of the comments, the SDT agrees that all the criteria for determining what causes an individual to "fail" the PRA are difficult to document, and has changed the order of the words in Requirement 4.3 to ensure entities are clear that a assessment "process" is acceptable. Information requested during an audit or investigation is covered under the NERC Rules of Procedure.

•Requirement R4.1: In response to comments regarding the word "initial" could indicate that this requirement must be done for existing individuals who already have access prior to V5 becoming enforceable, the team believes the word "initial" is needed to clarify that identity verification is only performed once, with the first PRA.

•Requirement R4 Part 4.2: In response to requests for clarification of the language, "resided and been employed," the SDT modified the language in Part 4.2 to clarify that "six months or more" applies to resided, employed, and attended school. The location of employment is where the individual actually worked, not necessarily the location of the corporate headquarters. The team recognizes there may be gaps if there are locations where an individual resided, been employed, or attended school for less than six months, but it does not preclude an entity from including those locations in its program.

•Requirement R4 Part 4.4: In response to requests for clarification as to why contractors must be separated out, rather than just having R4 be applicable to all individuals needing the access, the SDT reviewed Part 4.4, and the language is intended to verify that if an Entity is relying on the vendor's program, then the vendor's program must meet the specified criteria.

•Requirement R4 Part 4.4.: In response to comments to add "Parts 4.1 through 4.3" at the end of Part 4.4, that the measure should be consistent with the Requirement R5, Part 5.1 measure, which allows the use of attestations from vendors and contractors, the SDT has modified the requirement to include the reference to Requirement 4 Parts 4.1 through 4.3. The Responsible Entity may allow vendor attestations in accordance with its policies, practices, and

procedures.

•In response to comments that the Applicability stated in CIP-004-5, Table R4 - Personnel Risk Assessment Program, and CIP-004-5, Table R5 - Personnel Risk Assessment are inconsistent, the SDT agrees there needs to be consistency between the Applicability sections in R4 and R5, and has made the necessary changes.

•In response to comments to change "identify" to "identity," the SDT has changed Part 4.1 Rationale section to correct the typographical error.

•In response to comments that two defined terms be added to the glossary: Escorted Electronic Access and Unescorted Electronic Access, the SDT notes that the standards do not allow "escorted electronic access," and modifying the requirements to include the suggested language or adding the glossary terms. The SDT further clarified language relating to both electronic and physical access by stating "authorized electronic" and "authorized unescorted physical" to denote that all electronic access, whether "escorted" or not, must be authorized, and such authorization must meet the requirements of the standards.

•In response to comments that PRAs completed prior to V5 should be acceptable until the next time a PRA is required in the seven-year cycle, the SDT agrees and the Implementation Plan has been revised to allow the existing PRA to be "grandfathered" until it is time for its renewal. If the criminal history/background check for other compliance programs meets the new requirements in CIP-004-5, these would be acceptable.

•Requirement R4 Part 4.2: In response to comments that Requirement R4.2 lessens the requirements for international individuals, the SDT believes that it has not lessened the requirements for international individuals, but recognizes the need for vendor attestations, if an entity chooses to accept them.

•Requirement R4: In response to comments that the Measures require that the personnel risk assessment include a seven-year criminal history check, the requirement does not, the SDT has rewritten the requirement to clarify that a personnel risk assessment is needed to attain and retain authorized electronic or authorized unescorted physical access.

•In response to comments of FBI background checks qualifying as acceptable, the SDT believes FBI background checks would be acceptable if they meet the requirements of CIP-004-5.

•In response to comment to eliminate the requirement, the SDT thanks you for your comment, but believes the requirement is necessary.

•In response to comments to require why a seven-year background could not be performed will add additional costs, contributing little or no value to the personnel risk assessment program, the SDT believes documenting why a complete

seven-year criminal history check could not be performed demonstrates due diligence in meeting the requirement.

•In response to comments that there are no other FERC directives for the personnel risk assessment program requirement, the SDT believes the changes in CIP-004-5 increase the security posture of the entity over previous versions of the standard.

•In response to comments that the combination of requirements has the effect of discouraging entities from subjecting contractors to internal programs for entity employees because the burden of collecting, validating, and protecting information for non-employees is so overwhelming, the SDT believes Requirement 4.4 provides the flexibility to use the same process for contractors as employees.

•In response to comments that residency and educational history is not relevant to a criminal history, the SDT reviewed the requirement, Part 4.2 does not require an assessment of residency or educational history. It is intended to identify locations where the criminal history check should be performed.

•In response to a recommendation to modify this requirement to include the use of a National Criminal Research Database, which is believed to cover all of these requirements and show reasonable due diligence, the SDT disagrees with the assertion that the National Criminal Research Database covers all the requirements in CIP-004-5.

•In response to comments that the requirement only states criminal record checks and not other checks, such as random drug and alcohol testing, the SDT believes the addition of random drug and alcohol testing would be an expansion of the scope and is not under consideration at this time.

•In response to comments to leverage the Transportation Worker Identification Credential (TWIC) program, or to create a similar program specific to the electric sector, the SDT appreciates your comment, but it is not within our purview.

•In response to comments to align with the National Institute of Standards and Technology Interagency Report 7628 (NISTIR 7628) High-level requirements, the requirement should be elaborated, the SDT has reviewed the Personnel Screening requirements in NISTIR 7628, SG.PS-3, but believes Requirement 4 is appropriate.

•In response to comments of Table R4, Part 4.2 on Page 17, delete the phrase "regardless of duration," commenting that it does not add to the meaning since there is a six-month exception for certain addresses, the SDT believes the term “regardless of duration” means that the location of current residence must be included in the criminal history check, even if the individual has lived there less than six months. The concern with using the term “county of residence” is that it may not be applicable throughout the US and Canada.

•In response to comments that dormant accounts with privileges could be misused, the SDT believes revocation of access requirements in Requirement R7 provide for removal of such privileges.

QUESTION 17 – CIP-004 R5:

CIP-004-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in *CIP-004-5 Table R5 – Personnel Risk Assessment."* **The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.**

SUMMARY:

Based on stakeholder comments, the SDT made clarifying changes to Requirement R5 and Part 5.1 and significant changes to Part 5.2 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

• Requirement R5 – Added "to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems" for added clarity per comments received.

• Part 5.1 –Updated language per comment received to "Have a personnel risk assessment performed as specified in CIP-004-5, Requirement R4 prior to being granted authorized electronic or authorized unescorted…".

• Part 5.2 – The language has been modified to clarify that the current personnel risk assessment should be no older than seven years.

• Low Impact BES Cyber Assets have been moved into CIP-003-5 to emphasize the programmatic nature of the controls.

• Applicability has been revised to High Impact and Medium Impact BES Cyber Assets as in Requirement R4.

• Personnel risk assessments are addressed in two requirements with the requirement to have a "program" in Requirement R4 and "implementation" of that program in Requirement R5.

• The SDT believes that Requirement R5 is necessary because it required completion of the personnel risk assessment in Requirement R4 before access is granted.

• In regards to providing evidence of the personnel risk assessments during an audit, the SDT reminds commenters that information requested during an audit or investigation is covered under the NERC Rules of Procedures.

• The SDT disagrees with the assertion that the National Criminal Research Database covers all the requirements in CIP-004-5.

• The Implementation Plan has been revised to allow existing personnel risk assessments to be grandfathered until renewal time.

• The SDT recognizes the need to rely on information provided by the individual in identifying residence locations. The SDT has created requirements for a records check, not requirements that an individuals' fraud on one of those checks would necessitate a self-report, and the SDT respectfully disagrees that an individual's fraud would constitute noncompliance with the requirement so long as the responsible entity conducted the records check as required.

QUESTION 18 – CIP-004 R6:

CIP-004-5 R6 states "Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in *CIP-004-5 Table R6 – Access Management Program."* **The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R6 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.**

SUMMARY:

Based on stakeholder comments, the SDT made no changes to Requirement R6 but made significant changes to each of its Parts (Parts 6.1 through 6.6) and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, “initially upon the effective date”
- Requirements – Use of the phrase, “where technically feasible”
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The majority of comments on for CIP-004-5 R6 centered on the authorization language in requirement parts 6.1 through 6.3. In particular, commenters expressed disapproval of the CIP Senior Manager or delegate(s) authorizing access and the difficulty in auditing “the minimum necessary for performing assigned work functions.”

Regarding the inclusion of “CIP Senior Manager or delegate(s)”, we are reverting to previous language found in CIP-003-4 where the Responsible Entity maintains a list of authorizers. To avoid cross-referencing among Standards, which allows for independent revisions to Standards on a going-forward basis, the SDT combined parts from CIP-003-4, CIP-004-4 and CIP-007-4 in this requirement. CIP-004-4 R4 requires entities to maintain a list of personnel with authorized access. CIP-007-4 R5 Part 5.1.1 requires entities to ensure user accounts are implemented by approved designated personnel with a reference to CIP-003-4 R5. It’s in CIP-003-4 R5, nested through 2 references, where entities are required to designate authorizers by name and annually review the list of authorizers in CIP-003-4 R5 (nested through 2 references).

To address comments on the audit ability of “the minimum necessary” language in what was included in Parts 6.1, 6.2, 6.3, 6.5, and 6.6, (now 6.2, 6.3, 6.4, 6.6 and 6.7 in the revised draft of the standard) the SDT substituted the following language: “those that the Responsible Entity determines are necessary for performing assigned work functions.” This replaces what previous approved versions of CIP Cyber Security Standards had as “need to know” and makes clear that is the Responsible Entity who makes the determination of what is considered necessary. The compliance evidence necessary to demonstrate this would be showing that consideration was given to the required work functions as part of the provisioning process. When role-based access is configured, the necessary evidence would be documenting the type of access each role has and determining the level of access an individual needs to perform their assigned work functions. Demonstrating compliance can be much easier for simple access control systems such as generation control systems and relay where only one level of access exists. If access is only used occasionally or in emergencies, then it would still be considered necessary for the assigned work function.

Several commenters also expressed the view that the quarterly review (Part 6.5 in the revised standard) should be

extended to be performed annually. In response, the quarterly verification process comes from the previously approved CIP-004-3. The purpose of having a quarterly review is not for assuming the process is broken, but rather, for preventing unauthorized access as quickly as possible. In order to implement an effective access management program, this control is necessary to ensure the unauthorized access is revoked in a timely manner. There were also a few commenters who expressed the opinion that the review language significantly increases the scope of work for a quarterly review. In response, the changes made to this draft are in response to past industry comments and general feedback that the following phrase, "review the list of its personnel who have such access…" is not well understood or consistently implemented.

In addition, several comments expressed concern over the use of the words "calendar quarter." To clarify, performing the obligations in 6.4 (Part 6.5 in the revised standard) at the beginning of one calendar quarter and the end of the subsequent calendar quarter is an acceptable method for satisfying this requirement. The use of "calendar quarter" in this case will be easier for entities to maintain compliance deadlines.

Other modifications include specifying the authorization of access for BES Cyber System Information was limited to repositories instead of the BES Cyber System Information itself, which can be very extensive. The measures have also been modified to remove references to evidence sampling.

QUESTION 19 – CIP-004 R7:

CIP-004-5 R7 states "Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in *CIP-004-5 Table R7 – Access Revocation*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R7 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made no changes to Requirement R7 but made significant changes to Parts 7.1 though 7.5 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

There were a number of comments submitted on CIP-004-5, Requirement R7 that express concerns of the majority of respondents. These are:

1. Removal of access "at the time of resignation or termination."
2. Various comments on the use of "next calendar day" for an access removal timeframe.
3. The requirements around reassignments or transfers.
4. Removal of access to BES Cyber System information.
5. The use of the term "extenuating circumstances" as it applies to compliance with Part 7.5 (changing passwords).

6. The inclusion of medium impact assets for removing shared accounts and changing passwords following a termination action.
7. Retroactive terminations or resignations
8. Application Guideline – No action required to revoke access in the case of a death of an employee.

We believe that the responses to these comments strike a well-orchestrated balance between industry concerns and addressing FERC Order No. 706 directives. The Standards Drafting Team provides the following summary responses:

1. Removal of access "at the time of resignation or termination"

First, the term "termination actions" was added to respond to numerous industry comments. The drafting team decided to consolidate both terminations and resignations since both of those actions are required to be addressed by FERC Order No. 706 to be completed "immediately." Immediately is definitively clear but realistically and from an audit perspective, subject to interpretation. Accordingly, the drafting team adjusted the requirement (see Part 7.1 in the revised standard) to read "initiate the process to revoke" unescorted physical and electronic access to BES Cyber Systems "upon the effective date and time of the termination and complete the revocation within 24 hours after the effective date of the termination action." Because various entities have diverse processes in place for initiating termination actions, the revised requirement considers those differences and establishes a 24-hour metric for audits based on the established date and time of the process start time.

2. "Next calendar day" for access removal time frame

The use of "next calendar day" is consistent throughout the Version 5 standards. While the drafting team is sensitive to the difficulties inherent to revoking access outside of normal working hours, the time lags, particularly in the case of terminations, could expose the entity to malicious activity. The time frame remains in effect for all termination actions.

3. Reassignments and Transfers

To address reassignments and transfers, the drafting team revised the requirement to specify that one must "revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the reassignment or transfer. The requirement allows retention of access that the entity considers necessary as long as a review of all accesses is completed by the next calendar day following the transfer or reassignment and that any unnecessary accesses are removed at that time.

4. Removal of access to BES Cyber System Information. (Part 7.3 in the revised standard)

There were many comments highlighting the difficulties associated with ensuring that all access to BES Cyber System Information was removed. Some entities suggested the use of the term "repositories" to identify those areas where such information is stored. The drafting team chose not to integrate the term "repositories" because in an audit situation, use of a repository could become an incidental piece of evidence. Because BES Cyber System Information may be housed in numerous locations throughout an organization, the drafting team chose to revise the requirement to revoke an individual's "access to the physical and electronic locations" to locations where the Responsible Entity stores BES Cyber System information. This alleviates the issue of trying to track each individual hard copy of such information. It also prompts entities to try to consolidate BES Cyber System Information and limit its storage to as few locations as possible.

5. Use of the term "extenuating circumstances" as it applies to changing passwords in the event of a termination action. (Part 7.5)

"Extenuating circumstances" has been removed from the requirement. The requirement now states that a responsible entity may determine and document that "operating circumstances" require a longer time period to effect necessary password changes. Once the operating circumstances end, passwords must be changed within ten days.

6. The inclusion of medium impact assets for removing shared accounts and changing passwords following a termination action.

In both Parts 7.4 and 7.5, medium impact assets were inadvertently included in the applicability section. The medium impact assets have been removed from the revocation of individual user account and shared password requirements.

7. "Retroactive" terminations or resignations.

A number of respondents cited retroactive terminations or resignations as complicating the access removal process and time frame requirements. The drafting team attempted to clarify that though there may be retroactive resignations, retroactive terminations are an unfamiliar concept. The drafting team believes that an individual cannot effectively be terminated on a prior date and continue working. If a business unit "intends" to terminate an individual at some future date, the termination is not effective until the actual action is taken. By the same reasoning, an individual can decide to resign effective on some future date. The resignation is not effective until the actual projected date. In the case of

retroactive resignations, an individual may "resign" by leaving a voicemail on a manager's phone over the weekend. Realistically, the resignation cannot be processed until the manager is aware of the employee's action. Once there is awareness, the process initiation and 24-hour requirement begins.

8. Revocation of access in the event of an employee's death

There have been a number of comments discussing the Application Guideline not listing revocation requirements in the event of an employee's death. The drafting team agrees that there is a security risk if no action is taken. We have adjusted the Application Guideline to reflect expeditious removal of access.

QUESTION 20 – CIP-004 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-004-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to all the VSLs except for the VSLs for R4 which had only a minor change.

Please see the redlined version of the standard for the complete set of revisions.

One commenter suggested the VRF for revoking access should be medium. In response, we note that the currently approved VRF for access revocation is lower and we have no compelling justification for modification at this time.

For R1, several commenters suggested a more granular break out for missing a single quarter. One entity suggested that failure to document the program be a lower VSL than failing to implement the program. Several commenters noted the Severe VSL failure to document or implement the program negated the High VSL failure to perform on a quarterly basis. In response and regarding the granular break-out, a single violation of this requirement would be on a per quarter basis. So, instead, we provided more levels of severity according to the time of an entity performance beyond missing a calendar quarter. Regarding the documentation and implementation of the program in the Severe VSL, we modified this to include documentation only.

For R2, several commenters suggested a more granular break out than what was proposed. In response, we provided additional granularity based on the amount of training content an entity failed to document.

For R3, several commenters suggested a more granular break out on percentages of missed training. One entity commented that this requirement should be written as a find, fix, repeat process, and the VSL should be based on the

amount of time to fix the error. Another entity indicated the Severe VSL negated the High VSL. In response, we have provided additional granularity based on the number of individuals missing training in a calendar year. Regarding the find, fix, repeat process, if the VSLs were gradated on the amount of time to fix the error, that would indicate that the requirement allows individuals to access without training as long as the entity caught the error in a specified amount of time. Such a requirement would not achieve the reliability objective to provide ongoing training. In essence, an entity would never violate the requirement so long as the violation was caught within an acceptable period of time. Regarding the Severe VSL, we have modified this to make clear that it applies when the Responsible Entity does not implement the training program at all.

For R4, one entity noted the High VSL refers to "required documented results" and to Part 4.5. The documented results are a requirement of R5 and there is no Part 4.5. Another entitysuggested a lower VSL for lack of documentation. In response, we have removed references to "required documented results." Regarding a lower VSL for lack of documentation, the FERC makes clear in its March 18, 2010, Order on CIP VSLs that a VSL cannot be lower for failure to document because documentation indicates and provides evidence of a consistent practice.

For R5, one entity suggested breaking out the VSL so that one individual not having a complete update every seven years is a moderate, and two or more becomes a high VSL. Other commenters suggested simplifying the language in the High VSL to "Personnel risk assessments are not updated at least once every seven years." They also suggested the failure to document should not be a Severe VSL. In response, we have gradated much of the VSL based on the number of individuals not having a PRA and have simplified the language similar to what was suggested.

For R6, one entity noted the Severe VSL refers to a nonexistent Part 6.7. Another entity commented that administrative errors found during quarterly and annual assessments should not be considered a violation. Another entity suggested breaking out the quarterly and annual assessment VSLs based on percentages. Another entity commented that for VSLs gradating on counts, there should be a timeframe identified. Another entity suggested making separate VSLs for requirement parts instead of having long or clauses. In response, we note that administrative errors not leading to unauthorized access are not violations of the Standard. We have also gradated the VSLs, both on the number of individuals not having authorization and on the time beyond performing required assessments. We have also identified timeframes for the aforementioned counts.

For R7, several commenters suggested VSLs be broken out by percentages. Some commenters suggested breaking out the violations by specific numbers of individuals who did not have their access revoked. In response, we have provided further gradation on the number of individuals. We chose not to use percentages because it becomes less meaningful with a smaller sample size and the risk for a large company for one failed access revocation is the same as for a smaller

company.

QUESTION 21 – CIP-005 R1:

CIP-005-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made no changes to R! but did make significant changes to Parts 1.1 through 1.5 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

There were numerous comments concerning the Requirement R1 Part 1.1 requirement on Low Impact systems. The SDT has moved all requirements concerning Low Impact systems from the entire suite of CIP standards to CIP-003 and rewrote the Requirement R1 Part 1.1 at a higher level. The SDT has also re-invoked the ESP definition from previous versions in order to use it to handle the 'high watermark' comments and clarify what entities are to do when systems of mixed impact classifications are within one ESP. The applicability of R1 has been clarified and changed in order to match previous versions and not create recursion in the requirement (ESPs around ESP devices). The SDT has clarified in the responses that the malicious communications requirement has been intentionally written at a level that does not require

specific technologies (such as IDS, although IDS is used as an example in the measures). The SDT also clarifies that the requirements that were noted as deleted (R1.1-R1.3) were from previous versions as they were definitional in nature. New requirements with those numbers have been added. The SDT also clarified that outbound permissions on Electronic Access Points (EAPs) are now required as a first level of defense against compromised systems in the ESP. Guidance has been added to the standard with further explanation.

The term "non-interactive" in the applicability column of Requirement R1.4 was removed. Commenters found this term confusing. "Non-interactive" was originally included to distinguish it from the Interactive Remote Access covered in Requirement R2. The term "explicit" in Requirement R1.3 was removed because of commenter suggestions that the term is superfluous. In Requirement R1.5, many commenters expressed confusion around detecting malicious communication "at each EAP". The SDT recognizes the confusion and potential for multiple interpretations, and in response, it has made the requirement less specific to focus on the objective of detecting malicious communications. One commenter suggested that R1.5 was overly prescriptive and should be written to allow entities to choose how to address Order No. 706, paragraphs 486-503. In response, the SDT believes that would cause numerous comments from industry as to its audit ability. To address the full intent of the Order's language, nearly 6 paragraphs would need to be included to clarify what is and is not acceptable. The SDT has chosen instead to narrow the requirement to something that does meet FERC's intention, while wording it in such a way that it remains quite flexible and not tied to a particular technology such as IDS. IDS is only mentioned in the Measures as an example of evidence.

QUESTION 22 – CIP-005 R2:

CIP-005-5 R2 states "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in *CIP-005-5 Table R2 – Remote Access Management*.**" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.**

SUMMARY:

Based on stakeholder comments, the SDT made a clarifying change to Requirement R2 and made significant changes to Parts 2.1 through 2.3 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, “initially upon the effective date”
- Requirements – Use of the phrase, “where technically feasible”
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The majority of comments for CIP-005-5, Requirement R2 were aligned to a few areas. The three most commented on issues for CIP-005-5 R2 were: (1) the starting and the ending point for encryption, (2) clarification of multi-factor authentication, and (3) the prescriptive nature of the requirements for Intermediate Device.

The majority of comments regarding CIP-005-5, Requirement R2 requested clarification on the initiating and the terminating point for required encryption. In response to comments, Part 2.2 has been modified to state that encryption must terminate at the Intermediate Device. Encryption initiates at the Cyber Asset performing Interactive Remote Access.

The second most noted comment was requesting clarification on where multi-factor authentication is required. To address the comments submitted, the definition of Intermediate Device has been updated to require that access control is performed by the Intermediate Device. This would include multi-factor authentication.

Many commenters also raised concerns with the note regarding UserID not being an authentication factor included in Measure 2.3. The note in the Measure regarding User ID has been removed in response to those concerns. Clarification of multi-factor authentication has been added to Requirement Part 2.3, and further information regarding multi-factor authentication is included in Guidance for Secure Interactive Remote Access published by NERC in July 2011.

Regarding the third area of comments, the SDT considers Requirement R2 Part 2.1 to be broad in implementation, and the requirement allows for appropriate flexibility in the design of remote access architecture. Intermediate Device is not defined to be technology specific. The requirement has been drafted to allow a Responsible Entity to define the infrastructure that meets the needs and capabilities of its organization, while also specifying a set of parameters. Varying examples of remote access system design are included in Guidance for Secure Interactive Remote Access published by NERC in July 2011.

Additionally, many commenters noted concerns regarding the need for Technical Feasibility Exceptions. To address these

comments, the SDT notes that all parts of Requirement R2 are eligible for a Technical Feasibility Exception.

Commenters requested segregation of dialup from network based remote access. Dial-up is addressed in other requirements. However, the securing of remote access using dial-up is only addressed in this requirement. As such, the content is relevant to this requirement and the SDT did not segregate this requirement.

QUESTION 23 – CIP-005 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-005-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the VSLs for R1 and R2 but did not change the VRFs.

Please see the redlined version of the standard for the complete set of revisions.

Commenters recommended segregating the VSLs by the percentage of number of failures to protect the Interactive Remote Access sessions. Due to the protective measures generally being enterprise-level solutions, this sort of gradation of the violation severity is not appropriate and would be onerous in retaining evidence of compliance.

Comments were submitted requesting VSLs identified by the criticality of the asset. The applicability of the requirement addresses the impact of the asset. The requirements are written to address the protection of the assets already identified. The VSLs have been modified to address the implementation of the appropriate protective measures.

Comments were made to propose estimation of the monetary penalties associated with a potential violation of the requirements. This information is available in Appendix 4B of the NERC Rules of Procedure.

Overall, the primary issue for the comments related to the CIP-005-5 R2 Violation Severity Levels (VSLs) were that all violations would be deemed as severe rather than the VSLs being graduated based on risk. In response to the comments, the VSLs have been modified to address not implementing the required procedural or technical controls.

QUESTION 24 – CIP-006 R1:

CIP-006-5 R1 states "Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R1 and all of its Parts 1.1 through 1.6 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The entire contents of CIP-006-5 are intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

In addition to several comments that assisted the drafting team in making positive revisions to correct for consistency, eliminate ambiguity, or provide clarity, the SDT considered several constructive comments and made substantive changes to CIP-006-5.

Other modifications were added to address FERC Order No. 706, Paragraphs 572 and 575, which were directives for physical security (defense in depth), and to address industry comments. These modifications include, but are not

limited to, the following general concepts:

- The language of R1 has been modified to clarify the scope as applicable to BES Cyber Assets, BES Cyber Systems, Electronic Control Monitoring systems and Physical Access Controls Systems.
- The phrase “real- time alerts” has been removed, and the requirement expanded to clarify the intent.
- The measures have been modified to agree with the requirements to track access (i.e., ingress only).
- The phrase “access point” has been removed, and the language has been clarified to reflect the SDT’s intent.
- Information on access openings has been provided in the Guidelines and Technical Basis section of the standard.
- The requirement around physically protecting Physical Access Control Systems is limited to restricting access using operational or procedural controls, and the language has been clarified to reflect this intent.
- “Where technically feasible” language has been added in cases where it may not be possible to implement two or more different physical access controls due to physical restrictions, with an expectation that this language will not be abused to deviate from the intent of this standard. The language has been modified to clarify the intent that two different physical access control mechanisms are required, not two completely independent physical access control systems
- The requirements in this standard have been reworded such that an entity must utilize one (or more) physical access control(s) to allow physical access into a PSP to only those individuals that are authorized. There is no explicit requirement for a completely enclosed ("six-wall") border.
- The SDT attempted to stay away from detailed “how” questions posed in an attempt to all different implementation methods that obtained the same minimal risk level.
- Recommendations on the management of CANs were viewed as outside the scope of the SDT.

More specifically, commenters raised several issues, which are discussed in greater detail in the paragraphs that follow.

As described in the summary response to “Defined Physical Boundary,” the SDT has changed this term back to “Physical Security Perimeter” in response to comments. Note, however, that the definition of the term, “Physical Security Perimeter” has changed significantly from the currently-used definition.

Commenters requested greater clarity with respect to the phrase “Issue real-time alerts” in Requirement R1, parts R1.4 and R1.5, and the drafting team agrees and has modified the requirement to remove “Issue real-time alerts.” Instead, the requirement language requires issuing “an alarm or alert in response to detected unauthorized . . . to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes . . .” (These parts are R1.5 and R1.7 in draft

2). That also ties in better with the requirements on incident response, which addresses commenters concern that there are requirements to alert, but not to respond. The requirement to detect unauthorized circumvention and alerting has also been separated into two requirements, with additional clarification provided in the new wording.

Commenters noted concern with R1.4's (now R1.5) used of "access point" and the phrase has been removed to clarify the SDT's intent. The requirement now references "unauthorized circumvention of a physical access control into a Physical Security Perimeter".

Commenters also suggested that "sufficient" in R1.6 was subjective. The use of "sufficient information to uniquely individual" is intended to provide flexibility to the entities. It is expected that the responsible entity's plan will define what set of information is adequate by demonstrating the ability to uniquely identify individuals from the logged records.

Commenters also suggested that Parts R1.2 and R1.3's measures implied a requirement to track egress. The measures have been modified so that they better align with the requirement to track access (i.e., ingress only).

In response to concerns that Part R1.3's TFE language may lead to increased TFEs, the SDT notes that in some cases it may not be possible to implement two or more different physical access controls due to physical restrictions and equipment locations. Because of this, the language "Where technically feasible" has been included. As is the case with any technical feasibility language within the standard, meeting the requirement language is the goal.

In response to concern that CIP-006 raises a conflict with the BES Exception criteria, for certain generation facilities, particularly those under 75 MVA, the SDT addressed the concern in Section 4 (Applicability) of the standard itself. Section 4 clearly stipulates under Facilities 4.2.3: "Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities." (Underline added). Only those Facilities that are deemed to be BES Facilities are in scope for the standard. If these Generation facilities are excepted from the BES definition, then they are also excepted from the applicability of these CIP Cyber Security standards.

Commenters recommended including the wording from CAN-0031, "That any opening that does not have physical preventative measures in place is less than 96 square inches. That any opening greater than 96 square inches, with its shortest side greater than 6 inches in length, is protected against entry by the use of bars, wire mesh or other permanently installed barrier that leaves no opening greater than 6 inches on its shortest side." In response, the SDT notes that Information on openings has been provided in the guidance. Importantly, the requirement is to restrict entry into a Physical Security Perimeter. The revised standard does not identify any specific size requirements and does not reference the term "access point". The SDT expects that if such an opening exists and cannot be eliminated, then it will have to be considered an "access point in a Defined Physical Boundary" with the appropriate controls applied. In Version 5's CIP-006 proposal, there is no requirement to ensure a completely enclosed ("six-wall") border. The requirements

have been reworded such that an entity must utilize one (or more) physical access control(s) to allow physical access into a PSP to only those individuals that are authorized.

This provides entities the option to implement alternatives to restrict access that may be more practicable or economical than a completely enclosed border without requiring the submission of a TFE. As noted, the guidance document states that in many instances a completely enclosed border this will remain a primary control for controlling access. In terms of controlling access, the CAN's information on the size of an opening that constitutes an access point would still apply insofar as a larger opening would need controls in place to allow access to only those individuals authorized, and a smaller opening (that an individual cannot pass though) would not require those additional controls.

Some commenters suggested that the CAN should be required, but the issue of retiring CANs is outside the scope of the drafting team. However, with the greater specificity of the requirements surrounding this issue in Version 5, the SDT understands that contrary language and instruction through requirement language may result in the withdrawal of the CAN.

In response to concerns surrounding the testing requirements of every two years (and a preference for every three years), the SDT notes that the modification to every 2 years is in direct response to FERC Order No. 706, paragraph 581's directive to test more frequently than every three years. Furthermore, if the active monitoring can be demonstrated to meet the requirements of the semi-annual testing (including validation of correct operation for all locally mounted hardware or devices at the Defined Physical Boundary) then this would most likely meet the two year testing requirement.

In response to commenters' suggestion that associated Physical Access Control Systems be added to applicability of R1.2 and R1.3, there is no explicit requirement to have Physical Access Control Systems protected by a Physical Access Control System (PACS). This is consistent with CIP-006 versions 1-4. The requirement around physically protecting PACSs is limited to restricting access using operational or procedural controls, and the language has been clarified to convey this intent.

Commenters questioned what was meant by two or more "different and complementary" controls under Requirement R1.3. This comes from a directive in FERC Order No. 706, Paragraph 572, but the SDT has made significant clarification to the language (and removing "complementary," while supporting the concept). The SDT addressed this in CIP-006-5, Requirement R1 (Part 1.3) for High Impact BES Cyber Assets, by requiring Responsible Entities to "utilize two or more different physical access controls to collectively allow physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access." This clarifies the intent that two different physical access controls are required, not two completely independent physical access control systems.

In response to questions surrounding the meaning of "associated with" in the applicability tables, it means "associated with" the High, Medium, or Low classification BES Cyber Systems (with or without additional conditionals) identified in that applicability section. The SDT has made significant revisions to the background and "applicability columns in tables" section of the standards to better explain this concept.

In response to suggestions to clarify the entry and exit logging requirements in R2.2, the SDT added clarifying language allowing for logging "first entry" and "last exit" from the Physical Security Perimeter.

In response to comments that suggested very specific artifacts for compliance, the SDT's intent is to identify "what" is necessary for protection without adding the specificity on "how" to achieve that performance.

Commenters suggested that for R1 overall, the SDT needs to include language that allows for deviations from the controls during CIP Exceptional Circumstances because there may be circumstances that require providing physical access control to individuals not on the authorized list, but this is not appropriate in CIP-006; the SDT notes that the CIP Exceptional Circumstances are addressed under CIP-004 – Authorization.

For logging access under R1.6 (now R1.8), some commenters questioned whether it included just the date, or also the time. The SDT has clarified the language by specifying that it includes both the date "and time."

Commenters asked whether cabling must be protected between Defined Physical Boundaries (now Physical Security Perimeters), and the SDT notes that the requirements apply to Cyber Systems and Cyber Assets. With the changes to glossary term, "Cyber Asset," along with the determination in Project 2008-10's interpretation of CIP-006 (approved by NERC BOT, but not yet approved by FERC) that "wire" is not a Cyber Asset, the requirements in CIP-006 do not apply to wiring or cabling.

Some commenters questioned what was meant by "locally mounted hardware devices." The SDT has clarified the language in the background and applicability explanations, which clarifies that "locally mounted hardware devices" is intended to refer to "dumb" devices that do not perform any authentication functions independently.

In response to suggestions to allow for CIP Exceptional Circumstances to except one from logging, the SDT did not see a reliability related reason to suspend logging just because of a CIP Exceptional Circumstance.

QUESTION 25 – CIP-006 R2:

CIP-006-5 R2 states "Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program.*" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made minor changes to Requirement R2 and significant changes to Parts 2.1 and 2.2 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

(1) Part 2.1 and Part 2.2 - Applicability – revised Medium Impact to include only routable or dial-up access in order to limit the need for visitor controls.

(2) Part 2.2 – Changed "…of the entry and exit…" to "…of the initial entry and last exit…" for clarification.

(3) Part 2.2 – Changed "… individual point of contact." to "…name of an individual point of contact responsible for the visitor." in order to clarify "point of contact" and that it may be a different person than the escort.

Several commenters requested clarification as to whether physical access logs are required for physical access to Physical Access Control Systems. The SDT confirms that physical access logs for authorized users and visitors are **not required** for

physical access to Physical Access Control Systems.

Several commenters recommended the removal of "continuous" from "Require continuous escorted access…..". The SDT believes "continuous" should remain and notes that "continuous" is in version 3 and 4 requirement wording.

Additional requirements were proposed that the SDT believes go beyond what should be required as minimum level of visitor controls needed.

Measure for Part 2.2 – Comments were received to remove "and" from this measure. The SDT does not agree with removing "and" since the measure also states "not limited to" and for the examples provided both items would be needed to demonstrate compliance. The responsible entity must have the required language in its visitor control program AND must have evidence that it has implemented this program.

• •The SDT agreed with other comments and added the ability to deviate from Requirement R2, Part 2.1 and Part 2.1 during CIP Exceptional Circumstances, and added a new Part 2.3 to clarify that visitor logs only need to be retained for 90 calendar days. The SDT also updated change descriptions to reflect current requirement wording.

QUESTION 26 – CIP-006 R3:

CIP-006-5 R3 states "Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in *CIP-006-5 Table R3 – Maintenance and Testing Program*.**" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.**

SUMMARY:

Based on stakeholder comments, the SDT made minor changes to Requirement R3 and significant changes to Parts 3.1 and 3.2 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"

- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

(1) Part 3.1 – Removed "prior to commissioning" per commenters suggestion.

(2) Part 3.1 – Changed "…to ensure the required functionality is being provided." to "… to ensure they function properly."

(3) Parts 3.1, 3.2,– Applicability – specified High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable in order to clarify which "locally mounted hardware or devices" are applicable.

(4) Part 3.2 – Expanded on Part 3.2 to require retention of outage records for 12 months.

(5) Applicability – Changed from "Associated Physica Access Control Systems" to "Physical Access Control Systems associated with" to standardize across the CIP standards.

Part 3.1 - Comments were split where maintenance and testing was concerned. Some commenters felt that maintenance and testing should be done more often while others wanted to revert to the current three years. Based on SDT discussions and the FERC directive in Order No. 706, paragraph 581, the SDT continues to believe that 24 months is appropriate.

Some commenters indicated that tracking of outages should only include Physical Access Control Systems. The SDT believes that tracking of outages should include more than just outages to the Physical Access Control Systems because other outages may be relevant for forensics purposes.

QUESTION 27 – CIP-006 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-006-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the VSLs for all three of the requirements in this standard but did not make any changes to the VRFs.

The drafting team appreciates the numerous comments pointing out the incorrect references to items in the requirements shown in the Table of Compliance Elements. These references have been corrected. These reference

corrections also addressed several comments on the High VSL for R1 stating the standard did not mention a 15 minute requirement. The correct reference is to Part 1.5, which does include this time requirement.

On the comments to reduce the VRF for R2 to Lower, the drafting team points out that the current VRF level for visitor control is Medium and believes this is the right level based on the definition of a Lower and a Medium VRF. A lower VRF is associated with a requirement that is administrative and, if violated, would never lead to cascading, uncontrolled separation, or instability. Requirement R2 includes "implementation" of the visitor control program, thus this requirement is not administrative and doesn't qualify for the "Lower" VRF.

Similarly, the use of the term "continuous" is in the current version of the standard and is intended to mean the escort should always be in close proximity to the visitor and aware of the visitor's actions.

The drafting team corrected the confusion over the term "each" in the Moderate VSL for R2 as pointed out by one commenter by specifying that it applies to the initial entry and final exit, not each entry and each exit.

As to the comments that there should be a Lower VSL for processes that are implemented but not documented, the drafting team does not agree. It is not clear how an entity consistently implements processes that are not documented. There was one comment that failure to adequately document information to uniquely identify an individual is more severe than failure to implement two or more controls to restrict access for High Impact BES Cyber Systems. If the individual is unknown and accessing an unknown area as described in the comments, this would be a potential Cyber Security Incident and handled as such. The Lower VSL is intended to capture an instance where an authorized individual appropriately accesses a Physical Security Perimeter, but for some reason, uniquely identifying information is not captured.

Finally, the drafting team believes the differentiation between High and Medium Impact BES Cyber Systems is done with the controls, if necessary, so it does not warrant separate entries in the Table of Compliance Elements.

QUESTION 28 – CIP-007 R1:

CIP-007-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT did not make any significant changes to Requirement R1 but did make significant changes to Parts 1.1 and 1.2 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

In response to numerous comments the SDT has rewritten Requirement R1, Part 1.1 to:

(1) specify the requirement applies to applicable Cyber Assets

(2) to provide the ability to specify port ranges, as well as service names for those with truly dynamic port ranges, and

(3) enabling of only necessary ports – revised Part 1.1 now reads: "For applicable Cyber Assets and where technically feasible, enable only logical network accessible ports needed, including port ranges or services where needed to handle dynamic ports."

The SDT notes that those ports and services that are allowed to cross an ESP are explicitly documented at that level in CIP-005. The SDT has left the term 'ports and services' in recognition that ports are actually just the listening 'channel' for a service, and we've added that services can be designated as needed to handle such things as remote procedure call (RPC) which use random, dynamic ports.

Numerous commenters noted the amount of work involved in creating screenshots. Based on these comments, the SDT removed "screenshots" as an example in measure 1.1.

Based on comments received concerning the clarity of the phrase, "Disable or restrict the use of . . ." in Requirement R1,

Part 1.2, the SDT has changed Part 1.2 to read "Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media." and has removed screen shots or pictures from the example measures. This requirement is in response to FERC's interpretation order that required the ERO to address the issue.

A commenter proposed a more graded approach to the level of security required in the standards. The SDT believes it does have a graded approach to the standards where higher impact systems have stricter requirements. The current requirements in V3-V4 of the CIP standards are carried forward as practical to the same types of cyber assets in V5 (medium impact), with a few more stringent requirements being applied to the high impact systems, especially where needed to meet the outstanding directives from Order 706.

A minority view held the guidelines provided additional requirements. The SDT notes that guidelines are not enforceable and are not requirements. Only the actual requirements are mandatory and enforceable. The SDT's intent in providing guidelines is to provide examples of how something could be met, and it is not intended to enhance the requirement language itself in any way.

QUESTION 29 – CIP-007 R2:

CIP-007-5 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT did not make any significant changes to Requirement R2 but did make significant changes to the Parts 2.1 through 2.4 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"

- Requirements – Use of the phrase, “where technically feasible”
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Several commenters stated that the last sentence on sorting (“The list could be sorted by BES Cyber System or source.”) in Measure 2.1 was not needed. The SDT agrees and has deleted the last sentence of the measure.

Commenters raised issues with the language that suggested that ‘updates’ (old Part 2.2, now Part 2.3 in the updated standard) might be interpreted to include all updates, not just security-related updates. The SDT agrees and has incorporated the existing language from Version 4 to clarify that only security related updates are in scope.

Commenters raised issues with using the term ‘remediation plan’ (old Part 2.2, now Part 2.3 in the updated standard) and many suggested changing to ‘mitigation plan’. The SDT agrees; however, the term ‘mitigation plan’ has numerous meanings as it pertains to NERC standards, compliance, and enforcement and could cause further confusion. The SDT has changed the language to call for a ‘plan’. Further, many commenters questioned whether the plan is specific to the patch or the overall process. The SDT clarifies that a plan is needed per patch. The plan is simply the way the entity chooses to mitigate the vulnerability exposed by the security patch, either by installing the patch or taking other measures. The plan can consist of a simple notation that the patch will be applied in the Responsible Entity’s normal patch management process.

Numerous comments were made as to the clarity and order of the requirement Parts in the table, in particular Parts 2.2 and 2.3. There were also comments stating that the measures did not match the requirements. The SDT agrees and has reworked the requirements in the table to more closely model Version 4’s language, and the SDT made revisions to the requirements and measures in the standard for additional clarity.

There were a few commenters who called for patching requirements on low impact systems. The SDT believes that although low impact systems should be patched, the compliance burden of tracking every patch for every low impact asset is an onerous burden and thus has not required it in this mandatory, enforceable, and auditable standard.

Several comments concerned devices that can not be patched or for which no patch sources are available. The SDT has modified the requirement to better account for that possibility and to handle devices that are not updateable or have no patching source. Part 2.1 in the revised standard includes the following language: “…shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets

that are updateable and for which a patching source exists."

Many comments concerned the fact that no maximum timeframe for patching is required. The SDT is allowing flexibility in the patching implementation timeframe. The desired behavior from this requirement is that entities are tracking and are aware of vulnerabilities in their systems that patches expose and create a plan to mitigate those vulnerabilities. The SDT is not mandating the installation of all patches, but rather focusing on the entity's response to the vulnerability. The SDT has taken into consideration that control system patching itself is a risk to reliability and that there are entire seasons in our business where the risk of making changes to control systems that could affect availability outweighs the risk of compromise. The SDT believes that if entities are required to be aware of vulnerabilities in their systems, they can then make informed risk decisions that are in the best interest of overall reliability.

Some commenters requested clarification regarding who is responsible for identifying the sources of the patches and what level of patching requirements were required. The SDT clarifies that the Responsible Entity identifies the sources as part of its overall patch management process and it is up to the Responsible Entity to choose the source of the patch based on its maintenance contracts, etc. While the SDT has changed the requirement to incorporate V1-V4 language, it cannot prescriptively describe every piece of software/firmware that should/should not be patched. The SDT notes that the software/firmware should include those that affect the Responsible Entity's system's capability to perform its function in support of BES reliability.

One commenter stated that Project 2009-06 is an interpretation which was not adequately addressed in this standard and suggested that the SDT revise the requirement to either require Responsible Entities to have documented procedures for supervised electronic access or specifically state that no supervised electronic access is allowed. The SDT notes that the notion of "supervised" or "supervision" relates to physical access, not electronic access. All electronic access must be authorized, regardless of whether "supervised" or "escorted" and all authorization must occur pursuant to the requirement language.

Many commenters were concerned about the time allotted for completing the assessment and creating a plan. The SDT has revised the requirement and added a two step process with 30 days for completing the assessment and 30 days for creating/revising the plan.

Many commenters raised concerns regarding the intent of "CIP Exceptional Circumstances." The SDT has removed "CIP Exceptional Circumstances" from the requirement.

A few commenters stated that Part 2.2 went beyond the stated rationale of requiring the current assessment to include the identification of what/who the source of the patch is so the time of availability can be determined. The commenters also felt that requiring a plan and an assessment was beyond the rationale and that a "plan" should not be required as it

implies a more extensive documentation of the patch reviews which will require additional paperwork that will not add value to the patch process. The SDT clarifies that the plan is the result of the assessment, if the assessment by the entity determines the patch to be applicable to their BES Cyber Assets. The SDT agrees and has reworked the requirements in the table to more closely model V4 language and added steps for additional clarity. The 'plan' is simply the entity's own plan for how to handle the vulnerability, which can include the installation of the patch using normal patch routines, or the implementation of new measures, or documentation of already existing measures. The requirement also now calls for a separate 'assessment', which is an assessment for applicability to the entity's systems and environment. The 'plan' for handling the vulnerability is then only needed for patches that are applicable. The timeframe can be a date certain or an event-based date.

A few commenters stated that firmware should not be included in the requirement as very few vendors post when firmware updates become available. A concern was also raised regarding the fact that firmware was mentioned in Part 2.1, but CIP-010 did not require the documentation of firmware levels. The SDT appreciates the comment, but has left firmware in scope, as entities do need to watch for any future firmware updates that address security issues, even if there are very few. The SDT has revised CIP-010 to require firmware level for cyber assets that don't have software versions.

Some commenters requested clarification on the definition of "defined timeframe." The SDT has removed "defined" and specifies instead that "the plan shall include the Responsible Entity's planned actions to mitigate the vulnerabilities exposed by each security patch and a timeframe to complete these mitigations."

A couple commenters suggested that the bulleted list in the measures for Part 2.3 (now Part 2.4 in the revised standard) should be separated by "or." The STD notes that the NERC standards convention is that bulleted lists mean "or" and numbered lists mean "and". Each bullet is separated by semi-colons and "or" has been added after the second to last bullet.

Some commenters raised concerns regarding applicability. The SDT has modified the applicability sections of all of the CIP Version 5 standards to be consistent.

One commenter was concerned that allowing entities to rely on a vendor to "certify" a patch before it is considered available would be an unnecessary delay and would increase the risk to the reliability of the BES. The SDT agrees with the points the commenter made, but in a mandatory and enforceable standard the SDT believes it is fraught with issues to require Responsible Entities to know and track the ultimate original source of all vulnerabilities in all software components of all BES Cyber Assets. As this standard expands in scope to include all types of field devices, the SDT believes it is problematic to measure and enforce such a requirement on all of an entity's purpose-built devices (i.e.,

substation IED's) that may have a vulnerability due to something found in some commercial real-time operating system kernel or embedded Linux kernel or Windows CE version in the device's firmware. The SDT believes it is reasonable and measurable for the entity to track the manufacturer of the device for firmware patches rather than the ultimate sources of vulnerabilities in embedded subcomponents. The SDT agrees that some poor vendor practices exist, but believes a CIP standard enforced on the Responsible Entities is not the place to deal with poor vendor practices. While the requirement is not a perfect control, we believe it is a large step in the right direction.

One commenter suggested that a more proactive mitigation, such as an upgrade plan, should be required for systems that do not require patches, but are still vulnerable to malicious exploitation. Further, the commenter was concerned that the requirement did not properly address increasing malicious attacks, mostly exploiting zero-day vulnerabilities. The SDT realizes that no single control is perfect at eliminating all risk and therefore the collection of standards accomplishes defense in depth with multiple levels of security concepts. The SDT does not believe that in a mandatory and enforceable standard that upgrades of functioning equipment should be required due solely to cyber security issues. The SDT also notes that patches do not address zero-day vulnerabilities, as they are 'zero day' because the vulnerability was previously unknown and thus no patches exist.

QUESTION 30 – CIP-007 R3:

CIP-007-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R3 – Malicious Code Prevention*.**" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.**

SUMMARY:

Based on stakeholder comments, the SDT did not make any changes to Requirement R3 or Part 3.1 but did make significant changes to the Parts 3.2 through 3.5 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity. Please see the redlined version of the standard for a complete set of revisions.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity

- Requirements - Use of the phrase, “initially upon the effective date”
- Requirements – Use of the phrase, “where technically feasible”
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The SDT received comments on the inclusion of the term “‘Maintenance Cyber Assets.”’ The SDT agreed with those comments as that occurrence of the term was missed as we changed “‘Maintenance Cyber Assets”’ to “‘Transient Cyber Assets’.” It has been removed from the standard (and so has the concept of “‘Transient Cyber Assets”’).

Numerous comments were received on the Transient Cyber Asset (“TCA”) requirements. The SDT agrees with many of the comments and has deleted those requirements. Part 3.4 required malware prevention tools on TCA’s. The point of the requirement is the protection of BES Cyber Systems from the introduction of malware, and that is included in Part 3.1. Part 3.5 covered logging of TCA connections, which provided no clear reliability benefit. Both have been struck. The SDT removed the term Transient Cyber Asset as a proposed glossary term, and the SDT added the concept of the previous definition to BES Cyber Asset as an exclusion. The SDT also considered the numerous auditing and evidence issues these two requirements posed and agreed to delete them.

The SDT received comments on the absence of ‘where technically feasible’ to allow for Technical Feasibility Exception (“TFE”)E requests. The SDT has not included this in R3, but R3 does not require specific external or locally installed controls as in previous versions. Parts 3.1 and 3.2 speak to “deploy methods. . .” and “mitigate the threat of . . .” Neither of those parts require particular external or dedicated controls, and it is expected that such requirements can be accomplished without a TFE. Furthermore, Part 3.3 is clear in its language that it only applies to devices that use signatures or patterns, and the SDT has added clarifying language to account for cases where a signature or pattern is only available infrequently. If a method doesn’t use signatures or patterns, Part 3.3 imposes no obligation upon it. For that reason, the SDT expects a TFE is not necessary. Overall, the SDT has crafted R3 in such a manner to clarify the desired results-based outcome without specifying technology-restrictive controls that would necessitate a TFE. In addition, the included guidance on R3 lists numerous methods an entity can use to meet the requirement.

The SDT received comments that the applicability of R3 should specifically exclude Low Impact BES Cyber Systems. The SDT disagrees with the comment, as the Applicability column throughout the standards specify what is in scope, not what is out of scope. An entity cannot be held to a requirement on a system if that system is not specifically noted in the

applicability column. In addition, with the now clarified "'high water marking"' concept of ESPs and "'Associated Protected Cyber Assets"' it is possible that if Low Impact Cyber Assets are within the same Electronic Security Perimeter ("ESP") with Medium or High impact systems, then they will be in scope of this requirement.

The SDT received comments suggesting limiting the malware requirement to only those medium impact BES Cyber Systems that have External Routable Connectivity. The SDT disagrees as the malware threat is not introduced solely through external network access. The SDT believes that most malware threats in a control system environment enter through portable media or locally connected devices. Stuxnet is one high profile example. For these reasons, tThe SDT has not made the suggested change.

The SDT received comments that the malware requirement should apply to Low Impact BES Cyber Systems. The SDT agrees that this is a good practice, however, in a mandatory and enforceable standard the evidence burden for all cyber assets would divert resources from higher impact systems and tasks. The SDT has purposefully decided to require only programmatic requirements for Low Impact assets and not require inventories or lists (which would be required for any device or system level requirement compliance measurement). This is due primarily to the large order of magnitude of cyber assets that would be in this category and the desire to have the industry not focusing the majority of its efforts on the lowest impact systems. For these reasons, tThe SDT has not made the suggested change.

The SDT received numerous comments on the "wheres" and "hows" of applying this requirement. The SDT has taken the approach of making this a competency based requirement and has stated a high level "what" with no "how.". The issue with previous versions of the standard is that it required a particular technology on all cyber assets, many of which could not meet the requirement. MAs malware prevention is a technical field in which technology is constantly changing and improving and new paradigms are constantly emerging in how to handle the issues, therefore, the SDT has made this a very high level requirement so as to allow entities to keep up- to- date with state of the art tools in this area and to do what makes sense adapt to for the specific systems and situations. There are no prescriptive "silver bullets" that can be specified without recreating the current state of generating more TFE's than incidents of compliance.

The SDT received comments around the terms "disarm or remove" concerning malware threats. Commentoers suggested that in some instances, removing or disarming is not the correct behavior. The SDT agreed and has changed to the following suggested language: to "mitigate the threat of."

The SDT received comments that Part 3.1 should include "based on the Cyber Assets susceptibility to malware" and that "Methods do not have to be used on every single Cyber Asset." The SDT disagrees as adding 'susceptibility' to the requirement is another element that could require some form of evidence from every entity for every Cyber Asset. For these reasons, tThe SDT has not made the change. The SDT has also made the requirement applicable at the systems

level, so that every Cyber Asset is not included. The included guidance discusses this issue and allows for the expressed concern.

The SDT received comments on the signature or pattern update requirement. The SDT agreed with these comments and has made numerous changes to add clarity to handle several special circumstances, as well as allow 35 days so that normal monthly update cycles have a chance to execute (35 days to account for 31 day months, or months that may start or end on a weekend or holiday, while generally supporting "once-a-month" frequency).

The SDT received comments on adding testing of signatures to the requirement. The SDT does not agree that this needs to be a prescriptive requirement. Some cyber assets may need testing because the impact of any false positive on reliability may be great, but other cyber assets within the system may benefit from the more timely and automated deployment of signatures where the impact of a false positive may be negligible. For these reasons, the SDT has not made the suggested change.

The SDT received comments that the signature update process should change from monthly to weekly. The SDT disagrees in that too frequent of a prescriptive requirement may preclude some entities from fully testing updates for those systems where the impact of a false positive is great. The point of the requirement is to state how stale signatures can be; it is not the prescription of ideal state. Other commenters suggested that monthly updates were too short for those who need to do manual updates of signatures. The SDT disagreed, in that if the situation calls for signature updates to be less timely than monthly, then other malware prevention solutions may need to be pursued.

Several other comments concerned the signature update requirement (R3.3), but the SDT stresses the conditional nature of the requirement's wording. It only applies in situations where the entity has chosen malware prevention techniques that are dependent on signature or pattern updates. There are numerous other solutions that are not dependent on signature or pattern updates and this requirement does not apply in those instances.

The SDT received comments that Part 3.2 should be part of an incident response in CIP-008-5. The SDT disagrees and does not believe the two are mutually exclusive. Simply invoking an incident response plan would not be sufficient as the malware would not be required to ever be mitigated. Part 3.2 ensures that the threat from the malware is mitigated. Some commenters requested a definite timeframe for the mitigation, but the SDT disagrees, as that will be situation specific. At times it may be the best course of action on a particular Cyber Asset to leave the malware in place for a time for forensic purposes (to discover what it is doing and who it is communicating with without alerting potential attackers).

Commenters raised issues with proving the 30 day timeframe for updates and suggested adding "from an identified source" for the signature or pattern updates. The SDT agrees and has made the suggested change.

QUESTION 31 – CIP-007 R4:

CIP-007-5 R4 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R4 – Security Event Monitoring*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT not make any changes to Requirement R4 or Part 4.4 but did make significant changes to Parts 4.1, 4.2, 4.3 and 4.5 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

General Measures concern: The SDT can not determine what an auditor will or will not request as evidence of compliance. The measures as written provide examples of strong supporting evidence of requirement compliance but do not preclude an entity from providing actual logs as evidence if the entity feels this represents appropriate evidence of compliance .... Actual alerts

In response: To the breadth of expressed industry concerns throughout the course of the 706 SDT effort, the SDT has gone to great effort in an attempt to create balanced standards which provide reasonable critical infrastructure cyber security, the latitude to address current and future technical conditions and moderate audit impact.

The SDT has reassessed the overall scope and applicability during the comment review period, and has concluded that CIP-007-5, R4 represents an approach which is a reasonable effort to advance the cyber security of the Bulk Electric System and critical infrastructure overall.

CIP-007-5 M4: With respect to the use of the word "must" rather than "may,", measure is stated in the context of the overall Standard, CIP-007-5, R4, which specifies a requirement for one or more documented processes and the implementation of those processes. M4 specifies evidence must include each of those documented processes, and further includes the evidence recommended in the Measures section of the table of Requirements as appropriate proof of the implementation of the standard, ; though such evidence may exist in many forms.

The SDT thanks you for your comments and consideration in review of CIP-007-5, R4. The responses were varied, decidedly insightful, and, in many cases provided much appreciated suggestions for change. After review of the submitted comments, the SDT updated the requirements with a goal toward improvement and enhancement, while trying to maintain a balance of reasonable critical infrastructure cyber security, latitude to address current and future technical conditions, and to moderate audit impact.

R4.1 received several comments expressing the need to include stronger TFE exclusion language. The SDT determined this is not necessary; but, following lengthy discussion, did determine to modify the language in an attempt to strengthen the basis for not requiring TFE exclusion language. In the context of R4.1, the requirement is to log (in a central repository) the specified event types only if a systemSystem or asset has previously detected and logged such events. Essentially, if event detection and logging at the asset does not occur, there is nothing subject to the R4.1 requirement of logging.

Another common concern with R4.1 was the use of the word "any" being too broad to scope the body of required event types. The SDT feels the use of the word "any" in this context is appropriate and provides an essential scope of security practice for the applicable systemSystems and assets for the purposes stated by the requirement.

R4.1.4: "Any detected potential malicious activity" raised two common themes;

1) The use of the word "potential" was far too broad in scope, a concern with which the SDT agreed and consequently removed the word "potential; and

2) Define "malicious activity," which the SDT determined was not necessary, as the standard English dictionary definitions of the words "malicious" and "activity" provide sufficient definition for behaviors to detect and log, and there is no real benefit to establishing a NERC glossary definition for "Malicious Activity".

Though some comments were received suggesting the removal of the enumerated listed of event types, and removal of

the “at a minimum” language, the SDT persists in the assertion that the enumerated list provides a minimum consistent with previous versions of CIP-005 and CIP-007, and retaining the use of “at a minimum” avoids interpretations that the event types can only be the types enumerated and provides latitude for entities to apply stronger cyber security controls to mitigate risks as warranted.

For R4.2, several comments noted concerns regarding the use of the term ”Real-time” in the requirement and related requests for removal or definition. The SDT offers that “Real-time,” in the context of R4.2 alerting, is appropriate. The intent is to establish that an entity alert on events with an aspect of urgency and immediate concern and respond in a manner of urgency and immediate concern, at least within the context of “Real-time,” as established within the CIP-002 Standard for determination of BES impact.

This is not a requirement that the systems Systems or assets themselves perform an alert, but rather a requirement that the entity implement a method to produce a real-timeReal-time alert upon detection of the stated conditions. The requirement has been updated in an effort to clarify this intent and to further specify the minimum set of events which necessitate a Real-time alert. The method of detection and alerting is not specified, leaving it to the Responsible Entity to develop such methodologies as would be determined appropriate to the level of risk.

The most significant changes were implemented across R4.2, R4.3, and R4.5 in an effort to better focus the intent and action of each and eliminate the conflicts noted in and across R4.3 and R4.5. The action to detect and alert logging errors has been moved from R4.3 and R4.5 to R4.2; leaving R4.3 focused on responding to logging failures, and R4.5 focused on summary review of logs. This largely addresses the confusion within R4.3 and R4.5 regarding dealing with the timing imposition of multiple interdependent actions for logging failures. To address concerns with the lack of specificity, R4.2 was modified to specify a minimum set of security events to alert on, including logging failures.

In addition to the inherent conflicts noted above, R4.3 received several comments and requests to extend the logging failure detection and response activation time frame to “next business day,” rather than “next calendar day” on the basis of potential increase in staffing burden to meet the requirement. Here the SDT continues with the belief that the activity response time threshold of “next calendar day” is reasonable for the applicable systems and assets. These system have sufficient import to warrant consistent detection and logging of at least the minimum behaviors noted. However, the requirement was updated to separate the detection requirement and to more clearly establish the “next calendar day” response activity applies after detection has occurred. It should be noted that this is not specifically a requirement to resolve the issue within that time frame. The action is to activate the response which leaves the Responsible Entity with discretion to assess the risk conditions and alleviate the condition accordingly.

It should also be noted that, wherein some comments were concerned with clarity in understanding what constitutes a

logging failure, the SDT offers that in the context of R4.3, "event logging failures" is intended to direct a Responsible Entity to address logging failures which otherwise prevent a Responsible Entity from performing the activities required by R4 on the whole.

R4.4, in turn, carried several comments to the effect that 90 days of log data was of limited or no benefit, and potentially onerous; or the requirement is actually a compliance data retention function and did not belong in a standard requirement . The SDT offers that this is not considered a data retention requirement. This is a standard requirement to ensure sufficient log data is kept by the Responsible Entity to achieve the intent of requirement 4.1; "for identification of, and after-the-fact investigations of, BES Cyber Security Incidents," and the activities of 4.5, "Review a summarization or sampling of logged events at a minimum every two weeks to identify undetected BES Cyber Security Incidents.".

Several other comments for R4.4 raised concern with the phrase "records-of-disposition" in the measures. The SDT recognizes the concerns with the phrase "records of disposition" in the measures, and has updated them to indicate that this is one of a list of potential documentation and has expanded the list of potential evidence to include log data retention configuration reports.

With respect to increasing applicability of 4.4 (90 day log retention) to a broader set of medium, the SDT considered increasing the scope, and concluded that the benefit of increasing the applicable systems or asset scope to include more Medium Impact installations would be less than the potential compliance burden of implementation. The SDT would like to note, however, that any Responsible Entity may go beyond the requirements in the interest of advancing security.

For R4.5, beyond the issues of conflict with 4.3, comments for R4.5 focused on the opinion that a two-week cycle of log summary review was too frequent, once a month was sufficient, and a perceived lack of benefit of such activity. The SDT believes that reviewing logged events at least every two weeks is a reasonable security practice for risks associated with the applicable systems and assets, and reasonably addresses the concerns raised by FERC Order 706, Paragraphs 525 and 628. An intent of this requirement is to supplement the alerting process and ensure entities are regularly reviewing logs for conditions which may not be already be identified for alerting, or indicate changing conditions which warrant an update to the conditions for alerting.

The requirement specifies a timeframe and scope of review, but not the manner of review. The SDT believes by not specifying the manner of review, Responsible Entities may engage in automated or manual review in accordance with their current or future capabilities.

QUESTION 32 – CIP-007 R5:

CIP-007-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R5 – System Access Controls*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT did not make any changes to Requirement R5 but did made significant changes to Parts 5.1 through 5.7 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

For Requirement CIP-007-5 R5 Part 5.1, many commenters did not believe the language was clear on the intent and felt extending this requirement to all components and accounts was not operationally feasible. In response, we have modified Requirement Part 5.1 according to commenters' suggestions. Part 5.1 is now limited to user access authentication and substitutes the word "enforce" for "validate" to provide clarity on the expectation. The reference to internal and remote access paths in the measures has also been removed.

In addition, the increase to 8 character passwords (see Part 5.5 in the revised standard) is part of an overall approach to making password requirements more flexible and appropriate to the risk reduction provided.

For Requirement CIP-007-5 R5 Part 5.2, (now Part 5.5 in the revised standard) commenters generally had 2 issues: (1) it

was unclear whether this requirement applied to individual accounts or types of accounts and (2) the CIP Senior Manager should not be required to authorize these accounts. In response, we have modified the requirement to make clear it applies to specific account types and have removed the requirement that the CIP Senior Manager or delegate authorize the account types.

Requirement CIP-007-5 R5 Part 5.3 refers to documenting personnel with access to shared accounts, which provides additional control to shared account and carries forward from the previous versions of CIP-007 Part 5.2.2.

For Requirement CIP-007-5 R5 Part 5.4, commenters overwhelmingly disagreed with application to all Responsible Entities. In response, we have moved all requirements applying to Low Impact BES Cyber Systems or all Responsible Entities to CIP-003-5 and made clear the requirements were programmatic and did not require a full inventory of BES Cyber Assets.

For Requirement CIP-007-5 R5 Part 5.5, most commenters expressed concern that the password change periodicity left too much open for interpretation. In response, we have moved the password change limitation to Part 5.5.4, reverted to an annual password change requirement and applied it to Medium Impact BES Cyber Systems with Routable External Connectivity.

Modifications were also made to the applicability section to address commenter concerns and to clarify that TFE requests may be submitted for this requirement.

QUESTION 33 – CIP-007 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-007-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the VSLs for all of the Requirements (R1 through R5) but did not make any changes to any of the VRFs.

A number of commenters suggested that the VSLs for CIP-007 should be revised so that each requirement has a complete set of four VSLs rather than only a 'High' and 'Severe.' For Requirements R2 and R3, the SDT adopted these suggestions by providing gradations based on how substantially the Responsible Entity missed the timeframe for compliance. For other Requirements, the drafting team did not adopt these suggestions because this approach is inconsistent with the FERC guideline for VSLs that requires each VSL to be based on a single instance of non-compliance (as opposed to cumulative instances). In the case of disabling ports, each port that is not disabled is a single instance of non-compliance,

and it is not possible to be partially compliant.

Several other clarifications to the VSLs for CIP-007-5 were suggested, and the SDT discussed each of the suggestions and adopted those that were consistent with NERC and FERC guidelines for VSLs.

A number of commenters made reference to the need to consider risk in assigning VSLs. Risk is not a factor in VSL assignments – a VSL is a measure of the degree of non-compliance, where a Severe VSL indicates total non-compliance or compliance that entirely misses the reliability intent of the Requirement, and a Lower VSL indicates that the entity was compliant with a substantial portion of the Requirement, but was not 100% compliant.

One commenter recommended changing the VRF for Requirement R2 from Medium to High. The drafting team did not adopt this suggestion because the comment seemed to be conflating VRFs and VSLs.

A small number of commenters suggested assigning multiple VRFs to each Requirement based on whether the systems in question were Medium Impact or High Impact. The SDT did not adopt this suggestion because each Requirement is required to have a single VRF. A single commenter suggested that the Requirements be split into separate Requirements for High and Medium Impact systems, for the same reason, and the drafting team declined ot adopt this suggestion because the team believes that VRFs and VSLs are used in combination with the particular facts of an entity's performance in determining a fair sanction for non-compliant performance.

QUESTION 34 – CIP-008 R1:

CIP-008-5 R1 states "Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications*.**" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.**

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the rationale and measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity

- Requirements - Use of the phrase, “initially upon the effective date” in Requirements
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The two most commented on issues for CIP-008-5 R1 were (1) coordination with the drafting of EOP-004-2 and (2) the applicability of R1 to all Responsible Entities.

Regarding the draft EOP-004-2, commenters expressed concern with the parallel drafting of EOP-004-2 and CIP-008-5. Some commenters noted the identification of reportable incidents was already covered in EOP-004-2 and the proposed requirements in CIP-008-5 resulted in double jeopardy. In response, the SDT continues to coordinate with Project 2009-01 in their revisions to EOP-004-2. CIP-008-5 requires a process to identify Reportable BES Cyber Security Incidents and EOP-004-2 requires the actual reporting. EOP-004-2 is being revised to refer to “reportable Cyber Security Incidents identified in CIP-008-3 and successor Standards”. We have also reverted to using the term “Cyber Security Incident” to allow the Standards to synchronize. We still propose the glossary term “Reportable Cyber Security Incidents” with a capital “R” as a means of scoping the types of Cyber Security Incidents for which an entity must test, review and perform lessons learned activities. These are also the types of incidents to which the draft EOP-004-2 refers as reportable Cyber Security Incidents. Several commenters also expressed concern about the absence of direction in 1.2 and 1.3 on which entities/agencies should receive reports on Reportable BES Cyber Security Incidents.

Many commenters disagreed with the expanse in scope of CIP-008-5 R1 to include all Responsible Entities. In particular, several noted the applicability was inappropriate because these cyber systems did not have requirements for an ESP and a PSP as referenced in the initial draft definition of BES Cyber Security Incident. In response, the applicability to all Responsible Entities for incident response is appropriate here because having an incident response capability is one of the more effective security controls to address multi-site cyber-attacks on the grid. Please refer to our summary consideration for question 49 regarding the inclusion of certain requirements applicable to all Responsible Entities. All requirements previously posted in CIP-004-5 through CIP-011-1 applying to Low Impact BES Cyber Systems or All Responsible Entities have moved to CIP-003-5 and apply to All Responsible Entities. We have made this change in response to comments to ensure these requirements have similar wording and measures. Also, the definition of BES Cyber Security Incident includes those incidents affecting the BES Cyber System in addition to those incidents associated with the ESP and PSP. Thus, the requirement to implement an incident response plan for High and Medium Impact BES Cyber Systems is now addressed in CIP-003-5, Requirement R1 – and the requirement to implement an incident response

plan for BES Cyber Systems not identified as High or Medium Impact Cyber Systems is addressed in CIP-003-5 Requirement R2. The revised CIP-008-5 does not include any requirements with applicability that says, "All Responsible Entities."

A few commenters expressed concern that applying requirements for incident response implicitly requires protection and monitoring controls. In response, we note the requirements to monitor for security events in CIP-006-5 and CIP-007-5 are applicable to only Medium and High Impact BES Cyber Systems. CIP-008-5 R1 only requires entities have a process to identify BES Cyber Security Incidents. There is no further requirement regarding the operation of event sources that may inform the identification of such incidents.

Some commenters noted that some of the change descriptions and justifications for Requirement R1 and its Parts were not correct. In response, we have modified the rationale and change descriptions for the main requirement and each of its Parts and added details to the justifications where previous documentation was insufficient or incorrect.

Other modifications include an expansion of requirement Part 1.3 into multiple requirement Parts to improve clarity. We also added "groups" in addition to "individuals" for response roles as recognition that incident response tasks may be assigned to a group rather than specific individuals. Guidance was added to CIP-008-5 R1 at the end of the document based on several commenters suggestions, including adding references to assist entities in developing an incident response plan.

QUESTION 35 – CIP-008 R2:

CIP-008-5 R2 states "Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in *CIP-008-5 Table R2 –BES Cyber Security Incident Response Plan Implementation and Testing."* **The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.**

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the requirement and its Parts and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, “initially upon the effective date” in Requirements
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The three most commented on issues for CIP-008-5 R2 were (1) the use of “initially upon the effective date” for periodic performance requirements in Part 2.2, (2) various concerns and disagreement with documenting deviations from the response plan and (3) having data retention requirements in requirement Part 2.3 instead of the compliance section.

In response to the first issue, references to the initial performance in requirements to test and review in CIP-008-5 have been moved to the implementation plan and allow a 12 month time period after the effective date to perform these tasks.

Several commenters noted the requirement to document deviations is administratively burdensome with no real security benefit. They state that entities should not be required to follow the plan because of all the uncertainties associated with a security incident. The SDT agrees that allowances should be made to deviate in the execution of a plan. The addition of this requirement is to address a concern expressed in the FERC Order 706 paragraph 694. This requirement ensures the plan will be used but does not restrict entities from taking needed deviations.

> Order 706 Paragraph 694: For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan. We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard

Commenters also state an explicit requirement to “implement” the plan in Part 2.2 is redundant with the main requirement. In response, we note Part 2.2 further indicates how the BES Cyber Security Incident response plan may be implemented according to the required periodicity and is therefore not duplicative of the main requirement R2. The requirement to “implement” the plan means the plan must be used, but this does not imply all parts of the plan are exercised.

In response to having data retention requirements, Part 2.3 has been modified to remove the actual retention period to

avoid conflicting with the retention periods specified in the compliance section of the Standard. However, the requirement to retain incident documentation is still necessary to ensure data for post-event analysis remains available.

Some commenters noted that some of the change descriptions and justifications for Requirement R2 and its Parts were not correct. In response, we have modified the rationale and change descriptions for the main requirement and each of its Parts and added details to the justifications where previous documentation was insufficient or incorrect.

Corporate Compliance noted the requirements in R2 applied to BES Cyber Security Incidents which can be very expansive. We agree and have modified the scope of these requirements to Reportable BES Cyber Security Incidents.

Other modifications include switching the order of Parts 2.1 and 2.2 to emphasize the main subject of the requirement. We also improved the wording in what is now Part 2.2 based on multiple commenters' suggestions. Guidance was added to CIP-008-5 R2 at the end of the document based on multiple commenters suggestions to add details about expectations with respect to exercising the response plan.

QUESTION 36 – CIP-008 R3:

CIP-008-5 R3 states "Conduct sufficient reviews, updates and communications to verify the REs response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R3, Parts 3.1 through 3.5 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date" in Requirements
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The primary issue raised by commenters for CIP-008-5 R3 was the clarity in time intervals. Many commenters felt the 30 day window for performing the lessons learned review and additional 60 days for updating was too short in some instances. In response, we have modified the language according to multiple suggestions to make clear the time intervals. We mistakenly proposed 60 calendar days in the posted version, not realizing there was already 30 days to perform the review. The 30 calendar days given to identify any changes from lessons learned and additional 30 days to update the plan (total of 60 days from response plan test) is consistent with FERC directives in Order 706 paragraphs 651, 728, and 731 that 30 calendar days is sufficient for updating documentation. Many commenters also distinguished that the review period in R3.2 should be initiated after the event has completed.

> Order 706 Paragraph 651: The Commission adopts a modified version of the CIP NOPR proposal. We direct the ERO to revise Requirement R9 to state that the changes resulting from modifications to the system or controls shall be documented quicker than 90 calendar days. The Commission believes that 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process or procedure to secure the system against a known risk. Therefore, the Commission believes that 90 days is too long to allow a responsible entity to have incorrect documentation. Thirty days should be sufficient time to update any necessary documentation.
>
> Order 706 Paragraph 728: The Commission stated its concern that individuals responsible for activating and implementing a recovery plan must have the most current information available, and its belief that a 90-day time lag between when a weakness in a recovery plan is discovered and when it is corrected and communicated to such responsible personnel is too long.172 We noted that failure for the responsible personnel to have current information about a recovery plan could cause unnecessary delay in restoring critical cyber assets to service and thereby jeopardize the reliability of the Bulk-Power System. Therefore, the Commission proposed to direct the ERO to modify Requirement R3 of CIP-009-1 to shorten the timeline for updating recovery plans to 30 days, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. We stated our belief that a 30 day requirement for updating the recovery plans will promote timely incorporation of

lessons learned during exercises and actual events, while acknowledging that 90 days is reasonable for the completion of personnel training sessions, due to varied shifts schedules and other feasibility issues with regard to facility and organization.

Order 706 Paragraph 731: The Commission adopts the CIP NOPR proposal to direct the ERO to modify Requirement R3 of CIP-009-1 to shorten the timeline for updating recovery plans. We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective. As we stated with respect to change made pursuant to CIP-007-1, the Commission believes that having correct documentation is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could attempt to operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process or procedure to secure the system against a known risk. Therefore, the Commission believes that 90 days is too long to allow a responsible entity to have incorrect documentation. Thirty days should be sufficient time to update any necessary documentation. Northern Indiana has not provided us sufficient reason to change the CIP NOPR proposal. Finally, as stated with respect to the documentation requirements in CIP-007-1, the 30 day period should begin upon final implementation of the modifications.

For requirement Part 3.4, several commenters noted that the term “organizational changes” is overly broad. In response, we have modified the Part 3.4 to specifically include organizational changes from the required plan components in R1. This has also been modified to limit these changes to those that “impact the ability to execute the plan”.

For Part 3.5, we have replaced the requirement to “communicate updates” with more specifically, “distribute updates”. Several comments also asked that the phrase “initially upon the effective date of the standard” in Part 3.1 be changed or moved to the implementation plan, and this change was adopted – the implementation plan now allows a 12 month times period after the effective date to perform these tasks.

Some commenters noted that some of the change descriptions and justifications for Requirement R3 and its Parts were not correct. In response, we have modified the change descriptions for the main requirement and each of its Parts and added details to the justifications where previous documentation was insufficient or incorrect.

Guidance was added to CIP-008-5 R3 at the end of the document based on multiple commenters’ suggestions. In particular, we have added timelines to illustrate the timing intervals in R3.

QUESTION 37 – CIP-008 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-008-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to VSLs but made no changes to the VRFs.

Please see the redlined version of the standard for the complete set of revisions.

The majority of commenters expressed the need for gradated VSLs, particularly in the timed requirements. In response, we have modified the VSLs to include varying degrees of severity based on the number of days/months late in performance of a requirement.

We incorporated a suggestion to include requirement references to the VSL parts to make it easier to see that noncompliance with each of the Parts is addressed in the set of VSLs associated with each requirement.

We have also updated the VSL language to reflect the changes made to the language in the requirements in CIP-008-5.

QUESTION 38 – CIP-009 R1:

CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*.**" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.**

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement T1 and Parts 1.1 through 1.5 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"

- Requirements – Use of the phrase, “where technically feasible”
- Measures - Use of the word, “must”

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

(1) Part 1.1 - Rationale has been corrected per comments received by removing the reference to Order 706.

(2) Part 1.2 - Returned to the original wording which refers to roles and responsibilities for recovery plan but does not require identification of individuals responsible for the recovery efforts

(3) Part 1.3 - “Protection” requirement has been removed as it was duplicated elsewhere in the CIP-011 requirements.

(4) Part 1.3 - Replaced “restore” with “recover” in order to reinforce the concept of BES system recovery and to specifically exclude full facility restoration.

(5) Part 1.4 and 1.5 - Column headings have been corrected.

(6) Part 1.5 - Was changed to require entities to have a process or guidance to preserve data in their plan and excepting the preservation of data for CIP Exceptional Circumstances so as to not impede or restrict system restoration. The SDT determined that this requirement should remain in the recovery standard versus moving to the response standard, the recovery sequences can have preplanned preservation of data not requiring TFEs.

Some commenters made generic suggestions for improvements to the set of CIP standards and the response to these comments is included in the "Summary Response to Generic Comments" at the front of this report.

QUESTION 39 – CIP-009 R2:

CIP-009-5 R2 states “Each Responsible Entity shall implement one or more processes that collectively address the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.”* **The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.**

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R2 Parts 2.1, 2.2 and 2.3 and to the

associated rationales, and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

(1) Part 2.1 – Replaced "implement" with "test" and deleted the requirement to complete the initial test upon the effective date of the standard.

(2) Part 2.2 – Changed, "…test any information…" to "…test information…"

(3) Part 2.2 – Wording was changed to ensure that recovery information on backup media is "useable and is compatible with current system configurations. " The change was in response to comments that "reflecting current configurations" would be too difficult, as the term "current" was too vague.

(4) Part 2.2 – In response to concerns over requirement language implying that the information must "reflect" current configurations, the SDT believes that it would be sufficient to test that the information remains compatible with current system configurations and has clarified the language to specivy that the test "is compatible with" current configurations.

(5) Part 2.3 – In response to stakeholder concerns that testing plans was burdensome, changed the applicability to require testing only for High Impact BES Systems to focus this requirement on the most critical systems.

(6) Part 2.3 – In response to stakeholder comments indicating that Part 2.3 duplicates Part 2.1 the SDT disagrees because Part 2.3 requires a more thorough operational exercise once every three years than the simpler test required in Part 2.1.

QUESTION 40 – CIP-009 R3:

CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to Requirement R3 Parts 3.1, 3.2, 3.3, and 3.4 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The SDT has made changes to in response to stakeholder comments. Highlights of the changes are shown below. Please see the redlined version of the standard for complete set of revisions to the requirements and measures.

(1) Part 3.1 - In response to many comments disagreeing with the need for an initial review, the SDT essentially removed all Part 3.1 review requirements. Adequate reviews are in the requirements that follow, and the SDT substituted the requirement to conduct reviews with a requirement to document any identified deficiencies or lessons learned associated with each recovery plan test or actual incident recovery within 30 calendar days after completion of the

test or recovery.

(2) Part 3.2 – Part 3.2 was moved to Part 3.1. CIP-009-5 Requirement R1 already compels the responsible entity to have a recovery plan, and the plan will already have been reviewed when it was developed and approved. In addition, there will be reviews as each recovery plan test or actual incident recovery lessons learned are incorporated .

(3) Comments regarding improving alignment with CIP 008-5 were received. Part 3.2 essentially remains as it was previously in Part 3.3 while maintaining consistency with CIP 008-5, with 30 days to update the recovery plan after completion of Part 3.1 documentation of deficiencies or lessons learned.

(4) Part 3.3 – Part 3.3 was rewritten align with CIP 008-5 while clarifying, in response to comments, that the responsible entity has the lead in determining changes that would impact its ability to execute the recovery plan.

(5) Part 3.4 – Replaced "communicate all" with "distribute" to clarify and improve the audit ability.

(6) Measures – Associated measures were also updated to reflect the changes to the associated requirements

Following is a response concerning stakeholder objections to the language in Part 3.1 to have the review of the recovery plan "initially upon the effective date":

In several instances in the Version 5 requirements, the SDT proposed periodic performance of some requirements, and they specified in the first posted draft's requirement language that the first iteration must be performed "initially upon the effective date." Several commenters raised concerns with this language, and they suggested that not all initial performances should occur upon or before the effective date. The SDT agrees, and it has evaluated each periodic performance requirement. Consequently, the drafting team has removed "initially upon the effective date" from all the CIP standards, and references to the initial performance in the requirements have been moved to the implementation plan.

Former part 3.2 (now part 3.1) – Some stakeholders indicated that 30 days was not sufficient to update documentation and the SDT disagrees. Given the importance of having these plans in place the SDT believes that 30 days is sufficient to update documentation.

Former part 3.4 (now part 3.3) – Some stakeholders questioned the need for Part 3.4 – the requirement to update the recovery plans. The SDT believes that current part 3.3 is in alignment with FERC Order 706, paragraph 686.

> Order 706 Paragraph 686:"The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills,

and responses to actual incidents, all of which must include lessons learned. The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.

QUESTION 41 – CIP-009 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-009-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the VSLs for all of the requirements in CIP-009 but made no changes to the VRFs.

The majority of commenters who provided comments on proposed VRFs and VSLs asked for gradated VSLs, particularly in requirements specifying a time period. In response, the SDT has reworked all of the VSLs. They are now gradated, and they are based on the number of days/months late for particular requirements that specify periodic performance. In most cases, the team fully gradated the requirement to account for Low, Moderate, High, and Severe VSLs.

Some commenters were concerned that the VSLs require 100% compliance, but the SDT notes that the FERC and NERC guidelines for VSLs require each VSL to account for all levels of noncompliance. However, as noted earlier, the SDT has made significant efforts to make the VSLs in this standard gradated in nature, such that smaller violations fall within the "lower" VSL. Other comments recommend a Corrective Action Program (CAP) be implemented by registered entities, but the SDT notes that a Corrective Action Program is not the same as a VSL. A VSL accounts for the level of noncompliance, and the Corrective Action Program comes after one has already determined some level of noncompliance. While noting the value of Corrective Action Programs in certain circumstances, the VSL or the standard itself is distinct from this enforcement mechanism.

Some commented on the evidence retention period for the standard and expressed concern over the authority for a CEA to ask an entity to provide other evidence to show that it was compliant for any period since the last audit that may exceed the specified evidence retention period. The commenter noted concern that the guidance is contradictory. The SDT notes that the evidence retention language the commenter is concerned about is boilerplate language for the evidence retention section, and it is meant to specify that the evidence required during that additional period is not necessarily the full amount of evidence that is otherwise required during the specified evidence retention period. The Rules of Procedure Appendix 4c - Section 3.1.4.2 that became effective Jan 1 2011 identifies that the CEA can ask an

entity to demonstrate that it was compliant for the full period of time since the last audit without regard to what is stated in the evidence retention section of the standard.

One commenter suggested that periodic requirements that require performance "...initially upon the effective date..." be moved to the implementation plan. The SDT agrees, and all periodic requirements' initial performance is now outlined in the implementation plan.

Finally, the drafting team notes that it has updated the VSLs in the standard to reflect the draft requirement language in CIP-009-5.

QUESTION 42 – CIP-010 R1:

CIP-010-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management*.**" The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.**

SUMMARY:

Based on stakeholder comments, the SDT did not make any significant changes to Requirement R1, but did make significant changes to its rationale and to Parts 1.1 through 1.5 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Requirements – Use of the phrase, "where technically feasible"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

Numerous comments were centered around several main issues. In response to those comments, the SDT has made revisions to the main parts and sub-parts in Requirement R1. Please see the redline version of the standard for complete revisions. Below is a highlight of the revisions:

(1) Part 1.1 - Removed physical location from part 1.1.1.

(2) Part 1.2 - Removed CIP Senior Manager language for authorization of deviations to existing baseline configurations.

(3) Part 1.3 - Added clarity around updating documents around NERC Standards to CIP-005 and CIP-007.

(4) Part 1.4 - Removed scripts from formerly part 1.1.4 now part 1.1.3.

(5) Part 1.4 - Added clarity around cyber security controls to reference CIP-005 through CIP-007.

(6) Part 1.5 - Allowed for TFEs and production environments where the test is performed in a manner that minimizes adverse effects.

Following are responses to comments:

Part 1.1 – 'Grouping' is one method that an entity could use to identify multiple software programs. Requirement R1 Part 1.1 is written to allow flexibility for entities to develop their baseline configuration with the items required as they see fit.

Part 1.3 – The phrase "as necessary" is used to limit the amount of effort required in regards to updating the baseline configuration and other documentation required by a NERC CIP Standard.

Part 1.1.3 – The intent of CIP-010-1 Requirement R1 Part1.1.3 is to be able to define what commercially available application software should exist on the responsible entity's BES Cyber System. If additional software has been unintentionally installed, the entity should be able to document this so as to be able to identify software that was maliciously installed in future assessments. The SDT believes that even certain software changes can unexpectedly lead to exploited vulnerabilities or other adverse effects. Therefore, changes include any changes that deviate from baseline configurations.

Part 1.1.3 – The SDT intent of "commercially available" and "intentionally installed" in regards to application software was to be able to restrict the identification of "notepad" applications, but include the identification of commercially available software such as Linux or Windows.

Formerly Parts 1.1.5 and 1.1.6 (Parts 1.1.4 and 1.1.5 in the revised standard) - The SDT intentionally used "any" as a modifier for the items that should be included in a baseline configuration. The term "any" suggests that if the item does not exist on the BES Cyber System, then the entity would not need to include the item in its baseline configuration. If "any" was not included, then an entity would be required to have an item on its baseline configuration that may not be installed on the BES Cyber System.

Parts 1.4.1 and 1.5.2 – Work together in an effort to ensure changes are tested properly. Prior to implementing a change to a BES Cyber System that deviates from the existing baseline configuration, an entity must determine the impacted cyber security controls (added language specifying cyber security controls identified in CIP-005 through CIP-007) according to CIP-010-1 Requirement R1 Part 1.4. CIP-010-1 Requirement R1 Part 1.5 asks entities to test the controls prior to implementing the change in a production environment. Entities are then to verify that the controls determined in CIP-010.1 Requirement R1 Part 1.4.1 were not adversely affected by the change.

Part 1.4.2 – The SDT's use of availability is in regards to the BES Cyber System's ability to operate as designed after a change to the baseline configuration has been made. The concept presented here is to be able to meet the FERC Order 706 directive around "processes that permit a reasonably high level of confidence modifications do not have unintended consequence".

Parts 1.4 and 1.5 – CIP-010-1 Requirement R1 Part 1.4 Part1.5 are different requirements that can be taken as complementary rather than duplicative for Control Centers. CIP-010 R1 Part 1.5 requires testing changes in the test environment, while CIP-010-1 Part 1.4 requires researching and documenting changes. Due to the level of impact of a compromised Control Center, the SDT believes that testing changes in a test environment is necessary and contributes to the overall prevention of unauthorized modifications of the BES Cyber System.

Part 1.5 – The SDT believes that CIP-010-1 Requirement R1 Part 1.5.1 written as is presents a sufficiently, clear objective. The precursor to Part 1.5.1 and Part 1.5.2 is "entrance criteria" text ensuring the related parts are only applicable if there is a change that deviates from the existing baseline configuration for Control Centers. The SDT believes "including a description of the measures used to account for any differences in operation between the test and production environment" is necessary since it may not always be possible for test environments to exactly mimic production environments.

Parts 1.5.1 and 1.5.2 – The language of CIP-010-1 Requirement R1 Part 1.5 requires the documentation of differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments. If the entity can demonstrate proper documentation that its model takes into account the details of CIP-010-1 Part 1.5, then the entity would not be in

violation of the requirement.

Following is response to comments concerning applicability:

The SDT has modified the applicability sections of all of the CIP Version 5 standards for consistency.

Following is a response to comments concerning baseline configuration:

Part 1.1 – The SDT believes that CIP-010-1 Part 1.1 does indeed adhere to FERC Order 706, paragraph 399.

> Order 706 Paragraph 399: Many of the comments address practical issues involved in addressing accidental consequences and malicious actions, and we recognize that such issues exist. We, thus, agree with Puget Sound that change control and configuration management processes for critical cyber assets cannot ensure 100 percent integrity for those assets when making changes. We do not seek absolute assurances but rather are concerned that there be processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. However, we reject Puget Sound's proposal that the Reliability Standard should expressly recognize that absolute assurances are not required.
>
> We also believe that our revised directive to the ERO on Requirement R6 addresses Puget Sound's concern about the limitations imposed by a test environment.

The SDT believes that establishing a baseline configuration is the first step to "provide an express acknowledgment of the need for change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." Accordingly, the SDT believes that the baseline configuration should be included in CIP-010-1 Requirement R2 Part2.1. CIP-010-1 Part 1.1 has been modified in consideration of your comment. The SDT believes that monitoring for changes to baseline configuration, in combination with the change management processes defined in CIP-010-1 R1, can aid in preventing unauthorized modifications to BES Cyber Systems. This new requirement was also added to address the remaining objectives of FERC Order 706 (Paragraph 397).

> Order 706 Paragraph 397: Based upon the comments received the Commission is altering its position on how best to address the apparent deficiencies of Requirement R6 in CIP-003-1. The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes. The Commission believes that these considerations are significant aspects of change control and configuration management
>
> that deserve express acknowledgement in the Reliability Standard. While we agree with Entergy that the NIST

Security Risk Management Framework offers valuable guidance on how to deal with these matters, our concern here is that the potential problems alluded to be explicitly acknowledged. Our proposal does not speak to how these problems

should be addressed. We do not believe that the changes will have burdensome consequences, but we also note that addressing any unnecessary burdens can be dealt with in the Reliability Standards development process.

Following are responses to comments concerning documentation:

Some comments suggested that the Version 5 standards should not have any documentation requirements. In general, the SDT has endeavored to remove or minimize requirements that exist solely for purposes of creating documentation. However, there are other factors that support the use of requiring documentation in certain instances. The SDT has attempted to strike the appropriate balance.

The SDT notes that many NERC standards require some level of procedure documentation to support the pre-thought responses to known conditions or to ensure consistent responses when known events happen. Furthermore, certain documentation is essential to measure what needs to be secured. The SDT has sought to minimize such documentation requirements, and it has tried to provide detailed guidance. However, guidance alone is not a sufficient place for such documentation needs, as guidance is not mandatory or enforceable.

Following are responses to comments concerning evidence retention:

Some commenters raised concerns about the evidence retention periods in the standards, to include concern that they are not the same as those in Version 4, that they increase the period from one to three years, or raised concerns that they have a general misunderstanding over retention when the period between compliance audits may exceed the frequency stated.

The evidence retention periods in the compliance section of the standards have been modified to make clear the expectation from the CMEP that entities have compliance evidence for the entire audit period. Furthermore, in some cases, compliance retention is different than records retention for the purpose of security analysis. The “requirement” level retention, where applicable, relates to maintaining records long enough to analyze them for security purposes, anomalous behavior, etc. – these retention periods are for records that are retained by the responsible entity for the responsible entity’s own use; “compliance” retention, as specified in the compliance section of the standard, deals with demonstrating that the requirement has been met (e.g., to demonstrate that the entity has maintained a “rolling” 90-day set of logs throughout the entire compliance audit period where the requirement specifies logging for 90 days) – these

retention periods are solely for the purpose of demonstrating compliance. With respect to increases in the evidence retention periods from one to three years, the SDT notes that the initial evidence retention language pre-dates the establishment of the compliance program and its associated documented procedures. The compliance program requires that entities must "demonstrate compliance" for the entire compliance period (not that they must maintain all records for the entire compliance period). Note the distinction between demonstrating compliance and maintaining all records noted in the requirements (e.g., again, to maintain records for 90 days for security analysis vs. demonstrating that records have been kept for a rolling 90-day period for an entire compliance period, whether 3 or 6 years).

Following are responses to comments concerning the test and production environments in Requirement R1, Part 1.5:

The language of CIP-010-1 Part 1.5 requires the documentation of differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments. If the entity can demonstrate proper documentation that their model takes into account the details of CIP-010-1 R1.5, then the entity would not be in violation of the requirement.

The language of CIP-010-1 Requirement R3, Part 3.2 requires the documentation of differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments. If the entity can demonstrate proper documentation that their model takes into account the details of CIP-010-1 R1.5, then the entity would not be in violation of the requirement.

Prior to implementing a change to a BES Cyber System that deviates from the existing baseline configuration, an entity must determine the impacted cyber security controls (added language specifying cyber security controls identified in CIP-005 through CIP-007) according to CIP-010-1 Part 1.4 (CIP-010-1 Requirement R4, Part 4.1.1). CIP-010-1 Part 1.5 (applicable to High Impact BES Cyber Systems only) asks entities to test the controls prior to implementing the change in a production environment and then document the results. Entities are then to verify that the controls determined in CIP-010.1 Part 1.4.1 were not adversely affected by the change (CIP-010-1 Part 1.4.2). This process ensures that (quoting FERC Order 706) "a reasonably high level of confidence modifications do not have unintended consequence".

Following is a response to comments concerning measures:

The SDT reminds commenters, as stated in the Background of the standard, "Measures… provide examples of evidence to show documentation and implementation of specific elements required in the documentation process".

QUESTION 43 – CIP-010 R2:

CIP010-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring."* **The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.**

SUMMARY:

Based on stakeholder comments, the SDT did not make any significant changes to Requirement R2 but did make significant changes to Part 2.1 and the associated rationale and measure. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The SDT has made several changes to CIP-010-1 Requirement R2 in consideration of industry comments:

(1) Clarity has been added regarding monitoring for configuration changes.

(2) Part 2.1 - The language "monitor for changes to the baseline configuration" to "monitor continuously or periodically, not to exceed once every 35 calendar days". The 35 calendar days reflects, generally, a "monthly" timeframe while allowing for slight flexibility for weekends, holidays, etc., that might fall at the beginning or end of a particular month.

Following are responses to various comments:

The applicability of CIP-010-1, Requirement R2 incorrectly identified Medium Impact BES Cyber Systems during the last posting. This was a transcription mistake from earlier drafts, and Medium Impact BES Cyber Systems have been removed

from the applicability.

In response to how to automate finding the difference between ephemeral and unauthorized ports. CIP-010-1 Requirement R1's baseline configuration identifies available ports for the BES Cyber System (while CIP-005-5 references the enabling of ports).

An unauthorized change would be a change that deviates from what the entity had identified on its baseline configuration. Recall that the baseline configuration is looking only at logical network accessible ports. A concern of double jeopardy between Requirements R1 and R2 was raised. The SDT believes that Requirements R1 and R2 in combination provide for the effective "monitoring of the configuration of the BES Cyber System and provides an express acknowledgement of the need to consider malicious actions along with intentional change." The SDT does not feel this creates double jeopardy.

Comments were received concerning the burden of detecting unauthorized changes and the load placed on systems caused by automation. The SDT believes that monitoring for changes to baseline configuration, in combination with the change management processes defined in CIP-010-1 R1, can aid in preventing unauthorized modifications to BES Cyber Systems. This new requirement was also added to address the remaining objectives of FERC Order 706 (Paragraph 397).

> Order 706 Paragraph 397: Based upon the comments received the Commission is altering its position on how best to address the apparent deficiencies of Requirement R6 in CIP-003-1. The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes. The Commission believes that these considerations are significant aspects of change control and configuration management that deserve express acknowledgement in the Reliability Standard. While we agree with Entergy that the NIST Security Risk Management Framework offers valuable guidance on how to deal with these matters, our concern here is that the potential problems alluded to be explicitly acknowledged. Our proposal does not speak to how these problems should be addressed. We do not believe that the changes will have burdensome consequences, but we also note that addressing any unnecessary burdens can be dealt with in the Reliability Standards development process.

As stated in the CIP-010-1 Guidelines, "It should be understood that the intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). It is for this reason that automated technical monitoring was not explicitly required and an entity may choose to accomplish this requirement through manual procedural controls."

Following is a response to comments concerning evidence retention:

Some commenters raised concerns about the evidence retention periods in the standards, to include concern that they are not the same as those in Version 4, that they increase the period from one to three years, or a that they have a general misunderstanding over retention when the period between compliance audits may exceed the frequency stated.

The evidence retention periods in the compliance section of the standards have been modified to make clear the expectation from the CMEP that entities have compliance evidence for the entire audit period. Furthermore, in some cases, compliance retention is different than records retention for the purpose of security analysis. The "requirement" level retention, where applicable, relates to maintaining records long enough for the responsible entity to analyze them for its own security purposes, anomalous behavior, etc.; "compliance" retention, as specified in the compliance section of the standard, deals with demonstrating that the requirement has been met (e.g., to demonstrate that the entity has maintained a "rolling" 90-day set of logs throughout the entire compliance audit period where the requirement specifies logging for 90 days). With respect to increases in the evidence retention periods from one to three years, the SDT notes that the initial evidence retention language pre-dates the establishment of the compliance program and its associated documented procedures. The compliance program requires that entities must "demonstrate compliance" for the entire compliance period (not that they must maintain all records for the entire compliance period). Note the distinction between demonstrating compliance and maintaining all records noted in the requirements (e.g., again, to maintain records for 90 days for security analysis vs. demonstrating that records have been kept for a rolling 90-day period for an entire compliance period, whether 3 or 6 years).

Following are responses concerning technical feasibility exceptions:

In regards to technical feasibility, the SDT notes the technically feasible language in CIP-010-1 R2 is consistent with its use in other V5 standards.

Some commenters asked whether the Technical Feasibility Exception ("TFE") process in the NERC Rules of Procedure, Appendix 4D, will be revised upon changes made to these standards. The SDT notes that requirements that require the submission of a TFE are identified in the NERC Rules of Procedure and changes to that document are outside of the scope of this SDT. Historically, phrases such as "where/when technically feasible" have been considered trigger language for requirements necessitating a TFE when alternative measures are implemented. It is expected that the NERC TFE process will be modified to specify which requirements of Version 5's standards will require TFE submissions once the standards are finalized and submitted to the Commission.

Other commenters were concerned that "where technically feasible" suggests that an entity may unilaterally decide that a requirement does not apply, without filing for a TFE. The SDT respectfully notes that entities are required to be compliant with all NERC reliability standards for which their function is applied. In some cases, compliance is

demonstrated by showing that the entity has no applicable assets; in other cases, compliance is demonstrated through the TFE process. In no case does any language in a NERC reliability standard grant an exemption from compliance to applicable Responsible Entities.

QUESTION 44 – CIP-010 R3:

CIP-010-1 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3– Vulnerability Assessments*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Based on stakeholder comments, the SDT did not make any significant changes to Requirement R3 but did make significant changes to Parts 3.1 through 3.4 and to the associated rationales and measures. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Several comments submitted in response to this question were submitted in response to every question and address the following generic issues:

- Applicability (Section 4 of the standard) – specific suggestions for adding clarity
- Requirements - Use of the phrase, "initially upon the effective date"
- Measures - Use of the word, "must"

Rather than repeat the issue and response here, the SDT has provided its response to these generic issues at the front of this report.

Please see the redlined version of the standard for the complete set of revisions.

The SDT has made several changes to CIP-010-1 Requirement R3 parts and the associated measures in consideration of industry comments. Below is a highlight of the revisions. Please see the redline version of the standard for a complete set of revisions to the requirements and measures:

(1) Part 3.1 - Removed "initially upon the effective date".

(2) Part 3.1 - Clarified security controls to refer to CIP-005 through CIP-007.

(3) Part 3.2 - Removed "initially upon the effective date" and replaced with "where technically feasible".

(4) Part 3.2 - Allowed for production environments where the test is performed in a manner that minimizes adverse effects.

(5) Part 3.3 - Applicability – added Associated Protected Cyber Assets.

(6) Part 3.3 - Added …" and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset)."

(7) Part 3.4 - Added "any remediation or mitigation action items."

(8) M3.1 - Changed to "once" every calendar year and added "or".

(9) M3.2 - Changed to "at least once every 36 calendar months between assessments."

(10) M3.3 - Removed BES.

(11) M3.4 - Added …"documented" proposed dates of completion "for the action plan…"

Following are responses to various comments:

Requirement R3 – When asked about Vulnerability Assessments, the SDT responds that Vulnerability Assessments act as a component in an overall program to periodically ensure the proper implementation of security controls as well as to continually improve the posture of BES Cyber Systems. This new requirement was also added to address the remaining objectives of FERC Order 706 (Paragraph 644).

> Order 706 Paragraph 644: The Commission agrees with ISO-NE that hardware and software is implemented in diverse ways throughout the industry, but does not believe that this renders providing guidance infeasible. We also agree that overly rigid guidance could result in responsible entities failing to properly test for vulnerabilities specific to the entities' environments and systems. The Commission does not believe that the revised Reliability Standard should be inflexible. It should encourage responsible entities to take into account emerging and diverse technologies and newly discovered vulnerabilities as they emerge. The Commission believes that it is appropriate to leave such guidance to the Reliability
>
> Standards development process. Further, we leave it to the ERO's discretion whether to put guidance in the

revised Reliability Standard or a reference document.

Requirement R3 and parts – Please note that neither Requirement R3 nor its parts use the term passive vulnerability assessment.

Part 3.1 - A request for clarification of whether variances noted in the assessment would be required to self-report was noted. No, the purpose of a vulnerability assessment is the ability to detect vulnerabilities that have been previously unknown.

Part 3.1 – A commenter notes the annual vulnerability assessments on Medium Impact Cyber Systems will prove to be very costly and resource intensive for utilities with multiple substations in this category that are geographically dispersed and suggests allowing two years between vulnerability assessments. The SDT notes that Part 3.1 requires a paper or active vulnerability assessment to determine the extent to which the security controls identified in CIP-005 through CIP-007 are implemented correctly and operating as designed. The SDT does not prescribe what should be included in an entity's paper or active vulnerability assessment as this is left for the entity to determine. The annual timeframe is carried over from CIP-007-4 Requirement R8 and at this time the SDT does not have sufficient data to justify extending the timeframe as proposed.

Part 3.2 - Requires the documentation of differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments. If the entity can demonstrate proper documentation that its model takes into account the details of CIP-010-1 Part 1.5, then the entity would not be in violation of the requirement.

Part 3.2- Request for clarification of what a "test environment" is compared to a "production environment." As stated in Guidelines, "Additionally, the entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a control center BES Cyber System which may not be able to be replicated such as a legacy map-board controller or the numerous data communication links from the field or to other control centers (such as by ICCP)."

Part 3.3 - CIP Exceptional Circumstances is a newly defined term that will be included in the NERC Glossary of terms with NERC CIP V5 standards approval. CIP Exceptional Circumstances are defined as "A situation that involves one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of

large scale workforce availability." The intent was to capture circumstances that may require exceptions to the NERC CIP standards.

Part 3.3 - Is not covered by the Implementation Plan by design, as it is a requirement specifying vulnerability assessments for adding Cyber Assets to High Impact BES Cyber Systems.

Part 3.4 –A question was asked about what date the auditor will audit against if there is not an exact time period listed in the requirement e.g. 90 days. The SDT notes that an auditor would audit the requirement based on the planned date that identified and documented by the responsible entity in its action plan. The SDT did not specify acceptable deviation between the environments as the requirement language only requires documentation and the measures used to account for any differences.

Part 3.4 - A concern was expressed about the potential need for a CAN around the acceptable deviation between test and production that auditors will allow. The SDT did not specify acceptable deviation between the environments as the requirement language only requires documentation and the measures used to account for any differences.

Following is a response to comments concerning measures:

The SDT reminds commenters, as stated in the Background of the standard, "Measures… provide examples of evidence to show documentation and implementation of specific elements required in the documentation process".

Following is a response concerning wireless review in the Guidelines section versus the Requirement section:

Since wireless can be a potential attack vector, "Wireless Review" and "Wireless Scanning" elements were included in the Guidelines and Technical Basis section for CIP-010-1 R3. Guidance provides details on the elements that should be included within an active vulnerability assessment. In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

QUESTION 45 – CIP-010 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-010-1? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the VSLs for all requirements, and changed the VRF for R1 and R2 from Lower to Medium. In addition, the SDT added another time horizon, "Long-term Planning" to R3.

Several comments were received concerning the severity of the VSLs. While the SDT appreciates the perspectives of the

commenters, the SDT notes the VSLs are aligned with mapped requirements from Version 4 of related standards.

A comment was received concerning the VSLs having the potential to cause double jeopardy. The SDT notes that only requirements can put an entity in the position of double jeopardy.

For comments related to evidence retention and baseline configuration, the SDT refers the commenters to the summary for Question 42.

QUESTION 46 – CIP-011 R1:

CIP-011-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-011-5 Table R1 – Information Protection*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

Comments regarding Question #46 dealt with several topics, including: (1) the scope of CIP 011-5 R1, (2) confusion concerning assessments, (3) measures used to identify BES Cyber System Information, (4) overlap with access control, and (5) consistent wording.

(1) Scope of CIP 011-5 R1

Several commenters responded that the scope for CIP 011-5 was too broad. In keeping with prior versions of CIP, the "Associated Protected Cyber Assets" has been removed from the scope of CIP 011-5, thus narrowing the scope of the standard further.

Some commenters were confused about which requirements applied to Low Impact BES Cyber Systems. The scope of CIP 011-5 does not apply to any Low Impact BES Cyber Systems. With the next posting, the drafting team has taken additional actions to make clear which requirements apply to Low Impact systems. These requirements have been grouped in the policy requirements of CIP-003-5.

Some commenters asked how the requirement to protect information applies to third parties with whom the entity may do business. The requirements to identify and control access to information apply to entities and also to third parties with whom the entity may share the information. If the third party is not registered as an entity, it may be difficult for NERC to enforce the standard upon the third party. The drafting team believes it is incumbent upon the Responsible Entity to ensure that BES Cyber System Information is handled in accordance with the CIP standards if that entity decides

to share the information with a third party.

Entities asked if CIP 011 R1 pertains to information concerning BES Cyber Systems or if it pertains to information stored within BES Cyber Systems. The SDT discussed this matter during drafting team meetings. CIP 011 R1 is about information concerning BES Cyber Systems regardless of where such information is stored. Both information "about" the BES Cyber System and information residing "in" the BES Cyber System would be within the scope for Requirement R1 in CIP 011.

There were multiple comments suggesting that CIP 011-5 R1 was overly burdensome. The drafting team does not agree that CIP 011-5 is overly burdensome. The components required in CIP 011-5 are that the entity have a BES Cyber System Information protection program, that BES Cyber System information can be identified, that the program include procedures for handling the information, that adherence to the program is annually assessed, action is taken to address deficiencies identified in the assessment, and that BES Cyber System information is removed from devices prior to their destruction or release for re-use. These requirements are very similar to what has been required in previous versions of CIP standards.

(2) Confusion Concerning Assessments

There were many comments regarding the initial assessment as required in CIP 011-5 Requirement R1, Part 1.3. Regarding Part 1.3., the SDT agrees with these comments concerning the initial assessment and has modified this language. The words "initially upon the effective date of the standard" have been removed from the requirement. The initial instance of periodic requirements is addressed in the revised Implementation Plan.

Multiple commenters asked if a deficiency identified in the annual assessment would become a self- report. The drafting team consulted the NERC Compliance department and was informed that the discovery of a deficiency (if it is a "possible violation") is reportable as a self-report.

(3) Measures Used to Identify BES Cyber System Information

There were many comments about measures, interpretation of measures, and changes to measures. The SDT believes that measures are meant to show the types of evidence that might be used to demonstrate implementation of the requirement. The measures are not intended to be a prescriptive list of what must be utilized to demonstrate compliance unless there is only one way of demonstrating compliance. If a requirement states that the responsible entity must have a procedure, then the measure clearly states that the responsible entity "must" have the procedure to demonstrate compliance. Most requirements to "have" a documented procedure also have a requirement to "implement" that procedure. Because there are typically many ways of demonstrating that the entity has "implemented" a procedure, then the associated measure provides examples of ways entities "may" demonstrate compliance. The measures are intended to provide guidance to the entity and are not meant to be mandatory and enforceable. The SDT

does not intend the measure to be an exhaustive list of acceptable forms of evidence, but rather a list of possible examples. However, at the urging of comments, the SDT added more specifics concerning what types of measures are acceptable. Although labeling or marking information was mentioned in the measure for Requirement R1 Part 1.1, it is not specifically required. The entity has flexibility to use some other method to identify its BES Cyber System Information.

There was some confusion about the "methods" to identify BES Cyber System Information in Requirement R1 Part 1.1. The SDT added the language "documented and implemented" to Part 1.1 to clarify that the methods selected by the entity to identify BES Cyber System information must be written and that evidence of implementation is required.

(4) Overlap in Access Control

There were several comments pointing out the overlap between access control for information, which was included in both in CIP 011-5 R1.2 and also in CIP 004-5. The Requirement for procedures relating to access control was removed from CIP 011-5 and is only referenced in CIP 004-5, thus eliminating duplication.

(5) Consistent Wording

Some commenters objected to the use of the words "protection process" when the reference in previous versions was to "protection program." Regarding the use of the phrase "protection process" in R1.3, the drafting team agrees with the comments and has modified the language so that R1 and R1.3 are in agreement and reference information "protection program."

Commenters asked that the phrase "date of the order" at the beginning of the standard be replaced with the phrase "effective date of the order." The drafting team agrees that the phrase "effective date of the order should be used for clarity, and this change was implemented in the "Effective Dates" section of the revised standard .

Multiple commenters asked that the Summary of Changes in the Rationale section include the specific previous requirements from which CIP version 5 was developed. The SDT agrees, and a corresponding change has been made to include those requirements.

QUESTION 47 – CIP-011 R2:

CIP-011-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-011-5 Table R2 – Media Reuse and Disposal*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

SUMMARY:

There were several summary topics of interest to commenters: (1) scope of the requirement, (2) footnote used in the posting, and (3) application within the same physical boundary, and (4) amount of specific direction included in the requirement and (5) alternative wording suggestions. (1) Scope of the Requirement

Multiple commenters requested changes in applicability to reduce the scope of this requirement. The SDT considered the suggested changes to applicability. However, the posted applicability is in keeping with previous versions of CIP, and the SDT believes the applicability is appropriate. Therefore, the SDT has decided not to make changes in applicability as suggested by the commenters.

Multiple entities commented that the information protection requirements were not wide spread enough and should cover all computer processing and storage assets such as in printer memory, email servers, etc. The SDT discussed this recommendation in drafting team meetings. It is not the intent of the drafting team to include email servers, printer memory, etc. in this requirement. The drafting team appreciates the comments that expand the scope of what is currently covered under CIP-011. While the drafting team agrees that such expansion of scope may increase overall security posture, the scope will not be expanded at this time.

Some commenters were confused about which requirements applied to Low Impact BES Cyber Systems. CIP-011 does not apply to Low Impact systems. The drafting team moved all requirements that apply to Low Impact systems into CIP-003-5.

(2) Footnote Used in the Posting

There were many comments objecting to the use of the footnote in the posting. The footnote was meant to clarify what the SDT meant when they referred to "media" within this standard. Footnotes are acceptable in standards provided the footnote provides clarity without including mandatory performance not addressed in the requirement itself. However, there was an overwhelming response from industry asking for removal or modification of the footnote. In response to industry's concerns, the SDT removed the footnote. The information contained in the footnote, which broadly identified

media, has been removed from Requirement R2, Part 2.1. The pertinent information has been incorporated into Part 2.1 for clarity.

Some commenters wanted the term "media" added to the NERC Glossary and they also questioned why the term "release for reuse" was used in R2 rather than the term "redeployment" While the SDT considered adding the term "media" to the Glossary, it has declined to do so since the term is only referenced within two of the CIP standards. The intent in changing from the term "redeployment" was to make clear that an entity could remove the asset from service without redeploying the asset. Requirement R2 in version 5 does not apply until the time the asset is released for re-use.

(3) Application with the Same Physical Boundary

Some comments related to reuse of the asset within the same physical control zone. The SDT agrees with the concerns expressed, and the SDT has modified the language in the requirement to address the concerns. Additional language has been added to specify that the requirement does not apply to reuse within the same BES Cyber System or associated Cyber Asset by adding the parenthetical "(except in other high impact or medium impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Asset)". Comments were also received concerning the removal of the media from the Cyber Asset to allow off-line analysis, which would be neither reuse nor disposal. The SDT believes that the current language allows for off line analysis. The requirement applies prior to the time the asset is released for re-use. If the Cyber Asset is off line for analysis but has not been released for re-use, the requirement does not apply. Guidelines supplied in the standard cover this situation. Guidelines state: "This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as that should not constitute a release for reuse."

Commenters also wanted clarity around situations where the asset was removed from the Defined Physical Boundary. The SDT agrees, and SDT added additional language to address these concerns. Chain of custody must be maintained if the BES Cyber Asset is removed from the Defined Physical Boundary prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information.

(4) Specific Direction Included in the Requirement

Some entities asked that the requirement only specify that a process is needed and the method for sanitizing the information be left to the discretion of the entity. Other commenters asked that a specific method such as National Institute of Standards and Technology (NIST) SP800-88 be set forth . The SDT considered the benefits of each approach. The method that an entity chooses to implement to meet these requirements is left to the discretion of the entity. Guidance suggests that entities review NIST 800-88 for additional implementation methods. While guidance is provided for the sake of clarity, the guidance is not mandatory and enforceable.

Some commenters asked for additional clarity concerning the measures. Additional specific examples were added to the measures to provide the desired clarity including references to chain of custody if removed from the Physical Boundary and evidence of encryption if retained within the Physical Boundary.

(5) Alternative Wording Suggestions

Some commenters asked that the phrase "take action to prevent unauthorized retrieval" be changed to "prevent unauthorized retrieval." The SDT considered the alternate language but decided not to make the suggested change. The SDT does not believe the recommended change is appropriate. An entity can certainly "take action" to prevent unauthorized retrieval and such actions can be verified as stated in the posted requirement language. Take action is the phrase currently used in the requirement. The entity may not be able to present evidence that they have "prevented" any and all unauthorized retrieval as some commenters suggested in the proposed requirement language.

Industry comments pointed out that the original posting stated "Prior to the disposal of BES Cyber Assets…" the entity must take action to prevent unauthorized retrieval of information. Industry comments suggested that the phrase should read "Prior to the disposal of BES Cyber Assets that contain BES Cyber System information…" the entity must take action to prevent unauthorized retrieval of information. The SDT agrees that the recommendation clarifies the intent and has made a corresponding change to Requirement R2, Part 2.1 and Part 2.2 language so they both state "that contain BES Cyber System Information."

In some cases, entities asked that the two parts in R2 be consolidated such as: "Prior to the physical removal of BES Cyber Asset media from a Defined Physical Boundary, the Responsible Entity shall implement a 7-pass media overwrite, degauss, or physically destroy BES Cyber Asset media. Each instance shall be documented within thirty (30) calendar days of occurrence." While the SDT agrees that information related to the Defined Physical Boundary must be included, the SDT disagrees with the proposal to reduce the two parts to one, and has left the requirement as two parts because one part deals with reuse and the other with disposal.

Commenters pointed out that the last paragraph in the Guidelines section referred to "erased" and not "cleared". The SDT agrees and has made the conforming change to "cleared."

Some commenters objected to the use of the word "destroy" in R2.2. of the posting. The SDT understands the issue pointed out by the industry. The requirement provides an alternate path. Destruction is only needed in the event that unauthorized retrieval cannot be prevented. The SDT has modified the language in the requirement to more closely resemble the recommendation made by commenters. The revised Part 2.2 now states, "…to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media."

QUESTION 48 – CIP-011 VRFs & VSLs:

Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-011-1? If not, please provide suggested improvements on the proposed VRFs and VSLs.

SUMMARY:

There were several issues of interest to commenters concerning the CIP 011 VRFs and VSLs including: (1) lack of a posted VSL and VRF Analysis, (2) VSLs - various wording changes, (3) level prescribed for VRFs, (4) level prescribed for VSLs, and (5) question concerning the purpose of guidelines.

(1) VSL and VRF Analysis

Commenters stated that "A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards…" The SDT consulting with NERC staff on this issue. The VSL and VRF analysis is under development and will be posted soon.

(2) VSLs – Various Wording Changes

Some commenters proposed removal of the first paragraph in the VSLs for R1 as they indicated the paragraph was mirrored within the subsequent paragraphs that better frame the violation. The drafting team agrees with this recommendation but has modified the VSL language rather than remove the paragraph.

Other commenters proposed that the phrase "as stated in the requirement" be added to the CIP 011-5 R1 High VSL. The SDT has modified the VSLs to add clarity about the levels of noncompliance, and they have made them more consistent with the other standards.

In response to comments, the SDT has also modified the VSLs related to R2. Previously, the VSLs referred to preventing unauthorized retrieval from "media" and flash drives would have been in scope. That was not the drafting team's intent. The VSLs now refer to preventing unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. The modification more closely reflects the drafting team's intent. The flash drives do not meet the definition of a BES Cyber Asset and would not be in scope.

Some commenters asked that the VSLs be re-written by device type. The SDT considered this proposal, but has decided not to re-write the VSLs to reflect severity levels specific to device type as this would make the VSLs overly complex.

Some comments recommended a stepped approach for CIP 011-5 R2 such as: If the process to prevent unauthorized retrieval wasn't done on 1 device that would be low 2-5 moderate, more than 5 is high. The SDT considered an approach such as the one suggested. However, the SDT believes it would be very difficult to consider the various sizes of

entities in the approach. For example, a smaller entity may have only 1 or 2 devices to which R2 applies during a year. Therefore, using the logic that was suggested, failure to implement R2 for any device would result in a low or moderate VSL for that entity. The drafting team has decided not to adopt the approach suggested. The current VSLs are in keeping with the levels of VSLs which were previously approved by FERC for the corresponding requirements in previous versions, and the SDT believes they are appropriate.

(3) Level Prescribed for VRF's

Some industry comments indicated they believed a medium VRF for Requirement 1 was too high. The SDT reviewed the VRF assignment. The VRF of medium as assigned in CIP V5 is similar to the VRF that was assigned in previous approved versions of CIP. The requirement calls for an information protection program that includes methods for the identification of BES Cyber System information, procedures for handling the information, and a periodic assessment of the entity's adherence to its program with steps to correct deficiencies identified. CIP 011-5 does not apply to Low Impact BES Cyber Systems. The SDT believes that, given the importance of protecting BES Cyber System Information at the Medium and High Impact levels, the VRF of medium is reasonable. The VRF for R2 is lower as it is an administrative requirement and a violation would not, under any anticipated circumstances, lead to cascading, instability, or uncontrolled separation.

(4) Level Prescribed for VSLs

In some cases, the commenters indicated that the VSLs for CIP 011-5 R1 are too high and a few comments indicated that "perfection" was mandated in this requirement and the VSLs. The SDT reviewed the VSLs and does not agree with such comments.

The SDT believes that the need to have an information protection program, methods to identify the information to be protected, and handling procedures for BES Cyber System information are so basic that a VSL of Severe is appropriate if those things are not in place. The assessment of adherence is only required once per year, and a VSL of High seems appropriate to the SDT for failure to comply. The drafting team does not agree that this requirement or the corresponding VSL/VRF mandate perfection. The drafting team believes that the intent of the VSLs, which align with the previously approved VSLs for the corresponding requirements are appropriate and meet the NERC and FERC guidelines.

Some commenters indicated that the VSLs for CIP 011-5 R2 were too high and that a VSL of low or moderate would be appropriate. The currently approved VSLs for the previously posted requirement (CIP 007 R7) are comparable. To be rated as "lower" the noncompliant performance would have to have only a minor impact in meeting the reliability-related intent of the requirement. To be rated as "moderate" the noncompliant performance would have to meet a significant part of the reliability-related intent of the requirement. The SDT did add a "Moderate" VSL for the situation where the entity failed to maintain chain of custody but did not change other VSLs to Moderate as failure to prevent

unauthorized access or failure to destroy the media meet the criteria for a **Moderate VSL. Purpose of Guidelines**

Commenters requested that the material in the guidelines become part of the standard and that entities be allowed to reference such guidelines during audits. The SDT considered this issue. Guidelines are meant to provide context, examples, and illustrations to facilitate understanding for both the responsible entity and the compliance enforcement authority. With results-based standards, guidelines are attached to the associated standard and are posted with the standard as.

QUESTION 49 – Implementation Plan:
Do you agree with the proposed implementation plan? If so, please explain and provide specific suggestions for improvement.

SUMMARY:

There were several summary positions provided by commenters to this question in addition to those addressing the implementation plan. For the comments addressing the implementation plan, the primary issues or concerns expressed were: (1) the applicability to low impact BES Cyber Systems, (2) the 18 month time frame being too short, (3) general confusion about the version ¾/5 transition process and (4) initial performance of periodic performance requirements.

Applicability to Low Impact BES Cyber Systems:

Several commenters noted the significant effort necessary to implement requirements applying to Low Impact BES Cyber Systems. Many commenters did not feel the requirements should apply to Low Impact BES Cyber Systems at all. Several commenters also pointed out the proposed effective date of 18 months minimum cannot be achieved for low impact BES Cyber Systems.

All requirements previously posted in CIP-004-5 through CIP-011-1 applying to Low Impact BES Cyber Systems or All Responsible Entities have moved to CIP-003-5 and apply to All Responsible Entities. We have made this change in response to multiple comments to ensure these requirements have similar wording and measures.

Applying the said requirement in CIP-003-5 to all Responsible Entities recognizes the following characteristics about threats to cyber systems: (1) the imperfect nature of categorization, (2) the scale of magnitude in multi-site attacks and (3) the exploitation of trust relationships in lesser protected cyber systems.

First, the criteria in attachment 1 of CIP-002-5 provides improvement in the consistency of identifying and categorizing BES Cyber Systems, but it cannot account for the underlying complexity of the BES and its cyber systems. The criteria primarily account for larger cyber system targets of the BES at a point in time, but the risk to the BES is dynamic and

complex.

Second, the scale of magnitude for cyber-attacks is much more expansive than natural occurring hazards or physical threats. Cyber-attacks transcend the barriers of physical presence, which means a single attack may have no geographical limitations.

Finally, a cyber-attack can exploit trust relationships with lesser protected cyber systems, for example, through inter-utility data exchange. The target cyber systems identified through the Attachment 1 criteria have requirements applied in CIP-003 through CIP-011 that help prevent such exploitation, but the necessity of trusting the lesser-protected cyber systems introduces a risk that cannot be appropriately mitigated through internal controls alone.

The drafting team is unaware of any tools to model multi-site attacks and recognizes the complexity of doing so. Also, the drafting team is not implying an approach where everything must be protected at the same level. Instead, we propose an approach where each Responsible Entity has the foundational elements of a cyber-security program, which includes having a policy, increasing organizational awareness, implementing physical and electronic boundary controls, mitigating the use of default passwords and having an incident response capability.

This approach aligns with the NIST Risk Management Framework concept where all cyber systems have protection at some level and is responsive to the FERC Order 706 directive to consider applicable features of the NIST framework (paragraph 25).

> Order 706 Paragraph 25: The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework.

18 month Effective Date and Exceptions for Low Impact BES Cyber Systems:

We have extended the effective date in this posting to 24 months minimum based on feedback from a majority of commenters that 18 months was not sufficient. The purpose of having 18 months was to provide a reasonable path for bypassing version 4 of the CIP Cyber Security Standards, but the commenter feedback overall indicated more time for implementation in version 5 was more important than bypassing version 4.

We have also extended the effective date for requirements applying to those BES Cyber Systems not categorized as High or Medium to 36 months minimum. This reflects a risk-based approach to allow entities to focus on the high and medium impact BES Cyber Systems first and is responsive to the proportionally large number of low impact BES Cyber Systems for

an entity.

General Confusion about the Version ¾/5 Transition:

Many commenters expressed confusion and had questions about the transition from version 3 to version 4 to version 5. The majority of those commenting about this subject indicated the industry should not try to bypass version 4 as a tradeoff to approve version 5 faster. There were a few commenters who encouraged bypassing version 4.

In response, we recognize the unfortunate timing between version 4 and version 5. We also recognize the timeframes in the proposed implementation plan are contingent upon yet uncertain regulatory action. The commenter feedback overall indicated more time for implementation in version 5 was more important than bypassing version 4, and there should be a concerted effort with the compliance enforcement program to provide flexibility for entities to make the transition in a reasonable manner.

We have extended the effective date in revised Implementation Plan to a 24 months minimum. While this change will likely extend the effective date of version 5 beyond the effective date of version 4, we have left the option to bypass version 4 until the FERC issues a final order on version 4. These version 5 Standards address the additional directives from FERC Order 706 which version 4 did not address, and the SDT is attempting to address these in the most timely manner possible.

Initial performance of periodic performance requirements:

Commenters suggested the initial performance of periodic performance requirements should be addressed in the implementation plan rather than requiring the initial performance on or before the effective date throughout the Standards. In response, references to the initial performance in requirements having periodic performance obligations have been moved to the implementation plan and allow a 12 month time period for initial performance for most requirements. The quarterly review in CIP-004-5 R6 Part 6.4 allows a 3 month time period for initial performance, and the CIP Senior Manager approvals in CIP-002-5 R3 and CIP-003-5 R4 must be performed on or before the Effective Date.

QUESTION 50 – Other Comments:

SUMMARY:

In addition to responses submitted to the SDT for consideration through the use of the official comment form accompanying the formal comment period that ended on January 6, 2012, the SDT received some comments that accompanied a stakeholder's ballot or through email. In most cases, those comments were aggregated and included with the comment report for the question that most closely matched the issue. Others, as here, were consolidated into one

comment report. Even though the comment form did not ask a "Question 50," for organizational purposes, we have classified this report as "Question 50."

Several commenters provided alternative approaches, citing costs, complexity, or exceeding FERC Order 706 (e.g., not prescribing "low impact" standards). The SDT has reviewed carefully the directives in Order No. 706, and the alternatives suggested would not be responsive, collectively, to FERC Order No. 706. The team has approached the remaining directives in Order No. 706 by providing an impact-based framework that accounts for various levels of risk to the BES, and this approach balances experience in implementing Versions 1 through 3. The SDT must address all FERC directives in Order No. 706, and the SDT aims at being fully responsive to all directives. In particular, the SDT has responded to FERC's directive regarding consideration of the NIST framework.

Some pointed out that TOs do not have Control Centers. The SDT has modified the standard to remove TO Control Centers. However, TOs that have agreements with TOPs to perform some of the functional obligations by their Control Centers are in scope.

Some commenters were concerned with the possibility of a discrepancy with UVLS/UFLS systems and BES Cyber Asset. The SDT believes that there is no discrepancy between the definition of a BES Cyber Asset and UVLS/UFLS systems. The definition of the BES Cyber System includes a Cyber Asset, which excludes electro-mechanical relays by definition of a Cyber Asset. The SDT believes that Cyber Assets used in UFLS systems meet the modified definition of BES Cyber Assets in the updated draft.

Some comments suggested concern with the evidence retention requirements, which the SDT has modified and made consistent. There is a difference between the retention specified in a requirement and the retention specified in evidence. For example, if a requirement requires logs for the last 90 days, the entity is only required the logs for the last 90 days. However, the entity must retain evidence that the entity has kept 90 days of log during the audit period (such as a record of the execution of the log closing script). Compliance Section: The boiler plate Compliance section has been reviewed by the appropriate NERC staff.

Guidelines and Technical Basis: The compliance requirements of standards are provided in the requirements section. The Guidelines and Technical basis section only provide contextual information to the requirements.

"On or before the effective date": The language has been removed and the initial requirements have been defined in the Implementation Plan.

Concerns with the Applicability Section 4 (confusion over application to facilities or entities): The Applicability Section has been substantively rewritten to provide more clarity and addresses the comments.

Measures. Concern with “must v. may”: (See language in Summary Document of common issues) The language in the measures for main requirements state measures that “must” be provided. The measures in the parts of the main requirement use the language “may” as these measures provide examples of quality evidence to demonstrate compliance.

Use of Definitions in Background: The SDT has made changes where appropriate in both the background and definitions.

In response to concern over a proposed defined term, “BES Reliability Operating Services” has been removed as a definition used in the standard, but has instead been moved to the Guidelines and Technical Basis section as guidance for Responsible Entities in an initial scoping for applicable BES Cyber Assets.

Other commenters raised specific issues with specific standards that are addressed in the summary responses to those questions. In particular, however, the SDT notes that it has changed VSLs to better match the requirement language, considering where appropriate to gradate the VSLs. In other cases, the VSLs remain binary, as the SDT considered guidelines for VSLs from FERC and NERC to inform their analsyis.

In response to concern over the criteria used to categorize BES Cyber Systems, and a suggestion to use Version 4’s bright line, The SDT has made significant changes to the standards to address these comments. The SDT has used Version 4 criteria with modifications to address gaps identified after version 4.

In response to concern over different entities that share facilities, and how that affects compliance with CIP-004-5’s PRA requirements, and a suggestion that attestations be allowed, the SDT expects that the Responsible Entity owning the asset is responsible for compliance to the CIP standards and will be responsible for the requirement. In a shared access situation, this Responsible Entity is required to perform the Personnel Risk Assessment according to the specified requirement. In cases where the Responsible Entity does not have access to the specific details of the personnel risk assessment, as would be the case for contractors or employees of another entity, attestations may be acceptable. The obligations of the other entity also owning other facilities may include risk assessments for their personnel under this requirement if such access is to BES Cyber Systems they own in the shared facility.

Finally, the Smart Grid Interoperability Panel (SGIP)of the Cyber Security Working Group (CSWG) provided an extensive matrix mapping the Version 5 requirements to the high-level security requirements (HLRs) in the National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628, Guidelines for Smart Grid Cyber Security. The NISTIR 7628 is available at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

This mapping identifies any gaps between CIP v5 and the NISTIR 7628 HLRs and recommendations to the CIP drafting team to consider. The complete mapping (Excel file) will be submitted to the CIP drafting separately as a reference document. Some sections of the comment form have been left blank because no gaps or recommendations were

identified.

The SDT appreciates the extensive analysis done by the SGIP/CSWG and has considered the specific comments provided by the CSWG in other sections of the comment document.

The CIP Cyber Security Standards are enforced by a strict compliance regime where non-compliance is penalized, with substantive financial penalties in many cases. This is in contrast to the SGIP NISTIR standards which are currently provided as guidelines for use in implementation of SmartGrid systems. In contrast to SmartGrid systems, the systems to which CIP standards apply range from a large range of legacy systems with very basic cyber security capabilities to newer systems implemented in the Bulk Electric System which have more extensive cyber security control capabilities. Hence, especially in the Low Impact section, the large number of devices and the extremely diverse capabilities of these devices would unduly subject entities to non-compliance if a strict base of requirements were imposed, as modeled in the NISTIR and the NIST-800-53 control catalog.

In recognition of the diversity and capabilities of covered devices, and recognizing the strict compliance model currently in force for the NERC Reliability Standards, the SDT chose an adaptation of the NIST model that would be practical and implementable in that environment. In reviewing controls, the SDT, in its early development, considered both the NIST 800-53 control catalog, as well as the DHS Catalog of Control Systems Security, which are largely based on NIST 800-53.

The mapping provided by the CSWG completes the work done by the SDT, for which the SDT expresses its thanks for the large effort required. The subteams for the various standards have separately provided responses to the CSWG's comments in the consideration of comments for each standard.

Regarding comments on the application of the NIST framework, the CIP Cyber Security Standards are enforced by a strict compliance regime where non-compliance is penalized, with substantive financial penalties in many cases. This is in contrast to the NIST standards which are currently provided as guidelines for use in implementation of systems. The SDT chose an adaptation of the NIST model that would be practical and implementable in the CIP environment. In reviewing controls, the SDT, in its early development, considered both the NIST 800-53 control catalog, as well as the DHS Catalog of Control Systems Security, which are largely based on NIST 800-53.

In response to comments on consistency of terms and language, the Drafting Team has reviewed all definitions and the language of the standard and has made appropriate corrections where applicable, including the reinstatement of terms such as Electronic Security Perimeter and Physical Security Perimeter. The SDT has made many changes to the definitions of BES Cyber Asset and BES Cyber System and has now consistently used BES Cyber System in the applicability column of requirements. Proposed defined terms are in a separate Definitions document, and will be part of the NERC Glossary of

Terms when approved.

With respect to communication links between Electronic Security Perimeters, the inclusion of these communication links in the applicability would introduce Cyber Assets that the Responsible Entity does not own, operate, or have control over, and the drafting team has therefore not removed the exclusion.

Regarding comments on CIP Exceptional Circumstances, the standards do not allow the invocation of CIP Exceptional Circumstances for all requirements, only for those that are explicitly allowed. The SDT has allowed such invocation in cases where a temporary suspension of the requirement is necessary in certain circumstances to allow for first responders.

In the standards, when the term "Cyber Assets" is used without "BES", this is intentional, as these may include Cyber Assets other than BES Cyber Assets (such as Electronic Access Control or Monitoring Systems, Physical Access Control Systems, etc.).

In the context of these standards, the term "security plan" includes any plan required by the standards (e.g. physical security plan, incident response plan, and recovery plan).

In response to comments on Procurement Policies, NERC Reliability Standards apply to users, operators, and owners of the Bulk Electric System. The policy requirements specified in R2 are necessarily limited to those in which specific NERC requirements exist and Responsible Entities are required to demonstrate implementation. Procurement policies would require an implementation that has certain requirements on entities not covered by NERC Reliability Standards (e.g. vendors and manufacturers).

Regarding resiliency, the SDT believes that the resiliency policy is covered by the policy for system recovery.

Regarding policies for third party and outsourced partners, these would be included in the responsible Entity's obligations for those systems under the scope of the CIP standards.

The SDT believes that availability is implicitly covered by the requirements of the Recovery Plan, especially related to the conditions for the activation of the recovery plan.

Regarding Personnel Risk Assessment of third party and outsourced vendors, the standard requires that the Personnel Risk Assessment be performed for any personnel, including third party and outsourced vendors for applicable systems.

The policy for Interactive Remote Access is appropriately in the Security management section as a policy requirement.

Language in contracts that requires vendors, contractors, or consultants adhere to the Responsible Entity's policies and

controls is not explicitly required, but would be a component of the Interactive Remote Access policy.

Regarding responsibility for compliance in a shared access environment, the Responsible Entity owning the asset is responsible for compliance to the CIP standard. In a shared access situation, this Responsible Entity is required to perform the Personnel Risk Assessment according to the specified requirement. In cases where the Responsible Entity does not have access to the specific details of the personnel risk assessment, as would be the case for contractors or employees of another entity, attestations may be acceptable. The obligations of the other entity also owning other facilities may include risk assessments for their personnel under this requirement if such access is to BES Cyber Systems they own in the shared facility.

"Where technically feasible" is not considered as a loophole as currently implemented. The SDT understands that there are devices which have integrated dial-up access capabilities where strict compliance is not achievable. In those cases, the Responsible Entity may use the Technical Feasibility Exception (TFE) process under the NERC Rules of Procedure, Appendix 4D, which includes compensating and mitigating measures and an implementation schedule for remediation monitored by a Compliance Enforcement Authority. TFEs are only allowed where there is triggering language in the standard.

For Dial-up access, this is included in the definition of Interactive Remote Access, and therefore included in the requirements for Interactive Remote Access.

Regarding testing of physical security controls, the SDT discussed this requirement and agreed that a reduction of the testing from once every 3 years to once every 2 years is appropriate.

Regarding the Protection of BES Cyber System Information, the SDT has required identification of, access control to and processes for handling of BES Cyber System Information and has left it to the entity on the exact way in which they can meet the performance requirements.

Project 2008-06 - Cyber Security Order 706 - V5

Working Draft (April 10, 2012) of Consideration of Issues and Directives

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 233 (Related paragraph: 25) Para 233 "The Commission continues to believe and is further persuaded by the comments that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. Moreover, we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk-Power System should be addressed in NERCs Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need	FERC Order 706	It is important to highlight differences between NERC's and NIST's approaches. At the root of these differences are divergent responsibilities and goals. NIST is providing standards and guidance for U.S. Federal Agencies in managing risks to their information and Systems in support of their unique missions. NERC, on the other hand, has the role of setting standards for managing risks to systems in support of a shared community mission to ensure the reliability of the BES. This difference is important because it enables the industry to develop better detail about the impacts that they need to avoid in order to achieve their mission. NIST does not enjoy this benefit, as they are providing standards to almost 200 different organizations, each with vastly different missions. The advantage that the NERC Standards enjoy enables a focus on a relatively small number of reliability services that need to be protected. This ultimately means that the NERC Standards can be more tailored and appropriate to the industry than a wholesale adoption of the NIST Risk Management Framework. Four key features of the NIST Risk Management Framework were incorporated into Version 5 of NERC CIP Standards: (1) ensuring that all BES Cyber Systems associated with the Bulk Power System, based on their function, receive some level of protection, (2) customizing protection to the mission of the cyber systems subject to protection, (3) a tiered approach to security controls which specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk Power System, and (4) the concept of the BES Cyber System itself. Features 2 and 3 above are tightly coupled. In the NIST Risk Management Framework, there is a concept of tailoring and scoping which allows the organization to determine which controls are applicable to their specific environment. In the NERC compliance framework, all requirements are mandatory and enforceable, and, therefore, this concept does not translate directly. As such, the customization of protections by

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
for new CIP Reliability Standards, or as part of an assessment of NERCs performance of its responsibilities as the ERO." Para 25 "The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework. "		mission is based upon the environment that the BES Cyber System supports (control center, transmission facility, generation facility) and utilizes the tiered model and the requirement applicability to provide this customization to the individual environments that together support a combined mission of Bulk Power System reliability. The NIST Security Control Catalogue in 800-53, Revision 3 was also used as a reference in addressing many of the FERC directives in Order No. 706. Additionally, the SDT added members representing federal agencies and NIST, in particular, to the drafting team during development.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 and 249 Para 258 "Likewise, the ERO should consider Northern Californias suggestion that the ERO establish a formal feedback loop to assist the industry in developing policies and procedures." Para 249 "In contrast, FirstEnergy agrees that NERC should provide guidance to entities without a wide-area view, such as a generation owner or a partial generation owner, on how to approach a risk-based assessment. Likewise, Northern California suggests that NERC establish a process for informal, case-by-case consultations with responsible entities that need assistance in complying with CIP-002-1. In addition, as part of the re-examination of CIP-002-1, Northern California encourages the incorporation of a formalized feedback loop to assist the industry in developing policies and procedures."	FERC Order 706	CIP-002-5 classifies BES Cyber Systems through impact thresholds, and does not use risk-based assessments performed by individual entities. CIP-002-5, Attachment 1's bright line criteria were developed in consideration of a wide area view, and it obviates the need for a formal feedback loop or a need for a wide area view by smaller entities.
Para 258 and 252	FERC Order 706	CIP-002-5 classifies BES Cyber Systems through impact thresholds, and does not use risk-based assessments performed by individual entities. Having risk-based approaches to

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 "As to Entergys suggestion that the ERO provide a DBT profile of potential adversaries, the ERO should consider this issue in the Reliability Standards development process." Para 252 "Entergy suggests, as an alternative approach to critical asset identification, that the ERO provide a Design-Basis Threat (DBT) a profile of the type, composition, and capabilities of an adversary that would assist the industry as a technical baseline against which to establish the proper designs, controls and processes. Entergy claims that a DBT approach would address many of the Commissions concerns regarding the risk-based methodology. For example, a DBT would focus the appropriate emphasis on the potential consequences from an outage of a critical asset. In addition, a DBT would address the Commissions concern that responsible entities will not have enough guidance in developing a risk-based methodology and not know how to identify a critical asset. Entergy contends that a DBT		applying cyber security requirements is a worthy objective and will continue to be explored, but the complexity and subjectivity it adds is beyond the scope of these revisions. CIP-002-5, Attachment 1's bright line criteria uses an impact-based approach as an alternative to DBT.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
approach would provide the industry with more certainty in implementing the CIP Reliability Standards."		
Para 272 (1 of 2) "Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, **the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset.** In doing so, the ERO should consider Juniper's comments. Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data."	FERC Order 706	This was completed by CIPC in the Version 3 CIP standards guidelines. The guidelines are entitled "Identifying Critical Assets" and "Identifying Critical Cyber Assets" and are available for download from www.nerc.com.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 272 (2 of 2) "Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset. In doing so, the ERO should consider Juniper's comments. **Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data."**	FERC Order 706	Guidance developed for CIP-002-5 addresses situational awareness and inter-utility data exchange.
Para 285 (related paragraph: 278) Para 285 "The Commission directs the ERO to consider the comment from ISA99 Team [ISA99 Team objects to the exclusion of	FERC Order 706	The exclusion of Cyber Assets based on non-routable protocols has been removed from CIP-002-5, and added as a scoping filter for requirements where: (i) the use of non-routable protocols is a mitigating factor for the vulnerabilities a requirement addresses, and (ii) implementation of routable protocols would be required to comply with the requirement (e.g. malware updates, security event monitoring, and alerting, etc.).

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience]." Para 278 "ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience. In contrast, Energy Producers notes that CIP-002-1 as proposed by NERC provides that a critical cyber asset must have either routable protocols or a dial-up connection. Energy Producers states that this is a useful, objective criterion which will assist in the unambiguous identification of such assets and therefore should be retained."		

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 296 "With regard to METC-ITC's comment, the ERO should consider in its Reliability Standards development process the suggestion that the CIP Reliability Standards require oversight by a corporate officer (or the equivalent, since some entities do not have corporate officers) rather than by a "senior manager."	FERC Order 706	The requirement that the senior manager have "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" ensures that the senior manager is of the sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for Responsible Entities; from municipal, cooperative, federal agencies, investor-owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis. In Version 5, this is addressed in the definition of CIP Senior Manager. The SDT believes the filing for Version 2 also addressed this issue.
Para 321 " SPP and ReliabilityFirst suggest modifying CIP-002-1 to allow an entity to rely upon the assessment of another entity with interest in the matter. We believe that this is a worthwhile suggestion for the ERO to pursue and the ERO should consider this proposal in the Reliability Standards development process. We note that, even without such a provision, an entity such as a small generator operator is not foreclosed from consulting with a balancing authority or other appropriate entity with a wide-area view of the transmission system."	FERC Order 706	The SDT considered this suggestion, and it believes that the change to "bright line" criteria for identifying BES Cyber Systems, along with refining the scope of certain requirements through applicability columns based on impact and connectivity characteristics, addresses this concern.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 355 (also see paragraph 356) "The Commission believes that responsible entities would benefit from additional guidance regarding the topics and processes to address in the cyber security policy required pursuant to CIP-003-1. While commenters support the need for guidance, many are concerned about providing such guidance through a modification of the Reliability Standard. We are persuaded by these commenters. Accordingly, the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address. However, we will not dictate the form of such guidance. For example, the ERO could develop a guidance document or white paper that would be referenced in the Reliability Standard. On the other hand, if it is determined in the course of the Reliability Standards development process that specific guidance is important enough to be incorporated directly into a Requirement, this option is not foreclosed. The entities remain responsible, however, to comply with the cyber security policy pursuant to CIP-003-1."		The SDT has chosen to provide guidance to Responsible Entities through the introduction of topical areas in the requirement language that must be addressed in cyber security policies in CIP-003-5, Requirement R1 and R2. Additionally, as directed, the SDT has provided guidance about these topical areas in the Guidelines and Technical Basis section of Reliability Standard CIP-003-5.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 376 "... the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards. In response to EEI, we believe that this clarification is needed because, for example, it is important that a responsible entity understand that exceptions that individually may be acceptable must not lead cumulatively to results that undermine compliance with the Requirements themselves."	FERC Order 706	The SDT removed the CIP-003-4 requirement to document exceptions to the Cyber Security Policy. • The SDT considers this a general management issue that is not within the scope of a compliance requirement. • The SDT found no reliability basis in this requirement. • Removal of this requirement provides clarity that the only exceptions to the requirements is through the defined Technical Feasibility Exception process, where specifically allowed.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 386 "The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly. In general, the Commission agrees with commenters and believes that access to protected information should cease as soon as possible but not later than 24 hours from the time of termination for cause."	FERC Order 706	To address this directive, in CIP-004-5, Requirement R7, Responsible Entities must revoke access to the electronic and physical locations where it stores BES Cyber System Information. This could include records, closets, substation control houses, records management systems, file shares, or other physical and logical areas under the Responsible Entity's control.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 397 and 398 "The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes. The Commission believes that these considerations are significant aspects of change control and configuration management that deserve express acknowledgement in the Reliability Standard. While we agree with Entergy that the NIST Security Risk Management Framework offers valuable guidance on how to deal with these matters, our concern here is that the potential problems alluded to be explicitly acknowledged. Our proposal does not speak to how these problems should be addressed. We do not believe that the changes will have burdensome consequences, but we also note that addressing any unnecessary burdens can be dealt with in the Reliability Standards development process."	FERC Order 706	Two new requirements were added to address this change CIP-010-1, Requirement R1 (Item 1.4), requires additional testing prior to a configuration change in a test environment. CIP-010-1, Requirement R2 (Item 2.1), requires monitoring of the configuration of the BES Cyber System. • The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System. • Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) prior to their implementation in the production environment to aid in identifying any accidental consequences of the change.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 412 "The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world."	FERC Order 706	The SDT addresses this through the defense in depth framework that has been designed through the full suite of revised CIP Standards. The standards address defense in depth through personnel management, systems management, and information management. The Standards are written in the perspective that the Responsible Entity is required to protect its critical systems from internal and external threat. The requirements include both preventive and detective controls. The requirements mandate appropriate vetting of personnel to minimize the risk of internal threat. They then build upon this through secure system design for internal use and remote access. These controls are further enhanced by the requirement of robust monitoring and alerting activities.
Para 433 ". . . we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard."	FERC Order 706	The SDT addressed this by determining that identification of certain core training elements would be beneficial, and the identification of those core training elements that must be provided in the training program should be role based, as required in CIP-004-5, Requirement R2.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 434 "The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets."	FERC Order 706	The SDT added this as a topic for role-specific training in CIP-004-5, Requirement R2 (Part 2.10). Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 435 "Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves."	FERC Order 706	The SDT has considered the issue and has determined that no modifications are necessary. In practice, this training is often conducted as computer-based training (CBT), and the training is aimed at an entity's own policies. As such, as long as the training material itself is adequate, which can be evaluated through the existing audit process, security trainers themselves do not need any particular or specialized training.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 446 (1 of 2) (Review the referenced Comments) " APPA/LPPC seek **clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees.** SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees. The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."	FERC Order 706	The SDT clarifies the discretion in reviewing personnel risk assessments in CIP-004-5, Requirement R4, by requiring the Responsible Entity to establish and document criteria for personnel risk assessments. The requirements in CIP-004-5 also provide additional detail about what type of records (whether criminal, work history, domicile, etc) a Responsible Entity must examine.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 446 (2 of 2) (Review the Referenced Comments) "APPA/LPPC seek clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees. **SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees.** The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."	FERC Order 706	In CIP-004-5, Requirement R4, the SDT has specified that the seven-year criminal history records check must include current residence, regardless of duration; and cover at least all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six months or more, resided, been employed, and/or attended school.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 460 "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."	FERC Order 706	In CIP-004-5, Requirement R7, the SDT has addressed this directive by requiring revocation of access concurrent with the termination or disciplinary action (Part 7.1), or by the end of the calendar day in cases of transfers or reassignments (Part 7.2). In reviewing how to modify the requirement relating to transfers or reassignments, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement (Part 7.2) from NIST 800-53, Version 3, to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers. CIP-004-5, Requirement R7 (Part 7.4) augments the requirements in Parts 7.1 and 7.2 that respond to the directive. In order to meet the immediate time frame, Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement (Part 7.4) provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
Para 464 "We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification."	FERC Order 706	The SDT notes that it addresses this issue in previous versions of the CIP standards. Version 2 added the requirement for a Personnel risk assessment prior to being granted access, and Version 3 required implementation of a visitor control program. The changes made to the requirements in Version 5 maintain and improve upon these requirements. CIP-004-5, Requirement R5 makes clear that individuals not properly authorized for unescorted physical access will not have such access. CIP-006-5 restricts access through implementation of a visitor management program.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 473 "The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entitys obligations regarding vendors with access to critical cyber assets."	FERC Order 706	CIP-002-5, Requirement R1 makes clear that asset owners are responsible for complying with the standards.
Para 476 "We direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent with the Commissions determinations above."	FERC Order 706	Guidance in CIP-002-5 states that the owning Responsible Entity is responsible for complying with the CIP Cyber Security Standards. Furthermore, the guidelines and technical basis for CIP-002-5 states that where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 496 (Related: Para 503) Para 496 "The Commission adopts the CIP NOPRs proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter" Para 503 "The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures."	FERC Order 706	The drafting team addresses this in CIP-005-5, Requirement R1 (Item 1.4). Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures, such that the cyber assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls; thus the drafting team has decided to add the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs. The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs as a second security measure for High Impact BES Cyber Systems.
Para 502 "The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process."	FERC Order 706	The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs as a second security measure for High Impact BES Cyber Systems.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 504 (Related: Para 495) Para 504 "The ERO should consider in the Reliability Standards development process Northern Indiana's and Xcel's concerns regarding the phrase "single access point at the dial up device." Para 495 "Northern Indiana and Xcel ask the Commission to clarify or direct the ERO to clarify the phrase "single access point at the dial up device" in CIP-005-1, Requirement R1.2. Xcel asks whether this refers to the initiating device, the device at the point of termination, or both. Northern Indiana would not modify CIP-005-1, but urges that any modifications to Requirement R2 should allow continued reliance on legacy systems."	FERC Order 706	The SDT has deleted the troublesome language relating to "single access point at the dial up device," and the SDT has clarified that an Electronic Security Perimeter applies to routable connectivity.CIP-005-5 also separated the requirement for dial-up connectivity, specifying in CIP-005-5, R1.4, that a Responsible Entity must perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible, on its high and medium impact BES Cyber Systems with dial-up connectivity.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 511 "The Commission adopts the CIP NOPRs proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies."	FERC Order 706	CIP-005-5, Requirement R2 has additional security requirements for remote access from the work started in the Urgent Action Revisions to CIP-005-3. One of these requirements is two-factor authentication and specific examples of two-factor authentication are provided in the referenced guideline.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 525 "The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily..." Para 628. "Requirement R6 of CIP-007-1 does not address the frequency with which log should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly..."	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of every two weeks. CIP-007-5, Requirement R4, combines CIP-005-4, Requirement R5 and CIP-007-4, Requirement R6, and addresses FERC's directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor". The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach to specify a minimum set of security event types to log and review, and allows the entity to define relevant security events in addition to the specified minimum. In addition, CIP-007-5, Requirement R4, sets up parameters for the logging and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC Order 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings.
Para 526 (1 of 2) ". . . the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments.	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of every two weeks. (Also see response to paragraph 525).

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 526 (2 of 2) "The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs."	FERC Order 706	CIP-007-5, Requirement R4, sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. (Also see response to paragraph 525).
Para 528 "The Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs."	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of every two weeks. In addition, CIP-007-5, Requirement R4, sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC Order 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings. (Also see response to paragraph 525).
Para 541 ". . . we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments."	FERC Order 706	In CIP-010-1, Requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires annual paper assessments in the intervening years.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 542 ". . . the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems."	FERC Order 706	In CIP-010-1, Requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires annual paper assessments in the intervening years.
Para 544 (1 of 2) "the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification."	FERC Order 706	The SDT addresses this paragraph in CIP-010-1, Requirement R3. • The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new Cyber Asset undergo an active vulnerability assessment. • An exception is made for specified CIP Exceptional Circumstances. • Additionally, the new requirement in CIP-010, Requirement R1 (Part 1.5) requires testing of all changes for High Impact BES Cyber Systems that deviate from the baseline configuration in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) to ensure that required security controls are not adversely affected.
Para 544 (2 of 2) ". . . we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment"	FERC Order 706	The SDT has added a requirement in CIP-010-5, R3.3, to perform an active vulnerability assessment of a new Cyber Asset in High Impact BES Cyber Systems.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 547 ". . . we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"	FERC Order 706	In CIP-010-1, Requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires annual paper assessments in the intervening years.
Para 572 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."	FERC Order 706	The SDT addressed this in CIP-006-5, Requirement R1 (Part 1.3) for High Impact BES Cyber Assets, by requiring Responsible Entities to "utilize two or more different physical access controls to collectively allow physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access."
Para 581 "The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years."	FERC Order 706	The SDT addressed this in CIP-006-5, Requirement R3 (Part 3.1) by changing the frequency to a 24-month testing cycle; after deliberation and consideration, the SDT determined that a requirement of more frequent testing (e.g., 12 months), was too often.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 609, Sentence 5 "The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a representative system one that includes the essential equipment and adequately represents the functioning of the production system. **We therefore direct the ERO to develop requirements addressing what constitutes a representative system and to modify CIP-007-1 accordingly.** The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."	FERC Order 706	The SDT has introduced the concept of a “baseline configuration” around which the change control process is based. The SDT further utilizes this “baseline configuration” to provide clarity as to what is considered a representative System as it relates to performing active vulnerability assessments in CIP-010-1.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 609, Sentence 6 "The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a representative system one that includes the essential equipment and adequately represents the functioning of the production system. We therefore direct the ERO to develop requirements addressing what constitutes a representative system and to modify CIP-007-1 accordingly. **The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."**	FERC Order 706	The SDT has provided additional guidance on testing systems in the Guidelines and Technical Basis section of CIP-010-1. Furthermore, and in addition to guidance, the requirements of CIP-010-1 R1.5 and CIP-010-1 R3.2 identify a “representative system” as a system that exists in a test environment (or production environment where tests can be performed in a manner that minimizes adverse effects) that models the baseline configuration of the BES Cyber System in a production environment. This baseline configuration concept is developed by entities in CIP-010-1 R1.1 and further contains details on what constitutes a “representative system”.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 610 ". . . we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above."	FERC Order 706	CIP-010-1, Requirements R1 (Part 1.5) requires Responsible Entities to account for any additional differences between the two systems, the SDT proposes using the words similar to those directly from FERC Order No. 706, paragraph 610: "Document the differences between the test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) and the production environment including a description of the measures used to account for any differences in operation between the test and production environments."
Para 611 "With respect to MidAmericans proposal that the differences between the testing and production environments only be reported when the production and test environments are established, the ERO should consider this matter in the Reliability Standards development process However, the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."	FERC Order 706	The SDT has added a requirement for the Responsible Entity to, "document…the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments." The SDT has included this requirement for each test performed in the representative environment. The SDT appreciates the concern brought up by MidAmerican and believes that entities should be free to use the same documentation multiple times to provide compliance with this requirement so as to minimize the documentation overhead, but also believes that it is important for entities to give consideration to the configuration of their representative system each time a test is performed in order to ensure the validity of the test results.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Paras 622 (Related: See Paras 614 and 619) "Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere."	FERC Order 706	The "acceptance of risk" language was removed in Version 2, and it has not been used in Version 5. Malicious software prevention exceptions have been placed under the TFE process since Version 2.
Para 622 (Related: See Paras 614 and 619) "The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above."	FERC Order 706	The drafting team addressed this in CIP-007-5, Requirement R3. The drafting team is taking the approach of making this requirement a competency-based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive. When remote access is used to connect to a BES Cyber Asset, an intermediate device is required in CIP-005-5, Requirement R2 (Part 2.1) and guidance is further included for the cyber security policy in CIP-003-5, Requirement R2 to maintain up-to-date anti-malware software and patch levels before initiating interactive remote access.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 628 "The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1."	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of every two weeks.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 633 "The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it."	FERC Order 706	The SDT addresses this directive in CIP-011-1, Requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from the BES Cyber Asset. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal. Additional guidance was added to the standard as further clarification: Media sanitization is generally classified into four categories: disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes. This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 635 "the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."	FERC Order 706	The SDT addresses this directive in CIP-011-1, Requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from the BES Cyber Asset. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal. Additional guidance was added to the standard as further clarification: Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes. This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 643 (1 of 2) **"The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments**, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."	FERC Order 706	In order to provide more direction on what "features, functionality, and vulnerabilities" should be addressed in a vulnerability assessment, the SDT included guidance in CIP-010-1 on active and paper vulnerability assessment. The SDT further referenced NIST SP800-115 to provide entities additional guidance on how to conduct a vulnerability assessment.
Para 643 (2 of 2) "The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, **and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."**	FERC Order 706	In CIP-010-1, R3 (Part 3.4), the SDT added a requirement for an entity planned date of completion to the remediation action plan following a vulnerability assessment.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 660 (Related, See Para 661) "The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. In developing the guidance, the ERO should consider the specific examples provided by commenters, described above. However, we direct the ERO to develop and provide guidance on the term reportable incident. The Commission is not opposed to the suggestion that the ERO create a reference document containing the reporting criteria and thresholds and requiring responsible entities to comply with the reference document in the revised Reliability Standard CIP-008-1, but will allow the ERO to determine the best method to accomplish the goal of better defining reportable incident."	FERC Order 706	In addition to defining the term Reportable Cyber Security Incident as one that compromises or disrupts the functional tasks of a Responsible Entity, CIP-008-5 also provides further guidance for determining a Reportable Cyber Security Incident in the "Guidelines and Technical Basis" section of the standard. The definition and guidance describe a reportable incident based on characteristics of impact to the BES, rather than enumerating threats and characteristics of malware. The draft Standard EOP-004-2 provides reporting criteria for Reportable Cyber Security Incidents.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 661 (Related, See Para 660) "the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."	FERC Order 706	CIP-008-5 addresses the four parts of this directive as follows: 1. Added: Reportable Cyber Security Incidents include, as a minimum, any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. In turn, a Cyber Security Incident includes a malicious act or suspicious event that compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter. 2. Retired CIP-008-4, R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in the draft EOP-004-2, Requirement 1, Part 1.3. 3. See 1 above 4. Guidance and measurements have been developed to be auditable and enforceable.
Para 673 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order 706	Cyber Security - Incident Reporting and Response Planning: Retired CIP-008-4, R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in the draft EOP-004-2, Requirement 1, Part 1.3.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 676 "The Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order 706	Cyber Security - Incident Reporting and Response Planning: Retired CIP-008-4, R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in the draft EOP-004-2, Requirement 1, Part 1.3.
Para 686 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned."	FERC Order 706	In CIP-008-5, R3 (Parts 3.3 and 3.4) the SDT includes additional specification on the update of response plan and modifies the response plan requirements to incorporate lessons learned. Maintenance of documentation of paper drills, full operational drills, and responses to actual incidents is part of the documentation required to demonstrate compliance with the security controls in CIP-008-5 and is already subject to the evidence retention requirements associated with all NERC Reliability Standards.
Para 687 (also see Footnote in Order) "In light of the comments received, the Commission clarifies that, with respect to full operational testing under CIP-008-1,	FERC Order 706	CIP 008-5 Part 2.1 is written to allow the testing requirement to be satisfied by responding to an actual Reportable Cyber Security Incident; or with a paper drill or table top exercise; or with a full operational exercise. The reporting of Cyber Security Incidents is addressed in the draft EOP-004-2, Requirement 1, Part 1.3.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
such testing need not require a responsible entity to remove any systems from service. The Commission understands that use of the term full operational exercise in this context can be confusing. We interpret the priority of the testing required by this provision to be that planned response actions are exercised in reference to a presumed or hypothetical incident contemplated by the cyber security response plan, and not necessarily that the presumed incident is performed on the live system. A responsible entity should assume a certain type of incident had occurred, and then ensure that its employees take what action would be required under the response plan, given the hypothetical incident. A responsible entity must ensure that it is properly identifying potential incidents as physical or cyber and contacting the appropriate government, law enforcement or industry authorities. CIP-008-1 should require a responsible entity to verify the list of entities that must be called pursuant to its cyber security incident response plan and that the contact numbers at those agencies are correct. The ERO should clarify this in the revised Reliability Standard and may use a term different than		The Guidelines and Technical Basis section of CIP-008-5 refer to operational exercises in the FEMA Homeland Security Exercise Evaluation Program as one of the following three types: drill, functional exercise, and full-scale exercise. It defines that “[a] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, emergency operation centers, etc.) and "boots on the ground" response (e.g., firefighters decontaminating mock victims).” The SDT believes the term operational exercise has become well understood and appropriate for both incident response and recovery exercises.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
full operational exercise."		
Para 694 "For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard"	FERC Order 706	The SDT added in CIP-009-5, R2, a requirement to implement the recovery plan.
Para 706 "The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard."	FERC Order 706	CIP-009-5, R1 (Part 1.5) requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service. The SDT captured the objective of this control, but did not explicitly use the term "forensics" due to the legal interpretations associated with the term.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 710 (Related: Para 706) "Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report."	FERC Order 706	CIP-009-5, R1 (Part 1.5) requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service. .
Para 725 "The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years."	FERC Order 706	CIP-009-5, R2 (Part 2.3) requires an operational exercise at least once every three calendar years.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 739 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."	FERC Order 706	In CIP-009-5, R1 (Part 1.4) the SDT added requirements related to restoration processes based on review of the DHS Controls, and requires verification initially after backup to ensure that the process completed successfully. In CIP-009-5, R2 (Part 2.2), requires a Responsible Entity to ensure that the information is useable and is compatible with current system configurations at High Impact BES Cyber Systems or Medium Impact BES Cyber Systems at Control Centers.
Para 748 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."	FERC Order 706	In CIP-009-5, R1 (Part 1.4) the SDT added requirements related to restoration processes based on review of the DHS Catalog of Control Systems Security: Recommendations for Standards Developers (a derivation of NIST SP800-53 for Control Systems), and requires verification initially after backup to ensure that the process completed successfully.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
	NERC Alert regarding remote access VPN vulnerabilities	Addressed in CIP-005-5 ▪ Creates basic requirements to protect critical systems from untrusted networks. ▪ Identifies protective measures that provide secure access to critical systems. ▪ Helps ensure secure practices by employees, contractors, and service vendors to minimize exploitation of vulnerabilities. ▪ Addresses questions regarding ability to audit or enforce the requirement through the design of clear measures. ▪ Significant guidance provided to address implementation options for organizations of differing sizes, capabilities, and complexity. Additional information is provided in "Guidance for Secure Interactive Remote Access" published by NERC in July 2011. Additionally, remote access is specifically required to be included in an entity's cyber security policy. Guidance is included to assist the entity in determining what this topic in the cyber security policy should address.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 13 "The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."	Order Approving Interpretation of Reliability Standard CIP-007-2 in Docket No. RD10-3-000, March 18, 2010	CIP-007-5, R1 (Part 1.2) requires Responsible Entities (for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers) to "protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media."

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2008-06 - Cyber Security Order 706 - V5

Working Draft (April 10, 2012) of Consideration of Issues and Directives ~~for Project 2008-06—Cyber Security—Order 706~~

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 233 (Related paragraph: 25) ~~We~~ Para 233 "The Commission continues to believe and is further persuaded by the comments that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. Moreover, we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk-	FERC Order 706	It is important to highlight differences between NERC's and NIST's approaches. At the root of these differences ~~is the~~are divergent responsibilities and goals. NIST is providing standards and guidance for U.S. Federal Agencies in managing risks to their information and ~~systems~~Systems in support of their unique missions. NERC, on the other hand, has the role of setting standards for managing risks to systems in support of a shared community mission to ensure the reliability of the BES. This difference is important because it enables the industry to develop better detail about the impacts that they need to avoid in order to achieve their mission. NIST does not enjoy this benefit, as they are providing standards to almost ~~two hundred~~200 different organizations, each with vastly different missions. The advantage that the NERC Standards enjoy enables a focus on a relatively small number of reliability services that need to be protected. This ultimately means that the NERC Standards can be more tailored and appropriate to the industry than a wholesale adoption of the NIST Risk Management Framework. Four key features of the NIST Risk Management Framework were incorporated into ~~version~~Version 5 of NERC CIP Standards: (1) ensuring that all BES Cyber Systems associated with the Bulk-Power System, based on their function, receive some level of protection, (2) customizing protection to the mission of the cyber systems subject to protection, (3) a tiered approach to security controls which specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk- Power

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Power System should be addressed in NERCs Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need for new CIP Reliability Standards, or as part of an assessment of NERCs performance of its responsibilities as the ERO." Para 25 "The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework. "		System, and (4) the concept of the BES Cyber System itself. Features 2 and 3 above are tightly coupled. In the NIST Risk Management Framework, there is a concept of tailoring and scoping which allows the organization to determine which controls are applicable to their specific environment. In the NERC compliance framework, all requirements are mandatory and enforceable, and, therefore, this concept does not translate directly. As such, the customization of protections by mission is based upon the environment that the BES Cyber System supports (control center, transmission facility, generation facility) and utilizes the tiered model and the requirement applicability to provide this customization to the individual environments that together support a combined mission of Bulk Power System ~~Reliability~~reliability. The NIST ~~security control catalogue~~Security Control Catalogue in 800-53~~ revision~~, Revision 3 was also used as a reference in addressing many of the FERC directives in Order No. 706. Additionally, the SDT added members representing federal agencies and NIST, in particular, to the drafting team during development.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 and 249 Para 258 "Likewise, the ERO should consider Northern Californias suggestion that the ERO establish a formal feedback loop to assist the industry in developing policies and procedures." Para 249 "In contrast, FirstEnergy agrees that NERC should provide guidance to entities without a wide-area view, such as a generation owner or a partial generation owner, on how to approach a risk-based assessment. Likewise, Northern California suggests that NERC establish a process for informal, case-by-case consultations with responsible entities that need assistance in complying with CIP-002-1. In addition, as part of the re-examination of CIP-002-1, Northern California encourages the incorporation of a formalized feedback loop to assist the industry in developing policies and procedures."	FERC Order 706	CIP-002-5 classifies BES Cyber Systems through impact thresholds, and does not use risk-based assessments performed by individual entities. CIP-002-5, Attachment 1's bright line criteria were developed in consideration of a wide area view, and it obviates the need for a formal feedback loop or a need for a wide area view by smaller entities.
Para 258 and 252 "	FERC Order 706	CIP-002-5 classifies BES Cyber Systems through impact thresholds, and does not use risk-based assessments performed by individual entities. ~~Risk~~ Having risk-based approaches

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258. "As to Entergys suggestion that the ERO provide a DBT profile of potential adversaries, the ERO should consider this issue in the Reliability Standards development process.." Para 252. "Entergy suggests, as an alternative approach to critical asset identification, that the ERO provide a Design-Basis Threat (DBT) a profile of the type, composition, and capabilities of an adversary that would assist the industry as a technical baseline against which to establish the proper designs, controls and processes. Entergy claims that a DBT approach would address many of the Commissions concerns regarding the risk-based methodology. For example, a DBT would focus the appropriate emphasis on the potential consequences from an outage of a critical asset. In addition, a DBT would address the Commissions concern that responsible entities will not have enough guidance in developing a risk-based methodology and not know how to identify a critical asset. Entergy contends that a DBT		to applying cyber security requirements is a worthy objective and will continue to be explored, but the complexity and subjectivity it adds is beyond the scope of these revisions. CIP-002-5, Attachment 1's bright line criteria uses an impact-based approach as an alternative to DBT.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	Source	Consideration of Issue or Directive
approach would provide the industry with more certainty in implementing the CIP Reliability Standards."		

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 282272 (1 of 2) The Commission directs the ERO to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets. "Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, **the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset.** In doing so, the ERO should consider Juniper's comments. Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data."	FERC Order 706	The definition of BES Cyber Asset as used in CIP-002-5 requires Responsible Entities to consider misuse of the Cyber Assets in identifying BES Cyber Systems.This was completed by CIPC in the Version 3 CIP standards guidelines. The guidelines are entitled "Identifying Critical Assets" and "Identifying Critical Cyber Assets" and are available for download from www.nerc.com.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 272 (2 of 2) "Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset. In doing so, the ERO should consider Juniper's comments. **Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data."**	FERC Order 706	Guidance developed for CIP-002-5 addresses situational awareness and inter-utility data exchange.
Para 285 (related paragraph: 278) Para 285 "The Commission directs the ERO to consider the comment from ISA99 Team [ISA99 Team objects to the exclusion of	FERC Order 706	The exclusion of Cyber Assets based on non-routable protocols has been removed from CIP-002-5, and added as a scoping filter for requirements where: (i) the use of non-routable protocols is a mitigating factor for the vulnerabilities a requirement addresses, and (ii) implementation of routable protocols would be required to comply with the requirement (e.g. malware updates, security event monitoring, and alerting, etc.).

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience~~].~~]." Para 278 "ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience. In contrast, Energy Producers notes that CIP-002-1 as proposed by NERC provides that a critical cyber asset must have either routable protocols or a dial-up connection. Energy Producers states that this is a useful, objective criterion which will assist in the unambiguous identification of such assets and therefore should be retained."		

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 296 "With regard to METC-ITC's comment, the ERO should consider in its Reliability Standards development process the suggestion that the CIP Reliability Standards require oversight by a corporate officer (or the equivalent, since some entities do not have corporate officers) rather than by a "senior manager."	FERC Order 706	The requirement that the senior manager have "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" ensures that the senior manager is of the sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for Responsible Entities; from municipal, cooperative, federal agencies, investor-owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis. In Version 5, this is addressed in the definition of CIP Senior Manager. The SDT believes the filing for Version 2 also addressed this issue.
Para 321 ~~"Para 321.~~ " SPP and ReliabilityFirst suggest modifying CIP-002-1 to allow an entity to rely upon the assessment of another entity with interest in the matter. We believe that this is a worthwhile suggestion for the ERO to pursue and the ERO should consider this proposal in the Reliability Standards development process. We note that, even without such a provision, an entity such as a small generator operator is not foreclosed from consulting with a balancing authority or other appropriate entity with a wide-area view of the transmission system."	FERC Order 706	The SDT considered this suggestion, and it believes that the change to "bright line" criteria for identifying BES Cyber Systems, along with refining the scope of certain requirements through applicability columns based on impact and connectivity characteristics, addresses this concern.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 355 (also see paragraph 356) "The Commission believes that responsible entities would benefit from additional guidance regarding the topics and processes to address in the cyber security policy required pursuant to CIP-003-1. While commenters support the need for guidance, many are concerned about providing such guidance through a modification of the Reliability Standard. We are persuaded by these commenters. Accordingly, the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address. However, we will not dictate the form of such guidance. For example, the ERO could develop a guidance document or white paper that would be referenced in the Reliability Standard. On the other hand, if it is determined in the course of the Reliability Standards development process that specific guidance is important enough to be incorporated directly into a Requirement, this option is not foreclosed. The entities remain responsible, however, to comply with the cyber security policy pursuant to CIP-003-1."		The SDT has chosen to provide guidance to Responsible Entities through the introduction of topical areas in the requirement language that must be addressed in cyber security policies in CIP-003-5, Requirement R1 and R2. Additionally, as directed, the SDT has provided guidance about these topical areas in the Guidelines and Technical Basis section of Reliability Standard CIP-003-5.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 376 " ". . . the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards. In response to EEI, we believe that this clarification is needed because, for example, it is important that a responsible entity understand that exceptions that individually may be acceptable must not lead cumulatively to results that undermine compliance with the Requirements themselves."	FERC Order 706	The SDT removed the CIP-003-4 requirement to document exceptions to the Cyber Security Policy. • The SDT considers this a general management issue that is not within the scope of a compliance requirement. • The SDT found no reliability basis in this requirement. • Removal of this requirement provides clarity that the only exceptions to the requirements is through the defined Technical Feasibility Exception process, where specifically allowed.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 386 "The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly. In general, the Commission agrees with commenters and believes that access to protected information should cease as soon as possible but not later than 24 hours from the time of termination for cause."	FERC Order 706	To address this directive, in CIP-004-5, Requirement R7, Responsible Entities ~~are required to~~must revoke access to the electronic and physical locations where it stores BES Cyber System Information. This could include records, closets, substation control houses, records management systems, file shares, or other physical and logical areas under the Responsible Entity's control.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 397 and 398 "The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes.". The Commission believes that these considerations are significant aspects of change control and configuration management that deserve express acknowledgement in the Reliability Standard. While we agree with Entergy that the NIST Security Risk Management Framework offers valuable guidance on how to deal with these matters, our concern here is that the potential problems alluded to be explicitly acknowledged. Our proposal does not speak to how these problems should be addressed. We do not believe that the changes will have burdensome consequences, but we also note that addressing any unnecessary burdens can be dealt with in the Reliability Standards development process."	FERC Order 706	Two new requirements were added to address this change CIP-010-1, Requirement R1 (~~item~~Item 1.4), requires additional testing prior to a configuration change in a test environment. CIP-010-1, Requirement R2 (~~item~~Item 2.1), requires monitoring of the configuration of the BES Cyber System. • The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System. • Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) prior to their implementation in the production environment to aid in identifying any accidental consequences of the change.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 412 "The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world."	FERC Order 706	The SDT addresses this through the defense in depth framework that has been designed through the full suite of revised CIP Standards. The standards address defense in depth through personnel management, systems management, and information management. The Standards are written in the perspective that the Responsible Entity is required to protect its critical systems from internal and external threat. The requirements include both preventive and detective controls. The requirements mandate appropriate vetting of personnel to minimize the risk of internal threat. They then build upon this through secure system design for internal use and remote access. These controls are further enhanced by the requirement of robust monitoring and alerting activities.
Para 433 " ". . . we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard."	FERC Order 706	The SDT addressed this by determining that identification of certain core training elements would be beneficial, and the identification of those core training elements that must be provided in the training program should be role based, as required in ~~in~~ CIP-004-5, Requirement R2.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 434 "The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets."	FERC Order 706	The SDT added this as a topic for role-specific training in CIP-004-5, Requirement R2 (~~item~~Part 2.10). Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 435 "Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves."	FERC Order 706	The SDT has considered the issue and has determined that no modifications are necessary. In practice, this training is often conducted as computer--based training (CBT).), and the training is aimed at an entity's own policies. As such, as long as the training material itself is adequate, which can be evaluated through the existing audit process, security trainers themselves do not need any particular or specialized -training..

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 446 (1 of 2) ~~"Para 446.~~ (Review the referenced Comments) " APPA/LPPC seek **clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees.** SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees. The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."	FERC Order 706	The SDT clarifies the discretion in reviewing personnel risk assessments in CIP-004-5, Requirement R4, by ~~establishing~~requiring the Responsible Entity to establish and document criteria for personnel risk assessments. The requirements in CIP-004-5 also provide additional detail about what type of records (whether criminal, work history, domicile, etc) a Responsible Entity must examine.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 446 (2 of 2) (Review the Referenced Comments) "APPA/LPPC seek clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees. **SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees.** The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."	FERC Order 706	In CIP-004-5, Requirement R4, the SDT has specified that the seven-year criminal history records check must include current residence, regardless of duration; and cover at least all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six months or more, resided, been employed, and/or attended school.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 460 "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."	FERC Order 706	In CIP-004-5, Requirement R7, the SDT has addressed this directive by requiring revocation of access concurrent with the termination or disciplinary action (~~item~~Part 7.1~~)~~), or by the end of the calendar day in cases of transfers or reassignments (~~item~~Part 7.2). In reviewing how to modify the requirement relating to transfers or reassignments, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement (~~item~~Part 7.2) from NIST 800-53~~ version~~, Version 3, to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers. CIP-004-5, Requirement R7 (~~item~~Part 7.4) augments the requirements in ~~items~~Parts 7.1 and 7.2 that respond to the directive. In order to meet the immediate ~~timeframe~~time frame, Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement (~~item~~Part 7.4) provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 464 "We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification~~.~~."	FERC Order 706	~~CIP-004-5, Requirement R5 (item 5.1), requires a personnel risk assessment as a condition of being granted access, with exceptions only for specific CIP Exceptional Circumstances which are outlined in the proposed glossary definition of the aforementioned term.~~ The SDT notes that it addresses this issue in previous versions of the CIP standards. Version 2 added the requirement for a Personnel risk assessment prior to being granted access, and Version 3 required implementation of a visitor control program. The changes made to the requirements in Version 5 maintain and improve upon these requirements. CIP-004-5, Requirement R5 makes clear that individuals not properly authorized for unescorted physical access will not have such access. CIP-006-5 restricts access through implementation of a visitor management program.
Para 473 "The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entitys obligations regarding vendors with access to critical cyber assets~~.~~."	FERC Order 706	CIP-002-5, Requirement R1 makes clear that asset owners are responsible for complying with the ~~Standards~~standards.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 476 "We direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent with the Commissions determinations above~~.~~."	FERC Order 706	Guidance in CIP-002-5 ~~advises~~states that the owning Responsible ~~Entities determine who~~Entity is responsible for complying with the CIP Cyber Security Standards. Furthermore, the guidelines and technical basis for CIP-002-5 states that where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.
Para 496 (Related: Para 503) Para 496 "The Commission adopts the CIP NOPRs proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter" Para 503 "The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures."	FERC Order 706	~~The proposed requirement requires a Responsible Entity to deploy methods to inspect communications and detect potential malicious communications for all External Connectivity (Intrusion Detection).~~ The drafting team addresses this in CIP-005-5, Requirement R1 (~~item~~Item 1.4). Per FERC Order No. 706, ~~p~~Paragraphs 496-503, ~~ESP's~~ESPs need two distinct security measures, such that the cyber assets do not lose all perimeter protection if one measure fails or is ~~mis-configured.~~misconfigured. The Order makes clear this is not simple redundancy of firewalls~~,~~; thus the drafting team has decided to add the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs. The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs as a second security measure for High Impact BES Cyber Systems.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 502 "The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process."	FERC Order 706	The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs as a second security measure for High Impact BES Cyber Systems.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 503504 (Related: Para 495) " Para 504 "The Commission is directing the ERO to reviseshould consider in the Reliability StandardStandards development process Northern Indiana's and Xcel's concerns regarding the phrase "single access point at the dial up device." Para 495 "Northern Indiana and Xcel ask the Commission to clarify or direct the ERO to require two or more defensive measures."clarify the phrase "single access point at the dial up device" in CIP-005-1, Requirement R1.2. Xcel asks whether this refers to the initiating device, the device at the point of termination, or both. Northern Indiana would not modify CIP-005-1, but urges that any modifications to Requirement R2 should allow continued reliance on legacy systems."	FERC Order 706	The SDT has deleted the troublesome language relating to "single access point at the dial up device," and the SDT has clarified that an Electronic Security Perimeter applies to routable connectivity.CIP-005-5 also separated the requirement for dial-up connectivity, specifying in CIP-005-5, R1.4, that a Responsible Entity must perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible, on its high and medium impact BES Cyber Systems with dial-up connectivity. The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs as a second security measure for High Impact BES Cyber Systems.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 511 "The Commission adopts the CIP NOPRs proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies.."	FERC Order 706	CIP-005-5, Requirement R2 has additional security requirements for remote access from the work started in the Urgent Action Revisions to CIP-005-3. One of these requirements is two-factor authentication and specific examples of two-factor authentication are provided in the referenced guideline.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
~~Paras 525, 526, 528, and 628~~ Para 525~~.~~ "The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily…" Para ~~526. "the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90-day increments.~~ ~~The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs."~~ ~~Para 528. "The Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs."~~	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of every two weeks. CIP-007-5, Requirement R4, combines CIP-005-4, Requirement R5 and CIP-007-4, Requirement R6, and addresses FERC's directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor". The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach ~~similar~~ to ~~NIST 800-53~~specify a minimum set of security event types to log and ~~requires~~review, and allows the entity to define ~~the~~relevant security events ~~relevant~~ in addition to the ~~system~~specified minimum. In addition, ~~this requirement~~CIP-007-5, Requirement R4, sets up parameters for the ~~monitor~~logging and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC Order 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 526 (1 of 2) "... the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments.	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of every two weeks. (Also see response to paragraph 525).
Para 526 (2 of 2) "The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs."	FERC Order 706	CIP-007-5, Requirement R4, sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. (Also see response to paragraph 525).
Para 528 "The Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs."	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of every two weeks. In addition, CIP-007-5, Requirement R4, sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC Order 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings. (Also see response to paragraph 525).

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
~~Paras 541, 542, and 547~~ Para 541 "…. we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments." ~~Para 542. "the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems."~~ ~~Para 547. "we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"~~	FERC Order 706	In CIP-010-1, Requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires annual paper assessments in the intervening years.
Para 542 "… the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems."	FERC Order 706	In CIP-010-1, Requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires annual paper assessments in the intervening years.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 544 (1 of 2) "the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification." ~~"we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment"~~	FERC Order 706	The SDT addresses this paragraph in CIP-010-1, Requirement R3. • The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new Cyber Asset undergo an active vulnerability assessment. • An exception is made for specified CIP Exceptional Circumstances. • Additionally, the new requirement in CIP-010, Requirement R1 (~~item~~Part 1.5) requires testing of all changes for High Impact BES Cyber Systems that deviate from the baseline configuration in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) to ensure that required security controls are not adversely affected.
Para 544 (2 of 2) ". . . we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment"	FERC Order 706	The SDT has added a requirement in CIP-010-5, R3.3, to perform an active vulnerability assessment of a new Cyber Asset in High Impact BES Cyber Systems.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 547 ". . . we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"	FERC Order 706	In CIP-010-1, Requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires annual paper assessments in the intervening years.
Para 572 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."	FERC Order 706	The SDT addressed this in CIP-006-5, Requirement R1 (~~item~~Part 1.3) for High Impact BES Cyber Assets, by requiring Responsible Entities to "utilize two or more different physical access controls to collectively allow physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access."

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 581 "The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years."	FERC Order 706	The SDT addressed this in CIP-006-5, Requirement R3 (~~item~~Part 3.1) by changing the frequency to a 24-~~-~~month testing cycle; after deliberation and consideration, the SDT determined that a requirement of more frequent testing (e.g., 12 months), was too often.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 609, Sentence 5 "The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a representative system one that includes the essential equipment and adequately represents the functioning of the production system. **We therefore direct the ERO to develop requirements addressing what constitutes a representative system and to modify CIP-007-1 accordingly.** The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."	FERC Order 706	The SDT has introduced the concept of a "baseline configuration" around which the change control process is based. The SDT further utilizes this "baseline configuration" to provide clarity as to what is considered a representative System as it relates to performing active vulnerability assessments in CIP-010-1.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 609, Sentence 6 "The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a representative system one that includes the essential equipment and adequately represents the functioning of the production system. We therefore direct the ERO to develop requirements addressing what constitutes a representative system and to modify CIP-007-1 accordingly. **The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."**	FERC Order 706	The SDT has provided additional guidance on testing systems in the Guidelines and Technical Basis section of CIP-010-1. Furthermore, and in addition to guidance, the requirements of CIP-010-1 R1.5 and CIP-010-1 R3.2 identify a "representative system" as a system that exists in a test environment (or production environment where tests can be performed in a manner that minimizes adverse effects) that models the baseline configuration of the BES Cyber System in a production environment. This baseline configuration concept is developed by entities in CIP-010-1 R1.1 and further contains details on what constitutes a "representative system".

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 610 "... we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above."	FERC Order 706	CIP-010-1, Requirements R1 (Part 1.5) requires Responsible Entities to account for any additional differences between the two systems, the SDT proposes using the words similar to those directly from FERC Order No. 706, paragraph 610: "Document the differences between the test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) and the production environment including a description of the measures used to account for any differences in operation between the test and production environments."

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
~~Paras 609, 610, and 611~~ ~~Para 609. "We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."~~ ~~Para 610. "we direct the ERO to revise the Reliability Standard to require each responsible entity to document~~ Para 611 "With respect to MidAmericans proposal that the differences between the testing and production environments ~~in a manner consistent with the discussion above."~~ ~~Para 611. "~~only be reported when the production and test environments are established, the ERO should consider this matter in the Reliability Standards development process However, the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."	FERC Order 706	~~CIP-010-1, Requirement R1 (item 1.4), provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.~~ • The SDT ~~proposes to require~~has added a ~~"representative system" or test system for those High Impact Control Centers to use~~requirement for the ~~purposes of testing proposed changes and performing active vulnerability assessments.~~ • ~~The SDT proposes using the defined baseline configuration of a BES Cyber System for the measuring stick as to whether a test system is truly representative of the production system.~~ • ~~To account for any additional differences between the two systems, the SDT proposes using the words directly from FERC Order 706 "Document~~ Responsible Entity to, "document…the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments."- The SDT has included this requirement for each test performed in the representative environment. The SDT appreciates the concern brought up by MidAmerican and believes that entities should be free to use the same documentation multiple times to provide compliance with this requirement so as to minimize the documentation overhead, but also believes that it is important for entities to give consideration to the configuration of their representative system each time a test is performed in order to ensure the validity of the test results.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Paras 622 (Related: See Paras 614 and 619) "Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere."	FERC Order 706	The "acceptance of risk" language was removed in Version 2, and it has not been used in Version 5. Malicious software prevention exceptions have been placed under the TFE process since Version 2.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 622 (Related: See Paras ~~620~~614 and ~~622~~619) ~~Para 620. "The Commission will not adopt Consumers' recommendation that every system in an electronic security perimeter does not need antivirus software. Critical cyber assets must be protected, regardless of the operating system being used. Consumers has not provided convincing evidence that any specific operating system is not directly vulnerable to virus attacks. Virus technology changes every day. Therefore we believe it is in the public interest to protect all cyber assets within an electronic security perimeter, regardless of the operating system being used…"~~ ~~Para 622.~~ "The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above~~.~~."	FERC Order 706	The drafting team addressed this in CIP-007-5, Requirement R3. The drafting team is taking the approach of making this requirement a competency~~-~~-based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive. ~~• The SDT rewrote the requirement as a competency based requirement that does not prescribe technology.~~ ~~• The SDT added Maintenance to cover malware on removable media.~~ ~~The drafting team also created a new requirement, CIP-007-5, Requirement R3 (item 3.4), to protect against personnel introducing malicious code when temporarily connecting to a BES Cyber Asset for Maintenance purposes.~~ When remote access is used to connect to a BES Cyber Asset, an intermediate device is required in CIP-005-5, Requirement R2 (~~item~~Part 2.1) and guidance is further included for the cyber security policy in CIP-003-5, Requirement R2 to maintain up-to-date anti-malware software and patch levels before initiating interactive remote access.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 628. "The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1."	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of every two weeks.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
~~Paras 633 and 635~~ Para 633~~.~~ "The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it." ~~Para 635. "the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."~~	FERC Order 706	The SDT addresses ~~these directives~~this directive in CIP-011-1, Requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from ~~media.~~the BES Cyber Asset. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal. Additional guidance was added to the standard as further clarification: Media sanitization is generally classified into four categories: disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes. This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 635 "the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."	FERC Order 706	The SDT addresses this directive in CIP-011-1, Requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from the BES Cyber Asset. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal. Additional guidance was added to the standard as further clarification: Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes. This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 643 (1 of 2) **"The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments**, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."	FERC Order 706	~~In CIP-010-1, R3 (item 3.4), the SDT added a requirement for an entity planned date of completion to the remediation action plan following a vulnerability assessment.~~ In order to provide more direction on what "features, functionality, and vulnerabilities" should be addressed in a vulnerability assessment, the SDT included guidance in CIP-010-1 on active and paper vulnerability assessment. The SDT further referenced NIST SP800-115 to provide entities additional guidance on how to conduct a vulnerability assessment.
Para 643 (2 of 2) "The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, **and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."**	FERC Order 706	In CIP-010-1, R3 (Part 3.4), the SDT added a requirement for an entity planned date of completion to the remediation action plan following a vulnerability assessment.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 660 (Related, See Para 661) "The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. In developing the guidance, the ERO should consider the specific examples provided by commenters, described above. However, we direct the ERO to develop and provide guidance on the term reportable incident. The Commission is not opposed to the suggestion that the ERO create a reference document containing the reporting criteria and thresholds and requiring responsible entities to comply with the reference document in the revised Reliability Standard CIP-008-1, but will allow the ERO to determine the best method to accomplish the goal of better defining reportable incident."	FERC Order 706	In addition to defining the term Reportable Cyber Security Incident as one that compromises or disrupts the functional tasks of a Responsible Entity, CIP-008-5 also provides further guidance for determining a Reportable Cyber Security Incident in the "Guidelines and Technical Basis" section of the standard. The definition and guidance describe a reportable incident based on characteristics of impact to the BES, rather than enumerating threats and characteristics of malware. The draft Standard EOP-004-2 provides reporting criteria for Reportable Cyber Security Incidents.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 661 (Related, See Para 660) "the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."	FERC Order 706	CIP-008-5 addresses the four parts of this directive as follows: 1. Added: Reportable Cyber Security Incidents include, as a minimum, any Cyber Security Incident that has compromised or disrupted ~~a BES Reliability Operating Service~~one or more reliability tasks of a functional entity. In turn, a Cyber Security Incident includes a malicious act or suspicious event that compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter. 2. Retired CIP-008-4, R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in the draft EOP-004-2, Requirement 1, Part 1.3. 3. See 1 above 4. Guidance and measurements have been developed to be auditable and enforceable.
Para 673 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order 706	Cyber Security - Incident Reporting and Response Planning: Retired CIP-008-4, R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in the draft EOP-004-2, Requirement 1, Part 1.3.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 676 "The Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order 706	Cyber Security - Incident Reporting and Response Planning: Retired CIP-008-4, R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in the draft EOP-004-2, Requirement 1, Part 1.3.
Para 686 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned~~.."~~ ."	FERC Order 706	In CIP-008-5, R3 (~~items~~Parts 3.3 and 3.4~~),~~) the SDT includes additional specification on the update of response plan and modifies the response plan requirements to incorporate lessons learned. Maintenance of documentation of paper drills, full operational drills, and responses to actual incidents is part of the documentation required to demonstrate compliance with the security controls in CIP-008-5 and is already subject to the evidence retention requirements associated with all NERC Reliability Standards.
Para 687 (also see Footnote in Order) "In light of the comments received, the Commission clarifies that, with respect to	FERC Order 706	CIP 008-5 Part 2.1 is written to allow the testing requirement to be satisfied by responding to an actual Reportable Cyber Security Incident; or with a paper drill or table top exercise; or with a full operational exercise. The reporting of Cyber Security Incidents

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
full operational testing under CIP-008-1, such testing need not require a responsible entity to remove any systems from service. The Commission understands that use of the term full operational exercise in this context can be confusing. We interpret the priority of the testing required by this provision to be that planned response actions are exercised in reference to a presumed or hypothetical incident contemplated by the cyber security response plan, and not necessarily that the presumed incident is performed on the live system. A responsible entity should assume a certain type of incident had occurred, and then ensure that its employees take what action would be required under the response plan, given the hypothetical incident. A responsible entity must ensure that it is properly identifying potential incidents as physical or cyber and contacting the appropriate government, law enforcement or industry authorities. CIP-008-1 should require a responsible entity to verify the list of entities that must be called pursuant to its cyber security incident response plan and that the contact numbers at those agencies are correct. The ERO should clarify this in the revised Reliability		is addressed in the draft EOP-004-2, Requirement 1, Part 1.3. The Guidelines and Technical Basis section of CIP-008-5 refer to operational exercises in the FEMA Homeland Security Exercise Evaluation Program as one of the following three types: drill, functional exercise, and full-scale exercise. It defines that "[a] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, emergency operation centers, etc.) and "boots on the ground" response (e.g., firefighters decontaminating mock victims)." The SDT believes the term operational exercise has become well understood and appropriate for both incident response and recovery exercises.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Standard and may use a term different than full operational exercise."		
Para 694 "For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard"	FERC Order 706	The SDT added in CIP-009-5, ~~R1~~R2, a requirement to implement the recovery plan.
Para 706 "The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard."	FERC Order 706	CIP-009-5, R1 (~~item~~Part 1.5) requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service. The SDT captured the objective of this control, but did not explicitly use the term "forensics" due to the legal interpretations associated with the term.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 710 ~~and~~(Related: Para 706) "Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report."	FERC Order 706	CIP-009-5, R1 (~~item~~Part 1.5) requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service. .
Para 725 "The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years."	FERC Order 706	CIP-009-5, R2 (~~item~~Part 2.3) requires an operational exercise at least once every three calendar years.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 739 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."	FERC Order 706	In CIP-009-5, R1 (~~item~~Part 1.4~~),~~) the SDT added requirements related to restoration processes based on review of the DHS Controls, and requires verification initially after backup to ensure that the process completed successfully. In CIP-009-5, R2 (~~item~~Part 2.2), ~~the SDT~~ requires ~~an initial~~a Responsible Entity to ensure that the information is useable and ~~once every calendar year test of the data~~is compatible with current system configurations at High Impact BES Cyber Systems or Medium Impact BES Cyber Systems at Control Centers.
Para 748 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."	FERC Order 706	In CIP-009-5, R1 (~~item~~Part 1.4~~),~~) the SDT added requirements related to restoration processes based on review of the DHS Catalog of Control Systems Security: Recommendations for Standards Developers (a derivation of NIST SP800-53 for Control Systems), and requires verification initially after backup to ensure that the process completed successfully.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
	NERC Alert regarding remote access VPN vulnerabilities	Addressed in CIP-005-5 ▪ Creates basic requirements to protect critical systems from untrusted networks. ▪ Identifies protective measures that provide secure access to critical systems. ▪ Helps ensure secure practices by employees, contractors, and service vendors to minimize exploitation of vulnerabilities. ▪ Addresses questions regarding ability to audit or enforce the requirement through the design of clear measures. ▪ Significant guidance provided to address implementation options for organizations of differing sizes, capabilities, and complexity. Additional information is provided in "Guidance for Secure Interactive Remote Access" published by NERC in July 2011. Additionally, remote access is specifically required to be included in an entity's cyber security policy. Guidance is included to assist the entity in determining what this topic in the cyber security policy should address.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 13~~.~~ "The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."	Order Approving Interpretation of Reliability Standard CIP-007-2 in Docket No. RD10-3-000, March 18, 2010	~~The SDT addressed this issue in CIP-007-5, R1, by having a requirement to disable or restrict use of physical I/O ports. The SDT changed the 'needed for normal or emergency operations' to those ports that are documented with reasons why they are necessary. In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.~~CIP-007-5, R1 (Part 1.2) requires Responsible Entities (for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers) to "protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media."

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Twelve Successive Ballot Windows Now Open for Ten Standards, Implementation Plan and Definitions: May 11, 2012 – May 21, 2012

Now Available

Ballot windows for ten CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1), a set of new and revised NERC glossary definitions, and a proposed implementation plan are open Friday, May 11 through **8 p.m. Eastern on Monday, May 21, 2012**.

CIP-002-5 requires the categorization of BES Cyber Systems according to bright-line criteria that characterize their impact on the reliable operation of the BES according to "bright-line" criteria contained in Attachment 1 – Impact Rating Criteria of the draft CIP-002-5 standard.

CIP-003-5 through CIP-009-5, CIP-010-1 and CIP-011-1 in the draft Version 5 CIP Cyber Security Standards define the cyber security requirements to be applied to the BES Cyber Systems according to the categorization performed in CIP-002-5.

CIP-003 through CIP-009 generally follow the organization of Versions 1-4 of CIP-003 through CIP-009. CIP-010-1 is a new standard that contains the Configuration Management and Vulnerability Assessment requirements previously defined across several CIP standards in Versions 1 through 4. CIP-011-1 is a new standard that defines information protection requirements previously defined across many standards in Versions 1 through 4.

In addition, the following documents have been posted to assist stakeholders in their review:

Consideration of Comments Report – Provides a summary of the modifications made to the proposed standards based on comments submitted during a formal comment period and initial ballots that ended January 6, 2012. Please note that because of the large volume of comments received, the Standards Committee has authorized the SDT to provide detailed summary responses to each question in lieu of the usual practice of providing individual responses to each comment. The SDT believes that the summary responses address all of the comments received, and encourages stakeholders to carefully review the summary consideration in conjunction with the posted redlines. The drafting team received two requests for additional clarification and these requests and the drafting team's responses have been posted.

- Mapping Document - Identifies each requirement in the already-approved Version 4 CIP standards and identifies how the requirement has been treated in the Version 5 CIP standards (which includes CIP-002-5 through CIP-009-5 and CIP-010-1 and CIP-011-1).
- Clean versions of the approved versions of CIP-002-4 through CIP-009-4 - these are posted because the extent of the changes to each of the standards makes redlines of the posted draft standards against the approved standards impractical.
- Unofficial comment forms in Word format – Note that the comment form has been divided into four separate documents to make it more manageable. These correspond to four separate electronic comment forms. The unofficial forms are provided for informal use when compiling responses – the final comments must be submitted through the electronic forms.

Instructions for Balloting

Members of the ballot pools associated with this project may log in and submit their votes for the standards, implementation plan and definitions by clicking here.

Due to modifications to NERC's balloting software, voters will no longer able to submit commits via the balloting software.

Next Steps

The drafting team will consider all comments submitted during this formal comment and ballot period to determine whether to make additional revisions to the standards.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90-days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing

and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, were approved by the Board of Trustees in January of 2011. On April 19, 2012, FERC issued an order approving Version 4 of the Cyber Security Standards (Order No. 761), and directing NERC to file Version 5 of the CIP Reliability Standards by March 31, 2013.

One of the ERO's priorities is to develop a robust set of critical infrastructure reliability standards that enable the industry to adapt to continuously changing threats and vulnerabilities by emphasizing security risk management. The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the BES, while recognizing the differing roles of each entity in the operation of the BES, the criticality and vulnerability of the cyber systems needed to support BES reliability, and the risks to which they are exposed.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Formal Comment Period Now Open: April 12, 2012 – May 21, 2012

Twelve Successive Ballot Windows Open for Ten Standards, Implementation Plan and Definitions: May 11, 2012 – May 21, 2012

Now Available

Ten CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1), a set of new and revised NERC Glossary definitions, and a proposed implementation plan have been posted for a formal 40-day comment period through **8 p.m. Eastern on Monday, May 21, 2012**.

CIP-002-5 requires the categorization of these BES Cyber Systems according to bright-line criteria that characterize their impact on the Reliability Operations Services according to "bright-line" criteria contained in Attachment 1 – Impact Categorization of BES Cyber Assets and BES Cyber Systems of the draft CIP-002-5 standard.

CIP-003-5 through CIP-009-5, CIP-010-1 and CIP-011-1 in the draft Version 5 CIP Cyber Security Standards define the cyber security requirements to be applied to the BES Cyber Systems according to the categorization performed in CIP-002-5.

CIP-003 through CIP-009 generally follow the organization of Versions 1-4 of CIP-003 through CIP-009. CIP-010-1 is a new standard that contains the Configuration Management and Vulnerability Assessment requirements previously defined across several CIP standards in Versions 1 through 4. CIP-011-1 is a new standard that defines Information Protection and Media Sanitization requirements previously defined across many standards in Versions 1 through 4.

In addition, the following documents have been posted to assist stakeholders in their review:

- Consideration of Comments Report – Provides a summary of the modifications made to the proposed standards based on comments submitted during a formal comment period and initial ballots that ended January 6, 2012. Please note that because of the large volume of comments received, the Standards Committee has authorized the SDT to provide detailed summary responses to each question in lieu of the usual practice of providing individual responses to each comment. The SDT believes that the summary responses address all of the comments received, and encourages stakeholders to carefully review the summary consideration in conjunction with the posted redlines. If after reviewing these documents, a stakeholder does not find a response to a comment that they submitted, they may request an individual response

by submitting their request following the instructions below, no later than 5 p.m. Eastern on Friday, April 27. The SDT will provide an individual response within 15 days of receipt of a request.

- Mapping Document - Identifies each requirement in the already-approved Version 4 CIP standards and identifies how the requirement has been treated in the Version 5 CIP standards (which includes CIP-002-5 through CIP-009-5 and CIP-010-1 and CIP-011-1).
- Clean versions of the approved versions of CIP-002-4 through CIP-009-4 - These are posted because the extent of the changes to each of the standards makes a redline of the posted draft standards against the approved standards impractical.
- Unofficial comment forms in Word format – Note that the comment form has been divided into four separate documents to make it more manageable. These correspond to four separate electronic comment forms. The unofficial forms are provided for informal use when compiling responses – the final comments must be submitted through the electronic forms.

Note that the Standards Committee has authorized an extended formal comment period (40 days), with a successive ballot window during the last 10 days of the comment period, in consideration of the large number of Version 5 CIP standards.

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Monday, May 21, 2012**. Please use the following comment forms to submit comments.

Comment Form A: CIP-002 and CIP-003
Comment Form B: CIP-004 through CIP-007
Comment Form C: CIP-008 through CIP-011
Comment Form D: Definitions and Implementation Plans

If you experience any difficulties in using the electronic forms, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

Comments must be submitted through the electronic comment forms (links shown above). Due to modifications to NERC's balloting software, voters will no longer able to submit commits via the balloting software.

Instructions for Requesting an Individual Response to a Comment Submitted

After reviewing the Consideration of Comments, a commenter may request additional clarity by using the "Instructions for Requesting Additional Clarity" form included with this notification. Complete the form and submit by email to sarcomm@nerc.net, **no later than 5:00 p.m. Eastern time on Friday, April 27, 2012**.

Next Steps
Twelve successive ballots (one for each of the ten standards, one for the definitions, and one for the implementation plan associated with these standards) will be conducted beginning on Friday, May 11, 2012 through 8 p.m. Eastern on Monday, May 21, 2011.

Background
In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90-days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related issues of FERC Order No. 706.

One of the ERO's priorities is to develop a robust set of critical infrastructure reliability standards that enable the industry to adapt to continuously changing threats and vulnerabilities by emphasizing security risk management. NERC staff and industry are working together to accomplish this goal in 2012.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Project 2008-06 Cyber Security Order 706

Request for Additional Clarity in Response to Comment Submitted

In November 2011, the Project 2008-06 CSO 706 SDT posted ten CIP Version 5 CIP standards, a set of new and revised definitions, and the associated implementation plan for a parallel formal comment period and initial ballots of each standard, the definitions as a group, and the implementation plan. The formal comment period and ballots closed on January 6, 2012.

The SDT received an extremely large volume of comments in response to this posting, and in March 2012 the Standards Committee waived the requirement that the Cyber 706 SDT provide individual responses and directed the team to focus on providing detailed summary responses to each question subject to the following conditions:

- Each summary response should address the comments submitted, in aggregate, such that the summary response clearly addresses all of the comments submitted.
- As part of the Consideration of Comments report, add a paragraph that clarifies that the drafting team developed summary responses rather than individual responses with the approval of the Standards Committee and *invite any stakeholder who believes his or her comment was not adequately addressed to submit a written request for additional clarity within 15 calendar days to the team's advisor with a commitment that the team will provide a written response within 15 calendar days.*

Accordingly, the SDT requests that stakeholders that submitted comments carefully review the summary Consideration of Comments, along with the redline versions of each standard, the definitions, and implementation plan. If, after reviewing the team's summary consideration, you believe that additional clarification is needed in response to a comment that you submitted, please submit your request for clarification according to the following instructions.

Requests for additional clarification are limited to issues identified in comments that were formally submitted during the comment period that ended January 6, 2012. The drafting team is not required to address any new issues through this form; those should be submitted as comments during the comment period that is open through Monday, May 21, 2012.

Instructions for Requesting Additional Clarity

Complete the form below and submit by email to sarcomm@nerc.net, **no later than 5:00 p.m. Eastern time on Friday, April 27, 2012**. All requests will be posted on the Project 2008-06 project page as soon as practical but no later than two business days after receipt. The SDT's response to each request will be posted and sent to the requester no later than 15 calendar days after the request is received.

Name of individual submitting original comment	Organization	Date of this request
Original Comment (or portion of comment) for which additional response clarification is requested		
Specific question or request for clarification explaining stakeholder belief that original comment was not adequately addressed (please be specific to assist the drafting team in being responsive)		
SDT Response:		

Cyber Security (Project 2008-06)

Status	Date	Submitter	Organization
Request for Additional Clarity			
Request	April 13, 2012	Jeffrey L. Millennor	Bonneville Power Administration NNT
Request with Response	April 30, 2012		
Request	April 24, 2012	Joanna Luong-Tran	TransAlta Centralia Generation
Request with Response	May 8, 2012		

To download a file click on the file using your right mouse button, then save it to your computer in a directory of your choice.
Documents in the PDF format require use of the Adobe Reader® software. Free Adobe Reader® software allows anyone view and print Adobe Portable Document Format (PDF) files.

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Advance Notice: Formal Comment Period Will Open for Ten Standards, Implementation Plan and Definitions: Thursday, April 12, 2012

The Project 2008-06 Standards Drafting Team has carefully considered stakeholder input from a parallel formal comment period and initial ballots that ended in January. In response to stakeholder feedback, the team has revised and submitted clean and redline versions of ten standards (CIP-002-5 through CIP-011-1), the associated definitions and implementation plan, and numerous supporting documents for posting for a parallel formal comment period and successive ballot. The comment period is currently scheduled to begin on Thursday, April 12, 2012 and end at 8 p.m. Eastern on Monday, May 21, 2012.

To provide stakeholders with as much time as possible to review the changes to the documents since the last posting, the comment period has been extended to 40 days and this advance notice is being provided. Clean and redline versions of the standards and the unofficial (Word version) comment forms have been posted on the project page already.

Please note that this advance notice is being provided as a courtesy; the electronic comment form will not be available until the formal comment period opens on Thursday, April 12 and because some documents are still being reviewed, not all documents are posted yet and it is possible that changes may still be made to posted documents. If it is necessary to make changes to any of the documents that are posted for this advance review, we will indicate specifically which documents have changed in the formal announcement when the comment period opens as well as on the project page.

Link to Project Page

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in

September of 2009 with additional directives to be addressed within 90 days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related issues of FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement - Updated

Project 2008-06 Cyber Security Order 706 (CIP Version 5)

Successive Ballot Results

Now Available

Twelve initial ballot windows for the following ten CIP standards, one ballot for the associated implementation plan, and one ballot for a set of new and revised NERC Glossary definitions, closed on Monday, May 21, 2012. The drafting team thanks stakeholders for the careful consideration of such a large volume of documents, and for the substantive and constructive feedback received.

Voting statistics for each ballot are listed below, and the Ballot Results webpage provides a link to the detailed results.

Ballot	Results
CIP-002-5 Cyber Security — BES Cyber System Identification	Quorum: 86.63% Approval: 37.37%
CIP-003-5 Cyber Security — Security Management Controls	Quorum: 87.45% Approval: 60.55%
CIP-004-5 Cyber Security — Personnel and Training	Quorum: 87.40% Approval: 38.81%
CIP-005-5 Cyber Security — Electronic Security Perimeter(s)	Quorum: 86.98% Approval: 55.08%
CIP-006-5 Cyber Security — Physical Security	Quorum: 87.22% Approval: 38.50%
CIP-007-5 Cyber Security — Systems Security Management	Quorum: 87.01% Approval: 45.78%
CIP-008-5 Cyber Security — Incident Reporting and Response Planning	Quorum: 86.19% Approval: 67.19%
CIP-009-5 Cyber Security — Recovery Plans for BES Cyber Assets and Systems	Quorum: 87.01% Approval: 60.19%
CIP-010-1 Cyber Security — Configuration Change Management	Quorum: 86.39% Approval: 47.92%
CIP-011-1 Cyber Security — Information Protection	Quorum: 86.39% Approval: 58.23%
CIP V5 Implementation Plan	Quorum: 85.12% Approval: 66.23%
CIP V5 Definitions	Quorum: 84.09% Approval: 47.88%

Next Steps
The drafting team will consider all comments submitted, and based on the comments will determine whether to make additional changes to each of the standards, the implementation plan, and the definitions. When the drafting team has completed its revisions, the team will submit the revised documents, along with its consideration of comments received for a quality review of the standards prior to the next posting.

Background
In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

Version 5 of the NERC CIP Cyber Security Standards is intended to address all remaining standards related issues of FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed. Additional information about the project is available on the project webpage.

Standards Development Process
The Standards Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 CIP-002-5 CSO706 V5
Ballot Period:	5/11/2012 - 5/21/2012
Ballot Type:	Initial
Total # Votes:	421
Total Ballot Pool:	486
Quorum:	**86.63 % The Quorum has been reached**
Weighted Segment Vote:	37.37 %
Ballot Results:	**The drafting team will consider comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	28	0.286	70	0.714	10	17
2 - Segment 2.	11	1	5	0.5	5	0.5	1	0
3 - Segment 3.	120	1	29	0.296	69	0.704	10	12
4 - Segment 4.	38	1	8	0.229	27	0.771	1	2
5 - Segment 5.	103	1	28	0.35	52	0.65	10	13
6 - Segment 6.	60	1	12	0.279	31	0.721	5	12
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	11	0.7	3	0.3	4	0.4	1	3
9 - Segment 9.	9	0.2	1	0.1	1	0.1	2	5
10 - Segment 10.	9	0.7	5	0.5	2	0.2	1	1
Totals	**486**	**7.6**	**119**	**2.84**	**261**	**4.76**	**41**	**65**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	

1	Balancing Authority of Northern California	Kevin Smith	Negative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Negative	
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi		
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland		
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Negative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Negative	
1	Dominion Virginia Power	Michael S Crowley	Negative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Negative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	
1	Idaho Power Company	Ronald D. Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Negative	
1	Kansas City Power & Light Co.	Michael Gammon	Negative	
1	Keys Energy Services	Stanley T Rzad	Negative	
1	Lakeland Electric	Larry E Watt	Negative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Negative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	
1	National Grid	Saurabh Saksena	Negative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Negative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	
1	Oncor Electric Delivery	Brenda Pulis	Negative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Abstain	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Abstain	
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Negative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	
1	Sacramento Municipal Utility District	Tim Kelley	Negative	
1	Salmon River Electric Cooperative	Kathryn Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Negative	
1	Sierra Pacific Power Co.	Rich Salgo	Negative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	
1	Trans Bay Cable LLC	Steven Powell	Negative	
1	Transmission Agency of Northern California	Bryan Griess	Abstain	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Negative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	
2	Midwest ISO, Inc.	Marie Knox	Negative	
2	New Brunswick System Operator	Alden Briggs	Negative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	

3	Alabama Power Company	Richard J. Mandes	Negative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	
3	Central Electric Power Cooperative	Ralph J Schulte	Negative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Abstain	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Negative	
3	City of Redding	Bill Hughes	Abstain	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Negative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Negative	
3	ComEd	Bruce Krawczyk	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	
3	Consumers Energy	Richard Blumenstock	Negative	
3	Consumers Power Inc.	Roman Gillen	Negative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	
3	Cowlitz County PUD	Russell A Noble	Negative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Negative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Negative	
3	Gulf Power Company	Paul C Caldwell	Negative	
3	Hydro One Networks, Inc.	David Kiguel	Negative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill		
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	
3	Lincoln Electric System	Jason Fortik		
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	
3	Madison Gas and Electric Co.	Darl Shimko	Negative	

3	Manitoba Hydro	Greg C. Parent	Negative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Negative	
3	Modesto Irrigation District	Jack W Savage		
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	Marilyn Brown	Negative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Negative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Negative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Negative	
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Negative	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	South Mississippi Electric Power Association	Gary Hutson		
3	Southern California Edison Co.	David B Coher	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe	Negative	
3	Tampa Electric Co.	Ronald L. Donahey	Negative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	
3	Westar Energy	Bo Jones	Negative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Negative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Abstain	
4	City Utilities of Springfield, Missouri	John Allen	Negative	
4	Consumers Energy	David Frank Ronk	Negative	
4	Cowlitz County PUD	Rick Syring	Negative	
4	Detroit Edison Company	Daniel Herring	Affirmative	

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	
4	LaGen	Richard Comeaux	Negative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Negative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Negative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
4	WPPI Energy	Patrick Connors	Negative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Negative	
5	Avista Corp.	Edward F. Groce	Negative	
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore	Abstain	
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Abstain	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Negative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	
5	Cowlitz County PUD	Bob Essex	Negative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Negative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	
5	Duke Energy	Dale Q Goodwine	Negative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	

5	Exelon Nuclear	Michael Korchynsky	Abstain	
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Negative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Negative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	
5	Madison Gas and Electric Co.	Steven Schultz	Negative	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Negative	
5	New York Power Authority	Gerald Mannarino	Negative	
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Negative	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Negative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Negative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Negative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Negative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	
5	Westar Energy	Bryan Taggart		
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
5	WPPI Energy	Steven Leovy	Negative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall		
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Negative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Abstain	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Negative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda L Powell	Negative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	
6	Duke Energy Carolina	Walter Yeager	Negative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Negative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Negative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Negative	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Negative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Negative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Negative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Edward C Stein	Affirmative	
8		James A Maenner	Abstain	
8		Roger C Zaklukiewicz	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		

8	JDRJC Associates	Jim Cyrulewski		
8	Network & Security Technologies	Nicholas Lauriat	Negative	
8	Pacific Northwest Generating Cooperative	Margaret Ryan	Negative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Negative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 CIP-003-5 CSO706 V5
Ballot Period:	5/11/2012 - 5/21/2012
Ballot Type:	Initial
Total # Votes:	425
Total Ballot Pool:	486
Quorum:	**87.45 % The Quorum has been reached**
Weighted Segment Vote:	60.55 %
Ballot Results:	**The drafting team will consider comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	59	0.584	42	0.416	10	14
2 - Segment 2.	11	1	7	0.7	3	0.3	1	0
3 - Segment 3.	120	1	56	0.571	42	0.429	11	11
4 - Segment 4.	38	1	17	0.486	18	0.514	1	2
5 - Segment 5.	103	1	49	0.613	31	0.388	10	13
6 - Segment 6.	60	1	23	0.548	19	0.452	6	12
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	11	0.7	4	0.4	3	0.3	1	3
9 - Segment 9.	9	0.2	1	0.1	1	0.1	2	5
10 - Segment 10.	9	0.7	6	0.6	1	0.1	1	1
Totals	**486**	**7.6**	**222**	**4.602**	**160**	**2.999**	**43**	**61**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	
1	American Electric Power	Paul B. Johnson	Negative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Negative	
1	Dominion Virginia Power	Michael S Crowley	Negative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Negative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Negative	
1	Keys Energy Services	Stanley T Rzad	Negative	
1	Lakeland Electric	Larry E Watt	Negative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Arnold J. Schuff	Affirmative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Affirmative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Negative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	
1	Oncor Electric Delivery	Brenda Pulis	Negative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Abstain	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Abstain	
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Negative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Abstain	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Negative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Negative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	

3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Abstain	
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	
3	City of Lodi, California	Elizabeth Kirkley	Abstain	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Negative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Affirmative	
3	Consumers Energy	Richard Blumenstock	Negative	
3	Consumers Power Inc.	Roman Gillen	Negative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Negative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill		
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	
3	Lincoln Electric System	Jason Fortik		
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	Marilyn Brown	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Negative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Negative	
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Negative	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	South Mississippi Electric Power Association	Gary Hutson		
3	Southern California Edison Co.	David B Coher	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Negative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Negative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Negative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	

4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	
4	LaGen	Richard Comeaux	Negative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
4	WPPI Energy	Patrick Connors	Negative	
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	
5	Avista Corp.	Edward F. Groce	Negative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore	Abstain	
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	

5	Exelon Nuclear	Michael Korchynsky	Abstain	
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Negative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Negative	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart		
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
5	WPPI Energy	Steven Leovy	Negative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall		
6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda L Powell	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Negative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Negative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Negative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Negative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner	Abstain	
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		

8	JDRJC Associates	Jim Cyrulewski		
8	Network & Security Technologies	Nicholas Lauriat	Negative	
8	Pacific Northwest Generating Cooperative	Margaret Ryan	Negative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results	
Ballot Name:	Project 2008-06 CIP-004-5 CSO706 V5
Ballot Period:	5/11/2012 - 5/21/2012
Ballot Type:	Initial
Total # Votes:	423
Total Ballot Pool:	484
Quorum:	**87.40 % The Quorum has been reached**
Weighted Segment Vote:	38.81 %
Ballot Results:	**The drafting team will consider comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	37	0.37	63	0.63	11	14
2 - Segment 2.	10	0.9	0	0	9	0.9	1	0
3 - Segment 3.	120	1	50	0.521	46	0.479	13	11
4 - Segment 4.	38	1	15	0.469	17	0.531	4	2
5 - Segment 5.	103	1	32	0.416	45	0.584	13	13
6 - Segment 6.	60	1	15	0.357	27	0.643	6	12
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	2	0.2	4	0.4	1	3
9 - Segment 9.	9	0.2	1	0.1	1	0.1	2	5
10 - Segment 10.	9	0.6	4	0.4	2	0.2	2	1
Totals	**484**	**7.3**	**156**	**2.833**	**214**	**4.467**	**53**	**61**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	
1	American Electric Power	Paul B. Johnson	Negative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Negative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Affirmative	
1	Dominion Virginia Power	Michael S Crowley	Negative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Negative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	
1	Idaho Power Company	Ronald D. Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Negative	
1	Keys Energy Services	Stanley T Rzad	Negative	
1	Lakeland Electric	Larry E Watt	Negative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Negative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Negative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	
1	Oncor Electric Delivery	Brenda Pulis	Negative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Abstain	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Abstain	
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Negative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Abstain	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Negative	
1	South Mississippi Electric Power Association	Rodney A. Wilson		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Abstain	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Negative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	
2	California ISO	Rich Vine	Negative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Negative	
2	Independent Electricity System Operator	Barbara Constantinescu	Negative	
2	Midwest ISO, Inc.	Marie Knox	Negative	
2	New Brunswick System Operator	Alden Briggs	Negative	
2	New York Independent System Operator	Gregory Campoli	Negative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Negative	
3	AEP	Michael E Deloach	Negative	
3	Alabama Power Company	Richard J. Mandes	Negative	

3	Alameda Municipal Power	Douglas Draeger	Abstain	
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Negative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	
3	City of Lodi, California	Elizabeth Kirkley	Abstain	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	
3	Consumers Energy	Richard Blumenstock	Negative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Abstain	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	
3	Flathead Electric Cooperative	John M Goroski	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Negative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Negative	
3	Gulf Power Company	Paul C Caldwell	Negative	
3	Hydro One Networks, Inc.	David Kiguel	Negative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill		
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik		
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Negative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	
3	Manitoba Hydro	Greg C. Parent	Negative	

3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Negative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	Marilyn Brown	Negative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Negative	
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	South Mississippi Electric Power Association	Gary Hutson		
3	Southern California Edison Co.	David B Coher	Negative	
3	Tacoma Public Utilities	Travis Metcalfe	Negative	
3	Tampa Electric Co.	Ronald L. Donahey	Negative	
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Negative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Negative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Negative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	
4	Consumers Energy	David Frank Ronk	Negative	
4	Cowlitz County PUD	Rick Syring	Abstain	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	

4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	
4	LaGen	Richard Comeaux	Negative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
4	WPPI Energy	Patrick Connors	Negative	
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	
5	Avista Corp.	Edward F. Groce	Negative	
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore	Abstain	
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	
5	Cowlitz County PUD	Bob Essex	Abstain	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Negative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	
5	Duke Energy	Dale Q Goodwine	Negative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky	Abstain	

5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Negative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Negative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Negative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Negative	
5	New York Power Authority	Gerald Mannarino	Negative	
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Negative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	
5	Southern Company Generation	William D Shultz	Negative	
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart		
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
5	WPPI Energy	Steven Leovy	Negative	
5	Xcel Energy, Inc.	Liam Noailles	Negative	
6	ACES Power Marketing	Jason L Marshall		

6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda L Powell	Negative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	
6	Duke Energy Carolina	Walter Yeager	Negative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Negative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Negative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Negative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Negative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	
6	South Mississippi Electric Power Association	Joel Rogers		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Roger C Zaklukiewicz	Negative	
8		Edward C Stein	Affirmative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski		

8	Network & Security Technologies	Nicholas Lauriat	Negative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson	Negative	
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results	
Ballot Name:	Project 2008-06 CIP-005-5 CSO706 V5
Ballot Period:	5/11/2012 - 5/21/2012
Ballot Type:	Initial
Total # Votes:	421
Total Ballot Pool:	484
Quorum:	**86.98 % The Quorum has been reached**
Weighted Segment Vote:	55.08 %
Ballot Results:	**The drafting team will consider comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	53	0.53	47	0.47	11	14
2 - Segment 2.	10	0.9	5	0.5	4	0.4	1	0
3 - Segment 3.	120	1	64	0.667	32	0.333	13	11
4 - Segment 4.	38	1	16	0.5	16	0.5	4	2
5 - Segment 5.	103	1	41	0.547	34	0.453	13	15
6 - Segment 6.	60	1	20	0.476	22	0.524	6	12
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	4	0.4	2	0.2	1	3
9 - Segment 9.	9	0.2	1	0.1	1	0.1	2	5
10 - Segment 10.	9	0.6	3	0.3	3	0.3	2	1
Totals	**484**	**7.3**	**207**	**4.02**	**161**	**3.28**	**53**	**63**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	
1	American Electric Power	Paul B. Johnson	Negative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Affirmative	
1	Dominion Virginia Power	Michael S Crowley	Negative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Negative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	
1	Idaho Power Company	Ronald D. Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Negative	
1	Lakeland Electric	Larry E Watt	Negative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Affirmative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Affirmative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	
1	Oncor Electric Delivery	Brenda Pulis	Negative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Abstain	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Abstain	
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Negative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Abstain	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Negative	
1	South Mississippi Electric Power Association	Rodney A. Wilson		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Abstain	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Negative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Negative	
2	New York Independent System Operator	Gregory Campoli	Negative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	

3	Alameda Municipal Power	Douglas Draeger	Abstain	
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	
3	City of Lodi, California	Elizabeth Kirkley	Abstain	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Affirmative	
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Abstain	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	
3	Flathead Electric Cooperative	John M Goroski	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Negative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Negative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill		
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik		
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	
3	Manitoba Hydro	Greg C. Parent	Affirmative	

3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	Marilyn Brown	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Negative	
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Negative	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	South Mississippi Electric Power Association	Gary Hutson		
3	Southern California Edison Co.	David B Coher	Negative	
3	Tacoma Public Utilities	Travis Metcalfe	Negative	
3	Tampa Electric Co.	Ronald L. Donahey	Negative	
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Negative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Negative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Negative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Abstain	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	

4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	
4	LaGen	Richard Comeaux	Negative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
4	WPPI Energy	Patrick Connors	Negative	
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	
5	Avista Corp.	Edward F. Groce	Negative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore	Abstain	
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Abstain	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Negative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky	Abstain	

5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Negative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Negative	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel		
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Negative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart		
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
5	WPPI Energy	Steven Leovy	Negative	
5	Xcel Energy, Inc.	Liam Noailles	Negative	
6	ACES Power Marketing	Jason L Marshall		

6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda L Powell	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Negative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Negative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Negative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Negative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	
6	South Mississippi Electric Power Association	Joel Rogers		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski		

8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Negative	
10	New York State Reliability Council	Alan Adamson	Negative	
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 CIP-006-5 CSO706 V5
Ballot Period:	5/11/2012 - 5/21/2012
Ballot Type:	Initial
Total # Votes:	423
Total Ballot Pool:	485
Quorum:	**87.22 % The Quorum has been reached**
Weighted Segment Vote:	38.50 %
Ballot Results:	**The drafting team will consider comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	39	0.386	62	0.614	10	14
2 - Segment 2.	11	1	3	0.3	7	0.7	1	0
3 - Segment 3.	120	1	37	0.381	60	0.619	12	11
4 - Segment 4.	38	1	10	0.313	22	0.688	4	2
5 - Segment 5.	103	1	30	0.39	47	0.61	12	14
6 - Segment 6.	60	1	12	0.279	31	0.721	5	12
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	3	0.3	3	0.3	1	3
9 - Segment 9.	9	0.2	1	0.1	1	0.1	2	5
10 - Segment 10.	9	0.6	4	0.4	2	0.2	2	1
Totals	**485**	**7.4**	**139**	**2.849**	**235**	**4.552**	**49**	**62**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	
1	American Electric Power	Paul B. Johnson	Negative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Negative	
1	Avista Corp.	Scott J Kinney	Negative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Negative	
1	Dominion Virginia Power	Michael S Crowley	Negative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Negative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Negative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	
1	Idaho Power Company	Ronald D. Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Negative	
1	Keys Energy Services	Stanley T Rzad	Negative	
1	Lakeland Electric	Larry E Watt	Negative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Negative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Negative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	
1	Oncor Electric Delivery	Brenda Pulis	Negative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Abstain	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Negative	
1	Potomac Electric Power Co.	David Thorne	Abstain	
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Negative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Abstain	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Negative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Negative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	
2	California ISO	Rich Vine	Negative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Negative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Negative	
2	New York Independent System Operator	Gregory Campoli	Negative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	

3	Alabama Power Company	Richard J. Mandes	Negative	
3	Alameda Municipal Power	Douglas Draeger	Abstain	
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Negative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	
3	City of Lodi, California	Elizabeth Kirkley	Abstain	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Negative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Negative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	
3	Cowlitz County PUD	Russell A Noble	Abstain	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Negative	
3	Georgia Systems Operations Corporation	William N. Phinney	Negative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Negative	
3	Hydro One Networks, Inc.	David Kiguel	Negative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill		
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	
3	Lincoln Electric System	Jason Fortik		
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Negative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Negative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	Marilyn Brown	Negative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Negative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Negative	
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Negative	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	South Mississippi Electric Power Association	Gary Hutson		
3	Southern California Edison Co.	David B Coher	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe	Negative	
3	Tampa Electric Co.	Ronald L. Donahey	Negative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	
3	Westar Energy	Bo Jones	Negative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Negative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Abstain	
4	Detroit Edison Company	Daniel Herring	Affirmative	

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Negative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	
4	LaGen	Richard Comeaux	Negative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
4	WPPI Energy	Patrick Connors	Negative	
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	
5	Avista Corp.	Edward F. Groce	Negative	
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore	Abstain	
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Abstain	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	
5	Duke Energy	Dale Q Goodwine	Negative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	

5	Exelon Nuclear	Michael Korchynsky	Abstain	
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Negative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Negative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	
5	MEAG Power	Steven Grego	Negative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Negative	
5	New York Power Authority	Gerald Mannarino	Negative	
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel		
5	Portland General Electric Co.	Gary L Tingley	Negative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Negative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	
5	Westar Energy	Bryan Taggart		
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
5	WPPI Energy	Steven Leovy	Negative	
5	Xcel Energy, Inc.	Liam Noailles	Negative	

6	ACES Power Marketing	Jason L Marshall		
6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda L Powell	Negative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	
6	Duke Energy Carolina	Walter Yeager	Negative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Negative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Negative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Negative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	John Jamieson	Negative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Negative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz	Negative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		

8	JDRJC Associates	Jim Cyrulewski		
8	Network & Security Technologies	Nicholas Lauriat	Negative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson	Negative	
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 CIP-007-5 CSO706 V5
Ballot Period:	5/11/2012 - 5/21/2012
Ballot Type:	Initial
Total # Votes:	422
Total Ballot Pool:	485
Quorum:	**87.01 % The Quorum has been reached**
Weighted Segment Vote:	45.78 %
Ballot Results:	**The drafting team will consider comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	49	0.485	52	0.515	10	14
2 - Segment 2.	11	1	4	0.4	6	0.6	1	0
3 - Segment 3.	120	1	54	0.568	41	0.432	14	11
4 - Segment 4.	38	1	14	0.452	17	0.548	5	2
5 - Segment 5.	103	1	33	0.434	43	0.566	12	15
6 - Segment 6.	60	1	15	0.349	28	0.651	5	12
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	3	0.3	3	0.3	1	3
9 - Segment 9.	9	0.2	1	0.1	1	0.1	2	5
10 - Segment 10.	9	0.6	3	0.3	3	0.3	2	1
Totals	**485**	**7.4**	**176**	**3.388**	**194**	**4.012**	**52**	**63**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	
1	American Electric Power	Paul B. Johnson	Negative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Affirmative	
1	Dominion Virginia Power	Michael S Crowley	Negative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Negative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	
1	Idaho Power Company	Ronald D. Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Negative	
1	Keys Energy Services	Stanley T Rzad	Negative	
1	Lakeland Electric	Larry E Watt	Negative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Negative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Negative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Affirmative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	
1	Oncor Electric Delivery	Brenda Pulis	Negative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Abstain	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Abstain	
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Negative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Abstain	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Negative	
1	South Mississippi Electric Power Association	Rodney A. Wilson		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Affirmative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Negative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Negative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Negative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Negative	
2	New York Independent System Operator	Gregory Campoli	Negative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	

3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Abstain	
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	
3	City of Lodi, California	Elizabeth Kirkley	Abstain	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Affirmative	
3	Consumers Energy	Richard Blumenstock	Negative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Abstain	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	
3	Flathead Electric Cooperative	John M Goroski	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Abstain	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Negative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Negative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill		
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik		
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Negative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	Marilyn Brown	Negative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Negative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Negative	
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Abstain	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	South Mississippi Electric Power Association	Gary Hutson		
3	Southern California Edison Co.	David B Coher	Negative	
3	Tacoma Public Utilities	Travis Metcalfe	Negative	
3	Tampa Electric Co.	Ronald L. Donahey	Negative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Negative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Negative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Negative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	
4	Consumers Energy	David Frank Ronk	Negative	
4	Cowlitz County PUD	Rick Syring	Abstain	
4	Detroit Edison Company	Daniel Herring	Affirmative	

4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Abstain	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	
4	LaGen	Richard Comeaux	Negative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
4	WPPI Energy	Patrick Connors	Negative	
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	
5	Avista Corp.	Edward F. Groce	Negative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore	Abstain	
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	
5	Cowlitz County PUD	Bob Essex	Abstain	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Negative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	
5	Duke Energy	Dale Q Goodwine	Negative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	

5	Exelon Nuclear	Michael Korchynsky	Abstain	
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Negative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Negative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Negative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Negative	
5	New York Power Authority	Gerald Mannarino	Negative	
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Negative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel		
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Negative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart		
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
5	WPPI Energy	Steven Leovy	Negative	
5	Xcel Energy, Inc.	Liam Noailles	Negative	

6	ACES Power Marketing	Jason L Marshall		
6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda L Powell	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	
6	Duke Energy Carolina	Walter Yeager	Negative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Negative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Negative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Negative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Negative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Negative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	
6	South Mississippi Electric Power Association	Joel Rogers		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Edward C Stein	Affirmative	
8		James A Maenner	Abstain	
8		Roger C Zaklukiewicz	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		

8	JDRJC Associates	Jim Cyrulewski		
8	Network & Security Technologies	Nicholas Lauriat	Negative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Negative	
10	New York State Reliability Council	Alan Adamson	Negative	
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 CIP-008-5 CSO706 V5
Ballot Period:	5/11/2012 - 5/21/2012
Ballot Type:	Initial
Total # Votes:	418
Total Ballot Pool:	485
Quorum:	**86.19 % The Quorum has been reached**
Weighted Segment Vote:	67.19 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	63	0.63	37	0.37	10	15
2 - Segment 2.	11	1	8	0.8	2	0.2	1	0
3 - Segment 3.	120	1	70	0.737	25	0.263	13	12
4 - Segment 4.	38	1	17	0.531	15	0.469	4	2
5 - Segment 5.	103	1	48	0.64	27	0.36	12	16
6 - Segment 6.	60	1	26	0.634	15	0.366	6	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	4	0.4	2	0.2	1	3
9 - Segment 9.	9	0.2	2	0.2	0	0	2	5
10 - Segment 10.	9	0.6	4	0.4	2	0.2	2	1
Totals	**485**	**7.4**	**242**	**4.972**	**125**	**2.428**	**51**	**67**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Negative	
1	Avista Corp.	Scott J Kinney	Negative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi		
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Affirmative	
1	Dominion Virginia Power	Michael S Crowley	Negative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Negative	
1	Lakeland Electric	Larry E Watt	Negative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Arnold J. Schuff	Affirmative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Affirmative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	
1	Oncor Electric Delivery	Brenda Pulis	Negative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Abstain	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Abstain	
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Negative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Abstain	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	ISO New England, Inc.	Kathleen Goodman	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Negative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	

3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Abstain	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Abstain	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Negative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	
3	City of Lodi, California	Elizabeth Kirkley	Abstain	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Affirmative	
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Abstain	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Negative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill		
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik		
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	Marilyn Brown	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Negative	
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Abstain	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	South Mississippi Electric Power Association	Gary Hutson		
3	Southern California Edison Co.	David B Coher	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe		
3	Tampa Electric Co.	Ronald L. Donahey	Negative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Negative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Negative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Negative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Abstain	
4	Detroit Edison Company	Daniel Herring	Affirmative	

4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	
4	LaGen	Richard Comeaux	Negative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
4	WPPI Energy	Patrick Connors	Negative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	
5	Avista Corp.	Edward F. Groce	Negative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore	Abstain	
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Negative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick		
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Abstain	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Negative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	

5	Exelon Nuclear	Michael Korchynsky	Abstain	
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Negative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Negative	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel		
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart		
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
5	WPPI Energy	Steven Leovy	Negative	
5	Xcel Energy, Inc.	Liam Noailles	Negative	

6	ACES Power Marketing	Jason L Marshall		
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Negative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda L Powell	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Negative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Negative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Negative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill		
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		

8	JDRJC Associates	Jim Cyrulewski		
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson	Negative	
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results	
Ballot Name:	Project 2008-06 CIP-009-5 CSO706 V5
Ballot Period:	5/11/2012 - 5/21/2012
Ballot Type:	Initial
Total # Votes:	422
Total Ballot Pool:	485
Quorum:	**87.01 % The Quorum has been reached**
Weighted Segment Vote:	60.19 %
Ballot Results:	**The drafting team will consider comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	58	0.58	42	0.42	11	14
2 - Segment 2.	11	1	5	0.5	5	0.5	1	0
3 - Segment 3.	120	1	63	0.663	32	0.337	14	11
4 - Segment 4.	38	1	18	0.563	14	0.438	4	2
5 - Segment 5.	103	1	44	0.587	31	0.413	13	15
6 - Segment 6.	60	1	23	0.561	18	0.439	7	12
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	5	0.5	1	0.1	1	3
9 - Segment 9.	9	0.2	1	0.1	1	0.1	2	5
10 - Segment 10.	9	0.6	4	0.4	2	0.2	2	1
Totals	**485**	**7.4**	**221**	**4.454**	**146**	**2.947**	**55**	**63**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Negative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Affirmative	
1	Dominion Virginia Power	Michael S Crowley	Negative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Negative	
1	Lakeland Electric	Larry E Watt	Negative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Affirmative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	
1	Oncor Electric Delivery	Brenda Pulis	Negative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Abstain	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Abstain	
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Negative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Negative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Abstain	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Abstain	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Negative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Negative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Negative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	

3	Alabama Power Company	Richard J. Mandes	Negative	
3	Alameda Municipal Power	Douglas Draeger	Abstain	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Abstain	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Negative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	
3	City of Lodi, California	Elizabeth Kirkley	Abstain	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Abstain	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Negative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Negative	
3	Gulf Power Company	Paul C Caldwell	Negative	
3	Hydro One Networks, Inc.	David Kiguel	Negative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill		
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik		
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Negative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Negative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	Marilyn Brown	Negative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Negative	
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Abstain	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	South Mississippi Electric Power Association	Gary Hutson		
3	Southern California Edison Co.	David B Coher	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Negative	
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Negative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Abstain	
4	Detroit Edison Company	Daniel Herring	Affirmative	

4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	
4	LaGen	Richard Comeaux	Negative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
4	WPPI Energy	Patrick Connors	Negative	
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	
5	Avista Corp.	Edward F. Groce	Negative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore	Abstain	
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Abstain	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Negative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	

5	Exelon Nuclear	Michael Korchynsky	Abstain	
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Negative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Negative	
5	New York Power Authority	Gerald Mannarino	Negative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel		
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Negative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart		
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
5	WPPI Energy	Steven Leovy	Negative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall		
6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda L Powell	Negative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Negative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Negative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Negative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		

8	JDRJC Associates	Jim Cyrulewski		
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Negative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 CIP-010-5 CSO706 V5
Ballot Period:	5/11/2012 - 5/21/2012
Ballot Type:	Initial
Total # Votes:	419
Total Ballot Pool:	485
Quorum:	**86.39 % The Quorum has been reached**
Weighted Segment Vote:	47.92 %
Ballot Results:	**The drafting team will consider comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	47	0.47	53	0.53	10	15
2 - Segment 2.	11	1	2	0.2	8	0.8	1	0
3 - Segment 3.	120	1	55	0.579	40	0.421	13	12
4 - Segment 4.	38	1	15	0.469	17	0.531	4	2
5 - Segment 5.	103	1	39	0.513	37	0.487	12	15
6 - Segment 6.	60	1	17	0.415	24	0.585	6	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	4	0.4	2	0.2	1	3
9 - Segment 9.	9	0.2	2	0.2	0	0	2	5
10 - Segment 10.	9	0.6	3	0.3	3	0.3	2	1
Totals	**485**	**7.4**	**184**	**3.546**	**184**	**3.854**	**51**	**66**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	
1	American Electric Power	Paul B. Johnson	Negative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Negative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Negative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi		
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Affirmative	
1	Dominion Virginia Power	Michael S Crowley	Negative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Negative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	
1	Idaho Power Company	Ronald D. Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Negative	
1	Keys Energy Services	Stanley T Rzad	Negative	
1	Lakeland Electric	Larry E Watt	Negative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Negative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	
1	Oncor Electric Delivery	Brenda Pulis	Negative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Abstain	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Abstain	
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Negative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Negative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Abstain	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Negative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Negative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Negative	
2	Independent Electricity System Operator	Barbara Constantinescu	Negative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	
2	Midwest ISO, Inc.	Marie Knox	Negative	
2	New Brunswick System Operator	Alden Briggs	Negative	
2	New York Independent System Operator	Gregory Campoli	Negative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	

3	Alabama Power Company	Richard J. Mandes	Negative	
3	Alameda Municipal Power	Douglas Draeger	Abstain	
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	
3	City of Lodi, California	Elizabeth Kirkley	Abstain	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	
3	Consumers Energy	Richard Blumenstock	Negative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Abstain	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Negative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	
3	Flathead Electric Cooperative	John M Goroski	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Negative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Negative	
3	Gulf Power Company	Paul C Caldwell	Negative	
3	Hydro One Networks, Inc.	David Kiguel	Negative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill		
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik		
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Negative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Negative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	Marilyn Brown	Negative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Negative	
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Abstain	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	South Mississippi Electric Power Association	Gary Hutson		
3	Southern California Edison Co.	David B Coher	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe		
3	Tampa Electric Co.	Ronald L. Donahey	Negative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Negative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Negative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	
4	Consumers Energy	David Frank Ronk	Negative	
4	Cowlitz County PUD	Rick Syring	Abstain	
4	Detroit Edison Company	Daniel Herring	Negative	

4	Flathead Electric Cooperative	Russ Schneider	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	
4	LaGen	Richard Comeaux	Negative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
4	WPPI Energy	Patrick Connors	Negative	
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	
5	Avista Corp.	Edward F. Groce	Negative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore	Abstain	
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick		
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	
5	Cowlitz County PUD	Bob Essex	Abstain	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Negative	
5	Detroit Edison Company	Christy Wicke	Negative	
5	Dominion Resources, Inc.	Mike Garton	Negative	
5	Duke Energy	Dale Q Goodwine	Negative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	

5	Exelon Nuclear	Michael Korchynsky	Abstain	
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Negative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Negative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Negative	
5	New York Power Authority	Gerald Mannarino	Negative	
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart		
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
5	WPPI Energy	Steven Leovy	Negative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall		
6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda L Powell	Negative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	
6	Duke Energy Carolina	Walter Yeager	Negative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Negative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Negative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Negative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Negative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	
6	Tacoma Public Utilities	Michael C Hill		
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Negative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Roger C Zaklukiewicz	Affirmative	
8		Edward C Stein	Affirmative	
8		James A Maenner	Abstain	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		

8	JDRJC Associates	Jim Cyrulewski		
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Negative	
10	New York State Reliability Council	Alan Adamson	Negative	
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 CIP-011-1 CSO706 V5
Ballot Period:	5/11/2012 - 5/21/2012
Ballot Type:	Initial
Total # Votes:	419
Total Ballot Pool:	485
Quorum:	**86.39 % The Quorum has been reached**
Weighted Segment Vote:	58.23 %
Ballot Results:	**The drafting team will consider comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	59	0.59	41	0.41	10	15
2 - Segment 2.	11	1	6	0.6	4	0.4	1	0
3 - Segment 3.	120	1	52	0.547	43	0.453	13	12
4 - Segment 4.	38	1	13	0.406	19	0.594	4	2
5 - Segment 5.	103	1	47	0.618	29	0.382	12	15
6 - Segment 6.	60	1	23	0.548	19	0.452	5	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	5	0.5	1	0.1	1	3
9 - Segment 9.	9	0.2	1	0.1	1	0.1	2	5
10 - Segment 10.	9	0.6	4	0.4	2	0.2	2	1
Totals	**485**	**7.4**	**210**	**4.309**	**159**	**3.091**	**50**	**66**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi		
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Negative	
1	Dominion Virginia Power	Michael S Crowley	Negative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Negative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D. Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Negative	
1	Keys Energy Services	Stanley T Rzad	Negative	
1	Lakeland Electric	Larry E Watt	Negative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Negative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Arnold J. Schuff	Affirmative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Affirmative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Negative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	
1	Oncor Electric Delivery	Brenda Pulis	Negative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Abstain	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Abstain	
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Negative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence	Abstain	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Negative	
2	ISO New England, Inc.	Kathleen Goodman	Negative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Negative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Negative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	

3	Alabama Power Company	Richard J. Mandes	Negative	
3	Alameda Municipal Power	Douglas Draeger	Abstain	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Abstain	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	
3	City of Lodi, California	Elizabeth Kirkley	Abstain	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Negative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Negative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	
3	Cowlitz County PUD	Russell A Noble	Abstain	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Negative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Negative	
3	Hydro One Networks, Inc.	David Kiguel	Negative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill		
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	
3	Lincoln Electric System	Jason Fortik		
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	

3	Manitoba Hydro	Greg C. Parent	Negative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Negative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Negative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Negative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Negative	
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Abstain	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	South Mississippi Electric Power Association	Gary Hutson		
3	Southern California Edison Co.	David B Coher	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe		
3	Tampa Electric Co.	Ronald L. Donahey	Negative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Negative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	
3	Westar Energy	Bo Jones	Negative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Negative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Negative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Abstain	
4	Detroit Edison Company	Daniel Herring	Affirmative	

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	
4	LaGen	Richard Comeaux	Negative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
4	WPPI Energy	Patrick Connors	Negative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Affirmative	
5	Avista Corp.	Edward F. Groce	Negative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore	Abstain	
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick		
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Abstain	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Affirmative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	

5	Exelon Nuclear	Michael Korchynsky	Abstain	
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Abstain	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Negative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Negative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	
5	U.S. Bureau of Reclamation	Martin Bauer	Affirmative	
5	Westar Energy	Bryan Taggart		
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
5	WPPI Energy	Steven Leovy	Negative	
5	Xcel Energy, Inc.	Liam Noailles	Negative	

6	ACES Power Marketing	Jason L Marshall		
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda L Powell	Negative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Negative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Negative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Negative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	
6	Tacoma Public Utilities	Michael C Hill		
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner	Abstain	
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		

8	JDRJC Associates	Jim Cyrulewski		
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Negative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson	Negative	
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 CIP Implementation Plan SB
Ballot Period:	5/11/2012 - 5/21/2012
Ballot Type:	Initial
Total # Votes:	412
Total Ballot Pool:	484
Quorum:	**85.12 % The Quorum has been reached**
Weighted Segment Vote:	66.23 %
Ballot Results:	**The drafting team will consider comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	62	0.66	32	0.34	14	17
2 - Segment 2.	10	0.8	6	0.6	2	0.2	2	0
3 - Segment 3.	120	1	68	0.708	28	0.292	11	13
4 - Segment 4.	38	1	20	0.625	12	0.375	4	2
5 - Segment 5.	103	1	44	0.595	30	0.405	11	18
6 - Segment 6.	60	1	23	0.548	19	0.452	6	12
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	5	0.5	1	0.1	1	3
9 - Segment 9.	9	0.1	1	0.1	0	0	3	5
10 - Segment 10.	9	0.5	3	0.3	2	0.2	2	2
Totals	**484**	**7**	**232**	**4.636**	**126**	**2.364**	**54**	**72**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Affirmative	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Affirmative	
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Negative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Abstain	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Negative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Negative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	
1	Idaho Power Company	Ronald D. Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Negative	
1	Keys Energy Services	Stanley T Rzad	Negative	
1	Lakeland Electric	Larry E Watt	Negative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour		
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Negative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Affirmative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Abstain	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	
1	Oncor Electric Delivery	Brenda Pulis		
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Abstain	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Abstain	
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Negative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence		
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Negative	
1	South Mississippi Electric Power Association	Rodney A. Wilson		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Affirmative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	
1	Trans Bay Cable LLC	Steven Powell	Negative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Negative	
2	New York Independent System Operator	Gregory Campoli	Negative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Abstain	
3	Alabama Power Company	Richard J. Mandes	Affirmative	

3	Alameda Municipal Power	Douglas Draeger		
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	
3	City of Lodi, California	Elizabeth Kirkley		
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	
3	Consumers Energy	Richard Blumenstock	Negative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Negative	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	
3	Flathead Electric Cooperative	John M Goroski	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Negative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Negative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill		
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik		
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Abstain	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	
3	Manitoba Hydro	Greg C. Parent	Negative	

3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	Marilyn Brown	Negative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Negative	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	South Mississippi Electric Power Association	Gary Hutson		
3	Southern California Edison Co.	David B Coher	Negative	
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Negative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Negative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Negative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	

4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
4	WPPI Energy	Patrick Connors	Negative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Negative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore	Abstain	
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Negative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Negative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Energy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Michael Korchynsky	Abstain	

5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Negative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Negative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Negative	
5	New York Power Authority	Gerald Mannarino	Negative	
5	NextEra Energy	Allen D Schriver	Negative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel		
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Negative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Negative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	
5	U.S. Bureau of Reclamation	Martin Bauer	Abstain	
5	Westar Energy	Bryan Taggart		
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
5	WPPI Energy	Steven Leovy	Negative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall		

6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda L Powell	Negative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Negative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Negative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Negative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Negative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Negative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Negative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Negative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Negative	
6	South Mississippi Electric Power Association	Joel Rogers		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		James A Maenner	Abstain	
8		Roger C Zaklukiewicz	Affirmative	
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski		

8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Abstain	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley		
10	New York State Reliability Council	Alan Adamson	Negative	
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 CIP Definition SB
Ballot Period:	5/11/2012 - 5/21/2012
Ballot Type:	Initial
Total # Votes:	407
Total Ballot Pool:	484
Quorum:	**84.09 % The Quorum has been reached**
Weighted Segment Vote:	47.88 %
Ballot Results:	**The drafting team will consider comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	47	0.505	46	0.495	13	19
2 - Segment 2.	10	0.8	3	0.3	5	0.5	2	0
3 - Segment 3.	120	1	41	0.436	53	0.564	12	14
4 - Segment 4.	38	1	13	0.382	21	0.618	2	2
5 - Segment 5.	103	1	31	0.425	42	0.575	11	19
6 - Segment 6.	60	1	19	0.452	23	0.548	5	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.7	5	0.5	2	0.2	0	3
9 - Segment 9.	9	0.1	1	0.1	0	0	3	5
10 - Segment 10.	9	0.5	3	0.3	2	0.2	2	2
Totals	**484**	**7.1**	**163**	**3.4**	**194**	**3.7**	**50**	**77**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Negative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Negative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Negative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Negative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi		
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl		
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Negative	
1	Dominion Virginia Power	Michael S Crowley	Negative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Negative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Affirmative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Abstain	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	
1	Idaho Power Company	Ronald D. Schellberg		
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw		
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Negative	
1	Keys Energy Services	Stanley T Rzad	Negative	
1	Lakeland Electric	Larry E Watt	Negative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour		
1	Minnesota Power, Inc.	Randi K. Nyholm	Negative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Negative	
1	Nebraska Public Power District	Cole C Brodine	Negative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Negative	
1	New York Power Authority	Arnold J. Schuff	Affirmative	
1	New York State Electric & Gas Corp.	Raymond P Kinney	Affirmative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Negative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Abstain	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Abstain	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain	
1	Omaha Public Power District	Doug Peterchuck	Negative	
1	Oncor Electric Delivery	Brenda Pulis		
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Negative	
1	PECO Energy	Ronald Schloendorn	Abstain	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Abstain	
1	PowerSouth Energy Cooperative	Larry D Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A Koelsch	Negative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn Spence		
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Abstain	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Negative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson		
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	
1	Tampa Electric Co.	Beth Young	Negative	
1	Tennessee Valley Authority	Larry Akens	Abstain	
1	Trans Bay Cable LLC	Steven Powell	Negative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Negative	
1	Tucson Electric Power Co.	John Tolo		
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton		
1	Westar Energy	Allen Klassen	Negative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Negative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Negative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Negative	
2	New Brunswick System Operator	Alden Briggs	Negative	
2	New York Independent System Operator	Gregory Campoli	Negative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Abstain	
3	Alabama Power Company	Richard J. Mandes	Negative	

3	Alameda Municipal Power	Douglas Draeger		
3	Ameren Services	Mark Peters	Negative	
3	American Public Power Association	Nathan Mitchell	Abstain	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Negative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blachly-Lane Electric Co-op	Bud Tracy	Negative	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Negative	
3	Central Electric Power Cooperative	Ralph J Schulte	Affirmative	
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Negative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	
3	City of Lodi, California	Elizabeth Kirkley		
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Negative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk	Abstain	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll	Negative	
3	Consumers Energy	Richard Blumenstock	Negative	
3	Consumers Power Inc.	Roman Gillen	Negative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Negative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Negative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Negative	
3	FirstEnergy Energy Delivery	Stephan Kern	Negative	
3	Flathead Electric Cooperative	John M Goroski	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Georgia Power Company	Anthony L Wilson	Negative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Negative	
3	Gulf Power Company	Paul C Caldwell	Negative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Negative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill		
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Negative	
3	Lincoln Electric System	Jason Fortik		
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Abstain	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Negative	
3	Manitoba Hydro	Greg C. Parent	Negative	

3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Negative	
3	Mississippi Power	Jeff Franklin	Negative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Negative	
3	New York Power Authority	Marilyn Brown	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Negative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Negative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Negative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Negative	
3	Piedmont EMC	Robin W Blanton	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Negative	
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Negative	
3	Public Utility District No. 1 of Clallam County	David Proebstel	Affirmative	
3	Puget Sound Energy, Inc.	Erin Apperson		
3	Raft River Rural Electric Cooperative	Heber Carpenter	Negative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Abstain	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens		
3	South Carolina Electric & Gas Co.	Hubert C Young	Abstain	
3	South Mississippi Electric Power Association	Gary Hutson		
3	Southern California Edison Co.	David B Coher	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe		
3	Tampa Electric Co.	Ronald L. Donahey	Negative	
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Negative	
3	Westar Energy	Bo Jones	Negative	
3	Wisconsin Electric Power Marketing	James R Keller	Negative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Negative	
3	Xcel Energy, Inc.	Michael Ibold	Negative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Negative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Negative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	
4	Consumers Energy	David Frank Ronk	Negative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Affirmative	

4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	
4	Imperial Irrigation District	Diana U Torres	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Negative	
4	LaGen	Richard Comeaux	Abstain	
4	Madison Gas and Electric Co.	Joseph DePoorter	Negative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Negative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Negative	
4	Northern California Power Agency	Tracy R Bibb	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Negative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Negative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace		
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Negative	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Negative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	
4	WPPI Energy	Patrick Connors	Negative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Negative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Negative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla		
5	Bonneville Power Administration	Francis J. Halpin	Negative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore	Abstain	
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason		
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick		
5	City of Tallahassee	Brian Horton		
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Negative	
5	Consumers Energy Company	David C Greyerbiehl	Negative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Abstain	
5	Dairyland Power Coop.	Tommy Drea	Negative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin	Abstain	
5	Energy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Michael Korchynsky	Abstain	

5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Negative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Negative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver		
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	
5	Madison Gas and Electric Co.	Steven Schultz	Negative	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Negative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Negative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Negative	
5	New York Power Authority	Gerald Mannarino	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi	Affirmative	
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Negative	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Negative	
5	Platte River Power Authority	Roland Thiel		
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Fossil LLC	Tim Kucey	Negative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Abstain	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic	Abstain	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Negative	
5	Tampa Electric Co.	RJames Rocha	Negative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Abstain	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Negative	
5	Tri-State G & T Association, Inc.	Barry Ingold	Negative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	
5	U.S. Bureau of Reclamation	Martin Bauer	Negative	
5	Westar Energy	Bryan Taggart		
5	Wisconsin Electric Power Co.	Linda Horn	Negative	
5	WPPI Energy	Steven Leovy	Negative	
5	Xcel Energy, Inc.	Liam Noailles	Negative	
6	ACES Power Marketing	Jason L Marshall		

6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	
6	APS	RANDY A YOUNG	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Negative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda L Powell	Negative	
6	Dominion Resources, Inc.	Louis S. Slade	Negative	
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entergy Services, Inc.	Terri F Benoit		
6	Exelon Power Team	Pulin Shah	Abstain	
6	FirstEnergy Solutions	Kevin Querry	Negative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer		
6	Lakeland Electric	Paul Shipps	Negative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Negative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Negative	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Negative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Negative	
6	Orlando Utilities Commission	Claston Augustus Sunanon		
6	PacifiCorp	Scott L Smith	Negative	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Negative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Negative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Abstain	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative	
6	Tacoma Public Utilities	Michael C Hill		
6	Tampa Electric Co.	Benjamin F Smith II		
6	Tenaska Power Services Co.	John D Varnell		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Westar Energy	Grant L Wilkerson	Negative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski		

8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Negative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Abstain	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley		
10	New York State Reliability Council	Alan Adamson	Negative	
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Individual or group. (119 Responses)
Name (77 Responses)
Organization (77 Responses)
Group Name (42 Responses)
Lead Contact (42 Responses)
Question 1 (106 Responses)
Question 2 (107 Responses)
Question 3 (0 Responses)
Question 3 Comments (119 Responses)
Question 4 (100 Responses)
Question 5 (102 Responses)
Question 6 (100 Responses)
Question 7 (102 Responses)
Question 8 (100 Responses)
Question 9 (101 Responses)
Question 10 (0 Responses)
Question 10 Comments (119 Responses)

Individual
David Proebstel
Clallam County PUD No.1
Yes
Yes
No comment
Yes
Yes
Yes
Yes
Yes
Yes
No comment
Individual
Monica - TEST
TEST
Yes
Yes
this is a test to add comments to a field.
Yes
Yes
Yes
Yes
Yes
Yes
test
Individual
John Falsey
Edison Mission Marketing & Trading
Yes
Yes

Yes
No
Yes
No
Yes
Yes
CIP-003-5 R2-I agree with Cyber systems in the Medium and High categories need documented policies, but not for the low category
Group
Northeast Power Coordinating Council
Guy Zito
No
No
Request clarification on the Applicability of Distribution Providers (DP) and Load Serving Entities (LSE). 1. Does 4.1.2 mean that any DPs owning assets in 4.2.2 need to comply with these CIP Standards? 2. Does 4.1.6 mean that LSEs owning assets in 4.2.1 need to comply with these CIP Standards? 3. Does 4.2.2 mean that only these DP assets are covered by these CIP Standards? 4. Does 4.2.1 mean that only these LSE assets are covered by these CIP Standards? 5. Does the DP's third bullet in 4.2.2 apply to only protection systems, not UFLS or UVLS since those load shedding systems are covered by the DP's first bullet? Note the NERC definition of "protection systems" includes load shedding systems, which generates this question. 6. Section 4.2 should explicitly state that UFLS Systems that perform automatic load shedding of less than 300 MW are specifically excluded. Request clarification on High Impact 1.3 and 1.4's use of "associated data centers". Are these the "computer rooms" that service a Control Center? Request clarification on the Standard Drafting Team (SDT) expectations on Medium Impact 2.1. Does the SDT expect that the "aggregate highest rate net Real Power capability of the preceding 12 months" will not flip flop on this threshold? In other words, does the SDT expect these asset to remain on one side or the other of this threshold? Recommend a change to R1's VSLs since Lower and Severe use 100 or more High and Medium BES Cyber Systems while moderate and High uses BES Cyber Assets. Request clarification and consistency. Recommend BES Cyber Assets so that ISOs can easily hit their thresholds. Requirement 1.2 of CIP-002-5 should be revised to use the same language as Attachment 1. The wording presently reads: "Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; " Suggested rewording: Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used BY AND LOCATED AT the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; Requirement 1.3 of CIP-002-5 should be revised to use the same language as Attachment 1. The wording presently reads: "Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;" Suggested rewording: Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) ASSOCIATED WITH the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;
Yes
Yes
Yes
Yes
No
No
Recommend changing M5 from "signed" to "approved" since some companies use other approval processes. Also these Measures criteria need to be aligned with the Requirements. Measure M5 includes "to approve or authorize specifically identified items" while R5 states "and approved by the CIP Senior Manager". Request a re-written M6 since it appears to add a new Requirement--"that

within 30 days of discharging the delegated authority". Recommend updating CIP-003 R2's Violation Risk Factor in the Table of Compliance Elements. That VRF is "medium" while the Requirements and Measures show R2 as "low".
Group
AEP Standards based SME list
Gerald Freese
Yes
Yes
No
No
Yes
Yes
Yes
Yes
CIP-003: 1. R2 – What level of detail is required in the cyber security policy for Low impact BES Cyber Systems? How strict must the security program defined in this policy be? There are no requirements in CIP-004-CIP-011 to use as guidance. With the existing Version 3 standards Responsible Entities cyber security policies are reviewed by auditors to determine if each of the CIP-004-CIP-009 requirements are repeated word for word from the standard; presumably this will be expected by the auditors for High and Medium BES Cyber Systems under R1. What will be used as guidance under R2? In addition, the following is a previous comment that still has outstanding issues: 2. AEP believes the inclusion of the word "implement" in CIP-003-5 Requirement R2 may open entities up to double jeopardy with CIP-004 – CIP-011. The security controls for 1.1 – 1.9 are implemented as part of CIP-004 – CIP-011. If the implementation of the cyber security policy is audited then would it not be an audit of the CIP-004 – CIP-011 requirements? AEP recommends removing the word "implement" in this instance. 3. (1) R1 – The implementation and documentation of the items 1.1-1.10 that are required to be defined in the cyber security policy are also implemented as part of CIP-004-CIP-011 compliance. This represents double jeopardy. (2) R2 – What level of detail is required in the cyber security policy for Low impact BES Cyber Systems? How strict must the security program defined in this policy be? There are no requirements in CIP-004-CIP-011 to use as guidance. With the existing Version 3 standards Responsible Entities cyber security policies are reviewed by auditors to determine if each of the CIP-004-CIP-009 requirements are repeated word for word from the standard; presumably this will be expected by the auditors for High and Medium BES Cyber 4. AEP is also concerned that a Registered Entity with only Low Impact BES Cyber Systems would be unable to "implement" their cyber security policy since some of these areas are not applicable to them. Are those entities expected to go beyond the standards requirements and provide evidence they have done so? Again, AEP recommends removing the word "implement" in this instance. 5. In CIP-003-5 Measure M2 the standard states "Records that indicate the required ten topics were implemented." This measure should not be required, as the actual implementation of the policy is addressed in the implementation of the requirements of CIP-004 through CIP-011. If you have a non-compliance issue with a requirement in CIP-006 would the entity be non-compliant with the policy in CIP-003-5 R2? AEP recommends striking item #2 from Measure M2.
Individual
Brian Evans-Mongeon
Utility Services Inc.
No
No
The following comments concern the Applicability section of all of the CIP standards CIP-002-5 through CIP-009-5, CIP-010-1, CIP-011-1. (1) Use of "Facilities" (1.a) Section 4.2 is titled "Facilities" with a capital F. The capitalization designates this section as a defined NERC Term. This may be viewed as applying the standard to a broader area than intended, and not to only those facilities identified within section 4.2. Modifying the language from "Facilities" to "Systems covered by this Standard" would alleviate the confusion. (1.b) The use of "BES Facilities" is inappropriate as it is not a

defined term. The definition of “Facilities” refers to BES Elements making the use of “BES Facilities” redundant. (1.c) Section 4.2.4.1 again states “Facilities” with a capital F. In this case it is seems that the NERC defined term is the intent, and not the meaning throughout the rest of section 4.2. This inconsistence will invariably lead to some level of confusion. (2) Applicability of LSE’s: LSEs, as determined by NERC in 2008, do not own or have physical assets. Because no assets are actually owned, LSE’s should be removed from the applicability section of the standard. If it is determined that an LSE does own physical assets are these standards only applicable to those assets identified in 4.2.1 (3) Protection Systems inclusive of UFLS and UVLS: The DP’s third bullet in 4.2.2 does not clearly apply to only transmission Protection Systems, excluding UFLS or UVLS since those load-shedding systems which are covered by the DP’s first bullet. Note the NERC Definition of "Protection Systems" includes load-shedding systems and PRC-005-2 will group UFLS and UVLS systems alongside other Protection Systems. Clarification is required to ensure UFLS and UVLS systems under 300MW are removed from applicability. We recommend revising the third bullet to read "A Protection System (other than a UFLS or UVLS System) that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard." (4) To make it clear that the standards apply only to DP owned systems listed in section 4.2.2, suggest adding the following in the Exemptions section: “4.2.4.4 Cyber Assets that are owned by Distribution Providers or Load Serving Entities and that are not associated with the Facilities, Systems and equipment described in 4.2.1 or 4.2.2.” (7) R1.1 Utility Services support the comments made by Massachusetts Municipal Wholesale Electric Company in that R1.1 appears to require the entity to maintain a list of “Facilities, Systems, or equipment that meet the criteria specified in CIP-002-5, Attachment 1.” This seems to be inconsistent with what is stated in the Rationale and the Guidelines, which only refer to identifying BES Cyber Assets and BES Cyber Systems. We suggest that the SDT clarify the intent and the auditable requirement by adding an explanation to the Rationale, Guidelines or M1. (6) R2 - It is unclear exactly what is to be reviewed. The rationale for R2 starts with “The lists required by Requirement R1 are reviewed”. The bullet for R1.3 states “shall default to the category of low impact and do not require discrete identification”. Our understanding is that “discrete identification” is synonymous with “list”. It seems that based on R1.3 a list would not be created for Low Impact but per R2 this non-existent list must be reviewed. It may be interpreted that the only way to review a blank list is to review a list of all cyber systems and then justify why each system is either not listed as a High, Medium or Low asset. Recommend that the annual review requirement be added to R1.4 and clarify that the review is of the “identification” process and resulting lists.
Yes
Yes
Yes
Yes
Yes
Yes
(1) The Violation Risk Factor stated in CIP-003-5 R2 should agree with the VRF listed in the Table of Compliance Elements. (2) It should be clarified that the contents for the policies listed in R1 and R2 are not required to include elements that maybe detailed in other CIP standards. I.e.. The R2.4 Incident response to a BES Cyber Security Incident does not require the elements and timelines contained in CIP-008-5. (3) Utility Services agrees with and supports the comments submitted by MMWEC concerning R1.1.
Group
Snohomish County PUD
Benjamin Beberness
Yes
Yes
Impact Rating Criteria: Medium Impact Rating 2.5 – Snohomish would like clarity on how the ”Weight Value per Line” is applied. Medium Impact Rating 2.10 – The CIP-002-5, 2.10 wording is confusing and should be clarified - would CIP-002-5, 2.10 apply to an RE with a load over 968 MW in the Western Interconnection just because their UFLS scheme requires the arming of 31% of the load-meeting the 300 MW armed load threshold? The electric industry is confused on how to interpret the UFLS/UVLS thresholds in CIP-002-5, 2.10 and there are a number of interpretations being discussed

in various forums which highlights the need for clearer language. Public Utility District No. 1 of Snohomish County (“SNPD”) interprets the latest CIP-002-5, 2.10 language “…Each System or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW…” to mean a registered entity can arm 300 MW of load and over in its UFLS/UVLS program, if the System or group of Elements are installed at numerous circuits, feeders, or station (less than 300 MW individually) where a failure of the System or group of Elements is not under a common control system (or power source/battery) the CIP-002-5 would not apply. SNPD requests that the SDT comment on whether the interpretation above is accurate. Furthermore, SNPD ask that an example be added to the Application Guidelines for 2.10. The example should highlight a UFLS or UVLS program that meets or exceeds 300 MW but is separated into multiple System or group of Elements where all System or group of Elements are less than 300 MW individually and therefore would not meet the CIP-002-5, 2.10 thresholds. Secondly, because UFLS and UVLS requirements are addressed in the family of PRC Reliability Standards SNPD supports removing the UFLS, UVLS, and other safety net schemes from the family of CIP Reliability Standards. Medium Impact Rating 2.11 – SNPD disagrees with the CIP-002-5, 2.11 as it dictates that all registered Balancing Authorities and Transmission Operators are automatically assigned a Medium Impact Rating (M). There are many very small Balancing Authorities and Transmission Operators that have little to no reliability impact to neighboring systems and should not be included as a medium impact rating. In addition the assigned registration as a TOP is extremely subjective. The NERC Statement of Compliance Registry Criteria (“SCRC”), section III (d), uses the same criteria to define both Transmission Owner (“TO”) and Transmission Operator (“TOP”) . In addition, the application of this criteria, especially as to under what circumstances an entity is a TO and not a TOP is not defined and is not consistent through the regions. SNPD supports removing section 2.11 as there is no “reliability based” justification that registration as TOP justifies a Medium Impact Rating. If they registration thresholds were removed from section 2.11 SNPD would change its vote to affirmative. General comment: If a TO is also a GO and either the TO or GO requirements result in a medium or high impact rating, it is not clear whether the impact rating applies to all Cyber Assets that support the TO and GO operation or just the category that triggers the high or medium impact rating. The SDT should clarify this concern. The draft CIP versions 5 Reliability Standards are very BES definition centric. Due to the proposed changes to the BES definition it is very difficult for the electric industry to comment on a standard as it is unclear if the current or proposed BES definition will be applied. This change in the definition could significantly change the applicability of the version 5 CIP Reliability Standards. Although it is clear the SDT has made attempts to size the applicability of the CIP version 5 requirements with the size of the registered entity, the current draft will cause significant resource burdens on facilities that have demonstrated they cannot impact the reliability of the BES. As a Transmission Dependent Utility SNPD supports a reliable system because we are at the end of the system and SNPD’s customers are exposed to all disturbances on the main grid. However, SNPD also supports efficiency and spending significant resources with little to no benefit is not beneficial to the reliability of the BES or to the Level of Service (“LOS”) SNPD provides its customers.
Yes
No
Yes
Yes
Yes
Yes
CIP-003-5 R2 NIST clearly outlines what should go into a cyber security program. Snohomish would recommend that NIST is referenced. Additionally, cyber security policies should include the life cycle of a cyber asset: Pre-purchase • Vendors and utilities follow secure development life cycle • Utilities ensure contractual language regarding security in contracts • Utilities utilize security best practice through RFP and contract negotiations. o Include language in contract stating that the software will be tested and security incidents will be categorized. o Include contractual language that states security vulnerabilities based on their category must be resolved prior to go live. o Etc. Implementation • Utilities utilize security best practice through project lifecycle. o Test for security vulnerabilities o Treat as defects and ensure that system does not go live with any critical issues. o Etc. • Document the security design and architecture of the system • Utilities utilize security best practice through project lifecycle. Monitor/control/ Incident response • Document your security monitoring process and demonstrate implementation • Document the security controls and demonstrate implementation •

Document how the organization will respond to a cyber incident and exercise the plan.
Individual
Anthony Jablonski
ReliabilityFirst
ReliabilityFirst votes in the affirmative for the standard but offers the following recommendations regarding the Violation Severity Levels. CIP-002-5 1. VSL for Requirement R1 a. Requirement 1, Part 1.4 starts off with the words “Review (and update as needed) the identification…” and the associated VSL only states the “…failed to update…” For consistency with the requirement, ReliabilityFirst recommends modifying the VSL to state “…failed to review (and updated as needed)…” This recommendation is based on the FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement. 2. VSLs for Requirement R2 a. The VSL for Requirement R2 uses the phrase “…failed to complete its annual review…” though the associated requirement itself states “…shall have its CIP Senior Manager or delegate approve the identifications…”. For consistency with the requirement, ReliabilityFirst recommends modifying the VSL to begin with the following: “The Responsible Entity failed to have its CIP Senior Manager or delegate approve the identifications…” This recommendation is based on the FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement.
ReliabilityFirst votes in the affirmative for the standard but offers the following recommendations regarding the Violation Severity Levels. CIP-003-5 1. VSL for Requirement R3 a. The VSL introduces more detail then what is stated in the associated Requirement R3. Based on the FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement. For consistency with the requirement, ReliabilityFirst recommends modifying the VSL as follows: “The Responsible Entity failed to identify a CIP Senior Manager by name.” 2. VSL for Requirement R6 a. For consistency with the other VSLs, ReliabilityFirst recommends modifying the beginning of the VSLs as follows: “The Responsible Entity failed to…” Also, the term “effective date” in the VSL is not referenced anywhere within Requirement R6. ReliabilityFirst recommends modifying the two VSL as follows: i. High VSL – The Responsible Entity failed to document a change to one of the delegations within 30 calendar days of the change. ii. Severe VSL - The Responsible Entity failed to document a change to the CIP Senior Manager, OR more than one of the delegations within 30 calendar days of the change.
Individual
Jianmei Chai
Consumers Energy Company
No
Yes
R1 & R1.4 - “Review” has been added to R1 (R1.4) thus requiring excessive documentation that such review was completed for any and every change in facilities, regardless of whether it is obvious that some changes will not result in a change in identification or categorization. Eliminate the word “Review” from R1.4 since the goal of R1 is simply to “Update as needed the identification…”. A review will still be necessary to identify whether an update is needed, but documentation of the review itself for any and every change in facilities would not be implied. Section A, paragraph 4.2 - The SDT needs to clarify the “Applicability” such that a registered entity, such as a Distribution Provider or Load Serving Entity, only needs to evaluate those assets specifically associated with its registration. Section A. 4.2.1 and 4.2.2 seem to imply this, but Section B, R1 does not provide any specific direction limiting a DP or LSE’s applicability. Section A, paragraph 4.2.2, third (unnumbered bullet) - The requirements for Distribution Providers to include facilities containing “A Protection System that applies to Transmission …” is a new unsubstantiated requirement for Low Impact systems, and inconsistent (omitted) with the Medium Impact requirements for all other entities in Attachment 1, Section 2. The requirement should be deleted, or if such systems are to be included, these need to be better defined and only those that reach the level of impacting one or more Interconnection IROLs should be considered.
Yes
No
Yes

Yes
Yes
Yes
R2.4 - This Requirement essentially implies that Low Impact assets need to have in place system(s) to monitor or somehow detect potential cyber security incidents in order to respond to the incidents. Although an entity may choose to handle such a response in a variety of ways, there is no need to have this detailed in a policy or procedure for low impact assets.
Group
NESCOR/NESCO
Annabelle Lee
Phrasing around the term "adversely impact" have been addressed in this new draft. However, it still may be helpful to provide some context around the meaning of "adversely impact". It is understood that in may not be practical given the variables one might need to consider.
No
No
No
R1: This requirement continues to list a series of policies that do not clearly identify what actual components of such security policies categories would be essential to help assure that an expected security state is achieved and maintained. The policy levels do not provide enough granularity to assure that there is a consistent and common approach to security policies. The standard could be modified to require entities to not only address the topics identified in the version 5 requirement, but to address them in a manner that reflects a clear relationship of policy and underlying process and/or control framework to the types of BES assets being afforded the protection of the Policy. R2: The security policies listed in this requirement should be applicable to all assets regardless of impact. Not including physical control policies and security awareness for high and medium impact assets does not match common security practices. It also does not seem to be a practical or sensical approach to dismiss assets not identified as medium or high from policy categories listed in CIP-003 R1. The standard should be modified to expand Cyber Security Policy to all levels of BES Cyber Systems, requiring the policy enumeration of protective measures afforded to operational assets. Application Guidelines for R2: There are a number of technical issues raised here that, in some cases, can be technically enforced, and not just required by policy. Consider moving and/or adding these to other CIPs where they are more appropriate. Also many of these issues go beyond the scope of the standards and are not required for compliance. This may cause confusion as to what is required for compliance. (1) Organization stance on use of wireless networks (this would be optimally addressed in CIP005) (2) Monitoring and logging of ingress and egress at Electronic Access Points (this is in CIP007 R4.1.1) (3) Maintaining up-to-date anti-malware software before initiating interactive remote access (is in CIP007 R3.4) (4) Maintaining up-to-date patch levels for operating system and applications used to initiate the interactive remote access before initiating interactive remote access (this would be optimally addressed in CIP007 R2.x) (5) Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating interactive remote access (this would be optimally addressed in CIP005) (6) For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s interactive remote access controls (this would be optimally addressed in CIP011 R1.x) (7) Monitoring and logging of physical ingress and egress (this would be optimally addressed in CIP006 R1.x, noting that egress logging / monitoring in not in the current CIP standards) (8)Availability of spare components (this was in CIP v1-v4, but doesn’t appear to be in CIP v5) (9) Break- fix processes (this would be optimally addressed in CIP010 R1.x)
Individual
Scott Bos
Muscatine Power and Water
No
Yes
For Criteria 2.11 - A BA or TOP may only provide a very small number of individual functions as described within the Functional Model based on the amount of CFRs and JROs that NERC has accepted. Not all BA's and TOP's have the same impact on the BES as a larger BA or TOP. As written,

2.11 will require every BA and TOP that is registered as such as being in the “medium” category. This one size fits all approach is not practical or logical. As stated in FERC Order 706, paragraph 253, FERC clearly speaks of being flexible “However, we are persuaded by commenter’s that stress the need for flexibility and the need to take account of the individual circumstances of a responsible entity.” We recommend that BA’s be viewed as in Attachment 1, CIP-002-4 brightline criteria 1.17.
Yes
No
Yes
Yes
Yes
Yes
[Proposed Change] CIP-003 R1 Each Responsible Entity for the identified BES Cyber Systems critical to the operation of high impact and medium impact BES Sites shall implement one or more documented cyber security policies that address the following topics: Keep 1.1 – 1.10 as is.
Group
ACES Power Marketing
Jason Marshall
No
No
(1) We thank the drafting team for restructuring the standard to focus on identifying Facilities and Elements that meet the criteria in Attachment 1 first and then subsequently the supporting Cyber Systems. We think this is a better approach than attempting to evaluate all Cyber System first. The previous approach would have compelled an inventory of every potential Cyber System or Cyber Asset supporting the registered entity’s Facilities and Elements. This new approach does not require such an inventory. (2) Conceptually, we agree that a review should be conducted for changes to the BES Elements or Facilities for the impact on identification of Facilities and equipment per Requirement R1 Part 1.3. However, we are concerned that “change to BES Elements or Facilities” is not well defined and that a registered entity will have to inventory all changes to demonstrate if the modification caused a “change in the identification or categorization of BES Cyber Systems from a lower to higher impact category.” By “change to BES Elements or Facilities”, we assume the drafting team is primarily referring to a change in transmission system topology and addition or retirement of Facilities. Many other changes would not be included. For example, changing the ratio on a CT or replacing a relay would not qualify as a change under Part 1.4. We suggest the drafting team modify Part 1.4 to clarify that it is only those changes that affect transmission topology or are equipment additions/retirements that are included. Additionally, we suggest the drafting team expand the Application Guidelines section to fully explain its intent. (3) Requirement R2 and its associated measurement are not in alignment. The requirement compels the CIP Senior Manager or delegate to “approve the identifications required by Requirement R1 at least once each calendar year”. It does not compel the CIP Senior Manager or delegate to “review and update, where applicable, the identification and categorization” as stated in the Measurement M2. While we agree that it would be difficult to approve without conducting a review, we do not believe the intent for Requirement R2 should be for the CIP Senior Manager or delegate to perform the update as suggested in the measure, particularly considering that Part 1.4 already requires an update for changes to BES Elements and Facilities. (4) “Categorization” is not consistently used in the requirements and measures. Requirement R2 specifically uses the term “identifications” and the associated measurement uses the terms “identifications and categorization”. Is there a difference? “Categorization” is also not used in Requirement R1. For consistency, we suggest using the same term consistently throughout all the requirements and measures. (5) The purpose statement uses the term adverse impact. Because the term is very similar to the NERC defined term Adverse Reliability Impact, we suggest a footnote is needed to clarify that the drafting team is not intending to use Adverse Reliability Impact and indeed intends an impact that is less than an Adverse Reliability Impact. (6) We disagree with including LSE as an applicable entity. Per the NERC functional model, LSEs do not own or operate UFLS or UVLS relays. Page 26 of the Reliability Functional Model Technical Document makes this clear with the statement, “Unlike the Distribution Provider, the Load-Serving Entity does not have Bulk Electric System assets (“wires”) but does take title to energy.” The only role that is given to the LSE in the

Reliability Functional Model is to “participate in under-frequency load shedding systems and under-voltage load shedding systems through identification of critical customer loads that are to be excluded from load shedding systems”. They are given no role to own, install or maintain UFLS or UVLS. They simply assist in the identification of critical loads to help ensure they are not inadvertently included in the UFLS or UVLS program. Because the standard only envisions inclusion of LSEs due to UVLS and UFLS, their complete removal from the standard is warranted. (7) Use of Systems is not consistent with the NERC Glossary definition throughout many sections of the standard and application guidelines. The NERC Glossary defines System as: “A combination of generation, transmission, and distribution components.” In section 4.2.2, how can a Distribution Provider have a System when two (generation and transmission) of three required elements to meet the definition are not included? Use of “System” in the first bullet under section 4.2.2 clearly does not intend the NERC Glossary definition but rather a computer or control system. It appears that a wholesale find and replace was performed on “system” between versions which may have contributed to this problem. There are many other instances in the Application Guidelines requiring the use of System that is questionable as well. (8) Use of language “required by a NERC or Regional Reliability Standard” used throughout Applicability Section 4.2.2 (Distribution Providers) is problematic and vague. The first bullet refers to UFLS or UVLS relays that are required. The second bullet refers to Special Protection System or Remedial Action Schemes that are required. Finally, the third bullet refers to Protection Systems that are required. There are currently no enforceable standards that explicitly require a UVLS, UFLS, Protection System or Special Protection Systems. Protection Systems are such a basic necessity that it is not necessary to have requirements to install Protection Systems. At best, FAC-001-0 requirements compel Transmission Owners to have facility connection requirements for system protection but it only applies to new interconnections. The Commission only recently approved PRC-006-1. It is the only NERC standard that could be pointed to as requiring UFLS. While there are some standards such as the TPL family that could be viewed as indirectly requiring some Protection Systems, UFLS, UVLS and Special Protection Systems to meet performance requirements, no specific type is required. For instance, are overload relays required, distance relays or both? These decisions are governed by a registered entity’s protection philosophy and not any specific standard. Also, a Distribution Provider could argue that no Protection System they have installed is required by a standard but that they have agreed with their Transmission Owner to install a Protection System on the low side of a distribution transformer because it is more cost effective. It is possible this standard could incent them to resist these configurations in the future. (9) It is not clear why “Bulk Power” is capitalized in the second paragraph of the Rationale box for R1. (10) We recommend that Measurement M1 be clarified that the “list of changes to the BES” per Part 1.4 may be an acknowledgement that there were no changes. (11) What is the justification for the values used for the VSLs in Requirement R1? For example, how were 40 Facilities and 100 Cyber Systems arrived at for the Lower VSL? A justification needs to be provided? Why not use 80 Facilities and 200 Cyber Systems? (12) For Requirement R2, the language of the VSLs is not consistent with the requirement. The requirement only requires “annual” approval. It does not explicitly require a “review”. “Review” is added to the VSL which makes the VSL inconsistent with the FERC guideline that prohibits the VSL from modifying the requirement. (13) It is not clear why “associated data centers” was added to the four high impact criteria. The appropriate Cyber Systems from the “associated data centers” will already be included through identification of Cyber Systems in Part 1.2 and 1.3 of Requirement R1. Those Cyber Systems in these “associated data centers” will be identified because they support the ability of System Operators to perform the “functional obligations of the” (identified in Attachment 1 Criteria 1.1 through 1.4) Transmission Operator, Balancing Authority, Reliability Coordinator and Generator Operators. (14) While we agree with the 15 minute limit for Cyber Systems, it is not clear how its inclusion in Attachment 1 is helpful or accomplishes the intent of the drafting team. The criteria in Attachment 1 is applied to “Facilities, Systems, or equipment” through Part 1.1 of Requirement R1. It is not applied to the Cyber Systems identified in Parts 1.2 and 1.3 of the requirement. Thus, the 15 minutes appears to be inadvertently applied to the “Facilities, Systems, or equipment” when it was intended to be applied to their supporting Cyber Systems. (15) Criterion 2.3 focuses on the long-term planning horizon which is contrary to the standard. The standard focuses on reliability impacts caused on the BES in a 15 minute timeframe from the misuse, degradation or unavailability of the BES Cyber Asset or BES Cyber System. It does not make sense to subject BES Cyber Assets and/or BES Cyber Systems within a generator plant or GOP control center to these standards if a generator is identified as needed for reliability four years out but is not identified from year 0-3. This needs to be further clarified. (16) It would be helpful if the application guidelines clarify how the Reliability Coordinator,

Transmission Planner or Planning Coordinator will notify the Generator Owner, Generator Operator, Transmission Owner and Transmission Operator that their equipment meets criteria 2.3 and 2.6. (17) Criterion 2.8 needs supporting explanation in the Application Guidelines explaining how the Transmission Owner will determine that a generator it does not own or operate meets the criteria in Part 2.3. Otherwise, it is not clear how the Transmission Owner will know that its interconnection equipment to the generator should be included in this Medium Impact Rating. (18) We thank the drafting team for mitigating some of the risks surrounding inclusion of Blackstart Resources and Cranking Paths by moving them to the low impact category. However, we simply do not believe they need to be included. When a restoration plan is implemented, manual switching and operation is usually necessary. It is highly unlikely that a cyber security incident would occur because many communication paths will be down forcing entities to rely on radio communications. Continuing with their inclusion at any level will likely lead to erosion of the number of Generator Operators willing to offer this service. (19) Cranking Paths are not included in the current Bulk Electric System (BES) definition, are not included in the recently approved definition, and have been removed (as presented by the BES SDT Chair at the April 11 and 12 Standards Committee meeting) from the SAR for the phase 2 modifications to the BES definition. Since NERC legal staff recently confirmed at the April 11 and 12 Standards Committee meeting that standards are generally written for the BES, inclusion of Cranking Paths would deviate from this guidance by drawing in non-BES equipment. Cranking Paths can include sub-transmission and even distribution equipment. (20) Use of “regional load shedding program” in Attachment 1 Criterion 2.10 is problematic. There are currently no enforceable standards for regional load shedding programs. Also, the recently Commission approved PRC-006-1 places the responsibility for establishing a UFLS program on the Planning Coordinator. Planning Coordinator areas do not necessarily follow regional boundaries. (21) In the Application Guideline section regarding reliability operating services, many of the services are attributed to incorrect Functional Entities. In the Dynamic Response section, LSE is incorrectly attributed to under and over frequency relay protection and under and over voltage relay protection. Software used to calculate ACE is incorrectly attributed to the RC. RC’s don’t calculate ACE but gather ACE through ICCP from the BAs. In the Controlling Voltage section, DPs are incorrectly included. No NERC standard gives a DP responsibility for voltage. By including DPs, there is an implication that distribution equipment is intended to be included. In the Restoration BES section, off-site power for nuclear facilities is attributed to the TOP when the NUC-001 standard more broadly describes a transmission entity which includes other Functional Entities besides the TOP. In the Inter-Entity Coordination section, the TOP and GOP should not be included in scheduled interchange as they have no role in interchange scheduling. Because there could be some disagreement over which Functional Entities apply to each reliability operating service and the list of issues we identified is not exhaustive, we recommend removing all references to Functional Entities as the simplest solution. (22) There is a statement in the first paragraph of the “Applicability to Distribution Providers and Load Serving Entities” section of the Application Guidelines that states the qualifications for inclusion of the Distribution Provider are based on requirements applicable to Distribution Providers in EOP-005 and registration. This statement could actually be contradictory to Applicability section 4.2.2 which includes more applicability than just restoration per EOP-005. The statement should either be deleted or further explained. (23) We believe the statements beginning on page 26 of the High Impact section of the applicability guidelines regarding TOP delegation to the TO should be removed. If the TOP has delegated some functions to the TO that would otherwise have been carried out in the TOP Control Center and might have resulted in additional TOP BES Cyber Assets and BES Cyber Systems being identified as High Impact, this delegation should not have an impact on the TO’s categorization of BES Cyber Systems and BES Cyber Assets. First, the TOP is still responsible and can’t pass that responsibility on through a delegation agreement. Thus, the TOP and TO will have to address this issue in their delegation agreement. Second, the TOP likely does not own these BES Cyber Assets at the TO but rather the TO likely owns them. They should be classified according to the criteria established for TOs in Attachment 1. Use of the term asset in the definition requires ownership by the responsible entity. If it is not owned by the TOP, it is not a TOP asset and, thus, not a TOP BES Cyber Asset. Third and final, this is a registration issue that should not be addressed in cyber security standards but in the registration criteria. (24) Page 27in the application guidelines, Category D contingency should be removed. The TPL standards only require a Planning Coordinator or Transmission Planner to document the impacts of Category D contingencies. There are no performance requirements for Category D contingencies. Thus, it is highly unlikely that any Planning Coordinator or Transmission Planner could ever justify the costs for reliability must run units through

Category D contingencies to its regulator, and, thus, there likely will not be any. (25) On page 28 in the Application Guidelines section, there is an explanation that Attachment 1 Criterion 2.4 excludes 500 kV collector buses. These 500 kV collector buses are part of the Generator Interconnection Facility. While we agree with the intent, this exclusion must be explicitly included in Criterion 2.4. Because the Commission has defined the requirements are the standard, the requirement needs to stand alone. Since the requirement does not reference the Application Guidelines but only the criteria in Attachment 1, we are concerned if Criterion 2.4 is not modified to account for this exclusion, the exclusion will not be considered by compliance and enforcement personnel. (26) The Application Guidelines on page 30 state the highest MW rating for the preceding 12 months will be used for Attachment 1 criterion 2.10 regarding load shedding systems. Rating is not the right word. Rather, the highest hourly integrated load is more correct. Instantaneous load should not be considered.
No
No
No
No
Yes
Yes
(1) Regarding Section 4.2.4 Exemptions: This section was changed from the last posting to indicate the exemptions are for CIP-002-5. CIP-002-5 already has the same exact exemption language. Either this reference should be changed back to CIP-003-5 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (2) Regarding Background Section 5: The second paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. Which is it? We support the latter. (3) Regarding Question 4 (CIP-003-5 R1): The Guidelines and Technical Basis section of the Standard for R1 states that, “The Responsible Entity should consider the following for each of the required topics in its cyber security policy…” Any number of dictionaries define “should” as the past tense of “shall” which is used to express obligation, duty or expectation. A synonym of “should” is “must.” None of the bullets listed under the required topics in the Guidelines and Technical Basis section for R1 are included in the actual Requirement R1. Using the word “should” in this section implies that Responsible Entities must consider each of the items listed for the required topics, hence, creating requirements within the Guidelines and Technical Basis section of the Standard. If the intent of the SDT is to make the items requirements, the items should be moved to R1. This will reduce compliance risk by leaving no doubt as to the minimum amount of information that is to be included for each topic. (4) Regarding Question 4 (CIP-003-5 R1): Part 1.5 needs to be clarified that the NERC Glossary definition of System does not apply. (5) Regarding Question 4 (CIP-003-5 R1): The application guidelines for interactive remote access regarding inclusion of language in contracts with vendors, consultants and contractors should be modified. The guidelines state that the language should require them to adhere to the responsible entity’s Interactive Remote Access controls. While we agree, in general, that contracts should reflect this language, the guidelines should be clear that this only applies to contracts executed after the enforcement date of this standard. Applying this standard to existing contracts could compel the responsible entity to renegotiate all contracts which puts the responsible entity at a significant disadvantage particularly with some contracts such as those with EMS vendors. (6) Regarding Question 5 (CIP-003-5 R2): Why does Requirement 2 state that it applies to BES Cyber Systems not identified as high and medium impact? Wouldn’t it be simpler to state that it applies to low impact BES Cyber Systems? (7) Regarding Question 5 (CIP-003-5 R2): Requirement R2 should also be modified to make it clear that an entity may write exceptions into their cyber security policies. FERC made it clear in Order 672 that only the requirements in a standard are enforceable and part of the standard. Thus, while the application guidelines make it clear the responsible entity can write in exceptions to its cyber security policy, the application guidelines are not enforceable and there is no way of ensuring that auditors follow them. (8) Regarding Question 7 (CIP-003-5 R4): While the application guidelines are clear that electronic approval is acceptable, the measurement may create the impression that a workflow showing review is not sufficient to indicate CIP Senior Manager approval. Our concern is that an auditor may expect a “wet ink” signature per bullet 2 of the measurement. The measure should make clear that electronic approvals through tools such as workflows are acceptable and “wet ink” signatures are optional. (9) Regarding Question 9 (CIP-003-5 R6): Four VSLs could and should be written based on the number of days late that the

change to CIP Senior Manager or delegates was documented. (10) Regarding the Application Guidelines: The paragraph under Requirement R3 should apply to what is now Requirement R4 as a result of re-ordering the requirements from the previous draft. In the previous draft R3 requires the review and approval of the cyber security policies by the CIP Senior Manager at least once each calendar year, not to exceed 15 calendar months… This is now Requirement R4.

Group

PPL Corporation NERC Registered Affiliates

Stephen Berger

No

Yes

1.) The standard CIP-002 R1 still states that entities do not have to identify your Low Impact assets; however, in CIP-003 R2 entities still have requirements that must be applied to them. In CIP-003 R2 it also states an inventory list is not required, but PPL Affiliates question how the auditors will treat this, as well as future CAN's that may state you need to have a list for them to audit. 2.) The proposed criteria for selecting high, medium, and low impact facilities can inappropriately make Distribution Providers and Load Serving Entities subject to the standards. PPL Affiliates suggest that the standard note that the 300 MW is calculated as total potential load shed that can occur without operator involvement. Only single circuit interruptions or automated schemes that are capable of shedding more than 300 MW of load without system operator intervention should be subject to the standard. Therefore, PPL Affiliates suggest the following changes in the Distribution Provider and Load Serving Entity sections to address this concern: • The draft standard states the DP and LSE may be considered medium impact facilities if: Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES: o A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more. As used in this requirement, the definition of common control system should distinguish between automated load shedding schemes that may result in a load-shed level of 300 megawatts in the aggregate across multiple facilities and both operator-initiated load shedding and single breaker/feeder control/protection systems. o A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard o A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard Load Serving Entity: o With the NERC BOT approval of PRC-006-1 and subsequent FERC filing (Docket No. RM06-16-000), NERC has recognized that LSEs have no role in UFLS/UVLS programs. The Applicability Section for CIP Version 5 Standards includes LSEs with UFLS/UVLS equipment. This is inconsistent with NERC BOT's recognition that LSEs do not serve a role in such programs. Therefore it is unnecessary to include such a qualified LSE in the Applicability Section. The LSE should be removed from the applicability (remove entire Applicability section 4.1.6 and 4.2.1) of CIP Version 5. 4.) PPL Affiliates are concerned with the VSLs • The VSLs for R1 apply varying levels of penalties for "incorrectly" classifying facilities as high and medium impact facilities. In fact, if 15% of the facilities are not identified or incorrectly categorized a severe violation level would exist and subject the responsible entity to potentially large fines. • PPL Affiliates are concerned that the standard does not identify who will do a review of the classification of facilities. Leaving the review to the auditor can result in severe penalties if they find a categorization is inappropriate. • In many if not most instances there is no cookie cutter approach to system design and operation which drives the categorization of facilities. Each responsible entity will make their classification of each facility based on system designs and operational considerations that are unique to their system and may likely differ among entities. The standard should not allow the auditors to dismiss the knowledge used to make the unique categorization levels. • PPL Affiliates believe the standard should be modified to remove the ability of the auditor to disregard categorizations made by responsible entities based on their first hand experience. If a baseline categorization is made (see above) the auditor should not be able to question a categorization but can review it for completeness. If a categorization change is ultimately made the auditor should not claim a violation of the requirement has occurred and no penalty should be assessed. • PPL Affiliates suggest removing from the VSL penalties for R1 for "incorrectly" classifying facilities. There is flexibility in the definition of High and Medium Impact facilities and the standards appear to recognize that system design and operation are in many instances not identical across the industry. A medium impact facility in one utility may be a high in another due to design and operation. Giving the audit

team the ability to change classification and then assess potentially a severe violation determination along with penalties is not appropriate for at least the short run where responsible entities are gaining experience in how the audit teams are viewing classifications. Different audit teams may view each classification differently. At least in the short run an “incorrect” classification of a facility should not be viewed as a violation. That language should be removed from the VSL table.
Yes
No
Yes
Yes
Yes
Yes
1.) PPL Affiliates require clarification on the R2 expectations of “documented cyber security policies” for the specific requirements of low impact assets which are not defined in the details in CIP-005, CIP-006, and CIP-007 whereas high and medium impact assets are. CIP-003 R2 should therefore explicitly clarify these expectations of low impact assets. 2.) PPL Affiliates have concerns with R2, and support the associated EEI comments noted below: EEI comments: EEI members are concerned regarding the potential need to discretely demonstrate compliance at the equipment level. The requirements are framed in a way that may lead an auditor to require discrete identification to adequately demonstrate compliance. This provides conflicting messages that could impede approval of protection controls for BES Cyber Systems used within High and Medium Impact facilities. Propose changing "For BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics" to "For BES Cyber Systems used in facilities not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics:
Individual
Marcus Freeman
North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency
No
Yes
The revised applicability criteria (located at Sections 4.2.1 and 4.2.2) for Load-Serving Entities (“LSEs”) and Distribution Providers (“DPs”) that may have under-frequency load shedding (“UFLS”) devices installed within their electric systems remain confusing and should be further clarified. Many LSEs and DPs participate in regional UFLS programs but contribute less than 300 MW of load shed (indeed, many such entities’ individual peak loads may be substantially less than 300 MW). Participation by these entities in regional UFLS programs may arise because a regional program directly requires LSEs and/or DPs to have UFLS programs. It may also arise because a contractual agreement between the LSE/DP and its Transmission Operator or Transmission Service Provider requires the LSE/DP to install UFLS relays and participate in the Transmission Operator’s or Transmission Service Provider’s UFLS program, which itself may have been developed to comply with a regional UFLS obligation and shed more than 300 MW of load, including a portion of the LSE/DP load. As currently proposed, the applicability criteria for LSEs and DPs suggests that their participation in any required regional program that sheds 300 MW or more subjects them to CIP-002-5, irrespective of whether equipment actually owned or operated by the LSE or DP itself is capable of shedding at least 300 MW. NCEMPA understands that the Standards Drafting Team has attempted to clarify this issue by adding the phrase “under a common control system” to the applicability language. However, “common control system” has not been defined or explained, and this terminology may have different meanings to different protection system engineers. If the applicability language related to UFLS equipment is not clarified, LSEs and DPs may not know what their compliance obligations are with respect to CIP-002-5, and Regional Entities may interpret and apply the applicability language differently in different regions or mistakenly apply the criteria to LSEs and DPs that the Drafting Team intends to be excluded from CIP-002-5. To remedy the ambiguity in the currently-drafted applicability criteria, NCEMPA and NCMPA1 suggests that the following formulation of the DP/LSE applicability language be adopted: Ownership or operation of equipment or devices that are (i) configured to perform automatic under-frequency or under-voltage Load shedding, without human operator initiation, (ii) capable of shedding a total of 300 MW or more of the LSE/DP’s load, and (iii) required

for compliance with a NERC or Regional Reliability Standard governing under-frequency or under-voltage Load shedding. Conforming changes to reflect the above-referenced modification to Section 4 should also be reflected in Attachment 1, Part 2.10. Additionally, examples of different load shed configurations would aid the industry in understanding the intended scope of the applicability criteria. The examples should make clear that only LSEs/DPs that are individually capable of shedding at least 300 MW of load are considered within the scope of CIP-002-5. Additionally, a second criterion applicable to DPs is unclear. Specifically, Section 4.2.2 provides that DPs with a “Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard” are subject to CIP-002-5. The specific Protection Systems that this criterion is intended to describe should be further explained. NCEMPA is aware that some industry participants may misinterpret this criterion to pertain to any transmission Protection Systems that are tested and maintained under PRC-005. However, PRC-005 does not require the installation of Protection Systems; rather, it requires Protection System testing and maintenance. Absent further explanation regarding the nature of this criterion, it should be eliminated. Finally, to the extent that the Drafting Team intends to retain the current applicability language and, consequently, for LSEs and DPs that own/operate relays that shed less than 300 MW of load to be subject to CIP-002-5, NCEMPA and NCMPA1 urges the Standards Drafting Team to revise Attachment 1 to classify Cyber Systems associated with UFLS/UVLS equipment as Low Impact, rather than Medium Impact. There is no obvious justification for small LSEs/DPs to be subject to the full panoply of requirements that apply to owners of Medium Impact assets.
Individual
Frank Dessuit
NIPSCO
No
No
1.1, 1.2 and 1.3 – The term “Used for” should be replaced with “that entity deemed essential”. 1.4- This standard should state “new or changes to a modified criteria rating needs to be compliant within 60 days of going into production”. M1- The measure and the requirement should read: “a list of changes to the BES (with a date for each change) that cause a change in the impact rating of the Facilities, Systems, or equipment from a lower to a higher impact category.” R2- Rationales should not be formally incorporated into the standard. Information in the rationale should be addressed as part of a non-binding informational document, e.g., a FAQ process. The rationale conflicts with the requirement time frames. (1 year vs 15 months).
Yes
Yes
Yes
Yes
Yes
Yes
Group
BC Hydro
Patricia Robertson
No
No
1) The new “bright line” method complicates the process the Registered Entities will need to go through to identify those cyber assets that are critical to the reliability of the BES. It limits the Registered Entity’s ability to apply rational judgement in identifying CCAs that was available in versions 1 to 3. 2) The high and medium impact asset descriptions, in general, need to be rewritten. Upon initial review, BC Hydro found it difficult to understand what assets would need to be identified based on the new criteria. It is recommended that one or two examples be provided for each as to what types of assets the criteria is referring or provision of a guideline document. 3) The term "adversely impact" is not clearly defined. 4) Suggest changing wording “would, within 15 minutes,

adversely impact" to "could adversely impact." There is a significant difference between would and could. At what point does the clock start ticking to determine the 15 minute timeframe? 5) The "15 minute" time limit seems arbitrary; how was this number arrived at; why not 20 minutes? 6) The term "interconnection" needs to be more clearly defined. 7) Prescribing calendar year not to exceed 15 months overrides an entities own definition of annual per NERC's CAN-008 and could lead to violations
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Heather Laws
Portland General Electric
No
Yes
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
Yes
Yes
Yes
Yes
Yes
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
Individual
Michael Falvo
Independent Electricity System Operator
Yes
Yes
Yes
Yes
No
No
No
No
Although IESO agrees with the requirements outlined in CIP-003, R3, we believe the definition of the NERC Senior Manager needs to include the ongoing compliance related responsibilities of the role, specifically to identify the operation and maintenance of the standard requirements. IESO believes

that the CIP-003-5, R6, M6 needs to be clarified and reworded.
Individual
Cristina Papuc
TransAlta Centralia Generation LLC
No
TransAlta recommends removing the criterion 2.11 (2), “control an aggregate highest rated net Real Power capacity of the preceding 12 calendar months equal to or exceeding 300MW or more of BES generation”, because TransAlta does not believe that there are technical basis provided consistently to categorize the generation Control Center as the medium impact. The details are, 1. TransAlta believes “The value of 300 MW is the same value used for UFLS and UVLS” as mentioned in the guidelines and technical basis section of CIP-002-5 (the first paragraph in Page 28), is inappropriate justification for medium impact. 300 MW number in the UFLS and UVLS is irrelevant to the impact level of generation Control Center. As TransAlta commented on the draft 1, “The UVLS and UFSL are triggered by the voltage and frequency, not directly by the generation loss.” In the draft 1 comment records, Robert Mathew from Pacific Gas and Electric Company also raised the same issue about using 300MW, i.e. “300MW of in many cases does not qualify as significant impact. Also 300 MW of generation should not be equated to 300 MW of UFLS/UVLS.” 2. In the SDT response to the TransAlta requests for additional clarify, it says “The intent of this criterion is to include all generation Control Centers.” However, there is no technical justification of this intent in any document. Without technical justification, TransAlta does not agree to this intent. 3. The intent to categorize all generation Control Centers as medium impact has the technical deficiency. The loss of a single 500MW unit generation (not meeting any criteria 2.3 and 2.6) controlled by a control room would have a low impact according to the criteria 3 while a loss of Control Center controlling 300MW generation(not meeting criteria 2.3 and 2.6) would have a medium impact according to the criterion 1.12. This does not make sense in regards to the loss of generation capacity. 4. In the SDT response to the TransAlta requests for additional clarity, the second sentence is confusing when talking about excluding some Control Centers. On one side, it recognizes these facilities as generation Control Centers “because they control geographically dispersed locations”. On the other side, these facilities “function more as a single generation facility control room”. So are these facilities really generation Control Centers or control rooms? This response creates more confusion between the Control Center and control room. 5. There is no consistency in justification of generation Control Centers as medium impact. In the SDT response to the TransAlta requests for addition clarity, the 300MW is picked for the purpose to excluding certain generation Control Centers, “…300MW specifically in consideration of those generation Control Centers….” However, in the guidelines and technical basis section, the 300 MW is picked, “the same value used for UFLS and UVLS.” So the reasons to pick 300MW are not consistent.
Group
IRC Standards Review Committee
Christine Hasha
No
Yes
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding CIP-002-5, question 3. The IRC respectfully provides these additional comments. Regarding Requirement 1, the IRC requests that specific language be added describing the standards applicable to third party functions, and information within those standards, that are relevant to criticality determinations under CIP-002-4 Attachment 1 criteria 2.3 and 2.6. This will facilitate uniform application of criticality determination under Attachment 1 criteria 2.3 and 2.6, which, in turn, will support efficient and effective application of CIP-002-5.
Yes
Yes
Yes
Yes
Yes
Yes

The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding CIP-002-5, question 10. The IRC respectfully provides these additional comments. Regarding CIP-003-5 R3 (question 6), the IRC requests revising the measure to, “Evidence may include, but is not limited to, a dated approval by the CIP Senior Manager, listing named personnel, by name or title, who are delegated the authority to approve or authorize specifically identified items.” Approved is the term used in the requirement language. Regarding CIP-003-4 R4 (question 7), the IRC requests revising item 2 in the measure to, “A dated approval by the CIP Senior Manager for each cyber security policy that indicates annual approval.” Approval is the term used in the requirement language.
Group
Texas RE NERC Standards Review Subcommittee
Brenda Hampton
No
No
(1) The Background section or Application Guidelines of CIP-002-5 should provide more discussion and detailed examples of the BES Cyber System concept. Multiple examples should be provided to address typical Responsible Entity configurations. This broader understanding will aid personnel in compliance decisions and, later, in the appropriate development of Reliability Standard Audit Worksheets (RSAWs). (2) We agree with the SDT that there is no need to have a discrete list of Low Impact Cyber Systems/Assets as stated in R1.3. However, the wording in Attachment 1 is in conflict with R1.3. To resolve the contradiction and provide clarity, revise R1 and Attachment 1 as follows. In Requirement R1.2, add qualifier “For each High Impact Facility, System or equipment, identify…” In Requirement R1.3, add qualifier “For each High or Medium Impact Facility, System or equipment, identify…” On Attachment 1, under High Impact Rating (H), change “Each BES Cyber System used by and located at” to “The following Facilities, Systems or equipment”. Under Medium Impact Rating (M), change “Each BES Cyber System, not included in Section 1, above, associated with the following” to read “Facilities, Systems or equipment, not included in Section 1, above, associated with the following”. Under Low Impact Rating (L), remove “Each BES Cyber System associated with:”. Once a facility is identified as Low Impact, there should be no need to further identify individual Cyber Systems in that facility as High, Medium, or Low. (3) Revise Attachment 1, Item 2.8 “Transmission Facilities providing the generator interconnection…” to read “generation interconnection facility...” This term was developed under Project 2010-07. This is an important distinction as Transmission Facilities are subject to all TO/TOP requirements, while a generation interconnection facility is subject only to a selected subset. (4) Attachment 1, Item 2.11 (2) should be removed. Item 2.11 (2) classifies “Control centers and associated data centers not included in the High Impact Rating (H), above, that…control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.” Inclusion of these control centers has been justified by the drafting team as analogous to the automatic load-shedding item (2.10), although in the source direction, not the sink. However, the difference is extensive. A compromised automated load shedding system will lead to an immediate loss in service. A generator control center can deploy other compensating measures before the impact is noticed. In addition, the loss in 300 MW of load has deep historical ties to reliability – a connection captured in DOE and NERC Disturbance reporting. Conversely, the loss of generation is historically tied to Interconnection reserve capability – which aligns with the 1500 MW number used in Item 2.1. We have not seen data that indicates that a control center controlling 300 MW of aggregated generation poses an additional reliability risk that would justify the cost of implementing over 100 CIP requirements. Furthermore, we have not seen a FERC directive calling for it. We recommend that the sentence be stricken to allow the industry to focus on the truly critical systems. Further, we agree with the concepts discussed in TransAlta Centralia Generation’s request for clarification. Justification and supporting information should be provided when identifying specific thresholds of MW capability or other similar criteria in defining BES Assets.
Yes
No
No
Yes
No

No
(1) Consider changing the word “topics” in R. 1 and other places to “elements” since the 10 identified areas are elements of the Cyber Security Program. (2) In Requirement R1, 1.10, consider changing the word “declaring” to “identifying”. (3) In Requirement R2, replace “BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics:” with “Each Responsible Entity shall implement one or more documented cyber security policies to address the following topics for BES Cyber Systems of low impact:” (4) To reduce ambiguity in determining reasonable evidence for meeting requirement R2, consider adding additional detail to M2 such as: M2.1 Evidence may include, but is not limited to, policies that address periodic high-level training, less formal reviews with appropriate personnel, or the posting of cyber security policies on the corporate Intranet site/company bulletin boards. M2.2 Evidence may include, but is not limited to, policies that address operational or procedural controls which restrict physical access. M2.3 Evidence may include, but is not limited to, policies that address operational or procedural controls which restrict electronic access. M2.4 Evidence may include, but is not limited to, policies that address identification and reporting of BES Cyber Security Incidents. (5) Consider combining the R6 content applicable to naming the CIP Senior Manager with R3. This will eliminate ‘double jeopardy’ concerns where failure to adequately document changes will now result in the violation of only a single requirement. Suggested wording: “Each Responsible Entity shall identify a CIP Senior Manager by name. Any changes to the CIP Senior Manager shall be documented within thirty calendar days of a change.” (6) Consider combining the R6 content associated with delegations with R5 to eliminate ‘double jeopardy’ concerns. Suggested wording: “Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate and the date of the delegation, and approved by the CIP Senior Manager. Each Responsible Entity shall document any changes to delegations within thirty calendar days of the change. Delegation changes do not need to be reinstated with a change to the delegator.”
Individual
Steven Powell
Trans Bay Cable
No
Yes
Criteria 2.11 categorize all TOP Control Centers as Medium impact on BES. This criteria is too inclusive and includes control centers of low impact TOP’s. This result in the applicability of security controls that are not at all aligned with the risk that these control centers (dispatch control centers) could have on the BES. To avoid this situation 2.11 should align with 2.5 but instead of focusing on a single station or substation; consider all of the facilities that the control center controls. If the total aggregate value of all transmission facilities does not exceed a value of 3000 (see 2.7) the control centers should not be designated as Medium impact. Therefore 2.11 would read Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners with a “total weighted aggregate value” that exceeds 3,000 for all Transmission Facilities controlled by the Control Center per criterion 2.5.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
G. Copeland
Pattern
Yes
We are concerned with Attachment 1, 2.11 - Control Centers and associated data centers controling and monitoring generation resources at an aggregate rated net RealPower capability of 300MW or

more of BES generation appears not sufficiently justified. If a control center were to monitore and control 10x (aggregate) 30 MW generation facilities that are interconnected to the BES system (although it is currently not clear if this meets the term "BES generation") it is not clear how such a Control Center becomes critical enough to the BES to be rated at medium impact particularly if all of these facilities are intermittend resources and neither facility would even be considered critical enough on its own that it had to be on the NERC Compliance Registry. And even if the (IPP) facilities are large enough in scale to meet NERC registration criteria they are usually still not critical enough for the individual region/are to have a significant impact since the individul facility cannot guarantee generation/capacity due to the nature of the fuel source. None of these IPP facilities are considered reliability facilities (Reliability Must Run, Resource Adequacy facilities, Black Start etc) and since Black Start Resources are rated as Low Impact it becomes even more difficult to follow the argument that an aggregate 300 MW of generation at a Control Center is a sound technical justifiction as criteria for Medium Impact Rating. It is also difficult to understand the justification how a Control Center of aggregate 300 MW IPP resources can compare to the impact a TOP/BA Control Center has on the BES. Finally, the loss of a single 500MW unit generation (not meeting any criteria 2.3 and 2.6) controlled by a control room would have a low impact according to the criteria 3 while a loss of Control Center controlling 300 MW generation(not meeting criteria 2.3 and 2.6) would have a medium impact according to the criterion 1.12. This does not make sense in regards to the loss of generation capacity. Since the term Control Center is not in the current NERC Glossary I would appreciate to maintain in the draft standard a reference/ clarification on generation Control Center, control room and "controling" generation to help clarify which facilities would fall under the category defined by 2.11.
No
Yes
Individual
Chris de Graffenried
Consolidated Edison Co. of NY, Inc.
1. Section 4.2 of CIP-002-5 should explicitly state that UFLS Systems that perform automatic load shedding of less than 300 MW are specifically excluded. 2. Requirement 1.2 of CIP-002-5 should be revised to use the same language as Attachment 1: FROM: Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; TO: Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used BY AND LOCATED AT the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; 3. Requirement 1.3 of CIP-002-5 should be revised to use the same language as Attachment 1: FROM: Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; TO: Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) ASSOCIATED WITH the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;
Individual
Edward Bedder
Orange and Rockland Utlities Inc.
1.Section 4.2 of CIP-002-5 should explicitly state that UFLS Systems that perform automatic load shedding of less than 300 MW are specifically excluded. 2.Requirement 1.2 of CIP-002-5 should be revised to use the same language as Attachment 1: FROM: Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; TO: Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used BY AND LOCATED AT the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; 3.Requirement 1.3 of CIP-002-5 should be revised to use the same language as

Attachment 1: FROM: Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; TO: Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) ASSOCIATED WITH the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;
Individual
Michael Jones
National Grid
No
Yes
We recommend the following wording for R 1.2 (we moved “high impact to be in front of Facilities): 1.2. Identify each BES Cyber System and its associated BES Cyber Asset(s) used for the high impact Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; We recommend the following wording for R1.3 (we moved “medium impact” to be in front of Facilities): 1.3 Identify each BES Cyber System and its associated BES Cyber Asset(s) used for the medium impact Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; We also recommend that the CIP Process Flow on the last page be updated to show clearly that the identification of BES Cyber Assets should occur first, followed by identification of BES CYBER Systems.
Yes
Yes
Yes
Yes
Yes
Yes
Group
Southwest Power Pool Regional Entity
Emily Pennel
No
Yes
(1) Section 4.2.2, last bullet: All single points of failure in the cranking path should be protected from the black start resource (or injection point if the entity relies on cranking power from an adjoining entity) to the generation unit(s) to be started. Additionally, this section needs to be clarified as necessary to ensure that a Responsible Entity that elects to receive electric power from a neighboring entity as opposed to providing its own black start resource views the cranking path generation source as the point of injection (typically a tie substation) into the Responsible Entity’s transmission or distribution system. (2) Section 4.2.4.2 attempts to define exemptions for communication links, but fails to include the exclusion of end points to those circuits (see CIP-005/R1.3). (3) Throughout the standards, the phrasing “would affect” or similar is used. The requirements should be prospective and use the phrase “could” instead of “would.” The impact of a failure or compromise cannot always be predicted with certainty and entities could use the phrasing to argue that certain BES Cyber Systems do not meet the bright line criteria based on that lack of certainty. Use of “could” is consistent with the application guideline for R1 where the entity is expected to assume the vulnerability exists and that the probability is 100%. The standard needs to be precise in that regard; entities are not held to the expectations found in guidance. (4) The last paragraph on Page 7 leaves it up to the entity to determine the level of granularity when identifying the BS Cyber Systems and instructs the entity to take into consideration the operational environment and scope of management. First of all, what is reasonable? Left to the discretion of the entity, grouping of assets may be unreasonable, such as declaring the entire sets of unrelated assets in a data center as a BES Cyber System. Second, how is the operational environment and scope of management evaluated? Is this an auditable expectation?

(5) The SDT continues to insist there is no need to identify the low impact BES Cyber Systems and their associated Cyber Assets (e.g., R1.3). This causes an auditability issue. The auditor will want to understand all of the BES Cyber Systems and associated Cyber Assets evaluated by the entity in order to verify all high and medium impact BES Cyber Systems have been properly identified and classified. This can only be accomplished by having the entity produce a comprehensive list. (6) The example of “Electronic Access Control or Monitoring Systems” references Certificate Authorities. As strictly stated, this could be problematic if the entity relies upon a commercial Certificate Authority. In the same definition, it would be helpful to refer to the SIEM, SEIM, and SIM in addition to the SEM. Finally, in the same definition, it would be helpful to refer to “intrusion protection systems” as well. (7) The definition of Protected Cyber Assets should include local attached storage, network attached storage (NAS) and storage area networks (SAN). (8) In R1, reference is made to a time horizon. Please footnote the reference. (9) R1.1, R1.2, and R1.3 should also require the identified items to be documented. R1.4 allows identification information to be updated within 60 days of placing the element or facility into service. If this is a planned change, the identification should be completed as part of the planning and preparation prior to the operational or in-service date. (10) R1.4 includes a condition where the BES element or facility change causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category. You have to complete the R1.1, R1.2, and R1.3 identification in sequence, hence the condition is problematic. It would be better to require the identification process review to be performed and in a separate sentence, require the update if the condition is met. (11) M1 should require all changes to be documented to ensure nothing has been overlooked. (12) The rationale for R2 stipulates the lists from R1 are to be “reviewed.” This is inconsistent with the actual requirement to “approve.” (13) M2 references “review and update.” This is not in the requirement. (14) In the VSL for R1, the failure to identify even one “High” impacting BES Cyber System should be a “Severe” violation due to the potential risk. (15) The reference to “review” in the R2 VSL is not a requirement found in the language of R2. (16) Criteria 2.1 of Attachment 1 refers to an impact in 15 minutes. This is going to be very difficult for the entity to demonstrate during an audit. (17) Instead of referring to a 15 minute interval in Criteria 2.2 of Attachment 1, simply refer to BES Cyber Systems that operate the reactive resource(s). (18) Is the transmission facility referenced in Criteria 2.8 of Attachment 1 a substation (or switchyard) or something more granular? (19) Criteria 2.9 uses the phrase “would” instead of “could.” (20) In the guidance discussing Restoration of the BES, should “Coordination” be the responsibility of GOPs, TOPs, and RCs? (21) The first bullet in the guidance for the overall application of Attachment 1 allows the entity to determine the grouping of facilities. Entities should be required to group all facilities in a substation into one set for transmission. (22) The threshold in criteria 2.1 of Attachment 1 should regionalize the threshold to more approximately reflect regional operational conditions. (23) The criteria for categorizing a control center does not take into consideration the interconnectivity of the BES Cyber Systems as required in the FERC order approving Version 4 of the CIP standards. Any BA, TOP, or GOP control center that uses ICCP to exchange data with other entities should be categorized as High. The concept of mutual distrust does not work because ICCP communication is over a trusted path and there are sufficient vulnerabilities in the ICCP foundational code to be a high risk. (24) How was 1000 MVARs “deemed” to be reasonable? (25) for restoration facility criteria, consider categorizing black start resources required for starting adjoining entities “medium” while leaving self-starting entity’s black start resources as low. (26) Facilities in the cranking path for system restoration that are single points of failure should be categorized as Medium impact. (27) The criteria needs to address the situation where the Responsible Entity elects to receive cranking power from a neighboring utility as opposed to self-providing with its own black start generation resource. In that instance, the entity’s cranking path must be understood to begin at the point of injection, typically a tie substation, and not at a defined generation resource.
Yes
No
No
No
No
Yes
(1) R1 needs to be clarified that the cyber security policies need to support the requirements by meeting or exceeding the expectations of the requirement and not be contrary to the requirement elements. (2) R3 needs to be clarified as to whether the Senior Manager can be self-appointed. (3)

The appointment of the Senior Manager still needs to include the title or position of the individual to prevent ambiguity when there are multiple personnel with the same name. (4) An organization chart as evidence (referenced in M3) is not sufficient to document the appointment of the Senior Manager. In the absence of a specific “CIP Senior Manager” or similar title, there is no way to determine who the Senior Manager is on the organization chart. Additionally, as organization charts tend to regularly change, a dated organization chart does not adequately identify the date of appointment. This example of evidence should be removed from this requirement. (5) The Responsible Entities need to fully understand that the suggested evidence in M4 requires a dated signature, either physical (“wet ink”) or electronic, demonstrating the review and approval. An entry in the revision history typically precedes any approval action and therefore does not by itself adequately demonstrate approval or attest to such action. (6) R5 needs to be modified to require the delegation document to include the specific scope of the delegation. Doing so would then comport with the example evidence found in M5, which references “specifically identified items.” (7) The VSL for R4 needs to include a condition where not all of the security policies have been reviewed, irrespective of the approval of any of those reviewed. The Severe VSL language includes the condition where Responsibility has not reviewed the policies *AND* the Senior Manager had not approved all of the policies within the required time period. Perhaps the “and” should be changed to “or”. (8) The guidelines for R1 should include instructions that a high-level policy document should include referential links to the additional documentation for continuity and completeness. (9) It is not appropriate for the guidelines to instruct the independent auditor on how to audit the requirement. R2 requires the implementation of documented policies. Auditor discretion is necessary to determine how to audit compliance with the requirement to document and implement cyber security policies that meet the minimum expectations defined in the requirement. (10) The guideline for R5 references “delegation of the delegation authority.” This does not comport with the requirement itself, which requires all delegations to be approved by the Senior Manager. (11) The guidance regarding delegations of authority should include comments on documented revocation of delegated authorities and the need to specify the scope of the delegated authority.
Individual
Mario Lajoie
Hydro-Quebec TransEnergie
No
Yes
(1) No need for a bullet in 1.3 as it is a single element, not a list. HQT proposes that the text be included in the above section (2) Table of Compliance Elements - Moderate and High VSL - Entities with fewer than 40 facilities identified in R1 : 4 or 6 facilities not identified fall outside of the given intervals (“more than two, but fewer than four” and “more than four, but fewer than six” should be changed to “more than two but less than or equal to four” and “more than four, but less than or equal to six) (3) Table of Compliance Elements : Language added for RE with fewer or greater than 40 facilities in R1 is inconsistent with existing language. Recommend change to existing language to account for the shift from identifying BES Cyber Sytems to identifying Facilities (4) Attachment 1 parts 1.2 and 1.4 : Request clarification to whether or not the 1500 MW refers to criterion 2.1. If so, it should point directly to that criterion. (5) Attachment 1 parts 2.1 and 2.2 : The 15 minutes criterion is arbitrary, hardly measurable and adds confusion to whether or not a Cyber Asset should be considered. HQT recommends to remove the last sentence regarding the 15 minutes OR provide entities with a clear and repeatable methodology as a guideline to identify such systems. HQT considers that interpretation of those criteria can greatly differ from different entities which is not faithful to the “bright-line” concept. A bright-line criterion should not leave room for interpretation (6) Attachment 1 part 2.2 : It should specify “in absolute value” or “maximum variation of reactive power” to account for facilities that have for instance synchronous condenser (e.g. how a -250 to +300 MVAR nameplate value should be considered). (7) Attachment 1 part 2.3 : Considering there is no NERC standard requiring the PC or TP to inform GO and GOP of such facilities, how this criterion can be applied. HQT considers that this is not a “bright-line” criterion and recommends to remove it OR provide entities with a clearly defined and consistent way of identifying such facilities.(8) Attachment 1 part 2.10 : Considering multiple ways to apply or interpret this criterion, HQT recommends to specify the way to measure the load shedding capability by proposing this wording "Each System or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, with an aggregate lowest rated net Real Power capability

of the preceding 12 calendar months equal to or exceeding 300 MW or more, implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS), as required by its regional load shedding program.". Rationale: A facility should be considered medium impact BES Asset when its minimum shedding load capability is kept all year long over 300 MW, meaning we can always rely on at least 300 MW as the last layer of defense to avoid collapsing of the grid.
Yes
Yes
Yes
Yes
Yes
Yes
We agree with the comments provided by the NPCC TFIST
Individual
Thomas A Foreman
Lower Colorado River Authority
Yes
Yes
Yes
No
Yes
Yes
Yes
Yes
R2: to match the rest of the proposed language, the VRF for R2 should be “Lower” to match the standard language (p. 9) and in the text it should also be changed to “Lower” instead of “Medium” (p. 14).
Group
NRG Companies
Alan Johnson
Yes
No
Revise Attachment 1, Item 2.8 “Transmission Facilities providing the generator interconnection…” to read “generation interconnection facility...” This term was developed under Project 2010-07. This is an important distinction as Transmission Facilities are subject to all TO/TOP requirements, while a generation interconnection facility is subject only to a selected subset. Attachment 1, Item 2.11 (2) should be removed. Item 2.11 (2) classifies “Control centers and associated data centers not included in the High Impact Rating (H), above, that…control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.” We have not seen data that indicates that a control center controlling 300 MW of aggregated generation on more than one physical footprint (such as control of small remote sites which would be low impact) poses an additional reliability risk that would justify the cost of implementing over 100 CIP requirements. . Furthermore, we have not seen a FERC directive calling for it. We recommend that the sentence be stricken to allow the industry to focus on the truly critical systems. Finally, for generation control centers the BES Cyber systems should be considered only if they are shared at the central location, and not inclusive of all systems resident within the control center. This should be empirically clear.
Yes
No
Yes
Yes
No

No
In Requirement R2, replace “BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics:” with “Each Responsible Entity shall implement one or more documented cyber security policies to address the following topics for BES Cyber Systems of low impact:” Requirement 2 does not provide any specifics for providing guidance for compliance and/or audit. To reduce ambiguity in determining reasonable evidence for meeting requirement R2, consider adding additional detail to M2 such as: M2.1 Evidence may include, but is not limited to, policies that address periodic high-level training, less formal reviews with appropriate personnel, or the posting of cyber security policies on the corporate Intranet site/company bulletin boards. M2.2 Evidence may include, but is not limited to, policies that address operational or procedural controls which restrict physical access such as card key, special locks, security personnel, or other authentication methods. M2.3 Evidence may include, but is not limited to, policies that address operational or procedural controls which restrict electronic access from public or other less trusted network zones through proxy servers, DMZ, password protections, or other authentication methods. M2.4 Evidence may include, but is not limited to, policies that address identification of BES Cyber Security Incidents and the reporting of cyber intrusions to ES-ISAC.
Individual
Eric Scott
City of Palo Alto
Section 4.2.2, Bullet 3 states: “A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard.” Palo Alto is a small entity which has no critical cyber assets. Palo Alto is concerned that this language may be intrepreted such that Palo Alto could be determined to have critical cyber assets. Palo Alto requests that the SDT clarify which “Protection Systems” it is referring to in this bullet. Palo Alto requests that for each "Protection System" the SDT identify the NERC or Regional Reliabity Standard that establishes the requirement for each "Protection System" and that this information be included in the guidance.
Yes
Individual
Ed Nagy
LCEC
No
No
Comments: 1) Attachment 1 criterion 2.11 categorizes all Transmission Operator (TOP) and Transmission Owner (TO) Control Centers as Medium impact to the BES. This criterion is too inclusive as it includes Control Centers of low impact Radial Transmission Owners and Operators unnecessarily. This results in the applicability of security controls that are not at all aligned with the risk that these Control Centers could have on the BES. To avoid this situation, Criterion 2.11 could be aligned with criterion 2.5 but instead of focusing on a single station or substation; consider all of the facilities that the Control Center controls. If the “total aggregate value” of ALL Transmission Facilities does not exceed a value of 3,000; the Control Centers should not be designated as Medium impact. For Example: 2.11. Control Centers not included in High Impact Rating (H), above, that (1) perform the functional obligations of the Balancing Authority (2) perform the functional obligations of Transmission Operator with a “total weighted aggregate value” that exceeds 3,000 for ALL Transmission Facilities controlled by the Control Center per criterion 2.5; or (3) control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation. The point that must be stressed here is that if ALL of the Transmission Facilities being operated by the Transmission Operator COMBINED DO NOT justify a BES impact rating of Medium, how can the Control Centers be considered Medium impact? Comment: 2) Attachment 1 criterion 2.10 should include the word AND after the first portion of the criterion that details the capabilities of the system to qualify for inclusion under this criterion. (e.g. automatic load shedding, common control system, without human operator initiation). Without making this change, there is a chance that this criterion will be misinterpreted to include a collection of discreet relays who’s sum exceeds 300MW which is not the intent and has been verified by NERC. For example: 2.10 Each System or group of

Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more AND implements Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS), as required by its regional load shedding program. Comments: In CIP-002-5 Attachment 1 section 2.11 the term “associated data centers” has been introduced without it being clearly defined. One might assume that this is referring to the data centers that contain BES Cyber Systems and Assets only but this is not clear. Data centers that are owned by the entity but do not contain BES Cyber Systems or Assets could be interpreted by an auditor as being “associated” due to network connectivity that exists outside of the ESP. Recommend removing the term “associated data centers” from the standard as it does not add any additional value or context that is not already addressed by other ESP & PSP requirements.
Yes
No
Yes
Yes
Yes
Yes
Comments: Requirement 1.10 was added to address CIP Exceptional Circumstances. This definition is defined but is too broad. It includes safety related issues and response by emergency services for example. It is difficult to determine the appropriate scope of what should be included in the security policies as a result of this.
Individual
Robert Mathews
Pacific Gas and Electric Company
No
Yes
Attachment 1 Criteria 2.11 is not acceptable because there is no technical basis for the 300 MW threshold for inclusion of Control Centers and associated data centers as Medium under 2.11 “2) control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.” Rationale: The 300 MW of generation threshold in 2.11 is apparently derived from the 300 MW in 2.10 relating to UFLS/UVLS. 300 MW of generation should not be equated to 300 MW of UFLS/UVLS. While the loss of load may have similar impacts as loss of generation in a general sense, equating the “last ditch efforts to save the BES” provided by UVLS/UFLS is not in the same as any loss of load or any loss of generation. Automatic Generation Control (AGC), spinning reserve, etc. are mechanisms to make up for lost generation, which are not “last ditch”. Suggest Standard Revisions: 2.11. Control Centers and associated data centers not included in High Impact Rating (H), above, that perform the functional obligations of Balancing Authority or Transmission Operator.
Yes
Yes
Yes
Yes
Yes
Yes
Guidelines and Technical Basis for R1.4 Bullet 3 on page 18 still includes egress. Suggest striking egress to conform with changes to CIP-006.
Group
Duke Energy
Greg Rowland
No
Yes
(1) Section A Introduction. 1. Title currently says, “Cyber Security – BES Cyber System Categorization”. This is not the same as the heading in the document which says, “Cyber Security – BES Cyber Asset and BES Cyber System Categorization”. Duke suggests changing the title in A1 to

read the same as the header. (2) Section A Introduction. 4.2.4.3 currently says, “In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.”. This incorrectly assumes that all regulated devices by the NRC are inside the boundaries of a nuclear plant. Duke suggests rewording to the following, “The Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.”. This will provide the exemption for any devices regulated by the NRC, regardless of their physical location. NOTE that this comment applies to ALL CIP Standards CIP-002-5 through CIP-011-5. (3) Section A Introduction. Background section “Reliable Operation of the BES”. The sentence “In order to identify them, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for functional entities in the NERC Functional Model” is incorrectly stated. The NERC Functional Model identifies functions and not functional entities. Duke suggests rewording this sentence to read, “In order to identify them, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to the reliability tasks identified for functions in the NERC Functional Model.”. (4) Requirement R1 - It would be helpful to clarify that BES Cyber Systems inherit their impact rating from the facility by describing them as “BES Cyber Systems of a high impact facility”, for example, rather than “high impact BES Cyber Systems”. This will avoid the confusion of whether a Cyber System requires its own impact rating independent of the facility. By Enhancing the CIP process flow on page 33 to indicate that the assets inherit the impact of the facility, there may be greater industry approval. As it currently exists, the process flow has as its first box the identification of BES Cyber Assets and BES Cyber systems. This first box should capture the identification of facilities that satisfy the impact criterion. Duke supports EEI’s suggestions that this process flow be enhanced, and possibly moved to the requirements section to provide a prescriptive methodology to ensure this “facilities first” approach provides clear directives to the industry. (5) Requirement R1 - Rather than the current approach to identify “Facilities, Systems, and equipment,” modify this to identify High Impact Sites, Medium Impact Sites with all BES Sites not identified as High Impact or Medium Impact being identified as Low Impact. For Low Impact, maintaining inventories at the site level would avoid the concern that discrete equipment identification is required. Duke supports EEI’s comments on this. (6) Requirement R1.3 – Duke suggests that the bulleted item that appears in R1.3 should be removed. With the proposal in (5) stated above, if the Low Impact Sites have already been identified, there is no need to have a requirement NOT to list the BES Cyber Systems at those sites. The requirement should only be that Low Impact Sites have been identified, therefore discrete identification of the Low Impact BES Systems would never need to be addressed. (7) Requirement R1.4 – Duke suggests deleting this requirement. The current wording of R1.4 would require the full list of facilities and systems to be reviewed every time a change is made to BES Elements or Facilities. In a larger company, this is a continuous process and would require constant review of the lists. Duke feels that the Implementation Plan adequately covers the need to monitor for entities to monitor for changes to their BES Elements or Facilities such that compliance can be met for any newly categorized BES Cyber System. (8) Measure M1. Duke suggests that the standard verbiage in front of every measure be changed from “Acceptable evidence includes, but is not limited to” to “Non-prescriptive examples are”. Duke believes this more adequately demonstrates that the measures are examples, and should not be the minimum which would be needed to demonstrate compliance with any particular requirement. NOTE that this comment applies to ALL CIP Standards CIP-002-5 through CIP-011-5. (9) Attachment 1, statement under Header 1 “High Impact Rating”. Duke suggests that the following sentence be removed, “Each BES Cyber System used by and located at:” as Duke is proposing, per (5) above, that sites be assessed against the criteria within Attachment 1. (10) Attachment 1, statement under Header 2 “Medium Impact Rating”. Duke suggests that the following sentence be removed, “Each BES Cyber System, not included in Section 1, above, associated with the following:” as Duke is proposing, per (5) above, that sites be assessed against the criteria within Attachment 1. (11) Attachment 1, Criterion 2.1. This criterion currently contains information for assessing BES Cyber Systems, which is no longer appropriate, per Duke’s proposal in (5) above, when categorizing sites. Duke suggests that the language, “For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equate or exceed 1500 MW in a single Interconnection.” be removed. This 15 window is already implied in the definition of BES Cyber Assets and doesn’t need to be re-stated here. (12) Attachment 1, Criterion 2.5. It is unclear how to treat a double circuit line in this criterion. Please clarify how a

double circuit line (i.e., two circuits connected between the same substations and referred to as a line) should be treated when calculating the “aggregate weighted value” of a Transmission Facility. If the intent was to assign weight per each circuit, change the last sentence of the criterion to “The aggregate weighted value for a Transmission Facility is determined by summing the “weight value per circuit” shown in the table below for each circuit leaving the station that is connected to another Transmission station or substation”. Change the title of the second column in the table to “Weight Value per Circuit”. (13) Attachment 1, Criterion 2.3. The phrase in this criterion, “in the planning horizon of more than one year” is confusing – it is not clear when the one year is measured from. Duke proposes the phrase to change to “with a duration of more than one year in the planning horizon.”. (14) Attachment 1, Criterion 2.10. The wording in this criterion changed from “Each System or Facility” in version 4 to “Each System or group of Elements”. This could be read to include individual, unconnected relays that have a common trip set point. Duke suggests the following rewording to clarify it is control system and not individual relays. “Each System or group of Elements that performs automatic Load shedding under a single common control system (excluding individual, unconnected relays), without human operation initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS), as required by its regional load shedding program. (15) Attachment 1, statement under Header 3 “Low Impact Rating”. Duke suggests that the following sentence be removed, “Each BES Cyber System, associated with:” as Duke is proposing, per (5) above, that sites be assessed against the criteria within Attachment 1. (16) Attachment 1, criteria 3.2 and 3.3. Duke suggests moving these criteria back to the Medium Impact classification. Duke does not agree with the assertions that having this criteria in Medium Impact would cause entities to remove facilities from their restoration plans in order to lessen the compliance burden associated with CIP. Duke believes that the basis for the impact any facility has on the reliability of the BES, should be unassociated with the compliance aspects. Blackstart resources should be appropriately represented as having a medium impact to the overall reliability of the BES.
No
No
No
No
No
Yes
(1) Requirement R1.3. The list of sub-requirements under R1 all appear to align with the set of CIP standards with the exception of R1.3. Interactive Remote Access is covered under the other sections like “Electronic Security Perimeters” and “System Security” and should need to be called out specifically. Duke suggests removing R1.3 as a way to better align this list with the remainder of the CIP standards. (2) Requirement R2. Duke suggests rewording this requirement for better readability. Rather than stating the requirement as a negative, Duke suggests the following replacement language, “For Low Impact BES Cyber Systems, each Responsible Entity shall implement one or more documented cyber security policies that addresses the following topics.”. (3) Requirement R2. Duke suggests rewording the last statement of the requirement, after the sub-requirements have been listed to, “An inventory, list, or discrete identification of Low Impact BES Cyber Systems is not required.” Without the “Low Impact” phrase, this could incorrectly be applied to any BES Cyber Systems which is assumed to not be the intent. (4) Requirement R3. Duke suggests rewording this requirement to “Each Responsible Entity shall identify the role of CIP Senior Manager by name.” Duke is suggesting this change as the current wording may be interpreted to mean that auditors would be looking for someone with the job title of CIP Senior Manager. Entities should be given the explicit permission to identify the CIP Senior Manager by role at a minimum, without necessarily creating a title. (5) Measure M3. The guidance portion related to M3 provides some details that Duke suggests would be better included in the actual language of M3. This language is referring to the guidance that dated/signed approvals, designations, etc can be electronic or hardcopy. (6) Measure M4. Duke recommends that consistency be applied to the way measures are formatted throughout the standard. Currently, some are bulleted (implying an OR statement in between them) and some are numbered (implying an AND statement in between them). If measures are intended to be non-prescriptive, all measures should be written consistently with bulleted items and “or” statements placed at the end of every bullet. NOTE that this comment applies to ALL CIP Standards CIP-002-5 through CIP-011-5. (7) Requirement R5. Duke is concerned with the last phrase of the requirement reading, “and approved by the CIP Senior Manager”. The current language suggests that the CIP

Senior Manager would have to approve his/her own delegations, while it should be implied that the naming of a delegation carries with it the approval of CIP Senior Manager. Duke suggests rewording this phrase to “as approved by the CIP Senior Manager” to lessen the burden of documenting an additional approval that shouldn’t be required.
Individual
Martyn Turner
LCRA Transmission Services Corporation
Yes
Yes
Yes
No
Yes
Yes
Yes
Yes
R2: to match the rest of the proposed language, the VRF for R2 should be “Lower” to match the standard language (p. 9) and in the text it should also be changed to “Lower” instead of “Medium” (p. 14).
Individual
Michelle R D'Antuono
Ingleside Cogeneration LP
No
Yes
Ingleside Cogeneration supports the greater part of the categorization criteria supplied in CIP-002-5-Attachment 1. However, we have a few major concerns which prevents us from entering a “yes” response in our ballot. The first is there should be one additional category added to the CIP Version 5 Standards, which should be “No Impact”. In the SDT’s Consideration of Comments document, the justification for eliminating this category was that it was a key feature of the NIST Risk Management framework. However, FERC Order 706 paragraphs 25 and 233 do not require strict adherence to NIST, only that the ERO strongly consider their application with respect to BES cyber security. We believe that the size and variety of programmable devices that support BES facilities is far outside of the practical application of the NIST framework – which should be directed at the most vulnerable systems first. Otherwise industry and compliance resources will be overwhelmed with tracking adherence in small systems, to the detriment of the larger ones. In addition, the text in Item 2.8 calls for a Medium-Impact categorization of certain “Transmission Facilities providing the generator interconnection…”, this terminology is inconsistent with that developed under Project 2010-07, which uses “generation interconnection Facility” instead. This is an important distinction, because a Transmission Facility is subject to every TO/TOP requirement, while a generation interconnection Facility is subject to a special subset only. It took a long time for the GOTO team to craft acceptable language, and we recommend it to be used here. We also disagree with Item 2.11, which assigns a Medium-Impact rating for “Control Centers and associated data centers not included in High Impact Rating (H), above, that: … control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.” This has been justified by the drafting team as analogous to the automatic load-shedding item (2.10), although in the source direction, not the sink. However, the difference is extensive. A compromised automated load shedding system will lead to an immediate loss in service. A generator control center can deploy other compensating measures before the impact is noticed. In addition, the loss in 300 MW of load has deep historical ties to reliability – a connection captured in DOE and NERC Disturbance reporting. Conversely, the loss of generation is historically tied to Interconnection reserve capability – which aligns with the 1500 MW number used in Item 2.1. We have not seen data that indicates that a Control Center controlling 300 MW of aggregated generation poses an additional reliability risk that would justify the cost of implementing over 100 CIP requirements. Furthermore, we have not seen a FERC directive calling for it. We recommend that the sentence be stricken to allow

the industry to focus on the truly critical systems.
Yes
No
Yes
Yes
Yes
Yes
Ingleside Cogeneration LP is very supportive of the reduction in the requirements applicable to Responsible Entities with identified Low-Impact BES Cyber Systems. The volume of new CIP policies that will be need to be developed and implemented is enormous – and should be approached at a high level initially. Over time, future versions of CIP-003 can require more detail, provided they are vetted through the Standards Development Process. However, we are concerned that there is too much leeway for interpretation in the language of the requirements and the associated text in the "Guidelines and Technical Basis". R2 only calls for policies which "address" four specific topics in Low-Impact policies, but no limits are given. The guidelines express the intent to "outline a set of basic protections", but is offset by a statement that "cyber security policy must cover in sufficient detail the 4 topical areas". In order to eliminate any ambiguity which will serve to incentivize the development of CANs, we suggest the following language to be added to R2.1 through R2.4: 2.1 Cyber security awareness. Acceptable policies will address periodic high-level training, less formal reviews with appropriate personnel, or the posting of cyber security policies on the corporate Intranet site/company bulletin boards. 2.2 Physical access control. Acceptable policies will address operational or procedural controls which restrict physical access such as card key, special locks, security personnel, or other authentication methods. 2.3 Electronic access control. Acceptable policies will address operational or procedural controls which restrict electronic access from public or other less trusted network zones through proxy servers, DMZ, password protections, or other authentication methods. 2.4 Incident response to a BES Cyber Security Incident. Acceptable policies will address high-level training to identify BES Cyber Security Incidents and the reporting of cyber intrusions to ES-ISAC.
Individual
Joe Petaski
Manitoba Hydro
No
Yes
"…associated data centers" in Attachment 1 -1.1, 1.2, 1.3 and 1.4 are unclear. It needs to clarify what degree of the communication or connection between associated data centre and a control centre is deemed to be an associated data centre, otherwise, it can be very broad.
Yes
Yes
Yes
Yes
Yes
Individual
Kayleigh Wilkerson
Lincoln Electric System
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Group
Arizona Public Service Company
Janet Smith
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Michael Schiavone
Niagara Mohawk (dba National Grid)
No
Yes
We recommend the following wording for R 1.2 (we moved “high impact to be in front of Facilities): 1.2. Identify each BES Cyber System and its associated BES Cyber Asset(s) used for the high impact Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; We recommend the following wording for R1.3 (we moved “medium impact” to be in front of Facilities): 1.3 Identify each BES Cyber System and its associated BES Cyber Asset(s) used for the medium impact Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; We also recommend that the CIP Process Flow on the last page be updated to show clearly that the identification of BES Cyber Assets should occur first, followed by identification of BES CYBER Systems
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Yuling Holden
PSEG
No
Yes
Attachment 1 section 1.4 and 2.11 contains the undefined word “control.” PSEG believes “control” must be clarified to ensure it is consistent with the description under the BES reliability operating service “Monitoring and Control” in the latest version of CIP-002-5, p. 23. The Control Center definition, which uses the phrase “monitor and control,” should also capture aspects of in a manner consistent with what is included under Monitoring and Control service (i.e. all methods of operating breakers and switches, SCADA, and substation automation). Additionally, in the CIP-002-5 v5, p. 24, the BES reliability operating service “Situational Awareness,” as written, could inadvertently capture monitoring and alerting activities that are performed for general management and economic / market

decision making. For example, monitoring EMS status information and alarms by areas that do not have the physical or automated control of the equipment; and the authority to change a generating asset's output should be excluded to ensure they are not inadvertently captured in the application of this standard.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Jonathan Appelbaum
United Illuminating Company
Yes
Yes
UI Agrees with EEI Consensus comments. In addition for R1.4 does within 60 days mean plus or minus 60 days or at least 60 days prior to being placed into operaton. Second Comment is referring to Guidance in CIP-002 for identifying Transmission Owner assets that are being used by a Transmission Operator to perform the TOP functional obligation. (1) UI believes the guidance should be specific as to whether the performance of remote switching by a Transmission Owner from its control center under the direction of the Transmission Operator is performing a functional obligation of the TOP. (2) Similarly, in an Emergency the TOP may direct its Transmission Owners and Distribution Providers to perform manual load shed, would this cause the Transmission Owner Control Center to come into scope as performing a functional obligation of the TOP. (3) If Data from a medium impact substation passes to Transmission Owner data center on the Transmission Owner network, and is then sent to an ICCP server to its TOP and RC is the data center performing the functional obligation of the TOP. Third Comment relates to Technical Guidance for the application of CIP-002 which should provide increased clarity on the acceptability of segmenting facilities at a single site to achieve tiering of impacts. The present explanation on page 25 of 33, first bullet, describes separating transmission equipment from distribution equipment. The explanation should allow for separation of Transmission Facilities as well. For example, assume a transmission substation where two 500 kV lines connect, two 345 kV lines connect and six 115 kV lines. The 500 kV lines would cause the site to be categorized as Medium Impact. We propose that only the 500 kV Facilities would be categorized as Medium Impact and the 345 kV Facilities and 115 kV Facilities would be Low Impact. With proper cyber network segmentations it is achievable to separate the BES Cyber Systems associated with the 500 kV medium impact facilities from the BES Cyber Systems associated with the 345 kV and 115 kV Low impact facilities.
Yes
Yes
Yes
No
Yes
Yes
UI concurs with EEI consensus comments. In addition, R1 requires implementation of the Policies. The entire suite of CIP standards is the implementation of processes to comply with the standards and the Policy. Implementation of Interactive Remote Access Policy required by CIP-003 1.3 is what the Requirements in CIP-005 and CIP-007 is accomplishing. If the other CIP standards were not in existence then we can understand the need to require implementation of the Policies. The requirement requires proof of implementation which means duplicating the evidence submissions for the entire sutie of CIP Standards.The Rationale box states this requirement is about demonstrating management's supports the cyber security program. The Guidelines does not clarify or explain what implementation means. UI suggests the phrasing Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall have one or more documented cyber security policies that

address the following topics. For R2 it is appropriate to keep implementation because the other CIP Standards do not address BES Cyber Systems associated with Low impact Facilities. For R4 We believe the use of reviewed and approved is unnecessary. We believe that the requirement should only be for approval. The completion of the review is attainment of the Senior Manager's approval. We do not believe that the drafting team desired to track the review periodicity separate from the approval periodicity.
Individual
John Souza
Turlock Irrigation District
Yes
Yes
Attachment 1, parts 1.2 and 1.4, contain the words "generation assets that meet criteria 2.3, 2.6, and 2.9". However, some of the assets mentioned in criteria 2.6 and 2.9 are not "generation" assets and therefore would be unintentionally excluded from parts 1.2 and 1.4 if the current wording is retained. We suggest changing "generation assets" to "assets" in parts 1.2 and 1.4 of Attachment 1.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Alice Ireland
Xcel Energy
Yes
Yes
No
No
Yes
Yes
No
Yes
1) R1 (and R2) it's unclear what 'implement' entails (do we need to provide evidence of communication, training? – those aren't listed in M2). 2) R1 Our company has a limited set of Policies, instead putting detailed information into standards and procedures that are in force through a Policy. We would like the flexibility to cover R1.1-R1.10 through a combination of policies and standards. 3) R5 please define 'where allowed by the CIP standards'. It is unclear where it is required to have formal delegation, and where it is obvious that the Sr. Mgr. will not be performing the function (for example, approval of access to systems and provisioning which are performed by a separate group of individuals who may or may not report, operationally, to the Sr. Mgr). 4) R1.10 'provisions for declaring' CIP Exceptional Circumstances should be clarified to not imply that we list all possible scenarios where we would invoke CIP Exceptional Circumstances. Suggest instead 'process for declaring' which would focus on how to communicate and document the circumstances and rationale for declaring at the time of the event.
Group
PNGC Comment Group
Ron Sporseen
Yes
Yes

The PNGC Comment Group is in agreement with NRECA's comments on CIP-002 and CIP-003: 4.2.1 and 4.2.2, and Attachment 1, 2.10 – The threshold for 300 MW of UFLS or UVLS load shedding is clear, but saying “that are part of a Load shedding program” implies that an entity could have only 50 MW of load that will be shed as part of a larger 300 MW “program” and be drawn into the applicability and required to comply with the Medium Impact facility requirements. Another scenario is where a DP with a 250 MW load shedding program not associated with any other group would not come into applicability at all. NRECA recommends that the SDT provide guidance with very clear examples of scenarios that would include or exclude DP or LSE entities from required compliance with CIP Version 5 standards. Under the inclusion threshold for DP, 4.2.2, third bullet, states: “A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard.” NRECA recommends that the following language be added to the end of that bullet; “, and where the Protection System is connected to a supervisory control system providing remote operation capability.” This language will help to further appropriately clarify the scope of applicable Protection Systems in the CIP standards. Attachment 1 2.10 – see comment above 2.11 – The 300 MW value should be revised to 1500 MW to properly align it with 2.1 in the Medium Category. The 300 MW value has not been adequately technically justified and the resulting potential compliance obligation actions and costs that could be required will likely far outweigh the reliability benefit of keeping the 300 MW value in this section. If the change to 1500 MW is made, then all other Control Centers, and associated data centers, not included in the High or Medium Category will be included in the Low Category. This is a major issue for NRECA. It will be difficult to support CIP-002-5 without this revision.
Yes
Yes
Yes
Yes
Yes
Yes
CIP-003 – Ballot Recommendation – Negative R2 – NRECA is concerned that even though it is stated that a list of Low Category assets is not required for compliance, we do not see how compliance could be proven/demonstrated without such a list. Given that the requirements for Low Category assets are intended to be programmatic in nature, and not asset specific, NRECA requests that the SDT make changes necessary to not in effect require a list of Low Category assets to demonstrate compliance.
Individual
Russ Schneider
Flathead Electric Co-op
Yes
Yes
Under the inclusion threshold for DP, 4.2.2, third bullet,: “A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard.” Flathead requests that this be clarified to only include configurations “, and where the Protection System is connected to a supervisory control system providing remote operation capability.”
No
No
Individual
Chris Higgins on behalf of BPA CIP Team
Bonneville Power Administration
No
Yes
BPA recommends the SDT replace “…affect the Reliable Operation of the BES” in the definitions, background, guidelines, and wherever possible throughout the standard with “…prevent the entity from maintaining the reliable operation of the BES.” The latter is a much more succinct requirement because it allows for the use of the word “prevent” to establish a threshold. The terms “affect” or

“negatively impact,” which are inconsistently used throughout the standard are vague, and subject to interpretation. BPA approves of the 15 minute window to help define the Real-Time environment and was only able to understand the intent of the SDT by reading page 32 of the SDT’s reply to previous comments. BPA recommends the language used to articulate the Real-Time window of 15 minutes, found on page 32 of the SDT’s reply to previous comments, be used in the definitions, background and guidelines document. BPA recommends the SDT create a term (e.g. Critical Asset, BES Asset, or something similar) for the phrase “Facilities, systems or equipment that meet the criteria specified in CIP-002-5, Attachment 1 – Impact Rating Criteria.” This would make the definitions easier to read, and facilitate discussion and documentation requirements. BPA recommends the SDT consider that the process for identifying BES Cyber Assets is typically different in Control Centers than in the field. Control Centers will identify BES Cyber Systems (e.g. information systems like SCADA and AGC) first, and then identify the BES Cyber Assets that those systems comprise. While field sites will typically identify BES Cyber Assets first, and then group those Cyber Assets into BES Cyber Systems. These “BES Cyber Systems,” in many cases, will be little more than collections of devices organized by type; they may be geographically separated with no connectivity or limited serial connections. BPA HAS CONCERNS with: 1) Potential problems emerging from using the same term (i.e. BES Cyber System) to describe two disparate structures with intrinsically different characteristics. 2) The inability to apply controls intended for BES Cyber systems that are information systems on BES Cyber Systems that are collections of standalone devices (relays, telemetry, GPS) which meet the definition of BES Cyber Asset, but can only be accessed physically (i.e. non-routable, non-dial up accessible) or via point-to-point serial connection. BPA believes these devices must be secure and questions whether a “one size fits all” approach is the most efficient and effective use of the standard. Would it not make more sense to tailor a portion of the standard to these types of devices specifically? BPA recommends that the SDT provide clarity on what is included in the “Facilities, systems, equipment” specified in Attachment 1. There is also an inconsistency between this phrase in the definitions and Attachment 1; “Systems” being capitalized in the former and not the latter. BPA requests the SDT address an apparent conflict between the BES Cyber Asset definition and the CIP-002 guidelines. The proposed definition of BES Cyber Asset focuses on real-time by applying to cyber assets that would adversely impact BES operations (via Facilities, Systems or equipment) within 15 minutes if destroyed, degraded, or otherwise rendered unavailable when needed. In the CIP-002-5 Application Guidelines, “Current Day and Next Day planning” systems are included in the Situational Awareness component. As the 15 minute window pertains to the Cyber Asset, rather than the asset itself (i.e. Facilities, Systems or equipment), any Cyber Asset that would be included in a “Current Day and Next Day planning” system would not meet the current criteria for a BES Cyber Asset, unless such a planning horizon was 15 minutes or less.
Yes
No
Yes
Yes
Yes
Yes
R1 provides a list of mandatory topics on which BPA is to write policy. The guidelines provide more granular topics that BPA is to address. BPA believes that it should be able to have a cyber security program which includes policies that are relevant to our environment. Should BPA’s policies encompass some or all of the topics listed in the standard, than that is what BPA believes is needed to maintain and secure our environment. BPA does not favor requirements that are seemingly in place for the sake of compliance. BPA recommends removing the list of mandatory cyber security policy topics and associated granular requirements in listed in the guidelines. Regarding R2 – BPA recognizes that CIP version 5 does not require low impact systems to be documented. How is BPA to certify the application of these polices on systems which are not required to document? For example, BPA’s access control policy for Low impact system could state that we require strong passwords however, if are not required to have a list of these systems, how can BPA be held accountable in ensuring the policies are being applied? Therefore, BPA recommends removing R2 from the CIP-003 version 5 standard OR require low impact systems to be documented in regard to R2 accordingly.
Individual
Larry Watt

Lakeland Electric
No
No
"Please see comments submitted by FMPA through the formal comment process."
Yes
No
No
No
No
No
"Please see comments submitted by FMPA through the formal comment process."
Individual
David R. Rivera
New York Power Authority
No
No
NYPA agrees with NPCC comments, plus - In Attachment 1, please clarify 'Functional Obligations' (1.3) and 'Data Center' (1.4). Can we have clarification on what is meant by 'Associated Contingencies' in reference to the derivation of IROL (2.6)?
Yes
Yes
Yes
Yes
No
No
NYPA agrees with NPCC comments
Individual
Ron Donahey
Tampa Electric Company
No
No
Tampa Electric supports the Edison Electric Institute (EEI) comments especially related to the identification of Low Impact BES CS at a Facility level. Listing all the Cyber Assets associated with a Low Impact Facility as this would add administrative burden and not provide additional BES CS security or BES reliability. Tampa Electric offers these changes to CIP-002 with the following additional clarifications and suggestions: Q1. Tampa Electric suggests that SDT provide examples of potential assets for control center, transmission substations, and power generation in each type (BES Cyber System, BES Cyber Assets, Associated Electronic Control & Monitoring, Associated Physical Access Control, Electronic Access Point, etc.) How far does the BES Cyber System extend? EMS is definitely a BES Cyber System; does it extend to the switches, routers, time & frequency devices, Digis, Front End Processors etc.? This could be handled through the definition or guideline. Q2. Tampa Electric provides the following additional clarifications and suggestions: For Control Centers, substations and generation – Tampa Electric suggests that SDT provide examples of assets in each type of this new breakout/definition (BES Cyber System, BES Cyber Assets, Associated Electronic Control & Monitoring, Associated Physical Access Control, Electronic Access Point, etc.). Tampa Electric also requests that the SDT provide supporting documentation similar to Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets.
Yes
No
No
No

No
No
Tampa Electric supports the comments submitted by EEI. In addition, Tampa Electric suggests that there is a clerical error in the Introduction, section 4.2.4 where it provides exemptions from CIP-002-5. This would seem to reference exemptions from CIP-003-5. We request additional clarification for M2 to describe what would be sufficient in terms of evidence? We note that the R4 rationale is a sentence fragment (ends at 'proving'). We suggest that the SDT review the R4 rationale: this requirement is for approval but the R4 rationale calls for availability of the policy to all personnel. For R5, please clarify if the standards state which can be delegated? Tampa Electric suggests that the VRFs – R2 should be Lower as they apply for lower impact systems. In the Application Guidelines R3, should this reference R3 or R5?
Individual
Brian S. Millard
Tennessee Valley Authority
Yes
Yes
Request clear definition of "BES Element". General comment to all Measures - Remove the" not limited to" clause. These are examples of proof of compliance. This might be taken by auditors to mean must. This should include the word "example". R1.3 - How do you prove a Low impact facility classification with no discrete identification process? Attachment 1, 2.3 - Should there be a megawatt qualifier? Attachment 1, 2.11 - Replace 300 MW with 1500 to be consistent with other standards. Attachment 1, 3.2 - Change to blackstart resources not otherwise classified as high or medium is low.
Yes
Yes
Yes
No
Yes
Yes
CIP-003-5 R4 as stated doesn't clearly define the extent to which policies will have to be signed by the CIP Senior Manager. Without clear guidance this may lead to signatures on all implementing policies throughout the company. This could delay updates and implementation. Delegation should be allowed beyond an overarching policy. R1 and R2 state each Responsible Entity shall implement one or more documented cyber security policies that address select topics and M1 and M2 states Evidence must include one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics. Does this mean that the Senior Manager must approve all cyber security related processes, procedures, and plans in addition to the high level cyber security policy? R1.3 - Delete interactive remote sessions this is included in 1.2. R3 - Allow to define CIP senior manager by name, title or role instead of just name. R4 - This is the only area CIP senior manager cannot delegate authority. Add delegate authority.
Individual
Thomas Washburn
FMPP
See FMPA comments for all of the CIP V5
Individual
Annette Johnston
MidAmerican Energy Company
No
No
GENERAL COMMENTS: (1) ANNUAL: MidAmerican Energy proposes the text for all annual requirements be revised to reduce the administrative burden of tracking two dates, which would be necessary based on the draft 2 language of "at least once each calendar year, not to exceed 15 calendar months…" The following proposed text would allow entities to track one date instead of two

for its annual reviews: “once each calendar year or a period not to exceed 15 calendar months.” (2) BLACKSTART/CRANKING PATH UNITS: We understand the rationale behind removal of the blackstart and cranking path units by deleting 2.4 and 2.5 from the CIP-002 Attachment 1. We think it will be critical to include technical and risk-based justification for not “lessening” the standard by making this change. CIP-002 R1 COMMENTS: (3) MidAmerican Energy Company supports the MRO NERC Standard Review Forum’s proposed solution that clarifies the flow for identifying BES Cyber Systems. It is important to note that the proposal supports and does not change the SDT’s desired flow for identifying BES Systems, does not change the outcome for identified high and medium BES Cyber Systems and does not change the SDT’s identification of blackstart resources and cranking paths as low. The proposal retains Attachment 1 high and medium unchanged. The proposal supports SDT’s intent that lists of low Cyber Assets are not required. (4) The proposal first identifies BES Sites (a new definition), some of which would be identified as low and used for the CIP-003 R2 programmatic controls for lows. The proposal bounds the scope for lows by defining low BES Sites positively (what they are) instead of in the negative (what they are not) and revises part 3 of Attachment 1 for lows accordingly. The proposal leverages lists entities need to have for Operating and Planning Reliability Standards so that new development is not required for the proposed BES Sites. (5) The proposed draft 3 approach addresses industry confusion with draft 2 for clarity of flow of identifying BES Cyber Assets and BES Cyber Systems subject to CIP. The proposed wording more closely follows the description of flow in version 4. Stated again, the proposed wording does not change the SDT’s intended flow and is offered constructively for consideration to resolve confusion over the wording of the flow in draft 2. (6) The proposal is offered to help gain approval of CIP-002-5. The proposal also supports EEI’s key issues strategies: defines low impact at a site level, proposes language to address zero-defect requirements, differentiates VRFs by BES Cyber System impact categories and refines “annual.” (7) A summary of key proposed draft 3 CIP-002 requirements follows, along with measures, VRFs, VSLs and rationale. (8) BES SITE: Substations 100kV and above, generating units above (insert # to set the floor) MW (MVA?), control centers and backup control centers used by NERC certified operators to support the real time operations of the interconnected Bulk Electric System, Blackstart Resources, Cranking Path and initial switching requirements. [Note to SDT: The lists are based on existing lists entities need for Operating and Planning Reliability Standards applicable to their NERC registration criteria.] (9) FLOW FOR PROPOSED CIP-002-5 DRAFT THREE: R1. Select BES sites. ** R2. Identify high impact Facilities, systems or equipment at BES sites on the R1 BES Sites list using Att 1 Part 1. Identify the high impact BES Cyber Assets used by the high impact Facilities, systems, equipment in R2. ** R3. Identify medium impact Facilities, systems or equipment on the R1 BES Sites list using Att 1 Part 2. Identify the medium impact BES Cyber Assets used by the medium impact Facilities, systems, equipment in R3. ** R4. Identify BES Sites on the R1 BES Sites list that are not included in high or medium. These BES Sites are low. ** R5. Identify the Electronic Access Control or Monitoring Systems and the Physical Access Control Systems. ** R6. Identify Protected Cyber Assets. Assign medium or high. ** R7. Senior manager approve lists in R2-R3 once per calendar year or not to exceed 15 months between approvals. (10) RATIONALE FOR FLOW CONSTRUCTION: Senior manager approval of highs and mediums corresponds to existing requirements for approval of Critical Cyber Assets in version 4. (Note: Flow is proposed as separate Rs, but could be constructed as sub-requirements.) R5 and R6: CIP versions 1-4 identified the following: ESP control or monitoring (CIP-005); noncritical (CIP-005); and PSP authorize or log (CIP-006). CIP version 5 draft two assumes identification of EACs, PACs and Protected Cyber Assets in CIP-003 through -011, but technically does not identify them anywhere in CIP-002 through -011. Propose identification of these in CIP-002. Propose all EACs and PACs are medium, even if associated with high. Inherently, they should not have a 15 minute impact on the grid directly. Differentiating these systems between high and medium causes further complexity without a commensurate increase in security. Some devices that are included as Cyber Assets in these systems are not all capable of the additional controls applied to high and would require TFEs for the high controls and/or create additional work, much manual, without commensurate increase in security. (11) ATTACHMENT 1: 3. Low Impact Rating: R3.1- Substations 100kV and above and not included in medium or high; R3.2: Generating units __ MW (or MVA?) and above and not included in medium or high. (insert # to set the floor – number may be higher than but should not be lower than the minimum aligned with NERC Registration Criteria.); R3.3: control centers and backup control centers used by NERC certified operators to support the real time operations of the interconnected Bulk Electric System and not included in medium or high; R3.4: Blackstart Resources and not included in medium or high; R3.5: Cranking Path and initial switching requirements and not included in medium or high. (12) CONTINUOUS IMPROVEMENT vs. ZERO

DEFECT: Include language in the requirement(s), except senior manager approval, that aligns with prior FERC orders speaking to cultures of compliance that implement, detect, correct and prevent. “The Responsible Entity shall update list(s) as necessary, and review list(s) once each calendar year or not to exceed 15 months between reviews. Each Responsible Entity shall implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations, per se.” NIST 800-53 minimum assurance requirements for security controls emphasize continuous improvement, expect “expeditious” correction (“timely” for lows) and do not expect perfection. The NIST 800-53 quote is included at the end of these comments. It is also proposed in response to FERC’s order on find, fix and track. In paragraph 81 (included at the end of these comments), FERC asked industry for proposals to revise or remove requirements to focus resources on serious risks to reliability. It also aligns with preliminary efforts to move toward more risk based auditing. (13) VRFs FOR CIP-002: Separating requirements, allows different VRFs for different requirements. No high VRFs are proposed based on a review of all VRFs for all Reliability Standards. High impact category is proposed for medium VRF. All else is proposed for lower VRF. (14) VSLs for identification: Lower-Did not take corrective action, if needed, that may prevent recurrence of flaws; Moderate- Did not correct flaws detected; Higher: Did not measure performance to detect flaws; Severe- Did not implement. (15) VSLs for Senior Manager approval: Lower-Failed to complete senior manager review according to Requirement R7 for more than 30, but less than 41 calendar days; Moderate- Failed to complete senior manager review according to Requirement R7 for more than 40, but less than 51 calendar days; Higher- Failed to complete senior manager review according to Requirement R7 for more than 50, but less than 61 calendar days; Severe-Failed to complete senior manager review according to Requirement R7 for more than 60, calendar days. (16) NIST 800-53 Appendix E: Appendix E describes the minimum assurance requirements for security controls in low-impact, moderate-impact, and high-impact information systems. For security controls in low-impact systems, the emphasis is on the control being in place with the expectation that no obvious errors exist and that as flaws are discovered, they are addressed in a timely manner. For security controls in moderate-impact systems, in addition to the assurance requirements for low-impact systems, the emphasis is on increasing the grounds for confidence in control correctness. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer or control implementer incorporates, as part of the control, specific capabilities to increase grounds for confidence that the control meets its function or purpose. For security controls in high-impact systems, in addition to the assurance requirements for moderate-impact systems, the emphasis is on requiring within the control, the capabilities that are needed to support ongoing, consistent operation of the control and to support continuous improvement in the control’s effectiveness. There are additional assurance requirements available to developers/implementers of security controls supplementing the minimum assurance requirements for the moderate-impact and high impact information systems in order to protect against threats from highly skilled, highly motivated, and well-resourced threat agents. This level of protection is necessary for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above. (17) FERC order paragraph 81: The Commission notes that NERC’s FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently. (18) CIP possible violations were 91 percent of the FFTs in the order. CIP standards occupy 8 of the top 10 most violated standards slots.
No
No

Yes
No
No
No
(1) CIP-003 R1 REQUIREMENT: In its draft 1 comments, MidAmerican Energy proposed language closer to CIP-003-4 R1 on the cyber security policy. FERC directed the ERO to provide additional guidance for topics and processes that the cyber security policy should address, but FERC did not direct any changes to the requirement itself. In its consideration of comments, the standards drafting team stated it was attempting to bring the language in line with NERC Results Based standard format. However, draft 2 does not move toward results-based and, in fact, moves away from results based by becoming prescriptive with the enumerated topics. MidAmerican proposes deleting the enumerated topics in 1.1 through 1.10. Refer to “the CIP standards” (but not by number) to make the scope of the policies clear, but flexible enough if there are changes in the CIP standards in the future. Incorporate R4 into R1 and R2. MEC proposes the following language: “Document and implement a cyber security policy that represents management’s commitment and ability to secure its BES Cyber Assets. The Responsible Entity shall, at minimum, ensure the cyber security policy addresses the CIP standards, including provision for CIP Exceptional Circumstances. NEW R1.1. MidAmerican Energy proposes CIP-002 R4 be incorporated into R1 as a new R1.1. (2) CIP-003 R1 GUIDANCE: The guidance in the first paragraph is sufficient to meet the FERC directive. Delete the enumerated topics, which suggest far too much detail for a policy. (3) CIP-003 R2 REQUIREMENT: The following is proposed: “For low BES Sites each Responsible Entity shall: implement policies; measure performance to detect flaws in its policies; correct detected flaws in its policies expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations, per se. The following topics shall be addressed in policies …” (4) Restructure R2.1 to be the four programmatic controls and create a new R2.2 to cover the R4 approval (deleting draft 2 R4). (5) R2.1.1 AWARENESS: This is acceptable if CIP-002 is changed to require identification of BES Sites, and this is applied at the site level for lows. (6) R2.3: Qualify electronic access control for external routable connectivity or dial up accessibility. This prioritizes resources on the higher risk areas. (7) R2.4: MidAmerican Energy proposes limiting this requirement to “incident response” and delete the phrase “to a BES Cyber Security Incident.” This requirement still refers to “BES Cyber Security Incident,” but “BES” has been removed from the glossary term. Low impact does not require PSPs or ESPs, but the definition of a Cyber Security Incident is specific to an incident that compromises or was an attempt to compromise an ESP or PSP. While it may be possible to have some type of incident response for low impact, it cannot be tied to the glossary term of Cyber Security Incidents because of the lack of ESPs and PSPs for low impact BES Cyber Systems. (8) CONTINUOUS IMPROVEMENT: MidAmerican Energy believes that version 5 of the CIP standards provides the opportunity to move toward results based standards that focus on continuous improvement for improving reliability rather than “zero defect” compliance. Throughout our comments, we provide suggested language to incorporate the concepts of measuring performance to detect flaws, correct flaws and take action that may prevent recurrence (if applicable for the flaw). The CIP standards were eight of the top 10 most violated standards in 2011, and 91 percent of the find, fix and track violations approved by FERC in March 2012. FERC invited NERC to revise or remove requirements that do not improve reliability. NIST 800-53 App. E Minimum Assurance Requirements recognize flaws will be discovered and focus on continuous improvement. Other federal regulators, including the EPA and NRC, do not enforce zero-defect forever compliance. MidAmerican Energy is proposing language be added to the R2 requirement statement that flaws that have been detected and corrected would not be violations. (9) CIP-003 R2 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (10) CIP-003 R2 GUIDANCE: Revise to correspond to use of “low BES Sites” in proposed changes to R2. (11) CIP-003 R4 REQUIREMENT: Incorporate this into R1 and R2 as mentioned above, and delete R4. (12) CIP-003 R3, R5 and R6 REQUIREMENTS: ** CONSOLIDATE REQUIREMENTS: Only one requirement is needed to accomplish the reliability benefit of clear accountability within an organization for certain security matters. Combine requirements R3, R5 and R6 into one. ** ANNUAL: Revise the requirement to ““once each calendar year or a period not to exceed 15 calendar months.” (13) CIP-003 R4 REQUIREMENT: Incorporate this requirement into R1 and R2 and delete R4.
Group

FirstEnergy
Doug Hohlbaugh
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
FE suggests that the measure for M2 be adjusted to remove the phrase “or plans that demonstrate the implementation of the required topics”. The text seems to imply an auditor may be looking for specific application or implementation of the required R2 policies on individual low impact BES Cyber Systems even though a discrete list of those systems is not required. (Please see our comments in Form D question 16)
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
No
Yes
(Comment 1) R1.1 appears to require the entity to maintain a list of “Facilities, Systems, or equipment that meet the criteria specified in CIP-002-5, Attachment 1.” This seems to be inconsistent with what is stated in the Rationale and the Guidelines, which only refer to identifying BES Cyber Assets and BES Cyber Systems. We suggest that the SDT clarify the intent and the auditable requirement by adding an explanation to the Rationale, Guidelines or M1. (The following comments 2 through 5 apply to section 4.2 for all of the CIP standards.) (Comment 2) Change “One or more of the Systems or programs” to “One or more of the FOLLOWING systems or programs.” (Comment 3) We support comments submitted by APPA for Question 3 regarding the Applicability section (especially with regard to the third bullet of 4.2.2) and Attachment 1. (Comment 4) We recommend the following addition to section “4.2.4 Exemptions” in order to clarify that only the systems specified under section “4.2” are in scope for DPs and LSEs: “4.2.4.4 Cyber Assets that are owned by DPs or LSEs and that are not associated with the Facilities, systems or equipment described in 4.2.1 or 4.2.2.” (Comment 5) Since the glossary definition of “System” is “A combination of generation, transmission, AND distribution components,” we question whether a DP or LSE would own a “System”. Please check each use of capitalized “System” in section 4.2, especially when used as “UFLS System” or “UVLS System”, in order to clarify applicability.
Yes
Yes
Yes
Yes
Yes
Yes
MMWEC agrees with and supports the comments submitted by APPA. We are concerned that R1.1 will present compliance challenges, since it is unclear what constitutes sufficient “implementation of the required topics.” More suggestions or examples in the Guidance section regarding the content of the policies for Low Impact entities may help.
Individual
Bob Thomas
Illinois Municipal Electric Agency
No
No

Illinois Municipal Electric Agency supports comments submitted by American Public Power Association and Florida Municipal Power Agency.
Yes
No
No
No
No
No
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Group
Dominion
Connie Lowe
No
Yes
- In CIP-002-5 Attachment 1, the threshhold in 2.11 should be changed to 1500MW to be consistent with other medium impact facilities (generation units). The language should be changed to: "2.11. Control Centers and associated data centers not included in High Impact Rating (H), above, that: (1) perform the functional obligations of Balancing Authority or Transmission Operator, or (2) control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW or more of BES generation." -The Use Case: CIP Process Flow in the Application Guidelines of CIP-002 contains the term "External Connectivity" in the third and fourth process boxes. This term is not a defined term. The term either needs to be changed to "External Routable Connectivity" or the capitalization on the term removed.
Yes
Yes
No
No
Yes
Yes
CIP-003-R3 - R3 should be reworded to be "Each Responsible Entity shall identify a CIP Senior Manager by name, title, or role." in order to allow Responsible Entities additional flexibility and to reduce the impact of personnel changes on policy and procedure documentation. CIP-003-R4 - The introductory language in Measure M4 for 4.2 reads as though the two items identfied as expected evidence are optional. The introductory language to the measure should be changed to, "Examples of evidence include:".
Group
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)
David Dockery, NERC Reliability Compliance Coordinator, AECI
No
Yes
[Introduction, p 6, part 4.2.2 REPLACE: “A Protection System” WITH: “A Protection System (other than UFLS or UVLS Systems)” Rationale: AECI agrees that PRC-005-2 will likely classify UFLS and UVLS systems as Protection Systems. While the second bullet above demonstrates intent of this standard to be limited in scope to UVLS and UFLS Systems of sizes that would clearly impact the BES, this bullet could inadvertently include the remaining UVLS and UFLS unless specifically stated to exclude them.] [Introduction, p 6, part 4.2.4 ADD: “4.2.4.4 Cyber Assets that are owned by Distribution Providers or Load Serving Entities and that are not associated with the Facilities, Systems and equipment specifically described within parts 4.2.1 or 4.2.2 above.” RATIONALE: Further clarifies the CIP SDT’s intent of scope represented within parts 4.2.1 and 4.2.2, and aligns with the SDT’s earlier responses back to comments voiced concerning scope of the CIP Standards upon DPs and LSEs.] [Requirement R2, p 11, Measurement M1 REMOVE: “and update, where applicable” RATIONALE: AECI’s agrees with others in industry, that the CIP Senior Manager or delegate is likely not to be the individual(s) updating the identifications required by R1.]

[==========Begin Proposed block of changes========== [Introduction] [AECI is herein proposing several changes to CIP-002-5, Appendix 1, pp 17 & 18, parts 1.2, 1.3, & 1.4, 2.10, and 2.11, in order to resolve technical discrepancies in MW impacts, and in particular deal with part 2.11's implication that any BA or TOP of any size is at least a Medium Impact, as well as the part 2.11 implication that any 300 MW has Medium Impact upon the BES, which is simply not the case. Therefore, AECI suggests revising the Bright-lines for High Impact from 1500 to 3000 MW and controlling two or more elements. The Bright-lines for Medium Impact would be 1500 MW and controlling one or more elements. This will provide a more well-defined difference between High and Medium.] [In addition, part 2.10 changes deal with the same 300 MW impact issue, in addressing centralized UVLS and UFLS system impact sizing, differentiating the two. AECI recommends changing 2.10 as described below.] [All changes are detailed below.] [End Introduction] [Appendix 1, p 17, part 1.2 REPLACE: 1500 MW WITH: 3000 MW REPLACE: "one or more" WITH: "two or more" RATIONALE: Assess High Impact to twice that of Medium Impact potential] [Appendix 1, p 17, part 1.3 REPLACE: "one or more" WITH: "two or more" RATIONALE: Assess High Impact to twice that of Medium Impact potential] [Appendix 1, p 17, part 1.4 REPLACE: 1500 MW WITH: 3000 MW REPLACE: "one or more" WITH: "two or more" RATIONALE: Assess High Impact to twice that of Medium Impact potential] [Appendix 1, p17, part 2.10 REPLACE: "of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) " WITH: "of 800 MW or more implementing Under Voltage Load Shedding (UVLS) or implementing Under Frequency Load Shedding (UFLS) within a single Interconnection in excess of thresholds in Table X (Derived once from 5%-droop for peak Interconnection load 2012, constrained to 5% error) [[Table X [[Interconnection,UFLS MW Threshold, Notes]] [[Eastern, 1500 MW,(computed value of 4144 MW capped at 1500 MW)]] [[Western, 1400 MW,(computed value was 1437 MW)]] [[ERCOT,750 MW,(computed value was 772 MW)]] [[QUEBEC,300 MW,(computed value was 310 MW)"]]]] RATIONALE: 1) Assess threshold for UVLS, no greater than a single large 800 MWnet coal-fired plant, because UVLS impacts are more localized and so a commiserate threshold is prudent in order to avoid cascading outages. 2) Assess UFLS Medium impact MW threshold level commiserate with Interconnection impacts, where no more than 5% of an Interconnection's droop-characteristic governor-responses from nominal frequency to first-step UFLS relays per PRC-006 is allowed be risked within a centralized UFLS. However, the corresponding guidelines should note that, should an Entity's centralized UFLS system fail, they could individually be assessed a Severe VSL for under-performance, and their RC be assessed greater than Low VSL for their aggregate failure to perform per current VSLs for Requirement 9 of PRC-006-1, page 13. (While this 5% margin agrees with PRC-006 Low Violation Severity Level for Interconnection Impacts, that Entity's business risk of violation due to their UFLS system's failure, could be enormous under NERC Standard PRC-006.)] [Appendix 1, p 17, part 2.11 REPLACE: "(1) perform the functional obligations of Balancing Authority or Transmission Operator, or (2) control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation." WITH: "(1) perform the functional obligations of Balancing Authority or Generation Operator, and control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW or more of BES generation, or (2) perform the functional obligations of the Transmission Operator, that includes control of one or more of the assets that meet criteria 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10. RATIONALE: Align Medium impact Medium impact 1500 MW or Asset amounts. (And see AECI recommendations for Parts 1.2..1.4 High impact ratings.)] ==========End Proposed block of changes==========]
Yes
Yes
Yes
Yes
Yes
Yes
[FYI - p 9 R2 VRF is Low, but p 14 R2 VRF table indicates Medium but should be Low]
Group
Family Of Companies (FOC) including OPC, GTC & GSOC
Guy Andrews
Yes

Yes
none
Yes
Yes
Yes
Yes
Yes
Yes
none
Individual
Richard Salgo
NV Energy
No
Yes
The SDT has made tremendous progress on this posting of CIP-002-5. The comments that follow are specific to the items in CIP-002-5 Attachment 1: 1.2: We recommend removal of reference to criteria 2.9 first because the use of SPS threshold is inappropriate for classifying a control center as High Impact, and second, a generating asset cannot “meet” criterion 2.9. Also, the list of criteria uses the word “and” (“2.3, 2.6, and 2.9”), which is to say that in order to qualify, it satisfies ALL of these three criteria. Did the SDT intend to use the word “or” instead of “and”? 1.4: Same comment as 1.2 above. 2.1: We are concerned about the use of the “preceding 12 months” when determining the capability of the subject generation. It would seem that a forward look is more appropriate given the nature of the subsequent requirements. 2.3: We appreciate the discretion being given to the PC or TP to determine and communicate Adverse Reliability Impact; however, we question whether there is any industry guidance for the PC or TP to make this determination in a consistent fashion. 2.4: We would like clarity, either through Guidance or preferably in the language of this item, that stations at the receiving end of a radial 500kV line are NOT included in criterion 2.4. Absent this clarity, the 500kV receiving station could be inappropriately classified as Medium Impact, when it’s purpose is clearly distribution (non-BES). Consistent with the Guidance Document Transmission section discussion regarding part 2.4, the receiving station should not be considered Medium Impact even though it contains 500kV elements. 2.6: We suggest additional clarity or guidance on the intent of “derivation” in this item as it refers to IROL’s. Suggest a re-write of this criterion, but since we have no clear understanding of the intent, we cannot suggest language. As written, we are unclear as to what “associated contingencies” is referring. 2.11: We are in disagreement with the 300MW threshold for a “control center” that controls BES generation. It is unclear whether this refers to the BA/TOP control center or if this applies to generating plant control rooms. In any event, the 300MW appears to be too low when compared with the 1500MW Medium Impact threshold for the generation assets themselves.
Yes
Yes
Yes
Yes
Yes
Yes
Group
Southern Company Services, Inc.
Antonio Grayson
No
Yes
(1) Regarding CIP-002-5 R1, the essentially real-time update of potentially huge lists is problematic. The requirement to review (and update as needed) the identification within 60 calendar days creates

challenges, particularly for utilities with large amounts of facilities or systems or those experiencing constant change. The implicit requirement of needing a master list of all “BES Changes” simply to prove the start time of a 60 day update period creates an extensive new documentation requirement that is unnecessary and overly burdensome. Southern suggests refocusing R1 towards security and/or reliability outcomes rather than maintaining extensive lists of assets and changes. In addition, Southern suggests changing the review and updating of lists to be an annual activity, as to differentiate this documentation exercise from other more security or reliability focused requirements found later in the requirements. Additionally, Southern recommends deleting R1.4. (2) Regarding CIP-002-5 R1, Southern strongly suggests that the SDT consider re-using lists, where possible, as required by other NERC reliability standards to promote consistency between the reliability standards in lieu of creating a documentation exercise that has the potential to create double jeopardy in other reliability standards. (3) Regarding CIP-002-5, on page 2 of 33, the footnote, “In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4” is an incredibly important aspect of applying the standards. Southern suggests that the footnote needs to be promoted into the actual text of the section Effective Dates on page 2. (4) Regarding CIP-002-5, on page 18 of 33, criteria 2.11 should be removed. The stated intention in the guidance is to eliminate "run of the river" hydro control room situations from being considered control centers, but the 300MW threshold is too low to accomplish this. Southern suggests an explicit exclusion of "run of the river" hydro control rooms in the definition of control center and then remove this criterion. The SDT can then determine whether the other control centers under 1500MW should fall into the medium or low impact category. (5) Regarding CIP-002-5, on page 19 of 33, criteria 3.2 and 3.3 should have the qualifier of “not otherwise classified as high or medium” as criteria 3.1 has. Blackstart units or cranking path substations could have met other High or Medium impact criteria and this appears to mandate that they be classified as Low impact. The facility definition should cover this occurrence. (6) The varying language regarding destroyed, degraded, or otherwise rendered unavailable and its variations found on pgs. 6, 8, 18(twice), 20 and 30 needs to be consistent. (7) Page 18, criteria 2.7 should be limited to NUC-001-2 R9.2.2 to scope the applicability of the requirements. Additionally, on pg. 19 Southern suggests adding "from Blackstart Resources to restoration unit switchyards" after "Cranking Path" in criteria 3.3 to provide additional clarity. (8) Regarding CIP-002-5, Southern suggests the following proposed solution to the auditing/evidence issues of Low Impact BES Cyber Systems. Southern suggests defining a new term “BES Site” to reduce the confusion regarding the already defined terms "Facility" and "System" in the NERC glossary that do not fit the concept these standards seem to address. "BES Sites” would be defined so that it refers to individual generation plants, dams, and renewable farms, transmission substations, and control centers; those classes of sites that we traditionally think of when applying the CIP standards. As a result, CIP-002 R1 can be rephrased with language similar to the following: “1.1 Identify the High Impact BES Sites that meet the criteria specified in CIP- 002-5, Attachment 1 – Impact Rating Criteria Parts 1.1 to 1.4 1.2 Identify the Medium Impact BES Sites that meet the criteria specified in CIP-002-5, Attachment 1 – Impact Rating Criteria Parts 2.1 to 2.11; 1.3 BES Sites which are not identified as High Impact or Medium Impact shall be identified as Low Impact BES Sites; 1.4 Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used for the High Impact BES Sites identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; 1.5 Identify each Medium impact BES Cyber System and its associated BES Cyber Asset(s) used for the Medium Impact BES Sites identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;” For Low Impact BES Sites, this would require the entity to maintain inventories at the "site" level (a list of all BES substations and <1500MW plants for example) and not the cyber device level. We could then propose to change the single low impact requirement in CIP-003 R2 to: “R2. The Responsible Entity shall implement one or more documented cyber security policies for each BES Site that address the following topics: [Violation Risk Factor: Low] [Time Horizon: Operations Planning] . 2.1 Cyber security awareness; . 2.2 Physical access control; . 2.3 Electronic access control; and . 2.4 Incident response to a BES Cyber Security Incident.” This would allow for all BES Cyber Systems at all BES Sites to be implicitly covered by this one requirement. High and Medium Impact BES Cyber Systems would also be covered by the more detailed policy requirement (R1) and the remainder of CIP-003 to CIP-011. Accordingly, the evidence of implementation of the policy for Low Impact BES Sites would bes at a site level and not at an individual cyber asset level.

Yes
Yes
No
Yes
Yes
Yes
(1) Regarding CIP-003-5, Southern supports EEI expressed concerns about any language that would require responsible entities to demonstrate delegation all the way down to the equipment level. Delegation requirements for device level activities would be overly burdensome, would be a significant increase in required documentation, and offers no improvement to actual security or reliability. (2) Regarding CIP-003-5, R1.3, Southern suggests removing R1.3 concerning Interactive Remote Access as a discrete item. All the other subrequirements align with a CIP standard and this should be covered as part of R1.2. Southern views R1.3 as a subset of R1.2 which already covers remote access. (3) Regarding CIP-003-5, R2, Southern suggests the SDT consider the proposed “BES Site” concept proposed above and revising the language towards a defined Low Impact BES Site rather than a description based on what things are not as the current language reflects. (4) Regarding CIP-003-5, R3, Southern suggests allowing for the CIP Senior Manager to be designated by role or title rather than by the individual's name. (5) Regarding CIP-003-5, R4, Southern suggests clarifying that for other than R4, all other required activities of the NERC CIP Senior Manager may be delegated.
Group
MRO NSRF
Will Smith
No
Yes
1] The proposed methodology prescribed by Requirement 1 is in direct conflict with the structure of the definition for BES Cyber Asset and BES Cyber System. The impact rating should align with the facility (BES Site) instead of the cyber asset. [R1 Proposed Flow] 1.1-Based on the definition for a BES Site, each entity should create a list of BES Sites. This step will determine for the entity, which sites have zero BES impact vs.which sites have an impact and will be later divided into high, medium, and low. The criteria for BES Site can also be considered the positive definition or threshold for Low Sites. These are sites that, based on the definition, will have some impact and require, at a minimum, programmatic protection at the Site level. There will be no need to identify the cyber assets associated with sites that have zero impact or those that remain in the Low category. All Sites will have the protections afforded the Low sites, but for those meeting the Medium and High criteria, additional protections are required, as well as the enumeration and classification of the cyber assets critical to providing the BES functionality of the location. After identifying the BES Sites, the Medium and High criteria must be considered for each Site. The following is a proposed flow for which the order can be modified while maintaining efficacy. 1.2- Based on the candidate list for sites with BES impact created from the execution of the first step, identify the High impact sites using the criteria in the attachment. A candidate list for cyber assets required in order for the BES Site to perform its reliability function(s) will be created for the High Sites. The cyber assets that are critical to the performance of the reliability function will then be divided into those with (A) or without (B)External Routable Connectivity, those cyber assets used for Electronic (C) or Physical Access (D) Control or Monitoring, and those cyber assets connected within the same ESP (E) as the cyber assets necessary for the performance of the reliability function. 1.3 – Based on the sites that remain on the candidate list and are not High impact, determine the medium sites based on the criteria in the attachment. A candidate list for cyber assets required in order for the BES Site to perform its reliability function(s) will be created for the Medium Sites. The cyber assets that are critical to the performance of the reliability function will then be divided into those with (F) or without (G)External Routable Connectivity, those cyber assets used for Electronic (H) or Physical Access (I) Control or Monitoring, and those cyber assets connected within the same ESP (J) as the cyber assets necessary for the performance of the reliability function. Note: There are 10 types of cyber assets positively identified through this process, each with varying levels of risk to the BES if compromised or rendered unavailable. This, potentially, creates more than 10 levels of protection to be enumerated throughout the rest of CIP-003 through CIP-011. For administrative ease, the MRO NSRF recommends grouping these types of cyber assets based on their actual level of risk in each scenario involving a potential

incident that is either cyber or physical in nature and based on the External Routable Connectivity. The rest of the Standards should be written to address each type or grouping of asset. Silence on any one type or grouping will lead to confusion regarding the necessary protective measures and commensurate improvement to security posture. 1.4 – Everything that made the initial candidate list requires protection of some sort, so if it didn't get picked for High or Medium, it gets assessed at Low, because it met the threshold criteria in the BES Site definition. Verbiage in the definitions and the requirements should support this process flow, which will allow the enumeration of High Sites, Medium Sites, and Lows Sites (since we all know a list is required to demonstrate even programmatic elements of CIP compliance). The lists of Cyber Assets will only be required at Medium and High Sites. If possible and feasible, the criteria for dividing the sites into those categories should be progressive in nature, allowing clear demarcation and rationale for the criteria chosen. Additionally, the rest of the Standards should address the requirements progressively for the asset types based on risk. The shift from the current draft to one with obvious progression throughout the CIP-002 methodology and again throughout the rest of the Standards will allow for ease of application at each entity. The current draft does not provide the entities with clear understanding of the order and rationale for identifying the scope of applicability for the CIP Standards, and the MRO NSRF feels that the entities can't be successful with the current format. [2] Change the CIP-002 VSLS to reflect "BES Sites" instead of "Facilities" as those would be the enumerated list. In its current state, it conflicts with the statement that low and zero impact sites do not require enumeration. [3] All VSLs should change the impact designation from cyber asset based to site-based. "High," "Medium," or "Low" designations should precede the word "Site" not "BES Cyber Asset" or "BES Cyber System." Please give consideration to the following suggestions: For Criterion 2.5 – Replace the latest revised wording with the following more accurate and precise wording of, "Transmission Facilities operated between 200 kV and 499 kV that are located at a single station or substation, which is connected to three or more other station or substations by lines operated between 200 kV and 499 kV and which possess an "aggregate weighted value" exceeding 3000. The "aggregated weighted value" of the station or substation is determined by summing the "weight value per line" shown in the table below for each BES Transmission Line that is connected to another Transmission station or substation." This proposed wording properly associates the aggregated weighted value with a station or substation, not a Facility (e.g. BES line, transformer, or generator element). The proposed wording also qualifies that the applicable Facilities are the ones at the qualifying station or substations. In the case of an applicable transmission line, the criteria is only the portion of the line's Facilities at qualifying substation, not the portion of the line's Facilities at the other substation, unless the station or substation at the other end of the line also meets the aggregated weight value threshold. For Criterion 2.6 – Replace the unclear wording of '. . . as critical to the derivation of IROLs and their associated contingencies' with wording of, '. . . as Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more IROL violations', which would be consistent with wording used in Criterion 2.8 and 2.9. The Facilities that could cause an IROL to be violated are usually different from the Facilities that IROL was developed to assure would not cause an unacceptable impact on the reliability of the BES when they are lost. For Criteria 2.11; Note that a BA or TOP may only provide a very small number of individual functions as described within the Functional Model based on the amount of CFRs and JROs that NERC has accepted. Every BA and TOP does not have the same impact on the BES as a larger BA or TOP. As written, 2.11 will require every BA and TOP that is registered as such as being in the "medium" category. This one size fits all approach does not work. Another concern with criteria 2.11 is that a TOP registered as a TOP does not "control" any "real power". As stated in FERC Order 706, paragraph 253, FERC clearly speaks of being flexible "However, we are persuaded by commenter's that stress the need for flexibility and the need to take account of the individual circumstances of a responsible entity." Recommend that BA's be viewed as in Attachment 1, CIP-002-4 brightline criteria 1.17.
Yes
No
Yes
Yes
Yes
Yes
(1) [Proposed Verbiage] CIP-003 R1 Each Responsible Entity for the identified BES Cyber Systems critical to the operation of high impact and medium impact BES Sites shall implement one or more

documented cyber security policies that address the following topics: Keep 1.1 – 1.10 as is. (2) [Proposed Verbiage] CIP-003 R2. For BES Sites identified as low impact, each Responsible Entity shall provide guidance with one or more documented cyber security policies that address the following topics: [Violation Risk Factor: Low] [Time Horizon: Operations Planning] The programmatic elements identified in the sub-requirements may remain, as is. (3) VSLs should reflect the actual risk to the BES when one or more elements are missing. The absence of a program should be high or severe, but the lack of discrete components should start at Low. Please note that the above changes apply to structure and not content of what the SDT is intending to accomplish.
Individual
Steve Karolek
Wisconsin Electric Power Company
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Calendar year and 15 months are mutually exclusive. This requirement should use the term "Annual" as applied in NERC CAN-0010. Further, the term Annual should be added to the NERC Glossary of Terms. (2) Enhancing the CIP process flow on page 33 to indicate that the assets inherit the impact of the Facility, there may be greater industry approval. As it currently exists, the process flow has as its first box the identification of BES Cyber Assets and BES Cyber systems. This first box should capture the identification of Facilities that satisfy the impact criterion. This process flow should be enhanced, and possibly moved to the requirements section to provide a prescriptive methodology to ensure this "Facilities first" approach provides clear directives to the industry. (3) We feel the wording of requirement 1 with respect to planned in service time of 6 months introduces additional documentation requirements of what is planned and additional requirements to ensure the plans are followed. These additional requirements do nothing to enhance the reliability of the BES.
Yes
No
Yes
No
No
Yes
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Calendar year and 15 months are mutually exclusive. This requirement should use the term "Annual" as applied in NERC CAN-0010. Further, the term Annual should be added to the NERC Glossary of Terms. (2) We are concerned about the level of delegation which needs to be specifically delegated by the CIP Senior Manager. This should be limited to high-level delegations of responsibility. Specific assignment of duties at the "worker" level is best done by supervisors and managers of the related processes. (3) Wisconsin Electric recognizes that not all BES Facilities have a "high" or "medium" impact on the BES and that there may be Cyber Assets and/or Cyber Systems located at those facilities. However Wisconsin Electric believes that the industry does not at this time have consensus on how to identify, classify and secure those Cyber Assets and Cyber Systems. In the interest of moving this version of the standard forward, we believe that all requirements not applicable to those Cyber Assets and Cyber Systems essential to the functional obligations performed at "high" or "medium" impact BES Facilities be removed from the standards and dealt with in a future version. (4) Guidance for physical security includes the phrase "and egress". Since the requirements for exit readers have been removed with this draft, the wording with respect to egress should also be removed.
Group
Western Area Power Administration
Brandy A. Dunn
No
Yes
a) General - Study based exceptions should be allowed. Given that a substation may fall into the

medium category under the bright line criteria, an entity should be able to show through study work that loss of the substation does not lead to voltage collapse or cascading outages, and thus exclude its inclusion in the medium category through studies. b) General - The “Guidelines and Technical Basis” section of the standard is problematic. It basically states that any element or system of elements that has an adverse impact on BES services should be listed. This is an issue because elements incorporated into the BES will always have an impact, otherwise they would not exist. This section of the standard goes on to define conditions that will always skew the impact toward adverse, and the impact is not quantified, so the reader is left with the implication that any adverse impact requires listing of the asset. Perhaps this is the intent, and if so why have the pretense of the “bright line” criteria? Simply declare all BES transmission elements as Medium and be done with it. Otherwise, the level of impact needs to be defined such as “additional elements which, upon loss, will lead to voltage collapse or cascading outages” in addition to or instead of the specific “bright line” criteria defined in Attachment 1 of the standard. c) Attachment 1, 2.5: The discussion in the Application Guidelines under transmission part 2.5 (page 29): This section claims that the average MVA line loading used in a report used as a reference for quantifying risk is 700 MVA for 230 kV lines, and 1300 MVA for 345 kV lines. It is not clear where this averaging took place, but at least one TO is outside the norm, with emergency ratings of the highest rated line of each voltage class under 72% of those values, let alone the average line loading. This goes directly to the greatest weakness of this revision of CIP-002-5, and that is that the standard does not allow for systems that are different than the model system used to baseline the standard, nor does it allow study-based exceptions. d) Attachment 1, 2.9: Given that the SPS could have an impact on IROLs, this standard implies that all components of the SPS are designated as medium without regard to whether loss of those elements of the SPS system would lead to the referenced IROL violation. The SPS can be designed so that incorrect readings or misoperation of a given element of the system has either no impact or acts to run the SPS in the “safest” manner. If this is the case, the individual elements of the SPS should not require a medium designation, and should be allowed for in the standard. e) Attachment 1, 2.10: Given that a system results in load shedding over 300 MW, if the system is a set of relays set to work on observation of a system variable such as frequency or voltage, independent of the other elements of the load shedding system (ie relays at substations distributed across the TO’s system, set to trip for various under voltage or frequency levels, but not in communications with each other), it should not be necessary to declare each of the relays and therefore each substation as medium assets.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Ralph Meyer
The Empire District Electric Company
No
Yes
We need a clear definition of dial-up to eliminate the confusion of what dial-up includes and what it does not include; for example leased lines to modem banks should not be included. Without a clear definition auditors could interpret devices that are used for point-to-point communication over leased lines as dial-up and include these devices as dial-up assets under the CIP standards.4. Need clarity on which Transmission Owners’ control centers who are not Operators will be classified as High Impact. Attachment 1-Item 1.3 – uses the term “functional obligation”. This term is not defined. Also not clear is the meaning of –to control- an asset.
Yes
Yes
Yes
Yes

Yes
Yes
Low Impact BES Cyber Systems: EDE propose removing BES Cyber Systems used within Low Impact facilities from the current draft 2 standards to provide consistent standards at a later date. This will ensure BES Cyber Systems used within High and Medium Impact facilities will achieve the benefit of the enhanced standard unimpeded from Low Impact concerns. R5 : What is meant by the words “specific actions”? This is not in the definitions and we suggest striking the words “specific actions” as it is too subjective to audit. There is a clerical error in the Introduction, section 4.2.4 where it provides exemptions from CIP-002-5. This would seem to reference exemptions from CIP-003-5. R2 VSL:b. Given the R2 requirement for BES Cyber Systems used within Low Impact facilities, the VSL should be shifted to the left to use Lower/Moderate VSLs. Per the subjects covered within CIP-003, there are no direct impacts on BES reliability should a policy clerical error occur or Senior Manager designation not be captured adequately.
Individual
Daniel Duff
Liberty Electric Power LLC
Yes
Yes
2.11 generation control centers (with) 300 Mw of Real Power. No technical basis for choosing 300 Mw. No indication as to why a facility which serves as a control room for 350 Mw from units at remote locations would have a greater impact on BES than a 1000 Mw facility at a single location.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
Please give consideration to the following suggestions: For Criterion 2.5 – Replace the latest revised wording with the following more accurate and precise wording of, “Transmission Facilities operated between 200 kV and 499 kV that are located at a single station or substation, which is connected to three or more other station or substations by lines operated between 200 kV and 499 kV and which possess an “aggregate weighted value” exceeding 3000. The “aggregated weighted value” of the station or substation is determined by summing the “weight value per line” shown in the table below for each BES Transmission Line that is connected to another Transmission station or substation.” This proposed wording properly associates the aggregated weighted value with a station or substation, not a Facility (e.g. BES line, transformer, or generator element). The proposed wording also qualifies that the applicable Facilities are the ones at the qualifying station or substations. In the case of an applicable transmission line, the criteria is only the portion of the line’s Facilities at qualifying substation, not the portion of the line’s Facilities at the other substation, unless the station or substation at the other end of the line also meets the aggregated weight value threshold. For Criterion 2.6 – Replace the unclear wording of ‘. . . as critical to the derivation of IROLs and their associated contingencies’ with wording of, ‘. . . as Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more IROL violations’, which would be consistent with wording used in Criterion 2.8 and 2.9. The Facilities that could cause an IROL to be violated are usually different from the Facilities that IROL was developed to assure would not cause an unacceptable impact on the reliability of the BES when they are lost.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form A.
Group

Edison Electric Institute
David Batz
(1.)Change time frame in all affected standards to read 'once each calendar year OR a period not to exceed 15 calendar months '. The affected standards are CIP-004 R3.2, R6.6, R6.7; CIP-007 R5.6; CIP-008 R2.1, R3.1; CIP-009 R2.1, 2.2; CIP-010 R3.1; and CIP-011 R1.3. (2.)Rather than the current approach to identify 'Facilities, Systems, and equipment,' modify this to identify High Impact Sites, Medium Impact Sites with all BES Sites not identified as High Impact or Medium Impact being identified as Low Impact. For Low Impact, maintaining inventories at the site level would avoid the concern that discrete equipment identification is required. (3.) We need a clear definition of dial-up to eliminate the confusion of what dial-up includes and what it does not include; for example leased lines to modem banks should not be included. Without a clear definition auditors could interpret devices that are used for point-to-point communication over leased lines as dial-up and include these devices as dial-up assets under the CIP standards.; (4.)Need clarity on which Transmission Owners' control centers who are not Operators will be classified as High Impact. Attachment 1-Item 1.3 - uses the term 'functional obligation'. This term is not defined. Also not clear is the meaning of -to control- an asset. The example to demonstrate the confusion is a Transmission Owner Control Center that can remote open/close breakers but only under the direction of the Transmission Operator. The Transmission Owner does not have the functional obligation of the Transmission Operator and the Transmission Operator has the Operating Authority over the breakers. Suggest that clarity in 1.3 can be obtained by restating as: perform the functional obligations of the Transmission Operator for the assets that meet criteria 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.1., and adding to the technical guidance clarification that a Cyber System that can remote operate assets that meet criteria 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10 where the Entity is not performing the functional obligation of a Transmission Operator are Medium impact. This comment also applies to Attachment 1 - Item 2.11.
(1.)Low Impact BES Cyber Systems a. The current wording reflects an attempt by the CIP SDT to provide 'protection' from discrete identification of low impact BES cyber systems, yet the requirements are (still) framed in a way that would require discrete identification to adequately demonstrate compliance. This provides conflicting messages that would impede approval of protection controls for BES Cyber Systems used within High and Medium Impact facilities. (2.) Throughout the standard, references to Low/Medium/High Impact should be applied to facilities and not BES Cyber Systems. Per CIP-002 Attachment A, it is the facilities which determine the Impact and not the BES Cyber System. Rather than the existing R1 language 'Each Responsible Entity for its high impact and medium impact BES Cyber Systems,' use 'Each Responsible Entity for its BES Cyber Systems used in high impact and medium impact facilities.' This will clarify the facility first approach. (3.) There is a clerical error in the Introduction, section 4.2.4 where it provides exemptions from CIP- 002-5. This would seem to reference exemptions from CIP-003-5. (4.) R2 a. Original language - For BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics: b. Proposed change - For BES Cyber Systems used in facilities not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics: c. Rationale: The shift of impact ratings to facilities supports the process in which facilities determine impact. (5.) R2 VSL a. The Table of Compliance Elements references a Medium VRF whereas the requirement identifies a Low VRF. b. Given the R2 requirement for BES Cyber Systems used within Low Impact facilities, the VSL should be shifted to the left to use Lower/Moderate VSLs. Per the subjects covered within CIP-003, there are no direct impacts on BES reliability should a policy clerical error occur or Senior Manager designation not be captured adequately. (6.) R3 - The R6 content applicable to R3, requiring the documenting of changes to the Senior Manager within 30 days, should be included within R3. This will eliminate 'double jeopardy' concerns where failure to adequately document changes will now result in the violation of a single requirement. (7.)R4 - VSLs a. Propose framing review violations as lower/medium VSLs as follows: i. Lower - Policies have not been reviewed within 30 days of annual review time periods ii. Medium - Policies have not been reviewed within 60 days of annual review time periods b. For Policy approval: iii. High - Policy has not been approved within 30 days of annual approval timelines iv. Severe - Policy has not been approved within 60 days of annual approval timelines c. Rationale - There is a difference between approved policy and review of policies. The current approach repeats the violation in which 'not all policies have been approved within the required time period,' which creates confusion. By recognizing the difference in importance (approve vs. review) and framing review violations as less

severe, this provides a more relevant scale. (8.) R5 a. The R6 content applicable to R5, requiring the documenting of changes to delegations within 30 days, should be included within R5. This will eliminate 'double jeopardy' concerns where failure to adequately document changes will now result in the violation in the violation of a single requirement. b. What is meant by the words 'specific actions'? We suggest striking the words 'specific actions' as it is too subjective to audit. (9.) R6 - Propose removal once recommended changes to R3 and R5 are enacted. This requirement simply identifies time constraints to document changes to R3 and R5 requirements. Any violation of this requirement would also result in the violation of R3 or R5 and introduces 'double jeopardy' concerns. (10.) Remove 'egress' from Guidelines 1.4

Individual

Kirit Shah

Ameren

No

Yes

(1)We appreciate the effort and detail that the SDT went through to develop this draft revision 5 to standard CIP-002. However, we believe the SDT has not provided clarity to the language of the proposed requirements, and has combined Facilities, Cyber Systems, and associated Cyber Assets such that it is confusing. We proposed that SDT start by developing a flowchart of the identification process, and the requirements, they should be pulled from the flowchart. Please notice that on page 33 of the Application Guideline there is a process flow chart, but also note that it does not start with a Facility and we feel this needs to be revised to add clarity and details. We feel that this flow chart should be part of the standard. Further, R1 and its sub-requirements should strictly address the identification of Facilities that impact the reliability of the BES. R2 and its sub-requirements should address the identification of BES Cyber Assets, and R3 and its sub-requirements should address the identification of BES Cyber Systems. The existing R2 approval of the facility identification should then become R4. (2)We recommend that Facilities are the first place to begin with when identifying cyber assets, because that is where Impact to the BES originates, even though there are questions about how we define various facilities; RTU's and substations. Then it will be clear that we are addressing BES Cyber Systems which are used in High, Medium or Low Impact Facilities. Attachment 1 should be retitled Facility Rating Criteria. Item 1, High Impact Rating (H) should be changed to High Impact Facilities (H) as it applies to BES Facilities and not to BES Cyber Systems. Item 2, Medium Impact Rating (M) should be changed to Medium Impact Facilities (M) BES Facilities and not to BES Cyber Systems. Item 3, Low Impact Rating (L) should be changed to Low Impact Facilities (L). If requirements are developed for Low Impact Facilities, they should be included as a separate standard. (3) No definition for "Adverse Impact of the reliable operations of the BES" is included in the standard or the application guidelines. In this regard, we suggest SDT to provide the definition of "Adverse Impact of the reliable operations of the BES" included on page 8 in the section on Real Time Operations, and also clarify is it the Impact on the BES or Impact on a Facility. Also note that definition of BES Cyber Asset (in the definition document) does not include the word "adverse" related to reliable operation of the BES. Suggest consistency or using NERC Glossary term "Adverse Reliability Impact" (pg 4 of the NERC glossary) definition to define/replace "Adverse Impact of the reliable operations of the BES". Definition of Adverse Reliability Impact is "The impact of an event that results in Bulk Electric System instability or Cascading." (4) The "15 minute time frame" included in the definition of BES Cyber Assets is problematic to provide evidence during the compliance audit. We suggest adding some guidance to the CIP-002-5 standard to help understand what type of evidence would suffice or identify some examples of BES Cyber Assets that would create an Adverse Reliability Impact within 15 minutes. (5) We ask that the SDT clarify their intention on page 8 under “Reliable Operation of the BES. The second sentence states “BES Cyber System perform or support any BES reliability function according to those reliability tasks identified for Functional entities in the NERC Function Model.” Even with the guidelines attached to CIP-002-5, we read this statement to mean all BES reliability function must be cross referenced against the system they use, and any system that may impact one of these functions in any way, must have security protections. (6) R1.3 states “low impact does not require discrete identification,” and Attachment 1 shows a list of Low assets requiring protection. These statements are all contradictory with R1.4 that states entities must track changes in the impact categorization from a lower to higher impact category to update the BES Cyber Asset list. The current wording is such that it will require discrete identification of low Impact Cyber Assets to adequately demonstrate compliance and this is a conflicting message that would impede approval. We

would propose to the SDT removing BES Cyber Systems used within Low Impact Facilities from the current draft 2 standards. If the drafting team must keep the Low Impact Facilities in scope, an entity should only be required to keep a list of facilities and not the cyber asset list. (7) The format of the draft standard is completely different from the other NERC reliability standards; for example, the background section in CIP-002-5 is included prior to the requirements and then application guidelines follow at the end. If the background and application guidelines are to be retained, we suggest both to be included at the end of the standard.
No
No
No
No
No
No
(1) R1 – Proposed word change for the requirement - “Each Responsible Entity for its high impact and medium impact BES Cyber Systems,” should be changed to “Each Responsible Entity for its BES Cyber Systems used in High Impact and Medium Impact Facilities.” This will clarify the Facility first approach. (2) R2 – Proposed word change for the requirement – "For BES Cyber Systems used in Facilities not identified as High Impact or Medium Impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics". The shift of impact ratings to Facilities supports that it is the Facilities which determines the impact. (3) R2 VSL - The VSL should be shifted to the left to use Lower/Moderate VSLs. Also note that the Table of Compliance Elements references a Medium VRF whereas the requirement identifies a Low VRF. (4) R3 – Need to add applicable content from R6 to R3 requirement, language should be added requiring the documenting of changes to the Senior Manager within 30 days, within R3. This will eliminate ‘double jeopardy’ concerns where failure to adequately document changes will only result in the violation of a single requirement. (5) R4 – Need to remove the words "and R2" from the requirement. This will eliminate the security policies for Low Impact BES Cyber Systems having to be signed by the Senior Manger each calendar year. We would suggest that these r policies for Lower Impact can be signed by a delegate instead of the Senior Manager. (6) R4 – We suggest the following changes for the R4 VSLs: Rationale – There is a difference between approving the policies and review of policies as written this repeats the violation in which ‘not all policies have been approved within the required time period,’ which creates confusion. (a) Lower – Policies have not been reviewed within 30 days of annual review time periods. (b) Medium – Policies have not been reviewed within 60 days of annual review time periods. (c) High – Policy has not been approved within 30 days of annual approval timelines. (7) R5 – Need to add applicable content from R6 to R5 requirement, requiring the documenting of changes to delegations within 30 days, should be included within R5. This will eliminate ‘double jeopardy’ concerns where failure to adequately document changes will only result in the violation of a single requirement. Also define and clarify the phrase “where allowed by the CIP Standards”. (8) R6 – We recommend that SDT remove this requirement, it simply identifies time constraints to document changes to R3 and R5 requirements as stated in our comment for R3 and R5 above. Not removing this requirement introduces ‘double jeopardy’ concerns. If requirement R6 must stay need to replace the word "delegator" with "Senior Manger" to help clarify this requirement.
Group
Salt River Project
Sara McCoy
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Individual
Michael Lombardi
Northeast Utilities
Yes
Yes
Attachment 1, Section 2.5 - We agree with the Drafting Team that the use of “aggregate weighted values” provides an objective approach for determining the potential impact level used for categorizing BES Cyber Assets. However, we also believe that due to variations between electrical systems that “one size does not fit all” and a mechanism should be in place to allow the asset owners to refine the impact level using studies and risk base analysis. Attachment 1, Section 2.6 - refers to facilities “that are identified by its Reliability Coordinator, Planning Coordinator or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.” Please clarify under which reliability requirement the Reliability Coordinator (RC), Planning Coordinator (PC) and Transmission Planner (TP) is required to inform each of the “Responsible Entities” associated with CIP-002-5. Without a notification requirement for the RC, PC and TP, the Responsible Entities are at risk of not complying with this standard. Attachment 1, Section 2.11 - Control Center is not a NERC defined term. Please clarify that Control Center used in this context refers to Regional (RTO/ISO) and Local (LCC) control centers and not the main control room of generating stations/units. Consider organizing the “Guidelines and Technical Basis” by subject (e.g., Transmission, Generation, etc.)
Yes
Yes
Yes
Yes
Yes
Yes
R1 and R2 - Recommend that a cross reference associated with each of the listed topics is provided. For example, revise 1.1 Personnel Security to read 1.1 Personnel Security (CIP-004) R5 - the first sentence of the rationale for R5 states: “The intent of the requirement is to ensure clear accountability within an organization for certain security matters.” It is not clear what is meant by “certain security matters.” Recommend that clarification be provided regarding what the limitations are concerning the delegation of authority by the CIP Manager.
Group
Florida Municipal Power Agency
Frank Gaffney
No
No
FMPA has comments for both Question 1 and Question 2. However, those questions no longer have a comments box in which to insert them. After speaking with Steven Noess at NERC, I was told that I could insert them here. (1) Question 1: First, FMPA wishes to thank the SDT for all of their hard work and a significantly better product than earlier versions. However, there are a few issues that cause us to vote negative as described in these comments. Requirement R1 is silent on what relationship to an asset or cyber system causes an entity to be responsible for that asset or cyber system which creates many opportunities for double jeopardy. For instance, is the owner or operator responsible? Is the outsourcer or outsource responsible? As written, if the GO and GOP, or TO and TOP are different entities, it would seem that both are responsible for the same thing creating conflict and double jeopardy, and in some ways decreasing security due to this ambiguity of authority. Due to the many types of different business arrangements that exist and the fact that we shouldn’t care who is responsible as long as one registered entity takes responsibility, FMPA suggests adding a statement something like: “If an asset or cyber system is used by more than one entity, the entities may decide amongst themselves which entity will take full responsibility for the standards for that asset or cyber system”. The sub-bullets of R1 use the term “Systems” which is defined in the NERC Glossary as including distribution, i.e., “A combination of generation, transmission, and distribution components”.

Distribution is specifically excluded from the standards through the Federal Power Act, Section 215, at (a)(1) and (i)(1). FMPA believes the SDT intends this phrase to only apply to UFLS and UVLS. As such, the term “Systems” should be eliminated since the term “equipment” is sufficient. Although we are appreciative of the efforts to minimize impacts on microprocessor based UFLS and UVLS relays, we are still very concerned of the broad reaching consequences of application of the standards to every microprocessor based relay whether or not that relay has connectivity via routable protocol. In the last round of comments, FMPA proposed the addition of a De Minimus Impact category, which the SDT interpreted narrowly as meaning only impact without a risk adjustment. While we understand that the impact of a relay is the same whether connected via routable protocol or not, we also recognize that the risk of malicious activity is significantly higher for relays connected via routable protocol. Hence, we amend our recommendation to create a De Minimus Risk category for which the standards would not be applicable for BES Cyber Assets that would fall within the Low Impact category but are not connected by routable protocol. Such a step would significantly reduce the administrative burden of the standards at little to no risk to reliability. (2) Question 2 comments: R2 has become redundant as a result of R1 bullet 1.4. The only purpose of an annual review is for change management, which is now covered by R1 bullet 1.4. Having a senior manager approve is simply an internal control not worthy of a requirement. FMPA proposes deleting R2, especially in light of paragraph 81 of the FERC Order approving Find Fix Track Report (FFTR).
Yes
No
No
No
No
No
FMPA has comments for both Question 4 through Question 9. However, those questions no longer have a comments box in which to insert them. After speaking with Steven Noess at NERC, I was told that I could insert them here. (1) Question 5: The word “implement” is problematic for Low Impact assets. The definitions of “implement” is “carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures”. Using such a definition means that for Low Impact assets, detailed end result measures of implementation would be needed to prove compliance with the requirement, including system by system information regarding access controls, granting access, denying access, etc., (otherwise, how would an entity prove that a electronic access policy was implemented?) which does not meet the intent of the SDT to remain at a “programmatic” level for Low Impact system. FMPA suggest using the phrase “in force”, e.g., “For BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall have one or more documented cyber security policies in force that address the following topics.” Rewording the requirement in this way would mean that the only evidence needed is the policy itself, and not additional proof that the policy was implemented. (2) Question 6: R3 is an internal control not worthy of a requirement, especially in light of paragraph 81 of the FERC Order approving Find Fix Track Report. FMPA suggests deleting the requirement. (3) Question 7: R4 is an internal control not worthy of a requirement, especially in light of paragraph 81 of the FERC Order approving Find Fix Track Report. FMPA suggests deleting the requirement. (4) Question 8: R5 is an internal control not worthy of a requirement, especially in light of paragraph 81 of the FERC Order approving Find Fix Track Report. FMPA suggests deleting the requirement. (5) Question 9: R6 is an internal control not worthy of a requirement, especially in light of paragraph 81 of the FERC Order approving Find Fix Track Report. FMPA suggests deleting the requirement.
Individual
Brian J Murphy
NextEra Energy, Inc.
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. 1. R1.4. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program as is appropriate for that entity. Thus, NextEra disagrees with the implementation of an arbitrary deadline, and, therefore, that

R1.4 be revised to read as follows: “Review, keep current and update, at a timeframe that the Responsible Entity deems necessary, the identification in Requirement R1, Parts 1.1, 1.2, and 1.3 of when a change to BES Elements or Facilities is placed into operation, which is planned to be in service for more than six calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category. “ 2. R2. As a preferred alternative to that suggested by EEI, NextEra does not agree that a CIP Senior Manager is necessary to implement a robust, current and updated CIP compliance program. Thus, NextEra requests that the concept of a CIP Senior Manager be deleted from all CIP Reliability Standards. For support, NextEra notes that there is no evidence that without a CIP Senior Manager there is any additional risk to the BES. Further, the unnecessary focus on title of an employee and the duties of an employee is not only micromanaging a Responsibility Entity, but also takes away essential flexibility from an entity to design a CIP compliance program that best promotes cyber security. NextEra further believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R2 be revised to read as follows: “ The Responsible Entity shall approve the identifications required by Requirement R1 as the Entity deems necessary.” 3. As a preferred alternative to that suggested by EEI, with respect to CIP-002-5 Attachment 1, Section 2 (Medium Impact Rating), NextEra is concerned that the draft language in Section 2.1 (and elsewhere) does not appropriately take into consideration the significant operational differences between wind and solar generation (intermittent resources) as compared to fossil generation. Wind and solar units, because of their intermittent nature, do not pose the same cyber security threat to the grid as traditional fossil units. NextEra therefore requests that drafting team adopt rating criteria for Attachment 1 that differentiates between intermittent resources and fossil resources and does not automatically result in a Medium Impact Rating for wind and solar units unless a Transmission Operator, Reliability Coordinator, Planning Coordinator, or Transmission Planner has in writing specifically identified the wind or solar unit as critical to reliability. In other words, NextEra requests that the Low Impact Rating be adopted as the default category for wind and solar units that are part of the Bulk Electric System. 4. As a preferred alternative to that suggested by EEI, NextEra also supports Mid-American's proposals on CIP-002-5 and in particular adding language as follows: Each Responsible Entity shall implement R1; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws in the application of the criteria set forth in R1.1 through R1.5 do not constitute per se violations of R1 NextEra also prefers the following language that provides for 15 months be used for the annual review processes in CIP-00-5: “The Responsible Entity shall update these lists as necessary, and review the list(s) at least once each calendar year or not to exceed 15 months between reviews.”
No
No
No
No
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. R3-R6. As a preferred alternative to that suggested by EEI, NextEra does not agree that a CIP Senior Manager is necessary to implement a robust, current and updated CIP compliance program. Thus, as noted above, NextEra requests that the concept of a CIP Senior Manager be deleted from all CIP Reliability Standards. The unnecessary focus on title of an employee and the duties of an employee is not only micromanaging responsible entities, but also takes away essential flexibility from an entity to design a CIP compliance program that best promotes cyber security. Therefore, NextEra requests the deletion of R3, R5, and R6. NextEra further believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R4 be revised to read as follows: “Each Responsible Entity shall review and update cyber security policies identified in Requirements R1 and R2, at a timeframe that the Entity deems necessary.”
Group
Madison Gas and Electric Company
Joseph DePoorter

No
Yes
Please see the MRO NSRF Comments. MGE has the following addition comments concerning CIP-002-5: For Criteria 2.11; A BA or TOP may only provide a very small number of individual functions as described within the Functional Model (and within the Application Guidelines) based on the CFR or JRO that they have filed at NERC. Every BA and TOP does not have the same impact on the BES as a larger BA or TOP. As written, 2.11 will require every BA and TOP that is registered as such as being in the “medium” category. This one size fits all approach does capture the entities that have an impact on the BES. The SDT uses a threshold of “300 MW or more of BES generation” based on a 300 MW limit of UFLS and UVLS within the Application Guide. Within a UFLS or UVLS system, the control is “instantaneous” where a BA that is responsible for 300 MW or more of BES generation can only “control” the generation. Recommend the words “controllable in real time” be added. This will take into consideration the ownership of joint generation units that BA’s may share. Recommend the second sentence of 2.11 to read; “… of the preceding 12 calendar equal to or exceeding the controllable in real time amount of 300 MW or more BES generation”. This slight change will support FERC Order 706, paragraph 253, FERC clearly speaks of being flexible “However, we are persuaded by commenter’s that stress the need for flexibility and the need to take account of the individual circumstances of a responsible entity.” The SDT may wish to maintain what is presently approved that BA’s be viewed as in Attachment 1, CIP-002-4 brightline criteria 1.17 concerning a BA control center “Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection”. This is presently FERC approved where the 300 MW threshold is only based on UFLS or UVLS thresholds (and has no firm basis). The 1500 MW comment is based on criteria 2.1 of version 5. Where the generation threshold of 1500 MW is used to assure that generation is captured as a medium impact. This provides a consistent approach that a generator within a BA area with the 1500 MW threshold and the BA are assigned the same level of impact to the BES. Another concern with criteria 2.11 is that a TOP registered as a TOP does not “control” any “real power”.
Yes
No
Yes
Yes
Yes
Yes
Please see the MRO NSRF Comments.
Group
Pepco Holdings Inc & Affiliates
David Thorne
Yes
Yes
1)2.7 of Attachment 1 Does not take into consideration Facilities not identified as “Transmission” i.e. Sub-Transmission or Distribution facilities that are essential to meeting NPIR’s. This requirement is presumptive to being high voltage BES components only. 2)Shouldn’t a facility be considered essential if it is required by a Nuclear Plant License/NRC regardless of the voltage of the service. 3)Section 3.3 of Att. 1, What is the point to identify “Low Impact Cyber Systems” but have no discrete identification requirements of the resource. Could this result in a null list? 4) Does R2 this supersede an entities definition of Annual?
Yes
No
Yes
Yes
Yes
Yes
1) O5 - R2--If discrete identification is not required then enforcement becomes ambiguous. 2) O4--R4

--Yes, but does this supersede an entities definition of annual if so then it must be made clear 15 months is an absolute value from the prior review. Also if an additional 3 mo. is granted can the review be made 3 mo. prior to its due date and be considered valid? If so the review should be performed each calendar year on the anniversary + or – 3 months.

Group

National Rural Electric Cooperative Association (NRECA)

Barry Lawson

4.2.1 and 4.2.2, and Attachment 1, 2.10 – The threshold for 300 MW of UFLS or UVLS load shedding is clear, but saying "that are part of a Load shedding program" implies that an entity could have only 50 MW of load that will be shed as part of a larger 300 MW "program" and be drawn into the applicability and required to comply with the Medium Impact facility requirements. Another scenario is where a DP with a 250 MW load shedding program not associated with any other group would not come into applicability at all. NRECA recommends that the SDT provide guidance with very clear examples of scenarios that would include or exclude DP or LSE entities from required compliance with CIP Version 5 standards. Under the inclusion threshold for DP, 4.2.2, third bullet, states: "A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard." NRECA recommends that the following language be added to the end of that bullet; ", and where the Protection System is connected to a supervisory control system providing remote operation capability." This language will help to further appropriately clarify the scope of applicable Protection Systems in the CIP standards. Attachment 1 2.10 – see comment above 2.11 – The 300 MW value should be revised to 1500 MW to properly align it with 2.1 in the Medium Category. The 300 MW value has not been adequately technically justified and the resulting potential compliance obligation actions and costs that could be required will likely far outweigh the reliability benefit of keeping the 300 MW value in this section. If the change to 1500 MW is made, then all other Control Centers, and associated data centers, not included in the High or Medium Category will be included in the Low Category. This is a major issue for NRECA. It will be difficult to support CIP-002-5 without this revision.

No

R2 – NRECA is concerned that even though it is stated that a list of Low Category assets is not required for compliance, we do not see how compliance could be proven/demonstrated without such a list. Given that the requirements for Low Category assets are intended to be programmatic in nature, and not asset specific, NRECA requests that the SDT make changes necessary to not in effect require a list of Low Category assets to demonstrate compliance.

Individual

Christina Conway

Oncor Electric Delivery Company LLC

No

Yes

GENERAL CIP-002-5 COMMENTS: (1) The Background section or Application Guidelines of CIP-002-5 should provide more discussion and detailed examples of the "BES Cyber System" concept. Multiple examples should be provided to address typical varying Responsible Entity configurations. This will aide in explaining the new "BES Cyber System" concept to the Responsible Entities. If there is a better understanding of the concept and how it applies to various facilities/assets, then Responsible Entities will be more likely to support the standards. (2) A high level summary of the CIP version 5 standards that shows the interaction between each standard, applicability type, and definition should be provided with the next draft. This will help resolve any remaining inconsistencies and overlaps between standards prior to the next draft. (3) Oncor supports the comments submitted by EEI in response to this question. ATTACHMENT 1 AND R1 REQUIREMENT COMMENTS: Oncor supports the proposed solution developed by the Midwest Reliability Organization NERC Standard Review Forum to clarify the flow for identifying BES Cyber Systems. Draft 2 of CIP-002-5 Requirement 1 appropriately reflects an attempt to provide 'protection' from forcing Registered Entities to discretely identify BES Cyber Systems used at Low Impact Facilities. Unfortunately, the language in this requirement is inconsistent with CIP-003-5 Requirement 2, which requires a Registered Entity to implement one or more documented cyber security policies for "BES Cyber Systems not identified as high impact or medium impact." To demonstrate that it has implemented the required cyber security policies for "BES Cyber Systems not identified as high impact or medium impact," a Registered Entity would likely

be forced to develop a list of low impact BES Cyber Systems. This is a significant point of concern given the resources, processes, time, and documentation that would be required to ensure the ability to demonstrate compliance for low impact BES Cyber Systems.
Yes
No
No
Yes
No
No
R2 REQUIREMENT COMMENTS: Oncor supports the proposed solution developed by the Midwest Reliability Organization NERC Standard Review Forum to clarify the flow for identifying BES Cyber Systems. Draft 2 of CIP-002-5 Requirement 1 appropriately reflects an attempt to provide 'protection' from forcing Registered Entities to discretely identify BES Cyber Systems used at Low Impact Facilities. Unfortunately, the language in this requirement is inconsistent with CIP-003-5 Requirement 2, which requires a Registered Entity to implement one or more documented cyber security policies for "BES Cyber Systems not identified as high impact or medium impact." To demonstrate that it has implemented the required cyber security policies for "BES Cyber Systems not identified as high impact or medium impact," a Registered Entity would likely be forced to develop a list of low impact BES Cyber Systems. This is a significant point of concern given the resources, processes, time, and documentation that would be required to ensure the ability to demonstrate compliance for low impact BES Cyber Systems. R3 REQUIREMENT COMMENTS: The CIP-003-5 R6 content that is applicable to CIP-003-5 R3, which requires the documentation of changes to the Senior Manager within 30 days, should be included within CIP-003-5 R3. This will eliminate 'double jeopardy' concerns where failure to adequately document changes could result in the violation of two requirements. R5 REQUIREMENT COMMENTS: The CIP-003-5 R6 content that is applicable to CIP-003-5 R5, which requires the documentation of changes to delegations within 30 days, should be included within CIP-003-5 R5. This will eliminate 'double jeopardy' concerns where failure to adequately document changes could result in the violation of two requirements. R6 REQUIREMENT COMMENTS: CIP-003-5 R6 should be removed after the recommended changes to CIP-003-5 R3 and CIP-003-5 R5 suggested above are adopted. This requirement simply identifies time constraints to document personnel changes in positions described in CIP-003-5 R3 and CIP-003-5 R5. Any violation of this requirement could also result in the violation of CIP-003-5 R3 or CIP-003-5 R5 and introduces 'double jeopardy' concerns. GENERAL COMMENT: Oncor supports the comments submitted by EEI in response to this question.
Individual
Gregory J. LeGrave
Wisconsin Public Service Corporation and Upper Pennisula Power Company
No
No
WPS and UPPCO support the comments submitted by EEI and the MRO NSRF. In addition WPS and UPPCO make the following comments: • The requirements on Low Impact Assets are too vague to assure consistent implementation and enforcement. Since the assets are self-described as having a low impact on the BES these requirements should be deleted. Barring deletion, the drafting team should better describe the requirements • The re-definition of annual is arbitrary and capricious and does not improve the safety, security, or reliability of the BES. • The definitions continue to be too complex and unclear. The drafting team needs to simplify and clarify the terms to assure consistent implementation and enforcement
No
No
No
No
No
No
WPS and UPPCO support the comments submitted by EEI and the MRO NSRF. In addition WPS and UPPCO make the following comments: • The requirements on Low Impact Assets are too vague to

assure consistent implementation and enforcement. Since the assets are self-described as having a low impact on the BES these requirements should be deleted. Barring deletion, the drafting team should better describe the requirements • The re-definition of annual is arbitrary and capricious and does not improve the safety, security, or reliability of the BES. • The definitions continue to be too complex and unclear. The drafting team needs to simplify and clarify the terms to assure consistent implementation and enforcement
Individual
Don Jones
Texas Reliability Entity
No
No
•Blackstart Units should not be discounted from the audit program. Blackstart Units should be rated at least at medium if not always high. •Items designated as low need to be documented. This covers the aspect of a whole, complete, and accurate evaluation. •The standard as drafted may dramatically affect the applicability of the CIP standards for a majority of GOPs which is not in the best interest of reliability. This is accomplished by the criteria included in Attachment 1 which requires a generation threshold of 1500 MW and the criteria language included in 2.3, 2.6 and 2.9. Was there any analysis or data on the effect that this would have on the applicability of CIPs for GOP CIP programs? The language appears to be worst case scenario from a planning perspective and seems to place an unreasonable high bar for the CIPs applicability to GOPs. In addition, what is the process or mechanism used to notify a GOP of such a designation from its PC or TP? •The VSLs for R1 include language stating, “For a Responsible Entities with more than a total of 40 facilities....” What is the significance of the quantity of 40 facilities and if a Responsible Entity has less than 40 facilities how would that impact the VSL analysis? Also, R1 includes Systems or equipment yet the VSLs make no mention. Is there a reason for the exclusions?
Yes
Yes
No
Yes
Yes
Yes
•The designated Senior Manager documentation should include title and documented responsibilities. •If R2 does not require an inventory list or discrete identification of the BES Cyber Systems (that have not been identified as high or medium impact) how would a CEA assess compliance with this requirement?
Individual
Don Schmit
Nebraska Public Power District
No
Yes
[1] The proposed methodology prescribed by Requirement 1 is in direct conflict with the structure of the definition for BES Cyber Asset and BES Cyber System. The impact rating should align with the facility (BES Site) instead of the cyber asset. [R1 Proposed Flow] 1.1-Based on the definition for a BES Site, each entity should create a list of BES Sites. This step will determine for the entity, which sites have zero BES impact vs. which sites have an impact and will be later divided into high, medium, and low. The criteria for BES Site can also be considered the positive definition or threshold for Low Sites. These are sites that, based on the definition, will have some impact and require, at a minimum, programmatic protection at the Site level. There will be no need to identify the cyber assets associated with sites that have zero impact or those that remain in the Low category. All Sites will have the protections afforded the Low sites, but for those meeting the Medium and High criteria, additional protections are required, as well as the enumeration and classification of the cyber assets critical to providing the BES functionality of the location. After identifying the BES Sites, the Medium and High criteria must be considered for each Site. The following is a proposed flow for which the order can be modified while maintaining efficacy. 1.2- Based on the candidate list for sites with BES

impact created from the execution of the first step, identify the High impact sites using the criteria in the attachment. A candidate list for cyber assets required in order for the BES Site to perform its reliability function(s) will be created for the High Sites. The cyber assets that are critical to the performance of the reliability function will then be divided into those with (A) or without (B) External Routable Connectivity, those cyber assets used for Electronic (C) or Physical Access (D) Control or Monitoring, and those cyber assets connected within the same ESP (E) as the cyber assets necessary for the performance of the reliability function. 1.3 – Based on the sites that remain on the candidate list and are not High impact, determine the medium sites based on the criteria in the attachment. A candidate list for cyber assets required in order for the BES Site to perform its reliability function(s) will be created for the Medium Sites. The cyber assets that are critical to the performance of the reliability function will then be divided into those with (F) or without (G) External Routable Connectivity, those cyber assets used for Electronic (H) or Physical Access (I) Control or Monitoring, and those cyber assets connected within the same ESP (J) as the cyber assets necessary for the performance of the reliability function. Note: There are 10 types of cyber assets positively identified through this process, each with varying levels of risk to the BES if compromised or rendered unavailable. This, potentially, creates more than 10 levels of protection to be enumerated throughout the rest of CIP-003 through CIP-011. For administrative ease, the MRO NSRF recommends grouping these types of cyber assets based on their actual level of risk in each scenario involving a potential incident that is either cyber or physical in nature and based on the External Routable Connectivity. The rest of the Standards should be written to address each type or grouping of asset. Silence on any one type or grouping will lead to confusion regarding the necessary protective measures and commensurate improvement to security posture. 1.4 – Everything that made the initial candidate list requires protection of some sort, so if it didn't get picked for High or Medium, it gets assessed at Low, because it met the threshold criteria in the BES Site definition. Verbiage in the definitions and the requirements should support this process flow, which will allow the enumeration of High Sites, Medium Sites, and Lows Sites (since we all know a list is required to demonstrate even programmatic elements of CIP compliance). The lists of Cyber Assets will only be required at Medium and High Sites. If possible and feasible, the criteria for dividing the sites into those categories should be progressive in nature, allowing clear demarcation and rationale for the criteria chosen. Additionally, the rest of the Standards should address the requirements progressively for the asset types based on risk. The shift from the current draft to one with obvious progression throughout the CIP-002 methodology and again throughout the rest of the Standards will allow for ease of application at each entity. The current draft does not provide the entities with clear understanding of the order and rationale for identifying the scope of applicability for the CIP Standards, and the NPPD feels that the entities can't be successful with the current format. [2] Change the CIP-002 VSLS to reflect "BES Sites" instead of "Facilities" as those would be the enumerated list. In its current state, it conflicts with the statement that low and zero impact sites do not require enumeration. [3] All VSLs should change the impact designation from cyber asset based to site-based. "High," "Medium," or "Low" designations should precede the word "Site" not "BES Cyber Asset" or "BES Cyber System."
Yes
No
Yes
Yes
Yes
Yes
(1) [Proposed Verbiage] CIP-003 R1 Each Responsible Entity for the identified BES Cyber Systems critical to the operation of high impact and medium impact BES Sites shall implement one or more documented cyber security policies that address the following topics: Keep 1.1 – 1.10 as is. (2) [Proposed Verbiage] CIP-003 R2. For BES Sites identified as low impact, each Responsible Entity shall provide guidance with one or more documented cyber security policies that address the following topics: [Violation Risk Factor: Low] [Time Horizon: Operations Planning] The programmatic elements identified in the sub-requirements may remain, as is. Remove the statement eliminating the need to enumerate low facilities, as it is in conflict with the rest of the verbiage and definitions in the CIP-002-5 and CIP-003-5. (3) VSLs should reflect the actual risk to the BES when one or more elements are missing. The absence of a program should be high or severe, but the lack of discrete components should start at Low.

Group
Luminant
Rick Terrill
No
Yes
Luminant thanks the SDT for their work and the changes made in response to previous comments. In particular Luminant agrees with moving Blackstart Resources to Low Impact for improved BES reliability, and we support the consolidation of Low Impact requirements into one standard. For all responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
Individual
Stephanie Monzon
PJM Interconnection
Yes
Yes
Yes
No
Yes
No
No
No
R3 - We agree with the requirement but have issues with the definition of a CIP Senior Manager in that the definition should include the operation and maintenance of the requirements (ongoing compliance). Looking at the definition of a CIP Senior Manager it appears that after the requirements are implemented, according to the implementation plan, that there is no longer a need for a “CIP Senior Manager”. This appears to contradict what is required in CIP-003 R4 & R5 – Change the verbiage from “dated signature” to “dated approval”. The current verbiage does not take into account electronic workflow approvals. M6 Please update this verbiage so that it is clearer and more easily understood
Individual
Andrew Gallo
City of Austin dba Austin Energy
No
No
Please see the comments submitted by the Texas Reliability Entity NERC Standards Review Subcommittee to which Austin Energy has subscribed.
Yes
No
No
Yes
No
No
Please see the comments submitted by the Texas Reliability Entity NERC Standards Review Subcommittee to which Austin Energy has subscribed.
Group
Southern California Edison Company
Nathan Smith
Yes

Yes
SCE comments to CIP-002-5: -Introduction A. 3. Purpose: Please clarify the term “misuse”. “Misuse” does not have to be malicious. Perhaps the section should be revised to say “…impact that loss, compromise, or intended malicious misuse of those BES Cyber...” -Facilities 4.1.6: Revise “Load-Serving Entity that owns Facilities” to “Load-Serving Entity that operates owns Facilities” to be consistent with the PRC standards.
Yes
Yes
Yes
Yes
Yes
Yes
SCE Comments to CIP-003-5 -R5: Please list the areas that do allow delegations.
Individual
Kathleen Goodman
ISO New England
No
No
Request clarification on the Applicability of Distribution Providers (DP) and Load Serving Entities (LSE). 1. Does 4.1.2 mean that any DPs owning assets in 4.2.2 need to comply with these CIP Standards? 2. Does 4.1.6 mean that LSEs owning assets in 4.2.1 need to comply with these CIP Standards? 3. Does 4.2.2 mean that only these DP assets are covered by these CIP Standards? 4. Does 4.2.1 mean that only these LSE assets are covered by these CIP Standards? 5. Does the DP’s third bullet in 4.2.2 apply to only protection systems, not UFLS or UVLS since those load shedding systems are covered by the DP’s first bullet? Note the NERC definition of “protection systems” includes load shedding systems, which generates this last question. 6. Section 4.2 should explicitly state that UFLS Systems that perform automatic load shedding of less than 300 MW are specifically excluded. Request clarification on High Impact 1.3 and 1.4’s use of “associated data centers”. Are these the “computer rooms” that service a Control Center? Request clarification on the Standard Drafting Team (SDT) expectations on Medium Impact 2.1. Does the SDT expect that the “aggregate highest rate net Real Power capability of the preceding 12 months” will not flip flop on this threshold? In other words, does the SDT expect these asset to remain on one side or the other of this threshold? Recommend a change to R1’s VSLs since Lower and Severe use 100 or more High and Medium BES Cyber Systems while moderate and High uses BES Cyber Assets. Request clarification and consistency. Recommend BES Cyber Assets so that ISOs can easily hit their thresholds. Requirement 1.2 of CIP-002-5 should be revised to use the same language as Attachment 1. The wording presently reads: “Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; “ Suggested rewording: Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used BY AND LOCATED AT the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; Requirement 1.3 of CIP-002-5 should be revised to use the same language as Attachment 1. The wording presently reads: “Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;” Suggested rewording: Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) ASSOCIATED WITH the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;
Yes
Yes
Yes
Yes
No

No
Recommend changing M5 from “signed” to “approved” since some companies use other approval processes. Also these Measures criteria need to be aligned with the Requirements. Measure M5 includes “to approve or authorize specifically identified items” while R5 states “and approved by the CIP Senior Manager”. Request a re-written M6 since it appears to add a new Requirement--“that within 30 days of discharging the delegated authority”. Recommend updating CIP-003 R2’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures show R2 as “low”.
Group
SMUD & BANC
Joe Tarantino
No
No
ISSUE: The summation of actual peak-load seasonal MVA ratings for each circuit should be the measure to determine Medium Impact Rating (M) for Transmission facilities where three or more connections to other Transmission stations or substations. Assessment utilizing the MVA threshold better aligns with other NERC Reliability Standards’ criteria for system impact and is a better measure to determine Medium Impact Rating of Transmission facilities. The reason for including peak load season is so that entities are not required by an auditor to use the higher winter continuous ratings for a system that is summer peaking . We offer the following language for consideration. SUGGESTION: The summation of actual MVA peak-load seasonal ratings for each circuit should be the measure to determine Medium Impact Rating (M) for Transmission facilities at a single station or substation that are operating between 200 kV and 499 kV, are connected to three or more other Transmission stations or substations, and which exceeding 3,000 MVA. The MVA for a Transmission Facility is determined by summing the peak load season continuous ratings in MVA for each incoming or outgoing BES Transmission Line that is connected to another Transmission station or substation.
Individual
Scott Harris
Kansas City Power & Light
Yes
No
The “Low” category in Attachment 1 includes all BES Facilities not included in the High and Medium categories. Many BES Facilities serve customer load that have no impact on the operating reliability of the bulk electric system. Low designations should focus on those facilities that have an impact on the reliability of the bulk electric system not included in the High and Medium category. Recommend modifying the “Low” category to the following: Each BES Cyber System associated with: 3.1. BES Facilities not categorized in Section 1 as having a High Impact Rating (H) or Section 2 as having a Medium Impact Rating (M) and having an direct impact on supporting the reliability of the BES. 3.2. Blackstart Resources. 3.3. Elements in the Cranking Path and initial switching requirements.
No
No
No
No
Yes
No
R1 & R2: Recommend striking “and evidence of processes, procedures, or plans that demonstrate the implementation of required topics” from the Measure. Requiring the additional evidence beyond the policy expands the scope of the requirement that is unattainable because Entities won’t know what is sufficient to prove compliance. R3: Recommended wording addition: “Senior Manager by name or Title.” R6: Recommend striking this requirement and moving the change to Senior Manager to R3 and the change to delegates to R5.
Individual

Nick Lauriat
Network & Security Technologies, Inc.
No
Yes
N&ST has observed that with each revision more and more assets are the in the “Low Impact” category, and that owners of “Low Impact” BES Cyber Systems are basically obligated to do nothing. Increasing the size of the low impact category decreases the cyber security of the Bulk Electric System. N&ST strongly cautions against increasing the size of the low impact category (especially for generation assets), and urges the drafting team to attempt to make “medium impact” the default category, rather than “low impact.” N&ST is especially troubled that with the removal of black start, it is basically safe to assume that by the time these standards go in to effect that almost no generation assets in North America will meet the “medium impact” designation. Like others, N&ST expects that this set of cyber security standards should be built to stand the test of time. It's difficult to imagine a different, later drafting team doing a better job creating reliability standards for cyber security. As such, the drafting team should carefully consider whether these standards are challenging enough, or allow entities to (permanently) place assets in the "Low Impact" category simply by making a few network changes.
Yes
No
No
Yes
Yes
Yes
In CIP-003 Requirement R2, N&ST observed that one of the specific requirements is that “For BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies (for)...Incident response to a BES Cyber Security Incident.” Despite this, CIP-008-5 does not apply to low impact BES Cyber Systems. N&ST believes that CIP-008-5 should be very “achievable” even for an entity with only low impact BES Cyber Systems. Why not make CIP-008-5 the yardstick that entities with only low impact BES Cyber Systems are measured against? N&ST also observed the same problem regarding CIP-003-5 and CIP-004 “awareness.” If entities are really, truly free to define their own programs for low impact BES Cyber Systems outside of any standards / requirements, perhaps the drafting team should specifically state that? In CIP-003 Requirement R3, N&ST believes the text stating the CIP Senior Manager must have “the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards” should be in the R3 requirement statement, not just the accompanying “Rationale” statement.
Group
Progress Energy
Jim Eckelkamp
No
No
:Progress Energy agrees with EEI and additionally Progress Energy recommends that if any further changes are made to Attachment 1, they be based on alignment with the other Reliability Standards, e.g., TPL, EOP, etc. Progress Energy supports the Standards Drafting Team’s efforts to seek the input of the Operations Committee with regards to the Blackstart issue.
No
No
No
No
No
No
Progress Energy agrees with EEI comments with the modified and additional comments below R1= Original: Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall

implement one or more documented cyber security policies that address the following topics. Proposed: Each Responsible Entity for its BES Cyber Systems used in high impact and medium impact facilities shall implement one or more documented security policies that address the following topics. Rationale: references to Low/Medium/High Impact should be applied to facilities and not BES Cyber Systems. R2= Original: For BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics: Proposed: For Facilities identified as not having high impact or medium impact BES Cyber Systems, each Responsible Entity shall document security policies and implement an awareness program that addresses the following topics: 2.1 Cyber security awareness; 2.2 Physical access control; 2.3 Electronic access control; and 2.4 Incident response to a BES Cyber Security Incident. An inventory, list, or discrete identification of BES Cyber Systems is not required. Measure: Evidence must include one or more documented cyber security policies and evidence of processes or procedures. Rationale: If concern from the industry regarding CIP-003-5 R2 is focused on 1) wanting to keep low impact at the site level verses the asset level, and 2) concern around using the word "implementation" (both of which bring into question what evidence would be needed to prove compliance), we feel the following language will meet the intent and address the concerns: R3= Comment: The R6 content applicable to R3, requiring the documenting of changes to the Senior Manager within 30 days, should be included within R3. This will eliminate 'double jeopardy' concerns where failure to adequately document changes will now result in the violation of a single requirement. R4= VSL's: a. Propose framing review violations as lower/medium VSLs as follows: i. Lower – Policies have not been reviewed within 30 days of annual review time periods ii. Medium – Policies have not been reviewed within 60 days of annual review time periods b. For Policy approval: i. High – Policy has not been approved within 30 days of annual approval timelines ii. Severe – Policy has not been approved within 60 days of annual approval timelines Rationale – There is a difference between approved policy and review of policies. The current approach repeats the violation in which 'not all policies have been approved within the required time period,' which creates confusion. By recognizing the difference in importance (approve vs. review) and framing review violations as less severe, this provides a more relevant scale. R5= Comment: The R6 content applicable to R3, requiring the documenting of changes to the Senior Manager within 30 days, should be included within R3. This will eliminate 'double jeopardy' concerns where failure to adequately document changes will now result in the violation of a single requirement. R6= Should be removed and content included in R3 Additional Comments below a. Comments: The current wording reflects an attempt by the CIP SDT to provide 'protection' from discrete identification of low impact BES cyber systems, yet the requirements are (still) framed in a way that would require discrete identification to adequately demonstrate compliance. This provides conflicting messages that would impede approval of protection controls for BES Cyber Systems used within High and Medium Impact facilities. b. Remove "egress" from Guidelines 1.4

Individual

John Allen

City Utilities of Springfield, MO

No

Yes

City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. But, we do not agree with the current draft of CIP-002-5 that forces all small Control Centers into the Medium Impact classification, subjecting them to the onerous compliance obligations of CIP-003 through CIP-011. Today there are many small entities with Control Centers that are not identified as Critical Assets, because studies show that the loss or compromise of their whole system would not cause a significant impact to the BES. However, it is our understanding that the impact of these small systems to the BES is not the purpose for this classification. Instead the reason for identifying all Control Centers is to address FERC's concern regarding "connectivity" to High Impact Control Centers. We believe that this concern is valid and can be addressed without the enormous compliance burden placed on small entities and the ERO by the proposed draft of CIP-002-5. It is timely that NERC is actively looking for ways to reduce the compliance monitoring burden on the Regional Entities. Significant work is being performed by the BES Definition SDT to properly identify Facilities that are important to the BES. There is also NERC's Risk Based Compliance initiative that is working to develop metrics that will classify an entity based on its risk to the BES. The goal is to reduce the amount of ERO resources needed to monitor the low

risk entities. However, it appears that CIP-002-5 is not consistent with these efforts. Therefore, NERC and the SDT should consider the huge impact of the proposed criteria in CIP-002-5 on compliance monitoring resources that are already overloaded. NERC and the drafting team should also consider the unintended consequence of diverting large amounts of industry resources to address requirements that could (emphasis added) impact the reliable operation of the BES, when at the same time NERC and the industry is diligently working to focus resources on the ones we know (emphasis added) impact reliability. It is important to note that with the recent approval of Version 4 “bright-line criteria”, the “High Impact” Control Centers will be secured, not only from vulnerabilities to outside attacks, but also from “connectivity” to other Control Centers. Each entity must be responsible for securing its own electronic security perimeter(s) and there is no possible way to remove all vulnerabilities and secure all of the “weakest links” that CIP-002-5 is attempting to address. Besides, how do you plan to secure all of the other networks that are "connected" to the High Impact Control Centers that are outside of FERC/NERC jurisdiction? However, we believe it is reasonable to support a set of standards that apply programmatic requirements to small Control Centers for such things as: 1. Control and monitoring of electronic access 2. Control and monitoring of physical access 3. Personnel risk assessments 4. Training 5. Incident response 6. Recovery plans Therefore, we propose the following options for the SDT to consider: 1. Create a size limit for “Medium Impact” Control Centers. For example, raise the threshold for “High Impact” Control Centers to 3000 MW and move the 1500 MW threshold to “Medium Impact”. Then classify all other Control Centers as “Low Impact” and add programmatic requirements to CIP-002 through CIP-009. 2. Remove the proposed requirements in CIP-003 through CIP-009 for “Medium Impact” Control Centers and replace with programmatic requirements. 3. Move criteria 2.11 into the “Low Impact” category and add programmatic requirements to CIP-002 through CIP-009. If there is concern that an entity with a “Low Impact” Control Center would not have enough incentive for security, then you could add a requirement that would change the compliance obligations based on a security incident due to negligence. For example, the entity could do an analysis to determine if the event was related to an issue of non-compliance with one of its programs. If so, then the Regional Entity could increase compliance monitoring of the entity’s programs for a period of time until the entity demonstrates that it has things under control. The changes we propose would decrease the financial impact on small entities by reducing the amount of compliance documentation required, while still ensuring a base-line of protection for those cyber systems that are connected to “High Impact” Control Centers via ICCP or other applications. It would also bring the CIP Standards into line with the Risk-Based Compliance initiative at NERC by matching an entity’s compliance obligations according to its risk to the BES. This would ensure that the ERO has adequate resources in the future to monitor the cyber systems that are critical to the reliable operation of the BES.
Yes
Yes
Yes
Yes
Yes
Yes
City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. We support the comments submitted by SPP and APPA.
Group
NCEMC
Scott Brame
No
Yes
(1) 4.2.1 and 4.2.2, and Attachment 1, 2.10 – The threshold for 300 MW of UFLS or UVLS load shedding is clear, but saying “that are part of a Load shedding program” implies that an entity could have only 50 MW of load that will be shed as part of a larger 300 MW “program” and be drawn into the applicability and required to comply with the Medium Impact facility requirements. Another scenario is where a DP with a 250 MW load shedding program not associated with any other group would not come into applicability at all. NCEMC recommends that the SDT provide guidance with very

clear examples of scenarios that would include or exclude DP or LSE entities from required compliance with CIP Version 5 standards. (2) Under the inclusion threshold for DP, 4.2.2, third bullet, states: “A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard.” NCEMC recommends that the following language be added to the end of that bullet; “, and where the Protection System is connected to a supervisory control system providing remote operation capability.” This language will help to further appropriately clarify the scope of applicable Protection Systems in the CIP standards. (3) Attachment 1 2.11 – The 300 MW value should be revised to 1500 MW to properly align it with 2.1 in the Medium Category. The 300 MW value has not been adequately technically justified and the resulting potential compliance obligation actions and costs that could be required will likely far outweigh the reliability benefit of keeping the 300 MW value in this section. If the change to 1500 MW is made, then all other Control Centers, and associated data centers, not included in the High or Medium Category will be included in the Low Category. This is a major issue for NCEMC. It will be difficult to support CIP-002-5 without this revision. (4) We disagree with including LSE as an applicable entity. Per the NERC function model, LSE’s do not own or operate UFLS or UVLS relays. Page 26 of the Reliability Functional Model Technical Document makes this clear with the statement, “Unlike the Distribution Provider, the Load-Serving Entity does not have Bulk Electric System assets (“wires”) but does take title to energy.” The only role that is given to the LSE in the Reliability Functional Model is to “participate in under-frequency load shedding systems and under-voltage load shedding systems through identification of critical customer loads that are to be excluded from load shedding systems”. They are given no role to own, install or maintain UFLS or UVLS. They simply assist in the identification of critical loads to help ensure they are not inadvertently included in the UFLS or UVLS program. Because the standard only envisions inclusion of LSES due to UVLS and UFLS, their complete removal from the standard is warranted. (5) Use of Systems is not consistent with the NERC Glossary definition throughout many sections of the standard and application guidelines. The NERC Glossary defines System as: “A combination of generation, transmission, and distribution components.” In section 4.2.2, how can a Distribution Provider have a System when two (generation and transmission) of three required elements to meet the definition are not included? Use of “System” in the first bullet under section 4.2.2 clearly does not intend the NERC Glossary definition but rather a computer or control system. It appears that a wholesale find and replace was performed on “system” between versions which may have contributed to this problem. There are many other instances in the Application Guidelines requiring the use of System that is questionable as well. (6) It is not clear why “Bulk Power” is capitalized in the second paragraph of the Rationale box for R1. (7) We recommend that Measurement M1 be clarified that the “list of changes to the BES” per Part 1.4 may be an acknowledgement that there were no changes. (8) What is the justification for the values used for the VSLs in Requirement R1? For example, how were 40 Facilities and 100 Cyber Systems arrived at for the Lower VSL? A justification needs to be provided? Why not use 80 Facilities and 200 Cyber Systems? (9) Criterion 2.3 focuses on the long-term planning horizon which is contrary to the standard. The standard focuses on reliability impacts caused on the BES in a 15 minute timeframe from the misuse, degradation or unavailability of the BES Cyber Asset or BES Cyber System. It does not make sense to subject BES Cyber Assets and/or BES Cyber Systems within a generator plant or GOP control center to these standards if a generator is identified as needed for reliability four years out but is not identified from year 0-3. This needs to be further clarified. (10) It would be helpful if the application guidelines clarify how the Reliability Coordinator, Transmission Planner or Planning Coordinator will notify the Generator Owner, Generator Operator, Transmission Owner and Transmission Operator that their equipment meets criteria 2.3 and 2.6. (11) Criterion 2.8 needs supporting explanation in the Application Guidelines explaining how the Transmission Owner will determine that a generator it is does not own or operate meets the criteria in Part 2.3. Otherwise, it is not clear how the Transmission Owner will know that its interconnection equipment to the generator should be included in this Medium Impact Rating. (12) There is a statement in the first paragraph of the “Applicability to Distribution Providers and Load Serving Entities” section of the Application Guidelines that states the qualifications for inclusion of the Distribution Provider are based on requirements applicable to Distribution Providers in EOP-005 and registration. This statement could actually be contradictory to Applicability section 4.2.2 which includes more applicability than just restoration per EOP-005. The statement should either be deleted or further explained. (13) The Application Guidelines on page 30 state the highest MW rating for the preceding 12 months will be used for Attachment 1 criterion 2.10 regarding load shedding systems. Rating is not the right word. Rather, the highest hourly integrated load is more correct. Instantaneous load should not be

considered.
No
No
Yes
Yes
Yes
Yes
(1) Regarding Section 4.2.4 Exemptions: This section was changed from the last posting to indicate the exemptions are for CIP-002-5. CIP-002-5 already has the same exact exemption language. Either this reference should be changed back to CIP-003-5 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (2) Regarding Question 4 (CIP-003-5 R1): Part 1.4 needs to be clarified that the NERC Glossary definition of System does not apply. (3) Regarding Question 4 (CIP-003-5 R1): The application guidelines for interactive remote access regarding inclusion of language in contracts with vendors, consultants and contractors should be modified. The guidelines state that the language should require them to adhere to the responsible entity's Interactive Remote Access controls. While we agree, in general, that contracts should reflect this language, the guidelines should be clear that this only applies to contracts executed after the enforcement date of this standard. Applying this standard to existing contracts could compel the responsible entity to renegotiate all contracts which puts the responsible entity at a significant disadvantage particularly with some contracts such those with EMS vendors. (4) Regarding Question 5 (CIP-003-5 R2): NCEMC is concerned that even though it is stated that a list of Low Category assets is not required for compliance, we do not see how compliance could be proven/demonstrated without such a list. Given that the requirements for Low Category assets are intended to be programmatic in nature, and not asset specific, NCEMC requests that the SDT make changes necessary to not in effect require a list of Low Category assets to demonstrate compliance. (5) Regarding Question 5 (CIP-003-5 R2): Requirement R2 should also be modified to make it clear that an entity may write exceptions into their cyber security policies. FERC made it clear in Order 672 that only the requirements in a standard are enforceable and part of the standard. Thus, while the application guidelines make it clear the responsible entity can write in exceptions to its cyber security policy, the application guidelines are not enforceable and there is no way of ensuring that auditors follow them. (6) Regarding Question 9 (CIP-003-5 R6): Four VSLs could and should be written based on the number of days late that the change to CIP Senior Manager or delegates was documented. (7) Regarding the Application Guidelines: The paragraph under Requirement R3 should apply to what is now Requirement R4 as a result of re-ordering the requirements from the previous draft. In the previous draft R3 requires the review and approval of the cyber security policies by the CIP Senior Manager at least once each calendar year, not to exceed 15 calendar months… This is now Requirement R4.
Individual
Scott Miller
MEAG Power
Yes
Yes
The summation of actual MVA ratings for each circuit should be the measure to determine Medium Impact Rating (M) for Transmission facilities where three or more connections to other Transmission stations or substations. Assessment utilizing the MVA threshold better aligns with other NERC Reliability Standards. In Attachment 1, please clarify 'Functional Obligations' (1.3) and 'Data Center' (1.4) CIP-002-5, 2.11 as it is dictates that all registered Balancing Authorities and Transmission Operators are automatically assigned a Medium Impact Rating (M). There are many very small Balancing Authorities and Transmission Operators that have little to no reliability impact to neighboring systems and should not be included as a medium impact rating. In addition the assigned registration as a TOP is extremely subjective. The NERC Statement of Compliance Registry Criteria ("SCRC"), section III (d), address the Transmission Owner ("TO")/Transmission Operator ("TOP") uses the same criteria to define both TO and TOPs. However, the application of what entities registers or is required to register as a Transmission Owner and not as a TOP is not defined and is not consistent though regions or North America. Section 2.11 should be removed because there is no "reliability based" justification that registration as TOP justifies a Medium Impact Rating. If the

registration thresholds were removed from section 2.11 we would likely change its vote to affirmative.
Yes
No
Yes
Yes
Yes
Yes
CIP 003-5 R2 states that the Responsible Entity for BES Cyber Systems not identified as High Impact or Medium Impact (i.e., Interpreted as “Low Impact” BES Cyber Systems) “shall implement one of more documented cyber security policies that address the following topics: 2.1 Cyber security awareness; 2.2 Physically access control; 2.3 Electronic access control; and 3) Incident response to a BES Cyber Security Incident”. This proposed language in CIP 003-5 R2 is “loose” and allows for potential future interpretation – via new NERC CAN’s, new NERC RSAW’s, NERC Regional Entity interpretations during Functional Entity audits, etc. - Which industry may (or may not) agree with in the future. Recommendation: 1) Eliminate ALL CIP 003-5 R2 requirements associated with BES Cyber Systems that are not High or Medium Impact – as Low Impact systems are Non Impact systems that should not impact BES system operating conditions – such as BES instability, separation, or cascading OR 2) Have the CIP drafting team address specific “prescriptive” Low Impact BES Cyber System requirements within CIP 003-5 through CIP 011-5 (for cyber security awareness/training, physical access control, electronic access control, incident response, etc.) – similar to the way the prescriptive requirements have been written for Medium and High Impact BES Cyber Systems.
Individual
Nathan Mitchell
American Public Power Association
No
Yes
APPA agrees in part with the changes the SDT made to the applicability section for DPs and LSEs. The SDT has made it clear that not all DPs and LSEs need to comply with these standards, only those who own and operate specific BES Facilities are required to comply. This will help eliminate the exercise of proving that some small entities do not own cyber assets that impact the BES, therefore CIP Reliability Standards do not apply to them. However, there are still some questions on the criteria the SDT used as a threshold in the Applicability section 4.2 Facilities. Point 1: The threshold for 300 MW of UFLS or UVLS load shedding is clear, but saying “that are part of a Load shedding program” implies that an entity could have only 50 MW of load that will be shed as part of a larger 300 MW “program” and will be drawn into the applicability and required to comply with the Medium Impact facility requirements. Another scenario where a DP with a 250 MW load shedding program not associated with any other group would not come into applicability at all. APPA recommends that the SDT provide guidance with very clear examples of scenarios that would include or exclude DP or LSE entities from required compliance with CIP Version 5 standards. There must be a clear designation of the applicability of this standard so small entity impact can be minimized. Point 2: The SDT should strike the wording in the Special Protection System bullet of 4.2.2: “is required by a NERC or Regional Reliability Standard” and replace that with a threshold such as “where the Special Protection System or Remedial Action Scheme controls xxxxMW or more of peak resources.” Or designate the BA or another entity to determine the critical SPS and RAS by adding; “where the SPS and RAS is designated by the BA as critical.” A clear threshold will prevent future non-CIP standards from dictating applicability with the current CIP standard without due process through standards development. There must be a clear designation of the applicability of this standard so small entity impact can be minimized. Point 3: Under the inclusion threshold for DP the SDT states: “A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard.” APPA recommends that the SDT remove the “Protection System” bullet since it causes way too much confusion and will allow future non-CIP standards to dictate applicability with the current CIP standard without due process. At a minimum the SDT needs to clarify which “Protection Systems” they are referring to in this bullet. If the SDT did not intend on bringing in all other UFLS and UVLS relays not designated in the first bullet, there must be a clarifying exclusions such as: “Protection Systems (excluding UFLS and UVLS relays not covered above)…” If these

suggestions are not accepted by the SDT, there must at least be clear guidance on what specific Protection Systems are referred to in this bullet. APPA would even suggest that current standards that apply to this bullet be listed in the guidance. There must be a clear designation of the applicability of this standard so small entity impact can be minimized. Point 4: APPA agrees with the changes the SDT made to Attachment 1. We would like to commend the SDT for their insight in changing the designation of Blackstart Resources and Cranking Paths from Medium to Low Impact. This change will help avoid the reliability impact to the BES of Blackstart Resources being removed from the Transmission Operators Restoration Plan if those units become uneconomic due to compliance costs. This truly prioritizes reliability of the BES and mitigates the negative impacts of a compliance requirement. The following are further changes needed in Attachment 1: As stated in comments on the Definition of Control Center: APPA Recommendation: Clarify in guidance what “control” within the Control Center definition means. If the SDT uses the CIP Version 1 FAQ response as the guidance: “monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction” APPA recommends that control centers which use only manual or voice instruction as the control be designated as Low Impact facilities in CIP-002-5 Attachment 1. This designation will help reduce the burden of compliance for small entities that chose to use this cyber risk mitigation method. Criteria 2.10 in Attachment 1 is still unclear and should be changed. Similar to APPA’s statement in Point 1 above, 2.10 “Each System or group of Elements that performs automatic Load shedding…” implies that an entity could have only 50 MW of load that will be shed as part of a System or group of Elements in a larger 300 MW “program” and be required to identify their UFLS system as a Medium Impact facility and comply with all CIP requirements. Another scenario where a DP with a 250 MW load shedding program not associated with any other group would not come into CIP applicability at all. APPA recommends that entities with UFLS and UVLS systems below 300 MW be classified as Low Impact facilities. APPA believes that Criteria 2.11 in Attachment 1 should at a minimum designate all control centers with control of less than 300 MW of resources as Low Impact. This will clearly define a lower threshold as requested for in 2.10 above and reduce the burden of compliance for small entities.
Yes
Yes
No
No
No
No
APPA agrees with the STD proposal to include all of the programmatic requirements for BES Cyber Systems not identified as High Impact or Medium Impact in one requirement. This will help the industry focus their compliance efforts on documenting the development and implementation of policies for the four sub requirements. However, APPA is concerned about the audit process that is implied in the Measures section. M2 states: “evidence of processes, procedures, or plans that demonstrate the implementation of the required topics.” It has been stated at various STD meetings that auditors will need to measure “implementation” by sampling physical or electronic access controls at specific facilities or equipment. In order for sampling to be random and in accordance with auditing practice, there needs to be a data set to sample. This is contrary to the note in Requirement R2 that states: “An inventory, list, or discrete identification of BES Cyber Systems is not required.” APPA recommends that the SDT work with NERC enforcement staff in crafting an RSAW that will include evaluation of the documented processes, procedures and/or plans as the auditor’s first measure of implementation. APPA recommends removal of CIP-003-5 R3, and R5 since CIP-002-5 Requirement R2 implies that all of the documentation is done to designate the CIP Senior Manager and requiring further documentation does not improve BES reliability. The review process of CIP-003-5 Requirement R3 should be included in R1 and R2. This will eliminate unnecessary documentation requirements from the standards and may help reduce the paperwork burden of the small responsible entities.
Group
SPP and specific Member companies
Lesley Bingham
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
1. In CIP-003-5 Measure 4, the measure says “Evidence may include but is not limited to” and then lists two numbered items connected by the word “and”. If evidence “may include”, then the items below are suggestions, not requirements. As they read now, they are both required and not strictly examples of appropriate evidence. These should be bulleted (i.e. example items which are not the only methods for compliance) and either one, if presented, should be appropriate evidence. Specifically, if a document management system captures and tracks approvals, that should be sufficient evidence for this requirements. A hard copy with a wet ink signature should not also be required for compliance. 2. CIP-003-5 R5 states that the CIP Senior Manager may delegate authority “where allowed by the CIP Standards”. It would be helpful to have the standards where it is not allowed listed in this requirement. While the goal of having clear standards that do not point to other standards is laudable, citing the specific items that cannot be delegated would provide much-appreciated clarity. 3. CIP-003-5 R6 needs additional clarification. Certainly, changes to the CIP Senior Manager should be reflected in timely updates to the authorization document. A new delegation should also be similarly captured. However, what is not clear is what smaller changes should be reflected. Specifically, the sentence “Delegation changes do not need to be reinstated with a change to the delegator” is confusing. Does this mean that if the CIP Senior Manager changes, the downstream delegations do not change and only the documentation pertaining to the CIP Senior Manager needs to be approved by the “high level official” who designates the CIP Senior Manager? Or does this indicate that if delegations are specified by title and the person carrying the title changes, no update of documentation is needed as long as the new title holder can also carry the delegated approval (i.e. Director of Physical Security approves—by delegation—physical access requests, specific person leaves, replacement Director retains approval rights)? It would be more clear to state “Each Responsible Entity shall document any changes to the CIP Senior Manager or any delegated authority, whether by name or by title, within thirty calendar days of the change.”
Individual
Jennifer White
Alliant Energy
No
Yes
[1] The proposed methodology prescribed by Requirement 1 is in direct conflict with the structure of the definition for BES Cyber Asset and BES Cyber System. The impact rating should align with the facility (BES Site) instead of the cyber asset. [R1 Proposed Flow] 1.1-Based on the definition for a BES Site, each entity should create a list of BES Sites. This step will determine for the entity, which sites have zero BES impact vs.which sites have an impact and will be later divided into high, medium, and low. This also creates positive definition or threshold for Low Sites. These Low sites, based on the criteria, will have some impact and require, at a minimum, programmatic protection at the Site level. There will be no need to identify the cyber assets associated with sites that have zero impact or those that remain in the Low category. All Low, Medium, and High Sites will have the protections afforded the Low sites, but for those meeting the Medium and High criteria, additional protections are required, as well as the enumeration and classification of the cyber assets critical to providing the BES functionality of the location. After identifying the Low BES Sites, the Medium and High criteria must be considered for each Site. The following is a proposed flow for which the order can be modified while maintaining efficacy. Also, the proposed flow may require an adjustment of the criteria, if any of the High criteria are dependent on Medium criteria output. The order should, when applied, be progressive in nature and not require jumping from one criteria list to another. 1.2 – Based on the sites that remain on the candidate list, determine the medium sites based on the criteria in the attachment. A candidate list for cyber assets required in order for the BES Site to perform its reliability function(s) will be created for the Medium Sites. The cyber assets that are critical to the

performance of the reliability function will then be divided into those with (F) or without (G)External Routable Connectivity, those cyber assets used for Electronic (H) or Physical Access (I) Control or Monitoring, and those cyber assets connected within the same ESP (J) as the cyber assets necessary for the performance of the reliability function. 1.3- Based on the candidate list for sites with BES impact created from the execution of the first step and second step, identify the High impact sites using the criteria in the attachment. A candidate list for cyber assets required in order for the BES Site to perform its reliability function(s) will be created for the High Sites. The cyber assets that are critical to the performance of the reliability function will then be divided into those with (A) or without (B)External Routable Connectivity, those cyber assets used for Electronic (C) or Physical Access (D) Control or Monitoring, and those cyber assets connected within the same ESP (E) as the cyber assets necessary for the performance of the reliability function. Note: There are 10 types of cyber assets positively identified through this process, each with varying levels of risk to the BES if compromised or rendered unavailable. This, potentially, creates more than 10 levels of protection to be enumerated throughout the rest of CIP-003 through CIP-011. For administrative ease, Alliant Energy recommends grouping these types of cyber assets based on their actual level of risk in each scenario involving a potential incident that is either cyber or physical in nature and based on the External Routable Connectivity. The rest of the Standards should be written to address each type or grouping of asset. Silence on any one type or grouping will lead to confusion regarding the necessary protective measures and commensurate improvement to security posture. 1.4 – Everything that made the initial candidate list requires protection of some sort, so if it didn't get picked for High or Medium, it gets assessed at Low, because it met the threshold criteria in the BES Site definition. Verbiage in the definitions and the requirements should support this process flow, which will allow the enumeration of High Sites, Medium Sites, and Lows Sites (since we all know a list is required to demonstrate even programmatic elements of CIP compliance). The lists of Cyber Assets will only be required at Medium and High Sites. If possible and feasible, the criteria for dividing the sites into those categories should be progressive in nature, allowing clear demarcation and rationale for the criteria chosen. Additionally, the rest of the Standards should address the requirements progressively for the asset types based on risk. The shift from the current draft to one with obvious progression throughout the CIP-002 methodology and again throughout the rest of the Standards will allow for ease of application at each entity. The current draft does not provide the entities with clear understanding of the order and rationale for identifying the scope of applicability for the CIP Standards, and the MRO NSRF feels that the entities can't be successful with the current format. [2] Change the CIP-002 VSLS to reflect "BES Sites" instead of "Facilities" as those would be the enumerated list. In its current state, it conflicts with the statement that low and zero impact sites do not require enumeration. [3] All VSLs should change the impact designation from cyber asset based to site-based. "High," "Medium," or "Low" designations should precede the word "Site" not "BES Cyber Asset" or "BES Cyber System." [Proposed Draft CIP-002-5] This is one of several proposed drafts for CIP-002-5. Others are being offered through independent contacts with the SDT. Recommend considering the following, in whole or in part, as an alternative to the currently drafted CIP-002-5. Requirements R1. BES Site Identification – Each Responsible Entity shall identify BES Sites as determined through an annual application of the criteria contained in CIP-002-5 Attachment 1 – Impact Rating Criteria Parts 3.1 – 3.5. The Responsible Entity shall use this candidate list to further identify the BES Sites as Low, Medium, or High Impact BES Sites using the following applications: [Violation Risk Factor: High] R1.1. Using the list of BES Sites identified in R1, identify Medium Impact BES Sites as determined through an annual application of the criteria contained in CIP-002-5 Attachment 1 – Impact Rating Criteria Parts 2.1 – 2.11. R1.2 Using the list of BES Sites identified in R1 and R1.1, identify High Impact BES Sites as determined through an annual application of the criteria contained in CIP-002-5 Attachment 1 – Impact Rating Criteria Parts 1.1 – 1.4. R1.3 BES Sites failing to be identified in R1.1 and R2.2 while meeting the minimum criteria for CIP-002-5 Attachment 1 – Impact Rating Criteria Parts 3.1 – 3.5 shall be identified as Low Impact BES Sites. Low Impact BES Sites are not subject to CIP-002-5 R2. R1.4 Review (and update as needed) the identification in Requirement R1, Parts 1.1, 1.2, and 1.3 within 60 calendar days of when a change to a BES Site is placed into operation, which is planned to be in service for more than six calendar months and causes a change in the identification or categorization of the BES Site from a lower to a higher impact category. M1. Acceptable evidence may include, but is not limited to, dated electronic or physical lists required by Requirement R1, Parts 1.1, 1.2 and 1.3, and a list of changes to the BES (with a date for each change) that cause a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. R2. BES Cyber System Identification – Using the lists of High and Medium

Impact BES Sites pursuant to Requirement R1.1 and R1.2, the Responsible Entity shall develop risk category lists of BES Cyber Systems essential to the performance of reliability functions at each BES Site. In order to apply protective measures based on security and BES functionality risk, the Responsible Entity shall identify: [Violation Risk Factor: High] R2.1.BES Cyber Systems with External Routable Connectivity R2.2 BES Cyber Systems without External Routable Connectivity R2.3 Physical Access Control and Monitoring Systems R2.4 Electronic Access Control and Monitoring Systems R2.5 Associated Protected Cyber Assets within the ESP of a BES Cyber System with External Routable Connectivity R2.6 Review (and update as needed) the lists identified in Requirements R2.1 – R2.5, Parts 1.1, 1.2, and 1.3 within 30 calendar days of when a change to a BES Cyber System is placed into operation, which is planned to be in service for more than six calendar months and causes a change in the categorization of the BES Cyber System or BES Cyber Asset(s). M2. Acceptable evidence may include, but is not limited to, dated electronic or physical lists required by Requirement R2, Parts 2.1- 2.5, and a list of changes to the BES Cyber System (with a date for each change) that cause a change in the categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher risk category. R3. Annual Approval – The Responsible Entity shall have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 and R2 at least once each calendar year, not to exceed 15 calendar months between approvals, even if it has no identified items in Requirement R1, Parts 1.1, 1.2, or 1.3. [Violation Risk Factor: Lower] M2. Acceptable evidence may include, but is not limited to, electronic or physical dated and signed records, even if the lists are null, to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate review and update, where applicable, the identification and categorization of BES Sites, BES Cyber Systems, and their associated risk categorizations for any associated cyber assets, at least once each calendar year, not to exceed 15 calendar months between occurrences. Alliant Energy agrees with the MRO NSRF comments related to the criteria in attachment 1.
Yes
No
Yes
Yes
Yes
Yes
(1) [Proposed Verbiage] CIP-003 R1 Each Responsible Entity for the identified BES Cyber Systems critical to the operation of high impact and medium impact BES Sites shall implement one or more documented cyber security policies that address the following topics: Keep 1.1 – 1.10 as is. (2) [Proposed Verbiage] CIP-003 R2. For BES Sites identified as low impact, each Responsible Entity shall provide guidance with one or more documented cyber security policies that address the following topics: [Violation Risk Factor: Low] [Time Horizon: Operations Planning] The programmatic elements identified in the sub-requirements may remain, as is. (3) VSLs should reflect the actual risk to the BES when one or more elements are missing. The absence of a program should be high or severe, but the lack of discrete components should start at Low. Please note that the above changes apply to structure and not content of what the SDT is intending to accomplish.
Group
Dairyland Power Cooperative
Tommy Drea
No
Yes
Please see MRO NSRF comments.
Yes
No
Yes
Yes
Yes
Yes
Please see MRO NSRF comments.
Individual

Tracy Richardson
Springfield Utility Board
No
Yes
CIP-002-5 Attachment 1 – Impact Categorization of BES Cyber Assets and Cyber Systems addresses Impact Categorization, but there appears to be no guidance in the actual identification of BES Cyber Assets and BES Cyber Systems. In the Background statement of each of the Version 5 CIP Standards, it is noted that, “Standard CIP-00X-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the Version 5 CIP Cyber Security Standards.” However, CIP-002-5 is titled BES Cyber Asset and BES Cyber System Categorization, with no mention of identification. Measure 1 for Requirement 1 of CIP-002-5 requires physical lists for High and Medium categorization; however there is no list requirement for Low Impact. The following Version 5 CIP (CIP-003 through CIP-011) Standard Requirements imply or assume that all Responsible Entities (regardless of impact) have created a list identifying BES Cyber Assets and BES Cyber Systems. SUB recommends either adding a Low Impact BES Cyber Assets and BES Cyber Systems list requirement, or altogether removing the Requirement for those with a Low-Impact (or no impact) categorization. SUB believes more guidance and clarity should be provided for the actual identification of BES Cyber Assets and BES Cyber Systems, and suggests general guidelines be provided on how Registered Entities would identify demarcation points where a BES Cyber Asset and/or BES Cyber System begin and end. It is also SUB’s recommendation that a bright-line criteria method for Registered Entities to demonstrate “no impact” and be given an outright exemption from Standards CIP-003-5 through CIP-011-5. SUB is concerned with the inclusion of Distribution Providers (DPs) in the Version 5 CIP Standards, as well as with the qualifiers proposed for Load-Serving Entities in the Applicability section of CIP-002-5. This inclusion will draw in small entities with no operational capabilities and cause them to go through an administrative burden of proving they either do not provide BES Reliability Operating Services or they do not have cyber assets associated with this equipment. SUB recommends that a bright line criteria method for Registered Entities to demonstrate “no impact” and be given an outright exemption from CIP-003-5 through CIP-011-5.
Yes
Yes
Yes
Yes
Yes
Yes
SUB has no additional comments since the last comment period.
Individual
Maggy Powell
Exelon Corporation and its affiliates
No
Yes
CIP-002-5, Attachment 1, 2.3 and 2.6: The language in these requirements provide for entities other than the registered entity to designate assets for treatment as Medium level assets. As written, the process is a unilateral decision when it should be a more collaborative determination process with a mutual understanding of the decision. Further, 2.6 enables RCs, PCs or TPs to identify assets for inclusion, but does not require that they inform the assets owners/operators of the identification as the language should and does in 2.3. These are serious concerns. Sections 2.3 and 2.6 should include language to challenge the inclusion of assets by other entities perhaps in conjunction with the BES exception process or an alternate mechanism to challenge. CIP-002-5, Attachment 1, 2.10: We accept the 300 MW threshold; however, the number lacks a technical justification and basis in reliability. The history of the 300 MW as a trigger for OE-417 reporting is not relevant to reliability nor is it sufficient justification for standard requirements. The language around the threshold is critical to

the threshold as to the appropriate applicability of the requirements. So while we accept the language in 2.10, the context of the threshold should remain part of the standard development record to avoid future expansion of requirements at the 300 MW threshold. CIP-002-5, Attachment 1, 2.11: Similar to 2.10, there is little basis for the 300MW threshold. We recognize that determining an appropriate, reliability-based threshold is a challenge. At least the 1500 MW threshold has a more relevant to reliability as an average of contingency reserves. CIP-002-5, Attachment 1, 3.: While we suspect that 3.2 and 3.3 are specifically identified in the attachment because they were previously identified elsewhere in the language in earlier drafts, because they are no longer listed in sections 1 or 2, they should automatically be classified as Low. It is not necessary to include 3.2 or 3.3. Consider updating the section 3 language to more simply read: 3. Low Impact Rating (L) - Each BES Cyber System associated with BES Facilities not categorized in Section 1 as having a High Impact Rating (H) or Section 2 as having a Medium Impact Rating (M). BES Cyber Systems that are not identified as high impact or medium impact shall default to the category of low impact and do not require discrete identification.
Yes
No
Yes
Yes
No
Yes
CIP-003-5, R2: In R2, the language restates that the requirement applies to BES Cyber Systems not identified as high or medium impact rather than specifically saying low. We understand that this wording is intentional to avoid suggesting that "identifying" systems as low impact requires a list to demonstrate compliance. While the language is somewhat awkward, we support this approach. Maintaining a complete list of low impact assets to demonstrate 100% compliance presents significant compliance risk, while missing the value of policies addressing the cited topics of concern. The implementation of cyber security policies and practices applicable to low impact systems is more relevant to reliability than a list identifying low impact systems. Leaving a system covered by the policies and practices off a list is irrelevant to reliability. To further clarify the R2 language, please consider adding discussion of the reasoning behind the specific language in the guideline section. CIP-003-5, R5: R5 is acceptable; however, for consistency, M5 should read like M6. Please revise the first line to read: "Evidence may include, but is not limited to, dated documentation, …"
Group
Western Electricity Coordinating Council
Steve Rueckert
No
Yes
Identification of BES Facilities, systems and elements: WECC objects to the proposed the Impact Rating Criteria (“Criteria”) changes in “Attachment 1, 1. High Impact Rating.” The proposed changes exclude a number of BA and TOP Control Centers, Backup Control Centers, and Data Centers. Further, the proposed changes are inconsistent with the mandates of FERC Order 706 . FERC does not distinguish Transmission Operator control centers as posing “less of a risk.” FERC Order 706 at 280 states that “it is difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be identified as a Critical Assets.” FERC Order 761 goes further addressing CIP Version 5 stating: we continue to expect comprehensive protection of all control centers and control systems as NERC works to comply with requirement of Order No. 706.” WECC recommends that all Control Centers, backup Control Centers, and associated data centers used to perform function obligations of the RC, BA and TOP should be categorized as “High Impact” facilities. WECC objects to the categorization of “Blackstart Resources” and “Elements in a Cranking Path and initial switch requirements” as “Low Impact.” FERC explicitly rejected the rationale underpinning this categorization. FERC Order 761 at 47 states: “We [the Commission] disagree with MISO that designating a “must run” unit as a Critical Asset may create an incentive for generator owners and generator operators to remove units from service prior to their designation as Critical Assets.” WECC Enforcement recommends that “Blackstart Resources” and “Elements in a Cranking Path and Initial Switch Requirements” be categorized as “High Impact” or, at

least as “Medium Impact.” WECC objects to proposed changes in Criteria 2.6 and Criteria 2.9, that eliminate consideration of facilities critical to derivations of SOLs and contingencies for transmission paths listed in the most current table titled “Major WECC Transfer Paths in the BES.” WECC does not rely on derivation of IROLS. Consideration of Major WECC Transfer Paths must be considered to ensure reliability in the Western Interconnection. In the event that WECC may monitor their system for IROL’s the language in the standard should stipulate “continuous IROL’s.” R1.1. WECC recommends that R1.1 use consistent terms. R1.1 requires the identification of certain facilities, and “systems,” or equipment”. The VSL for R1.1, however, only references the number of facilities and does not reference “systems” or “equipment.” The terms “systems” and “equipment” are undefined and create ambiguity. To be consistent, the VSL for R1.1 should include “systems” and “equipment” and the terms “systems” or “equipment” should either be defined or revised to “BES systems and BES equipment.” Enforcement also recommends that R1.1 explicitly require entities to “identify and list” facilities as either “high” impact facilities, or as “medium” impact facilities.” This would be consistent with R1.2 and R1.3 requires separate identification of High impact BES Cyber Systems and Medium BES Cyber Systems. R1.2 WECC recommends that R1.2 require entities to identify each High impact BES Cyber System and Cyber Assets comprising that BES Cyber System. Further, Enforcement proposes that additional clarification be provided for the term “used for.” R1.3 WECC proposes that references to “systems or equipment” be stricken or defined for reasons stated above. Enforcement recommends that R1.3 require entities to identify and document each High impact BES Cyber System and Cyber Asset comprising that BES Cyber System. Further, Enforcement proposes that additional clarification be provided for the term “used for” R1.4 WECC objects to R1.4 in its entirety. The change to any BES Element or Facility should, automatically trigger a review. Further, the addition of facilities or any BES Element should also be considered in any review under R1.4. Limiting a review to facilities “planned to be in service for more than six calendar months” is unenforceable. The term “planned” is ambiguous. What would constitute evidence of “planning?” What if the duration of the change is “planned” for 6 months, but exceeds the 6 month period. Is the change still exempt because at the time of implementation, the change was “planned” not to exceed 6 months? Further, R1.4 review is triggered only after determining there is a “change in the identification or categorization of BES Cyber Systems.” It is impossible to identify this change, however, without first conducting a review. Enforcement recommends rewriting the proposed requirement to first require a review of any change to BES facilities or systems, regardless of their duration. Secondly, based on this review, Enforcement recommends that entities then identify BES Cyber Assets or BES Cyber Systems that should be categorized from a loser to higher impact category.
Yes
Yes
Yes
Individual
Scott Berry
Indiana Municipal Power Agency
No
No
IMPA does not agree with the wording in Attachment 1, Section 2, Subsection 2.11, to be used for determining if each BES Cyber Systems associated with Control Centers and associated data centers that are not designated as having a High Impact Rating (H) should have a Medium Impact Rating. More specifically in Subsection 2.11 part (2): “control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.” This is an overly broad definition that will cause smaller Control Centers that control several smaller generation Facilities over multiple Balancing Authority Areas to have a Medium Impact Rating because the aggregate real power capability they control is equal to or exceeds 300 MW. IMPA would propose that the wording be modified to include only those Control Centers and associated data centers that control an aggregate real power capability equal to or exceeding 300 MW in a single Balancing Authority Area. GOPs already have a relationship with their respective BA(s) and this would be a natural extension of the Functional Model that is already in place. In addition, as currently written the inclusion of “Control Center” and “monitor and control” will cause non-operating entities (entities that don’t directly control generation and may only have a hand in the scheduling for startup

of the generation prior to the actual real time operation/control of the unit by operating personnel) to have a Medium Impact Rating for a Control Center that clearly should be Low Impact.
Individual
Gregory Campoli
NYISO
No
Yes
The references to NIST and Risk Methodology seem puzzling. In utilizing FISMA and as a result NIST, impact is assigned by classification of levels of confidentiality, integrity and availability of data and by using Risk Assessments to apply additional appropriate and commensurate security controls. In contrast, the application of CIP security controls have no dependency on Risk Assessment or from the impact to an organization through compromise of data confidentially and integrity. Additionally, CIP specifically uses only vulnerability assessments without regard to threats and probability calculations in the “Risk” equation. - CIP standards are applied without regard of compromise to confidentiality and integrity of data and only on merits regarding impact in support of the Bulk Electric System. In addition, FIPS 199 supports data impact assessment as a component of a cyber system(s) as well as data in other forms. One parallel exists between the two frameworks only by using availability of a BES Cyber System and therefore the availability of its data to support the BES; as cyber systems are a means of supplying data one could use the definition of BES Cyber System to mean data AND function. CIP High, Medium or Low impact level is determined as a function or mission of cyber assets in support of the BES. Other factors affect impact such as proximity to other critical cyber assets along with other supporting monitoring and authentication processes. It isn’t until CIP 011 that the standards specifically address information protection and effects of data compromise as leading to potential instability of the BES. - FISMA calls for FIPS 199 to assess impact by determining the confidentiality, integrity and availability of data either alone or part of a larger system or systems. FISMA additionally requires application of baseline security controls from NIST 800-53 commensurate to the assigned impact level. Additional security controls are implemented as a result of Risk Assessments within the cyber system lifecycle. CIP has no application of Cyber System Lifecycles within the context of ongoing evaluation security controls. - FISMA allows the application of technical, operational and managerial controls of equal proportion without an compulsory dependence on technical controls. CIP utilizes, in lieu of technical controls, Technical Feasibility Exceptions as compensating measures.
Yes
Yes
Yes
No
Yes
Yes
CIP-003 R4 M4 item 2 change the words “dated signature” to “dated approval” for better alignment with the requirement. CIP-003-5 R5 M5 change the word “signed” to “approved” for better alignment with the requirement.
Individual
Linda Jacobson-Quinn
Farmington Electric Utility System
Yes
Yes
FEUS agrees with the comments submitted by APPA. The second criteria for Attachment 1.4 – “control of one or more of the generation assets that meet criteria 2.3, 2.6 and 2.9,” should the and be an or?
Yes
Yes
Yes
Yes

Yes
Yes
FEUS agrees with the comments submitted by APPA
Individual
Scott Kinney
Avista
see comments provided by EEI
See comments provided by EEI
Group
CenterPoint Energy
John Brockhan
No
Yes
CenterPoint Energy appreciates the evident consideration of previous comments; however, the Company disagrees with the overall changes made to CIP-002-5 since the last formal comment period. Specific suggestions and/or proposals for alternative language are as follows: R1.1 – CenterPoint Energy recommends that the sentence end after “Attachment 1” as the additional description of the Impact Rating Criteria does not enhance the requirement. R1.4 – CenterPoint Energy requests examples of changes to be covered under this requirement. Attachment 1 - CenterPoint Energy proposes that the introductory paragraphs under each of the Impact Rating Criteria be deleted as it may create uncertainty in what is being identified through the application of Attachment 1 (ex. Facilities and equipment versus BES Cyber Systems). CenterPoint Energy understands that Attachment 1 is now focused on Facilities; therefore, the phrase “used by and located at” is no longer needed. CenterPoint Energy also has significant concerns with criteria 2.5. As currently defined, the values force a label of critical on non-critical Facilities as proven by intricate studies performed by transmission planning engineers. CenterPoint Energy recommends the values be revised as follows: Voltage Value of a Line 200 kV – 399 kV – Weight Value per Line - 800; Voltage Value of a line 400kV to 499 kV – Weight Value per Line – 1300. CenterPoint Energy shares the auditability and documentation concerns discussed in industry groups and committees such as Edison Electric Institute (EEI) and Texas Reliability Entity NERC Standards Review Subcommittee (NSRS) regarding the low impact criteria, “BES Cyber Systems which are not included in high impact or medium impact shall default to the category of low impact and do not require discrete identification.” Given the removal of the blanket connectivity exclusion in CIP-002, CenterPoint Energy recommends that significant consideration be given to each requirement to be applied in Medium Impact Facilities that do not have External Routable Connectivity. CenterPoint Energy supports the efforts to enhance security and minimize recently identified vulnerabilities (ex. Stuxnet). Several changes made since the last formal comment period have addressed some concerns; however, there are a few requirements for which applicability should still be addressed. CenterPoint Energy has made specific subsequent comments per Standard.
Yes
Yes
Yes
Yes
Yes
Yes
CenterPoint Energy recommends that the phrase, “in sufficient detail” be removed from the Guidelines and Technical Basis as it is subjective. CenterPoint Energy also notes that Account Management under Personnel Security appears to be out of place and recommends that the topic be moved under System Security. Under Electronic Security Perimeters, the topic, “Organization stance on use of wireless networks” is not in the Standards/Requirements. CenterPoint Energy proposes that this topic be removed to better align with the Standards/Requirements. Under Remote Access, the topic “Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating Interactive Remote Access” is also not in the Standards/ Requirements. CenterPoint Energy recommends that the topic be removed. The phrase, “For vendors, contractors, or consultants: include language in

contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls" is not in Standards/Requirements and should also be removed. Under Provisions for CIP Exceptional Circumstances, "Processes to allow for exceptions to policy that do not violate CIP requirements" is Contradictory to the CIP Exceptional Circumstance definition. CenterPoint Energy also prefers removal or an alternative to the word, "violate", be used.
Individual
James TUcker
Deseret Power
Yes
Yes
4.2.1 and 4.2.2, and Attachment 1, 2.10 – The threshold for 300 MW of UFLS or UVLS load shedding is clear, but saying "that are part of a Load shedding program" implies that an entity could have only 50 MW of load that will be shed as part of a larger 300 MW "program" and be drawn into the applicability and required to comply with the Medium Impact facility requirements. Another scenario is where a DP with a 250 MW load shedding program not associated with any other group would not come into applicability at all. DESERET POWER recommends that the SDT provide guidance with very clear examples of scenarios that would include or exclude DP or LSE entities from required compliance with CIP Version 5 standards. Under the inclusion threshold for DP, 4.2.2, third bullet, states: "A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard." DESERET POWER recommends that the following language be added to the end of that bullet; ", and where the Protection System is connected to a supervisory control system providing remote operation capability." This language will help to further appropriately clarify the scope of applicable Protection Systems in the CIP standards. Attachment 1 2.10 – see comment above 2.11 – The 300 MW value should be revised to 1500 MW to properly align it with 2.1 in the Medium Category. The 300 MW value has not been adequately technically justified and the resulting potential compliance obligation actions and costs that could be required will likely far outweigh the reliability benefit of keeping the 300 MW value in this section. If the change to 1500 MW is made, then all other Control Centers, and associated data centers, not included in the High or Medium Category will be included in the Low Category. This is a major issue for DESERET POWER. It will be difficult to support CIP-002-5 without this revision.
Yes
No
Yes
Yes
Yes
Yes
R2 – DESERET POWER is concerned that even though it is stated that a list of Low Category assets is not required for compliance, we do not see how compliance could be proven/demonstrated without such a list. Given that the requirements for Low Category assets are intended to be programmatic in nature, and not asset specific, DESERET POWER requests that the SDT make changes necessary to not in effect require a list of Low Category assets to demonstrate compliance.
Individual
Warren Rust
Colorado Springs Utilities
Yes
Yes
Colorado Springs Utilities appreciates the energy the SDT has had to expend to this point as well as this opportunity to continue to comment on this evolving draft standard. CSU is also grateful for the thoughtful comments of others and agrees with comments submitted by SMUD, AECI & SNPD regarding CIP-002-5, Appendix 1; to wit: Criterion 2.5: The summation of actual MVA ratings for each circuit should be the measure to determine Medium Impact Rating (M) for Transmission facilities where three or more connections to other Transmission stations or substations. Assessment utilizing the MVA threshold better aligns with other NERC Reliability Standards' criteria for system impact and is a better measure to determine Medium Impact Rating of Transmission facilities. [original comment

SMUD] [SNPD] disagrees with the CIP-002-5, 2.11 as it dictates that all registered Balancing Authorities and Transmission Operators are automatically assigned a Medium Impact Rating (M). There are many very small Balancing Authorities and Transmission Operators that have little to no reliability impact to neighboring systems and should not be included as a medium impact rating. In addition the assigned registration as a TOP is extremely subjective. The NERC Statement of Compliance Registry Criteria (“SCRC”), section III (d), address the Transmission Owner (“TO”)/Transmission Operator (“TOP”) uses the same criteria to define both TO and TOPs. However, the application of what entities registers or is required to register as a Transmission Owner and not as a TOP is not defined and is not consistent though regions or North America. SNPD supports removing section 2.11 as there is no “reliability based” justification that registration as TOP justifies a Medium Impact Rating. [or consider AECI's recommendation, below] [AECI] is ... proposing several changes to CIP-002-5, Appendix 1, pp 17 & 18, parts 1.2, 1.3, & 1.4, 2.10, and 2.11, in order to resolve technical discrepancies in MW impacts, and in particular deal with part 2.11’s implication that any BA or TOP of any size is at least a Medium Impact, as well as the part 2.11 implication that any 300 MW has Medium Impact upon the BES, which is simply not the case. Therefore, AECI suggests revising the Bright-lines for High Impact from 1500 to 3000 MW and controlling two or more elements. The Bright-lines for Medium Impact would be 1500 MW and controlling one or more elements. This will provide a more well-defined difference between High and Medium. In addition, part 2.10 changes deal with the same 300 MW impact issue, in addressing centralized UVLS and UFLS system size and impact, necessarily differentiating the two. AECI recommends changing 2.10 as described below. All changes are summarized below. CIP-002-5, Appendix 1, p 17, part 1.2 Replace: 1500 MW With: 3000 MW Replace: “one or more” With: “two or more” Rationale: Assess High Impact to twice that of Medium Impact potential CIP-002-5, Appendix 1, p 17, part 1.3 Replace: “one or more” With: “two or more” Rationale: Assess High Impact to twice that of Medium Impact potential CIP-002-5, Appendix 1, p 17, part 1.4 Replace: 1500 MW With: 3000 MW Replace: “one or more” With: “two or more” Rationale: Assess High Impact to twice that of Medium Impact potential CIP-002-5, Appendix 1, p17, part 2.10 Replace: “of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) ” With: “of 800 MW or more implementing Under Voltage Load Shedding (UVLS) or implementing Under Frequency Load Shedding (UFLS) within a single Interconnection in excess of thresholds in Table X (Derived once from 5%-droop for peak Interconnection load 2012, constrained to 5% error) Table X Interconnection UFLS Peak MW Threshold Eastern 1500 MW (cap on computed value of 4144 MW) Western 1400 MW (computed value was 1437 MW) ERCOT 750 MW (computed value was 772 MW) QUEBEC 300 MW (computed value was 310 MW)” Rationale: 1) Assess threshold for UVLS, no greater than a single large 800 MWnet coal-fired plant, because UVLS impacts are more localized and so a commiserate threshold is prudent in order to avoid cascading outages. 2) Assess UFLS Medium impact MW threshold level commiserate with Interconnection impacts, where no more than 5% of an Interconnection’s droop-characteristic governor-responses from nominal frequency to first-step UFLS relays per PRC-006 is allowed be risked within a centralized UFLS. However, the corresponding guidelines should note that, should an Entity’s centralized UFLS system fail, they could individually be assessed a Severe VSL for under-performance, and their RC be assessed greater than Low VSL for their aggregate failure to perform per current VSLs for Requirement 9 of PRC-006-1, page 13. (While this 5% margin agrees with PRC-006 Low Violation Severity Level for Interconnection Impacts, that Entity’s business risk of violation due to their UFLS system’s failure, could be enormous under NERC Standard PRC-006.) CIP-002-5, Appendix 1, p 17, part 2.11 Replace: “(1) perform the functional obligations of Balancing Authority or Transmission Operator, or (2) control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.” With: “(1) perform the functional obligations of Balancing Authority or Generation Operator, and control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW or more of BES generation, or (2) perform the functional obligations of the Transmission Operator, that includes control of one or more of the assets that meet criteria 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10. Rationale: Align Medium impact Medium impact 1500 MW or Asset amounts. (And see AECI recommendations for Parts 1.2..1.4 High impact ratings.)
Yes
Yes
Yes
Yes

Yes
Yes
Group
Tri-State G&T - Transmission
Tracy Sliman
No
Yes
Increase threshold for High Impact from 1500 to 3000 and increase threshold for Medium Impact from 300 to 1500.
Yes
Yes
Yes
Yes
Yes
Yes
Group
Seattle City Light
Pawel Krupa
General Comments: SCL does not support the approach proposed in version 5 of the CIP Standards, either as to fundamentals or details. Fundamentally SCL believes the v5 approach is flawed and will introduce significant compliance burden without ensuring cyber security for the BES. Detailed concerns remain as provided previously (please refer to comments submitted by SCL on January 6, 2012). Although today's enforcable CIP Standards share many of the flaws of v5, SCL believes industry would be better served by developing maturity around the existing Standards while developing a new, different approach to cyber security that is based on the established practices and theory of the information technology industry.
Individual
Steve Alexanderson
Central Lincoln
Yes
Yes
We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
Yes
Yes
Yes
Yes
Yes
Yes
1. Thank you for consolidating the low impact requirements. 2. We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
Individual

Oscar Alvarez
Los Angeles Department of Water and Power
Yes
Yes
LADWP does not have extensive comments on this matter at this time.
Yes
Yes
Yes
Yes
Yes
Yes
LADWP does not have extensive comments on this matter at this time.
Individual
John Tolo
Tucson Electric Power
Yes
Yes
The wording in Appendix 1. Criteria 2.3, where commas were added before and after “as necessary”, is unusual and seems to add confusion. The commas weren’t there in Draft 1 or Version 4’s attachment. Suggest removing the commas surrounding as necessary. TEPC agrees with EEI’s comment to CIP-002 regarding wording of facilities and clarifying the approach “Facilities, Systems, and equipment”.
Yes
Yes
No
Yes
No
No
R3, R5, and R6: Agree with EEI comment: Move R6 content applicable to R3 and R5 and remove R6 requirement, which will eliminate ‘double jeopardy’ concerns. Suggested language for R3: Each Responsible Entity shall identify a CIP Senior Manager by name, and document any change within 30 days. Suggested language for R5: Add applicable section of R6 to this requirement – “Delegation changes do not need to be reinstated with a change to the delegator.” Remove R6.
Individual
Russell A. Noble
Cowlitz County PUD
No
Yes
Cowlitz agrees with comments submitted by APPA, and in addition adds emphasis regarding the applicability section 4.2.2, second and third bullets where the verbiage “is required by a NERC or Regional Reliability Standard” is used. This implies that a Reliability Standard may be written to require the installation of equipment. This violates the statutory limitations established in regard to Reliability Standard development which “…does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Rather, it appears the SDT intent was to point to standards which followed the statutory allowance to write requirements governing “the design of planned additions or modification to such facilities.” However, such a Standard applicability would be vague and difficult to track. Cowlitz strongly advises that section 4.2.2 be revised such that it stands on its own, and does not require a general search through all the Reliability Standards to establish applicability.
Yes
Yes

No
No
No
No
Please refer to the comments submitted by APPA.
Group
PacifiCorp
Sandra Shaffer
No
No
• PacifiCorp supports the EEI consensus comments in general for item no. 3, but specifically endorses the approach to CIP-002-5 set forth in the alternate draft CIP-002-5 presented byproposal of MEC and -Alliant. PacifiCorp has consistently advocated this kind of approach from the first distribution of the Version No. 5 draft standards. The SDT has made minor stepincremental changes in response to industry comments on the framework of CIP-002-5, but has not made the wholesale structural change to the framework of CIP-002-5 that needs to be made to render the vital process of identifying the assets to be regulated under the standards simple and straightforward. PacifiCorp shares the industry opinion that the suite of Version No. 5 standards cannot and should not be supported by the industry until the fundamental problems with CIP-002-5 are corrected. PacifiCorp strongly recommends that the alternate CIP-002-5 be adopted in lieu of the current SDT draft, and that SDT efforts be re-directed at refining and improving the alternate approach. Comments on MidAmerican-Alliant Version---- The Requirement/Measurement language presented in the MEC-Alliant version of CIP-002 is easy to interpret and eliminates . The straight forward criteria will eliminate confusion for auditing efforts. • PacifiCorp agrees with the industry consensus provided in EEI's comments that external connectivity needs to be taken into much greater consideration in the suite of standards. The problem with including a qualifier in every requirement where connectivity is an issue is that this approach does not create any clean, bright lines of applicability, and only increases the complexity of the standards (requiring separate tracking for every asset that requires different treatment under the standards). The solution is to establish a bright line (between Medium and High impact rating facilities/assets) at a higher structural level in the standards. While PacifiCorp still believes that an "external connectivity" requirement should be universally applied to all regulated cyber assets, PacifiCorp is much more persuaded that it is particularly important to protect cyber assets in a High impact rating facility, regardless of whether those assets have/use external connectivity or not. But this is not true for cyber assets associated with Medium or Low impact rating facilities. Implementation of this bright line could be fairly simply accomplished by adding the following two sentences to the end of the definition of BES Cyber Asset: o "Unless integrated into a BES Cyber System that qualifies as a "High Impact Rating" BES Cyber System, a Cyber Asset is not considered a BES Cyber Asset unless it [uses/enables] external connectivity functionality (via either routable or dialup connectivity). All Cyber Assets integrated into BES Cyber Systems which have been designated as "High Impact Rating" BES Cyber Systems are automatically deemed to be BES Cyber Assets, regardless of whether they [use/enable] external connectivity or not." Any areas that dictate an exception to this bright line rule could then be addressed as a true exceptions, rather than the current situation where external connectivity is addressed in every requirement and sub-requirement that has a direct impact on a regulated cyber asset. • Another important issue that needs to be addressed is the proliferation of zero defect standards that impose large administrative burdens with no commensurate protections to the bulk electric system. nclusion is the "…detect flaws expeditiously;.." clause. 100% compliance is an untenable position in many instances throughout the suite of draft standards (including CIP-002-5), and creates an unreasonable burden on both entities and auditing bodies with no clear improvement in reliability. Utilities Responsible entities must be afforded the ability to manage business concerns that do not materially impact reliability within normal operational practices. PacifiCorp supports the various EEI consensus comments and specific language suggested in the alternate CIP-002-5 proposal of MEC and -Alliant alternate CIP-002-5 that eliminates administrative violations where flaws have been detected and corrected expeditiously.
Response to #1 • The process flow is a significant improvement over the last version (generally moving from analysis of the general to the specific), but the draft published by the SDT still clings to the erroneous view that BES Cyber Assets/BES Cyber Systems can exist independent of Facilities.

PacifiCorp strongly supports the alternate version of CIP-002 put forth by MidAmerican Energy Company (“MEC”)/Alliant, as such version presents a much clearer approach to the identification of high and medium impact BES assets. PacifiCorp believes that the industry and the drafting effort will be much better served by adopting and refining the alternate version of CIP-002-5 proposed by MEC-Alliant. See comments below in response to #3. • Facilities need to be categorized first (High, Medium and Low), and then the associated BES Cyber Assets and BES Cyber Systems, as is done in the current version of the standard and the MEC-Alliant proposed alternate version of CIP-002-5. • While the process steps in the current version of CIP-002 appear to move from general to specific, the substance of the defined terms that are used in the process steps (trying to ferret out BES Cyber Assets/Systems independent of BES Facilities) has the registered entity bouncing back and forth between the general and the specific, rendering the initial fundamental process of identifying assets to be regulated convoluted and confusing. • The term “BES Elements” needs to be eliminated from R1.4. Since Low BES Cyber Systems (BES Elements) are not discretely identified (and rightly so because it would be a waste of resources to track things on such an insignificant level), changes to those BES Elements are not discretely tracked either (making R1.4 impossible both to comply with and to audit since most relevant changes will be from a Low to a Medium category). Changes to Facilities which would move the Facility from a Low to a Medium category can and should be tracked. It is much more relevant to talk about changes that result in a significant change to a Facility than to changes to the Elements of a Facility. The Elements (BES Cyber Assets/Systems) are automatically re-categorized by association with the Facility when a change is implemented at the Facility level. • The process flow is a significant improvement over the last version (generally moving from analysis of the general to the specific), but the draft published by the SDT still clings to the erroneous view that BES Cyber Assets/BES Cyber Systems can exist independent of Facilities. PacifiCorp strongly supports the alternate version of CIP-002 put forth by MidAmerican Energy Company (“MEC”)/Alliant, as such version presents a much clearer approach to the identification of high and medium impact BES assets. PacifiCorp believes that the industry and the drafting effort will be much better served by adopting and refining the alternate version of CIP-002-5 proposed by MEC-Alliant. See comments below in response to #3. • Facilities need to be categorized first (High, Medium and Low), and then the associated BES Cyber Assets and BES Cyber Systems, as is done in the current version of the standard and the MEC-Alliant proposed alternate version of CIP-002-5. • While the process steps in the current version of CIP-002 appear to move from general to specific, the substance of the defined terms that are used in the process steps (trying to ferret out BES Cyber Assets/Systems independent of BES Facilities) has the registered entity bouncing back and forth between the general and the specific, rendering the initial fundamental process of identifying assets to be regulated convoluted and confusing. • The term “BES Elements” needs to be eliminated from R1.4. Since Low BES Cyber Systems (BES Elements) are not discretely identified (and rightly so because it would be a waste of resources to track things on such an insignificant level), changes to those BES Elements are not discretely tracked either (making R1.4 impossible both to comply with and to audit since most relevant changes will be from a Low to a Medium category). Changes to Facilities which would move the Facility from a Low to a Medium category can and should be tracked. It is much more relevant to talk about changes that result in a significant change to a Facility than to changes to the Elements of a Facility. The Elements (BES Cyber Assets/Systems) are automatically re-categorized by association with the Facility when a change is implemented at the Facility level. Response to #2 An annual period for this requirement is sufficient and adding the “not to exceed 15 calendar months” requirement is not warranted. There are many very good reasons that the timing of an entity’s annual review and assessment of its assets needs to be shifted or scheduled outside of a 15- month window from the last review. This requirement adds a layer of administrative compliance that is not supported by a reciprocal improvement to the reliability of the Bulk electric System.
Individual
Tony Kroskey
Brazos Electric Power Cooperative
No
No
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
No

No
No
No
Yes
Yes
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
Group
Puget Sound Energy, Inc.
Tom Flynn
Yes
Yes
None
Yes
Yes
Yes
Yes
Yes
Yes
Group
PNM Resources
Michael Mertz
No
Yes
See comment submission from EEI.
No
Yes
Yes
Yes
Yes
Yes
See comment submission from EEI.
Individual
Darcy O'Connell
California ISO
Yes
Yes
Yes
No
No
No
No
CIP-003 R3 we agree with the requirement but have issues with the definition of a CIP Senior Manager in that the definition should include the operation and maintenance of the requirements (ongoing compliance). Looking at the definition of a CIP Senior Manager it appears that the after the requirements are implemented, according to the implementation plan, that there is no longer a need

for a “CIP Senior Manager”. This appears to contradict what is required in CIP-003. CIP-003 R4 M4 item 2 change the words “dated signature” to “dated approval” for better alignment with the requirement. CIP-003-5 R5 M5 change the word “signed” to “approved” for better alignment with the requirement. CIP-003 R6 M6 needs to be reworded and clarified.
Individual
Martin Bauer
US Bureau of Reclamation
No
Yes
1. Add another categorization level of “Minimal Impact” BES Cyber Systems which are not included in high impact, medium impact, or low impact shall default to the category of minimal impact, which includes small control centers that control an aggregate highest rated net Real Power capability of the preceding 12 calendar months ranging from 300 to 700 MW of BES generation and Blackstart resources and generators rated below 75 MVA. Minimal impact facilities do not require further consideration. 2. Section “Categorization Criteria” Change third sentence to read “All BES Cyber Systems or Facilities not included in Attachment 1 – Impact Rating Criteria, Parts 1.1 to 1.4 and Parts 2.1 to 2.11 defaults to be low impact and do not require discrete identification; or minimal impact and do not require further consideration.” Change Section 3.2 to read Blackstart Resources rated at 75 MVA or greater. 3.3 Elements in the cranking path of black start resources rated 75 MVA or greater and initial switching requirements. (Rationale: If the BES impact rating is “minimal” then no further consideration should be required, including any associated access protection system requirements. Small control centers that control and Blackstart resources/generators rated below 75 MVA would be included in the “minimal impact” category, thus reducing costs/resource burdens for smaller facilities, and the likelihood of entities removing Blackstart resources from restoration plans.
Yes
Yes
Yes
Yes
Yes
Yes
Group
Hydro One
Sasa Maljukan
No
Yes
Yes
Yes
Yes
Yes
No
Yes
Recommend changing R5 from “sign” to “approval” since some companies use other approval processes. Also these Measures criteria to align with Requirement. This Measure includes “to approve or authorize specifically identified items” while the Requirement states “and approved by the CIP Senior Manager” Request a re-written M6 since it appears to add a new Requirement – “that within 30 days of discharging the delegated authority” Recommend updating CIP-003 R2’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures shows R2 as “low”

Name (63 Responses)
Organization (63 Responses)
Group Name (40 Responses)
Lead Contact (40 Responses)
Question 1 (92 Responses)
Question 2 (92 Responses)
Question 3 (92 Responses)
Question 4 (92 Responses)
Question 5 (91 Responses)
Question 6 (91 Responses)
Question 7 (92 Responses)
Question 8 (0 Responses)
Question 8 Comments (103 Responses)
Question 9 (0 Responses)
Question 9 Comments (103 Responses)
Question 10 (91 Responses)
Question 1 (90 Responses)
Question 12 (0 Responses)
Question 12 Comments (103 Responses)
Question 13 (0 Responses)
Question 13 Comments (103 Responses)
Question 14 (91 Responses)
Question 12 (90 Responses)
Question 12 (91 Responses)
Question 12 (0 Responses)
Question 17 Comments (103 Responses)
Question 12 (93 Responses)
Question 12 (93 Responses)
Question 12 (92 Responses)
Question 12 (92 Responses)
Question 12 (92 Responses)
Question 23 (0 Responses)
Question 23 Comments (103 Responses)
Question 12 (0 Responses)
Question 24 Comments (103 Responses)

Individual
David Proebstel
Clallam County PUD No.1
Yes
Yes
Yes
Yes
Yes
Yes
Yes
no comment
no comment
Yes
Yes
no comment
no comment
Yes

Yes
Yes
no comment
Yes
Yes
Yes
Yes
Yes
no comment
no comment
Group
Northeast Power Coordinating Council
Guy Zito
No
No
Yes
No
Yes
Yes
No
Recommend removing “, but not limited to,” from R1 Part 1.1 Measure since the Measures are only guidance. Recommend removing “potential” from R2 Part 2.7 since an incident is determined to be real or potential during the follow up investigation. Request additional clarification on R2 Part 2.10 in the Application Guidelines. From the CIP-004-5 Table R2 - Cyber Security Training Program, the use of the terms interconnectivity and interoperability with regard to FERC Order No. 706 needs to be clarified to make the differences and applications of the terms understood. Request clarification on R4 Part 4.2 since it is not clear if the numbers should be read as “and” plus does the six months apply to all of the numbers? Prior versions of R4 Part 4.3 had exclusions for laws or collective bargaining agreements. Please add the exclusions or explain why the exclusions were dropped. Recommend different VSL thresholds for R3. Differentiating by individuals is bad for large organizations. Differentiating by percentage of associated is staff is bad for small organizations. Recommend different VSL thresholds for R5. Differentiating by individuals is bad for large organizations. Differentiating by percentage of associated is staff is bad for small organizations.
Request a more clearly worded R6 Part 6.4. The intent appears to be authorizing (electronic/physical) access to BES Cyber Systems Information. Request additional clarification in this Requirement and Application Guidelines. Note that Requirement 6.1.3 also uses “physical and electronic locations.” In R7 Part 7.4, recommend changing “Requirements R7.1 and R7.3” to “Requirement R7 Parts 7.1 and 7.3.” In the corresponding Measure, recommend changing “removal” to “revoke” for consistency with the Requirement. In some systems removal results in removing all corresponding records which makes it hard to provide the proper records to the auditor. Recommend updating the R7’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures show R7 as “low”.
No
No
Recommend removing “, but is not limited to, ” from R1 Part 1.1 since the Measure’s scope already includes all of the possible Cyber Assets Measures should not dictate Requirements. If correct, then how can CIP- 005 R1 Part 1.5’s Measure specify “intrusion detection system” when the Requirement does not specify a technology? Also specifying a technology may prevent a newer, better technology from being used until the Standard is updated. Recommend changing R1 Part 1.5 from “intrusion detection system” to “detection system”. Request for clarification on how the math for R1 is done in the VRF/VSLs.
Request clarification on R2 Part 2.1 – can the Intermediate Device be on the ESP? Can the Intermediate Device also be an EAP? Recommend changing R2 Part 2.3 from “Factors must be at

least two of the three following categories" to "Multi-factor include, but are not limited to" which allows future technology without a Standards update.
Yes
No
Recommend changing the testing in R3 Part 3.1 so that the High Impact BES Cyber Systems are tested every 24 months and Medium Impact BES Cyber Systems with External Routable Connectivity are tested every 36 months.
Yes
No
No
No
No
For R2, request clarification if the SDT's intent is that the following timeline will be compliant or not. 1) on 5/1/2012 the patch is identified; 2) by 6/1/2012 complete the assessment for applicability (30 days); 3) by 7/1/2012 the plan is developed and defined for testing plus implementation (30 days); 4) per the plan, testing completed by 9/1/2012; 5) per the plan, patch deployed by 10/12/2012; 6) on 10/30/2012 patch fails (through no fault of testing); 7) emergency patch back out on 11/1/2012; 8) per plan, develop mitigation plan by 12/1/2012 (30 days); 9) per original plan, mitigation testing completed by 2/1/2013; and 10) per original plan, mitigation patch deployed on 3/12/2013 Recommend changing R3 Part 3.3 so that Medium Impact remote locations with no external connectivity (isolated networks) have more than 35 days Suggest changing R4 Rational from "(1) immediate detection" to "(1) real time detection" to be consistent with Part 4.2 Request clarification on R4 Part 4.1.1. The CIP Standards expect "deny by default" firewall rule which results in dropping offending packets such that there is nothing to log. How can the Registered Entity meet Part 4.1.1 criteria of logging failed access attempts at the EAP? The wording in the Measures column does not reflect what the Requirement is stipulating. Recommend removing "malicious" from R4 Part 4.1.4 since "malicious" is determined after the fact and Parts 4.1.1, 4.1.2 and 4.1.3 capture the events that may be malicious. For R1 as written, recommend that missing one port is too high since the PSP is the first layer of defense. Missing one physical port should not be a Severe VSL. Recommend this is a Low VSL. Recommend increasing percentages from Low – Moderate – High – Severe. Recommend that the number of assets should be another differentiator for R3's Low – Moderate – High – Severe. Recommend that the difference between R4's Low – Medium – High – Severe should be number of assets with two weeks throughout. Recommend that R4 should start with a Low VSL and use the number of assets combined with the number of accounts as a difference between Low – Medium – High - Severe.
Request clarification of R5 Part 5.7. Does the technical feasibility apply to both "the number of unsuccessful authentication attempts" and "generate alerts after a threshold of unsuccessful log in attempts" or only the "authentication attempts?"
Group
PPL Corporation NERC Registered Affiliates
Stephen Berger
Yes
No
Yes
No
Yes
No
Yes
1.) CIP-004 R2. Members of the SDT explained that the intent of "personnel who have …access…" be limited to company personnel, not vendors or others. This needs to be clarified if that is the intent.
1.) PPL Affiliates support the associated EEI comments for R6.3 : EEI Comments: Propose changing "The individual(s) designated in Part 6.1 shall authorize unescorted physical access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP

Exceptional Circumstances." To "The individual(s) designated in Part 6.1 shall authorize unescorted physical access into Physical Security Perimeter(s) that the Responsible Entity determines is appropriate, except for CIP Exceptional Circumstances." In order to scope this requirement to the PSP.
No
No
1.) The definition of "External Routable Connectivity" is currently limited to a BES Cyber System that is accessible from a Cyber Asset that is outside its associated ESP. This should be expanded to include any Cyber Asset, not just BES Cyber Systems.
No
No
Yes
1.) R1: PPL Affiliates request removal of the "External Dial-up Connectivity" in the VSL table under the Severe VSL Column heading on the bottom right of page 23 of 29 in CIP-006-5. Dial-up connectivity is not included in the applicable columns associated with any of the CIP-006-5 Requirement Parts. 2.) PPL Affiliates have concerns about R1.4 and R1.6 and the 99.9% uptime requirement: PPL Affiliates appreciates all the value-added work the SDT has provided on the CIP Version 5 project. PPL Affiliates would like the SDT to consider changing R1.4 and R1.6 language to 'Implement controls that monitor access to the Physical Security Perimeter 24 hours a day, seven days a week.' PPL Affiliates believe that the requirement of having 24x7 controls restricts access appropriately. PPL Affiliates understand the requirement of 24x7 means very high availability. PPL Affiliates assumes the added language was intended to prevent frequent downtime causing risk to the control. However, the proposed phrase '(with 99.9% availability), for unauthorized circumvention of a physical access control into a PSP' increases documentation requirements without increasing BES reliability or reducing risk of unauthorized access. 3.) R2.1: PPL Affiliates request that the SDT revise R2.1 to read 'Require continuous escorted access of all Visitors within each PSP, except during CIP Exceptional Circumstances', with Visitors defined as 'Any individual (employee or non-employee) without unescorted physical access. PPL Affiliates' concern over the proposed language is that the phrase 'who are known or guests ' could be confusing. Additionally, defining visitor that is in other requirements proposed language clarifies those standards as well.
No
Yes
Yes
Yes
Yes
1.) R1.2: Regarding the requirement to "[p]rotect against the use of unnecessary physical input/output ports…", this may go further than the intent of the referenced FERC order from 3/18/2010, and in any case will be very difficult to implement as written. Prior discussions over the past couple of years had focused around the protection of unused network access ports. This has been broadened to every conceivable input/output port on an asset. Signage does very little to protect against this use, and other controls (like physically disabling USB ports to prevent connection of portable media devices) can limit recovery options during emergencies. The same is true with software solutions, though these can overridden by administrators. In general, PPL Affiliates support focusing on unused network ports and eliminate the rest. There are other protective controls in the requirements to deal with potential malware infections that could be introduced via portable media.
Group
CIP Version 5 Comment SME list
Gerald Freese
Yes
No
No

No
Yes
No
No
1. R2.1: While this requirement has been improved to clarify the entity is the one who identifies each role and the training required for each role, it is still not explicit that the training required are the topics in R2.2 through R2.10. 2. It should be made clear that R2.2 through R2.10 are a “pick list” to choose from for each role, and an entity has license to choose as few as one topic (or as many as 9 topics) for a particular role. 3. AEP is uncertain whether a single role, with all training (R2.2 through R2.10) is acceptable. For large entities, who don’t necessarily classify personnel by “role”, an extensive effort to create “roles” to offer narrowly differentiated instruction may not be commensurate with the reliability and security gain. Moreover, to fully utilize the “roles” at large entities (where personnel might “wear several hats”) may require hundreds of roles, with a single person filling multiple roles at the same time. This would result in a multidimensional matrix to determine training requirements, again not be commensurate with the reliability and security gain. AEP recommends that if it is acceptable to offer a single training program to multiple roles, the drafting team clarify that in the standards. 4.2.2, 4.2.3 - Is “six months” contiguous? If you go home to a residence in a different county / state on weekends, does that count against your six month boundary? Does it reset the timer? Or is the six months an absolute timer over the course of a year? Or some other interval? For large entities, this still represents an enormous amount of work by skilled functionaries who can figure out in which county a particular school is located, or where a particular work location is. Bottom line – it would be easy to hide a location where a crime occurred, and it would be impossible for the entity to figure out whether the list was truthful and complete. AEP believes this simply cannot be accomplished through the NERC regulatory model. Criminal background check vendors do not provide services that can verify the accuracy or inclusivness of locations where people have worked or attended school
4. R7.2: Similar to R7.1, problematic. Removing access by the end of the next calendar day Effective dates for new jobs could be Saturdays. This one also entails extensions of access for training, transition, etc. Reword. 5. R7.1 – AEP believes this should clarify that “complete the revocation” refers exclusively to “unescorted physical access and Interactive Remote Access.” Recommend adding the specific actions required in the wording of the requirement. 6. AEP believes that “voluntary” terminations (retirements, co-op students returning to school, etc.) really should be treated differently than “involuntary” termination actions. AEP suggests allowing for a difference between a mutually accepted “termination or separation” and a “termination for cause” and incorporating that concept into 7.1 and 7.2. 7. Since there is no requirement for revocation of “balance of access” R7.4 for Medium Impact BES Cyber Systems, is there a particular timeline required? Recommend a timeline be developed that provides auditable records for removing balance of access.
No
Yes
R1:) The applicability column should be modified to High and Medium with External Routable Connectivity. Standalone networks would be required to declare an ESP but there would be no requirements applied to the ESP. The ESP documentation of standalone networks would provide no reliability benefit to the BES. 2. R1.3: Need additional clarification on the requirement; perhaps through guidance. “Require inbound and outbound access permissions.” This requirement implies that in addition to establishing inbound Access Control Lists (ACLs) that a second set of ACLs is required for outbound communications. This is particularly a concern because it applies to Medium impact as well as High Impact Electronic Access Points. 3. R1.4: This requirement refers repeatedly to “dial-up connectivity.” Is dial-up connectivity defined to include for example, ISDN connections or is it limited to modems? Recommend that a definition be developed for “dial-up connectivity to eliminate confusion on the scope of the requirement. 4. R1.5: This requirement states that entities must “have a method for detecting malicious communications.” Malicious communications is a vague term that could apply to a host of items, not all of which would be associated with attacks on systems or networks. Suggest rewording to reflect the intent of the requirement. For example, qualify the term with a caveat such as “known or suspected to disrupt, destroy or otherwise compromise Electronic Access Points.”
R2: The applicability column for R2.1, R2.2, and R2.3 should be modified to High and Medium with

External Routable Connectivity or dial-up connectivity. Unless External Routable Connectivity or dial-up connectivity exists, Interactive Remote Access or an Intermediate Device does not exist.
No
Yes
Yes
1. R1.4 should be considered for removal. Monitoring 24x7x365 with a 99.9% uptime would require extensive resources and may be technically unrealistic. Recommend changing the actual requirement for 99.9% uptime to “document any disruption of uptime, root cause and remediation actions”, or words to that effect. 2. R1.3 – Asks for two or more different physical access controls to collectively allow physical access into Physical Security Perimeters. Would these be applied to the Physical Security Perimeter specifically or in a defense in depth concept, be applied to external fencing around the facility as well? Recommend that guidance be provided that clarifies how “defense in depth” should be viewed for the completion of this requirement. 3. 1.7 – The time frame of 15 minutes is questionable. Also, the administrative burden providing documented proof of initiation of alarm investigation is excessive and adds little if anything to increasing or maintaining BES reliability. The 15 minute time frame would mean that a 16 minute response time would be a violation. If we are keeping the documentation requirement, then the time limit needs to be extended. Recommend, however, that we remove the documentation requirements.
Yes
Yes
No
No
Yes
1. R2.3- Recommend a rewording of "vulnerabilities exposed by each security patch" to some thing closer to "vulnerabilities remediated by each security patch." The security patch is not what exposes the vulnerability. 2. R3.1- Is "or" appropriate in "deter, detect, or prevent malicious code"? This seems to indicate that an entity only has to "deter" malicious code, which could simply be addressed by a security awareness campaign. 3. R4.1- Recommend that this requirement be rewritten with a "where technically feasible" addition. 4. R4.1.4- Recommend that guidance provide a more concrete explanation of what would be included in "malicious activity."
5. R5.6- Recommend that the second measure be modified to include a dated attestation that passwords were changed. Lacking that, there is no consistent means of verifying that the requirement has been met.
Individual
Michael Falvo
Independent Electricity System Operator
No
No
No
Yes
Yes
No
No
For CIP-004-5, R2, IESO disagrees with the “role-based cyber security training” approach, and suggest SDT change this requirement based on or tailored to job function based training approach. In its current form, the “role-based” statement in this requirement infers that the training should be provided based on permissions or access should be role based. For CIP-004-5, R2.1, change “identification of each role” to “identification of roles based on job functions” required for BES cyber access. For CIP-004-5, R2.10, IESO suggests that SDT to modify this requirement to clearly to emphasise the intent of the requirement, as the current form does not give us a clear picture of what was intended. For CIP-004-5, R3, similar to the comments and rationale provided on CIP-004-5, R2, that the “role-based cyber security training” need to be replaced with training based on or tailored to job function.

For CIP-004-5 R6 Part 6.6, IESO suggests the removal of measure 2.A: “summary description of privileges associated with each group or role”. For CIP-004 R6 – Part 6.1 – 6.1.3: states “access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity.” This statement implies that having physical access to BES systems alone is enough for someone to gain access to the information residing within it, which is misleading. The building maintenance staff, such as Janitors, and many IT staff may have access to the data center where the BES system is situated; however, this does not grant them automatic electronic access to the system or the data residing within that system. For CIP-004-5, R7.2: IESO suggest that the one day duration to revoke access for reassignments or transfers is too restrictive and should be changed to a 30 day duration to complete these revocations. The sections CIP-004-5, R7.4, and 7.5 deal with termination, which is more risky scenario than reassignments and transfer actions, and prescribes a 30 day window to revoke access and IESO suggests the duration should be adopted for the rules outlined in CIP-004-5, R7.2 for reassignments or transfers.
No
Yes
For CIP-005-5, R1.5: IESO believes it is not appropriate to prescribe Intrusion Detection System (IDS) as the only measure for detecting malicious communication. In fact, IESO believes that it is reasonable to state that statements within a standard should only focus on requirements relating to a specific topic, and no specific technologies should be referenced anywhere within it as means to gain compliance.
No
No
No
For CIP-006 R1 – Parts 1.4 and 1.6: These rules require multiple controls must be in place for the monitoring, which IESO disagrees. We suggest SDT to change the phrase “Have Controls” to “Have Control(s)”. For CIP-006 R1 – Parts 1.5 and 1.7: IESO suggest the removal of the “BES Cyber Security Incident Response Plan”, since physical security incidents are not considered cyber security incidents.
No
Yes
No
No
No
For CIP-007-5 R3 - Part 3.1: IESO suggest the removal of the word “deter” from the requirement as it is not possible to “deter” malicious code from entering through an electronic communication. For CIP-007-5 R3 - Part 3.2: The second and third bullets reference technologies, which is not appropriate and should be removed from this section. This first bullet point alone is enough to measure the compliance of this requirement. For CIP-007-5 R4 and R3: For maintaining consistency throughout the standard, IESO suggest the use of “malicious code” rather than “malicious software”, which is referenced here. For CIP-007-5 R4.1.4: Unless the SDT defines what “malicious activity” is, the IESO suggests the removal of this phrase. For CIP-007-5 R4.2: The term “real-time alerts” is not defined, and using this term in the standard without the definition it is open for interpretation. With this current form, it is not clear whether “real-time alerts” are alerts triggered as they received by the monitoring facility or it is at the time of actually occurred on the target BES system. For CIP-007-5 R4.5: IESO believes the measure should include the clause “where automated processes and alerting are not possible” as part of the measure. It should not be necessary to maintain manual tracking and review of alerts, if alerts are triggered automatically and followed up through a ticketing system, for example.
For CIP-007-5, Part 5.1: The meaning of the term “user access” is not clear and needs to be defined. For CIP-007-5, Part 5.3: IESO suggests that the measure should be reworded to include “authorized access”: “Evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.” For CIP-007-5, Part 5.4: IESO suggest the words “devices” and “instances of application” should be removed from the requirements to leave only “Cyber Asset”. The following is the suggested new requirement: “Change default passwords,

where technically feasible, unless the default password is unique to the Cyber Asset." For CIP-007-5, Part 5.5 and Part 5.6: Since IESO is a unionized work place, it may be difficult to obtain attestations from union members in order to satisfy second bullet within the measure for this requirement. IESO suggests adding a new measure that includes procedural control and a training aspect to handle this requirement. For CIP-007-5, Part 5.5.1: IESO request that this requirement should be reworded to remove the phrase "the lesser of" to the following: "Password length that is, at least, eight characters or the maximum length supported by the Cyber Asset", and Part 5.5.2 reword to "Minimum password complexity that is at least three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset." For CIP-007-5, Part 5.7: IESO recommends that the SDT to define the number of unauthenticated logon attempts and a threshold number that is reached before an alert is triggered. Without having these numbers defined within the standard requirements, it will be inconsistent between entities.
Group
Southwest Power Pool Regional Entity
Emily Pennel
Yes
No
No
Yes
No
No
No
(1) Requirements R2, R3, R4, and R5 should be applicable to Medium Impact BES Cyber Systems irrespective of any External Routable Connectivity or dial-up connectivity. BES Cyber Systems and their component Cyber Assets generally have security controls and inherent vulnerabilities to insider threats whether or not they also have connectivity beyond the fence. (2) Part 2.10 properly requires training content on risks associated with a BES Cyber System's electronic interconnectivity and interoperability. This connectivity does not have to be beyond the Local Area Network, further supporting the need to make R2 applicable to all Medium Impact BES Cyber Systems. (3) The suggested evidence for Part 3.1 should be clarified to expect both the individual training records and the date access was first authorized. Both elements are necessary to demonstrate compliance. (4) R5.2 needs to be modified to require the personnel risk assessment to be updated prior to the seventh anniversary of the previous assessment. The use of the term "calendar years" could be misconstrued by the Responsible Entity as any time in the calendar year (January 1 – December 31) in which the PRA reaches its seventh anniversary, even though the requirement also states the expectation that the current PRA is no older than seven years. (5) The High VSL for R1 should be modified to require the missed awareness training to occur within the following calendar quarter. A failure to provide awareness training for two or more consecutive quarters should be a severe VSL. (6) The Moderate VSL for R2 should apply if the Responsible Entity failed to include 2 "or 3" of the required training content. (7) The guideline for R3 refers to CIP Exceptional Circumstances that are "approved" by the senior manager or delegate. CIP-003-5 / R1.10 only requires the Responsible Entity to document and implement provisions for declaring and responding to CIP Exceptional Circumstances. R1.10 does not prescribe a governance structure that requires senior manager or delegate approval.
(1) Requirements R2, R3, R4, and R5 should be applicable to Medium Impact BES Cyber Systems irrespective of any External Routable Connectivity or dial-up connectivity. BES Cyber Systems and their component Cyber Assets generally have inherent vulnerabilities to insider threats whether or not they also have connectivity beyond the fence. (2) The "and" at the end of Part 6.1.2 should be "and/or". (3) The evidence supporting Part 6.6 needs to demonstrate that user accounts have been properly provisioned, essentially access has been granted on the correct Cyber Assets with the correct access rights. (4) R7 should include provisions for documenting a transition period to allow for continued access for a defined period of time following a transfer. The time period for revoking unneeded access would commence with the expiration of the transition period. (5) Part 7.1 should include the requirement to disable or revoke all individualized domain user accounts held by the terminated staff. (6) The change rationale for Part 7.2 refers to a NIST SP 800-53 control requiring a

review of access. This could cause some Responsible Entity confusion as the requirement is to "revoke" access, not "review" such access. If the expectation is to revoke only the access the Responsible Entity has reviewed and determined to no longer be necessary, the requirement should be restated to reflect that expectation. (7) Part 7.4 should also include Medium Impact BES Cyber Systems or another requirement should be defined that includes the Medium Impact systems. As written, the Medium Impact BES Cyber Systems essentially fall through the cracks and individual user accounts will never have to be revoked. (8) Passwords for administratively privileged shared accounts should be changed much faster than the 30 calendar days specified in Part 7.5. (9) The second bullet of the example evidence for Part 7.5 should be clarified that password reset is only required if the individual being transferred no longer needs such access in the new position or role. (10) The guidance for R7.1 should also include the revocation of domain account access.
No
Yes
(1) Part 1.1 should also apply to associated Protected Cyber Assets as stipulated in the language of the requirement. (2) The measures for Part 1.2 still need a process to verify all Electronic Access Points have been identified. A network diagram does not demonstrate compliance by itself. (3) The percentages found in the VSLs will be difficult to determine. Does the percentage refer to "permit statements?" The number of Cyber Assets associated with the permitted access? The number of ports used permitted traffic? Something else? The VSL as written is too vague to be measurable. (4) The guidance for R1 discusses the limitations on the ability of a BES Cyber System to communicate through the EAP. This commentary appears to conflict with the requirement for an intermediate system (jump host) that essentially denies the ability of the Cyber Asset within the ESP to communicate with any other system outside of the ESP.
(1) R2 should also apply to Physical Access Control Systems and systems serving as Electronic Security Perimeter Access Points.
No
Yes
No
(1) The requirements need to be applicable to the associate physical access control and electronic access control and monitoring systems. (2) The term "availability" as used in Part 1.4 and Part 1.6 needs to be defined. Does the availability calculation include outages for planned maintenance activities, or only unplanned outages? (3) The testing required by Part 3.1 needs to include the logging and monitoring systems to verify proper operation. (4) The Moderate and High VSLs for R1 need additional clarification. The difference between unauthorized physical access and unauthorized circumvention of a physical access control is not clear. The expectation needs to be explained. (5) The Lower VSL for R3 needs to refer to 12 "calendar" months of outages to comport with the language of the requirement. (6) The description of Alarm Systems used to monitor physical access in the guidelines for R1 states the alarm needs to provide for "immediate" notification. The requirement in Part 1.5 states the notification must occur within 15 minutes of detection. (7) The description of Video Recording used to log physical access needs to clarify that the recorded video needs to be date/time stamped. (8) The guidelines for R1 needs to define the difference between unauthorized physical access and unauthorized circumvention of a physical access control. (9) It is not clear from the FERC comments in Order 706 that two complementary controls can be implemented on a single Physical Access Control System as stated in the guidelines for R1. Paragraph 562 (the FERC NOPR "proposal") states that "use of a minimum of two different security procedures would, for example, enable continuous security protection when one of the security protection measures is undergoing maintenance and provides redundant security protection in the event that one of the measures is breached." Implementing two controls on a single access control system does not address the single point of failure concern. (10) The guideline for R1 requires physical barriers for any opening exceeding 96 square inches with one side exceeding 6 inches. This explanation needs to be modified to stipulate the side exceeding six inches is the short side. Otherwise, this explanation could result in nonsensical dimensions requiring physical barriers. (11) The drafting team should consider the use of electronic barriers (e.g., infrared beams) in lieu of physical barriers for openings exceeding 96 square inches. There may be operational or technical limitations that preclude the use of physical barriers, such as impeding air flow through the protected opening. (12) The guidelines for R2 need to clarify that general logging of entry into a facility that is not entirely a PSP does not constitute logging of

entry into the PSP. The guidelines also need to address logging requirements when entering multiple PSPs in the course of the visit (either moving from one PSP to another or entering progressive perimeters). (13) The equipment to be tested per the guidelines for R3 should include the logging and monitoring systems (e.g., door contacts that generate forced open and door held alarms).
No
No
No
No
No
(1) Part 1.1 needs to consider more than “listening” ports. An unexpected connected port could indicate a successful compromise of the Cyber Asset with the malware making an outbound connection to a Command and Control system. (2) The “signage” referenced in the example measures for Part 1.2 is a weak control that does not provide an adequate level of protection as required. (3) Security patch management is a key fundamental control that should be applied to all Cyber Assets, including Low Impacting BES Cyber Systems. (4) Allowing the Responsible Entity to select a SCADA vendor as their source of potentially applicable patches increases the risk to the BES. The Responsible Entity needs to monitor the original source of a patch, such as Microsoft for Windows patches, and assess applicability within 30 calendar days of the initial patch release. There is a difference between “applicable” and “installable.” Waiting for the SCADA vendor to “certify” a patch as compatible is an issue of ability to install, not applicability. Requiring the Responsible Entity to assess for applicability based on the original patch provider’s release does not jeopardize any contracts or maintenance agreements. The entity still has the ability to self-determine the patch can or cannot be installed or wait for the vendor certification before installing. In the interim, the Responsible Entity, having determined a patch is applicable, can and should implement compensating measures until such time as the patch is certified. Allowing the Responsible Entity to rely upon a SCADA vendor’s certification as the trigger for the assessment process could result in patches that are not considered for an excessive period of time if the vendor does not report out the patch until it is “certified.” (5) Part 2.3 needs to be more specific as to the expectation of patch implementation. Part 2.3 only requires the entity to develop a timeframe to complete the identified mitigations, with no parameters defining an acceptable timeframe. For example, a Responsible Entity that chooses to not install any Oracle patches nor apply any interim compensating measures except as part of a planned end-of-life server upgrade would have to be found compliant, yet has done nothing to mitigate the risk imposed by the un-patched vulnerability. That renders Part 2.3 nonsensical. (6) Malicious code prevention is another fundamental control that should apply to all Cyber Assets capable of running anti-malware solutions, including Low Impacting BES Cyber Systems. (7) Updating anti-malware signature files every 35 days opens a window of unacceptable risk. As written, the requirement of Part 3.3 could possibly be gamed to not install any recent signature file. The Change Rationale expresses the desired outcome, but the requirement is not as clear. (8) Signature files still need to be “staged” (a form of testing) before implementing in the production environment. There is too much past history of a corrupted or faulty signature file being implemented that then improperly determines key software to be malware. This could be catastrophic if numerous Responsible Entities using the same anti-malware provider all implement a faulty update that quarantines or deletes critical software systems used to manage BES reliability. (9) The suggested evidence for Part 4.1 should include samples of logs demonstrating that the appropriate events are being logged. (10) Part 4.2 should prescribe a minimum expected set of security events for which alerts should be issued (if the Cyber Asset is capable of detecting and logging those types of events. Examples include failed login attempt threshold exceeded, account lockout, key software failures, and virus or malware alerts. (11) What is the expected delivery time for a “real-time” alert? (12) The example measures for Part 4.2 should include examples of issued alerts. (13) Part 4.3 presumes, but does not prescribe, a mechanism for monitoring for and detecting logging system failures. (14) Part 4.4 should also apply to Medium Impact BES Cyber Systems not in a control center that are capable of generating and storing security event logs. (15) Part 4.5 needs to define minimum expectations for sampling logged events. For example, is 1 out of 100 logs adequate? 30 minutes of logs in the two-week period? Ideally, an event log analysis tool (SIM, SEM, SIEM, or SEIM) should be required in the control center environment, especially for High Impacting BES Cyber Systems. (16) The guidelines for R1 need to discuss the importance of monitoring more than just Listening ports (see comment 1, above). (17) The guidelines for R2.1 need to discuss the difference between applicable and implementable (see comment 4, above). (18) The guidelines for

Part 2.2 state that the Responsible Entity must be allowed to evaluate their individual risk exposure and determine if any compensating steps are to be taken. This is, in effect, acceptance of risk. FERC has already clearly stated that Responsible Entities cannot accept risk in Order 706. (19) The guidelines for Part 2.2 should discuss what “applicable” means. It is not clear from the discussion that Responsible Entities are only required to monitor patches for installed software. (20) The guidelines for Part 3.3 should discuss the importance of staging (“testing”) anti-malware updates before implementing into production. (21) Alerts on a system display, as referenced in the guidelines for Part 4.2, only work if the display is monitored. The guideline needs to make that concept clear.
(1) System access control is a fundamental control that should also apply to Low Impacting BES Cyber Systems. (2) Part 5.2 needs to clarify what is meant by “generic account types,” Does this, for example, include the “IWAM” and “IUSR” accounts created with the installation of Microsoft IIS? (3) When should default passwords be changed per Part 5.4? (4) Allowing a default password to remain unchanged per Part 5.4 is a very poor control in light of the recent RuggedCom issue where the default password was unique to the device but was based on a readily available piece of information, the MAC address, and easily determined. This control only makes sense if the unique password is truly random, such as might be the case with the “IWAM” and “IUSR” user accounts associated with Microsoft IIS. (5) Part 5.5 should require password complexity and other settings to be technically enforced to the maximum extent possible. (6) Part 5.7 should define the minimum acceptable failed login attempt threshold parameters. (7) The High VSL for R5 refers to failing to implement procedures to authorize the “use of” certain account types. Requirement R5 does not require authorization of “use”, only enablement. (8) The Severe VSL for R5 includes criteria for failure to implement procedures for password-based user authentication. Does this inadvertently mandate the use of passwords? Does it require password procedures even if passwords are not used? (9) The guidelines for R5 need to define what a “generic” account is. (10) The guidelines for Part 5.5 states the technical or procedural enforcement of password parameters are only required where passwords are the “only” credential used to authenticate individuals. Requirement R5, Part 5.5, does not contain the same stipulation. (11) The table at the end of the R5 guidelines needs modification. The table should make it clear that shorter passwords need to be changed more frequently. Additionally, the suggested change periodicity of two years or more for system account passwords with 25+ pseudo-random characters is inconsistent with the stated requirement to change passwords at least annually.
Individual
Mario Lajoie
Hydro-Quebec TransEnergie
Yes
No
Yes
Yes
Yes
No
No
(1) We agree with the comments provided by the NPCC TFIST on CIP-004 (2)Change table in 2.1 "Identification of Each role" by "identification of ROLE
(1)E7.5 - Technical Feasibility Exception (TFE) should be allowed (2) the requirement (R7) should apply only on interactive account.
No
No
(1) We agree with the comments provided by the NPCC TFIST (2)E1.5 - We don't think that we need to deploy an IDS for every ESP. The requirements should requires that some IDS should be deployed between the ESP Access point and the Internet but with no particular specification. This way, we could deploy a few IDS within our corporate network at the most critical node instead of deploying and managing an IDS for every ESP. So we would like the requirements to let the entity decide where to strategically place IDS based n their own network structure and also, based on their own risk assessment and analysis. (3) We believe that the "intermediate device" should be protected by a PSP but should not be in the same EAP that BES CYBER ASSET.

(1) We agree with the comments provided by the NPCC TFIST
No
No
No
(1)We agree with the comments provided by the NPCC TFIST (2) Request for clarification on R1.5 and R1.7 have to do physical and human intervention within 15 minutes of detection. This is not possible for a remote site where there is no staff on site. (3) CIP-006-5 R2 The non-compliance during emergencies should not lead violations (4) We recommend changing the testing in R3 Part 3.1 so that the High Impact Bes Cyber System are tested every 24 months and Medium with external routable are test every 36 MONTHS.
No
No
No
No
Yes
(1) R1.2: Evidence may also include rationale for use of necessary and unprotected physical input/output ports. (2) R2.1: "a patch management program" should be specified directly in R2 instead of R2.1 as the latter should only cover the tracking requirement of this program a patch management process doesn't "include" a patch management program, although the opposite could be true. (3) R2.3: Replace "exposed" with "adressed", as patches don't expose vulnerabilities. (4) HQT believes that timeframes given for R2: Security Patch Management (30 days) to make plan and R3.3 Update Malicious Code Prevention (35 days) should not be applied to all Medium Impact BES Cyber Systems but only to Medium Impact BES Cyber Systems with External Routable Connectivity. (5) Timeframe should be longer for Medium Impact BES Cyber Systems without External Routable Connectivity. Rationale: (a) because they are less reachable, they are less prone to an attack, that doesn't mean no protection is required, but it's lesser urgent than those with External Routable Connectivity; (b) without External Routable Connectivity, there is no easy technical means to automatically update security patches or signature files at such relative high frequency and mostly require manual intervention and travelling. By letting as drafted, Utilities will avoid implementing code protections that use signatures or patterns in Medium Impact BES Cyber Systems without External Routable Connectivity that could help to enhance the protection of those Cyber Assets even if those protections are not using the most recent signatures or patterns file. (5) We support the TFIST NPCC comment about CIP-007 R4 (6) Bug WITH Rational of R4 : we are difficulty to compliant with "immediate detection" (7) R4.3 : We consider it to be not required. 24hr delay is too much short and too many operational and temporary stuation may arise which come back to normal shortly after (24-48hr). Because of the distances it would be impossible to make a correction procedure in some cases in next calendar day (8) We support TFIST NPCC comment about R4.5
Individual
Thomas A Foreman
Lower Colorado River Authority
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

No
Yes
Yes
R 1.4: We suggest specifying that planned maintenance be excluded and apply the 99.9% requirement only to unplanned outages. R1.6: We suggest specifying that planned maintenance be excluded and apply the 99.9% requirement only to unplanned outages.
Yes
Yes
Yes
No
No
In R4.1, we recommend the addition of the term “Where technically feasible” for all of the sub-requirements.
In R5.2, change the wording as follows: The Responsible Entity must document enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). In M5.2, change the wording as follows: Evidence may include, but is not limited to, a listing of enabled default or generic account types in use. R5.3 - Remove the word “authorized” from this requirement. This could be interpreted as requiring an additional authorization for access to these shared or default accounts. R5.4 – Change wording to: Change default passwords where technically feasible.
Individual
Glen Sutton
ATCO Electric
Yes
Yes
Yes
Yes
Yes
Yes
No
R7.2 requires, for reassignments or transfers, unnecessary electronic and physical access is revoked by the end of the next business day. The time constraint seems to be excessive for internal moves. Consider increasing the time frame (i.e. 3 business days) for this requirement.
Yes
Yes
R1.1 does not list “Associated Protected Cyber Assets” in the applicability column but lists them in the requirements column. Associated Protected Cyber Assets should appear in the applicability column. CIP-005 no longer lists Associated Electronic and Monitoring Systems or Associated Physical Access Control systems for any of the CIP-005 perimeter requirements. It does not seem that this is a step forward in security for these systems. Question: Is it the intention of the SDT to not require perimeter security for Associated Electronic and Monitoring Systems or Associated Physical Access Control systems?
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Request for clarification: R4: It is unclear in R4.2 what is meant by “detected failure of 4.1 event logging”. Is this to be taken as event failures (unsuccessful login attempts) or failures of logging sources to correctly log events?
Individual
Ed Nagy
LCEC
Yes
No
Yes
No
No
Yes
No
Comment: 1) R7.2 Needs to state “interactive remote access” as in R7.1. Other electronic access such as user account and shared account requirements are covered in R7.4 & R7.5.
Yes
Yes
No
No
No
Comments: 1) 1.4 states that controls must be in place to monitor the physical security perimeter 24/7. Need to clarify what is meant by this. Does this mean monitoring of all access points or is there something more being implied? If the intent is to monitor the access points, this should be stated. 2) The requirement for 99.9% availability does not state a period which will lead to subjectivity and auditing issues. Is the intent for this to be a monthly or annual metric? 3) 1.5 no longer requires response to unauthorized access attempts but uses the term circumvention of a physical control. I think this is a positive change from a compliance perspective but leaves a gap that could be addressed through periodic PACS log review. 4)1.6 & 1.7 should be re-worded to focus on unauthorized access to the PSP containing the PACS as opposed to the PACS itself. Same comment on availability metric without period. 5) 1.8 Need to determine what is acceptable when it comes to identifying an individual. For example, is an access card and PACS log considered acceptable evidence? An auditor could interpret that a stronger level of authentication be required. Does including the individuals name on a sign in sheet constitute identification? 6) 1.9 Retention requirement of 90 days for logs will not match the audit period or expectation of auditors unless it is made clear that the solution and process be audited but that sampling can only be required within the retention period. Comments: 1) 2.1 The concept of continuous escorted access makes sense but should be more clearly defined. If the escort and visitor enter and exit the PSP at the same time, is this considered to be sufficient evidence of “continuous escorted access”? 2) 2.3 Retention requirement of 90 days for logs will not match the audit period or expectation of auditors unless it is made clear that the solution and process be audited but that sampling can only be required within the retention period Comments: Table R3 Many physical access control systems do not include any maintenance requirements so this should not be required. Testing needs to be more clearly defined. Is the expectation that each access control device be tested to ensure operation when presented with the appropriate credentials and that access is denied when presented with the incorrect credentials?
No
No

Yes
No
Yes
Comments: 1) R1.1 Should not include the term services as the clear intent with this requirement is to enable only the required logical network ports or sockets. If a service is network based, it is covered by the port/socket. Comments: R2 The patch management process should include a periodic review of all patch sources. (30 days is appropriate). The applicability review should take place within 30 days of the date the site/source review was executed. Using availability of the patch will be difficult to manage from a compliance and auditing perspective. For example, the monthly source review could take place on the first of the month; a patch is released on the second day of the month but is not identified until the first day of the next month. Is the patch release date available on the vendors site? Will it still be available at the time of the audit? Comments: R4.4 Retention of logs for 90 days makes sense but does not meet the expectation of auditors. The standards must differentiate between auditing of the systems and processes that are in place to meet the requirements and the retention of logs for the entire audit period. Auditors expect to be able to ask for logs for any day within the previous three years in most cases.
Group
NRG Energy Companies
Alan Johnson
Yes
No
Yes
No
Yes
No
No
In requirement R2, replace the reference to role-based training with training appropriate to job function. This will eliminate potential confusion about the term “role-based”, which is often associated with IT access control. Suggested wording “Each Responsible Entity shall have a cyber security training program, appropriate to job function, to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.”
In R7.2, replace “…that the Responsible Entity determines is not necessary by the end of the next calendar day following the reassignment or transfer.” with “…one calendar day after the determination that access is no longer needed.” Generally, there is no reason to believe a reassigned or transferred employee is a threat to security and there will be occasion where these employees will need temporary continuing access (e.g. training new employee in position). Please clarify what are user role categories in Requirement R6.6.
Yes
No
In Requirement 1.5, the Measure could be interpreted to prescribe the use of an Intrusion Detection System, however, such a system is not prescribed in a requirement. The references to IDS should be removed. Other systems and tools can be used to detect malicious communications.
1. The definition of Interactive Remote Access (or applicability of CIP-005-5 R2.1, R2.2 and R2.3) should be adjusted to reflect the exclusion of serially connected/non-routable/non-network connected devices. There is minimal/zero reliability benefit and significant cost associated with applying this requirement to all serially connected/non-routable/non-network connected devices that require remote access. Authentication when establishing connectivity to these systems is covered by CIP-005-5 R1.4 and provides the required cyber security. The cleanest way to correct this issue is to adjust the definition of Interactive Remote Access as follows: “All user-initiated access by a person employing a remote access client or other remote access technology using a routable protocol or dial-up. Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic

Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications." This definition is also found on Comment Form D, question 12. 2. From V5R1 Consideration of Comments – Definition of EAP section (this helps justify that Interactive Remote Access should not apply to serially connected/non-routable/non-network connected devices): "The SDT has not included serial, non-routable communications within the definition of EAP (other than with respect to dialup in CIP-005 R1.4). Dedicated serial communications are intentionally left out of scope, as the SDT believes it would be inappropriate for the standards to mandate a universal perimeter or firewall type security across all entities and all serial communication situations. There is no 'firewall' capability for a RS232 cable run between two cyber assets. Without a clear security control that can be applied in most every circumstance, such a requirement would just generate TFEs." 3. Suggest adding guidance to provide clarity on what is meant by a remote access client and/or remote access technology. In addition, how would two factor authentication be monitored for outside vendor support?
No
Yes
No
1. Requirements R1.4 and R1.6 call for 99.9% reliability of monitoring systems. The documentation required to prove this level of reliability would require extensive resources to satisfy. In addition, it's not clear if these requirements allow for alternate or redundant controls when the primary system is unavailable. For physical access controls, CIP standards should not be so restrictive as to limit options to only electronic methods. The 99.9% availability should be replaced with an allowance for documentation of system maintenance or outages with use of compensatory activities for monitoring. 2. In Requirements 1.5 and 1.7, an exception should be made for system maintenance or outages that last more than 15 minutes so they do not automatically create a violation. During a system maintenance activity such as required patching, the alerting system may not be functional for a period of more than 15 minutes. Unauthorized access may be detected, but not alerted during the maintenance activity. The performance of a required activity such as patching should not put a company in violation of the standard. Allow for documentation of system maintenance or outages and the use of compensatory measures, if required. 3. Requirement 1.7 should be revised from "within 15 minutes of the unauthorized physical access." to "within 15 minutes of detection."
No
Yes
Yes
No
No
1. The applicability of CIP-007-5 R2.1, R2.2, R2.3 and R2.4 to "Medium Impact BES Cyber Systems" should be limited to "Medium Impact BES Cyber Systems with External Routable Connectivity." The exclusion of cyber systems/assets with no routable connectivity will eliminate a significant burden of tracking and documentation requirements associated with serially connected devices that would have minimal impact to reliability. This is particularly burdensome for systems that are geographically dispersed and would require direct personnel interaction and physical access to each device to deploy patches to non-externally routable systems. 2. Modify Requirement R 4.1.3 from "detected and logged malicious software…" to "detected and logged malicious code…" 3. Eliminate requirement R4.1.4. The term "malicious activity" is ambiguous. 4. In Requirement R4.2, revise language to replace real-time with an actual target timeframe and refer to capability of the system rather than using the term technically feasible. Suggested language "Issue and alarm or alert, within 15 minutes, for security events that the Responsible Entity determines necessitate an alert, that includes, as a minimum, each of the following types of events where the BES Cyber System is capable:". Modify Requirement 4.2.1 to read "detected events per R4.1; and". 5. Requirement 4.3 is not consistent with 15 minute interval to address monitoring.
1. In Requirement R5.1, authentication should be done for accounts, not for user access. Suggest revising to read "Enforce authentication of accounts when accessing applicable Cyber Assets, where technically feasible". 2. Applicability for R5.2 should be the same as R5.3 – only applicable to external routable connectivity. Change "delegate" to "delegate(s)" as companies may choose to have one or

more delegates, depending on how they structure their program. Alternatively, consider removing R5.2 and R5.3 altogether as these requirements may already be covered by CIP-004 R6. 3. Requirement 5.5 –will this new requirement remove the CAN-017 requirements? 4. Requirement 5.6- this should consider account authorization not user accounts as explained in R5.1. 5. CIP-007-5 Part 5.7: Recommended change, “Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful login attempts, where technically feasible.” Please provide guidance on what is considered a suitable minimum threshold.
Group
Duke Energy
Greg Rowland
Yes
No
No
No
Yes
No
No
(1) Background section, “Applicability Columns in Tables:” section. Duke is concerned with the description for the bulleted item, “Associated Electronic Access Control or Monitoring Systems”. The last statement, “Examples include, but not are limited to firewalls, authentication servers, and log monitoring and alerting systems” is not part of the defined term of Electronic Access Control or Monitoring Systems. Duke suggests removal of the last statement as an apparent prescriptive list of examples may not always be true. Firewalls may exist which don’t control access to the ESP(s) or BES Cyber Systems, so they shouldn’t fall into consideration of this applicability. NOTE that this comment applies to ALL CIP Standards CIP-002-5 through CIP-011-5. (2) Requirement R2.2. The requirement states “Training content on the cyber security policies protecting the Responsible Entity’s BES Cyber Systems”. This does not match the applicability section of the R2.2 as other types of systems are also included such as Associated Physical Access Control Systems. This makes it very confusing as to what the requirement is actually applicable to. Duke suggests not repeating any terms used in the applicability section within the language of the actual requirement and instead using a phrase such as “protecting the Responsible Entity’s applicable Cyber Assets as listed in the “Applicable BES Cyber Systems and associated Cyber Assets” section of R2.2”. NOTE that this comment applies to ALL CIP Standards CIP-002-5 through CIP-011-5. (3) Requirement R3.1. Duke suggests that the phrase “and documentation” be removed from the requirement. This phrase is redundant to the requirement R2 which requires the documentation of the training needed. (4) Requirement R3.1 and R3.2. Duke is concerned with the lack of clarity as to who is to receive the training as required by R3.1 and R3.2. Currently, no language exists within the requirement as to who needs to receive this training and Duke does not feel that is acceptable. With the current wording, one could simply train a single individual before granting an entire group of people access to BES Cyber Systems. Duke does not believe that is the intent of these requirements and believes the standard should be specific as to who is required to receive the training. (5) Requirement R4.1. Duke is confused by the term “initial” in this requirement. What is the drafting team’s intent of this word? Is the intent that even those individuals who are covered under an existing PRA for the previous versions of CIP would be required to get another “initial” PRA prior to implementation of version 5? Duke feels that would be unnecessarily burdensome and costly. Duke is also concerned by the implications of demonstrating “initial” PRA’s for compliance. Would Duke be expected to retain evidence for individuals from audit to audit, to continue to prove that each individual had an “initial” PRA, even if it was conducted 10 years ago and a new 7-year has been conducted since? The wording of the requirement would seem to suggest this. (6) Requirement R4.2. Duke suggests modifying the last phrase of “the subject has, for six months or more” to “the subject has, for six consecutive months or more” to further clarify that the time duration only makes sense if it is assessed consecutively. (7) Requirement R4.2.1, R4.2.2 and R4.2.3. These statements need to be assessed as a list of “OR”s. The current wording suggests that only the locations that meet all 3 criteria need to be reviewed in the process. (8) Requirement R4.4. Duke suggests removing the requirement R4.4. Duke does not believe this statement should warrant its own requirement. As currently drafted, this would require an entity who has no contractors or service vendors with access to still have a process or criteria for verifying that the PRAs are performed in

accordance with R4.1 to R4.3.
(1) Rationale for R6. Duke suggests that the last statements in the rationale section be incorporated into the language of the actual requirements. The statements, “For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R6 are not applicable. However, the Responsible Entity should document such configurations”. These statements are critical to meeting compliance with R6 and need to be incorporated into the language of the requirements as opposed to existing solely within the rationale section. (2) Requirement R6.1. Duke suggests that the phrase in this requirement be modified to read, “Designate one or more individual(s), by name or by role, to authorize:”. This will give entities the flexibility in designating a job role with the authority to make specific changes without having to change its documented designees every time there is a person entering or leaving a role. (3) Requirements R6.2, R6.3, and R6.4. Duke suggests that the phrase “Responsible Entity” within the requirement be replaced with “individual(s)”. This clarifies that the authority lies specifically within the individuals who have been delegated that function and that the Responsible Entity is not itself directly involved in the authorization process. (4) Requirement R6.4. Duke is concerned with the existing language of this requirement and that the physical locations where electronic BES Cyber System Information would also have to be restricted access areas. These locations, may be off-site, or may not be controlled by the entity. Duke suggests the splitting of R6.4 into two different requirements. The first requirement should require the entity to identify the repositories that store either physical media containing BES Cyber System Information (paper copies) or the electronic storage of BES Cyber System Information. The second requirement should be the authorization of access to only those designated repositories that have been identified by the entity. (5) Requirement R6.6. Duke would like to propose the following rewording of this requirement to “For electronic access, verify at least once each calendar year, not to exceed 15 calendar months, that the user accounts, user account groups, or user role categories on applicable Cyber Assets, and their specific, associated privileges are correct and are those the Responsible Entity determines necessary for performing work functions.” The existing wordings use of the word “all” could be misinterpreted that this requirement must be met for more devices than those listed in the applicability section of the requirement. (6) Requirement R7.2. Duke proposes the following rewording of this requirement to “For reassignments or transfers, revoke the individual’s electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the notification of reassignment or transfer.” The inserting of the phrase “notification of” emphasizes that the Responsible Entity can only act as fast as it receives appropriate internal notification of a change requiring the revocation of access. (7) Requirement R7.5. Duke proposes the following rewording of this requirement to “For termination actions, reassignments, or transfers, change passwords for shared account(s) known to the user within 30 calendar days of the notification of termination action, reassignment, or transfer of the user. If the Responsible Entity determines and documents that CIP Exceptional Circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the CIP Exceptional Circumstances”. The inserting of the phrase “notification of” emphasizes that the Responsible Entity can only act as fast as it receives appropriate internal notification of a change requiring the need to change passwords. The replacement of the phrase “extenuating operating circumstances” with “CIP Exceptional Circumstances” is meant to use the specific defined term created for an event like this. (8) Application Guidelines Section for R7. Duke is concerned with the scenario of “death” appearing as a termination action that needs to follow the requirements in R7 for immediate initiation of access revocation. Duke recommends that the Guideline section clarify that the “effective date and time of the termination action” in the “death” scenario not to begin until the Responsible Entity is notified.
No
No
(1) Background section, “Applicability Columns in Tables:” section. Duke is concerned with the description for the bulleted item, “Medium Impact BES Cyber Systems at Control Centers”. The phrase “located at a Control Center” is not consistent with the application of CIP-002. CIP-002 requires the identification of BES Cyber Systems “associated” with a Control Center, not just those physically located at a Control Center. Duke suggests using the word “associated” here instead of “located at”. NOTE that this comment applies to ALL CIP Standards CIP-002-5 through CIP-011-5. (2) Background section, “Applicability Columns in Tables:” section. Duke is concerned with the description for the bulleted item, “Medium Impact BES Cyber Systems with External Routable Connectivity”. The last sentence states that “This also excludes Cyber Assets in the BES Cyber System that cannot be

directly accessed through External Routable Connectivity". This is confusing. CIP-002 allows for the grouping of Cyber Assets into Cyber Systems such that the applicability to the system can be analyzed to the whole and protections can be applied accordingly, as opposed to each individual Cyber Asset. Duke recommends that this theme be carried consistently throughout the each standard and once a Cyber System is grouped, it should not have to be broken up to assess individual Cyber Asset impact. In this circumstance, either the system itself has External Routable Connectivity or it doesn't, and protections can be applied to the system as a whole. NOTE that this comment applies to ALL CIP Standards CIP-002-5 through CIP-011-5. (3) Measure 1.1. This measure is inconsistent with the respective Requirement R1.1. Duke suggests striking the phrase "uniquely identifiable" as there is no requirement to uniquely identify each Cyber Asset within each ESP. This comment assumes that corrections are made such that the Requirement R1.1 is only applicable to the applicability section and not to the words currently stated within the requirement. (4) Requirement 1.5. The requirement here needs to be clarified as to where the entity needs to be able to detect malicious communications. It is Duke's understanding that the intent of this requirement is to detect malicious communications that originate outside the ESP and attempt to transverse the boundary of the ESP through one of the applicable types of Electronic Access Points. If this is true, then the requirement should be reworded to say, "Have a method for detecting malicious communications originating on a Cyber Asset outside of the Electronic Security Perimeter that attempts to transverse the boundary of the Electronic Security Perimeter through one of the applicable types of Electronic Access Points".

(1) Requirement R2. Duke recommends striking the phrase "where technically feasible" and inserting it at the end of every sub-requirement for R2. In previous versions, it is not very clear that statements within a main requirement effectively flow down to the sub-requirements. In addition, it is difficult to determine why creating a process would not be technically feasible as the current language suggests. (2) Requirement 2.1. Duke recommends rewording the requirement to "Utilize an Intermediate Device such that the authorized user initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset". Duke suggests replacing the term "Cyber Asset" with "authorized user" as it more closely aligns with the proposed definition of Interactive Remote Access as originating from a human and not from an automatic process that may be running on a Cyber Asset. (3) Requirement 2.2. Duke recommends striking the phrase, "in order to protect the confidentiality and integrity of each Interactive Remote Access session". This phrase is opinion as to what purpose encryption could serve and not integral to the requirement. Thus Duke recommends removing it. (4) Requirement R2.3. Duke recommends rephrasing the beginning portion of this requirement to read, "Require multi-factor authentication to the Intermediate Device for all Interactive Remote Access sessions". This wording change clarifies that multi-factor authentication is only needed at one point during the process and not to every element needed to support Interactive Remote Access.

No

No

Yes

(1) Requirements R1.2 and R1.3. The current wording of these requirements can be read to mean that ONLY those with individuals who have authorized physical access can enter a PSP. This would specifically exclude visitors from ever entering the PSP, even if allowed by another requirement. Duke suggests appending the requirements with the following language, "This requirement does not apply to visitors who may enter a Physical Security Perimeter in compliance with CIP-006-5 R2.". (2) Requirement R1.3. Duke recommends replacing the phrase "controls" with "authentication methods". This change allows entities the flexibility of utilizing two or more access authentication means that may exist with the same control. For example, a badge reader that has a keypad for a user to also enter a PIN number may be misinterpreted as a single control since it resides within the same device. This clarifies that this type of device is multiple authentication methods and therefore in compliance with the requirement. (3) Requirement R1.4. Duke is concerned with the current language of this requirement. The current wording suggests that the entire Physical Security Perimeter must be monitored for unauthorized access. This could incorrectly be interpreted to mean that the walls/ceiling/floor/etc. of the perimeter themselves must be monitored. The usage of the 99.9% availability term is also very confusing, as there is no guidance as to how this can be achieved or to what the availability is to be measuring (over what time period? to any one device? to the system as a whole? etc.). Duke recommends that this requirement be written more similarly to CIP-007-5 R4.3 where alerts need to be generated when monitoring tools are not available. Also enabling the use of

an alternative measure to support monitoring while the primary tool is unavailable will aid the entities in meeting availability concerns. (4) Requirement 1.5. Duke recommends replacing the term “circumvention” with “access”. Duke feels that the word access more adequately reflects the concern of being alerted to a situation only once actual access is obtained, not necessarily just when a control is circumvented (in the possible instance of circumvention without anyone actually gaining access to the restricted area). (5) Requirements 1.6 and 1.7. Duke recommends removing requirements R1.6 and R1.7. There is no requirement requiring Physical Access Control Systems to be within physically protected boundaries such as PSP’s, thus having controls to monitor and alert to unauthorized access are inconsistent with the remainder of CIP-006-5. (6) Requirement R1.8. Duke recommends removal of the parenthetical, “through automated means or by personnel who control entry”. This phrase is unnecessarily prescriptive and the requirement should allow the entities to log entry with whatever vehicle they determine is appropriate for their situation. (7) Requirement R2.1. Duke recommends rewording the parenthetical to “individuals who are not authorized for unescorted physical access). It is not necessary for the requirement to state that visitors have to be known or be guests. The requirement reads more clearly when visitors are acknowledged to be anyone who does not have authorized access.
No
No
No
No
No
(1) Requirement 2.2. Duke suggests that 30 days be changed to 35 days to allow for monthly patch cycles and increase efficiency. (2) Requirement R2.3. The change rationale section includes a lot of good and detailed explanation that may be better served within the actual requirement. Duke recommends that the wording be re-evaluated to determine if any of the language can be moved to the requirement to clarify the drafting team’s intent. (3) Requirement R2.4. Duke recommends striking this requirement. The need to implement the plan is redundant with the combination of the main requirement R2 requiring that entities implement the processes that are developed to meet the sub-requirements, in this case R2.3. The only difference here is the inclusion of “CIP Exceptional Circumstances” which should be moved to the language of R2. (4) Requirement R3.3. The requirement here to update “protections that uses signatures or patterns” incorrectly assumes a specific type of technology is being used to meet compliance with CIP-007 R3. If an entity does not employ a technology that uses signatures or patterns for malicious code prevention, that entity would still have to have a documented process to meet compliance with CIP-007 R3.3 (per language in the main requirement CIP-007 R3). (5) Requirement R3.3. Duke believes that the 35 calendar day update is too prescriptive and recommends a 95 calendar day update instead. Duke feels that this update period is better suited to the industry environment. (6) Requirement R4.1. Duke recommends rewording the first part of the requirement to read, “Log events for identification of, per device capability, each of the following types of events:”. This clarifies the drafting team’s intent that TFE’s are not required in this sub-requirement, if the device is not capable of detecting or logging the type of event found in the sub-sub-requirements. (7) Requirement R4.2.1. Duke recommends that the term “malicious activity” be replaced with “Cyber Security Incident”. Duke feels Cyber Security Incident better reflects the intent of the drafting team. If this is not the intent, Duke recommends the drafting team clarify the term “malicious activity” as its usage here is very vague and it is unclear how, if at all, it relates back to the types of events in R4.1. (8) Requirement R4.3. Duke suggests rewording this requirement to say, “Activate a response to human detected logging failures before the end of the next calendar day after discovery”. Duke believes that this wording allows the proper flexibility to the entity to begin the clock by which they have to activate a response, no sooner than they become aware of the problem. (9) Requirement R4.4. Duke suggests rewording this requirement to say, “Retain BES Cyber System [sic] logs of events identified in Part 4.1 for at least…”. This wording change clarifies that all logs identified in R4.1 must be retained instead of requiring the entity to assume which ones in R4.1 may actually be related to security events. (10) Requirement R4.5. Duke recommends that the drafting team put additional clarity within the requirement. The current wording is too vague for an entity to determine what is an acceptable summarization or sampling size. Although the Application Guidelines section references a NIST standard for more information, Duke feels the requirement should either be more prescriptive, or clarified that the entity is allowed to come up with its own criteria by rewording the requirement to say, “Review a summarization or

sampling of logged events deemed appropriate by the entity, at a minimum every two weeks to identify undetected Cyber Security Incidents". (11) Measure 4.5. Duke recommends striking the words, "signed and" from the measures section. Suggesting that signed evidence is needed is inappropriate. Having documentation that is dated showing the review should be adequate enough to demonstrate compliance.
(1) Requirement R5.1. Duke requests that the drafting team review the applicability within R5. This requirement does not align with the requirements in CIP-004 to track/manage those with user access. (2) Requirement R5.2. Duke recommends removing this requirement in its entirety. Duke does not believe having CIP Senior Manager authorization of default accounts provides any additional security benefit, nor is it required per an Order 706 directive. (3) Requirement R5.3, Change Rationale. The statement, "Added "authorize" access to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement" is too important to leave totally within the Change Rationale section. Duke requests that the drafting team incorporate this verbiage into the requirement as the current word "authorize" does not carry this message on its own clearly. (4) Requirement R5.4. Duke suggests beginning this requirement with "Change known default passwords". Recent news has shown that OEMs often will not disclose the existence of default accounts and the entities should not be held liable when this is the case. Duke also recommends that the drafting team provide clarity on what types of account passwords need to be changed, and that this requirement should only be addressing user or individual accounts and not system accounts. (5) Requirement R5.5. Duke questions the need for a TFE within this requirement. The only circumstances that would warrant a TFE would be identical across the industry for the same devices. Duke does not understand the value that this serves. Duke believes that TFEs should only be needed in unique circumstances and not when a widely-used device is unable to meet the requirements. Duke recommends that the drafting team rework the language within this requirement to not require a TFE, but only that the entity document where passwords cannot be changed due to technical limitations. (6) Measure R5.4. Duke suggests that the phrase "when new devices are deployed" from the first bulleted item. Duke feels that this is redundant, and potentially contradictory, to the implementation plan which describes when an entity must meet compliance with a requirement. (7) Measures R5.5 and R5.6. Duke believes that the second bulleted item should be removed in its entirety. Suggesting that individual attestations would be a good way to demonstrate compliance that the individuals have a password that conforms to policy is inappropriate. Attestations are cumbersome in large organizations and provide no more evidence of compliance than simply providing the password procedure/policy that individuals must conform to. Duke suggests replacing this bullet with the ability to present the procedure/policy as a means to demonstrate compliance. (8) Requirement R5.7. Duke suggests striking this requirement in its entirety. The first means of meeting this requirement, technically limiting the number of unsuccessful authentication attempts actually opens up a vulnerability to a malicious attack by means of a DOS attack. The latter half of the requirement may be partially redundant to requirement CIP-007 R4.2 and may not be technically feasible on all devices. Duke does not believe there is a significant enough increase to security to introduce this requirement and believes it should be removed as it is not specifically required per Order 706.
Individual
Martyn Turner
LCRA Transmission Services Corporation
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

No
Yes
Yes
R1.4: We suggest specifying that planned maintenance be excluded and apply the 99.9% requirement only to unplanned outages. R1.6: We suggest specifying that planned maintenance be excluded and apply the 99.9% requirement only to unplanned outages.
Yes
Yes
Yes
No
No
In R4.1, we recommend the addition of the term “Where technically feasible” for all of the sub-requirements.
In R5.2, change the wording as follows: The Responsible Entity must document enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). In M5.2, change the wording as follows: Evidence may include, but is not limited to, a listing of enabled default or generic account types in use. R5.3 - Remove the word “authorized” from this requirement. This could be interpreted as requiring an additional authorization for access to these shared or default accounts. R5.4 – Change wording to: Change default passwords where technically feasible.
Individual
Jianmei Chai
Consumers Energy Company
Yes
Yes
Yes
Yes
Yes
Yes
No
R7 – Please provide better definition of “schedule”, “immediate”, and “revocation”, and better examples for each subject. R7.2 - We disagree with the current language because it can unnecessarily restrict the entity from having sufficient transition time between the person leaving and the new person replacing them. The entity should be allowed to specify what their local process is, and timelines, for handling these kinds of revocations to ensure they can plan for continuity of operations properly.
Yes
Yes
Yes
Yes
Yes
No
Yes
Yes
Yes
No

R1 – Please provide justification to include physical ports.
R5 - The length of time between password changes in this requirement are excessive. Passwords should be changed far more frequently. Recommend at least quarterly (at least once every 90 calendar days).
Individual
Kayleigh Wilkerson
Lincoln Electric System
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
LES recommends the Applicability columns for the CIP-005-5 Table R2 be revised to exempt non-routable protocol. Suggested wording includes: "High Impact BES Cyber Systems with External Routable Connectivity" and "Medium Impact BES Cyber Systems with External Routable Connectivity".
No
Yes
Yes
Yes
No
Yes
[R1] In all applicability columns for CIP-007-5 Table R1, where medium impact facilities are included, recommend including “with external routable connectivity”. [R2] LES is concerned whether including the monitoring of all installed cyber asset manufacturers is feasible. [R3 – R3.3] should be revised to account for the differing methods that can be utilized as part of R3.1. As an example, per R3.1, a company can use policies as a method to deter, detect, or prevent malicious code. However, if a company were to adopt policies as their method, R3.3 would not be applicable as there would be no malicious code to update. [R4.1], the Measure includes the phrase “is capable of detecting”. LES supports this phrase and believes it should be incorporated into the Requirement so companies are not required to replace equipment. Additionally, the “as a minimum” included in R4.1 seems to contradict the understanding of the Measure.
Individual
Joe Petaski
Manitoba Hydro
“BES cyber assets” should be changed to “applicable cyber assets” because the applicability column includes Associated PACS and Associated EACMS.
In Part 1.1 table, “Associated Protected Cyber Asset” is missing. Given that CIP-006-5 doesn’t address that all cyber assets within ESP shall reside within PSP, is it intent that the Protected Cyber Asset within ESP can reside outside PSP?

Group
Arizona Public Service Company
Janet Smith
Yes
No
Yes
Yes
Yes
Yes
No
AZPS recommends moving the statement “Based on their role, some personnel may not require training on all topics” from the rationale for R2 into the appropriate sub-requirements. The intent is to make clear to an auditor that not all topics are required for all roles – and to put that language in the requirements themselves. AZPS recommends changing the words “security controls” in the table 2.2 Measures to “cyber security policies”. AZPS recommends modifying the table 2.3 Measures to make them consistent with those in the table 2.2 Measures. AZPS would like clarity added to the following statement in the table 2.10 Requirements “Training content on risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets”. AZPS would like specificity in the table 2.10 Measures to help identify what must be covered in the training materials under requirement 2.10 to be auditably compliant.
AZPS recommends changing the words “next calendar day” in the table 7.2 Requirements to “one calendar week”. AZPS believes a timeline as restrictive as the next calendar day does not provide any value to the overall security posture. Someone transferred to another department, who at one time had a given level of access, does not constitute an immediate threat and in fact having to react in such a manner for the sake of compliance will potentially result in decreased system reliability. Additionally, this is a more stringent requirement than the one for terminations since terminations give additional time for the full revocation of individual user accounts outside of remote access and physical access. Reassignments and transfers are a significantly lower risk than terminations. AZPS recommends adding the words “for reassignments, or transfers” to the table 7.4 Requirements in order to bring the requirements for reassignments and transfers into alignment with the requirement for terminations.
Yes
Yes
No
Yes
Yes
AZPS would like specificity added in the table 1.4 Requirements to define how 99.9% availability should be calculated.
Yes
No
Yes
Yes
Yes
AZPS recommends changing the word “processes” in the CIP-007-5 R2 and M2 statements to “program” in order to match the table 2.1 Requirements.
Individual
Michael Schiavone

Niagara Mohawk (dba National Grid)
Yes
No
Yes
Yes
Yes
Yes
Yes
Regarding R2, we do not believe that role based training is necessary. The personnel performing the job functions are familiar with the various controls due to their job requirements. General training in CIP, as required under the current version, is all that should be required.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Yes
The intent of 4.1 as written in the Guidelines and Technical Basis section is inconsistent with the requirement. The guidance states that “It is not the intent that if a device cannot log a particular event that a TFE must be generated”. If the intent is to not be out of compliance when a device cannot log certain events, it should be stated as such in the requirement.
Individual
Michael Jones
National Grid
Yes
No
Yes
Yes
Yes
Yes
Yes
Regarding R2, we do not believe that role based training is necessary. The personnel performing the job functions are familiar with the various controls due to their job requirements. General training in CIP, as required under the current version, is all that should be required.
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
No
Yes
The intent of 4.1 as written in the Guidelines and Technical Basis section is inconsistent with the requirement. The guidance states that “It is not the intent that if a device cannot log a particular event that a TFE must be generated”. If the intent is to not be out of compliance when a device cannot log certain events, it should be stated as such in the requirement.
Individual
Jonathan Appelbaum
United illuminating Company
Yes
Yes
Yes
Yes
Yes
Yes
Yes
UI concurs with EEi Consensus comments. In addition for R1 UI suggests explicitly stating that this program does not apply to contractors and vendors not directly employed by the Responsible Entity. For R3 The Drafting Team should include a solution for SCADA Support Vendors that require remote access to provide support to the SCADA system, for example ABB support personnel supporting an ABB SCADA environment. It is inefficient to require these vendors to complete every Responsible Entity’s training program. The Draft Standard may provide enough flexibility by allowing an Entity to declare the role of SCADA Support Vendor as requiring no training provided. If the SDT agrees that the flexibility exists then we suggest adding into guidance the concept that SCADA support personnel of the OEM SCADA environment are allowed to forego the Responsible Entity’s training program when performing remote access support functions.
UI concurs with EEi Consensus comments.
Yes
Yes
UI concurs with EEi Consensus comments.
UI concurs with EEi Consensus comments.
No
Yes
Yes
UI concurs with EEi Consensus comments.
Yes
Yes
Yes
Yes
Yes
UI concurs with EEi Consensus comments.
UI concurs with EEi Consensus comments.
Individual

Alice Ireland
Xcel Energy
Yes
Yes
Yes
Yes
Yes
No
No
1) CIP-004-5 R2.2-2.10 contains elements which can comprise a training program. If role-based training is required (as indicated by R. 2.1), can a Responsible Entity choose from those elements to create a training program for different roles? Or must all roles identified receive some training from each of the elements in R. 2.2-2.10? If all roles must receive some training for each of the elements in R. 2.2-2.10, what is the value of having role-based training? 2) If all roles must receive some kind of training on all elements of R. 2.2-2.10, we would recommend adding the following language to each of the sub-requirements: Training content should be provided to each identified role based on the level of understanding needed for each. Each identified role must [or must not if Responsible Entities can choose which elements to include] be provided training on this element.
1. The Rationale implies that we need to have our Sr. Mgr. delegate authority to individuals responsible for approving access. Is that the case? 2. The Rationale notes access must be addressed by specific Cyber Asset. Does that mean we need to review/approve access by CA not by location or application/system? 3. R6.2 and R6.3 remove 'for performing assigned work functions' as it is unclear how that would be determined, and subject to different interpretation by the entity and the region. 4. R6.4 remove 'physical and' because it imposes a requirement to create physical access controls and authorization processes to an office that may have a printout of Cyber System Information. 5. R6.7 remove reference in Measures 2 and 3 to 'privileges' as 'privileges' are not mentioned in the requirement. 6. R6.7 clarify Measure 1 – is a 'listing of authorizations' the same as a current list of those with access? 7. R7.2 Rationale and Guideline both indicate that the Review needs to occur by the end of the next day; however the Requirement says that the access must be removed by the end of the next day. We propose allowing 7 days to perform the review, and when access is determined to no longer be required, it be removed by the end of the next business day after that determination is made. It is not feasible to review and revoke access by the next calendar day particularly when you factor in weekends and holidays. 8. R7.3 is not feasible nor is it necessary to act that quickly when we have already disabled remote access (network accounts). A user cannot access a file share without a valid network account. Given the low risk, this timeline is particularly out of line with that imposed in R7.4 which allows 30 days to disable access to CAs. We propose a similar time – 30 days to remove access to Cyber System Information. 9. The Measure for 7.5 does not indicate what would be appropriate evidence for the "extenuating operating circumstances". If documentation is required, the measure should state "Additional documentation for 'extenuating operating circumstances' consists of an overview of the situation, approval by the CIP Senior Manager or delegate, and attestation that the situation has been addressed" or other concrete examples.
No
Yes
The FERC order 706 states that there needs to be an additional level of perimeter protection, but an IDS does not provide protection, just detection. An IPS would allow for protection of malicious software but would require a large investment in personnel and hardware.
None
No
No
No
1) CIP-006-5 R1 states: "Each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.". Xcel Energy requests

clarification regarding the definition of the need for a Physical Security Plan. As stated, it may be interpreted to say that it pertains to each singular cyber asset, system Electronic Access Control or Monitoring Systems and Physical Access Control Systems. Is it NERC's intention to require each entity to provide a singular Physical Security Plan for the above mentioned assets as a single asset? If not, Xcel Energy recommends the language be modified to reflect the need for a Physical Security Plan to include the parts of CIP-006-5 R1, similar to what is in the existing standards. 2) CIP-006-5 R1.3, Xcel Energy seeks clarification regarding additional protection of requiring "two or more different physical access controls". This requirement could result in additional TFEs and add additional management to both the industry and entities. Additionally, most Critical Facilities already contain layered security perimeters, the additional cost of having two factor authentication appears to outweigh the benefit. 3) CIP-006-5 R1.4: the "99% availability" seems both arbitrary and hard to prove (in fact, there are no examples provided in the Measures column for how to prove you have this level of availability). The phrase "with 99.9% availability" should be replaced with language along the lines of "with outages of not more than X per year and of no more than Y minutes duration each allowed." 4) CIP-006-5 R1.7 states, "Issue and alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan…". Xcel Energy seeks clarification on the word "personnel". Could this be a department or does the requirement specify/intend to have entities name each individual? 5) CIP-006-5 R2.1 Measures states, "Evidence may include, but is not limited to, language in a visitor control program…". Xcel Energy seeks clarification concerning a visitor control program. Is it NERC's intent to have an independent visitor control program or is it sufficient to have the language contained within the Physical Security Plan or other procedure? 6) CIP-006-5 R3.1 states, "Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly." The definition of Physical Access Control System does not include the locally mounted hardware. Is it NERC's intent of this requirement to demonstrate maintenance and testing of both the Physical Access Control System and the locally mounted hardware or is the intent that the test of the locally mounted hardware would exhibit that the Physical Access Control System is functioning? Additionally, the Severe VSL for R3 states, "The Responsible Entity has not documented and implemented a maintenance and testing program for Physical Access Control Systems. (3.1)" If the intent of the requirement is to test the locally mounted hardware and the Physical Access Control System(s) it is suggested the language be changed to: "Maintenance and testing of both the Physical Access Control System(s) and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly." 7) For the measures of CIP-006-5 R3.1, Xcel Energy seeks clarification of what evidence would constitute a "dated maintenance record"? Would a manually created documentation outline illustrating what assets were tested be sufficient or is the electronic record from the Physical Access Control System required? 8) In the Compliance section it states, "The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit. Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer." Since this definition exists in the Standard, is it necessary to indicate on the Requirement level the minimum amount of time to retain records? For example, R1.9 and R2.3 specify retention for 90 calendar days, R3.2 states 12 calendar months.
No
No
Yes
Yes
Yes
1) R1. Not all operating systems will give the RE the ability to disable physical I/O ports, such as USB ports, based upon type usage. Typically, USB ports are disabled by grouping and not by function. If a USB Keyboard and Mouse are used, but other devices are not allowed, then there may be technical feasibility to implement these restrictions. 2) R2. We would dispute the need to create a document every time a patch is released, but rather have a standard process for dealing with released patches

and then document any exceptions to the stated policy. 3) R4.2.1: replace “detected malicious activity” with “detected Cyber Security Incident” 4) R4.5: replace “undetected Cyber Security Incidents” with “potential Cyber Security Incidents not previously identified or detected.”
None
Group
PNGC Comment Group
Ron Sporseen
Yes
Yes
Yes
Yes
Yes
Yes
R1.4 – The requirement for 99.9% availability for physical security perimeter controls is problematic due to requiring tracking of availability without defining a time period for determining the percentage. The SDT needs to revisit this requirement to reduce the complexity of tracking such availability and to create a clear requirement on this issue.
Yes
Yes
Yes
Yes
Yes
Individual
John Souza
Turlock Irrigation District
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Individual
Rich Salgo
NV Energy
Yes
Yes
Yes
Yes
Yes
Yes
No
The only disagreement is with R7, specifically part 7.2, as we feel it is impractical to expect that the access requirements of a transferred employee will be assessed in every case within 24 hours of the transfer. We must realize that the employee in question retains the same amount of training and personnel risk assessment before and after the transfer; nothing about the worthiness for access changes as a result of the transfer. We understand the predicament that the SDT has in satisfaction of the Commission directive in Order 706 Paragraph 460 and 461, and believe that the SDT has found an innovative way to accomplish the directive. We simply register our comment about the lack of practicality of the requirement.
Yes
Yes
No
Yes
Yes
In Requirement R1, parts 1.4 and 1.6, rather than specifying a 99.9% availability requirement, we suggest that the requirement be restructured to instead require the implementation of alternate methods to substitute for the loss of any monitoring functionality. Also in Requirement R1, part 1.7, we note that it may be difficult to demonstrate that 15 minutes did not elapse prior to receipt of an alarm, particularly since the alarm is the only data that is captured for evidence. One would assume that the alarm is coincident with the event, but is that sufficient for evidentiary purposes?
Yes
Yes
Yes
Yes
Yes
Individual
Chris Higgins on behalf of BPA CIP Team
Bonneville Power Administration
Yes
Yes

Yes
No
Yes
Yes
No
Regarding R4 – BPA believes the assessment of residence, schooling and employment falls outside the boundary of a criminal history check. Verification of schooling, employments and residence is typically a function of employment eligibility verification and should not be considered a part of the assessment processes for risk associated with access to sensitive areas. Such risk analysis is typically based on character, trustworthiness and any revealed pattern of adverse behavior, which are only able to be assessed in reviewing the criminal history check.
Regarding R7 and R7.1 – BPA believes the requirement is for, “All Terminations” and the requirement does not recognize that not all Terminations are adverse. Contract completions and other similarly non-threatening or non-adversarial ends to employment should not be lumped in with adversarial Terminations or Terminations that create or result from a security risk. BPA believes that the RE needs to have the flexibility to determine whether they feel there is a threat or not. Twenty –four hours should not be applied where there is no threat/risk Regarding R7.2, R7.3 – BPA believes that the, “By the end of the next calendar day” is too aggressive. Essentially it is the same as within 24 hours. When persons are reassigned or transferred it can take a number of days to determine whether they will continue to need the access they previously had. A reassignment or Transfer triggers a series of events such as contact with the loosing and gaining managers, verification of the move, review of the position requirements etc, which will result in a determination of whether the access privileges are necessary or not. There are times when this process of determination may take a week. The previous requirement of 7 days was reasonable and adequate; therefore, BPA suggests returning to that number. R7.4 – BPA believes that, "Revoke individuals users accounts ON BES Cyber Assets" should be changed to "Revoke individuals access TO BES Cyber Assets." BPA believes that this is an important distinction because most field BES Cyber Assets do not have individual user accounts. In the utility field environment many brands and models of devices are being used. For those that do have individual user account capability, they are often not used because most BES Cyber Assets cannot be centrally managed. Since the process of revoking access privileges on each device can take up to a year or longer because it requires a site visit to each asset and for system with a significant number of assets which also covers a large geographic area that effort in combination with the necessary equipment outage to make the change introduces new reliability risks to the BES. It is more common for BPA field organizations to place other access control devices in front of such field devices. These other devices can be centrally managed. So access is controlled to the device rather that by the device itself. Field Example: Protective Relays – Most do not have individual user accounts. Many also do not have the capability to allow central access control management. Because they don't have user accounts the only way to revoke access on the devices is to change the passwords for all access levels. This means logging on to many hundreds to possibly thousands of relays to change passwords. Because access to the relays to change passwords opens the relay at the change level, it presents an increased risk to the BES because it requires a physical equipment outage to make the change resulting in many more outages impacting potentially the state of the BES and once access is granted, one can change any type of setting on the relay . It certainly could not be accomplished in 30 days. Access can be revoked to these assets by revoking the Central Electronic Access Privileges that allow access through the access control devices to the assets. This coupled with physical access revocation (both of which can be centrally managed) provides complete revocation of access to the assets. This can be accomplished a very short time. BPA suggests changing CIP-004 R7.4 to: “For Termination actions, revoke the individuals user accounts on BES Cyber Assets…” to, for termination actions, revoke the individuals access to BES Cyber Assets…” Regarding R7.5 – Most Protective Relays use Access Levels and Codes or Passwords. These are shared among the crews that support the assets. Again as with 7.4 above, this can be hundreds to thousands of devices. Again, BPA believes that this may not be accomplishable within the 30 day time frame.
No
No
BPA finds that there is still confusion regarding how the requirements apply to serial devices. This isn't fully answered in the requirements themselves or the guidance. BPA takes the guidelines for R1

on Page 22, Paragraph 2 to mean that direct serial connected devices are not included in this standard, but further clarification is required. BPA is still uncertain about the intent of the standard in regards to securing serial devices. BPA also understands the requirements as stating that currently no EAPs and thus no ESP boundaries can be defined based on serial communications. This would mean that serial devices or serial communications equipment connected to routable networks within an ESP could possibly extend an ESP far outside the boundaries of a defined PSP. BPA requests that the requirements be changed to address this problem. It is acceptable industry practice to connect control centers to substations and other field equipment using serial communications. The way that CIP 005-5 is currently written could be taken to mean that a control center ESP connected through serial links to various field sites would actually extend the ESP. This could create very large network areas that would have to be compliant. There should be some way to define where an ESP's boundaries are when dealing with serial communications. Not knowing the intent of the SDT, BPA can offer no suggestions. BPA requests that the standard provide examples, if any, of where serial devices would be in scope as well as examples of where serial devices could be used where they are out of scope. Regarding R1.1: The "Applicable BES Cyber Systems and associated Cyber Assets" should use "Medium Impact BES Cyber Systems with External Routable Connectivity" instead of the broader "Medium Impact BES cyber systems". In addition, it should be made clear in the standard and not just the guidelines that the requirement applies only to Cyber Assets that use a routable protocol. BPA suggests adding "BES Cyber Assets or Associated Cyber Asset that do not use a routable protocol do not have to reside within a routable ESP" to the end of the requirement. Regarding R1.2: BPA supports this requirement. Regarding R1.3: The "Applicable BES Cyber Systems and associated Cyber Assets" should use "Medium Impact BES Cyber Systems with External Routable Connectivity" instead of the broader "Medium Impact BES cyber systems". In addition, it should be made clear in the standard and not just the guidelines that the requirement applies only to Cyber Assets that use a routable protocol. BPA suggests adding "BES Cyber Assets or Associated Cyber Asset that do not use a routable protocol do not have to reside within a routable ESP" to the end of the requirement. Regarding R1.4: BPA supports this requirement and recommends the removal of "where technically feasible". Regarding R1.5: BPA supports this requirement. Regarding R1 VRFs and VSLs: BPA supports the factors and levels.

Regarding R2.1: BPA believes that the current wording of R2.1 is too vague, too complicated and doesn't adequately provide intent of the guidance. BPA recommends rewording requirement for R2.1 to read: "All Interactive Remote Access must be made through an Intermediate Device that enforces authentication. Direct Interactive Remote Access between a remote Cyber Asset and a BES Cyber System is not allowed." BPA also recommends that guidance lists some of the acceptable Intermediate Devices or methods, such as VPNs, terminal servers, jump boxes, etc. Regarding R2.2: BPA supports this requirement. Regarding R2.3: BPA supports this requirement. Regarding R2 VRFs and VSLs: Yes – BPA supports these factors and levels.

No

Yes

Yes

Regarding CIP-006-5 Table R1: R1, 1.4 and Application Guidelines under R1 specifically referencing opening greater than 96 square inches would be considered an access point. BPA believes that R1-1.4 "99.9% availability" in the current context is unclear to the scope and meaning. For example, does this percentage of availability apply per location, per device or all devices and locations? What is the duration of the reset cycle (i.e., 24 hours, annual)? Does "99.9% availability" only apply to unplanned outages or does this also apply to planned outages? Additionally, if this measure requires evidence that may include and is "not limited to" (i.e., monitoring logs?) documentation to support and/or demonstrate 99.9% availability of the controls that monitor the Physical Security Perimeter (PSP) for unauthorized circumvention of a physical access, does this also imply the need for 99.9% or greater percentage of availability for the reporting/logging mechanism and all of its relevant components? Does "twenty four hours a day, seven days a week" equal or equivalent to "continuous, real-time or perpetual?" For example, a local end-point device may serve as the primary control used to monitor for the circumvention of a PSP; if this device maintains continuous logging (residing in local system memory) within a defined and acceptable availability percentage, does this demonstrate compliance? Attempting to specify a percentage of availability within an undefined process description lacks the necessary context to provide clear guidance at this time. Our recommendation is to provide further clarification to both scope and meaning with detailed provisions allowing for both planned and

unplanned outages. Application Guidelines: The citations used for CAN 0031 and now included in CIP 006 V-5 draft are inappropriate standards for the utility industry. Department of Defense and Central Intelligence Directive sources cited as a basis for the language in CAN 0031, which is now applied to the Guidelines and Technical Basis for CIP 006 Version 5 Draft; are tied directly to that of National Defense and National Security interests (i.e. Nuclear Reactors and Special Nuclear Materials (SNM) and Weapons of Mass Destruction (WMD). Electric utility entities do not posses, process or produce the kinds of information and material intended to be protected by the referenced standards. In no case are public or private utility industry entities operating under a national security classification other than nuclear power facilities which are regulated under other standards. The protection of Special Nuclear Material (SNM), Sensitive Compartmented Information Facilities, (SCIF) and other highly sensitive national security information and material demand standards to prevent intrusions, and unauthorized access to material and information which is not present in the utility environment. The application guideline is attempting to address a vulnerability for which no accompanying risk appears to exist. BPA owns approximately 300 substations located across its service area. BPA's service area includes all or parts of eight western states. A review of security incident records dating back to 2003 show there have not been any intrusions by way of windows, or openings of 96 square inches. (The size of notebook paper)Previous versions of CIP 006 require utilities to implement technical and /or procedural controls to detect and respond to apparent unauthorized access attempts. This version and the cited guidelines are a significant shift in direction moving from "detect" to "prevent" intrusion. This shift in strategy has an exceptional cost impact with little return on investment. The guideline defines an "access point" as any "opening" greater than 96 square inches with one side greater than 6 inches in length. NERC does not provide a definition pertaining to what constitutes an opening. It is essential to know what NERC will consider to be an opening in order for entities to effectively implement the standard. BPA considers an access point as a portal intended for normal human ingress and egress purposes. Without context regarding access points and openings, BPA cannot determine what it will take to become or remain compliant with this requirement. Given the forgoing comments, the needed clarity for the definition of access point, and opening, and unclear indications of what vulnerability is intended to be mitigated by the NERC CIP 006 V.5 Application Guidelines; BPA is voting "No."
No
No
No
No
No
BPA finds it difficult to discuss only the changes made since that last voting period, since not all comments were addressed adequately. These comments address drafts 1 and 2 for all of CIP-007 R1, R2, R3, and R4. Regarding "Background "Applicability Columns in Tables", BPA believes the "Associated Electronic Access Control or Monitoring Systems", "Associated Physical Access Control Systems", and "Associated Protected Cyber Assets" are definitions and should be included in the proposed Definitions, so that entities may comment and vote on them. In addition, BPA believes the term "associated" is too vague. For example, it is difficult to see how an Associated Protected Cyber Asset differs from a Protected Cyber Asset, since in many cases the only "association" would be that Associated Protected Cyber Asset is within ESP, as are all Protected Cyber Assets. Finally, "Associated Physical Access Control Systems" uses the term "External Routable Connectivity", it is unclear whether it is the Physical Access Control System or the BES Cyber Asset that has the External Routable Connectivity, nor is it clear why the other Associated Cyber Assets do not refer to External Routable Connectivity. It is difficult to offer suggestions when we are still unclear on the SDT intent. Regarding 1.1 "Applicability" – BPA believes the 'Medium Impact Cyber Assets' are subject to the requirement only if they have External Routable Connectivity. All Associated assets are subject to the Requirement, regardless of connectivity. BPA recommends adding "with External Routable Connectivity" to the associated Cyber Assets. Regarding 1.1 "Requirements" – BPA believes the requirement is not consistent with the Guidelines, which states "If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'" That statement modifies the requirement and is inappropriate in a guideline. In addition, including it as part of the requirement would eliminate numerous Technical Feasibility Exceptions. BPA recommends it be moved from the Guidelines to the Requirement. Regarding 2.2 "Guidelines" – BPA

believes the guidelines add additional requirements which are valid and should be in the Requirements. BPA suggests rewriting the Requirements section as “Evaluate the security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified in Part 2.1. The assessment must include determination of the applicability of each patch to the entity’s specific environment and systems as well as reason for a patch’s non-applicability.” Regarding 2.3 “Guidelines” – BPA believes the first sentence of Guidelines restates the Requirement with different wording. BPA is unclear on how this adds new information and believes it gives the appearance of levying an additional requirement. BPA recommends deleting the first sentence of Guidelines 2.3. Regarding 2.4 “Requirements” – If you agree that referring to an existing plan is acceptable than, BPA believes that there is no need to state “For each plan created or revised in Part 2.3…” in the Requirement. BPA suggests “For each plan in Part 2.3…” This would also accommodate the suggested change to R2.3. Regarding 3.1 “Guidelines” – BPA believes the Guidelines make it very clear that the Responsible Entity can determine that a particular Cyber Asset or group of Cyber Assets is not susceptible to malware and needs little or no protection. Regarding 3.1 “Requirements” – BPA agrees with and applauds the decision not to require anti-malware tools on every Cyber Asset. “BES Cyber System” groups Cyber Assets for convenience. R3.1 could be still be construed to apply to each Cyber Asset in the BES Cyber System. BPA believes that R3.1 needs to be explicit. BPA suggests “For Cyber Assets within the scope of CIP-007 R3.1, and which the Responsible Entity has determined to be susceptible to malware intrusion, deploy method(s) to deter, detect, or prevent malicious code. These need not be deployed on every applicable Cyber Asset, as long as each applicable Cyber Asset is protected.” Regarding 3.1 “Measures” – BPA believes that the Measures should be reworded to incorporate the changes to R3.1. BPA suggests rewording as follows “Evidence may include and is not limited to: (1) Documentation of any determinations that specific Cyber Assets or specific types of Cyber Assets are not susceptible to malware and if applicable(2) Records of the Responsible Entity’s deployment of these methods; i.e. through traditional antivirus, system hardening, policies, etc.” Regarding 3.2 “Guidelines” – BPA believes that it should be noted that the Guidelines state, “If a specific Cyber Asset has no updateable software and its executing code cannot be altered…” Since there are other documents associated with Version 5 which clearly implies devices are Cyber Assets only if their executing code can be changed, this is an example of the uncertainty of the definition of “Cyber Asset” and needs to be clarified. Regarding 4.1 “Requirements” – BPA believes that the Requirement does not allow for the SDT intent as stated in the Guidelines. BPA recommends revising the first sentence of the requirement to read “…types of events that the device can log:”. Regarding 4.1 “Measures” – BPA believes the Measures conflicts with the Requirement, unless the Requirement is corrected as identified above. Regarding 4.2 “Applicability” – BPA believes that Medium Impact Cyber Assets are subject to the requirement only if they have External Routable Connectivity. All Associated assets are subject to the Requirement, regardless of connectivity. BPA recommends adding “with External Routable Connectivity” to the associated Cyber Assets. Regarding 4.2 “Guidelines” – As written, the Requirement does not prohibit the use of procedural controls to achieve compliance. The Guidelines imply that the intent was compliance by technical means. Was that the intent of the SDT? The guidelines and Requirements are not consistent. . BPA suggests that the following sentence be inserted at the start of the Guidelines for 4.2.: “Although manually-generated alerts may be the only means available, automated alerts provide an additional level of security.” Regarding 4.3 “Applicability” – BPA believes Medium Impact Cyber Assets are subject to the requirement only if they have External Routable Connectivity. As the requirement is written, all Associated assets are subject to the Requirement, regardless of connectivity. BPA recommends adding “with External Routable Connectivity” to the associated Cyber Assets. Regarding 4.4 “Requirements” – BPA believes R4.4 still does not prevent a violation for a failure of the logging system. In particular, a hardware failure of media used to store logs would be a violation. In addition, the phrase “where technically feasible” forces Technical Feasibility Exceptions even in the case of a hardware failure of the logging system. This could require after-the-fact submissions of Technical Feasibility Exceptions, which would serve no purpose. Technical Feasibility Exceptions should only be needed in the very rare cases of a logging system that is inherently incapable of providing for long-term retention of logs. BPA suggests rewording as follows: “Unless prevented by a failure of system(s) used for logging, retain BES Cyber System security-related event logs identified in Requirement 4.1 for at least the last 90 consecutive calendar days, where technically feasible.” Regarding 4.5 “Requirements” – BPA believes that, “…at a minimum every two weeks” could be construed as “no less than two weeks apart.” BPA suggests “Review a summarization or sampling of logged events at intervals of no greater than 15 days to identify undetected Cyber Security

Incidents."
BPA recognizes the difficulty of discussing only the changes made since that last voting period, since not all comments were addressed adequately. These comments address all of CIP-007 R5. Regarding 5.1 "Requirements" – Given the extensive comments on CAN-0017 and difficulty in interpreting the draft 1of CIP-007 R5, BPA suggest that the question of technical or procedural controls and the acceptability of procedural controls without technical controls should be explicitly addressed. This is especially important for physical access, where procedural controls such as human guards controlling access are often the best approach. BPA recommends "Using either technical or procedural controls, enforce authentication of all user access, where technically feasible. Technical controls are not required if procedural controls are in place." Regarding 5.3 "Applicability" – BPA believes Medium Impact assets must have External Routable Connectivity to be subject to the requirement. The requirement states that all Associated assets are subject, regardless of connectivity. BPA recommends adding "with External Routable Connectivity" to the associated Cyber Assets. Regarding 5.5 "Requirements" – BPA believes the suggested password length and complexity are certainly not excessive for password-only authentication. Multi-factor authentication often uses a token and Personal Identification Number (PIN). Such authentication is much stronger than simple passwords, even with numeric-only PINs. Unfortunately, PINs could be construed as a form of password and are subject to R5.5. To clarify the difference, BPA recommends replacing "For password-base user authentication,…" with "For user authentication that uses only passwords…". Regarding 5.6 "Applicability" – BPA believes that Medium Impact assets must have External Routable Connectivity to be subject to the requirement. The requirements states that all Associated assets are subject, regardless of connectivity. BPA recommends adding "with External Routable Connectivity" to the associated Cyber Assets. Regarding 5.6 "Requirements" – BPA recognizes that the requirement has the same issue with multi-factor authentication that R5.5 has. In addition, passwords must be changed every calendar year, not to exceed 15 months. The table that follows R5.5 in the Guidelines suggests changing passwords "During regularly scheduled maintenance" or "During scheduled plant outages" for shared accounts at various locations other than control centers. BPA suggests, "For user authentication that uses only passwords, either technically or procedurally enforce password changes or an obligation to change the password at least once each calendar year, not to exceed 15 calendar months between changes. Changes that can only be performed during regularly scheduled maintenance or scheduled plant outages can be delayed until the next scheduled maintenance or scheduled plant outage, if necessary. Passwords need not be changed if access has been disabled or otherwise prevented until the reinstatement of access." The language change reflects the guidance given in Requirement 5.5's table, where the periodicity of password changes are recommended, and ties it to Requirement 5.6. This suggestion will promote consistency in the Standard. Regarding 5.7 "Requirements" – As noted for R5.1, it is possible that there could be Cyber Assets that do not use technical means of authentication, especially for physical access. As R5.7 is currently worded, this situation would require a Technical Feasibility Exception for lack of technical enforcement of a non-technical control. BPA recommends rewording the requirement to, "For those systems and access for which technical authentication controls are used, and where technically feasible, limit the number…"
Individual
Benjamin Bebernes
Snohomish County PUD
Yes
No
Yes
No
Yes
Yes
No
CIP-004-5 R2 Training should entail security principles not individual processes. The security principles for controlling the BES cyber assets and the storage should be the same. In addition, in most companies the staff isn't this specialized and tends to be supporting everything. Visitors are always escorted, so training should not be required. What could be done is hand them a form to sign that indicates they are entering a BES facility and they are to behave in a certain way (ex. always remain with escort). 2.8 Discusses training on a recovery plan, but what could be more relevant to

keeping the lights on during cyber incidents is the business continuity plan. I would recommend that training occur on the business continuity plan as well or the recovery plan includes the business continuity plan. CIP-004-5 R7, CIP-004-5, Requirement R1, R2, R3, R4, R5, R6, R7 When employees are transferring within a company there may be a need to have a transition period that overlaps with new responsibilities. So how do you define the transfer date? Snohomish would recommend that the access management process include a mechanism for transfers that can document a date that the access will be removed that may be separate from the official start date in new role. The evidence would be the same except the date is the date specified versus the date the person starts new role.
Yes
Yes
CIP-005-5 R1 1.5 requires a method for detecting malicious communication. This should include a “where technically feasible” clause.
Yes
Yes
Yes
Yes
Yes
No
No
No
CIP-007-5 R3 “In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.” This would require specific policies regarding the use of any type of portable storage such as thumb drives, CD/DVD, portable hard drives, or any other potential storage medium. It would also require specific controls on uncontrolled access to the internet and personal e-mail. The current requirement is way too broad for consistent application. It appears that the requirement has been defined to allow for greater flexibility, however, compliance has been made more difficult by the wording. Documentation every 35 days would be burdensome due to the various signature file updates, OS vendor updates, and control console scanning logs. Use of whitelisting is listed as an option and this has proven technically infeasible for most environments. CIP-007-5 R4 The standard requires manual review of logs, documentation of the review, and an attestation that nothing was identified of a security nature. The sheer volume of logs makes this requirement an audit trap. An automated SIEM is the only real solution and the cost of implementing such a system for a small utility is prohibitive. A documented sampling of logs meets the requirement, but does not provide for any real additional security. This requirement needs more developmental maturity before implementation.
. CIP-007-5 R5 This must include technically feasible on all points due to the nature of the equipment.
Individual
Larry Watt
Lakeland Electric
Yes
Yes
Yes
Yes
Yes
No
No

"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
Yes
Yes
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
No
No
No
"Please see comments submitted by FMPA through the formal comment process."
No
Yes
Yes
No
No
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
Individual
Ron Donahey
Tampa Electric Company
Yes
No
No
Yes
Yes
No
No
Tampa Electric supports the comments submitted by Edison Electric Institute (EEI). In addition, Tampa Electric is concerned that there will be an administrative burden based on the many versions of training programs tailored to specific roles.
Tampa Electric supports the comments submitted by EEI. Tampa Electric also suggests that the, measures for 6.3 and 6.4 need additional clarification. Tampa Electric is concerned that R6 is an administrative burden with little additional benefit to the security and reliability of the BES. R6.7 is unclear regarding the location.
No
No
Tampa Electric supports the EEI Comments and would appreciate additional clarification related to a proposed definition of “dial-up” connectivity. Should this be defined by what is accessible via the PSTN? Would dial-up (out-of-band) connectivity originating internal to the ESP via a non-public network connection qualify as a dial-up connection that should be afforded CIP005 R1.4 authentication protection? And if so, can the authentication be performed by an intermediary device and pass such credentials allowing for access? For CIP-005 R1.5, please add external routable connectivity to the applicability.
Comments: CIP-005 R2.2 requires encryption for all interactive remote access sessions. Please confirm the interpretation that this requires that only the communication path between the originating device and the intermediary device to be encrypted. For CIP-005 R2.3, Tampa Electric requests the SDT provide clarification related to multi-factor authentication related to whether one-time password (OTP) devices combined with a personal network ID/password combination qualify as multi-factor authentication?
No
No

No
Tampa Electric agrees with the comments provided by EEI. In addition, Tampa Electric raises the following questions. For R1.4: The term “circumvention” is unclear; please provide additional context for improved understanding. For example, how would an entity monitor for this circumvention, for an action like piggybacking or tailgating? R1.4 should include the assets (PACS) that are currently under R1.6. The measure is the same for both R1.4 and R1.6 and requirements are basically the same. This introduces double jeopardy. We also are concerned with the 99.9% availability requirement as stated; this should be struck. It will be difficult if not impossible to track across an entire PACS system (all components). This would not allow for outages and potentially routine maintenance. For R1.3, Tampa Electric requests additional clarification related to the language “two or more different physical access controls” as the current language suggests at two systems to control access into PSP. This could be an issue if guards are not considered adequate to control access to the Control Center (High Impact) PSP. For R1.7 restates R1.5. R1.5 should include the assets (PACS) that are currently under R1.7. The measure is the same for both R1.5 and R1.7 and requirements are basically the same. This introduces double jeopardy Tampa Electric suggests that it is unclear if the Response plan must include a physical presence (human) to respond to an alarm or “Alert.” This requirement as stated also employs circular logic.
Yes
No
Yes
No
No
Tampa Electric supports the comments submitted by EEI. In addition, for CIP-007 R1.2, we request that the SDT provide clarification of physical ports, in particular whether physical ports can be protected via common method (port lock – key), or is there a requirement for unique protections for each port on each device? Tampa Electric suggests that for CIP-007 R2.1, documenting the sources for patches should be a one-time exercise unless additional software is added to the baseline. For CIP-007 R2.3, Tampa Electric requests the SDT provide guidance for procedure if patches cannot be applied, whether technically or operationally not feasible. Would separate TFE/OFEs be required for each exception? Would the TFP/OFE be required once/monthly/annually for the same exception? For CIP-007 R4.2, Tampa Electric requests additional clarification related to alerting for malicious (AV) events. If malicious activity is detected, is an alert required if the entity has automatic controls to quarantine? For CIP-007 R4.3, Tampa Electric requests that the SDT provide clarification on what qualifies as a “response” to logging failures before end of next calendar day. Is it acceptable for the logging failure to be acknowledged even if cannot be corrected by end of next calendar day. CIP-007 R4.5, Tampa Electric requests the SDT to provide guidance requested for what constitutes a “sampling” of logged events… and what evidence should accompany the “review” (logging sample?) It should not refer to an external standard to provide this guidance.
Tampa Electric supports the comments provided by EEI. If the EEI comments are not adopted, Tampa Electric requests clarification for R5.2 on “generic account types” as specific examples of account types are given in the Application Guidelines, p. 46.
Individual
Annette Johnston
MidAmerican Energy Company
Yes
No
No
No
No
No
No
(1) CIP-004 R1 REQUIREMENT: 1) We propose the word “calendar” be deleted to allow entities flexibility of using a different quarterly basis. 2) The word “cyber” should be deleted from the term “cyber security practices” so it is not misunderstood to mean that the scope excludes physical security

topics. (2) CIP-004 R1 GUIDANCE: The following sentence appears to be a statement to the drafting team that should have been deleted: “Guidance: Describe example mechanisms used to demonstrate the availability of this information.” (3) CIP-004 R2 REQUIREMENT: (a) APPLICABILITY: MidAmerican Energy disagrees with the expansion of scope from draft 1 to draft 2 to include associated Physical Access Control Systems and associated Electronic Control or Monitoring Systems in the training requirements. This is an expansion from version 4, which was not directed by FERC. APPLICABILITY: MidAmerican Energy appreciates the addition of “external routable connectivity or dial-up connectivity” in R2 and remaining CIP-004 requirements. (b) In addition, the draft 2 applicabilities for PACS between the standards are not consistent. For example, CIP-006 requires only operational or procedural controls for PACS. Because a PSP is not required for PACS, an entity would not be required to have a list of who has physical access to them, and therefore, would not have a list of who needs training. MEC proposes deleting the PACs and EACs from all of the R2 applicabilities, consistent with scope in V4. (c) R2.1 ROLE-BASED TRAINING: MidAmerican Energy disagrees with the requirement to identify each role and training required for each role, which was not ordered by FERC and is becoming more prescriptive instead of results-based. The requirement is not clear whether one training role and one comprehensive training program for all roles and responsibilities would be acceptable. The rationale infers there must be multiple training modules, which will result in a significant increase in the administrative and documentation burden on entities that have existing training programs. MidAmerican continues to support making the FERC directed changes to version 4, without the significant change to require identification of “each role and training required for each role.” MidAmerican Energy would support deleting R2.1 and changing the R2 statement to include the concept of roles and responsibilities, using language closer to version 4 language, such as: “Each Responsible Entity shall have a cyber security training program to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes the applicable items in CIP-004-5 Table 2 – Cyber Security Training Program, appropriate to personnel roles and responsibilities.” If R2.1 remains, it should clarify that an entity can be compliant if they elect to have one role or elect to have few roles (for example, as a role for those with only physical access, a role for those with cyber access, a role for only information access). (d) R2.2: Revise to: “Training content on the availability of cyber security policies.” There is a significant difference between training content on the policies themselves, vs. the availability of the policies, which is how the requirement should be written, based on its reference of CIP-003-4 R1.2. (e) R2.3: In requirements that include associated systems (which are not BES Cyber Systems), the text of the requirement should reference “applicable Cyber Assets” instead of BES Cyber Systems. We have recommended associated systems be removed from the applicability, but if this change is not made, this requirement should be changed to: “Training content on the physical access controls protecting the applicable Cyber Assets.” (f) R2.5: MidAmerican does not object to this requirement, but the change rationale of “no significant change from previous versions” is incorrect since visitor control program was not included in the training requirements in version 4. (g) R2.6: no comments (h) R2.7: The wording is too prescriptive. Change to: “Training content on BES Cyber Security Incidents” and then delete R2.9. (i) R2.10: Revise the wording to eliminate conflicts with applicabilities and still meet FERC language concepts from paragraph 434: “Training content on security risks associated with networking hardware and software electronic interconnectivity and interoperability.” Good draft two includes the word “risks.” Add “security” to risks and be sure to retain. This is a good change the clarifies the training is on risks, not on how to interconnect networks. (4) CIP-004 R2 GUIDANCE: The following sentence appears to be a statement to the drafting team that should have been deleted: “Provide guidance or a local definition of “role appropriate” as it is used in the standard.” Add the statement in guidance such as: “It is acceptable to have one training program covering all of the required topics, if an entity chooses to provide the same program to all authorized personnel covering all roles and responsibilities.” See also comments on R2.1 (5) CIP-004 R3 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, to prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (b) R3.1: Delete “and documentation” from the requirement. The requirement should be to complete the training before access is used. Documentation is covered by the measure. This should not be considered a violation. We have recommend associated systems be removed from the applicability due to scope expansion. “BES Cyber Systems” should be changed to “applicable Cyber Assets” in the requirement text. (c) R3.2: Delete “and documentation” from the requirement. Documentation is covered by the measure. (d) ANNUAL: Revise “at least once each

calendar year, not to exceed 15 calendar months," to "once each calendar year or a period not to exceed 15 calendar months between training." (6) CIP-004 R3 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. CIP-004 R3 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower. (7) CIP-004 R4 REQUIREMENT: (a) R4 requires a personnel risk assessment program. We propose the R4 parts be written parallel to the parts in R2, which requires a training program. See following comments. (b) R4.1 proposed text: "Program content on an initial personnel risk assessment that includes identity verification. (c) R4.2: Delete the following text: "4.2.1. resided; 4.2.2. been employed (if applicable); and 4.2.3. attended school (if applicable)." The deleted text could be moved to guidelines. The text was from failed interpretation 2009-23. Since the industry rejected this text, it should not be included in version 5. This text is too prescriptive and not in response to a directive. We propose the following text for R4.2: "Program content on seven year criminal history records check. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed." (c) R4.3: Revise to: "Program content on a process or criteria to evaluate personnel risk assessments to determine when to deny authorized access." (d) R4.4: Revise to: "Program content on a process or criteria for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4, Parts 4.1 through 4.3." Or alternatively, delete the requirement as duplicative of those parts and clarify in the R statement above the table that it R4 applies to all personnel, including contractors or service vendors. (8) CIP-004 R4 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower. (9) CIP-004 R5 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, to prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (b) R5.1 REQUIREMENT: Revise the text to make it clear that the PRA must be performed before the first authorization. The following text is proposed: "Have a personnel risk assessment prior to accessing applicable Cyber Assets, except for CIP Exceptional Circumstances. Subsequent authorizations within the life-time of PRAs do not require repeating the background check." (10) CIP-004 R5 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (11) CIP-004 R5 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower.

(1) CIP-004 R6 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, to prevent recurrence of flaws. (b) R6.1 Delete "or dial-up connectivity" from the applicability to be consistent with applicabilities on other standards. R6.1.2: Revise to "unescorted physical access into a PSP" since it is possible to authorize access for a PSP. Associated PACS do not require a PSP. (c) R6.2: Delete "or dial-up connectivity" from the applicability to be consistent with applicabilities on other standards. Although the word "minimum" was deleted from draft 2, we still think there is too much ambiguity with the phrase "necessary for performing assigned work functions" and it should be delted. We propose revising this requirement to: "The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is appropriate, except for CIP Exceptional Circumstances." (d) R6.3: Delete "or dial-up connectivity" from the applicability to be consistent with applicabilities on other standards. To eliminate ambiguity, we propose replacing the term "necessary for performing assigned work functions," with "appropriate." (e) R6.4: Delete "or dial-up connectivity" from the applicability to be consistent with applicabilities on other standards. To eliminate ambiguity, we propose replacing the term "necessary for performing assigned work functions," with "appropriate for the roles and responsibilities." (f) R6.5 AND R.6.6: MidAmerican commented on draft 1 that R6.5 and R6.6 are major scope expansion not directed by FERC. The SDT responded that the changes were made because of past industry comments that "review the list of its personnel who have such access" is not well understood or consistently implemented. We continue to feel the requirements are not just clarification, but are expanding scope, as well as overlapping requirements between R6.5 and R6.6. The additional administrative work created is not offset by a commensurate improvement in security. MidAmerican proposes supports and will participate in

working toward language to alleviate these concerns. (g) R6.5/R6.6 APPLICABILITIES: Delete “or dial-up connectivity” from the applicability to be consistent with applicabilities on other standards. (h) R6.6: ANNUAL: Revise “at least once each calendar year, not to exceed 15 calendar months between verifications,” to “once each calendar year or a period not to exceed 15 calendar months between verifications.” (i) R6.6 REQUIREMENT: Change “performing assigned work functions” with “are appropriate.” R6.6 MEASURES: Replace the numbered list with bullets and “or.” (j) R6.7: ANNUAL: Revise “at least once each calendar year, not to exceed 15 calendar months between verifications” to “once each calendar year or a period not to exceed 15 calendar months between verifications.” R6.7 REQUIREMENT: delete “minimum” since it was deleted in the requirement. R6.7 MEASURES: Change numbered list to bullets with “or.” Delete “any” in the measure. Revise the measures to correspond to other changes listed above. (2) CIP-004 R6 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (3) CIP-004 R7 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, to prevent recurrence of flaws. (b) Immediate revocation of access is listed on the EEI REAC key issue list. Though FERC Order 706 mandated “immediate” revocation, many entities consider the scope of cyber assets in the applicability too broad and problematic. We think two changes balance security and resource requirements: (i) Incorporate the language suggested that allows detection and correction without it being a violation. (i) Limit the immediate revocation to high impact BES Cyber Systems, and allow additional time for the other asset categories. MidAmerican suggests limiting the draft 2 R7.1-R7.3 to High Impact BES Cyber Assets which may require writing new parts for the medium impact BES Cyber Assets. Requirements for medium should not increase the current version 4 compliance thresholds. (c) R7.4 and R7.5 already are limited to high impact, which we agree with. Another major issue of concern to the industry is access revocation of contractors. Draft 2 does not specifically address differences in the requirements based on employees vs. contractors. We would like to work with the SDT to find some solutions to this issue. (d) R7.1 REQUIREMENT: Change the requirement text to identify the time the termination action is communicated to address concerns regarding notification of terminations that are predated or retroactive. Proposed text: “For all termination actions, initiate the process to revoke the individual’s unescorted physical access and Interactive Remote Access upon the effective date and time of the communication of the termination action, and complete the revocation within 24 hours after the effective date and time of the communication of the termination action.” (d) R7.1 MEASURES: Change the numbered list to bullets with “or.” Add a measure for completion, since the measures listed are for initiation. (e) R7.2: Change the requirement text to incorporate the initiation of revocation, along with the determination that access is no longer needed. Proposed text: “For reassignments or transfers, initiate revocation of the individual’s electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the determination that access is no longer necessary.” Change the numbered list to bullets with “or.” Add a measure for completion, since the measures listed are for initiation. (f) R7.3: We propose this be limited to terminations for cause for employees. We think additional discussion is needed for contractor processes. Change the requirement text to incorporate the initiation of revocation. (g) R7.4: No comments. (h) R7.5: Add “to BES Cyber Assets” to the requirement to align with R7.4 which includes the phrase: “For termination actions, reassignments, or transfers, change passwords for shared account(s) to BES Cyber Assets known to the user within 30 calendar days of the termination action, reassignment, or transfer of the user.” (4) CIP-004 R7 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention.
No
No
(1) CIP-005 R1 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, to prevent recurrence of flaws. (b) R1.1: APPLICABILTY: MidAmerican Energy recommends the applicability for 1.1 be High Impact BES Cyber Systems with External Routable Connectivity, Medium Impact BES Cyber Systems with External Routable Connectivity and Associated Protected Cyber Assets. This

moves the external routable qualifier out of the requirement into the applicability where it belongs and makes 1.1 parallel to 1.2. (c) R1.1 REQUIREMENT Proposed Text: “Applicable Cyber Assets shall reside within a defined ESP.” The proposed changes move text referencing applicability to the applicability part of the table. This also removes text from the requirement that is redundant to the definition of ESP (see comment above). (d) R1.2 REQUIREMENT Proposed text: “All External Routable Connectivity must be through an identified Electronic Access Point (EAP).” By definition, external routable connectivity ties the ESP to the Cyber Asset so the reference to ESP is circular when the definition of NERC is applied. This also eliminates the use of “through” twice in the same sentence. (e) R1.3 No comments. (f) R1.4 MidAmerican Energy recommends this requirement be deleted. Dial-up authentication belongs in table 2 for interactive remote access management. Table 2 already has requirement 2.3, which requires authentication for Interactive Remote Access. (g) R1.5 MEASURES: Change “and” to “or” and use bullets for 1. and 2. The two sub bullets for 1. could be separated so there are three bullets as examples. (2) CIP-005 R1 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (3) CIP-005 R1 VRF: In its May 18, 2007 order on violation risk factors, FERC identified five guidelines for approval of VRFs, including consistency among reliability standards. After reviewing VRFs on all existing NERC standards, MidAmerican Energy Company is proposing a change to the VRFs on several of the version 5 draft 2 requirements, including CIP-005 R1. We agree the VRF should be medium for the high impact BES Cyber Systems, but we think the VRF should be lower for the medium impact BES Cyber Systems.
(1) CIP-005 R2 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, to prevent recurrence of flaws. (b) R2.1-2.3APPLICABILITY: MidAmerican recommends adding “with External Routable Connectivity” for each applicability because it directs this requirement to the greatest risk and where there are the greatest security benefits to be achieved and the most mature technology. BES Cyber Assets in medium dial up accessible substations pose less risk and technology is not as proven. The applicability should be compared to proposed changes to relevant definitions where the proposal is remove dialup from the definition(s). (c) R2.1 REQUIREMENT Proposed text: “Restrict Interactive Remote Access to only authorized users such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.” This does not prescribe how technologically to accomplish this and allows for application proxy firewalls. (d) R2.3 REQUIREMENT: see applicability comment for externally routable. (e) As recommended in R1, move CIP-005 R1.4 for dial-up authentication to R2 and incorporate multi-factor authentication. This eliminates redundancy and double jeopardy. Add “where technically feasible.” (2) CIP-005 R2 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (3) CIP-005 R2 VRF: We agree the VRF should be medium for the high impact BES Cyber Systems. To be consistent with other reliability standards, we think the VRF should be lower for the medium impact BES Cyber Systems.
No
No
No
(1) CIP-006 R1 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, to prevent recurrence of flaws. (b) R1.1: No comments. (c) R1.2: No comments. (d) R1.3: The SDT states in its consideration of comments that changes were made to clarify that two different physical access controls are required, not two completely independent physical access control systems. However, there still has been considerable discussion on what is meant by this requirement during industry association meetings. Clarify the requirement by adding a sentence, such as the statement in the consideration of comments: “Two different physical access controls are required, not two completely independent physical access control systems.” The guidance is clear, for example, that bio and PIN is okay. This reflects the concept in the requirement which will be enforced. (e) R1.4 and R1.5: V4 required monitoring of PSP access points. V5 eliminates the concept of access points and six-wall borders. R1.4 and R1.5 require monitoring for “unauthorized circumvention of a physical access

control into a PSP" and issuing an alarm "in response to detected unauthorized circumvention of a physical access control into a PSP." This could be read to mean monitoring and alerting of the entire PSP, such that video and/or motion detection would be needed for compliance. We understand the intent of the SDT in adding the 99.9% availability in R1.4; however, we think it would require extensive documentation to track compliance. Our proposed text in the R statement above the table will address the concern with zero defect compliance with this requirement, without less documentation burden. We propose combining R1.4 and R1.5 into the following revised text that addresses the concerns with monitoring the PSP. We suggest replacing the term "monitor" with "alert" since the intent is to provide alerts: "Have controls that provide alerts for detected unauthorized circumvention of physical access controls for the Physical Security Perimeter. Respond within 15 minutes of detection of unauthorized circumvention of a physical access control. If a six-wall border is established for the PSP, alerting is only required for access points into the PSP. If a six-wall border is not established, alerting of the entire PSP is required." (f) R1.6 and R1.7: Combine these parts, remove the 99.9% availability reference and replace "monitor" with "alert." The following text is proposed: "Have controls that provide alerts for detected unauthorized circumvention of physical access controls for the Physical Access Control Systems. Respond within 15 minutes of detection of dtected unauthorized circumvention of physical access controls to a Physical Access Control System." (g) R1.8: No comments. (h) R1.9: No comments. (2) CIP-006 R1 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (3) CIP-006 R1 VRF: We agree the VRF should be medium for the high impact BES Cyber Systems. To be consistent with other reliability standards, we think the VRF should be lower for the medium impact BES Cyber Systems. (4) CIP-006 R2 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, to prevent recurrence of flaws. (b) R2.1: The addition of the words "who are known or guests and" makes it sound like guests are unknown people. We think the requirement is clear with the following text: "Require continuous escorted access of individuals not authorized for unescorted physical access, except during CIP Exceptional Circumstances." (c) R2.2: No comments. (d) R2.3: No comments. (5) CIP-006 R2 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. CIP-006 R2 VRF: We agree the VRF should be medium for the high impact BES Cyber Systems. To be consistent with other reliability standards, we think the VRF should be lower for the medium impact BES Cyber Systems. (6) CIP-006 R3 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, to prevent recurrence of flaws. (b) R3.1: Change all references (within the applicability, requirement, measure and guidance) from "locally mounted hardware or devices" to "locally mounted devices." The guidance states that testing includes motion sensors, electronic lock control mechanisms and badge readers, which most people would not think of as hardware. Hardware could be interpreted to include door hinges and screws, which should not be included in the requirement. (c) R3.2: In applicability, change "locally mounted hardware or devices" to "locally mounted devices." Change the text requirement to focus on the defined term: "Document outages for Physical Access Control Systems and retain the outage records for at least 12 calendar months." Or, alternatively, move the document retention to the Compliance section C. (6) CIP-006 R3 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention.
No
No
No
No
No
(1) CIP-007 R1 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, to prevent

recurrence of flaws. (b) R1.1 REQUIREMENT: Add the following statement to the requirement text: “If a device has no provision for disabling or restricting logical ports on the devices, then those ports that are open are deemed necessary.” Add the following guidelines: “An example of a device that has no provision for disabling or restricting logical ports on the devices are purpose built devices that run from firmware with no port configuration available.” (c) R1.1 MEASURES: Add a fourth bullet to address CIP-005-4 R2.2: Listing of access points to the Electronic Security Perimeter(s), including configuration of ports and services, individually or by specified grouping. (d) R1.1 GUIDANCE: Remove the reference to CIP-005 R1 to protect the network, since this isn’t applicable with version 5. 3) R1.2: Revise the text to begin with “Have methods to protect against…” since the VSL is for not having methods. (2) CIP-007 R1 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (3) CIP-007 R1 VRF: We agree the VRF should be medium for the high impact BES Cyber Systems. To be consistent with other reliability standards, we think the VRF should be lower for the medium impact BES Cyber Systems. (4) CIP-007 R2 APPLICABILITIES: Add “External Routable Connectivity” to the Medium Impact BES Cyber Systems for all of the parts of R2. The security risk level is different on purpose built Cyber Assets that don’t have external routable connectivity or dial up accessibility. Focus resources on the higher risks. (5) CIP-007 R2 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, to prevent recurrence of flaws. (b) R2.1 REQUIREMENT: We think it is important to include security upgrades in this requirement. We propose the following text to make it clear that upgrades are included: “A patch management program for tracking, evaluating, and installing cyber security patches and security upgrades for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches and security upgrades for applicable Cyber Assets that are updateable and for which a patching or upgrade source exists.” (c) R2.2 REQUIREMENT: We appreciate the change that was made in CIP-007 R3.3 to allow 35 days and request R2.2 to be changed to 35 days to allow the normal monthly update cycles to have a chance to execute. (d) R2.3 REQUIREMENT: As stated in R2.1, we think it is important to include security upgrades. Change “applicable patches” to “applicable security patches and security upgrades.” Change “security patch” to “security patch or security upgrade.” We believe the primary focus should be on installing the security patches or upgrades and moderating the amount of documentation. (For example, about 160 Windows based Cyber Assets have 84,000 distinct patch assessment outcomes, a subset, but significant scale of which require installation. We suggest changing to 60 calendar days and adding the following sentence to the requirement: “a remediation plan is not required for security patches or security upgrades installed within 60 days of release from the identified source.” This incents prompt implementation which is good for security and reduces paperwork which frees resources for other security adding work. Delete or revise the word “dated” since the guidance suggests a plan could be based on the next outage. (e) R2.4 REQUIREMENT: We appreciate the flexibility provided in R2.3, including the possibility of an “open ended” plan similar to a TFE without an expiration date. However, we think additional flexibility is needed to allow the plans to be revised. As written, R2.4 does not allow the plan to be revised, except in CIP Exceptional Circumstances. NERC has recognized the need for entities to make changes to implementation plans, such as with TFEs. Revise the requirement to: “For each plan created or revised in Part 2.3, implement the plan, except for CIP Exceptional Circumstances. If the plan cannot be implemented within the timeframe specified, revise the plan before the timeframe expires and implement according to the revisions.” (6) CIP-007 R2 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (7) CIP-007 R2 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower. (8) CIP-007 R3 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, to prevent recurrence of flaws. (b) R3.1 REQUIREMENT: MidAmerican provided comments on draft 1 that the requirement needs to be clear on the competency based approach. There is some excellent description of this, but it is only in the summary of changes and application guidelines, which are not enforceable. We proposed the following revised text: "Deploy method(s) to deter, detect, or prevent malicious code based on the Cyber Asset's susceptibility to malware. Methods do not have to be used

on every single Cyber Asset." In the consideration of comments, the SDT stated that adding "susceptibility" to the requirement is another element that could require some form of evidence from every entity for every Cyber Asset. The SDT further states the requirement is "applicable at the systems level, so that every Cyber Asset is not included." However, this requirement also applies to Associated Protected Assets, which is at the asset level. We continue to have concerns that the requirement, as written, does not clearly state that methods are not required on every asset. We would appreciate the opportunity to discuss acceptable solutions with the SDT. One idea would be to add the following sentence to address the associated protected Cyber Assets: "Associated protected Cyber Assets may be included in the methods for the BES Cyber Systems with which they are associated." Perhaps a better solution proposed in other MidAmerican comments is to rephrase the applicability, such as, "high impact BES Cyber Systems, including Associated Protected Cyber Assets." (c) R3.1 GUIDANCE: The last sentence in the R3.1 section of the guidance has a statement "should not require a TFE." This makes it sound like there is an option for a TFE. Reword to make it clearer that TFEs are not available and not needed. (d) R3.2 REQUIREMENT: Add the following sentence: "Mitigation for the Associated Protected Assets may be accomplished through other applicable systems." (e) R3.3: No comments. (9) CIP-007 R3 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (10) CIP-007 R3 VRF: We agree the VRF should be medium for the high impact BES Cyber Systems. To be consistent with other reliability standards, we think the VRF should be lower for the medium impact BES Cyber Systems. (11) CIP-007 R4 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, to prevent recurrence of flaws. (b) R4.1: Many in the industry requested that the requirement be revised to make it clear that TFEs are not needed if a device cannot log. In its consideration of comments, the SDT stated TFE exclusion language is not necessary but attempted to strengthen the basis for not requiring TFE exclusion language. MidAmerican Energy believes that adding TFE exclusion language will eliminate the need for discussion on this in the future, especially with auditors. Since there continue to be questions from many entities about the meaning of the requirement, we again suggest the following sentence be added to the requirement: "Devices that cannot log a particular event do not require a TFE to be generated." (c) R4.2 REQUIREMENT: We continue to have concern with the use of the term "real time" and don't think the changes addressed this concern. The term "real time" has an implied meaning in the industry, and it's not used in that manner within this requirement. This requirement exceeds the scope of version 5 without a FERC directive, and draft 2 has become more prescriptive with the listing of the types of events. In its consideration of comments, the SDT states "This is not a requirement that the systems or assets themselves perform an alert, but rather a requirement that the entity implement a method to produce a real-time alert upon detection of the stated conditions." However, the requirement, as written, does not match the SDT's explanation. We would propose the requirement be revised to better reflect the SDT's intent: "Have methods to generate alerts, where technically feasible, for events that the Responsible Entity determines necessary." "Malicious activity" in R.4.2.1 should be "security event," if this item remains in the requirement. (d) R4.3 REQUIREMENT: Add "after detection" at the end of the sentence. (e) R4.4 REQUIREMENT: Change to "Retain BES Cyber System and BES Cyber Asset…" R4.4 MEASURES: Change number list to bullets with "or" in between. (f) R4.5 APPLICABILITIES: Change the applicabilities to "High Impact BES Cyber Systems, including Associated Protected Cyber Assets." This clarifies that logging reviews do not apply at the asset level. Exclude the Associated Electronic Control or Monitoring Systems and Associated Physical Access Control Systems. (g) R4.5 REQUIREMENT: Revise the text to make it clearer that the entity determines which logs should be reviewed or sampled. Proposed text: "Review a summarization or sampling of logged events, as deemed appropriate by the Responsible Entity, at a minimum every two weeks to identify undetected Cyber Security Incidents." (12) CIP-007 R4 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (13) CIP-007 R4 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower.

(1) CIP-007 R5 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, to prevent

recurrence of flaws. (b) R5.1 APPLICABILITIES: The applicabilities in CIP-007-5 R5 should be consistent with those in CIP-004-5 R6 and R7. Therefore, change “medium impact BES Cyber Systems” to “medium impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity.” (c) R5.2 REQUIREMENT: This requirement should be deleted since it duplicates CIP-004 R6.2, creating double jeopardy. When we designated an approver in CIP-004, it also covers accounts. In addition, the requirement still has the CIP Senior Manager authorization, even though consideration of comments indicates it was removed. (d) R5.3: This requirement should be deleted since it duplicates CIP-004 R6, creating double jeopardy. If the SDT believes the requirement is necessary, we request an explanation of the difference between this requirement and CIP-004-5 R6.2. The following concept from the rationale is good information and should be incorporated within CIP-004 or elsewhere, if this requirement is deleted: sharing of password is not a violation. (e) R5.4 REQUIREMENT: : Consider changinge “default passwords” to “known user default passwords” or clarifying what passwords are included in this requirement. Start with the TFE phrase. The placement of “technically feasible” in draft two creates some confusion. (f) R5.4 MEASURES: Delete: “when new devices are deployed” because timeframes are covered in implementation plan. (e) R5.5: No comments. (f) R5.6: ANNUAL: Revise “at least once each calendar year, not to exceed 15 calendar months between changes,” to “once each calendar year or a period not to exceed 15 calendar months between changes.” (g) R5.6 REQUIREMENT: Some assets may not be capable of password changes, either technically or operationally. We suggest the following revised text to address this concern but eliminate the need for a TFE (with the proposed changes, the phrase “or obligation to change the password” can be deleted): “For password-based user authentication, either technically or procedurally enforce password changes, within capabilities of the device or operational requirements, at least once each calendar year, not to exceed 15 calendar months between changes.” (h) R5.6 GUIDANCE: The table has not been updated. (i) R5.7 REQUIREMENT: This new requirement was not directed by FERC and it overlaps with CIP-007 R4.2, presenting the possibility of double jeopardy. It also will likely generate many TFEs. We think it should be deleted, and information regarding the number of unsuccessful login attempts could be added to the guidance of CIP-007 R4.2. If the requirement is not deleted, it should be revised to eliminate any overlap with R4.2. Text could be revised to: “Limit, where technically feasible, the number of unsuccessful authentication attempts, unless an alert is generated for R4.2.” (i) R5.7 GUIDANCE: There is no guidance provided for this requirement. (2) CIP-007 R5 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (3) CIP-007 R5 VRF: We agree the VRF should be medium for the high impact BES Cyber Systems. To be consistent with other reliability standards, we think the VRF should be lower for the medium impact BES Cyber Systems.
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
Yes
Yes
Yes
Yes
Yes
Yes
The intent of R4.2 is not clear. If the intent is to require criminal history checks from every location where an individual has lived or worked regardless of official residence, we suggest the following wording: “4.2.1. resided; or 4.2.2 been physically located for employment ; or 4.2.3. been physically located to attend school.” This would also appropriately exclude remote employment and on-line classes.
Yes
No
“Intrusion detection system” has a specific connotation in the computer security community. For the Measures for R1.5, we recommend changing “intrusion detection system” to “detection system” to be in line with the requirement and allow for various appropriate technologies for complying with the

requirement.
Change R2.3 to read “Require multi-factor authentication for all Interactive Remote Access sessions.” Move bullets to the Guidelines. Multi-factor authentication is well understood in the computer security community.
Yes
Yes
No
(Comment 1) The definition for “Locally mounted hardware or devices at the Physical Security Perimeter” (last paragraph of the Background section, page 8) expands upon the definition of Physical Access Control System. A badge reader that stores data and independently performs access authentication would not likely be vulnerable to tampering and would pose less risk than a badge reader that could be remotely accessed through a network. Suggest striking “does not contain or store access control information or independently perform access authentication“ and replacing with “does not communicate using a routable protocol.” (Comment 2) In Measures for 1.2 and 1.3, recommend striking “card reader” from the phrase “card reader logs.” (Comment 3) In Measure for 1.6, please replace both instances of “Physical Security Perimeter” with “Physical Access Control System” to align with the requirement.
Yes
No
Yes
No
No
(Comment 1) Implementation plans must be revised sometimes due to testing results, new information or operational factors. In R2.4, do "CIP Exceptional Circumstances" provide entities with the latitude to revise implementation plans and timeframes if necessary? If not, please add the following to R2.4, "Document the execution status of any remediation or mitigation action items, including any changes to the plan or timeframe." (Comment 2) R4.1 – recommend changing “each of the following types” to “each of the following types that the system is capable of detecting and logging” in order to clarify SDT’s intent as indicated in both the Measure and the Guidance. (Comment 3) Measure for 4.3, suggest replacing “events” with “failures” for clarity.
For clarity, suggest changing R5.7 to read “Generate alerts after a threshold of unsuccessful login attempts or limit, where technically feasible, the number of unsuccessful authentication attempts.”
Individual
Jim Howard
Lakeland Electric
Yes
Yes
Yes
Yes
No
No
No
see comments submitted by FMPA through the formal comment process
see comments submitted by FMPA through the formal comment process
Yes
Yes
see comments submitted by FMPA through the formal comment process
see comments submitted by FMPA through the formal comment process
No
No
No

see comments submitted by FMPA through the formal comment process
No
Yes
Yes
No
No
see comments submitted by FMPA through the formal comment process
see comments submitted by FMPA through the formal comment process
Group
Dominion
Connie Lowe
Yes
No
No
No
Yes
No
No
CIP-004-5 R2 - The language in 2.9 (Training content on response to BES Cyber Security Incidents.) dupicates a portion of the language in 2.7 (Training content on identification of a potential BES Cyber Security Incident and initial notifications in accordance with the entity's incident response plan). Part 2.9 should be deleted in its entirety. CIP-004-5 R3 - Part 3.1 should be revised to remove the "and documentation" wording documentation is a measure and proof of compliance of execution of the requirement. Also, training is required prior to granting authorized unescorted physical access OR authorized electronic access. The proposed wording is: "Require completion of the training specified in CIP-004-5, Requirement R2 prior to granting authorized electronic access or authorized unescorted physical access to applicable systems, except during CIP Exceptional Circumstances." CIP-004-5 R4 - The first sentence of Part 4.2 should be revised to "consecutive" months for clarity as follows: "Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six consecutive months or more:" - In Part 4.4, the order of the words "criteria" and "process" is inconsistent with Part 4.3. For consistency, the words in the requirement should be reordered as follows, "Process or criteria for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4, Parts 4.1 through 4.3"
CIP-004-5 R6 - Part 6.1 should allow for role-based designations. The first sentence should be revised as follows, "Designate one or more individual(s) or role(s) to authorize:" - Part 6.2 can be simplified for clarity and intent by removing the clause "required work functions". The language of the requirement should be changed as follows, "The individual(s) or role(s) designated in Part 6.1 shall authorize electronic access deemed necessary by the Responsible Entity, except for CIP Exceptional Circumstances." - Part 6.3 can be simplified for clarity and intent by removing the clause "required work functions". The language of the requirement should be changed as follows, "The individual(s) or role(s) designated in Part 6.1 shall authorize unescorted physical access deemed necessary by the Responsible Entity, except for CIP Exceptional Circumstances." - Part 6.4 needs to be clarified; electronic "locations" is not a typical term and should be replaced with "repositories". The language of the requirement should be changed as follows, "The individual(s) identified in Part 6.1 shall authorize access to the designated physical and electronic repositories where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determines are necessary for performing assigned work functions, except for CIP Exceptional Circumstances." - Part 6.5 should be limited to individuals who are CURRENTLY provisioned to limit the scope of the review. The review isn't intended to perform a reconciliation of all individuals who may have gained and lost access during the review period. The language of the requirement should be changed as follows, "Verify at least once each calendar quarter that individuals currently provisioned for authorized electronic access or authorized unescorted physical access have associated authorization records" - Part 6.6 is too broad by using the

word "all" with regard to user accounts rather than "applicable". The language of the requirement should be changed as follows, "For electronic access, verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all applicable user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines necessary for performing assigned work functions." - Part 6.7 needs to have the word "privileges" inserted into the stated requirement after the word "access" to be consistent with the change rationale as well as have confirming language applied to electronic "locations". The language of the requirement should be changed as follows, "Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, that access privileges to the designated physical and electronic repositories where BES Cyber System Information is stored by the Responsible Entity are correct and those that the Responsible Entity determines necessary for performing assigned work functions." CIP-004-5 R7 - Part 7.3 should be updated with conforming language using the term "repositories" as a result of changes suggested for previous requirements as follows, "For termination actions, revoke the individual's access to the designated physical and electronic repositories where BES Cyber System Information is stored by the Responsible Entity by the end of the next calendar day following the effective date and time of the termination action" - Part 7.4 Applicability should include "Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity" for consistency with 7.1 through 7.3 CIP-004-5 GUIDANCE - Access revocation timing requirements associated with the death of an employee should be treated similar to a 'normal' termination and not be treated similarly to a 'for cause' termination.
No
No
CIP-005-5 R1 - The applicability column for Part 1.1 should include the items in Part 1.2 which are High Impact BES Cyber Systems with External Routable Connectivity, Medium Impact BES Cyber Systems with External Routable Connectivity, Associated Protected Cyber Assets applicable to High and Medium Impact BES Cyber Systems with External Routable Connectivity. - The requirement for Part 1.1 should remove the reference to Associated Protected Cyber Assets. The revised language of the requirement is, "All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP. " - The Measure for Part 1.1 includes all Cyber Assets, but the Applicability includes only BES Cyber Systems. Either the Applicability needs to be extended to Associated Protected Cyber Assets or the Measure needs to be restricted to BES Cyber Systems.
CIP-005-5 R2 - The "Technical Feasibility" language is included in the header of standard (which is about developing processes) and seems to imply that technical feasibility exceptions can be taken for any of the Parts. It isn't possible to take a technical feasibility exception for the development of a process; however, it is possible to take a technical feasibility exception for the technical components required in the Parts to the Requirement. For clarity, we recommend the technical feasibility language be applied to each of the Parts of the requirements (see examples below) and removed from the header. The proposed language for the requirement is, "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items...". - Part 2.1 requires clarity because cyber assets themselves cannot initiate Remote Interactive Sessions. The language of the requirement should be simplified to, "Utilize an Intermediate Device such that the Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset, where technically feasible." - In Part 2.2 the portion of the sentence after "intermediate device" is editorial and can be moved to Application Guidance as it doesn't add value to the requirement. The language of the requirement should be changed to "Utilize encryption for all Interactive Remote Access sessions that terminate at an Intermediate Device, where technically feasible."
No
No
Yes
CIP-006-5 ALL - Parts 1.2 and 1.3 as worded would prevent an escorted person from entering the PSP. The language of the requirements needs to be clear that escorted individuals are able to enter a PSP. The phrase "and their associated visitors" should be added to the end of each of the requirements to correct. As an example, Part 1.2 would be rephrased as " Utilize at least one physical access control to allow physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access and their associated visitors." - The

measures of Parts 1.2 and 1.3 need to be updated to reflect escorted visitor access. The language of the measure should be changed as follows, " Evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how access is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs and/or visitor logs." - The degree to which the controls in Part 1.4 aren't clear and when combined with the 99.9% availability, make the Part impossible to comply with. For example, an entity might have to monitor for individuals breaking through a concrete block wall or digging a tunnel to break in through a floor. "Have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized circumvention of a physical access control into a Physical Security Perimeter." We suggest the language be reverted to the language in CIP006-4c, R5. - Part 1.5 should be changed for clarity by replacing the words "unauthorized circumvention" with "tampering". The revised language of the requirement should be "Issue an alarm or alert in response to detected tampering of a physical access control into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection." - Parts 1.6 and 1.7 can be merged into Parts 1.4 and 1.5 respectively. - Change Part R1.7 to "Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the detection of unauthorized access." The word "detection" is required to clarify when the clock starts for determining compliance. - Simplify Part 2.1 by stating that any unauthorized individual is to be escorted. The revised language should be, "Require continuous escorted access of all individuals not authorized for unescorted physical access within each Physical Security Perimeter, except during CIP Exceptional Circumstances."
No
Yes
Yes
Yes
No
CIP-007-5-R1 - Part 1.1 requires clarification. The old language included "ports and services" whereas the new language includes "ports or services". The intent is only to track logical ports and related services. The following language should be used for the requirement, " For applicable Cyber Assets and where technically feasible, enable only logical network accessible ports needed, including port ranges and related services where needed to handle dynamic ports. " - Part 4.1 replace the first sentence with "Log events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, per device capability, each of the following types of events." to better clarify that the requirement is limited per the capability of each of the devices in the Cyber System. - The language of Part 4.2.1 should be replaced with "detected cyber security event; and" since not all events are necessarily malicious. - Part 4.3 should be reworded as "Activate a response to a human detected event logging failure before the end of the next calendar day" to clarify that the clock needs to start upon a person picking up the notification, not when a system identifies the problem. - The wording in Part 4.5 should be changed to "Review a summarization or sampling as deemed appropriate by the Responsible Entity at a minimum every two weeks to identify undetected Cyber Security Incidents. " Rationale: It should be clear that the entity determines which logs should be reviewed or sampled to avoid confusion during audits.
CIP-007-5-R5 - Replace Part 5.1 with "Enforce authentication of all user account access, where technically feasible" to clarify that the access is electronic access and not physical access and to clarify that the requirement is to validate the accounts and not who is using the accounts (which is technically infeasible). Also, the applicability of the requirement should be limited High and Medium BES Cyber Systems with External Routable Connectivity. - Part 5.4 should be replaced with "Change known default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on Cyber Assets.". The addition of the word "known" is required to address system accounts that are not available to be changed without requiring a TFE. An example of such an account is the Windows "system" account. Also, the first measure should be changed to "Records of a procedure that passwords are changed when new devices are in production". Devices may be deployed, but not actively operating in production until their configuration is completed in the production environment. - The measures of Parts 5.5 and 5.6 should be modified for clarity of intent by replacing the second bullet with "Attestations that include a reference to the documented

procedures that were followed." The phrase “by individuals” is extraneous and the documented procedure will define the password parameters. The Application Guidelines for these requirements should also note that a single attestation may be used for both group of individuals performing password updates and groups of like assets that follow the same documented procedure. - Part 5.7, as written, is not recommended as it would create a potential vulnerability in the form of a Denial of Service attack. Limiting the language to "user accounts" eases this concern. The proposed language for this requirement is "Limit, where technically feasible, the number of unsuccessful authentication attempts for user accounts or generate alerts after a threshold of unsuccessful login attempts for all accounts."
Group
NESCOR/NESCO
Annabelle Lee
No
No
No
No
R3: Users of low impact BES cyber systems/assets also need basic cyber security training. Consider revising the training requirement to include basic cyber security training for all individuals. R4.2: The requirement only states criminal record checks and not other checks, such as random drug and alcohol testing. When people are drugged and/or intoxicated with alcohol, they may do things unknowingly, such as disclosing confidential information, losing confidential documentation and critical systems, and/or making improper judgments when running BES systems. Furthermore, drug and alcohol testing is reasonably commonplace in other industries and reasonable for both cyber security and safety. There should be consideration in this requirement to include drug and alcohol testing within the constraints of state laws and collective bargaining agreements. R4.4: It may be difficult to find contractors or vendors who have performed all the criteria listed in R4 (Personnel Risk Assessment Program). In many cases, these contractors and/or vendors, have been working for utilities for many years without any background or criminal check. What if the utility cannot get all that information? What if a utility finds something from the criminal record of a contractor who has been with them for several years? In these cases, what should the utility do? Additionally, must vendors be authorized to provide criminal background check information to the utility for their employees, which would require permission from the employee? Or can the vendor assert to the utility that it has obtained and verified this information in accordance with the CIPs? Current practice is to have the vendor and/or contractor attest to the fact that background checks (in accordance to the requirement) have been completed. Leveraging the TWIC program or creating a similiar program specific to the electric sector would lead to a consistent approach to 3rd party background screening and potentially reduce industry work effort on this activity.
R7.4 and 7.5: The requirements 7.4 and 7.5 allow time to remove physical and logical access privileges. Requirement 7.1 requires that termination procedures be initiated immediately. 7.4 and 7.5 allow a malicious individual time to initiate an attack.
No
No
There is no clear requirement that non-routable communications between two ESPs, such as between a substation and control center, be encrypted or have their integrity assured. Technical solutions exist to secure serial SCADA communications, both in the form of proprietary vendor products, as well as standards such as IEEE 1711 (developed from AGA12) and Secure DNP3. We suggest that all non-routable persistent communications links between ESPs be protected with strong encryption and integrity. Furthermore, the endpoint devices providing the encryption and authentication should be considered part of the ESPs and subject to all other CIP requirements for cyber assets belonging to an ESP. The lack of commercially available perimeter security solutions for non-routable protocols, pointed out in the Application Guidelines for CIP-005-5, further emphasizes the need for cryptographic protection of serial links. NERC's Consideration of Comments does not address this comment. This comment directly addresses point 86 in FERC 18 CFR Part 40 approving CIP v4, which states "…we support the elimination of the blanket exemption for non-routable connected cyber systems…" R1.3: We agree with identifying and documenting a business purpose for all inbound and outbound access from an EAP. However, this requirement should distinguish access through different

kinds of perimeters: 1. EAP allows traffic in/out over an encrypted link to/from another EAP owned/operated by the same entity; 2. EAP allows traffic in/out over a private but unencrypted link (eg. MPLS, point-to-point microwave) to/from another EAP owned/operated by the same entity; 3. EAP allows traffic in/out over an encrypted link to/from a system or EAP owned/operated by a different entity; 4. EAP allows traffic in/out over a private but unencrypted link to/from a system or EAP owned/operated by a different entity; 5. EAP allows traffic in/out over the public Internet. These cases involve differing degree of risk, with cases 1 and 2 being generally reasonable and justifiable; cases 3 and 4 utilities risky and avoidable with appropriate VPN technology, and case 5 being of far too high a risk to be acceptable, in our opinion, for any business purpose. A comment in the summary of changes for R1 states that "the non-routable protocol exclusion no longer exists". However, R1.1 and R1.2 all provide exclusions for non-routable protocols. We note that exclusions that existed in draft 1 R1.3 and R1.5 have been removed. There also remain exclusions in CIP 007 R1 and R4. We recommend removing all non-routable protocol exclusions, as the summary of changes claims. Despite the many changes in the language there is still too much ambiguity. "A method" for detecting communications is only also only half of the equation. There should be a method for detecting and addressing or mitigating detected anomalies. Perhaps a better phrasing would be: "Document and implement methods for detecting and addressing communications that have the characteristics of malicious or unexpected activity."
No
No
R1: As stated, "Define operational or procedural controls to restrict physical access." How is this consistent with the little or no security requirements for low impact systems? Also, as stated, low impact systems do not have to be uniquely identified. R3: NERC could consider adding a requirement to retest if the system fails.
No
No
No
No
No
R1: Table R1 is referred to as Ports & Services, but the controls are all about Ports, and there are no controls about services. NERC could consider either removing the reference to services or introduce a control to require an analysis of which services are running, and to disable or remove any services that are not necessary. Since Draft 1, the word “services has been added to the Requirements, but this does not address the point of this comment. Under the Guidelines and Technical Basis for Requirement R1, 1.1 the draft states “. . . therefore it is the intent that the control be on the device itself; blocking ports at the perimeter does not satisfy this requirement”. This seems to exclude the use of an intermediate device immediately preceding/inline with the device, thereby removing a valid security defense mechanism. Inline security mechanisms where no path around them exists enable security functionality to be placed in a manner to ensure they are engaged and also allow multiple solutions to be used where existing systems lack protection. An example would be a dedicated firewall and IPS system placed directly between a critical system and all connections, ensuring they are in the path of all traffic and allowing specialized security functions not available on some systems. A rewording of the quote above would add the option of providing non-bypassable security controls. “. . . therefore it is the intent that the control be on the device itself, or positioned inline in a non-bypassable manner; blocking ports at the perimeter does not satisfy this requirement”. R2: Patch management could also be considered for low impact systems. If the same operating system or application is used on low and medium/high impact BES systems, the patch should be applied to all the systems to mitigate the vulnerability. R2.1: This requirement states the need to identify the source or sources to be monitored for security patches, updates, etc. However, there is no mention of how frequent the responsible entity should be conducting this activity. It can be inferred from R2.2 that this activity must be conducted, at a minimum, every 29 days or less; however, as written, compliance is limited to identifying a source or sources and does not account for how often monitoring is to be conducted. If the intent is to have the responsible entity frequently monitor the identified sources so security patches, updates, etc. are discovered within 30 days of their release then the requirement should be more clear as to the monitoring expectations. As stated, "Update malicious

code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns)." This requirement is specific to profiles. There are other techniques that address anomaly-based behavior analysis and heuristics based analysis/detection. NERC could consider revising the requirement to address other types of malicious code detection. R3.3: Previous draft stated 30 days between updates, this version increased it to 35 days. Again, 35 days is a lifetime when considering updating signatures/pattern files to malicious-code protection tools. Consider shortening this to a lesser period of time that is commensurate to the risk. The current requirement statement is long and confusing as well. Consider breaking it up into multiple sentence with clear requirement statements. R4: As stated, "Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert." This is not specific to cyber security. Is that the intent? R4.2: There is still no requirement within the set of CIP standards 002-5 through 011-5 that make it clear that trained, knowledgeable and aware people are essential to making a security logging system fully functional. CIP-004-5 training requirements mention role-based training but without specific descriptions a responsible entity could have the alert analysis (and the R4.5 summary review) accomplished by an administrator who has no training or skills to perform such activity. Effective security log management requires aware and skilled personnel watching the log systems and output.
R5.2: As stated, "The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types." How implement least privilege and other security controls if they are not defined in policy? This does not restrict the use of administrator, shared, etc. account types. These could be limited based on least privilege and need to know. As stated, "Identify individuals who have authorized access to shared accounts." Why only shared accounts? Consider identifying individuals with privileges – particularly those with access to administrator accounts. It is particularly important to identify administrators with privileges to modify the software itself. For example, I was unable to find a requirement in the standard that would discourage combined accounts for both operating and modifying software. CIP mitigations against malicious software currently appear limited to detection methods in CIP 010 - this would strengthen that position and is an auditable special case of least privilege in accordance with NIST 800-53 AC-6 control enhancement 2, which is required in the NIST baseline for moderate and high impact systems. It reads: "The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined list of security functions or security-relevant information], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions." For CIP, at a minimum, "modification of software executing on medium or high impact BES systems" could be filled in the square brackets of this NIST requirement.
Group
FirstEnergy
Doug Hohlbaugh
Yes
Yes
Yes
Yes
Yes
No
No
We suggest modifying R2, part 2.7 to incorporate both training on “identification and response” and eliminating part 2.9. Our suggested re-write for R2, Part 2.7 is “Training content on identification, initial notification and response of a potential BES Cyber Security Incident in accordance with the entity’s incident response plan.” If this change is agreed to, conforming changes are also required to the Measure for part 2.7 to capture the inclusion of response.
(1) R6, parts 6.1, 6.2 6.3 and 6.4 we recommend replacing the word “designate” with “identify”. The term designate could cause confusion and need for interpretation as to who designated the authority to an individual(s) for authorizing access. This designation does not appear to be in the spirit of CIP-003-5 R5 (CIP Sr. Manager Delegate) nor should it be, therefore we recommend the change to “identify”. (2) In R6, part 6.5 related to the quarterly reviews of access provisions, the standard should permit a “find and fix” or “corrective action” approach for inadvertent access provisions that

are “found and fixed” based on two conditions – a) the error is corrected during the next quarterly review period occurring after initial access provisioning is granted and b) access to the area(s) provisioned was never used. Inadvertent access provisions can sometimes occur for employees having the same name (e.g. relatives Jr. vs. Sr.) and if identified and mitigated in a timely manner (next quarter) there should be no noncompliance if no actual reliability threat (no actual access) has occurred. As written, the standard promotes zero tolerance and is outside the spirit of these quarterly access reviews. (3) R7, part 7.1 - We do not support a need to revoke all access within 24-hours. This requirement is overly burdensome – especially in the case of trusted employee transfers who pose no real reliability threat. The 24-hour termination should be limited to “for cause” terminations of employment and additional flexibility built in for other situations (transfers, retirements, etc.) Consider and “equally and effective alternative” to the immediate terminations directed by FERC. If the concern from FERC is that the seven day period is too long then maybe some middle ground (3 business days) can be struck for the transfers and retirement scenarios. This requirement as written has the potential for numerous violations with questionable reliability benefit.
Yes
No
R2, Part 2.1, 2.2 and 2.3 require use of an Intermediate Device, encryption and multi-factor authentication, respectively. The requirements apply to Medium Impact BES Cyber Assets with no additional qualifiers; therefore it appears these would apply to all Medium BES Cyber Assets, even those with no external connectivity. These requirements should be limited to Medium BES Cyber Assets with External Routable Connectivity. Left unchanged will bring into scope a significant increase of cyber assets with no remote access capability for which the requirements are not feasible. Furthermore, the authentication for Medium BES Cyber Assets with dial-up connectivity is covered in CIP-005 R1, part 1.4 and CIP-005-5 R2, part 2.3, applicable to all Medium BES Cyber Assets, describes a need or multi-factor authentication and appears to be in conflict with R1 part 1.4.
No
Yes
Yes
FE’s concern with CIP-006-5 is requirement R1, part 1.4 which obligates a responsible entity to have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability). The requirement while well intended will likely lead to need for interpretation or guidance on the calculation of the 99.9% metric. For example, what is being measured the central monitoring station, the access panel controlling multiple points of entry at a substation, each door alarm or motion detector? Also, on what periodicity is the 99.9% stat based on? Is it an annualized calculation, intended to be a continuous running total 99.9% threshold? In summary, if kept, more guidance is required for how we measure and the period used for calculating the availability stat.
Yes
No
No
No
No
R2 (all parts), R3 (all parts), R4 part 4.1- these requirements deal with patch management, detecting and mitigating malicious code, logging and investigating cyber security incidents. The requirements apply to Medium Impact BES Cyber Assets with no additional qualifiers; therefore it appears these would apply to all Medium BES Cyber Assets, even those with no external connectivity. These requirements should be limited to Medium BES Cyber Assets with External Routable Connectivity. Left unchanged these will bring into scope a significant increase of cyber assets with no remote access capability for which the requirements are not feasible. Performing the requirements without remote diagnostics or service capability will require on-site visits to hundreds of remote substation locations to address a threat which can only be applied locally and having no ability to propagate to other BES locations. FE respectfully requests that the drafting team revise the applicability as requested above or provide the technical rationale for including cyber assets with no remote connectivity.
R5 part 5.1, 5.2 and 5.4 these requirements relate to enforcing access authentication, enabling

default or generic account types and revising default passwords. In regards to the Medium BES Cyber Asset applicability, FE believes it is important to limit to Medium BES Cyber Assets with external routable connectivity. Additionally, the applicability in question appears to be out of synch with CIP-004-5 R6, part 6.2 at least in regard to CIP-007-5 R5, 5.1. If the team believes dial-up should also be included, it would be an improvement over the existing draft text which includes cyber assets having no remote connectivity.
Group
MRO NSRF
WILL SMITH
Yes
No
No
Yes
Yes
Yes
No
: [R1] Though we recommend changing “ongoing reinforcement of cyber security practices” to “ongoing reinforcement of security practices” to prevent limiting awareness messages to cyber to the exclusion of physical security awareness, as well. [R2] Each type of role-based training, Part 2.2-2.10, should be optional for some identified roles and required for others, and that distinction should be programmatically documented. That needs to be clearer in the structure of this requirement. If each of Part 2.2 through 2.10 were preceded with “Based on the role identified in Part R2.1…“ The way this is written today, it appears as though all of this training is required for anyone with any type of access. Additionally, some of this training should not be given to someone before the access is granted, based on the sensitivity of the information. Recovery information, for example, should wait until the access is completely authorized and the person has met all prerequisites and other operational training. [R3] Legacy phrasing with regard to the date overall training is required was sufficient as long as it was broad enough to educate those granted physical or electronic access. More specific, role-based training should be provided within an appropriate timeframe after acquiring certain responsibilities and should be necessary for retaining those responsibilities. The date of the acquisition of those responsibilities should be tied to departmental documentation and roles/responsibilities lists instead of HR reports on official job change. This allows for transitions required by reliable operations, as well as training periods. Also, with respect to demonstrating training when the access is attained, it forces the entity to maintain a complete history for each person who has ever had access and what training he or she has received since the very first access was obtained. This could be decades worth of training materials, so we’d support the addition of a retention guideline that refers to access attained since the last audit. [R4]With respect to demonstrating initial PRA when the access is attained, it forces the entity to maintain a complete history for each person who has ever had access and the PRA he or she had when the very first access was obtained. This could be decades worth of PRA materials, so we’d support the addition of a retention guideline that refers to access attained since the last audit.
[R7.2]: Too short a time span. Recommend returning to legacy timeframes for job changes within an organization or extending the allowable timeframe based on business days instead of calendar days. For a job change, there is no urgency associated, so weekend access removals are unnecessary. Additionally, there need to be provisions within the Standards for situations where a person will need to straddle two jobs until a replacement is up to speed. [R7.3]: Too short a time span. Recommend extending the allowable timeframe based on business days instead of calendar days. The access removals associated with 7.1 should be sufficient to compensate for the risk introduced by waiting through a weekend for information access removals. [R7.4]: If 'revoke' in this case means to 'delete' the user account from the system, we disagree. We would disable the account and possibly change the account password but when you delete a Windows account you can never reclaim the original GUID that Windows assigns to the unique account. Therefore, reporting, file ownership and anything relating to the GIUD will have been lost and difficult to track past account activity. This may be true for other operating systems as well. : If disabling their domain accounts and physical access effectively terminates access, do we still need the urgency of 24 hrs? I understand the logic behind this but would rather see this as a 30 day requirement. [R7.5]: The "out" for extenuating operating

circumstances should be applied to all CIP 4 R7 requirements.
No
Yes
[R1.1] Proposed verbiage change for the applicability. [R1.1] “All BES Cyber Assets…” should apply to BES Cyber Assets associated with High and Medium Impact Sites that have external routable connectivity. There should not be an obligation to create an ESP with an EAP around an otherwise isolated network. This ties into the proposed definition for ESP and should be considered along with that proposed definition. [R1.2] Recommend combining 1.1 and 1.2, after the changes to the applicability and definitions are completed. [R1.5] Change applicability verbiage to Electronic Access Points associated with ESPs at High Impact Sites and Electronic Access Points associated with ESPs at Medium Impact Control Centers. The requirement is very subjective and may not be feasible for encrypted communications. This requirement needs to be clarified or stricken.
NONE
No
Yes
Yes
: [R1.2] Ensure applicability statements clarify that the associated EAC and Protected Cyber Assets are those associated with Medium Sites. [R1.4] –The identified percentage requires a level of tracking for monitoring that may not be technically feasible. Additionally, a .1% down time for monitoring security will accumulate for monthly planned outages to implement patches so would like to see allowances for this. A percentage uptime figure should be removed from the standard. Placing specific values such as this should not be included in standards and are audit bait that auditors will try to prove rather than focusing on overall security posture. If an entity can show all outages and maintenance and associated compensating controls during the outage, this is sufficient control, as is required in R3.2 already. Proposed Verbiage: Have controls that monitor the PSP 24X7 with mechanisms for identifying and documenting planned or unplanned outages. [R1.5]: Recommend striking the reference to “within 15 minutes of detection” and, instead, require the documentation of appropriate response timing within incident response plans. [R1.6] The identified percentage requires a level of tracking for monitoring that may not be technically feasible. Recommend have controls that monitor the PSP 24X7 with mechanisms for identifying and documenting planned or unplanned outages. [R1.7]: Recommend striking the reference to “within 15 minutes of detection” and, instead, require the documentation of appropriate response timing within incident response plans.
Yes
No
No
No
No
Ensure the “zero defect” language in the VSLs is changed to be in alignment with EEI comments and the requirements, themselves. R1 – Consider exempting routable protocol on Medium Impact facilities for all CIP-007 R1 sub-requirements to maintain consistency. As currently drafted, some sub-requirements in R1 are exempt from routable protocol whereas others are not. Refer to the “Change Rationale” provided by the drafting team in R5.6 for the justification for this change. In all applicability columns, (CIP-007) where medium impact facilities are included, recommend including “with external routable connectivity”. [R1.1] Propose defining “network accessible” to clarify the requirements around the additional controls offered by firewalls and ports accessible only to the local host and whether those controls can be considered sufficient. Also recommend adding the routable connectivity qualifier on the whole of R1, including High and Associated cyber assets. [R2] Although LES recognizes the revision as a good idea, we question whether including the monitoring of all installed cyber asset manufacturers is feasible. [R2.3] Recommend removing the term “dated” from the action plan to allow waiting for an outage or window that is not yet scheduled. [R2.4] Recommend adding flexibility to change the plan without risking non-compliance. Proposed Verbiage – “For each plan created or revised in 2.3, document the actual implementation date and the reasoning for any discrepancies between the planned and actual implementation.” [R3 – R3.3] should be revised to account for the differing methods that can be utilized as part of R3.1. As an example, per R3.1, a company can use policies as a method to deter, detect, or prevent malicious code. If a company were

to adopt policies as their method, R3.3 would not be applicable as there would be no malicious code to update. [R3.3] This applicability should be limited to just those systems with External Routable Connectivity. Without that connectivity, the monthly signature updates are not commensurate with the actual risk. [R4.1], the Measure includes the phrase “is capable of detecting”. LES supports this phrase and believes it should be incorporated into the Requirement so companies are not required to replace equipment. Additionally, the “as a minimum” included in R4.1 seems to contradict the understanding of the Measure. [R4.1]Proposed Verbiage: “Within the capabilities of the BES Cyber System, log events such that Cyber Security Incidents can be identified and investigated. Event types include: …” [R4.2] Proposed Verbiage: “Within the capabilities of the BES Cyber System, generate alerts for detected security events that the responsible entity…” [R4.3] Recommend striking this requirement or changing the verbiage to “Document the controls implemented to identify and respond to detected logging failures. Document detected logging failures along with any discrepancies between the actual response and the documented response plan.” [R4.4] Proposed Verbiage: Remove “Where technically feasible” and precede requirement with “Within the capabilities of the BES Cyber System. [R4.5] Ensure “High” is a qualifier for each of the systems identified in the applicability column. Proposed Verbiage to add clarity: “Document and implement a program to review a summarization or sampling of logged events, at a minimum, every two weeks, to identify un-alerted Cyber Security Incidents.” Rationale – with the documentation of a program, the entity can define the criteria for sampling and summaries without risking a finding of non-compliance when not meeting the interpretation-based expectation of an auditor.
[R5.1] Propose change to “within the capability of the BES Cyber System” instead of “technically feasible.” [R5.2] The CIP Senior Manager will not have the technical expertise to recognize the actual risk introduced by the presence or quantity of default or generic account types. The turnover rate at the organizational level at which this level of expertise exists would create a prohibitively administratively burdensome process without adding the desired oversight. Recommend striking this requirement or changing to allow designation similar to CIP-004 R6, without direct documentation ties to the Sr Mgr. [R5.4] Recommend changing “technically feasible” language to “within the capabilities of the system or allowable by support vendors.” Proposed Verbiage: “To the extent allowable by the support vendors and capabilities of the system, change default passwords, unless the default password is unique to the device or instance of the application.” Removed “on cyber assets” to align with the cyber system applicability column. [R5.5] Proposed Verbiage for 5.5.1: “Password length that is, at least, eight characters or the up to the maximum allowable by the system if that maximum is less than eight.” Carry this change through 5.5.2 to add clarity. [R5.6] Don’t touch this one – it’s great as it is. [R5.7] Recommend changing technically feasible language to “Where system capability or operational risk allow, limit the number of unsuccessful…”
Group
Southern Company Services, Inc.
Antonio Grayson
Yes
Yes
Yes
No
Yes
No
No
(1) Across all standards, the Measures need to be listed as “Examples” and be in a bulleted list “or” format. (2) Across each table in CIP-004-5, the table column header currently labeled “Applicable BES Cyber Systems and associated Cyber Assets” needs to be relabeled “Applicability” for consistency across all CIP standards. (3) Regarding CIP-004-5, R2, Southern suggests that it would be helpful if there was additional clarity around who must be trained, namely: “personnel with approved unescorted access or approved electronic access must have been trained.” (4) Regarding CIP-004-5, R3, Southern suggests removing the requirement of documentation as documentation is usually the measure. (5) Regarding CIP-004-5, R4, Southern believes that a timeline needs to be established. In 4.2, add “consecutive” before “six months or more”. Rationale: a support person, over a period of years, could accumulate six months in total. (6) Regarding CIP-004-5, R4, 4.2.1, 4.2.2 and 4.2.3 should be changed to a bulleted list. In 4.2.2 change the “and” to “or”. (7) Regarding CIP-004-5,

R4.1, this ‘bootstrap’ type requirement should be audited once per individual. As written, it would require the retention of this initial PRA for each individual forever. The requirement needs a maximum retention time per individual. (8) Regarding CIP-004-5, R4.1 needs a grandfathering provision (possibly in the implementation plan) for currently approved personnel. Rationale: Anyone with a documented background meeting the NERC CIP background requirements within the last seven years should be considered as already meeting the requirement. NERC CIP version 5 should not require that new background investigations be completed for those personnel who already have valid background documentation. (9) Regarding CIP-004-5, R4.3 and R4.4, the phrase “criteria or process” should be consistent between R4.3 and R4.4.
(1) Regarding CIP-004-5, R6, the rationale includes the important note that R6 does not apply to BES Cyber Systems that do not have user accounts defined. This needs to be included in the requirement itself rather than the rationale. (2) Regarding CIP-004-5, R6.1, change "designate" to "designate by name, role, or title" to clarify that entities can designate by title or role. (3) Regarding CIP-004-5, R6.2, “need to know” may be difficult to prove during an audit and represents a security guideline or rule of thumb that will be subject to varying interpretations. Southern suggests returning to language which demonstrates personnel have been “approved for access”. Southern believes that having approved approvers who grant all access is proof that :need to know" is considered for each request. (4) Regarding CIP-004-5, R6.3 implies that evidence of determination of need for performing work functions is needed for each physical access. Documentation of all roles and activities in advance is difficult for unescorted individuals. Southern suggests removing the words “that the Responsible Entity determines is necessary for performing assigned work functions” from the requirement. (5) Regarding CIP-004-5, R6.4, the SDT should consider whether this would include offsite storage of encrypted backup media or information being sent via postal service? If so, no entity can comply with the generic nature of this requirement. Southern suggests that the use of generic terms like “location” be struck and replaced throughout the standard as it applies to information protection with “designated repositories”. A similar change is required for R6.7. (6) Regarding CIP-004-5, R6.5, change “individuals provisioned” to “individuals currently provisioned” to eliminate from scope those who were provisioned but no longer need access. (7) Regarding CIP-004-5, R6.6, does "all user accounts and groups" on an EACM include all groups that may have nothing to do with CIP? If not, Southern suggests replacing "all" with “BES Cyber System” and clarifying intent within guidance and measures. (8) Regarding CIP-004-5, R6.6, in general, in terms of information management, “locations” needs to be replaced with “designated repositories” along with a requirement to list the repositories. The rationale for this change is that a location could be interpreted to be a car or an ipad, etc. For the purposes of information protection, designated repositories should be established. (9) Regarding CIP-004-5, R6.6, within the wording of the Measure, replace “Evidence may include, but is not limited to, documentation of the review including:” with “Example of the review of applicable cyber systems:”. (10) Regarding CIP-004-5, R7, 7.1, not all terminations are of equal risk (such as employee death). Southern strongly suggests restricting the tightest timeframes for deprovisioning to those terminations of higher risk, such as for cause terminations. In 7.2, the timeframe for completion of the activity should be based on the notification of re-assignment or transfer. In 7.3, the focus needs to be changed from "locations" to "designated repositories." In R7.4 – change "revoke" to either "remove or disable". In R7.5 – Southern recommends having the quarterly review be the cleanup of individual user accounts and not be considered a violation.
Yes
Yes
(1) Regarding CIP-005-5, R1, Southern suggests adding guidance to allow for implementation of IDS anywhere, internal or external to an ESP. Additionally, it’s not clear exactly how wireless networks are potentially impacted by CIP-005. (2) Regarding CIP-005-5, R1.1, the Measures should call for BES Cyber Systems to be documented rather than every component. (3) Regarding CIP-005-5, R1.4, if an entity does not use dialup, is a program required to authenticate dialup access? Consider using "if applicable" in the requirement. (4) Regarding CIP-005-5, R1.5 needs clarification on the path to be protected: internal, external, or both internal and external, and inbound and/or outbound.
(1) Regarding CIP-005-5, R2, clarification is needed that if "where technically feasible" occurs in the overall Requirement statement that it equally applies to all items in the subsequent table. (2) Regarding CIP-005-5, R2.2, the sentence in requirement should end after "Intermediate Device". The remainder of the sentence relates to overall rationale and not a requirement. (3) Regarding CIP-005-5, R2.3, clarification is needed that the two-factor authentication is to the Intermediate Device only.

No
Yes
Yes
(1) Regarding CIP-006-5, R1.2 and R1.3 as worded prevents escorted personnel from entering a PSP. Southern suggests deleting the word "unescorted" and clarifying that escorted personnel are authorized in this instance. (2) Regarding CIP-006-5, R1.3 needs clarification that multi-factor authentication, such as a physical badge and a biometric on the same access control system, is acceptable. (3) Regarding CIP-006-5, R1.4, measuring the 99.9% availability as included within the requirement causes more issues than it solves. Southern strongly suggests striking the 99.9% availability concept and language from all requirements and replacing it with the outage response requirements, including human observation, similar to the electronic monitoring requirement in CIP-007-5 R3. Additionally, Southern suggests noting that R3.2 implies that R1.4 is not necessarily 24x7 to allow for normal activities and unplanned outages. (4) Regarding CIP-006-5, Southern supports EEI's comments and strongly suggests returning to the monitoring of defined access points rather than the monitoring of perimeters. R1.4 needs to be deleted and R1.5 needs to be changed to “identified unauthorized access”. (5) Regarding CIP-006-5, R1.6 and R1.7 can be deleted if PACMS are added to the applicability column of R1.5. Therefore, Southern suggests removing R1.6 and R1.7 and putting PACMs in the applicability of R1.5.
Yes
Yes
Yes
Yes
No
(1) Regarding CIP-007-5, R1.1, Southern beleives that the measures for R1.1 do not satisfy the requirement. The Measures need to be reviewed to ensure the meet the requirement. The first measure should be deleted. (2) Regarding CIP-007-5, R2.2 and R2.3, the 30 calendar days needs to be changed to 35 calendar days to allow for coverage of monthly reports. Additionally, Southern believes there is an issue of double jeopardy between R2.2 and 2.3 that needs to be resolved. (3) Regarding CIP-007-5, R2.4, Southern believes that there is an issue of double jeopardy that needs to be resolved. Is the failure to implement in R2.4 also a failure of the "implement" in the overall Requirement? (4) Regarding CIP-007-5, R4, Southern suggests that the SDT consider referencing 800-137 within the appropriate guidance language. (5) Regarding CIP-007-5, R4.1, Southern suggests changing "at a minimum" with "per device capability". (6) Regarding CIP-007-5, R4.3, Southern suggests appending “after identification of the failure” to clarify when the response period begins.
(1) Regarding CIP-007-5, R5.2, Southern questions the benefit of a senior manager approving that generic accounts exist when we already have to authorize individuals to use those accounts. This is a too low level task for a senior manager. To address this issue and to avoid unnecessary duplication, Southern strongly suggests removing R5.2 as the security intent is achieved through R5.3. (2) Regarding CIP-007-5, R5.3, the point concerning lost or inappropriate passwords in the change rationale is an important point and Southern suggests moving it to the guidance. (3) Regarding CIP-007-5, R5.5, Southern suggests that the "attestation" in the measures be changed to "documentation". (4) Regarding CIP-007-5, R5.7, Southern strongly suggests deleting the requirement as it is not in Order 706 and it provides opportunity for denial of service attacks. Locking out accounts may be viable in the IT systems, but may introduce more risk in BES Cyber Systems if critical accounts can be locked out by simply trying known invalid credentials. If the requirement stays, we suggest moving ‘where technically feasible’ to the beginning of the requirement so it is clear that a TFE is available for both options.
Group
Western Area Power Administration
Brandy A. Dunn
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
No
No
No
R1.4 and R1.6 “require 99.9% availability”; a definition of this requirement is need. Does this include maintenance and testing time? Upgrade time? Also, what are acceptable monitoring methods to meet the “controls that monitor” intent?
No
No
Yes
No
Yes
CAN-0019 is in development to answer the question, “What is the acceptable time to install a software patch before a TFE is required?” CIP-007-5 R2 states that a remediation plan must be developed within 30 days, but does not answer the question. Please identify an acceptable interval for completion of the remediation plan. Is one year too long? Can a remediation plan state that implementation will start after 6 years?
Individual
Brian S. Millard
Tennessee Valley Authority
Yes
Yes
Yes
Yes
Yes
Yes
Yes
CIP-004-5 R2 - Remove “role-based cyber security training” to training based or tailored to job function. Role-based infers that training should be based on access permissions or that access should be role based. R2.1 - Change “identification of each role” to “identification of roles” required for BES cyber access. Remove R2.10, What is the intent of this requirement? There is no additional value in this requirement as it is already covered in 2.2 through 2.9. CIP-004-5 R3 - Remove “role-based cyber security training” to training based or tailored to job function. Role-based infers that training should be based on access permissions or that access should be role based. CIP-004-05 R 2.8 - Remove the requirement for training content for recovery plans for BES Cyber Systems. Rationale to apply this training to all personnel who have access to BES Cyber Systems is flawed. A small subset of skilled individuals would be responsible for executing recovery plans not the entire CIP population. R3.1 - Requirement should not include documentation, this is a measure. R4.1 - Time period for retention is not defined. Need to include provision for grandfathering older standard requirements. R4.2 - Include the word “consecutive” prior to six months. Make a bulleted list to represent and “or” list. CIP-004-5 R4 - The ability to verify criminal history for employees who haven’t resided in the US for more than a few years may cause employment issues for employees.

Rational R6 - User Accounts are not defined or called out in actual standard. R6.1 - Designate one or more individuals by names or roles. R6.2 - Remove “the Responsible Entity determines”, the function of the authorizer in R6.1 is to ensure need. R6.4 - Use the word “designated repository” instead of “location”. With location, this could be an iPad. R6.5 - Add “currently” between” individuals provisioned”. Reword to match current quarterly review and comparison of who needs access versus who has access. R6.6 - Replace “all” with BES cyber systems. Change number list in measures to bulleted list to represent an “or” list. R6.7 - Use the word “designated repository” instead of “location”. R7.1 - Employee death should be classified differently than termination. Possibly use no longer requiring access vs. termination. 7.1 should be reserved for someone who is a risk. R7.2 - Insert “notification of” prior to reassignments. Allow for one barrier approach or effectively remove. R7.3 - Use the word “designated repository” instead of “location”.
Yes
Yes
CIP-005 R1.7 - Language in this standard is conflicting and arbitrary. The measures section of R1.7 references a specific term with Intrusion Detection Systems. There are numerous types of technology which can identify malicious traffic. Remove the measures language or make it technology agnostic. The expansion of the requirements and assets covered under R1 will require the addition of personnel and systems that are not currently in place today. The requirement for 1.5 is “Have a method for detecting malicious communications.” The intention of this standard is unclear. It is not clear what “malicious communications” is, nor is it clear what an acceptable method is. Is an IP address ping sweep “malicious communication”? If so, then could you just have a firewall send alerts when there are dropped packets? The Measures section mentions intrusion detection systems but does not discuss what minimum configuration requirements are needed. As written, it appears that a poorly implemented IDS would meet the word of the standard. For example, it sounds like one would only need to provide a configuration file of an IDS and documentation of where it is located, but not have to provide evidence that it is continuously working or that its configuration is appropriate. R1.1 Measures - Delete “uniquely identifiable”, should be with all BES in ESP not at component level. R1.4 - Include applicable, you do not need to have a program if you don’t need or use dial up connectivity.
CIP-005 R2.2 - The requirement does not reference specific types or standards for acceptable levels of encryption. This will lead to regions interpreting this differently and impact the ability of the business to meet this requirement. Consider referencing NIST approved encryption methodologies (i.e. NIST SP800-77 or NIST SP800-111). R2.2 - End the sentence after intermediate device. Balance is commentary. R2.3 - Clarify that this is to the intermediate device only.
No
Yes
Yes
R1.2 - As worded, this prevents an escorted person from entering the PSP. R1.3 - Modify controls wording to be multi-factor authentication. As worded this prevents an escorted person from entering the PSP. R1.4 Meeting the 99.9% is not possible. How do we measure and what is the threshold? Suggest rewording to be like CIP-007 R 4.3. Need to include provisions for mitigation with personnel. Consider making applicable to only High impacts and lesser degree for Medium impacts. Bounds should be set around monitoring. Consider limiting to physical access points. R1.5- Replace “circumvention” with “access”.
Yes
Yes
Yes
Yes
No
CIP-007 R2.3 - Due to the sheer number and volume of patches that are issued for both information technology and operational technology this requirement becomes overly burdensome. CIP-007 R 4.2 - The term “necessitate a real-time alert” is introduced to the standard. Is there a threshold for what is deemed a real-time alert? The term is unnecessarily vague and will lead to regional interpretation issues. Suggest striking the term. CIP-007 R 4.5 - This requirement should be reworded to address manual review at a minimum every two weeks for manual logging activity and should be excluded where automated monitoring programs are in place (i.e. Managed Security Service

Provider).Additional resources would be required for managing and monitoring additional devices that would be covered in the revised requirement. R2 - No requirement to maintain a system that is patchable thereby, rewarding obsolescence. Understandably, a grace period for upgrading to a patchable should be allowed, but to never require upgrading is too liberal and a security risk. R2.2 - Change 30 days to 35 days in order to allow monthly evaluations. R3.3 - Update cycle too aggressive. It should match patching requirements for practical testing, scheduling, and outage installation. Language will force online updates with undue risk. R4.1 - Replace “minimum” with “per device capability”. R4.3 - Change detected to indicate human detected. Add “after notification” to the end of “next calendar day”. R4.4 - Remove Security Event Logs and replace with previous 4.1 logs.
R5.2 - Recommend deleting requirement. The CIP Senior Manager approval of shared accounts adds administrative burden without cyber security benefits. R5.7 - Recommend deleting requirement. This could result in control system lockout and have a negative impact on reliability.
Group
Edison Electric Institute
David Batz
(1.) Unescorted Cyber Access category should be introduced to allow for more effective interaction with vendor support services. Much of the CIP-004 personnel risk assessment requires extensive dependencies on supporting evidence which is not available under standard support contracts which require 24*7 staffing. There currently exists tools to monitor interaction of remote vendor support and limiting requirements to those having unescorted access within the CIP requirements will allow more effective focus of resources. (2.) Other applicability concerns - There is general inconsistency among the applicability of requirements in CIP-004-5 with respect to how they apply to training, personnel risk assessment, and authorization and revocation requirements for different types of access. The applicability of each requirement should be reviewed from a functional perspective to determine how it applies to different types of physical, electronic, and information access. The primary concern is that the applicability of 'Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity' is applied to all CIP-004 R2 through R7 requirements. This is not appropriate in many requirements due to the overriding applicability of other CIP V5 Standards. In some instances the inconsistency can be cleared up by changing the applicability from 'Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity' to 'Medium Impact BES Cyber System with External Routable Connectivity.' There are also several instances in which different types of access are addressed within the same requirement. Due to the varying applicability of different access types, it appears it will be necessary to separate these requirements into multiple requirements to properly address the applicability concerns. As one example, the applicability of CIP-004 for physical access control systems exceeds that of CIP-006. To increase consistency within the standards, references to dial-up connectivity has been removed where alignment within CIP-006 is necessary. Dial-Up access is only referenced within CIP-004 applicability columns (within the Standard). (3.) Suggest limiting applicability to the access control of BES Cyber Systems. There is confusion where electronic and physical access control systems fall within the requirements, whether the applicability is limited to access control of BES Cyber Systems. (4.) With respect to R5.1, there is some concern regarding the current triggers of 'being granted' access and authorizing access. There was some discussion of replacing 'being granted' with 'provisioning,' but no clear consensus was identified. (5.) R1.1 - Requirements a. Propose changing the phrase 'ongoing reinforcement of cyber security practices,' to 'ongoing reinforcement of security practices.' By dropping 'cyber,' a more general security awareness program can be implemented, addressing cyber and physical awareness topics. b. Insert 'unescorted' into 'authorized unescorted electronic' references. This allows entities to focus on unauthorized access rather while allowing for vendor support services. (6.) R2.1 - Requirements, Rewording a. Original - Identification of each role and training required for each role. b. Proposed - Identification of training content appropriate for individuals and their responsibilities c. Rationale - The rewording allows for increased flexibility in an entities training approach, while ensuring topics adequately cover CIP training requirements. (7.) R2.2 - Requirements, Rewording a. Original - Training content on the cyber security policies protecting the Responsible Entity's BES Cyber Systems. b. Proposed - Training content on the cyber security policies protecting applicable cyber assets. c. Rationale - This allows for training to be targeted addressing applicable cyber assets (to include BES Cyber Assets where applicable). (8.) R2.3 - Requirements, Rewording a. Original - Training content on the physical access controls protecting the Responsible Entity's BES Cyber Systems. b. Proposed Training content on the physical access

controls protecting applicable cyber assets. c. Rationale - This allows for training to be targeted addressing applicable cyber assets (to include BES Cyber Assets where applicable). (9.) R3.1 - change reference from 'BES Cyber Systems' to 'applicable cyber assets' to ensure training adequately covers relevant and applicable cyber assets. (10.) R4.1 - Requirements, Rewording a. Original - An initial personnel risk assessment ('PRA') that includes identify verification. b. Proposed - Program content on an initial personnel risk assessment that includes identity verification. c. Rationale - This requirement should address the contents of a supporting program rather than individual artifacts of evidence. (11.) R4.2 - Requirements, Rewording a. Original - Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six months or more: b. Proposed - Seven year criminal history records check including current residence, regardless of duration, and covering all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six consecutive months or more: c. Rationale - Two changes have been made. 'At least' was dropped in front of 'all' as it was redundant with 'at least all.' Also, 'consecutive' was added in the middle of 'six months' to provide greater clarity in terms of what the criteria is. (12.) R5.1 - Requirements, Rewording a. Original - Have a personnel risk assessment performed as specified in CIP-004-5, Requirement R4 prior to being granted authorized electronic or authorized unescorted physical access, except for CIP Exceptional Circumstances. b. Proposed - Have a personnel risk assessment as specified in CIP-004-5, Requirement R4 prior to gaining authorized electronic or authorized unescorted physical access, except for CIP Exceptional Circumstances. Subsequent authorizations, within the life-time of PRA events, do not require repeating the background check. c. Rationale - while not perfect, it was determined that 'gaining' would be better terminology than 'granting.' The additional language regarding not repeating this requirement provides clarity that this process is to be conducted once for any/all authorized access and is not subject to additional PRAs as additional access requirements are identified. (13.) R5.1 - Measures, Rewording (First bullet) a. Original - Dated records showing that personnel risk assessments were completed before authorized electronic or authorized unescorted physical access was authorized; or b. Proposed - Records showing that personnel risk assessments were performed before authorized unescorted electronic or authorized unescorted physical access was gained. c. Rationale - There is repetition of 'authorized' within this measure which is confusing. By replacing the last word with provisioned, the event is better captured to ensure compliance with the PRA requirement. (14.) R5.2 - Measures, Rewording a. Original - Evidence may include, but is not limited to, current and previous personnel risk assessment records. b. Proposed - Evidence may include, but is not limited to, current personnel risk assessment records. c. Rationale - Given the 7 year cycle, ensuring that the current records are in place should satisfy this requirement. Addition of previous PRA records only adds to the archival length to a period of (up to) 14 years without any benefit to security.

(15.) R6.1 a. Applicability should remove references to dial-up connectivity b. Measure should add 'unescorted' in front of electronic access. c. Rationale - this provides more effective applicable cyber assets to enact these requirements. Adding unescorted access allows for vendor support requirements without elevating this into 'authorized electronic access' category. (16.) R6.2 Requirement Rewording a. Original - The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances. b. Proposed - The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is appropriate. c. Rational - assessing the appropriateness of access permissions is more effective then assessing 'necessary.' (17.) R6.3 Requirement Rewording a. Applicability should remove references to dial-up connectivity b. Original - The individual(s) designated in Part 6.1 shall authorize unescorted physical access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances. c. Proposed - The individual(s) designated in Part 6.1 shall authorize unescorted physical access into Physical Security Perimeter(s) that the Responsible Entity determines is appropriate, except for CIP Exceptional Circumstances. d. Rationale - Providing a scope of PSP access frames this requirement within the context of the CIP scope, focusing on defined PSP access. (18.) R6.6 Requirement Rewording a. Original - For electronic access, verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all user accounts, user account groups, or user role categories, and their specific associated privileges are correct and are those that the Responsible Entity determines necessary for performing assigned work functions. b. Proposed - For electronic access, verify at least once each calendar year, or not to exceed 15 calendar

months between verifications, that BES Cyber System access privileges are appropriate for the individual(s) or role(s) responsibilities. c. Rationale - The current language provides too prescriptive a list of evidence in support of this requirement. By eliminating 'all,' identifying BES Cyber System access privileges will frame the context of this requirement effectively. Focusing on ensuring the privileges are appropriate vs. 'correct,' allows for assessing the privileges. (19.) R6.6 Measures - This should be a bulleted list to support an 'or' assessment of the evidence. (20.) R6.7 Measures - The numbered list should be a bulleted list to support an 'or' assessment of the evidence. a. Last bullet - Rewrite i. Original - Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions. ii. Proposed - Evidence showing a verification of the authorization and any permissions were confirmed. iii. Rationale - The edits provide a greater focus on the root concerns to address the Requirement. (21.) R7.1 - Requirement Rewrite a. Original - For all termination actions, initiate the process to revoke the individual's unescorted physical access and interactive Remote Access upon the effective date and time of the termination action, and complete the revocation within 24 hours after the effective date and time of the termination action. b. Proposed - For all termination actions, initiate the process to revoke the individual's unescorted physical access and interactive Remote Access upon the effective date and time of the communication of the termination action, and complete the revocation within 24 hours after the effective date and time of the communication of the termination action. c. Rationale - By identifying the time the termination action is communicated, concerns regarding notification of terminations which are pre-dated or retro-active can be alleviated by using the communication time as the trigger event. (22.) R7.1 - Measure should show a bulleted list to reflect the 'or' approach to supporting evidence. (23.) R7.2 - Requirements Rewrite a. Original - For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the reassignment or transfer. b. Rewrite - For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the determination that access is no longer necessary. c. Rationale - The rewording provides greater support and recognition that this process can take place until all legacy access is no longer needed, within a transition period that can take place indefinitely. By assigning the response time to the determination event, deadlines are aligned more effectively. (24.) R7.2 - Measure should show a bulleted list to reflect the 'or' approach to supporting evidence. (25.) R7.5 - Frame the requirement against BES Cyber System shared accounts to provide alignment with BES Cyber Systems.

(1.) While dial-up connectivity requirements are proposed to be moved to CIP-007-5, R5.1, there should be a definition identifying what constitutes 'dial-up.' EEI membership discussed varying interpretations that indicate a clearer definition would help identifying the applicable cyber assets. Proposed definition: Dial-Up connectivity - Connectivity to BES Cyber Assets (or associated Protected Cyber Assets) which is publically accessible using the Publically Switched Telephone Network (PSTN). (2.) Definition - Intermediate Device a. Modify the definition to allow for Intermediate Devices to terminate on an Electronic Access Point or to be external to the ESP. b. Rationale - This will ensure applicable Intermediate Devices are not 'disqualified' from operating as such should they have an interface which is an electronic access point into the ESP. (3.) Introduction - 4.2.2: This should reference CIP-005-5 (rather than CIP-002-5). (4.) R1.1: Applicability a. Add Associated Protected Cyber Assets with External Routable Connectivity b. Rationale - This addition aligns with the requirement, in which associated Protected Cyber Assets are also required to reside within a defined ESP. (5.) R1.2 Applicability a. Add Associated Protected Cyber Assets with External Routable Connectivity b. Rationale - This addition aligns with the requirement, in which associated Protected Cyber Assets are also required to reside within a defined ESP. (6.) R1.4 a. This requirement is very similar to CIP-007-5 R5.1, with the exception of dial-up applicability. b. Propose adding BES Cyber Assets with dial-up connectivity used within High and Medium Impact facilities into CIP-007 R5.1, and removing R1.4 from CIP-005-5. c. Rationale - This identifies all BES Cyber Assets that require authentication into a single requirement, resulting in a more concise standard. (7.) R1.5 Measures - there should be bullets (rather than numbers) identifying 'or' instances.

(8.) R2.1, 2.2, 2.3 Requirements - Proposed Change a. Original - Utilize encryption for all Interactive Remote Access sessions that terminate at an Intermediate Device in order to protect the confidentiality and integrity of each Interactive Remote Access session. b. Proposed - Utilize encryption for all routable Interactive Remote Access sessions that terminate at an Intermediate Device. c. Rationale - The addition of 'routable' in front of Interactive Remote Access sessions provides a clear filter that aligns with the Interactive Remote Access concept. (9.) R2.3:

Requirements - Move examples cited into the measures for the three factors cited, leaving the requirement with the description of the factor. The measures would frame examples appropriate to each factor. (10.) R2.4: Clarification as to where the authentication needs to take place. Can the multi-factor authentication be done at the intermediate device or does it need to be done at the access point to the ESP.
(1.) R1.4 is seen as a deal breaker and should be considered for removal. Monitoring 24*7*365 with a 99.9% uptime would require extensive resources to satisfy the supporting documentation. Comment to revise is contained in the comment on R1.5. R3.2 justifies that this level of monitoring is not required. (2.) Focusing on unauthorized circumvention of physical access control could be interpreted as monitoring for perimeter breaches outside of the current physical access points. This could lead to exhaustive monitoring tools which may still allow for unmonitored locations that result in a violation of this requirement. (3.) The category of 'locally mounted hardware or devices at the Physical Security Perimeter(s)' requires additional detail. This originates within the PSP definition (where locally mounted hardware is exempt) and extends into the CIP-006 requirements. By defining something by what it is not, there is a risk that it may include a number of devices beyond the intended PSP devices. (4.) Introduction - Section 4.2.3: By citing 'All BES Facilities' there may be a perceived exclusion of ISOs from applicability. This should reference the ISO role as also being subject to CIP-006-5. (5.) The applicability within this Standard was a topic of extensive discussion. a. Within 1.1-1.8, it is unclear whether 1.1 is intended to apply to devices not cited within 1.2- 8. Per the first draft, 1.1 was intended to capture devices not subject to subsequent standards. If this is the approach for draft 2, the applicability should include (only) dial-up accessible and externally routable devices. Associated Electronic Access Control devices should also be included within R1.1 applicability. b. In any event, this may be an instance in which diagrams or other graphical aides may benefit the understanding of what devices are subject to what requirements via a series of pictures. (6.) The concept of 'two or more different physical access controls' needs additional supporting documentation, including appropriate strategies to satisfy this requirement. Can a common server that satisfies authentication request from multiple access controls satisfy this requirement' Is the intent to require two 'keys' or authentication factors' It is also unclear how two factor authentication would fit into satisfying this requirement. (7.) Introduction 4.2.4: This should reference CIP-006-5 (rather than CIP-002-5). (8.) R1.5 a. Requirement: This includes content similar to R1.4, which has been proposed for removal. The concept of 'unauthorized circumvention of a physical access control' may require resources and technology which may still be inadequate to identify any/all instances of circumvention. Changing 'unauthorized circumvention' to 'unauthorized access' may better frame this requirement, but may not satisfy the root concern intended by the SDT. b. Measures - there should be bullets (rather than numbers) identifying 'or' instances. (9.) R1.7 Requirements & Measures - Change a. Original - Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the unauthorized physical access. b. Proposed - Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System within 15 minutes of the detected unauthorized physical access. (10.) R2.1 - Requirements a. Original - Require continuous escorted access of visitors (individuals who are known or guests, and not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances. b. Proposed - Require continuous escorted access of individuals not authorized for unescorted physical access. c. Rationale - The additional words did not provide any greater clarity. (11.) R3.2 a. Applicability - Remove 'Locally mounted hardware or devices at the physical security perimeter associated with:' Rationale - documenting outages for locally mounted hardware is currently too vague and resource intensive with minimal security benefit. By ensuring that Physical Access Control Systems adequately document their outages, the root concern should be addressed. b. Requirement - Change i. Original - Document outages for physical access control, logging, and alerting systems and retain the outage records for at least 12 months. ii. Propose - Document outages for physical access control systems and retain the outage records for at least 12 calendar months. iii. Rationale - By focusing on the Physical Access Control Systems, satisfactory outage records should be achieved. (12.) VSL - R1/High: The second paragraph on page 23 should read 'The Responsible Entity does not have controls' (13.) VSL - R1/Medium: Remove 'or external dial-up connectivity. (1.2)' from the end of the second paragraph. (14.) VSL - R2 Moderate: Remove 'on a daily basis,' from the 1st paragraph on page 25. (15.) Application Guidelines a. Page 28 - Remove 'Methods to monitor physical access include:' section as it relates to R1.4, which has been proposed for removal. b. Page 29, second paragraph - Remove. The applicability of the 96 square inch opening

provides no benefit to applicability.
(1.) R2, all sub-requirements Applicable BES Cyber Systems and associated Cyber Assets: Change 'Medium Impact BES Cyber Systems' to 'Medium Impact BES Cyber Systems with External Routable Connectivity'. Rationale: For non-externally routable or dialup systems this will create a large amount of document requirements without adding much security. (2.) R1.1 a. Applicable BES Cyber Systems and associated Cyber Assets: Clarify how 'Associated Protected Cyber Assets' is a modifier to the 'High Impact BEST Cyber Systems' and 'Medium Impact BES Cyber Systems with External Routable Connectivity' rather than an independent set of assets. One option is to add 'and Associated Protected Cyber Assets' to each of the High and Medium categories in this requirement. b. Requirements i. Does the 'where technically feasible' language imply that TFEs are required when it is not technically feasible' ii. There was discussion about how 'needed' should be defined, and whether it's up to the asset owner to determine the need for a port to be accessible, or whether the auditor has the ability to decide. This issue was tabled, and there may suggested language provided. (3.) R1.2 a. Requirements: Discussions around whether the physical security measures already accommodate this requirement, but it was brought up that FERC specifically requires this. b. Measures: Suggest a clarification that these measures be implemented at the device level if that is the intent. (4.) R2.1 Requirements: Original - 'A patch management program for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets.' Proposed - 'A patch management program for tracking, evaluating, and installing cyber security patches and/or security updates for applicable Cyber Assets.' (5.) R2.2 Requirements: Change 30 to 35 calendar days to assist with monthly patch cycles and increase efficiency (6.) Requirement 3 & 4, all sub-requirements a. Associated Protected Cyber Assets i. Concern: The inclusion of this category in the requirements for Malicious Code Prevention and Security Event Monitoring implies that these requirements apply to every device in the category. This departs from the goal of applying these controls at the system level. ii. Suggestion: Clarify that these requirements do not apply to all assets individually, by removing the category, or modifying the requirement. (7.) User vs. System password: A long discussion ensued that there is no clear delineation between system passwords and user passwords. Does a user password have an identity associated with it' What about systems that use system ids/passwords, do those qualify as user or system passwords' Clarification of this issue would be helpful. (8.) R4.1 a. Add the term 'where technically feasible' to the requirement language b. Rationale: Not all systems can support the logging requirements in 4.1.1-4.1.4. (9.) R4.2.1 a. Change 'detected malicious activity' to 'detected cyber security event' b. Rationale: not all security events are malicious (10.) R4.3 a. Requirement i. Change 'Activate a response to detected event' to 'Activate a response to human-detected event' ii. Rationale: the requirements do not distinguish between the detection of an event by a system and a person. A person may not see the event at the same time it is generated by a system, so the requirement should be clarified to reflect that the deadline for a response be tied to human detection. b. Requirement: Change 'next calendar day' to 'next business day' to accommodate off-hour staff coverage. c. Measures: Change 'attestation' to 'documentation' for clarity. (11.) R4.5 a. Applicability i. Consolidate 'High Impact BES Cyber Systems' and 'Associated Protected Cyber Assets', by changing the wording to 'High Impact BES Cyber Systems with Associated Protected Cyber Assets' ii. Rationale: Clarifies that the logging reviews do not apply at the asset level. b. Requirement i. Change the wording to 'Review a summarization or sampling of logged events, as deemed appropriate by the Responsible Entity, at a minimum' ii. Rationale: It should be clear that the entity determines which logs should be reviewed or sampled, to avoid confusion during audits.
(12.) R5.1 a. Applicability i. Change 'Medium Impact BES Cyber Systems' to 'Medium Impact BES Cyber Systems with External Routability or dial -up' ii. Rationale: Consistency with CIP-004 R6.2 (13.) R5.2: Delete requirement. Rationale: Covered by CIP-004 R6.2 (14.) R5.3 Delete requirement, and move rationale to CIP-004 R6. Rationale: Covered by CIP-004 R6. (15.) R5.4 a. Applicability i. Change 'Medium Impact BES Cyber Systems' to 'Medium Impact BES Cyber Systems with External Routability or dial -up' ii. Rationale: Consistency with CIP-004 R6.2 b. Requirement i. Change the wording from 'Change default passwords' to 'Change known default passwords' ii. Rationale: Manufacturers sometimes use system passwords that are not known to the entities. c. Measures i. Remove the language from the first bullet 'when new devices are deployed' ii. Rationale: Time frames are covered elsewhere in the Standards (16.) R5.5 Measures a. Change the second bullet to 'Documentation of procedural controls' b. Rationale: Procedural controls for changing passwords are covered elsewhere (17.) R5.6 a. Requirement i. Add the language 'within the capabilities of the device or operational requirements' to the beginning of the requirement. ii. Rationale: Some vendors do not ensure correct operation of the system if certain passwords are changed. b. Measures i. Change the

second bullet to 'Documentation of procedural controls' ii. Rationale: Procedural controls for changing passwords are covered elsewhere
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form B.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form B.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form B.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form B.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form B.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form B.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form B.
Individual
Ralph Meyer
The Empire District Electric Company
Yes
Yes
Yes
Yes
Yes
Yes
Yes
1. Unescorted Cyber Access category should be introduced to allow for more effective interaction with vendor support services. Much of the CIP-004 personnel risk assessment requires extensive dependencies on supporting evidence which is not available under standard support contracts which require 24*7 staffing. There currently exists tools to monitor interaction of remote vendor support and limiting requirements to those having unescorted access within the CIP requirements will allow more effective focus of resources. 2. Other applicability concerns – the applicability of CIP-004 for physical access control systems exceeds that of CIP-006. To increase consistency within the standards, references to dial-up connectivity has been removed where alignment within CIP-006 is necessary. Dial-Up access is only referenced within CIP-004 applicability columns (within the Standard). 3. There is also confusion where electronic and physical access control systems fall within the requirements, whether the applicability is limited to access control of BES Cyber Systems. 4. 6. R2.1 – Requirements, Rewording a. Original – Identification of each role and training required for each role. b. Proposed – Identification of training content appropriate for individuals and their responsibilities c. Rationale – The rewording allows for increased flexibility in an entities training approach, while ensuring topics adequately cover CIP training requirements.
15. R6.1 a. Applicability should remove references to dial-up connectivity b. Measure should add ‘unescorted’ in front of electronic access. c. Rationale – this provides more effective applicable cyber assets to enact these requirements. Adding unescorted access allows for vendor support requirements without elevating this into ‘authorized electronic access’ category. 16. R6.2 Requirement Rewording a. Original – The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances. b. Proposed – The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is appropriate for the individual role and responsibility. c. Rational – assessing the appropriateness of access permissions is more effective

then assessing ‘necessary.’ 17. R6.3 Requirement Rewording a. Original – The individual(s) designated in Part 6.1 shall authorize unescorted physical access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances. b. Proposed – The individual(s) designated in Part 6.1 shall authorize unescorted physical access into Physical Security Perimeter(s) that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances. c. Rationale – Providing a scope of PSP access frames this requirement within the context of the CIP scope, focusing on defined PSP access. 18. R6.6 Requirement Rewording a. Original – For electronic access, verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all user accounts, user account groups, or user role categories, and their specific associated privileges are correct and are those that the Responsible Entity determines necessary for performing assigned work functions. b. Proposed – For electronic access, verify at least once each calendar year, not to exceed 15 calendar months between verifications, that BES Cyber System access privileges are appropriate for the individual(s) or role(s) responsibilities. c. Rationale – The current language provides too prescriptive a list of evidence in support of this requirement. By eliminating “all,” identifying BES Cyber System access privileges will frame the context of this requirement effectively. Focusing on ensuring the privileges are appropriate vs. “correct,” allows for assessing the privileges. 19. R6.6 Measures – This should be a bulleted list to support an “or” assessment of the evidence. 20. R6.7 Measures – The numbered list should be a bulleted list to support an “or” assessment of the evidence. a. Last bullet – Rewrite i. Original – Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions. ii. Proposed – Evidence showing a verification of the authorization and any permissions were confirmed. iii. Rationale – The edits provide a greater focus on the root concerns to address the Requirement. 21. R7.1 – Requirement Rewrite a. Original – For all termination actions, initiate the process to revoke the individual’s unescorted physical access and interactive Remote Access upon the effective date and time of the termination action, and complete the revocation within 24 hours after the effective date and time of the termination action. b. Proposed – For all termination actions, initiate the process to revoke the individual’s unescorted physical access and interactive Remote Access upon the effective date and time of the communication of the termination action, and complete the revocation within 24 hours after the effective date and time of the communication of the termination action. c. Rationale – By identifying the time the termination action is communicated, concerns regarding notification of terminations which are pre-dated or retro-active can be alleviated by using the communication time as the trigger event. 22. R7.1 – Measure should show a bulleted list to reflect the “or” approach to supporting evidence. 23. R7.2 – Requirements Rewrite a. Original – For reassignments or transfers, revoke the individual’s electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the reassignment or transfer. b. Rewrite – For reassignments or transfers, revoke the individual’s electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the determination. c. Rationale – The rewording provides greater support and recognition that this process can take place until all legacy access is no longer needed, within a transition period that can take place indefinitely. By assigning the response time to the determination event, deadlines are aligned more effectively. 24. R7.2 – Measure should show a bulleted list to reflect the “or” approach to supporting evidence. 25. R7.5 – Frame the requirement against BES Cyber System shared accounts to provide alignment with BES Cyber Systems.
Yes
Yes
1. While dial-up connectivity requirements are proposed to be moved to CIP-007-5, R5.1, there should be a definition identifying what constitutes “dial-up.” EEI membership discussed varying interpretations that indicate a clearer definition would help identifying the applicable cyber assets. Proposed definition: Dial-Up connectivity – Connectivity to BES Cyber Assets (or associated Protected Cyber Assets) which is publically accessible using the Publically Switched Telephone Network (PSTN). 2. Definition – Intermediate Device a. Modify the definition to allow for Intermediate Devices to terminate on an Electronic Access Point or to be external to the ESP. b. Rationale – This will ensure applicable Intermediate Devices are not ‘disqualified’ from operating as such should they have an interface which is an electronic access point into the ESP.
8. R2.2 Requirements – Proposed Change a. Original – Utilize encryption for all Interactive Remote

Access sessions that terminate at an Intermediate Device in order to protect the confidentiality and integrity of each Interactive Remote Access session. b. Proposed – Utilize encryption for all routable Interactive Remote Access sessions that terminate at an Intermediate Device in order to protect the confidentiality and integrity of each Interactive Remote Access session. c. Rationale – The addition of 'routable' in front of Interactive Remote Access sessions provides a clear filter that aligns with the Interactive Remote Access concept.
Yes
Yes
Yes
11. R3.2 a. Applicability – Remove "Locally mounted hardware or devices at the physical security perimeter associated with:" Rationale – documenting outages for locally mounted hardware is currently too vague and resource intensive with minimal security benefit. By ensuring that Physical Access Control Systems adequately document their outages, the root concern should be addressed. b. Requirement – Change i. Original – Document outages for physical access control, logging, and alerting systems and retain the outage records for at least 12 months. ii. Propose – Document outages for physical access control systems and retain the outage records for at least 12 calendar months. iii. Rationale – By focusing on the Physical Access Control Systems, satisfactory outage records should be achieved.
Yes
Yes
Yes
No
Yes
1. R2, all sub-requirements Applicable BES Cyber Systems and associated Cyber Assets: Change "Medium Impact BES Cyber Systems" to "Medium Impact BES Cyber Systems with External Routable Connectivity". Rationale: For non-externally routable or dialup systems this will create a large amount of document requirements without adding much security. 2. R1.1 a. Applicable BES Cyber Systems and associated Cyber Assets: Clarify how "Associated Protected Cyber Assets" is a modifier to the "High Impact BEST Cyber Systems" and "Medium Impact BES Cyber Systems with External Routable Connectivity" rather than an independent set of assets. One option is to add "and Associated Protected Cyber Assets" to each of the High and Medium categories in this requirement. b. Requirements i. Does the "where technically feasible" language imply that TFEs are required when it is not technically feasible? ii. There was discussion about how "needed" should be defined, and whether it's up to the asset owner to determine the need for a port to be accessible, or whether the auditor has the ability to decide. This issue was tabled, and there may suggested language provided. 3. R1.2 a. Requirements: Discussions around whether the physical security measures already accommodate this requirement, but it was brought up that FERC specifically requires this. b. Measures: Suggest a clarification that these measures be implemented at the device level if that is the intent. 4. R2.1 Requirements: Original – "A patch management program for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets." Proposed - "A patch management program for tracking, evaluating, and installing cyber security patches and/or security updates for applicable Cyber Assets." 5. R2.2 Requirements: Change 30 to 35 calendar days to assist with monthly patch cycles and increase efficiency 6. Requirement 3 & 4, all sub-requirements a. Associated Protected Cyber Assets i. Concern: The inclusion of this category in the requirements for Malicious Code Prevention and Security Event Monitoring implies that these requirements apply to every device in the category. This departs from the goal of applying these controls at the system level. ii. Suggestion: Clarify that these requirements do not apply to all assets individually, by removing the category, or modifying the requirement. 7. User vs. System password: A long discussion ensued that there is no clear delineation between system passwords and user passwords. Does a user password have an identity associated with it? What about systems that use system ids/passwords, do those qualify as user or system passwords? Clarification of this issue would be helpful. 8. R4.1 a. Add the term "where technically feasible" to the requirement language b. Rationale: Not all systems can support the logging requirements in 4.1.1-4.1.4. 9. R4.2.1 a. Change "detected malicious activity" to "detected cyber security event" b. Rationale: not all security events are malicious 10. R4.3 a. Requirement i. Change "Activate a response to detected event…" to "Activate a response to human-detected event…" ii. Rationale: the requirements do not distinguish between the detection of an event

by a system and a person. A person may not see the event at the same time it is generated by a system, so the requirement should be clarified to reflect that the deadline for a response be tied to human detection. b. Requirement: Change “next calendar day” to “next business day” to accommodate off-hour staff coverage. c. Measures: Change “attestation” to “documentation” for clarity. 11. R4.4 a. Applicability i. Remove the three “Associated…” systems/assets from the applicability section ii. Rationale: Confusing because the requirement states “BES Cyber System” which does not include these associated systems. b. Measures: Change the numbers to bullets for document consistency 12. R4.5 a. Applicability i. Consolidate “High Impact BES Cyber Systems” and “Associated Protected Cyber Assets”, by changing the wording to “High Impact BES Cyber Systems with Associated Protected Cyber Assets” ii. Rationale: Clarifies that the logging reviews do not apply at the asset level. b. Applicability i. Remove “Associated Physical Access Control Systems” and “Associated Electronic Access Control or Monitoring Systems” ii. Rationale: c. Requirement i. Change the wording to “Review a summarization or sampling of logged events, as deemed appropriate by the Responsible Entity, at a minimum…” ii. Rationale: It should be clear that the entity determines which logs should be reviewed or sampled, to avoid confusion during audits.
13. R5.1 a. Applicability i. Change “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routability or dial -up” ii. Rationale: Consistency with CIP-004 R6.2 14. R5.2: Delete requirement. Rationale: Covered by CIP-004 R6.2 15. R5.3 Delete requirement, and move rationale to CIP-004 R6. Rationale: Covered by CIP-004 R6. 16. R5.4 a. Applicability i. Change “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routability or dial -up” ii. Rationale: Consistency with CIP-004 R6.2 b. Requirement i. Change the wording from “Change default passwords…” to “Change known default passwords…” ii. Rationale: Manufacturers sometimes use system passwords that are not known to the entities. c. Measures i. Remove the language from the first bullet “…when new devices are deployed” ii. Rationale: Time frames are covered elsewhere in the Standards 17. R5.5 Measures a. Change the second bullet to “Documentation of procedural controls” b. Rationale: Procedural controls for changing passwords are covered elsewhere 18. R5.6 a. Requirement i. Add the language “unless it impacts operation of the BES” to the end of the requirement. ii. Rationale: Some vendors do not ensure correct operation of the system if certain passwords are changed. b. Measures i. Change the second bullet to “Documentation of procedural controls” ii. Rationale: Procedural controls for changing passwords are covered elsewhere
Individual
Kirit Shah
Ameren
Yes
No
No
No
Yes
No
No
(1) General comments – We suggest that anywhere that the words "authorized electronic" is used in CIP-004 should be replaced with "unescorted authorized electronic"; this language change would allow an entity to have escorted electronic access. Also, the words "but is not limited to" needs to be removed from the measures to clarify what documentation is needed for compliance. (2) R1.1 – Remove the word "cyber" in front of the words "security practices" in the requirement. This will allow and entity to broaden its security awareness program to include physical or other types of security practices outside of just cyber. (3) R2.1 – Change the language in the requirement to "Identification of appropriate training required for individual based on their responsibilities". This wording would allow more flexibility in the type of training each individual would receive and not require an entity to create roles. (4) R2.2 – Add the word "Applicable" before the word "Entity" to require training for only the applicable BES Cyber Systems and not for all BES Cyber Systems in the requirement. (5) R2.3 – (a) Add the word "Applicable" before the word "Entity" to require training for only the applicable BES Cyber Systems and not for all BES Cyber Systems in the requirement. (b) In the Applicability section this training should only be required for "Associated Physical Access Control Systems for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity".

This language change would limit only individuals that have access to the Physical Access Control Systems to take this training. (6) R2.4 – (a) Add the word "Applicable" before the word "Entity" to require training for only the applicable BES Cyber Systems and not for all BES Cyber Systems in the requirement. (b) In the Applicability section this training should only be required for "Associated Electronic Access Control or Monitoring Systems for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity". This language change would limit only individuals that have access to the Electronic Access Control or Monitoring Systems to take this training. (7) R2.8 – Currently Recovery Plan information is considered confidential. Labeling specific information to be held in a training program should be removed, and information should be at the discretion of the entity to put into their program. (8) R2.10 – Remove the words "Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems" from the Applicability section. This language change would remove personnel that have access to "Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems" from taking training on "BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets". (9) R3 – “Role Based cyber security training is very vague. How many roles does the SDT intend for entities to define. If there are specific roles to cover, they should be included in the standard. (10) R3.1 and R3.2 – Add the word "Applicable" in front of the words "training specified" and change "BES Cyber Systems" to "applicable cyber assets" in the requirement. These word changes will help clarify what type of training is needed to meet this requirement. (11) R4.1 – Add the words "A documented personnel risk assessment program requiring" at the beginning of the requirements. This word change will help clarify that a program needs to be established for personnel risk assessments. (12) R4.2 – (a) Remove the words "at least" and add the words "consecutive" in front of the words "six months" in the requirement. These word changes help clarify this requirement. (b) Remove items 4.2.1, 4.2.2, and 4.2.3. The requirements of the PRA and action based on the results should be the discretion of the entity. (13) R4.3 – Remove the words "or criteria" in the requirement and the words "or criteria identified" in the measures. This wording helps clarify that you need a process to evaluate personnel risk assessments. (14) R5.2 – Add the word "one" in front of the word "previous" in the measures. This wording helps an entity to only have to have one previous personnel risk assessment for documentation purposes.

(1) General comments – (a) For all of R6 remove the words "dial-up connectivity" in the applicability. This change matches this requirement with other dial-up connectivity requirements. (b) The words "but is not limited to" needs to be removed from the measures to clarify what documentation is needed for compliance. (2) R6.1 – (a) Remove the words "dial-up connectivity" in the applicability. (b) Add the words "to a Physical Security Perimeter" after the words "unescorted physical access" in the applicability. These changes match this requirement with other dial-up connectivity and unescorted physical access requirements. (3) R6.2 – Remove the words "for performing assigned work functions" after the word necessary in the requirement. This change helps clarify this requirement. (4) R6.3 – Change the wording of the requirement to "The individual(s) designated in Part 6.1 shall authorize unescorted physical access into Physical Security Perimeter(s) that the Responsible Entity determines is necessary, except for CIP Exceptional Circumstances". This change matches this requirement with other unescorted physical access requirements. (5) R6.4 – Remove the words "are necessary for performing assigned work functions" and replace with "are necessary" in the requirements. This change helps clarify this requirement. (6) R6.5 – Add the words "to BES Cyber Systems" after the words "physical access" in the requirements. This clarifies what type of access needs to be verified each quarter. (7) R6.6 – Replace the word "all" with "BES Cyber Systems" and replace the word "correct" with "necessary" in the requirements. This change helps clarify this requirement. (8) R7.1 – (a) Replace the words "upon the effective date" with "within 24 hours" and replace "24 hours" with "7 business days" in the requirement. This will give an entity a reasonable and achievable time to remove access. Allow seven days. (b) Change the numbers to bullets in the measures to reflect the list approach. (9) R7.2 – (a) Replace the words "by the end of the next calendar day" with "within 7 business days" in the requirement. This helps match the access removal time to the security risk of the access being removed. For a transfer an employee who is still an employee of the company in good standing should not require an end of the next calendar day removal, but should be given 7 days (b) Change the numbers to bullets in the measures to reflect the list approach. (10) R7.3 – Replace the words "by the end of the next calendar day" with "within 7 days" in the requirement. This helps match the access removal time to the security risk of the access being removed. For a removal of access to only information, this type of access should not be required to be removed by the end of the next calendar day.

Yes
No
(1) R1.1 - Add the words "Associated Protected Cyber Assets with External Routable Connectivity" to the applicability in order to align the applicability with the requirement. (2) R1.2 - Add the words "with External Routable Connectivity" after the words "Associated Protected Cyber Assets" to the applicability in order to align the applicability with the requirement. (3) R1.5 – Remove the word "and" and make the numbers into bullets in the measure to help clarify the instance of "or" instead of "and".
(1) R2.1 and R2.2 – (a) The words "with External Routable Connectivity or dial-up" should be added to the applicability after the words "Medium Impact BES Cyber Systems". Otherwise, encryption would be required for all Interactive Remote access to substations (which will fall under these requirements) which would be difficult to implement if even possible. (b) Add the word "Routable" in front of the words "Interactive Remote Access" to clarify that the type of remote access that is allowed for this requirement. (2) R2.3 – Move the examples in the requirement to the measures section to give examples of what is appropriate for multi-factor authentication.
No
Yes
Yes
(1) General Comments – (a) CIP-006 is very confusing and there needs to be a matrix or flowchart added to the guidance section to clarify what devices and associated devices need to be included in a Physical Security Perimeter and what type of monitoring is required for these devices. (b) What is the extent of monitoring of the Physical Security Perimeter that should be implemented; the text seems to indicate the entire perimeter (six wall boundary) needs to be monitored and not just the access points that are required today. This would require complete monitoring of the six sided perimeter with cameras, motion detectors, glass breaks and so forth. This is a substantial change from the current CIP standard and would be a burden on entities to implement and have controls that monitor the PSP 99.9% of the time. We would suggest that if a six wall border can be established than only the access points need to be monitored; otherwise, if a six wall border cannot be established only then, have the entire Physical Security Perimeter monitored. (2) R1.1 – The words "with External Routable Connectivity or dial-up" should be added to the applicability after the words "Medium Impact BES Cyber Systems"; otherwise, physical security would be required at all substation with Medium Impact BES Cyber Systems. (3) R1.3 – Replace the words "two or more different physical access control to collectively" to "two factor authentication to" in the requirements. The requirement wordings are confusing and as written may require two different physical access control systems to control access to a Physical Security Perimeters. (4) R1.4 and R1.5 – (a) These requirements require monitoring and alerting for the entire Physical Security Perimeters (PSP) instead of just the access points to the PSP. This requirement needs to be reworded so that if a six-wall border can be established than only the access points to a PSP need to have monitoring and alerting and not the entire PSP. If a six-wall border cannot be established only then require monitoring and alerting for the entire PSP. (b) Add the words "access point" after the words "Physical Security Perimeter" to clarify that you only have to monitor and alarm events on the Physical Security Perimeter access points. (5) R1.4 and R1.6 - These requirements needs to be reworded to remove the 99.9% availability language. Suggest coming up with a more reasonable time frame than 99.9% availability; for example, entity shall have no outage longer than 4 hours for monitoring the Physical Security Perimeters access points. (6) R1.7 – Add the word "detected" in front of the word "unauthorized" in the requirement. This helps clarify the standard on when the 15 minute time frame starts. (7) 3.1 – Add the words "associated with the Physical Access Control system" after the word "devices" in the requirement to clarify what devices need to be tested.
Yes
Yes
Yes
Yes
No
(1) R2.3 – Change 30 days to 35 days in the requirement to match the other requirements in CIP-007. (2) R3.1, R3.2, R3.3, and R4.1 - The words "with External Routable Connectivity or dial-up"

should be added to the applicability after the words "Medium Impact BES Cyber Systems". Currently technology does not exist to meet compliance with these requirements for some serial connected devices; for example programmable protective relays. (3) R3.2 – Add the words "within 35 calendar days" at the end the requirement. There is currently no time frame to mitigate the identification of malicious code and this change would match the other requirements in CIP-007. (4) R4.1 – Add the words "where technically feasible" at the end of the requirement to cover system that cannot log all of the events outlined in R4.1.1-R4.1.4. (5) R4.3 – Reword the requirement to "Activate a response to a human-detected event logging failures before the end of the next business day after the events detection." Changing the requirement gives clarification on when the clock starts for a detected event. (6) R4.4 – Change e the numbers to the bullet format in the Meausres for consistency and match other measures in CIP-007. (7) R4.5 – Performing a sample review every 2 weeks is too tight of a requirement. We would suggest changing the requirement to every 2 months or 3 months to give the entity adequate time to complete the review.
(1) R5.1 – The words "with External Routable Connectivity or dial-up" should be added to the applicability after the words "Medium Impact BES Cyber Systems". Currently, technology does not exist to meet compliance with these requirements for serial connected devices; for example programmable protective relays. (2) R5.5 – Change the second bullet in the measures to "Documentation that the procedurally enforced passwords meet the password parameters". This would eliminate having to get an attestation from SMEs every time they complete a password change.
Group
Associated Electric Cooperative, Inc (NCR01177, JRO00088)
David Dockery, NERC Reliability Compliance Coordinator, AECI
Yes
Yes
Yes
Yes
Yes
Yes
Yes
[Requirement R7 REPLACE: "by the end of the next calendar day" WITH: "within 24 hours" RATIONALE: Eliminate opportunity for failures due to close but not same timing within same requirement - 24 hours -vs- end of next calendar day. AECI does not feel the benefit is worth industry risk of non-compliance.] [R7 - AECI is also proposing an entire block of changes to the R7.x Rows of the Requirement/Applicability matrix, grouping all of the "For termination actions..." together and ahead of the "For reassignments or transfers...", in order to assist the industry in topically managing CIP requirements based upon employment changes. Please email David Dockery, ddockery@aeci.org, for an electronic copy of those proposed changes.]
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
[Measures R4.1 & R4.5 REPLACE: “signed and dated documentation showing the review occurred”

WITH: “documentation clearly identifying the reviewer and date of review” RATIONALE: Clarification that Entity normative forms of identification, other than electronic or paper signatures, could be acceptable.]
Group
Salt River Project
Sara McCoy
Yes
Yes
Yes
Yes
No
Yes
Yes
CIP-004 R5: This requirement should state that the PRAs need to be updated every 7 years in order to retain cyber access and unescorted physical access. The current wording would indicate that update is required if a PRA was done regardless of whether the person still has access or not.
Yes
Yes
No
Yes
Yes
CIP-006 R1.6: SRP would like clarification regarding this requirement. Does R1.6 require that the Physical Access Control System be within a Physical Security Perimeter? The requirement refers to PACS while the measurement refers to PSP.
Yes
Yes
Yes
No
No
CIP-007 R4 Bullet Point 4.2.2: Is this referring to the identification of any of the events listed in 4.1, or is it referring to the logging mechanism to capture the events? CIP-007 R4.5: SRP requests clarification regarding the 'review' of logged events. Is this a manual review of logged events? SRP believes a manual review every two weeks is a time intensive effort that may not have the intended benefits if too repetitious. SRP suggests a monthly review of logged events.
CIP-007 R5.5: SRP would like to see the verbiage in this requirement changed. SRP suggest using verbiage similar to the CIP-005 R2 which allows for RSA multifactor authentication. This change would allow the option of utilizing multifactor authentication which is actually more secure than only the password complexity now stated in the requirement.
Group
Texas RE NERC Standards Review Subcommittee
Brenda Hampton
Yes
No
No
No
No

No
No
(1) In requirement R2, replace the reference to role-based training with training appropriate to job function. This will eliminate potential confusion about the term “role-based”, which is often associated with IT access control. Suggested wording “Each Responsible Entity shall have a cyber security training program, appropriate to job function, to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.” (2) For requirements R2.2, R2.3, and R2.4, remove “protecting the Responsible Entity’s BES Cyber Systems”. This reference is already covered more explicitly in the applicability column. (3) Remove requirement R2.10. In complying with requirements R2.1 through R2.9, risks associated with BES cyber security will already be addressed. (4) The following refers to a common concern with CIP-004-5 and recommends various changes to requirements R2 through R7. There are inconsistencies in the applicability requirements of CIP-004-5 regarding requirements for training, PRAs, authorization and revocation for different types of access (physical, electronic, information). The primary concern is that the applicability of Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity is applied to all CIP-004 R2 through R7 requirements. This is not appropriate in all cases due to overriding applicability in other CIP V5 standards. In some instances, the inconsistency can be cleared up by simply changing the applicability from “Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity” to “Medium Impact BES Cyber System with External Routable Connectivity”. There are several instances where it appears it will be necessary to separate the requirement into two requirements to properly address the applicability concerns. Physical access: Per CIP-006-5 R1, physical access to Medium Impact BES Cyber Systems without External Routable Connectivity should not be subject to the training, PRA, authorization and revocation requirements in CIP-004-5. The inclusion of “dial-up connectivity” in the applicability column of requirements related to physical access goes beyond the intended applicability in CIP-006-5 R1. To correct this issue, the applicability of CIP-004-5 R2.3, R2.5, R6.3 can be modified to remove the reference to dial-up connectivity in the applicability column. The requirements for CIP-004-5 R3.1, R3.2, R4 (and sub parts), R5 (and sub parts), R6.1, R7.1, R7.2 will likely need to be split into multiple requirements to properly address the applicability scope differences. Electronic access: The applicability of revocation requirements in CIP-004-5 R7.1 for Interactive Remote Access should be modified to exclude dial-up connectivity. This requirement will likely need to be split into multiple requirements to properly address the applicability scope differences. A suggested revised definition for Interactive Remote Access is provided in Form D. Information access: The applicability of CIP-011-1 R1 and R2 to Medium Impact BES Cyber Systems is proposed to be limited to Medium Impact BES Cyber Systems with External Routable Connectivity to maintain consistency with the scope of cyber systems/assets currently covered by similar requirements in CIP version 4. Should this proposal be adopted it will become necessary to adjust the CIP-004-5 requirements for information access accordingly. To correct this issue the applicability of CIP-004-5 R2.6, R6.4, R6.7 and R7.3 can be modified to remove the reference to dial-up connectivity in the applicability column. The requirements for CIP-004-5 R6.1 will likely need to be split into multiple requirements to properly address the applicability scope differences. We would be happy to provide an Applicability Review matrix that includes additional supporting detail if the SDT would like a copy.
(1) In R7.2, replace “…that the Responsible Entity determines is not necessary by the end of the next calendar day following the reassignment or transfer.” with “…one calendar day after the determination that access is no longer needed.” Generally, there is no reason to believe a reassigned or transferred employee is a threat to security and there will be occasion where these employees will need temporary continuing access (e.g. training new employee in position). (2) Refer to comments on question 8 for additional comments on R6 and R7.
Yes
No
In Requirement 1.5, the Measure could be interpreted to prescribe the use of an Intrusion Detection System, however, such a system is not prescribed in a requirement. The references to IDS should be removed. Other systems and tools can be used to detect malicious communications.
(1) The definition of Interactive Remote Access (or applicability of CIP-005-5 R2.1, R2.2 and R2.3) should be adjusted to reflect the exclusion of serially connected/non-routable/non-network connected devices. There is minimal/zero reliability benefit and significant cost associated with applying this

requirement to all serially connected/non-routable/non-network connected devices that require remote access. Authentication when establishing connectivity to these systems is covered by CIP-005-5 R1.4 and provides the required cyber security. The cleanest way to correct this issue is to adjust the definition of Interactive Remote Access as follows: “All user-initiated access by a person employing a remote access client or other remote access technology using a routable protocol or dial-up. Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.” This definition is also found on Comment Form D, question 12. From V5R1 Consideration of Comments – Definition of EAP section (this helps justify that Interactive Remote Access should not apply to serially connected/non-routable/non-network connected devices): “The SDT has not included serial, non-routable communications within the definition of EAP (other than with respect to dialup in CIP-005 R1.4). Dedicated serial communications are intentionally left out of scope, as the SDT believes it would be inappropriate for the standards to mandate a universal perimeter or firewall type security across all entities and all serial communication situations. There is no ‘firewall’ capability for a RS232 cable run between two cyber assets. Without a clear security control that can be applied in most every circumstance, such a requirement would just generate TFEs.” (2) In addition, the applicability of CIP-005-5 R2.1, R2.2 and R2.3 should be changed from “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routable Connectivity.”
No
Yes
No
(1) Requirements R1.4 and R1.6 call for 99.9% reliability of monitoring systems. The documentation required to prove this level of reliability and costs associated with this level of reliability would require extensive resources to satisfy. In addition, it’s not clear if these requirements allow for alternate or redundant controls when the primary system is unavailable. For physical access controls, CIP standards should not be so restrictive as to limit options to only electronic methods. The 99.9% availability requirement should be removed and replaced with an allowance for documentation of system maintenance or outages with use of compensatory activities for monitoring. (2) In Requirements 1.5 and 1.7, an exception should be made for system maintenance or outages that last more than 15 minutes so they do not automatically create a violation. During a system maintenance activity such as required patching, the alerting system may not be functional for a period of more than 15 minutes. Unauthorized access may be detected, but not alerted during the maintenance activity. The performance of a required activity such as patching should not put a company in violation of the standard. Allow for documentation of system maintenance or outages and the use of compensatory measures, if required. (3) Requirement 1.7 should be revised from “within 15 minutes of the unauthorized physical access.” to “within 15 minutes of detection.” (4) In Requirement R3.1, remove reference to or provide additional specificity regarding “locally mounted hardware or devices at the Physical Security Perimeter(s)”. This originates within the Physical Access Control System definition (where locally mounted hardware is exempt) and extends into the CIP-006 requirements. By defining something by what it is not, there is a risk that it may include a number of devices beyond the intended PSP devices. Documenting outages for locally mounted hardware is currently too vague and resource intensive with minimal security benefit.
Yes
No
No
No
No
(1) The 30-day timeframe in CIP-007-5 R2.2 should be increased to at least 35 days to allow for monthly processes. (2) The applicability of CIP-007-5 R2.1, R2.2, R2.3 and R2.4 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity.” The exclusion of cyber systems/assets with no routable connectivity will eliminate a significant burden of tracking and documentation requirements associated with serially connected

devices that would have minimal impact to reliability. This is particularly burdensome for systems that are geographically dispersed and would require direct personnel interaction and physical access to each device to deploy patches to non-externally routable systems. (3) Under measures, M2.4 bullet 2 should be revised to read “Records of implementation of vendor recommended or other appropriate mitigations;” to eliminate any misunderstanding and allow for appropriate mitigation plans that are different than a vendor-recommended plan. (4) Revise Requirement R3.1 to read “Deploy method(s) to deter, detect, or prevent malicious code within an ESP.”, and Requirement R3.2 to read “Mitigate the threat of identified malicious code within an ESP.” The result is the scope change to include only systems that reside within a “logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.” This would restrict the scope to systems that are capable of utilizing network antimalware products since a routable protocol is being used. An infection to a system where a routable protocol is not being used has minimal impact to BES because the infection has no ability to spread. In addition these systems are not normally susceptible to traditional malware. (5) For Requirement R4.1, modify the requirement to read: “Log events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events, for applicable BES Cyber Systems which are capable of detecting and logging the events:” to eliminate requirement for those systems where it is not possible to log access events (e.g. legacy relays). (6) Modify Requirement R 4.1.3 from “detected and logged malicious software…” to ”detected and logged malicious code…” (7) Eliminate requirement R4.1.4. The term “malicious activity” is ambiguous. (8) In Requirement R4.2, revise language to replace real-time with an actual target timeframe and refer to capability of the system rather than using the term technically feasible. Suggested language “Issue and alarm or alert, within 15 minutes, for security events that the Responsible Entity determines necessitate an alert, that includes, as a minimum, each of the following types of events where the BES Cyber System is capable:”. Modify Requirement 4.2.1 to read “detected events per R4.1; and”.
(1) Propose change to applicability for Requirement R5.1 to exclude authentication requirements for local electronic access associated with high/med individual serially connected/non-networked/non-routable connected devices. (2) In Requirement R5.1, authentication should be done for accounts, not for user access. Suggest revising to read “Enforce authentication of accounts when accessing applicable Cyber Assets, where technically feasible”. (3) Applicability for R5.2 should be the same as R5.3 – only applicable to external routable connectivity. Change “delegate” to “delegate(s)” as companies may choose to have one or more delegates, depending on how they structure their program. Alternatively, consider removing R5.2 and R5.3 altogether as these requirements may already be covered by CIP-004 R6. (4) In light of the recent RuggedComm vulnerability and backdoor account it appears R5.4 needs to be reworded. The current wording would allow for password similar to the RuggedComm vulnerability. A unique password to a device is find as long as it cannot be determined based upon properties of the device. CIP-007-5 Part 5.4: Recommended change, “Change known default passwords, where technically feasible, unless the default password is unique to the Cyber Asset.” This allows for unique passwords. (5) CIP-007-5 Part 5.7: Recommended change, “Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful login attempts, where technically feasible.” Please provide guidance on what is considered a suitable minimum threshold.
Individual
Daniel Duff
Liberty Electric Power LLC
Yes
No
No
No
No
Yes
Yes
The standard still does not have a mechanism which allows for a vendor controlled cyber security system. Suggested language: A Registered Entity allowing cyber access to a vendor providing support services shall be deemed in compliance with Requirements 2 through 5 of this standard if all of the following criteria are met 1) the vendor has instituted a cyber security program which contains all of

the elements detailed in Requirements 2 through 5 of this standard; 2) the vendor has provided the RE a list of employees authorized for cyber access prior to gaining access to the asset; 3) there is a methodology for confirming the identity of the vendor employee at the time of access and 4) access to the asset remains in control of the RE at all times (through control of such means as a physical connection to the asset). This would allow REs to continue to receive vendor support for trip analysis, troubleshooting, etc and avoid long travel time delays before returning a unit to service. This requirement is another example of the huge problem of "mission creep" within the standards. When initially written, the standard was not designed to apply to small entities which rely on outside vendors for support services. The Risk Based Assessment was used to filter out those REs. Today, we see the same standard language, but the Risk Based Assessment has been replaced with criteria which will potentially capture many small merchant companies which pose little risk to the BES. (Example - a company with 310 Mw of peaking plants with one control room and two locations). The SDT must recognize that not every power producer controls thousands of Mw of generation, and that provisions for independent producers that reflect the realities of the business must be written into any standard that covers these entities.
Yes
No
Multi-factor recognition gains little in reliability and should not be a requirement.
No
Yes
Yes
The requirement for "99.9% availability" needs further definition. As written, the time period "24 hours a day/7 days a week" is the only time frame noted in the standard. 99.9% availability for any particular week would mean a ten minute outage of a system would put an entity into violation space.
Yes
Yes
Yes
Yes
No
Disagree with the proscription for passwords. Password formatting has a history of rapid change, and codifying a system into a standard which can take years to change is an unforced error. Further, less complex passwords can have greater degrees of entropy than the system proposed, so an entity could impose requirements which are much stronger than the standard requires, but be in violation of the standard.
Group
Colorado Springs Utilities
Jenn Eckels
Yes
Yes
Yes
No
Yes
Yes
No
Table R4: Personnel Risk Assessment Program: Colorado Springs Utilities would like more clarification on what level is required of the documented criteria (specific convictions, time passed since conviction, severity, etc.). Also, we are concerned that the documented criteria must also adhere to other laws and regulations. For example, creating a screening matrix weeding out those with criminal offenses based on legally defensible reasons (nature and gravity of the offense, time passed since

conviction and/or completion of sentence, nature of the job held or sought) has a high risk of adversely impacting those in a protected class.
Table R7.1: Access Revocation: Colorado Springs Utilities believes that the language in the requirement table seems to contradict the Change Rationale table.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Family Of Companies (FOC) including OPC, GTC & GSOC
Guy Andrews
Yes
Yes
No
Yes
Yes
Yes
No
(R1)The drafting team should make clear in the Guidelines and technical basis section what the term "Responsible Entity's personnel" is intended to mean. Is this only employees of the Responsible Entity or does it also include contractors and vendors? (R2) The drafting team should consider combining CIP-004-5 R2 parts 2.7 and 2.9. Initial notifications, discussed in 2.7, could be considered part of the response action identified in 2.9. At the very least, these two parts should be listed consecutively to improve readability. (R3) R3 should make clear who needs to receive the training. The requirement itself mentions only access to BES Cyber Systems, but the applicability of the parts identifies other systems. However, the language in the part itself is ambiguous. Recommend modifying the language in the main requirement of R3 to state "applicable BES Cyber Systems and associated Cyber Assets" to match the heading of the table. (R4) See comment regarding R3 about ambiguous language.
(R6) Recommend a corresponding annual review that provisioned physical security privileges are those that a Responsible Entity determines necessary for performing assigned work functions. (R7) We disagree with the requirement to initiate the process to revoke access "upon the effective date and time" of the termination action. This language obligates the Responsible Entity to initiate this action precisely on this date and time. Initiating this process prior to would not meet the definition of "upon." Additionally, this obligates the entity to demonstrate that it met 2 distinct timetables "initiated…upon" and "complete…within 24 hours." We understand the intent is to encourage the entity to begin the process immediately, consistent with FERC Order 706, but we believe the drafting team has inadvertently set up a compliance trap for the industry. We recommend this language be changed to "For all termination actions, initiate the process to revoke the individual's unescorted physical access and Interactive Remote Access as part of the termination action, and complete the revocation within 24 hours after the effective date and time of the termination action. (R7 - part 7.5) We question the need to modify passwords for shared user accounts if there is no corresponding

requirement to disable individual accounts for the user who was reassigned or transferred. Additionally, as passwords are not a required authentication mechanism, we recommend that this requirement be modified to "change any shared authentication factors that are known."
No
No
(Part 1.1) The text of the requirement part includes "associated Protected Cyber Assets" but the applicability does not. Please clarify. (Part 1.5) Part 1.5 states that each entity must have a method for detecting malicious communications. This is vague. What level of detection is required? Would simply having log entries sent to a server for analysis be sufficient? Would it be sufficient if combined with a MSP service? The measures imply that only IDS would suffice, but entities have a right to more than an implication of what is required. If the SDT wants to require IDS, then it should be clearly stated. If not, it should provide a measurable standard of what level of detection is required. IDS devices could be incorporated into an access point, or located within an ESP; therefore the applicability only to EAPs may not be appropriate.
It is not clear whether the entire chain,: from user to Intermediate Device, and from Intermediate Device to Cyber System, must be encrypted or only one of the links. Please clarify.
No
Yes
Yes
(R1) We strongly disagree with requirement parts 1.4 and 1.6. Given the large number of field assets that are applicable to this requirement, a 2 hour monitoring outage that occurred more than 4 times in a year for any single facility would mean violation with this requirement. A single chronic communications circuit would easily put many entities into a non-compliant state. We recommend that CIP-006 utilize the same strategy employed in CIP-007 R4, part 4.3 - requiring the detection of failures and activating a response. We believe this incentivizes the proper behavior without causing unnecessary compliance issues. (Part 1.1 and Part 1.3) The requirement for two physical access controls goes beyond current industry standards and is not sufficiently connected to increased reliability to justify the expense involved. The definition of physical access control is not sufficiently clear. The language Physical Security Perimeter has been restored to the requirement, but there is no requirement to actually establish a PSP or a statement as to what devices must be within a PSP. We recommend that R1.1 be modified by adding “into each Physical Security Perimeter”. (Part 1.4) R1.4 Controls should control things; not monitor things. We recommend deleting the words “Have controls that” or changing them to “Implement measures to”. Automated systems typically cannot detect unauthorized physical access because they cannot distinguish between authorized key access and unauthorized key access. Consider adding the word “potential” before “unauthorized” if your intent is to monitor for events that may be unauthorized circumvention of a physical access control, such as a “forced open alarm” which could be the result of an authorized key entry or true forced entry. (Part 1.5) R1.5 Note that R1.5 does not require alerting on repeated invalid access attempts. Since access was denied, the control has not been circumvented. We do not object to this approach, but we want to be certain that this was the intent of the SDT. (Part 1.6) It is not clear what an entity is supposed to do to meet this requirement. How does one detect unauthorized physical access to a Physical Access Control System? Especially since the standard rationale for R1.1 states that Physical Access Control Systems do not themselves need to be protected by a Physical Access Control System. In light of this statement the measure for 1.6 makes no sense.
No
Yes
No
Yes
Yes
(Part 1.1) R1.1 requires that only needed ports be enabled. This implies that an entity must be able to justify the assertion that a port is needed. But the measures make no mention of the inclusion of the application for each port. It should be made clear, one way or another whether you are looking for a simply listing of the ports, or whether an entity needs to document the purpose or application of each port. (Part 1.2) The requirement is vague. It does not make clear what level of protection is required. The measure attempts to add more detail, but that is not the correct purpose of a measure;

if disabling the port in software, using a physical port lock or signage are the three possible solutions they should be included as such in the requirement. If those are not the only three possibilities entities need more specific information about what level of protection is required. Allowing protection via signage makes the requirement of little value. What is the reliabiliy benefit of having signage for physical ports? The standard requires protection only of unnecessary physical ports. The term unnecessary is vague. Many, if not most, physical console ports are used only for initial programming and then remain available for emergencies. If these ports are covered then the requirement is contrary to reliability because it encourages disabling or physically locking these ports that are already located in secure areas and can be critical for restoring failed systems. This requirement will delay or prevent responses to system failures in that case. If these ports are not covered then what is the point of the requirement? (Part 3.1) R3.1 is vague. It does not make clear what is required to meet it. Would a corporate policy stating that employees should not visit sites known to be sources of malware be sufficient by itself? The measures make some attempt to add detail (which is not the purpose of a measure), but even they are vague. For example, what constitutes “system hardening”, and “policies” could be almost any appropriate use policy. (Part 3.2) R3.2 is vague as well. What level of mitigation is required? We already mitigate this threat by the measures required by CIP 5 (limiting active ports on the perimeter). If that is enough, this requirement is duplicative; if it is not, how is an entity to know what additional steps are required? (Part 4.1) R4.1.4 is vague. What activities, beyond those listed in 4.1.1-4.1.3 would be included? (applies to 4.2.1 as well)
(Part 5.1) For systems not associated with control centers, please clarify that "user access" does not include the ability to interact with the LED/LCD panel on the front of a device (such as a protective relay or meter).
Individual
Brian J Murphy
NextEra Energy, Inc.
No
No
No
No
No
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R1.1 be revised to read as follows: “A security awareness program that, at a timeframe deemed necessary by the Responsible Entity, conveys ongoing reinforcement of cyber security practices for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems. “ And, also R3.2 to be revised to read as follows: “Require completion and documentation of the training specified in CIP-004-5, Requirement R2 as deemed necessary by the Responsible Entity.” Also, R4.2 should be revised to require that the Responsible Entity have a current criminal background check, and not impose or suggest arbitrary timeframes that unnecessarily and overly complicate or micromanage the intent of the requirement. R4.2 should be revised to read as follows: “A current and up-to-date criminal history as the Responsibility Entity deems necessary.” Similarly, R5.2 should read as follows: “A current and up-to-date PRA with no lapses in criminal history, unless such lapses are justified and documented.”
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and micromanagement of the program. To implement these changes, NextEra requests that R6.5 be revised to read as follows: “Verify, at a timeframe that the Responsible Entity deems necessary, that individuals provisioned for authorized electronic access or authorized unescorted physical access have associated authorization records. “ Similarly, revise R6.6 and R6.7 to read as follows: “For electronic access, verify, at a timeframe that the Responsible Entity deems necessary,

that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines necessary for performing assigned work functions." "Verify, at a timeframe that the Responsible Entity deems necessary, that access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity are correct and those that the Responsible Entity determines necessary for performing assigned work functions. " Also, to provide for the recognition of extenuating circumstances (such as a hurricane or some other unforeseeable event), R7.1 and R7.3 should be revised to read as follows: "For all termination actions, initiate the process to revoke the individual's unescorted physical access and Interactive Remote Access upon the effective date and time of the termination action, and complete the revocation within 24 hours after the effective date and time of the termination action, unless there are extenuating circumstances that impact the completion of the revocation within 24 hours and such extenuating circumstances are documented." "For termination actions, revoke the individual's access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity by the end of the next calendar day following the effective date and time of the termination action, unless there are extenuating circumstances that impact the completion of the revocation within 24 hours and such extenuating circumstances are documented." Also, it is unclear what the wording of R7.2 means. While it may be understood the language is mirroring FERC's directive, it is generally understood that a Responsibility Entity needs flexibility to prioritize and implement compliance in a manner appropriate for the circumstances and situations. For example, for any employee that is reassigned for disciplinary reasons, a tight timeframe is appropriate, but for a normal employee transfer such a tight timeframe is unnecessary and inappropriately places an emphasis on revocation versus other aspects of the CIP program. Thus, additional flexibility, as appropriate, needs to be added to R7.2 as follows: "For reassignments or transfers involving disciplinary action, revoke the individual's electronic and physical access that by the end of the next calendar day following the reassignment or transfer, and for reassignments or transfers that do not involve disciplinary action, revoke in timeframes as deemed appropriate and documented in a procedure by the Responsible Entity."
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
No
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R3.2 be revised to read as follows: "Document outages for physical access control, logging, and alerting systems and retain the outage records for a time period as deemed necessary by the Responsible Entity." Also, NextEra does not take issue with the applicability sections of CIP-006-4 R1.3 through R1.6 or R3.1 or conceptually what the requirements are attempting to accomplish, but Nextera does believe that these requirements need to be revised in order to practically and cost effectively promote reliability and physical security. Thus, NextEra provides specific edits and a justification for the edits below for each of these requirements. R1.3 (edited) "Utilize one physical access control and one defense in depth control to allow physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access." NextEra believes that requiring two physical access controls or a technical feasible exception is unnecessarily redundant and does not promote cyber security in a practical or cost effective manner. Instead, NextEra is confident that requiring one physical access control and one defense in depth control is appropriate and will protect against unauthorized physical access. It is also NextEra's view that these two controls should be required, and, therefore, the technical feasibity exception language has been deleted. R1.4 (edited) "Have a control, as required in R1.3, that monitors the Physical Security Perimeter twenty four hours a day, seven days a week for unauthorized circumvention of a physical access control into a Physical Security Perimeter. In the event of an outage of the control, the Responsible Entity must take appropriate action to ensure there is no unauthorized circumvention into

the Physical Security Perimeter during the duration of the outage. The Responsible Entity must document the temporary approach used during the outage of the control, and document that no unauthorized circumvention into the Physical Security Perimeter occurred during the outage." NextEra agrees that 100% perfection is not possible, given the possibility of a malfunction or damage to a Physical Security Perimeter control. NextEra does not agree with the use of an unsupported, arbitrary 99.9% threshold. Instead, NextEra believes the same goal of security is accomplished if an appropriate reaction to the temporary outage of a control is taken and documented. Thus, NextEra recommends that its edits to R1.4 and R1.6, below, be employed instead of the 99.9% threshold. R1.5 (edited) "Within 15 minutes of an employee or agent of the Responsible Entity becoming aware that a Physical Security Perimeter has been breached by an unauthorized circumvention of a physical access control, the Responsible Entity shall issue an alarm or alert on the unauthorized circumvention of a physical access control to the personnel identified in the BES Cyber Security Incident Response Plan." Although NextEra agrees with the intent of R1.5, as worded it is not clear what is required by whom and when the 15 minutes starts to run. Thus, NextEra recommends that its edits to R1.5 be adopted to better explain the step-by-step process of the event and the action to be taken. R1.6 (edited) "Have a control, as required in R1.3, that monitors the Physical Security Perimeter twenty four hours a day, seven days a week for unauthorized circumvention of a physical access control into a Physical Security Perimeter. In the event of an outage of the control, the Responsible Entity must take appropriate action to ensure there is no unauthorized circumvention into the Physical Security Perimeter during the duration of the outage. The Responsible Entity must document the temporary approach used during the outage of the control, and document that no unauthorized circumvention into the Physical Security Perimeter occurred during the outage." R3.1 (edited) "Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter shall be conducted at least once every 36 calendar months to ensure the control, hardware or device properly function." NextEra finds no justification for increasing the maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter from 36 months (as is currently required in CIP-006-3) to 24 months. Although NextEra does not question the importance of maintenance and testing required in R3.1, its experience demonstrates that during a three year test of each Physical Access Control System and locally mounted hardware or devices, only minor, if any, issues are detected. These results suggest that any increase in testing intervals is not required to promote reliability or cyber security. Also, such an increase in testing intervals unnecessarily negatively impacts the cost effectiveness of implementing a cyber security compliance plan. In addition, NextEra believes that the R3.1 grammar and clarity can be improved. Accordingly, NextEra recommends that its edits to R3.1 be adopted.
No
No
No
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R.4.4 and R4.5 be revised to read as follows: "Retain BES Cyber System security-related event logs identified in Part 4.1 for a time period as the Responsible Entity deems necessary and where technically feasible." "Review a summarization or sampling of logged events at a timeframe as deemed necessary by the Responsible Entity to identify undetected Cyber Security Incidents."
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to EEI's comments, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R.5.6 be revised to read as follows: "For password-based user authentication, either technically or procedurally, that enforces password changes or an obligation to change the password at a timeframe deemed necessary by the Responsible Entity."
Individual

Michael Lombardi
Northeast Utilities
Yes
No
No
Yes
Yes
Yes
No
R2 and R3 – Recommend that Requirement R2 and R3 be revised to specify a general awareness training program is necessary to retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems. As currently proposed, requiring a role-based cyber security training program to retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems is problematic and provides little or no corresponding benefit. For example, a potentially problematic condition includes how to handle granting access to employees that have more than one role yet have only completed training for one role only – would they qualify for unescorted physical access or not? Similarly, as personnel are assigned new / additional roles, is their unescorted access jeopardized based on their increased responsibility? FERC Order 706, Para 434 does not specify role based training but indicates: “We [FERC] agree with commenters that information concerning vulnerabilities should be revealed on a need to know basis and not universally. However, any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions or inactions could, even inadvertently, affect cyber security.”
R7 – While Part 7.5 addresses that the Responsible Entity can determine and document that extenuating operating circumstances require a longer time period for changing passwords; it does not appear that a similar provision exists to allow the Responsible Entity to determine and document that extenuating operating circumstances can require a longer time period for revocation of access privileges. Recommend that Requirement R7 be revised (pursuant with FERC Order706, Para 463) to acknowledge that the Responsible Entity can determine and document that extenuating operating circumstances require a longer time period (beyond the default 24 hours) for the revocation of access privileges. FERC Order 706, Para 463 states: “We [FERC] acknowledge that not all disciplinary actions warrant revocation of access privileges. In addition, certain personnel transfers can require a protracted transitional process that warrants retention of access privileges after the formal transfer date. There may be operational reasons that justify retention of access privileges after an employee transfers, but the default procedure should be to cancel access privileges at transfer and to document any exceptions to that policy for audit purposes.”
Yes
Yes
None
Request clarification on R2 Part 2.2 - Is the entire link from field device to desktop user required to be encrypted, or just the desktop to intermediate device, or field device to intermediate device?
No
Yes
Yes
Table R1, Part 1.6 - Requires 99.9% availability yet no availability methodology or time frame is provided. Please clarify how the availability calculation should be performed. A simple example of the need for clarification is: a physical access control system is unavailable for 4 hours on one day but is available for the remainder of the year. Hence daily availability = 83.33% (20/24 hours), weekly availability = 97.62% (164/168 hours), and the annual availability = 99.95% (8756/8760). Additionally, please clarify the applicability of this requirement, e.g., is it to the overall control system or each individual door, panel, etc? Please clarify how scheduled outage time is handled (and whether it is excluded from the availability calculation). Lastly, please provide the basis for 99.9%.
Yes
Yes

Yes
Yes
Yes
Table R1, Part 1.2 - Suggest Measure be revised to remove “signage” as an alternative to physically securing a port. Table R2, Part 2.4 - Appears change rationale is from Part 2.2 and does not address 2.4. Table R3, Part 3.3 - suggest rewording from “(this does not require use of every available release, but that for every release that is available, at least one update has occurred within 35 calendar days from that release)” to “(this does not require use of every available release, but that for every release that is applicable, at least one update has occurred within 35 calendar days from that release). Table R4, Part 4.2 - Suggest “real-time” be removed as determinations are not made in real time. Rather, events are capture and evaluated. Table R4, Part 4.5 - Consideration of Comments from the prior posting indicated “Responsible Entities may engage in automated or manual review in accordance with their current or future capabilities.” The flexibility and the allowed use of automated reviews is appreciated. Application Guidelines - Please provide more details in the Application Guidelines on TFEs that may be allowed on equipment that does not run malicious code Request clarification on R4, Parts 4.1.1, 4.1.2, 4.1.3, 4.1.4 - Are log events required for local, remote or both types of access?
None
Group
Florida Municipal Power Agency
Frank Gaffney
Yes
Yes
Yes
Yes
Yes
No
No
(1) Question 5: The end of the sentence of bullet 5.2 should be changed to include “calendar”, e.g., “no older than seven calendar years”.
(1) Question 6: R6 has too many proscriptive internal controls within the bullets that should be eliminated, especially in light of paragraph 81 of the FERC Order approving Find Fix Track and Report, e.g., there is no need to designate individuals able to authorize, etc. Bullets 6.6 and 6.7 are unnecessary and are redundant to 6.5. In other words, 6.6 and 6.7 are too proscriptive for how to accomplish 6.5. (2) Question 7: Bullet 7.1 is impossible from a temporal perspective. It is impossible to “initiate the process to revoke … upon the effective … time of the termination action”, literally meaning simultaneity which is impossible to achieve. The only important part to the bullet is to revoke access within 24 hours and the rest should be eliminated.
Yes
Yes
No
No
No
(1) Question 14: See comments on definition of Physical Security Perimeter. Bullets 1.7 and 1.8 could be interpreted as requiring continuous availability of alarming and logging systems. FMPA suggests adding the 99.9% availability used in bullet 1.6 to bullets 1.7 and 1.8 as well. Bullet 1.9 is a data retention requirement that is a compliance element, not a requirement (especially in light of paragraph 81 of the FERC Order approving FFTR), and should be deleted. READ-ONLY ACCESS There is no provision for a “read only” version of electronic access without meeting the requirements for unescorted electronic access. We believe that there ought to be a method for “escorted” electronic access, e.g., read-only access, e.g., something akin to WebEx – if you let someone view your screen

but don't give them control, that would be a form of "read only" supervised access. This kind of access should be encouraged, for a number of reasons, including: 1) Having this form of 'read only' access makes it easier for companies to get support on issues without having to worry about a litany of training & background check issues 2) By not having so many people with access to critical assets, it obviously lowers the number of people on your lists which makes tracking people less of a burden. Also by keeping the list smaller you inherently gain security. 3) Assuming you have internal employees actually performing the access (or "driving", if you will), it has the potential for them to increase their comprehension of how things work, thereby creating a more robust BES by having better educated operators 2- QUESTION 15: Bullet 2.1 is not measurable without video surveillance or similar surveillance. Continuous is impossible to prove without such surveillance. Is that the intent of the SDT? The Measure does not match the Requirement. Bullet 2.3 is a data retention requirement that is a compliance element, not a requirement (especially in light of paragraph 81 of the FERC Order approving FFTR), and should be deleted. 3- QUESTION 16: The second part of Bullet 3.2: "and retain the outage records for at least 12 calendar months" is a data retention requirement that is a compliance element, not a requirement (especially in light of paragraph 81 of the FERC Order approving FFTR), and should be deleted.
No
Yes
Yes
No
No
1- QUESTION 18: For CIP-007-5 bullet 1.1, the auditors have taken the word "services" to mean "applications" running on a computer. Which means right now they expect you to show all the things that MIGHT start on a Windows (or Unix) box, and if they're not needed, disable them. We believe the SDTs intent is concerning network communications and not services like those that automatically configure to connected hardware. We suggest to include the following language in the bullet: "that initiate or receive network communications" after "services", i.e: "For applicable Cyber Assets and where technically feasible, enable only logical network accessible ports needed, including port ranges or services that initiate or receive network communications where needed to handle dynamic ports." 2- QUESTION 21: Bullet 4.1 implies a 100% availability of a logging system. FMPA suggests using the 99.9% availability used in CIP-006-5 Bullet 1.6. Bullet 4.4 is a data retention requirement that is a compliance element, not a requirement (especially in light of paragraph 81 of the FERC Order approving FFTR), and should be deleted.
QUESTION 22: Bullet 5.2 is an internal control not worthy of a requirement, especially in light of paragraph 81 of the FERC Order approving Find Fix Track Report. FMPA suggests deleting the bullet.
Individual
Yuling Holden
PSEG
Yes
Yes
Yes
Yes
No
Yes
Yes
In R5.2, change the measure "Evidence may include, but is not limited to, current and previous personnel risk assessment records" to delete the word "current." There is no benefit to keeping records that may go back 14 years.
Yes
No
We are struggling with dial-up applicability as it relates to interactive remote access. Specifically, is a

dial-back modem can be considered as an Intermediary Device? If it is, then there are difficulties in meeting complying with R2 (such as 2.3 and 2.2). If it is not, then how can it be an option within R1 (R1.4)?
No
Yes
Yes
R1.6: Monitoring 24*7*365 with a 99.9% uptime would require extensive resources to satisfy the supporting documentation. Please provide a basis for the requiring a 99.9% uptime. Also, we are looking to clarify the method that is used to calculate the percentage of availability for our systems. For example: If a badge reader is malfunctioning, but the door is locked, so no access is granted, would this count as an outage, as the security of the site was not compromised? With regard to the Measure for R1.6: It seems that there is a significant difference between the Requirement and the Measure. We propose the following language in the Measure to appropriately correlate the two: instead of “Evidence may include, but is not limited to, documentation of controls that monitor the Physical Security Perimeter for unauthorized circumvention of a physical access control into a Physical Security Perimeter.” We propose “Evidence may include, but is not limited to, documentation of controls that monitor the Physical Access Control System.”
Yes
Yes
Yes
No
Yes
For Requirement R4.5, Please provide guidance as to what acceptable tolerance range for such sampling. Once this clarification is provided, our objection would be removed VSLs: R1: There is only a Severe VSL. We would like to see a gradation with regard to the VSLs – If a single device is affected, there may be less severity than if many devices are affected. R2 -R3: R2 escalates by 15-day increments and R3 escalate by 10-day increments. We believe there should be consistency across similar VSLs. General comment on requirements with only a Severe VSLs: There should be gradations that include lower VSLs on the basis of the difference between missing a subset of the devices or systems and missing all of such systems.
Group
Pepco Holdings Inc & Affiliates
David Thorne
Yes
Yes
Yes
Yes
Yes
No
Yes
1) Q6—R6 -NOT CLEAR: individuals provisioned for authorized electronic access or authorized unescorted physical access have associated authorization records. Change Rational: This requirement clarifies the review should occur between the provisioned access and authorized access. What review? Are they not 2 different authorizations?
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Group
National Rural Electric Cooperative Association (NRECA)
Barry Lawson
No
R1.4 – The requirement for 99.9% availability for physical security perimeter controls is problematic due to requiring tracking of availability without defining a time period for determining the percentage. The SDT needs to revisit this requirement to reduce the complexity of tracking such availability and to create a clear requirement on this issue.
Individual
Jennifer Wright
San Diego Gas & Electric
No
No
Individual
Don Jones
Texas Reliability Entity
Yes
Yes
Yes
Yes
Yes
Yes
No
CIP-004-005 Table R7 part 7.4 should be deleted. Allowing 30 calendar days is excessive. CIP-004-005 Table R7 part 7.5 should include Medium Impact BES Cyber Systems.
Yes

Yes
No
Yes
No
R1.7 does not indicate follow up on the unauthorized access alert by the personnel identified in the BES Cyber Security Incident Response Plan. R3.1 should be tested annually.
Yes
Yes
Yes
Yes
Yes
Individual
Don Schmit
Nebraska Public Power District
Yes
No
No
Yes
Yes
Yes
No
[R1] though we recommend changing “ongoing reinforcement of cyber security practices” to “ongoing reinforcement of security practices” to prevent limiting awareness messages to cyber to the exclusion of physical security awareness, as well. [R2] Each type of role-based training, 2.2-2.10, should be optional for some identified roles and required for others, and that distinction should be programmatically documented. That needs to be clearer in the structure of this requirement. If each of 2.2 through 2.10 were preceded with “Based on the role identified in R2.1…“ The way this is written today, it appears as though all of this training is required for anyone with any type of access. Additionally, some of this training should not be given to someone before the access is granted, based on the sensitivity of the information. Recovery information, for example, should wait until the access is completely authorized and the person has met all prerequisites and other operational training. [R3] Legacy phrasing with regard to the date overall training is required was sufficient as long as it was broad enough to educate those granted physical or electronic access. More specific, role-based training should be provided within an appropriate timeframe after acquiring certain responsibilities and should be necessary for retaining those responsibilities. The date of the acquisition of those responsibilities should be tied to departmental documentation and roles/responsibilities lists instead of HR reports on official job change. This allows for transitions required by reliable operations, as well as training periods. Also, with respect to demonstrating training when the access is attained, it forces the entity to maintain a complete history for each person who has ever had access and what training he or she has received since the very first access was obtained. This could be decades worth of training materials, so we’d support the addition of a retention guideline that refers to access attained since the last audit. [R4] With respect to demonstrating initial PRA when the access is attained, it forces the entity to maintain a complete history for each person who has ever had access and the PRA he or she had when the very first access was obtained. This could be decades worth of PRA materials, so we’d support the addition of a retention guideline that refers to access attained since the last audit.
R7.2: Too short a time span. Recommend returning to legacy timeframes for job changes within an organization or extending the allowable timeframe based on business days instead of calendar days. For a job change, there is no urgency associated, so weekend access removals are unnecessary. Additionally, there need to be provisions within the Standards for situations where a person will need

to straddle two jobs until a replacement is up to speed. R7.3: Too short a time span. Recommend extending the allowable timeframe based on business days instead of calendar days. The access removals associated with 7.1 should be sufficient to compensate for the risk introduced by waiting through a weekend for information access removals. R7.4: If 'revoke' in this case means to 'delete' the user account from the system, we disagree. We would disable the account and possibly change the account password but when you delete a Windows account you can never reclaim the original GUID that Windows assigns to the unique account. Therefore, reporting, file ownership and anything relating to the GIUD will have been lost and difficult to track past account activity. This may be true for other operating systems as well. : If disabling their domain accounts and physical access effectively terminates access, do we still need the urgency of 24 hrs? I understand the logic behind this but would rather see this as a 30 day requirement. R7.5: The "out" for extenuating operating circumstances should be applied to all CIP 4 R7 requirements.
No
Yes
[R1.1] Proposed verbiage change for the applicability. R1.1 “All BES Cyber Assets…” should apply to BES Cyber Assets associated with High and Medium Impact Sites that have external routable connectivity. There should not be an obligation to create an ESP with an EAP around an otherwise isolated network. This ties into the proposed definition for ESP and should be considered along with that proposed definition. [R1.2] Recommend combining 1.1 and 1.2, after the changes to the applicability and definitions are completed. [R1.5] Change applicability verbiage to Electronic Access Points associated with ESPs at High Impact Sites and Electronic Access Points associated with ESPs at Medium Impact Control Centers. The requirement is very subjective and may not be feasible for encrypted communications. This requirement needs to be clarified or stricken.
None.
No
Yes
Yes
R1.2 Ensure applicability statements clarify that the associated EAC and Protected Cyber Assets are those associated with Medium Sites. R1.4 –The identified percentage requires a level of tracking for monitoring that may not be technically feasible. Additionally, a .1% down time for monitoring security will accumulate for monthly planned outages to implement patches so would like to see allowances for this. A percentage uptime figure should be removed from the standard. Placing specific values such as this should not be included in standards and are audit bait that auditors will try to prove rather than focusing on overall security posture. If an entity can show all outages and maintenance and associated compensating controls during the outage, this is sufficient control, as is required in R3.2 already. Proposed Verbiage: Have controls that monitor the PSP 24X7 with mechanisms for identifying and documenting planned or unplanned outages. R1.5: Recommend striking the reference to “within 15 minutes of detection” and, instead, require the documentation of appropriate response timing within incident response plans. R1.6 The identified percentage requires a level of tracking for monitoring that may not be technically feasible. Recommend have controls that monitor the PSP 24X7 with mechanisms for identifying and documenting planned or unplanned outages. R1.7: Recommend striking the reference to “within 15 minutes of detection” and, instead, require the documentation of appropriate response timing within incident response plans.
Yes
No
No
No
No
Ensure the “zero defect” language in the VSLs is changed to be in alignment with EEI comments and the requirements, themselves. [R1.1] Propose defining “network accessible” to clarify the requirements around the additional controls offered by firewalls and ports accessible only to the local host and whether those controls can be considered sufficient. Also recommend adding the routable connectivity qualifier on the whole of R1, including High and Associated cyber assets. [R2.3] Recommend removing the term “dated” from the action plan to allow waiting for an outage or window that is not yet scheduled. [R2.4] Recommend adding flexibility to change the plan without risking

non-compliance. Proposed Verbiage – “For each plan created or revised in 2.3, document the actual implementation date and the reasoning for any discrepancies between the planned and actual implementation.” [R3.3] This applicability should be limited to just those systems with External Routable Connectivity. Without that connectivity, the monthly signature updates are not commensurate with the actual risk. [R4.1]Proposed Verbiage: “Within the capabilities of the BES Cyber System, log events such that Cyber Security Incidents can be identified and investigated. Event types include: …” [R4.2] Proposed Verbiage: “Within the capabilities of the BES Cyber System, generate alerts for detected security events that the responsible entity…” [R4.3] Recommend striking this requirement or changing the verbiage to “Document the controls implemented to identify and respond to detected logging failures. Document detected logging failures along with any discrepancies between the actual response and the documented response plan.” [R4.4] Proposed Verbiage: Remove “Where technically feasible” and precede requirement with “Within the capabilities of the BES Cyber System. [R4.5] Ensure “High” is a qualifier for each of the systems identified in the applicability column. Proposed Verbiage to add clarity: “Document and implement a program to review a summarization or sampling of logged events, at a minimum, every two weeks, to identify un-alerted Cyber Security Incidents.” Rationale – with the documentation of a program, the entity can define the criteria for sampling and summaries without risking a finding of non-compliance when not meeting the interpretation-based expectation of an auditor.
[R5.1] Propose change to “within the capability of the BES Cyber System” instead of “technically feasible.” [R5.2] The CIP Senior Manager will not have the technical expertise to recognize the actual risk introduced by the presence or quantity of default or generic account types. The turnover rate at the organizational level at which this level of expertise exists would create a prohibitively administratively burdensome process without adding the desired oversight. Recommend striking this requirement or changing to allow designation similar to CIP-004 R6, without direct documentation ties to the Sr Mgr. [R5.4] Recommend changing “technically feasible” language to “within the capabilities of the system or allowable by support vendors.” Proposed Verbiage: “To the extent allowable by the support vendors and capabilities of the system, change default passwords, unless the default password is unique to the device or instance of the application.” Removed “on cyber assets” to align with the cyber system applicability column. [R5.5] Proposed Verbiage for 5.5.1: “Password length that is, at least, eight characters or the up to the maximum allowable by the system if that maximum is less than eight.” Carry this change through 5.5.2 to add clarity. [R5.6] Don’t touch this one – it’s great as it is. [R5.7] Recommend changing technically feasible language to “Where system capability or operational risk allow, limit the number of unsuccessful…”
Individual
AnthonyJablonski
ReliabilityFIrst
CIP-004-5 1. VSL for Requirement R1 a. ReliabilityFirst recommends modifying the ”Severe” VSL to state: “failed to implement its documented” to be consistent with the language in Requirement R1. This recommendation is based on the FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement. 2. VSL for Requirement R2 a. A reference to Part 2.1 (Identification of each role and training required for each role) is missing from the VSLs. If a responsible entity failed to include Part 2.1 in their training program, it is unclear what VSL category the responsible entity would fall under. ReliabilityFirst recommends adding a VSL which is associated with Part 2.1. b. The “High” VSL should be revised to reference missing “3 or more.” As stated in the current VSLs, the “Moderate” VSL jumps from missing “2 or more” to missing “4 or more” in the “High” VSL. 3. VSL for Requirement R3 a. The SDT may want to consider making the VSLs size natural similar to the way the VSLs for CIP-002-5 Requirement R1 are set up. For example, for Responsible Entities with more than 40 individuals use percentages and for Responsible entities with less than 40 individuals use a finite number. In some instances, applying a fixed number to an entity with a large size may result in a determination of violation that is higher or lower than might have been intended. Similarly, applying a percentage to an entity with a small size may result in grading a violation higher or lower than might be intended. 4. VSL for Requirement R4 a. There appears to be a typo in the “High” VSL. The reference to the parenthetical (4.5) should correctly point to (4.4). There is no Part 4.5 listed in the Requirement R4 table. 5. VSL for Requirement R5 a. ReliabilityFirst recommends modifying the “Severe” VSL to state: “The Responsible Entity failed to implement one or more documented processes for personnel risk assessments. (R5)” to be consistent with the language in Requirement R5. b. The SDT may want to

consider making the VSLs size natural similar to the way the VSLs for CIP-002-5 Requirement R1 are set up. For example, for Responsible entities with more than 40 individuals use percentages and for Responsible entities with less than 40 individuals use a finite number. In some instances, applying a fixed number to an entity with a large size may result in a determination of violation that is higher or lower than might have been intended. Similarly, applying a percentage to an entity with a small size may result in grading a violation higher or lower than might be intended.
CIP-004-5 VSLs 1. VSL for Requirement R6 a. ReliabilityFirst recommends modifying the “Severe” VSL to state “…failed to implement one or more documented...” to be consistent with the language in Requirement R6 2. VSL for Requirement R7 a. ReliabilityFirst recommends modifying the “Severe” VSL to state “…failed to implement one or more documented...” to be consistent with the language in Requirement R7. This recommendation is based on the FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement. b. For the “Moderate”, “High” and “Severe” VSLs, why is the following standard number and requirement number specifically spelled out in the VSL: “CIP-004-5 R7”? To be consistent with the format other VSLs, ReliabilityFirst recommends removing this language.
CIP-005-5 1. VSL for Requirement R1 a. ReliabilityFirst recommends modifying the first “Lower VSL” to state "failed implement one or more documented processes" to be consistent with the language in Requirement R1. Furthermore, ReliabilityFirst recommends moving this “Lower” VSL to the “Severe” category. If a Responsible Entity failed to implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1, ReliabilityFirst believes that entity has completely missed the intent of the requirement and should be “Severe” b. The VSL under the “Severe” category which states “External Routable Connectivity through the ESP was not through an identified EAP according to Requirement R1, part 1.2.” appears to be incomplete. ReliabilityFirst recommends modifying the VSL by adding the following language to the beginning of the VSL to make it a complete thought: “The Responsible Entity did not have all…”
CIP-005-2 VSL 1. VSL for Requirement R2 a. ReliabilityFirst recommends modifying the first “Lower” to state: "failed to implement one or more documented processes" to be consistent with the language in Requirement R2. Furthermore, ReliabilityFirst recommends moving this VSL to the “Severe” category. If a Responsible failed to implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2, ReliabilityFirst believes that entity has completely missed the intent of the requirement and should be “Severe”. b. ReliabilityFirst recommends adding the last bullet under the “Severe” category as a bullet under the “High” category as well (i.e. if you missed one of the three bullets you are a “High”. If you miss two of the three bullets you are a “Severe”).
CIP-006-5 1. VSL for Requirement R1 a. The second “High” VSL (the one dealing with Part 1.6) needs to have the erroneous word “has” removed from the beginning. ReliabilityFirst recommends the following: “The Responsible Entity does not have controls that monitor…” b. The fourth “Severe” VSL (the one dealing with Part 1.4) needs to have the erroneous word “has” removed from the beginning. ReliabilityFirst recommends the following: “The Responsible Entity does not have controls that monitor…” 2. VSLs for Requirement R3 a. To add further clarity to the “Moderate” VSL, ReliabilityFirst recommends the following: “The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems, but the testing was not performed on a cycle within 24 calendar months. (3.1)”
CIP-007-5 1. General comments on all VSLs a. ReliabilityFirst recommends adding a reference to the associated “Part” in which each VSL is related to. Without referencing the associated Part number, it is very hard to trace the VSL back to the associated Part number. 2. VSL for Requirement R1 a. ReliabilityFirst recommends modifying the first “Severe” VSL to state: “…failed to implement one or more documented...” to be consistent with the language in Requirement R1. This recommendation is based on the FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement. 3. VSL for Requirement R2 a. ReliabilityFirst recommends modifying the first “Severe” VSL to state: “…failed to implement one or more documented...” to be consistent with the language in Requirement R2. This recommendation is based on the FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement. 4. VSL for Requirement R3 a. ReliabilityFirst recommends modifying the first “Severe” VSL to state: “…failed to implement one or more documented...” to be consistent with the language in Requirement R3. This recommendation is based on the FERC Guideline 3, VSL assignment should be

consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement. 5. VSL for Requirement R4 a. ReliabilityFirst recommends modifying the first “Severe” VSL to state: “…failed to implement one or more documented…” to be consistent with the language in Requirement R4. This recommendation is based on the FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement.
CIP-007-5 1. VSLs for Requirement R5 a. ReliabilityFirst recommends modifying the first “Severe” VSL to state: “…failed to implement one or more documented…” to be consistent with the language in Requirement R5. This recommendation is based on the FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement. b. It appears a number of the Parts listed in the CIP-007-5 Table are not mentioned in the associated VSLs. The language in the VSLs needs to be consistent with the language in the associated Parts and cannot add requirements. For example it is unclear which VSL corresponds to Part 5.2. There is no mention of a “CIP Senior Manager or delegate” in any of the VSLs.
Individual
Christina Conway
Oncor Electric Delivery Company LLC
Yes
No
No
No
No
No
No
APPLICABILITY COMMENTS THAT APPLY TO CIP-004-5 R2 THROUGH R7: (1) There is general inconsistency among the applicability of requirements in CIP-004-5 with respect to how they apply to training, personnel risk assessment, and authorization and revocation requirements for different types of access. The applicability of each requirement should be reviewed from a functional perspective to determine how it applies to different types of physical, electronic, and information access. (2) Oncor’s primary concern is that the applicability of “Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity” is applied to all CIP-004 R2 through R7 requirements. This is not appropriate in many requirements due to the overriding applicability of other CIP V5 Standards. As Oncor describes below, in some instances the inconsistency can be cleared up by changing the applicability from “Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity” to “Medium Impact BES Cyber System with External Routable Connectivity.” (3) There are also several instances in which different types of access are addressed within the same requirement. Due to the varying applicability of different access types, it appears it will be necessary to separate these requirements into multiple requirements to properly address the applicability concerns. (4) Physical access: Per CIP-006-5 R1, physical access to “Medium Impact BES Cyber Systems without External Routable Connectivity” should not be subject to the training, PRA, and authorization and revocation requirements in CIP-004-5. The inclusion of “dial-up connectivity” in the applicability column of requirements related to physical access goes beyond the intended applicability in CIP-006-5 R1. To correct this issue, the applicability of CIP-004-5 R2.3, R2.5, and R6.3 should be modified to remove the references to “dial-up connectivity” in the applicability column. The requirements for CIP-004-5 R3.1, R3.2, R4 (and sub parts), R5 (and sub parts), R6.1, R7.1, and R7.2 will likely need to be split into multiple requirements to properly address the applicability scope differences. (5) Electronic access: The applicability of revocation requirements in CIP-004-5 R7.1 for Interactive Remote Access should be modified to exclude “dial-up connectivity.” This requirement will likely need to be split into multiple requirements to properly address the applicability scope differences. (6) Information access: There are inconsistencies between CIP-004-5 and CIP-011-1 with respect to the applicability of BES Cyber System Information requirements. CIP-004-5 R2.3, R6.1, R6.4, R6.7 and R7.3 should be modified to match the applicability of CIP-011-1. Additionally, if a change that Oncor in proposing to CIP-011-1 R1 and R2 is accepted, then there will be further inconsistency between CIP-004-5 and CIP-011-1 that should be reconciled. In its comments to CIP-011-1, Oncor proposes that the applicability to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity” to maintain

consistency with the scope of cyber systems/assets currently covered by similar requirements in CIP version 4. If Oncor's proposal for CIP-011-1 is adopted, it will become necessary to adjust the CIP-004-5 requirements for information access accordingly. To correct this issue, the applicability of CIP-004-5 R2.6, R6.4, R6.7 and R7.3 should be modified to remove the reference to "dial-up connectivity" in the applicability column. The requirements for CIP-004-5 R6.1 will likely need to be split into multiple requirements to properly address the applicability scope differences. R2 REQUIREMENT COMMENTS: The phrase "protecting the Responsible Entity's BES Cyber Systems" should be removed from the end of CIP-004-5 R2.2, R2.3 and R2.4 since applicability is addressed in the applicability column of each sub requirement. This change will also make R2.2, R2.3 and R2.4 consistent with the other R2 sub requirements. FURTHER R2 APPLICABILITY COMMENTS: There is an inconsistency between the applicability of CIP-004-5 R2.8 and CIP-009-5 that should be corrected so that the applicability of both sections match. Both CIP-004-5 R2.8 and CIP-009-5 address recovery plans; thus their applicability logically should be the same. In its comments on CIP-009-5, Oncor proposes that the applicability of CIP-009-5 R1.1, R1.2, R1.3 and R1.5 to "Medium Impact BES Cyber Systems" should be limited to "Medium Impact BES Cyber Systems at Control Centers." This change would concentrate the efforts of Responsible Entities on areas where the potential reliability impacts are the highest and would avoid the implementation of Standards that place additional/duplicate requirements on cyber systems/assets covered under the PRC standards. If Oncor's proposal for CIP-009 is adopted, it will become necessary to adjust the applicability of CIP-004-5 R2.8 by replacing "Medium Impact BES Cyber Systems with External Routable Connectivity or Dial-up Connectivity" with "Medium Impact BES Cyber Systems at Control Centers." R3 REQUIREMENT COMMENTS: The reference to "BES Cyber Systems" in CIP-004-5 R3.1 should be changed to "applicable cyber assets" to maintain consistent use of the applicability column. GENERAL COMMENTS: (1) Oncor supports the comments submitted by EEI in response to this question. (2) Oncor supports the comments submitted by the Texas RE NERC Standards Review Subcommittee in response to this question.

APPLICABILITY COMMENTS THAT APPLY TO CIP-004-5 R2 THROUGH R7: (1) There is general inconsistency among the applicability of requirements in CIP-004-5 with respect to how they apply to training, personnel risk assessment, and authorization and revocation requirements for different types of access. The applicability of each requirement should be reviewed from a functional perspective to determine how it applies to different types of physical, electronic, and information access. (2) Oncor's primary concern is that the applicability of "Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity" is applied to all CIP-004 R2 through R7 requirements. This is not appropriate in many requirements due to the overriding applicability of other CIP V5 Standards. As Oncor describes below, in some instances the inconsistency can be cleared up by changing the applicability from "Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity" to "Medium Impact BES Cyber System with External Routable Connectivity." (3) There are also several instances in which different types of access are addressed within the same requirement. Due to the varying applicability of different access types, it appears it will be necessary to separate these requirements into multiple requirements to properly address the applicability concerns. (4) Physical access: Per CIP-006-5 R1, physical access to "Medium Impact BES Cyber Systems without External Routable Connectivity" should not be subject to the training, PRA, and authorization and revocation requirements in CIP-004-5. The inclusion of "dial-up connectivity" in the applicability column of requirements related to physical access goes beyond the intended applicability in CIP-006-5 R1. To correct this issue, the applicability of CIP-004-5 R2.3, R2.5, and R6.3 should be modified to remove the references to "dial-up connectivity" in the applicability column. The requirements for CIP-004-5 R3.1, R3.2, R4 (and sub parts), R5 (and sub parts), R6.1, R7.1, and R7.2 will likely need to be split into multiple requirements to properly address the applicability scope differences. (5) Electronic access: The applicability of revocation requirements in CIP-004-5 R7.1 for Interactive Remote Access should be modified to exclude "dial-up connectivity." This requirement will likely need to be split into multiple requirements to properly address the applicability scope differences. (6) Information access: There are inconsistencies between CIP-004-5 and CIP-011-1 with respect to the applicability of BES Cyber System Information requirements. CIP-004-5 R2.3, R6.1, R6.4, R6.7 and R7.3 should be modified to match the applicability of CIP-011-1. Additionally, if a change that Oncor in proposing to CIP-011-1 R1 and R2 is accepted, then there will be further inconsistency between CIP-004-5 and CIP-011-1 that should be reconciled. In its comments to CIP-011-1, Oncor proposes that the applicability to "Medium Impact BES Cyber Systems" should be limited to "Medium Impact BES Cyber Systems with External Routable Connectivity" to maintain consistency with the scope of cyber systems/assets currently covered by similar requirements in CIP

version 4. If Oncor's proposal for CIP-011-1 is adopted, it will become necessary to adjust the CIP-004-5 requirements for information access accordingly. To correct this issue, the applicability of CIP-004-5 R2.6, R6.4, R6.7 and R7.3 should be modified to remove the reference to "dial-up connectivity" in the applicability column. The requirements for CIP-004-5 R6.1 will likely need to be split into multiple requirements to properly address the applicability scope differences. R7 REQUIREMENT COMMENTS: The requirement language for CIP-004-5 R7.2 should be modified as follows: "For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the DETERMINATION THAT ACCESS IS NO LONGER NECESSARY." This provides clarity regarding the timing of the access revocation. GENERAL COMMENTS: (1) Oncor supports the comments submitted by EEI in response to this question. (2) Oncor supports the comments submitted by the Texas RE NERC Standards Review Subcommittee in response to this question.
Yes
No
GENERAL COMMENTS: (1) Oncor supports the comments submitted by EEI in response to this question. (2) Oncor supports the comments submitted by the Texas RE NERC Standards Review Subcommittee in response to this question.
R2 APPLICABILITY COMMENTS: (1) The definition of "Interactive Remote Access" or applicability of CIP-005-5 R2.1, R2.2 and R2.3 should be adjusted to reflect the exclusion of serially connected/non-routable/non-network connected devices. There is minimal reliability benefit and significant cost associated with applying the CIP-005-5 R2 requirements to all serially connected/non-routable/non-network connected devices that require remote access. Authentication when establishing connectivity to these systems is covered by CIP-005-5 R1.4 and provides the required cyber security. The cleanest way to correct this issue is to adjust the definition of "Interactive Remote Access" as follows: "All user-initiated access OF BES CYBER ASSETS WITHIN AN ELECTRONIC SECURITY PERIMETER by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether routable or dial-up access, using a client or remote access technology. Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications." Alternatively, the applicability of CIP-005-5 R2.1, R2.2 and R2.3 could be changed from "Medium Impact BES Cyber Systems" to "Medium Impact BES Cyber Systems with External Routable Connectivity." (2) There is no mention of serially connected/non-routable/non-network connected devices in the CIP Awareness Bulletin (Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)) that initiated the CIP-005-3 SAR or the Guidance for Secure interactive Remote Access that was ultimately issued after the CIP-005-3 revisions were not adopted. All discussions in these documents are in the context of IP addressable devices connected to a network that could be protected through the use of VPNs, proxy servers, etc. The current definition of "Electronic Security Perimeter" in the "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" has evolved to make a delineation between devices that are connected to a network via routable protocol and those that are not. This approach is consistent with and further supports Oncor's proposal to adjust the definition of "Interactive Remote Access" to exclude serially connected/non-routable/non-network connected devices. (3) In addition, in Consideration of Comments – Cyber Security Order 706 Version 5 CIP Standards (definition of "Electronic Access Point" section), it provides the following: "The SDT has not included serial, non-routable communications within the definition of EAP (other than with respect to dialup in CIP-005 R1.4). Dedicated serial communications are intentionally left out of scope, as the SDT believes it would be inappropriate for the standards to mandate a universal perimeter or firewall type security across all entities and all serial communication situations. There is no 'firewall' capability for a RS232 cable run between two cyber assets. Without a clear security control that can be applied in most every circumstance, such a requirement would just generate TFEs." This demonstrates that the SDT considered and rejected the inclusion of serial, non-routable devices and specifically chose not to include them in the definition of "Electronic Access Point." Thus, Oncor's proposal is simply urging that the same approach be taken with respect to "Interactive Remote Access" and that it not include serially connected/non-routable/non-network connected devices. (4) Oncor further requests additional information in the guidance section that addresses what is and is not a remote access client or remote access technology.GENERAL COMMENT: Oncor supports the comments submitted by EEI in response

to this question.
No
Yes
No
R1 REQUIREMENT COMMENTS: (1) The 99.9% availability requirements associated with CIP-006-5 R1.4 and CIP-006-5 R1.6 would place an undue burden on the Registered Entities to accomplish the desired availability and maintain satisfactory supporting documentation while resulting in negligible reliability improvements when applied to “Medium Impact BES Cyber Systems with External Routable Connectivity.” These requirements are particularly troublesome when considered in the context of remote switching station locations that are subject to the performance of communication channels to achieve these requirements. One could assume that to reliably achieve a 99.9% availability of Physical Security Perimeter monitoring/control, it would be necessary to post a guard (or have someone on-site) 24x7x365. For these reasons Oncor proposes to limit the applicability of these requirements to High Impact BES Cyber Systems. As CIP-006-5 R1.4 and R1.6 apply to “Medium Impact BES Cyber Systems with External Routable Connectivity,” the required availability should be reduced to a more reasonable percentage (99% or less) to accommodate potential communication channel outages. (2) CIP-006-5 R1.5 should be modified as follows to clarify what type of activity is being monitored and ensure that the 15-minute clock does not start until the message reaches the monitoring location: “Issue an alarm or alert in response to detected unauthorized ACCESS into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection AT THE MONITORING LOCATION.” CIP-006-5 R1.4 and 1.6 address the availability requirements of the access and monitoring systems, thus CIP-006-5 R1.5 should only address how the detection is handled after notice is received at the monitoring location. (3) CIP-006-5 R1.7 should be modified as follows to clarify that the 15-minute clock starts after unauthorized physical access is detected: “Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the DETECTED unauthorized physical access.” R2 REQUIREMENT COMMENTS: The wording of CIP-006-5 R2.1 should be simplified by shifting the focus from visitors to individuals. Proposed wording for CIP-006-5 R2.1: “Require continuous escorted access of INDIVIDUALS NOT AUTHORIZED FOR UNESCORTED PHYSICAL ACCESS within each Physical Security Perimeter, except during CIP Exceptional Circumstances.” R3 APPLICABILITY AND REQUIREMENT COMMENTS: The category of “locally mounted hardware or devices at the Physical Security Perimeter” requires additional detail, or it should be removed. This concept originates within the “Physical Access Control System” definition (where locally mounted hardware is exempt) and extends into the CIP-006 requirements. The term “locally mounted hardware or devices at the Physical Security Perimeter” is overly broad and could arguably include hardware and devices that have little or no impact on security. Likewise, documenting outages for “locally mounted hardware” could require significant resources and yet provide minimal, if any, security benefit. Therefore, Oncor proposes that “locally mounted security devices” be substituted in place of “locally mounted hardware or devices.” GENERAL COMMENTS: (1) Oncor supports the comments submitted by EEI in response to this question. (2) Oncor supports the comments submitted by the Texas RE NERC Standards Review Subcommittee in response to this question.
Yes
No
No
No
No
R2 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-007-5 R2.1, R2.2, R2.3 and R2.4 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity.” The exclusion of cyber systems/assets with no routable connectivity will eliminate a significant burden of tracking and documentation requirements associated with serially connected devices that would have minimal impact to reliability. This is particularly burdensome for systems that are geographically dispersed and would require direct personnel interaction and physical access to each device to deploy patches to non-externally routable systems. R2 REQUIREMENT COMMENTS: The 30-day timeframe in CIP-007-5 R2.2 should be increased to at least 35 days to allow for monthly processes. R3 APPLICABILITY COMMENTS: (1) Oncor proposes that

the applicability of CIP-007-5 R3.1, R3.2 and R3.3 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity.” This will minimize the application of these requirements to devices that are not susceptible to malicious code because they are not connected to a network with external routable connectivity. (2) The applicability of CIP-007-5 R3.3 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity” in recognition of the need for external connectivity to accomplish the 35-day update cycle. Registered Entities may be encouraged to remove malicious code protections that use signatures or patterns from medium impact systems without external connectivity if they are required to visit the site every 35 days to update signatures or patterns. R4 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-007-5 R4.1 and R4.4 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity.” This will minimize the application of these requirements to devices that are not capable of the detecting/logging requirements in CIP-007-5 R4.1, thus reducing documentation requirements that have no impact on security. R4 REQUIREMENT COMMENTS: (1) In addition to the applicability changes, Oncor requests that the ”Requirement” language of CIP-007-5 R4.1 be revised to match the ”Measures” language as follows: “Log events OF WHICH THE BES CYBER SYSTEM IS CAPABLE OF DETECTING AND, FOR GENERATED EVENTS THE BES CYBER SYSTEM IS CONFIGURED TO LOG for identification of and after the fact investigations of….” (2) A qualifier should be added to the end of CIP-007-5 R4.1.4 to indicate that malicious activity should be detected and logged “as required in the cyber security incident response plan.” GENERAL COMMENTS: (1) Oncor supports the comments submitted by EEI in response to this question. (2) Oncor supports the comments submitted by the Texas RE NERC Standards Review Subcommittee in response to this question.
R5 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-007-5 R5.1 and R5.4 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity or Dial-up Connectivity.” This will create consistency with the applicability of CIP-004-5 R6.2 and correctly captures the asset classifications for which authentication would provide a reliability benefit. R5 REQUIREMENT COMMENTS: (1) CIP-007-5 R5.2 and R5.3 are redundant to CIP-004-5 R6 and should be removed. Authorized access is addressed in CIP-004-5. (2) The requirement language of CIP-007-5 R5.4 should be modified as follows: “Change KNOWN default passwords, where technically feasible, unless the default password is unique to the device of instance of the application, on Cyber Assets.” This will prevent Registered Entities from being held responsible for accounts that are unknown to them. GENERAL COMMENT: Oncor supports the comments submitted by EEI in response to this question.
Group
Luminant
Rick Terrill
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
Individual
Stephanie Monzon
PJM Interconnection
Yes

No
No
No
Yes
No
No
R2 - Remove “role-based cyber security training” to training based or tailored to job function. Role-based seems that it is inferring that training should be based on permissions or that access should be role based. R2.1 - Change “identification of each role” to “identification of roles” required for BES cyber access. Consider removing R2.10, it is difficult to determine the intention of this requirement. It does not add anything that is not covered in 2.2 through 2.9 R3 - Remove “role-based cyber security training” to training based or tailored to job function. Role-based seems that it is inferring that training should be based on permissions or that access should be role based R 4.3 –We believe that the term “criteria” should be left out of the requirement. Reviewing PRAs is a highly subjective process that is handled on a case by case basis, and we believe that only a process that helps drive decisions should be included here.
R 6.6 - Remove Measure “2. A summary description of privileges associated with each group or role;“ R 7.2 –In reassignments or transfers knowledge transfer can take extended period of time (some positions that are recently vacated also are not immediately filled when transfer/reassignment is completed). Stipulations should be present to allow for this knowledge transfer to ensure that access is not revoked before it is truly not needed any longer. The change rationale does not match part 7.2. As stated above, the requirement in the table currently reflects the need to cut access immediately as of the transfer, rather than allowing for proper transition plans to be executed. Measures for 7.2 contain numbered list. The opening line should read ‘Evidence must include’. Or the list should be changed to a bulleted list.
No
No
Part 5.1 remove the word “all” or be specific to scope. Define what is meant by “user access”. Provide better examples for measures in order to provide guidance for intention of the requirement. Reword requirement to “Enforce authentication of interactive user access to Applicable BES Cyber Systems and associated Cyber Assets, where technically feasible.” or change to require authentication of accounts. R1.1 – Requirements mention Cyber assets that are not in the applicability column R1.2 Add external routable verbiage under applicability of last item R1.3 & 1.5 Access points for assets needs to be clarified. Is it ESP? R1.4 Add associated Cyber assets in applicability column R1.5 The Measures are prescribing an Intrusion Detection System, however such system is not prescribed in a requirement. The references to an IDS should be removed or it should mention that other methods are available. Other systems and tools can be used to detect malicious communication other than an IDS.
We will wait for IRC comments
No
No
Yes
R1.8 – Please add verbiage to include exit as well as entrance. There also needs to be an exception to include emergency exit such as fire drill (CIP Exceptional Circumstance) Evidence retention – Is it evidence or data that should be kept for 90 daysit? One may be able to show evidence of logs but not be able to produce the actual data itself R2 - Measure in Part 2.2 appears to be a copy and paste error. Suggest revisiting Measure 2.2 as it does not align with the requirement R3.2 says to retain records for 12 months. In order to meet the 3 year requirement could we get clarity on producing evidence of compliance vs the actual data?
No
No
No
No
No

R1 - Instead of class of cyber asset, use verbiage from CIP 10 Requirements need to address justification for ports & services that are enabled R2 Please provide clarity on what constitutes a security patch Please provide clarity on what it means for a cyber asset to be updateable R2.2 can a control system vendor be referenced as the source for the 30 day timeline even if the patch originates from a technology vendor? Please provide clarity on what “applicability” means 2.3 “the vulnerabilities within exposed by each security patch” insinuates that the security patches create vulnerabilities R3 R3 and R4 one states malicious code and the other states malicious software. Suggest changing to malicious code for consistency. Part 4.1.4 suggest removing this part. Otherwise, define what is malicious activity. This is subject to interpretation. Malicious activity requires analysis and is not something that can be logged. Part 4.2.1 suggest removing this part. Otherwise, define what is malicious activity. This is subject to interpretation. Malicious activity requires analysis and is not something that can be logged. Part 4.2 remove “real-time”. Is real-time when the event is received by a tool or when the event occurred on a cyber asset. Some events may only be processed by a tool on a daily basis (batch). Part 4.3 standardize with CIP-006 R1.6 in regards to availability and keeping records for outages. Is the requirement in regards to the security monitoring logging capability or in regards to a cyber asset not logging? R4.4 should be bullets rather than numbers Part 4.5 should only pertain to where automated processes and alerting are not possible. Evidence retention – Is it evidence or data that should be kept for 90 daysit? One may be able to show evidence of logs but not be able to produce the actual data itself
5.6 does not match he other R5 sections in the Applicability column. “Medium Impact BES Cyber Systems at Control Centers with External Routable Connectivity" R5 & R6, remove attestation as a measure, instead “provide procedure” R5.6 Periodically spelled incorrectly as “Periodicity”
Individual
Frank Dessuit
NIPSCO
Yes
Yes
Yes
No
Yes
Yes
No
R2: Change the measure to indicate “Cyber Security policies” instead of “Security Controls” to be consistent with the requirement. R4: NERC should clarify whether modifications to this standard require current personnel with access to undergo another background check, or whether they be grandfathered in. Setting a hard line of when employees “fail” a PRA is difficult, as it may determine on what role the individual is performing. It might even be more difficult to have “fails” defined for each role within the organization. The registered entity should be permitted to establish criteria that includes the entity using judgmental decision making. 4.2.3 NERC should clarify whether this applies to distance learning (e.g., online universities). 4.2. NERC should clarify whether this requirement applies to the location a contractor has been working at or his company headquarters. 4.3 Requirements will need to be negotiated with applicable unions and labor agreements. 5.2 NERC should clarify whether data retention of the current and previous personnel risk assessment records requires a responsible entity to maintain 14 years of background history.
R7: NERC should provide a precise definition of “Termination Actions”. 7.5 This requirement is overly and unduly burdensome because physical and interactive remote access has already been removed. With these accesses being removed entities should be able to change shared account passwords on their normal schedules. 7.2 There are times when a transferred employee still needs access due to transitional responsibilities; therefore, access will be required beyond the next calendar day. The requirement should be changed to state that the employee’s access will be removed at the end of the transitional period.
Yes
Yes
1.1, “Associated Protected Cyber Assets” should be removed from the requirement or added to the Applicable BES Cyber Systems and Associated Cyber Assets column.

No
Yes
Yes
R1.6 – NERC should resolve inconsistencies in the measures and the requirements.
Yes
Yes
Yes
No
Yes
R4.1 – No TFE's are allowed on this requirement. NIPSCO is concerned that not all devices can satisfy this requirement. R2.2 and 2.3 – Change the applicability to 35 calendar days to allow for a once a month frequency with slight flexibility to account for months with 31 days or for beginning or ending of months on weekends
Individual
Andrew Gallo
City of Austin dba Austin Energy
Yes
No
No
No
No
No
No
Please see the comments submitted by the Texas Reliability Entity NERC Standards Review Subcommittee to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Reliability Entity NERC Standards Review Subcommittee to which Austin Energy has subscribed.
Yes
No
Please see the comments submitted by the Texas Reliability Entity NERC Standards Review Subcommittee to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Reliability Entity NERC Standards Review Subcommittee to which Austin Energy has subscribed.
No
Yes
No
The Requirement 1.7 table states: "Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the unauthorized physical access." Austin Energy believes the following language better reflects the purpose of the Standard: "Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the Physical Security Plan within 15 minutes of the unauthorized physical access." Additionally, please see the comments submitted by the Texas Regional Entity's NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Yes
No
No
No
No

Please see the comments submitted by the Texas Regional Entity's NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Regional Entity's NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Individual
Steve Karolek
Wisconsin Electric Power Company
No
No
No
No
No
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Calendar year and 15 months are mutually exclusive. This requirement should use the term "Annual" as applied in NERC CAN-0010. Further, the term Annual should be added to the NERC Glossary of Terms. (2) Table R1 Part 1.1 simplify wording from "conveys ongoing reinforcements" to "reinforces". (3) Table R4 Part 4.2 strike "at least" from the phrase "covering at least all locations" since all should be all and there is nothing more for it to be least of. Also, add the word "consecutive" to the six months requirement and specify "or" between resided or employed or attended school. (4) Table R4 Part 4.3 and Part 4.4 needs clarification that either a process or a list of criteria is sufficient for compliance. (5) Table R5 Part 5.1 delete the word "granted" from the phrase as it is redundant and potentially misleading. (6) Table R5 Part 5.1, remove the adjective "authorized" where it appears in the phrases "authorized electronic" and "authorized unescorted" as this adds confusion. (7) The first paragraph of guidelines and technical basis for R4 and R5 is a single sentence which runs on for 115 words. Please break this paragraph into discrete thoughts with shorter and easier to understand sentences.
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Calendar year and 15 months are mutually exclusive. This requirement should use the term "Annual" as applied in NERC CAN-0010. Further, the term Annual should be added to the NERC Glossary of Terms. (2) Table R6 Part 6.5 Measures column, please apply consistency of word order to "Dated document of verification..." and "Documentation of dated verification..." We have no preference for which order as long as there is consistency applied. (3) Table R7 Part 7.1 The current language and application guidelines fail to account for a few out-of-service transactions in which entities will not be able to meet the standard. For instance, an individual might be temporarily suspended while a performance or a misconduct investigation occurs. Perhaps ten days later, the individual is terminated but the effective date of the termination is the last day worked. The compliance personnel may be notified and act promptly on the date that the employer determines the individual should be terminated, but the records will indicate that compliance personnel acted ten days late. Consequently, we recommend a change from the wording "For termination actions, initiate the process to revoke the individual's unescorted physical access and Interactive Remote Access upon the effective date and time of the termination action and complete the revocation within 24 hours after the effective date and time of the termination action" to "For termination actions, initiate the process to revoke the individual's unescorted physical access and Interactive Remote Access when the entity determines that the individual should be terminated and complete the revocation within 24 hours after the effective date and time of the such determination". (4) VSLs for R7, Moderate. The sample violations should be moved down the scale one notch each. A single failure to revoke access for one individual should be in the lower VSL column, not the moderate VSL column. This also makes it consistent with the failure to act on a timely basis in the revocation of access to BES Cyber Information for a single individual.
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications (1) Table R1 Part 1.5 Measures column says "may include but is

not limited to". This is not consistent with the use of numbered lists separated by "and" which require inclusion of all list items. This wording needs to be clarified to indicate whether this is an "and" requirement which must include all items or an "or" requirement which may include but is not limited to these example items.
Wisconsin Electric Power Company supports EEI Member Consensus comments as submitted by EEI.
No
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Table R1 Part 1.5, simplify the wording "...unauthorized circumvention of a physical access control..." to "...unauthorized access..." (2) Table R1 Part 1.7 we suggest the action be related to detection. "...within 15 minutes of detecting unauthorized physical access". (3) VSL table R2 Moderate, delete "on a daily basis" which adds nothing to the meaning and, in fact, may lead to confusion in compliance. For example, what would a compliant record look like for a visitor whose visit lapsed from one calendar day into the next? (4) In the guidelines and technical basis for R1, delete any reference to the maximum size (96 square inches) of an opening. With the end of "six-wall perimeters", and the establishment of the requirement to enforce access control for the physical border surrounding locations, the number is meaningless.
No
No
No
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Table R1 Part 1.1 the listing of listening ports and services appears to be overlap or duplication with the baseline configuration requirements of CIP-010 and Wisconsin Electric is concerned about potential "double jeopardy" issues if something is missed on a list. If we have to retain the list for CIP-010 it should not also be required for CIP-007.
Wisconsin Electric Power Company supports EEI Member Consensus comments as submitted by EEI.
Individual
Kathleen Goodman
ISO New England Inc.
No
No
Yes
No
Yes
Yes
No
Recommend removing “, but not limited to,” from R1 Part 1.1 Measure since the Measures are only guidance Recommend removing “potential” from R2 Part 2.7 since an incident is determined to be real or potential during the follow up investigation. Request additional clarification on R2 Part 2.10 in the Application Guidelines. From the CIP-004-5 Table R2 - Cyber Security Training Program, the use of the terms interconnectivity and interoperability with regard to FERC Order No. 706 needs to be clarified to make the differences and applications of the terms understood. Request clarification on R4 Part 4.2 since it is not clear if the numbers should be read as “and” plus does the six months apply to all of the numbers? Prior versions of R4 Part 4.3 had exclusions for laws or collective bargaining agreements. Please add the exclusions or explain why the exclusions were dropped. Recommend different VSL thresholds for R3. Differentiating by individuals is bad for large organizations. Differentiating by percentage of associated is staff is bad for small organizations. Recommend different VSL thresholds for R5. Differentiating by individuals is bad for large organizations. Differentiating by percentage of associated is staff is bad for small organizations.
Request a more clearly worded R6 Part 6.4. The intent appears to be authorizing (electronic/physical)

access to BES Cyber Systems Information. Request additional clarification in this Requirement and Application Guidelines. Note that Requirement 6.1.3 also uses “physical and electronic locations.” In R7 Part 7.4, recommend changing “Requirements R7.1 and R7.3” to “Requirement R7 Parts 7.1 and 7.3.” In the corresponding Measure, recommend changing “removal” to “revoke” for consistency with the Requirement. In some systems removal results in removing all corresponding records which makes it hard to provide the proper records to the auditor. Recommend updating the R7’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures show R7 as “low”.
No
No
Recommend removing “, but is not limited to, ” from R1 Part 1.1 since the Measure’s scope already includes all of the possible Cyber Assets Measures should not dictate Requirements. If correct, then how can CIP-005 R1 Part 1.5’s Measure specify “intrusion detection system” when the Requirement does not specify a technology? Also specifying a technology may prevent a newer, better technology from being used until the Standard is updated. Recommend changing R1 Part 1.5 from “intrusion detection system” to “detection system” Request for clarification on how the math for R1 is done in the VRF/VSLs.
Request clarification on R2 Part 2.1 – can the Intermediate Device be on the ESP? Can the Intermediate Device also be an EAP? Recommend changing R2 Part 2.3 from “Factors must be at least two of the three following categories” to “Multi-factor include, but are not limited to” which allows future technology without a Standards update.
Yes
No
Recommend changing the testing in R3 Part 3.1 so that the High Impact BES Cyber Systems are tested every 24 months and Medium Impact BES Cyber Systems with External Routable Connectivity are tested every 36 months.
Yes
No
No
No
No
For R2, request clarification if the SDT’s intent is that the following timeline will be compliant or not. 1) on 5/1/2012 the patch is identified; 2) by 6/1/2012 complete the assessment for applicability (30 days); 3) by 7/1/2012 the plan is developed and defined for testing plus implementation (30 days); 4) per the plan, testing completed by 9/1/2012; 5) per the plan, patch deployed by 10/12/2012; 6) on 10/30/2012 patch fails (through no fault of testing); 7) emergency patch back out on 11/1/2012; 8) per plan, develop mitigation plan by 12/1/2012 (30 days); 9) per original plan, mitigation testing completed by 2/1/2013; and 10) per original plan, mitigation patch deployed on 3/12/2013 Recommend changing R3 Part 3.3 so that Medium Impact remote locations with no external connectivity (isolated networks) have more than 35 days Suggest changing R4 Rational from “(1) immediate detection” to “(1) real time detection” to be consistent with Part 4.2 Request clarification on R4 Part 4.1.1. The CIP Standards expect “deny by default” firewall rule which results in dropping offending packets such that there is nothing to log. How can the Registered Entity meet Part 4.1.1 criteria of logging failed access attempts at the EAP? The wording in the Measures column does not reflect what the Requirement is stipulating. Recommend removing “malicious” from R4 Part 4.1.4 since “malicious” is determined after the fact and Parts 4.1.1, 4.1.2 and 4.1.3 capture the events that may be malicious For R1 as written, recommend that missing one port is too high since the PSP is the first layer of defense. Missing one physical port should not be a Severe VSL. Recommend this is a Low VSL. Recommend increasing percentages from Low – Moderate – High – Severe. Recommend that the number of assets should be another differentiator for R3’s Low – Moderate – High – Severe. Recommend that the difference between R4’s Low – Medium – High – Severe should be the number of assets with two weeks throughout Recommend that R4 should start with a Low VSL and use the number of assets combined with the number of accounts as a difference between Low - Medium - High - Severe.
Request clarification of R5 Part 5.7. Does the technical feasibility apply to both “the number of

unsuccessful authentication attempts" and "generate alerts after a threshold of unsuccessful log in attempts" or only the "authentication attempts?"
Group
SMUD & BANC
Joe Tarantino
No
No
Part 6.5 requires that the entity verify each calendar quarter that individuals provisioned for authorized electronic access or authorized electronic access or authorized unescorted physical access have associated authorization records. The measures include "Documentation of the dated verification between a list of individuals who have been authorized for access …. And a list of individuals provisioned for access…". The reason a review should be necessary is the possibility that there is an error that needs to be corrected. The evidence in the Measures requires perfection on the part of the entity because it requires a dated verification between a list of individuals who have been authorized for access and a list of individuals provisioned for access. The event that a mismatch is discovered should give the entity the opportunity to fix the problem rather than be a violation. As worded, any mismatch discovered would result in a violation. Therefore, the standard requires perfection – anything less is a violation. It is suggested that the Measures be changed to simply prove that the review was completed while leaving the results of the verification out of the Measure. Parts 6.6 and 6.7 - Similar to our comment on Part 6.5, the Measures should only require verification that the entity performed the verification while leaving the results of the verification out of the Measure. This is especially true in the item number 4 in the measures: "Dated evidence showing verification of the privileges for the group are authorized…". Suggest wording in the measures that states, "Evidence … that proves the entity performed the annual verification." This reflects our previous comments on this issue. It appears that the standard is requiring perfection. If so, what is the point of the quarterly review? As worded, it looks like the purpose of the quarterly review is to find violations rather than give the entity an opportunity to fix the problem. Part 7.1 provides for limited revocation (remote access and physical access) for all terminations in 24 hours while Part 7.2 requires that all electronic access not needed is revoked by the end of the next calendar day for reassignments and transfers. Part 7.2 is inconsistent with the Rationale in 7.4, which states "Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability." If this statement is true for Part 7.4, then it is also true for Part 7.2 because in both cases, individual account access is revoked in both cases. The transfer or reassignment presents a special problem. If physical access needs for the new position and the old position are the same, but cyber access needs between the two positions are different, then one cannot use the mechanism of fast revocation of physical access and remote access to prevent the employee from accessing accounts he/she previously had access to in the old position, but has no need to access in the new position. While this logically leads to the conclusion that all cyber access needs to be removed very quickly, this conclusion conflicts with the Rationale that entities need time to comply. The same reasons that would have made it difficult for entities to remove all cyber access for terminations in a very short timeframe are the same reasons that would make it difficult to remove cyber access in the same timeframe for reassignments and transfers. It is suggested that entities be given a minimum of 7 days to revoke unneeded access for assignments and transfers.
No
No
No
No
Req. R1 1. SMUD appreciates the changes made by the drafting team with respect to the physical ports. The language in Draft 2 is much preferred over the language in Draft 1. However, the physical protection of all assets including physical ports is already covered in the physical security perimeter defined in CIP-006-5. SMUD's opinion is that the protection of physical ports defined in this section is

duplicative, and presents unnecessary burden to the entities. 2. The Rationale for R1 for this draft no longer includes a reference to physical ports. But requirement R1.2 concerns physical ports. The Rationale doesn't match requirement R1.2. Req. R2 1. Requirement R2.3 goes beyond the control of an entity that is reliant on a vendor to identify and provide patches for vulnerabilities. The entity's only typical options are to either install the patch or not install the patch. a. The vendor's development cycle may be the only path by which the vulnerability can be addressed. b. The entity cannot typically specify a specific timeframe in which the vulnerabilities will be addressed in the written plan that is required by R2.3 without basing its timing on the completion of the vendor's development cycle. 2. It is unnecessarily burdensome to require the entity to write a new remediation plan (or revise an existing one) for every patch because the entity generally simply installs the patch. It is suggested that a remediation plan only be required when the entity determines that it should not install the patch. This meets the intent of the Change Rationale shown in Table R2 of CIP-007-5. a. In the event the entity chooses to install the patch, documented tracking of the handling of the patch could be executed through an entity's documented procedures. In this case, there is no need for a remediation plan. The procedures the entity uses to define the workflow should be part of the Patch Management program that is already required. b. In the event the entity determines that it is too risky to install the patch, a written plan could be required to direct the entity to document what it plans to do to mitigate the vulnerability. 3. Regarding the dated plan referenced in Parts 2.3 and 2.4, it is possible that the entity's only option would be to notify the vendor and wait for a subsequent patch. In this situation, the entity will be able take steps toward final resolution, but would not be in the position to mitigate the vulnerability within any specified timeframe. The entity would be unable to specify when the vulnerability will be mitigated in the plan. Even though the entity could revise the plan to change the date the vulnerability would be mitigated, it is unnecessarily burdensome to require the entity to do so. 4. Measures on 2.4. It is appreciated that the team added the bullet items "Records of the installation of the patch"; and "Records of implementation of vendor recommended mitigations". It is still not clear that certification of installation of a patch onto a BES cyber system (for example: through a workflow) would be considered sufficient evidence. An auditor may interpret "Records of installation of the patch" to mean that records need to be kept for every machine. It is suggested that the wording be included to state that acceptable evidence would include certification by the installer that the patch was installed on the BES cyber system or BES cyber asset. Req. R4 SMUD appreciates the changes made to this section in the previous draft. In part 4.4, Measure 2 requests information about log data that is not part of the requirement. Thus, item 2 doesn't match the requirement and adds unnecessary burden for the entity. Measure 1 proves the existence of log information for 90 days. Measure 3 proves that the system is configured for 90 log retention. Taken together Measure 1 and Measure 3 prove that the system meets the requirement.
The "Summary of Changes" section includes a statement that says that requiring "the identification and management of shared account access have been removed." Requirement 5.3 states "Identify individuals who have authorized access to shared accounts". The Measure to Requirement 5.3 states includes the phrase "…listing of shared accounts and the individuals who have access to each shared account." While the Measure includes the phrase, "Evidence may include, but is not limited to,…", the example still requires identification and management of shared accounts. Requirement 5.4. The Phrase "on Cyber Assets" may add confusion. It appears that the intent of the requirement would be met (without change) if this phrase were removed. Requirement 5.5.2. "Minimum password complexity that is the lesser of three or more different types of characters (eg. uppercase alphabetic, lower case alphabetic, numeric, non-alphanumeric) or …" It is appreciated that the intent is to give maximum flexibility to the entity by leaving it to the entity to define character types. Unfortunately, there is no definition for the word "types". Instead, the language presents the types as an example: "(eg. uppercase alphabetic, lower case alphabetic, numeric, non-alphanumeric)". The ability to enforce or comply with Part 5.5 depends upon a definition of what really constitutes a character "type", or, alternatively, a different way of defining password complexity.
Group
Southern California Edison company
Nathan Smith
No
No
No

No
No
No
No
SCE Comments to CIP-004-5 -R3.1: We suggest revising the requirement to say “documentation of the training specified, for their role, in CIP-004-5,..” -R3.2: We suggest revising the requirement to say “documentation of the training specified, for their role, in CIP-004-5,..”
SCE comments to CIP-004-5 -R6.1.3: Please clarify that if a person has BES Cyber System Information on their work computer or in their work station, authorized access to the computer and workstation is not required pursuant to R6.1. -R6.1.3: Please clarify if access beyond the workstation is applicable to R6.1? -R6.4: Please revise as follows: “…is stored by the Responsible Entity that the Responsible Entity determines are necessary for performing assigned work functions, except for CIP Exceptional Circumstances, pursuant to the Responsible Entity’s BES Cyber System information protection program.” -R7.1 and R7.5: These requirements appear inconsistent with each other. Please clarify R7.5 is only applicable to shared user accounts. -R7.4: Please revise as follows: “…within 30 calendar days of the effective date of the termination action. The registered entity will ensure that in the case of employee terminations, all information copied from its repositories by a terminated person is recovered or rendered useless within 30 days of that person’s termination, pursuant to the Responsible Entity’s BES Cyber System information protection program.” -R7.5: Please revise as follows: “For termination actions, reassignments, or transfers, change passwords for shared account(s) known to the user within 30 calendar days of the completion of the termination action, reassignment, or transfer of the user.”
No
Yes
SCE Comments to CIP-005-5 -R1.1: The phrase “associated protected cyber assets” should be relocated to the applicability section. - R1.3: Tracking the rationale for granting access permissions for sixty-thousand ports is burdensome. We suggest tracking the rationale for granting access permissions based upon a class of assets or the type of access required; or replacing the word “rationale” with the word “criteria”. Also please define the term “access permissions”. -R1.5: Many of the assets that fall into Medium Impact cannot accommodate an automated method for detecting malicious software. We suggest removing Medium Impact assets from the applicability.
Yes
Yes
Yes
SCE Comments to CIP-006-5 -R1.4: Please revise the requirement to the following: “…for unauthorized circumvention of a physical access control into a Physical Security Perimeter. The 99% availability includes times when back-up monitoring systems are deployed.” -R1.5: Please revise to the following: “…alert in response to detected unauthorized physical access of a Physical Security Perimeter…” Violation Severity Level for R1.9: Please remove the “did not retain physical access logs for 45 days” scope from the Severe category and move it to the Low or Medium category, as not retaining a log itself will not degrade the functionality of the BES.
No
No
No
No
No
SCE Comments to CIP-007-5 -R1.1: Please revise as follows: “…and where technically feasible, enable only required logical network accessible ports…” -R1.2: Please remove the word “unnecessary” from the requirements globally and replace it with “not required”. -R3.1: Please revise the Measures section as follows: “…Entity’s performance of these processes (e.g., through traditional antivirus, system hardening, non-software policies, etc.).”
SCE Comments to CIP-007-5 -R5.3: It is unclear what protection is gained by maintaining a list of persons that have access to shared accounts on Cyber Assets with no external routable protocol.

Please limit the applicability to High Impact Cyber Systems and Medium Impact BES Cyber Systems with external routable connectivity. -R5.7 Please clarify that printers and multifunction machines are out of scope. Please also revise the applicability section to remove “Associated Protected Cyber Assets” from the applicability section as this term could be applied to assets that do not have BES Cyber System Information, and have little impact upon the BES.
Individual
Scott Miller
MEAG Power
Yes
Yes
Yes
Yes
Yes
Yes
No
In R2 Part 2.10, “training content on risks associated” – it’s not clear what is required. Awareness and other training (i.e. part 2.4) would cover this area in general; we don’t believe that this specific training module is required.
CIP 004-5 R7 (Table R7 - Part 7.1) requires that the revocation process be completed within 24 hours for termination actions involving employees with access to certain Medium Impact BES Cyber Systems. While MEAG Power agrees that this 24 hour termination period should be the standard for employees that have been terminated and previously having access to High Impact BES Cyber Systems, the standard should allow a more reasonable response time (suggested 48 hours) for employees having access to Medium Impact BES Cyber Systems and associated protected information.
Yes
Yes
No
Yes
Yes
R1 (Parts 1.4 and 1.6) mentions that Physical Access Control Systems should have a “99.9% availability” – which so– but perhaps this 99.9% needs clarifying under CIP 006 R1 at this time. In R1, the references to 99.9% availability are not clear. There is no guidance as to how this can be measured. Also, how is one to know unauthorized circumvention? This could be interpreted to equate to a violation if there is a substation circuit downtime at any given site that is >9 hours in any one year. It is common for telco circuits to go down 1-3 times a year - probably averaging somewhere around 24-48 hours per circuit downtime event – therefore, if circuit downtime contributes against the 99.9%, there will be multiple violations at multiple sites per year. It could be argued that the centralized physical access computer system should have a 99.9% availability – which will require utilities to have primary and backup server systems in place to meet the 99.9% availability of the overall service. R1 needs to be clarified. R 1.4: We suggest specifying that planned maintenance be excluded and apply the 99.9% requirement only to unplanned outages. R1.6: We suggest specifying that planned maintenance be excluded and apply the 99.9% requirement only to unplanned outages. The proposed language for CIP 006-5 R1 (Table R1 - Part 1.3) stipulates for High Impact BES Cyber Systems the requirement that “Where technically feasible, utilize two or more different physical access controls to collectively allow physical access into Physical Security Perimeters….”. Currently, many in the industry question if two different control systems are required. It would be recommended to clarify in the requirement that two authentication methods using the same control system are compliant (for example, badge/thumbprint).
Yes
Yes

Yes
Yes
Yes
Individual
Heather Laws
Portland General Electric
Yes
Yes
Yes
Yes
Yes
Yes
Yes
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
Yes
Yes
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
No
No
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
Yes
Yes

Yes
Yes
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
Group
Progress Energy
Jim Eckelkamp
No
No
No
No
No
No
No
Progress Energy agrees with EEI comments with the modified and additional comments below: R1= Original R1.1: A security awareness program that, at least once each calendar quarter, conveys ongoing reinforcement of cyber security practices for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems. Proposed R1.1: A security awareness program that, at least once each calendar quarter, conveys ongoing reinforcement of cyber security practices for the Responsible Entity's personnel who have unescorted authorized electronic or authorized unescorted physical access to BES Cyber Systems. Rationale: Unescorted Cyber Access category should be introduced to allow for more effective interaction with vendor support services. Much of the CIP-004 personnel risk assessment requires extensive dependencies on supporting evidence which is not available under standard support contracts which require 24*7 staffing. There currently exists tools to monitor interaction of remote vendor support and limiting requirements to those having unescorted access within the CIP requirements will allow more effective focus of resources R2= This only applies to personnel who have escort duties; and only applies to people who have unescorted access; not access to media. Need to add whether they need training for each of the three bullets. Insert "unescorted" into "authorized unescorted electronic" references. This allows entities to focus on unauthorized access rather while allowing for vendor support services. R2.2 – Requirements, Rewording Original: Training content on the cyber security policies protecting the Responsible Entity's BES Cyber Systems. Proposed: Training content on the cyber security policies protecting applicable cyber assets. Rationale: This allows for training to be targeted addressing applicable cyber assets (to include BES Cyber Assets where applicable). R2.3 – Requirements, Rewording Original: Training content on the physical access controls protecting the Responsible Entity's BES Cyber Systems. Proposed: Training content on the physical access controls protecting applicable cyber assets. Rationale: This allows for training to be targeted addressing applicable cyber assets (to include BES Cyber Assets where applicable). R3= R3.1 – change reference from "physical access to BES Cyber Systems" to "physical access to applicable cyber assets" to ensure training adequately covers relevant and applicable cyber assets. R4= R4.1 – Requirements, Rewording Original: An initial personnel risk assessment ("PRA") that includes identify verification. Proposed: Program content on an initial personnel risk assessment that includes identity verification. Rationale: This requirement should address the contents of a supporting program rather than individual artifacts of evidence. R4.2 – Requirements, Rewording Original: Seven year criminal history

records check including current residence, regardless of duration, and covering at least all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six months or more: Proposed: Seven year criminal history records check including current residence, regardless of duration, and covering all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six consecutive months or more: Rationale: Two changes have been made. “At least” was dropped in front of “all” as it was redundant with “at least all.” Also, “consecutive” was added in the middle of “six months” to provide greater clarity in terms of what the criteria is. R5= R5.1 – Requirements, Rewording Original: Have a personnel risk assessment performed as specified in CIP-004-5, Requirement R4 prior to being granted authorized electronic or authorized unescorted physical access, except for CIP Exceptional Circumstances. Proposed: Have a personnel risk assessment as specified in CIP-004-5, Requirement R4 prior to gaining authorized electronic or authorized unescorted physical access, except for CIP Exceptional Circumstances. Subsequent authorizations, within the life-time of PRA events, do not require repeating the background check. Rationale: while not perfect, it was determined that “gaining” would be better terminology than “granting.” The additional language regarding not repeating this requirement provides clarity that this process is to be conducted once for any/all authorized access and is not subject to additional PRAs as additional access requirements are identified. R5.1 – Measures, Rewording (First bullet) Original: Dated records showing that personnel risk assessments were completed before authorized electronic or authorized unescorted physical access was authorized; or Proposed: Records showing that personnel risk assessments were performed before authorized unescorted electronic or authorized unescorted physical access was gained. Rationale: There is repetition of “authorized” within this measure which is confusing. By replacing the last word with provisioned, the event is better captured to ensure compliance with the PRA requirement. R5.2 – Measures, Rewording Original: Evidence may include, but is not limited to, current and previous personnel risk assessment records. Proposed: Evidence may include, but is not limited to, current personnel risk assessment records. Rationale: Given the 7 year cycle, ensuring that the current records are in place should satisfy this requirement. Addition of previous PRA records only adds to the archival length to a period of (up to) 14 years without any benefit to security.

R6= R6.1 Applicability should remove references to dial-up connectivity Comment: Measure should add ‘unescorted’ in front of electronic access. Rationale: this provides more effective applicable cyber assets to enact these requirements. Adding unescorted access allows for vendor support requirements without elevating this into ‘authorized electronic access’ category. R6.2 Requirement Rewording Original: The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances. Proposed: The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is appropriate. Rational: assessing the appropriateness of access permissions is more effective then assessing ‘necessary.’ R6.3 Requirement Rewording Applicability should remove references to dial-up connectivity Original: The individual(s) designated in Part 6.1 shall authorize unescorted physical access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances. Proposed: The individual(s) designated in Part 6.1 shall authorize unescorted physical access into Physical Security Perimeter(s) that the Responsible Entity determines is appropriate, except for CIP Exceptional Circumstances. Rationale: Providing a scope of PSP access frames this requirement within the context of the CIP scope, focusing on defined PSP access. R6.6 Requirement Rewording Original: For electronic access, verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all user accounts, user account groups, or user role categories, and their specific associated privileges are correct and are those that the Responsible Entity determines necessary for performing assigned work functions. Proposed: For electronic access, verify at least once each calendar year, or not to exceed 15 calendar months between verifications, that BES Cyber System access privileges are appropriate for the individual(s) or role(s) responsibilities. Rationale: The current language provides too prescriptive a list of evidence in support of this requirement. By eliminating “all,” identifying BES Cyber System access privileges will frame the context of this requirement effectively. Focusing on ensuring the privileges are appropriate vs. “correct,” allows for assessing the privileges. R6.6 Measures – This should be a bulleted list to support an “or” assessment of the evidence. R6.7 Measures – The numbered list should be a bulleted list to support an “or” assessment of the evidence. a. Last bullet – Rewrite i. Original – Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions. ii. Proposed – Evidence showing a

verification of the authorization and any permissions were confirmed. iii. Rationale – The edits provide a greater focus on the root concerns to address the Requirement. R7= R7.1 – Requirement Rewrite Original: For all termination actions, initiate the process to revoke the individual's unescorted physical access and interactive Remote Access upon the effective date and time of the termination action, and complete the revocation within 24 hours after the effective date and time of the termination action. Proposed: For all termination actions, initiate the process to revoke the individual's unescorted physical access and interactive Remote Access upon the effective date and time of the communication of the termination action, and complete the revocation within 24 hours after the effective date and time of the communication of the termination action. Rationale: By identifying the time the termination action is communicated, concerns regarding notification of terminations which are pre-dated or retro-active can be alleviated by using the communication time as the trigger event. R7.1 – Measure should show a bulleted list to reflect the "or" approach to supporting evidence. R7.2 – Requirements Rewrite Original: For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the reassignment or transfer. Proposed: For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the determination that access is no longer necessary. Rationale: The rewording provides greater support and recognition that this process can take place until all legacy access is no longer needed, within a transition period that can take place indefinitely. By assigning the response time to the determination event, deadlines are aligned more effectively. R7.2 – Measure should show a bulleted list to reflect the "or" approach to supporting evidence.
No
No
Progress Energy agrees with EEI comments with the modified and additional comments below: R1= R1.1: Applicability Comment: Add Associated Protected Cyber Assets with External Routable Connectivity Rationale: This addition aligns with the requirement, in which associated Protected Cyber Assets are also required to reside within a defined ESP. R1.2 Applicability Comment: Add Associated Protected Cyber Assets with External Routable Connectivity Rationale: This addition aligns with the requirement, in which associated Protected Cyber Assets are also required to reside within a defined ESP. R1.4 Comment: This requirement is very similar to CIP-007-5 R5.1, with the exception of dial-up applicability. Propose: adding BES Cyber Assets with dial-up connectivity used within High and Medium Impact facilities into CIP-007 R5.1, and removing R1.4 from CIP-005-5. Rationale: This identifies all BES Cyber Assets that require authentication into a single requirement, resulting in a more concise standard. R1.5 Measures – there should be bullets (rather than numbers) identifying 'or' instances.
Progress Energy agrees with EEI comments with the modified and additional comments below: 1. R2.1, 2.2, 2.3 Requirements – Proposed Change Original: Utilize encryption for all Interactive Remote Access sessions that terminate at an Intermediate Device in order to protect the confidentiality and integrity of each Interactive Remote Access session. Proposed: Utilize encryption for all routable Interactive Remote Access sessions that terminate at an Intermediate Device. Rationale: The addition of 'routable' in front of Interactive Remote Access sessions provides a clear filter that aligns with the Interactive Remote Access concept.
No
No
No
Progress Energy agrees with EEI comments with the modified and additional comments below: R1= CIP-006-5 R1.4 currently states: Have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized circumvention of a physical access control into a Physical Security Perimeter 1. Strike out "(with 99.9% availability)" and instead add language such as, "Establish a documented process to implement compensating measures for loss of specific functions of the Physical Access Control System". For example the loss of monitoring functionality of the PACS may be compensated by roving patrols physically monitoring PSPs or if electronic logging capability is lost manual logging can be implemented. 2. Revise language to align with legacy language in previous version that specifies monitoring at all physical access points to the PSP. Revised language R1.4 would read: Define and implement controls that monitor physical

access points of the Physical Security Perimeter for unauthorized physical access into a Physical Security Perimeter. Establish a documented process to implement compensating measures in the event the physical access control system is non functional Rationale for change to R1.4: 1. Attempting to impose a requirement to have the physical access control system available 99.9% is not realistic or possible given some of the environments where they are being implemented (e.g., substations, a variety of types of bldgs at generation sites). It does not take into consideration possible network outages of the WAN (which entities have no control over), does not take into consideration remote locations with infrequent use (it is possible for a alarm contact to go bad with no indication of such unless one was continuously testing alarms) or the difficulty in tracking the various types of outages (no defined formula for determining the 99.9% availability). Furthermore, it does not allow entities to implement compensating measures as a means to remain compliant in the event the system is not available. The availability should be addressed by a robust maintenance program that allows for broken equipment to be found, recorded and mitigated in a timely manner without recording violations. 2. The requirement as it is written seems to imply entities would need to employ some type of interior motion detection within the PSP that would alert if physical access controls were circumvented. This seems to increase scope of the original monitoring requirement when alarms and alerts were limited to physical access points. Implementing interior motion sensors within PSPs throughout the various generation/transmission sites would provide little or no return on investment, as existing physical security controls (e.g., perimeter fencing, card access) should be sufficient based on low probability that a cyber attack will be initiated at the device level. There are no known physical security threats against cyber assets that would warrant such prescribed language. In addition, various types of interior motion detection sensors (e.g., interior microwave sensors, passive infrared, and proximity sensors) are not full proof and all are prone to nuisance alarms. Nuisance alarms vary based on type, but can be triggered by objects being moved by air currents generated by heating, ventilation, and air conditioning (HVAC) systems or fans and fluorescent lighting, interference from various electromagnetic fields, small/large insects, change in temperature, vibrations, dust, etc. CIP-006-5 R1.5 currently states: Upon detection of an unauthorized circumvention of a physical access control into a Physical Security Perimeter notification to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection. 1. Revise language to align with legacy language in previous version that specifies monitoring at all physical access points to the PSP. Revised language for R1.5 would read: Issue an alarm or alert in response to detected unauthorized physical access at all access points to a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection. Rationale for change for R1.5: There may not be an alarm or alert of unauthorized access, but just a response. CIP-006-5 R1.6 currently states: Have controls that monitor each Physical Access Control System twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized physical access to a Physical Access Control System. 1. Strike out “(with 99.9% availability)” and instead add language such as, “Establish a documented process to implement compensating measures for loss of specific functions of the Physical Access Control System”. For example the loss of monitoring functionality of the PACS may be compensated by roving patrols physically monitoring PSPs or if electronic logging capability is lost manual logging can be implemented. 2. Revise language to align with legacy language in previous version that specifies monitoring at all physical access points. Revised language for R1.6 would read: Have controls that monitor physical access points to the Physical Access Control System for unauthorized physical access. Rationale for change for R1.6: Refer to Rational for Change for R1.4 CIP-006-5 R1.7 currently states: Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the unauthorized physical access. 1. Revise language to align with legacy language in previous version that specifies monitoring at all physical access points. Rationale for change for R1.7: There may not be an alarm or alert of unauthorized access, but just a response. Revised language for R1.7 would read: Upon detection of an unauthorized circumvention of a physical access control into a Physical Security Perimeter notification to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection. R2= R2.1 – Requirements Original: Require continuous escorted access of visitors (individuals who are known or guests, and not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances. Proposed: Require continuous escorted access of individuals not authorized for unescorted physical access. Rationale: The additional words did not provide any greater clarity. R3= Applicability: Remove “Locally mounted hardware or devices at the physical security perimeter associated with:” Rationale:

documenting outages for locally mounted hardware is currently too vague and resource intensive with minimal security benefit. By ensuring that Physical Access Control Systems adequately document their outages, the root concern should be addressed. a. Requirement – Change Original: Document outages for physical access control, logging, and alerting systems and retain the outage records for at least 12 months. Propose: Document outages for physical access control systems and retain the outage records for at least 12 calendar months. Rationale: By focusing on the Physical Access Control Systems, satisfactory outage records should be achieved. Additional Comments: Comments: VSL – R1/High: The second paragraph on page 23 should read "The Responsible Entity does not have controls…" VSL – R1/Medium: Remove "or external dial-up connectivity. (1.2)" from the end of the second paragraph. VSL – R2 Moderate: Remove "on a daily basis," from the 1st paragraph on page 25. Application Guidelines a. Page 28 – Remove "Methods to monitor physical access include:" section as it relates to R1.4, which has been proposed for removal. b. Page 29, second paragraph – Remove. The applicability of the 96 square inch opening provides no benefit to applicability. Focusing on unauthorized circumvention of physical access control could be interpreted as monitoring for perimeter breaches outside of the current physical access points. This could lead to exhaustive monitoring tools which may still allow for unmonitored locations that result in a violation of this requirement.
No
No
No
No
No
Progress Energy agrees with EEI comments with the modified and additional comments below: R1= R1.1 Comment: Applicable BES Cyber Systems and associated Cyber Assets: Clarify how "Associated Protected Cyber Assets" is a modifier to the "High Impact BEST Cyber Systems" and "Medium Impact BES Cyber Systems with External Routable Connectivity" rather than an independent set of assets. One option is to add "and Associated Protected Cyber Assets" to each of the High and Medium categories in this requirement. a. Requirements i. Does the "where technically feasible" language imply that TFEs are required when it is not technically feasible? ii. There was discussion about how "needed" should be defined, and whether it's up to the asset owner to determine the need for a port to be accessible, or whether the auditor has the ability to decide. This issue was tabled, and there may suggested language provided. R1.2 Requirements: Discussions around whether the physical security measures already accommodate this requirement, but it was brought up that FERC specifically requires this. Measures: Suggest a clarification that these measures be implemented at the device level if that is the intent. R2= R2.1 Requirements: Original: A patch management program for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets." Proposed: A patch management program for tracking, evaluating, and installing cyber security patches and/or security updates for applicable Cyber Assets." R2.2 Requirements: Change 30 to 35 calendar days to assist with monthly patch cycles and increase efficiency R3= Concern: The inclusion of this category in the requirements for Malicious Code Prevention and Security Event Monitoring implies that these requirements apply to every device in the category. This departs from the goal of applying these controls at the system level. Suggestion: Clarify that these requirements do not apply to all assets individually, by removing the category, or modifying the requirement. R4= R4.1 Comment: Add the term "where technically feasible" to the requirement language Rationale: Not all systems can support the logging requirements in 4.1.1-4.1.4. R4.2.1 Comment: Change "detected malicious activity" to "detected cyber security event" Rationale: not all security events are malicious R4.3 Requirement Comment: Change "Activate a response to detected event…" to "Activate a response to human-detected event…" Rationale: the requirements do not distinguish between the detection of an event by a system and a person. A person may not see the event at the same time it is generated by a system, so the requirement should be clarified to reflect that the deadline for a response be tied to human detection. Requirement: Comment: Change "next calendar day" to "next business day" to accommodate off-hour staff coverage. Measures: Change "attestation" to "documentation" for clarity. 1. R4.5 Applicability Comment: Consolidate "High Impact BES Cyber Systems" and "Associated Protected Cyber Assets", by changing the wording to "High Impact BES Cyber Systems with Associated Protected Cyber Assets" Rationale: Clarifies that the logging reviews do not apply at the asset level. Requirement Comment: Change the wording to "Review a summarization or sampling of logged events, as deemed appropriate by the Responsible Entity, at a minimum…" Rationale: It

should be clear that the entity determines which logs should be reviewed or sampled, to avoid confusion during audits. Requirement Comment: R4.5 – standard is asking for review every two weeks Propose: monthly review
Progress Energy agrees with EEI comments with modified and additional comments below R5.1 Applicability Comment: Change “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routability or dial -up” Rationale: Consistency with CIP-004 R6.2 R5.2: Delete requirement. Rationale: Covered by CIP-004 R6.2 R5.3 Delete requirement Rationale: Covered by CIP-004 R6 and move rationale to CIP-004 R6. R5.4 Applicability Comment: Change “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routability or dial -up” Rationale: Consistency with CIP-004 R6.2 R5.1 Requirement Comment: Change the wording from “Change default passwords…” to “Change known default passwords…” Rationale: Manufacturers sometimes use system passwords that are not known to the entities. R5.1 Measures Comment: Remove the language from the first bullet “…when new devices are deployed” Rationale: Time frames are covered elsewhere in the Standards R5.5 Measures Comment: Change the second bullet to “Documentation of procedural controls” Rationale: Procedural controls for changing passwords are covered elsewhere R5.6 Requirement Comment: Add the language “within the capabilities of the device or operational requirements” to the beginning of the requirement. Rationale: Some vendors do not ensure correct operation of the system if certain passwords are changed. R5.6 Measures Comment: Change the second bullet to “Documentation of procedural controls” Rationale: Procedural controls for changing passwords are covered elsewhere
Individual
John Allen
City Utilities of Springfield, MO
No
No
No
No
No
No
No
City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. We agree with the comments from SPP and APPA and believe the requirements are getting close to being acceptable for those cyber systems that could cause a significant impact to the BES. However, we cannot support this Standard due to the onerous requirements for a small entity’s Control Center that are considered a threat to reliability due to their connectivity to High Impact Control Centers. We could support a standard that has programmatic requirements for these small Control Centers. See our response to Comment Form A, question 3.
City Utilities of Springfield, Missouri agree with the comments from SPP and APPA and believe the requirements are getting close to being acceptable for those cyber systems that could cause a significant impact to the BES. However, we cannot support this Standard due to the onerous requirements for a small entity’s Control Center that are considered a threat to reliability due to their connectivity to High Impact Control Centers. We could support a standard that has programmatic requirements for these small Control Centers. See our response to Comment Form A, question 3.
No
No
City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. We agree with the comments from SPP and APPA and believe the requirement is getting close to being acceptable for those cyber systems that could cause a significant impact to the BES. However, we cannot support this Standard due to the onerous requirements for a small entity’s Control Center that are considered a threat to reliability due to their connectivity to High Impact Control Centers. We could support a standard that has programmatic requirements for these small Control Centers. See our response to Comment Form A, question 3.

City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. We agree with the comments from SPP and APPA and believe the requirement is getting close to being acceptable for those cyber systems that could cause a significant impact to the BES. However, we cannot support this Standard due to the onerous requirements for a small entity's Control Center that are considered a threat to reliability due to their connectivity to High Impact Control Centers. We could support a standard that has programmatic requirements for these small Control Centers. See our response to Comment Form A, question 3.
No
No
No
City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. We agree with the comments from SPP and APPA and believe the requirements are getting close to being acceptable for those cyber systems that could cause a significant impact to the BES. However, we cannot support this Standard due to the onerous requirements for a small entity's Control Center that are considered a threat to reliability due to their connectivity to High Impact Control Centers. We could support a standard that has programmatic requirements for these small Control Centers. See our response to Comment Form A, question 3.
No
No
No
No
No
City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. We agree with the comments from SPP and APPA and believe the requirements are getting close to being acceptable for those cyber systems that could cause a significant impact to the BES. However, we cannot support this Standard due to the onerous requirements for a small entity's Control Center that are considered a threat to reliability due to their connectivity to High Impact Control Centers. We could support a standard that has programmatic requirements for these small Control Centers. See our response to Comment Form A, question 3.
City Utilities of Springfield, Missouri agree with the comments from SPP and APPA and believe the requirement is getting close to being acceptable for those cyber systems that could cause a significant impact to the BES. However, we cannot support this Standard due to the onerous requirements for a small entity's Control Center that are considered a threat to reliability due to their connectivity to High Impact Control Centers. We could support a standard that has programmatic requirements for these small Control Centers. See our response to Comment Form A, question 3.
Individual
Nick Lauriat
Network & Security Technologies, Inc.
Yes
Yes
Yes
No
Yes
No
No
In Requirement R4, N&ST observes the drafting team has attempted to address numerous concerns about the difficult in systematically checking criminal history in locations not associated with actual residence (as recorded by the Social Security Administration). The fact of the matter is that requiring entities to do a criminal history check anywhere other than the addresses on file with the Social Security Administration is a faulty approach. Candidates can easily conceal criminal history by

forgetting or ignoring a county / state where arrest may have occurred (which could be quite different from the work location or location of the educational institution). N&ST recommends the drafting team not require additional documentation from the entity, but simply require the type of information (e.g., residence) likely to be available programmatically during a commercial personnel risk assessment.
In Requirement R6, N&ST observes that as written, it appears to be required that individuals be authorized for all three types of access listed in 6.1.1 through 6.1.3. Suggest rewording to say, “Designate one or more individual(s) to authorize one or more of the following types of access:” In Requirement R7.2, N&ST observes that the drafting team appears to have inadvertently made this requirement more stringent, in terms of time allowed to complete, than Requirements R7.1 and R7.3.
Yes
Yes
No
Yes
Yes
N&ST observes that CIP-006-5 articulates a number of requirements for PSPs without ever including a requirement about what needs to be inside the PSP! N&ST suggests that Requirement R1.1 be reworded to “Define operational or procedural controls to restrict physical access to only those individuals who are authorized.”
Yes
No
No
No
Yes
In Requirement R2, N&ST observes that entities are not required to commit to any specific date to either install an applicable patch or implement other vulnerability mitigation measures. If the drafting team hopes to “get ahead” of CANs in this area, CIP-007-5 cannot remain silent on this point. In Requirement R3, N&ST observes that the wording of associated Measure suggests an entity could claim compliance with nothing more than a policy advising users to exercise caution. In Requirement R4.1, N&ST believes that this is likely to be not technically feasible for all applicable systems, and believes it should be TFE eligible (like Requirement R4.2).
Individual
Brian Evans-Mongeon
Utility Services Inc
Yes
Yes
Yes
No
Yes
Yes
Yes
The comments submitted for the Applicability Section 4.0 of CIP-002-5 would be applicable to this Standard. (1) R4.2 Recommend that 4.2.1 – 4.2.3 be replaced by bullets and that the “and” in 4.2.2 be replaced by an “or”. The current language would require that all three elements be met at the same location and time period, before a criminal history check would need to be done.
(1) The Violation Risk Factor stated in CIP-004-5 R7 should agree with the VRF listed in the Table of Compliance Elements.
Yes
Yes
The comments submitted for the Applicability Section 4.0 of CIP-002-5 would be applicable to this

Standard.
Yes
Yes
Yes
The comments submitted for the Applicability Section 4.0 of CIP-002-5 would be applicable to this Standard. Utility Services supports the comments made by MMWEC in their Comments 1, 2 and 3 for CIP-006-5.
Yes
No
Yes
No
Yes
The comments submitted for the Applicability Section 4.0 of CIP-002-5 would be applicable to this Standard. Utility Services supports the comments made by MMWEC in their Comments 1, 2 and 3 for CIP-007-5 R1, R2, R3, R4.
Utility Services supports the comments made by MMWEC CIP-007-5 R5.
Group
NCEMC
Scott Brame
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Yes
Yes
(1) R1.4 – The requirement for 99.9% availability for physical security perimeter controls is problematic due to requiring tracking of availability without defining a time period for determining the percentage. The SDT needs to revisit this requirement to reduce the complexity of tracking such availability and to create a clear requirement on this issue.
Yes
Yes
Yes
Yes
Yes
Group
Dairyland Power Cooperative

Tommy Drea
Yes
No
No
Yes
Yes
Yes
No
Please see MRO NSRF Comments.
Please see MRO NSRF Comments.
No
Yes
The CIP-005 standard does not adequately define or address security controls required for non-routable devices. There needs to be some identifiable security requirements for serial devices that communicate external to the ESP. This needs to address the full variety of connectivity situations. For instance, communications with a remote serial end point is likely to occur over an enterprise or commercial communications infrastructure. The communications network infrastructure may contain devices utilizing either IP transport or IP management access. It would be incorrect to define this communications path as “direct serial”. Is such a path considered routable? Does it require security controls? Does it matter if the remote system is protected by security controls? Consider the following items in comparison to the draft 2 “Application Guidelines” section of CIP-004-4 draft 2. This section of draft 2 states that serial connections are not considered routable—and also that devices that communication externally with serial connections are not considered Electronic Access Points. • The “Identifying Critical Cyber Assets” Security Guideline section D defines serial devices that are connected to a network device (i.e. Terminal server, or RTU concentrator) as being “routable” by virtue that they can be accessed over a routable network. • NERC Notice of Penalty (NOP) NP12-4-000 outlines a violation of CIP-005-1 R2 that appears to be related to using external terminal server solutions to critical serial devices. It seems the utility expected the direct serial cable to be the ESP boundary. Without further details, it is unclear if there is a contradiction between guidelines. If the intention of the draft 2 guideline section is to make a blanket statement on serial being excluded from any definition of routable, then these items above are in contradiction. If this point in the draft 2 guideline is only to address serial devices that cannot be routed to, the standard is severely lacking in guidance as to how to address serial communications that do not meet the criteria of “direct serial”. The definition of a “Direct serial, non-routable” connection should be further defined. Distinctions should be made about other situations -- such as serial devices connected to terminal servers, or substation to substation communications that are serial, but pass across a broader routable communications infrastructure. Without further guidance, the draft 2 guidance makes it look acceptable for any kind of communications path to be connected to a serial device (such as pilot communications for an electronic protective relay on a bulk electric transmission line). From the draft 2 language, we could conclude that serial device probably would not need to be declared as critical unless it is network connected to the ESP—and even if it was there would be no electronic access requirements to apply. The NOP indicates that today, NERC considers serial devices at the ESP perimeter important enough to enforce a penalty. Draft 2 seems to dismiss the same issue from any regulation. It also seems contradictory that the same section that dismisses serial devices from requirements by virtue of not being routable also requires the inclusion of standalone networks (which are not externally routable) to meet the requirements of an ESP. Must BES Cyber systems that are non-routable reside in an ESP? CIP-007-5 R1.2 requires the disabling of physical input/output ports. Does the disabling of such ports potentially reclassify a device that would otherwise be considered a BES Cyber System? For instance, if a routable device had its physical network ports blocked—what otherwise might be a routable device cannot route. Example: A modern large-screen LCD television is intended to be used for a control center display of real-time operations information. If the TV has “Smart” functions (network application platform), it is more than a peripheral display—it is a programmable computing platform. Such a device used for real-time monitoring meets the criteria for a BES Cyber System. Will physically blocking the network ports reclassify the TV as a simple display peripheral, and allow it not to be subject to all CIP requirements of a BES Cyber System? If such a device is allowed to be neutered into something that would not otherwise be considered a BES Cyber

System, is it no longer subject to other CIP requirements? If so, how would this be distinguished from other device situations—such as a relay control device that directly operates BES transmission equipment, but has no routable connectivity. Is the definition of a BES Cyber System sufficient to provide clarity in more complex situations? Also please see MRO NSRF Comments.
Please see MRO NSRF comments.
No
Yes
Yes
Please see MRO NSRF comments.
No
No
No
No
No
Only some requirements state that they are applicable to “Medium Impact BES Cyber Systems with External Routable Activity”. Since this is the only part of the applicability language that mentions “routable”, it is not clear from the context what the requirement is applicable to. Is the intended meaning a High Impact BES Cyber System is subject to the requirement whether or not it is routable (includes serial devices)? Or is the intended meaning that routable High Impact BES Cyber Systems are all subject to the requirement whether or not it is externally connected (excludes serial devices)? The answer to the above question should clarify whether the CIP-007-5 requirements R1.2, R2.1, 2.2, R2.3, R2.4, R3.3, R4.1, R4.4, R4.5, R5.1, R5.2, R5.4, R5.5, R5.7 apply to non-routable serial devices. With the change to eliminate much of the routable/non-routable language, it is unclear which applicability interpretation to take. CIP-007-5 R1.2 requires the disabling of physical input/output ports. Does the disabling of such ports potentially reclassify a device that would otherwise be considered a BES Cyber System? For instance, if a routable device had its physical network ports blocked—what otherwise might be a routable device cannot route. Example: A modern large-screen LCD television is intended to be used for a control center display of real-time operations information. If the TV has “Smart” functions (network application platform), it is more than a peripheral display—it is a programmable computing platform. Such a device used for real-time monitoring meets the criteria for a BES Cyber System. Will physically blocking the network ports reclassify the TV as a simple display peripheral, and allow it not to be subject to all CIP requirements of a BES Cyber System? If such a device is allowed to be neutered into something that would not otherwise be considered a BES Cyber System, is it no longer subject to other CIP requirements? If so, how would this be distinguished from other device situations—such as a relay control device that directly operates BES transmission equipment, but has no routable connectivity. Is the definition of a BES Cyber System sufficient to provide clarity in more complex situations? Also see MRO NSRF comments.
CIP-007-5 R5.5 states the maximum time between changing any password as 15 months. The Guidelines and Technical Basis section for R5 offers an example password expiration length table that varies based on complexity. It is an interesting table with a good scheme. It also suggests a maximum time length of two years or more for a very complex password. While there seems to be justification for this time period based on the complexity—the table contradicts R5.5’s direct requirements. Is it intended that entities can construct a well reasoned set of password expiration times of any time interval—or is the maximum interval still required to be constrained by 15 months? Also see MRO NSRF comments.
Individual
Jennifer White
Alliant Energy
Yes
No
No
Yes
Yes
Yes

No
Alliant Energy voted “No” on the Standard, as a whole, due to the significance of the changes we propose herein. Many requirements, if changed in accordance with our sometimes minor verbiage proposals, would be a “Yes.” [R1] Though we recommend changing “ongoing reinforcement of cyber security practices” to “ongoing reinforcement of security practices” to prevent limiting awareness messages to cyber to the exclusion of physical security awareness, as well. [R2] The main requirement appears to provide programmatic flexibility for the entity to determine which roles to identify. The content identified in Part 2.2-2.10, however, is very specific and may not align with the roles identified by the organization, so there should be some flexibility to omit or make optional some of the sub-requirements for some identified roles. As long as that distinction is programmatically documented, the entity should not fear non-compliance. The way this is it written today, it appears as though all of this training is required for anyone with any type of access. Additionally, some of this training should not be given to someone before the access is granted, based on the sensitivity of the information. Recovery information, for example, should wait until the access is completely authorized and the person has met all prerequisites and other operational training. [Intent?] If the intent of the SDT is that each of 2.2-2.10 should be included in at least one of the roles defined such that all topics are eventually covered by the entity, but not necessarily for every role and not necessarily for “attain” as long as they are covered in “retain” – this is a good intention, but not clearly stated. However, the VSL table is additionally problematic with respect to this intended flexibility. [Proposed Verbiage: R2] Each Responsible Entity shall have a role-based cyber security training program to attain authorized electronic access or authorized unescorted physical access to BES Cyber Systems. The training program(s) must also address elements necessary to retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems. The program(s) must collectively include the assignment of each of the elements in 2.2 – 2.10 to at least one of the identified roles within 2.1. Rationale-the change to “both attain and retain” allows the entity to have programs for attaining that differ from the requirements necessary to retain access, and the existence of two approaches allows the entity to keep sensitive information related to recovery in the “retain” program so sensitive information is not provided prior to access. [Proposed Verbiage: R2.1] Add the following sentence into the main body of the Requirement, immediately following the existing verbiage. “Each identified role must be associated to a minimum of one training content element defined in 2.2 - 2.10 and identified roles must collectively cover content all elements defined in 2.2 - 2.10.” [Recommendation] Remove the reference to the sub-requirements 2.2-2.10 in the VSLs to allow necessary flexibility within programmatic definitions. [Recommendation] If the verbiage recommendation is accepted, the VSLs are fine. If not, the VSLs need to be changed to accurately reflect that each role does not need *every* element. [Proposed Verbiage] for Low, Medium, and High VSLs, add the word “collectively” in front of “include number of the required training content elements….” [R3] Legacy phrasing with regard to the date overall training is required was sufficient as long as it was broad enough to educate those granted physical or electronic access. If corrections are made to R2 to reflect that some of the training elements may be required to “retain” instead of “attain” the following change may not be necessary. Otherwise, more specific, role-based training should be provided within an appropriate timeframe after acquiring certain responsibilities and should be necessary for retaining those responsibilities. The date of the acquisition of those responsibilities should be tied to departmental documentation and roles/responsibilities lists instead of HR reports on official job change. This allows for transitions required by reliable operations, as well as training periods. Also, with respect to demonstrating training when the access is attained, it forces the entity to maintain a complete history for each person who has ever had access and what training he or she has received since the very first access was obtained. This could be decades worth of training materials, so we’d support the addition of a retention guideline that refers to access attained since the last audit. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program or the failure to implement a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. [R4]With respect to demonstrating initial PRA when the access is attained, it forces the entity to maintain a complete history for each person who has ever had access and the PRA he or she had when the very first access was obtained. This could be decades worth of PRA materials, so we’d support the addition of a retention guideline that refers to access attained since the last audit. [Recommendation] Align the measure for R4.4 with the requirement, itself. Change the language in the requirement to include

reference to a vendor contract or legal agreement, and from “verifying” to “assuring.” The measures should be proof of that process or contract rather than what seems to be a copy of the vendor’s actual program. This may be difficult or impossible to achieve. [Proposed Verbiage] Acceptable evidence may include, but is not limited to, the entity’s documented personnel risk assessment program with the criteria, process, or contract identified. These VSLs are fine. [R5] Same intent and assumptions for R4. Additionally, the measures are good. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program or the failure to implement a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs.
[R6] This requirement is appropriately written and attainable. Thank you. Recommend changing the VSLs to eliminate zero defect problem. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program or the failure to implement a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. [R7.1]: Recommend changing the verbiage in the last sentence to indicate that the 24 hour clock is related to the initiation, rather than the termination so as not to create two problems should the entity miss the initiation. [Proposed Verbiage] “...and complete the revocation within 24 hours after the effective date and time of the initiation of access revocation." [R7.2]: Too short a time span. Recommend returning to legacy timeframes for job changes within an organization or extending the allowable timeframe based on business days instead of calendar days. For a job change, there is no urgency associated, so weekend access removals are unnecessary. Additionally, there need to be provisions within the Standards for situations where a person will need to straddle two jobs until a replacement is up to speed. [R7.3]: Too short a time span. Recommend extending the allowable timeframe based on business days instead of calendar days. The access removals associated with 7.1 should be sufficient to compensate for the risk introduced by waiting through a weekend for information access removals. [R7.4]: If 'revoke' in this case means to 'delete' the user account from the system, we disagree. [Recommended Verbiage] Change “revoke” to “disable.” [Rationale] We would disable the account and possibly change the account password but when you delete a Windows account you can never reclaim the original GUID that Windows assigns to the unique account. Therefore, reporting, file ownership and anything relating to the GIUD will have been lost and difficult to track past account activity. This may be true for other operating systems as well. [R7.5]: The "out" for extenuating operating circumstances should be applied to all CIP 4 R7 requirements. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program or the failure to implement a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs.
No
Yes
Alliant Energy voted “No” on the Standard, as a whole, due to the significance of the changes we propose herein. Agree EEI Comments with respect to moving applicability elements out of the main requirement in the table. Limit applicability to the applicability column. [R1.1] “All BES Cyber Assets…” should apply to BES Cyber Assets associated with High and Medium Impact Sites that have external routable connectivity. There should not be an obligation to create an ESP with an EAP around an otherwise isolated network. This ties into the proposed definition for ESP and should be considered along with that proposed definition. [R1.2] Recommend combining 1.1 and 1.2, after the changes to the applicability and definitions are completed. [R1.4] Recommend changing “where technically feasible” to “within the capabilities of the system.” [R1.5] Change applicability verbiage to Electronic Access Points associated with ESPs at High Impact Sites and Electronic Access Points associated with ESPs at Medium Impact Control Centers. Rationale – the current phrasing would suggest the need to implement external routable connectivity in otherwise isolated networks to meet this requirement. Additionally, the requirement is very subjective and may not be feasible for encrypted communications. This requirement needs to be clarified or stricken. Does this relate to just ingress.

egress, or both? Measures should be written to allow the entity to come up with different, but equally effective solutions. The “and” between the measures implies that both are required, at a minimum. Instead, wholly different options may exist. [VSLs] The percentages are problematic as it is not clear what, exactly, is being measured. How does an entity count or measure External Routable Connectivity? Is it rules, external devices, internal devices, or something else? These need to be written such that they apply to the program, itself, and continues to maintain the zero tolerance approach, and they are not progressive. The Low currently states criteria that aren’t even used in the rest. Recommend, instead, that they be structured such that a Severe is the lack of a program or the failure to implement a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria.
[R2] Replace “Where technically feasible” with “Within the capabilities of…” to eliminate the allusion to maintaining the TFE process. Alliant Energy agrees with the EEI comments related to moving the applicability statements out of the requirement and limiting them to just the applicability table. With these minor changes, Alliant Energy supports this requirement and its intentions.
No
Yes
Yes
Alliant Energy was very close to voting “Yes” on this requirement. While most of it is appropriate, the comments mentioned herein warranted a “No” vote until corrected. [R.1] Recommend referring to Electronic Access Control Systems in the same way that Physical Access Control Systems are mentioned for clarity and consistency. The definitions of both take care of the monitoring component, so there is no added benefit to mentioning the Monitoring component again in the language of the Requirement. [R1.1] If we will be measured on implementing, the requirement, itself, should indicate it, rather than just putting that word in the measures. Additionally, the applicability, measures, change description, and main requirement do not align with respect to whether or not EACs or PACs should be protected. There are conflicting messages and they should be corrected. [R1.2] Recommend changing “allow” to “restrict” within the requirement. [R1.4] –The identified percentage requires a level of tracking for monitoring that may not be technically feasible. Additionally, a .1% down time for monitoring security will accumulate for monthly planned outages to implement patches so would like to see allowances for this. A percentage uptime figure should be removed from the standard. Placing specific values such as this should not be included in standards and are a distraction that auditors will try to prove rather than focusing on overall security posture. If an entity can show all outages and maintenance and associated compensating controls during the outage, this is sufficient control, as is required in R3.2 already. Proposed Verbiage: Have controls that monitor the PSP 24X7 with mechanisms for identifying and documenting planned or unplanned outages. [R1.5]: Recommend striking the reference to “within 15 minutes of detection” and, instead, require the documentation of appropriate response timing within incident response plans. [R1.6] The identified percentage requires a level of tracking for monitoring that may not be technically feasible. Recommend have controls that monitor the PSP 24X7 with mechanisms for identifying and documenting planned or unplanned outages. [R1.7]: Recommend striking the reference to “within 15 minutes of detection” and, instead, require the documentation of appropriate response timing within incident response plans. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program or the failure to implement a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria.
Yes
No
No
No
No

Alliant Energy voted “No” on the Standard, as a whole, due to the significance of the changes we propose herein. Many requirements, if changed in accordance with our sometimes minor verbiage proposals, would be a “Yes.” [R1] – Consider adding a qualifier for external routable protocol on Medium Impact facilities for all CIP-007 R1 sub-requirements to maintain consistency. Refer to the “Change Rationale” provided by the drafting team in R5.6 for the justification for this change. In all applicability columns, (CIP-007) where medium impact facilities are included, recommend including “with external routable connectivity”. [R1.1] Recommend adding the routable connectivity qualifier on the whole of R1, including High and Associated cyber assets. Recommend changing “Where technically feasible” to “Within the capabilities of the system…” Additionally, Alliant Energy supports EEI comments related to the elimination of applicability components within the requirement and move them to the applicability column. Discussion of cyber assets in this context is in direct conflict with the BES Cyber System concept and needs to be stricken. [VSL Recommendation] This VSL is written as a zero tolerance violation. There is also no progression. Recommend, instead, that they be structured such that a Severe is the lack of a program or the failure to implement a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria. [R2.1] Alliant Energy agrees with EEI comments related to the inclusion of cyber assets in the requirement, itself, instead of limiting applicability components to the applicability column. Also, the cyber system concept is in direct conflict with a specific requirement applied at the device level. [R2.3] Recommend removing the term “dated” from the action plan to allow waiting for an outage or window that is not yet scheduled. If "dated" cannot be removed, recommend inserting the word "estimated" in front of timeframe. [R2.4] Recommend adding flexibility to change the plan without risking non-compliance. Proposed Verbiage – “For each plan created or revised in 2.3, document the actual implementation date and the reasoning for any discrepancies between the estimated timeframe and actual implementation.” [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program or the failure to implement a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria. [R3 – R3.3] should be revised to account for the differing methods that can be utilized as part of R3.1. As an example, per R3.1, a company can use policies as a method to deter, detect, or prevent malicious code. If a company were to adopt policies as their method, R3.3 would not be applicable as there would be no malicious code to update. [R3.3] This applicability should be limited to just those systems with External Routable Connectivity. Without that connectivity, the monthly signature updates are not commensurate with the actual risk. Additional verbiage needs to be added to reflect the potential that the only implemented controls are system hardening and/or policies in 3.1. Because these devices tend to be those in TFEs for malware protection, some accommodation must be made here. [R4.1]Proposed Verbiage: “Within the capabilities of the BES Cyber System, log events such that Cyber Security Incidents can be identified and investigated. Event types include: …” [R4.2] Proposed Verbiage: “Within the capabilities of the BES Cyber System, generate alerts for detected security events that the responsible entity…” [R4.3] Recommend striking this requirement or changing the verbiage to “Document the controls implemented to identify and respond to detected logging failures. Document detected logging failures along with any discrepancies between the actual response and the documented response plan.” No reference to a timeframe should be included in the requirement, but it may make sense to require its inclusion in the documented plan. [R4.4] Proposed Verbiage: Remove “Where technically feasible” and precede requirement with “Within the capabilities of the BES Cyber System. [R4.5] Alliant Energy would like clarification on the intent of this requirement. In its current state, it is highly subjective. While we recognize that the possibility exists that system alerts are not working properly and that the entity should be verifying functionality, a manual review of logs in addition to implemented automated parsing and alerting will not add security. The criteria configured into an automated system are intended to match the criteria used by a person manually reviewing logs; it’s just that the automated system allows the immediate and rapid parsing of voluminous records. Alliant Energy would like to understand what security goal is strived for within this requirement. Additionally, this requirement states a “how” without stating a “why,”

which prevents the entity from finding a better or more efficient way of achieving the same goal. Recommend stating the goal within the requirement and leaving it to the entity to define the program that meets the goal. [Proposed Verbiage to add clarity]: “Document and implement a secondary control(s), and an associated interval, not to exceed 2 weeks, to assure the generation, capture, monitoring, and alerting of events as identified in 4.1. Move the summarization or sampling verbiage to the measures. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program or the failure to implement a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria.
[R5.1] Propose change to “within the capability and operation of the BES Cyber System” instead of “technically feasible.” [R5.2] The CIP Senior Manager will not have the technical expertise to recognize the actual risk introduced by the presence or quantity of default or generic account types. The turnover rate at the organizational level at which this level of expertise exists would create a prohibitively administratively burdensome process without adding the desired oversight. Recommend striking this requirement or changing to allow designation similar to CIP-004 R6, without direct documentation ties to the Sr Mgr. [R5.4] Recommend changing “technically feasible” language to “within the capabilities of the system or allowable by support vendors.” Proposed Verbiage: “To the extent allowable by the support vendors and capabilities of the system, change publicly-available or industry-known default passwords.” Removed “on cyber assets” to align with the cyber system applicability column. [R5.5] Proposed Verbiage for 5.5.1: “Password length that is, at least, eight characters or the up to the maximum allowable by the system if that maximum is less than eight.” Carry this change through 5.5.2 to add clarity. [R5.6] Don’t touch this one – it’s great as it is. [R5.7] Recommend changing technically feasible language to “Where system capability or operational risk allow, limit the number of unsuccessful…” [VSLs] These are more in alignment with the expectations of the industry. Perhaps a Low and Medium could be created.
Group
ACES Power Marketing
Jason Marshall
No
No
No
No
No
Yes
No
(1) Regarding Question 1 (CIP-004-5 R1): Conceptually, we agree with the requirement and the attempt “to remove the need to ensure everyone with… access ‘received’ ongoing reinforcement” which was expressed in the change rationale for Part 1.1. However, we do not believe the requirement accomplishes this intent. Part 1.1 includes “for the Responsible Entity’s personnel who have authorized… access”. How does a responsible entity prove that it reinforced security awareness to personnel with authorized electronic and/or authorized unescorted physical access unless they maintain a training record for each of these personnel? We think removing “for the Responsible Entity’s personnel who have authorized… access” would help solve this issue. (2) Regarding Question 2 (CIP-004-5 R2): While we agree with the concept that a responsible entity should be able to structure their training to various roles, we believe that Part 2.1 needs to be optional. Smaller entities may find it more cost effective to deliver the same training to everyone rather than develop role based training. As long as it covers all required parts, this should be allowed. (3) Regarding Question 3 (CIP-004-5 R3): Requirement R3 would be clearer if it referenced Requirement R2 rather than repeating much of the language from Requirement R2. Requirement R3 is simply a requirement to implement the training program from Requirement R2. Thus, we suggest replacing everything after “to attain and retain… access” with “required for CIP-004-5 R2”. (4) Regarding Questions 2, 3, 4 and 5 (CIP-004-5 R2, R3, R4 and R5): The main requirements are written such that they apply to all BES Cyber Systems including low impact systems. The risk assessment program is only supposed to cover

the “Applicable BES Cyber Systems and associated Cyber Assets” identified in the Table. After the clause “authorized electronic access or authorized unescorted physical access” within the main requirement, we suggest changing “to BES Cyber Systems” to “Applicable BES Cyber Systems and associated Cyber Assets”. The rationale box for the requirement also needs to be modified. (5) Regarding Question 4 (CIP-004-5 R4): We thank the drafting team for clarifying that the risk assessment is limited to addresses with a duration of six months or more. Short term addresses may not be reported by the employee, vendor or contractor and may not show up in a records check. (6) Regarding Question 5 (CIP-004 R5): The measure for Part 5.2 of Requirement R5 needs to be modified. As written now, the only evidence that it lists is the personnel risk assessment. This is contrary to Part 4.4 of Requirement R4 which describes that the personnel risk assessment program must have a criteria or process to verify that the personnel risk assessment has been performed for vendors or contractors. Having a copy of a personnel risk assessment for non-employees is contrary to some state laws. A simple solution would be to include other types of evidence in the measure such as attestations from contractors and vendors or receipts (or other equivalent forms of evidence) from companies that perform personnel risk assessments that identify the name of the contractor or vendor. (7) Regarding Question 2 (CIP-004-5 R2 VSLs): It is not clear if missing three parts of the requirement is a Moderate or High VSL. Moderate is missing two and High is missing four. (8) Regarding Question 5 (CIP-004-5 R5 VSLs): Given the number of notice of penalties that have been issued regarding personnel risk assessments, it is clear that documentation is difficult to maintain for personnel risk assessments. Thus, escalating to higher VSLs for each missing personnel risk assessment seems excessive and inconsistent with actual penalties that have been issued for missing personnel risk assessments. This is particularly true for employees that have had an annual performance review and are in good standing. For long-tenured employees in good standing, the personnel risk assessment is little more than an administrative check.
(1) Regarding Question 6 (CIP-004-5 R6): For more clarity, we suggest that Parts 6.2, 6.3, and 6.4 should be modified to refer to Parts 6.1.1, 6.1.2, and 6.1.3 respectively rather than just Part 6.1. (2) Regarding Question 7 (CIP-004-5 R7): In Part 7.2, revoking access for employees that have been reassigned or transferred by the end of the next calendar day is too short a time frame particularly for those employees in good standing. (3) Regarding Question 7 (CIP-004-5 R7): Part 7.4 needs to be clarified that revocation of user accounts does not necessarily mean deletion of the accounts. Accounts may need to be disabled due to the unique characteristics of the operating system. Deletion on certain operating systems can have unintended consequences. (4) Regarding Question 7 (CIP-004-5 R7): The measures in Part 7.5 only account for the 30 days within the requirement and not the 10 days after “extenuating operating circumstances”. It needs to account for this latter part of the requirement. (5) Regarding Question 7 (CIP-004-5 R7): There is an extraneous 77 in front of the reference next to the change rationale box. (6) Regarding Question 7 (CIP-004-5 R7 VSLs): The Lower VSL regarding passwords for joint accounts does not make sense. It includes the statement “for one or more individuals”. Since it is a joint account there will always be more than one individual. (7) Regarding Background Section 5: The third paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. Which is it? We support the latter. (8) Regarding Question 6 (CIP-004-5 R6 and R7): Measures for Parts 6.6, 6.7 and 7.1 are inconsistent with the statement in the background section which says that a numbered listed includes all required evidence. The measures specifically say “evidence may include, but is not limited to”. We agree with the actual statement in the measure and believe the background section should be updated. (9) It is not clear why Parts 6.1, 6.4, 6.7 and 7.3 are included in CIP-004-5 R6 and R7 and not CIP-011-1. These parts deal with protecting BES Cyber System Information. Protecting BES Cyber System Information is consistent with the stated purpose of CIP-011-1 but is not consistent with the stated purpose of CIP-004-5. The purpose of CIP-004-5 is essentially to minimize risk from individuals accessing BES Cyber Systems while the purpose of CIP-011-1 is to prevent unauthorized access to BES Cyber System Information. To avoid confusion, we suggest moving them to CIP-011-1.
No
No
(1) In Part 1.1, the requirement and applicability are not consistent. The requirement states that it applies to all BES Cyber Assets which would include low impact BES Cyber Systems. The applicability column limits applicability to high impact and medium impact BES Cyber Systems. For consistency,

we suggest changing “All BES Cyber Assets” to “BES Cyber Assets within applicable BES Cyber Systems” within the main requirement. (2) In the background section, there is no description of “High Impact BES Cyber Systems with External Routable Connectivity” which is included in Part 1.2.
(1) The requirement and definition need to further clarify what constitutes Interactive Remote Access. Is accessing a BES Cyber Asset within the Electronic Security Perimeter from another trusted network (i.e. a company LAN without BES Cyber Systems or BES Cyber Assets) considered Interactive Remote Access or does it only constitute Interactive Remote Access if it is from an untrusted network? (2) Part 2.3 should further clarify multi-factor authentication (MMA). Does MMA apply to the remote session through the ESP, to the Intermediate Device, or both?
No
Yes
Yes
(1) Regarding Applicability Section 4.2.4 Exemptions: This was changed from the last posting to indicate the exemptions are for CIP-002-5. CIP-002-5 already has the same exact exemption language. Either this reference should be changed back to CIP-006-5 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (2) Regarding the Applicability Section please see comments submitted by ACES Power Marketing regarding Applicability in Comment Form A, Question 3, Comments 6-9. (3) Regarding Question 14 (CIP-006-5 R1): It is unclear how the “operational and procedural controls to restrict physical access” required in R1 Part 1.1 differ from the “physical access controls” required in Parts 1.2 and 1.3. Suggested methods for restricting physical access are given in the “Guidelines and Technical Basis” section, but none are given for “operational and procedural controls.” Additional discussion in the application guidelines on these operational and procedural controls would be helpful in understanding them. (4) Regarding Question 14 (CIP-006-5 R1): The addition of the list (BES Cyber Assets, BES Cyber Systems, etc.) to the main requirement creates ambiguity. This has the effect of including low impact BES Cyber Systems, BES Cyber Assets, etc. into the requirement. In effect, now a documented physical security plan is required for them without any of the requirement parts applying. We suggest either removing the list or adding “applicable” in front of the list to make it clear that only those items in the applicability column are intended. (5) Regarding Question 14 (CIP-006-5 R1): We disagree with including 99.9% availability in Part 1.4 and Part 1.6. First, outages for planned updates will accumulate greater than 0.1% outage time. Second, this refocuses the requirements from enabling requirements that focus on security posture to actual performance. Third, it essentially creates a requirement within a requirement. Fourth, it creates additional unnecessary evidence generation. Not only will the entity have to prove it enabled monitoring but it will have to prove the monitoring worked. If the purpose is to prove monitoring worked, then eliminate the enabling requirements and just state the availability requirement. At least, this way the registered entity only has to show actual availability for evidence. Fifth, availability would be better suited for a responsible entity to use as an internal control for self-assessment of a security program rather than as an enforceable requirement. Sixth and finally, Requirement R3 obviates the need for an availability requirement. R3 compels the entity to maintain and test their physical access control systems and to document any outages. Thus, availability is likely to be as high as reasonably possible which may not quite reach 99.9%. (6) Regarding CIP-006-5 R1 and R2: Parts 1.9 and 2.3 regarding data retention belongs in the evidence retention section. Otherwise, it is in direct conflict with the statement “shall retain data or evidence for each requirement in this standard for three calendar years” from the evidence retention section. (7) Regarding the VRF for CIP-006-5 R2: A visitor control program is intended to identify and log visitors to the Physical Security Perimeter (PSP). They cannot gain access due to other requirements such as CIP-006-5 Requirement R1 that compels the responsible entity to establish physical access controls. Furthermore, the training requirements of CIP-004-5 compel a responsible entity’s personnel with authorized unescorted physical access to have been trained on who has access and that visitors must be escorted. Thus, the visitor control program can only be an administrative function that is truly intended to keep track of those visitors that have been to the PSP. By definition, administrative requirements should have a Lower VRF. Thus, CIP-006-5 Requirement R2 should have a Lower VRF. (8) Regarding CIP-006-5 R2 VSLs: A Lower VSL could be written. For example, missing one entry in the in the visitor log could be written as a Lower VSL rather than a Moderate VSL. (9) Regarding Background Section 5: The third paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. Which is it? We support

the latter.
Yes
Yes
Yes
Yes
Yes
(1) Regarding Applicability Section 4.2.4 Exemptions: This was changed from the last posting to indicate the exemptions are for CIP-002-5. CIP-002-5 already has the same exact exemption language. Either this reference should be changed back to CIP-007-5 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (2) Regarding the Applicability Section please see comments submitted by ACES Power Marketing regarding Applicability in Comment Form A, Question 3, Comments 6-9. (3) Regarding the VSLs for CIP-007-5 R1 - Because there are likely many ports for Requirement R1, the four VSLs could be written based on the percentage of ports missing from documentation. (4) Regarding the VSLs for CIP-007-5 R2-4 - For Requirements R2-R4, there will likely be many BES Cyber Systems to which the requirements apply. Four VSLs could easily be written based on the number of BES Cyber Systems for which the requirement was missed. (5) Regarding CIP-007-5 R4: Part 4.4 regarding data retention belongs in the evidence retention section. Otherwise, it is in direct conflict with the statement “shall retain data or evidence for each requirement in this standard for three calendar years” from the evidence retention section.
Individual
David R. Rivera
New York Power Authority
No
No
Yes
No
Yes
Yes
No
NYPA agrees with NPCC comments, plus - In R2 Part 2.10, “training content on risks associated” – it’s not clear what is required. Awareness and other training (i.e. part 2.4) would cover this area in general; we don’t believe that this specific training module is required.
NYPA agrees with NPCC comments.
No
No
NYPA agrees with NPCC comments, plus – In R2, allow an exclusion for the devices that accessed or interrogated in a read-only mode.
NYPA agrees with NPCC comments, plus – In R2, allow an exclusion for the devices that accessed or interrogated in a read-only mode.
Yes
Yes
No
In R1 (parts 1.4 and 1.6), the references to 99.9% availability are not clear. There is no guidance as to how this can be measured; therefore recommend removing the availability reference as the entity will already have compensating measures in their physical security plan. Also, how is one to know unauthorized circumvention?
Yes
No
No
No

No
NYPA agrees with NPCC comments.
NYPA agrees with NPCC comments, plus – In R5.1, is too restrictive and expansive for 'Medium' BES Cyber Systems. We suggest replacing "all user access" with "access to configuration or programming resources" or "cyber access".
Individual
Tracy Richardson
Springfield Utility Board
No
Yes
Yes
Yes
Yes
Yes
No
SUB agrees with CIP-004-5 Requirements R1, R2, R3, R4, and R5 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
In Part 7.2 Requirements for reassignments or transfers, "by the end of the next calendar day" does not take into consideration weekend days. SUB would recommend "by the end of the next business day" for High and Medium Impact. SUB agrees with CIP-004-5 R7 not being applicable to Low Impact BES Cyber Assets and Cyber Systems.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Robert Mathews
Pacific Gas and Electric Company
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
No
Yes
Yes
R1.4 is unacceptable as stated. Rationale: While the recognition that 100% availability of the monitoring systems may not be feasible is good, the specific requirement for 99.9% availability has no technical basis and likely will result in imprudent use of resources to provide the specific data needed to demonstrate performance to this specific level for a large quantity of devices or processes, many which may not have the capabilities to even provide the data necessary to perform an availability calculation. In the Guidelines and Technical Basis section for R1 on page 28, Alarm Systems and Human Observation are mentioned as methods to monitor physical access. Measuring the availability of human observation or components of an alarm system such as door or window contacts to the 99.9% threshold is likely not feasible or prudent. Suggest Standard Revisions: Have controls that monitor the Physical Security Perimeter for unauthorized circumvention of a physical access control into a Physical Security Perimeter.
Yes
No
No
No
Yes
Rationale: Medium Impact BES Cyber System without External Routable Connectivity (isolated computer systems) should not be subject to the same requirements in R2.1, 2,2, 2.3, 2.4; R3.1, 3.2, 3.3 and R4.1 as those with external routable connectivity. For example some systems without external routable connectivity cannot employ monitoring, patching and malicious code protection mechanisms used on systems with external routable connectivity. Suggest Standard Revisions: Revise R2.1, 2,2, 2.3, 2.4; R3.1, 3.2, 3.3 and R4.1 applicability to Medium Impact BES Cyber Systems with External Routable Connectivity
Group
SPP and Member companies
Lesley Bingham
Yes
No
Yes
Yes
Yes
Yes
No
CIP-004-5 R2.2-2.10 contain elements which can comprise a training program. If role-based training is required (as indicated by R. 2.1), can a Responsible Entity choose from those elements to create a training program for different roles? Or must all roles identified receive some training from each of the elements in R. 2.2-2.10? If all roles must receive some training for each of the elements in R. 2.2-2.10, what is the value of having role-based training? If all roles must receive some kind of training on all elements of R. 2.2-2.10, we would recommend adding the following language to each of the sub-requirements: Training content should be provided to each identified role based on the level of understanding needed for each. Each identified role must [or must not if Responsible Entities can choose which elements to include] be provided training on this element.
Table 7 is focused on Access Revocation and the time guidelines called for are stringent. While no one advocates orphaned accounts, the HR and IT processes which must support access revocation can take time and cause conflict with these standards, at best or non-compliance, at worst. The processes are designed to capture appropriate approvals, create a trail of activity which can be used as audit

evidence, and other activities which are designed to provide compliance. Realistically, these efforts take time—time which the standard does not allow for. Smaller entities without an on-call staff will have difficulty complying. Terminations are not uniform and may call for different responses. The 24 hour timeframe does not allow for consideration of a response which may be appropriate for the situation. The language in 7.5 acknowledging extenuating circumstances would be a helpful addition to Part 7.1, 7.2, and 7.3 The Measures in 7.1 suggest that a system-generated workflow is required. Managing the trail of activities for a termination can easily be managed via emails sent from activity initiator to approvers, on to implementation resources and an email back to the group when the access is revoked. Is such a “paper trail” considered adequate? The Measures in 7.2 do not provide additional security and extend what is already a time-sensitive and time consuming process. Also recommend changing these to a list of bullets from numbers and removing the “and” from the first item. Part 7.3 should be accomplished as required when Part 7.1 is completed. To have a separate item for this seems to be little more than an audit trap. The Measure for 7.5 does not indicate what would be appropriate evidence for the “extenuating operating circumstances”. If documentation is required, the measure should state “Additional documentation for ‘extenuating operating circumstances’ consists of an overview of the situation, approval by the CIP Senior Manager or delegate, and attestation that the situation has been addressed” or other concrete examples.
No
Yes
1. Part 1.3 requires monitoring and documentation of all outbound traffic. While such is absolutely a good practice, it will be an expensive burden for many entities. If monitoring only inbound traffic for a Physical Security Perimeter is deemed to be adequate, it should be adequate for the Electronic Security Perimeter. Recommend dropping requirement for outbound traffic. 2. Part 1.4 assumes that there will be dial-up connectivity in the ESP of all Responsible Entities. How can an entity prove a negative if they do not allow dial-up? Recommend adding a sentence to the requirement which states “Dial-up connectivity may not allowed by all Responsible Entities and this requirement may not apply for all situations.” Recommend adding a sentence to the Measure to state “Evidence may include an attestation of connectivity options where dial-up connectivity is not present in a Responsible Entity’s ESP.” 3. The Measures in Part 1.5 are still heavily centered on a single technology as the primary means of compliance—Intrusion Detection Systems. Recommend adding language to lessen focus on IDS. Examples could include “Evidence that intrusion detection or other monitoring systems are functioning” or “Documentation showing where intrusion detection or other monitoring systems are deployed.” It’s also important to note that “malicious” activity cannot be determined strictly by watching for an activity. Traffic to an ESP which is malicious may in fact appear to be normal. The qualification of “malicious” vs “normal” requires knowing an actor’s intent, which cannot always be gleaned from log entries.
No
Yes
Yes
1. Part 1.4 requires a specific availability requirement that may be hard to measure for some controls. For example, how do you measure the availability of a guard? While availability targets are certainly valuable, defining this narrowly will provide a burden for tracking and measuring for entities. 2. Part 1.6 requires a specific availability requirement that may be hard to measure for some controls. For example, how do you measure the availability of a guard? While availability targets are certainly valuable, defining this narrowly will provide a burden for tracking and measuring for entities. 3. Part 3.2 requires documentation of outages for the physical access control, logging and alerting systems. This would be a better place for the availability requirements currently in Part 1.4 and 1.6.
Yes
Yes
No
No
Yes
1. Part 1.2 and Part 2.1 have better language than the previous release of the standard. Specifically, it is helpful that the Standard Drafting Team recognizes that some devices are not able to be updated.

2. Part 3.3 is confusing. Breaking this up into separate sentences will provide clarity. Recommend “Update malicious code protections that use signatures or patterns at least once within 35 calendar days of each available signature or pattern release. This does not require use of every available release, but where a release is available, at least one update has occurred within 35 calendar days from that release. If a Responsible Entity determines and documents that specific updates of signature or pattern releases will negatively affect the Cyber Asset or BES Cyber System, those specific releases are not required to be applied.” 3. Part 4.1 needs to include the “capable of detecting” in the Requirement and not solely in the measure. Recommend “Log events, where the System is capable of detecting such, for the identification of….” Part 4.1.4 requires the logging of “malicious activity”, but analysis of intent is required to determine if an action is malicious. The disagreement here is not to say that the industry shouldn’t do logging of sufficient information for adequate Cyber Incident Response. What should be avoided is language which could allow an auditor to request a list of all log data which shows malicious activity. Any log file will only record what actions were taken—not the intent behind the actions. Recommend language “log user and system activities determined to be indicators of misconduct”. Part 4.2 again uses the phrase “malicious activity” and the same objections apply. Recommend use of “suspicious”, “unusual” or “detected activity which the Responsible entity determines as not normal”. Part 4.5 requires a manual review of logs for which the Responsible Entity has already generated alerts. Recommend changing to “Review a summarization or sampling of logged events that the Responsible Entity has determined could identify previously undetected Cyber Security Incidents. Such a review will be conducted every two weeks at a minimum.”
1. Part 5.1 only mentions user accounts and does not address the other types of accounts covered in the table in the Application Guidelines. If user account is a distinct term separate from the other types of accounts in the table, then User Account should be defined in the Definitions and should clarify that the term addresses interactive accounts used by individual persons. This would be distinct from system-to-system process communications. Such accounts should have initial and annual password change requirements and robust password composition requirements. System accounts should also be defined to clarify that these are non-interactive accounts which may be installed on a device from the manufacturer or required for use software, but will never be used during a login process by an individual person user. These accounts can have other protections, but should not be subject to the initial password change or annual password change requirement. These accounts are not generally built in a way which allows for uncomplicated password changes and such changes can be highly disruptive to the devices where they exist. Often, touching these accounts for a password change puts the reliability of the device at a higher risk than the risk of a long-used password. The table in the Application Guidelines is helpful, but since it is not a part of the standard, Responsible Entities will not be able to take advantage of the assistance of the types of accounts noted and the suggested periodicity of password change. Adding this table to the plain language of the standard could be beneficial to Responsible Entities. 2. Part 5.5 is an improvement in password composition language. Thank you for your efforts, Standard Drafting Team. 3. Part 5.6 could be clarified to be applied to only individual user accounts with the addition of this sentence at the end of the requirement: “This is not intended to apply to non-interactive, non-user assigned accounts.”
Group
IRC Standards Review Committee
Christine Hasha
Yes
No
No
No
No
Yes
Yes
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding question 8. The IRC respectfully provides these additional comments. The IRC requests that CIP-004-5 Measure 1.1 (question 1) be changed from “but not limited to” to “but is not limited to”. This is consistent with the other measures contained within the standard.

The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding question 9. The IRC respectfully provides these additional comments.
Yes
Yes
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding question 12.
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding question 13.
No
Yes
No
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding question 17. The IRC requests that CIP-006 Requirement 1.4 and 1.6 (question 14) be modified from “Have controls” to “Have control(s)”. The IRC requests that CIP-006-5 Requirement 1.5 and 1.7 (question 14) remove reference to “BES Cyber Security Incident Response Plan” since this is a Physical Incident and not cyber. Request that Requirement 1.5 be revised to “Issue an alarm or alert in response to detected unauthorized circumvention of a physical access control into a Physical Security Perimeter within 15 minutes of detection.” Request that Requirement 1.7 to “Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System within 15 minutes of the unauthorized physical access.” The IRC requests that CIP-006 Measure 2.2 (question 15) be modified to “Evidence may include, but is not limited to, records of manual or automated logging of the entry and exit of visitors into the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor’s name, and the name of an individual point of contact responsible for the visitor.”
Yes
Yes
Yes
No
Yes
The IRC supports comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) on the following items. • The 30-day timeframe in CIP-007-5 R2.2 should be increased to at least 35 days to allow for monthly processes. • The applicability of CIP-007-5 R2.1, R2.2, R2.3 and R2.4 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity.” The exclusion of cyber systems/assets with no routable connectivity will eliminate a significant burden of tracking and documentation requirements associated with serially connected devices that would have minimal impact to reliability. This is particularly burdensome for systems that are geographically dispersed and would require direct personnel interaction and physical access to each device to deploy patches to non-externally routable systems. • Under measures, M2.4 bullet 2 should be revised to read “Records of implementation of vendor recommended or other appropriate mitigations;” to eliminate any misunderstanding and allow for appropriate mitigation plans that are different than a vendor-recommended plan. • Modify Requirement R 4.1.3 from “detected and logged malicious software…” to ”detected and logged malicious code…” • Eliminate requirement R4.1.4. The term “malicious activity” is ambiguous. • Modify Requirement 4.2.1 to read “detected events per R4.1; and” The IRC requests that CIP-007-5 Requirement 3.1 (question 20) be modified to remove strike the word “deter”. Deter and prevent are redundant of each other. The IRC requests that CIP-007-5 Requirement 3.3 (question 20) be modified as, “For signature- or pattern-based malicious code protections, update the signatures or patterns within 35 calendar days of each available signature or pattern release. Signature or pattern releases may be grouped together for the 35 day update. This excludes releases that negatively affect the Cyber Asset or BES Cyber System.” The IRC requests that CIP-007-5 Requirement R4.1 (question 21) be modified as, “Log events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events, where technically feasible:” The IRC requests that CIP-007-5 Requirement 4.5 (question 21) be modified as, “Where manual logging is used, review a summarization or sampling of logged events at a minimum every two weeks to identify undetected Cyber Security Incidents.” This should only apply where automated processes and alerting are not

possible.
The IRC supports comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) on the following items. • In Requirement R5.1, authentication should be done for accounts, not for user access. Suggest revising to read “Enforce authentication of accounts when accessing applicable Cyber Assets, where technically feasible”. • CIP-007-5 Part 5.4: Recommended change, “Change known default passwords, where technically feasible, unless the default password is unique to the Cyber Asset.” This allows for unique passwords. • CIP-007-5 Part 5.7: Recommended change, “Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful login attempts, where technically feasible.” Please provide guidance on what is considered a suitable minimum threshold. The IRC requests that CIP-007-5 Requirements 5.2 and 5.3 (question 22) have the same applicability. Requirement 5.3 should be modified to remove “with external routable connectivity” from the applicability. The IRC requests that CIP-007-5 Requirement 5.2 (question 22) be modified to “delegate(s).” The IRC requests that CIP-007-5 Measure 5.3 (question 22) be modified to, “Evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.” The IRC requests that CIP-007-5 Measure 5.5 (question 22) be modified to, 5.5.1. Password length that is the lesser of: • At least eight characters; or • Maximum length supported by the Cyber Asset; and 5.5.2. Password complexity that is the lesser of: • Three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric); or • Maximum complexity supported by the Cyber Asset. The IRC requests that CIP-007-5 Measure 5.5 and 5.6 (question 22) be modified to remove reference to attestations. Some organizations are dependent on unions that will not allow for attestations by union members. Add measure that states “Documentation of the registered entity’s procedural solution and training program to educate its affected personnel on its procedural solution.”
Individual
Gregory Campoli
NYISO
Yes
Yes
Yes
No
Yes
No
No
• Please clarify R4 4.2 for how six months is applied • Please clarify how R6.5 requires quarterly review for authorization with R6.6 and R6.7 annual really includes a complete review. Don’t the same “shared” accounts count in both R6.5 and R6.6?
• R7.4 should refer to R7 part 7.1 and 7.3 • R7 Measure change “removal” to “revoke” to be consistent with requirement. • R7 VLFs should be consistent
No
No
• Recommend removing “but is not limited to” from R1 1.1. • R1.5 change from “intrusion detection” system to “detection system”. • Measure 1.7 IDS is too prescriptive and recommend more generic language.
• There appears to be technical conflict in R2.2 between using encryption and IDS monitoring as SSH would prevent IDS from identifying events depending upon implementations. • R2.3 should reference “Multi-factor” solution but not be limited to list as some place you are or other options may be a solution.
No
No
Yes
• R1.3 don’t start with TFE and refer to multifactor control • R1.4 remove 99.9 availability to allow for alternative physical controls with guards as mitigation. • R1.5 a security guard could perform the detection, alerting and response so they would document the event… • Parts 1.5 and 1.7 remove reference to “BES Cyber Security Incident Response Plan” since this is a Physical Incident and not

cyber. • Part 1.5 Revert to the wording that was in the previous draft of CIP Version 5. • R1.6 remove 99.9 availability to allow for alternative physical controls with guards as mitigation. • CIP-006 R2 - Measure in Part 2.2 appears to be a copy and paste error. Suggest revisiting Measure 2.2 as it does not align with the requirement.
No
No
Yes
No
No
• R5 – Can multifactor replace passwords without a TFE?
Individual
Linda Jacobson-Quinn
Farmington Electric Utility System
Yes
Yes
Yes
Yes
Yes
No
No
: 6.1: It is not clear of the individual(s) must be identified by name or if it can be by title. FEUS requests the SDT clarify. 6.1.3: This should be removed – the protections should be included in the information protection program provided by CIP-011-1. It is noted the measures include, “and access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity.” FEUS is concerned that electronic information may be stored in an electronically secured location (aka laptop or encrypted/protected USB) but the physical location may be very mobile in that ‘physical’ location varies. In additional, even printed material may be ‘mobile’. For example, printed copies physically transferred from a Primary Control Center to a Backup Control in which the physical location may be a briefcase in the direct control of someone with access. This type of situation is better handled by an individual’s information protection program rather than the Access Management Program. 6.4 should be removed from this Requirement included in the information protection program provided by CIP-011-1. At a minimum, the SDT should clarify what is meant by physical access. See comments for 6.1.3 – the physical location of printed or electronically stored information may not be stationary and may be impossible to control based on the circumstance. This would be better defined in the Information Protection Program to allow flexibility. 6.7: See comments for 6.1.3 and 6.4 7.3: FEUS feels this would be better defined by an entities Information Protection Program; see comments in R6 regarding the physical location of System Information
Yes
Yes
Yes
Yes
Yes
R1.4 and R1.6 the SDT should define what periodicity the 99.9% availability is determined (monthly, quarterly, annually)
Yes
Yes
Yes
Yes

Yes
Individual
Maggy Powell
Exelon Corporation and its affiliates
No
No
No
No
No
Yes
No
CIP-004-5, R1: We appreciate that the standard consolidates the descriptions of Applicable BES Cyber Systems and Associated Cyber Assets into section 5 to make the table column headings more readable. To clearly direct readers, a notation added to the column heading referencing where to find the descriptions would be useful. CIP-004-5, M1: M1.1 - the list of evidence of distribution options should read "or" rather than "and". The guideline language reinforces that evidence of distribution does not require many or all of these items to demonstrate compliance. CIP-004-5, R2: Further clarification is needed to avoid requiring that every person with access receive training on each topic in 2.2 through 2.10. Training programs should have the latitude to define the type and depth of training appropriate to the role the person has. If all are to train on every topic at depth, it contradicts the concept of role-based training and creates an extraordinarily cumbersome training program. Consider the following revision to R2.1: "Identification of each role and applicable training as defined in R2.2 through R2.10 required for each role." CIP-004-5, R2, R3, R4: The use of the terms "attain" and "retain" are awkward. Consider replacing "attain" and "retain" with "acquire" and "maintain" respectively in R2, R3 and R4. CIP-004-5, R5/M5: We appreciate the acceptance of attestations from contractors or service vendors verifying PRAs.
CIP-004-5, R7: The timing requirements dictated in the requirements indirectly require that entities automate their access programs. As a consequence, automation creates added complications in managing access revocation, for instance, defining what distinguishes a transfer. A new office location or phone number may or may not be a transfer. Further, it's not clear why access revocation requirements for transfers are more stringent than for terminations. The added 30 days for terminations would be valuable for transfers as well. Further latitude within the requirement language is needed to allow internal management of transfers.
No
Yes
CIP-005-5, R1: We recognize and appreciate that the qualifier "technically feasible" gives entities the needed flexibility to meet the security goal in circumstance where the stated requirement is not feasible. It may be useful to clarify in the background or guideline that if not technically feasible, entities are expected to go through the TFE process. Further, NERC Staff should recognize that the Rules of Procedure will likely need revision to accommodate the revised standards that allow for technical feasibility exceptions. The request to approve the ROP revisions should be submitted concurrently with the filing of CIP V5. CIP-005-5, Page #s: One minor note, the page numbers on pages 10-15 of CIP-005-5 are not showing as the others do.
No
No
Yes
CIP-006-5, R1: 1.4 and 1.6 includes a 99.9% availability. We appreciate the latitude to allow for some outage without creating a compliance burden, but greater clarity is needed on how the 99.9% is measured. How was this percent chosen? What goes into the calculation? Does maintenance count? What period is covered to measure? etc. As well, this proposal prompts demonstration of compliance

questions such as what period of time should records cover to demonstrate compliance, etc. CIP-006-5, R1 VSL: We understand the logical basis for the different treatment of dial-up, and previous discussions of CIP-006 and treatment of dial-up is clear; however, the Severe VSL under R1 specifically calls out dial-up. Please clarify expectations concerning BES Cyber Systems with dial-up connectivity either by removing the reference in the VSL or further discussion in the guidelines. CIP-006-5, R2: The wording in 2.2 is awkward: "Require manual or automatic logging of the entry and exit of visitors into the Physical Security Perimeter …" One cannot exit into something. Consider the revision: "Require manual or automatic logging of visitors for entry to and exit from the Physical Security Perimeter …"
No
No
Yes
Yes
Yes
CIP-007-5, R1: M1.1, bullet two should allow for listings of classes of Cyber Assets as in bullet one. Consider revising the second bullet in M1.1 to read: "Listings of the listening ports on the Cyber Assets or class of Cyber Assets from…" CIP-007-5, R2: R2.3 needs revision to clarify the timing expectations. Thirty days from the evaluation completion is acceptable to create a plan; however, revising the plan should be allowed as information and circumstance dictates. The timing should not impose restrictions on prudent revisions to plans. For instance, information regarding a patch may be discovered while testing in the environment indicating that the patch may be harmful or may fail in the environment. A revision to the plan should be allowed to accommodate such new information. Further, the patch implementation should not be required merely to meet a compliance obligation when risks to implementation are discovered during testing or other information sources. The requirement language may need additional language to allow for patch failure. CIP-007-5, R2.4 and R3.3: please offer guidance on what/how much information is expected to demonstrate implementation of a patch plan and implementation of updated signature or pattern files every 35 calendar days. A representative or statistical sample should be acceptable for compliance.
CIP-007-5, R5: The SDT should better align the guidance language to match the requirement language.
Individual
Scott Kinney
Avista Corp
See comments provided by EEI
See comments provided by EEI
See comments provided by EEI
See comments provided by EEI
See comments provided by EEI
See comments provided by EEI
See comments provided by EEI
Group
CenterPoint Energy
John Brockhan
Yes
No
No
No
Yes
Yes
Yes
R2 - CenterPoint Energy believes that the current wording for the training standards creates unnecessary complexity for training, especially entities that may have designed one, all-

encompassing program for compliance with the current version of the CIP Standards. CenterPoint Energy also requests clarification for this requirement and sub-requirements for whether each trainee has to receive all training specified in 2.2 - 2.10. or could the program for each trainee be selective as some information should not go beyond system administrators to protect systems security. CenterPoint Energy recommends the following wording: ""Each Responsible Entity shall have a cyber security training program appropriate to job function…" . R3/R4 – CenterPoint Energy requests clarification on which Associated Physical Access Control Systems/Associated Electronic Access Control or Monitoring Systems are in scope. The Company proposes that the requirement applies to those systems associated with High Impact and Medium with External Routable Connectivity only. R3.2 – CenterPoint Energy proposes that the Standard Drafting Team consider combining 3.2 with 3.1. R4.2 – Under Measures, CenterPoint Energy recommends the wording "As described in Requirement 4.2" instead of "in accordance with this part."
R6 - CenterPoint Energy requests clarification on the term "stored". Is this term used to refer to electronic copies? R7.1 and R7.2 – Under Measures, CenterPoint Energy recommends changing the numbered list to bullets and replacing "and" with "or". R7.2 - CenterPoint Energy agrees with the comments submitted by EEI and NSRS that access for reassigned or transferred employees should not require revocation by the end of the next calendar day.
No
No
R1.1 - CenterPoint Energy recommends that the SDT add "with External Routable Connectivity" to the Medium Impact applicability as the Company believes that if there is no external connection, the risk is low. If a bad actor penetrates the Physical Security Perimeter, then the device login passwords are defense from unauthorized user access. R1.3 – CenterPoint Energy also recommends that the SDT add "with External Routable Connectivity" to the Medium Impact applicability for this requirement as the application of this control to a non-networked environment does not appear logical. R1.5 – It appears that the measures are focused on intrusion detection systems. CenterPoint Energy proposes that the SDT add "or other monitoring systems" after intrusion detection systems.
R2.1/2.2/2.3 - CenterPoint Energy also recommends that the SDT add "with External Routable Connectivity" to the Medium Impact applicability for this requirement as the requirements reference external remote access. CenterPoint Energy also agrees with the comments submitted by NSRS.
No
Yes
No
R1.1- CenterPoint Energy prefers the Draft 1 version of the measures for this requirement. ("Evidence may include, but is not limited to, documented operational or procedural controls exist and have been implemented.") R1.4 – CenterPoint Energy strongly disagrees with the 99.9% availability statistic introduced in this draft. CenterPoint Energy suggests that the SDT consider provisions for exceptions or manual monitoring and revise the percentage referenced. R1.5 – CenterPoint Energy requests clarification on the term "detected". R1.6 - CenterPoint Energy recommends that the measures be revised to read "access to the "Physical Access Control System". Additionally, CenterPoint proposes that the SDT combine 1.4, 1.5, 1.6, and 1.7. R1.8 – CenterPoint Energy has strong concerns regarding the manageability of this requirement. Attempting to apply this requirement to facilities in the field (i.e. substations) is onerous and adds little to actual security. The Company is concerned that some entities may need to make extensive and expensive changes to some of their facilities to comply. In addition, the Guidelines and Technical Basis states that FERC Order 706, paragraph 572 does not require two or more different and complementary physical access controls; therefore, CenterPoint Energy recommends deleting the requirement. If the SDT is determined to leave the requirement, CenterPoint Energy recommends deleting the Medium Impact applicability. Even with this reduced applicability, CenterPoint Energy recommends adding to the Measures "Video recording; Electronic capture of video images of sufficient quality to determine identity". CenterPoint Energy also generally agrees with the comments submitted by EEI and NSRS.
No
No
No
No

No
R1.1 - CenterPoint Energy requests that the SDT clarify "needed" and recommends replacing the term, “listening”, with enabled. R1.2 – CenterPoint Energy recommends that the SDT remove "signage" from the measures. The Physical Security Perimeter and logical disabling where possible should be sufficient to reasonably protect against unauthorized use. R2.1 – 2.4 – CenterPoint Energy agrees with the comments submitted by EEI in the proposal to add “with External Routable Connectivity” to the Medium Impact applicability. R3 - CenterPoint Energy proposes that the SDT add “with External Routable Connectivity” to the Medium Impact applicability as the requirement cannot be implemented in absence of remote access. R4.1 - CenterPoint Energy proposes that the SDT add “with External Routable Connectivity” to the Medium Impact applicability. CenterPoint Energy recommends adding “where the BES Cyber System is capable” after “Log events” since some legacy systems may not be capable of logging all the events specified in R4.1.1 – R2.1.4. CenterPoint Energy also recommends removing R4.1.4 because the term “malicious activity” is ambiguous and requires an analysis of intent. R4.3 – CenterPoint Energy recommends that the SDT add “after discovery” to the requirement.
R5.2 – CenterPoint Energy agrees with the comments submitted by EEI and recommends deleting this requirement. The requirement may be a problem during storm restoration or emergencies and ultimately, effect reliability. R5.5 – CenterPoint Energy recommends that the measure related to an attestation be deleted as it is not apparent what an attestation will provide that the policy/procedure will not. R5.6 – CenterPoint Energy recommends that the measure related to an attestation for this requirement be deleted and replaced with procedural documentation. CenterPoint Energy also generally agrees with the comments submitted by EEI and NSRS.
Individual
James Tucker
Deseret Power
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
No
Yes
R1.4 – The requirement for 99.9% availability for physical security perimeter controls is problematic due to requiring tracking of availability without defining a time period for determining the percentage. The SDT needs to revisit this requirement to reduce the complexity of tracking such availability and to create a clear requirement on this issue.
Yes
Yes
Yes
Yes
Yes

Group
Seattle City Light
Pawel Krupa
General comments: SCL does not support the approach proposed in version 5 of the CIP Standards, either as to fundamentals or details. Fundamentally SCL believes the v5 approach is flawed and will introduce significant compliance burden without ensuring cyber security for the BES. Detailed concerns remain as provided previously (please refer to comments submitted by SCL on January 6, 2012). Although today's enforcable CIP Standards share many of the flaws of v5, SCL believes industry would be better served by developing maturity around the existing Standards while developing a new, different approach to cyber security that is based on the established practices and theory of the information technology industry.
Group
Tri-State G&T - Transmission
Tracy Sliman
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Steve Alexanderson
Central Lincoln
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Thank you for removing low impact.
This does not relate to any of the requirements, but since no question was provided for Applicability, we are putting our comment here. We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
Yes
Yes
This does not relate to any of the requirements, but since no question was provided for Applicability, we are putting our comment here. We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
We’d still like to know where to find the “Secure Remote Access Reference Document” referenced in the Guidelines section under R2.
Yes
Yes
Yes
1. Thank you for removing low impact. 2. We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
Yes
Yes
Yes
Yes
Yes
This does not relate to any of the requirements, but since no question was provided for Applicability, we are putting our comment here. We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
Thank you for removing low impact.
Group
PacifiCorp
Sandra Shaffer
PacifiCorp support comments submitted by EEI.

Individual
Russell A. Noble
Cowlitz County PUD
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
John Tolo
Tucson Electirc Power
Yes
Yes
Yes
Yes
Yes
Yes
No
General comment: Agree with EEI's comments to insert "unescorted" into "authorized electronic" references. This allows the access needed for vendor support which was deemed not in the language of the standard in interpretation of CIP-004 for WECC
R7 – TEPC feels the timing should be based on the determination of when access is not necessary, rather than the date of the transfer. The SDT seemed to recognize that the reassignment date might not align with when access was no longer needed, and that a determination was needed. However they did not carry that through to the date of revocation. Suggested wording: For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the determination. TEPC also agrees with EEI's statement for R6.2: The individual(s) designated in Part 6.1 shall authorize unescorted physical access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances." To "The individual(s) designated in Part 6.1 shall authorize unescorted physical access into Physical Security Perimeter(s) that the

Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances.", in order to scope this requirement to the PSP.
Yes
No
R1.4 TEPC agrees with EEI's comment: This requirement is very similar to CIP-007-5 R5.1, with the exception of dial-up applicability. Propose adding BES Cyber Assets with dial-up connectivity used within High and Medium Impact facilities into CIP-007 R5.1, and removing R1.4 from CIP-005-5. This identifies all BES Cyber Assets that require authentication into a single requirement, resulting in a more concise standard. CIP-007 R5.1 already seems to require this, without the specific wording. This could result in double jeopardy.
Yes
Yes
Yes
Yes
No
Yes
No
No
TEPC agrees with the following EEI comments: for all sub-requirements limit scope to Medium Impact BES Cyber Systems with External Routable Connectivity instead of just Medium Impact. Without this change, the patching will apply to closed networks, greatly increasing resource requirements; and R2.2, change 30 to 35 calendar days to assist with monthly patch cycles and increase efficiency. TEPC feels for R4.1 that the TFE should be related to the logging, which takes place at the system level, rather than in 4.2 for the alerting; R4.2 – Remove the TFE from this requirement. TEPC also agrees with the EEI comments for R4.
TEPC agrees with EEI comments for R5. R5.1, R5.4: Change "Medium Impact BES Cyber Systems" to "Medium Impact BES Cyber Systems with External Routability or dial -up". Rationale: Consistency with CIP-004 R6.2; R5.2: Delete requirement since it's covered by CIP-004 R6.2; and R5.3: Delete requirement and move rationale to CIP-004 R5 since it's covered by CIP-004 R6;
Individual
Oscar Alvarez
Los Angeles Department of Water and Power
Yes
Yes
Yes
Yes
Yes
Yes
No
LADWP does not have extensive comments on this matter at this time.
The proposed time limits for revoking access upon terminations and transfers for the next calendar day present extreme challenges, especially when taking into consideration terminations or transfers that occur on Fridays. More time needs to be given. The next business day for terminations and 3 business days for transfers will make these processes manageable.
Yes
Yes
LADWP does not have extensive comments on this matter at this time.
LADWP does not have extensive comments on this matter at this time.
No

No
No
R1.1 defines operational or procedural controls to restrict physical access to Associated Systems. Need to remove applicability of this requirement for Associated Systems. Existing Standard Operating Procedures address and restrict physical access to Associated Systems. Demonstration of existing procedures should be sufficient to meet the intent of this requirement. R1.3 requires utilization of two or more different and complementary physical access controls. This presents technical challenges and may not create additional security. One control should suffice. Depth of defense already exists through gates, security personnel and card reader systems. The current requirement of one or more physical access methods has been implemented with little or no problems encountered. The increase to two or more physical access controls may bring about unintended consequences and complexity. NERC should provide compliance feedback to industry demonstrating that "one or more" physical access methods have proven ineffective. Additionally, High Impact Control Centers typically have stringent physical security controls and monitoring. R1.6 does not address access log retention. The preference is to maintain a log retention timeframe of ninety calendar days. A log retention timeframe of ninety days maintains the status quo. R3 requires maintenance and testing every 24 months. We prefer that the maintenance and testing cycle be no longer than three years. Equipment failure rates do not support the need for maintenance and testing every two years. Manufacturer mean time before failure rates are in excess of three years. We believe maintaining the three year cycle is reasonable and effective. Additionally, equipment is monitored and malfunctions are reported immediately, thus negating the need for a two year maintenance and testing cycle.
Yes
Yes
Yes
No
Yes
R4.3 requires that before the end of the next calendar day to activate a response to detected event logging failures. This presents a very short time frame to come up with a way to rectify an issue that may require extended investigation. Entities require more time to research and investigate logging failures to come up with a recommended response.
LADWP does not have extensive comments on this matter at this time.
Individual
Tony Kroskey
Brazos Electric Power Cooperative
No
No
No
No
No
Yes
No
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
No
No
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
We thank the SDT for improvements to the draft standard, however, we still believe there is room for

more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
No
Yes
Yes
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
Yes
Yes
Yes
Yes
Yes
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
Group
Puget Sound Energy, Inc.
Tom Flynn
Yes
Yes
Yes
Yes
Yes
Yes
No
In Requirement R1.1 in the phrase "…ongoing reinforcement of cyber security practices," the term "cyber" often is understood to mean computer or electronic. PSE recommends dropping the word "cyber" from the phrase in order to make clear that the requirement for a security awareness program would address both cyber and physical awareness topics. In the Measure for R1.1, the evidence required includes the "documented security awareness program." PSE feels that evidence of the distribution and materials associated with the quarterly reinforcement, and the audience of that material should be sufficient and that a documented awareness program is beyond what would be necessary to show compliance with the requirement. PSE recommends removing the requirement for the documented awareness program from the measures as required evidence. PSE views the granting of authorized electronic or authorized unescorted physical access as being dependent upon 1) the successful completion of a personnel risk assessment (PRA), 2) successful completion of appropriate training and 3) authorization from the owner of the asset for which access is being requested, the order of these 3 actions not being important. The Measures for R5.1 require that personnel risk assessments be completed before authorized electronic or authorized unescorted physical access is "authorized". PSE proposes that the wording in both bullet items in the Measure be changed from "access was authorized" to "access was granted". This would allow asset owners the ability to authorize access pending the successful completion of the PRA and/or training. This would also be more consistent with the wording in the requirement which indicates that the PRA must be performed prior to "granting" access.
1) In R6.4, PSE requests clarification around the intent of the requirement to track authorized access to the physical and electronic locations where BES Cyber System Information is stored. Is the requirement regarding physical location intended to include physical access to file servers hosting BES Cyber System Information in electronic format or is it intended to be limited to physical access to locations where BES Cyber System Information in stored in hardcopy format? 2) In R7.2, the

requirement is to revoke unnecessary access by the end of the next calendar day following a reassignment or transfer. As pointed out in the change rationale, the need for access may change over time. Often when an employee transfers there is a transition period where the employee may continue to require previous access to help support the old position. As currently written, there is no requirement to revoke the access if the determination of unnecessary access occurs after the next calendar day following the reassignment or transfer. PSE contends that a more effective control would result if the language of the requirement was changed to something similar to the following: "For reassignments, or transfers, review the individual's electronic and physical access and revoke any unnecessary access by the end of the next calendar day following the reassignment or transfer. Electronic and/or physical access required beyond that date is to be revoked by the end of the next calendar day following the determination that the access is no longer required." The Measures for this requirement should be updated accordingly. 3) In R7.3, similar to R6.4, clarification is needed regarding physical access to BES Cyber System Information. 4) In R7.5, PSE recommends changing "shared account(s)" to "BES Cyber System shared account(s)."
Yes
Yes
No
Yes
Yes
Comments: Recommendation to included cameras in the examples provided for "Locally mounted hardware or devices at the Physical Security Perimeter" because cameras tend to have the same characteristics as motion sensors, electronic lock control mechanisms, and badge readers. R1.6: The requirement states that the entity must have "controls that monitor each Physical Access Control System" but the measures reference documentation of controls that monitor the Physical Security Perimeter. PSE request clarity on whether the controls referenced in R1.6 are for the PACS or the PSP. R1.7: The requirement states that an alarm must be issued within 15 minutes of an unauthorized physical access being detected but the guidelines and technical basis state under methods to monitor physical access state that "…alarms must provide for immediate notification…" PSE suggests that the methods to monitor physical access to updated to reflect the 15 minutes defined in R1.7.
Yes
Yes
Yes
Yes
Yes
• Requirement 2, all sub-requirements: Applicable BES Cyber Systems and associated Cyber Assets - Change "Medium Impact BES Cyber Systems" to "Medium Impact BES Cyber Systems with External Routable Connectivity". Rationale: For non-externally routable or dialup systems the requirement, as currently written will create a large amount of compliance documentation without adding much security. • R1.1: Does the "where technically feasible" language imply that Technical Feasibility Exceptions (TFEs) are required when it is not technically feasible? • R2.1: Proposed - "A patch management program for tracking, evaluating, and installing cyber security patches and/or security updates for applicable Cyber Assets." • R2.2: Change 30 to 35 calendar days to assist with monthly patch cycles, increase efficiency, and align to other requirement's timeframe (ex: CIP-007, R3.3). • R3&4: Associated Protected Cyber Assets: Concern: The inclusion of this category in the requirements for Malicious Code Prevention and Security Event Monitoring implies that these requirements apply to every device in the category. This departs from the goal of applying these controls at the system level. Suggestion: Clarify that these requirements do not apply to all assets individually, by removing the category, or modifying the requirement. • R4.1: Add the term "where technically feasible" to the requirement language and specify that a TFE would be required in these circumstances. Rationale: Not all systems can support the logging requirements in 4.1.1-4.1.4. • R4.2.1: Change "detected malicious activity" to "detected cyber security event". Rationale: not all security events are malicious, which the standard utilizes R4.3 to make the determination if the cyber security event logged was

malicious in intent. • R4.3: Change “Activate a response to detected event…” to “Activate a response to human-detected event…”Rationale: the requirements do not distinguish between the logging of an event by a system and when that event is detected by a person. A person may not see the event at the same time it is generated by a system, so the requirement should be clarified to reflect that the deadline for a response be tied to human detection of the logged event. • R4.3: Change “next calendar day” to “next business day” to accommodate off-hour staff coverage. • R4.5: Applicability - Consolidate “High Impact BES Cyber Systems” and “Associated Protected Cyber Assets”, by changing the wording to “High Impact BES Cyber Systems with Associated Protected Cyber Assets”. Rationale: Clarifies that the logging reviews do not apply at the asset level. • R4.5: Change the wording to “Review a summarization or sampling of logged events, as deemed appropriate by the Responsible Entity, at a minimum…”. Rationale: It should be clear that the entity determines which logs should be reviewed or sampled, to avoid confusion during audits.
• R5.1, R5.4: Change “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routable Connectivity or dial –up connectivity”. Rationale: Consistency with CIP-004 R6.2 • R5.2: Delete requirement since it’s covered by CIP-004 R6.2 • R5.3: Delete requirement and move rationale to CIP-004 R5 since it’s covered by CIP-004 R6 • R5.4: Change the wording from “Change default passwords…” to “Change known default passwords…”. Rationale: Manufacturers sometimes use system passwords that are not known to the entities. • M5.4: Remove the language from the first bullet “…when new devices are deployed”. Rationale: Time frames are covered elsewhere in the Standards
Group
PNM Resources
Michael Mertz
Yes
No
No
No
Yes
No
No
See comment submission from EEI.
See comment submission from EEI.
No
No
See comment submission from EEI.
See comment submission from EEI.
No
No
No
See comment submission from EEI.
No
No
No
No
No
See comment submission from EEI.
See comment submission from EEI.
Individual
Martin Bauer
US Bureau of Reclamation
Yes

Yes
Yes
Yes
Yes
Yes
No
The 30 day revocation does not adequately prevent malicious use. To fully mitigate potential for harm, accounts should be revoked much sooner.
Yes
Yes
No
Yes
Yes
The two different physical access controls requirement would not allow the use of Pin and Card systems. The Pin and Card system is a Two Factor authentication. The Pin data is on the Card which makes it part of the same system. If the intent is to allow Two Factor authentication as described in the Guidelines and Technical Basis the language in the requirement must clearly state it. To reiterate Two Factor authentication is not same as two different physical access controls. The language in the requirement read "utilize (insert "a two factor authentication") or two or more different…. .
Yes
Yes
Yes
Yes
Yes
Individual
Scott Harris
Kansas City Power & Light
No
No
No
No
Yes
No
No
R1.1: According to the Guidelines and Technical Bases Section “the Responsible Entity is not required to provide records that show that each individual received or understood the information.” This is not clearly stated in the requirement. Suggested change: 1.1 A security awareness program that, at least once each calendar quarter, makes available ongoing reinforcement of cyber security practices to the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems. R2.1: An entities size will determine the necessity of multiple roles. For example, a company with 300 employees may require one role whereas a company with 30,000 employees will likely need several roles. This requirement should allow for these differences. Suggested Change: 2.1 Identify one or more roles. R2.2: According to the Rationale for R2, based on their role, some personnel may not require training on all topics; however, it is not stated in the Requirement. Also, according to the Guidelines and Technical Basis, training shall cover items appropriate to personnel roles and responsibilities. Suggested Change: 2.2 Cyber security training for

each role identified in 2.1 shall include one or more of the following topics appropriate to personnel responsibilities: R3.2: This requirement alone will dramatically increase time spent administering training because it requires staff to track numerous training dates as opposed to annual training dates. When combined with role-based training introduced in CIP-004-5, R2.1, it will require additional staff to manage. This places an undue burden on entities and Regional Entities. Suggested Change: 3.2 Require completion and documentation of the training specified in CIP-004-5, Requirement R2 once every calendar year. R4.2: Whereas Requirement 4.1 may slightly reduce the complexity and cost of background checks, this requirement complicates the task and will ultimately increase the cost of background checks as well as the amount of paperwork involved by forcing REs to document the reasons full seven year criminal history records checks were not performed. This task is unnecessary and adds little or no value to personnel risk assessment programs. I would suggest removing the second sentence in Requirement 4.2. Suggested Change: 4.2 Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six months or more: 4.2.1. resided; 4.2.2. been employed (if applicable); and 4.2.3. attended school (if applicable). R4.3 & 4.4: Examples of criteria in Requirement 4.3 & 4.4 or its Measures section are not provided. Suggested Change: Add criteria in Requirement or, at a minimum, add an “Evidence may include, but it not limited to:” section under its Measures to guide entities.
R6.5: The following statement in the Rationale for R6 on is not addressed in the Requirement or its Measures section: “If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement.” The inclusion of this statement in the Requirement in some manner would enable REs to find and fix this problem discovered during quarterly and annual audits rather than self-reporting them. Suggested Change: 6.5 Verify at least once each calendar quarter that individuals for which provisioning of authorized electronic access or authorized unescorted physical access in fact transpired have associated authorization records. R7 General: It is not clear that FERC’s order regarding “immediate” access removals be done that the requirements in versions 3 and 4 were found to be inadequate by FERC in addressing this concern. What was the motivation for the version 5 change in time frame from 7 calendar days to 1 calendar day? R7.1: In “Draft 1”, the SDT used the phrase “at the time” and in the Change Rationale section under Requirement 7.1 they stated that this requirement “specifies revocation concurrent with the termination instead of within 24 hours.” In “Draft 2”, the SDT allows the entity to initiate the process to revoke unescorted physical access and Interactive Remote Access upon the effective date and time of the termination action and complete the revocation within 24 hours after the effective date and time of the termination action. This is a significant improvement; however, in most circumstances still unrealistic. Suggested Change: 7.1 For all termination actions, initiate the process to revoke the individual’s unescorted physical access and Interactive Remote Access upon notification of the effective date and time of the termination action, and complete the revocation by the end of the next business day after the effective date and time of the termination action. R7.2: Although requiring revocation of access for reassignments and transfers “by the end of the next calendar day” is a more realistic time frame than the 24-hour time frame under Requirement 7.1, it gives entities little or no time to find and fix problems. Currently, entities have seven days to complete the process. Considering access revocation, especially in the case of transfers, is difficult and has many variables including the need for multiple supervisor approvals, limiting time to complete the process would dramatically increase the number of self-reports involving access revocation thereby creating an even more substantial paperwork nightmare for NERC. The SDT must reconsider the seven-day window allowed to revoke access under CIP-004-3, R4.2. Suggested Change: 7.2 For reassignments or transfers, revoke the individual’s electronic and physical access that the Responsible Entity determines is not necessary within seven days following the reassignment or transfer.
No
No
R1.1: Requirement statement seems to add to the scope of the applicability assets. Reword the requirements section. Current Applicable Statement: High Impact BES Cyber Systems Medium Impact BES Cyber Systems Suggested Applicable Statement: High Impact BES Cyber Systems and Associated Protected Cyber Assets with External Routable Connectivity Medium Impact BES Cyber Systems and Associated Protected Cyber Assets with External Routable Connectivity Current

Requirement Statement: All BES Cyber Assets and associated Protected Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP. Suggested Requirement Statement: Applicable Assets connected to a network via a routable protocol shall reside within a defined ESP. R1.3: Change the word “rational” to “reason”
Move examples cited into the measures for the three factors cited, leaving the requirement with the description of the factor. The measures would frame examples appropriate to each factor. The strike through wording needs to be moved to the measurements section. • Something the individual knows (including, but not limited to, passwords or PINs. User ID is not an authentication factor); • Something the individual has (including, but not limited to, tokens, digital certificates, or smart cards); or • Something the individual is (including, but not limited to, fingerprints, iris scans, or other biometric characteristic).
No
Yes
Yes
R1.3: This requirement requires more than one access control system that can uniquely identify a person for facilities in the High category. This requirement is will costly to implement and does not recognize defense in depth, or organizational and procedural controls that can be implemented in the temporary absence of a control. Recommend the following change to recognize the layering of defenses: Where technically feasible and for facilities with one layer of physical protection, utilize two or more different physical access controls to collectively allow physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access. R1.4: It is not clear that requirement R1.4 is for monitoring of the entry points into the Physical Security Perimeter (PSP) and not monitoring the equipment that monitors the entry points into the PSP. Recommend the following for clarity: Have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized access into a Physical Security Perimeter.
No
No
No
No
No
R1.1: Applicable BES Cyber Systems and associated Cyber Assets: Clarify how “Associated Protected Cyber Assets” is a modifier to the “High Impact BES Cyber Systems” and “Medium Impact BES Cyber Systems with External Routable Connectivity” rather than an independent set of assets. One option is to add “and Associated Protected Cyber Assets” to each of the High and Medium categories in this requirement. Additional clarification should also be available with respect to how ports are defined as “needed.” Suggested change: “For applicable Cyber Assets with logical network ports, enable only approved logical network accessible ports, including port ranges or services where needed to handle dynamic ports.” R1.2: This control is redundant and is covered through other physical security related requirements. All medium and high impact systems should already be protected. Signage is not going to be helpful in addition to the existing screening, escorting, barrier placement, physical access logging, and monitoring controls in place. R2.1: The measures should include better guidance as to what is considered to be an appropriate source of security patch information. Are entities able to use third parties for patch information instead of manufacturer-specific patch release information? R2.2: Change 30 to 35 calendar days to assist with monthly patch cycles and increase efficiency. R2.3: There is some confusion over the ability to revise an existing plan when new information comes to light. Recommend changing R2.3 to, “For applicable patches identified in Part 2.2, create a dated plan or revise an existing plan within 35 calendar days of the initial evaluation completion or identification of need to revise an existing plan. The plan shall include the Responsible Entity’s planned actions to mitigate the vulnerabilities exposed by each security patch and a timeframe to complete these mitigations.” R2.4: The current wording implies that the plan must be implemented within the timeframe specified in the original plan. Recommend change to, “Implement each plan created in Part 2.3, or a successfully revised version of the plan, within the timeframe specified in the plan, except for CIP Exceptional Circumstances.” R3: Associated Protected Cyber Assets: The inclusion of this category in the requirements for Malicious Code Prevention and Security Event Monitoring implies that these requirements apply to every device in the category. This departs from the goal of applying

these controls at the system level. Suggestion: Clarify that these requirements do not apply to all assets individually, by removing the category, or modifying the requirement. R3.3: Recommended that “with external routable protocol” be added to the applicable section. R4.1.4: Remove 4.1.4 – it will be difficult to detect and log for unspecified malicious activity and impossible to prove we are logging malicious activity if we do not have any malicious activity. R4.2: The sub-requirements imply that entities will be required to constantly prove the negative with regard to malicious activity. There are many ways of detecting malicious activity or the failure of a logging activity, and some of them cannot be automated to allow for alerting in a manner that would satisfy the requirement. Recommend, “Generate alerts for security events that the Responsible Entity determines necessitate a real-time alert.” R4.3: This will require Entities to make increased financial and manpower investments in efforts to be compliant. One calendar day is unrealistic and unattainable in most circumstances. Change next calendar day to next business day, “Activate a response to alerts generated in compliance with R4.2 by the end of the next business day.” In the Measures: Change “attestation” to “documentation” for clarity. R4.4: Applicability is confusing because the requirement states “BES Cyber System” which does not include these associated systems. Remove the three “Associated…” systems/assets from the applicability section. R4.5: Applicability is confusing and suggest change to requirement for clarification, “Review a sample of logged events at a minimum every two weeks to confirm that logs are being generated as expected.” Consolidate “High Impact BES Cyber Systems” and “Associated Protected Cyber Assets”, by changing the wording to “High Impact BES Cyber Systems with Associated Protected Cyber Assets” Remove “Associated Physical Access Control Systems” and “Associated Electronic Access Control or Monitoring Systems”
R5.4: Clarify that default passwords that are unchanged will require changing according to R5.6. R5.5: Attestations in the measures section should be removed. R5.6: Add where technically feasible or “unless the BES will be negatively impacted” verbiage to the end of the requirement. R5.7: Current language implies that generating alerts for unsuccessful login attempts is not a method of “limiting the number of unsuccessful authentication attempts.” This could be interpreted to mean that a TFE should be generated when an entity has established a failed login alerting threshold but not implemented other means to limit unsuccessful attempts. The end result would require entities to fill out quite a bit of paperwork to account for all of the TFEs. A description of “alerting” or other methods for “limiting” the number of attempts can be placed in the measures. Recommend, “Limit the number of unsuccessful authentication attempts after a threshold of unsuccessful login attempts, or document other means by which the number of unsuccessful authentication attempts can be minimized.”
Individual
Darcy O'Connell
California ISO
No
No
No
Yes
Yes
No
No
CIP-004-5 R1 M1. Change “but not limited to” to “but is not limited to” CIP-004-5 R2 - Remove “role-based cyber security training” to training based or tailored to job function. Role-based seems that it is inferring that training should be based on permissions or that access should be role based. R2.1 - Change “identification of each role” to “identification of roles” required for BES cyber access. Consider removing R2.10, it is difficult to determine the intention of this requirement. It does not add anything that is not covered in 2.2 through 2.9. CIP-004-5 R3 - Remove “role-based cyber security training” to training based or tailored to job function. Role-based seems that it is inferring that training should be based on permissions or that access should be role based.
CIP-004-5 R6 Part 6.6 - Remove Measure “2. A summary description of privileges associated with each group or role;“ CIP-004 R6 – Part 6.1 – 6.1.3 states “access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity.” The wording should be cleaned up for physical location. i.e. a janitor has access to a data center therefore he has physical access to BES Cyber System Information because the data is stored on a SAN in the data

center. CIP-004-5 R7 - R7.2 For reassignments and transfers suggest changing the duration from one calendar day to 30 calendar days as is prescribed for terminations in Parts7.4 and 7.5. A termination is a higher risk vs. a transfer.
No
The Measures in Part 1.7 are prescribing an Intrusion Detection System however such system is not prescribed in a requirement. The references to an IDS should be removed. Other systems and tools can be used to detect malicious communication other than an IDS. Requiring encryption in CIP-005 R2 Part 2.2 will not allow an IDS to detect malicious communication. Especially if ssh is used between the intermediate device and the cyber asset.
No
No
Yes
CIP-006 R1 – Parts 1.4 and 1.6 change “Have controls” to “Have control(s)” Parts 1.5 and 1.7 remove reference to “BES Cyber Security Incident Response Plan” since this is a Physical Incident and not cyber. Part 1.5 Revert to the wording that was in the previous draft of CIP Version 5. CIP-006 R2 - Measure in Part 2.2 appears to be a copy and paste error. Suggest revisiting Measure 2.2 as it does not align with the requirement.
No
Yes
No
No
No
CIP-007 R1 R1.2 Suggest replacing the requirement with a requirement for the Responsible Entity to implement a policy regarding the use of physical ports. CIP-007-5 R3 - Part 3.1 strike the word “deter” in the requirement. Not sure how you deter malicious code. Part 3.2 Measures should be limited to response actions for detection malicious code. Remove bullets 2 and 3 for the measures. Part 3.3 The sentence structure for the requirement is awkward. Please reword the requirement for easier read. CIP-007-5 R4 - R3 and R4 one states malicious code and the other says malicious software. Suggest changing to malicious code for consistency. Part 4.1.4 suggest removing this part. Otherwise, define what is malicious activity. This is subject to interpretation. Malicious activity requires analysis and is not something that can be logged. Part 4.2.1 suggest removing this part. Otherwise, define what is malicious activity. This is subject to interpretation. Malicious activity requires analysis and is not something that can be logged. Part 4.2 remove “real-time”. Is real-time when the event is received by a tool or when the event occurred on a cyber asset. Some events may only be processed by a tool on a daily basis (batch). Part 4.3 standardize with CIP-006 R1.6 in regards to availability and keeping records for outages. Is the requirement in regards to the security monitoring logging capability or in regards to a cyber asset not logging? Part 4.5 should only pertain to where automated processes and alerting are not possible.
Part 5.1 remove the word “all” or be specific to scope. Define what is meant by “user access”. Provide better examples for measures in order to provide guidance for intention of the requirement. Reword requirement to “Enforce authentication of interactive user access to Applicable BES Cyber Systems and associated Cyber Assets, where technically feasible.” or change to require authentication of accounts. Part 5.2 suggest rewording to “The CIP Senior Manager or delegate(s) must authorize enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). “ Part 5.3 for the measure reword to “Evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.” Part 5.4 reword to “Change default passwords, where technically feasible, unless the default password is unique to the Cyber Asset.” Part 5.5.1 reword to “Password length that is, at least, eight characters or the maximum length supported by the Cyber Asset; and” Part 5.5.2 reword to “Minimum password complexity that is at least three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.” Part 5.5 Remove Measure around attestations. Additionally, some organizations are dependent on unions that will not allow for attestations by union members. Add measure that states “Documentation of the registered entity’s procedural solution and training

program to educate its affected personnel on its procedural solution." Part 5.6 Remove Measure around attestations. Additionally, some organizations are dependent on unions that will not allow for attestations by union members. Add measure that states "Documentation of the registered entity's procedural solution and training program to educate its affected personnel on its procedural solution." Part 5.7 reword to "Where technically feasible, limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful login attempts." Should there be a recommended minimum for both?
Group
BC Hydro
Patricia Robertson
Yes
No
Yes
No
Yes
Yes
No
1) Requirement R2.5: question - is the Registered Entity expected to track the names of all individuals who have undertaken training related to the visitor control program? If yes, what evidence will need to be provided that this training was completed? 2) Requirement 4.3: "Process or criteria used to evaluate personnel risk assessments to determine when to deny authorized access". Access decisions will be based on a case-by-case basis and on the facts surrounding each; as such, defining such a process that will be adhered to each and every time may be difficult to define. Recommend changing the word "process" to "guideline"
Requirement 7: for conditions where access is to be revoked by "next calendar day" it is requested that this time period be restated to "next business day" to account for weekends and statutory holidays; the time period in which to revoke access would also be based on risk
Yes
Yes
No
No
Yes
1) Requirement 1.4: I agree with the Registered Entity looking to achieve high availability (HA) for physical access control (systems) but 99.9 % seems excessive; it is unclear as to how the Registered Entity is expected to evidence the 99.9% HA; there will be legitimate scenarios, such as patching the OS, where it may be difficult to meet the 99.9% HA as there are scenarios where the system is down very briefly for maintenance, such brief time periods where the system may be down, for example a reboot to allow installation of patches (what is there are a large number of patches to be installed throughout the year?).2) Requirement 1.7: for clarification, an alarm is required to be generated within 15 minutes resulting to a potential PSP breach, not the response. It is not always possible to initiate a response for remote unmanned sites where someone can be on site within 15 minutes, it may take hours, to investigate a potential PSP breach 3) Requirement 1.9: clarification is required that only the most recent 90 days of logs need to be retained by the Registered Entity as opposed to being required to demonstrate that for any day within the audit period 90 days of data was retained. 4) Requirement 2.3: clarification is required that only the most recent 90 days of visitor logs need to be retained by the Registered Entity as opposed to being required to demonstrate that for any day within the audit period that 90 days of data was retained.
Yes
Yes
Yes
Yes

Yes
Group
Hydro One
Sasa Maljukan
No
No
Yes
No
Yes
Yes
No
Recomend removing word “potential” from R2 part 2.7 since an incident is determined to be real or potential only during the follow up investigation R4, part 4.2 it pelase include wording to state that PRA should include all bulleted items (4.2.1 through 4.2.3) to avoid confusion. Privious version of R4 part 4.3 had exclussion for laws or collective barganing agreements. Pelase add the exclussion or explain why the exclussions were dropped.
No
No
Recommend removing “, but is not limited to, ” from R1 Part 1.1 since the Measure’s scope already includes all of the possible Cyber Assets We understand that Measures should not dictate Requirements. If correct, then how can CIP- 005 R1 Part 1.5’s Measure specify “intrusion detection system” when the Requirement does not specify a technology. Also specifying a technology may prevent a newer, better technology from being used until the Standard is updated. Recommend changing R1 Part 1.5 from “intrusion detection system” to “detection system” Request for clarification on how the math for R1 is done in the VRF/VSLs
Request clarification on R2 Part 2.1 – can the Intermediate Device can be on the ESP? In other words, can the Intermediate Device also be an EAP? Recommend changing R2 Part 2.3 from “Factors must be at least two of the three following categories” to “Multi-factor include, but are not limited to” which allows future technology without a Standards update
No
Yes
No
Recommend changing the testing in R3 Part 3.1 so that the High Impact BES Cyber Systems are tested every 24 months and Medium Impact BES Cyber Systems with External Routable Connectivity are test every 36 months
Yes
No
No
No
No
For R2, request clarification if the SDT’s intent is that the following timeline will be compliant or not? 1) on 5/1/2012 the patch is identified; 2) by 6/1/2012 complete the assessment for applicability (30 days); 3) by 7/1/2012 the plan is developed and defined for testing plus implementation (30 days); 4) per the plan, testing completed by 9/1/2012; 5) per the plan, patch deployed by 10/12/2012; 6) on 10/30/2012 patch fails (through no fault of testing); 7) emergency patch back out on 11/1/2012; 8) per plan, develop mitigation plan by 12/1/2012 (30 days); 9) per original plan, mitigation testing completed by 2/1/2013; and 10) per original plan, mitigation patch deployed on 3/12/2013 Recommend changing R3 Part 3.3 so that Medium Impact remote locations with no external connectivity (isolated networks) have more than 35 days Suggest changing R4 Rational from “(1)

immediate detection" to "(1) real time detection" to be consistent with Part 4.2 Request clarification on R4 Part 4.1.1. The CIP Standards expect "deny by default" firewall rule which results in dropping offending packets such that there is nothing to log. How can the Registered Entity meet Part 4.1.1 criteria of logging failed access attempts at the EAP? Recommend removing "malicious" from R4 Part 4.1.4 since "malicious" is determined after the fact and Parts 4.1.1, 4.1.2 and 4.1.3 capture the events that may be malicious • R4.5 – Bi-weekly manual reviews of sampling of logged events –what is considered a "sampling of logged events"? Is this a percentage of logs received (on average)? Who make the determination that an appropriate number of logs have been reviewed ? how will auditor determine that a manual review had been completed? What is the ultimate value of a manual review? For R1 as written, recommend that missing one port is too high since the PSP is the first layer of defense. Missing one physical port should not be a Severe VSL. Recommend this is a Low VSL. Recommend increasing percentages from Low – Moderate – High – Severe Recommend that the number of assets should be another differentiator for R3's Low – Moderate – High – Severe Recommend that the difference between R4's Low – Medium – High – Severe should be number of assets with two weeks throughout Recommend that R4 should start with a Low VSL and use the number of assets combined with the number of accounts as a difference between Low – Medium – High - Severe
Request clarification on R5 Part 5.7. Does the technical feasibility apply to both "the number of unsuccessful authentication attempts" and "generate alerts after a threshold of unsuccessful login attempts" or only the "authentication attempts?"

Name (60 Responses)
Organization (60 Responses)
Group Name (36 Responses)
Lead Contact (36 Responses)
Question 1 (86 Responses)
Question 2 (86 Responses)
Question 3 (85 Responses)
Question 4 (0 Responses)
Question 4 Comments (96 Responses)
Question 5 (87 Responses)
Question 6 (86 Responses)
Question 7 (86 Responses)
Question 7 Comments (96 Responses)
Question 8 (0 Responses)
Question 8 Comments (96 Responses)
Question 9 (85 Responses)
Question 10 (87 Responses)
Question 11 (86 Responses)
Question 12 (0 Responses)
Question 12 Comments (96 Responses)
Question 13 (87 Responses)
Question 14 (86 Responses)
Question 15 (0 Responses)
Question 15 Comments (96 Responses)

Individual
David Proebstel
Clallam County PUD No.1
Yes
Yes
Yes
No comment
Yes
Yes
Yes
no comment
no comment
Yes
Yes
Yes
no comment
Yes
Yes
no comment
Group
Northeast Power Coordinating Council
Guy Zito
No
No
No
Request clarification on the EOP-004-2 reference in the R1 Rational. The previous version of EOP-004-2 was not accepted by the industry. What is the plan if future versions of EOP-004-2 are not

accepted? Recommend changing the first bullet in R2 Part 2.1 from “By responding to an actual Reportable Cyber Security Incident; ” to “By responding to a Cyber Security Incident” since this covers the Reportable Incidents plus the non-reportable incidents Recommend updating R2 Part 2.3 since the existing language does specify a retention period. Recommend changing R3 Part 3.1 from “Review and update” to “Review and update, as needed,” since some years the Cyber Security Incident response plan will not need updating Recommend changing R3 Part 3.3 from “Update the Cyber Security Incident response plan ” to “Update, as needed, the Cyber Security Incident response plan”. For R1.3, and R1.4 wording needs to be added to state that physical security incidents need to be included as well as for Cyber Security Incidents.
No
No
No
Recommend removing R1 Part 1.5 since this Requirement is forensics and/or Lessons Learned. The priority is Reliability or recovery, forensics. The title of this Standard is Recovery Plans for BES Cyber Systems. Request clarification on R2 Part 2.2. Is this a media test? Can the test be on a sample BES Cyber System? Recommend updating the Measure for R2 Part 2.3 to reference an updated Implementation Plan’s Initial Performance of Certain Period Requirements. This Requirement – Part combination is not identified in the existing Periodic Requirements. As requested in the first posting, request removing these bookends from this Measure Recommend changing from the reference from “R1.2” to “Part 1.2” in R3 Part 3.4 for correctness.
No
No
No
Request clarification of R1 Part 1.1.2. Does “applications” mean “SCADA, EMS, State Estimator, IDC, etc.” instead of “device drivers, DLL, applications included in an operating system or package, etc.?” Request clarification of R1 Part 1.1.3. Would a version control tool/system (like CVS) demonstrate the custom software’s version? Request clarification on R1 Part 1.3. Each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005 and CIP-007? In R1 Part 1.3, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations. Recommend removing the 30 day time frame in R1 Part 1.3 that applies to CIP-005 and/or CIP-007. Those Standards should specify their time frames. Recommend that the 30 days apply to only updating the baseline configuration (this Part). Request clarification on R1 Part 1.4.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? In R1 Part 1.4.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations. Recommend removing R1 Part 1.4.2 because “availability” has not been part of the Requirements in the past, is not a FERC requirement and can be interpreted multiple ways. In R1 Part 1.5, recommend changing from “Where technically feasible, for each change that deviates from the existing baseline configuration ” to “Testing cyber security control, where technically feasible, for each change that deviates from the existing baseline configuration” for clarity. For R2 Part 2.1, recommend the previous Version 5 words since this updated Part is not understandable. Request clarification on R3 Part 3.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? In R3 Part 3.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations. Recommend that R3 Part 3.1start with its purpose – for example, Active vulnerability assessment. Request clarification on R3 Part 3.2. If this is a paper exercise it should be performed once every 36 months. Recommend that R3 Part 3.2 start with its purpose – for example, “Perform active vulnerability assessment, where technically feasibly….”. Recommend that R3 Part 3.3 start with “Perform an active vulnerability assessment, of the new cyber assets prior to business deployment, except for CIP Exceptional Circumstances and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset).” Recommend updating CIP-010 R1’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures shows R1 as “low”. Recommend updating CIP-010 R2’s Violation Risk Factor in the Table of Compliance Elements. That

VRF is “medium” while the Requirements and Measures shows R2 as “low”.
Yes
No
The second paragraphs of R2 Parts 2.1 and 2.2 are the same. Recommend removing them from Parts 2.1 and 2.2, and make a into a new Part 2.3 for clarity.
Individual
Frank Dessuit
NIPSCO
No
Yes
Yes
NERC should clarify why the word “dated” has been added to the measures used throughout this requirement. NERC should clarify the use of “reliability tasks” in this proposed standard, specifically, whether they are the same “reliability tasks” as required by PER-005. NERC should provide clarification on the terms “Cyber Security Incident” and “Reportable Cyber Security Incident”.
No
Yes
Yes
NERC should provide a definition of the term “recovery,” and whether it is meant to apply to disaster recovery / business continuity focusing on recovery of functionality or capability of a system, or to restoration after an individual asset loss, or both.
Yes
Yes
Yes
R1 indicates a process for a change occurring. NERC should clarify if R2 identifies an undocumented change, would a self report be required, or is the “document and investigate” language of R2 intended to eliminate the need for self reports to R1? NERC should also clarify whether all VAs must be performed prior to the CIP V 5 effective date, and whether entities have an additional year or 3 years from the effective date.
Yes
Yes
Individual
Thomas C. Duffy
Central Hudson Gas & Electric Corporation
Yes
Yes
Yes
No
Yes
Yes
Requirements 1.1, 1.2, 1.3 and 1.5: The applicable 'systems and assets' for these requirements should be changed from 'Medium Impact BES Cyber Systems' to 'Medium Impact BES Cyber Systems at Control Centers' to agree with the rest of the requirements of the standard. All the requirements should apply and they should apply only to Control Center assets.
No
No

No
This standard should not be applicable to all 'Medium Impact BES Cyber Systems'. It should be applicable to only 'Medium Impact BES Cyber Systems at Control Centers' and 'Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity'.
Yes
Yes
Individual
Michael Falvo
Independent Electricity System Operator
Yes
Yes
Yes
No
No
Yes
CIP-009-5 R1, Part 1.3: – IESO suggests the change of word “recover” to “restore” outlined within the requirement. CIP-009-5 R1, Part 1.4: IESO suggests the change of word “recovery” to “restoration” outlined within the requirement. We also suggest that the following terms should be defined: recover recovery, restore and restoration. CIP-009-5 R2 - Part 2.2: IESO believes the usage of “backup media” is antiquated and most entities use redundancy for restoration. The use of redundancy for restoration should be referenced, or the backup media should be defined to include the new technologies.
No
No
No
CIP-010-1 R1 - Part 1.4.1: An entity could face double jeopardy in that non compliance with this requirement means non-compliance with the requirements in the referenced standards. CIP-010-1 R1 - Part 1.5.1: The “where technically feasible” clause is not applicable here; therefore, IESO is recommending the removal of this clause from this requirement. CIP-010-1 R2 - Part 2.1: Unless the term “continuously” is defined, IESO recommends the removal of this word from the requirement.
Yes
No
CIP-011-1 R2 - Part 2.1: IESO recommends that the requirements outlined here should be broken out into two separate sections: one for cyber assets that contains BES Cyber System Information (i.e. network diagram) and the other pertaining to Cyber Assets within an ESP.
Group
Comment Development SME list
Gerald S. Freese
Yes
Yes
Yes
Yes
Yes
Yes
1. R1.3- In the requirement, the word “recover” is used to refer to functionality of a BES Cyber System in a backup and storage regimen. Recommend rewording the requirement to “to restore BES

Cyber System." 2. R1.4: Compliance with R2 should be sufficient. It is very difficult to demonstrate initial verification of this information after the backup. Compliance with R2 should adequately test this process. AEP recommends merging this with R2. 3. R1.5- Preservation efforts may impede the recovery process and reduce reliability as BES Cyber Systems are out of service for an extended period of time while the data is preserved. This seems like a “nice to have” but could be an unnecessary distraction during a stressful time where SMEs should be focused on recovery. Worse still, this could cause double jeopardy with CIP-008. AEP recommends moving this to CIP-008, or making this a guideline. 4. R2.2- This requires that information used in the recovery of BES Cyber Systems stored on backup media be tested once each calendar year. There are no boundaries set on the extent of data required to be tested. Recommend wording in the measures that clarifies that a sampling of information is sufficient.
Yes
Yes
Yes
1. R1.1 While we acknowledge the removal of the term "script" from the requirement, we feel that there should be some clarification of what "custom software" means. We would recommend that the wording be changed to "Any custom application software developed for the entity." 2. R1.1: Could recording software “hashes” be used as an alternative to recording version levels to verify that no unauthorized changes have been made to software on the BES Cyber Asset? AEP recommends this be added to the measures or guidance for this requirement. 3. R1.1.4 should be applicable to systems with external routable connectivity only. 4. R1.1.3: The requirement is not clear in how to determine boundaries on software installed on BES Cyber Assets. Are individual “applications” subject to this? Which “utility applications” are subject to this? Is the version “product level” or “executable level”? Recommend that this requirement at least be addressed in guidance to ensure that “custom software” is neither over or under assessed to meet the requirement. 5. R1.1.4: Please define or provide guidance on “logical network accessible ports”? 6. R1.2: In the measures, "Documentation that the change was performed in accordance with the requirement." To what is the term requirement referring? Recommend removing this item from the measure. 7. R1.3: Using other standards references in the requirement is misleading, time consuming and not in keeping with the intent of a concise security standard. Recommend more use of examples without the reference to the standard numbers. 8. R1.4.1: Remove standards references from the requirement. Provide examples and perhaps add the references to the measures as the source of the data. 9. R3.3: AEP recommends the measure say “of any tools used to perform the assessment” or something similar, since “tools” may not be used in this active vulnerability assessment. 10. R3.4: If security controls tested in the assessment are found to be deficient, would that not be a violation of the CIP standards requirement for that security control? That would require a self report. Could the self report mitigation plan be used as the action plan for 3.4? 11. CIP-010 R1: CIP-007 R1.1 requires a Responsible Entity “..enable only logical network accessible ports…” if they have a High Impact BES Cyber System or Medium Impact BES Cyber System with External Routable Connectivity. For consistency, the applicability of CIP-010 R1 should be changed to High and Medium Impact BES Cyber System with External Routable Connectivity or item 1.1.4 should be removed. (2) R3.1 the specific security controls requirements from CIP-005, CIP-006, and CIP-007 that must be assessed should be defined.
Yes
Yes
Group
Southwest Power Pool Regional Entity
Emily Pennel
Yes
No
No
(1) The CIP-008 requirements should also be applicable to related EACMS and PACS systems. (2) Part 2.1 permits a paper drill, tabletop exercise, or full operational exercise. Such activity must include a reportable incident scenario. (3) Part 2.1 should require a periodic full operational exercise in the absence of a live, Reportable Cyber Security Incident. Otherwise, Responsible Entities will continue to

only perform a weak tabletop exercise of limited value. (4) Part 2.2 assumes that null deviations need to be documented as well. The requirement language should clearly state that expectation to remove any ambiguity of the expectations placed upon the Responsible Entity. (5) The requirement for lessons learned in Part 3.2 should stipulate that null lessons learned be documented if there were no lessons learned. (6) The High and Severe VSLs for Requirement R3 presumes there must have been lessons learned. The VSLs need to provide for documented occasions where no lessons learned were developed. (7) The guidelines for Part 1.2 defined a Reportable Cyber Security Incident as a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. This definition is too vague and could result in a complete compromise and failure of a BES Cyber Asset not being considered due to available redundant systems being available. (8) The guidelines for R3 properly states that it is possible to have a BES Reportable Cyber Security Incident without any documented lessons learned. The guidance should advise the reader that a null document is still required to demonstrate that an after action review was conducted and no lessons learned were developed.

No

No

No

(1) Part 1.1 needs to define a minimum set of conditions that would require activation of a recovery plan. Otherwise, entities are free to raise the bar to any height, such as only activating the recovery plan in the event of a catastrophic loss of the facility housing the BES Cyber Assets. (2) Requirement R1 needs to make clear that recovery plans for BES Cyber Systems need to contain the necessary steps for restoring the BES Cyber System to a state where it is ready to assume its normal operating role in all respects. The recovery plan is not the same as a Continuity of Operations plan as required by EOP-008. (3) The suggested evidence for Part 1.3 should include documented configuration settings, documented build/restoration procedures, and retention of installation media. (4) The requirement of Part 1.4 is vague and needs clarification. Does verification simply mean a catalog of the backup media demonstrating that the media can be successfully read? Does it mean a comparison of the data recorded on the media against the data that was backed up? Or does it mean a test restoration? (5) Part 2,2 needs to clarify what is meant by the requirement to ensure the information is useable and “is compatible with current system configurations.” (6) Part 2.2 needs to clarify that a test of the information requires either recovery from an actual incident or an operational exercise, either option requiring a system restoration. A tabletop exercise should not be permitted as it will not achieve the intent of the requirement. (7) Requirement R1 needs to clarify the expected level of detail or granularity in the recovery plans. Otherwise, a very generic plan could result in a simple recovery of a minor workstation using a plan also applicable to a complicated SCADA server. (8) The requirement for lessons learned in Part 3.1 should stipulate that null lessons learned be documented if there were no lessons learned. (9) The moderate VSL for Requirement R1 should apply when the recovery plans do not address “one” (not “all”) of the referenced requirements. (10) The High and Severe VSLs for Requirement R3 presumes there must have been lessons learned. The VSLs need to provide for documented occasions where no lessons learned were developed.

No

No

No

(1) Part 1.1.2 should clarify how granular the version identifier should be. Is only the major release level sufficient? Or is minor release level documentation expected? (2) Part 1.1.2 should exclude the anti-malware signature file version identifiers due to the volatility of frequent updates. (3) Part 1.4.1 is likely to result in the Responsible Entity declaring that no Cyber Security Controls are expected to change and thus no testing is required. The purpose of testing is to verify nothing unexpectedly changed and the requirement needs to make that expectation clear. (4) Does Part 1.5.2 permit the documentation of a stand-alone test environment with identified differences from the production environment? Or must the test environment and differences be documented with each change package? (5) Is the assessment required by Part 3.2 in lieu of or in addition to the assessment required by Part 3.1 in the calendar year the Part 3.2 assessment is conducted? (6) Part 3.3 should also apply to Physical Access Control Systems. (7) The High VSL for R1 should apply when the Responsible Entity failed to authorize “one or more” (not “any”) baseline configuration changes. (8)

The phrase “and to document those changes” in the first condition of the High VSL for R1 should be deleted as it is duplicative of the second condition. (9) A VSL condition needs to be defined for R2 for a missed periodicity. (10) The last condition of the Severe VSL for R3 only triggers if all three required elements are missing (due to the use of “and”). A lesser VSL needs to be defined for missing one or two of the three required elements, or the Severe VSL needs to change the “and” to “or.” (11) In the guidance for R3, the passive network discovery should be a review of network connectivity to identify Electronic Access Points. A discovery process cannot presume all access points have already been identified. (12) In the guidance for R3, the passive vulnerability review should include a predecessor step to review the security and configuration policies for the referenced items. Then the review of the actual controls should be conducted to confirm they continue to conform to the policies. (13) In the guidance for R3, the active network discovery should include a physical inspection for those devices that are either incapable of or are configured to not respond to traditional active discovery tools.
No
No
(1) The “methods to identify BES Cyber System Information” requirement in Part 1.1 is vague. Is the required method to determine what information should be considered protected (information characteristic) or is the required method to document that the information is protected (labeling)? (2) The exception found in the first paragraph of Part 2.1 makes no sense and needs to be clarified or stricken. (3) What does “who has possession” mean in the second paragraph of Part 2.1 and in the second paragraph of Part 2.2? Is this an individual? Or would a way bill for a shipment sent by commercial courier be sufficient, even no hand-to-hand chain of custody is maintained? (4) It is not clear if Parts 2.1 and 2.2 permit media to be removed and possibly replaced with clean media, with the Cyber Asset then being redeployed or disposed of while the removed media continues to be maintained until separate erasure or destruction. Parts 2.1 and 2.2 need to track the media and not necessarily the Cyber Asset the media is associated with.
Individual
Thomas A Foreman
Lower Colorado River Authority
Yes
Yes
Yes
Yes
Yes
Yes
No
Yes
Yes
In R1, section 1.1.5 indicates a need for baselining security patches. Section 1.3 requires updating documentation of changes to the baseline within 30 days of changes. This would require updating baseline documentation any time security patches are applied. We would recommend striking security patches from this documentation requirement to streamline security updates.
Yes
Yes
Individual
Glen Sutton
ATCO Electric
Yes
Yes

Yes
Yes
Yes
Yes
Yes
No
Yes
Comment: R2.1 change configuration monitoring presents a significant amount of effort to implement. Specifically the 35 day window does not allow for much flexibility when attempting to perform a manual monthly check of baselines. Additionally, it may not be technically feasible to implement automated baseline monitoring tools within non-standard IT environments where a significant amount of devices and custom applications cannot be monitored with off the shelf products. Consider increasing the 35 day window to 60 or 90 days to provide more flexibility in performing manual baseline comparisons.
Yes
Yes
Individual
Martyn Turner
LCRA Transmission Serivces Corporation
Yes
Yes
Yes
Yes
Yes
Yes
No
Yes
Yes
In R1, section 1.1.5 indicates a need for baselining security patches. Section 1.3 requires updating documentation of changes to the baseline within 30 days of changes. This would require updating baseline documentation any time security patches are applied. We would recommend striking security patches from this documentation requirement to streamline security updates.
Yes
Yes
Group
Duke Energy
Greg Rowland
No
No
No
(1) Requirement R1.1. “Processes” should be rewritten as “Process(es)” to allow entities flexibility to combine all elements of R1.1 into a single process if they so choose. (2) Requirement R1.4. Duke

recommends removing this requirement in its entirety. Incident handling is assumed to be contained within requirement CIP-008 R1.1 to “respond” to Cyber Security Incidents. (3) Requirement R1.5. Duke recommends that the drafting team coordinate this requirement with the EOP drafting team. This requirement appears to be duplicative to one that appears in EOP-004-2 that could create a spot of double jeopardy in the case of non-compliance. Duke recommends that this requirement only appear in 1 place and suggests that any Cyber Security related requirement should appear only in the CIP standards. (4) Requirement R2.1. Duke recommends that the requirement be rewritten to say, “Test the response plan(s) per CIP-008 R1, at least once every…”. The current term “BES Cyber Security Incident response plan” is not a defined term and cannot be assumed to be the ones referenced in R1. (5) Requirement R2.1. Duke asks that the drafting team clarify how many of the response plans, if there are multiple, need to be tested on an annual basis. If the entity creates a dozen response plans, is it the intent of the drafting team that each response plan be tested? Or is testing one response plan per entity sufficient? Would there be justification in testing a sampling of the response plans with a minimum of one? Duke requests that the drafting team provide more clarity. (6) Measure R2.1. Duke recommends striking the reference to “lessons-learned” as they are not specifically required under the requirement. (7) Requirement R2.2. The current language, “Use the incident response plan under Requirement R1” incorrectly assumes that the entity only has 1 response plan developed, when the requirement allows for the development of multiple plans. Duke suggests rewording this to allow for the entity to “Use the applicable incident response plan under Requirement R1”. (8) Requirement R2.3. Duke recommends that the drafting team coordinate this requirement with the EOP drafting team. This requirement appears to be duplicative to one that appears in EOP-004-2 that could create a spot of double jeopardy in the case of non-compliance. Duke recommends that this requirement only appear in 1 place and suggests that any Cyber Security related requirement should appear only in the CIP standards. (9) Requirement R3.2. Duke recommends rewording this requirement as follows, “Document any lessons learned associated with a Cyber Security Incident test, per R2.1, or actual incident response to a Reportable Cyber Security Incident, per R2.2, within 30 calendar days after completion of the test or actual incident response.”. The insertion of requirement references adds clarity to what is to be documented. (10) Requirement R3.4. Duke suggests striking this requirement in its entirety. The current wording is overly burdensome and would require an update to the plan any time a staffing change occurs. Duke feels that this can be accomplished in the periodic testing of the plan and any updates can be made at that time.

No

No

No

(1) Measure R1.3. Duke recommends that the term “successfully” be striken from the measures section. Duke does not agree with the assumption that merely having the information for recovery available will guarantee successfully recovery of the Cyber Asset. (2) Requirement R1.4. The requirement here to verify backup media “initially after backup” is confusing. This incorrectly assumes that the entity is responsible for creating all backups to backup media. The requirement does not account for the possibility that an OEM may create a backup months or years before delivery of the product that the entity would have no means of testing “initially”. Duke requests that the drafting team reword this requirement to only require backup verification when the entity creates the backup. (3) Requirement 1.5. Duke requests that this requirement be reviewed by the drafting team. The current language assumes a cyber event has triggered activation of the recovery plan and therefore the preserving of forensic evidence would be critical. However, the recovery plan may be invoked due to “normal” equipment failure or another type of event in which preserving data/forensic evidence would be unnecessary. Duke suggests that the preservation of data only be required if the recovery plan is triggered due to a Cyber Security incident response plan in CIP-008. (4) Requirement R2.1. Duke asks that the drafting team clarify how many of the recovery plans, if there are multiple, need to be tested on an annual basis. If the entity creates a dozen recovery plans, is it the intent of the drafting team that each recovery plan be tested? Or is testing one recovery plan per entity sufficient? Would there be justification in testing a sampling of the recovery plans with a minimum of one? Duke requests that the drafting team provide more clarity. (5) Requirement R2.2. Duke recommends striking the phrase, “to ensure that the information is useable and is compatible with current system configurations”. Duke believes this information is unnecessarily prescriptive and the requirement

should allow the entity the flexibility to use reasonable judgment as to what the test needs to cover. (6) Requirement R3.3. Duke suggests striking this requirement in its entirety. The current wording is overly burdensome and would require an update to the plan any time a staffing change occurs. Duke feels that this can be accomplished in the periodic testing of the plan and any updates can be made at that time. (7) Requirement R3.4. Duke is concerned with the current wording of this requirement. There doesn't seem to be consideration that multiple recovery plans may exist within a single entity. If there are, the requirement is unclear in which plans must be sent to which individuals. The requirement could be misinterpreted to read that any time a single plan changes, all individuals identified in R1.2 must be made aware of the change, even if they are not associated with that specific plan. Duke recommends that the drafting team add additional clarity to the requirement to account for the possibility of multiple plans.
No
No
No
(1) Requirement R1.1. Duke disagrees with the wording of the requirement to apply to "each Cyber Asset indentified, individually or by group" as this is inconsistent with the language in CIP-002 that allows Cyber Assets to be grouped in the beginning of the process into Cyber Systems. Once grouped as a Cyber System, that is how they should be referred to in the remainder of the standards and CIP-010 R1.1 should only apply to applicable Cyber Systems where the requirement may be met at the system level as opposed to the individual Cyber Asset level. (2) Requirement R1.1.1. Duke recommends that the word "exists" be replaced with "is installed". This clarifies that the entity does not have to consider any operating system that could be installed on a Cyber System but may not currently be installed. (3) Requirement R1.1.2. Duke recommends that the word "intentionally" be removed from the requirement. Duke feels that this word is too subjective and could be a compliance issue when one has to demonstrate intent. (4) Requirements R1.1.4 and R1.1.5. Duke is concerned that these requirements are redundant/conflicting with requirements in CIP-007 requiring the entity to manage ports and a patch management program. Duke recommends that requirements related to these controls only appear in one area in the standard and recommend that they be removed from CIP-007 and remain solely within CIP-010. (5) Measure R1.2. Duke recommends that the parenthetical, "performed by the individual or group with the authority to authorize the change" be stricken from the measures section. Duke believes this is unnecessarily prescriptive and doesn't match the requirement as there is no requirement as to who is allowed to make the change. (6) Requirement R1.4.1. Duke recommends removing this sub-sub-requirement in its entirety. Duke does not see the value in determining the controls that could be impacted prior to the change and see the requirement in R1.4.2 as the important step in the process, regardless of what was expected to happen. (7) Requirement R1.4.2. Duke recommends that the drafting team clarify what is meant by "required controls". When referencing entire standards, is it the drafting team's intent that every requirement be re-verified, like a self-audit, when a change is made? Duke requests that instead of using a vague term such as "required controls" that language be inserted to point to specific requirements that must be verified per this requirement. (8) Requirement R1.5.1. Duke recommends that the drafting team clarify what is meant by "required cyber security controls". This language doesn't exactly match that in R1.5, and it is confusing for the entity to determine exactly what should be tested. Duke requests that instead of using a vague term such as "required cyber security controls" that language be inserted to point to specific requirements that must be tested per this requirement. (9) Requirement R1.5.2. Duke believes that the following language should be removed from the sub-sub-requirement, "including a description of the measures used to account for any differences in operation between the test and production environments". Duke does not understand the intent of requiring this type of documentation as it provides no security benefit and only invites auditors to unnecessarily critique the methods that the entity determines are appropriate to address the differences between the two environments. (10) Requirement R2.1. Duke recommends that the term "continuously" be removed from the requirement. Duke feels that "periodically" captures the intent of an adequate timeframe. There is no reason an entity couldn't employ a continuous monitoring process to go above-and-beyond the standard but the requirement should only spell out the minimum needed to address compliance. (11) Measure R2.1. The current measure says investigation would be needed for any "unauthorized changes" while the requirement calls for monitoring of all changes. Duke suggests that the word unauthorized be added to the requirement such that monitoring is only necessary for unauthorized changes. (12) Requirement R3.1. Duke

recommends that the drafting team clarify what is meant by “cyber security controls”. This language is confusing for the entity to determine exactly what should be tested. Duke requests that instead of using a vague term such as “cyber security controls” that language be inserted to point to specific requirements that must be tested per this requirement. If there is a desire for the drafting team to allow flexibility for the entity to determine what to include in its vulnerability assessment, then all prescriptions should be removed and the language of the requirement could be ended after the words “vulnerability assessment”. (13) Measure R3.1. Duke believes the last phrase in the first bulleted item needs to be removed, “and the individuals who performed the assessment”. This does not align with the requirement and does not provide any value to meeting compliance. (14) Measure R3.1. Duke believes the last phrase in the second bulleted item needs to be removed, “and the output of the tools used to perform the assessment” as this is covered by R3.4 and is not part of the requirement R3.1. (15) Requirement R3.2. Duke believes that the following language should be removed from the requirement, “including a description of the measures used to account for any differences in operation between the test and production environments”. Duke does not understand the intent of requiring this type of documentation as it provides no security benefit and only invites auditors to unnecessarily critique the methods that the entity determines are appropriate to address the differences between the two environments. (16) Measure R3.2. Duke believes that the phrase, “the output of the tools used to perform the assessment” should be removed. This is covered by R3.4 and is not part of the requirement R3.2. (17) Requirement R3.3. Duke is confused by the reference in this requirement to a new Cyber Asset. If a new Cyber Asset is part of an existing Cyber System, then is this requirement applicable? Duke feels that the direction made in CIP-002 should hold true here and a vulnerability assessment would only be required for new Cyber Systems (or those other systems/assets within the applicability section). (18) Requirement R3.3. Duke is confused when there is specific language as to the content of the vulnerability assessment in other sub-requirements of R3 and not within R3.3. Duke recommends that consistency be used and language like that seen in R3.1 be removed to be consistent with the other sub-requirements. (19) Measure R3.3. Duke believes that the phrase, “the output of the tools used to perform the assessment” should be removed. This is covered by R3.3 and is not part of the requirement R3.2. (20) Requirement R3.4. This requirement says to “document the results of the assessments”. Duke is confused as to which assessments require result documentation. Is it the intent that this be all assessments in R3? If so, Duke asks that clarity be added to the requirement to address exactly what needs to be documented here. (21) Requirement R3.4. Duke is concerned with the phrase “remediate or mitigate vulnerabilities identified in the assessments”. Duke has seen regions address this phrase differently and it is not generally understood what the drafting team intends with this statement. Is the intent that identified vulnerabilities do not constitute violations of the requirements that they are found against? If so, Duke requests that the drafting team clearly identify what discovery of vulnerabilities mean and how they are to be addressed in terms of compliance with the other requirements/standards.
No
No
(1) Requirements R1.1 and R1.2. The phrase “and implemented” needs to be removed as it is redundant to the main requirement R1 requiring implementation of the sub-requirements. (2) Requirement R1.2. Duke recommends removing the phrase “including storage, transit, and use” as this is unnecessarily prescriptive. Duke believes the entity should have the flexibility to define their own information protection program and what elements it needs to include based on what is or is not allowed within its own organization. For example, an entity may not authorize transit and therefore requiring a handling process to cover transit would be meaningless. (3) Requirement R1.3. Duke is concerned with the phrase “implement an action plan to remediate deficiencies identified during the assessment”. Duke has seen regions address this phrase differently and it is not generally understood what the drafting team intends with this statement. Is the intent that identified deficiencies do not constitute violations of the requirements that they are found against? If so, Duke requests that the drafting team clearly identify what discovery of deficiencies mean and how they are to be addressed in terms of compliance with the other requirements/standards. (4) Requirement R2.1. Duke recommends rewording the second paragraph of the requirement to the following, “If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information, the responsibility entity shall maintain a chain of custody process, which addresses the control of the device while it is outside of a Physical Security Perimeter”. The suggested language change is to demonstrate that the entity may not

always maintain possession of the device and as long as it follows the process, it is meeting compliance with the requirement. (5) Requirement R2.2. Duke recommends rewording the second paragraph of the requirement to the following, “If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsibility entity shall maintain a chain of custody process, which addresses the control of the device while it is outside of a Physical Security Perimeter”. The suggested language change is to demonstrate that the entity may not always maintain possession of the device and as long as it follows the process, it is meeting compliance with the requirement.
Individual
Mario Lajoie
Hydro-Quebec TransEnergie
Yes
Yes
Yes
(1) We approve CIP-008 but we support requests clarification follow by NPCC TFIST
Yes
Yes
Yes
(1) We support the comments follow by NPCC TFIST about request clarification
No
No
No
(1) We support comments follow by NPCC TFIST (2)R1.4 :We believe that 1.4 should only apply to Medium impact BES cyber systems with external routable"
Yes
Yes
Group
NRG Energy Companies
Alan Johnson
Yes
Yes
No
1. Requirement R3.2 requires documentation of lessons learned within 30 calendar days after completion of test or actual incident response. This may not allow enough time to complete the investigation and determine appropriate lessons learned. Suggest a change to 60 calendar days. 2. The 30-day timing requirement in CIP-008-5 R3.4 should be extended to 60 calendar days such that the overall timing for the activities in CIP-008-5 R3 is more reasonable. This would allow for a consistent 90-day timeline for planned changes as well as responses to Cyber Security Incidents. 3. Requirement R3.3 implies that the Cyber Security Incident Response plan must be updated based on any documented lessons learned. However, lessons learned may not impact any change in the plan but relate to execution of the plan and performance of the personnel in that execution. This should be reworded to include “as applicable”. 4. Requirement R3.5 – Table 3- identifies possible evidence that can be used to communicate updates of the plan. These suggested media reflects a poor choice of vehicles to communicate these updates to affected personnel due to the confidentiality of the material.
No
Yes
No
Requirement R3.4 – Table 3- identifies possible evidence that can be used to communicate updates of

the plan. These suggested media reflects a poor choice of vehicles to communicate these updates to affected personnel due to the confidentiality of the material.
In Requirement R3.3, 30 days should be extended to 60 calendar days to make the overall timing for the activities in R3 more reasonable. This would allow for a consistent 90-day timeline for planned changes as well as lessons learned from the use/testing of the recovery plan.
No
No
No
1. Revise Requirement R1.3 from a 30 day timeline to 90 days (or removed) to allow for sufficient time to process/document the required changes and verifications. The 35-day timeline in Requirement R2.1 should be extended to 90 days to allow for a quarterly review process. 2. The applicability of CIP-010-1 R3.1 and R3.4 should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity or Dial-up Connectivity.” This modification would eliminate existing discrepancies between the applicability of CIP-005, CIP-006, and CIP-007 and the applicability of CIP-010. This modification also supports the proposed applicability of CIP-005-5 and CIP-007-5 such that the vulnerability assessments are directed towards cyber systems with connectivity. Oncor 3. In requirement R3, please clarify whether an external vendor needs to perform the annual Vulnerability Assessment or can the Responsible Entity perform the task reviewed by its Internal Audit group. 4. Additionally R1.4.1 and R3 specifies that CIP-006-5 controls need to be included in the Vulnerability Assessment. As this is a substantial change from the prior definition of CVA, can guidance be provided for this assessment?
No
Yes
Individual
Jianmei Chai
Consumers Energy Company
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
R3.1 & R3.3 - The Requirement to perform Vulnerability testing and documentation for Medium Impact cyber assets outside of a control center should be deleted. In a field environment, where individual assets may number in the hundreds, and where the potential impact is typically much less, the effort is not only problematic but has the potential to reduce, not improve reliability. R3.3 & R3.4 - Why R3.3 does not include Medium Impact BES Cyber Systems while R3.4 does. Until the bright-line criteria have been assessed against the company assets, it is difficult to determine the impact this will have on Medium Impact BES Cyber Systems.
Yes
Yes
R2.2 – Please clarify “chain of custody”.
Individual
Kayleigh Wilkerson
Lincoln Electric System

Yes
Yes
Yes
No
No
Yes
No
No
No
[R1] Outside of PCs and protective relays, LES does not believe there is a need to collect the information in CIP-010 R1. This Requirement should only apply to a subset of cyber assets like PCs and protective relays.
Yes
Yes
[R1.1] Recommend striking the first bullet in the Measures or changing it to indicate that a label of “confidential” is sufficient. The current measure is phrased such that it requires information to be labeled as CIP information, instead of just confidential. This increases the chances that someone will know how to use it maliciously if they do get unauthorized access to it. Suggest legacy verbiage indicating a classification in alignment with “confidential.” The current verbiage did not prevent organizations from assigning a “CIP Confidential” label to documentation or preclude a protection program that had only one level of protected information.
Individual
Joe Petaski
Manitoba Hydro
In R2.1, it is unclear what makes an operational exercise to be deemed as “full”. We suggest changing “with a full operational exercise” to “with an operational exercise”.
R2.1: The “chain of custody” documentation is too onerous for many situations (including moving cyber assets from one PSP room to another!). we suggest rewording: “Or alternatively, the responsible entity shall have procedural controls to ensure the BES Cyber System Information remains at all times in the possession of personnel who are authorized for access to the BES Cyber System Information.”
Individual
Michael Schiavone
Niagara Mohawk (dba National Grid)
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Group
Arizona Public Service Company
Janet Smith
Yes
Yes
Yes
Yes
Yes
No
AZPS recommends that the table 1.4 Requirements should read "Verify that backups of information essential to recovery complete successfully."
AZPS recommends changing the word “Distribute” in the table 3.4 Requirement to “Communicate”. AZPS believe the plans are CIP Confidential Information that may be best communicated via a link to the updated plan to ensure only those with authorization are able to access the document.
Yes
Yes
Yes
Yes
Yes
Individual
Michael Jones
National Grid
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Jonathan Appelbaum

The united illuminating Company
Yes
Yes
Yes
UI concurs with EEi Consensus comments.In a addition, for R 2 we are concerned with plural in plan(s). A Registered Entity may have one plan that explains response to different types of incidents. It should be clear that only one Test of the plan is required, as opposed to testing every incident response tree.
Yes
Yes
Yes
UI agrees with EEI consensus comments
UI agrees with EEI consensus comments
No
No
No
UI agrees with EEI consensus comments
Yes
No
UI agrees with EEI consensus comments
Individual
Alice Ireland
Xcel Energy
No
Yes
Yes
Regarding CIP-008-5 R1: Regarding the definition of reportable cyber security incident: CIP-008-5 R1 points to EOP-004-2 for the definition of a reportable cyber security incident. EOP-004-2 points back to CIP-008-5 for the reporting criteria. The reference to EOP-004-2 seems unnecessary. The CIP v5 definitions define a reporting cyber security incident as, “Any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.” This definition is much broader than the definition of cyber security incident. “Reliability tasks” is undefined as is “compromised or disrupted.”
Yes
Yes
No
We suggest that R3.2, 3.3, and 3.4 be deleted and R3.1 replaced with the following language: “For any required change to the recovery plan (due to deficiencies or lessons learned from recovery plan tests or actual incident recoveries, or changes in roles, responsibilities, or technology), update the recovery plan and distribute updates to each individual responsible under R1.2 within 60 calendar days.”
Yes
Yes
Yes
No
No
1) R1.1 introduces less flexibility by implying that we need to have a classification (or at least labeling scheme) for ‘BES Cyber Systems Information’ rather than allowing us to classify and handle the same way we classify and handle other types of corporate information. Recommend removing from

Evidence the reference to labeling. 2) R1.2 there is no definition of ‘use’ of information. How is that different from access (which is handled in a different standard), labeling (covered in R1.1), and release to authorized others (covered in ‘transit’ and access). Recommend removing the word ‘use’ from the requirement. 3) R2.2 is unclear if scope is the storage media within the Cyber Asset (2.1) or if it also includes backup media. It just says storage media which can mean many things. Please clarify. 4) R2.2 please clarify ‘chain of custody’ documentation requirements. Is that simply the name of the person and the start/end time of possession. 5) R2.1 redeployment/reuse and 2.2 disposal are very similar in language, consider consolidating into a single requirement.
Individual
John Souza
Turlock Irrigation District
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Chris Higgins on behalf of BPA CIP Team
Bonneville Power Administration
Yes
Yes
Yes
Yes
No
Yes
Regarding R2.2 which states: “Test information used in the recovery of BES Cyber Systems that is stored on backup media at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and is compatible with current system configurations”. BPA believes this requirement could be interpreted to mean that the entity is required to recover the data to a functionally equivalent system and operate the system to determine whether the data is usable or not. In the security and IT industry, it is understood that the purpose of testing backups is to determine whether the data that you thought you backed up was actually backed up, and is recoverable from the media. First, when the data is initially stored on the backup media, it is verified to ensure successful backup. Later, when the backup is tested, it is typically accomplished by reading the data on the backup media to determine if the media is still readable. It is BPA’s interpretation that the new standard as written appears to compel entities to perform operational testing on a functionally equivalent system to validate the usability of the data rather than performing a restoration to validate the viability of the data. BPA recommends the following rewrite to clarify that the intent of the requirement is to validate the viability of the backup media: “Test Backup Media containing information used in the recovery of BES Cyber Systems at least once each calendar year,

not to exceed 15 calendar months between tests, to ensure that the information is usable and is compatible with current system configurations". Regarding Table R2.2 Measures: BPA believes the language of the Measures should be revised to align with the language that was removed from the requirement. BPA recommends: "Evidence may include and is not limited to, dated evidence of a test of information used in the recovery of a BES Cyber System that is stored on backup media at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is usable and is compatible with current system configurations: Regarding R2.2, BPA believes the entity needs to test the backup media and the Measures in Table 2 need to reflect the same language.
Yes
No
Yes
While BPA agrees with the goal in R2.1 of automated monitoring of baseline configuration changes, BPA believes a 35 day requirement is far too aggressive to accomplish on some Cyber Assets where automated monitoring is not possible and given the large number of devices BPA has that will need to be manually monitored for changes. For these cyber assets, BPA suggests an annual review period is more feasible as it will be in line with normal periodic maintenance cycles. As discussed in the Guidelines, for some cyber assets it is not technically possible to implement automated monitoring due to the capabilities of the device. For other cyber assets, while it may be technically possible to monitor, the inability to integrate with a centralized automatic monitoring system (e.g. Tripwire) without significant system and/or network changes is problematic. This will likely expose the cyber asset to additional cyber security risks if added to a primary network just for monitoring purposes, hence reducing overall security and reliability. For cyber assets such as a terminal servers used for SCADA RTU serial communication, the risk of inadvertent or unauthorized changes is minimized by other compensating measures, including and not limited to, isolation on small private networks. Even if manual monitoring is acceptable in this situation, it has the potential to introduce additional risk of inadvertent accidental changes due to an increase in frequency of human interaction with the device that will need to be completed to perform the required monitoring. Additionally, the explanation provided in the Guidelines for this requirement about the acceptability of using a manual process is not clear regarding when technical feasibility exception will be allowed. BPA believes the explanation needs to be clarified. An example would be very helpful. Suggested Changes: BPA would like to see this requirement implemented for devices that can accomplish it automatically. All devices that cannot implement this requirement automatically should be allowed a technical feasibility exception. The proposed change to requirement 2.1 is as follows: Where technically feasible, automatically monitor changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1), and document and investigate detected unauthorized changes. BPA agrees with the intent of the CIP-010 guidelines and can vote vote yes on the standard should the drafting team address BPA's concerns regarding requirement 2.1. For BPA to have an affirmative position for this standard, CIP-010 R2.2 language needs to be revised to the following: "Where technically feasible, automatically monitor changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1), and document and investigate detected unauthorized changes". If the SDT does not agree with the removal of manual, periodic monitoring, than at a minimum, BPA suggests extending the monitoring period of 35 calendar days to annual monitoring.
Yes
Yes
Individual
Benjamin Beberness
Snohomish County PUD
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
Yes
CIP-011-1 R1 The draft CIP versions 5 Reliability Standards are very BES definition centric. Due to the proposed changes to the BES definition it is very difficult for the electric industry to comment on a standard as it is unclear if the currently or proposed BES definition will be applied. This change in the definition could significantly change the applicability of the version CIP Reliability Standards. Although it is clear the SDT has made attempts to size the applicability of the CIP version 5 requirements with the size of the registered entity, the current draft will cause significant resource burdens on facilities that have demonstrated they cannot impact the reliability of the Bulk Electric System. As a Transmission Dependent Utility SNPD supports a reliable system because we are at the end of the system and SNPD's customers are exposed to all disturbances on the main grid. However SNPD also support efficiency and spending significant resources with little to benefit is not beneficial to the reliability of the BES or to the Level of Service ("LOS") SNPD provides its customers.
Group
PPL Corporation NERC Registered Affiliates
Stephen Berger
Yes
Yes
No
1.) PPL Affiliates appreciate all the value-added work the SDT has provided on the CIP Version 5 project. PPL Affiliates would like the SDT to consider changing CIP-008 R3.2 to include language for consistency with the ERO Event Analysis Process. • PPL Affiliates submit for consideration the following language... 'Document any lessons learned associated with a Cyber Security Incident test incident response within 30 calendar days after completion of the test incident response. Document any lessons learned associate with an actual Reportable Cyber Security Incident per the ERO Event Analysis Process Appendix E when the Cyber Security Incident results in an event on Appendix E. If the Cyber Security Incident did not result in an ERO Event Analysis per Appendix E, the lessons learned shall be performed within 30 calendar days.' • PPL Affiliates believe that the consistency of reporting requirements for the lessons learned eases the training and compliance requirements without any adverse impact on reliability
No
Yes
No
R3.1/R3.2: Requirement to document lessons learned and update recovery plans accordingly within 30 days, though feasible following an exercise, would likely be too prescriptive following an actual recovery. This is due to the time required to effectively evaluate the circumstances and response to an actual recovery (especially a major event). 90 days or longer would be more appropriate in such an instance.
R1.4: It seems that "…verified initially after backup…" is confusing to many. If the intent is to run a verification pass on the backup media to assure that this matches the source (an automated function with most backup software), then this should be made clearer. If the intent is simply to verify a successful backup occurred (as per the Measures), then this should be made clear.
Yes
Yes
Yes

Yes
Yes
Individual
Larry Watt
Lakeland Electric
Yes
No
No
"Please see comments submitted by FMPA through the formal comment process."
No
Yes
Yes
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
Yes
Yes
Yes
"Please see comments submitted by FMPA through the formal comment process."
Yes
Yes
"Please see comments submitted by FMPA through the formal comment process."
Individual
Ron Donahey
Tampa Electric Company
No
No
No
Tampa Electric is in support of the comments from EEI for CIP-008-5
No
No
No
Tampa Electric is in support of the comments from EEI for CIP-009-5 R3
Tampa Electric is in support of the comments from EEI for CIP-009-5
No
No
No
Tampa Electric suggests that it is not clear if this means a vulnerability assessment is required for every cyber asset or a sampling of cyber assets. As this relates to relays, it seems like once a set of cyber security controls are in place and tested to be adequate then a review of those controls at a single location would be adequate if the same controls are used everywhere. As more equipment gets pulled into scope doing annual reviews such as required here will become increasingly onerous. For R1.2, Tampa Electric recommends that applicability be changed to High Impact BES Cyber Systems only. In addition, there is ambiguity in the phrase “Documentation that the change was performed in accordance with the requirement.” For R1.3, Tampa Electric suggests 90-calendar days due to outside vendor responses needed. For R1.4, Tampa Electric suggests that the legacy CIP-007 R1 language should be used. We also request clarification on R1.4.2: What is considered BES Cyber System “availability” – if one component has an issue is that the entire system? Should availability read “reliability”? For R 2.1, Tampa Electric suggests the SDT modify requirements language to be more consistent with updated R1, which is to get rid of the baseline language. Please provide clarification

on what is considered the “record of investigation?” Also, if no change is detected during a monitoring period, how does an entity demonstrate “no change”? For R3.1, Tampa Electric recommends that the SDT add “externally routable” to Medium Impact, Associated Protected Cyber Assets. We would also like clarification for the following question: Does this requirement mean each system individually has to be assessed or does grouping of the same technology qualify?
Yes
No
Tampa Electric agrees with the comments submitted by EEI. In addition, we note that the Rationale for R1 is incomplete, stopping in mid-sentence. For CIP-011-1 R2.1, Tampa Electric would like to raise a concern related to hardware failures for systems where the entity is under contract with a third party company that owns the hardware and software. If the failed equipment must be returned to that company under the terms of the contract, there appears to be no way to destroy the information. For restoration of functionality, it may not be under the entity’s direct control to be able to track and document all hand-offs of equipment to restore service. For CIP-011-1 R2.2, Tampa Electric suggests the same concern raised in R2.1. In addition, outsourcing arrangements may prevent the documentation of all hand-offs of information and tracking that information through disposal.
Individual
David R. Rivera
New York Power Authority
No
No
No
NYPA agrees with NPCC comments
No
No
No
In R1 Part 1.5, the reference to forensics should not be part of the CIP-009 Standard.
No
No
NYPA agrees with NPCC comments, plus - NYPA would like to emphasize the suggestion of returning to the Draft 1 text.
Yes
No
NYPA agrees with NPCC comments.
Individual
Annette Johnston
MidAmerican Energy Company
No
No
No
(1) CIP-008 APPLICABILITIES: Add the qualifier “with External Routable Connectivity” to all of the medium impact BES Cyber System applicability listings in CIP-008, to ensure consistency between the standards. Some requirements of other standards (CIP-005, -006, -007) that “feed into” CIP-008 include this qualifier. For example, CIP-006 does not require monitoring for dial-up BES Cyber Systems, so it would be difficult for dial-up systems to meet the CIP-008 requirements. (2) CIP-008 GUIDELINES: We recommend references to the DHS and NIST documents be deleted, since NERC does not track those documents to determine if they remain consistent with the NERC standards. It would be more appropriate to include references to NERC documents, such as the Security Guideline: Threat and Incident Reporting, if NERC plans to continue to maintain this document. (3) CIP-008 R1 REQUIREMENT: (a) R1.1: No comments. (b) R1.2: MidAmerican Energy has provided comments on the definition of Reportable Cyber Security Incident to eliminate the term “reliability tasks,” since this

term is not defined or explained. While the SDT notes in the consideration of comments that they are continuing to coordinate with Project 2009-01, we still believe that CIP-008-5 should be written to “stand on its own” in the event CIP version 5 becomes effective before EOP-004-2. CIP-008-3 required a process for reporting to ES-ISAC. We propose revising R1.2 to ensure CIP-008-5 includes processes to report. Proposed text: “Processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and to report.” (c) R1.3: No comments. (d) R1.4: No comments. (e) R1.5: No comments. (4) CIP-008 R2 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. See rationale in comment form D question 17 and comment form A question 4 comments 12, 16, 17 and 18. (b) R2.1: ANNUAL: Revise “at least once each calendar year, not to exceed 15 calendar months between executions,” to “once each calendar year or a period not to exceed 15 calendar months between executions.” Rationale: see comment form D question 17. (c) R2.2: Delete this part, since the R2 statement above the table already states the entity “shall implement the plan” (use the plan). In addition, the statement “Document deviations from the plan” is duplicative of R3.2, which requires documentation of lessons learned. During an actual incident, there may not be time to document deviations “during the response.” These deviations might be documented after the response, but they would be covered in R3.2 as lessons learned. (d) R2.3: Delete this part, since evidence retention is already covered in C.1.2. If this is retained, the word “relevant” should be deleted. (5) CIP-008 R2 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (6) CIP-008 R3 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (b) R3.1: This requirement is duplicative with R2.1 and presents double jeopardy. R3.1 should be deleted. (c) R3.2-R3.5: In its CIP-008 consideration of comments, the SDT quoted paragraphs from Order 706 that were not CIP-008 directives (P651-CIP-007; P728-CIP-009; P731-CIP-009). The only FERC directive for CIP-008 was paragraph 686, which directed revisions to address lessons learned. While we support making timely updates to the Cyber Security Incident response plan, we believe R3.1-R3.5 has significantly increased the documentation burden associated with CIP-008 requirements due to the tracking of multiple dates. In paragraph 731, FERC stated “We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective.” We believe that updates to plans are not effectively in place until it has been communicated, and that it will be more efficient for entities to track one date rather than four date requirements included in draft 2. We propose consolidation of R3.2-R3.5 into one part to ensure lessons learned, updates to the plan and communications are completed within the 90 days achieves FERC 706 but is less prescriptive and less of a documentation burden. Examples of changes that would require updates to the plan in R3.4 can be moved to guidelines. Following is proposed text: R3.1: “Update the Cyber Security Incident response plan(s) and communicate the updates within 90 calendar days of a test, actual recovery or changes that impact the ability to execute the plan. Updates from tests or actual recovery shall include lessons learned.” (d) R3 MEASURES: With the consolidated R3.1 requirement, the following is proposed for measures: “Examples: 1) revised response plan(s) that include dated references to lessons learned from tests, actual recovery or changes that impact the ability to execute the plan; 2) dated emails, newsletters, training or other communications regarding the plan updates.” CIP-008 R3 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention.
No
No
No
(1) CIP-009 R1 REQUIREMENT: (a) R1.1: No comments. (b) R1.2: No comments. (c) R1.3: Change

“BES Cyber System” to “applicable Cyber Assets” in the requirement, since it applies to more than just BES Cyber Systems. FERC 706 had two different directives in paragraphs 739 and 748, which are listed in the change description with CIP-009 R1.4. We think paragraph 748 would be better addressed by adding a phrase to R1.3. The directive is to have procedures to ensure verification that backups are successful. Since R1.3 is to have processes, we think the following revised text would address paragraph 748: “One or more processes for the backup and storage of information required to recover applicable Cyber Asset functionality. Processes should include verification that backups are successful and backup failures are addressed so that backups are available for future use.” (d) R1.4: By addressing Order 706, paragraph 748 in R1.3, we think R1.4 should be revised to be focused on paragraphs 732-739. We do not support the draft 2 text that includes the term “initially,” since this would be a significant administrative burden that goes beyond the FERC directive. In paragraph 739, FERC directs the ERO to incorporate guidance, so we think the directive could be met with guidance. However, we would support the new requirement if the scope is revised to better reflect the directive in these paragraphs. In paragraph 739, FERC refers to “significant changes made to the operational control system.” FERC did not express concern about Physical Access Control Systems or Electronic Access Control or Monitoring Systems. We suggest these be deleted from the applicability. We propose the following revised text to better reflect FERC’s concern with significant changes: “Information essential to BES Cyber System recovery that is stored on backup media shall be verified after a significant change to the hardware or software to ensure that the backup process completed successfully.” We suggest a 90 day evidence retention on this new requirement. R1.4 is not listed in the implementation plan. With our revised text, it would not need to be included in the implementation plan. (e) R1.5: While we think draft 2 has addressed some of our concerns with draft 1, changes made to the definition of CIP Exceptional Circumstance introduce some new issues. In most cases when the recovery plan is invoked, there will be a hardware, software or equipment failure. The revised definition of CIP Exceptional Circumstance includes “an imminent or existing hardware, software, or equipment failure.” Under draft 2, CIP-009 R1.5 would never be required because of the addition of CIP Exceptional Circumstances to R1.5 and the addition of hardware, software or equipment failures to the definition. We propose the following text that would eliminate this issue but still meet the FERC directive in paragraph 706: “Processes to preserve data necessary to determine the cause of a BES Cyber Incident that triggers activation of the recovery plan(s), within capabilities of the device or operational requirements. Data preservation should not impede or restrict system restoration.” Limit the applicability for this new requirement to high impact BES Cyber Systems and medium impact BES Cyber Systems at control centers. (2) CIP-009 R1 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower. (3) CIP-009 R2 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (b) R2.1: ANNUAL: Revise “at least once each calendar year, not to exceed 15 calendar months between tests,” to “once each calendar year or a period not to exceed 15 calendar months between tests.” APPLICABILITY: The applicability is limited to high impact and medium impact at control centers, along with their associated EACs and PACs. This means testing for substations and generating plants that are not high is not included. Was this the intent of the SDT? (c) R2.2: ANNUAL: Revise “at least once each calendar year, not to exceed 15 calendar months between tests,” to “once each calendar year or a period not to exceed 15 calendar months between tests.” (d) REQUIREMENT TEXT: We continue to have concerns with the addition of the phrase “is compatible with current systems.” An entity will need significantly more documentation associated with the tests in order to show auditors that the backup media was “compatible with current systems.” The FERC directives in paragraphs 739 and 748 state that auditors should be able to look at a responsible entity’s policies, procedures and records to determine how the testing is done and what recent tests have been performed.” We do not believe the FERC directive requires the additional phrase. We also suggest adding a phrase that would eliminate the possibility of double jeopardy with EOP-008. Here is proposed revised text to address both concerns: “Unless covered by EOP-008, test a representative sample of information used in the recovery of BES Cyber Systems that is stored on backup media at least once each calendar year, or a period not to exceed 15 calendar months between tests, to verify the backup media is operational and the information is useable.” (e)MEASURES AND CHANGE DESCRIPTION: Remove references to “initially.” (f) R2.3: Add a phrase that eliminates the possibility of double jeopardy with EOP-008: “Unless covered by EOP-008, test ….” and add “representative sample of.” (4) CIP-009 R2 VSLs:

Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (5) R3 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (b) In Order 706, paragraph 731, FERC stated "We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective." We believe that updates to the plan are not effectively in place until it has been communicated, and that it will be more efficient for entities to track one date rather than four date requirements included in draft 2. We propose consolidation of the four subparts of R3 into one subpart that ensures up-to-date recovery plans and communications within the 90 days required in FERC 706 but is less prescriptive and less of a documentation burden. Delete R3.2, R3.3 and R3.4 and use the following text for R3.1: "Update recovery plan(s) and communicate the updates within 90 calendar days of a test, actual recovery or changes that impact the ability to execute the plan. Updates from tests or actual recovery shall include lessons learned. (c) R3 MEASURES: With the consolidated R3.1 requirement, the following is proposed for measures: "Examples: 1) revised recovery plan(s) that include dated references to lessons learned from tests, actual recovery or changes that impact the ability to execute the plan; 2) dated emails, newsletters, training or other communications regarding the plan updates." (5) R3 GUIDANCE: Add the following to guidance: "Individuals responsible for activating and implementing a recovery plan should have information needed to recover their assets. R3 is meant to ensure recovery plans are up to date and available to individuals who need them. The following are examples of items that might require updates and communications within the 90 day timeline: * changes needed as a result of lessons learned from a test or actual recovery; * changes in roles and responsibilities." (6) CIP-009 R3 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention.
No
No
No
(1) CIP-010 R1 REQUIREMENT: MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (a) R1.1 APPLICABILITY: MidAmerican Energy proposes limiting this documentation-laden requirement to high impact. If that is not possible add "with external routable connectivity" to medium impact. Version 4 did not apply to noncritical. (b) R1.1 REQUIREMENT: MidAmerican Energy proposes changing this requirement to a program or performance based level to allow the entity more flexibility with configuration change management, eliminate proposed duplication with other requirements and prevent the addition of unnecessary documentation burden. For example, what is prescribed precludes entities from using a program like Tripwire, which does automated file to file comparisons to look for and report changes. Also, there are several instances in the proposed requirement that increase the risk for double jeopardy by duplicating other requirements. For example: 1.1.1, 1.1.2 and 1.1.3 are covered in CIP-009 R1.3; 1.1.4 is covered in CIP-007 R1.1; and 1.1.5 is covered in CIP-007 R2.3. In the FERC FFT order (docket RC11-6-000) paragraph 81, FERC invites NERC to gain efficiencies and minimize compliance backlogs by removing "requirements that likely provide little protection for Bulk-Power System reliability or may be redundant." Requirement 1.1.4 would require the industry to account for more than a billion ports if each of 214 entities had less than 100 routable assets. Requirement 1.1.5 would require an entity to document tens of thousands of unique patch installs for less than 200 Windows based Cyber Assets. (c) R1.2 APPLICABILITY: MidAmerican Energy proposes adding "with external routable connectivity" to medium impact. (d) R1.2 REQUIREMENT Proposed text: "Authorize changes to: security controls, operating systems, application software versions, custom software, ports or patches. Authorize changes to add or remove hardware." This addresses the SDT's intention to explicitly authorize changes. (e) R1.3 APPLICABILTY: MidAmerican Energy proposes adding "with external routable connectivity" to medium impact. (f) R1.3 REQUIREMENT: The change rationale for

this requirement states it is equivalent to the previous versions (CIP-007 R9 and CIP-005 R5); however, we think this V5 requirement significantly expands the scope of the documentation burden beyond the earlier versions, beyond what FERC has directed and beyond what is needed to ensure security of the grid. FERC's concern with up-to-date documentation is stated in paragraph 651 of Order 706 in the CIP-007 section: "The Commission believes that having correct documentation of methods, processes and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information." Version 1 of CIP-007 required 90 days. In response to Order 706, version 2 was revised to 30 days for CIP-007 – meeting the directive. MidAmerican Energy also has concerns about possible triple jeopardy with the references to CIP-005 and CIP-007. Because FERC's concern is included in the CIP-007 section of Order 706 and the systems security controls are included in CIP-007-5, it may be better to move this requirement to CIP-007 and CIP-005 as a requirement to update and designate what documentation in the respective standards requires updates within what timeframe. (g) R1.4 APPLICABILITY: MidAmerican Energy proposes adding "with external routable connectivity" to medium impact. (h) R1.4 REQUIREMENT: MidAmerican Energy is concerned about scope expansion with the term "BES Cyber System availability". Delete this phrase. For example, does this mean there is a violation if you do a re-boot after a patch installation and the system is down momentarily (and is therefore "unavailable") during the re-boot? Current v4 and VSLs do not indicate this. Also, change the word "determined" to "identified". Absolute assurances are not required; see FERC Order 706 paragraph 399. (i) R1.5 (1.5.1) REQUIREMENT: MidAmerican Energy proposes deleting "that models the baseline configuration to ensure that required cyber security controls are not adversely affected." This is redundant to the concept in the last sentence, which requires documenting differences between test and production when a test environment is used. (2) CIP-010 R1 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (3) CIP-010 R2 REQUIREMENT: MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. 1) R2.1 APPLICABILITY: Remove Associated Physical Access Control Systems and Associated Electronic Access Control and Monitoring Systems and Associated Protected Cyber Assets. This is a new requirement and appropriate to the risks for high impact. 2) R2.1 REQUIREMENT: "Where technically feasible, monitor at least every 35 days for unauthorized changes. Document and investigated detected unauthorized changes." Adding "unauthorized changes." Double jeopardy exists for this requirement with R1. Move the requirement to R1. If a paperwork error occurs in authorizing a change and this requirement uncovers it, this should be addressed under R1, not a separate R. (4) CIP-010 R2 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (5) CIP-010 R3 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (b) R3.1: ANNUAL: Revise "at least once each calendar year, not to exceed 15 calendar months between assessments," to "once each calendar year or a period not to exceed 15 calendar months between assessments." (c) R3.1 APPLICABILITY: MidAmerican Energy proposes adding "with external routable connectivity" to medium impact and associated protected cyber assets. (d) R3.1 REQUIREMENT: Remove references to other CIP standards because it creates risk of double jeopardy. (e) R3.2 REQUIREMENT: MidAmerican Energy proposes ending this requirement after the words, "…that minimizes adverse effects)." Delete "that models the baseline configuration of the BES Cyber System in production." This is redundant to the concept in the last sentence which requires documenting differences between test and production when a test environment is used. (f) R3.3 REQUIREMENT: MidAmerican Energy proposes to change the words "prior to adding" (which is prior to being in scope) to "before closing the change." The Cyber Asset is not a new BES Cyber Asset until it has been installed. Some vulnerability assessments actions only add value to assess after connected to the ESP as part of implementation and post implementation testing. Also, move the parenthetical explanation of a like replacement to guidance. (g) R3.4 APPLICABILITY: MidAmerican Energy proposes adding "with external routable connectivity"

to medium impact and associated protected cyber assets. (h) R3.4 REQUIREMENT: Simplify wording of requirement to minimize documentation and focus on the cyber security related outcome. MidAmerican Energy proposed text: “Document identified vulnerabilities. Establish and implement plans for mitigation or remediation of identified vulnerabilities.” (6) CIP-010 R3 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (7) CIP-010 R3 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower.
No
No
(1) CIP-011 R1 REQUIREMENT: 1) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (a) R1.1: The R1 statement requires “implementing.” “Documentation” is for evidence. Text: “One or more methods to identify BES Cyber System Information.” (b) R1.2: No comments. (c) R1.3: ANNUAL: Revise “at least once each calendar year, not to exceed 15 calendar months between assessments,” to “once each calendar year or a period not to exceed 15 calendar months between assessments.” (2) CIP-011 R1 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (3) CIP-011 R1 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower. (4) CIP-011 R2 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (b) R2.1 and R2.2: The applicability includes dial-up medium impact BES Cyber Systems. The second paragraph in this requirement is contradictory with the applicability, since it references PSPs and dial-up assets do not have to be in a PSP. (c) We do not support the requirement for chain of custody. This is a legal term that requires significant administrative and documentation burden. (d) Order 706 paragraph 631 states “the requirement ultimately needs to assure that there is no opportunity for unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it.” Paragraph 633 in the determination states “clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it” and notes there is a difference between redeploying and discarding. Guidance is a place to clarify. However, the last sentence of guidance in draft two should consider adding “purge” as an option along with “clear.” The proposed parenthetical in R2.1 also provides some clarity. Note: We would also propose adding information to guidelines regarding “out of control of the entity or its contractors.” If an entity has shipped an asset to an outside vendor to do the destruction or sanitization or to conduct analysis of a failed Cyber Asset, a secured shipper would be considered secure for handling purposes. (e) Because of these issues, we propose R2.1 and R2.2 be combined and added to the table for R1 where R1.2 requires handling procedures for BES Cyber System Information. This reduces double jeopardy. Start the text with: “Prior to the disposal or applicable Cyber Assets that contain BES Cyber Information or to the reuse of” (f) The second paragraph of R2.1 should be deleted as redundant to handling required in R1.2. (g) Add “for reuse” after “except” in the parenthetical in R2.1. (i) If it’s necessary to keep the content of the second paragraph of R2.2, we suggest it be incorporated into R1.2, since it relates to information handling and transit. Text such as: “One or more documented and implemented procedures for handling BES Cyber System Information during storage, transit and use, as well as, procedures for preventing unauthorized retrieval when an applicable Cyber Asset is removed from the Physical Security Perimeter before action is taken to prevent unauthorized retrieval from the data storage media.” (5) CIP-011 R2 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention.
Group
MRO NSRF
Will SMith
Yes

No
Yes
Overall it seems as if the standards writers are attempting to work out some subjectivity and ambiguity issues in regards to establishing sufficiency in meeting the requirements of the standards. We do not believe that they have fully resolved these issues. [R2.2] – VSL must change for this such that it is not a violation if the incident response plan is not followed for an actual event. The requirement to document deviations is sufficient to meet the intended goal of ensuring the currency of the plan and updating it to reflect things discovered during actual incidents or drills. [R 3.1] – Suggest strike “and update” to IR plan review. It is possible that the plan is found sufficient after the review and would not require an update. Suggest verbiage “update, if necessary.” [R3.5] – Suggest striking “distribute”. What constitutes distribution? Suggest retaining “notification” approach. Distributing CIP protected data could pose technical issues, especially outside vendors. Notification, as long as the vendor had access would eliminate the need to actually distribute the plan to affected individuals
No
No
Yes
The MRO NSRF believes that the level of descriptiveness and compliance thereof, woudl be disruptive and prohibitive. [R1] – The standard isn’t clear whether the recovery plans are for recovery of the asset, system, or function? Please clarify. [R1.4] – Recommend striking associated physical access control systems and associated electronic access control systems from the applicability section. The wording of the requirement is unclear. What constitutes “initial,” “verification,” or “ensure the process completed successfully”? Suggest prescriptive wording if these terms are to be used. The current draft verbiage leaves too much up to the subjective interpretation of the auditor, and, if intended to be a daily or weekly check, could be administratively burdensome. Proposed Verbiage to align with FERC order 706: “Within the capabilities of the backup system and upon completion of a significant production change within a BES Cyber System, such as adding a new form of hardware or significant new software, data essential to BES Cyber System recovery that is stored on backup media shall be verified at the time the backup is created. Verification means the automated process typically incorporated into the automated backup process validates the bit count or similar technical function.” [R1.5] – Without tying this requirement to a Cyber Security Incident, there will be no forensic value in retaining the data if the event was not related to any malicious attempt. Proposed Verbiage: “Processes to preserve data, except for CIP Exceptional Circumstances, for analysis or diagnosis of the cause of a Cyber Security Incident that triggers activation of the recovery plan(s).” [R2.1] - Are the tests specified in R2 required for each cyber asset, cyber system, or each plan? In other words, does an entity need to do a “full operational exercise” on all systems, or is a representative sampling sufficient? [R2.2] – Is this in reference to the applications and other binaries used to restore or the actual plan itself? Suggest clarification. [R2.3] – Is this requirement implying the need for a bare-metal restore for all CIP assets? Doing so would be cost-prohibitive and potentially jeopardize the stability of the BES. Some CCAs utilize a “standby” system for testing. [R3.4] – Once again the use of the word “distribution”. If I notified a vendor of an update to the plan stored in CIP protected area, it would achieve the objective without the burden of any CPI issues in its “distribution”.
No
No
No
[R1.1.3] – Proposed verbiage: “Any custom compiled software”. [R1.4] – Propose striking 1.4.1 to eliminate speculation or an implicit requirement to have a testing environment outside of 1.5. Instead, the CIP-005, CIP-006, and CIP-007 list should be moved to 1.4.2. This strike also removes the inflexibility as it relates to emergency change that exists in the current draft verbiage. In the absence of striking 1.4.1, recommend adding the CIP Exception Circumstances verbiage to 1.4 to allow emergency changes necessary to ensure operability/reliability. For those circumstances, 1.4.2 should suffice. [R2.1] – Recommend replacing “technically feasible” with “Within the capabilities of the system or network configuration.” Recommend striking the associated systems and cyber assets and leaving this to High Impact BES Cyber Systems with External Routable Connectivity. This also exceeds FERC 706, so we recommend increasing the interval of change detection to an annual or

quarterly verification, because a manual process of verifying the baseline will be administratively burdensome. [R3] – What is the definition of an “active vulnerability assessment”? What would be considered an appropriate infeasibility for performing such a test? Would the entity need to perform an “active vulnerability assessment” on all systems, or is a representative sampling sufficient? Recommend striking “CIP-006” from the list of cyber security controls assessed, as this is duplicative of the testing and maintenance requirement but increases the interval to annual instead of every 24 months.
Yes
Yes
[R1.1] Recommend striking the first bullet in the Measures or changing it to indicate that a label of “confidential” is sufficient. The current measure is phrased such that it requires information to be labeled as CIP information, instead of just confidential. This increases the chances that someone will know how to use it maliciously if they do get unauthorized access to it. Suggest legacy verbiage indicating a classification in alignment with “confidential.” The current verbiage did not prevent organizations from assigning a “CIP Confidential” label to documentation or preclude a protection program that had only one level of protected information. [R2.1 and 2.2] Recommend striking “chain of custody” to avoid connotations associated with legal definitions of this term that should not apply here. If the intent is to ensure positive control of the device until the information is removed, the phrasing should be in alignment with that. This phrasing should also allow secure methods of transport to the vendor if that is required within support contracts
Individual
Richard Salgo
NV Energy
Yes
Yes
Yes
Yes
Yes
Yes
No
Yes
Yes
We note that in R1, part 1.4.2, the verification that controls are not adversely affected is to occur “following the change”, but there is no specification as to how long an entity may take to make this verification. This appears to be a weakness, and we presume that an auditor will attempt to pass judgment on an entity’s promptness of verification.
Yes
Yes
Group
NESCOR/NESCO
Annabelle Lee
No
No
R1: Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com/ General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library Part 2.2: Part 2.2 does not address new vulnerabilities or threats. Consider adding a requirement that the plan be revised based on new threats/vulnerabilities. As stated, "Retain relevant documentation related to Reportable

BES Cyber Security Incidents for three calendar years." Is this sufficient for law enforcement, state, and federal requirements? Also, if the documentation is in electronic form, consider storing it in encrypted form and signed to ensure confidentiality, non-repudiation, and integrity. As stated, "Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary." Consider revising the plan if there are incidents, new vulnerabilities, new threats, and modified security configurations. As stated, "Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan." Consider modifying other relevant documentation, e.g., configuration management plan, access control policies, audit policies, etc.
No
Yes
R1.3: For Part 1.4, what does “verified initially” mean? Each time the backup runs, or the first time after the asset was commissioned? (Could be years ago). If the latter, evidence retention might be an issue for long-life assets. As stated, "Conditions for activation of the recovery plan(s)." The terms “response plans” and “recovery plans” are not adequately defined. It is not clear what the differences are between the two types of plans. R3.2: For an actual incident recovery, consider requiring that the data produced in R1.5 be assessed in reviewing the recovery process. This might be included in the requirement, in the measures, or both. R3.4: NERC could consider updating the Measures in Part 3.5 of CIP-009-5 Table R3 to ensure communication of update activities be conducted in a manner that requires an irrefutable acknowledgment on the part of the receiver of the communication. As stated, "Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned." and "Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2." These plans may require changes to other applicable plans, procedures, and documentation, e.g., configuration management documentation, security configurations, access control policies and procedures. R3.2: For an actual incident recovery, consider requiring that the data produced in R1.5 be assessed in reviewing the recovery process. This might be included in the requirement, in the measures, or both. R3.4: NERC could consider updating the Measures in Part 3.5 of CIP-009-5 Table R3 to ensure communication of update activities be conducted in a manner that requires an irrefutable acknowledgment on the part of the receiver of the communication. As stated, "Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned." and "Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2." These plans may require changes to other applicable plans, procedures, and documentation, e.g., configuration management documentation, security configurations, access control policies and procedures.
No
No
No
R1.1: As stated, "Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels." This is not a comprehensive list of what could be included for each cyber asset. It is not clear how this list applies if the device is hardware only. Also consider adding communication protocols. NERC could consider adding a requirement to include in the baseline any non-standard configurations of the BIOS, operating system, services, etc. For example, BIOS version, BIOS boot disk order, BIOS password, changes to Windows registry entries, changes to service/task scheduling priorities, addition of periodic processes via modifications of tools like crontab, etc. NERC could consider adding a requirement to explicitly include in the baseline any remote access services, eg. RDP, VNC, PCanywhere, etc. NERC could consider adding programmable device load versioning to

the list of items in the configuration baseline. This should include any executable or loadable image that can be modified without requiring physical access to BES Cyber System component internals. Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library R2: Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library R3: There are no requirements that an entity identify or document third party connections to BES Cyber Assets. Such connections are common and a high source of potential risk. NERC could consider developing requirements to identify and document third party connections, and authenticate and control access, both ephemeral (remote access) and persistent, from such connections. Furthermore, any and all requirements specified by the CIPs for the BES Cyber Assets accessed, including technical controls, policies, background checks, information handling, etc., should also apply to the third party systems. R3.2: R3.2 calls for vulnerability assessments every three years. CIP 007-3 R8 requires vulnerability assessments annually. No rationale is given for weakening this requirement. As of January 2 2012, the National Vulnerability Database contains 49053 CVE vulnerabilities, with 11 being added per day. Even without likely acceleration of this growth rate, this implies 4000 new vulnerabilities will be discovered each year. Even if only a small percentage of these apply to BES cyber assets, this could mean a significant number of KNOWN vulnerabilities in BES cyber assets by the time a vulnerability assessment comes due. Because of the constant change and introduction of new vulnerabilities, revising the time frame to three years seems inconsistent with this constantly changing vulnerability environment. Consider modifying the time frame to annually, or less.
No
No
This CIP does not address how third parties (consultants, contractors, vendors, etc.) should handle BES Cyber System information. Where 3rd parties have persistent or ephemeral remote access to Cyber Assets, they have implicit access to BES Cyber Asset information. NERC could consider applying all information requirements of CIP 011 to any 3rd parties with such access.
Group
Dominion
Connie Lowe
Yes
No
Yes
CIP-008-5-R2 - Part 2.1 Remove the acronym "BES" to be consistent with all the other requirements. Include in measures as an example, "dated evidence of a lessons-learned report from an actual cyber security incident".
No
Yes
Yes
CIP-009 R1: - Part 1.1: change the measures to be "Evidence may include, but is not limited to, one or more plans that include language identifying general conditions for activation of the recovery plan(s)." - Part 1.4 is confusing as written and should be rephrased with "Validate the successful completion of backup processes for information essential to BES Cyber System recovery directly associated with a significant production change" - Part 1.5 should be reworded as " Processes to preserve data, except for CIP Exceptional Circumstances, for analysis or diagnosis of the cause of any Cyber Security Incident that triggers activation of the recovery plan(s).". By replacing the word "event" with Cyber Security Incident adds clarity to which events require data preservation. CIP-009 R2: - Part 2.3 should be reworded to be "Test a representation of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise." Rationale: All high impact BES Cyber Systems are already subject to other NERC Standards that require testing of backup and recovery of

components on a yearly basis. CIP-009 Application Guidelines - For consistency, CIP-009 should have a published Application Guidelines. No Application Guidelines exist for this Standard.
No
Yes
No
CIP-010-1-R1 - The term "BES Cyber Asset" should be replaced with "applicable Cyber Asset" to better align with the Applicability column - Part 1.1.5 should be clarified to identify only those patches applied to the asset at the time the baseline is established and not all possible historic patches available for the asset. The language of the requirement should be, " Any security patches applied to the applicable Cyber Asset." - The measures of 1.1 need to be updated to be consistent with the "or by group" language of the Requirements such that both bullet points add "or group" after the term "Cyber Assets". The proposed language for the measures would read, " Examples of acceptable evidence include:…" • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset or group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset or group." - Part 1.3 needs to define specifically the expected documentation requirements from CIP-005 and CIP-007 for clarity. Additionally, the Applicability columns of CIP-005 and CIP-007 for the associated documentation requirements should match the appliability column of Part 1.3. - Similar to Part 1.3, Part 1.4.1 needs to define specifically the expected documentation requirements from CIP-005, CIP-006, and CIP-007 for clarity. - The language in Part 1.4.1 which essentially allows an impact analysis to be performed to determine which controls may need to be retested after the change should be retained. - Part 1.4.2: "BES Cyber Asset" should be replaced with "applicable Cyber Asset" as noted previously - Part 1.5.1 should be altered to, "Prior to implementing any change in the production environment, test the changes in a test environment that models the baseline configuration or in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that required cyber security controls are not adversely affected; and". The parenthetical expression adds no value. - Part 3.1 needs to define specifically the expected documentation requirements from CIP-005, CIP-006, and CIP-007 for clarity. - Part 3.2 replace the language of the requirement with the following: "Where technically feasible, at least once every 36 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the production baseline configuration of the Cyber System or in a production environment where the test is performed in a manner that minimizes adverse effects. If a test environment was used, document the differences between the test environment and the production environment including a description of the measures used to account for any differences in baseline configuration between the test and production environments." The parenthetical expression adds no value - Part 3.3 should be reworded for clarity as follows: " Prior to adding a new Cyber Asset perform an active vulnerability assessment of the new Cyber Asset except 1) for CIP Exceptional Circumstances and 2) performing like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset." - The language of Part 3.4 should be changed to, "Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified, if any, in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items." The term "if any" was added to denote the need to document the results of assessments that identified no vulnerabilities.
No
No
CIP-011-1 - Part 1.1 clarify intent by rewording with the following suggested language "One or more documented and implemented methods to identify information or information repositories as meeting the definition of BES Cyber System Information." - Part 2.1 needs to be simplified as: "Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information , the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset." The second paragragh adds no additional value and the term "chain of custody" implies a legal definition that goes beyond what we understand is the intent of the requirement. Also, the second bullet should be eliminated in the Measures section for consistency. The following bullet should be removed, " If removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval of information, a chain of custody record that was maintained." - Part 2.2 needs to be simplified as " Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the

unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media." The second paragragh adds no additional value and the term "chain of custody" implies a legal definition that goes beyond what we understand is the intent of the requirement. The fourth bullet in the measures section should be removed for consistency with the removal of the second paragraph in the requirements. The following bullet should be removed, " If removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval of information, chain of custody record that was maintained."
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
Yes
Yes
Yes
No
Yes
Yes
Please remove R1 Part 1.5 since this Requirement is not related to asset recovery. Most companies already include event analysis of system failures as an engineering practice. This could be included in Guidance as a suggestion. If the intention is to provide data for forensics, then this should be included in cyber security incident response planning (CIP-008) not CIP-009.
No
Yes
Yes
(Comment 1) We agree that documentation should be part of the change process. We agree with the SDT's approach of using CIP-010-1 R1.3 to require updating of documentation when a baseline configuration changes. We prefer this to the current CIP version 3 requirements (CIP-005-3 R5 and CIP-007-3 R9) to review and update documentation. (Comment 2) R1.4.1 references to "cyber security controls identified in CIP-005, CIP-006, and CIP-007" are too vague and open-ended and subject to auditor interpretation. This could be interpreted as requiring a full vulnerability assessment on devices within the ESP after a change to a single system. We suggest limiting the determination and verification of potential affected controls to the specific BES Cyber System that is being changed. Also, we suggest providing information in the guidance section on controls to be considered similar to the guidance that was provided for CIP-010 R3.
Yes
Yes
For clarity, we recommend deleting the second paragraph in each of requirement 2.1 and 2.2 and creating a third sub-requirement (2.3) that states "If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity shall maintain chain of custody, which identifies who has possession of the device while it is outside of a Physical Security Perimeter."
Individual
Chris Plensdorf
Detroit Edison Company
Yes
Yes
Yes
Yes
Yes

Yes
No
No
Yes
We are concerned that the SDT does not understand the extent of work necessary to meet proposed requirement CIP-010 R1.1.5. Based on requirement 1.5, the baseline required for each cyber asset may change frequently and require documentation of a new baseline monthly as the asset is patched for security vulnerabilities. The term baseline may be inappropriate for this requirement as it us written. Perhaps the term configuration log would be more appropriate. We found the language in requirement CIP-010 R2.1 to be amiguous and confusing as it may suggest that twice per 35 calendar days is non-compliant which would certainly then mean that continuous is non-compliant also. Possibly replace "not to exceed once every 35 calendar days" with "not less than once per 35 calendar days"
Yes
Yes
Group
Southern Company Services, Inc.
Antonio Grayson
Yes
Yes
Yes
(1) Regarding CIP-008-5, R1.1 and R1.2 need to allow for one or multiple processes. Southern suggests changing to ‘one or more processes’ throughout the standard. (2) Regarding CIP-008-5, R1.1 and R1.4 are essentially redundant. ‘Respond’ in R1.1 and ‘handling’ in R1.4 are the same. Southern suggests deleting R1.4 to avoid unnecessary duplication. (3) Regarding CIP-008-5, R1.5, Southern suggests changing “that should receive communication” with “that must be sent communication”. Southern also suggests changing the “individuals and” to “individuals or” to help eliminate double jeopardy issues with EOP-004 which specifies the external communications. (4) Regarding CIP-008-5, R2.1, Southern suggests changing “BES Cyber Security Incident response plan(s)” to “incident response plans identified in R1”. R2.2 follows this approach and it avoids the awkward combination of a definition in the name of a plan. (5) Regarding CIP-008-5, R2.1 needs clarification that if an entity has numerous response plans if[?]each one must be tested every year. (6) Regarding CIP-008-5, R2.1 Measures include a specific lessons learned dated report which is not part of the requirement. Southern suggests deleting “a lessons-learned report” from the Measures. (7) Regarding CIP-008-5, R2.2 reads as though only one test plan can exist which is in conflict with R2.1. Southern suggests that the language be changed to allow for multiple plans to exist. (8) Regarding CIP-008-5, R2.3, is there double jeopardy here with record retention requirements in EOP-004? Southern suggests removing R2.3 and let EOP-004 handle all aspects of reporting and retention. (9) Regarding CIP-008-5, R3.4, Southern suggests returning to V4 language. It seems that to audit this requirement a master list of “technology changes” would need to be produced with an analysis of which ones did or did not affect any incident response plans. A date for each “technology change” would also be required in this master list so the 30 day clock can be audited.
No
No
Yes
(1) Regarding CIP-009-5, R1.3, Southern suggests striking the word “successfully” in the measure. (2) Regarding CIP-009-5, R1.4 needs to have provisions for vendor or other 3rd party backups or the initial media. If what is needed to recover a system is simply a reload from the vendor software CD, how does an entity prove that it was verified initially? Southern suggests adding to the beginning of the requirement “Responsible Entity created backups of information essential…”. Additionally,

Southern strongly suggests that the requirement be reworded to match the Measure. Proposed language, “The backup process for information essential to BES Cyber System recovery that is stored on backup media shall be verified to ensure the backup process completed successfully.” (3) Regarding CIP-009-5, R1.5 needs additional conditions for invocation [?]. Some activities captured within the requirement are normal course of business vs. cyber attack. A malfunctioning motherboard after a known power surge or lighting strike should not invoke a forensics process. Southern suggest replacing “any event” with “Reportable Cyber Security Incident” to address when forensics is required. (4) Regarding CIP-009-5, R2.1, an entity could have hundreds of recovery plans for all different types of systems. Is it permissible to test one plan for each representative type of cyber system or must it be shown for every individual BES Cyber System as per the applicability column? If so, this should be clarified in the requirement. Additionally, consider if “or” is needed after the first bullet, as shown in the second bullet. (5) Regarding CIP-009-5, R2.2 could imply that if daily backups are taken, every one of those daily backups should be tested annually. The requirement should not require the test of a year’s worth of backup tapes, just the last one or a representative sample. It takes too long of a period of time to restore every backup and would be a waste of resources. Proposed text: “Test a representative sample of information used in the recovery of BES Cyber Systems that is stored on backup media, at least once each calendar year, not to exceed 15 calendar months between sample tests, to ensure that the information is useable and is compatible with current system configurations.” (6) Regarding CIP-009-5, R2.3 needs additional clarity that all recovery plans do not have to be “fully operationally tested” at the same time. Utilities need the flexibility to test individual recovery plans at different times within the three-year period. Southern proposes replacing the second occurrence of “plans” with “plan” in the first sentence of the requirement. Additionally, the initial test for this particular requirement needs to be within the first full 3-year period following the compliance date. (7) Regarding CIP-009-5, R3.4, the focus of the requirement should be on “notification” not “distributing”. Proposed text: “Notify responsible individuals under R1.2 of recovery plan updates within 30 calendar days of the update being completed.”
No
No
No
(1) In general regarding draft 2 of CIP-010-1, Southern strongly suggests that the SDT return to the approved language in CIP-003-4 R6 and CIP-007-R1 with targeted and efficient changes to address FERC orders. (2) Regarding CIP-010-1 R1, R1.1.1 Southern suggests changing “exists” to “is either operating or running”. (3) Regarding CIP-010-1 R1, R1.1.5 changes too frequently to be in the baseline and should be removed. The evaluation of each patch is already included in CIP-007-5. (4) Regarding CIP-010-1 R1, there is opportunity for double jeopardy with R1.1.4 and R1.1.5 and CIP-007 that could be resolved by making CIP-010-1 activities distinct from CIP-007-5 required activities. (5) Regarding CIP-010-1 R1, R1.3 creates opportunity for double jeopardy and needs to be revised or removed. (6) Regarding CIP-010-1 R1, R1.4.1 should be deleted and the word “applicable” added into R1.4.2. This would eliminate the extra documentation step represented by R1.4.1. Southern believes R1.4.1 where “could be impacted” is used will cause all entities to document every control for every change in order to avoid zero-defect audit enforcement when some situation can be devised where “could be impacted” is a remote possibility. Southern believes that documenting “what could be impacted” is not a reliability benefit, it’s the verification that controls are not affected by a change. (7) Regarding CIP-010-1 R1, R1.4.2 we suggest deleting “and the BES Cyber System availability”. If a change such as a vendor patch causes an unforeseen outage on a single device, is that a cyber security violation? (8) Regarding CIP-010-1 R1, as written, it’s not clear what the essential difference is between R1.4 and R1.5 is for High Impact Systems. Additionally, there appears an opportunity for double jeopardy in R1.4 and R1.5. Southern recommends removing the overlap in applicability of the two requirements and adding clarifying language as to what is intended and required in R1.4 vs. R1.5. Simpler, higher-level language needs to be developed for R1.4 and R1.5. Both are confusing as to what is expected and how they do or don’t relate to one another. (9) Regarding CIP-010-1 R3, proposed text for R3.1: “At least once every calendar year or not to exceed 15 calendar months between assessments, conduct a paper or active vulnerability assessment (leveraging previous cyber security controls test results where possible) to determine the extent to which identified cyber security controls are implemented correctly and operating as designed.” Rationale for Changes to R3.1: For reasons stated earlier in comments and in agreement with EEI’s comments, the “At least once every calendar year, not to exceed 15 calendar months” needs to be replaced with “At least

once every calendar year or not to exceed 15 calendar months." Additionally, it is not apparent what "cyber security controls" exist in CIP-006. CIP-006 defines physical security controls and should not be listed in this requirement as it is duplicative of the testing and maintenance already required under CIP-006-5. Additionally, this requirement, by referring to other standards, creates a double jeopardy situation. The dependency on other standards needs to be removed and replaced by "identified cyber security controls". Additionally, for efficiency, the requirement needs to leverage the cyber security control reviews that are already being conducted in other standards, and require an additional new assessment only if one has not been already conducted in the previous 15 months. This clarification needs to be explicit in the requirement and added to guidance. (10) Regarding R3.2, it's not clear how this requirement is different from what is already required in CIP-007. (11) Regarding R3.4, replace "remediate or mitigate vulnerabilities" with "implement lessons learned (if any)" for consistency with other standards and eliminate extra documentation tracking requirements. Proposed text: "Document the results of the assessment and the action plan to implement lessons learned (if any) identified in the asessments including the proposed date of completing the action plans."
Yes
No
(1) Regarding CIP-011-5, R1.1 and R1.2, Southern suggests deleting the phrase "and implemented" as it is a duplicate of the verb in the main Requirement. (2) Regarding CIP-011-5, replace "to remediate deficiencies" with "for lessons learned (if any)". This is a find and fix requirement and should not be a compliance violation. (3) Regarding CIP-011-5, the term "chain of custody" has a well understood legal definition not appropriate for the NERC CIP standards. The focus of 2.1 and 2.2 needs to return to the CIP-003-4 R4 and R5 language. Replace "maintain of chain of custody" with "maintain a process to document the control of the device". Additionally, the term "chain of custody" needs to be removed from the measures. (4) Additionally regarding CIP-011-5, R2.1, the requirement of "who has possession" needs to be removed as the process to document control of the device may include couriers or external vendors.
Individual
Brian S. Millard
Tennessee Valley Authority
Yes
Yes
Yes
R1.1 - Replace "Processes" with "Process(es)". You could have just one process. R1.5 - Replace "that should" with "must", and "receive communication" with "be sent communication". Replace "individuals and" with "individuals or". This limits double jeopardy related to external organization communications which are included in EOP-004 requirements. R2.3 - EOP-004 record retention requirements may result in double jeopardy, this requirement is redundant and should be removed.
Yes
Yes
Yes
R1.3 - In measures remove "successfully". R1.4 introduces questions about response for when a backup fails. If a single monthly backup succeeds, is that good enough? What is verified initially? Is this a daily check for backups or is weekly verification sufficient? If a log is printed or a snapshot taken monthly for evidence sufficient if alerting to x-number of failures is part of the process or is evidence collection required upon completion of the backup? R1.5 - Need to have provisions to identify that this is as a result of a malicious threat and not process or equipment fault.
Yes
Yes
Yes
R1 requires additional personnel and systems to accommodate the expansion of test and acceptance environments to meet new test requirements. R1.1 - 1.1.4 and 1.1.5 are duplicates of CIP 007 and CIP 010. Would create double jeopardy consolidate in one place. R1.4 - consider dropping 1.4.1, this is covered in 1.4.2. Move CIP-005, CIP-006, and CIP-007 statement into 1.4.2. Strike "and the BES

Cyber System availability” from 1.4.2. R3.4 - Replace “remediate vulnerabilities identified with “incorporate lessons learned”.
Yes
Yes
R1.3 - Replace “remediate deficiencies identified" with “incorporate lessons learned”.
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form C.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form C.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form C.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form C.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form C.
Individual
Ralph Meyer
The Empire District Electric Company
No
No
No
1. In all requirements, remove references to systems & assets and rely on the applicability column to specify applicability. 2. In all measures section remove the term “…but not limited to…” 3. Change all instances of Medium Impact BES Cyber Systems to “Medium Impact BES Cyber Systems with External Routable Connectivity” for consistency with CIP-005, CIP-006, and CIP-007 4. CIP-008 R1.2 requires the Plan to have: A process to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident. The definition of Reportable Cyber Security Incident is in the definitions as “Any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.” As written the Entity is to develop a process to determine if a cyber security incident compromises or disrupts a reliability task. But the list of reliability tasks is not defined in the Standards. Suggested changes to definition of Reportable Cyber Security Incident, to also be included in the requirement a. Suggestion 1) Any Cyber Security Incident that has disrupted the operation of the BES resulting in a violation of a SOL or IROL. b. Suggestion 2) Any Cyber Security Incident that has compromised or disrupted the operation of the BES and requires reporting per EOP-004. 5. R2 – Allow for an exception to the time frames listed in the event of CIP Exceptional Circumstances 6. R2.1 a. Remove the word “BES” from the Requirement to be consistent with R1. b. Remove the words “lessons-learned report that includes a” from the Measures because the following items do not necessarily fall into the lessons learned category. c. Add a 2nd Measure “OR documentation from an actual Reportable Cyber Security Incident” as an alternative to the listed evidence. 7. R3.1: Change the Requirement to read “Review and update each Cyber Security Incident response plan for accuracy and completeness once each calendar year or a period not to exceed 15 calendar months between reviews except for CIP Exceptional Circumstances.” Rationale: Reduce significant confusion 8. R3.2 a. Clarify Requirement as follows: “R.3.2 “Maintain a current and up-to-date Cyber Security Incident Response Plan that (1) includes or references, as appropriate, documentation of any lessons that may have been learned in connection with a Cyber Security Incident test or actual incident response performed pursuant to CIP-008-5 R2, within 90 days of the performance of such test or actual incident response; and (2) includes changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change.” b. Clarify Measures as follows: “Evidence may include, but is not limited to, a dated, revised Cyber Security Incident Response Plan(s) that (1) includes or references, as appropriate, dated documentation of lessons learned, if any, associated with tests of or actual responses using the Cyber Security Incident

Response Plan(s), within 90 days after completion of such test or actual incident response; and (2) reflects changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change." 9. R3.3 & R3.4: Remove these requirements as they are now incorporated into the proposed R3.2.
No
No
No
10. R3: In Order 706, paragraph 731, FERC stated "We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective." We believe that updates to the plan are not effectively in place until it has been communicated, and that it will be more efficient for entities to track one date rather than four date requirements included in draft 2. We propose consolidation of the four subparts of R3 into one subpart that ensures up-to-date recovery plans and communications within the 90 days required in FERC 706 but is less prescriptive and less of a documentation burden. Delete R3.2, R3.3 and R3.4 and use the following text for R3.1: "Update recovery plan(s) and communicate the updates within 90 calendar days of a test, actual recovery or changes that impact the ability to execute the plan. Updates from tests or actual recovery shall include lessons learned. R3 MEASURES: With the consolidated R3.1 requirement, the following is proposed for measures: "Evidence may include, but is not limited to: 1) revised recovery plan(s) that include dated references to lessons learned from tests, actual recovery or changes that impact the ability to execute the plan; 2) dated emails, newsletters, training or other communications regarding the plan updates." R3 VSLs: Replace the draft 2 VSLs with the following. Lower VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 90 and less than 120 days of the change, test or actual recovery. Moderate VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 120 and less than 150 days of the change, test or actual recovery. High VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 150and less than 180 days of the change, test or actual recovery. Severe VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 180 and less than 210 days of the change, test or actual recovery. R3 GUIDANCE: Add the following to guidance: "Individuals responsible for activating and implementing a recovery plan should have information needed to recover their assets. R3 is meant to ensure recovery plans are up to date and available to individuals who need them. The following are examples of items that might require updates and communications within the 90 day timeline: * changes needed as a result of lessons learned from a test or actual recovery; * changes in roles and
No
No
No
1. In all requirements, remove references to systems & assets and rely on the applicability column to specify applicability. 2. In all measures section remove the term "…but not limited to…" 3. R1 is too prescriptive. Recommend that the CIP v3/v4 language replace 1.1-1.4, but specifically address the Order 706 requirements for malicious changes. 4. R1: remove Associated assets/systems from applicability because they represent an increase in scope from CIP v3/v4 5. R2: remove Associated assets/systems from applicability because they go beyond Order 706. 6. R1.1: Add "with External Routability" to Medium Impact BES Cyber Systems 7. R1.4: Remove "High Impact" from Applicability because it is repetitious with R1.5. 8. R3.1 a. Applicability: Add "with External Routability" to Medium Impact BES Cyber Systems and Associated Protected Cyber Assets. b. Requirement: Change to read: "At least once every calendar year, or up to 15 months between assessments, conduct a paper and/or active vulnerability assessment to determine the extent to which the cyber security controls identified in CIP-005, CIP-006, and CIP-007 are implemented correctly and operating as designed. Any paper and/or active vulnerability assessment already performed in the implementation of other CIP standards are not included in this requirement". Rationale: avoid double jeopardy. 9. R3.2: Remove the words "that models the baseline configuration of the BES Cyber System in a production environment" after the parentheses. 10. R3.3: Change the words "prior to adding" to "as part of the

change prior to completing the commissioning of". Rationale: clarity 11. R3.4: Change the requirement to read: "Document identified vulnerabilities. Establish planned or completed dates relating to the mitigation or remediation of identified vulnerabilities." Rationale: As worded, the language increases the compliance-tracking burden to all sorts of other documentation including action plans, plan status, etc. The proposed language shifts the focus of the requirement back towards a cyber security related outcome, i.e. mitigated vulnerabilities. This is accomplished by staying away from language that requires documentation overhead. Language on action plans should be moved into the guidance documentation.
No
No
1. In all requirements, remove references to systems & assets and rely on the applicability column to specify applicability. 2. In all measures section remove the term "…but not limited to…" 3. Applicability for all requirements should add "Medium Impact BES Cyber Systems with External Routability" to all "Medium Impact BES Cyber Systems" 4. Several requirements use the terminology "BES Cyber System Information", however this creates an inconsistency with all the "Associated…" assets in the Applicability column. Suggestion is to leave the applicability in that column, and don't name asset/system types in the requirement. 5. The length of the "Applicability…" column title can cause confusion about the systems/assets that are within scope. Suggest changing the column heading to "Applicability". 6. R2 uses the term "chain of custody" in several places. This is a legal term that relates to evidence. Suggest replacing it with "possession" or "control". 7. R1.3: Change Requirement & Measure language time frames by removing "at least" and replacing with "once each calendar year or a period not to exceed 15 months". 8. R2.1: In parenthetical text in Requirement change to read "(except for reuse in other high impact…)" for clarity.
Individual
Kirit Shah
Ameren
Yes
Yes
Yes
(1) General Comment – For all the measures for CIP-008 the wording "with External Routable or Dial-up connectivity" should be added to the applicability of Medium Impact BES Cyber Systems due to the added amount of documentation that would be needed for no additional security benefit to the BES. (2) R2.1 – Remove the words "BES" in front of the words "Cyber Security Incident" from the requirement to match the references to "Cyber Security Incident" in all the other requirements for CIP-008. (3) R2.1 - Insert "or" after the first bullet in the requirements. As currently worded entities must perform 2 of the 3 exercises to meet compliance. (4) R2.3 – Remove 'relevant' in the requirements or clearly define what relevant records are to eliminate subjective interpretation (perhaps refer to M2.3 within the requirement).
Yes
Yes
Yes
(1) R1.3 – The words "and associated system" needs to be added after "BES Cyber System" in the requirements and measures to clarify that this requirement applies to the associated systems. (2) R1.4 – (a) The requirement should be reworded to "Information essential to BES Cyber System recovery that is stored on backup media shall be verified after each backup to ensure that the backup process completed successfully." (b) The words "for 90 days" need to be added after the word "logs" in the measures. Currently there is no time frame for how long these logs need to be retained. (3) R2.1 - Insert "or" after the first bullet in the requirements. As currently worded entities must perform 2 of the 3 exercises to meet compliance. (4) R2.3 – The requirements asks entities to perform a functional test of the recovery plans every 36 calendar months. What M&T or DR industry standard does the 36 month recommendation come from? We suggest that some guidance be added to the standard to explain why 36 calendar months was selected.
No

Yes
Yes
(1) General Comment – (a) For all the measures for CIP-010 the wording "with External Routable or Dial-up connectivity" should be added the applicability of Medium Impact BES Cyber Systems. Currently technology does not exist to meet compliance with these requirements for serial connected devices; for example programmable protective relays. (b) For all the applicability for CIP-010 remove "Associated Protected Cyber Assets" to match the current CIP standards. (2) R1.1 – We request that the requirement be reworded to "Develop a baseline configuration for each Cyber Asset identified, individually or by group. The requirements in 1.1.1 to 1.1.5 go above and beyond what most baseline software can do today and would require manual inventorying of baseline systems instead of using automated process. (3) R1.4 – Remove "High Impact BES Cyber Systems" from the applicability since High Impact BES Cyber Systems is covered in R1.5. This requirement is confusing since this requirement is also covered in R1.5 (4) R2.1 – We request a change of wording for “monitor continuously or periodically, not to exceed once every 35 calendar days” to “document changes tracked through the Entity’s change management program” in the requirement. To check the baseline configuration of every system will be overly burdensome to entities. We suggest changing the 35 calendar day requirement to every 90 days.
Yes
No
(1) General Comment – For all the measures for CIP-011 the wording "with External Routable or Dial-up connectivity" should be added the applicability of Medium Impact BES Cyber Systems. Currently technology does not exist to meet compliance with these requirements for serial connected devices; for example programmable protective relays. (2) R2.1 – The Applicable section needs to be adjusted or requirement changed to reflect BES Cyber Systems and Associated systems that do not need to be in a Physical Security Perimeter. We would suggest removing the words "Physical Security Perimeter" and replace with "secured area" to help clarify this requirement. (3) R2.1-R2.2 – The SDT had stated “Chain of Custody” for all devices while outside of the ESP in the requirements. Please clarify what is the intent of “Chain of Custody.” Is it the intent of the SDT to require hermetically sealed evidence containers that are not accessed through the same opening more than once and every person accessing the device has a personally identifiable seal? We suggest using different wordings or an approach such as retired asset must remain in the custody of the entity at all the time.
Group
Salt River Project
Sara McCoy
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
CIP-011 R2: SRP suggests adding further detail on what qualifies as protected information. This would assist entities in identifying said information. Current verbiage allows for entity interpretation.
Group
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)

David Dockery, NERC Reliability Compliance Coordinator, AECI
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Texas RE NERC Standards Review Subcommittee
Brenda Hampton
No
No
No
(1) The applicability of CIP-008-5 R1, R2 and R3 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity or Dial-up Connectivity.” This modification would support the current applicability and proposed changes to the applicability of CIP-005-5, CIP-006-5 and CIP-007-5 and would align the incident response plan to those cyber systems that have connectivity. (2) CIP-008-5 R2.3 requires retention of relevant records and should be relocated to Section C1.2 regarding Evidence Retention. (3) Combine Requirement R3.2 and R3.3 and allow 60 calendar days to complete the investigation, determine appropriate lessons learned, and update the response plan. (4) The 30-day timing requirement in CIP-008-5 R3.4 should be extended to 60 calendar days such that the overall timing for the activities in CIP-008-5 R3 is more reasonable. This would allow for a consistent 90-day timeline for planned changes as well as responses to Cyber Security Incidents.
No
Yes
No
(1) Combine Requirement R3.2 and R3.3 and allow 60 calendar days to document identified deficiencies or lessons learned, and update the recovery plan(s). (2) In Requirement R3.3, 30 days should be extended to 60 calendar days to make the overall timing for the activities in R3 more reasonable. This would allow for a consistent 90-day timeline for planned changes as well as lessons learned from the use/testing of the recovery plan.
(1) The applicability of CIP-009-5 R1.1, R1.2, R1.3 and R1.5 should be limited to “Medium Impact BES Cyber Systems at Control Centers.” This will concentrate efforts on areas where reliability impacts are the highest and avoid placing additional/duplicate requirements on cyber systems/assets covered under the PRC Standards. (2) The misoperation of relaying systems is covered under the PRC Standards and should be excluded from CIP-009-5 R1.5. (3) Comments on CIP-009-5 R3 are in Question 7 Comments.
No
Yes
No

(1) The applicability of CIP-010-1 R1.1, R1.2, R1.3 and R1.4 should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity.” Consider limiting to Control Centers only. As the requirements are currently written, they mandate the creation of an asset register for a large population of cyber assets that are not connected to a network via a routable protocol and are already covered under the PRC Standards. This will place an undue burden on the Responsible Entity without enhancing reliability. (2) Split Requirement R1.3 into two Requirements. For High Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, leave the requirement at 30 days. For Medium Impact BES Cyber Systems with External Routable Connectivity, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, extend time to 60 days to allow for sufficient time to process/document the required changes and verifications. (3) The applicability of CIP-010-1 R3.1 and R3.4 should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity or Dial-up Connectivity.” This modification would eliminate existing discrepancies between the applicability of CIP-005, CIP-006, and CIP-007 and the applicability of CIP-010. This modification also supports the proposed applicability of CIP-005-5 and CIP-007-5 such that the vulnerability assessments are directed towards cyber systems with connectivity.
No
No
The applicability of Requirements R1.1, R1.2, R1.3, R2.1, and R2.2 should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity” to maintain consistency with the scope of cyber systems/assets currently covered by similar requirements in the CIP version 4 Standards. The inclusion of cyber systems/assets with no routable connectivity will significantly increase documentation requirements with no benefit to reliability.
Group
FirstEnergy
Doug Hohlbaugh
Yes
Yes
Yes
R3, Part 3.4 requires an update to an entity’s Cyber Security Incident response plan(s) within 30 calendar days of certain changes (plan roles/responsibilities or technical). The preceding R3 requirements require plan updates (as needed) based on lessons learned through application of the plan through a test or actual incident and at a minimum the plan must be reviewed and updated annually. FE believes that R3, part 3.4 will subject responsible entities to undue compliance burden that is best left as a best practice and not a mandatory and enforceable reliability requirement. The reviews and updates occurring through the lessons learned (3.2, 3.3) and the annual plan reviews (3.1) should suffice for the updates needed.
Yes
Yes
Yes
R3, Part 3.3 requires an update to an entity’s recovery plan(s) within 30 calendar days of certain changes (plan roles/responsibilities or technical). The preceding R3 requirements require plan updates (as needed) based on lessons learned through application of the plan through a test or actual incident and at minimum the plan must be reviewed and updated annually. FE believes that R3, part 3.3 will subject responsible entities to undue compliance burden that is best left as a best practice and not a mandatory and enforceable reliability requirement. The reviews and updates occurring through the lessons learned should suffice for the updates needed.
No
Yes
Yes
R1 refers to baselines and what is desired via the requirements appears to be documentation of the current configuration of the Cyber Asset. The main goal of FE’s proposed change (see following text)

is to eliminate the word "baseline". FE believes a risk exists to confuse the purpose with security baselines we create today for devices. The following is draft language proposed for R1. R1.1 Document the configuration, which shall include the following for each Cyber Asset identified, individually or by group: R1.1.1 - R1.1.5 no changes R1.2 Authorize and document changes, individually or by group to each Cyber Asset identified that would affect: R1.2.1 Operating system(s) (including version), or firmware where no independent operating system exists; R1.2.2 Any commercially available or open-source application software (including version) intentionally installed on the BES Cyber Asset; R1.2.3 Any custom software developed for the entity; R1.2.4 Any logical network accessible ports; and R1.2.5 Any security patches. R1.3 For a change identified in R1.2 update configuration documentation for each Cyber Asset identified and other documentation required by CIP-005 and CIP-007 as necessary within 30 calendar days of completing the change. R1.4 For a change identified in R1.2: R1.4.1 - R1.4.3 no changes R1.5 Where technically feasible, for each change identified in R1.2: R1.5.1 - R1.5.2 no changes
Yes
Yes
Group
Family Of Companies (FOC) including OPC, GTC & GSOC
Guy Andrews
No
Yes
Yes
(R1) It is not clear how the process to respond to Cyber Security Incidents required by R1.1 differs from the procedure to handle Cyber Security Incidents required by R1.4. Whatever distinction there might be is further muddled by the fact that the measure for R1.4 includes both processes and procedures and refers to a response as well as to “handling” the incident. We recommend that R1.4 be deleted or the requirements be rewritten to clarify the distinction between the requirements.
No
No
No
(Part 3.2) R3.2 The measure should address the anticipated evidence for a situation where there are no deficiencies. Do you require documentation within 30 days stating that there were none, or is an attestation at a later date adequate? (Part 3.4) In R3.4 “Distribute” is the wrong word and should be replaced with “make available”. Distribute implies actively sending someone the document. A change will frequently affect only a small subset of the people responsible for the plan. An email summarizing the changes and containing a link to the new version is the typical way of handling this and is completely adequate to support the purpose of the requirement
(Part 1.4) R1.4 does not fit with the parent requirement or with the other subrequirements. R 1 is about what the plan must contain. R1.4 is for a specific action (verifying backup data). You could state that the plan must have a process for verifying backup data or you could move this to a separate requirement, but it does not belong here as written. (Part 1.5) R1.5 is too vague. Specifically, it does not provide entities with adequate information to determine what data needs to be preserved. This requirement could reduce reliability. The measure implies a requirement to mirror data before proceeding to recovery. First it is improper to include a requirement in a measure; second, it should be left to the entity whether understanding the cause of the failure is important enough to justify delaying recovery to preserve this data (whatever it is eventually specified to be). Thirdly, there are a multitude of ways a system can fail, and it is not reasonable to develop processes for each possibility. Although we agree that a fault analysis is a worthy endeavor, we do not believe it is measureable enough to be written into the standards at this time. We believe the R3.1 requirement to conduct a post incident analysis is sufficient to address the continual improvement of processes and technology. Finally, the last part of the measure, a procedure for "taking the important assessment steps necessary to avoid reintroducing the precipitating or corrupted data" does not seem to provide evidence of "processes to preserve data . . . for analysis or diagnosis" (Part 2.2) The measure for R2.2 requires evidence of a test when it is initially stored; the requirement no longer includes this. The measure should be modified to match the current draft of the requirement. It is not

clear whether an entity must test all information or a sample of the information to comply with this requirement. Please clarify. (Part 2.3) A recovery plan may be comprised of one overall plan with a number of underlying processes for different failure scenarios, each of which may have different variations based on the details of the failure. It is not clear whether an entity needs to test, 1) the overall plan using at least one of the underlying processes, 2) the overall plan and each underlying process, or 3) every possible variation of the plan and processes.
Yes
Yes
Yes
(Part 1.1) Why is "BES Cyber Asset" used in 1.1.2 and only Cyber Asset used in 1.1? In R1.1.3 Consider deleting “developed for the entity”. It appears that the intent is to capture all software in 1.1. As written the requirement could exclude custom software such as scripts that were originally developed for another entity. (Part 1.3) In R1.3 Greater specificity is needed regarding the documentation required under CIP -005 and CIP-007 that must be updated. We don’t believe that this requirement captures what the SDT intended. R1.5 requires updates only when the baseline is altered. For example, a network could be reconfigured significantly without any change in the baseline, but with substantial changes in network diagrams etc. R1.3 would not require an update in that case. Consider requiring an update of relevant documentation within CIP005 and CIP-007 in those standards instead of in CIP 010. (Part 1.5) R1.5.2 Consider deleting the portion of the requirement from the word “including” on. It may not be worthwhile to take measures to account for differences between the test and production requirements. Additionally, the requirement gives entities no standard about how significant the measures must be. Must they totally account for the differences (this is not achievable without completely replicating your production environment which could be prohibitively expensive). Would a single trivial measure that accomplishes little be sufficient? The requirement states that an entity must describe the measures used but does not explicitly require it to use measures (to account for differences between test and production). Would a statement that no measures were taken be adequate for compliance? Entities need a clear statement of what is expected. If the text is retained, consider allowing as an alternative a statement that the entity is aware of, and accepts the risk of, differences in the environments. (Part 3.1) R3.1 Consider deleting the reference to CIP-006 in this requirement. Entities are already required to test their systems by CIP-006 R3.1. If that test does not adequately cover the scope required we recommend you make the change there instead of having pieces of physical security testing in two separate standards. (Part 3.2) Is the scope of this VA CIP-005 and CIP-007 or did you intend to include CIP-006? We recommend excluding CIP-006 since testing of physical security systems is covered in that standard, but either way, it should be explicitly stated. (Part 3.3) R3.3 To improve clarity consider adding “to determine the extent to which the cyber security controls identified in CIP-005, and CIP-007 are implemented correctly and operating as designed.” We assume you did not intend to require a review of CIP006 at this point, but since it is not describing the scope the requirement specified, it implies that it would be the same as 3.1.
No
Yes
(Part 1.1) In R1.1 and 1.2 the addition of the words “and implemented” is redundant and confusing. The parent requirement already requires the implementation of the program. The additional bullet in the measures is also puzzling. We do not see how “Repository or designated electronic and physical location” would be evidence that an entity has established methods to identify BES Cyber System Information. (Part 1.2) R1.2. Consider changing “or” to “and” in the measures. It seems that you would want both evidence that the procedures had been established and that it was followed. (Part 1.2 and 1.3) R1.2-R1.3 It should be clarified whether a single identified instance of deviation from the Information Protection Program (either identified in the 1.3 assessment or otherwise) would be considered a violation of R1.2. If it is, then the requirement to have an action plan to remediate deficiencies would be duplicative of the entity’s mitigation plan. (Part 2.1 and 2.2) "device" should be replaced with "Cyber Asset."
Individual
Michael Lombardi
Northeast Utilities
Yes

Yes
Yes
Table R1 through R3, Applicable BES Cyber Systems and associated Cyber Assets - Recommend expanding the applicability from “High Impact BES Cyber Systems” and “Medium Impact BES Cyber Systems” to include “Associated Physical Access Control Systems,” “Associated Electronic Access Control or Monitoring Systems” and “Associated Protected Cyber Assets.”
Yes
Yes
Yes
None
None
Yes
Yes
Yes
None
Yes
Yes
Table R1, Part 1.2 - Please clarify: (1) what is meant by transit plus include exclusionary clause as to what it does not mean; (2) what records are required for handling information.
Individual
Brian J Murphy
NextEra Energy, Inc.
No
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R2.1, R3.1 and R3.2 be revised to read as follows (and delete R3.3 and R3.4 to be combined in a new R3.2): R.2.1 “Test the BES Cyber Security Incident response plan(s) at a timeframe deemed necessary by the Responsible Entity: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise; or • With a full operational exercise.” R.3.1 “Review and update each Cyber Security Incident response plan for accuracy and completeness at a timeframe deemed necessary by the Responsible Entity.” R.3.2 “Maintain a current and up-to-date Cyber Security Incident Response Plan, including (1) the documentation of any lessons learned associated with a Cyber Security Incident test or actual incident response; (2) roles or responsibilities; (3) cyber Security Incident response groups or individuals or (4) technology changes.”
No
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R2.1, R2.2, R2.3 and R3.1 be revised to read as follows (and delete R3.2 and R3.3 that will be combined into a new R3.1) R2.1 “Test the recovery plan(s) referenced in Requirement R1 at a timeframe deemed necessary by the Responsible Entity: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.” R2.2 “Test information used in the recovery of BES Cyber Systems that is stored on backup media at a timeframe deemed necessary by the Responsible Entity to ensure that the information is useable and is compatible with current system configurations.” R2.3 “Test each of the recovery plans referenced in Requirement R1 at a timeframe deemed necessary by the Responsible Entity through an operational exercise of the

recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise." R.3.1 "Maintain a current and up-to-date Recovery Plan, including (1) the documentation of any lessons learned associated with a Cyber Security Incident test or actual incident response; (2) roles or responsibilities; (3) cyber Security Incident response groups or individuals and (4) technology changes."
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R2.1, R2.2, R2.3 and R3.1 be revised to read as follows (and delete R3.2 and R3.3 that will be combined into a new R3.1) R2.1 "Test the recovery plan(s) referenced in Requirement R1 at a timeframe deemed necessary by the Responsible Entity: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise." R2.2 "Test information used in the recovery of BES Cyber Systems that is stored on backup media at a timeframe deemed necessary by the Responsible Entity to ensure that the information is useable and is compatible with current system configurations." R2.3 "Test each of the recovery plans referenced in Requirement R1 at a timeframe deemed necessary by the Responsible Entity through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise." R.3.1 "Maintain a current and up-to-date Recovery Plan, including (1) the documentation of any lessons learned associated with a Cyber Security Incident test or actual incident response; (2) roles or responsibilities; (3) cyber Security Incident response groups or individuals and (4) technology changes."
No
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R3.1 be revised to read as follows: "At a timeframe deemed necessary by the Responsible Entity, conduct a paper or active vulnerability assessment to determine the extent to which the cyber security controls identified in CIP-005, CIP-006, and CIP-007 are implemented correctly and operating as designed."
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R1.3 be revised to read as follows: "At a timeframe deemed necessary by the Responsible Entity, assess adherence to its BES Cyber System Information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment."
Group
Florida Municipal Power Agency
Frank Gaffney
Yes
No
No
1- QUESTION 2: We believe there is a typo in bullet 2.2, the "of" in the first sentence should be an "or". Bullet 2.3 is a data retention requirement that is a compliance element, not a requirement (especially in light of paragraph 81 of the FERC Order approving FFTR), and should be deleted. 2- QUESTION 3: Bullets 3.3 and 3.4 cover change management of the Cyber Security Incident response plan and Bullet 3.1 is duplicative and should be deleted (especially in light of paragraph 81 of the FERC Order approving FFTR). Alternatively, bullets 3.3 and 3.4 can be deleted in favor of bullet 3.1. Bullet 3.2 belongs in R2, not R3.

No
Yes
Yes
1- QUESTION 5: Bullet 1.4 uses an ambiguous term “verify”. Does “verify” mean that the information is retrievable from the back-up media, or does it mean that it is identical to the original information? If the latter, then R2 bullet 2.2 is not needed.
Yes
Yes
Yes
Yes
Yes
Group
National Rural Electric Cooperative Association (NRECA)
Barry Lawson
No
R1.3 – NRECA requests clarification regarding whether “deficiencies identified during the assessment” are considered violations of the standard. NRECA believes these deficiencies should not be considered violations and requests that the SDT make this clear in the requirement language.
Group
Pepco Holdings Inc & Affiliates
David Thorne
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Yuling Holden
PSEG
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
R3 - the VSL does not address the 36 month timeline in Requirement 3.2 and only the timelines in R3.1. We suggest adding a modification via an "or" statement in all VSLs • Low- An active vulnerability assessment of High Impact BES Systems was completed more than 36 months but less than 39 months since the last one • Medium- An active vulnerability assessment of High Impact BES Systems was completed more than 39 months but less than 42 months since the last one • High- An active vulnerability assessment of High Impact BES Systems was completed more than 42 months but less than 45 months since the last one • Severe- An active vulnerability assessment of High Impact BES Systems was completed more than 45 months since the last one
No
Yes
Measure for R1.2: This measure does not specify what records could be used to indicate consistency with the entity's documented procedures. Please provide guidance as to what acceptable methods could be used for compliance – would sampling work in this case, and if so, what is the acceptable tolerance range for such sampling?
Group
Western Area Power Administration
Brandy A. Dunn
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
No
Yes
Yes
Individual
Daniel Duff
Liberty Electric Power, LLC
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
No
No
The definition of BES Cyber Information needs to be made clearer regarding assets such as relay test laptops which may leave the control of the RE.
Individual
Don Jones
Texas Reliability Entity
Yes
Yes
No
CIP-008-5 R2 fails include “each” of the applicable items.
No
Yes
Yes
CIP-009-5 R3 does not include defined roles and responsibilities.
No
Yes
No
CIP-010-1 R1 (1.2) does not indicate the appropriate authorizing individual or delegate. CIP-010-1 R3 does not always include Medium Impact in its scope. CIP-010-1 R3 does not define what is comprised by an active vulnerability assessment. CIP-010-1 R3 does not include an annual review, but only enforces a review every 36 calendar months.
No
Yes
CIP-011-1 R1 does not mandate the identification of protected information (e.g. confidential).
Individual
Don Schmit
Nebraska Public Power District
Yes
No
Yes
Overall it seems as if the standards writers are attempting to work out some subjectivity and ambiguity issues in regards to establishing sufficiency in meeting the requirements of the standards. I do not believe that they have fully resolved these issues. CIP 8 R2.2 – VSL must change for this such that it is not a violation if the incident response plan is not followed for an actual event. The requirement to document deviations is sufficient to meet the intended goal of ensuring the currency of the plan and updating it to reflect things discovered during actual incidents or drills. CIP 8 r3.1 – Suggest strike “and update” to IR plan review. It is possible that the plan is found sufficient after the review and would not require an update. Suggest verbiage “update, if necessary.” CIP 8 r3.5 – Suggest striking “distribute”. What constitutes distribution? Suggest retaining “notification” approach.

Distributing CIP protected data could pose technical issues, especially outside vendors. Notification, as long as the vendor had access would eliminate the need to actually distribute the plan to affected individuals.
No
No
Yes
Once again it is straightforward to see the objectives the drafters are trying to accomplish, but the reality of this level of descriptiveness and compliance thereof, would be disruptive and prohibitive. CIP 9 r1 – The standard isn't clear whether the recovery plans are for recovery of the asset, system, or function. CIP 9 r1.4 – Recommend striking associated physical access control systems and associated electronic access control systems from the applicability section. The wording of the requirement is unclear. What constitutes "initial," "verification," or "ensure the process completed successfully"? Suggest prescriptive wording if these terms are to be used. The current draft verbiage leaves too much up to the subjective interpretation of the auditor, and, if intended to be a daily or weekly check, could be administratively burdensome. Proposed Verbiage to align with FERC order 706: "Within the capabilities of the backup system and upon completion of a significant production change within a BES Cyber System, such as adding a new form of hardware or significant new software, data essential to BES Cyber System recovery that is stored on backup media shall be verified at the time the backup is created. Verification means the automated process typically incorporated into the automated backup process validates the bit count or similar technical function." CIP 9 r1.5 – Without tying this requirement to a Cyber Security Incident, there will be no forensic value in retaining the data if the event was not related to any malicious attempt. Proposed Verbiage: "Processes to preserve data, except for CIP Exceptional Circumstances, for analysis or diagnosis of the cause of a Cyber Security Incident that triggers activation of the recovery plan(s)." CIP 9 r2.1 - Are the tests specified in R2 required for each cyber asset, cyber system, or each plan? In other words, does an entity need to do a "full operational exercise" on all systems, or is a representative sampling sufficient? CIP 9 r2.2 – Is this in reference to the applications and other binaries used to restore or the actual plan itself? Suggest clarification. CIP 9 r2.3 – Is this requirement implying the need for a bare-metal restore for all CIP assets? Doing so would be cost-prohibitive and potentially jeopardize the stability of the BES. Some CCAs utilize a "standby" system for testing. CIP 9 r3.4 – Once again the use of the word "distribution". If I notified a vendor of an update to the plan stored in CIP protected area, it would achieve the objective without the burden of any CPI issues in its "distribution".
No
No
No
CIP 10 r1.1.3 – Proposed verbiage: "Any custom compiled software" CIP 10 r1.4 – Propose striking 1.4.1 to eliminate speculation or an implicit requirement to have a testing environment outside of 1.5. Instead, the CIP-005, CIP-006, and CIP-007 list should be moved to 1.4.2. This strike also removes the inflexibility as it relates to emergency change that exists in the current draft verbiage. In the absence of striking 1.4.1, recommend adding the CIP Exception Circumstances verbiage to 1.4 to allow emergency changes necessary to ensure operability/reliability. For those circumstances, 1.4.2 should suffice. CIP 10 r2.1 – Recommend replacing "technically feasible" with "Within the capabilities of the system or network configuration." Recommend striking the associated systems and cyber assets and leaving this to High Impact BES Cyber Systems with External Routable Connectivity. This also exceeds FERC 706, so we recommend increasing the interval of change detection to an annual or quarterly verification, because a manual process of verifying the baseline will be administratively burdensome. CIP 10 r3 – What is the definition of an "active vulnerability assessment"? What would be considered an appropriate infeasibility for performing such a test? Would the entity need to perform an "active vulnerability assessment" on all systems, or is a representative sampling sufficient? Recommend striking "CIP-006" from the list of cyber security controls assessed, as this is duplicative of the testing and maintenance requirement but increases the interval to annual instead of every 24 months.
Yes
Yes
[R1.1] Recommend striking the first bullet in the Measures or changing it to indicate that a label of

“confidential” is sufficient. The current measure is phrased such that it requires information to be labeled as CIP information, instead of just confidential. This increases the chances that someone will know how to use it maliciously if they do get unauthorized access to it. Suggest legacy verbiage indicating a classification in alignment with “confidential.” The current verbiage did not prevent organizations from assigning a “CIP Confidential” label to documentation or preclude a protection program that had only one level of protected information. [R2.1 and 2.2] Recommend striking “chain of custody” to avoid connotations associated with legal definitions of this term that should not apply here. If the intent is to ensure positive control of the device until the information is removed, the phrasing should be in alignment with that. This phrasing should also allow secure methods of transport to the vendor if that is required within support contracts.
Group
Luminant
Rick Terrill
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
Individual
Stephanie Monzon
PJM Interconnection
Yes
No
No
R2 – This comment actually applies to all CIP requirements in that an expanded glossary would be extremely helpful. Much of the discussion surrounding the review of requirements is trying to determine NERCs meaning of a word vs our meaning of a word. Here in CIP 8 R2 & R3 we picked out records, technology change, and routable. If we knew what NERC’s intent of what that means we would be better prepared to understand how our measures met the requirement. The meanings of words are also situational from requirement to requirement. The words restore & recovery mean different things depending on the area being examined R3 – Please ensure that the verbiage on “any changes” more in line with CIP 9
No
No
No
R2 – This comment actually applies to all CIP requirements in that an expanded glossary would be extremely helpful. Much of the discussion surrounding the review of requirements is trying to determine NERCs meaning of a word vs our meaning of a word. Here in CIP 9 R1, R2 & R3 we picked out recover, restore, operational exercise, & technology change. If we knew what NERC’s intent of what that means we would be better prepared to understand how our measures met the requirement. The meanings of words are also situational from requirement to requirement. The words restore & recovery mean different things depending on the area being examined R3 The following phrasing is helpful and similar verbiage should be used elsewhere when referencing evidence: Evidence may include, but is not limited to, dated documentation reflecting changes made to the recovery plan(s) in response to the following changes that the responsible entity determined would impact the plan or the ability to execute the plan: • Roles or responsibilities; or • Technology changes.
No

No
No
R1.1 Port should be updated to say ports & services This comment actually applies to all CIP requirements in that an expanded glossary would be extremely helpful. Much of the discussion surrounding the review of requirements is trying to determine NERCs meaning of a word vs our meaning of a word. Here in CIP 10 R1 we picked out Baseline & differences in operation.. If we knew what NERC's intent of what that means we would be better prepared to understand how our measures met the requirement. The meanings of words are also situational from requirement to requirement. Baseline could be implemented many different ways depending on a company's individual strategy R1.5.1 By using the word "model" rather than identical we assume that there is flexibility with the differences between the state and scope of production vs test R2.1 Remove the words continually, it insinuates real time monitoring This can be interpreted as not needing to self report and no remediation necessary R3 Please clarify what is meant by Electronic Access Control or Monitoring Systems R3.3 A cyber asset can be placed into an ESP before remediations of identified vulnerabilities? R3.4 "the planned date of completing the action plan" - is this the completion of the formulation of the plan or the completion of the tasks within the plan?
No
No
R1.2 – "One or more documented and implemented procedures for handling BES Cyber System Information, including storage, transit, and use." Should be for the secure handling of BES Cyber.....
Group
Edison Electric Institute
David Batz
(1.) In all requirements in all standards, and in rationale & guidelines, remove references to systems & assets and rely on the applicability column to specify applicability. Replace globally with Applicable Cyber Systems in rationale and guidance. (2.) In all measures section remove the term 'but not limited to' (3.) Change all instances of Medium Impact BES Cyber Systems to 'Medium Impact BES Cyber Systems with External Routable Connectivity' for consistency with CIP-005, CIP-006, and CIP-007 (4.) CIP-008 R1.2 requires the Plan to have: A process to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident. The definition of Reportable Cyber Security Incident is in the definitions as 'Any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.' As written the Entity is to develop a process to determine if a cyber security incident compromises or disrupts a reliability task. Suggested changes to definition of Reportable Cyber Security Incident, to also be included in the requirement a. Suggestion 1) Any Cyber Security Incident that has disrupted the operation of the BES resulting in a violation of a SOL or IROL. b. Suggestion 2) Any Cyber Security Incident that has compromised or disrupted the operation of the BES and requires reporting per EOP-004. (5.) R2 - Allow for an exception to the time frames listed in the event of CIP Exceptional Circumstances (6.) R2.1 a. Remove the word 'BES' from the Requirement to be consistent with R1. b. Remove the words 'lessons-learned report that includes a' from the Measures because the following items do not necessarily fall into the lessons learned category. c. Add a 2nd Measure 'OR documentation from an actual Reportable Cyber Security Incident' as an alternative to the listed evidence. (7.) R3.1: Change the Requirement to read 'Review and update each Cyber Security Incident response plan for accuracy and completeness once each calendar year or a period not to exceed 15 calendar months between reviews except for CIP Exceptional Circumstances.' Rationale: Reduce significant confusion (8.) R3.2 a. Clarify Requirement as follows: 'R.3.2 'Maintain a current and up-to-date Cyber Security Incident Response Plan that (1) includes or references, as appropriate, documentation of any lessons that may have been learned in connection with a Cyber Security Incident test or actual incident response performed pursuant to CIP-008-5 R2, within 90 days of the performance of such test or actual incident response; and (2) includes changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change.' b. Clarify Measures as follows: 'Evidence may include, but is not limited to, a dated, revised Cyber Security Incident Response Plan(s) that (1) includes or references, as appropriate, dated documentation of lessons learned, if any, associated with tests of or actual responses using the Cyber Security Incident Response Plan(s), within 90 days after completion of such test or actual incident response; and (2) reflects changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change.' (9.)

R3.3 & R3.4: Remove these requirements as they are now incorporated into the proposed R3.2.
(1.) In all measures section remove the term 'but not limited to' (2.) In 'Guidelines and Technical Basis' section, list specific FAQs and CIPC guidelines that are applicable. (3.)Remove 'Associated'Systems' from R1-R3 because Order 706 does not require them. (4.) R1.4: a. Replace Requirement language with 'Upon completion of a significant production change within a BES Cyber System, such as adding a new form of hardware or significant new software, information essential to BES Cyber System recovery that is stored on backup media shall be verified at the time the backup is created. Verification means the automated process typically incorporated into the automated backup process validates the bit count or similar technical function.' b. Measures i. What is the evidence retention period' 90 days' Old backup logs are not relevant. ii. What is the evidence of verification' (5.) R1.5 a. In the requirement, replace the word 'event' with 'Cyber Security Incident'. b. In the requirement, add the words 'when it does impact reliability' to the end. (6.) R2.1: Modify the first part of the requirements language to read 'Test a representation of the recovery plans(s) referenced in Requirement R1 once each calendar year or not more than 15 calendar months between tests except for CIP Exceptional Circumstances.' Rationale: Reduce significant confusion. (7.) R2.2 a. Change the first 3 words of the requirement to read 'Test representative information'. b. Measures: Remove the words 'when initially stored and' to be consistent with the requirement. (8.) R2.3: Change the 2nd word 'each' to 'a representation' in the requirement. (9.) R3: In Order 706, paragraph 731, FERC stated 'We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective.' We believe that updates to the plan are not effectively in place until it has been communicated, and that it will be more efficient for entities to track one date rather than four date requirements included in draft 2. We propose consolidation of the four subparts of R3 into one subpart that ensures up-to-date recovery plans and communications within the 90 days required in FERC 706 but is less prescriptive and less of a documentation burden. Delete R3.2, R3.3 and R3.4 and use the following text for R3.1: 'Update recovery plan(s) and communicate the updates within 90 calendar days of a test, actual recovery or changes that impact the ability to execute the plan. Updates from tests or actual recovery shall include lessons learned. R3 MEASURES: With the consolidated R3.1 requirement, the following is proposed for measures: 'Evidence may include, but is not limited to: 1) revised recovery plan(s) that include dated references to lessons learned from tests, actual recovery or changes that impact the ability to execute the plan; 2) dated emails, newsletters, training or other communications regarding the plan updates.' R3 VSLs: Replace the draft 2 VSLs with the following. Lower VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 90 and less than 120 days of the change, test or actual recovery. Moderate VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 120 and less than 150 days of the change, test or actual recovery. High VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 150and less than 180 days of the change, test or actual recovery. Severe VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 180 and less than 210 days of the change, test or actual recovery. R3 GUIDANCE: Add the following to guidance: 'Individuals responsible for activating and implementing a recovery plan should have information needed to recover their assets. R3 is meant to ensure recovery plans are up to date and available to individuals who need them. The following are examples of items that might require updates and communications within the 90 day timeline: * changes needed as a result of lessons learned from a test or actual recovery; * changes in roles and responsibilities.'
(1.) In all requirements, remove references to systems & assets and rely on the applicability column to specify applicability. (2.) In all measures section remove the term 'but not limited to' (3.) R1 is too prescriptive. Recommend that the CIP v3/v4 language replace 1.1-1.4, but specifically address the Order 706 requirements for malicious changes. (4.) R1: remove Associated assets/systems from applicability because they represent an increase in scope from CIP v3/v4 (5.) R2: remove Associated assets/systems from applicability because they go beyond Order 706. (6.) R1.1-R1.4: Add 'with External Routability' to Medium Impact BES Cyber Systems (7.) R1.4: Remove 'High Impact' from Applicability because it is repetitious with R1.5. (8.) R3.1, R3.4 a. Applicability: Add 'with External Routability' to Medium Impact BES Cyber Systems and Associated Protected Cyber Assets. b. Requirement: Change to read: 'At least once every calendar year, or up to 15 months between

assessments, conduct a paper and/or active vulnerability assessment to determine the extent to which the cyber security controls are implemented correctly and operating as designed. Any paper and/or active vulnerability assessment already performed in the implementation of other CIP standards are not included in this requirement'. Rationale: avoid double jeopardy. (9.) R3.2: Remove the words 'that models the baseline configuration of the BES Cyber System in a production environment' after the parentheses. (10.) R3.3: Change the words 'prior to adding' to 'as part of the change prior to completing the commissioning of'. Rationale: clarity (11.) R3.4: Change the requirement to read: 'Document identified vulnerabilities. Establish planned or completed dates relating to the mitigation or remediation of identified vulnerabilities.' Rationale: As worded, the language increases the compliance-tracking burden to all sorts of other documentation including action plans, plan status, etc. The proposed language shifts the focus of the requirement back towards a cyber security related outcome, i.e. mitigated vulnerabilities. This is accomplished by staying away from language that requires documentation overhead. Language on action plans should be moved into the guidance documentation.
(1.) In all requirements, remove references to systems & assets and rely on the applicability column to specify applicability. (2.) In all measures sections in all standards and requirements remove the term 'but not limited to' The default should be an 'or', and any 'and' should be explicit. Rationale: these are examples only. Using the 'limited to' language creates confusion about whether they're necessary or sufficient. (3.) Applicability for all requirements should be changed from 'Medium Impact BES Cyber Systems' to 'Medium Impact BES Cyber Systems with External Routable Connectivity' (4.) Several requirements use the terminology 'BES Cyber System Information', however this creates an inconsistency with all the 'Associated' assets in the Applicability column. Suggestion is to leave the applicability in that column, and don't name asset/system types in the requirement. (5.) The length of the 'Applicability' column title can cause confusion about the systems/assets that are within scope. Suggest changing the column heading to 'Applicability'. (6.) R2 uses the term 'chain of custody' in several places. This is a legal term that relates to evidence, and is not appropriate in the CIP standards. EEI strongly suggests replacing it with 'possession' or 'control'. (7.) R1.3: Change Requirement & Measure language time frames by removing 'at least' and replacing with 'once each calendar year or a period not to exceed 15 months'. (8.) R2.1: In parenthetical text in Requirement change to read '(except for reuse in other high impact)' for clarity.
Individual
Kathleen Goodman
ISO New England Inc.
No
No
No
Request clarification on the EOP-004-2 reference in the R1 Rational. The previous version of EOP-004-2 was not accepted by the industry. What is the plan if future versions of EOP-004-2 are not accepted? Recommend changing the first bullet in R2 Part 2.1 from “By responding to an actual Reportable Cyber Security Incident; ” to “By responding to a Cyber Security Incident” since this covers the Reportable Incidents plus the non-reportable incidents Recommend updating R2 Part 2.3 since the existing language does specify a retention period. Recommend changing R3 Part 3.1 from “Review and update” to “Review and update, as needed,” since some years the Cyber Security Incident response plan will not need updating Recommend changing R3 Part 3.3 from “Update the Cyber Security Incident response plan ” to “Update, as needed, the Cyber Security Incident response plan”. For R1.3, and R1.4 wording needs to be added to state that physical security incidents need to be included as well as for Cyber Security Incidents.
No
No
No
Recommend removing R1 Part 1.5 since this Requirement is forensics and/or Lessons Learned. The priority is Reliability or recovery, forensics. The title of this Standard is Recovery Plans for BES Cyber Systems. Request clarification on R2 Part 2.2. Is this a media test? Can the test be on a sample BES Cyber System? Recommend updating the Measure for R2 Part 2.3 to reference an updated

Implementation Plan's Initial Performance of Certain Period Requirements. This Requirement – Part combination is not identified in the existing Periodic Requirements. As requested in the first posting, request removing these bookends from this Measure. Recommend changing from the reference from "R1.2" to "Part 1.2" in R3 Part 3.4 for correctness.
No
No
No
Request clarification of R1 Part 1.1.2. Does "applications" mean "SCADA, EMS, State Estimator, IDC, etc." instead of "device drivers, DLL, applications included in an operating system or package, etc.?" Request clarification of R1 Part 1.1.3. Would a version control tool/system (like CVS) demonstrate the custom software's version? Request clarification on R1 Part 1.3. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005 and CIP-007? In R1 Part 1.3, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations. Recommend removing the 30 day time frame in R1 Part 1.3 that applies to CIP-005 and/or CIP-007. Those Standards should specify their time frames. Recommend that the 30 days apply to only updating the baseline configuration (this Part). Request clarification on R1 Part 1.4.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? In R1 Part 1.4.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations. Recommend removing R1 Part 1.4.2 because "availability" has not been part of the Requirements in the past, is not a FERC requirement and can be interpreted multiple ways. In R1 Part 1.5, recommend changing from "Where technically feasible, for each change that deviates from the existing baseline configuration " to "Testing cyber security control, where technically feasible, for each change that deviates from the existing baseline configuration" for clarity. For R2 Part 2.1, recommend the previous Version 5 words since this updated Part is not understandable. Request clarification on R3 Part 3.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? In R3 Part 3.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations. Recommend that R3 Part 3.1start with its purpose – for example, Active vulnerability assessment. Request clarification on R3 Part 3.2. If this is a paper exercise it should be performed once every 36 months. Recommend that R3 Part 3.2 start with its purpose – for example, "Perform active vulnerability assessment, where technically feasibly….". Recommend that R3 Part 3.3 start with "Perform an active vulnerability assessment, of the new cyber assets prior to business deployment, except for CIP Exceptional Circumstances and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset)." Recommend updating CIP-010 R1's Violation Risk Factor in the Table of Compliance Elements. That VRF is "medium" while the Requirements and Measures shows R1 as "low". Recommend updating CIP-010 R2's Violation Risk Factor in the Table of Compliance Elements. That VRF is "medium" while the Requirements and Measures shows R2 as "low".
Yes
No
The second paragraphs of R2 Parts 2.1 and 2.2 are the same, Recommend removing them from Parts 2.1 and 2.2, and make a new Part 2.3 for clarity.
Individual
Christina Conway
Oncor Electric Delivery Company LLC
No
No
No
CIP-008-5 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-008-5 R1, R2 and R3 to "Medium Impact BES Cyber Systems" should be limited to "Medium Impact BES Cyber Systems with External Routable Connectivity or Dial-up Connectivity." This modification would support the current applicability and Oncor's proposed changes to the applicability of CIP-005-5, CIP-006-5 and CIP-007-5 and would align the incident response plan to those cyber systems that have connectivity.

R2 REQUIREMENT COMMENTS: CIP-008-5 R2.3 requires retention of relevant records and should be relocated to Section C1.2 regarding Evidence Retention. R3 REQUIREMENT COMMENTS: The 30-day timing requirement in CIP-008-5 R3.4 should be extended to 60 calendar days such that the overall timing for the activities in CIP-008-5 R3 is more reasonable. This would allow for a consistent 90-day timeline for planned changes as well as responses to Cyber Security Incidents. GENERAL COMMENTS: (1) Oncor supports the comments submitted by EEI in response to this question. (2) Oncor supports the comments submitted by the Texas RE NERC Standards Review Subcommittee in response to this question.
No
Yes
No
R1 APPLICABILITY COMMENTS: (1) Oncor proposes that the applicability of CIP-009-5 R1.1, R1.2, R1.3 and R1.5 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems at Control Centers.” This will concentrate efforts on areas where reliability impacts are the highest and avoid placing additional/duplicate requirements on cyber systems/assets covered under the PRC Standards. (2) The misoperation of relaying systems is covered under the PRC Standards and should be excluded from CIP-009-5 R1.5. R3 REQUIREMENT COMMENTS: The 30-day timing requirement in CIP-009-5 R3.3 should be extended to 60 calendar days such that the overall timing for the activities in CIP-009-5 R3 is more reasonable. This would allow for a consistent 90-day timeline for planned changes as well as lessons learned from the use/testing of the recovery plan. GENERAL COMMENTS: (1) Oncor supports the comments submitted by EEI in response to this question. (2) Oncor supports the comments submitted by the Texas RE NERC Standards Review Subcommittee in response to this question.
No
No
No
R1 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-010-1 R1.1, R1.2, R1.3 and R1.4 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems at Control Centers.” As the requirements are currently written, they mandate the creation of an asset register for a large population of cyber assets that are not connected to a network via a routable protocol and are already covered under the PRC Standards. This will place an undue burden on the Responsible Entity without enhancing reliability. R1 REQUIREMENT COMMENTS: Oncor proposes that the 30-day timeline in CIP-010-1 R1.3 should be extended to 90 days (or removed) to allow for sufficient time to process/document the required changes and verifications. R2 REQUIREMENT COMMENTS: Oncor proposes that the 35-day timeline in CIP-010-1 R2.1 should be extended to 90 days to allow for a quarterly review process. R3 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-010-1 R3.1 and R3.4 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity or Dial-up Connectivity.” This modification would eliminate existing discrepancies between the applicability of CIP-005, CIP-006, and CIP-007 and the applicability of CIP-010. This modification also supports Oncor’s proposed applicability of CIP-005-5 and CIP-007-5 such that the vulnerability assessments are directed towards cyber systems with connectivity. GENERAL COMMENTS: (1) Oncor supports the comments submitted by EEI in response to this question. (2) Oncor supports the comments submitted by the Texas RE NERC Standards Review Subcommittee in response to this question.
No
No
R1 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-011-1 R1.1, R1.2 and R1.3 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity” to maintain consistency with the scope of cyber systems/assets currently covered by similar requirements in the CIP version 4 Standards. The inclusion of cyber systems/assets with no routable connectivity will significantly increase documentation requirements with no benefit to reliability. R2 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-011-1 R2.1 and R2.2 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity” to maintain consistency with the scope of cyber systems/assets currently covered by similar

requirements in the CIP version 4 Standards. The inclusion of cyber systems/assets with no routable connectivity will significantly increase documentation requirements with no benefit to reliability. GENERAL COMMENTS: (1) Oncor supports the comments submitted by EEI in response to this question. (2) Oncor supports the comments submitted by the Texas RE NERC Standards Review Subcommittee in response to this question.
Group
SMUD & BANC
Joe Tarantino
No
No
No
1. The requirement to document deficiencies or lessons learned Part 3.1 is counter-productive because the requirement will encourage entities to fail to admit that there is a deficiency or lesson in the first place. In the absence of Part 3.1, an entity is more likely to update its plan immediately based upon any newly discovered deficiency. Further, Part 3.1 duplicates the work in the periodic review. In any periodic review, entities will be aware of recoveries made during the period in question and will update their plans accordingly. 2. Enforcement of the provisions 3.1 and 3.2 will be questionable at best, because it is possible that when the plan was exercised, it worked as intended without any identified deficiencies or lessons to be learned. While not stated in the requirements, the entity is left to wonder whether or not it would be in violation if it were not to identify something, and may force the entity to document that the plan worked as intended. This is unnecessarily burdensome to the entity. It is sufficient to have a requirement that the Recovery Plan exists and that it is reviewed for possible changes within prescribed time periods. 3. Exercise of a Recovery Plan does not necessarily lead to the need to update it. Entities will still have the option to update the plan if deficiencies are discovered between the periodic reviews. 4. For 3.1 and 3.2 there really isn't a need for two steps, two separate documents, and time frames for compliance. The same value would be achieved by combining 3.1 and 3.2 into a single item – which is to simply update the test plan within a fixed time frame as a result of deficiencies or lessons learned. Itemized deficiencies or lessons learned could be included in plan document itself. A change log in the Recovery Plan document would accomplish this function. Having two requirements instead of one causes unnecessary exposure to the entity for violations and introduces burdensome administration tasks that are not necessary. Simple is better. 5. Requirement 3.1 states that identified deficiencies or lessons learned from the recovery plan test or incident recovery be documented within 30 calendar days after completion of the test or recovery. Requirement 3.2 requires that the recovery plan be updated based upon any documented deficiencies or lessons learned within 30 calendar days after the documentation required by Part 3.1. This approach has the unintended consequence of encouraging entities to delay the documentation of deficiencies or lessons learned to the end of the 30 day period defined in Part 3.1, because the 30 day period in Part 3.2 to update for the plan begins at the moment the entity documents the Part 3.1 deficiencies. This is a penalty for acting quickly. The approach also makes tracking for compliance overly complicated. To correct this, the periods for both 3.1 and 3.2 should begin as of the date of the completion of the test or recovery. To have similar timeframes without penalizing the entity for acting quickly, the period for 3.1 should begin the day after completion of the test or recovery and be 30 days long. Similarly, the period in which to update the Recovery Plan should begin the day after completion of the test or recovery and be 60 days long.
In Part 1.4, the change to the Measures that change the words "dated evidence of the verification that the backup process completed successfully" to "dated evidence or logs confirming that the backup process completed successfully" is an improvement. It is still not clear, however, that the word "logs" means that employee confirmation that the backup process completed successfully is sufficient. Logs typically imply that there is a requirement for system generated proof. SMUD's original comment is that requiring dated system generated evidence … results in unnecessary administrative burden to the entity because of the never ending need to collect and store evidence repeatedly for many systems. Employee verification that the backup and verification processes were completed via a time-stamped workflow should be sufficient evidence. A: Our comment for this requirement is similar to the prior draft. Changes were made by the team, but our concern regarding administrative burden were not addressed by the change. B: In Part 2.3, in the measures, the

wording change from “initially upon the effective date of the standard” to ”prior to the effective date of the standard” implies that evidence generated prior to the effective date of the standard can make the difference between complying or not complying with the standard. This leads to inadvertently requiring entities to do something prior to the effective date of the standard in order to comply. The new wording addresses our prior issue, but the Measures cannot reference activities that pre-date the effective date of the standard. Everything else looks OK.
No
No
R1: Part 1.4.2 requires the entity to verify that the “required controls and BES Cyber System availability” are not adversely affected. It doesn’t make sense to require the entity to verify BES Cyber System availability resulting from the change. Whenever there is an availability problem, it will be detected and acted upon when it occurs. A future availability problem cannot be verified before it occurs. It is suggested that the phrase “BES Cyber System availability” be removed from this requirement. Part 1.5.2 places an excessive administrative burden on the entities. R2: In Part 2.1, the language “not to exceed once every 35 calendar days” can be interpreted to mean that this cannot be done more than once every 35 days. This is obviously not the intent.
Individual
Andrew Gallo
City of Austin dba Austin Energy
No
No
No
CIP-003, R2 requires that low impact assets have a cyber security policy that addresses incident response to a BES Cyber Security Incident. CIP-008 deals with the creation of a cyber security incident response plan. Accordingly, CIP-008, Table R1, Parts 1.4 and 1.5 should include low impact assets. Additionally, please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
No
Yes
No
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
No
Yes
No
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
No
No
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Group
Southern California Edison Company
Nathan Smith
Yes
Yes
Yes
SCE Comments to CIP-008-5 Please revise R3.4 to define “Technology changes” as changes to the internal environment that impact existing BES Cyber Systems.

Yes
Yes
Yes
No comments
No comments
Yes
Yes
Yes
SCE Comments to CIP-010-1 -R1.1 Please add the following flexibility to the “Effective Dates” Section as it is difficult to do accurately within the currently planned implementation window: “CIP-010-5, Requirement R1.1 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. “ As we are sure the SDT is aware, the automation required to manage the base line configuration may impact Cyber Assets processor speeds, thus making the BES react more slowly.
Yes
Yes
SCE Comments to CIP-011-1 -R2.1 Please revise as follows: “…BES Cyber System Information (except redeployment in other high impact or medium impact BES Cyber Systems…” -R2.2 Please add the word “applicable” in front of “Cyber Asset” globally in the requirement.
Individual
Scott Miller
MEAG Power
Yes
Yes
Yes
In R1 Part 1.5, the reference to forensics should not be part of the CIP-009 Standard
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Heather Laws
Portland General Electric
Yes
Yes
Yes
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI’s suggestions to strengthen the wording of this standard.

Yes
Yes
Yes
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
Yes
Yes
Yes
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
Yes
Yes
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
Individual
Brian Evans-Mongeon
Utility Services Inc.
Yes
Yes
Yes
No Comments
No
Yes
Yes
Utility Services supports the comments made by MMWEC for CIP-009-5 T1, Part 1.5.
No
Yes
Yes
Utility Services supports the comments made by MMWEC in their Comments regarding CIP-010-1 R2.
Yes
Yes
Utility Services supports the comments made by MMWEC in their Comments for CIP-007-5 R2.1 and R2.2.
Individual
John Allen
City Utilities of Springfield, MO
No

No
No
City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. We agree with the comments from SPP and APPA and believe the requirements are getting close to being acceptable for those cyber systems that could cause a significant impact to the BES. However, we cannot support this Standard due to the onerous requirements for a small entity's Control Center that are considered a threat to reliability due to their connectivity to High Impact Control Centers. We could support a standard that has programmatic requirements for these small Control Centers. See our response to Comment Form A, question 3.
No
No
No
City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. We agree with the comments from SPP and APPA and believe the requirements are getting close to being acceptable for those cyber systems that could cause a significant impact to the BES. However, we cannot support this Standard due to the onerous requirements for a small entity's Control Center that are considered a threat to reliability due to their connectivity to High Impact Control Centers. We could support a standard that has programmatic requirements for these small Control Centers. See our response to Comment Form A, question 3.
No
Yes
No
City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. We agree with the comments from SPP and APPA and believe the requirements are getting close to being acceptable for those cyber systems that could cause a significant impact to the BES. However, we cannot support this Standard due to the onerous requirements for a small entity's Control Center that are considered a threat to reliability due to their connectivity to High Impact Control Centers. We could support a standard that has programmatic requirements for these small Control Centers. See our response to Comment Form A, question 3.
No
No
City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. We agree with the comments from SPP and APPA and believe the requirements are getting close to being acceptable for those cyber systems that could cause a significant impact to the BES. However, we cannot support this Standard due to the onerous requirements for a small entity's Control Center that are considered a threat to reliability due to their connectivity to High Impact Control Centers. We could support a standard that has programmatic requirements for these small Control Centers. See our response to Comment Form A, question 3.
Individual
Steve Karolek
Wisconsin Electric Power Company
No
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Calendar year and 15 months are mutually exclusive. This requirement should use the term "Annual" as applied in NERC CAN-0010. Further, the term Annual should be added to the NERC Glossary of Terms.

No
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Calendar year and 15 months are mutually exclusive. This requirement should use the term "Annual" as applied in NERC CAN-0010. Further, the term Annual should be added to the NERC Glossary of Terms.
No
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Calendar year and 15 months are mutually exclusive. This requirement should use the term "Annual" as applied in NERC CAN-0010. Further, the term Annual should be added to the NERC Glossary of Terms.
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Calendar year and 15 months are mutually exclusive. This requirement should use the term "Annual" as applied in NERC CAN-0010. Further, the term Annual should be added to the NERC Glossary of Terms.
Group
Dairyland Power Cooperative
Tommy Drea
Yes
No
Yes
Please see MRO NSRF comments.
No
No
Yes
Please see MRO NSRF comments.
No
No
No
Please see MRO NSRF comments.
Yes
Yes
Please see MRO NSRF comments.
Group
Progress Energy
Jim Eckelkamp
No
No
No
Progress Energy agrees with EEI comments with the modified and additional comments below: R1= Comment: Need to change the definition for Cyber Security Incident Progress Energy agrees with EEI comments with the modified and additional comments below: Original: Any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. Proposed: Any

Cyber Security Incident that has compromised or disrupted the operation of the BES and requires reporting per EOP-004. R2= Comments: Remove the word “BES” from the Requirement to be consistent with R1. Remove the words “lessons-learned report that includes a” from the Measures because the following items do not necessarily fall into the lessons learned category. Add a 2nd Measure “OR documentation from an actual Reportable Cyber Security Incident” as an alternative to the listed evidence. R3= R.3.2 Comment: Requirement - Clarify as follows “Maintain a current and up-to-date Cyber Security Incident Response Plan that (1) includes or references, as appropriate, documentation of any lessons, if any that may have been learned in connection with a Cyber Security Incident test or actual incident response performed pursuant to CIP-008-5 R2, within 90 days of the performance of such test or actual incident response; and (2) includes changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change.” Comment: Measures - Clarify as follows: “Evidence may include, but is not limited to, a dated, revised Cyber Security Incident Response Plan(s) that (1) includes or references, as appropriate, dated documentation of lessons learned, if any, associated with tests of or actual responses using the Cyber Security Incident Response Plan(s), within 90 days after completion of such test or actual incident response; and (2) reflects changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change.” R3.3 & R3.4: Remove these requirements as they are now incorporated into the proposed R3.2.
No
No
No
Progress Energy agrees with EEi comments with the modified and additional comments below 1. R3: In Order 706, paragraph 731, FERC stated “We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective.” We believe that updates to the plan are not effectively in place until it has been communicated, and that it will be more efficient for entities to track one date rather than four date requirements included in draft 2. We propose consolidation of the four subparts of R3 into one subpart that ensures up-to-date recovery plans and communications within the 90 days required in FERC 706 but is less prescriptive and less of a documentation burden. Delete R3.2, R3.3 and R3.4 and use the following text for R3.1: “Update recovery plan(s) and communicate the updates within 90 calendar days of a test, actual recovery or changes that impact the ability to execute the plan. Updates from tests or actual recovery shall include lessons learned. R3 MEASURES: With the consolidated R3.1 requirement, the following is proposed for measures: “Evidence may include, but is not limited to: 1) revised recovery plan(s) that include dated references to lessons learned from tests, actual recovery or changes that impact the ability to execute the plan; 2) dated emails, newsletters, training or other communications regarding the plan updates.” R3 VSLs: Replace the draft 2 VSLs with the following. Lower VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 90 and less than 120 days of the change, test or actual recovery. Moderate VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 120 and less than 150 days of the change, test or actual recovery. High VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 150and less than 180 days of the change, test or actual recovery. Severe VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 180 and less than 210 days of the change, test or actual recovery. R3 GUIDANCE: Add the following to guidance: “Individuals responsible for activating and implementing a recovery plan should have information needed to recover their assets. R3 is meant to ensure recovery plans are up to date and available to individuals who need them. The following are examples of items that might require updates and communications within the 90 day timeline: * changes needed as a result of lessons learned from a test or actual recovery; * changes in roles and responsibilities.”
Comments: In all measures section remove the term “…but not limited to…” In “Guidelines and Technical Basis” section, list specific FAQs and CIPC guidelines that are applicable. Remove “Associated…Systems” from R1-R3 because Order 706 does not require them.
No
No

No
Progress Energy agrees with EEI comments with the modified and additional comments below R1= Comment: R1 Requirement - is too prescriptive. Recommend that the CIP v3/v4 language replace 1.1-1.4, but specifically address the Order 706 requirements for malicious changes. Comment: R1 Requirement remove Associated assets/systems from applicability because they represent an increase in scope from CIP v3/v4 Comment: R1.4 - Applicability - : Remove “High Impact” Rationale: it is repetitious with R1.5. Comment: R1.4 Requirement – There is no time requirement, but there wasn’t one in previous versions either. R2= Comment: R2.1 – Requirement - this is a borderline show stopper – will be burdensome and nothing gained from it except a lot of TFE paperwork to track Proposed: Recommend removing requirement R3= Comment: R3.1 & R3.4 – Applicability- Add “with External Routability” to Medium Impact BES Cyber Systems and Associated Protected Cyber Assets Original: R3.1 - Requirement - At least once every calendar year, not to exceed 15 calendar months between assessments, conduct a paper or active vulnerability assessment to determine the extent to which the cyber security controls identified in CIP-005, CIP-006, and CIP-007 are implemented correctly and operating as designed. Proposed: At least once every calendar year, not to exceed 15 calendar months between assessments, conduct a paper or active vulnerability assessment to determine the extent to which the cyber security controls are implemented correctly and operating as designed. Original: R3.2 Requirement - Where technically feasible, at least once every 36 calendar months between assessments, perform an active vulnerability assessment in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline configuration of the BES Cyber System in a production environment. If a test environment was used, document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments. Proposed: Where technically feasible, at least once every 36 calendar months between assessments, perform an active vulnerability assessment in a test environment. If a test environment was used, document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.
No
No
Progress Energy agrees with EEI comments with the modified and additional comments below: R1= Comment: R1.3 - Requirement & Measure - Change language time frames by removing “at least” and replacing with “once each calendar year or a period not to exceed 15 months”. R2= Comment: R2 uses the term “chain of custody” in several places. This is a legal term that relates to evidence, and is not appropriate in the CIP standards. EEI strongly suggests replacing it with “possession” or “control”. Comment: R2.1 – Requirement - In parenthetical text in change to read “(except for reuse in other high impact…)” for clarity. Additional Comments Comments: In all requirements, remove references to systems & assets and rely on the applicability column to specify applicability. In all measures sections in all standards and requirements remove the term “…but not limited to…” The default should be an “or”, and any “and” should be explicit. Rationale: these are examples only. Using the “limited to” language creates confusion about whether they’re necessary or sufficient. Applicability for all requirements should be changed from “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routable Connectivity” Several requirements use the terminology “BES Cyber System Information”, however this creates an inconsistency with all the “Associated…” assets in the Applicability column. Suggestion is to leave the applicability in that column, and don’t name asset/system types in the requirement. The length of the “Applicability…” column title can cause confusion about the systems/assets that are within scope. Suggest changing the column heading to “Applicability”.
Individual
Jennifer White
Alliant Energy
Yes
No
Yes
Overall it seems as if the standards writers are attempting to work out some subjectivity and ambiguity issues in regards to establishing sufficiency in meeting the requirements of the standards.

We do not believe that they have fully resolved these issues. Alliant Energy voted “No” on the Standard, as a whole, due to the significance of the changes we propose herein. Many requirements, if changed in accordance with our sometimes minor verbiage proposals, would be a “Yes.” [R2.2] – VSL must change for this such that it is not a violation if the incident response plan is not followed for an actual event. The requirement to document deviations is sufficient to meet the intended goal of ensuring the currency of the plan and updating it to reflect things discovered during actual incidents or drills. [R 3.1] – Suggest striking “and update” to IR plan review. It is possible that the plan is found sufficient after the review and would not require an update. Suggest verbiage “update, if necessary.” [R3.5] – Suggest striking “distribute”. What constitutes distribution? Suggest retaining “notification” approach. Distributing CIP protected data could pose technical issues, especially outside vendors. Notification, as long as the vendor had access would eliminate the need to actually distribute the plan to affected individuals. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs.

No

No

Yes

Comments: Once again it is straightforward to see the objectives the drafters are trying to accomplish, but the reality of this level of descriptiveness and compliance thereof, would be disruptive and prohibitive. Alliant Energy voted “No” on the Standard, as a whole, due to the significance of the changes we propose herein. [R1] – The standard isn’t clear whether the recovery plans are for recovery of the asset, system, or function? Please clarify. Recommendation – the recovery should be for the function to link appropriately with the purpose of the CIP Standards. Otherwise, system is the lowest level of granularity that remains in alignment with the proposed BES Cyber System methodology. [R1.4] – Recommend striking associated physical access control systems and associated electronic access control systems from the applicability section. The wording of the requirement is unclear. What constitutes “initial,” “verification,” or “ensure the process completed successfully”? Suggest prescriptive wording if these terms are to be used. The current draft verbiage leaves too much up to the subjective interpretation of the auditor, and, if intended to be a daily or weekly check, could be administratively burdensome. Proposed Verbiage to align with FERC order 706: “Within the capabilities of the backup system and upon completion of a significant production change within a BES Cyber System, such as adding a new form of hardware or significant new software, data essential to BES Cyber System recovery that is stored on backup media shall be verified at the time the backup is created. Verification means the automated process typically incorporated into the automated backup process validates the bit count or similar technical function.” [R1.5] – Without tying this requirement to a Cyber Security Incident, there will be no forensic value in retaining the data if the event was not related to any malicious attempt. Proposed Verbiage: “Processes to preserve data, except for CIP Exceptional Circumstances, for analysis or diagnosis of the cause of a Cyber Security Incident that triggers activation of the recovery plan(s).” [VSL] These are appropriate. [R2.1] - Are the tests specified in R2 required for each cyber asset, cyber system, or each plan? In other words, does an entity need to do a “full operational exercise” on all systems, or is a representative sampling sufficient? [R2.2] – Is this in reference to the applications and other binaries used to restore or the actual plan itself? Suggest clarification. [Proposed Verbiage] “Validate the integrity of the stored backup information at least once per calendar year to ensure that the information is useable and is compatible with current system configurations.” [R2.3] – Is this requirement implying the need for a bare-metal restore for all CIP assets? Doing so would be cost-prohibitive and potentially jeopardize the stability of the BES. Some CCAs utilize a “standby” system for testing. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria. [R3.4] – Once again the use of the word “distribution”. If I notified a vendor of an update to

the plan stored in CIP protected area, it would achieve the objective without the burden of any CPI issues in its “distribution”. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria.
No
No
No
Alliant Energy voted “No” on the Standard, as a whole, due to the significance of the changes we propose herein. [R1.1] Recommend striking the applicability component of the main requirement. Applicability should be limited to the applicability column. [R1.1.3] – Proposed verbiage: “Any custom compiled software”. [R1.4] – Propose striking 1.4.1 to eliminate speculation or an implicit requirement to have a testing environment outside of 1.5. Instead, the CIP-005, CIP-006, and CIP-007 list should be moved to 1.4.2. This strike also removes the inflexibility as it relates to emergency change that exists in the current draft verbiage. In the absence of striking 1.4.1, recommend adding the CIP Exception Circumstances verbiage to 1.4 to allow emergency changes necessary to ensure operability/reliability. For those circumstances, 1.4.2 should suffice. If the intent of 1.4.1 is to expand the scope to include an understanding of potential impact outside of the existing baseline, this can be achieved without 1.4.1 with proposed verbiage: For a change that deviates from the existing baseline configuration or may have an impact on controls implemented for CIP-005, CIP-006, or CIP-007: and then skip to 1.4.2. [1.5] Recommend changing “where technically feasible” to “Where test environments exist” [VSL Recommendation] This VSL is written as a zero tolerance violation, even to the extent of indicating “any” undocumented change is a violation. Recommend, instead, that they be structured such that a Severe is the lack of a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria. [R2.1] – Recommend replacing “technically feasible” with “Within the capabilities of the system or network configuration.” Recommend striking the associated systems and cyber assets and leaving this to High Impact BES Cyber Systems with External Routable Connectivity. This also exceeds FERC 706, so we recommend increasing the interval of change detection to an annual or quarterly verification, because a manual process of verifying the baseline will be prohibitively administratively burdensome. Also, ports and services are an annual requirement, but they are also included in the baseline configuration here. This would require a validation of logical network accessible ports on a monthly basis and not tied to significant change. This creates a conflict within the standard. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria. [R3] – What is the definition of an “active vulnerability assessment”? What would be considered an appropriate infeasibility for performing such a test? Would the entity need to perform an “active vulnerability assessment” on all systems, or is a representative sampling sufficient? Recommend striking “CIP-006” from the list of cyber security controls assessed, as this is duplicative of the testing and maintenance requirement but increases the interval to annual instead of every 24 months. [R3.2] Recommend replacing “where technically feasible” with “Where a test environment exists or allowable within the operational risk of the production environment…” [R3.4] Recommend changing “planned date” to “estimated timeframe.” [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program or the failure to implement a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ

results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria.
Yes
Yes
Alliant Energy voted “Yes” on this requirement but still suggest adjustments per the suggestions herein: [R1.1] Recommend striking the first bullet in the Measures or changing it to indicate that a label of “confidential” is sufficient. The current measure is phrased such that it requires information to be labeled as CIP information, instead of just confidential. This increases the chances that someone will know how to use it maliciously if they do get unauthorized access to it. Suggest legacy verbiage indicating a classification in alignment with “confidential.” The current verbiage did not prevent organizations from assigning a “CIP Confidential” label to documentation or preclude a protection program that had only one level of protected information. [VSL Recommendation] This VSL is written as a zero tolerance violation with respect to the failure to implement even one action plan. Recommend, instead, that they be structured such that a Severe is the lack of a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. [R2.1 and 2.2] Recommend striking “chain of custody” to avoid connotations associated with legal definitions of this term that should not apply here. If the intent is to ensure positive control of the device until the information is removed, the phrasing should be in alignment with that. This phrasing should also allow secure methods of transport to the vendor if that is required within support contracts. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program or the failure to implement a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria.
Individual
Tracy Richardson
Springfield Utility Board
No
Yes
No
SUB is concerned that the Requirements of CIP-008-5 create potential conflict with the Requirements of EOP-004-2. The development of the two Standards appears to be in parallel with one another, rather than working together. SUB recommends more coordination between the Version 5 CIP SDT and the EOP-004-2 SDT. SUB understands CIP-008-5 to be the “Incident Response Plan” and EOP-004-2 requires the development of an “Operating Plan for Event Reporting.” However, CIP-008-5 Table R1, Part 1.1 requires a process to “identify, classify, and respond to BES Cyber Security Incidents” while EOP-004-2 R1.1 requires; “A process for identifying events listed in Attachment 1.” SUB recommends the SDT revise the CIP-008-5 Requirement and Measure in Table R1, Part 1.1 to remove the terms “identify” and “classify.”
Yes
Yes
Yes
No
No
No
The definition of the term “configuration” is unclear. Configuration is not clearly defined in the Glossary of Terms Used in NERC Reliability Standards, Definitions of Terms Used in Version 5 CIP Cyber Security Standards, nor in the CIP-010-1 Cyber Security – Configuration Management and

Vulnerability Assessments Standard. Are “configuration management”, “configuration change management”, and “asset management” intended to be synonymous in the way they are used in the CIP-010-1 Standard? Configuration is only mentioned in terms of “security configurations”. SUB recommends that a specific definition be provided for Configuration, Configuration Management, Configuration Change Management, and/or Asset Management. Perhaps, based on the extensive changes to definitions in Version 5 of the CIP Standards, it would be appropriate to create a CIP-specific glossary of terms used in the CIP Standards. SUB recommends that the development of NERC Standard CIP-010-1 be a separate effort from the development of CIP Version 5 Standards.
Yes
Yes
Group
ACES Power Marketing
Jason Marshall
Yes
No
No
(1) In regards to the Applicability Section please see comments submitted by ACES Power Marketing regarding Applicability in Comment Form A, Question 3, Comments 6-9. (2) Regarding Section 4.2.4 Exemptions: This section was changed from the last posting to indicate the exemptions are for CIP-002-5. CIP-002-5 already has the same exact exemption language. Either this reference should be changed back to CIP-008-5 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (3) In regards to Question 1 (CIP-008-5 R1): In the Rationale section it says, “Once the severity of an event or events rises to the level of becoming a Reportable Cyber Security Incident, NERC EOP-004 directs further external reporting actions and timing requirements.” The Guidelines and Technical Basis section for R1 under the Application Guidelines states, “The reporting obligations for Reportable Cyber Security Incidents are found in EOP-004-2.” In reading through EOP-004 it is still not clear how the two standards are to work with one another for reporting Cyber Security Incidents in regards to whom the report should be communicated. CIP-008-5 R1.5 states, “Internal groups or individuals and external organizations that should receive communication of the Cyber Security Incidents.” The Measure for CIP-008-5 R1.5 states that, “Evidence may include, but is not limited to, dated Cyber Security incident response process(es) or procedure(s) that list internal groups or individuals … and external organizations (e.g., law enforcement, ES-ISAC, software vendors, other affected entities) that should receive communication.” The Measure gives examples of entities that should receive communication. Is it up to the Responsible Entity to figure out to which external parties they should report Cyber Security Incidents? The drafting team should consider if a minimum list of required external entities is necessary to ensure consistent reporting and consistent auditing. (4) In regards to Question 2 (CIP-008-5 R2): Requirement R2.2 needs to be clarified. It reads, “Use the incident response plan under Requirement R1 when responding to or performing an exercise of a Reportable Cyber Security Incident.” This sentence when grammatically dissected says, “Use the plan when responding to an exercise or when performing an exercise…” We believe the intent of the SDT was to say, “when responding to a Reportable Cyber Security Incident or when performing an exercise of a Reportable Cyber Security Incident response plan.” Please re-phrase for clarity. (5) Regarding Question 2 (CIP-008-5 R2): The Rationale box and Part 2.2 uses the term “incident response plan” in place of “Cyber Security Incident response plan” as identified in Requirement R1. For consistency and clarity, we recommend using the more formal “Cyber Security Incident response plan” from Requirement R1. (6) Regarding Question 2 (CIP-008-5 R2): Part 2.1 states that the responsible entity is to test the BES Cyber Security Incident response plan. It indicates that response to an actual Reportable Cyber Security Incident would meet the requirement. Because response to an actual Reportable Cyber Security Incident would be an exercise of the response plan and not a test, we suggest changing “Test” to “Exercise”. (7) In regards to Question 3 (CIP-008-5 R3): The main requirement R3 is very similarly worded to the main Requirement R2. R2 focuses on testing and exercising the plan (implementation). R3 focuses on reviewing and updating the plan. R3 should be re-worded to better align with the objective. The Rationale for R3 states that “sufficient reviews, updates and communications” are conducted. To capture this, alternative language could be, “Each Responsible Entity shall review, update and distribute its documented Cyber Security Incident

response plan(s) to collectively …" Furthermore, this would make the requirement more consistent with the parallel requirement CIP-009-5 R3. (8) In regards to Question 3 (CIP-008-5 R3): The use of the word "within" throughout the R3 sub-requirements is confusing when used to reference number of days. One meaning of "within" is "inside a boundary." This could be interpreted as inside 30 calendar days but not including the 30th day. The meaning of "within" in the context of the requirements is "not beyond" or "not exceeding." Why not simply replace "within" with "does not exceed" to avoid confusion? In R3.1 "not to exceed 15 calendar months between reviews" is pretty clear. We recommend using similar language in R3.2 – R3.5 and the associated VSLs. (9) In regards to Question 3 (CIP-008-5 R3): Requirement R3.2 says to, "Document any lessons learned associated with a Cyber Security Incident test or actual incident response to a Reportable Cyber Security Incident within 30 calendar days…" The Measure states that, "Evidence may include, but is not limited to, dated documentation of lessons learned, if any…" If there are no lessons learned, what is the Responsible Entity obligated to do to comply with the requirement? Is documentation stating there were no lessons learned from the incident sufficient? (10) In regards to Question 3 (CIP-008-5 R3): In the VRF/VSL section for R3, the words "within 30 and less than 60 calendar days" is very confusing. Using "and" means both conditions must be true. Anything within 30 days is automatically going to be less than 60 days so the phrase is redundant. Does the SDT mean to say, "greater than 30 but less than 60 calendar days?" (11) In regards to Question 3 (CIP-008-5 R3): The sub-requirement references in parentheses for the R3 VSLs are not represented correctly. For example, for the Lower VSL, the sub-requirement reference is to R3.4. It should be R3.5 since R3.5 requires the distribution of updates. All of the references in the VSLs for R3 need to be corrected. (12) In regards to Question 3 (CIP-008-5 R3): In the Guidelines and Technical Basis section for R3, the second sentence says, "There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.2 and (2) organizational or technology changes from Part 3.4." Isn't there a third requirement that would also trigger a plan update? R3.1 says, "Review and update each Cyber Security Incident response plan for accuracy and completeness at least once each calendar year, not to exceed 15 calendar months between reviews." The calendar year review would also trigger a plan update while not necessarily meeting the criteria of R3.2 or R3.4. Simply revising the date the plan was reviewed is technically an update. An erratum change would also qualify as an update. (13) Regarding Background Section 5: The third paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. Which is it? We support the latter.

No

Yes

No

(1) In regards to the Applicability Section please see comments submitted by ACES Power Marketing regarding Applicability in Comment Form A, Question 3, Comments 6-9. (2) Regarding Section 4.2.4 Exemptions: This section was changed from the last posting to indicate the exemptions are for CIP-002-5. CIP-002-5 already has the same exact exemption language. Either this reference should be changed back to CIP-009-5 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (3) Regarding Question 5 (CIP-009-5 R1): The drafting team should develop application guidelines for these requirements. At the very least, the reference to the FAQs and CIPC Guidelines should be more specific with links to each guideline and FAQ. (4) Regarding the VSLs for CIP-009-5 R1: An additional gradation has been added, which is an improvement, but since there are five parts to R1, having four VSLs based on gradations of the number of parts missed would be a further improvement. (5) Regarding Question 6 (CIP-009-5 R2): Parts 2.1 and 2.3 state that the responsible entity is to test the BES Cyber Security Incident response plan. Both indicate that response to an actual Reportable Cyber Security Incident would meet the requirement. Because response to an actual Reportable Cyber Security Incident would be an exercise of the response plan and not a test, we suggest changing "Test" to "Exercise". (6) Regarding Question 6 (CIP-009-5 R2): Part 2.2 should clarify that actual recovery of a BES Cyber System using the backup media meets the requirement. (7) Regarding Question 7 (CIP-009-5 R3): Part 3.4 needs to be modified to be consistent with Part 1.2 of Requirement R1. Part 3.4 requires the recovery plan to be distributed to "each individual responsible under R1.2". First, R1.2 needs to be changed to Requirement R1, Part 1.2 to be consistent with language NERC submitted to the Commission describing the use of parts in place of sub-

requirements. Second, Requirement R1, Part 1.2 was modified to remove the need to identify specific individuals in the recovery plan. This was done to eliminate the documentation challenges associated with maintaining recovery plans every time there is a personnel change. We suggest replacing “each individual” with “responders” from Part 1.2. Third, “distribute” should be changed to “make available” or “notify”. Distributing implies that the actual recovery plans should be communicated (i.e. email attachment, hand delivered). All that is needed is for the responders to be made aware an update has occurred to a recovery plan. (8) Regarding the VSLs for CIP-009-5 R3, the words “within 30 and less than 60 calendar days” is very confusing. Using “and” means both conditions must be true. Anything within 30 days is automatically going to be less than 60 days so the phrase is redundant. Does the SDT mean to say, “greater than 30 but less than 60 calendar days?” (9) Regarding Background Section 5: The third paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. Which is it? We support the latter.

No

No

Yes

(1) In regards to the Applicability Section please see comments submitted by ACES Power Marketing regarding Applicability in Comment Form A, Question 3, Comments 6-9. (2) Regarding Section 4.2.4 Exemptions: This section was changed from the last posting to indicate the exemptions are for CIP-002-5. CIP-002-5 already has the same exact exemption language. Either this reference should be changed back to CIP-010-1 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (3) Regarding Question 9 (CIP-010-1 R1): Removal of BES before Cyber Asset in Part 1.1 has the impact of greatly expanding the requirement. By definition a Cyber Asset is any “programmable electronic device”. Thus, computer systems that have absolutely no impact on the Bulk Electric System could be pulled into the requirement. We recommend not only adding BES back to Cyber Asset but also clarifying that the requirement only applies to applicable BES Cyber Assets. Thus, we suggest replacing “Cyber Asset” with “applicable BES Cyber Asset” throughout Part 1.1 and its associated measure. (4) Regarding Question 9 (CIP-010-1 R1): The timeline established for Part 1.3 conflicts with some of the timelines established in CIP-005-5 and CIP-007-5. For example, Part 3.3 in CIP-007-5 requires an update of “malicious code protections” at least once every 35 days. CIP-010-1 R1 Part 1.3 requires updates to the baseline configuration within 30 days which would also included updating “malicious code protections”. We suggest removing CIP-005 and CIP-007 as a reference to eliminate this issue. (5) Regarding Question 9 (CIP-010-1 R1): Part 1.3 presents opportunities for double jeopardy by including references from CIP-005 and CIP-007. If a change to the ports configuration is made but documentation from CIP-005 and CIP-007 is not updated, CIP-010-1 R1, CIP-005 and CIP-007 could all be violated simultaneously. (6) Regarding Question 9 (CIP-010-1 R1): Part 1.4 is partially redundant, unnecessary and completely ambiguous. It essentially says that the responsible entity needs to identify the “required cyber security controls identified in CIP-005, CIP-006 and CIP-007” in Part 1.4.1. First, they are not controls but requirements and should be referred to as such. Second, CIP-005, CIP-006, and CIP-007 are standards that should stand alone without the need to have another requirement say that they should be implemented. Thus, we are left unsure what the intent of this requirement is. (7) Regarding Question 9 (CIP-010-1 R1): To ensure the statement in parentheses in Part 1.5.1 has the same impact as the rest of the requirement, the parentheses should be removed. The statement with the parentheses is not an explanatory statement but actually modifies the requirement. (8) Regarding Question 9 (CIP-010-1 R1): The Measure for Part 1.3 should be clarified to say “within 30 calendar days” to be consistent with the Requirement. (9) Regarding Question 9 (CIP-010-1 R1): Part 1.4 should be given an exclusion for CIP Exceptional Circumstances. (10) Regarding Question 10 (CIP-010-1 R2): Part 2.1 conflicts with the application guidelines. The application guidelines explain that periodic monitoring is included in the requirement to allow for monitoring of BES Cyber Assets that don’t have the capability to be monitored continuously. Thus, a responsible entity could manually check the baseline configuration at least once every 35 days. While a periodic manual check would always seem to be technically feasible, it may not be practical based on staffing levels. Thus, it is not clear if the clause “where technically feasible” applies to both the continuous and periodic monitoring. (11) Regarding Question 10 (CIP-010-1 R2): To ensure the statement in parentheses in Part 3.2 has the same impact as the rest of the requirement, the parentheses should be removed. The statement with the parentheses is not an

explanatory statement but actually modifies the requirement. (12) Regarding Question 11 (CIP-010-1 R3): Part 3.3 appears to be missing “and” after the parenthesis. Without the parenthetical, it should read “Except for CIP Exceptional Circumstances and like replacements and prior to adding a new Cyber Asset…” (13) In regards to Question 11 (CIP-010-1 R3): Part 3.4 does not specify a deadline for documenting the results of the assessments and the action plan to remediate or mitigate vulnerabilities. We suggest a 30-day limit for documentation associated with this requirement. Otherwise, debates could arise between the registered entity and regional entities on what constitutes timely compliance. Along with adding a deadline to the actual requirement, we recommend also adding levels of VSL gradation for not meeting the 30-day limit. (14) Regarding Background Section 5: The third paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. Which is it? We support the latter.
Yes
No
(1) In regards to the Applicability Section please see comments submitted by ACES Power Marketing regarding Applicability in Comment Form A, Question 3, Comments 6-9. (2) Regarding Section 4.2.4 Exemptions: This section was changed from the last posting to indicate the exemptions are for CIP-002-5. CIP-002-5 already has the same exact exemption language. Either this reference should be changed back to CIP-011-1 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (3) Regarding Question 13 (CIP-011-1 R1): There is a missing “or” after the first bullet of the measure. (4) Regarding Question 14 (CIP-011-1 R2): BES should be inserted prior to Cyber Assets in Part 2.2. Otherwise the requirement could be expanded to cover any computer or control system that does not impact the BES. Cyber Asset has a much different meaning than BES Cyber Asset. (5) Regarding Background Section 5: The third paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. Which is it? We support the latter.
Individual
Anthony Jablonski
ReliabilityFirst
CIP-008-5 1. VSL for Requirement R2 a. The last VSL under the “High” category seems to be erroneous. It states “The Responsible Entity does not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)” though it does not relate to associated Requirement R2 Part 2.2 in any manner. ReliabilityFirst Recommends deleting this VSL. 2. VSL for Requirement R3 a. General comment – References to the Part numbers are incorrect for a number of the VSLs. For example, the “Lower” VSL has an incorrect reference to Part 3.4. The reference should be to Part 3.5. ReliabilityFirst recommends checking the references to the Part numbers to ensure accuracy. b. A VSL associated with Requirement 3, Part 3.1 is missing from the VSL table. Part 3.1 states: “Review and update each Cyber Security Incident response plan for accuracy and completeness at least once each calendar year, not to exceed 15 calendar months between reviews.” ReliabilityFirst recommends adding a VSL associated with Part 3.1.
CIP-009-5 1. VSL for Requirement R1 a. ReliabilityFirst believes the “Moderate” VSL has a typo. The “Moderate” VSL incorrectly states: “do not address all of the requirements.” Based on the gradation of other VSLs for R1, ReliabilityFirst believes this VSL should be modified to correctly state “do not address one of the requirements.” 2. VSL for Requirement R2 a. There seems to be a conflict between the first and second VSLs under the “Severe” category (the VSLs associated with Part 2.1 and Part 2.2). The VSL for Part 2.1 indicates “18 calendar months” and the VSL for Part 2.2 indicates “19 calendar months”. Even though these are separate Parts, the timeframes are of the same length in the requirement and ReliabilityFirst recommends these two VSLs be modified to be consistent. 3. VSL for Requirement R3 a. The first VSL under the “Moderate” category has an incorrect parenthetical reference to Part 3.1. This VSL is actually associated with Part 3.2. b. The second VSL under the “High” category has an incorrect reference to Part 3.2 within the VSL itself. ReliabilityFirst recommends modifying the VSL as follows: “…60 calendar days after the documentation required by R3 Part 3.1. (3.2)”

CIP-010-1 1. VSL for Requirement R1 a. ReliabilityFirst recommends adding a reference to the associated “Part” in which each VSL is related to. It is very hard trying to trace the VSL back to the associated Part number. For example, if a Responsible Entity failed to comply with Parts 1.1 or 1.5, it is unclear which VSL they would fall under. Also, based on FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement. New terminology in the VSLs should be avoided that doesn’t already exist in the associated requirement. 2. VSL for Requirement R2 a. ReliabilityFirst recommends modifying the first “Severe” VSL to state: “The Responsible Entity has not implemented a configuration monitoring process” to be consistent with the language in Requirement R2. Also, there is no mention of the Responsible Entity monitoring continuously or periodically, not to exceed once every 35 calendar days, for changes to the baseline configuration (per Part 2.1) in the VSLs. ReliabilityFirst recommends the following: “The Responsible Entity has not implement one or more documented processes to monitor continuously or periodically, not to exceed once every 35 calendar days, for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1). 3. VSL for Requirement R3 a. All the VSLs for Requirement R3 start off with the language: “The Responsible Entity has established one or more documented” while Requirement R3 requires the Responsible Entity to “…implement one or more documented processes…”. To be consistent with the requirement, ReliabilityFirst recommends the VSLs should start off with the following language: “The Responsible Entity has implemented one or more documented processes…” b. ReliabilityFirst recommends adding a reference to the associated "Part" in which each VSL is related to. Without referencing the associated Part number, it is very hard to trace the VSL back to the associated Part number. Also, based on FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement. New terminology in the VSLs should be avoided that doesn’t already exist in the associated requirement.
CIP-011-1 1. General comment for VSLs for Requirements R1 and R2 a. ReliabilityFirst recommends adding a reference to the associated “Part” in which each VSL is related to. Without referencing the associated Part number, it is very hard to trace the VSL back to the associated Part number.
Individual
Robert Mathews
Pacific Gas and Electric Company
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Comments: In R2, replace “chain of custody” with “possession” or “control” as chain of custody is a legal term related to evidence
Group
SPP and Member companies
Lesley Bingham
Yes
Yes
Yes

Part 3 can be shortened to two sub-requirements by leaving Part 3.1 as is and adding the following as Part 3.2 “For any required change to the recovery plan (due to deficiencies or lessons learned from recovery plan tests or actual incident recoveries, or changes in roles, responsibilities, or technology), update the recovery plan and distribute updates to each individual responsible under R1.3 within 60 calendar days”.
Yes
Yes
Yes
Yes
Yes
Yes
If an entity is building systems with a documented baseline and monitoring it closely, the vulnerability assessment prior to deployment will have no benefit. Additionally, it will be difficult (not to mention expensive) to establish a production-like environment which would produce an accurate vulnerability assessment.
Yes
Yes
Group
IRC Standards Review Committee
Christine Hasha
Yes
Yes
Yes
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding the combination of CIP-008-5 Requirements 3.2 and 3.3 under question 4.
Yes
Yes
Yes
The IRC requests combining Requirement R3.1 and R3.2 and allow 60 calendar days to document identified deficiencies or lessons learned, and update the recovery plan(s).
The IRC requests combining Requirement R3.1 and R3.2 and allow 60 calendar days to document identified deficiencies or lessons learned, and update the recovery plan(s).
Yes
Yes
No
The IRC believes that CIP-010-1 Requirement 3.1 could be seen as redundant to 1.3. A vulnerability assessment should not be a compliance check of the controls listed in CIP-005, CIP-006, and CIP-007. Requirements 3.3 and Part 3.4 define what is meant for a vulnerability assessment. This may not be sufficient to address current vulnerabilities. The IRC requests clarification of whether the vulnerability assessment is to check against known vulnerabilities or simply a compliance check of the CIP requirements. The IRC requests that CIP-010-1 Requirement 3.2 have Associated Electronic Access Control or Monitoring Systems and Associated Protected Cyber Asset added to the applicability.
Yes
Yes
Individual
Scott Kinney
Avista

See comments provided by EEI
See comments provided by EEI
See comments provided by EEI
See comments provided by EEI
See comments provided by EEI
Individual
Gregory Campoli
NYISO
No
No
No
• R1 – Concerns EOP-004-3 is not accepted and the reference between future and requirement may not link well. Should not assume EOP-004-3 is approved. • R2 Part 2.1 Recommend changing the first bullet from “By responding to an actual Reportable Cyber Security Incident; ” to “By responding to a Cyber Security Incident” since this covers the Reportable Incidents plus the non-reportable incidents • Recommend updating R2 Part 2.3 since the existing language does specify a retention period. • Recommend changing R3 Part 3.1 from “Review and update” to “Review and update, as needed,” since some years the Cyber Security Incident response plan will not need updating
No
No
• R1.5 – Recovery plans are for restoring service. ITIL incident management is for restoring service which is the priority for BES support. Root cause analysis is where forensics would be considered and could really detract from BES operations. Priority is to Availability impact for BES cyber systems so don’t introduce conflict with forensics in the requirements. Best practice should be forensics. • R2.3 may have bookends on periodic requirements in the requirement so please clarify.
No
No
No
• R1 Please clarify what “intentionally installed software” covers as systems come with applications and device drivers that may include executable and DLL files. • Request clarification of R1 Part 1.1.2. Does “applications” mean “SCADA, EMS, State Estimator, IDC, etc” instead of “device drivers, DLL, applications included in an operating system or package, etc?” • Request clarification of R1 Part 1.1.3. Would a version control tool/system (like CVS) demonstrate the custom software’s version? • Request clarification on R1 Part 1.3. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005 and CIP-007? • In R1 Part 1.3, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations • Recommend removing the 30 day time frame in R1 Part 1.3 that applies to CIP-005 and/or CIP-007. Those Standards should specify their time frames. Recommend that the 30 days apply to only updating the baseline configuration (this Part) • Request clarification on R1 Part 1.4.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? • In R1 Part 1.4.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations • Recommend removing R1 Part 1.4.2 because “availability” has not been part of the Requirements in the past, is not a FERC requirement and can be interpreted multiple ways • In R1 Part 1.5, recommend changing from “Where technically feasible, for each change that deviates from the existing baseline configuration ” to “Testing cyber security control, where technically feasible, for each change that deviates from the existing baseline configuration” for clarity • For R2 Part 2.1, recommend the previous version 5 words since this updated Part is not understandable • Request clarification on R3 Part 3.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? • In R3 Part 3.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations • Recommend that R3 Part 3.1start with its purpose – for example, Active vulnerability assessment • Request

clarification on R3 Part 3.2. If this is a paper exercise it should be performed once every 36 months. • Recommend that R3 Part 3.2 start with its purpose – for example, “Perform active vulnerability assessment, where technically feasibly….”. • Recommend that R3 Part 3.3 start with “Perform an active vulnerability assessment, of the new cyber assets prior to business deployment, except for CIP Exceptional Circumstances and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset).” • Recommend updating CIP-010 R1’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures shows R1 as “low” • Recommend updating CIP-010 R2’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures shows R2 as “low”
Yes
No
• R2 Recommend moving the second paragraphs of R2 Parts 2.1 and 2.2 into a new Part 2.3 for clarity.
Individual
Linda Jacobson-Quinn
Farmington Electric Utility System
Yes
Yes
Yes
No
Yes
Yes
R1.4 states backup media shall be “verified initially after backup,” the terms verified initially are vague. Many automatic backup systems run a series of backups at different times and report if the backup was successful. FEUS recommends the drafting team revise R1.4 to state “verified the backup was successful by the end of the next business day.” FEUS recommends revising to align with the measures, “Information essential to BES Cyber System recovery that is stored on backup media shall be confirmed to ensure that the backup process completed successfully.” Additionally, the evidence required to demonstrate with R1.4 would be burdensome to maintain for three years since most entities run multiple backups on multiple systems at different periodicities. FEUS recommends changing the data retention to R1.4 to 90 calendar days.
Yes
Yes
Yes
Yes
Yes
See comments submitted with CIP-004; CIP-004-5 R6.1.3: This should be removed – the protections should be included in the information protection program provided by CIP-011-1. It is noted the measures include, “and access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity.” FEUS is concerned that electronic information may be stored in an electronically secured location (aka laptop or encrypted/protected USB) but the physical location may be very mobile in that ‘physical’ location varies. In additional, even printed material may be ‘mobile’. For example, printed copies physically transferred from a Primary Control Center to a Backup Control in which the physical location may be a briefcase in the direct control of someone with access. This type of situation is better handled by an individual’s information protection program rather than the Access Management Program. CIP-004-5 R6.4 should be removed from this Requirement included in the information protection program provided by CIP-011-1. At a minimum, the SDT should clarify what is meant by physical access. See comments for CIP-004-5 R6.1.3 – the physical location of printed or electronically stored information may not be stationary and may be

impossible to control based on the circumstance. This would be better defined in the Information Protection Program to allow flexibility. CIP-004-5 R6.7: See comments for 6.1.3 and 6.4 CIP-004-5 R7.3: FEUS feels this would be better defined by an entities Information Protection Program; see comments in R6 regarding the physical location of System Information
Individual
Maggy Powell
Exelon Corporation and its affiliates
No
No
No
CIP-008-5, R1: The examples in M1.4 are confusing relative to R1.4. Post-incident analysis does not seem to track with the requirement for incident handling procedures. Recovery is covered in CIP-009. It's conceivable that an entity may have one document to demonstrate evidence for multiple requirements associated with incidents; however, the examples imply that recovery documentation would suffice as evidence for the incident handling procedures. Please remove "(e.g., containment, eradication, recovery, post-incident analysis)" from M1.4. CIP-008-5, R2: The defined term for Cyber Security Incident does not include BES and shouldn't be added in R2.1. Please remove "BES" from R2.1 to read: "Test the Cyber Security Incident response plan(s) …" CIP-008-5, R2: Also, for consistency, R2.2 should spell out Cyber Security Incident. Update R2.2 to read: "Use the Cyber Security Incident response plan …" CIP-008-5, R3: Two bullets in M3.5 are not cited as forms of evidence. Please update M3.5 to read: "Evidence of distribution of updates may include, but is not limited to: - Emails; - Delivery receipts from USPS or other mail service; - Delivery receipts from electronic distribution system; or - Training sign-in sheets.
No
No
No
CIP-009-5, R1: M1.3 is missing an "and." For consistency with R1.3, M1.3 should read: "Evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information…" CIP-009-5, R1: In R1.4, It is clearer to us for the terms "verified" and "initially" to be reversed in order. Please consider revising R1.4 to read: "Information essential to BES Cyber System recovery that is stored on back up media shall be initially verified after backup...” Even with the above proposed revision, R1.4 raises significant questions about what is intended by the terms “initially,” “verified” and “backup.” By extension, the compliance demonstration obligations under M1.4 also depend on the intended type of backup, the quantity of data and duration of record keeping. As currently written, CIP-009-5, R1.4 is unclear and could impose a compliance burden in terms of manpower and documentation to comply that overwhelming outweighs a benefit to reliability or security. We suspect that the intent is to ensure that the backup process works reliably and that verification would be satisfied by a confirmation of the completed backup process. As the SDT revisits R1.4, it may be useful to consider dropping the word “initially”. Further, we expect that the requirement obligation does not warrant recording daily or continual backups and a subset of data should be sufficient to demonstrate compliance. Depending on the intended “verification” and “backup” type, M1.4 may need to define "logs" as operational logs and thereby limiting the data retention to 90 days. Alternatively, set a number of backups, perhaps 10, as a level sufficient to demonstrate that the backup works reliably. Perhaps contributing to the confusion with R1.4 is that CIP-009-3 R5 called for an annual requirement for testing backup media and is no longer part of the standard or discussed in the rationale. We recognize that the proposal cites CIP-009-5, R1.4 as a new requirement; however, some discussion of the evolution may help further clarify the intent. CIP-009-5, R2: Relative to the R2 test requirements, please discuss what/how much information is intended for the test. A representative sample should be acceptable to demonstrate a test. CIP-009-5, R3: As in CIP-008, R3.5, two bullets in CIP-009, M3.4 are not cited as forms of evidence. Please update M3.4 to read: "Evidence of distribution of updates may include, but is not limited to: - Emails; - Delivery receipts from USPS or other mail service; - Delivery receipts from electronic distribution system; or - Training sign-in sheets.
No

Yes
No
CIP-010-1, R1: In R1.3.3 the use of the undefined term “custom software developed for the entity” does not clearly include or exclude user applied parameters used to configure core functions in a device’s standard software or firmware; relay settings are an example of this. As well, please discuss what may be grouped under R1.1.” CIP-010-1, R1: R1.1.2 should not have BES in front of Cyber Asset. Please revise R1.1.2 to read: "Any commercially available or open-sources application software (including version) intentionally installed on the Cyber Asset;" CIP-010-1, R1: More problematic in R1.1.2 is the term “intentionally.” Inclusion of this term raises the question of how to prove intentional or unintentional installation. For instance, if an entity installs commercially available software, but is unaware that the package also included java software, what are the obligations of the entity? We suggest removing the word intentionally so that R1.1.2 reads: "Any commercially available or open-sources application software (including version) installed on the Cyber Asset;" CIP-010-1, R1: A word order adjustment to R1.5.1 will improve clarity. Please consider revising R1.5.1 to read: "Prior to implementing any change in the production environment, test the changes in a test environment that models the baseline configuration (or in a production environment where the test is performed in a manner that minimizes adverse effects) to ensure that required cyber security controls are not adversely affected; and" CIP-010-1, R3: A word order adjustment to R3.2 will improve clarity. Please consider revising R3.2 to read: "Where technically feasible, at least once every 36 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment (or in a production environment where the test is performed in a manner that minimizes adverse effects). ..." CIP-010-1, R3: As well, R3.3 is not clearly stated. Please consider revising R3.3 to read: “Prior to adding a new Cyber Asset, perform an active vulnerability assessment of the new Cyber Asset (except in CIP Exceptional Circumstances or when a replacement Cyber Asset is of the same type and same baseline configuration of the previous Cyber Asset).” CIP-010-1, R3: R3.4 does not clearly identify which vulnerability assessments correlate with the action plans. Please confirm that the action plans in R3.4 refer to the vulnerability assessments in CIP-010-1, R3.1, R3.2 and R3.3. Please consider revising to R 3.4 to read: "Document the results of the assessments conducted per CIP-010-1 R3, Part 3.1, 3.2 or 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items."
No
No
CIP-011-1, General: The component obligations under CIP-011-1 are not clearly split into the requirement divisions. The table headers under R2 may be adding to the confusion as they are different for R2.1 and for R2.2. It appears that the general heading for the R2 tables should be Reuse and Disposal. Then the sub-requirements should breakout the requirements specific to BES Cyber Assets and Media respectively. R1 addresses information, but does not discuss disposal and destruction of information. R2 discussed disposal but does not discuss disposal of information. CIP-011-1, R1: Did the drafting team intend to include procedures for disposal and destruction under R1.2? Or does R2 cover the relevant measures for destruction and disposal? CIP-011-1, R1: M1.1 lists "Repository or designated electronic and physical location" as evidence. Please clarify how the repository demonstrates that documents are identified and BES Cyber System Information. It is important to clarify that while a repository may be a tool for BES Cyber System Information, all information within a repository may not automatically be subject to the restrictions associated with BES Cyber Security Information. CIP-011-1, R1: FYI - the reference to prior version under R1.2 refers to CIP-003-3, R5.3. This should perhaps be listed under R1.3 instead. CIP-011-1, R1: Is classification or determination of BES Cyber System Information a required part of the handling procedures for R1.2? CIP-003-4 specifically required classification of CCA information (CIP-003-4, R4. Information Protection —The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.) It’s not clear that classification or determination continues within CIP-011. CIP-011-1, R1: Part 1.2 Change Rationale states that the SDT removed the language “protect” information and replaced it with “handling” information to clarify that protection is required. To be more clear, should it be “One or more documented and implemented procedures for the protection and handling of BES Cyber System Information…”?
Group

CenterPoint Energy
John Brockhan
No
No
No
R1.5 – CenterPoint Energy recommends removing this requirement or alternatively, proposes that "Reportable" be added to Cyber Security Incident. R2.2 – CenterPoint Energy believes this requirement is too prescriptive as it relates to documenting deviations and recommends that the SDT remove "documentation of deviations" as deviations will be captured in lessons learned. R3.1 - CenterPoint Energy proposes the following alternative language to indicate annual requirements: “Once per calendar year but there should be no more than 15 months between activities." CenterPoint Energy also recommends that the SDT add "except in CIP Exceptional Circumstances” as also noted in the comments submitted by EEI. R3.2/R3.3 – CenterPoint Energy proposes that "if any" be added to the noted requirements. CenterPoint Energy also request that “with External Routable Connectivity” be added to the Medium Impact Applicability as also noted in the comments of EEI and NSRS. Guidelines & Technical Basis – CenterPoint Energy recommends that the guidance for Requirement 3 be updated to reflect changes to the requirement since the last formal comment period. CenterPoint Energy also agrees with the comments submitted by NSRS for this Standard.
No
Yes
No
R3.1 – CenterPoint Energy recommends that the SDT merge 3.1 and 3.2 and change the timeframe to 60 days as similarly noted in the comments submitted by EEI. CenterPoint Energy also agrees with the comments submitted by NSRS.
No
No
No
R1 - CenterPoint Energy believes that the changes to this requirement are too prescriptive and burdensome, particularly for the substation environment. The Company also recommends that this requirement and all of its sub requirements should not be applicable to Medium Impact Facilities as it is not a FERC directive to include such Facilities. The Guidelines and Technical Basis is also only targeted at Control Centers. R2.1 – CenterPoint Energy proposes that the SDT change the timeframe associated with this requirement to 90 days. R3.1 - CenterPoint Energy recommends that the SDT add “with External Routable Connectivity” to the Medium Impact applicability for this requirement. R3.4 - CenterPoint Energy recommends that the SDT add “with External Routable Connectivity” to the Medium Impact applicability for this requirement. CenterPoint Energy also generally agrees with the comments submitted by NSRS.
No
Yes
R1.1/1.3 - CenterPoint Energy recommends that the SDT add “with External Routable Connectivity” to the Medium Impact applicability for this requirement. CenterPoint Energy also agrees with the comments submitted by NSRS.
Individual
James Tucker
Deseret Power
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
Yes
R1.3 – DESERET POWER requests clarification regarding whether “deficiencies identified during the assessment” are considered violations of the standard. DESERET POWER believes these deficiencies should not be considered violations and requests that the SDT make this clear in the requirement language.
Group
Tri-State G&T - Transmission
Tracy Sliman
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
No
Clarify that deficiencies found are not to be considered a violation.
Group
Seattle City Light
Pawel Krupa
General Comments: SCL does not support the approach proposed in version 5 of the CIP Standards, either as to fundamentals or details. Fundamentally SCL believes the v5 approach is flawed and will introduce significant compliance burden without ensuring cyber security for the BES. Detailed concerns remain as provided previously (please refer to comments submitted by SCL on January 6, 2012). Although today's enforcable CIP Standards share many of the flaws of v5, SCL believes industry would be better served by developing maturity around the existing Standards while developing a new, different approach to cyber security that is based on the established practices and theory of the information technology industry.
Individual
Steve Alexanderson P.E.
Central Lincoln

Yes
Yes
Yes
We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
Yes
Yes
Yes
We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
Yes
Yes
Yes
We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
Yes
Yes
We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
Group
PacifiCorp
Sandra Shaffer
PacifiCorp support comments submitted by EEI.
Individual
John Tolo
Tucson Electric Power
Yes
Yes
Yes
TEPC agrees with EEI Comments: Change all instances of Medium Impact BES Cyber Systems to “Medium Impact BES Cyber Systems with External Routable Connectivity” for consistency with CIP-005, CIP-006, and CIP-007.
Yes
Yes

No
TEPC agrees with EEI comments: : R2.1: Modify the first part of the requirements language to read "Test a representation of the recovery plans(s) referenced in Requirement R1 once each calendar year or not more than 15 calendar months between tests except for CIP Exceptional Circumstances." Rationale: Reduce significant confusion. R2.2: a) Change the first 3 words of the requirement to read "Test representative information"., R3: In Order 706, paragraph 731, FERC stated "We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective." We believe that updates to the plan are not effectively in place until it has been communicated, and that it will be more efficient for entities to track one date rather than four date requirements included in draft 2. We propose consolidation of the four subparts of R3 into one subpart that ensures up-to-date recovery plans and communications within the 90 days required in FERC 706 but is less prescriptive and less of a documentation burden. Delete R3.2, R3.3 and R3.4 and use the following text for R3.1: "Update recovery plan(s) and communicate the updates within 90 calendar days of a test, actual recovery or changes that impact the ability to execute the plan. Updates from tests or actual recovery shall include lessons learned. R3 MEASURES: With the consolidated R3.1 requirement, the following is proposed for measures: "Evidence may include, but is not limited to: a) revised recovery plan(s) that include dated references to lessons learned from tests, actual recovery or changes that impact the ability to execute the plan; b) dated emails, newsletters, training or other communications regarding the plan updates." R3 VSLs: Replace the draft 2 VSLs with the following. Lower VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 90 and less than 120 days of the change, test or actual recovery. Moderate VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 120 and less than 150 days of the change, test or actual recovery. High VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 150and less than 180 days of the change, test or actual recovery. Severe VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 180 and less than 210 days of the change, test or actual recovery. R3 GUIDANCE: Add the following to guidance: "Individuals responsible for activating and implementing a recovery plan should have information needed to recover their assets. R3 is meant to ensure recovery plans are up to date and available to individuals who need them. The following are examples of items that might require updates and communications within the 90 day timeline: * changes needed as a result of lessons learned from a test or actual recovery; * changes in roles and responsibilities."
No
Yes
Yes
TEPC agrees with the following comments from EEI: R1: remove Associated assets/systems from applicability because they represent an increase in scope from CIP v3/v4; 3) R2: remove Associated assets/systems from applicability because they go beyond Order 706. R1.1: Add "with External Routability" to Medium Impact BES Cyber Systems; 5) R1.4: Remove "High Impact" from Applicability because it is repetitious with R1.5. R3.1: a) Applicability: Add "with External Routability" to Medium Impact BES Cyber Systems and Associated Protected Cyber Assets.
Yes
Yes
Individual
Russell A. Noble
Cowlitz County PUD
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Oscar Alvarez
Los Angeles Department of Water and Power
Yes
Yes
Yes
LADWP does not have extensive comments on this matter at this time.
Yes
No
Yes
R2.1 states that the entity is to test the recovery plan(s) every calendar year, not to exceed 15 months. R2.3 seems to be a facsimile of 2.1, yet adds a longer timeframe for compliance. We need clarification on the timeframes, as there may be overlap between the two activities. Furthermore, there needs to be clarification or additional guidance for the types of operational excercises the drafting team is requesting entities to perform per R2.3.
Yes
Yes
No
R3.3 states that prior to adding a new Cyber Asset to a BES Cyber System, the entity is to perform an active vulnerability assessment of the cyber asset. It is problematic to perform an active vulnerability assessment prior to installing a new Cyber Asset. Furthermore, the term "Active vulnerability assessment" is not defined. Under the assumption that an "active vulnerability assessment" is the actual performance of an entities vulnerability assessment program, there are sufficient controls in place that would deem an "active vulnerability assessment" unnecessary, such as change management procedures. Therefore, we request that R3.3 be removed.
Yes
Yes
LADWP does not have extensive comments on this matter at this time.
Individual
Tony Kroskey
Brazos Electric Power Cooperative
No
No
No
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.

No
Yes
No
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
No
No
Yes
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
Yes
No
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
Group
Puget Sound Energy, Inc.
Tom Flynn
Yes
Yes
Yes
R3.2 states that "…lessons learned associated with a Cyber Security Incident test or actual incident response to a Reportable Cyber Security Incident within 30 calendar days after the completion of the test or actual incident response." While 30 calendar days would be sufficient time to document lessons learned from a test of the plan or a minor incident, there is the potential of larger or more complex incidents requiring considerably longer than 30 calendar days to accurately document lessons learned. Recommendation: Add language to the requirement to say that the CIP Sr. Manager or delegate is required to approve any lessons learned documentation that will exceed 30 days to complete.
Yes
No
No
(1) In the Measure for R2.2, the evidence required includes the "BES Cyber Systems that is stored on backup media when initially stored and at least once each calendar year…" PSE feels the wording suggests you have to test the backup media twice, and requests that the words "when initially stored" be dropped from the measure. This clears up any confusion on when the backup evidence must be tested "once each calendar year…". (2) In Requirement R3.2, when referring to "Update the recovery plan(s) based on any documented deficiencies or lessons learned within 30 calendar days", PSE feels that 3.3 is sufficient to tracking changes to the documentation based on implementations from the lessons learned. Applying lessons learned could require program, process and technology changes that may take several months to a year to implement. At which time documentation changes would then be updated according to Requirement 3.3. PSE recommends removing this requirement and clarifying the need for this updating in accordance to 3.1 and 3.3 respectively.
Yes
Yes
Yes
R1.5 states: "Where technically feasible, for each change that deviates from the existing baseline configuration…" The updated wording in R1.5.1 seems to remove any chance of a technical

infeasibility. Is a Technical Feasibility Exception (TFE) expected in cases where an entity cannot test in a test environment or cannot document that the test performed in a production environment is done in a manner that minimizes adverse effects? Suggestion: Remove “where technically feasible” since the new wording in R1.5.1 provides options for an entity to determine production environment tests that minimize adverse effects.
Yes
Yes
R2.1 – The measures state that evidence may include “Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information…” PSE requests clarity as to what form of record should be produced to provide evidence that action has been taken. Does the SDT believe that an attestation from the individual performing the action or a completed change control document would constitute sufficient evidence? R2.2 - The measures stat that evidence may include "Other records showing actions taken to prevent unauthorized retrieval such as encrypting, retaining in the Physical Security Perimeter;" PSE requests clarity as to what form of record should be produced to provide evidence that action has been taken. Does the SDT believe that an attestation from the individual performing the action or a completed change control document would constitute sufficient evidence?
Group
PNM Resources
Michael Mertz
No
No
No
See comment submission from EEI.
No
No
No
See comment submission from EEI.
See comment submission from EEI.
No
No
No
See comment submission from EEI.
No
No
See comment submission from EEI.
Individual
Scott Harris
Kansas City Power & Light
No
No
Yes
R1.2: The definition of reportable cyber security incident is unclear. DOE form 417 explains what must be reported. R2: Add “except for CIP exceptional standards.” To the requirement
No
Yes
Yes
R1.4: The only way to ensure that a backup was completed successfully is to restore data from a backup. Suggested change: 1.4 Incomplete or failed backups for information essential to BES Cyber System recovery shall generate alerts.

No
No
No
General: In all requirements sections, remove references to systems & assets and rely on the applicability column to specify applicability. R1: R1 is too prescriptive. Recommend that the CIP v3/v4 language replace 1.1-1.4, but specifically address the Order 706 requirements for malicious changes. Remove Associated assets/systems from applicability because they represent an increase in scope from CIP v3/v4. R1.1-R1.4: Adjust requirement to require a baseline configuration for only devices that use a routable protocol. All devices will require entities to make increased financial and manpower investments to comply. It does not recognize the other controls for hardware or software changes, malware and virus defenses, or physical and electronic access controls to prevent unauthorized changes. Recommend that the CIP v3/v4 language replace 1.1-1.4, but specifically address the Order 706 requirements for malicious changes. Add “with External Routability” to Medium Impact BES Cyber Systems. R2: Remove Associatted assets/systems from applicability because they go beyond Order 706. R2.1: Adjust requirement to require a baseline configuration for only devices that use a routable protocol. All devices will require entities to make increased financial and manpower investments to comply. It does not recognize the other controls for hardware or software changes, malware and virus defenses, or physical and electronic access controls to prevent unauthorized changes. Remove Associated assets/systems from applicability because they go beyond Order 706. R3.2: Remove the words “that models the baseline configuration of the BES Cyber System in a production environment” after the parentheses. R3.3: Change the words “prior to adding” to “as part of the change prior to completing the commissioning of”. R3.4: Change the requirement to read: “Document identified vulnerabilities. Establish planned or completed dates relating to the mitigation or remediation of identified vulnerabilities.” Rationale: As worded, the language increases the compliance-tracking burden to all sorts of other documentation including action plans, plan status, etc. The proposed language shifts the focus of the requirement back towards a cyber security related outcome, i.e. mitigated vulnerabilities. This is accomplished by staying away from language that requires documentation overhead. Language on action plans should be moved into the guidance documentation.
No
No
R1.2: What is meant by transmittal, distribution and disposal requires further clarification and parameters in the Measures section. Suggested change: One or more documented and implemented procedures for handling BES Cyber System Information. Information handling procedures shall detail access, sharing, copying, transmittal, distribution, and disposal or destruction of BES Cyber System Information. R1.3: Suggested Change: Once each calendar year or a period not to exceed 15 months, assess adherence to its BES Cyber System Information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. R2.1: Suggested change: Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except in other high impact or medium impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Asset), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset. If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information, the responsible entity shall maintain documentation that identifies who has possession of the device while it is outside of a Physical Security Perimeter. R2.2: Suggested change: Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media. If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity shall maintain documentation that identifies who has possession of the device while it is outside of a Physical Security Perimeter.
Individual
Richard Vine
California Independent System Operator

Yes
Yes
Yes
None
No
No
Yes
CIP-009-5 R1 – Suggest in Part 1.3 change the word “recover” to “restore”. In Part 1.4 change the word “recovery” to “restoration”. Define the terms recover, recovery, restore and restoration. Recovery – Implementing the prioritized actions required to return the processes and support functions to operational stability following an interruption or disaster. Restoration – Implementing actions for the repair or relocation of the primary site and its contents, and for the resumption of normal operations at the primary site. Part 1.4 reference backup media however this technology is antiquated and entities are using redundancy for restoration in which these requirements do not pertain. Change 1.3, 1.4, 2.1 and 2.2 to remove High Impact BES cyber systems from scope CIP-009-5 R2 - Part 2.2 references backup media however this technology is antiquated and entities are using redundancy for restoration in which these requirements do not pertain. Part 2.3 should reference EOP-008 in that EOP-008 would suffice meeting this requirement. Change 2.3 to say: “At least every 90 days, demonstrate that primary and backup BES cyber systems are independently capable of providing operational functionality to the associated control center.” Note: this wording attempts to be consistent with EOP-008 R6.
No
No
No
CIP-010-1 R1 - Part 1.4.1 – this can introduce double jeopardy in that non compliance with this requirements means non-compliance with the requirements in the referenced standards. Part 1.5.1 – remove the parenthesis but keep the text. What does “technically feasible” pertain to in this requirement? Part 1.5.2 – ISO/RTOs believe that testing in a production environment is not a sound security practice. CIP-010-1 R2 - Part 2.1 – Remove the words “continuously” CIP-010-1 R3 - Part 3.1 the requirement is redundant to 1.3. A vulnerability assessment should not be a compliance check. Part 3.3 and Part 3.4 define what is meant for a vulnerability assessment. Is it a “nessus scan” or is it a compliance check for CIP requirements? Applicable BES Cyber Systems and associated Cyber Assets differs between Part 3.3 and Part 3.4.
Yes
No
CIP-011-1 R2 - Part 2.1 appears to be two requirements and should be broken out if that is the intent. The current wording appears to pertain to cyber assets that contains BES Cyber System Information (i.e network diagram). The second sentence appears to pertain to Cyber Assets within an ESP.
Group
Hydro One
Sasa Maljukan
No
No
No
Request clarification on the EOP-004-2 reference in the R1 Rational. The previous version of EOP-004-2 was not accepted by the industry. What is the plan if future versions of EOP-004-2 are not accepted? Recommend changing the first bullet in R2 Part 2.1 from “By responding to an actual Reportable Cyber Security Incident; ” to “By responding to a Cyber Security Incident” since this covers the Reportable Incidents plus the non-reportable incidents Recommend updating R2 Part 2.3 since the existing language does specify a retention period. Recommend changing R3 Part 3.1 from “Review and update” to “Review and update, as needed,” since some years the Cyber Security

Incident response plan will not need updating Recommend changing R3 Part 3.3 from “Update the Cyber Security Incident response plan ” to “Update, as needed, the Cyber Security Incident response plan”
No
No
No
Is a Business Continuity Plan, where operations are transferred from the main control centre and continued at a back-up control centre, considered a recovery plan?
Recommend removing R1 Part 1.5 since this Requirement is forensics and/or Lessons Learned. The priority is Reliability or recovery, forensics. The title of this Standard is Recovery Plans for BES Cyber Systems. Request clarification on R2 Part 2.2. Is this a media test? Can the test be on a sample BES Cyber System? Recommend updating the Measure for R2 Part 2.3 to reference an updated Implementation Plan’s Initial Performance of Certain Period Requirements. This Requirement – Part combination is not identified in the existing Periodic Requirements. As requested in the first posting, request removing these bookends from this Measure Recommend changing from the reference from “R1.2” to “Part 1.2” in R3 Part 3.4 for correctness
No
No
No
Request clarification of R1 Part 1.1.2. Does “applications” mean “SCADA, EMS, State Estimator, IDC, etc” instead of “device drivers, DLL, applications included in an operating system or package, etc?” Request clarification of R1 Part 1.1.3. Would a version control tool/system (like CVS) demonstrate the custom software’s version? Request clarification on R1 Part 1.3. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005 and CIP-007? In R1 Part 1.3, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations Recommend removing the 30 day time frame in R1 Part 1.3 that applies to CIP-005 and/or CIP-007. Those Standards should specify their time frames. Recommend that the 30 days apply to only updating the baseline configuration (this Part) Request clarification on R1 Part 1.4.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? In R1 Part 1.4.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations Recommend removing R1 Part 1.4.2 because “availability” has not been part of the Requirements in the past, is not a FERC requirement and can be interpreted multiple ways In R1 Part 1.5, recommend changing from “Where technically feasible, for each change that deviates from the existing baseline configuration ” to “Testing cyber security control, where technically feasible, for each change that deviates from the existing baseline configuration” for clarity For R2 Part 2.1, recommend the previous version 5 words since this updated Part is not understandable Request clarification on R3 Part 3.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? In R3 Part 3.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations Recommend that R3 Part 3.1start with its purpose – for example, Active vulnerability assessment Request clarification on R3 Part 3.2. If this is a paper exercise it should be performed once every 36 months. Recommend that R3 Part 3.2 start with its purpose – for example, “Perform active vulnerability assessment, where technically feasibly….”. Recommend that R3 Part 3.3 start with “Perform an active vulnerability assessment, of the new cyber assets prior to business deployment, except for CIP Exceptional Circumstances and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset).” Recommend updating CIP-010 R1’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures shows R1 as “low” Recommend updating CIP-010 R2’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures shows R2 as “low”
Yes
No
Recommend moving the second paragraphs of R2 Parts 2.1 and 2.2 into a new Part 2.3 for clarity.

Name (59 Responses)
Organization (59 Responses)
Group Name (36 Responses)
Lead Contact (36 Responses)
Question 1 (85 Responses)
Question 2 (85 Responses)
Question 3 (85 Responses)
Question 4 (83 Responses)
Question 5 (84 Responses)
Question 5 Comments (95 Responses)
Question 6 (84 Responses)
Question 7 (84 Responses)
Question 8 (0 Responses)
Question 8 Comments (95 Responses)
Question 9 (0 Responses)
Question 9 Comments (95 Responses)
Question 10 (0 Responses)
Question 10 Comments (95 Responses)
Question 11 (0 Responses)
Question 11 Comments (95 Responses)
Question 12 (0 Responses)
Question 12 Comments (95 Responses)
Question 13 (0 Responses)
Question 13 Comments (95 Responses)
Question 14 (0 Responses)
Question 14 Comments (95 Responses)
Question 15 (77 Responses)
Question 15 Comments (95 Responses)
Question 16 (0 Responses)
Question 16 Comments (95 Responses)
Question 17 (0 Responses)
Question 17 Comments (95 Responses)

Individual
David Proebstel
Clallam County PUD No.1
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Individual
Michelle R D'Antuono
Ingleside Cogeneration LP
No
Yes
Yes
Yes
Yes
Yes
Yes
For the most part, Ingleside Cogeneration LP supports the transition of asset-based cyber protection to one based on BES Cyber Systems. The concept reflects the fact that attackers look to compromise distributed systems, not necessarily individual components. A system-based approach should capture weaknesses that are not obvious when looked at in piece-part. However, we are concerned with the elimination of redundancy as a consideration as required in the definition of BES Cyber Asset. It includes a statement that the redundancy of “affected Facilities, Systems, and equipment shall not be considered when determining adverse impact.” As a time tested way to preserve reliability, we don’t see why such a technique can be dismissed out of hand. Ingleside Cogeneration fully understands that a cyber attack may simultaneously compromise multiple systems, but there are methods to reduce the risk – for example, by using redundant systems using fundamentally different programmable components/schema. Every tool in the toolbox must be available. However, the definition as written provides an economic disincentive to use redundancy to protect against cyber intrusions. We don’t believe this is the drafting team’s intent, and we recommend the sentence be removed.
Group
Northeast Power Coordinating Council
Guy Zito
No
Yes
Yes
Yes
Yes
No
No
For clarity, suggest changing the BES Cyber Asset definition from "it is directly connected to a Cyber Asset within an ESP" to "it is directly connected to a network, or to a Cyber Asset within an ESP".

Request clarification on the definition of EAP. Must it be routable protocol on both sides?
The definition of Reportable Cyber Security uses the terms "compromised" and "disrupted" plus the phrase "reliability tasks of a functional entity". All three need their own definition/clarification.
No
Although the proposed Version 5 Implementation Plan states that “Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan,” there are concerns that need clarification. The concerns refer to the transition from the currently effective Version 3, through Version 4 and finally to Version 5. Given that (a) the Version 4 Standards and associated Implementation Plan were recently approved by FERC; (b) the proposed Version 5 Implementation Plan contains a minimum 24-month period for enforcement means that there will be a period of time during which Version 4 would be effective; and (c) when Version 4 becomes effective there will be newly identified CAs that will have to be made compliant. In order to comply with Version 4 requirements, entities will be need to allocate funding and resources to perform work necessary to become compliant at newly identified facilities. Much of this work must be performed in anticipation of the enforcement date. Once Version 5 becomes effective, application of the proposed categorization of BES Cyber Systems may very well result in much of the work done for Version 4 compliance being in the end unnecessary. Request clarification on the Disaster Recovery's "completion of the restoration activities" (top of the clean version's page 5). What event/action/etc. signifies this completion?
Section 5 for CIP-003-5 is the only place that explains how to read the bullets and numbers in the Measures. From the second paragraph of Section 5, "Measures provide examples of evidence to show documentation and implementation of the requirement. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence." Request clarification this bullets and numbers explanations applies to the Requirements and Applicability sections of each of CIP-002-5 - CIP-011-1. If this was the SDT's intent, then recommend this clarification be added to Section 5 of each of CIP-002-5 - CIP-011-1. General comment--recommend that each Requirement’s Part identify that Part’s goal.
Individual
Frank Dessuit
NIPSCO
No
Yes
Yes
Yes
No
No
No
We agree with the new definitions of BES Cyber System and BES Cyber Asset. However, NIPSCO requests what is the definition of “programmable” electronic device and what is included in such device. In addition, it is recommended that the word “data in those devices” be removed from the description.
NIPSCO requests further review of the description and recommends that the description should include a defined list of what is included in the PSP
NIPSCO requests elimination of “Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants” from the definition of Interactive Remote

Access.
NIPSCO request the addition BES Cyber Asset be added to the scope of the ESP definition. . NIPSCO requests that the term “cyber system” be changed to a “cyber asset,” to the scope of the external routable connectivity definition.
NIPSCO requests further clarification on what is meant by an, “attempt to disrupt” and an “attempt to compromise” as it is applied to an event and how to show evidence of such intent. NIPSCO recommends to use either “compromises” or “confirmed attempt to disrupt,” to replace attempt to disrupt and attempt to compromise. NIPSCO request clarification for “reliability tasks”. Are they the same reliability tasks as required by PER-005?
Yes
Individual
Roger Dufresne
Hydro-Québec Production
Yes
Yes
Yes
Yes
Yes
No
Yes
"Protected cyber asset" definition is hard to understand and confusing. Clarification should be done with a more concise ans structure statement.
Group
Comment Development SME List
Gerald Freese
No
Yes
Yes
Yes
No
Yes
Yes
(1) BES Cyber Asset - The third sentence states "Each BES Cyber Asset is included in one or more BES Cyber Systems." This statement adds no additional substance to the definition. It should be removed and placed into guidance for determining BES Cyber Systems. 2) BES Cyber System – The definition is not clear as to whether the BES Cyber Assets need to be connected to and/or interact

with each other to be considered a BES Cyber System. For example, would a group of 6 protective relays in the field that are all performing protection functions for a generating unit be considered a BES Cyber System if they are not connected together.
1) Intermediate Device – The second sentence should be removed from the definition. The second sentence is stating a required architectural design. If it is a required design then it should be covered in a requirement and not stated in a definition; we recommend adding the statement to a requirement in CIP-005.
Yes
(1) BES Cyber Asset - The third sentence states "Each BES Cyber Asset is included in one or more BES Cyber Systems." This statement adds no additional substance to the definition. It should be removed and placed into guidance for determining BES Cyber Systems. (2) BES Cyber System – The definition is not clear as to whether the BES Cyber Assets need to be connected to and/or interact with each other to be considered a BES Cyber System. For example, would a group of 6 protective relays in the field that are all performing protection functions for a generating unit be considered a BES Cyber System if they are not connected together. (1) Intermediate Device – The second sentence should be removed from the definition. The second sentence is stating a required architectural design. If it is a required design then it should be covered in a requirement and not stated in a definition; we recommend adding the statement to a requirement in CIP-005.
Individual
Michael Falvo
Independent Electricity System Operator
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Steven Powell
Trans Bay Cable
No

Yes
Yes
No
No
Data Centers need to be definded. This term was added in CIP V5 and a definition should be provided to ensure consistancy across all RC's
Yes
Yes
Add definition for data center
No
No address of CIP V4 was made
Group
Southwest Power Pool Regional Entity
Emily Pennel
No
Yes
No
No
Yes
No
No
The definition of Cyber Asset ignores data in motion. The definition either needs to drop the added language “in those devices” or add language regarding data both at rest and in motion.
No
The definition of CIP Exceptional Circumstances includes the condition “an imminent or existing hardware, software, or equipment failure.” This language essentially eliminates the need for conducting a personnel risk assessment and Cyber Security training for vendor support staff. The condition needs to be modified to permit the exceptional circumstance only in the event of a failure requiring vendor support from personnel that do not routinely support the impacted system. The idea is that the call center technical support team (such as from Cisco or Oracle) could provide support in an exceptional circumstance but routine support from, for example, an EMS vendor would require the support staff to have been pre-trained and pre-screened.
Physical Access Control Systems need to include the workstations used to provision access rights and to monitor alarms. The Physical Security Perimeter needs to include the qualification “capable of deterring unauthorized physical access.” A gate and climbable fence do not deter unauthorized access and should not be considered a physical border for the purposes of the definition.
No
The Electronic Access Point definition needs to say “allows or is capable of allowing” routable communication in order to pick up a dual-homed Cyber Asset, including laptops with wireless not hardware-disabled. The External Routable Connectivity needs to consider inside-to-outside connectivity and not just outside-to-inside connectivity.
Reportable Cyber Security Incident needs to include an incident that has compromised or disrupted a

BES Cyber System whether or not the reliability tasks of a functional entity have been compromised or disrupted. Otherwise, entities will argue that redundancy eliminates the need to report because the ability to fail over to a backup system means operations was not disrupted.
No
The requirements of CIP-005-3 R2 are not sufficiently unique or complex as to warrant an additional year to implement. Responsible Entities will be able to leverage their High and Medium impacting controls to apply to the Low Impacting systems. Additionally there is no reason why the first instance of a requirement cannot be performed within the two year preparation time prior to the effective date of the standards. Why would you allow, for example a year after the effective date of the standards to conduct the first training or to verify that provisioned access is correct?
None
Individual
Thomas A Foreman
Lower Colorado River Authority
Yes
Yes
Yes
Yes
Yes
Yes
No
Change the definition for Cyber Security Incident as follows: Cyber Security Incident Any A malicious act or suspicious event that: • Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System.
Yes
Individual
Glen Sutton
ATCO Electric
Yes
Yes
Yes
Yes
Yes
CIP-002 provides examples or Electronic access control and monitoring systems as well as Physical access control systems. These could be removed from CIP-002 and added to the definitions for these defined terms
Yes
Yes

Yes
Group
NRG Energy Companies
Alan Johnson
No
No
Yes
Yes
Yes
No
No
The BES Cyber system classification should be empirically clear to correlate the facility impact rating criteria per CIP-002-5 Attachment 1 with the classification of impact of associated BES systems within that facility. For example, a high impact facility must classify the BES systems as only high impact.
1. Definition is incomplete with the inclusion of BES Cyber Assets/Systems. Proposed new definition of Control Center: “One or more facilities hosting BES Cyber Assets/Systems including operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability functional tasks of:…….” 2. In addition, the threshold for control centers at generation facilities exceeding 300MWs and under 1500MWs, as written, is classified as medium impact. This classification should exclude those facilities that provide control of remote sites such as gas turbines. Generally these remote sites would be considered low impact facilities but due to the central dispatch, these sites automatically are classified as medium impact facilities. Please clarify. 3. The generation control center definition should further delineate if the BES systems are shared or not. There are scenarios that exist with more than one entity dispatched from one center and no shared BES system exists between the entities. This should not result in inclusion as medium impact risk to the BES as currently written.
Does the definition of ESP presume the presence of an Electronic Access Point? In other words, does a BES Cyber System with no External Routable Connectivity fall within the scope of the CIP standards? Clarifying this point will pre-empt the need for interpretation or a CAN later.
Cyber Security Incident – remove the words “or suspicious event”. Suspicious is too vague and subject to interpretation. Suggest the definition be changed to: “A malicious act that (1) Compromises, or was an attempt to compromise a BES Cyber System, and (2) Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.”
Yes

Individual
Martyn Turner
LCRA Transmission Services Corporation
Yes
Yes
Yes
Yes
Yes
Yes
No
Change the definition for Cyber Security Incident as follows: Cyber Security Incident Any A malicious act or suspicious event that: • Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System.
Yes
Individual
Jianmei Chai
Consumers Energy Company
No
Yes
Yes
Yes
Yes
Yes
Yes
BES Cyber Asset - The definition of BES Cyber Asset continues to remain vague. Although CIP-002 and the SDT have made progress toward creating “bright-line” evaluation criteria in the standard and Attachment I for Facilities, Systems and equipment, by using the phrase “adversely affect the reliable operation” in the definition, the BES Cyber Asset definition continues from Draft #1 to not provide bright-line criteria. BES equipment is frequently removed from operation with no reliability effect, yet would be in-scope in the proposed standard. In addition, not all BES facilities, systems and equipment, nor cyber/programmable devices, are of the same value or importance of function. In the proposed standard, a configurable electronic panel meter (providing local, seldom-used indication) in a substation, would rise to the same level of compliance as an RTU or protective relay in that same substation. In this regard, we recommend that the SDT consider developing bright-line criteria that could be used for defining BES Cyber Assets at different levels based on the asset’s impact of MW levels, system disturbance potential, or other substantial BES events. In Attachment 1, Section 2, (and especially item 2.5) the SDT seems comfortable eliminating applicability for facilities of lower voltages or MW value. It would seem foolish to then include cyber assets at other facilities, if the impact on reliability due to a compromised cyber asset was small.

No
Page 5 of the clean version Implementation Plan states “The following security requirements in CIP-003 through CIP-011 apply to …..”, however, there is no CIP-003 requirement included. Please correct as needed. Several Implementation Plan associated requirements (e.g. CIP-003-5 R2.4, CIP-007-5 R7.2, CIP-010-1 R3.1 & R3.3, etc.) need to be revised before they could have appropriate implementation schedule.
Individual
Joe Petaski
Manitoba Hydro
Yes
No
No
No
Yes
Yes
Yes
We suggest adding the word “NERC certified” before “operating personnel”.
It is not clear what the “unauthorized distribution” mean. Authorized distribution should be clarified.
Given that the handling of a PACS alert could be a cell phone, an email server or a PC, it doesn’t mean they become the PACS. Only the computer that initiates the alert should be considered part of the PACS. We suggest changing “alert” to “initiate alerts”.
No
Individual
Michael Schiavone
Niagara Mohawk (dba National Grid)
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
We recommend adding definition of “annual” to the definitions document. The definition should be “once per calendar year”.
Individual
Michael Jones
National Grid
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
We recommend adding definition of “annual” to the definitions document. The definition should be “once per calendar year”.
Individual
Jonathan Appelbaum
United Illuminating company
Yes
Yes
Yes
Yes
No
UI believes that Electronic Access Control or Monitoring System this is limited to the firewall appliance that gathers traffic information and enforces the ruleset. Informally UI has heard that this term is meant to include or log monitors and gathering appliances, any devices that analyze logs and generate alerts, the password servers, and it applies to both remote access communication and individual log ons. The scope should be narrowed to all the controls around the firewall appliance.
Yes

Yes
UI Agrees with EEI Consensus comments
UI Agrees with EEI Consensus comments
UI Agrees with EEI Consensus comments
UI Agrees with EEI Consensus comments
UI Agrees with EEI Consensus comments
UI Agrees with EEI Consensus comments
UI Agrees with EEI Consensus comments
Yes
UI Agrees with EEI Consensus comments
UI Agrees with EEI Consensus comments. In addition Ui would appreciate the incorporation of allowable defects and corrections in the implementation of the CIP program. NIST does allow a security program to identify and self-correct errors as a control. UI would also like the introduction of escorted electronic access via WEBEX remote sessions to allow for SCADA support, maybe limited to Medium assets. We also believe the Standards force each SCADA support Vendor to take each entity's training program when this is very inefficient.
Group
Arizona Public Service Company
Janet Smith
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Alice Ireland
Xcel Energy
Yes
No
No
Yes
Yes
Yes

No
For item 4) we suggest that the intent needs to be made clear that this applies to BES assets, and that location should be defined. We propose the following revision: "…4) a Generator Operator for BES generation Facilities at two or more locations. A location is defined as a separate property with a continuous physical boundary."
The definition of CIP Exceptional Circumstances has been changed to include "an imminent or existing hardware, software, or equipment failure…" As written, this is far too broad (for example, as written, each time we have a single asset fail we could declare an Exceptional Circumstance). At a minimum, this phrase should be re-written to narrow its scope or, even better, stripped out entirely from the definition.
The definition of cyber security incident now includes "Physical Security Perimeter." This is a significant change in the definition of a cyber-security incident and the impact will be difficult to assess. The definition is also narrowed to "Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter" or "Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." Disruption is not defined and it is unclear if non-malicious "disruptions" are excluded.
Yes
Group
PNGC Comment Group
Ron Sporseen
Yes
No
Yes
Yes
Yes
Yes
Yes
Control Center – NRECA is concerned that in this definition the mere presence of a SCADA HMI might be considered a Control Center by a CEA if it could possibly be used to control BES assets in real-time even if an entity does not use it that way. Some of the registered entities do not man these control centers 24/7 and are unable to perform real time control after hours, or any other time that other duties take them 15 minutes away from the computer. In some instances these entities might be registered as TOPs only because they own a limited and discrete 115 kV facility that no other entity was willing to register as a TOP for. Often times this 115 kV facility performs no reliability function. NRECA suggests adding "24/7 to the first sentence of the Control Center definition as shown in the underlined text: "One or more facilities hosting operating personnel 24/7 that monitor and control the Bulk Electric System (BES) in real-time …"
CIP Senior Manager – In this definition replace "CIP Standards" with CIP-002 through CIP-011. If this is not completed, this definition would apply to CIP-001 which still exists and is an unrelated standard. This revision will provide clarity to the limit of the definition.

Yes
Individual
John Souza
Turlock Irrigation District
Yes
Yes
Yes
Yes
Yes
No
Yes
In the definition of an ESP, we believe that "BES Cyber Systems" should be changed to "BES Cyber Assets" because entities are allowed to group such Assets into Systems at their discretion and the grouping they select may result in a particular ESP surrounding only a portion of a System and other ESPs surrounding the remaining portions of the System.
No
See question 16 comment
Although we agree with the Implementation Plan in general, we believe that the last section of the Plan which contains a table showing which Requirements apply to Associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets is redundant and should be removed. The Standards already contain this information in a more granular form (at the sub-part level). If the table remains as part of the Implementation Plan then it should include the same granularity of the Standards. Also, there are a number of errors in the table, such as: (1) the introductory sentence states “CIP-003 through CIP-011” however, CIP-003 is not part of the table, (2) CIP-005 has one part (part R1.2) which is applicable to Protected Cyber Assets but is not listed in the table, (3) CIP-009 has various Requirements which are missing from the table.
In all places where the statement “Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and ....” should be revised now that CIP Version 4 has been approved by FERC. We would like to thank and applaud the members of the SDT for the work they have done, especially for the work involved in this second draft.
Individual
Chris Higgins on behalf of BPA CIP Team
Bonneville Power Administration
No
Yes
No
Yes
No
No

No
BES Cyber Asset: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.) Regarding the BES Cyber System: BPA has no comments. Cyber Asset: Facilities, Systems, or equipment which if destroyed, degraded, or otherwise rendered unavailable when needed, would prevent the responsible entity from maintaining the reliable operation of the BES. (e.g. criteria specified in CIP-002-5, Attachment 1 - Impact Rating Criteria)
Regarding BES Cyber System Information: BPA believes the definition is acceptable, it could be made clearer by breaking the second sentence into a list, as in limited to: Security procedures developed by the responsible entity; Security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that could be used to allow unauthorized access or unauthorized distribution; Collections of network addresses; or Network topology of the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, and not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Regarding CIP Exceptional Circumstances: It is often impossible to determine the outcome of a situation until after the fact. BPA recommends: A situation that involves or threatens to involve more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability. Regarding CIP Senior Manager: BPA has no comments.
Regarding Electronic Access Control and Monitoring Systems: BPA has no comment. Regarding Interactive Remote Access: BPA thinks that including "Interactive remote access does not include system-to-system process communications." is appropriate and has concerns with the other parts of this definition. In particular, BPA believes that trying to list all the possibilities is confusing and unnecessary. BPA suggests the following rewording: Interactive Remote Access: All human-initiated routable or dial-up access that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s). (Ownership of the Cyber Asset used to initiate Remote Access is not relevant to the definition of Remote Access.) Interactive remote access does not include system-to-system process. Regarding Intermediate Device: The second sentence states an unnecessary requirement that would not increase the security of the systems NERC CIP is intended to protect. BPA believes it should be deleted.
Regarding Electronic Access Point: BPA has no comment. Regarding Electronic Security Perimeter: BPA has no comment. Regarding External Routable Connectivity: BPA believes that "External Routable Connectivity" should only apply if the routable connection goes all the way to the BES Cyber Asset. Since this has been a topic of concern in the past, BPA suggests the following revision: External Routable Connectivity: A BES Cyber System that is accessible from a Cyber Asset that is outside the BES Cyber Asset's associated Electronic Security Perimeter via a bi-directional routable protocol connection terminating at a BES Cyber Asset that is part of the BES Cyber System. Regarding Protected Cyber Asset: As stated, the definition would cause maintenance devices such as handheld cable testing devices to be included as Protective Cyber Assets, even if they were only connected to the network for a few seconds. At the same time, BPA realizes that any network device poses a higher risk than a directly connected device. BPA suggests the following revision: A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter (A Cyber Asset is not a Protected Cyber Asset if it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes and it is directly connected to a Cyber Asset within an ESP or to a BES Cyber Asset for 30 consecutive calendar days or less, or used for such purposes and connected for less than 30 days to a routable network within an ESP protecting BES Cyber Assets.).
Regarding Cyber Security Incident: BPA recognizes that the proposed definition combines two

separate types of incidents; a cyber incident and a physical security incident. Unauthorized physical access into a physical security perimeter does not automatically lead to a “cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, miss-operation, or non-operation, adversely impact one or more Facilities, Systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System.” Unauthorized entry or access to a facility containing such cyber assets can be one of many types of incidents; burglary, theft, or inadvertent circumvention of a policy, practice or system. Thus it would be classified as a physical security incident and handled accordingly and not as a Cyber Incident. Combining the two events together will potentially lead to the false classification and analysis of events. BPA believes that Physical Security Incidents should be a separate category of incident, and only when a physical security incident is shown to be related to an attempt to disrupt the BES should it be examined in context of a cyber security incident, and only if there are indications of a cyber security nexus. Regarding Reportable Cyber Security Incident: BPA believes this definition is too open. Many events may compromise or disrupt one or more reliability tasks and may not be caused by a person, not be done with malicious intent and in the end, not be determined to be a cyber security issue at all. Suggested Change: Any Cyber Security event that has compromised or disrupted one or more reliability tasks of a functional entity, which through investigation and escalation, has been determined by the Responsible Entity to be reportable to ES-ISAC.
Yes
Individual
Benjamin Beberness
Snohomish County PUD
No
No
Yes
No
Yes
Yes
Yes
BES Cyber Asset, BES Cyber System, and Cyber Asset: The draft CIP versions 5 Reliability Standards are very BES definition centric. Due to the proposed changes to the BES definition it is very difficult for the electric industry to comment on a standard as it is unclear if the currently or proposed BES definition will be applied. This change in the definition could significantly change the applicability of the version CIP Reliability Standards. Although it is clear the SDT has made attempts to size the applicability of the CIP version 5 requirements with the size of the registered entity, the current draft will cause significant resource burdens on facilities that have demonstrated they cannot impact the reliability of the Bulk Electric System. As a Transmission Dependent Utility SNPD supports a reliable system because we are at the end of the system and SNPD’s customers are exposed to all disturbances on the main grid. However SNPD also support efficiency and spending significant resources with little to benefit is not beneficial to the reliability of the BES or to the Level of Service (“LOS”) SNPD provides its customers. Control Cente: SNPD disagrees with the CIP-002-5, 2.11 as it dictates that all registered Balancing Authorities and Transmission Operators are automatically assigned a Medium Impact Rating (M). There are many very small Balancing Authorities and Transmission Operators that have little to no reliability impact to neighboring systems and should not be included as a medium impact rating. In addition the assigned registration as a TOP is extremely subjective. The NERC Statement of Compliance Registry Criteria (“SCRC”), section III (d), uses the same criteria to define both Transmission Owner (“TO”) and Transmission Operator (“TOP”) . In addition, the application of this criteria, especially as to under what circumstances an entity is a TO and not a TOP is not defined and is not consistent through the regions. SNPD supports removing section 2.11 as there is no “reliability based” justification that registration as TOP justifies a Medium

Impact Rating.
The draft CIP versions 5 Reliability Standards are very BES definition centric. Due to the proposed changes to the BES definition it is very difficult for the electric industry to comment on a standard as it is unclear if the currently or proposed BES definition will be applied. This change in the definition could significantly change the applicability of the version CIP Reliability Standards. Although it is clear the SDT has made attempts to size the applicability of the CIP version 5 requirements with the size of the registered entity, the current draft will cause significant resource burdens on facilities that have demonstrated they cannot impact the reliability of the Bulk Electric System. As a Transmission Dependent Utility SNPD supports a reliable system because we are at the end of the system and SNPD's customers are exposed to all disturbances on the main grid. However SNPD also support efficiency and spending significant resources with little to benefit is not beneficial to the reliability of the BES or to the Level of Service ("LOS") SNPD provides its customers.
The draft CIP versions 5 Reliability Standards are very BES definition centric. Due to the proposed changes to the BES definition it is very difficult for the electric industry to comment on a standard as it is unclear if the currently or proposed BES definition will be applied. This change in the definition could significantly change the applicability of the version CIP Reliability Standards. Although it is clear the SDT has made attempts to size the applicability of the CIP version 5 requirements with the size of the registered entity, the current draft will cause significant resource burdens on facilities that have demonstrated they cannot impact the reliability of the Bulk Electric System. As a Transmission Dependent Utility SNPD supports a reliable system because we are at the end of the system and SNPD's customers are exposed to all disturbances on the main grid. However SNPD also support efficiency and spending significant resources with little to benefit is not beneficial to the reliability of the BES or to the Level of Service ("LOS") SNPD provides its customers.
No
Group
PPL Corporation NERC Registered Affiliates
Stephen Berger
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

1.) PPL Affiliates recommend addition of definitions of “Impact” and “Adverse” in regards to CIP-002 (BES Adverse Reliability Impacts). 2.) PPL Affiliates recommend the addition of a definition for “Common Control System” in regards to CIP-002 Attachment 1, Section 2.10.
Individual
Larry Watt
Lakeland Electric
No
No
Yes
No
No
"Please see comments submitted by FMPA through the formal comment process."
No
No
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
Yes
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
Individual
Ron Donahey
Tampa Electric Company
No
Yes
Yes
Yes
Yes
Yes
No
Tampa Electric recommends that the SDT improve the definition of the BES Cyber Asset, Cyber System, and Cyber Assets related to “adversely impact” one or more BES Reliability Operating Services in order to provide clarity. The current NERC Glossary of Terms used in NERC Reliability Standards shows: Adverse Reliability Impact (BOT Approved: 2/7/2006 FERC Approved: 3/16/2007 [Archive] The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection. Adverse Reliability Impact (BOT Approved: 8/4/2011 FERC has not approved) [Archive] The impact of an event that results in Bulk Electric System instability or Cascading.
BES Cyber Asset – • redundancy shall not be considered - does this go against the basic tenets of system planning? How does this affect subs when load is automatically re-routed: • 30 consecutive calendar days or less – what does this mean? Are we talking about USB connected devices? Why not spell out qualified devices, e.g., non-cyber devices, laptops, etc. External routable connectivity – do

we need a definition of routable? Intermediate device – what security is required for the intermediate device? Does this leave a risk that entities might leave it on the corporate network? Transient cyber asset –check 'final' (remove redline)
The SDT should consider definitions should reflect the language in the OE-417 to enable entities to comply with both sets of requirements.
Yes
Tampa Electric suggests that the SDT review the table on the pp. 5-6 for security requirements that apply to EACMs, PACS, or Protected Cyber Assets. We noted that there may be discrepancies for the determination of what applies to which systems.
Tampa Electric appreciates the efforts of the Standards Drafting Team, NERC, and Registered Entities in the development of version 5 of the CIP standards.
Individual
Annette Johnston
MidAmerican Energy Company
No
No
No
No
No
Yes
No
(1) BES CYBER ASSET: The word "Systems" should not be capitalized. "Systems" is not a defined term. (2) BES CYBER SYSTEM: No comment. (3) BES SITES: In conjunction with our CIP-002 comments, we propose a new definition be created for BES Sites. Substations 100kV and above, generating units above (insert # to set the floor) MW (MVA?), control centers and backup control centers used by NERC certified operators to support the real time operations of the interconnected Bulk Electric System, Blackstart Resources, Cranking Path and initial switching requirements. [Note to SDT: The lists are based on existing lists entities need for Operating and Planning Reliability Standards applicable to their NERC registration criteria.] Consider also if "BES CIP Sites" would be better to reserve the definition solely for CIP and avoid future possible issues or confusion with Operations and Planning Reliability Standards. (4) CYBER ASSET: No comment.
(1) CONTROL CENTER: V5 creates a CIP-specific definition of Control Center. CIP standards are not the only NERC standards using the term. The CIP definition does not fit the context of the other NERC standards. Multiple definitions across reliability standards for the same term are confusing to implement and complicate auditing. The 300 MW threshold in the proposed V5 definition has little basis relative to reliability. Control center should remain undefined in the CIP V5 standards and all references should be lower case. Create a separate project for creation of a definition that would apply across all NERC standards – consistent with strategy for one of EEI's key issues.
(1) BES CYBER SYSTEM INFORMATION: MidAmerican Energy would support the revised definition, if the following sentence was removed from the definition and put into guidelines: "Examples of BES Cyber System Information may include, but are not limited to, security procedures developed by the responsible entity and security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System." (2) CIP EXCEPTIONAL CIRCUMSTANCES: We appreciate revisions made to the definition to allow "similar conditions." The SDT added "an imminent or existing hardware, software, or equipment failure" in response to comments. This seems to introduce issues with other requirements. For example, equipment failures covered by this definition likely would lead to invoking the CIP-009 recovery plan. CIP-009 R1.5 requires processes to preserve data, except for CIP Exceptional Circumstances. Based on the revised definition of CIP Exceptional Circumstance, CIP-

009 R1.5 would never be required in the case of an equipment failure. (3) CIP EXCEPTIONAL CIRCUMSTANCES – USE IN THE STANDARDS: There is a lack of clarity within the standards regarding use of CIP Exceptional Circumstances, since there is not one requirement like there was in version 4 for exceptions. By specifically mentioning CIP Exceptional Circumstance in only certain requirements, does that mean it cannot be used in any requirements where it is not mentioned? The guidance on CIP-003 R1.10 is confusing. (4) CIP SENIOR MANAGER: No comments.
(1) PHYSICAL ACCESS CONTROL SYSTEMS: No comments. (2) PHYSICAL SECURITY PERIMETER: The definition is contradictory to the applicabilities throughout the standards. For example, medium impact BES Cyber Assets or Systems without external routable connectivity do not require a PSP. This issue would be resolved with the following suggested text: “the physical border surrounding locations in which applicable Cyber Assets reside, and for which access is controlled.”
(1) ELECTRONIC ACCESS CONTROL OR MONITORING SYSTEMS: The glossary term should be Electronic Access Control Systems to be consistent with the glossary term Physical Access Control Systems. Introduction of the word “perform” creates confusion. Introduction of “or BES Cyber Systems” creates confusion and potentially expands the scope. We propose the following: “Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s).” (2) INTERACTIVE REMOTE ACCESS: The definition is contradictory to requirements, since the definition currently refers to dial-up access but dial-up assets are not required to be in an ESP. We suggest the following revised introductory sentence: “All routable user-initiated access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity’s Electronic Security Perimeter(s), using a client or remote access technology.” Delete “whether routable or dial-up.” (3) INTERMEDIATE DEVICE: The definition should be revised to allow application proxy firewalls. The following is proposed: “A Cyber Asset or collection of Cyber Assets that restrict Interactive Remote Access to only authorized users. The Intermediate Device may terminate on an EAP or be external to the ESP.”
We do not have any comments on these four terms.
(1) CYBER SECURITY INCIDENT: No comments. (2) REPORTABLE CYBER SECURITY INCIDENT: The revised definition is not clear due to the use of “reliability tasks,” which is not defined or explained. We suggest this definition be an extension of Cyber Security Incident. Cyber Security Incidents include attempts, which should not be reportable. The following is proposed as the definition for Reportable Cyber Security Incidents to clearly distinguish the difference that an event must actually have compromised or caused a disruption to be considered reportable: “A Cyber Security Incident that compromised the ESP or PSP or disrupted the operation of an applicable BES Cyber Asset or low BES Site.” (3) In Order 706, paragraph 660, FERC directed the ERO to provide guidance regarding what should be included in the term “reportable incident.” The directive was for guidance, and not for this information to be included within the standard itself. Since there is no guidance for definitions, we suggest additional information and examples of Reportable Cyber Security Incidents be provided in the CIP-008 guidelines and replace the fourth paragraph in guidance for R1.
No
(1) INITIAL PERFORMANCE REQUIREMENTS: CIP-009 R1.4 refers to verifying “initially” after backup. We have proposed revised text for this requirement to remove the term “initially.” If this is not changed, the implementation plan should make it clear that entities do not have to complete this requirement until backup is performed. (The term “initially” does not refer to the initial implementation of V5.) (2) CIP-010 R3.2 is a 36-month requirement, so the initial performance should not be required in 12 months. Change the initial performance to 36 months. (3) TRANSITION FROM V4 TO V5: The following statement makes it sounds like V4 will not become effective: “Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective.” Remove this language and reconsider the July 15 references. There is now an order to implement V4. V4 was approved by FERC on April 19, 2012. V4’s effective date is April 1, 2014 (first day of the eighth calendar quarter after approval.)
(1) KEY ISSUES TO ADDRESS: MidAmerican Energy is committed to helping find solutions that will result in timely industry approval of V5, and we welcome the opportunity to discuss the key issues and solutions with the drafting team. MidAmerican Energy feels several key issues must be addressed to achieve industry approval with draft 3 and meet the targeted schedule. These issues have been discussed with other entities through EEI and other industry groups. We have incorporated details on

most of these issues and proposed solutions throughout our comments, but also provide a summary here. (a) Issue: Low Impact BES Cyber Assets in scope. There is an audit issue of providing evidence of policy implementation on low impact Cyber Assets. Solution: As discussed in our CIP-002 comments, we support the MRO NSRF's proposed revisions to CIP-002 that provides a solution to this issue. The CIP-003 R2 requirement would be applied to CIP Sites, not individual Cyber Assets. (b) Issue: Inclusion of Cyber Assets regardless of connectivity. Solution: Add External Routable Connectivity as a qualifier in the applicability column for more requirements throughout the standards. Many types of industrial control type Cyber Assets have very limited capability for a number of the CIP requirements and are generally a low security risk as an attack vector when they do not have External Routable Connectivity. Focus industry resources on higher risks and select requirements for the addition of External Routable Connectivity where these devices will generate TFEs and/or violations if TFEs are not available. (c) Issue: Zero-defect requirements with compliance (not reliability) risk. Solution: The statements for the requirements above the tables require implementing the elements of the table. Add language in the statement for the requirement above the table to incorporate the concepts of continuous improvement, such as: "The Responsible Entity shall measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations, per se." NIST 800-53 Appendix E minimum assurance requirements for security controls emphasize continuous improvement, expect "expeditious" correction ("timely" for lows) and do not expect perfection. It is also proposed in response to FERC's order on find, fix and track. In paragraph 81, FERC asked industry for proposals to revise or remove requirements to focus resources on serious risks to reliability. It also aligns with preliminary efforts to move toward more risk based auditing. (d) Issue: Complexity of Applying the Requirements. There are approximately 20 applicability variations, which makes it complicated to map the requirements to the specific classification of assets. Solution: MidAmerican Energy has created an Excel spreadsheet tool to use in analyzing the applicability variations. This spreadsheet has been provided separately to the SDT. The spreadsheet could be used as the starting point to produce a comprehensive mapping of each classification of asset, including all applicable requirements in a single document. The mapping document should be posted with draft 3 to demonstrate how an entity would actually apply the requirements. It is a final check before approval that the requirements are in sync across all standards and a valuable tool for entities to use in implementation. (e) Issue: Blackstart units and cranking paths moved to Low Impact. Solution: Provide sufficient technical and risk-based justification to support regulatory approvals of this key issue. (f) Issue: Immediate revocation of access. V5 requires that the revocation process be initiated immediately and completed within 24 hours. FERC Order 706 directed "immediate" revocation. However, BES Cyber Systems are categorized now taking risk into account. Solution: Limit to high impact Cyber Assets only. Allow reasonable response time for medium impact and protected information, for example, retain V4 timing. In addition, CIP-004-5 R7 is a candidate for the proposed continuous improvement language in the requirement section. See c) above. (g) Issue: Physical Access Controls for High Impact. Many in the industry question if two different control systems are required. Solution: Clarify in CIP-006-5 R1.3 that two authentication methods using the same control system are compliant, for example badge and PIN or bio and PIN or badge and bio. (h) Issue: Violation Risk Factors. One VRF is assigned to a requirement, regardless if it applies to both high and medium impact. Solution: Where a medium VRF is proposed, revise it to medium for high impact and lower for medium impact. Change some mediums to lower. NERC's VRF summary table needs to be flexible enough to accommodate the arrival of categorization without driving multiple requirements just to reflect different VRFs that correspond to different impact categories. (i) Issue: Definition of Annual. Annual is not in the NERC glossary. CAN-0010 establishes once per calendar year (unless the entity elects the tighter period of once within a 12-month period). V5 is more restrictive than the CAN and creates a second criterion for reaching compliance in 12 requirements. V5 creates a CIP-specific meaning of annual that is different than other standards. Solution: Use "annual" in V5 references, or use "once per calendar year or a period not to exceed 15 calendar months between occurrences." This proposal is not more restrictive than CAN-0010 and provides entities with more workload scheduling flexibility. (j) Issue: Definition of Control Center. V5 creates a CIP-specific definition of Control Center. CIP standards are not the only NERC standards using the term. Solution: Do not include a definition of control center in V5, but create a separate project for creation of a definition that would apply across all NERC standards. (k) Issue: PSP Monitoring and Alerting for entire PSP. Solution: MidAmerican Energy has provided suggested text to allow entities to monitor only access points into the PSP, if a six-wall border is established. (2) GUIDELINES: Due to the extensive amount of

materials to review in a limited timeframe, most entities focused their time reviewing the requirements, measures and VSLs. We have provided very few comments on the guidelines and technical basis sections due to time constraints. In addition, some standards had little or no guidelines in draft 2. It will take SDT resource time to get guidelines written for these standards for draft 3. We suggest considering separating the guidelines from the ballot process for standards for draft 3, to allow the drafting team to focus its efforts on making changes to the requirements, measures and VSLs to ensure approval of draft 3. The guidelines then can be finished on a separate timeline under the process in the NERC Standards Process Manual. It appears the manual provides a separate, quicker process for approving supporting documents like guidelines. (3) TABLE HEADERS: Change the column heading “Applicable BES Cyber Systems and associated Cyber Assets” to “Applicability.” The longer heading is confusing when there are no associated Cyber Assets listed in the column. (4) CAPITALIZATION WITHIN TABLE APPLICABILITY: Only words that are to be defined in the NERC glossary should be capitalized within the applicability column of the tables. For example, High Impact BES Cyber Systems should be changed to high impact BES Cyber Systems. (5) REFERENCES TO BES CYBER ASSETS/SYSTEMS: Throughout the requirements, rationales and guidelines, there are references to BES Cyber Assets and BES Cyber Systems, which are sometimes contradictory to the applicabilities. To eliminate this confusion, requirement text, rationales and guidelines should not include applicability. Rely on information in the applicability column to provide specific information on what assets are covered by the requirement. See especially CIP-004, -005, -007, -009, -010, -011. (6) MEASURES: Use the term “Examples” to introduce each of the measures. This would replace the standard language of “may include….but not limited to.” Auditors may interpret the current wording to mean that every item listed is required. In addition, verify that any measure that uses “and” instead of “or” is meant to require each of the items listed in the measures and format accordingly per the established convention for bullets vs. numbers. (7) ATTESTATIONS: There seems to be confusion within the industry regarding the use of attestations and when they are acceptable. Some of the measures in version 5 specifically list attestations. Does this preclude the use of attestations just because they are not specifically mentioned within the measures? (8) RECORDS RETENTION: Some requirements in V4 are for records retention, such as 90 days or 3 years. Draft 2 V5 appears to have a universal 3 year retention requirement in each standard under C. Compliance 1.2 Evidence Retention. Additionally, some V5 has some requirements for different retention periods. Is a requirement for evidence retention a “result” in the spirit of results based standards? Consider removing evidence retention requirements and incorporate them in the C. Compliance section with reference to their specific R and unique retention period, for example, 90 days. (9) A. INTRODUCTION 4. APPLICABILITY 4.2.3: Commenters have questioned if 4.2.3 should be removed because it may inadvertently create an exclusion for some control centers for entities that do not have BES Facilities. (10) Associated Protected Cyber Assets: These are listed in applicability throughout the requirements in all standards. Taken literally, for many requirements, it could be read to mean that while the control can be executed at a “System” level for highs, mediums, PACs and EACs, the control would have to be done on every Protected Cyber Asset. The Protected Cyber Assets should be covered as part of applying the control to their associated system. This is not clear in draft two. A possible solution is to revise applicability to, for example, “high impact BES Cyber Systems, including their associated Protected Cyber Assets.” In this way, the Protecteds are included in applying the control to the high.
Individual
Bob Thomas
Illinois Municipal Electric Agency
No
No
Yes
No
No
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
No
No
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.

Illinois Municipal Electric Agency supports comments submitted by American Public Power Association and Florida Municipal Power Agency.
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Yes
Illinois Municipal Electric Agency supports comments submitted by American Public Power Association.
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Individual
Richard Salgo
NV Energy
Yes
No
Yes
Yes
Yes
No
Yes
Control Center as it applies to the function of a Generation Operator has a threshold of generation located at two or more locations. This single qualifier could unintentionally sweep in the control centers for multi-location generation of very small capacity. We suggest that a capacity qualifier be added to this definition.
Connectivity: this definition begins with “A BES Cyber System that…” The noun in the defined term, Connectivity, cannot be defined as a “BES Cyber System”. We suggest the following re-write for the beginning of the definition: “External Routable Connectivity - The ability for a BES Cyber System to be accessible from a Cyber Asset…”
Yes
Group
Madison Gas and Electric Company
Joseph DePoorter
No
No
No
No
No
No

No
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Group
MRO NSRF
WILL SMITH
No
Yes
No
No
No
No
Yes
[A]The comments submitted by the MRO NSRF should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. [1]The NSRF comments on these definitions are predicated by our position that CIP-002-5 is fundamentally flawed, and the proposed methodology prescribed by Requirement 1 is in direct conflict with the structure of the definition for BES Cyber Asset and BES Cyber System. More specifically, the impact rating should align with the facility instead of the cyber asset. Based on this position, the NSRF proposes the following changes to the definitions of “BES Cyber Asset” and “BES Cyber System”. [Proposed Verbiage] “BES Cyber Asset” should be defined as: “A Cyber Asset that if rendered unavailable, degraded, or misused would prevent one or more BES Sites from performing its reliability function for the Bulk Electric System. Redundancy of affected BES Sites and BES Cyber Assets shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is connected to a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)”. [Proposed Verbiage] The definition of “BES Cyber System” may then by modified as: “One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks at a BES Site for a functional entity.” [Clarification] NSRF requests clarification regarding demonstrating compliance for a BES Cyber System when not every device within the system can meet the requirement applied to the system, as a whole. We recommend that the system be not be found in a state of “non-compliant” as long as one or more devices within the identified system can fully meet the documented requirement and as long as every device within the system is documented as to its capability for meeting that requirement. If this is not the intent of the SDT, this issue must be addressed along with the definitions, because it is at this fundamental level that the Standards may or may not be applicable. [2] NSRF recommends the addition of a definition for a “BES Site” to be described as: “A registered entity-owned geographic location that: (1) performs the functional obligations of the Reliability Coordinator, Balancing Authority, Generator Operator, Generator Owner, Interchange Coordinator, Reliability Coordinator, Transmission Operator, or Transmission Owner, including Control Centers, Backup Control Centers and associated data centers that support those functional obligations, and(2) contains UFLS or UVLS Systems that are part of a

Load shedding program and Load-Serving Entity functional obligation, or(3) provides the protection or restoration of the BES while performing the functional obligations of Distribution Provider, or (4) provides Blackstart Resources, (and) that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact the reliability of the BES."
NONE
[Proposed Verbiage] BES Cyber System Information: Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System, as defined within the Entity's information protection program. Examples of BES Cyber System Information may include, but are not limited to, entity-specific security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses or security configuration information without context, ESP names, or policy statements. (Rationale: Removed the indication that the information had to be developed by the entity but still allowed for the omission of publicly-available vendor information in the program's protection. Removed redundancy for "allowing unauthorized access". Added security configuration information to the list of information without context that should not need special protection.E.g. generic hardening procedures.) [Proposed Verbiage] CIP Senior Manager: One management official with overall accountability and responsibility for the implementation of the entity's NERC CIP program. (Rationale: removed "senior" to avoid implication that the official needs to be of a certain "rank" within the organization. Removed leading and added accountability phrasing to more accurately reflect the actual role within the organization.) [Proposed Verbiage] CIP Exceptional Circumstance: A situation that involves one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident that may require emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of workforce availability. (Rationale: removed "large scale" from the phrase regarding workforce availability. Workforce limitations may be localized or involve small numbers of personnel but may impact operations significantly. Added "that may" in front of 'require emergency assistance' to allow the entity to define the appropriate response on a case by case basis.)
NSRF appreciates the modifications made by the SDT to the standard and definitions related to physical security. [Proposed Verbiage] Physical Access Control Systems: Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. (Rationale: In order to remove the ambiguity around whether or not workstations used only for monitoring physical security alarms are subject to CIP requirements (e.g. guard's desk), the word "alert" has been removed. The inclusion of "control" and "log" still ensure that the equipment that requires protection is included in the definition.)
[A] The comments submitted by the MRO NSRF should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. The definition of Electronic Access Control or Monitoring Systems is still too vague. For Access Control, specifically, does this mean every cyber system that might contribute to the authentication, authorization, and accounting ("AAA") of a person crossing an EAP? If an entity uses Windows Active Directory for firewall authentication, for instance, this could be interpreted to mean every domain controller in the company is in scope. Extending that argument, the Help Desk PC that is used to grant access to the Windows Active Directory could be interpreted as being part of the AAA process, and therefore is itself an Electronic Access Control cyber asset. Likewise, a PC used at the guard desk (or third-party managed security provider) that is used to monitor alerts from the EAP could be considered a Cyber Asset used for Monitoring. Recommend the SDT provide a comprehensive list of cyber asset examples or "bright-line" set of criteria for Electronic Access Control or Monitoring Systems. [Proposed Verbiage] Electronic Access Control or Monitoring Systems: Cyber Assets that perform electronic access control or electronic access monitoring for Interactive Remote Access to the Electronic Security Perimeter(s) or Cyber Assets that perform electronic access control

or electronic access monitoring for Interactive Remote Access to BES Cyber Systems. Secondly, the NSRF would like to request that the SDT define the term “Access” used here and throughout the CIP standards, especially as it relates to cyber systems, or, specifically state that an entity can make their own definition of access such that different treatment can be given to high-risk access versus low-risk access. (“High-risk” meaning the ability to interact with, operate, modify, or cause availability issues with a BES Cyber System). Specific examples where “access”, if left undefined, could cause problems for an entity are: VMWare hypervisors, Oracle database clusters, or NAS systems that contain both BES and non-BES data/systems. Is the entity required to give CIP-004 treatment, for example, to an accounting clerk who has “access” to a receivables data table on an Oracle cluster that also hosts the backend database to a (BES) load control or EMS system? Does access to SCADA data, or a BES Energy Management System that also operates Distribution count?
[A]The comments submitted by the MRO NSRF should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. Does the definition of ESP presume the presence of an Electronic Access Point? In other words, does a BES Cyber System with no External Routable Connectivity fall within the scope of the CIP standards?Clarifying this point will pre-empt the need for interpretation or a CAN later. [Proposed Verbiage] Electronic Security Perimeter (“ESP”): A network to which BES Cyber Systems are connected using a routable protocol, surrounded by a logical border and which are only remotely accessible through an Electronic Access Point(s).
NONE
No
[1]In section 5 under “Initial Performance of Certain Periodic Requirements”, requirement CIP-010-5 R3, Part 3.2 is listed as needing to be initially performed within the first 12 calendar months. We request that this be pushed to at least 24 months to enable registered entities to perform two annual vulnerability assessments before attempting an active VA. Secondly, if industry approves the implementation requirements for planned and unplanned changes as being consistently 12 months, please collapse this section and simply state as such. The Disaster Recovery guidance is confusing, it seems to say “don’t hold up restoration for the sake of compliance, just be sure you’re in compliance at the end of restoration”, which seems to conflict. Please redraft to make it more clear what this intent of this section is. [2]The period between Version 4 and Version 5 enforceability needs to be addressed as it relates to Sites or Cyber Assets potentially requiring more protection in Version 4 than in Version 5. A transition period or a way to replace Version 4 with Version 5 protections must be allowed.
NONE
Group
Dominion
Connie Lowe
Yes
Yes
No
Yes
Yes
Yes
Yes
- The definition of BES Cyber Security Information is more clear if the last sentence is moved in front of the examples. The recommended definition is as follows, " Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by

themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures developed by the responsible entity and security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System. " - CIP Exceptional Circumstances: The definition should not be a prescriptive list and should allow each entity to define additional items as deemed appropriate. The recommended language for the definition is, " A situation that impact safety or BES reliability. Examples may include a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability."
Yes
GENERAL COMMENTS - 4.2.4 in the Applicability Section of all Standards states "Exceptions: The following are exempt from Standard CIP-002-5" as boiler plate language. The language contained in 4.2.4 needs to be updated to reference the the Standard within which the Applicability Section resides. For instance, 4.2.4 of the Applicability Section of CIP-003-5 states, "Exemptions: The following are exempt from Standard CIP-002-5" and should state, "Exemptions: The following are exempt from Standard CIP-003-5" - It should not be possible for Application Guidelines to change separately from the Standards themselves in such a way that the revised Application Guidelines would materially alter the interpretation of the requirement or add a "hidden" requirement not published in the Standard. - Where terms are defined in the glossary of terms, there is no need to duplicate the definition in the standards. An example of this is BES Cyber Asset where the definition is replicated in CIP-002. This definition should be removed from CIP-002 - The "not limited to" clause in the Measures section could be construed as "must have" evidence requirements. Where the clause exists, the starting phrase of the measure should be " Examples of acceptable evidence include..." along with a bulleted list. - CIP Exceptional Circumstances are only mentioned in CIP-004 and CIP-007. Since the timing of a CIP Exceptional Circumstance can't be predicted, CIP Exceptional Circumstances should be able to be applied to the overwhelming majority of the CIP Standards with few exceptions. Due to the lack of a "CIP Exceptional Circumstance" clause in most of the requirements, it appears as though strict compliance to the standards must be kept with little relief during these events. The ability to declare a "CIP Exceptional Circumstance" when appropriate and temporarily suspend strict compliance when it's in the best interest of the safety of personnel or the restoration or reliability of the Bulk Electric System is a critical concept that must be incorporated to guarantee the adoption of the CIP Standards. All requirements which result in the development of policies and procedures should not be subject to CIP Exceptional Circumstances, examples include CIP-002 (all), CIP-003 (all), and CIP-004 R2. Requirements that are expected to be executed during normal operations or under a defined periodic frequency should be able to be suspended where deemed appropriate upon a CIP Exceptional Circumstance, examples include CIP-004 R1.1, R3.2, R6.5, R6.6, R7.x; CIP-006 R1.2, R1.3, R1.4, R1.6, R1.8, R3.1; CIP-007 R2.3, R4.2, R4.5, R5.6; CIP-010 R3.1, and CIP-011 R1.3 - Clarify in the standards that CIP Exceptional Circumstances do not require or necessitate filing TFEs. - Should an entity determine through the use of the bright-line criteria in CIP-002 that it doesn't have any High or Medium Impact Cyber Systems, general clarity should be provided in Standards CIP-004 through CIP-011 as to whether or not additional Policies and Procedures need to be developed to address Standards which do not apply. - Where "associated" systems are identified in the Applicability column, the systems to which they are associated must be identified. An example of this is " Associated Physical Access Control Systems" which would be clarified if restated as " Associated Physical Access Control Systems for High Impact BES Cyber Systems" - The term "BES Cyber Assets", when used in the Requirements column should be replaced with the term "applicable Cyber Assets" to ensure the

applicability of the requirement in the Requirements column is in sync with the applicable Cyber Systems in the Applicability column. - The Applicability column should be consistently labeled "Applicability" across all of the tables in the standards.
Group
Southern Company Services, Inc.
Antonio Grayson
Yes
Yes
No
No
Yes
Yes
Yes
(1) Southern believes that for the purposes of the CIP standards a definition is needed and the current definition is acceptable.
(1) On page 1 of the definitions, the reference of “but are not limited to” in the second sentence of the definition of BES Cyber System Information definition should be struck. The word “example” by definition means that the list is not intended to be all inclusive. (2) On page 2, in the definition of CIP Exceptional Circumstance, the list of examples provided should not be considered to be all inclusive. In addition to the proposed change in the text, this point needs to be brought forth in the guidance. Original Text: A situation that involves one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability. "Proposed Text:" A situation that involves one or more of the following, or similar, conditions that impact safety or BES reliability: examples may include a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability".
1) The definition of Physical Access Control Systems needs to ensure electronic visitor log books are not captured under the definition, and needs to include the word “or” instead of “and” . Original Text: "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers". Proposed Text: "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, electronic visitor log books, or badge readers".
No
Regarding the implementation plan, CIP-009-5, R2.3 is not listed as a recurring periodic activity in the “Initial Performance of Certain Periodic Requirements” table and should be. A full 3 years is needed to conduct an operational exercise of each recovery plan refrerenced in CIP-009-5 R1. Additionally, in the implementation plan, all the requirements are not identified in the initial section.
Southern’s comments on the overall standards (CIP-002 to CIP-011) include: (1) Across all CIP standards, measures need to be examples, not “may include, but not limited to”. The provided measures are “examples” and should be listed as such without further qualification. We suggest beginning all measures with the phrase “Example measures may include…” Listing examples without

calling them examples and including the “may include, but not limited to” language creates unnecessary confusion and conflict during all compliance activities, and especially during compliance audits. While Southern is supportive of the drafting team’s intent, under the present language Registered Entities cannot know if the listed measures are necessary, sufficient, neither, or both. (2) Across all CIP standards, in general, the language “at least once each calendar year, not to exceed 15 calendar months” creates two problems. First, a responsible entity has to perform two checks, one for calendar year and one for 15 months. Second, in any given calendar year, a 4th quarter activity cannot roll forward a quarter, however, 1st, 2nd, and 3rd quarter activity can roll to the following quarter in the following year. Southern suggests in each standard and requirement, where applicable, replace the text, “at least once each calendar year, not to exceed 15 calendar months” with the following proposed language: “at least annually, not to exceed 15 calendar months”. Alternatively, consider the equivalent language of “at least once each calendar year or not to exceed 15 calendar months”. (3) Across all CIP standards, measures need to be bullet points, not numbered lists. Numbered lists imply that all list entries are required rather than being examples. (4) Across all CIP standards, the SDT should clarify applicability of the 4.2.4.3 exemption to include any system covered under a NRC security plan, even if on a voluntary basis. (5) Across all CIP standards, a clarification is needed in the Reliable Operation of the BES section, sentence 2 (found on Page 8 of CIP-002, but needs to be clarified in all CIP standards). Rationale: Reliability tasks in the functional model apply to functions not Functional Entities as found in section. Original Wording: "In order to identify them, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for functional entities in the NERC Functional Model". Proposed Wording: "In order to identify them, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for functions in the NERC Functional Model." (6) Across all CIP standards, the applicability of each requirement should be exclusively in the Applicability column. There are numerous requirements where different types of systems are listed in the applicability column, but the requirement statement itself says “BES Cyber Systems”
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
No
Yes
Yes
Yes
Yes
Yes
Yes
The Consideration of Comments for Transient Cyber Asset in the previous draft states “The SDT has also incorporated suggestions that the connections could be made not only to another Cyber Asset, but also to the network within the ESP.” However, “network” was omitted from the parenthetical exclusion for temporary assets in the definition of “BES Cyber Asset” in this draft. Please clarify whether the exclusion in the parentheses applies to a Cyber Asset that is connected to a network (for example, connected to a non-programmable device such as a layer 1 Ethernet hub.) We suggest changing “it is directly connected to a Cyber Asset within an ESP, or to a BES Cyber Asset” to “it is directly connected to a Cyber Asset within an ESP, or to a BES Cyber Asset, OR TO A NETWORK within the ESP”.
MMWEC agrees with and supports the comments submitted by APPA.
Yes

MMWEC agrees with and supports the comments submitted by APPA.
MMWEC agrees with and supports the comments submitted by APPA.
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
No
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
Please give consideration to the following suggestion: BES Cyber Asset – Replace the text at the end of the first paragraph, “. . . would affect the reliable operation of the Bulk Electric System”, to use a more clearly defined NERC Glossary term, “. . . would have an Adverse Reliability impact on the Bulk Electric System.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
Group
NESCOR/NESCO
Annabelle Lee
No
The implementation plan calls for CIPv5 to come into effect July 1, 2015 (which has been moved out 6 months from the version one draft). Given that CIPv5 has already been in the works for more than two years, it is not clear why the effective date is three years in the future.
For all places where a requirement states "at least once every calendar year thereafter, not to exceed 15 months…”, this means that if the activity is performed every 15 months, then it would have only been performed 4 times in 5 calendar years. This contradicts the "at least once every calendar year…" Similarly for “every 39 months…”. To ensure that aircraft receive annual inspections once a year, Federal Aviation Regulation (FAR) 91.409(a) requires that" no person may operate an aircraft unless, within the preceding 12 calendar months, it has had (1) an annual inspection in accordance with part 43" etc. This wording precludes attempts to extendthe word "annual" to mean longer than one year, and we suggest that similar wording could be used in the CIPs. For example, "an entity is out of compliance with requirement Rxxx unless, within the preceding 12 calendar months, it has performed X Y Z". As stated in the document, "...from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities." Redundancy is not an appropriate mitigation for all vulnerabilities, but it is a mitigation for some. NERC may want to consider revising the sentence and being more specific when redundancy is not appropriate. As stated in the Table of Compliance elements, "100 High and Medium Impact BES Cyber Assets/Systems." Why are cyber assets listed in

some VSLs and cyber systems listed in others? As stated, "The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” The term element is not defined nor related to cyber assets/systems. NERC may want to consider adding a definition for element. NERC may want to consider adding iteration/feedback loops to the use case CIP process flow diagram. There is no clear requirement that non-routable communications between two ESPs, such as between a substation and control center, be encrypted or have their integrity assured. Technical solutions exist to secure serial SCADA communications, both in the form of proprietary vendor products, as well as standards such as IEEE 1711 (developed from AGA12) and Secure DNP3. We suggest that all non-routable persistent communications links between ESPs be protected with strong encryption and integrity. Furthermore, the endpoint devices providing the encryption and authentication should be considered part of the ESPs and subject to all other CIP requirements for cyber assets belonging to an ESP. The lack of commercially available perimeter security solutions for non-routable protocols, pointed out in the Application Guidelines for CIP-005-5, further emphasizes the need for cryptographic protection of serial links. NERC's Consideration of Comments does not address this comment. This comment directly addresses point 86 in FERC 18 CFR Part 40 approving CIP v4, which states "…we support the elimination of the blanket exemption for non-routable connected cyber systems…" Cyber assets associated with data networks and data communications links between discrete ESPs, rather than being exempt from CIP requirements, could be specifically included, and exempt only when all communications between those ESPs are encrypted and have their integrity assured. IPSec VPNs have been a mature technology for many years, as are SSL VPNs. Given that these technologies are widely used in other industries, and that devices implementing them are available in industrial- and substation-grade form factors, we recommend that all routable communications, not just remote access connections, be protected with strong encryption and integrity (message authentication), using encryption technologies such as site-to-site secure VPNs. Secure VPNs should not be confused with technologies such as MPLS and GRE that can segregate traffic, but do not encrypt, and are therefore only secure if every intermediate device in the traffic path is secure. Furthermore, the endpoint devices providing the encryption and authentication should be considered part of the ESPs and subject to all other CIP requirements for cyber assets belonging to an ESP. If communications assets are exempt from the CIPs as the draft currently states and communications are not encrypted and integrity verified, then every radio, modem, hub, communications device, wire, and fiber can provide an attacker with access to and the ability to falsify critical control system communications. This particularly applies to most private WANs leased from communications service providers: if communications over private WANs are not encrypted, then compromise of the service provider via mis-configuration, vulnerabilities in equipment, or insider collusion by employees of the service provider, could lead to compromise of multiple utility communications networks. This particularly applies to communications across the public Internet. Fully addressing security of communications links may require more than just removal of the A 4.2.4.2 exception. This topic seems sufficiently important to merit its own CIP section covering appropriate requirements for end-to-end protection of communications (encryption, integrity verification, key management, etc.). It is not clear that Security Event Monitoring as called out in CIP 007 is required of all EAPs. NERC could consider security event monitoring be required of all EAPs, regardless of impact level. CIP 011 does not address how third parties (consultants, contractors, vendors, etc.) should handle BES Cyber System information. Where 3rd parties have persistent or ephemeral remote access to Cyber Assets, they have implicit access to BES Cyber Asset information. NERC could consider applying all information requirements of CIP 011 to any 3rd parties with such access.
Individual
Brian S. Millard
Tennessee Valley Authority
Yes
Yes
Yes
Yes
Yes

Yes
Definition is too broad and subjective.
External Routable Connectivity - Insert “OSI layer level” in front of accessible in definitions.
Yes
Individual
Kirit Shah
Ameren
No
Yes
No
No
No
Yes
Yes
(1) BES Cyber Assets - The phrase "affect the reliable operation of the BES" used in the definition of a BES Cyber Asset needs to be defined, because one can argue that everything "affects" the reliable operation of the BES. Note that the word "adverse impact" is used with impact of the cyber asset on the Facility, while in CIP-002, page 8, it is used with impact on reliable operation of the BES. Please provide a definition and consistency between definition and CIP-002-5 documents.
Cyber System Information – This definition is poorly worded and seems convoluted. Please revise it so entities understand the intent of the SDT. One suggestion is to strike "but are not limited to" and "but not limited to" in the definition.
(1) Physical Access Control Systems – Please put a comma after second ‘Physical Security Perimeter’ so the ‘such as’ is referencing Cyber Assets, not ‘locally mounted hardware or devices’.
(1) Intermediate Device – The definition of an Intermediate Device should be changed to "A Cyber Asset or Collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate Device must be terminated on an Electric Access Point or be external to the Electronic Security Perimeter".
Yes
(1) Initial Performance of Certain Periodic Requirements – CIP-010 R3.2 should be given 36 calendar months instead of 12 calendar months to match the requirement timeframe. (2) Proposed Effective Date for Version - Delete the final sentence on Page 2, Part 1, starting with “Notwithstanding any order to the contrary…” and footnote #1 that goes with it since CIP version 4 has now been approved.
(1) There needs to be definition of "Dial-up Connectivity" added to the definitions. We suggest the following wording "Connectivity to a BES Cyber Asset (or associated Protected Cyber Assets) which uses a Public Switched Telephone Network (PSTN) that requires a number to be dialed".
Group
Salt River Project

Sara McCoy
Yes
Yes
Yes
Yes
No
SRP suggests clarification on the SDT's definition of Intermediate Device. Is it referring to a proxy type of device or some type of authentication device prior to accessing a BES Cyber System or Protected Cyber Asset?
Yes
Yes
Group
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)
David Dockery
No
Yes
No
Yes
Yes
Yes
No
[BES Cyber Asset, Definitions, p 1 REPLACE: “, and is used for” WITH: “, and is only used for” RATIONALE: AECI agrees with other commenters on the need for this clarification.]
[BES Cyber System Information, Definitions, pp 1 & 2 REPLACE: “the BES Cyber System” WITH: “a BES Cyber System” (all instances) RATIONALE: An Entity could have more than one BES Cyber System, or Information related to another Entity’s BES Cyber System.]
[Cyber Security Incident, Bullet #1, Defintions, p 1 REPLACE: “the Electronic Security” WITH: “a BES Cyber System’s Electronic Security” RATIONALE: Exclude all incidents of Physical Security Perimeter or Electronic Security Perimeter tampering, where no BES Cyber Systems are being protected, from being necessarily included as evidence and with necessary proof of evaluation that they were in fact not BES Cyber System related incidents.]
No
[Page 2, Part 1, final sentence beginning with, “Notwithstanding any order to the contrary…” REMOVE: the entire sentence along with accompanying footnote #1, or reword effectively. RATIONALE: The FERC Order accepting CIPv4 specifically states that it will supersede CIPv3, so this

sentence and footnote is now misleading at best. ALTERNATIVE: Restate this sentence such that it does, if approved by FERC, do what is suggested.]
[Page 2, Part 1, final sentence beginning with, “Notwithstanding any order to the contrary…” REMOVE: the entire sentence along with accompanying footnote #1, or reword effectively. RATIONALE: The FERC Order accepting CIPv4 specifically states that it will supersede CIPv3, so this sentence and footnote is now misleading at best. ALTERNATIVE: Restate this sentence such that it does, if approved by FERC, do what is suggested.] (Sorry, did not anticipate the comment-box on Question 15 above, so this is duplicated)
Group
FirstEnergy
Doug Hohlbaugh
No
Yes
Yes
Yes
Yes
No
Yes
(1) BES Cyber Asset – This definition states a “A Cyber Asset that if rendered unavailable, degraded, or misused ...” and FE suggests that the word “misused” be dropped from the definition to bring consistency with the latter part of the definition. Additionally, the preceding terms “rendered unavailable” and “degraded” better illustrate the intended risk or compromise to a BES cyber asset that warrants consideration to BES reliability risk. (2) BES Cyber System – FE proposes the following definition for BES Cyber System – “One or more BES Cyber Assets logically grouped by a responsible entity and interconnected via a routable protocol to perform one or more reliability tasks for a functional entity.” Similar to the proposed change for External Routable Connectivity, the BES Cyber System definition should be based on the routable connectivity of BES Cyber Assets. Non-routable devices (such as serially-connected RTUs) should fall outside of the BES Cyber System -- since they do not communicate via a routable protocol.
(1) External Routable Connectivity – We propose the definition focus on the cyber asset being routable and be re-written to state “A BES Cyber Asset that communicates with a Cyber Asset that is outside its associated Electronic Security Perimeter via a bi-directional routable protocol connection.” The reason for this change is that by defining external routable connectivity with respect to the BES Cyber Asset, rather than the BES Cyber System -- we take non-routable devices out of scope, as they are today. As written, we believe that all generation and transmission RTUs, relays, and any other devices that are part of the EMS or GMS BES Cyber Systems could potentially be brought in-scope. This would significantly increase the scope of covered assets, without a commensurate increase in security or reliability to the BES. There is other language in the Version 5 standard that needs to change to reflect this modification. For example, all of the "applicability" tables are based on the high/medium/low BES Cyber Systems "with External Routable Connectivity or dial-up connectivity." The applicability of the CIP Standards should be based on the qualifying connectivity of the BES Cyber Asset -- not the qualifying connectivity of the BES Cyber System (since the latter would bring assets into scope -- like serially-connected RTUs -- that do not have such qualifying connectivity). (2) Electronic Security Perimeter (ESP) – Similarly we suggest that the ESP definition be revised to focus on cyber assets and read “The logical border surrounding a network to which BES Cyber Assets are connected using a routable protocol.”

FE supports the Implementation Plan as stated in draft 2. However, we ask that the drafting team clarify their reasons for extending the low impact implementation plan by an additional 12 months beyond the high/medium impact requirements. Our understanding is that the additional time allotted is to allow industry to focus explicitly on meeting the requirements of the high/medium assets since they pose the greater risk to the BES. We concur with this approach, however, we are concerned that the very reason of this phased in implementation plan – permitting focus on high/medium BES Cyber Systems - once initial implementation periods are over will be lost during industry's on-going effort to ensure reliable cyber asset security. It should be recognized that expanding the scope to include low impact assets may in fact reduce security, since it diverts the focus of technical and compliance resources off of the areas that most require it. Due to the large administrative overhead involved and the compliance risk that it creates, low impact cyber assets and cyber systems should be out-of-scope entirely. On the other hand, draft 2 of CIP V5 appears to have greatly reduced the obligations for low impact cyber, to the point that the only requirement is a “policy document” in CIP-003-5 R3 with no requirement for an inventory, list, or discrete identification of low impact BES Cyber Systems and no other low impact requirements found within the CIP V5 standards. Based on the additional one-year allotted in the implementation plan, it is unclear what may be within scope of an audit of low impact cyber beyond the policy document in CIP-003 R3. We ask the team to clarify their reasons for the one-year extension and further explain the intended measures for ensuring CIP-003 R3 is met. Please see FE Comment Form A, Question #10 for changes we believe are needed for the measure of CIP-003 R3.
FE appreciates the efforts of the CIP draft team and it’s recognized that many of our prior comments are now reflected in the draft 2 set of CIP V5. We appreciate the team accepting our and others proposal to eliminate the use of BES Reliability Operating Services and to retain some of the existing terminology such as Physical Security Perimeter. As reflected in our comments we remain concerned that the standards need to remain focused on routable connectivity risk exposure and we offer some definitional changes in this regard. However, at a minimum we believe it is critically important to limit many of the requirement applicability associated with Medium BES Cyber Systems to Medium BES Cyber with External Routable Connectivity. Our submitted comments provide specific feedback in this regard.
Group
Duke Energy
Greg Rowland
No
No
No
No
No
No
No
(1) BES Cyber Asset. The definition of BES Cyber Asset is convoluted and confusing. The order of the phrase in the first sentence, “its required operation, mis-operation, or non-operation” needs to be changed at a minimum – the “required” seems to apply to mis-operation as well as operation. The first sentence overall is too long and confusing. And the sentence on redundancy is inconsistent with the first sentence; the first sentence uses the phrase “adversely impact” with respect to the Cyber Asset and the phrase “affect the reliable operation of the BES” with respect to Facilities, Systems or equipment, but the second sentence uses the phrase “adverse impact” with respect to Facilities, Systems and equipment. Duke recommends the following replacement definition, “A Cyber Asset that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the need, activation or exercise of the compromised Facility, System, or equipment.”. (2) BES Cyber System. Duke suggests that the definition be reworded to “One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks identified for functions in the NERC Functional Model.” This clarifies how the NERC Functional Model should be used in the assessment.
(1) The definition of Control Center uses language inconsistent with the NERC Functional Model. Duke

suggests the following rewording, “One or more facilities hosting functional entities that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks of functions in the NERC Functional Model of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.”
(1) BES Cyber System Information. Duke does not agree with examples being included in a definition. Examples should be reserved for guidance only and the definition should be limited to only prescriptive measures. Duke recommends rewording this definition to “Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System.”. (2) CIP Exceptional Circumstance. Duke, however, sees the list of events provided in this definition as prescriptive and necessary. However, Duke recommends that the beginning be reworded to, “A situation that includes, but is not limited to, one or more of the following conditions that impact safety…”. Duke believes that this wording change adds flexibility to the entity to expand the definition to other events not listed, but at a minimum to consider those listed.
(1) Physical Access Control Systems. Duke does not agree with examples being included in a definition. Examples should be reserved for guidance only and the definition should be limited to only prescriptive measures. The exclusion of “devices at the Physical Security Perimeter” is also confusing. Could this inappropriately be interpreted to mean micros used for physical access control?
(1) Interactive Remote Access. Duke recommends that the following sentence, “Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants.” be removed. This section attempts to cover all methods of remote access, and appears to cover all types, but in the case that it doesn’t, the definition shouldn’t be limiting to just these scenarios. It is Duke’s opinion that the presentation of these scenarios is unnecessary. (2) Intermediate Device. Duke is concerned with the phrase “performing access control” existing as part of the definition of an Intermediate Device. Is it the drafting team’s intent that an Intermediate Device is also meeting the definition of an Electronic Access Control or Monitoring System? If so, Duke thinks that should be clarified in the definition of an Intermediate Device by saying that it is a specific class of EACMS devices. If it wasn’t the intent, distinction should be drawn between the two definitions.
(1) External Routable Connectivity. Duke would like to request that the drafting team consider using technical terms, such as the inclusion of network layers, to clarify what is meant by “accessible…via a bi-directional routable protocol”. Using network layers to quantify exactly the types of connections that are considered “externally routable” will aid in the entity’s assessment of this criteria. (2) Protected Cyber Asset. Duke would suggest removing the parentheses from the definition. Duke does not understand their purpose here.
(1) Reportable Cyber Security Incident. Duke suggests the following rewording of the definition to, “Any Cyber Security Incident that has compromised or disrupted one or more reliability tasks identified for functions in the NERC Functional Model.” This clarifies the appropriate references back to the NERC Functional Model.
No
(1) Proposed Effective Date for Version 5 CIP Cyber Security Standards. The first sentence states that “Responsible entities shall comply with all requirements…”. This is in direct conflict with the next section titled “Initial Performance of Certain Periodic Requirements” which allows for some of the requirements to be initially compliant with after the initial effective date. Duke recommends replacing the word “all” with “the requirements in CIP-002, CIP-003…except for those listed below in the Initial Performance of Certain Periodic Requirements section”. (2) Proposed Effective Date for Version 5 CIP Cyber Security Standards. In the first listed item there is a reference to the fact that, “Notwithstanding any order to the contrary…”. Duke suggests that this language be removed. Duke sees this as unnecessary as FERC is able to approve/reject any or all of the Implementation Plan regardless of the language that is put in. Duke sees this type of language as unnecessary. (3) Unplanned Changes Resulting in a Higher Categorization. Duke has a concern that in the attempt by the drafting team to clarify the difference between a planned change and an unplanned change, a lot of unfair assumptions are made. For example, unplanned changes don’t account for a vertically-integrated utility. Does an entity have to talk to another entity that shares the same ownership for evaluation of a “planned” change? The examples provided cannot possibly address all scenarios and it

leaves the entities in a state of uncertainty as to which change the fall into. Duke suggests a simplification of addressing the addition of new Cyber Systems, reclassified Cyber Systems, etc. Duke requests that all scenarios of new or reclassified Cyber Assets that are intended to fall into the Implementation Plan have a single time window to meet compliance. Duke suggests that a 12-month implementation plan be used after the effective date of the change has been made. Duke also suggests that this section of the Implementation Plan cover the addition of EACMs, PACs, Protected Cyber Assets, and Low Impact BES Cyber Systems. Finally, Duke suggests that the 12-month implementation window be used for some of the requirements, but those identified in the “Initial Performance of Certain Periodic Requirements” be used for this section as well.
Group
Family Of Companies (FOC) including OPC, GTC & GSOC
Guy Andrews
Yes
Yes
Yes
Yes
No
see comments question 12
Yes
No
(BES Cyber Asset) Recommend modifying the parenthetical phrase. It is currently difficult to understand. We recommend the following modification: "A Cyber Asset is not a BES Cyber Asset if it is directly connected to a Cyber Asset within an ESP, including BES Cyber Assets, for 30 consecutive calendar days or less, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
none
none
none
We recommend adding the words “owned by or under the control of the Responsible Entity” to prevent the inclusion of equipment owned by Managed Security Providers in the standards. (Intermediate Device) The Devices involved in access control have been interpreted to include an entity's AAA servers; applying this interpretation to the proposed definition of Intermediate Device contains a requirement, which is not appropriate: “The Intermediate Device must not be located inside the Electronic Security Perimeter.”would prohibit an entity from protecting its AAA server(s) within an ESP. Consider rewriting the definition as follows: "A Cyber Asset or collection of Cyber Assets located on, or outside of the Electronic Security Perimeter that performs access control to restrict Interactive Remote Access to only authorized users". To qualify as an Intermediate Device, the asset(s) that actually restrict access must be located outside or on the ESP; devices that do not directly restrict access, but perform related functions such as authentication, authorization and logging may reside within the ESP." (Electronic Access Control and Monitoring Systems) We recommend adding the words “owned by or under the control of the Responsible Entity” to prevent the inclusion of equipment owned by Managed Security Providers in the standards.
(Protected Cyber Asset) See comment regarding BES Cyber Asset.
We believe “was an attempt” should be changed to “had the potential”. To know whether something was an attempt an entity would have to determine the intent of the perpetrator, who is many times never identified. Also, why would we want to exclude accidents which had the potential to disrupt operations from the scope of the standards?
Yes
none
none
Group

Texas RE NERC Standards Review Subcommittee
Brenda Hampton
No
No
No
No
No
See NSRS comments on Question 12.
Yes
No
(1) A Cyber Asset is not necessarily programmable. Modify the definition of Cyber Asset to read: “A Cyber Asset may be a programmable device (e.g., EPROM, microprocessor, etc.) that uses any combination of hardware, firmware, software, and/or data to execute internally stored programs and algorithms, including numerous arithmetic or logic operations, without operator action. Solid state devices (e.g., electro-mechanical on/off devices, relays, hard-wired logic devices, circuit boards, etc.) that do not have firmware and/or software are not considered Cyber Assets.” (2) In the definition of BES Cyber Asset, the discussion of redundancy is confusing, at best. We suggest replacing “Redundancy of affected Facilities, Systems, and equipment shall not be considered when determining adverse impact.” with “The use of redundant Facilities, Systems, or equipment to improve reliability and availability cannot form the basis to exclude assets from being considered as BES Cyber Assets.”
Modify the definition of Control Center to read: “One or more facilities hosting BES Cyber Assets/Systems including operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability functional tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generation Operator for generation Facilities at two or more locations.”
(1) In the second sentence of BES Cyber System Information, please strike the qualifier “…developed by the responsible entity” or, modify it to say “…security procedures followed by the responsible entity and whose disclosure could be used to gain unauthorized access”. The justification being that smaller entities may have their entire program developed, implemented, and/or managed by third-parties. (2) Modify the definition of CIP Senior Manager to read: “A single senior management official with overall accountability and responsibility for the implementation of the entity’s NERC CIP program” so as not to imply that it is a required that this person “lead” the implementation. (3) Modify the definition of CIP Exceptional Circumstances to read: “A situation that involves one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.”
Modify the definition of Physical Access Control System to read: “Cyber Assets that control, detect, alarm, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Revise definition of Interactive Remote Access to read: “All user-initiated access by a person employing a remote access client or other remote access technology using a routable protocol or dial-up. Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.” Also consider adding a paragraph in the guidance section on what qualifies as a remote access client/remote access technology.
(1) Consider providing examples in the definition for Electronic Access Point. (2) Consider providing examples in the definition for Electronic Security Perimeter. (3) In the definition of a Protected Cyber Asset, suggest removing the parenthesis but keep the wording as a separate sentence.
(1) The words “malicious” and “suspicious” are subject to interpretation. Based on this, modify the definition of Cyber Security Incident to read: “A malicious act or suspicious event, as determined by

the registered entity, that: (1) Compromises, or was a plausible attempt to compromise a BES Cyber System, and/or (2) Disrupts, or was a plausible attempt to disrupt, the operation of a BES Cyber System." (2) Currently the definition for Reportable Cyber Security Incident includes a reference to a reliability task. This is not a defined term and can be interpreted in many ways. We suggest modifying the definition to read "Any Cyber Security Incident that has compromised or disrupted one or more reliability functions."
Yes
In section 5 under "Initial Performance of Certain Periodic Requirements", requirement CIP-010-5 R3, Part 3.2 is listed as needing to be initially performed within the first 12 calendar months. We request that this be pushed to at least 24 months to enable registered entities to perform two annual vulnerability assessments before attempting an active vulnerability assessment.
See Question 15 for comments on the Implementation Plan.
Members of the Texas RE NERC Standards Review Subcommittee want to express our appreciation for the hard work of the Project 2008-06 CIP V5 Standard Drafting Team in responding to prior industry comments. We agree with many of the changes made since the previous version posting and are pleased with the progress that the team has made thus far.
Individual
Brian J Murphy
NextEra Energy, Inc.
No
No
No
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
Group
National Rural Electric Cooperative Association (NRECA)
Barry Lawson
No
No
Control Center – NRECA is concerned that in this definition the mere presence of a SCADA HMI might be considered a Control Center by a CEA if it could possibly be used to control BES assets in real-time even if an entity does not use it that way. Some of the registered entities do not staff these control centers 24/7 and are unable to perform real time control after hours, or any other time that other duties take them 15 minutes away from the computer. In some instances these entities might be registered as TOPs only because they own a limited and discrete 115 kV facility that no other entity

was willing to register as a TOP for. Often times this 115 kV facility performs no reliability function. NRECA suggests adding “24/7" to the first sentence of the Control Center definition as shown in the following text: “One or more facilities hosting operating personnel 24/7 that monitor and control the Bulk Electric System (BES) in real-time …”
CIP Senior Manager – In this definition replace “CIP Standards” with "CIP-002 through CIP-011." If this is not completed, this definition would apply to CIP-001 which still exists and is an unrelated standard. NRECA believes this revision will provide clarity to the limit of the definition.
Group
Florida Municipal Power Agency
Frank Gaffney
No
No
Yes
No
No
No
No
The definition of BES Cyber Asset uses the term “Systems” which is defined in the NERC Glossary as including distribution, i.e., “A combination of generation, transmission, and distribution components”. Distribution is specifically excluded from the standards through the Federal Power Act, Section 215, at (a)(1) and (i)(1). FMPA suggests eliminating the term altogether since the more general “equipment” already covers everything not covered by the term “Facilities”.
The definition of Control Center is ambiguous with its use of the phrase “perform the reliability functional tasks of”. If a Distribution Provider has a communication link from its SCADA system to a TOPs Control Center that sends the TOP data concerning load at more than one location, is that performing a monitoring function of a TOP? We do not believe that is the intent of the SDT, but, the phrase could be interpreted in that way. We suggest changing the phrase to specify that a Control Center is that BES Cyber System for which the System Operator has a Human Machine Interface.
The definition of Physical Security Perimeter is ambiguous as to whether it is two dimensional or three dimensional, and how such a perimeter might be different for High and Medium Impact systems. In other words, clarity as to the vertical dimension is needed, what size access “hole” needs to be controlled and is considered a physical access point (the 96 square inches in the guide is not enforceable, only requirements are enforceable), etc. Without such clarity, FMPA cannot vote Affirmative because entities will not know what is required and will likely have more surprises like CAN-0031 (which we believe is unenforceable).
The definition of Intermediate Device includes a requirement within it which should instead be included within the requirements of the standards, i.e.: “The Intermediate Device must not be located inside the Electronic Security Perimeter” should be deleted. The definition of Interactive Remote Access includes a sentence that adds no value, and does not address all circumstances: “Remote access may be initiated from …” should be deleted. It is possible to initiate remote access from assets owned by others not listed.
The definition of Protected Cyber Assets, which now excludes “transient devices”, which are considered cyber assets connected inside an ESP or attached to a Critical Asset for 30 days or less, we believe is too lenient on transient assets which can be used to “spread” Stuxnet type malware.

While we agree with treating transient devices differently than Protected Cyber Assets, we also believe there should be a requirement of a scan for malware on the transient device before it is connected to anything inside the boundary of the ESP for Medium and High Impact. FMPA believes that Transient Devices should be separately defined with an associated requirement within the standards.
The definition of a Cyber Security Incident includes an element that is not measurable as that term is used in the standards. It is essentially impossible to measure “an attempt to compromise” or “an attempt to disrupt”. This un-measurable definition will cause CIP-008-5 to be un-measurable. We suggest changing these terms to be measurable, e.g., attempts with known malicious intent such as discovered by malware protection.
Yes
COMMENTS ON APPICABILITY Under Applicability section 4.2.2, the phrase: “Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:” is ambiguous as to whether the following bullets is an exhaustive list (i.e.) or an “including but not limited to” list (e.g.). FMPA suggests clarifying that it is an exhaustive list by inserting “i.e.” at the end of the phrase. Under Applicability section 4.2.2, 3rd bullet, “A Protection System that applies to Transmission” is ambiguous. Instead, the term should be changed to “transmission Protection System” as used in PRC-004-2 and PRC-005-1 and for which there is a FERC approved interpretation (Project 2009 17). Under bullet 4.2.2, the term “required” is inappropriate for the 2nd and 3rd bullets, i.e., “… required by a NERC or Regional Reliability Standard”. Use of the word “required” implies an obligation to have evidence of why it is required. A more appropriate reference is “applicable”, e.g., “… applicable to a non-CIP NERC or Regional Reliability Standard” (the non-CIP is needed to prevent circular logic). Under bullet 4.2.2, the bullet on Cranking Paths needs to specify whose plan, i.e., “… in accordance with the applicable TOPs Restoration Plan.” COMMENTS ON COMPLIANCE ELEMENTS Measures are not enforceable and must not use the word “must”. On evidence retention, rather than restating the language of CMEP section 3.1.4.2, the evidence retention section of the standard should simply refer to that section of the CMEP so that if the ROP / CMEP is changed, the standards would not also need to be changed. As stated here, if the ROP/CMEP were to be changed, all the standards that repeat this language would also need to be changed with such change needing the approval of FERC, creating a lot of wasted effort and energy. FMPA understands that this section of the CMEP is currently being reviewed and evaluated for change. COMMENTS THAT APPLY TO SEVERAL DIFFERENT STANDARDS / REQUIREMENTS At least once a calendar year is sufficient, there is no reliability need for the “but not to exceed 15 calendar months” in any of the requirements that include that phrase. In reference to tables within the Requirements of nearly all of the standards, it is ambiguous as to whether the bullets are an exhaustive list (i.e.) or an “including but not limited to” list (e.g.). It is imperative that it be made clear that the list is an exhaustive list; otherwise the parent requirement can be interpreted as applying to all BES Cyber Systems, including Low Impact, when that is not the intent for many of the requirements. Change Management: there are several places in the standards where both: 1) an annual review is required, and 2) a requirement to change within 30 days of lessons learned or a change to systems/personnel. Both change management methods are not needed and the SDT ought to choose one method or the other to reduce administrative burden. This duplication of effort is made even worse with a third method of change management embedded within CIP-010-5, R3. TFEs: TFEs are an administrative nightmare with a very high administrative cost for little to no benefit to reliability. We recognize that the phrase “where technically feasible” is important because in some cases, it is not technically feasible. However, to reduce the administrative nightmare, it would be helpful to specify what would be required, if anything, if it were not technically feasible, so that a minimal amount of TFEs would need to be tracked. Such requirements would look like an “if” statement, e.g., if technical feasible to this, if not do that. In such a way, many TFEs could be eliminated.
Individual
Yuling Holden
PSEG
Yes
No

Yes
Yes
Yes
Yes
Yes
The definition of Control Center includes the undefined phrase “control of the Bulk Electric System (BES) in real-time to perform reliability functional tasks…” PSEG believes “control” must be clarified to ensure economic and market decision are not inadvertently captured by this definition. CIP-00-.5 (draft) page 23 of 33 includes a description of Monitoring and Control. The Control Center definition should capture the aspects of “control” in a manner consistent with what is included under Monitoring and Control (i.e. all methods of operating breakers and switches, SCADA, and substation automation). For CIP Exceptional Circumstance, even though the definition states “the following, or similar conditions,” we suggest changing “a natural disaster” to “a natural or human–caused disaster.”
Yes
Individual
Don Jones
Texas Reliability Entity
Yes
No
Yes
Yes
Yes
Yes
Yes
Individual
Daniel Duff
Liberty Electric Power LLC
No

No
No
Yes
Yes
Yes
Yes
Did not vote negative due to the definitions, but the definition of Cyber Asset suggests the reason the assets were grouped was for reliability. Would be better if the term was defined as a group of cyber assets used to enable functional interaction with or control of elements of the Bulk Electric System.
BES Cyber System Information needs to be clarified to exclude such items as the specific test formatting for relays and associated test results.
Yes
Group
Luminant
Rick Terrill
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
Individual
Stephanie Monzon
PJM Interconnection
Yes
No

Yes
Yes
Yes
Yes
Yes
Facility is unclear, definition would help with interpretation.
Yes
Individual
Kathleen Goodman
ISO New England Inc.
No
Yes
Yes
Yes
Yes
No
No
For clarity, suggest changing the BES Cyber Asset definition from "it is directly connected to a Cyber Asset within an ESP" to "it is directly connected to a network, or to a Cyber Asset within an ESP".
Request clarification on the definition of EAP. Must it be routable protocol on both sides?
The definition of Reportable Cyber Security uses the terms "compromised" and "disrupted" plus the phrase "reliability tasks of a functional entity". All three need their own definition/clarification.
No
Although the proposed Version 5 Implementation Plan states that “Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan,” there are concerns that need clarification. The concerns refer to the transition from the currently effective Version 3, through Version 4 and finally to Version 5. Given that (a) the Version 4 Standards and associated Implementation Plan were recently approved by FERC; (b) the proposed Version 5 Implementation Plan contains a minimum 24-month period for enforcement means that there will be a period of time during which Version 4 would be effective; and (c) when Version 4 becomes effective there will be newly identified CAs that will have to be made compliant. In order to comply with Version 4 requirements, entities will be need to allocate funding and resources to perform work necessary to become compliant at newly identified

facilities. Much of this work must be performed in anticipation of the enforcement date. Once Version 5 becomes effective, application of the proposed categorization of BES Cyber Systems may very well result in much of the work done for Version 4 compliance being in the end unnecessary. Request clarification on the Disaster Recovery's "completion of the restoration activities" (top of the clean version's page 5). What event/action/etc. signifies this completion?
Section 5 for CIP-003-5 is the only place that explains how to read the bullets and numbers in the Measures. From the second paragraph of Section 5, "Measures provide examples of evidence to show documentation and implementation of the requirement. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence." Request clarification this bullets and numbers explanations applies to the Requirements and Applicability sections of each of CIP-002-5 - CIP-011-1. If this was the SDT's intent, then recommend this clarification be added to Section 5 of each of CIP-002-5 - CIP-011-1. General comment--recommend that each Requirement’s Part identify that Part’s goal.
Group
Edison Electric Institute
David Batz
EEI REAC KEY ISSUES ISSUE 1: Low Impact BES Cyber Assets in scope (1.) FERC's version 4 Order 761 expects all BES Cyber assets should be in scope in V5. (2.) Audit issue of providing evidence of policy implementation on Low impact cyber assets. STRATEGY: Focus on 'BES site' level definition for Lows with security policy applied to sites, not individual cyber assets. ISSUE 2: Inclusion of Cyber Assets regardless of connectivity (1.) Blanket connectivity exclusion removed in CIP-002. Connectivity addressed in applicability column of requirements in CIP-003 to CIP-011. (2.) Example substation: Non-externally routable cyber assets increase cyber asset count 40% and some medium requirements are not good fits. STRATEGY: More liberal use of 'External Routable Connectivity' qualifier in the applicability column for more requirements throughout standards. ISSUE 3: Zero-defect requirements with compliance (not reliability) risk (1.) 8 of top 10 most violated standards in 2011. (2.) 91% of FFTs approved by FERC in March order which invited proposals to revise or remove requirements. (3.) NIST 800-53 App. E Minimum Assurance Requirements recognize flaws will be discovered and focus on continuous improvement. (4.) Other federal regulators do not enforce zero-defect perfection forever. STRATEGY: Overall NERC Standards issue and a philosophical change to requirements. Likely not to be fixed between drafts 2 and 3. Add language to the Requirement statement above the table for selected requirements. Language to incorporate the concepts of measuring performance to detect flaws, correcting flaws, taking action that may prevent recurrence (if applicable for the flaw) and flaws that have been detected and corrected are not violations. Reflect same concepts in the VSLs. ISSUE 4: Complexity of Applying the Requirements (1.) There are approximately 20 applicability references, so it's complicated to map the requirements to the classification of assets. (2.) However, this is the result of breaking up 'one size fits all' type requirements STRATEGY: The drafting team needs to produce a comprehensive mapping of each of classification of asset including all applicable requirements in a single document for and post it with Draft 3 to demonstrate how an entity would actually apply the requirements. Focus on sites for CIP-002 and Low and add requirements for medium and high per attachment 1. ISSUE 5: Blackstart units and cranking paths moved to Low Impact (1.) Concern that it is a lessening of V1-V4, FERC may remand STRATEGY: File as-is with technical and risk-based justification for not 'lessening' the standard. ISSUE 6: Immediate Revocation of access (1.) V5 requires that the revocation process be initiated immediately and completed within 24 hours. (2.) Though FERC Order 706 mandated 'immediate' revocation, many entities consider it

unattainable. STRATEGY: Limit to High Impact cyber assets only. Allow reasonable response time for Medium Impact and protected information. An example of unacceptable 'zero defect' risk, and a candidate for above strategy to add language in Requirement statement. ISSUE 7: Physical Access Controls for High Impact (1.) FERC Order 706 directed defense in depth ('two or more'). (2.) V5 limits this to control centers only. (3.) Many in the industry question if two different control systems are required. STRATEGY: Clarify in the Requirement that two authentication methods using the same control system are compliant (for example, badge/thumbprint). ISSUE 8: Violation Risk Factors (1.) One VRF is assigned to a requirement, regardless if it applies to both high and medium impact. STRATEGY: Where a medium VRF is proposed, revise it to medium for high impact and lower for medium impact. Change some mediums to lower. This may require double the number of requirements in order to have different VRFs for Highs and Mediums as NERC's format is rigid. ISSUE 9: Definition of Annual (1.) Annual is not in the NERC Glossary. V5 requires 'at least once every calendar year, but not to exceed 15 calendar months.' CAN-0010 establishes once per calendar year (unless the entity elects the tighter period of once within the last 12-month period). (2.) V5 is more restrictive than the NERC CAN. V5 creates a second criterion for reaching compliance in the 12 requirements where the above phrase is used. V5 creates a CIP-specific meaning of annual that is different from the other NERC standards. STRATEGY: Use 'annual' in V5. Alternatively, use 'once per calendar year or not to exceed 15 calendar months between occurrences.' This proposal is not more restrictive than CAN-0010. The proposal provides entities with more workload scheduling flexibility. ISSUE 10: Control Center Definition (1.) V5 creates a CIP-specific definition of 'Control Center.' CIP standards are not the only NERC standards using the term control center. (2.) The proposed CIP definition does not fit the context of the other NERC standards. Multiple definitions across reliability standards for the same term are confusing to implement and complicate auditing. (3.) The 300MW threshold in the proposed V5 definition has little basis relative to reliability. STRATEGY: Control Center should remain undefined in the CIP V5 standards and all references should be lower case. Create a separate project for team of experts in this area to devise a definition for the NERC Glossary of Terms. ISSUE 11: Physical Security Perimeter (PSP) Monitoring and Alerting (1.) V5 CIP-006 requires monitoring the PSP 24/7 for 'unauthorized circumvention of a physical access control into a PSP' and issuing an alarm 'in response to detected unauthorized circumvention of a physical access control into a PSP' in R1.4 and R1.5, respectively. (2.) V4 required monitoring and alerting of PSP access points. V5 eliminates the concept of access points and six-wall border. (3.) V5 can be read to mean monitoring and alerting of the entire PSP, not just the access points, such that video and/or motion detection would be needed for compliance. As such, V4 monitoring and alerting of access points for existing six-wall border PSPs may not be compliant for V5. STRATEGY: Clarify in the requirements R1.4 and R1.5 that if a six-wall border can be established then only the access points to a PSP need to have monitoring and alerting and not the entire PSP. If a six-wall border cannot be established then require monitoring and alerting for the entire PSP.
Individual
Andrew Gallo
City of Austin dba Austin Energy
No
No
No
No
No
Yes
No
Please see the comments submitted by the Texas Regional Entity's NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Regional Entity's NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Regional Entity's NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Regional Entity's NERC Standards Review

Subcommittee, to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Regional Entity's NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Regional Entity's NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Regional Entity's NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Yes
Please see the comments submitted by the Texas Regional Entity's NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Individual
Christina Conway
Oncor Electric Delivery Company LLC
Yes
Yes
Yes
Yes
No
INTERACTIVE REMOTE ACCESS COMMENTS: (1) Oncor has proposed that the definition of "Interactive Remote Access" or the applicability of CIP-005-5 R2 should be adjusted to reflect the exclusion of serially connected/non-routable/non-network connected devices. There is minimal reliability benefit and significant cost associated with applying the CIP-005-5 R2 requirements to all serially connected/non-routable/non-network connected devices that require remote access. Authentication when establishing connectivity to these systems is covered by CIP-005-5 R1.4 and provides the required cyber security. The cleanest way to correct this issue is to adjust the definition of "Interactive Remote Access" as follows: "All user-initiated access OF BES CYBER ASSETS WITHIN AN ELECTRONIC SECURITY PERIMETER by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether routable or dial-up access, using a client or remote access technology. Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications." Alternatively, the applicability of CIP-005-5 R2 could be changed from "Medium Impact BES Cyber Systems" to "Medium Impact BES Cyber Systems with External Routable Connectivity." (2) There is no mention of serially connected/non-routable/non-network connected devices in the CIP Awareness Bulletin (Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)) that initiated the CIP-005-3 SAR or the Guidance for Secure interactive Remote Access, which was ultimately issued after the CIP-005-3 revisions were not adopted. All discussions in these documents are in the context of IP addressable devices connected to a network that could be protected through the use of VPNs, proxy servers, etc. The current definition of "Electronic Security Perimeter" in the "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" has evolved to make a delineation between devices that are connected to a network via routable protocol and those that are not. This further supports Oncor's proposed adjustment to the definition of "Interactive Remote Access." (3) In addition, in Consideration of Comments – Cyber Security Order 706 Version 5 CIP Standards (definition of "Electronic Access Point" section), it provides the following: "The SDT has not included serial, non-routable communications within the definition of EAP (other than with respect to dialup in CIP-005 R1.4). Dedicated serial communications are intentionally left out of scope, as the SDT believes it would be inappropriate for the standards to mandate a universal perimeter or firewall type security across all entities and all serial communication situations. There is no 'firewall' capability for a RS232 cable run between two cyber assets. Without a clear security control that can be applied in most every circumstance, such a requirement would just generate TFEs." This demonstrates that the SDT considered and rejected the inclusion of serial, non-routable devices and specifically chose not to include them in the definition of "Electronic Access Point." Thus, Oncor's proposal is simply

urging that the same approach be taken with respect to “Interactive Remote Access” and that it should also not apply to serially connected/non-routable/non-network connected devices. (4) Oncor further requests additional information in the guidance section that addresses what is and is not a remote access client or remote access technology.
Yes
Yes
N/A
N/A
N/A
N/A
INTERACTIVE REMOTE ACCESS COMMENTS: (1) Oncor has proposed that the definition of “Interactive Remote Access” or the applicability of CIP-005-5 R2 should be adjusted to reflect the exclusion of serially connected/non-routable/non-network connected devices. There is minimal reliability benefit and significant cost associated with applying the CIP-005-5 R2 requirements to all serially connected/non-routable/non-network connected devices that require remote access. Authentication when establishing connectivity to these systems is covered by CIP-005-5 R1.4 and provides the required cyber security. The cleanest way to correct this issue is to adjust the definition of “Interactive Remote Access” as follows: “All user-initiated access OF BES CYBER ASSETS WITHIN AN ELECTRONIC SECURITY PERIMETER by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity’s Electronic Security Perimeter(s), whether routable or dial-up access, using a client or remote access technology. Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.” Alternatively, the applicability of CIP-005-5 R2 could be changed from “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routable Connectivity.” (2) There is no mention of serially connected/non-routable/non-network connected devices in the CIP Awareness Bulletin (Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)) that initiated the CIP-005-3 SAR or the Guidance for Secure interactive Remote Access, which was ultimately issued after the CIP-005-3 revisions were not adopted. All discussions in these documents are in the context of IP addressable devices connected to a network that could be protected through the use of VPNs, proxy servers, etc. The current definition of “Electronic Security Perimeter” in the “Definitions of Terms Used in Version 5 CIP Cyber Security Standards” has evolved to make a delineation between devices that are connected to a network via routable protocol and those that are not. This further supports Oncor’s proposed adjustment to the definition of “Interactive Remote Access.” (3) In addition, in Consideration of Comments – Cyber Security Order 706 Version 5 CIP Standards (definition of “Electronic Access Point” section), it provides the following: “The SDT has not included serial, non-routable communications within the definition of EAP (other than with respect to dialup in CIP-005 R1.4). Dedicated serial communications are intentionally left out of scope, as the SDT believes it would be inappropriate for the standards to mandate a universal perimeter or firewall type security across all entities and all serial communication situations. There is no ‘firewall’ capability for a RS232 cable run between two cyber assets. Without a clear security control that can be applied in most every circumstance, such a requirement would just generate TFEs.” This demonstrates that the SDT considered and rejected the inclusion of serial, non-routable devices and specifically chose not to include them in the definition of “Electronic Access Point.” Thus, Oncor’s proposal is simply urging that the same approach be taken with respect to “Interactive Remote Access” and that it should also not apply to serially connected/non-routable/non-network connected devices. (4) Oncor further requests additional information in the guidance section that addresses what is and is not a remote access client or remote access technology.
N/A
N/A
Yes
N/A
(1) In the comments that Oncor has submitted on Draft 2 Version 5 of the CIP Standards, there are

several instances in which Oncor has made specific suggestions for revised language that it was not able to provide in response to earlier draft versions. When Draft 2 Version 5 was made available, Oncor formed a team that performed an in-depth analysis of it from a broad cross-functional perspective. That team carefully analyzed each standard, the interactions of the standards, and how those standards could potentially impact reliability. This in-depth analysis led Oncor to the positions presented in its comments on Draft 2 Version 5. Oncor is committed to a successful ballot of CIP Version 5 and looks forward to the inclusion of these comments in Draft 3. (2) One of Oncor's primary concerns with Draft 2 of Version 5 of the CIP Standards is its broad application of many CIP requirements to cyber assets regardless of their connectivity, which results in an unreasonable expansion of the applicability of the CIP requirements to assets for which the additional requirements will provide minimal or no reliability benefit. Oncor urges the SDT to evaluate each draft standard and ensure that the protection each standard affords is applied in a reasonable manner. In its comments on each requirement in Draft 2, Oncor has identified those instances in which it believes that the applicability of the requirement has been expanded beyond what is reasonable and has provided language that identifies a more reasonable and appropriate applicability for that requirement. (3) Oncor also suggests the Standard Drafting Team develop a high level summary of the CIP Version 5 standards that shows the interaction between each standard, applicability type, and definition and provide that summary with the next draft. This will help eliminate any remaining inconsistencies and overlaps between standards prior to the next draft. (4) Oncor participated in the development of EEI consensus comments and supports the comments that EEI has submitted, as indicated in the individual question responses. (5) Oncor participated in the development of the Texas RE NERC Standards Review Subcommittee consensus comments and supports the comments that the Texas RE NERC Standards Review Subcommittee has submitted, as indicated in the individual question responses.
Individual
Scott Miller
MEAG Power
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Southern California Edison
Nathan Smith
Yes
No
Yes

Yes
Yes
SCE Comments to CIP-5 Definitions -Interactive Remote Access: Why is dial-up access considered here but not in all definitions? Please add the following definition: -Dial-up Access: Connectivity through 10-digit phone numbers dialed by a human using conventional public telephone lines.
No
Yes
-BES Cyber Asset: Although the definition is much improved it still does not prescribe how to document that an asset has been connected to the BES for less than 30 days. -CIP Senior Manager: Is the phrase "…overall authority and responsibility for…" intended to carry a different meaning from "…overall responsibility and authority for…" as it is written both ways in reference to the CIP Senior Manager?
-Control Center: What does the term "operating personnel" mean? We suggest revising this term to "BES operating personnel" or some other clarifying term.
-CIP Senior Manager: Is the phrase "…overall authority and responsibility for…" intended to carry a different meaning from "…overall responsibility and authority for…" as it is written both ways in reference to the CIP Senior Manager?
No comments
No comments
-Electronic Access Point: Please confirm the notion that cyber assets only communicate with other cyber assets?
No comments
No
SCE Comments to the CIP-5 Implementation Plan Initial Performance of Certain Periodic Requirements Section 5 provides a list of CIP Standards and Requirements that require compliance on a different schedule. Some standards require compliance as soon as within 14 days of the Effective Date of the Version 5 CIP Cyber Security Standards, however, the Proposed Effective Date for Version 5 CIP Cyber Security Standards Section provides for a 24 month implementation window. Please clarify that there is a minimum 24 month implementation window for all CIP Version Five standards.
Repeating, Initial Performance of Certain Periodic Requirements Section 5 provides a list of CIP Standards and Requirements that require compliance on a different schedule. Some standards require compliance as soon as within 14 days of the Effective Date of the Version 5 CIP Cyber Security Standards, however, the Proposed Effective Date for Version 5 CIP Cyber Security Standards Section provides for a 24 month implementation window. Please clarify that there is a minimum 24 month implementation window for all CIP Version Five standards.
-Protected Cyber Assets: The definition does not prescribe how to document that an asset has been connected to the BES for less than 30 days. Please add the following definition: -Dial-up Access: Connectivity through 10-digit phone numbers dialed by a human using conventional public telephone lines.
Individual
Heather Laws
POrtland General Electric
Yes
No
Yes
Yes
Yes
Yes
Yes
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary

to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
Yes
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
Individual
Don Schmit
Nebraska Public Power District
No
Yes
No
No
No
No
Yes
[A]The comments submitted by NPPD should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. The NPPD comments on these definitions are predicated by our position that CIP-002-5 is fundamentally flawed, and the proposed methodology prescribed by Requirement 1 is in direct conflict with the structure of the definition for BES Cyber Asset and BES Cyber System. More specifically, the impact rating should align with the facility instead of the cyber asset. Based on this position, the NPPD proposes the following changes to the definitions of "BES Cyber Asset" and "BES Cyber System". "BES Cyber Asset" should be defined as: "A Cyber Asset that if rendered unavailable, degraded, or misused would prevent one or more BES Sites from performing its reliability function for the Bulk Electric System. Redundancy of affected BES Sites and BES Cyber Assets shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is connected to a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)". The definition of "BES Cyber System" may then by modified as: "One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks at a BES Site for a functional entity." NPPD recommends the addition of a definition for a "BES Site" to be described as: "A registered entity-owned geographic location that: (1) performs the functional obligations of the Reliability Coordinator, Balancing Authority, Generator Operator, Generator Owner, Interchange Coordinator, Reliability Coordinator, Transmission Operator, or Transmission Owner, including Control Centers, Backup Control Centers and associated data centers that support those functional obligations, and (2) contains UFLS or UVLS Systems that are part of a Load shedding program and Load-Serving Entity

functional obligation, or (3) provides the protection or restoration of the BES while performing the functional obligations of Distribution Provider, or (4) provides Blackstart Resources, (and) that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact the reliability of the BES."
None.
[A]The comments submitted by NPPD should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. [Proposed Verbiage] BES Cyber System Information: Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System, as defined within the Entity's information protection program. Examples of BES Cyber System Information may include, but are not limited to, entity-specific security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses or security configuration information without context, ESP names, or policy statements. (Rationale: Removed the indication that the information had to be developed by the entity but still allowed for the omission of publicly-available vendor information in the program's protection. Removed redundancy for "allowing unauthorized access." Added security configuration information to the list of information without context that should not need special protection. E.g. generic hardening procedures.) [Proposed Verbiage] CIP Senior Manager: One management official with overall accountability and responsibility for the implementation of the entity's NERC CIP program. (Rationale: removed "senior" to avoid implication that the official needs to be of a certain "rank" within the organization. Removed leading and added accountability phrasing to more accurately reflect the actual role within the organization.) [Proposed Verbiage] CIP Exceptional Circumstance: A situation that involves one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident that may require emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of workforce availability. (Rationale: removed "large scale" from the phrase regarding workforce availability. Workforce limitations may be localized or involve small numbers of personnel but may impact operations significantly. Added "that may" in front of 'require emergency assistance' to allow the entity to define the appropriate response on a case by case basis.)
[A] The comments submitted by NPPD should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. NPPD appreciates the modifications made by the SDT to the standard and definitions related to physical security. [Proposed Verbiage] Physical Access Control Systems: Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. (Rationale: In order to remove the ambiguity around whether or not workstations used only for monitoring physical security alarms are subject to CIP requirements (e.g. guard's desk), the word "alert" has been removed. The inclusion of "control" and "log" still ensure that the equipment that requires protection is included in the definition.)
[A] The comments submitted by NPPD should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. The definition of Electronic Access Control or Monitoring Systems is still too vague. For Access Control, specifically, does this mean every cyber system that might contribute to the authentication, authorization, and accounting ("AAA") of a person crossing an EAP? If an entity uses Windows Active Directory for firewall authentication, for instance, this could be interpreted to mean every domain controller in the company is in scope. Extending that argument, the Help Desk PC that is used to grant access to the Windows Active Directory could be interpreted as being part of the AAA

process, and therefore is itself an Electronic Access Control cyber asset. Likewise, a PC used at the guard desk (or third-party managed security provider) that is used to monitor alerts from the EAP could be considered a Cyber Asset used for Monitoring. Recommend the SDT provide a comprehensive list of cyber asset examples or “bright-line” set of criteria for Electronic Access Control or Monitoring Systems. [Proposed Verbiage] Electronic Access Control or Monitoring Systems: Cyber Assets that perform electronic access control or electronic access monitoring for Interactive Remote Access to the Electronic Security Perimeter(s) or Cyber Assets that perform electronic access control or electronic access monitoring for Interactive Remote Access to BES Cyber Systems. Secondly, the NPPD would like to request that the SDT define the term “Access” used here and throughout the CIP standards, especially as it relates to cyber systems, or, specifically state that an entity can make their own definition of access such that different treatment can be given to high-risk access versus low-risk access. (“High-risk” meaning the ability to interact with, operate, modify, or cause availability issues with a BES Cyber System). Specific examples where “access”, if left undefined, could cause problems for an entity are: VMWare hypervisors, Oracle database clusters, or NAS systems that contain both BES and non-BES data/systems. Is the entity required to give CIP-004 treatment, for example, to an accounting clerk who has “access” to a receivables data table on an Oracle cluster that also hosts the backend database to a (BES) load control or EMS system? Does access to SCADA data, or a BES Energy Management System that also operates Distribution count?
[A] The comments submitted by NPPD should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. Does the definition of ESP presume the presence of an Electronic Access Point? In other words, does a BES Cyber System with no External Routable Connectivity fall within the scope of the CIP standards? Clarifying this point will pre-empt the need for interpretation or a CAN later. [Proposed Verbiage] Electronic Security Perimeter (“ESP”): A network to which BES Cyber Systems are connected using a routable protocol, surrounded by a logical border and which are only remotely accessible through an Electronic Access Point(s).
None.
No
[A] The comments submitted by NPPD should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. [1]In section 5 under “Initial Performance of Certain Periodic Requirements”, requirement CIP-010-5 R3, Part 3.2 is listed as needing to be initially performed within the first 12 calendar months. We request that this be pushed to at least 24 months to enable registered entities to perform two annual vulnerability assessments before attempting an active VA. Secondly, if industry approves the implementation requirements for planned and unplanned changes as being consistently 12 months, please collapse this section and simply state as such. The Disaster Recovery guidance is confusing, it seems to say “don’t hold up restoration for the sake of compliance, just be sure you’re in compliance at the end of restoration”, which seems to conflict. Please redraft to make it more clear what this intent of this section is. [2]The period between Version 4 and Version 5 enforceability needs to be addressed as it relates to Sites or Cyber Assets potentially requiring more protection in Version 4 than in Version 5. A transition period or a way to replace Version 4 with Version 5 protections must be allowed.
None.
Individual
Brian Evans-Mongeon
Utility Services Inc.
Yes
Yes
Yes
Yes

Yes
Yes
No
Utility Services supports the comments made by MMWEC in their Comments for BES Cyber Asset and BES Cyber System.
Please clarify the meaning of the word “locations”. Are properties that share the same BES point of interconnect considered to be one location? Suggest adding "and with two or more points of interconnection to the BES."
Utility Services suggest the removal of the word “single” from the CIP Senior Manager designation. “Official” is singular thereby making the word “single”, redundant.
None
None
None
None
Yes
None
None
None
Group
NCEMC
Scott Brame
Yes
No
No
Yes
Yes
Yes
Yes
NCEMC is concerned that in this definition the mere presence of a SCADA HMI might be considered a Control Center by a CEA if it could possibly be used to control BES assets in real-time even if an entity does not use it that way. Some of the registered entities do not man these control centers 24/7 and are unable to perform real time control after hours, or any other time that other duties take them 15 minutes away from the computer. In some instances these entities might be registered as TOPs only because they own a limited and discrete 115 kV facility that no other entity was willing to register as a TOP for. Often times this 115 kV facility performs no reliability function. NCEMC suggests adding “24/7 to the first sentence of the Control Center definition as shown in the underlined text: “One or more facilities hosting operating personnel 24/7 that monitor and control the Bulk Electric System (BES) in real-time …”
CIP Senior Manager – In this definition replace “CIP Standards” with CIP-002 through CIP-011. If this is not completed, this definition would apply to CIP-001 which still exists and is an unrelated standard. This revision will provide clarity to the limit of the definition.
Yes

Group
Dairyland Power Cooperative
Tommy Drea
No
Yes
No
No
No
Please see MRO NSRF comments.
No
Yes
Please see MRO NSRF comments.
Please see MRO NSRF comments.
Please see MRO NSRF comments.
Please see MRO NSRF comments.
Please see MRO NSRF comments.
Please see MRO NSRF comments.
Please see MRO NSRF comments.
No
Please see MRO NSRF comments.
Please see MRO NSRF comments.
Please see MRO NSRF comments.
Individual
Jennifer White
Alliant Energy
No
Yes
No
No
No
No
Yes
Alliant Energy voted “No” on this list of definitions as we believe it is in fundamental conflict with the rest of the Standards. Proposed definitions herein should be considered within the context of the requirements, as well, due to considerable dependency between the proposed definitions and the proposed language changes throughout the rest of the Standards. Alliant Energy supports the MRO NSRF comments, as well. [1]Alliant Energy’s recommendations on these definitions are predicated by our position that CIP-002-5 is fundamentally flawed, and the proposed methodology prescribed by Requirement 1 is in direct conflict with the structure of the definition for BES Cyber Asset and BES Cyber System. More specifically, the impact rating should align with the facility instead of the cyber asset. Based on this position, Alliant Energy proposes the following changes to the definitions of “BES Cyber Asset” and “BES Cyber System”. [Proposed Verbiage] “BES Cyber Asset” should be defined as: “A Cyber Asset that within 15 minutes of being rendered unavailable, degraded, or misused would prevent one or more BES Sites from performing its reliability function for the Bulk Electric System. Redundancy of affected BES Sites and BES Cyber Assets shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is connected to a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)”. [Proposed Verbiage] The definition of “BES Cyber

System" may then by modified as: "One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks at a BES Site for a functional entity." [Clarification] Alliant Energy requests clarification regarding demonstrating compliance for a BES Cyber System when not every device within the system can meet the requirement applied to the system, as a whole. We recommend that the system be not be found in a state of "non-compliant" as long as one or more devices within the identified system can fully meet the documented requirement and as long as every device within the system is documented as to its capability for meeting that requirement. If this is not the intent of the SDT, this issue must be addressed along with the definitions, because it is at this fundamental level that the Standards may or may not be applicable. [2] Alliant Energy recommends the addition of a definition for a "BES Site" to be described as: A registered entity-owned geographic location that: (1) performs the functional obligations of the Reliability Coordinator, Balancing Authority, Generator Operator, Generator Owner, Interchange Coordinator, Reliability Coordinator, Transmission Operator, or Transmission Owner, including Control Centers, Backup Control Centers and associated data centers that support those functional obligations, and(2) meets the criteria in CIP-002-5 Attachment 1 – Impact Rating Criteria Parts 3.1 – 3.5 and that (3) within 15 minutes of being rendered unavailable, degraded, or misused would prevent the entity from performing its reliability function for the Bulk Electric System.

[Proposed Verbiage] BES Cyber System Information: Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System, as defined within the Entity's information protection program. Examples of BES Cyber System Information may include, but are not limited to, entity-specific security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses or security configuration information without context, ESP names, or policy statements. (Rationale: Removed the indication that the information had to be developed by the entity but still allowed for the omission of publicly-available vendor information in the program's protection. Removed redundancy for "allowing unauthorized access". Added security configuration information to the list of information without context that should not need special protection.E.g. generic hardening procedures.) [Proposed Verbiage] CIP Senior Manager: One management official with overall authority, accountability, and responsibility for the implementation of the entity's NERC CIP program. (Rationale: removed "senior" to avoid implication that the official needs to be of a certain "rank" within the organization. Removed leading and added accountability phrasing to more accurately reflect the actual role within the organization.) [Proposed Verbiage] CIP Exceptional Circumstance: A situation that involves one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident that may require emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of workforce availability. (Rationale: removed "large scale" from the phrase regarding workforce availability. Workforce limitations may be localized or involve small numbers of personnel but may impact operations significantly. Added "that may" in front of 'require emergency assistance' to allow the entity to define the appropriate response on a case by case basis.)

Alliant Energy appreciates the modifications made by the SDT to the standard and definitions related to physical security. [Proposed Verbiage] Physical Access Control Systems: Cyber Assets that control or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. (Rationale: In order to remove the ambiguity around whether or not workstations used only for monitoring physical security alarms are subject to CIP requirements (e.g. guard's desk), the word "alert" has been removed. The inclusion of "control" and "log" still ensure that the equipment that requires protection is included in the definition. Also, the alerting requirement is still included in the Standards, so the protection will not be eliminated.)

[A] The comments submitted by the Alliant Energy should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead

of with the draft verbiage. Electronic Access Control and Monitoring Systems should be reduced to "Electronic Access Control Systems" and defined in the same structure as PACs. This is just for consistency and ease of use. If they perform the same functions, they should be parallel. Removed BES Cyber Systems to add clarity regarding the function of the EAP and the controls already required when External Routable Connectivity is at play. The definition of Electronic Access Control or Monitoring Systems is potentially still too vague. For Access Control, specifically, does this mean every cyber system that might contribute to the authentication, authorization, and accounting ("AAA") of a person crossing an EAP? If an entity uses Windows Active Directory for firewall authentication, for instance, this could be interpreted to mean every domain controller in the company is in scope. Extending that argument, the Help Desk PC that is used to grant access to the Windows Active Directory could be interpreted as being part of the AAA process, and therefore is itself an Electronic Access Control cyber asset. Likewise, a PC used at the guard desk (or third-party managed security provider) that is used to monitor alerts from the EAP could be considered a Cyber Asset used for Monitoring. Recommend the SDT provide a comprehensive list of cyber asset examples or "bright-line" set of criteria for Electronic Access Control or Monitoring Systems. [Proposed Verbiage] Electronic Access Control or Monitoring Systems: "Cyber Assets that perform electronic access control or electronic access monitoring for Interactive Remote Access to the Electronic Security Perimeter(s)."

[A]The comments submitted by Alliant Energy should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. Does the definition of ESP presume the presence of an Electronic Access Point? In other words, does a BES Cyber System with no External Routable Connectivity fall within the scope of the CIP standards?Clarifying this point will pre-empt the need for interpretation or a CAN later. [Proposed Verbiage] Electronic Security Perimeter ("ESP"): A network to which BES Cyber Systems are connected using a routable protocol, surrounded by a logical border and which are only remotely accessible through an Electronic Access Point(s). [Proposed Verbiage] Protected Cyber Asset: "A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter (a Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes)." Removed "directly" to allow connection within the ESP without requiring the connection to be through a BES Cyber System or Cyber Asset.

[Proposed Verbiage] Remove "Any" from Reportable to be consistent with the change to Cyber Security Incident.

No

Alliant Energy voted "No" to the proposed implementation plan due to the comments herein. [1]In section 5 under "Initial Performance of Certain Periodic Requirements", requirement CIP-010-5 R3, Part 3.2 is listed as needing to be initially performed within the first 12 calendar months. We request that this be pushed to at least 24 months to enable registered entities to perform two annual vulnerability assessments before attempting an active VA. Secondly, if industry approves the implementation requirements for planned and unplanned changes as being consistently 12 months, please collapse this section and simply state as such. The Disaster Recovery guidance is confusing, it seems to say "don't hold up restoration for the sake of compliance, just be sure you're in compliance at the end of restoration", which seems to conflict. Please redraft to make it more clear what this intent of this section is. [2]The period between Version 4 and Version 5 enforceability needs to be addressed as it relates to Sites or Cyber Assets potentially requiring more protection in Version 4 than in Version 5. A transition period or a way to replace Version 4 with Version 5 protections must be allowed.

[VSL] Alliant Energy strongly recommends that the VSLs be revisited to address the zero tolerance approach. Additionally, they are structured such that there is no variance in severity based on the impact rating of the cyber system or the specific element of the sub-requirement. This needs to be addressed in order to ensure that the entities can be held accountable at the right level based on actual risk. [BES Cyber Systems and BES Cyber Assets] If the creation of the BES Cyber System was introduced with the intent to eliminate the need for TFEs, Alliant Energy agrees with the intention, but not the execution. The concept is not applied consistently throughout the Standards, insofar as there

are requirements that apply at the device level. Additionally, it is not clear how many of the BES Cyber Assets within a system must meet the requirement in order to avoid a finding of non-compliance for the system. Alliant Energy recommends returning to the Critical Cyber Asset terminology, as it allows entities to retain currently existing documentation if it is sufficient to meet the new Standards. Also, this terminology can be successfully used to implement programs while avoiding the TFE if the proposed recommendations related to the VSLs and the implementation of programs that recognize and mitigate for specific configuration. The Standards should be written such that the entity's understanding of its own devices and vulnerabilities is required, not that device by device configuration constitutes a violation.
Individual
Nathan Mitchell
American Public Power Association
Yes
Yes
Yes
Yes
Yes
Yes
Yes
APPA agrees with the revised definition of Control Center. The SDT has focused the definition to the core of what a Control Center really is; real-time operations, hosting operating personnel, and perform the functions of RC, BA, TOP, or GOP. With this clear definition, many small entities will be spared the burden of proving that their distribution dispatch centers are not Control Centers. However, in the webinar conducted by the SDT a question was raised on the issue of "manual and voice instruction" as a "control" where this term is used in the definition. The SDT referred this question back to the CIP Version 1 FAQ from May 9, 2005 where it was stated: "monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction." APPA has a real concern that the SDT has interpreted the term "control" in a way that will eliminate the option of removing/not installing "remote accessible or automatic controls" as a way to mitigate the risk of a cyber incident within a "monitor only" control center. This type of control center should not be required to implement the High or Medium Impact requirements in CIP-003-5 through CIP-011-5 nor document compliance with these standards. APPA believes that having an intelligent operator as the device between the monitored cyber asset and the actual "manual or voice instruction control" is "air gapped." APPA believes that a control center built without remote accessible or automatic controls should be designated as a Low Impact facility. This designation will help reduce the burden of compliance for small entities that chose to use this cyber risk mitigation method. APPA Recommendation: Clarify in guidance what "control" within the Control Center definition means. If the SDT uses the CIP Version 1 FAQ response as the guidance: "monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction" APPA recommends that control centers which use only manual or voice instruction as the control be designated as Low Impact facilities in CIP-002-5 Attachment 1.
Yes
APPA agrees with the revision of the implementation timeframe. Having a High and Medium Impact implementation timeframe set at 24 months or July 1, 2015 will focus the industry on developing compliance documentation for these critical facilities first. This may work well with the CIP Version 4 coordination as most of those facilities identified in Attachment 1 may already be identified and in the

process to be covered under a compliance plan. APPA agrees with the 36 month or July 1, 2016 implementation plan for Low Impact facilities. This will give those entities setting up completely new CIP compliance programs enough time to budget and incorporate these plans prior to enforcement.
APPA has focused our comments on the impact of the standards on small entities. We recommend that the SDT take a close look at the applicability and the requirements in all of the CIP Version 5 standards. Where the standards are applicable to small entities the SDT needs to account for the impact on small entities and only include those requirements if they are absolutely critical for the protection of the reliability of the BES. If these requirements must be included, than the SDT should allow for a small entity exemption process.
Individual
Tracy Richardson
Springfield Utility Board
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
David R. Rivera
New York Power Authority
No
Yes
Yes
Yes
Yes
No
No
NYPA agrees with NPCC comments.
NYPA agrees with NPCC comments
NYPA agrees with NPCC comments
No

NYPA agrees with NPCC comments, plus - NYPA would like clarification regarding implementation time periods for disaster recovery (pg 4,5); there is an allowance to handle the emergency without worrying about compliance activities but then they want compliance to be met otherwise it's a violation. What is the time frame to get the system compliant after the disaster recovery? Also, the section on "Initial performance of certain periodic requirements" should include CIP-009 R2 part 2.3 under item 5.
NYPA agrees with NPCC comments, plus - NYPA would like clarification regarding implementation time periods for disaster recovery (pg 4,5); there is an allowance to handle the emergency without worrying about compliance activities but then they want compliance to be met otherwise it's a violation. What is the time frame to get the system compliant after the disaster recovery? Also, the section on "Initial performance of certain periodic requirements" should include CIP-009 R2 part 2.3 under item 5.
Group
Progress Energy
Jim Eckelkamp
Yes
Yes
Yes
Yes
Yes
Yes
No
Yes
Progress Energy agrees with EEI comments with the modified and additonal comments below: Issue = Low Impact BES Cyber Assets in scope • FERC's version 4 Order 761 expects all BES Cyber assets should be in scope in V5. • Audit issue of providing evidence of policy implementation on Low impact cyber assets. Strategy =Focus on 'BES site' level definition for Lows with security policy applied to sites, not individual cyber assets. Issue = Inclusion of Cyber Assets regardless of connectivity • Blanket connectivity exclusion removed in CIP-002. Connectivity addressed in applicability column of requirements in CIP-003 to CIP-011. • Example substation: Non-externally routable cyber assets increase cyber asset count 40% and some medium requirements are not good fits. Strategy = More liberal use of 'External Routable Connectivity' qualifier in the applicability column for more requirements throughout standards. Issue= Zero-defect requirements with compliance (not reliability) risk • 8 of top 10 most violated standards in 2011. • 91% of FFTs approved by FERC in March order which invited proposals to revise or remove requirements. • NIST 800-53 App. E Minimum Assurance Requirements recognize flaws will be discovered and focus on continuous improvement. • Other federal regulators do not enforce zero-defect perfection forever. Strategy= Overall NERC Standards issue and a philosophical change to requirements. Likely not to be fixed between drafts 2 and 3. Issue= Complexity of Applying the Requirements • There are approximately 20 applicability references, so it's complicated to map the requirements to the classification of assets. • However, this is the result of breaking up 'one size fits all' type requirements Strategy= The drafting team needs to produce a comprehensive mapping of each of classification of asset including all applicable

requirements in a single document for and post it with Draft 3 to demonstrate how an entity would actually apply the requirements. Focus on sites for CIP-002 and Low and add requirements for medium and high per attachment 1. issue= Blackstart units and cranking paths moved to Low Impact • Concern that it is a lessening of V1-V4, FERC may remand Strategy= File as-is with technical and risk-based justification for not “lessening” the standard. Issue= Immediate Revocation of access • V5 requires that the revocation process be initiated immediately and completed within 24 hours. • Though FERC Order 706 mandated “immediate” revocation, many entities consider it unattainable. Strategy= Limit to High Impact cyber assets only. Allow reasonable response time for Medium Impact and protected information. An example of unacceptable “zero defect” risk, and a candidate for above strategy to add language in Requirement statement. Issue= Physical Access Controls for High Impact • FERC Order 706 directed defense in depth (“two or more”). • V5 limits this to control centers only. • Many in the industry question if two different control systems are required. Strategy= Clarify in the Requirement that two authentication methods using the same control system are compliant (for example, badge/thumbprint). Issue= Violation Risk Factors • One VRF is assigned to a requirement, regardless if it applies to both high and medium impact. Strategy= Where a medium VRF is proposed, revise it to medium for high impact and lower for medium impact. Change some mediums to lower. This may require double the number of requirements in order to have different VRF’s for Highs and Mediums as NERC’s format is rigid. Issue= Definition of Annual • Annual is not in the NERC Glossary. CAN-0010 establishes once per calendar year (unless the entity elects the tighter period of once within the last 12-month period). • V5 requires “at least once every calendar year, but not to exceed 15 calendar months”. • V5 is more restrictive than the NERC CAN and V5 creates a second criterion for reaching compliance in the 12 requirements where the above phrase is used. Strategy= Consider using “annual” in V5 and the use of “or”.
Individual
Maggy Powell
Exelon Corporation and its affiliates
No
No
No
No
No
No
Yes
BES Cyber Asset – support as proposed BES Cyber System – The use of the terms “responsible entity" and "functional entity" is inconsistent and confusing. It appears that the proposal is to define new terms to describe items that are covered by existing definitions. In other standard development projects we’ve seen similar attempts (i.e. NUC-001 and the definition of “Transmission Entity”) which resulted in added confusion. Defining new terms when existing terms suffice should be avoided. Our assumption is that the definition of Functional Entity refers to the term as defined in the Functional Model. It is critical to clarify that we are consistently using one definition, so please clarify whether the SDT intended to refer to this definition. Responsible Entity is not defined in the NERC Glossary of Terms or Functional Model; though, it is capitalized in the Applicability section (section 4) of the CIP version 5 standards. The term is not capitalized in the BES Cyber System definition. Is the responsible entity in the BES Cyber System definition intended to be the same as Responsible Entity in the Applicability? Further, the creation of a "responsible entity" may go beyond the boundary of a registered functional entity. Only a registered entity can be accountable to the standards even if that entity arranges/contracts for another party to conduct a function covered by a standard. To clarify and avoid a potential expansion of scope, consider the following revision: "BES Cyber System - One or more BES Cyber Assets logically grouped to perform one or more reliability tasks for a Functional Entity." Cyber Asset - Support as proposed
Control Center should not be defined as part of the CIP standards. The complexities around control centers warrant that a focused team work to define control center as part of a separate project. Further, other standards beyond CIP utilize the term “control center” and the context for those standards is relevant to the discussion in defining the term. If defined by the CIP standards, it will be

inappropriate to apply that definition to the same term in another standard. As well, multiple definitions across reliability standards will be confusing and complicates auditing. The project to define Bulk Electric System (BES) included the task to identify all locations and contexts in which the BES term appeared. In developing an appropriate definition, the analysis included this look at the term's role across all standards. Definition of Control Centers should be afforded the same analysis. Control Center should remain undefined in the CIP V5 standards and all references should be lower case. Specific to the proposed language, it is problematic that the definition is not aligned with reliability impact. Defining a control center by the number of associated locations is not indicative of the role to reliability that the particular control center may or may not play. While CIP-002 Attachment 1 attempts to delineate degree of impact through thresholds (i.e. 300 MW for Medium in 2.11) these thresholds are weakly aligned with reliability impact. For example, a single generating facility's control room could control 1000 MW at a single location and not be a control center, but another facility's control room could control 290 MW in the location in which it resides along with remote start capability for another facility's 90 MW unit and become a control center. The perverse incentive created is to disconnect remote connectivity which is contrary to reliable practice. We recognize the challenge in finding an appropriate threshold measure and struggle to offer an alternative. Thus, we prefer that a focused team tackle the matter. Inclusion of this definition is a primary reason for the NEGATIVE votes on CIP-002. While definitions cover the full suite of standards, we opted to reflect the definition's influence on voting in the CIP-002 ballot to enable our support for some standards. If the SDT insists on creating a control center definition, we suggest that the definition focus on applicability to the CIP standards by naming the definition "CIP Control Center." This will limit the impact on the use of control center in other standards, but still provide a model definition for the term. To clarify the definition language further, please consider the following revisions: A facility hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability functional tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at three or more locations, or 4) a Generation Operator for generation Facilities at three or more locations.

BES Cyber System Information – support as proposed CIP Exceptional Circumstances – The definition appears to be too broad and as a result causes concerns with CIP-006 Parts 2.1 and 2.2 (and others). For example, under the proposed version of the definition CIP-006-5 Part 2.1 requires continuous escort of visitors except in a CIP Exceptional Circumstance. This case allows a blanket exception for all visitors within the PSP to avoid escort (including ones already inside under escort), which seems contrary to the intent of Part 2.1 (actual intent being things like emergency medical personnel). It seems appropriate to require continuous escort under the following conditions: civil unrest; imminent or existing hardware, software, or equipment failure; enactment of a mutual assistance agreement; and impediment of large scale workforce availability. To remedy this issue, we recommend that these situations and the words "or similar," be removed from the definition of CIP Exceptional Circumstance to read: CIP Exceptional Circumstance - A situation that involves one or more of the following conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, a Cyber Security Incident requiring emergency assistance, and a response by emergency services. CIP Senior Manager – support as proposed

Physical Access Control Systems – support as proposed Physical Security Perimeter – We appreciate the return to PSP. For consistency, the definition should read "Control or Monitoring". Proposed revision: Physical Security Perimeter – "The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled."

Electronic Access Control and Monitoring Systems – support as proposed Interactive Remote Access – The language is not clear as to what is to be accessed. To clarify, consider the following revision: Interactive Remote Access - All user-initiated access to a BES Cyber Asset by a person that originates from a Cyber Asset outside the Electronic Security Perimeter that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether routable or dial-up access, using a client or remote access technology. Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications. Intermediate Device – The term "device" raises concern. The term "device" is understood in practice as describing a broader set of assets than appropriate to apply in the CIP standards. In addition, it's not clear whether

software is considered a device even though we recognize that software runs on something that could be considered the device. To clarify, please consider replacing "Intermediate Device" with "Intermediate Cyber Asset".
Electronic Access Point – Some confusion remains about whether an EAP is part of the ESP or not. As we understand the intention is for an EAP is a point on the ESP. The example referenced is an EAP could be a port on a firewall, but not the firewall itself. The term “interface” is understood by some to be card or item inside the ESP rather than on the ESP as the definition seems to intend. Please consider removing the term “interface” so that the definition reads: Electronic Access Point (“EAP”) - A Cyber Asset on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter. Electronic Security Perimeter – support as proposed External Routable Connectivity – The current language defines "connectivity" as a system rather than a state in which the system finds itself. Consider the following revision: "External Routable Connectivity - The property of a BES Cyber System that is accessible from a Cyber Asset that is outside its associated Electronic Security Perimeter via a bi-directional routable protocol connection." Protected Cyber Asset – support as proposed
Cyber Security Incident – support as proposed Reportable Cyber Security Incident – support as proposed
No
While the revised Implementation Plan is an improvement, concerns remain. The sections on unplanned and planned changes are incomplete and the examples are contradictory. The proposed Implementation Plan clearly states that an unplanned change includes a generation plant modification changing its rated output. Typically, the entity that owns that generation site has to plan to change the output. The document states that planned changes are changes which were planned and implemented by the responsible entity. Where would an up-rate of a generation site reside - planned or unplanned? Further, the plan calls for one year (two years if first time) to comply with the suite of standards if it is an unplanned change. The comprehensive nature of the standards is independent of whether a change is planned or unplanned. There does not appear to be added reliability risk associated with planned changes, therefore, we propose that any change, planned or unplanned be given a year (two years if first time) to comply with the standards. We support the Previous Identity Verification language.
VSLs: VSLs do not cover scenario for failure to update documentation of BES Cyber Assets for more than 80 days but less than 90 days, i.e., moderate VSL covers 70 - 80 days and high VSL covers 90 - 100 calendar days. Please correct calendar ranges for moderate and high VSLs. It remains unclear how the numbers within the VSLs relate to reliability. Applicability: Similar to our concerns with the definition of BES Cyber System, the Applicability language appears to define new terms to describe items that are covered by existing definitions. In other standard development projects we’ve seen similar attempts (i.e. NUC-001 and the definition of “Transmission Entity”) which resulted in added confusion. Defining new terms when existing terms suffice should be avoided. Our assumption is that the definition of Functional Entity refers to the term as defined in the Functional Model. It is critical to clarify that we are consistently using one definition, so please clarify whether the SDT intended to refer to this definition. Responsible Entity is not defined in the NERC Glossary of Terms or Functional Model; though, it is capitalized in the Applicability section (section 4) of the CIP version 5 standards. It is not capitalized in other points in the standards. Further, the creation of a "responsible entity" definition may go beyond the boundary of a registered functional entity. Only a registered entity can be accountable to the standards even if that entity arranges/contracts for another party to conduct a function covered by a standard. Exemptions: We support the continued use of the language in 4.2.4.3 to reiterate the nuclear plant exemption, providing clarity in cyber security regulation of nuclear facilities. This exemption is consistent with the approved Version 4 Standards, the March 10, 2011 FERC Order (Docket# RM06-22-014) and the Memorandum of Understanding between NERC and the NRC (dated 12/30/2009).
Individual
Steve Karolek
Wiscsonsin Electric Power Company
No

Yes
Yes
Yes
No
No
Yes
Wisconsin Electric Power Company supports EEI Member Consensus comments as submitted by EE
In the definition of Interactive Remote Access, it is not necessary to discuss who owns a specific Cyber Asset from which it is initiated. The list provided does not appear to be inclusive enough. For example, what about a Cyber Asset owned by a hotel at which an employee or contractor is staying? What about a Cyber Asset owned by an "Internet Cafe" or a public library?
The definition of "External Routable Connectivity" needs to be reworded to clarify it is the ability to communicate with a BES Cyber System. The current wording says External Routable Connectivity "(is) A BES Cyber System..."
Yes
The term "Annual" should specifically added to the definitions as applied in NERC CAN-0010. This definition of Annual should be used throughout the standards in place of "each calendar year, not to exceed 15 months" since "calendar year" and "15 months" are incompatible measures. There are three months of the calendar year where a circumstance which causes an expected process to be executed longer than 12 months but less than 15 months since the previous execution would result in a violation of the "each calendar year" portion of the requirement.
Individual
Linda Jacobson-Quinn
Farmington Electric Utility System
No
No
Yes
Yes
Yes
Yes
No
BES Cyber System, Control Center, and Reportable Cyber Security Incident: BES Cyber System and Reportable Cyber Security Incident definitions refer to “reliability tasks”; while the definition of Control Center refers to “reliability functional tasks of a RC, BA, TOP or GOP” the drafting team should clarify if these tasks are intended to be the same
BES Cyber System, Control Center, and Reportable Cyber Security Incident: BES Cyber System and Reportable Cyber Security Incident definitions refer to “reliability tasks”; while the definition of Control Center refers to “reliability functional tasks of a RC, BA, TOP or GOP” the drafting team should clarify if these tasks are intended to be the same

BES Cyber System, Control Center, and Reportable Cyber Security Incident: BES Cyber System and Reportable Cyber Security Incident definitions refer to “reliability tasks”; while the definition of Control Center refers to “reliability functional tasks of a RC, BA, TOP or GOP” the drafting team should clarify if these tasks are intended to be the same
Yes
Group
Western Electricity Coordinating Council
Steve Rueckert
WECC believes that the Interchange Coordinator should be removed from the Applicability section of the CIP Version 5 standards. With the new Impact Rating Criteria found in CIP-002-5 Attachment 1, rather than the Risk-Based Assessment Methodology in versions 1-3, an Interchange Coordinator would have no critical assets, and subsequently no critical cyber assets in its role as an Interchange Coordinator. Any assets that meet the criteria in Attachment 1 for an entity registered as an Interchange Coordinator will be owned and operated through its registration as a different functional entity. If the Interchange Coordinator remains in the Applicability section of the CIP Version 5 standards, NERC should clarify the relationship between the currently registered function of Interchange Authority and the function identified in the Functional Model of the Interchange Coordinator.
Individual
John Allen
City Utilities of Springfield, MO
No
Yes
Yes
Yes
Yes
No
No
City Utilities of Springfield, MO agrees with the comments from SPP and APPA.
City Utilities of Springfield, MO agrees with the comments from SPP and APPA.
City Utilities of Springfield, MO agrees with the comments from SPP and APPA.
Yes

Group
ACES Power Marketing
Jason Marshall
No
No
No
Yes
No
Yes
Yes
(1) The clarity of the definition of BES Cyber Asset has been improved greatly. However, we are confused by the statement that a BES Cyber Asset is included in a BES Cyber System. From the background section of CIP-002-5, we thought that the responsible entity had the option of utilizing BES Cyber Systems. If so, then “is included” should be changed to “may be included”. Otherwise, the background section needs to state directly that all medium and high impact BES Cyber Assets must be grouped into BES Cyber Systems. (2) For BES Cyber System, we suggest replacing “to perform” with “to facilitate performance”. Often times, the BES Cyber System is used by a System Operator but the BES Cyber System does not actually perform the reliability task. The System Operator performs the task. An EMS is an excellent example. The EMS does not perform the reliability task. It only facilitates the System Operator performing the reliability task.
(1) We remain unconvinced that a definition of Control Center is needed particularly given that the EOP-008-1 standard regarding backup control centers/functionality was written without a definition. At a minimum, we recommend that the drafting team consult the EOP-008-1 drafting team regarding the definition. (2) If the definition persists, we suggest changing operating personnel to System Operators. System Operators clarifies that it is truly a control center and not a control house at a substation for instance. We also recommend deleting “reliability” or “functional” from the description of tasks. Since the functional model is focused on reliability tasks, they are essentially redundant.
(1) Please change “security procedures developed by the responsible entity” to “security procedures”. Many registered entities utilize consultants to write security procedures. Technically, one could exclude consultant developed security procedures with the current language. (2) While we agree that a safety issue should constitute a CIP Exceptional Circumstance, in general, safety issues are not subject to NERC standards. In this case, an unsafe condition would temporarily exempt the responsible entity from strict compliance with specific requirements identifying a CIP Exceptional Circumstance as an exception. Safety is regulated by other governmental agencies.
For Interactive Remote Access, it is not clear why bullet 1 is needed in the definition. What can be meant by Responsible Entity that is not covered by employees, vendors, contractors or consultants? If the Responsible Entity’s Cyber Asset is used by the employee, vendor, contractor or consultant, it will be covered in bullets 2 and 3. It is also not clear why ownership was added to bullets 2 and 3. Ownership is not relevant. The key is whether the Cyber Asset was used to initiate access.
Reportable BES Cyber Security Incident needs to be coordinated with the Disturbance and Sabotage Reporting standards drafting team.
Yes
(1) Overall, we agree with the implementation plan. However, some changes are needed. The implementation plan needs to clearly state when initial compliance is required for non-periodic requirements. Because there is a list of initial performance requirements for periodic requirements, it is implied that compliance is required for all other requirements on the effective date of the standard.

A direct statement to this effect would be perfectly clear. (2) The purpose of the table listing applicability on the last page to the three types of Cyber Assets is not clear. Their applicability is included in the standard. An explanation before the table would be helpful in understanding its inclusion. (3) The section on Disaster Recovery needs to more clearly state that there is a reasonable expectation that an entity may need a grace period after a significant outage (i.e. widespread outages caused by a hurricane). The section is clear that the focus should be first on recovering the system. However, it seems to imply that a responsible entity should be in compliance immediately following restoration activities. This is not likely as many BES Cyber Systems or BES Cyber Assets may have been replaced or reconfigured (i.e. relays) to accommodate rapid restoration. It will take time to make them compliant after the restoration period.
Individual
Robert Mathews
Pacific Gas and Electric Company
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Scott Berry
Indiana Municipal Power Agency
No
IMPA believes there needs to be a better feel or definition for what “monitoring and control” means. For instance, does a fax and/or e-mail constitute a manual control or is a manual control performed when a control switch is physically engaged by an operator? Also, if a Control Center is not staffed 24 x 7 x 365 but it does perform the reliability functional tasks of either 1), 2), 3), or 4) during normal work days does this constitute real-time control?? IMPA does not understand how voice instruction is part of the “monitor and operating control function.”(Reference: Frequently Asked Questions Cyber Security Standards CIP-002 – CIP-009 dated May 9, 2005) These terms are too broad and can very easily be defined in multiple ways by multiple people, especially auditors. These terms need to be defined by NERC before inclusion in this proposed standard. For instance, what might help to better define what a Control Center is for a Transmission Operator is to use a “aggregate weighted value” similar to that proposed in Attachment 1, Section 2.5 – there are many smaller entities that may have Transmission Facilities at only two locations that are between 100 kV to 199 kV and have a Control Center staffed during normal work days that will be forced to assign their Control Center a Medium

Impact Rating when is should be Low. When it comes to generation, a Control Center may monitor and control two generation sites that each has 160 MW for peaking use (low capacity factor). Under this condition, the Control Center would be a medium impact when it should be a low impact. Please see IMPA's recommendation on Form A, question 3 for the definition of Control Center.
Individual
Rolynda Shumpert
South Carolina Electric and Gas
One item that I do not see explicitly addressed in the standards would be how to treat temporary reconfigurations of the system that may elevate an asset that is normally not classified as a BES Cyber System to a higher status. Would a temporary system alignment require that the requirements for a Medium Impact be invoked on that temporary system while it is in that configuration? There are probably other examples of temporary system alignments that could elevate an asset's impact rating that should be addressed under the CIP standards, or maybe it is already included and I overlooked it when I reviewed the standards.
Group
Western Area Power Administration
Brandy A. Dunn
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Define “Associated Data Centers”
Group
SPP and Member companies
Lesley Bingham
No
Yes
Yes
Yes
Yes
No
Yes
BES Cyber Asset includes a sentence in parentheses which provides an example of what is not a BES Cyber Asset. In the previous version of the standard, this was a stand-alone definition for the term “Transient BES Cyber Asset”. It is more clear to have this defined separately than included in the definition of BES Cyber Asset. Whether it is termed a “Transient BES Cyber Asset” or is given another name is at the discretion of the Standards Drafting Team. A definition should state what a term IS; not what it is NOT.
Protected Cyber Asset includes a sentence in parentheses which provides an example of what is not a Protected Cyber Asset. In the previous version of the standard, this was a stand-alone definition for the term “Transient BES Cyber Asset”. It is more clear to have this defined separately than included in the definition of Protected Cyber Asset. Whether it is termed a “Transient BES Cyber Asset” or is given another name is at the discretion of the Standards Drafting Team. A definition should state what a term IS; not what it is NOT.
Yes
Group
IRC Standards Review Committee
Christine Hasha
Yes
No
Yes
Yes
No
No
Yes
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding the BES Cyber Asset definition under question 8.
Regarding the definition of Control Center (question 2), the IRC requests clarification of word

“facility”. Does this include (1) the control room where system operations personnel work; (2) the data center housing the cyber assets; (3) all of a multi-purpose building containing 1 and 2; or (4) all of the above?
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding the CIP Exceptional Circumstance definition under question 10. The IRC respectfully provides these additional comments. The IRC requests modification of the definition of CIP Senior Manager (question 3) to read, “A single senior management official with overall authority and responsibility for the implementation of and continuing adherence to the Responsible Entity’s NERC CIP program”. This is to not imply that it is required that this person “lead” the implementation and ensure involvement beyond initial implementation.
The IRC requests modification of the definition of Physical Access Control Systems (question 4) to replace “exclusive of” with “excluding”.
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding the Interactive Remote Access definition under question 12.
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) under question 13. The IRC respectfully provides these additional comments. The IRC requests modification of the definition of External Routable Connectivity to, “A bi-directional routable protocol connection that is used to access a Cyber Asset within an Electronic Security Perimeter from a Cyber Asset that is outside the Electronic Security Perimeter.”
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) under question 14.
Yes
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) under question 16.
Individual
Gregory Campoli
NYISO
No
Yes
Yes
Yes
Yes
No
No
• BES Cyber Asset definition from "it is directly connected to a Cyber Asset within an ESP" to "it is directly connected to a network, or to a Cyber Asset within an ESP"
• Intermediate device location seems too prescriptive as different technology combinations may allow the DMZ and device location to be different that defined.
• Electronic Access Point (“EAP”) A Cyber Asset interface on an Electronic Security Perimeter that allows externally routable bi-directional communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter or inbound communications to a Cyber Asset within the Electronic Security Perimeter.
• Physical Security Event is a suspicious event that is monitored prompting a Physical Security Investigation • Cyber Security Event is a suspicious event that is monitored prompting a Cyber Security Investigation • Physical Security Investigation is the process defined by the entity to investigation events that are identified to the Physical Security controls or impacts the operations of

the facility. • Cyber Security Investigation is the process defined by the entity to investigate events that are identified to the BES Cyber Assets, BES Cyber Assets, Protected Cyber Assets and that are suspicious or may impact the operation of the cyber asset. • Physical Security Incidents are the result of investigations or processes that identify the impact of the event to the Physical Security Perimeter, controls or facility. • Cyber Security Incidents are the results of the investigations or process that identify the impact of the event upon the BES Cyber Asset, BES Cyber System, or Protected Cyber Asset. • Reportable Physical Security Incident is a compromise or interruption to the Physical Security Perimeter, controls or facility. • The definition of Reportable Cyber Security uses the terms "compromised" and "disrupted" plus the phrase "reliability tasks of a functional entity" All three need their own definition/clarification.
No
• Concerned with the Version 3, to Version 4 to Version 5 implementation path and hope FERC and NERC will work to resolve the path forward to minimize implementation risk to the industry • Request clarification on the Disaster Recovery's "completion of the restoration activities" (top of the clean version's page 5). What event/action/etc signifies this completion?
• Section 5 for CIP-003-5 is the only place that explains how to read the bullets and numbers in the Measures. From the second paragraph of Section 5, "Measures provide examples of evidence to show documentation and implementation of the requirement. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence." Request clarification this bullets and numbers explanations applies to the Requirements and Applicability sections of each of CIP-002-5 - CIP-011-1. If this was the SDT's intent, then recommend this clarification be added to Section 5 of each of CIP-002-5 - CIP-011-1. • General comment – recommend that each Requirement's Part identify that Part's goal
Group
Tri-State G&T - Transmission
Tracy Sliman
Yes
Yes
No
Yes
Yes
Yes
Yes
In definition of CIP Senior Manager replace "CIP Standards" with "CIP-002 through CIP011". In definition of Control Center add 24/7 to the first sentence. "One or more facilities hosting operating personnel 24/7 that monitor and control the Bulk Electric System (BES) in real-time …"
Yes
Group
CenterPoint Energy
John Brockhan
No

No
No
No
No
Yes
No
CenterPoint Energy requests clarification on the term “adversely impact” and the point in time when the clock starts for the criteria of “within 15 minutes”. Additionally, the definition for BES Cyber Asset states that “Redundancy shall not be considered when determining availability.” CenterPoint Energy requests clarification on whether this concept has been reasoned for application in a substation environment, specifically in the instance of primary/backup relays and identical redundant systems.
CenterPoint Energy agrees with the comments submitted by EEI regarding a definition for Control Center.
CenterPoint Energy proposes that the definition of CIP Senior Manager is not needed as a glossary term, but is acceptable in the requirement description.
CenterPoint Energy recommends that the term “alert” be removed or replaced with “alarm” in the definition of Physical Access Control Systems.
CenterPoint Energy agrees with the comments submitted by NSRS regarding the definition of “Interactive Remote Access”.
CenterPoint Energy believes “was an attempt” is vague and seeks clarification on how such an attempt will be determined. An alternative would be to delete the phrases “or was an attempt to compromise” and “or was an attempt to disrupt”. CenterPoint Energy also agrees with the comments submitted by NSRS regarding revisions to the definition of “Reportable Cyber Security Incident” and replacement of the term “reliability tasks” with “reliability functions”.
No
CenterPoint Energy recommends a table format for the “Initial Performance of Certain Periodic Requirements”. Also CIP-010-5, Part 3.2 is listed with the “Within 12 calendar months” activities. According to the requirement, it should be performed “once every 36 calendar months”.
Individual
James Tucker
Deseret Power
No
No
No
Yes
Yes
Yes
Yes
Control Center – DESERET POWER is concerned that in this definition the mere presence of a SCADA HMI might be considered a Control Center by a CEA if it could possibly be used to control BES assets in real-time even if an entity does not use it that way. Some of the registered entities do not man these control centers 24/7 and are unable to perform real time control after hours, or any other time that other duties take them 15 minutes away from the computer. In some instances these entities might be registered as TOPs only because they own a limited and discrete 115 kV facility that no other entity was willing to register as a TOP for. Often times this 115 kV facility performs no reliability function. DESERET POWER suggests adding “24/7 to the first sentence of the Control Center definition

as shown in the underlined text: “One or more facilities hosting operating personnel 24/7 that monitor and control the Bulk Electric System (BES) in real-time …”
CIP Senior Manager – In this definition replace “CIP Standards” with CIP-002 through CIP-011. If this is not completed, this definition would apply to CIP-001 which still exists and is an unrelated standard. This revision will provide clarity to the limit of the definition.
Yes
Individual
Jennifer Wright
San Diego Gas & Electric
San Diego Gas & Electric (“SDG&E”) proposes the following changes to the definition of “Cyber Security Incident”: “A malicious act or suspicious event that: • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter, or, • Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or, • Is a violation or imminent threat of a violation of computer security policies, acceptable use policies, or standard security practices impacting or within covered Electronic Security Perimeters or Physical Security Perimeters."
A. Throughout the standards, the terms “data” and “information” are used interchangeably. The term “data” should be used when referring to a collection of facts in any form, and “information” should be used when referring to a message that has been received and understood. B. The CIP standards need to be more closely aligned with the comparable NIST or ISO standards. C. The CIP standards still hold the responsible entity completely accountable with no accountability to the vendors that supply and support the in scope systems. The standards should be made applicable to these third parties, specifically those third parties that are sole providers of products and or services that are needed to comply with NERC CIP standards. The standards also need to apply to organizations; public and private that have access to and or the ability to manage assets that are in-scope for NERC CIP. Past comments have alluded to the fact that utility companies have the ability to choose to engage certain third parties. While this may be the case for certain types of products and or services, this is not factual given stipulations by third parties to manage certain aspects of the grid and or products provided. Examples are turbine maintenance and Cal-ISO connectivity. In addition, Smart Grid will introduce new technologies for the automation of grid activities, whereby third parties and or union affiliates will be responsible for installing, maintaining and or troubleshooting grid technologies that have the potential to be in scope for NERC CIP. D. Comment Form B, Question 2: Although the wording of CIP-004-5, R2 appears to require role based awareness and training, the associated tables appear to apply requirements to systems, not to roles. SDG&E recommends applying awareness and training requirements solely to roles. E. Comment Form B, Question 14: Parts 1.4 and 1.6 of CIP-006-5 Table R1 require controls that monitor Physical Security Perimeters and Physical Access Control Systems twenty four hours a day, seven days a week “with 99.9% availability.” This 99.9% availability is an arbitrary criterion. Does the 99.9% apply per day, per week, per month, or per year?

99.9% equates to an allowable down time of 8.76 hours per year. Physical access control systems can experience momentary loss of connectivity between system servers and local controllers that may result in interruption of alarm monitoring for a few seconds or less. Will each of these momentary interruptions be a violation when they exceed 0.01% in one day/week/month/year? How is this criterion applied to multiple controllers? If 100 controllers have an interruption for one second, is the down time the same as if one controller has an interruption of one second? Part 1.5 of CIP-006-5 Table R1 requires an alarm or alert in response to detected “unauthorized circumvention” of a physical access control into a PSP. “Unauthorized circumvention” seems to imply hostile intent and successful penetration of the PSP access point. Is this the intent?
Group
Seattle City Light
Pawel Krupa
General Comments: SCL does not support the approach proposed in version 5 of the CIP Standards, either as to fundamentals or details. Fundamentally SCL believes the v5 approach is flawed and will introduce significant compliance burden without ensuring cyber security for the BES. Detailed concerns remain as provided previously (please refer to comments submitted by SCL on January 6, 2012). Although today's enforcable CIP Standards share many of the flaws of v5, SCL believes industry would be better served by developing maturity around the existing Standards while developing a new, different approach to cyber security that is based on the established practices and theory of the information technology industry.
Group
PacifiCorp
Sandra Shaffer
PacifiCorp supports the comments submitted by EEI.
Individual
Steve Alexanderson P.E.
Central Lincoln
Yes
No
Yes
Yes

Yes
Yes
Yes
We thank the SDT for removing the circularity and overreach of the prior definition. It occurs to us, however, that the mere presence of a SCADA HMI might be considered a Control Center by a CEA if it could possibly be used to control BES assets in real-time even if an entity does not use it that way. Many of the registered entities do not man these stations 24/7 and cannot perform real time control after hours or any other time that other duties take them 15 minutes away from the computer. In addition, these entities might be registered as TOPs only because they happen to own a piece of 115 kV equipment that no other entity was willing to register as an operator for, even if that device performs no reliability function. We suggest “One or more facilities hosting operating personnel 24/7 that monitor and control the Bulk Electric System (BES) in real-time …”
Yes
Individual
Russell A. Noble
Cowlitz County PUD
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Cowlitz agrees with the comments submitted by APPA. Cowlitz also adds that a Control Center which should be afforded any Medium or High impact assessment should also be manned at all times, i.e., 24/7. There exist small TOP entities whose existence is strictly due to the unwillingness of any neighboring entity to cover for their TO registration. Such TOP entities may only own a few 115 kV devices which have no operational reliability function other than to drop load, or break a transmission loop designed solely to improve local quality of service. Since there is no need to monitor the operational status of such transmission systems in real time, these small entities will only have personnel at the “controls” as needed. Therefore, Cowlitz suggests the definition be changed to include “One or more facilities hosting operating personnel 24/7 who monitor and control the BES in real-time.
Yes

Cowlitz agrees with the comments submitted by APPA.
Cowlitz agrees with the comments submitted by APPA.
Individual
Tony Kroskey
Brazos Electric Power Cooperative
No
No
No
Yes
No
Yes
Yes
We thank the SDT for improvements to the draft definitions, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
We thank the SDT for improvements to the draft definitions, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
We thank the SDT for improvements to the draft definitions, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
We thank the SDT for improvements to the draft definitions, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
We thank the SDT for improvements to the draft definitions, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
We thank the SDT for improvements to the draft definitions, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
We thank the SDT for improvements to the draft definitions, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
Yes
We thank the SDT for improvements to the implementation plan. Please see the formal comments of ACES Power Marketing.
Please see the formal comments of ACES Power Marketing.
Individual
Scott Harris
Kansas City Power & Light
No
No
Yes
Yes
No
Yes
Yes

Cyber Assets – The proposed definition uses the description “programmable electronic devices”. The CIP Standard is intended to prevent the compromise of the security awareness and security functions of cyber systems and components through malicious acts either by remote tampering or local tampering. The description of “programmable electronic devices” is too broad a term to use in this definition. There are many devices that could be considered programmable such as program logic controllers, devices that are configurable by firmware changes, and devices that are configurable by hardware switches. None of these devices have operating systems nor interconnectivity through routable protocol that can compromise their intended function. The proposed CIP Standards do not recognize the limits of these devices and subsequently impose unrealistic requirements of change control, account management, electronic user access records, etc. Considering the broad application in the proposed CIP Standards of this definition, this definition needs to be revised to the following: “Electronic devices that can execute code and use a routable protocol to receive or transmit information, including attached peripheral hardware and software installed on those devices.”
Subscribe to the comments submitted on behalf of EEI.
No other comments.
Dial-Up Provide a definition of “dial-up” for clarity in the standards. Proposed Definition: Dial-Up Connectivity – Connectivity to BES Cyber Assets (or associated Protected Cyber Assets) which is publically accessible using the Publically Switched Telephone Network (PSTN). Intermediate Device Modify the definition to allow for Intermediate Devices to terminate on an Electronic Access Point or to be external to the ESP. Rationale – This will ensure applicable Intermediate Devices are not ‘disqualified’ from operating as such should they have an interface which is an electronic access point into the ESP. Associated Electronic Access Control or Monitoring Systems – Applies to each Electronic Access Control or Monitoring System directly monitoring or negotiating access to applicable high impact BES Cyber Systems or medium impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems. Associated Physical Access Control Systems – Applies to each Physical Access Control System directly negotiating access to applicable high impact BES Cyber Systems or medium impact BES Cyber Systems with External Routable Connectivity.
No other comments.
No other comments.
No other comments.
No
Until the scope of the assets and components comes to rest, it is not possible to make a determination that the implementation plan has sufficient time to implement these requirements.
Zero-defect requirements: Many of the CIP standards and requirements involve actions that are repeated hundreds of times such as access reviews, personnel training, access removals, etc. In those instances, the Violation Severity Levels dictate a failure of a single instance is an absolute failure of the requirement and does not recognize the hundreds of successes. In some regards, the current Find, Fix, and Track settlement processes recognize these instances and manage them appropriately. However, the Standards would be greatly improved by incorporating an appropriate ratio of success to failure in the VSL’s thereby recognizing the real risk to the BES.
Individual
Martin Bauer
US Bureau of Reclamation
No
Yes
Yes
Yes
Yes
Yes
Yes

BES Cyber assets for a Blackstart generator or resource smaller than 75MVA shoud not be considered BES Cyber Assets. This may reduce the risk of entities with smaller BES resources removing those resources from restoration plan(s).
Individual
Richard Vine
California Independent System Operator
No
No
No
No
No
No
BES Cyber Asset – Remove the 15 minute criteria as it is believed that it will lower the security of assets by removing them from qualifications. Suggest a table based on functional criteria.
No comments
1. BES Cyber System Information – define what it is meant by “or pose a security threat”. Suggest removing this wording as this is subject to interpretation. 2. CIP Senior Manager – the definition should include the operation and maintenance of the requirements (ongoing compliance). It appears that after the requirements are implemented, according to the implementation plan, that there is no longer a need for a “CIP Senior Manager”. This appears to contradict CIP-003.
Physical Access Control Systems - Replace the word “exclusive” with “excluding”
For Interactive Remote Access reword “…2) Cyber Assets used or owned by employees, and” to “…2) Cyber Assets used by employees”. Employee owned devices should not be allowed to be used for remote access to BES Cyber Assets.
1. Provide examples in the definition for Electronic Access Point and Electronic Security Perimeter. 2. External Routable Connectivity – This should also pertain to Protected Cyber Asset. BES Cyber System is a group therefore the term should be replaced with BES Cyber Asset. The definition should be reword to “A bi-directional routable protocol connection that is ….”. A suggestion for re-writing the definition may look something like “A bi-directional routable protocol connection that is used to access a BES Cyber Asset or Protected Cyber Asset from a Cyber Asset that is outside the associated Electronic Security Perimeter.” 3. Protected Cyber Asset – suggest removing the parenthesis but keep the wording as a separate sentence.
Cyber Security Incident – remove the words “or suspicious event”. Suspicious is too vague and subject to interpretation. Suggest the definition be changed to: “A malicious act that: • Compromises, or was an attempt to compromise a BES Cyber System • Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.”
Yes
None
None
Group

Hydro One
Sasa Maljukan
No
Yes
Yes
Yes
Yes
No
No
for clarity, suggest changing the BES Cyber Asset definition from "it is directly connected to a Cyber Asset within an ESP" to "it is directly connected to a network, or to a Cyber Asset within an ESP"
Request clarification on the definition of EAP, must it be routable protocol on both sides?
The definition of Reportable Cyber Security uses the terms "compromised" and "disrupted" plus the phrase "reliability tasks of a functional entity" All three need their own definition/clarification.
No
Although the proposed version 5 implementation plan states that “Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan,” there are concerns that need clarification. The concerns refer to the transition from the currently effective version 3, through version 4 and finally to version 5. Given that (a) the version 4 standards and associated implementation plan were recently approved by FERC; (b) the proposed version 5 implementation plan contains a minimum 24-month period for enforcement means that there will be a period of time during which version 4 would be effective; and (c) when version 4 becomes effective there will be newly identified CAs that will have to be made compliant. In order to comply with version 4 requirements, entities will be need to allocate funding and resources to perform work necessary to become compliant at newly identified facilities. Much of this work must be performed in anticipation of the enforcement date. Once version 5 becomes effective, application of the proposed categorization of BES Cyber Systems may very well result in much of the work done for version 4 compliance being in the end unnecessary.
Request clarification on the Disaster Recovery's "completion of the restoration activities" (top of the clean version's page 5). What event/action/etc signifies this completion?
Section 5 for CIP-003-5 is the only place that explains how to read the bullets and numbers in the Measures. From the second paragraph of Section 5, "Measures provide examples of evidence to show documentationand implementation of the requirement. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence." Request clarification this bullets and numbers explanations applies to the Requirements and Applicability sections of each of CIP-002-5 - CIP-011-1. If this was the SDT's intent, then recommend this clarification be added to Section 5 of each of CIP-002-5 - CIP-011-1. General comment – recommend that each Requirement’s Part identify that Part’s goal

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards
Comment Form A
CIP-002 and CIP-003 Questions

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Summary Consideration, Explanation, and Common Responses to Global Changes and to Issues and Comments Frequently Repeated

In response to draft 2 of the Version 5 CIP Cyber Security Standards, the Standards Drafting Team (SDT) received significant input from a wide variety of perspectives. All of that input greatly helped the team to refine the standards and associated documents, and the set of standards now posted reflects all of that combined input. There were several varied perspectives in the comments, and the SDT attempted to address each comment as responsively as possible.

There were several changes that reflected careful consideration of several comments that affected the standards on a global basis, whether in format, style, or substance. In addition, there were several comments the SDT considered that were repeated across multiple questions, sometimes submitted by the same entity to each or to many of the questions. Rather than explaining in detail the global changes in response to each question, and rather than responding separately to the frequently repeated comments in each question, the SDT addresses those global issues and general comments in this section.

Many comments related to specific language suggestions or to specific compliance concerns. The SDT has responded to those comments in each of the individual questions summaries that follow this section. Those comments were thorough and varied, and they reflected diverse perspectives and topics. The SDT expended considerable work in reviewing, discussing, and responding to all of these inputs, and it believes that the major issues have been addressed responsively in this posted draft CIP Version 5 package. As a result, the changes have been significant and substantive in all of the draft CIP Version 5 standards and Implementation Plan. The SDT believes this posting package addresses all of the substantive issues received from the previous two iterations of comments and various other inputs.

Change in labeling of the applicability columns in the tables to "Applicable Systems"
After posting draft 1 of CIP Version 5, commenters expressed concern that merely using "Applicability" as the title of the applicability columns in the Requirement tables (in CIP-004 through CIP-011) created confusion with the actual "Applicability" section of the standards. In response, for draft 2, the SDT added specificity and labeled those columns "Applicable BES Cyber Systems and associated Cyber Assets." In response to that change in draft 2, commenters expressed concern with the length and suggested that the SDT label the applicability column "Applicability." Therefore, the SDT is proposing to label these columns, "Applicable Systems." This should eliminate any confusion with the applicability section of the standards themselves while also providing appropriate brevity.
Handling of "associated" Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCA) (and the associated change to their use in the "Applicable Systems" column of the requirement tables)
In previous drafts, in the applicability columns (now "applicable systems" columns), the standards used a term "Associated Protected Cyber Assets," "Associated Electronic Access Control or Monitoring

Systems," and "Associated Physical Access Control Systems" where it intended that the requirement part be applicable to not only the applicable high or medium impact BES Cyber Systems, but also to other Cyber Assets or systems, as specified, associated with those BES Cyber Systems. Also, for Protected Cyber Assets, the requirement applied to Cyber Assets or lower impact BES Cyber Systems that were in the same ESP as the applicable BES Cyber System. There was confusion the precise meaning or application of the "associated" systems, and the SDT has made the link more explicit in this draft. One of the fundamental concepts of CIP Version 5 is that it is adopting a systems approach, and those "associated" systems should be more closely connected with the applicable subject of the requirement. Therefore the SDT has moved the associated systems to follow immediately after the subject of the requirement and clarified that they are "associated with" that specify type of BES Cyber System or other applicable system. Mitigation for the associated systems may be accomplished through other applicable systems.

High Watermarking Concept

The CIP Version 5 Standards use a term "Protected Cyber Assets" to refer to those Cyber Assets that are within the ESP, which in previous versions of the standards were "other (non-critical) Cyber Assets within the ESP" (see CIP-005-4, Requirement R1, Part 1.4, and CIP-007-4). Additionally, in Version 5, a Protected Cyber Asset can also be a BES Cyber System of a lower impact classification if it is within the same ESP as a higher impact BES Cyber System.

For example, CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The standard does not require segmenting of BES Cyber Systems by impact classification, and many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and systems within the ESP will be elevated to the level of the highest impact BES Cyber System present in

the ESP. The standard accomplishes this by defining all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

Measures: "but not limited to"

Many commenters expressed concern about or questioned the meaning of the use of "but not limited to" in the previous draft and asked for it to be removed from the measures. The concern as the SDT understood it was that "but not limited to" could be used to request evidence beyond that which is specified in the measure even if the entity has otherwise provided what the measure describes. With respect to "but not limited to," the SDT specifically inserted that phrase to assist the Responsible Entity, particularly in light of technologies that may change. It is not intended to be used as a mechanism to request additional evidence beyond that which is required to demonstrate compliance. The SDT is concerned that removing "but not limited to" opens the same question (albeit in slightly different context) as the CIP Interpretation Drafting Team just answered with respect to the interpretation of CIP-002 (versions 1 through 4) for Duke Energy (NERC Standards Development Project 2010-INT-05). Namely, are the measures listed exhaustive/prescriptive or are they illustrative? By including a qualifier such as "but not limited to," as is common in statutory drafting and in other legal contexts, the SDT intends to signal that the measures are not exhaustive. It provides flexibility to the Responsible Entity on what is acceptable. For example and for purposes of illustration, if one said "evidence may include an orange, a lime, or a lemon," one could expect that perhaps only an orange, a lime, or a lemon would be appropriate. However, if one said, "evidence may include, but is not limited to, an orange, a lime, or a lemon," one could just as reliably expect that an orange, a lime, or a lemon would be appropriate, but it would also be reasonable that something not explicitly enumerated by the list, but similar in nature to items on the list, such as a tangerine, may also be acceptable. Importantly, that is not the same as additionally requiring a tangerine even though one already has an orange; however, that is the concern manifested in the comments. To address the commenters' concerns, however, the SDT has made a slight change in support of signaling in all measures that they are examples and that the list of examples is not exhaustive. The SDT believes that it is providing sufficient flexibility in this manner—and for the Responsible Entities' benefit—in clarifying that measures are not prescriptive lists while also attempting to allay fears that "but not limited to" will be used in a manner that expands the requirement. Rather than stating "Evidence may include, but is not limited to, . . ." the SDT has added the "example" concept to precede "evidence" (e.g., "**An example of** evidence may include, but is not limited to, . . ." or "**Examples of** evidence may include, but are not limited to, . . .").

Movement to focus on correcting deficiencies in certain requirements:
In response to several comments, the SDT has incorporated within CIP Version 5 a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. Note that, where used, the addition of language modifies "implement"; it does not itself require or specify internal controls, though it certainly enables their use for those entities that have adopted an internal controls or compliance management approach. Where used, the requirements incorporate the forward-looking language into the main requirement, which ties in with CIP Version 5's use of accompanying tables. It is presented in those requirements as follows:

> "Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** one or more documented processes (or program, etc., as specified by the requirement) that collectively include each of the applicable items in [the referenced table]."

The SDT also considered several alternatives and additions to this language. For example, some alternatives proposed modifying "process" (or program, etc.), while others suggested to add language specifying certain things that are not violations in addition to the requirement language. Many of the ideas or suggestions presented concepts that the team agrees with, but they are more appropriate for other aspects of monitoring compliance with the standards, not for inclusion within the standards themselves. Language indicating what is not a violation is more appropriate for compliance tools such as the RSAW. The SDT also notes that the VSLs will reflect this approach where the approach is used, and the SDT is actively working with NERC Compliance Operations to prepare the RSAWs for the CIP Version 5 standards. Furthermore, the SDT expects continued participation by industry in providing input into the RSAW development following approval of the standards, and the SDT notes that a draft RSAW for part of CIP-006-5 is posted for comment and for illustrative purposes.

The SDT is charged with writing straightforward requirements stating the desired behavior that will maximize reliability of the BES. The CIP requirements are written to require documented processes that must address the elements in the tables that accompany the requirements. These tables therefore set the parameters for the processes. There are no issues with documenting the processes – the entity must have the processes and they must have the parameters as outlined in the requirement tables.

The compliance concerns, especially those related to zero tolerance for deficiencies, is not related to the documenting of the processes, but in the implementation of the processes. The process should have numerous 'bright line' parameters that outline the goal the industry striving towards. A concern applies when implementing the processes in a world of tens of thousands of people and hundreds of

thousands of Cyber Assets. In certain cases, absolute perfection forever is not reasonable, even if it is desirable.

In light of the direction toward a risk-based approach to compliance monitoring by NERC, The CIP SDT had an opportunity to do to address this issue in certain requirements within the standards themselves. As described above, the SDT included a phrase to modify the verb 'implement' in several (but not all) of the requirements in CIP V5. Entities are to have the processes; the processes must meet the requirements in the tables; and the entities shall implement those processes in a manner that identifies, assesses, and corrects deficiencies.
The emphasis of the self-correcting language is on the implementation of the processes. The processes themselves cannot miss required parts or parameters as outlined in the tables.

Implementation Plan proposal to extend Version 3 until Version 5 remains unchanged in this draft
In light of the order approving the CIP Version 4 standards (FERC Order No. 761), several commenters asked about the drafting team's proposal in the implementation plan to extend Version 3 until the effective date of Version 5. The SDT's proposal, if approved—and its intent for Version 5 to supersede Version 4 and to extend the effectiveness of Version 3 until Version 5 goes into effect—remains unchanged.
In the implementation plan for the CIP Version 5 standards, the SDT has previously proposed to extend Version 3 until the effective date of Version 5. In doing so, the effective date proposes that Version 4 will be superseded by Version 5 and not go into effect. Even though Version 4 has been approved by order, the SDT always contemplated such approval during the development of the implementation plan language. That order does not change the SDT's proposal. The expectation that there would be an order in early to mid 2012 is why the SDT included language in the implementation plan's effective date to specify that the extension of Version 3 until Version 5, and that Version 4 would not go into effect, would occur "notwithstanding any order to the contrary." There is no change in the SDT's intent and proposal to extend Version 3 until Version 5, and for Version 5 to supersede Version 4, notwithstanding the recent order approving Version 4. The SDT also understands, as is the case for any standards proposal by the industry, that the proposal is subject to approval by regulatory authorities.

Stakeholders will notice that within the individual standards for CIP Version 5, the effective dates have been modified so that they are specific to the particular standard. In doing so, the reference to extending Version 3 and superseding Version 4 has been removed, as the Implementation Plan is the appropriate place for that language (where it remains, as described above). Thus, while there is no change to the SDT's proposal, the individual, standard-by-standard effective dates have been modified to comport with the style and form of other NERC Reliability Standards.

Annual v. 15 calendar months
Several commenters expressed dissatisfaction with the standards' use of the phrase ". . . at least once every calendar year, but not to exceed 15 calendar months . . ." for describing the required frequency

of performance on some requirements. Some entities expressed a desire to simply use "annual," while others suggested changing the "but" to an "or." The SDT has discussed alternative approaches and is using the term ". . . at least once every 15 months . . ." to provide reasonable flexibility to Responsible Entities while meeting the intent of the requirements. As explained in the global comment section of the response to comments for draft 2, simply using "once per calendar year" creates a potential for bi-annual bookending that the SDT does not intend. Similarly, the SDT understands that the use of both "calendar year" and "15 calendar months" was unnecessarily complicated. The SDT acknowledges that there is a CAN that addresses "annual," but that applies where the standard does not make clear what it means in its use of the term. In CIP Version 5, there is an opportunity and an obligation to unambiguously reference the periodic time parameter. Furthermore, one of the objectives of the SDT in Version 5 is to consider applicable CANs and use language that would no longer require a CAN to clarify an audit interpretation. Instead, the SDT used specific language to clarify a time parameter that approximates one year in time while also accounting for operational realities that make a 15 month parameter more reasonable. The term "annual" is no longer used in these CIP standards for periodic requirements, and, therefore, the CAN on the word "annual" can no longer apply.

TFE v. Per Cyber Asset Capability

Historically, phrases such as "where/when technically feasible" have been considered trigger language for requirements necessitating a technical feasibility exception ("TFE") in instances where a device could not meet the required parameter. The SDT has spent considerable time reviewing each use of TFE language in CIP Version 5 where it is necessary.

The SDT has also determined that there are some requirement parts that should not require a TFE, as certain parameters are not essential themselves, but should apply if a device is capable of the parameter. This is distinct from the reasoning for requirements with TFE language. In the latter requirements, a certain performance or parameter is required, regardless of technology, device, etc. By using "per (device/system) capability," the SDT does not intend that the specific parameter or performance is required regardless of capability, but only applicable on devices that have that capability. For example, proposed CIP-007-5, Requirement R4, Part 4.1 requires "Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents . . ." Here, the SDT does not intend to require event logging. However, if a Responsible Entity is using a device that can log events, it is required to enable event logging to the extent the device is capable.
The phrase "where technically feasible" indicates that the standard requires strict compliance without a TFE. As mentioned above, the drafting team does not intend for some requirements to be TFE-triggering. The underlying rationale for a TFE is that there is legacy equipment in place that is not readily compatible with a modern environment where cyber security issues are a concern.[2] Under such circumstances, the responsible entity must file a TFE that demonstrates strict compliance with an

[2] Order Approving Technical Feasibility Exception Procedures and Ordering Compliance Filing, Paragraph 3

applicable requirement is not technically possible and that there is an alternative course of action that will protect the reliability of the Bulk-Power System to an equal or greater degree than strict compliance.[3]

While a TFE requires an entity to show why strict compliance with an applicable requirement is not technically possible, "per device capability" clarifies that the requirement is only applicable to the devices for which compliance with a particular requirement is possible in the first instance. This provides reasonable flexibility to the industry while also retaining the TFE concept where necessary. Thus, the "per device capability" alternative reduces the need for TFEs and will be less onerous on entities. The SDT does not intend to eliminate TFEs altogether, but proposes to use the "per device capability" as an alternative that is effective in protecting the reliability of the Bulk-Power System.

VSLs

In previous drafts of the Version 5 CIP Cyber Security Standards, VSLs were posted concurrent with each standard. For this posting, the VSLs are presented in one document. They will continue to be prepared for posting for non-binding poll during the recirculation ballot. The VSLs should not be a basis for a ballot determination, and the SDT will continue to refine them as necessary.

Applicability Section of the standards (Introduction - Section 4 – Applicability)

There were several comments about the Applicability section of the standards in various comments related to specific standards. The SDT has reviewed those suggestions and made several changes to the applicability sections of each standard.

Several commenters stated that in part 4.2 of section 4, the criteria for qualified Distribution Providers and Load Serving Entities for UVLS/UFLS systems remain unclear. Specifically, the language was not clear on whether the 300 MW of load referred to the DPs and LSEs' share or to the total load shed. In addition, they also noted that the language for Transmission Protection systems is unclear and needs clarification to more precisely describe the protection systems that are in scope. They also suggested that these should be moved to Low Impact because there is no justification for small entities to be subjected to the requirements for Low and Medium entities. The SDT has proposed modified language to clarify the qualifications for UFLS and UVLS systems that specifies that they are those UFLS or UVLS systems that are part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard and that perform automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. With regard to the impact classification, the SDT believes that because of the function that UVLS and UFLS systems play in last ditch efforts to stabilize the BES, the 300 MW threshold provides a measure of impact that justifies the classification as medium impact systems: lower impact systems have already been removed from the scope and are not subject to these standards.

[3] Id, Paragraphs 5 and 8

Many references in the applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

Several comments indicated that LSEs should not be included in section 4 since the NERC Functional Model does not include any tasks related to the implementation and operation of load shedding systems. The SDT reviewed the LSEs tasks in the NERC Functional Model and has removed LSEs from the applicability of the CIP standards.

Several commenters suggested that the following language be added to the end of the criterion for Protection Systems: "and where the Protection System is connected to a supervisory control system providing remote operation capability." The SDT has reviewed the proposed addition to section 4.2.2 for Protection Systems and does not believe that the additional language to restrict the scope to only those Protection Systems that are remotely operated is intended or justified in the scope of section 4.2.2. The SDT notes that the proposed addition makes the assumption that all cyber vulnerabilities are based on remote operation capability. This would provide an incomplete mitigation for cyber threats that do not rely on remote operation for execution.

Several commenters stated that the inclusion of the glossary term "Systems" does not apply to DPs as used in section 4.2.2. One comment also pointed out that this is true in many other places where the term is used, while others' comments pointed out inconsistencies in the use of the term. The SDT notes that the terms Facilities, systems and equipment is always used in combination in the context of this application. The SDT has considered the intent of the terms in its uses and agrees that the glossary term "Systems" does not reflect the intent, and the SDT has made those changes where appropriate. In addition, the SDT believes that the issue is relieved with the changes made to refer to "assets" when referring to a group of Facilities, systems or equipment at a given location.

One comment stated that the statement at the beginning of the guideline and technical basis section that refers to applicability to DPs that refer to EOP-005 should be deleted since section 4.2.2 scopes more than EOP-005. In response, the SDT notes that the paragraph also includes reference to the registration criteria, in addition to EOP-005. The SDT believes the reference is appropriate.

One comment noted that in section 4, part 4.2.2, all single points of failure in the cranking paths should be protected and that where the Blackstart Resource is outside of the Responsible Entity's ownership, that the part of the cranking path that is the injection point to the cranking path to the unit to be

started should be specified. The SDT notes that Section 4.2.2 is not the criterion for determining the protection of the cranking path, but rather defines which part of a DPs equipment is in scope.

One comment suggested additional qualification in section 4 to ensure that the exemption section covers all facilities covered under a cyber security plan under the Nuclear Regulatory Commission (NRC) regulations. The SDT agrees with the clarification and has included the suggestion in the language in section 4 that covers nuclear facilities. The language has been added to section 4.2.4.3 to read: "In nuclear plants, the Systems, structures, and components that are regulated by the NRC under a cyber security plan pursuant to 10 C.F.R. Section 73.54."

One comment discussed the use of the phrase "required by a NERC standard" in section 4 and instances of affected Facilities, systems and equipment where there is no requirement to implement them by a NERC standard. The SDT agrees with the discussion and has made modifications to the language to more accurately reflect the intent.

One comment stated that section 4.2.4.2 attempts to define exemptions for communication links, but fails to include the exclusion of end points to those circuits (see CIP-005/R1.3). The SDT notes that end-points of circuits that are access points are included by the definition of Electronic Access Points (i.e. they are not "between" ESPs).

Reason for CIP Version 5

Some commenters inquired in their comments why CIP Version 5 was necessary, or they expressed a preference to continue under existing versions of the CIP Standards. To facilitate understanding of the reasons for Version 5 as part of the obligation to address the remaining directives in FERC Order No. 706, the SDT offers the following explanation and review of the previous versions of the NERC CIP Reliability Standards.

The NERC Board of Trustees adopted the first version of the CIP Reliability Standards on May 2, 2006. On August 28, 2006, NERC submitted to FERC for approval the Version 1 CIP Reliability Standards. On January 18, 2008, FERC issued its Order No. 706. In this order, FERC approved the Version 1 CIP Reliability Standards and issued more than 100 directives to NERC that included modifying the standards. An SDT began a phased-in approach to respond to the directives in FERC Order No. 706. As part of that phased-in approach, the SDT addressed the directives in the order that it could respond to quickly, and it developed a plan to address the remaining directives.

Version 2 of the CIP Reliability Standards was adopted by the NERC Board of Trustees on May 6, 2009. On May 22, 2009, NERC submitted to FERC for approval the Version 2 CIP Reliability Standards. On September 30, 2009 FERC issued its Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing. In this Order FERC approved the Version 2 CIP Reliability Standards and issued four additional directives to NERC that included modifying the

standards, with a required response in 90 days. At that time the SDT had to abandon it plan for addressing the outstanding directives in Order No. 706 and had to immediately address the newly issued directives.

Version 3 of the CIP Reliability Standards was adopted by the NERC Board of Trustees on December 16, 2009. On December 29, 2009, NERC submitted to FERC for approval the Version 3 CIP Reliability Standards. On March 31, 2010 FERC issued its Order on Compliance. In this Order FERC approved the Version 3 CIP Reliability Standards.

Version 4 of the CIP Reliability Standards (CIP-002-4 through CIP-009-4) was developed as an interim step to address the more immediate concerns from FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period. The Commission approved Version 4 on April 18, 2012.

Work has continued on further improvements to the standards, including responses to the remaining Commission directives from FERC Order No. 706, and it is these further enhanced standards that will be submitted to the Commission as Version 5. The next version of the CIP Reliability Standards will build on the Version 4 standards' establishment of uniform criteria for the identification of Critical Assets.

Version 5 of the CIP Reliability Standards provides a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

The changes in Version 5 also present many strategic advantages. Chiefly, a significant deliverable is to close out FERC Order No. 706. More importantly, Version 5 aligns to essential reliability functions and provides significant flexibility to entities in adapting requirements to individual operations.

Version 5 represents a systems-based approach to standards, which provides an opportunity to implement solutions and tailor security based on function, connectivity, risk, and impact. That flexibility represents a significant transition from the "in or out" demarcation for applying requirements in Versions 1 through 4 of the standards, as the drafting team has been able to structure Version 5 in a way that more finely tunes the applicability of each requirement based on connectivity, impact, and other characteristics.

Version 5 is also an experience-based set of standards. It is the first opportunity for the industry to evaluate, consider and incorporate lessons learned from implementation and audit of Versions 1 through 3, and the requirements aim to provide clearer emphasis on the required results. Collectively, the Version 5 standards support continued improvement in support of protecting against compromises that could lead to misoperation or instability in the Bulk Electric System.

NERC Quality Review

In addition to the changes that were made in response to comments, the SDT also submitted the set of standards to NERC for a quality review (QR). In response to the QR, the SDT made several changes for clarity, most of which related to style and form, grammar, word choice, etc.

The Applicability section was modified in response to QR to add "Interchange Authority" to the list of functional entities. The NERC Functional Model lists "Interchange Coordinator" while the registration criteria list "Interchange Authority," and they are not yet synchronized. Until that occurs, the SDT specifies that the standards apply to "Interchange Coordinator or Interchange Authority."
The SDT removed CIP-004-5, Requirement R4, Part R4.2. In previous drafts of the CIP standards (which was Requirement R6), the standard required designation of "one or more individuals" to authorize access, followed by a second requirement part for that individual to authorize based on need. The SDT has determined that the designation of one or more individuals is administrative in nature and is something that should be addressed by the Responsible Entity's plan, not by a requirement part. The performance required is now addressed through one requirement part.

The SDT also removed CIP-006, Requirement R3, Part R3.2, which required that Responsible Entities document outages for physical access control, logging, and alerting systems and retain the outage records for at least 12 calendar months. This requirement was a documentation requirement, and the SDT, in adding the modifying language to "identify, assess, and correct deficiencies" to Requirement R1, determined that the documentation requirement to log outages was not necessary.

Index to Questions, Comments, and Responses

Summary Consideration, Explanation, and Common Responses to Global Changes and to Issues and Comments Frequently Repeated 2

Questions with Summaries Included: 26

QUESTION A3 – CIP-002-5: 26

QUESTION A10 – CIP-003-5: 40

Questions with Votes Only: 44

1. Requirement R1 of draft CIP-002-5 requires the identification of high and medium impact BES Cyber Systems as described in Attachment 1. Further, it requires a Responsible Entity to review (and update as needed), the required identification within 60 calendar days of when a change to BES Elements or Facilities is placed into operation, which is planned to be in service for more than 6 calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category. Do you agree with the proposed Requirement R1? 44

2. Requirement R2 of draft CIP-002-5 states, "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once each calendar year, not to exceed 15 calendar months between approvals, even if it has no identified items in Requirement R1, Parts 1.1, 1.2, or 1.3." Do you agree with the proposed Requirement R2? 52

4. CIP-003-5 R1 states "Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall implement one or more documented cyber security policies that address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R1? 61

5. CIP-003-5 R2 states "Each Responsible Entity for its BES Cyber Systems not identified as high impact or medium impact shall implement one or more documented cyber security policies to address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2? 69

6. CIP-003-5 R3 states "Each Responsible Entity shall identify a CIP Senior Manager by name." Do you agree with the proposed Requirement R3? 77

7. CIP-003-5 R4 states "Each Responsible Entity shall review and obtain CIP Senior Manager approval for cyber security policies identified in Requirements R1 and R2, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals." Do you agree with the proposed Requirement R4? 85

8. CIP-003-5 R5 states "Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate and the date of the delegation, and approved by the CIP Senior Manager." Do you agree with the proposed Requirement R5? 93

9. CIP-003-5 R6 states "Each Responsible Entity shall document any changes to the CIP Senior Manager or any delegations within thirty calendar days of the change. Delegation changes do not need to be reinstated with a change to the delegator." Do you agree with the proposed Requirement R5? 101

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Bruce Metruck	New York Power Authority	NPCC	6
12.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
13.	Robert Pellegrini	The United Illuminating Company	NPCC	1
14.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
15.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
16.	Brian Robinson	Utility Services	NPCC	8
17.	Michael Jones	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Don Weaver	New Brunswick System Operator	NPCC	2
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3
24.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5

2.	Group	Annabelle Lee	NESCOR/NESCO									

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3.	Group	Jason Marshall	ACES Power Marketing					X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Tim Soles	Occidental Power Services, Inc.	ERCOT 3										
4.	Andy Gallo	Austin Energy	ERCOT 1										
5.	Andy Gallo	Austin Energy	ERCOT 3										
6.	Andy Gallo	Austin Energy	ERCOT 4										
7.	Andy Gallo	Austin Energy	ERCOT 5										
8.	Andy Gallo	Austin Energy	ERCOT 6										
8.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8. Annie Terracciano	Northern Lights Inc.	WECC 3										
9. Aleka Scott	PNGC	WECC 4										
10. Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11. Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12. Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13. Margaret Ryan	PNGC	WECC 8										
12. Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13. Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14. Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3. M & A Electric Power Cooperative			SERC 1, 3										
4. Northeast Missouri Electric Power Cooperative			SERC 1, 3										
5. N.W. Electric Power Cooperative, Inc.			SERC 1, 3										
6. Sho-Me Power Electric Cooperative			SERC 1, 3										
15.	Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X						
Additional Member		Additional Organization	Region Segment Selection										
1. Oglethorpe Power Corporation			SERC 5										
2. Georgia Transmission Corporation			SERC 1										
16.	Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X
Additional Member		Additional Organization	Region Segment Selection										
1. MAHMOOD SAFI		OPPD	MRO 1, 3, 5, 6										
2. CHUCK LAWERENCE		ATC	MRO 1										
3. TOM WEBB		WPS	MRO 3, 4, 5, 6										
4. JODI JENSON		WAPA	MRO 1, 6										
5. KEN GOLDSMITH		ALTW	MRO 4										
6. DAVE RUDOLPH		BEPC	MRO 1, 3, 5, 6										
7. JOE DEPOORTER		MGE	MRO 3, 4, 5, 6										
8. SCOTT NICKELS		RPU	MRO 4										
9. TERRY HARBOUR		MEC	MRO 1, 3, 5, 6										
10. MARIE KNOX		MISO	MRO 2										
11. LEE KITTELSON		OTP	MRO 1, 3, 4, 5										
12. SCOTT BOS		MPW	MRO 6, 1, 3, 5										
13. TONY EDDLEMAN		NPPD	MRO 1, 3, 5										
14. THERESA ALLARD		MPC	MRO 1, 3, 5, 6										
17.	Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing													
18.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				
Additional Member		Additional Organization	Region Segment Selection										
1. Timothy Beyrle		City of New Smyrna Beach	FRCC 4										
2. James Howard		Lakeland Electric	FRCC 3										

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. Greg Woessner	Kissimmee Utility Authority	FRCC 3										
4. Lynne Mila	City of Clewiston	FRCC 3										
5. Joe Stonecipher	Beaches Energy Services	FRCC 1										
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC 4										
7. Randy Hahn	Ocala Utility Services	FRCC 3										
19. Group	Joseph DePoorter	Madison Gas and Electric Company			X	X	X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Darl Shimko	MGE	MRO 3										
2. Joseph DePoorter	MGE	MRO 4										
3. Steve Schultz	MGE	MRO 5										
4. Jeff Keebler	MGE	MRO 6										
20. Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							
Additional Member	Additional Organization	Region Segment Selection										
1. Mark Jones	Pepco	RFC 1										
21. Group	Rick Terrill	Luminant					X					
Additional Member	Additional Organization	Region Segment Selection										
1. Mike Laney	Luminant Generation Company LLC	ERCOT 5										
2. Tim Soles	Occidental Power Services, Inc.	ERCOT 6										
3. Tim Soles	Occidental Power Services, Inc.	ERCOT 3										
4. Andy Gallo	Austin Energy	ERCOT 1										
5. Andy Gallo	Austin Energy	ERCOT 3										
6. Andy Gallo	Austin Energy	ERCOT 4										
7. Andy Gallo	Austin Energy	ERCOT 5										
8. Andy Gallo	Austin Energy	ERCOT 6										
9. Brenda Hampton	Luminant Energy Company LLC											
22. Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Kevin Smith	BANC	WECC 1										
23. Group	Scott Brame	NCEMC	X				X					
Additional Member	Additional Organization	Region Segment Selection										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Rayburn Country Electric Cooperative			SPP										
2. Empire District Electric			SPP	1									
3. City Utilities of Springfield			SPP	4									
4. Westar Energy			SPP	1, 3, 5, 6									
5. Cleco Power			SPP	1, 3, 5, 6									
25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Pawel Krupa			WECC	1									
2. Dana Wheelock			WECC	3									
3. Hao Li			WECC	4									
27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Denise Lietz		Puget Sound Energy	WECC	1									
2. Erin Apperson		Puget Sound Energy	WECC	3									
28.	Group	Michael Mertz	PNM Resources	X		X							
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Laurie Williams		Public Service Co. of New Mexico	WECC	1									
2. Michael Mertz		Public Service Co. of New Mexico	WECC	3									
29.	Group	Sasa Maljukan	Hydro One	X									
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. David Kiguel		Hydro One	NPCC	1									
30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION A3 – CIP-002-5:

If you disagree with the changes made to CIP-002-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to attachment 1 and provided clarity to the requirements and associated rationales and measures. The explanations below describe the modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity in language.

Introduction - Section 4 – Applicability

There were several comments on this section in response to question A3, but the issues and responses relate generally to all of the standards. The discussion and response to comments on this section is provided earlier in this document in the Summary Consideration, Explanation, and Common Responses to Global Changes and to Issues and Comments Frequently Repeated section.

Requirement R1

Substantial changes were made to both the structure and the approach in Requirement R1: while the end result is a categorized list of high and medium impact BES Cyber Systems, there were many changes made to address concerns related to Low Impact assets and an asset based approach to deriving BES Cyber Systems. Many comments suggested a more prescriptive approach to the methodology used to arrive at the objective lists, including suggestions to add a flow-chart to the requirement: the SDT made a number of changes to address the "what" instead of the "how", and added substantive qualifications to better define the assets affected.

In particular, several commenters stated that the requirement to review and update the categorization on every change to the BES was an onerous burden in a company with a large number of constantly changing BES Facility configuration. The SDT has reviewed comments and is persuaded by the arguments presented. The SDT also considers that an annual review and update for BES Facilities, given the long term implementation of BES Facility changes, together with the requirements for BES Cyber Systems change control, provide a framework that provides the controls necessary.

Several commenters stated that the requirements for identification in Requirement R1 of CIP-002-5 be modified to require reference to “BES Sites” rather than Facilities, systems and equipment. One comment also suggested that inventories for Low Impact would allow requirements for low impact to be at the site level. Many comments suggested a Facilities impact-based approach to the derivation of the impact of BES Cyber Systems. The SDT has considered the suggestion and made modifications to the current CIP-002-5 requirements to incorporate the concepts using language already used in the criteria and Version 4 approved standards. While the terms Facilities, systems and equipment are precisely the same terms used in the definition of Critical Assets in prior versions, the SDT has made modifications to the proposed language to use the term “assets”, a term familiar to the industry in compliance activities for prior versions.

In response to numerous comments on the issue of asset-based derivation of cyber system impact, the SDT made substantive changes to Requirement R1s language and structure to include this approach. While Requirement R1 is ultimately intended to result in categorized BES Cyber Systems for the application of cyber security requirements, the SDT has made changes to the language and contents of Requirement R1 as well as the criteria in attachment 1 in consideration of comments received.

Several commenters commented on the use of the capitalized term Bulk Power in the rationale for Requirement R1. The paragraph has been deleted and the term is no longer used in the rationale.

One commenter suggested that a bullet is not required in requirement part 1.3 of Requirement R1. The comment also suggested an inconsistency between Requirement R1 and the associated VSL. The SDT has redrafted Requirement R1 in consideration of comments and the bulleted clause is now in the applicable part of the requirement. The inconsistency in the VSL has been corrected.

One commenter suggested that the SDT continues to insist there is no need to identify the low impact BES Cyber Systems and their associated Cyber Assets (e.g., R1.3) and that this causes an auditability issue. The SDT believes that an “asset” based approach in the revised draft and the requirement for the list of assets containing Low Impact BES Cyber Systems provides relief to the auditing issue.

Several commenters requested an explanation of the values used in the VSLs for Requirement R1. The SDT notes that the values are based on FERC Guidelines for VSLs that use percentages. Many entities commented on the need for absolute values for smaller entities since percentages would provide an unfair bias for small entities that would more easily reach percent based thresholds.

One comment stated that the SDT should consider reusing lists generated by other standards. The SDT notes that evidence used for other reliability standards can be presented for these CIP standards as long as they provide the evidence required to demonstrate compliance to the CIP requirement.

One commenter suggested that requirement parts 1.1, 1.2 and 1.3 should also include documentation as part of the requirement and that requirement part 1.4 should require the update prior to commissioning. The SDT's approach to requirement definition focuses on results and believes that a requirement to "document" does not directly result in the reliable operation of the BES. The SDT has defined the required functional result that directly contributes to the reliable operation of the BES. Requirement R1.4 has been removed by SDT in consideration of comments received.

One commenter suggested that by specifying requirements for Low Impact, CIP-002-5 implies a list of BES Cyber Systems. The commenter further suggested either requiring a list of Low Impact Cyber Systems or removing Low Impact altogether. The SDT notes that requirements must be explicit and that CIP-002-5 has made it clear and explicit that a list of Low Impact BES Cyber Systems is not required. However, in the new draft, a list of Low Impact assets is required to facilitate the application of policy requirements to Low Impact assets.

Several commenters suggested many editorial changes to the language used in Requirement R1. The SDT has made fundamental structural and language changes to Requirement R1 to address comments received.

Requirement R2

One commenter suggested that the rationale for Requirement R2 does not include approval of the lists. The SDT notes that the last sentence in the rationale refers to the approval process.

One commenter made many remarks on inconsistencies between the Requirement R2 language, the measure and the VSLs. The SDT has made modifications to R2 and its measures and VSLs for consistency.

Many commenters suggested alternative language, or reverting to the use of the term annual for the clause describing the annual review and approval. One commenter also inquired as to whether the clause supersedes an entity's definition of annual. The SDT has discussed alternative approaches and is using the term "at least once every 15 months" to provide reasonable flexibility to Responsible Entities while meeting the intent of the requirements. The SDT has intentionally not used the word "annual". This term is no longer used in these CIP standards for periodic requirements

and therefore, the CAN on the word annual can no longer apply in this requirement. One of the objectives of the SDT in Version 5 is to consider applicable CANs and use language that would no longer require a CAN to clarify audit interpretation. Instead, the SDT used specific language that implements its intent. This topic is also discussed in greater detail in the introductory, global section of these comment responses.

Attachment 1

Section 1 - High Impact Control Centers

One commenter stated that criteria for control centers fail to consider inter-Control Center connectivity and that the concept of mutual distrust does not work because of trusted paths. The SDT has included consideration of connectivity in the application of requirements. The applicability of mutual distrust depends on specific considerations of network configuration. A blanket statement based on an assumed configuration does not support the generalized comment. The SDT believes that requirements in the standards for protection of BES Cyber Systems provide a basis for Responsible Entities to implement the necessary protection in their network and system design.

Several commenters stated that the introductory text in High and Medium Impact criteria should be deleted or modified due to the change in approach for facilities based impact. The SDT notes that Requirement R1 still requires, ultimately, the categorization of BES Cyber Systems for the application of requirements. The SDT believes that the introductory text in the criteria for High and Medium is still required to express this result.

One commenter suggested on the inclusion of “associated data centers” in the control center criteria and argued that the BES Cyber Systems in these “data centers” would already be included. The SDT has made revisions to the definition of Control Centers, has now included data centers in the definition, and removed the phrase from attachment 1.

Many comments were received on the relationship of TO Control Centers and the functional obligations of TOPs. There was also a comment on the section in the guidance that pertains to TO Control Centers that perform the functional obligations of the TOP. In particular, one comment suggested removal of the guidance, citing ownership issues and issues with NERC Functional Entity registration. The SDT believes that the criterion in question is used to determine the impact of the BES Cyber Systems, and that, irrespective of registration issues, if these Cyber Systems perform a function that is relevant to the functional obligation of a TOP, and that this is formally delegated, then the impact should be appropriately assessed as such. The issue of ownership is a non-issue since the responsibility for compliance to the applicable requirements resides with the owner of the identified BES Cyber Systems that provide that function.

Several commenters suggested that the language used in criterion 1.3 with respect to TOP Control Centers needed clarification and that the guidance for this criterion should explicitly say that TO Control Centers that do not perform the functional obligation of the TOP should be classified as Medium. The SDT has inserted additional guidance to clarify this point. A TO facility that does not perform or does not have an obligation to perform any of the reliability tasks of a BA, TOP or GOP does not meet the definition of a Control Center and the BES Cyber Systems should be evaluated according to the criteria in attachment 1. TOs should review the functional tasks of a TOP and those of a TO and ensure they are not delegated any of these functional tasks through an agreement or a contract. In particular, TOs should note that the functional model does not list real-time operational tasks for that entity.

One commenter asked whether a TO Control Center that performs an operation under the direction of a TOP is performing a functional obligation of a TOP. The NERC Functional Model does not include operation of BES Facilities under the tasks or obligations of a TO, but does include them under the obligations of a TOP. If the TO has an obligation (contractually or because of some other formal agreement) to operate BES assets, whether it is in an emergency or in normal operational circumstances, under the direction of a TOP, then that Cyber System is used to perform the functional obligation of a TOP. The functional obligation of operational control of the BES asset has been delegated to the TO.

One commenter also asked whether a TO data center that collects data and then processes that data for transmission to the TOP is performing a functional obligation of the TOP. The SDT has moved the data center association to the definition of a Control Center and associates it with the facility hosting the operating personnel. In the scenario described, the TO data center is not associated with the BES Cyber Systems owned by the TOP. The “data center” described is analogous to field data aggregating facilities and are evaluated as BES Cyber Systems necessary for providing situation awareness for real-time operations, and should not be evaluated as TOP Control Center “data centers”.

One commenter suggested a number of modifications to the criteria aimed at better stratifying the distinction of Medium from High Impact, especially in the case of BA and TOP Control Centers. The SDT considered the suggestions and has made a number of modifications to address the comments. On another suggestion of increasing the threshold for High Impact BA and GOP Control Centers to 3000 MW, the SDT notes that the stratification of the High Impact from Medium Impact is mostly based on impact due to the wide area reliability tasks of the Functional Entities. However, the SDT has included modifications that provide some stratification of the levels for BA, TOP and GOP Control Centers which are consistent with thresholds approved in Version 4. On the subject of UFLS thresholds, the SDT reviewed recent developments in Regional Standards for UFLS and the tolerances specified in these standards as a basis for evaluation of

the current threshold: the SDT concluded that the current threshold represents a reasonable representation of the level of tolerance in these standards so far.

Several commenters suggested that Control Centers that use voice or manual instructions be categorized as Low Impact. The SDT notes that Cyber Systems that provide information to Control Center operators that use manual or voice to effect control operations on BES assets in real-time based on that information must be subject to the same protection as those that trigger automated operation. If the communication or manual operation results from information provided for real-time operations, there is no rationale for categorizing them as a lower impact.

One commenter suggested that the word "control" in the definition of Control Center requires more explanation and that the situation awareness section of the guidelines on BES Reliability Operating Services could include cyber systems used in collecting data for management and engineering analysis. The SDT has provided, in the guideline, the type of operations included in the use of the word. The definition provides further qualification in the context of the Control Center. The word "control" is used in several other standards and is a well understood concept in the BES environment. The intent of the situation awareness section in the guideline on BES Reliability Operating Services is to broadly define a reliability function and is not meant to be used solely for the qualification of applicable BES Cyber Systems: it is intended to be a first step in qualifying a population of Cyber Systems for further application of additional qualifications in the definition of BES Cyber Systems, applicable assets and the impact criteria in attachment 1.

One commenter stated that criteria 1.2 and 1.4 in attachment 1 qualify assets affected as "generation assets" and pointed out that not all assets in scope are strictly "generation assets". The SDT agrees and has made the suggested modification.

One commenter requested clarification on whether the 1500 MW in requirement parts 1.2 and 1.4 of attachment 1 referred to criterion 2.1. The SDT responds that the 1500 MW refers to total aggregate generation of 1500 MW, and is not tied to criterion 2.1.

Section 2 - Medium Impact

Several commenters stated that the 15 minute criterion in requirement part 2.1 of attachment 1 is unnecessary and redundant. Another commenter stated that this 15 minute clause was contrary to the "bright-line" concept. One commenter also stated that the inclusion of the 15 minute qualification in the criteria was inappropriate because the criteria define BES asset impact. The addition of this qualification resulted from previous comments and sought to

provide clarity in the scope of BES Cyber Systems to be included in consideration of this criterion. Where the qualification is included, the language makes it clear that it applies to the effect of the BES Cyber System.

There was a comment that the 15 minute in criterion 2.1 and 2.2 is going to be difficult to prove in an audit and suggested the term "that operate the reactive resource" instead in 2.2. As stated in the guideline, the intent of the 15 minute is to provide a boundary to the impact to real-time operations. The alternative use of the term "real-time" does not provide a useful defined term. The SDT believes that the commenter's suggestion to use the term "that operate" in criterion 2.2 restricts the full scope of cyber systems that affect the real-time operation of the BES for reactive resources.

The commenter further suggested that criterion 2.1 should consider regional operational conditions and requested clarification on the 1000 MVAR threshold for 2.2. For 2.1, the SDT considered regional variations in determining this threshold and notes that this is the approved Version 4 criterion. For 2.2, the SDT consulted with operational and planning experts during the development of this criterion in Version 4.

One commenter stated that the commas around the words "as necessary" in criterion 2.3 were confusing. The SDT has reviewed the criterion and agrees that the commas are misplaced and have altered the intent of the criterion. The SDT has made changes to the placement of the commas to clarify the intent.

One commenter requested clarification on the use of the phrase "long term planning horizon" in criterion 2.3. The SDT notes that criterion 2.3 of attachment 1 does not use the phrase "long term planning horizon" but uses a specified one year or more near-term timeframe. The SDT notes the intent is to avoid the identification of generation facilities that could be used to remediate short term reliability issues.

Two commenters requested additional clarification in the notifications to asset owners in criteria 2.3 and 2.6. For 2.3, the notification is affected as part of the execution of a contract. For 2.6, the applicable IROL reliability standards require that the asset owners be notified. These standards do not specify how the notification is to be done, but that notification must be performed.

One commenter suggested that in requirement part 2.2 of attachment 1, the nameplate value should be qualified to account for ranges. The SDT has included a qualification of "maximum" in the criterion.

One commenter stated that criterion 2.3 references the long term planning horizon, contrary to the real-time operations aspect of the CIP standards. In addition, the commenter suggested that additional guidance be provided as to the notification of such obligations. Also, the commenter requested similar clarification in the guideline for criterion 2.8. The SDT points out that the criterion states that the designation of the asset is performed as part of a planning activity that has a time horizon of one year or more (near-term) by the Planning Coordinator or Transmission Planner, but the impact of a compromise of an affected BES Cyber System would meet the qualification for real-time operations. Additional clarification on notifications has been added to the guideline for criteria 2.3 and 2.8.

One commenter stated that the guidance section that refers to the category D contingency of TPL standards in the discussion of criterion 2.3 is unlikely and suggests removing it. The SDT has removed the reference in the guideline.

One commenter suggested using the phrase “generation interconnection facility” instead of “Transmission Facilities providing the generation interconnection required to connect generator output to the Transmission Systems Transmission Facilities” in criterion 2.8, citing the term used in Project 2010-07. Another commenter suggested on the exclusion of generation plant collector buses in criterion 2.4 and 2.5 in the guidance and suggested an explicit exclusion in the requirement. The SDT reviewed the standards in Project 2010-07 and has not found “generation interconnection facility” as a defined term in the NERC Glossary. The term is however used in the PRC standard in the project. The SDT intends that the application of this criterion to Transmission Owner/Transmission Operator owned and generator owned Transmission Facilities that provide this interconnection of generator output to the Transmission system. However, for clarity and to address the exclusion of these facilities in criteria 2.4 and 2.5 that one comment stated, the SDT has added this term as an inclusion in 2.8.

One commenter suggested alternative language for criterion 2.5 to clarify the application of the aggregate rating. The SDT made modifications to the language in 2.5 to clarify the application of the aggregate to the sum of applicable Transmission facilities at the station.

Many commenters suggested using, for criterion 2.6, the same language used in criteria 2.8 and 2.9. The SDT notes that in criterion 2.6, the criterion refers directly to the Facilities that make up the IROL and has used the exact language used in the IROL standards that require the identification of these specific Facilities. Criteria 2.8 and 2.9 apply to Facilities that could indirectly cause a violation or reduction of the IROLs.

Several comments were on the reasons for the removal of the WECC specific qualifications for those criteria that are based on IROLs. The SDT understands that the commenter has reconsidered its position on IROLs and that other changes in attachment 1 negate the need for any WECC specific qualification.

Several commenters requested information on the standards that require notification of asset owners for IROLs in criterion 2.6. One commenter also stated that the term Control Center is not a NERC defined term and to organize the guidelines by transmission, generation, etc. The SDT notes that the guidelines for criterion 2.6 provides information on the NERC Reliability Standard that contains these requirements (FAC-014) that require identification of these assets and notification to applicable owning Functional Entities. The term Control Center is a proposed defined term in this CIP standards package and the guidelines for criteria are organized by generation and transmission.

One commenter inquired as to why all facilities necessary for the NIPR (not just Transmission Facilities) are not included in criterion 2.7 (Nuclear Interface facilities). The SDT notes that the scope of applicability in NUC-001 is limited to transmission entities listed, which consists of registered entities.

One commenter requested clarification in the application guideline on how, in criterion 2.8, the TO would obtain information on whether generation it does not own or operate meets criterion 2.3. The SDT included additional guidance in the application guideline section.

One commenter stated that the UVLS/UFLS in criterion 2.10 that refers to the 300 MW threshold should specify the lowest rating in the last 12 months. Several commenters stated that the use of the highest MW rating in the guidelines and technical basis on UVLS/UFLS should be changed to “hourly integrated load”. The SDT has not specified the methodology used to determine the 300 MW and has deferred to the requirements of the applicable regional UFLS/UVLS standards.

One commenter stated that criterion 2.10 might imply that individual unconnected relays in a load shedding program under a common trip point would be included and suggested excluding these. The SDT believes that the qualification of a common control system addresses this concern and believes that the exclusion language has the unintended consequence of excluding individual relays irrespective of their impact.

One commenter stated that the language in criterion 2.10 which specifies “regional load shedding programs” is problematic since there is no such requirement and pointed out that PRC standards place the responsibility for

establishing UFLS programs on the Planning Coordinator. The SDT has made modifications to section 4 that pertains to load shedding and criterion 2.10 to more accurately reflect the requirements of the PRC standards.

There was a comment that for criterion 2.10, the language suggests that any compromised component that make up SPS, RAS or automated switching system is required to be protected regardless of if it has an effect on the IROL or not. The SDT notes that the current language does not imply this requirement. The current language only applies if the compromise, whether of one or more components of the SPS, RAS or automated switching system, would cause a violation of one or more IROLs or "cause a reduction of one or more IROLs".

One commenter suggested setting a threshold for Special Protection Systems for applicability of these CIP standards. The SDT notes that all Special Protection Systems, irrespective of any threshold, are designated as Critical Assets under Version 4. The SDT notes that this has been the case because of the critical function provided by Special Protection Systems in the reliable operation of the BES.

Numerous commenters stated that in part 2.11 of attachment 1, the threshold for generation Control Centers should be changed to 1500 MW for consistency with the generation threshold in other criteria in Medium Impact. One commenter also pointed out an inconsistent term in the flow chart in the guidelines and technical basis section. In the same area, another commenter commented that part 2.11 should be removed and that the specific hydro situation should be handled in the definition. The SDT's intent in 2.11 is to include as Medium all the remaining Control Centers not already classified as High, because of the functions provided by Control Centers. In defining a 300 MW threshold for generation Control Centers in 2.11, the SDT was attempting to address a situation specific to hydro-electric generation Facilities. The SDT has removed this artificial threshold in view of changes made to this criterion. Further, the SDT made modifications in the threshold in the criterion for generation Control Centers to address these comments. The inconsistency of terms used in the flowchart has been corrected.

Several entities commented on the removal in draft two of criteria for restoration resources (blackstart units and cranking paths) from the Medium category. Some were in favor of this removal while others were not. Specifically, one commenter made several comments regarding generation and cranking path restoration resources. One comment read that restoration resources should be rated as Medium Impact. In contrast, another commenter suggested that restoration resources should not be included in the scope of the application of the CIP standards because of the absence of the need for remote data communication in the event of a restoration and the exclusion of cranking path from the definition of the BES. In response, in addition to the justification provided as part of the draft two materials, the SDT has

further considered industry input and comments in the consideration of these criteria with respect to their effect on overall reliable operation of the BES and has now removed them from High or Medium Impact criteria. In response, the SDT notes that the assumption that remote access through data communications is necessary for the realization of cyber security threats represents an incomplete mitigation approach, and that the CIP standards are aimed at protecting cyber systems that would impact the real-time operation of the BES, not solely those that directly operate elements of the BES. NERC Reliability Standards that govern the operation of load shedding programs and the protection of the BES elements are other examples of such approaches.

Section 3 – Low Impact

One commenter noted that the criteria in section 3 of attachment 1 should include the phrase "not included in high or medium". The SDT has made the necessary clarification.

General Comments

One commenter suggested that the footnote regarding the effective date of Version 5 and the effective date of Version 4 should be moved to the main text of the effective date. The SDT considered moving this footnote, but believes that movement of the footnote could cause unnecessary confusion, since the effect would not be different. The footnote simply clarifies the effective language that Version 4 does not go into effect and is superseded by Version 5.

There was a comment that the varying language regarding the phrase "destroyed, degraded, or otherwise rendered unavailable" and its variations needs to be consistent. In addition, Southern Company provided additional clarification language for the cranking path criterion in Low Impact. The SDT has reviewed the uses of the term and has ensured consistency when referencing Facilities or BES Cyber Systems. The main difference is the addition of "destroyed" and "otherwise rendered unavailable" in the case of Facilities. The SDT has added the suggested clarification in criterion 3.3.

One comment was on the use of the word "would" instead of "could" in the standards and recommended the use of the prospective word "could". The SDT believes that the use of the word "would" is appropriate to describe the certain impact of a compromise due to an exploitation of vulnerability.

One commenter stated that the last paragraph on page seven leaves it up to the registered entity to determine the level of granularity when identifying the BES Cyber Systems and instructs the registered entity to take into consideration the operational environment and scope of management and raised questions of auditability in the text. The SDT notes that the background and guideline sections are only providing context to the standards. The only auditable parts of the

standards are the applicable definitions and requirements. The SDT directs the commenter to the definition of BES Cyber System for effective application of the requirements.

There was a comment on the examples for Electronic Access Control and Monitoring Systems in the background section, specifically the use of certificate authorities, security event monitoring systems and intrusion detection systems. The SDT uses the term "Certificate Authorities" as an example of the type of cyber assets owned by the Responsible Entity that would be subject to the CIP standards if it relates to a function that is used within the scope of a BES Cyber System. The SDT has used the generic term "security event monitoring systems" as a generic functional term and has specifically avoided the use of the various acronyms used to include this function. This is also true of the term "intrusion detection systems": the SDT is providing an example of the function, and the term "intrusion prevention systems" includes functions that are not within the scope of the requirements. The SDT acknowledges that intrusion prevention systems necessarily include an intrusion detection function.

One commenter suggested the inclusion of network attached storage and storage area networks in the examples for Protected Cyber Assets. Examples provided are not intended to be exhaustive lists, but are intended to provide some examples of the types of systems that could meet the requirements for the definition of Protected Cyber Assets. They are not intended to mean that all of these types of systems are necessarily Protected Cyber Assets, but are examples of systems that could be Protected Cyber Assets if they meet the definition.
SPP suggested footnoting the time horizon reference in requirements. Time Horizons are standard designations used in all requirements and is a standard requirement for all NERC standards requirements. They are required characteristics of each requirement in the same way that Violation Risk Factors are. The SDT believes that footnotes for these are not required as they are generically defined in other NERC documents.

One commenter requested clarification of the general use of transmission facility and its scope. In using terms such as "Facility" in the criteria, the SDT has made substantial changes to Requirement R1 that provides flexibility to the Responsible Entity to define what the term includes within the definition of the requirement. Requirement R1 now includes a listing of the types of assets to be considered that provides a more defined scope to the applicability of CIP-002-5 and the CIP cyber security standards. Within these, Responsible Entities have flexibility in defining the sets within these considerations for application of the criteria.

One commenter requested clarification on entities that have coordination responsibilities. The SDT notes that the table in the guidance provides guidance on those entities that have responsibilities for inter-entity coordination. In a

restoration scenario, those Responsible Entities that require inter-entity coordination to perform their functions that require such coordination have responsibility for this coordination.

One commenter pointed to an inconsistency between the title of the standard and the heading of the document. The SDT corrected the inconsistency.

One commenter stated that the NERC Functional Model does not define Functional Entities. The SDT notes that the current version of the Functional Model (Version 5) defines both Reliability Functions and the Functional Entity that performs the tasks. In addition, there are further responsibilities defined under Functional Entities which are specifically defined in relation with other Functional Entities.

A commenter requested additional guidance in the concept of BES Cyber System. The SDT has made several modifications to the guidance for the overall concept of BES Cyber System, including additional peripheral terms related to BES Cyber Systems, such as Protected Cyber Assets. The SDT believes these additional clarifications provide the additional guidance on the concepts.

There was a comment on the guidance on BES Reliability Operating Services provided for optional use by entities as an aid to scope BES Cyber Systems in the guideline section of the standards. One commenter also suggested removing the designation of Functional Entities for the BES Reliability Operating Services to minimize differing opinions. The SDT made several modifications to this section in consideration of these comments where appropriate. With respect to comments on voltage control and Distribution Providers, the Functional Model clearly lists voltage reduction in its tasks. The designation of Functional Entities is provided as guidance and resulted from comments from previous drafts. The SDT believes that this information provides additional guidance for some Responsible Entities in scoping their BES Cyber Systems.

One commenter suggested that the format of the standard is different and suggested moving the background to the end together with the guideline. The SDT has used the standard template for results based standards and is the recommended standards development format and approach.

There was a suggestion that the rationale should not be part of the standard. The rationale statements will be removed from the official filing and included as information, together with the guidance information.

Several comments were on the use of bright lines and the problem with a one size fits all approach without provisions for studies and engineering analysis and the requirement to require at least some protection for all BES assets. The SDT notes that the objective of Version 5 of the CIP standards is to provide some level of protection to all BES Cyber Systems according to the impact to the real-time operation of the BES assets they are supporting. The bright line based approach was approved by industry stakeholders and FERC as part of Version 4.

One commenter suggested the use of a more definitive term “prevent” in qualifying impact on functions in the reliable operation of the BES. In addition, there was a suggestion for an explanation of the use of the 15 minute window in the definition of BES Cyber Asset. The SDT believes that the word “prevent” does not provide a qualification for the full scope of applicability, but a subset. The intent of the SDT is to ensure that impacts also cover impairment as well as outright “prevention”. An explanation of the 15 minute window is in the background section of the standard under real-time operations.

One comment suggested that the stipulation of ownership for compliance responsibility is inconsistent with PRC standards that also stipulate “operate”. The SDT has consistently maintained that responsibility for compliance is the asset owner’s.

There was a general comment on the application of FISMA and the NIST framework in relation to the CIP standards. The SDT notes that CIP V5 considered the NIST framework as one of the inputs to the drafting of these standards in response to FERC Order 706. The SDT did not consider FISMA requirements, but rather the NIST Risk management framework as directed by Order 706. The SDT also considered input from several other frameworks and has used those inputs in the drafting of standards that are subject to compulsory compliance and enforcement. The NIST 800-53 series is characterized as guidelines for controls, not compliance requirements.

QUESTION A10 – CIP-003-5:

If you disagree with the changes made to CIP-003-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the major issues identified through the comment form with CIP-003-5 included (1) the list of low impact BES Cyber Systems for Requirement R2, (2) demonstration of policy implementation, (3) clarity of policy topics in Requirement R2, and (4) the reliability benefit of the annual review/approval of the cyber security policies as well as maintaining documentation of changes to the CIP Senior Manager and delegates.

List of Low Impact BES Cyber Systems for Requirement R2

Numerous commenters identified concerns that while the SDT intended to provide protection from discrete identification of Low Impact BES Cyber Systems, there was still significant concern that this would still be required in order to demonstrate compliance with the requirement. Additionally, commenters suggested that the object of the policy for Low Impact BES Cyber Systems should be on the facilities (or "sites") themselves and not specifically the Low Impact BES Cyber Systems. The SDT continues to believe that the identification of low impact BES Cyber Systems would not be required in order to comply with CIP-003-5 R2. However, the SDT also agrees with commenters that a facilities based approach to the low impact policy comes with a number of benefits. Among these being the creation of a reasonable level of abstraction (the facility) of which to refer to the low impact BES Cyber Systems, thus facilitating any necessary sampling during an audit, without explicitly needing a list of these cyber systems themselves. Consequently, CIP-003-5 R2 has leveraged a reference to CIP-002-5 where facilities with low impact BES Cyber Systems are identified. The SDT believes this approach will provide consistency of application of the policy for low impact BES Cyber Systems, provide a reasonable approach for audit oversight, and create additional clarity on the evidentiary expectations.

Policy Implementation

There were a number of comments that expressed issues with ambiguity in the use of the term "implement" as it relates to the cyber security policies in both CIP-003-5 R1 and R2. In reviewing this comment, the SDT noted that the obligation to "implement" the cyber security policy has existed since version 1 of the CIP standards. Additionally, FERC directed the ERO in Order 706 to "to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards." While this directive did not specifically direct changes to the cyber security policy, as this policy already had the obligation to implement in version 1, the SDT is cognizant that any change to the contrary would require reasonable justification.

As it relates to the CIP-003-5 R1 cyber security policy for medium impact and high impact BES Cyber Systems, the SDT believes there is sufficient justification to make a modification to the language of the requirement in order to provide the clarity that the industry desires around the obligation to "implement." The SDT strongly believes that it has not lessened the obligation to implement the cyber security policy. However, given the required scope of the CIP-003-5 R1 cyber security policies, the SDT believes that implementation of these cyber security policies is effectively demonstrated through compliance with CIP-004-5 through CIP-011-1. Therefore, the SDT has chosen to remove the term "implement" from CIP-003-5 R1. The SDT believes that this should provide clarity as to the expectation of implementation as well as to relieve concerns of double jeopardy between CIP-003-5 R1 and the entire body of CIP-004-5 though CIP-011-1.

The SDT has handled this concern differently for the low impact cyber security policies in CIP-003-5 R2. As there are no corresponding requirements in CIP-004-5 through CIP-011-1 that require explicit implementation of areas addressed by the low impact policy, there are no double jeopardy concerns. The SDT has attempted to provide structure around the obligation to implement the cyber security policies through the global modifications that provide for continuous improvement and the identification, assessment, and correction of deficiencies. The expectation of the SDT is that entities will define cyber security policies that address the four required areas and put these policies in effect using an overall framework that provides reasonable assurance that the policies are applied through methods that identify, assess, and correct any deficiencies.

Policy Topic Clarity for Low Impact Policy

In addition to ambiguity over the implementation of the cyber security policy for low impact BES Cyber Systems, commenters expressed concern over the clarity of the individual policy topics for low impact BES Cyber Systems. The SDT appreciates these comments and has made some modifications to the topic language. However, the SDT understands that these modifications do not completely alleviate the concerns around individual topical clarity. The SDT has modified the topic "Physical access controls" to "Physical security controls" and "Electronic access controls" to "Electronic access controls for external routable protocol connections and Dial-up Connectivity." The SDT chose to not add too much additional detail to these policy topics in recognition of the wide range of environmental, geographic, technical, operational, and logistical differences that may exist amongst the set of low impact BES Cyber Systems. As such, the SDT's intent is to allow Responsible Entities to have flexibility to design and implement the most efficacious security program possible for their particular set of low impact BES Cyber Systems. The modification to physical security controls over physical access controls acknowledges this approach. "Physical security controls" gives great discretion to the Responsible Entity to choose controls that are effective. The SDT believes the paradigm shifts in NERC CIP Reliability

standards allowing for multiple levels of security (high, medium, and low) and creating an atmosphere of continuous improvements through the identification, assessment, and correction of deficiencies will address the concerns of compliance risk that are driving the need for more prescriptiveness in requirements language. Additionally, the SDT added the language to R2.3 "…for external routable protocol connections and Dial-up Connectivity" to address the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact.

Reliability Benefit and Double Jeopardy Concerns of Requirements R3, R5, and R6

Numerous commenters also raised questions about either the reliability benefit or double jeopardy of requirements R3, R5, and R6. Often, these questions were tied to work going on in NERC standards related to Paragraph 81 of the FERC Order approving the FFT process. The comments about their reliability benefit sometimes hinged on them being a requirement in and of themselves, rather than a component of the requirements for R1, R2, and R4 in draft two. The double jeopardy concerns also raised similar questions as to whether a violation of R3, R5, and R6 in draft two would also constitute a violation of R1, R2, and R4 of draft two. The SDT agreed with these concerns. The SDT believes that the same reliability and security objectives will be reached, while alleviating unnecessary compliance concerns, by combining these requirements. As such, the review and approval for each of the cyber security policies has been added as an obligation in the security policy requirements (R1 and R2) themselves. Additionally, the obligation to keep the CIP Senior Manager and delegation documentation up-to-date has been added to those requirements (now R3 and R4), respectively.

Modify Signature to Approval in Measures

Several commenters mentioned the use of "signature" in the measures when the requirement called for "approval." The SDT had never intended to imply that a wet ink signature was the only acceptable form of evidence of approval. Language in the guidelines and technical basis section further clarified that hardcopy or electronic approvals were acceptable. The SDT has modified all instances of "signature" in the measures in CIP-003-5 to "approval' to prevent any confusion and better align with the language in the requirement itself.

Minority Comments

The SDT also received a number of different comments that asked various questions or raised assorted concerns about the topics that were included in Requirement R1. Among other things, these comments mentioned confusion about the guidance related to terms used in the policy topics, inclusion of Interactive Remote Access separate from ESPs, and the relationship between these topics and CIP-004-5 through CIP-011-1. The intention of the SDT was for these policy items

to individually reference each of the standards CIP-004-5 through CIP-011-1. As such, the SDT has chosen to align the policy topics with the title of the other CIP standards (with some exceptions) and include a specific reference to the standards itself in order to clarify that alignment. As mentioned in the discussion of policy implementation above, the SDT's expectation is that implementation of the cyber security policy for medium and high impact BES Cyber Systems will be demonstrated through compliance with CIP-004-5 through CIP-011-1.

Typographical Errors

Several commenters also noted a typographical error where the VRF for CIP-003-5 R2 was listed as low in the requirement and medium in the VSL table. The SDT appreciates commenters pointing this out. The intention of the SDT was for the VRF of CIP-003-5 R1 for medium and high impact BES Cyber Systems to be medium, consistent with CIP-003-4 R1 and for the VRF of CIP-003-5 R2 to be low due to the lesser risk associated with low impact BES Cyber Systems. The SDT has corrected this mistake.

VSL Comments not responded to:

One comment suggested that Requirement R6 should have four VSLs based on days late. The SDT has removed the requirement because the addition of language to identify, assess, and correct deficiencies in what is now Requirement R4 covers the documentation of delegations.

One comment stated to start missing discrete elements of a program as low VSLs in Requirement R2. The SDT has made this change.

One comment suggested to use Lower/Moderate VSLs for Requirement R2 instead. In response, the VSLs only address the degree to which entities can violate a requirement and not the risk power to the BES from said violations.

For the Requirement R4 VSLs, there was a comment that the VSL should read: Lower/Medium – Lack of Review High/Severe – Lack of Approval. This requirement has been removed because the annual review is already accomplished in Requirement R1 and the need to have a CIP Senior Manager sign the policy is administrative in nature.

There was a comment that the VSL for Requirement R3 is more detailed than the requirement itself. The SDT has updated the VSL to match the requirement.

Questions with Votes Only:

1. **Requirement R1 of draft CIP-002-5 requires the identification of high and medium impact BES Cyber Systems as described in Attachment 1. Further, it requires a Responsible Entity to review (and update as needed), the required identification within 60 calendar days of when a change to BES Elements or Facilities is placed into operation, which is planned to be in service for more than 6 calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category. Do you agree with the proposed Requirement R1?**

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
ACES Power Marketing	No
PPL Corporation NERC Registered Affiliates	No
BC Hydro	No
IRC Standards Review Committee	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No

Organization	Yes or No
Duke Energy	No
Dominion	No
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	No
MRO NSRF	No
Florida Municipal Power Agency	No
Madison Gas and Electric Company	No
Luminant	No
SMUD & BANC	No
Progress Energy	No
NCEMC	No
Dairyland Power Cooperative	No
Western Electricity Coordinating Council	No
CenterPoint Energy	No
Tri-State G&T - Transmission	No
PacifiCorp	No

Organization	Yes or No
PNM Resources	No
Hydro One	No
Southern Company Services, Inc.	No
Western Area Power Administration	No
Utility Services Inc.	No
Consumers Energy Company	No
Muscatine Power and Water	No
North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency	No
NIPSCO	No
Portland General Electric	No
TransAlta Centralia Generation LLC	No
Trans Bay Cable	No
National Grid	No
Hydro-Quebec TransEnergie	No
LCEC	No

Organization	Yes or No
Pacific Gas and Electric Company	No
Ingleside Cogeneration LP	No
Manitoba Hydro	No
Niagara Mohawk (dba National Grid)	No
PSEG	No
Bonneville Power Administration	No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Illinois Municipal Electric Agency	No
NV Energy	No
Wisconsin Electric Power Company	No
The Empire District Electric Company	No

Organization	Yes or No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Texas Reliability Entity	No
Nebraska Public Power District	No
City of Austin dba Austin Energy	No
ISO New England	No
Network & Security Technologies, Inc.	No
City Utilities of Springfield, MO	No
American Public Power Association	No
Alliant Energy	No
Springfield Utility Board	No
Exelon Corporation and its affiliates	No

Organization	Yes or No
Indiana Municipal Power Agency	No
NYISO	No
Cowlitz County PUD	No
Brazos Electric Power Cooperative	No
US Bureau of Reclamation	No
NRG Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
SPP and specific Member companies	Yes
Puget Sound Energy, Inc.	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes

Organization	Yes or No
Arizona Public Service Company	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Services Corporation	Yes
Lincoln Electric System	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Xcel Energy	Yes
Flathead Electric Co-op	Yes
Tennessee Valley Authority	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes

Organization	Yes or No
PJM Interconnection	Yes
Kansas City Power & Light	Yes
MEAG Power	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes

2. Requirement R2 of draft CIP-002-5 states, "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once each calendar year, not to exceed 15 calendar months between approvals, even if it has no identified items in Requirement R1, Parts 1.1, 1.2, or 1.3." Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
ACES Power Marketing	No
BC Hydro	No
Texas RE NERC Standards Review Subcommittee	No
NRG Companies	No
Florida Municipal Power Agency	No
SMUD & BANC	No
Progress Energy	No
PacifiCorp	No
Utility Services Inc.	No

Organization	Yes or No
NIPSCO	No
LCEC	No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
NextEra Energy, Inc.	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Texas Reliability Entity	No
City of Austin dba Austin Energy	No
ISO New England	No

Organization	Yes or No
Kansas City Power & Light	No
Indiana Municipal Power Agency	No
Brazos Electric Power Cooperative	No
PPL Corporation NERC Registered Affiliates	Yes
IRC Standards Review Committee	Yes
Southwest Power Pool Regional Entity	Yes
Duke Energy	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes

Organization	Yes or No
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Luminant	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
Hydro One	Yes

Organization	Yes or No
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency	Yes
Portland General Electric	Yes

Organization	Yes or No
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
Pattern	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes

Organization	Yes or No
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Xcel Energy	Yes
Flathead Electric Co-op	Yes
Bonneville Power Administration	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Ameren	Yes
Northeast Utilities	Yes
Oncor Electric Delivery Company LLC	Yes
Nebraska Public Power District	Yes

Organization	Yes or No
PJM Interconnection	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes
MEAG Power	Yes
American Public Power Association	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
California ISO	Yes
US Bureau of Reclamation	Yes

4. CIP-003-5 R1 states "Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall implement one or more documented cyber security policies that address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
NESCOR/NESCO	No
ACES Power Marketing	No
Duke Energy	No
Progress Energy	No
NCEMC	No
PNM Resources	No
AEP Standards based SME list	No
Xcel Energy	No
MidAmerican Energy Company	No
Ameren	No

Organization	Yes or No
NextEra Energy, Inc.	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Kansas City Power & Light	No
Brazos Electric Power Cooperative	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Southwest Power Pool Regional Entity	Yes
NRG Companies	Yes
PNGC Comment Group	Yes

Organization	Yes or No
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Florida Municipal Power Agency	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Hydro One	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes

Organization	Yes or No
Portland General Electric	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes

Organization	Yes or No
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Lakeland Electric	Yes
New York Power Authority	Yes
Tampa Electric Company	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Illinois Municipal Electric Agency	Yes
NV Energy	Yes
Wisconsin Electric Power Company	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Oncor Electric Delivery Company LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
City of Austin dba Austin Energy	Yes
ISO New England	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes
MEAG Power	Yes
American Public Power Association	Yes
Alliant Energy	Yes

Organization	Yes or No
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
California ISO	Yes
US Bureau of Reclamation	Yes

5. **CIP-003-5 R2 states "Each Responsible Entity for its BES Cyber Systems not identified as high impact or medium impact shall implement one or more documented cyber security policies to address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2?**

Summary Consideration:

Organization	Yes or No
NESCOR/NESCO	No
ACES Power Marketing	No
PPL Corporation NERC Registered Affiliates	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No
NRG Companies	No
Duke Energy	No
MRO NSRF	No
Florida Municipal Power Agency	No

Organization	Yes or No
Madison Gas and Electric Company	No
Pepco Holdings Inc & Affiliates	No
National Rural Electric Cooperative Association (NRECA)	No
Progress Energy	No
NCEMC	No
Dairyland Power Cooperative	No
AEP Standards based SME list	No
Snohomish County PUD	No
Edison Mission Marketing & Trading	No
Consumers Energy Company	No
Muscatine Power and Water	No
Lower Colorado River Authority	No
LCEC	No

Organization	Yes or No
LCRA Transmission Services Corporation	No
Ingleside Cogeneration LP	No
Xcel Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service	No

Organization	Yes or No
Corporation and Upper Pennisula Power Company	
Nebraska Public Power District	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Kansas City Power & Light	No
Network & Security Technologies, Inc.	No
MEAG Power	No
Alliant Energy	No
Exelon Corporation and its affiliates	No
Deseret Power	No
Brazos Electric Power Cooperative	No
Northeast Power Coordinating Council	Yes
BC Hydro	Yes

Organization	Yes or No
IRC Standards Review Committee	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Southern California Edison Company	Yes
SPP and specific Member companies	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes

Organization	Yes or No
PNM Resources	Yes
Hydro One	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Utility Services Inc.	Yes
NIPSCO	Yes
Portland General Electric	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes

Organization	Yes or No
Pacific Gas and Electric Company	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
New York Power Authority	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes

Organization	Yes or No
Texas Reliability Entity	Yes
ISO New England	Yes
City Utilities of Springfield, MO	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
California ISO	Yes
US Bureau of Reclamation	Yes

6. CIP-003-5 R3 states "Each Responsible Entity shall identify a CIP Senior Manager by name." Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
ACES Power Marketing	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
Florida Municipal Power Agency	No
Progress Energy	No
Southern Company Services, Inc.	No
Independent Electricity System Operator	No

Organization	Yes or No
Lakeland Electric	No
Tampa Electric Company	No
Illinois Municipal Electric Agency	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Texas Reliability Entity	No
City of Austin dba Austin Energy	No
Kansas City Power & Light	No
Network & Security Technologies, Inc.	No
American Public Power Association	No

Organization	Yes or No
Tucson Electric Power	No
Cowlitz County PUD	No
Brazos Electric Power Cooperative	No
California ISO	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
NRG Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC)	Yes

Organization	Yes or No
including OPC, GTC & GSOC	
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
Hydro One	Yes

Organization	Yes or No
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes
Portland General Electric	Yes
Trans Bay Cable	Yes
National Grid	Yes

Organization	Yes or No
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
City of Palo Alto	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Xcel Energy	Yes
Bonneville Power	Yes

Organization	Yes or No
Administration	
New York Power Authority	Yes
Tennessee Valley Authority	Yes
MidAmerican Energy Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
Wisconsin Electric Power Company	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
ISO New England	Yes
City Utilities of Springfield,	Yes

Organization	Yes or No
MO	
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

7. **CIP-003-5 R4 states "Each Responsible Entity shall review and obtain CIP Senior Manager approval for cyber security policies identified in Requirements R1 and R2, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals." Do you agree with the proposed Requirement R4?**

Summary Consideration:

Organization	Yes or No
NESCOR/NESCO	No
ACES Power Marketing	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
Florida Municipal Power Agency	No
Progress Energy	No
Edison Mission Marketing & Trading	No
Independent Electricity System Operator	No

Organization	Yes or No
Pattern	No
United Illuminating Company	No
Lakeland Electric	No
Tampa Electric Company	No
Tennessee Valley Authority	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
Ameren	No
NextEra Energy, Inc.	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
PJM Interconnection	No
Kansas City Power & Light	No

Organization	Yes or No
American Public Power Association	No
NYISO	No
Cowlitz County PUD	No
Brazos Electric Power Cooperative	No
California ISO	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
Texas RE NERC Standards Review Subcommittee	Yes
NRG Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes

Organization	Yes or No
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes

Organization	Yes or No
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
Hydro One	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes

Organization	Yes or No
Portland General Electric	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
Turlock Irrigation District	Yes

Organization	Yes or No
Xcel Energy	Yes
Bonneville Power Administration	Yes
New York Power Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Oncor Electric Delivery Company LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
City of Austin dba Austin Energy	Yes
ISO New England	Yes

Organization	Yes or No
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
US Bureau of Reclamation	Yes

8. CIP-003-5 R5 states "Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate and the date of the delegation, and approved by the CIP Senior Manager." Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No
NRG Companies	No
Duke Energy	No
Florida Municipal Power Agency	No
Progress Energy	No
Hydro One	No

Organization	Yes or No
Independent Electricity System Operator	No
Xcel Energy	No
Flathead Electric Co-op	No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper	No

Organization	Yes or No
Pennisula Power Company	
PJM Interconnection	No
City of Austin dba Austin Energy	No
ISO New England	No
American Public Power Association	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Cowlitz County PUD	No
California ISO	No
ACES Power Marketing	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes

Organization	Yes or No
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes

Organization	Yes or No
NIPSCO	Yes
Portland General Electric	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes

Organization	Yes or No
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Kansas City Power & Light	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield,	Yes

Organization	Yes or No
MO	
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

9. CIP-003-5 R6 states "Each Responsible Entity shall document any changes to the CIP Senior Manager or any delegations within thirty calendar days of the change. Delegation changes do not need to be reinstated with a change to the delegator." Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Texas RE NERC Standards Review Subcommittee	No
NRG Companies	No
Florida Municipal Power Agency	No
Progress Energy	No
Portland General Electric	No
Independent Electricity System Operator	No
Flathead Electric Co-op	No

Organization	Yes or No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
ISO New England	No
Kansas City Power & Light	No

Organization	Yes or No
American Public Power Association	No
Tucson Electric Power	No
Cowlitz County PUD	No
California ISO	No
ACES Power Marketing	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
Southwest Power Pool Regional Entity	Yes
Duke Energy	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric	Yes

Organization	Yes or No
Cooperative, Inc. (JRO00088, NCR01177)	
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes

Organization	Yes or No
Hydro One	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes
Trans Bay Cable	Yes

Organization	Yes or No
Pattern	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes

Organization	Yes or No
Xcel Energy	Yes
Bonneville Power Administration	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
Wisconsin Electric Power Company	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes

Organization	Yes or No
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards

Comment Form B

CIP-004 through CIP-007 Questions

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Index to Questions, Comments, and Responses

Questions with Summaries Included: 17
QUESTION B8 – CIP-004-5, R1, R2, R3, R4 or R5: 17
QUESTION B9 – CIP-004-5, R6 or R7: 22
QUESTION B12 – CIP-005-5, R1: 41
QUESTION B13 – CIP-005-5, R2: 52
QUESTION B17 – CIP-006-5: 55
QUESTION B23 – CIP-007-5, R1, R2, R3 or R4: 58
QUESTION B24– CIP-007-5 REQUIREMENT R5: 84
Questions with Votes Only: 94
1. CIP-004-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 94
2. CIP-004-5 R2 states "Each Responsible Entity shall have a role-based cyber security training program to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 101
3. CIP-004-5 R3 states "Each Responsible Entity shall implement its documented role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3? 109
4. CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4? 117
5. CIP-004-5 R5 states "Each Responsible Entity shall implement one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable elements in CIP-004-5 Table R5 –

Personnel Risk Assessment." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5? 125

6. CIP-004-5 R6 states "Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R6? 133

7. CIP-004-5 R7 states "Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R7? 141

10. CIP-005-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 149

11. CIP-005-5 R2 states "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 157

14. CIP-006-5 R1 states "Each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? .. 164

15. CIP-006-5 R2 states "Each Responsible Entity shall implement one or more documented visitor control programs that include each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 172

16. CIP-006-5 R3 states "Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3? 180

18. CIP-007-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 188

19. CIP-007-5 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 196

20. CIP-007-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3? 204

21. CIP-007-5 R4 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4? 212

22. CIP-007-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5? 220

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Bruce Metruck	New York Power Authority	NPCC	6
12.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
13.	Robert Pellegrini	The United Illuminating Company	NPCC	1
14.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
15.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
16.	Brian Robinson	Utility Services	NPCC	8
17.	Michael Jones	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Don Weaver	New Brunswick System Operator	NPCC	2
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3
24.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5

2.	Group	Annabelle Lee	NESCOR/NESCO									

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3.	Group	Jason Marshall	ACES Power Marketing					X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Tim Soles	Occidental Power Services, Inc.	ERCOT 3										
4.	Andy Gallo	Austin Energy	ERCOT 1										
5.	Andy Gallo	Austin Energy	ERCOT 3										
6.	Andy Gallo	Austin Energy	ERCOT 4										
7.	Andy Gallo	Austin Energy	ERCOT 5										
8.	Andy Gallo	Austin Energy	ERCOT 6										
8.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8. Annie Terracciano	Northern Lights Inc.	WECC 3										
9. Aleka Scott	PNGC	WECC 4										
10. Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11. Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12. Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13. Margaret Ryan	PNGC	WECC 8										
12. Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13. Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14. Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3. M & A Electric Power Cooperative			SERC 1, 3										
4. Northeast Missouri Electric Power Cooperative			SERC 1, 3										
5. N.W. Electric Power Cooperative, Inc.			SERC 1, 3										
6. Sho-Me Power Electric Cooperative			SERC 1, 3										
15.	Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X						
Additional Member		Additional Organization	Region Segment Selection										
1. Oglethorpe Power Corporation			SERC 5										
2. Georgia Transmission Corporation			SERC 1										
16.	Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X
Additional Member		Additional Organization	Region Segment Selection										
1. MAHMOOD SAFI		OPPD	MRO 1, 3, 5, 6										
2. CHUCK LAWERENCE		ATC	MRO 1										
3. TOM WEBB		WPS	MRO 3, 4, 5, 6										
4. JODI JENSON		WAPA	MRO 1, 6										
5. KEN GOLDSMITH		ALTW	MRO 4										
6. DAVE RUDOLPH		BEPC	MRO 1, 3, 5, 6										
7. JOE DEPOORTER		MGE	MRO 3, 4, 5, 6										
8. SCOTT NICKELS		RPU	MRO 4										
9. TERRY HARBOUR		MEC	MRO 1, 3, 5, 6										
10. MARIE KNOX		MISO	MRO 2										
11. LEE KITTELSON		OTP	MRO 1, 3, 4, 5										
12. SCOTT BOS		MPW	MRO 6, 1, 3, 5										
13. TONY EDDLEMAN		NPPD	MRO 1, 3, 5										
14. THERESA ALLARD		MPC	MRO 1, 3, 5, 6										
17.	Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing													
18.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				
Additional Member		Additional Organization	Region Segment Selection										
1. Timothy Beyrle		City of New Smyrna Beach	FRCC 4										
2. James Howard		Lakeland Electric	FRCC 3										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3. Greg Woessner	Kissimmee Utility Authority	FRCC	3										
4. Lynne Mila	City of Clewiston	FRCC	3										
5. Joe Stonecipher	Beaches Energy Services	FRCC	1										
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4										
7. Randy Hahn	Ocala Utility Services	FRCC	3										
19. Group	Joseph DePoorter	Madison Gas and Electric Company				X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Darl Shimko	MGE	MRO	3										
2. Joseph DePoorter	MGE	MRO	4										
3. Steve Schultz	MGE	MRO	5										
4. Jeff Keebler	MGE	MRO	6										
20. Group	David Thorne	Pepco Holdings Inc & Affiliates		X		X							
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Mark Jones	Pepco	RFC	1										
21. Group	Rick Terrill	Luminant						X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Mike Laney	Luminant Generation Company LLC	ERCOT	5										
2. Tim Soles	Occidental Power Services, Inc.	ERCOT	6										
3. Tim Soles	Occidental Power Services, Inc.	ERCOT	3										
4. Andy Gallo	Austin Energy	ERCOT	1										
5. Andy Gallo	Austin Energy	ERCOT	3										
6. Andy Gallo	Austin Energy	ERCOT	4										
7. Andy Gallo	Austin Energy	ERCOT	5										
8. Andy Gallo	Austin Energy	ERCOT	6										
9. Brenda Hampton	Luminant Energy Company LLC												
22. Group	Joe Tarantino	SMUD & BANC		X		X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Kevin Smith	BANC	WECC	1										
23. Group	Scott Brame	NCEMC		X				X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Rayburn Country Electric Cooperative			SPP										
2. Empire District Electric			SPP	1									
3. City Utilities of Springfield			SPP	4									
4. Westar Energy			SPP	1, 3, 5, 6									
5. Cleco Power			SPP	1, 3, 5, 6									
25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Pawel Krupa			WECC	1									
2. Dana Wheelock			WECC	3									
3. Hao Li			WECC	4									
27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Denise Lietz		Puget Sound Energy	WECC	1									
2. Erin Apperson		Puget Sound Energy	WECC	3									
28.	Group	Michael Mertz	PNM Resources	X		X							
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Laurie Williams		Public Service Co. of New Mexico	WECC	1									
2. Michael Mertz		Public Service Co. of New Mexico	WECC	3									
29.	Group	Sasa Maljukan	Hydro One	X									
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. David Kiguel		Hydro One	NPCC	1									
30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION B8 – CIP-004-5, R1, R2, R3, R4 or R5:

If you disagree with the changes made to CIP-004-5, Requirements R1, R2, R3, R4 or R5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the requirements, measures, and VSLs associated with Requirement R1, R2 R3, R4 or R5 of CIP-004-5. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Note

In draft two, Requirement R2 required a documented process for its role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems while Requirement R3 was the implementation of that process. Requirement R4 required one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems while Requirement R5 was the implemented of the one or more documented processes. In preparing CIP-004-5 for draft 3, the SDT determined that Requirements R2 and R3 could be combined, and so could Requirements R4 and R5. In that way, the requirements more closely match most other requirements in CIP-004-5 through CIP-011-5 to implement a documented process, and it also facilitated inclusion of the correcting deficiencies approach, explained in the common response section of this comment response, so that the resulting requirements, draft 3's Requirements R2 and R3, could be implemented "in a manner that identifies, assesses, and corrects deficiencies." Therefore, Requirement R6 from draft 2 was renumbered to Requirement R4 in draft 3, and Requirement R7 from draft 2 was renumbered as Requirement R5. For the purposes of the comment summaries and responses for this question, the requirement number references refer to the requirement numbers as listed in draft 2, unless otherwise noted.

General

The applicable systems section has been reviewed and revised to help ensure consistency within CIP-004-5 and with the other CIP standards. This should also make clear that these requirements are not applicable to Low Impact BES Cyber Systems. The SDT has decided not to include the concept of authorized unescorted electronic access. Individuals with

authorized electronic access must be trained and have a personnel risk assessment performed as per the requirements. This applies to all personnel including employees, vendors and contractors. For example, the question on a vendor controlled system would require the vendor to meet the requirements as set forth in CIP-004-5.

The SDT has stricken the "attain and retain" language for the training requirement, but has chosen to keep it for the personnel risk assessment requirements. The difference between those words and "acquire and maintain" are negligible.

The SDT does not agree with the suggestion to make Requirements R2 and R3 an expansion of the awareness program instead of training. The SDT believes that for protection of these BES Cyber Systems more targeted training is needed.

The guidelines and technical basis section has been updated to better align with the new draft content and organization. One areas of focus is the training content on networking hardware and software and other issues of electronic interconnectivity. More description around the criminal history check has also been added.

Requirement R1

The SDT has added language in the change rationale section to reinforce the concept that a registered entity does not need to ensure or prove all authorized personnel have received awareness. The language in R1.1 has also been revised to further clarify this point through the use of the word, reinforces. Also, the SDT has added language to clarify that awareness of cyber security practices can include physical security information.

The SDT appreciates the suggestions to allow the registered entity to define the timeline for awareness reinforcement or their own quarters, but believes the language is best retained as written for consistency.

In the measures for Requirement R1, the SDT has removed the reference to "documented security awareness program" and has modified the language to be consistent with the other CIP standards. The language, "not limited to" has also been revised and reviewed for consistency across the standards.

Requirement R2/Requirement R3

These two requirements have been combined into a single requirement which covers the training content in R2.1, in a single table, and the training frequency in R2.2 and R2.3. Another key change in R2 is the modification of the language to clarify that the registered entity is able to determine their training program(s) to fit their needs and it can be based on role, function or responsibility. In concert with this change, Table R2 section 2.1 was deleted to help eliminate the

language focusing on role based training. Training is required of individuals with authorized, unescorted physical access or authorized electronic access as per the revised R2.2 and R2.3. In addition to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity, the SDT believes training is also needed for individuals with access to Physical Access Control Systems and Electronic Access Control or Monitoring Systems. Also, the SDT has removed the reference to BES Cyber Systems in Table R2 formerly in sections R2.2, R2.3 and R2.4. For Table R2 previous section 2.5, the Change Rationale has been modified to reflect this is a new training requirement. Also, this training should be tracked for personnel involved in the visitor control process in accordance with Table R3 section 3.2 The SDT agrees that recovery plan information referenced in Table R2, previous section 2.8 should be labeled appropriately. The training content on cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets will remain in Table R2 as it is a new requirement from FERC Order 706 and the SDT has provided additional guidance to clarify the intent of this entry.

For Table R2, previous section 2.2, the SDT believes the training should be focused on policy content, not availability, and has made no changes. In Table R2, the SDT has chosen to retain both identification of incidents and response to incidents as separate content as the personnel who need to be trained on each may be different. The scope of training on recovery plans is left to the registered entity and no changes have been made to the standard. Also, the SDT believes the focus of recovery is the specific recovery plans, not the business impact analysis. The measure for Table R2 has been modified to focus on training material as evidence and the guidance has been revised to reflect the type of content this training should include.

The SDT has edited the language formerly in R3 for clarity with removal of the role based reference and the attain/retain language. Since there are no references to evidence retention in the requirement part 1.2, evidence retention, of the compliance section of the standard applies. The reference to documentation that was in Table R3 section 3.1 has been removed as it is covered in the measure.

The SDT does not agree that access to Low Impact Cyber Systems need the training defined in R2. Also, R2 has language included (in a manner that identifies, assesses, and corrects deficiencies) as suggested by some comments to allow detection and correction of flaws. The proposal to allow the registered entity to define the timeline for training was not supported by the SDT. For 2.2 and 2.3 (formerly in Table R3 section 3.2), the SDT believes the language is sufficiently clear that the time interval is between training dates and does not need that language added. BES Cyber Systems was changed to applicable cyber assets in 2.2. The two entries on initial and recurring training are now in Table R2. The SDT

has revised the language in the measure for these two entries to make it clear the focus is on training records which should include training date and date access is granted.

Requirement R4/Requirement R5

As suggested, the SDT has combined these two requirements into one and it is now Requirement R3. The SDT has modified the language formerly in Requirement R4 to help clarify that identity confirmation and criminal history check are part of the personnel risk assessment (PRA). The PRA is the outcome of the process or criteria used by a registered entity to evaluate the results of the identity verification (for the initial PRA) and seven year criminal history records check to determine what, if any, authorized access to grant to employees, contractors or vendors. The level of documentation for the process or criteria is left to the registered entity, but should be sufficient for a third party to understand how the decision is made. In defining the seven year criminal history records check, it is not the intent for the registered entity to evaluate the individual's residence locations, education or prior employment. The language has been revised to indicate the criminal history records check should cover locations where the individual has resided/lived for six consecutive months during the past seven years. The initial identity confirmation, even if performed under prior versions of the standards, is sufficient for the employment duration of the individual. The initial identity verification, criminal history check and PRA should be retained in accordance with requirement part 1.2 in the evidence retention component of the compliance section of the standard. A PRA performed under previous versions of the standards is valid until it reaches the end of its seven year lifespan. The intent of the SDT is that the PRA in effect is no older than seven years. The SDT has provided guidance on the acceptable documentation for an exception to the seven year criminal history records check which includes agreements with labor unions. If the registered entity is unable to fully complete the seven year criminal history records check, the SDT feels it is important to document the reasons for the exception so it will not be removing that piece of the requirement. Also, the timeframe for renewal of the criminal history records check is currently seven years and the SDT believes it should remain as such. Drug and alcohol checks are typically performed by entities under an existing program and the SDT chooses not to add this to the requirement. In section 3.3 of the new Table R3, the term process is used to define the method used by a registered entity to evaluate the results of the criminal history records check. Although a "Transportation Worker Identification Credential (TWIC)-like" program would be helpful to facilitate compliance with the PRA requirements, the SDT does not have the authority to make that happen. Measures – The Measures have been revised to focus on examples consisting of documentation. For example, a dated copy of the current PRA, which was performed in the previous seven calendar years, would be sufficient.

VRF/VSL

The language in the VRF for R2 has been changed to remove the reference to role based training. The SDT reviewed the VRFs for R3, R4 and R5 (as indicated above, R3 from draft 2 is now in R2, and R4 and R5 from draft 2 have been combined into R3 in draft 3) to consider if the rating should be a Lower risk factor. The SDT believes the risk associated with violations of these requirements is higher than for R1 and R2; hence the Medium risk factor is appropriate. The VSL for R1 has been modified to include the case where the Responsible Entity failed to implement on-going security awareness for two or more consecutive quarters as the next step above the criteria for High. Since the Medium severity level is for missing two content topics, the High should follow as three or more, not four or more. Commenters also asked whether the size of the company matters in the VSL for R3 (which is now in R2). In response, the SDT has modified the VSL for High and Severe according to the suggestion. The VSL targets the BES Cyber System and does not account for company size. Commenters suggested the Moderate and High VSL language for R4 (now R3) should be swapped on the basis that not performing an identity verification and a background check is worse than failing to document the results. (Also, the incorrect reference in draft 2's R4 to "4.5", which does not exist, has been corrected). In response, the SDT has modified the language for the Severe VSL to include the case where a registered entity failed to implement its PRA processes. Commenters also asked whether the size of the company matters in the VSL for R5 (which is now in R3). In response, the VSL targets the BES Cyber System and does not account for company size.

QUESTION B9 – CIP-004-5, R6 or R7:

If you disagree with the changes made to CIP-004-5, Requirements R6 or R7 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the major concerns with CIP-004 Requirements R6 and R7 center on removal of access privileges under various categories of termination actions. In addition, there were repeated instances noting a lack of clarity regarding access approvals, personnel transfers or reassignments and the proper storage and handling of NERC CIP information.

Note

In draft two, Requirement R2 required a documented process for its role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems while Requirement R3 was the implementation of that process. Requirement R4 required one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems while Requirement R5 was the implemented of the one or more documented processes. In preparing CIP-004-5 for draft 3, the SDT determined that Requirements R2 and R3 could be combined, and so could Requirements R4 and R5. In that way, the requirements more closely match most other requirements in CIP-004-5 through CIP-011-5 to implement a documented process, and it also facilitated inclusion of the correcting deficiencies approach, explained in the common response section of this comment response, so that the resulting requirements, draft 3's Requirements R2 and R3, could be implemented "in a manner that identifies, assesses, and corrects deficiencies." Therefore, Requirement R6 from draft 2 was renumbered to Requirement R4 in draft 3, and Requirement R7 from draft 2 was renumbered as Requirement R5.

Applicability Section

As in other Version 5 standards, in CIP-004, requirement part 4.1 (formerly part 6.1), there were several comments on changing instances of Medium Impact BES Cyber Systems to "Medium Impact BES Cyber Systems with External Routable Connectivity." Commenters also commented that "dial-up connectivity" should be removed from the applicability section to be consistent with the applicability sections of other Version 5 standards. In both of these cases, the SDT has revised the standard to reflect these comments.

Requirement R4 (formerly R6) General Comments

Multiple commenters recommended that new or additional items or items currently found in the rationale section should be modified and listed as requirements at the requirement level.

Comments suggested modification to allow for self-correction in certain cases, so that each responsible entity shall implement: measure performance to detect flaws; correct detected flaws expeditiously, and if needed take corrective action to prevent recurrence of flaws. This is a general requirement that applies to the Requirement R4 (formerly R6) sub requirements. Though not necessary from a procedural perspective, more instruction on what needs to be considered in the standards is better than insufficient information. The SDT has incorporated the correcting deficiencies modification to the implementation wording in CIP-004-5 in Requirements R2, R3 and R4.

Commenters recommended that the rationale discussing controls for BES Cyber Systems without user accounts should be added to the appropriate requirements in Requirement R4 (formerly R6). The SDT has moved that discussion from the rationale section to the requirement tables.

A commenter suggested that requirement parts 4.2, and 4.3 (formerly covered in parts 6.2, 6.3 and 6.4) be modified to include requirement parts 4.11, 4.12 and 4.13 (formerly parts 6.11, 6.12 and 6.13) along with part 4.1 (formerly part 6.1) in the requirement table. The SDT has combined requirement parts 4.2, 4.3 and 4.4, which now directly reference those sub-parts in part 4.1.

R4.3 (formerly 6.3)
Commenters recommended that there be a corresponding annual review of provisioned physical security privileges necessary for performing assigned work functions. The SDT has combined requirement parts 4.2, 4.3 and 4.4 (formerly parts 6.2, 6.3 and 6.4). The measures in the new requirement part 4.2 call for signed documents, automated workflow approvals or email showing persons with access have authorizations and similar or the same records showing the consideration of appropriate privileges on the basis of need…" These measures apply to electronic access, unescorted physical access into a PSP and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Part 4.3 (formerly part 6.5)
Commenters asked for clarification on the reviews of authorized and provisioned electronic access and unescorted physical access. The SDT has modified part 4.3 to clarify the requirement. It now reads "verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records."

R4 (formerly R6)

Some commented that the measures for 4.1 (formerly part 6.1) should include unescorted electronic access. The issue with this is that electronic access, by its digital nature cannot be escorted. Consequently, there is no "unescorted" electronic access. Electronic access to data or systems is either authorized or unauthorized. One could call it "supervised" access but the problem lies with a "supervisor" having to be continuously diligent and unerringly able to determine if the supervised user is doing anything malicious. This is not possible and frankly constitutes a threat to network integrity and data confidentiality. The recommended option would be to identify those contractors who require electronic access and run them through the personnel appraisal and the training processes and grant them appropriate access privileges. There are no other means to help ensure there are no unauthorized accesses or data disclosures.

Requirement Part 4.1 (formerly 6.1)

One commented that formerly sub-requirements 6.1.1, 6.1.2 and 6.1.3 (current 4.1.1, 4.1.2 and 4.1.3) would be clearer if the requirement was written, "Designate one or more individual(s) to authorize one or more of the following types of access". The SDT has changed the requirement to "have a process to authorize". This negates the need to specifically identify an approver and highlights consideration of "need" for physical access, electronic access and access to "designated" physical and electronic storage locations for BES Cyber System Information.

One commenter suggested that current requirement part 4.1 should include the names and roles of individuals who authorize the various types of access. The SDT has changed the requirement to "have a process to authorize". This negates the need to specifically identify an approver and highlights consideration of "need" for physical access, electronic access and access to "designated" physical and electronic storage locations for BES Cyber System Information.

One commenter recommended changing the term "designate" in current requirement parts 4.1, 4.2 and 4.3 (formerly parts 6.1, 6.2 and 6.3) to "identify.' The SDT has changed requirement 4.1 to "have a process to authorize". This negates the need to specifically designate or identify an approver and highlights consideration of "need" for physical access, electronic access and access to "designated" physical and electronic storage locations for BES Cyber System Information. The SDT has also combined 4.2, 4.3 and 4.4 into a single requirement (4.2).

Several commenters pointed out that access to physical and electronic locations where BES Cyber System Information is stored should have greater clarity around the word "physical". The requirement part 4.1 (formerly part 6.1) has been

changed to clarify storage locations for BES Cyber System Information. It now reads, "access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Several commenters recommended revising the phrase "unescorted physical access" to "unescorted physical access into a PSP." The SDT agrees and has made that change.

Multiple commenters stated that requirement part 4.1 (formerly part 6.1) should allow for roles in the designation of those individuals who can authorize the various accesses. The SDT believes that changing the requirement to "have a process" allows the entity the flexibility to construct their authorization process in a way that best suits their needs.

Requirement Part 4.2 (formerly Part 6.2)

Several commenters recommended that requirement parts 6.2 and 6.3 be revised for clarity. They proposed that requirement parts 6.2 and 6.3 be changed to read, "the individual(s) or role(s) designated in requirement part 6.1 shall authorize electronic access deemed necessary by the Responsible Entity, except for CIP Exceptional Circumstances." To respond to the comment, requirement parts 4.2, 4.3 and 4.4 have been combined into a single requirement part 4.2. At the same time, the individual authorization has been replaced with a process in requirement part 4.1. The process merely provides a means to authorize, and is implemented in the manner preferred by the Responsible Entity.

Several commenters also suggested that instead of the phrase "deemed necessary," "deemed appropriate" would be more accurate – stating that deeming appropriate is easier than deeming necessary. The SDT used the term "necessary…for performing assigned work functions" to better focus on specific accesses and minimize generalization and audit interpretation issues.

One commenter suggested the phrase "Responsible Entity" be removed from parts 4.2, 4.3 and 4.4 (formerly 6.2, 6.3, and 6.4). The requirements state "that the Responsible Entity determines is necessary." The SDT believes that the term "Responsible Entity" removes a degree of specificity that could be problematic if individuals change frequently or the determination of "necessary" is made by more than one individual within the organization. The SDT has combined requirement parts 4.2, 4.3 and 4.4 and has referenced a process required in part 4.1 "have a process" that allows flexibility to establish authorization frameworks tailored to the Responsible Entity's needs.

One commenter stated that the phrase "need to know" in requirement part 4.2 (formerly Part 6.2) is difficult to quantify and is subject to interpretation. They recommended removing that phrase, believing that approvers who grant all access

"deemed necessary" strongly indicates that determinations of need to know are part of the authorization process. The SDT has removed references referring to "need to know."

Many commenters recommended revising the phrase "unescorted physical access" to read "unescorted physical access into a PSP." For clarity, the SDT has changed the wording to "access into the Physical Security Perimeter."

One commenter stated that requirement part 6.3 (now covered under new part 4.1) implies that determination of need for performing work functions is needed for each physical access. They recommended that Responsible Entities document all roles and activities in advance, negating the need for the Responsible Entity restating access they have "determined is necessary." The SDT has combined the requirement parts 4.2, 4.3 and 4.4 and established a requirement for a "process" to develop an authorization framework best suited to the Responsible Entity's needs. This will allow the commenter's company to document all roles and activities in advance if that is the company's preference.

One commenter recommended removal of the phrase "for performing assigned work functions" due to concerns with potential interpretation requests. The SDT believes that since "work functions" are not subject to audits, there is no need to remove the conditional phrase. In addition, there must be some frame of reference for authorizing accesses and work functions are a logical baseline.

Many commenters suggested changing the wording of requirement part 6.4 (now covered under new part 4.1) from "location" to designated repository. The SDT believes that specifying a designated location is less subject to interpretation and in most cases exempts portable equipment from being identified as a "repository" in the event that NERC CIP information may be temporarily resident on such equipment. The SDT has retained the term "designated locations" since a location more often connotes multiple purposes. In contrast a repository, similar to location by definition, still carries connotations of a specified area, limited to a specific function. "Location" provides flexibility and designating locations removes incidental temporary storage on non-designated devices from the audit process.

One commenter questioned the following: Is the "intent of the requirement to track authorized access to the physical and electronic locations where BES Cyber System Information is stored. Is the requirement regarding physical location intended to include physical access to file servers hosting BES Cyber System Information in electronic format or is it intended to be limited to physical access to locations where BES Cyber System Information in stored in hardcopy format?" The SDT believes that unescorted physical access includes to both hard copy data and access to equipment used for storing electronic copies. Although physical proximity to equipment does not constitute electronic access, from

an information protection standpoint, access to that equipment could result in damage or destruction of those devices storing electronic copies.

One commenter suggested that in requirement part 6.4, (now covered under new part4.1)to eliminate ambiguity, that the term “necessary for performing assigned work functions,” be replaced with “appropriate for the roles and responsibilities.” The SDT understands the concern. In this case replacing “necessary” with “appropriate” does little to eliminate ambiguity. In addition, both terms are likely to prompt interpretations. Also, not all entities are configured to grant authorizations by roles and responsibilities. To address the entirety of the CIP affected population, the SDT believes that the original wording provides more universal applicability.

One commenter believes that requirement part 6.4 (now covered in new part 4.1) should be separated into two requirements. The first requirement would be to identify the repositories that store either physical media containing BES Cyber System Information (paper copy) or the electronic storage of BES Cyber System Information. The second requirement would be the authorization of access to only those designated repositories that have been identified by the entity. The SDT believes that using the term “locations”, as long as they are “designated” serves the same purpose as an identified repository. Because “designated” has been added to the requirement, so must a measure to acknowledge the existence and itemize “designated storage locations.” This will add another measure but will also reduce the potential for audit interpretation and ambiguity.

One commenter recommended that the words “are necessary for performing assigned work functions” be replaced simply with “are necessary”. The SDT believes that this revision, although more economical, could create a situation where the question is asked “necessary for what?” To avoid that possibility “necessary for assigned work functions” is less likely to prompt questions of scope of authorizations.

One commented that the words “physical and” should be removed because it imposes a requirement to create physical access controls and authorization processes to an office that may have a printout of Cyber System Information. The SDT notes that if, as suggested by a number of other companies, “designated locations” are used, incidental, non-designated temporary locations of NERC CIP System Information will not be subject to that requirement.

Former Requirement Part 6.3

Former requirement part 6.3 prescribed specific ways to conduct authorizations and referenced individuals designated in former part 6.1. The SDT has instead changed the language in part 4.1 to require the Responsible Entity to "Have a process to authorize . . .", which could certainly include designating one or more individuals, etc., as part of the process, but the requirements do not specifically prescribe the administrative method of achieving the required performance. Thus, former Requirement Part 6.3 no longer exists in the same manner as presented during draft 2.

Several commenters stated that because of potential minor errors or mismatches associated with the required review of authorizations and provisioned individuals, requirement part 4.3 (formerly part 6.5) should be subject to the FFT process. The SDT understands the concern, but FFT is not a function of the requirement. That is a function of potential violations and determined after the fact, not in the standard requirement itself.

One commenter recommended that the following statement from the rationale for requirement part 4.3 (formerly part 6.5) be entered into the requirement or its Measures section: "If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement." While that statement offers some clarification in guidance, the SDT cannot add a requirement or measure that makes a determination whether or not a particular error is a violation.

One commenter stated that requirement parts 4.3 and 4.4 (formerly parts 6.5 and 6.6) are major scope expansions which were not directed by FERC. They further claim that the requirements overlap and are not contributing to a commensurate improvement to security. The SDT believes that reviews such as those in parts 4.3 and 4.4 (formerly parts 6.5 and 6.6) do in fact provide a means to identify indicators of malicious activities, rogue accounts, retained accounts that are no longer authorized, etc. The fact that FERC did not direct the requirement development does not negate the validity or the need for the requirements.

Several commenters recommended adding "currently" between "individuals provisioned". The SDT agrees with the recommendation and will take appropriate action. The SDT has reworded the requirement part 4.3 (formerly part 6.5) to "individuals with an *active* electronic access…"

One commenter stated that requirement part 4.5 (formerly part 6.7) should be revised as follows, “Verify, at a timeframe that the Responsible Entity deems necessary, that individuals provisioned for authorized electronic access or authorized unescorted physical access have associated authorization records.” The SDT believes that there must be a specified review period and associated evidence to ensure that Responsible Entities consistently meet the requirement.

One commenter suggested adding the words "to BES Cyber Systems" after the words "physical access" in part 4.3 (formerly part 6.5). The SDT believes this proposed revision is already addressed in the Applicable Systems section of the requirement.

One commenter suggested that in the measures section, there should be consistency of word order between "dated document of verification..." and "documentation of dated verification”. The first measure asks for “dated documentation of verification,” which simply provides a point in time wherein the verifications were performed. The second measure requires a document that provides times of specific verifications themselves, of authorization for access and provisioning of access. The SDT changed the language to provide clarity and consistency to the measure. The consistent language now reads, “dated documentation of the verification.”

Requirement Part 6.4

One commented that the measures in requirement parts 4.4 and 4.5 (formerly parts 6.6 and 6.7) contain contradictory constructions. The background section states that a numbered list includes all required evidence. In the measure, however, these parts state that evidence “may include, but is not limited to.” The SDT has added the phrase “that includes all of the following” to reconcile the format with the intent of the measure.

Several commenters stated that the wording in requirement part 4.4 (formerly part 6.6) is too prescriptive, specifically “verifications that all user accounts, user account groups, or user role categories and their specific associated privileges.” They proposed substituting that wording to read, “verifications that BES Cyber System access privileges are appropriate for the individual(s) or role(s) responsibilities.” The SDT believes that the word appropriate is too vague and subject to interpretation. The goal is to verify access to specific accounts. In this case, the existing wording maintains the scope and leaves no ambiguity around which accounts require verification. Regarding the list of measures, the SDT has revised the measure by adding “that includes all of the following” to reconcile the format with the intent of the measures.

Several commenters stated that the measures should only require verification that the entity performed the verification while leaving the results of the verification out of the measure. The SDT believes that requiring verification should

specify those items to be verified. Asking for a "listing of all accounts/account groups", a "description of privileges", "accounts assigned" and 'verification that privileges are authorized and appropriate" does not expand scope. Confirming that "verification" was performed would assume that all registered entities would perform the verification on the same lists of required items. If the items are not articulated, there are no assurances that the data would be consistently derived or complete.

One commenter recommended changing the words "performing assigned work functions" to "are appropriate". The SDT believes that the use of appropriate to define specific standard provisions is too vague and subject to interpretation.

One commenter stated that the scope of requirement part 4.4 (formerly part 6.6) has been expanded above and beyond what has been directed by FERC. The SDT has taken very positive steps to meet the requirements of the FERC directives. In establishing some requirements, the only way to effectively validate that the provisions have been met is to identify the need for specific information that links the requirement to the compliance actions. There may be an increased number of these instances. The important factor is that FERC directives do not limit the detail of the required evidence. The SDT believes that the requirement and measures increase the level of security. Unauthorized, expired or mis-assigned access to BES Cyber Systems represents potential vulnerabilities that could be exploited if not addressed with these administrative requirements.

One commenter also recommended that the wording of the "annual requirement" be worded as follows, "once each calendar year of a period not to exceed 15 calendar months between verifications." The SDT has changed the requirement to read "once every 15 calendar months to incorporate the additional 3 months of previously discretionary time directly into the requirement."

One commenter believed that the word "all", referring to user accounts is too broad. Dominion suggested that the word "applicable" be added after "all" to point to those user accounts, etc that are directly associated with the requirement. The SDT has changed the requirement to read "user accounts on all applicable cyber assets" to maintain the appropriate scope of the requirement.

One commented that requirement parts 6.6 and 6.7 should be revised to allow responsible entities to perform verifications of user accounts, user account groups or user role categories and their specific associated privileges at "a timeframe that the Responsible Entity deems necessary." NextEra also suggested that this also applies to verifying "access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity

are correct…" Although there are a number of companies that would comply with the requirement according to its intent under a self-imposed timeframe, there is no way to ensure that this would be the case. The SDT feels that the annual requirement should remain in place to help ensure consistent compliance actions.

Several commenters recommended changing requirement parts 6.6 and 6.7 to remove "all" referring to reviews of user accounts, user account groups, or user role categories. They recommend replacing "all" with "BES Cyber Systems." The SDT believes that reviews should be performed only on applicable cyber assets. The requirement has been revised as follows: "that user accounts on all applicable cyber assets, user account groups, etc.

Some commenters also commented that "locations" in requirement parts 6.4 and 6.7 should be replaced with designated repositories and include a requirement to list the repositories. The SDT has reworded the requirement to read "designated storage locations for BES Cyber System Information, whether physical or electronic." It has also added a requirement to designate storage locations and a measure to provide a list of designated storage locations. This will remove incidental temporary storage on non-designated devices from the audit process.

Some commenters suggested that the language in the second measure, "A summary description of privileges associated with each group or role", be removed. The SDT believes that understanding the privileges associated with specific roles is a necessary data point for verification that the privileges for specific groups are authorized and appropriate for the work functions performed by those assigned to the groups.

Requirement Part 6.5

Many commenters suggested in some manner to move former parts 6.1, 6.4, 6.7, and 7.3 (now, collectively, parts 4.1, 4.5, and 5.3) into CIP-011. In response, the SDT has revised former parts 6.1 and 6.4 to require a process without specifying how to conduct the authorizations. The SDT notes that CIP-004-5's authorization requirements relate to individuals' access, while CIP-011-1 specifies the information protection requirements.

Some commenters expressed concerns that the measures of requirement part 4.5 (formerly part 6.7) do not need to include the phrase "the minimum necessary for performing assigned work functions." In response, one of the most important aspects of authorizations and privileges is that they be granted using a "least privilege" approach. Otherwise the possibility exists that authorizations are provided or maintained for individuals who do not need them based on expediency rather than a comprehensive review.

One commenter suggested removing the term “minimum” from the third measure of Part 4.5 (formerly part 6.7) since it was removed from the requirement. The SDT agrees with this suggestion and has revised the measure accordingly.

One commenter recommended that the word “privileges” be added to part 4.5 (formerly Part 6.7) after the word “access.” The proposed wording of the requirement would be “verify at least once per calendar year, but not to exceed 15 calendar months between verifications, that access privileges to the designated physical and electronic repositories where BES Cyber System Information is stored by the Responsible Entity are correct and those that the Responsible Entity determines necessary for performing assigned work functions." The SDT concurs with this addition since it adds clarity to the requirement. It has added “privileges” to the requirement. In a related recommendation, another commenter suggested the word “privileges” be removed from the measure since it is not in the Part 4.5. Adding the word privileges as discussed above will alleviate those concerns.

Some commenters recommended removing requirement parts 4.4 and 4.5 (formerly parts 6.6 and 6.7) because they are too prescriptive in their attempt to accomplish requirement part 4.3 (formerly part 6.5). The SDT believes that verification of requirement part 4.3 hinges upon the existence and validation of requirements listed in 4.4 and 4.5.

One commenter also questioned whether a listing of authorizations is the same as a list of those with access. Authorizations provide a type of eligibility for access. A list of those with access may include someone without that authorization and a potential security issue. That is why the reviews of authorizations, access and privileges are critical to compliance with the standards requirements.

Requirement R5 (Formerly R7) Applicability Section

A few commenters suggested that the applicability of revocation requirements in CIP-004-5 R5 (formerly R7) for interactive remote access should be modified to exclude dial-up connectivity. In response, the dial-up connectivity reference is removed from CIP-004-5 in its entirety.

Commenters also recommended that applicability to “Medium Impact BES Cyber Systems” be limited to those with “External Routable Connectivity” to maintain consistence with other cyber systems/assets currently covered by similar requirements in CIP-004. External Routable Connectivity has already been added to the applicability section for CIP-004.

Requirement R5 (Formerly R7) General Comments

Several commenters expressed concern on requirement part 5.2 (formerly part 7.2) for transfers and reassignments. They believe that the timing of access removal should be based on the determination of when access is no longer necessary, rather than limiting it to a specific time frame related to the transfer or reassignment date. The SDT has revised part 5.2 (formerly part 7.2 as follows: "For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access".

For requirement part 5.1 (formerly part 7.1), a commenter suggested that part of the FERC Order 706 be more clearly reflected in the requirements. Specifically they would like documentation in the requirement that highlights FERC's statement that exceptions to revocation policy are allowed as long as they are properly documented for audit purposes. Paragraph 462 of Order 706 states that, "revocation should be immediate upon the employee's notification of any personnel action requiring revocation of access. However, the ERO may define what circumstances justify an exception that is other than immediate and determine what is the fastest revocation possible." In response, this is not a SDT issue. Creating exceptions for directives in a FERC Order is a separate process undertaken by the ERO. In any event, it is not simply a documentation requirement. Circumstances warranting exceptions have to be identified and then approved. This of course is done against a backdrop of "immediate" revocation stated in the order.

A few recommended that the requirement for revocation based on the "next calendar day" should be changed to "next business day." Another commenter proposed that "next calendar day" be replaced by "within 24 hours." The SDT believes that next business day does not fall under the intent of the FERC Order Directives. Next business day if a weekend or holiday period is in progress could extend the revocation process for two or three additional days. "Within 24 hours" is actually less time than is allowed by the "end of the next calendar day." For the purposes of these comment responses, the SDT feels that next calendar day best meets the FERC Order directive and provides better security than next business day.

Some commenters also expressed concern that the 24 hour revocation requirements may not realistic given numerous and diverse HR and IT processes throughout the industry. Essentially they, along with one other commenter, advocated returning to a framework that allows different time frames for different types of termination actions. The SDT has revised the requirement to state that there must be a process to initiate removal of an individual's ability for unescorted physical access and interactive remote access. This is based on the premise that removal of the ability for access may be different than deletion, disabling, revocation or removal of all access rights. Considering that what is required is initiating

a process (which may allow for internal processes that serve as trigger points) at the time of the termination action and completing the process within 24 hours, the SDT believes this is a reasonable time frame.

Requirement Part 5.1 (formerly 7.1)
Commenters recommended that the criteria for termination action timeframes should include a reference to the communication of the intention to terminate to provide a type of time stamp for gauging compliance with related requirements of the standard. While the communication of a termination action is not mentioned specifically in the requirement, initiating the process required by requirement part 5.1 (formerly part 7.1) would probably include those trigger points for individual companies. This allows greater flexibility and more concise monitoring of the required timeframe.

Several commenters expressed concern with the format of the measures in Requirements R4 and R5 (formerly Requirements R6 and R7). They are concerned that the background section states that all numbered lists in the measures are all required evidence. However, the measure list states that the "evidence may include but is not limited to." The SDT has revised the measures by adding the following statement: "An example of evidence may include, but is not limited to *documentation of all of the following*: This sentence is followed by numbered measures. This is primarily a formatting issue and this revision should alleviate the discrepancy.

One commenter suggested that the requirement should include "disable or revoke all individualized domain user accounts held by the terminated staff." The SDT believes that removing unescorted physical (preventing any entry into an entity's facilities) and interactive remote access should prevent any further access by the individual after termination.

Some commenters stated that requiring access revocation within 24 hours for all types of terminations is overly burdensome. They believe the 24 hour requirement should be limited to "for cause" terminations with additional flexibility built in for other situations. Other commenters recommended that the 24 hour time frame should apply only to High Impact Assets. The SDT has revised the requirement to state that there must be a process to initiate removal of an individual's ability for unescorted physical access and interactive remote access. This is based on the premise that removal of the ability for access may be different than deletion, disabling, revocation or removal of all access rights. Considering that what is required is initiating a process (allowing for internal processes) at the time of the termination action and completing the process within 24 hours, the SDT feels this is a reasonable time frame.

A few commenters stated that requirement parts 5.1 and 5.5 (formerly parts 7.1 and 7.5) seem inconsistent regarding shared user accounts. The SDT sees no inconsistency and believes that the current requirements are clear and sufficiently differentiated. Requirement part 5.1 considers the first tier of access; unescorted physical and interactive remote electronic access. Requirement part 5.5 specifies changing passwords for shared accounts and provides a 30-day time frame for its completion.

One commenter recommended a change to part 5.1 formerly part 7.1) that changes the 24 hour requirement to the end of the next business day after the effective date and time of the termination action. The SDT believes this falls outside of the FERC Directive intent, particularly as it applies to the "next business day." The next business day could increase the access revocation time frame to well over the 24 hours currently stated in the requirement.

One commenter recommended that requirement parts 5.1 and 5.3 (formerly parts 7.1 and 7.3) be revised to include a statement on extenuating circumstances associated with the impact of completion of revocation within 24 hours. FERC has allowed "extenuating operating circumstances" which have a specific application in requirement part 5.5 (formerly part 7.5), due to the complexity and scope of the password change task. Extenuating circumstances outside of that definition are undefined and could be misconstrued as any circumstance that is perceived as an impediment to completion of the requirement. In addition, adding "extenuating circumstances" to these requirements could set a precedent for other requirements, negating the timeliness and effectiveness of underlying security intent.

One commenter suggested clarifying language to the wording of the requirement to make it clear that the 24-hour clock is related to the initiation of the termination process, not the complete termination actions themselves. The SDT has clarified that there must be a process to initiate removal of an individual's ability for access. Initiation of the process must be concurrent with a termination action. Completion of the removal is required within 24 hours of initiating the process.

One commenter believes that termination criteria should vary according to the situation. They would like the tightest timeframes reserved for terminations for cause. The SDT has maintained the 24 hour requirement for termination actions based mainly on the FERC 706 Order requirement that termination be executed immediately.

One commenter commented on a situation where a suspended individual is terminated ten days from the suspension date. While the termination action was initiated in compliance with the requirements of R5 (formerly R7), the effective date of the termination shows up in the records as 10 days prior to the action being initiated. The SDT believes that in

these situations, documentation of the suspension along with what a suspension entails regarding any network or system accesses, and a documented company statement verifying the entities suspension procedures and subsequent termination should be sufficient to provide evidence of compliance to an auditor.

Requirement Part 5.2 (formerly 7.2)
Many commenters are concerned about the 24 hour requirement for removal of access for those individuals transferred or reassigned. The SDT understands the issue with access often being required after the transfer for various lengths of time. Rather than specify numbers of days within which an entity must complete the reassignment or transfer activities, the SDT has reworded the requirement to the following: "For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access."

One commenter would like reassignments or transfers based on the notification of reassignment or transfer. Rather than specify numbers of days within which an entity must complete the reassignment or transfer activities, the SDT has reworded the requirement and proposes the following changes: "For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

Requirement Part 5.3 (formerly 7.3)
A few commenters requested clarification on physical access to BES Cyber Systems and storage requirement wording in general. The requirement specifies that the access applies to those "designated physical and electronic locations where BES Cyber System Information is stored." In the requirement the term "designated" has been added. For the measures, evidence includes workflow or sign-off forms verifying access removal to "designated" physical areas or cyber systems. The term designated removes the unintended consequence of BES Cyber System Information temporarily resident on work stations, laptops, flash drives, etc. These areas are consequently not identified as storage "locations."

Some commenters suggested replacing the words "by the end of the next calendar day" to "within 7 days" or 30 days, respectively in the requirement. The SDT believes that since access removal in requirement part 5.1 (formerly part 7.1) will in many cases, constitute removal of access to BES Cyber System Information, that this requirement should retain its

original wording. In addition, in FERC Order 706, Paragraph 386 requires that there be "prompt revocation of access to protected information." Seven or 30 days would not be considered "prompt" by FERC.

One commenter commented that "next calendar day" for removal of access to BES Cyber System Information is too short a time span. The SDT points out that FERC Order 706 dictates prompt removal of access. The phrase "next business day" for example could mean substantially longer time periods over weekends and some holiday periods.

One commenter recommended the use of the word "repository" over "locations" in the requirement. The word "location" was chosen by the SDT to ensure there was no ambiguity within the requirement. Location is considered a general area, with multiple uses and is not limited to a specific function. A "repository" on the other hand, connotes specific use…for storage of BES Cyber Security Information. The use of location will help avoid any tendency toward requiring exclusivity of purpose and preclude potential violations.

One commenter commented that locations should be changed to designated repositories. The SDT believes that specifying a designated repository is less subject to interpretation and in most cases exempts portable equipment from being identified as a "location" in the event that NERC CIP information may be temporarily resident on such equipment. The SDT has retained the term "designated locations" since a location more often connotes multiple purposes. In contrast a repository, similar to location by definition, still carries connotations of a specified area, limited to a specific function. "Location" provides flexibility and designating locations removes incidental temporary storage on non-designated devices from the audit process.

Requirement Part 5.4 (formerly 7.4)

Some commenters would like to expand the applicability of requirement part 7.4 to include Medium Impact BES Cyber Systems. The SDT has carefully weighed the applicability of requirement parts throughout the family of Version 5 CIP standards, and, on balance, it believes that the levels of protection for Medium Impact BES Cyber Systems in other requirement parts throughout CIP-004-5 provide an appropriate balance in applying impact-based protections that are graduated between High Impact BES Cyber Systems and Medium Impact Cyber Systems.

One commenter suggested a revision for recovery of all information copied from repositories. The SDT notes that the requirements set out the requirements that must be part of the required processes. The SDT believes that the information protections in CIP-011-1 and the access requirements in CIP-004-5 adequately serve the purpose of protecting BES Cyber Systems while allowing sufficient flexibility to entities in implementing their processes or programs.

A few commenters recommended changing “Requirement parts 5.1 and 5.3 (formerly parts 7.1 and R7.3)” to “Requirement R5, Parts 5.1 and 5.3 (formerly R7 Parts 7.1 and 7.3.”)They also recommended changing the word “removal” to “revoke” for consistency with the requirement. Another commenter also suggested changing “revoke” to either remove or disable. In some systems removal results in removing all corresponding records which makes it hard to provide the proper records to the auditor. The SDT has retained “removal” in part 5.1 along with a clarification which is provided in the requirement language. The SDT retained the term “revoked” in part 5.3 to conform to the overall R5 Requirement.

One commented that the phrase "revoke individual users accounts on BES Cyber Assets" should be changed to "revoke individual access to BES Cyber Assets." The commenter believes that this is an important distinction because most field BES Cyber Assets do not have individual user accounts. In the utility field environment many brands and models of devices are being used. For those that do have individual user account capability, they are often not used because most BES Cyber Assets cannot be centrally managed. Since the process of revoking access privileges on each device can take up to a year or longer because it requires a site visit to each asset and for system with a significant number of assets which also covers a large geographic area that effort in combination with the necessary equipment outage to make the change introduces new reliability risks to the BES. It is more common for the commenter’s field organizations to place other access control devices in front of such field devices. These other devices can be centrally managed. So access is controlled to the device rather that by the device itself. Field Example: Protective Relays - Most do not have individual user accounts. Many also do not have the capability to allow central access control management. Because they don't have user accounts the only way to revoke access on the devices is to change the passwords for all access levels. This means logging on to many hundreds to possibly thousands of relays to change passwords. Because access to the relays to change passwords opens the relay at the change level, it presents an increased risk to the BES because it requires a physical equipment outage to make the change resulting in many more outages impacting potentially the state of the BES and once access is granted, one can change any type of setting on the relay. It certainly could not be accomplished in 30 days. Access can be revoked to these assets by revoking the Central Electronic Access Privileges that allow access through the access control devices to the assets. This coupled with physical access revocation (both of which can be centrally managed) provides complete revocation of access to the assets. This can be accomplished a very short time.

One comment suggested that in CIP-004 R5.4 (formerly R7.4): “For Termination actions, revoke the individuals user accounts on BES Cyber Assets…” to, for termination actions, revoke the individuals access to BES Cyber Assets…” The SDT has modified part 5.4 to read, “for termination actions, revoke the access to individual’s user accounts (unless already

revoked in accordance with requirement parts 5.1 or 5.3) (formerly parts 7.1 and 7.3) within 30 calendar days of the effective date of the termination action."

Some commenters disagreed with the statement that the word "revoke" in this case means to "delete" the user account from the system. We would disable the account and possibly change the account password but when you delete a Windows account you can never reclaim the original Globally Unique Identifier (GUID that Windows assigns to the unique account. Therefore, reporting, file ownership and anything relating to the GUID will have been lost and difficult to track past account activity. This may be true for other operating systems as well. If disabling their domain accounts and physical access effectively terminates access, do we still need the urgency of 24 hrs? I understand the logic behind this but would rather see this as a 30 day requirement. The SDT has used the term revoke to essentially make an account "inactive". It does not delete the account. Also, requirement part 5.4 has been modified in the "Applicable Systems" section. It now includes only "High Impact BES Cyber Systems and Electronic Access Control or Monitoring Systems that are associated with High Impact BES Cyber Systems." Further, the requirement allows revocation of individual's user accounts within 30 days of the effective date of the termination action.

One commenter questioned that since there is no requirement for revocation of balance of access in 5.4 (formerly part 7.4) for Medium Impact BES Cyber Systems, is there a particular timeline required? The commenter recommended that a timeline be developed that provides auditable records for removing balance of access. In response, the SDT notes that requirement part 5.4 in the applicable systems does not include Medium Impact BES Cyber Systems. Under those circumstances the audit process would not be considering Medium Impact balance of access.

Requirement Part 7.5

One commenter points out that requirement part 5.5 (formerly part 7.5) only accounts for the 30 days within the requirement and not the 10 days after "extenuating operating circumstances". The SDT has provided measure in part 5.5 to cover that previous omission.

One commenter suggested that the second bullet of the example evidence for requirement part 5.5 (formerly part 7.5) should be clarified that password reset is only required if the individual being transferred no longer needs such access in the new position or role. In response, the SDT has modified the measures to clarify that password resets must be completed within 30 days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

One commenter recommended that requirement part 5.5 (formerly part 7.5) be revised to include both terminations and reassignments or transfers. The SDT has added part 5.5 to the requirement to cover the reassignments and transfers.

One commenter suggested that the quarterly review should be converted to a quarterly “cleanup” of individual user accounts and not be considered a violation, and the SDT notes that that a cleanup could certainly a way of identifying, assessing, and correcting any deficiencies, which now modifies “implement” in the main requirement (see summary response to common issues at the beginning of this document), and for that reason, the required performance of the requirement remains a review.

One commented that if an entity can determine and document that extenuating operating circumstances require a longer time period for changing passwords; it should also apply to allow the Responsible Entity to determine and document that extenuating operating circumstances that can require a longer time period for revocation of access privileges. The SDT believes that since revoking physical and interactive remote (tier 1) access is typically a centralized and relatively uncomplicated process, that the time frames for completion are adequate. In addition, the FERC Order 706 requires “immediate” revocation of access. Providing a conditional caveat “for extenuating operating circumstances would in all probability meet with FERC resistance and result both in subjective application and interpretation.

One commenter questioned the need to modify passwords for shared user accounts if there is no corresponding requirement to disable individual accounts for the user who was reassigned or transferred. Additionally, as passwords are not a required authentication mechanism, we recommend that this requirement be modified to "change any shared authentication factors that are known." The SDT has revised requirement part 5.5 (formerly part 7.5) to accommodate reassignments and transfers as well as termination actions. Requirement part 5.5 reads, “For reassignments, or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.”

QUESTION B12 – CIP-005-5, R1:

If you disagree with the changes made in CIP-005-5, Requirement R1 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to CIP-005-5 Requirement R1.

General Comments

One commenter suggested that the communications links between ESP's should be included and that all the External Routable Connectivity exclusions should be eliminated. In response, all BES Cyber Systems have been included within the scope of Version 5 and the blanket exemption filter in CIP-002-5 has been eliminated. The ERC filter is now used on individual requirements where routable connectivity is either needed to meet the intent of the requirement or in general there is insufficient risk from other forms of communication to enforce a mandatory and auditable requirement upon every instance in every registered entity. Communication links have been excluded from this body of standards from the beginning as it is a cyber asset focused standard, and the vast majority of cyber assets used in communications between ESP's are not within the control of the registered entities but are leased services from telecommunication providers.

A few commenters requested clarity around the inclusion of serial devices and another commenter also requested specific clarification concerning the extension of ESPs over large areas via serial communications along with a request for clarification of 'direct serial' used in the guidance. In response, the SDT has focused on the communications requirements of the standards for the highest risk forms of communication – routable protocol networks and public switched telephone network (PSTN) accessible dial-up connections. It is a vital point that all BES Cyber Assets, including all serial devices, are included in the standards and are subject to all the requirements in CIP-003-5 to CIP-011-1 except those where they are specifically excluded. CIP-005-5, however, is focused on those two higher risk forms of connectivity and do not have mandatory requirements on serial, non dial-up forms of communication. As to the extension of ESPs over large areas via serial communications, the SDT notes that ESPs are for routable communication only and the SDT does not envision single BES Cyber Systems being defined in such a way that large geographical areas are involved. It is envisioned that a BES Cyber System would encompass cyber assets at a single site only – larger systems would be broken

at least into smaller systems by site. For example, a registered entity would not define all the components of an EMS including all field Remote Terminal Units (RTUs) as a single BES Cyber System. The components of that system at each location could be grouped together as the BES Cyber System for that location. Registered entities have great flexibility in their declaration of a BES Cyber System, but need to take into account ESPs and PSPs as well as all other applicable requirements as they do so. In response to the 'direct serial', that is used in the guidance as a term that refers to serial communications that is not routable protocol or dial-up in nature.

One commenter stated that clarity is needed concerning how wireless networks are impacted by CIP-005-5. In response, the SDT notes that these standards are at a higher and logical level and stay above the transport level. The SDT concentrated on protecting the BES Cyber Systems regardless of the physical transport in order to state the goal and also to future-proof the standards against an ever increasing variety of transports. Adequately addressing more detailed technical aspects would require standards per transport. However, the SDT does note that the radio/access point of a wireless network should be considered by the Responsible Entity to see if it should be included as an EAP.

Introduction Section

There was a comment that in the introduction section concerning exemptions (4.2.4) there is a reference to CIP-002-5 that should be CIP-005-5. In response, the SDT has made the change.

Background Section

One comment stated that the applicability of the background section does not address High Impact BES Cyber Systems with External Routable Connectivity and this is used in the standard. In response, the SDT agrees and has added the appropriate language which reads, "**High Impact Protected Cyber Systems with External Routable Connectivity** – Only applies to High Impact Protected Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the Protected Cyber System that cannot be directly accessed through External Routable Connectivity."

One comment read that Medium Impact BES Cyber Systems at Control Centers should be "associated with" instead of "located at". In response, the phrase 'located at' is used to appropriately limit the scope as the case could be made that

every Cyber Asset is ultimately 'associated with' a control center and could inappropriately identify every Cyber Asset as high impact.

One commenter stated that the section concerning Medium Impact BES Cyber Systems with External Routable Connectivity have the last sentence be deleted as it requires not treating the cyber system as one system, but as individual Cyber Assets. In response, there are several requirements (CIP-007-5 in particular) that do apply at the individual cyber asset level within a system and this sentence clarifies that for those requirements only those cyber assets within a system that have external routable connectivity are in scope if the requirement has this applicability.

Requirement Part 1.1

Many commenters commented that the applicability should include the ERC filter and thus remove the applicability language from the requirement itself and also make it parallel with R1.2, potentially even combining R1.1 and R1.2 into one. In response, the two requirements are purposely not parallel. R1.1 requires an ESP (a *logical* border) around every routable protocol network that contains a BES Cyber System even if it is an isolated network and has no external connectivity. The logical border (ESP) is used then as a boundary to define the 'associated Protected Cyber Assets' and raise the impact level of the included Cyber Assets to the 'high water mark' of the highest impact level system in the ESP. R1.2 is an additional requirement for those networks that have external routable connectivity to protect that external connectivity. In essence, Requirement R1.1 is the "identify your associated PCA's and adjust your impact levels" requirement. R1.2 is where external routable connectivity comes in and the logical border becomes more physical with the requirement of Electronic Access Points (EAPs).

Many commenters responded that the applicability needs to be removed from the requirement and the measure. Others commented that Associated Protected Cyber Assets should be included in the applicability as well. In response, the SDT has added the Associated Protected Cyber Assets to the applicable systems column.

There was one comment which stated that documentation on ESP's on isolated networks provides no reliability benefits. In response, the standards are concerned with all threat vectors, not just those originating from external networks. Portable media and insiders are two of many other threat vectors that can reach isolated networks. The SDT feels that knowing what all other network neighbors are on even isolated routable protocol networks containing a BES Cyber

System (the 'Associated Protected Cyber Assets') does have a reliability benefit. The logical border concept of the ESP also defines a 'trust zone' where all Cyber Assets sharing a network with a BES Cyber System need to be protected to equal levels, even on isolated networks.

One commenter stated that the measure should allow for documentation at the BES Cyber System level rather than the individual component level. In response, the SDT agrees and has made a change to the measure to allow documentation at either level.

One commenter requested clarification on whether ESPs are required for EACMs and PACMs. In response, the SDT clarifies that ESPs are not required on EACMs and notes that EAPs are EACMs and the standard avoids recursive effect of requiring ESPs around the cyber assets on the ESP. As for PACMs, the SDT notes that without an ability to make a distinction between "field-devices" (i.e. door readers, etc.) and "central servers", requiring ESPs would be problematic. The intent for protecting PACS is primarily through the CIP-007 requirements for authorization, access control, and logging and monitoring for these systems.

Requirement Part 1.2

One comment stated that the phrase "through the ESP" was redundant in light of the definition of External Routable Connectivity and should be deleted which would also eliminate the use of "through" twice in the existing requirement. In response, the SDT agrees and has deleted the phrase.

One commenter wrote that the measures should include a process to verify that all EAP's are identified as providing a network diagram is not sufficient. In response, the SDT notes that the requirement does not call for a verification process thus the measure should not imply that is a requirement. The requirement states the desired end goal and the entity is responsible for providing sufficient evidence. Network diagrams that depict all external routable communication paths with identified EAP's are listed as one possible example.

Several commenters stated that the applicability should be 'Associated PCA's with ERC'. In response, the SDT agrees and notes that the PCA for this requirement part are associated with high and medium impact BES Cyber Systems with External Routable Connectivity.

Requirement Part 1.3

A few commenters expressed concerns regarding the monitoring and documentation of all outbound traffic. Inbound only monitoring on PSPs is sufficient and suggest dropping the outbound on ESPs. In response, the SDT believes this is an essential element in combating today's electronic attacks and reiterates the following from the included guidance: "The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked."

Several commenters suggested that the applicability should be "Medium Impact BCS with ERC". In response, the SDT notes that the applicability is to EAPs that are associated with High or Medium Impact BES Cyber Systems specifically. If these applicable systems have no External Routable Connectivity, then they will have no EAPs and the requirement therefore does not apply to those systems.

One commenter suggested that the word "rationale" should be changed to "reason." In response, the SDT agrees as this makes the requirement language the same as that used in the measures and in the change rationale. The change has been made.

One commenter noted that tracking the rationale for 60000 ports is burdensome and asked that this be changed to allow for this on a class basis or 'criteria'. In response, the SDT notes the requirement does not require that all 65535 ports be documented as this is a 'deny by default' requirement and only the remaining open ports (those that 'grant access') should be documented. A necessary step in preventing rogue communications to or from a BES Cyber System is to know what the normal communications include and why they are needed.

Requirement Part 1.4

Multiple commenters stated that R1.4 is essentially the same as CIP-007-5 R5.1 and suggest that dial-up be added to CIP-007-5 R5.1 and R1.4 deleted to avoid potential double jeopardy. In response, the SDT notes that CIP-007 R5.1 is specific to user access, while CIP-005-5 R1.4 applies to any access including machine to machine. CIP-005 concerns the security of the 'network' level and requires that there be some form of authentication before a 'network' connection is established to the BES Cyber System. In essence, there should be some form of EAP-like functionality on dialups. Once a connection is made, then CIP-007 applies as we've moved from the 'network' level security to device level security and any user access has to be authenticated at the device.

One comment suggested that R1.4 should be deleted as it is included in R2. In response, the SDT notes that this requirement requires some form of authentication for all dialup connectivity regardless of whether it is machine or user based, while R2 only applies to 'Interactive Remote Access' which is user-based. The intent of R1.4 is that no BES Cyber System, which by definition can have a 15 minute impact on BES reliability, should be directly reachable by simply dialing a phone number, regardless of how it is intended to be used. Therefore R2 contains requirements that are in addition to R1.4 when the intent of the connection is user based Interactive Remote Access.

Several commenters asked if an entity has no dialup capability to applicable systems, are they required to have processes that would authenticate this access? The commenters suggested that the qualifier 'if applicable' be added. In response, the SDT notes the applicability column states that it only applies to systems "with dial-up connectivity" and therefore if an entity has no such systems, there are no systems to which this requirement applies and no process is required. The complete applicability of all requirements throughout the standards is contained within the applicability column and therefore every requirement in the standards has an implied 'if or where applicable' clause.

One commenter suggested that the "where technically feasible" clause should be changed to 'within system capabilities.' In response, the SDT notes that BES Cyber Systems, which by definition can have a 15 minute impact on BES reliability, should not be directly reachable by simply dialing a phone number. If that is not an inherent capability of the system,

then the SDT feels it necessary to add additional equipment with this capability to the system or file for a TFE so that a mitigation plan can be documented to handle the vulnerability.

One commenter suggested that 'where technically feasible' should be deleted. In response, the SDT notes the phrase is an indication of where TFE's may even be requested if the requirement cannot be met on a particular system. Since the SDT is not aware of all situations, it is felt that if an entity cannot meet this requirement on a system that they should be allowed to request a TFE and document a mitigation plan if the TFE is granted.

One commenter suggested that "Associated PCA's" should be added to the applicability. In response, the SDT agrees that any dialup connectivity to any system or Cyber Asset within the ESP, which by definition means the Cyber Asset is also routably connected to a BES Cyber System, should be included. The suggested change has been made.

Multiple commenters suggested that the term 'dial-up connectivity' should be defined to avoid future confusion and should include the notion of access from the PSTN. In response, the SDT is adding a proposed NERC Glossary definition of Dial-up Connectivity.

Requirement Part 1.5

Numerous commenters suggested that the measure only specifies IDS technology and should be made more generic to match the requirement. In response, the SDT agrees and has changed the measure to match the requirement, using IDS as one example.

There were multiple comments that detecting 'malicious' communications requires knowing the sender's intent. Malicious traffic may indeed appear normal. In response, the SDT is adding the phrase "known or suspected" to clarify that the intent is not to detect 100% of all malicious communications, but that communication that has attributes of known or suspected malicious communications.

Multiple commenters asked for clarity as to where the malicious communications inspection should occur and does the direction of the traffic matter. Another commenter stated that only one IDS could be utilized between all ESP's and the

Internet and one per EAP should not be required. In response, the SDT notes the applicability is set at the EAP level and therefore every EAP at Control Centers needs to be covered by the entity's method for detecting malicious communications. The specific architecture and placement is not prescribed. The SDT notes that since this applies to Control Centers, both inbound and outbound traffic should be subject to the detection and has added clarifying language to the standard. For example, if a BES Cyber System in a Control Center begins sending known malicious packets or attempting to communicate with known malicious 'command and control' hosts on the Internet that would warrant detection here and alerting through CIP-007 R4.

Several commenters suggested that the applicability should change to "Electronic Access Points associated with ESPs at High Impact Sites and Electronic Access Points associated with ESPs at Medium Impact Control Centers" as the current phrasing would suggest the need to implement external routable connectivity in otherwise isolated networks. In response, the SDT notes that the requirement is applicable to EAPs and EAPs are only required where External Routable Connectivity is present, therefore isolated networks would not have EAPs and the requirement would not be applicable. However, isolated networks do have ESPs, so bringing the term ESP into the applicability may further confuse the issue.

There were several comments that raised a concern that the requirement is subjective and may not be feasible for encrypted traffic. In response, the SDT has written this requirement in response to FERC Order 706 and the directive to have two or more security measures at each ESP. The Order further clarifies that this is not simply redundant firewalls, but two separate security measures. The SDT has already reduced the subjectivity somewhat from 'two security measures' to 'detect malicious communications'. In today's technology, this would in most cases (but not all) involve the implementation of an Intrusion Detection System, but the SDT does not want to specify products or toolsets within the CIP standards to help future-proof the requirements. If a better toolset is available in the future that is not called "IDS" we would not want these standards to preclude the use of it, so we've deliberately used admittedly more subjective language ("a method for detecting…") in this case. As to the feasibility with encrypted communications, it is true that the methods will be 'blind' to the content of encrypted sessions but it is left to the entities to determine the relative value between maintaining true end-to-end encryption over terminating the encryption and inspecting the traffic at the ESP. The SDT notes that if the traffic is 'Interactive Remote Access', the encryption must terminate per R2 at the Intermediate Device which cannot reside within the ESP.

In the measures section, there were multiple comments to change the word “and” to “or” and to use bullets. In response, the SDT feels a generic paragraph is easier for clarity than bullets. The measure reads, “Examples of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.”

One commenter suggested that the phrase “where technically feasible” should be added to the requirement. In response, the SDT notes that this requirement is limited to Control Center environments. These are the highest risk locations and the SDT feels that in these instances some form of malicious communications detection (IDS) is always possible on routable protocol communications (EAP’s are required only on routable protocol communications).

One commenter stated that External Routable Connectivity should be added to the applicability. In response, the SDT notes that the applicability is to EAP’s which are only required for routable communication points.

Several commenters stated that detection is only one half of the issue and the standard needs to require addressing or mitigating the detected threat. In response, the SDT notes that EAP’s are EACM’s and are thus covered by CIP-007 R4’s Security Event Monitoring requirements and tie into CIP-008. Therefore the SDT feels that the ‘other half’ of the issue is covered by other standards. Xcel suggests that Intrusion Prevention Systems should be included instead of detection systems. In response, the SDT notes that in a control systems environment, the impact of preventing communications that may be the result of false positives may be greater than allowing the communication. Therefore we do not feel it necessary to require in a mandatory and enforceable manner that all suspected malicious communications should be prevented in all situations. That decision is best made by the Responsible Entity based on the specific situation and potential impacts.

One commenter suggested that the Medium Impact should be removed from the applicability as many of the Cyber Assets can’t perform this requirement. In response, the SDT notes that while many Cyber Assets in substations or plants (field locations) may not be able to perform this requirement, the Medium Impact systems are limited to those in Control Centers where the SDT feels the most risk is present and control center systems typically have the most capability to meet this requirement.

Guidance Section

One commenter stated that the guidance for R1 discusses the limitations on the ability of a BES Cyber System to communicate through the EAP and an apparent conflict with the requirement for an intermediate system (jump host) that essentially denies the ability of the Cyber Asset within the ESP to communicate with any other system outside of the ESP. In response, the SDT notes that the Intermediate Device is required only for human-machine interactive login sessions ("Interactive Remote Access") while the Requirement R1 is concerned with machine to machine sessions as well, which do not require an Intermediate Device. Requirement R2 builds upon Requirement R1.4 when the session meets the definition of Interactive Remote Access.

VRF/VSL Section

There was a comment on how the math is done on the VSL for Requirement R1. The SDT has modified the VSL for R1 to remove percentage calculations. We agree the percentage would be difficult to determine in most implementations. Furthermore, the FERC VSL Order addressing CIP Standards discourages specifying failure to document processes as a lower VSL than failure to implement.

There was a comment that suggested the VSL be medium for high impact and lower for medium impact. In response, the VRF by itself does not account for violations from different types of systems, but the SDT expects the impact level of the BES Cyber System to factor into the assessment of penalties.

One commenter suggested the ROP will need to change with changes to TFEs. Although the SDT does not draft Rules of Procedure changes, the SDT expects that this will be a part of the implementation of Version 5.

One commenter recommended modifying the first "Lower" to state: "failed to implement one or more documented processes" to be consistent with the language in Requirement R2. Furthermore, the commenter recommended moving this VSL to the "Severe" category. The lower VSL is intended for the situation where the entity has only failed to document the process(es). Where the entity has failed to implement one of the technology-based solutions listed in the table, those would fall in the moderate to severe categories based on number of technology-based solutions not implemented. The Lower VSL has been revised to clarify this further. Also by the FERC Guidelines for CIP standards, the failure to document processes should be the same level as the failure to implement a process. We have corrected the VSLs for R2.

One commenter recommended that the VSL for CIP-005-5 R2 VSLs be revised to address the approach to detect flaws; correct detected flaws expeditiously. Upon review of the approach to implement preventive, detective, and corrective controls, CIP-005-5 R2 was not identified as a requirement that would be appropriate for this approach. Therefore, the VSL was not modified as requested.

One commenter agreed that the VRF should be medium for the high impact BES Cyber Systems but that the VRF should be lower for the medium impact BES Cyber Systems. In response, VRFs are assigned for an entire requirement and are not assigned to the underlying sub-requirements or parts.

QUESTION B13 – CIP-005-5, R2:

If you disagree with the changes made in CIP-005-5, Requirement R2 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the SDT has made significant changes to CIP-005-5 Requirement R2. The explanations below describe the changes made based on stakeholder comments – the SDT made other minor edits for improved clarity.

TFE Relevance

In response to concerns that the phrase "where technically feasible" should be removed to eliminate reference of maintaining the TFE process, the SDT notes that TFEs will continue to be used in appropriate requirements unless and until such time that the NERC ROP is modified to address exceptional circumstances. The SDT has reviewed each use of a TFE throughout the CIP Version 5 standards very carefully and specifically, and in each instance where that phrase is used, the SDT understands that there may be circumstances where it could be necessary for an entity.

In response to multiple comments that the applicability of TFEs is not clear within the TFE language included in the overall Requirement language, the SDT has moved the TFE language to the table elements.

Applicability

Several comments stated that instances of Medium Impact BES Cyber Systems should be changed to "Medium Impact BES Cyber Systems with External Routable Connectivity". This is a valid concern, and in response, the SDT has added the language to the applicability section of the table.

There was also a comment that the requirement should apply to Physical Access Control Systems and systems serving as ESP Access Points. In response, the SDT believes that since these systems generally do not reside within the ESP of a BES Cyber Asset, it would not be appropriate to apply these Requirements to those Cyber Asset types.

Requirement Part 2.1: Intermediate Device

There was a comment requesting that the reference to Intermediate Device be removed from the requirement. In response, the SDT notes that the Intermediate Device is a defined term that is only used within this one requirement. The device functionality is necessary to ensure that proper protections are put in place for Interactive Remote Access

sessions. The use of Intermediate Devices allow the client machine to exchange data to a Cyber Asset within an ESP without making direct communication and opening the Cyber Asset to vulnerabilities of the client machine.

Several commenters requested improvements to the language in requirement part 2.1 to clarify that a Cyber Asset cannot initiate Interactive Remote Access. In response, the SDT has clarified the language to address this concern by specifying use of an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset. However, the language was not modified to address the person using Interactive Remote Access since the requirement is intended to provide protection from malicious software and communications.

Commenters requested clarification on the location of an Intermediate Device and whether an Intermediate Device can also be an EAP. In response, the SDT notes that the definition of Intermediate Device has only one restriction on the location of the Intermediate Device and that is that the Intermediate Device must not reside in an ESP. Other requirements of the Intermediate Device remain flexible to allow the entity to implement a solution that best meets their needs.

Requirement Part 2.2: Encryption

Several commenters requested that the information regarding the purpose of encryption be removed and added to guidance. The use of "in order to protect the confidentiality and integrity of each Interactive Remote Access session" was intended to help clarify the encryption means that were appropriate.This language has been removed, allowing the Responsible Entity the flexibility to implement the level of encryption appropriate to their organization. Additional references regarding encryption are available in the *Guidance for Secure Interactive Remote Access* document. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

Several commenters requested clarification on the termination point of required encryption. The requirement states the encryption is to terminate at an Intermediate Device. The Intermediate Device may be one or more assets performing the required functions. Encryption should not be perfromed within the Electronic Security Perimeter due to the negative impact on the monitoring for malicious or suspicous communications.

Requirement Part 2.3: Multi-Factor Authentication

Several commenters requested that the examples of multi-factor authorization be removed from the requirements. In response, the SDT has removed the examples from this requirement part, and the requirement part simply reads, "Require multi-factor authentication for all Interactive Remote Access sessions."

Several comments recommended more flexibility regarding the use of multi-factor authentication to allow for future technology changes without a Standards update. In response, the SDT has made this change within the measure so that it is listed as an example, but the requirement can account for future technology changes as commenters suggest.

Many comments requested clarification as to where the multi-factor authentication needs to take place. In response, the SDT has modified the Requirement to state that multi-factor authentication to the Intermediate Device is required for all Interactive Remote Access sessions. Furthermore, the definition of Intermediate Device specifies that access control be performed at the Intermediate Device. The Intermediate Device may be one or more assets performing the required functions.

QUESTION B17 – CIP-006-5:

If you disagree with the changes made to CIP-006-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, there were changes to the applicability section, the requirement parts for added clarity, and removal of unnecessary requirement parts that were documentation related.

General

The "identifies, assesses, and corrects deficiencies" language has been added to Requirement R1 and Requirement R2 since these formerly were zero defect requirements. The SDT believes this is an improvement in the compliance process.

The applicability section was renamed to applicable systems to help clarify the scope of that requirement. Also, the applicable systems entries in each table were reviewed to ensure it matched the requirement language for consistency within this standard and with the other CIP Version 5 standards.

The SDT made changes to table R1 to address concerns on the applicability of requirement parts 1.1, 1.2, and 1.3 that had layered versus exclusive applicability. The table no longer uses layered applicability to be consistent with tables in other CIP standards.

The wording of requirement parts 1.2 and 1.3 has been revised to clarify unescorted access is restricted to those authorized for such access, but escorted individuals can enter a Physical Security Perimeter (PSP).

There was consideration of combining monitoring and issuing an alarm/alert into a single table entry, but these are separate actions and needed separate table entries. Even with separate table entries, each is part of a single requirement.

The SDT has removed the 99.9% availability requirement and requirement part 3.2 to document outages for physical access control, logging, and alerting systems. The Physical Security Plan(s) should address how an entity deals with unavailability of these systems.

Requirement parts 1.4 and 1.5 have been modified to remove the reference to circumvention of a control. The new language is monitoring and issuing alarms/alerts for detected access through a physical access point into a PSP. Designation of physical access points to the PSP should be noted in the physical security plan(s).

A PACS is not required to be within a PSP. Unauthorized physical access is to be restricted. The alarm or alert is for detection of unauthorized physical access similar to the language in requirement parts 1.4 and 1.5, although a PSP is not required.

Data retention requirements that differ from the compliance data retention requirements have explicit language in the requirement table. For example, the retention requirement of 90 days for retention of physical access entry logs is specified in requirement part 1.9.

CIP 006 Requirement R1.3

Language has been added to this table, *"… two or more different physical access controls to collectively allow unescorted physical access into Physical Security Perimeters,"* to clarify that two completely independent physical access control systems are not required. For example, a card key and biometric scan using the same Physical Access Control System for validation is acceptable. Also, the SDT has chosen not to use the words "two factor authentication" since, for example, some field locations could use two separate locks. Further, the SDT believes there may be some locations, particularly for field assets, that may not permit two or more different controls, so the TFE clause remains.

CIP 006 Requirement R1.5 & R1.7

The SDT heard the concerns expressed by industry about when the 15-minute clock begins. The language in the standard has been changed to begin once detected. Also, the language referring to the Cyber Security Incident Response Plan remains as that plan could cover physical incidents related to access to cyber assets.

CIP 006 Requirement R1.8

The SDT has chosen to retain the phrase *"… through automated means or by personnel who control entry."* It confirms in the requirement that a person cannot self-log their entry into a Physical Security Perimeter and that the use of a guard is an acceptable method to log entry.

CIP-006 Requirement R2

This requirement does not state that the visitor control program(s) has to be a standalone document/program. If the entity chooses to include the required language within the Physical Security Plan, that is acceptable.

CIP 006 Requirement R2.1

The language in the parenthetical "*(individuals who are known or guests, and not authorized for unescorted physical access)"* has been removed. A "visitor" is anyone who does not have authorized unescorted physical access inside the PSP. This could include employees, contractors, service vendors, etc. The measure indicates that evidence may include documentation of the visitor control program and visitor logs. There is no reference to "proof" that a visitor was continuously escorted.

CIP-006 Requirement R2.2

The language was edited to correct the implication that a visitor exits to a PSP. Also, the measure was modified to better match with the requirement.

CIP-006 Requirement R3

The SDT considered the suggestion to remove the term "hardware" from the phrase "… locally mounted hardware and devices…" used throughout this requirement. This same phrase has been used in previous versions and is understood to exclude hardware such as door hinges, screws, etc. Also, there is new language in the background section regarding applicable systems that provides additional information on locally mounted hardware or devices.

CIP-006 Requirement R3.1

The SDT believes the key role played by the PACS and associated hardware and devices in protecting High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity warrants a 24-month testing cycle. PACS used for Medium Impact BES Cyber Systems without External Routable Connectivity do not have this requirement.

QUESTION B23 – CIP-007-5, R1, R2, R3 or R4:

If you disagree with the changes made in CIP-007-5, Requirement R1, R2, R3 or R4 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:
Based on stakeholder comments,

General Comments
One entity commented that there is a reference in the 4.2.4 exemptions section that refers to CIP-002 but should refer to CIP-007. In response, the SDT agrees and has made the change.

Several commenters commented that either all VSLs or VSLs for certain requirements should be based on percentage of cyber assets missed. Using percentages based on Cyber Assets on CIP-007-5 Requirements is problematic because Requirements do not have a singular mapping to assets. Also, it is possible for a single Cyber Asset to have multiple violations.

One commented that all Severe VSLs should state the phrase "failed to implement one or more documented." The SDT reviewed this suggestion, and "did not implement" as the SDT proposes is consistent with the SDT's intent.

Requirement R1 General Comments
One commenter suggested that the rationale section for Requirement R1 needs to include physical ports. In response, the SDT agrees and has added this to the rationale.

Several commenters stated that throughout Requirement R1, the applicability for Medium impact should be limited to Medium Impact with external routable connectivity (ERC). In response, the SDT notes that Requirement R1.1 which applies to network accessible ports is already limited to those systems with ERC. Requirement R1.2 refers to physical ports that could be used by someone physically present to inadvertently or intentionally compromise a BES Cyber System. In this case, ERC does not matter and the SDT believes the ERC exclusion should not be considered in this case.

There were a few suggestions that the High Impact systems should include the ERC filter as well. In response, the SDT notes that since Version 1 of the CIP-002 standard, lack of external routable (or dial-up) connectivity has been a blanket exemption everywhere except Control Centers, where even standalone networks were still to be considered as Critical Cyber Assets. Since High Impact in Version 5 refers to Control Centers, the SDT cannot 'go backwards' without sufficient justification, which we believe is absent.

One commenter suggested that the words "and Services" should be dropped from the title as the requirement concerns only network ports. In response, the SDT notes that ports are opened by services and that typically a port is disabled or closed by disabling the corresponding service. The requirement also allows for services that use wide ranges of dynamic ports that need to be enabled to be documented as the service name rather than a dynamic port range. Therefore the SDT believes the 'and Services' is appropriate.

Several commenters stated that the Requirement R1 measures may also include rationale as to why ports are necessary or clarify in the requirement. In response the SDT agrees and has added a specific measure for documentation of the need for all enabled ports.

Requirement Part 1.1

One commenter suggested that the phrase "ports or services" should be "ports and services". In response, the SDT notes that the use of the word "or" is intentional to allow for circumstances where a Cyber Asset uses one service that is on one port, another service that uses a range of ports, or a service that uses dynamic ports without a defined range (e.g. may use anything over 1024). The entity should be allowed to document the enabled single ports, port ranges, or in the case of the dynamic ports, the service that is enabled. Therefore the SDT feels the word "or" is appropriate.

Two commenters suggested that the sentence in the guidance concerning cyber assets that allow for no port management and therefore all open ports are deemed 'needed' should be part of the requirement. In response, the SDT agrees and has moved the sentence to the requirement.

One commenter suggested that the phrase 'where technically feasible' should be replaced with 'within device capabilities'. In response, the SDT notes that devices that do not allow for port management will have their ports determined as 'needed' thus the TFE will be seldom used. However, the SDT wanted to allow for entities to request a TFE for any special cases.

One commenter suggested that the requirement should consider more than listening ports but should also include unexpected connected ports making outbound connections. In response, the SDT notes that this risk is covered at one level by CIP-005's new outbound rule requirement. The SDT also notes that this requirement requires evidence of a known port configuration for the cyber asset and it is unclear how an entity could perform this for 'unexpected' ports.

Several commenters asked for clarification as to how "associated PCA's" applies and is not an independent set of individual assets. In response, the SDT notes that most of CIP-007, and Requirement R1 in particular, must be implemented at an individual cyber asset level and the requirement thus starts with 'For applicable Cyber Assets'. Ports and services are enabled or disabled on individual Cyber Assets and most of CIP-007 can't be done at a 'system' level but at a Cyber Asset level. For example, if an entity does not need telnet service, then the only way to prove that it has been disabled is on an individual Cyber Asset basis – ports and services are by nature not implemented on a 'group' of Cyber Assets but on individual Cyber Assets.

FMPA and LCEC commented that the SDT should add the phrase "that initiate or receive network communications" after the word "services" or delete services and let ports handle it. In response, the SDT notes that the services is part of "port ranges or services" and are two levels at which the entity can document the enabled logical network accessible ports. This was added primarily to handle dynamic ports. Some systems will use a particular dynamic port out of a small range of ports and documenting that range is acceptable. Other services may pick a dynamic port out of all the high ports (any port between 1024 and 65535 e.g. RPC) and the SDT's intent is to allow for documenting the need at the service name level.

Some commenters suggested that clarification that the Responsible Entity determines the need of port should be included. In response, the SDT agrees and has added clarifying language.

One commenter suggested that the phrase "enable only logical network accessible ports needed" should be "enable only required logical network accessible ports." In response, the SDT notes that the intent is to document the business or technical justification for all open ports. In previous drafts, numerous comments were received to change the word "justification" to "need", which was accepted by the SDT. The SDT also notes there is a difference in "required" and "needed" and thinks "needed" is a more appropriate term due to instances where a Cyber Asset may be fully able to perform its basic function without the port enabled (thus the port is not technically "required"), but the port is "needed" for other purposes. Similarly, KCPL commented that the "needed" should be changed to "approved" for clarity. In

response, the SDT notes that these ports are part of the tracked baseline configuration in CIP-010 and approvals occur there. The SDT has therefore not brought in the approval process into CIP-007.

One commenter suggested commented that 'listening' should be replaced with 'enabled'. In response, the SDT believes the term 'listening' is more descriptive as the intended scope is those ports that can actually be reached from the network. A port can be 'enabled' at one level (a config file), but blocked by other means lower in the OS (e.g. TCP_Wrappers) such that it is not actually 'listening'. The end goal is blocking accessibility from the network to unneeded ports and the SDT believes 'listening' better captures that goal.

One commenter suggested that a fourth bullet should be added to the measures to address CIP-005-4 R2.2: Listing of access points to the ESPs, including configuration of ports and services, individually or by specified grouping. In response, the SDT agrees that EAP's should be highlighted and has added this to the first bullet point.

One commenter suggested that the measure should add the phrase "or class of Cyber assets" to the second bullet. In response, the SDT agrees and has added the phrase "individually or by group" to the bullet point.

One commenter suggested that the first bullet under the measures should be deleted as it doesn't meet the requirement. In response, the SDT agrees that a simple listing of port need is not sufficient to meet the requirement and has replaced that measure with the phrase "Documentation of the need for all enabled ports individually or by group".

One commenter suggested that the list of listening ports could be a source of double jeopardy with CIP-010's baseline configuration requirements. In response, the SDT notes that the requirement is concerned only with the enabling of only needed ports irrespective of any documentation. The list of enabled ports is a requirement in the baseline configuration requirement in CIP-010. The SDT believes that failing to maintain the baseline configuration and failing to actually go to a Cyber Asset and disable unneeded ports are two different requirement violations. The measures for this requirement refer to listings of ports as evidence, but that evidence could be the same evidence required for CIP-010. Being able to utilize a single piece of evidence for proof of compliance with two different requirements is not double jeopardy.

There was a commenter who suggested that instead of the phrase 'class of cyber asset' the language from CIP-010 should be used. Also, the requirements should address justification of enabled ports. In response, the SDT agrees and notes that justification is addressed by the phrase 'needed by the Responsible Entity' and the measure has been changed to

now call for documentation of the need for all enabled ports. The SDT also agrees with the 'class of cyber asset' comment and has incorporated the language 'individually or by group' from CIP-010 as suggested.

One commenter suggested that the reference to CIP-005-5 R1 to protect the network in the guidance should be deleted. In response, the SDT agrees and has deleted the language, leaving only the clarification that blocking ports at the ESP does not substitute for the device level requirement.

One commenter suggested that the guidance should allow for disabling ports 'inline in a non-bypassable manner'. In response, the SDT agreed with this in the draft 1 comment phase and made that change between drafts 1 and 2.

Requirement Part 1.2

There was a comment that the text should be revised to begin with the phrase "Have methods to protect against…" since the VSL is for not having methods. In response, the SDT notes that the overall Requirement R1 is to "implement documented processes" and changing this to have methods would add another level of abstraction such that the overall requirement would be "implement documented processes to have methods to protect."

A commenter suggested that this requirement should be replaced with a 'implement a policy' type requirement. In response, the SDT does not believe that a policy only requirement would meet the FERC directive in Docket No. RD10-3-000 of March 18, 2010, which is the genesis of this requirement.

Several commenters suggested that signage is a weak control that does not provide adequate protection. In response, the SDT notes that signage was never meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. The industry has made several comments as to the other preventative and detective measures that are required before physical access to a physical port is ever achieved. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who plugs his infected smart phone into an operator console USB port "just to charge the battery".

Several commenters stated that this requirement needs further justification for its existence. In response, the SDT notes that this requirement was added to address FERC's Docket No. RD10-3-000 of March 18, 2010 which states, "However, like NERC, we are concerned that neither CIP-007-2 in particular, nor the CIP reliability standards in general, adequately address technical opportunities to mitigate risks associated with unused physical ports. The practice of disabling or otherwise securing unused physical ports is a basic and integral component of sound defense-in-depth cyber security practices, yet it is absent from the current reliability standards. The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP reliability standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."

One commenter stated that entities may not be able to block physical ports based on usage using the example of unplugging a USB keyboard or mouse and using a thumb drive in that enabled port. In response, the SDT notes the requirement is to "protect against the use" and purposefully does not use the verb "prevent" in recognition that the control is not effective in prevention in many cases as the industry has pointed out. The intent of the requirement is not to be a 100% preventative control, but is a last measure in a defense in depth layered control environment to make personnel think before attaching to a BES Cyber System in the highest risk areas.

There was a comment that this requirement should be limited to network ports as portable media is handled elsewhere. In response, the SDT notes that BES Cyber System Information on portable media is handled elsewhere, not the portable media itself. Portable media is becoming a primary means of entry into entities and the SDT believes that to meet FERC's intent, portable media and console command ports should remain in scope.

One commeneter asked for clarity on whether the disabling of physical ports could potentially reclassify a device that would otherwise be considered a BES Cyber System. For instance, if a routable device had all of its physical network ports blocked then what otherwise might be a routable device cannot route. In response, the SDT notes that the ability to communicate outside of itself is not a determining factor as to whether a Cyber Asset is or is not a BES Cyber Asset or BES Cyber System; the Cyber Asset's function as it pertains to BES reliability determines that. So although a Cyber Asset may indeed be a BES Cyber Asset, if all communication ports are disabled then the BES Cyber Asset would have no External Routable Connectivity or dial-up connectivity and thus none of the requirements which have that condition in the applicability column would apply. The specific example of the programmable television monitor provided would have to be determined by the Responsible Entity as to whether the monitor met the definition of a BES Cyber Asset. If the

monitor is not a BES Cyber Asset, then it is not a part of a BES Cyber System. The SDT notes that BES Cyber Systems consist of one or more BES Cyber Assets, not every programmable electronic device.

There was a comment asking for clarity as to whether ports could be protected via a common method or must the protections be per port. In response, the SDT notes that the requirement is not prescriptive in this manner and does not preclude either as the measures and guidance allow for directive measures.

One commenter stated that the word "unnecessary" should be changed to "not required". In response, the SDT is allowing for slightly more flexibility than is denoted by terms such as "required" or "not required". A port may be "necessary" for some use of the entity but not technically "required" for the operation of the device.

Requirement R2 General Comments

Several respondents commented that patch management should apply to all applicable Cyber Assets including all Low Impact. In response, the SDT believes that while managing patches on all Cyber Assets is a best practice, making this a mandatory and auditable requirement would divert the industry's attention to managing an onerous burden of records on orders of magnitude more devices at the lowest impact level. The SDT has been careful to balance what is absolutely required in a mandatory and enforceable manner and the burden of proof such a change would entail with maintaining a high degree of industry focus on the higher risk assets. If we overburden the Low impact classes, it would be easy to divert an inordinate amount of industry focus to the lowest impact assets if we don't maintain that balance. The SDT also believes that many devices will probably have some portion of the population declared as medium impact and thus many entities will need to handle any vulnerabilities on those devices and oftentimes will just patch all devices of that type.

There were many commenters that suggested that all sub requirements should have the applicability changed to medium impact with ERC. In response, the SDT notes that managing security patches or otherwise mitigating the vulnerabilities the patches address is a core activity in protecting our critical infrastructure. While external routable connectivity does increase the risk, the lack thereof does not reduce it to an acceptable level as many threats enter the environment by other means such as thumb drives, laptops, smart phones, etc. The SDT does not believe we can adequately protect the infrastructure if we only concern ourselves with patching devices with external connectivity due to the remaining threat vectors. However, the SDT does understand the evidence burden and has made changes to this requirement to reduce that burden. The requirement now allows entities to focus on a monthly 'batch' cycle of patches rather than tracking timelines for every individual patch, and no documented mitigation plans are needed if patches are installed within the 70 day time period. It is the SDT's intent that these and other changes in this requirement will relieve the documentation

burden while still requiring the performance of this basic security activity. The essence of this requirement is to have the industry watching and aware of vulnerabilities in their BES Cyber Systems, whether they are routably connected or not, and mitigating those vulnerabilities. Many patches may address vulnerabilities that the entity has already mitigated through existing means and require no action. In fact, it is expected that the lack of external routable connectivity would be used as a major factor in many applicability decisions and/or mitigation plans where that is the case.

Several commenters stated that the requirement should not require a documented remediation plan for every patch, but outline a standard patch mgt process with documented deviations. In response, the SDT agrees and has modified part 2.3 to allow for this.

There were a couple of comments that clarification is needed on failed patches installed well after the 60 days but according to the entity's plan. In response, the SDT has modified the requirements such that a plan may be revised (see requirement part 2.4).

One commenter suggested that the word "processes" should be changed to "program" throughout R2 so it aligns with 2.1. In response, the SDT agrees the terms should match, but notes that Requirement R2 (above the tables) uses the word "processes" and has changed the term "program" in 2.1 to "process" so that the entire requirement uses the same term.

One commenter stated that the requirement in essence rewards obsolescence and never requires upgrading to a patchable system. In response, the SDT notes that the standard's intent is to secure the infrastructure that is in place without requiring equipment upgrades of currently functional equipment solely for security purposes. Cyber security risks are one factor in the decision to upgrade. The SDT also notes that cyber risk is determined by many factors, and older equipment could actually have a lower cyber security risk. These decisions are best left to the Responsible Entity to make based on the specific circumstances rather than mandated unilaterally in a cyber security standard.

There was a comment that clarity should be provided on what constitutes a "security patch" and what is "updateable". In response, the SDT agrees and has added clarifying sentences to the guidance section of the standard for part 2.1.

Requirement Part 2.1

Multiple comments stated that the phrase "security patches" should be changed to "patches and security upgrades". In response, the SDT is concerned with expanding the scope beyond patches to words such as upgrades or updates. The

SDT does not desire to create the situation where a vendor creates a new version of their software, mentions something new about security in the new version, and suddenly everyone is under mandatory compliance obligation to either upgrade or create a plan. Cyber security features are one component of an upgrade decision. The SDT believes that keeping this requirement to the word "patches", which are fixes to their existing version, is what should be mandatory. The SDT also notes that patches are a fix to a specific vulnerability, which is what the requirement is based upon as it is under obligation to mitigate the vulnerability.

One commenter suggested that applicability and compensating measures should be determined based on original source of patch (e.g. Microsoft) rather than the SCADA vendor. In response, the SDT agrees that this is a best practice so that vulnerabilities may be mitigated in the shortest timeframe possible, even before the patch is certified by the SCADA vendor. The SDT notes that the provided example is the most obvious one with Microsoft, however if included in a mandatory and auditable environment this would extend to the seemingly unlimited non-obvious situations where an entity buys a system from vendor 'X', but vendor 'X' is using software components from 20 other vendors. The entity does not know all the original sources of all components of the system. Situations such as what is the RTOS (Real Time Operating System) involved in a particular digital relay would arise, and why didn't the entity track the vulnerability info for that RTOS directly from that vendor rather than the relay vendor's firmware levels? The entity is not a direct customer of that RTOS vendor and may not have access to that information. In summary, while the SDT believes this is a best practice in some situations, making it mandatory and auditable in every situation is not something that entities can comply with as the standard expands in scope to every BES Cyber Asset in the field.

There was a recommendation that more guidance is needed on appropriate patch sources. In response, the SDT notes that the 'appropriate sources' was added to this requirement from Version 4 so that a definite start date for the evaluation timeframe could be determined. The appropriate source is going to be dependent on the situation. If the Responsible Entity has a control system from vendor who invalidates support contracts if the system is patched outside of their approval, then the vendor should be the appropriate source. If the system were custom built by the Responsible Entity, then the vendor for each of the components used to build the system would be the appropriate source.

One commenter recommended that the program should be specified in Requirement R2 and not Requirement R2.1 as a process does not include a program. In response, the SDT agrees and has changed the word "program" in R2.1 to "process" so that it agrees with Requirement R2.

Some commenters said that the process should include a periodic review (monthly) of all patch sources rather than maintaining timeframes per patch. In response, the SDT agrees and has made changes to the language to incorporate this concept.

There was a comment that the requirement should insure that documentation of sources is a onetime exercise unless new software is added to the baseline. In response, the SDT agrees and has clarified this in the guidance section of the standard.

Requirement Part 2.2

Numerous commenters suggested a change to 35 calendar days to allow for a monthly cycle. In response, the SDT agrees and has made the suggested change.

One commenter requested that the guideline states that entities are allowed to evaluate and accept risk which FERC Order 706 disallows. In response, the SDT agrees and has modified the guidance.

There were a few commenters that requested additional clarity on what the term 'applicability' means. In response, the SDT agrees and has added clarification to the guidance section.

One commenter suggested alternative wording, "Evaluate the security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified in requirement part 2.1. The assessment must include determination of the applicability of each patch to the entity's specific environment and systems as well as reason for a patch's non-applicability." In response, the SDT has modified this requirement to incorporate a monthly review of the patch sources, but has chosen not to get more prescriptive with the term applicability within the requirement. The SDT believes that evaluating applicability necessarily means that the entity will be documenting the final determination for their environment.

Requirement Part 2.3

Some commenters proposed changes to the timeframe and process such that it would allow 60 days and have no remediation plan required if the patch is installed within 60 days. In response, the SDT agrees and has modified the requirement so that applying the patch or creating or revising a mitigation plan are all choices the entity can take within the second 35 day period. The SDT notes, however, that the timeframe is 70 days total with 35 days for tracking and

determining applicability and 35 days for either installing or determining the mitigation plan. It is not 35 days plus an additional 60 days for the second step.

There were multiple comments that the word "dated" should be revised since it is open-ended. In response the SDT believes the word "dated" is necessary and the requirement would be open-ended if it had no date required for the plan. The date of the plan in requirement part 2.3 is what part 2.4 depends upon.

One commenter stated that the requirement was overly burdensome due to the sheer number of patches. In response, the SDT notes that due to the burden the auditable cyber assets are limited to High and Medium Impact Systems and associated systems. The SDT has changed the requirement so that the tracking can be on a monthly basis for all patches released that month rather than on an individual patch basis, which should help.

Some commenters suggested that specificity is needed as to a maximum timeframe. It is compliant with the requirement to state a timeframe of the phrase "End of Life Upgrade". In response, the SDT has had numerous discussions around this issue. The SDT has decided that the reliability risk of putting prescriptive and mandatory timeframes for patching outweigh the risks of having an open-ended patching timeframe. There are numerous reasons. One reason is the industry goes through periods of time during seasons of the year that we refer to as "nobody is touching nothing" mode because the risk of any change to equipment or systems invokes an availability risk when the asset is depended upon the most. Tripping a generating unit on a 100-degree day because a standard said we were out of time to patch it to fix some minor issue is not acceptable. Another reason is we are in a largely legacy equipment environment as this standard expands outside of control centers where there are no patch management solutions. Upgrading the firmware in thousands of digital relays is something that must be planned and executed very cautiously. Firmware based devices will require planned outages for patches and present the risk of "bricking" the asset. So for these and other reasons, the SDT has decided the implementation timeframe is best left up to the entity rather than enforcing some arbitrary timeframe. The requirement is that they have a dated plan and must work towards that plan. We believe this is the best tradeoff between the risk of someone exploiting a vulnerability and the inherent risk of changing code in devices where availability is paramount. If the SDT set a maximum timeframe to handle these sorts of cases, we would have numerous comments about how the timeframe is too long. We believe that setting a timeframe to handle these cases would actually draw a line in the sand that would have the unintended consequence of all patch timeframes moving toward that timeframe. If the entity has to set its own timeframe and defend it, then they won't all tend to move towards the maximum timeframe specified in the requirement.

Two commenters suggested that the requirement should allow for revision to an existing plan. In response, the SDT agrees and has changed the language to allow for revisions.

There were a few recommendations that the word “exposed” should be “addressed”. In response, the SDT agrees and has made the change.

There was a comment that a potential double jeopardy issue exists between requirement parts 2.2 and 2.3. In response, the SDT has made numerous changes to these requirements and believes that any double jeopardy issues have been addressed.

One commenter stated that an evaluation of the language in the change rationale should be done to determine what needs to move into the requirement itself. In response, the SDT believes that what remains in the rationale is rationale and has no actionable requirements that could be moved to the requirement itself. However the SDT agrees the language in the rationale should be preserved and has moved it to the guidance section as well.

There was a comment that addressing the vulnerability could be entirely dependent on vendor’s patch development timeframe to address a vulnerability. In response, the SDT notes that the process begins upon the release of the patch from the source identified by the Responsible Entity. The patch has been developed and is available before the process required in R2.2 and following starts.

One commenter asked about the need for TFEs where patches cannot be applied. In response, the SDT notes the intent is that TFEs are not required at any step in the process. The process has been designed to alleviate the need and guidance has been included as well to address this issue.

There was a comment that the first sentence in the guidelines for Requirement R2.3 is a restatement with different wording and may imply other requirements. In response, the SDT agrees and has changed the guidance to more closely match the requirement.

Requirement Part 2.4

Multiple commenters stated that the plans should allow for revision in other than CIP Exceptional Circumstances before the timeframe expires. In response, the SDT agrees and has added the ability to revise the plan if done through an approved process such that the revision or extension is approved by the CIP Senior Manager or delegate.

An issue was raised that there is a potential double jeopardy issue as 2.4 duplicates Requirement R2 where 'implement' is required. In response, the SDT does not believe that a double jeopardy issue exists because the implement in the overall requirement is for the patch management process, whereas the implement in R2.4 is for the individual patch. If R2.4 does not have an implement requirement at the patch level, then the 'implement' in the overall requirement only applies to drafting a plan.

One commenter suggested that guidance should be offered on how much information is expected to demonstrate implementation. In response, the SDT notes that example measures are provided and that the requirement is for the implementation of a mitigation plan, thus the measures would be records of the implementation of the plan. The plan may include such things as installing the patch and the measure would be a record of the installation, or the plan may include the disabling of an affected service, or the adding of a signature to an IDS, or a change to a host based firewall to handle the vulnerability and the measure would be the record of the completion of these changes.

There was a comment that the change rationale is from 2.2 and doesn't address 2.4. In response, the SDT agrees and has updated the rationale to match the changes in the requirement.

To address the comments that bullet 2 of the measure should read "records of vendor recommended or other appropriate mitigations" the SDT agrees and has added "or other appropriate" to the measure.

Requirement R2 VSL

One commented that the R2 and R3 VSLs increment by different ranges. In response, R3 has been modified to remove specific timeframes in the Requirement and the VSL has removed the referenced increments.

Requirement R3 General Comments

One commenter requested that the requirement should apply to all applicable Cyber Assets including all Low Impact. In response, the SDT believes that while this is a best practice, making this a mandatory and auditable requirement would divert the industry's attention to managing an onerous burden of records on orders of magnitude more devices at the lowest impact level. The SDT has been careful to balance what is absolutely required in a mandatory and enforceable manner and the burden of proof such a change would entail with maintaining a high degree of industry focus on the higher risk assets. If we overburden the Low impact classes, it would be easy to divert an inordinate amount of industry

focus to the lowest impact assets if we don't maintain that balance. The SDT believes that keeping the requirements on Low impact systems at a programmatic level rather than a device level is the only way to keep that balance.

Multiple commenters suggested that the applicability should change to all medium impact with ERC. In response, the SDT disagrees because the threat of malicious code is not limited to introduction through external routable connectivity. The threat of malicious code is arguably higher from portable media, temporarily connected cyber assets (vendor laptops, etc) and inadvertent insider actions.

Requirement Part 3.1

There were a few comments which stated that the intent should be clarified and suggested language includes "Deploy method(s) to deter, detect, or prevent malicious code based on the Cyber Asset's susceptibility to malware. Methods do not have to be used on every single Cyber Asset." In response, the SDT notes that the applicability is at the 'system' level and the intent is to keep it at that level as this is a requirement where the 'system' level is beneficial. Therefore, the SDT believes it is best to not fill the requirement with language at an individual cyber asset level.

There were several concerns that Requirements R3.1 and R3.2 are too vague. In response, the SDT notes that the requirements are indeed written at a very high level but the SDT believes it is necessarily so. Malicious code protection is at the 'forefront of the fight' and is rapidly evolving and changing to match the ever changing and morphing threat. The SDT believes the protection of our infrastructure can be better accomplished if we do not have prescriptive technical methods detailed in this requirement. This could have the unintended effect in the future of stifling innovation and the use of new and better tools that would provide better protection but not be compliant with what the SDT would specify today. It does not produce a standard that is future-proof. All previous versions of the standard did prescribe a particular technology and method that must be used on all applicable cyber assets, and while that had no vagueness it became a huge burden on the industry for TFE's, putting the industry's focus on what could not be done rather than what could be done. Therefore, the SDT is leaving this requirement at a very high level that is in essence "think through the problem of malicious code introduction, detection, and prevention and come up with the best methods to handle the problem in each particular situation, and then document and do those methods." The SDT believes reliability will be better served in the long run by a requirement like this for such areas as the malicious code 'arms race' environment that we find ourselves in.

There were multiple comments asking if the 'or' is appropriate. There was another question if an awareness campaign to deter is ok. There was a suggested that the word 'deter' should be stricken. In response, the SDT notes that the

requirement was worded with the 'or' and 'deter' to avoid zero-defect language. If the requirement was to detect or prevent all malicious code, then despite an entity's best efforts if some zero-day malware did make it onto an applicable cyber asset the entity would be in violation of the requirement. As malware detection and prevention is an inexact science and essentially an 'arms race', the SDT did not want to word the requirement in such a way that it required perfection in an imperfect environment with imperfect tools.

There was many comments that the 'Associated PCAs' are included at a Cyber Asset (device) level, not a system level and should be deleted or clarified how the 'system' concept will apply. In response, the SDT notes that malware prevention really is at a Cyber Asset level and recognizes that the associated PCA's could be included by reference in the documentation the entity supplies for Requirement R3.1.

One commented stated Requirement R3.1 and R3.2 should be revised to "deploy methods … within an ESP" to scope to routable assets within the ESP. In response, the SDT notes that ESP's are only required around routable protocol connected cyber assets, however malware protection is required on all cyber assets in scope. Malware is a risk even on isolated systems; it may not be able to easily spread in non-routable environments, but it can be coded to have a specific impact even on isolated systems (e.g. Stuxnet was coded to do its harm when it reached a specific system and could travel by USB portable media). Therefore the SDT has chosen to not limit the malware prevention requirement to only routable protocol accessible systems in ESPs.

One commenter suggested that the measures should be revised to, "Entity's performance of these processes (e.g., through traditional antivirus, system hardening, non-software policies, etc.)." In response, the SDT notes the only suggested change is the phrase 'non-software' in front of 'policies'. The SDT does not wish to make the measure more prescriptive than the requirement itself. Since malware prevention is an ever changing 'arms race' type environment where the controls needed are changing as the threat constantly evolves, the SDT is leaving this requirement at a high level. This will allow entities to adapt as the threat adapts while also reducing the need for TFEs.

One commenter stated that the last sentence of the guidance says 'should not require a TFE' making it unclear whether TFEs are an option or not. In response, the SDT agrees and has struck the phrase.

Requirement Part 3.2

One commenter recommended that the following sentence be added: “Mitigation for the Associated Protected Assets may be accomplished through other applicable systems.” In response, the SDT agrees that this is possible and the entity could state how the mitigation covers the associated PCA’s in their documentation for this requirement.

One commenter suggested that the wording “within 35 days” should be added as malware mitigation timeframe. In response, the SDT has chosen not to include a mitigation timeframe as in some cases the entity may be working with government or law enforcement in an ongoing investigation. In APT cases, quick mitigation may just force the moving of the attack while investigations are ongoing. The SDT feels that a mandatory timeframe would interfere with investigations in cases such as these.

Two commenters recommended that the measures should be limited to response actions for detected malware and remove other bullets. In response the SDT agrees and has removed the example measures that were more focused on specific technologies.

One commenter stated that in the guidelines it discusses ‘non-changeable software’ and asks if this is in conflict with definition of Cyber Asset. In response, the SDT believes it is not in conflict. Cyber Asset is a programmable electronic device and devices that are not updateable by the user, but are software or firmware based and do execute a program would still be classified as Cyber Assets.

Requirement Part 3.3

There were many comments that Medium impact locations with no remote connectivity need more than 35 days for signature updates or should not be in scope. Some commented that 35 days is too long for malware updates and it should be shortened. In response, the SDT agrees with both positions and realizes that specifying a time frame on a requirement such as this often means picking a timeframe that is usually not long enough for all of the more extreme cases while at the same time is too long for most ‘normal’ cases. The SDT has decided that it is in the best interest of reliability to revert this requirement back to its V1-V4 language that did not include a timeframe. Order 706 did not direct such a modification and the SDT is more concerned about preventing the unintended consequences of this timeframe and their resulting impacts to reliability. As one example, the SDT does not want to incent entities to remove antivirus products from systems in the field and expose them to a decade’s worth of viruses because they may not be able to get last month’s signatures on in 35 days. The SDT believes its in the best interest of reliability to allow entities to put antivirus software on all assets where they can and require processes to test and install the updates without specifying an ‘arbitrary’ timeframe that satisfies no one.

One commenter stated that 35 days is too long for malware updates and should be shortened. In response, the SDT agrees with both positions and realizes that specifying a timeframe on a requirement such as this often means picking a timeframe that is usually not long enough for all the more extreme cases while at the same time is too long for most 'normal' cases. The SDT has decided that it is in the best interest of reliability to revert this requirement back to its V1-V4 language that did not include a timeframe. Order No. 706 did not direct such a modification and the SDT is more concerned with the unintended consequences of this timeframe and the resulting impacts to reliability. As one example, the SDT does not want to incent entities to remove antivirus products from systems in the field and expose them to a decade's worth of viruses because they may not be able to get last month's signatures on in 35 days. The SDT believes it is in the best interest of reliability to allow entities to put antivirus software on all assets where they can and require processes to test and install the updates without specifying an 'arbitrary' timeframe that satisfies no one.

Several commenters wrote that the requirement is not as clear as the change rationale and the requirement could be gamed to not install any recent sigs. In response, the SDT agrees and has rewritten the requirement for clarity.

A few comments stated that signature updates need to be staged to avoid a large impact of false positives. The included guidance should address this as well. In response, the SDT agrees and has reverted the language back to its V1-V4 state that did include a process for testing and installing the signature updates.

Some commenters questioned that if an entity does not use signature based tools, if they still have a process to update the signatures per the overall requirement. In response, the SDT notes the specific sub requirement is conditional and only applies to "for those methods identified in requirement part 3.1 that use signatures or patterns…" and therefore if an entity has no such methods, the requirement does not apply.

One commenter recommended that the word "available" should be changed to "applicable". In response, the SDT has rewritten the requirement for clarity and to address this and several other comments.

A commenter suggested that the requirement should allow for other anomaly or heuristics based analysis/detection, not just signature updates. In response, Requirement R3.1 allows for any method to be used so that the requirement does not preclude the use of any technology or tool as they constantly improve to keep up with the threats. Requirement R3.3 in particular is only applicable when an entity chooses to use a signature or pattern based tool in order to keep them updated in a timely manner; it does not require their use.

One commenter asked for clarity on what TFEs are allowed for equipment that doesn't run malicious code tools. In response, the SDT notes the requirement has been written at a much higher level than previous versions. The included guidance has numerous suggested methods up to and including policy level measures. Therefore, the SDT feels that TFEs are no longer an issue as the requirement no longer prescriptively requires a single technology tool for addressing the issue.

Requirement R4 General Comments

There were several comments that the rationale language should change 'immediate' detection to 'real time detection' to be consistent with 4.2. In response, the SDT received numerous comments that pointed out issues with the term 'real time' and has deleted it, as well as removing 'immediate' in the rationale.

There was a comment seeking clarity as to whether log events are required for local, remote, or both types of access. In response, the SDT notes that the requirement applies to both High and Medium impact BES Cyber Systems as well as all associated EACMs. The EACMs will include the EAPs for the associated perimeters. Therefore the logging is for both; local access at the BES Cyber Systems themselves, and remote access through the EAP.

One commenter suggested that the guidance include NIST 800-137 as a resource. In response, the SDT agrees and has added the reference to the guidance.

Requirement Part 4.1

Many commenters recommended that the requirement should add the phrase "per device capability". In response, the SDT agrees and has added this concept to the language.

Numerous commenters asked that it be clarified that devices that cannot log do not require a TFE. In response, the SDT has added device capability condition statements to the requirement such that the requirement does not apply if the device does not log the events. In addition, the bulleted list of logged events includes the qualifier 'detected' so that if a device cannot detect such events, then there is nothing to log.

There were several suggestions that 'where technically feasible' should be added to all. In response, the SDT's intent is that the requirement is worded so that what is required matches the device's capability and no more and avoids the use of TFE's due to prescriptive requirements that assume technical capabilities of large classes of Cyber Assets.

Tucson, and SME List commented that TFE should be applied to the logging, not the alerting in 4.2 and suggest removing the TFE in 4.2. In response, the SDT has changed both 4.1 and 4.2 to include the 'per device capability' concept rather than allowing TFE's.

Multiple commenters suggested said that the applicability should change to Medium Impact with ERC. In response, the SDT notes that logging should be enabled wherever it is available. If an isolated or standalone BES Cyber Asset is compromised, then the logs on that device may be the only data the entity will have to investigate the incident.

One commenter suggested that the measures should include samples of logs showing the events are being logged. In response, the SDT agrees and has added the additional example measure.

One commenter suggested that the requirement implies 100% availability of the logging system and suggests adding the 99.9% availability. In response, the SDT notes the comments where the 99.9% was added in CIP-006 pointed out numerous issues with that approach. The SDT believes that the inclusion of Requirement R4.3 states that 100% availability is not required and handles the issue by requiring the entity to have processes in place to respond to outages in a timely manner.

Several commenters sought clarity as to log failed access attempts when deny by default means offending packets are dropped such that there is nothing to log. In response, the SDT notes that a denied access attempt is a failed access attempt.

There were several commenters who suggested that 'malicious software' should be changed to 'malicious code' to be consistent with Requirement R3. In response, the SDT agrees and has made the change.

Many commenters recommended dropping the requirement since its determined after the fact, requires knowledge of intent, and it's not possible to produce a log of 'malicious activity'. In response, the SDT agrees and has removed the sub requirement.

Several commented stated that 4.1.4 is too vague and needs more guidance as to what activities beyond 4.1.1 to 4.1.3 would be included. In response, the SDT agrees and has removed the sub requirement.

One commenter stated that malicious activity should be detected and logged 'as required in the cyber security incident response plan'. In response, the SDT notes that based on several other industry comments, this sub requirement has been removed.

Requirement Part 4.2

Several commenter stated that 'real time' is not the appropriate phrase and some suggested changing to "Have methods to generate alerts, where technically feasible, for events that the Responsible Entity determines necessary." In response, the SDT agrees and has deleted the 'real time' phrase.

Also, others commented that 'real time' should change to 15 minutes and add 'where the BES Cyber System is capable.' In response, the SDT agrees and has deleted the 'real time' phrase and the 'per Cyber Asset or BES System capability' has been added.

A few commenters recommended that 'within the BCS capabilities' be added. In response, the SDT agrees and has added the appropriate phrase.

One commenter stated that a minimum expected set of security events for which alerts should be issued should be prescribed (if the Cyber Asset is capable of detecting and logging those types of events). Examples include failed login attempt threshold exceeded, account lockout, key software failures, and virus or malware alerts. They also commented that the guidance includes alerts to a display that may not be monitored. In response, the SDT notes that detected malicious code is included, as is detected event logging failure. The SDT agrees that unsuccessful login attempt threshold should be added as it is a requirement in CIP-007 R5.7 and has made this addition. The SDT notes that account lockout is a subset (or post action) of unsuccessful login attempt threshold and has not included it.

There was a comment that the requirement should only apply to Associated Protected Cyber Assets with ERC. In response, the SDT believes that if the BES Cyber Systems have External Routable Connectivity that the associated PCAs will also have that connectivity. In the envisioned rare instance where this is not the case, the requirement allows for the entity to do what is within the device's capability and no more.

One respondent commented that we need a requirement that trained and knowledgeable people perform the event monitoring activity. In response, the SDT agrees that this is certainly reasonable, but disagrees that it should be an

auditable requirement as it raises too many audit issues, such as what do the terms 'trained' and 'knowledgeable' mean and what is sufficient for each?

A commenter questioned is an alert required for malicious activity if it is automatically quarantined? In response, the SDT notes that alerts are required for detection of malicious code regardless of any subsequent mitigation actions taken. The SDT believes that if malicious code gets through the layers of defense and makes it way on to a BES Cyber System, that is an event that needs the entity's timely attention and response so the defenses can be shored up for the zero-day that is not detected and quarantined.

One commenter wrote that it was unclear as to whether 'detected failure' refers to logging a failure of some event or failure of logging. In response, the SDT has added a clarification that it is failure of the requirement part 4.1 event logging. This would include the failure of the applicable systems logging capability.

There was a recommendation that the measures should include examples of alerts issued. In response, the SDT agrees and has added this as one of the example measures.

Multiple comments suggested that 4.2.1 should change to 'detected cyber security event' since not all events are necessarily malicious. In response, the SDT agrees and has changed this part to refer to detected malicious code rather than malicious activity.

There were numerous comments suggesting to change the wording in 4.2.1 to 'detected events per 4.1'. In response, the SDT agrees and has added the reference to 4.1 for clarity.

One commenter stated that the guidance implies that only technical means are allowed, but requirement does not preclude procedural controls. In response, the SDT notes that the requirement language is the ruling language and guidance is not auditable and is provided to provide further context or examples or assistance in how entities may want to approach meeting the requirement.

Requirement Part 4.3

There were a multitude of commenters who recommended that the requirement add the phrase "human detected event logging failure" to clarify when the clock starts. In response, the SDT agrees with the concept and has changed the

language to require that the response timeframe begins with the alert of the failure. Therefore, the timeframe begins after something or someone has detected the failure and has generated an alert as in 4.2.

One commenter suggested that 'after notification' should be added after 'next calendar day'. In response, the SDT agrees with the concept and has changed the language to require that the response timeframe begins with the alert of the failure. Therefore, the timeframe begins after something or someone has detected the failure and has generated an alert as in 4.2.

A few respondents commented that the requirement should be struck or change the verbiage to "Document the controls implemented to identify and respond to detected logging failures. Document detected logging failures along with any discrepancies between the actual response and the documented response plan." In response, the SDT agrees and has struck the requirement.

A few commenters stated that the next calendar day is not enough time to rectify issues. In response, the SDT notes the timeframe is to 'activate' a response, not to resolve the issue. The SDT has chosen this in recognition that depending on what caused the failure, there may be widely varying timeframes to resolve the issue. Therefore, the requirement is for timely initiation of a response.

One commenter noted that the requirement presumes but does not prescribe a mechanism for monitoring for logging system failures. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

Several commenter responded that the timeframe is too short due to distances or other operational situations. There was also a suggestion is to include 'next business day'. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

There was one comment that this should only apply to Cyber Assets with ERC. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

Several commenters recommended that outage handling should be standardized with CIP-006. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

There were several comments that the measure should change the word 'attestation' to 'documentation'. In response, the SDT agrees and has made the change.

One comment suggested that the measure should change 'events' to 'failures' to better align with the requirement. In response, the SDT agrees and has made the change.

Requirement Part 4.4

There was a comment that the requirement should change to "Retain BES Cyber System and BES Cyber Asset". In response, the SDT agrees with the concept that the applicability in the requirement did not match the applicability column and has removed the applicability from the requirement by replacing 'BES Cyber System' with 'applicable'.

There were several comments that the TFE language should be struck and add 'within the BCS capabilities." In response, the SDT notes that this requirement is scoped to Control Center environments where the highest degree of logging is required and has the highest degree of more capable Cyber Assets. The SDT feels that in this environment, the industry really should push for 90 days of log retention on these systems.

One commenter suggested that this should apply to all Medium's that can store logs, not just those at control centers. In response, the SDT notes that with the vastly increased numbers and types of field devices that Version 5 will bring into scope, most of which are legacy devices, that putting a mandatory requirement in place that prescribes the length of log retention is not warranted and would cause numerous TFE's.

One commenter wrote that 'identified in 4.1' should be the main qualification for log retention and delete the 'security related' portion for clarity. In response, the SDT agrees and has removed the phrasing.

Some commenters stated that this is in conflict with evidence retention section. Auditors expect to ask for any day's logs in past three years. In response, the SDT has added guidance around this topic. The requirement that is to be audited is

that applicable cyber assets maintain 90 days of logs. The compliance evidence requirement is that the entity be able to show that for the historical compliance period, the applicable cyber systems maintained 90 days of logs. The guidance speaks of records of disposition of logs after their 90 days is up.

BPA commented that a media hardware failure that results in loss of stored logs is still a violation. In response, the SDT agrees and has added "except under CIP Exceptional Circumstances" to the requirement as it includes hardware failure.

One commenter stated that this should allow for a timeframe as determined by the Responsible Entity. In response, the SDT notes that 90 days has been the precedent through the previous CIP versions and having no bound means that zero days is valid if determined by the entity. The SDT believes that 90 days is a sufficient lower bound for Control Center environments and has no justification for lowering it in the highest risk environments.

A commenter suggested that the applicability should apply to medium impact with ERC. In response, the SDT notes that this applies to Control Centers. Throughout the history of the CIP standards, all cyber assets in a Control Center are in scope regardless of external connectivity. The SDT believes there is insufficient justification to lower the standard on this point.

One commenter implied that measure 2 requests info about log data that is not in the requirement. Measures 1 and 3 cover the requirement. In response, the SDT agrees and has moved this to the guidance section with a more detailed explanation of the difference between the requirement's retention period for security purposes and the overall standard's requirement for compliance measurement purposes.

Requirement Part 4.5

Many responders commented that clarity around who determines the appropriate sampling should be added by including 'sampling as deemed appropriate by the Responsible Entity'. In response, the SDT agrees and has made the change.

Several commenters noted that the applicability should be 'High impact including associated PCA' to clarify logging reviews aren't at the device level and should exclude EACM/PACMs. In response, the SDT agrees and has modified the applicability, however EACMs should be included. Since Electronic Access Points to ESP's are EACMs, this is one of the primary logs that should be reviewed.

Several commenters expressed concern that this needs some minimum expectations for logged event review. In response, the SDT notes the intent is included in the requirement which is to identify undetected security incidents. The FERC Order in paragraphs 525 and 628 states, "However, the Commission continues to believe that, while automated review systems provide a reasonable day-to-day check of the system and a convenient screening for obvious system breaches, periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings. Furthermore, manual review is beneficial to judge the effectiveness of protection measures, such as firewall settings. If a firewall setting is incorrect or ineffective, an automated review system may not identify a cyber security intrusion. For those entities without automated log review and alerts, it is even more important to perform a manual review because this will be the only review of the logs." The SDT believes the intent is that entities manually review logs to insure that automated tools are tuned and alerting on real incidents. The SDT does not believe it should get more prescriptive with the requirement.

There were several commenters who noted that the requirement should change to "Document and implement a secondary control(s), and an associated interval, not to exceed two weeks, to assure the generation, capture, monitoring, and alerting of events as identified in 4.1." In response, the SDT notes that the FERC Order 706 in paragraphs 525 and 628 are explicit about a manual review. Also, the events identified in 4.1 are requirements so identifying events in 4.5 that should have been caught in 4.1 is a violation. The intent is for the entity to review the logs to see if there are events happening (other than those in 4.1) that the entity should be alerting on. In essence, this is a 'tuning' requirement to insure that an entity's automated Security Information and Event Management (SIEM) type tools are not missing conditions that are appearing in the logs and going undetected.

One commenter suggested that the requirement should change 'undetected' to 'potential Cyber Security Incidents not previously identified or detected'. In response, the SDT notes that in draft one the language included terms such as "unanticipated" and "potential" and received numerous comments to remove these subjective terms.

There were a number of concerns that two weeks is too short and suggest monthly or two month periodicity. In response, the SDT notes that in paragraph 628 of FERC Order 706 states, "The Commission continues to believe that, in general, logs should be reviewed at least weekly", but leaves it to the ERO to determine the appropriate timeframe. The SDT believes that bi-weekly is an appropriate timeframe given the Commission's statement concerning weekly reviews.

There was a comment that the phrase “at a minimum every two weeks” could be misconstrued and suggested to mean “at intervals no greater than 15 days.” In response, the SDT agrees that two weeks is a maximum not a minimum and adopts the suggested change.

There was a suggestion in changing the requirement to read “Review a summarization or sampling of logged events that the Responsible Entity has determined could identify previously undetected Cyber Security Incidents. Such a review will be conducted every two weeks at a minimum.” In response, the SDT agrees with the issue and has reworded the requirement based on this and other comments to utilize ‘intervals no greater than 15 days’ for greater specificity.

One commenter suggested that the timeframe should be determined by the Responsible Entity. In response, the SDT notes that in paragraph 628 of FERC Order 706 the Commission ordered the ERO to determine an appropriate timeframe that is less than the 90 days in the requirements of previous versions while stating that weekly reviews are their recommendation. The SDT sees no justification for how this directive can be met if the timeframe is left completely up to the entity to determine.

There were multiple suggestions that the applicability should only apply when automated processes and alerting are not possible or no managed service provider is utilized. In response, the SDT notes from paragraph 525 of FERC Order 706 that “the Commission continues to believe that, while automated review systems provide a reasonable day-to-day check of the system and a convenient screening for obvious system breaches, periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings.” The Commission goes on to order the inclusion of manual review even if automated alerts are employed.

One commenter stated that a SIEM is the only real solution and is too expensive for small entities. In response, the SDT notes the requirement is for a manual review, not an automated review. Paragraph 525 of Order 706 makes it clear that even if automated systems are used, the manual review is still required. The requirement does not require installation of SIEM tools, but requires manual review even if SIEM tools are in use.

Several commenters noted that the phrase “signed and” should be deleted in the measure (also in 4.1 measure). In response, the SDT agrees that a signed approval of the review is not in the requirement and this has been deleted from the measure.

QUESTION B24– CIP-007-5 REQUIREMENT R5:

If you disagree with the changes made to CIP-007-5, Requirement R5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, some of the key issues expressed by commenters included (1) the applicability to Medium Impact BES Cyber Systems with external routable connectivity, particularly in requirement part 5.1 and (2) the obligation for the CIP Senior Manager to authorize specific account types for BES Cyber Systems. The consideration of comments according to major issues and standard sections follows.

Correcting Deficiencies

One comment stated that this requirement should have a find, fix, track, and report mechanism built in so that entities can fix administrative deficiencies rather than consider them a violation of the requirement. In response, the CIP Version 5 approach to correcting deficiencies is that each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable items in the specified table. This approach of correcting deficiencies complements the compliance concept of internal controls.

Applicability to Low Impact

One commenter suggested that CIP-007-5 R5 should apply to Low Impact BES Cyber Systems. In response, we note the challenge of applying device-specific mandatory and enforceable requirements to low impact BES Cyber Systems exists in the overwhelming number of BES Cyber Assets. NERC survey results from the 2011 CIP filing indicate 90% of the facilities would be considered low impact, and each of these sites can have a potentially large number of Cyber Assets. As a result, the SDT has taken the approach of applying policy level requirements to BES Cyber Systems with the understanding and expectation that the compliance audit and enforcement of the policies will adapt to the significant increase.

TFE for all Requirement Parts

One commenter suggested adding TFE language for the entire requirement due its technical nature. In response, the SDT has identified requirement parts that intentionally allow for a safe-harbor exception process where equivalent mitigation can be shown. However, in some cases, we do not intend the technical limitations of the device to indicate a violation or need for safe-harbor (e.g. password complexity).

Multifactor Authentication
One commenter questioned if multi-factor authentication can replace password authentication without a TFE. In response, the SDT notes that the said requirement applies to password-only authentication but do not preclude other strong authentication mechanisms.

Procedural Controls
One commenter suggested, with regard to CAN-0017, procedural controls should be explicitly allowed in the requirement. However, the SDT points out that Compliance Application Notices do not carry forward to new versions of the standard. Previous versions require both procedural and technical controls for passwords, but this language is not included in the current draft. It would cause more confusion to explicitly allow procedural controls for each requirement part.

Version 5
One commenter provided its fundamental objection to Version 5 and suggested that implementation of the current CIP standards should be allowed to mature. The SDT is required to address all the FERC directives from Order 706, and FERC Order 706 has directed the ERO to complete consideration of Order 706 directives by March 31st, 2013.

Summary of Changes Section
Two commenters noted the summary of changes does not correspond to requirements for shared accounts, and in response the SDT has deleted this section which was held over from previous versions.

Requirement Part 5.1
Several entities commented this requirement part should be limited to medium impact with External Routable Connectivity, and the SDT has made this change. However, this requirement still applies to Medium Impact BES Cyber Systems at Control Centers.

Several commented that user access should be a defined term and security controls for system accounts should also exist. In response, we provide a definition in the guidelines, and we believe this term is well understood. In addition, the SDT has added a qualifier for this to apply to interactive user access. We do not define the same controls for system access due to the widely diverse way this could apply. System accounts do not uniformly apply across all devices and operating systems.

Several entities suggested rewording the phrase “where technically feasible” to “within the capability of the BES Cyber System”. In response, the alternative language would not change the TFE trigger for this requirement. There are several instances in which strict compliance can still be met in the absence of a specific technology mechanism to enforce access. The SDT has provided examples in the rationale box for requirement part 5.1 and improved the requirement language to make this point clear.

One commenter requested clarification that user access does not mean front panel read-outs on a device. In response, the SDT has changed “user access” to “interactive user access”, and the SDT has added a rationale statement further describing the intent of this requirement, in which the SDT has explicitly stated front panel read-outs do not qualify as interactive user access.

One commenter proposed that this requirement should be rephrased to limit to only electronic access. In response, the subject matter of the standard and requirement suffice to make the distinction, and we do not want to limit or confuse the possibility of using properly configured physical access controls to demonstrate compliance with this requirement.

One commenter suggested this apply to accounts and not user access. In response, the SDT has chosen to apply this to interactive user access because there may be instances where you do not want to enforce authentication for read-only access.

One commenter suggested specifying the phrase “applicable cyber assets” to qualify this requirement, but the applicability column already qualifies the requirement.

Requirement Part 5.2

Several entities suggested deleting requirement part 5.2 because it is already covered by the CIP-004-5 requirement to authorize users. In response, this requirement only deals with identifying the use of account types. It has been modified to make the intent clearer. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The requirement part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Several commenters advised removing the CIP Senior Manager as the person authorizing these account types. In response, the SDT chose not to remove this in the previous posting as suggested by our previous response to comments, and the SDT has removed the CIP Senior Manager as the person authorizing the account types in this posting.

One commenter proposed that generic accounts must be specified. In response, the SDT has added examples in the guidance section of this standard. The section added reads: "Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level."

One commenter suggested removing the word "authorized" from this requirement. The SDT has incorporated this suggestion by replacing the word "authorized" with the phrase "identify and inventory".

There was a comment submitted as to whether this requirement restricts the use of the specified account types. In response, identification of the accounts provides the necessary control. We do not specify these accounts must be disabled or removed because they are sometimes necessary for operation. Restricting these based on least privilege or need to know is already covered in CIP-004-5 R6.

One commenter suggested that authorization by "delegate(s)" be substitute for "delegate". However, the SDT has removed the requirement to authorize by CIP Senior Manager based on other commenters.

Requirement Part 5.3

Several comments suggested deleting requirement part 5.3 because it is already covered in CIP-004-5 requirements to authorize access. However, the identification of individuals with access to shared account has the additional objective of mitigating the risk of unauthorized access through shared accounts. This differs from the CIP-004-5 Requirement R6 to authorize access. An entity can authorize access and still not know who has access to a shared account. This would make it difficult to revoke access when it is no longer needed.

Several suggested incorporating the change rationale stating that the phrase "individuals storing, losing or inappropriately sharing a password is not a violation of this requirement." In response, the SDT has added this language to the rationale box for CIP-007-5 R5. The language in this section reads, "The term "authorized" is used in the

requirement to make clear that an individual storing, losing or inappropriately sharing a password is not a violation of this requirement."

Multiple commenters suggested adding the word "authorized" as a qualifier for access to correspond to the requirement language, and the SDT has made this change.

One commenter suggested that this requirement does not go far enough to restrict the use of privileged access, particularly when operating software. In response, CIP-004-5 R6 restricts the use of privileged access to only those having a documented business need. We do not specify the individual use of privileged and non-privileged access because this is not auditable for mandatory enforceable requirements. This is a good practice, but if this practice were codified in a standard, any individual not following the policy would impose monetary penalties on an organization.

One commenter suggested that the external routable connectivity qualifier should be removed for this Requirement Part in the applicability to match requirement part 5.2. In response, the requirement parts are unrelated, and the qualifier matches that of CIP-004-5 R6, which requires the authorization for electronic access.

Requirement Part 5.4

Several comments suggested revising this requirement part to address a recent RuggedCom vulnerability where a default password was unique to publicly known attributes of the device. In response, the SDT has removed the requirement exception where the "default password is unique to the device or instance of the application", and specified in the rationale that "pseudo-randomly system generated passwords are not considered default passwords".

Several commenters suggested adding the word "known" as a qualifier to default password to avoid the case where the entity was not aware of an undocumented default password by the vendor. The SDT has made this change.

There were several comments that the measure should change the phrase "new devices are deployed" to "new devices are in production" and one commenter suggested removing the phrase altogether since timeframes are covered in the implementation plan. The SDT has made this change from the word "deployed" to "in production", but the timeframe here does not conflict with the implementation timeframe and provides example, high quality evidence to meet this requirement.

One commenter requested clarification of when the default password should be changed. In response, we do not specify a timeframe (i.e. when cyber assets go into production) which could be misinterpreted. Instead, as with all requirements of CIP-007-5, this requirement must be met when a device becomes one of the applicable systems or assets.

Several commenters suggested removing the term "Cyber Assets" within the requirement to match the applicability of BES Cyber System. In response, the SDT has removed this language in deference to the applicability column.

One commenter requested clarification that default password that are unchanged would require changing according to R5.6. In response, this may be the case for interactive user accounts, but this is not necessary to state in the requirement. Changing default passwords meets a different objective to prevent unauthorized access from known credentials.

One commenter suggested excepting when a password is unique to the device. However, many commenters point out that doing so would allow for vulnerabilities where the uniqueness of the device where publicly known (i.e. MAC address).

Requirement Part 5.5

Several commenters suggested modifying the measure for requirement part 5.5 and requirement part 5.6 to better describe the attestation. Another commenter suggested replacing attestations with the ability to present a procedure. Others noted that it is not possible to obtain attestation from unionized workers and suggested adding a separate requirement to use training as a procedural control in place of attestations. In response, the SDT has used provided language to better describe the attestation evidence. The suggestion to use presentation of a procedure as a replacement cannot be used as evidence of implementing a procedure. The suggestion to have a further requirement for training is already covered in the training program specified in CIP-004-5.

One commenter stated that password complexity should be enforced to the maximum extent technically possible. In response, the SDT noted such a policy would create situations where users must write down passwords to remember them. The maximum extent could be exorbitant in some cases.

One commenter also stated that the guidelines state this requirement part is for password-only authentication, but the requirement does not include the same stipulation. BPA and Salt River Project made similar comments to distinguish the case where a PIN is used for multi-factor authentication. In response, the SDT has changed "password-based" to "password-only" in both requirement part 5.5 and 5.6.

Several commenters suggested using verbiage for requirement part 5.5.1: “Password length that is, at least, eight characters or the up to the maximum allowable by the system if that maximum is less than eight.” In response, although the proposed verbiage is cleaner, it becomes less clear once we specify “system” and the number of characters in the proposal. The SDT therefore decided to continue with the currently drafted language.

One commenter questioned if this new requirement will remove CAN-0017. In response, CANs do not apply to future versions of the standard, and the SDT has explicitly addressed the issue raised by CAN-0017 that either technical or procedural mechanisms can meet the requirement.

One commenter stated that it does not agree with the proscription of password requirements. In response, the SDT has included more prescriptive password requirements in response to a large number of industry comments against having added flexibility. However, the SDT has also attempted to remove some of the problematic provisions of the current version of password requirements that would allow entities to have stronger password policies.

One commenter suggested that the password complexity in requirement part 5.5.2 should specify or define the word “type”. In response, the examples provided in the requirement suffice for specifying password character types. The SDT believes these terms are well-understood by industry and do not necessitate further definitions.

Requirement Part 5.6

Several commenters pointed out the guidance, particularly the recommended password length table, has not updated to reflect the requirement. In response, the SDT has deleted sections of the guidance which no longer have relevance to the requirement.

Several commenters suggested adding a technical feasibility clause to this requirement part because some devices do not allow this capability. In response, the SDT notes that this only applies to user access, and the SDT has modified the requirement part to clarify this. The language as the end of this requirement part reads, “…at least once each calendar year, not to exceed 15 calendar months between changes, where technically feasible.”

One commenter suggested this requirement part explicitly apply to interactive user access, and the SDT has modified this requirement part to address the concern. The beginning of this requirement part reads, “For password-only authentication for interactive user access, either technically or procedurally enforce password changes…”

One commenter suggested adding the language “unless it impacts operation of the BES” to this requirement part. In response, the SDT has added the phrase “where technically feasible” to address these type of exceptions.

One commenter suggested the applicability of 5.6 be modified to match other requirement parts in CIP-007-5 R5. In response, the applicability to those Medium Impact BES Cyber Systems with External Routable Connectivity is due to the periodic nature of this requirement, which may only be feasible on large systems by having such connectivity. The commenter also suggested periodically is misspelled periodicity, but the SDT intends the latter as this is an attribute of the policy instead of a modifier.

One commenter suggested incorporating the language in the guidance table to include periodicity provisions for plant outages and disabled accounts. In response, for disabled accounts, a password change is not required because these do not qualify as providing interactive user authentication. The requirement does not have provisions for plant outages due to the widely varying schedules for plant outages. The SDT also notes that this requirement applies to those Medium Impact BES Cyber Systems with External Routable Connectivity.

A commenter proposed having a password change every 15 months. The SDT has incorporated this suggestion as part of an overall modification of annual periodic requirements in the CIP standards.

A commenter proposed to allow the entity to specify a password change periodicity, but the SDT has specified this periodicity based on a large number of comments against having this flexibility.

There was one comment that suggested the password change periodicity should be much shorter (i.e. quarterly). In response, the SDT notes that password change requirements should be considered in context with all of the password requirements, and shorter password change requirements can often result in poor password protection and selection by individuals.

Requirement Part 5.7

Several commenters suggested this requirement has the potential for creating a denial of service vulnerability to lockout all accounts to the system if entities configure all accounts for lockout. The SDT has not included the proposal to specify “user accounts” for limiting login attempts because it is too specific and has the potential to cause confusion. Although

the requirement does not prescribe this vulnerability, it does allow for it. Consequently, the SDT has included guidance in avoiding this configuration in the rationale.

Several commenters requested clarification on what the clause "where technically feasible" qualifies for this requirement part. In response, this requirement part has been modified to make clear the TFE triggering language qualifies both options. Furthermore, a TFE would only be necessary based on failure to implement either option.

Several commenters suggested this requirement should be deleted as it was not directed by FERC or otherwise align with the alerting requirements of CIP-007-5 requirement part 4.2. In response, this requirement is part of a more reasonable overall password security standard. As a trade-off to providing more flexibility to password policies, this requirement is highly effective to prevent online password attacks. This does not duplicate CIP-007-5 requirement part 4.2 because this alert is not required to be configured by that requirement.

One commenter requested additional guidance on the threshold for unsuccessful login attempts. The SDT has added this to the guidance section of this standard. Language was added which reads, "The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate."

Multiple commenters suggested that a minimum threshold parameter for account lockout should be specified. In response, a value is not specified here because this requirement protects against password cracking through online password cracking. Given the additional password policy requirements, the threshold for this setting can be very high, up to 100 or more.

One commenter requested the requirement part make clear these do not apply to Protected Cyber Assets such as printers and multi-function machines. In response, this requirement does apply to Protected Cyber Assets. This is a part of an overall protection against unauthorized access, which would include Protected Cyber Assets that have direct connections with the BES Cyber System.

VRFs

There was one comment that suggested the VRF should be Lower for Medium Impact BES Cyber Systems. In response, the impact level of the BES Cyber System is accounted for by the applicability of CIP-004 through CIP-011 requirements. A violation for a Medium Impact BES Cyber System cannot be considered directly with a High Impact BES Cyber System because they have less application of compensating security requirements.

VSLs

There was one comment that noted the High VSL includes the phrase “use of” where the associated requirement refers to only enablement of generic accounts and that the Severe VSL includes criteria for failure to implement password procedures, which might imply the required use of passwords. The VSL language regarding the enablement of generic account types has been updated to match the requirement. We do not agree the Severe VSL language implies a requirement to only use passwords. The VSLs are only used to describe violations, and use of authentication alternatives to passwords would not be a violation.

One commenter noted the Severe VSL is not consistent with the requirement and the SDT has updated the VSLs to align with modifications to the requirement.

Guideline

There was a recommendation that the guideline section needs to define generic accounts, and the SDT has added this to the guidelines.

Questions with Votes Only:

CIP-004, CIP-005, CIP-006 and CIP-007 Questions:

1. CIP-004-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
NESCOR/NESCO	No
ACES Power Marketing	No
Hydro One	No
Southern California Edison company	No
Progress Energy	No
Independent Electricity System Operator	No

Organization	Yes or No
NextEra Energy, Inc.	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
New York Power Authority	No
Springfield Utility Board	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC Registered Affiliates	Yes
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
Duke Energy	Yes
PNGC Comment Group	Yes

Organization	Yes or No
Dominion	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes

Organization	Yes or No
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes

Organization	Yes or No
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
MidAmerican Energy Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes

Organization	Yes or No
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Oncor Electric Delivery Company LLC	Yes
PJM Interconnection	Yes
NIPSCO	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes

Organization	Yes or No
Utility Services Inc	Yes
Alliant Energy	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

2. **CIP-004-5 R2 states "Each Responsible Entity shall have a role-based cyber security training program to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?**

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
ACES Power Marketing	No

Organization	Yes or No
SPP and Member companies	No
IRC Standards Review Committee	No
CenterPoint Energy	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Arizona Public Service Company	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No

Organization	Yes or No
LCEC	No
Niagara Mohawk (dba National Grid)	No
National Grid	No
Snohomish County PUD	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Northeast Utilities	No
San Diego Gas & Electric	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No

Organization	Yes or No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Alliant Energy	No
New York Power Authority	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No
PNGC Comment Group	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc (NCR01177,	Yes

Organization	Yes or No
JRO00088)	
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes

Organization	Yes or No
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Lakeland Electric	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
PSEG	Yes
Texas Reliability Entity	Yes
NIPSCO	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes

Organization	Yes or No
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

3. CIP-004-5 R3 states "Each Responsible Entity shall implement its documented role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
ACES Power Marketing	No
IRC Standards Review Committee	No

Organization	Yes or No
CenterPoint Energy	No
PNM Resources	No
CIP Version 5 Comment SME list	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Northeast Utilities	No
Nebraska Public Power District	No

Organization	Yes or No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
Alliant Energy	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes

Organization	Yes or No
NRG Energy Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
SPP and Member companies	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Hydro One	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes

Organization	Yes or No
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
PSEG	Yes
Texas Reliability Entity	Yes
NIPSCO	Yes

Organization	Yes or No
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

4. CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
Texas RE NERC Standards Review Subcommittee	No
Colorado Springs Utilities	No
ACES Power Marketing	No
IRC Standards Review	No

Organization	Yes or No
Committee	
CenterPoint Energy	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Southern Company Services, Inc.	No
Southern California Edison company	No
Progress Energy	No
LCEC	No
Bonneville Power Administration	No
Snohomish County PUD	No
MidAmerican Energy Company	No

Organization	Yes or No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Utility Services Inc	No
New York Power Authority	No

Organization	Yes or No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
Southwest Power Pool Regional Entity	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes

Organization	Yes or No
NCEMC	Yes
SPP and Member companies	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Arizona Public Service Company	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Independent Electricity System Operator	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services	Yes

Organization	Yes or No
Corporation	
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
MEAG Power	Yes
Portland General Electric	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of	Yes

Organization	Yes or No
Water and Power	
US Bureau of Reclamation	Yes
California ISO	Yes

5. CIP-004-5 R5 states "Each Responsible Entity shall implement one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Texas RE NERC Standards Review Subcommittee	No
ACES Power Marketing	No
IRC Standards Review Committee	No
Salt River Project	No
Southern California Edison company	No
Progress Energy	No
LCEC	No
MidAmerican Energy	No

Organization	Yes or No
Company	
Lakeland Electric	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
PSEG	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Northeast Power Coordinating Council	Yes

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	Yes
NRG Energy Companies	Yes
Duke Energy	Yes
PNGC Comment Group	Yes
Dominion	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes

Organization	Yes or No
SPP and Member companies	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
BC Hydro	Yes
Hydro One	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Independent Electricity	Yes

Organization	Yes or No
System Operator	
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes

Organization	Yes or No
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
NIPSCO	Yes
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes

Organization	Yes or No
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

Organization	Yes or No
Kansas City Power & Light	Yes
California ISO	Yes

6. CIP-004-5 R6 states "Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R6?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
FirstEnergy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
Pepco Holdings Inc & Affiliates	No
SMUD & BANC	No

Organization	Yes or No
PNM Resources	No
CIP Version 5 Comment SME list	No
Southern Company Services, Inc.	No
Southern California Edison company	No
Progress Energy	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Xcel Energy	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Lakeland Electric	No
Ameren	No

Organization	Yes or No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
NYISO	No
Farmington Electric Utility System	No
Kansas City Power & Light	No
California ISO	No
Northeast Power Coordinating Council	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Hydro One	Yes
Arizona Public Service	Yes

Organization	Yes or No
Company	
Western Area Power Administration	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
NIPSCO	Yes
ISO New England Inc.	Yes

Organization	Yes or No
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes

Organization	Yes or No
US Bureau of Reclamation	Yes

7. CIP-004-5 R7 states "Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R7?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Colorado Springs Utilities	No

Organization	Yes or No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Florida Municipal Power Agency	No
SMUD & BANC	No
ACES Power Marketing	No
SPP and Member companies	No
Puget Sound Energy, Inc.	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Arizona Public Service Company	No
Southern Company Services, Inc.	No
Southern California Edison company	No

Organization	Yes or No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
ATCO Electric	No
LCEC	No
Consumers Energy Company	No
Xcel Energy	No
NV Energy	No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No

Organization	Yes or No
Lakeland Electric	No
Ameren	No
NextEra Energy, Inc.	No
Northeast Utilities	No
Texas Reliability Entity	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
MEAG Power	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Network & Security Technologies, Inc.	No
Alliant Energy	No
New York Power Authority	No
Springfield Utility Board	No
NYISO	No
Farmington Electric Utility System	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Los Angeles Department of Water and Power	No
Brazos Electric Power Cooperative	No
US Bureau of Reclamation	No
Kansas City Power & Light	No
California ISO	No

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	Yes
PNGC Comment Group	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Services	Yes

Organization	Yes or No
Corporation	
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
PSEG	Yes
Portland General Electric	Yes
Utility Services Inc	Yes
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes

Organization	Yes or No
Cowlitz County PUD	Yes

10. CIP-005-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
MRO NSRF	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
ACES Power Marketing	No

Organization	Yes or No
SPP and Member companies	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
CIP Version 5 Comment SME list	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Xcel Energy	No
Bonneville Power Administration	No
Tampa Electric Company	No
MidAmerican Energy	No

Organization	Yes or No
Company	
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Alliant Energy	No
New York Power Authority	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No

Organization	Yes or No
NRG Energy Companies	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Oncor Electric Delivery Company LLC	Yes

Organization	Yes or No
NIPSCO	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of	Yes

Organization	Yes or No
Water and Power	
US Bureau of Reclamation	Yes

11. CIP-005-5 R2 states "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No

Organization	Yes or No
ACES Power Marketing	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
Progress Energy	No
Hydro-Quebec TransEnergie	No
Lincoln Electric System	No
Bonneville Power Administration	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No

Organization	Yes or No
PSEG	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
New York Power Authority	No
NYISO	No
Tucson Electric Power	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
Southwest Power Pool Regional Entity	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Southern California Edison company	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba	Yes

Organization	Yes or No
National Grid)	
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
NIPSCO	Yes
MEAG Power	Yes

Organization	Yes or No
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

14. CIP-006-5 R1 states "Each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards	No

Organization	Yes or No
Review Subcommittee	
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Florida Municipal Power Agency	No
NCEMC	No
ACES Power Marketing	No
SPP and Member companies	No
IRC Standards Review Committee	No
CenterPoint Energy	No
Puget Sound Energy, Inc.	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Arizona Public Service	No

Organization	Yes or No
Company	
Southern Company Services, Inc.	No
Western Area Power Administration	No
Salt River Project	No
National Rural Electric Cooperative Association (NRECA)	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Lower Colorado River Authority	No
LCEC	No
LCRA Transmission Services Corporation	No

Organization	Yes or No
Lincoln Electric System	No
United illuminating Company	No
Xcel Energy	No
NV Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Lakeland Electric	No
Tennessee Valley Authority	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Northeast Utilities	No
PSEG	No

Organization	Yes or No
San Diego Gas & Electric	No
Texas Reliability Entity	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
MEAG Power	No
Portland General Electric	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Alliant Energy	No

Organization	Yes or No
Pacific Gas and Electric Company	No
NYISO	No
Exelon Corporation and its affiliates	No
Deseret Power	No
Los Angeles Department of Water and Power	No
Brazos Electric Power Cooperative	No
US Bureau of Reclamation	No
Kansas City Power & Light	No
California ISO	No
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Pepco Holdings Inc & Affiliates	Yes
Tri-State G&T - Transmission	Yes

Organization	Yes or No
Southern California Edison company	Yes
Clallam County PUD No.1	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
The Empire District Electric Company	Yes
Utility Services Inc	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Farmington Electric Utility	Yes

Organization	Yes or No
System	
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes

15. CIP-006-5 R2 states "Each Responsible Entity shall implement one or more documented visitor control programs that include each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Duke Energy	No
Dominion	No
Florida Municipal Power Agency	No
PNM Resources	No
BC Hydro	No
Western Area Power Administration	No
Progress Energy	No
Independent Electricity	No

Organization	Yes or No
System Operator	
Hydro-Quebec TransEnergie	No
LCEC	No
Xcel Energy	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Lakeland Electric	No
NextEra Energy, Inc.	No
PJM Interconnection	No
Wisconsin Electric Power Company	No
Portland General Electric	No
City Utilities of Springfield, MO	No
NYISO	No
Exelon Corporation and its	No

Organization	Yes or No
affiliates	
Deseret Power	No
Los Angeles Department of Water and Power	No
California ISO	No
Northeast Power Coordinating Council	Yes
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC)	Yes

Organization	Yes or No
including OPC, GTC & GSOC	
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Hydro One	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes

Organization	Yes or No
Southern California Edison company	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power	Yes

Organization	Yes or No
Administration	
Snohomish County PUD	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Oncor Electric Delivery Company LLC	Yes
NIPSCO	Yes
City of Austin dba Austin Energy	Yes

Organization	Yes or No
ISO New England Inc.	Yes
MEAG Power	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

Organization	Yes or No
Kansas City Power & Light	Yes

16. CIP-006-5 R3 states "Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
NESCOR/NESCO	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
IRC Standards Review Committee	No
CenterPoint Energy	No

Organization	Yes or No
PNM Resources	No
Hydro One	No
Western Area Power Administration	No
Progress Energy	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
LCEC	No
Xcel Energy	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Lakeland Electric	No
NextEra Energy, Inc.	No

Organization	Yes or No
Texas Reliability Entity	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
Portland General Electric	No
City Utilities of Springfield, MO	No
New York Power Authority	No
Los Angeles Department of Water and Power	No
PPL Corporation NERC Registered Affiliates	Yes
Duke Energy	Yes
Dominion	Yes
FirstEnergy	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Southern California Edison company	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
NIPSCO	Yes
MEAG Power	Yes
Network & Security	Yes

Organization	Yes or No
Technologies, Inc.	
Utility Services Inc	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

Organization	Yes or No
Kansas City Power & Light	Yes
California ISO	Yes

18. CIP-007-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Florida Municipal Power Agency	No
SMUD & BANC	No

Organization	Yes or No
CenterPoint Energy	No
PNM Resources	No
Western Area Power Administration	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
LCEC	No
Consumers Energy Company	No
Xcel Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
MidAmerican Energy	No

Organization	Yes or No
Company	
Lakeland Electric	No
NextEra Energy, Inc.	No
PJM Interconnection	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
NYISO	No
Exelon Corporation and its affiliates	No
Kansas City Power & Light	No
California ISO	No
Northeast Power Coordinating Council	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
MRO NSRF	Yes

Organization	Yes or No
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Hydro One	Yes
CIP Version 5 Comment SME list	Yes

Organization	Yes or No
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
NV Energy	Yes

Organization	Yes or No
Snohomish County PUD	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Oncor Electric Delivery Company LLC	Yes
NIPSCO	Yes
City of Austin dba Austin Energy	Yes

Organization	Yes or No
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

19. CIP-007-5 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
SMUD & BANC	No
CenterPoint Energy	No
PNM Resources	No

Organization	Yes or No
Hydro One	No
Arizona Public Service Company	No
Western Area Power Administration	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Hydro-Quebec TransEnergie	No
LCEC	No
Lincoln Electric System	No
Xcel Energy	No
Bonneville Power Administration	No
Tampa Electric Company	No
MidAmerican Energy Company	No

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Utility Services Inc	No
Alliant Energy	No
New York Power Authority	No

Organization	Yes or No
Pacific Gas and Electric Company	No
NYISO	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Kansas City Power & Light	No
PPL Corporation NERC Registered Affiliates	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
Dominion	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power	Yes

Organization	Yes or No
Agency	
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Independent Electricity System Operator	Yes

Organization	Yes or No
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
NIPSCO	Yes
MEAG Power	Yes
Portland General Electric	Yes
Springfield Utility Board	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power	Yes

Organization	Yes or No
Cooperative	
US Bureau of Reclamation	Yes
California ISO	Yes

20. CIP-007-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
SPP and Member companies	No
CenterPoint Energy	No

Organization	Yes or No
PNM Resources	No
Hydro One	No
CIP Version 5 Comment SME list	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Bonneville Power Administration	No
Snohomish County PUD	No
MidAmerican Energy Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No

Organization	Yes or No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Alliant Energy	No
New York Power Authority	No
Pacific Gas and Electric Company	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC	Yes

Organization	Yes or No
Registered Affiliates	
NRG Energy Companies	Yes
PNGC Comment Group	Yes
Dominion	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes

Organization	Yes or No
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes

Organization	Yes or No
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes

Organization	Yes or No
NIPSCO	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes

Organization	Yes or No
US Bureau of Reclamation	Yes

21. CIP-007-5 R4 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No

Organization	Yes or No
SMUD & BANC	No
SPP and Member companies	No
IRC Standards Review Committee	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
CIP Version 5 Comment SME list	No
Western Area Power Administration	No
Salt River Project	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No

Organization	Yes or No
Hydro-Quebec TransEnergie	No
Lower Colorado River Authority	No
LCEC	No
LCRA Transmission Services Corporation	No
Niagara Mohawk (dba National Grid)	No
National Grid	No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Lakeland Electric	No

Organization	Yes or No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
PSEG	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Utility Services Inc	No

Organization	Yes or No
Alliant Energy	No
New York Power Authority	No
Pacific Gas and Electric Company	No
NYISO	No
Tucson Electric Power	No
Los Angeles Department of Water and Power	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC Registered Affiliates	Yes
PNGC Comment Group	Yes
Dominion	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes

Organization	Yes or No
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Clallam County PUD No.1	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
United illuminating Company	Yes
Xcel Energy	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
MEAG Power	Yes
Portland General Electric	Yes
Springfield Utility Board	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes

Organization	Yes or No
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

22. CIP-007-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No

Organization	Yes or No
SMUD & BANC	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
Southern Company Services, Inc.	No
Salt River Project	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Lower Colorado River Authority	No
LCRA Transmission Services Corporation	No
Consumers Energy Company	No

Organization	Yes or No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Lakeland Electric	No
Tennessee Valley Authority	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No

Organization	Yes or No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
Portland General Electric	No
City Utilities of Springfield, MO	No
Alliant Energy	No
New York Power Authority	No
NYISO	No
Tucson Electric Power	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC Registered Affiliates	Yes
PNGC Comment Group	Yes
Associated Electric	Yes

Organization	Yes or No
Cooperative, Inc (NCR01177, JRO00088)	
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Western Area Power Administration	Yes
Clallam County PUD No.1	Yes
Hydro-Quebec TransEnergie	Yes
ATCO Electric	Yes
LCEC	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Northeast Utilities	Yes
PSEG	Yes

Organization	Yes or No
Texas Reliability Entity	Yes
NIPSCO	Yes
MEAG Power	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

Organization	Yes or No
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards
Comment Form C
CIP-008 through CIP-011

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Index to Questions, Comments, and Responses

Questions with Summaries Included: 16
QUESTION C4 – CIP-008-5: 16
QUESTION C8 – CIP-009-5: 26
QUESTION C12 – CIP-010-1: 39
QUESTION C15 – CIP-011-5: 63
Questions with Votes Only: 71
1. CIP-008-5 R1 states "Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 71
2. CIP-008-5 R2 states "Each Responsible Entity shall implement its documented Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 78
3. CIP-008-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?..... 85
5. CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?..... 92
6. CIP-009-5 R2 states "Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 99
7. CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3? 106
9. CIP-010-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration

Change Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 113

10. CIP-010-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 120

11. CIP-010-1 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3? 127

13. CIP-011-1 R1 states "Each Responsible Entity shall implement an information protection program that includes each of the applicable items in CIP-011-1 Table R1 – Information Protection." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 134

14. CIP-011-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 141

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
11. Bruce Metruck	New York Power Authority	NPCC 6										
12. Lee Pedowicz	Northeast Power Coordinating Council	NPCC 10										
13. Robert Pellegrini	The United Illuminating Company	NPCC 1										
14. Si Truc Phan	Hydro-Quebec TransEnergie	NPCC 1										
15. David Ramkalawan	Ontario Power Generation, Inc.	NPCC 5										
16. Brian Robinson	Utility Services	NPCC 8										
17. Michael Jones	National Grid	NPCC 1										
18. Michael Schiavone	National Grid	NPCC 1										
19. Wayne Sipperly	New York Power Authority	NPCC 5										
20. Tina Teng	Independent Electricity System Operator	NPCC 2										
21. Don Weaver	New Brunswick System Operator	NPCC 2										
22. Ben Wu	Orange and Rockland Utilities	NPCC 1										
23. Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC 3										
24. Silvia Parada Mitchell	NextEra Energy, LLC	NPCC 5										
2. Group	Annabelle Lee	NESCOR/NESCO										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3. Group	Jason Marshall	ACES Power Marketing						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Tim Soles	Occidental Power Services, Inc.	ERCOT 3										
4.	Andy Gallo	Austin Energy	ERCOT 1										
5.	Andy Gallo	Austin Energy	ERCOT 3										
6.	Andy Gallo	Austin Energy	ERCOT 4										
7.	Andy Gallo	Austin Energy	ERCOT 5										
8.	Andy Gallo	Austin Energy	ERCOT 6										
8.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8. Annie Terracciano	Northern Lights Inc.	WECC 3										
9. Aleka Scott	PNGC	WECC 4										
10. Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11. Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12. Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13. Margaret Ryan	PNGC	WECC 8										
12. Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13. Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14. Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. M & A Electric Power Cooperative		SERC	1, 3									
4. Northeast Missouri Electric Power Cooperative		SERC	1, 3									
5. N.W. Electric Power Cooperative, Inc.		SERC	1, 3									
6. Sho-Me Power Electric Cooperative		SERC	1, 3									
15. Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X						
Additional Member	Additional Organization	Region	Segment Selection									
1. Oglethorpe Power Corporation		SERC	5									
2. Georgia Transmission Corporation		SERC	1									
16. Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X
Additional Member	Additional Organization	Region	Segment Selection									
1. MAHMOOD SAFI	OPPD	MRO	1, 3, 5, 6									
2. CHUCK LAWERENCE	ATC	MRO	1									
3. TOM WEBB	WPS	MRO	3, 4, 5, 6									
4. JODI JENSON	WAPA	MRO	1, 6									
5. KEN GOLDSMITH	ALTW	MRO	4									
6. DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6									
7. JOE DEPOORTER	MGE	MRO	3, 4, 5, 6									
8. SCOTT NICKELS	RPU	MRO	4									
9. TERRY HARBOUR	MEC	MRO	1, 3, 5, 6									
10. MARIE KNOX	MISO	MRO	2									
11. LEE KITTELSON	OTP	MRO	1, 3, 4, 5									
12. SCOTT BOS	MPW	MRO	6, 1, 3, 5									
13. TONY EDDLEMAN	NPPD	MRO	1, 3, 5									
14. THERESA ALLARD	MPC	MRO	1, 3, 5, 6									
17. Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing												
18. Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				
Additional Member	Additional Organization	Region	Segment Selection									
1. Timothy Beyrle	City of New Smyrna Beach	FRCC	4									
2. James Howard	Lakeland Electric	FRCC	3									

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. Greg Woessner	Kissimmee Utility Authority	FRCC 3										
4. Lynne Mila	City of Clewiston	FRCC 3										
5. Joe Stonecipher	Beaches Energy Services	FRCC 1										
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC 4										
7. Randy Hahn	Ocala Utility Services	FRCC 3										
19. Group	Joseph DePoorter	Madison Gas and Electric Company			X	X	X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Darl Shimko	MGE	MRO 3										
2. Joseph DePoorter	MGE	MRO 4										
3. Steve Schultz	MGE	MRO 5										
4. Jeff Keebler	MGE	MRO 6										
20. Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							
Additional Member	Additional Organization	Region Segment Selection										
1. Mark Jones	Pepco	RFC 1										
21. Group	Rick Terrill	Luminant					X					
Additional Member	Additional Organization	Region Segment Selection										
1. Mike Laney	Luminant Generation Company LLC	ERCOT 5										
2. Tim Soles	Occidental Power Services, Inc.	ERCOT 6										
3. Tim Soles	Occidental Power Services, Inc.	ERCOT 3										
4. Andy Gallo	Austin Energy	ERCOT 1										
5. Andy Gallo	Austin Energy	ERCOT 3										
6. Andy Gallo	Austin Energy	ERCOT 4										
7. Andy Gallo	Austin Energy	ERCOT 5										
8. Andy Gallo	Austin Energy	ERCOT 6										
9. Brenda Hampton	Luminant Energy Company LLC											
22. Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Kevin Smith	BANC	WECC 1										
23. Group	Scott Brame	NCEMC	X				X					
Additional Member	Additional Organization	Region Segment Selection										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Rayburn Country Electric Cooperative			SPP										
2. Empire District Electric			SPP	1									
3. City Utilities of Springfield			SPP	4									
4. Westar Energy			SPP	1, 3, 5, 6									
5. Cleco Power			SPP	1, 3, 5, 6									
25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Pawel Krupa			WECC	1									
2. Dana Wheelock			WECC	3									
3. Hao Li			WECC	4									
27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Denise Lietz		Puget Sound Energy	WECC	1									
2. Erin Apperson		Puget Sound Energy	WECC	3									
28.	Group	Michael Mertz	PNM Resources	X		X							
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Laurie Williams		Public Service Co. of New Mexico	WECC	1									
2. Michael Mertz		Public Service Co. of New Mexico	WECC	3									
29.	Group	Sasa Maljukan	Hydro One	X									
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. David Kiguel		Hydro One	NPCC	1									
30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION C4 – CIP-008-5:

If you disagree with the changes made to CIP-008-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, most of the comments resulted in changes that improved clarity and did not require significant structural revisions. The consideration of comments according to major issues and standard sections follows.

References to EOP-004-2

The comments received for CIP-008-5 and EOP-004-2 both indicated support for handling the reporting of Cyber Security Incidents in CIP-008-5. EOP-004-2 received a much lower ballot approval in its most recent posting primarily for the one hour timeframe required for reporting Cyber Security Incidents. The commenters concern for EOP-004-2 was the lack of a timeframe for identifying a Cyber Security Incident. The required CIP-008-5 processes make clear that reporting to the ES-ISAC occurs within one hour of the analysis to determine whether an event would constitute a Cyber Security Incident. As a result, both drafting teams agreed to move the Cyber Security Incident reporting to the ES-ISAC to CIP-008-5. However, the SDT wishes to stress the reporting threshold is not necessarily one hour from the Cyber Security Incident occurrence. Instead, the threshold accounts for the analysis that must be performed in identifying the Cyber Security Incident. The incident could even have occurred much earlier without any observable behavior. Also, entities can still have a single reporting process to comply with the new versions of EOP-004 and CIP-008.

Applicability Section

Several commented that all instances of Medium Impact BES Cyber Systems should be changed to "Medium Impact BES Cyber Systems with External Routable Connectivity". In response, we note that CIP-008-5 addresses incident response and reporting and the lack of external routable connectivity would not address this issue. It is possible for a Cyber Security Incident to occur on such cyber systems through insider attacks or other means of penetrating the physical or electronic boundaries. This does not create an inconsistency among the standards or implied requirement for monitoring because an entity can have a monitoring program to detect incidents that does not fully meet the requirements of CIP-006-5 and CIP-007-5.

There were several comments that stated CIP-008-5 should apply to Electronic Access Control and Monitoring Systems and Physical Access Control Systems. In response, applicability to these systems is unnecessary because the incident is associated to the BES Cyber Systems. Incidents occurring on perimeter systems would target the system and not the perimeter.

Other General Comments

One commenter requested clarification why the word "dated" has been added to the measures in these requirements. In response, dated documentation is used to clarify that such evidence is necessary to demonstrate time-based requirements.

There was a comment that suggested the word "annual" should be a defined in the NERC Glossary. In response, the SDT has chosen not to define annual because the periodicity for requirements in CIP may be different than requirements in other standards, and the definition of annual may have many interpretations.

Guidelines

One commenter suggested that references to DHS and NIST should not reside in the standard because NERC does not track those documents to ensure consistency. In response, the external references are dated to a specific version to address the case where future revisions do not remain consistent with the standard.

There was a comment that the definition of Reportable Cyber Security Incident is too vague and could result in the interpretation that activation of redundant systems causes the reporting not to be considered. In response, the SDT has clarified in the guideline that this is not the case. The SDT has added a clarification that the absence of lessons learned must still be documented.

One commenter proposed revisions requirements to "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has considered this approach and has added to certain requirements "… identify, assess, and correct deficiencies…", which is explained in detail in the global summary portion of this document, above.

Background

One commenter stated that the background section for CIP-008-5 is contradictory in reference to measures by stating a numbered list is all-inclusive but measures serve only as examples. In response, the SDT notes that the background section states "A numbered list in the measure means the evidence example". This means the example evidence must include all of the items, but there may be other examples of evidence to meet the requirement. Both statements are true.

Requirement Part 1.1 and 1.2
Based on a comment, the SDT changed "Processes" to "One or more processes" for clarity.

Several commenters propose including additional specificity in the process for determining if an incident is reportable. The SDT has extensively discussed this issue, and the problem with additional specificity in Cyber Security Incidents is difficulty in exhaustively enumerating situations to report. Also, the reporting of incidents associated with damage alone can result in under-reporting, which does not meet the objective of this Requirement.

Requirement Part 1.4
Several commenters stated that 1.1 (responding) and 1.4 (handling) are essentially the same and proposed to delete 1.4**.** The SDT notes that while 1.1 addresses the initial identification and response to incidents, 1.4 addresses the actions to perform for resolving individual incidents. These are distinct activities.

One commenter suggested the that the applicability include low impact BES Cyber Systems because CIP-003-5 requires implementation of a policy addressing incident response, but CIP-003-5 intentionally centralizes all the requirements for low impact BES Cyber Systems which does not include specific elements of the plan.

There was a comment that suggested removing the parenthetical phrase for incident handling because recovery and post-incident analysis are covered elsewhere. In response, the SDT agrees that post-incident analysis is already handled in Requirement R3 of CIP-008-5 and clarifies the recover activities here pertain only to the incident. Recovery includes the confirmation that the incident has been resolved.

One commenter suggested adding wording to clarify physical security incidents need to be considered. In response, the SDT notes that the definition of Cyber Security Incidents includes physical intrusions.

Requirement Part 1.5

There was a comment that stated it is unclear if the list of internal and external contacts refer to those in EOP-004-2 or if there is a need to have a minimum list of contacts. In response, the internal or external contacts that an entity would need to include to ensure proper reporting for EOP-004-2 should be part of this list. Additional contacts are appropriate as necessary components of an incident response plan, but who resides in this list is left up to the entity.

A commenter suggested that the use of external organizations could result in double jeopardy with EOP-004-2. However, EOP-004-2 requires specific organizations whereas CIP-008-5 leaves the inclusion of additional external organizations up to the entity as a necessary part of the incident response plan. Double jeopardy does not exist here because there is not a requirement in CIP-008-5 to report.

One commenter proposed to replace the phrase "should receive communication" with "must be sent communication". In response, the SDT notes that this part of the incident response plan does not necessarily constitute required communication, but communication must be covered as a component of the plan.

Requirement R2

One commenter proposed adding an exception for the timeframes based on CIP Exceptional Circumstances. In response, the SDT notes that CIP Exceptional Circumstances have not applied to annual periodic performances requirements because of the flexibility in the timeframe of when an entity can perform this requirement.

Requirement Part 2.1

In response to a comment that 2.1 should expand to include all Cyber Security Incidents, the SDT continues to limit these requirements to Reportable Cyber Security Incidents because of the lessons learned and plan updates associated with each Reportable Cyber Security Incident. It is possible for Cyber Security Incidents to occur much more frequently.

In response to a comment, the SDT has removed the word "BES" before "BES Incident Response Plan" for consistency.

One commenter suggested revising the language of "at least once each calendar year, not to exceed 15 calendar months between executions" to "once each calendar year or a period not to exceed 15 calendar months between executions". The SDT notes that the language that exists is sufficient as currently written.

One commenter suggested using the term “exercise” instead of “test” because an actual exercise would suffice. In response, we had several comments to the contrary in the previous posting. The SDT uses test here because the word “exercise” is commonly used in reference to a planned execution.

One commenter suggested removing the lessons learned report from the measure because it is not part of the requirement. In response, we note that the measure only serves as an example, and a lessons-learned report would be an example measure for 2.1.

One commenter suggested that a full operational exercise should be required in the absence of an actual incident. In response, we suggest that the quality of an exercise does not depend on the type. It is possible to have a higher quality tabletop exercise than a full operational exercise.

One commenter suggested placing an “or” between all exercise examples, but this is not necessary because the “or” in the second bullet qualifies the entire list.

One commenter suggested expanding the scope of actual incidents that qualify as an exercise to include any Cyber Security Incident, but this would not exercise a key component of identifying and communicating a Reportable Cyber Security Incident.

One commenter proposed to remove any timeframes associated with the test. The SDT disagrees because absence of time requirements makes the expected performance of the standard less clear and does not respond to directives from the FERC Order 706.

Two commenters suggested adding a specific reference to R1 to clarify the linkage, but the context of the Requirement in its use of Cyber Security Incident response plan is clear enough to avoid needing a direct linkage.

In response to several commenters, the word “plan(s)” was modified to “each plan” for added clarity.

In response to one commenter, the SDT qualified that the phrase “when responding to” is in regards to the Reportable BES Cyber Security Incident.

Based on comments, the SDT clarified exercises were for Reportable Cyber Security Incidents.

Based on comments, the SDT has removed the word “BES” from this requirement part.

Requirement Part 2.2
One commenter stated that this requirement part should be deleted because the main requirement part already addresses implementation and documented deviations are redundant with lessons learned. In response, the SDT points out that implementation of the plan does not necessarily mean that it be used during an incident or exercise. Some entities may interpret that a plan is implemented regardless of whether or not it is actually used. This additional requirement adds clarity in the expected outcome. The same is also true of lessons learned not having the full meaning of documenting deviations from the plan. However, we agree that the documentation should not necessarily occur concurrent with the incident and have modified this requirement part accordingly.

One commenter suggested requiring documentation for the lack of deviations from the plan. In response, we do not agree this language is necessary. The absence of deviations may be a common occurrence and the requirement to have such documentation is highly administrative. We believe this is different than the case of not having any lessons learned which should be a much less common occurrence.

One commenter suggested requiring plan updates for new vulnerabilities and threats. The SDT agrees this would be appropriate if the plan were not sufficient to address new vulnerabilities and threats, but measurable criteria for what constitutes a new vulnerability or threat does not exist and could likely not be determined by anyone other than the Responsible Entity.

In response to a comment, the SDT replaced the phrase “incident response plan” with “Cyber Security Incident response plan” for consistency.

In response to several commenters, the word “plan” was changed to “plan(s)” for consistency.

Requirement Part 2.3
One commenter proposed that 2.3 should be moved to the compliance evidence section of the standard. In response, the evidence retention section cannot add a new requirement, and without 2.3 there is no requirement to retain evidence of the incident.

Several commenters suggested the language for requirement part 2.3 include a retention period, but this requirement was modified in response to comments that the retention period be covered in the compliance evidence section of the standard. As a result, part 2.3 includes the requirement to retain the records, which may not have been necessary to retain anywhere else in the standard, and the compliance evidence section defines the retention period.

There were several commenters who stated that this requirement part could have double jeopardy with EOP-004-2, but lack of documentation for reporting purposes would not be a violation of CIP-008-5. Also, EOP-004-2 evidence retention does not necessarily cover evidence related to a Cyber Security Incident.

One commenter suggested storing the evidence in encrypted form. In response, CIP-011-1 addresses the storage of BES Cyber System Information. Specific implementation of this requirement is appropriately left to the entity.

The SDT has removed the word "relevant" responding to comments that it adds unneeded subjectivity.

One commenter questioned whether three calendar years is sufficient for retaining incident evidence for law enforcement, state, and federal requirements, but the evidence retention is a minimum for the purpose of the Standard. If additional requirements outside of the NERC Reliability Standards indicate a longer retention period for a particular entity, then the entity would choose the longer period. There is no conflict.

Requirement R3

One commenter proposed that the main requirement should more closely align with CIP-009-5 R3 and focus on maintaining, and not implementing, the plan. The SDT agrees.

One commenter suggested the word "full" be deleted from "full operational exercise" because it is unclear what it implies. The SDT agrees.

Requirement Part 3.1

Several entities have commented this requirement part is duplicative with testing in R2 and monitoring for plan changes in R3. The SDT agrees and has deleted this requirement part.

In response to a comment that proposed to consider additional changes that trigger a review of the incident response plan, the lessons learned requirements suffice for updating the plan in response to incidents. Changes to the security

configuration already trigger updates in requirement part 3.4. In many cases the incident response plan is written at a high enough level to preclude necessitating changes in response to new threats and vulnerabilities.

Requirement Part 3.2

There were several comments that the various dates for updating the plan significantly increase the compliance tracking burden and that a plan has not truly updated until the entity distributes those updates to the required individuals. The SDT agrees and has collapsed previously posted requirement parts 3.2, 3.3 and 3.5 into a single requirement part 3.1. The additional requirement part 3.4 for monitoring plan changes and 3.5 has collapsed into a single requirement part 3.2. Some commenters suggested that both requirements should allow a consistent 90 days, but the updating of the plan in response to changes does not require the same level of updates as those required from lessons learned. Therefore the different timeframes in these requirement parts are appropriate.

One commenter suggested tying this requirement explicitly with both 2.1 and 2.2. In response, the cross-referencing of requirements could cause more confusion than clarity. The SDT feels this explicit tie is best accomplished in the guidance.

One comment proposed to remove any timeframes associated with plan updates. The SDT disagrees because absence of time requirements makes the expected performance of the standard less clear and does not respond to directives from the FERC Order 706.

There was a comment that suggested that 30 days may not be sufficient time to make complex changes from lessons learned. In response, the SDT believes the updated requirement allowing 90 days for the complete time is sufficient for even complex changes.

One commenter suggested changing this requirement part to include language for consistency with the ERO Event Analysis Process. The ERO Events Analysis Process is not a NERC Reliability Standard, and the SDT is not mandating referenced actions that are not developed through the NERC process or an equivalent ANSI Certified process. The SDT also notes that the proposed requirement language leaves flexible “how” to perform the requirement. Entities may choose to follow the procedures outlined in the ERO Events Analysis Process to comply with the requirement, but are not required to. The SDT also understands that the NERC CIPC is planning to form a working group to develop guidelines for analyzing cybersecurity events using a parallel process to the recently approved ERO Events Analysis Process. Specifying

that the ERO Events Analysis Process be used in response to CIP-008 Reportable Cybersecurity Incidents is premature and will remove any perceived or required flexibility in developing cybersecurity-specific procedures under that group.

Several commenters suggested clarifying the expectation when there are no lessons learned. In response, we have made this explicit in both the requirement and measure.

In response to one comment, the SDT has added examples of evidence for lessons learned.

In responses to multiple comments, the SDT changed the phrase "within 90 days" to "not to exceed 90 calendar days" for clarity.

Requirement Part 3.3
In response to a comment, it is not necessary to modify this requirement to state "update as needed" because the requirement part ties to "any lessons learned" which carries the same effect.

Requirement Part 3.4
One commenter suggested reverting to previously approved language for updates and notes that evidence to meet this requirement would include lists of technology changes. In response, the SDT notes that such evidence would be required in the previously approved version if specific technology was referenced in the plan. The changes identified here are to provide additional clarity in the types of changes that should trigger an update.

Several commenters proposed that the term "technology changes" needs to be defined. The SDT notes this only includes technology changes that would impact the ability to execute the plan. Because this term is so contextual to the plan, it would cause more problems to define it. Entities should review their plans to see whether or not they have technology as a key element of the plan. The guidance specifies that "technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems."

Requirement Part 3.5
Several commenters suggested changing the word "distribute" to "notify" for announcing changes to the incident response plan due to the uncertainty of what constitutes distribution and the possible issues with information sensitivity. The SDT agrees.

One commenter suggested the evidence examples of distributing the plan could result in a violation of confidentiality, but, while each example can specify additional mechanisms to preserve confidentiality, this was not the intention of the measure. In some cases, incident response plans may not contain confidential information.

VSLs

One commenter recommended that the documentation of the absence of any lessons learned should be included in the VSLs. In response, the absence of lessons learned has been included in the VSL.

One commenter recommended that the VSL should not include failure to follow the plan during an incident and the VSL associated with lack of documentation of deviations suffices. The SDT agrees and does not need to modify the VSLs.

QUESTION C8 – CIP-009-5:

If you disagree with the changes made in CIP-009-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the primary concerns regarding CIP-009-5 expressed in comments were (1) backup media verification procedures in requirement parts 1.4 and 2.2, (2) data preservation procedures in 1.5 and (3) timeframe requirements in Requirement R3 on the lessons learned and plan update activities. The consideration of comments according to major issues and standard sections follows.

Applicability

One commenter suggested that the applicability for all requirements in this standard should limit to Medium Impact BES Cyber Systems at Control Centers to appropriately focus on the higher risk cyber systems and avoid conflict with PRC Standards. In response, the loss of Medium Impact BES Cyber Systems has impact to the BES and the recovery operation for these cyber systems should be addressed in this standard.

The applicability is limited to high impact and medium impact at control centers, along with their associated EACs and PACs, which means testing for substations and generating plants that are not high impact is not included. A commenter asked for confirmation on whether this was the SDT's intent. Yes, it was.

One comment suggested that applicability to associated Cyber Assets should be removed because the FERC has not directed to do so. In response, these continue to apply from all prior versions to the associated Cyber Assets.

Other General Comments

One commenter proposed modifying the main requirement part and corresponding VSLs for R2 and R3 to allow for a flaw remediation process. In response, we have modified the main requirement part for R2 to eliminate the zero tolerance obligations because of the possible magnitude of plans and backup media which require testing. However, we do not incorporate the same changes for R3 because the requirements here do not have the same zero-tolerance concerns and they specify the procedures that must be in place to ensure better response plan flaw remediation.

Guidelines

Several commented that application guidelines should be included for CIP-009-5, and we have added these.

Background

One commenter suggested that the background section is contradictory by saying that measures are not all-inclusive but numbered list provide an all-inclusive example. In response, the background section states, "A numbered list in the measure means the evidence example includes all of the items in the list." This refers to the single example and is different than an all-inclusive list of evidence examples. Accordingly, if an entity did not provide all parts of the numbered list of evidence, then they would not fully meet the requirement. However, they could still provide alternate forms of evidence outside of the example.

Measures

There was a comment that the measures should be clarified with the following language: "Evidence may include, but is not limited to, a dated, revised Cyber Security Incident Response Plan(s) that (1) includes or references, as appropriate, dated documentation of lessons learned, if any, associated with tests of or actual responses using the Cyber Security Incident Response Plan(s), within 90 days after completion of such test or actual incident response; and (2) reflects changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change." The SDT notes that the language in the requirement is clear and that the measures provide adequate examples of evidence. Each requirement part addresses different levels of that may be expected.

Requirement R1

One comment proposed to add a requirement for restoring the BES Cyber System to a state where it is ready to assume its normal operating role in all respects. They also commented that the requirement should state the level of granularity required for a plan. In response, it would be problematic to standardize and audit a normal operating role. The SDT is uncertain as to the meaning of this term. The purpose of this standard is "to recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES." It is inappropriate to specify the level of detail required for a recovery plan.

Several commenters suggested that the standard is not clear whether the recovery plans are for recovery of the asset, system, or function. In response, the stated purpose for the standard is "to recover reliability functions performed by

BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES."

One commenter asked the following: "is a Business Continuity Plan, where operations are transferred from the main control center and continued at a back-up control centre, considered a recovery plan?" In response, this could constitute a recovery plan according to Requirement R1 with the additional components listed in the requirement parts. However, restoration of the reliability function meets the purpose of this standard.

Requirement Part 1.1
One commenter suggested removing "specific" activations from the measure, and we have done so.

One commenter suggested the minimum conditions for activating a response should be specified. Otherwise entities can choose an inappropriately high bar. In response, any minimum enumeration of recovery conditions would equate to defining system failure and doing so for a highly variant population of systems across the BES is not feasible.

Requirement Part 1.3
Several commenters suggested changing the phrase "BES Cyber System" to "applicable Cyber Assets". However, "restoring BES Cyber System" functionality describes the objective of the requirement part and not the applicability.

One commenter suggested addressing FERC Order 706 paragraph 748 by appending the suggested text from the Order to this Requirement Part addressing backup media. We agree this is clearer and have incorporated their suggestion in requirement part 1.4 because of the difference in applicability from 1.3.

One commenter suggested modifying this requirement part measure to provide alternate forms of evidence and avoid the interpretation that evidence must be shown for each occurrence in a high-frequency operational requirement. In response, the SDT has modified the measure according to these suggestions.

Several commenters suggested removing the qualifier word "successfully" from the measure and the SDT has done so.

One commenter suggested including documented configuration settings, documented build/restoration procedures, and retention of installation media for example evidence. The SDT has added these to the technical guidelines section of the standard.

Several commenters suggested replacing the word “recover” with “restore” to describe the purpose of the backup media. In response, we retain the use of “recover” to avoid confusion. Both words mean to return something to a normal or former condition, and the SDT finds these words can be used interchangeably while still communicating the same concept.

One commenter noted the measure is missing an “and”, and the SDT has corrected this oversight.

Requirement Part 1.4

Several commenters expressed confusion around the term “initially” in the requirement, and the SDT has removed this term by tying the verification processes to the backup and storage processes in 1.3. The resulting language should provide more clarity and eliminates the term “initially”.

One commenter suggested addressing FERC Order 706 paragraphs 732-734 in this requirement section or moving this to guidance. In response, the resulting directive in paragraph 739 is addressed by the proposed text to address 748. Another commenter also supported the proposed language in the FERC Order. In response, verifying the operability of backup media is addressed by verifying successful completion and addressing failures of the backup process. Short of performing a full restoration, monitoring the backup process provides the appropriate assurance in the integrity of the backup for constantly changing systems. We have also added further guidance for this requirement part.

One commenter stated that FERC did not express concern over Physical Access Control Systems and Electronic Access Control and Monitoring Systems and applicability for these should be removed. In response, we retain the applicability from previous versions of the standard to which the FERC Order was addressed.

Several commenters requested further clarification about the meaning of verification of backup media. In response, the verification of backup media is dependent upon the tool performing the backup. This could include checking for read/write errors or performing a checksum during the backup operation. The SDT has clarified this requirement to read verification of successful completion.

One commenter suggested this requirement part be modified to address 3rd parties performing the backup or providing a backup, and the requirement has been modified to address these concerns.

Several commented on the 90 day retention period for the logs specified in this requirement part measure. In response, the reason for having 90 day retention for BES Cyber System logs is the potentially large volume, but there is no such concern for the evidence example for this requirement part.

One commenter does not believe this requirement part belongs as written here, and we note the overall modifications to this requirement part better fits the overall objective of Requirement R1.

One commenter stated that the term "backup media" is antiquated and should be replaced with redundancy terminology. In response, we disagree the term is antiquated, but if redundancy is being used for recovery, then processes should exist to regularly verify the redundancy and address failures.

One commenter asked the following questions: If a single monthly backup succeeds, is that good enough? What is verified initially? Is this a daily check for backups or is weekly verification sufficient? If a log is printed or a snapshot taken monthly for evidence sufficient if alerting to x-number of failures is part of the process or is evidence collection required upon completion of the backup? In response to these questions, the currently proposed requirement does not specify a timing that is sufficient for verification due to the widely varying backup methodologies that exist for the applicable systems. A printed log or periodic automated sampling of the backup process would be considered sufficient evidence for this requirement.

One commenter stated that the only way to verify backup completion is to restore from backup. In response, completion of the backup process or routine is different than successful restoration, and we contend the former can be verified outside of a full restoration.

Requirement Part 1.5

Several commenters suggested replacing the word "event" with the phrase "Cyber Security Incident" to better scope when it is necessary to preserve data. In response, we have made this change and modified the requirement to better qualify the purpose of preservation. The requirement should read clearly that data must be retained until a Cyber Security Incident may be ruled out as the cause of the recovery operation.

One commenter suggested removing this requirement part because it addresses forensics and not recovery. In response, this requirement part ensures data collection procedures are included in the recovery plan to allow the performance of after-the-fact analysis. This is appropriate to require as part of the recovery operation.

One commenter suggested that with changes to the definition of CIP Exceptional Circumstances to include “an imminent or existing hardware, software, or equipment failure”, this requirement would never invoke. Their proposed language incorporates the concept of CIP Exceptional Circumstances, and we have included much of the proposed wording in the revised requirement part. The commenter also proposed to limit this requirement part to Medium Impact BES Cyber Systems at Control Centers, but neither the threat nor the operational circumstances for field assets preclude applicability for this requirement part. This requirement allows sufficient flexibility to apply in widely varying environments. The modifications here also address other comments about clarifying the procedures should not impact reliability.

One comment suggested that the PRC Standards already cover this for relay misoperation, but these standards do not address specifically the failure of a Cyber Asset nor do they address the preservation of data from Cyber Assets.

One commenter stated that this requirement implies an obligation to mirror data in the measure, should be left up to the entity to determine whether or not to delay recover for the purpose of preserving data, and an entity cannot determine the preservation of data given the many ways in which a system can fail. In response, we first note that a measure is only an example and does not imply an obligation to mirror data. Second, the SDT has taken an exception to add an explanatory note in the requirement cautioning against impeding recovery for data preservation. Finally, this requirement part does not envision an entity determining every way in which a Cyber System can fail. This only obligates the entity to include data preservation procedures in the recovery plan. There was a second comment on the guidance language in the measure, and the SDT agrees the language does not readily associate itself to the requirement and has been removed.

One comment suggested that this requirement part should be part of root-cause analysis and not impede system restoration. The SDT agrees and notes the requirement part does not address forensics but only the preservation of data to support root-cause analysis and forensics after-the-fact.

Requirement Part 2.1

One commenter suggested for this requirement part and requirement part 2.3 that the word “exercise” should be used in place of “test” since an actual recovery operation can be used for compliance. However, several commenters suggested the converse in the last posting, and we are not compelled the difference in terminology changes the meaning of the requirement.

One commenter suggested revising the language of “at least once each calendar year, not to exceed 15 calendar months between executions” to “once each calendar year or a period not to exceed 15 calendar months between executions”. The SDT notes that the language that exists is sufficient as currently written.

Several commenters requested clarity about whether or not each recovery plan must be tested annually. In response, we have modified this requirement to explicitly state that each recovery plan must be tested as was the intent. We do not specify a representative sampling of plans be tested as some suggest because the proposals do not include enough information to objectively determine what constitutes a representative sample. However, we do note that it is possible to singularly test multiple cyber systems if they are similar in nature.

One commenter suggested that all backup media should not be required for testing but only the one needed for recovery, and we have modified the requirement to include this condition.

One commenter suggested that “or” should be added to the first bullet point or it is otherwise required. In response, the or in the second bullet point modifies the entire list.

Requirement Part 2.2

One commenter asked if this requirement part includes a media test and whether this can be performed on a sample system. In response, this can include a media test on a sample system provided some verification to ensure the information is current and useable occurs. We have modified the measure for this requirement part to make this clearer.

One commenter suggested allowing an actual recovery operation to substitute for the testing of backup media, and we have made this change.

One commenter proposed to replace the requirement with “Unless covered by EOP-008, test a representative sample of information used in the recovery of BES Cyber Systems that is stored on backup media at least once each calendar

year, or a period not to exceed 15 calendar months between tests, to verify the backup media is operational and the information is useable." The concern surrounds possible double jeopardy with EOP-008 and clarity around "compatibility with current system configurations." In response for EOP-008-1 R7, failure to meet this requirement does not indicate a failure for EOP-008-1 and vise-versa. This requirement concerns the testing of backup media, which may not be used for recovery with EOP-008-1. For the proposed language, we have incorporated the "representative sample of information" in testing to clarify the obligation, but we retain the purpose of verifying compatibility with current system configurations. Only ensuring the usability of backup media does not capture the intent that the backup media is currently usable for performing the BES Cyber System function.

One commenter suggested striking the phrase "to ensure that the information is useable and is compatible with current system configurations" and believes it should be left up to the Responsible Entity to determine, whether another commenter requested further clarification about this phrase. In response, the testing of backup media alone is not specific enough to ensure clarity of the requirement. The phrase in question is necessary for entities to know what they should be testing. We have added additional technical guidelines for this requirement.

One commenter suggested that this requirement should state that a tabletop exercise should not be permitted. In response, the testing of backup media may be performed as a separate process or as a part of the recovery plan exercise. There is not a need to specify which type of exercises aligns with this process.

One commenter suggested that the term "backup media" is antiquated and should be replaced with redundancy terminology. In response, we disagree the term is antiquated, but if redundancy is being used for recovery, then processes should exist to test the redundant systems in accordance with this requirement part.

Several commenters proposed the phrase "validate the integrity of the stored information" as a substitute for current language regarding the testing of backup media. In response, validating the integrity of the information can be interpreted widely from a bit comparison to a sampling. We believe our proposed revisions provide enough specificity and flexibility to be widely applied.

One comment proposed to focus the requirement on backup media rather than information used for recovery. In response, we use the term information here because of the various ways entities implement backup policies, which may include replication technologies. Backup media was not well understood by the team and many participants to include replication.

Requirement Part 2.3

Several comment that the measure references performance of this requirement prior to the Effective Date, and that this requirement part should be included in the Implementation Plan. In response, we have removed this language from the measure and added this requirement part to the Implementation Plan.

One commenter suggested testing a representative of a plan with a rationale that High Impact BES Cyber Systems already have a requirement to test backup media annually. In response, we do not see a significant change in the proposed wording. The requirement to test backup media does not require a full operational restoration.

One commenter requested clarity that all recovery plans do not have to be tested at the same time. In response, the requirement only specifies the obligation to test recovery plans at a periodicity. It would not violate the requirement to test individual plans at different periods while still meeting the periodicity obligation.

One commenter requested a basis for the 36 months period. In response, we incorporated this timeframe from the FERC Order 706 directive.

One commenter suggested testing a "representative" rather than "each" BES Cyber System. In response, if an entity can test a representative BES Cyber System for multiple systems, then they have complied with the requirement to test "each" BES Cyber System.

One commenter noted that an entity may have several failure scenarios and it is unclear if all of these must be tested. In response, we have added guidance in the technical guidelines section of the Standard to clarify that not all failures scenarios must be tested, but that the test should ensure the plan is up to date and test at least one process to restore the applicable cyber systems.

One commenter suggested that EOP-008 R6 should suffice for this requirement part. In response, EOP-008-1 R6 requires independent backup functionality, but this does not imply an obligation to perform a functional test. The compliance processes to comply with EOP-008-1 should certainly ease compliance with this requirement part.

Several respondents asked whether a full operational exercise means a bare-metal recovery and comments that doing so would be cost prohibitive, while another commenter suggested also requested further clarification around

the term "operational exercise". In response, the SDT has provided well established definitions of operational exercises that would comply with the requirement, which do not imply a full recovery demonstration.

Requirement R3
Requirement R3 has been modified to correspond with similar commenter suggestions in CIP-008-5 R3.

One commenter suggested that Requirement R3 does not include defined roles and responsibilities. As we understand the comment, the roles and responsibilities refer to those required parts of the response plan specified in Requirement R1.

Requirement Part 3.1
Several commenters noted that the various dates for updating the plan significantly increase the compliance tracking burden and that a plan has not truly updated until the entity distributes those updates to the required individuals. The SDT agrees and has collapsed previously posted requirement parts 3.1, 3.2 and 3.4 into a single requirement part 3.1. The additional requirement part 3.3 for monitoring plan changes and 3.4 has collapsed into a single requirement part 3.2. Some comment that both requirements should allow a consistent 90 days, but the updating of the plan in response to changes does not require the same level of updates as those required from lessons learned. Therefore the different timeframes in these requirement parts are appropriate.

A few commenters suggested updating plans based on lessons learned is not necessary because these changes would be captured in technology and personnel changes. In response, the updates here capture improvements to the plan as determined through a lessons learned exercise.

One commenter suggested that the evidence collected in requirement part 1.5 should be part of the review process. They also commented that other related plans (i.e. configuration management plans) be updated as necessary as part of the review process. In response, the evidence collected in requirement part 1.5 may not be reviewed by a third party and we do not feel it is necessary to specifically call out this activity in the requirement part. Also, we cannot add an obligation to update other plans as necessary in a way that would be objectively measurable.

One commenter suggested that 30 days may not be sufficient time to make complex changes from lessons learned. In response, the SDT believes the updated requirement allowing 90 days for the complete time is sufficient for even complex changes.

Several commenters have suggested clarifying the expectation when there are no lessons learned. In response, we have made this explicit in both the requirement and measure.

Several commenters stated that requiring entities to perform lessons learned is counterproductive because it encourages entities not to admit there is a deficiency in the first place. In response, the inclusion of a lessons learned process provides a standard practice across the industry, which would otherwise be inconsistency applied at best. Furthermore, it addresses a FERC Order 706 directive to include lessons learned processes as part of a recovery plan test.

Requirement Part 3.3

One commenter suggested modifying the references to other standard requirement parts, removing references to individuals and modifying the communication of plan updates to be more specific. In response, the SDT has made several modifications to Requirement R3 to align with modifications to CIP-008-5 that address these concerns.

Several commenters proposed removing this requirement and addressing plan updates in guidance, but placing the plan items that would trigger a change in guidance would add a high degree of subjectivity to the requirement. Specifying what changes should constitute an update ensures objectivity in demonstrating compliance with this requirement.

One commenter proposed removing this requirement or clarifying the tie back to Requirement R1.2. In response, this requirement is necessary to ensure the recovery plan remains current and carries forward from the requirement to update on any changes. They also expressed concern that this requirement part could be interpreted that a change to any plan must be communicated to all individuals specified in requirement part 1.2. In response, we have removed the explicit tie to requirement part 1.2 to avoid such an interpretation.

One commenter suggested that the plan maintenance would create an undue compliance burden. In response, the SDT notes this requirement carries forward from previous versions and ensures the recovery plans remain up to date through organizational changes.

Requirement Part 3.4

Several commenters suggested changing the word “distribute” to “notify” for announcing changes to the incident response plan due to the uncertainty of what constitutes distribution and the possible issues with information sensitivity. The SDT agrees.

One commenter suggested the distribution of plan updates should include some irrefutable evidence on the part of the receiver. In response, we do not believe the added qualification would have the desired benefit. Individuals can choose to ignore the content regardless of the evidence of receipt.

One commenter stated that the example evidence for communicating plan updates is a poor choice because of the confidentiality of such information. In response, the examples do not necessitate the sharing of sensitive information but only that the individuals be notified. We have included additional guidelines to consider the sensitivity of the information when sending the required notifications.

VRF

One commenter proposed that the VRF should be Lower for consistency with other requirements. In response, we retain the previously FERC approved VRF of Medium for this requirement because failure to have restoration procedures directly affects the BES reliability function of High and Medium impact BES Cyber Systems.

VSLs

The VSLs have been updated corresponding to changes made to requirements in CIP-009-5.

One commenter suggested that “within 30 days” should be changed to “greater than 30 days”. The SDT agrees and has made this change.

Several commenters suggested that the moderate VSL for Requirement R1 should address “one” and not “all” missing elements of the plan. The SDT agrees and has made this change.

One commenter suggested that the VSL for Requirement R3 should capture not documenting the absence of lessons learned. The SDT agrees and has made this change.

One commenter proposed to replace the Requirement R3 VSLs with graduation from 90-210 days beyond the required obligation. The SDT agrees and has made this change.

One commenter noted the graduation of VSLs for requirement part 2.2 incorrectly lists a period of within 19 calendar months for the Severe category, and the SDT has modified this to be 18 calendar months.

QUESTION C12 – CIP-010-1:

If you disagree with the changes made in CIP-010-1 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the primary concerns regarding CIP-010-1 expressed in comments were (1) references to CIP-005, CIP-006, and CIP-007 within CIP-010, (2) scope of baseline configuration items in R1.1, (3) applicability including associated assets/systems and also including "external routable connectivity" language, (4) requirement language above and beyond FERC Order 706, and (5) other requirement and measure language modifications. The sections below are a summary of the comments received and include SDT responses for CIP-010-1.

CIP-010-1 General Comments

Many commenters requested an explanation for why CIP-010 depends on CIP-005, CIP-006, and CIP-007. Based on previous requirements in older versions of CIP-003, CIP-005, and CIP-007 (CIP-006 has since been removed from requirement language), the SDT combined the various requirements related to configuration change management and vulnerability assessments to create CIP-010. Both configuration change management and vulnerability assessment require validation that controls from CIP-005 and CIP-007 are not affected. Therefore, CIP-010 references CIP-005 and CIP-007. The SDT does not believe this cross-referencing creates a "double jeopardy" situation. Whether the requirement existed in CIP-005 or CIP-007, if an issue is discovered, then the issue would be a violation of where the requirement was enforced (CIP-005 or CIP-007) rather than in the requirement which enforced the search for issues (CIP-010). New "identify, assess, and correct deficiencies" requirement language will also aid in compliance concerns.

Several commenters mentioned that they desired a return to the approved language in CIP-003-4 Requirement R6 and CIP-007-1 Requirement R1 with targeted and efficient changes to address the FERC order. Another commenter further recommended a return to the draft 1 language. The SDT disagrees with their determination and believes that the current CIP-010-1 language is proper and in order. Based on this commenting period, the SDT has revised language for clarity and consistency. Language was also modified in an effort to address industry comments.

Numerous commenters recommended that all references to Medium Impact BES Cyber Systems in CIP-010 applicability include: "with External Routable Connectivity." The SDT does not agree with the addition of External Routable Connectivity to CIP-010 applicability. Whether a cyber asset has some type of connectivity or not, it can still be pervious

to vulnerabilities (i.e., Stutnex). The SDT's determination is in accordance with FERC Order 761, Paragraph 86. Therefore, external routable connectivity exclusion language was not included in the applicability for CIP-010.

One commenter proposed removing from the measures: "… and the output of the tools used to perform the assessment," since this is thought to be a part of CIP-010-1 Requirement R3.4. The SDT does not agree with this modification since CIP-010-1 Requirement R3.4 asks for the results of the assessments, while CIP-010-1 Requirements R3.1 through R3.3 are referring to the output of any tools used to perform the assessment. In consideration of this comment and other industry comments, the SDT included "any" to the requirement in the case that no tools were used to perform the assessment.

Several commenters suggested the removal of: "… but not limited to …" in CIP-010 measures. The SDT has modified measure language in consideration of their comment. The SDT also emphasizes that the: "… but not limited to …" is supposed to benefit the responsible entity and not create an item for auditors to use against them.

Multiple commenters suggested that specific controls from CIP-005 and CIP-007 be identified in CIP-010-1 Requirements R1.3, R1.4.1, and R3.1 so there would be no need for interpretations. These comments were taken into consideration, and the related requirement sub-parts were modified accordingly. The references to CIP-005 and CIP-007 were removed from some requirement sub-parts. Also, per consideration of these comments, CIP-006 was removed from requirement language where the language was present.

One commenter believed that some requirements in CIP-010 expand the scope and documentation burden beyond earlier CIP standards versions due to CIP-005 and CIP-007 references. In consideration of these comments, the SDT has modified CIP-010-1 Requirements R1.3 and R3.1 accordingly. References to CIP-005 and CIP-007 have been removed from the sub-part requirement language. It should be noted that the SDT disagreed to removing these references in Requirement R1.4.1. The SDT also added the reference to Requirement R1.5.1 for consistency across Requirement R1.

One commenter recommended adding a reference to the associated requirement part in which each CIP-010-1 VSL is related. The VSLs are written at the higher-level requirement, but do include elements that refer to the various requirement parts. Therefore, the SDT does not believe that the associated requirement part needs to be included in the VSL. One commenter continued to suggest that the VSL language should more closely mirror the requirement language. The SDT has taken into consideration this comment and modified the VSL language accordingly.

One commenter mentioned that having a documented baseline and monitoring it closely makes the vulnerability assessment prior to deployment have no benefit. The SDT does not agree with this assessment, as a vulnerability assessment is more than just monitoring for changes to the baseline. Please see the guidelines section of the standard for CIP-010-1 Requirement R3. Also, other commenters mentioned that establishing a production-like environment that could produce an active vulnerability assessment would be difficult and expensive. The SDT added the language: "… production environment where the test is performed in a manner that minimizes adverse effects …" for instances when a test environment is not available.

One commenter recommended an expanded glossary of the many terms used in CIP-010. The SDT has taken this comment into consideration and has expanded upon the guidelines to include more guidance around terms related to the baseline configuration and cyber security controls.

One commenter recommended further items to be incorporated into the baseline configuration; including communication protocols, non-standard BIOS configurations, and other items. The SDT believes that the requirement language is sufficient as written, as adding additional items into the baseline configuration at this time period would be difficult to support consensus.

One commenter recommended that CIP-010-1 have an effective date that is 12 months after the effective date of the CIP V5 standards. The SDT will take this comment into consideration, as this comment references the Implementation Plan and not necessarily language within the CIP-010-1 standard.

One commenter commented on the use of the term "Configuration" versus "configuration." The SDT has revised CIP-010-1 to only use "configuration," since it was not the SDT's intent to include "Configuration," as this is not a NERC defined glossary term. Furthermore, another commenter questioned if the terms: "configuration management," "configuration change management," and "asset management" were synonymous terms. The SDT has revised CIP-010-1 to only use "configuration change management" for less confusion. "Asset management" is not synonymous with the other words in the previously mentioned sentence. "Asset management" where it is used (R1.1 measures) refers to SAP, Maximo, Cascade, Passport, or other asset management software. Also, due to other questions around the baseline configuration, the SDT has added further guidance to aid in entities' development of their baselines.

Applicability Section

A couple comments mentioned that the exemption language in Section 4.2.4 should be changed back to the previous ballot's CIP-010-1 language or this section should be struck if it truly only applies to CIP-002-5. The difference between the initial ballot posting and successive ballot posting is 4.2.3.5, which states that: "Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes."

One commenter recommended the striking of the applicability component of the main requirement. If the commenter is referring to Section 4 of CIP-010, then this section is required for NERC standards to identify the standard's applicability to Responsible Entities, while the (newly termed) "applicable systems" columns in the tables refers to the scope of systems to which a specific requirement row applies.

Many commenters recommended removing some or all associated assets/systems from various applicability sections in the CIP-010 requirements because they represent an increase in scope from CIP V3/V4. The SDT disagrees with this assessment, as CIP Version 3 and Version 4 standards mention applicability to cyber assets within the ESP. The cyber assets that could exist within an ESP would include Associated Protected Cyber Assets, Associated Electronic Access Control or Monitoring Systems, and Associated Physical Access Control Systems. Therefore, the SDT does not believe that the assets/systems from CIP-010's applicability represent an increase in scope from CIP Version 3 and Version 4 standards.

One commenter expressed concern over 4.2.2, bullet 3, which references: "… Transmission where the Protection System is required by a NERC or Regional Reliability Standard." The concern was that CIP-010-1 was requiring the installation of a Transmission Protection System. This assessment is incorrect. CIP-010-1 does not require the installation of a Transmission Protection System, but other NERC or Regional Reliability Standards may require the installation of a Transmission Protection System.

Guidelines Section

Several commenters suggested adding the phrase: "network connectivity to identify" to the Requirement R3 guidance with regard to passive network discovery. The standard has been modified in consideration of these comments to include the phrase. One commenter made several other suggestions (such as the addition of details on baseline configurations and cyber security controls) in regards to guidance that informed the SDT's modification of that section.

Background Section

Several commenters mentioned that the third paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. The SDT believes that this third paragraph is clear in stating:

- A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence.
- The word "required" is not used to describe numbered or bulleted lists. The SDT wishes to emphasize that measures are only examples of evidence.

Requirement R1

One commenter proposed revision of the Requirement R1 to: "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has added the "in a manner that identifies, assesses, and corrects deficiencies" language to the requirement, which is described above.

One commenter proposed that the requirement be changed to a program- or performance-based level to allow more flexibility (citing FERC FFT Order, Paragraph 81). The comment furthermore mentions that programs such as Tripwire would not be able to be used. Other commenters had similar comments in regards to the prescriptive language of CIP-010-1 Requirement R1.1. Based on the revised "identify, assess, and correct deficiencies" language, the SDT believes that more flexibility is achieved through an entity's internal controls process. Furthermore, the SDT believes that programs such as Tripwire could be used to aid in compliance with CIP-010-1 Requirement R2.

One commenter believed that information in Requirement R1 should only be collected for personal computers and protective relays. The SDT disagrees with this comment, as the applicability should involve all BES Cyber Assets, BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems since these assets can be found within the same Electronic Security Perimeter.

One commenter asked if recording software "hashes" can be used as an alternative to recording version levels to verify that no unauthorized changes have been made to software on the BES Cyber Asset. The SDT attempted to provide flexibility to allow the entity to determine how to track changes. However, in regards to CIP-010-1 Requirement R1, the baseline configuration still must be documented. If an entity is able to use software "hashes" to monitor for changes to the baseline configuration of a BES Cyber System, then this solution could be used for CIP-010-1 Requirement R2.1.

One commenter proposed a modification to language in CIP-010-1 Requirement R1 to eliminate the term "baseline" so that it is not confused with the security baselines that they create today for devices. Two other commenters also wanted to remove the "baseline" from CIP-010-1 requirement language. The SDT disagrees with the proposed change and believes that the language, as is with the term "baseline," is sufficient.

Requirement Part 1.1

A few commenters emphasized that Version 4 did not apply to noncritical; but in accordance with FERC Order 761, Paragraph 86, these assets/systems should be included in CIP-010-1 Requirement R1.1. Therefore, external routable connectivity exclusion language was not included in the applicability for CIP-010-1 Requirement R1.1. Numerous commenters also alternatively recommended that CIP-010-1 Requirement R1.1 applicability only include High Impact BES Cyber Systems. The SDT disagrees and continues to cite FERC Order 761, Paragraph 86.

Several commenters disagreed with the use of the phrase: "… each Cyber Asset identified, individually or by group." The SDT has revised the requirement language in regards to their comment so as to ensure baselines can be defined at the individual or group level.

One commenter also desired a clarification of what may be grouped under CIP-010-1 Requirement R1.1. The SDT hopes that the revised requirement language provides additional clarity.

Requirement Part 1.1, Sub-Part 1.1.1

One commenter believed that this requirement is covered in CIP-009 Requirement R.1.3. The SDT disagrees with this comment as the process for the backup and storage of information required to recover BES Cyber System functionality is not required to include baseline configuration items.

Several commenters recommended replacing "exists" with "is either operating or running." Another commenter believed the wording of "is installed" is also sufficient. The SDT wants to underscore that "exists" refers to the case when an asset has firmware instead of an Operating System.

Requirement Part 1.1, Sub-Part 1.1.2

One commenter mentioned that "BES Cyber Asset" should be replaced with "applicable Cyber Asset." Other commenters had a similar position with regards to the use of "BES Cyber Asset." These comments were taken into consideration and

the related requirement sub-part was modified. The phrase "on the BES Cyber Asset" was removed from the requirement sub-part for consistency.

Multiple commenters requested clarification on the "applications." Does "applications" mean "SCADA, EMS, State Estimator, etc." instead of "device drivers and DLL applications" included in an operating system or package?" In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

One commenter believed that this requirement is covered in CIP-009 Requirement R.1.3. The SDT disagrees with this comment, as the process for the backup and storage of information required to recover BES Cyber System functionality is not required to include baseline configuration items.

A couple commenters suggested the removal of the word "intentionally" from the requirement language. The SDT believes that the use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for cyber asset use should be included. It is not the SDT's intent for notepad, calculator, DLL, device drivers, or other applications included in an operating system package to be considered as commercially available or open-source application software. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

Several entities requested clarity on how granular the version identifier should be. The SDT provides flexibility for entities to determine what version levels should be tracked. The purpose of tracking the version allows entities to keep abreast of the version levels in their inventory. If software manufacturers alert entities to vulnerabilities in their software, the affected population could be identified through software version. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

Several entities suggested that sub-part 1.1.2 should exclude anti-malware signature file version identifiers due to the volatility of frequency updates. The SDT believes that only version levels that can aid in recognizing affected software should be tracked. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

Requirement Part 1.1, Sub-Part 1.1.3

Multiple entities asked if a version control tool/system (like Concurrent Versions Systems) could demonstrate the custom software's version. In consideration of these comments, this requirement sub-part has been reworded to be "custom software installed." However, even in its successive ballot form, the requirement sub-part did not require the custom software version. Instead, the requirement sub-part requires the identification of the custom software.

One commenter believed that this requirement is covered in CIP-009 Requirement R.1.3. The SDT disagrees with this comment, as the process for the backup and storage of information required to recover BES Cyber System functionality is not required to include baseline configuration items.

Multiple commenters suggested removing "developed for the entity." The SDT has taken this comment into consideration and modified the requirement language accordingly.

There were several commenters who proposed modified language to clarify the term "custom software." The SDT disagrees with these proposed changes, but has reworded the requirement language in an attempt to provide additional clarity.

Requirement Part 1.1, Sub-Part 1.1.4

There were many commenters who believed that this requirement is covered in CIP-007. The SDT remarks that CIP-007 is evaluating what patches should be installed, while CIP-010 handles the patch being implemented (i.e., going through the configuration change management process).

One commenter believed that CIP-010-1 Requirement R1.1.4 would require the industry to account for more than a billion ports if each of 214 entities had less than 100 routable assets. Only ports which are accessible need to be included in the baseline. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

One commenter asked for clarity around "logical network accessible ports." In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

One commenter mentioned that the applicability columns from CIP-007 should match the applicability column in CIP-010-1 Requirement R1. The SDT does not agree with this comment, as the concept in CIP-010 is to identify logical network accessible ports, while CIP-007 requests entities to enable logical network accessible ports.

Requirement Part 1.1, Sub-Part 1.1.5
One commenter mentioned that CIP-010-1 Requirement R1.1.5 should be clarified to identify only those patches applied to the asset at the time the baseline is established and not all possible historic patches available for the asset. This comment was taken into consideration and the related requirement sub-part was modified.

Many commenters believed that this requirement is covered in CIP-007. The SDT remarks that CIP-007 is evaluating what should be used, while CIP-010 is the implementation.

One commenter believed that CIP-010-1 Requirement R1.1.5 would require an entity to document tens of thousands of unique patch installs for less than 200 Windows based Cyber Assets. Only historic or current patches that have been applied would be included in the baseline.

Several comments raised the concern Requirment R1.1.5 changes too frequently to be in the baseline and should be removed; that the evaluation of each patch is already included in CIP-007-5. The SDT believes that CIP-010-1 Requirment R1.1.5 is supposed to be a comprehensive listing of the patches that have been installed on the device. Patches are not required to be evaluated with this requirement. Instead, if a patch has been added to the device, then an update of the baseline is required.

Measures for Requirement Part 1.1
Per a comment, “or group” was added to CIP-0101 Requirement R1.1 measures to make consistent the requirement language and measures.

Requirement Part 1.2
One commenter proposed a rewording of CIP-010-1 Requirement R1.2 to: “Authorize changes to: security controls, operating systems, application software versions, custom software, ports or patches. Authorize changes to add or remove hardware.” The SDT disagrees with this comment, as the requirement language is consistent with other similar CIP Version 5 requirement language.

One commenter proposed indicating the appropriate authorizing individual or delegate in the requirement. The SDT believes that the requirement is sufficient, as is since it provides flexibility so that the entity can select the appropriate authorizing individual.

Measures for Requirement Part 1.2

One commenter recommended the removal of language in measures around individuals or groups with the authority to authorize the change. The SDT believes that measures are only examples of evidence. To be in compliance with the requirement language, an entity could authorize change by an individual, a group, or other entity-determined method.

There were two comments that recognized a concern with the language: "Documentation that the change was performed in accordance with the requirement." There was another suggestion to remove this language since it is not clear to what term the requirement is referring. The SDT believes that since the measure is for CIP-010-1 Requirement R1.2, that the language in the measure directly refers to CIP-010-1 Requirement R1.2 language only. While the SDT considered adding a reference to CIP-010-1 Requirement R1.2 in the measure to make explicit the requirement to which the measure language was referring, for consistency across CIP-010, this change was not made.

Requirement Part 1.3

One commenter mentioned that the applicability columns from CIP-005 and CIP-007 should match the applicability column of CIP-010-1 Requirement R1.3. This comment was taken into consideration and the related requirement sub-part was modified accordingly. The reference to CIP-005 and CIP-007 was removed from the requirement sub-part; and, therefore, the applicability columns between the standards do not need to be consistent.

There were many commenters that expressed concern with the 30-day time frame. Other commenters recommended the removal of the 30-day time frame for updating the baseline configuration. The SDT disagrees with the commenters and believes that a 30-day time frame allows entities time to update their baseline configuration documentation. Similiarly, other commenters had issues with the 30-day time frame and the references to CIP-005 and CIP-007. These issues are no longer a concern, as the SDT has removed the reference to CIP-005 and CIP-007 in regards to the 30-day time frame.

Two commenters were concerned about 'triple', or 'double' jeopardy with CIP-005 and CIP-007. One commenter suggested a revision or removal of the references, while another suggested that the requirement be moved to CIP-005 or CIP-007. In consideration of their comment, the SDT has modified CIP-010-1 Requirement R1.3 accordingly. In response, references to CIP-005 and CIP-007 have been removed from the sub-part requirement language.

Requirement Part 1.4

Many comments stated that "High Impact BES Cyber Systems" should be removed from applicability in CIP-010-1 Requirement R1.4 since this requirement sub-part is repetitious with CIP-010-1 Requirement R1.5. While CIP-010-1 Requirement R1.4 has been modified due to comments from industry, the SDT disagrees that CIP-010 Requirement R1.4 is repetitious with CIP-010-1 Requirement R1.5. CIP-010-1 Requirement R1.5 requires entities to test their baseline configuration changes in a test environment and document the results, while CIP-010-1 Requirement R1.4 requires entities to identify cyber security controls and then verify that these identified cyber security controls and system availability are not adversely affected after making the change.

A bevy of commenters believed that this requirement should include an exclusion for CIP Exceptional Circumstances. The SDT does not agree with this comment, as even after the CIP Exceptional Circumstance has happened, an entity should determine that controls were not adversely affected.

Several commenters suggested that guidance be added on cyber security controls. The SDT has taken their comment into consideration (in addition to other similar inquiries on cyber security controls) and added additional information on cyber security controls in CIP-010 guidance.

One commenter proposed the following language for this requirement part: "For a change that deviates from the existing baseline configuration or may have an impact on controls implemented for CIP-005, CIP-006, or CIP-007, [do 1.4.2]." While the SDT considered this approach, the SDT believes the current requirement language is sufficient as is.

CIP-010-1 Requirement Part 1.4, Sub-Part 1.4.1

One commenter suggested a language change of "determined" to "identified." The SDT disagrees with this proposed change and believes that the current language is sufficient as is.

One commenter believed CIP-010-1 Requirement R1.4.1 where "could be impacted" is used will cause all entities to document every control for every change in order to avoid zero-defect audit enforcement when some situation can be devised where "could be impacted" is a remote possibility. Southern believed that documenting "what could be impacted" is not a reliability benefit, it's the verification that controls are not affected by a change. The SDT agrees with their recommended change, and the requirement language has been updated accordingly in Requirement R1 with: "implement, in a manner that identifies, assesses, and corrects deficiencies," to avoid the zero-defect audit enforcement concern.

Several commenters believed that CIP-010-1 Requirement R1.4.1 could result in the Responsible Entity declaring that no cyber security controls are expected to change and, thus, no testing is required. The SDT does not agree with this assessment, as the requirement requires documentation of what could be changed followed by verification that potentially impacted controls were not affected in CIP-010-1 Requirement R1.4.2.

Many commenters recommended the removal of Requirement R1.4.1. The concept is that an entity identifies all related controls that could be impacted based on all requirements in CIP-005 and CIP-007. Therefore, the SDT believes that by mentioning CIP-005 and CIP-007, there is no need for interpretations. In fulfilling the requirement, an entity must identify that a particular change impacts CIP-005-5 Requirement R1 or CIP-005-5 Requirement R1 and CIP-005-5 Requirement R2. If all requirements in CIP-005 and CIP-007 may be affected by a deviation to the existing baseline configuration, then this would be documented in accordance to CIP-010-1 Requirement R1.4.1. It should also be mentioned that CIP-010-1 Requirement R1.4 is not repetitious with CIP-010-1 Requirement R1.5. CIP-010-1 Requirement R1.5 requires entities to test their baseline configuration changes in a test environment and document the results, while CIP-010-1 Requirement R1.4 requires entities to identify cyber security controls and then verify that these identified cyber security controls and system availability are not adversely affected after making the change.

CIP-010-1 Requirement Part 1.4, Sub-Part 1.4.2

One commenter mentioned that “BES Cyber Asset” should be replaced with “applicable Cyber Asset.” This comment was taken into consideration and the related requirement sub-part was modified. The phrase “BES Cyber System” was removed from the requirement sub-part for consistency.

Many commenters expressed concern with CIP-010-1 Requirement R1.4.2’s “availability” term. The SDT has modified the requirement language in consideration of these comments. The “available” term has been removed.

One commenter proposed that the word “determined” be changed to “identified.” The SDT disagrees with this proposed change and believes that the current language is sufficient as is.

One commenter believed the term “applicable” should be added for clarity. The SDT remarks that “applicable” is not required, as CIP-010 Requirement R1.4.2 points to CIP-010-1 Requirement R1.4.1, which ensures entities only look at the potentially impacted controls.

One commenter requested clarification of use of the term "required controls." The word required refers to the cyber security controls in CIP-005 and CIP-007 that were applied based on asset identification in CIP-002. While the SDT references all of CIP-005 and all of CIP-007, CIP-010-1 Requirement R1.4.1 requires entities to identify those controls in CIP-005 and CIP-007 that are potentially impacted. Therefore, CIP-010-1 Requirement R1.4.2 is only looking at the controls identified in CIP-010-1 Requirement R1.4.1.

One commenter proposed the addition of a time frame for how long an entity may take to make the verification required in CIP-010-1 Requirement R1.4.2. The SDT has taken this into consideration. The SDT also believes that the "identify, assess, and correct deficiencies" should provide aid in compliance concerns regarding this requirement.

CIP-010-1 Requirement Part 1.5, Sub-Part 1.5.1

Multiple commenters expressed concern with the language in CIP-010-1 Requirement R1.5.1. A few of the aforementioned organizations mentioned that the parenthetical expression in CIP-010-1 Requirement R1.5.1 should be altered to no longer include parenthesis. This comment was taken into consideration and the related requirement sub-part was modified. The language in the requirement part has been altered. Other organizations recommended changing CIP-010-1 Requirement R1.5.1 language to: "testing cyber security controls, where technically feasible, for each change that deviates from the existing baseline configuration" for clarity. The SDT has reworded requirement language based on industry comment and hopes that the changes provide additional clarity. Alternatively, other organizations proposed the removal of the following language in CIP-010-1 Requirement R1.5.1: "…that models the baseline configuration to ensure that required cyber security controls are not adversely affected." This is redundant to the concept in the last sentence, which requires documenting differences between test and production when a test environment is used. The SDT disagrees with the comment, as documenting the differences between the test and production environment is a completely separate task compared to modeling the baseline configuration. Modeling the baseline configuration is an attempt to re-create the baseline configuration on a single asset, while documenting differences between the test and production environment would simulate the rest of the assets in that environment and how they function together. Other organizations were concerned that the revised language in the posted standard removed the possibility for a technical feasibility exception. The SDT does not agree, as old, legacy systems may not be available in a test environment and there may be no way to utilize a production environment where a test can be performed in a manner that minimizes adverse effects.

One commenter asked if this requirement interferes with CIP-010-1 Requirement R1.4 for High Impact Systems. There was a suggestion to remove the overlap in applicability of the two requirements and adding clarifying language as to

what is intended and required in CIP-010-1 Requirement R1.4 vs. CIP-010-1 Requirement R1.5. The SDT wishes to underscore that CIP-010-1 Requirement R1.4 is not repetitious with CIP-010-1 R1.5. CIP-010-1 R1.5 requires entities to test their baseline configuration changes in a test environment and document the results, while CIP-010-1 Requirement R1.4 requires entities to identify cyber security controls and then verify that these identified cyber security controls and system availability are not adversely affected after making the change.

One commenter requested clarification of use of the term: "required controls." The SDT responds by claiming that "required" refers to the cyber security controls in CIP-005 and CIP-007 that were applied based on asset identification in CIP-002. Additional information on cyber security controls were added in CIP-010-1 Guidelines for Requirement R1.

Several commenters expressed concern over the "where technically feasible" language. Alliant Energy proposed that: "where technically feasible" should be changed to "where test environments exist." One commenter wanted to know what the language pertained to. The SDT does not agree with the proposed modification. The language in the requirement allows for test environments to exist in a production environment where the test is performed in a manner that minimizes adverse effects. Also, it should be made clear that the exception language refers to both CIP-010-1 Requirement R1.5.1 and Requirement R1.5.2.

Requirement Part 1.5, Sub-Part 1.5.2

Some commenters believed that the following language should be removed from the sub-requirement: "including a description of the measures used to account for any differences in operation between the test and production environments." Another commenter stated that they do not understand the intent of requiring this type of documentation, as it provides no security benefit and only invites auditors to unnecessarily critique the methods that the entity determines are appropriate to address the differences between the two environments. The SDT does not agree with this assessment and believes the documentation of the differences is important.

SPP RE and City Utilities of Springfield, MO asked if CIP-010-1 Requirement R1.5.2 permits the documentation of a stand-alone test environment with identified differences from the production environment. The SDT concurs that the requirement language requests documentation of the differences between the test and production environment, if a test environment was used. If the differences did not change from change to change, then the same documentation would be included with each change package that is processed.

Requirement R1 VRFs

Based on numerous comments, the VRFs in Table of Compliance Elements now match the VRF as identified at the requirements and measures section of the standard. This modification is for both CIP-010-1 Requirement R1 and Requirement R2.

Requirement R1 VSLs

There were two commenters who suggested that in corresponding to the proposed revisions to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. The SDT will take this into consideration, as we apply the non-zero defect forward looking compliance process.

Two commenters suggested that "any" be changed to "one or more" in the High VSL for CIP-010-1 Requirement R1. The SDT has updated the VSL language per the comment's recommended change.

One commenter believed that the phrase "and to document those changes" in the first condition of the High VSL for CIP-010-1 Requirement R1 should be deleted, as it is duplicative of the second condition. The SDT has removed the second condition due to modification to the requirement language to remove reference to other CIP standards in CIP-010-1 Requirement R1.3.

Main Requirement R2

One commenter proposed revision of the Requirement R1 to: "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has considered this approach in accordance with the FFT process. The following language has been added to requirement language: "identifies, assesses, and corrects deficiencies…"

Requirement Part 2.1

Many comments were on the initial ballot posting language, as the successive ballot posting language is not understandable. The SDT has modified the requirement in consideration of their comment.

One commenter believed that double jeopardy exists with CIP-010-1 Requirement R1 and CIP-010-1 Requirement R2.1. If a paperwork error occurs in authorizing a change and this requirement uncovers it, this should be addressed under CIP-010-1 Requirement R1, not a separate requirement. The SDT disagrees with this assessment. CIP-010-1 Requirement

R2.1 does not create a double jeopardy situation with CIP-010-1 Requirement R1 since the violation would be in CIP-010-1 Requirement R1, not in CIP-010-1 Requirement R2.1. CIP-010-1 Requirement R2.1 requires entities to document and investigate detected unauthorized changes. If one of the unauthorized changes is due to a violation of CIP-010-1 Requirement R1, then the self-report would be on CIP-010-1 Requirement R1 and not on CIP-010-1 Requirement R2.1. However, based on the new "identifies, assesses, and corrects deficiencies" language, if an issue is detected, based on an entity's internal control processes, this would not be a self-report. Other commenters stated on CIP-010-1 Requirement R2 creating a situation where a need would exist to self-report. With the new requirement language of "identifies, assesses, and corrects deficiencies," a self-report would not be necessary.

Many commenters essentially mentioned concerns centered on technical feasibility language. Some of the aforementioned organizations requested that the term "continuous" be removed from requirement language; while others proposed language that would remove the technical feasibility exception. The SDT has modified the requirement language in consideration of these comments. One commenter further commented that the language should be revised in such a way that only devices that can monitor automatically should be included; otherwise, a technical feasibility exception should be allowed. The SDT has modified the language such that monitoring could be done manually or continuously depending on the device.

One commenter suggested a change to the following language: "Document changes tracked through the entity's change management program." The SDT does not agree with this approach and believes the language is sufficient as is. One commenter recommended a similar approach of modifying the language due to their desired removal of "baseline" term use.

Many commenters suggested a different time frame for monitoring. The suggestion called for a 90-day instead of 35-day time frame, while other commenters suggested an annual or quarterly time frame. The SDT believes that a 35-day time frame is sufficient for an "express acknowledgement."

One commenter believed that the requirement will be burdensome and nothing gained from it except a lot of TFE paperwork to track. The SDT disagrees with this comment, as the requirement was added based on FERC Order 706.

One commenter asked if no change is detected during a monitoring period, how an entity can demonstrate that "no change" occurred. The requirement language mentions that only detected unauthorized changes need to be documented and investigated. If there is no change, then this would not need to be documented.

Measures for Requirement Part 2.1

One commenter emphasized that the requirement requires monitoring for all changes, yet the measure mentions calls for investigation of any unauthorized changes. They believe that the requirement language should be changed to include "unauthorized" changes such that monitoring is only necessary for unauthorized changes. The SDT does not agree with this assessment and believes that the requirement language and measures are sufficient as is.

One commenter requested clarity on the phrase "record of investigation." "Record of investigation" would be some type of documentation that shows that a detected unauthorized change was documented and investigated accordingly.

Requirement R2 VRFs

Multiple commenters stated that the VRFs in the table of compliance elements now matches the VRF as identified at the requirements and measures section of the standard. This modification is for both CIP-010-1 Requirements R1 and R2.

Requirement R2 VSLs

Several commenters suggested that in corresponding to the proposed revisions to the requirement statement, the VSLs should be revised to: "severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention." The SDT will take this into consideration as we apply the "non-zero defect forward looking compliance process."

Two commenters believed that a new gradated VSL should be introduced due to time-period language added in the previous posting. The SDT has taken this comment into consideration. While gradated VSLs were not introduced, since the requirement language includes "… identify, assess, and correct deficiencies…", the VSLs have been updated. .

Requirement R3

One commenter proposed a revision to Requirement R1 to read: "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has considered this approach in accordance with the FFT process. The following language has been added to requirement language: "identifies, assesses, and corrects deficiencies…"

A few commenters mentioned that the applicability between CIP-010-1 Requirements R3.3 and R3.4 differed. The SDT recognizes this difference and emphasizes that these are two different requirements and, hence, the applicability should be different.

One commenter asked if all Vulnerability Assessments under Requirement R3 must be performed prior to Version 5's Effective Date or whether entities have an additional year or three years from the effective date. The answer to NIPSCO's question can be found in the CIP Version 5 Implementation Plan. CIP-010-1 Requirements R3.1 and R3.2 must initially be complied with 12 months after the Effective Date of the CIP Version 5 standards.

One commenter asked why CIP-010-1 Requirement R3 does not always include Medium Impact in its scope. The SDT believes that the applicability as is can be considered sufficient. TRE also had concerns that the Requirement R3 does not include an annual vulnerability assessment. This is incorrect as CIP-010-1 Requirement R3.1 requires an annual vulnerability, while CIP-010-1 Requirement R3.2 requires a 36-month vulnerability assessment (for the applicable systems).

One commenter asked for clarity over the inclusion in applicability of Electronic Access Control or Monitoring Systems in CIP-010-1 Requirement R3. This requirement has the same applicability for these systems as in previous NERC CIP version. Therefore, the SDT believes that these systems should remain included in the applicability for CIP-010-1 Requirement R3.

One commenter asked if vulnerability assessments are required for every cyber asset or a sampling of cyber assets. Per applicable systems section, the vulnerability assessment is required for the systems listed.

Requirement Part 3.1

Commenters recommended that the requirement start with its purpose. The SDT disagrees with this comment, as the requirement language is consistent with other similar CIP V5 requirement language.

Many commenters proposed to reword Requirement R3.1 with the following language: "once each calendar year or a period not to exceed 15 calendar months between assessments." The SDT has taken these comments under consideration and is modifying the requirement sub-part language accordingly. One commenter proposed alternative language allowing an entity determined time frame. The SDT disagrees with this comment since the 15 calendar months' time frame is sufficient.

A few commenters believed that double jeopardy exists with reference to CIP-005, CIP-006, and CIP-007. The SDT does not agree, as if controls are not implemented correctly, then this would be a violation in the respective CIP standard, and not CIP-010-1.

Many commenters recommended that CIP-006 be removed from requirement language. The SDT agrees and has removed the reference to CIP-006.

Multiple commenters had concerns on what exactly constituted an active vulnerability assessment. The SDT points to guidance in CIP-010 on Requirement R3 in regards to recommended elements of an active vulnerability assessment. Also, other commenters asked if an active vulnerability assessment must be done for all systems or a representative sampling. Per the applicable systems section of the table for Requirement R3, the active vulnerability assessment must be done for all applicable systems.

One commenter requested clarification on whether an external vendor needs to perform the annual vulnerability assessment or can the Responsible Entity perform this task. The SDT provides enough flexibility in the requirement so that the RE can determine the solution that best meets its needs.

Several commenters believed that CIP-010-1 Requirement R3.1 is redundant with CIP-010-1 Requirement R1.3. The SDT does not agree, as CIP-010-1 Requirement R3.1 requires an annual vulnerability assessment, while CIP-010-1 Requirement R1.3 requires an update of the baseline configuration for a change that deviates from the existing baseline configuration.

Measure for Requirement Part 3.1

One commenter believed that reference to “individuals” in the first bulleted item needs to be removed. The SDT emphasizes that measures are only examples of evidence. However, the SDT has modified the measure language in consideration of the comment.

Requirement Part 3.2

Many commenters expressed concern with the language in CIP-010-1 R3.2. Another comment mentioned that the parenthetical expression in CIP-010-1 R3.2 should be altered to no longer include parenthesis. This comment was taken into consideration and the related requirement sub-part was modified. The language in the requirement part has been

altered. Furthermore, the commenters recommended that this requirement start with its purpose. The SDT disagrees with these comments as the requirement language is consistent with other similar CIP Version 5 requirement language.

Multiple commenters asked for clarification on CIP-010-1 Requirement R3.2 in regards to this being a paper exercise. The requirement language mentions active vulnerability assessment. In response, please see the guidance section on additional details on an active vulnerability assessment.

Multiple commenters proposed the removal of the language: "that models the baseline configuration to ensure that required cyber security controls are not adversely affected" in CIP-010-1 Requirement R3.2, commenting that it is redundant to the concept in the last sentence, which requires documenting differences between test and production when a test environment is used. The SDT does not agree with this assessment. CIP-010-1, Requirement R3.2.1 requires performing an active vulnerability assessment in an environment that models the baseline configuration of the BES Cyber System in a production environment, while CIP-010-1 Requirement R3.2.2 requires documenting the results of testing, and if, a test environment was used, documenting the differences.

One commenter asked how is this requirement differs from CIP-007. The SDT remarks that CIP-010-1 Requirement R3.2 is related to completing a vulnerability assessment every three years to assess controls in CIP-007 (and CIP-005) are implemented correctly.

One commenter believed that the following language should be removed from the sub-requirement: "including a description of the measures used to account for any differences in operation between the test and production environments." One commenter stated that they do not understand the intent of requiring this type of documentation, as it provides no security benefit and only invites auditors to unnecessarily critique the methods that the entity determines are appropriate to address the differences between the two environments. The SDT does not agree with this assessment and believes the documentation of the differences is important in establishing how the testing environments differ.

A few commenters asked if the assessment in CIP-010-1 Requirement R3.2 is in lieu of or in addition to the assessment required by CIP-010-1 Requirement R3.1 in the calendar year that the CIP-010-1 Requirement R3.2 assessment is conducted. The SDT believes that CIP-010-1 Requirement R3.2 is in lieu of CIP-010-1 Requirement R3.1 in the calendar year that CIP-010-1 Requirement R3.2 is conducted.

One commenter asked if CIP-006 is within scope of CIP-010-1 Requirement R3.2. The SDT has removed the reference to CIP-006 in CIP-010-1 Requirement R3.1, and is not a similar reference in CIP-010-1 Requirement R3.2.

One commenter proposed that the phrase: "where technically feasible" should be changed to "where test environments exist." The SDT does not agree with this modification since language in the requirement allows for "test environments" to exist in a production environment where the test is performed in a manner that minimizes adverse effects.

There was a comment mentioned that CIP-010-1 Requirement R3.2 requires assessments every three years, while CIP-007-3 Requirement R8 required vulnerability assessments annually. It was thought that we weakened the requirement; however, CIP-010-1 Requirement R3.1 requires an annual vulnerability and, therefore, the annual requirement in CIP-007-3 Requirement R8 was not weakened.

A commenter requested that associated electronic access control or monitoring systems and associated protected cyber assets should be added to the applicability for Requirement R3.2. For consistency in CIP-010-1, the SDT does not agree with the proposed change in applicability.

Requirement Part 3.3

One commenter believed it to be problematic to perform an active vulnerability assessment prior to installing a new Cyber Asset. The SDT acknowledges the concern, but emphasizes that an active vulnerability assessment is not required in the cases of a CIP Exceptional Circumstance or like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset.

One commenter believed that the term "active vulnerability assessment" is not defined. The SDT disagrees with this statement, as guidance is provided that aids in understanding an active vulnerability assessment. Furthermore, the commenter stated that since sufficient change management controls exist that an active vulnerability assessment is unnecessary. The SDT disagrees with this statement, as the configuration change management controls in CIP-010-1 Requirements R1 and R2 are in place for changes that deviate from the existing baseline configuration, while vulnerability assessments in CIP-010-1 Requirement R3 are for ensuring proper controls and detecting vulnerabilities.

One commenter mentioned that the parenthetical expression in CIP-010-1 Requirement R3.3 should be altered to no longer include parenthesis. This comment was taken into consideration and the related requirement sub-part was modified. The language in the requirement part has been altered.

Multiple commenters expressed concern around the language in CIP-010-1 Requirement R3.3. Some of the aforementioned organizations recommended that this requirement start with its purpose. Other organizations recommended a revision of the language. The SDT has taken these comments into consideration and modified the requirement language accordingly.

Multiple commenters suggested revisions to "prior to adding" language. One commenter proposed that instead of "prior to adding," that the requirement language should read: "before closing the change." Some vulnerability assessments actions only add value to assess after connected to the ESP as part of implementation and post implementation testing. The SDT disagrees with the proposed change and believes that the current language is sufficient based on other comments from industry.

One commenter believed that the parenthetical explanation of a like replacement should be moved to guidance. The SDT disagrees with the proposed change and believes that the current language is sufficient based on other comments from industry.

Several commenters believed that CIP-010-1 Requirement R3.3 appears to be missing "and" after the parenthesis. Without the parenthetical, it should read "Except for CIP Exceptional Circumstances and like replacements and prior to adding a new Cyber Asset..."

A couple commenters suggested that Physical Access Control Systems should be added in the applicable systems column. The SDT does not agree with their proposed change, as references to Physical Access Control Systems and CIP-006-1 have been removed throughout CIP-010-1.

One commenter expressed confusion around the use of the term: "new Cyber Asset." The commenter questioned if this term references a new Cyber Asset that is part of an existing Cyber System, or a new Cyber Asset per CIP-002. The SDT remarks that CIP-010-1 Requirement R3.3 is for new Cyber Assets with baseline configurations that do not currently exist. Therefore, a new Cyber Asset that is part of an existing Cyber System (and that has an existing baseline configuration) does not require an active vulnerability assessment per CIP-010-1 Requirement R3.3.

Several commenters believed that the language should be consistent among CIP-010-1 Requirements R3.1 through R3.3 in regards to vulnerability assessments. The SDT has modified the requirements accordingly in consideration of their comment.

A commenter asked if cyber assets can be placed in ESP before remediation of identified vulnerabilities. The SDT remarks that cyber assets can only be placed in ESP before remediation of identified vulnerabilities if a CIP Exceptional Circumstance exists or the cyber asset is a "like replacement."

CIP-010-1 Requirement Part 3.4

One commenter suggested that the term "if any" be added in CIP-010-1 Requirement R3.4 to denote the need to document the results of assessments that identified no vulnerabilities. The SDT disagrees as the language in CIP-010-1 Requirement R3.4 follows closely to the language in its previous instance in an earlier CIP standards version.

Many commenters expressed concern with the phrase: "remediate or mitigate vulnerabilities" and the related documentation. Another commenter proposed to replace "remediate or mitigate vulnerabilities" with "implement lessons learned (if any)" for consistency with other standards and eliminate extra documentation tracking requirements. The SDT developed this requirement language directly from the previous CIP versions. The concept is that an entity must document how they plan to remediate or mitigate identified vulnerabilities. CIP-010-1 Requirement R3 becomes an internal controls requirement to ensure that cyber security controls are properly implemented. While other commenters asked if it is the intent that identified vulnerabilities would not constitute violations of requirements they are found against. It is not the SDT's intent that an identified vulnerability would not constitute a violation of other requirements. While CIP-010 would not be violated, the respective CIP-005 or CIP-007 standard may be violated. The SDT does believe that the self-report mitigation plan could be used as the action plan for Requirement R3.4.

Several entities believed that the deadline for documenting the results of the assessment and the action plan should be specified. They suggested a 30-day limit. Also, they suggested including levels of gradation for not meeting the 30-day limit. One commenter took a different approach and recommended that "planned date" be changed to "estimated time frame." The SDT believes that the requirement language is sufficient as is.

Several commenters believed that more specificity should be added around the term “assessments” in CIP-010-1 Requirement R3.4. The SDT has modified the language in consideration of these comments and the text: “conducted pursuant to Parts 3.1, 3.2, and 3.3” was added to the requirement language.

One commenter asked for clarity in regards to the phrase “planned date of completing the action plan.” Is this the completion of the formulation of the plan or the completion of the tasks within the plan? The SDT articulates that the planned date of completing the action plan is related to the completion of the tasks within the plan.

Requirement R3 VRFs

There were multiple comments on VRFs, and the VRFs in Table of Compliance Elements now matches the VRF as identified at the Requirements and Measures section of the standard. This modification is for both CIP-010-1 Requirements R1 and R2.

Requirement R3 VSLs

Several commenters believed that corresponding to the proposed revisions to the requirement statement that the VSLs should be revised to read: “severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention.” The SDT has taken this comment into consideration as we applied the “identify, assess, and correct” approach; however, that language should not be included here. The reasoning behind this decision is due to the CIP-010-1 R3 Requirement’s indirect (mentioned in R3 Guidance) reference to CIP-005 and CIP-007. The related language would relate to the timely performance of completing a vulnerability assessment instead of identifying and correcting deficiencies which may be a part of the related CIP-005 and CIP-007 langauge (CIP-005 does not include this language in its requirements).

Several commenters proposed that the third condition in Severe VSL have the word “or” instead of “and.” The SDT has modified the language in response to their comment.

One commenter believed that the VSL does not address the 36-month timeline in CIP-010-1 Requirement R3.2. Furthermore, the commenter proposed additional language to address this timeline. The SDT has taken this comment into consideration and modified the VSL language accordingly.

QUESTION C15 – CIP-011-5:

If you disagree with the changes made in CIP-011-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, there were many global comments that related not only to CIP-011, but to all of the CIP standards.

Annual Requirements

Many commenters objected to the posted language referencing annual requirements. Several suggested alternative ways to express the frequency for an annual requirement. The SDT considered all of the recommendations and decided use the phrase "at least once every 15 calendar months" (or similar) to express the frequency for annual requirements.

Use of the phrase "but not limited to" in measures language

The SDT received many comments objecting to the phrase "but not limited to" within the measures. Some comments suggested removal of the term; others recommended a default to the use of the word "or," while others suggested the use of the word "and." Commenters believed that using the "but not limited to" language creates confusion about whether the specified measures are necessary or sufficient. The SDT has considered this issue carefully. The SDT has modified the language to "examples of acceptable evidence include, but are not limited to." The phrase "but not limited to" is designed to be of benefit to the Responsible Entity, not be a back door "gotcha" for auditors. Use of the phrase allows the entity flexibility in the type of evidence they are able to provide both now and in the future.

Applicability Column Title

The length of the applicability column title caused confusion about the systems/assets that are within scope for some entities. Several commenters suggested shortening the column heading to "applicability." The SDT recalls that the title of the column as previously posted was in response to comments from the first posting. SDT has renamed the column "applicable systems."

The SDT received many comments stating that: "Medium Impact BES Cyber Systems should be limited to Medium Impact BES Cyber Systems with External Routable Connectivity to maintain consistency with the scope of cyber systems/assets currently covered by similar requirements in the CIP Version 4 standards." A main goal of the SDT is to implement the FERC directives in Order 706 and Order 761. Order 761 states that FERC: "…supports the elimination of the blanket

exemption for non-routable connected cyber systems…continued blanket exemption in Version 5 would not adequately address risk." The SDT has considered each requirement concerning handling the exemption for non-routable connections. The SDT does not agree that in CIP-011 the scope should be limited to only BES Cyber Systems with External Routable Connectivity, as recommended in some comments.

Many commenters requested the removal of all references to systems and assets in requirements and that the SDT rely on the applicability column only to specify applicability. The SDT agrees with this recommendation. Wherever possible, the assets in scope will be indicated only in the applicability column. Several commenters suggested that the SDT remove all references to applicable assets in requirements and rely on the applicability column only to specify the Cyber Assets that are in scope. The SDT agrees. Wherever possible, the requirements have been streamlined to only reference applicable Cyber Assets within the applicability column.

Some commenters stated that the rationale for CIP-011 Requirement R1 was incomplete as originally posted. On May 8, 2012, NERC was alerted that the text contained in the rationale box for Requirement R1 of CIP-011-1 appeared to be incomplete. NERC corrected this by issuing revised language that modified the text box size to display all of the text.

Some commenters recommended that entities should define their own info protection program. They suggested that compliance would be evaluated based on how the entity complied with their defined programs. The SDT discussed this comment, but disagrees. The SDT believes it would be doing the industry a disservice to leave the process completely up to the entity. As part of its change, the SDT seeks to clarify what is required to meet compliance. The SDT believes that if the requirements are not defined or entity defined, NERC will be forced to issue Compliance Application Notices in the future to provide clarity, and auditors will be forced to inject their own audit measurements. In the interest of providing clarity, the SDT believes it is important to provide a consistent threshold for compliance.

The SDT received comments asking that the team revert to legacy language used in previous versions of the CIP standards (V1 and V3). SDT considered this request, but believes that many entities have made good suggestions, which improve legacy language. Legacy language will be utilized in all cases where it is appropriate for the purposes of minimizing changes that the registered entities must make to their ongoing programs.

CIP-011 Requirement R1 calls for each Responsible Entity to implement an information protection program that includes applicable items, and Requirement R1.1 requires methods to identify such information. Many entities commented that Requirement R1.1 was too vague. In fact, several entities indicated they were confused as to whether the requirement

called for determining what information should be protected or if the requirement mandated labeling of the information. Some entities asked if specific classification was required. A few entities suggested that a specific classification, such as "confidential," should be included in the requirement. The SDT has considered this but does not believe it is appropriate to dictate a specific classification, such as "confidential." Some entities may use other classifications such as "CIP-Confidential," "Non-Public," "Highly Confidential," or many other designations. It is not the intent of the SDT to force all Registered Entities to modify their compliance documentation by mandating specific classifications. This initial part of the information protection program simply requires that the information in scope and to be protected is identified in some manner. Specific classification of information may be used as a method for identification, but is not specifically required. One commenter provided a specific recommendation to clarify that the information to be identified is that which is explained in the definition of BES Cyber System Information. The SDT agrees with this comment. The SDT is also responsive to industry comments and has enhanced the measures section of Requirement R1.

Some entities pointed out that the word "implemented" is unnecessary in the Requirement R1.1 requirement because it is contained in the overall Requirement R1 requirement language. They asked that the word "implement" be removed from Requirement R1.1 because it was redundant. Other entities stated that documentation is for measures or evidence, and the word "documented" should be removed from Requirement R1.1 requirement. The SDT has removed both "implemented" and "documented" from the requirement language. The term documented has been moved to the measures section.

There were additional comments related to the measures for Requirement R1.1. Some commenters asked how a repository could be a measure, and others asked for additional clarity. A repository could be a measure if the entity designated the repository or a section of the repository as the location for identifying and housing BES Cyber System Information and explained the protections afforded by the repository in the entity's Information Protection Program. It would be up to the entity to explain in their information protection program how the repository was used to identify their BES Cyber System Information.

In CIP-011 Requirement R1.2, many commenters again asked that additional clarification be added to the requirement concerning procedures for handling of BES Cyber System Information. The SDT agrees and has modified the requirement to clarify that handling procedures required are those which explain how the BES Cyber System Information is protected and secured.

Several comments asked for additional specifics concerning several topics regarding BES Cyber System Information; including transit, handling, and transmittal. The SDT agrees with this. The guidance section has been greatly expanded to address the topics requested.

Several entities desired additional specifics concerning the measures for Requirement R1.2. One entity commented: "This measure does not specify what records could be used …would sampling work in this case, and if so, what is the acceptable tolerance range for such sampling?" The SDT disagrees that it would serve the industry to mandate this level of specifics within CIP-011. It is the SDTs intent that the entities document their information protection program and associated procedures in accordance with the CIP-011 requirements, and that the entity maintains records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented program and associated procedures. A measure has been added which specifies this intent.

There were several comments requesting that the SDT address third party handling of BES Cyber System Information. The SDT agrees with this comment. Additional information has been added to guidance to cover this topic.

There were comments asking for more specifics concerning the topics of transit, handling, transmittal, distribution, physical access, purge, use, and disposal. The guidance section has been significantly enhanced to address the topics for which additional direction is warranted.

Some commenters recommended including procedures for reuse and disposal within Requirement R1. The SDT does not agree. SDT believes that the topic of reuse and disposal is complex and requires the specifics currently afforded the topic as specified in Requirement R2. If the topic was included in the Requirement R1 procedures, it could result in double jeopardy during audits, as auditors review compliance with Requirement R1 procedures and Requirement R2 handling during reuse and disposal.

Commenters stated that the reference to prior version under Requirement R1.2 refers to CIP-003-3, Requirement R5.3. They recommended that the reference be moved to Requirement R1.3. The SDT agrees.

The SDT received many comments related to Requirement R1.3. Many commenters recommended that the team specify that deficiencies found in the annual assessment should not be considered violations or potential violations. Some commenters asked that the SDT specify which deficiencies would be considered violations and which would not be considered violations. Commenters asked that the word "deficiencies" be changed to "lessons learned" or "flaws." The

SDT notes that the word “deficiencies” is appropriate because a deficiency notes there is a lack of completeness or insufficiency exists.

Some asked that the entire requirement be handled under the NERC FFT program and eliminated from the requirements. It is not up to the SDT to make the determination as to what is and what is not a violation. The SDT sought guidance from NERC and regional audit staff. The audit staff advised that some deficiencies could be seen as self-reportable violations or potential violations during audit if the entity failed to adhere to one of the specified sub-requirements. Other deficiencies might simply be process improvements or opportunities for improvements that do not violate any BES Cyber System Information sub-requirement from CIP-011. Further, the requirement calls for a periodic “assessment,” and such “assessment” may reveal things that went well in addition to things that could be improved. After considering industry comments and consulting with audit and NERC staff, the requirement will be handled under the Paragraph 81 project from the FERC Order on the find, fix, track and report process.

Some commenters did not like the grouping of all access control requirements within CIP 004. They asked that the requirement parts dealing with access to information be moved into CIP-011. This was discussed among the SDT. It was decided that the majority of entities favored the grouping of all access control within CIP 004. For consistency and in response to many previous comments, all access control requirements have been grouped into CIP 004. The requirement parts dealing with access control for BES Cyber System Information have, therefore, not been moved into CIP-011.

Some commenters asked where specifically the process covering reuse and disposal is required. Requirement R2 states: “Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal.” Therefore, Requirement R2 requires the entity to define their process concerning the topics within Requirement R2.

The SDT received comments questioning a discrepancy between the types of systems referenced in the definition of BES Cyber System Information vs. the applicability column for Requirement R2. Associated Protected Cyber Assets is included in the applicability column, but is not specifically referenced in the definition. The SDT’s intent is that if BES Cyber System Information as defined in the standard exists in the data storage media of applicable Cyber Assets, then Requirement R2 applies.

One commenter pointed out that the component obligations under CIP-011-1 are not clear and that the table headers under Requirement R2 may be adding to the confusion, as they are different for Requirements R2.1 and for R2.2. The SDT agrees and has corrected the table headers so that they are consistent within Requirement R2.

The second paragraph in Requirements R2.1 and R2.2 that deal with removal of the device from the PSP generated many comments. Some commenters asked that the language concerning removal from the PSP be clarified. Others asked that the language be moved to a separate part. Others stated that the language adds no value and asked that the language concerning removal from the PSP be deleted from the requirement part altogether. A few commenters suggested simplified language, and such comments were very much appreciated. The SDT has decided to remove from the requirement language dealing with removal from the PSP. The SDT will address the topic of removal from the PSP within the guidance section. The SDT made corresponding changes to the measures section.

Many commenters objected to use of the term "chain of custody" in Requirements R2.1 and R2.2. They stated that this is a legal term, and they believe it is not appropriate in the CIP standards. Others commented that the intended use of the term "who has possession," as used in the requirement, was unclear. The SDT has decided to remove the entire second paragraph from Requirements R2.1 and R2.2, including the reference to "chain of custody." The SDT made corresponding changes to the measures section and any reference to terms such as "chain of custody" has been removed from the measures section, as well.

Some commenters recommended combining Requirements R2.1 and R2.2 into one requirement part. The SDT disagrees with this recommendation. SDT believes there are sufficient differences in the handling of release for reuse versus disposal to warrant retaining both Requirement R2.1 and Requirement R2.2.

Within the Requirement R2.1 language, some commenters asked for additional clarity concerning the exception, which provides for reuse within other high impact or medium impact BES Cyber Systems. The SDT agrees with this comment and has added additional clarity to the guidance language specifying that the re-use exception applies to re-use in other systems that are identified in the applicable systems column as protections will continue after re-use.

The SDT received comments asking that "BES" be inserted in front of "Cyber Assets" within the reference to "applicable Cyber Assets that contain BES Cyber System Information…" within Requirements R2.1 and R2.2. The SDT disagrees with this direction. The requirement parts are applicable to Associated Physical Access Control Systems, Associated Electronic

Access Control or Monitoring Systems, and Associated Protected Cyber Assets. Therefore, the scope of Cyber Assets which may contain BES Cyber System Information is larger than the suggested term "BES Cyber Assets."

The SDT received at least one comment stating that it was unclear if Requirement R2.2 meant the storage media within the Cyber Asset, or if it also includes backup media. The requirement states: "Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media." The SDT's intent is that the scope includes the Cyber Asset data storage media. The scope of this requirement is not far reaching to include all possible locations of downstream information, such as backup copies outside the Cyber Asset. However, such copies of BES Cyber System Information would be governed by Requirement R1.

Some entities also asked for additional specifics concerning the actions a Responsible Entity shall take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media. One commenter questioned whether an attestation was specifically mandated. An attestation is not required by the standard. It is not the intent of the SDT to mandate specific actions within the requirements. However, the guidance section has been greatly expanded with guidance taken from NIST SP800-88, which provides additional assistance to entities.

One entity stated that it is not clear if requirement parts 2.1 and 2.2 permit media to be removed and possibly replaced with clean media, with the Cyber Asset then being redeployed or disposed of while the removed media continues to be maintained until separate erasure or destruction. The SDT considered this question and believes that the answer is: Yes, such actions would be permitted. The requirement calls for the entity to "take action to prevent unauthorized retrieval." This provides flexibility for the entity. As long as the entity documented the actions that they undertook; i.e., removing the media, securing the media, sanitizing the media in accord with the requirements, such action should be permitted.

SDT received the following comment: requirement part 2.1 appears to be two requirements and should be broken out if that is the intent. The current wording appears to pertain to cyber assets that contain BES Cyber System Information (i.e., network diagram). The second sentence appears to pertain to Cyber Assets within an ESP. There were other commenters asking for clarity concerning the storage media and the targets for sanitation in Requirement R2. Requirement R2 applies to any information within the Cyber Asset data storage media that meets the definition of BES Cyber System Information.

A few commenters stated that the standard needs to track the media and not necessarily the Cyber Asset the media is associated with. The SDT agrees with this comment. The Requirement R2 language has been modified to include the reference to "data storage media."

VSLs and VRFs

The SDT received at least one comment asking that the VRF for Requirement R1 be lowered. The SDT disagrees with the industry comment. The VRF for Requirement R1 is Medium in keeping with the FERC approved current VRF for this requirement. The VRF for Requirement R2 is already lower.

One commenter asked that the SDT add the "part" reference to the VSL so that the reader could easily understand the requirement number to which the VSL referred. The SDT agrees with this comment, and added the references to the VSL's.

Multiple commenters objected to the "zero defect" approach to VSL's for Requirement R2. The SDT agrees. The previously posted Requirement R2 VSLs have been modified to be less "device" specific. In the future, there will be additional emphasis on the entity providing good processes and security controls.

One commenter provided specific language for VSL's. Corresponding to recommendations that had been made concerning requirements, they asked that the VSLs should be revised to: Severe-not implemented, Higher-not measuring to detect, Moderate-not correcting detected flaws, Lower-not considering prevention. However, the requirement does not address prevention, and the VSLs must correspond to the requirements.

NERC will be sharing additional information on VRFs and VSLs in keeping with NERC's implementation of the FFT program.

Questions with Votes Only:

CIP-008, CIP-009, CIP-010 and CIP-011 Questions: Question 1

1. **CIP-008-5 R1 states "Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?**

Organization	Yes or No
Northeast Power Coordinating Council	No
Duke Energy	No
NESCOR/NESCO	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
PNM Resources	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No

Organization	Yes or No
NIPSCO	No
Xcel Energy	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Springfield Utility Board	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No

Organization	Yes or No
Kansas City Power & Light	No
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes

Organization	Yes or No
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes

Organization	Yes or No
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes

Organization	Yes or No
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
California Independent System Operator	Yes

2. **CIP-008-5 R2 states "Each Responsible Entity shall implement its documented Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?**

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
ACES Power Marketing	No
PNM Resources	No
Dairyland Power Cooperative	No

Organization	Yes or No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Lakeland Electric	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No

Organization	Yes or No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes

Organization	Yes or No
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes

Organization	Yes or No
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes

Organization	Yes or No
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Springfield Utility Board	Yes

Organization	Yes or No
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
California Independent System Operator	Yes

3. CIP-008-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
PPL Corporation NERC Registered Affiliates	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
ACES Power Marketing	No
PNM Resources	No
Progress Energy	No
CenterPoint Energy	No

Organization	Yes or No
Hydro One	No
Lakeland Electric	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Springfield Utility Board	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
MRO NSRF	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review	Yes

Organization	Yes or No
Committee	
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes

Organization	Yes or No
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes

Organization	Yes or No
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Nebraska Public Power District	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
Pacific Gas and Electric Company	Yes

Organization	Yes or No
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Kansas City Power & Light	Yes
California Independent System Operator	Yes

5. CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
PPL Corporation NERC Registered Affiliates	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No

Organization	Yes or No
Florida Municipal Power Agency	No
SMUD & BANC	No
ACES Power Marketing	No
PNM Resources	No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
NIPSCO	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
Lincoln Electric System	No
Lakeland Electric	No

Organization	Yes or No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
Utility Services Inc.	No

Organization	Yes or No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
NYISO	No
Farmington Electric Utility System	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Pepco Holdings Inc & Affiliates	Yes

Organization	Yes or No
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces	Yes

Organization	Yes or No
Corporation	
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes

Organization	Yes or No
PSEG	Yes
Liberty Electric Power, LLC	Yes
MEAG Power	Yes
Portland General Electric	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

6. CIP-009-5 R2 states "Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
MRO NSRF	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
SMUD & BANC	No
Puget Sound Energy, Inc.	No
PNM Resources	No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
Progress Energy	No

Organization	Yes or No
Hydro One	No
Independent Electricity System Operator	No
Lincoln Electric System	No
Bonneville Power Administration	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Alliant Energy	No
NYISO	No
Exelon Corporation and its affiliates	No
Los Angeles Department of Water and Power	No
California Independent System Operator	No
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
FirstEnergy	Yes

Organization	Yes or No
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes

Organization	Yes or No
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes

Organization	Yes or No
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
Oncor Electric Delivery Company LLC	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes

Organization	Yes or No
Utility Services Inc.	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes

7. **CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?**

Summary Consideration:

Organization	Yes or No
NRG Energy Companies	No
PPL Corporation NERC Registered Affiliates	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
SMUD & BANC	No
PNM Resources	No
Arizona Public Service Company	No
Progress Energy	No
Hydro One	No
Tampa Electric Company	No

Organization	Yes or No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
City of Austin dba Austin Energy	No
Oncor Electric Delivery Company LLC	No
CenterPoint Energy	No
Xcel Energy	No
New York Power Authority	No
MidAmerican Energy Company	No
PJM Interconnection	No
ISO New England Inc.	No
ACES Power Marketing	No
Puget Sound Energy, Inc.	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Brazos Electric Power Cooperative	No
IRC Standards Review Committee	Yes
The united illuminating Company	Yes
Lakeland Electric	Yes
Southern California Edison Company	Yes
Clallam County PUD No.1	Yes

Organization	Yes or No
Northeast Utilities	Yes
Portland General Electric	Yes
MRO NSRF	Yes
NESCOR/NESCO	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
Comment Development SME list	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes

Organization	Yes or No
Western Area Power Administration	Yes
Dairyland Power Cooperative	Yes
Tri-State G&T - Transmission	Yes
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes

Organization	Yes or No
National Grid	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
MEAG Power	Yes
Utility Services Inc.	Yes

Organization	Yes or No
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Kansas City Power & Light	Yes
California Independent System Operator	Yes
Luminant	
American Transmission Company, LLC	
Avista	

9. CIP-010-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
FirstEnergy	No
SMUD & BANC	No
ACES Power Marketing	No
PNM Resources	No

Organization	Yes or No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
Lower Colorado River Authority	No
LCRA Transmission Serivces Corporation	No
Hydro-Quebec TransEnergie	No
Lincoln Electric System	No
The united illuminating Company	No
Tampa Electric Company	No

Organization	Yes or No
MidAmerican Energy Company	No
NV Energy	No
Massachusetts Municipal Wholesale Electric Company	No
Detroit Edison Company	No
The Empire District Electric Company	No
Ameren	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No

Organization	Yes or No
Utility Services Inc.	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
Springfield Utility Board	No
NYISO	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
PPL Corporation NERC Registered Affiliates	Yes
Associated Electric	Yes

Organization	Yes or No
Cooperative, Inc. (NCR01177, JRO00088)	
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes

Organization	Yes or No
MEAG Power	Yes
Portland General Electric	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

10. CIP-010-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
MRO NSRF	No
NESCOR/NESCO	No
SMUD & BANC	No
ACES Power Marketing	No
PNM Resources	No
Southern Company Services, Inc.	No
Western Area Power Administration	No

Organization	Yes or No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
ATCO Electric	No
Hydro-Quebec TransEnergie	No
Lincoln Electric System	No
The united illuminating Company	No
Bonneville Power Administration	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy	No

Organization	Yes or No
Company	
Detroit Edison Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Electric Power Company	No
Alliant Energy	No
Springfield Utility Board	No
NYISO	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No

Organization	Yes or No
California Independent System Operator	No
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes

Organization	Yes or No
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Serivces Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes

Organization	Yes or No
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

11. CIP-010-1 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
IRC Standards Review Committee	No
PNM Resources	No
Southern Company Services, Inc.	No

Organization	Yes or No
Western Area Power Administration	No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Consumers Energy Company	No
Lincoln Electric System	No
The united illuminating Company	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy	No

Organization	Yes or No
Company	
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
Springfield Utility Board	No

Organization	Yes or No
NYISO	No
Exelon Corporation and its affiliates	No
Los Angeles Department of Water and Power	No
Kansas City Power & Light	No
California Independent System Operator	No
PPL Corporation NERC Registered Affiliates	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes

Organization	Yes or No
SPP and Member companies	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Niagara Mohawk (dba National Grid)	Yes

Organization	Yes or No
National Grid	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
MEAG Power	Yes

Organization	Yes or No
Portland General Electric	Yes
Utility Services Inc.	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes

13. CIP-011-1 R1 states "Each Responsible Entity shall implement an information protection program that includes each of the applicable items in CIP-011-1 Table R1 – Information Protection." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
PNM Resources	No
National Rural Electric Cooperative Association (NRECA)	No
Progress Energy	No
CenterPoint Energy	No

Organization	Yes or No
Tri-State G&T - Transmission	No
Xcel Energy	No
Snohomish County PUD	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
PSEG	No
Liberty Electric Power, LLC	No
Texas Reliability Entity	No
PJM Interconnection	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Exelon Corporation and its affiliates	No
Deseret Power	No
Kansas City Power & Light	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes

Organization	Yes or No
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes

Organization	Yes or No
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power	Yes

Organization	Yes or No
Administration	
Lakeland Electric	Yes
Tampa Electric Company	Yes
New York Power Authority	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
Nebraska Public Power District	Yes
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes

Organization	Yes or No
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
California Independent System Operator	Yes

14. CIP-011-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
ACES Power Marketing	No
PNM Resources	No
Southern Company Services, Inc.	No
Progress Energy	No
Tri-State G&T - Transmission	No

Organization	Yes or No
Hydro One	No
Independent Electricity System Operator	No
The united illuminating Company	No
Xcel Energy	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
Ameren	No
NextEra Energy, Inc.	No
Liberty Electric Power, LLC	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery	No

Organization	Yes or No
Company LLC	
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Pacific Gas and Electric Company	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes

Organization	Yes or No
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes

Organization	Yes or No
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes

Organization	Yes or No
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards
Comment Form D
Definitions and Implementation Plans

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Index to Questions, Comments, and Responses

Questions with Summaries Included: 15

QUESTION D8 – DEFINITIONS: 15

QUESTION D9 – DEFINITIONS: 19

QUESTION D10 – DEFINITIONS: 22

QUESTION D11 – DEFINITIONS: 25

QUESTION D12 – DEFINITIONS: 27

QUESTION D13 – DEFINITIONS: 30

QUESTION D14 – DEFINITIONS: 35

QUESTION D16 – IMPLEMENTATION PLAN: 38

QUESTION D17 – DEFINITIONS AND IMPLEMENTATION PLAN: 42

Questions with Votes Only: 51

1. Do you agree with the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset? 51

2. Do you agree with the proposed definition of Control Center? 57

3. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager? 64

4. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager? 71

5. Do you agree with the proposed definitions of Electronic Access Control or Monitoring Systems, Interactive Remote Access, and Intermediate Device? 78

6. Do you agree with the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset? 85

7. Do you agree with the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident? 92

15. Do you agree with the changes made to the proposed implementation plan since the last formal comment period? 99

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Bruce Metruck	New York Power Authority	NPCC	6
12.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
13.	Robert Pellegrini	The United Illuminating Company	NPCC	1
14.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
15.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
16.	Brian Robinson	Utility Services	NPCC	8
17.	Michael Jones	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Don Weaver	New Brunswick System Operator	NPCC	2
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3
24.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5

2.	Group	Annabelle Lee	NESCOR/NESCO									

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3.	Group	Jason Marshall	ACES Power Marketing					X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Tim Soles	Occidental Power Services, Inc.	ERCOT 3										
4.	Andy Gallo	Austin Energy	ERCOT 1										
5.	Andy Gallo	Austin Energy	ERCOT 3										
6.	Andy Gallo	Austin Energy	ERCOT 4										
7.	Andy Gallo	Austin Energy	ERCOT 5										
8.	Andy Gallo	Austin Energy	ERCOT 6										
8.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8. Annie Terracciano	Northern Lights Inc.	WECC 3										
9. Aleka Scott	PNGC	WECC 4										
10. Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11. Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12. Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13. Margaret Ryan	PNGC	WECC 8										
12. Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13. Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14. Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3. M & A Electric Power Cooperative			SERC 1, 3										
4. Northeast Missouri Electric Power Cooperative			SERC 1, 3										
5. N.W. Electric Power Cooperative, Inc.			SERC 1, 3										
6. Sho-Me Power Electric Cooperative			SERC 1, 3										
15.	Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X						
Additional Member		Additional Organization	Region Segment Selection										
1. Oglethorpe Power Corporation			SERC 5										
2. Georgia Transmission Corporation			SERC 1										
16.	Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X
Additional Member		Additional Organization	Region Segment Selection										
1. MAHMOOD SAFI		OPPD	MRO 1, 3, 5, 6										
2. CHUCK LAWERENCE		ATC	MRO 1										
3. TOM WEBB		WPS	MRO 3, 4, 5, 6										
4. JODI JENSON		WAPA	MRO 1, 6										
5. KEN GOLDSMITH		ALTW	MRO 4										
6. DAVE RUDOLPH		BEPC	MRO 1, 3, 5, 6										
7. JOE DEPOORTER		MGE	MRO 3, 4, 5, 6										
8. SCOTT NICKELS		RPU	MRO 4										
9. TERRY HARBOUR		MEC	MRO 1, 3, 5, 6										
10. MARIE KNOX		MISO	MRO 2										
11. LEE KITTELSON		OTP	MRO 1, 3, 4, 5										
12. SCOTT BOS		MPW	MRO 6, 1, 3, 5										
13. TONY EDDLEMAN		NPPD	MRO 1, 3, 5										
14. THERESA ALLARD		MPC	MRO 1, 3, 5, 6										
17.	Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing													
18.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				
Additional Member		Additional Organization	Region Segment Selection										
1. Timothy Beyrle		City of New Smyrna Beach	FRCC 4										
2. James Howard		Lakeland Electric	FRCC 3										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3. Greg Woessner	Kissimmee Utility Authority	FRCC	3										
4. Lynne Mila	City of Clewiston	FRCC	3										
5. Joe Stonecipher	Beaches Energy Services	FRCC	1										
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4										
7. Randy Hahn	Ocala Utility Services	FRCC	3										
19. Group	Joseph DePoorter	Madison Gas and Electric Company				X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Darl Shimko	MGE	MRO	3										
2. Joseph DePoorter	MGE	MRO	4										
3. Steve Schultz	MGE	MRO	5										
4. Jeff Keebler	MGE	MRO	6										
20. Group	David Thorne	Pepco Holdings Inc & Affiliates		X		X							
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Mark Jones	Pepco	RFC	1										
21. Group	Rick Terrill	Luminant						X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Mike Laney	Luminant Generation Company LLC	ERCOT	5										
2. Tim Soles	Occidental Power Services, Inc.	ERCOT	6										
3. Tim Soles	Occidental Power Services, Inc.	ERCOT	3										
4. Andy Gallo	Austin Energy	ERCOT	1										
5. Andy Gallo	Austin Energy	ERCOT	3										
6. Andy Gallo	Austin Energy	ERCOT	4										
7. Andy Gallo	Austin Energy	ERCOT	5										
8. Andy Gallo	Austin Energy	ERCOT	6										
9. Brenda Hampton	Luminant Energy Company LLC												
22. Group	Joe Tarantino	SMUD & BANC		X		X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Kevin Smith	BANC	WECC	1										
23. Group	Scott Brame	NCEMC		X				X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Rayburn Country Electric Cooperative			SPP										
2. Empire District Electric			SPP	1									
3. City Utilities of Springfield			SPP	4									
4. Westar Energy			SPP	1, 3, 5, 6									
5. Cleco Power			SPP	1, 3, 5, 6									
25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Pawel Krupa			WECC	1									
2. Dana Wheelock			WECC	3									
3. Hao Li			WECC	4									
27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Denise Lietz		Puget Sound Energy	WECC	1									
2. Erin Apperson		Puget Sound Energy	WECC	3									
28.	Group	Michael Mertz	PNM Resources	X		X							
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Laurie Williams		Public Service Co. of New Mexico	WECC	1									
2. Michael Mertz		Public Service Co. of New Mexico	WECC	3									
29.	Group	Sasa Maljukan	Hydro One	X									
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. David Kiguel		Hydro One	NPCC	1									
30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION D8 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the SDT modified some of the definitions. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity. Please see the redlined version of the definitions for a complete set of revisions to each definition.

BES Cyber Asset

Several commenters stated that the definition of BES Cyber Asset was confusing, citing the complex construction of the definition and the fact that it stated that each BES Cyber Asset must be part of a BES Cyber System while the background and technical basis stated that Responsible Entities had flexibility in using BES Cyber Asset or BES Cyber Systems. Many provided alternative language. Multiple commenters asked whether there is a need for network connectivity between BES Cyber Assets to be considered a BES Cyber System. The SDT made the addition of the statement about each being part of at least one BES Cyber System to the definition of BES Cyber Asset to ensure that each Cyber Asset would be included in at least one BES Cyber System, and did not preclude the option of having a BES Cyber System that consists of a single BES Cyber Asset. The SDT believes this preserves entities' flexibility while providing better homogeneity in the application of requirements: requirements uniformly apply to BES Cyber Systems. There is no presumption of connectivity options in the definition of a BES Cyber System, but Responsible Entities may find that application of requirements and relationship with other definitions such as ESPs may be significant input to the Responsible Entities' options.

Several commenters suggested that the definition of BES Cyber Asset include an addition in its qualification for connection to a network within an ESP in addition to connection to a Cyber Asset within an ESP. The SDT believes that the clarification is useful in ensuring the application to those transient cyber assets that are connected to the network as well as directly to the Cyber Assets within an ESP and has made the modification to address the comment.

One commenter suggested modifications to definitions of Cyber Asset. The SDT considered these comments and does not believe that these suggestions are substantively different or would add clarity to the definitions.

One commenter suggested dropping the word “misused” from the definition of BES Cyber Asset. The SDT has specifically included the word “misuse” in response to comments from FERC Order 706 and believes that it includes intent of a malicious compromise that is not otherwise conveyed.

Mid-American’s comment with respect to the use of the capitalized term “Systems” has been addressed and the definition now used the more generic term “systems” instead of the defined term.

One comment was on the use of the verb phrase “affect the reliable operation…” The SDT considered these comments and believes that this verb phrase is appropriate as it applies to the Facilities, systems and equipment, not the BES Cyber System.

Many commented on the complexity of the parenthetical sentence in the definition of BES Cyber Asset and suggested alternative language: the SDT considered these comments and believes that the suggested alternatives do not add additional clarity to the definition. In addition, other commenters stated that the parenthetical qualification should be used in defining the term Transient Cyber Asset. The SDT considered the options and chose to not have a separately defined term because of the very small number of requirements where it is used.

Many entities commented on the use of “adversely impact” in the definition of BES Cyber Asset and suggested using the defined term “Adverse Reliability Impact” instead. The SDT considered the use of the defined term and believes that the defined term describes an impact which is much more severe than the intent of the term used in the definition.

Several commenters requested clarification of the terms “within 15 minutes”: the SDT has included additional clarification in the guidelines and technical basis section.

–One commenter suggested to remove the 15 minute criteria as it is believed that it will lower the security of assets by removing them from qualifications. In response, The SDT notes that, in using 15 minutes, it is attempting to articulate a time boundary for “Real-time” impact. The term “Real-time” in the Glossary of Terms used in NERC Reliability Standards did not provide enough specificity in the definition for this purpose. The SDT scoped the CIP standards to those Cyber Assets that would have an effect on Real-time operations.

Many entities commented on the qualification on "redundancy" in the definition of BES Cyber Asset. The SDT believes that the impact of a cyber asset on the function of a given Facility, system or equipment is independent on whether that Facility, system or equipment is redundant or not: in most cases, the redundancy is configured to handle loss of a Facility, but does not consider degradation or misuse of that Facility, system or equipment. The application guidelines and technical basis section contains a discussion of this concept.

One entity suggests that the definition of BES Cyber Asset is much improved still does not prescribe how to document that an asset has been connected to the BES for less than 30 days. It is not the purpose of the definition to prescribe methods of documentation. That flexibility is left to the entity. Assets connected on a transient, temporary basis are not intended to be a BES Cyber Asset, and the 30 days in the definition is intended to clarify that temporary connections, e.g., for maintenance purposes, are not intended to be included within the definition.

BES Cyber Systems

One commenter suggested replacing "to perform" with "used to facilitate the performance of…", citing examples where the BES Cyber System may not directly perform a reliability function, but may support one or more functions. The SDT believes that the introduction of the proposed language would result in further questions on the meaning of the word "facilitate" and the extent of the scope of that term.

In response to a suggestion to use the word "identified for functions…" the SDT believes that the suggested wording did not bring additional clarity to the definition of BES Cyber Systems.

One commenter stated that the use of the term "Responsible Entity" is confusing, citing overlap, redundancy or conflict with the term Functional Entity. The SDT believes that these are two distinctly different terms: the Responsible Entity refers to the set of Functional Entities that is responsible for compliance to the requirements of the standard. Within a given standard, a given set of requirements may apply to different Functional Entities, depending on the specific requirements. The term "responsible entity" is defined in the applicability section. The application of the defined term that contains the term "responsible entity" in a standard is subject to the preamble in Section 4.

Cyber Asset

Multiple comments were provided on the use of the word "programmable" in the definition of Cyber Asset, citing that it was too broad, and the need for a routable connectivity qualification. The SDT considered these comments and notes

that the definition of Cyber Asset as it pertains to "programmable electronic devices" is part of the current approved definition. The SDT further believes that consideration of connectivity in this generic definition is inappropriate.

One commenter stated that the qualification of "…data in these devices…" ignores data in motion. The SDT believes that the inclusion of data other than that in these devices has unintended consequences in the application of requirements.

Other

Multiple commenters suggested the addition of a defined term BES Site, or similar concepts: the SDT has considered the rationale and has opted to use the concepts in the drafting of new language and approach in the requirement language and attachments, instead of defining a term that would be used in only a few requirements.

One commenter requested that the language for the defined term Protected Cyber Asset be reviewed for clarity. The SDT has reviewed the definition and made modifications to the definition and added guidance in the background section to clarify the concept.

QUESTION D9 – DEFINITIONS:

Do you have any comments on the changes to the proposed definition of Control Center? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the SDT modified all of the definitions based on stakeholder comments. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity. Please see the redlined version of the definitions for a complete set of revisions to each definition.

Many commenters questioned the need for a definition of Control Center, citing standards in other reliability standards that also have control center applicability without the need for a formal definition. The SDT notes that the Control Center is subject to a number of High and Medium Impact criteria and that they host a large number of BES Cyber Systems that are essential to the reliable operation of the BES. The SDT believes that, because of these necessarily crucial functions, a formal definition is appropriate to clearly define the scope of applicability, as demonstrated by many questions on differentiation between a facility's control room, which is typically considered part of the facility, and Control Centers, which are considered separate facilities hosting operating personnel controlling and monitoring multiple facilities. Many commented that a formal definition used in the CIP context could be confusing to the industry in the context of other reliability standards that apply to control centers. The SDT believes that a formal definition clarifies the scope of applicability for Control Centers and would not affect other reliability standards that have not used the defined term, but rather a "common" undefined term for control center. NERC's standard use of capitalized terms for NERC Glossary defined terms provides clarity on when the defined term is used.

Two commenters proposed alternative language for the definition of the Control Center that uses Functional Entities. The SDT has considered the alternatives and believes that the proposals contain a circular reference that would not provide better clarity. The SDT has carefully considered the current proposed language and believes that it accurately describes the intended target of applicability.

Others suggested that Control Centers that use voice or manual instructions be categorized as Low Impact. The SDT notes that Cyber Systems that provide information to Control Center operators that use manual or voice to effect control operations on BES assets in real-time based on that information must be subject to the same protection as those that

trigger automated operation. If the communication or manual operation results from information provided for real-time operations, there is no rationale for categorizing them as a lower impact.

Multiple commenters expressed concern that in certain instances, a facility may not be performing the function of a TOP 24/7 and remains unmanned the rest of the time, and suggested the addition of the 24/7 qualification. The SDT sees no rationale in adding this qualifier, since the impact of the facility that performs these functions remains the same. In the same comment, commenters cited the case of a TOP registration for a single facility. The SDT responds that the "control and monitoring" facility of a single facility does not meet the definition of a Control Center, but rather as part of the facility it is controlling.

Several commenters suggested slightly modified language which focuses on hosted BES Cyber Systems rather than operating personnel. One commenter suggested that the Control Center is the BES Cyber System that performs these functions. The SDT believes that operating personnel is central to the traditional understanding of a Control Center facility. The definition currently specifies one or several facilities. In the facilities (or site) based approach, the identification of the BES Cyber Systems that perform the Control Center functions may bring in other facilities such as data centers that perform these functions.

Many commenters requested clarifications on the terms "facility" and "locations" used in the definition of the Control Center. The SDT uses the general term "facility" (as opposed to the glossary term "Facility") in its generic sense of one or several physical structures that comprise a Transmission substation or station, a generating plant or a Control Center. In the case of a Control Center, a facility could be considered a building or campus consisting of several closely located buildings. However, additional facilities may be brought in as the BES Cyber Systems are defined, including associated data centers that perform the reliability tasks. In the context of the definition of Control Center, a location generally refers to the set of BES Facilities at a single site, and generally constitutes a single point of connection to the BES. Because of the many types of configurations, the SDT used the generally accepted concept of geographic location rather than including all the nuances of the different ways Facilities are connected to the BES.

One commenter requested a definition for data center. The SDT believes that "data center" is a well understood term and that many definitions of data center exist elsewhere that adequately explain what they are.

One commenter pointed out that the SDT uses the term reliability functional tasks and reliability tasks interchangeably in the standard. The SDT has used the terms interchangeably for the reliability tasks defined in the NERC functional model. The SDT has made the change in the definition of Control Center to be consistent to the use of reliability tasks elsewhere.

One commenter requested further qualification of the term “operating personnel”. The SDT notes that this term is used in many reliability standards, in particular, the PER series of standards. They are used to refer to personnel that perform the real-time control and monitoring operations necessary for the real-time functions for RC, BA, TOP and GOP functional entities. The definition of the Control Center refers to these functions.

One commenter suggested the addition of “NERC Certified” to operating personnel. The SDT notes that the addition of the term NERC Certified restricts the applicability of the term to just RCs, BAs and TOPs, since there is no requirement for certification of GOP operating personnel. This is not the intent of the SDT in drafting this definition.

One commenter suggested that Control Center as it applies to the function of a Generation Operator has a threshold of generation located at two or more locations, and that this single qualifier could unintentionally sweep in the control centers for multi-location generation of very small capacity. The commenter suggested that a capacity qualifier be added to this definition. The SDT does not think that the threshold should be in the definition, but has amended the criterion for generation Control Centers in the Medium Impact category that addresses this comment. BES Cyber Systems for Control Centers below the Medium Impact threshold must still be protected as Low Impact. See the response to A03 - Attachment 1, Medium Impact.

QUESTION D10 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the comments related to these definitions largely noted minor improvements to the definitions rather than identifying major issues or disagreement.

BES Cyber System Information

Several comments about the definition of BES Cyber System Information highlighted minor issues with the structure of the definition rather than its content. Commenters suggested re-organizing the definition such that the list of examples came last. The SDT considered this comment and agreed that it made the definition more readable without changing its overall intent. This suggestion has the effect of collecting the explanatory language together to improve comprehension of the definition. Some commenters suggested that the examples should be removed from the definition altogether. The SDT noted that it is not uncommon to find examples in definitions in the NERC Glossary of Terms Used in NERC Reliability Standards (e.g. Facility, Operating Plan, Year One, etc.). Additionally, the SDT had concerns about removing the list of examples, since a similar list of examples has been used since the version 1 CIP Standard to provide direction as to what information should be included in the NERC CIP information protection program. The SDT believed that continuing to provide a list of examples would facilitate a transition between Version 3 and 4 of the CIP standards to Version 5.

Additionally, some commenters took issue with the phrase "developed by the Responsible Entity" as it relates to security procedures and security information. The commenters noted that protection of security information might be appropriate even if this information was developed by an outside party. The SDT agrees with this comment. The intent of the SDT was to prevent the inclusion of information that might be publicly available. Therefore, the SDT has modified the definition to better align with the intent and has clarified that security procedures and security information "not publicly available" are examples of BES Cyber System Information.

Some commenters noted ambiguity in the definition of BES Cyber System Information in the phrase "unauthorized distribution" of information. The SDT appreciates the concern over ambiguity, but encourages the industry to consider this definition in context of the overall information security program that is required under NERC CIP-011-1 and related

requirements in NERC CIP-004-5. Consideration of "unauthorized distribution" should be taken in the context that access to locations where information that has been judged to meet this definition is stored is required to be authorized in CIP-004-5 R4, part 4.1, element 4.1.3 and proper handling of this information is required in CIP-011-1 R1, part 1.2. The Responsible Entity should use this context to determine whether this information, in the hands of someone who has not been granted access "based on need," could lead to a compromise in security, directly or indirectly, of the BES Cyber System.

Other commenters noted ambiguity over the phrase "pose a security threat" and recommended that this phrase be removed. The concept of posing a "security threat" to the BES Cyber System should also be considered in context of the requirements of the NERC CIP Standards, particularly CIP-011-1 R1. BES Cyber System Information is intended to be identified and protected in accordance with an overall information protection program. As such, it is anticipated that the Responsible Entity will include some process to identify the information applicable to this program. As not all information will lead to directly gaining access to BES Cyber Systems but may in other ways compromise the overall security of the BES Cyber System, the SDT does feel that it is prudent to remove this phrase.

CIP Exceptional Circumstances

Several commenters identified an issue with the phrase in the definition of CIP Exceptional Circumstances that included "an imminent or existing hardware, software, or equipment failure." Commenters pointed out that the collection of forensic data in CIP-009-5 Requirement R1.5, draft 2 was subject to CIP Exceptional Circumstances. Through the inclusion of hardware, software, or equipment failure as a CIP Exceptional Circumstance, a Responsible Entity could essentially choose to never comply with the collection of forensic data. After consideration, the SDT chose to modify the requirement in CIP-009-5 R1.5 to indicate that data preservation should not impede or restrict recovery. The SDT believes that hardware, software, or equipment failure is a reasonable component to include as a CIP Exceptional Circumstance given the cyber-physical relationship of the electric grid and its supporting Cyber Assets.

Additionally, commenters noted that the involvement of the conditions identified in the definition of CIP Exceptional Circumstances is not always known ahead of time. Specifically, commenters suggested that the SDT add the phrase "threatens to involve." The SDT considered this suggestion and decided that given the supporting framework required through the cyber security policies in CIP-003-5 to invoke a CIP Exceptional Circumstance, this was a reasonable and beneficial modification to the definition.

Commenters also questioned when CIP Exceptional Circumstances can be invoked. No modification was made to the standard, but in response, the intent of the SDT is to allow the use of CIP Exceptional Circumstances only where specifically identified in the language of the requirement. Additionally, CIP Exceptional Circumstances should be declared using the provisions identified in the Responsible Entity's cyber security policy as per CIP-003-5 R1.

CIP Senior Manager

Numerous commenters suggested minor modifications to the definition of CIP Senior Manager. The intent of the SDT was to include a definition of CIP Senior Manager in the NERC Glossary of Terms Used in NERC Reliability Standards so as to make clear who the required approver is when the term is used across the body of CIP Standards. The SDT did not intend to modify the content of the definition, which has remained unchanged since version 2 of CIP-003-2 when the role of the senior manager was clarified in response to FERC Order 706, paragraph 381. The SDT was compelled, given the current state of the CIP Standards being in their 5th version, by comments that suggested that in addition to the authority and responsibility for leading and managing the implementation of the requirements, that the CIP Senior Manager should also have the overall authority and responsibility for leading and managing "continuing adherence" to the requirements within the NERC CIP standards.

The SDT also received comments that the definition of CIP Senior Manager should specifically call out CIP-002 through CIP-011 as this is the set of cyber security standards to which the CIP Senior Manager has the authority and responsibility for. The SDT received similar comments in response to draft 1 of the posting of this definition. At that time, the SDT responded that the definition was only applicable where it is specifically used in the standards. Additionally, the concern appeared to specifically reference CIP-001, which at the time was planned for retirement as part of project 2009-1. However, given the dynamic nature of project 2009-1 and the relative ease to which this definition could be modified in the future should additional standards be added to which the CIP Senior Manager authority should apply, the SDT is persuaded to include a reference specifically to "CIP-002 through CIP-011" in the definition of CIP Senior Manager.

QUESTION D11 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Physical Access Control Systems and Physical Security Perimeter? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the SDT has address all comments and has made clarifying changes to the definitions.

Physical Security Perimeter (PSP)

One commenter proposed modifying the definition to apply only for applicable BES Cyber Systems. However, applicability cannot be determined by a definition. We have clarified in the applicability column in standards CIP-004 through CIP-011 that PSPs are not applicable solely upon meeting the definition.

One commenter requested that a list of example Cyber Assets that should be included within a PSP. In response, the standards specify more clearly which Cyber Assets must reside in a PSP.

One commenter suggested the definition of PSP should reference the correct defined term: Electronic Access Control or Monitoring Systems, and the SDT has made this change.

One commenter suggested that the definition is ambiguous about (1) whether the perimeter is two or three dimensional, (2) whether there are different expectations for High and Medium BES Cyber Systems and (3) what size hole provides access. In response, the additional specificity for the perimeter and access points would limit the options entities have in applying the requirement. The SDT believes we have struck the right balance in this requirement to allow entities flexibility in their approach while describing the end result. In regard to the difference between physical protection in High and Medium Impact BES Cyber Systems, this is specified in CIP-006-5.

Physical Access Control System (PACS)

Several commenters proposed removing "alert" from the definition to avoid the interpretation that security guard workstations are included in scope. In response, the alerting component should include the system sending out the alert

and does not include all recipient persons or devices of the alert. We do not believe this needs further clarification in the definition.

One commenter suggested that examples should not be included in the definition and the wording "exclusive of devices…at the PSP" could exclude more asset than intended. In response, we note that examples should not change the definition but can be helpful in forming context. For PACS, these examples are useful for explicitly clarifying perimeter devices, which by nature cannot have the same physical protection are outside of scope.

One commenter suggested putting a comma to make clear the example applies to Cyber Assets. In response, the example does modify the locally mounted hardware and devices and not the Cyber Assets. In other words, the example is for the exclusion.

One commenter suggested that the SDT needs to ensure electronic visitor log books are not captured in the definition and that the exclusion uses "or" instead of "and" for the examples. In response, a visitor log book would not be within scope because it logs visitors and not access, and including an electronic visitor log book could cause the interpretation that any additional logging would be considered out of scope. Also, "or" and "and" are logically interchangeable in the example list, and we do not find a need to make any change.

One commenter suggested that monitoring Cyber Assets should be included in the definition. In response, we did not include monitoring devices because those are typically outside of the PSP and serve as a supplementary protection. Although these can be used to comply with monitoring requirements, it becomes problematic to apply additional CIP Standards requirements without creating a complex protection loop.

One commenter suggested changing the word "exclusive" to "excluding", but the SDT chooses to retain the originally posted wording.

One commenter suggested the definition should include workstations used to provision physical access and monitor alarms. In response, the proposal would expand the definition scope beyond what the SDT considers unacceptable risk. The level of effort required to protect this significant population of assets would far exceed the security benefit of doing so. As an example, this could include all cell phones and pagers carried by staff for responding to alarms.

QUESTION D12 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Electronic Access Control and Monitoring Systems, Interactive Remote Access, and Intermediate Device? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, clarifying language was added to each definition to highlight stakeholders concerns.

Interactive Remote Access

Several commenters requested clarification for the inclusion of dial-up access in the definition. Upon further review, this has been removed from the definition. The important part to note is that Interactive Remote Access is when using a remote access client or other remote access technology, regardless of the type of connectivity.

One commenter proposed that the definition of Interactive Remote Access be modified to exclude serially connected, non-routable, non-network connected devices. The definition did not include serially connected, non-routable, non-network connected devices. However, the definition has been modified to specifically address the use of a routable protocol.

Several commenters requested restructuring of the definition to highlight the criteria for identifying Interactive Remote Access. The definition has been updated as requested to highlight that the first criteria is the use of a remote access client or other remote access technology.

Several commenters requested more information regarding examples of a remote access client or remote access technology. Additional information is available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested that list item two, "Cyber Assets used or owned by employees" be modified as "Cyber Assets used by employees". The commenter considers employee-owned devices inappropriate for use in Interactive Remote Access. Employee-owned devices were added to the definition based on comments received in Project 2010-15:

Expedited Revisions to CIP-005-3. This was added to address industry need to have remote access not limited to use of only company-owned assets for remote access. This is in support of pandemic and other emergency planning situations.

One commenter recommended adding the words "owned by or under the control of the Responsible Entity" to prevent the inclusion of equipment owned by Managed Security Providers in the standards. Connections by vendors, contractors, and consultants should be protected to the same standard as assets owned by the entity. Assets owned or used by vendors, contractors, and consultants were added to the definition based on comments received in Project 2010-15: Expedited Revisions to CIP-005-3. This was added to address industry need to have remote access not limited to use of only company-owned assets for remote access. This is in support of pandemic and other emergency planning situations.

Multiple commenters noted that the sentence beginning with "Remote access may be initiated from ..." adds no value, does not address all circumstances, and should be deleted. They further noted it is possible to initiate remote access from assets owned by others not listed. The information was added to the definition based on comments received in Project 2010-15: Expedited Revisions to CIP-005-3. This was added to address industry need to have remote access not limited to use of only company-owned assets for remote access. Please see the opposing perspective noted by other entities. The definition states that access "may be initiated" and not "shall be initiated" to allow for flexibility and not define the three scenarios as the finite and final list.

Intermediate Device

One commenter was concerned with the phrase "performing access control" existing as part of the definition of an Intermediate Device. It is the SDTs intent that an Intermediate Device is classified as an Electronic Access Control or Monitoring System. The definition of Electronic Access Controls or Monitoring Systems has been modified to include Intermediate Device.

One commenter requested clarification as to the types of devices that could be used as an Intermediate Device. The SDT specifically did not list proxy or other technology to allow flexibility in how an entity may implement a solution that best meets their needs. Per CIP-005-5 Requirement R2.1, the Intermediate Device must be used before accessing a BES Cyber System or Protected Cyber Asset. Per the definition, the Intermediate Device must not be inside of an ESP. Additional references regarding the Intermedate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

Multiple commenters noted concerns with the language, “The Intermediate Device must not be located inside the Electronic Security Perimeter”. Comments were received that this should be added to the requirements and removed from the definition. Some consider the second sentence of the definition to be unnecessary, too prescriptive, and should be deleted. Some offered recommendations for changes to the definition to allow for future technology developments.

- The SDT considers this language to be defining and clarification of the device. The performance under the requirement is that an entity utilizes the intermediate device. Further, definitions are part of the standards and carry the same force as the requirements.
- The location of the Intermediate Device was included in the definition to address numerous industry questions on this matter both in Project 2008-06 Cyber Security Order 706 Version 5 CIP standards and Project 2010-15: Expedited Revisions to CIP-005-3. Many entities have raised questions regarding the location of the device based on termination point of encryption and other issues.
- The only restriction placed on the Intermediate Device is that it not be inside of an ESP. Access authentication should be performed before the user is granted access through the ESP. Encryption should be terminated outside of the Electronic Security Perimeter so that event logging within the ESP is not negatively impacted. The SDT specifically did not list other specifics to allow flexibility in how an entity may implement a solution that best meets their needs whether through the use of a multi-purpose device or other architecture. Additional references regarding the Intermediate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter noted concerns that the term "device" is not clear in defining the Intermediate Device. They recommend using the term “Intermediate Cyber Asset”. The definition includes the term “Cyber Asset” which is defined as “programmable electronic devices including the hardware, software, and data in those devices”. The SDT has chosen the unique term “Intermediate Device” to allow for the use of one or more Cyber Assets making up the device.

QUESTION D13 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the SDT clarified language to the definitions.

Electronic Access Point

Multiple commenters asked for clarity if an Electronic Access Point (EAP) must be routable on both sides. In response, the SDT's intent is that if the device is accessible from outside the Electronic Security Perimeter (ESP) with a routable protocol then an EAP must be put in place. Therefore, just as in the Critical Cyber Asset Identification Guidelines of today, the 'inside' does not have to be routable. For example, if the entity has a digital relay and has the serial port used for console access (non-routable serial communications) attached to a serial-to-IP gateway such that the relay's command console is addressable from outside the ESP via a routable protocol (e.g. <IP Address>:<Port #> will connect you to the relay), then this meets the definition of External Routable Connectivity and an EAP is required.

One commenter provided an alternate definition that included the phrase "externally routable bi-directional communication" and added "or inbound communications to a Cyber Asset within the Electronic Security Perimeter" to the end. In response, the SDT notes that the direction of the communication is an aspect of External Routable Connectivity definition. The Electronic Access Point is an intentionally broader definition and its main function is to deny all access by default and only allow needed traffic to cross the ESP, regardless of direction.

One commenter asked that it be clarified as to whether an EAP is part of the ESP or not? In response, the SDT notes that an EAP is part of an ESP as it is the point where the routable communication from outside the ESP is allowed to cross the ESP to Cyber Assets inside the ESP.

One commenter suggested that the term "interface" be removed and have the definition reference a Cyber Asset. In response, the SDT notes that the inclusion of interface is meant to address the situation where an entity has a firewall as an EAP that has numerous interfaces to different networks and only one goes to a network that has applicable Cyber

Assets. The inclusion of 'interface' means the requirements would be concerned with only those interfaces that communicate with applicable Cyber Assets and not to interfaces that do not have any applicable Cyber Assets. The SDT also notes that the requirements in CIP-005 that apply directly to EAPs concern an interface (deny by default, methods for inspecting for malicious communications, etc).

One commenter suggested that the definition add "allows or is capable of allowing" to include dual homed Cyber Assets including laptops with wifi that is not hardware disabled. In response, the SDT believes that for a mandatory requirement the enforceable point should be binary – either communication is allowed to cross an ESP or it isn't – and the standards should avoid dealing with all possible capabilities.

One commenter asked for confirmation of the notion that Cyber Assets only communicate with other Cyber Assets. In response, the SDT notes that Cyber Asset is the basic unit of these standards and there is no lower level term. As Cyber Asset is a 'programmable electronic device', the SDT believes this covers most all situations. The SDT notes that Cyber Assets includes most all network gear as well, not just servers and workstations.

Electronic Security Perimeter

Several commenters suggested that examples should be included. In response, the SDT is not including examples in this term. Since terms such as ESP often refer to cyber technology that is constantly changing and developing, there is a tendency for examples to become outdated. The SDT used guidance instead to discuss examples rather than definitions. When the term is then used in a requirement, there is a tendency for the examples to then become prescriptive and mandatory, which is not the purpose of examples.

Multiple commenters provided some clarifying questions: Does an ESP presume the presence of EAP? Does a BES Cyber System with no External Routable Connectivity fall into scope? In response, the SDT clarifies that the ESP does not presume the presence of an EAP and BES Cyber Systems without External Routable Connectivity are in scope of the CIP standards. The ESP is a 'logical border' around a routable protocol network to which a BES Cyber System is connected. An isolated network with no external connectivity has an ESP; a logical border. The ESP is used to determine the 'Associated Protected Cyber Assets' as well as the collection of Cyber Systems and Assets that will be elevated to the impact level of the highest impact BES Cyber System/Asset in the ESP (see the definition of Protected Cyber Asset). If routable protocol communications cross the ESP, then an EAP is required.

Several commenters stated that this should be applicable to BES Cyber Asset instead of BES Cyber System. In response, the SDT notes that the BES Cyber System grouping is up to the entity and the concepts of electronic and physical security perimeters need to be taken into account. An entity is free to define every individual BES Cyber Asset as its own unique BES Cyber System and in essence make the entire standard Cyber Asset based. The grouping into systems is at the entity's discretion, but should be done with the requirements in mind.

External Routable Connectivity

Multiple commenters suggested that clarity is needed concerning the focus on Cyber Asset connectivity, rather than a 'system' with connectivity. Does a 'system' with one routable device mean all cyber assets in the system meet the applicability? This applies to the ESP definition as well. In response, the SDT has updated the definition to be at the Cyber Asset level rather than the BES Cyber System level. The intent is that Cyber Assets that have External Routable Connectivity must meet the applicable requirements and Cyber Assets that do not meet the definition are exempt from the requirement.

Several commenters suggested that the definition should include the OSI network layers. The SDT has chosen to not include Open System Interconnection (OSI) layers in the definition at this point. It is believed that with the history of the CIP standards being based on 'routable protocol' since its inception that there is a sufficient understanding of these terms at this point.

Multiple commenters suggested that the definition should be reworded to be a property of a BES Cyber Asset, not the asset itself. In response, the SDT agrees and has changed the definition to begin with "The ability to access…"

One commenter suggested that the definition should only apply if routable connection goes all the way to a BES Cyber Asset within the ESP. In response, the SDT is trying to incorporate the situation (identified in the current CCA Identification Guidelines) where an Ethernet/serial gateway is used at the perimeter. A BES Cyber Asset may have a serial connection from its console port to the Ethernet/serial gateway such that from outside the ESP the device's console port is directly addressable using a routable protocol, usually simply in the form of <ip address:port #>. The SDT's intent is for the definition to capture any device that is accessible from outside the ESP with a bi-directional routable protocol.

One commenter suggested that the definition needs to consider inside to outside connectivity not just outside in. In response, the SDT does consider 'inside out' connectivity in the requirements (e.g. outbound rules on EAP's). However, the intent with this definition is to focus on the higher level of threat that outside-in connectivity presents as well as to

give some credit for more secure network architectures that only push data out and don't allow outside-in connectivity (data diodes, etc.).

A few commenters commented that the definition should be Cyber Asset based rather than strictly limited to BES Cyber Systems. In response, the SDT has clarified that access is from a Cyber Asset that is outside of the BES Cyber System's associated Electronic Security Perimeter via a bi-directional routable protocol connection.

Protected Cyber Asset

Multiple commenters suggested that the parentheses should be removed, keeping the sentence concerning temporarily connected Cyber Assets. In response, the SDT agrees and has made the suggested change.

One commenter suggested that the temporarily connected Cyber Asset exclusion should be pulled out and made into a separate definition. In response, the SDT in this instance would be defining a term simply to use the term in the definition of another term. Therefore the SDT believes it is more straightforward to include a more complete definition in the ultimate term we are defining, and see no issue with stating what something is and what it is not while defining it.

Multiple commenters suggested that this should allow for network connection of temporarily connected Cyber Assets, suggesting that 'directly' be removed to allow connection within the ESP without requiring connection through a Cyber Asset. In response, the SDT notes that a network switch is a Cyber Asset and thus network connections are included. However, the SDT agrees that this point needs more clarity and has deleted the word 'directly' and clarified that it is a connection either to a Cyber Asset in the ESP or the network within an ESP.

One commenter suggested that a separate definition for Transient Cyber Asset should be included and have a requirement to scan for malware before connection. In response, the SDT notes that this was included in previous drafts but was removed in this draft in response to comments. Numerous comments were received pointing out the audit issues of such a requirement. How does one prove that a list of temporarily connected devices is complete? How does one prove that virus scans were done on a device that was there one minute and gone the next? How does one maintain and prove a complete inventory of all temporarily connected devices? Commenters also pointed out that the object of protection is the BES Cyber System – the goal is to protect BES Cyber Systems from all threats including temporarily connected devices. There were also numerous issues raised concerning TFE's as many troubleshooting and maintenance devices are 'programmable electronic devices' and would thus be Cyber Assets but have no antivirus available. A cable scanner used to diagnose cabling issues may be a programmable electronic device and then require a TFE. In response to

all these issues, the SDT decided to remove the requirement. However, the SDT notes that CIP-007 R3 requires an entity to deploy method(s) to deter, detect, or prevent malicious code and it is expected that such measures as scanning temporarily connected laptops and other similar devices may be included in these methods.

QUESTION D14 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, several changes have been made to clarify language in the definitions.

General Comments

Several commenters stated that the phrase "reliability tasks of the functional entity" is unclear and needs to be replaced or further defined. In response, the phrase reliability tasks of the functional entity comes from the definition of BES Cyber System and the reliability tasks are those specified in the NERC Functional Model.

Several commenters suggested that the terms compromise and disrupt need to have their own definition. In response, the words compromise and disrupt carry forward from the previously approved definition and we have not received compelling indication that these terms need further clarification.

Several commenters suggested that the phrase "was an attempt to compromise" is vague and should be deleted. In response, this phrase captures those incidents that do not necessarily succeed but should prompt investigation.

One commenter suggested replacing the phrase "reliability tasks of the functional entity" with "reliability tasks identified for functions in the NERC Functional Model." The SDT does not specify the NERC Functional Model, which is not a document subject to the standards development process, but the SDT believes that the phrase adequately conveys those tasks.

One comment was on the phrase "malicious and suspicious" is subject to interpretation and proposed adding the qualifying phrase, "as determined by the Responsible Entity." In response, the definition should not include this phrase because it is not a requirement, and CIP-008-5 already specifies the obligation for the Responsible Entity to make this determination.

One commenter suggested qualifying the term ESP and PSP with BES Cyber System to avoid having to demonstrate compliance with perimeters that do not protect BES Cyber Systems. In response, the requirement in CIP-008-5 makes this distinction in the applicability section.

One commenter suggested that the definition of Control Center uses a different term "reliability functional tasks" and requests clarification if this term means something different. In response, the SDT has clarified the language to read "reliability tasks".

One commenter suggested that the DOE OE-417 form should be considered to allow entities to comply with both requirements. In response, the SDT has reviewed the latest version of this form and do not find any reporting requirements that would conflict with those in CIP-008-5.

Cyber Security Incident

Several commenters suggested replacing the phrase "was an attempt" with "has the potential" in the definition of Cyber Security Incident because an attempt implies knowing the intent of the perpetrator and it excludes accidents which have the potential to compromise the BES Cyber System. In response, we have not significantly changed the currently approved definition and do not find the need to incorporate the proposed modifications. Both phrases communicate the desired result that an unsuccessful attack or compromise would be considered a Cyber Security Incident.

There was a suggestion that the definition of Cyber Security Incident now includes PSPs and the impact will be difficult to assess. In response, the current approved definition includes PSPs.

One commenter proposed to amend the definition of Cyber Security Incident to include: "Is a violation or imminent threat of a violation of computer security policies, acceptable use policies, or standard security practices impacting or within covered ESPs or PSPs." In response, violation of policies can be covered in an entity definition of a cyber security incident, but the Glossary definition has a focus on impact in order to broadly apply the standard.

One commenter suggested that physical security incidents should have its own definition and not be included as part of a Cyber Security Incident. In response, a physical security breach into a perimeter protecting the BES Cyber System provides enough cause for concern in the integrity of the BES Cyber System to warrant classification of a Cyber Security Incident. Individual entities may use distinct terms and response teams for these types of incidents, and the obligations in CIP-008-5 would still apply.

Several commenters proposed removing the phrase "suspicious event" from Cyber Security Incident. In response, the term suspicious event captures those incidents prompting further investigation in which the entity may not determine the cause or motive.

Reportable Cyber Security Incident

SPP RE expressed concerns that Reportable Cyber Security Incidents would not include those incidents in which redundancy mitigated the impact. In response, we have provided guidance in CIP-008-5 that Reportable Cyber Security Incidents would also include those that triggered an activation of redundant systems.

There was a proposal to replace "Any" with "A" to start the definition of Reportable Cyber Security Incident and we have done so.

One commenter proposed the following definition of Reportable Cyber Security Incident: "Any Cyber Security event that has compromised or disrupted one or more reliability tasks of a functional entity, which through investigation and escalation, has been determined by the Responsible Entity to be reportable to ES-ISAC." In response, this proposed definition includes a requirement, which should remain in the standard. The requirement in CIP-008-5 still provides leeway to the entity in determining Reportable Cyber Security Incidents.

One commenter stated that the definition needs to be coordinated with the EOP-004-2 drafting team. In response, both the CIP Version 5 and EOP-004-2 drafting teams have agreed to move all reporting obligations for Cyber Security Incidents to CIP-008-5.

One commenter proposed the definition for Reportable Cyber Security Incident in order to avoid using the term functional tasks, "A Cyber Security Incident that compromised the ESP or PSP or disrupted the operation of an applicable BES Cyber Asset or low BES Site."

One commenter proposed to add additional guidance in CIP-008-5. In response, the use of functional tasks ties the reportable incident to a specific reliability function. Without this qualification, the definition can easily be interpreted to include nominal security events as reportable. The SDT has already added additional guidance on distinguishing a Reportable Cyber Security Incident.

QUESTION D16 – IMPLEMENTATION PLAN:

If you disagree with the changes made to the Implementation Plan since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, there were not many changes made to the Implementation Plan, but the comments and comment responses below provide clarity into some of the concerns regarding the proposed effective date, the possibility of bypassing Version 4, and the initial performance of certain periodic requirements.

Proposed Effective Date

One commenter suggested that the effective date conflicts with the initial performance of requirements section and should specifically mention this in the effective date language as an exception. In response, we do not feel this is necessary. The implementation plan enumerates any exceptions to the effective date of the standard. The alternative of including all such exceptions in the effective date language would make the language unreasonably complex.

One commenter agreed with the approach to focus on the high and medium impact BES Cyber Systems but questions the need for an additional year of implementation time for low impact BES Cyber Systems particularly if no inventory is necessary. SPP RE also agrees an additional year for compliance with CIP-003-5 R2 is unnecessary. In response, the need for an additional year of implementation for low impact BES Cyber Systems exists to allow entities to formulate and implement effective security solutions for physical and electronic perimeter protection. Despite not requiring an inventory of low impact BES Cyber Systems, entities must still implement these policy changes in applicable locations where no perimeter protection currently exists.

Several commenters questioned why the effective date is so far out given that the standards have been in development for more than two years. In response, the development timeframe of the standards do not determine when entities begin planning compliance. Rather, entities have assurance in the finality of the standards upon FERC approval. The number of cyber systems applicable in this standard far exceeds any previous version of the standard. The SDT reasons it will take two budget cycles for entities to plan and implement these standards.

Bypassing Version 4

Several commented that language to extend the Version 3 effective period and bypass Version 4 should be removed because the recent FERC Order has solidified the effective date for Version 4 as April 1, 2014. Other comments request a

transitional plan to address the period of compliance between Version 4 and 5. In response, the SDT observes that the provisions to bypass Version 4 remain in the implementation plan and are subject to approval by the industry and FERC. This is explained in greater detail in the summary section at the beginning of this document.

Initial Performance of Certain Periodic Requirements

One commenter stated that for non-periodic requirements, the IP should state entities comply with all other requirements on the effective date. In response, this is already stated in the effective date language. The periodic requirements are exceptions to this language.

Several commented that CIP-010-1 requirement part 3.2 and CIP-009-5 requirement part 2.3 have a 36 month periodic performance requirement and should have an initial performance not exceeding 36 months after the effective date. Yet, although the periodicity for this requirement is 36 months, the initial performance should occur closer to the effective date of the standard. However, we are persuaded by arguments that initial exercises should be conducted prior to the operational exercise active vulnerability assessment.

Several commented that the language "…Notwithstanding any order to the contrary…" is unnecessary because the FERC can approve or remand any part of the implementation plan if it so chooses. While this is true, the inclusion of this language allows that decision to be made without the tremendous overhead of going through the standards development process.

One commenter argued that the periodic requirements section requires compliance as early as 14 days after the effective date, but the effective date allows 24 months. In response, this is true, and all of the specified periodic performance requirements occur after the effective date, which is at least 24 months.

One commenter argued the initial performance of the requirement should be performed prior to the effective date. They questioned why a year would be necessary to hold the first training or verify provisioned access. In response, the SDT disagrees with compliance prior to the effective date for two reasons. First, the effective date of the standard indicates when Version 5 becomes effective and previous versions retire. Requirements that obligate performance on a specific day cannot technically be compliant prior to the effective date. Second, the specified periodic requirements are mostly verification assessments or updates for existing security controls, and the objective is to have the security controls in place upon the effective date.

Based on comments received, CIP-009-5 requirement part 2.3 has been added to the list of periodic requirements that must be implemented no later than 12 months after the effective date.

One commenter noted that CIP-009-5 Requirement R1.4 still contains language requiring an initial performance. However, the intent of this requirement was not to obligate an initial periodic performance, and we have modified the requirement language to remove the word "initial".

Planned or Unplanned Changes

Several commenters suggested all new or reclassified Cyber Systems have the same timeframe of 12 months to achieve compliance. In response, we have updated the implementation plan based on changes to CIP-002-5 that remove obligations to update the BES Cyber System categorization within 60 days. This provides entities additional time to demonstrate full compliance for planned changes. Unplanned changes resulting in a higher categorization continue to allow the additional year to demonstrate full compliance for the affected BES Cyber Systems.

The Planned or Unplanned Changes section was collapsed into one section based on multiple comments, and it has been clarified that for *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System, with additional time to comply for requirements as specified and in the same manner as in the section *Initial Performance of Certain Periodic Requirements*. For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards, according to timelines specified in a separate table, following the identification and categorization of the affected BES Cyber System, with the additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Time Periods for Disaster Recovery

Several commenters requested clarity on what constitutes the completion of the Disaster Recovery. In response, the use of the defined term CIP Exceptional Circumstance throughout the CIP Cyber Security Standards eliminates the need to define a special case in the implementation plan for Disaster Recovery. Entities can take exceptions from the Requirements where CIP Exceptional Circumstances is specified.

One commenter suggested that the Disaster Recovery section seems to suggest not holding up restoration for compliance but entities would need to be compliant when restoration activities are complete. In response, this section

has been removed and we defer to the use of CIP Exceptional Circumstances throughout the CIP Cyber Security Standards to provide entities clarity on when and where exceptions to the Requirements can occur.

Applicability Reference Tables

One commenter requested additional clarification regarding the purpose of the applicability tables and others noted inconsistencies with the table. In response, we have corrected inconsistency errors, changed the title and provided introductory remarks. These tables are intended only for convenience. The SDT chose not to include this in a background or guidance section because requirement numbering will change in future revisions.

QUESTION D17 – DEFINITIONS AND IMPLEMENTATION PLAN:

If you have comments or specific suggestions that you have not been able to provide in response to the previous questions, please provide those comments here. Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the implementation plan was modified appropriately and certain areas were modified for clarity. Entities should refer to the individual responses to comments in the definitions questions for the SDT's response to comments for individual definitions. Many commenters provided comments on the positive direction of the posted draft. The SDT thanks these commenters and appreciates the encouraging remarks.

Several comments were toward the approach to requirements that result in a zero tolerance aspect for deficiencies in compliance monitoring. The SDT has proposed additional language that, together with a framework that also includes VSL language and RSAW audit guidance language, addresses the larger issue and shifts the focus of certain requirements to correcting deficiencies. This is explained in greater detail in the summary explanation at the beginning of this document.

Several commenters expressed their concerns on the protection of Low Impact BES Cyber Systems and the compliance demonstration of requirements that apply to them. The SDT has spent considerable time and effort to work with stakeholders on addressing this issue and believes that the approach in the new proposed draft addresses the concerns.

Multiple commenters reiterated concerns on the broad application of CIP V5 irrespective of connectivity. The SDT has included consideration of connectivity in the applicability of requirements and believes that this approach appropriately addresses applicability differences due to connectivity type. The SDT reiterates its posture that, while connectivity is an important vector for cyber security threats, it is not the only one and that the CIP standards encompass a holistic approach to the protection of BES Cyber Systems.

There were multiple comments that suggested the phrase "but not limited to…" may be construed as required evidence. The SDT agrees with the comment and is using the standard language "Example(s) of evidence may include, but is not limited to…" to convey two concepts in the measure: the evidence in the measure are not required evidence but represents examples of quality evidence, and entities may present other evidence that may be presented in lieu of the ones described or in addition to them.

Multiple comments were based on the definition of periodic requirements, with another commenter citing the CAN on Annual that has been published. The SDT notes that CANs provide guidance for auditors, are not interpretations of standard requirements and are not the basis for changes to requirements. The SDT has considered all outstanding CANs as additional input to the development of these standards, and where the CANs result from unclear requirement language, the SDT has drafted language with a goal of eliminating the need of a CAN for auditing purposes. Since the word annual is not used in the V5 CIP standards, the term does not apply. The SDT has drafted language that reflects its intent while providing adequate flexibility to minimize zero defect effects.

Several commenters requested a global clarification similar to section 5 of CIP-003 that explains the significance of the use of bulleted and numbered items. Another comment was on the bullets in section 4, part 4.2.2. The SDT will insert a paragraph in the background section to include such explanations.

There were several comments on the use of a single VRF for each requirement, irrespective of whether it applies to High Impact or Medium Impact. Another comment was on the VSLs and the differentiation required to handle zero defect. VRFs are used as one of many input variables used to determine the sanction in the case of a violation of a standard. The current sanction table used for calculating regulatory sanctions is based on VRFs at a requirement level. However, there are many other considerations in the determination of a sanction for a specific violation. Until the current development of the evolving enforcement model is better defined, it is premature to effect changes to the VRF. Regarding VSLs, the SDT notes that VSLs are used after the fact, i.e. when a violation has already occurred. The SDT believes that VRFs, VSLs and RSAWs, together with appropriate requirement language, must together provide a complete framework to address the zero defect issue. The ballot for VRFs and VSLs is a non-binding ballot, and there is likely to be changes to accommodate evolving concepts in handling zero defect compliance and risk based compliance assessments.

Several comments were on the compliance section on records retention and retention requirements in standards requirements. Retention requirements, when specified in requirements, are requirements for technical reasons, such as event log retention for forensic purposes. The retention periods specified in the compliance section are meant to apply to records required for demonstrating compliance. For example, if 90 day event log retention is specifically required in a requirement, the Responsible Entity is expected to retain records that demonstrate that it has kept 90 days of logged events for the 3 years, not that it has kept 3 years' worth of these event logs. Under the compliance section, these could be log entries of the process that maintains a minimum of 90 days of log events.

Several commenters suggested that all sub-requirement parts should state the goal. The SDT generally provides the goal either in the body of the main text for the requirement, or in the rationale box. The SDT believes that the goal of each subpart is mostly self-evident given the overall requirement objective, and that addition of a goal for each subpart would be redundant and unnecessary in most cases.

There were several comments surrounding the need for a definition of Control Centers. The SDT directs entities to its summary response to Question D9 on this issue.

There were several comments on the removal of restoration resources from Medium Impact criteria, and cited the need to provide adequate justification. It is not clear to the SDT whether these comments were in support of this change. However, as a matter of normal SDT stakeholder input consideration, extensive debate on this issue was conducted in the NERC operating and planning technical committees, without a clear resolution. As a matter of procedure, the SDT must provide justification for changes from one release to another and has received stakeholder comments supporting this change.

There were multiple suggestions that a summary of the CIP Version 5 standards and the interaction between the requirements and their applicability be provided by the SDT. The SDT is focused on addressing technical issues from comments on requirements and on the standards themselves. The SDT appreciates any input provided by stakeholders, and it plans to facilitate distribution of an informational summary addressing this concern that was prepared by certain stakeholders that have been collaborating with the SDT. However, the formal posting with the standards would require other types of SDT, NERC and other stakeholder groups' review and/or approval and is not an appropriate venue for making compliance management tools available to stakeholders.

There were several comments on the issue of physical access controls for High Impact, specifically on whether two different access control systems are required. The SDT has provided guidance on this issue in the guidelines and technical basis section of CIP-006 that indicate that the intent of the requirements is not to require different control systems.

Numerous commenters expressed concern with the term "Associated Protected Cyber Assets". In considering these comments, the SDT noted that the concept of high water marking for Impact Level within an ESP was not very clear. The SDT has defined a term Protected Cyber Assets to incorporate the concept of BES Cyber Systems, their associated Cyber Assets within the same ESP and the concept of High Water Marking for Impact level within an ESP.

There were several comments that a definition for dial-up connectivity is needed. The SDT has included a definition for "Dial-up Connectivity" in this draft proposal.

There were comments on the use of "Associated…" in the applicability column of requirement tables. The SDT has made some changes to the language used to clarify the applicability and has also used the defined term Protected Cyber Assets to further clarify applicability.

There were comments relating to a number of editorial and stylistic issues related to table headers, capitalization and inconsistencies of terms. The SDT has considered these comments and made the appropriate changes.

One commenter recommended that the exemptions section in the applicability section should be specific to the standard, and not say CIP-002-5 in standards other than CIP-002. The SDT agrees and has made the appropriate changes in the standards.

One commenter suggested that the application guidelines should be allowed to change from standard to standard and that glossary terms should not be defined again in the standard. The SDT disagrees that application guidelines should be the same for all standards, but does agree that there should not be any incompatibility or inconsistency between the guidelines and the standards. The SDT also agrees that there should not be any definitions repeated in a standard when they are proposed glossary terms. The SDT will ensure consistency between guidelines and standard requirements. The SDT notes that the notes on glossary terms in the guidelines or background section are intended to provide additional explanantion of the terms and not be replacement definitions for the proposed terms for the NERC glossary. The requirements in the standard are the ultimate source of authoritative text for compliance.

One commenter suggested that the requirements that should be subject to CIP Exceptional Circumstances should be extended to most requirements except those in CIP-002, CIP-003 and CIP-004, and provided a list of requirements that should be subject to CIP Exceptional Circumstances. The SDT has carefully selected requirements that it believes are appropriately suitable for a CIP Exceptional Circumstance in order to facilitate the handling of emergency situations and timely electronic and physical access for first responders. With regard to a comment on ensuring that CIP Exceptional Circumstance would not require a TFE, the SDT has no jurisdiction over Rules of Procedure and cannot predict what regulators will deem to be TFE triggering language in the future. It is not the SDT's intent that CIP Exceptional Circumstances be TFE triggering language, but rather, that the Responsible Entity has carefully defined its policies and

procedures for declaring and ending CIP Exceptional Circumstances as required in CIP-003, and that any specific CIP Exceptional Circumstance be documented as required to demonstrate compliance to the specific CIP requirement.

One commenter suggested that it should be clear that no policies or procedures are required for CIP-004 to CIP-011 Responsible Entities that do not have High or Medium Impact BES Cyber Systems. There is no requirement in CIP-004 through CIP-011 that is applicable to Low Impact BES Cyber Systems. This is clear in the applicability column of the requirements tables.

There was a comment on the incorporation of guidelines and technical basis in the standards, citing stakeholders' time constraints in reviewing guidelines during the comment period. The SDT has spent considerable time drafting guidelines and providing the technical basis for requirements as part of the structure of results based standards. The SDT believes that the guidelines and technical basis provides valuable information to stakeholders during the comment and balloting process. It provides valuable input to stakeholders on the intent of the SDT, both during the development and the implementation phases of the standards. This approach has received overwhelmingly positive feedback from stakeholders. While the SDT understands that these guidelines and technical basis are not intended to be used instead of, or in addition to requirements, the SDT believes they provide valuable context to the standards' requirements.

There was one comment on the use of attestations as measures, citing industry confusion on the appropriate use of attestations. The absence of "attestations" in the measures does not imply that attestations are not appropriate measures of compliance, but that the SDT chose to use more specific examples of evidence for these requirements. Whether attestations are appropriate measures of compliance depends on the requirement. The SDT has used attestations where it may more likely be the measure that can be produced as evidence of compliance, with no implication that it is the only way of demonstrating compliance.

One commenter suggested that part 4.2.3 of the applicability section (Section 4) may inadvertently create an exemption for Control Centers. While certain Functional Entities may not own BES Facilities as described in the NERC Glossary, they perform reliability functions as the Functional Entity listed in 4.1 for BES Facilities. The introductory paragraph of 4.2 specifically refers to "…Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above …"

One commenter requested clarification or a definition of "Adverse Reliability Impact": this term is defined in the NERC Glossary of Terms.

One commenter requested a formal definition for “Common Control System”: the SDT believes that the term control system is a widely understood term of art used in electric reliability operation and engineering and that it does not require specific definition in these standards.

One comment suggested that the standards use data and information interchangeably. The SDT notes that it has used data when referring to a set of values (numeric or otherwise) in its raw form, and to information when referring to data processed for a specific use.

One commenter noted that the CIP standards should be aligned more closely to the NIST or ISO standards. The SDT uses many frameworks (including the ones cited) as sources for the development of requirements. The SDT notes that both of the cited standards are general purpose cyber security standards and guidelines not intended for any specific industry use. The SDT believes that the mandatory nature for standards specifically for the BES poses unique challenges and requires an appropriately developed approach.

There was one comment that was extensively on the scope of applicability to asset owners and operators only, and the absence of compliance for suppliers and other third party providers. The SDT notes that these mandatory standards are developed under the jurisdiction of the ERO and that they can only be applied to NERC Registered Entities.

One comment was on the awareness and training requirement in CIP-004 R2 and role based awareness training. The comment was specific that the items in the table in R2 referred to systems while the requirement cited role based training. Table R2 contains the requirements for the required content of the training program, but the level at which the training is provided in each item is based on the role of the individual taking the training.

One comment was extensively on the 99.9% availability specification in CIP-006. The SDT has redrafted the requirement and the 99.9% specification has been removed.

There was one comment on the effect of the application of the CIP standards on small entities. The SDT notes that BES Cyber Systems are categorized based on reliability impact rather than on entity size. The SDT has developed the requirements to be commensurate with the level of impact on the BES. The SDT has not included entity size as an input to the applicability of requirements.

One comment was extensively on section 4.2.2. The SDT notes that section 4.2.2 is not intended to specify the impact criteria, but the scope. Consequently, many of the terms used are extracted from the registration criteria for DPs. Many of the comments presented have been incorporated in the proposed new draft, while a few are appropriate as part of the criteria.

One commenter made many remarks on global sections used in all standards. These will be reviewed by NERC standard staff as standard templates applicable to NERC standards.

There was a comment on the use of "where technically feasible" and the commenter suggested the use of language that would specify compensating controls. The SDT notes that there were requirements in CIP Versions 1-4 that had alternative language to allow compensating controls, but that the language was added to TFE triggers.

One commenter requested a definition of "Associated Data Centers". Please refer to the summary response on this issue to comments on D9.

One commenter was concerned with the periodic requirements, specifically on the 15 month period for periodic requirements intended to be performed annually. The commenters suggested alternative language that would ensure strict compliance with a 12 month period. The intent of the SDT in specifying a 15 month period for annual requirements is to provide some flexibility to entities in the framework of attenuating zero defect requirements. The comments imply that Responsible Entities would aim for strict minimum compliance at the cost of increased non-compliance risk. From the practical implementation standpoint, the SDT understands that most Responsible Entities will implement a process that would ensure the performance in a period less than 15 months (an annual period is easier to track from the compliance management standpoint) for assured compliance.

One comment was raised on the SDT's discussion of redundancy as not being a mitigation for cyber security vulnerabilities and stated that redundancy provide mitigation for some cyber security vulnerabilities. While redundancy provides some mitigation for recovery requirements, the SDT has not found a compelling case where strict redundancy of using an exactly mirrored system configuration would provide mitigation of a cyber security vulnerability. It is the SDT's opinion that such configurations have the unintended effect, from the cyber security (not operational) standpoint, of increasing the attack surface. The SDT does agree that configurations that provide redundancy of function rather than system redundancy can provide mitigation if implemented with systems dissimilar enough to provide mitigation of certain system specific cyber security vulnerabilities.

One comment was on the term Facility and its relation to systems, also stating that the term element is undefined. The SDT has used the term Facility in its defined meaning in the NERC Glossary when used in its capitalized form. The term Facility is used to refer to groups physical BES Elements. The NERC Glossary has a definition of Element used in the context of the BES. In cases where the SDT intends a broader scope to include systems, the SDT has used "Facilities, systems and equipment".

There was a comment on the exemption from the standards of cyber assets between discrete ESPs. In particular, the commenter suggested requirements to implement end-to-end encryption. The commenter seems to suggest that such encryption should be required for routable and non-routable protocols. In addition, the commenters suggest that EAPs should be subject to cyber security requirements. The SDT has not required specific technologies to protect information between ESPs, but has focused instead on the cyber security objectives of access control and monitoring of traffic across EAPs. The comments do not seem to take into account communication between ESPs of real-time, latency sensitive applications common in control systems. The authenticity and integrity of application data or information is not always implemented using communication encryption technology, but may be implemented at other layers of the overall stack without the latency overhead of encryption. The commenters also seem to interchangeably use EAPs and the cyber assets that implement the EAP. The CIP definition of an EAP is an interface. There are however requirements, including security event monitoring requirements, that are applicable to the Cyber Assets that perform access control and monitoring functions, including those that implement an EAP, for electronic and physical access.

A commenter suggested that BES information protection requirements should apply to third parties. The SDT agrees and expects the Responsible Entity to comply with requirements for protecting and handling BES protected information, whether such information is accessed or handled by its own employees and third parties. The requirements in CIP-011 require the Responsible Entity to implement processes to ensure such access control and handling.

One commenter provided its fundamental objection to Version 5 and suggested that implementation of the current CIP standards should be allowed to mature. The SDT is required to address all the FERC directives from Order 706, and FERC Order 706 has directed the ERO to complete consideration of Order 706 directives by March 31st, 2013.

One commenter suggested that the statement in the implementation plan that starts with "Not withstanding any order to the contrary…" should be amended in light of Order 706. The SDT believes that the window for the application of the statement is still possible given the deadline in Order 761.

One commenter inquired on when a cyber system would have to come into compliance as a result of an emergency. One commenter also inquired on how to treat temporary elevation. If the cyber system is re-categorized or is a new cyber system as a result of that emergency or unplanned change, the implementation table specifies 12 months.

There was a comment on missing requirements in item 5 of the Implementation Plan. The SDT has included these requirements.

One commenter pointed out that the background section dealing with reliable operation of the BES contains an unclear reference to the Functional Model. The SDT has added qualifications that clarify that both reliability tasks defined in the Functional Model and the functional entity's relationships with other functional entities are considered.

One commenter suggested that there are requirements where the text of the requirement specifies BES Cyber Systems when the applicability column specifies more than BES Cyber Systems. The SDT has reviewed the language of the requirements where this occurs to ensure consistency with the applicability column. In cases where more than BES Cyber Systems apply, the SDT generally uses "applicable Cyber Assets."

One commenter expressed the need for the concept of escorted electronic access for remote support using technologies such as WebEx. The fundamental concept in escorted access is not only that of continuous visibility on the actions of the escorted individual, but also the capability of timely intervention in the case of inappropriate action. The SDT believes that total support for this concept is not possible in an electronic access scenario.

One commenter stated that in its opinion, the functional entity Interchange Coordinator (IC) does not have any asset that would be included, and should therefore not be included in the applicability section. The SDT reviewed the reliability tasks for the IC function as well as the responsibilities of the IC Functional Entity in its relationship with other functional entities in the Functional Model and noted real-time responsibilities in the latter in relation to BAs and RCs.

Questions with Votes Only:

1. Do you agree with the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Madison Gas and Electric Company	No
MRO NSRF	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
FirstEnergy	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No

Organization	Yes or No
ACES Power Marketing	No
SPP and Member companies	No
Comment Development SME List	No
Dairyland Power Cooperative	No
CenterPoint Energy	No
Hydro One	No
Ingleside Cogeneration LP	No
NIPSCO	No
Trans Bay Cable	No
Consumers Energy Company	No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	No
American Transmission Company, LLC	No
Ameren	No
NextEra Energy, Inc.	No
Liberty Electric Power LLC	No
ISO New England Inc.	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No
Alliant Energy	No
New York Power Authority	No
Exelon Corporation and its affiliates	No
Wiscsonsin Electric Power Company	No
Farmington Electric Utility System	No
City Utilities of Springfield, MO	No
NYISO	No

Organization	Yes or No
Deseret Power	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
US Bureau of Reclamation	No
California Independent System Operator	No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
NCEMC	Yes
IRC Standards Review Committee	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes

Organization	Yes or No
Southern California Edison	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Xcel Energy	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Tennessee Valley Authority	Yes
PSEG	Yes
Texas Reliability Entity	Yes
PJM Interconnection	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes

2. Do you agree with the proposed definition of Control Center?

Organization	Yes or No
NRG Energy Companies	No
PNGC Comment Group	No
Madison Gas and Electric Company	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
NCEMC	No
ACES Power Marketing	No
IRC Standards Review Committee	No
National Rural Electric Cooperative Association (NRECA)	No
Southern California Edison	No

Organization	Yes or No
CenterPoint Energy	No
Manitoba Hydro	No
Xcel Energy	No
Snohomish County PUD	No
Lakeland Electric	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
NV Energy	No
NextEra Energy, Inc.	No
PSEG	No
Texas Reliability Entity	No
Liberty Electric Power LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No

Organization	Yes or No
POrtland General Electric	No
Exelon Corporation and its affiliates	No
Farmington Electric Utility System	No
Indiana Municipal Power Agency	No
Deseret Power	No
Central Lincoln	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
Northeast Power Coordinating Council	Yes
Southwest Power Pool Regional Entity	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes

Organization	Yes or No
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
SPP and Member companies	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Progress Energy	Yes
Western Area Power Administration	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
NIPSCO	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes

Organization	Yes or No
United Illuminating company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
ISO New England Inc.	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
Nebraska Public Power District	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
American Public Power Association	Yes

Organization	Yes or No
Springfield Utility Board	Yes
New York Power Authority	Yes
Wiscsonsin Electric Power Company	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Cowlitz County PUD	Yes
US Bureau of Reclamation	Yes

3. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager?

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Madison Gas and Electric Company	No
MRO NSRF	No
Dominion	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
NCEMC	No
ACES Power Marketing	No
Southern Company Services, Inc.	No
National Rural Electric	No

Organization	Yes or No
Cooperative Association (NRECA)	
Dairyland Power Cooperative	No
Tri-State G&T - Transmission	No
CenterPoint Energy	No
Manitoba Hydro	No
Xcel Energy	No
Bonneville Power Administration	No
MidAmerican Energy Company	No
Ameren	No
NextEra Energy, Inc.	No
Liberty Electric Power LLC	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No
Alliant Energy	No

Organization	Yes or No
Exelon Corporation and its affiliates	No
Deseret Power	No
Brazos Electric Power Cooperative	No
California Independent System Operator	No
Northeast Power Coordinating Council	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
SPP and Member companies	Yes

Organization	Yes or No
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Southern California Edison	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
NIPSCO	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes

Organization	Yes or No
Trans Bay Cable	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Illinois Municipal Electric Agency	Yes
NV Energy	Yes

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
PSEG	Yes
Texas Reliability Entity	Yes
PJM Interconnection	Yes
ISO New England Inc.	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
New York Power Authority	Yes
Wiscsonsin Electric Power Company	Yes

Organization	Yes or No
Farmington Electric Utility System	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

4. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager?

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Madison Gas and Electric Company	No
MRO NSRF	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
CenterPoint Energy	No
Trans Bay Cable	No
Manitoba Hydro	No

Organization	Yes or No
Snohomish County PUD	No
Lakeland Electric	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Ameren	No
NextEra Energy, Inc.	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No
Alliant Energy	No
Exelon Corporation and its affiliates	No
California Independent System Operator	No
Northeast Power Coordinating Council	Yes
NRG Energy Companies	Yes

Organization	Yes or No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Salt River Project	Yes
Southern California Edison	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
NIPSCO	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes

Organization	Yes or No
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Tampa Electric Company	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes

Organization	Yes or No
ISO New England Inc.	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
New York Power Authority	Yes
Wiscsonsin Electric Power Company	Yes
Farmington Electric Utility System	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes

Organization	Yes or No
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

5. Do you agree with the proposed definitions of Electronic Access Control or Monitoring Systems, Interactive Remote Access, and Intermediate Device?

Organization	Yes or No
Salt River Project	No
Trans Bay Cable	No
United Illuminating company	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Texas RE NERC Standards Review Subcommittee	No
Dairyland Power Cooperative	No
Lakeland Electric	No
Illinois Municipal Electric Agency	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Madison Gas and Electric Company	No

Organization	Yes or No
MRO NSRF	No
Duke Energy	No
Florida Municipal Power Agency	No
ACES Power Marketing	No
IRC Standards Review Committee	No
Comment Development SME List	No
CenterPoint Energy	No
NIPSCO	No
Bonneville Power Administration	No
MidAmerican Energy Company	No
Ameren	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No

Organization	Yes or No
Alliant Energy	No
Exelon Corporation and its affiliates	No
Wiscsonsin Electric Power Company	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
Southern California Edison	Yes
ATCO Electric	Yes
Northeast Power Coordinating Council	Yes
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
PPL Corporation NERC	Yes

Organization	Yes or No
Registered Affiliates	
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
NCEMC	Yes
SPP and Member companies	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes

Organization	Yes or No
Ingleside Cogeneration LP	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Tampa Electric Company	Yes
NV Energy	Yes

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
ISO New England Inc.	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
New York Power Authority	Yes
Farmington Electric Utility System	Yes

Organization	Yes or No
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
US Bureau of Reclamation	Yes
Luminant	
American Transmission Company, LLC	

6. Do you agree with the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Madison Gas and Electric Company	No
MRO NSRF	No
FirstEnergy	No
Duke Energy	No
Florida Municipal Power Agency	No
SPP and Member companies	No
IRC Standards Review Committee	No

Organization	Yes or No
Southern California Edison	No
Dairyland Power Cooperative	No
Hydro One	No
NIPSCO	No
Hydro-QuÃ©bec Production	No
Turlock Irrigation District	No
Bonneville Power Administration	No
Lakeland Electric	No
Illinois Municipal Electric Agency	No
NV Energy	No
NextEra Energy, Inc.	No
ISO New England Inc.	No
Nebraska Public Power District	No
Alliant Energy	No
New York Power Authority	No

Organization	Yes or No
Exelon Corporation and its affiliates	No
Wiscsonsin Electric Power Company	No
City Utilities of Springfield, MO	No
NYISO	No
California Independent System Operator	No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Texas RE NERC Standards Review Subcommittee	Yes

Organization	Yes or No
NCEMC	Yes
ACES Power Marketing	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
CenterPoint Energy	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
Independent Electricity System Operator	Yes

Organization	Yes or No
Trans Bay Cable	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Xcel Energy	Yes
Snohomish County PUD	Yes
Tampa Electric Company	Yes
MidAmerican Energy Company	Yes
Massachusetts Municipal	Yes

Organization	Yes or No
Wholesale Electric Company	
Tennessee Valley Authority	Yes
Ameren	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
City of Austin dba Austin Energy	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
Farmington Electric Utility	Yes

Organization	Yes or No
System	
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

7. Do you agree with the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Madison Gas and Electric Company	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
Duke Energy	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
Progress Energy	No

Organization	Yes or No
CenterPoint Energy	No
Hydro One	No
NIPSCO	No
Lower Colorado River Authority	No
LCRA Transmission Services Corporation	No
Xcel Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
NextEra Energy, Inc.	No
ISO New England Inc.	No

Organization	Yes or No
City of Austin dba Austin Energy	No
Utility Services Inc.	No
New York Power Authority	No
Farmington Electric Utility System	No
City Utilities of Springfield, MO	No
NYISO	No
California Independent System Operator	No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes
Dominion	Yes
FirstEnergy	Yes
NCEMC	Yes

Organization	Yes or No
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Southern California Edison	Yes
Dairyland Power Cooperative	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes

Organization	Yes or No
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes

Organization	Yes or No
Ameren	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Nebraska Public Power District	Yes
Alliant Energy	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
Wiscsonsin Electric Power Company	Yes

Organization	Yes or No
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

15. Do you agree with the changes made to the proposed implementation plan since the last formal comment period?

Organization	Yes or No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
Southern California Edison	No
Dairyland Power Cooperative	No
Hydro One	No
Trans Bay Cable	No
Turlock Irrigation District	No
NextEra Energy, Inc.	No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
MRO NSRF	No
NESCOR/NESCO	No
Duke Energy	No

Organization	Yes or No
Southern Company Services, Inc.	No
CenterPoint Energy	No
Consumers Energy Company	No
Manitoba Hydro	No
Snohomish County PUD	No
MidAmerican Energy Company	No
ISO New England Inc.	No
Nebraska Public Power District	No
Alliant Energy	No
New York Power Authority	No
Exelon Corporation and its affiliates	No
NYISO	No
Kansas City Power & Light	No
Texas RE NERC Standards Review Subcommittee	Yes

Organization	Yes or No
United Illuminating company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Brazos Electric Power Cooperative	Yes
Utility Services Inc.	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes

Organization	Yes or No
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes

Organization	Yes or No
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes
Bonneville Power Administration	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Illinois Municipal Electric Agency	Yes
NV Energy	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
PSEG	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
City of Austin dba Austin Energy	Yes

Organization	Yes or No
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
American Public Power Association	Yes
Wiscsonsin Electric Power Company	Yes
Farmington Electric Utility System	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
California Independent System Operator	Yes

Organization	Yes or No
Madison Gas and Electric Company	
Luminant	
American Transmission Company, LLC	

END OF REPORT

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: On September 21, 2012, this draft was revised to clarify references from "generator interface facility" to "generator interconnection Facility" in Attachment 1, criteria 2.4, 2.5, and 2.8. As noted on page 33 of the consideration of comments, form A, the SDT intended to use "generator interconnection Facility." It also corrects instances of incorrect functional model references from "Generation Operator" to "Generator Operator" and corrects the numbering format in Attachment 1, section 3.

No other changes were made to this standard or any of the other CIP V5 standards currently posted, except for a conforming change from "Generation Operator" to "Generator Operator" in the definitions document.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the third posting of Version 5 of the CIP Cyber Security Standards for a 30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the second posting and ballot.

Anticipated Actions	Anticipated Date
30-day Formal Comment Period with Parallel Successive Ballot	September 2012
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-002-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required CIP-002-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-5

3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-5:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Background:

This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.

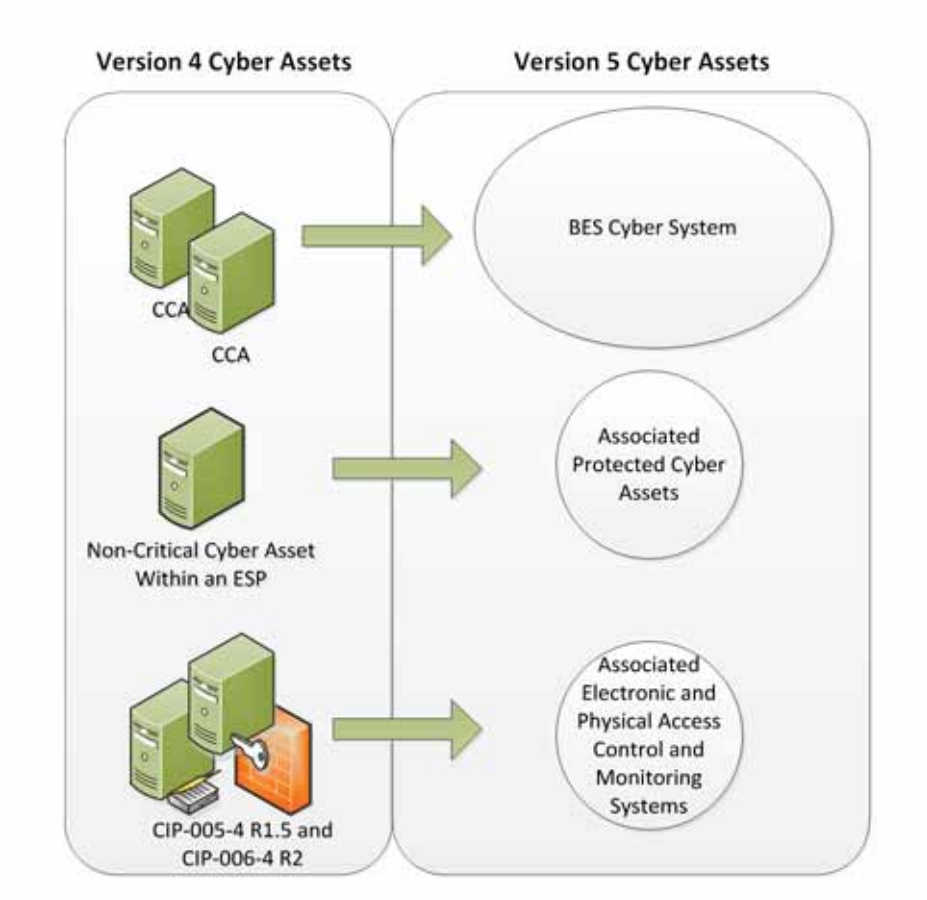

In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets , and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and

scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS") – Examples include: Electronic Access Points, Intermediate Devices, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")– Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA") – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

Rationale – R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts R1.1 through R1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

1. Control Centers and backup Control Centers;
2. Transmission substations and stations;
3. Generation resources;
4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration;
5. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

R1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

R1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

R1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts R1.1 and R1.2.

Rationale – R2

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

R2. The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

R2.1 Review (and update as needed) the identification in Requirement R1 and its parts at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

R2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5 - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation that is connected to three or more other Transmission stations or substations and has an "aggregate weighted values" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission substations and stations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)

- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact that the BES assets that these BES Cyber Systems support, on the reliable operation of the BES.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5, these groups of Facilities, systems, and equipment are designated as BES Assets. For example, an identified BES Asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

<u>High Impact Rating (H)</u>

This category includes those BES Cyber Systems, used by and at Control Centers and associated data centers, that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission

Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, BAs, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of BAs with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the RRO which coordinates actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party), usually in the form of a formal agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for Generation Owners and Generator Operators

which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1. The value of 300 MW is the same value used for UFLS and UVLS.

- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

  It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a

Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

  - 230 kV –> 700 MVA
  - 345 kV –> 1,300 MVA
  - 500 kV –> 2,000 MVA
  - 765 kV –> 3,000 MVA

  In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

  - For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that

are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.

- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.

- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

  In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market.

  The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

  Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

  BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP

standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.

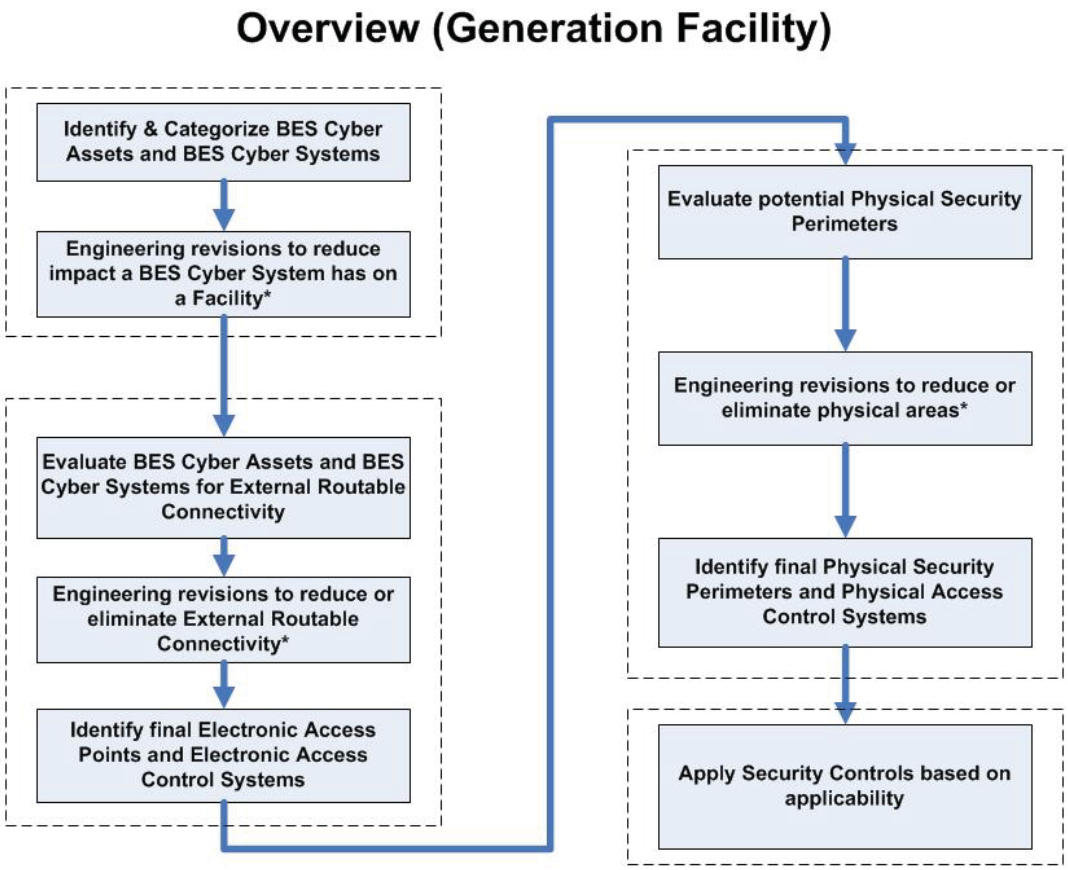

* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: On September 21, 2012, this draft was revised to clarify references from "generator interface facility" to "generator interconnection Facility" in Attachment 1, criteria 2.4, 2.5, and 2.8. As noted on page 33 of the consideration of comments, form A, the SDT intended to use "generator interconnection Facility." It also corrects instances of incorrect functional model references from "Generation Operator" to "Generator Operator" and corrects the numbering format in Attachment 1, section 3.

No other changes were made to this standard or any of the other CIP V5 standards currently posted, except for a conforming change from "Generation Operator" to "Generator Operator" in the definitions document.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the ~~second~~third posting of Version 5 of the CIP Cyber Security Standards for a ~~40~~30-day formal comment period. An initial concept paper, ~~-~~Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5~~-~~, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ~~first~~ ballot.~~–~~ A second posting of Version 5 ~~reverts to the original organization of the standards, with some changes, and~~was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the ~~first~~second posting and ballot.

Anticipated Actions	Anticipated Date
~~40~~30-day Formal Comment Period with Parallel Successive Ballot	~~April~~September 2012
Recirculation ballot	~~June~~November 2012
BOT adoption	~~June~~December 2012

Effective Dates

1. **24 Months Minimum** – ~~The Version 5~~ CIP ~~Cyber Security Standards, except for CIP-003-5, Requirement R2,~~-002-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. ~~CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.~~[1]
2. In those jurisdictions where no regulatory approval is required~~, the Version 5~~ CIP ~~Cyber Security Standards, except for CIP-003-5, Requirement R2,~~-002-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, ~~and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval,~~ or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

~~[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.~~

3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

~~4.~~1. Title: Cyber Security — BES Cyber System Categorization

~~5.~~2. Number: CIP-002-5

~~6.~~3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

~~7.~~4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of ~~Functional Entities~~functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific ~~Functional Entity~~functional entity or subset of ~~Functional Entities~~functional entities are the applicable entity or entities, the ~~Functional Entity~~functional entity or ~~Entities~~entities are specified explicitly.

4.1.1. Balancing Authority

~~7.1.1. Distribution Provider that owns Facilities described in 4.2.2~~

~~7.1.2. Generator Operator~~

~~7.1.3. Generator Owner~~

~~7.1.4. Interchange Coordinator~~

~~7.1.5. Load-Serving Entity that owns Facilities described in 4.2.1~~

~~7.1.6. Reliability Coordinator~~

~~7.1.7. Transmission Operator~~

~~7.1.8. Transmission Owner~~

~~4.2. Facilities:~~

~~7.2.1. Load Serving Entity:~~ ~~One~~one or more of the ~~UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard~~following Facilities, systems, and ~~that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.~~

~~4.2.2~~**4.1.2.** ~~**Distribution Provider**: One or more of the Systems or programs designed, installed, and operated~~equipment for the protection or restoration of the BES:

4.1.2.1. ~~A~~ Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS ~~System~~) system that~~-~~:

4.1.2.1.1. is part of a Load shedding program ~~required by~~that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ~~that~~

~~**4.1.2.1.**~~**4.1.2.1.2.** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. ~~A~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. ~~A~~Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

~~**1.**~~**4.1.2.4.** Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers ~~and Load-Serving Entities~~: :**

~~4.2.3~~All BES Facilities.

~~4.2.4~~**4.2.3.** **Exemptions:** The following are exempt from Standard CIP-002-5:

~~4.2.4.1~~**4.2.3.1.** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.4.2~~**4.2.3.2.** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.4.3~~**4.2.3.3.** ~~In nuclear plants, the Systems~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~8.~~5. **Background:**

This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, ~~Systems~~systems, and equipment~~;~~, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300

MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.

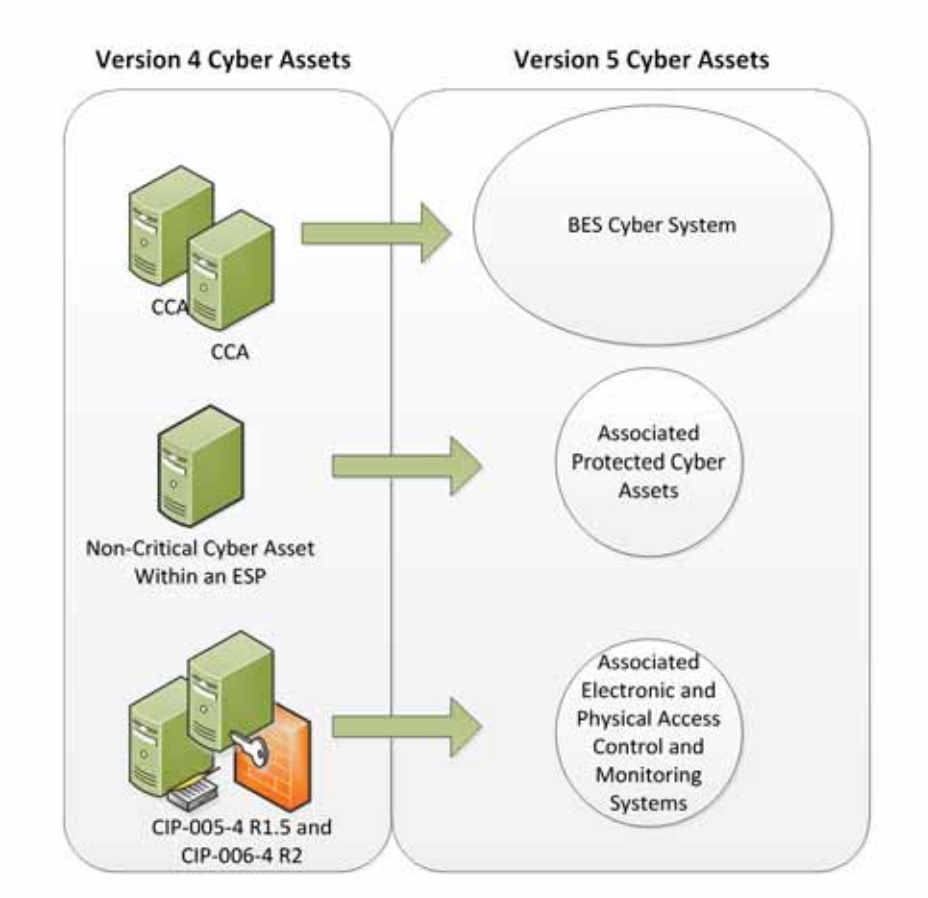

In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets~~. So~~ , and it becomes clearer in the requirement

that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System~~.~~ within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify ~~them~~BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems ~~and their associated BES Cyber Assets~~ for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, ~~Parts~~Criteria 1.1 to 1.4 and ~~Parts~~Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the ~~rest~~remainder of the Version 5 CIP Cyber Security Standards.

~~Associated~~ Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their ~~proximity~~location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS") – Examples include: Electronic Access Points, Intermediate Devices, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems –("PACS")– Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA") – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

~~**Rationale – R1:**~~

~~BES Cyber Systems and their associated BES Cyber Assets have varying impact on the reliable operation of the BES. Once they have been identified, they must be categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to categorize these BES Cyber Systems in accordance with their impact on the BES. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.~~

~~The configuration of the BES is subject to changes due to new demands and requirements for Bulk Power and to environmental changes and operational events. When changes to the BES are planned, the effect of these changes on the set of identified and categorized BES Cyber Systems must be analyzed to ensure that the adequate level of protection is still applied to them.~~

Rationale – R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

R1. Each Responsible Entity shall~~:~~ implement a process that considers each of the following assets for purposes of parts R1.1 through R1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

1. ~~Identify Facilities,~~ Control Centers and backup Control Centers;
2. Transmission substations and stations;
3. Generation resources;
4. Systems~~, or equipment that meet the criteria~~ and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration;

5. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
6. For Distribution Providers, Protection Systems specified in ~~CIP-002-5,~~ Applicability section 4.2.1 above.

~~1.1.~~**R1.1.** Identify each of the high impact BES Cyber Systems according to Attachment 1~~— Impact Rating Criteria Parts 1.1 to~~ , Section 1~~.4 and Parts 2.1 to 2.11;~~ , if any, at each asset;

~~1.2.~~**R1.2.** Identify each ~~high~~of the medium impact BES Cyber ~~System and its associated BES Cyber Asset(s) used for the Facilities,~~ Systems~~, or equipment identified in Requirement R1 Part 1.1~~ according to ~~the criteria contained in CIP-002-5,~~ Attachment 1~~— Impact Rating Criteria;~~ , Section 2, if any, at each asset; and

~~3.~~ Identify each ~~medium~~asset that contains a low impact BES Cyber System ~~and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1~~ according to ~~the criteria contained in CIP-002-5,~~ Attachment 1~~— Impact Rating Criteria;~~

- ~~BES Cyber Systems which are not included in high impact or medium impact shall default to the category of low impact and do not require discrete identification; and~~

~~1.4.~~**R1.3.** ~~Review (and update as needed) the identification in Requirement R1, Parts 1.1, 1.2, and 1.3 within 60 calendar days of when a change to BES Elements or Facilities~~, Section 3, if any (a discrete list of low impact BES Cyber Systems is ~~placed into operation, which is planned to be in service for more than six calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category.~~ not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, ~~Parts 1.1, 1.2 and 1.3, and a list of changes to the BES (with a date for each change) that cause a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.~~ and Parts R1.1 and R1.2.

Rationale – R2

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

R2. The Responsible Entity shall ~~have~~: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

R2.1 Review (and update as needed) the identification in Requirement R1 and its parts at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

~~**R2.**~~**R2.2** Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once ~~each calendar year, not to exceed~~every 15 calendar months ~~between approvals~~, even if it has no identified items in Requirement R1~~, Parts 1.1, 1.2, or 1.3. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*~~.

~~**M2.**~~ **M2.** Acceptable evidence includes, but is not limited to, electronic or physical dated ~~and signed~~ records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate ~~review and update, where applicable, the identification and categorization of Facilities, Systems,~~approve the identifications required in Requirement R1 and ~~equipment, and their associated BES Cyber Systems and BES Cyber Assets,~~its parts at least once ~~each calendar year, not to exceed~~every 15 calendar months ~~between occurrences~~, even if it has none identified in Requirement R1~~, Parts 1.1, 1.2, or 1.3~~ and its parts, as required by ~~requirement~~Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~entity~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain ~~data or~~ evidence ~~for~~of each requirement in this standard for three calendar years~~ or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer~~.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the ~~duration~~time specified above, whichever is longer.
- ~~The Compliance Enforcement Authority~~The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

~~Table of Compliance Elements~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	
~~R1~~	~~Operations Planning~~	~~High~~	~~For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, five percent or fewer Facilities have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1;~~ ~~Or~~ ~~For Responsible Entities with a total of 40 or fewer Facilities, 2 or fewer Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1;~~ ~~Or~~ ~~For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer of high and medium impact BES Cyber Systems have not been identified or categorized or have been incorrectly~~	~~For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than five percent but less than or equal to 10 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1;~~ ~~Or~~ ~~For Responsible Entities with a total of 40 or fewer Facilities, more than two, but fewer than four Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1;~~ ~~Or~~ ~~For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Assets, more than five percent but less than or equal to 10 percent~~	~~For Responsible Entities with more than a total of 40 Facilities in Requirement R1, Part 1.1, more than 10 percent but less than or equal to 15 percent of Facilities have not been identified or have been incorrectly identified, according to Requirement R1, Part 1.1;~~ ~~Or~~ ~~For Responsible Entities with a total of 40 or fewer Facilities, more than four, but fewer than six Facilities in Requirement R1, Part 1.1, have not been identified or have been incorrectly identified according to Requirement R1, Part 1.1;~~ ~~For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Assets, more than 10 percent but less than or equal to 15 percent~~	~~Fo En th Fa Re 1.1 pe ha ide be ide Re 1.1~~ ~~Or~~ ~~Fo En 40 me in Pa be ha ide Re 1.1~~ ~~Or~~ ~~Fo En th hig im Sy pe BE ha ca be~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	
			~~categorized at a lower category;~~ ~~Or~~ ~~For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Assets, five or fewer high and medium impact BES Cyber Assets have not been identified or categorized or have been incorrectly categorized at a lower category;~~ ~~Or~~ ~~The Responsible Entity failed to update its documentation of high and medium impact BES Cyber Assets in accordance with Requirement R1, Part 1.4 for more than 60, but less than or equal to 70 calendar days following the completion of the change.~~	~~of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category;~~ ~~Or~~ ~~For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Assets, more than five but less than or equal to 10 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category;~~ ~~Or~~ ~~The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with Requirement R1, Part 1.4 for more than 70, but less than or equal to 80 calendar days following the completion of the change.~~	~~of identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category;~~ ~~Or~~ ~~For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category;~~ ~~Or~~ ~~The Responsible Entity failed to update its documentation of BES Cyber Assets in accordance with Requirement R1, Part 1.4 for more than 90, but less than or equal to 100 calendar days following the completion of the change.~~	~~ca~~ ~~ca~~ ~~Or~~ ~~Fo~~ ~~En~~ ~~10~~ ~~me~~ ~~Cy~~ ~~th~~ ~~Cy~~ ~~no~~ ~~or~~ ~~inc~~ ~~at~~ ~~Or~~ ~~Th~~ ~~fai~~ ~~de~~ ~~Cy~~ ~~ac~~ ~~Re~~ ~~1.~~ ~~ca~~ ~~fo~~ ~~co~~ ~~ch~~
~~R2~~	~~Operations Planning~~	~~Lower~~	~~The Responsible Entity failed to complete its annual review or approval by the CIP~~	~~The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager~~	~~The Responsible Entity failed to complete its annual review or approval by the CIP Senior Manager~~	~~Th~~ ~~fai~~ ~~an~~ ~~ap~~ ~~Se~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	
			~~Senior Manager according to Requirement R2 for more than 30, but less than or equal to 40 calendar days of the latest required date.~~	~~according to Requirement R2 for more than 40, but less than or equal to 50 calendar days of the latest required date.~~	~~according to Requirement R2 for more than 50, but less than or equal to 60 calendar days of the latest required date.~~	~~ac Re me da re~~

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5 - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center~~,~~ or backup Control Center~~, and associated data centers~~ used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center~~,~~ or backup Control Center~~, and associated data centers~~ used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of ~~1500~~3000 MW in a single Interconnection, or 2) ~~that includes control of~~for one or more of the ~~generation~~ assets that meet ~~criteria~~criterion 2.3, 2.6, ~~and~~or 2.9.

1.3. Each Control Center~~,~~ or backup Control Center~~, and associated data centers~~ used to perform the functional obligations of the Transmission Operator~~, that includes control of~~ for one or more of the assets that meet ~~criteria~~criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center~~,~~ or backup Control Center~~, and associated data centers~~ used to perform the functional obligations of the ~~Generation~~ Generator Operator ~~that includes control~~ for one or more of the assets that meet criterion 2.1~~) for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection or 2) that includes control of one or more of the generation assets that meet criteria~~, 2.3, 2.6, ~~and~~or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1~~,~~ above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of

1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary~~,~~ to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation that ~~are operating between 200 kV and 499 kV, are~~is connected to three or more other Transmission stations or substations~~,~~ and ~~which possess~~has an "aggregate weighted values" exceeding 3000 according to the table below. The "aggregate weighted value" for a ~~Transmission Facility~~single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming ~~or~~and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
~~100kV to 199 kV~~less than 200 kV (not applicable)	~~0~~ (not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, ~~Parts~~criterion 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS~~)~~), or automated switching ~~Systems~~System that operates BES Elements, that, if destroyed, degraded,

misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each ~~System~~system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing ~~Under Voltage Load Shedding~~ undervoltage load shedding (UVLS) or ~~Under Frequency Load Shedding~~underfrequency load shedding (UFLS~~), as required by its regional~~) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control ~~Centers and associated data centers~~Center or backup Control Center, not already included in High Impact Rating (H~~),~~) above, ~~that: (1)~~used to perform the functional obligations of ~~Balancing Authority or Transmission~~the Generator Operator~~, or (2) control~~ for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding ~~300~~1500 MW ~~or more~~in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of ~~BES~~the Transmission Operator not included in High Impact Rating (H), above.

~~2.11.~~2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating (L)

~~Each BES Cyber System associated with:~~

~~**3.1.** BES Facilities not categorized in Section 1 as having a High Impact Rating (H) or Section 2 as having a Medium Impact Rating (M).~~

~~**3.2.** Blackstart Resources.~~

~~**3.3.** Elements in the Cranking Path and initial switching requirements.~~

BES Cyber Systems ~~that are~~ not included in ~~high impact~~Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

4.1. Control Centers and ~~medium impact shall default to the category of low impact~~backup Control Centers.

4.2. Transmission substations and ~~do not require discrete identification~~stations.

4.3. Generation resources.

4.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

4.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

4.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A- BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	~~LSE~~	GOP	GO
Dynamic Response		X	X	X	X	~~X~~	X	X
Balancing Load & Generation	X	X	X	X	X	~~X~~	X	X
Controlling Frequency		X					X	X
Controlling Voltage			X	X	X	~~X~~		X
Managing Constraints	X		X				X	
Monitoring and Control			X				X	
Restoration			X				X	
Situation Awareness	X	X	X				X	
Inter-Entity coordination	X	X	X	X			X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, ~~x-formers~~transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays ~~&~~, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP~~,LSE~~)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP~~,LSE~~)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA) ~~(RC)~~
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP~~,LSE~~)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP~~,LSE~~)

- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day ~~&~~and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers ~~and Load Serving Entities~~

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

~~Similarly, it is expected that only Load-Serving Entities that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. These qualifications are based on the requirements for registration as a Load Serving Entity. Additional qualifications for thresholds in Attachment 1, as specified in Section 4 of CIP-002, also apply.~~

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems ~~and their associated BES Cyber Assets~~ according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of

the impact that the ~~Facilities, Systems and equipment~~BES assets that these BES Cyber Systems support, on the reliable operation of the BES.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for ~~Facilities, Systems and equipment~~BES assets not specified in ~~Parts~~Attachment 1, Criteria 1.1 – 1.4 and ~~Parts~~Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1. ~~While the criteria are based on the scope of the BES Facilities, Systems and equipment, this is used here as a measure of the impact of the BES Cyber System for the purpose of categorization.~~

- When the drafting team uses the term "Facilities", ~~it leaves~~there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5, these groups of Facilities, systems, and equipment are designated as BES Assets. For example, an identified BES Asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers and associated data centers, that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or ~~Generation~~ Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, ~~Parts~~Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named ~~Functional Entities~~functional entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, BAs, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of BAs with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are ~~parts~~criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- ~~Part~~Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used

1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units ~~with capability higher than 1500 MW~~ are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In ~~Part~~Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator as necessary to avoid BES Adverse Reliability Impacts in the ~~long term~~ planning horizon of one year or more are categorized as medium impact. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  ~~In the specification of the "long-term planning horizon," in this criterion, the drafting team sought to ensure that such BES Facilities would be designated in the time horizon described in the NERC document "Time Horizons," which defines long-term planning horizon as "a planning horizon of one year or longer."~~

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, ~~or a Category D contingency as defined in TPL-004,~~ then BES Cyber Systems for that unit are categorized as medium impact.

  ~~Part~~The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the RRO which coordinates actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability

Coordinators or other necessary party), usually in the form of a formal agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  ~~-~~IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- ~~Part~~Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- ~~Part~~Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the ~~Transmission Operator or Balancing Authority, and Generation~~ Generator Operator for an aggregate generation of ~~300~~1500 MW or higher in a single interconnection, and ~~which~~that have not already been included in Part 1. The value of 300 MW is the same value used for UFLS and UVLS. ~~This ensures that Control Centers for significant impact are included. Smaller Control Centers that qualify for the definition of generation Control Centers, but which are really controlling local generation for small downstream generation facilities and do not meet the 300 MW threshold are categorized as low impact.~~

- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

~~Parts~~

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as

stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4~~-2.11~~ through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). ~~Part~~Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- ~~Part~~Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

  It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in ~~Part 1~~Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it ~~doesn't~~does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- ~~Part~~Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.

  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

- 230 kV –> 700 MVA
- 345 kV –> 1,300 MVA
- 500 kV –> 2,000 MVA
- 765 kV –> 3,000 MVA

~~In the case of~~In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

- For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location~~.~~ or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers ~~would~~may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.
  ~~Part~~
- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.
- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

- ~~Part~~Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- ~~Part~~Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in ~~Parts~~Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.

- ~~Part~~Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- ~~Part~~Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of ~~Part~~Criterion 2.~~12~~10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those ~~Under Frequency Load Shedding~~ underfrequency load shedding (UFLS) ~~facilities~~Facilities and ~~Systems~~systems and ~~Under Voltage Load Shedding~~ undervoltage load shedding (UVLS) ~~Systems~~systems and Elements that would be ~~implemented as part of~~ subject to a regional ~~load~~Load shedding requirement to prevent Adverse Reliability Impact. These include automated ~~Under Frequency Load Shedding Systems~~UFLS systems or ~~Under Voltage Load Shedding Systems~~UVLS systems that are capable of ~~load~~Load shedding 300 MW or more. It should be noted that those qualifying ~~Systems~~systems which require a human operator to arm the ~~System~~system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW ~~rating~~Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  ~~Within an operational environment, the drafting team understands that the real-time impact to the Bulk Electric System of a loss of load, or the equivalent amount of generation, will be similar, with loss of load resulting in a frequency high condition and a loss of generation resulting in a frequency low condition.~~ This particular threshold (300 MW) was

provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market.

~~Part 2.11~~The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of ~~Balancing Authorities or Transmission Operators not already categorized as high impact and at generation Control Centers that control generation of 300 MW or more. These include Control Centers for Transmission Owners which perform the function obligation of a Transmission Operator.~~a Transmission Operator and that have not already been categorized as high impact.

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that ~~these~~low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and

other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.

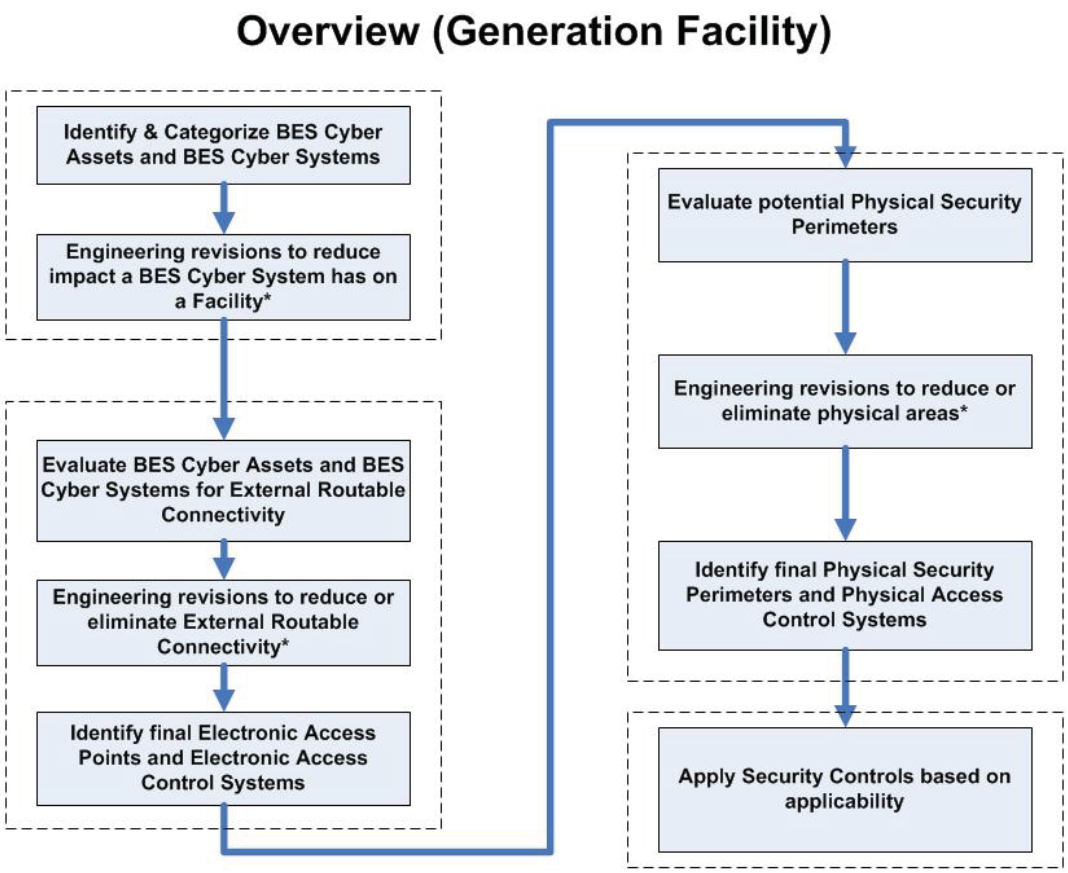

* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: On September 14, 2012, NERC was alerted that the reference to CIP-002-5 in Requirement R2 of CIP-003-5 was incorrect.

This revised draft corrects the reference from "CIP-002-5, Requirement R2, Part R1.3" to "CIP-002-5, Requirement R1, Part R1.3." It is clear by the reference's context that it should be Requirement R1.

No other changes were made to this standard or any of the other CIP V5 standards currently posted.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the third posting of Version 5 of the CIP Cyber Security Standards for a 30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the second posting and ballot.

Anticipated Actions	Anticipated Date
30-day Formal Comment Period with Parallel Successive Ballot	September 2012
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-003-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale – R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale – R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

Review and approval of the cyber security policy at least every 15 calendar months ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- **2.1** Cyber security awareness;
- **2.2** Physical security controls;
- **2.3** Electronic access controls for external routable protocol connections and Dial-up Connectivity; and
- **2.4** Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale – R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale – R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of the initial delegation and any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-5, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not

necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-5, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-5, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: On September 14, 2012, NERC was alerted that the reference to CIP-002-5 in Requirement R2 of CIP-003-5 was incorrect.

This revised draft corrects the reference from "CIP-002-5, Requirement R2, Part R1.3" to "CIP-002-5, Requirement R1, Part R1.3." It is clear by the reference's context that it should be Requirement R1.

No other changes were made to this standard or any of the other CIP V5 standards currently posted.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the ~~second~~third posting of Version 5 of the CIP Cyber Security Standards for a ~~40~~30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ~~first~~ ballot.~~–~~ A second posting of Version 5 ~~reverts to the original organization of the standards with some changes and~~was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the ~~first~~second posting and ballot.

Anticipated Actions	Anticipated Date
~~40~~30-day Formal Comment Period with Parallel Successive Ballot	~~April~~September 2012
Recirculation ballot	~~June~~November 2012
BOT adoption	~~June~~December 2012

Effective Dates

1. **24 Months Minimum** – ~~The Version 5~~ CIP ~~Cyber Security Standards~~-003-5, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. ~~Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.~~[1]

2. In those jurisdictions where no regulatory approval is required, ~~the Version~~ CIP-003-5 ~~CIP Cyber Security Standards~~, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

~~[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	~~Update version from "3" to "4".~~ Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of ~~Functional Entities~~functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific ~~Functional Entity~~functional entity or subset of ~~Functional Entities~~functional entities are the applicable entity or entities, the ~~Functional Entity~~functional entity or ~~Entities~~entities are specified explicitly.

4.1.1 Balancing Authority

~~**4.1.2 Distribution Provider** that owns **Facilities described in 4.2.2**~~

~~**4.1.3 Generator Operator**~~

~~**4.1.4 Generator Owner**~~

~~**4.1.5 Interchange Coordinator**~~

~~**4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1**~~

~~**4.1.7 Reliability Coordinator**~~

~~**4.1.8 Transmission Operator**~~

~~**4.1.9 Transmission Owner**~~

~~**4.2. Facilities:**~~

~~**4.2.1 Load Serving Entity:** One~~one or more of the ~~UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard~~following Facilities, systems, and ~~that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.~~

~~**4.2.2**~~**4.1.2** ~~**Distribution Provider**: One or more of the Systems or programs designed, installed, and operated~~equipment for the protection or restoration of the BES:

4.1.2.1 ~~A~~ Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS ~~System~~) system that~~-~~:

4.1.2.1.1 is part of a Load shedding program ~~required by~~that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ~~that~~

•**4.1.2.1.2** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

•**4.1.2.2** ~~A~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

•**4.1.2.3** ~~A~~Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is ~~required by~~ subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

•**4.2.1.4** Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3 4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: : All BES Facilities.

All BES Facilities.

4.2.4 4.2.3 Exemptions: The following are exempt from Standard CIP-002003-5:

4.2.4.1 4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 4.2.3.3 In nuclear plants, the SystemsThe systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 -For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Measures provide examples of evidence to show documentation and implementation of the requirement. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess,

and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

~~These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as ~~they feel~~it believes necessary in their documented processes, but they must address the applicable requirements. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the ~~table~~preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale – R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall ~~implement~~review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 Personnel ~~security;~~& training (CIP-004);

~~**1.2**~~ Electronic Security Perimeters~~;~~

~~**1.3**~~**1.2** (CIP-005) including Interactive Remote Access;

~~**1.4**~~**1.3** Physical security~~;~~ of BES Cyber Systems (CIP-006);

~~**1.5**~~**1.4** System security~~;~~ management (CIP-007);

~~**1.6**~~**1.5** Incident reporting and response~~;~~ planning (CIP-008);

~~**1.7**~~**1.6** Recovery plans~~;~~ for BES Cyber Systems (CIP-009);

~~**1.8**~~**1.7** Configuration change management~~;~~ and vulnerability assessments (CIP-010);

~~**1.9**~~**1.8** Information protection~~;~~ (CIP-011); and

~~**1.10**~~**1.9** ~~Provisions for declaring~~Declaring and responding to CIP Exceptional Circumstances.

~~**M1.** Evidence must include~~**M1.** Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale – R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

Review and approval of the cyber security policy at least every 15 calendar months ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Cyber security awareness;

2.2 Physical security controls;

2.3 Electronic access controls for external routable protocol connections and Dial-up Connectivity; and

2.4 Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics.; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. For BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics: *[Violation Risk Factor: Low] [Time Horizon: Operations Planning]*

2.1 Cyber security awareness;

2.2 Physical access control;

2.3 Electronic access control; and

2.4 Incident response to a BES Cyber Security Incident.

An inventory, list, or discrete identification of BES Cyber Systems is not required.

M2. Evidence must include one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics.

Rationale – R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests that the SDT consider whether the single senior manager should be a corporate officer or equivalent. ~~The SDT believes that the requirement that the senior manager have~~ As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name~~.~~ and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. ~~Evidence~~ An example of evidence may include, but is not limited to~~:~~

- ~~A~~, a dated and ~~signed~~approved document from a high level official designating the name of the individual identified as the CIP Senior Manager~~; or~~.

- ~~A dated organizational chart designating the name of the individual identified as the CIP Senior Manager.~~

Rationale – R4:

~~Annual review and approval~~The intent of the ~~cyber~~requirement is to ensure clear accountability within an organization for certain security ~~policy~~matters. It also ensures that ~~the policy is~~ delegations are kept up-to-date and ~~periodically reaffirms management's commitment to~~ that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the ~~protection of its BES Cyber Systems.~~ 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With

~~**R4.** Each Responsible Entity shall review and obtain CIP Senior Manager approval for cyber security policies identified in Requirements R1 and R2, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*~~

~~**M4.** Evidence may include, but is not limited to:~~

1. ~~Revision history, records of review, or workflow evidence from a document management system that indicate annual review of each cyber security policy; and~~
2. ~~A dated signature by the CIP Senior Manager for each cyber security policy that indicates annual approval.~~

~~**Rationale – R5:**~~

~~The intent of the requirement is to ensure clear accountability within an organization for certain security matters.~~

~~In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.~~

~~**R5.**~~

R4. The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation~~, and~~; approved by the CIP Senior Manager; and updated within 30 days of the initial delegation and any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

~~**M5.** Evidence~~**M4.** An example of evidence may include, but is not limited to, a dated document, ~~signed~~approved by the CIP Senior Manager, listing ~~named personnel~~individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

~~**Rationale – R6:**~~

~~The intent of the requirement is to ensure that delegations are kept up-to-date and that individuals do not assume undocumented authority.~~

~~**R6.** Each Responsible Entity shall document any changes to the CIP Senior Manager or any delegations within thirty calendar days of the change. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*~~

~~**M6.** Evidence may include, but is not limited to, dated documentation that includes the name of the CIP Senior Manager or documentation that includes the names or titles of any delegations, that is current to within 30 days with the name or title of anyone who performed a required approval or authorization.~~

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~entity~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain ~~data or~~ evidence ~~for~~of each requirement in this standard for three calendar years~~ or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer~~.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the ~~duration~~time specified above, whichever is longer.
- ~~The Compliance Enforcement Authority~~The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

~~Table of Compliance Elements~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1~~	~~Operations Planning~~	~~Medium~~	~~N/A~~	~~N/A~~	~~The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required Parts 1.1 to 1.10.~~	~~The Responsible Entity has not implemented any cyber security policy,~~ ~~Or~~ ~~The Responsible Entity has implemented at least one policy but has failed to address two or more of the required Parts 1.1 to 1.10.~~
~~R2~~	~~Operations Planning~~	~~Medium~~	~~N/A~~	~~N/A~~	~~The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required Parts 2.1 to 2.4.~~	~~The Responsible Entity has not implemented any cyber security policy,~~ ~~Or~~ ~~The Responsible Entity has implemented at least one policy but has failed to address two or more of the required Parts 2.1 to 2.4.~~
~~R3~~	~~Operations~~	~~Medium~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity has not identified, by~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning					name, a single senior management official ("the CIP Senior Manager") with overall authority and responsibility for leading and managing implementation of the requirements within the CIP group of standards.
R4	Operations Planning	Lower	N/A	N/A	The Responsible Entity has reviewed its cyber security policy or policies, but not all of them have been approved by the CIP Senior Manager within the required time period.	The Responsible Entity has not reviewed the cyber security policy or policies and the CIP Senior Manager has not approved all of them within the required time period.
R5	Operations Planning	Lower	N/A	The Responsible Entity failed to document the approval and authorization of one delegation (by title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of two delegations (by title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of three or more delegations (by title or name of the delegate) as required.

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R6~~	~~Operations Planning~~	~~Lower~~	~~N/A~~	~~NA~~	~~Change to one delegation was not documented within 30 calendar days of the effective date.~~	~~A change to the CIP Senior Manager, Or more than one delegation was not documented within 30 calendar days of the effective date.~~

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the ~~10~~nine topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-5, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel ~~Security~~& training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account ~~Management~~management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points

~~1.3. Remote Access~~

- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating ~~system~~systems and applications used to initiate ~~the Interactive Remote Access before initiating~~ Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

~~1.4~~1.3 Physical ~~Security~~security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress ~~and egress~~

~~1.5~~1.4 System ~~Security~~security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

~~1.6~~1.5 Incident ~~Response~~reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.~~7~~6 Recovery ~~Plans~~plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.~~8~~7 Configuration ~~Change Management~~change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.~~9~~8 Information ~~Protection~~protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

~~1.10 Provisions for~~1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a ~~compliance~~reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

~~**Requirement**~~ In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the ~~4~~four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the

audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not necessary. The SDT also notes that in ~~topics 2.2 and~~topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

~~In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.~~

~~**Requirement R5**~~The intent of CIP-003-5, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-5, Requirement ~~R5~~R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the ~~Standard Drafting Team~~SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. ~~As detailed in the examples provided in the Measure, a~~ A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

~~**Requirement R6:**~~

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the third posting of Version 5 of the CIP Cyber Security Standards for a 30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the second posting and ballot.

Anticipated Actions	Anticipated Date
30-day Formal Comment Period with Parallel Successive Ballot	September 2012
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-004-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-004-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-5

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-5:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

Requirements and Measures

Rationale for R1: Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices and associated physical security practices for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).
Reference to prior version: *CIP-004-4, R1*		**Change Rationale:** *Changed to remove the need to ensure or prove everyone with authorized* electronic or authorized unescorted physical *access "received" ongoing reinforcement – to state that security awareness has been reinforced.* *Moved example mechanisms to guidance.*	

Rationale for R2: To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:
   - The visitor control program
   - Electronic interconnectivity supporting the operation and control of BES Cyber Systems
   - Storage media as part of the handling of BES Cyber Systems information
2. Change references from Critical Cyber Assets to BES Cyber Systems.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
Reference to prior version: *CIP004-4, R2.2.1*		**Change Rationale:** *Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
Reference to prior version: *CIP004-4, R2.1*		**Change Rationale:** *Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.*	
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.
Reference to prior version: *CIP004-4, R2.3*		**Change Rationale:** *Updated to replace "annually" with "once every 15 calendar months."*	

Rationale for R3: To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Addressed interpretation request in guidance. Specified that identity confirmation is only required for each individual's initial assessment. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.*	

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.*	

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
Reference to prior version: *NEW*		Change Rationale: *There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.*	
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.
Reference to prior version: *CIP-004-4, R3.3*		Change Rationale: *Separated into its own table item.*	

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.
Reference to prior version: *CIP-004-3, R3, R3.3*		**Change Rationale**: *Whether for initial access or maintaining access, establishes that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment.*	

Rationale for R4: To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.
Reference to prior version: *CIP 003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1*		**Change Rationale:** Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
Reference to prior version: *CIP 004-4, R4.1*		**Change Rationale:** *Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.*	

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.
Reference to prior version: *CIP 007-4, R5.1.3*		**Change Rationale:** *Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary.*	

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.
Reference to prior version: *CIP-003-4, R5.1.2*		**Change Rationale:** *Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.*	

Rationale for R5: The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate."

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R5 – Access Revocation*. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
Reference to prior version: *CIP 004-4, R4.2*		**Change Rationale:** *The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards* ***to require immediate revocation*** *for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*	

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
Reference to prior version: *CIP-004-4, R4.2*		**Change Rationale:** *FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.*	

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date and time of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.
Reference to prior version: *NEW*		**Change Rationale:** *FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.*	

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
Reference to prior version: *NEW*		**Change Rationale:** *FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.*	

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.
Reference to prior version: *CIP-007-4, R5.2.3*		**Change Rationale:** *To provide clarification of expected actions in managing the passwords.*	

Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Regional Variances

None.

Interpretations

None.

Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1: The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and does not require reconfirmation during the tenure of employment.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

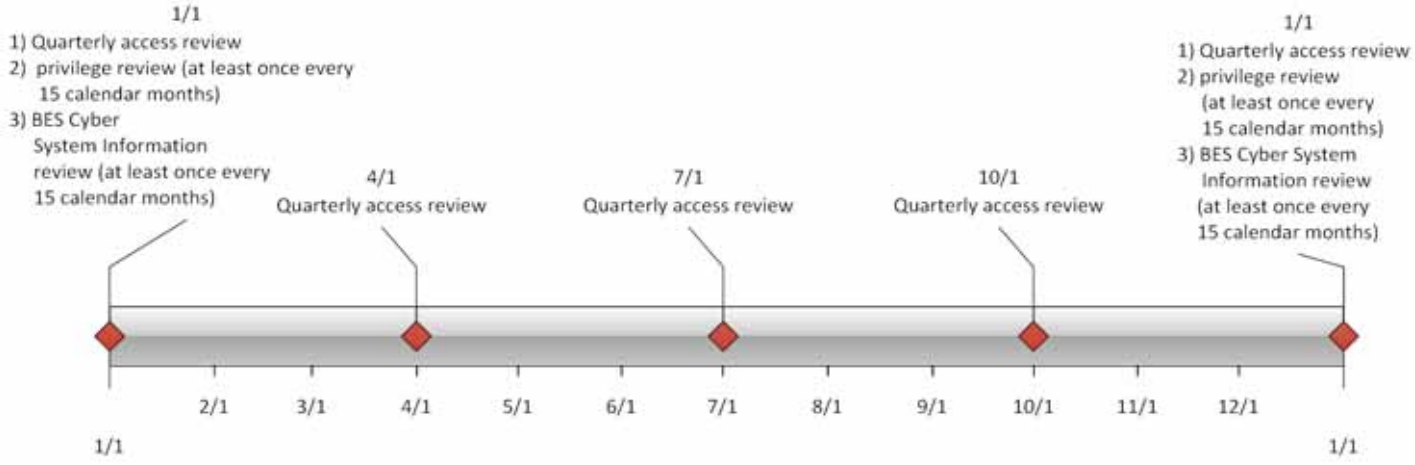

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the ~~second~~third posting of Version 5 of the CIP Cyber Security Standards for a ~~40~~30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ~~first~~ ballot.~~–~~ A second posting of Version 5 ~~reverts to the original organization of the standards with some changes and~~was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the ~~first~~second posting and ballot.

Anticipated Actions	Anticipated Date
~~40~~30-day Formal Comment Period with Parallel Successive Ballot	~~April~~September 2012
Recirculation ballot	~~June~~November 2012
BOT adoption	~~June~~December 2012

Effective Dates

1. **24 Months Minimum** – ~~The Version 5~~ CIP ~~Cyber Security Standards, except for CIP-003-5, Requirement R2,~~ -004-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. ~~CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.~~[1]

2. In those jurisdictions where no regulatory approval is required, ~~the Version~~ CIP-004-5 ~~CIP Cyber Security Standards, except for CIP-003-5, Requirement R2,~~ shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, ~~and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees approval,~~ or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] ~~In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

~~A.~~ Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-5

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems ~~against compromise that could lead to misoperation or instability in the BES.~~.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of ~~Functional Entities~~functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific ~~Functional Entity~~functional entity or subset of ~~Functional Entities~~functional entities are the applicable entity or entities, the ~~Functional Entity~~functional entity or ~~Entities~~entities are specified explicitly.

   4.1.1. Balancing Authority

   ~~**4.1.2. Distribution Provider** that owns **Facilities described in 4.2.2**~~

   ~~**4.1.3. Generator Operator**~~

   ~~**4.1.4. Generator Owner**~~

   ~~**4.1.5. Interchange Coordinator**~~

   ~~**4.1.6. Load-Serving Entity that owns Facilities described in 4.2.1**~~

   ~~**4.1.7. Reliability Coordinator**~~

   ~~**4.1.8. Transmission Operator**~~

   ~~**4.1.9. Transmission Owner**~~

   ~~**4.2. Facilities:**~~

   ~~**4.2.1. Load Serving Entity:** One~~one or more of the ~~UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard~~following Facilities, systems, and ~~that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.~~

   ~~**4.2.2**~~**4.1.2.** ~~**Distribution Provider**: One or more of the Systems or programs designed, installed, and operated~~equipment for the protection or restoration of the BES:

   4.1.2.1. ~~A~~ Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS ~~System~~) system that~~-~~:

4.1.2.1.1. is part of a Load shedding program ~~required by~~that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ~~that~~

•**4.1.2.1.2.** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

•**4.1.2.2.** ~~A~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

•**4.1.2.3.** ~~A~~Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

•**4.1.2.4.** Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~4.2.3~~4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers ~~and Load-Serving Entities~~: ~~All BES Facilities.~~:

All BES Facilities.

~~4.2.4~~4.2.3. Exemptions: The following are exempt from Standard CIP-~~002~~004-5:

~~4.2.4.1~~4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.4.2~~4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.4.3~~4.2.3.3. ~~In nuclear plants, the Systems~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for ~~a~~the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as ~~they feel~~it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

~~Applicability Columns in Tables:~~

~~Each table row~~ Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an ~~applicability~~"Applicable Systems" column to further define the scope of systems to which a specific requirement row applies ~~to BES Cyber Systems and associated Cyber Assets~~. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the ~~applicability~~"Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~.
- **~~Associated~~ Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber

System~~ in the applicability column~~. Examples include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- ~~**Associated** ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity~~ in the applicability column~~.

~~B.~~Requirements and Measures

Rationale for R1: Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R1 – Security Awareness Program			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	~~A security~~Security awareness ~~program~~ that, at least once each calendar quarter, ~~conveys ongoing reinforcement of~~reinforces cyber security practices and associated physical security practices for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	~~Evidence must include the documented security awareness program, and additional~~ An example of evidence ~~to demonstrate that this program was implemented. Evidence of implementation~~ may include, but is not limited to, documentation that the quarterly reinforcement has been provided. ~~Evidence~~ Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).
Reference to prior version: *CIP-004-4, R1*		**Change Rationale:** *Changed to remove the need to ensure or prove everyone with authorized* electronic or authorized unescorted physical *access "received" ongoing reinforcement – to state that ~~the program conveys~~security awareness ~~and measures that reinforcement "~~has been ~~provided."~~reinforced.* *Moved example mechanisms to guidance.*	

CIP-004-5 Table R1 – Security Awareness Program			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
		~~*Changed to record delivery.*~~	

Rationale for R2: To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems ~~-~~covers the proper policies, access controls, and procedures to protect BES Cyber Systems~~.~~ and are trained before access is authorized.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:
   - The visitor control program
   - Electronic interconnectivity supporting the operation and control of BES Cyber Systems
   - Storage media as part of the handling of BES Cyber Systems information
2. Change references from Critical Cyber Assets to BES Cyber Systems.

R2. Each Responsible Entity shall ~~have~~implement, in a ~~role-based~~manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to ~~attain and retain authorized electronic access~~individual roles, functions, or ~~authorized unescorted physical access to BES Cyber Systems that~~ responsibilities that collectively includes each of the applicable ~~items~~requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable ~~items~~requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program*~~.~~ and additional evidence to demonstrate implementation of the program(s).

CIP-004-5 Table R2 – Cyber Security Training Program			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
~~2.1~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Identification of each role and training required for each role.~~	~~Acceptable evidence must include a list of roles and what training is needed for each role.~~
~~**Reference to prior version:** NEW~~		~~**Change Rationale:** *The first thing needed in a role-based training program is to understand what roles individuals have so that the Responsible Entity can plan what training modules it needs to provide.*~~	

~~2.2~~**Part**	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring~~**Applicable Systems**	~~Training content on the cyber security policies protecting the Responsible Entity's BES Cyber Systems.~~**Requirements**	~~Evidence may include, but is not limited to, training material on the security controls that have been implemented to protect BES Cyber Systems.~~**Measures**
~~**Reference to prior version:**~~ ~~*CIP004-4, R2.2.1*~~	~~**Change Rationale:** *Removed to address cyber security issues, not the business function. The previous version was focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security.*~~		

CIP-004-5 Table R2 – Cyber Security Training Program				
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~	
2.~~3~~1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS		Training content on ~~the physical~~: 2.1.1. Cyber security policies; 2.1.2. Physical access controls ~~protecting the Responsible Entity's~~; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials ~~on the proper use of physical access controls for BES Cyber Systems.~~.
			2.1.9. Cyber security risks associated with a BES Cyber System's	

CIP-004-5 Table R2 – Cyber Security Training Program			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
~~**Reference to prior version:**~~ ~~*CIP004-4, R2.2.1 and R2.2.2*~~		~~**Change Rationale:** *Minor wording changes.*~~	

CIP-004-5 Table R2 – Cyber Security Training Program			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
Reference to prior version: *CIP004-4, R2.2.4.1*	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Training content on the electronic access controls protecting the Responsible Entity's BES Cyber Systems.~~	**Change Rationale:** *Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.* ~~Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the electronic access controls to protect BES Cyber Systems.~~

CIP-004-5 Table R2 – Cyber Security Training Program			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
~~**Reference to prior version:**~~ ~~*CIP004-4, R2.2.1 and R2.2.2*~~		~~**Change Rationale:** *Minor wording changes.*~~	
~~2.5~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Training content on the visitor control program.~~	~~Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the visitor control program.~~
~~**Reference to prior version:**~~ ~~*NEW*~~		~~**Change Rationale:** *No significant change from previous versions.*~~	

CIP-004-5 Table R2 – Cyber Security Training Program			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
~~2.6~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Training content on handling of BES Cyber System Information and its storage.~~	~~Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the handling of BES Cyber System Information, including its storage.~~
~~**Reference to prior version:**~~ ~~*CIP004-4, R2.2.3*~~		~~**Change Rationale:** *Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage media; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16.*~~	

CIP-004-5 Table R2 – Cyber Security Training Program				
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~	
2.~~7~~2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS		~~Training content on identification of a potential BES Cyber Security Incident and initial notifications in accordance with the entity's incident response plan~~ Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to, training ~~material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the identification of a potential BES Cyber Security Incident~~records and ~~associated notifications~~documentation of when CIP Exceptional Circumstances were invoked.
Reference to prior version: ~~*CIP-004-4, R2.2.4 (new; implied but not stated in CIP-004-4 or CIP-008-4)*~~*CIP004-4, R2.1*			**Change Rationale:** ~~*Core training on the identification and reporting*~~*Addition of* ~~*a Cyber Security Incident;*~~ *exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph* ~~*413; Related to*~~*431 is detailed in CIP-*~~*008*~~*003-5*~~*& DHS Incident Reporting requirements for those with roles in incident reporting*~~.	

CIP-004-5 Table R2 – Cyber Security Training Program				
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~	
2.~~8~~3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS		~~Training content on recovery plans for BES Cyber Systems.~~Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to, dated individual training ~~material such as power point presentations, instructor notes, student notes, handouts, or other training materials on recovery plans for BES Cyber Systems~~records.
Reference to prior version: *CIP004-4, R2.~~2.4~~3*			~~**Change Rationale:**~~ **Change Rationale:** *Updated to replace "annually" with "once every 15 calendar months."* ~~*Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413.*~~	

CIP-004-5 Table R2 – Cyber Security Training Program			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
~~2.9~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Training content on response to BES Cyber Security Incidents.~~	~~Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the response to a BES Cyber Security Incident.~~
~~**Reference to prior version:**~~ ~~*CIP004-4, R2.2.4*~~		~~**Change Rationale:** *Minor wording changes.*~~	

CIP-004-5 Table R2 – Cyber Security Training Program			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
~~2.10~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Training content on risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.~~	~~Evidence may include, but is not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials on the electronic interconnectivity and interoperability with other Cyber Assets.~~
~~**Reference to prior version:**~~ ~~*NEW*~~		~~**Change Rationale:** *Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.*~~	

~~**Rationale for R3:** To ensure that personnel with authorized electronic access or authorized unescorted physical access are trained in the policies, access controls, and procedures to protect the BES Cyber Systems.~~

~~**Summary of Changes:** Re-organization of the training requirements into the respective requirements for "program" and "implementation" of the training.~~

~~**R3.** Each Responsible Entity shall implement its documented role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R3 - Cyber Security Training. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*~~

~~**M3.** Evidence must include, but is not limited to, documentation that the training was provided as defined in *CIP-004-5 Table R3 - Cyber Security Training.*~~

~~**CIP-004-5 Table R3 – Cyber Security Training**~~			
~~**Part**~~	~~**Applicable BES Cyber Systems and associated Cyber Assets**~~	~~**Requirements**~~	~~**Measures**~~
~~3.1~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Require completion and documentation of the training specified in CIP-004-5, Requirement R2 prior to granting authorized electronic access and authorized unescorted physical access to BES Cyber Systems, except during CIP Exceptional Circumstances.~~	~~Evidence may include, but is not limited to, for each individual requiring authorized electronic or authorized unescorted physical access, dated individual training records, the date authorized electronic or authorized unescorted physical access was first granted, or a dated log or documentation of when CIP Exceptional Circumstances were invoked and revoked.~~
~~**Reference to prior version:**~~ ~~*CIP004-4, R2.1*~~		~~**Change Rationale:** *Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.*~~	

~~CIP-004-5 Table R3 – Cyber Security Training~~			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
~~3.2~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Require completion and documentation of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months.~~	~~Evidence may include, but is not limited to, dated individual training records.~~
~~**Reference to prior version:**~~ ~~*CIP004-4, R2.3*~~		~~**Change Rationale:** *Updated to further define what "Annual" training means.*~~	

~~**Rationale for R4:** To ensure that individuals who need authorized electronic or unescorted physical access to BES Cyber Systems have been assessed for risk.~~

~~**Summary of Changes:** Specify that the seven year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.~~

~~**R4.** Each Responsible Entity shall have~~

Rationale for R3: To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively ~~includes~~include each of the applicable ~~items~~requirement parts in *CIP-004-5 Table ~~R4~~R3 – Personnel Risk Assessment Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

~~M4~~M3. Evidence must include the documented personnel risk assessment ~~program~~programs that collectively ~~includes~~include each of the applicable ~~items~~requirement parts in *CIP-004-5 Table ~~R4~~R3 – Personnel Risk Assessment Program~~.~~* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5 Table ~~R4~~R3 – Personnel Risk Assessment Program			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
~~4~~3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~ EACMS; and 2. PACS	~~An initial personnel risk assessment ("PRA") that includes~~Process to confirm identity ~~verification~~.	~~Acceptable~~An example of evidence ~~must~~may include, but is not limited to, documentation of the ~~documented personnel risk assessment program with a requirement for an initial personnel risk assessment that includes~~Responsible Entity's process to confirm identity ~~verification~~.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Addressed interpretation request in guidance. Specified that identity ~~verification~~confirmation is only required for each individual's initial assessment. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.*	

CIP-004-5 Table ~~R4~~R3 – Personnel Risk Assessment Program			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
~~4~~3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~ EACMS; and 2. PACS	~~Seven~~ Process to perform a seven year criminal history records check ~~including~~as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration~~,~~; and ~~covering at least all~~ 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has~~,~~ resided for six consecutive months or more~~:~~. ~~4.2.1. resided;~~ ~~4.2.2. been employed (if applicable); and~~ ~~4.2.3. attended school (if applicable).~~ If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	~~Acceptable~~An example of evidence ~~must~~may include, but is not limited to, documentation of the ~~documented personnel risk assessment program with a requirement for~~Responsible Entity's process to perform a seven~~-~~ year criminal history ~~record~~records check ~~in accordance with this part.~~ ~~.~~

Reference to prior version: *CIP004-4, R3.1*	**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided~~, been employed, and/or attended school~~ for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.*

CIP-004-5 Table R4R3 – Personnel Risk Assessment Program			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
43.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivityand their associated: Associated Physical Access Control Systems 1. Associated Electronic Access Control or Monitoring Systems EACMS; and 2. PACS	Process or criteria used to evaluate personnel risk assessments to determine when to deny authorizedcriminal history records checks for authorizing access.	AcceptableAn example of evidence mustmay include, but is not limited to, documentation of the documented personnel risk assessment program with theResponsible Entity's process or criteria identifiedto evaluate criminal history records checks.
Reference to prior version: *NEW*		Change Rationale: *There should be documented criteria or a process used to evaluate personnel risk assessmentscriminal history records checks for authorizing access.*	

~~4~~3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~ EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted ~~pursuant~~according to ~~CIP-004-5 R4,~~ Parts ~~4~~3.1 through ~~4~~3.3.	~~Acceptable~~An example of evidence ~~must~~may include, but is not limited to, documentation of the ~~documented personnel risk assessment program with the~~Responsible Entity's criteria or process ~~identified~~for verifying contractors or service vendors personnel risk assessments.
Reference to prior version: *CIP-004-4, R3.3*		Change Rationale: *Separated into its own table item.*	

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**

3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.
Reference to prior version: *CIP-004-3, R3, R3.3*		**Change Rationale**: *Whether for initial access or maintaining access, establishes that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment.*	

~~**Rationale for R5:** To ensure that individuals who have authorized access to BES Cyber Systems have been assessed for risk.~~

~~**R5.**~~

Rationale for R4: To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

R4. Each Responsible Entity shall implement ~~one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems~~, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

~~collectively include each of the applicable elements in *CIP-004-5 Table R5 – Personnel Risk Assessment. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*~~

~~**M5.** Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-004-5 Table R5 – Personnel Risk Assessment* and additional evidence to demonstrate that these processes were implemented as described in the Measures column of the table.~~

~~CIP-004-5 Table R5 – Personnel Risk Assessment~~			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirement~~	~~Measures~~
~~5.1~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Have a personnel risk assessment performed as specified in CIP-004-5, Requirement R4 prior to being granted authorized electronic or authorized unescorted physical access, except for CIP Exceptional Circumstances.~~	~~Evidence may include, but is not limited to:~~ • ~~Dated records showing that personnel risk assessments were completed before authorized electronic or authorized unescorted physical access was authorized; or~~ • ~~Dated records showing that, before authorized electronic or authorized unescorted access was authorized, the Responsible Entity received dated documentation or attestations from contractors or service vendors verifying that personnel risk assessments were conducted pursuant to CIP-004-5, Requirement R4.~~
~~**Reference to prior version:**~~ ~~*CIP-004-3, R3, R3.3*~~		~~**Change Rationale**: *Minor wording changes and added the ability to accept attestations from contractors or vendors.*~~	

~~CIP-004-5 Table R5 – Personnel Risk Assessment~~			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirement~~	~~Measures~~
~~5.2~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Update each personnel risk assessment at least once every seven calendar years after the initial or previous personnel risk assessment such that the current PRA is no older than seven years.~~	~~Evidence may include, but is not limited to, current and previous personnel risk assessment records.~~
~~**Reference to prior version:**~~ ~~*CIP-004-4, R3.2*~~		~~**Change Rationale:** *Eliminated the "for cause" renewal.*~~	

~~**Rationale for R6:** To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.~~

~~Access is physical, logical, and remote permissions granted to all Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).~~

~~CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.~~

~~Quarterly reviews in Part 6.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.~~

~~If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.~~

~~For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R6 are not applicable. However, the Responsible Entity should document such configurations.~~

~~**Summary of Changes:** The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.~~

~~**R6.** Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in *CIP-004-5 Table R6 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*~~

~~M6~~M4. Evidence must include the documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-004-5 Table ~~R6~~R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

~~**Reference to prior version:**~~ ~~*CIP-003-4, R5.1; CIP-007-4, R5.1.1*~~		~~**Change Rationale:** Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent.~~	
~~**CIP-004-5 Table R6 – Access Management Program**~~			
~~**Part**~~	~~**Applicability**~~	~~**Requirements**~~	~~**Measures**~~
~~6.2~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances.~~	~~Evidence may include, but is not limited to, a signed document, automated workflow approval, or email showing persons with electronic access have authorization, and similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.~~

CIP-004-5 Table ~~R6~~R4 – Access Management Program			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Reference to prior version: *CIP 003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1*	**Change Rationale:** Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*

6.34.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivityand their associated: Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems 1. EACMS; and 2. PACS	The individual(s) designated in Part 6.1 shall authorize unescorted physical access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances. Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	EvidenceExamples of evidence may include, but isare not limited to, : • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of people with unescorted physical access, a signed document, automated workflow approval, or email showing persons with unescorted physicalpersonnel who have access have (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization, and similar forms) and a list of individuals provisioned for access (i.e., provisioning forms or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.shared account listing).

Reference to prior version:	**Change Rationale:** *Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.*
CIP 004-4, R4.1	

~~CIP-004-5 Table R6 – Access Management Program~~			
~~**Part**~~	~~**Applicability**~~	~~**Requirements**~~	~~**Measures**~~

~~6.4~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~The individual(s) designated in Part 6.1 shall authorize access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determines are necessary for performing assigned work functions, except for CIP Exceptional Circumstances.~~	~~A signed document, automated workflow approval or email showing persons with access to BES Cyber System Information have authorization, and similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization.~~
~~**Reference to prior version:**~~ ~~*CIP-003-4, R5.2*~~		~~**Change Rationale:** *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003 and CIP-007 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*~~	

~~CIP-004-5 Table R6 – Access Management Program~~			
~~Part~~	~~Applicability~~	~~Requirements~~	~~Measures~~
~~6.5~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Verify at least once each calendar quarter that individuals provisioned for authorized electronic access or authorized unescorted physical access have associated authorization records.~~	~~Evidence may include, but is not limited to:~~ ~~• Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or~~ ~~• Documentation of the dated verification between a list of individuals who have been authorized for access (i.e. authorization forms) and a list of individuals provisioned for access (i.e. provisioning forms or shared account listing).~~

CIP-004-5 Table ~~R6~~R4 – Access Management Program			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**
~~6.6~~4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. EACMS; and 2. PACS	For electronic access, verify at least once ~~each calendar year, not to exceed~~every 15 calendar months ~~between verifications,~~ that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary ~~for performing assigned work functions~~.	~~Evidence~~An example of evidence may include, but is not limited to, documentation of the review ~~including~~that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.
Reference to prior version: *CIP 007-4, R5.1.3*		**Change Rationale:** *Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary ~~for performing assigned work functions.~~.*	

CIP-004-5 Table ~~R6~~R4 – Access Management Program			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**
~~6.7~~4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. EACMS; and 2. PACS	Verify at least once ~~per calendar year, but not to exceed~~every 15 calendar months ~~between verifications,~~ that access to the ~~physical and electronic~~designated storage locations ~~where~~for BES Cyber System Information ~~is stored by the Responsible Entity~~, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	~~Evidence~~An example of evidence may include, but is not limited to, the ~~following~~ documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.
Reference to prior version: *CIP-003-4, R5.1.2*		**Change Rationale:** *Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.*	

Rationale for R5~~7~~: The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (~~i.e.~~e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to all Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate."

~~**R7**~~

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable ~~items~~requirement parts in *CIP-004-5 Table ~~R7~~R5 – Access Revocation. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning].*

~~M7~~M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable ~~items~~requirement parts in *CIP-004-5 Table ~~R7~~R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table ~~R7~~R5 – Access Revocation			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**
~~7~~5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	~~For all termination actions, initiate the~~A process to ~~revoke the~~initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon ~~the effective date and time of the~~a termination action, and complete the ~~revocation~~removals within 24 hours ~~after the effective date and time~~ of the termination action~~.~~ (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	~~Evidence~~An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
~~77Reference~~Reference to prior version: *CIP 004-4, R4.2*		**Change Rationale:** *The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards* ***to require immediate revocation*** *for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*	

CIP-004-5 Table ~~R7~~R5 – Access Revocation			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**
~~7~~5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic ~~and~~access to individual accounts and authorized unescorted physical access that the Responsible Entity determines ~~is~~are not necessary by the end of the next calendar day following the ~~reassignment or transfer~~date that the Responsible Entity determines that the individual no longer requires retention of that access.	~~Evidence~~An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
Reference to prior version: *CIP-004-4, R4.2*		**Change Rationale:** *FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.*	

CIP-004-5 Table ~~R7~~R5 – Access Revocation			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**
~~7~~5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity ~~or dial-up connectivity~~and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the ~~physical and electronic~~ designated storage locations ~~where~~for BES Cyber System Information ~~is stored by the Responsible Entity~~, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date and time of the termination action.	~~Evidence~~An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.
Reference to prior version: *NEW*		**Change Rationale:** *FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.*	

CIP-004-5 Table ~~R7~~R5 – Access Revocation			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**
~~7~~5.4	High Impact BES Cyber Systems and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ • EACMS	For termination actions, revoke the individual's non-shared user accounts ~~on BES Cyber Assets~~ (unless already revoked ~~in accordance with Requirements R7~~according to Parts 5.1 or ~~R7~~5.3) within 30 calendar days of the effective date of the termination action.	~~Evidence~~An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
Reference to prior version: *NEW*		**Change Rationale:** *FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.*	

CIP-004-5 Table ~~R7~~R5 – Access Revocation			
Part	**~~Applicability~~Applicable Systems**	**Requirements**	**Measures**
~~7~~5.5	High Impact BES Cyber Systems and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ • EACMS	For termination actions~~, reassignments, or transfers~~, change passwords for shared account(s) known to the user within 30 calendar days of the termination action~~, reassignment, or transfer of the user.~~. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; ~~or~~ • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers~~.~~; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.
Reference to prior version: *CIP-007-4, R5.2.3*		**Change Rationale:** *To provide clarification of expected actions in managing the passwords.*	

~~C.~~Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~entity~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain ~~data or~~ evidence ~~for~~of each requirement in this standard for three calendar years~~ or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer~~.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the ~~duration~~time specified above, whichever is longer.
- ~~The Compliance Enforcement Authority~~The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

~~Table of Compliance Elements~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1~~	~~Operations Planning~~	~~Lower~~	~~The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)~~	~~The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)~~	~~The Responsible Entity did not convey on-going security awareness reinforcement at least once for a calendar quarter and did so beyond 30 calendar days after the start of a subsequent calendar quarter. (1.1)~~	~~The Responsible Entity did not document a security awareness program. (R1)~~
~~R2~~	~~Operations Planning~~	~~Lower~~	~~The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 1 of the required training content as detailed in 2.2 through 2.10.~~	~~The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 2 of the required training content as detailed in 2.2 through 2.10.~~	~~The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 4 or more of the training content as detailed in 2.2 through 2.10.~~	~~The Responsible Entity did not have the required role-based training. (R2)~~
~~R3~~	~~Operations Planning.~~	~~Medium~~	~~With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not~~	~~With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not~~	~~With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not~~	~~With the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
			~~train 1 individual prior to their being granted electronic and unescorted physical access in a calendar year. (3.1)~~ ~~OR~~ ~~The Responsible Entity did not train 1 individual authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)~~	~~train 2 individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1)~~ ~~OR~~ ~~The Responsible Entity did not train 2 individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)~~	~~train 3 individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1)~~ ~~OR~~ ~~The Responsible Entity did not train 3 individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)~~	~~train 4 or more individuals prior to their being granted electronic and unescorted physical access in a calendar year. (3.1)~~ ~~OR~~ ~~The Responsible Entity did not train 4 or more individuals authorized for electronic and unescorted physical access in a calendar year not exceeding 15 months between training. (3.2)~~ ~~OR~~ ~~The Responsible Entity did not implement at all its cyber security training program. (R3)~~
~~**R4**~~	~~**Operations Planning**~~	~~**Medium**~~	~~N/A~~	~~The Responsible Entity has a personnel risk assessment program, as stated in~~	~~The Responsible Entity has a personnel risk assessment program, as stated in~~	~~The Responsible Entity did not have a personnel risk assessment program,~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
				~~Requirement R4, for individuals having authorized cyber or authorized unescorted physical access, but the program does not include identity verification or a criminal history records check. (4.1) (4.2)~~	~~Requirement R4, for individuals having authorized cyber or authorized unescorted physical access, but the program did not include the required documented results or the program did not include criteria or process to determine when authorized access shall not be granted. (4.3)(4.5)~~	~~as stated in Requirement R4, for individuals having authorized cyber or authorized unescorted physical access. (R4)~~
~~**R5**~~	~~**Same Day Operations**~~	~~**Medium**~~	~~Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 1 individual prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1)~~ ~~OR~~	~~Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 2 individuals prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1) OR~~ ~~The Responsible Entity did not update~~	~~Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 3 individuals prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1)~~ ~~OR~~	~~The Responsible Entity did not have a documented process for personnel risk assessments. (R5)~~ ~~OR~~ ~~Except for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessments for 4 or more individuals~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
			~~The Responsible Entity did not update personnel risk assessments every seven years for 1 individual within seven years after the initial performance or last update of the personnel risk assessment. (5.2)~~	~~personnel risk assessments every seven years for 2 individuals within seven years after the initial performance or last update of the personnel risk assessment. (5.2)~~	~~The Responsible Entity did not update personnel risk assessments every seven years for 3 or more individuals within seven years after the initial performance or last update of the personnel risk assessment. (5.2)~~	~~prior to granting authorized electronic and unescorted physical access in a calendar year. (5.1)~~
~~**R6**~~	~~**Operations Planning and Same Day Operations**~~	~~**Lower**~~	~~The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity~~	~~The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity~~	~~The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity~~	~~The Responsible Entity did not have a documented process for access management. (R6)~~ ~~OR~~ ~~The Responsible Entity did not designate one or more individual(s) to authorize electronic access, unescorted physical access, or access to the physical and electronic~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
			~~determined was necessary for performing assigned work functions. (6.2) (6.3) (6.4)~~ ~~OR~~ ~~The Responsible Entity did verify within 17 calendar months but not within 15 calendar months that: (6.6) (6.7)~~ ~~• all user accounts, user account groups, and user role categories were correct, or~~ ~~• their specific, associated privileges were correct or that they were those that that the Responsible~~	~~determined was necessary for performing assigned work functions and one user was granted access without authorization by the individual(s) designated in 6.1. (6.2) (6.3) (6.4)~~ ~~OR~~ ~~The Responsible Entity did not verify within the calendar quarter that individuals provisioned for unescorted physical access and electronic access had associated authorization records. (6.5)~~ ~~OR~~ ~~The Responsible Entity did verify within 19 calendar months but not within 17 calendar months that: (6.6)~~	~~determined was necessary for performing assigned work functions and two users were granted access without authorization by the individual(s) designated in 6.1. (6.2) (6.3) (6.4)~~ ~~OR~~ ~~The Responsible Entity did verify within 21 calendar months but not within 19 calendar months that: (6.6) (6.7)~~ ~~• all user accounts, user account groups, and user role categories are correct, or~~ ~~• their specific, associated privileges were~~	~~locations where BES Cyber System Information is stored by the Responsible Entity. (6.1)~~ ~~OR~~ ~~The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, and access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determined was necessary for performing assigned work functions and three or more users were granted access without authorization~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
			~~Entity determined necessary for performing assigned work functions.~~ ~~• access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing assigned work functions.~~	~~(6.7)~~ ~~• all user accounts, user account groups, and user role categories were correct, or~~ ~~• their specific, associated privileges were correct or that they were those that the Responsible Entity determined necessary for performing assigned work functions.~~ ~~• access to the physical and electronic locations where BES Cyber System~~	~~correct or that they were those that that the Responsible Entity determined necessary for performing assigned work functions.~~ ~~• access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for~~	~~by the individual(s) designated in 6.1. (6.2) (6.3) (6.4)~~ ~~OR~~ ~~The Responsible Entity did not verify within 24 calendar months that: (6.6) (6.7)~~ ~~• all user accounts, user account groups, and user role categories were correct, or~~ ~~• their specific, associated privileges were correct or that they were the those that that the Responsible Entity determined necessary for~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
				~~Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing assigned work functions.~~	~~performing assigned work functions.~~	~~performing assigned work functions, or~~ ~~• access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing assigned work functions.~~
~~**R7**~~	~~**Same Day Operations and Operations Planning**~~	~~**Medium**~~	~~Revocation of access to BES Cyber Information was not accomplished for 1 or more individuals~~	~~The Responsible Entity did not revoke unneeded unescorted physical or electronic access within the~~	~~The Responsible Entity did not revoke unneeded unescorted physical or electronic access according to~~	~~The Responsible Entity did not have a documented process for initiating the unescorted physical or~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
			~~within the specified time frame (7.3);~~ ~~OR~~ ~~User accounts on BES Cyber Assets were not revoked for one or more individuals within the specified time frame (7.4);~~ ~~OR~~ ~~User passwords on BES Cyber Asset shared accounts were not changed for one or more individuals within the specified time frame; (7.5)~~ ~~OR~~ ~~Following the determination and documentation of extenuating operating circumstances, passwords for shared accounts were not changed for one or~~	~~specified times in CIP-004-5 R7 for one individual who was terminated, resigned, was reassigned, or transferred. (7.1 and 7.2)~~	~~the specified times in CIP-004-5 R7 for two individuals who were terminated, resigned, reassigned or transferred.(7.1 and 7.2)~~	~~electronic access revocation process; OR The Responsible Entity did not revoke unneeded access according to the specified times in CIP-004-5 R7 for three or more individuals who were terminated, resigned, reassigned, or transferred. (7.1 and 7.2)~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
			~~more individuals within 10 days following the end of the extenuating operating circumstances. (7.5)~~			

~~D.~~Regional Variances

None.

~~E.~~Interpretations

None.

~~F.~~Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should ~~reference sound~~reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

~~Guidance: Describe example mechanisms used to demonstrate the availability of this information~~

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

~~Note: Provide guidance or a local definition of "role appropriate" as it is used in this standard.~~

~~**Requirement R3:**~~

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and does not require reconfirmation during the tenure of employment.

~~NOTE: Program specified exceptional circumstances can include a specified individual to declare an emergency.~~

~~**Requirement R4 and R5:**~~

~~Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access when called for in CIP-004-1 Table R4 – Personnel Risk Assessment, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency~~

~~response, to ensure that personnel who have such access have had their identity verified, then been assessed for risk.~~A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, ~~or~~ individuals who may have resided in locations from where it is not possible to obtain a criminal history records check~~.~~, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement ~~R6~~R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly ~~and annual~~ reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The ~~annual~~ privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement ~~R6~~R4 is included below.

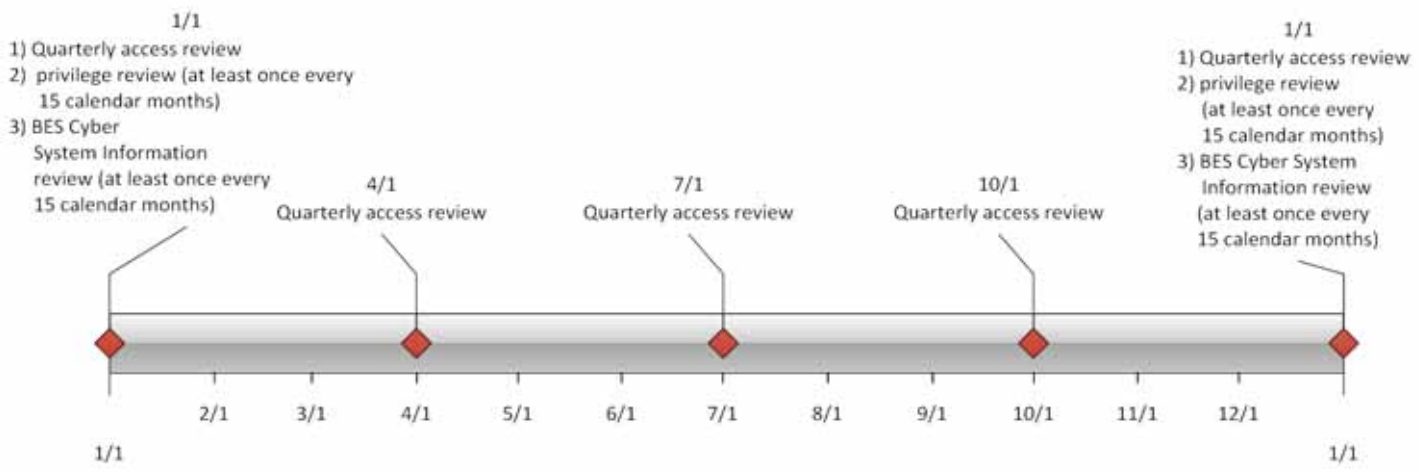

Separation of duties should be considered when performing the reviews in Requirement ~~R6~~R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or ~~annual~~at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement ~~R6~~R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement ~~R7~~R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common ~~examples~~scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
~~Termination prior to notification~~	~~Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.~~
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement ~~R7~~R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, ~~the requirement states~~ a review of access privileges ~~must~~should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as

part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the third posting of Version 5 of the CIP Cyber Security Standards for a 30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the second posting and ballot.

Anticipated Actions	Anticipated Date
30-day Formal Comment Period with Parallel Successive Ballot	September 2012
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-005-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-005-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-5

3. Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-005-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes.

These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity.

This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for R1: The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*	
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and BES Cyber System.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
Reference to prior version: *CIP-005-4, R2.1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.*	
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
Reference to prior version: *CIP-005-4, R2.3*		**Change Rationale:** *Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.*	

Rationale for R2: Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in *Guidance for Secure Interactive Remote Access* published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate Device serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate Device also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate Device. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Utilize an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
Reference to prior version: *New*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate Device.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.
Reference to prior version: *CIP-007-5, R3.1*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.*	

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
Reference to prior version: *CIP-007-5, R3.2*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The standard does not require segmenting of BES Cyber Systems by impact classification, and many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and systems within the ESP will be elevated to the level of the highest impact BES Cyber System present in the ESP. The standard accomplishes this by defining all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be

applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the ~~second~~third posting of Version 5 of the CIP Cyber Security Standards for a ~~40~~30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ~~first~~ ballot.~~–~~ A second posting of Version 5 ~~reverts to the original organization of the standards with some changes and~~was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the ~~first~~second posting and ballot.

Anticipated Actions	Anticipated Date
~~40~~30-day Formal Comment Period with Parallel Successive Ballot	~~April~~September 2012
Recirculation ballot	~~June~~November 2012
BOT adoption	~~June~~December 2012

Effective Dates

1. **24 Months Minimum** – ~~The Version 5~~ CIP ~~Cyber Security Standards, except for CIP-003-5, Requirement R2,~~ -005-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. ~~CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.~~[1]

2. In those jurisdictions where no regulatory approval is required, ~~the Version~~ CIP-005-5 ~~CIP Cyber Security Standards, except for CIP-003-5, Requirement R2,~~ shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, ~~and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval,~~ or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] ~~In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-5

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of ~~Functional Entities~~functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific ~~Functional Entity~~functional entity or subset of ~~Functional Entities~~functional entities are the applicable entity or entities, the ~~Functional Entity~~functional entity or ~~Entities~~entities are specified explicitly.

4.1.1 Balancing Authority

~~**4.1.2 Distribution Provider** that owns **Facilities described in 4.2.2**~~

~~**4.1.3 Generator Operator**~~

~~**4.1.4 Generator Owner**~~

~~**4.1.5 Interchange Coordinator**~~

~~**4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1**~~

~~**4.1.7 Reliability Coordinator**~~

~~**4.1.8 Transmission Operator**~~

~~**4.1.9 Transmission Owner**~~

~~**4.2. Facilities:**~~

~~**4.2.1 Load Serving Entity:** One~~one or more of the ~~UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard~~following Facilities, systems, and ~~that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.~~

~~**4.2.2**~~**4.1.2 ~~Distribution Provider~~**~~: One or more of the Systems or programs designed, installed, and operated~~equipment for the protection or restoration of the BES:

4.1.2.1 ~~A~~ Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS~~System~~) system that~~-~~:

4.1.2.1.1 is part of a Load shedding program ~~required by~~that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ~~that~~

•**4.1.2.1.2** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

•**4.1.2.2** ~~A~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

•**4.1.2.3** ~~A~~Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

•**4.1.2.4** Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~4.2.3~~4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers ~~and Load-Serving Entities~~: ~~All BES Facilities.~~:

All BES Facilities.

~~4.2.4~~4.2.3 Exemptions: The following are exempt from Standard CIP-~~002~~005-5:

~~4.2.4.1~~4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.4.2~~4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.4.3~~4.2.3.3 ~~In nuclear plants, the Systems~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for ~~a~~the requirement's common subject matter.

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as ~~they feel~~it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

~~**Applicability Columns in Tables:**~~

~~Each table row~~ Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk

Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an ~~applicability~~"Applicable Systems" column to further define the scope of systems to which a specific requirement row applies~~ to BES Cyber Systems and associated Cyber Assets.~~ . The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the ~~applicability~~"Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **High Impact BES Cyber Systems with ~~dial~~Dial-up ~~connectivity~~Connectivity** – Only applies to high impact BES Cyber Systems with ~~dial~~Dial-up ~~connectivity~~Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center~~ and categorized as medium impact according to the CIP-002-5 identification and categorization processes~~.
- **Medium Impact BES Cyber Systems with ~~dial~~Dial-up ~~connectivity~~Connectivity** – Only applies to medium impact BES Cyber Systems with ~~dial~~Dial-up ~~connectivity~~Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **~~Associated~~ Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System~~ in the applicability column~~.

- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System ~~in the applicability column~~.

B. Requirements and Measures

Rationale for R1: The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All ~~BES Cyber Assets and associated Protected~~applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	~~Evidence~~An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*	
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • ~~Associated Protected Cyber Assets~~PCA	All External Routable Connectivity ~~through the ESP~~ must be through an identified Electronic Access Point (EAP).	~~Evidence~~An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and BES Cyber System.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the ~~rationale~~reason for granting access, and deny all other access by default.	~~Evidence~~An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
Reference to prior version: *CIP-005-4, R2.1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.*	
1.4	High Impact BES Cyber Systems with ~~dial~~Dial-up ~~connectivity~~Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with ~~dial-up connectivity~~Dial-up Connectivity and their associated: • PCA	~~Perform~~Where technically feasible, perform authentication when establishing ~~dial~~Dial-up ~~connectivity~~Connectivity with ~~the BES~~applicable Cyber ~~System, where technically feasible~~Assets.	~~Evidence~~An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
Reference to prior version: *CIP-005-4, R2.3*		**Change Rationale:** *Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have ~~a method~~one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	~~Evidence~~An example of evidence may include, but is not limited to~~:~~ ~~1. Evidence~~, documentation that ~~intrusion~~malicious communications detection ~~systems are functioning:~~ ~~• Configuration files of intrusion detection systems deployed to monitor an EAP; or~~ ~~• Logs that were generated by an~~methods (e.g. intrusion detection system~~;~~ ~~and~~ ~~2. Documentation showing where intrusion detection systems were deployed~~, application layer firewall, etc.) are implemented.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.*	

~~**Rationale for R2:** Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements or guidance documents are available to either require or recommend how secure remote access to BES Cyber Systems can or should be accomplished. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences.~~

~~Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.~~

~~Additional information is provided in *Guidance for Secure Interactive Remote Access* published by NERC in July 2011.~~

~~**Summary of Changes:** This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.~~

Rationale for R2: Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in *Guidance for Secure Interactive Remote Access* published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate Device serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate Device also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate Device. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable ~~items~~requirement parts, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable ~~items~~requirement parts in *CIP-005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • ~~Associated Protected Cyber Assets~~ PCA	Utilize an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access ~~a BES Cyber System or Protected~~an applicable Cyber Asset.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to, network diagrams or architecture documents.
Reference to prior version: *New*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • ~~Associated Protected Cyber Assets~~ PCA	~~Utilize encryption for~~For all Interactive Remote Access sessions~~-~~, utilize encryption that ~~terminate~~terminates at an Intermediate Device ~~in order to protect the confidentiality and integrity of each Interactive Remote Access session~~.	~~Evidence~~An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-5, R3.1*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.*	
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • ~~Associated Protected Cyber Assets~~ PCA	Require multi-factor authentication for all Interactive Remote Access sessions. ~~Factors must be at least two of the three following categories:~~ • ~~Something the individual knows (including, but not limited to, passwords or PINs. User ID is not an authentication factor);~~ • ~~Something the individual has (including, but not limited to, tokens, digital certificates, or smart cards); or~~ • ~~Something the individual is (including, but not limited to, fingerprints, iris scans, or other biometric characteristic).~~	~~Evidence~~An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
Reference to prior version: *CIP-007-5, R3.2*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~entity~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain ~~data or~~ evidence ~~for~~of each requirement in this standard for three calendar years~~ or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer~~.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the ~~duration~~time specified above, whichever is longer.
- ~~The Compliance Enforcement Authority~~The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

~~Table of Compliance Elements~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1~~	~~Operations Planning and Same Day Operations~~	~~Medium~~	~~The Responsible Entity failed to document one or more processes for *CIP-005-5 Table R1 – Electronic Security Perimeter* according to Requirement R1.~~ ~~OR~~ ~~The Responsible Entity failed to document 5% or less of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2;~~ ~~OR~~ ~~The Responsible Entity failed to document 5% or less of inbound and outbound access permissions, including~~	~~The Responsible Entity failed to document more than 5% but less than or equal to 10% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2;~~ ~~OR~~ ~~The Responsible Entity failed to document more than 5% but less than or equal to 10% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part 1.3.~~	~~The Responsible Entity failed to document more than 10% but less than or equal to 15% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2;~~ ~~OR~~ ~~The Responsible Entity failed to document more than 10% but less than or equal to 15% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part 1.3.~~	~~The Responsible Entity failed to document more than 15% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2;~~ ~~OR~~ ~~The Responsible Entity failed to document more than 15% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part 1.3.~~ ~~OR~~ ~~The Responsible Entity~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
			~~the rationale for granting access according to Requirement R1, part 1.3.~~			~~did not have all BES Cyber Assets and associated Protected Cyber Assets connected to a network via a routable protocol within a defined ESP according to Requirement R1, part 1.1.~~ ~~OR~~ ~~External Routable Connectivity through the ESP was not through an identified EAP according to Requirement R1, part 1.2.~~ ~~OR~~ ~~The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default according to~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Requirement R1, part 1.3. OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible according to Requirement R1, part 1.4. OR The Responsible Entity did not have a method for detecting malicious communications according to Requirement R1, part 1.5.
R2	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity failed to document one or more processes for *CIP-005-5 Table R2 – Interactive Remote*	The Responsible Entity failed to implement the required multi-factor authentication according to	The Responsible Entity failed to implement one of the following: • Intermediate	The Responsible Entity failed to implement two or more of the following:

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
			~~Access according to Requirement R2.~~	~~Requirement R2, Part 2.3.~~	~~Device according to Requirement R2, Part 2.1;~~ ~~OR~~ ~~• Encryption according to Requirement R2, Part 2.2.~~	~~• Intermediate Device according to Requirement R2, Part 2.1 (2.1);~~ ~~• Encryption according to Requirement R2, Part 2.2;~~ ~~OR~~ ~~• Multi-factor authentication according to Requirement R2, Part 2.3.~~

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The standard does not require segmenting of BES Cyber Systems by impact classification, and many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and systems within the ESP will be elevated to the level of the highest impact BES Cyber System present in the ESP. The standard ~~handles~~accomplishes this by defining all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, ~~the~~ each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise~~.~~ and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable~~,~~ connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be

applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the ~~SDT's~~Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then ~~the~~ Requirement R2 ~~requirements~~ also ~~apply~~applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear that this is not ~~simple~~simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the third posting of Version 5 of the CIP Cyber Security Standards for a 30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the second posting and ballot.

Anticipated Actions	Anticipated Date
30-day Formal Comment Period with Parallel Successive Ballot	September 2012
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-006-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-5

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-006-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale: Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed.

Summary of Changes: The entire content of CIP-006-5 is intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

Added details to address FERC Order No. 706, Paragraph 572, directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.
Reference to prior version: *CIP-006-4c, R2.1 for Physical Access Control Systems* *New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity*		**Change Description and Justification:** *Change Description and Justification: To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected by a Physical Security Perimeter.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
Reference to prior version: *CIP006-4c, R3 & R4*		**Change Description and Justification:** *This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
Reference to prior version: CIP006-4c, R3 & R4		**Change Description and Justification:** *The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.* *Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.* *FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).*	

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*	
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
Reference to prior version: CIP006-4c, R5		**Change Description and Justification:** *Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the unauthorized physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.
Reference to prior version: CIP006-4c, R5		**Change Description and Justification:** *Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.
Reference to prior version: CIP-006-4c, R6		**Change Description and Justification:** *CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.* *Examples of logging methods have been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change.*	

Rationale: To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.
Reference to prior version: *CIP-006-4c, R1.6.2*		**Change Description and Justification:** *Added the ability to not do this during CIP Exceptional Circumstances.*	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
Reference to prior version: *CIP-006-4c R1.6.1*		**Change Description and Justification:** *Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.*	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change*	

Rationale: To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.
Reference to prior version: *CIP-006-4c, R8.1 and R8.2*		**Change Description and Justification:** *Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Outage records should address when the installed control, monitor, and logging systems or hardware at access points are broken or unavailable.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the ~~second~~third posting of Version 5 of the CIP Cyber Security Standards for a ~~40~~30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ~~first~~ ballot.~~–~~ A second posting of Version 5 ~~reverts to the original organization of the standards with some changes and~~was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the ~~first~~second posting and ballot.

Anticipated Actions	Anticipated Date
~~40~~30-day Formal Comment Period with Parallel Successive Ballot	~~April~~September 2012
Recirculation ballot	~~June~~November 2012
BOT adoption	~~June~~December 2012

Effective Dates

1. **24 Months Minimum** – ~~The Version 5~~ CIP ~~Cyber Security Standards, except for CIP-003-5, Requirement R2,~~-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. ~~CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.~~[1]

2. In those jurisdictions where no regulatory approval is required, ~~the Version~~ CIP-006-5 ~~CIP Cyber Security Standards, except for CIP-003-5, Requirement R2,~~ shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, ~~and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval,~~ or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] ~~In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-5

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of ~~Functional Entities~~functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific ~~Functional Entity~~functional entity or subset of ~~Functional Entities~~functional entities are the applicable entity or entities, the ~~Functional Entity~~functional entity or ~~Entities~~entities are specified explicitly.

4.1.1 Balancing Authority

~~**4.1.2 Distribution Provider** that owns **Facilities described in 4.2.2**~~

~~**4.1.3 Generator Operator**~~

~~**4.1.4 Generator Owner**~~

~~**4.1.5 Interchange Coordinator**~~

~~**4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1**~~

~~**4.1.7 Reliability Coordinator**~~

~~**4.1.8 Transmission Operator**~~

~~**4.1.9 Transmission Owner**~~

~~**4.2. Facilities:**~~

~~**4.2.1 Load Serving Entity:** One~~one or more of the ~~UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard~~following Facilities, systems, and ~~that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.~~

~~**4.2.2**~~**4.1.2** ~~**Distribution Provider**: One or more of the Systems or programs designed, installed, and operated~~equipment for the protection or restoration of the BES:

4.1.2.1 ~~A~~ Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS~~System~~) system that~~-~~:

4.1.2.1.1 is part of a Load shedding program ~~required by~~that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ~~that~~

•**4.1.2.1.2** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

•**4.1.2.2** ~~A~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

•**4.1.2.3** ~~A~~Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

•**4.1.2.4** Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3~~4~~4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers ~~and Load-Serving Entities~~: ~~All BES Facilities.~~:

All BES Facilities.

4.2.~~4~~4.2.3 Exemptions: The following are exempt from Standard CIP-~~002~~006-5:

~~4.2.4.1~~4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.4.2~~4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.4.3~~4.2.3.3 ~~In nuclear plants, the Systems~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for ~~a~~the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as ~~they feel~~it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

~~Applicability Columns in Tables:~~

~~Each table row~~ Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an ~~applicability~~"Applicable Systems" column to further define the scope of systems to which a specific requirement row applies ~~to BES Cyber Systems and associated Cyber Assets.~~ . The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the ~~applicability~~"Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity.

This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- ~~**Associated**~~ **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System~~ in the applicability column~~. Examples include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- ~~**Associated**~~ **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System~~ with External Routable Connectivity in the applicability column~~.
- ~~**Associated**~~ **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System~~ in the applicability column~~.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity ~~in the applicability column~~, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale: Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed.

Summary of Changes: The entire contents of CIP-006-5 are intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

Added details to address FERC Order No. 706, Paragraph 572, directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans ~~for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that~~ that collectively include all of the applicable ~~items~~requirement parts in *CIP-006-5 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security ~~plan or~~ plans that collectively include all of the applicable ~~items~~requirement parts in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.1	~~High Impact BES Cyber Systems~~ Medium Impact BES Cyber Systems without External Routable Connectivity ~~Associated~~ Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	~~Evidence~~An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist ~~and have been implemented.~~ .
Reference to prior version: *CIP-006-4c, R2.1 for Physical Access Control Systems* *New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity*		**Change Description and Justification:** *Change Description and Justification: To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected by a Physical ~~Access Control System.~~Security Perimeter.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	~~Evidence~~An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by ~~card reader~~access logs.
Reference to prior version: *CIP006-4c, R3 & R4*		**Change Description and Justification:** *This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~ EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	~~Evidence~~An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by ~~card reader~~access logs.
Reference to prior version: CIP006-4c, R3 & R4		**Change Description and Justification:** *The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.* *Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.* *FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: Associated Electronic Access Control or Monitoring Systems 1. Associated Protected Cyber Assets EACMS; and 2. PCA	Have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), Monitor for unauthorized circumvention of access through a physical access control point into a Physical Security Perimeter.	Evidence An example of evidence may include, but is not limited to, documentation of controls that monitor the Physical Security Perimeter for unauthorized circumvention of access through a physical access control point into a Physical Security Perimeter.
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: Associated Electronic Access Control or Monitoring Systems 1. Associated Protected Cyber Assets EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized circumvention ofaccess through a physical access controlpoint into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection.	EvidenceAn example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized circumvention ofaccess through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*	
1.6	Physical Access Control Systems Associated(PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity •	Have controls that monitorMonitor each Physical Access Control System twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized physical access to a Physical Access Control System.	EvidenceAn example of evidence may include, but is not limited to, documentation of controls that monitor the Physical Security Perimeter for unauthorized circumvention of a physical access control into a Physical Security Perimeterto a PACS.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
Reference to prior version: CIP006-4c, R5		**Change Description and Justification:** *Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	
1.7	Physical Access Control Systems Associated(PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity •	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the unauthorized physical access.	EvidenceAn example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.
Reference to prior version: CIP006-4c, R5		**Change Description and Justification:** *Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~ EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	~~Evidence~~An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.
Reference to prior version: CIP-006-4c, R6		**Change Description and Justification:** *CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.* *~~-~~Examples of logging methods have been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~ EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	~~Evidence~~An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change.*	

Rationale: To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable ~~items~~requirement parts in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable ~~items~~requirement parts in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: ~~Associated Electronic Access Control or Monitoring Systems~~ ~~Associated Protected Cyber Assets~~ 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are ~~known or guests, and~~provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	~~Evidence~~An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.
Reference to prior version: *CIP-006-4c, R1.6.2*		**Change Description and Justification:** *Added the ability to not do this during CIP Exceptional Circumstances.*	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~ EACMS; and 2. PCA	Require manual or automated logging of ~~the~~visitor entry into and exit ~~of visitors into~~from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	~~Evidence~~An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
Reference to prior version: *CIP-006-4c R1.6.1*		**Change Description and Justification:** *Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.*	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~ EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	~~Evidence~~An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change*	

Rationale: To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable ~~items~~requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable ~~item~~requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity •	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	~~Evidence~~An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.
Reference to prior version: *CIP-006-4c, R8.1 and R8.2*		**Change Description and Justification:** *Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.*	

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirement**	**Measures**
~~3.2~~	~~Physical Access Control Systems associated with:~~ ~~• High Impact BES Cyber Systems~~ ~~• Medium Impact BES Cyber Systems with External Routable Connectivity~~ ~~Locally mounted hardware or devices at the Physical Security Perimeter associated with:~~ ~~• High Impact BES Cyber Systems~~ ~~• Medium Impact BES Cyber Systems with External Routable Connectivity~~	~~Document outages for physical access control, logging, and alerting systems and retain the outage records for at least 12 calendar months.~~	~~Evidence may include, but is not limited to, the outage records and availability of outage records for the preceding 12 calendar months.~~
~~**Reference to prior version:**~~ ~~*CIP-006-4c, R8.3*~~		~~**Change Description and Justification:** *No change.*~~	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~entity~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain ~~data or~~ evidence ~~for~~of each requirement in this standard for three calendar years~~ or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer~~.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the ~~duration~~time specified above, whichever is longer.
- ~~The Compliance Enforcement Authority~~The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

~~Table of Compliance Elements~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1~~	~~Long Term Planning~~ ~~Same-Day Operations~~	~~Medium~~	~~The Responsible Entity has documented and implemented physical access controls, but logging of authorized physical entry through any Physical Security Perimeter does not provide sufficient information to uniquely identify the individual and date of entry. (1.8)~~ ~~OR~~ ~~The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days. (1.9)~~	~~The Responsible Entity has documented and implemented physical access controls, but it does not alert for unauthorized physical access to Physical Access Control Systems or does not communicate such alerts within 15 minutes to identified personnel(1.7)~~ ~~OR~~ ~~The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days. (1.9)~~	~~The Responsible Entity has documented and implemented physical access controls, but does not alert for unauthorized circumvention of a physical access control into a Physical security Perimeter or does not communicate such alerts within 15 minutes to identified personnel. (1.5)~~ ~~OR~~ ~~The Responsible Entity has does not have controls that monitor each Physical Access Control System twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized physical access to a Physical~~	~~The Responsible Entity did not document or implement operational or procedural controls to restrict physical access to only those individuals who are authorized. (1.1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented physical access controls, but at least one method does not exist to restrict access to Medium Impact BES Cyber Systems with External Routable Connectivity or External Dial-up Connectivity. (1.2)~~ ~~OR~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
					~~Access Control Systems. (1.6)~~ ~~OR~~ ~~The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days. (1.9)~~	~~The Responsible Entity has documented and implemented physical access controls, but two or more different methods do not exist to restrict access to High Impact BES Cyber Systems. (1.3)~~ ~~OR~~ ~~The Responsible Entity has does not have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized circumvention of a physical access control into a Physical Security Perimeter. (1.4)~~ ~~OR~~ ~~The Responsible Entity retained physical~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						access logs for less than 45 calendar days. (1.9)
R2	**Same-Day Operations**	**Medium**	N/A	The Responsible Entity included a visitor control program in its physical security plan, but did not log each of the initial entry and last exit dates and times of the visitor on a daily basis, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity included a visitor control program in its physical security plan, but failed to retain visitor logs for at least ninety days. (2.3)	The Responsible Entity included a visitor control program in its physical security plan, but it did not meet the requirements for continuous escort. (2.1)	The Responsible Entity has failed to include or implement a visitor control program to provide required escorted access of visitors within any Physical Security Perimeter. (2.1)
R3	**Long Term Planning**	**Lower**		The Responsible Entity has documented and	The Responsible Entity did not document	The Responsible Entity has not documented

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
			~~The Responsible Entity did not retain outage records for at least 12 months of outages for physical access control, logging, and alerting systems. (3.2)~~	~~implemented a maintenance and testing program for Physical Access Control Systems, but the testing was not performed on a cycle of not more than 24 calendar months. (3.1)~~	~~outages for physical access control, logging, and alerting systems for Physical Access Control Systems as required. (3.2)~~	~~and implemented a maintenance and testing program for Physical Access Control Systems. (3.1)~~

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods ~~to restrict~~of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (~~i.~~e.g., key or card key) would provide access through both.

~~Typically any opening greater than 96 square inches, with one side greater than six inches in length, would be considered an access point into the Physical Security Perimeter. Protective measures such as bars, wire mesh, or other permanently installed metal barrier could be used to reduce the opening size, as long as it is leaves no opening greater than 96 square inches, or no more than six inches on its shortest side.~~

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a ~~Point~~point of ~~Contact~~contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Outage records should address when the installed control, monitor, and logging systems or hardware at access points are broken or unavailable.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the third posting of Version 5 of the CIP Cyber Security Standards for a 30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the second posting and ballot.

Anticipated Actions	Anticipated Date
30-day Formal Comment Period with Parallel Successive Ballot	September 2012
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-007-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-007-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-5

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-007-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident

response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for R1: The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are needed. Physical I/O ports were added in response to a FERC order. The unneeded physical ports in control center environments (which are the highest risk, most impactful areas) should be protected as well.

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.
Reference to prior version: *CIP-007-4, R2.1 and R2.2*		**Change Description and Justification:** *The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.*	

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
Reference to prior version: *NEW*		**Change Description and Justification:** *On March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.*	

Rationale for R2: Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" and there has been confusion as to what constitutes the availability date. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.
Reference to prior version: *CIP-007, R3*		**Change Rationale:** *The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches. Documenting the source is used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.
Reference to prior version: *CIP-007, R3.1*		**Change Rationale:** *Similar to the current wording but added "from the source or sources identified in 2.1" to clarify the 30-day time frame.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
Reference to prior version: *CIP-007, R3.2*		**Change Rationale:** *The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.*	
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.
Reference to prior version: *CIP-007, R3.2*		**Change Rationale:** *Similar to the current wording but added that the plan must be implemented within the timeframe specified in the plan, or in a revised plan as approved by the CIP Senior Manager or delegate.*	

Rationale for R3: Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.

Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"

In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
Reference to prior version: *CIP-007-4, R4; CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.*	

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of identified malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
Reference to prior version: *CIP-007-4, R4* *CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes.*	

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.
Reference to prior version: *CIP-007-4, R4; CIP-007-4, R4.2*		**Change Rationale:** *Requirement essentially unchanged from previous versions; updated to refer to previous parts of the requirement table.*	

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Summary of Changes: Beginning in Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor."

The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the System. There are a few events explicitly listed that if a Cyber Asset or BES Cyber System can log, then it must log.

In addition, this requirement sets up parameters for the monitoring and reviewing of processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
Reference to prior version: *CIP-005-4, R3; CIP-007-4, R5, R5.1.2, R6.1, andR6.3*		**Change Description and Justification:** *This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, includingpaper or system generated list showing how alerts are configured.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.2*		**Change Description and Justification:** *This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate a response.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.4*		**Change Rationale:** *No substantive change.*	
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.5*		**Change Description and Justification:** *Beginning in Paragraph 525 and also 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for an approximately biweekly summary or sampling review of logs.*	

Rationale for R5: To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

Summary of Changes (From R5):

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT feels these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.
Reference to prior version: *CIP-007-4, R5*		**Change Rationale:** *The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.
Reference to prior version: *CIP-007-4, R5.2 and R5.2.1*		**Change Rationale:** *CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.
Reference to prior version: *CIP-007-4, R5.2.2*		**Change Rationale:** *No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
Reference to prior version: *CIP-007-4, R5.2.1*		**Change Rationale:** *The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.
Reference to prior version: *CIP-007-4, R5.3*		**Change Rationale:** *CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
Reference to prior version: *CIP-007-4, R5.3.3*		**Change Rationale:** **This was originally Requirement R5.5.3, but moved to add "external routable connectivity" to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.
Reference to prior version: *New Requirement*		**Change Rationale:** *Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product.

The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration."

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of

reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device, but the entity disables or neglects to enable that logging, it is a violation. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-

time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the ~~second~~third posting of Version 5 of the CIP Cyber Security Standards for a ~~40~~30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and ~~first~~ ballot.~~–~~ A second posting of Version 5~~ reverts~~, which reverted to the original organization of the standards with some changes~~ and~~, was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the ~~first~~second posting and ballot.

Anticipated Actions	Anticipated Date
~~40~~30-day Formal Comment Period with Parallel Successive Ballot	~~April~~September 2012
Recirculation ballot	~~June~~November 2012
BOT adoption	~~June~~December 2012

Effective Dates

1. **24 Months Minimum** – ~~The Version 5~~ CIP ~~Cyber Security Standards, except for CIP-003-5, Requirement R2,~~-007-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. ~~CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.~~[1]

2. In those jurisdictions where no regulatory approval is required, ~~the Version~~ CIP-007-5 ~~CIP Cyber Security Standards, except for CIP-003-5, Requirement R2,~~ shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, ~~and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval,~~ or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] ~~In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-5

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of ~~Functional Entities~~functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific ~~Functional Entity~~functional entity or subset of ~~Functional Entities~~functional entities are the applicable entity or entities, the ~~Functional Entity~~functional entity or ~~Entities~~entities are specified explicitly.

4.1.1 Balancing Authority

~~**4.1.2 Distribution Provider** that owns **Facilities described in 4.2.2**~~

~~**4.1.3 Generator Operator**~~

~~**4.1.4 Generator Owner**~~

~~**4.1.5 Interchange Coordinator**~~

~~**4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1**~~

~~**4.1.7 Reliability Coordinator**~~

~~**4.1.8 Transmission Operator**~~

~~**4.1.9 Transmission Owner**~~

~~**4.2. Facilities:**~~

~~**4.2.1 Load Serving Entity:** One~~one or more of the ~~UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard~~following Facilities, systems, and ~~that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.~~

~~**4.2.2**~~**4.1.2** ~~**Distribution Provider**: One or more of the Systems or programs designed, installed, and operated~~equipment for the protection or restoration of the BES:

4.1.2.1 ~~A~~ Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS ~~System~~) system that~~-~~:

4.1.2.1.1 is part of a Load shedding program ~~required by~~that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ~~that~~

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 ~~A~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 ~~A~~Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3~~4~~.2.2 Responsible Entities listed in 4.1 other than Distribution Providers ~~and Load-Serving Entities~~: ~~All BES Facilities.~~:

All BES Facilities.

4.2.4~~4~~.2.3 Exemptions: The following are exempt from Standard CIP-~~002~~007-5:

4.2.4.~~1~~4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.~~2~~4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.~~3~~4.2.3.3 ~~In nuclear plants, the Systems~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for ~~a~~the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as ~~they feel~~it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

~~Applicability Columns in Tables:~~

~~Each table row~~ Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an ~~applicability~~"Applicable Systems" column to further define the scope of systems to which a specific requirement row applies ~~to BES Cyber Systems and associated Cyber Assets.~~ . The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the ~~applicability~~"Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center ~~and categorized as medium impact according to the CIP-002-5 identification and categorization processes~~.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- ~~**Associated**~~ **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a

~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

- ~~**Associated**~~ **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System~~ with External Routable Connectivity in the applicability column~~.
- ~~**Associated**~~ **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System~~ in the applicability column~~.

B. Requirements and Measures

Rationale for R1: The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are needed. Physical I/O ports were added in response to a FERC order. The unneeded physical ports in control center environments (which are the highest risk, most impactful areas) should be protected as well.

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-007-5 Table R1 – Ports and Services. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-007-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	~~For applicable Cyber Assets and where~~Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to: • ~~Listings~~Documentation of the ~~needed~~need for all enabled ports ~~by Cyber Asset or class of~~on all applicable Cyber Assets~~;~~ and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.
Reference to prior version: *CIP-007-4, R2.1 and R2.2*		**Change Description and Justification:** *The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.*	

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	~~Evidence~~An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
Reference to prior version: *NEW*		**Change Description and Justification:** *~~In the~~On March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.*	

Rationale for R2: Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" and there has been confusion as to what constitutes the availability~~.~~ date. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-007-5 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-007-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	A patch management ~~program~~process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	~~Evidence must~~An example of evidence may include, but is not limited to, documentation of a patch management ~~program~~process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
Reference to prior version: *CIP-007, R3*		**Change Rationale:** *The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches. Documenting the source is used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	~~Evaluate the~~ At least once every 35 calendar days, evaluate security patches for applicability ~~within 30 calendar days of availability of the patch~~that have been released since the last evaluation from the source or sources identified in Part 2.1.	~~Evidence~~An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources ~~within 30~~at least once every 35 calendar days ~~of availability~~.
Reference to prior version: *CIP-007, R3.1*		**Change Rationale:** *Similar to the current wording but added "from the source or sources identified in 2.1" to clarify the 30-day time frame.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, ~~create a dated plan or revise an existing plan~~ within ~~30~~35 calendar days of the evaluation completion~~.~~ ~~The~~, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities ~~exposed~~addressed by each security patch and a timeframe to complete these mitigations.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to~~, a~~: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities ~~exposed~~addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
Reference to prior version: *CIP-007, R3.2*		**Change Rationale:** *The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan ~~as created or revised~~ within the timeframe specified in the plan, ~~except for~~unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP ~~Exceptional Circumstances~~Senior Manager or delegate.	~~Evidence~~An example of evidence may include, but is not limited to~~:~~ • ~~Records of the installation of the patch;~~ • ~~Records~~, records of implementation of ~~vendor recommended~~ mitigations~~;~~ • ~~Exports from automated patch management tools that provide installation date;~~ • ~~Verification of BES Cyber System Component software revision;~~ • ~~Registry exports that show software has been installed; or~~ • ~~Evidence that affected services have been disabled.~~ .
Reference to prior version: *CIP-007, R3.2*		**Change Rationale:** *Similar to the current wording but added ~~"from~~that the ~~source or sources identified in Part 2.1" to clarify~~plan must be implemented within the ~~30-day time frame~~timeframe specified in the plan, or in a revised plan as approved by the CIP Senior Manager or delegate.*	

~~**Rationale for R3:** Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.~~

~~**Summary of Changes:** In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.~~

~~Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"~~

~~In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.~~

Rationale for R3: Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.

Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"

In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ ~~Associated Protected Cyber Assets~~ 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	~~Evidence~~An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
Reference to prior version: *CIP-007-4, R4; CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.*	

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	Mitigate the threat of identified malicious code.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to: • ~~Predetermined~~ Records of response ~~actions~~processes for malicious code detection~~;~~ • ~~Configuration of anti-virus response actions (e.g., quarantine, alert, etc.) to detected~~Records of the performance of these processes when malicious code~~; or~~ • ~~Configuration of white-listing application to notify appropriate personnel of unauthorized applications~~ is detected.
Reference to prior version: *CIP-007-4, R4* *CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes.*	

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	~~Update malicious code protections that use signatures or patterns at least once within 35 calendar days of each available signature or pattern release (this does not require use of every available release, but that for every release that is available, at least one update has occurred within 35 calendar days from that release), except for signature or pattern releases that the Responsible Entity documents as negatively affecting the Cyber Asset or BES Cyber System.~~ For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	~~Evidence~~An example of evidence may include, but is not limited to~~:~~ • ~~Documentation~~, documentation showing the ~~configuration of signature, or pattern updates~~process used for ~~automated controls; or~~ • ~~Work logs showing~~ the ~~signature, or pattern updates for manual controls~~update of signatures or patterns.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-4, R4; CIP-007-4, R4.2*		~~**Change Rationale:** *See the Summary of Changes. This part is written to ensure that signatures or patterns are updated within 35 days of release, but does not require installation of all releases so long as any given update occurs within 35 calendar days of each release. The part does not require update within 35 days of a particular release in cases where the Responsible Entity documents that the signature or pattern release negatively affects the Cyber Asset or BES Cyber System. Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.*~~ **Change Rationale:** *Requirement essentially unchanged from previous versions; updated to refer to previous parts of the requirement table.*	

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the ~~immediate~~ detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and ~~respond to~~notify personnel of audit processing failures.

Summary of Changes: Beginning in Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor."

The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the System. There are a few events explicitly listed that if a Cyber Asset or BES Cyber System can log, then it must log.

In addition, this requirement sets up parameters for the ~~monitor~~monitoring and ~~review~~reviewing of processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	~~Log events~~Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. ~~detected and logged~~Detected successful login attempts; ~~4.1.1.~~ Detected failed access attempts ~~at Electronic Access Points;~~ 4.1.2. ~~detected and logged successful~~ and failed login attempts; ~~4.1.3. detected and logged~~Detected malicious ~~software; and~~ ~~4.1.4.~~4.1.3. ~~detected and logged malicious activity~~code.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required ~~event~~ types~~.~~ of events.
Reference to prior version: *CIP-005-4, R3; CIP-007-4, R5, R5.1.2, R6.1, andR6.3*		**Change Description and Justification:** *This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines ~~necessitate a real-time~~necessitates an alert, that includes, as a minimum, each of the following types of events ~~where technically feasible:~~(per Cyber Asset or BES Cyber System capability): 4.2.1. ~~detected~~Detected malicious ~~activity~~code from Part 4.1; and 4.2.2. ~~detected~~Detected failure of Part 4.1 event logging. ~~4.2.2.~~	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to, paper or system-generated listing of security events ~~which~~that the Responsible Entity determined necessitate ~~real-time~~ alerts ~~and paper~~, includingpaper or system generated list showing how ~~real-time~~ alerts are configured.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.2*		**Change Description and Justification:** *This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate ~~an immediate~~a response.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
~~4.3~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ ~~Associated Protected Cyber Assets~~	~~Activate a response to detected event logging failures before the end of the next calendar day.~~	~~Evidence may include, but is not limited to, documentation describing the response and its timing, or an attestation indicating that no such events occurred.~~
~~**Reference to prior version:**~~ ~~*New Requirement*~~		~~**Change Rationale:** *This requirement was derived from NIST 800-53 version 3 AU-5, which addresses response to audit processing failures. Misunderstandings with previous versions considered the failure of the security event monitoring and alerting system itself to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.*~~	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
4.~~4~~3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	~~Retain BES Cyber System security-related~~Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days~~, where technically feasible~~ except under CIP Exceptional Circumstances.	~~Evidence~~ Examples of evidence may include, but ~~is~~are not limited to~~:~~ ~~1. security-related~~ , documentation of the event ~~logs from the past 90 days;~~ ~~2. records of disposition of security-related event logs beyond 90 days up to the evidence retention period;~~log retention process and ~~3.~~ paper or system generated reports showing log retention configuration set at 90 days or greater.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.4*		**Change Rationale:** *No substantive change.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
4.~~5~~4	High Impact BES Cyber Systems and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; and 2. PCA	Review a summarization or sampling of logged events ~~at a minimum every two weeks~~as determined by the Responsible Entity at intervals no greater than 15 days to identify undetected Cyber Security Incidents.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to, documentation describing the review, any findings from the review (if any), ~~signed~~ and dated documentation showing the review occurred.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.5*		**Change Description and Justification:** *Beginning in Paragraph 525 and also 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for ~~a weekly~~an approximately biweekly summary or sampling review of logs.*	

Rationale for R5: To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

~~**Summary of Changes (From R5):** CIP-007-4, Requirements R5.2.2 and R5.2.3 requiring the identification and management of shared account access have been removed. These requirements already exist in the authorization, security event monitoring and revocation of access, and guidance for these requirements makes clear the consideration of shared accounts. The requirement to identify and determine acceptable use for these accounts remains and the standard includes additional guidance on types of accounts to identify and appropriate use of these account types.~~

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

Summary of Changes (From R5):

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT feels these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-007-5 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-007-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ ~~Associated Physical Access~~ at Control ~~Systems~~Centers and their associated: ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and **3.** PCA	~~Enforce~~Have a method(s) to enforce authentication of ~~all~~interactive user access, where technically feasible.	~~Evidence~~An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

Reference to prior version: *CIP-007-4, R5*	**Change Rationale:** *The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.*

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	~~The CIP Senior Manager or delegate must authorize~~Identify and inventory all enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	~~Evidence~~An example of evidence may include, but is not limited to, a listing of accounts by account types ~~and signed documentation or workflow by a CIP Senior Manager or delegate~~ showing the ~~approval of~~ enabled or generic account types in use for the BES Cyber System.
Reference to prior version: *CIP-007-4, R5.2 and R5.2.1*		**Change Rationale:** *CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	~~Evidence~~An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.
Reference to prior version: *CIP-007-4, R5.2.2*		**Change Rationale:** *No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	Change known default passwords, ~~where technically feasible, unless the default password is unique to the device or instance of the application, on~~per Cyber ~~Assets.~~Asset capability	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to: • Records of a procedure that passwords are changed when new devices are ~~deployed~~in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
Reference to prior version: *CIP-007-4, R5.2.1*		**Change Rationale:** *The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	For password-~~based user~~only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations ~~by individuals~~ that include a reference to the ~~procedurally enforced passwords meet the password parameters~~documented procedures that were followed.

Reference to prior version: *CIP-007-4, R5.3*	**Change Rationale:** *CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.*

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	~~For~~Where technically feasible, for password-~~based user~~only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once ~~each calendar year, not to exceed~~every 15 calendar months ~~between changes~~.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations ~~by individuals~~ that include a reference to the ~~procedurally enforced passwords meet the password parameters~~documented procedures that were followed.
Reference to prior version: *CIP-007-4, R5.3.3*		**Change Rationale:** **This was originally Requirement R5.5.3, but moved to add "external routable connectivity" to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	~~Limit, where~~Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or ~~generate~~ • Generate alerts after a threshold of unsuccessful ~~login~~authentication attempts.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to: • Documentation of the~~-~~ account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.
Reference to prior version: *New Requirement*		**Change Rationale:** *Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~entity~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain ~~data or~~ evidence ~~for~~of each requirement in this standard for three calendar years~~ or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer~~.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the ~~duration~~time specified above, whichever is longer.
- ~~The Compliance Enforcement Authority~~The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

~~Table of Compliance Elements~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1~~	~~Same Day Operations~~	~~Medium~~	~~N/A~~	~~N/A~~		~~The Responsible Entity did not have a documented process that included the applicable items in *CIP-007-5 Table R1.* (R1)~~ ~~OR~~ ~~The Responsible Entity had unneeded logical network accessible ports enabled.~~ ~~OR~~ ~~The Responsible Entity had no methods to protect unnecessary physical input/output ports used for network connectivity, console commands, or removable media.~~
~~R2~~	~~Operations Planning~~	~~Medium~~	~~The Responsible Entity did not evaluate the~~	~~The Responsible Entity did not evaluate the~~	~~The Responsible Entity did not evaluate the~~	~~The Responsible Entity did not have a~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
			~~security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified.~~ ~~OR~~ ~~The Responsible Entity did not create a plan or revise and existing plan within 30 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.~~	~~security patches for applicability within 45 calendar days of availability of the patch from the source or sources identified.~~ ~~OR~~ ~~The Responsible Entity did not create a plan or revise and existing plan within 45 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.~~	~~security patches for applicability within 60 calendar days of availability of the patch from the source or sources identified.~~ ~~OR~~ ~~The Responsible Entity did not create a plan or revise and existing plan within 60 calendar days of the evaluation completion to mitigate the vulnerabilities exposed by applicable security patches with a timeframe for mitigation.~~	~~documented process that included the applicable items in *CIP-007-5 Table R2.* (R2)~~ ~~OR~~ ~~The Responsible Entity did not have a patch management program for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets or did not track for the release cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.~~ ~~OR~~ ~~The Responsible Entity did not implement the plan as created or~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
						~~revised within the timeframe specified in the plan.~~
~~R3~~	~~Same Day Operations~~	~~Medium~~	~~Where signatures or patterns are used, the Responsible Entity did update malicious code protections that use signatures or patterns at least once within 45 calendar days of each available signature or pattern release, but not within 35 calendar days. (3.3)~~	~~Where signatures or patterns are used, the Responsible Entity did update malicious code protections that use signatures or patterns at least once within 55 calendar days of each available signature or pattern release, but not within 45 calendar days. (3.3).~~	~~Where signatures or patterns are used, the Responsible Entity did not update malicious code protections that use signatures or patterns at least once within 55 calendar days of each available signature or pattern release. (3.3).~~	~~The Responsible Entity did not have a documented process that included the applicable items in *CIP-007-5 Table R3.* (R3)~~ ~~OR~~ ~~The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code.~~ ~~OR~~ ~~The Responsible Entity did not mitigate the threat of identified malicious code.~~
~~R4~~	~~Same Day Operations and~~	~~Medium~~	~~N/A~~	~~The Responsible Entity failed to identify and implement methods to~~	~~The Responsible Entity failed to activate a response to rectify the~~	~~The Responsible Entity did not have a documented process~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
	~~**Operations Assessment**~~			~~review a summarization of logged events every two weeks.~~	~~event logging failure before the end of the next calendar day.~~ ~~OR~~ ~~The Responsible Entity failed to identify and implement methods to retain BES Cyber System security-related events for at least the last 90 consecutive days, where technically feasible.~~	~~that included the applicable items in *CIP-007-5 Table R4.* (R4)~~ ~~OR~~ ~~The Responsible Entity failed to implement methods to generate alerts for events that it determines to necessitate a real-time alert.~~ ~~OR~~ ~~The Responsible Entity failed to log detected events necessary for the identification and after-the-fact investigation of Cyber Security Incidents.~~
~~**R5**~~	~~**Operations Planning**~~	~~**Medium**~~	~~N/A~~	~~N/A~~	~~The Responsible Entity failed to implement procedures to authorize the use of administrative, shared,~~	~~The Responsible Entity did not have a documented process that included the applicable items in~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
					~~default, and other generic account types.~~ ~~OR~~ ~~The Responsible Entity failed to implement procedures to identify the individuals with authorized access to shared accounts.~~	~~*CIP-007-5 Table R5.* (R5)~~ ~~OR~~ ~~The Responsible Entity failed to implement methods to validate credentials before granting electronic access to BES Cyber Systems.~~ ~~OR~~ ~~The Responsible Entity failed to implement procedures for password-based user authentication.~~ ~~OR~~ ~~The Responsible Entity failed to implement procedures to change or have unique default passwords, where technically feasible.~~

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement ~~1~~R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border ~~is a requirement in CIP-005, Requirement R1 to protect the network and~~ does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with ~~a low~~lower tier documents establishing the more detailed process followed for individual systems. ~~Low~~Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware~~,~~ (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist.~~–~~ The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within ~~30~~35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. ~~The~~It is possible security patches, hotfixes, and~~/or~~ updates ~~or compensating measures~~ may reduce the reliability of the system~~. The Responsible Entity must be allowed to evaluate their individual risk exposure~~, and ~~determine if actions must be taken to secure~~entities should take this into account when determining the ~~system~~type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan ~~within 30 days~~ which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities ~~exposed~~addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration~~". If the entity is going to install the patch, the plan can consist of a a simple record that normal patch installation process from 2.1 will be followed and designate the date of the patch installation.~~."

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code

cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code~~ and should not require a TFE.~~.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The ~~requirement~~entity is ~~written~~ to ~~handle two update frequency situations.~~

> ~~1) For those technologies~~have a documented process that ~~are providing very frequent updates (at most monthly but often daily or sometimes hourly),~~includes the ~~updates applied to the applicable Cyber Assets should be no more than 35 calendar days old. In these instances, this is a 'maximum staleness' requirement. It does not require that every update within a 35 day period be applied, but that the currently installed update be no more than 35 days old.~~
>
> ~~2) For those technologies that provide less frequent updates that are more than 35 days, the requirements should be applied within 35 days of the last available update.~~

~~Testing~~testing and installation of signature or pattern updates~~ is not required.~~. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times~~.~~ with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device, but the entity disables or neglects to enable that logging, it is a violation. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts

- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

~~**4.3.** Event logging failures occur when the components of the BES Cyber System cannot log events the Responsible Entity designated in 4.1. The most common reason for event logging failures is the event log being filled up beyond its configured storage threshold. However, there may be any number of other reasons for event logging failures.~~

~~For centralized logging systems, it should not be considered a failure if communication goes down between the Cyber Asset and the logging system if the Cyber Asset can store the logs locally for a period of time until the communication comes back up.~~

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.~~5~~4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.

- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.4.~~1~~ Reference the Requirement's rationale.

5.2 Where possible, ~~any~~default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase

alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.

~~The requirement to change passwords permits the Responsible Entity to determine the periodicity of the password change in their policies and procedures based on a number of factors. The following table suggests appropriate periodicity requirements for passwords based on these factors.~~

~~Account Type~~	~~Impact Level~~	~~Significance of passwords in preventing unauthorized access~~	~~Existing Service Agreements~~	~~Suggested Periodicity of Password Change~~
~~User account password~~	~~High~~	~~Primary access path~~	~~None.~~	~~90 days~~
~~User account password~~	~~Medium~~	~~Primary access path~~	~~None.~~	~~180 days~~
~~Shared account Password for a microprocessor relay, PLC, RTU, etc.~~	~~Medium~~	~~Local access path. Individuals must authenticate at an upstream device prior to gaining access.~~	~~None.~~	~~During regularly scheduled maintenance~~
~~Shared account password for a generation control system~~	~~Medium~~	~~Local access path. Individuals must authenticate at an upstream device prior to gaining access.~~	~~None.~~	~~During scheduled plant outages~~
~~Administrative account passphrase with 15+ characters~~	~~High or Medium~~	~~Local access path. Remote user must be authenticated using a different account~~	~~None.~~	~~One year~~
~~System account password with 25+ pseudo-random characters~~	~~High or Medium~~	~~Local access path~~	~~None.~~	~~Two years or more~~

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the third posting of Version 5 of the CIP Cyber Security Standards for a 30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the second posting and ballot.

Anticipated Actions	Anticipated Date
30-day Formal Comment Period with Parallel Successive Ballot	September 2012
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-008-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-008-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-5

3. Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-008-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes.

These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

B. Requirements and Measures

Rationale for R1: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions. These are described below each Requirement Part.

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from identification.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).*	

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.*	
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Conforming change to reference new defined term Cyber Security Incidents.*	

Rationale for R2: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test each Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 months between executions of the plan(s): • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** *Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.*	

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain records related to Reportable Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.
Reference to prior version: *CIP-008, R2*		**Change Description and Justification:** *Removed references to the retention period because the Standard addresses data retention in the Compliance Section.*	

Rationale for R3: Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident.*

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	After completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response, and not to exceed 90 calendar days after completion: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *CIP-008, R1.5*		**Change Description and Justification:** *Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.*	

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	After a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan, not to exceed 60 calendar days: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *CIP-008, R1.4*		**Change Description and Justification:** *Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a Cyber Security Incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. Table top exercises (TTX) can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response

activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

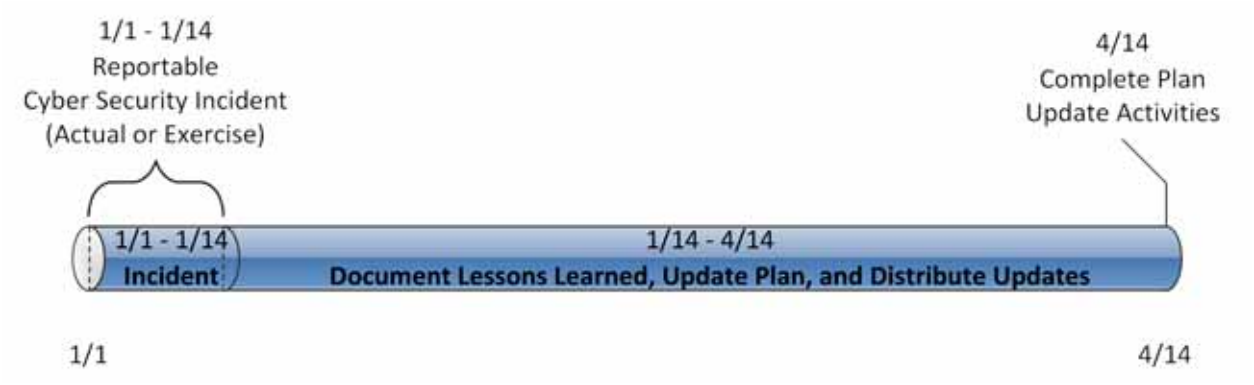

Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the incident and documenting the lessons learned as soon after the incident as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the incident response team.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

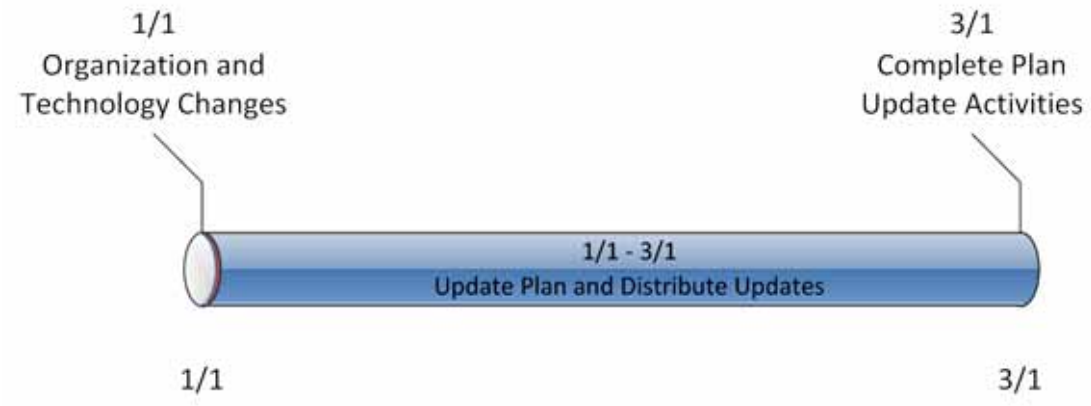

Figure 2: Timeline for Plan Changes in 3.2

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the ~~second~~third posting of Version 5 of the CIP Cyber Security Standards for a ~~40~~30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5~~-~~, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ~~first~~ ballot.~~–~~ A second posting of Version 5 ~~reverts to the original organization of the standards with some changes, and~~was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the ~~first~~second posting and ballot.

Anticipated Actions	Anticipated Date
~~40~~30-day Formal Comment Period with Parallel Successive Ballot	~~April~~September 2012
Recirculation ballot	~~June~~November 2012
BOT adoption	~~June~~December 2012

Effective Dates

1. **24 Months Minimum** – ~~The Version 5~~ CIP ~~Cyber Security Standards, except for CIP-003-5, Requirement R2,~~-008-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. ~~CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.~~[1]

2. In those jurisdictions where no regulatory approval is required, ~~the Version~~ CIP-008-5 ~~CIP Cyber Security Standards, except for CIP-003-5, Requirement R2,~~ shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, ~~and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval,~~ or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] ~~In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-5

3. Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of ~~Functional Entities~~functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific ~~Functional Entity~~functional entity or subset of ~~Functional Entities~~functional entities are the applicable entity or entities, the ~~Functional Entity~~functional entity or ~~Entities~~entities are specified explicitly.

4.1.1 Balancing Authority

~~**4.1.2 Distribution Provider** that owns **Facilities described in 4.2.2**~~

~~**4.1.3 Generator Operator**~~

~~**4.1.4 Generator Owner**~~

~~**4.1.5 Interchange Coordinator**~~

~~**4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1**~~

~~**4.1.7 Reliability Coordinator**~~

~~**4.1.8 Transmission Operator**~~

~~**4.1.9 Transmission Owner**~~

~~**4.2. Facilities:**~~

~~**4.2.1 Load Serving Entity:** One~~one or more of the ~~UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard~~following Facilities, systems, and ~~that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.~~

~~**4.2.2**~~**4.1.2** ~~**Distribution Provider**: One or more of the Systems or programs designed, installed, and operated~~equipment for the protection or restoration of the BES:

4.1.2.1 ~~A~~ Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS ~~System~~) system that~~-~~:

4.1.2.1.1 is part of a Load shedding program ~~required by~~that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ~~that~~

•**4.1.2.1.2** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

•**4.1.2.2** ~~A~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

•**4.1.2.3** ~~A~~Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

•**4.1.2.4** Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.34.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities**: All BES Facilities.:

All BES Facilities.

4.2.44.2.3 **Exemptions:** The following are exempt from Standard CIP-002008-5:

4.2.4.14.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.24.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.34.2.3.3 In nuclear plants, the SystemsThe systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for athe requirement's common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items

~~in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as ~~they feel~~it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

~~Applicability Columns in Tables:~~

~~Each table row~~ Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an ~~applicability~~"Applicable Systems" column to further define the scope of systems to which a specific requirement row applies~~ to BES Cyber Systems and associated Cyber Assets.~~ . The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the ~~applicability~~"Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

B. Requirements and Measures

Rationale for R1: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. ~~Once the severity of an event or events rises to the level of becoming a Reportable Cyber Security Incident, NERC EOP-004 directs further external reporting actions and timing requirements.~~ An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: ~~The requirement to report the incident has been removed and incorporated in the draft EOP-004-2 Standard. Other wording~~Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions. These are described below each Requirement Part.

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable ~~items~~requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable ~~items~~requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	~~Processes~~One or more processes to identify, classify, and respond to Cyber Security Incidents.	~~Evidence~~An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	~~A process~~One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from identification.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents~~.~~ and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *~~EOP-004-2 will address~~Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).*	
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	~~Evidence~~An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.*	
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	~~Evidence~~An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery~~,~~ ~~post-~~/incident ~~analysis~~resolution).
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Conforming change to reference new defined term Cyber Security Incidents.*	

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
~~1.5~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems~~	~~Internal groups or individuals and external organizations that should receive communication of the Cyber Security Incidents.~~	~~Evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that list internal groups or individuals (e.g., other departments, monitoring staff) and external organizations (e.g., law enforcement, ES-ISAC, software vendors, other affected entities) that should receive communication.~~
~~**Reference to prior version:** *CIP-008, R1.2*~~		~~**Change Description and Justification:** *Clarified the term "communication plan" by specifying the elements that need to be included.*~~	

Rationale for R2: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the ~~incident~~Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response ~~plan(s)~~plans to collectively include each of the applicable ~~items~~requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable ~~items~~requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test ~~the BES~~each Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 months between executions of the plan(s): • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With ~~a full~~an operational exercise of a Reportable Cyber Security Incident.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the ~~incident~~Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** *Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.*	
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain ~~relevant~~ records related to Reportable Cyber Security Incidents.	~~Evidence~~An example of evidence may include, but is not limited to, dated documentation~~;~~, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.
Reference to prior version: *CIP-008, R2*		**Change Description and Justification:** *Removed references to the retention period because the Standard addresses data retention in the Compliance Section.*	

Rationale for R3: Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single ~~incident~~Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

R3. Each Responsible Entity shall ~~implement one or more documented processes that collectively include~~maintain each of its Cyber Security Incident response plans according to each of the applicable ~~items~~requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include~~-~~, but is not limited to, documentation that collectively demonstrates maintenance of each ~~of~~ Cyber Security Incident response plan according to the applicable ~~documented processes that include each of the applicable items~~requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident ~~Response Plan Review, Update and Communication~~* ~~and additional evidence to demonstrate implementation as described in the Measures column of the table.~~.

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**

3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	~~Review and update each~~ After completion of a Cyber Security Incident response plan ~~for accuracy and completeness at least once each calendar year,~~ (s) test or actual Reportable Cyber Security Incident response, and not to exceed ~~15~~90 calendar ~~months between reviews~~days after completion: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	~~Evidence~~ An example of evidence may include, but is not limited to, ~~dated~~all of the following: 1. Dated documentation of ~~a~~ post incident(s) review ~~of each~~meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) ~~at least once every calendar year, not to exceed 15 calendar months between reviews,~~test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and ~~an updated~~revised Cyber Security Incident response plan ~~if necessary~~showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *CIP-008, R1.5*		**Change Description and Justification:** *Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.*	

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	After a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan, not to exceed 60 calendar days: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *CIP-008, R1.~~5~~4*		**Change Description and Justification:** *~~Specified what~~Specifies the ~~annual review entails~~activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.*	

~~CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication~~			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
~~3.2~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems~~	~~Document any lessons learned associated with a Cyber Security Incident test or actual incident response to a Reportable Cyber Security Incident within 30 calendar days after completion of the test or actual incident response.~~	~~Evidence may include, but is not limited to, dated documentation of lessons learned, if any, associated with the Cyber Security Incident Response Plan(s) test or actual incident response within 30 calendar days after completion of the test or actual incident response.~~
~~**Reference to prior version:**~~ ~~*CIP-008, R1.5*~~		~~**Change Description and Justification:** *Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.*~~	
~~3.3~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems~~	~~Update the Cyber Security Incident response plan based on any documented lessons learned within 30 calendar days after the documentation required by Part 3.2.~~	~~Evidence may include, but is not limited to:~~ ~~• Dated, documented lessons learned from the Cyber Security Incident documentation required by Part 3.2 and the dated, revised Cyber Security Incident response plan showing any changes based on that documentation; or~~ ~~• A dated action plan from the documentation required by Part 3.2 showing the resolved action item for Cyber Security Incident response plan updates.~~

~~Reference to prior version:~~ ~~*CIP-008, R1.4*~~	**~~Change Description and Justification:~~** ~~*Included additional specification on update of response plan addresses FERC Order No. 706, Paragraph 686, to modify on lessons learned.*~~

~~CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication~~			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirements~~	~~Measures~~
~~3.4~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems~~	~~Update the Cyber Security Incident response plan(s) within 30 calendar days of any of the following changes that the Responsible Entity determines would impact the ability to execute the plan:~~ • ~~Roles or responsibilities;~~ • ~~Cyber Security Incident response groups or individuals; or~~ • ~~Technology changes.~~	~~Evidence may include, but is not limited to, dated documentation reflecting changes made to the Cyber Security Incident response plan within 30 calendar days from and in response to the following changes that the Responsible Entity determined would impact the ability to execute the plan:~~ • ~~Roles or responsibilities;~~ • ~~Cyber Security Incident response groups or individuals; or~~ • ~~Technology changes.~~

~~Reference to prior version:~~ ~~*CIP-008, R1.4*~~	**~~Change Description and Justification:~~** ~~*Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.*~~

~~3.5~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems~~	~~Distribute updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 30 calendar days of the update being completed.~~	~~Evidence of distribution of updates may include, but is not limited to:~~ • ~~Emails;~~ • ~~USPS or other mail service;~~ • ~~Electronic distribution system; or~~ • ~~Training sign-in sheets.~~
~~**Reference to prior version:**~~ ~~*New Requirement*~~		~~**Change Description and Justification:** *Specifies activities required to maintain the plan.*~~	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~entity~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain ~~data or~~ evidence ~~for~~of each requirement in this standard for three calendar years~~ or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer~~.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the ~~duration~~time specified above, whichever is longer.
- ~~The Compliance Enforcement Authority~~The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

~~Table of Compliance Elements~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1~~	~~Long Term Planning~~	~~Lower~~	~~N/A~~	~~N/A~~	~~The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3)~~ ~~OR~~ ~~The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)~~ ~~OR~~ ~~The Responsible Entity has developed the Cyber Security Incident response plan(s), but~~	~~The Responsible Entity has not developed a Cyber Security Incident response plan to identify, classify, and respond to Cyber Security Incidents. (1.1)~~ ~~OR~~ ~~The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include processes to identify Reportable Cyber Security Incidents. (1.2)~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
					~~the plan does not include internal groups or individuals or external organizations that should receive communication of the Cyber Security Incident. (1.5)~~	
~~R2~~	~~Operations Planning~~ ~~Real-time Operations~~	~~Lower~~	~~The Responsible Entity has not tested the Cyber Security Incident response plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)~~	~~The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)~~	~~The Responsible Entity has not tested the Cyber Security Incident response plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1)~~ ~~OR~~ ~~The Responsible Entity does not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)~~	~~(2.1) The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan.~~ ~~OR~~ ~~The Responsible Entity does not use its Cyber Security Incident response plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)~~ ~~OR~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
						~~The Responsible Entity does not retain relevant records related to Reportable Cyber Security Incidents. (2.3)~~
~~R3~~	~~Operations Assessment~~	~~Lower~~	~~The Responsible Entity has not distributed updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 30 and less than 60 calendar days of the update being completed. (3.4)~~	~~The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 30 and less than 60 calendar days after the documentation required by 3.1. (3.2)~~ ~~OR~~ ~~The Responsible Entity has not updated the Cyber Security Incident response plan(s) within 30 and less than 60 calendar days of any of the following changes that the responsible entity~~	~~The Responsible Entity has not documented any lessons learned within 30 and less than 60 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1)~~ ~~OR~~ ~~The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 60 calendar days after the documentation required by 3.1. (3.2)~~ ~~OR~~	~~The Responsible Entity has not documented any lessons learned within 60 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1)~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
				~~determines would impact the ability to execute the plan: (3.3)~~ ~~• roles or responsibilities, or~~ ~~• Cyber Security Incident response groups or individuals, or~~ ~~• technology changes.~~ ~~OR~~ ~~The Responsible Entity has not distributed updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 60 calendar days of the update being completed. (3.4)~~	~~The Responsible Entity has not updated the Cyber Security Incident response plan(s) within 60 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.3)~~ ~~• roles or responsibilities, or~~ ~~• Cyber Security Incident response groups or individuals, or~~ ~~• technology changes.~~	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of ~~an incident~~a Cyber Security Incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary.

~~The reporting obligations for Reportable Cyber Security Incidents are found in EOP-004-2. This standard only requires the entity to identify such incidents. However, an entity may include identification and reporting procedures in the same plan to comply with both standards.~~

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the ~~incident~~Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. ~~TTXs~~Table top exercises (TTX) can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.~~2~~1 and (2) organizational or technology changes from Part 3.~~4~~2.

The documentation of lessons learned from Part 3.~~2~~1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a ~~BES~~ *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

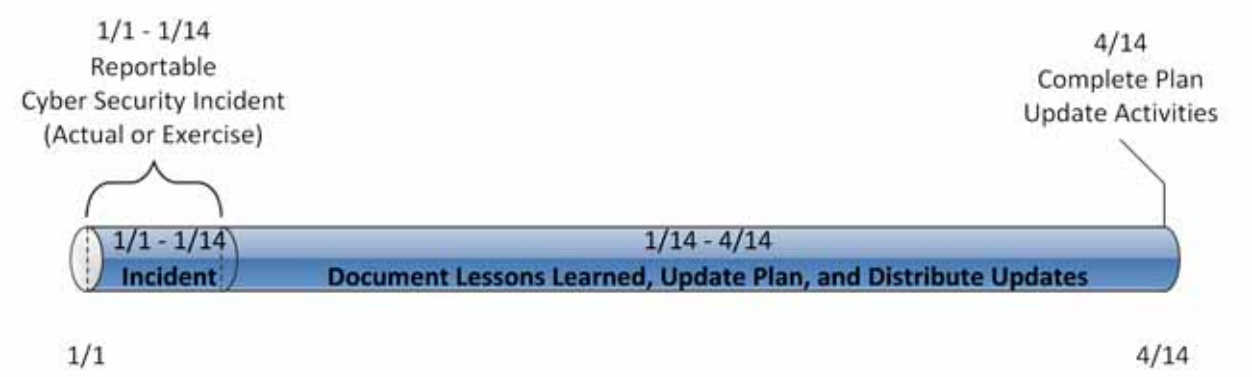

Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

~~Part 3.3 requires an entity to update the plan within 30 days of the documented lessons learned. This recognizes the time it may take to propose solutions to the lessons learned and complete the review and approval process.~~

~~Part 3.5 requires an entity to distribute the plan within 30 calendar days of the plan update. The measure specifies this can be accomplished through email, USPS, electronic distribution system (e.g., workflow software), or training records.~~

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the incident and documenting the lessons learned as soon after the incident as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the incident response team.

The plan change requirement in Part 3.~~4~~2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

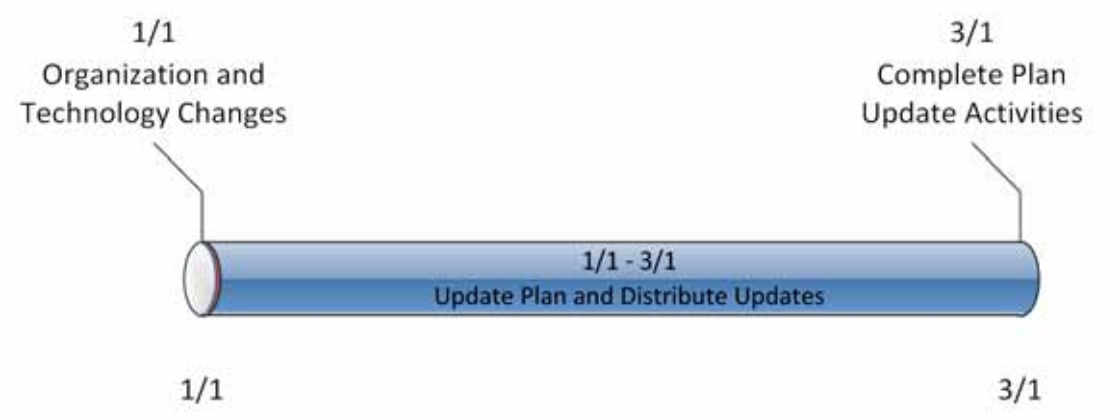

Figure 2: Timeline for Plan Changes in 3.4~~2~~2

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the third posting of Version 5 of the CIP Cyber Security Standards for a 30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the second posting and ballot.

Anticipated Actions	Anticipated Date
30-day Formal Comment Period with Parallel Successive Ballot	September 2012
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-009-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-5

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-009-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident

response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for R1: Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
Reference to prior version: *CIP-009, R1.1*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
Reference to prior version: *CIP-009, R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.
Reference to prior version: *CIP-009, R4*		**Change Description and Justification:** *Addresses FERC Order Paragraph 739 and 748. The modified wording was abstracted from Paragraph 744.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Addresses FERC Order Section 739 and 748.*	
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), per device capability. Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added requirement to address FERC Order No. 706, Paragraph 706.*	

Rationale for R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months between tests of the plan: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Minor wording change; essentially unchanged.*	

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
Reference to prior version: *CIP-009, R5*		**Change Description and Justification:** *Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.*	

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.*	

Rationale for R3: To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

Summary of Changes: Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	After completion of a recovery plan test or actual recovery, and not to exceed 90 calendar days: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *CIP-009, R1 and R3*		**Change Description and Justification:** *Added the timeframes for performing lessons learned and completing the plan updates.This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	After a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan, and not to exceed 60 calendar days: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the specific changes that would require an update.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation

procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons

learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

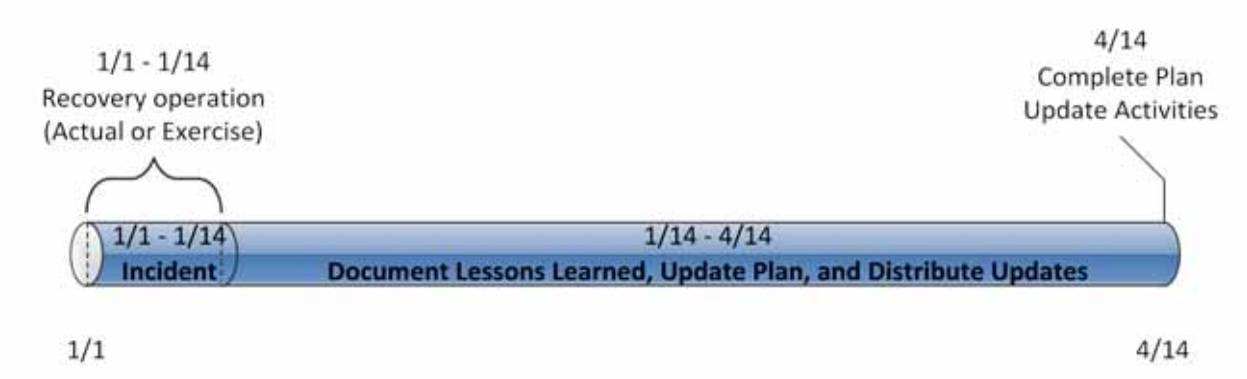

R1. **Figure 1: CIP-009-5 R3 Timeline**

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

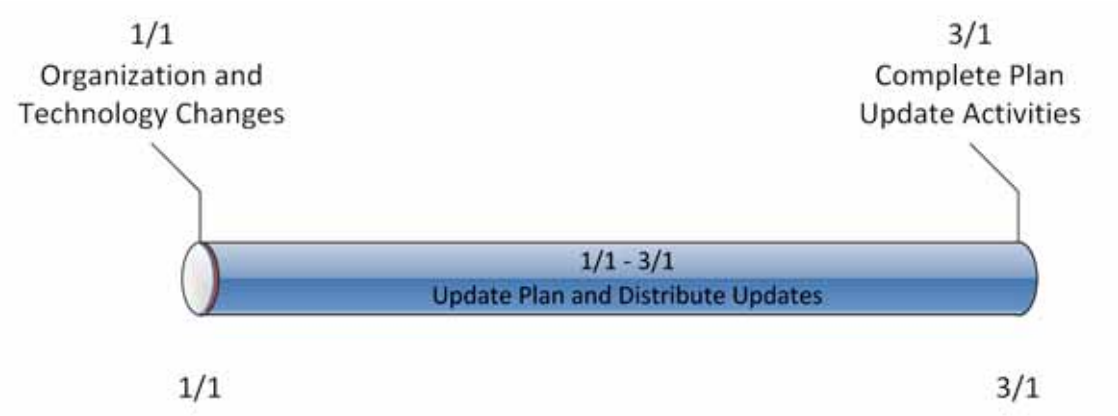

R2. **Figure 2: Timeline for Plan Changes in 3.2**

When notifying individuals of response plan changes, entities should keep in mind that recovery plans are considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the ~~second~~third posting of Version 5 of the CIP Cyber Security Standards for a ~~40~~30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ~~first~~ ballot.~~–~~ A second posting of Version 5 ~~reverts to the original organization of the standards with some changes and~~was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the ~~first~~second posting and ballot.

Anticipated Actions	Anticipated Date
~~40~~30-day Formal Comment Period with Parallel Successive Ballot	~~April~~September 2012
Recirculation ballot	~~June~~November 2012
BOT adoption	~~June~~December 2012

Effective Dates

1. **24 Months Minimum** – ~~The Version 5~~ CIP ~~Cyber Security Standards, except for CIP-003-5, Requirement R2,~~-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. ~~CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this Implementation Plan.~~ [1]

2. In those jurisdictions where no regulatory approval is required, ~~the Version~~ CIP-009-5 ~~CIP Cyber Security Standards, except for CIP-003-5, Requirement R2,~~ shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, ~~and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval,~~ or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] ~~In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their Implementation Plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the Implementation Plan and standards for CIP-002-4 through CIP-009-4.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-5

3. Purpose: ~~–~~To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: ~~———~~ For the purpose of the requirements contained herein, the following list of ~~Functional Entities~~functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific ~~Functional Entity~~functional entity or subset of ~~Functional Entities~~functional entities are the applicable entity or entities, the ~~Functional Entity~~functional entity or ~~Entities~~entities are specified explicitly.

4.1.1 Balancing Authority

~~**4.1.2 Distribution Provider** that owns **Facilities described in 4.2.2**~~

~~**4.1.3 Generator Operator**~~

~~**4.1.4 Generator Owner**~~

~~**4.1.5 Interchange Coordinator**~~

~~**4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1**~~

~~**4.1.7 Reliability Coordinator**~~

~~**4.1.8 Transmission Operator**~~

~~**4.1.9 Transmission Owner**~~

~~**4.2. Facilities:**~~

~~**4.2.1 Load Serving Entity:** One~~one or more of the ~~UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard~~following Facilities, systems, and ~~that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.~~

~~**4.2.2**~~**4.1.2** ~~**Distribution Provider**: One or more of the Systems or programs designed, installed, and operated~~equipment for the protection or restoration of the BES:

4.1.2.1 ~~A~~ Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS ~~System~~) system that~~-~~:

4.1.2.1.1 is part of a Load shedding program ~~required by~~that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ~~that~~

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 ~~A~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 ~~A~~Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3~~4~~.2.2 Responsible Entities listed in 4.1 other than Distribution Providers ~~and Load-Serving Entities~~: ~~All BES Facilities.~~:

All BES Facilities.

4.2.4~~4~~.2.3 Exemptions: The following are exempt from Standard CIP-~~002~~009-5:

4.2.4.~~1~~4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.~~2~~4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.~~3~~4.2.3.3 ~~In nuclear plants, the Systems~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for ~~a~~the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as ~~they feel~~it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

~~Applicability Columns in Tables:~~

~~Each table row~~ Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an ~~applicability~~"Applicable Systems" column to further define the scope of systems to which a specific requirement row applies ~~to BES Cyber Systems and associated Cyber Assets.~~ . The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the ~~applicability~~"Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- ~~**Associated**~~ **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System ~~in the applicability column~~. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- ~~**Associated**~~ **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a ~~corresponding~~referenced high impact BES

Cyber System or medium impact BES Cyber System with External Routable Connectivity~~ in the applicability column~~.

B. Requirements and Measures

Rationale for R1: Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber ~~Assets and BES Cyber Systems~~System functionality occurs.

Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable ~~items~~requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable ~~items~~requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	~~Evidence~~An example of evidence may include, but is not limited to, one or more plans that include language identifying ~~specific~~ conditions for activation of the recovery plan(s).
Reference to prior version: *CIP-009, R1.1*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	Roles and responsibilities of responders.	~~Evidence~~An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
Reference to prior version: *CIP-009, R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	~~Evidence~~An example of evidence may include, but is not limited to, documentation of specific processes for the backup~~,~~ and storage~~,~~ of information required to ~~successfully~~ recover BES Cyber System functionality.
Reference to prior version: *CIP-009, R4*		**Change Description and Justification:** *~~Minor~~Addresses FERC Order Paragraph 739 and 748. The modified wording ~~changes; essentially unchanged~~was abstracted from Paragraph 744.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	~~Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.~~One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	~~Evidence~~ An example of evidence may include, but is not limited to, ~~dated evidence or~~ logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Addresses FERC Order Section 739 and 748.*	

1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	~~Processes~~One or more processes to preserve data~~, except~~ for ~~CIP Exceptional Circumstances, for analysis or diagnosis of~~determining the cause of ~~any event~~a Cyber Security Incident that triggers activation of the recovery plan(s~~).~~), per device capability. Data preservation should not impede or restrict recovery.	~~Evidence~~An example of evidence may include, but is not limited to, procedures to preserve data~~;~~, such as preserving a corrupted drive~~,~~ or making a data mirror of the system before proceeding with recovery~~, or taking the important assessment steps necessary to avoid reintroducing the precipitating or corrupted data~~.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added requirement to address FERC Order No. 706, Paragraph 706.*	

~~**Rationale for R2:** To verify the Responsible Entities Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.~~

~~NIST SP 800-84 identifies the following types of exercises widely used in information system programs by single organizations:~~

~~**Tabletop Exercises.** Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an Emergency and their responses to a particular Emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.~~

~~**Functional Exercises.** Functional exercises allow personnel to validate their operational readiness for Emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, Emergency notifications, System equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual Emergency situation, but in a simulated manner.~~

Rationale for R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable ~~items~~requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable ~~items~~requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	Test each of the recovery ~~plan(s)~~plans referenced in Requirement R1 at least once ~~each calendar year, not to exceed~~every 15 calendar months between tests of the plan: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	~~Evidence~~An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once ~~each calendar year, not to exceed~~every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Minor wording change; essentially unchanged.*	

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	Test a representative sample of information used ~~in the recovery of~~ to recover BES Cyber ~~Systems that is stored on backup media~~System functionality at least once ~~each calendar year, not to exceed~~every 15 calendar months ~~between tests,~~ to ensure that the information is useable and is compatible with current ~~system~~ configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	~~Evidence~~ An example of evidence may include, but is not limited to, ~~dated evidence of a~~operational logs or test ~~of information used in~~results with criteria for testing the ~~recovery of BES Cyber Systems that is stored on backup media when initially stored~~usability (e.g. sample tape load, browsing tape contents) and ~~at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and is compatible~~compatibility with current system configurations~~.~~ (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
Reference to prior version: *CIP-009, R5*		**Change Description and Justification:** *~~Combined~~Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement ~~from CIP-009 R5 included requirement to test when initially stored. Addresses~~Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.*	

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	~~Evidence~~ Examples of evidence may include, but ~~is~~are not limited to ~~Dated evidence~~, dated documentation of: • An operational exercise ~~prior to the effective date of the standard and~~ at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual ~~incident~~recovery response ~~which~~that occurred within the 36 calendar month timeframe that exercised the recovery plans.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.*	

Rationale for R3: To ~~enable~~improve the ~~continued~~ effectiveness of ~~the Responsible Entities response plan's for planned and consistent restoration of~~ BES Cyber System~~(s).~~

~~**Summary of Changes:** Addressed~~ recovery plan~~ review, update, and communication specifications~~ (s) following a test, and to ensure ~~that~~ the maintenance and distribution of the recovery ~~plans remain updated~~plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and ~~individuals are aware of the~~ (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates~~.~~ and distributes the plan.

Summary of Changes: Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable ~~items~~requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable ~~items~~requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication

Part	Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~	Requirements	Measures
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	~~Document any identified deficiencies or lessons learned associated with each~~ After completion of a recovery plan test or actual ~~incident~~ recovery ~~within 30~~, and not to exceed 90 calendar days ~~after completion of~~ : 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the ~~test or recovery.~~ absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	~~Evidence~~An example of evidence may include, but is not limited to, ~~dated~~all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery ~~within 30 calendar days after completion of the test~~ or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
~~Reference to prior version:~~ *~~CIP-009, R1 and R3~~*		**~~Change Description and Justification:~~** *~~Added the time frame for update.~~*	
~~3.2~~**Reference to prior version:** *CIP-009, R1 and R3*	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems at Control Centers.~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Update the recovery plan(s) based on any documented deficiencies or lessons learned within 30 calendar days after the documentation required by Part 3.1.~~**Change Description and Justification:** *Added the timeframes for performing lessons learned and completing the plan updates.This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.*	~~Evidence may include, but is not limited to, dated, documented deficiencies or lessons learned required by Part 3.1 and the dated, revised recovery plan(s) based on that documentation.~~
~~Reference to prior version:~~ *~~CIP-009, R3~~*		**~~Change Description and Justification:~~** *~~Added the timeframe for update.~~*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
3.~~3~~2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ 1. ~~Associated Electronic Access Control or Monitoring Systems~~EACMS; and 2. PACS	~~Update recovery plan(s) within 30 calendar days of any of~~ After a change to the ~~following changes~~roles or responsibilities, responders, or technology that the Responsible Entity determines would impact ~~the plan or~~ the ability to execute the recovery plan, and not to exceed 60 calendar days: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan~~:~~ of the updates. ~~• Roles or responsibilities; or~~ ~~• Technology changes.~~	~~Evidence~~ An example of evidence may include, but is not limited to, ~~dated documentation reflecting~~all of the following: Dated and revised recovery plan with changes ~~made~~ to the ~~recovery plan(s) in response to the following changes that the responsible entity determined would impact the plan or the ability to execute the plan:~~ 1. ~~Roles~~roles or responsibilities~~;~~, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • ~~Technology changes.~~Electronic distribution system; or • Training sign-in sheets.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
~~**Reference to prior version:**~~ ~~*New Requirement*~~		~~**Change Description and Justification:** *Ensures that recovery plans stay updated.*~~	
~~3.4~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems at Control Centers.~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~Distribute recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within 30 calendar days of the update being completed.~~	~~Evidence of distribution of updates may include, but is not limited to:~~ ~~• Emails;~~ ~~• USPS or other mail service;~~ ~~• Electronic distribution system; or~~ ~~• Training sign-in sheets.~~
Reference to prior version: *New Requirement*		**Change Description and Justification:** ~~*Ensures that recovery personnel are aware of*~~ *Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to* any *changes* ~~*to recovery plans*~~*. The modifications make clear the specific changes that would require an update*.	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~entity~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain ~~data or~~ evidence ~~for~~of each requirement in this standard for three calendar years~~ or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer~~.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the ~~duration~~time specified above, whichever is longer.
- ~~The Compliance Enforcement Authority~~The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

~~Table of Compliance Elements~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1~~	~~Long-term Planning~~	~~Medium~~	~~N/A~~	~~The Responsible Entity has developed recovery plan(s), but the plan(s) do not address all of the requirements included in Parts 1.2 through 1.5.~~	~~The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.~~	~~The Responsible Entity has not created recovery plan(s) for BES Cyber Systems.~~ ~~OR~~ ~~The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1.~~ ~~OR~~ ~~The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.~~
~~R2~~	~~Operations Planning~~ ~~Real-time~~	~~Lower~~	~~The Responsible Entity has not tested the recovery plan(s) according to R2 Part~~	~~The Responsible Entity has not tested the recovery plan(s) within 16 calendar months,~~	~~The Responsible Entity has not tested the recovery plan(s) according to R2 Part~~	~~The Responsible Entity has not tested the recovery plan(s) according to R2 Part~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
	~~**Operations**~~		~~2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)~~ ~~OR~~ ~~The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2)~~ ~~OR~~ ~~The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)~~	~~not exceeding 17 calendar months between tests of the plan. (2.1)~~ ~~OR~~ ~~The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2)~~ ~~OR~~ ~~The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)~~	~~2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1)~~ ~~OR~~ ~~The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (2.2)~~ ~~OR~~ ~~The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (2.3)~~	~~2.1 within 18 calendar months between tests of the plan. (2.1)~~ ~~OR~~ ~~The Responsible Entity has not tested the information used in the recovery of BES Cyber Systems according to R2 Part 2.2 within 19 calendar months between tests. (2.2)~~ ~~OR~~ ~~The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3)~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R3~~	~~Operations Assessment~~	~~Lower~~	~~The Responsible Entity has not distributed updates of the recovery plan to each person or group with a defined role in the recovery plan(s) within 30 and less than 60 calendar days of the update being completed. (3.4)~~	~~The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 30 and less than 60 calendar days after the documentation required by R3 Part 3.1. (3.1)~~ ~~OR~~ ~~The Responsible Entity has not updated the Recovery plan(s)(s) within 30 and less than 60 calendar days of any of the changes listed in R3 Part 3.3 that the responsible entity determines would impact the ability to execute the plan (3.3)~~	~~The Responsible Entity has not documented any lessons learned within 30 and less than 60 calendar days of each recovery plan test or actual incident recovery. (3.1)~~ ~~OR~~ ~~The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 60 calendar days after the documentation required by R3 Part 3.2. (3.2)~~ ~~OR~~ ~~The Responsible Entity has not updated the recovery plan(s)(s) within 60 calendar~~	~~The Responsible Entity has not documented any lessons learned within 60 calendar days of each recovery plan test or actual incident recovery. (3.1)~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
				~~OR~~ ~~The Responsible Entity has not distributed updates of the recovery plan(s) to each person or group with a defined role in the recovery plan(s) within 60 calendar days of the update being completed. (3.4)~~	~~days of any of the changes listed in R3 Part 3.3 that the responsible entity determines would impact the ability to execute the plan. (3.3)~~	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

~~(SEE FAQs AND CIPC GUIDELINES AS A BASIS.)~~**Section 4 – Scope of Applicability of the CIP Cyber Security Standards**

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

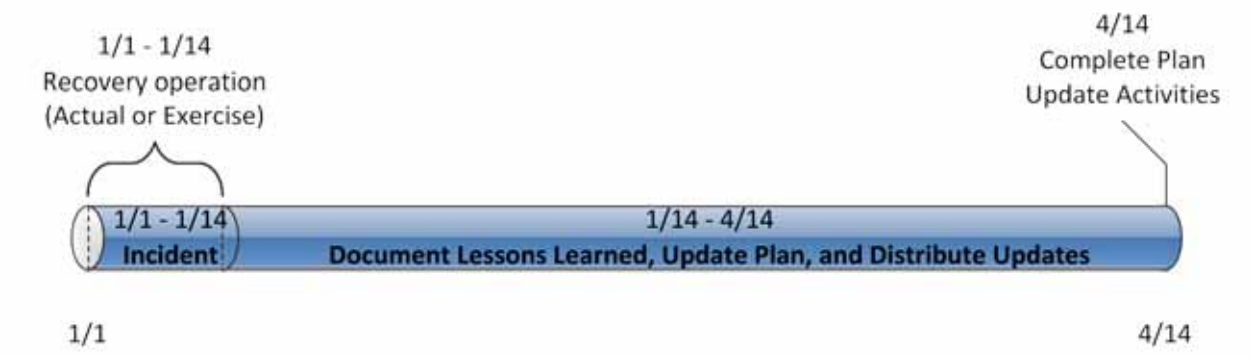

R1. **Figure 1: CIP-009-5 R3 Timeline**

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

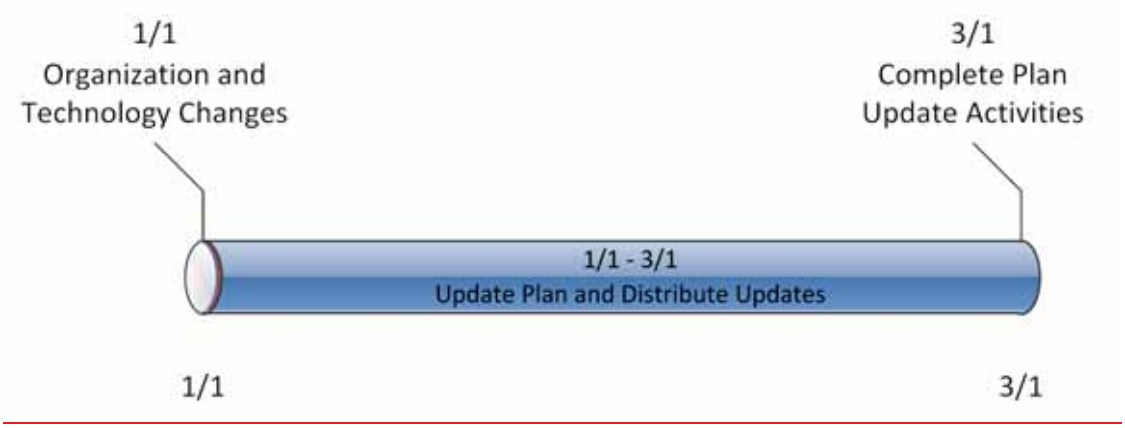

R2. **Figure 2: Timeline for Plan Changes in 3.2**

When notifying individuals of response plan changes, entities should keep in mind that recovery plans are considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the third posting of Version 5 of the CIP Cyber Security Standards for a 30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the second posting and ballot.

Anticipated Actions	Anticipated Date
30-day Formal Comment Period with Parallel Successive Ballot	September 2012
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-010-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-010-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-1

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-010-1:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-010-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the

documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)**– Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)**– Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System

B. Requirements and Measures

Rationale – R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.
Reference to prior version: *New Requirement*		**Change Rationale:** *The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.
Reference to prior version: *CIP-007-3, R9; CIP-003-3, R6*		**Change Rationale:** *The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3, Requirement R6.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
Reference to prior version: *CIP-007-3, R9; CIP-005-3, R5*		**Change Rationale:** *Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment, or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.* *This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.*	

Rationale – R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.
Reference to prior version: *New Requirement*		**Change Rationale:** *The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.* *This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397.* *Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.*	

Rationale – R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.
Reference to prior version: *CIP-005-4, R4; CIP-007-4, R8*		**Change Rationale:** *As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.* *As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.*	
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).
Reference to prior version: *CIP-005-3, R4.5; CIP-007-3, R8.4*		**Change Rationale:** *Added a requirement for an entity planned date of completion as per the directive in FERC Order No. 706, Paragraph 643.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If

additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-5. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-5 R2.1 requires entities to track, evaluate, and install security patches, CIP-010 R1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.

4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the ~~second~~third posting of Version 5 of the CIP Cyber Security Standards for a ~~40~~30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ~~first~~ ballot.~~–~~ A second posting of Version 5 ~~reverts to the original organization of the standards with some changes and~~was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the ~~first~~second posting and ballot.

Anticipated Actions	Anticipated Date
~~40~~30-day Formal Comment Period with Parallel Successive Ballot	~~April~~September 2012
Recirculation ballot	~~June~~November 2012
BOT adoption	~~June~~December 2012

Effective Dates

1. **24 Months Minimum** – ~~The Version 5~~ CIP ~~Cyber Security Standards, except for CIP-003-5, Requirement R2,~~ -010-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. ~~CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.~~[1]

2. In those jurisdictions where no regulatory approval is required, ~~the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2,~~CIP-010-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, ~~and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval,~~ or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] ~~In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.~~

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-1

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of ~~Functional Entities~~functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific ~~Functional Entity~~functional entity or subset of ~~Functional Entities~~functional entities are the applicable entity or entities, the ~~Functional Entity~~functional entity or ~~Entities~~entities are specified explicitly.

4.1.1 Balancing Authority

~~**4.1.2 Distribution Provider** that owns **Facilities described in 4.2.2**~~

~~**4.1.3 Generator Operator**~~

~~**4.1.4 Generator Owner**~~

~~**4.1.5 Interchange Coordinator**~~

~~**4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1**~~

~~**4.1.7 Reliability Coordinator**~~

~~**4.1.8 Transmission Operator**~~

~~**4.1.9 Transmission Owner**~~

~~**4.2. Facilities:**~~

~~**4.2.1 Load Serving Entity:** One~~one or more of the ~~UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard~~following Facilities, systems, and ~~that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.~~

~~**4.2.2**~~**4.1.2** ~~**Distribution Provider**: One or more of the Systems or programs designed, installed, and operated~~equipment for the protection or restoration of the BES:

4.1.2.1 A Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS System) system that-:

4.1.2.1.1 is part of a Load shedding program required bythat is subject to one or more requirements in a NERC or Regional Reliability Standard; and that

•**4.1.2.1.2** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

•**4.1.2.2** AEach Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required bysubject to one or more requirements in a NERC or Regional Reliability Standard.

•**4.1.2.3** AEach Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is required bysubject to one or more requirements in a NERC or Regional Reliability Standard.

•**4.1.2.4** Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~4.2.3~~4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers ~~and Load-Serving Entities~~: ~~All BES Facilities.~~:

All BES Facilities.

~~4.2.4~~4.2.3 Exemptions: The following are exempt from Standard CIP-~~002-5~~010-1:

~~4.2.4.1~~4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.4.2~~4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.4.3~~4.2.3.3 ~~In nuclear plants, the Systems~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-010-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table*

Reference]." The referenced table requires the applicable items in the procedures for ~~a~~the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as ~~they feel~~it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

~~Applicability Columns in Tables:~~

~~Each table row~~ Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an ~~applicability~~"Applicable Systems" column to further define the scope of systems to which a specific requirement row applies ~~to BES Cyber Systems and associated Cyber Assets.~~ . The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- ~~**Associated**~~ **Electronic Access Control or Monitoring Systems** ~~–~~**(EACMS)**– Applies to each Electronic Access Control or Monitoring System associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System ~~in the applicability column~~. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

- ~~Associated~~ **Physical Access Control Systems –(PACS)–** Applies to each Physical Access Control System associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity~~ in the applicability column~~.
- ~~Associated~~ **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System~~ in the applicability column.~~

B. Requirements and Measures

Rationale – R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-010-1 Table R1 – Configuration Change Management*. *[Violation Risk Factor: ~~Lower~~Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following ~~for each Cyber Asset identified, individually or by group~~items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed ~~on the BES Cyber Asset~~; 1.1.3. Any custom software ~~developed for the entity~~installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset~~.~~, individually or by group.
Reference to prior version: *New Requirement*		**Change Rationale:** *The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.
Reference to prior version: *CIP-007-3, R9; CIP-003-3, R6*		**Change Rationale:** *The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3, Requirement R6.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration ~~and other documentation required by CIP-005 and CIP-007~~ as necessary within 30 calendar days of completing the change.	~~Evidence~~An example of evidence may include, but is not limited to, updated baseline documentation ~~for changes that impacted CIP-005 or CIP-007 documentation, and relevant CIP-005 or CIP-007 documentation,~~ with a date that is within 30 calendar days of the date of the completion of the change.
Reference to prior version: *CIP-007-3, R9; CIP-005-3, R5*		**Change Rationale:** *Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ ~~Associated Protected Cyber Assets~~ 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls ~~identified~~ in CIP-005~~, CIP-006,~~ and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify ~~these~~that required cyber security controls determined in 1.4.1 ~~and the BES Cyber System availability~~ are not adversely affected; and 1.4.3. Document the results of the verification.	~~Evidence~~An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.5	High Impact BES Cyber ~~System~~Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment ~~(or~~, or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects~~)~~, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	~~Evidence~~An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.* *This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.*	

Rationale – R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring. [Violation Risk Factor: ~~Lower~~Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R2 – Configuration Monitoring			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; and 2. PCA	~~Where technically feasible, monitor continuously or periodically, not to exceed~~Monitor at least once every 35 calendar days~~,~~ for changes to the baseline configuration (as ~~defined per CIP-010~~described in Requirement R1, Part 1.1~~) and document~~). Document and investigate detected unauthorized changes.	~~Evidence~~An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration ~~of the BES Cyber System~~ along with records of investigation for any unauthorized changes that were detected ~~by the system~~.
Reference to prior version: *New Requirement*		**Change Rationale:** *The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.* *This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397.* *Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.*	

Rationale – R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-010-1 Table R3– Vulnerability Assessments. [Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	At least once every ~~calendar year, not to exceed~~ 15 calendar months ~~between assessments~~, conduct a paper or active vulnerability assessment ~~to determine the extent to which the cyber security controls identified in CIP-005, CIP-006, and CIP-007 are implemented correctly and operating as designed~~.	~~Evidence~~Examples of evidence may include, but ~~is~~are not limited to: • A document listing the date of the assessment (performed at least once every ~~calendar year, not to exceed~~ 15 calendar months ~~between assessments~~), the controls assessed for each BES Cyber System along with the method of assessment~~, and the individuals who performed the assessment;~~,; or • A document listing the date of the assessment and the output of ~~the~~any tools used to perform the assessment.
Reference to prior version: *CIP-005-4, R4; CIP-007-4, R8*		**Change Rationale:** *As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months ~~between assessments,~~: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a ~~test environment (or in a~~ production environment where the test is performed in a manner that minimizes adverse effects~~)~~, that models the baseline configuration of the BES Cyber System in a production environment~~. If~~; and 3.2.2 Document the results of the testing and, if a test environment was used, ~~document~~ the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	~~Evidence~~An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months ~~between assessments~~), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.* *As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	
3.3	High Impact BES Cyber Systems and their associated: ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PCA	~~Except~~Prior to adding a new Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements ~~(~~of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing ~~BES Cyber Asset), prior to adding a new Cyber Asset perform an active vulnerability assessment of the new Cyber Asset.~~ Cyber Asset.	~~Evidence~~An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of ~~the~~any tools used to perform the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems~~.~~ and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	~~Evidence~~An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).
Reference to prior version: *CIP-005-3, R4.5; CIP-007-3, R8.4*		**Change Rationale:** *Added a requirement for an entity planned date of completion as per the directive in FERC Order No. 706, Paragraph 643.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~entity~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain ~~data or~~ evidence ~~for~~of each requirement in this standard for three calendar years~~ or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer~~.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the ~~duration~~time specified above, whichever is longer.
- ~~The Compliance Enforcement Authority~~The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

~~Table of Compliance Elements~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1~~	~~Operations Planning~~	~~Medium~~	~~N/A~~	~~N/A~~	~~The Responsible Entity has established a configuration management program, but failed to authorize any changes to the baseline configuration and to document those changes.~~ ~~OR~~ ~~The Responsible Entity updated the baseline configuration, but failed to update the required documentation within 30-days of the change being completed.~~	~~The Responsible Entity has not established any configuration management programs.~~ ~~OR~~ ~~The Responsible Entity did not implement a configuration management program~~ ~~OR~~ ~~The Responsible Entity has established a configuration management program, but failed to establish a documented baseline~~ ~~OR~~ ~~The Responsible Entity has established a configuration management program, but with respect to the~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
						~~changes in the baseline configuration, did not determine the required cyber security controls identified in CIP-005, CIP-006, and CIP-007 that could be impacted by the changes; or did not verify that the controls were not adversely affected when the change was implemented.~~
~~R2~~	~~Operations Planning~~	~~Medium~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity has not established a configuration monitoring process for changes to the baseline.~~ ~~OR~~ ~~The Responsible Entity has not investigated a detected unauthorized change to the baseline configuration.~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
						~~OR~~ ~~The Responsible Entity has established a configuration monitoring process for changes to the baseline but failed to document a detected unauthorized change.~~
~~R3~~	~~Long-term Planning and Operations Planning~~	~~Medium~~	~~The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems.~~	~~The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not performed an active vulnerability assessment on a new Cyber Asset prior to adding it to an applicable BES Cyber System.~~ ~~OR~~	~~The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems.~~	~~The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems.~~ ~~OR~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
				~~The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems.~~		~~The Responsible Entity has not established any vulnerability assessment processes for one of its applicable BES Cyber Systems.~~ ~~OR~~ ~~The Responsible Entity has established and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but failed to perform an active vulnerability assessment in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
						~~configuration of its applicable BES Cyber Systems.~~ ~~OR~~ ~~The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, and the execution status of the mitigation plans.~~

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If

additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-5. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-5 R2.1 requires entities to track, evaluate, and install security patches, CIP-010 R1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their ~~Vulnerability Assessment~~vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.

3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the third posting of Version 5 of the CIP Cyber Security Standards for a 30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the second posting and ballot.

Anticipated Actions	Anticipated Date
30-day Formal Comment Period with Parallel Successive Ballot	September 2012
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-011-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-011-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-1

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-011-1:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-011-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)**– Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System

Rationale – R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Summary of Changes: CIP 003-4 R4, R4.2, and R 4.3 have been moved to CIP 011 R1. CIP-003-4, Requirement R4.1 was moved to the definition of BES Cyber System Information.

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-1 Table R1 – Information Protection. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Methods to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.
Reference to prior version: *CIP-003-3, R4; CIP-003-3, R4.2*		**Change Rationale:** *The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection (*e.g., confidential, public, internal use only, etc.*) This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.*	

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedures for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).
Reference to prior version: *CIP-003-3, R4;*		**Change Rationale:** *The SDT changed the language from "protect" information to "Procedures for protecting and securely handling" to clarify the protection that is required.*	

Rationale – R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.
Reference to prior version: *CIP-007-3, R7.2*		**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*	

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of a an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.
Reference to prior version: *CIP-007-3, R7.1*		**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.* *The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the

analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

~~**Note**: On May 8, 2012, NERC was alerted that the text contained in the Rationale box for Requirement R1 of CIP-011-1 appeared to be incomplete.~~

~~This revised draft corrects the text box size to display all of the text (none of the text was changed).~~

~~No other changes were made to this standard or any of the other CIP V5 standards currently posted.~~

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the ~~second~~third posting of Version 5 of the CIP Cyber Security Standards for a ~~40~~30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ~~first~~ ballot.~~–~~ A second posting of Version 5 ~~reverts to the original organization of the standards with some changes and~~was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706~~,~~ approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the ~~first~~second posting and ballot.

Anticipated Actions	Anticipated Date
~~40~~30-day Formal Comment Period with Parallel Successive Ballot	~~April~~September 2012
Recirculation ballot	~~June~~November 2012
BOT adoption	~~June~~December 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2,-011-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]

2. In those jurisdictions where no regulatory approval is required, Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2,CIP-011-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2, shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-1

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of ~~Functional Entities~~functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific ~~Functional Entity~~functional entity or subset of ~~Functional Entities~~functional entities are the applicable entity or entities, the ~~Functional Entity~~functional entity or ~~Entities~~entities are specified explicitly.

4.1.1 Balancing Authority

~~**4.1.2 Distribution Provider** that owns **Facilities described in 4.2.2**~~

~~**4.1.3 Generator Operator**~~

~~**4.1.4 Generator Owner**~~

~~**4.1.5 Interchange Coordinator**~~

~~**4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1**~~

~~**4.1.7 Reliability Coordinator**~~

~~**4.1.8 Transmission Operator**~~

~~**4.1.9 Transmission Owner**~~

~~**4.2. Facilities:**~~

~~**4.2.1 Load Serving Entity:** One~~one or more of the ~~UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard~~following Facilities, systems, and ~~that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.~~

~~**4.2.2**~~**4.1.2 ~~Distribution Provider~~**~~: One or more of the Systems or programs designed, installed, and operated~~equipment for the protection or restoration of the BES:

4.1.2.1 ~~A~~ Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS ~~System~~) system that~~-~~:

4.1.2.1.1 is part of a Load shedding program ~~required by~~that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ~~that~~

•**4.1.2.1.2** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

•**4.1.2.2** ~~A~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

•**4.1.2.3** ~~A~~Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

•**4.1.2.4** Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.3~~4.2.2~~ Responsible Entities listed in 4.1 other than Distribution Providers ~~and Load-Serving Entities~~: ~~All BES Facilities.~~:

All BES Facilities.

4.2.4~~4.2.3~~ Exemptions: The following are exempt from Standard CIP-~~002-5~~011-1:

4.2.4.1~~4.2.3.1~~ Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2~~4.2.3.2~~ Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3~~4.2.3.3~~ ~~In nuclear plants, the Systems~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-011-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for ~~a~~the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as ~~they feel~~it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

~~Applicability Columns in Tables:~~

~~Each table row~~ Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an ~~applicability~~"Applicable Systems" column to further define the scope of systems to which a specific requirement row applies ~~to BES Cyber Systems and associated Cyber Assets.~~ . The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the ~~applicability~~"Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- ~~**Associated**~~ **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System ~~in the applicability column~~. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- ~~**Associated**~~ **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity ~~in the applicability column~~.

- ~~**Associated**~~ **Protected Cyber Assets** ~~–~~**(PCA)**~~–~~ Applies to each Protected Cyber Asset associated with a ~~corresponding~~referenced high impact BES Cyber System or medium impact BES Cyber System ~~in the applicability column.~~

Rationale – R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Summary of Changes: CIP 003-4 R4, R4.2, and R 4.3 have been moved to CIP 011 R1. CIP-003-4, Requirement R4.1 was moved to the definition of BES Cyber System Information.

B. Requirements and Measures

R1. Each Responsible Entity shall implement ~~an~~, in a manner that identifies, assesses, and corrects deficiencies, one or more documented information protection program(s) that collectively includes each of the applicable ~~items~~requirement parts in *CIP-011-1 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning~~.]~~].*

M1. Evidence for the information protection program must include the applicable ~~items~~requirement parts in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. EACMS; and 2. PACS	~~One or more documented and implemented methods~~Methods to identify information that meets the definition of BES Cyber System Information.	~~Evidence may~~Examples of acceptable evidence include, but ~~is~~are not limited to~~,~~: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify ~~it~~BES Cyber System Information as ~~BES Cyber System Information;~~ designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or ~~designated~~ electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.
Reference to prior version: *CIP-003-3, R4; CIP-003-3, R4.2*		**Change Rationale:** *The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection* (e.g., confidential, public, internal use only, etc.) *This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.*	

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. EACMS; and 2. PACS	~~One or more documented~~Procedures for protecting and ~~implemented procedures for~~securely handling BES Cyber System Information, including storage, transit, and use.	~~Evidence may~~Examples of acceptable evidence include, but ~~is~~are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure~~; or~~ • ~~Procedures for handling, which include topics such as the storage, transit, and use of BES Cyber System Information.~~ • (s).
Reference to prior version: *CIP-003-3, R4; ~~CIP-003-3 R5.3~~*		**Change Rationale:** *The SDT ~~removed~~changed the language ~~to~~from "protect" information to "Procedures for protecting and ~~replaced it with "~~securely handling" to clarify the protection that is required.*	

~~CIP-011-1 Table R1 – Information Protection~~			
~~Part~~	~~Applicable BES Cyber Systems and associated Cyber Assets~~	~~Requirement~~	~~Measure~~
~~1.3~~	~~High Impact BES Cyber Systems~~ ~~Medium Impact BES Cyber Systems~~ ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~	~~At least once every calendar year, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.~~	~~Evidence may include, but is not limited to, once every calendar year, not to exceed 15 months between assessments, the documented review of adherence to its BES Cyber System Information protection program, assessment results, action plan, and evidence to demonstrate that the action plan was implemented.~~
~~**Reference to prior version:**~~ ~~*CIP-003-3, R4.3*~~		~~**Change Rationale:** *No significant changes.*~~	

Rationale – R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable ~~items~~requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable ~~items~~requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except ~~in other high impact or medium impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Asset~~for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset~~.~~ ~~If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information, the responsible entity shall maintain chain-of-custody, which identifies who has possession of the device while it is outside of a Physical Security Perimeter.~~ data storage media.	~~Evidence may~~Examples of acceptable evidence include, but ~~is~~are not limited to: • Records ~~of~~tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information~~;~~ such as clearing, purging, or destroying; or • ~~If removed from~~Records tracking actions such as encrypting, retaining in the Physical Security Perimeter ~~prior to action taken~~or other methods used to prevent unauthorized retrieval of ~~information, a chain of custody record that was maintained.~~ • BES Cyber System Information.

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R7.2*		**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*	

CIP-011-1 Table R2 – ~~Media~~BES Cyber Asset Reuse and Disposal			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**

CIP-011-1 Table R2 – ~~Media~~BES Cyber Asset Reuse and Disposal			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: ~~Associated Physical Access Control Systems~~ ~~Associated Electronic Access Control or Monitoring Systems~~ 1. ~~Associated Protected Cyber Assets~~EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media. ~~If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity shall maintain chain of custody, which identifies who has possession of the device while it is outside of a Physical Security Perimeter.~~	~~Evidence may~~Examples of acceptable evidence include, but ~~is~~are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of a an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of ~~a~~ an applicable Cyber Asset~~;~~. ~~• Other records showing actions taken to prevent unauthorized retrieval such as encrypting, retaining in the Physical Security Perimeter; or~~ ~~• If removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval of information, chain of custody record that was maintained.~~

CIP-011-1 Table R2 – ~~Media~~BES Cyber Asset Reuse and Disposal			
Part	**Applicable ~~BES Cyber~~ Systems ~~and associated Cyber Assets~~**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R7.1*		**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.* *The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~entity~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain ~~data or~~ evidence ~~for~~of each requirement in this standard for three calendar years~~ or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer~~.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the ~~duration~~time specified above, whichever is longer.
- ~~The Compliance Enforcement Authority~~The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

~~Table of Compliance Elements~~

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1~~	~~Operations Planning~~	~~Medium~~	~~N/A~~	~~The Responsible Entity has implemented a BES Cyber System Information protection program that includes one or more methods to identify BES Cyber System Information, one or more handling procedures for BES Cyber System Information, and has assessed adherence periodically as stated in Part 1.3, but has failed to implement an action plan to remediate deficiencies identified during the assessment.~~	~~The Responsible Entity has implemented a BES Cyber System Information protection program that includes one or more methods to identify BES Cyber System Information and one or more handling procedures for BES Cyber System Information, but has failed to assess adherence periodically as stated in Part 1.3, to its BES Cyber System Information protection program.~~	~~The Responsible Entity has not implemented a BES Cyber System Information protection program.~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program, but has not implemented one or more methods to identify BES Cyber System Information~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information~~

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						protection program, but has not implemented one or more procedures for handling BES Cyber System Information.
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity failed to maintain chain of custody for Cyber Assets that contain BES Cyber System Information that have been removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval or destroying the data storage media.	The Responsible Entity has documented one or more processes, including both reuse and disposal, to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Assets, but the Responsible Entity either failed to take action to prevent the unauthorized retrieval of BES Cyber System Information from a Cyber Asset that contained BES Cyber System Information or failed to destroy the	The Responsible Entity has not documented or implemented any disposal or reuse processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset.

~~R #~~	~~Time Horizon~~	~~VRF~~	~~Violation Severity Levels~~			
			~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
					~~data storage media.~~	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

~~*Assumptions:*~~ Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. ~~The Responsible Entity may retain all of the information about BES Cyber Systems in a separate repository or physical or electronic location with access control implemented for both the repository and the BES Cyber Assets. Additional methods for implementing the requirement are suggested in the measures section.~~

~~While separating BES Cyber System Information into~~Identifying separate classifications of BES Cyber System Information is not specifically required~~ as it was in version 4~~. However, a Responsible Entity maintains ~~that~~the flexibility to do so if ~~desired~~they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional

classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. ~~Topics that are appropriate for information handling~~ R1.2 requires one or more procedures ~~include access, sharing, copying, transmittal, distribution,~~for the protection and ~~disposal or destruction of~~ secure handling BES Cyber System Information~~.~~, including storage, transit, and use.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an

electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

~~This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it must be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 5 CIP Cyber Security Standards

September 17, 2012

Note: On September 17, 2012, NERC was alerted that some references in the "Initial Performance of Certain Periodic Requirements" section were incorrectly synchronized to certain changes that occurred in the standards since draft 2.

This revised draft corrects the reference from "CIP-007-5, Requirement R4, Part 4.5" to "CIP-007-5, Requirement R4, Part R4.4," it removes the references to "CIP-007-5, Requirement R3, Part 3.3" and "CIP-011-1, Requirement R1, Part 1.3," and it removes the duplicate reference to CIP-009-5, Requirement R2, Part 2.3. It also corrects instances of typographical spelling errors of "identified" and "security."

No other changes were made to this implementation plan or any of the other CIP V5 standards currently posted.

Prerequisite Approvals

All Version 5 CIP Cyber Security Standards and the proposed additions, modifications, and retirements of terms to the *Glossary of Terms* used in *NERC Reliability Standards* must be approved before these standards can become effective.

Applicable Standards

The following standards and definitions, collectively referred to as "Version 5 CIP Cyber Security Standards,"[1] are covered by this Implementation Plan:

CIP–002–5 — Cyber Security — BES Cyber System Categorization
CIP–003–5 — Cyber Security — Security Management Controls
CIP–004–5 — Cyber Security — Personnel and Training
CIP–005–5 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–5 — Cyber Security — Physical Security of BES Cyber Systems
CIP–007–5 — Cyber Security — Systems Security Management
CIP–008–5 — Cyber Security — Incident Reporting and Response Planning
CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems
CIP–010–1 — Cyber Security — Configuration Change Management and Vulnerability Assessments
CIP–011–1 — Cyber Security — Information Protection

[1] Although CIP-010-1 and CIP-011-1 are proposed as first versions, any reference to "Version 5 CIP Cyber Security Standards" includes CIP-010-1 and CIP-011-1, in addition to CIP-002-5 through CIP-009-5, because CIP-010-1 and CIP-011-1 were developed as part of the "Version 5 CIP Cyber Security Standards" development process.

"Definitions of Terms used in Version 5 CIP Cyber Security Standards" document, which includes proposed additions, modifications, and retirements of terms to the *Glossary of Terms used in NERC Reliability Standards*.

These standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

When these standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards become effective, the responsible entities identified in the Applicability Section of the standard must comply with the requirements.

Proposed Effective Date for Version 5 CIP Cyber Security Standards

Responsible entities shall comply with all requirements in CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 as follows:

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[2]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5 R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Initial Performance of Certain Periodic Requirements

Specific Version 5 CIP Cyber Security Standards have periodic requirements that contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to,

[2] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

". . . at least once every 15 calendar months . . .", and responsible entities shall comply initially with those periodic requirements as follows:

1. On or before the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-002-5, Requirement R2
   - CIP-003-5, Requirement R1
2. On or before the Effective Date of CIP-003-5, Requirement R2 for the following requirement:
   - CIP-003-5, Requirement R2
3. Within 14 calendar days after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-007-5, Requirement R4, Part 4.4
4. Within 35 calendar days after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-010-1, Requirement R2, Part 2.1
5. Within three calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5, Requirement R4, Part 4.2
6. Within 12 calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5, Requirement R2, Part 2.3
   - CIP-004-5, Requirement R4, Parts 4.3 and 4.4
   - CIP-006-5, Requirement R3, Part 3.1
   - CIP-008-5, Requirement R2, Part 2.1
   - CIP-008-5, Requirement R3, Part 3.1
   - CIP-009-5, Requirement R2, Parts 2.1, 2.2
   - CIP-009-5, Requirement R3, Part 3.1
   - CIP-010-5, Requirement R3, Parts 3.1
7. Within 24 calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-009-5, Requirement R2, Part 2.3
   - CIP-010-1, Requirement R3, Part 3.2

8. Within 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment for the following requirement:
   - CIP-004-5, Requirement R3, Part 3.5.

Previous Identity Verification

A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be reperformed under CIP-004-5 R4, Part 4.1.

Planned or Unplanned Changes Resulting in a Higher Categorization

Planned changes refer to any changes of the electric system or BES Cyber System as identified through the annual assessment under CIP-002-5, Requirement R2, which were planned and implemented by the responsible entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the Version 5 CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System, as identified through the annual assessment under CIP-002-5, Requirement R2, which were not planned by the responsible entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-5, Attachment 1, criteria.

For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same

manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies first medium impact or high impact BES Cyber System	24 months

Applicability Reference Tables

The following tables are provided as a convenient reference to show which requirements in the Version 5 CIP Cyber Security Standards apply to specific Cyber Assets.

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-004-5 R2	Cyber Security Training Program	X	X	
CIP-004-5 R3	Personnel Risk Assessment Program	X	X	
CIP-004-5 R4	Access Management Program	X	X	
CIP-004-5 R5	Access Revocation	X	X	

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-005-5 R1 Part 1.2	Electronic Security Perimeter			X
CIP-005-5 R2	Remote Access Management			X
CIP-006-5 R1	Physical Security Plan	X	X	X
CIP-006-5 R2	Visitor Control Program	X		X
CIP-006-5 R3	Maintenance and Testing Program		X	
CIP-007-5 R1	Ports and Services	X	X	X
CIP-007-5 R2	Security Patch Management	X	X	X
CIP-007-5 R3	Malicious Code Prevention	X	X	X
CIP-007-5 R4	Security Event Monitoring	X	X	X
CIP-007-5 R5	System Access Control	X	X	X
CIP-010-1 R1	Configuration Change Management	X	X	X
CIP-010-1 R2	Configuration Monitoring	X	X	X
CIP-010-1 R3	Vulnerability Assessments	X	X	X
CIP-011-1 R1	Information Protection	X	X	
CIP-011-1 R2	BES Cyber Asset Reuse and Disposal	X	X	X

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 5 CIP Cyber Security Standards

~~April 10~~September 17, 2012

Note: On September 17, 2012, NERC was alerted that some references in the "Initial Performance of Certain Periodic Requirements" section were incorrectly synchronized to certain changes that occurred in the standards since draft 2.

This revised draft corrects the reference from "CIP-007-5, Requirement R4, Part 4.5" to "CIP-007-5, Requirement R4, Part R4.4," it removes the references to "CIP-007-5, Requirement R3, Part 3.3" and "CIP-011-1, Requirement R1, Part 1.3," and it removes the duplicate reference to CIP-009-5, Requirement R2, Part 2.3. It also corrects instances of typographical spelling errors of "identified" and "security."

No other changes were made to this implementation plan or any of the other CIP V5 standards currently posted.

Prerequisite Approvals

All Version 5 CIP Cyber Security Standards and the proposed additions, modifications, and retirements of terms to the *Glossary of Terms* used in *NERC Reliability Standards* must be approved before these standards can become effective.

Applicable Standards

The following standards and definitions, collectively referred to as "Version 5 CIP Cyber Security Standards,"[1] are covered by this Implementation Plan:

CIP–002–5 — Cyber Security — BES Cyber System Categorization
CIP–003–5 — Cyber Security — Security Management Controls
CIP–004–5 — Cyber Security — Personnel and Training
CIP–005–5 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–5 — Cyber Security — Physical Security of BES Cyber Systems
CIP–007–5 — Cyber Security — Systems Security Management
CIP–008–5 — Cyber Security — Incident Reporting and Response Planning
CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems
CIP–010–1 — Cyber Security — Configuration Change Management and Vulnerability Assessments
CIP–011–1 — Cyber Security — Information Protection

[1] Although CIP-010-1 and CIP-011-1 are proposed as first versions, any reference to "Version 5 CIP Cyber Security Standards" includes CIP-010-1 and CIP-011-1, in addition to CIP-002-5 through CIP-009-5, because CIP-010-1 and CIP-011-1 were developed as part of the "Version 5 CIP Cyber Security Standards" development process.

- "Definitions of Terms used in Version 5 CIP Cyber Security Standards" document, which includes proposed additions, modifications, and retirements of terms to the *Glossary of Terms used in NERC Reliability Standards*.

These standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

When these standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards become effective, the responsible entities identified in the Applicability Section of the standard must comply with the requirements.

Proposed Effective Date for Version 5 CIP Cyber Security Standards

Responsible entities shall comply with all requirements in CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 as follows:

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[2]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5 R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Initial Performance of Certain Periodic Requirements

Specific Version 5 CIP Cyber Security Standards have periodic requirements that contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to,

[2] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

". . . at least once ~~each~~every 15 calendar ~~year . . .~~"months . . .", and responsible entities shall comply initially with those periodic requirements~~,~~ as follows:

1. On or before the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-002-5, Requirement R2
   - CIP-003-5 ~~R4~~, Requirement R1

2. On or before the Effective Date of CIP-003-5, Requirement R2 for the following requirement:
   - CIP-003-5, Requirement R2

~~2.~~3. Within 14 calendar days after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-007-5, Requirement R4, Part 4.4~~5~~

~~3.~~4. Within 35 calendar days after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - ~~CIP-007-5 R3 Part 3.3~~
   - CIP-010-1, Requirement R2, Part 2.1

~~4.~~5. Within three calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5 ~~R6~~, Requirement R4, Part ~~6.5~~4.2

~~5.~~6. Within 12 calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5 ~~R3~~, Requirement R2, Part 2.3~~.2~~
   - CIP-004-5 ~~R6~~, Requirement R4, Parts ~~6.6~~4.3 and ~~6.7~~4.4
   - CIP-006-5, Requirement R3, Part 3.1
   - CIP-008-5, Requirement R2, Part 2.1
   - CIP-008-5, Requirement R3, Part 3.1
   - CIP-009-5, Requirement R2, Parts 2.1, 2.2 ~~and 2.2~~
   - CIP-009-5, Requirement R3, Part 3.1
   - CIP-010-5, Requirement R3, Parts 3.1 ~~and 3.2~~
   - ~~CIP-011-5 R1, Part 1.3~~

7. Within 24 calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-009-5, Requirement R2, Part 2.3

- CIP-010-1, Requirement R3, Part 3.2

~~6.~~8. Within 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment for the following requirement:

- CIP-004-5 ~~R5~~, Requirement R3, Part 3.5.~~2.~~

Previous Identity Verification

A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be reperformed under CIP-004-5 R4, Part 4.1.

Planned or Unplanned Changes Resulting in a Higher Categorization

Planned changes refer to any changes of the electric system or BES Cyber System~~,~~ as ~~described in~~identified through the annual assessment under CIP-002-5, ~~R1.1~~Requirement R2, which were planned and implemented by the responsible entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the Version 5 CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System, as ~~described in~~identified through the annual assessment under CIP-002-5, ~~R1.1~~Requirement R2, which were not planned by the responsible entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-5, Attachment 1, criteria.

For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System~~, as required in CIP-002-5, R1.1~~ and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System~~, as required~~

~~in CIP-002-5, R1.4:~~ and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies first medium impact or high impact BES Cyber System	24 months

~~**Additional Guidance and Implementation Time Periods for Disaster Recovery**~~
~~A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003-5, R1.~~

Applicability Reference Tables

The ~~rationale for this is that the primary task~~ following ~~a disaster is the restoration of the power system and the ability to serve customer Load. Cyber security provisions~~tables are ~~implemented to support reliability and operations. If restoration were to be slowed to ensure full compliance with~~ provided as a convenient reference to show which requirements in the Version 5 CIP Cyber Security Standards~~, restoration could be hampered and reliability could be harmed.~~

~~However, following the completion of the restoration activities, the entity is obligated to comply with the Version 5 CIP Cyber Security Standards at the restored Facilities, and be able to demonstrate full compliance in a spotcheck or audit; or file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.~~

~~**The following security requirements in CIP-003 through CIP-011**~~ apply to ~~**these Associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected**~~specific Cyber Assets.

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-004-5 R2	Cyber Security Training Program	X	X	
~~CIP-004-5 R3~~	~~Cyber Security Training~~	~~X~~	~~X~~	
CIP-004-5 ~~R4~~R3	Personnel Risk Assessment Program	X	X	
~~CIP-004-5 R5~~	~~Personnel Risk Assessment~~	~~X~~	~~X~~	
CIP-004-5 ~~R6~~R4	Access Management Program	X	X	
CIP-004-5 ~~R7~~R5	Access Revocation	X	X	
CIP-005-5 R1 Part 1.2	Electronic Security Perimeter			X
CIP-005-5 R2	Remote Access Management			X
CIP-006-5 R1	Physical Security Plan	X	X	X
CIP-006-5 R2	Visitor Control Program	X		X
CIP-006-5 R3	Maintenance and Testing Program		X	
CIP-007-5 R1	Ports and Services	X	X	X
CIP-007-5 R2	Security Patch Management	X	X	X
CIP-007-5 R3	Malicious Code Prevention	X	X	X
CIP-007-5 R4	Security Event Monitoring	X	X	X
CIP-007-5 R5	System Access Control	X	X	X

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-010-1 R1	Configuration Change Management	X	X	X
CIP-010-1 R2	Configuration Monitoring	X	X	X
CIP-010-1 R3	Vulnerability Assessments	X	X	X
CIP-011-1 R1	Information Protection	X	X	
CIP-011-1 R2	BES Cyber Asset Reuse and Disposal	X	X	X

Definitions of Terms Used in Version 5 CIP Cyber Security Standards

This section includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards and proposes terms for retirement. Terms already defined in the Glossary of Terms used in NERC Reliability Standards are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary. New defined terms are underscored. For existing glossary terms, new language is shown as underscored, while deleted language is shown as stricken. The list of terms proposed for retirement is at the end of the document.

Note: On September 21, 2012, consistent with corrections to CIP-002-5, this draft was revised to correct the incorrect functional model reference in Control Center from "Generation Operator" to "Generator Operator"

No other changes were made to the definitions or any of the other CIP V5 standards currently posted except as specified in CIP-002-5.

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

BES Cyber System

One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

BES Cyber System Information

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security

information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

CIP Exceptional Circumstance

A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.

Control Center

One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

Cyber Assets

Programmable electronic devices, ~~and communication networks~~ including the hardware, software, and data in those devices.

Cyber Security Incident

~~Any~~ A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter ~~of a Critical Cyber Asset~~, or~~,~~
- Disrupts, or was an attempt to disrupt, the operation of a ~~Critical Cyber Asset~~ BES Cyber System.

Dial-up Connectivity

A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.

Electronic Access Control or Monitoring Systems ("EACMS")

Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Devices.

Electronic Access Point ("EAP")

A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Electronic Security Perimeter ("ESP")

The logical border surrounding a network to which ~~Critical Cyber Assets~~ BES Cyber Systems are connected using a routable protocol ~~and for which access is controlled~~.

External Routable Connectivity

The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.

Interactive Remote Access

User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Intermediate Device

A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate Device must not be located inside the Electronic Security Perimeter.

Physical Access Control Systems ("PACS")

Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Physical Security Perimeter ("PSP")

~~The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.~~

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside, and for which access is controlled.

Protected Cyber Assets ("PCA")

One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Reportable Cyber Security Incident

A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.

Terms to be retired from the *Glossary of Terms used in NERC Reliability Standards* **once the standards that use those terms are replaced:**

Critical Assets

Critical Cyber Assets

Definitions of Terms Used in Version 5 CIP Cyber Security Standards

This section includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards and proposes terms for retirement. Terms already defined in the Glossary of Terms used in NERC Reliability Standards are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary. New defined terms are underscored. For existing glossary terms, new language is shown as underscored, while deleted language is shown as stricken. The list of terms proposed for retirement is at the end of the document.

Note: On September 21, 2012, consistent with corrections to CIP-002-5, this draft was revised to correct the incorrect functional model reference in Control Center from "Generation Operator" to "Generator Operator"

No other changes were made to the definitions or any of the other CIP V5 standards currently posted, except as specified in CIP-002-5.

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, ~~Systems~~systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, ~~Systems~~systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

~~**Cyber Security Incident**~~

~~Any A malicious act or suspicious event that:~~

- ~~Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,~~
- ~~Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset BES Cyber System.~~

[SWN1]

BES Cyber System

One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

BES Cyber System Information

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. ~~Examples of BES Cyber System Information may include, but are not limited to, security procedures developed by the responsible entity and security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.~~ BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

CIP Exceptional Circumstance

A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.

Control Center

One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability ~~functional~~ tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for ~~Transmission~~transmission Facilities at two or more locations, or 4) a ~~Generation~~ Generator Operator for generation Facilities at two or more locations.

Cyber Assets

Programmable electronic devices, ~~and communication networks~~ including the hardware, software, and data in those devices.

Cyber Security Incident

~~Any~~ A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter ~~of a Critical Cyber Asset~~, or~~.~~
- Disrupts, or was an attempt to disrupt, the operation of a ~~Critical Cyber Asset~~ BES Cyber System.

Dial-up Connectivity

A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.

Electronic Access Control or Monitoring Systems ("EACMS")

Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Devices.

Electronic Access Point ("EAP")

A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Electronic Security Perimeter ("ESP")

The logical border surrounding a network to which ~~Critical Cyber Assets~~ BES Cyber Systems are connected using a routable protocol ~~and for which access is controlled~~.

External Routable Connectivity

~~A~~ The ability to access a BES Cyber System ~~that is accessible~~ from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.

Interactive Remote Access

~~All user~~User-initiated access by a person ~~that~~employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s~~), whether routable~~) or ~~dial-up access, using~~at a ~~client or remote access technology.~~ defined Electronic Access Point (EAP). Remote access may be initiated from:~~-~~ 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants.~~-~~ Interactive remote access does not include system-to-system process communications.

Intermediate Device

A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate Device must not be located inside the Electronic Security Perimeter.

Physical Access Control Systems ("PACS")

Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Physical Security Perimeter ("PSP")

~~The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.~~

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside, and for which access is controlled.

Protected Cyber ~~Asset~~Assets ("PCA")

~~A~~One or more Cyber ~~Asset~~Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter ~~(a~~. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is ~~directly~~ connected either to a Cyber Asset within ~~an~~the ESP or to ~~a BES Cyber Asset~~the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes~~)~~.

Reportable Cyber Security Incident

~~Any~~A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.

Terms to be retired from the *Glossary of Terms used in NERC Reliability Standards* **once the standards that use those terms are replaced:**

Critical Assets

Critical Cyber Assets

Unofficial Comment Form

Request for Comments Regarding the Draft of CIP Cyber Security Standards Version 5

Please **DO NOT** use this form for submitting comments. Please use the electronic form to submit comments to the revisions to outstanding Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs). The electronic comment form must be completed by **October 10, 2012**.

If you have questions please contact Steven Noess at steven.noess@nerc.net or 404-446-9691. All project-related documents are available on the project page.

Background Information

The Project 2008-06 Standard Drafting Team (SDT) is seeking industry feedback on this Version 5 of the CIP Cyber Security Standards and its Implementation Plan for consideration by the SDT in finalizing Version 5 and related documents.

The SDT has carefully considered several thousand pages of formal comments as well as extensive informal stakeholder feedback from drafts 1 and 2 of Version 5 of the CIP Cyber Security Standards. There were, understandably, varied perspectives and suggestions, often including divergent views on how to address the same standard or Requirement. After thorough review of all of the previous feedback, the SDT believes that the set of standards now posted represent significant improvement and incorporation of those viewpoints in such a manner as to reflect the industry's consensus position. The SDT encourages stakeholders to read the General Summary Consideration of Comments as it provides a high level overview of the feedback and the efforts the team has made to incorporate stakeholder viewpoints to produce a quality set of consensus standards.

The SDT thanks you for your continued participation and interest in the development of Version 5 of the CIP Cyber Security Standards. At this stage of the development process, the SDT has considered several very specific alternatives to almost all requirements and proposed definitions. In each case, the SDT thoroughly considered proposed changes and evaluated them carefully by considering several important variables, such as, but not limited to, whether such changes were in the interest of cyber security and reliability, whether they would improve or reduce consensus, whether they had unintended consequences for other types of entities, and whether they were in support of the SDT's obligation to respond to directives in FERC Order No. 706.

Instructions:

At this point, the SDT believes that the industry has made a significant investment in improving the CIP Version 5 standards, and the drafting team has done its best to be responsive to all inputs, recognizing that it is not possible to adopt every suggestions and also recognizing the considerable diversity of entities and assets to which the standards will apply. Therefore, in response to the brief questions below, please limit your comments to those topics or issues for which a change would be essential as a

condition to change your vote to an affirmative vote. Also, please refrain from providing duplicates of detailed comments that have already been provided in response to draft 1 and draft 2 (you may simply say "See comments on draft 2.")

IMPORTANT:

Please note that the official comment form *does not* retain formatting (even if it appears to transfer formatting when you copy from the unofficial Word version of the form into the official electronic comment form). If you enter extra carriage returns, bullets, automated numbering, symbols, bolding, italics, or any other formatting, that formatting will not be retained when you submit your comments.

Questions:

1. If, after reviewing the posted standards and General Summary of Consideration of Comments, you do not support one or more of the 10 standards, the implementation plan or set of definitions, please indicate the specific item you do not support (the standard and Requirement number, specific defined term, or implementation plan) and the specific reason you cannot support it here.

   Comments:

2. If you have a brief comment you would like to provide that has not already been provided among the previously submitted feedback in response to draft 1 and draft 2, please provide it here. Please limit your comment to 200 words or less.

   Comments:

Project 2008-06 - Cyber Security Order No. 706 - V5

Working Draft (September 11, 2012) of Consolidated VSLs from all standards

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1;

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES	Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and	Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and	OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized or have been incorrectly categorized

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium	medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified;	BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible	at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			BES Cyber Systems have not been identified.	OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber Systems have not been identified.	Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	
R2	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (R2.2)	failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (R2.2)	failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (R2.2)	identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			review in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1)	months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did	within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar	documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar months of the previous approval. (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				complete this approval in less than or equal to 17 calendar months of the previous approval. (R1)	months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	
R2	**Operations Planning**	**Lower**	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible	The Responsible Entity did not document or implement any cyber security policies for assets with a low impact rating that address the topics as required by R2. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2)	Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this	Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but did complete this approval in less than or equal to 17	review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but did complete this approval in less than or equal to 18	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar months of the previous approval. (R2)	calendar months of the previous approval. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices and associated physical security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices and associated physical security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices and associated physical security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices and associated physical security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and	did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to	did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to	OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a	The Responsible Entity has a program for	The Responsible Entity has a program for	The Responsible Entity did not have all of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk	conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did	conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and	required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel	did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel	physical access for four or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and	Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and	Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and	checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized	did not identify, assess, and correct the deficiencies. (3.5)	did not identify, assess, and correct the deficiencies. (3.5)	for access authorization for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter, and did not	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2)	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identify, assess and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies.	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	storage locations where BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)	Information is correct and necessary within 15 calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	Information is correct and necessary within 15 calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1) OR	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4)	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's	Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR	access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances, and did not identify, assess, and correct			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the deficiencies. (5.5)			

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning and Same Day Operations**	**Medium**			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-5 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						permissions and deny all other access by default. (1.3) OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has a process to log authorized physical entry through any Physical Security Perimeter with sufficient information to identify the individual and date of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8) OR The Responsible Entity has a process to log authorized physical entry through any Physical Security Perimeter with sufficient information to identify the individual and date of	The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7) OR The Responsible Entity	The Responsible Entity has a process to alert for unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to alert for unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5) OR	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity documented and implemented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			entry but did not identify, assess, or correct the deficiencies. (1.8) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)	has a process communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)	The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical	operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.6) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified deficiencies but did not assess or correct the deficiencies. (1.9)	deficiencies, but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct deficiencies. (1.9)	(1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						different controls, but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						correct the deficiencies. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4) OR The Responsible Entity does not have a process to alert for unauthorized access through a physical access point into a Physical security Perimeter or to communicate such

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						personnel(1.7) OR The Responsible Entity does not have a process to log authorized physical entry through any Physical Security Perimeter with sufficient information to identify the individual and date of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9)
R2	**Same-Day Operations**	**Medium**	N/A	The Responsible Entity included a visitor	The Responsible Entity included a visitor	The Responsible Entity has failed to include or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				control program that requires logging of each of the initial entry and last exit dates and times of the visitor on a daily basis, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or correct the	control program that requires continuous escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1) OR The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)	implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				deficiencies. (2.2) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)		at least ninety days. (2.3)
R3	**Long Term Planning**	**Lower**	The Responsible Entity has documented and implemented a maintenance and	The Responsible Entity has documented and implemented a maintenance and	The Responsible Entity has documented and implemented a maintenance and	The Responsible Entity has not documented and implemented a maintenance and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			testing program for Physical Access Control Systems, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	testing program for Physical Access Control Systems, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	testing program for Physical Access Control Systems, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	testing program for Physical Access Control Systems. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems, but did not complete required testing within 27 calendar months. (3.1)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible,	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* and has identified deficiencies but did not assess or correct the deficiencies. (R1) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* but did not identify, assess, or correct the deficiencies. (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				unnecessary physical input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)	had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)	
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity did not implement or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)	correct the deficiencies. (2.1) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65	document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* but did not identify, assess, or correct the deficiencies. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the	evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did	calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources identified but did not identify, assess, or	OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated	correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the	obtain approval by the CIP Senior Manager or delegate and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated	deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)		correct the deficiencies. (2.4)
R3	**Same Day Operations**	**Medium**		The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and has identified deficiencies but did not assess or correct the deficiencies. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of identified malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.2)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R3* and has identified deficiencies but did not assess or correct the deficiencies. (R3) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)	OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of identified malicious code and did not identify, assess, or correct the deficiencies. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and	did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R3* and did not identify, assess, or correct the deficiencies. (R3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					has identified deficiencies but did not assess or correct the deficiencies. (3.3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies. (3.3)	OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies. (3.1)
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security	The Responsible Entity did not implement or document one or more process(es) that included the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or	Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or	events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and has identified deficiencies but did not assess or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems	applicable items in *CIP-007-5 Table R4* and has identified deficiencies but did not assess or correct the deficiencies. (R4) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4* and did not identify, assess, or correct the deficiencies. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	(per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and has identified deficiencies but did	(per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and has identified deficiencies but did not assess or correct the deficiencies. (4.1) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct the deficiencies. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					not assess or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					sampling of logged events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and has identified deficiencies but did	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and has identified deficiencies but did not assess or correct the deficiencies. (R5) OR The Responsible Entity did not implement or document one or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not	of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and did not	not assess or correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented	more process(es) that included the applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and has identified deficiencies but did not assess or correct the deficiencies. (5.1) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identify, assess, or correct the deficiencies. (5.6)	identify, assess, or correct the deficiencies. (5.6)	process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and has identified deficiencies but did not assess or correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3)	has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and did not identify, assess, or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords and has identified deficiencies but did not assess or correct the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only	deficiencies. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within	technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and did not identify,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					17 calendar months but less than or equal to 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal	assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					to 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and has identified deficiencies but did not assess or correct the deficiencies. (5.7) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber Security Incident

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						response plan, but did not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	(2.1) The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Operations Assessment	Lower	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident.	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident	(3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				response groups or individuals, or • Technology changes.		

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected(2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests, and when tested, any	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Part 2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1) OR	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				• Technology changes.	• Responders, or Technology changes.	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and	The Responsible Entity has documented and implemented a configuration management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and	The Responsible Entity has documented and implemented a configuration management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and	The Responsible Entity has not documented or implemented any configuration management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline	identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to determine required	correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline	management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			configuration and identified deficiencies in the verification documentation but assess or correct the deficiencies. (1.4.3) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the verification documentation. (1.4.3)	security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the	configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s)	OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				existing baseline configuration but did not identify, assess, or correct the deficiencies in the determination of affected security controls. (1.4.1)	that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to verify that required	process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2) OR The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did	not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					not identify, assess, or correct the deficiencies in the required controls. (1.4.2) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process for testing changes in an	the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and identified deficiencies but did not assess or correct the	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficiencies. (1.5.2) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)	
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days and identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days but did not identify, assess, or correct the deficiencies. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	less than 21, months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A		The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not	The Responsible Entity has not implemented a BES Cyber System Information protection program (R1).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented a BES Cyber System Information protection program which	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					includes one or more procedures for protection and secure handling BES Cyber System Information but did not identify, assess, or correct the deficiencies. (1.2)	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any disposal or reuse processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset as specified in R 2. (2.1)

Project 2008-06 - Cyber Security Order No. 706 - V5
Working Draft (September 11, 2012) of Consolidated VSLs from all standards

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	High	For Responsible Entities with more than a total of 40 FacilitiesBES assets in Requirement R1, Part 1.1, five percent or fewer FacilitiesBES assets have not been identified or have been incorrectly identifiedconsidered according to Requirement R1, Part 1.1; Or OR For Responsible Entities with a total of	For Responsible Entities with more than a total of 40 FacilitiesBES assets in Requirement R1, Part 1.1, more than five percent but less than or equal to 10 percent of FacilitiesBES assets have not been identified or have been incorrectly identifiedconsidered, according to Requirement R1, Part 1.1; Or OR For Responsible Entities with a total of	For Responsible Entities with more than a total of 40 FacilitiesBES assets in Requirement R1, Part 1.1, more than 10 percent but less than or equal to 15 percent of FacilitiesBES assets have not been identified or have been incorrectly identifiedconsidered, according to Requirement R1, Part 1.1; Or OR For Responsible Entities with a total of	For Responsible Entities with more than a total of 40 FacilitiesBES assets in Requirement R1, Part 1.1, more than 15 percent of FacilitiesBES assets have not been identified or have been incorrectly identifiedconsidered, according to Requirement R1, Part 1.1; OrOR For Responsible Entities with a total of 40 or fewer FacilitiesBES assets, more than six FacilitiesBES assets in

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			40 or fewer Facilities,BES assets, 2 or fewer FacilitiesBES assets in Requirement R1, Part 1.1, have not been identified or have been incorrectly identifiedconsidered according to Requirement R1, Part 1.1; Or OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer of high and medium impact identified BES Cyber Systems have not been identified or categorized or have	40 or fewer FacilitiesBES assets, more than two, but fewer than or equal to four FacilitiesBES assets in Requirement R1, Part 1.1, have not been identified or have been incorrectly identifiedconsidered according to Requirement R1, Part 1.1; Or OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber AssetsSystems, more than five percent but less than or equal to 10 percent of identified BES Cyber AssetsSystems have	40 or fewer FacilitiesBES assets, more than four, but fewer than or equal to six FacilitiesBES assets in Requirement R1, Part 1.1, have not been identified or have been incorrectly identifiedconsidered according to Requirement R1, Part 1.1; OR For Responsible Entities with more than a total of 100 high or medium impact BES Cyber AssetsSystems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber AssetsSystems have not been categorized	Requirement R1, Part 1.1, have not been identified or have been incorrectly identifiedconsidered according to Requirement R1, Part 1.1; Or OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; Or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			been incorrectly categorized at a lower category; Or OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber AssetsSystems, five or fewer high and medium impact identified BES Cyber AssetsSystems have not been identified or categorized or have been incorrectly categorized at a lower category;. Or TheOR For Responsible Entity failed to update its	not been categorized or have been incorrectly categorized at a lower category; Or OR For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber AssetsSystems, more than five but less than or equal to 10 identified BES Cyber AssetsSystems have not been categorized or have been incorrectly categorized at a lower category;. Or TheOR For Responsible Entity failed to update its	or have been incorrectly categorized at a lower category; Or OR For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category;. Or TheOR For Responsible Entity failed to update its documentation of BES Cyber Assets in	OR For Responsible Entities- with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category;. Or TheOR For Responsible Entity failed to update its documentationEntities with more than a total of 100 high and medium impact BES Cyber Systems in accordance with Requirement R1, Part 1.4 for more than 100 calendar days

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			documentationEntities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Assets in accordance with Requirement R1, Part 1.4 for more than 60, but less than or equal to 70 calendar days following the completion of the changeSystems, five or fewer high or medium BES Cyber Systems have not been	documentation of BES Cyber Assets in accordanceEntities with Requirement R1, Part 1.4 for more than 70,a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 80 calendar days following the completion10 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of the change100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber	accordanceEntities with Requirement R1, Part 1.4 for more than 90,a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 100 calendar days following the completion of the change15 high or medium BES Cyber Systems have not been	following the completion, more than 15 percent of the changehigh or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identified.	Systems have not been identified.	identified.	
R2	**Operations Planning**	**Lower**	The Responsible Entity failed todid not complete its annual review orand update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 for more than 30,within 15 calendar months but less than or equal	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its annual review or approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 for more than 40,within 16 calendar months but less than or equal	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its annual review or approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 for more than 50,within 17 calendar months but less than or equal	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its annual review or approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 for more than 60within 18 calendar daysmonths of the latest required date. previous approval.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			to 4016 calendar daysmonths of the latest required date.previous approval. (R2.2)	to 5017 calendar daysmonths of the latest required date. previous approval. (R2.2)	to 6018 calendar daysmonths of the latest required date. previous approval. (R2.2)	(R2.2)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	~~N/A~~The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	~~N/A~~The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this	The Responsible Entity ~~has~~documented and implemented ~~at least~~ one or more cyber security ~~policy~~policies for its high impact and medium impact BES Cyber Systems, but ~~has failed to~~ did not address ~~one~~three of the nine topics required ~~Parts 1.1 to~~ by R1. (R1) ~~1.10.~~OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES	The Responsible Entity ~~has not~~ documented and implemented ~~any~~one or more cyber security ~~policy,~~ ~~Or~~ ~~The Responsible Entity has implemented at least one policy~~policies for its high impact and medium impact BES Cyber Systems, but ~~has failed to~~did not address ~~two~~four or more of the nine topics required by R1. (R1) ~~Parts 1.1 to 1.10.~~OR The Responsible Entity did not have any ~~one or more~~ documented cyber security policies for its high impact and medium impact BES Cyber Systems

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1)	review in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar	as required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar months of the previous approval. (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				the previous approval. (R1)	months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	
R2	**Operations Planning**	**Medium Lower**	N/AThe Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with	N/AThe Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented	The Responsible Entity has documented and implemented at least one or more cyber security policy, but has failed to policies for assets with a low impact rating that address only one of the topics as required Parts 2.1by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR	The Responsible Entity hasdid not implemented document or implement any cyber security policy, policies for assets with a low impact rating that address the topics as required by R2. Or OR The Responsible Entity hasdocumented and implemented one or more cyber security policies for assets with a low impact rating that address one of the topics as required by R2 and has identified deficiencies but

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			a low impact rating that address only three of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or	one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review.	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this review in less than	~~did not assess or correct the deficiencies. (R2)~~ ~~OR~~ ~~The Responsible Entity documented and~~ ~~implemented~~ ~~at least one policy but has failed~~~~one or more cyber security policies for assets with a low impact rating that address one of the topics as required by R2 but did not identify, assess, or correct the deficiencies.~~ OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	(R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R2)	or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager or delegate according to ~~2.4.~~Requirement R2 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager or delegate according to ~~address two or more of the required Parts 2.1 to 2.4.~~Requirement R2 within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Operations Planning	Medium	N/A	N/A	N/A	The Responsible Entity has not identified, by name, a single senior management official ("the CIP Senior Manager") with overall authority and responsibility for leading and managing implementation of the requirements within the CIP group of standards.
R4 R3	Operations Planning	LowerMedium	N/AThe Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	N/AThe Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has reviewed its cyber security policy or policiesidentified by name a CIP Senior Manager, but did not all of them have been approved by document changes to the CIP Senior Manager within	The Responsible Entity has not reviewed theidentified, by cyber security policy or policies and the name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not approved all of them within the required time

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					50 calendar days but did document this change in less than 60 calendar days of the required time period.change. (R3)	period.document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R5 R4	Operations Planning	Lower	N/AThe Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity failed to has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the approval and authorization of one delegation (by title or namedelegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity failed to document the approval and authorization of two delegations (by title or name of the delegate) as required.The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, and has identified	The Responsible Entity failedhas used delegated authority for actions where allowed by the CIP Standards, but does not have a process to document thedelegate actions from the CIP Senior Manager. (R4) approval and authorization of three or more delegations (by title or name of the delegate) as required.OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~delegate) as required.~~	deficiencies but did not assess or correct the deficiencies. (R4) OR The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, but did not identify, assess, or correct the deficiencies.(R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the	the delegate within 60 calendar days of the change. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	
~~R6~~	~~Operations Planning~~	~~Lower~~	~~N/A~~	~~NA~~	~~Change to one delegation was not documented within 30 calendar days of the effective date.~~	~~A change to the CIP Senior Manager, Or more than one delegation was not documented within 30 calendar days of the effective date.~~

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not ~~convey on-going~~reinforce cyber security ~~awareness reinforcement at least once for~~practices and associated physical security practices during a calendar quarter ~~and~~but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not ~~convey on-going~~reinforce cyber security ~~awareness reinforcement at least once for~~practices and associated physical security practices during a calendar quarter ~~and~~but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not ~~convey on-going~~reinforce cyber security ~~awareness reinforcement at least once for~~practices and associated physical security practices during a calendar quarter ~~and~~but did so within the subsequent quarter but beyond 30 calendar days after the start of ~~a subsequent~~that calendar quarter. (1.1)	The Responsible Entity did not document ~~a~~or implement any security awareness ~~program~~process(es) to reinforce cyber security practices and associated physical security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
~~**R2**~~	~~**Operations Planning**~~	~~**Lower**~~	~~The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 1 of the required training~~	~~The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 2 of the required training~~	~~The Responsible Entity did define the roles that require training and did have the required role-based training, but did not include 4 or more of the training content as~~	~~The Responsible Entity did not have the required role-based training. (R2)~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content as detailed in 2.2 through 2.10.	content as detailed in 2.2 through 2.10.	detailed in 2.2 through 2.10.	
R3 R2	Operations Planning	Medium Lower	With The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not train 1 individual) prior to their being granted authorized electronic	With The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not train 2 individuals) prior to their being granted authorized electronic	With The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not train 3 individuals) prior to their being granted authorized electronic	With The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			and authorized unescorted physical access in a calendar year. (3.1) OR The Responsible Entity , and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train 1one individual with authorized for electronic and or authorized unescorted physical access in awithin 15 calendar year not exceeding 15 months between training. (3.2) of the previous training completion date, and did not identify, assess and correct the	and authorized unescorted physical access in a calendar year. (3.1) OR The Responsible Entity , and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train 2two individuals with authorized for electronic and or authorized unescorted physical access in awithin 15 calendar year not exceeding 15 months between training. (3.2of the previous training completion date, and did not identify, assess and correct the	and authorized unescorted physical access in a calendar year. (3.1) OR The Responsible Entity , and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train 3three individuals with authorized for electronic and or authorized unescorted physical access in awithin 15 calendar year not exceeding 15 months between training. (3.2) of the previous training completion date, and did not identify, assess and correct the	security training program but failed to train four or more individuals (with the exception of policy-identified CIP Exceptional Circumstances, the Responsible did not train 4 or more individuals) prior to their being granted authorized electronic and authorized unescorted physical access in a calendar year. (3.1, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity did notimplemented a cyber security training program but failed to train 4four or more individuals with authorized for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies. (2.3)	deficiencies. (2.3)	deficiencies. (2.3)	electronic and or authorized unescorted physical access in awithin 15 calendar year not exceeding 15 months betweenof the previous training. (3.2) OR The Responsible Entity completion date, and did not implement at all its cyber security training program. (R3identify, assess and correct the deficiencies. (2.3)
R4	Operations Planning	Medium	N/A	The Responsible Entity has a personnel risk assessment program, as stated in Requirement R4, for individuals having authorized cyber or authorized unescorted physical access, but the program does not include identity	The Responsible Entity has a personnel risk assessment program, as stated in Requirement R4, for individuals having authorized cyber or authorized unescorted physical access, but the program did not include the required	The Responsible Entity did not have a personnel risk assessment program, as stated in Requirement R4, for individuals having authorized cyber or authorized unescorted physical access. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				verification or a criminal history records check. (4.1) (4.2)	documented results or the program did not include criteria or process to determine when authorized access shall not be granted. (4.3)(4.5)	
R5 R3	Same Day Operations Planning	Medium	ExceptThe Responsible Entity has a program for CIP Exceptional Circumstances, the Responsible Entityconducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not perform personnel risk assessments for 1 individual prior to conduct the PRA as a condition of granting authorized electronic and or authorized unescorted physical access in a calendar year. (5.1for one	ExceptThe Responsible Entity has a program for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessmentsconducting Personnel Risk Assessments (PRAs) for 2 individuals prior to , including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic and or authorized unescorted physical access in a calendar year. (5.1) for two individuals, and did	ExceptThe Responsible Entity has a program for CIP Exceptional Circumstances, the Responsible Entity did not perform personnel risk assessmentsconducting Personnel Risk Assessments (PRAs) for 3 individuals prior to , including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic and or authorized unescorted physical access in a calendar year. (5.1for three individuals, and	The Responsible Entity did not have aall of the required elements as described by 3.1 through 3.4 included within documented processprogram(s) for personnel risk assessments. (R5) OR Exceptimplementing Personnel Risk Assessments (PRAs), for CIP Exceptional Circumstances, the individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did not update personnel risk assessments every seven years for 1 individual within seven years after the initial performance or last update of the personnel risk assessment. (5.2)conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4)	not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did not update personnel risk assessments every seven years for 2 individuals within seven years after the initial performance or last update of the personnel risk assessment. (5.2conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4)	did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did not update personnel risk assessments every seven years for 3 or more individuals within seven years after the initial performance or last update of the personnel risk assessment. (5.2) conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4)	unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not perform personnel risk assessments for 4 or more individuals prior toconduct the PRA as a condition of granting authorized electronic and or authorized unescorted physical access for four or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in ~~a~~ 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						electronic or authorized unescorted physical access within 7 calendar year. (years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5.1)
R6 R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorizeverify that individuals with active electronic access,or active unescorted physical access, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determined was	The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determined was necessary for performing assigned	The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorizeverify that individuals with active electronic access,or active unescorted physical access, or access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determined was	The Responsible Entity did not have a implement any documented processprogram(s) for access management. (R6R4) OR The Responsible Entity did not designatehas implemented one or more individual(s) documented program(s) for access management that includes a process to authorize electronic access, unescorted

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			necessary for performing assigned work functions. (6.2) (6.3) (6.4) OR The Responsible Entity did verify within 17 have authorization records during a calendar monthsquarter but did so less than 10 calendar days after the start of a subsequent calendar quarter, and did not within 15 calendar months that: (6.6) (6.7identify, assess and correct the deficiencies. (4.2) allOR • The Responsible Entity has implemented processes to verify that user accounts, user account groups, andor user role categories were	work functions and one user was granted access without authorization by the individual(s) designated in 6.1. (6.2) (6.3) (6.4) OR The Responsible Entity did not verify within the calendar quarter that individuals provisioned forwith active electronic or active unescorted physical access and electronic access had associatedhave authorization records. (6.5) OR The Responsible Entity did verify within 19 during a calendar monthsquarter but not within 17 calendar months that: (6.6) (6.7did so between 10 and 30 calendar days	necessary for performing assigned work functions and two users were granted access without have authorization by the individual(s) designated in 6.1. (6.2) (6.3) (6.4)records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity did verify within 21 calendar months but not within 19 calendar months has implemented processes to verify that: (6.6) (6.7) • all user accounts, user	physical access, or access to the physical and electronic designated storage locations where BES Cyber System Information is stored by the Responsible Entity. (6located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not authorize or have the individual(s) designated in 6.1 authorize electronic access, unescorted physical access, and access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determined was

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct, or • , and their specific, associated privileges were are correct or that they were those that that the Responsible Entity determined necessary for performing assigned work functions.and necessary within 15 calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.3) OR • The Responsible Entity has implemented processes to verify that access to the physical and electronicdesignated storage locations	after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) all OR • The Responsible Entity has implemented processes to verify that user accounts, user account groups, andor user role categories were correct, or • , and their specific, associated privileges wereare correct or that they were those that the Responsible Entity determined necessary for	account groups, andor user role categories are correct, or • , and their specific, associated privileges were correct or that they were those that that the Responsible Entity determined necessary for performing assigned work functions.are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR • The Responsible Entity has implemented processes to verify that	necessary for performing assigned work functions and three or more users were granted access without authorization by the individual(s) designated in 6.1. (6.2) (6.3) (6.4)verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity did nothas implemented processes to verify within 24 calendar months that: (6.6) (6.7) • all user accounts, user

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			wherefor BES Cyber System Information is stored bycorrect and necessary within 15 calendar months of the Responsible Entity was correct previous verification but for one BES Cyber System Information storage location, privileges were incorrect or that unnecessary, and did not identify, assess and correct the access was what the Responsible Entity determined necessary for performing assigned work functions.deficiencies. (4.4)	performing assigned work functions. access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity was correct or that the access was what the Responsible Entity determined necessary for performing assigned work functions.necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR • The Responsible	access to the physical and electronicdesignated storage locations wherefor BES Cyber System Information is stored bycorrect and necessary within 15 calendar months of the Responsible Entity was correct previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or that unnecessary, and did not identify, assess, and correct the access was what the Responsible Entity determined necessary for performing assigned work functions.deficiencies. (4.4)	account groups, andor user role categories were correct, or • , and their specific, associated privileges were correct or that they were the those that that the Responsible Entity determined necessary for performing assigned work functions, orare correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR • The Responsible Entity has implemented processes to verify that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)		access to the ~~physical and electronic~~designated storage locations ~~where~~for BES Cyber System Information is ~~stored by~~correct and necessary within 15 calendar months of the ~~Responsible Entity was correct~~ previous verification but for four or ~~that~~ more BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the ~~access was what the Responsible Entity determined necessary for performing assigned work functions.~~deficiencies. (4.4)
~~R7~~	**Same**	**Mediu**	~~Revocation of~~The	The Responsible Entity	The Responsible Entity	The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	Day Operations and Operations Planning	m	Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information ~~was~~ but, for one individual, did not ~~accomplished for 1 or more individuals within the specified~~ do so by the end of the next calendar day following the effective date and time ~~frame (7~~of the termination action, and did not identify, assess, and correct the deficiencies. (5.3~~);~~) OR ~~User~~The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts ~~on BES Cyber~~	~~did not revoke unneeded~~ has implemented one or more process(es) to remove the ability for unescorted physical ~~or electronic access~~ access and Interactive Remote Access upon a termination action or complete the removal within ~~the specified times in CIP-004-5 R7~~24 hours of the termination action but did not initiate those removals for one individual ~~who was terminated, resigned, was reassigned, or transferred. (7~~, and did not identify, assess, and correct the deficiencies. (5.1~~ and 7~~) OR The Responsible Entity has implemented one or more process(es) to	~~did not revoke unneeded~~ has implemented one or more process(es) to remove the ability for unescorted physical ~~or electronic access according to the specified times in CIP-004-5 R7~~access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals ~~who were terminated, resigned, reassigned or transferred.(7~~, and did not identify, assess, and correct the deficiencies. (5.1~~ and 7~~) OR The Responsible Entity has implemented one or	~~did~~has not ~~have a~~ implemented any documented ~~process~~program(s) for ~~initiating the~~ access revocation for electronic access, unescorted physical access, or ~~electronic access revocation process;~~ BES Cyber System Information storage locations. (R5) OR The Responsible Entity ~~did not revoke unneeded access according~~has implemented one or more process(es) to ~~the specified times in CIP-004-5 R7~~remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Assets wereupon termination action but did not revokeddo so for within 30 calendar days of the date of termination action for one or more individuals within the specified time frame (7, and did not identify, assess, and correct the deficiencies. (5.4);) OR UserThe Responsible Entity has implemented one or more process(es) to change passwords on BES Cyber Assetfor shared accounts were not changedknown to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or	determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do	more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for	within 24 hours of the termination action but did not initiate those removals for three or more individuals who were terminated, resigned, reassigned, or transferred. (7, and did not identify, assess, and correct the deficiencies. (5.1 and 7) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			transfer for one or more individuals~~ within the specified time frame; (7~~, and did not identify, assess, and correct the deficiencies. (5.5) OR ~~Following the determination and documentation of~~The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances~~,~~ following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts ~~were not changed for one or more individuals~~known to the user within 10 calendar days following the end of the	so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			extenuating operating circumstances~~. (7~~, and did not identify, assess, and correct the deficiencies. (5.5)			

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning and Same Day Operations**	**Medium**	~~The Responsible Entity failed to document one or more processes for *CIP-005-5 Table R1 – Electronic Security Perimeter* according to Requirement R1.~~ ~~OR~~ ~~The Responsible Entity failed to document 5% or less of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2;~~	~~The Responsible Entity failed to document more than 5% but less than or equal to 10% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2;~~ ~~OR~~ ~~The Responsible Entity failed to document more than 5% but less than or equal to 10% of inbound and outbound access permissions, including the~~	The Responsible Entity ~~failed to document more than 10% but less than or equal to 15% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2;~~ ~~OR~~ ~~The Responsible Entity failed to document more than 10% but less than or equal to 15% of~~did not have a method for detecting malicious communications for both inbound and outbound ~~access permissions, including the rationale for granting access according to Requirement R1, part 1.3.~~communications. (1.5)	The Responsible Entity ~~failed to~~did not document one or more ~~than 15% of External Routable Connectivity through the ESP through an identified~~processes for *CIP-005-5 Table R1 –* Electronic ~~Access Point (EAP) according to Requirement R1, part 1.2;~~ ~~OR~~ ~~The Responsible Entity failed to document more than 15% of inbound and outbound access permissions, including the rationale for granting access according to Requirement~~ *Security Perimeter.* (R1~~, part 1.3.~~) OR The Responsible Entity did not have all ~~BES Cyber Assets and associated~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~OR~~ ~~The Responsible Entity failed to document 5% or less of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part 1.3.~~	~~rationale for granting access according to Requirement R1, part 1.3.~~		~~Protected~~applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP~~ according to Requirement R1, part~~). (1.1~~.~~) OR External Routable Connectivity through the ESP was not through an identified EAP~~ according to Requirement R1, part 1.2.~~. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default ~~according to Requirement R1, part 1.3.~~. (1.3) OR The Responsible Entity did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						not perform authentication when establishing dial-up connectivity with the ~~BES~~applicable Cyber ~~System~~Assets, where technically feasible ~~according to Requirement R1, part~~ . (1.4~~.~~ ~~OR~~ ~~The Responsible Entity did not have a method for detecting malicious communications according to Requirement R1, part 1.5.~~)
R2	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity ~~failed to document one or more~~ does not have documented processes for ~~*CIP-005-5 Table R2 – Interactive Remote Access* according to~~one or more of the	The Responsible Entity ~~failed to~~did not implement processes for one of the ~~required multi-factor authentication according to~~applicable items for Requirement ~~R2, Part~~Parts 2.1	The Responsible Entity ~~failed to~~did not implement ~~one~~processes for two of the ~~following:~~ ~~• Intermediate Device according to~~applicable items for Requirement ~~R2, Part~~Parts 2.1~~;~~ ~~OR~~ ~~• Enc~~	The Responsible Entity ~~failed to~~did not implement ~~two or more~~processes for three of the ~~following:~~ ~~• Intermediate Device according to~~applicable items for Requirement ~~R2, Part~~Parts 2.1 ~~(2.1);~~ ~~• Encryption according to~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			applicable items for Requirement ~~R2.~~Parts 2.1 through 2.3.	through 2.3.	~~ryption according to Requirement R2, Part~~ through 2.~~2~~3.	~~Requirement R2, Part 2.2;~~ ~~OR~~ • ~~Multi-factor authentication according to Requirement R2, Part~~through 2.3.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has ~~documented and implemented physical access controls,~~a process to log authorized physical entry through any Physical Security Perimeter with sufficient information to identify the individual and date of entry and identified deficiencies but ~~logging of~~did not assess or correct the deficiencies. (1.8) OR The Responsible Entity has a process to log authorized physical entry through any Physical Security Perimeter ~~does not provide~~with sufficient	The Responsible Entity has ~~documented and implemented~~a process to alert for unauthorized physical access ~~controls,~~to Physical Access Control Systems and identified deficiencies but ~~it does not~~did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems ~~or does~~but did not identify, assess, or correct the deficiencies. (1.7) OR	The Responsible Entity has ~~documented and implemented physical access controls, but does not~~ a process to alert for unauthorized ~~circumvention of~~access through a physical access ~~control~~point into a Physical security Perimeter ~~or does~~and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to alert for unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies.	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access ~~to only those individuals who are authorized~~. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity documented and implemented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			information to ~~uniquely~~ identify the individual and date of entry but did not identify, assess, or correct the deficiencies. (1.8) OR The Responsible Entity ~~retained~~has a process to retain physical access logs for 90 calendar days and identified deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for ~~75 or more calendar days, but for less than~~ 90 calendar days~~. (1.9)~~ but did not identify, assess, or	The Responsible Entity has a process communicate ~~such~~ alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity ~~retained physical access logs for 60 or more calendar days,~~has a process communicate alerts within 15 minutes to identified personnel but ~~for less than 75 calendar days~~did not identify, assess, or correct the deficiencies. (1.~~9)~~7)	(1.5) OR The Responsible Entity has a process to communicate ~~such~~ alerts within 15 minutes to identified personnel~~. (1.5)~~ ~~OR~~ ~~The Responsible Entity has does~~ and identified deficiencies but did not ~~have controls that~~assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5) OR	operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one ~~method~~control does not exist to restrict access to ~~Medium Impact BES Cyber~~Applicable Systems~~ with External Routable Connectivity or External Dial-up Connectivity~~. (1.2) OR The Responsible Entity has documented and implemented physical access controls,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct the deficiencies. (1.9)		The Responsible Entity has a process to monitor ~~each~~ for unauthorized physical access to a Physical Access Control ~~System twenty four hours a day, seven days~~Systems and identified deficiencies but did not assess or correct the deficiencies. (1.6) OR The Responsible Entity has a ~~week (with 99.9% availability),~~process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6) OR The Responsible Entity ~~retained~~has a process	~~but~~restricts access to Applicable Systems using at least one control, and identified deficiencies, but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two ~~or more~~ different

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					to retain physical access logs for ~~45 or more~~90 calendar days and identified deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days~~, but for less than 60 calendar days~~ but did not identify, assess, or correct deficiencies. (1.9)	~~methods~~controls do not exist to restrict access to ~~High Impact BES Cyber~~Applicable Systems. (1.3) OR The Responsible Entity ~~has~~ documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Applicable Systems using at least two different controls, but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity does not have ~~controls that~~a process to monitor ~~the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability),~~ for unauthorized ~~circumvention of~~access through a physical access ~~control~~point into a Physical Security Perimeter. (1.4) OR The Responsible Entity ~~retained~~has a process

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or correct the deficiencies. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4) OR The Responsible Entity does not have a process to alert for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						unauthorized access through a physical access point into a Physical security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Systems or to communicate such alerts within 15 minutes to identified personnel(1.7) OR The Responsible Entity does not have a process to log authorized physical entry through any Physical Security Perimeter with sufficient information to identify the individual and date of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for ~~less than 45~~90 calendar days. (1.9)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Same-Day Operations**	**Medium**	N/A	The Responsible Entity included a visitor control program ~~in its physical security plan, but did not log~~that requires logging of each of the initial entry and last exit dates and times of the visitor on a daily basis, the visitor's name, and the point of contact~~.~~ and identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program ~~in its physical security plan,~~that requires	The Responsible Entity included a visitor control program ~~in its physical security plan,~~that requires continuous escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but ~~it~~ did not ~~meet the requirements for continuous escort~~assess or correct deficiencies. (2.1) OR The Responsible Entity included a visitor control program that requires continuous escorted access of	The Responsible Entity has failed to include or implement a visitor control program ~~to provide required~~that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but ~~failed~~did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the	visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)	OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				deficiencies. (2.3)		
R3	**Long Term Planning**	**Lower**	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems, but did not ~~retain outage records for at least 12~~complete required testing within 24 calendar months ~~of outages for physical access control, logging, and alerting systems.~~but did complete required testing within 25 calendar months. (3.~~2)~~1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems, but ~~the~~did not complete required testing ~~was not performed on a cycle of not more than 24~~within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	The Responsible Entity ~~did not document outages for physical access control, logging,~~has documented and ~~alerting systems~~implemented a maintenance and testing program for Physical Access Control Systems ~~as~~, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.~~2)~~1)	The Responsible Entity has not documented and implemented a maintenance and testing program for Physical Access Control Systems. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems, but did not complete required testing within 27 calendar months. (3.1)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	~~N/A~~The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible	The Responsible Entity did not ~~have a documented~~implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* and has identified deficiencies but did not assess or correct the deficiencies. (R1) OR The Responsible Entity ~~had unneeded logical network accessible ports enabled.~~did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* but did not identify, assess, or correct the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				physical input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)	ports enabled but did not identify, assess, or correct the deficiencies. (1.1)	deficiencies. (R1) ~~OR~~ ~~The Responsible Entity had no methods to protect unnecessary physical input/output ports used for network connectivity, console commands, or removable media.~~
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within ~~30~~35 calendar days ~~of availability~~but less than 50 calendar days of the ~~patch from~~last	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets and has identified deficiencies	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1)	The Responsible Entity did not ~~have a documented~~implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			evaluation for the source or sources identified~~.~~ and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity ~~did not~~ has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the	but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled	OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within	did not ~~have a~~ implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* but did not identify, assess, or correct the deficiencies. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management ~~program~~but did not include any processes for tracking, evaluating, ~~and~~or installing cyber security patches for applicable Cyber Assets ~~or~~ and has identified deficiencies but did not ~~track~~assess or correct the deficiencies. (2.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise ~~and~~an existing mitigation plan within ~~30~~35 calendar days but less than 50 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the deficiencies. (2.3)	released security patches for applicability but did not evaluate the security patches for applicability within ~~45~~50 calendar days ~~of availability~~but less than 65 calendar days of the ~~patch from~~last evaluation for the source or sources identified~~.~~ and has identified deficiencies but did not assess or correct the deficiencies. (2.2) ~~OR~~ ~~The Responsible Entity did not~~ OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security	~~60~~65 calendar days of ~~availability of~~ the ~~patch from~~last evaluation for the source or sources identified~~.~~ and has identified deficiencies but did not assess or correct the deficiencies. (2.2) ~~OR~~ ~~The Responsible Entity did not~~ OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the	The Responsible Entity has documented or implemented one or more process(es) for ~~the release~~patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets ~~that are updateable and for which~~but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches ~~with~~, did not apply the applicable patches, create a ~~timeframe for mitigation.~~ dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated	days source or sources identified but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise ~~and~~an existing mitigation plan within ~~60~~65 calendar days of the evaluation completion and has identified deficiencies but did not assess or	CIP Senior Manager or delegate and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity documented a ~~patching source exists.~~mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				mitigation plan, or revise ~~and~~an existing mitigation plan within ~~45~~50 calendar days but less than 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches ~~with~~, did not apply the applicable patches, create a ~~timeframe for mitigation.~~ dated mitigation plan, or	correct the deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches ~~with~~, did not apply the applicable patches, create a ~~timeframe for mitigation.~~ dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan~~.~~ and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or correct the deficiencies. (2.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)		
R3	**Same Day Operations**	**Medium**	~~Where signatures or patterns are used, the Responsible Entity did update malicious code protections that use signatures or patterns at least once within 45 calendar days of each available signature or pattern release, but not within 35 calendar days. (3.3)~~	~~Where~~The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did ~~update malicious code protections that use~~not address testing the signatures or patterns ~~at least once within 55 calendar days of each available signature or pattern~~	~~Where~~The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of identified malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.2) OR The Responsible Entity	The Responsible Entity did not ~~have a documented~~implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R3* and has identified deficiencies but did not assess or correct the deficiencies. (R3) OR The Responsible Entity did not implement or document one or more

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~release, but not within 45 calendar days~~and has identified deficiencies but did not assess or correct the deficiencies. (3.3~~).~~) OR The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)	has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of identified malicious code and did not identify, assess, or correct the deficiencies. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections ~~that use signatures or patterns at least once within 55 calendar days of each available~~	process(es) that included the applicable items in *CIP-007-5 Table R3* and did not identify, assess, or correct the deficiencies. (R3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code~~.~~ and has identified deficiencies but did not assess or correct the deficiencies. (3.1) OR The Responsible Entity ~~did not mitigate the threat of identified~~has

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~signature or pattern release. (3.3).~~and has identified deficiencies but did not assess or correct the deficiencies. (3.3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies. (3.3)	implemented one or more documented process(es) for malicious code~~.~~ prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies. (3.1)
R4	**Same Day Operations and Operations Assessment**	**Medium**	~~N/A~~The Responsible Entity has documented and implemented one or more process(es) to identify undetected	The Responsible Entity ~~failed~~has documented and implemented one or more process(es) to identify ~~and implement methods~~	~~The Responsible Entity failed to activate a response to rectify the event logging failure before the end of the~~	The Responsible Entity did not ~~have a documented~~ implement or document one or more

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every	~~to review a~~undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every ~~two weeks.~~15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or	~~next calendar day.~~ The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and has identified deficiencies but did not assess or correct the deficiencies. (4.2) OR The Responsible Entity ~~failed to~~ has documented and implemented one or more process(es) to	process(es) that included the applicable items in *CIP-007-5 Table R4* and has identified deficiencies but did not assess or correct the deficiencies. (R4) OR The Responsible Entity ~~failed to implement methods to generate alerts for events that it determines to necessitate a real-time alert.~~did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4* and did not identify, assess, or correct the deficiencies. (R4) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify ~~and implement methods to~~ , assess, or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional	The Responsible Entity ~~failed~~has documented and implemented one or more process(es) to log ~~detected~~events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events ~~necessary~~described in 4.1.1 through 4.1.3 and has identified deficiencies but did not assess or correct the deficiencies. (4.1) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the ~~identification and after-the-fact investigation of Cyber Security Incidents.~~Applicable

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Circumstances) but did not retain ~~BES Cyber System security-related events~~ applicable event logs for at least the last 90 consecutive days~~, where technically feasible.~~ and has identified deficiencies but did not assess or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive	Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct the deficiencies. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					days and did not identify, assess, or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)	
R5	**Operations Planning**	**Medium**	~~N/A~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change	~~N/A~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change	The Responsible Entity ~~failed to implement procedures to authorize~~has implemented one or more documented process(es) for System Access Controls but, did not include the ~~use~~identification or inventory of ~~administrative, shared,~~ all enabled default~~,~~	The Responsible Entity did not ~~have a documented~~implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and has identified deficiencies but did not assess or correct the deficiencies. (R5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months	the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months	~~and~~ or other generic account types~~.~~, either by system, by groups of systems, by location, or by system type(s) and has identified deficiencies but did not assess or correct the deficiencies. (5.2) OR The Responsible Entity ~~failed to implement procedures to~~ has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s)	OR The Responsible Entity ~~failed to implement methods to validate credentials before granting electronic access to BES Cyber Systems.~~did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5) OR The Responsible Entity ~~failed to implement procedures~~has implemented one or more documented process(es) for ~~password-based user~~ System Access Controls

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	and did not identify, assess, or correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts~~.~~ and has identified deficiencies but did not assess or correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the	but, where technically feasible, does not have a method(s) to enforce authentication~~.~~ of interactive user access and has identified deficiencies but did not assess or correct the deficiencies. (5.1) OR The Responsible Entity ~~failed to implement procedures to~~has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and did not identify, assess, or correct the deficiencies. (5.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change ~~or have unique~~known default passwords~~, where technically feasible.~~ and has identified deficiencies but did not assess or correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally	deficiencies. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within	authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					17 calendar months but less than or equal to 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and has identified deficiencies but did not assess or correct the deficiencies. (5.7) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4) ~~OR~~ ~~The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include internal groups or individuals or external organizations that should receive communication of the Cyber~~	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~Security Incident. (1.5)~~	Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but did not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) ~~according to R2 Part 2.1~~ within 17 calendar months, not exceeding 18 calendar	(2.1) The Responsible Entity has not tested the Cyber Security Incident response plan(s)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			response plan(s) ~~according to R2 Part 2.1~~ within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)		months between tests of the plan. (2.1) OR The Responsible Entity ~~does~~did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	within 19 calendar months between tests of the plan. OR The Responsible Entity ~~does not use its Cyber Security Incident response plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)~~ ~~OR~~ ~~The Responsible Entity does~~did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not ~~distributed updates of the Cyber Security Incident response plan to~~notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within ~~30 and~~greater than 90 but less than ~~60~~120 calendar days of ~~the update being completed.~~a	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within ~~30~~90 and less than ~~60~~120 calendar days ~~after the documentation required by~~ of a test or actual incident response to a Reportable Cyber Security Incident. (3.1~~. (3~~.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) ~~within 30~~or notified each person or	The Responsible Entity has ~~not~~neither documented lessons learned nor documented the absence of any lessons learned within ~~30~~90 and less than ~~60~~120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within ~~60~~120 calendar days ~~after the documentation required by~~ of a test or actual incident response to a Reportable Cyber Security Incident. (3.1~~. (3~~.2) OR The Responsible Entity has not updated the Cyber Security Incident response	The Responsible Entity has ~~not~~neither documented lessons learned nor documented the absence of any lessons learned within ~~60~~120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			test or actual incident response to a Reportable Cyber Security Incident. (3.~~4~~1.3)	group with a defined role within 60 and less than ~~60~~90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.~~3~~2) • ~~roles~~Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • ~~technology~~Technology changes. ~~OR~~ • ~~The Responsible Entity has not distributed updates of the Cyber Security Incident response plan to each person or group with a defined role in the Cyber Security Incident response plan within 60 calendar days of the update being completed. (3.4)~~	plan(s) ~~within 60~~or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.~~3~~2) • ~~roles~~Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • ~~technology~~Technology changes.	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address ~~all~~one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but -the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.
R2	**Operations Planning** **Real-time**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months,	The Responsible Entity has not tested the recovery plan(s) according to R2 Part	The Responsible Entity has not tested the recovery plan(s) according to R2 Part

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations		2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan~~.~~, and when tested, any deficiencies were identified, assessed, and corrected(2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber ~~Systems~~System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests, and when tested, any deficiencies were identified, assessed,	not exceeding 17 calendar months between tests of the plan~~.~~, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber ~~Systems~~System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR	2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan~~.~~, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber ~~Systems~~System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR	2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has ~~not~~ tested the ~~information used in the~~ recovery ~~of BES Cyber Systems~~plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2 ~~within 19 calendar months between tests. (2.2~~.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests~~. (2.3)~~, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests~~. (2.3)~~, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests~~.~~, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not ~~distributed updates of the recovery plan to~~notified each person or group with a defined role in the recovery plan(s) of updates within ~~30~~90 and less than ~~60~~210 calendar days of the update being completed. (3.~~4)~~1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within ~~30~~90 and less than ~~60~~210 calendar days ~~after the documentation required by R3 Part~~ of each recovery plan test or actual recovery. (3.1.~~(3.1~~2) OR The Responsible Entity has not notified each person or group with a defined role in the	The Responsible Entity has ~~not~~neither documented lessons learned nor documented the absence of any lessons learned within ~~30~~90 and less than ~~60~~210 calendar days of each recovery plan test or actual ~~incident~~ recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within	The Responsible Entity has ~~not~~neither documented lessons learned nor documented the absence of any lessons learned within ~~60~~210 calendar days of each recovery plan test or actual ~~incident~~ recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the ~~Recovery~~recovery plan(s~~)(s)~~) or notified each person or group with a defined role within ~~30~~60 and less than ~~60~~90 calendar days of any of the following changes ~~listed in R3 Part 3.3~~ that the responsible entity determines would impact the ability to execute the plan: (3.~~3~~2) ~~OR~~ • ~~The Responsible Entity has not distributed~~	~~60~~120 calendar days ~~after the documentation required by R3 Part~~ of each recovery plan test or actual recovery. (3.~~2. (3~~1.2) OR The Responsible Entity has not updated the recovery plan(s~~)(s)~~) or notified each person or group with a defined role within ~~60~~90 calendar days of any of the following changes ~~listed in R3 Part 3.3~~ that the responsible entity determines would impact the ability to execute the plan~~.~~: (3.~~3~~2) • Roles or responsibilities, or • Responders, or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~updates of the recovery plan(s) to each person or group with a defined role in the recovery plan(s) within 60 calendar days of the update being completed.~~ ~~(3.4)~~Roles or responsibilities, or • Responders, or • Technology changes.	Technology changes.	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	~~N/A~~The Responsible Entity has documented and implemented a configuration management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR	~~N/A~~The Responsible Entity has documented and implemented a configuration management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess	The Responsible Entity has ~~established~~documented and implemented a configuration management ~~program, but failed to authorize any changes to the~~ process(es) that includes only two of the required baseline ~~configuration and to document those changes.~~items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity ~~updated~~has documented and implemented a configuration management process(es) that includes three of the	The Responsible Entity has not ~~established~~documented or implemented any configuration management ~~programs.~~process(es). (R1) OR The Responsible Entity ~~did not implement~~has documented and implemented a configuration management ~~program~~process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has ~~established~~documente

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has documented and implemented a configuration management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration and identified deficiencies in the verification documentation but assess or correct the deficiencies. (1.4.3)	and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a	required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration~~,~~ management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but ~~failed to update the required~~ did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) that	d and implemented a configuration management ~~program, but failed to establish a documented baseline~~process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has ~~established~~documented and implemented a configuration management ~~program,~~process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but ~~with respect to the~~did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the verification documentation. (1.4.3)	change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the determination of	requires authorization and documentation for changes that deviate from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) to update baseline	not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes ~~in~~that deviate from the existing baseline configuration~~, did not~~. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				affected security controls. (1.4.1)	configurations within 30~~-~~ calendar days of ~~the~~completing a change~~ being completed.~~(s) that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.3) OR	does not have a process(es) to determine ~~the~~ required~~ cyber~~ security controls ~~identified~~ in CIP-005~~, CIP-006,~~ and CIP-007 that could be impacted by ~~the changes; or~~ a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2) OR The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline	required controls were not adversely affected ~~when~~following the change ~~was implemented.~~. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					configuration but did not identify, assess, or correct the deficiencies in the required controls. (1.4.2) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process for testing changes in an environment that	differences between the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and identified deficiencies but did not assess or correct the deficiencies. (1.5.2) OR The Responsible Entity	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)	
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not ~~established~~documented or implemented a ~~configuration monitoring~~ process(es) to monitor for-, investigate, and document detected unauthorized changes

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						to the baseline~~.~~ at least once every 35 calendar days. (2.1) OR The Responsible Entity has ~~not investigated~~documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized ~~change~~changes to the baseline ~~configuration.~~at least once every 35 calendar days and identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has ~~established~~documented and implemented a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~configuration monitoring~~ process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline ~~but failed to document a detected unauthorized change.~~ at least once every 35 calendar days but did not identify, assess, or correct the deficiencies. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has ~~established~~implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability	~~The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not performed an active vulnerability assessment on a new~~	The Responsible Entity has ~~established~~implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability	The Responsible Entity has ~~established~~not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	~~Cyber Asset prior to adding it to an applicable BES Cyber System.~~ ~~OR~~ ~~The Responsible Entity has established~~The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR	assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has ~~not established any~~implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)		last active assessment on one of its applicable BES Cyber Systems~~.~~.(3.2) OR The Responsible Entity has ~~established~~implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but ~~failed to~~did not perform ~~an~~the active vulnerability assessment in a ~~test environment (or in a production environment where the test is performed in a~~ manner that ~~minimizes adverse effects) that~~ models ~~the~~an existing baseline

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has ~~established~~implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						mitigation plans. (3.4)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	~~The Responsible Entity has implemented a BES Cyber System Information protection program that includes one or more methods to identify BES Cyber System Information, one or more handling procedures for BES Cyber System Information, and has assessed adherence periodically as stated in Part 1.3, but has failed to implement an action plan to remediate deficiencies identified during the assessment.~~	The Responsible Entity has implemented a BES Cyber System Information protection program ~~that~~which includes one or more methods to identify BES Cyber System Information and ~~one or more handling procedures for BES Cyber System Information,~~has identified deficiencies but ~~has failed to~~ did not assess ~~adherence periodically as stated in Part~~ or correct the deficiencies. (1.~~3, to its~~1) OR The Responsible Entity has implemented a BES Cyber System Information protection	The Responsible Entity has not implemented a BES Cyber System Information protection program~~.~~ (R1). ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System Information protection program, but has not implemented one or more methods to identify BES Cyber System Information~~ ~~OR~~ ~~The Responsible Entity has implemented a BES Cyber System~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					program~~.~~ which includes one or more methods to identify BES Cyber System Information but did not identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented a BES	~~Information protection program, but has not implemented one or more procedures for handling BES Cyber System Information.~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information but did not identify, assess, or correct the deficiencies. (1.2)	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity ~~failed to maintain chain of custody~~implemented one or more documented processes but did not include processes for ~~Cyber Assets that contain~~ reuse as to prevent the unauthorized retrieval of BES Cyber System Information ~~that have been removed~~ from the ~~Physical Security Perimeter prior to action taken to prevent unauthorized retrieval or~~	The Responsible Entity ~~has documented~~ implemented one or more documented processes~~, including both reuse and~~ but did not include disposal~~,~~ or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber ~~Assets, but the~~	The Responsible Entity has not documented or implemented any disposal or reuse processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset~~.~~ as specified in R 2. (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~destroying the data storage media.~~BES Cyber Asset. (2.1)	~~Responsible Entity either failed to take action to prevent the unauthorized retrieval of BES Cyber System Information from a Cyber~~ Asset ~~that contained BES Cyber System Information or failed to destroy the data storage media~~(2.2) .	

Project 2008-06 - Cyber Security Order 706 - Version 5

Working Draft (September 11, 2012) of Mapping Document Showing Translation of CIP-002-4 to CIP-009-4 into CIP-002-5 to CIP-009-5, CIP-010-1, and CIP-011-1.

Standard: CIP-002-4 – Cyber Security—Critical Asset Identification		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-002-4 R1.	CIP-002-5 R1.1	Critical Asset Identification – Instead of identifying Critical Assets as in previous versions, the Responsible Entity must Identify Facilities, systems, or equipment that meet the criteria specified in CIP-002-5, Attachment 1.
CIP-002-4 R2.	CIP-002-5 R1.2, R1.3	Critical Cyber Asset Identification – Using the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 Impact Rating Criteria, the Responsible Entity must identify and categorize its BES Cyber Systems as high impact or medium impact. BES Cyber Systems not identified as high impact or medium impact default to low impact. New standard identifies BES Cyber Systems as a grouping of BES Cyber Assets because it allows entities to apply some requirements at a system rather than asset level.

Standard: CIP-002-4 – Cyber Security—Critical Asset Identification		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-002-4 R2.	DELETED	Routable protocol exemption – A complete exemption of Cyber Assets based on communication characteristics no longer applies. This is because the vulnerability some security requirements address is not mitigated by the lack of routable protocols (e.g., training, response, recovery, etc.) Where the lack of routable protocols itself meets the requirement objective, the exemption is applied at the requirement level.
CIP-002-4 R3.	CIP-002-5 R2, R2.1, R2.2	Annual Approval – R2.1 states that the review must be at least once every 15 calendar months. However, the CIP Sr. Manager now approves identifications required in CIP-002-5 R1 as noted above.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R1.	CIP-003-5 R1, 1.1 through 1.9	Cyber Security Policy – Includes high impact and medium impact BES Cyber Systems. A separate requirement applies to low impact BES Cyber Systems. Clarified that the cyber security policy needs to only reference the subject matter topics at a high level rather than each individual requirement in the CIP Cyber Security Standards.
CIP-003-4 R1.1.	CIP-003-5 R 1.9	Provision for emergency situations – Identified the specific exceptional circumstances in which emergency exceptions can be taken in response to the directive in FERC Order No. 706, Paragraph 443.
NEW	CIP-003-5 R2	Cyber Security Policy for BES Cyber Systems not identified as high or medium impact (low impact). Clarified programmatic controls that apply to low impact BES Cyber Systems and that discrete identification of such systems is not required. Added that the CIP Senior Manager approve the policies at least once every 15 calendar months.
CIP-003-4 R1.2.	DELETED	The Cyber Security Policy is readily available –This was in response to general confusion around the term “readily available.” Training requirements in CIP-004-5 provide for knowledge of policy.
CIP-003-4 R1.3.	CIP-003-5 R1	The review and approval by the CIP Senior Manager at least once every 15 calendar months language has been added to R1.
CIP-003-4 R2.	CIP-003-5 R3	Single senior manager – Created a definition of CIP Senior Manager to facilitate references across standards.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R2.1.	CIP-003-5 R3	The CIP Senior Manager shall be identified by name, title, and date of designation – The CIP Senior Manager only needs to be identified by name. The other details were considered unnecessary, administrative requirements.
CIP-003-4 R2.2.	CIP-003-5 R3	Changes to the CIP Senior Manager and any delegations must be documented within 30 calendar days of the change.
CIP-003-4 R2.3.	CIP-003-5 R4	Delegate authority – Made clear that where allowed by the standards, the CIP Senior Manager may delegate authority and such delegations must be documented. Added that the Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a process to delegate actions, unless no delegations are used.
CIP-003-4 R2.4.	DELETED	Authorize and document any exception – The FERC Order No. 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the standards.
CIP-003-4 R3.	DELETED	Exceptions – The FERC Order No. 706 made clear that you could not take exceptions to areas of your Cyber Security Policy that were also required as part of other NERC CIP requirements. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the standards.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R3.1.	DELETED	Exceptions - Requirement R3 is deleted.
CIP-003-4 R3.2.	DELETED	Exceptions - Requirement R3 is deleted.
CIP-003-4 R3.3.	DELETED	Exceptions - Requirement R3 is deleted.
CIP-003-4 R4.	CIP-011-1 R1, 1.1, 1.2	Information Protection - Removed language to "protect" information, and replaced with requirements for methods to identify BES Cyber System Information and procedures for handling BES Cyber System Information, including storage, transit, and use to clarify the protection that is required. Added language that the entity implements its information protection programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-003-4 R4.1.	Definition	Identification – Replaced this requirement with the defined term BES Cyber System Information.
CIP-003-4 R4.2.	CIP-011-5 R1.1	Classification – Removed the explicit requirement for classification, as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.
CIP-003-4 R4.3.	CIP-011-5 R1.3	Assessment – No significant changes.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R5.	CIP-004-5 R4.4	Authorize personnel for access to protected information – Clarified: "Program for managing access" included the authorization of access, as well as handling and access control procedures. Grouped requirements for electronic access, physical access, and access to BES Cyber System Information in CIP 004-5 R4. Added language that the entity implements its documented access management programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-003-4 R5.1.	CIP-004-5 R4.1	Authorizing personnel.
CIP-003-4 R5.1.1.	CIP-004-5 R4.1	Have a process to authorize, which could include identifying specific personnel to authorize access.
CIP-003-4 R5.1.2.	CIP-004-5 R4.3, R4.4	Verification.
CIP-003-4 R5.2.	CIP-004-5 R4.3, R4.4	Verify access privileges – Moved requirement to ensure consistency among access reviews. Clarified precise meaning in the term "annual". Clarified what was necessary in performing verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.
CIP-003-4 R5.3.	CIP-004-5 R4.3, R4.4	Annual Review – No significant changes.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R6.	CIP-010-1 R1, R2	Change Control and Configuration Management – Moved configuration change management to a separate standard because of the additional requirements necessary for satisfying FERC directives, and the subject matter in CIP version 4 is spread across CIP-003-4 and CIP-007-4. The baseline requirement is incorporated from the *DHS Catalog for Control Systems Security*. The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed. Added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-4 R6. Added language that the entity implements its documented processes in a manner that identifies, assesses, and corrects deficiencies.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R1.	CIP-004-5 R1, 1.1	Security awareness program and quarterly reinforcement - Changed to remove the need to ensure everyone with authorized access receive this material, and moved example mechanisms to guidance.
CIP-004-4 R2.	CIP-004-5 R2	Training - Addition of identifying the training content. Adding content for the visitor control program and storage as part of the handling of BES Cyber Systems information. Also added the FERC Order No. 706, directed electronic interconnectivity supporting the operation and control of BES Cyber Systems. This requirement is also reorganized into the respective requirements for "program" and "implementation" of the training. Added language that the entity implements its documented programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-004-4 R2.1.	CIP-004-5 R2.2	Training prior to authorized access – No significant changes.
CIP-004-4 R2.2.	CIP-004-5 R2.1.1-2.1.9	Training subject matter – This requirement is reorganized into the respective requirements for "program" and "implementation" of the training.
CIP-004-4 R2.2.1.	CIP-004-5 R2.1	Proper use of CCAs – Changed to refer to BES Cyber Systems. Requirement now addresses cyber security issues, not the business or functional use of the BES Cyber System.
CIP-004-4 R2.2.2.	CIP-004-5 R2.1	Physical and electronic access controls training – No significant changes. Refers to BES Cyber Systems.
CIP-004-4 R2.2.3.	CIP-004-5 R2.1	Information handling training – Core training added for the handling of BES Cyber System Information, with the addition of storage media.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R2.2.4.	CIP-004-5 R2.1, R2.1.1-R2.1.9	Incident identification and notification, incident handling and CCA recovery training – Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for individuals having a role in the recovery to address FERC Order No. 706, Paragraph 413.
CIP-004-4 R2.3.	CIP-004-5 R2.3	Annual training – Replaced "Annually" with "at least once every 15 calendar months."
CIP-004-4 R3.	CIP-004-5 R3	Personnel Risk Assessment –. Added language that the entity implements its documented programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-004-4 R3.1.	CIP-004-5 R3.1, 3.2.1, 3.2.2	Identification and 7-year criminal check – Addressed interpretation request in guidance. Specified that identity verification is only required for each individual's initial assessment. Specified that the 7-year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for 6 consecutive months or more, including current residence, regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full 7-year check cannot be performed.
CIP-004-4 R3.2.	CIP-004-5 R3.5	Perform the PRA every 7 years– Removed the "for cause" part of the requirement.
CIP-004-4 R3.3.	CIP-004-5 R3.4	Addresses the contractor or vendor performed PRA.
NEW	CIP-004-5 R3.3	Process to evaluate criminal history records checks for authorizing access.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R4.	CIP-004-5 R4.1, 4.3	Authorize access - CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need-to-know" basis, or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.
CIP-004-4 R4.1.	CIP-004-5 R4.2	Quarterly review of access – Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4 R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.
CIP-004-4 R4.2.	CIP-004-5 R5	Prevent further access - The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the standards to require immediate revocation for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination, instead of within 24 hours. For transfers, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53, Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.
NEW	CIP-004-5 R2.1	Added to help facilitate understanding what roles the entity has to support the role-based training program.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-004-5 R2.1.4	Visitor control program training – Personnel administering the visitor control program and/or providing escort should be part of the core training per FERC Order No. 706, Paragraph 432.
NEW	CIP-004-5 R3.3	PRA failure criteria – Requires process or criteria to evaluate personnel risk assessments to determine when to deny authorized access.
NEW	CIP-004-5 R5.2	Transfers – The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53, Version 3, to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-004-5 R5.4	Completion of revocation – The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the standards to require immediate revocation for any person no longer needing access. In order to meet the immediate time frame, entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
NEW	CIP-004-5 R5.5	Completion of revocation (shared accounts) – To provide clarification of expected actions in managing the passwords

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R1.	CIP-005-5 R1.1	Electronic Security Perimeter identification – Changes include referencing the defined terms Electronic Access Point and BES Cyber System.
CIP-005-4a R1.1.	Definition	Access Points – This was moved to the definition of Electronic Access Points.
CIP-005-4a R1.2.	Guidance	Dial-up accessible CCA – This is a clarifying statement that was moved to Guidance.
CIP-005-4a R1.3.	Guidance	Communication links between ESPs – This is a clarifying statement that was moved to Guidance.
CIP-005-4a R1.4.	Applicability	Applicability for Non-Critical Cyber Asset – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.5.	Applicability	Access control and monitoring Cyber Assets – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.6.	Measures	Maintain Documentation – This is a measure for the requirement to have ESP documentation.
CIP-005-4a R2.	CIP-005-5 R1	Electronic Access Controls – No significant changes.
CIP-005-4a R2.1.	CIP-005-5 R1.2, 1.3	Deny access by default - Changes include referring to the defined term Electronic Access Point, and to focus on the entity knowing and having justification for what it allows through the EAP. R1.3 explicitly states the network admission control includes both inbound and outbound connections.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R2.2.	CIP-007-5 R1.1, 1.2	Enable specific ports/services – Consolidated port hardening requirements to CIP-007.
CIP-005-4a R2.3.	CIP-005-5 R1.4	Secure dial-up – Changed to refer to the defined term Electronic Access Point. Added clarification as to the goal of "secure," which is that the BES Cyber System should not be directly accessible with a phone number only.
CIP-005-4a R2.4.	CIP-005-5 R2,2.3	Strong access control – Added a new requirement for remote access in response to increased vulnerabilities in VPN technology. This requirement also clarified strong access control meant multi-factor (or more) authentication.
CIP-005-4a R2.5.	Measures	Example of evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.1.	CIP-004-5 R4	The processes for access request and authorization – Consolidated with other similar requirements to CIP-004-5 R4.
CIP-005-4a R2.5.2.	Measures	The authentication methods – Example of evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.3.	Measures	The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4. Example of evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.4.	Measures	The controls used to secure dial-up accessible connections. Example of evidence requirements are considered as part of the measure.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R2.6.	DELETED	Appropriate Use Banner – The drafting team considered this requirement administrative. The objective of having an appropriate use banner is to prevent accidental use of the system and help allow prosecution of unauthorized individuals accessing the system. The drafting team did not consider either of these rising to the level of meeting a reliability objective.
CIP-005-4a R3.	CIP-007-5 R4, 4.1	Monitoring Electronic Access – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the standards.
CIP-005-4a R3.1.	CIP-007-5 R4, 4.1	Dial-up Accessible – Removed specific references to dial-up devices. Incorporated into logging/monitoring requirements. The drafting team did not feel further referencing this technology was necessary.
CIP-005-4a R3.2.	CIP-007-5, R4, 4.2	Alerts – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the standards.
CIP-005-4a R4.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements.
CIP-005-4a R4.1.	Measures	A document identifying the vulnerability assessment process – Example of evidence requirements are considered as part of the measure.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R4.2.	CIP-010-1 R3.1, 3.2	A review to verify that only ports and services required for operations at these access points are enabled - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to Guidance.
CIP-005-4a R4.3.	CIP-010-1 R3.1, 3.2	The discovery of all access points to the Electronic Security Perimeter - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to Guidance.
CIP-005-4a R4.4.	CIP-010-1 R3.1, 3.2	A review of controls for default accounts, passwords, and network management community strings - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to Guidance.
CIP-005-4a R4.5.	CIP-010-1 R3.4	Mitigation plan - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. Added element to have an entity defined date of completion of the mitigation plan per FERC Order No. 706, Paragraph 643.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R5.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.1.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.2.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.3.	CIP-007-5 R4.4	Retain relevant log information – Log retention requirements are consolidated to CIP-007-5 R4.
NEW	CIP-005-5 R1.5	Inspect and detect potential malicious communications – Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The order makes clear this is not simple redundancy of firewalls; thus the drafting team has decided to add the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs.
NEW	CIP-005-5 R2.1,2.2	Remote Access: intermediate device and encryption – This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R1.	CIP-006-5 R1	Physical Security Plan – Removed the requirement for senior management approval of the physical security plan because there is already approval of the physical security policy and delegation of the task in complying for this program. Additional approval is not considered necessary to meeting the reliability objective of physical security for the BES Cyber System.
CIP-006-4c R1.1.	CIP-006-5 R1.2, 1.3	Physical Security Perimeter – For high impact BES Cyber Systems clarified that two or more different physical access controls (this does not require two completely independent physical access control systems) must be used to collectively allow unescorted physical access into Physical Security Perimeters.
CIP-006-4c R1.2.	DELETED	No longer requires identification of all physical access points.
CIP-006-4c R1.3.	CIP-006-5 R1.4, 1.5	Monitor physical access – A documented plan is required as part of CIP-006-5 R1 that references the new alerting term in Table Row 1.5. Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.
CIP-006-4c R1.4.	CIP-004-5 R2.3	Appropriate use of access controls – The term “appropriate” used in prior versions is subject to a high degree of subjectivity. The training requirement specifies role-based training on physical access controls.
CIP-006-4c R1.5.	CIP-004-5 R4 and R5	Review of access authorization requests and revocation of access authorization requirements were consolidated to CIP-004-5.
CIP-006-4c R1.6.	CIP-006-5 R2	Visitor control program - A documented program is required as part of CIP-006-5 R2. Otherwise, no significant change.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R1.6.1.	CIP-006-5 R2.2	Log entry and exit of visitors - Addressed multi entry requirements and added the point of contact of who can be considered the sponsor for the person to enter the DPB. There is no need to document the escort or handoffs between escorts.
CIP-006-4c R1.6.2.	CIP-006-5 R2.1	Continuous escorted access of visitors – No significant change.
CIP-006-4c R1.7.	DELETED	Update of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R1.8.	DELETED	Annual review of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R2.	Applicability	Protection of Physical Access Control Systems – Applicability to Physical Access Control and Monitoring Systems were moved to the Applicability section of each security requirement, and added this as a defined term in the glossary.
CIP-006-4c R2.1.	Applicability, CIP-006-5 R1.1	Physical Access Control Systems be protected from unauthorized physical access - Applicability to Physical Access Control Systems were moved to the Applicability section of each security requirement. For this particular requirement, see CIP-006-5, Item 1.1, which applies to Physical Access Control Systems.
CIP-006-4c R2.2.	CIP-006-5 R1.6, 1.7	Protection of Physical Access Control Systems - Applicability to Physical Access Control Systems were moved to the Applicability section of each security requirement throughout CP version 5.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R3.	Applicability	Protection of Electronic Access Control Systems - Applicability to what protections Electronic Access Control and Monitoring Systems need were moved to the Applicability section of each security requirement.
CIP-006-4c R4.	CIP-006-5 R1.2, 1.3	Physical Access Controls – R1.3 addresses FERC Order No. 706 Paragraph 572 related directives for physical security defense in depth by providing the examples in the guidance document of physical security defense in depth via multifactor authentication or layered Physical Security Perimeter(s).
CIP-006-4c R5.	CIP-006-5 R1.4, 1.5, 1.6, 1.7	Monitor physical access – Changed the term to alert for unauthorized access and clarified the actions taken for review of unauthorized physical access alerts. Examples of methods to implement have been moved to the Guidance section of this requirement.
CIP-006-4c R6.	CIP-006-5 R1.8,	Log physical access – CIP-006-4 R6 was specific to the logging of access at identified access points. This now more generally requires logging of physical access into the defined physical boundary. Examples of methods to implement have been moved to the Guidance section of this requirement.
CIP-006-4c R7.	CIP-006-5 R1.9 and CIP-008-5 Evidence Retention	Access log retention - Retain relevant incident related log information is addressed in CIP-008-5.
CIP-006-4c R8.	CIP-006-5 R3	Maintenance and Testing.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R8.1.	CIP-006-5 R3.1	Physical access control system three-year testing and maintenance – Shortened periodicity of testing to 24 calendar months to address FERC Order No. 706, Paragraph 581 directives. Added testing of locally mounted security hardware devices.
CIP-006-4c R8.2.	REMOVED	Testing and maintenance records are considered the measurement of Item 3.1.
CIP-006-4c R8.3.	REMOVED	Removed. With the addition of the "identify, assess, and correct deficiencies" language in CIP-006-5, Requirement R1, this requirement part is no longer necessary.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R1.	CIP-010-1 R1.4	Assess security controls following changes - Provides clarity on when testing must occur, and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.
CIP-007-4 R1.1.	CIP-010-1 R1.5	Test procedures – This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.
CIP-007-4 R1.2.	CIP-010-1 R1.5	Testing reflects production environment - This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.
CIP-007-4 R1.3.	CIP-010-1 R1.4, 1.5	The Responsible Entity shall document test results. The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R2.	CIP-007-5 R1	Ports and Services – The requirement focuses on the entity knowing, and only allowing those ports that are necessary. The additional classification of "normal" or "emergency" added no value and has been removed. Added language that the entity implements its documented programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-007-4 R2.1.	CIP-007-5 R1.1	Enable only those ports and services required for normal and emergency operations –. The requirement focuses on the entity knowing and allowing those ports necessary. The additional classification of 'normal or emergency' added no value and has been removed.
CIP-007-4 R2.2.	CIP-007-5 R1.1, 1.2	Disable other ports/services –In March 18, 2010 FERC issued an order to approve NERC"s interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.
CIP-007-4 R2.3.	DELETED	Compensating measures – See description and justification for CIP-007-4 R2.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R3.	CIP-007-5 R2	Security Patch Management – The existing wording, or CIP-007-4 R3, R3.1 and R3.2 was separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "Document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades." There has been confusion as to what constitutes the availability. Due to issues that may occur regarding control system vendor license and service agreements flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets. Added language that the entity implements its documented programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-007-4 R3.1.	CIP-007-5 R2.2	Assess patches – Similar to the current wording, but added reference to "identification of a source or sources that the Responsible Entity tracks" to establish where the release is from. The word in previous versions: "The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades," has led to varying opinions as to what constitutes "availability" of the patches or upgrades. The addition attempts to clarify where the release is from. There was a change made that reads "since the last evaluation at least once every 35 calendar days".

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R3.2.	CIP-007-5 R2.3, 2.4	Implement patches - This is the same concept as in the current CIP-007 R3.2 wording; however, a 35 calendar day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used. Splitting the implementation of security related patches, hot fixes, and/or updates into a separate item from compensating measures will provide granularity. Automated processes allow the implementation to be documented and confirmed electronically in a short time period. Manual processes may take an extended period of time to complete documentation of the installation. Priority should be given to the implementation rather than the documentation.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R4.	CIP-007-5 R3, 3.1, 3.2, 3.3	Malicious Software Prevention – In prior versions, this requirement has arguably been the single greatest generator of TFE's as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method, nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a Responsible Entity does this should be detailed in its Cyber Security Policy so that it can be audited for compliance…" In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level, and regardless of technology, along with the enhanced change management requirements, meets this directive.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R4.1.	CIP-007-5 R3.1	Malware prevention tools – See description and justification for CIP-007-4 R3.
CIP-007-4 R4.2.	CIP-007-5 R3.2, 3.3	Update malicious code detections – See description and justification for CIP-007-4 R3.
CIP-007-4 R5.	CIP-007-5 R5.1	Use at least one authentication method – The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase, "that minimize the risk of unauthorized access," was removed and more appropriately captured in the Rationale Statement.
CIP-007-4 R5.1.	CIP-004-5 R4.1,	Access authorization – CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need-to-know" basis, or with respect to work functions performed. These were consolidated in CIP-004-5 R4.1 to ensure consistency in the requirement language.
CIP-007-4 R5.1.1.	CIP-003-5 R5.2	Access authorization – CIP-003-5 R5.2 requires CIP Senior Manager or delegate approval for all requirements for authorization in the CIP Cyber Security Standards.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R5.1.2.	CIP-007-5 R4.1	Identify security events for after-the-fact investigation – This requirement is derived from NIST 800-53, Version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the phrase, "system events related to cyber security," from informal comments received. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP, as required in CIP-005-4 R3, and user access and activity logs, as required in CIP-007-5 R5, are also included here.
CIP-007-4 R5.1.3.	CIP-004-5 R4.3	Account privilege verification – Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions. Stated that the account privilege verification be conducted at least once every 15 calendar months.
CIP-007-4 R5.2.	CIP-007-5 R5.2	Identify account types and determine acceptable use – CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure, at best.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R5.2.1.	CIP-007-5 R5.4	Change default vendor passwords – The requirement for the "removal, disabling, or renaming of such accounts where possible," has been removed and incorporated into Guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded, uniquely generated default password was manufactured with the BES Cyber System.
CIP-007-4 R5.2.2.	CIP-007-5 R5.3	Identify those individuals with access to shared accounts - No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.
CIP-007-4 R5.2.3.	CIP-007-5 R5.2, 5.3	Identify account types and determine acceptable use – No significant changes.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R5.3.	CIP-007-5 R5.5	Implement a password policy – CIP-007-4 R5.3 requires the use of passwords, and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials, while recognizing password parameters alone do not achieve this. The drafting team believes allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.
CIP-007-4 R5.3.1.	CIP-007-5 R5.5	Password length – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.2.	CIP-007-5 R5.5	Password complexity – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.3.	CIP-007-5 R5.5, 5.6	Password change frequency – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R6.	CIP-007-5 R4	Security Status Monitoring – Consolidated requirements for monitoring electronic events into CIP-007-5 R4.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R6.1.	CIP-007-5 R4.1	Identify security events – This requirement is derived from NIST 800-53, Version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the phrase, "system events related to cyber security" from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP, as required in CIP-005-4 R3, and user access and activity logs, as required in CIP-007-5 R5, are also included here.
CIP-007-4 R6.2.	CIP-007-5 R4.2	Identify security events for Real-time alerting – This requirement is derived from alerting requirements in CIP-005-4 R3.2 and CIP-007-4 R6.2, in addition to NIST 800-53, Version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.
CIP-007-4 R6.3.	CIP-007-5 R4.1	Identify security events for after-the-fact investigation – See description and justification for CIP-007-4 R6.1.
CIP-007-4 R6.4.	CIP-007-5 R4.4	Retain relevant log information – No significant changes.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R6.5.	CIP-007-5 R4.5	Review logs – Beginning in Paragraph 525, and also Paragraph 628 of the FERC Order No. 706, the commission directs a manual review of security event logs on a more periodic basis, and suggests a weekly review. The order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.
CIP-007-4 R7.	CIP-011-1 R2.1	Disposal or Redeployment – Consistent with FERC Order No. 706, Paragraph 631, clarified that the goal was to prevent the unauthorized retrieval of information from the asset, removing the word “erase” as, depending on the media itself, erasure may not be sufficient to meet this goal. Moved requirement explicitly requiring records of destruction/redeployment to a measure of compliance. Added requirement for chain of custody if the device is taken outside the Physical Security Perimeter.
CIP-007-4 R7.1.	CIP-011-1 R2.2	Disposal - Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the asset, removing the word “erase” since, depending on the media itself, erasure may not be sufficient to meet this goal. Moved requirement explicitly requiring records of destruction/redeployment, to a measure of compliance. Added requirement for chain of custody if the device is taken outside the Physical Security Perimeter.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R7.2.	CIP-011-1 R2.1	Redeployment – See description and justification for CIP-007-4 R7.
CIP-007-4 R7.3.	Measures	See description and justification for CIP-007-4 R7.
CIP-007-4 R8.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated requirements for vulnerability assessments from CIP-005-4 and CIP-007-4.
CIP-007-4 R8.1.	Measures	A document identifying the vulnerability assessment process – This is example evidence required for compliance.
CIP-007-4 R8.2.	CIP-010-1 R3.1, 3.2	Ports and services review – As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are included in Guidance.
CIP-007-4 R8.3.	CIP-010-1 R3.1, 3.2	A review of controls for default accounts – As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are included in Guidance.
CIP-007-4 R8.4.	CIP-010-1 R3.4	Mitigation plan – Added a requirement for an entity planned date of completion as per the FERC directive in Order No. 706, Paragraph 643.
CIP-007-4 R9.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
NEW	CIP-007-5 R1.2	Restrict physical I/O ports – In March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g., TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-007-5 R2.1	Identify patch sources – Defining the source(s) that a Responsible Entity monitors for the release of security related patches, hot fixes, and/or updates will provide a starting point for assessing the effectiveness of the patch management process. Documenting the source is also used to determine when the assessment time frame clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.
NEW	CIP-007-5 R4.3	Generate Real-time alerts and respond to audit-processing failures – This requirement was derived from NIST 800-53, Version 3 AU-5, which addresses response to audit processing failures. Some interpretations of version 4 CIP Cyber Security Standards considered the failure of the security event monitoring and alerting system to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.
NEW	CIP-007-5 R5.7	Limits or alerts on exceeding unsuccessful log in attempts threshold – Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-008-4 R1.	CIP-008-5 R1	Cyber Security Incident Response Plan – Separated requirement into multiple requirements in a comparable manner as CIP-009-4, where individual aspects of maintaining the plan are listed as separate requirements.
CIP-008-4 R1.1.	CIP-008-5 R1.1, 1.2	Identify reportable cyber security events – Defined the term Reportable Cyber Security Incident and further described the meaning in relation to CIP-008-5. "Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity. EOP-004-2 will address the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. In R1.2, language was added to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) and that notification, even if a preliminary notice, exceed one hour.
CIP-008-4 R1.2.	CIP-008-5 R1.3, R1.4	Roles and responsibilities of incident response teams –Replaced "incident response teams" with "incident response groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams. Conforming change to reference new defined term Cyber Security Incidents.
CIP-008-4 R1.3.	DELETED	Reporting cyber security incidents – Coordinated with EOP-004-2 drafting team to ensure EOP-004-2 becomes the single standard for reporting incidents, and ensure EOP-004-2 references the defined term Reportable Cyber Security Incidents.

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-008-4 R1.4.	CIP-008-5 R3.1.2, 3.4	Update incident response plan following review – Included additional specification on update of response plan. Addresses FERC Order No. 706, Paragraph 686 directive to modify on lessons learned. Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.
CIP-008-4 R1.5.	CIP-008-5 R3.1, R3.3	Review incident response plans annually – Specified what the annual review entails. Addresses FERC Order No. 706, Paragraph 686 to document test, or actual incidents and lessons learned.
CIP-008-4 R1.6.	CIP-008-5 R2.1, 2.2	Test incident response plans annually – Allows deviation from plan(s) during actual events or testing if deviations are recorded for review, and specifies activities required to maintain the plan. In R2.1, changed "Annually" to at least once every 15 calendars months.
CIP-008-4 R2.	CIP-008-5 R2.3	Cyber Security Incident Documentation –Removed references to the retention period because the standard addresses data retention in the Compliance section.
NEW	CIP-008-5 R3.1.1	Document any lessons learned - Addresses FERC Order No. 706, Paragraph 686 to document test or actual incidents and lessons learned.
NEW	CIP-008-5 R3.1,R3.3.1	Communicate incident response plan updates – Added specific timing requirement on communication of plan changes based on review of the DHS Controls and NIST 800-53 guideline.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-4 R1.	CIP-009-5 R1, R3.1, R3.3	Recovery Plan – Added requirement for documentation of any identified deficiencies or lessons learned. Added the requirement to additionally review plans after technology changes. Added requirement parts to document any lessons learned (3.3.1), update recovery plan based on documented lessons learned (3.3.2), and notify each person or group of any updates to the recovery plan (3.3.1).
CIP-009-4 R1.1.	CIP-009-5 R1.1	Conditions for activation of recovery plan – Minor wording changes, essentially unchanged.
CIP-009-4 R1.2.	CIP-009-5 R1.2	Roles and responsibilities of recovery plan responders – No significant changes.
CIP-009-4 R2.	CIP-009-5 R2, R2.1	Test recovery plan annually – Added language that the entity implements its documented programs in a manner that identifies, assesses, and corrects deficiencies. Changed “Annually” to at least once every 15 calendars months.
CIP-009-4 R3.	CIP-009-5 R3.2	Review results of recovery plan activities (tests, events) – Added the time frame for update.
CIP-009-4 R4.	CIP-009-5 R1.3	Backup processes – No significant changes.
CIP-009-4 R5.	CIP-009-5 R2.2	Test information used for recovery – Combined requirement from CIP-009-4 R5 and included requirement to test when initially stored. Addresses FERC Order No. 706, Directives 739 and 748 related to testing of backups. Changed “Annually” to at least once every 15 calendars months.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-009-5 R1.4	Testing of backup media – Addresses FERC Order No. 706, Paragraph 739 and 748 directives regarding the testing of backup media.
NEW	CIP-009-5 R1.5	Process to preserve data for analysis – Added requirement to address FERC Order No. 706, Paragraph 706, regarding the necessity to have procedures in place to retain Cyber Asset evidence as part of the recovery planning.
NEW	CIP-009-5 R2.3	Test each of the recovery plans for high impact BES Cyber Systems at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. Addresses FERC Order No. 706, Paragraph 725, to add the requirement that the recovery plan test be a full operational test once every 3 years.
NEW	CIP-009-5 R3.4	Communicate recovery plan updates – This change ensures that recovery personnel are aware of any changes to recovery plans.
Standard: New Requirements in CIP-010-1 and CIP-011-1		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-1 R1.1	Baseline configuration – Baseline requirement incorporated from the DHS Catalog for Control Systems Security (also NIST 800-53). The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-1 R2.1	The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes. This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397. DHS Catalog & addresses FERC Order No. 706, Paragraph 397. Thirty-five calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.
NEW	CIP-010-1 R3.2	Live Vulnerability Assessment for high impact BES Cyber Systems – Addresses FERC Order No. 706, Paragraph 541, 542, 544, and 547 directives regarding the performance of a live vulnerability assessment.
NEW	CIP-010-1 R3.3	Perform active VA on new BES Cyber Assets for high impact - Addresses FERC Order No. 706, Paragraph 541, 542, 544, and 547 directives regarding the performance of a vulnerability assessment prior to placing a new Cyber Asset into production.

Project 2008-06 - Cyber Security Order 706 - Version 5

Working Draft (~~April XX, 2012~~September 11, 2012) of Mapping Document Showing Translation of CIP-002-4 to CIP-009-4 into CIP-002-5 to CIP-009-5, CIP-010-1, and CIP-011-1.

Standard: CIP-002-4 – Cyber Security—Critical Asset Identification		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-002-4 R1.	CIP-002-5 R1.1	Critical Asset Identification – Instead of identifying Critical Assets as in previous versions, the Responsible Entity must Identify Facilities, s~~S~~ystems, or equipment that meet the criteria specified in CIP-002-5, Attachment 1.
CIP-002-4 R2.	CIP-002-5 R1.2, R1.3	Critical Cyber Asset Identification – Using the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 Impact Rating Criteria, the Responsible Entity must identify and categorize its BES Cyber Systems as high impact or medium impact. BES Cyber Systems not identified as high impact or medium impact default to low impact. New ~~Standard~~ standard identifies BES Cyber Systems as a grouping of BES Cyber Assets because it allows entities to apply some requirements at a system rather than asset level.

Standard: CIP-002-4 – Cyber Security—Critical Asset Identification		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-002-4 R2.	DELETED	Routable protocol exemption – A complete exemption of Cyber Assets based on communication characteristics no longer applies. This is because the vulnerability some security requirements address is not mitigated by the lack of routable protocols (e.g., training, response, recovery, etc.) Where the lack of routable protocols itself meets the requirement objective, the exemption is applied at the requirement level.
CIP-002-4 R3.	CIP-002-5 R2, R2.1, R2.2	Annual Approval – ~~No significant changes to the approval.~~R2.1 states that the review must be at least once every 15 calendar months. However, the CIP Sr. Manager now approves identifications required in CIP-002-5 R1 as noted above.
~~NEW~~	~~CIP-002-5 1.4~~	~~Update and re-categorize for changes to BES – Specifies time frame for complying with all re-categorization of items identified in CIP 002-5 R1 following a change, which is planned to be in service for more than six calendar months.~~

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R1.	CIP-003-5 R1, 1.1 through 1.9	Cyber Security Policy – Includes high impact and medium impact BES Cyber Systems. A separate requirement applies to low impact BES Cyber Systems. Clarified that the cyber security policy needs to only reference the subject matter topics at a high level rather than each individual requirement in the CIP Cyber Security Standards.
CIP-003-4 R1.1.	CIP-003-5 RR1, 1.910	Provision for emergency situations – Identified the specific exceptional circumstances in which emergency exceptions can be taken in response to the directive in FERC Order No. 706, Paragraph 443.
NEW	CIP-003-5 R2	Cyber Security Policy for BES Cyber Systems not identified as high or medium impact (low impact). Clarified programmatic controls that apply to low impact BES Cyber Systems and that discrete identification of such systems is not required. Added that the CIP Senior Manager approve the policies at least once every 15 calendar months.
CIP-003-4 R1.2.	DELETED	The Cyber Security Policy is readily available –This was in response to general confusion around the term "readily available." Training requirements in CIP-004-5 provide for knowledge of policy.
CIP-003-4 R1.3.	CIP-003-5 R1 4	Annual review and approval – No significant change. The review and approval by the CIP Senior Manager at least once every 15 calendar months language has been added to R1.
CIP-003-4 R2.	CIP-003-5 R3	Single senior manager – Created a definition of CIP Senior Manager to facilitate references across standards.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R2.1.	CIP-003-5 R3	The CIP Senior Manager shall be identified by name, title, and date of designation – The CIP Senior Manager only needs to be identified by name. The other details were considered unnecessary, administrative requirements.
CIP-003-4 R2.2.	CIP-003-5 R3~~6~~	Changes to the CIP Senior Manager and any delegations must be documented within 30 calendar days of the change.
CIP-003-4 R2.3.	CIP-003-5 ~~R5~~R4	Delegate authority – Made clear that where allowed by the standards, the CIP Senior Manager may delegate authority and such delegations must be documented. Added that the Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a process to delegate actions, unless no delegations are used.
CIP-003-4 R2.4.	DELETED	Authorize and document any exception – The FERC Order No. 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the standards.
CIP-003-4 R3.	DELETED	Exceptions – The FERC Order No. 706 made clear that you could not take exceptions to areas of your Cyber Security Policy that were also required as part of other NERC CIP requirements. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the standards.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R3.1.	DELETED	Exceptions - Requirement R3 is deleted.
CIP-003-4 R3.2.	DELETED	Exceptions - Requirement R3 is deleted.
CIP-003-4 R3.3.	DELETED	Exceptions - Requirement R3 is deleted.
CIP-003-4 R4.	CIP-011-1 R1, 1.1, 1.2	Information Protection - Removed language to "protect" information, and replaced with requirements for methods to identify BES Cyber System Information and procedures for– handling BES Cyber System Information, including storage, transit, and use to clarify the protection that is required. Added language that the entity implements its information protection programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-003-4 R4.1.	Definition	Identification – Replaced this requirement with the defined term BES Cyber System Information.
CIP-003-4 R4.2.	CIP-011-5 R1.1	Classification – Removed the explicit requirement for classification, as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.
CIP-003-4 R4.3.	CIP-011-5 R1.3	Assessment – No significant changes.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R5.	CIP-004-5 ~~R6~~R4.4~~,~~	Authorize personnel for access to protected information – Clarified: "Program for managing access" included the authorization of access, as well as handling and access control procedures. Grouped requirements for electronic access, physical access, and access to BES Cyber System Information in CIP 004-5 ~~R6~~R4. Added language that the entity implements its documented access management programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-003-4 R5.1.	CIP-004-5 ~~R6~~R4.1	Authorizing personnel.
CIP-003-4 R5.1.1.	CIP-004-5 ~~R6~~R4.1	~~Personnel shall be identified.~~Have a process to authorize, which could include identifying specific personnel to authorize access.
CIP-003-4 R5.1.2.	CIP-004-5 ~~R6~~R4.3, R4.4~~7~~	Verification.
CIP-003-4 R5.2.	CIP-004-5 ~~R6~~R4.3, R4.4~~7~~	Verify access privileges ~~annually~~ – Moved requirement to ensure consistency among access reviews. Clarified precise meaning in the term "annual". Clarified what was necessary in performing verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.
CIP-003-4 R5.3.	CIP-~~011-1 1.3~~004-5 R4.3, R4.4	Annual Review – No significant changes.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R6.	CIP-010-1 R1, R2	Change Control and Configuration Management – Moved configuration change management to a separate standard because of the additional requirements necessary for satisfying FERC directives, and the subject matter in CIP version 4 is spread across CIP-003-4 and CIP-007-4. The baseline requirement is incorporated from the *DHS Catalog for Control Systems Security*. The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed. Added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-4 R6. Added language that the entity implements its documented processes in a manner that identifies, assesses, and corrects deficiencies.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R1.	CIP-004-5 R1, 1.1	Security awareness program and quarterly reinforcement - Changed to remove the need to ensure everyone with authorized access receive this material, and moved example mechanisms to ~~Guidance~~guidance.
CIP-004-4 R2.	CIP-004-5 R2~~, R3~~	Training - Addition of identifying the ~~roles that require~~ training content. Adding ~~specific role-based training~~ content for the visitor control program and storage ~~media~~ as part of the handling of BES Cyber Systems information. Also added the FERC Order No. 706, directed electronic interconnectivity supporting the operation and control of BES Cyber Systems. This requirement is also reorganized into the respective requirements for "program" and "implementation" of the training. Added language that the entity implements its documented programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-004-4 R2.1.	CIP-004-5 ~~R3.1~~R2.2	Training prior to authorized access – No significant changes.
CIP-004-4 R2.2.	CIP-004-5 R2.1.1-2.1.9~~0~~	Training subject matter – This requirement is reorganized into the respective requirements for "program" and "implementation" of the training.
CIP-004-4 R2.2.1.	CIP-004-5 R2.~~2~~1	Proper use of CCAs – Changed to refer to BES Cyber Systems. Requirement now addresses cyber security issues, not the business or functional use of the BES Cyber System.
CIP-004-4 R2.2.2.	CIP-004-5 R2.1~~3,2.4~~	Physical and electronic access controls training – No significant changes. Refers to BES Cyber Systems.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R2.2.3.	CIP-004-5 R2.1~~6~~	Information handling training – Core training added for the handling of BES Cyber System Information, with the addition of storage media.
CIP-004-4 R2.2.4.	CIP-004-5 R2.~~7,2.8,2.9~~1, R2.1.1-R2.1.9	Incident identification and notification, incident handling and CCA recovery training – Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for individuals having a role in the recovery to address FERC Order No. 706, Paragraph 413.
CIP-004-4 R2.3.	CIP-004-5 R2.3~~3.2~~	Annual training – Replaced "Annually" with "~~calendar year, not to exceed 15 months."~~ at least once every 15 calendar months."
CIP-004-4 R3.	CIP-004-5 R~~4, R5, 5.1~~3	Personnel Risk Assessment – ~~Split into two requirements, R4 R3 to define the PRA program, and R5 R4 to implement the program for individuals prior to obtaining authorized access~~. Added language that the entity implements its documented programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-004-4 R3.1.	CIP-004-5 R3.1, ~~4~~3~~R~~.2.1~~1~~, 3~~4~~.2.2	Identification and 7-year criminal check – Addressed interpretation request in ~~Guidance~~guidance. Specified that identity verification is only required for each individual's initial assessment. Specified that the 7-year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for 6 consecutive months or more, including current residence, regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full 7-year check cannot be performed.
CIP-004-4 R3.2.	CIP-004-5 ~~R5~~R3.~~2~~5	Perform the PRA every 7 years– Removed the "for cause" part of the requirement.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R3.3.	CIP-004-5 ~~R4~~R3.4	Addresses the contractor or vendor performed PRA.
NEW	CIP-004-5 R3.3	Process to evaluate criminal history records checks for authorizing access.
CIP-004-4 R4.	CIP-004-5 R4~~6~~.1~~2~~, 4~~6~~.3	Authorize access - CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need-to-know" basis, or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.
CIP-004-4 R4.1.	CIP-004-5 ~~R6~~R4.~~5~~2	Quarterly review of access – Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4 R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R4.2.	CIP-004-5 R5~~7~~	Prevent further access - The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the standards to require immediate revocation for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination, instead of within 24 hours. For transfers, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53, Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.
NEW	CIP-004-5 R2.1	Added to help facilitate understanding what roles the entity has to support the role-based training program.
NEW	CIP-004-5 R2.1.4~~5~~	Visitor control program training – Personnel administering the visitor control program and/or providing escort should be part of the core training per FERC Order No. 706, ~~-~~Paragraph 432.
~~NEW~~	~~CIP-004-5 R2.10~~	~~Electronic interconnectivity training – Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems per FERC Order No. 706 - Paragraph 434.~~
NEW	CIP-004-5 R4~~3~~.3	PRA failure criteria – Requires process or criteria to evaluate personnel risk assessments to determine when to deny authorized access.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-004-5 R5~~7~~.2	Transfers – The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53, Version 3, to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.
NEW	CIP-004-5 R5~~7~~.4	Completion of revocation – The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the standards to require immediate revocation for any person no longer needing access. In order to meet the immediate time frame, entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
NEW	CIP-004-5 R5~~7~~.5	Completion of revocation (shared accounts) – To provide clarification of expected actions in managing the passwords

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R1.	CIP-005-5 R1.1	Electronic Security Perimeter identification – Changes include referencing the defined terms Electronic Access Point and BES Cyber System.
CIP-005-4a R1.1.	Definition	Access Points – This was moved to the definition of Electronic Access Points.
CIP-005-4a R1.2.	Guidance	Dial-up accessible CCA – This is a clarifying statement that was moved to Guidance.
CIP-005-4a R1.3.	Guidance	Communication links between ESPs – This is a clarifying statement that was moved to Guidance.
CIP-005-4a R1.4.	Applicability	Applicability for Non-Critical Cyber Asset – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.5.	Applicability	Access control and monitoring Cyber Assets – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.6.	Measures	Maintain Documentation – This is a measure for the requirement to have ESP documentation.
CIP-005-4a R2.	CIP-005-5 R1	Electronic Access Controls – No significant changes.
CIP-005-4a R2.1.	CIP-005-5 R1.2, 1.3	Deny access by default - Changes include referring to the defined term Electronic Access Point, and to focus on the entity knowing and having justification for what it allows through the EAP. R1.3 explicitly states the network admission control includes both inbound and outbound connections.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R2.2.	CIP-007-5 R1.1, 1.2	Enable specific ports/services – Consolidated port hardening requirements to CIP-007.
CIP-005-4a R2.3.	CIP-005-5 R1.4	Secure dial-up – Changed to refer to the defined term Electronic Access Point. Added clarification as to the goal of "secure," which is that the BES Cyber System should not be directly accessible with a phone number only.
CIP-005-4a R2.4.	CIP-005-5 R2,2.3	Strong access control – Added a new requirement for remote access in response to increased vulnerabilities in VPN technology. This requirement also clarified strong access control meant ~~two~~multi-factor (or more) authentication.
CIP-005-4a R2.5.	Measures	Example of evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.1.	CIP-004-5 R4~~6~~	The processes for access request and authorization – Consolidated with other similar requirements to CIP-004-5 ~~R6~~R4.
CIP-005-4a R2.5.2.	Measures	The authentication methods ~~-~~ – Example of evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.3.	Measures	The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4. Example of evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.4.	Measures	The controls used to secure dial-up accessible connections. Example of evidence requirements are considered as part of the measure.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R2.6.	DELETED	Appropriate Use Banner – The drafting team considered this requirement administrative. The objective of having an appropriate use banner is to prevent accidental use of the system and help allow prosecution of unauthorized individuals accessing the system. The drafting team did not consider either of these rising to the level of meeting a reliability objective.
CIP-005-4a R3.	CIP-007-5 R4, 4.1	Monitoring Electronic Access – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the standards.
CIP-005-4a R3.1.	CIP-007-5 R4, 4.1	Dial-up Accessible – Removed specific references to dial-up devices. Incorporated into logging/monitoring requirements. The drafting team did not feel further referencing this technology was necessary.
CIP-005-4a R3.2.	CIP-007-5, R4, 4.2	Alerts – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the standards.
CIP-005-4a R4.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements.
CIP-005-4a R4.1.	Measures	A document identifying the vulnerability assessment process ~~-~~ Example of evidence requirements are considered as part of the measure.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R4.2.	CIP-010-1 R3.1, 3.2	A review to verify that only ports and services required for operations at these access points are enabled - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to Guidance.
CIP-005-4a R4.3.	CIP-010-1 R3.1, 3.2	The discovery of all access points to the Electronic Security Perimeter - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to Guidance.
CIP-005-4a R4.4.	CIP-010-1 R3.1, 3.2	A review of controls for default accounts, passwords, and network management community strings - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to Guidance.
CIP-005-4a R4.5.	CIP-010-1 R3.4	Mitigation plan - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. Added element to have an entity defined date of completion of the mitigation plan per FERC Order No. 706, Paragraph 643.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R5.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.1.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.2.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.3.	CIP-007-5 R4.4	Retain relevant log information – Log retention requirements are consolidated to CIP-007-5 R4.
NEW	CIP-005-5 R1.5	Inspect and detect potential malicious communications – Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The order makes clear this is not simple redundancy of firewalls; thus the drafting team has decided to add the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs.
NEW	CIP-005-5 R2.1,2.2	Remote Access: intermediate device and encryption – This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R1.	CIP-006-5 R1	Physical Security Plan – Removed the requirement for senior management approval of the physical security plan because there is already approval of the physical security policy and delegation of the task in complying for this program. Additional approval is not considered necessary to meeting the reliability objective of physical security for the BES Cyber System.
CIP-006-4c R1.1.	CIP-006-5 R1.2, 1.3	Physical Security Perimeter – For high impact BES Cyber Systems clarified that two or more different physical access controls (this does not require two completely independent physical access control systems) must be used to collectively allow unescorted physical access into Physical Security Perimeters.
CIP-006-4c R1.2.	DELETED	No longer requires identification of all physical access points.
CIP-006-4c R1.3.	CIP-006-5 R1.4, 1.5	Monitor physical access – A documented plan is required as part of CIP-006-5 R1 that references the new alerting term in Table Row 1.5. Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.
CIP-006-4c R1.4.	CIP-004-5 R2.3	Appropriate use of access controls – The term "appropriate" used in prior versions is subject to a high degree of subjectivity. The training requirement specifies role-based training on physical access controls.
CIP-006-4c R1.5.	CIP-004-5 ~~R6~~ R4 and ~~R7~~R5	Review of access authorization requests and revocation of access authorization requirements were consolidated to CIP-004-5.
CIP-006-4c R1.6.	CIP-006-5 R2	Visitor control program - A documented program is required as part of CIP-006-5 R2. Otherwise, no significant change.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R1.6.1.	CIP-006-5 R2.2	Log entry and exit of visitors - Addressed multi entry requirements and added the point of contact of who can be considered the sponsor for the person to enter the DPB. There is no need to document the escort or handoffs between escorts.
CIP-006-4c R1.6.2.	CIP-006-5 R2.1	Continuous escorted access of visitors – No significant change.
CIP-006-4c R1.7.	DELETED	Update of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R1.8.	DELETED	Annual review of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R2.	Applicability	Protection of Physical Access Control Systems – Applicability to Physical Access Control and Monitoring Systems were moved to the Applicability section of each security requirement, and added this as a defined term in the glossary.
CIP-006-4c R2.1.	Applicability, CIP-006-5 R1.1	Physical Access Control Systems be protected from unauthorized physical access - Applicability to Physical Access Control Systems were moved to the Applicability section of each security requirement. For this particular requirement, see CIP-006-5, Item 1.1, which applies to Physical Access Control Systems.
CIP-006-4c R2.2.	CIP-006-5 R1.6, 1.7	Protection of Physical Access Control Systems - Applicability to Physical Access Control Systems were moved to the Applicability section of each security requirement throughout CP version 5.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R3.	Applicability	Protection of Electronic Access Control Systems - Applicability to what protections Electronic Access Control and Monitoring Systems need were moved to the Applicability section of each security requirement.
CIP-006-4c R4.	CIP-006-5 R1.2, 1.3	Physical Access Controls – R1.3 addresses FERC Order No. 706 Paragraph 572 related directives for physical security defense in depth by providing the examples in the guidance document of physical security defense in depth via multifactor authentication or layered Physical Security Perimeter(s).
CIP-006-4c R5.	CIP-006-5 R1.4, 1.5, 1.6, 1.7	Monitor physical access – Changed the term to alert for unauthorized access and clarified the actions taken for review of unauthorized physical access alerts. Examples of methods to implement have been moved to the Guidance section of this requirement.
CIP-006-4c R6.	CIP-006-5 R1.8,	Log physical access – CIP-006-4 R6 was specific to the logging of access at identified access points. This now more generally requires logging of physical access into the defined physical boundary. Examples of methods to implement have been moved to the Guidance section of this requirement.
CIP-006-4c R7.	CIP-006-5 R1.9 and CIP-008-5 Evidence Retention	Access log retention - Retain relevant incident related log information is addressed in CIP-008-5.
CIP-006-4c R8.	CIP-006-5 R3	Maintenance and Testing.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R8.1.	CIP-006-5 R3.1	Physical access control system three-year testing and maintenance – Shortened periodicity of testing to ~~2 years~~24 calendar months to address FERC Order No. 706, Paragraph 581 directives. Added testing of locally mounted security hardware devices.
CIP-006-4c R8.2.	REMOVED	Testing and maintenance records are considered the measurement of Item 3.1.
CIP-006-4c R8.3.	~~CIP-006-5 R3.2~~REMOVED	~~Retain outage records – No significant changes.~~Removed. With the addition of the "identify, assess, and correct deficiencies" language in CIP-006-5, Requirement R1, this requirement part is no longer necessary.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R1.	CIP-010-1 R1.4	Assess security controls following changes - Provides clarity on when testing must occur, and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.
CIP-007-4 R1.1.	CIP-010-1 R1.5	Test procedures – This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.
CIP-007-4 R1.2.	CIP-010-1 R1.5	Testing reflects production environment - This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.
CIP-007-4 R1.3.	CIP-010-1 R1.4, 1.5	The Responsible Entity shall document test results. The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R2.	CIP-007-5 R1	Ports and Services – The requirement focuses on the entity knowing, and only allowing those ports that are necessary. The additional classification of "normal" or "emergency" added no value and has been removed. Added language that the entity implements its documented programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-007-4 R2.1.	CIP-007-5 R1.1	Enable only those ports and services required for normal and emergency operations – ~~See description and justification for CIP-007-4 R2~~. The requirement focuses on the entity knowing and allowing those ports necessary. The additional classification of 'normal or emergency' added no value and has been removed.
CIP-007-4 R2.2.	CIP-007-5 R1.1, 1.2	Disable other ports/services – ~~See description and justification for CIP-007-4 R2.~~ In March 18, 2010 FERC issued an order to approve NERC"s interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.
CIP-007-4 R2.3.	DELETED	Compensating measures – See description and justification for CIP-007-4 R2.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R3.	CIP-007-5 R2	Security Patch Management – The existing wording, or CIP-007-4 R3, R3.1 and R3.2 was separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "Document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades." There has been confusion as to what constitutes the availability. Due to issues that may occur regarding control system vendor license and service agreements flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets. Added language that the entity implements its documented programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-007-4 R3.1.	CIP-007-5 R2.2	Assess patches – Similar to the current wording, but added reference to "identification of a source or sources that the Responsible Entity tracks" to establish where the release is from. The word in previous versions: "The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades," has led to varying opinions as to what constitutes "availability" of the patches or upgrades. The addition attempts to clarify where the release is from. There was a change made that reads "since the last evaluation at least once every 35 calendar days".

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R3.2.	CIP-007-5 R2.3, 2.4	Implement patches - This is the same concept as in the current CIP-007 R3.2 wording; however, a ~~30~~35 ~~-day~~calendar day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used. Splitting the implementation of security related patches, hot fixes, and/or updates into a separate item from compensating measures will provide granularity. Automated processes allow the implementation to be documented and confirmed electronically in a short time period. Manual processes may take an extended period of time to complete documentation of the installation. Priority should be given to the implementation rather than the documentation.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R4.	CIP-007-5 R3, 3.1, 3.2, 3.3	Malicious Software Prevention – In prior versions, this requirement has arguably been the single greatest generator of TFE's as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method, nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a Responsible Entity does this should be detailed in its Cyber Security Policy so that it can be audited for compliance…" In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level, and regardless of technology, along with the enhanced change management requirements, meets this directive.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R4.1.	CIP-007-5 R3.1	Malware prevention tools – See description and justification for CIP-007-4 R3.
CIP-007-4 R4.2.	CIP-007-5 R3.2, 3.3	Update malicious code detections – See description and justification for CIP-007-4 R3.
CIP-007-4 R5.	CIP-007-5 R5.1	Use at least one authentication method – The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase, "that minimize the risk of unauthorized access," was removed and more appropriately captured in the Rationale Statement.
CIP-007-4 R5.1.	CIP-004-5 R4~~6~~.1, ~~6.2~~	Access authorization – CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need-to-know" basis, or with respect to work functions performed. These were consolidated in CIP-004-5 ~~R6~~R4.1 ~~and 6.2~~ to ensure consistency in the requirement language.
CIP-007-4 R5.1.1.	CIP-003-5 R5.2	Access authorization – CIP-003-5 R5.2 requires CIP Senior Manager or delegate approval for all requirements for authorization in the CIP Cyber Security Standards.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R5.1.2.	CIP-007-5 R4.1	Identify security events for after-the-fact investigation – This requirement is derived from NIST 800-53, Version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the phrase, "system events related to cyber security," from informal comments received. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP, as required in CIP-005-4 R3, and user access and activity logs, as required in CIP-007-5 R5, are also included here.
CIP-007-4 R5.1.3.	CIP-004-5 R4.3~~6.6~~	~~Annual account~~Account privilege verification – Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions. Stated that the account privilege verification be conducted at least once every 15 calendar months.
CIP-007-4 R5.2.	CIP-007-5 R5.2	Identify account types and determine acceptable use – CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure, at best.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R5.2.1.	CIP-007-5 R5.4	Change default vendor passwords – The requirement for the "removal, disabling, or renaming of such accounts where possible," has been removed and incorporated into Guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded, uniquely generated default password was manufactured with the BES Cyber System.
CIP-007-4 R5.2.2.	CIP-007-5 R5.3	Identify those individuals with access to shared accounts - No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.
CIP-007-4 R5.2.3.	CIP-007-5 R5.2, 5.3	Identify account types and determine acceptable use – No significant changes.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R5.3.	CIP-007-5 R5.5	Implement a password policy – CIP-007-4 R5.3 requires the use of passwords, and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials, while recognizing password parameters alone do not achieve this. The drafting team believes allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.
CIP-007-4 R5.3.1.	CIP-007-5 R5.5	Password length – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.2.	CIP-007-5 R5.5	Password complexity – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.3.	CIP-007-5 R5.5, 5.6	Password change frequency – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R6.	CIP-007-5 R4	Security Status Monitoring – Consolidated requirements for monitoring electronic events into CIP-007-5 R4.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R6.1.	CIP-007-5 R4.1	Identify security events – This requirement is derived from NIST 800-53, Version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the phrase, "system events related to cyber security" from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP, as required in CIP-005-4 R3, and user access and activity logs, as required in CIP-007-5 R5, are also included here.
CIP-007-4 R6.2.	CIP-007-5 R4.2	Identify security events for Real-time alerting – This requirement is derived from alerting requirements in CIP-005-4 R3.2 and CIP-007-4 R6.2, in addition to NIST 800-53, Version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.
CIP-007-4 R6.3.	CIP-007-5 R4.1	Identify security events for after-the-fact investigation – See description and justification for CIP-007-4 R6.1.
CIP-007-4 R6.4.	CIP-007-5 R4.4	Retain relevant log information – No significant changes.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R6.5.	CIP-007-5 R4.5	Review logs – Beginning in Paragraph 525, and also Paragraph 628 of the FERC Order No. 706, the commission directs a manual review of security event logs on a more periodic basis, and suggests a weekly review. The order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.
CIP-007-4 R7.	CIP-011-1 R2.1	Disposal or Redeployment – Consistent with FERC Order No. 706, Paragraph 631, clarified that the goal was to prevent the unauthorized retrieval of information from the asset, removing the word “erase” as, depending on the media itself, erasure may not be sufficient to meet this goal. Moved requirement explicitly requiring records of destruction/redeployment to a measure of compliance. Added requirement for chain of custody if the device is taken outside the Physical Security Perimeter.
CIP-007-4 R7.1.	CIP-011-1 R2.2	Disposal - Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the asset, removing the word “erase” since, depending on the media itself, erasure may not be sufficient to meet this goal. Moved requirement explicitly requiring records of destruction/redeployment, to a measure of compliance. Added requirement for chain of custody if the device is taken outside the Physical Security Perimeter.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R7.2.	CIP-011-1 R2.1	Redeployment – See description and justification for CIP-007-4 R7.
CIP-007-4 R7.3.	Measures	See description and justification for CIP-007-4 R7.
CIP-007-4 R8.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated requirements for vulnerability assessments from CIP-005-4 and CIP-007-4.
CIP-007-4 R8.1.	Measures	A document identifying the vulnerability assessment process – This is example evidence required for compliance.
CIP-007-4 R8.2.	CIP-010-1 R3.1, 3.2	Ports and services review – As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are included in Guidance.
CIP-007-4 R8.3.	CIP-010-1 R3.1, 3.2	A review of controls for default accounts – As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are included in Guidance.
CIP-007-4 R8.4.	CIP-010-1 R3.4	Mitigation plan – Added a requirement for an entity planned date of completion as per the FERC directive in Order No. 706, Paragraph 643.
CIP-007-4 R9.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
NEW	CIP-007-5 R1.2	Restrict physical I/O ports – In March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g., TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-007-5 R2.1	Identify patch sources – Defining the source(s) that a Responsible Entity monitors for the release of security related patches, hot fixes, and/or updates will provide a starting point for assessing the effectiveness of the patch management ~~program~~process. Documenting the source is also used to determine when the assessment time frame clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.
NEW	CIP-007-5 R4.3	Generate Real-time alerts and respond to audit-processing failures – This requirement was derived from NIST 800-53, Version 3 AU-5, which addresses response to audit processing failures. Some interpretations of version 4 CIP Cyber Security Standards considered the failure of the security event monitoring and alerting system to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.
NEW	CIP-007-5 R5.7	Limits or alerts on exceeding unsuccessful log in attempts threshold – Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-008-4 R1.	CIP-008-5 R1	Cyber Security Incident Response Plan – Separated requirement into multiple requirements in a comparable manner as CIP-009-4, where individual aspects of maintaining the plan are listed as separate requirements.
CIP-008-4 R1.1.	CIP-008-5 R1.1, 1.2	Identify reportable cyber security events – Defined the term Reportable Cyber Security Incident and further described the meaning in relation to CIP-008-5. "Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity. EOP-004-2 will address the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. In R1.2, language was added to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) and that notification, even if a preliminary notice, exceed one hour.
CIP-008-4 R1.2.	CIP-008-5 R1.3, R1.4~~, 1.5~~	Roles and responsibilities of incident response teams –Replaced "incident response teams" with "incident response groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams. Conforming change to reference new defined term Cyber Security Incidents. ~~Clarified the term "communication plan" by specifying the elements that need to be included.~~

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-008-4 R1.3.	DELETED	Reporting cyber security incidents – Coordinated with EOP-004-2 drafting team to ensure EOP-004-2 becomes the single standard for reporting incidents, and ensure EOP-004-2 references the defined term Reportable Cyber Security Incidents.
CIP-008-4 R1.4.	CIP-008-5 R3.1.2~~3~~, 3.4	Update incident response plan following review – Included additional specification on update of response plan. Addresses FERC Order No. 706, Paragraph 686 directive to modify on lessons learned. Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.
CIP-008-4 R1.5.	CIP-008-5 R3.1, ~~3.3~~R3.3	Review incident response plans annually – Specified what the annual review entails. Addresses FERC Order No. 706, Paragraph 686 to document test, or actual incidents and lessons learned.
CIP-008-4 R1.6.	CIP-008-5 R2.1, 2.2	Test incident response plans annually – Allows deviation from plan(s) during actual events or testing if deviations are recorded for review, and specifies activities required to maintain the plan. In R2.1, changed "Annually" to at least once every 15 calendars months.
CIP-008-4 R2.	CIP-008-5 R2.3	Cyber Security Incident Documentation –Removed references to the retention period because the standard addresses data retention in the Compliance section.
NEW	CIP-008-5 R3.1.1~~2~~	Document any lessons learned - Addresses FERC Order No. 706, Paragraph 686 to document test or actual incidents and lessons learned.

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-008-5 R3.1,R3.~~5~~3.1	Communicate incident response plan updates – Added specific timing requirement on communication of plan changes based on review of the DHS Controls and NIST 800-53 guideline.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-4 R1.	CIP-009-5 R1, R3.1, R3.3	Recovery Plan – Added requirement for documentation of any identified deficiencies or lessons learned. Added the requirement to additionally review plans after technology changes. Added requirement parts to document any lessons learned (3.3.1), update recovery plan based on documented lessons learned (3.3.2), and notify each person or group of any updates to the recovery plan (3.3.1).
CIP-009-4 R1.1.	CIP-009-5 R1.1	Conditions for activation of recovery plan – Minor wording changes, essentially unchanged.
CIP-009-4 R1.2.	CIP-009-5 R1.2	Roles and responsibilities of recovery plan responders – No significant changes.
CIP-009-4 R2.	CIP-009-5 R2, R2.1~~.1~~	Test recovery plan annually – Added language that the entity implements its documented programs in a manner that identifies, assesses, and corrects deficiencies.~~No significant changes.~~ Changed "Annually" to at least once every 15 calendars months.
CIP-009-4 R3.	CIP-009-5 R3.2	Review results of recovery plan activities (tests, events) – Added the time frame for update.
CIP-009-4 R4.	CIP-009-5 R1.3	Backup processes – No significant changes.
CIP-009-4 R5.	CIP-009-5 R2.2	Test information used for recovery – Combined requirement from CIP-009-4 R5 and included requirement to test when initially stored. Addresses FERC Order No. 706, Directives 739 and 748 related to testing of backups. Changed "Annually" to at least once every 15 calendars months.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-009-5 R1.4	Testing of backup media – Addresses FERC Order No. 706, Paragraph 739 and 748 directives regarding the testing of backup media.
NEW	CIP-009-5 R1.5	Process to preserve data for analysis – Added requirement to address FERC Order No. 706, Paragraph 706, regarding the necessity to have procedures in place to retain Cyber Asset evidence as part of the recovery planning.
NEW	CIP-009-5 R2.3	Test each of the recovery plans for high impact BES Cyber Systems at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. Addresses FERC Order No. 706, Paragraph 725, to add the requirement that the recovery plan test be a full operational test once every 3 years.
NEW	CIP-009-5 R3.4	Communicate recovery plan updates – This change ensures that recovery personnel are aware of any changes to recovery plans.
Standard: New Requirements in CIP-010-1 and CIP-011-1		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-1 R1.1	Baseline configuration – Baseline requirement incorporated from the DHS Catalog for Control Systems Security (also NIST 800-53). The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-1 R2.1	The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes. This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397. DHS Catalog & addresses FERC Order No. 706, Paragraph 397. Thirty-five calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.
NEW	CIP-010-1 R3.2	Live Vulnerability Assessment for high impact BES Cyber Systems – Addresses FERC Order No. 706, Paragraph 541, 542, 544, and 547 directives regarding the performance of a live vulnerability assessment.
NEW	CIP-010-1 R3.3	Perform active VA on new BES Cyber Assets for high impact - Addresses FERC Order No. 706, Paragraph 541, 542, 544, and 547 directives regarding the performance of a vulnerability assessment prior to placing a new Cyber Asset into production.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-4

3. Purpose: NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its records of approvals as specified in Requirement R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 The Regional Entity shall serve as the Compliance Enforcement Authority with the following exceptions:

- For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.2. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change “Control Center” to “control center”	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-4

3. Purpose: Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-003-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-4 Requirement R2.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance	

		Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-4

3. Purpose: Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-004-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-004-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);

- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program. Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-4a

3. Purpose: Standard CIP-005-4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4a should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-005-4a, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-4a:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4a.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.1 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.1 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.2 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-4a from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Developed separately.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2	Approved by NERC Board of	Modifications to clarify the requirements and to bring the compliance elements into	Revised.

	Trustees 5/6/09	conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Changed CIP-005-2 to CIP-005-3. Changed all references to CIP Version "2" standards to CIP Version "3" standards. For Violation Severity Levels, changed, "To be developed later" to "Developed separately."	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010	Addition
4a	01/24/11	Adopted by the NERC Board of Trustees	Update to conform to changes to CIP-002-4 (Project 2008-06) Update version number from "3" to "4a"

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-4c

3. Purpose: Standard CIP-006-4 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-4c should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-006-4c, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-006-4c:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the

Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-4c for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	May 2, 2006	Adopted by NERC Board of Trustees	
1	January 18, 2008	FERC Order issued approving CIP-006-1	
	February 12, 2008	Interpretation of R1 and Additional Compliance Information Section 1.4.4 adopted by NERC Board of Trustees	Project 2007-27
2		Updated version number from -1 to -2 Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	Project 2008-06
2	May 6, 2009	Adopted by NERC Board of Trustees	
	August 5, 2009	Interpretation of R4 adopted by NERC Board of Trustees	Project 2008-15
2	September 30, 2009	FERC Order issued approving CIP-006-2	
3	November 18, 2009	Updated version number from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized. Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	Project 2009-21
3	December 16, 2009	Adopted by NERC Board of Trustees	
	February 16, 2010	Interpretation of R1 and R1.1 adopted by NERC Board of Trustees	Project 2009-13
3	March 31, 2010	FERC Order issued approving CIP-006-3	
2a/3a	July 15, 2010	FERC Order issued approving the Interpretation of R1 and R1.1. Updated version numbers from -2/-3 to -2a/-3a.	
4	January 24,	Adopted by NERC Board of Trustees	

	2011		
3c/4c	May 19, 2011	FERC Order issued approving two interpretations: 1) Interpretation of R1 and Additional Compliance Information Section 1.4.4; and 2) Interpretation of R4. Updated version number from -3/-4 to -3c/-4c.	

Appendix 1

Requirement Number and Text of Requirement
R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following: R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
Question
If a completely enclosed border cannot be created, what does the phrase, "to control physical access" require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption? Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?
Response
For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are "physical in nature." The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

Appendix 2

Interpretation of Requirement R1.1.

Request: *Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*

Interpretation:

Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border.

CIP-006-1 — Requirement 1.1 requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

CIP-006-1 — Additional Compliance Information 1.4.4 identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.

1.4. Additional Compliance Information

1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.

Appendix 3

The following interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R4 was developed by the standard drafting team assigned to Project 2008-14 (Cyber Security Violation Severity Levels) on October 23, 2008.

Request:

1. *For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*
2. *Does the term, "time of access" mean logging when the person entered the facility or does it mean logging the entry/exit time and "length" of time the person had access to the critical asset?*

Interpretation:

No, monitoring and logging of access are only required for ingress at this time. The term "time of access" refers to the time an authorized individual enters the physical security perimeter.

Requirement Number and Text of Requirement

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-4

3. Purpose: Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-007-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-4 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	

		Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-4

3. Purpose: Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-008-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-4 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated Version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-4

3. Purpose: Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-009-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-009-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards
Comment Form A
CIP-002 and CIP-003 Questions

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Summary Consideration, Explanation, and Common Responses to Global Changes and to Issues and Comments Frequently Repeated

In response to draft 2 of the Version 5 CIP Cyber Security Standards, the Standards Drafting Team (SDT) received significant input from a wide variety of perspectives. All of that input greatly helped the team to refine the standards and associated documents, and the set of standards now posted reflects all of that combined input. There were several varied perspectives in the comments, and the SDT attempted to address each comment as responsively as possible.

There were several changes that reflected careful consideration of several comments that affected the standards on a global basis, whether in format, style, or substance. In addition, there were several comments the SDT considered that were repeated across multiple questions, sometimes submitted by the same entity to each or to many of the questions. Rather than explaining in detail the global changes in response to each question, and rather than responding separately to the frequently repeated comments in each question, the SDT addresses those global issues and general comments in this section.

Many comments related to specific language suggestions or to specific compliance concerns. The SDT has responded to those comments in each of the individual questions summaries that follow this section. Those comments were thorough and varied, and they reflected diverse perspectives and topics. The SDT expended considerable work in reviewing, discussing, and responding to all of these inputs, and it believes that the major issues have been addressed responsively in this posted draft CIP Version 5 package. As a result, the changes have been significant and substantive in all of the draft CIP Version 5 standards and Implementation Plan. The SDT believes this posting package addresses all of the substantive issues received from the previous two iterations of comments and various other inputs.

Change in labeling of the applicability columns in the tables to "Applicable Systems"
After posting draft 1 of CIP Version 5, commenters expressed concern that merely using "Applicability" as the title of the applicability columns in the Requirement tables (in CIP-004 through CIP-011) created confusion with the actual "Applicability" section of the standards. In response, for draft 2, the SDT added specificity and labeled those columns "Applicable BES Cyber Systems and associated Cyber Assets." In response to that change in draft 2, commenters expressed concern with the length and suggested that the SDT label the applicability column "Applicability." Therefore, the SDT is proposing to label these columns, "Applicable Systems." This should eliminate any confusion with the applicability section of the standards themselves while also providing appropriate brevity.
Handling of "associated" Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCA) (and the associated change to their use in the "Applicable Systems" column of the requirement tables)
In previous drafts, in the applicability columns (now "applicable systems" columns), the standards used a term "Associated Protected Cyber Assets," "Associated Electronic Access Control or Monitoring

Systems," and "Associated Physical Access Control Systems" where it intended that the requirement part be applicable to not only the applicable high or medium impact BES Cyber Systems, but also to other Cyber Assets or systems, as specified, associated with those BES Cyber Systems. Also, for Protected Cyber Assets, the requirement applied to Cyber Assets or lower impact BES Cyber Systems that were in the same ESP as the applicable BES Cyber System. There was confusion the precise meaning or application of the "associated" systems, and the SDT has made the link more explicit in this draft. One of the fundamental concepts of CIP Version 5 is that it is adopting a systems approach, and those "associated" systems should be more closely connected with the applicable subject of the requirement. Therefore the SDT has moved the associated systems to follow immediately after the subject of the requirement and clarified that they are "associated with" that specify type of BES Cyber System or other applicable system. Mitigation for the associated systems may be accomplished through other applicable systems.

High Watermarking Concept

The CIP Version 5 Standards use a term "Protected Cyber Assets" to refer to those Cyber Assets that are within the ESP, which in previous versions of the standards were "other (non-critical) Cyber Assets within the ESP" (see CIP-005-4, Requirement R1, Part 1.4, and CIP-007-4). Additionally, in Version 5, a Protected Cyber Asset can also be a BES Cyber System of a lower impact classification if it is within the same ESP as a higher impact BES Cyber System.

For example, CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The standard does not require segmenting of BES Cyber Systems by impact classification, and many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and systems within the ESP will be elevated to the level of the highest impact BES Cyber System present in

the ESP. The standard accomplishes this by defining all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

Measures: "but not limited to"

Many commenters expressed concern about or questioned the meaning of the use of "but not limited to" in the previous draft and asked for it to be removed from the measures. The concern as the SDT understood it was that "but not limited to" could be used to request evidence beyond that which is specified in the measure even if the entity has otherwise provided what the measure describes. With respect to "but not limited to," the SDT specifically inserted that phrase to assist the Responsible Entity, particularly in light of technologies that may change. It is not intended to be used as a mechanism to request additional evidence beyond that which is required to demonstrate compliance. The SDT is concerned that removing "but not limited to" opens the same question (albeit in slightly different context) as the CIP Interpretation Drafting Team just answered with respect to the interpretation of CIP-002 (versions 1 through 4) for Duke Energy (NERC Standards Development Project 2010-INT-05). Namely, are the measures listed exhaustive/prescriptive or are they illustrative? By including a qualifier such as "but not limited to," as is common in statutory drafting and in other legal contexts, the SDT intends to signal that the measures are not exhaustive. It provides flexibility to the Responsible Entity on what is acceptable. For example and for purposes of illustration, if one said "evidence may include an orange, a lime, or a lemon," one could expect that perhaps only an orange, a lime, or a lemon would be appropriate. However, if one said, "evidence may include, but is not limited to, an orange, a lime, or a lemon," one could just as reliably expect that an orange, a lime, or a lemon would be appropriate, but it would also be reasonable that something not explicitly enumerated by the list, but similar in nature to items on the list, such as a tangerine, may also be acceptable. Importantly, that is not the same as additionally requiring a tangerine even though one already has an orange; however, that is the concern manifested in the comments. To address the commenters' concerns, however, the SDT has made a slight change in support of signaling in all measures that they are examples and that the list of examples is not exhaustive. The SDT believes that it is providing sufficient flexibility in this manner—and for the Responsible Entities' benefit—in clarifying that measures are not prescriptive lists while also attempting to allay fears that "but not limited to" will be used in a manner that expands the requirement. Rather than stating "Evidence may include, but is not limited to, . . ." the SDT has added the "example" concept to precede "evidence" (e.g., "**An example of** evidence may include, but is not limited to, . . ." or "**Examples of** evidence may include, but are not limited to, . . .").

Movement to focus on correcting deficiencies in certain requirements:
In response to several comments, the SDT has incorporated within CIP Version 5 a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. Note that, where used, the addition of language modifies "implement"; it does not itself require or specify internal controls, though it certainly enables their use for those entities that have adopted an internal controls or compliance management approach. Where used, the requirements incorporate the forward-looking language into the main requirement, which ties in with CIP Version 5's use of accompanying tables. It is presented in those requirements as follows:

> "Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** one or more documented processes (or program, etc., as specified by the requirement) that collectively include each of the applicable items in [the referenced table]."

The SDT also considered several alternatives and additions to this language. For example, some alternatives proposed modifying "process" (or program, etc.), while others suggested to add language specifying certain things that are not violations in addition to the requirement language. Many of the ideas or suggestions presented concepts that the team agrees with, but they are more appropriate for other aspects of monitoring compliance with the standards, not for inclusion within the standards themselves. Language indicating what is not a violation is more appropriate for compliance tools such as the RSAW. The SDT also notes that the VSLs will reflect this approach where the approach is used, and the SDT is actively working with NERC Compliance Operations to prepare the RSAWs for the CIP Version 5 standards. Furthermore, the SDT expects continued participation by industry in providing input into the RSAW development following approval of the standards, and the SDT notes that a draft RSAW for part of CIP-006-5 is posted for comment and for illustrative purposes.

The SDT is charged with writing straightforward requirements stating the desired behavior that will maximize reliability of the BES. The CIP requirements are written to require documented processes that must address the elements in the tables that accompany the requirements. These tables therefore set the parameters for the processes. There are no issues with documenting the processes – the entity must have the processes and they must have the parameters as outlined in the requirement tables.

The compliance concerns, especially those related to zero tolerance for deficiencies, is not related to the documenting of the processes, but in the implementation of the processes. The process should have numerous 'bright line' parameters that outline the goal the industry striving towards. A concern applies when implementing the processes in a world of tens of thousands of people and hundreds of

thousands of Cyber Assets. In certain cases, absolute perfection forever is not reasonable, even if it is desirable.

In light of the direction toward a risk-based approach to compliance monitoring by NERC, The CIP SDT had an opportunity to do to address this issue in certain requirements within the standards themselves. As described above, the SDT included a phrase to modify the verb 'implement' in several (but not all) of the requirements in CIP V5. Entities are to have the processes; the processes must meet the requirements in the tables; and the entities shall implement those processes in a manner that identifies, assesses, and corrects deficiencies.
The emphasis of the self-correcting language is on the implementation of the processes. The processes themselves cannot miss required parts or parameters as outlined in the tables.

Implementation Plan proposal to extend Version 3 until Version 5 remains unchanged in this draft
In light of the order approving the CIP Version 4 standards (FERC Order No. 761), several commenters asked about the drafting team's proposal in the implementation plan to extend Version 3 until the effective date of Version 5. The SDT's proposal, if approved—and its intent for Version 5 to supersede Version 4 and to extend the effectiveness of Version 3 until Version 5 goes into effect—remains unchanged.
In the implementation plan for the CIP Version 5 standards, the SDT has previously proposed to extend Version 3 until the effective date of Version 5. In doing so, the effective date proposes that Version 4 will be superseded by Version 5 and not go into effect. Even though Version 4 has been approved by order, the SDT always contemplated such approval during the development of the implementation plan language. That order does not change the SDT's proposal. The expectation that there would be an order in early to mid 2012 is why the SDT included language in the implementation plan's effective date to specify that the extension of Version 3 until Version 5, and that Version 4 would not go into effect, would occur "notwithstanding any order to the contrary." There is no change in the SDT's intent and proposal to extend Version 3 until Version 5, and for Version 5 to supersede Version 4, notwithstanding the recent order approving Version 4. The SDT also understands, as is the case for any standards proposal by the industry, that the proposal is subject to approval by regulatory authorities.

Stakeholders will notice that within the individual standards for CIP Version 5, the effective dates have been modified so that they are specific to the particular standard. In doing so, the reference to extending Version 3 and superseding Version 4 has been removed, as the Implementation Plan is the appropriate place for that language (where it remains, as described above). Thus, while there is no change to the SDT's proposal, the individual, standard-by-standard effective dates have been modified to comport with the style and form of other NERC Reliability Standards.

Annual v. 15 calendar months
Several commenters expressed dissatisfaction with the standards' use of the phrase ". . . at least once every calendar year, but not to exceed 15 calendar months . . ." for describing the required frequency

of performance on some requirements. Some entities expressed a desire to simply use "annual," while others suggested changing the "but" to an "or." The SDT has discussed alternative approaches and is using the term ". . . at least once every 15 months . . ." to provide reasonable flexibility to Responsible Entities while meeting the intent of the requirements. As explained in the global comment section of the response to comments for draft 2, simply using "once per calendar year" creates a potential for bi-annual bookending that the SDT does not intend. Similarly, the SDT understands that the use of both "calendar year" and "15 calendar months" was unnecessarily complicated. The SDT acknowledges that there is a CAN that addresses "annual," but that applies where the standard does not make clear what it means in its use of the term. In CIP Version 5, there is an opportunity and an obligation to unambiguously reference the periodic time parameter. Furthermore, one of the objectives of the SDT in Version 5 is to consider applicable CANs and use language that would no longer require a CAN to clarify an audit interpretation. Instead, the SDT used specific language to clarify a time parameter that approximates one year in time while also accounting for operational realities that make a 15 month parameter more reasonable. The term "annual" is no longer used in these CIP standards for periodic requirements, and, therefore, the CAN on the word "annual" can no longer apply.

TFE v. Per Cyber Asset Capability

Historically, phrases such as "where/when technically feasible" have been considered trigger language for requirements necessitating a technical feasibility exception ("TFE") in instances where a device could not meet the required parameter. The SDT has spent considerable time reviewing each use of TFE language in CIP Version 5 where it is necessary.

The SDT has also determined that there are some requirement parts that should not require a TFE, as certain parameters are not essential themselves, but should apply if a device is capable of the parameter. This is distinct from the reasoning for requirements with TFE language. In the latter requirements, a certain performance or parameter is required, regardless of technology, device, etc. By using "per (device/system) capability," the SDT does not intend that the specific parameter or performance is required regardless of capability, but only applicable on devices that have that capability. For example, proposed CIP-007-5, Requirement R4, Part 4.1 requires "Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents . . ." Here, the SDT does not intend to require event logging. However, if a Responsible Entity is using a device that can log events, it is required to enable event logging to the extent the device is capable.
The phrase "where technically feasible" indicates that the standard requires strict compliance without a TFE. As mentioned above, the drafting team does not intend for some requirements to be TFE-triggering. The underlying rationale for a TFE is that there is legacy equipment in place that is not readily compatible with a modern environment where cyber security issues are a concern.[2] Under such circumstances, the responsible entity must file a TFE that demonstrates strict compliance with an

[2] Order Approving Technical Feasibility Exception Procedures and Ordering Compliance Filing, Paragraph 3

applicable requirement is not technically possible and that there is an alternative course of action that will protect the reliability of the Bulk-Power System to an equal or greater degree than strict compliance.[3]

While a TFE requires an entity to show why strict compliance with an applicable requirement is not technically possible, "per device capability" clarifies that the requirement is only applicable to the devices for which compliance with a particular requirement is possible in the first instance. This provides reasonable flexibility to the industry while also retaining the TFE concept where necessary. Thus, the "per device capability" alternative reduces the need for TFEs and will be less onerous on entities. The SDT does not intend to eliminate TFEs altogether, but proposes to use the "per device capability" as an alternative that is effective in protecting the reliability of the Bulk-Power System.

VSLs

In previous drafts of the Version 5 CIP Cyber Security Standards, VSLs were posted concurrent with each standard. For this posting, the VSLs are presented in one document. They will continue to be prepared for posting for non-binding poll during the recirculation ballot. The VSLs should not be a basis for a ballot determination, and the SDT will continue to refine them as necessary.

Applicability Section of the standards (Introduction - Section 4 – Applicability)

There were several comments about the Applicability section of the standards in various comments related to specific standards. The SDT has reviewed those suggestions and made several changes to the applicability sections of each standard.

Several commenters stated that in part 4.2 of section 4, the criteria for qualified Distribution Providers and Load Serving Entities for UVLS/UFLS systems remain unclear. Specifically, the language was not clear on whether the 300 MW of load referred to the DPs and LSEs' share or to the total load shed. In addition, they also noted that the language for Transmission Protection systems is unclear and needs clarification to more precisely describe the protection systems that are in scope. They also suggested that these should be moved to Low Impact because there is no justification for small entities to be subjected to the requirements for Low and Medium entities. The SDT has proposed modified language to clarify the qualifications for UFLS and UVLS systems that specifies that they are those UFLS or UVLS systems that are part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard and that perform automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. With regard to the impact classification, the SDT believes that because of the function that UVLS and UFLS systems play in last ditch efforts to stabilize the BES, the 300 MW threshold provides a measure of impact that justifies the classification as medium impact systems: lower impact systems have already been removed from the scope and are not subject to these standards.

[3] Id, Paragraphs 5 and 8

Many references in the applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

Several comments indicated that LSEs should not be included in section 4 since the NERC Functional Model does not include any tasks related to the implementation and operation of load shedding systems. The SDT reviewed the LSEs tasks in the NERC Functional Model and has removed LSEs from the applicability of the CIP standards.

Several commenters suggested that the following language be added to the end of the criterion for Protection Systems: "and where the Protection System is connected to a supervisory control system providing remote operation capability." The SDT has reviewed the proposed addition to section 4.2.2 for Protection Systems and does not believe that the additional language to restrict the scope to only those Protection Systems that are remotely operated is intended or justified in the scope of section 4.2.2. The SDT notes that the proposed addition makes the assumption that all cyber vulnerabilities are based on remote operation capability. This would provide an incomplete mitigation for cyber threats that do not rely on remote operation for execution.

Several commenters stated that the inclusion of the glossary term "Systems" does not apply to DPs as used in section 4.2.2. One comment also pointed out that this is true in many other places where the term is used, while others' comments pointed out inconsistencies in the use of the term. The SDT notes that the terms Facilities, systems and equipment is always used in combination in the context of this application. The SDT has considered the intent of the terms in its uses and agrees that the glossary term "Systems" does not reflect the intent, and the SDT has made those changes where appropriate. In addition, the SDT believes that the issue is relieved with the changes made to refer to "assets" when referring to a group of Facilities, systems or equipment at a given location.

One comment stated that the statement at the beginning of the guideline and technical basis section that refers to applicability to DPs that refer to EOP-005 should be deleted since section 4.2.2 scopes more than EOP-005. In response, the SDT notes that the paragraph also includes reference to the registration criteria, in addition to EOP-005. The SDT believes the reference is appropriate.

One comment noted that in section 4, part 4.2.2, all single points of failure in the cranking paths should be protected and that where the Blackstart Resource is outside of the Responsible Entity's ownership, that the part of the cranking path that is the injection point to the cranking path to the unit to be

started should be specified. The SDT notes that Section 4.2.2 is not the criterion for determining the protection of the cranking path, but rather defines which part of a DPs equipment is in scope.

One comment suggested additional qualification in section 4 to ensure that the exemption section covers all facilities covered under a cyber security plan under the Nuclear Regulatory Commission (NRC) regulations. The SDT agrees with the clarification and has included the suggestion in the language in section 4 that covers nuclear facilities. The language has been added to section 4.2.4.3 to read: "In nuclear plants, the Systems, structures, and components that are regulated by the NRC under a cyber security plan pursuant to 10 C.F.R. Section 73.54."

One comment discussed the use of the phrase "required by a NERC standard" in section 4 and instances of affected Facilities, systems and equipment where there is no requirement to implement them by a NERC standard. The SDT agrees with the discussion and has made modifications to the language to more accurately reflect the intent.

One comment stated that section 4.2.4.2 attempts to define exemptions for communication links, but fails to include the exclusion of end points to those circuits (see CIP-005/R1.3). The SDT notes that end-points of circuits that are access points are included by the definition of Electronic Access Points (i.e. they are not "between" ESPs).

Reason for CIP Version 5

Some commenters inquired in their comments why CIP Version 5 was necessary, or they expressed a preference to continue under existing versions of the CIP Standards. To facilitate understanding of the reasons for Version 5 as part of the obligation to address the remaining directives in FERC Order No. 706, the SDT offers the following explanation and review of the previous versions of the NERC CIP Reliability Standards.

The NERC Board of Trustees adopted the first version of the CIP Reliability Standards on May 2, 2006. On August 28, 2006, NERC submitted to FERC for approval the Version 1 CIP Reliability Standards. On January 18, 2008, FERC issued its Order No. 706. In this order, FERC approved the Version 1 CIP Reliability Standards and issued more than 100 directives to NERC that included modifying the standards. An SDT began a phased-in approach to respond to the directives in FERC Order No. 706. As part of that phased-in approach, the SDT addressed the directives in the order that it could respond to quickly, and it developed a plan to address the remaining directives.

Version 2 of the CIP Reliability Standards was adopted by the NERC Board of Trustees on May 6, 2009. On May 22, 2009, NERC submitted to FERC for approval the Version 2 CIP Reliability Standards. On September 30, 2009 FERC issued its Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing. In this Order FERC approved the Version 2 CIP Reliability Standards and issued four additional directives to NERC that included modifying the

standards, with a required response in 90 days. At that time the SDT had to abandon it plan for addressing the outstanding directives in Order No. 706 and had to immediately address the newly issued directives.

Version 3 of the CIP Reliability Standards was adopted by the NERC Board of Trustees on December 16, 2009. On December 29, 2009, NERC submitted to FERC for approval the Version 3 CIP Reliability Standards. On March 31, 2010 FERC issued its Order on Compliance. In this Order FERC approved the Version 3 CIP Reliability Standards.

Version 4 of the CIP Reliability Standards (CIP-002-4 through CIP-009-4) was developed as an interim step to address the more immediate concerns from FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period. The Commission approved Version 4 on April 18, 2012.

Work has continued on further improvements to the standards, including responses to the remaining Commission directives from FERC Order No. 706, and it is these further enhanced standards that will be submitted to the Commission as Version 5. The next version of the CIP Reliability Standards will build on the Version 4 standards' establishment of uniform criteria for the identification of Critical Assets.

Version 5 of the CIP Reliability Standards provides a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

The changes in Version 5 also present many strategic advantages. Chiefly, a significant deliverable is to close out FERC Order No. 706. More importantly, Version 5 aligns to essential reliability functions and provides significant flexibility to entities in adapting requirements to individual operations.

Version 5 represents a systems-based approach to standards, which provides an opportunity to implement solutions and tailor security based on function, connectivity, risk, and impact. That flexibility represents a significant transition from the "in or out" demarcation for applying requirements in Versions 1 through 4 of the standards, as the drafting team has been able to structure Version 5 in a way that more finely tunes the applicability of each requirement based on connectivity, impact, and other characteristics.

Version 5 is also an experience-based set of standards. It is the first opportunity for the industry to evaluate, consider and incorporate lessons learned from implementation and audit of Versions 1 through 3, and the requirements aim to provide clearer emphasis on the required results. Collectively, the Version 5 standards support continued improvement in support of protecting against compromises that could lead to misoperation or instability in the Bulk Electric System.

NERC Quality Review

In addition to the changes that were made in response to comments, the SDT also submitted the set of standards to NERC for a quality review (QR). In response to the QR, the SDT made several changes for clarity, most of which related to style and form, grammar, word choice, etc.

The Applicability section was modified in response to QR to add "Interchange Authority" to the list of functional entities. The NERC Functional Model lists "Interchange Coordinator" while the registration criteria list "Interchange Authority," and they are not yet synchronized. Until that occurs, the SDT specifies that the standards apply to "Interchange Coordinator or Interchange Authority."
The SDT removed CIP-004-5, Requirement R4, Part R4.2. In previous drafts of the CIP standards (which was Requirement R6), the standard required designation of "one or more individuals" to authorize access, followed by a second requirement part for that individual to authorize based on need. The SDT has determined that the designation of one or more individuals is administrative in nature and is something that should be addressed by the Responsible Entity's plan, not by a requirement part. The performance required is now addressed through one requirement part.

The SDT also removed CIP-006, Requirement R3, Part R3.2, which required that Responsible Entities document outages for physical access control, logging, and alerting systems and retain the outage records for at least 12 calendar months. This requirement was a documentation requirement, and the SDT, in adding the modifying language to "identify, assess, and correct deficiencies" to Requirement R1, determined that the documentation requirement to log outages was not necessary.

Index to Questions, Comments, and Responses

Summary Consideration, Explanation, and Common Responses to Global Changes and to Issues and Comments Frequently Repeated 2

Questions with Summaries Included: 26

QUESTION A3 – CIP-002-5: 26

QUESTION A10 – CIP-003-5: 40

Questions with Votes Only: 44

1. Requirement R1 of draft CIP-002-5 requires the identification of high and medium impact BES Cyber Systems as described in Attachment 1. Further, it requires a Responsible Entity to review (and update as needed), the required identification within 60 calendar days of when a change to BES Elements or Facilities is placed into operation, which is planned to be in service for more than 6 calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category. Do you agree with the proposed Requirement R1? 44

2. Requirement R2 of draft CIP-002-5 states, "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once each calendar year, not to exceed 15 calendar months between approvals, even if it has no identified items in Requirement R1, Parts 1.1, 1.2, or 1.3." Do you agree with the proposed Requirement R2? 52

4. CIP-003-5 R1 states "Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall implement one or more documented cyber security policies that address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R1? 61

5. CIP-003-5 R2 states "Each Responsible Entity for its BES Cyber Systems not identified as high impact or medium impact shall implement one or more documented cyber security policies to address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2? 69

6. CIP-003-5 R3 states "Each Responsible Entity shall identify a CIP Senior Manager by name." Do you agree with the proposed Requirement R3? 77

7. CIP-003-5 R4 states "Each Responsible Entity shall review and obtain CIP Senior Manager approval for cyber security policies identified in Requirements R1 and R2, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals." Do you agree with the proposed Requirement R4? 85

8. CIP-003-5 R5 states "Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate and the date of the delegation, and approved by the CIP Senior Manager." Do you agree with the proposed Requirement R5? 93

9. CIP-003-5 R6 states "Each Responsible Entity shall document any changes to the CIP Senior Manager or any delegations within thirty calendar days of the change. Delegation changes do not need to be reinstated with a change to the delegator." Do you agree with the proposed Requirement R5? 101

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Bruce Metruck	New York Power Authority	NPCC	6
12.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
13.	Robert Pellegrini	The United Illuminating Company	NPCC	1
14.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
15.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
16.	Brian Robinson	Utility Services	NPCC	8
17.	Michael Jones	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Don Weaver	New Brunswick System Operator	NPCC	2
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3
24.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5

2.	Group	Annabelle Lee	NESCOR/NESCO									

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3.	Group	Jason Marshall	ACES Power Marketing					X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Tim Soles	Occidental Power Services, Inc.	ERCOT 3										
4.	Andy Gallo	Austin Energy	ERCOT 1										
5.	Andy Gallo	Austin Energy	ERCOT 3										
6.	Andy Gallo	Austin Energy	ERCOT 4										
7.	Andy Gallo	Austin Energy	ERCOT 5										
8.	Andy Gallo	Austin Energy	ERCOT 6										
8.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8. Annie Terracciano	Northern Lights Inc.	WECC 3										
9. Aleka Scott	PNGC	WECC 4										
10. Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11. Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12. Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13. Margaret Ryan	PNGC	WECC 8										
12. Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13. Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14. Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3. M & A Electric Power Cooperative			SERC 1, 3										
4. Northeast Missouri Electric Power Cooperative			SERC 1, 3										
5. N.W. Electric Power Cooperative, Inc.			SERC 1, 3										
6. Sho-Me Power Electric Cooperative			SERC 1, 3										
15.	Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X						
Additional Member		Additional Organization	Region Segment Selection										
1. Oglethorpe Power Corporation			SERC 5										
2. Georgia Transmission Corporation			SERC 1										
16.	Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X
Additional Member		Additional Organization	Region Segment Selection										
1. MAHMOOD SAFI		OPPD	MRO 1, 3, 5, 6										
2. CHUCK LAWERENCE		ATC	MRO 1										
3. TOM WEBB		WPS	MRO 3, 4, 5, 6										
4. JODI JENSON		WAPA	MRO 1, 6										
5. KEN GOLDSMITH		ALTW	MRO 4										
6. DAVE RUDOLPH		BEPC	MRO 1, 3, 5, 6										
7. JOE DEPOORTER		MGE	MRO 3, 4, 5, 6										
8. SCOTT NICKELS		RPU	MRO 4										
9. TERRY HARBOUR		MEC	MRO 1, 3, 5, 6										
10. MARIE KNOX		MISO	MRO 2										
11. LEE KITTELSON		OTP	MRO 1, 3, 4, 5										
12. SCOTT BOS		MPW	MRO 6, 1, 3, 5										
13. TONY EDDLEMAN		NPPD	MRO 1, 3, 5										
14. THERESA ALLARD		MPC	MRO 1, 3, 5, 6										
17.	Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing													
18.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				
Additional Member		Additional Organization	Region Segment Selection										
1. Timothy Beyrle		City of New Smyrna Beach	FRCC 4										
2. James Howard		Lakeland Electric	FRCC 3										

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. Greg Woessner	Kissimmee Utility Authority	FRCC 3										
4. Lynne Mila	City of Clewiston	FRCC 3										
5. Joe Stonecipher	Beaches Energy Services	FRCC 1										
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC 4										
7. Randy Hahn	Ocala Utility Services	FRCC 3										
19. Group	Joseph DePoorter	Madison Gas and Electric Company			X	X	X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Darl Shimko	MGE	MRO 3										
2. Joseph DePoorter	MGE	MRO 4										
3. Steve Schultz	MGE	MRO 5										
4. Jeff Keebler	MGE	MRO 6										
20. Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							
Additional Member	Additional Organization	Region Segment Selection										
1. Mark Jones	Pepco	RFC 1										
21. Group	Rick Terrill	Luminant					X					
Additional Member	Additional Organization	Region Segment Selection										
1. Mike Laney	Luminant Generation Company LLC	ERCOT 5										
2. Tim Soles	Occidental Power Services, Inc.	ERCOT 6										
3. Tim Soles	Occidental Power Services, Inc.	ERCOT 3										
4. Andy Gallo	Austin Energy	ERCOT 1										
5. Andy Gallo	Austin Energy	ERCOT 3										
6. Andy Gallo	Austin Energy	ERCOT 4										
7. Andy Gallo	Austin Energy	ERCOT 5										
8. Andy Gallo	Austin Energy	ERCOT 6										
9. Brenda Hampton	Luminant Energy Company LLC											
22. Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Kevin Smith	BANC	WECC 1										
23. Group	Scott Brame	NCEMC	X				X					
Additional Member	Additional Organization	Region Segment Selection										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Rayburn Country Electric Cooperative			SPP										
2. Empire District Electric			SPP	1									
3. City Utilities of Springfield			SPP	4									
4. Westar Energy			SPP	1, 3, 5, 6									
5. Cleco Power			SPP	1, 3, 5, 6									
25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Pawel Krupa			WECC	1									
2. Dana Wheelock			WECC	3									
3. Hao Li			WECC	4									
27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Denise Lietz		Puget Sound Energy	WECC	1									
2. Erin Apperson		Puget Sound Energy	WECC	3									
28.	Group	Michael Mertz	PNM Resources	X		X							
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Laurie Williams		Public Service Co. of New Mexico	WECC	1									
2. Michael Mertz		Public Service Co. of New Mexico	WECC	3									
29.	Group	Sasa Maljukan	Hydro One	X									
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. David Kiguel		Hydro One	NPCC	1									
30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION A3 – CIP-002-5:

If you disagree with the changes made to CIP-002-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to attachment 1 and provided clarity to the requirements and associated rationales and measures. The explanations below describe the modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity in language.

Introduction - Section 4 – Applicability

There were several comments on this section in response to question A3, but the issues and responses relate generally to all of the standards. The discussion and response to comments on this section is provided earlier in this document in the Summary Consideration, Explanation, and Common Responses to Global Changes and to Issues and Comments Frequently Repeated section.

Requirement R1

Substantial changes were made to both the structure and the approach in Requirement R1: while the end result is a categorized list of high and medium impact BES Cyber Systems, there were many changes made to address concerns related to Low Impact assets and an asset based approach to deriving BES Cyber Systems. Many comments suggested a more prescriptive approach to the methodology used to arrive at the objective lists, including suggestions to add a flow-chart to the requirement: the SDT made a number of changes to address the "what" instead of the "how", and added substantive qualifications to better define the assets affected.

In particular, several commenters stated that the requirement to review and update the categorization on every change to the BES was an onerous burden in a company with a large number of constantly changing BES Facility configuration. The SDT has reviewed comments and is persuaded by the arguments presented. The SDT also considers that an annual review and update for BES Facilities, given the long term implementation of BES Facility changes, together with the requirements for BES Cyber Systems change control, provide a framework that provides the controls necessary.

Several commenters stated that the requirements for identification in Requirement R1 of CIP-002-5 be modified to require reference to “BES Sites” rather than Facilities, systems and equipment. One comment also suggested that inventories for Low Impact would allow requirements for low impact to be at the site level. Many comments suggested a Facilities impact-based approach to the derivation of the impact of BES Cyber Systems. The SDT has considered the suggestion and made modifications to the current CIP-002-5 requirements to incorporate the concepts using language already used in the criteria and Version 4 approved standards. While the terms Facilities, systems and equipment are precisely the same terms used in the definition of Critical Assets in prior versions, the SDT has made modifications to the proposed language to use the term “assets”, a term familiar to the industry in compliance activities for prior versions.

In response to numerous comments on the issue of asset-based derivation of cyber system impact, the SDT made substantive changes to Requirement R1s language and structure to include this approach. While Requirement R1 is ultimately intended to result in categorized BES Cyber Systems for the application of cyber security requirements, the SDT has made changes to the language and contents of Requirement R1 as well as the criteria in attachment 1 in consideration of comments received.

Several commenters commented on the use of the capitalized term Bulk Power in the rationale for Requirement R1. The paragraph has been deleted and the term is no longer used in the rationale.

One commenter suggested that a bullet is not required in requirement part 1.3 of Requirement R1. The comment also suggested an inconsistency between Requirement R1 and the associated VSL. The SDT has redrafted Requirement R1 in consideration of comments and the bulleted clause is now in the applicable part of the requirement. The inconsistency in the VSL has been corrected.

One commenter suggested that the SDT continues to insist there is no need to identify the low impact BES Cyber Systems and their associated Cyber Assets (e.g., R1.3) and that this causes an auditability issue. The SDT believes that an “asset” based approach in the revised draft and the requirement for the list of assets containing Low Impact BES Cyber Systems provides relief to the auditing issue.

Several commenters requested an explanation of the values used in the VSLs for Requirement R1. The SDT notes that the values are based on FERC Guidelines for VSLs that use percentages. Many entities commented on the need for absolute values for smaller entities since percentages would provide an unfair bias for small entities that would more easily reach percent based thresholds.

One comment stated that the SDT should consider reusing lists generated by other standards. The SDT notes that evidence used for other reliability standards can be presented for these CIP standards as long as they provide the evidence required to demonstrate compliance to the CIP requirement.

One commenter suggested that requirement parts 1.1, 1.2 and 1.3 should also include documentation as part of the requirement and that requirement part 1.4 should require the update prior to commissioning. The SDT's approach to requirement definition focuses on results and believes that a requirement to "document" does not directly result in the reliable operation of the BES. The SDT has defined the required functional result that directly contributes to the reliable operation of the BES. Requirement R1.4 has been removed by SDT in consideration of comments received.

One commenter suggested that by specifying requirements for Low Impact, CIP-002-5 implies a list of BES Cyber Systems. The commenter further suggested either requiring a list of Low Impact Cyber Systems or removing Low Impact altogether. The SDT notes that requirements must be explicit and that CIP-002-5 has made it clear and explicit that a list of Low Impact BES Cyber Systems is not required. However, in the new draft, a list of Low Impact assets is required to facilitate the application of policy requirements to Low Impact assets.

Several commenters suggested many editorial changes to the language used in Requirement R1. The SDT has made fundamental structural and language changes to Requirement R1 to address comments received.

Requirement R2

One commenter suggested that the rationale for Requirement R2 does not include approval of the lists. The SDT notes that the last sentence in the rationale refers to the approval process.

One commenter made many remarks on inconsistencies between the Requirement R2 language, the measure and the VSLs. The SDT has made modifications to R2 and its measures and VSLs for consistency.

Many commenters suggested alternative language, or reverting to the use of the term annual for the clause describing the annual review and approval. One commenter also inquired as to whether the clause supersedes an entity's definition of annual. The SDT has discussed alternative approaches and is using the term "at least once every 15 months" to provide reasonable flexibility to Responsible Entities while meeting the intent of the requirements. The SDT has intentionally not used the word "annual". This term is no longer used in these CIP standards for periodic requirements

and therefore, the CAN on the word annual can no longer apply in this requirement. One of the objectives of the SDT in Version 5 is to consider applicable CANs and use language that would no longer require a CAN to clarify audit interpretation. Instead, the SDT used specific language that implements its intent. This topic is also discussed in greater detail in the introductory, global section of these comment responses.

Attachment 1

Section 1 - High Impact Control Centers

One commenter stated that criteria for control centers fail to consider inter-Control Center connectivity and that the concept of mutual distrust does not work because of trusted paths. The SDT has included consideration of connectivity in the application of requirements. The applicability of mutual distrust depends on specific considerations of network configuration. A blanket statement based on an assumed configuration does not support the generalized comment. The SDT believes that requirements in the standards for protection of BES Cyber Systems provide a basis for Responsible Entities to implement the necessary protection in their network and system design.

Several commenters stated that the introductory text in High and Medium Impact criteria should be deleted or modified due to the change in approach for facilities based impact. The SDT notes that Requirement R1 still requires, ultimately, the categorization of BES Cyber Systems for the application of requirements. The SDT believes that the introductory text in the criteria for High and Medium is still required to express this result.

One commenter suggested on the inclusion of “associated data centers” in the control center criteria and argued that the BES Cyber Systems in these “data centers” would already be included. The SDT has made revisions to the definition of Control Centers, has now included data centers in the definition, and removed the phrase from attachment 1.

Many comments were received on the relationship of TO Control Centers and the functional obligations of TOPs. There was also a comment on the section in the guidance that pertains to TO Control Centers that perform the functional obligations of the TOP. In particular, one comment suggested removal of the guidance, citing ownership issues and issues with NERC Functional Entity registration. The SDT believes that the criterion in question is used to determine the impact of the BES Cyber Systems, and that, irrespective of registration issues, if these Cyber Systems perform a function that is relevant to the functional obligation of a TOP, and that this is formally delegated, then the impact should be appropriately assessed as such. The issue of ownership is a non-issue since the responsibility for compliance to the applicable requirements resides with the owner of the identified BES Cyber Systems that provide that function.

Several commenters suggested that the language used in criterion 1.3 with respect to TOP Control Centers needed clarification and that the guidance for this criterion should explicitly say that TO Control Centers that do not perform the functional obligation of the TOP should be classified as Medium. The SDT has inserted additional guidance to clarify this point. A TO facility that does not perform or does not have an obligation to perform any of the reliability tasks of a BA, TOP or GOP does not meet the definition of a Control Center and the BES Cyber Systems should be evaluated according to the criteria in attachment 1. TOs should review the functional tasks of a TOP and those of a TO and ensure they are not delegated any of these functional tasks through an agreement or a contract. In particular, TOs should note that the functional model does not list real-time operational tasks for that entity.

One commenter asked whether a TO Control Center that performs an operation under the direction of a TOP is performing a functional obligation of a TOP. The NERC Functional Model does not include operation of BES Facilities under the tasks or obligations of a TO, but does include them under the obligations of a TOP. If the TO has an obligation (contractually or because of some other formal agreement) to operate BES assets, whether it is in an emergency or in normal operational circumstances, under the direction of a TOP, then that Cyber System is used to perform the functional obligation of a TOP. The functional obligation of operational control of the BES asset has been delegated to the TO.

One commenter also asked whether a TO data center that collects data and then processes that data for transmission to the TOP is performing a functional obligation of the TOP. The SDT has moved the data center association to the definition of a Control Center and associates it with the facility hosting the operating personnel. In the scenario described, the TO data center is not associated with the BES Cyber Systems owned by the TOP. The “data center” described is analogous to field data aggregating facilities and are evaluated as BES Cyber Systems necessary for providing situation awareness for real-time operations, and should not be evaluated as TOP Control Center “data centers”.

One commenter suggested a number of modifications to the criteria aimed at better stratifying the distinction of Medium from High Impact, especially in the case of BA and TOP Control Centers. The SDT considered the suggestions and has made a number of modifications to address the comments. On another suggestion of increasing the threshold for High Impact BA and GOP Control Centers to 3000 MW, the SDT notes that the stratification of the High Impact from Medium Impact is mostly based on impact due to the wide area reliability tasks of the Functional Entities. However, the SDT has included modifications that provide some stratification of the levels for BA, TOP and GOP Control Centers which are consistent with thresholds approved in Version 4. On the subject of UFLS thresholds, the SDT reviewed recent developments in Regional Standards for UFLS and the tolerances specified in these standards as a basis for evaluation of

the current threshold: the SDT concluded that the current threshold represents a reasonable representation of the level of tolerance in these standards so far.

Several commenters suggested that Control Centers that use voice or manual instructions be categorized as Low Impact. The SDT notes that Cyber Systems that provide information to Control Center operators that use manual or voice to effect control operations on BES assets in real-time based on that information must be subject to the same protection as those that trigger automated operation. If the communication or manual operation results from information provided for real-time operations, there is no rationale for categorizing them as a lower impact.

One commenter suggested that the word "control" in the definition of Control Center requires more explanation and that the situation awareness section of the guidelines on BES Reliability Operating Services could include cyber systems used in collecting data for management and engineering analysis. The SDT has provided, in the guideline, the type of operations included in the use of the word. The definition provides further qualification in the context of the Control Center. The word "control" is used in several other standards and is a well understood concept in the BES environment. The intent of the situation awareness section in the guideline on BES Reliability Operating Services is to broadly define a reliability function and is not meant to be used solely for the qualification of applicable BES Cyber Systems: it is intended to be a first step in qualifying a population of Cyber Systems for further application of additional qualifications in the definition of BES Cyber Systems, applicable assets and the impact criteria in attachment 1.

One commenter stated that criteria 1.2 and 1.4 in attachment 1 qualify assets affected as "generation assets" and pointed out that not all assets in scope are strictly "generation assets". The SDT agrees and has made the suggested modification.

One commenter requested clarification on whether the 1500 MW in requirement parts 1.2 and 1.4 of attachment 1 referred to criterion 2.1. The SDT responds that the 1500 MW refers to total aggregate generation of 1500 MW, and is not tied to criterion 2.1.

Section 2 - Medium Impact

Several commenters stated that the 15 minute criterion in requirement part 2.1 of attachment 1 is unnecessary and redundant. Another commenter stated that this 15 minute clause was contrary to the "bright-line" concept. One commenter also stated that the inclusion of the 15 minute qualification in the criteria was inappropriate because the criteria define BES asset impact. The addition of this qualification resulted from previous comments and sought to

provide clarity in the scope of BES Cyber Systems to be included in consideration of this criterion. Where the qualification is included, the language makes it clear that it applies to the effect of the BES Cyber System.

There was a comment that the 15 minute in criterion 2.1 and 2.2 is going to be difficult to prove in an audit and suggested the term "that operate the reactive resource" instead in 2.2. As stated in the guideline, the intent of the 15 minute is to provide a boundary to the impact to real-time operations. The alternative use of the term "real-time" does not provide a useful defined term. The SDT believes that the commenter's suggestion to use the term "that operate" in criterion 2.2 restricts the full scope of cyber systems that affect the real-time operation of the BES for reactive resources.

The commenter further suggested that criterion 2.1 should consider regional operational conditions and requested clarification on the 1000 MVAR threshold for 2.2. For 2.1, the SDT considered regional variations in determining this threshold and notes that this is the approved Version 4 criterion. For 2.2, the SDT consulted with operational and planning experts during the development of this criterion in Version 4.

One commenter stated that the commas around the words "as necessary" in criterion 2.3 were confusing. The SDT has reviewed the criterion and agrees that the commas are misplaced and have altered the intent of the criterion. The SDT has made changes to the placement of the commas to clarify the intent.

One commenter requested clarification on the use of the phrase "long term planning horizon" in criterion 2.3. The SDT notes that criterion 2.3 of attachment 1 does not use the phrase "long term planning horizon" but uses a specified one year or more near-term timeframe. The SDT notes the intent is to avoid the identification of generation facilities that could be used to remediate short term reliability issues.

Two commenters requested additional clarification in the notifications to asset owners in criteria 2.3 and 2.6. For 2.3, the notification is affected as part of the execution of a contract. For 2.6, the applicable IROL reliability standards require that the asset owners be notified. These standards do not specify how the notification is to be done, but that notification must be performed.

One commenter suggested that in requirement part 2.2 of attachment 1, the nameplate value should be qualified to account for ranges. The SDT has included a qualification of "maximum" in the criterion.

One commenter stated that criterion 2.3 references the long term planning horizon, contrary to the real-time operations aspect of the CIP standards. In addition, the commenter suggested that additional guidance be provided as to the notification of such obligations. Also, the commenter requested similar clarification in the guideline for criterion 2.8. The SDT points out that the criterion states that the designation of the asset is performed as part of a planning activity that has a time horizon of one year or more (near-term) by the Planning Coordinator or Transmission Planner, but the impact of a compromise of an affected BES Cyber System would meet the qualification for real-time operations. Additional clarification on notifications has been added to the guideline for criteria 2.3 and 2.8.

One commenter stated that the guidance section that refers to the category D contingency of TPL standards in the discussion of criterion 2.3 is unlikely and suggests removing it. The SDT has removed the reference in the guideline.

One commenter suggested using the phrase “generation interconnection facility” instead of “Transmission Facilities providing the generation interconnection required to connect generator output to the Transmission Systems Transmission Facilities” in criterion 2.8, citing the term used in Project 2010-07. Another commenter suggested on the exclusion of generation plant collector buses in criterion 2.4 and 2.5 in the guidance and suggested an explicit exclusion in the requirement. The SDT reviewed the standards in Project 2010-07 and has not found “generation interconnection facility” as a defined term in the NERC Glossary. The term is however used in the PRC standard in the project. The SDT intends that the application of this criterion to Transmission Owner/Transmission Operator owned and generator owned Transmission Facilities that provide this interconnection of generator output to the Transmission system. However, for clarity and to address the exclusion of these facilities in criteria 2.4 and 2.5 that one comment stated, the SDT has added this term as an inclusion in 2.8.

One commenter suggested alternative language for criterion 2.5 to clarify the application of the aggregate rating. The SDT made modifications to the language in 2.5 to clarify the application of the aggregate to the sum of applicable Transmission facilities at the station.

Many commenters suggested using, for criterion 2.6, the same language used in criteria 2.8 and 2.9. The SDT notes that in criterion 2.6, the criterion refers directly to the Facilities that make up the IROL and has used the exact language used in the IROL standards that require the identification of these specific Facilities. Criteria 2.8 and 2.9 apply to Facilities that could indirectly cause a violation or reduction of the IROLs.

Several comments were on the reasons for the removal of the WECC specific qualifications for those criteria that are based on IROLs. The SDT understands that the commenter has reconsidered its position on IROLs and that other changes in attachment 1 negate the need for any WECC specific qualification.

Several commenters requested information on the standards that require notification of asset owners for IROLs in criterion 2.6. One commenter also stated that the term Control Center is not a NERC defined term and to organize the guidelines by transmission, generation, etc. The SDT notes that the guidelines for criterion 2.6 provides information on the NERC Reliability Standard that contains these requirements (FAC-014) that require identification of these assets and notification to applicable owning Functional Entities. The term Control Center is a proposed defined term in this CIP standards package and the guidelines for criteria are organized by generation and transmission.

One commenter inquired as to why all facilities necessary for the NIPR (not just Transmission Facilities) are not included in criterion 2.7 (Nuclear Interface facilities). The SDT notes that the scope of applicability in NUC-001 is limited to transmission entities listed, which consists of registered entities.

One commenter requested clarification in the application guideline on how, in criterion 2.8, the TO would obtain information on whether generation it does not own or operate meets criterion 2.3. The SDT included additional guidance in the application guideline section.

One commenter stated that the UVLS/UFLS in criterion 2.10 that refers to the 300 MW threshold should specify the lowest rating in the last 12 months. Several commenters stated that the use of the highest MW rating in the guidelines and technical basis on UVLS/UFLS should be changed to “hourly integrated load”. The SDT has not specified the methodology used to determine the 300 MW and has deferred to the requirements of the applicable regional UFLS/UVLS standards.

One commenter stated that criterion 2.10 might imply that individual unconnected relays in a load shedding program under a common trip point would be included and suggested excluding these. The SDT believes that the qualification of a common control system addresses this concern and believes that the exclusion language has the unintended consequence of excluding individual relays irrespective of their impact.

One commenter stated that the language in criterion 2.10 which specifies “regional load shedding programs” is problematic since there is no such requirement and pointed out that PRC standards place the responsibility for

establishing UFLS programs on the Planning Coordinator. The SDT has made modifications to section 4 that pertains to load shedding and criterion 2.10 to more accurately reflect the requirements of the PRC standards.

There was a comment that for criterion 2.10, the language suggests that any compromised component that make up SPS, RAS or automated switching system is required to be protected regardless of if it has an effect on the IROL or not. The SDT notes that the current language does not imply this requirement. The current language only applies if the compromise, whether of one or more components of the SPS, RAS or automated switching system, would cause a violation of one or more IROLs or "cause a reduction of one or more IROLs".

One commenter suggested setting a threshold for Special Protection Systems for applicability of these CIP standards. The SDT notes that all Special Protection Systems, irrespective of any threshold, are designated as Critical Assets under Version 4. The SDT notes that this has been the case because of the critical function provided by Special Protection Systems in the reliable operation of the BES.

Numerous commenters stated that in part 2.11 of attachment 1, the threshold for generation Control Centers should be changed to 1500 MW for consistency with the generation threshold in other criteria in Medium Impact. One commenter also pointed out an inconsistent term in the flow chart in the guidelines and technical basis section. In the same area, another commenter commented that part 2.11 should be removed and that the specific hydro situation should be handled in the definition. The SDT's intent in 2.11 is to include as Medium all the remaining Control Centers not already classified as High, because of the functions provided by Control Centers. In defining a 300 MW threshold for generation Control Centers in 2.11, the SDT was attempting to address a situation specific to hydro-electric generation Facilities. The SDT has removed this artificial threshold in view of changes made to this criterion. Further, the SDT made modifications in the threshold in the criterion for generation Control Centers to address these comments. The inconsistency of terms used in the flowchart has been corrected.

Several entities commented on the removal in draft two of criteria for restoration resources (blackstart units and cranking paths) from the Medium category. Some were in favor of this removal while others were not. Specifically, one commenter made several comments regarding generation and cranking path restoration resources. One comment read that restoration resources should be rated as Medium Impact. In contrast, another commenter suggested that restoration resources should not be included in the scope of the application of the CIP standards because of the absence of the need for remote data communication in the event of a restoration and the exclusion of cranking path from the definition of the BES. In response, in addition to the justification provided as part of the draft two materials, the SDT has

further considered industry input and comments in the consideration of these criteria with respect to their effect on overall reliable operation of the BES and has now removed them from High or Medium Impact criteria. In response, the SDT notes that the assumption that remote access through data communications is necessary for the realization of cyber security threats represents an incomplete mitigation approach, and that the CIP standards are aimed at protecting cyber systems that would impact the real-time operation of the BES, not solely those that directly operate elements of the BES. NERC Reliability Standards that govern the operation of load shedding programs and the protection of the BES elements are other examples of such approaches.

Section 3 – Low Impact

One commenter noted that the criteria in section 3 of attachment 1 should include the phrase "not included in high or medium". The SDT has made the necessary clarification.

General Comments

One commenter suggested that the footnote regarding the effective date of Version 5 and the effective date of Version 4 should be moved to the main text of the effective date. The SDT considered moving this footnote, but believes that movement of the footnote could cause unnecessary confusion, since the effect would not be different. The footnote simply clarifies the effective language that Version 4 does not go into effect and is superseded by Version 5.

There was a comment that the varying language regarding the phrase "destroyed, degraded, or otherwise rendered unavailable" and its variations needs to be consistent. In addition, Southern Company provided additional clarification language for the cranking path criterion in Low Impact. The SDT has reviewed the uses of the term and has ensured consistency when referencing Facilities or BES Cyber Systems. The main difference is the addition of "destroyed" and "otherwise rendered unavailable" in the case of Facilities. The SDT has added the suggested clarification in criterion 3.3.

One comment was on the use of the word "would" instead of "could" in the standards and recommended the use of the prospective word "could". The SDT believes that the use of the word "would" is appropriate to describe the certain impact of a compromise due to an exploitation of vulnerability.

One commenter stated that the last paragraph on page seven leaves it up to the registered entity to determine the level of granularity when identifying the BES Cyber Systems and instructs the registered entity to take into consideration the operational environment and scope of management and raised questions of auditability in the text. The SDT notes that the background and guideline sections are only providing context to the standards. The only auditable parts of the

standards are the applicable definitions and requirements. The SDT directs the commenter to the definition of BES Cyber System for effective application of the requirements.

There was a comment on the examples for Electronic Access Control and Monitoring Systems in the background section, specifically the use of certificate authorities, security event monitoring systems and intrusion detection systems. The SDT uses the term "Certificate Authorities" as an example of the type of cyber assets owned by the Responsible Entity that would be subject to the CIP standards if it relates to a function that is used within the scope of a BES Cyber System. The SDT has used the generic term "security event monitoring systems" as a generic functional term and has specifically avoided the use of the various acronyms used to include this function. This is also true of the term "intrusion detection systems": the SDT is providing an example of the function, and the term "intrusion prevention systems" includes functions that are not within the scope of the requirements. The SDT acknowledges that intrusion prevention systems necessarily include an intrusion detection function.

One commenter suggested the inclusion of network attached storage and storage area networks in the examples for Protected Cyber Assets. Examples provided are not intended to be exhaustive lists, but are intended to provide some examples of the types of systems that could meet the requirements for the definition of Protected Cyber Assets. They are not intended to mean that all of these types of systems are necessarily Protected Cyber Assets, but are examples of systems that could be Protected Cyber Assets if they meet the definition.
SPP suggested footnoting the time horizon reference in requirements. Time Horizons are standard designations used in all requirements and is a standard requirement for all NERC standards requirements. They are required characteristics of each requirement in the same way that Violation Risk Factors are. The SDT believes that footnotes for these are not required as they are generically defined in other NERC documents.

One commenter requested clarification of the general use of transmission facility and its scope. In using terms such as "Facility" in the criteria, the SDT has made substantial changes to Requirement R1 that provides flexibility to the Responsible Entity to define what the term includes within the definition of the requirement. Requirement R1 now includes a listing of the types of assets to be considered that provides a more defined scope to the applicability of CIP-002-5 and the CIP cyber security standards. Within these, Responsible Entities have flexibility in defining the sets within these considerations for application of the criteria.

One commenter requested clarification on entities that have coordination responsibilities. The SDT notes that the table in the guidance provides guidance on those entities that have responsibilities for inter-entity coordination. In a

restoration scenario, those Responsible Entities that require inter-entity coordination to perform their functions that require such coordination have responsibility for this coordination.

One commenter pointed to an inconsistency between the title of the standard and the heading of the document. The SDT corrected the inconsistency.

One commenter stated that the NERC Functional Model does not define Functional Entities. The SDT notes that the current version of the Functional Model (Version 5) defines both Reliability Functions and the Functional Entity that performs the tasks. In addition, there are further responsibilities defined under Functional Entities which are specifically defined in relation with other Functional Entities.

A commenter requested additional guidance in the concept of BES Cyber System. The SDT has made several modifications to the guidance for the overall concept of BES Cyber System, including additional peripheral terms related to BES Cyber Systems, such as Protected Cyber Assets. The SDT believes these additional clarifications provide the additional guidance on the concepts.

There was a comment on the guidance on BES Reliability Operating Services provided for optional use by entities as an aid to scope BES Cyber Systems in the guideline section of the standards. One commenter also suggested removing the designation of Functional Entities for the BES Reliability Operating Services to minimize differing opinions. The SDT made several modifications to this section in consideration of these comments where appropriate. With respect to comments on voltage control and Distribution Providers, the Functional Model clearly lists voltage reduction in its tasks. The designation of Functional Entities is provided as guidance and resulted from comments from previous drafts. The SDT believes that this information provides additional guidance for some Responsible Entities in scoping their BES Cyber Systems.

One commenter suggested that the format of the standard is different and suggested moving the background to the end together with the guideline. The SDT has used the standard template for results based standards and is the recommended standards development format and approach.

There was a suggestion that the rationale should not be part of the standard. The rationale statements will be removed from the official filing and included as information, together with the guidance information.

Several comments were on the use of bright lines and the problem with a one size fits all approach without provisions for studies and engineering analysis and the requirement to require at least some protection for all BES assets. The SDT notes that the objective of Version 5 of the CIP standards is to provide some level of protection to all BES Cyber Systems according to the impact to the real-time operation of the BES assets they are supporting. The bright line based approach was approved by industry stakeholders and FERC as part of Version 4.

One commenter suggested the use of a more definitive term “prevent” in qualifying impact on functions in the reliable operation of the BES. In addition, there was a suggestion for an explanation of the use of the 15 minute window in the definition of BES Cyber Asset. The SDT believes that the word “prevent” does not provide a qualification for the full scope of applicability, but a subset. The intent of the SDT is to ensure that impacts also cover impairment as well as outright “prevention”. An explanation of the 15 minute window is in the background section of the standard under real-time operations.

One comment suggested that the stipulation of ownership for compliance responsibility is inconsistent with PRC standards that also stipulate “operate”. The SDT has consistently maintained that responsibility for compliance is the asset owner’s.

There was a general comment on the application of FISMA and the NIST framework in relation to the CIP standards. The SDT notes that CIP V5 considered the NIST framework as one of the inputs to the drafting of these standards in response to FERC Order 706. The SDT did not consider FISMA requirements, but rather the NIST Risk management framework as directed by Order 706. The SDT also considered input from several other frameworks and has used those inputs in the drafting of standards that are subject to compulsory compliance and enforcement. The NIST 800-53 series is characterized as guidelines for controls, not compliance requirements.

QUESTION A10 – CIP-003-5:

If you disagree with the changes made to CIP-003-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the major issues identified through the comment form with CIP-003-5 included (1) the list of low impact BES Cyber Systems for Requirement R2, (2) demonstration of policy implementation, (3) clarity of policy topics in Requirement R2, and (4) the reliability benefit of the annual review/approval of the cyber security policies as well as maintaining documentation of changes to the CIP Senior Manager and delegates.

List of Low Impact BES Cyber Systems for Requirement R2

Numerous commenters identified concerns that while the SDT intended to provide protection from discrete identification of Low Impact BES Cyber Systems, there was still significant concern that this would still be required in order to demonstrate compliance with the requirement. Additionally, commenters suggested that the object of the policy for Low Impact BES Cyber Systems should be on the facilities (or "sites") themselves and not specifically the Low Impact BES Cyber Systems. The SDT continues to believe that the identification of low impact BES Cyber Systems would not be required in order to comply with CIP-003-5 R2. However, the SDT also agrees with commenters that a facilities based approach to the low impact policy comes with a number of benefits. Among these being the creation of a reasonable level of abstraction (the facility) of which to refer to the low impact BES Cyber Systems, thus facilitating any necessary sampling during an audit, without explicitly needing a list of these cyber systems themselves. Consequently, CIP-003-5 R2 has leveraged a reference to CIP-002-5 where facilities with low impact BES Cyber Systems are identified. The SDT believes this approach will provide consistency of application of the policy for low impact BES Cyber Systems, provide a reasonable approach for audit oversight, and create additional clarity on the evidentiary expectations.

Policy Implementation

There were a number of comments that expressed issues with ambiguity in the use of the term "implement" as it relates to the cyber security policies in both CIP-003-5 R1 and R2. In reviewing this comment, the SDT noted that the obligation to "implement" the cyber security policy has existed since version 1 of the CIP standards. Additionally, FERC directed the ERO in Order 706 to "to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards." While this directive did not specifically direct changes to the cyber security policy, as this policy already had the obligation to implement in version 1, the SDT is cognizant that any change to the contrary would require reasonable justification.

As it relates to the CIP-003-5 R1 cyber security policy for medium impact and high impact BES Cyber Systems, the SDT believes there is sufficient justification to make a modification to the language of the requirement in order to provide the clarity that the industry desires around the obligation to "implement." The SDT strongly believes that it has not lessened the obligation to implement the cyber security policy. However, given the required scope of the CIP-003-5 R1 cyber security policies, the SDT believes that implementation of these cyber security policies is effectively demonstrated through compliance with CIP-004-5 through CIP-011-1. Therefore, the SDT has chosen to remove the term "implement" from CIP-003-5 R1. The SDT believes that this should provide clarity as to the expectation of implementation as well as to relieve concerns of double jeopardy between CIP-003-5 R1 and the entire body of CIP-004-5 though CIP-011-1.

The SDT has handled this concern differently for the low impact cyber security policies in CIP-003-5 R2. As there are no corresponding requirements in CIP-004-5 through CIP-011-1 that require explicit implementation of areas addressed by the low impact policy, there are no double jeopardy concerns. The SDT has attempted to provide structure around the obligation to implement the cyber security policies through the global modifications that provide for continuous improvement and the identification, assessment, and correction of deficiencies. The expectation of the SDT is that entities will define cyber security policies that address the four required areas and put these policies in effect using an overall framework that provides reasonable assurance that the policies are applied through methods that identify, assess, and correct any deficiencies.

Policy Topic Clarity for Low Impact Policy

In addition to ambiguity over the implementation of the cyber security policy for low impact BES Cyber Systems, commenters expressed concern over the clarity of the individual policy topics for low impact BES Cyber Systems. The SDT appreciates these comments and has made some modifications to the topic language. However, the SDT understands that these modifications do not completely alleviate the concerns around individual topical clarity. The SDT has modified the topic "Physical access controls" to "Physical security controls" and "Electronic access controls" to "Electronic access controls for external routable protocol connections and Dial-up Connectivity." The SDT chose to not add too much additional detail to these policy topics in recognition of the wide range of environmental, geographic, technical, operational, and logistical differences that may exist amongst the set of low impact BES Cyber Systems. As such, the SDT's intent is to allow Responsible Entities to have flexibility to design and implement the most efficacious security program possible for their particular set of low impact BES Cyber Systems. The modification to physical security controls over physical access controls acknowledges this approach. "Physical security controls" gives great discretion to the Responsible Entity to choose controls that are effective. The SDT believes the paradigm shifts in NERC CIP Reliability

standards allowing for multiple levels of security (high, medium, and low) and creating an atmosphere of continuous improvements through the identification, assessment, and correction of deficiencies will address the concerns of compliance risk that are driving the need for more prescriptiveness in requirements language. Additionally, the SDT added the language to R2.3 "…for external routable protocol connections and Dial-up Connectivity" to address the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact.

Reliability Benefit and Double Jeopardy Concerns of Requirements R3, R5, and R6

Numerous commenters also raised questions about either the reliability benefit or double jeopardy of requirements R3, R5, and R6. Often, these questions were tied to work going on in NERC standards related to Paragraph 81 of the FERC Order approving the FFT process. The comments about their reliability benefit sometimes hinged on them being a requirement in and of themselves, rather than a component of the requirements for R1, R2, and R4 in draft two. The double jeopardy concerns also raised similar questions as to whether a violation of R3, R5, and R6 in draft two would also constitute a violation of R1, R2, and R4 of draft two. The SDT agreed with these concerns. The SDT believes that the same reliability and security objectives will be reached, while alleviating unnecessary compliance concerns, by combining these requirements. As such, the review and approval for each of the cyber security policies has been added as an obligation in the security policy requirements (R1 and R2) themselves. Additionally, the obligation to keep the CIP Senior Manager and delegation documentation up-to-date has been added to those requirements (now R3 and R4), respectively.

Modify Signature to Approval in Measures

Several commenters mentioned the use of "signature" in the measures when the requirement called for "approval." The SDT had never intended to imply that a wet ink signature was the only acceptable form of evidence of approval. Language in the guidelines and technical basis section further clarified that hardcopy or electronic approvals were acceptable. The SDT has modified all instances of "signature" in the measures in CIP-003-5 to "approval' to prevent any confusion and better align with the language in the requirement itself.

Minority Comments

The SDT also received a number of different comments that asked various questions or raised assorted concerns about the topics that were included in Requirement R1. Among other things, these comments mentioned confusion about the guidance related to terms used in the policy topics, inclusion of Interactive Remote Access separate from ESPs, and the relationship between these topics and CIP-004-5 through CIP-011-1. The intention of the SDT was for these policy items

to individually reference each of the standards CIP-004-5 through CIP-011-1. As such, the SDT has chosen to align the policy topics with the title of the other CIP standards (with some exceptions) and include a specific reference to the standards itself in order to clarify that alignment. As mentioned in the discussion of policy implementation above, the SDT's expectation is that implementation of the cyber security policy for medium and high impact BES Cyber Systems will be demonstrated through compliance with CIP-004-5 through CIP-011-1.

Typographical Errors

Several commenters also noted a typographical error where the VRF for CIP-003-5 R2 was listed as low in the requirement and medium in the VSL table. The SDT appreciates commenters pointing this out. The intention of the SDT was for the VRF of CIP-003-5 R1 for medium and high impact BES Cyber Systems to be medium, consistent with CIP-003-4 R1 and for the VRF of CIP-003-5 R2 to be low due to the lesser risk associated with low impact BES Cyber Systems. The SDT has corrected this mistake.

VSL Comments not responded to:

One comment suggested that Requirement R6 should have four VSLs based on days late. The SDT has removed the requirement because the addition of language to identify, assess, and correct deficiencies in what is now Requirement R4 covers the documentation of delegations.

One comment stated to start missing discrete elements of a program as low VSLs in Requirement R2. The SDT has made this change.

One comment suggested to use Lower/Moderate VSLs for Requirement R2 instead. In response, the VSLs only address the degree to which entities can violate a requirement and not the risk power to the BES from said violations.

For the Requirement R4 VSLs, there was a comment that the VSL should read: Lower/Medium – Lack of Review High/Severe – Lack of Approval. This requirement has been removed because the annual review is already accomplished in Requirement R1 and the need to have a CIP Senior Manager sign the policy is administrative in nature.

There was a comment that the VSL for Requirement R3 is more detailed than the requirement itself. The SDT has updated the VSL to match the requirement.

Questions with Votes Only:

1. **Requirement R1 of draft CIP-002-5 requires the identification of high and medium impact BES Cyber Systems as described in Attachment 1. Further, it requires a Responsible Entity to review (and update as needed), the required identification within 60 calendar days of when a change to BES Elements or Facilities is placed into operation, which is planned to be in service for more than 6 calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category. Do you agree with the proposed Requirement R1?**

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
ACES Power Marketing	No
PPL Corporation NERC Registered Affiliates	No
BC Hydro	No
IRC Standards Review Committee	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No

Organization	Yes or No
Duke Energy	No
Dominion	No
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	No
MRO NSRF	No
Florida Municipal Power Agency	No
Madison Gas and Electric Company	No
Luminant	No
SMUD & BANC	No
Progress Energy	No
NCEMC	No
Dairyland Power Cooperative	No
Western Electricity Coordinating Council	No
CenterPoint Energy	No
Tri-State G&T - Transmission	No
PacifiCorp	No

Organization	Yes or No
PNM Resources	No
Hydro One	No
Southern Company Services, Inc.	No
Western Area Power Administration	No
Utility Services Inc.	No
Consumers Energy Company	No
Muscatine Power and Water	No
North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency	No
NIPSCO	No
Portland General Electric	No
TransAlta Centralia Generation LLC	No
Trans Bay Cable	No
National Grid	No
Hydro-Quebec TransEnergie	No
LCEC	No

Organization	Yes or No
Pacific Gas and Electric Company	No
Ingleside Cogeneration LP	No
Manitoba Hydro	No
Niagara Mohawk (dba National Grid)	No
PSEG	No
Bonneville Power Administration	No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Illinois Municipal Electric Agency	No
NV Energy	No
Wisconsin Electric Power Company	No
The Empire District Electric Company	No

Organization	Yes or No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Texas Reliability Entity	No
Nebraska Public Power District	No
City of Austin dba Austin Energy	No
ISO New England	No
Network & Security Technologies, Inc.	No
City Utilities of Springfield, MO	No
American Public Power Association	No
Alliant Energy	No
Springfield Utility Board	No
Exelon Corporation and its affiliates	No

Organization	Yes or No
Indiana Municipal Power Agency	No
NYISO	No
Cowlitz County PUD	No
Brazos Electric Power Cooperative	No
US Bureau of Reclamation	No
NRG Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
SPP and specific Member companies	Yes
Puget Sound Energy, Inc.	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes

Organization	Yes or No
Arizona Public Service Company	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Services Corporation	Yes
Lincoln Electric System	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Xcel Energy	Yes
Flathead Electric Co-op	Yes
Tennessee Valley Authority	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes

Organization	Yes or No
PJM Interconnection	Yes
Kansas City Power & Light	Yes
MEAG Power	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes

2. Requirement R2 of draft CIP-002-5 states, "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once each calendar year, not to exceed 15 calendar months between approvals, even if it has no identified items in Requirement R1, Parts 1.1, 1.2, or 1.3." Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
ACES Power Marketing	No
BC Hydro	No
Texas RE NERC Standards Review Subcommittee	No
NRG Companies	No
Florida Municipal Power Agency	No
SMUD & BANC	No
Progress Energy	No
PacifiCorp	No
Utility Services Inc.	No

Organization	Yes or No
NIPSCO	No
LCEC	No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
NextEra Energy, Inc.	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Texas Reliability Entity	No
City of Austin dba Austin Energy	No
ISO New England	No

Organization	Yes or No
Kansas City Power & Light	No
Indiana Municipal Power Agency	No
Brazos Electric Power Cooperative	No
PPL Corporation NERC Registered Affiliates	Yes
IRC Standards Review Committee	Yes
Southwest Power Pool Regional Entity	Yes
Duke Energy	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes

Organization	Yes or No
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Luminant	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
Hydro One	Yes

Organization	Yes or No
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency	Yes
Portland General Electric	Yes

Organization	Yes or No
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
Pattern	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes

Organization	Yes or No
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Xcel Energy	Yes
Flathead Electric Co-op	Yes
Bonneville Power Administration	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Ameren	Yes
Northeast Utilities	Yes
Oncor Electric Delivery Company LLC	Yes
Nebraska Public Power District	Yes

Organization	Yes or No
PJM Interconnection	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes
MEAG Power	Yes
American Public Power Association	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
California ISO	Yes
US Bureau of Reclamation	Yes

4. CIP-003-5 R1 states "Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall implement one or more documented cyber security policies that address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
NESCOR/NESCO	No
ACES Power Marketing	No
Duke Energy	No
Progress Energy	No
NCEMC	No
PNM Resources	No
AEP Standards based SME list	No
Xcel Energy	No
MidAmerican Energy Company	No
Ameren	No

Organization	Yes or No
NextEra Energy, Inc.	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Kansas City Power & Light	No
Brazos Electric Power Cooperative	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Southwest Power Pool Regional Entity	Yes
NRG Companies	Yes
PNGC Comment Group	Yes

Organization	Yes or No
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Florida Municipal Power Agency	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Hydro One	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes

Organization	Yes or No
Portland General Electric	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes

Organization	Yes or No
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Lakeland Electric	Yes
New York Power Authority	Yes
Tampa Electric Company	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Illinois Municipal Electric Agency	Yes
NV Energy	Yes
Wisconsin Electric Power Company	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Oncor Electric Delivery Company LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
City of Austin dba Austin Energy	Yes
ISO New England	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes
MEAG Power	Yes
American Public Power Association	Yes
Alliant Energy	Yes

Organization	Yes or No
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
California ISO	Yes
US Bureau of Reclamation	Yes

5. **CIP-003-5 R2 states "Each Responsible Entity for its BES Cyber Systems not identified as high impact or medium impact shall implement one or more documented cyber security policies to address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2?**

Summary Consideration:

Organization	Yes or No
NESCOR/NESCO	No
ACES Power Marketing	No
PPL Corporation NERC Registered Affiliates	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No
NRG Companies	No
Duke Energy	No
MRO NSRF	No
Florida Municipal Power Agency	No

Organization	Yes or No
Madison Gas and Electric Company	No
Pepco Holdings Inc & Affiliates	No
National Rural Electric Cooperative Association (NRECA)	No
Progress Energy	No
NCEMC	No
Dairyland Power Cooperative	No
AEP Standards based SME list	No
Snohomish County PUD	No
Edison Mission Marketing & Trading	No
Consumers Energy Company	No
Muscatine Power and Water	No
Lower Colorado River Authority	No
LCEC	No

Organization	Yes or No
LCRA Transmission Services Corporation	No
Ingleside Cogeneration LP	No
Xcel Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service	No

Organization	Yes or No
Corporation and Upper Pennisula Power Company	
Nebraska Public Power District	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Kansas City Power & Light	No
Network & Security Technologies, Inc.	No
MEAG Power	No
Alliant Energy	No
Exelon Corporation and its affiliates	No
Deseret Power	No
Brazos Electric Power Cooperative	No
Northeast Power Coordinating Council	Yes
BC Hydro	Yes

Organization	Yes or No
IRC Standards Review Committee	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Southern California Edison Company	Yes
SPP and specific Member companies	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes

Organization	Yes or No
PNM Resources	Yes
Hydro One	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Utility Services Inc.	Yes
NIPSCO	Yes
Portland General Electric	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes

Organization	Yes or No
Pacific Gas and Electric Company	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
New York Power Authority	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes

Organization	Yes or No
Texas Reliability Entity	Yes
ISO New England	Yes
City Utilities of Springfield, MO	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
California ISO	Yes
US Bureau of Reclamation	Yes

6. CIP-003-5 R3 states "Each Responsible Entity shall identify a CIP Senior Manager by name." Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
ACES Power Marketing	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
Florida Municipal Power Agency	No
Progress Energy	No
Southern Company Services, Inc.	No
Independent Electricity System Operator	No

Organization	Yes or No
Lakeland Electric	No
Tampa Electric Company	No
Illinois Municipal Electric Agency	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Texas Reliability Entity	No
City of Austin dba Austin Energy	No
Kansas City Power & Light	No
Network & Security Technologies, Inc.	No
American Public Power Association	No

Organization	Yes or No
Tucson Electric Power	No
Cowlitz County PUD	No
Brazos Electric Power Cooperative	No
California ISO	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
NRG Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC)	Yes

Organization	Yes or No
including OPC, GTC & GSOC	
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
Hydro One	Yes

Organization	Yes or No
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes
Portland General Electric	Yes
Trans Bay Cable	Yes
National Grid	Yes

Organization	Yes or No
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
City of Palo Alto	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Xcel Energy	Yes
Bonneville Power	Yes

Organization	Yes or No
Administration	
New York Power Authority	Yes
Tennessee Valley Authority	Yes
MidAmerican Energy Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
Wisconsin Electric Power Company	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
ISO New England	Yes
City Utilities of Springfield,	Yes

Organization	Yes or No
MO	
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

7. **CIP-003-5 R4 states "Each Responsible Entity shall review and obtain CIP Senior Manager approval for cyber security policies identified in Requirements R1 and R2, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals." Do you agree with the proposed Requirement R4?**

Summary Consideration:

Organization	Yes or No
NESCOR/NESCO	No
ACES Power Marketing	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
Florida Municipal Power Agency	No
Progress Energy	No
Edison Mission Marketing & Trading	No
Independent Electricity System Operator	No

Organization	Yes or No
Pattern	No
United Illuminating Company	No
Lakeland Electric	No
Tampa Electric Company	No
Tennessee Valley Authority	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
Ameren	No
NextEra Energy, Inc.	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
PJM Interconnection	No
Kansas City Power & Light	No

Organization	Yes or No
American Public Power Association	No
NYISO	No
Cowlitz County PUD	No
Brazos Electric Power Cooperative	No
California ISO	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
Texas RE NERC Standards Review Subcommittee	Yes
NRG Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes

Organization	Yes or No
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes

Organization	Yes or No
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
Hydro One	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes

Organization	Yes or No
Portland General Electric	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
Turlock Irrigation District	Yes

Organization	Yes or No
Xcel Energy	Yes
Bonneville Power Administration	Yes
New York Power Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Oncor Electric Delivery Company LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
City of Austin dba Austin Energy	Yes
ISO New England	Yes

Organization	Yes or No
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
US Bureau of Reclamation	Yes

8. CIP-003-5 R5 states "Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate and the date of the delegation, and approved by the CIP Senior Manager." Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No
NRG Companies	No
Duke Energy	No
Florida Municipal Power Agency	No
Progress Energy	No
Hydro One	No

Organization	Yes or No
Independent Electricity System Operator	No
Xcel Energy	No
Flathead Electric Co-op	No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper	No

Organization	Yes or No
Pennisula Power Company	
PJM Interconnection	No
City of Austin dba Austin Energy	No
ISO New England	No
American Public Power Association	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Cowlitz County PUD	No
California ISO	No
ACES Power Marketing	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes

Organization	Yes or No
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes

Organization	Yes or No
NIPSCO	Yes
Portland General Electric	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes

Organization	Yes or No
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Kansas City Power & Light	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield,	Yes

Organization	Yes or No
MO	
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

9. CIP-003-5 R6 states "Each Responsible Entity shall document any changes to the CIP Senior Manager or any delegations within thirty calendar days of the change. Delegation changes do not need to be reinstated with a change to the delegator." Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Texas RE NERC Standards Review Subcommittee	No
NRG Companies	No
Florida Municipal Power Agency	No
Progress Energy	No
Portland General Electric	No
Independent Electricity System Operator	No
Flathead Electric Co-op	No

Organization	Yes or No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
ISO New England	No
Kansas City Power & Light	No

Organization	Yes or No
American Public Power Association	No
Tucson Electric Power	No
Cowlitz County PUD	No
California ISO	No
ACES Power Marketing	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
Southwest Power Pool Regional Entity	Yes
Duke Energy	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric	Yes

Organization	Yes or No
Cooperative, Inc. (JRO00088, NCR01177)	
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes

Organization	Yes or No
Hydro One	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes
Trans Bay Cable	Yes

Organization	Yes or No
Pattern	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes

Organization	Yes or No
Xcel Energy	Yes
Bonneville Power Administration	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
Wisconsin Electric Power Company	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes

Organization	Yes or No
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards

Comment Form B

CIP-004 through CIP-007 Questions

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Index to Questions, Comments, and Responses

Questions with Summaries Included: 17
QUESTION B8 – CIP-004-5, R1, R2, R3, R4 or R5: 17
QUESTION B9 – CIP-004-5, R6 or R7: 22
QUESTION B12 – CIP-005-5, R1: 41
QUESTION B13 – CIP-005-5, R2: 52
QUESTION B17 – CIP-006-5: 55
QUESTION B23 – CIP-007-5, R1, R2, R3 or R4: 58
QUESTION B24– CIP-007-5 REQUIREMENT R5: 84
Questions with Votes Only: 94
1. CIP-004-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 94
2. CIP-004-5 R2 states "Each Responsible Entity shall have a role-based cyber security training program to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 101
3. CIP-004-5 R3 states "Each Responsible Entity shall implement its documented role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3? 109
4. CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4? 117
5. CIP-004-5 R5 states "Each Responsible Entity shall implement one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable elements in CIP-004-5 Table R5 –

Personnel Risk Assessment." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5? 125

6. CIP-004-5 R6 states "Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R6? 133

7. CIP-004-5 R7 states "Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R7? 141

10. CIP-005-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 149

11. CIP-005-5 R2 states "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 157

14. CIP-006-5 R1 states "Each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? .. 164

15. CIP-006-5 R2 states "Each Responsible Entity shall implement one or more documented visitor control programs that include each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 172

16. CIP-006-5 R3 states "Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3? 180

18. CIP-007-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 188

19. CIP-007-5 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 196

20. CIP-007-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3? 204

21. CIP-007-5 R4 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4? 212

22. CIP-007-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5? 220

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Bruce Metruck	New York Power Authority	NPCC	6
12.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
13.	Robert Pellegrini	The United Illuminating Company	NPCC	1
14.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
15.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
16.	Brian Robinson	Utility Services	NPCC	8
17.	Michael Jones	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Don Weaver	New Brunswick System Operator	NPCC	2
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3
24.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5

2.	Group	Annabelle Lee	NESCOR/NESCO									

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3.	Group	Jason Marshall	ACES Power Marketing					X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Tim Soles	Occidental Power Services, Inc.	ERCOT 3										
4.	Andy Gallo	Austin Energy	ERCOT 1										
5.	Andy Gallo	Austin Energy	ERCOT 3										
6.	Andy Gallo	Austin Energy	ERCOT 4										
7.	Andy Gallo	Austin Energy	ERCOT 5										
8.	Andy Gallo	Austin Energy	ERCOT 6										
8.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8. Annie Terracciano	Northern Lights Inc.	WECC 3										
9. Aleka Scott	PNGC	WECC 4										
10. Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11. Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12. Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13. Margaret Ryan	PNGC	WECC 8										
12. Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13. Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14. Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3. M & A Electric Power Cooperative			SERC 1, 3										
4. Northeast Missouri Electric Power Cooperative			SERC 1, 3										
5. N.W. Electric Power Cooperative, Inc.			SERC 1, 3										
6. Sho-Me Power Electric Cooperative			SERC 1, 3										
15.	Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X						
Additional Member		Additional Organization	Region Segment Selection										
1. Oglethorpe Power Corporation			SERC 5										
2. Georgia Transmission Corporation			SERC 1										
16.	Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X
Additional Member		Additional Organization	Region Segment Selection										
1. MAHMOOD SAFI		OPPD	MRO 1, 3, 5, 6										
2. CHUCK LAWERENCE		ATC	MRO 1										
3. TOM WEBB		WPS	MRO 3, 4, 5, 6										
4. JODI JENSON		WAPA	MRO 1, 6										
5. KEN GOLDSMITH		ALTW	MRO 4										
6. DAVE RUDOLPH		BEPC	MRO 1, 3, 5, 6										
7. JOE DEPOORTER		MGE	MRO 3, 4, 5, 6										
8. SCOTT NICKELS		RPU	MRO 4										
9. TERRY HARBOUR		MEC	MRO 1, 3, 5, 6										
10. MARIE KNOX		MISO	MRO 2										
11. LEE KITTELSON		OTP	MRO 1, 3, 4, 5										
12. SCOTT BOS		MPW	MRO 6, 1, 3, 5										
13. TONY EDDLEMAN		NPPD	MRO 1, 3, 5										
14. THERESA ALLARD		MPC	MRO 1, 3, 5, 6										
17.	Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing													
18.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				
Additional Member		Additional Organization	Region Segment Selection										
1. Timothy Beyrle		City of New Smyrna Beach	FRCC 4										
2. James Howard		Lakeland Electric	FRCC 3										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3. Greg Woessner	Kissimmee Utility Authority	FRCC	3										
4. Lynne Mila	City of Clewiston	FRCC	3										
5. Joe Stonecipher	Beaches Energy Services	FRCC	1										
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4										
7. Randy Hahn	Ocala Utility Services	FRCC	3										
19. Group	Joseph DePoorter	Madison Gas and Electric Company				X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Darl Shimko	MGE	MRO	3										
2. Joseph DePoorter	MGE	MRO	4										
3. Steve Schultz	MGE	MRO	5										
4. Jeff Keebler	MGE	MRO	6										
20. Group	David Thorne	Pepco Holdings Inc & Affiliates		X		X							
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Mark Jones	Pepco	RFC	1										
21. Group	Rick Terrill	Luminant						X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Mike Laney	Luminant Generation Company LLC	ERCOT	5										
2. Tim Soles	Occidental Power Services, Inc.	ERCOT	6										
3. Tim Soles	Occidental Power Services, Inc.	ERCOT	3										
4. Andy Gallo	Austin Energy	ERCOT	1										
5. Andy Gallo	Austin Energy	ERCOT	3										
6. Andy Gallo	Austin Energy	ERCOT	4										
7. Andy Gallo	Austin Energy	ERCOT	5										
8. Andy Gallo	Austin Energy	ERCOT	6										
9. Brenda Hampton	Luminant Energy Company LLC												
22. Group	Joe Tarantino	SMUD & BANC		X		X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Kevin Smith	BANC	WECC	1										
23. Group	Scott Brame	NCEMC		X				X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Rayburn Country Electric Cooperative			SPP										
2. Empire District Electric			SPP	1									
3. City Utilities of Springfield			SPP	4									
4. Westar Energy			SPP	1, 3, 5, 6									
5. Cleco Power			SPP	1, 3, 5, 6									
25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Pawel Krupa			WECC	1									
2. Dana Wheelock			WECC	3									
3. Hao Li			WECC	4									
27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Denise Lietz		Puget Sound Energy	WECC	1									
2. Erin Apperson		Puget Sound Energy	WECC	3									
28.	Group	Michael Mertz	PNM Resources	X		X							
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Laurie Williams		Public Service Co. of New Mexico	WECC	1									
2. Michael Mertz		Public Service Co. of New Mexico	WECC	3									
29.	Group	Sasa Maljukan	Hydro One	X									
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. David Kiguel		Hydro One	NPCC	1									
30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION B8 – CIP-004-5, R1, R2, R3, R4 or R5:

If you disagree with the changes made to CIP-004-5, Requirements R1, R2, R3, R4 or R5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to the requirements, measures, and VSLs associated with Requirement R1, R2 R3, R4 or R5 of CIP-004-5. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Note

In draft two, Requirement R2 required a documented process for its role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems while Requirement R3 was the implementation of that process. Requirement R4 required one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems while Requirement R5 was the implemented of the one or more documented processes. In preparing CIP-004-5 for draft 3, the SDT determined that Requirements R2 and R3 could be combined, and so could Requirements R4 and R5. In that way, the requirements more closely match most other requirements in CIP-004-5 through CIP-011-5 to implement a documented process, and it also facilitated inclusion of the correcting deficiencies approach, explained in the common response section of this comment response, so that the resulting requirements, draft 3's Requirements R2 and R3, could be implemented "in a manner that identifies, assesses, and corrects deficiencies." Therefore, Requirement R6 from draft 2 was renumbered to Requirement R4 in draft 3, and Requirement R7 from draft 2 was renumbered as Requirement R5. For the purposes of the comment summaries and responses for this question, the requirement number references refer to the requirement numbers as listed in draft 2, unless otherwise noted.

General

The applicable systems section has been reviewed and revised to help ensure consistency within CIP-004-5 and with the other CIP standards. This should also make clear that these requirements are not applicable to Low Impact BES Cyber Systems. The SDT has decided not to include the concept of authorized unescorted electronic access. Individuals with

authorized electronic access must be trained and have a personnel risk assessment performed as per the requirements. This applies to all personnel including employees, vendors and contractors. For example, the question on a vendor controlled system would require the vendor to meet the requirements as set forth in CIP-004-5.

The SDT has stricken the "attain and retain" language for the training requirement, but has chosen to keep it for the personnel risk assessment requirements. The difference between those words and "acquire and maintain" are negligible.

The SDT does not agree with the suggestion to make Requirements R2 and R3 an expansion of the awareness program instead of training. The SDT believes that for protection of these BES Cyber Systems more targeted training is needed.

The guidelines and technical basis section has been updated to better align with the new draft content and organization. One areas of focus is the training content on networking hardware and software and other issues of electronic interconnectivity. More description around the criminal history check has also been added.

Requirement R1

The SDT has added language in the change rationale section to reinforce the concept that a registered entity does not need to ensure or prove all authorized personnel have received awareness. The language in R1.1 has also been revised to further clarify this point through the use of the word, reinforces. Also, the SDT has added language to clarify that awareness of cyber security practices can include physical security information.

The SDT appreciates the suggestions to allow the registered entity to define the timeline for awareness reinforcement or their own quarters, but believes the language is best retained as written for consistency.

In the measures for Requirement R1, the SDT has removed the reference to "documented security awareness program" and has modified the language to be consistent with the other CIP standards. The language, "not limited to" has also been revised and reviewed for consistency across the standards.

Requirement R2/Requirement R3

These two requirements have been combined into a single requirement which covers the training content in R2.1, in a single table, and the training frequency in R2.2 and R2.3. Another key change in R2 is the modification of the language to clarify that the registered entity is able to determine their training program(s) to fit their needs and it can be based on role, function or responsibility. In concert with this change, Table R2 section 2.1 was deleted to help eliminate the

language focusing on role based training. Training is required of individuals with authorized, unescorted physical access or authorized electronic access as per the revised R2.2 and R2.3. In addition to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity, the SDT believes training is also needed for individuals with access to Physical Access Control Systems and Electronic Access Control or Monitoring Systems. Also, the SDT has removed the reference to BES Cyber Systems in Table R2 formerly in sections R2.2, R2.3 and R2.4. For Table R2 previous section 2.5, the Change Rationale has been modified to reflect this is a new training requirement. Also, this training should be tracked for personnel involved in the visitor control process in accordance with Table R3 section 3.2 The SDT agrees that recovery plan information referenced in Table R2, previous section 2.8 should be labeled appropriately. The training content on cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets will remain in Table R2 as it is a new requirement from FERC Order 706 and the SDT has provided additional guidance to clarify the intent of this entry.

For Table R2, previous section 2.2, the SDT believes the training should be focused on policy content, not availability, and has made no changes. In Table R2, the SDT has chosen to retain both identification of incidents and response to incidents as separate content as the personnel who need to be trained on each may be different. The scope of training on recovery plans is left to the registered entity and no changes have been made to the standard. Also, the SDT believes the focus of recovery is the specific recovery plans, not the business impact analysis. The measure for Table R2 has been modified to focus on training material as evidence and the guidance has been revised to reflect the type of content this training should include.

The SDT has edited the language formerly in R3 for clarity with removal of the role based reference and the attain/retain language. Since there are no references to evidence retention in the requirement part 1.2, evidence retention, of the compliance section of the standard applies. The reference to documentation that was in Table R3 section 3.1 has been removed as it is covered in the measure.

The SDT does not agree that access to Low Impact Cyber Systems need the training defined in R2. Also, R2 has language included (in a manner that identifies, assesses, and corrects deficiencies) as suggested by some comments to allow detection and correction of flaws. The proposal to allow the registered entity to define the timeline for training was not supported by the SDT. For 2.2 and 2.3 (formerly in Table R3 section 3.2), the SDT believes the language is sufficiently clear that the time interval is between training dates and does not need that language added. BES Cyber Systems was changed to applicable cyber assets in 2.2. The two entries on initial and recurring training are now in Table R2. The SDT

has revised the language in the measure for these two entries to make it clear the focus is on training records which should include training date and date access is granted.

Requirement R4/Requirement R5

As suggested, the SDT has combined these two requirements into one and it is now Requirement R3. The SDT has modified the language formerly in Requirement R4 to help clarify that identity confirmation and criminal history check are part of the personnel risk assessment (PRA). The PRA is the outcome of the process or criteria used by a registered entity to evaluate the results of the identity verification (for the initial PRA) and seven year criminal history records check to determine what, if any, authorized access to grant to employees, contractors or vendors. The level of documentation for the process or criteria is left to the registered entity, but should be sufficient for a third party to understand how the decision is made. In defining the seven year criminal history records check, it is not the intent for the registered entity to evaluate the individual's residence locations, education or prior employment. The language has been revised to indicate the criminal history records check should cover locations where the individual has resided/lived for six consecutive months during the past seven years. The initial identity confirmation, even if performed under prior versions of the standards, is sufficient for the employment duration of the individual. The initial identity verification, criminal history check and PRA should be retained in accordance with requirement part 1.2 in the evidence retention component of the compliance section of the standard. A PRA performed under previous versions of the standards is valid until it reaches the end of its seven year lifespan. The intent of the SDT is that the PRA in effect is no older than seven years. The SDT has provided guidance on the acceptable documentation for an exception to the seven year criminal history records check which includes agreements with labor unions. If the registered entity is unable to fully complete the seven year criminal history records check, the SDT feels it is important to document the reasons for the exception so it will not be removing that piece of the requirement. Also, the timeframe for renewal of the criminal history records check is currently seven years and the SDT believes it should remain as such. Drug and alcohol checks are typically performed by entities under an existing program and the SDT chooses not to add this to the requirement. In section 3.3 of the new Table R3, the term process is used to define the method used by a registered entity to evaluate the results of the criminal history records check. Although a "Transportation Worker Identification Credential (TWIC)-like" program would be helpful to facilitate compliance with the PRA requirements, the SDT does not have the authority to make that happen. Measures – The Measures have been revised to focus on examples consisting of documentation. For example, a dated copy of the current PRA, which was performed in the previous seven calendar years, would be sufficient.

VRF/VSL

The language in the VRF for R2 has been changed to remove the reference to role based training. The SDT reviewed the VRFs for R3, R4 and R5 (as indicated above, R3 from draft 2 is now in R2, and R4 and R5 from draft 2 have been combined into R3 in draft 3) to consider if the rating should be a Lower risk factor. The SDT believes the risk associated with violations of these requirements is higher than for R1 and R2; hence the Medium risk factor is appropriate. The VSL for R1 has been modified to include the case where the Responsible Entity failed to implement on-going security awareness for two or more consecutive quarters as the next step above the criteria for High. Since the Medium severity level is for missing two content topics, the High should follow as three or more, not four or more. Commenters also asked whether the size of the company matters in the VSL for R3 (which is now in R2). In response, the SDT has modified the VSL for High and Severe according to the suggestion. The VSL targets the BES Cyber System and does not account for company size. Commenters suggested the Moderate and High VSL language for R4 (now R3) should be swapped on the basis that not performing an identity verification and a background check is worse than failing to document the results. (Also, the incorrect reference in draft 2's R4 to "4.5", which does not exist, has been corrected). In response, the SDT has modified the language for the Severe VSL to include the case where a registered entity failed to implement its PRA processes. Commenters also asked whether the size of the company matters in the VSL for R5 (which is now in R3). In response, the VSL targets the BES Cyber System and does not account for company size.

QUESTION B9 – CIP-004-5, R6 or R7:

If you disagree with the changes made to CIP-004-5, Requirements R6 or R7 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the major concerns with CIP-004 Requirements R6 and R7 center on removal of access privileges under various categories of termination actions. In addition, there were repeated instances noting a lack of clarity regarding access approvals, personnel transfers or reassignments and the proper storage and handling of NERC CIP information.

Note

In draft two, Requirement R2 required a documented process for its role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems while Requirement R3 was the implementation of that process. Requirement R4 required one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems while Requirement R5 was the implemented of the one or more documented processes. In preparing CIP-004-5 for draft 3, the SDT determined that Requirements R2 and R3 could be combined, and so could Requirements R4 and R5. In that way, the requirements more closely match most other requirements in CIP-004-5 through CIP-011-5 to implement a documented process, and it also facilitated inclusion of the correcting deficiencies approach, explained in the common response section of this comment response, so that the resulting requirements, draft 3's Requirements R2 and R3, could be implemented "in a manner that identifies, assesses, and corrects deficiencies." Therefore, Requirement R6 from draft 2 was renumbered to Requirement R4 in draft 3, and Requirement R7 from draft 2 was renumbered as Requirement R5.

Applicability Section

As in other Version 5 standards, in CIP-004, requirement part 4.1 (formerly part 6.1), there were several comments on changing instances of Medium Impact BES Cyber Systems to "Medium Impact BES Cyber Systems with External Routable Connectivity." Commenters also commented that "dial-up connectivity" should be removed from the applicability section to be consistent with the applicability sections of other Version 5 standards. In both of these cases, the SDT has revised the standard to reflect these comments.

Requirement R4 (formerly R6) General Comments

Multiple commenters recommended that new or additional items or items currently found in the rationale section should be modified and listed as requirements at the requirement level.

Comments suggested modification to allow for self-correction in certain cases, so that each responsible entity shall implement: measure performance to detect flaws; correct detected flaws expeditiously, and if needed take corrective action to prevent recurrence of flaws. This is a general requirement that applies to the Requirement R4 (formerly R6) sub requirements. Though not necessary from a procedural perspective, more instruction on what needs to be considered in the standards is better than insufficient information. The SDT has incorporated the correcting deficiencies modification to the implementation wording in CIP-004-5 in Requirements R2, R3 and R4.

Commenters recommended that the rationale discussing controls for BES Cyber Systems without user accounts should be added to the appropriate requirements in Requirement R4 (formerly R6). The SDT has moved that discussion from the rationale section to the requirement tables.

A commenter suggested that requirement parts 4.2, and 4.3 (formerly covered in parts 6.2, 6.3 and 6.4) be modified to include requirement parts 4.11, 4.12 and 4.13 (formerly parts 6.11, 6.12 and 6.13) along with part 4.1 (formerly part 6.1) in the requirement table. The SDT has combined requirement parts 4.2, 4.3 and 4.4, which now directly reference those sub-parts in part 4.1.

R4.3 (formerly 6.3)
Commenters recommended that there be a corresponding annual review of provisioned physical security privileges necessary for performing assigned work functions. The SDT has combined requirement parts 4.2, 4.3 and 4.4 (formerly parts 6.2, 6.3 and 6.4). The measures in the new requirement part 4.2 call for signed documents, automated workflow approvals or email showing persons with access have authorizations and similar or the same records showing the consideration of appropriate privileges on the basis of need…" These measures apply to electronic access, unescorted physical access into a PSP and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Part 4.3 (formerly part 6.5)
Commenters asked for clarification on the reviews of authorized and provisioned electronic access and unescorted physical access. The SDT has modified part 4.3 to clarify the requirement. It now reads "verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records."

R4 (formerly R6)

Some commented that the measures for 4.1 (formerly part 6.1) should include unescorted electronic access. The issue with this is that electronic access, by its digital nature cannot be escorted. Consequently, there is no "unescorted" electronic access. Electronic access to data or systems is either authorized or unauthorized. One could call it "supervised" access but the problem lies with a "supervisor" having to be continuously diligent and unerringly able to determine if the supervised user is doing anything malicious. This is not possible and frankly constitutes a threat to network integrity and data confidentiality. The recommended option would be to identify those contractors who require electronic access and run them through the personnel appraisal and the training processes and grant them appropriate access privileges. There are no other means to help ensure there are no unauthorized accesses or data disclosures.

Requirement Part 4.1 (formerly 6.1)

One commented that formerly sub-requirements 6.1.1, 6.1.2 and 6.1.3 (current 4.1.1, 4.1.2 and 4.1.3) would be clearer if the requirement was written, "Designate one or more individual(s) to authorize one or more of the following types of access". The SDT has changed the requirement to "have a process to authorize". This negates the need to specifically identify an approver and highlights consideration of "need" for physical access, electronic access and access to "designated" physical and electronic storage locations for BES Cyber System Information.

One commenter suggested that current requirement part 4.1 should include the names and roles of individuals who authorize the various types of access. The SDT has changed the requirement to "have a process to authorize". This negates the need to specifically identify an approver and highlights consideration of "need" for physical access, electronic access and access to "designated" physical and electronic storage locations for BES Cyber System Information.

One commenter recommended changing the term "designate" in current requirement parts 4.1, 4.2 and 4.3 (formerly parts 6.1, 6.2 and 6.3) to "identify.' The SDT has changed requirement 4.1 to "have a process to authorize". This negates the need to specifically designate or identify an approver and highlights consideration of "need" for physical access, electronic access and access to "designated" physical and electronic storage locations for BES Cyber System Information. The SDT has also combined 4.2, 4.3 and 4.4 into a single requirement (4.2).

Several commenters pointed out that access to physical and electronic locations where BES Cyber System Information is stored should have greater clarity around the word "physical". The requirement part 4.1 (formerly part 6.1) has been

changed to clarify storage locations for BES Cyber System Information. It now reads, "access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Several commenters recommended revising the phrase "unescorted physical access" to "unescorted physical access into a PSP." The SDT agrees and has made that change.

Multiple commenters stated that requirement part 4.1 (formerly part 6.1) should allow for roles in the designation of those individuals who can authorize the various accesses. The SDT believes that changing the requirement to "have a process" allows the entity the flexibility to construct their authorization process in a way that best suits their needs.

Requirement Part 4.2 (formerly Part 6.2)

Several commenters recommended that requirement parts 6.2 and 6.3 be revised for clarity. They proposed that requirement parts 6.2 and 6.3 be changed to read, "the individual(s) or role(s) designated in requirement part 6.1 shall authorize electronic access deemed necessary by the Responsible Entity, except for CIP Exceptional Circumstances." To respond to the comment, requirement parts 4.2, 4.3 and 4.4 have been combined into a single requirement part 4.2. At the same time, the individual authorization has been replaced with a process in requirement part 4.1. The process merely provides a means to authorize, and is implemented in the manner preferred by the Responsible Entity.

Several commenters also suggested that instead of the phrase "deemed necessary," "deemed appropriate" would be more accurate – stating that deeming appropriate is easier than deeming necessary. The SDT used the term "necessary…for performing assigned work functions" to better focus on specific accesses and minimize generalization and audit interpretation issues.

One commenter suggested the phrase "Responsible Entity" be removed from parts 4.2, 4.3 and 4.4 (formerly 6.2, 6.3, and 6.4). The requirements state "that the Responsible Entity determines is necessary." The SDT believes that the term "Responsible Entity" removes a degree of specificity that could be problematic if individuals change frequently or the determination of "necessary" is made by more than one individual within the organization. The SDT has combined requirement parts 4.2, 4.3 and 4.4 and has referenced a process required in part 4.1 "have a process" that allows flexibility to establish authorization frameworks tailored to the Responsible Entity's needs.

One commenter stated that the phrase "need to know" in requirement part 4.2 (formerly Part 6.2) is difficult to quantify and is subject to interpretation. They recommended removing that phrase, believing that approvers who grant all access

"deemed necessary" strongly indicates that determinations of need to know are part of the authorization process. The SDT has removed references referring to "need to know."

Many commenters recommended revising the phrase "unescorted physical access" to read "unescorted physical access into a PSP." For clarity, the SDT has changed the wording to "access into the Physical Security Perimeter."

One commenter stated that requirement part 6.3 (now covered under new part 4.1) implies that determination of need for performing work functions is needed for each physical access. They recommended that Responsible Entities document all roles and activities in advance, negating the need for the Responsible Entity restating access they have "determined is necessary." The SDT has combined the requirement parts 4.2, 4.3 and 4.4 and established a requirement for a "process" to develop an authorization framework best suited to the Responsible Entity's needs. This will allow the commenter's company to document all roles and activities in advance if that is the company's preference.

One commenter recommended removal of the phrase "for performing assigned work functions" due to concerns with potential interpretation requests. The SDT believes that since "work functions" are not subject to audits, there is no need to remove the conditional phrase. In addition, there must be some frame of reference for authorizing accesses and work functions are a logical baseline.

Many commenters suggested changing the wording of requirement part 6.4 (now covered under new part 4.1) from "location" to designated repository. The SDT believes that specifying a designated location is less subject to interpretation and in most cases exempts portable equipment from being identified as a "repository" in the event that NERC CIP information may be temporarily resident on such equipment. The SDT has retained the term "designated locations" since a location more often connotes multiple purposes. In contrast a repository, similar to location by definition, still carries connotations of a specified area, limited to a specific function. "Location" provides flexibility and designating locations removes incidental temporary storage on non-designated devices from the audit process.

One commenter questioned the following: Is the "intent of the requirement to track authorized access to the physical and electronic locations where BES Cyber System Information is stored. Is the requirement regarding physical location intended to include physical access to file servers hosting BES Cyber System Information in electronic format or is it intended to be limited to physical access to locations where BES Cyber System Information in stored in hardcopy format?" The SDT believes that unescorted physical access includes to both hard copy data and access to equipment used for storing electronic copies. Although physical proximity to equipment does not constitute electronic access, from

an information protection standpoint, access to that equipment could result in damage or destruction of those devices storing electronic copies.

One commenter suggested that in requirement part 6.4, (now covered under new part4.1)to eliminate ambiguity, that the term “necessary for performing assigned work functions,” be replaced with “appropriate for the roles and responsibilities.” The SDT understands the concern. In this case replacing “necessary” with “appropriate” does little to eliminate ambiguity. In addition, both terms are likely to prompt interpretations. Also, not all entities are configured to grant authorizations by roles and responsibilities. To address the entirety of the CIP affected population, the SDT believes that the original wording provides more universal applicability.

One commenter believes that requirement part 6.4 (now covered in new part 4.1) should be separated into two requirements. The first requirement would be to identify the repositories that store either physical media containing BES Cyber System Information (paper copy) or the electronic storage of BES Cyber System Information. The second requirement would be the authorization of access to only those designated repositories that have been identified by the entity. The SDT believes that using the term “locations”, as long as they are “designated” serves the same purpose as an identified repository. Because “designated” has been added to the requirement, so must a measure to acknowledge the existence and itemize “designated storage locations.” This will add another measure but will also reduce the potential for audit interpretation and ambiguity.

One commenter recommended that the words “are necessary for performing assigned work functions” be replaced simply with “are necessary”. The SDT believes that this revision, although more economical, could create a situation where the question is asked “necessary for what?” To avoid that possibility “necessary for assigned work functions” is less likely to prompt questions of scope of authorizations.

One commented that the words “physical and” should be removed because it imposes a requirement to create physical access controls and authorization processes to an office that may have a printout of Cyber System Information. The SDT notes that if, as suggested by a number of other companies, “designated locations” are used, incidental, non-designated temporary locations of NERC CIP System Information will not be subject to that requirement.

Former Requirement Part 6.3

Former requirement part 6.3 prescribed specific ways to conduct authorizations and referenced individuals designated in former part 6.1. The SDT has instead changed the language in part 4.1 to require the Responsible Entity to "Have a process to authorize . . .", which could certainly include designating one or more individuals, etc., as part of the process, but the requirements do not specifically prescribe the administrative method of achieving the required performance. Thus, former Requirement Part 6.3 no longer exists in the same manner as presented during draft 2.

Several commenters stated that because of potential minor errors or mismatches associated with the required review of authorizations and provisioned individuals, requirement part 4.3 (formerly part 6.5) should be subject to the FFT process. The SDT understands the concern, but FFT is not a function of the requirement. That is a function of potential violations and determined after the fact, not in the standard requirement itself.

One commenter recommended that the following statement from the rationale for requirement part 4.3 (formerly part 6.5) be entered into the requirement or its Measures section: "If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement." While that statement offers some clarification in guidance, the SDT cannot add a requirement or measure that makes a determination whether or not a particular error is a violation.

One commenter stated that requirement parts 4.3 and 4.4 (formerly parts 6.5 and 6.6) are major scope expansions which were not directed by FERC. They further claim that the requirements overlap and are not contributing to a commensurate improvement to security. The SDT believes that reviews such as those in parts 4.3 and 4.4 (formerly parts 6.5 and 6.6) do in fact provide a means to identify indicators of malicious activities, rogue accounts, retained accounts that are no longer authorized, etc. The fact that FERC did not direct the requirement development does not negate the validity or the need for the requirements.

Several commenters recommended adding "currently" between "individuals provisioned". The SDT agrees with the recommendation and will take appropriate action. The SDT has reworded the requirement part 4.3 (formerly part 6.5) to "individuals with an *active* electronic access…"

One commenter stated that requirement part 4.5 (formerly part 6.7) should be revised as follows, “Verify, at a timeframe that the Responsible Entity deems necessary, that individuals provisioned for authorized electronic access or authorized unescorted physical access have associated authorization records.” The SDT believes that there must be a specified review period and associated evidence to ensure that Responsible Entities consistently meet the requirement.

One commenter suggested adding the words "to BES Cyber Systems" after the words "physical access" in part 4.3 (formerly part 6.5). The SDT believes this proposed revision is already addressed in the Applicable Systems section of the requirement.

One commenter suggested that in the measures section, there should be consistency of word order between "dated document of verification..." and "documentation of dated verification”. The first measure asks for “dated documentation of verification,” which simply provides a point in time wherein the verifications were performed. The second measure requires a document that provides times of specific verifications themselves, of authorization for access and provisioning of access. The SDT changed the language to provide clarity and consistency to the measure. The consistent language now reads, “dated documentation of the verification.”

Requirement Part 6.4

One commented that the measures in requirement parts 4.4 and 4.5 (formerly parts 6.6 and 6.7) contain contradictory constructions. The background section states that a numbered list includes all required evidence. In the measure, however, these parts state that evidence “may include, but is not limited to.” The SDT has added the phrase “that includes all of the following” to reconcile the format with the intent of the measure.

Several commenters stated that the wording in requirement part 4.4 (formerly part 6.6) is too prescriptive, specifically “verifications that all user accounts, user account groups, or user role categories and their specific associated privileges.” They proposed substituting that wording to read, “verifications that BES Cyber System access privileges are appropriate for the individual(s) or role(s) responsibilities.” The SDT believes that the word appropriate is too vague and subject to interpretation. The goal is to verify access to specific accounts. In this case, the existing wording maintains the scope and leaves no ambiguity around which accounts require verification. Regarding the list of measures, the SDT has revised the measure by adding “that includes all of the following” to reconcile the format with the intent of the measures.

Several commenters stated that the measures should only require verification that the entity performed the verification while leaving the results of the verification out of the measure. The SDT believes that requiring verification should

specify those items to be verified. Asking for a "listing of all accounts/account groups", a "description of privileges", "accounts assigned" and 'verification that privileges are authorized and appropriate" does not expand scope. Confirming that "verification" was performed would assume that all registered entities would perform the verification on the same lists of required items. If the items are not articulated, there are no assurances that the data would be consistently derived or complete.

One commenter recommended changing the words "performing assigned work functions" to "are appropriate". The SDT believes that the use of appropriate to define specific standard provisions is too vague and subject to interpretation.

One commenter stated that the scope of requirement part 4.4 (formerly part 6.6) has been expanded above and beyond what has been directed by FERC. The SDT has taken very positive steps to meet the requirements of the FERC directives. In establishing some requirements, the only way to effectively validate that the provisions have been met is to identify the need for specific information that links the requirement to the compliance actions. There may be an increased number of these instances. The important factor is that FERC directives do not limit the detail of the required evidence. The SDT believes that the requirement and measures increase the level of security. Unauthorized, expired or mis-assigned access to BES Cyber Systems represents potential vulnerabilities that could be exploited if not addressed with these administrative requirements.

One commenter also recommended that the wording of the "annual requirement" be worded as follows, "once each calendar year of a period not to exceed 15 calendar months between verifications." The SDT has changed the requirement to read "once every 15 calendar months to incorporate the additional 3 months of previously discretionary time directly into the requirement."

One commenter believed that the word "all", referring to user accounts is too broad. Dominion suggested that the word "applicable" be added after "all" to point to those user accounts, etc that are directly associated with the requirement. The SDT has changed the requirement to read "user accounts on all applicable cyber assets" to maintain the appropriate scope of the requirement.

One commented that requirement parts 6.6 and 6.7 should be revised to allow responsible entities to perform verifications of user accounts, user account groups or user role categories and their specific associated privileges at "a timeframe that the Responsible Entity deems necessary." NextEra also suggested that this also applies to verifying "access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity

are correct…" Although there are a number of companies that would comply with the requirement according to its intent under a self-imposed timeframe, there is no way to ensure that this would be the case. The SDT feels that the annual requirement should remain in place to help ensure consistent compliance actions.

Several commenters recommended changing requirement parts 6.6 and 6.7 to remove "all" referring to reviews of user accounts, user account groups, or user role categories. They recommend replacing "all" with "BES Cyber Systems." The SDT believes that reviews should be performed only on applicable cyber assets. The requirement has been revised as follows: "that user accounts on all applicable cyber assets, user account groups, etc.

Some commenters also commented that "locations" in requirement parts 6.4 and 6.7 should be replaced with designated repositories and include a requirement to list the repositories. The SDT has reworded the requirement to read "designated storage locations for BES Cyber System Information, whether physical or electronic." It has also added a requirement to designate storage locations and a measure to provide a list of designated storage locations. This will remove incidental temporary storage on non-designated devices from the audit process.

Some commenters suggested that the language in the second measure, "A summary description of privileges associated with each group or role", be removed. The SDT believes that understanding the privileges associated with specific roles is a necessary data point for verification that the privileges for specific groups are authorized and appropriate for the work functions performed by those assigned to the groups.

Requirement Part 6.5

Many commenters suggested in some manner to move former parts 6.1, 6.4, 6.7, and 7.3 (now, collectively, parts 4.1, 4.5, and 5.3) into CIP-011. In response, the SDT has revised former parts 6.1 and 6.4 to require a process without specifying how to conduct the authorizations. The SDT notes that CIP-004-5's authorization requirements relate to individuals' access, while CIP-011-1 specifies the information protection requirements.

Some commenters expressed concerns that the measures of requirement part 4.5 (formerly part 6.7) do not need to include the phrase "the minimum necessary for performing assigned work functions." In response, one of the most important aspects of authorizations and privileges is that they be granted using a "least privilege" approach. Otherwise the possibility exists that authorizations are provided or maintained for individuals who do not need them based on expediency rather than a comprehensive review.

One commenter suggested removing the term “minimum” from the third measure of Part 4.5 (formerly part 6.7) since it was removed from the requirement. The SDT agrees with this suggestion and has revised the measure accordingly.

One commenter recommended that the word “privileges” be added to part 4.5 (formerly Part 6.7) after the word “access.” The proposed wording of the requirement would be “verify at least once per calendar year, but not to exceed 15 calendar months between verifications, that access privileges to the designated physical and electronic repositories where BES Cyber System Information is stored by the Responsible Entity are correct and those that the Responsible Entity determines necessary for performing assigned work functions." The SDT concurs with this addition since it adds clarity to the requirement. It has added “privileges” to the requirement. In a related recommendation, another commenter suggested the word “privileges” be removed from the measure since it is not in the Part 4.5. Adding the word privileges as discussed above will alleviate those concerns.

Some commenters recommended removing requirement parts 4.4 and 4.5 (formerly parts 6.6 and 6.7) because they are too prescriptive in their attempt to accomplish requirement part 4.3 (formerly part 6.5). The SDT believes that verification of requirement part 4.3 hinges upon the existence and validation of requirements listed in 4.4 and 4.5.

One commenter also questioned whether a listing of authorizations is the same as a list of those with access. Authorizations provide a type of eligibility for access. A list of those with access may include someone without that authorization and a potential security issue. That is why the reviews of authorizations, access and privileges are critical to compliance with the standards requirements.

Requirement R5 (Formerly R7) Applicability Section

A few commenters suggested that the applicability of revocation requirements in CIP-004-5 R5 (formerly R7) for interactive remote access should be modified to exclude dial-up connectivity. In response, the dial-up connectivity reference is removed from CIP-004-5 in its entirety.

Commenters also recommended that applicability to “Medium Impact BES Cyber Systems” be limited to those with “External Routable Connectivity” to maintain consistence with other cyber systems/assets currently covered by similar requirements in CIP-004. External Routable Connectivity has already been added to the applicability section for CIP-004.

Requirement R5 (Formerly R7) General Comments

Several commenters expressed concern on requirement part 5.2 (formerly part 7.2) for transfers and reassignments. They believe that the timing of access removal should be based on the determination of when access is no longer necessary, rather than limiting it to a specific time frame related to the transfer or reassignment date. The SDT has revised part 5.2 (formerly part 7.2 as follows: "For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access".

For requirement part 5.1 (formerly part 7.1), a commenter suggested that part of the FERC Order 706 be more clearly reflected in the requirements. Specifically they would like documentation in the requirement that highlights FERC's statement that exceptions to revocation policy are allowed as long as they are properly documented for audit purposes. Paragraph 462 of Order 706 states that, "revocation should be immediate upon the employee's notification of any personnel action requiring revocation of access. However, the ERO may define what circumstances justify an exception that is other than immediate and determine what is the fastest revocation possible." In response, this is not a SDT issue. Creating exceptions for directives in a FERC Order is a separate process undertaken by the ERO. In any event, it is not simply a documentation requirement. Circumstances warranting exceptions have to be identified and then approved. This of course is done against a backdrop of "immediate" revocation stated in the order.

A few recommended that the requirement for revocation based on the "next calendar day" should be changed to "next business day." Another commenter proposed that "next calendar day" be replaced by "within 24 hours." The SDT believes that next business day does not fall under the intent of the FERC Order Directives. Next business day if a weekend or holiday period is in progress could extend the revocation process for two or three additional days. "Within 24 hours" is actually less time than is allowed by the "end of the next calendar day." For the purposes of these comment responses, the SDT feels that next calendar day best meets the FERC Order directive and provides better security than next business day.

Some commenters also expressed concern that the 24 hour revocation requirements may not realistic given numerous and diverse HR and IT processes throughout the industry. Essentially they, along with one other commenter, advocated returning to a framework that allows different time frames for different types of termination actions. The SDT has revised the requirement to state that there must be a process to initiate removal of an individual's ability for unescorted physical access and interactive remote access. This is based on the premise that removal of the ability for access may be different than deletion, disabling, revocation or removal of all access rights. Considering that what is required is initiating

a process (which may allow for internal processes that serve as trigger points) at the time of the termination action and completing the process within 24 hours, the SDT believes this is a reasonable time frame.

Requirement Part 5.1 (formerly 7.1)
Commenters recommended that the criteria for termination action timeframes should include a reference to the communication of the intention to terminate to provide a type of time stamp for gauging compliance with related requirements of the standard. While the communication of a termination action is not mentioned specifically in the requirement, initiating the process required by requirement part 5.1 (formerly part 7.1) would probably include those trigger points for individual companies. This allows greater flexibility and more concise monitoring of the required timeframe.

Several commenters expressed concern with the format of the measures in Requirements R4 and R5 (formerly Requirements R6 and R7). They are concerned that the background section states that all numbered lists in the measures are all required evidence. However, the measure list states that the "evidence may include but is not limited to." The SDT has revised the measures by adding the following statement: "An example of evidence may include, but is not limited to *documentation of all of the following*: This sentence is followed by numbered measures. This is primarily a formatting issue and this revision should alleviate the discrepancy.

One commenter suggested that the requirement should include "disable or revoke all individualized domain user accounts held by the terminated staff." The SDT believes that removing unescorted physical (preventing any entry into an entity's facilities) and interactive remote access should prevent any further access by the individual after termination.

Some commenters stated that requiring access revocation within 24 hours for all types of terminations is overly burdensome. They believe the 24 hour requirement should be limited to "for cause" terminations with additional flexibility built in for other situations. Other commenters recommended that the 24 hour time frame should apply only to High Impact Assets. The SDT has revised the requirement to state that there must be a process to initiate removal of an individual's ability for unescorted physical access and interactive remote access. This is based on the premise that removal of the ability for access may be different than deletion, disabling, revocation or removal of all access rights. Considering that what is required is initiating a process (allowing for internal processes) at the time of the termination action and completing the process within 24 hours, the SDT feels this is a reasonable time frame.

A few commenters stated that requirement parts 5.1 and 5.5 (formerly parts 7.1 and 7.5) seem inconsistent regarding shared user accounts. The SDT sees no inconsistency and believes that the current requirements are clear and sufficiently differentiated. Requirement part 5.1 considers the first tier of access; unescorted physical and interactive remote electronic access. Requirement part 5.5 specifies changing passwords for shared accounts and provides a 30-day time frame for its completion.

One commenter recommended a change to part 5.1 formerly part 7.1) that changes the 24 hour requirement to the end of the next business day after the effective date and time of the termination action. The SDT believes this falls outside of the FERC Directive intent, particularly as it applies to the "next business day." The next business day could increase the access revocation time frame to well over the 24 hours currently stated in the requirement.

One commenter recommended that requirement parts 5.1 and 5.3 (formerly parts 7.1 and 7.3) be revised to include a statement on extenuating circumstances associated with the impact of completion of revocation within 24 hours. FERC has allowed "extenuating operating circumstances" which have a specific application in requirement part 5.5 (formerly part 7.5), due to the complexity and scope of the password change task. Extenuating circumstances outside of that definition are undefined and could be misconstrued as any circumstance that is perceived as an impediment to completion of the requirement. In addition, adding "extenuating circumstances" to these requirements could set a precedent for other requirements, negating the timeliness and effectiveness of underlying security intent.

One commenter suggested clarifying language to the wording of the requirement to make it clear that the 24-hour clock is related to the initiation of the termination process, not the complete termination actions themselves. The SDT has clarified that there must be a process to initiate removal of an individual's ability for access. Initiation of the process must be concurrent with a termination action. Completion of the removal is required within 24 hours of initiating the process.

One commenter believes that termination criteria should vary according to the situation. They would like the tightest timeframes reserved for terminations for cause. The SDT has maintained the 24 hour requirement for termination actions based mainly on the FERC 706 Order requirement that termination be executed immediately.

One commenter commented on a situation where a suspended individual is terminated ten days from the suspension date. While the termination action was initiated in compliance with the requirements of R5 (formerly R7), the effective date of the termination shows up in the records as 10 days prior to the action being initiated. The SDT believes that in

these situations, documentation of the suspension along with what a suspension entails regarding any network or system accesses, and a documented company statement verifying the entities suspension procedures and subsequent termination should be sufficient to provide evidence of compliance to an auditor.

Requirement Part 5.2 (formerly 7.2)
Many commenters are concerned about the 24 hour requirement for removal of access for those individuals transferred or reassigned. The SDT understands the issue with access often being required after the transfer for various lengths of time. Rather than specify numbers of days within which an entity must complete the reassignment or transfer activities, the SDT has reworded the requirement to the following: "For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access."

One commenter would like reassignments or transfers based on the notification of reassignment or transfer. Rather than specify numbers of days within which an entity must complete the reassignment or transfer activities, the SDT has reworded the requirement and proposes the following changes: "For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

Requirement Part 5.3 (formerly 7.3)
A few commenters requested clarification on physical access to BES Cyber Systems and storage requirement wording in general. The requirement specifies that the access applies to those "designated physical and electronic locations where BES Cyber System Information is stored." In the requirement the term "designated" has been added. For the measures, evidence includes workflow or sign-off forms verifying access removal to "designated" physical areas or cyber systems. The term designated removes the unintended consequence of BES Cyber System Information temporarily resident on work stations, laptops, flash drives, etc. These areas are consequently not identified as storage "locations."

Some commenters suggested replacing the words "by the end of the next calendar day" to "within 7 days" or 30 days, respectively in the requirement. The SDT believes that since access removal in requirement part 5.1 (formerly part 7.1) will in many cases, constitute removal of access to BES Cyber System Information, that this requirement should retain its

original wording. In addition, in FERC Order 706, Paragraph 386 requires that there be "prompt revocation of access to protected information." Seven or 30 days would not be considered "prompt" by FERC.

One commenter commented that "next calendar day" for removal of access to BES Cyber System Information is too short a time span. The SDT points out that FERC Order 706 dictates prompt removal of access. The phrase "next business day" for example could mean substantially longer time periods over weekends and some holiday periods.

One commenter recommended the use of the word "repository" over "locations" in the requirement. The word "location" was chosen by the SDT to ensure there was no ambiguity within the requirement. Location is considered a general area, with multiple uses and is not limited to a specific function. A "repository" on the other hand, connotes specific use…for storage of BES Cyber Security Information. The use of location will help avoid any tendency toward requiring exclusivity of purpose and preclude potential violations.

One commenter commented that locations should be changed to designated repositories. The SDT believes that specifying a designated repository is less subject to interpretation and in most cases exempts portable equipment from being identified as a "location" in the event that NERC CIP information may be temporarily resident on such equipment. The SDT has retained the term "designated locations" since a location more often connotes multiple purposes. In contrast a repository, similar to location by definition, still carries connotations of a specified area, limited to a specific function. "Location" provides flexibility and designating locations removes incidental temporary storage on non-designated devices from the audit process.

Requirement Part 5.4 (formerly 7.4)

Some commenters would like to expand the applicability of requirement part 7.4 to include Medium Impact BES Cyber Systems. The SDT has carefully weighed the applicability of requirement parts throughout the family of Version 5 CIP standards, and, on balance, it believes that the levels of protection for Medium Impact BES Cyber Systems in other requirement parts throughout CIP-004-5 provide an appropriate balance in applying impact-based protections that are graduated between High Impact BES Cyber Systems and Medium Impact Cyber Systems.

One commenter suggested a revision for recovery of all information copied from repositories. The SDT notes that the requirements set out the requirements that must be part of the required processes. The SDT believes that the information protections in CIP-011-1 and the access requirements in CIP-004-5 adequately serve the purpose of protecting BES Cyber Systems while allowing sufficient flexibility to entities in implementing their processes or programs.

A few commenters recommended changing “Requirement parts 5.1 and 5.3 (formerly parts 7.1 and R7.3)” to “Requirement R5, Parts 5.1 and 5.3 (formerly R7 Parts 7.1 and 7.3.”)They also recommended changing the word “removal” to “revoke” for consistency with the requirement. Another commenter also suggested changing “revoke” to either remove or disable. In some systems removal results in removing all corresponding records which makes it hard to provide the proper records to the auditor. The SDT has retained “removal” in part 5.1 along with a clarification which is provided in the requirement language. The SDT retained the term “revoked” in part 5.3 to conform to the overall R5 Requirement.

One commented that the phrase "revoke individual users accounts on BES Cyber Assets" should be changed to "revoke individual access to BES Cyber Assets." The commenter believes that this is an important distinction because most field BES Cyber Assets do not have individual user accounts. In the utility field environment many brands and models of devices are being used. For those that do have individual user account capability, they are often not used because most BES Cyber Assets cannot be centrally managed. Since the process of revoking access privileges on each device can take up to a year or longer because it requires a site visit to each asset and for system with a significant number of assets which also covers a large geographic area that effort in combination with the necessary equipment outage to make the change introduces new reliability risks to the BES. It is more common for the commenter’s field organizations to place other access control devices in front of such field devices. These other devices can be centrally managed. So access is controlled to the device rather that by the device itself. Field Example: Protective Relays - Most do not have individual user accounts. Many also do not have the capability to allow central access control management. Because they don't have user accounts the only way to revoke access on the devices is to change the passwords for all access levels. This means logging on to many hundreds to possibly thousands of relays to change passwords. Because access to the relays to change passwords opens the relay at the change level, it presents an increased risk to the BES because it requires a physical equipment outage to make the change resulting in many more outages impacting potentially the state of the BES and once access is granted, one can change any type of setting on the relay. It certainly could not be accomplished in 30 days. Access can be revoked to these assets by revoking the Central Electronic Access Privileges that allow access through the access control devices to the assets. This coupled with physical access revocation (both of which can be centrally managed) provides complete revocation of access to the assets. This can be accomplished a very short time.

One comment suggested that in CIP-004 R5.4 (formerly R7.4): “For Termination actions, revoke the individuals user accounts on BES Cyber Assets…” to, for termination actions, revoke the individuals access to BES Cyber Assets…” The SDT has modified part 5.4 to read, “for termination actions, revoke the access to individual’s user accounts (unless already

revoked in accordance with requirement parts 5.1 or 5.3) (formerly parts 7.1 and 7.3) within 30 calendar days of the effective date of the termination action."

Some commenters disagreed with the statement that the word "revoke" in this case means to "delete" the user account from the system. We would disable the account and possibly change the account password but when you delete a Windows account you can never reclaim the original Globally Unique Identifier (GUID that Windows assigns to the unique account. Therefore, reporting, file ownership and anything relating to the GUID will have been lost and difficult to track past account activity. This may be true for other operating systems as well. If disabling their domain accounts and physical access effectively terminates access, do we still need the urgency of 24 hrs? I understand the logic behind this but would rather see this as a 30 day requirement. The SDT has used the term revoke to essentially make an account "inactive". It does not delete the account. Also, requirement part 5.4 has been modified in the "Applicable Systems" section. It now includes only "High Impact BES Cyber Systems and Electronic Access Control or Monitoring Systems that are associated with High Impact BES Cyber Systems." Further, the requirement allows revocation of individual's user accounts within 30 days of the effective date of the termination action.

One commenter questioned that since there is no requirement for revocation of balance of access in 5.4 (formerly part 7.4) for Medium Impact BES Cyber Systems, is there a particular timeline required? The commenter recommended that a timeline be developed that provides auditable records for removing balance of access. In response, the SDT notes that requirement part 5.4 in the applicable systems does not include Medium Impact BES Cyber Systems. Under those circumstances the audit process would not be considering Medium Impact balance of access.

Requirement Part 7.5

One commenter points out that requirement part 5.5 (formerly part 7.5) only accounts for the 30 days within the requirement and not the 10 days after "extenuating operating circumstances". The SDT has provided measure in part 5.5 to cover that previous omission.

One commenter suggested that the second bullet of the example evidence for requirement part 5.5 (formerly part 7.5) should be clarified that password reset is only required if the individual being transferred no longer needs such access in the new position or role. In response, the SDT has modified the measures to clarify that password resets must be completed within 30 days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

One commenter recommended that requirement part 5.5 (formerly part 7.5) be revised to include both terminations and reassignments or transfers. The SDT has added part 5.5 to the requirement to cover the reassignments and transfers.

One commenter suggested that the quarterly review should be converted to a quarterly “cleanup” of individual user accounts and not be considered a violation, and the SDT notes that that a cleanup could certainly a way of identifying, assessing, and correcting any deficiencies, which now modifies “implement” in the main requirement (see summary response to common issues at the beginning of this document), and for that reason, the required performance of the requirement remains a review.

One commented that if an entity can determine and document that extenuating operating circumstances require a longer time period for changing passwords; it should also apply to allow the Responsible Entity to determine and document that extenuating operating circumstances that can require a longer time period for revocation of access privileges. The SDT believes that since revoking physical and interactive remote (tier 1) access is typically a centralized and relatively uncomplicated process, that the time frames for completion are adequate. In addition, the FERC Order 706 requires “immediate” revocation of access. Providing a conditional caveat “for extenuating operating circumstances would in all probability meet with FERC resistance and result both in subjective application and interpretation.

One commenter questioned the need to modify passwords for shared user accounts if there is no corresponding requirement to disable individual accounts for the user who was reassigned or transferred. Additionally, as passwords are not a required authentication mechanism, we recommend that this requirement be modified to "change any shared authentication factors that are known." The SDT has revised requirement part 5.5 (formerly part 7.5) to accommodate reassignments and transfers as well as termination actions. Requirement part 5.5 reads, “For reassignments, or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.”

QUESTION B12 – CIP-005-5, R1:

If you disagree with the changes made in CIP-005-5, Requirement R1 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language

SUMMARY:

Based on stakeholder comments, the SDT made significant changes to CIP-005-5 Requirement R1.

General Comments

One commenter suggested that the communications links between ESP's should be included and that all the External Routable Connectivity exclusions should be eliminated. In response, all BES Cyber Systems have been included within the scope of Version 5 and the blanket exemption filter in CIP-002-5 has been eliminated. The ERC filter is now used on individual requirements where routable connectivity is either needed to meet the intent of the requirement or in general there is insufficient risk from other forms of communication to enforce a mandatory and auditable requirement upon every instance in every registered entity. Communication links have been excluded from this body of standards from the beginning as it is a cyber asset focused standard, and the vast majority of cyber assets used in communications between ESP's are not within the control of the registered entities but are leased services from telecommunication providers.

A few commenters requested clarity around the inclusion of serial devices and another commenter also requested specific clarification concerning the extension of ESPs over large areas via serial communications along with a request for clarification of 'direct serial' used in the guidance. In response, the SDT has focused on the communications requirements of the standards for the highest risk forms of communication – routable protocol networks and public switched telephone network (PSTN) accessible dial-up connections. It is a vital point that all BES Cyber Assets, including all serial devices, are included in the standards and are subject to all the requirements in CIP-003-5 to CIP-011-1 except those where they are specifically excluded. CIP-005-5, however, is focused on those two higher risk forms of connectivity and do not have mandatory requirements on serial, non dial-up forms of communication. As to the extension of ESPs over large areas via serial communications, the SDT notes that ESPs are for routable communication only and the SDT does not envision single BES Cyber Systems being defined in such a way that large geographical areas are involved. It is envisioned that a BES Cyber System would encompass cyber assets at a single site only – larger systems would be broken

at least into smaller systems by site. For example, a registered entity would not define all the components of an EMS including all field Remote Terminal Units (RTUs) as a single BES Cyber System. The components of that system at each location could be grouped together as the BES Cyber System for that location. Registered entities have great flexibility in their declaration of a BES Cyber System, but need to take into account ESPs and PSPs as well as all other applicable requirements as they do so. In response to the 'direct serial', that is used in the guidance as a term that refers to serial communications that is not routable protocol or dial-up in nature.

One commenter stated that clarity is needed concerning how wireless networks are impacted by CIP-005-5. In response, the SDT notes that these standards are at a higher and logical level and stay above the transport level. The SDT concentrated on protecting the BES Cyber Systems regardless of the physical transport in order to state the goal and also to future-proof the standards against an ever increasing variety of transports. Adequately addressing more detailed technical aspects would require standards per transport. However, the SDT does note that the radio/access point of a wireless network should be considered by the Responsible Entity to see if it should be included as an EAP.

Introduction Section

There was a comment that in the introduction section concerning exemptions (4.2.4) there is a reference to CIP-002-5 that should be CIP-005-5. In response, the SDT has made the change.

Background Section

One comment stated that the applicability of the background section does not address High Impact BES Cyber Systems with External Routable Connectivity and this is used in the standard. In response, the SDT agrees and has added the appropriate language which reads, "**High Impact Protected Cyber Systems with External Routable Connectivity** – Only applies to High Impact Protected Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the Protected Cyber System that cannot be directly accessed through External Routable Connectivity."

One comment read that Medium Impact BES Cyber Systems at Control Centers should be "associated with" instead of "located at". In response, the phrase 'located at' is used to appropriately limit the scope as the case could be made that

every Cyber Asset is ultimately 'associated with' a control center and could inappropriately identify every Cyber Asset as high impact.

One commenter stated that the section concerning Medium Impact BES Cyber Systems with External Routable Connectivity have the last sentence be deleted as it requires not treating the cyber system as one system, but as individual Cyber Assets. In response, there are several requirements (CIP-007-5 in particular) that do apply at the individual cyber asset level within a system and this sentence clarifies that for those requirements only those cyber assets within a system that have external routable connectivity are in scope if the requirement has this applicability.

Requirement Part 1.1

Many commenters commented that the applicability should include the ERC filter and thus remove the applicability language from the requirement itself and also make it parallel with R1.2, potentially even combining R1.1 and R1.2 into one. In response, the two requirements are purposely not parallel. R1.1 requires an ESP (a *logical* border) around every routable protocol network that contains a BES Cyber System even if it is an isolated network and has no external connectivity. The logical border (ESP) is used then as a boundary to define the 'associated Protected Cyber Assets' and raise the impact level of the included Cyber Assets to the 'high water mark' of the highest impact level system in the ESP. R1.2 is an additional requirement for those networks that have external routable connectivity to protect that external connectivity. In essence, Requirement R1.1 is the "identify your associated PCA's and adjust your impact levels" requirement. R1.2 is where external routable connectivity comes in and the logical border becomes more physical with the requirement of Electronic Access Points (EAPs).

Many commenters responded that the applicability needs to be removed from the requirement and the measure. Others commented that Associated Protected Cyber Assets should be included in the applicability as well. In response, the SDT has added the Associated Protected Cyber Assets to the applicable systems column.

There was one comment which stated that documentation on ESP's on isolated networks provides no reliability benefits. In response, the standards are concerned with all threat vectors, not just those originating from external networks. Portable media and insiders are two of many other threat vectors that can reach isolated networks. The SDT feels that knowing what all other network neighbors are on even isolated routable protocol networks containing a BES Cyber

System (the 'Associated Protected Cyber Assets') does have a reliability benefit. The logical border concept of the ESP also defines a 'trust zone' where all Cyber Assets sharing a network with a BES Cyber System need to be protected to equal levels, even on isolated networks.

One commenter stated that the measure should allow for documentation at the BES Cyber System level rather than the individual component level. In response, the SDT agrees and has made a change to the measure to allow documentation at either level.

One commenter requested clarification on whether ESPs are required for EACMs and PACMs. In response, the SDT clarifies that ESPs are not required on EACMs and notes that EAPs are EACMs and the standard avoids recursive effect of requiring ESPs around the cyber assets on the ESP. As for PACMs, the SDT notes that without an ability to make a distinction between "field-devices" (i.e. door readers, etc.) and "central servers", requiring ESPs would be problematic. The intent for protecting PACS is primarily through the CIP-007 requirements for authorization, access control, and logging and monitoring for these systems.

Requirement Part 1.2

One comment stated that the phrase "through the ESP" was redundant in light of the definition of External Routable Connectivity and should be deleted which would also eliminate the use of "through" twice in the existing requirement. In response, the SDT agrees and has deleted the phrase.

One commenter wrote that the measures should include a process to verify that all EAP's are identified as providing a network diagram is not sufficient. In response, the SDT notes that the requirement does not call for a verification process thus the measure should not imply that is a requirement. The requirement states the desired end goal and the entity is responsible for providing sufficient evidence. Network diagrams that depict all external routable communication paths with identified EAP's are listed as one possible example.

Several commenters stated that the applicability should be 'Associated PCA's with ERC'. In response, the SDT agrees and notes that the PCA for this requirement part are associated with high and medium impact BES Cyber Systems with External Routable Connectivity.

Requirement Part 1.3

A few commenters expressed concerns regarding the monitoring and documentation of all outbound traffic. Inbound only monitoring on PSPs is sufficient and suggest dropping the outbound on ESPs. In response, the SDT believes this is an essential element in combating today's electronic attacks and reiterates the following from the included guidance: "The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked."

Several commenters suggested that the applicability should be "Medium Impact BCS with ERC". In response, the SDT notes that the applicability is to EAPs that are associated with High or Medium Impact BES Cyber Systems specifically. If these applicable systems have no External Routable Connectivity, then they will have no EAPs and the requirement therefore does not apply to those systems.

One commenter suggested that the word "rationale" should be changed to "reason." In response, the SDT agrees as this makes the requirement language the same as that used in the measures and in the change rationale. The change has been made.

One commenter noted that tracking the rationale for 60000 ports is burdensome and asked that this be changed to allow for this on a class basis or 'criteria'. In response, the SDT notes the requirement does not require that all 65535 ports be documented as this is a 'deny by default' requirement and only the remaining open ports (those that 'grant access') should be documented. A necessary step in preventing rogue communications to or from a BES Cyber System is to know what the normal communications include and why they are needed.

Requirement Part 1.4

Multiple commenters stated that R1.4 is essentially the same as CIP-007-5 R5.1 and suggest that dial-up be added to CIP-007-5 R5.1 and R1.4 deleted to avoid potential double jeopardy. In response, the SDT notes that CIP-007 R5.1 is specific to user access, while CIP-005-5 R1.4 applies to any access including machine to machine. CIP-005 concerns the security of the 'network' level and requires that there be some form of authentication before a 'network' connection is established to the BES Cyber System. In essence, there should be some form of EAP-like functionality on dialups. Once a connection is made, then CIP-007 applies as we've moved from the 'network' level security to device level security and any user access has to be authenticated at the device.

One comment suggested that R1.4 should be deleted as it is included in R2. In response, the SDT notes that this requirement requires some form of authentication for all dialup connectivity regardless of whether it is machine or user based, while R2 only applies to 'Interactive Remote Access' which is user-based. The intent of R1.4 is that no BES Cyber System, which by definition can have a 15 minute impact on BES reliability, should be directly reachable by simply dialing a phone number, regardless of how it is intended to be used. Therefore R2 contains requirements that are in addition to R1.4 when the intent of the connection is user based Interactive Remote Access.

Several commenters asked if an entity has no dialup capability to applicable systems, are they required to have processes that would authenticate this access? The commenters suggested that the qualifier 'if applicable' be added. In response, the SDT notes the applicability column states that it only applies to systems "with dial-up connectivity" and therefore if an entity has no such systems, there are no systems to which this requirement applies and no process is required. The complete applicability of all requirements throughout the standards is contained within the applicability column and therefore every requirement in the standards has an implied 'if or where applicable' clause.

One commenter suggested that the "where technically feasible" clause should be changed to 'within system capabilities.' In response, the SDT notes that BES Cyber Systems, which by definition can have a 15 minute impact on BES reliability, should not be directly reachable by simply dialing a phone number. If that is not an inherent capability of the system,

then the SDT feels it necessary to add additional equipment with this capability to the system or file for a TFE so that a mitigation plan can be documented to handle the vulnerability.

One commenter suggested that 'where technically feasible' should be deleted. In response, the SDT notes the phrase is an indication of where TFE's may even be requested if the requirement cannot be met on a particular system. Since the SDT is not aware of all situations, it is felt that if an entity cannot meet this requirement on a system that they should be allowed to request a TFE and document a mitigation plan if the TFE is granted.

One commenter suggested that "Associated PCA's" should be added to the applicability. In response, the SDT agrees that any dialup connectivity to any system or Cyber Asset within the ESP, which by definition means the Cyber Asset is also routably connected to a BES Cyber System, should be included. The suggested change has been made.

Multiple commenters suggested that the term 'dial-up connectivity' should be defined to avoid future confusion and should include the notion of access from the PSTN. In response, the SDT is adding a proposed NERC Glossary definition of Dial-up Connectivity.

Requirement Part 1.5

Numerous commenters suggested that the measure only specifies IDS technology and should be made more generic to match the requirement. In response, the SDT agrees and has changed the measure to match the requirement, using IDS as one example.

There were multiple comments that detecting 'malicious' communications requires knowing the sender's intent. Malicious traffic may indeed appear normal. In response, the SDT is adding the phrase "known or suspected" to clarify that the intent is not to detect 100% of all malicious communications, but that communication that has attributes of known or suspected malicious communications.

Multiple commenters asked for clarity as to where the malicious communications inspection should occur and does the direction of the traffic matter. Another commenter stated that only one IDS could be utilized between all ESP's and the

Internet and one per EAP should not be required. In response, the SDT notes the applicability is set at the EAP level and therefore every EAP at Control Centers needs to be covered by the entity's method for detecting malicious communications. The specific architecture and placement is not prescribed. The SDT notes that since this applies to Control Centers, both inbound and outbound traffic should be subject to the detection and has added clarifying language to the standard. For example, if a BES Cyber System in a Control Center begins sending known malicious packets or attempting to communicate with known malicious 'command and control' hosts on the Internet that would warrant detection here and alerting through CIP-007 R4.

Several commenters suggested that the applicability should change to "Electronic Access Points associated with ESPs at High Impact Sites and Electronic Access Points associated with ESPs at Medium Impact Control Centers" as the current phrasing would suggest the need to implement external routable connectivity in otherwise isolated networks. In response, the SDT notes that the requirement is applicable to EAPs and EAPs are only required where External Routable Connectivity is present, therefore isolated networks would not have EAPs and the requirement would not be applicable. However, isolated networks do have ESPs, so bringing the term ESP into the applicability may further confuse the issue.

There were several comments that raised a concern that the requirement is subjective and may not be feasible for encrypted traffic. In response, the SDT has written this requirement in response to FERC Order 706 and the directive to have two or more security measures at each ESP. The Order further clarifies that this is not simply redundant firewalls, but two separate security measures. The SDT has already reduced the subjectivity somewhat from 'two security measures' to 'detect malicious communications'. In today's technology, this would in most cases (but not all) involve the implementation of an Intrusion Detection System, but the SDT does not want to specify products or toolsets within the CIP standards to help future-proof the requirements. If a better toolset is available in the future that is not called "IDS" we would not want these standards to preclude the use of it, so we've deliberately used admittedly more subjective language ("a method for detecting…") in this case. As to the feasibility with encrypted communications, it is true that the methods will be 'blind' to the content of encrypted sessions but it is left to the entities to determine the relative value between maintaining true end-to-end encryption over terminating the encryption and inspecting the traffic at the ESP. The SDT notes that if the traffic is 'Interactive Remote Access', the encryption must terminate per R2 at the Intermediate Device which cannot reside within the ESP.

In the measures section, there were multiple comments to change the word “and” to “or” and to use bullets. In response, the SDT feels a generic paragraph is easier for clarity than bullets. The measure reads, “Examples of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.”

One commenter suggested that the phrase “where technically feasible” should be added to the requirement. In response, the SDT notes that this requirement is limited to Control Center environments. These are the highest risk locations and the SDT feels that in these instances some form of malicious communications detection (IDS) is always possible on routable protocol communications (EAP’s are required only on routable protocol communications).

One commenter stated that External Routable Connectivity should be added to the applicability. In response, the SDT notes that the applicability is to EAP’s which are only required for routable communication points.

Several commenters stated that detection is only one half of the issue and the standard needs to require addressing or mitigating the detected threat. In response, the SDT notes that EAP’s are EACM’s and are thus covered by CIP-007 R4’s Security Event Monitoring requirements and tie into CIP-008. Therefore the SDT feels that the ‘other half’ of the issue is covered by other standards. Xcel suggests that Intrusion Prevention Systems should be included instead of detection systems. In response, the SDT notes that in a control systems environment, the impact of preventing communications that may be the result of false positives may be greater than allowing the communication. Therefore we do not feel it necessary to require in a mandatory and enforceable manner that all suspected malicious communications should be prevented in all situations. That decision is best made by the Responsible Entity based on the specific situation and potential impacts.

One commenter suggested that the Medium Impact should be removed from the applicability as many of the Cyber Assets can’t perform this requirement. In response, the SDT notes that while many Cyber Assets in substations or plants (field locations) may not be able to perform this requirement, the Medium Impact systems are limited to those in Control Centers where the SDT feels the most risk is present and control center systems typically have the most capability to meet this requirement.

Guidance Section

One commenter stated that the guidance for R1 discusses the limitations on the ability of a BES Cyber System to communicate through the EAP and an apparent conflict with the requirement for an intermediate system (jump host) that essentially denies the ability of the Cyber Asset within the ESP to communicate with any other system outside of the ESP. In response, the SDT notes that the Intermediate Device is required only for human-machine interactive login sessions ("Interactive Remote Access") while the Requirement R1 is concerned with machine to machine sessions as well, which do not require an Intermediate Device. Requirement R2 builds upon Requirement R1.4 when the session meets the definition of Interactive Remote Access.

VRF/VSL Section

There was a comment on how the math is done on the VSL for Requirement R1. The SDT has modified the VSL for R1 to remove percentage calculations. We agree the percentage would be difficult to determine in most implementations. Furthermore, the FERC VSL Order addressing CIP Standards discourages specifying failure to document processes as a lower VSL than failure to implement.

There was a comment that suggested the VSL be medium for high impact and lower for medium impact. In response, the VRF by itself does not account for violations from different types of systems, but the SDT expects the impact level of the BES Cyber System to factor into the assessment of penalties.

One commenter suggested the ROP will need to change with changes to TFEs. Although the SDT does not draft Rules of Procedure changes, the SDT expects that this will be a part of the implementation of Version 5.

One commenter recommended modifying the first "Lower" to state: "failed to implement one or more documented processes" to be consistent with the language in Requirement R2. Furthermore, the commenter recommended moving this VSL to the "Severe" category. The lower VSL is intended for the situation where the entity has only failed to document the process(es). Where the entity has failed to implement one of the technology-based solutions listed in the table, those would fall in the moderate to severe categories based on number of technology-based solutions not implemented. The Lower VSL has been revised to clarify this further. Also by the FERC Guidelines for CIP standards, the failure to document processes should be the same level as the failure to implement a process. We have corrected the VSLs for R2.

One commenter recommended that the VSL for CIP-005-5 R2 VSLs be revised to address the approach to detect flaws; correct detected flaws expeditiously. Upon review of the approach to implement preventive, detective, and corrective controls, CIP-005-5 R2 was not identified as a requirement that would be appropriate for this approach. Therefore, the VSL was not modified as requested.

One commenter agreed that the VRF should be medium for the high impact BES Cyber Systems but that the VRF should be lower for the medium impact BES Cyber Systems. In response, VRFs are assigned for an entire requirement and are not assigned to the underlying sub-requirements or parts.

QUESTION B13 – CIP-005-5, R2:

If you disagree with the changes made in CIP-005-5, Requirement R2 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the SDT has made significant changes to CIP-005-5 Requirement R2. The explanations below describe the changes made based on stakeholder comments – the SDT made other minor edits for improved clarity.

TFE Relevance

In response to concerns that the phrase "where technically feasible" should be removed to eliminate reference of maintaining the TFE process, the SDT notes that TFEs will continue to be used in appropriate requirements unless and until such time that the NERC ROP is modified to address exceptional circumstances. The SDT has reviewed each use of a TFE throughout the CIP Version 5 standards very carefully and specifically, and in each instance where that phrase is used, the SDT understands that there may be circumstances where it could be necessary for an entity.

In response to multiple comments that the applicability of TFEs is not clear within the TFE language included in the overall Requirement language, the SDT has moved the TFE language to the table elements.

Applicability

Several comments stated that instances of Medium Impact BES Cyber Systems should be changed to "Medium Impact BES Cyber Systems with External Routable Connectivity". This is a valid concern, and in response, the SDT has added the language to the applicability section of the table.

There was also a comment that the requirement should apply to Physical Access Control Systems and systems serving as ESP Access Points. In response, the SDT believes that since these systems generally do not reside within the ESP of a BES Cyber Asset, it would not be appropriate to apply these Requirements to those Cyber Asset types.

Requirement Part 2.1: Intermediate Device

There was a comment requesting that the reference to Intermediate Device be removed from the requirement. In response, the SDT notes that the Intermediate Device is a defined term that is only used within this one requirement. The device functionality is necessary to ensure that proper protections are put in place for Interactive Remote Access

sessions. The use of Intermediate Devices allow the client machine to exchange data to a Cyber Asset within an ESP without making direct communication and opening the Cyber Asset to vulnerabilities of the client machine.

Several commenters requested improvements to the language in requirement part 2.1 to clarify that a Cyber Asset cannot initiate Interactive Remote Access. In response, the SDT has clarified the language to address this concern by specifying use of an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset. However, the language was not modified to address the person using Interactive Remote Access since the requirement is intended to provide protection from malicious software and communications.

Commenters requested clarification on the location of an Intermediate Device and whether an Intermediate Device can also be an EAP. In response, the SDT notes that the definition of Intermediate Device has only one restriction on the location of the Intermediate Device and that is that the Intermediate Device must not reside in an ESP. Other requirements of the Intermediate Device remain flexible to allow the entity to implement a solution that best meets their needs.

Requirement Part 2.2: Encryption

Several commenters requested that the information regarding the purpose of encryption be removed and added to guidance. The use of "in order to protect the confidentiality and integrity of each Interactive Remote Access session" was intended to help clarify the encryption means that were appropriate.This language has been removed, allowing the Responsible Entity the flexibility to implement the level of encryption appropriate to their organization. Additional references regarding encryption are available in the *Guidance for Secure Interactive Remote Access* document. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

Several commenters requested clarification on the termination point of required encryption. The requirement states the encryption is to terminate at an Intermediate Device. The Intermediate Device may be one or more assets performing the required functions. Encryption should not be perfromed within the Electronic Security Perimeter due to the negative impact on the monitoring for malicious or suspicous communications.

Requirement Part 2.3: Multi-Factor Authentication

Several commenters requested that the examples of multi-factor authorization be removed from the requirements. In response, the SDT has removed the examples from this requirement part, and the requirement part simply reads, "Require multi-factor authentication for all Interactive Remote Access sessions."

Several comments recommended more flexibility regarding the use of multi-factor authentication to allow for future technology changes without a Standards update. In response, the SDT has made this change within the measure so that it is listed as an example, but the requirement can account for future technology changes as commenters suggest.

Many comments requested clarification as to where the multi-factor authentication needs to take place. In response, the SDT has modified the Requirement to state that multi-factor authentication to the Intermediate Device is required for all Interactive Remote Access sessions. Furthermore, the definition of Intermediate Device specifies that access control be performed at the Intermediate Device. The Intermediate Device may be one or more assets performing the required functions.

QUESTION B17 – CIP-006-5:

If you disagree with the changes made to CIP-006-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, there were changes to the applicability section, the requirement parts for added clarity, and removal of unnecessary requirement parts that were documentation related.

General

The "identifies, assesses, and corrects deficiencies" language has been added to Requirement R1 and Requirement R2 since these formerly were zero defect requirements. The SDT believes this is an improvement in the compliance process.

The applicability section was renamed to applicable systems to help clarify the scope of that requirement. Also, the applicable systems entries in each table were reviewed to ensure it matched the requirement language for consistency within this standard and with the other CIP Version 5 standards.

The SDT made changes to table R1 to address concerns on the applicability of requirement parts 1.1, 1.2, and 1.3 that had layered versus exclusive applicability. The table no longer uses layered applicability to be consistent with tables in other CIP standards.

The wording of requirement parts 1.2 and 1.3 has been revised to clarify unescorted access is restricted to those authorized for such access, but escorted individuals can enter a Physical Security Perimeter (PSP).

There was consideration of combining monitoring and issuing an alarm/alert into a single table entry, but these are separate actions and needed separate table entries. Even with separate table entries, each is part of a single requirement.

The SDT has removed the 99.9% availability requirement and requirement part 3.2 to document outages for physical access control, logging, and alerting systems. The Physical Security Plan(s) should address how an entity deals with unavailability of these systems.

Requirement parts 1.4 and 1.5 have been modified to remove the reference to circumvention of a control. The new language is monitoring and issuing alarms/alerts for detected access through a physical access point into a PSP. Designation of physical access points to the PSP should be noted in the physical security plan(s).

A PACS is not required to be within a PSP. Unauthorized physical access is to be restricted. The alarm or alert is for detection of unauthorized physical access similar to the language in requirement parts 1.4 and 1.5, although a PSP is not required.

Data retention requirements that differ from the compliance data retention requirements have explicit language in the requirement table. For example, the retention requirement of 90 days for retention of physical access entry logs is specified in requirement part 1.9.

CIP 006 Requirement R1.3

Language has been added to this table, *"… two or more different physical access controls to collectively allow unescorted physical access into Physical Security Perimeters,"* to clarify that two completely independent physical access control systems are not required. For example, a card key and biometric scan using the same Physical Access Control System for validation is acceptable. Also, the SDT has chosen not to use the words "two factor authentication" since, for example, some field locations could use two separate locks. Further, the SDT believes there may be some locations, particularly for field assets, that may not permit two or more different controls, so the TFE clause remains.

CIP 006 Requirement R1.5 & R1.7

The SDT heard the concerns expressed by industry about when the 15-minute clock begins. The language in the standard has been changed to begin once detected. Also, the language referring to the Cyber Security Incident Response Plan remains as that plan could cover physical incidents related to access to cyber assets.

CIP 006 Requirement R1.8

The SDT has chosen to retain the phrase *"… through automated means or by personnel who control entry."* It confirms in the requirement that a person cannot self-log their entry into a Physical Security Perimeter and that the use of a guard is an acceptable method to log entry.

CIP-006 Requirement R2

This requirement does not state that the visitor control program(s) has to be a standalone document/program. If the entity chooses to include the required language within the Physical Security Plan, that is acceptable.

CIP 006 Requirement R2.1

The language in the parenthetical "*(individuals who are known or guests, and not authorized for unescorted physical access)"* has been removed. A "visitor" is anyone who does not have authorized unescorted physical access inside the PSP. This could include employees, contractors, service vendors, etc. The measure indicates that evidence may include documentation of the visitor control program and visitor logs. There is no reference to "proof" that a visitor was continuously escorted.

CIP-006 Requirement R2.2

The language was edited to correct the implication that a visitor exits to a PSP. Also, the measure was modified to better match with the requirement.

CIP-006 Requirement R3

The SDT considered the suggestion to remove the term "hardware" from the phrase "… locally mounted hardware and devices…" used throughout this requirement. This same phrase has been used in previous versions and is understood to exclude hardware such as door hinges, screws, etc. Also, there is new language in the background section regarding applicable systems that provides additional information on locally mounted hardware or devices.

CIP-006 Requirement R3.1

The SDT believes the key role played by the PACS and associated hardware and devices in protecting High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity warrants a 24-month testing cycle. PACS used for Medium Impact BES Cyber Systems without External Routable Connectivity do not have this requirement.

QUESTION B23 – CIP-007-5, R1, R2, R3 or R4:

If you disagree with the changes made in CIP-007-5, Requirement R1, R2, R3 or R4 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:
Based on stakeholder comments,

General Comments
One entity commented that there is a reference in the 4.2.4 exemptions section that refers to CIP-002 but should refer to CIP-007. In response, the SDT agrees and has made the change.

Several commenters commented that either all VSLs or VSLs for certain requirements should be based on percentage of cyber assets missed. Using percentages based on Cyber Assets on CIP-007-5 Requirements is problematic because Requirements do not have a singular mapping to assets. Also, it is possible for a single Cyber Asset to have multiple violations.

One commented that all Severe VSLs should state the phrase "failed to implement one or more documented." The SDT reviewed this suggestion, and "did not implement" as the SDT proposes is consistent with the SDT's intent.

Requirement R1 General Comments
One commenter suggested that the rationale section for Requirement R1 needs to include physical ports. In response, the SDT agrees and has added this to the rationale.

Several commenters stated that throughout Requirement R1, the applicability for Medium impact should be limited to Medium Impact with external routable connectivity (ERC). In response, the SDT notes that Requirement R1.1 which applies to network accessible ports is already limited to those systems with ERC. Requirement R1.2 refers to physical ports that could be used by someone physically present to inadvertently or intentionally compromise a BES Cyber System. In this case, ERC does not matter and the SDT believes the ERC exclusion should not be considered in this case.

There were a few suggestions that the High Impact systems should include the ERC filter as well. In response, the SDT notes that since Version 1 of the CIP-002 standard, lack of external routable (or dial-up) connectivity has been a blanket exemption everywhere except Control Centers, where even standalone networks were still to be considered as Critical Cyber Assets. Since High Impact in Version 5 refers to Control Centers, the SDT cannot 'go backwards' without sufficient justification, which we believe is absent.

One commenter suggested that the words "and Services" should be dropped from the title as the requirement concerns only network ports. In response, the SDT notes that ports are opened by services and that typically a port is disabled or closed by disabling the corresponding service. The requirement also allows for services that use wide ranges of dynamic ports that need to be enabled to be documented as the service name rather than a dynamic port range. Therefore the SDT believes the 'and Services' is appropriate.

Several commenters stated that the Requirement R1 measures may also include rationale as to why ports are necessary or clarify in the requirement. In response the SDT agrees and has added a specific measure for documentation of the need for all enabled ports.

Requirement Part 1.1

One commenter suggested that the phrase "ports or services" should be "ports and services". In response, the SDT notes that the use of the word "or" is intentional to allow for circumstances where a Cyber Asset uses one service that is on one port, another service that uses a range of ports, or a service that uses dynamic ports without a defined range (e.g. may use anything over 1024). The entity should be allowed to document the enabled single ports, port ranges, or in the case of the dynamic ports, the service that is enabled. Therefore the SDT feels the word "or" is appropriate.

Two commenters suggested that the sentence in the guidance concerning cyber assets that allow for no port management and therefore all open ports are deemed 'needed' should be part of the requirement. In response, the SDT agrees and has moved the sentence to the requirement.

One commenter suggested that the phrase 'where technically feasible' should be replaced with 'within device capabilities'. In response, the SDT notes that devices that do not allow for port management will have their ports determined as 'needed' thus the TFE will be seldom used. However, the SDT wanted to allow for entities to request a TFE for any special cases.

One commenter suggested that the requirement should consider more than listening ports but should also include unexpected connected ports making outbound connections. In response, the SDT notes that this risk is covered at one level by CIP-005's new outbound rule requirement. The SDT also notes that this requirement requires evidence of a known port configuration for the cyber asset and it is unclear how an entity could perform this for 'unexpected' ports.

Several commenters asked for clarification as to how "associated PCA's" applies and is not an independent set of individual assets. In response, the SDT notes that most of CIP-007, and Requirement R1 in particular, must be implemented at an individual cyber asset level and the requirement thus starts with 'For applicable Cyber Assets'. Ports and services are enabled or disabled on individual Cyber Assets and most of CIP-007 can't be done at a 'system' level but at a Cyber Asset level. For example, if an entity does not need telnet service, then the only way to prove that it has been disabled is on an individual Cyber Asset basis – ports and services are by nature not implemented on a 'group' of Cyber Assets but on individual Cyber Assets.

FMPA and LCEC commented that the SDT should add the phrase "that initiate or receive network communications" after the word "services" or delete services and let ports handle it. In response, the SDT notes that the services is part of "port ranges or services" and are two levels at which the entity can document the enabled logical network accessible ports. This was added primarily to handle dynamic ports. Some systems will use a particular dynamic port out of a small range of ports and documenting that range is acceptable. Other services may pick a dynamic port out of all the high ports (any port between 1024 and 65535 e.g. RPC) and the SDT's intent is to allow for documenting the need at the service name level.

Some commenters suggested that clarification that the Responsible Entity determines the need of port should be included. In response, the SDT agrees and has added clarifying language.

One commenter suggested that the phrase "enable only logical network accessible ports needed" should be "enable only required logical network accessible ports." In response, the SDT notes that the intent is to document the business or technical justification for all open ports. In previous drafts, numerous comments were received to change the word "justification" to "need", which was accepted by the SDT. The SDT also notes there is a difference in "required" and "needed" and thinks "needed" is a more appropriate term due to instances where a Cyber Asset may be fully able to perform its basic function without the port enabled (thus the port is not technically "required"), but the port is "needed" for other purposes. Similarly, KCPL commented that the "needed" should be changed to "approved" for clarity. In

response, the SDT notes that these ports are part of the tracked baseline configuration in CIP-010 and approvals occur there. The SDT has therefore not brought in the approval process into CIP-007.

One commenter suggested commented that 'listening' should be replaced with 'enabled'. In response, the SDT believes the term 'listening' is more descriptive as the intended scope is those ports that can actually be reached from the network. A port can be 'enabled' at one level (a config file), but blocked by other means lower in the OS (e.g. TCP_Wrappers) such that it is not actually 'listening'. The end goal is blocking accessibility from the network to unneeded ports and the SDT believes 'listening' better captures that goal.

One commenter suggested that a fourth bullet should be added to the measures to address CIP-005-4 R2.2: Listing of access points to the ESPs, including configuration of ports and services, individually or by specified grouping. In response, the SDT agrees that EAP's should be highlighted and has added this to the first bullet point.

One commenter suggested that the measure should add the phrase "or class of Cyber assets" to the second bullet. In response, the SDT agrees and has added the phrase "individually or by group" to the bullet point.

One commenter suggested that the first bullet under the measures should be deleted as it doesn't meet the requirement. In response, the SDT agrees that a simple listing of port need is not sufficient to meet the requirement and has replaced that measure with the phrase "Documentation of the need for all enabled ports individually or by group".

One commenter suggested that the list of listening ports could be a source of double jeopardy with CIP-010's baseline configuration requirements. In response, the SDT notes that the requirement is concerned only with the enabling of only needed ports irrespective of any documentation. The list of enabled ports is a requirement in the baseline configuration requirement in CIP-010. The SDT believes that failing to maintain the baseline configuration and failing to actually go to a Cyber Asset and disable unneeded ports are two different requirement violations. The measures for this requirement refer to listings of ports as evidence, but that evidence could be the same evidence required for CIP-010. Being able to utilize a single piece of evidence for proof of compliance with two different requirements is not double jeopardy.

There was a commenter who suggested that instead of the phrase 'class of cyber asset' the language from CIP-010 should be used. Also, the requirements should address justification of enabled ports. In response, the SDT agrees and notes that justification is addressed by the phrase 'needed by the Responsible Entity' and the measure has been changed to

now call for documentation of the need for all enabled ports. The SDT also agrees with the 'class of cyber asset' comment and has incorporated the language 'individually or by group' from CIP-010 as suggested.

One commenter suggested that the reference to CIP-005-5 R1 to protect the network in the guidance should be deleted. In response, the SDT agrees and has deleted the language, leaving only the clarification that blocking ports at the ESP does not substitute for the device level requirement.

One commenter suggested that the guidance should allow for disabling ports 'inline in a non-bypassable manner'. In response, the SDT agreed with this in the draft 1 comment phase and made that change between drafts 1 and 2.

Requirement Part 1.2

There was a comment that the text should be revised to begin with the phrase "Have methods to protect against…" since the VSL is for not having methods. In response, the SDT notes that the overall Requirement R1 is to "implement documented processes" and changing this to have methods would add another level of abstraction such that the overall requirement would be "implement documented processes to have methods to protect."

A commenter suggested that this requirement should be replaced with a 'implement a policy' type requirement. In response, the SDT does not believe that a policy only requirement would meet the FERC directive in Docket No. RD10-3-000 of March 18, 2010, which is the genesis of this requirement.

Several commenters suggested that signage is a weak control that does not provide adequate protection. In response, the SDT notes that signage was never meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. The industry has made several comments as to the other preventative and detective measures that are required before physical access to a physical port is ever achieved. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who plugs his infected smart phone into an operator console USB port "just to charge the battery".

Several commenters stated that this requirement needs further justification for its existence. In response, the SDT notes that this requirement was added to address FERC's Docket No. RD10-3-000 of March 18, 2010 which states, "However, like NERC, we are concerned that neither CIP-007-2 in particular, nor the CIP reliability standards in general, adequately address technical opportunities to mitigate risks associated with unused physical ports. The practice of disabling or otherwise securing unused physical ports is a basic and integral component of sound defense-in-depth cyber security practices, yet it is absent from the current reliability standards. The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP reliability standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."

One commenter stated that entities may not be able to block physical ports based on usage using the example of unplugging a USB keyboard or mouse and using a thumb drive in that enabled port. In response, the SDT notes the requirement is to "protect against the use" and purposefully does not use the verb "prevent" in recognition that the control is not effective in prevention in many cases as the industry has pointed out. The intent of the requirement is not to be a 100% preventative control, but is a last measure in a defense in depth layered control environment to make personnel think before attaching to a BES Cyber System in the highest risk areas.

There was a comment that this requirement should be limited to network ports as portable media is handled elsewhere. In response, the SDT notes that BES Cyber System Information on portable media is handled elsewhere, not the portable media itself. Portable media is becoming a primary means of entry into entities and the SDT believes that to meet FERC's intent, portable media and console command ports should remain in scope.

One commeneter asked for clarity on whether the disabling of physical ports could potentially reclassify a device that would otherwise be considered a BES Cyber System. For instance, if a routable device had all of its physical network ports blocked then what otherwise might be a routable device cannot route. In response, the SDT notes that the ability to communicate outside of itself is not a determining factor as to whether a Cyber Asset is or is not a BES Cyber Asset or BES Cyber System; the Cyber Asset's function as it pertains to BES reliability determines that. So although a Cyber Asset may indeed be a BES Cyber Asset, if all communication ports are disabled then the BES Cyber Asset would have no External Routable Connectivity or dial-up connectivity and thus none of the requirements which have that condition in the applicability column would apply. The specific example of the programmable television monitor provided would have to be determined by the Responsible Entity as to whether the monitor met the definition of a BES Cyber Asset. If the

monitor is not a BES Cyber Asset, then it is not a part of a BES Cyber System. The SDT notes that BES Cyber Systems consist of one or more BES Cyber Assets, not every programmable electronic device.

There was a comment asking for clarity as to whether ports could be protected via a common method or must the protections be per port. In response, the SDT notes that the requirement is not prescriptive in this manner and does not preclude either as the measures and guidance allow for directive measures.

One commenter stated that the word "unnecessary" should be changed to "not required". In response, the SDT is allowing for slightly more flexibility than is denoted by terms such as "required" or "not required". A port may be "necessary" for some use of the entity but not technically "required" for the operation of the device.

Requirement R2 General Comments

Several respondents commented that patch management should apply to all applicable Cyber Assets including all Low Impact. In response, the SDT believes that while managing patches on all Cyber Assets is a best practice, making this a mandatory and auditable requirement would divert the industry's attention to managing an onerous burden of records on orders of magnitude more devices at the lowest impact level. The SDT has been careful to balance what is absolutely required in a mandatory and enforceable manner and the burden of proof such a change would entail with maintaining a high degree of industry focus on the higher risk assets. If we overburden the Low impact classes, it would be easy to divert an inordinate amount of industry focus to the lowest impact assets if we don't maintain that balance. The SDT also believes that many devices will probably have some portion of the population declared as medium impact and thus many entities will need to handle any vulnerabilities on those devices and oftentimes will just patch all devices of that type.

There were many commenters that suggested that all sub requirements should have the applicability changed to medium impact with ERC. In response, the SDT notes that managing security patches or otherwise mitigating the vulnerabilities the patches address is a core activity in protecting our critical infrastructure. While external routable connectivity does increase the risk, the lack thereof does not reduce it to an acceptable level as many threats enter the environment by other means such as thumb drives, laptops, smart phones, etc. The SDT does not believe we can adequately protect the infrastructure if we only concern ourselves with patching devices with external connectivity due to the remaining threat vectors. However, the SDT does understand the evidence burden and has made changes to this requirement to reduce that burden. The requirement now allows entities to focus on a monthly 'batch' cycle of patches rather than tracking timelines for every individual patch, and no documented mitigation plans are needed if patches are installed within the 70 day time period. It is the SDT's intent that these and other changes in this requirement will relieve the documentation

burden while still requiring the performance of this basic security activity. The essence of this requirement is to have the industry watching and aware of vulnerabilities in their BES Cyber Systems, whether they are routably connected or not, and mitigating those vulnerabilities. Many patches may address vulnerabilities that the entity has already mitigated through existing means and require no action. In fact, it is expected that the lack of external routable connectivity would be used as a major factor in many applicability decisions and/or mitigation plans where that is the case.

Several commenters stated that the requirement should not require a documented remediation plan for every patch, but outline a standard patch mgt process with documented deviations. In response, the SDT agrees and has modified part 2.3 to allow for this.

There were a couple of comments that clarification is needed on failed patches installed well after the 60 days but according to the entity's plan. In response, the SDT has modified the requirements such that a plan may be revised (see requirement part 2.4).

One commenter suggested that the word "processes" should be changed to "program" throughout R2 so it aligns with 2.1. In response, the SDT agrees the terms should match, but notes that Requirement R2 (above the tables) uses the word "processes" and has changed the term "program" in 2.1 to "process" so that the entire requirement uses the same term.

One commenter stated that the requirement in essence rewards obsolescence and never requires upgrading to a patchable system. In response, the SDT notes that the standard's intent is to secure the infrastructure that is in place without requiring equipment upgrades of currently functional equipment solely for security purposes. Cyber security risks are one factor in the decision to upgrade. The SDT also notes that cyber risk is determined by many factors, and older equipment could actually have a lower cyber security risk. These decisions are best left to the Responsible Entity to make based on the specific circumstances rather than mandated unilaterally in a cyber security standard.

There was a comment that clarity should be provided on what constitutes a "security patch" and what is "updateable". In response, the SDT agrees and has added clarifying sentences to the guidance section of the standard for part 2.1.

Requirement Part 2.1

Multiple comments stated that the phrase "security patches" should be changed to "patches and security upgrades". In response, the SDT is concerned with expanding the scope beyond patches to words such as upgrades or updates. The

SDT does not desire to create the situation where a vendor creates a new version of their software, mentions something new about security in the new version, and suddenly everyone is under mandatory compliance obligation to either upgrade or create a plan. Cyber security features are one component of an upgrade decision. The SDT believes that keeping this requirement to the word "patches", which are fixes to their existing version, is what should be mandatory. The SDT also notes that patches are a fix to a specific vulnerability, which is what the requirement is based upon as it is under obligation to mitigate the vulnerability.

One commenter suggested that applicability and compensating measures should be determined based on original source of patch (e.g. Microsoft) rather than the SCADA vendor. In response, the SDT agrees that this is a best practice so that vulnerabilities may be mitigated in the shortest timeframe possible, even before the patch is certified by the SCADA vendor. The SDT notes that the provided example is the most obvious one with Microsoft, however if included in a mandatory and auditable environment this would extend to the seemingly unlimited non-obvious situations where an entity buys a system from vendor 'X', but vendor 'X' is using software components from 20 other vendors. The entity does not know all the original sources of all components of the system. Situations such as what is the RTOS (Real Time Operating System) involved in a particular digital relay would arise, and why didn't the entity track the vulnerability info for that RTOS directly from that vendor rather than the relay vendor's firmware levels? The entity is not a direct customer of that RTOS vendor and may not have access to that information. In summary, while the SDT believes this is a best practice in some situations, making it mandatory and auditable in every situation is not something that entities can comply with as the standard expands in scope to every BES Cyber Asset in the field.

There was a recommendation that more guidance is needed on appropriate patch sources. In response, the SDT notes that the 'appropriate sources' was added to this requirement from Version 4 so that a definite start date for the evaluation timeframe could be determined. The appropriate source is going to be dependent on the situation. If the Responsible Entity has a control system from vendor who invalidates support contracts if the system is patched outside of their approval, then the vendor should be the appropriate source. If the system were custom built by the Responsible Entity, then the vendor for each of the components used to build the system would be the appropriate source.

One commenter recommended that the program should be specified in Requirement R2 and not Requirement R2.1 as a process does not include a program. In response, the SDT agrees and has changed the word "program" in R2.1 to "process" so that it agrees with Requirement R2.

Some commenters said that the process should include a periodic review (monthly) of all patch sources rather than maintaining timeframes per patch. In response, the SDT agrees and has made changes to the language to incorporate this concept.

There was a comment that the requirement should insure that documentation of sources is a onetime exercise unless new software is added to the baseline. In response, the SDT agrees and has clarified this in the guidance section of the standard.

Requirement Part 2.2

Numerous commenters suggested a change to 35 calendar days to allow for a monthly cycle. In response, the SDT agrees and has made the suggested change.

One commenter requested that the guideline states that entities are allowed to evaluate and accept risk which FERC Order 706 disallows. In response, the SDT agrees and has modified the guidance.

There were a few commenters that requested additional clarity on what the term 'applicability' means. In response, the SDT agrees and has added clarification to the guidance section.

One commenter suggested alternative wording, "Evaluate the security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified in requirement part 2.1. The assessment must include determination of the applicability of each patch to the entity's specific environment and systems as well as reason for a patch's non-applicability." In response, the SDT has modified this requirement to incorporate a monthly review of the patch sources, but has chosen not to get more prescriptive with the term applicability within the requirement. The SDT believes that evaluating applicability necessarily means that the entity will be documenting the final determination for their environment.

Requirement Part 2.3

Some commenters proposed changes to the timeframe and process such that it would allow 60 days and have no remediation plan required if the patch is installed within 60 days. In response, the SDT agrees and has modified the requirement so that applying the patch or creating or revising a mitigation plan are all choices the entity can take within the second 35 day period. The SDT notes, however, that the timeframe is 70 days total with 35 days for tracking and

determining applicability and 35 days for either installing or determining the mitigation plan. It is not 35 days plus an additional 60 days for the second step.

There were multiple comments that the word "dated" should be revised since it is open-ended. In response the SDT believes the word "dated" is necessary and the requirement would be open-ended if it had no date required for the plan. The date of the plan in requirement part 2.3 is what part 2.4 depends upon.

One commenter stated that the requirement was overly burdensome due to the sheer number of patches. In response, the SDT notes that due to the burden the auditable cyber assets are limited to High and Medium Impact Systems and associated systems. The SDT has changed the requirement so that the tracking can be on a monthly basis for all patches released that month rather than on an individual patch basis, which should help.

Some commenters suggested that specificity is needed as to a maximum timeframe. It is compliant with the requirement to state a timeframe of the phrase "End of Life Upgrade". In response, the SDT has had numerous discussions around this issue. The SDT has decided that the reliability risk of putting prescriptive and mandatory timeframes for patching outweigh the risks of having an open-ended patching timeframe. There are numerous reasons. One reason is the industry goes through periods of time during seasons of the year that we refer to as "nobody is touching nothing" mode because the risk of any change to equipment or systems invokes an availability risk when the asset is depended upon the most. Tripping a generating unit on a 100-degree day because a standard said we were out of time to patch it to fix some minor issue is not acceptable. Another reason is we are in a largely legacy equipment environment as this standard expands outside of control centers where there are no patch management solutions. Upgrading the firmware in thousands of digital relays is something that must be planned and executed very cautiously. Firmware based devices will require planned outages for patches and present the risk of "bricking" the asset. So for these and other reasons, the SDT has decided the implementation timeframe is best left up to the entity rather than enforcing some arbitrary timeframe. The requirement is that they have a dated plan and must work towards that plan. We believe this is the best tradeoff between the risk of someone exploiting a vulnerability and the inherent risk of changing code in devices where availability is paramount. If the SDT set a maximum timeframe to handle these sorts of cases, we would have numerous comments about how the timeframe is too long. We believe that setting a timeframe to handle these cases would actually draw a line in the sand that would have the unintended consequence of all patch timeframes moving toward that timeframe. If the entity has to set its own timeframe and defend it, then they won't all tend to move towards the maximum timeframe specified in the requirement.

Two commenters suggested that the requirement should allow for revision to an existing plan. In response, the SDT agrees and has changed the language to allow for revisions.

There were a few recommendations that the word “exposed” should be “addressed”. In response, the SDT agrees and has made the change.

There was a comment that a potential double jeopardy issue exists between requirement parts 2.2 and 2.3. In response, the SDT has made numerous changes to these requirements and believes that any double jeopardy issues have been addressed.

One commenter stated that an evaluation of the language in the change rationale should be done to determine what needs to move into the requirement itself. In response, the SDT believes that what remains in the rationale is rationale and has no actionable requirements that could be moved to the requirement itself. However the SDT agrees the language in the rationale should be preserved and has moved it to the guidance section as well.

There was a comment that addressing the vulnerability could be entirely dependent on vendor’s patch development timeframe to address a vulnerability. In response, the SDT notes that the process begins upon the release of the patch from the source identified by the Responsible Entity. The patch has been developed and is available before the process required in R2.2 and following starts.

One commenter asked about the need for TFEs where patches cannot be applied. In response, the SDT notes the intent is that TFEs are not required at any step in the process. The process has been designed to alleviate the need and guidance has been included as well to address this issue.

There was a comment that the first sentence in the guidelines for Requirement R2.3 is a restatement with different wording and may imply other requirements. In response, the SDT agrees and has changed the guidance to more closely match the requirement.

Requirement Part 2.4

Multiple commenters stated that the plans should allow for revision in other than CIP Exceptional Circumstances before the timeframe expires. In response, the SDT agrees and has added the ability to revise the plan if done through an approved process such that the revision or extension is approved by the CIP Senior Manager or delegate.

An issue was raised that there is a potential double jeopardy issue as 2.4 duplicates Requirement R2 where 'implement' is required. In response, the SDT does not believe that a double jeopardy issue exists because the implement in the overall requirement is for the patch management process, whereas the implement in R2.4 is for the individual patch. If R2.4 does not have an implement requirement at the patch level, then the 'implement' in the overall requirement only applies to drafting a plan.

One commenter suggested that guidance should be offered on how much information is expected to demonstrate implementation. In response, the SDT notes that example measures are provided and that the requirement is for the implementation of a mitigation plan, thus the measures would be records of the implementation of the plan. The plan may include such things as installing the patch and the measure would be a record of the installation, or the plan may include the disabling of an affected service, or the adding of a signature to an IDS, or a change to a host based firewall to handle the vulnerability and the measure would be the record of the completion of these changes.

There was a comment that the change rationale is from 2.2 and doesn't address 2.4. In response, the SDT agrees and has updated the rationale to match the changes in the requirement.

To address the comments that bullet 2 of the measure should read "records of vendor recommended or other appropriate mitigations" the SDT agrees and has added "or other appropriate" to the measure.

Requirement R2 VSL

One commented that the R2 and R3 VSLs increment by different ranges. In response, R3 has been modified to remove specific timeframes in the Requirement and the VSL has removed the referenced increments.

Requirement R3 General Comments

One commenter requested that the requirement should apply to all applicable Cyber Assets including all Low Impact. In response, the SDT believes that while this is a best practice, making this a mandatory and auditable requirement would divert the industry's attention to managing an onerous burden of records on orders of magnitude more devices at the lowest impact level. The SDT has been careful to balance what is absolutely required in a mandatory and enforceable manner and the burden of proof such a change would entail with maintaining a high degree of industry focus on the higher risk assets. If we overburden the Low impact classes, it would be easy to divert an inordinate amount of industry

focus to the lowest impact assets if we don't maintain that balance. The SDT believes that keeping the requirements on Low impact systems at a programmatic level rather than a device level is the only way to keep that balance.

Multiple commenters suggested that the applicability should change to all medium impact with ERC. In response, the SDT disagrees because the threat of malicious code is not limited to introduction through external routable connectivity. The threat of malicious code is arguably higher from portable media, temporarily connected cyber assets (vendor laptops, etc) and inadvertent insider actions.

Requirement Part 3.1

There were a few comments which stated that the intent should be clarified and suggested language includes "Deploy method(s) to deter, detect, or prevent malicious code based on the Cyber Asset's susceptibility to malware. Methods do not have to be used on every single Cyber Asset." In response, the SDT notes that the applicability is at the 'system' level and the intent is to keep it at that level as this is a requirement where the 'system' level is beneficial. Therefore, the SDT believes it is best to not fill the requirement with language at an individual cyber asset level.

There were several concerns that Requirements R3.1 and R3.2 are too vague. In response, the SDT notes that the requirements are indeed written at a very high level but the SDT believes it is necessarily so. Malicious code protection is at the 'forefront of the fight' and is rapidly evolving and changing to match the ever changing and morphing threat. The SDT believes the protection of our infrastructure can be better accomplished if we do not have prescriptive technical methods detailed in this requirement. This could have the unintended effect in the future of stifling innovation and the use of new and better tools that would provide better protection but not be compliant with what the SDT would specify today. It does not produce a standard that is future-proof. All previous versions of the standard did prescribe a particular technology and method that must be used on all applicable cyber assets, and while that had no vagueness it became a huge burden on the industry for TFE's, putting the industry's focus on what could not be done rather than what could be done. Therefore, the SDT is leaving this requirement at a very high level that is in essence "think through the problem of malicious code introduction, detection, and prevention and come up with the best methods to handle the problem in each particular situation, and then document and do those methods." The SDT believes reliability will be better served in the long run by a requirement like this for such areas as the malicious code 'arms race' environment that we find ourselves in.

There were multiple comments asking if the 'or' is appropriate. There was another question if an awareness campaign to deter is ok. There was a suggested that the word 'deter' should be stricken. In response, the SDT notes that the

requirement was worded with the 'or' and 'deter' to avoid zero-defect language. If the requirement was to detect or prevent all malicious code, then despite an entity's best efforts if some zero-day malware did make it onto an applicable cyber asset the entity would be in violation of the requirement. As malware detection and prevention is an inexact science and essentially an 'arms race', the SDT did not want to word the requirement in such a way that it required perfection in an imperfect environment with imperfect tools.

There was many comments that the 'Associated PCAs' are included at a Cyber Asset (device) level, not a system level and should be deleted or clarified how the 'system' concept will apply. In response, the SDT notes that malware prevention really is at a Cyber Asset level and recognizes that the associated PCA's could be included by reference in the documentation the entity supplies for Requirement R3.1.

One commented stated Requirement R3.1 and R3.2 should be revised to "deploy methods … within an ESP" to scope to routable assets within the ESP. In response, the SDT notes that ESP's are only required around routable protocol connected cyber assets, however malware protection is required on all cyber assets in scope. Malware is a risk even on isolated systems; it may not be able to easily spread in non-routable environments, but it can be coded to have a specific impact even on isolated systems (e.g. Stuxnet was coded to do its harm when it reached a specific system and could travel by USB portable media). Therefore the SDT has chosen to not limit the malware prevention requirement to only routable protocol accessible systems in ESPs.

One commenter suggested that the measures should be revised to, "Entity's performance of these processes (e.g., through traditional antivirus, system hardening, non-software policies, etc.)." In response, the SDT notes the only suggested change is the phrase 'non-software' in front of 'policies'. The SDT does not wish to make the measure more prescriptive than the requirement itself. Since malware prevention is an ever changing 'arms race' type environment where the controls needed are changing as the threat constantly evolves, the SDT is leaving this requirement at a high level. This will allow entities to adapt as the threat adapts while also reducing the need for TFEs.

One commenter stated that the last sentence of the guidance says 'should not require a TFE' making it unclear whether TFEs are an option or not. In response, the SDT agrees and has struck the phrase.

Requirement Part 3.2

One commenter recommended that the following sentence be added: “Mitigation for the Associated Protected Assets may be accomplished through other applicable systems.” In response, the SDT agrees that this is possible and the entity could state how the mitigation covers the associated PCA’s in their documentation for this requirement.

One commenter suggested that the wording “within 35 days” should be added as malware mitigation timeframe. In response, the SDT has chosen not to include a mitigation timeframe as in some cases the entity may be working with government or law enforcement in an ongoing investigation. In APT cases, quick mitigation may just force the moving of the attack while investigations are ongoing. The SDT feels that a mandatory timeframe would interfere with investigations in cases such as these.

Two commenters recommended that the measures should be limited to response actions for detected malware and remove other bullets. In response the SDT agrees and has removed the example measures that were more focused on specific technologies.

One commenter stated that in the guidelines it discusses ‘non-changeable software’ and asks if this is in conflict with definition of Cyber Asset. In response, the SDT believes it is not in conflict. Cyber Asset is a programmable electronic device and devices that are not updateable by the user, but are software or firmware based and do execute a program would still be classified as Cyber Assets.

Requirement Part 3.3

There were many comments that Medium impact locations with no remote connectivity need more than 35 days for signature updates or should not be in scope. Some commented that 35 days is too long for malware updates and it should be shortened. In response, the SDT agrees with both positions and realizes that specifying a time frame on a requirement such as this often means picking a timeframe that is usually not long enough for all of the more extreme cases while at the same time is too long for most ‘normal’ cases. The SDT has decided that it is in the best interest of reliability to revert this requirement back to its V1-V4 language that did not include a timeframe. Order 706 did not direct such a modification and the SDT is more concerned about preventing the unintended consequences of this timeframe and their resulting impacts to reliability. As one example, the SDT does not want to incent entities to remove antivirus products from systems in the field and expose them to a decade’s worth of viruses because they may not be able to get last month’s signatures on in 35 days. The SDT believes its in the best interest of reliability to allow entities to put antivirus software on all assets where they can and require processes to test and install the updates without specifying an ‘arbitrary’ timeframe that satisfies no one.

One commenter stated that 35 days is too long for malware updates and should be shortened. In response, the SDT agrees with both positions and realizes that specifying a timeframe on a requirement such as this often means picking a timeframe that is usually not long enough for all the more extreme cases while at the same time is too long for most 'normal' cases. The SDT has decided that it is in the best interest of reliability to revert this requirement back to its V1-V4 language that did not include a timeframe. Order No. 706 did not direct such a modification and the SDT is more concerned with the unintended consequences of this timeframe and the resulting impacts to reliability. As one example, the SDT does not want to incent entities to remove antivirus products from systems in the field and expose them to a decade's worth of viruses because they may not be able to get last month's signatures on in 35 days. The SDT believes it is in the best interest of reliability to allow entities to put antivirus software on all assets where they can and require processes to test and install the updates without specifying an 'arbitrary' timeframe that satisfies no one.

Several commenters wrote that the requirement is not as clear as the change rationale and the requirement could be gamed to not install any recent sigs. In response, the SDT agrees and has rewritten the requirement for clarity.

A few comments stated that signature updates need to be staged to avoid a large impact of false positives. The included guidance should address this as well. In response, the SDT agrees and has reverted the language back to its V1-V4 state that did include a process for testing and installing the signature updates.

Some commenters questioned that if an entity does not use signature based tools, if they still have a process to update the signatures per the overall requirement. In response, the SDT notes the specific sub requirement is conditional and only applies to "for those methods identified in requirement part 3.1 that use signatures or patterns…" and therefore if an entity has no such methods, the requirement does not apply.

One commenter recommended that the word "available" should be changed to "applicable". In response, the SDT has rewritten the requirement for clarity and to address this and several other comments.

A commenter suggested that the requirement should allow for other anomaly or heuristics based analysis/detection, not just signature updates. In response, Requirement R3.1 allows for any method to be used so that the requirement does not preclude the use of any technology or tool as they constantly improve to keep up with the threats. Requirement R3.3 in particular is only applicable when an entity chooses to use a signature or pattern based tool in order to keep them updated in a timely manner; it does not require their use.

One commenter asked for clarity on what TFEs are allowed for equipment that doesn't run malicious code tools. In response, the SDT notes the requirement has been written at a much higher level than previous versions. The included guidance has numerous suggested methods up to and including policy level measures. Therefore, the SDT feels that TFEs are no longer an issue as the requirement no longer prescriptively requires a single technology tool for addressing the issue.

Requirement R4 General Comments

There were several comments that the rationale language should change 'immediate' detection to 'real time detection' to be consistent with 4.2. In response, the SDT received numerous comments that pointed out issues with the term 'real time' and has deleted it, as well as removing 'immediate' in the rationale.

There was a comment seeking clarity as to whether log events are required for local, remote, or both types of access. In response, the SDT notes that the requirement applies to both High and Medium impact BES Cyber Systems as well as all associated EACMs. The EACMs will include the EAPs for the associated perimeters. Therefore the logging is for both; local access at the BES Cyber Systems themselves, and remote access through the EAP.

One commenter suggested that the guidance include NIST 800-137 as a resource. In response, the SDT agrees and has added the reference to the guidance.

Requirement Part 4.1

Many commenters recommended that the requirement should add the phrase "per device capability". In response, the SDT agrees and has added this concept to the language.

Numerous commenters asked that it be clarified that devices that cannot log do not require a TFE. In response, the SDT has added device capability condition statements to the requirement such that the requirement does not apply if the device does not log the events. In addition, the bulleted list of logged events includes the qualifier 'detected' so that if a device cannot detect such events, then there is nothing to log.

There were several suggestions that 'where technically feasible' should be added to all. In response, the SDT's intent is that the requirement is worded so that what is required matches the device's capability and no more and avoids the use of TFE's due to prescriptive requirements that assume technical capabilities of large classes of Cyber Assets.

Tucson, and SME List commented that TFE should be applied to the logging, not the alerting in 4.2 and suggest removing the TFE in 4.2. In response, the SDT has changed both 4.1 and 4.2 to include the 'per device capability' concept rather than allowing TFE's.

Multiple commenters suggested said that the applicability should change to Medium Impact with ERC. In response, the SDT notes that logging should be enabled wherever it is available. If an isolated or standalone BES Cyber Asset is compromised, then the logs on that device may be the only data the entity will have to investigate the incident.

One commenter suggested that the measures should include samples of logs showing the events are being logged. In response, the SDT agrees and has added the additional example measure.

One commenter suggested that the requirement implies 100% availability of the logging system and suggests adding the 99.9% availability. In response, the SDT notes the comments where the 99.9% was added in CIP-006 pointed out numerous issues with that approach. The SDT believes that the inclusion of Requirement R4.3 states that 100% availability is not required and handles the issue by requiring the entity to have processes in place to respond to outages in a timely manner.

Several commenters sought clarity as to log failed access attempts when deny by default means offending packets are dropped such that there is nothing to log. In response, the SDT notes that a denied access attempt is a failed access attempt.

There were several commenters who suggested that 'malicious software' should be changed to 'malicious code' to be consistent with Requirement R3. In response, the SDT agrees and has made the change.

Many commenters recommended dropping the requirement since its determined after the fact, requires knowledge of intent, and it's not possible to produce a log of 'malicious activity'. In response, the SDT agrees and has removed the sub requirement.

Several commented stated that 4.1.4 is too vague and needs more guidance as to what activities beyond 4.1.1 to 4.1.3 would be included. In response, the SDT agrees and has removed the sub requirement.

One commenter stated that malicious activity should be detected and logged 'as required in the cyber security incident response plan'. In response, the SDT notes that based on several other industry comments, this sub requirement has been removed.

Requirement Part 4.2

Several commenter stated that 'real time' is not the appropriate phrase and some suggested changing to "Have methods to generate alerts, where technically feasible, for events that the Responsible Entity determines necessary." In response, the SDT agrees and has deleted the 'real time' phrase.

Also, others commented that 'real time' should change to 15 minutes and add 'where the BES Cyber System is capable.' In response, the SDT agrees and has deleted the 'real time' phrase and the 'per Cyber Asset or BES System capability' has been added.

A few commenters recommended that 'within the BCS capabilities' be added. In response, the SDT agrees and has added the appropriate phrase.

One commenter stated that a minimum expected set of security events for which alerts should be issued should be prescribed (if the Cyber Asset is capable of detecting and logging those types of events). Examples include failed login attempt threshold exceeded, account lockout, key software failures, and virus or malware alerts. They also commented that the guidance includes alerts to a display that may not be monitored. In response, the SDT notes that detected malicious code is included, as is detected event logging failure. The SDT agrees that unsuccessful login attempt threshold should be added as it is a requirement in CIP-007 R5.7 and has made this addition. The SDT notes that account lockout is a subset (or post action) of unsuccessful login attempt threshold and has not included it.

There was a comment that the requirement should only apply to Associated Protected Cyber Assets with ERC. In response, the SDT believes that if the BES Cyber Systems have External Routable Connectivity that the associated PCAs will also have that connectivity. In the envisioned rare instance where this is not the case, the requirement allows for the entity to do what is within the device's capability and no more.

One respondent commented that we need a requirement that trained and knowledgeable people perform the event monitoring activity. In response, the SDT agrees that this is certainly reasonable, but disagrees that it should be an

auditable requirement as it raises too many audit issues, such as what do the terms 'trained' and 'knowledgeable' mean and what is sufficient for each?

A commenter questioned is an alert required for malicious activity if it is automatically quarantined? In response, the SDT notes that alerts are required for detection of malicious code regardless of any subsequent mitigation actions taken. The SDT believes that if malicious code gets through the layers of defense and makes it way on to a BES Cyber System, that is an event that needs the entity's timely attention and response so the defenses can be shored up for the zero-day that is not detected and quarantined.

One commenter wrote that it was unclear as to whether 'detected failure' refers to logging a failure of some event or failure of logging. In response, the SDT has added a clarification that it is failure of the requirement part 4.1 event logging. This would include the failure of the applicable systems logging capability.

There was a recommendation that the measures should include examples of alerts issued. In response, the SDT agrees and has added this as one of the example measures.

Multiple comments suggested that 4.2.1 should change to 'detected cyber security event' since not all events are necessarily malicious. In response, the SDT agrees and has changed this part to refer to detected malicious code rather than malicious activity.

There were numerous comments suggesting to change the wording in 4.2.1 to 'detected events per 4.1'. In response, the SDT agrees and has added the reference to 4.1 for clarity.

One commenter stated that the guidance implies that only technical means are allowed, but requirement does not preclude procedural controls. In response, the SDT notes that the requirement language is the ruling language and guidance is not auditable and is provided to provide further context or examples or assistance in how entities may want to approach meeting the requirement.

Requirement Part 4.3

There were a multitude of commenters who recommended that the requirement add the phrase "human detected event logging failure" to clarify when the clock starts. In response, the SDT agrees with the concept and has changed the

language to require that the response timeframe begins with the alert of the failure. Therefore, the timeframe begins after something or someone has detected the failure and has generated an alert as in 4.2.

One commenter suggested that 'after notification' should be added after 'next calendar day'. In response, the SDT agrees with the concept and has changed the language to require that the response timeframe begins with the alert of the failure. Therefore, the timeframe begins after something or someone has detected the failure and has generated an alert as in 4.2.

A few respondents commented that the requirement should be struck or change the verbiage to "Document the controls implemented to identify and respond to detected logging failures. Document detected logging failures along with any discrepancies between the actual response and the documented response plan." In response, the SDT agrees and has struck the requirement.

A few commenters stated that the next calendar day is not enough time to rectify issues. In response, the SDT notes the timeframe is to 'activate' a response, not to resolve the issue. The SDT has chosen this in recognition that depending on what caused the failure, there may be widely varying timeframes to resolve the issue. Therefore, the requirement is for timely initiation of a response.

One commenter noted that the requirement presumes but does not prescribe a mechanism for monitoring for logging system failures. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

Several commenter responded that the timeframe is too short due to distances or other operational situations. There was also a suggestion is to include 'next business day'. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

There was one comment that this should only apply to Cyber Assets with ERC. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

Several commenters recommended that outage handling should be standardized with CIP-006. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

There were several comments that the measure should change the word 'attestation' to 'documentation'. In response, the SDT agrees and has made the change.

One comment suggested that the measure should change 'events' to 'failures' to better align with the requirement. In response, the SDT agrees and has made the change.

Requirement Part 4.4

There was a comment that the requirement should change to "Retain BES Cyber System and BES Cyber Asset". In response, the SDT agrees with the concept that the applicability in the requirement did not match the applicability column and has removed the applicability from the requirement by replacing 'BES Cyber System' with 'applicable'.

There were several comments that the TFE language should be struck and add 'within the BCS capabilities." In response, the SDT notes that this requirement is scoped to Control Center environments where the highest degree of logging is required and has the highest degree of more capable Cyber Assets. The SDT feels that in this environment, the industry really should push for 90 days of log retention on these systems.

One commenter suggested that this should apply to all Medium's that can store logs, not just those at control centers. In response, the SDT notes that with the vastly increased numbers and types of field devices that Version 5 will bring into scope, most of which are legacy devices, that putting a mandatory requirement in place that prescribes the length of log retention is not warranted and would cause numerous TFE's.

One commenter wrote that 'identified in 4.1' should be the main qualification for log retention and delete the 'security related' portion for clarity. In response, the SDT agrees and has removed the phrasing.

Some commenters stated that this is in conflict with evidence retention section. Auditors expect to ask for any day's logs in past three years. In response, the SDT has added guidance around this topic. The requirement that is to be audited is

that applicable cyber assets maintain 90 days of logs. The compliance evidence requirement is that the entity be able to show that for the historical compliance period, the applicable cyber systems maintained 90 days of logs. The guidance speaks of records of disposition of logs after their 90 days is up.

BPA commented that a media hardware failure that results in loss of stored logs is still a violation. In response, the SDT agrees and has added "except under CIP Exceptional Circumstances" to the requirement as it includes hardware failure.

One commenter stated that this should allow for a timeframe as determined by the Responsible Entity. In response, the SDT notes that 90 days has been the precedent through the previous CIP versions and having no bound means that zero days is valid if determined by the entity. The SDT believes that 90 days is a sufficient lower bound for Control Center environments and has no justification for lowering it in the highest risk environments.

A commenter suggested that the applicability should apply to medium impact with ERC. In response, the SDT notes that this applies to Control Centers. Throughout the history of the CIP standards, all cyber assets in a Control Center are in scope regardless of external connectivity. The SDT believes there is insufficient justification to lower the standard on this point.

One commenter implied that measure 2 requests info about log data that is not in the requirement. Measures 1 and 3 cover the requirement. In response, the SDT agrees and has moved this to the guidance section with a more detailed explanation of the difference between the requirement's retention period for security purposes and the overall standard's requirement for compliance measurement purposes.

Requirement Part 4.5

Many responders commented that clarity around who determines the appropriate sampling should be added by including 'sampling as deemed appropriate by the Responsible Entity'. In response, the SDT agrees and has made the change.

Several commenters noted that the applicability should be 'High impact including associated PCA' to clarify logging reviews aren't at the device level and should exclude EACM/PACMs. In response, the SDT agrees and has modified the applicability, however EACMs should be included. Since Electronic Access Points to ESP's are EACMs, this is one of the primary logs that should be reviewed.

Several commenters expressed concern that this needs some minimum expectations for logged event review. In response, the SDT notes the intent is included in the requirement which is to identify undetected security incidents. The FERC Order in paragraphs 525 and 628 states, "However, the Commission continues to believe that, while automated review systems provide a reasonable day-to-day check of the system and a convenient screening for obvious system breaches, periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings. Furthermore, manual review is beneficial to judge the effectiveness of protection measures, such as firewall settings. If a firewall setting is incorrect or ineffective, an automated review system may not identify a cyber security intrusion. For those entities without automated log review and alerts, it is even more important to perform a manual review because this will be the only review of the logs." The SDT believes the intent is that entities manually review logs to insure that automated tools are tuned and alerting on real incidents. The SDT does not believe it should get more prescriptive with the requirement.

There were several commenters who noted that the requirement should change to "Document and implement a secondary control(s), and an associated interval, not to exceed two weeks, to assure the generation, capture, monitoring, and alerting of events as identified in 4.1." In response, the SDT notes that the FERC Order 706 in paragraphs 525 and 628 are explicit about a manual review. Also, the events identified in 4.1 are requirements so identifying events in 4.5 that should have been caught in 4.1 is a violation. The intent is for the entity to review the logs to see if there are events happening (other than those in 4.1) that the entity should be alerting on. In essence, this is a 'tuning' requirement to insure that an entity's automated Security Information and Event Management (SIEM) type tools are not missing conditions that are appearing in the logs and going undetected.

One commenter suggested that the requirement should change 'undetected' to 'potential Cyber Security Incidents not previously identified or detected'. In response, the SDT notes that in draft one the language included terms such as "unanticipated" and "potential" and received numerous comments to remove these subjective terms.

There were a number of concerns that two weeks is too short and suggest monthly or two month periodicity. In response, the SDT notes that in paragraph 628 of FERC Order 706 states, "The Commission continues to believe that, in general, logs should be reviewed at least weekly", but leaves it to the ERO to determine the appropriate timeframe. The SDT believes that bi-weekly is an appropriate timeframe given the Commission's statement concerning weekly reviews.

There was a comment that the phrase “at a minimum every two weeks” could be misconstrued and suggested to mean “at intervals no greater than 15 days.” In response, the SDT agrees that two weeks is a maximum not a minimum and adopts the suggested change.

There was a suggestion in changing the requirement to read “Review a summarization or sampling of logged events that the Responsible Entity has determined could identify previously undetected Cyber Security Incidents. Such a review will be conducted every two weeks at a minimum.” In response, the SDT agrees with the issue and has reworded the requirement based on this and other comments to utilize ‘intervals no greater than 15 days’ for greater specificity.

One commenter suggested that the timeframe should be determined by the Responsible Entity. In response, the SDT notes that in paragraph 628 of FERC Order 706 the Commission ordered the ERO to determine an appropriate timeframe that is less than the 90 days in the requirements of previous versions while stating that weekly reviews are their recommendation. The SDT sees no justification for how this directive can be met if the timeframe is left completely up to the entity to determine.

There were multiple suggestions that the applicability should only apply when automated processes and alerting are not possible or no managed service provider is utilized. In response, the SDT notes from paragraph 525 of FERC Order 706 that “the Commission continues to believe that, while automated review systems provide a reasonable day-to-day check of the system and a convenient screening for obvious system breaches, periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings.” The Commission goes on to order the inclusion of manual review even if automated alerts are employed.

One commenter stated that a SIEM is the only real solution and is too expensive for small entities. In response, the SDT notes the requirement is for a manual review, not an automated review. Paragraph 525 of Order 706 makes it clear that even if automated systems are used, the manual review is still required. The requirement does not require installation of SIEM tools, but requires manual review even if SIEM tools are in use.

Several commenters noted that the phrase “signed and” should be deleted in the measure (also in 4.1 measure). In response, the SDT agrees that a signed approval of the review is not in the requirement and this has been deleted from the measure.

QUESTION B24– CIP-007-5 REQUIREMENT R5:

If you disagree with the changes made to CIP-007-5, Requirement R5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, some of the key issues expressed by commenters included (1) the applicability to Medium Impact BES Cyber Systems with external routable connectivity, particularly in requirement part 5.1 and (2) the obligation for the CIP Senior Manager to authorize specific account types for BES Cyber Systems. The consideration of comments according to major issues and standard sections follows.

Correcting Deficiencies

One comment stated that this requirement should have a find, fix, track, and report mechanism built in so that entities can fix administrative deficiencies rather than consider them a violation of the requirement. In response, the CIP Version 5 approach to correcting deficiencies is that each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable items in the specified table. This approach of correcting deficiencies complements the compliance concept of internal controls.

Applicability to Low Impact

One commenter suggested that CIP-007-5 R5 should apply to Low Impact BES Cyber Systems. In response, we note the challenge of applying device-specific mandatory and enforceable requirements to low impact BES Cyber Systems exists in the overwhelming number of BES Cyber Assets. NERC survey results from the 2011 CIP filing indicate 90% of the facilities would be considered low impact, and each of these sites can have a potentially large number of Cyber Assets. As a result, the SDT has taken the approach of applying policy level requirements to BES Cyber Systems with the understanding and expectation that the compliance audit and enforcement of the policies will adapt to the significant increase.

TFE for all Requirement Parts

One commenter suggested adding TFE language for the entire requirement due its technical nature. In response, the SDT has identified requirement parts that intentionally allow for a safe-harbor exception process where equivalent mitigation can be shown. However, in some cases, we do not intend the technical limitations of the device to indicate a violation or need for safe-harbor (e.g. password complexity).

Multifactor Authentication
One commenter questioned if multi-factor authentication can replace password authentication without a TFE. In response, the SDT notes that the said requirement applies to password-only authentication but do not preclude other strong authentication mechanisms.

Procedural Controls
One commenter suggested, with regard to CAN-0017, procedural controls should be explicitly allowed in the requirement. However, the SDT points out that Compliance Application Notices do not carry forward to new versions of the standard. Previous versions require both procedural and technical controls for passwords, but this language is not included in the current draft. It would cause more confusion to explicitly allow procedural controls for each requirement part.

Version 5
One commenter provided its fundamental objection to Version 5 and suggested that implementation of the current CIP standards should be allowed to mature. The SDT is required to address all the FERC directives from Order 706, and FERC Order 706 has directed the ERO to complete consideration of Order 706 directives by March 31st, 2013.

Summary of Changes Section
Two commenters noted the summary of changes does not correspond to requirements for shared accounts, and in response the SDT has deleted this section which was held over from previous versions.

Requirement Part 5.1
Several entities commented this requirement part should be limited to medium impact with External Routable Connectivity, and the SDT has made this change. However, this requirement still applies to Medium Impact BES Cyber Systems at Control Centers.

Several commented that user access should be a defined term and security controls for system accounts should also exist. In response, we provide a definition in the guidelines, and we believe this term is well understood. In addition, the SDT has added a qualifier for this to apply to interactive user access. We do not define the same controls for system access due to the widely diverse way this could apply. System accounts do not uniformly apply across all devices and operating systems.

Several entities suggested rewording the phrase “where technically feasible” to “within the capability of the BES Cyber System”. In response, the alternative language would not change the TFE trigger for this requirement. There are several instances in which strict compliance can still be met in the absence of a specific technology mechanism to enforce access. The SDT has provided examples in the rationale box for requirement part 5.1 and improved the requirement language to make this point clear.

One commenter requested clarification that user access does not mean front panel read-outs on a device. In response, the SDT has changed “user access” to “interactive user access”, and the SDT has added a rationale statement further describing the intent of this requirement, in which the SDT has explicitly stated front panel read-outs do not qualify as interactive user access.

One commenter proposed that this requirement should be rephrased to limit to only electronic access. In response, the subject matter of the standard and requirement suffice to make the distinction, and we do not want to limit or confuse the possibility of using properly configured physical access controls to demonstrate compliance with this requirement.

One commenter suggested this apply to accounts and not user access. In response, the SDT has chosen to apply this to interactive user access because there may be instances where you do not want to enforce authentication for read-only access.

One commenter suggested specifying the phrase “applicable cyber assets” to qualify this requirement, but the applicability column already qualifies the requirement.

Requirement Part 5.2

Several entities suggested deleting requirement part 5.2 because it is already covered by the CIP-004-5 requirement to authorize users. In response, this requirement only deals with identifying the use of account types. It has been modified to make the intent clearer. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The requirement part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Several commenters advised removing the CIP Senior Manager as the person authorizing these account types. In response, the SDT chose not to remove this in the previous posting as suggested by our previous response to comments, and the SDT has removed the CIP Senior Manager as the person authorizing the account types in this posting.

One commenter proposed that generic accounts must be specified. In response, the SDT has added examples in the guidance section of this standard. The section added reads: "Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level."

One commenter suggested removing the word "authorized" from this requirement. The SDT has incorporated this suggestion by replacing the word "authorized" with the phrase "identify and inventory".

There was a comment submitted as to whether this requirement restricts the use of the specified account types. In response, identification of the accounts provides the necessary control. We do not specify these accounts must be disabled or removed because they are sometimes necessary for operation. Restricting these based on least privilege or need to know is already covered in CIP-004-5 R6.

One commenter suggested that authorization by "delegate(s)" be substitute for "delegate". However, the SDT has removed the requirement to authorize by CIP Senior Manager based on other commenters.

Requirement Part 5.3

Several comments suggested deleting requirement part 5.3 because it is already covered in CIP-004-5 requirements to authorize access. However, the identification of individuals with access to shared account has the additional objective of mitigating the risk of unauthorized access through shared accounts. This differs from the CIP-004-5 Requirement R6 to authorize access. An entity can authorize access and still not know who has access to a shared account. This would make it difficult to revoke access when it is no longer needed.

Several suggested incorporating the change rationale stating that the phrase "individuals storing, losing or inappropriately sharing a password is not a violation of this requirement." In response, the SDT has added this language to the rationale box for CIP-007-5 R5. The language in this section reads, "The term "authorized" is used in the

requirement to make clear that an individual storing, losing or inappropriately sharing a password is not a violation of this requirement."

Multiple commenters suggested adding the word "authorized" as a qualifier for access to correspond to the requirement language, and the SDT has made this change.

One commenter suggested that this requirement does not go far enough to restrict the use of privileged access, particularly when operating software. In response, CIP-004-5 R6 restricts the use of privileged access to only those having a documented business need. We do not specify the individual use of privileged and non-privileged access because this is not auditable for mandatory enforceable requirements. This is a good practice, but if this practice were codified in a standard, any individual not following the policy would impose monetary penalties on an organization.

One commenter suggested that the external routable connectivity qualifier should be removed for this Requirement Part in the applicability to match requirement part 5.2. In response, the requirement parts are unrelated, and the qualifier matches that of CIP-004-5 R6, which requires the authorization for electronic access.

Requirement Part 5.4

Several comments suggested revising this requirement part to address a recent RuggedCom vulnerability where a default password was unique to publicly known attributes of the device. In response, the SDT has removed the requirement exception where the "default password is unique to the device or instance of the application", and specified in the rationale that "pseudo-randomly system generated passwords are not considered default passwords".

Several commenters suggested adding the word "known" as a qualifier to default password to avoid the case where the entity was not aware of an undocumented default password by the vendor. The SDT has made this change.

There were several comments that the measure should change the phrase "new devices are deployed" to "new devices are in production" and one commenter suggested removing the phrase altogether since timeframes are covered in the implementation plan. The SDT has made this change from the word "deployed" to "in production", but the timeframe here does not conflict with the implementation timeframe and provides example, high quality evidence to meet this requirement.

One commenter requested clarification of when the default password should be changed. In response, we do not specify a timeframe (i.e. when cyber assets go into production) which could be misinterpreted. Instead, as with all requirements of CIP-007-5, this requirement must be met when a device becomes one of the applicable systems or assets.

Several commenters suggested removing the term "Cyber Assets" within the requirement to match the applicability of BES Cyber System. In response, the SDT has removed this language in deference to the applicability column.

One commenter requested clarification that default password that are unchanged would require changing according to R5.6. In response, this may be the case for interactive user accounts, but this is not necessary to state in the requirement. Changing default passwords meets a different objective to prevent unauthorized access from known credentials.

One commenter suggested excepting when a password is unique to the device. However, many commenters point out that doing so would allow for vulnerabilities where the uniqueness of the device where publicly known (i.e. MAC address).

Requirement Part 5.5

Several commenters suggested modifying the measure for requirement part 5.5 and requirement part 5.6 to better describe the attestation. Another commenter suggested replacing attestations with the ability to present a procedure. Others noted that it is not possible to obtain attestation from unionized workers and suggested adding a separate requirement to use training as a procedural control in place of attestations. In response, the SDT has used provided language to better describe the attestation evidence. The suggestion to use presentation of a procedure as a replacement cannot be used as evidence of implementing a procedure. The suggestion to have a further requirement for training is already covered in the training program specified in CIP-004-5.

One commenter stated that password complexity should be enforced to the maximum extent technically possible. In response, the SDT noted such a policy would create situations where users must write down passwords to remember them. The maximum extent could be exorbitant in some cases.

One commenter also stated that the guidelines state this requirement part is for password-only authentication, but the requirement does not include the same stipulation. BPA and Salt River Project made similar comments to distinguish the case where a PIN is used for multi-factor authentication. In response, the SDT has changed "password-based" to "password-only" in both requirement part 5.5 and 5.6.

Several commenters suggested using verbiage for requirement part 5.5.1: “Password length that is, at least, eight characters or the up to the maximum allowable by the system if that maximum is less than eight.” In response, although the proposed verbiage is cleaner, it becomes less clear once we specify “system” and the number of characters in the proposal. The SDT therefore decided to continue with the currently drafted language.

One commenter questioned if this new requirement will remove CAN-0017. In response, CANs do not apply to future versions of the standard, and the SDT has explicitly addressed the issue raised by CAN-0017 that either technical or procedural mechanisms can meet the requirement.

One commenter stated that it does not agree with the proscription of password requirements. In response, the SDT has included more prescriptive password requirements in response to a large number of industry comments against having added flexibility. However, the SDT has also attempted to remove some of the problematic provisions of the current version of password requirements that would allow entities to have stronger password policies.

One commenter suggested that the password complexity in requirement part 5.5.2 should specify or define the word “type”. In response, the examples provided in the requirement suffice for specifying password character types. The SDT believes these terms are well-understood by industry and do not necessitate further definitions.

Requirement Part 5.6

Several commenters pointed out the guidance, particularly the recommended password length table, has not updated to reflect the requirement. In response, the SDT has deleted sections of the guidance which no longer have relevance to the requirement.

Several commenters suggested adding a technical feasibility clause to this requirement part because some devices do not allow this capability. In response, the SDT notes that this only applies to user access, and the SDT has modified the requirement part to clarify this. The language as the end of this requirement part reads, “…at least once each calendar year, not to exceed 15 calendar months between changes, where technically feasible.”

One commenter suggested this requirement part explicitly apply to interactive user access, and the SDT has modified this requirement part to address the concern. The beginning of this requirement part reads, “For password-only authentication for interactive user access, either technically or procedurally enforce password changes…”

One commenter suggested adding the language “unless it impacts operation of the BES” to this requirement part. In response, the SDT has added the phrase “where technically feasible” to address these type of exceptions.

One commenter suggested the applicability of 5.6 be modified to match other requirement parts in CIP-007-5 R5. In response, the applicability to those Medium Impact BES Cyber Systems with External Routable Connectivity is due to the periodic nature of this requirement, which may only be feasible on large systems by having such connectivity. The commenter also suggested periodically is misspelled periodicity, but the SDT intends the latter as this is an attribute of the policy instead of a modifier.

One commenter suggested incorporating the language in the guidance table to include periodicity provisions for plant outages and disabled accounts. In response, for disabled accounts, a password change is not required because these do not qualify as providing interactive user authentication. The requirement does not have provisions for plant outages due to the widely varying schedules for plant outages. The SDT also notes that this requirement applies to those Medium Impact BES Cyber Systems with External Routable Connectivity.

A commenter proposed having a password change every 15 months. The SDT has incorporated this suggestion as part of an overall modification of annual periodic requirements in the CIP standards.

A commenter proposed to allow the entity to specify a password change periodicity, but the SDT has specified this periodicity based on a large number of comments against having this flexibility.

There was one comment that suggested the password change periodicity should be much shorter (i.e. quarterly). In response, the SDT notes that password change requirements should be considered in context with all of the password requirements, and shorter password change requirements can often result in poor password protection and selection by individuals.

Requirement Part 5.7

Several commenters suggested this requirement has the potential for creating a denial of service vulnerability to lockout all accounts to the system if entities configure all accounts for lockout. The SDT has not included the proposal to specify “user accounts” for limiting login attempts because it is too specific and has the potential to cause confusion. Although

the requirement does not prescribe this vulnerability, it does allow for it. Consequently, the SDT has included guidance in avoiding this configuration in the rationale.

Several commenters requested clarification on what the clause "where technically feasible" qualifies for this requirement part. In response, this requirement part has been modified to make clear the TFE triggering language qualifies both options. Furthermore, a TFE would only be necessary based on failure to implement either option.

Several commenters suggested this requirement should be deleted as it was not directed by FERC or otherwise align with the alerting requirements of CIP-007-5 requirement part 4.2. In response, this requirement is part of a more reasonable overall password security standard. As a trade-off to providing more flexibility to password policies, this requirement is highly effective to prevent online password attacks. This does not duplicate CIP-007-5 requirement part 4.2 because this alert is not required to be configured by that requirement.

One commenter requested additional guidance on the threshold for unsuccessful login attempts. The SDT has added this to the guidance section of this standard. Language was added which reads, "The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate."

Multiple commenters suggested that a minimum threshold parameter for account lockout should be specified. In response, a value is not specified here because this requirement protects against password cracking through online password cracking. Given the additional password policy requirements, the threshold for this setting can be very high, up to 100 or more.

One commenter requested the requirement part make clear these do not apply to Protected Cyber Assets such as printers and multi-function machines. In response, this requirement does apply to Protected Cyber Assets. This is a part of an overall protection against unauthorized access, which would include Protected Cyber Assets that have direct connections with the BES Cyber System.

VRFs

There was one comment that suggested the VRF should be Lower for Medium Impact BES Cyber Systems. In response, the impact level of the BES Cyber System is accounted for by the applicability of CIP-004 through CIP-011 requirements. A violation for a Medium Impact BES Cyber System cannot be considered directly with a High Impact BES Cyber System because they have less application of compensating security requirements.

VSLs

There was one comment that noted the High VSL includes the phrase “use of” where the associated requirement refers to only enablement of generic accounts and that the Severe VSL includes criteria for failure to implement password procedures, which might imply the required use of passwords. The VSL language regarding the enablement of generic account types has been updated to match the requirement. We do not agree the Severe VSL language implies a requirement to only use passwords. The VSLs are only used to describe violations, and use of authentication alternatives to passwords would not be a violation.

One commenter noted the Severe VSL is not consistent with the requirement and the SDT has updated the VSLs to align with modifications to the requirement.

Guideline

There was a recommendation that the guideline section needs to define generic accounts, and the SDT has added this to the guidelines.

Questions with Votes Only:

CIP-004, CIP-005, CIP-006 and CIP-007 Questions:

1. CIP-004-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
NESCOR/NESCO	No
ACES Power Marketing	No
Hydro One	No
Southern California Edison company	No
Progress Energy	No
Independent Electricity System Operator	No

Organization	Yes or No
NextEra Energy, Inc.	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
New York Power Authority	No
Springfield Utility Board	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC Registered Affiliates	Yes
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
Duke Energy	Yes
PNGC Comment Group	Yes

Organization	Yes or No
Dominion	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes

Organization	Yes or No
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes

Organization	Yes or No
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
MidAmerican Energy Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes

Organization	Yes or No
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Oncor Electric Delivery Company LLC	Yes
PJM Interconnection	Yes
NIPSCO	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes

Organization	Yes or No
Utility Services Inc	Yes
Alliant Energy	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

2. **CIP-004-5 R2 states "Each Responsible Entity shall have a role-based cyber security training program to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?**

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
ACES Power Marketing	No

Organization	Yes or No
SPP and Member companies	No
IRC Standards Review Committee	No
CenterPoint Energy	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Arizona Public Service Company	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No

Organization	Yes or No
LCEC	No
Niagara Mohawk (dba National Grid)	No
National Grid	No
Snohomish County PUD	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Northeast Utilities	No
San Diego Gas & Electric	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No

Organization	Yes or No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Alliant Energy	No
New York Power Authority	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No
PNGC Comment Group	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc (NCR01177,	Yes

Organization	Yes or No
JRO00088)	
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes

Organization	Yes or No
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Lakeland Electric	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
PSEG	Yes
Texas Reliability Entity	Yes
NIPSCO	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes

Organization	Yes or No
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

3. CIP-004-5 R3 states "Each Responsible Entity shall implement its documented role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
ACES Power Marketing	No
IRC Standards Review Committee	No

Organization	Yes or No
CenterPoint Energy	No
PNM Resources	No
CIP Version 5 Comment SME list	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Northeast Utilities	No
Nebraska Public Power District	No

Organization	Yes or No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
Alliant Energy	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes

Organization	Yes or No
NRG Energy Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
SPP and Member companies	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Hydro One	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes

Organization	Yes or No
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
PSEG	Yes
Texas Reliability Entity	Yes
NIPSCO	Yes

Organization	Yes or No
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

4. CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
Texas RE NERC Standards Review Subcommittee	No
Colorado Springs Utilities	No
ACES Power Marketing	No
IRC Standards Review	No

Organization	Yes or No
Committee	
CenterPoint Energy	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Southern Company Services, Inc.	No
Southern California Edison company	No
Progress Energy	No
LCEC	No
Bonneville Power Administration	No
Snohomish County PUD	No
MidAmerican Energy Company	No

Organization	Yes or No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Utility Services Inc	No
New York Power Authority	No

Organization	Yes or No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
Southwest Power Pool Regional Entity	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes

Organization	Yes or No
NCEMC	Yes
SPP and Member companies	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Arizona Public Service Company	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Independent Electricity System Operator	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services	Yes

Organization	Yes or No
Corporation	
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
MEAG Power	Yes
Portland General Electric	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of	Yes

Organization	Yes or No
Water and Power	
US Bureau of Reclamation	Yes
California ISO	Yes

5. CIP-004-5 R5 states "Each Responsible Entity shall implement one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Texas RE NERC Standards Review Subcommittee	No
ACES Power Marketing	No
IRC Standards Review Committee	No
Salt River Project	No
Southern California Edison company	No
Progress Energy	No
LCEC	No
MidAmerican Energy	No

Organization	Yes or No
Company	
Lakeland Electric	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
PSEG	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Northeast Power Coordinating Council	Yes

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	Yes
NRG Energy Companies	Yes
Duke Energy	Yes
PNGC Comment Group	Yes
Dominion	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes

Organization	Yes or No
SPP and Member companies	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
BC Hydro	Yes
Hydro One	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Independent Electricity	Yes

Organization	Yes or No
System Operator	
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes

Organization	Yes or No
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
NIPSCO	Yes
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes

Organization	Yes or No
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

Organization	Yes or No
Kansas City Power & Light	Yes
California ISO	Yes

6. CIP-004-5 R6 states "Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R6?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
FirstEnergy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
Pepco Holdings Inc & Affiliates	No
SMUD & BANC	No

Organization	Yes or No
PNM Resources	No
CIP Version 5 Comment SME list	No
Southern Company Services, Inc.	No
Southern California Edison company	No
Progress Energy	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Xcel Energy	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Lakeland Electric	No
Ameren	No

Organization	Yes or No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
NYISO	No
Farmington Electric Utility System	No
Kansas City Power & Light	No
California ISO	No
Northeast Power Coordinating Council	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Hydro One	Yes
Arizona Public Service	Yes

Organization	Yes or No
Company	
Western Area Power Administration	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
NIPSCO	Yes
ISO New England Inc.	Yes

Organization	Yes or No
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes

Organization	Yes or No
US Bureau of Reclamation	Yes

7. CIP-004-5 R7 states "Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R7?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Colorado Springs Utilities	No

Organization	Yes or No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Florida Municipal Power Agency	No
SMUD & BANC	No
ACES Power Marketing	No
SPP and Member companies	No
Puget Sound Energy, Inc.	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Arizona Public Service Company	No
Southern Company Services, Inc.	No
Southern California Edison company	No

Organization	Yes or No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
ATCO Electric	No
LCEC	No
Consumers Energy Company	No
Xcel Energy	No
NV Energy	No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No

Organization	Yes or No
Lakeland Electric	No
Ameren	No
NextEra Energy, Inc.	No
Northeast Utilities	No
Texas Reliability Entity	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
MEAG Power	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Network & Security Technologies, Inc.	No
Alliant Energy	No
New York Power Authority	No
Springfield Utility Board	No
NYISO	No
Farmington Electric Utility System	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Los Angeles Department of Water and Power	No
Brazos Electric Power Cooperative	No
US Bureau of Reclamation	No
Kansas City Power & Light	No
California ISO	No

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	Yes
PNGC Comment Group	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Services	Yes

Organization	Yes or No
Corporation	
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
PSEG	Yes
Portland General Electric	Yes
Utility Services Inc	Yes
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes

Organization	Yes or No
Cowlitz County PUD	Yes

10. CIP-005-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
MRO NSRF	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
ACES Power Marketing	No

Organization	Yes or No
SPP and Member companies	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
CIP Version 5 Comment SME list	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Xcel Energy	No
Bonneville Power Administration	No
Tampa Electric Company	No
MidAmerican Energy	No

Organization	Yes or No
Company	
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Alliant Energy	No
New York Power Authority	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No

Organization	Yes or No
NRG Energy Companies	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Oncor Electric Delivery Company LLC	Yes

Organization	Yes or No
NIPSCO	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of	Yes

Organization	Yes or No
Water and Power	
US Bureau of Reclamation	Yes

11. CIP-005-5 R2 states "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No

Organization	Yes or No
ACES Power Marketing	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
Progress Energy	No
Hydro-Quebec TransEnergie	No
Lincoln Electric System	No
Bonneville Power Administration	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No

Organization	Yes or No
PSEG	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
New York Power Authority	No
NYISO	No
Tucson Electric Power	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
Southwest Power Pool Regional Entity	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Southern California Edison company	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba	Yes

Organization	Yes or No
National Grid)	
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
NIPSCO	Yes
MEAG Power	Yes

Organization	Yes or No
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

14. CIP-006-5 R1 states "Each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards	No

Organization	Yes or No
Review Subcommittee	
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Florida Municipal Power Agency	No
NCEMC	No
ACES Power Marketing	No
SPP and Member companies	No
IRC Standards Review Committee	No
CenterPoint Energy	No
Puget Sound Energy, Inc.	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Arizona Public Service	No

Organization	Yes or No
Company	
Southern Company Services, Inc.	No
Western Area Power Administration	No
Salt River Project	No
National Rural Electric Cooperative Association (NRECA)	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Lower Colorado River Authority	No
LCEC	No
LCRA Transmission Services Corporation	No

Organization	Yes or No
Lincoln Electric System	No
United illuminating Company	No
Xcel Energy	No
NV Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Lakeland Electric	No
Tennessee Valley Authority	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Northeast Utilities	No
PSEG	No

Organization	Yes or No
San Diego Gas & Electric	No
Texas Reliability Entity	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
MEAG Power	No
Portland General Electric	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Alliant Energy	No

Organization	Yes or No
Pacific Gas and Electric Company	No
NYISO	No
Exelon Corporation and its affiliates	No
Deseret Power	No
Los Angeles Department of Water and Power	No
Brazos Electric Power Cooperative	No
US Bureau of Reclamation	No
Kansas City Power & Light	No
California ISO	No
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Pepco Holdings Inc & Affiliates	Yes
Tri-State G&T - Transmission	Yes

Organization	Yes or No
Southern California Edison company	Yes
Clallam County PUD No.1	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
The Empire District Electric Company	Yes
Utility Services Inc	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Farmington Electric Utility	Yes

Organization	Yes or No
System	
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes

15. CIP-006-5 R2 states "Each Responsible Entity shall implement one or more documented visitor control programs that include each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Duke Energy	No
Dominion	No
Florida Municipal Power Agency	No
PNM Resources	No
BC Hydro	No
Western Area Power Administration	No
Progress Energy	No
Independent Electricity	No

Organization	Yes or No
System Operator	
Hydro-Quebec TransEnergie	No
LCEC	No
Xcel Energy	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Lakeland Electric	No
NextEra Energy, Inc.	No
PJM Interconnection	No
Wisconsin Electric Power Company	No
Portland General Electric	No
City Utilities of Springfield, MO	No
NYISO	No
Exelon Corporation and its	No

Organization	Yes or No
affiliates	
Deseret Power	No
Los Angeles Department of Water and Power	No
California ISO	No
Northeast Power Coordinating Council	Yes
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC)	Yes

Organization	Yes or No
including OPC, GTC & GSOC	
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Hydro One	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes

Organization	Yes or No
Southern California Edison company	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power	Yes

Organization	Yes or No
Administration	
Snohomish County PUD	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Oncor Electric Delivery Company LLC	Yes
NIPSCO	Yes
City of Austin dba Austin Energy	Yes

Organization	Yes or No
ISO New England Inc.	Yes
MEAG Power	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

Organization	Yes or No
Kansas City Power & Light	Yes

16. CIP-006-5 R3 states "Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
NESCOR/NESCO	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
IRC Standards Review Committee	No
CenterPoint Energy	No

Organization	Yes or No
PNM Resources	No
Hydro One	No
Western Area Power Administration	No
Progress Energy	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
LCEC	No
Xcel Energy	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Lakeland Electric	No
NextEra Energy, Inc.	No

Organization	Yes or No
Texas Reliability Entity	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
Portland General Electric	No
City Utilities of Springfield, MO	No
New York Power Authority	No
Los Angeles Department of Water and Power	No
PPL Corporation NERC Registered Affiliates	Yes
Duke Energy	Yes
Dominion	Yes
FirstEnergy	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Southern California Edison company	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
NIPSCO	Yes
MEAG Power	Yes
Network & Security	Yes

Organization	Yes or No
Technologies, Inc.	
Utility Services Inc	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

Organization	Yes or No
Kansas City Power & Light	Yes
California ISO	Yes

18. CIP-007-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Florida Municipal Power Agency	No
SMUD & BANC	No

Organization	Yes or No
CenterPoint Energy	No
PNM Resources	No
Western Area Power Administration	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
LCEC	No
Consumers Energy Company	No
Xcel Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
MidAmerican Energy	No

Organization	Yes or No
Company	
Lakeland Electric	No
NextEra Energy, Inc.	No
PJM Interconnection	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
NYISO	No
Exelon Corporation and its affiliates	No
Kansas City Power & Light	No
California ISO	No
Northeast Power Coordinating Council	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
MRO NSRF	Yes

Organization	Yes or No
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Hydro One	Yes
CIP Version 5 Comment SME list	Yes

Organization	Yes or No
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
NV Energy	Yes

Organization	Yes or No
Snohomish County PUD	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Oncor Electric Delivery Company LLC	Yes
NIPSCO	Yes
City of Austin dba Austin Energy	Yes

Organization	Yes or No
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

19. CIP-007-5 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
SMUD & BANC	No
CenterPoint Energy	No
PNM Resources	No

Organization	Yes or No
Hydro One	No
Arizona Public Service Company	No
Western Area Power Administration	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Hydro-Quebec TransEnergie	No
LCEC	No
Lincoln Electric System	No
Xcel Energy	No
Bonneville Power Administration	No
Tampa Electric Company	No
MidAmerican Energy Company	No

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Utility Services Inc	No
Alliant Energy	No
New York Power Authority	No

Organization	Yes or No
Pacific Gas and Electric Company	No
NYISO	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Kansas City Power & Light	No
PPL Corporation NERC Registered Affiliates	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
Dominion	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power	Yes

Organization	Yes or No
Agency	
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Independent Electricity System Operator	Yes

Organization	Yes or No
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
NIPSCO	Yes
MEAG Power	Yes
Portland General Electric	Yes
Springfield Utility Board	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power	Yes

Organization	Yes or No
Cooperative	
US Bureau of Reclamation	Yes
California ISO	Yes

20. CIP-007-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
SPP and Member companies	No
CenterPoint Energy	No

Organization	Yes or No
PNM Resources	No
Hydro One	No
CIP Version 5 Comment SME list	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Bonneville Power Administration	No
Snohomish County PUD	No
MidAmerican Energy Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No

Organization	Yes or No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Alliant Energy	No
New York Power Authority	No
Pacific Gas and Electric Company	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC	Yes

Organization	Yes or No
Registered Affiliates	
NRG Energy Companies	Yes
PNGC Comment Group	Yes
Dominion	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes

Organization	Yes or No
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes

Organization	Yes or No
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes

Organization	Yes or No
NIPSCO	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes

Organization	Yes or No
US Bureau of Reclamation	Yes

21. CIP-007-5 R4 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No

Organization	Yes or No
SMUD & BANC	No
SPP and Member companies	No
IRC Standards Review Committee	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
CIP Version 5 Comment SME list	No
Western Area Power Administration	No
Salt River Project	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No

Organization	Yes or No
Hydro-Quebec TransEnergie	No
Lower Colorado River Authority	No
LCEC	No
LCRA Transmission Services Corporation	No
Niagara Mohawk (dba National Grid)	No
National Grid	No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Lakeland Electric	No

Organization	Yes or No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
PSEG	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Utility Services Inc	No

Organization	Yes or No
Alliant Energy	No
New York Power Authority	No
Pacific Gas and Electric Company	No
NYISO	No
Tucson Electric Power	No
Los Angeles Department of Water and Power	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC Registered Affiliates	Yes
PNGC Comment Group	Yes
Dominion	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes

Organization	Yes or No
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Clallam County PUD No.1	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
United illuminating Company	Yes
Xcel Energy	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
MEAG Power	Yes
Portland General Electric	Yes
Springfield Utility Board	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes

Organization	Yes or No
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

22. CIP-007-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No

Organization	Yes or No
SMUD & BANC	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
Southern Company Services, Inc.	No
Salt River Project	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Lower Colorado River Authority	No
LCRA Transmission Services Corporation	No
Consumers Energy Company	No

Organization	Yes or No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Lakeland Electric	No
Tennessee Valley Authority	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No

Organization	Yes or No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
Portland General Electric	No
City Utilities of Springfield, MO	No
Alliant Energy	No
New York Power Authority	No
NYISO	No
Tucson Electric Power	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC Registered Affiliates	Yes
PNGC Comment Group	Yes
Associated Electric	Yes

Organization	Yes or No
Cooperative, Inc (NCR01177, JRO00088)	
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Western Area Power Administration	Yes
Clallam County PUD No.1	Yes
Hydro-Quebec TransEnergie	Yes
ATCO Electric	Yes
LCEC	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Northeast Utilities	Yes
PSEG	Yes

Organization	Yes or No
Texas Reliability Entity	Yes
NIPSCO	Yes
MEAG Power	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

Organization	Yes or No
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards
Comment Form C
CIP-008 through CIP-011

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Index to Questions, Comments, and Responses

Questions with Summaries Included: 16
QUESTION C4 – CIP-008-5: 16
QUESTION C8 – CIP-009-5: 26
QUESTION C12 – CIP-010-1: 39
QUESTION C15 – CIP-011-5: 63
Questions with Votes Only: 71
1. CIP-008-5 R1 states "Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 71
2. CIP-008-5 R2 states "Each Responsible Entity shall implement its documented Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 78
3. CIP-008-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?..... 85
5. CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?..... 92
6. CIP-009-5 R2 states "Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 99
7. CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3? 106
9. CIP-010-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration

Change Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 113

10. CIP-010-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 120

11. CIP-010-1 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3? 127

13. CIP-011-1 R1 states "Each Responsible Entity shall implement an information protection program that includes each of the applicable items in CIP-011-1 Table R1 – Information Protection." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1? 134

14. CIP-011-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2? 141

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
11. Bruce Metruck	New York Power Authority	NPCC 6										
12. Lee Pedowicz	Northeast Power Coordinating Council	NPCC 10										
13. Robert Pellegrini	The United Illuminating Company	NPCC 1										
14. Si Truc Phan	Hydro-Quebec TransEnergie	NPCC 1										
15. David Ramkalawan	Ontario Power Generation, Inc.	NPCC 5										
16. Brian Robinson	Utility Services	NPCC 8										
17. Michael Jones	National Grid	NPCC 1										
18. Michael Schiavone	National Grid	NPCC 1										
19. Wayne Sipperly	New York Power Authority	NPCC 5										
20. Tina Teng	Independent Electricity System Operator	NPCC 2										
21. Don Weaver	New Brunswick System Operator	NPCC 2										
22. Ben Wu	Orange and Rockland Utilities	NPCC 1										
23. Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC 3										
24. Silvia Parada Mitchell	NextEra Energy, LLC	NPCC 5										
2. Group	Annabelle Lee	NESCOR/NESCO										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3. Group	Jason Marshall	ACES Power Marketing						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Tim Soles	Occidental Power Services, Inc.	ERCOT 3										
4.	Andy Gallo	Austin Energy	ERCOT 1										
5.	Andy Gallo	Austin Energy	ERCOT 3										
6.	Andy Gallo	Austin Energy	ERCOT 4										
7.	Andy Gallo	Austin Energy	ERCOT 5										
8.	Andy Gallo	Austin Energy	ERCOT 6										
8.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8. Annie Terracciano	Northern Lights Inc.	WECC 3										
9. Aleka Scott	PNGC	WECC 4										
10. Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11. Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12. Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13. Margaret Ryan	PNGC	WECC 8										
12. Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13. Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14. Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. M & A Electric Power Cooperative		SERC	1, 3									
4. Northeast Missouri Electric Power Cooperative		SERC	1, 3									
5. N.W. Electric Power Cooperative, Inc.		SERC	1, 3									
6. Sho-Me Power Electric Cooperative		SERC	1, 3									
15. Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X						
Additional Member	Additional Organization	Region	Segment Selection									
1. Oglethorpe Power Corporation		SERC	5									
2. Georgia Transmission Corporation		SERC	1									
16. Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X
Additional Member	Additional Organization	Region	Segment Selection									
1. MAHMOOD SAFI	OPPD	MRO	1, 3, 5, 6									
2. CHUCK LAWERENCE	ATC	MRO	1									
3. TOM WEBB	WPS	MRO	3, 4, 5, 6									
4. JODI JENSON	WAPA	MRO	1, 6									
5. KEN GOLDSMITH	ALTW	MRO	4									
6. DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6									
7. JOE DEPOORTER	MGE	MRO	3, 4, 5, 6									
8. SCOTT NICKELS	RPU	MRO	4									
9. TERRY HARBOUR	MEC	MRO	1, 3, 5, 6									
10. MARIE KNOX	MISO	MRO	2									
11. LEE KITTELSON	OTP	MRO	1, 3, 4, 5									
12. SCOTT BOS	MPW	MRO	6, 1, 3, 5									
13. TONY EDDLEMAN	NPPD	MRO	1, 3, 5									
14. THERESA ALLARD	MPC	MRO	1, 3, 5, 6									
17. Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing												
18. Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				
Additional Member	Additional Organization	Region	Segment Selection									
1. Timothy Beyrle	City of New Smyrna Beach	FRCC	4									
2. James Howard	Lakeland Electric	FRCC	3									

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
3. Greg Woessner	Kissimmee Utility Authority	FRCC 3										
4. Lynne Mila	City of Clewiston	FRCC 3										
5. Joe Stonecipher	Beaches Energy Services	FRCC 1										
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC 4										
7. Randy Hahn	Ocala Utility Services	FRCC 3										
19. Group	Joseph DePoorter	Madison Gas and Electric Company			X	X	X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Darl Shimko	MGE	MRO 3										
2. Joseph DePoorter	MGE	MRO 4										
3. Steve Schultz	MGE	MRO 5										
4. Jeff Keebler	MGE	MRO 6										
20. Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							
Additional Member	Additional Organization	Region Segment Selection										
1. Mark Jones	Pepco	RFC 1										
21. Group	Rick Terrill	Luminant					X					
Additional Member	Additional Organization	Region Segment Selection										
1. Mike Laney	Luminant Generation Company LLC	ERCOT 5										
2. Tim Soles	Occidental Power Services, Inc.	ERCOT 6										
3. Tim Soles	Occidental Power Services, Inc.	ERCOT 3										
4. Andy Gallo	Austin Energy	ERCOT 1										
5. Andy Gallo	Austin Energy	ERCOT 3										
6. Andy Gallo	Austin Energy	ERCOT 4										
7. Andy Gallo	Austin Energy	ERCOT 5										
8. Andy Gallo	Austin Energy	ERCOT 6										
9. Brenda Hampton	Luminant Energy Company LLC											
22. Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X				
Additional Member	Additional Organization	Region Segment Selection										
1. Kevin Smith	BANC	WECC 1										
23. Group	Scott Brame	NCEMC	X				X					
Additional Member	Additional Organization	Region Segment Selection										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Rayburn Country Electric Cooperative			SPP										
2. Empire District Electric			SPP	1									
3. City Utilities of Springfield			SPP	4									
4. Westar Energy			SPP	1, 3, 5, 6									
5. Cleco Power			SPP	1, 3, 5, 6									
25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Pawel Krupa			WECC	1									
2. Dana Wheelock			WECC	3									
3. Hao Li			WECC	4									
27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Denise Lietz		Puget Sound Energy	WECC	1									
2. Erin Apperson		Puget Sound Energy	WECC	3									
28.	Group	Michael Mertz	PNM Resources	X		X							
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Laurie Williams		Public Service Co. of New Mexico	WECC	1									
2. Michael Mertz		Public Service Co. of New Mexico	WECC	3									
29.	Group	Sasa Maljukan	Hydro One	X									
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. David Kiguel		Hydro One	NPCC	1									
30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION C4 – CIP-008-5:

If you disagree with the changes made to CIP-008-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, most of the comments resulted in changes that improved clarity and did not require significant structural revisions. The consideration of comments according to major issues and standard sections follows.

References to EOP-004-2

The comments received for CIP-008-5 and EOP-004-2 both indicated support for handling the reporting of Cyber Security Incidents in CIP-008-5. EOP-004-2 received a much lower ballot approval in its most recent posting primarily for the one hour timeframe required for reporting Cyber Security Incidents. The commenters concern for EOP-004-2 was the lack of a timeframe for identifying a Cyber Security Incident. The required CIP-008-5 processes make clear that reporting to the ES-ISAC occurs within one hour of the analysis to determine whether an event would constitute a Cyber Security Incident. As a result, both drafting teams agreed to move the Cyber Security Incident reporting to the ES-ISAC to CIP-008-5. However, the SDT wishes to stress the reporting threshold is not necessarily one hour from the Cyber Security Incident occurrence. Instead, the threshold accounts for the analysis that must be performed in identifying the Cyber Security Incident. The incident could even have occurred much earlier without any observable behavior. Also, entities can still have a single reporting process to comply with the new versions of EOP-004 and CIP-008.

Applicability Section

Several commented that all instances of Medium Impact BES Cyber Systems should be changed to "Medium Impact BES Cyber Systems with External Routable Connectivity". In response, we note that CIP-008-5 addresses incident response and reporting and the lack of external routable connectivity would not address this issue. It is possible for a Cyber Security Incident to occur on such cyber systems through insider attacks or other means of penetrating the physical or electronic boundaries. This does not create an inconsistency among the standards or implied requirement for monitoring because an entity can have a monitoring program to detect incidents that does not fully meet the requirements of CIP-006-5 and CIP-007-5.

There were several comments that stated CIP-008-5 should apply to Electronic Access Control and Monitoring Systems and Physical Access Control Systems. In response, applicability to these systems is unnecessary because the incident is associated to the BES Cyber Systems. Incidents occurring on perimeter systems would target the system and not the perimeter.

Other General Comments

One commenter requested clarification why the word "dated" has been added to the measures in these requirements. In response, dated documentation is used to clarify that such evidence is necessary to demonstrate time-based requirements.

There was a comment that suggested the word "annual" should be a defined in the NERC Glossary. In response, the SDT has chosen not to define annual because the periodicity for requirements in CIP may be different than requirements in other standards, and the definition of annual may have many interpretations.

Guidelines

One commenter suggested that references to DHS and NIST should not reside in the standard because NERC does not track those documents to ensure consistency. In response, the external references are dated to a specific version to address the case where future revisions do not remain consistent with the standard.

There was a comment that the definition of Reportable Cyber Security Incident is too vague and could result in the interpretation that activation of redundant systems causes the reporting not to be considered. In response, the SDT has clarified in the guideline that this is not the case. The SDT has added a clarification that the absence of lessons learned must still be documented.

One commenter proposed revisions requirements to "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has considered this approach and has added to certain requirements "… identify, assess, and correct deficiencies…", which is explained in detail in the global summary portion of this document, above.

Background

One commenter stated that the background section for CIP-008-5 is contradictory in reference to measures by stating a numbered list is all-inclusive but measures serve only as examples. In response, the SDT notes that the background section states "A numbered list in the measure means the evidence example". This means the example evidence must include all of the items, but there may be other examples of evidence to meet the requirement. Both statements are true.

Requirement Part 1.1 and 1.2
Based on a comment, the SDT changed "Processes" to "One or more processes" for clarity.

Several commenters propose including additional specificity in the process for determining if an incident is reportable. The SDT has extensively discussed this issue, and the problem with additional specificity in Cyber Security Incidents is difficulty in exhaustively enumerating situations to report. Also, the reporting of incidents associated with damage alone can result in under-reporting, which does not meet the objective of this Requirement.

Requirement Part 1.4
Several commenters stated that 1.1 (responding) and 1.4 (handling) are essentially the same and proposed to delete 1.4**.** The SDT notes that while 1.1 addresses the initial identification and response to incidents, 1.4 addresses the actions to perform for resolving individual incidents. These are distinct activities.

One commenter suggested the that the applicability include low impact BES Cyber Systems because CIP-003-5 requires implementation of a policy addressing incident response, but CIP-003-5 intentionally centralizes all the requirements for low impact BES Cyber Systems which does not include specific elements of the plan.

There was a comment that suggested removing the parenthetical phrase for incident handling because recovery and post-incident analysis are covered elsewhere. In response, the SDT agrees that post-incident analysis is already handled in Requirement R3 of CIP-008-5 and clarifies the recover activities here pertain only to the incident. Recovery includes the confirmation that the incident has been resolved.

One commenter suggested adding wording to clarify physical security incidents need to be considered. In response, the SDT notes that the definition of Cyber Security Incidents includes physical intrusions.

Requirement Part 1.5

There was a comment that stated it is unclear if the list of internal and external contacts refer to those in EOP-004-2 or if there is a need to have a minimum list of contacts. In response, the internal or external contacts that an entity would need to include to ensure proper reporting for EOP-004-2 should be part of this list. Additional contacts are appropriate as necessary components of an incident response plan, but who resides in this list is left up to the entity.

A commenter suggested that the use of external organizations could result in double jeopardy with EOP-004-2. However, EOP-004-2 requires specific organizations whereas CIP-008-5 leaves the inclusion of additional external organizations up to the entity as a necessary part of the incident response plan. Double jeopardy does not exist here because there is not a requirement in CIP-008-5 to report.

One commenter proposed to replace the phrase "should receive communication" with "must be sent communication". In response, the SDT notes that this part of the incident response plan does not necessarily constitute required communication, but communication must be covered as a component of the plan.

Requirement R2

One commenter proposed adding an exception for the timeframes based on CIP Exceptional Circumstances. In response, the SDT notes that CIP Exceptional Circumstances have not applied to annual periodic performances requirements because of the flexibility in the timeframe of when an entity can perform this requirement.

Requirement Part 2.1

In response to a comment that 2.1 should expand to include all Cyber Security Incidents, the SDT continues to limit these requirements to Reportable Cyber Security Incidents because of the lessons learned and plan updates associated with each Reportable Cyber Security Incident. It is possible for Cyber Security Incidents to occur much more frequently.

In response to a comment, the SDT has removed the word "BES" before "BES Incident Response Plan" for consistency.

One commenter suggested revising the language of "at least once each calendar year, not to exceed 15 calendar months between executions" to "once each calendar year or a period not to exceed 15 calendar months between executions". The SDT notes that the language that exists is sufficient as currently written.

One commenter suggested using the term “exercise” instead of “test” because an actual exercise would suffice. In response, we had several comments to the contrary in the previous posting. The SDT uses test here because the word “exercise” is commonly used in reference to a planned execution.

One commenter suggested removing the lessons learned report from the measure because it is not part of the requirement. In response, we note that the measure only serves as an example, and a lessons-learned report would be an example measure for 2.1.

One commenter suggested that a full operational exercise should be required in the absence of an actual incident. In response, we suggest that the quality of an exercise does not depend on the type. It is possible to have a higher quality tabletop exercise than a full operational exercise.

One commenter suggested placing an “or” between all exercise examples, but this is not necessary because the “or” in the second bullet qualifies the entire list.

One commenter suggested expanding the scope of actual incidents that qualify as an exercise to include any Cyber Security Incident, but this would not exercise a key component of identifying and communicating a Reportable Cyber Security Incident.

One commenter proposed to remove any timeframes associated with the test. The SDT disagrees because absence of time requirements makes the expected performance of the standard less clear and does not respond to directives from the FERC Order 706.

Two commenters suggested adding a specific reference to R1 to clarify the linkage, but the context of the Requirement in its use of Cyber Security Incident response plan is clear enough to avoid needing a direct linkage.

In response to several commenters, the word “plan(s)” was modified to “each plan” for added clarity.

In response to one commenter, the SDT qualified that the phrase “when responding to” is in regards to the Reportable BES Cyber Security Incident.

Based on comments, the SDT clarified exercises were for Reportable Cyber Security Incidents.

Based on comments, the SDT has removed the word “BES” from this requirement part.

Requirement Part 2.2
One commenter stated that this requirement part should be deleted because the main requirement part already addresses implementation and documented deviations are redundant with lessons learned. In response, the SDT points out that implementation of the plan does not necessarily mean that it be used during an incident or exercise. Some entities may interpret that a plan is implemented regardless of whether or not it is actually used. This additional requirement adds clarity in the expected outcome. The same is also true of lessons learned not having the full meaning of documenting deviations from the plan. However, we agree that the documentation should not necessarily occur concurrent with the incident and have modified this requirement part accordingly.

One commenter suggested requiring documentation for the lack of deviations from the plan. In response, we do not agree this language is necessary. The absence of deviations may be a common occurrence and the requirement to have such documentation is highly administrative. We believe this is different than the case of not having any lessons learned which should be a much less common occurrence.

One commenter suggested requiring plan updates for new vulnerabilities and threats. The SDT agrees this would be appropriate if the plan were not sufficient to address new vulnerabilities and threats, but measurable criteria for what constitutes a new vulnerability or threat does not exist and could likely not be determined by anyone other than the Responsible Entity.

In response to a comment, the SDT replaced the phrase “incident response plan” with “Cyber Security Incident response plan” for consistency.

In response to several commenters, the word “plan” was changed to “plan(s)” for consistency.

Requirement Part 2.3
One commenter proposed that 2.3 should be moved to the compliance evidence section of the standard. In response, the evidence retention section cannot add a new requirement, and without 2.3 there is no requirement to retain evidence of the incident.

Several commenters suggested the language for requirement part 2.3 include a retention period, but this requirement was modified in response to comments that the retention period be covered in the compliance evidence section of the standard. As a result, part 2.3 includes the requirement to retain the records, which may not have been necessary to retain anywhere else in the standard, and the compliance evidence section defines the retention period.

There were several commenters who stated that this requirement part could have double jeopardy with EOP-004-2, but lack of documentation for reporting purposes would not be a violation of CIP-008-5. Also, EOP-004-2 evidence retention does not necessarily cover evidence related to a Cyber Security Incident.

One commenter suggested storing the evidence in encrypted form. In response, CIP-011-1 addresses the storage of BES Cyber System Information. Specific implementation of this requirement is appropriately left to the entity.

The SDT has removed the word "relevant" responding to comments that it adds unneeded subjectivity.

One commenter questioned whether three calendar years is sufficient for retaining incident evidence for law enforcement, state, and federal requirements, but the evidence retention is a minimum for the purpose of the Standard. If additional requirements outside of the NERC Reliability Standards indicate a longer retention period for a particular entity, then the entity would choose the longer period. There is no conflict.

Requirement R3

One commenter proposed that the main requirement should more closely align with CIP-009-5 R3 and focus on maintaining, and not implementing, the plan. The SDT agrees.

One commenter suggested the word "full" be deleted from "full operational exercise" because it is unclear what it implies. The SDT agrees.

Requirement Part 3.1

Several entities have commented this requirement part is duplicative with testing in R2 and monitoring for plan changes in R3. The SDT agrees and has deleted this requirement part.

In response to a comment that proposed to consider additional changes that trigger a review of the incident response plan, the lessons learned requirements suffice for updating the plan in response to incidents. Changes to the security

configuration already trigger updates in requirement part 3.4. In many cases the incident response plan is written at a high enough level to preclude necessitating changes in response to new threats and vulnerabilities.

Requirement Part 3.2

There were several comments that the various dates for updating the plan significantly increase the compliance tracking burden and that a plan has not truly updated until the entity distributes those updates to the required individuals. The SDT agrees and has collapsed previously posted requirement parts 3.2, 3.3 and 3.5 into a single requirement part 3.1. The additional requirement part 3.4 for monitoring plan changes and 3.5 has collapsed into a single requirement part 3.2. Some commenters suggested that both requirements should allow a consistent 90 days, but the updating of the plan in response to changes does not require the same level of updates as those required from lessons learned. Therefore the different timeframes in these requirement parts are appropriate.

One commenter suggested tying this requirement explicitly with both 2.1 and 2.2. In response, the cross-referencing of requirements could cause more confusion than clarity. The SDT feels this explicit tie is best accomplished in the guidance.

One comment proposed to remove any timeframes associated with plan updates. The SDT disagrees because absence of time requirements makes the expected performance of the standard less clear and does not respond to directives from the FERC Order 706.

There was a comment that suggested that 30 days may not be sufficient time to make complex changes from lessons learned. In response, the SDT believes the updated requirement allowing 90 days for the complete time is sufficient for even complex changes.

One commenter suggested changing this requirement part to include language for consistency with the ERO Event Analysis Process. The ERO Events Analysis Process is not a NERC Reliability Standard, and the SDT is not mandating referenced actions that are not developed through the NERC process or an equivalent ANSI Certified process. The SDT also notes that the proposed requirement language leaves flexible “how” to perform the requirement. Entities may choose to follow the procedures outlined in the ERO Events Analysis Process to comply with the requirement, but are not required to. The SDT also understands that the NERC CIPC is planning to form a working group to develop guidelines for analyzing cybersecurity events using a parallel process to the recently approved ERO Events Analysis Process. Specifying

that the ERO Events Analysis Process be used in response to CIP-008 Reportable Cybersecurity Incidents is premature and will remove any perceived or required flexibility in developing cybersecurity-specific procedures under that group.

Several commenters suggested clarifying the expectation when there are no lessons learned. In response, we have made this explicit in both the requirement and measure.

In response to one comment, the SDT has added examples of evidence for lessons learned.

In responses to multiple comments, the SDT changed the phrase "within 90 days" to "not to exceed 90 calendar days" for clarity.

Requirement Part 3.3
In response to a comment, it is not necessary to modify this requirement to state "update as needed" because the requirement part ties to "any lessons learned" which carries the same effect.

Requirement Part 3.4
One commenter suggested reverting to previously approved language for updates and notes that evidence to meet this requirement would include lists of technology changes. In response, the SDT notes that such evidence would be required in the previously approved version if specific technology was referenced in the plan. The changes identified here are to provide additional clarity in the types of changes that should trigger an update.

Several commenters proposed that the term "technology changes" needs to be defined. The SDT notes this only includes technology changes that would impact the ability to execute the plan. Because this term is so contextual to the plan, it would cause more problems to define it. Entities should review their plans to see whether or not they have technology as a key element of the plan. The guidance specifies that "technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems."

Requirement Part 3.5
Several commenters suggested changing the word "distribute" to "notify" for announcing changes to the incident response plan due to the uncertainty of what constitutes distribution and the possible issues with information sensitivity. The SDT agrees.

One commenter suggested the evidence examples of distributing the plan could result in a violation of confidentiality, but, while each example can specify additional mechanisms to preserve confidentiality, this was not the intention of the measure. In some cases, incident response plans may not contain confidential information.

VSLs

One commenter recommended that the documentation of the absence of any lessons learned should be included in the VSLs. In response, the absence of lessons learned has been included in the VSL.

One commenter recommended that the VSL should not include failure to follow the plan during an incident and the VSL associated with lack of documentation of deviations suffices. The SDT agrees and does not need to modify the VSLs.

QUESTION C8 – CIP-009-5:

If you disagree with the changes made in CIP-009-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the primary concerns regarding CIP-009-5 expressed in comments were (1) backup media verification procedures in requirement parts 1.4 and 2.2, (2) data preservation procedures in 1.5 and (3) timeframe requirements in Requirement R3 on the lessons learned and plan update activities. The consideration of comments according to major issues and standard sections follows.

Applicability

One commenter suggested that the applicability for all requirements in this standard should limit to Medium Impact BES Cyber Systems at Control Centers to appropriately focus on the higher risk cyber systems and avoid conflict with PRC Standards. In response, the loss of Medium Impact BES Cyber Systems has impact to the BES and the recovery operation for these cyber systems should be addressed in this standard.

The applicability is limited to high impact and medium impact at control centers, along with their associated EACs and PACs, which means testing for substations and generating plants that are not high impact is not included. A commenter asked for confirmation on whether this was the SDT's intent. Yes, it was.

One comment suggested that applicability to associated Cyber Assets should be removed because the FERC has not directed to do so. In response, these continue to apply from all prior versions to the associated Cyber Assets.

Other General Comments

One commenter proposed modifying the main requirement part and corresponding VSLs for R2 and R3 to allow for a flaw remediation process. In response, we have modified the main requirement part for R2 to eliminate the zero tolerance obligations because of the possible magnitude of plans and backup media which require testing. However, we do not incorporate the same changes for R3 because the requirements here do not have the same zero-tolerance concerns and they specify the procedures that must be in place to ensure better response plan flaw remediation.

Guidelines

Several commented that application guidelines should be included for CIP-009-5, and we have added these.

Background

One commenter suggested that the background section is contradictory by saying that measures are not all-inclusive but numbered list provide an all-inclusive example. In response, the background section states, "A numbered list in the measure means the evidence example includes all of the items in the list." This refers to the single example and is different than an all-inclusive list of evidence examples. Accordingly, if an entity did not provide all parts of the numbered list of evidence, then they would not fully meet the requirement. However, they could still provide alternate forms of evidence outside of the example.

Measures

There was a comment that the measures should be clarified with the following language: "Evidence may include, but is not limited to, a dated, revised Cyber Security Incident Response Plan(s) that (1) includes or references, as appropriate, dated documentation of lessons learned, if any, associated with tests of or actual responses using the Cyber Security Incident Response Plan(s), within 90 days after completion of such test or actual incident response; and (2) reflects changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change." The SDT notes that the language in the requirement is clear and that the measures provide adequate examples of evidence. Each requirement part addresses different levels of that may be expected.

Requirement R1

One comment proposed to add a requirement for restoring the BES Cyber System to a state where it is ready to assume its normal operating role in all respects. They also commented that the requirement should state the level of granularity required for a plan. In response, it would be problematic to standardize and audit a normal operating role. The SDT is uncertain as to the meaning of this term. The purpose of this standard is "to recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES." It is inappropriate to specify the level of detail required for a recovery plan.

Several commenters suggested that the standard is not clear whether the recovery plans are for recovery of the asset, system, or function. In response, the stated purpose for the standard is "to recover reliability functions performed by

BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES."

One commenter asked the following: "is a Business Continuity Plan, where operations are transferred from the main control center and continued at a back-up control centre, considered a recovery plan?" In response, this could constitute a recovery plan according to Requirement R1 with the additional components listed in the requirement parts. However, restoration of the reliability function meets the purpose of this standard.

Requirement Part 1.1
One commenter suggested removing "specific" activations from the measure, and we have done so.

One commenter suggested the minimum conditions for activating a response should be specified. Otherwise entities can choose an inappropriately high bar. In response, any minimum enumeration of recovery conditions would equate to defining system failure and doing so for a highly variant population of systems across the BES is not feasible.

Requirement Part 1.3
Several commenters suggested changing the phrase "BES Cyber System" to "applicable Cyber Assets". However, "restoring BES Cyber System" functionality describes the objective of the requirement part and not the applicability.

One commenter suggested addressing FERC Order 706 paragraph 748 by appending the suggested text from the Order to this Requirement Part addressing backup media. We agree this is clearer and have incorporated their suggestion in requirement part 1.4 because of the difference in applicability from 1.3.

One commenter suggested modifying this requirement part measure to provide alternate forms of evidence and avoid the interpretation that evidence must be shown for each occurrence in a high-frequency operational requirement. In response, the SDT has modified the measure according to these suggestions.

Several commenters suggested removing the qualifier word "successfully" from the measure and the SDT has done so.

One commenter suggested including documented configuration settings, documented build/restoration procedures, and retention of installation media for example evidence. The SDT has added these to the technical guidelines section of the standard.

Several commenters suggested replacing the word “recover” with “restore” to describe the purpose of the backup media. In response, we retain the use of “recover” to avoid confusion. Both words mean to return something to a normal or former condition, and the SDT finds these words can be used interchangeably while still communicating the same concept.

One commenter noted the measure is missing an “and”, and the SDT has corrected this oversight.

Requirement Part 1.4

Several commenters expressed confusion around the term “initially” in the requirement, and the SDT has removed this term by tying the verification processes to the backup and storage processes in 1.3. The resulting language should provide more clarity and eliminates the term “initially”.

One commenter suggested addressing FERC Order 706 paragraphs 732-734 in this requirement section or moving this to guidance. In response, the resulting directive in paragraph 739 is addressed by the proposed text to address 748. Another commenter also supported the proposed language in the FERC Order. In response, verifying the operability of backup media is addressed by verifying successful completion and addressing failures of the backup process. Short of performing a full restoration, monitoring the backup process provides the appropriate assurance in the integrity of the backup for constantly changing systems. We have also added further guidance for this requirement part.

One commenter stated that FERC did not express concern over Physical Access Control Systems and Electronic Access Control and Monitoring Systems and applicability for these should be removed. In response, we retain the applicability from previous versions of the standard to which the FERC Order was addressed.

Several commenters requested further clarification about the meaning of verification of backup media. In response, the verification of backup media is dependent upon the tool performing the backup. This could include checking for read/write errors or performing a checksum during the backup operation. The SDT has clarified this requirement to read verification of successful completion.

One commenter suggested this requirement part be modified to address 3rd parties performing the backup or providing a backup, and the requirement has been modified to address these concerns.

Several commented on the 90 day retention period for the logs specified in this requirement part measure. In response, the reason for having 90 day retention for BES Cyber System logs is the potentially large volume, but there is no such concern for the evidence example for this requirement part.

One commenter does not believe this requirement part belongs as written here, and we note the overall modifications to this requirement part better fits the overall objective of Requirement R1.

One commenter stated that the term "backup media" is antiquated and should be replaced with redundancy terminology. In response, we disagree the term is antiquated, but if redundancy is being used for recovery, then processes should exist to regularly verify the redundancy and address failures.

One commenter asked the following questions: If a single monthly backup succeeds, is that good enough? What is verified initially? Is this a daily check for backups or is weekly verification sufficient? If a log is printed or a snapshot taken monthly for evidence sufficient if alerting to x-number of failures is part of the process or is evidence collection required upon completion of the backup? In response to these questions, the currently proposed requirement does not specify a timing that is sufficient for verification due to the widely varying backup methodologies that exist for the applicable systems. A printed log or periodic automated sampling of the backup process would be considered sufficient evidence for this requirement.

One commenter stated that the only way to verify backup completion is to restore from backup. In response, completion of the backup process or routine is different than successful restoration, and we contend the former can be verified outside of a full restoration.

Requirement Part 1.5

Several commenters suggested replacing the word "event" with the phrase "Cyber Security Incident" to better scope when it is necessary to preserve data. In response, we have made this change and modified the requirement to better qualify the purpose of preservation. The requirement should read clearly that data must be retained until a Cyber Security Incident may be ruled out as the cause of the recovery operation.

One commenter suggested removing this requirement part because it addresses forensics and not recovery. In response, this requirement part ensures data collection procedures are included in the recovery plan to allow the performance of after-the-fact analysis. This is appropriate to require as part of the recovery operation.

One commenter suggested that with changes to the definition of CIP Exceptional Circumstances to include “an imminent or existing hardware, software, or equipment failure”, this requirement would never invoke. Their proposed language incorporates the concept of CIP Exceptional Circumstances, and we have included much of the proposed wording in the revised requirement part. The commenter also proposed to limit this requirement part to Medium Impact BES Cyber Systems at Control Centers, but neither the threat nor the operational circumstances for field assets preclude applicability for this requirement part. This requirement allows sufficient flexibility to apply in widely varying environments. The modifications here also address other comments about clarifying the procedures should not impact reliability.

One comment suggested that the PRC Standards already cover this for relay misoperation, but these standards do not address specifically the failure of a Cyber Asset nor do they address the preservation of data from Cyber Assets.

One commenter stated that this requirement implies an obligation to mirror data in the measure, should be left up to the entity to determine whether or not to delay recover for the purpose of preserving data, and an entity cannot determine the preservation of data given the many ways in which a system can fail. In response, we first note that a measure is only an example and does not imply an obligation to mirror data. Second, the SDT has taken an exception to add an explanatory note in the requirement cautioning against impeding recovery for data preservation. Finally, this requirement part does not envision an entity determining every way in which a Cyber System can fail. This only obligates the entity to include data preservation procedures in the recovery plan. There was a second comment on the guidance language in the measure, and the SDT agrees the language does not readily associate itself to the requirement and has been removed.

One comment suggested that this requirement part should be part of root-cause analysis and not impede system restoration. The SDT agrees and notes the requirement part does not address forensics but only the preservation of data to support root-cause analysis and forensics after-the-fact.

Requirement Part 2.1

One commenter suggested for this requirement part and requirement part 2.3 that the word “exercise” should be used in place of “test” since an actual recovery operation can be used for compliance. However, several commenters suggested the converse in the last posting, and we are not compelled the difference in terminology changes the meaning of the requirement.

One commenter suggested revising the language of “at least once each calendar year, not to exceed 15 calendar months between executions” to “once each calendar year or a period not to exceed 15 calendar months between executions”. The SDT notes that the language that exists is sufficient as currently written.

Several commenters requested clarity about whether or not each recovery plan must be tested annually. In response, we have modified this requirement to explicitly state that each recovery plan must be tested as was the intent. We do not specify a representative sampling of plans be tested as some suggest because the proposals do not include enough information to objectively determine what constitutes a representative sample. However, we do note that it is possible to singularly test multiple cyber systems if they are similar in nature.

One commenter suggested that all backup media should not be required for testing but only the one needed for recovery, and we have modified the requirement to include this condition.

One commenter suggested that “or” should be added to the first bullet point or it is otherwise required. In response, the or in the second bullet point modifies the entire list.

Requirement Part 2.2

One commenter asked if this requirement part includes a media test and whether this can be performed on a sample system. In response, this can include a media test on a sample system provided some verification to ensure the information is current and useable occurs. We have modified the measure for this requirement part to make this clearer.

One commenter suggested allowing an actual recovery operation to substitute for the testing of backup media, and we have made this change.

One commenter proposed to replace the requirement with “Unless covered by EOP-008, test a representative sample of information used in the recovery of BES Cyber Systems that is stored on backup media at least once each calendar

year, or a period not to exceed 15 calendar months between tests, to verify the backup media is operational and the information is useable." The concern surrounds possible double jeopardy with EOP-008 and clarity around "compatibility with current system configurations." In response for EOP-008-1 R7, failure to meet this requirement does not indicate a failure for EOP-008-1 and vise-versa. This requirement concerns the testing of backup media, which may not be used for recovery with EOP-008-1. For the proposed language, we have incorporated the "representative sample of information" in testing to clarify the obligation, but we retain the purpose of verifying compatibility with current system configurations. Only ensuring the usability of backup media does not capture the intent that the backup media is currently usable for performing the BES Cyber System function.

One commenter suggested striking the phrase "to ensure that the information is useable and is compatible with current system configurations" and believes it should be left up to the Responsible Entity to determine, whether another commenter requested further clarification about this phrase. In response, the testing of backup media alone is not specific enough to ensure clarity of the requirement. The phrase in question is necessary for entities to know what they should be testing. We have added additional technical guidelines for this requirement.

One commenter suggested that this requirement should state that a tabletop exercise should not be permitted. In response, the testing of backup media may be performed as a separate process or as a part of the recovery plan exercise. There is not a need to specify which type of exercises aligns with this process.

One commenter suggested that the term "backup media" is antiquated and should be replaced with redundancy terminology. In response, we disagree the term is antiquated, but if redundancy is being used for recovery, then processes should exist to test the redundant systems in accordance with this requirement part.

Several commenters proposed the phrase "validate the integrity of the stored information" as a substitute for current language regarding the testing of backup media. In response, validating the integrity of the information can be interpreted widely from a bit comparison to a sampling. We believe our proposed revisions provide enough specificity and flexibility to be widely applied.

One comment proposed to focus the requirement on backup media rather than information used for recovery. In response, we use the term information here because of the various ways entities implement backup policies, which may include replication technologies. Backup media was not well understood by the team and many participants to include replication.

Requirement Part 2.3

Several comment that the measure references performance of this requirement prior to the Effective Date, and that this requirement part should be included in the Implementation Plan. In response, we have removed this language from the measure and added this requirement part to the Implementation Plan.

One commenter suggested testing a representative of a plan with a rationale that High Impact BES Cyber Systems already have a requirement to test backup media annually. In response, we do not see a significant change in the proposed wording. The requirement to test backup media does not require a full operational restoration.

One commenter requested clarity that all recovery plans do not have to be tested at the same time. In response, the requirement only specifies the obligation to test recovery plans at a periodicity. It would not violate the requirement to test individual plans at different periods while still meeting the periodicity obligation.

One commenter requested a basis for the 36 months period. In response, we incorporated this timeframe from the FERC Order 706 directive.

One commenter suggested testing a "representative" rather than "each" BES Cyber System. In response, if an entity can test a representative BES Cyber System for multiple systems, then they have complied with the requirement to test "each" BES Cyber System.

One commenter noted that an entity may have several failure scenarios and it is unclear if all of these must be tested. In response, we have added guidance in the technical guidelines section of the Standard to clarify that not all failures scenarios must be tested, but that the test should ensure the plan is up to date and test at least one process to restore the applicable cyber systems.

One commenter suggested that EOP-008 R6 should suffice for this requirement part. In response, EOP-008-1 R6 requires independent backup functionality, but this does not imply an obligation to perform a functional test. The compliance processes to comply with EOP-008-1 should certainly ease compliance with this requirement part.

Several respondents asked whether a full operational exercise means a bare-metal recovery and comments that doing so would be cost prohibitive, while another commenter suggested also requested further clarification around

the term "operational exercise". In response, the SDT has provided well established definitions of operational exercises that would comply with the requirement, which do not imply a full recovery demonstration.

Requirement R3
Requirement R3 has been modified to correspond with similar commenter suggestions in CIP-008-5 R3.

One commenter suggested that Requirement R3 does not include defined roles and responsibilities. As we understand the comment, the roles and responsibilities refer to those required parts of the response plan specified in Requirement R1.

Requirement Part 3.1
Several commenters noted that the various dates for updating the plan significantly increase the compliance tracking burden and that a plan has not truly updated until the entity distributes those updates to the required individuals. The SDT agrees and has collapsed previously posted requirement parts 3.1, 3.2 and 3.4 into a single requirement part 3.1. The additional requirement part 3.3 for monitoring plan changes and 3.4 has collapsed into a single requirement part 3.2. Some comment that both requirements should allow a consistent 90 days, but the updating of the plan in response to changes does not require the same level of updates as those required from lessons learned. Therefore the different timeframes in these requirement parts are appropriate.

A few commenters suggested updating plans based on lessons learned is not necessary because these changes would be captured in technology and personnel changes. In response, the updates here capture improvements to the plan as determined through a lessons learned exercise.

One commenter suggested that the evidence collected in requirement part 1.5 should be part of the review process. They also commented that other related plans (i.e. configuration management plans) be updated as necessary as part of the review process. In response, the evidence collected in requirement part 1.5 may not be reviewed by a third party and we do not feel it is necessary to specifically call out this activity in the requirement part. Also, we cannot add an obligation to update other plans as necessary in a way that would be objectively measurable.

One commenter suggested that 30 days may not be sufficient time to make complex changes from lessons learned. In response, the SDT believes the updated requirement allowing 90 days for the complete time is sufficient for even complex changes.

Several commenters have suggested clarifying the expectation when there are no lessons learned. In response, we have made this explicit in both the requirement and measure.

Several commenters stated that requiring entities to perform lessons learned is counterproductive because it encourages entities not to admit there is a deficiency in the first place. In response, the inclusion of a lessons learned process provides a standard practice across the industry, which would otherwise be inconsistency applied at best. Furthermore, it addresses a FERC Order 706 directive to include lessons learned processes as part of a recovery plan test.

Requirement Part 3.3

One commenter suggested modifying the references to other standard requirement parts, removing references to individuals and modifying the communication of plan updates to be more specific. In response, the SDT has made several modifications to Requirement R3 to align with modifications to CIP-008-5 that address these concerns.

Several commenters proposed removing this requirement and addressing plan updates in guidance, but placing the plan items that would trigger a change in guidance would add a high degree of subjectivity to the requirement. Specifying what changes should constitute an update ensures objectivity in demonstrating compliance with this requirement.

One commenter proposed removing this requirement or clarifying the tie back to Requirement R1.2. In response, this requirement is necessary to ensure the recovery plan remains current and carries forward from the requirement to update on any changes. They also expressed concern that this requirement part could be interpreted that a change to any plan must be communicated to all individuals specified in requirement part 1.2. In response, we have removed the explicit tie to requirement part 1.2 to avoid such an interpretation.

One commenter suggested that the plan maintenance would create an undue compliance burden. In response, the SDT notes this requirement carries forward from previous versions and ensures the recovery plans remain up to date through organizational changes.

Requirement Part 3.4

Several commenters suggested changing the word “distribute” to “notify” for announcing changes to the incident response plan due to the uncertainty of what constitutes distribution and the possible issues with information sensitivity. The SDT agrees.

One commenter suggested the distribution of plan updates should include some irrefutable evidence on the part of the receiver. In response, we do not believe the added qualification would have the desired benefit. Individuals can choose to ignore the content regardless of the evidence of receipt.

One commenter stated that the example evidence for communicating plan updates is a poor choice because of the confidentiality of such information. In response, the examples do not necessitate the sharing of sensitive information but only that the individuals be notified. We have included additional guidelines to consider the sensitivity of the information when sending the required notifications.

VRF

One commenter proposed that the VRF should be Lower for consistency with other requirements. In response, we retain the previously FERC approved VRF of Medium for this requirement because failure to have restoration procedures directly affects the BES reliability function of High and Medium impact BES Cyber Systems.

VSLs

The VSLs have been updated corresponding to changes made to requirements in CIP-009-5.

One commenter suggested that “within 30 days” should be changed to “greater than 30 days”. The SDT agrees and has made this change.

Several commenters suggested that the moderate VSL for Requirement R1 should address “one” and not “all” missing elements of the plan. The SDT agrees and has made this change.

One commenter suggested that the VSL for Requirement R3 should capture not documenting the absence of lessons learned. The SDT agrees and has made this change.

One commenter proposed to replace the Requirement R3 VSLs with graduation from 90-210 days beyond the required obligation. The SDT agrees and has made this change.

One commenter noted the graduation of VSLs for requirement part 2.2 incorrectly lists a period of within 19 calendar months for the Severe category, and the SDT has modified this to be 18 calendar months.

QUESTION C12 – CIP-010-1:

If you disagree with the changes made in CIP-010-1 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the primary concerns regarding CIP-010-1 expressed in comments were (1) references to CIP-005, CIP-006, and CIP-007 within CIP-010, (2) scope of baseline configuration items in R1.1, (3) applicability including associated assets/systems and also including "external routable connectivity" language, (4) requirement language above and beyond FERC Order 706, and (5) other requirement and measure language modifications. The sections below are a summary of the comments received and include SDT responses for CIP-010-1.

CIP-010-1 General Comments

Many commenters requested an explanation for why CIP-010 depends on CIP-005, CIP-006, and CIP-007. Based on previous requirements in older versions of CIP-003, CIP-005, and CIP-007 (CIP-006 has since been removed from requirement language), the SDT combined the various requirements related to configuration change management and vulnerability assessments to create CIP-010. Both configuration change management and vulnerability assessment require validation that controls from CIP-005 and CIP-007 are not affected. Therefore, CIP-010 references CIP-005 and CIP-007. The SDT does not believe this cross-referencing creates a "double jeopardy" situation. Whether the requirement existed in CIP-005 or CIP-007, if an issue is discovered, then the issue would be a violation of where the requirement was enforced (CIP-005 or CIP-007) rather than in the requirement which enforced the search for issues (CIP-010). New "identify, assess, and correct deficiencies" requirement language will also aid in compliance concerns.

Several commenters mentioned that they desired a return to the approved language in CIP-003-4 Requirement R6 and CIP-007-1 Requirement R1 with targeted and efficient changes to address the FERC order. Another commenter further recommended a return to the draft 1 language. The SDT disagrees with their determination and believes that the current CIP-010-1 language is proper and in order. Based on this commenting period, the SDT has revised language for clarity and consistency. Language was also modified in an effort to address industry comments.

Numerous commenters recommended that all references to Medium Impact BES Cyber Systems in CIP-010 applicability include: "with External Routable Connectivity." The SDT does not agree with the addition of External Routable Connectivity to CIP-010 applicability. Whether a cyber asset has some type of connectivity or not, it can still be pervious

to vulnerabilities (i.e., Stutnex). The SDT's determination is in accordance with FERC Order 761, Paragraph 86. Therefore, external routable connectivity exclusion language was not included in the applicability for CIP-010.

One commenter proposed removing from the measures: "… and the output of the tools used to perform the assessment," since this is thought to be a part of CIP-010-1 Requirement R3.4. The SDT does not agree with this modification since CIP-010-1 Requirement R3.4 asks for the results of the assessments, while CIP-010-1 Requirements R3.1 through R3.3 are referring to the output of any tools used to perform the assessment. In consideration of this comment and other industry comments, the SDT included "any" to the requirement in the case that no tools were used to perform the assessment.

Several commenters suggested the removal of: "… but not limited to …" in CIP-010 measures. The SDT has modified measure language in consideration of their comment. The SDT also emphasizes that the: "… but not limited to …" is supposed to benefit the responsible entity and not create an item for auditors to use against them.

Multiple commenters suggested that specific controls from CIP-005 and CIP-007 be identified in CIP-010-1 Requirements R1.3, R1.4.1, and R3.1 so there would be no need for interpretations. These comments were taken into consideration, and the related requirement sub-parts were modified accordingly. The references to CIP-005 and CIP-007 were removed from some requirement sub-parts. Also, per consideration of these comments, CIP-006 was removed from requirement language where the language was present.

One commenter believed that some requirements in CIP-010 expand the scope and documentation burden beyond earlier CIP standards versions due to CIP-005 and CIP-007 references. In consideration of these comments, the SDT has modified CIP-010-1 Requirements R1.3 and R3.1 accordingly. References to CIP-005 and CIP-007 have been removed from the sub-part requirement language. It should be noted that the SDT disagreed to removing these references in Requirement R1.4.1. The SDT also added the reference to Requirement R1.5.1 for consistency across Requirement R1.

One commenter recommended adding a reference to the associated requirement part in which each CIP-010-1 VSL is related. The VSLs are written at the higher-level requirement, but do include elements that refer to the various requirement parts. Therefore, the SDT does not believe that the associated requirement part needs to be included in the VSL. One commenter continued to suggest that the VSL language should more closely mirror the requirement language. The SDT has taken into consideration this comment and modified the VSL language accordingly.

One commenter mentioned that having a documented baseline and monitoring it closely makes the vulnerability assessment prior to deployment have no benefit. The SDT does not agree with this assessment, as a vulnerability assessment is more than just monitoring for changes to the baseline. Please see the guidelines section of the standard for CIP-010-1 Requirement R3. Also, other commenters mentioned that establishing a production-like environment that could produce an active vulnerability assessment would be difficult and expensive. The SDT added the language: "… production environment where the test is performed in a manner that minimizes adverse effects …" for instances when a test environment is not available.

One commenter recommended an expanded glossary of the many terms used in CIP-010. The SDT has taken this comment into consideration and has expanded upon the guidelines to include more guidance around terms related to the baseline configuration and cyber security controls.

One commenter recommended further items to be incorporated into the baseline configuration; including communication protocols, non-standard BIOS configurations, and other items. The SDT believes that the requirement language is sufficient as written, as adding additional items into the baseline configuration at this time period would be difficult to support consensus.

One commenter recommended that CIP-010-1 have an effective date that is 12 months after the effective date of the CIP V5 standards. The SDT will take this comment into consideration, as this comment references the Implementation Plan and not necessarily language within the CIP-010-1 standard.

One commenter commented on the use of the term "Configuration" versus "configuration." The SDT has revised CIP-010-1 to only use "configuration," since it was not the SDT's intent to include "Configuration," as this is not a NERC defined glossary term. Furthermore, another commenter questioned if the terms: "configuration management," "configuration change management," and "asset management" were synonymous terms. The SDT has revised CIP-010-1 to only use "configuration change management" for less confusion. "Asset management" is not synonymous with the other words in the previously mentioned sentence. "Asset management" where it is used (R1.1 measures) refers to SAP, Maximo, Cascade, Passport, or other asset management software. Also, due to other questions around the baseline configuration, the SDT has added further guidance to aid in entities' development of their baselines.

Applicability Section

A couple comments mentioned that the exemption language in Section 4.2.4 should be changed back to the previous ballot's CIP-010-1 language or this section should be struck if it truly only applies to CIP-002-5. The difference between the initial ballot posting and successive ballot posting is 4.2.3.5, which states that: "Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes."

One commenter recommended the striking of the applicability component of the main requirement. If the commenter is referring to Section 4 of CIP-010, then this section is required for NERC standards to identify the standard's applicability to Responsible Entities, while the (newly termed) "applicable systems" columns in the tables refers to the scope of systems to which a specific requirement row applies.

Many commenters recommended removing some or all associated assets/systems from various applicability sections in the CIP-010 requirements because they represent an increase in scope from CIP V3/V4. The SDT disagrees with this assessment, as CIP Version 3 and Version 4 standards mention applicability to cyber assets within the ESP. The cyber assets that could exist within an ESP would include Associated Protected Cyber Assets, Associated Electronic Access Control or Monitoring Systems, and Associated Physical Access Control Systems. Therefore, the SDT does not believe that the assets/systems from CIP-010's applicability represent an increase in scope from CIP Version 3 and Version 4 standards.

One commenter expressed concern over 4.2.2, bullet 3, which references: "… Transmission where the Protection System is required by a NERC or Regional Reliability Standard." The concern was that CIP-010-1 was requiring the installation of a Transmission Protection System. This assessment is incorrect. CIP-010-1 does not require the installation of a Transmission Protection System, but other NERC or Regional Reliability Standards may require the installation of a Transmission Protection System.

Guidelines Section

Several commenters suggested adding the phrase: "network connectivity to identify" to the Requirement R3 guidance with regard to passive network discovery. The standard has been modified in consideration of these comments to include the phrase. One commenter made several other suggestions (such as the addition of details on baseline configurations and cyber security controls) in regards to guidance that informed the SDT's modification of that section.

Background Section

Several commenters mentioned that the third paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. The SDT believes that this third paragraph is clear in stating:

- A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence.
- The word "required" is not used to describe numbered or bulleted lists. The SDT wishes to emphasize that measures are only examples of evidence.

Requirement R1

One commenter proposed revision of the Requirement R1 to: "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has added the "in a manner that identifies, assesses, and corrects deficiencies" language to the requirement, which is described above.

One commenter proposed that the requirement be changed to a program- or performance-based level to allow more flexibility (citing FERC FFT Order, Paragraph 81). The comment furthermore mentions that programs such as Tripwire would not be able to be used. Other commenters had similar comments in regards to the prescriptive language of CIP-010-1 Requirement R1.1. Based on the revised "identify, assess, and correct deficiencies" language, the SDT believes that more flexibility is achieved through an entity's internal controls process. Furthermore, the SDT believes that programs such as Tripwire could be used to aid in compliance with CIP-010-1 Requirement R2.

One commenter believed that information in Requirement R1 should only be collected for personal computers and protective relays. The SDT disagrees with this comment, as the applicability should involve all BES Cyber Assets, BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems since these assets can be found within the same Electronic Security Perimeter.

One commenter asked if recording software "hashes" can be used as an alternative to recording version levels to verify that no unauthorized changes have been made to software on the BES Cyber Asset. The SDT attempted to provide flexibility to allow the entity to determine how to track changes. However, in regards to CIP-010-1 Requirement R1, the baseline configuration still must be documented. If an entity is able to use software "hashes" to monitor for changes to the baseline configuration of a BES Cyber System, then this solution could be used for CIP-010-1 Requirement R2.1.

One commenter proposed a modification to language in CIP-010-1 Requirement R1 to eliminate the term "baseline" so that it is not confused with the security baselines that they create today for devices. Two other commenters also wanted to remove the "baseline" from CIP-010-1 requirement language. The SDT disagrees with the proposed change and believes that the language, as is with the term "baseline," is sufficient.

Requirement Part 1.1

A few commenters emphasized that Version 4 did not apply to noncritical; but in accordance with FERC Order 761, Paragraph 86, these assets/systems should be included in CIP-010-1 Requirement R1.1. Therefore, external routable connectivity exclusion language was not included in the applicability for CIP-010-1 Requirement R1.1. Numerous commenters also alternatively recommended that CIP-010-1 Requirement R1.1 applicability only include High Impact BES Cyber Systems. The SDT disagrees and continues to cite FERC Order 761, Paragraph 86.

Several commenters disagreed with the use of the phrase: "… each Cyber Asset identified, individually or by group." The SDT has revised the requirement language in regards to their comment so as to ensure baselines can be defined at the individual or group level.

One commenter also desired a clarification of what may be grouped under CIP-010-1 Requirement R1.1. The SDT hopes that the revised requirement language provides additional clarity.

Requirement Part 1.1, Sub-Part 1.1.1

One commenter believed that this requirement is covered in CIP-009 Requirement R.1.3. The SDT disagrees with this comment as the process for the backup and storage of information required to recover BES Cyber System functionality is not required to include baseline configuration items.

Several commenters recommended replacing "exists" with "is either operating or running." Another commenter believed the wording of "is installed" is also sufficient. The SDT wants to underscore that "exists" refers to the case when an asset has firmware instead of an Operating System.

Requirement Part 1.1, Sub-Part 1.1.2

One commenter mentioned that "BES Cyber Asset" should be replaced with "applicable Cyber Asset." Other commenters had a similar position with regards to the use of "BES Cyber Asset." These comments were taken into consideration and

the related requirement sub-part was modified. The phrase "on the BES Cyber Asset" was removed from the requirement sub-part for consistency.

Multiple commenters requested clarification on the "applications." Does "applications" mean "SCADA, EMS, State Estimator, etc." instead of "device drivers and DLL applications" included in an operating system or package?" In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

One commenter believed that this requirement is covered in CIP-009 Requirement R.1.3. The SDT disagrees with this comment, as the process for the backup and storage of information required to recover BES Cyber System functionality is not required to include baseline configuration items.

A couple commenters suggested the removal of the word "intentionally" from the requirement language. The SDT believes that the use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for cyber asset use should be included. It is not the SDT's intent for notepad, calculator, DLL, device drivers, or other applications included in an operating system package to be considered as commercially available or open-source application software. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

Several entities requested clarity on how granular the version identifier should be. The SDT provides flexibility for entities to determine what version levels should be tracked. The purpose of tracking the version allows entities to keep abreast of the version levels in their inventory. If software manufacturers alert entities to vulnerabilities in their software, the affected population could be identified through software version. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

Several entities suggested that sub-part 1.1.2 should exclude anti-malware signature file version identifiers due to the volatility of frequency updates. The SDT believes that only version levels that can aid in recognizing affected software should be tracked. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

Requirement Part 1.1, Sub-Part 1.1.3

Multiple entities asked if a version control tool/system (like Concurrent Versions Systems) could demonstrate the custom software's version. In consideration of these comments, this requirement sub-part has been reworded to be "custom software installed." However, even in its successive ballot form, the requirement sub-part did not require the custom software version. Instead, the requirement sub-part requires the identification of the custom software.

One commenter believed that this requirement is covered in CIP-009 Requirement R.1.3. The SDT disagrees with this comment, as the process for the backup and storage of information required to recover BES Cyber System functionality is not required to include baseline configuration items.

Multiple commenters suggested removing "developed for the entity." The SDT has taken this comment into consideration and modified the requirement language accordingly.

There were several commenters who proposed modified language to clarify the term "custom software." The SDT disagrees with these proposed changes, but has reworded the requirement language in an attempt to provide additional clarity.

Requirement Part 1.1, Sub-Part 1.1.4

There were many commenters who believed that this requirement is covered in CIP-007. The SDT remarks that CIP-007 is evaluating what patches should be installed, while CIP-010 handles the patch being implemented (i.e., going through the configuration change management process).

One commenter believed that CIP-010-1 Requirement R1.1.4 would require the industry to account for more than a billion ports if each of 214 entities had less than 100 routable assets. Only ports which are accessible need to be included in the baseline. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

One commenter asked for clarity around "logical network accessible ports." In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

One commenter mentioned that the applicability columns from CIP-007 should match the applicability column in CIP-010-1 Requirement R1. The SDT does not agree with this comment, as the concept in CIP-010 is to identify logical network accessible ports, while CIP-007 requests entities to enable logical network accessible ports.

Requirement Part 1.1, Sub-Part 1.1.5
One commenter mentioned that CIP-010-1 Requirement R1.1.5 should be clarified to identify only those patches applied to the asset at the time the baseline is established and not all possible historic patches available for the asset. This comment was taken into consideration and the related requirement sub-part was modified.

Many commenters believed that this requirement is covered in CIP-007. The SDT remarks that CIP-007 is evaluating what should be used, while CIP-010 is the implementation.

One commenter believed that CIP-010-1 Requirement R1.1.5 would require an entity to document tens of thousands of unique patch installs for less than 200 Windows based Cyber Assets. Only historic or current patches that have been applied would be included in the baseline.

Several comments raised the concern Requirment R1.1.5 changes too frequently to be in the baseline and should be removed; that the evaluation of each patch is already included in CIP-007-5. The SDT believes that CIP-010-1 Requirment R1.1.5 is supposed to be a comprehensive listing of the patches that have been installed on the device. Patches are not required to be evaluated with this requirement. Instead, if a patch has been added to the device, then an update of the baseline is required.

Measures for Requirement Part 1.1
Per a comment, “or group” was added to CIP-0101 Requirement R1.1 measures to make consistent the requirement language and measures.

Requirement Part 1.2
One commenter proposed a rewording of CIP-010-1 Requirement R1.2 to: “Authorize changes to: security controls, operating systems, application software versions, custom software, ports or patches. Authorize changes to add or remove hardware.” The SDT disagrees with this comment, as the requirement language is consistent with other similar CIP Version 5 requirement language.

One commenter proposed indicating the appropriate authorizing individual or delegate in the requirement. The SDT believes that the requirement is sufficient, as is since it provides flexibility so that the entity can select the appropriate authorizing individual.

Measures for Requirement Part 1.2

One commenter recommended the removal of language in measures around individuals or groups with the authority to authorize the change. The SDT believes that measures are only examples of evidence. To be in compliance with the requirement language, an entity could authorize change by an individual, a group, or other entity-determined method.

There were two comments that recognized a concern with the language: "Documentation that the change was performed in accordance with the requirement." There was another suggestion to remove this language since it is not clear to what term the requirement is referring. The SDT believes that since the measure is for CIP-010-1 Requirement R1.2, that the language in the measure directly refers to CIP-010-1 Requirement R1.2 language only. While the SDT considered adding a reference to CIP-010-1 Requirement R1.2 in the measure to make explicit the requirement to which the measure language was referring, for consistency across CIP-010, this change was not made.

Requirement Part 1.3

One commenter mentioned that the applicability columns from CIP-005 and CIP-007 should match the applicability column of CIP-010-1 Requirement R1.3. This comment was taken into consideration and the related requirement sub-part was modified accordingly. The reference to CIP-005 and CIP-007 was removed from the requirement sub-part; and, therefore, the applicability columns between the standards do not need to be consistent.

There were many commenters that expressed concern with the 30-day time frame. Other commenters recommended the removal of the 30-day time frame for updating the baseline configuration. The SDT disagrees with the commenters and believes that a 30-day time frame allows entities time to update their baseline configuration documentation. Similiarly, other commenters had issues with the 30-day time frame and the references to CIP-005 and CIP-007. These issues are no longer a concern, as the SDT has removed the reference to CIP-005 and CIP-007 in regards to the 30-day time frame.

Two commenters were concerned about 'triple', or 'double' jeopardy with CIP-005 and CIP-007. One commenter suggested a revision or removal of the references, while another suggested that the requirement be moved to CIP-005 or CIP-007. In consideration of their comment, the SDT has modified CIP-010-1 Requirement R1.3 accordingly. In response, references to CIP-005 and CIP-007 have been removed from the sub-part requirement language.

Requirement Part 1.4

Many comments stated that "High Impact BES Cyber Systems" should be removed from applicability in CIP-010-1 Requirement R1.4 since this requirement sub-part is repetitious with CIP-010-1 Requirement R1.5. While CIP-010-1 Requirement R1.4 has been modified due to comments from industry, the SDT disagrees that CIP-010 Requirement R1.4 is repetitious with CIP-010-1 Requirement R1.5. CIP-010-1 Requirement R1.5 requires entities to test their baseline configuration changes in a test environment and document the results, while CIP-010-1 Requirement R1.4 requires entities to identify cyber security controls and then verify that these identified cyber security controls and system availability are not adversely affected after making the change.

A bevy of commenters believed that this requirement should include an exclusion for CIP Exceptional Circumstances. The SDT does not agree with this comment, as even after the CIP Exceptional Circumstance has happened, an entity should determine that controls were not adversely affected.

Several commenters suggested that guidance be added on cyber security controls. The SDT has taken their comment into consideration (in addition to other similar inquiries on cyber security controls) and added additional information on cyber security controls in CIP-010 guidance.

One commenter proposed the following language for this requirement part: "For a change that deviates from the existing baseline configuration or may have an impact on controls implemented for CIP-005, CIP-006, or CIP-007, [do 1.4.2]." While the SDT considered this approach, the SDT believes the current requirement language is sufficient as is.

CIP-010-1 Requirement Part 1.4, Sub-Part 1.4.1

One commenter suggested a language change of "determined" to "identified." The SDT disagrees with this proposed change and believes that the current language is sufficient as is.

One commenter believed CIP-010-1 Requirement R1.4.1 where "could be impacted" is used will cause all entities to document every control for every change in order to avoid zero-defect audit enforcement when some situation can be devised where "could be impacted" is a remote possibility. Southern believed that documenting "what could be impacted" is not a reliability benefit, it's the verification that controls are not affected by a change. The SDT agrees with their recommended change, and the requirement language has been updated accordingly in Requirement R1 with: "implement, in a manner that identifies, assesses, and corrects deficiencies," to avoid the zero-defect audit enforcement concern.

Several commenters believed that CIP-010-1 Requirement R1.4.1 could result in the Responsible Entity declaring that no cyber security controls are expected to change and, thus, no testing is required. The SDT does not agree with this assessment, as the requirement requires documentation of what could be changed followed by verification that potentially impacted controls were not affected in CIP-010-1 Requirement R1.4.2.

Many commenters recommended the removal of Requirement R1.4.1. The concept is that an entity identifies all related controls that could be impacted based on all requirements in CIP-005 and CIP-007. Therefore, the SDT believes that by mentioning CIP-005 and CIP-007, there is no need for interpretations. In fulfilling the requirement, an entity must identify that a particular change impacts CIP-005-5 Requirement R1 or CIP-005-5 Requirement R1 and CIP-005-5 Requirement R2. If all requirements in CIP-005 and CIP-007 may be affected by a deviation to the existing baseline configuration, then this would be documented in accordance to CIP-010-1 Requirement R1.4.1. It should also be mentioned that CIP-010-1 Requirement R1.4 is not repetitious with CIP-010-1 Requirement R1.5. CIP-010-1 Requirement R1.5 requires entities to test their baseline configuration changes in a test environment and document the results, while CIP-010-1 Requirement R1.4 requires entities to identify cyber security controls and then verify that these identified cyber security controls and system availability are not adversely affected after making the change.

CIP-010-1 Requirement Part 1.4, Sub-Part 1.4.2

One commenter mentioned that “BES Cyber Asset” should be replaced with “applicable Cyber Asset.” This comment was taken into consideration and the related requirement sub-part was modified. The phrase “BES Cyber System” was removed from the requirement sub-part for consistency.

Many commenters expressed concern with CIP-010-1 Requirement R1.4.2’s “availability” term. The SDT has modified the requirement language in consideration of these comments. The “available” term has been removed.

One commenter proposed that the word “determined” be changed to “identified.” The SDT disagrees with this proposed change and believes that the current language is sufficient as is.

One commenter believed the term “applicable” should be added for clarity. The SDT remarks that “applicable” is not required, as CIP-010 Requirement R1.4.2 points to CIP-010-1 Requirement R1.4.1, which ensures entities only look at the potentially impacted controls.

One commenter requested clarification of use of the term "required controls." The word required refers to the cyber security controls in CIP-005 and CIP-007 that were applied based on asset identification in CIP-002. While the SDT references all of CIP-005 and all of CIP-007, CIP-010-1 Requirement R1.4.1 requires entities to identify those controls in CIP-005 and CIP-007 that are potentially impacted. Therefore, CIP-010-1 Requirement R1.4.2 is only looking at the controls identified in CIP-010-1 Requirement R1.4.1.

One commenter proposed the addition of a time frame for how long an entity may take to make the verification required in CIP-010-1 Requirement R1.4.2. The SDT has taken this into consideration. The SDT also believes that the "identify, assess, and correct deficiencies" should provide aid in compliance concerns regarding this requirement.

CIP-010-1 Requirement Part 1.5, Sub-Part 1.5.1

Multiple commenters expressed concern with the language in CIP-010-1 Requirement R1.5.1. A few of the aforementioned organizations mentioned that the parenthetical expression in CIP-010-1 Requirement R1.5.1 should be altered to no longer include parenthesis. This comment was taken into consideration and the related requirement sub-part was modified. The language in the requirement part has been altered. Other organizations recommended changing CIP-010-1 Requirement R1.5.1 language to: "testing cyber security controls, where technically feasible, for each change that deviates from the existing baseline configuration" for clarity. The SDT has reworded requirement language based on industry comment and hopes that the changes provide additional clarity. Alternatively, other organizations proposed the removal of the following language in CIP-010-1 Requirement R1.5.1: "…that models the baseline configuration to ensure that required cyber security controls are not adversely affected." This is redundant to the concept in the last sentence, which requires documenting differences between test and production when a test environment is used. The SDT disagrees with the comment, as documenting the differences between the test and production environment is a completely separate task compared to modeling the baseline configuration. Modeling the baseline configuration is an attempt to re-create the baseline configuration on a single asset, while documenting differences between the test and production environment would simulate the rest of the assets in that environment and how they function together. Other organizations were concerned that the revised language in the posted standard removed the possibility for a technical feasibility exception. The SDT does not agree, as old, legacy systems may not be available in a test environment and there may be no way to utilize a production environment where a test can be performed in a manner that minimizes adverse effects.

One commenter asked if this requirement interferes with CIP-010-1 Requirement R1.4 for High Impact Systems. There was a suggestion to remove the overlap in applicability of the two requirements and adding clarifying language as to

what is intended and required in CIP-010-1 Requirement R1.4 vs. CIP-010-1 Requirement R1.5. The SDT wishes to underscore that CIP-010-1 Requirement R1.4 is not repetitious with CIP-010-1 R1.5. CIP-010-1 R1.5 requires entities to test their baseline configuration changes in a test environment and document the results, while CIP-010-1 Requirement R1.4 requires entities to identify cyber security controls and then verify that these identified cyber security controls and system availability are not adversely affected after making the change.

One commenter requested clarification of use of the term: "required controls." The SDT responds by claiming that "required" refers to the cyber security controls in CIP-005 and CIP-007 that were applied based on asset identification in CIP-002. Additional information on cyber security controls were added in CIP-010-1 Guidelines for Requirement R1.

Several commenters expressed concern over the "where technically feasible" language. Alliant Energy proposed that: "where technically feasible" should be changed to "where test environments exist." One commenter wanted to know what the language pertained to. The SDT does not agree with the proposed modification. The language in the requirement allows for test environments to exist in a production environment where the test is performed in a manner that minimizes adverse effects. Also, it should be made clear that the exception language refers to both CIP-010-1 Requirement R1.5.1 and Requirement R1.5.2.

Requirement Part 1.5, Sub-Part 1.5.2

Some commenters believed that the following language should be removed from the sub-requirement: "including a description of the measures used to account for any differences in operation between the test and production environments." Another commenter stated that they do not understand the intent of requiring this type of documentation, as it provides no security benefit and only invites auditors to unnecessarily critique the methods that the entity determines are appropriate to address the differences between the two environments. The SDT does not agree with this assessment and believes the documentation of the differences is important.

SPP RE and City Utilities of Springfield, MO asked if CIP-010-1 Requirement R1.5.2 permits the documentation of a stand-alone test environment with identified differences from the production environment. The SDT concurs that the requirement language requests documentation of the differences between the test and production environment, if a test environment was used. If the differences did not change from change to change, then the same documentation would be included with each change package that is processed.

Requirement R1 VRFs

Based on numerous comments, the VRFs in Table of Compliance Elements now match the VRF as identified at the requirements and measures section of the standard. This modification is for both CIP-010-1 Requirement R1 and Requirement R2.

Requirement R1 VSLs

There were two commenters who suggested that in corresponding to the proposed revisions to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. The SDT will take this into consideration, as we apply the non-zero defect forward looking compliance process.

Two commenters suggested that "any" be changed to "one or more" in the High VSL for CIP-010-1 Requirement R1. The SDT has updated the VSL language per the comment's recommended change.

One commenter believed that the phrase "and to document those changes" in the first condition of the High VSL for CIP-010-1 Requirement R1 should be deleted, as it is duplicative of the second condition. The SDT has removed the second condition due to modification to the requirement language to remove reference to other CIP standards in CIP-010-1 Requirement R1.3.

Main Requirement R2

One commenter proposed revision of the Requirement R1 to: "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has considered this approach in accordance with the FFT process. The following language has been added to requirement language: "identifies, assesses, and corrects deficiencies…"

Requirement Part 2.1

Many comments were on the initial ballot posting language, as the successive ballot posting language is not understandable. The SDT has modified the requirement in consideration of their comment.

One commenter believed that double jeopardy exists with CIP-010-1 Requirement R1 and CIP-010-1 Requirement R2.1. If a paperwork error occurs in authorizing a change and this requirement uncovers it, this should be addressed under CIP-010-1 Requirement R1, not a separate requirement. The SDT disagrees with this assessment. CIP-010-1 Requirement

R2.1 does not create a double jeopardy situation with CIP-010-1 Requirement R1 since the violation would be in CIP-010-1 Requirement R1, not in CIP-010-1 Requirement R2.1. CIP-010-1 Requirement R2.1 requires entities to document and investigate detected unauthorized changes. If one of the unauthorized changes is due to a violation of CIP-010-1 Requirement R1, then the self-report would be on CIP-010-1 Requirement R1 and not on CIP-010-1 Requirement R2.1. However, based on the new "identifies, assesses, and corrects deficiencies" language, if an issue is detected, based on an entity's internal control processes, this would not be a self-report. Other commenters stated on CIP-010-1 Requirement R2 creating a situation where a need would exist to self-report. With the new requirement language of "identifies, assesses, and corrects deficiencies," a self-report would not be necessary.

Many commenters essentially mentioned concerns centered on technical feasibility language. Some of the aforementioned organizations requested that the term "continuous" be removed from requirement language; while others proposed language that would remove the technical feasibility exception. The SDT has modified the requirement language in consideration of these comments. One commenter further commented that the language should be revised in such a way that only devices that can monitor automatically should be included; otherwise, a technical feasibility exception should be allowed. The SDT has modified the language such that monitoring could be done manually or continuously depending on the device.

One commenter suggested a change to the following language: "Document changes tracked through the entity's change management program." The SDT does not agree with this approach and believes the language is sufficient as is. One commenter recommended a similar approach of modifying the language due to their desired removal of "baseline" term use.

Many commenters suggested a different time frame for monitoring. The suggestion called for a 90-day instead of 35-day time frame, while other commenters suggested an annual or quarterly time frame. The SDT believes that a 35-day time frame is sufficient for an "express acknowledgement."

One commenter believed that the requirement will be burdensome and nothing gained from it except a lot of TFE paperwork to track. The SDT disagrees with this comment, as the requirement was added based on FERC Order 706.

One commenter asked if no change is detected during a monitoring period, how an entity can demonstrate that "no change" occurred. The requirement language mentions that only detected unauthorized changes need to be documented and investigated. If there is no change, then this would not need to be documented.

Measures for Requirement Part 2.1

One commenter emphasized that the requirement requires monitoring for all changes, yet the measure mentions calls for investigation of any unauthorized changes. They believe that the requirement language should be changed to include "unauthorized" changes such that monitoring is only necessary for unauthorized changes. The SDT does not agree with this assessment and believes that the requirement language and measures are sufficient as is.

One commenter requested clarity on the phrase "record of investigation." "Record of investigation" would be some type of documentation that shows that a detected unauthorized change was documented and investigated accordingly.

Requirement R2 VRFs

Multiple commenters stated that the VRFs in the table of compliance elements now matches the VRF as identified at the requirements and measures section of the standard. This modification is for both CIP-010-1 Requirements R1 and R2.

Requirement R2 VSLs

Several commenters suggested that in corresponding to the proposed revisions to the requirement statement, the VSLs should be revised to: "severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention." The SDT will take this into consideration as we apply the "non-zero defect forward looking compliance process."

Two commenters believed that a new gradated VSL should be introduced due to time-period language added in the previous posting. The SDT has taken this comment into consideration. While gradated VSLs were not introduced, since the requirement language includes "… identify, assess, and correct deficiencies…", the VSLs have been updated. .

Requirement R3

One commenter proposed a revision to Requirement R1 to read: "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has considered this approach in accordance with the FFT process. The following language has been added to requirement language: "identifies, assesses, and corrects deficiencies…"

A few commenters mentioned that the applicability between CIP-010-1 Requirements R3.3 and R3.4 differed. The SDT recognizes this difference and emphasizes that these are two different requirements and, hence, the applicability should be different.

One commenter asked if all Vulnerability Assessments under Requirement R3 must be performed prior to Version 5's Effective Date or whether entities have an additional year or three years from the effective date. The answer to NIPSCO's question can be found in the CIP Version 5 Implementation Plan. CIP-010-1 Requirements R3.1 and R3.2 must initially be complied with 12 months after the Effective Date of the CIP Version 5 standards.

One commenter asked why CIP-010-1 Requirement R3 does not always include Medium Impact in its scope. The SDT believes that the applicability as is can be considered sufficient. TRE also had concerns that the Requirement R3 does not include an annual vulnerability assessment. This is incorrect as CIP-010-1 Requirement R3.1 requires an annual vulnerability, while CIP-010-1 Requirement R3.2 requires a 36-month vulnerability assessment (for the applicable systems).

One commenter asked for clarity over the inclusion in applicability of Electronic Access Control or Monitoring Systems in CIP-010-1 Requirement R3. This requirement has the same applicability for these systems as in previous NERC CIP version. Therefore, the SDT believes that these systems should remain included in the applicability for CIP-010-1 Requirement R3.

One commenter asked if vulnerability assessments are required for every cyber asset or a sampling of cyber assets. Per applicable systems section, the vulnerability assessment is required for the systems listed.

Requirement Part 3.1

Commenters recommended that the requirement start with its purpose. The SDT disagrees with this comment, as the requirement language is consistent with other similar CIP V5 requirement language.

Many commenters proposed to reword Requirement R3.1 with the following language: "once each calendar year or a period not to exceed 15 calendar months between assessments." The SDT has taken these comments under consideration and is modifying the requirement sub-part language accordingly. One commenter proposed alternative language allowing an entity determined time frame. The SDT disagrees with this comment since the 15 calendar months' time frame is sufficient.

A few commenters believed that double jeopardy exists with reference to CIP-005, CIP-006, and CIP-007. The SDT does not agree, as if controls are not implemented correctly, then this would be a violation in the respective CIP standard, and not CIP-010-1.

Many commenters recommended that CIP-006 be removed from requirement language. The SDT agrees and has removed the reference to CIP-006.

Multiple commenters had concerns on what exactly constituted an active vulnerability assessment. The SDT points to guidance in CIP-010 on Requirement R3 in regards to recommended elements of an active vulnerability assessment. Also, other commenters asked if an active vulnerability assessment must be done for all systems or a representative sampling. Per the applicable systems section of the table for Requirement R3, the active vulnerability assessment must be done for all applicable systems.

One commenter requested clarification on whether an external vendor needs to perform the annual vulnerability assessment or can the Responsible Entity perform this task. The SDT provides enough flexibility in the requirement so that the RE can determine the solution that best meets its needs.

Several commenters believed that CIP-010-1 Requirement R3.1 is redundant with CIP-010-1 Requirement R1.3. The SDT does not agree, as CIP-010-1 Requirement R3.1 requires an annual vulnerability assessment, while CIP-010-1 Requirement R1.3 requires an update of the baseline configuration for a change that deviates from the existing baseline configuration.

Measure for Requirement Part 3.1

One commenter believed that reference to “individuals” in the first bulleted item needs to be removed. The SDT emphasizes that measures are only examples of evidence. However, the SDT has modified the measure language in consideration of the comment.

Requirement Part 3.2

Many commenters expressed concern with the language in CIP-010-1 R3.2. Another comment mentioned that the parenthetical expression in CIP-010-1 R3.2 should be altered to no longer include parenthesis. This comment was taken into consideration and the related requirement sub-part was modified. The language in the requirement part has been

altered. Furthermore, the commenters recommended that this requirement start with its purpose. The SDT disagrees with these comments as the requirement language is consistent with other similar CIP Version 5 requirement language.

Multiple commenters asked for clarification on CIP-010-1 Requirement R3.2 in regards to this being a paper exercise. The requirement language mentions active vulnerability assessment. In response, please see the guidance section on additional details on an active vulnerability assessment.

Multiple commenters proposed the removal of the language: "that models the baseline configuration to ensure that required cyber security controls are not adversely affected" in CIP-010-1 Requirement R3.2, commenting that it is redundant to the concept in the last sentence, which requires documenting differences between test and production when a test environment is used. The SDT does not agree with this assessment. CIP-010-1, Requirement R3.2.1 requires performing an active vulnerability assessment in an environment that models the baseline configuration of the BES Cyber System in a production environment, while CIP-010-1 Requirement R3.2.2 requires documenting the results of testing, and if, a test environment was used, documenting the differences.

One commenter asked how is this requirement differs from CIP-007. The SDT remarks that CIP-010-1 Requirement R3.2 is related to completing a vulnerability assessment every three years to assess controls in CIP-007 (and CIP-005) are implemented correctly.

One commenter believed that the following language should be removed from the sub-requirement: "including a description of the measures used to account for any differences in operation between the test and production environments." One commenter stated that they do not understand the intent of requiring this type of documentation, as it provides no security benefit and only invites auditors to unnecessarily critique the methods that the entity determines are appropriate to address the differences between the two environments. The SDT does not agree with this assessment and believes the documentation of the differences is important in establishing how the testing environments differ.

A few commenters asked if the assessment in CIP-010-1 Requirement R3.2 is in lieu of or in addition to the assessment required by CIP-010-1 Requirement R3.1 in the calendar year that the CIP-010-1 Requirement R3.2 assessment is conducted. The SDT believes that CIP-010-1 Requirement R3.2 is in lieu of CIP-010-1 Requirement R3.1 in the calendar year that CIP-010-1 Requirement R3.2 is conducted.

One commenter asked if CIP-006 is within scope of CIP-010-1 Requirement R3.2. The SDT has removed the reference to CIP-006 in CIP-010-1 Requirement R3.1, and is not a similar reference in CIP-010-1 Requirement R3.2.

One commenter proposed that the phrase: "where technically feasible" should be changed to "where test environments exist." The SDT does not agree with this modification since language in the requirement allows for "test environments" to exist in a production environment where the test is performed in a manner that minimizes adverse effects.

There was a comment mentioned that CIP-010-1 Requirement R3.2 requires assessments every three years, while CIP-007-3 Requirement R8 required vulnerability assessments annually. It was thought that we weakened the requirement; however, CIP-010-1 Requirement R3.1 requires an annual vulnerability and, therefore, the annual requirement in CIP-007-3 Requirement R8 was not weakened.

A commenter requested that associated electronic access control or monitoring systems and associated protected cyber assets should be added to the applicability for Requirement R3.2. For consistency in CIP-010-1, the SDT does not agree with the proposed change in applicability.

Requirement Part 3.3

One commenter believed it to be problematic to perform an active vulnerability assessment prior to installing a new Cyber Asset. The SDT acknowledges the concern, but emphasizes that an active vulnerability assessment is not required in the cases of a CIP Exceptional Circumstance or like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset.

One commenter believed that the term "active vulnerability assessment" is not defined. The SDT disagrees with this statement, as guidance is provided that aids in understanding an active vulnerability assessment. Furthermore, the commenter stated that since sufficient change management controls exist that an active vulnerability assessment is unnecessary. The SDT disagrees with this statement, as the configuration change management controls in CIP-010-1 Requirements R1 and R2 are in place for changes that deviate from the existing baseline configuration, while vulnerability assessments in CIP-010-1 Requirement R3 are for ensuring proper controls and detecting vulnerabilities.

One commenter mentioned that the parenthetical expression in CIP-010-1 Requirement R3.3 should be altered to no longer include parenthesis. This comment was taken into consideration and the related requirement sub-part was modified. The language in the requirement part has been altered.

Multiple commenters expressed concern around the language in CIP-010-1 Requirement R3.3. Some of the aforementioned organizations recommended that this requirement start with its purpose. Other organizations recommended a revision of the language. The SDT has taken these comments into consideration and modified the requirement language accordingly.

Multiple commenters suggested revisions to "prior to adding" language. One commenter proposed that instead of "prior to adding," that the requirement language should read: "before closing the change." Some vulnerability assessments actions only add value to assess after connected to the ESP as part of implementation and post implementation testing. The SDT disagrees with the proposed change and believes that the current language is sufficient based on other comments from industry.

One commenter believed that the parenthetical explanation of a like replacement should be moved to guidance. The SDT disagrees with the proposed change and believes that the current language is sufficient based on other comments from industry.

Several commenters believed that CIP-010-1 Requirement R3.3 appears to be missing "and" after the parenthesis. Without the parenthetical, it should read "Except for CIP Exceptional Circumstances and like replacements and prior to adding a new Cyber Asset..."

A couple commenters suggested that Physical Access Control Systems should be added in the applicable systems column. The SDT does not agree with their proposed change, as references to Physical Access Control Systems and CIP-006-1 have been removed throughout CIP-010-1.

One commenter expressed confusion around the use of the term: "new Cyber Asset." The commenter questioned if this term references a new Cyber Asset that is part of an existing Cyber System, or a new Cyber Asset per CIP-002. The SDT remarks that CIP-010-1 Requirement R3.3 is for new Cyber Assets with baseline configurations that do not currently exist. Therefore, a new Cyber Asset that is part of an existing Cyber System (and that has an existing baseline configuration) does not require an active vulnerability assessment per CIP-010-1 Requirement R3.3.

Several commenters believed that the language should be consistent among CIP-010-1 Requirements R3.1 through R3.3 in regards to vulnerability assessments. The SDT has modified the requirements accordingly in consideration of their comment.

A commenter asked if cyber assets can be placed in ESP before remediation of identified vulnerabilities. The SDT remarks that cyber assets can only be placed in ESP before remediation of identified vulnerabilities if a CIP Exceptional Circumstance exists or the cyber asset is a "like replacement."

CIP-010-1 Requirement Part 3.4

One commenter suggested that the term "if any" be added in CIP-010-1 Requirement R3.4 to denote the need to document the results of assessments that identified no vulnerabilities. The SDT disagrees as the language in CIP-010-1 Requirement R3.4 follows closely to the language in its previous instance in an earlier CIP standards version.

Many commenters expressed concern with the phrase: "remediate or mitigate vulnerabilities" and the related documentation. Another commenter proposed to replace "remediate or mitigate vulnerabilities" with "implement lessons learned (if any)" for consistency with other standards and eliminate extra documentation tracking requirements. The SDT developed this requirement language directly from the previous CIP versions. The concept is that an entity must document how they plan to remediate or mitigate identified vulnerabilities. CIP-010-1 Requirement R3 becomes an internal controls requirement to ensure that cyber security controls are properly implemented. While other commenters asked if it is the intent that identified vulnerabilities would not constitute violations of requirements they are found against. It is not the SDT's intent that an identified vulnerability would not constitute a violation of other requirements. While CIP-010 would not be violated, the respective CIP-005 or CIP-007 standard may be violated. The SDT does believe that the self-report mitigation plan could be used as the action plan for Requirement R3.4.

Several entities believed that the deadline for documenting the results of the assessment and the action plan should be specified. They suggested a 30-day limit. Also, they suggested including levels of gradation for not meeting the 30-day limit. One commenter took a different approach and recommended that "planned date" be changed to "estimated time frame." The SDT believes that the requirement language is sufficient as is.

Several commenters believed that more specificity should be added around the term “assessments” in CIP-010-1 Requirement R3.4. The SDT has modified the language in consideration of these comments and the text: “conducted pursuant to Parts 3.1, 3.2, and 3.3” was added to the requirement language.

One commenter asked for clarity in regards to the phrase “planned date of completing the action plan.” Is this the completion of the formulation of the plan or the completion of the tasks within the plan? The SDT articulates that the planned date of completing the action plan is related to the completion of the tasks within the plan.

Requirement R3 VRFs

There were multiple comments on VRFs, and the VRFs in Table of Compliance Elements now matches the VRF as identified at the Requirements and Measures section of the standard. This modification is for both CIP-010-1 Requirements R1 and R2.

Requirement R3 VSLs

Several commenters believed that corresponding to the proposed revisions to the requirement statement that the VSLs should be revised to read: “severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention.” The SDT has taken this comment into consideration as we applied the “identify, assess, and correct” approach; however, that language should not be included here. The reasoning behind this decision is due to the CIP-010-1 R3 Requirement’s indirect (mentioned in R3 Guidance) reference to CIP-005 and CIP-007. The related language would relate to the timely performance of completing a vulnerability assessment instead of identifying and correcting deficiencies which may be a part of the related CIP-005 and CIP-007 langauge (CIP-005 does not include this language in its requirements).

Several commenters proposed that the third condition in Severe VSL have the word “or” instead of “and.” The SDT has modified the language in response to their comment.

One commenter believed that the VSL does not address the 36-month timeline in CIP-010-1 Requirement R3.2. Furthermore, the commenter proposed additional language to address this timeline. The SDT has taken this comment into consideration and modified the VSL language accordingly.

QUESTION C15 – CIP-011-5:

If you disagree with the changes made in CIP-011-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, there were many global comments that related not only to CIP-011, but to all of the CIP standards.

Annual Requirements

Many commenters objected to the posted language referencing annual requirements. Several suggested alternative ways to express the frequency for an annual requirement. The SDT considered all of the recommendations and decided use the phrase "at least once every 15 calendar months" (or similar) to express the frequency for annual requirements.

Use of the phrase "but not limited to" in measures language

The SDT received many comments objecting to the phrase "but not limited to" within the measures. Some comments suggested removal of the term; others recommended a default to the use of the word "or," while others suggested the use of the word "and." Commenters believed that using the "but not limited to" language creates confusion about whether the specified measures are necessary or sufficient. The SDT has considered this issue carefully. The SDT has modified the language to "examples of acceptable evidence include, but are not limited to." The phrase "but not limited to" is designed to be of benefit to the Responsible Entity, not be a back door "gotcha" for auditors. Use of the phrase allows the entity flexibility in the type of evidence they are able to provide both now and in the future.

Applicability Column Title

The length of the applicability column title caused confusion about the systems/assets that are within scope for some entities. Several commenters suggested shortening the column heading to "applicability." The SDT recalls that the title of the column as previously posted was in response to comments from the first posting. SDT has renamed the column "applicable systems."

The SDT received many comments stating that: "Medium Impact BES Cyber Systems should be limited to Medium Impact BES Cyber Systems with External Routable Connectivity to maintain consistency with the scope of cyber systems/assets currently covered by similar requirements in the CIP Version 4 standards." A main goal of the SDT is to implement the FERC directives in Order 706 and Order 761. Order 761 states that FERC: "…supports the elimination of the blanket

exemption for non-routable connected cyber systems…continued blanket exemption in Version 5 would not adequately address risk." The SDT has considered each requirement concerning handling the exemption for non-routable connections. The SDT does not agree that in CIP-011 the scope should be limited to only BES Cyber Systems with External Routable Connectivity, as recommended in some comments.

Many commenters requested the removal of all references to systems and assets in requirements and that the SDT rely on the applicability column only to specify applicability. The SDT agrees with this recommendation. Wherever possible, the assets in scope will be indicated only in the applicability column. Several commenters suggested that the SDT remove all references to applicable assets in requirements and rely on the applicability column only to specify the Cyber Assets that are in scope. The SDT agrees. Wherever possible, the requirements have been streamlined to only reference applicable Cyber Assets within the applicability column.

Some commenters stated that the rationale for CIP-011 Requirement R1 was incomplete as originally posted. On May 8, 2012, NERC was alerted that the text contained in the rationale box for Requirement R1 of CIP-011-1 appeared to be incomplete. NERC corrected this by issuing revised language that modified the text box size to display all of the text.

Some commenters recommended that entities should define their own info protection program. They suggested that compliance would be evaluated based on how the entity complied with their defined programs. The SDT discussed this comment, but disagrees. The SDT believes it would be doing the industry a disservice to leave the process completely up to the entity. As part of its change, the SDT seeks to clarify what is required to meet compliance. The SDT believes that if the requirements are not defined or entity defined, NERC will be forced to issue Compliance Application Notices in the future to provide clarity, and auditors will be forced to inject their own audit measurements. In the interest of providing clarity, the SDT believes it is important to provide a consistent threshold for compliance.

The SDT received comments asking that the team revert to legacy language used in previous versions of the CIP standards (V1 and V3). SDT considered this request, but believes that many entities have made good suggestions, which improve legacy language. Legacy language will be utilized in all cases where it is appropriate for the purposes of minimizing changes that the registered entities must make to their ongoing programs.

CIP-011 Requirement R1 calls for each Responsible Entity to implement an information protection program that includes applicable items, and Requirement R1.1 requires methods to identify such information. Many entities commented that Requirement R1.1 was too vague. In fact, several entities indicated they were confused as to whether the requirement

called for determining what information should be protected or if the requirement mandated labeling of the information. Some entities asked if specific classification was required. A few entities suggested that a specific classification, such as "confidential," should be included in the requirement. The SDT has considered this but does not believe it is appropriate to dictate a specific classification, such as "confidential." Some entities may use other classifications such as "CIP-Confidential," "Non-Public," "Highly Confidential," or many other designations. It is not the intent of the SDT to force all Registered Entities to modify their compliance documentation by mandating specific classifications. This initial part of the information protection program simply requires that the information in scope and to be protected is identified in some manner. Specific classification of information may be used as a method for identification, but is not specifically required. One commenter provided a specific recommendation to clarify that the information to be identified is that which is explained in the definition of BES Cyber System Information. The SDT agrees with this comment. The SDT is also responsive to industry comments and has enhanced the measures section of Requirement R1.

Some entities pointed out that the word "implemented" is unnecessary in the Requirement R1.1 requirement because it is contained in the overall Requirement R1 requirement language. They asked that the word "implement" be removed from Requirement R1.1 because it was redundant. Other entities stated that documentation is for measures or evidence, and the word "documented" should be removed from Requirement R1.1 requirement. The SDT has removed both "implemented" and "documented" from the requirement language. The term documented has been moved to the measures section.

There were additional comments related to the measures for Requirement R1.1. Some commenters asked how a repository could be a measure, and others asked for additional clarity. A repository could be a measure if the entity designated the repository or a section of the repository as the location for identifying and housing BES Cyber System Information and explained the protections afforded by the repository in the entity's Information Protection Program. It would be up to the entity to explain in their information protection program how the repository was used to identify their BES Cyber System Information.

In CIP-011 Requirement R1.2, many commenters again asked that additional clarification be added to the requirement concerning procedures for handling of BES Cyber System Information. The SDT agrees and has modified the requirement to clarify that handling procedures required are those which explain how the BES Cyber System Information is protected and secured.

Several comments asked for additional specifics concerning several topics regarding BES Cyber System Information; including transit, handling, and transmittal. The SDT agrees with this. The guidance section has been greatly expanded to address the topics requested.

Several entities desired additional specifics concerning the measures for Requirement R1.2. One entity commented: "This measure does not specify what records could be used …would sampling work in this case, and if so, what is the acceptable tolerance range for such sampling?" The SDT disagrees that it would serve the industry to mandate this level of specifics within CIP-011. It is the SDTs intent that the entities document their information protection program and associated procedures in accordance with the CIP-011 requirements, and that the entity maintains records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented program and associated procedures. A measure has been added which specifies this intent.

There were several comments requesting that the SDT address third party handling of BES Cyber System Information. The SDT agrees with this comment. Additional information has been added to guidance to cover this topic.

There were comments asking for more specifics concerning the topics of transit, handling, transmittal, distribution, physical access, purge, use, and disposal. The guidance section has been significantly enhanced to address the topics for which additional direction is warranted.

Some commenters recommended including procedures for reuse and disposal within Requirement R1. The SDT does not agree. SDT believes that the topic of reuse and disposal is complex and requires the specifics currently afforded the topic as specified in Requirement R2. If the topic was included in the Requirement R1 procedures, it could result in double jeopardy during audits, as auditors review compliance with Requirement R1 procedures and Requirement R2 handling during reuse and disposal.

Commenters stated that the reference to prior version under Requirement R1.2 refers to CIP-003-3, Requirement R5.3. They recommended that the reference be moved to Requirement R1.3. The SDT agrees.

The SDT received many comments related to Requirement R1.3. Many commenters recommended that the team specify that deficiencies found in the annual assessment should not be considered violations or potential violations. Some commenters asked that the SDT specify which deficiencies would be considered violations and which would not be considered violations. Commenters asked that the word "deficiencies" be changed to "lessons learned" or "flaws." The

SDT notes that the word “deficiencies” is appropriate because a deficiency notes there is a lack of completeness or insufficiency exists.

Some asked that the entire requirement be handled under the NERC FFT program and eliminated from the requirements. It is not up to the SDT to make the determination as to what is and what is not a violation. The SDT sought guidance from NERC and regional audit staff. The audit staff advised that some deficiencies could be seen as self-reportable violations or potential violations during audit if the entity failed to adhere to one of the specified sub-requirements. Other deficiencies might simply be process improvements or opportunities for improvements that do not violate any BES Cyber System Information sub-requirement from CIP-011. Further, the requirement calls for a periodic “assessment,” and such “assessment” may reveal things that went well in addition to things that could be improved. After considering industry comments and consulting with audit and NERC staff, the requirement will be handled under the Paragraph 81 project from the FERC Order on the find, fix, track and report process.

Some commenters did not like the grouping of all access control requirements within CIP 004. They asked that the requirement parts dealing with access to information be moved into CIP-011. This was discussed among the SDT. It was decided that the majority of entities favored the grouping of all access control within CIP 004. For consistency and in response to many previous comments, all access control requirements have been grouped into CIP 004. The requirement parts dealing with access control for BES Cyber System Information have, therefore, not been moved into CIP-011.

Some commenters asked where specifically the process covering reuse and disposal is required. Requirement R2 states: “Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal.” Therefore, Requirement R2 requires the entity to define their process concerning the topics within Requirement R2.

The SDT received comments questioning a discrepancy between the types of systems referenced in the definition of BES Cyber System Information vs. the applicability column for Requirement R2. Associated Protected Cyber Assets is included in the applicability column, but is not specifically referenced in the definition. The SDT’s intent is that if BES Cyber System Information as defined in the standard exists in the data storage media of applicable Cyber Assets, then Requirement R2 applies.

One commenter pointed out that the component obligations under CIP-011-1 are not clear and that the table headers under Requirement R2 may be adding to the confusion, as they are different for Requirements R2.1 and for R2.2. The SDT agrees and has corrected the table headers so that they are consistent within Requirement R2.

The second paragraph in Requirements R2.1 and R2.2 that deal with removal of the device from the PSP generated many comments. Some commenters asked that the language concerning removal from the PSP be clarified. Others asked that the language be moved to a separate part. Others stated that the language adds no value and asked that the language concerning removal from the PSP be deleted from the requirement part altogether. A few commenters suggested simplified language, and such comments were very much appreciated. The SDT has decided to remove from the requirement language dealing with removal from the PSP. The SDT will address the topic of removal from the PSP within the guidance section. The SDT made corresponding changes to the measures section.

Many commenters objected to use of the term "chain of custody" in Requirements R2.1 and R2.2. They stated that this is a legal term, and they believe it is not appropriate in the CIP standards. Others commented that the intended use of the term "who has possession," as used in the requirement, was unclear. The SDT has decided to remove the entire second paragraph from Requirements R2.1 and R2.2, including the reference to "chain of custody." The SDT made corresponding changes to the measures section and any reference to terms such as "chain of custody" has been removed from the measures section, as well.

Some commenters recommended combining Requirements R2.1 and R2.2 into one requirement part. The SDT disagrees with this recommendation. SDT believes there are sufficient differences in the handling of release for reuse versus disposal to warrant retaining both Requirement R2.1 and Requirement R2.2.

Within the Requirement R2.1 language, some commenters asked for additional clarity concerning the exception, which provides for reuse within other high impact or medium impact BES Cyber Systems. The SDT agrees with this comment and has added additional clarity to the guidance language specifying that the re-use exception applies to re-use in other systems that are identified in the applicable systems column as protections will continue after re-use.

The SDT received comments asking that "BES" be inserted in front of "Cyber Assets" within the reference to "applicable Cyber Assets that contain BES Cyber System Information…" within Requirements R2.1 and R2.2. The SDT disagrees with this direction. The requirement parts are applicable to Associated Physical Access Control Systems, Associated Electronic

Access Control or Monitoring Systems, and Associated Protected Cyber Assets. Therefore, the scope of Cyber Assets which may contain BES Cyber System Information is larger than the suggested term "BES Cyber Assets."

The SDT received at least one comment stating that it was unclear if Requirement R2.2 meant the storage media within the Cyber Asset, or if it also includes backup media. The requirement states: "Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media." The SDT's intent is that the scope includes the Cyber Asset data storage media. The scope of this requirement is not far reaching to include all possible locations of downstream information, such as backup copies outside the Cyber Asset. However, such copies of BES Cyber System Information would be governed by Requirement R1.

Some entities also asked for additional specifics concerning the actions a Responsible Entity shall take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media. One commenter questioned whether an attestation was specifically mandated. An attestation is not required by the standard. It is not the intent of the SDT to mandate specific actions within the requirements. However, the guidance section has been greatly expanded with guidance taken from NIST SP800-88, which provides additional assistance to entities.

One entity stated that it is not clear if requirement parts 2.1 and 2.2 permit media to be removed and possibly replaced with clean media, with the Cyber Asset then being redeployed or disposed of while the removed media continues to be maintained until separate erasure or destruction. The SDT considered this question and believes that the answer is: Yes, such actions would be permitted. The requirement calls for the entity to "take action to prevent unauthorized retrieval." This provides flexibility for the entity. As long as the entity documented the actions that they undertook; i.e., removing the media, securing the media, sanitizing the media in accord with the requirements, such action should be permitted.

SDT received the following comment: requirement part 2.1 appears to be two requirements and should be broken out if that is the intent. The current wording appears to pertain to cyber assets that contain BES Cyber System Information (i.e., network diagram). The second sentence appears to pertain to Cyber Assets within an ESP. There were other commenters asking for clarity concerning the storage media and the targets for sanitation in Requirement R2. Requirement R2 applies to any information within the Cyber Asset data storage media that meets the definition of BES Cyber System Information.

A few commenters stated that the standard needs to track the media and not necessarily the Cyber Asset the media is associated with. The SDT agrees with this comment. The Requirement R2 language has been modified to include the reference to "data storage media."

VSLs and VRFs

The SDT received at least one comment asking that the VRF for Requirement R1 be lowered. The SDT disagrees with the industry comment. The VRF for Requirement R1 is Medium in keeping with the FERC approved current VRF for this requirement. The VRF for Requirement R2 is already lower.

One commenter asked that the SDT add the "part" reference to the VSL so that the reader could easily understand the requirement number to which the VSL referred. The SDT agrees with this comment, and added the references to the VSL's.

Multiple commenters objected to the "zero defect" approach to VSL's for Requirement R2. The SDT agrees. The previously posted Requirement R2 VSLs have been modified to be less "device" specific. In the future, there will be additional emphasis on the entity providing good processes and security controls.

One commenter provided specific language for VSL's. Corresponding to recommendations that had been made concerning requirements, they asked that the VSLs should be revised to: Severe-not implemented, Higher-not measuring to detect, Moderate-not correcting detected flaws, Lower-not considering prevention. However, the requirement does not address prevention, and the VSLs must correspond to the requirements.

NERC will be sharing additional information on VRFs and VSLs in keeping with NERC's implementation of the FFT program.

Questions with Votes Only:

CIP-008, CIP-009, CIP-010 and CIP-011 Questions: Question 1

1. **CIP-008-5 R1 states "Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?**

Organization	Yes or No
Northeast Power Coordinating Council	No
Duke Energy	No
NESCOR/NESCO	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
PNM Resources	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No

Organization	Yes or No
NIPSCO	No
Xcel Energy	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Springfield Utility Board	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No

Organization	Yes or No
Kansas City Power & Light	No
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes

Organization	Yes or No
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes

Organization	Yes or No
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes

Organization	Yes or No
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
California Independent System Operator	Yes

2. **CIP-008-5 R2 states "Each Responsible Entity shall implement its documented Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?**

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
ACES Power Marketing	No
PNM Resources	No
Dairyland Power Cooperative	No

Organization	Yes or No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Lakeland Electric	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No

Organization	Yes or No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes

Organization	Yes or No
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes

Organization	Yes or No
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes

Organization	Yes or No
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Springfield Utility Board	Yes

Organization	Yes or No
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
California Independent System Operator	Yes

3. CIP-008-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
PPL Corporation NERC Registered Affiliates	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
ACES Power Marketing	No
PNM Resources	No
Progress Energy	No
CenterPoint Energy	No

Organization	Yes or No
Hydro One	No
Lakeland Electric	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Springfield Utility Board	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
MRO NSRF	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review	Yes

Organization	Yes or No
Committee	
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes

Organization	Yes or No
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes

Organization	Yes or No
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Nebraska Public Power District	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
Pacific Gas and Electric Company	Yes

Organization	Yes or No
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Kansas City Power & Light	Yes
California Independent System Operator	Yes

5. CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
PPL Corporation NERC Registered Affiliates	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No

Organization	Yes or No
Florida Municipal Power Agency	No
SMUD & BANC	No
ACES Power Marketing	No
PNM Resources	No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
NIPSCO	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
Lincoln Electric System	No
Lakeland Electric	No

Organization	Yes or No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
Utility Services Inc.	No

Organization	Yes or No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
NYISO	No
Farmington Electric Utility System	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Pepco Holdings Inc & Affiliates	Yes

Organization	Yes or No
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces	Yes

Organization	Yes or No
Corporation	
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes

Organization	Yes or No
PSEG	Yes
Liberty Electric Power, LLC	Yes
MEAG Power	Yes
Portland General Electric	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

6. CIP-009-5 R2 states "Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
MRO NSRF	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
SMUD & BANC	No
Puget Sound Energy, Inc.	No
PNM Resources	No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
Progress Energy	No

Organization	Yes or No
Hydro One	No
Independent Electricity System Operator	No
Lincoln Electric System	No
Bonneville Power Administration	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Alliant Energy	No
NYISO	No
Exelon Corporation and its affiliates	No
Los Angeles Department of Water and Power	No
California Independent System Operator	No
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
FirstEnergy	Yes

Organization	Yes or No
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes

Organization	Yes or No
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes

Organization	Yes or No
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
Oncor Electric Delivery Company LLC	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes

Organization	Yes or No
Utility Services Inc.	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes

7. **CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?**

Summary Consideration:

Organization	Yes or No
NRG Energy Companies	No
PPL Corporation NERC Registered Affiliates	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
SMUD & BANC	No
PNM Resources	No
Arizona Public Service Company	No
Progress Energy	No
Hydro One	No
Tampa Electric Company	No

Organization	Yes or No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
City of Austin dba Austin Energy	No
Oncor Electric Delivery Company LLC	No
CenterPoint Energy	No
Xcel Energy	No
New York Power Authority	No
MidAmerican Energy Company	No
PJM Interconnection	No
ISO New England Inc.	No
ACES Power Marketing	No
Puget Sound Energy, Inc.	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Brazos Electric Power Cooperative	No
IRC Standards Review Committee	Yes
The united illuminating Company	Yes
Lakeland Electric	Yes
Southern California Edison Company	Yes
Clallam County PUD No.1	Yes

Organization	Yes or No
Northeast Utilities	Yes
Portland General Electric	Yes
MRO NSRF	Yes
NESCOR/NESCO	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
Comment Development SME list	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes

Organization	Yes or No
Western Area Power Administration	Yes
Dairyland Power Cooperative	Yes
Tri-State G&T - Transmission	Yes
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes

Organization	Yes or No
National Grid	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
MEAG Power	Yes
Utility Services Inc.	Yes

Organization	Yes or No
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Kansas City Power & Light	Yes
California Independent System Operator	Yes
Luminant	
American Transmission Company, LLC	
Avista	

9. CIP-010-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
FirstEnergy	No
SMUD & BANC	No
ACES Power Marketing	No
PNM Resources	No

Organization	Yes or No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
Lower Colorado River Authority	No
LCRA Transmission Serivces Corporation	No
Hydro-Quebec TransEnergie	No
Lincoln Electric System	No
The united illuminating Company	No
Tampa Electric Company	No

Organization	Yes or No
MidAmerican Energy Company	No
NV Energy	No
Massachusetts Municipal Wholesale Electric Company	No
Detroit Edison Company	No
The Empire District Electric Company	No
Ameren	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No

Organization	Yes or No
Utility Services Inc.	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
Springfield Utility Board	No
NYISO	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
PPL Corporation NERC Registered Affiliates	Yes
Associated Electric	Yes

Organization	Yes or No
Cooperative, Inc. (NCR01177, JRO00088)	
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes

Organization	Yes or No
MEAG Power	Yes
Portland General Electric	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

10. CIP-010-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
MRO NSRF	No
NESCOR/NESCO	No
SMUD & BANC	No
ACES Power Marketing	No
PNM Resources	No
Southern Company Services, Inc.	No
Western Area Power Administration	No

Organization	Yes or No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
ATCO Electric	No
Hydro-Quebec TransEnergie	No
Lincoln Electric System	No
The united illuminating Company	No
Bonneville Power Administration	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy	No

Organization	Yes or No
Company	
Detroit Edison Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Electric Power Company	No
Alliant Energy	No
Springfield Utility Board	No
NYISO	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No

Organization	Yes or No
California Independent System Operator	No
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes

Organization	Yes or No
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Serivces Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes

Organization	Yes or No
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

11. CIP-010-1 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
IRC Standards Review Committee	No
PNM Resources	No
Southern Company Services, Inc.	No

Organization	Yes or No
Western Area Power Administration	No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Consumers Energy Company	No
Lincoln Electric System	No
The united illuminating Company	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy	No

Organization	Yes or No
Company	
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
Springfield Utility Board	No

Organization	Yes or No
NYISO	No
Exelon Corporation and its affiliates	No
Los Angeles Department of Water and Power	No
Kansas City Power & Light	No
California Independent System Operator	No
PPL Corporation NERC Registered Affiliates	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes

Organization	Yes or No
SPP and Member companies	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Niagara Mohawk (dba National Grid)	Yes

Organization	Yes or No
National Grid	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
MEAG Power	Yes

Organization	Yes or No
Portland General Electric	Yes
Utility Services Inc.	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes

13. CIP-011-1 R1 states "Each Responsible Entity shall implement an information protection program that includes each of the applicable items in CIP-011-1 Table R1 – Information Protection." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
PNM Resources	No
National Rural Electric Cooperative Association (NRECA)	No
Progress Energy	No
CenterPoint Energy	No

Organization	Yes or No
Tri-State G&T - Transmission	No
Xcel Energy	No
Snohomish County PUD	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
PSEG	No
Liberty Electric Power, LLC	No
Texas Reliability Entity	No
PJM Interconnection	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Exelon Corporation and its affiliates	No
Deseret Power	No
Kansas City Power & Light	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes

Organization	Yes or No
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes

Organization	Yes or No
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power	Yes

Organization	Yes or No
Administration	
Lakeland Electric	Yes
Tampa Electric Company	Yes
New York Power Authority	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
Nebraska Public Power District	Yes
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes

Organization	Yes or No
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
California Independent System Operator	Yes

14. CIP-011-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
ACES Power Marketing	No
PNM Resources	No
Southern Company Services, Inc.	No
Progress Energy	No
Tri-State G&T - Transmission	No

Organization	Yes or No
Hydro One	No
Independent Electricity System Operator	No
The united illuminating Company	No
Xcel Energy	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
Ameren	No
NextEra Energy, Inc.	No
Liberty Electric Power, LLC	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery	No

Organization	Yes or No
Company LLC	
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Pacific Gas and Electric Company	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes

Organization	Yes or No
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes

Organization	Yes or No
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes

Organization	Yes or No
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards
Comment Form D
Definitions and Implementation Plans

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Index to Questions, Comments, and Responses

Questions with Summaries Included: 15

QUESTION D8 – DEFINITIONS: 15

QUESTION D9 – DEFINITIONS: 19

QUESTION D10 – DEFINITIONS: 22

QUESTION D11 – DEFINITIONS: 25

QUESTION D12 – DEFINITIONS: 27

QUESTION D13 – DEFINITIONS: 30

QUESTION D14 – DEFINITIONS: 35

QUESTION D16 – IMPLEMENTATION PLAN: 38

QUESTION D17 – DEFINITIONS AND IMPLEMENTATION PLAN: 42

Questions with Votes Only: 51

1. Do you agree with the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset? 51

2. Do you agree with the proposed definition of Control Center? 57

3. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager? 64

4. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager? 71

5. Do you agree with the proposed definitions of Electronic Access Control or Monitoring Systems, Interactive Remote Access, and Intermediate Device? 78

6. Do you agree with the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset? 85

7. Do you agree with the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident? 92

15. Do you agree with the changes made to the proposed implementation plan since the last formal comment period? 99

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Bruce Metruck	New York Power Authority	NPCC	6
12.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
13.	Robert Pellegrini	The United Illuminating Company	NPCC	1
14.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
15.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
16.	Brian Robinson	Utility Services	NPCC	8
17.	Michael Jones	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Don Weaver	New Brunswick System Operator	NPCC	2
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3
24.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5

2.	Group	Annabelle Lee	NESCOR/NESCO									

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3.	Group	Jason Marshall	ACES Power Marketing					X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3.	Tim Soles	Occidental Power Services, Inc.	ERCOT 3										
4.	Andy Gallo	Austin Energy	ERCOT 1										
5.	Andy Gallo	Austin Energy	ERCOT 3										
6.	Andy Gallo	Austin Energy	ERCOT 4										
7.	Andy Gallo	Austin Energy	ERCOT 5										
8.	Andy Gallo	Austin Energy	ERCOT 6										
8.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
7. Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8. Annie Terracciano	Northern Lights Inc.	WECC 3										
9. Aleka Scott	PNGC	WECC 4										
10. Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11. Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12. Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13. Margaret Ryan	PNGC	WECC 8										
12. Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13. Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14. Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3. M & A Electric Power Cooperative			SERC 1, 3										
4. Northeast Missouri Electric Power Cooperative			SERC 1, 3										
5. N.W. Electric Power Cooperative, Inc.			SERC 1, 3										
6. Sho-Me Power Electric Cooperative			SERC 1, 3										
15.	Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X						
Additional Member		Additional Organization	Region Segment Selection										
1. Oglethorpe Power Corporation			SERC 5										
2. Georgia Transmission Corporation			SERC 1										
16.	Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X
Additional Member		Additional Organization	Region Segment Selection										
1. MAHMOOD SAFI		OPPD	MRO 1, 3, 5, 6										
2. CHUCK LAWERENCE		ATC	MRO 1										
3. TOM WEBB		WPS	MRO 3, 4, 5, 6										
4. JODI JENSON		WAPA	MRO 1, 6										
5. KEN GOLDSMITH		ALTW	MRO 4										
6. DAVE RUDOLPH		BEPC	MRO 1, 3, 5, 6										
7. JOE DEPOORTER		MGE	MRO 3, 4, 5, 6										
8. SCOTT NICKELS		RPU	MRO 4										
9. TERRY HARBOUR		MEC	MRO 1, 3, 5, 6										
10. MARIE KNOX		MISO	MRO 2										
11. LEE KITTELSON		OTP	MRO 1, 3, 4, 5										
12. SCOTT BOS		MPW	MRO 6, 1, 3, 5										
13. TONY EDDLEMAN		NPPD	MRO 1, 3, 5										
14. THERESA ALLARD		MPC	MRO 1, 3, 5, 6										
17.	Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing													
18.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				
Additional Member		Additional Organization	Region Segment Selection										
1. Timothy Beyrle		City of New Smyrna Beach	FRCC 4										
2. James Howard		Lakeland Electric	FRCC 3										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
3. Greg Woessner	Kissimmee Utility Authority	FRCC	3										
4. Lynne Mila	City of Clewiston	FRCC	3										
5. Joe Stonecipher	Beaches Energy Services	FRCC	1										
6. Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4										
7. Randy Hahn	Ocala Utility Services	FRCC	3										
19. Group	Joseph DePoorter	Madison Gas and Electric Company				X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Darl Shimko	MGE	MRO	3										
2. Joseph DePoorter	MGE	MRO	4										
3. Steve Schultz	MGE	MRO	5										
4. Jeff Keebler	MGE	MRO	6										
20. Group	David Thorne	Pepco Holdings Inc & Affiliates		X		X							
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Mark Jones	Pepco	RFC	1										
21. Group	Rick Terrill	Luminant						X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Mike Laney	Luminant Generation Company LLC	ERCOT	5										
2. Tim Soles	Occidental Power Services, Inc.	ERCOT	6										
3. Tim Soles	Occidental Power Services, Inc.	ERCOT	3										
4. Andy Gallo	Austin Energy	ERCOT	1										
5. Andy Gallo	Austin Energy	ERCOT	3										
6. Andy Gallo	Austin Energy	ERCOT	4										
7. Andy Gallo	Austin Energy	ERCOT	5										
8. Andy Gallo	Austin Energy	ERCOT	6										
9. Brenda Hampton	Luminant Energy Company LLC												
22. Group	Joe Tarantino	SMUD & BANC		X		X	X	X	X				
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										
1. Kevin Smith	BANC	WECC	1										
23. Group	Scott Brame	NCEMC		X				X					
Additional Member	**Additional Organization**	**Region**	**Segment Selection**										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Rayburn Country Electric Cooperative			SPP										
2. Empire District Electric			SPP	1									
3. City Utilities of Springfield			SPP	4									
4. Westar Energy			SPP	1, 3, 5, 6									
5. Cleco Power			SPP	1, 3, 5, 6									
25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Pawel Krupa			WECC	1									
2. Dana Wheelock			WECC	3									
3. Hao Li			WECC	4									
27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Denise Lietz		Puget Sound Energy	WECC	1									
2. Erin Apperson		Puget Sound Energy	WECC	3									
28.	Group	Michael Mertz	PNM Resources	X		X							
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Laurie Williams		Public Service Co. of New Mexico	WECC	1									
2. Michael Mertz		Public Service Co. of New Mexico	WECC	3									
29.	Group	Sasa Maljukan	Hydro One	X									
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. David Kiguel		Hydro One	NPCC	1									
30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION D8 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the SDT modified some of the definitions. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity. Please see the redlined version of the definitions for a complete set of revisions to each definition.

BES Cyber Asset

Several commenters stated that the definition of BES Cyber Asset was confusing, citing the complex construction of the definition and the fact that it stated that each BES Cyber Asset must be part of a BES Cyber System while the background and technical basis stated that Responsible Entities had flexibility in using BES Cyber Asset or BES Cyber Systems. Many provided alternative language. Multiple commenters asked whether there is a need for network connectivity between BES Cyber Assets to be considered a BES Cyber System. The SDT made the addition of the statement about each being part of at least one BES Cyber System to the definition of BES Cyber Asset to ensure that each Cyber Asset would be included in at least one BES Cyber System, and did not preclude the option of having a BES Cyber System that consists of a single BES Cyber Asset. The SDT believes this preserves entities' flexibility while providing better homogeneity in the application of requirements: requirements uniformly apply to BES Cyber Systems. There is no presumption of connectivity options in the definition of a BES Cyber System, but Responsible Entities may find that application of requirements and relationship with other definitions such as ESPs may be significant input to the Responsible Entities' options.

Several commenters suggested that the definition of BES Cyber Asset include an addition in its qualification for connection to a network within an ESP in addition to connection to a Cyber Asset within an ESP. The SDT believes that the clarification is useful in ensuring the application to those transient cyber assets that are connected to the network as well as directly to the Cyber Assets within an ESP and has made the modification to address the comment.

One commenter suggested modifications to definitions of Cyber Asset. The SDT considered these comments and does not believe that these suggestions are substantively different or would add clarity to the definitions.

One commenter suggested dropping the word “misused” from the definition of BES Cyber Asset. The SDT has specifically included the word “misuse” in response to comments from FERC Order 706 and believes that it includes intent of a malicious compromise that is not otherwise conveyed.

Mid-American’s comment with respect to the use of the capitalized term “Systems” has been addressed and the definition now used the more generic term “systems” instead of the defined term.

One comment was on the use of the verb phrase “affect the reliable operation…” The SDT considered these comments and believes that this verb phrase is appropriate as it applies to the Facilities, systems and equipment, not the BES Cyber System.

Many commented on the complexity of the parenthetical sentence in the definition of BES Cyber Asset and suggested alternative language: the SDT considered these comments and believes that the suggested alternatives do not add additional clarity to the definition. In addition, other commenters stated that the parenthetical qualification should be used in defining the term Transient Cyber Asset. The SDT considered the options and chose to not have a separately defined term because of the very small number of requirements where it is used.

Many entities commented on the use of “adversely impact” in the definition of BES Cyber Asset and suggested using the defined term “Adverse Reliability Impact” instead. The SDT considered the use of the defined term and believes that the defined term describes an impact which is much more severe than the intent of the term used in the definition.

Several commenters requested clarification of the terms “within 15 minutes”: the SDT has included additional clarification in the guidelines and technical basis section.

–One commenter suggested to remove the 15 minute criteria as it is believed that it will lower the security of assets by removing them from qualifications. In response, The SDT notes that, in using 15 minutes, it is attempting to articulate a time boundary for “Real-time” impact. The term “Real-time” in the Glossary of Terms used in NERC Reliability Standards did not provide enough specificity in the definition for this purpose. The SDT scoped the CIP standards to those Cyber Assets that would have an effect on Real-time operations.

Many entities commented on the qualification on "redundancy" in the definition of BES Cyber Asset. The SDT believes that the impact of a cyber asset on the function of a given Facility, system or equipment is independent on whether that Facility, system or equipment is redundant or not: in most cases, the redundancy is configured to handle loss of a Facility, but does not consider degradation or misuse of that Facility, system or equipment. The application guidelines and technical basis section contains a discussion of this concept.

One entity suggests that the definition of BES Cyber Asset is much improved still does not prescribe how to document that an asset has been connected to the BES for less than 30 days. It is not the purpose of the definition to prescribe methods of documentation. That flexibility is left to the entity. Assets connected on a transient, temporary basis are not intended to be a BES Cyber Asset, and the 30 days in the definition is intended to clarify that temporary connections, e.g., for maintenance purposes, are not intended to be included within the definition.

BES Cyber Systems

One commenter suggested replacing "to perform" with "used to facilitate the performance of…", citing examples where the BES Cyber System may not directly perform a reliability function, but may support one or more functions. The SDT believes that the introduction of the proposed language would result in further questions on the meaning of the word "facilitate" and the extent of the scope of that term.

In response to a suggestion to use the word "identified for functions…" the SDT believes that the suggested wording did not bring additional clarity to the definition of BES Cyber Systems.

One commenter stated that the use of the term "Responsible Entity" is confusing, citing overlap, redundancy or conflict with the term Functional Entity. The SDT believes that these are two distinctly different terms: the Responsible Entity refers to the set of Functional Entities that is responsible for compliance to the requirements of the standard. Within a given standard, a given set of requirements may apply to different Functional Entities, depending on the specific requirements. The term "responsible entity" is defined in the applicability section. The application of the defined term that contains the term "responsible entity" in a standard is subject to the preamble in Section 4.

Cyber Asset

Multiple comments were provided on the use of the word "programmable" in the definition of Cyber Asset, citing that it was too broad, and the need for a routable connectivity qualification. The SDT considered these comments and notes

that the definition of Cyber Asset as it pertains to "programmable electronic devices" is part of the current approved definition. The SDT further believes that consideration of connectivity in this generic definition is inappropriate.

One commenter stated that the qualification of "…data in these devices…" ignores data in motion. The SDT believes that the inclusion of data other than that in these devices has unintended consequences in the application of requirements.

Other

Multiple commenters suggested the addition of a defined term BES Site, or similar concepts: the SDT has considered the rationale and has opted to use the concepts in the drafting of new language and approach in the requirement language and attachments, instead of defining a term that would be used in only a few requirements.

One commenter requested that the language for the defined term Protected Cyber Asset be reviewed for clarity. The SDT has reviewed the definition and made modifications to the definition and added guidance in the background section to clarify the concept.

QUESTION D9 – DEFINITIONS:

Do you have any comments on the changes to the proposed definition of Control Center? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the SDT modified all of the definitions based on stakeholder comments. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity. Please see the redlined version of the definitions for a complete set of revisions to each definition.

Many commenters questioned the need for a definition of Control Center, citing standards in other reliability standards that also have control center applicability without the need for a formal definition. The SDT notes that the Control Center is subject to a number of High and Medium Impact criteria and that they host a large number of BES Cyber Systems that are essential to the reliable operation of the BES. The SDT believes that, because of these necessarily crucial functions, a formal definition is appropriate to clearly define the scope of applicability, as demonstrated by many questions on differentiation between a facility's control room, which is typically considered part of the facility, and Control Centers, which are considered separate facilities hosting operating personnel controlling and monitoring multiple facilities. Many commented that a formal definition used in the CIP context could be confusing to the industry in the context of other reliability standards that apply to control centers. The SDT believes that a formal definition clarifies the scope of applicability for Control Centers and would not affect other reliability standards that have not used the defined term, but rather a "common" undefined term for control center. NERC's standard use of capitalized terms for NERC Glossary defined terms provides clarity on when the defined term is used.

Two commenters proposed alternative language for the definition of the Control Center that uses Functional Entities. The SDT has considered the alternatives and believes that the proposals contain a circular reference that would not provide better clarity. The SDT has carefully considered the current proposed language and believes that it accurately describes the intended target of applicability.

Others suggested that Control Centers that use voice or manual instructions be categorized as Low Impact. The SDT notes that Cyber Systems that provide information to Control Center operators that use manual or voice to effect control operations on BES assets in real-time based on that information must be subject to the same protection as those that

trigger automated operation. If the communication or manual operation results from information provided for real-time operations, there is no rationale for categorizing them as a lower impact.

Multiple commenters expressed concern that in certain instances, a facility may not be performing the function of a TOP 24/7 and remains unmanned the rest of the time, and suggested the addition of the 24/7 qualification. The SDT sees no rationale in adding this qualifier, since the impact of the facility that performs these functions remains the same. In the same comment, commenters cited the case of a TOP registration for a single facility. The SDT responds that the "control and monitoring" facility of a single facility does not meet the definition of a Control Center, but rather as part of the facility it is controlling.

Several commenters suggested slightly modified language which focuses on hosted BES Cyber Systems rather than operating personnel. One commenter suggested that the Control Center is the BES Cyber System that performs these functions. The SDT believes that operating personnel is central to the traditional understanding of a Control Center facility. The definition currently specifies one or several facilities. In the facilities (or site) based approach, the identification of the BES Cyber Systems that perform the Control Center functions may bring in other facilities such as data centers that perform these functions.

Many commenters requested clarifications on the terms "facility" and "locations" used in the definition of the Control Center. The SDT uses the general term "facility" (as opposed to the glossary term "Facility") in its generic sense of one or several physical structures that comprise a Transmission substation or station, a generating plant or a Control Center. In the case of a Control Center, a facility could be considered a building or campus consisting of several closely located buildings. However, additional facilities may be brought in as the BES Cyber Systems are defined, including associated data centers that perform the reliability tasks. In the context of the definition of Control Center, a location generally refers to the set of BES Facilities at a single site, and generally constitutes a single point of connection to the BES. Because of the many types of configurations, the SDT used the generally accepted concept of geographic location rather than including all the nuances of the different ways Facilities are connected to the BES.

One commenter requested a definition for data center. The SDT believes that "data center" is a well understood term and that many definitions of data center exist elsewhere that adequately explain what they are.

One commenter pointed out that the SDT uses the term reliability functional tasks and reliability tasks interchangeably in the standard. The SDT has used the terms interchangeably for the reliability tasks defined in the NERC functional model. The SDT has made the change in the definition of Control Center to be consistent to the use of reliability tasks elsewhere.

One commenter requested further qualification of the term “operating personnel”. The SDT notes that this term is used in many reliability standards, in particular, the PER series of standards. They are used to refer to personnel that perform the real-time control and monitoring operations necessary for the real-time functions for RC, BA, TOP and GOP functional entities. The definition of the Control Center refers to these functions.

One commenter suggested the addition of “NERC Certified” to operating personnel. The SDT notes that the addition of the term NERC Certified restricts the applicability of the term to just RCs, BAs and TOPs, since there is no requirement for certification of GOP operating personnel. This is not the intent of the SDT in drafting this definition.

One commenter suggested that Control Center as it applies to the function of a Generation Operator has a threshold of generation located at two or more locations, and that this single qualifier could unintentionally sweep in the control centers for multi-location generation of very small capacity. The commenter suggested that a capacity qualifier be added to this definition. The SDT does not think that the threshold should be in the definition, but has amended the criterion for generation Control Centers in the Medium Impact category that addresses this comment. BES Cyber Systems for Control Centers below the Medium Impact threshold must still be protected as Low Impact. See the response to A03 - Attachment 1, Medium Impact.

QUESTION D10 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the comments related to these definitions largely noted minor improvements to the definitions rather than identifying major issues or disagreement.

BES Cyber System Information

Several comments about the definition of BES Cyber System Information highlighted minor issues with the structure of the definition rather than its content. Commenters suggested re-organizing the definition such that the list of examples came last. The SDT considered this comment and agreed that it made the definition more readable without changing its overall intent. This suggestion has the effect of collecting the explanatory language together to improve comprehension of the definition. Some commenters suggested that the examples should be removed from the definition altogether. The SDT noted that it is not uncommon to find examples in definitions in the NERC Glossary of Terms Used in NERC Reliability Standards (e.g. Facility, Operating Plan, Year One, etc.). Additionally, the SDT had concerns about removing the list of examples, since a similar list of examples has been used since the version 1 CIP Standard to provide direction as to what information should be included in the NERC CIP information protection program. The SDT believed that continuing to provide a list of examples would facilitate a transition between Version 3 and 4 of the CIP standards to Version 5.

Additionally, some commenters took issue with the phrase "developed by the Responsible Entity" as it relates to security procedures and security information. The commenters noted that protection of security information might be appropriate even if this information was developed by an outside party. The SDT agrees with this comment. The intent of the SDT was to prevent the inclusion of information that might be publicly available. Therefore, the SDT has modified the definition to better align with the intent and has clarified that security procedures and security information "not publicly available" are examples of BES Cyber System Information.

Some commenters noted ambiguity in the definition of BES Cyber System Information in the phrase "unauthorized distribution" of information. The SDT appreciates the concern over ambiguity, but encourages the industry to consider this definition in context of the overall information security program that is required under NERC CIP-011-1 and related

requirements in NERC CIP-004-5. Consideration of "unauthorized distribution" should be taken in the context that access to locations where information that has been judged to meet this definition is stored is required to be authorized in CIP-004-5 R4, part 4.1, element 4.1.3 and proper handling of this information is required in CIP-011-1 R1, part 1.2. The Responsible Entity should use this context to determine whether this information, in the hands of someone who has not been granted access "based on need," could lead to a compromise in security, directly or indirectly, of the BES Cyber System.

Other commenters noted ambiguity over the phrase "pose a security threat" and recommended that this phrase be removed. The concept of posing a "security threat" to the BES Cyber System should also be considered in context of the requirements of the NERC CIP Standards, particularly CIP-011-1 R1. BES Cyber System Information is intended to be identified and protected in accordance with an overall information protection program. As such, it is anticipated that the Responsible Entity will include some process to identify the information applicable to this program. As not all information will lead to directly gaining access to BES Cyber Systems but may in other ways compromise the overall security of the BES Cyber System, the SDT does feel that it is prudent to remove this phrase.

CIP Exceptional Circumstances

Several commenters identified an issue with the phrase in the definition of CIP Exceptional Circumstances that included "an imminent or existing hardware, software, or equipment failure." Commenters pointed out that the collection of forensic data in CIP-009-5 Requirement R1.5, draft 2 was subject to CIP Exceptional Circumstances. Through the inclusion of hardware, software, or equipment failure as a CIP Exceptional Circumstance, a Responsible Entity could essentially choose to never comply with the collection of forensic data. After consideration, the SDT chose to modify the requirement in CIP-009-5 R1.5 to indicate that data preservation should not impede or restrict recovery. The SDT believes that hardware, software, or equipment failure is a reasonable component to include as a CIP Exceptional Circumstance given the cyber-physical relationship of the electric grid and its supporting Cyber Assets.

Additionally, commenters noted that the involvement of the conditions identified in the definition of CIP Exceptional Circumstances is not always known ahead of time. Specifically, commenters suggested that the SDT add the phrase "threatens to involve." The SDT considered this suggestion and decided that given the supporting framework required through the cyber security policies in CIP-003-5 to invoke a CIP Exceptional Circumstance, this was a reasonable and beneficial modification to the definition.

Commenters also questioned when CIP Exceptional Circumstances can be invoked. No modification was made to the standard, but in response, the intent of the SDT is to allow the use of CIP Exceptional Circumstances only where specifically identified in the language of the requirement. Additionally, CIP Exceptional Circumstances should be declared using the provisions identified in the Responsible Entity's cyber security policy as per CIP-003-5 R1.

CIP Senior Manager

Numerous commenters suggested minor modifications to the definition of CIP Senior Manager. The intent of the SDT was to include a definition of CIP Senior Manager in the NERC Glossary of Terms Used in NERC Reliability Standards so as to make clear who the required approver is when the term is used across the body of CIP Standards. The SDT did not intend to modify the content of the definition, which has remained unchanged since version 2 of CIP-003-2 when the role of the senior manager was clarified in response to FERC Order 706, paragraph 381. The SDT was compelled, given the current state of the CIP Standards being in their 5th version, by comments that suggested that in addition to the authority and responsibility for leading and managing the implementation of the requirements, that the CIP Senior Manager should also have the overall authority and responsibility for leading and managing "continuing adherence" to the requirements within the NERC CIP standards.

The SDT also received comments that the definition of CIP Senior Manager should specifically call out CIP-002 through CIP-011 as this is the set of cyber security standards to which the CIP Senior Manager has the authority and responsibility for. The SDT received similar comments in response to draft 1 of the posting of this definition. At that time, the SDT responded that the definition was only applicable where it is specifically used in the standards. Additionally, the concern appeared to specifically reference CIP-001, which at the time was planned for retirement as part of project 2009-1. However, given the dynamic nature of project 2009-1 and the relative ease to which this definition could be modified in the future should additional standards be added to which the CIP Senior Manager authority should apply, the SDT is persuaded to include a reference specifically to "CIP-002 through CIP-011" in the definition of CIP Senior Manager.

QUESTION D11 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Physical Access Control Systems and Physical Security Perimeter? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the SDT has address all comments and has made clarifying changes to the definitions.

Physical Security Perimeter (PSP)

One commenter proposed modifying the definition to apply only for applicable BES Cyber Systems. However, applicability cannot be determined by a definition. We have clarified in the applicability column in standards CIP-004 through CIP-011 that PSPs are not applicable solely upon meeting the definition.

One commenter requested that a list of example Cyber Assets that should be included within a PSP. In response, the standards specify more clearly which Cyber Assets must reside in a PSP.

One commenter suggested the definition of PSP should reference the correct defined term: Electronic Access Control or Monitoring Systems, and the SDT has made this change.

One commenter suggested that the definition is ambiguous about (1) whether the perimeter is two or three dimensional, (2) whether there are different expectations for High and Medium BES Cyber Systems and (3) what size hole provides access. In response, the additional specificity for the perimeter and access points would limit the options entities have in applying the requirement. The SDT believes we have struck the right balance in this requirement to allow entities flexibility in their approach while describing the end result. In regard to the difference between physical protection in High and Medium Impact BES Cyber Systems, this is specified in CIP-006-5.

Physical Access Control System (PACS)

Several commenters proposed removing "alert" from the definition to avoid the interpretation that security guard workstations are included in scope. In response, the alerting component should include the system sending out the alert

and does not include all recipient persons or devices of the alert. We do not believe this needs further clarification in the definition.

One commenter suggested that examples should not be included in the definition and the wording "exclusive of devices…at the PSP" could exclude more asset than intended. In response, we note that examples should not change the definition but can be helpful in forming context. For PACS, these examples are useful for explicitly clarifying perimeter devices, which by nature cannot have the same physical protection are outside of scope.

One commenter suggested putting a comma to make clear the example applies to Cyber Assets. In response, the example does modify the locally mounted hardware and devices and not the Cyber Assets. In other words, the example is for the exclusion.

One commenter suggested that the SDT needs to ensure electronic visitor log books are not captured in the definition and that the exclusion uses "or" instead of "and" for the examples. In response, a visitor log book would not be within scope because it logs visitors and not access, and including an electronic visitor log book could cause the interpretation that any additional logging would be considered out of scope. Also, "or" and "and" are logically interchangeable in the example list, and we do not find a need to make any change.

One commenter suggested that monitoring Cyber Assets should be included in the definition. In response, we did not include monitoring devices because those are typically outside of the PSP and serve as a supplementary protection. Although these can be used to comply with monitoring requirements, it becomes problematic to apply additional CIP Standards requirements without creating a complex protection loop.

One commenter suggested changing the word "exclusive" to "excluding", but the SDT chooses to retain the originally posted wording.

One commenter suggested the definition should include workstations used to provision physical access and monitor alarms. In response, the proposal would expand the definition scope beyond what the SDT considers unacceptable risk. The level of effort required to protect this significant population of assets would far exceed the security benefit of doing so. As an example, this could include all cell phones and pagers carried by staff for responding to alarms.

QUESTION D12 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Electronic Access Control and Monitoring Systems, Interactive Remote Access, and Intermediate Device? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, clarifying language was added to each definition to highlight stakeholders concerns.

Interactive Remote Access

Several commenters requested clarification for the inclusion of dial-up access in the definition. Upon further review, this has been removed from the definition. The important part to note is that Interactive Remote Access is when using a remote access client or other remote access technology, regardless of the type of connectivity.

One commenter proposed that the definition of Interactive Remote Access be modified to exclude serially connected, non-routable, non-network connected devices. The definition did not include serially connected, non-routable, non-network connected devices. However, the definition has been modified to specifically address the use of a routable protocol.

Several commenters requested restructuring of the definition to highlight the criteria for identifying Interactive Remote Access. The definition has been updated as requested to highlight that the first criteria is the use of a remote access client or other remote access technology.

Several commenters requested more information regarding examples of a remote access client or remote access technology. Additional information is available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested that list item two, "Cyber Assets used or owned by employees" be modified as "Cyber Assets used by employees". The commenter considers employee-owned devices inappropriate for use in Interactive Remote Access. Employee-owned devices were added to the definition based on comments received in Project 2010-15:

Expedited Revisions to CIP-005-3. This was added to address industry need to have remote access not limited to use of only company-owned assets for remote access. This is in support of pandemic and other emergency planning situations.

One commenter recommended adding the words "owned by or under the control of the Responsible Entity" to prevent the inclusion of equipment owned by Managed Security Providers in the standards. Connections by vendors, contractors, and consultants should be protected to the same standard as assets owned by the entity. Assets owned or used by vendors, contractors, and consultants were added to the definition based on comments received in Project 2010-15: Expedited Revisions to CIP-005-3. This was added to address industry need to have remote access not limited to use of only company-owned assets for remote access. This is in support of pandemic and other emergency planning situations.

Multiple commenters noted that the sentence beginning with "Remote access may be initiated from ..." adds no value, does not address all circumstances, and should be deleted. They further noted it is possible to initiate remote access from assets owned by others not listed. The information was added to the definition based on comments received in Project 2010-15: Expedited Revisions to CIP-005-3. This was added to address industry need to have remote access not limited to use of only company-owned assets for remote access. Please see the opposing perspective noted by other entities. The definition states that access "may be initiated" and not "shall be initiated" to allow for flexibility and not define the three scenarios as the finite and final list.

Intermediate Device

One commenter was concerned with the phrase "performing access control" existing as part of the definition of an Intermediate Device. It is the SDTs intent that an Intermediate Device is classified as an Electronic Access Control or Monitoring System. The definition of Electronic Access Controls or Monitoring Systems has been modified to include Intermediate Device.

One commenter requested clarification as to the types of devices that could be used as an Intermediate Device. The SDT specifically did not list proxy or other technology to allow flexibility in how an entity may implement a solution that best meets their needs. Per CIP-005-5 Requirement R2.1, the Intermediate Device must be used before accessing a BES Cyber System or Protected Cyber Asset. Per the definition, the Intermediate Device must not be inside of an ESP. Additional references regarding the Intermedate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

Multiple commenters noted concerns with the language, “The Intermediate Device must not be located inside the Electronic Security Perimeter”. Comments were received that this should be added to the requirements and removed from the definition. Some consider the second sentence of the definition to be unnecessary, too prescriptive, and should be deleted. Some offered recommendations for changes to the definition to allow for future technology developments.

- The SDT considers this language to be defining and clarification of the device. The performance under the requirement is that an entity utilizes the intermediate device. Further, definitions are part of the standards and carry the same force as the requirements.
- The location of the Intermediate Device was included in the definition to address numerous industry questions on this matter both in Project 2008-06 Cyber Security Order 706 Version 5 CIP standards and Project 2010-15: Expedited Revisions to CIP-005-3. Many entities have raised questions regarding the location of the device based on termination point of encryption and other issues.
- The only restriction placed on the Intermediate Device is that it not be inside of an ESP. Access authentication should be performed before the user is granted access through the ESP. Encryption should be terminated outside of the Electronic Security Perimeter so that event logging within the ESP is not negatively impacted. The SDT specifically did not list other specifics to allow flexibility in how an entity may implement a solution that best meets their needs whether through the use of a multi-purpose device or other architecture. Additional references regarding the Intermediate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter noted concerns that the term "device" is not clear in defining the Intermediate Device. They recommend using the term “Intermediate Cyber Asset”. The definition includes the term “Cyber Asset” which is defined as “programmable electronic devices including the hardware, software, and data in those devices”. The SDT has chosen the unique term “Intermediate Device” to allow for the use of one or more Cyber Assets making up the device.

QUESTION D13 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the SDT clarified language to the definitions.

Electronic Access Point

Multiple commenters asked for clarity if an Electronic Access Point (EAP) must be routable on both sides. In response, the SDT's intent is that if the device is accessible from outside the Electronic Security Perimeter (ESP) with a routable protocol then an EAP must be put in place. Therefore, just as in the Critical Cyber Asset Identification Guidelines of today, the 'inside' does not have to be routable. For example, if the entity has a digital relay and has the serial port used for console access (non-routable serial communications) attached to a serial-to-IP gateway such that the relay's command console is addressable from outside the ESP via a routable protocol (e.g. <IP Address>:<Port #> will connect you to the relay), then this meets the definition of External Routable Connectivity and an EAP is required.

One commenter provided an alternate definition that included the phrase "externally routable bi-directional communication" and added "or inbound communications to a Cyber Asset within the Electronic Security Perimeter" to the end. In response, the SDT notes that the direction of the communication is an aspect of External Routable Connectivity definition. The Electronic Access Point is an intentionally broader definition and its main function is to deny all access by default and only allow needed traffic to cross the ESP, regardless of direction.

One commenter asked that it be clarified as to whether an EAP is part of the ESP or not? In response, the SDT notes that an EAP is part of an ESP as it is the point where the routable communication from outside the ESP is allowed to cross the ESP to Cyber Assets inside the ESP.

One commenter suggested that the term "interface" be removed and have the definition reference a Cyber Asset. In response, the SDT notes that the inclusion of interface is meant to address the situation where an entity has a firewall as an EAP that has numerous interfaces to different networks and only one goes to a network that has applicable Cyber

Assets. The inclusion of 'interface' means the requirements would be concerned with only those interfaces that communicate with applicable Cyber Assets and not to interfaces that do not have any applicable Cyber Assets. The SDT also notes that the requirements in CIP-005 that apply directly to EAPs concern an interface (deny by default, methods for inspecting for malicious communications, etc).

One commenter suggested that the definition add "allows or is capable of allowing" to include dual homed Cyber Assets including laptops with wifi that is not hardware disabled. In response, the SDT believes that for a mandatory requirement the enforceable point should be binary – either communication is allowed to cross an ESP or it isn't – and the standards should avoid dealing with all possible capabilities.

One commenter asked for confirmation of the notion that Cyber Assets only communicate with other Cyber Assets. In response, the SDT notes that Cyber Asset is the basic unit of these standards and there is no lower level term. As Cyber Asset is a 'programmable electronic device', the SDT believes this covers most all situations. The SDT notes that Cyber Assets includes most all network gear as well, not just servers and workstations.

Electronic Security Perimeter

Several commenters suggested that examples should be included. In response, the SDT is not including examples in this term. Since terms such as ESP often refer to cyber technology that is constantly changing and developing, there is a tendency for examples to become outdated. The SDT used guidance instead to discuss examples rather than definitions. When the term is then used in a requirement, there is a tendency for the examples to then become prescriptive and mandatory, which is not the purpose of examples.

Multiple commenters provided some clarifying questions: Does an ESP presume the presence of EAP? Does a BES Cyber System with no External Routable Connectivity fall into scope? In response, the SDT clarifies that the ESP does not presume the presence of an EAP and BES Cyber Systems without External Routable Connectivity are in scope of the CIP standards. The ESP is a 'logical border' around a routable protocol network to which a BES Cyber System is connected. An isolated network with no external connectivity has an ESP; a logical border. The ESP is used to determine the 'Associated Protected Cyber Assets' as well as the collection of Cyber Systems and Assets that will be elevated to the impact level of the highest impact BES Cyber System/Asset in the ESP (see the definition of Protected Cyber Asset). If routable protocol communications cross the ESP, then an EAP is required.

Several commenters stated that this should be applicable to BES Cyber Asset instead of BES Cyber System. In response, the SDT notes that the BES Cyber System grouping is up to the entity and the concepts of electronic and physical security perimeters need to be taken into account. An entity is free to define every individual BES Cyber Asset as its own unique BES Cyber System and in essence make the entire standard Cyber Asset based. The grouping into systems is at the entity's discretion, but should be done with the requirements in mind.

External Routable Connectivity

Multiple commenters suggested that clarity is needed concerning the focus on Cyber Asset connectivity, rather than a 'system' with connectivity. Does a 'system' with one routable device mean all cyber assets in the system meet the applicability? This applies to the ESP definition as well. In response, the SDT has updated the definition to be at the Cyber Asset level rather than the BES Cyber System level. The intent is that Cyber Assets that have External Routable Connectivity must meet the applicable requirements and Cyber Assets that do not meet the definition are exempt from the requirement.

Several commenters suggested that the definition should include the OSI network layers. The SDT has chosen to not include Open System Interconnection (OSI) layers in the definition at this point. It is believed that with the history of the CIP standards being based on 'routable protocol' since its inception that there is a sufficient understanding of these terms at this point.

Multiple commenters suggested that the definition should be reworded to be a property of a BES Cyber Asset, not the asset itself. In response, the SDT agrees and has changed the definition to begin with "The ability to access…"

One commenter suggested that the definition should only apply if routable connection goes all the way to a BES Cyber Asset within the ESP. In response, the SDT is trying to incorporate the situation (identified in the current CCA Identification Guidelines) where an Ethernet/serial gateway is used at the perimeter. A BES Cyber Asset may have a serial connection from its console port to the Ethernet/serial gateway such that from outside the ESP the device's console port is directly addressable using a routable protocol, usually simply in the form of <ip address:port #>. The SDT's intent is for the definition to capture any device that is accessible from outside the ESP with a bi-directional routable protocol.

One commenter suggested that the definition needs to consider inside to outside connectivity not just outside in. In response, the SDT does consider 'inside out' connectivity in the requirements (e.g. outbound rules on EAP's). However, the intent with this definition is to focus on the higher level of threat that outside-in connectivity presents as well as to

give some credit for more secure network architectures that only push data out and don't allow outside-in connectivity (data diodes, etc.).

A few commenters commented that the definition should be Cyber Asset based rather than strictly limited to BES Cyber Systems. In response, the SDT has clarified that access is from a Cyber Asset that is outside of the BES Cyber System's associated Electronic Security Perimeter via a bi-directional routable protocol connection.

Protected Cyber Asset

Multiple commenters suggested that the parentheses should be removed, keeping the sentence concerning temporarily connected Cyber Assets. In response, the SDT agrees and has made the suggested change.

One commenter suggested that the temporarily connected Cyber Asset exclusion should be pulled out and made into a separate definition. In response, the SDT in this instance would be defining a term simply to use the term in the definition of another term. Therefore the SDT believes it is more straightforward to include a more complete definition in the ultimate term we are defining, and see no issue with stating what something is and what it is not while defining it.

Multiple commenters suggested that this should allow for network connection of temporarily connected Cyber Assets, suggesting that 'directly' be removed to allow connection within the ESP without requiring connection through a Cyber Asset. In response, the SDT notes that a network switch is a Cyber Asset and thus network connections are included. However, the SDT agrees that this point needs more clarity and has deleted the word 'directly' and clarified that it is a connection either to a Cyber Asset in the ESP or the network within an ESP.

One commenter suggested that a separate definition for Transient Cyber Asset should be included and have a requirement to scan for malware before connection. In response, the SDT notes that this was included in previous drafts but was removed in this draft in response to comments. Numerous comments were received pointing out the audit issues of such a requirement. How does one prove that a list of temporarily connected devices is complete? How does one prove that virus scans were done on a device that was there one minute and gone the next? How does one maintain and prove a complete inventory of all temporarily connected devices? Commenters also pointed out that the object of protection is the BES Cyber System – the goal is to protect BES Cyber Systems from all threats including temporarily connected devices. There were also numerous issues raised concerning TFE's as many troubleshooting and maintenance devices are 'programmable electronic devices' and would thus be Cyber Assets but have no antivirus available. A cable scanner used to diagnose cabling issues may be a programmable electronic device and then require a TFE. In response to

all these issues, the SDT decided to remove the requirement. However, the SDT notes that CIP-007 R3 requires an entity to deploy method(s) to deter, detect, or prevent malicious code and it is expected that such measures as scanning temporarily connected laptops and other similar devices may be included in these methods.

QUESTION D14 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, several changes have been made to clarify language in the definitions.

General Comments

Several commenters stated that the phrase "reliability tasks of the functional entity" is unclear and needs to be replaced or further defined. In response, the phrase reliability tasks of the functional entity comes from the definition of BES Cyber System and the reliability tasks are those specified in the NERC Functional Model.

Several commenters suggested that the terms compromise and disrupt need to have their own definition. In response, the words compromise and disrupt carry forward from the previously approved definition and we have not received compelling indication that these terms need further clarification.

Several commenters suggested that the phrase "was an attempt to compromise" is vague and should be deleted. In response, this phrase captures those incidents that do not necessarily succeed but should prompt investigation.

One commenter suggested replacing the phrase "reliability tasks of the functional entity" with "reliability tasks identified for functions in the NERC Functional Model." The SDT does not specify the NERC Functional Model, which is not a document subject to the standards development process, but the SDT believes that the phrase adequately conveys those tasks.

One comment was on the phrase "malicious and suspicious" is subject to interpretation and proposed adding the qualifying phrase, "as determined by the Responsible Entity." In response, the definition should not include this phrase because it is not a requirement, and CIP-008-5 already specifies the obligation for the Responsible Entity to make this determination.

One commenter suggested qualifying the term ESP and PSP with BES Cyber System to avoid having to demonstrate compliance with perimeters that do not protect BES Cyber Systems. In response, the requirement in CIP-008-5 makes this distinction in the applicability section.

One commenter suggested that the definition of Control Center uses a different term "reliability functional tasks" and requests clarification if this term means something different. In response, the SDT has clarified the language to read "reliability tasks".

One commenter suggested that the DOE OE-417 form should be considered to allow entities to comply with both requirements. In response, the SDT has reviewed the latest version of this form and do not find any reporting requirements that would conflict with those in CIP-008-5.

Cyber Security Incident

Several commenters suggested replacing the phrase "was an attempt" with "has the potential" in the definition of Cyber Security Incident because an attempt implies knowing the intent of the perpetrator and it excludes accidents which have the potential to compromise the BES Cyber System. In response, we have not significantly changed the currently approved definition and do not find the need to incorporate the proposed modifications. Both phrases communicate the desired result that an unsuccessful attack or compromise would be considered a Cyber Security Incident.

There was a suggestion that the definition of Cyber Security Incident now includes PSPs and the impact will be difficult to assess. In response, the current approved definition includes PSPs.

One commenter proposed to amend the definition of Cyber Security Incident to include: "Is a violation or imminent threat of a violation of computer security policies, acceptable use policies, or standard security practices impacting or within covered ESPs or PSPs." In response, violation of policies can be covered in an entity definition of a cyber security incident, but the Glossary definition has a focus on impact in order to broadly apply the standard.

One commenter suggested that physical security incidents should have its own definition and not be included as part of a Cyber Security Incident. In response, a physical security breach into a perimeter protecting the BES Cyber System provides enough cause for concern in the integrity of the BES Cyber System to warrant classification of a Cyber Security Incident. Individual entities may use distinct terms and response teams for these types of incidents, and the obligations in CIP-008-5 would still apply.

Several commenters proposed removing the phrase "suspicious event" from Cyber Security Incident. In response, the term suspicious event captures those incidents prompting further investigation in which the entity may not determine the cause or motive.

Reportable Cyber Security Incident

SPP RE expressed concerns that Reportable Cyber Security Incidents would not include those incidents in which redundancy mitigated the impact. In response, we have provided guidance in CIP-008-5 that Reportable Cyber Security Incidents would also include those that triggered an activation of redundant systems.

There was a proposal to replace "Any" with "A" to start the definition of Reportable Cyber Security Incident and we have done so.

One commenter proposed the following definition of Reportable Cyber Security Incident: "Any Cyber Security event that has compromised or disrupted one or more reliability tasks of a functional entity, which through investigation and escalation, has been determined by the Responsible Entity to be reportable to ES-ISAC." In response, this proposed definition includes a requirement, which should remain in the standard. The requirement in CIP-008-5 still provides leeway to the entity in determining Reportable Cyber Security Incidents.

One commenter stated that the definition needs to be coordinated with the EOP-004-2 drafting team. In response, both the CIP Version 5 and EOP-004-2 drafting teams have agreed to move all reporting obligations for Cyber Security Incidents to CIP-008-5.

One commenter proposed the definition for Reportable Cyber Security Incident in order to avoid using the term functional tasks, "A Cyber Security Incident that compromised the ESP or PSP or disrupted the operation of an applicable BES Cyber Asset or low BES Site."

One commenter proposed to add additional guidance in CIP-008-5. In response, the use of functional tasks ties the reportable incident to a specific reliability function. Without this qualification, the definition can easily be interpreted to include nominal security events as reportable. The SDT has already added additional guidance on distinguishing a Reportable Cyber Security Incident.

QUESTION D16 – IMPLEMENTATION PLAN:

If you disagree with the changes made to the Implementation Plan since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, there were not many changes made to the Implementation Plan, but the comments and comment responses below provide clarity into some of the concerns regarding the proposed effective date, the possibility of bypassing Version 4, and the initial performance of certain periodic requirements.

Proposed Effective Date

One commenter suggested that the effective date conflicts with the initial performance of requirements section and should specifically mention this in the effective date language as an exception. In response, we do not feel this is necessary. The implementation plan enumerates any exceptions to the effective date of the standard. The alternative of including all such exceptions in the effective date language would make the language unreasonably complex.

One commenter agreed with the approach to focus on the high and medium impact BES Cyber Systems but questions the need for an additional year of implementation time for low impact BES Cyber Systems particularly if no inventory is necessary. SPP RE also agrees an additional year for compliance with CIP-003-5 R2 is unnecessary. In response, the need for an additional year of implementation for low impact BES Cyber Systems exists to allow entities to formulate and implement effective security solutions for physical and electronic perimeter protection. Despite not requiring an inventory of low impact BES Cyber Systems, entities must still implement these policy changes in applicable locations where no perimeter protection currently exists.

Several commenters questioned why the effective date is so far out given that the standards have been in development for more than two years. In response, the development timeframe of the standards do not determine when entities begin planning compliance. Rather, entities have assurance in the finality of the standards upon FERC approval. The number of cyber systems applicable in this standard far exceeds any previous version of the standard. The SDT reasons it will take two budget cycles for entities to plan and implement these standards.

Bypassing Version 4

Several commented that language to extend the Version 3 effective period and bypass Version 4 should be removed because the recent FERC Order has solidified the effective date for Version 4 as April 1, 2014. Other comments request a

transitional plan to address the period of compliance between Version 4 and 5. In response, the SDT observes that the provisions to bypass Version 4 remain in the implementation plan and are subject to approval by the industry and FERC. This is explained in greater detail in the summary section at the beginning of this document.

Initial Performance of Certain Periodic Requirements

One commenter stated that for non-periodic requirements, the IP should state entities comply with all other requirements on the effective date. In response, this is already stated in the effective date language. The periodic requirements are exceptions to this language.

Several commented that CIP-010-1 requirement part 3.2 and CIP-009-5 requirement part 2.3 have a 36 month periodic performance requirement and should have an initial performance not exceeding 36 months after the effective date. Yet, although the periodicity for this requirement is 36 months, the initial performance should occur closer to the effective date of the standard. However, we are persuaded by arguments that initial exercises should be conducted prior to the operational exercise active vulnerability assessment.

Several commented that the language "…Notwithstanding any order to the contrary…" is unnecessary because the FERC can approve or remand any part of the implementation plan if it so chooses. While this is true, the inclusion of this language allows that decision to be made without the tremendous overhead of going through the standards development process.

One commenter argued that the periodic requirements section requires compliance as early as 14 days after the effective date, but the effective date allows 24 months. In response, this is true, and all of the specified periodic performance requirements occur after the effective date, which is at least 24 months.

One commenter argued the initial performance of the requirement should be performed prior to the effective date. They questioned why a year would be necessary to hold the first training or verify provisioned access. In response, the SDT disagrees with compliance prior to the effective date for two reasons. First, the effective date of the standard indicates when Version 5 becomes effective and previous versions retire. Requirements that obligate performance on a specific day cannot technically be compliant prior to the effective date. Second, the specified periodic requirements are mostly verification assessments or updates for existing security controls, and the objective is to have the security controls in place upon the effective date.

Based on comments received, CIP-009-5 requirement part 2.3 has been added to the list of periodic requirements that must be implemented no later than 12 months after the effective date.

One commenter noted that CIP-009-5 Requirement R1.4 still contains language requiring an initial performance. However, the intent of this requirement was not to obligate an initial periodic performance, and we have modified the requirement language to remove the word "initial".

Planned or Unplanned Changes

Several commenters suggested all new or reclassified Cyber Systems have the same timeframe of 12 months to achieve compliance. In response, we have updated the implementation plan based on changes to CIP-002-5 that remove obligations to update the BES Cyber System categorization within 60 days. This provides entities additional time to demonstrate full compliance for planned changes. Unplanned changes resulting in a higher categorization continue to allow the additional year to demonstrate full compliance for the affected BES Cyber Systems.

The Planned or Unplanned Changes section was collapsed into one section based on multiple comments, and it has been clarified that for *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System, with additional time to comply for requirements as specified and in the same manner as in the section *Initial Performance of Certain Periodic Requirements*. For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards, according to timelines specified in a separate table, following the identification and categorization of the affected BES Cyber System, with the additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Time Periods for Disaster Recovery

Several commenters requested clarity on what constitutes the completion of the Disaster Recovery. In response, the use of the defined term CIP Exceptional Circumstance throughout the CIP Cyber Security Standards eliminates the need to define a special case in the implementation plan for Disaster Recovery. Entities can take exceptions from the Requirements where CIP Exceptional Circumstances is specified.

One commenter suggested that the Disaster Recovery section seems to suggest not holding up restoration for compliance but entities would need to be compliant when restoration activities are complete. In response, this section

has been removed and we defer to the use of CIP Exceptional Circumstances throughout the CIP Cyber Security Standards to provide entities clarity on when and where exceptions to the Requirements can occur.

Applicability Reference Tables

One commenter requested additional clarification regarding the purpose of the applicability tables and others noted inconsistencies with the table. In response, we have corrected inconsistency errors, changed the title and provided introductory remarks. These tables are intended only for convenience. The SDT chose not to include this in a background or guidance section because requirement numbering will change in future revisions.

QUESTION D17 – DEFINITIONS AND IMPLEMENTATION PLAN:

If you have comments or specific suggestions that you have not been able to provide in response to the previous questions, please provide those comments here. Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the implementation plan was modified appropriately and certain areas were modified for clarity. Entities should refer to the individual responses to comments in the definitions questions for the SDT's response to comments for individual definitions. Many commenters provided comments on the positive direction of the posted draft. The SDT thanks these commenters and appreciates the encouraging remarks.

Several comments were toward the approach to requirements that result in a zero tolerance aspect for deficiencies in compliance monitoring. The SDT has proposed additional language that, together with a framework that also includes VSL language and RSAW audit guidance language, addresses the larger issue and shifts the focus of certain requirements to correcting deficiencies. This is explained in greater detail in the summary explanation at the beginning of this document.

Several commenters expressed their concerns on the protection of Low Impact BES Cyber Systems and the compliance demonstration of requirements that apply to them. The SDT has spent considerable time and effort to work with stakeholders on addressing this issue and believes that the approach in the new proposed draft addresses the concerns.

Multiple commenters reiterated concerns on the broad application of CIP V5 irrespective of connectivity. The SDT has included consideration of connectivity in the applicability of requirements and believes that this approach appropriately addresses applicability differences due to connectivity type. The SDT reiterates its posture that, while connectivity is an important vector for cyber security threats, it is not the only one and that the CIP standards encompass a holistic approach to the protection of BES Cyber Systems.

There were multiple comments that suggested the phrase "but not limited to…" may be construed as required evidence. The SDT agrees with the comment and is using the standard language "Example(s) of evidence may include, but is not limited to…" to convey two concepts in the measure: the evidence in the measure are not required evidence but represents examples of quality evidence, and entities may present other evidence that may be presented in lieu of the ones described or in addition to them.

Multiple comments were based on the definition of periodic requirements, with another commenter citing the CAN on Annual that has been published. The SDT notes that CANs provide guidance for auditors, are not interpretations of standard requirements and are not the basis for changes to requirements. The SDT has considered all outstanding CANs as additional input to the development of these standards, and where the CANs result from unclear requirement language, the SDT has drafted language with a goal of eliminating the need of a CAN for auditing purposes. Since the word annual is not used in the V5 CIP standards, the term does not apply. The SDT has drafted language that reflects its intent while providing adequate flexibility to minimize zero defect effects.

Several commenters requested a global clarification similar to section 5 of CIP-003 that explains the significance of the use of bulleted and numbered items. Another comment was on the bullets in section 4, part 4.2.2. The SDT will insert a paragraph in the background section to include such explanations.

There were several comments on the use of a single VRF for each requirement, irrespective of whether it applies to High Impact or Medium Impact. Another comment was on the VSLs and the differentiation required to handle zero defect. VRFs are used as one of many input variables used to determine the sanction in the case of a violation of a standard. The current sanction table used for calculating regulatory sanctions is based on VRFs at a requirement level. However, there are many other considerations in the determination of a sanction for a specific violation. Until the current development of the evolving enforcement model is better defined, it is premature to effect changes to the VRF. Regarding VSLs, the SDT notes that VSLs are used after the fact, i.e. when a violation has already occurred. The SDT believes that VRFs, VSLs and RSAWs, together with appropriate requirement language, must together provide a complete framework to address the zero defect issue. The ballot for VRFs and VSLs is a non-binding ballot, and there is likely to be changes to accommodate evolving concepts in handling zero defect compliance and risk based compliance assessments.

Several comments were on the compliance section on records retention and retention requirements in standards requirements. Retention requirements, when specified in requirements, are requirements for technical reasons, such as event log retention for forensic purposes. The retention periods specified in the compliance section are meant to apply to records required for demonstrating compliance. For example, if 90 day event log retention is specifically required in a requirement, the Responsible Entity is expected to retain records that demonstrate that it has kept 90 days of logged events for the 3 years, not that it has kept 3 years' worth of these event logs. Under the compliance section, these could be log entries of the process that maintains a minimum of 90 days of log events.

Several commenters suggested that all sub-requirement parts should state the goal. The SDT generally provides the goal either in the body of the main text for the requirement, or in the rationale box. The SDT believes that the goal of each subpart is mostly self-evident given the overall requirement objective, and that addition of a goal for each subpart would be redundant and unnecessary in most cases.

There were several comments surrounding the need for a definition of Control Centers. The SDT directs entities to its summary response to Question D9 on this issue.

There were several comments on the removal of restoration resources from Medium Impact criteria, and cited the need to provide adequate justification. It is not clear to the SDT whether these comments were in support of this change. However, as a matter of normal SDT stakeholder input consideration, extensive debate on this issue was conducted in the NERC operating and planning technical committees, without a clear resolution. As a matter of procedure, the SDT must provide justification for changes from one release to another and has received stakeholder comments supporting this change.

There were multiple suggestions that a summary of the CIP Version 5 standards and the interaction between the requirements and their applicability be provided by the SDT. The SDT is focused on addressing technical issues from comments on requirements and on the standards themselves. The SDT appreciates any input provided by stakeholders, and it plans to facilitate distribution of an informational summary addressing this concern that was prepared by certain stakeholders that have been collaborating with the SDT. However, the formal posting with the standards would require other types of SDT, NERC and other stakeholder groups' review and/or approval and is not an appropriate venue for making compliance management tools available to stakeholders.

There were several comments on the issue of physical access controls for High Impact, specifically on whether two different access control systems are required. The SDT has provided guidance on this issue in the guidelines and technical basis section of CIP-006 that indicate that the intent of the requirements is not to require different control systems.

Numerous commenters expressed concern with the term "Associated Protected Cyber Assets". In considering these comments, the SDT noted that the concept of high water marking for Impact Level within an ESP was not very clear. The SDT has defined a term Protected Cyber Assets to incorporate the concept of BES Cyber Systems, their associated Cyber Assets within the same ESP and the concept of High Water Marking for Impact level within an ESP.

There were several comments that a definition for dial-up connectivity is needed. The SDT has included a definition for "Dial-up Connectivity" in this draft proposal.

There were comments on the use of "Associated…" in the applicability column of requirement tables. The SDT has made some changes to the language used to clarify the applicability and has also used the defined term Protected Cyber Assets to further clarify applicability.

There were comments relating to a number of editorial and stylistic issues related to table headers, capitalization and inconsistencies of terms. The SDT has considered these comments and made the appropriate changes.

One commenter recommended that the exemptions section in the applicability section should be specific to the standard, and not say CIP-002-5 in standards other than CIP-002. The SDT agrees and has made the appropriate changes in the standards.

One commenter suggested that the application guidelines should be allowed to change from standard to standard and that glossary terms should not be defined again in the standard. The SDT disagrees that application guidelines should be the same for all standards, but does agree that there should not be any incompatibility or inconsistency between the guidelines and the standards. The SDT also agrees that there should not be any definitions repeated in a standard when they are proposed glossary terms. The SDT will ensure consistency between guidelines and standard requirements. The SDT notes that the notes on glossary terms in the guidelines or background section are intended to provide additional explanantion of the terms and not be replacement definitions for the proposed terms for the NERC glossary. The requirements in the standard are the ultimate source of authoritative text for compliance.

One commenter suggested that the requirements that should be subject to CIP Exceptional Circumstances should be extended to most requirements except those in CIP-002, CIP-003 and CIP-004, and provided a list of requirements that should be subject to CIP Exceptional Circumstances. The SDT has carefully selected requirements that it believes are appropriately suitable for a CIP Exceptional Circumstance in order to facilitate the handling of emergency situations and timely electronic and physical access for first responders. With regard to a comment on ensuring that CIP Exceptional Circumstance would not require a TFE, the SDT has no jurisdiction over Rules of Procedure and cannot predict what regulators will deem to be TFE triggering language in the future. It is not the SDT's intent that CIP Exceptional Circumstances be TFE triggering language, but rather, that the Responsible Entity has carefully defined its policies and

procedures for declaring and ending CIP Exceptional Circumstances as required in CIP-003, and that any specific CIP Exceptional Circumstance be documented as required to demonstrate compliance to the specific CIP requirement.

One commenter suggested that it should be clear that no policies or procedures are required for CIP-004 to CIP-011 Responsible Entities that do not have High or Medium Impact BES Cyber Systems. There is no requirement in CIP-004 through CIP-011 that is applicable to Low Impact BES Cyber Systems. This is clear in the applicability column of the requirements tables.

There was a comment on the incorporation of guidelines and technical basis in the standards, citing stakeholders' time constraints in reviewing guidelines during the comment period. The SDT has spent considerable time drafting guidelines and providing the technical basis for requirements as part of the structure of results based standards. The SDT believes that the guidelines and technical basis provides valuable information to stakeholders during the comment and balloting process. It provides valuable input to stakeholders on the intent of the SDT, both during the development and the implementation phases of the standards. This approach has received overwhelmingly positive feedback from stakeholders. While the SDT understands that these guidelines and technical basis are not intended to be used instead of, or in addition to requirements, the SDT believes they provide valuable context to the standards' requirements.

There was one comment on the use of attestations as measures, citing industry confusion on the appropriate use of attestations. The absence of "attestations" in the measures does not imply that attestations are not appropriate measures of compliance, but that the SDT chose to use more specific examples of evidence for these requirements. Whether attestations are appropriate measures of compliance depends on the requirement. The SDT has used attestations where it may more likely be the measure that can be produced as evidence of compliance, with no implication that it is the only way of demonstrating compliance.

One commenter suggested that part 4.2.3 of the applicability section (Section 4) may inadvertently create an exemption for Control Centers. While certain Functional Entities may not own BES Facilities as described in the NERC Glossary, they perform reliability functions as the Functional Entity listed in 4.1 for BES Facilities. The introductory paragraph of 4.2 specifically refers to "…Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above …"

One commenter requested clarification or a definition of "Adverse Reliability Impact": this term is defined in the NERC Glossary of Terms.

One commenter requested a formal definition for “Common Control System”: the SDT believes that the term control system is a widely understood term of art used in electric reliability operation and engineering and that it does not require specific definition in these standards.

One comment suggested that the standards use data and information interchangeably. The SDT notes that it has used data when referring to a set of values (numeric or otherwise) in its raw form, and to information when referring to data processed for a specific use.

One commenter noted that the CIP standards should be aligned more closely to the NIST or ISO standards. The SDT uses many frameworks (including the ones cited) as sources for the development of requirements. The SDT notes that both of the cited standards are general purpose cyber security standards and guidelines not intended for any specific industry use. The SDT believes that the mandatory nature for standards specifically for the BES poses unique challenges and requires an appropriately developed approach.

There was one comment that was extensively on the scope of applicability to asset owners and operators only, and the absence of compliance for suppliers and other third party providers. The SDT notes that these mandatory standards are developed under the jurisdiction of the ERO and that they can only be applied to NERC Registered Entities.

One comment was on the awareness and training requirement in CIP-004 R2 and role based awareness training. The comment was specific that the items in the table in R2 referred to systems while the requirement cited role based training. Table R2 contains the requirements for the required content of the training program, but the level at which the training is provided in each item is based on the role of the individual taking the training.

One comment was extensively on the 99.9% availability specification in CIP-006. The SDT has redrafted the requirement and the 99.9% specification has been removed.

There was one comment on the effect of the application of the CIP standards on small entities. The SDT notes that BES Cyber Systems are categorized based on reliability impact rather than on entity size. The SDT has developed the requirements to be commensurate with the level of impact on the BES. The SDT has not included entity size as an input to the applicability of requirements.

One comment was extensively on section 4.2.2. The SDT notes that section 4.2.2 is not intended to specify the impact criteria, but the scope. Consequently, many of the terms used are extracted from the registration criteria for DPs. Many of the comments presented have been incorporated in the proposed new draft, while a few are appropriate as part of the criteria.

One commenter made many remarks on global sections used in all standards. These will be reviewed by NERC standard staff as standard templates applicable to NERC standards.

There was a comment on the use of "where technically feasible" and the commenter suggested the use of language that would specify compensating controls. The SDT notes that there were requirements in CIP Versions 1-4 that had alternative language to allow compensating controls, but that the language was added to TFE triggers.

One commenter requested a definition of "Associated Data Centers". Please refer to the summary response on this issue to comments on D9.

One commenter was concerned with the periodic requirements, specifically on the 15 month period for periodic requirements intended to be performed annually. The commenters suggested alternative language that would ensure strict compliance with a 12 month period. The intent of the SDT in specifying a 15 month period for annual requirements is to provide some flexibility to entities in the framework of attenuating zero defect requirements. The comments imply that Responsible Entities would aim for strict minimum compliance at the cost of increased non-compliance risk. From the practical implementation standpoint, the SDT understands that most Responsible Entities will implement a process that would ensure the performance in a period less than 15 months (an annual period is easier to track from the compliance management standpoint) for assured compliance.

One comment was raised on the SDT's discussion of redundancy as not being a mitigation for cyber security vulnerabilities and stated that redundancy provide mitigation for some cyber security vulnerabilities. While redundancy provides some mitigation for recovery requirements, the SDT has not found a compelling case where strict redundancy of using an exactly mirrored system configuration would provide mitigation of a cyber security vulnerability. It is the SDT's opinion that such configurations have the unintended effect, from the cyber security (not operational) standpoint, of increasing the attack surface. The SDT does agree that configurations that provide redundancy of function rather than system redundancy can provide mitigation if implemented with systems dissimilar enough to provide mitigation of certain system specific cyber security vulnerabilities.

One comment was on the term Facility and its relation to systems, also stating that the term element is undefined. The SDT has used the term Facility in its defined meaning in the NERC Glossary when used in its capitalized form. The term Facility is used to refer to groups physical BES Elements. The NERC Glossary has a definition of Element used in the context of the BES. In cases where the SDT intends a broader scope to include systems, the SDT has used "Facilities, systems and equipment".

There was a comment on the exemption from the standards of cyber assets between discrete ESPs. In particular, the commenter suggested requirements to implement end-to-end encryption. The commenter seems to suggest that such encryption should be required for routable and non-routable protocols. In addition, the commenters suggest that EAPs should be subject to cyber security requirements. The SDT has not required specific technologies to protect information between ESPs, but has focused instead on the cyber security objectives of access control and monitoring of traffic across EAPs. The comments do not seem to take into account communication between ESPs of real-time, latency sensitive applications common in control systems. The authenticity and integrity of application data or information is not always implemented using communication encryption technology, but may be implemented at other layers of the overall stack without the latency overhead of encryption. The commenters also seem to interchangeably use EAPs and the cyber assets that implement the EAP. The CIP definition of an EAP is an interface. There are however requirements, including security event monitoring requirements, that are applicable to the Cyber Assets that perform access control and monitoring functions, including those that implement an EAP, for electronic and physical access.

A commenter suggested that BES information protection requirements should apply to third parties. The SDT agrees and expects the Responsible Entity to comply with requirements for protecting and handling BES protected information, whether such information is accessed or handled by its own employees and third parties. The requirements in CIP-011 require the Responsible Entity to implement processes to ensure such access control and handling.

One commenter provided its fundamental objection to Version 5 and suggested that implementation of the current CIP standards should be allowed to mature. The SDT is required to address all the FERC directives from Order 706, and FERC Order 706 has directed the ERO to complete consideration of Order 706 directives by March 31st, 2013.

One commenter suggested that the statement in the implementation plan that starts with "Not withstanding any order to the contrary…" should be amended in light of Order 706. The SDT believes that the window for the application of the statement is still possible given the deadline in Order 761.

One commenter inquired on when a cyber system would have to come into compliance as a result of an emergency. One commenter also inquired on how to treat temporary elevation. If the cyber system is re-categorized or is a new cyber system as a result of that emergency or unplanned change, the implementation table specifies 12 months.

There was a comment on missing requirements in item 5 of the Implementation Plan. The SDT has included these requirements.

One commenter pointed out that the background section dealing with reliable operation of the BES contains an unclear reference to the Functional Model. The SDT has added qualifications that clarify that both reliability tasks defined in the Functional Model and the functional entity's relationships with other functional entities are considered.

One commenter suggested that there are requirements where the text of the requirement specifies BES Cyber Systems when the applicability column specifies more than BES Cyber Systems. The SDT has reviewed the language of the requirements where this occurs to ensure consistency with the applicability column. In cases where more than BES Cyber Systems apply, the SDT generally uses "applicable Cyber Assets."

One commenter expressed the need for the concept of escorted electronic access for remote support using technologies such as WebEx. The fundamental concept in escorted access is not only that of continuous visibility on the actions of the escorted individual, but also the capability of timely intervention in the case of inappropriate action. The SDT believes that total support for this concept is not possible in an electronic access scenario.

One commenter stated that in its opinion, the functional entity Interchange Coordinator (IC) does not have any asset that would be included, and should therefore not be included in the applicability section. The SDT reviewed the reliability tasks for the IC function as well as the responsibilities of the IC Functional Entity in its relationship with other functional entities in the Functional Model and noted real-time responsibilities in the latter in relation to BAs and RCs.

Questions with Votes Only:

1. Do you agree with the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Madison Gas and Electric Company	No
MRO NSRF	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
FirstEnergy	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No

Organization	Yes or No
ACES Power Marketing	No
SPP and Member companies	No
Comment Development SME List	No
Dairyland Power Cooperative	No
CenterPoint Energy	No
Hydro One	No
Ingleside Cogeneration LP	No
NIPSCO	No
Trans Bay Cable	No
Consumers Energy Company	No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	No
American Transmission Company, LLC	No
Ameren	No
NextEra Energy, Inc.	No
Liberty Electric Power LLC	No
ISO New England Inc.	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No
Alliant Energy	No
New York Power Authority	No
Exelon Corporation and its affiliates	No
Wiscsonsin Electric Power Company	No
Farmington Electric Utility System	No
City Utilities of Springfield, MO	No
NYISO	No

Organization	Yes or No
Deseret Power	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
US Bureau of Reclamation	No
California Independent System Operator	No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
NCEMC	Yes
IRC Standards Review Committee	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes

Organization	Yes or No
Southern California Edison	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Xcel Energy	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Tennessee Valley Authority	Yes
PSEG	Yes
Texas Reliability Entity	Yes
PJM Interconnection	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes

2. Do you agree with the proposed definition of Control Center?

Organization	Yes or No
NRG Energy Companies	No
PNGC Comment Group	No
Madison Gas and Electric Company	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
NCEMC	No
ACES Power Marketing	No
IRC Standards Review Committee	No
National Rural Electric Cooperative Association (NRECA)	No
Southern California Edison	No

Organization	Yes or No
CenterPoint Energy	No
Manitoba Hydro	No
Xcel Energy	No
Snohomish County PUD	No
Lakeland Electric	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
NV Energy	No
NextEra Energy, Inc.	No
PSEG	No
Texas Reliability Entity	No
Liberty Electric Power LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No

Organization	Yes or No
POrtland General Electric	No
Exelon Corporation and its affiliates	No
Farmington Electric Utility System	No
Indiana Municipal Power Agency	No
Deseret Power	No
Central Lincoln	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
Northeast Power Coordinating Council	Yes
Southwest Power Pool Regional Entity	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes

Organization	Yes or No
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
SPP and Member companies	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Progress Energy	Yes
Western Area Power Administration	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
NIPSCO	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes

Organization	Yes or No
United Illuminating company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
ISO New England Inc.	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
Nebraska Public Power District	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
American Public Power Association	Yes

Organization	Yes or No
Springfield Utility Board	Yes
New York Power Authority	Yes
Wiscsonsin Electric Power Company	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Cowlitz County PUD	Yes
US Bureau of Reclamation	Yes

3. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager?

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Madison Gas and Electric Company	No
MRO NSRF	No
Dominion	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
NCEMC	No
ACES Power Marketing	No
Southern Company Services, Inc.	No
National Rural Electric	No

Organization	Yes or No
Cooperative Association (NRECA)	
Dairyland Power Cooperative	No
Tri-State G&T - Transmission	No
CenterPoint Energy	No
Manitoba Hydro	No
Xcel Energy	No
Bonneville Power Administration	No
MidAmerican Energy Company	No
Ameren	No
NextEra Energy, Inc.	No
Liberty Electric Power LLC	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No
Alliant Energy	No

Organization	Yes or No
Exelon Corporation and its affiliates	No
Deseret Power	No
Brazos Electric Power Cooperative	No
California Independent System Operator	No
Northeast Power Coordinating Council	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
SPP and Member companies	Yes

Organization	Yes or No
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Southern California Edison	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
NIPSCO	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes

Organization	Yes or No
Trans Bay Cable	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Illinois Municipal Electric Agency	Yes
NV Energy	Yes

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
PSEG	Yes
Texas Reliability Entity	Yes
PJM Interconnection	Yes
ISO New England Inc.	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
New York Power Authority	Yes
Wiscsonsin Electric Power Company	Yes

Organization	Yes or No
Farmington Electric Utility System	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

4. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager?

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Madison Gas and Electric Company	No
MRO NSRF	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
CenterPoint Energy	No
Trans Bay Cable	No
Manitoba Hydro	No

Organization	Yes or No
Snohomish County PUD	No
Lakeland Electric	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Ameren	No
NextEra Energy, Inc.	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No
Alliant Energy	No
Exelon Corporation and its affiliates	No
California Independent System Operator	No
Northeast Power Coordinating Council	Yes
NRG Energy Companies	Yes

Organization	Yes or No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Salt River Project	Yes
Southern California Edison	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
NIPSCO	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes

Organization	Yes or No
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Tampa Electric Company	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes

Organization	Yes or No
ISO New England Inc.	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
New York Power Authority	Yes
Wiscsonsin Electric Power Company	Yes
Farmington Electric Utility System	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes

Organization	Yes or No
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

5. Do you agree with the proposed definitions of Electronic Access Control or Monitoring Systems, Interactive Remote Access, and Intermediate Device?

Organization	Yes or No
Salt River Project	No
Trans Bay Cable	No
United Illuminating company	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Texas RE NERC Standards Review Subcommittee	No
Dairyland Power Cooperative	No
Lakeland Electric	No
Illinois Municipal Electric Agency	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Madison Gas and Electric Company	No

Organization	Yes or No
MRO NSRF	No
Duke Energy	No
Florida Municipal Power Agency	No
ACES Power Marketing	No
IRC Standards Review Committee	No
Comment Development SME List	No
CenterPoint Energy	No
NIPSCO	No
Bonneville Power Administration	No
MidAmerican Energy Company	No
Ameren	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No

Organization	Yes or No
Alliant Energy	No
Exelon Corporation and its affiliates	No
Wiscsonsin Electric Power Company	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
Southern California Edison	Yes
ATCO Electric	Yes
Northeast Power Coordinating Council	Yes
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
PPL Corporation NERC	Yes

Organization	Yes or No
Registered Affiliates	
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
NCEMC	Yes
SPP and Member companies	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes

Organization	Yes or No
Ingleside Cogeneration LP	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Tampa Electric Company	Yes
NV Energy	Yes

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
ISO New England Inc.	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
New York Power Authority	Yes
Farmington Electric Utility System	Yes

Organization	Yes or No
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
US Bureau of Reclamation	Yes
Luminant	
American Transmission Company, LLC	

6. Do you agree with the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Madison Gas and Electric Company	No
MRO NSRF	No
FirstEnergy	No
Duke Energy	No
Florida Municipal Power Agency	No
SPP and Member companies	No
IRC Standards Review Committee	No

Organization	Yes or No
Southern California Edison	No
Dairyland Power Cooperative	No
Hydro One	No
NIPSCO	No
Hydro-QuÃ©bec Production	No
Turlock Irrigation District	No
Bonneville Power Administration	No
Lakeland Electric	No
Illinois Municipal Electric Agency	No
NV Energy	No
NextEra Energy, Inc.	No
ISO New England Inc.	No
Nebraska Public Power District	No
Alliant Energy	No
New York Power Authority	No

Organization	Yes or No
Exelon Corporation and its affiliates	No
Wiscsonsin Electric Power Company	No
City Utilities of Springfield, MO	No
NYISO	No
California Independent System Operator	No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Texas RE NERC Standards Review Subcommittee	Yes

Organization	Yes or No
NCEMC	Yes
ACES Power Marketing	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
CenterPoint Energy	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
Independent Electricity System Operator	Yes

Organization	Yes or No
Trans Bay Cable	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Xcel Energy	Yes
Snohomish County PUD	Yes
Tampa Electric Company	Yes
MidAmerican Energy Company	Yes
Massachusetts Municipal	Yes

Organization	Yes or No
Wholesale Electric Company	
Tennessee Valley Authority	Yes
Ameren	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
City of Austin dba Austin Energy	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
Farmington Electric Utility	Yes

Organization	Yes or No
System	
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

7. Do you agree with the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Madison Gas and Electric Company	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
Duke Energy	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
Progress Energy	No

Organization	Yes or No
CenterPoint Energy	No
Hydro One	No
NIPSCO	No
Lower Colorado River Authority	No
LCRA Transmission Services Corporation	No
Xcel Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
NextEra Energy, Inc.	No
ISO New England Inc.	No

Organization	Yes or No
City of Austin dba Austin Energy	No
Utility Services Inc.	No
New York Power Authority	No
Farmington Electric Utility System	No
City Utilities of Springfield, MO	No
NYISO	No
California Independent System Operator	No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes
Dominion	Yes
FirstEnergy	Yes
NCEMC	Yes

Organization	Yes or No
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Southern California Edison	Yes
Dairyland Power Cooperative	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes

Organization	Yes or No
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes

Organization	Yes or No
Ameren	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Nebraska Public Power District	Yes
Alliant Energy	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
Wiscsonsin Electric Power Company	Yes

Organization	Yes or No
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

15. Do you agree with the changes made to the proposed implementation plan since the last formal comment period?

Organization	Yes or No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
Southern California Edison	No
Dairyland Power Cooperative	No
Hydro One	No
Trans Bay Cable	No
Turlock Irrigation District	No
NextEra Energy, Inc.	No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
MRO NSRF	No
NESCOR/NESCO	No
Duke Energy	No

Organization	Yes or No
Southern Company Services, Inc.	No
CenterPoint Energy	No
Consumers Energy Company	No
Manitoba Hydro	No
Snohomish County PUD	No
MidAmerican Energy Company	No
ISO New England Inc.	No
Nebraska Public Power District	No
Alliant Energy	No
New York Power Authority	No
Exelon Corporation and its affiliates	No
NYISO	No
Kansas City Power & Light	No
Texas RE NERC Standards Review Subcommittee	Yes

Organization	Yes or No
United Illuminating company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Brazos Electric Power Cooperative	Yes
Utility Services Inc.	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes

Organization	Yes or No
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes

Organization	Yes or No
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes
Bonneville Power Administration	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Illinois Municipal Electric Agency	Yes
NV Energy	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
PSEG	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
City of Austin dba Austin Energy	Yes

Organization	Yes or No
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
American Public Power Association	Yes
Wiscsonsin Electric Power Company	Yes
Farmington Electric Utility System	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
California Independent System Operator	Yes

Organization	Yes or No
Madison Gas and Electric Company	
Luminant	
American Transmission Company, LLC	

END OF REPORT

Project 2008-06 - Cyber Security Order No. 706 - V5

Working Draft (September 11, 2012) of Consideration of Issues and Directives

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 233 (Related paragraph: 25) Para 233 "The Commission continues to believe and is further persuaded by the comments that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. Moreover, we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk-Power System should be addressed in NERCs Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need	FERC Order No. 706	In its development of CIP Version 5, the Standards Drafting Team (SDT) considered many existing cyber security frameworks. Notably, the SDT included consideration of the NIST Risk Management Framework, NIST Publication 800-53, as well as the "DHS Catalog of Control Systems Security: Recommendations for Standards Developers" in the development of its requirements for cyber systems categorization and applicable requirements. Five key features of the NIST Risk Management Framework were incorporated into Version 5 of NERC CIP Standards: (1) ensuring that all BES Cyber Systems associated with the Bulk Power System, based on their function, receive some level of protection, (2) customizing protection to the mission of the cyber systems subject to protection, (3) a tiered approach to security controls which specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk Power System, (4) the concept of the BES Cyber System itself, and (5) Version 5 has incorporated the "Assess" and "Monitor" processes of the NIST Risk Management Framework in the development of the requirements and enabled these processes through additional language for identifying, assessing, and correcting deficiencies in controls.. Features 2 and 3 above are tightly coupled. In the NIST Risk Management Framework, there is a concept of tailoring and scoping which allows the organization to determine which controls are applicable to their specific environment. In the NERC compliance framework, all requirements are mandatory and enforceable, and, therefore, this concept does not translate directly. As such, the customization of protections by mission is based upon the environment that the BES Cyber System supports (control center, transmission facility, generation facility) and utilizes the tiered model and the requirement applicability to provide this customization to the individual environments that together support a

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
for new CIP Reliability Standards, or as part of an assessment of NERCs performance of its responsibilities as the ERO." Para 25 "The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework. "		combined mission of Bulk Power System reliability. The NIST Security Control Catalogue in 800-53, Revision 3 and the DHS Catalog of Controls Systems Security were also used as a reference in addressing many of the FERC directives in Order No. 706. Additionally, the SDT included members representing federal agencies and NIST, in particular, during the development of these CIP standards.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 and 249 Para 258 "Likewise, the ERO should consider Northern Californias suggestion that the ERO establish a formal feedback loop to assist the industry in developing policies and procedures." Para 249 "In contrast, FirstEnergy agrees that NERC should provide guidance to entities without a wide-area view, such as a generation owner or a partial generation owner, on how to approach a risk-based assessment. Likewise, Northern California suggests that NERC establish a process for informal, case-by-case consultations with responsible entities that need assistance in complying with CIP-002-1. In addition, as part of the re-examination of CIP-002-1, Northern California encourages the incorporation of a formalized feedback loop to assist the industry in developing policies and procedures."	FERC Order No. 706	CIP-002-5 classifies BES Cyber Systems through impact thresholds, and does not use risk-based assessments performed by individual entities. CIP-002-5, Attachment 1's bright line criteria were developed in consideration of a wide area view, and it obviates the need for a formal feedback loop or a need for a wide area view by smaller entities.
Para 258 and 252	FERC Order No. 706	Early during the development of CIP-002-5, the SDT discussed the concept of Design-Basis Threat (DBT). The SDT, in CIP-002-5, classifies BES Cyber Systems through impact

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 "As to Entergys suggestion that the ERO provide a DBT profile of potential adversaries, the ERO should consider this issue in the Reliability Standards development process." Para 252 "Entergy suggests, as an alternative approach to critical asset identification, that the ERO provide a Design-Basis Threat (DBT) a profile of the type, composition, and capabilities of an adversary that would assist the industry as a technical baseline against which to establish the proper designs, controls and processes. Entergy claims that a DBT approach would address many of the Commissions concerns regarding the risk-based methodology. For example, a DBT would focus the appropriate emphasis on the potential consequences from an outage of a critical asset. In addition, a DBT would address the Commissions concern that responsible entities will not have enough guidance in developing a risk-based methodology and not know how to identify a critical asset. Entergy contends that a DBT		thresholds, and does not use risk-based assessments performed by individual entities. The complexity and subjectivity involved in an entity's risk-based assessment, such as one based on DBT, would run counter to the CIP-002-5 objectives of categorization based on impact defined by bright-line criteria. CIP-002-5, Attachment 1's bright line criteria uses an impact-based approach as an alternative to DBT. This approach was approved by the Commission in its Order No. 761 approving Version 4 of the CIP Cyber Security Standards.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
approach would provide the industry with more certainty in implementing the CIP Reliability Standards."		
Para 272 (1 of 2) "Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, **the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset.** In doing so, the ERO should consider Juniper's comments. Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data."	FERC Order No. 706	This was completed by CIPC in the Version 3 CIP standards guidelines. The guidelines are entitled "Identifying Critical Assets" and "Identifying Critical Cyber Assets" and are available for download from www.nerc.com.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 272 (2 of 2) "Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset. In doing so, the ERO should consider Juniper's comments. **Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data."**	FERC Order No. 706	Guidance developed for CIP-002-5 addresses situational awareness and inter-utility data exchange.
Para 285 (related paragraph: 278) Para 285 "The Commission directs the ERO to consider the comment from ISA99 Team	FERC Order No. 706	The exclusion of Cyber Assets based on non-routable protocols has been removed from CIP-002-5, and added as an applicability filter for requirements where: (i) the use of non-routable protocols is a mitigating factor for the vulnerabilities a requirement addresses, or (ii) implementation of routable protocols, when not otherwise used, would be required to comply with the requirement (e.g. malware updates, security event monitoring, and alerting, etc.).

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
[ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience].” Para 278 “ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience. In contrast, Energy Producers notes that CIP-002-1 as proposed by NERC provides that a critical cyber asset must have either routable protocols or a dial-up connection. Energy Producers states that this is a useful, objective criterion which will assist in the unambiguous identification of such assets and therefore should be retained.”		

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 296 "With regard to METC-ITC's comment, the ERO should consider in its Reliability Standards development process the suggestion that the CIP Reliability Standards require oversight by a corporate officer (or the equivalent, since some entities do not have corporate officers) rather than by a "senior manager."	FERC Order No. 706	The requirement that the senior manager have "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" ensures that the senior manager is of the sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for Responsible Entities, from municipal, cooperative, federal agencies, investor-owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis. In Version 5, this is addressed in the definition of CIP Senior Manager. The SDT believes the filing for Version 2 also addressed this issue.
Para 321 " SPP and ReliabilityFirst suggest modifying CIP-002-1 to allow an entity to rely upon the assessment of another entity with interest in the matter. We believe that this is a worthwhile suggestion for the ERO to pursue and the ERO should consider this proposal in the Reliability Standards development process. We note that, even without such a provision, an entity such as a small generator operator is not foreclosed from consulting with a balancing authority or other appropriate entity with a wide-area view of the transmission system."	FERC Order No. 706	The SDT believes that this suggestion would be applicable in a model of an entity's own risk-based methodology, where certain small entities may not benefit from a wider area view. The change to "bright line" criteria for identifying BES Cyber Systems in CIP-002-5, along with refining the scope of certain requirements through applicability columns based on impact and connectivity characteristics, no longer requires entities to use a self-defined risk-based methodology, which addresses this concern.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 355 (also see paragraph 356) "The Commission believes that responsible entities would benefit from additional guidance regarding the topics and processes to address in the cyber security policy required pursuant to CIP-003-1. While commenters support the need for guidance, many are concerned about providing such guidance through a modification of the Reliability Standard. We are persuaded by these commenters. Accordingly, the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address. However, we will not dictate the form of such guidance. For example, the ERO could develop a guidance document or white paper that would be referenced in the Reliability Standard. On the other hand, if it is determined in the course of the Reliability Standards development process that specific guidance is important enough to be incorporated directly into a Requirement, this option is not foreclosed. The entities remain responsible, however, to comply with the cyber security policy pursuant to CIP-003-1."		The SDT has chosen to provide guidance to Responsible Entities through the introduction of topical areas in the requirement language that must be addressed in cyber security policies in CIP-003-5, requirements R1 and R2. Additionally, as directed, the SDT has provided guidance about these topical areas in the Guidelines and Technical Basis section of Reliability Standard CIP-003-5.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 376 "... the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards. In response to EEI, we believe that this clarification is needed because, for example, it is important that a responsible entity understand that exceptions that individually may be acceptable must not lead cumulatively to results that undermine compliance with the Requirements themselves."	FERC Order No. 706	The SDT removed the CIP-003-4 requirement to document exceptions to the Cyber Security Policy. • The SDT considers this a general management issue that is not within the scope of a compliance requirement. • The SDT found no reliability basis in this requirement. • Removal of this requirement provides clarity that the only exceptions to the requirements is through the defined Technical Feasibility Exception process, where specifically allowed.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 386 "The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly. In general, the Commission agrees with commenters and believes that access to protected information should cease as soon as possible but not later than 24 hours from the time of termination for cause."	FERC Order No. 706	To address this directive, in CIP-004-5, requirement R5, Responsible Entities must revoke access to the electronic and physical locations where it stores BES Cyber System Information. This could include records, closets, substation control houses, records management systems, file shares, or other physical and logical areas under the Responsible Entity's control. The SDT specified the revocation action to be completed "by the end of the next calendar day following the effective date and time of the termination action" to provide a more defined time threshold, following the SDT's discussion of the difficulty in defining an exact time in a termination process that typically includes multiple steps and organizations within an entity.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 397 and 398 "The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes. The Commission believes that these considerations are significant aspects of change control and configuration management that deserve express acknowledgement in the Reliability Standard. While we agree with Entergy that the NIST Security Risk Management Framework offers valuable guidance on how to deal with these matters, our concern here is that the potential problems alluded to be explicitly acknowledged. Our proposal does not speak to how these problems should be addressed. We do not believe that the changes will have burdensome consequences, but we also note that addressing any unnecessary burdens can be dealt with in the Reliability Standards development process."	FERC Order No. 706	Two new requirements in a new standard CIP-010-1 were added to address this change: CIP-010-1, requirement R1 (part 1.5), requires additional testing prior to a configuration change in a test environment; CIP-010-1, requirement R2 (part 2.1), requires monitoring of the configuration of the BES Cyber System. • The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System. • Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) prior to their implementation in the production environment to aid in identifying any accidental consequences, to required cyber security controls, of the change.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 412 "The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world."	FERC Order No. 706	The SDT addresses this through the defense in depth framework that has been designed through the full suite of revised CIP Standards. The standards address defense in depth through personnel management, systems management, and information management. The Standards are written in the perspective that the Responsible Entity is required to protect its cyber systems from internal and external threat. The requirements include both preventive and detective controls. The requirements mandate appropriate vetting of personnel to minimize the risk of internal threat. They then build upon this through secure system design for internal use and remote access. These controls are further enhanced by the requirement of robust monitoring and alerting activities. Specific requirements in the identification and protection of physical and electronic security perimeters assume a default posture of "deny-by-default" to reinforce the posture of mutual distrust.
Para 433 ". . . we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard."	FERC Order No. 706	The SDT addressed this by determining that identification of certain core training elements would be beneficial, and the identification of those core training elements that must be provided in the training program should be role based, as required in CIP-004-5, requirement R2.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 434 "The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets."	FERC Order No. 706	The SDT added this as a topic for role-specific training in CIP-004-5, requirement R2 (part 2.1). Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems.
Para 435 "Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves."	FERC Order No. 706	The SDT has considered the issue and has determined that no modifications are necessary. In practice, this training is often conducted as computer-based training (CBT), and the training is aimed at an entity's own policies. The SDT believes that assessments of the adequacy of the training during the compliance monitoring process implicitly evaluate the adequate training of the trainers or the efficacy of the training method.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 446 (1 of 2) (Review the referenced Comments) " APPA/LPPC seek **clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees.** SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees. The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."	FERC Order No. 706	The SDT clarifies the discretion in reviewing personnel risk assessments in CIP-004-5, requirement R3, by requiring the Responsible Entity to establish and document criteria for personnel risk assessments. The requirements in CIP-004-5 also provide additional detail about what type of records (whether criminal, work history, domicile, etc) a Responsible Entity must examine.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 446 (2 of 2) (Review the Referenced Comments) "APPA/LPPC seek clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees. **SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees.** The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."	FERC Order No. 706	In CIP-004-5, requirement R3, the SDT has specified that the seven-year criminal history records check must include current residence, regardless of duration, and include other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 460 "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."	FERC Order No. 706	In CIP-004-5, requirement R5, the SDT has addressed this directive by requiring initiation of the revocation of physical and interactive remote access, to be completed within 24 hours of termination, concurrent with the termination or disciplinary action (Part 5.1), or by the end of the calendar day in cases of transfers or reassignments (Part 5.2) for access that the Responsible Entity determines is no longer needed.. CIP-004-5, requirement R5 (part 5.4) augments the requirements in parts 5.1 and 5.2 that respond to the directive. In order to meet the immediate time frame, Entities will likely have initial revocation procedures to prevent physical and interactive remote access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. Part 5.4 requires the Responsible Entity to complete the revocation process within the time specified (30 days). Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
Para 464 "We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification."	FERC Order No. 706	The SDT notes that it addresses this issue in previous versions of the CIP standards. Version 2 added the requirement for a personnel risk assessment prior to being granted access, and Version 3 required implementation of a visitor control program. The changes made to the requirements in Version 5 maintain and improve upon these requirements. CIP-004-5, requirement R4 makes clear that individuals not properly authorized for unescorted physical access will not have such access. CIP-006-5 restricts access through implementation of a visitor management program.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 473 "The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entitys obligations regarding vendors with access to critical cyber assets."	FERC Order No. 706	CIP-002-5, requirement R1 makes clear that asset owners are responsible for complying with the standards.
Para 476 "We direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent with the Commissions determinations above."	FERC Order No. 706	Guidance in CIP-002-5 states that the owning Responsible Entity is responsible for complying with the CIP Cyber Security Standards. Furthermore, the guidelines and technical basis for CIP-002-5 states that where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 496 (Related: Para 503) Para 496 "The Commission adopts the CIP NOPRs proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter" Para 503 "The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures."	FERC Order No. 706	The drafting team addresses this in CIP-005-5, requirement R1 (part 1.5). Per FERC Order No. 706, Paragraphs 496 through 503, Electronic Security Perimeters (ESP) need two distinct security measures, such that the cyber assets do not lose all perimeter protection if one measure fails or is misconfigured, in a defense-in-depth approach. The Order makes clear that this is not simple redundancy of firewalls; thus, the drafting team added the security requirement of malicious traffic inspection (IDS/IPS) as a second security control for electronic access points for High Impact BES Cyber Systems.
Para 502 "The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process."	FERC Order No. 706	The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security requirement of malicious traffic inspection (IDS/IPS) as a second security control for electronic access points for High Impact BES Cyber Systems.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 504 (Related: Para 495) Para 504 "The ERO should consider in the Reliability Standards development process Northern Indiana's and Xcel's concerns regarding the phrase "single access point at the dial up device." Para 495 "Northern Indiana and Xcel ask the Commission to clarify or direct the ERO to clarify the phrase "single access point at the dial up device" in CIP-005-1, Requirement R1.2. Xcel asks whether this refers to the initiating device, the device at the point of termination, or both. Northern Indiana would not modify CIP-005-1, but urges that any modifications to Requirement R2 should allow continued reliance on legacy systems."	FERC Order No. 706	The SDT has deleted the troublesome language relating to "single access point at the dial up device," and the SDT has clarified that an Electronic Security Perimeter applies to routable connectivity. CIP-005-5 also separated the requirement for dial-up connectivity, specifying in CIP-005-5, R1.4, that a Responsible Entity must perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible, on its high and medium impact BES Cyber Systems with dial-up connectivity.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 511 "The Commission adopts the CIP NOPRs proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies."	FERC Order No. 706	CIP-005-5, requirement R2 has additional security requirements for remote access from the work started in the Urgent Action Revisions to CIP-005-3. One of these requirements is two-factor authentication and specific examples of two-factor authentication are provided in the guideline referenced in the rationale for this requirement.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 525 "The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily…" Para 628. "Requirement R6 of CIP-007-1 does not address the frequency with which log should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly…"	FERC Order No. 706	In CIP-007-5, requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of once every 15 days. CIP-007-5, requirement R4, combines CIP-005-4, requirement R5 and CIP-007-4, requirement R6, and addresses FERC Order No. 706's directives from a system-wide perspective. The primary feedback received on this requirement from comment periods was the vagueness of terms "security event" and "monitor." The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach to specify a minimum set of security event types to log and review, and allows the entity to define relevant security events in addition to the specified minimum. In addition, CIP-007-5, requirement R4, sets up parameters for the logging and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC Order No. 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 526 (1 of 2) ". . . the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments.	FERC Order No. 706	In CIP-007-5, requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of once every 15 days. (Also see response to paragraph 525).
Para 526 (2 of 2) "The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs."	FERC Order No. 706	CIP-007-5, requirement R4, sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. (Also see response to paragraph 525).
Para 528 "The Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs."	FERC Order No. 706	In CIP-007-5, requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of once every 15 days. In addition, CIP-007-5, requirement R4, sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC Order No. 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings. (Also see response to paragraph 525).

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 541 ". . . we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments."	FERC Order No. 706	In CIP-010-1, requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires paper assessments at least once every 15 months in the intervening years.
Para 542 ". . . the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems."	FERC Order No. 706	In CIP-010-1, requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires paper assessments at least once every 15 months in the intervening years.
Para 544 (1 of 2) "the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification."	FERC Order No. 706	The SDT addresses this paragraph in CIP-010-1, requirement R3. • The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new Cyber Asset undergo an active vulnerability assessment. • An exception is made for specified CIP Exceptional Circumstances. • Additionally, the new requirement in CIP-010-1, requirement R1 (part 1.5) requires testing of all changes for High Impact BES Cyber Systems that deviate from the baseline configuration in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) to ensure that required security controls are not adversely affected.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 544 (2 of 2) “. . . we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment”	FERC Order No. 706	The SDT has added a requirement in CIP-010-5, requirement R3 (part 3.3), to perform an active vulnerability assessment of a new Cyber Asset in High Impact BES Cyber Systems.
Para 547 ". . . we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"	FERC Order No. 706	In CIP-010-1, requirement R3, the SDT has added requirements for an “active vulnerability assessment” to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires paper assessments at least once every 15 months in the intervening years.
Para 572 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."	FERC Order No. 706	The SDT addressed this in CIP-006-5, requirement R1 (part 1.3) for High Impact BES Cyber Assets, by requiring Responsible Entities to “utilize two or more different physical access controls to collectively allow physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.”

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 581 "The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years."	FERC Order No. 706	The SDT addressed this in CIP-006-5, requirement R3 (part 3.1) by changing the frequency to a 24-month testing cycle; after deliberation and consideration, the SDT determined that a requirement of more frequent testing (e.g., 12 months), would pose unreasonable burden for Responsible Entities with a large number of physical security perimeters dispersed over large geographic areas.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 609, Sentence 5 "The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a representative system one that includes the essential equipment and adequately represents the functioning of the production system. **We therefore direct the ERO to develop requirements addressing what constitutes a representative system and to modify CIP-007-1 accordingly.** The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."	FERC Order No. 706	The SDT has introduced the concept of a “baseline configuration” around which the change control process is based. The SDT further utilizes this “baseline configuration” to provide clarity as to what is considered a representative system as it relates to performing active vulnerability assessments in CIP-010-1.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 609, Sentence 6 "The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a representative system one that includes the essential equipment and adequately represents the functioning of the production system. We therefore direct the ERO to develop requirements addressing what constitutes a representative system and to modify CIP-007-1 accordingly. **The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."**	FERC Order No. 706	The SDT has provided additional guidance on testing systems in the Guidelines and Technical Basis section of CIP-010-1. Furthermore, and in addition to guidance, the requirements of CIP-010-1 R1.5 and CIP-010-1 R3.2 identify a "representative system" as a system that exists in a test environment (or production environment where tests can be performed in a manner that minimizes adverse effects) that models the baseline configuration of the BES Cyber System in a production environment. This baseline configuration concept is developed by entities in CIP-010-1 R1.1 and further contains details on what constitutes a "representative system."

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 610 “. . . we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above.”	FERC Order No. 706	CIP-010-1, requirements R1 (part 1.5) requires Responsible Entities to account for any additional differences between the two systems, the SDT proposes using the words similar to those directly from FERC Order No. 706, paragraph 610: “Document the differences between the test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.”

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 611 "With respect to MidAmericans proposal that the differences between the testing and production environments only be reported when the production and test environments are established, the ERO should consider this matter in the Reliability Standards development process However, the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."	FERC Order No. 706	The SDT has added a requirement for the Responsible Entity to, "document…the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments." The SDT has included this requirement for each test performed in the representative environment. The SDT appreciates the concern brought up by MidAmerican and believes that entities should be free to use the same documentation multiple times to provide compliance with this requirement so as to minimize the documentation overhead, but also believes that it is important for entities to give consideration to the configuration of their representative system each time a test is performed in order to ensure the validity of the test results.
Paras 622 (Related: See Paras 614 and 619) "Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere."	FERC Order No. 706	The "acceptance of risk" language was removed in Version 2, and it has not been used in Version 5. Malicious software prevention exceptions have been placed under the TFE process since Version 2.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 622 (Related: See Paras 614 and 619) "The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above."	FERC Order No. 706	The drafting team addressed this in CIP-007-5, requirement R3. The drafting team is taking the approach of making this requirement a competency-based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive. When remote access is used to connect to a BES Cyber Asset, an intermediate device is required in CIP-005-5, requirement R2 (part 2.1) and guidance is further included for the cyber security policy in CIP-003-5, Requirement R2 to maintain up-to-date anti-malware software and patch levels before initiating interactive remote access.
Para 628 "The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1."	FERC Order No. 706	In CIP-007-5, requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of once every 15 days.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 633 "The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it."	FERC Order No. 706	The SDT addresses this directive in CIP-011-1, requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from the BES Cyber Asset. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal. Additional guidance was added to the standard as further clarification: Media sanitization is generally classified into four categories: disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes. This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 635 "the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."	FERC Order No. 706	The SDT addresses this directive in CIP-011-1, requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from the BES Cyber Asset. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal. Additional guidance was added to the standard as further clarification: Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes. This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 643 (1 of 2) **"The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments**, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."	FERC Order No. 706	In order to provide more direction on what "features, functionality, and vulnerabilities" should be addressed in a vulnerability assessment, the SDT included guidance in CIP-010-1 on active and paper vulnerability assessment. The SDT further referenced NIST SP800-115 to provide entities additional guidance on how to conduct a vulnerability assessment.
Para 643 (2 of 2) "The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, **and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."**	FERC Order No. 706	In CIP-010-1, requirement R3 (part 3.4), the SDT added a requirement for an entity planned date of completion to the remediation action plan following a vulnerability assessment.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 660 (Related, See Para 661) "The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. In developing the guidance, the ERO should consider the specific examples provided by commenters, described above. However, we direct the ERO to develop and provide guidance on the term reportable incident. The Commission is not opposed to the suggestion that the ERO create a reference document containing the reporting criteria and thresholds and requiring responsible entities to comply with the reference document in the revised Reliability Standard CIP-008-1, but will allow the ERO to determine the best method to accomplish the goal of better defining reportable incident."	FERC Order No. 706	In addition to defining the term Reportable Cyber Security Incident as one that compromises or disrupts the functional tasks of a Responsible Entity, CIP-008-5 also provides further guidance for determining a Reportable Cyber Security Incident in the "Guidelines and Technical Basis" section of the standard. The definition and guidance describe a reportable incident based on characteristics of impact to the BES, rather than enumerating threats and characteristics of malware.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 661 (Related, See Para 660) "the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."	FERC Order No. 706	CIP-008-5 addresses the four parts of this directive as follows: 1. Added: Reportable Cyber Security Incidents include, as a minimum, any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. In turn, a Cyber Security Incident includes a malicious act or suspicious event that compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter. 2. CIP-008-4, requirement R1 (part 1.2) contains provisions for reporting Cyber Security Incidents. 3. See 1, above. 4. Guidance and measurements have been developed to provide information that may be used to enhance an auditable and enforceable standard.
Para 673 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order No. 706	Cyber Security Incident Reporting and Response Planning: CIP-008-4, requirement R1 (part 1.3) contains provisions for reporting Cyber Security Incidents to the ES-ISAC within one hour of identification, even if it is a preliminary report.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 676 "The Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order No. 706	Cyber Security - Incident Reporting and Response Planning: CIP-008-4, requirement R1 (part 1.3) contains provisions for reporting Cyber Security Incidents to the ES-ISAC within one hour of identification, even if it is a preliminary report. . Cyber Security - Incident Reporting and Response Planning: CIP-008-4, requirement R1 (part 1.3) contains provisions for reporting Cyber Security Incidents to the ES-ISAC within one hour of identification, even if it is a preliminary report.
Para 686 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned."	FERC Order No. 706	In CIP-008-5, Requirement R3 and its parts, the SDT includes additional specification on the update of response plan and modifies the response plan requirements to incorporate lessons learned. Maintenance of documentation of paper drills, full operational drills, and responses to actual incidents is part of the documentation required to demonstrate compliance with the security controls in CIP-008-5 and is already subject to the evidence retention requirements associated with all NERC Reliability Standards.
Para 687 (also see Footnote in Order) "In light of the comments received, the Commission clarifies that, with respect to full operational testing under CIP-008-1,	FERC Order No. 706	CIP 008-5, Requirement R2, Part 2.1 is written to allow the testing requirement to be satisfied by responding to an actual Reportable Cyber Security Incident; or with a paper drill or table top exercise; or with a full operational exercise. The reporting of Cyber Security Incidents is addressed in the requirement R1 (part 1.2).

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
such testing need not require a responsible entity to remove any systems from service. The Commission understands that use of the term full operational exercise in this context can be confusing. We interpret the priority of the testing required by this provision to be that planned response actions are exercised in reference to a presumed or hypothetical incident contemplated by the cyber security response plan, and not necessarily that the presumed incident is performed on the live system. A responsible entity should assume a certain type of incident had occurred, and then ensure that its employees take what action would be required under the response plan, given the hypothetical incident. A responsible entity must ensure that it is properly identifying potential incidents as physical or cyber and contacting the appropriate government, law enforcement or industry authorities. CIP-008-1 should require a responsible entity to verify the list of entities that must be called pursuant to its cyber security incident response plan and that the contact numbers at those agencies are correct. The ERO should clarify this in the revised Reliability Standard and may use a term different than		The Guidelines and Technical Basis section of CIP-008-5 refer to operational exercises in the FEMA Homeland Security Exercise Evaluation Program as one of the following three types: drill, functional exercise, and full-scale exercise. It defines that "[a] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, emergency operation centers, etc.) and "boots on the ground" response (e.g., firefighters decontaminating mock victims)." The SDT believes the term operational exercise has become well understood and appropriate for both incident response and recovery exercises.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
full operational exercise."		
Para 694 "For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard"	FERC Order No. 706	The SDT added in CIP-009-5, Requirement R2, a requirement to implement the recovery plan.
Para 706 "The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard."	FERC Order No. 706	CIP-009-5, Requirement R1, Part 1.5 requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service. The SDT captured the objective of this control, but did not explicitly use the term "forensics" due to the legal interpretations associated with the term.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 710 (Related: Para 706) "Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report."	FERC Order No. 706	CIP-009-5, Requirement R1, Part 1.5 requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service.
Para 725 "The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years."	FERC Order No. 706	CIP-009-5, Requirement R2, Part 2.3 requires an operational exercise at least once every three calendar years.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 739 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."	FERC Order No. 706	In CIP-009-5, Requirement R1, Part 1.4 the SDT added requirements related to restoration processes based on review of the DHS Controls, and requires verification initially after backup to ensure that the process completed successfully. In CIP-009-5, Requirement R2, part 2.2, requires a Responsible Entity to ensure that the information is useable and is compatible with current system configurations for High Impact BES Cyber Systems or Medium Impact BES Cyber Systems at Control Centers.
Para 748 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."	FERC Order No. 706	In CIP-009-5, Requirement R1, Part 1.4 the SDT added requirements related to restoration processes based on review of the DHS Catalog of Control Systems Security: Recommendations for Standards Developers (a derivation of NIST SP800-53 for Control Systems), and requires verification initially after backup to ensure that the process completed successfully.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
	NERC Alert regarding remote access VPN vulnerabilities	Addressed in CIP-005-5 ▪ Creates basic requirements to protect critical systems from untrusted networks. ▪ Identifies protective measures that provide secure access to critical systems. ▪ Helps ensure secure practices by employees, contractors, and service vendors to minimize exploitation of vulnerabilities. ▪ Addresses questions regarding ability to audit or enforce the requirement through the design of clear measures. ▪ Significant guidance provided to address implementation options for organizations of differing sizes, capabilities, and complexity. Additional information is provided in “Guidance for Secure Interactive Remote Access” published by NERC in July 2011. Additionally, remote access is specifically required to be included in an entity’s cyber security policy. Guidance is included to assist the entity in determining what this topic in the cyber security policy should address.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 13 "The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."	Order Approving Interpretation of Reliability Standard CIP-007-2 in Docket No. RD10-3-000, March 18, 2010	CIP-007-5, Requirement R1, Part 1.2 requires Responsible Entities (for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers) to "protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media."

Project 2008-06 - Cyber Security ~~Order 706~~Order No. 706 - V5

Working Draft (September~~April~~ ~~XX,~~11, 2012) of Consideration of Issues and Directives

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 233 (Related paragraph: 25) Para 233 "The Commission continues to believe and is further persuaded by the comments that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. Moreover, we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk-Power System should be addressed in NERCs Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need	FERC ~~Order 706~~Order No. 706	In its development of CIP Version 5, the Standards Drafting Team (SDT) considered many existing cyber security frameworks. Notably, the SDT included consideration of the NIST Risk Management Framework, NIST Publication 800-53, as well as the "DHS Catalog of Control Systems Security: Recommendations for Standards Developers" in the development of its reqwuirements for cyber systems categorization and applicable requirements. ~~It is important to highlight differences between NERC's and NIST's approaches. At the root of these differences are divergent responsibilities and goals. NIST is providing standards and guidance for U.S. Federal Agencies in managing risks to their information and Systems in support of their unique missions. NERC, on the other hand, has the role of setting standards for managing risks to systems in support of a shared community mission to ensure the reliability of the BES. This difference is important because it enables the industry to develop better detail about the impacts that they need to avoid in order to achieve their mission. NIST does not enjoy this benefit, as they are providing standards to almost 200 different organizations, each with vastly different missions. The advantage that the NERC Standards enjoy enables a focus on a relatively small number of reliability services that need to be protected. This ultimately means that the NERC Standards can be more tailored and appropriate to the industry than a wholesale adoption of the NIST Risk Management Framework.~~ Four key features of the NIST Risk Management Framework were incorporated into Version 5 of NERC CIP Standards: (1) ensuring that all BES Cyber Systems associated with the Bulk Power System, based on their function, receive some level of protection, (2) customizing protection to the mission of the cyber systems subject to protection, (3) a tiered approach to security controls which specifies the level of protection appropriate for systems based upon their importance to the

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
for new CIP Reliability Standards, or as part of an assessment of NERCs performance of its responsibilities as the ERO." Para 25 "The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework. "		reliable operation of the Bulk Power System, and (4) the concept of the BES Cyber System itself. Features 2 and 3 above are tightly coupled. In the NIST Risk Management Framework, there is a concept of tailoring and scoping which allows the organization to determine which controls are applicable to their specific environment. In the NERC compliance framework, all requirements are mandatory and enforceable, and, therefore, this concept does not translate directly. As such, the customization of protections by mission is based upon the environment that the BES Cyber System supports (control center, transmission facility, generation facility) and utilizes the tiered model and the requirement applicability to provide this customization to the individual environments that together support a combined mission of Bulk Power System reliability. The NIST Security Control Catalogue in 800-53, Revision 3 and the DHS Catalog of Controls Systems Security wereas also used as a reference in addressing many of the FERC directives in Order No. 706. Additionally, the SDT includedadded members representing federal agencies and NIST, in particular, to the drafting team during the development of these CIP standards.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 and 249 Para 258 "Likewise, the ERO should consider Northern Californias suggestion that the ERO establish a formal feedback loop to assist the industry in developing policies and procedures." Para 249 "In contrast, FirstEnergy agrees that NERC should provide guidance to entities without a wide-area view, such as a generation owner or a partial generation owner, on how to approach a risk-based assessment. Likewise, Northern California suggests that NERC establish a process for informal, case-by-case consultations with responsible entities that need assistance in complying with CIP-002-1. In addition, as part of the re-examination of CIP-002-1, Northern California encourages the incorporation of a formalized feedback loop to assist the industry in developing policies and procedures."	FERC ~~Order 706~~Order No. 706	CIP-002-5 classifies BES Cyber Systems through impact thresholds, and does not use risk-based assessments performed by individual entities. CIP-002-5, Attachment 1's bright line criteria were developed in consideration of a wide area view, and it obviates the need for a formal feedback loop or a need for a wide area view by smaller entities.
Para 258 and 252	FERC ~~Order 706~~Order No. 706	Early during the development of CIP-002-5, the SDT discussed the concept of Design-Basis Threat (DBT). The SDT, in CIP-002-5, classifies BES Cyber Systems through impact

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 "As to Entergys suggestion that the ERO provide a DBT profile of potential adversaries, the ERO should consider this issue in the Reliability Standards development process." Para 252 "Entergy suggests, as an alternative approach to critical asset identification, that the ERO provide a Design-Basis Threat (DBT) a profile of the type, composition, and capabilities of an adversary that would assist the industry as a technical baseline against which to establish the proper designs, controls and processes. Entergy claims that a DBT approach would address many of the Commissions concerns regarding the risk-based methodology. For example, a DBT would focus the appropriate emphasis on the potential consequences from an outage of a critical asset. In addition, a DBT would address the Commissions concern that responsible entities will not have enough guidance in developing a risk-based methodology and not know how to identify a critical asset. Entergy contends that a DBT		thresholds, and does not use risk-based assessments performed by individual entities. ~~Having risk-based approaches to applying cyber security requirements is a worthy objective and will continue to be explored, but~~ T~~t~~he complexity and subjectivity ~~that~~involved in an entity's risk-based assessment, such as one based on DBT,~~it adds is beyond the scope of these revisions~~would run counter to the CIP-002-5 objectives of categorization based on impact defined by bright-line criteria. CIP-002-5, Attachment 1's bright line criteria uses an impact-based approach as an alternative to DBT. This approach was approved by the Commission in its ~~o~~Order No. 761 approving Version 4 of the CIP Cyber Security Standards.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
approach would provide the industry with more certainty in implementing the CIP Reliability Standards."		
Para 272 (1 of 2) "Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, **the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset.** In doing so, the ERO should consider Juniper's comments. Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data."	FERC ~~Order 706~~Order No. 706	This was completed by CIPC in the Version 3 CIP standards guidelines. The guidelines are entitled "Identifying Critical Assets" and "Identifying Critical Cyber Assets" and are available for download from www.nerc.com.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 272 (2 of 2) "Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset. In doing so, the ERO should consider Juniper's comments. **Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data."**	FERC ~~Order 706~~Order No. 706	Guidance developed for CIP-002-5 addresses situational awareness and inter-utility data exchange.
Para 285 (related paragraph: 278) Para 285 "The Commission directs the ERO to consider the comment from ISA99 Team	FERC ~~Order 706~~Order No. 706	The exclusion of Cyber Assets based on non-routable protocols has been removed from CIP-002-5, and added as an applicability ~~scoping~~ filter for requirements where: (i) the use of non-routable protocols is a mitigating factor for the vulnerabilities a requirement addresses, or~~and~~ (ii) implementation of routable protocols, when not otherwise used, would be required to comply with the requirement (e.g. malware updates, security event monitoring, and alerting, etc.).

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
[ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience].” Para 278 “ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience. In contrast, Energy Producers notes that CIP-002-1 as proposed by NERC provides that a critical cyber asset must have either routable protocols or a dial-up connection. Energy Producers states that this is a useful, objective criterion which will assist in the unambiguous identification of such assets and therefore should be retained.”		

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 296 "With regard to METC-ITC's comment, the ERO should consider in its Reliability Standards development process the suggestion that the CIP Reliability Standards require oversight by a corporate officer (or the equivalent, since some entities do not have corporate officers) rather than by a "senior manager."	FERC ~~Order 706~~Order No. 706	The requirement that the senior manager have "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" ensures that the senior manager is of the sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for Responsible Entities,~~;~~ from municipal, cooperative, federal agencies, investor-owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis. In Version 5, this is addressed in the definition of CIP Senior Manager. The SDT believes the filing for Version 2 also addressed this issue.
Para 321 " SPP and ReliabilityFirst suggest modifying CIP-002-1 to allow an entity to rely upon the assessment of another entity with interest in the matter. We believe that this is a worthwhile suggestion for the ERO to pursue and the ERO should consider this proposal in the Reliability Standards development process. We note that, even without such a provision, an entity such as a small generator operator is not foreclosed from consulting with a balancing authority or other appropriate entity with a wide-area view of the transmission system."	FERC ~~Order 706~~Order No. 706	The SDT believes that this suggestion would be applicable in a model of an entity's own risk-based methodology, where certain small entities may not benefit from a wider area view. ~~The SDT considered this suggestion, and it believes that~~ T~~t~~he change to "bright line" criteria for identifying BES Cyber Systems in CIP-002-5, along with refining the scope of certain requirements through applicability columns based on impact and connectivity characteristics, ~~addresses this concern~~no longer requires entities to use a self-defined risk-based methodology, ~~and~~which addresses this concern~~-~~.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 355 (also see paragraph 356) "The Commission believes that responsible entities would benefit from additional guidance regarding the topics and processes to address in the cyber security policy required pursuant to CIP-003-1. While commenters support the need for guidance, many are concerned about providing such guidance through a modification of the Reliability Standard. We are persuaded by these commenters. Accordingly, the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address. However, we will not dictate the form of such guidance. For example, the ERO could develop a guidance document or white paper that would be referenced in the Reliability Standard. On the other hand, if it is determined in the course of the Reliability Standards development process that specific guidance is important enough to be incorporated directly into a Requirement, this option is not foreclosed. The entities remain responsible, however, to comply with the cyber security policy pursuant to CIP-003-1."		The SDT has chosen to provide guidance to Responsible Entities through the introduction of topical areas in the requirement language that must be addressed in cyber security policies in CIP-003-5, r~~R~~equirements R1 and R2. Additionally, as directed, the SDT has provided guidance about these topical areas in the Guidelines and Technical Basis section of Reliability Standard CIP-003-5.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 376 "... the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards. In response to EEI, we believe that this clarification is needed because, for example, it is important that a responsible entity understand that exceptions that individually may be acceptable must not lead cumulatively to results that undermine compliance with the Requirements themselves."	FERC ~~Order 706~~Order No. 706	The SDT removed the CIP-003-4 requirement to document exceptions to the Cyber Security Policy. • The SDT considers this a general management issue that is not within the scope of a compliance requirement. • The SDT found no reliability basis in this requirement. • Removal of this requirement provides clarity that the only exceptions to the requirements is through the defined Technical Feasibility Exception process, where specifically allowed.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 386 "The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly. In general, the Commission agrees with commenters and believes that access to protected information should cease as soon as possible but not later than 24 hours from the time of termination for cause."	FERC ~~Order 706~~Order No. 706	To address this directive, in CIP-004-5, r~~R~~equirement R5~~7~~, Responsible Entities must revoke access to the electronic and physical locations where it stores BES Cyber System Information. This could include records, closets, substation control houses, records management systems, file shares, or other physical and logical areas under the Responsible Entity's control. The SDT specified the revocation action to be completed "-by the end of the next calendar day following the effective date and time of the termination action" to provide a more defined time threshold, following the SDT's discussion of the difficulty in defining an exact time in a termination process that typically includes multiple steps and organizations within an entity.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 397 and 398 "The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes. The Commission believes that these considerations are significant aspects of change control and configuration management that deserve express acknowledgement in the Reliability Standard. While we agree with Entergy that the NIST Security Risk Management Framework offers valuable guidance on how to deal with these matters, our concern here is that the potential problems alluded to be explicitly acknowledged. Our proposal does not speak to how these problems should be addressed. We do not believe that the changes will have burdensome consequences, but we also note that addressing any unnecessary burdens can be dealt with in the Reliability Standards development process."	FERC ~~Order 706~~Order No. 706	Two new requirements in a new standard CIP-010-1 were added to address this change: CIP-010-1, r~~R~~equirement R1 (part~~Item~~ 1.5~~4~~), requires additional testing prior to a configuration change in a test environment; ~~.~~ CIP-010-1, r~~R~~equirement R2 (part~~Item~~ 2.1), requires monitoring of the configuration of the BES Cyber System. • The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System. • Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) prior to their implementation in the production environment to aid in identifying any accidental consequences, to required cyber security controls, of the change.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 412 "The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world."	FERC ~~Order 706~~Order No. 706	The SDT addresses this through the defense in depth framework that has been designed through the full suite of revised CIP Standards. The standards address defense in depth through personnel management, systems management, and information management. The Standards are written in the perspective that the Responsible Entity is required to protect its cyber~~critical~~ systems from internal and external threat. The requirements include both preventive and detective controls. The requirements mandate appropriate vetting of personnel to minimize the risk of internal threat. They then build upon this through secure system design for internal use and remote access. These controls are further enhanced by the requirement of robust monitoring and alerting activities. Specific requirements in the identification and protection of physical and electronic security perimeters assume a default posture of "deny-by-default" to reinforce the posture of mutual distrust.
Para 433 ". . . we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard."	FERC ~~Order 706~~Order No. 706	The SDT addressed this by determining that identification of certain core training elements would be beneficial, and the identification of those core training elements that must be provided in the training program should be role based, as required in CIP-004-5, r~~R~~equirement R2.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 434 "The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets."	FERC ~~Order 706~~Order No. 706	The SDT added this as a topic for role-specific training in CIP-004-5, r~~R~~equirement R2 (p~~P~~art 2.1~~0~~). Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 435 "Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves."	FERC ~~Order 706~~Order No. 706	The SDT has considered the issue and has determined that no modifications are necessary. In practice, this training is often conducted as computer-based training (CBT), and the training is aimed at an entity's own policies. ~~As such, as long as the training material itself is adequate, which can be evaluated through the existing audit process, security trainers themselves do not need any particular or specialized training.~~ The SDT believes that assessments~~-~~ of the adequacy of the training during the compliance monitoring process implicitly evaluate~~s~~ the adequate training of the trainers or the efficacy of the training method.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 446 (1 of 2) (Review the referenced Comments) " APPA/LPPC seek **clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees.** SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees. The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."	FERC ~~Order 706~~Order No. 706	The SDT clarifies the discretion in reviewing personnel risk assessments in CIP-004-5, r~~R~~equirement R3~~4~~, by requiring the Responsible Entity to establish and document criteria for personnel risk assessments. The requirements in CIP-004-5 also provide additional detail about what type of records (whether criminal, work history, domicile, etc) a Responsible Entity must examine.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 446 (2 of 2) (Review the Referenced Comments) "APPA/LPPC seek clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees. **SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees.** The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."	FERC ~~Order 706~~Order No. 706	In CIP-004-5, r~~R~~equirement R3~~4~~, the SDT has specified that the seven-year criminal history records check must include current residence, regardless of duration,~~;~~ and ~~cover~~ include ~~at least all~~other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has~~,~~ resided for six consecutive months or more~~, resided, been employed, and/or attended school~~.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 460 "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."	FERC ~~Order 706~~Order No. 706	In CIP-004-5, r~~R~~equirement R5~~7~~, the SDT has addressed this directive by requiring initiation of the revocation of physical and interactive remote access, to be completed within 24 hours of termination, concurrent with the termination or disciplinary action (Part 5~~7~~.1), or by the end of the calendar day in cases of transfers or reassignments (Part 5~~7~~.2) for access that the Responsible Entity determines is no longer needed.. ~~In reviewing how to modify the requirement relating to transfers or reassignments, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement (Part 7.2) from NIST 800-53, Version 3, to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.~~ CIP-004-5, r~~R~~equirement R5~~7~~ (p~~P~~art 5~~7~~.4) augments the requirements in p~~P~~arts 5~~7~~.1 and 5~~7~~.2 that respond to the directive. In order to meet the immediate time frame, Entities will likely have initial revocation procedures to prevent ~~remote and~~ physical and interactive remote access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. ~~This requirement (~~Part 5~~7~~.4~~)~~ requires the Responsible Entity to complete the revocation process within ~~provides~~ the ~~additional~~ time specified (30 days)~~to review and complete the revocation process~~. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.

Project 2008-06 Cyber Security Order 706Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 464 "We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification."	FERC Order 706Order No. 706	The SDT notes that it addresses this issue in previous versions of the CIP standards. Version 2 added the requirement for a pPersonnel risk assessment prior to being granted access, and Version 3 required implementation of a visitor control program. The changes made to the requirements in Version 5 maintain and improve upon these requirements. CIP-004-5, rRequirement R45 makes clear that individuals not properly authorized for unescorted physical access will not have such access. CIP-006-5 restricts access through implementation of a visitor management program.
Para 473 "The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entitys obligations regarding vendors with access to critical cyber assets."	FERC Order 706Order No. 706	CIP-002-5, rRequirement R1 makes clear that asset owners are responsible for complying with the standards.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 476 "We direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent with the Commissions determinations above."	FERC ~~Order 706~~Order No. 706	Guidance in CIP-002-5 states that the owning Responsible Entity is responsible for complying with the CIP Cyber Security Standards. Furthermore, the guidelines and technical basis for CIP-002-5 states that where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.
Para 496 (Related: Para 503) Para 496 "The Commission adopts the CIP NOPRs proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter" Para 503 "The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures."	FERC ~~Order 706~~Order No. 706	The drafting team addresses this in CIP-005-5, r~~R~~equirement R1 (part~~Item~~ 1.5~~4~~). Per FERC Order No. 706, Paragraphs 496~~-~~ through 503, Electronic Security Perimeters (ESP~~s~~) need two distinct security measures, such that the cyber assets do not lose all perimeter protection if one measure fails or is misconfigured, in a defense-in-depth approach. The Order makes clear that this is not simple redundancy of firewalls; thus, the drafting team ~~has decided to~~ added the security ~~measure~~ requirement of malicious traffic inspection (IDS/IPS) ~~a requirement for these ESPs~~as a second security control for electronic access points for High Impact BES Cyber Systems.~~.~~ ~~The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs as a second security measure for High Impact BES Cyber Systems.~~

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 502 "The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process."	FERC ~~Order 706~~Order No. 706	The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds- the security requirement of malicious traffic inspection (IDS/IPS) as a second security control for electronic access points for High Impact BES Cyber Systems. ~~the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs as a second security measure for High Impact BES Cyber Systems.~~

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 504 (Related: Para 495) Para 504 "The ERO should consider in the Reliability Standards development process Northern Indiana's and Xcel's concerns regarding the phrase "single access point at the dial up device." Para 495 "Northern Indiana and Xcel ask the Commission to clarify or direct the ERO to clarify the phrase "single access point at the dial up device" in CIP-005-1, Requirement R1.2. Xcel asks whether this refers to the initiating device, the device at the point of termination, or both. Northern Indiana would not modify CIP-005-1, but urges that any modifications to Requirement R2 should allow continued reliance on legacy systems."	FERC ~~Order 706~~Order No. 706	The SDT has deleted the troublesome language relating to "single access point at the dial up device," and the SDT has clarified that an Electronic Security Perimeter applies to routable connectivity. CIP-005-5 also separated the requirement for dial-up connectivity, specifying in CIP-005-5, R1.4, that a Responsible Entity must perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible, on its high and medium impact BES Cyber Systems with dial-up connectivity.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 511 "The Commission adopts the CIP NOPRs proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies."	FERC ~~Order 706~~Order No. 706	CIP-005-5, r~~R~~equirement R2 has additional security requirements for remote access from the work started in the Urgent Action Revisions to CIP-005-3. One of these requirements is two-factor authentication and specific examples of two-factor authentication are provided in the ~~referenced~~ guideline referenced in the rationale for this requirement.~~.~~

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 525 "The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily…" Para 628. "Requirement R6 of CIP-007-1 does not address the frequency with which log should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly…"	FERC ~~Order 706~~Order No. 706	In CIP-007-5, r~~R~~equirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of once every 15 days.~~every two weeks.~~ CIP-007-5, r~~R~~equirement R4, combines CIP-005-4, r~~R~~equirement R5 and CIP-007-4, r~~R~~equirement R6, and addresses FERC Order No. 706's~~'s~~ directives from a system-wide perspective. The primary feedback received on this requirement from ~~the informal~~ comment periods was the vagueness of terms "security event" and "monitor."~~.~~ The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach to specify a minimum set of security event types to log and review, and allows the entity to define relevant security events ~~-~~in addition to the specified minimum. In addition, CIP-007-5, r~~R~~equirement R4, sets up parameters for the logging and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC ~~Order 706~~Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC ~~Order 706~~Order No. 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 526 (1 of 2) "... the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments.	FERC ~~Order 706~~Order No. 706	In CIP-007-5, r~~R~~equirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of once every 15 days~~every two weeks~~. (Also see response to paragraph 525).
Para 526 (2 of 2) "The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs."	FERC ~~Order 706~~Order No. 706	CIP-007-5, r~~R~~equirement R4, sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of ~~the~~ FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. (Also see response to paragraph 525).
Para 528 "The Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs."	FERC ~~Order 706~~Order No. 706	In CIP-007-5, r~~R~~equirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of ~~every two weeks~~once every 15 days. In addition, CIP-007-5, r~~R~~equirement R4, sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of ~~the~~ FERC ~~Order 706~~Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC ~~Order 706~~Order No. 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings. (Also see response to paragraph 525).

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 541 "... we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments."	FERC ~~Order 706~~Order No. 706	In CIP-010-1, r~~R~~equirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires ~~annual~~ paper assessments at least once every 15 months in the intervening years.
Para 542 "... the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems."	FERC ~~Order 706~~Order No. 706	In CIP-010-1, r~~R~~equirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires ~~annual~~ paper assessments at least once every 15 months in the intervening years.
Para 544 (1 of 2) "the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification."	FERC ~~Order 706~~Order No. 706	The SDT addresses this paragraph in CIP-010-1, r~~R~~equirement R3. • The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new Cyber Asset undergo an active vulnerability assessment. • An exception is made for specified CIP Exceptional Circumstances. • Additionally, the new requirement in CIP-010-1, r~~R~~equirement R1 (p~~P~~art 1.5) requires testing of all changes for High Impact BES Cyber Systems that deviate from the baseline configuration in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) to ensure that required security controls are not adversely affected.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 544 (2 of 2) "... we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment"	FERC ~~Order 706~~Order No. 706	The SDT has added a requirement in CIP-010-5, requirement R3 (part ~~R~~3.3), to perform an active vulnerability assessment of a new Cyber Asset in High Impact BES Cyber Systems.
Para 547 "... we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"	FERC ~~Order 706~~Order No. 706	In CIP-010-1, r~~R~~equirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires ~~annual~~ paper assessments at least once every 15 months in the intervening years.
Para 572 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."	FERC ~~Order 706~~Order No. 706	The SDT addressed this in CIP-006-5, r~~R~~equirement R1 (p~~P~~art 1.3) for High Impact BES Cyber Assets, by requiring Responsible Entities to "utilize two or more different physical access controls to collectively allow physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access."

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 581 "The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years."	FERC ~~Order 706~~Order No. 706	The SDT addressed this in CIP-006-5, r~~R~~equirement R3 (p~~P~~art 3.1) by changing the frequency to a 24-month testing cycle; after deliberation and consideration, the SDT determined that a requirement of more frequent testing (e.g., 12 months), would pose unreasonable burden for Responsible Entities with a large number of physical security perimeters dispersed over large geographic areas~~was too often~~.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 609, Sentence 5 "The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a representative system one that includes the essential equipment and adequately represents the functioning of the production system. **We therefore direct the ERO to develop requirements addressing what constitutes a representative system and to modify CIP-007-1 accordingly.** The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."	FERC ~~Order 706~~Order No. 706	The SDT has introduced the concept of a "baseline configuration" around which the change control process is based. The SDT further utilizes this "baseline configuration" to provide clarity as to what is considered a representative s~~S~~ystem as it relates to performing active vulnerability assessments in CIP-010-1.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 609, Sentence 6 "The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a representative system one that includes the essential equipment and adequately represents the functioning of the production system. We therefore direct the ERO to develop requirements addressing what constitutes a representative system and to modify CIP-007-1 accordingly. **The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."**	FERC ~~Order 706~~Order No. 706	The SDT has provided additional guidance on testing systems in the Guidelines and Technical Basis section of CIP-010-1. Furthermore, and in addition to guidance, the requirements of CIP-010-1 R1.5 and CIP-010-1 R3.2 identify a "representative system" as a system that exists in a test environment (or production environment where tests can be performed in a manner that minimizes adverse effects) that models the baseline configuration of the BES Cyber System in a production environment. This baseline configuration concept is developed by entities in CIP-010-1 R1.1 and further contains details on what constitutes a "representative system."~~.~~

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 610 "... we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above."	FERC ~~Order 706~~Order No. 706	CIP-010-1, r~~R~~equirements R1 (p~~P~~art 1.5) requires Responsible Entities to account for any additional differences between the two systems, the SDT proposes using the words similar to those directly from FERC Order No. 706, paragraph 610: "Document the differences between the test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) and the production environment including a description of the measures used to account for any differences in operation between the test and production environments."

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 611 "With respect to MidAmericans proposal that the differences between the testing and production environments only be reported when the production and test environments are established, the ERO should consider this matter in the Reliability Standards development process However, the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."	FERC ~~Order 706~~Order No. 706	The SDT has added a requirement for the Responsible Entity to, "document…the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments." The SDT has included this requirement for each test performed in the representative environment. The SDT appreciates the concern brought up by MidAmerican and believes that entities should be free to use the same documentation multiple times to provide compliance with this requirement so as to minimize the documentation overhead, but also believes that it is important for entities to give consideration to the configuration of their representative system each time a test is performed in order to ensure the validity of the test results.
Paras 622 (Related: See Paras 614 and 619) "Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere."	FERC ~~Order 706~~Order No. 706	The "acceptance of risk" language was removed in Version 2, and it has not been used in Version 5. Malicious software prevention exceptions have been placed under the TFE process since Version 2.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 622 (Related: See Paras 614 and 619) "The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above."	FERC ~~Order 706~~Order No. 706	The drafting team addressed this in CIP-007-5, r~~R~~equirement R3. The drafting team is taking the approach of making this requirement a competency-based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive. When remote access is used to connect to a BES Cyber Asset, an intermediate device is required in CIP-005-5, r~~R~~equirement R2 (p~~P~~art 2.1) and guidance is further included for the cyber security policy in CIP-003-5, Requirement R2 to maintain up-to-date anti-malware software and patch levels before initiating interactive remote access.
Para 628 "The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1."	FERC ~~Order 706~~Order No. 706	In CIP-007-5, r~~R~~equirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of once every 15 days~~two weeks~~.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 633 "The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it."	FERC ~~Order 706~~Order No. 706	The SDT addresses this directive in CIP-011-1, r~~R~~equirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from the BES Cyber Asset. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal. Additional guidance was added to the standard as further clarification: Media sanitization is generally classified into four categories: disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes. This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 635 "the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."	FERC ~~Order 706~~Order No. 706	The SDT addresses this directive in CIP-011-1, r~~R~~equirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from the BES Cyber Asset. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal. Additional guidance was added to the standard as further clarification: Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes. This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 643 (1 of 2) **"The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments**, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."	FERC ~~Order 706~~Order No. 706	In order to provide more direction on what "features, functionality, and vulnerabilities" should be addressed in a vulnerability assessment, the SDT included guidance in CIP-010-1 on active and paper vulnerability assessment. The SDT further referenced NIST SP800-115 to provide entities additional guidance on how to conduct a vulnerability assessment.
Para 643 (2 of 2) "The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, **and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."**	FERC ~~Order 706~~Order No. 706	In CIP-010-1, requirement R3 (p~~P~~art 3.4), the SDT added a requirement for an entity planned date of completion to the remediation action plan following a vulnerability assessment.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 660 (Related, See Para 661) "The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. In developing the guidance, the ERO should consider the specific examples provided by commenters, described above. However, we direct the ERO to develop and provide guidance on the term reportable incident. The Commission is not opposed to the suggestion that the ERO create a reference document containing the reporting criteria and thresholds and requiring responsible entities to comply with the reference document in the revised Reliability Standard CIP-008-1, but will allow the ERO to determine the best method to accomplish the goal of better defining reportable incident."	FERC ~~Order 706~~Order No. 706	In addition to defining the term Reportable Cyber Security Incident as one that compromises or disrupts the functional tasks of a Responsible Entity, CIP-008-5 also provides further guidance for determining a Reportable Cyber Security Incident in the "Guidelines and Technical Basis" section of the standard. The definition and guidance describe a reportable incident based on characteristics of impact to the BES, rather than enumerating threats and characteristics of malware. ~~The draft Standard EOP-004-2 provides reporting criteria for Reportable Cyber Security Incidents.~~

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 661 (Related, See Para 660) "the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."	FERC ~~Order 706~~Order No. 706	CIP-008-5 addresses the four parts of this directive as follows: 1. Added: Reportable Cyber Security Incidents include, as a minimum, any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. In turn, a Cyber Security Incident includes a malicious act or suspicious event that compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter. 2. ~~Retired~~ CIP-008-4, requirement R1 (part ~~R~~1.2~~3~~) ~~which~~ contain~~ed~~s provisions for reporting Cyber Security Incidents. ~~This is now addressed in the draft EOP-004-2, Requirement 1, Part 1.3.~~ 3. See 1, above. 4. Guidance and measurements have been developed to provide information that may be used to enhance an ~~be~~ auditable and enforceable standard.
Para 673 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC ~~Order 706~~Order No. 706	Cyber Security ~~-~~ Incident Reporting and Response Planning: ~~Retired~~ CIP-008-4, requirement R1 (part ~~R~~1.3) ~~which~~ contain~~ed~~s provisions for reporting Cyber Security Incidents to the ES-ISAC within one hour of identification, even if it is a preliminary report. ~~. This is now addressed in the draft EOP-004-2, Requirement 1, Part 1.3.~~

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 676 "The Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC ~~Order 706~~Order No. 706	~~Cyber Security - Incident Reporting and Response Planning: Retired CIP-008-4, R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in the draft EOP-004-2, Requirement 1, Part 1.3.~~ Cyber Security - Incident Reporting and Response Planning: CIP-008-4, requirement R1 (part 1.3) contains provisions for reporting Cyber Security Incidents to the ES-ISAC within one hour of identification, even if it is a preliminary report. . Cyber Security - Incident Reporting and Response Planning: CIP-008-4, requirement R1 (part 1.3) contains provisions for reporting Cyber Security Incidents to the ES-ISAC within one hour of identification, even if it is a preliminary report.
Para 686 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned."	FERC ~~Order 706~~Order No. 706	In CIP-008-5, R~~r~~equirement R3 and its parts, ~~(Parts 3.3 and 3.4)~~ the SDT includes additional specification on the update of response plan and modifies the response plan requirements to incorporate lessons learned. Maintenance of documentation of paper drills, full operational drills, and responses to actual incidents is part of the documentation required to demonstrate compliance with the security controls in CIP-008-5 and is already subject to the evidence retention requirements associated with all NERC Reliability Standards.
Para 687 (also see Footnote in Order) "In light of the comments received, the Commission clarifies that, with respect to full operational testing under CIP-008-1,	FERC ~~Order 706~~Order No. 706	CIP 008-5, -R-~~r~~equirement R2, P~~(p~~Part 2.1~~)~~ is written to allow the testing requirement to be satisfied by responding to an actual Reportable Cyber Security Incident; or with a paper drill or table top exercise; or with a full operational exercise. The reporting of Cyber Security Incidents is addressed in the ~~draft EOP-004-2, Requirement 1, Part~~

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
such testing need not require a responsible entity to remove any systems from service. The Commission understands that use of the term full operational exercise in this context can be confusing. We interpret the priority of the testing required by this provision to be that planned response actions are exercised in reference to a presumed or hypothetical incident contemplated by the cyber security response plan, and not necessarily that the presumed incident is performed on the live system. A responsible entity should assume a certain type of incident had occurred, and then ensure that its employees take what action would be required under the response plan, given the hypothetical incident. A responsible entity must ensure that it is properly identifying potential incidents as physical or cyber and contacting the appropriate government, law enforcement or industry authorities. CIP-008-1 should require a responsible entity to verify the list of entities that must be called pursuant to its cyber security incident response plan and that the contact numbers at those agencies are correct. The ERO should clarify this in the revised Reliability Standard and may use a term different than		~~1.3~~requirement R1 (part 1.2). The Guidelines and Technical Basis section of CIP-008-5 refer to operational exercises in the FEMA Homeland Security Exercise Evaluation Program as one of the following three types: drill, functional exercise, and full-scale exercise. It defines that “[a] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, emergency operation centers, etc.) and "boots on the ground" response (e.g., firefighters decontaminating mock victims).” The SDT believes the term operational exercise has become well understood and appropriate for both incident response and recovery exercises.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
full operational exercise."		
Para 694 "For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard"	FERC ~~Order 706~~Order No. 706	The SDT added in CIP-009-5, R~~r~~equirement R2, a requirement to implement the recovery plan.
Para 706 "The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard."	FERC ~~Order 706~~Order No. 706	CIP-009-5, R~~r~~equirement R1, P~~ (p~~Part 1.5~~)~~ requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service. The SDT captured the objective of this control, but did not explicitly use the term "forensics" due to the legal interpretations associated with the term.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 710 (Related: Para 706) "Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report."	FERC ~~Order 706~~Order No. 706	CIP-009-5, R~~r~~equirement R1, P~~(p~~Part 1.5~~)~~ requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service. ~~.~~
Para 725 "The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years."	FERC ~~Order 706~~Order No. 706	CIP-009-5, R~~r~~equirement R2, P~~(p~~Part 2.3~~)~~ requires an operational exercise at least once every three calendar years.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 739 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."	FERC ~~Order 706~~Order No. 706	In CIP-009-5, R~~r~~equirement R1, P~~(p~~Part 1.4~~)~~ the SDT added requirements related to restoration processes based on review of the DHS Controls, and requires verification initially after backup to ensure that the process completed successfully. In CIP-009-5, R~~r~~equirement R2, ~~(p~~Part 2.2~~)~~, requires a Responsible Entity to ensure that the information is useable and is compatible with current system configurations for~~at~~ High Impact BES Cyber Systems or Medium Impact BES Cyber Systems at Control Centers.
Para 748 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."	FERC ~~Order 706~~Order No. 706	In CIP-009-5, R~~r~~equirement R1, P~~(p~~Part 1.4~~)~~ the SDT added requirements related to restoration processes based on review of the DHS Catalog of Control Systems Security: Recommendations for Standards Developers (a derivation of NIST SP800-53 for Control Systems), and requires verification initially after backup to ensure that the process completed successfully.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
	NERC Alert regarding remote access VPN vulnerabilities	Addressed in CIP-005-5 ▪ Creates basic requirements to protect critical systems from untrusted networks. ▪ Identifies protective measures that provide secure access to critical systems. ▪ Helps ensure secure practices by employees, contractors, and service vendors to minimize exploitation of vulnerabilities. ▪ Addresses questions regarding ability to audit or enforce the requirement through the design of clear measures. ▪ Significant guidance provided to address implementation options for organizations of differing sizes, capabilities, and complexity. Additional information is provided in "Guidance for Secure Interactive Remote Access" published by NERC in July 2011. Additionally, remote access is specifically required to be included in an entity's cyber security policy. Guidance is included to assist the entity in determining what this topic in the cyber security policy should address.

Project 2008-06 Cyber Security ~~Order 706~~Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 13 "The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."	Order Approving Interpretation of Reliability Standard CIP-007-2 in Docket No. RD10-3-000, March 18, 2010	CIP-007-5, R~~r~~equirement R1, P~~(p~~Part 1.2~~)~~ requires Responsible Entities (for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers) to "protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media."

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Twelve Successive Ballot Windows Now Open for Ten Standards, Implementation Plan and Definitions **October 1-10, 2012**

Now Available

Ballot windows for 10 CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1), a set of new and revised NERC Glossary definitions, and a proposed implementation plan are open Monday, October 1 through **8 p.m. Eastern on Wednesday, October 10, 2012.**

Please note: Balloters should note that since originally posting the draft 3 documents for formal comment, the drafting time made certain specific and limited corrections to CIP-002-5, CIP-003-5, the implementation plan, and the definitions document. Each of those revised documents indicates what was corrected in a prominent, red-texted box at the beginning of the document.

CIP-002-5 requires the categorization of Bulk Electric System (BES) Cyber Systems according to bright-line criteria for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES.

CIP-003-5 through CIP-009-5, CIP-010-1 and CIP-011-1 in the draft Version 5 CIP Cyber Security Standards define the cyber security requirements to be applied to the BES Cyber Systems according to the categorization performed in CIP-002-5.

CIP-003 through CIP-009 generally follows the organization of Versions 1-4 of CIP-003 through CIP-009. CIP-010-1 is a new standard that contains the Configuration Change Management and Vulnerability Assessment requirements previously defined across several CIP standards in Versions 1 through 4. CIP-011-1 is a new standard that defines Information Protection requirements previously defined across many standards in Versions 1 through 4.

In addition, the following documents have been posted to assist stakeholders in their review:

- Consideration of Comments Reports A through D – Provides a summary of the modifications made to the proposed standards based on comments submitted during a formal comment period and successive ballots that ended May 21, 2012. Please note that because of the large volume of comments received, the Standards Committee has authorized the SDT to provide detailed summary responses to each question in lieu of providing individual responses to each

comment. Report A provides a response for CIP-002 and CIP-003, Report B provides a response for CIP-004 through CIP-007, Report C provides a response for CIP-008 through CIP-011, and Report D provides a response for the Definitions and Implementation Plan. The SDT believes that the summary responses address all of the comments received, and encourages stakeholders to carefully review the summary consideration in conjunction with the posted redlines. Mapping Document - Identifies each requirement in the already-approved Version 4 CIP standards and identifies how the requirement has been treated in the Version 5 CIP standards (which include CIP-002-5 through CIP-009-5 and CIP-010-1 and CIP-011-1).

- Clean versions of the approved versions of CIP-002-4 through CIP-009-4 - these are posted because the extent of the changes to each of the standards makes a redline of the posted draft standards against the approved standards impractical.
- Unofficial comment form in Word format
- Consideration of Issues and Directives – The consideration of issues and directives provides the FERC issues and directives related to the CIP project and the associated consideration by the drafting team.
- VRFs and VSLs for all standards – The VRFs and VSLs for all of the standards have been consolidated into one document. The VSLs are still under development and the drafting team asks voters not to make their ballot decisions for the standards on the under development VSLs. A non-binding poll of the VRFs and VSLs will be conducted with the recirculation ballots of these standards.

Additionally, CIP-006-5 was drafted in conjunction with the development of the Reliability Standard Audit Worksheet (RSAW). The parallel development of these documents provided the opportunity for the drafting team to consider the compliance implications of the language in the family of CIP standards and to offer input into the language of the RSAW. The RSAW is posted for informal comments along with the standards.

Instructions

Members of the ballot pools associated with this project may log in and submit their votes for the standards, implementation plan and definitions by clicking here.

Please read carefully: All stakeholders with comments (both members of the ballot pool as well as other stakeholders, including groups such as trade associations and committees) must submit comments through the electronic comment form. During the ballot window, balloters who wish to submit comments with their ballot *may no longer enter comments on the balloting screen*, but may still enter the comments through the electronic comment form. Balloters who wish to express support for comments submitted by another entity or group will have an opportunity to enter that information and are not required to answer any other questions.

Next Steps

The drafting team anticipates posting the CIP V5 standards for recirculation ballot in November 2012.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90-days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related issues of FERC Order No. 706.

One of the ERO's priorities is to develop a robust set of critical infrastructure reliability standards that enable the industry to adapt to continuously changing threats and vulnerabilities by emphasizing security risk management. NERC staff and industry are working together to accomplish this goal in 2012.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the

BES. These standards recognize the differing roles of each entity in the operation of the BES, the criticality and vulnerability of the cyber systems needed to support BES reliability, and the risks to which they are exposed.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Formal Comment Period Now Open: September 11, 2012 – October 10, 2012

Upcoming:

Twelve Successive Ballot Windows Open for Ten Standards, Implementation Plan and Definitions: October 1, 2012 – October 10, 2012

Now Available

Ten CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1), a set of new and revised NERC Glossary definitions, and a proposed implementation plan have been posted for a formal 30-day comment period through **8 p.m. Eastern on Wednesday, October 10, 2012**.

CIP-002-5 requires the categorization of BES Cyber Systems according to bright-line criteria for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES.

CIP-003-5 through CIP-009-5, CIP-010-1 and CIP-011-1 in the draft Version 5 CIP Cyber Security Standards define the cyber security requirements to be applied to the BES Cyber Systems according to the categorization performed in CIP-002-5.

CIP-003 through CIP-009 generally follows the organization of Versions 1-4 of CIP-003 through CIP-009. CIP-010-1 is a new standard that contains the Configuration Change Management and Vulnerability Assessment requirements previously defined across several CIP standards in Versions 1 through 4. CIP-011-1 is a new standard that defines Information Protection requirements previously defined across many standards in Versions 1 through 4.

In addition, the following documents have been posted to assist stakeholders in their review:

- Consideration of Comments Reports A through D – Provides a summary of the modifications made to the proposed standards based on comments submitted during a formal comment period and successive ballots that ended May 21, 2012. Please note that because of the large volume of comments received, the Standards Committee has authorized the SDT to provide detailed summary responses to each question in lieu of providing individual responses to each comment. Report A provides a response for CIP-002 and CIP-003, Report B provides a response for CIP-004 through CIP-007, Report C provides a response for CIP-008 through CIP-011, and Report D provides a response for the Definitions and Implementation Plan. The SDT believes

that the summary responses address all of the comments received, and encourages stakeholders to carefully review the summary consideration in conjunction with the posted redlines. Mapping Document - Identifies each requirement in the already-approved Version 4 CIP standards and identifies how the requirement has been treated in the Version 5 CIP standards (which include CIP-002-5 through CIP-009-5 and CIP-010-1 and CIP-011-1).

- Clean versions of the approved versions of CIP-002-4 through CIP-009-4 - these are posted because the extent of the changes to each of the standards makes a redline of the posted draft standards against the approved standards impractical.
- Unofficial comment form in Word format
- Consideration of Issues and Directives – The consideration of issues and directives provides the FERC issues and directives related to the CIP project and the associated consideration by the drafting team.
- VRFs and VSLs for all standards – The VRFs and VSLs for all of the standards have been consolidated into one document. The VSLs are still under development and the drafting team asks voters not to make their ballot decisions for the standards on the under development VSLs. A non-binding poll of the VRFs and VSLs will be conducted with the recirculation ballots of these standards.

Additionally, CIP-006-5 was drafted in conjunction with the development of the Reliability Standard Audit Worksheet (RSAW). The parallel development of these documents provided the opportunity for the drafting team to consider the compliance implications of the language in the family of CIP standards and to offer input into the language of the RSAW. The RSAW is posted for informal comments along with the standards.

Instructions for Commenting

A formal comment period is open through **8 p.m. Eastern on Wednesday, October 10, 2012**. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page.

The SDT believes that the industry has made a significant investment in improving the CIP Version 5 standards, and the drafting team has done its best to be responsive to all inputs, recognizing that it is not possible to adopt every suggestion and also recognizing the considerable diversity of entities and assets to which the standards will apply. Therefore, please refrain from providing duplicates of detailed comments that have already been provided in response to draft 1 and draft 2 (instead, you may simply say "See comments on draft 2"). After reviewing the revised standards and other posted documents, please limit your comments in response to this posting to those topics or issues for which you believe a change is essential and without which you would not be willing to support the standards.

Please read carefully: All stakeholders with comments (both members of the ballot pool as well as other stakeholders, including groups such as trade associations and committees) must submit comments through the electronic comment form. During the ballot window, balloters who wish to submit comments with their ballot *may no longer enter comments on the balloting screen*, but may still enter the comments through the electronic comment form. Balloters who wish to express support for comments submitted by another entity or group will have an opportunity to enter that information and are not required to answer any other questions.

Next Steps

Twelve successive ballots (one for each of the ten standards, one for the definitions, and one for the implementation plan associated with these standards) will be conducted beginning on Monday, October 1, 2012 through 8 p.m. Eastern on Wednesday, October 10, 2012.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90-days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a

Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related issues of FERC Order No. 706.

One of the ERO's priorities is to develop a robust set of critical infrastructure reliability standards that enable the industry to adapt to continuously changing threats and vulnerabilities by emphasizing security risk management. NERC staff and industry are working together to accomplish this goal in 2012.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 (CIP Version 5)

Successive Ballot Results

Now Available

Twelve successive ballot windows for the following ten CIP standards, one ballot for the associated implementation plan, and one ballot for a set of new and revised NERC Glossary definitions, closed on Wednesday, October 10, 2012. The drafting team thanks stakeholders for the careful consideration of such a large volume of documents, and for the substantive and constructive feedback received.

Voting statistics for each ballot are listed below, and the Ballot Results webpage provides a link to the detailed results.

Ballot	Results
CIP-002-5 Cyber Security — BES Cyber System Identification	Quorum: 80.58% Approval: 74.85%
CIP-003-5 Cyber Security — Security Management Controls	Quorum: 80.37% Approval: 89.50%
CIP-004-5 Cyber Security — Personnel and Training	Quorum: 80.58% Approval: 85.58%
CIP-005-5 Cyber Security — Electronic Security Perimeter(s)	Quorum: 80.58% Approval: 89.46%
CIP-006-5 Cyber Security — Physical Security	Quorum: 80.58% Approval: 92.11%
CIP-007-5 Cyber Security — Systems Security Management	Quorum: 80.58% Approval: 87.73%
CIP-008-5 Cyber Security — Incident Reporting and Response Planning	Quorum: 80.58% Approval: 91.74%
CIP-009-5 Cyber Security — Recovery Plans for BES Cyber Assets and Systems	Quorum: 80.58% Approval: 91.73%
CIP-010-1 Cyber Security — Configuration Change Management	Quorum: 80.58% Approval: 84.60%
CIP-011-1 Cyber Security — Information Protection	Quorum: 80.58% Approval: 92.90%
CIP V5 Implementation Plan	Quorum: 78.93% Approval: 94.00%
CIP V5 Definitions	Quorum: 79.13% Approval: 91.59%

Next Steps
The drafting team will consider all comments submitted, and based on the comments will determine whether to make additional changes. If the drafting team determines that no substantive changes are required to address the comments, recirculation ballots will be conducted.

Background
In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

Version 5 of the NERC CIP Cyber Security Standards is intended to address all remaining standards related issues of FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed. Additional information about the project is available on the project page.

Standards Development Process
The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 Successive Ballot CIP-002-5
Ballot Period:	10/1/2012 - 10/10/2012
Ballot Type:	Initial
Total # Votes:	390
Total Ballot Pool:	484
Quorum:	**80.58 % The Quorum has been reached**
Weighted Segment Vote:	74.85 %
Ballot Results:	**The drafting team will review comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	71	0.717	28	0.283	8	18
2 - Segment 2.	10	0.9	8	0.8	1	0.1	1	0
3 - Segment 3.	120	1	74	0.747	25	0.253	4	17
4 - Segment 4.	38	1	19	0.679	9	0.321	1	9
5 - Segment 5.	103	1	57	0.77	17	0.23	7	22
6 - Segment 6.	60	1	32	0.727	12	0.273	3	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.3	1	0.1	2	0.2	1	6
9 - Segment 9.	9	0.2	2	0.2	0	0	1	6
10 - Segment 10.	9	0.6	5	0.5	1	0.1	0	3
Totals	**484**	**7**	**269**	**5.24**	**95**	**1.76**	**26**	**94**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Negative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Abstain	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Negative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Negative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Negative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Negative	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Negative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Negative	
1	Transmission Agency of Northern California	Bryan Griess	Abstain	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	

3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Negative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Negative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Negative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Negative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Negative	

3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Negative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	
3	Snohomish County PUD No. 1	Mark Oens	Negative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Negative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza		
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	
4	Consumers Energy	David Frank Ronk		
4	Cowlitz County PUD	Rick Syring		
4	Detroit Edison Company	Daniel Herring		
4	Flathead Electric Cooperative	Russ Schneider	Negative	

4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Abstain	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Negative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette		
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Negative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Negative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		

5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Negative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Abstain	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	

6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Negative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Negative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo		
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Edward C Stein		
8		Roger C Zaklukiewicz		
8		James A Maenner		
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Negative	

8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon		
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 Successive Ballot CIP-003-5
Ballot Period:	10/1/2012 - 10/10/2012
Ballot Type:	Initial
Total # Votes:	389
Total Ballot Pool:	484
Quorum:	**80.37 % The Quorum has been reached**
Weighted Segment Vote:	89.50 %
Ballot Results:	**The drafting team will review comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	90	0.909	9	0.091	7	19
2 - Segment 2.	10	0.9	9	0.9	0	0	1	0
3 - Segment 3.	120	1	92	0.92	8	0.08	3	17
4 - Segment 4.	38	1	26	0.897	3	0.103	0	9
5 - Segment 5.	103	1	68	0.907	7	0.093	6	22
6 - Segment 6.	60	1	41	0.932	3	0.068	3	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.3	1	0.1	2	0.2	1	6
9 - Segment 9.	9	0.2	2	0.2	0	0	1	6
10 - Segment 10.	9	0.6	5	0.5	1	0.1	0	3
Totals	**484**	**7**	**334**	**6.265**	**33**	**0.735**	**22**	**95**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Negative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	

3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Negative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	

3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Negative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza		
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk		
4	Cowlitz County PUD	Rick Syring		
4	Detroit Edison Company	Daniel Herring		
4	Flathead Electric Cooperative	Russ Schneider	Negative	

4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette		
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Negative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		

5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	

6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo		
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Roger C Zaklukiewicz		
8		James A Maenner		
8		Edward C Stein		
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Negative	

8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon		
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results	
Ballot Name:	Project 2008-06 Successive Ballot CIP-004-5
Ballot Period:	10/1/2012 - 10/10/2012
Ballot Type:	Initial
Total # Votes:	390
Total Ballot Pool:	484
Quorum:	**80.58 % The Quorum has been reached**
Weighted Segment Vote:	85.58 %
Ballot Results:	**The drafting team will review comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	86	0.878	12	0.122	8	19
2 - Segment 2.	10	0.9	8	0.8	1	0.1	1	0
3 - Segment 3.	120	1	91	0.91	9	0.09	3	17
4 - Segment 4.	38	1	23	0.852	4	0.148	2	9
5 - Segment 5.	103	1	65	0.867	10	0.133	7	21
6 - Segment 6.	60	1	38	0.884	5	0.116	4	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.3	1	0.1	2	0.2	1	6
9 - Segment 9.	9	0.2	2	0.2	0	0	1	6
10 - Segment 10.	9	0.6	5	0.5	1	0.1	0	3
Totals	**484**	**7**	**319**	**5.991**	**44**	**1.009**	**27**	**94**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Negative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Abstain	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Negative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	

3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Negative	

3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza		
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk		
4	Cowlitz County PUD	Rick Syring		
4	Detroit Edison Company	Daniel Herring		
4	Flathead Electric Cooperative	Russ Schneider	Negative	

4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Negative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette		
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		

5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Abstain	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	

6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo		
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Roger C Zaklukiewicz		
8		Edward C Stein		
8		James A Maenner		
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Negative	

8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon		
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 Successive Ballot CIP-005-5
Ballot Period:	10/1/2012 - 10/10/2012
Ballot Type:	Initial
Total # Votes:	390
Total Ballot Pool:	484
Quorum:	**80.58 % The Quorum has been reached**
Weighted Segment Vote:	89.46 %
Ballot Results:	**The drafting team will review comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	88	0.88	12	0.12	6	19
2 - Segment 2.	10	0.9	9	0.9	0	0	1	0
3 - Segment 3.	120	1	93	0.921	8	0.079	2	17
4 - Segment 4.	38	1	24	0.889	3	0.111	2	9
5 - Segment 5.	103	1	68	0.883	9	0.117	5	21
6 - Segment 6.	60	1	40	0.889	5	0.111	2	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.3	1	0.1	2	0.2	1	6
9 - Segment 9.	9	0.2	2	0.2	0	0	1	6
10 - Segment 10.	9	0.6	6	0.6	0	0	0	3
Totals	**484**	**7**	**331**	**6.262**	**39**	**0.738**	**20**	**94**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Negative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Negative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	

3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	

3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza		
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk		
4	Cowlitz County PUD	Rick Syring		
4	Detroit Edison Company	Daniel Herring		
4	Flathead Electric Cooperative	Russ Schneider	Negative	

4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette		
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		

5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	

6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo		
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		James A Maenner		
8		Edward C Stein		
8		Roger C Zaklukiewicz		
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Negative	

8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon		
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 Successive Ballot CIP-006-5
Ballot Period:	10/1/2012 - 10/10/2012
Ballot Type:	Initial
Total # Votes:	390
Total Ballot Pool:	484
Quorum:	**80.58 % The Quorum has been reached**
Weighted Segment Vote:	92.11 %
Ballot Results:	**The drafting team will reveiw comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	93	0.939	6	0.061	7	19
2 - Segment 2.	10	0.9	9	0.9	0	0	1	0
3 - Segment 3.	120	1	95	0.941	6	0.059	2	17
4 - Segment 4.	38	1	24	0.889	3	0.111	2	9
5 - Segment 5.	103	1	72	0.947	4	0.053	6	21
6 - Segment 6.	60	1	41	0.932	3	0.068	3	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.3	1	0.1	2	0.2	1	6
9 - Segment 9.	9	0.2	2	0.2	0	0	1	6
10 - Segment 10.	9	0.6	6	0.6	0	0	0	3
Totals	**484**	**7**	**343**	**6.448**	**24**	**0.552**	**23**	**94**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Abstain	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	

3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	

3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza		
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk		
4	Cowlitz County PUD	Rick Syring		
4	Detroit Edison Company	Daniel Herring		
4	Flathead Electric Cooperative	Russ Schneider	Negative	

4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette		
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		

5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Abstain	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	

6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo		
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Edward C Stein		
8		Roger C Zaklukiewicz		
8		James A Maenner		
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Negative	

8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon		
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results	
Ballot Name:	Project 2008-06 Successive Ballot CIP-007-5
Ballot Period:	10/1/2012 - 10/10/2012
Ballot Type:	Initial
Total # Votes:	390
Total Ballot Pool:	484
Quorum:	**80.58 % The Quorum has been reached**
Weighted Segment Vote:	87.73 %
Ballot Results:	**The drafting team will review comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	89	0.918	8	0.082	9	19
2 - Segment 2.	10	0.9	8	0.8	1	0.1	1	0
3 - Segment 3.	120	1	92	0.92	8	0.08	3	17
4 - Segment 4.	38	1	24	0.889	3	0.111	2	9
5 - Segment 5.	103	1	68	0.907	7	0.093	7	21
6 - Segment 6.	60	1	39	0.907	4	0.093	4	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.3	1	0.1	2	0.2	1	6
9 - Segment 9.	9	0.2	2	0.2	0	0	1	6
10 - Segment 10.	9	0.6	5	0.5	1	0.1	0	3
Totals	**484**	**7**	**328**	**6.141**	**34**	**0.859**	**28**	**94**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Abstain	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	

3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	

3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza		
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk		
4	Cowlitz County PUD	Rick Syring		
4	Detroit Edison Company	Daniel Herring		
4	Flathead Electric Cooperative	Russ Schneider	Negative	

4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette		
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		

5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Abstain	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	

6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo		
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Edward C Stein		
8		Roger C Zaklukiewicz		
8		James A Maenner		
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Negative	

8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon		
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 Successive Ballot CIP-008-5
Ballot Period:	10/1/2012 - 10/10/2012
Ballot Type:	Initial
Total # Votes:	390
Total Ballot Pool:	484
Quorum:	**80.58 % The Quorum has been reached**
Weighted Segment Vote:	91.74 %
Ballot Results:	**The drafting team will reveiw comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	92	0.911	9	0.089	5	19
2 - Segment 2.	10	0.9	9	0.9	0	0	1	0
3 - Segment 3.	120	1	95	0.941	6	0.059	2	17
4 - Segment 4.	38	1	24	0.889	3	0.111	2	9
5 - Segment 5.	103	1	73	0.948	4	0.052	5	21
6 - Segment 6.	60	1	42	0.933	3	0.067	2	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.3	1	0.1	2	0.2	1	6
9 - Segment 9.	9	0.2	2	0.2	0	0	1	6
10 - Segment 10.	9	0.6	6	0.6	0	0	0	3
Totals	**484**	**7**	**344**	**6.422**	**27**	**0.578**	**19**	**94**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	

3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	

3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza		
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk		
4	Cowlitz County PUD	Rick Syring		
4	Detroit Edison Company	Daniel Herring		
4	Flathead Electric Cooperative	Russ Schneider	Negative	

4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette		
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		

5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	

6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo		
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Edward C Stein		
8		Roger C Zaklukiewicz		
8		James A Maenner		
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Negative	

8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon		
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Projectd 2008-06 Successive Ballot CIP-009-5
Ballot Period:	10/1/2012 - 10/10/2012
Ballot Type:	Initial
Total # Votes:	390
Total Ballot Pool:	484
Quorum:	**80.58 % The Quorum has been reached**
Weighted Segment Vote:	91.73 %
Ballot Results:	**The drafting team will review comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	94	0.949	5	0.051	7	19
2 - Segment 2.	10	0.9	9	0.9	0	0	1	0
3 - Segment 3.	120	1	95	0.941	6	0.059	2	17
4 - Segment 4.	38	1	23	0.852	4	0.148	2	9
5 - Segment 5.	103	1	72	0.947	4	0.053	6	21
6 - Segment 6.	60	1	41	0.932	3	0.068	3	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.3	1	0.1	2	0.2	1	6
9 - Segment 9.	9	0.2	2	0.2	0	0	1	6
10 - Segment 10.	9	0.6	6	0.6	0	0	0	3
Totals	**484**	**7**	**343**	**6.421**	**24**	**0.579**	**23**	**94**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Abstain	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	

3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	

3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza		
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk		
4	Cowlitz County PUD	Rick Syring		
4	Detroit Edison Company	Daniel Herring		
4	Flathead Electric Cooperative	Russ Schneider	Negative	

4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Negative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette		
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		

5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Abstain	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	

6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo		
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Roger C Zaklukiewicz		
8		James A Maenner		
8		Edward C Stein		
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Negative	

8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon		
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 Successive Ballot CIP-010-1
Ballot Period:	10/1/2012 - 10/10/2012
Ballot Type:	Initial
Total # Votes:	390
Total Ballot Pool:	484
Quorum:	**80.58 % The Quorum has been reached**
Weighted Segment Vote:	84.60 %
Ballot Results:	**The drafting team will review comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	85	0.876	12	0.124	9	19
2 - Segment 2.	10	0.9	8	0.8	1	0.1	1	0
3 - Segment 3.	120	1	89	0.89	11	0.11	3	17
4 - Segment 4.	38	1	23	0.852	4	0.148	2	9
5 - Segment 5.	103	1	65	0.867	10	0.133	7	21
6 - Segment 6.	60	1	36	0.837	7	0.163	4	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.3	1	0.1	2	0.2	1	6
9 - Segment 9.	9	0.2	2	0.2	0	0	1	6
10 - Segment 10.	9	0.6	5	0.5	1	0.1	0	3
Totals	**484**	**7**	**314**	**5.922**	**48**	**1.078**	**28**	**94**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Negative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Negative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Abstain	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	

3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Negative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	

3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza		
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk		
4	Cowlitz County PUD	Rick Syring		
4	Detroit Edison Company	Daniel Herring		
4	Flathead Electric Cooperative	Russ Schneider	Negative	

4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette		
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Negative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Negative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Negative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Negative	
5	Exelon Nuclear	Michael Korchynsky		

5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Abstain	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	

6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Negative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo		
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Roger C Zaklukiewicz		
8		Edward C Stein		
8		James A Maenner		
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Negative	

8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon		
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
Advanced Search GO

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 Successive Ballot CIP-011-1
Ballot Period:	10/1/2012 - 10/10/2012
Ballot Type:	Initial
Total # Votes:	390
Total Ballot Pool:	484
Quorum:	**80.58 % The Quorum has been reached**
Weighted Segment Vote:	92.90 %
Ballot Results:	**The drafting team will review comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	93	0.949	5	0.051	8	19
2 - Segment 2.	10	0.9	9	0.9	0	0	1	0
3 - Segment 3.	120	1	94	0.949	5	0.051	4	17
4 - Segment 4.	38	1	24	0.889	3	0.111	2	9
5 - Segment 5.	103	1	74	0.961	3	0.039	5	21
6 - Segment 6.	60	1	42	0.955	2	0.045	3	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.3	1	0.1	2	0.2	1	6
9 - Segment 9.	9	0.2	2	0.2	0	0	1	6
10 - Segment 10.	9	0.6	6	0.6	0	0	0	3
Totals	**484**	**7**	**345**	**6.503**	**20**	**0.497**	**25**	**94**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	

1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	

3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	

3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Abstain	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza		
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk		
4	Cowlitz County PUD	Rick Syring		
4	Detroit Edison Company	Daniel Herring		
4	Flathead Electric Cooperative	Russ Schneider	Negative	

4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette		
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Affirmative	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		

5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	

6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo		
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Edward C Stein		
8		Roger C Zaklukiewicz		
8		James A Maenner		
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Negative	

8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon		
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
GO
Advanced Search

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 Successive Ballot Implementation Plan CIPV5 Sept 2012_in
Ballot Period:	10/1/2012 - 10/10/2012
Ballot Type:	Initial
Total # Votes:	382
Total Ballot Pool:	484
Quorum:	**78.93 % The Quorum has been reached**
Weighted Segment Vote:	94.00 %
Ballot Results:	**The drafting team will review comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	88	0.957	4	0.043	14	19
2 - Segment 2.	10	0.6	6	0.6	0	0	2	2
3 - Segment 3.	120	1	93	0.959	4	0.041	6	17
4 - Segment 4.	38	1	25	1	0	0	3	10
5 - Segment 5.	103	1	65	0.942	4	0.058	9	25
6 - Segment 6.	60	1	40	0.952	2	0.048	5	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.2	1	0.1	1	0.1	1	7
9 - Segment 9.	9	0.2	2	0.2	0	0	1	6
10 - Segment 10.	9	0.5	4	0.4	1	0.1	1	3
Totals	**484**	**6.5**	**324**	**6.11**	**16**	**0.39**	**42**	**102**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	

1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Abstain	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Abstain	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Abstain	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Abstain	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		

1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Abstain	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Affirmative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Affirmative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe		
2	Southwest Power Pool, Inc.	Charles Yeung		
3	AEP	Michael E Deloach	Affirmative	

3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Abstain	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	

3	Manitoba Hydro	Greg C. Parent	Negative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Abstain	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza		
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk		
4	Cowlitz County PUD	Rick Syring		
4	Detroit Edison Company	Daniel Herring		

4	Flathead Electric Cooperative	Russ Schneider	Abstain	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Abstain	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette		
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Negative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Abstain	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono		
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Abstain	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo		
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Roger C Zaklukiewicz		
8		Edward C Stein		
8		James A Maenner		
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		

8	JDRJC Associates	Jim Cyrulewski	Negative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon		
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Newsroom • Site Map • Contact NERC

SEARCH NERC.com
GO
Advanced Search

About NERC | Standards | Compliance | Assessments & Trends | Events Analysis | Programs

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 Successive Ballot Definitions CIPV5 September 2012_in
Ballot Period:	10/1/2012 - 10/10/2012
Ballot Type:	Initial
Total # Votes:	383
Total Ballot Pool:	484
Quorum:	**79.13 % The Quorum has been reached**
Weighted Segment Vote:	91.59 %
Ballot Results:	**The drafting team will review comments received.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	88	0.926	7	0.074	11	19
2 - Segment 2.	10	0.7	7	0.7	0	0	2	1
3 - Segment 3.	120	1	91	0.938	6	0.062	6	17
4 - Segment 4.	38	1	26	0.929	2	0.071	0	10
5 - Segment 5.	103	1	64	0.914	6	0.086	8	25
6 - Segment 6.	60	1	40	0.93	3	0.07	4	13
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.2	1	0.1	1	0.1	1	7
9 - Segment 9.	9	0.2	2	0.2	0	0	1	6
10 - Segment 10.	9	0.6	5	0.5	1	0.1	0	3
Totals	**484**	**6.7**	**324**	**6.137**	**26**	**0.563**	**33**	**101**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	

1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Abstain	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Abstain	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Abstain	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam		
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald		
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		

1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Negative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike		
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles Yeung		
3	AEP	Michael E Deloach	Affirmative	

3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Abstain	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Negative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble		
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	

3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Abstain	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza		
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Negative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk		
4	Cowlitz County PUD	Rick Syring		
4	Detroit Edison Company	Daniel Herring		

4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette		
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Negative	
5	Cowlitz County PUD	Bob Essex		
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		

5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Abstain	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono		
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla		
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Abstain	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo		
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F. Lemmons		
8		Roger C Zaklukiewicz		
8		James A Maenner		
8		Edward C Stein		
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		

8	JDRJC Associates	Jim Cyrulewski	Negative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon		
8	Volkmann Consulting, Inc.	Terry Volkmann		
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas Dvorsky		
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge		
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy
404.446.2560 voice : 404.446.2595 fax
Atlanta Office: 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2012 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Individual or group. (112 Responses)
Name (84 Responses)
Organization (84 Responses)
Group Name (28 Responses)
Lead Contact (28 Responses)
Question 1 (0 Responses)
Question 1 Comments (93 Responses)
Question 2 (0 Responses)
Question 2 Comments (93 Responses)

Individual
Brian S. Millard
Tennessee Valley Authority
Please see comments provided previously for CIP Version 5 Draft II standards CIP-002-5 through CIP-011-5, definitions, and implementation plan. Draft III Comments: CIP-002-5 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-002-5 R1 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-002-5 R2 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-004-5 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-004-5 R2.2 - CIP Exceptions Circumstance clause should be removed as it applies to numerous parts and is stated at the policy level. CIP-004-5 R3 - The subrequirements are unclear due to grammar. CIP-004-5 R5 - For transfers within the organization/entity, the change of the time required to revoke access from 7 calendar days to 1 calendar day adds no reliability benefit. CIP-005-5 R2.1 - Need clarification on protections to be afforded to an "intermediate device". CIP-005-5 R2.2 - It is reasonable to include traffic between the "intermediate device" and device(s) within the ESP to be in scope of CIP, as it traverses an EAP. To include traffic that originates beyond the "intermediate device" does not afford additional protection to the systems essential to the reliable operation of the BES. CIP-006-5 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-006-5 R1.6 - The definition of PACS includes badge readers which are on the unsecured side of a PSP, and therefore access to them cannot be controlled in the manner required by R1.6. CIP-006-5 R1.7 - The definition of PACS includes badge readers which are on the unsecured side of a PSP, and therefore access to them cannot be controlled in the manner required by R1.7. CIP-006-5 R2.1 - CIP Exceptions Circumstance clause should be removed as it applies to numerous parts and is stated at the policy level. CIP-006-5 R2.2 - CIP Exceptions Circumstance clause should be removed as it applies to numerous parts and is stated at the policy level. CIP-007-5 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-007-5 R1.2 - No clarification is made regarding physical I/O ports that are externally accessible. For example, most servers have PCI slots, CPU slots, memory slots, etc, which are physical I/O ports. As the standard is currently written, it would seem organizations need to disable these ports. Additionally, the language “console commands” is too ambiguous. CIP-007-5 R2.3 - "Available actions to entities should include: 1) Apply the patches 2) Develop dated implementation plan 3) Create/revise existing mitigation plan". In many cases, patches will be applied, but outside of a 35 day period to accommodate outage schedules for optimizing reliability and availability of systems. In many cases, when an applicable patch is provided by a vendor, there may be no additional mitigation implemented during the time from patch availability until installation. Requiring entities to “create a dated mitigation plan” or “revise an existing mitigation plan” will result in a paperwork exercise and yield no reliability or security benefits for the affected cyber assets. Adding an option to “Develop dated implementation plan” without requiring a mitigation plan to be created/modified permits entities to apply resources to application of patches and optimizing reliability. CIP-007-5 R2.4 - "Available actions to entities should include: 1) Apply the patches 2) Develop dated implementation plan 3) Create/revise existing mitigation plan". In many cases, patches will be applied, but outside of a 35 day period to accommodate outage schedules for optimizing reliability and availability of systems. In many cases, when an applicable patch is provided by a vendor, there may be no additional mitigation implemented during the time from patch availability until installation. Requiring entities to “create a dated mitigation plan” or “revise an existing mitigation plan” will result in a paperwork exercise and yield no reliability or security benefits for the affected cyber assets. Adding an option to “Develop dated implementation plan” without requiring a mitigation plan to be created/modified permits entities to apply resources to application of patches and optimizing reliability. CIP-007-5 R4.1.3 - The requirement for malicious code prevention methods to log is contained in the R3.2 subrequirement. Remove requirement 4.1.3 as it is redundant. CIP-007-5 R4.2 - 4.4 - The requirements and subrequirements have become less clear than previous revisions of the CIP standards. It is unclear if R4.4 replaces the previous monitoring requirements in their

entirety, or represents an additional manual sampling action that occurs outside of a primary monitoring process which may be automated. Please consider modifying the R4.2-4 subrequirements in their entirety to make it clear to RE's which logging is required, how logs should be monitored (manual, automated, or both), and what actions are required in the event of an interruption in logging. CIP-007-5 R4.4 - It is unclear if this replaces the previous monitoring requirements in their entirety, or represents an additional manual sampling action that occurs outside of the primary monitoring process. CIP-008-5 R3.2 - Update 60 day requirement to 90 days to be consistent with R3.1. CIP-009-5 R1.5 - Need clarification - the example provided seems like it would delay the recovery process, although it is stated that data preservation should not impede recovery. CIP-009-5 R2.3 - Discrepancy regarding the time frame for testing has been identified as 12 months In the Implementation Plan for V5 CIP Cyber Security Standards-section 6, and in section 7 as 24 months- which is correct? CIP-009-5 R3.2 - Update 60 day requirement to 90 days to be consistent with R3.1. CIP-010-5 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-010-5 R1 - Inconsistent time frame for completion of configuration control activities. This introduces the possibility of confusion in completing activities required for other CIP reliability standards. CIP-010-5 R2 - Inconsistent time frame for completion of configuration control activities. This introduces the possibility of confusion in completing activities required for other CIP reliability standards. CIP-010-5 R3.2 - What is the time period for documenting results? CIP-010-5 R3.3 - An effective active vulnerability assessment may not be possible on a system prior to connecting it to its network as many of the applications that run on a device may not function outside the presence of other peripheral devices (ie, SCADA client application won't launch without SCADA Master connectivity available). Therefore, any active vulnerability assessment would probably be limited to an AV scan and account review, at most. Both of which could be effectively controlled through the use of solid imaging/deployment procedures. Modify language so that it is not required prior to adding the asset to the production environment. CIP-010-5 R3.4 - What is the time period for documenting results? CIP-011-5 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-011-5 R1.2 - Clarify "transit"; is it in regards to physical or electronic transit? Definitions: There is still no clear definition for BES Cyber System. Definition provided for EACMS is inconsistent with definitions provided in the "Background" section of the CIP 002, 004, 006, 007, 009, 010, and 011 standards.

Group

Colorado Springs Utililties

Shannon Fair

No Comments for any of the NERC CIP requirements

N/A

Group

ACES Power

Jason Marshal

(1) We thank the drafting for improvements to the draft standard. However, we still believe there is room for more improvement before voting affirmative for CIP-002-5. We are concerned that the impact of the standards on small TOPs is not commensurate with their impact on reliability and is not consistent with BA and GOP criteria. Per criteria 1.3 and 2.12, all TOP control centers and backup control centers will be either High Impact or Medium Impact regardless of how small they are. Criteria 2.11 and 2.13 establish a 1500 MW floor for GOP and BAs. Why would similar floor not be established for the TOP? Is control of generation somehow less important than control of transmission? What if the BA and TOP are the same company? We have a member that has approximately 300 MW of load in their BA and their highest transmission voltage is 161 kV for their TOP. A Medium Impact assessment of their control center simply does not reflect the minimal reliability impact that this BA has on the Bulk Electric System. (2) CIP-002-5 through CIP-011-1, Applicability sections 4.1.2.4 and 4.2.1.4: Please strike "and group of Elements" as it is redundant with Cranking Path. By definition, the Cranking Path is "a portion of electric system that can be isolated and then energized to deliver electric power from a generation source". Cranking Path will include the "group of Elements meeting the initial switching requirements". Thus, the inclusion of this language is unnecessary and will only contribute to ambiguity. Distribution Providers will be forced to question if the drafting team intended to include something above and beyond the Cranking Path. (3) CIP-00-5 R1 and associated VSLs: The requirement uses the term "assets" and the VSL uses the term "BES assets". Both the requirement and VSL should consistently use that same term. (4) CIP-002-5 R1 Part 4 and Attachment 1 Criterion 3.4: Part 4 and Criterion 3.4 need to be modified to use language consistent with the EOP-005-2, EOP-006-2, and the Applicability section 4 of the CIP-002-5 through CIP-011-1 standards. Please change "blackstart generators" to "Blackstart Resources". Also, please change "substations in the electrical path of transmission lines" to "Cranking Path". Blackstart Resources and Cranking Path have specific meanings and are consistent with other standards. Use of terms that are not defined when specifically defined terms exists creates ambiguity in the meaning of the standard. It will cause registered entities to question if something else is meant by these terms. Furthermore, "substations in the electrical path of transmission lines" would not be consistent with the Applicability section regarding Distribution Providers since they will not have transmission lines. (5) CIP-002-5 R1.1 through R1.3 and

R2.1 and R2.2: Use of sub-requirements is inconsistent with the NERC filing in which NERC committed to using numbered or bulleted lists and which was approved by the Commission on May 19, 2011. Please change accordingly. (6) CIP-002-5 R2.1: Please modify "Review (and update as needed) the identification" to "Review the identification and update it if there are changes identified". Otherwise, it implies that the registered entity is to conduct additional reviews and updates whenever there might be a change which could compel the registered entity to continuously review its identification from Requirement R1. (7) CIP-002-5 Attachment 1: Please clarify "planning horizon of more than one year". Does this mean that it occurs in the planning horizon in multiple years (i.e. 2015 and 2016) or does it mean it covers any single planning year that is at least 12 months from the operating day? The Guidelines and Technical Basis don't offer any clarification because they use slightly different language ("of one year or more"). We suggest that the drafting team consider using the term "Year One" as it provides more clarification and there really is no need to look beyond the first year of the Near-Term Transmission Planning Horizon which is also a defined term. If a generation Facility is identified beyond Year One as required to avoid an Adverse Reliability Impact per Criterion 2.3, it is entirely possible that the planning assessment will change and obviate the need for the generator to avoid the Adverse Reliability Impact. (8) CIP-002-5 Attachment 1: Please change "System" to "system" in Criterion 2.9. It is not used consistently with the NERC Glossary definition. (9) CIP-002-5 Attachment 1: Please add a qualifier to Criterion 3.1 that clarifies it only applies to BA and GOP control centers. All RC and TOP control centers will have been included in Medium and High Impact through criteria 1.1, 1.3, and 2.12. (10) CIP-002-5 Attachment 1: In criterion 2.10, please strike "or group of Elements". Use of Elements is not consistent with the NERC definition. Elements are not typically components of a control system. Use of Elements here implies they are part of the control system for automatic Load shedding. (11) In the Guidelines and Technical Basis section beginning on page 17 and ending on page 22, we continue to believe the functional entities should be removed from the reliability operating services. Many of the reliability operating services are not attributed to correct functional entities. For instance, under ability to implement load changes for demand response under the Balancing Load and Generation section is incorrectly attributed to the TOP. The TOP will have nothing to do with Demand Response as this is a market function. Please see our previous comments for more examples. (12) In the Guidelines and Technical Basis section on page 21, the Managing Constraints section inappropriately attributes ATC to managing constraints. ATC is about selling transmission service and has nothing to do managing constraints. Transmission service is a right to use the system that may never be utilized and cannot itself cause a constraint. (13) On page 25 of the Guideline and Technical Basis in the fourth paragraph, please strike "which coordinates actions necessary for the implementation of these plans by affected parties". The RRO plays no such role. The coordination is performed by the Transmission Planner or the Planning Coordinator. Furthermore, inclusion of this language before the phrase "usually in the form of a formal agreement and/or contract" makes it sound like the RRO is negotiating the contract which they are not and cannot because they are not a party to such contracts. Please also note that RRO is not an appropriate reference for Regional Entity. (14) Please reword the second sentence in the last paragraph on page 25 regarding criterion 2.9. It is a run-on sentence and its meaning is not clear. (15) CIP-003-5 is dependent upon CIP-004 through CIP-011 being approved. We are concerned with the implementation of the standard if any of the other standards do not pass. (16) While we agree that CIP-003-5 does not need to require implementation, we suggest combining the implementation of security procedures in CIP-004 through CIP-011 that have actions associated with them. (17) CIP-003-5 Requirement R1 only applies to high impact and medium impact BES Cyber Systems. The requirement or measure should clearly state that low impact BES Cyber Systems do not apply to R1. (18) CIP-003-5 Requirement R2 is confusing in regard to low impact BES Cyber Systems. There is a sentence without any requirement or sub-part assigned to it that states an inventory, list or discrete identification is not required. Are low impact systems applicable to R2? Was this sentence meant to be part of the measure? Regardless of those questions, this sentence should be written in active voice, e.g., "Low impact BES Cyber Systems or low impact BES Cyber Assets are not required to have an inventory, list, or discrete identification." This sentence is confusing and does not tie into an obvious area of R2. We suggest clearly identifying the role of low impact BES Cyber Systems and Assets and the applicability to R2. Furthermore, it is not written consistently with CIP-002-5 R1.3 which is the first instance of trying to indicate an inventory is not required for low impact BES Cyber Systems. We suggest if it is retained it should be written consistently. (19) CIP-003-5 Requirement R2, parts 2.1 through 2.4, the SDT should consider combining these sub-parts. Awareness, security controls, access, and incident response are already listed in R1, part 1.3 and, therefore, this additional requirement is potentially redundant, unnecessary, and poses a risk of double jeopardy. If a responsible entity already addresses these items in cyber security policies that address high and medium impact BES Cyber Systems per R1, it should be free to apply all or parts of these same cyber security policies to low impact BES Cyber Systems per R2. Please clarify R1 and R2 so that this potential for double jeopardy is eliminated. (20) CIP-003-5 Requirement R2, part 2.3, for low impact BES Cyber Systems, we still have concerns about the modified language, "electronic access controls for external routable protocol connections and Dial-up Connectivity." We believe that the revised language also provides too much detail for these policy topics. The modification does not support the additional language and the responsible entity is in the best position to determine how to design its low impact BES Cyber System program based on the various differences that were mentioned in the previous drafts. (21) CIP-003-5 Requirement R3, does the CIP Senior Manager need to be a different person from the "high level official" that designates the CIP Senior Manager? There are instances where the CIP Senior Manager is going to be the same person in charge of the entity's compliance program. The SDT should consider what types of changes trigger documentation – "any change" could require documentation any time that CIP Senior Manager changes their title, gets promoted, etc. Regardless of a person's

position within the company, the designation of from the high level official would also put that person in the role of CIP Senior Manager. “Any change” should be only when that person leaves the organization or is no longer in the role of CIP Senior Manager. (22) CIP-003-5 Requirement R4, why does the Responsible Entity need to implement internal controls on delegating authority? The measure does not provide examples of internal controls, it only provides the end-state – a dated document showing the delegation. We recommend reducing the amount of words in R4. It is wordy and confusing. Why not use the language in the FERC Order or the Blackout Report (“clear lines of authority and ownership for security matters”). This would include delegations of authority. R3 and R4 could be combined and internal controls are not necessary for a result-based requirement. (23) If a delegate can delegate authority to another person (as contemplated in the Guidelines and Technical Basis section), that should be made clear in the requirement itself. In the phrase, “These delegations shall be documented, including the name or title of the delegate, the specific actions delegated,…” authority for specific actions should be delegated, not the actions themselves (use “the specific actions for which authority is delegated”). (24) CIP-004-5 Requirement R1, “reinforcement” is vague, ambiguous, and opens the door to subjectivity and misinterpretation. Does the SDT intend to have a quarterly training, or a quarterly newsletter, or just a poster on the wall or an intranet posting? These are all options in CIP-004-5 Table R1. We suggest clearly defining what is intended with Requirement R1. If the SDT is planning to use internal controls for the majority of the CIP standards, the Responsible Entity should be the one to define what is appropriate for “reinforcement.” We suggest either revising the language or removing it from the standard. There are already several standards that handle training and if the objective of this requirement is to have a poster on the wall that is administrative in nature. Please do not add requirements to the CIP standards that would be subject to Paragraph 81 retirement. (25) Requirement R1 (security awareness) looks like a purely administrative requirement. The risk to the BES because a quarterly awareness bulletin was not sent would be de minimis. If this requirement remains, it should be made clear that it is not a zero defect requirement. (26) CIP-004-5 Requirement R2 should be the only requirement for CIP-004-5. If the new paradigm for NERC is to shift to internal controls, then the SDT should not have any other requirements other than the overarching R2. The Training Content in CIP-004-5 Table R2 is too prescriptive and should be moved to the measures. If the Responsible Entity must create a Cybersecurity Training program, then the Responsible Entity should be able to determine the controls that ensure proper training is delivered to the appropriate personnel. (27) CIP-004-5 Requirement R2, Table R2, Part 2.2 is needs to be modified. As it is currently written, it literally says that access cannot be granted prior to completion of training. For newly responsible entities this language would be problematic because access has already been granted to existing employees before the standard is applicable. We suggest some language should be added to clarify that the training should be completed either prior to granting access or by the time the requirement applies to the responsible entity. . (28) The original rationale for the seven-year timeline was based on the Fair Credit Reporting Act (FCRA). We do not believe that the FCRA is a sound technical justification for criminal risk assessments. We suggest the SDT modify the timeline to 10 years to align with other governmental standards and practices. (29) CIP-004-5 Requirement R4, Part 4.2, requiring a validation of authorized access each quarter is reasonable but sounds a lot like an internal control. Thus, we are confused about what constitutes internal controls and what constitutes requirements. In the rationale for R4, the SDT states that administrative and clerical errors should not be a violation, and we agree. The Responsible Entity is in the best position to determine its internal practices and controls. We strongly suggest that the SDT remove Part 4.2 from Table R4 and provide it as an example of an internal control that the CEA would expect to see. This would allow the entity to determine the proper timeline for reviews by implementing controls that are based individual facts and circumstances. (30) CIP-004-5 Compliance Section, the evidence retention for verifying access should be less than the audit cycle (which is three years for BAs and TOPs), especially if the SDT plans to keep the quarterly reviews to verify that access has been properly removed. This is another administrative burden to maintain the documentation and we suggest reducing the evidence retention period to 15 months. (31) CIP-005-5, Requirement R1, Guidelines and Technical Basis, page 20: What is the rationale for standalone networks that have no external connectivity to other networks must have a defined Electronic Security Perimeter (ESP)? The risk basis for these networks that have no external connectivity are relatively low and therefore, do not need to be included in the standard. (32) CIP-005-5, VSL R1. The language in the VSL should match the same language and logic as R2. For example, the Responsible Entity should have a low VSL for not having a sub-part in its documented process, medium for not implementing one of the applicable items, high for not implementing two applicable items and severe for not implementing three applicable items. This would result in a more consistent application throughout the standard. (33) CIP-006-5, Requirement R1, Part 1.5 and Part 1.7. Combine the two requirements by adding Physical Access Control Systems (PACS) to Part 1.5 instead of separating the three assets into two requirements and measures since they are the same. It should read: Requirement: Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter and Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection. (34) CIP-006-5, R1.9 and R2.3: These are data retention requirements and should not be requirements of the Standard (35) In CIP-007-5 Requirements 3.1 - Deploy method(s) to deter, detect, or prevent malicious code, Requirements 3.2 - Mitigate the threat of identified malicious code and Requirements 3.3 - For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns. These three requirements do not have any timeline for action. Does the auditor audit when the activity occurred and audit only that a process is created and executed as per the registered entities procedure / process? (36) CIP-007-5 R4 – Security event monitoring does not state any requirements as to when the security events (Part 4.1: Log Events

and Part 4.2: Event Alerts) are to be reviewed, escalated and mitigated. The requirements state that the BES Cyber System be configured for event monitoring and alerts. Are there any requirements for immediate action from the IT Security personnel for detected failed access attempts, failed login attempts or specific event alerts? (37) CIP-007-5, R4.3This is a data retention requirements and should not be requirements of the Standard (38) In the Guidelines and Technical Basis Section for CIP-007-5 R4, it states, "Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring." Are these references to NIST the guiding principles and documentation for the development of the RSAWs and auditing of this requirement? (39) CIP-007-5 Part 5.1 and CIP-005-5 Part 2.3 – How do these parts differ? Both appear to require authentication of Interactive Remote Access sessions. (40) CIP-008-5, R2.3: These are data retention requirements and should not be requirements of the Standard. (41) In CIP-009-5 R2.2: How does a registered entity test a representative sample of information if per R2.1 they performed a paper drill? What sample of information is appropriate to ensure that in the information is useable and is compatible with current configurations from a paper drill? (42) Removal of BES before Cyber Asset in CIP-010-1, Requirement R1, Part 1.1 has the impact of greatly expanding the requirement. By definition a Cyber Asset is any "programmable electronic device." Thus, computer systems that have absolutely no impact on the Bulk Electric System could be pulled into the requirement. We recommend not only adding BES back to Cyber Asset but also clarifying that the requirement only applies to applicable BES Cyber Assets. Thus, we suggest replacing "Cyber Asset" with "applicable BES Cyber Asset" throughout Part 1.1 and its associated measure. (43) The timeline established for CIP-010-1, Requirement R1, Part 1.3 conflicts with some of the timelines established in CIP-005-5 and CIP-007-5. For example, Part 3.3 in CIP-007-5 requires an update of "malicious code protections" at least once every 35 days. CIP-010-1 R1 Part 1.3 requires updates to the baseline configuration within 30 days which would also included updating "malicious code protections". We suggest removing CIP-005 and CIP-007 as a reference to eliminate this issue. (44) CIP-010-1, Requirement R1, Part 1.3 presents opportunities for double jeopardy by including references from CIP-005 and CIP-007. If a change to the ports configuration is made but documentation from CIP-005 and CIP-007 is not updated, CIP-010-1 R1, CIP-005 and CIP-007 could all be violated simultaneously. (45) CIP-010-1, Requirement R1, Part 1.4.1, which cross-references CIP-005 and CIP-007 is loosely written and is open to subjectivity. The determination of security controls that "could be impacted" by the change does not reference any level of probability that the controls would be impacted, so any remote possibility could subject a Responsible Entity to a potential compliance violation. We suggest modifying Part 1.4.1 to eliminate cross-referencing other standards to avoid confusion and increase the probability for impacts by the change. A possible modification could state, "Prior to the change, determine cyber security controls that have a high likelihood to be impacted by the change." (46) CIP-010-1, Requirement R1, Part 1.4 should provide an exclusion for CIP Exceptional Circumstances. (47) CIP-010-1, Requirement R2, Part 2.1, is an internal control in itself. There is no need to have the preamble in R2 of identifies, assesses and corrects deficiencies; all the requirement needs to have is the table. Does the SDT intend to have Responsible Entities have identify, assess and correct around how they identify, assess and correct changes or does the SDT want the Responsible Entity to verify the changes, not the controls? Internal controls are unnecessary in this instance because the requirement is seeking an activity that is results based. (48) CIP-010-1, Requirement R3, the timing for performing an active vulnerability assessment is confusing. Part 3.1 states 15 calendar months and Part 3.2 states at least once every 36 calendar months. We suggest keeping active vulnerability assessments to Part 3.2, or once every 36 calendar months. (49) CIP-011-1 Part1.1 and 1.2 – Please change "Methods" to "Method(s)" and "Procedures" to "Procedure(s)". This is a long-held standard that NERC has used to indicate when there might be one or more than one item. Otherwise, the Parts literally compel more than one method and procedure when one might be sufficient. (50) CIP-011-1 Part 1.3 – Part 1.3 was struck in this version and focused on the periodicity of assessing adherence to the BES Cyber Information protection program. On the one hand, it seems odd to strike this requirement when it appears to be one of the few requirements that actually focus on an internal control. On the other hand, it meets two of the criteria (i.e. administrative and periodic) identified in the Paragraph 81 project for retirement of requirements. Perhaps, NERC needs to document what they consider good periodic review for these types of requirements in another document on internal controls for the CIP standards so registered entities will know what standard they are being measure against. (51) CIP-011-1 Part 2.2 – Why is the second bullet regarding "actions taken to prevent unauthorized retrieval of BES Cyber System Information" not consistent with the first bullet of Part 2.1. It seems they should be consistent.

(1) We support the concept of internal controls and agree that finding a violation for each instance is burdensome and unreasonable and evaluating possible deficiencies is a more efficient use of resources. (2) However, located throughout v5 is this section: "Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, . . . The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements." We find that this direction implies without making it clear that a set of internal controls (Internal Controls Environment) are required in order to be in compliance. Without an Internal Controls Environment, a registered entity cannot maintain a state of compliance with the requirement. We believe that this is an unreasonable burden for those small utilities who currently do not have a large internal audit function or internal controls based upon COSO. (3) In the Fall 2012 ERO Compliance Enforcement Authority Workshop, it clearly states that an entity's Internal Control Environment is to be audited based upon the COSO Framework and control types. The inclusion to identify the control activities as per the COSO components of internal control is not a requirement, however, the enforcement and auditing of the requirements will use COSO as the determining factor for completion and appraisal of compliance. Furthermore, if COSO is to be used as the

‘industry standard’ for auditing control activities, the above training and guidance does not clearly identify what are the definitions of the components and the level of control categories acceptable for compliance. More details, guidance and training are necessary to ensure that these COSO concepts are communicated to the registered entities in order to ensure that the registered entities meets the expected controls baseline for compliance. (4) Does the focus on the registered entity’s Internal Controls Environment replace the previous Internal Compliance Program (ICP) directed by FERC and assessed using the CPAW audit template? If so, where is this documented and what are the requirements for an Internal Control Environment? Doesn’t this new approach constitute a new set of indirect requirements to be placed on the registered entity that has not gone to a ballot vote by industry? If the COSO model is used and approved, are there some deficiencies that can be accepted by the registered entity as per their individual Risk Assessment? If not, then what is the requirement and guidance for an individual Risk Assessment for assessing risk to the reliability of the bulk power system? (5) As per COSO, the Internal Controls-Integrated Framework is based upon five components for a set of financial statements, not control systems. How does NERC believe that this set of audit components and internal controls relate to control systems and their IT cyber systems? (6) In the CIP-006-5 RSAW, it identifies these types of COSO Components: Control Environment (CE), Risk Assessment (RA), Control Activity (CA), Information and Communication (IC), and Monitoring (M) with these categories; Preventive, Detective, and Corrective. The inclusion to identify the COSO components and control categories of internal control is not a requirement; however, the enforcement and auditing of the requirements will use COSO as the determining factor for completion and appraisal of compliance. If COSO is to be used as the ‘industry standard’ for auditing control activities, the requirements and RSAW guidance do not clearly identify what are the definitions of the components and the level of control categories acceptable for compliance. (7) For a controls environment to be considered ‘effective’ or strong, the registered entity must implement layers of the previous mention categories: Administrative, Technical and Physical. The minimum for an effective control is to have at least one control activity in each of the three categories: preventative, detective and corrective. The strongest controls implement all nine layers (preventative, detective, and corrective implemented by using administrative methods, technical methods, and physical methods). We believe that this is an unreasonable burden for those small utilities who currently do not have a large internal audit function or set of controls based upon COSO. (8) In CIP-006-5 RSAW, it states: “Where the CEA is to report a possible non-compliance: 1. Deficiencies that create a high risk to the reliability of the bulk power system may be reported by the CEA as a finding of possible non-compliance. The CEA is to use his/her professional judgment to determine whether this is a necessary or appropriate action. NERC’s Enforcement Team has publically stated that they are recommending that SMEs be removed from the regional audit staff and replaced with professionally certified and trained auditors; not staff with electric utility experience. How does a certified professional auditor understand the potential high risk to the reliability of the bulk power system and make that determination of possible non-compliance and how can that be consistently applied to all certified professional auditors? Is there a master list of what constitutes a potential high risk to the BES? One could decide either way that an unauthorized access to the PSP, an open port, or an improperly managed ACL list is a potential high risk to the BES. What is the threshold to a potential high risk of the bulk reliability of the BES? (9) In CIP-006-5, it states, “The CEA can expect the Responsible Entity to have maintained a list of the deficiencies it identified as presenting minimal risk to bulk electric system reliability and shall, in that list, indicate: • the date the Responsible Entity identified the deficiency and the nature of the deficiency, • how the Responsible Entity determined the risk of the deficiency, • the manner of correction, the name of the person that reviewed the completion of correction, and the date of the completion of correction.” The CIP-006-5 RSAW states that the CEA can expect the Responsible Entity to have maintained a list of deficiencies. There are no requirements explicit for a list with the bullets points listed above? Is the list subjective and how long should this ‘expected’ but not required list be kept for record keeping? Is the list to be reviewed and signed by the designated NERC CIP Manager? (10) We are concerned about the consistent evaluation of internal controls from Regional audit staff. How is NERC planning to train the Regional auditors to ensure consistency during compliance audits? There are so many possible deficiencies that could occur on a daily basis and there is not clear guidance as how the Regions will decide on what is a possible high risk to the reliability of the bulk power system. (11) We recommend the SDT provide additional information in the RSAWs to show how the Regional auditors would assess compliance with a risk and control-based standard. With the change on focus for CIP version 5 in finding errors and fixing them, how are the Regions going to determine when a PV is to be issued? The Technical Justification and the RSAW do not provide enough information for the registered entity to determine when a CIP deficiency crosses the threshold of a possible high risk to the bulk power system. (12) We recommend adding more detail, perhaps including an application guidelines section for acceptable remediation of the deficient control. What documentation would then be required? The internal controls used to remedy deficiencies could turn into another documentation exercise instead of focusing on effective cyber security. We recommend the SDT consider ways of satisfying remediation without creating an unnecessary administrative burden for maintaining compliance. (13) The Measures in the standards do not appear to reflect the internal controls approach. When the requirements use the “identifies, assesses, and corrects deficiencies” language, should the measurement reflect this language that focuses on internal controls rather than the requirement? After all it is the internal control that is to be audited rather than the requirement directly. (14) Not all of the requirements use the “identifies, assesses, and corrects deficiencies” language? For those requirements that do not use this language, will compliance monitoring focus on individual instances of non-compliance? Will a zero-defect standard be used for these? (15) There are many requirements in the standards that look like internal controls. For example, there are several requirements that require a periodic activity or evaluation of the associated process or procedure. These requirements appear to be

internal controls. This causes confusion over what exactly NERC's view of internal control is and how they will be evaluated and monitored. As a result, we think better supporting documentation for what constitutes an internal control for CIP and how those internal controls will be monitored and evaluated by auditors should be developed. Furthermore, we think the SDT needs to consider eliminating many of these requirements that appear to be internal controls. (16) The standards inconsistently use "one or more processes" language. In some standards, this language was changed simply to "processes". In other standards, this language was introduced in place of "processes". CIP-008-5 Parts 1.1 and 1.2, CIP-005-5 Part 1.5, and CIP-011-1 Parts 1.1 and 1.2are examples of inconsistencies.

Individual

Jack Stamper

Clark Public Utilities

Group

NPCC

Guy Zito

We support these 10 Standards, the Implementation Plan and the set of Definitions but have the following comments For clarification, suggest adding "mimic display" to the second paragraph of CIP-007 R5 Rationale, resulting in "Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, mimic displays etc.)." CIP-008 R1 Part 1.2 requires reporting to the ES-ISAC which may not acceptable to the Canadians. Recommend new words that are acceptable to the Canadians. For consistency, recommend changing CIP-008 R2 Part 2.1 from "at least once every calendar year, not to exceed 15 months" to "at least once every 15 calendar months" For clarity, recommend changing CIP-009 R1 Part 1.5 from "One or more processes to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), per device capability. Data preservation should not impede or restrict recovery." to "One or more processes, per device capability, to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), except where data preservation impedes or restricts recovery."

Individual

Steve Alexanderson P.E.

Central Lincoln

This draft significantly changed CIP-002 R1 and the new language is very confusing. Central Lincoln understands that per R1 and R1.1, a responsible entity must implement a process to "Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset" using assets listed in bullets 1 through 6. When we try to parse the quoted statement above into more manageable bits, we see that the process must "identify each high impact BES Cyber System at each asset" Further parsing yields "identify at each asset." Our interpretation of this language calls for the process to require the physical marking of every asset that meets one or more of the criteria 1 through 6 while also meeting one or more of the criteria 1.1 through 1.4 of Attachment 1. This is a huge change from all prior versions of CIP-002. We don't believe the SDT intended for the process to require physical marking of relevant assets, but to require the listing of the relevant assets. We suggest "Identify and list each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at the asset level," and a similar rewrite of R1.2 would more closely match the SDT's intent.

Individual

Bernard Pelletier

HQ Transenergie

CIP-008-5 R.1.2 – Notify ES-ISAC may represent a national issue for Canadian entities. Recommends rewording to be sure the center to report to is approved by federal government like "… notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) or any other entity approved by their respective federal government

Individual

Daniel Inman

Minnkota Power Cooperative, INC.

Over Comment: We don't feel as though the current wording of the CIP Version 5 standards accomplishes the intended purpose. The stated purpose is "To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES." We believe that the standard as written evaluates only the impact of a degradation to a group of Facilities instead of evaluating the degradation of a BES Cyber System. Requirements R1.1 through R1.3 specify that the BES Cyber System is to be evaluated as a high, medium, or low impact as defined by Attachment 1. Attachment 1 gives criteria for evaluating the Facility or groups of Facilities, but not for BES Cyber Systems. The BES Cyber Systems

are globally given the same impact rating as the Facility or group of Facilities. We believe that once the Facility has an impact rating assigned, each individual BES Cyber System associated with the Facility should be evaluated for its impact on the Facility and given its own impact rating equal to or lower than the Facility's overall rating. This could be done by adding an Attachment 2 which describes the criteria for rating the impact of the BES Cyber System on the Facility. CIP-002-5 Guideline and Technical Basis: Requirement R1 on Page 22, last sentence of the first paragraph is confusing; "The criteria in Attachment 1 provide a measure of the impact that the BES assets that these BES Cyber Systems support, on the reliable operation of the BES." CIP-002-5 Attachment 1 criteria 2.1: The description uses "single plant location" and "single Interconnection" in the same sentence. In some situation these items may not have the same meeting. For example, two generating units in the same plant may connect to two different substations, or two different plants could connect to the same substation. Additionally, would you add multiple generators with different interconnection facilities which connect to different parts of the same substation? Need clarification on this criterion. CIP-002-5 Attachment 1 criteria 2.3: Is the term "generation Facility" in this criterion designed to cover a single unit at a facility, or all units at a single plant or Interconnection, as described in section 2.1? CIP-002-5 Attachment 1 criteria 2.3: The guidance document makes it sound like the Planning Coordinator would make the determination whether a plant is critical, not the Transmission Planner. The guidance document should be revised to reflect the standard, which states "Planning Coordinator or Transmission Planner", implying either Entity can make the determination. CIP-002-5 Attachment 1 criteria 2.3: Is the phrase, "such as due to a Category C3 contingency" intended to provide guidance to what faults to run? Is the term "Adverse Reliability Impact" which is used in Attachment 1, meant to be the criteria for all types of contingencies? CIP-002-5 Attachment 1 criteria 2.5: We would like to see clarification on how the following items are handles: 1) is/how is a DC line counted? 2) If you have a tie between two subs that has a transformer in series, does the line receive a weighting factor (seems to per guidance)? Do you use the higher or lower voltage? Is it the same for both ends of the line? Some notes are added in guidance, but they are not sufficient. CIP-002-5 Attachment 1 criteria 2.5: From the guidance document, it was clarified that radial facilities that only provide support for "single generation facilities" would not be included. What is the definition of a "single generation facility"? Uncertain situations might include two base load turbines aggregated on one line or wind farm collector subs which have multiple sites feeding into a single high voltage collector sub? CIP-002-5 Attachment 1 criteria 2.5: From the guidance document, in the last bullet on page 27, it is not clear what the statement "In these cases" is referring to, whether the designation as a single facility or multiple facilities. CIP-002-5 Attachment 1 criteria 2.5: From the guidance document, in the last bullet on page 28. How would classification of the number of substation connections be handled if two lines are parallel between the same two subs, but one has been tapped for local, non-networked load service? CIP-002-5 Attachment 1 criteria 2.8: Based on my reading of the standard, it appears that the loss of a Transmission Facility must result in loss of ALL of the generation that comprises the generation Facilities. For example, consider two 1000 MW generators located in a single plant and therefore given a Medium Impact Rating based solely on criterion 2.1. We believe that degradation of a Transmission Facility which only resulted in the loss of one of the two units would not meet the criteria in 2.8 (unless that generator was deemed critical on its own merits as well). We would like to see emphasis added that degradation of the Transmission Facility must result in loss of ALL of the generation that was included to force a Medium Impact Rating. CIP-002-5 Attachment 1 criteria 2.9: What is an automated switching system? Can this be more specifically defined, maybe by adding it to the guidance document? We believe this term should only be included if it is given a specific definition. Also, would end-to-end tripping be included in this definition? CIP-002-5 Attachment 1 criteria 2.9: We believe the following section in the guidance document is a run-on sentence and needs revision: "Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact." We suggest inserting a period before the words "Generation Owners" if this accurately captures the intent of the SDT in drafting the language. CIP-002-5 Attachment 1 criteria 2.10: The guidance document specifies that the SDT "chose the term 'Each' to represent that the criterion applied to a discrete System or Facility". Our interpretation of this statement is that a regional UFLS program which sheds more than 300 MW and is comprised of multiple independent UFLS relays in at different substations would not be given a Medium Impact Rating at the NERC or RRO program level. An individual relay would only be given a Medium Impact Rating if that relay shed more than 300 MW by itself. Is this understanding correct? CIP-002-5 Attachment 1 criteria 2.10: The guidance document notes that the ERCOT LaaR demand response program is excluded from the 2.10 criterion. Does any load management program used to off-set resources qualify for exclusion from this criterion? If so, please include a generic statement to that effect in the guidance.

Individual

Mike Marshall

Idaho Power Company

There is general agreement with the movement of the standards away from zero tolerance to an "identify and correct" philosophy so long as checks and balances are in place and the regulator supports the apparent spirit of what the Standards Drafting Team seems to have intended. Next, Criteria 2.8 of Attachment of CIP-002-5 implies that a transmission facility providing interconnection to a generation facility is considered to be in the medium

impact category if the generation owner categorized the generation facility as medium impact. In the case where the generation is not owned by the Transmission Owner this could put the Transmission Owner at the mercy of the Generation Owners application of the standard even if the Transmission Owners facilities would not otherwise be in scope. Next, the Standards continue to exempt cyber assets associated with communications networks and data communication links between Electronic Security Perimeters. Therefore, the internet protocol network used to monitor, control, and provision communications network infrastructure owned by electric utilities are exempted. Exempting the utility owned communications infrastructure creates a cyber security issue. Next, CIP-004-5 R5.2. requires that access for employees that are reassigned or transferred be change within 24 hours. The time frame listed is difficult to comply and is unnecessarily short when the employee is remaining with the company if the transfer or reassignment was in the normal course of business and not for disciplinary reasons. Next, in CIP-006-5 R1.1. the change description in the table states that Physical Access Control System (PACS) do not need to be in a Physical Security Perimeter (PSP). Does that include everything related to PACS? This wording seems contrary to the requirement wording of CIP-006-5 R1.7 in which physical access controls are required. Further clarification is needed. Next, the CIP-007-5 R2.2. change from 30 days to 35 days is excellent. This allows utilities to manage patches monthly coinciding with vendor releases without running into issues of the requirement being less than a full month. Practically however there is no reason this shouldn't be extended to 40 days to accommodate time to review the vendor releases. However, the additional 5 days will ensure that those utilities with patch management programs are not penalized due to variations in patch release dates from month to month. Next, the CIP-010-1 R3.3. requirement seems redundant with CIP-010-1 R1.5. The entity is required to test the new device against its baseline and cyber security controls for adverse affects (under R1.5.) and then again is required to do a vulnerability assessment which again is a check (under R3.3.) against cyber security controls. This needs further clarification as to what the difference for new cyber assets under these two sub-requirements. Next, the definition of a Cyber Asset should not include the nondescript term "data" as the majority of data in the cyber asset is not related to the security of the device. This could potentially be construed as all data; including data unrelated to CIP, the device, or security and could pose great logistical challenges. Clarification of "data" or removal of the term needs to be addressed. Next, the definition of an Electronic Access Control or Monitoring Systems ("EACMS") should explicitly exclude tools for vulnerability assessments and other monitoring not associated with real-time "access" monitoring. The current wording seems to include all devices that perform monitoring functions even if they are not associated with real-time "access" monitoring. In addition, CIP-004-5 R4.2. Requires a quarterly authorization records review. It seems that this is a step backward in security and is simply a documentation check. Documentary evidence is inherent the in the standards and a documentation check does not provide additional security. Also, the CIP-007-5 R4.1.2. requirement calls out failed access attempts and failed login attempts. It is unclear as to why "failed access attempts" and "failed login attempts" are separated. Are "failed access attempts" referring to physical access attempts? Are they referring to some other form of electronic access to undermine the login process? Further clarification is needed.

Group

Snohomish County PUD

Benajmin Beberness

CIP-002-5 Comments: Snohomish County Public Utility No. 1 ("SNPD") does not support CIP-002-5 – Attachment 1, Section 2.12. SNPD does not believe that all Transmission Operator control centers not included in the High Impact Rating should be automatically included in the Median Impact Rating. SNPD understands that control centers require an appropriate level of protection for the bulk electric system and its identified components. However, SNPD urges the Standard Drafting Team (SDT) to establish appropriate levels of impact (High, Medium & Low) through the application of a 1500 MW generation and 1000 MVAr bright-line thresholds. The SDT has made reasonable changes to the treatment of small BA and GOP control centers. Corresponding changes should be made to the treatment of small TOPs. SNPD supports the American Public Power Association's ("APPA") comments and proposals for CIP-002-5 and intends to ballot negative on CIP-002-5. However, if the APPA proposal is adopted, SNPD intends to change its ballot from negative to affirmative in the recirculation ballot. CIP-005-5 comments The requirements contained within NERC CIP v5 (current draft) need to be tempered with a risk-based approach as documented in NIST SP 800-37, Rev. 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach" or DOE/OE-0003, "ELECTRICITY SUBSECTOR CYBERSECURITY RISK MANAGEMENT PROCESS," May 2012. CIP-009-5 comments 1.5 The requirement to preserve a corrupted drive or a mirror of a failed system before proceeding with recovery is not practical. A failed system is a failed system. The complexities of a system in a data center or enterprise environment may severely limit our capabilities to preserve a system in its failed state.

SNPD would like to begin with a general comment on the Critical Infrastructure Protection ("CIP") Version 5 and CIP-010 and 011 Cyber Security Standards. The purpose given for CIP-002 reads in part: "To identify and categorize the BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES". Yet this same standard mandates a Medium Impact Rating in its Impact Rating Criteria to "Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H) above" (per Attachment 1, Section 2.12). This implies that every energy control center or backup control center used to perform the obligations of a Transmission Operator is inherently necessary for the reliable operation of the BES which is not

factually correct. SNPD Control center operates a Local Network that provides a distribution function to its customers. SNPD does not control frequency, voltage schedules, or calculate Available Transfer Capability ("ATC") on a WECC rated path. The only operating functions SNPD can perform to support BES reliability is to provide data and drop load if requested by the Bonneville Power Administration (SNPD's BA and TSP). However BPA has the ability to independently island or isolate the SNPD system. Furthermore, the definition of a BES Cyber Asset definition in these Draft Standards is "A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System.". SNPD is a distribution utility that also meets the registration criteria of a Transmission Operator and does have a Control Center. However, as a Distribution utility with very small generation resources, there is nothing that the loss, compromise or misuse of its cyber systems or cyber assets could have on the reliable operation of the Bulk Electric System. The Operations Center is in place to address planned and unplanned outages and load restoration on a Local Network. The goal and main mission of the SNPD Operations Center is to ensure that customer service levels are met and safety procedures are followed. The draft criteria for Attachment 1, Section 2.12 creates an unnecessary and onerous burden to utilities such as the SNPD without providing any benefit to the reliability of the Bulk Electric System. The draft criteria for Attachment 1, Section 2.12 should be amended so that it is clear that it applies only to those entities whose operations could have an impact on the Bulk Electric System. This can be accomplished by implementing one of the APPA recommendations.

Individual

Jennifer White

Alliant Energy

Alliant Energy acknowledges the substantial work done by the Standards Drafting Team to solve the industry issues between drafts 2 and 3, and we support most of the changes. Those changes allowed an affirmative vote on all ballots. We do have additional comments, however, that we would like to submit for consideration: Alliant Energy disagrees with the removal of "annual" obligations from all the Standards. The "once every 15 month" language can lead to a perception of loosened rigor around these activities, as it will allow entities to omit the activity for a calendar year. This decreases reliability and deviates from other NERC Standards. We recommend use of the term "annual," allowing the entity to define that term within its program, or, the alternative "Once per calendar year, not to exceed 15 calendar months." CIP-003-5 R4 – This requirement should not include the "identify, assess, and correct" language, as it is a results-based requirement where deficiencies are unlikely and, if they do exist, create a lot of risk for the organization related to unauthorized signatures. Also, strike the last sentence related to a change in the delegator. If either the delegator or the delegate changes, the delegations should be reviewed/updated. CIP-010-5 R1.4 – The "guesswork" initiated by CIP-010-5 R1.4.1 does not add value. This is especially true if the only thing that must be tested by R1.4.2 is the list of controls identified with the guesswork. The entity is enticed to round down. Recommend striking 1.4.1 completely and change 1.4.2 to say "Following the change, verify that cyber security controls are not adversely affected." Keep 1.4.3. CIP-010-5 R1.5 – We do not feel that emergency change controls necessary for reliability should be a TFE if related to a CIP Exceptional Circumstance. Recommend adding that verbiage to the beginning of the requirement. Alternatively, if it is the intention of the drafting team to indicate that a TFE is necessary if an entity doesn't have a test environment for a High Impact BES Cyber System, the TFE language should be moved down into the 1.5.1 or 1.5.2 to eliminate references to a TFE for each change.

As to the Implementation Plan - the verbiage allowing ambiguity until March 31, 2014 related to Version 4 is unreasonable. The deadline for FERC approval should be moved 6 months ahead of that deadline to allow entities who have to make transitions to Version 4 to hold off on infrastructure purchases until absolutely necessary without the risk that those purchases will be made moot and wasteful should FERC approve V5 (skipping V4) in the 11th hour. Set a reasonable deadline for skipping V4.

Individual

Jim Cyrulewski

JDRJC Associates, LLC

Individual

Melissa Kurtz

US Army Corps of Engineers

Individual

Alice Ireland

Xcel Energy

1) CIP-004-5 Requirement 4.1.3 expands the scope of personnel beyond CIP and requires a need to restrict and monitor access to additional data centers for individuals with "potential" physical access to systems containing CIP Information. For CIP Information, the risk impact is low as physical damage to equipment containing electronic information doesn't have any direct impact to the operations and reliability of the BES. In the General Summary of Consideration of Comments, the SDT defines physical access as both access to hard copy data and access to

equipment used for storing electronic copies. Based off the Applicable systems definition in CIP-006-5 there is no requirement to physically protect access to electronic systems that store information so to call in physical access controls for these devices under CIP-004-5 generically, is beyond the scope of the standard. 2) For consistency, we recommend modification to CIP-004-5 R5.3 language to follow the wording in R5.1 as it relates to the timeline to remove access. 3) CIP-005 R2.1 is still unclear if a VPN is an acceptable form of remote access. 4) CIP-007 R5.6 “where technically feasible” should be removed. 5) Suggested clarification to CIP-002-5 d3, Attach. 1, 2.1: “…For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, if lost or compromised, within 15 minutes, adversely impact the reliable operation. 6) In the Guidelines and Technical Basis section for CIP-006-5 under Requirement 1, Methods to monitor physical access include: “…These alarms must provide for immediate notification to personnel responsible for response.” We would suggest this section be edited to match the requirements of CIP-006-5 R1.5 and R1.7, “within 15 minutes of unauthorized physical access. It would also be suggested that the wording about Outage records be removed from the Guidelines and Technical Basis section as the Requirement was removed.

Individual

Jonathan Appelbaum

The united illuminating Company

UI seeks clarity on several topics in the Standard to allow implementation to progress correctly. Definitions- Is an EAP a PCA?; Bes Cyber System definition uses the word logically that may be mistakenly interpreted to mean networked instead of validly grouped; Implementation – Please maintain flexibility for an entity to either move from V4 to V5 or straight to V5. CIP-005- Can a switch be divided into multiple ESPs or have one port outside the ESP provided no routing between VLANs? And For R1.5 does two distinct machines need to be utilized, one as a firewall, and one as Intrusion prevention or can it be on one device (order706A par:66) and when the EAP is segmented into multiple networks where one is LAN is critical and one is Non-critical does an IDS need to be on each network segment monitoring inbound/outbound traffic on the segment or just at the EAP monitoring inbound/outbound traffic? CIP-007 R4.4 – A manual log review is a labor intensive outdated approach. The technical guidance should allow for use of network behavior analysis or other automated review process for this requirement. CIP-008 and CIP-009 both have document update requirements which are administrative which should be considered for removal. CIP-009 in technical guidance states recovery plans are BES Cyber Information which is not true by Definition and CIP-011.

Individual

Maggy Powell

Exelon Corporation and its affiliates

Exelon appreciates the hard work and devotion of the CSO 706 drafting team. The improvements made to draft 2 represent significant progress. Thank you for your effort. Below are remaining questions and comments that we request the SDT give serious consideration for revision to the proposed suite of CIP V5 standards: GENERAL: • Internal Control Language and VRFs/VSLs– The inclusion of the language “Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, . . .”, commonly referred to as internal control language, is a dramatic change in approach taken very late in the development process of the CIP V5 standards. Exelon appreciates the SDT’s attempt to recognize that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard and that enabling corrective action over compliance burden is preferable to the pursuit of reliability. However, the newness of putting this concept into the standard language raises significant uncertainty and confusion. Unfortunately, the currently proposed VRFs and VSLs do not clarify what a violation looks like under the new approach (nor does it indicate what is not considered a violation). At the core of the confusion is how such a programmatic approach will be audited. In supporting the CIP V5 standard proposals, Exelon is taking a leap of faith that NERC leadership and staff will work diligently and collaboratively to clarify the compliance component of this language to ensure that it fulfills the supported intent and creates no added compliance burden. Exelon supports the concept, but much more work is needed to understand and support the compliance obligations and enforcement measures around the concept. • Previous versions of the CIP standards incorporated headers to group the requirements. This practice was particularly useful to internal compliance management programs that deploy data mining, report creation/generation or database building by creating a consistent framework to the standards. Please consider returning to the practice by adding the following headers to the CIP V5 standards: • CIP002-5 Cyber Asset and Cyber System Categorization • R1. Identification and Categorization • R2. Review and Approval • CIP003-5 Security Management Controls • R1. Review and Approval of BES Cyber Systems Policies • R2. BES Cyber Systems Policies • R3. Identification of Leadership • R4. Delegation of Authority • CIP-004-5 Personnel and Training • R1. Security Awareness Program • R2. Training Programs • R3. Personnel Risk Assessments • R4. Access Management • R5. Access Revocation • CIP-005-5 Electronic Security Perimeter • R1. Electronic Security Perimeter • R2. Interactive Remote Access • CIP-006-5 Physical Security of BES Cyber Systems • R1. Physical Security Plans • R2. Visitor Control Programs • R3. Maintenance and Testing of Physical Access Control Systems • CIP-007-5 Systems Security Management • R1. Ports and Services. • R2. Patch Management • R3. Malicious Code Prevention • R4. Event Monitoring • R5. System Access Controls • CIP-008-5 Incident Reporting and Response Planning • R1. CSIRP Specifications • R2. CSIRP

Implementation and Planning • R3. CSIRP Review, Update and Communication • CIP-009-5 Recovery Plans for BES Cyber Systems • R1. Recovery Plan Specifications • R2. Recovery Plan Implementation and Testing • R3. Recovery Plan Review, Update and Communication • CIP-010-1 Configuration Change Management and Vulnerability Assessment • R1. Configuration Change Management • R2. Configuration Monitoring • R3. Vulnerability Assessments (Move to CIP-007-5. Please see comment below) • CIP-011-1 Information Protection • R1. Information Protection • R2. BES Cyber Asset Reuse and Disposal (Move to CIP-010-5, R4. Please see comment below) • Guidelines and Technical Basis, all V5 standards – At first glance, beginning the Guidelines and Technical Basis with "Section 4" seems to be citing section 4 of the Guidelines portion. Consider revising the title to read: "Scope of Section 4 Applicability of the CIP Cyber Security Standards. The same revision should be made to the other CIP V5 standards that incorporate the same section. • Guidelines and Technical Basis, all V5 standards (Reminder) – For continuity and to avoid future confusion, please revise guidance to be consistent with any changes made to the standard language. • Implementation Plan (Reminder) – As with the Guidelines and Technical Basis, please confirm that the implementation plan language is consistent with any changes made to the standard language. DEFINITIONS: • BES Cyber Asset – Please consider adding acronyms as in other definitions to read ("BES CA"). • BES Cyber System – Please consider adding acronyms as in other definitions to read ("BES CS"). • BES Cyber System Information – Please consider adding acronyms as in other definitions to read ("BES CSI"). • Control Center – As previously requested, please consider revision of the Control Center definition to read "CIP Control Center." A number of other standards refer to "control center" and the term as defined in the CIP V5 proposal is inappropriate to other situations. Identifying the definition as a CIP Control Center will help prevent confusion and inappropriate application of this definition to other standards. If the drafting team is unable to revise the definition title, please clarify that this definition is not applicable to other standards that utilize reference to "control center" in the lower case. CIP-002-5: • Background – On page 9 of CIP-002-5 clean version, Remove the “Card system” reference cited for PACS since that could be confused with card readers which are excluded as locally mounted hardware or devices the definition. Further distinction may be needed. • Attachment 1 – Attachment 1, 3. Low Impact Rating - For clarity, please change the word "Section" to "Criteria" to read: "BES Cyber Systems not included in Criteria 1 or 2 above…" This is more consistent with the title of Attachment 1 as Impact Rating Criteria and avoids confusion to reference of other sections of the standard. • Attachment 1 – Attachment 1, 3. Low Impact Rating – The addition of the sub-criteria (3.1 through 3.6) is a duplicate of what is already specified in Requirement 1 and does not necessarily clarify the language. CIP-003-5: • CIP-003-5 R1.1-R1.9 (Reminder) – For continuity and to avoid future confusion, please make sure that all titles referenced in the sub-requirements are consistent with final titles in the standards and track with any changes made though the development process. • CIP-003-5, R2 – The necessity of R2.4 is not clear. More guidance is needed for low assets to determine when something is considered a Cyber Security Incident since we are not required to monitor the electronic or physical perimeters for Low Impact systems. Is this to be defined by policy or by some other means? CIP-004-5: • CIP-004-5, R5.2 – As previously noted, the treatment of transfers (employees in good standing) remains more severe than for terminations in that terminations allow 30 days to remove all access. As well, the proposed CIP-004-5 requires that entities are to remove access by the end of the next calendar day following the determination that access is no longer needed. This is a new date that would require new administrative tracking. CIP-005-5: • Guidelines and Technical Basis – The first bullet under paragraph 2 in the Requirement R1 discussion cites 'Associated Protected Cyber Assets.' Associated should be lower case as it is not part of the definition. Same correction needed in the 4th paragraph starting "For example," of the same R1 section. CIP-007-5: • CIP-007-5, R2.2 - The rationale states a 30-day time frame while the requirement states 35 days. Please revise the rationale to be consistent with the requirement language. CIP-008-5: • CIP-008-5, R1.2 – The intent of the language in R1.2 appears to be to align the hour time frame as triggered by the determination rather than identification; however, the language can more clearly express that intent. Please consider the following revision: One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), which may be only a preliminary notice, shall not exceed one hour from determination. CIP-008-5, R3 – This requirement should include the internal controls language and allow entities to implement, in a manner that identifies, assesses, and corrects deficiencies since the time needed to complete a review, process updates and notifications is really contingent upon the severity and type of event. The 90 calendar days is an administrative requirement lending itself to a programmatic, internal control. CIP-009-5: • CIP-009-5, R1 Tables – R1.5 can be worded more clearly to align the device capability with preserving data. Please consider the following revision: “One or more processes to preserve data (per device capability) for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan. Data preservation should not impede or restrict recovery.” • CIP-009-5, R1 Tables – M1.5 should be revised to match: “An example of evidence may include, but is not limited to, procedures to preserve data where the device is capable, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.” CIP-010-1: • CIP-010 R3 – This requirement addresses Vulnerability Assessments, which may more appropriately align with CIP-007 as the standard geared to mitigating vulnerabilities. Please consider relocating CIP-010 R3 to CIP-007 as either R1 or as R6. CIP-011-1: • CIP-011-5 R2 — R2 discusses BES Cyber Asset Reuse and Disposal. This activity often falls under Configuration Management. Please consider moving this requirement to CIP-010-5, R4.

Group
Lakeland Electric
Mace Hunter

Individual
Tom Bowe
PJM Interconnection, L.L.C.
Definitions--Interactive Remote Access-- has requirement within the definition. This requirement should be pulled from the definition and added to the requirement in CIP-005 R2.2. CIP-004 R3 In some situations employee history is not available/released (e.g. country of origin denies access to documentation or limitations with Juvenile record access) How to comply in such situations? CIP-005—R3.2.1 Define "applicable asset". "Applicable Cyber Asset" should be called "Applicable System" to align with wording in column "Applicable Systems". CIP-007—R1. (Rational). New term "Control Center Environment" was introduced. Could potentially have different meaning than Control Center. Clarification is requested. CIP-010—R1.1 Clear understanding could not be established on the wording "intentionally install". Clarification is requested. CIP-010 R1.4 When testing Cyber Security Access controls, CIP-005 focuses on changes to ESP access points and CIP-010 focuses on logical perimeter (excluding access points). How will configuration changes within CIP-010 impact cyber security controls within CIP-005? CIP-10 R1.5. For further understanding of the sentence "Where Technically Feasible" please provide an example of the circumstances where TFE could be filled.
Individual
Michael Moltane
ITC
ITC will be voting "Affirmative" on the CIP v5 ballots, but does have one concern we would like noted: The intent of the Critical Infrastructure standard seeks to establish an industry wide objective to identify the facilities and cyber system that is misused or rendered unavailable will adversely impact the reliable operation of the BES. The BES Cyber System Categorization currently presented under CIP V5 is undermined when excluding, by classifying as low impact rating, systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. These facilities play a major role on BES operation and are receiving exclusion from protection and security controls very well defined and in line with FERC's Order 706. This exclusion does not foster the best outcome and leaves a major security hole and risk. The technical basis and guidelines presented for CIP-002-5 are very well connected to other NERC Reliability standards and provide a very good bridge to assure clear and consistent identification of systems and facilities.
Group
Florida Power & Light
Mike O'Neil
The drafting team has done an excellent job of improving Version 5 (V5) while also addressing many of FERC's Order 706 suggestions in the face of divergent industry views and points of emphasis. NextEra Energy, Inc. (NextEra) is voting Affirmative on CIP-002-5, CIP-003-5, CIP-005-5, CIP-008-5, CIP-011-5, and Definitions, while voting to Abstain with comments with respect to CIP-004-5, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-5, and the Implementation Plan. NextEra voters will reconsider Abstain positions on these 6 items (either for another successive ballot or upon a recirculation ballot) if: (a) the zero defect fix language ("in a manner that identifies, assesses, and corrects deficiencies" (the IAC Language)), which is applicable to 66 different requirements in draft 3 of V5, is supplemented, revised and/or better clarified; and (b) the Implementation Plan is improved, both as further described below. With respect to (a), the draft RSAW for CIP-006-5 is a welcome gesture and a step in the right direction, but it is flawed, insufficient, and does not change the fact that the IAC Language used in the standard is ambiguous and untested. The IAC Language does not explicitly address the issue of whether and, if so, when internally identified and corrected deficiencies constitute violations of the standard's requirements. The proposed RSAW language regarding "deficiencies" and "self-reporting" does not adequately resolve this ambiguity; if anything, it further muddies the water. It is unclear to NextEra whether any amount of verbiage in an RSAW can cure ambiguity flowing from the standard language itself. With respect to the words chosen, by prefacing the IAC Language with the phrase "in a manner that," which is itself prefaced by the words "shall implement," the requirement has become more, not less, rhetorically prescriptive. This is a step in the wrong direction, as NextEra and others were hoping the language chosen would not be in the form of an additional command, but would simply give their cyber security staff the freedom they need to develop robust internal correction programs, especially for high-volume, periodic activities. For companies like NextEra that operate in multiple NERC regions, the prospect of inconsistent and un-coordinated compliance evaluations raises serious concerns about whether the IAC Language could be applied and utilized in different ways across the country. To prevent this vacuum of ambiguity from being filled with negative unintended consequences, NERC must find an expeditious way to modify, clarify, or at least standardize the interpretation the IAC Language. One option is the insertion of an addendum to V5 between the putative approval of draft 3 on October 10, 2012 and the final recirculation ballot that must be held before the new standard is ripe enough to forward on to the NERC BOT. Such an addendum could be narrowly focused on soliciting stakeholder input and consensus regarding ways to modify, interpret and/or clarify the IAC Language in a way that makes sense for all stakeholders. NextEra's specific suggestion for improving the IAC Language is to

strike the entire phrase, then insert a new, longer sentence fragment at the end of the current sentence: "[Each Responsible Entity shall implement one or more documented physical security plans that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan], provided that internally identified deficiencies that are documented, assessed, and corrected if necessary as determined by the Responsible Entity, shall not constitute per se violations of this R1." The generic use of the legal phrase "per se" is a potentially promising way of addressing the violation issue directly in the standard itself. With more explicit, robust language in the standard, it would be easier for industry and NERC to facilitate a broader shift to risk-based auditing based on internal controls. To that end, in addition to changes to the standard itself, NextEra supports the following RSAW language for CIP standards with IAC Language: "Where the entity is identifying, assessing, and correcting its own deficiencies, the entity is satisfactorily performing the requirement." Also please consider this language for the RSAWs: "R1 Absent a possible violation that resulted in (or could have resulted in) a significant risk to the Bulk Electric System, no violation of R1 and its subrequirements shall be found, provided that the Responsible Entity has implemented a process for identifying, assessing, and correcting deficiencies with adherence to the items specified in Requirement R1." Moving to a new topic, item (b) above, NextEra has voted to Abstain with respect to the Implementation Plan for the following reasons. The Implementation Plan fails to specifically say that NERC will ask FERC to suspend the April 1, 2014 effective date for Version 4 (V4) when it submits V5 for FERC approval prior to March 31, 2012. Without suspension of the V4 effective date, NextEra is among those that will be forced to follow a parallel and costly approach to sustaining compliance to Version 3, implementing V4 by April 1, 2014 for newly identified Critical Assets, and implementing V5, which eliminates the term Critical Assets, for its presumed effective date of July 1, 2015. The current plan is a recipe for costly stranded costs that do not improve reliability. The drafting team can and should address this important problem in the Implementation Plan. Alternatively, NERC can and should ask FERC to move quickly to approve V5 once it is submitted for approval, or at least move quickly to suspend the effectiveness of V4 pending FERC's review of V5. In addition, NextEra believes the line between planned and unplanned changes is not always easy to maintain and there may be times it is appropriate to let a planned change become fully compliant at some time after the cyber system is commissioned. Similarly, after initial implementation of V5, there is an inadequate amount of time allotted for the implementation of the V5 Standards for BES Cyber Systems that go from the "Low" to "Medium" or "High" impact categorization based on unplanned enhancements and improvements to facilities. Responsible entities should be given 18-24 months, not merely 12 months, to comply, as many of the compliance activities can only be accomplished during planned outages at generation facilities. NextEra also finds the section on Initial Performance of Certain Periodic Requirements to be confusing and unnecessary and urges the drafting team to strike it or qualify these timing recommendations as proposed guidance, rather than a mandatory directive for all Responsible Entities to follow. If the section must remain, NextEra suggests it allow for an alternative timing option for periodic requirements that pegs all of the V5 requirements to the Effective Date and lets the Responsible Entity begin meeting the periodic items as they arise naturally in accordance with the CIP standards' periodic requirements.
NextEra thanks the drafting team for its hard work and the improvements it has made to Version 5.
Individual
David Rivera
New York Power Authority
Individual
Greg LeGrave
Wisconsin Public Service Corporation
Concern regarding Implementation Plan: WPS is seeking clarification regarding the NERC Implementation Plan and how 2015 audits will be conducted with regards to Version 3 and Version 5 of these standards. It is important that registered entities understand these details during this year of significant transition.
Individual
Kirit Shah
Ameren
None
(1)Replace undefined term "adversely impact" with "Adverse Reliability Impact" throughout the standard and definitions document to be consistent with the defined term in the NERC Glossary. (2)The "within 15 minute time frame" included in the definition of BES Cyber Assets is problematic to provide evidence during the audit. Add some examples, in the Guidance Document, of BES Cyber Assets that would create an Adverse Reliability Impact within 15 minutes. (3)The time frames to revoke access are still problematic considering the risk to the BPS. For a transfer, when an employee is still in a good standing and is still employed, why must an access be removed by the end of the next calendar day? Keep it at 7 days. (4)Provide guidance on how to comply with CIP-007 requirements on Medium BES Cyber Systems serial connected devices; (patching, anti-virus, etc. on large number of programmable protective relays); why other measures implemented for substation assets, such as, physical protection, are not adequate? (5)Include example diagrams, in CIP-002, page 27, to provide guidance application of each bullet in criterion 2.5. (6)Flowchart in CIP-002, page 32, is confusing and may belong with other CIP standards.

Individual
Michelle D'Antuono
Occidental Energy Ventures Corp.
Occidental Energy Ventures Corp. (OEVC) would like to point out that CIP-002-5, Attachment 1, Item 1.4, would require that a 1500 MW GOP Control Center take on a High impact rating, while the rest of the Facility is Medium impact. Even if the criterion is intended to apply to multiple locations, we believe that the aggregated generation should be 3000 MW or greater – consistent with the risk level assigned to a BA Control Center.
OEVC is greatly supportive of the RSAWs being developed concurrently with the CIP standards. However, we would like to see all ten RSAWs – as the enforcement of the risk-based language introduced in many of the Draft 3 requirements is critical to our acceptance. In particular, we are concerned that if CEAs simply continue to evaluate compliance using historical auditing techniques, the impact to our resources (and theirs) will not change. Unfortunately, the posted RSAW for CIP-006-5 only reinforces our belief that a "business-as-usual" approach has been taken. OEVC saw nothing in the RSAWs indicating a sensitivity to cost/benefit or that some risk is to be expected. In fact, we mostly see a rehash of the language in the standard itself, which is not helpful. A specific item that we believe deserves far more consideration is CIP-003-5, R2. In our view, there is too much leeway for CEAs to interpret the associated measure for the four cyber policies that all Responsible Entities must implement. It only points out the types of documents or other records that serve as proof of compliance. (No RSAW has been provided, but if it follows the pattern of the one posted for CIP-006-5, it will have the same issue.) OEVC believes that in order to eliminate any ambiguity which will serve to incentivize the development of CANs or other interpretive enforcement documents at a later date, guidance must be provided on the expectations for evidence of implementation "in a manner that identifies, assesses, and corrects deficiencies, calls for processes to be continually monitored, gaps identified, and deficiencies corrected." The "Guidelines and Technical Basis" section of CIP-003-5 has some good examples of acceptable policy CONTENT – and which could be easily incorporated in the measures and the RSAWs.
Group
PNGC Group Comments
Ron Sporseen
Group
Dominion
Greg Dodson
Certain 'periodic' requirements identified within draft 3 don't include the "zero-defect" language nor relief under CIP Exceptional Circumstances. While a Registered Entity is expected to comply with CIP requirements if at all possible during a CIP Exceptional Circumstance, we do not believe Registered Entities should be burdened with self-reports associated with identified instances of non-compliance caused directly by a CIP Exceptional Circumstance. Although the timing of the execution of 'periodic' requirements can be scheduled, the timing of CIP Exceptional Circumstances is inherently unknown and can conceivably overlap the timing of scheduled periodic requirements in such a way as to put a Registered Entity out of compliance with those requirements. We believe it's in the best interest of the reliability of the BES to record and track these instances of non-compliance as part of the process of bringing the affected BES Assets back into compliance rather than through a self-report process. Definitions (Suggested language changes for clarity): - Cyber Assets FROM: Programmable electronic devices including the hardware, software, and data in those devices. TO: Entity programmable electronic devices. RATIONAL: Simplicity. There's no need to include hardware, software, and data as this is understood and redundant. - Cyber Security Incident FROM: A malicious act or suspicious event that: - Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or, - Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System. TO: A malicious act or suspicious event that: - Compromises the Electronic Security Perimeter or Physical Security Perimeter or, - Disrupts the operation of a BES Cyber System. RATIONAL: The current definition is too broad and could be construed to require a review of single instances of erroneous network traffic (such as a mistyped URL). - Electronic Access Control or Monitoring Systems ("EACMs") FROM: Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Devices. TO: Cyber Assets that perform electronic access control or electronic access monitoring of Electronic Access Points. This includes Intermediate Devices. RATIONAL: The language in the definition is unnecessarily broad and pulls in devices other than those that are electronic access points into the ESP. - Physical Security Perimeter ("PSP") FROM: The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside, and for which access is controlled. TO: The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled. RATIONAL: Conforming language to use EACMs CIP-002-5 R1.1 and R1.2: For clarity, change the language of requirements R1.1 and R1.2 to correlate the asset being referred to in the sentence as one of the 6 asset classes identified in the main part of the requirement. The suggested language is "R1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, which are located at each asset in the list above; R1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, which are located at each asset in the list above; and" CIP-003-5: A clarification should be added to the Guidelines and Technical Basis section of CIP-003-5 for R1 to ensure Registered Entities and Compliance

Enforcement Agencies understand that a policy to demonstrate compliance with CIP-003 R1 isn't necessary if the Registered Entity doesn't have high impact and medium impact BES Cyber Systems. This clarification is needed to provide guidance to Registered Entities for determining when policies are and aren't needed. CIP-004-5: Given the lower Violation Risk Factor, R1 should include the "zero-defect" language to eliminate the possibility of a Registered Entity having to self-report under Part 1.1 as a result of a declared CIP Exceptional Circumstance. It's conceivable that a Registered Entity that has a major disruption coincident with the timing of when a periodic activity is due, a Registered Entity may miss performing quarterly security awareness reinforcement. The language of R1 should be changed to, "Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program." CIP-005-5: For clarity, part 2.2 should allow encryption to terminate at a firewall that protects an intermediate device in addition to the intermediate device itself. Part 2.2 should be rewritten to state "For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate Device or the firewall protecting the Intermediate Device." CIP-006-5: - Parts 1.5 and 1.7 include the term "BES Cyber Security Incident Response Plan" which is not a NERC defined term. Additionally, Parts 1.5 and 1.7 as written will have an unintended consequence of requiring Registered Entities to over-respond to instances of detected unauthorized access. The Parts incorrectly assume a one-to-one relationship such that events of detected unauthorized access on a physical security plan must also be investigated under the cyber incident response plan. Within the context of a physical security plan, a cyber incident response is triggered by the subset of detected events of unauthorized access that, upon the initial investigation phase of the physical security team, identify the possibility of a cyber breach. Cyber incident response teams are not typically contacted regarding all events of detected unauthorized physical security breaches and are dependent upon the physical security team to investigate and evaluate the circumstances behind the alarm. The requirement to notify the members identified on the cyber incident response plan of all alarms associated with "detected unauthorized access" prior to investigation by the physical security team is unnecessary and overly burdensome. The language of Part 1.5 should be changed to, "Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the physical security plan within 15 minutes of detection." The language of Part 1.7 should be changed to, "Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the physical security plan within 15 minutes of detection." The change recommended for Part 1.7 makes it consistent with Part 1.5 and in that an alarm or alert can only be generated based on a known detected event. - Given the lower Violation Risk Factor, R3 should include the "zero-defect" language to eliminate the possibility of a Registered Entity having to self-report under Part 3.1 as a result of a declared CIP Exceptional Circumstance. It's conceivable that a Registered Entity that has a major disruption coincident with the timing of when a periodic activity is due, a Registered Entity may appropriately miss the testing of locally mounted hardware or devices associated with a Physical Security Perimeter affected by the CIP Exceptional Circumstance on the 24 month cycle in deference to activities that restore the normal operation of the Bulk Electric System. The language of R3 should be changed to, "Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program." CIP-007-5: The TFE language of Part R5.6 is unnecessary given the ability to use either technical or procedural controls for enforcement. Additionally, the "per Cyber Asset capability" language used in Part 5.4 should be incorporated into Part 5.6 for consistency. The language of Part 5.6 should be clarified as follows "For password-only authentication for interactive user access, technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months." CIP-008-5: - Given the lower Violation Risk Factor, R2 should include the "zero-defect" language to eliminate the possibility of a Registered Entity having to self-report under Part 2.1 as a result of a declared CIP Exceptional Circumstance. It's conceivable that a Registered Entity that has a major disruption coincident with the timing of when a periodic activity is due, a Registered Entity may appropriately miss the testing of a Cyber Security Incident Response Plan on the 15 month cycle in deference to activities that restore the normal operation of the Bulk Electric System. The language of R2 should be changed to, "Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing." - Given the lower Violation Risk Factor, R3 should include the "zero-defect" language to eliminate the possibility of a Registered Entity having to self-report under Parts 3.1 and 3.2 as a result of a declared CIP Exceptional Circumstance. It's conceivable that a Registered Entity that has a major disruption coincident with the timing of when a periodic activity is due, a Registered Entity may appropriately miss 1) updating a Cyber Security Incident Response Plan within 90 calendar days of testing the plan (or an actual incident) or 2) updating the Cyber Security Incident Response Plan within 60 calendar days of identifying changes that may be required to execute the plan in deference to activities that restore the normal operation of the Bulk Electric System. The language of R3 should be changed to, "Each Responsible Entity shall maintain, in a manner that identifies, assesses, and corrects deficiencies, each of its Cyber Security Incident response plans according to each of the applicable items in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication." CIP-009-5: Given the lower Violation Risk Factor, R3 should include the "zero-defect" language to eliminate the possibility of a Registered Entity having to self-report under Parts 3.1 and 3.2 as a result of a declared CIP Exceptional Circumstance. It's conceivable that a Registered Entity that has a major disruption coincident with the timing of

when a periodic activity is due, a Registered Entity may appropriately miss 1) updating a recovery plan within 90 calendar days of testing the plan (or an actual recovery) or 2) updating the recovery plan within 60 calendar days of identifying changes that may be required to execute the plan in deference to activities that restore the normal operation of the Bulk Electric System. The language of R3 should be changed to, “Each Responsible Entity shall maintain, in a manner that identifies, assesses, and corrects deficiencies, each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.” CIP-010-5: No Comments CIP-011-5: No Comments

Individual

Nathan Mitchell

American Public Power Association

APPA does not believe that the SDT’s response to comments fully addressed the substantive concerns we raised in comments on the prior draft with respect to the applicability of CIP-002-5 to the control centers of Transmission Operators. Numerous public power and cooperative owned utilities pointed out in comments to CIP V5 draft 2 standards, that the TOP Control Center Applicability thresholds needed to be addressed in draft 3. Small responsible entities with control centers that do not control significant BES facilities should be subject to the low impact tier of the CIP Version 5 Reliability Standards. The Standard Drafting Team (SDT) has made reasonable changes to the treatment of small BA and GOP control centers. Corresponding changes should be made to the applicability to small TOPs. APPA provided the following comments on the draft 2 standards: APPA believes that Criterion 2.11 in Attachment 1 should at a minimum designate control centers with control of less than 300 MW of resources as Low Impact. This will clearly define a lower threshold as requested for in 2.10 above and reduce the burden of compliance for small entities. The BA and GOP medium impact thresholds were changed to 1500 MW, but the CIP Standard Drafting Team (SDT) was not able to come to consensus on a threshold that would properly differentiate between Medium and Low Impact for TOP Control Centers. APPA still believes that small TOP Control Centers that control Low Impact Transmission Facilities should not be included in the Medium Impact category. APPA offers the following recommended modification to Criterion 2.12 to address this inconsistent treatment of small TOP control centers: SDT Proposed Criterion 2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above. APPA Recommendation for Criterion 2.12: Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above that performs the functional obligations of the Transmission Operator for 3 or more transmission lines operating between 200kV and 299kV. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in Criteria 2.12 would be designated as Low Impact Rational: CIP Version 4 uses the bright line of 3 or more transmission lines operating at 300kV or above in criterion 1.7. From the weighted table in the draft 3 criterion 2.5, this would give a threshold of 1400 MVA between a Medium and Low Impact. The SDT acknowledges that transmission Facilities below 200kV are not applicable in the Medium Impact category. So it stands to reason that Control Centers that perform the functional obligations of the Transmission Operator for Low Impact Facilities should be designated as Low Impact. A threshold of three or more Transmission lines operating at over 200 kV and all Transmission Facilities operating at less than 200 kV will permit small TOPs to own and operate limited amounts of BES Transmission to connect local 115 and 138 kV networks to EHV BES Transmission Facilities, without imposing a disproportionate regulatory burden. APPA believes that this small but significant change would align the thresholds of all Control Centers and address the significant cost impact on small entities. APPA provided the following suggestion in the CIP V5 Draft 2 comments: APPA has focused our comments on the impact of the standards on small entities. We recommend that the SDT take a close look at the applicability and the requirements in all of the CIP Version 5 standards. Where the standards are applicable to small entities the SDT needs to account for the impact on small entities and only include those requirements if they are absolutely critical for the protection of the reliability of the BES. If these requirements must be included, then the SDT should allow for a small entity exemption process. Alternative Exception Process: APPA would offer the following alternative if the APPA recommendations for TOP thresholds are not adopted in a CIP-002-5 draft 4: APPA Recommendation for new Criteria 2.14: Each transmission Facility that its Planning Coordinator or Transmission Planner designates, and informs the Transmission Owner or Transmission Operator, should be excluded based on the following performance based exception process moving a TOP Control Center from Medium Impact to Low Impact: 1. If the TOP could demonstrate that another TOP had ultimate control or ability to isolate the excepted system, or 2. If the TOP has no ability to schedule voltage (reactive management), or 3. If it can be demonstrated that automatic or manual operation on the TOP system, including delayed clearing of category C events does not cause rating (including in the WECC region, TPL criteria) violations on neighboring TOPs. If the SDT provides reasonable changes to the treatment of small TOP control centers similar to the ones given to small BA and GOP control centers, APPA can recommend an affirmative vote on CIP-002-5. APPA also supports the comments of TAPS which asks the SDT to consider changing the applicability language in Sections 4.1.2.4 and 4.2.1.4 from "Each Cranking Path and group of Elements meeting the initial switching..." to "Each Cranking Path and group of Elements that are part of the BES and that meet the initial switching...."

Individual

Nicholas Lauriat

Network & Security Technologies, Inc.
N&ST chose to abstain.
N&ST chose to abstain.
Group
Detroit Edison
Kent J Kujala
Detroit Edison's comment pertains to CIP-007-5 Part 2.2 & 2.3. Clarification surrounding the use of the term, "mitigation plan" would be valuable. To clarify Part 2.2 perhaps mention that the mitigation plan is intended as an internal document and not submitted to the Regional Entity. Detroit Edison finds CIP V5 well written, organized, easy to understand and easy to follow.
Individual
Steven Wallace
Seminole Electric.com
Individual
J. S. Stonecipher, PE
City of Jacksonville Beach, FL dba/ Beaches Energy Services
We appreciate the hard and excellent work of the SDT to significantly improve the CIP Standards and develop a prudent method to protect the Bulk Electric System from cyber attacks. Although we have several comments, only one comment is causing us to vote Negative for any of the Standards. CIP-002-5, Attachment 1, Bullet 2.12: The SDT added thresholds for Control Centers for small GOPs and small BAs to define a boundary between “Medium” and “Low” Control Centers, but no equivalent threshold for small TOPs, which is inappropriate. Why would a small control center controlling 1499 MW of generation be “Low” whereas a small TOP’s control center for two 138 kV substations with only four 138 kV Facilities be “Medium”? We suggest that a threshold be added for small TOPs to distinguish between Medium and Low. The threshold can be design similar in concept to bullet 2.5, but including >100 kV and <200 kV Facilities with a score of 350. In this way, all of the transmission Facilities under the control of the Control Center could be added up and compared to the weighted score 3000 metric of bullet 2.5 to determine if that Control Center is Medium or Low.
These are issues that we believe should be fixed, but are not causing us to vote negatively. Zero-Defect solution doesn’t get us all the way there: The helpful phrase: “shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented … policies” was added to many requirements to try and address the “zero-defect” problem. However, by choosing the active word “implement”, the zero-defect problem is reintroduced. “Implement” means: “to fulfill, perform, carry out”, which means that in order to prove that a policy was carried out, detailed evidence of the results of executing the policy is needed, reintroducing the zero-defect problem. We recommend replacing the word “implement” with “institute” which means “to set into operation” or “to bring into practice or use” for which the evidence would be less onerous (e.g., the policy itself and proof that it was instituted, such as procedures that support the policy) avoiding reintroduction of the zero-defect problem. CIP-002-5, R1: How is an auditor to verify identification of all BES Cyber Systems that are applicable to R1.1 and R1.2? We wait with interest on what the RSAW will look like. CIP-003-5, R4: The SDT seems to intend to address the zero-defect issue; however, by not associating the documentation of delegation contained in the 3rd sentence to the process of the first sentence, the goal is not accomplished and a strict reading of the requirement still includes a zero-defect problem of needing to document delegation for every delegation and delegation change within 30 days because there is more than one requirement embedded in R4. CIP-006-5, R1: The standard does not answer the question “how big does an opening in the Physical Security Perimeter have to be before is it deemed an access point”? It seems the SDT wants to use the 96 square inches used by some defense agencies, if so, we recommend explicitly stating that in the Standard. CIP-006-5, R1.9 and R2.3, CIP-007-5, R4.3, CIP-008-5, R2.3: These are data retention requirements and should not be requirements of the Standard, especially considering the Paragraph 81 effort which is seeking to retire requirements just like this. CIP-006-5, R2.1: The measure does not match the requirement. The requirement is for “continuous escorted access”, the measure describes evidence at discrete points in time, not continuous. How is an entity to prove that a visitor was continuously escorted? Does this essentially mean video surveillance? Or written attestations of the person providing the escort?
Individual
Michael Falvo
Independent Electricity System Operator
The IESO supports all of 10 standards.
Section 1.1 under Compliance for each standard does not adequately address the Ontario compliance enforcement model. In Ontario the Market Assessment and Compliance Division (MACD) of the IESO is the compliance enforcement authority in Ontario. Suggest the section be revised to read: “1.1. Compliance Enforcement Authority: The Regional Entity, or in non-US jurisdictions an entity appointed by a local governmental authority, shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or

controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA." CIP-008 R1 Part 1.2 requires reporting to the ES-ISAC which may not acceptable to Canadians. Suggest the wording be revised to read: "One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) or for Canadian entities the Canadian Cyber Incident Response Centre (CCIRC). Initial notification to the ES-ISAC or CCIRC, which may be only a preliminary notice, shall not exceed one hour from identification." Note that this needs to be vetted with CCIRC for their concurrence. For clarification, suggest adding "mimic display" to the second paragraph of CIP-007 R5 Rationale, resulting in "Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, mimic displays etc.)." For consistency, recommend changing CIP-008 R2 Part 2.1 from "at least once every calendar year, not to exceed 15 months" to "at least once every 15 calendar months" For clarity, recommend changing CIP-009 R1 Part 1.5 from "One or more processes to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), per device capability. Data preservation should not impede or restrict recovery." to "One or more processes, per device capability, to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), except where data preservation impedes or restricts recovery."

Individual

Glen Sutton

ATCO Electric Ltd.

AE thanks the SDT for addressing their concerns from the previous draft. AE requests that the SDT add a definition for the term Physical Access Point ("PAP"). This definition could be similar in structure to the definition of Electron Access Point and could read: "Physical Access Point ("PAP"): A designated entry point on the Physical Security Perimeter that allows passage through the Physical Security Perimeter and for which access is controlled."

Group

Southern Company

Antonio Grayson

CIP-006-5 RSAW-Page 2, text as written: For the purpose of this RSAW, "deficiencies" refer to possible non-compliances with the standard; not all deficiencies would become issues on non-compliance. Proposed text: For the purpose of this RSAW, "deficiencies" refer to possible non-compliances with the standard; not all deficiencies would become issues of non-compliance. Rationale For Not Supporting: Use of proper English. CIP-006-5 RSAW-Page 9, text as written: Evidence that the entity has physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days prior to the date of the compliance monitoring for: Proposed text: Evidence that the entity has physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days beginning with the date of the compliance monitoring for: Rationale For Not Supporting: Pragmatic implementation of physical security perimeters typically involves clean up of users prior to the compliance date. Prior to the compliance date, logs may have a combination of authorized users and some users who need to be removed before the compliance date. Logs for auditing should be required as of the compliance date, not before. CIP-006-5 RSAW- Rationale For Not Supporting: We recommend standard citation guidance in the RSAW that will be used across all regions.

Individual

Oliver Burke

Entergy Services, Inc. (Transmission)

We do not support CIP-010-1 R1, specifically R1.5 and R1.5.2, a test environment that models the baseline configuration of the BES Cyber System in a production environment is not always practical. In such cases, the requirement to document the differences between the baseline configuration and the test environment each time testing is executed would result in an unreasonable burden on the entities that would not justify the effort required. Suggest modifying the requirement to require documentation only of "material" differences between the baseline configuration and the test environment to avoid the documentation of differences lacking security implications. Maintaining a baseline configuration for every BES Cyber System is excessive and provides marginal benefit to the reliability of the BES cyber system.

Re-numbering of Existing Requirements - For situations where requirements are being moved from their CIP Version 4 Standard to a new Standard in Version 5, the old requirement number should be retired, and not re-used. For Example, the current CIP-007-4 R1, "Test Procedures" and its subparts, have been moved to CIP-010-1 R1.4 & R1.5. As a result, CIP-007-4 R2 "Ports and Services" has been moved to CIP-007-5 R1. As a result, documentation for Ports and Services that is currently identified with CIP-007 R2 will need to be identified with CIP-007 R1 beginning on the effective date of Version 5 of the CIP Standards. This may lead to confusion on the part of the Responsible Entities staff, as well as the audit staff when looking at evidence for a particular standard. Zero-Defects Issue The Background section of each draft Standard states that "The intent is to change the basis of a violation in those requirements so that they are not focused on whether there is a deficiency, but on identifying,

assessing, and correcting deficiencies." The Standard should be clear as to how this will work in practice to avoid uncertainty on the part of Registered Entities and auditors. If this should be read (and enforced) to mean that so long as there is a program that "identifies, assesses, and corrects deficiencies" related to the Requirement individual deficiencies are not violations of the Requirement, the Standard must explicitly say so. As written it is unclear whether individual minor deficiencies should be considered violations and self-reported if the program has been otherwise properly implemented but, for example, an entity suffered an equipment failure resulting in a temporary deficiency. BES Cyber Asset and BES Cyber System Categorization - Brightline Criteria – Medium Impact Ratings "Each BES Cyber System, not included in Section 1, above, associated with the following: 2. 1 Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection. Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services " Comment: NERC Standard FAC-014-2 and its associated requirements (R5.1.1 and R5.1.3) states that 30 minutes to relieve the overload is sufficient. Similarly, Transmission Operators have 30 minutes to return the transmission system to within operating limits following an IROL violation under TOP-007-0 R2 or to return operations to proven reliable power system limits after entering an unknown operating state under TOP-004-2 R4. The new CIP requirements should utilize the same 30-minute period. It is inconsistent to have 30 minutes to address IROL violations but to measure adverse impacts on reliability under the CIP Standards on a significantly shorter time period. . Cyber Security – Personnel and Training R5 - Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in CIP-004-5 Table R5 – Access Revocation. R5.1 – A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights). Comment: The Requirement does not distinguish between termination for cause and termination without cause (i.e. voluntary terminations, the end of contract periods, etc.). For termination without cause, the risk associated with not immediately initiating removal of access and completing such removal within 24 hours is minimal. Avoiding such minimal risk does not justify the administrative burden that expedited access removals this would impose. The 24 hour requirement should be modified to apply only to involuntary terminations or terminations for cause, with voluntary terminations added to R5.2 because voluntary terminations present no more risk than reassignments or transfers. R5.2 requires revocation by the end of the next calendar day.

Individual

John Shaver

Southwest Transmission Cooperative Inc.

CIP-002-5 R 2.12. The TOPs only have a bright-line criteria for medium and high impact. There is not a lot of difference between the requirements of a high or medium impact facility. However, there are tremendous differences in compliance requirements between low and medium impact. The way the standard is written today, all control centers owned by the TOP, no matter how small their footprint, will be classified as either a medium or high impact facility, resulting in financially burdensome compliance obligations. The BAs and GOPs have the ability if they are small to be classified as a low impact facility, and it seems appropriate to classify TOPs by applying similar size thresholds. Thank you.

Individual

Scott Bos

Muscatine Power and Water

MPW would like to thank the 706 SDT on their accomplishments in the CIP-002-5 – Attachment 1 – Impact Rating Criteria. The SDT was sensible in considering the Control Centers and backup Control Centers used to perform the functional obligations of the smaller Generator Operator (Item 2.11 of the Impact Rating Criteria) and Balancing Authority (Item 2.13 of the Impact Rating Criteria) that have less than 1500 MW in a single Interconnection to have a Low Impact Rating. This makes a great deal of sense because these entities do not pose a major reliability risk to the BES. However, for the small vertically-integrated municipal utilities that meet the Low Impact Rating Criteria for their Control Centers and backup Control Centers in their functional roles as Generator Operator and Balancing Authority under the 1500 MW threshold, this same type of granularity is not afforded to them in their functional role of Transmission Operator. This is NOT bright line criteria. The same methodology that brought about the 1500 MW threshold for smaller Generator Operators and Balancing Authorities should be applied for their functional role of Transmission Operator. For this reason, MPW cannot support CIP-002-5. The SDT needs to understand that not all Transmission Operators are created equally. Especially not the Transmission Operators at the small vertically-integrated municipal utilities. For these Control Centers and backup Control Centers of these small utilities to carry the Medium Impact Rating just because they are registered as Transmission Operators would be exceedingly burdensome and not equitable based on their very low impact to the reliability of the Bulk

Electric System.
As mentioned before, there should be a threshold level for the Medium Impact Rating of the Control Centers and backup Control Centers used to perform the functional role of Transmission Operator. The logical criteria to look at for determining a threshold level would be voltage. The criteria for Item 2.12 of the CIP-002-5 – Attachment 1 – Impact Rating Criteria should be rewritten similar to: Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator with Transmission Facilities operating above 200 kV and not included in High Impact Rating (H), above. Other options would be to have the Impact Rating Criteria of the Control Centers and backup Control Centers used to perform the functional role of Transmission Operator be based on the total mileage of Transmission lines or the number of Transmission lines operated by the Transmission Operator. MPW would support CIP V5 if there was consideration provided for the small vertically-integrated municipal utility performing the functional role of Transmission Operator that operate two 161 kV lines totalling 32 miles. It does not seem equitable that our neighbors operate several hundreds of miles of Tranmission, much of it at 345 kV, and have the same Medium Impact Rating.
Individual
Russ Schneider
Flathead Electric Cooperative, Inc.
I would support the proposed revisions if the BES definition is approved by FERC and implemented in its current form. However, without the BES definition being final it is premature to support the changes and potentiall burdensome on potentially non-BES protection systems that may be properly part of a local network or radial distribution system.
Individual
Allen D. Schriver
NextEra Energy
The drafting team has done an excellent job of improving Version 5 (V5) while also addressing many of FERC's Order 706 suggestions in the face of divergent industry views and points of emphasis. NextEra Energy, Inc. (NextEra) is voting Affirmative on CIP-002-5, CIP-003-5, CIP-005-5, CIP-008-5, CIP-011-5, and Definitions, while voting to Abstain with comments with respect to CIP-004-5, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-5, and the Implementation Plan. NextEra voters will reconsider Abstain positions on these 6 items (either for another successive ballot or upon a recirculation ballot) if: (a) the zero defect fix language ("in a manner that identifies, assesses, and corrects deficiencies" (the IAC Language)), which is applicable to 66 different requirements in draft 3 of V5, is supplemented, revised and/or better clarified; and (b) the Implementation Plan is improved, both as further described below. With respect to (a), the draft RSAW for CIP-006-5 is a welcome gesture and a step in the right direction, but it is flawed, insufficient, and does not change the fact that the IAC Language used in the standard is ambiguous and untested. The IAC Language does not explicitly address the issue of whether and, if so, when internally identified and corrected deficiencies constitute violations of the standard's requirements. The proposed RSAW language regarding "deficiencies" and "self-reporting" does not adequately resolve this ambiguity; if anything, it further muddies the water. It is unclear to NextEra whether any amount of verbiage in an RSAW can cure ambiguity flowing from the standard language itself. With respect to the words chosen, by prefacing the IAC Language with the phrase "in a manner that," which is itself prefaced by the words "shall implement," the requirement has become more, not less, rhetorically prescriptive. This is a step in the wrong direction, as NextEra and others were hoping the language chosen would not be in the form of an additional command, but would simply give their cyber security staff the freedom they need to develop robust internal correction programs, especially for high-volume, periodic activities. For companies like NextEra that operate in multiple NERC regions, the prospect of inconsistent and un-coordinated compliance evaluations raises serious concerns about whether the IAC Language could be applied and utilized in different ways across the country. To prevent this vacuum of ambiguity from being filled with negative unintended consequences, NERC must find an expeditious way to modify, clarify, or at least standardize the interpretation the IAC Language. One option is the insertion of an addendum to V5 between the putative approval of draft 3 on October 10, 2012 and the final recirculation ballot that must be held before the new standard is ripe enough to forward on to the NERC BOT. Such an addendum could be narrowly focused on soliciting stakeholder input and consensus regarding ways to modify, interpret and/or clarify the IAC Language in a way that makes sense for all stakeholders. NextEra's specific suggestion for improving the IAC Language is to strike the entire phrase, then insert a new, longer sentence fragment at the end of the current sentence: "[Each Responsible Entity shall implement one or more documented physical security plans that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan], provided that internally identified deficiencies that are documented, assessed, and corrected if necessary as determined by the Responsible Entity, shall not constitute per se violations of this R1." The generic use of the legal phrase "per se" is a potentially promising way of addressing the violation issue directly in the standard itself. With more explicit, robust language in the standard, it would be easier for industry and NERC to facilitate a broader shift to risk-based auditing based on internal controls. To that end, in addition to changes to the standard itself, NextEra supports the following RSAW language for CIP standards with IAC Language: "Where the entity is identifying, assessing, and correcting its own deficiencies, the entity is satisfactorily performing the requirement." Also please consider this language for the RSAWs: "R1 Absent a possible violation that resulted in (or could have resulted in) a significant risk to the Bulk

Electric System, no violation of R1 and its subrequirements shall be found, provided that the Responsible Entity has implemented a process for identifying, assessing, and correcting deficiencies with adherence to the items specified in Requirement R1." Moving to a new topic, item (b) above, NextEra has voted to Abstain with respect to the Implementation Plan for the following reasons. The Implementation Plan fails to specifically say that NERC will ask FERC to suspend the April 1, 2014 effective date for Version 4 (V4) when it submits V5 for FERC approval prior to March 31, 2012. Without suspension of the V4 effective date, NextEra is among those that will be forced to follow a parallel and costly approach to sustaining compliance to Version 3, implementing V4 by April 1, 2014 for newly identified Critical Assets, and implementing V5, which eliminates the term Critical Assets, for its presumed effective date of July 1, 2015. The current plan is a recipe for costly stranded costs that do not improve reliability. The drafting team can and should address this important problem in the Implementation Plan. Alternatively, NERC can and should ask FERC to move quickly to approve V5 once it is submitted for approval, or at least move quickly to suspend the effectiveness of V4 pending FERC's review of V5. In addition, NextEra believes the line between planned and unplanned changes is not always easy to maintain and there may be times it is appropriate to let a planned change become fully compliant at some time after the cyber system is commissioned. Similarly, after initial implementation of V5, there is an inadequate amount of time allotted for the implementation of the V5 Standards for BES Cyber Systems that go from the "Low" to "Medium" or "High" impact categorization based on unplanned enhancements and improvements to facilities. Responsible entities should be given 18-24 months, not merely 12 months, to comply, as many of the compliance activities can only be accomplished during planned outages at generation facilities. NextEra also finds the section on Initial Performance of Certain Periodic Requirements to be confusing and unnecessary and urges the drafting team to strike it or qualify these timing recommendations as proposed guidance, rather than a mandatory directive for all Responsible Entities to follow. If the section must remain, NextEra suggests it allow for an alternative timing option for periodic requirements that pegs all of the V5 requirements to the Effective Date and lets the Responsible Entity begin meeting the periodic items as they arise naturally in accordance with the CIP standards' periodic requirements.

NextEra thanks the drafting team for its hard work and the improvements it has made to Version 5.

Individual

Yee Chou

American Electric Power

AEP does not support CIP-004, CIP-005 and CIP-010 for the following specific reasons: CIP-004 Requirement 3 involves performing personnel risk assessments (background checks) to employees and contractors alike. The current standards allow the entity to tailor their program, which could include different provisions for contractors versus employees if necessary. In addition, AEP has concerns that these and other changes have created requirements that are confusing and could be written clearer. CIP-005 Requirement 1.3 calls for requiring inbound and outbound access permission, including the reason for granting access, and deny all other access by default. Our major concern is regarding "outbound access permission". The target threat vectors to the BES Cyber Systems would be inbound to those networks and those attempts inbound into the networks need to be monitored and controlled. While there is the possibility that could be malicious code internal to these networks communicating, we think that tracking all outbound communication from one AEP trusted network to another AEP trusted network would more than double the monitoring that is required. In addition, the CIP standards have other controls to help monitor and detect the malicious code internal to the networks. CIP-010, Requirement 2.1 calls for monitoring at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1), and documenting and investigating detected unauthorized changes. AEP has internal processes for change management, which include approvals and controls, but AEP does not have tools for the detection of changes from the baseline for many systems. At this point in time, there are no tools commercially available that provide the necessary monitoring and tracking of changes of complex computer systems that indicate all of the changes made on top of the baseline configuration. This requirement might force us to perform cyber vulnerability assessment every 35 days which will consume major labor effort. In the meantime, we have additional comments to further improve clarity of the following standards: For CIP-002, Attachment 1, Sections 1.2 and 1.4 - change it to ".....assets that meet criterion.....2.6, or 2.9 (only if it is directly involved in the SPS functions). For CIP-003 AEP questions whether CIP-003 R1 and R2 match the parameters of efforts of team developed for Paragraph 81. The most elements required to be implement by policies are actually embedded in the remainder of the requirements in the other CIP standards. CIP-003 M1 – Does the wording of this measure infer that there has to be multiple procedures, whereas the requirement indicates that one or more procedures are valid? CIP-003 R2 – remove "shall implement" because a violation of a requirement might be a violation of the policy as well. For CIP-004, • R2 Language: o "…in a manner that identifies, assesses, and corrects deficiencies…" – does this mean that if we fail to meet all the requirements in the table that we can simply correct the problem and not self report? If so, we feel the language should be more definitive. o "…appropriate to individual roles, functions, or responsibilities…" – who defines what is / isn't appropriate? This looks like it leaves the auditors with a great deal of latitude to decide themselves what is appropriate / not appropriate. • Requirement 2.1.9 – suggest removal of this sub-requirement – otherwise, it would also apply to PCAs under the Applicable Systems o not sure what they mean by "cyber security risks" – seems rather vague and difficult to audit and subject to future CANs, interpretations, etc. o not sure what is meant by "interoperability" – seems vague and open to interpretation and a candidate for a future CAN, interpretation, CAR, etc. • Requirement 2.2 – If personnel change roles, it seems from the language in the requirement that they need to take the required training prior to assuming the new role. Is that the intention? If

so, this should be clarified in the requirement. • Requirement 3.3 – Suggest that the change rationale language match the language in the requirement. Specifically, “criteria” should be excluded – and only “process” be referenced. • Suggest removal of 3.3 and 3.4 – and roll them into 3.2. Also suggest that the reference to “contractors and service personnel” be rolled into the language of the R3 standard (i.e., make it applicable to both employees and contractors). Finally, note that 3.3 is completely redundant with 3.2. • Requirement 3.5 – suggest adding the word “calendar” before “years” For CIP-006, • R1.5 – suggest they remove the 15 minute maximum limit on the alarm /alert – leave the language as simply “Issue an alarm or alert in response to detected unauthorized circumvention of access through a physical access control point into a Physical Security Perimeter.” • R1.7 – suggest change to simply: “Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System.” • R1.8 – suggest they add “initial” before “entry” in the last sentence – this would make it align with R2.2 for visitors For CIP-008, • 4.1.2.3 – attachment 1 of CIP-002 would probably limit the impact to DPs (most would fall below medium) • R1.1 – definition of Cyber Security Incident – difficult to determine intent of potential attacker – “suspicious” is rather vague and would leave it to the entity to define for itself • R1.2 -- “…which may be only a preliminary notice, shall not exceed one hour from identification determination” – we question the value of having this time limit (but we realize it is in the FERC Order 706) – would require that entities install a time stamp step in their incident response process to indicate when something was identified as reportable and then retain all this information in records to prove compliance to auditors – seems to be a candidate for Paragraph 81… For CIP-009, • R1.3 - There should be consistency in the applicability to ensure consistency across the different standards. For example, some indicate "with External Routable Connectivity" or "without External Routable Connectivity" if it is not specified which apply? • R1.4 - Suggest removing "...and to address any backup failures." This may lead the reader to the notion of having another pre-determined plan to account for unknown issues during the backup. • R1.5 - The requirements could put the Registered Entity into a "Catch-22" scenario. They could try to comply with the requirement by saving logs, which might impede recovery. Who is given the discretion of making the determination of which approach should have been taken? It is likely that the auditor will have their own perspective after the fact which may not align with the thinking of the Registered Entity during the event. Poorly worded…. • R3.1 - "After completion of a recovery plan test or actual recovery and not to exceed 90 calendar days after completion..." should be stated at "After completion of a recovery plan test and not to exceed 90 calendar days after completion..." A lessons-learned activity should not be required for every failure of equipment in the field. For CIP-010, • R1.1 - AEP suggests to add "software package", not just "software". AEP would also ask clarification that these "items" are current, not any historical ones. • R1.3 - Should it be 35 calendar days which will be consistent with other requirements? • R1.5 - In the Measures, "description of how any differences were accounted for" is unreasonably challenging. It's not possible to scale this to any large number of BES Cyber Assets. • R2.1 - How do we detect "unauthorized changes"? Is this calling for CVA every 35 days? • R3.2 - The comment for R1.5 applies here. • R3.4 - Are the vulnerabilities identified in this assessment considered as "violations"? For CIP-011, • R1.2 – It is suggested that the last bullet for the Measures for Part 1.1 be added to Part 1.2. The following is the specified language “Repository or electronic and physical location designated for jousting BES Cyber System Information in the entity’s information protection program.” • CIP-011 R2 should contain the phrase “in a manner that identifies, assesses and correct deficiencies.” For Definition, • AEP Recommends that data center (used in the Control Center definition) be a defined term. • Cyber Assets - For the definition of Cyber Assets, how does the wiring between Cyber Assets come into play? • Electronic Access Point (“EAP”) - AEP recommends that definition be changed to: o "A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication..." From: o "...Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter." • Intermediate Device - Does this interpretation lead to the solutions like jump-hosts or do systems like SecureID or CISCO ACS qualify as Intermediate Devices? Also, as written would this definition lead Registered Entities to not have the Intermediate Devices in another ESP? • Reportable Cyber Security Incident - - This definition if very vague and AEP would develop its own definition.

SDT has done a good job further clarifing these standards. AEP is ready to provide full support once the issues in CIP-004, 005 and 010 are addressed properly.

Group

CenterPoint Energy

John Brockhan

Definitions – CenterPoint Energy does not support the definition proposed for Dial-up Connectivity, “A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.” The Company prefers a definition that is more aligned with what was previously provided in CIP-related FAQs, “any temporary (non-permanent), interruptible or not continuously connected communication access to a Critical Cyber Asset from any remote site. Using a modem over a land line, wireless technology, or VPN using a routable protocol to connect to a Critical Cyber Asset from one or more locations or by one or more users are examples of dial-up accessible access. Access to a Critical Cyber Asset via a permanent communication connection from a specific computer over a dedicated communication circuit would not be considered dial-up accessible access.” There are specific concerns with the proposed definition’s lack of consideration for the direction of communications versus the phrase “to connect to a Critical Cyber Asset from one or more locations” provided in the FAQs. Also as previously submitted, CenterPoint Energy believes “was an attempt” in the definition of “Cyber Security Incident” is vague and seeks clarification on how such an attempt

would be determined. An alternative would be to delete the phrases “or was an attempt to compromise” and “or was an attempt to disrupt”. CIP-002 – CenterPoint Energy also still has significant concerns with criteria 2.5. As currently defined, the values force a label of critical on non-critical Facilities as proven by intricate studies performed by transmission planning engineers. CenterPoint Energy recommends the values be revised as follows: Voltage Value of a Line 200 kV – 399 kV – Weight Value per Line - 800; Voltage Value of a line 400kV to 499 kV – Weight Value per Line – 1300. CIP-003 – The reference to “CIP-002-5, Requirement R2” should be to Requirement R1. CenterPoint Energy suggests that the phrase “low impact” be used in R2 as “high impact” and “medium impact” is used in R1. For example, the requirement would be as follows: “Each Responsible Entity for its low impact BES Cyber Systems shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]”. CenterPoint Energy questions the addition of the “zero defect language” to requirement, R4. (The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of the initial delegation and any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]) The Company believes that the requirement is binary in that delegations are assigned or not. CIP-006 – CenterPoint Energy questions the addition of the “zero defect language” to requirement, R1. (Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in CIP-006-5 Table R1 – Physical Security Plan. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].) The Company believes that the requirement is binary in that a documented physical security plan exists or not. CenterPoint Energy recommends that the Applicable Systems in R1.1 be revised from “Medium Impact BES Cyber Systems without External Routable Connectivity” to” Medium Impact BES Cyber Systems” as that has been the label for Medium Impact BES Cyber Systems not having External Routable Connectivity. (Unless there is a difference between the terms “Medium Impact BES Cyber Systems” and “Medium Impact BES Cyber Systems without External Routable Connectivity”) CIP-007 – CenterPoint Energy suggests the following alternate wording for requirement part, 5.2: ”Identify and inventory all KNOWN enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s)”. CenterPoint Energy still prefers that the SDT add “with External Routable Connectivity” to the Medium Impact applicability for the Patch Management requirements, R2.1 – R2.4. The Company understands the comments of the SDT; however, believes that a combination of no external routable connectivity, frequency of access to medium impact facilities, and policies reduces the risks to those facilities from the insider that would introduce threats (“thumb drives, laptops, smart phones”) into the environment to an acceptable level. While devices with no external connectivity may have some physical access risks associated with the use of thumb drives, laptops, etc., the fact that they are isolated from other BES devices must be considered when addressing appropriate protections. The lack of external connectivity reduces the risks to that isolated device; therefore, the risk to the BES is minimal. Additionally, physical security is adequate mitigation from the external threats as once physical security is breached; there are other immediate and evident concerns that do not involve BES Cyber Systems. Alternatively, CenterPoint Energy requests that the timeframes for requirement parts, 2.2 and 2.3 be revised to 90 days for Medium Impact BES Cyber Systems. CIP-008 – CenterPoint Energy is concerned with the reasonableness of the 1 hour reporting requirement in part 1.2 and recommends that the SDT increase the timeframe. CenterPoint Energy still believes that Part 2.2 is too prescriptive as it relates to documenting deviations and recommends that the SDT remove "documentation of deviations" as deviations in a sense should be captured in lessons learned (i.e. after-the-fact versus during critical time). CenterPoint Energy requests that the SDT add "except in CIP Exceptional Circumstances” and a sentence related to impeding recovery as noted in CIP-009 Part 1.5 (Data preservation should not impede or restrict recovery). CIP-009 – CenterPoint Energy is not sure of the placement or intent of Requirement Part 1.5 and requests that the SDT consider revising or moving this requirement to CIP-008. CenterPoint Energy requests clarification on the intended frequency of part 1.4 (“verify the successful completion of the backup processes”) and the reference to a “representative sample” in part 2.2. CIP-010 –CenterPoint Energy still prefers that the SDT add “with External Routable Connectivity” to the Medium Impact applicability to the requirements of this standard. No external routable connectivity, frequency of access to the facilities, and policies reduces the risks to those facilities from the insider that would introduce threats into the environment to an acceptable level. Additionally, physical security is adequate mitigation from the external threats as once physical security is breached; there are other immediate and evident concerns that do not involve BES Cyber Systems. CenterPoint Energy does not perceive how adding “with External Routable Connectivity” to the requirements explicitly conflicts with the FERC directive (elimination of the blanket exemption for non-routable connected cyber systems) as there are other standards and requirements that clearly demonstrate acknowledgement and response to the directive. Alternatively, the Company requests that requirement part, 1.3 be revised to 90 days for Medium Impact BES Cyber Systems. CenterPoint Energy proposes that the associated timeframe for requirement part, 1.3 (For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.) be updated to 90 days instead of 30 days. CenterPoint Energy proposes that the SDT

change the timeframe associated with requirement part, 2.1 to 90 days. CIP-011 – CenterPoint Energy recommends that the SDT add “with External Routable Connectivity” to the Medium Impact applicability for this standard.
CenterPoint Energy recommends the above changes for an affirmative vote on all ballots.
Individual
Brett Holland
Kansas City Power & Light and KCPL-GMO
N/A
It is essential that the standards contain everything that is required and to not intentionally or inadvertently include requirements by reference in other documents. The standards should stand on their own, without reference to other documents that introduce interpretation for requirements without use of established processes approved in the Rules of Procedure. Further, all definitions must be captured in the definitions document. We encourage the removal of “rationale” statements throughout as requirements do not consistently support the list. To prevent misinterpretation, “Electronic access controls for routable protocol connections and dial-up connectivity external to the ESP” is suggested for CIP-003 R2-2.3. In CIP-004 R5.3, change “by the end of the next calendar day” to “within 30 calendar days”. In CIP-007 R4.4, the “summarization” and “sampling” components are too broad. We encourage specificity in all measures. Additionally, the term “undetected” is unclear and confusing. Clarification, such as “logged but not previously selected for alerting or alarming” could be helpful. Lastly, CIP-010 R1.5.2 should specify to what level the differences must be documented between the test environment and the production environment to ensure cost benefit for the level of investment. In addition, KCP&L endorses the comments filed by SPP RTO.
Group
Southwest Power Pool Regional Entity
Emily Pennel
Implementation Plan: (1) Compliance with CIP-003-5/R2 upon the 13th calendar quarter is excessively long; especially considering the requirement is to draft a small number of policies. (2) Continued insistence that Version 4 will not see the light of day sends the wrong message to the registered entities that will face violations and possibly stiff penalties if they heed this message and Version 4 does go into effect. Given past history, it is exceptionally unlikely that FERC will approve Version 5 prior to the Version 4 effective date. The only way to realistically obviate Version 4 and retain Version 3 is for FERC to rescind Order 761. (3) The compliance expectation for CIP-002-5/R2 needs to be qualified with “in sufficient time to be able to ensure the identified BES Cyber Systems are compliant with the applicable requirements of CIP-003-5 through CIP-009-5 and CIP-010-1 through CIP-011-1 as of the effective date of these standards as adjusted by this implementation plan.” (4) To preclude record keeping issues, compliance with CIP-004-5/R4.2 should be required on or before the effective date. (5) To preclude initial errors, compliance with CIP-004-5/R4.3 and R4.4 should be required on or before the effective date. (6) The compliance statement for CIP-006-5/R3.1 should require testing within 24 months of the previous test for physical access controls subject to previous versions of the CIP standards and only allow 24 months from the version 5 effective date for newly in-scope physical access controls. (7) Including CIP-008-5/R3.1 in group 6 of the implementation plan is illogical as this activity is triggered by a test or an actual incident. (8) Including CIP-009-5/R3.1 in group 6 of the implementation plan is illogical as this activity is triggered by a test or an actual recovery event. (9) Compliance with CIP-010-1 (not CIP-010-5)/3.1 should be required on or before the effective date for any new Cyber Asset not subject to a previous version of the CIP standards. This is consistent with CIP-010-5/R3.3 that requires an active vulnerability assessment for any new Cyber Asset prior to placing the Cyber Asset into production. (10) CIP-011-1 (not CIP-011-5)/R1.3, included in group 6 of the implementation plan, does not exist. (11) CIP-009-5/R2.3 is included in both group 6 and group 7. (12) Compliance with CIP-010-1 (not CIP-010-5)/3.2 should be required on or before the effective date for any new Cyber Asset not subject to a previous version of the CIP standards. This is consistent with CIP-010-5/R3.3 that requires an active vulnerability assessment for any new Cyber Asset prior to placing the Cyber Asset into production. (13) Group 8 is not necessary as this requirement is already articulated in CIP-004-5/R3.5. If retained, the expectation should be modified to require an updated PRA “within 7 years of the anniversary date of the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards.” (14) In the “Previous Identity Verification” section, the reference to CIP-004-5/R4.1 is illogical. The reference is more likely CIP-00405/R3.1. (15) In the “Scenario of Unplanned Changes After the Effective Date” table, the last scenario (identifying the first medium impact or high impact BES Cyber System) needs to be clarified whether this applies to the first BES Cyber System as a location/facility or the first BES Cyber System identified overall (i.e., the Responsible Entity had no previously identified BES Cyber Systems whatsoever). (16) Under the weakest link principle, the CIP-004-5/R4 Access Management Program and the CIP-004-5/R5 Access Revocation requirements in the Applicability Reference Tables should also apply to Protected Cyber Assets. (17) In the Applicability Reference Tables, Physical Access Control Systems should be protected by an ESP-like perimeter in the same manner they are required to be protected under CIP Version 3. (18) In the Applicability Reference Tables, Electronic and Physical Access Control or Monitoring Systems should be subject to CIP-005-5/R2 Remote Access Management. Definitions of Terms: (1) Throughout the definitions, there continues to be references to “would” (e.g., would within 15 minutes… or would effect…). The criteria need to be prospective. From a risk perspective, if

something “could” happen, then entities should assume that under the right conditions it “would” happen and require the protective controls to be implemented. The use of “would” implies certainty and registered entities may argue over that distinction in determining certain BES Cyber Systems are not subject to the CIP standards. The definitions need to use the phrase “could” and not “would”. (2) Allowing a CIP Exceptional Circumstance may not always be appropriate in the instance of an “imminent or existing hardware, software, or equipment failure.” This provision allows a Responsible Entity to declare a “CIP Exceptional Circumstance” for petty issues that do not place the reliability of the BES at risk in order to bypass the requirements of the CIP standards. (3) The reference in the definition of Control Center to controlling the BES in real-time allows a Responsible Entity to take an entity-centric view and argue that while they may be controlling multiple facilities and performing the RC, BA, and/or TOP functions, they are not “controlling” the BES. The definition should remove the “BES control” reference and simply apply the definition to RC, BA, and TOP functions performed. (4) The definition of Cyber Security Incident should also apply to Protected Cyber Assets, EACMS, and PACS. (5) The definition of Electronic Security Perimeter allows the Responsible Entity to serially connect certain Cyber Assets (e.g., Digital Protective Control Devices) to a communications processor that, in turn, communicates to other Cyber Assets using a routable protocol, and in doing so declare that the DPCD do not need to reside within the ESP and therefore are not subject to the CIP standards. (6) The definition of Reportable Cyber Security Incident is too broad. Detected malware might not have disrupted or compromised a reliability task, but it has compromised the Cyber Asset where the reliability task is performed. Such malware could compromise the task in the future upon instruction from a command and control system with which it is communicating. Any malware infection of an in-scope Cyber Asset should be reported. General Comments Applicable to Multiple Standards: (1) The intent of a number of requirements is to change the basis of a violation so that the focus is on identifying, assessing, and correcting deficiencies. While the intent is noble and overall beneficial, there are two issues that need to be considered and addressed. First, at some point, the number of deficiencies found and corrected becomes excessive and is indicative of a poor or non-existent compliance program. The standards do not address the point at which “found, fixed, no harm, no foul,” especially for recurring failures with the same requirement, becomes a finding of overall non-compliance and is subject to a violation. Without boundaries, the Responsible Entity could continue to falter, do nothing significant to correct the underlying deficiencies, and hide behind the “find, fix, and essentially move on” approach. Even the Find, Fix, and Track (FFT) enforcement program has provisions for taking note of repeat incidents and elevates the FFT to a prosecuted violation for repeated failures. Second, there is no apparent requirement for the Responsible Entity to document the failure and the actions taken to correct and prevent further recurrences, similar to a mitigation plan for a violation under today’s standards. Without required documentation and an expectation of audit review, Compliance Enforcement Authorities will have no basis for judging the effectiveness of the audited entity’s internal compliance program. This is of significant concern for the CIP-007-5 requirements as they have the greatest impact on actually protecting the BES Cyber Systems. (2) There are a number of requirements that require a program or procedure to be documented, or for the Responsible Entity to have a method to perform some task, but do not explicitly require implementation. While implementation is implied, FERC found this to be a shortcoming in the CIP Version 1 standards and required the standards to be modified to explicitly require implementation of the documented process. To preclude a similar order by FERC in addressing the Version 5 standards, the language should be modified now to address and remedy the issue. (3) the accompanying guidelines contain significant valuable information and explanations of intent. Some of this guidance needs to be incorporated into the requirement itself. As Registered Entities are quick to point out, guidance is not an auditable requirement. If the guidance expresses an expectation, that expectation needs to be explicitly stated in the requirement. (4) Stated intervals in the standards are not consistent. Most “annual” requirements have been modified to require the activity at least once every 15 months. There are still a few requirements that require the event to occur each calendar year with no more than 15 months interval between activities. From both entity compliance and an audit perspective, requiring an activity to occur at least every calendar year with a defined maximum interval is easier to program and monitor. CIP-002-5: (1) Similar to the Definition of Terms, this standard and attachment use the term “would”, which implies an arguable certainty. The standard needs to take a prospective view and use the term “could”, requiring the Responsible Entity to assume that the criteria will come to fruition and in doing so properly identify BES Cyber Assets that require protection under these standards. (2) The examples of Physical Access Control Systems used within this and other CIP Version 5 standards needs to include the workstations used to provision physical (e.g., badge) access rights and/or are used by security personnel to monitor for and receive physical security alerts. Excluded from this definition are workstations that create the physical badge as long as that workstation and associated equipment only create the badge and are not used to provision access rights associated with the badge. (3) The use of the term “considers” in Requirement R1 leads to the same confusion as exists with the existing CIP-002-3 standard as some entities will argue that “consider” does not mandate a required subsequent action. The requirement should be restated as “For each asset type enumerated below, each Responsible Entity shall:”. (4) The assertion in Requirement R1.3 that the entity is not required to produce a list of low impact BES Cyber Systems renders this requirement not auditable for accuracy or completeness. To demonstrate that all high and medium impacting BES Cyber Systems have been properly categorized, the entity must be prepared to produce a list of all BES Cyber Systems that were evaluated, the remainder of which represent the low impacting BES Cyber Systems. The entity must also be prepared to demonstrate the minimal requirements applicable to low impacting BES Cyber Systems have been properly implemented, also requiring a list of impacted systems. CIP-002-5/Attachment 1 (Impact Rating Criteria): (1) the 3000 MW minimum specified in criterion 1.2 is excessive and does not appropriately reflect the potential risk a network-connected Balancing

Authority has not only upon its own service area but also upon the rest of North American BA, TOP, and RC registered entities with which it is directly or indirectly connected via the ICCP communication networks. (2) The 200 kV floor specified in criterion 2.5 does not adequately consider the risk to the BES imposed by large regional areas that are predominately sub-200 kV. The 2011 Southwestern blackout demonstrated just such a risk, even experiencing issues at sub-100 kV voltage levels that contributed to the disturbance. The BES is defined as 100 kV and above and the criterion needs to consider all of the BES in some manner. (3) The 1500 MW minimum specified in criterion 2.13 is excessive and unreasonably excludes a significant number of Balancing Authorities from meaningful participation in protecting the BES from cyber attack. Given that all BAs, TOPs, and RCs are interconnected via the ICCP links, these excluded Balancing Authorities could easily be the initial vector to attack the entire North American grid by exploiting trusted communication paths and exceptionally vulnerable ICCP systems to gain access to and compromise BES Cyber Systems essential to the reliability of the BES. Establishing criteria that effectively eliminates significant numbers of interconnected control centers fails to address the specific concerns outlined in both Order 706 and Order 761. (4) The use of the terms “critical” and “initial system restoration” in criterion 4.4 is problematic. Initial system restoration is not a defined term and registered entities have regularly argued that none of their resources are critical as they have many options from which to draw upon. The criterion needs to reflect the language and system restoration considerations found in EOP-005-2, Requirement R1, recognizing that it is not the role of the CIP compliance auditor to determine either the state at which initial system restoration is complete nor the viability of the EOP-005 system restoration plan when auditing this requirement. The criterion must provide certainty to both the Responsible Entity and the auditor and the current language falls short in that regard, suffering the same issues seen today in CIP-002-3. (5) The Low Impact Rating criteria needs to include automatic load shed systems that do not shed sufficient load to meet criterion 2.10. CIP-003-5: (1) The language of R1 and R2 could be improved by requiring one or more documented cyber security policies that “collectively” address the enumerated topics. (2) Requirement R3, as written, is not auditable and does not support the auditing of other requirements which require CIP Senior Manager approval. Identifying the CIP Senior Manager solely by name does not address the instances where there are multiple employees by that same name. The appointment must be able to uniquely identify the appointed CIP Senior Manager. Even an appointment by position title, as permitted for delegations of authority, is a superior approach to a name-only appointment document. Additionally, the absence of the effective date renders the 30-day update requirement not auditable and additionally precludes the verification of proper authorization where the approval of the CIP Senior Manager is required. (3) Similar to Requirement R2, an appointment of a delegate by name only does not uniquely identify the person being delegated authority. Delegating by position title is a far superior approach, especially as the delegation is permitted to succeed changes in both the CIP Senior Manager and the delegate him or herself. (4) In the discussion of possible controls to consider, the use of “ingress and egress” in section 1.2 is a physical access term being applied to logical access. “Login and logout” or “session initiation and termination” would be more appropriate language. Additionally, visitor management controls is conspicuous by its absence from the suggested controls in section 1.3. CIP-004-5: (1) It is not clear if the training required by Requirement R2 extends to contractors and vendor support staff. The extension is implied, but the requirement needs to be specific. The accompanying guidance is specific, however like the CIP standards FAQ today, guidance is not an auditable requirement. (2) It is not clear if the evaluation process specified in Requirement R3, Part 3.3 includes an expectation of clearly defined evaluation criteria for approval/disapproval of the access request. (3) It is not clear if the verification process specified in Requirement R3, Part 3.4 expects the Responsible Entity to perform the evaluation or permits the contractor or service vendor to perform an evaluation using its own criteria with an assertion to the Responsible Entity of compliance and acceptability. At a minimum, the Responsible Entity should be required to review and concur with the evaluation process and criteria used by the contractor or service provider if the entity is permitted to rely upon the assertion of the third-party provider. (4) Requirement R3, Part 3.5 needs to be clarified by replacing the phrase “within the last seven years” (that carries a similar ambiguity as the term “annual”) with the phrase “on or before the seventh anniversary of the previously conducted personnel risk assessment.” (5) Requirement R4, Part 4.2 should at least verify authorization records against actual access to detect any instance where access was erroneously granted or not revoked as expected. Verification of specific access rights is not required by the quarterly review, but verification of overall granted access is important and cannot be accomplished solely by a documentation review. (6) Requirement R5, Part 5.2 should be modified to revoke access by the end of the next “business” day as opposed to the next “calendar” day. As the revocation results from a reassignment or transfer, and not a termination for cause, the potential risk does not mandate a next calendar day revocation. CIP-005-5: (1) Requirement R1, Part 1.5 needs to include an explicit requirement for real-time monitoring and/or alerting upon detection of known or suspected malicious communication. Registered Entities will read the requirement explicitly and as written can make an argument that there is no requirement to monitor for or alert upon detected malicious traffic. CIP auditors have already encountered entities that deploy Intrusion Detection Systems but only monitor the IDS during normal business hours, or occasionally review the logs for events of interest. Simply detecting malicious traffic, with or without logging, does not address the immediate risk posed by the activity. CIP-006-5: (1) Requirement R1, Part 1.3 may not be responsive to FERC Order 706. The language of the requirement could be improved by adopting the “layered and complementary security procedures” language found in Paragraph 573 of Order 706 with a focus on defense in depth as articulated multiple times in the Order. The concern expressed by FERC staff at the time of the order was that the complementary controls be designed such that the failure of a single control did not result in a failure of the complementary control yielding uncontrolled access. In that light, the comment in the guidance section for this

requirement that states two-factor authentication would be acceptable is not appropriate. Instead, a series of access controlled doors or even a locked fence gate in combination with the control house at the substation could be acceptable. (2) Requirement R2, Part 2.2 as written could allow a logged entry/exit to span multiple days with no documentation of a significant gap in access. While the intent is to not require the visitor to log out and back in when briefly stepping out of the PSP (such as to retrieve tools or repair parts from the visitor's vehicle), the requirement should expect the visitor to sign out when departing the premises, such as going to lunch or overnight. (3) The 24 calendar month interval specified in Requirement R3, Part 3.1 is still excessive for normally occupied facilities such as a primary control center. This is especially true when the physical security controls are protecting high impacting BES Cyber Assets. CIP-007-5: (1) Requirement R2, Part 2.1 requires the Responsible Entity to identify a source or sources that the entity will track for the release of cyber security patches. The corresponding guidance suggests that the third-party SCADA system vendor is an appropriate source for patch availability notification. The ability of a Responsible Entity to wait until a SCADA system vendor "certifies" a patch before requiring the Responsible Entity to begin the assessment and follow-on patching process introduces unnecessary risk to the BES. There is a significant difference between assessing a patch for applicability and assessing a patch for installability. An applicable patch may be found to be incompatible with the third-party vendor's systems, would not be certified, and should not be installed. That does not mean the vulnerability being addressed by the patch should not be mitigated, rather it is incumbent upon the Responsible Entity to protect its systems in a timely manner. The Responsible Entity needs to select a patch availability source that is timely, including the original patch provider and well recognized general information providers like US-CERT, SANS @Risk, and nCircle. There is no harm in then waiting for the SCADA vendor to certify the patch before installing it, but the Responsible Entity is at least aware of the vulnerability, can assess the risk, and take appropriate interim action. (2) Requirement R2, Part 2.3 requires the Responsible Entity to either install the patch within 35 calendar days or simply create or update a mitigation plan. There are no boundaries of what is acceptable in a mitigation plan, no expectation of justifying the decision, and no requirement for CIP Senior Manager approval, thus allowing an entity to completely avoid the requirement to patch a critical system by creating an illogical plan with unreasonable milestone dates. The need to wait for a scheduled outage at a field asset is well understood. Allowing an entity to determine patches will only be installed when the control center server is replaced (typically every four years), as has been seen during a CIP audit, is unreasonable and poses significant risk to the reliability of the BES. This requirement does not require compensating measures appropriate to the vulnerability to be put into place until the patch is installed, thus furthering the potential risk. In effect, the provisions of this requirement have the potential of creating a paper exercise with little value, with an expectation that the CIP auditor simply accept the documented plan without comment. (3) Requirement R2, Part 2.4 furthers the inaction of the Responsible Entity by requiring the entity to follow the potentially illogical plan that the entity designed to avoid having to patch in the first place. As long as an extension of the plan is not required, there is still no CIP Senior Manager or delegate approval required. (4) Requirement R3, Part 3.1 requires the Responsible Entity to "deter, detect, or prevent" malicious code. As written, the entity has a choice of options, including an option to simply detect with no timeframe boundaries for when or how often the detection process must run or for monitoring the detection process itself. Simply detecting malware potentially places the BES at risk. The risk is mitigated proportionate to the time elapsed between the actual compromise, the detection, and the realization that malware has been detected. (5) Requirement R3, Part 3.3 requires the anti-malware updating process to address testing of the signature or pattern file. This requirement needs to be clarified. A number of Registered Entities have taken the position in the past that they address this aspect of the existing CIP Version 3 requirement by relying upon the vendor to test before release. (6) Requirement R4, Part 4.2 needs to be clarified whether the alert needs to be generated in real-time with automatic notification or if the alert can be generated by a long after-the-fact manual review of security event logs. (7) RequirementR4, Part 4.3 needs to be clarified whether original source logs must be retained or if post-log analysis summaries are sufficient. (8) Requirement R4, Part 4.4 needs to be clarified that the review of a summarization or sampling of logs is not acceptable as the primary means of log analysis and alert generation. The purpose of the manual review is to achieve a level of comfort that the log analysis tool is properly configured and is not missing important security events. A random sample review of logs otherwise runs a significant risk of completely missing security events that pose potential risk to BES reliability. (9) The term "generic account types" used in Requirement R5, Part 5.2 is not defined and has not been well understood to date by Registered Entities. (10) Requirement R5, Part 5.4, needs to be clarified that it pertains to active user accounts. There is no value to changing a password for an inactive or disabled user account until such time as the account is enabled. The requirement should also be clarified to require the initial password change prior to placing the BES Cyber Asset into service. (11) Requirement R5, Part 5.5 is limited to "password-only" authentication. The scope is too narrow and needs to include any use of a password for interactive access, even if part of a multi-factor authentication. This also needs to include user accounts that are capable of being used interactively even if the intended use is only programmatic (e.g., an FTP account). (12) Requirement R5, Part 5.7 should be clarified to establish an upper bound (or maximum number of attempts) to generate an alert or initiate an account lockout. CIP-008-5: (1) Requirement R2, Part 2.1 needs to be clarified whether a Cyber Security Incident response plan with multiple scenarios requires each scenario to be tested at least once per calendar year. (2) Requirement R2, Part 2.2 suffers a "catch-22." The requirement expects use of the Cyber Security Incident response plan when responding to a Reportable Security Incident, however execution of a step in the Cyber Security Incident response plan is required in order to determine if the incident is reportable. CIP-009-5: (1) Requirement R2, Part 2.1 needs to be clarified whether a recovery plan with multiple scenarios requires each scenario to be tested at least once

every 15 calendar months. (2) Requirement R2, Part 2.2 requires a “representative sample” of information used to recover BES System functionality to be tested. This requirement needs to be clarified. Does the requirement apply to only some or every Cyber Asset comprising a BES Cyber System? What is the minimum expectation of “representative sample?” Would a single file be sufficient, or is a partial or full restoration required (e.g., for one of multiple operator workstations)? (3) Requirement R2, Part 2.3 needs to be clarified whether a recovery plan with multiple scenarios requires each scenario to be tested at least once every 36 calendar months. CIP-010-1: (1) The term “active vulnerability assessment” used in Requirement R3, Parts 3.1, 3.2, and 3.3 needs to be formally defined. While the accompanying guidance attempts to define the use of the term, the guidance is not binding and is not auditable. (2) A paper vulnerability assessment, basically a documentation review, does little if anything to identify vulnerabilities present on a BES Cyber System. This requirement represents a significant step backward from the cyber vulnerability assessments required under the Version 3 CIP standards. CIP-011-1: (1) Requirement R1, Part 1.2 needs to be clarified to ensure protection and secure handling of BES Cyber System information when in transit both electronically and physically. For example, the entity should be required to protect such information when the media it resides on is being shipped by commercial carrier to a new location.

While certainly a major step in the right direction, many requirements provide no boundaries of acceptability, thus making any compliance audit highly subjective. No doubt, the auditors are qualified to subjectively determine when compliance is “good enough” but entities will likely disagree. This is going to cause significant issues down the road when the standards go into effect and compliance must be demonstrated.

Individual

Nazra Gladu

Manitoba Hydro

We don’t support certain requirements with comments as follows: Global comments: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies…” is difficult to interpret and therefore creates uncertainty as to what is required. The Background section of the standard indicates that the SDT intended the phrase to be aimed at “deficiencies in the implementation of certain requirements”. However, it is inconsistent to require “implementation” in a manner that does not require implementation, leaving the interpretation of this standard unclear. It also appears that the SDT did not want implementation failures to constitute violations. However, as drafted, the standard can still be interpreted to require an entity to implement its processes. It simply places an additional obligation on a Responsible Entity to detect and correct implementation failures. If the SDT wishes to eliminate violations for failure to implement a process, then there should be a separate requirement to detect, assess and correct deficiencies in implementation. Attachment 1 1.2-2), 1.3 & 1.4: It is not reasonable that a control center is classified as (H) High Impact Rating asset if it controls one Medium Impact Rating assets as defined in Section 2. As written, e.g., if a utility Control Center only controls a single Medium Impact Rating transmission or generation asset and one Low Impact Rating transmission or generation asset, its Control Center becomes a (H) Control Center that has the same classification as a large Transmission Operator Control Center facility! We suggest changing from “includes control of one or more of the assets...” to “includes control of two or more of the assets…” in Section 1.2-2), 1.3 and 1.4. Attachment 1 1.4: It is not reasonable that the GOP control centre has different MW threshold from the BA control centre. We suggest rewording 1.4 as following: “Each Control Center or backup Control Center used to perform the functional obligations of the Generation Operator: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.” Attachment 1 2.5: We suggest the following rewording the first sentence for increased clarity: “Transmission Facilities operated between 200 kV and 499 kV if the BES Transmission Lines that are operating between 200 kV and 499 kV at a single station or substation have an "aggregate weighted value" exceeding 3000 according to the table below and the single station or substation is connected to three or more other Transmission stations or substations that are each operating between 200 kV and 499 kV.” Attachment 1 2.9: Please clarify what is called “automated switching System” and why the ‘System’ is capitalized. Attachment 1 Section 3: The numbering 4.1-4.3 should be changed to 3.1-3.3. CIP-003-5: R1: Requirement R1 does not achieve its objective of ensuring that a cyber-security policy is kept” up to date” (as stated in the preceding rationale) as it only requires a Responsible Entity to periodically review the policy, but not revise the policy if it does not reflect actual practice. Furthermore, if the review of a policy every 15 months was intended to allow a Responsible Entity to revise a policy after changes in practice have already occurred, this implies that policies need not always be” up to date”. It also implies that Responsible Entities need not implement their actual policies as worded, which creates conflict with the intent, if not the requirements of R2 which still refers to a Responsible Entity “implementing” its policies. R2: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. R2 also references a review without requiring any action as a result of the review, as discussed for R1. R4: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. Also, the words “and updated” in R4 should be removed. It is not clear how or why an initial delegation would be “updated” within 30 days of the initial delegation if no changes are made to the delegation. We suggest changing the wording to read “…updated within 30 calendar days of any change to the delegation…” CIP-004-5: R2: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. R3: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. For clarity and to be consistent, a Part 3.6 analogous to CIP-004-5 R2 Part

2.2 should be added to CIP-004-5 Table R3. Currently R3 Parts have no clause to require that a PRA must be complete before granting access. Also R 3.5 should include a clause that it is subject to applicable law and collective bargaining unit agreements. We suggest adding Part 3.6 as the following: “Require completion of a PRA specified in Part 3.1 to 3.4 and in accordance with applicable law and collective bargaining unit agreements prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.” R3.1: It should clarify whose identity requires confirmation. R3.5: It does not meet the intent of 3.1 “Specified that identity confirmation is only required for each individual’s initial assessment” as the part specifies 3.1 to be completed every 7 years according to “Parts 3.1 to 3.4 within the last seven years”. We suggest rewording as follows: “Require completion of a criminal record check specified in Parts 3.2 to 3.4 for all individuals with authorized electronic or authorized unescorted physical access at least once every 7 calendar years.” R4: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. R 4.1: The phrase “based on need, as determined by the Responsible Entity” does not seem to add anything meaningful to the standard. The SDT should consider removing this phrase. R4.3: It is assuming an aspect (role-based privilege management) that has not been established nor defined in R4.1. We suggest either removing the phrase “and their specific associated privileges” from R4.3, or adding language regarding privilege levels in R4.1. R 5.1: Use of the phrase “termination action” could be interpreted to mean giving notice to terminate. Accordingly, for establishing the deadline by which a removal must be done, we suggest change the wording “termination of action” to “the effective date of the termination”. R5.3: The word “action” should be deleted from the last portion of the requirement. We suggest wording “the next calendar day following the effective date of the termination”. The phrase “and time” is unnecessary, given the reference to a calendar day rather than a twenty-four hour period. R5.4: Similarly, the word “action” should be deleted. CIP-006-5: R1: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. R1.5: The words “of the unauthorized access” should be added to the end of the sentence. R1.7: “detected” should be added in front of “unauthorized access” in the fifth line. R2: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. R2.2: It is unclear as to the time frame for this logging. Is the logging over a 24 hours period, during one business day, over the length of the visit (i.e. if someone is visiting for 3 days and coming and going each day)? We suggest putting a 12 hr timeline for last exit or “the last exit prior to leave the facility”. CIP-007: R1: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. R2: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. R3: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. R3.2: The word “identified” in the requirement is ambiguous and inconsistent with other malicious code phrases. We suggest changing to “detected”. R4: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. R4.5: To be consistent with other requirements, “15 days” should be changed to “15 calendar days”. R5: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. R5.4: The word 'known' is ambiguous - known to whom? Actual knowledge or ‘should have known’, ‘could have known’? For clarity, we suggest changing “known default passwords” to “knowable default passwords". CIP-008-5: R1.2: This needs clarification. Does notification to ESISAC occur only if an identified Cyber Security incident is determined to be a Reportable Cyber Security incident? Also, it’s not clear whether the one hour time line starts running at the identification of an identified Cyber Security incident or at the determination of that incident as reportable? Furthermore, there is no explanation of what a ‘preliminary notice’ is, is there a later final notice, etc. R2.1: “at least once every calendar year, not to exceed 15” is not consistent with the wording of other requirements. We suggest re-wording to read “at least once every 15 months”. R3.1 and R3.2: The wording needs to be rearranged to read better - the words 'No later than 90 calendar days after' should be added at the start of the sentence and deleted from the end. CIP-009-5: R1.2: This talks about 'responders' with no description or definition of who fits this category. R2: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. R2.1: The words 'between tests of the plan' are not needed. R3.1 and R3.2: The wording needs to be rearranged to read better - the words 'No later than 90 calendar days after' should be added at the start of the sentence and deleted from the end. CIP-010-5: R1: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. R1.1: We suggest adding the words 'for each Cyber Asset' to the first line after configuration. R1.5.1: The comma after 'minimizes adverse effects' doesn't make sense, this should be 'and'. R2: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. R3.2: The requirement interchanges the words "assessment" and "test". It is recommended that one word be used consistently so there is no confusion as to what is intended. R3.4: It refers to an action plan that there has been no earlier requirement to prepare or develop. The requirement needs to specifically require that one be prepared. CIP-011-5: R1: Use of the phrase “implement in a manner that detects, assesses and corrects deficiencies” creates interpretational problems as explained in the global comments. Definitions: BES Cyber System Information: Regarding “not publicly available”; as currently worded, if information about the BES Cyber Systems, PACSs and EACMs is made publicly available, it is not BES Cyber System Information and would not require protection There is a potential that sensitive information could be made public

and outside the scope of the definition. Control Centre: Suggested wording to improve clarity: “One of more facilities that host operating personnel who monitor and control the Bulk Electric System (BES) in real-time. These operating personnel perform the reliability tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generation Operator for generation Facilities at two or more locations. Control Centre facilities include associated data centers.” CIP Exceptional Circumstance: This definition needs appropriate punctuation to separate the items in the list. The suggested definition is: “A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.” External Routable Connectivity: We suggest replacing "its" with "the BES Cyber System" for additional clarity. Interactive Remote Access: The sentence "Remote access can be initiated from: ... contractors and consultants." is guidance information, and restricts the definition to only applying to Responsible Entity Cyber Assets, employees, vendors, contractors, and consultants. By definition, this would exclude interactive remote access by anyone else (public, non-legitimate users) from scope. We suggest removing the last sentence and providing this information in a guidance document. Reportable Cyber Security Incident: Remove this definition and address in a standard(s). Reporting obligations should be in a standard, not in a definition. Physical Security Perimeter: Protected Cyber Asset is missing from this PSP definition, otherwise CIP-006-5 won’t apply to PCA. Implementation Plan: 1. Under the heading “Proposed Effective Date for Version 5…”, there is a statement that “Notwithstanding any order to the contrary, CIP 002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this Implementation Plan.” This statement should either be stricken or at least confined to FERC orders. NERC does not have the legal authority to usurp regulatory orders, or other government approvals in Canadian jurisdictions, through publishing an implementation plan. The only possible exception is where the regulator itself (such as FERC) approves the implementation plan through issuing an order, usurping its previous orders. Since Canadian jurisdictions do not have regulators that issue orders approving implementation plans, this cannot be accomplished in Canada through an implementation plan. 2. In the section regarding periodic performance of certain requirements, NERC proposes to impose certain requirements before or on the effective date of a standard. Again, this goes beyond NERC’s legal authority. If a government or regulatory body determines an effective date for a standard, NERC cannot compel performance prior to that effective date. With respect to the imposition of certain periodic requirements on the effective date of a standard as well as periodically, the specific standard must be revised to include an additional requirement to perform that requirement on the effective date. An Implementation Plan is not a standard.

Individual

Andrew Z. Pusztai

American Transmission Company

Individual

Silvia Mitchell

NextEra Enregy

The drafting team has done an excellent job of improving Version 5 (V5) while also addressing many of FERC’s Order 706 suggestions in the face of divergent industry views and points of emphasis. NextEra Energy, Inc. (NextEra) is voting Affirmative on CIP-002-5, CIP-003-5, CIP-005-5, CIP-008-5, CIP-011-5, and Definitions, while voting to Abstain with comments with respect to CIP-004-5, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-5, and the Implementation Plan. NextEra voters will reconsider Abstain positions on these 6 items (either for another successive ballot or upon a recirculation ballot) if: (a) the zero defect fix language (“in a manner that identifies, assesses, and corrects deficiencies” (the IAC Language)), which is applicable to 66 different requirements in draft 3 of V5, is supplemented, revised and/or better clarified; and (b) the Implementation Plan is improved, both as further described below. With respect to (a), the draft RSAW for CIP-006-5 is a welcome gesture and a step in the right direction, but it is flawed, insufficient, and does not change the fact that the IAC Language used in the standard is ambiguous and untested. The IAC Language does not explicitly address the issue of whether and, if so, when internally identified and corrected deficiencies constitute violations of the standard’s requirements. The proposed RSAW language regarding “deficiencies” and “self-reporting” does not adequately resolve this ambiguity; if anything, it further muddies the water. It is unclear to NextEra whether any amount of verbiage in an RSAW can cure ambiguity flowing from the standard language itself. With respect to the words chosen, by prefacing the IAC Language with the phrase “in a manner that,” which is itself prefaced by the words “shall implement,” the requirement has become more, not less, rhetorically prescriptive. This is a step in the wrong direction, as NextEra and others were hoping the language chosen would not be in the form of an additional command, but would simply give their cyber security staff the freedom they need to develop robust internal correction programs, especially for high-volume, periodic activities. For companies like NextEra that operate in multiple NERC regions, the prospect of inconsistent and un-coordinated compliance evaluations raises serious concerns about whether the IAC Language could be applied and utilized in different ways across the country. To prevent this vacuum of ambiguity from being filled with negative unintended consequences, NERC must find an expeditious way to modify, clarify, or at least standardize the interpretation the IAC Language. One option is the insertion of an addendum to V5 between the

putative approval of draft 3 on October 10, 2012 and the final recirculation ballot that must be held before the new standard is ripe enough to forward on to the NERC BOT. Such an addendum could be narrowly focused on soliciting stakeholder input and consensus regarding ways to modify, interpret and/or clarify the IAC Language in a way that makes sense for all stakeholders. NextEra's specific suggestion for improving the IAC Language is to strike the entire phrase, then insert a new, longer sentence fragment at the end of the current sentence: "[Each Responsible Entity shall implement one or more documented physical security plans that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan], provided that internally identified deficiencies that are documented, assessed, and corrected if necessary as determined by the Responsible Entity, shall not constitute per se violations of this R1." The generic use of the legal phrase "per se" is a potentially promising way of addressing the violation issue directly in the standard itself. With more explicit, robust language in the standard, it would be easier for industry and NERC to facilitate a broader shift to risk-based auditing based on internal controls. To that end, in addition to changes to the standard itself, NextEra supports the following RSAW language for CIP standards with IAC Language: "Where the entity is identifying, assessing, and correcting its own deficiencies, the entity is satisfactorily performing the requirement." Also please consider this language for the RSAWs: "R1 Absent a possible violation that resulted in (or could have resulted in) a significant risk to the Bulk Electric System, no violation of R1 and its subrequirements shall be found, provided that the Responsible Entity has implemented a process for identifying, assessing, and correcting deficiencies with adherence to the items specified in Requirement R1." Moving to a new topic, item (b) above, NextEra has voted to Abstain with respect to the Implementation Plan for the following reasons. The Implementation Plan fails to specifically say that NERC will ask FERC to suspend the April 1, 2014 effective date for Version 4 (V4) when it submits V5 for FERC approval prior to March 31, 2012. Without suspension of the V4 effective date, NextEra is among those that will be forced to follow a parallel and costly approach to sustaining compliance to Version 3, implementing V4 by April 1, 2014 for newly identified Critical Assets, and implementing V5, which eliminates the term Critical Assets, for its presumed effective date of July 1, 2015. The current plan is a recipe for costly stranded costs that do not improve reliability. The drafting team can and should address this important problem in the Implementation Plan. Alternatively, NERC can and should ask FERC to move quickly to approve V5 once it is submitted for approval, or at least move quickly to suspend the effectiveness of V4 pending FERC's review of V5. In addition, NextEra believes the line between planned and unplanned changes is not always easy to maintain and there may be times it is appropriate to let a planned change become fully compliant at some time after the cyber system is commissioned. Similarly, after initial implementation of V5, there is an inadequate amount of time allotted for the implementation of the V5 Standards for BES Cyber Systems that go from the "Low" to "Medium" or "High" impact categorization based on unplanned enhancements and improvements to facilities. Responsible entities should be given 18-24 months, not merely 12 months, to comply, as many of the compliance activities can only be accomplished during planned outages at generation facilities. NextEra also finds the section on Initial Performance of Certain Periodic Requirements to be confusing and unnecessary and urges the drafting team to strike it or qualify these timing recommendations as proposed guidance, rather than a mandatory directive for all Responsible Entities to follow. If the section must remain, NextEra suggests it allow for an alternative timing option for periodic requirements that pegs all of the V5 requirements to the Effective Date and lets the Responsible Entity begin meeting the periodic items as they arise naturally in accordance with the CIP standards' periodic requirements.
NextEra thanks the drafting team for its hard work and the improvements it has made to Version 5.
Individual
Patrick Brown
Essential Power, LLC
1. Definitions - all standards Control Center: We believe that control centers require an appropriate level of protection for the bulk electric system and its components as identified in the FERC Orders 761 & 706. We also understand the expectation of "comprehensive protection of all control centers and control systems as NERC works to comply with the requirements of O-706". However, we urge the Drafting Team to establish appropriate levels of impact (High, Medium & Low) through the application of a 1500 MW generation and 1000 MVAr bright-line thresholds. This would be applied to Transmission Operator Control Centers where their impact would be minimal and would be consistent with the application of the generation and balancing authority bright lines as found in the Medium impact section of CIP-002-5 Attachment 1. Associated data centers: 'data centers' is not a defined term. The SDT should define the term, or add a statement that entities must define the term for themselves. 2. CIP-003 Background & all standards where the language is used Zero Defect/Internal Controls language: Although we fully support the implementation of Internal Controls as part of NERC's Reliability Based Standards initiative, it is unclear how this will be applied in practice. For those of us registered in multiple Regions, there is some concern regarding consistent application of this concept.
Individual
Tom Washburn
FMPP
Group

Wisconsin Electric Power Company NCR00951
Steve Karolek
CIP-002-5 “bright line criteria” #2.3, which states “2.3 Each Generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year” presents uncertainty and challenge to the industry. Unlike criteria 2.1, 2.2, 2.4, 2.5, 2.10, 2.11 and 2.13, all of which include specific measurable thresholds, criteria 2.3 relies on notification from a Registered Entity who is not subject to the CIP standards (none of the CIP standards are applicable to the PCs and TPs) related to a theoretically possible cascading islanding of firm load in a planning study of possible future conditions. The standard does not include any requirements specifying how we would document that we have or haven’t received such notice or worked with our PCs and TPs to determine if they have run any such studies. The standard does not include any requirements relating to the inputs and assumptions of any such studies, and the standard does not include any indication of what amount of firm load islanded represents an Adverse Reliability Impact. The criteria would be enhanced significantly with the inclusion of an applicability threshold of at least 300mw (analogous to the firm load control threshold in criteria 2.10 related to dropping firm load under UFLS or UVLS controls) and the standard would be enhanced with the addition of requirements providing direction on what type of compliance artifacts would be appropriate to demonstrate compliance with the notification aspects of the criteria. CIP-002-5 through CIP-009-5, CIP-010-1 and CIP-011-1 all contain boilerplate applicability language in section 4.2.2 which could be read and interpreted so as to exclude certain Registered Entities including RC, BA, LSA, IA and possibly others, from mandatory compliance to the NERC CIP standards requirements due to their not having any “BES Facilities”. Since section 4.2.2 does not appear to serve any specific purpose, our recommendation is to remove it from all of the draft CIP standards in order to eliminate the potential confusion and misinterpretation.
Individual
Don Jones Jones
Texas Reliability Entity
We are voting “no” on proposed standard CIP-010-1, because in Requirement 3 it is not clear regarding what comprises a complete and documented vulnerability assessment. This important requirement is subject to broad interpretation and too much subjective judgment. We recognize the attached guidelines provide elements that entities are “strongly encouraged” to include in a vulnerability assessment, but without mandatory elements or a clear definition we feel that this requirement may allow reliability gaps to exist.
The identify, assess, and correct (IAC) approach used in these standards does not require any interim reporting of deficiencies, or their frequency and severity. As the Compliance Enforcement Authority, we are concerned that with no timely information about deficiencies that occur we are not able to monitor an entity’s compliance with its own IAC process and the effectiveness of that process. For example, repeated deficiencies may indicate that the entity’s corrective actions are not effective, or that other mitigating measures need to be taken. We suggest adding a reporting process to provide information about an entity’s use of its IAC process (including identified deficiencies) between formal audits.
Individual
John Souza
Turlock Irrigation District
Individual
Rich Salgo
NV Energy
I will be voting affirmative for both of the Standards for which problems are noted below; however, I believe these two issues bear addressing by the SDT. CIP-002-5 Attachment 1 section 2.4: In this section, medium impact is assigned to Transmission Facilities operated at 500kV or higher. In the previous comment period, NV Energy noted that we believe an exclusion is warranted for distribution stations that are situated at the receiving end of a radial 500kV line. Specific instances exist of 500/69kV stations whose only purpose is to provide distribution service. In light of the SDT's clarification within 2.4 to specifically exclude collector buses for generation plants, we believe it is even more compelling that such an exclusion be given for receiving stations having 500kV or higher source voltages. Our review of the SDT's consideration of comments for the 2nd posting revealed no mention of this prior comment, while our understanding is that all negative comments received were owed a consideration through the Standards Development Process. CIP-004-5 R3.1 Under the parent requirement R3, the entity is to implement a risk assessment program to attain AND retain authorized access. Identity confirmation is one of the program elements, and it is prescribed in Part 3.1. However, the Change Rationale section for Part 3.1 states that it was specified that ID confirmation is only required for each individual's initial assessment. This change rationale would therefore indicate that ID confirmation is not required for retention of access, but only for the attainment of initial access. The SDT should address this inconistency and clearly indicate whether ID confirmation is required at the initial attainment of access, or for both attainment and retention of access.

Individual
Michael Mertz
PNM Resources
Minor recommended edits: CIP-008: Recommend changing 1 hour reporting window to 24 hours to align with EOP-004 CIP-010: R1.4.2 can be interpreted to mean “in production”, clarification recommended
Individual
Annette Johnston
MidAmerican Energy Company
MidAmerican Energy Company voted affirmative for all ballots. Specific, important items we do not support are detailed in question 2. Lack of clarity and/or transparency are the specific reasons for not supporting these items. Changes to clarify these items for a recirculation ballot to achieve the draft 3 intent are possible without being significant.
The following comments improve transparency and/or clarity of intent without being significant changes. (1) Zero defect: Add the following to requirements that include the “in a manner that” language: “Where the entity is identifying, assessing, and correcting its own deficiencies, the entity is satisfactorily performing the requirement.” (2) High water marking: Per the Guidelines and Technical Basis for CIP-005-5 R1, all of the Cyber Assets and systems, even other BES Cyber Systems of lesser impact, within the ESP will be elevated to the level of the highest impact BES Cyber System present in the ESP. This vital concept should be included in section 5 Background of every standard, not just in CIP-005 guidance. (3) ERC: This concept is included in section 5 Background of standards, “This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.” This vital concept should be included in the definition of External Routable Connectivity and include “ERC” as an acronym in the glossary. (4) 004 and 007 accesses: Issues with lack of understanding and inconsistent implementation have been identified for authorized access list and specific rights reviews in versions 1-3 CIP-004 R4, CIP-003 R5 and CIP-007 R5. We are concerned that CIP-004-5 R4.2 and R4.3 quarterly and annual verifications are predicated on some generalizations and/or assumptions that are not complete and will not sufficiently resolve the existing issues. And as drafted, an entity has to infer or assume from CIP-004-5 R4.4 that storage location accesses are not included in R4.2 or R4.3. Additionally, CIP-007-5 R5.2 and R5.3 will exacerbate the issues in CIP-004 R4.2 and R4.3. CIP-007-5 R5.2 and R5.3 can be achieved most effectively by consolidating them in CIP-004-5 R4 to eliminate redundancy, double jeopardy and improve clarity. Access authorizations and provisioning warrant further clarity in the recirculation ballot because they require significant resources, involve extensive complex data and are among the most currently violated requirements. We respectfully request reconsideration of the issues and the constructive solutions we offered to the drafting subteam for draft 3.
Individual
Steven Powell
Trans Bay Cable LLC
Comments with negative vote to CIP-002-v5 The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. The stated Purpose of the Standard CIP-002-5 as proposed is: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. TBC comments that it is not clear to our organization that certain provisions within this proposed Standard stand up to the test of commensurate with the adverse impact that loss, compromise, or misuse could have on the reliable operation of the BES. Using the stated Purpose statement as the measure during our final review of the proposed Standard and the accompanying definition of Control Center, TBC was not able to support an affirmative vote as outlined below: Criterion 2.5: It does not appear to TBC that the SDT has considered adequately the nuances of Direct Current facilities (at least those owned and/or operated by entities that are not part of a much larger integrated AC network that fall under any new “Control Center” definition by default) and the design and capabilities of such facilities when applying the attributes of the NERC “Integrated Risk Assessment Approach – Refinement to Severity Index” to DC facilities. The terminal voltage of a DC facility is not the driving factor of the severity of the risk to the Bulk Electric System rather it is the overall capability of the fully controllable system and the risk of compromise to that level. It is the opinion of TBC that a better approach to measure risk to the BES for DC facilities should be in parallel with what the SDT proposes for generators in criteria 2.11 and 2.13; Reasoning: DC systems are modeled almost exclusively in wide area models as a load at the source, and a source (generator) at the delivery point. For example a controller of two geographically and electrically diverse DC facilities with 345KV terminals capable of 700Mw each is to be scored to a weighted valued of 5200 under the proposal and therefore receive a Medium Impact Rating (if operated from a single control room or Control Center), compared to an owner/operator of two separate generators, rated at 700Mw each, and again in geographically and electrically diverse areas to be ranked at Low Impact. Or alternatively, a superior approach for DC facilities in which it is required to apply NERC Planning Category C or D

risk assessment to these facilities in aggregate; Reasoning: A single DC facility, if compromised is currently a NERC Category B contingency and therefore not a risk to the BES or IROL. If multiple DC facilities have common control points whether via control room, or “Control Center” the study of the area impact of the compromise of all DC facilities under the common control point is technically feasible and should be allowed by Standard rather than the proposed and inferior “Integrated Risk Assessment Approach” used as a proxy for the importance of AC facilities. Proposed Definition of “Control Center” In addition to our concern with the approach used in criteria 2.5, during our review and decision process regarding a positive or negative vote for CIP-002 v5 there were two items that we were not able to find consensus of meaning or any interpretation on to support a positive vote: • TBC needs clarification of what is meant by the term “associated data centers” as used in the proposed definition. • TBC needs clarification of what is meant by the term “locations” as used in the proposed definition.
Proposed Definition of “Control Center” In addition to our concern with the approach used in criteria 2.5, during our review and decision process regarding a positive or negative vote for CIP-002 v5 there were two items that we were not able to find consensus of meaning or any interpretation on to support a positive vote: • TBC needs clarification of what is meant by the term “associated data centers” as used in the proposed definition. • TBC needs clarification of what is meant by the term “locations” as used in the proposed definition.
Individual
Guy Andrews
Georgia System Operations Corporation
no comment
GSOC appreciates the CIP V5 SDT time and effort on addressing industry’s issues with the CIP standards. GSOC is strongly supports the following NRECA comment: Internal Control Language and VRFs/VSLs – The inclusion of the language “Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, . . .”, commonly referred to as internal control language, is a significant change to the CIP V5 standards that was added very late in the development process of these standards. GSOC appreciates the SDT’s efforts to address zero-defect language in the standards and to propose a potential alternative. The concept of permitting a registered entity to address deficiencies with corrective actions without them becoming violations is one that many can support. However, adding this internal control language so late in the drafting of the CIP V5 standards raises significant uncertainty and confusion. Also of concern is the fact that the currently proposed VRFs and VSLs do not clarify what a violation looks like under the new approach. The language is also unclear on what is not considered a violation. The primary concern and source of confusion is how such a programmatic approach will be audited. In supporting the CIP V5 standard proposals, GSOC is taking a leap of faith that NERC leadership and staff will work carefully and collaboratively with industry to clarify the compliance component of this language to ensure that it addresses the targeted intent and does not create any additional compliance burdens to the current substantive compliance burden that exist today. GSOC supports the internal controls concept, but significant work is needed to help industry to understand and support the compliance obligations and enforcement measures around this concept. This work needs to be completed well before the CIP V5 standards become effective and auditing begins on the new provisions – assuming appropriate regulatory approvals are secured.
Individual
Brian Evans-Mongeon
Utility Services
Utility Services believes that the applicability section of the standard creates instances of where the intended CIP applicability is not consistent between functional registrations. In Section 4.1.2.4, Cranking Paths owned by Distribution Providers are applicable to the CIP standards. However, under Section 4.2.2, only BES Facilities are applicable to Transmission Owners and Transmission Operators. Since Cranking Paths are not necessarily BES Facilities by either today’s regional definitions or the proposed BES Definition, the applicability language in the standard would only make Cranking Paths owned by Distribution Providers subject to the CIP standards. Cranking Paths owned or operated by TOs or TOPs would not applicable to the standard unless they are part of the BES. Therefore, Utility Services asks the SDT to consider changing the applicability language in Section 4.2.1.4 to from "Each Cranking Path and group of Elements meeting the initial switching..." to "Each Cranking Path and group of Elements that are part of the BES and that meet the initial switching..."
Individual
William O. Thompson
NIPSCO
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
(Comment 1) MMWEC supports the comments submitted by NPCC. (Comment 2) Section 4.1.2.4 includes ownership of a Cranking Path as a criterion for applicability of the CIP standards for Distribution Providers. However, Transmission Owners may own Cranking Paths that are less than 100 kv and not necessarily part of the

BES. As written, the CIP standards would not apply to those non-BES Cranking Paths owned by Functional Entities other than DPs because section 4.2.2 specifies "All BES Facilities" for applicability to other Functional Entities. 4.1.2.4 should be changed from "Each Cranking Path and group of Elements meeting the initial switching..." to "Each Cranking Path and group of Elements that are part of the BES and that meet the initial switching..." Each region may identify Cranking Paths that are critical to the restoration plan and may use the BES exception process to classify those Cranking Paths as BES Facilities. CIP standards should apply to Cranking Path cyber systems that are part of the BES and that are owned or operated by any Functional Entity. Cranking Path equipment that Regional Entities do not classify as part of the BES would be exempt from the CIP standards, unless the equipment is included due to other criteria. This will be consistent with the concept of protecting BES Cyber Systems, provide consistency of applicability across all Functional Entities regarding Cranking Paths and clarify which equipment owned by DPs is subject to CIP standards.

Group

National Rural Electric Cooperative Association (NRECA)

Barry Lawson

NRECA very much appreciates the efforts of the CIP V5 SDT on addressing industry's issues with the CIP V5 draft standards. Many issues have been satisfactorily addressed; however, NRECA remains concerned with the criteria in CIP-002-5, Attachment 1, as it relates to TOPs. We believe it is appropriate for TOPs to be treated similarly to BAs and GOPs as far as how they are ranked in the High, Medium and Low Impact Rating categories. BAs and GOPs are ranked in all three categories based on specific criteria – TOPs should receive similar treatment. NRECA strongly recommends the following changes to CIP-002-5 Attachment 1 to ensure the fair and equitable treatment of TOPs that only control facilities operated at less than 200 kV (new language is in ALL CAPs): 1. Criteria 1.3 does not require any changes. 2. Criteria 2.12 should be revised to state "Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above, AND THAT CONTROLS TRANSMISSION FACILITIES OPERATED AT 200 KV AND ABOVE." 3. A new criteria should be added to the Low Impact Rating (L) section to state "EACH CONTROL CENTER OR BACKUP CONTROL CENTER USED TO PERFORM THE FUNCTIONAL OBLIGATIONS OF THE TRANSMISSION OPERATOR NOT INCLUDED IN HIGH IMPACT RATING (H) OR MEDIUM IMPACT RATING (M), AND THAT ONLY CONTROLS TRANSMISSION FACILITIES OPERATED BELOW 200 KV."

Internal Control Language and VRFs/VSLs – The inclusion of the language "Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, . . .", commonly referred to as internal control language, is a significant change to the CIP V5 standards that was added very late in the development process of these standards. NRECA appreciates the SDT's efforts to address zero-defect language in the standards and to propose a potential alternative. The concept of permitting a registered entity to address deficiencies with corrective actions without them becoming violations is one that many can support. However, adding this internal control language so late in the drafting of the CIP V5 standards raises significant uncertainty and confusion. Also of concern is the fact that the currently proposed VRFs and VSLs do not clarify what a violation looks like under the new approach. The language is also unclear on what is not considered a violation. The primary concern and source of confusion is how such a programmatic approach will be audited. In supporting the CIP V5 standard proposals, NRECA is taking a leap of faith that NERC leadership and staff will work carefully and collaboratively with industry to clarify the compliance component of this language to ensure that it addresses the targeted intent and does not create any additional compliance burdens to the current substantive compliance burden that exists today. NRECA supports the internal controls concept, but significant work is needed to help industry to understand and support the compliance obligations and enforcement measures around this concept. This work needs to be completed well before the CIP V5 standards become effective and auditing begins on the new provisions – assuming appropriate regulatory approvals are secured.

Individual

Linda Campbell

FRCC

Identify, Assess, and Correct Deficiencies The language of "each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies." is somewhat problematic. This language does not outline the timeframe an entity has between identifying and correcting a deficiency. Can an entity take 24 months to correct a deficiency? Probably not, based on auditor judgment. However, this type of language leaves a lot to be interpreted on both the RE and the entity sides. Additionally, there is no language that addresses the magnitude of a deficiency. For example, if an entity finds that they did not deploy a method to deter, detect, or prevent malicious code on all 15 of its firewalls (CIP-007-5 R3) for two years but then determines right before an audit that they missed this requirement, does this qualify for "identify, assess, and correct deficiencies?" What if they identified 5 of those 15 as not being corrected? Is there a breaking point in terms of quantity before a deficiency becomes a possible violation or a Self Report is required? As written, the requirement does not set ANY time limit for mitigating "the threat of identified malicious code." An entity that decided the mitigation will have to wait until an outage 2 years out will still be in compliance but the threat to the BPS is still there. Ports and Services CIP-007-5, R1.1: "If a device has no provision for disabling or restricting logical ports on the device, then those ports that are open are deemed needed." The requirement does not provide any provisions for limiting access to those ports or

services that cannot be disabled. The requirement's measures ask for host-based protective measures. For those devices that are not capable of providing localized protective measures, such as relays, there is a question as to how this requirement would be met. Previously, when a port or service could not be disabled, a TFE would require mitigation of the potential vulnerability. Under CIP-007-5, if the entity leaves these ports and services open they are in compliance but there is a question of whether the vulnerability of the device still remains. Summary To better protect the BES, there is an advantage to moving towards V5 and bypassing V4. NERC's Risk Based approach is also the way the rest of other industries tackle security management. Entities will benefit more from an audit that is risk based because it provides for a tailored approach and allow fine-tuning to take place. Like V3, the V5 objective is to apply security in layers (known by other industries as defense-in-depth approach) so that if one area is compromised or circumvented, at least another measure continues to provide protection. Is a layered approach a 100% fool proof? No, take for example CIP-005 ; it implements a series of security controls, however, this does not mean that by passing the audit the entity is not vulnerable by the way it has implemented the controls. As stated above there still remains wording in the standards that should be clearly defined to reduce number of interpretations and increase consistency across regions. We believe it is in these areas where NERC and the SDT should make sure they reduce or eliminate these wording interpretation challenges. CIP 5 is a much more robust and complex set of standards that will require more compliance and auditing resources for both the ERO and the entity. I will vote for approval as it does a much more thorough job than the present standards in protecting the Bulk Power System.

Individual

Oscar Herrera

Los Angeles Department of Water and Power

CIP-004 R5.2 – The time limits for revoking access upon terminations and transfers being proposed for the next calendar day present extreme challenges. More time needs to be given. The next business day for terminations and 3 business days for transfers will make these processes manageable. The following additional requirements may be onerous compared to the benefit received: •Required IDS/IPS for firewalls •Encryption between links •Multi-factor authentication for remote access AND encryption CIP-006 Part 1.6 – A responsible entity needs to monitor each PACS system for unauthorized physical access to a PACS. However, there is no requirement that the PACS be contained within a PSP. Therefore, how does one control physical access to the PACS? CIP-006 Part 1.7 requires to issue an alarm or alert in response to detected unauthorized physical access to a PACS to personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the unauthorized physical access. However, CIP-008 does not include the PACS in the Cyber Security Incident Response Plan. CIP-006 Part 1.3 requires two or more different physical access controls… which is overkill. This presents technical challenges and may not create additional security. One control should suffice. Depth of defense already exists through gates, security personnel and card reader systems. The current requirement of one or more physical access methods has been implemented with little or no problems encountered. The increase to two or more physical access controls may bring about unintended consequences and complexity. NERC should provide compliance feedback to industry demonstrating that "one or more" physical access methods have proven ineffective. Additionally, High Impact Control Center typically already have stringent physical security controls and monitoring CIP-006 Part 2.2 would require manual or automated logging of entry and exit from the physical security perimeter. The requirement for egress has not been explicitly defined as a requirement. Preference is for ingress logging only. An egress requirement has been alluded to in the requirement. Access controls for egress presents a number of safety issues and concerns. CIP-007 Part 4.2 states that an entity needs to generate alerts for security events that the entity determines necessary. An entity defined security events seems like a questionable and subjective requirement. Further, although not explicitly stated in the standard, the guidelines and technical basis attachment suggests that R4.2 be in real-time and this may be an issue. CIP-009 Part 2.1 states that the entity is to test the recovery plan(s) every calendar year, not to exceed 15 months. Part 2.3 seems to be a facsimile of 2.1, yet adds a longer timeframe for compliance. We need clarification on the timeframes, as there may be overlap between the two activities. Furthermore, there needs to be clarification or additional guidance for the types of operational exercises the drafting team is requesting entities to perform per Part 2.3. CIP-010 Part 3.3 states that prior to adding a new Cyber Asset to a BES Cyber System, the entity is to perform an active vulnerability assessment of the cyber asset. It is problematic to perform an active vulnerability assessment prior to installing a new Cyber Asset. Furthermore, the term "Active vulnerability assessment" is not defined. Under the assumption that an "active vulnerability assessment" is the actual performance of an entities vulnerability assessment program, there are sufficient controls in place that would deem an "active vulnerability assessment" unnecessary, such as change management procedures. Therefore, we request that Part 3.3 be removed.

Individual

Thomas A Foreman

Lower Colorado River Authority

• In CIP005-5, R1.5, we propose the following: "Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. ESP-to-ESP communications within a discrete BES Cyber System shall be excluded." As an example, the communication links between a primary transmission control center and its backup control center shall be excluded. • For clarification, in CIP 007-5, R4.4,

in the requirements column of the table, the draft language indicates a need to review logs to “identify undetected Cyber Security Incidents.” Is this intended to be “identify detected Cyber Security Incidents?”

Individual

Kayleigh Wilkerson

Lincoln Electric System

Although supportive of the drafting team’s efforts and responsiveness in addressing our previous concerns, LES requests that the following concerns be considered prior to approval. CIP-002-5 R1: Recommend the 6 asset categories included as part of R1 be removed and the drafting team instead reference Attachment 1, if needed, to ensure consistency in language as well as prevent unnecessary duplication. CIP-002-5 Attachment 1-1.3: For Attachment 1-1.3 “Transmission Operator Control Centers”, LES believes additional thresholds should be included to better delineate High Impact from Medium to Low Impact Control Centers. Potential thresholds to include are as follows. (1.3). Each Control Center or Backup Control Center used to perform the functional obligations of the Transmission Operator for 4 or more of the assets that meet criterion 2.2, 2.4, 2.5, or 2.10; or for any asset that meets criterion 2.6, 2.7, 2.8, or 2.9. (2.12). Each Control Center or Backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2. 4, 2.5, or 2.10. CIP-002-5 Attachment 1-2.5: The total of the aggregated weighted values calculated should be divided by 2 to get a better representation of the impact to the BES for the loss of through flows. The number of lines should at least be increased to 4 or more to have at least a 2600 (MVA) aggregated weighted value impact to the BES. This would be more in line with the BA and GO bright-line thresholds. With only 3 lines at 300-499KV, an entity can only have a max through flow of 1300. When you only have 4 lines, the through flow increases to 2600 MVA (2 lines with flows in and 2 lines with flows out) Suggestion: Either take the Weight value per line and divide them in half: 200 kV to 299 kV 350 300 kV to 499 kV 650 Or as an alternate: 2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation that is connected to 4 or more other Transmission stations or substations and has “aggregate weighted values” exceeding 3000 according to the table below…..” CIP-005-5 Background Section: To ensure consistency between the standard and the list of “Definitions of Terms Used in Version 5 CIP Cyber Security Standards”, LES asks that the drafting team update the CIP-005-5 Background section to reflect the same definition as used in the list of definitions of terms. CIP-007-5 R2.1: The patch management process for substation or plant control systems could include security patches for Cyber Assets such as panel meters, relays, controllers, PLC's, and other electronic devices that are part of the BES Cyber System and do not have network connectivity. Recommend R2.1 and R2.2 be rewritten as follows to only include those assets that are connected to a network. (R2.1). For all Cyber Assets connected to a network via a routable protocol, the Responsible Entity has a patch management process for tracking, evaluating, and installing… (R2.2). For all Cyber Assets connected to a network via a routable protocol, at least once every 35 calendar days, evaluate security patches… CIP-007-5 R4.1: As currently written, R4.1 would necessitate the logging at every Cyber Asset that is capable when there is not a network at the BES Cyber System. As such, every Cyber Asset would be considered an access point. To prevent undue burden on registered entities, recommend R4.1 be rewritten as follows: (R4.1). For BES Cyber Systems that have Cyber Assets connected to a network via a routable protocol, log events at the BES Cyber System Level… CIP-007-5 R4.3: Recommend that the log retention requirements be included as part of the data retention portion of the standard rather than as part of the requirement. CIP-008-5 R1.3: Recommend removing R1.3 and leaving it to the registered entity’s discretion as to what information is to be included within the response plan(s). By creating an all-inclusive list of roles and responsibilities, an auditor could potentially question why certain roles or responsibilities were left out of the response plan or why particular individuals were granted certain roles or responsibilities (i.e. qualifications, experience…). If the entity has a Response Plan, that should be sufficient without needing an additional requirement for what should be included in the plan. CIP-008-5 R2.1: Recommend R2.1 be written to state that one Cyber Security Incident response plan would be sufficient for High Impact and Medium Impact BES Cyber Systems. Suggested wording includes the following: (R2.1). Test at least one High Impact and Medium Impact BES Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 months… CIP-008-5 R2.3: This requirement should be moved to the data retention portion of the standard. CIP-008-5 R3.2: As stated in R1.3, LES believes defining and listing individual roles and responsibilities as part of the Cyber Security Incident response plan(s) is needless administrative work and should be left to the discretion of the registered entity. If R3.2 is to be retained, recommend that at a minimum it be rewritten to remove R3.2.2 as well as the first paragraph and simply state the following: (R3.2). After an update to the Cyber Security Incident response plan(s) occurs, notify affected person(s) or group(s), not to exceed 60 calendar days. CIP-009-5 R1.2: Similar to comments made for CIP-008-5, LES believes R1.2 is an unnecessary administrative requirement that does not allow registered entities the flexibility to adapt and change their plan(s). If not removed, recommend that at a minimum, R1.2 be rewritten to state that an entity need only have responders in the event that the recovery plan(s) were to be activated. CIP-010-1 R1.1-R1.4: The requirements should only apply to networked Cyber Assets, otherwise a very labor intensive process will be needed for collecting and reviewing baseline configurations for numerous stand-alone electronic devices used in the BES Cyber Systems. Suggest adding the following statement at the beginning of each requirement: “For BES Cyber Systems that have Cyber Assets connected to a network via a routable protocol,…”. CIP-010-1 R3.4: Requirements 3.2 and 3.3 do not apply to Medium Impact BES Cyber Systems, however, R3.4 requires the entity to document the results of Parts 3.1, 3.2, and 3.3 for both High and Medium Impact BES Cyber Systems. To

ensure consistency with the individual Parts, recommend Part 3.4 Applicable Systems be modified as follows: -High Impact BES Cyber Systems (as it applies to Parts 3.2 and 3.3) and their associated:… -Medium Impact BES Cyber Systems (as it applies to Part 3.1) and their associated:…

Individual

Heather Laws

Portland General Electric Co.

n/a

DRAFT 3 - There are still several places where the details need to be cleaned up and consistent. See CIP-004 for the "and/or" and granting vs. provisioning inconsistancies in the rational, guidelines and even in the requirment and measures sections. Also very concerned that no where in CIP-006 does it say that you have to define a PSP. Is it just assumed? I don't think we can just assume.

Individual

Bob Thomas

Illinois Municipal Electric Agency

Individual

David Revill

Georgia Transmission Corporation

GTC appreciates the CIP V5 SDT's time and effort addressing industry's issues with the CIP standards. GTC supports the following NRECA comment: Internal Control Language and VRFs/VSLs – The inclusion of the language "Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, . . .", commonly referred to as internal control language, is a significant change to the CIP V5 standards that was added very late in the development process of these standards. GSOC appreciates the SDT's efforts to address zero-defect language in the standards and to propose a potential alternative. The concept of permitting a registered entity to address deficiencies with corrective actions without them becoming violations is one that many can support. However, adding this internal control language so late in the drafting of the CIP V5 standards raises significant uncertainty and confusion. Also of concern is the fact that the currently proposed VRFs and VSLs do not clarify what a violation looks like under the new approach. The language is also unclear on what is not considered a violation. The primary concern and source of confusion is how such a programmatic approach will be audited. In supporting the CIP V5 standard proposals, GSOC is taking a leap of faith that NERC leadership and staff will work carefully and collaboratively with industry to clarify the compliance component of this language to ensure that it addresses the targeted intent and does not create any additional compliance burdens to the current substantive compliance burden that exist today. GSOC supports the internal controls concept, but significant work is needed to help industry to understand and support the compliance obligations and enforcement measures around this concept. This work needs to be completed well before the CIP V5 standards become effective and auditing begins on the new provisions – assuming appropriate regulatory approvals are secured.

Individual

John Allen

City Utilities of Springfield, MO

City Utilities appreciates the changes made in the latest draft of CIP-002-5 to allow some BA Control Centers to be designated as Low Impact. However, we are continuing to vote negative on the Standard and ask the SDT to keep working to develop a bright-line for small TOP Control Centers that will allow them to properly be identified as Low Impact. If the next draft contains proper consideration for small TOPs, then we will vote affirmative in the next ballot period. City Utilities has worked with APPA and TAPS to provide options for the SDT to consider. City Utilities supports the comments submitted by these organizations.

Group

PacifiCorp

Ryan Millard

PacifiCorp is concerned: (1) with how CIP-002, Attachment 1 2.6 and 2.9, should be implemented within WECC due to the fact that IROLs have yet to be clearly defined by the RC and, once defined, may be short term in nature, making it very difficult to implement compliant CIPS programs that proactively identify all necessary BES Cyber Systems; (2) that the requirement for Responsible Entities to utilize two or more physical access controls, under CIP-006 R1.3, will be an increased expense and administrative burden for entities with only a minimal benefit to physical security; (3) that the short period between the effectiveness of approved Version 4 and advent of Version 5 requires fully revised CIPS compliance programs, making the back-to-back implementation of the different standard structures expensive and counter-productive. PacifiCorp recommends that NERC support an implementation approach whereby if Version 5 is approved, it would supersede Version 4 in its entirety. PacifiCorp

also recommends that the drafting team add an exclusionary concept to the definition of “External Routable Connectivity” so that Cyber Assets within a BES Cyber System that cannot be directly accessed through External Routable Connectivity would be expressly excluded from the definition, and add “ERC” as a defined acronym.

Individual

Linda Jacobson-Quinn

Farmington Electric Utility System

Individual

Southern California Edison Company

NERC Compliance Program

CIP 002 Attachment A Section 2.1 Please define “Commissioned Generation” Section 2.9 Please clarify how Attachment A Section 2.9 impacts entities with no IROLS? Attachment A Please clarify that since the term "associated data centers" has been removed from Attachment 1 in Draft 3, it should also be removed from the Guidelines and Technical Basis section: CIP 004 R5.2 Requirements Please clarify how to record the date that the entity determines that the individual no longer requires retention of access? CIP 007 Effective Dates …the effective date of the order providing applicable regulatory approval, and Requirement 5.2 shall become effective 12 months later, as to provide entities more time to identify and inventory all enabled default or other generic account types. R3.2 Applicability Revise to apply to Medium Impact assets with external routable protocol: “Medium Impact BES Cyber Systems with external routable protocol and their associated” R4.1 Requirements Revise to include the sentence from the guidance: …that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Individual

Joe O'Brien

NIPSCO

NIPSCO does not support the following definitions as proposed: a. BES Cyber Asset – The definition should reference “the items in Attachment 1” instead of “Facilities, systems, or equipment,” because “Facilities, systems, or equipment” is subjective and lends itself to differing interpretations, and Attachment 1 provides greater clarity and guidance on the criteria to define BES Cyber Assets. b. CIP Senior Manager – NIPSCO recommends modifying this definition to provide the clarification requested under RFI Project 2012-INT-06. Modify the definition to: “A single senior management official of a registered entity with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.” c. Cyber Asset – The proposed definition could be interpreted to require utilities to demonstrate consideration of – in addition to hardware – all software and data on each programmable electronic device, which would be impracticable and overly burdensome. NIPSCO recommends changing the definition to “Programmable electronic device.” d. BES Cyber System Information – The definition should include only BES Cyber System Information that is under the control of the responsible entity. e. Electronic Access Control or Monitoring Systems (“EACMS”) – The definition should not reference “Intermediate Device” because Intermediate Device is a uniquely defined term. f. Electronic Access Point (“EAP”) – The proposed definition is unclear. NIPSCO therefore offers the following suggested language: “A Cyber Asset interface to an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.” g. Electronic Security Perimeter (“ESP”) – The proposed definition is unclear. NIPSCO therefore offers the following suggested language: “The logical border to a network in which BES Cyber Systems are connected using a routable protocol.” h. Intermediate Device – NIPSCO recommends the definition change to remove “or collection of Cyber Assets.” This limits the scope to only those assets that are used directly in the access control to assets subject to the CIP standards, rather than the broader “collection of Cyber Assets,” which would include numerous cyber assets that an entity may deploy in a layered network architecture with numerous authentication points and isolation technology. i. Interactive Remote Access - NIPSCO recommends removing the 2nd sentence since the requirements specify the scope of applicability. The second sentence of the definition contains an applicability statement that is defining what remote access is not, and NIPSCO does not believe this adds any value to the definition and potentially introduces conflicts with specific architectures. j. Protected Cyber Assets – The proposed definition is unclear. NIPSCO therefore offers the following suggested language: “One or more Cyber Assets connected using a routable protocol within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter.” NIPSCO supports the Implementation Plan; however, recommends the removal of the Applicability Reference Tables as they do not appear to belong within an implementation plan document. NIPSCO does not support CIP-002-5 as proposed. The proposed language should be modified to specify that the applicable functional obligations referenced within R1.1 through R1.4, R2.11 and R2.12 apply to only those real time tasks identified in the Functional Model. NIPSCO also suggests that R1.3 be removed and that the Low categorization be eliminated. NIPSCO remains challenged with the approach of identifying the required Low assets within R1.3. The SDT has provided language to clarify that a discrete list is not required; however, NIPSCO seeks clarification on how an entity would demonstrate strict compliance with a requirement that directs an entity within the requirement to not create evidence. NIPSCO does not support CIP-003-5 as proposed. In R2, it is unreasonable to require an entity to

identify, assess, and correct the deficiencies of assets that it is not required to uniquely identify or inventory. NIPSCO seeks clarification on how an entity would demonstrate strict compliance with a requirement that directs the entity within the requirement to not create evidence. NIPSCO recommends removing this requirement. NIPSCO supports CIP-004-5 as proposed; however, NIPSCO recommends that the revocation periods for R5.3 and R5.4 be aligned to both be 30 days. Also, NIPSCO suggests that R5.3 should also apply to reassignments and transfers in addition to terminations and removal of access to BES Cyber Information. NIPSCO does not support CIP-005-5 as proposed. R1.3 should use the term “controls” instead of “permissions” to align with the measure language. Also, NIPSCO recommends changing R2.2 to “Interactive Remote Access sessions must utilize encryption to an Intermediate Device.” This would allow for termination of the encrypted communication at the VPN concentrator without the requirement to have encryption to every intermediary device along the path from the remote user to the BES Cyber Asset. Finally, NIPSCO recommends changing R2.3 to “Interactive Remote Access sessions must utilize multifactor authentication to an Intermediate Device.” This would allow for multifactor authentication to the VPN without the requirement to have multifactor authentication at every intermediary device along the path from the remote user to the BES Cyber Asset. NIPSCO supports CIP-006-5 as proposed NIPSCO does not support CIP-007-5 as proposed. R2.2: NIPSCO suggests changing the 35-days requirement to “monthly.” NIPSCO interprets the current requirement language as likely creating a rolling 35-day period for each individual BES Cyber Asset, and the triggering documentation presumably would need to be tracked individually to ensure that the task is continuously performed 35 days from the last time it was performed. Typical entity management programs would ensure that a task or set of tasks is completed within a month; however, the day of the month could vary based on holidays, vacations, system availability, and a number of other resource / process issues. The needed flexibility to manage our environments with a month-to-month time frame would be lost by moving to a prescriptive 35 day rolling window. For example, if an entity evaluated security patches for applicability for a set of systems on the 18th of October and then with the holidays in November they performed the task again on Nov 26th, it presumably would be out of compliance. Conversely, if the requirement stated “monthly” the entity presumably would be in compliance. Additionally, the tracking date of R2.2 has implications on the requirement date for R2.3. R2.3: If the SDT prefers to not use the phrase monthly, then NIPSCO recommends changing the requirement to 62 days. R2.3: NIPSCO suggests changing the 35-days requirement in R2.2 to “monthly.” NIPSCO interprets the current requirement language as likely creating a rolling 35-day period for each individual BES Cyber Asset, and the triggering documentation presumably would need to be tracked individually to ensure that the task is continuously performed 35-days from the last time it was performed. Typical entity management programs would ensure that a task or set of tasks is completed within a month; however, the day of the month could vary based on holidays, vacations, system availability, and a number of other resource / process issues. The needed flexibility to manage our environments with a month-to-month time frame would be lost by moving to a prescriptive 35 day rolling window. If the SDT prefers to not use the phrase monthly, then NIPSCO recommends changing the requirement to 62 days. R2.4: NIPSCO believes that the language in R2.4 should be aligned with the language in R2.3. Either both or neither should specify the approval requirement of the CIP Senior Manager or delegate. NIPSCO recommends “. . . timeframe specified in Part 2.3 is approved.” R3.1: NIPSCO believes that the use of the term “deter” is ambiguous and suggests removing the term from the requirement. R3.2: NIPSCO believes that the language used in the requirement is ambiguous. NIPSCO suggests replacing the language in the requirement to “Configure the measures implemented in R3.1 such that it blocks or prevents access to files with potentially harmful code.” This recommendation is based on the assumption that the recommendation for removal of the term “deter” is accepted in R3.1. R4.1: NIPSCO recommends changing R4.1.2 to remove “failed access.” The requirement would be “Detects failed login attempts.” R4.2: NIPSCO recommends changing the language of R4.2.2 to “Detected failed login attempts from Part 4.1.” 4.4: NIPSCO believes that the requirement is too ambiguous. It is unclear what would constitute a summarization or a valid sample. NIPSCO believes that the requirement to review ‘undetected’ Cyber Security Incidents is essentially a requirement to perform manual reviews. By requiring a manual review, the entities are encouraged to record the absolute minimum event types as to minimize the burden of the manual review. Further, the requirement to perform manual reviews would incentivize entities to not invest in systems that can perform automated log analysis and event correlation. 5.6: NIPSCO recommends that “. . . at least once every 15 calendar months” be replaced with “at least once each calendar year.” NIPSCO supports CIP-008-5 as proposed; however, NIPSCO recommends the following addition to the language of R1.2: “. . . Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from identification of the Reportable Cyber Security Incident.” This change adds clarity that the one-hour time frame begins when an incident is identified as a reportable incident. NIPSCO supports CIP-009-5 as proposed NIPSCO does not support CIP-010-5 as proposed. NIPSCO suggests that the 35-days requirement in R2.1 be changed to “monthly.” The requirement should state: “Monitor at least monthly for changes to the baseline configuration. . .” NIPSCO interprets the current requirement language as creating a rolling 35-day period for each individual BES Cyber Asset, and the triggering documentation would need to be tracked individually to ensure that the task is continuously performed 35-days from the last time it was performed. Typical entity management programs would ensure that a task or set of tasks is completed within a month; however, the day of the month could vary based on holidays, vacations, system availability, and a number of other resource / process issues. The needed flexibility to manage our environments with a month-to-month time frame would be lost by moving to a prescriptive 35 day rolling window. For example, if an entity performed a baseline review task for a set of systems on the 18th of October and then with the holidays in November it performed the task again on Nov 26th, the entity presumably would be out of compliance. Conversely, if the requirement stated “monthly” the

entity presumably would now be in compliance. If the SDT prefers to not use the phrase monthly, then NIPSCO recommends changing the requirement to 62 days. NIPSCO supports CIP-011-5 as proposed; however, NIPSCO notes a typo in R 2.2 in the “Measures” section at the first bullet, i.e., remove “a” prior to “an.”

NIPSCO believes the SDT has made significant improvement in the language and approach of the current V5 Draft 3. NIPSCO believes it is essential that the SDT continues on this path until industry approval is received in accordance with the Standards Drafting Process. These comments support the voting position of 4 NIPSCO voters in Segments 1,3,5,and 6.

Group

MRO NSRF

Joseph dePoorter

The MRO NSRF wish to make the following comments: CIP-002-5 R1 – For consistency and clarity, either remove the list of assets (1-6) and refer to the attachment or change R1.1 through R1.3 and R2.1 and R2.2to align the NERC filing in which NERC committed to using numbered or bulleted lists and which was approved by the Commission on May 19, 2011. Please change accordingly. CIP-002-5 through CIP-011-1, Applicability sections 4.1.2.4 and 4.2.1.4: Please strike “and group of Elements” as it is redundant with Cranking Path. By definition, the Cranking Path is “a portion of electric system that can be isolated and then energized to deliver electric power from a generation source”. Cranking Path will include the “group of Elements meeting the initial switching requirements”. Thus, the inclusion of this language is unnecessary and will only contribute to ambiguity. Distribution Providers will be forced to question if the drafting team intended to include something above and beyond the Cranking Path. CIP-002-5 R1 and associated VSLs: The requirement uses the term “assets” and the VSL uses the term “BES assets”. Both the requirement and VSL should consistently use that same term. CIP-002-5 R1 Part 4 and Attachment 1 Criterion 3.4: Part 4 and Criterion 3.4 need to be modified to use language consistent with the EOP-005-2, EOP-006-2, and the Applicability section 4 of the CIP-002-5 through CIP-011-1 standards. Please change “blackstart generators” to “Blackstart Resources”. Also, please change “substations in the electrical path of transmission lines” to “Cranking Path”. Blackstart Resources and Cranking Path have specific meanings and are consistent with other standards. Use of terms that are not defined when specifically defined terms exists creates ambiguity in the meaning of the standard. It will cause registered entities to question if something else is meant by these terms. Furthermore, “substations in the electrical path of transmission lines” would not be consistent with the Applicability section regarding Distribution Providers since they will not have transmission lines. CIP-002-5 R2.1: Please modify “Review (and update as needed) the identification” to “Review the identification and update it if there are changes identified”. Otherwise, it implies that the registered entity is to conduct additional reviews and updates whenever there might be a change which could compel the registered entity to continuously review its identification from Requirement R1. CIP-002-5 Attachment 1: Please change “System” to “system” in Criterion 2.9. It is not used consistently with the NERC Glossary definition. CIP-002-5 Attachment 1: Please add a qualifier to Criterion 3.1 that clarifies it only applies to BA and GOP control centers. All RC and TOP control centers will have been included in Medium and High Impact through criteria 1.1, 1.3, and 2.12. CIP-002-5 Attachment 1: In criterion 2.10, please strike “or group of Elements”. Use of Elements is not consistent with the NERC definition. Elements are not typically components of a control system. Use of Elements here implies they are part of the control system for automatic Load shedding. The CIP SMET disagrees with the removal of “annual” obligations from all the Standards. The “once every 15 month” language can lead to a perception of loosened rigor around these activities, as it will allow entities to omit the activity for a calendar year. This decreases reliability and deviates from other NERC Standards. We recommend use of the term “annual,” allowing the entity to define that term within its program. The definition of this term by the entity is consistent with an internal controls approach in mitigating security risks and provides a documented interpretation for the entity self-assessments and monitoring processes. An additional recommendation is to include the entity’s definition of its “annual” cycles within the policy documentation required by CIP-003 R1. CIP-003-5 R2 – Rather than refer back to CIP-002-5, include the appropriate verbiage referring to assets containing low impact BES Cyber Systems. Recommend “Each Responsible Entity for itsassets that contain a low impact BES Cyber System(a discrete list of low impact BES Cyber Systems is not required)shall implement…” This aligns with the phrasing in CIP-003 R1 and CIP-002 R1.3. CIP-003 R3 – The CIP Senior Manager relies on both the definition in the CIP Glossary and the “Responsible Entity” verbiage in every Standard in section 4. There isn’t a clear connection between these two, based on the inconsistent verbiage. Recommend addressing the definition or the verbiage in this requirement to allow a CIP Senior Manager to be based on the specific organizational structure. According to other risk management frameworks, Registered Entities should have flexibility in assigning the scope and responsibilities for CIP Senior Manager(s). CIP-003-5 R3 – The measure can be interpreted to mean that the person designating the CIP Senior Manager may have to be organizationally above the designee. In a small company, it might be reasonable that the highest level official designates him/herself as the CIP Senior Manager. This flexibility should be allowed and it should be clear within the verbiage of the measure. CIP-003-5 R4 – This requirement should not include the “identify, assess, and correct” language, as it is a results-based requirement where deficiencies are unlikely and, if they do exist, create a lot of risk for the organization related to unauthorized signatures. Also, strike the last sentence related to a change in the delegator. If either the delegator or the delegate changes, the delegations should be reviewed/updated. CIP-004-5 R2 – It is a security risk to address some of the concepts listed in 2.1.1 through 2.1.9 with every single person with a need for physical or cyber access to a cyber system, regardless of his or her role. This requirement should be broken out into those general concepts necessary for every access

type/role and those, more specific, concepts (2.1.8 and 2.1.9) that should be reserved for those with a role and are allowed after granting access and renewed annually. In the absence of that granularity, the training program could be ineffective due to the generic information that would be included to meet the requirement. However, in the absence of that approach, this requirement should be left at the current level of specificity (or lack, thereof), allowing the entity the flexibility to provide a minimal amount of training before granting access without requiring additional training afterwards. CIP-004 R4.3 – Provide clarity related to which accounts are subject to an annual review. Does this list of accounts include all of those enumerated in the guidance for CIP-007 R5 (p.43)? If so, this should be clearer. If not, is it the intention of the drafting team to omit that list of accounts from the annual and quarterly review requirements? CIP-005-5 R2.1, R2.2, and R2.3 – Add "Where technically feasible" to the front of both requirements. CIP-005-5 R2.1– This verbiage does not account for situations where the intermediate device can be locally accessed [a local administrator, for example] inside the PSP. This local access, due to the other restrictions around Intermediate Devices, will have the same security stance as someone remotely using the ID to get into the ESP. So, the verbiage in this requirement should account for local access to the ID. Recommend, "Utilize an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset, unless the Intermediate Device is used locally to directly access the Cyber Asset." CIP-005-5 R2.2 - This phrasing does not achieve the intention, which is to have traffic inspected by the IDS in an unencrypted state. So, if that's the intention, the phrasing needs to reflect that result, not the method, because this method, depending on the configuration, may not achieve the goal while it achieves compliance with the specific words. As technology changes, the method prescribed will become outdated. Instead, prescribe the result – encryption is part of the protocol with provisions for IDS efficacy. CIP-010-5 R1.4 – The "guesswork" initiated by CIP-010-5 R1.4.1 does not add value. This is especially true if the only thing that must be tested by R1.4.2 is the list of controls identified with the guesswork. The entity is enticed to round down. Recommend striking 1.4.1 completely and change 1.4.2 to say "Following the change, verify that cyber security controls are not adversely affected." Keep 1.4.3. CIP-010-5 R1.5 – We do not feel that emergency change controls necessary for reliability should be a TFE if related to a CIP Exceptional Circumstance. Recommend adding that verbiage to the beginning of the requirement. Alternatively, if it is the intention of the drafting team to indicate that a TFE is necessary if an entity doesn't have a test environment for a High Impact BES Cyber System, the TFE language should be moved down into the 1.5.1 or 1.5.2 to eliminate references to a TFE for each change.

None

Individual

RoLynda Shumpert

South Carolina Electric and Gas

1) The SDT should clarify their expectation on how low-impact BES Cyber Systems are identified in CIP-002-5 R1.3: Based on the definition of a BES Cyber System and BES Cyber Asset, an entity could find latitude with CIP-002-5 R1.3 to create an assessment methodology to determine whether it has any Low Impact BES Cyber Systems. If the entity can prove that the loss/compromise/degradation of each BES Facility identified under Part 4.2. and 4.3 has no impact on the overall BES, then the entity could justify having no Low Impact BES Cyber Systems identified for those parts. Was it the SDT's intent to accommodate this approach? Or, was it the SDT's intent that all cyber assets affiliated with the Facilities listed in Attachment 1 #4.2 and 4.3 be treated as Low Impact BES Cyber Systems, regardless of the Facilities impact on the BES? 2) For CIP-010-1 R2.1, extend monitoring period to 180 days. Depending on the number of BES Cyber Systems the 35 day requirement may become very burdensome to the BES Cyber Systems owners. If the BES Cyber Systems has a robust configuration management program every 180 days would be sufficient to document any change to the baseline. 3) Please provide clarity on the expectations of CIP-010-1 R3 Parts 3.1 and 3.2 in regards to the "High Impact BES Cyber Systems". Why does the "High Impact BES Cyber Systems" have two different time frames for an CVA (once every 15 calendar months and once every 36 calendar months). Both requirement could be met with a single CVA on the production environment. Correct? Was the intent to create a margin of variation to fit the Registered Entities systems? Or just an typographical error? 4) CIP 004-5, Table 5, Part 5.3 change rationale expects that BES Cyber System Information may reside in a file management system, but CIP 011-5 seems to assume it only resides on a BES system or in a PSP. CIP 010 requires testing of all changes if technically feasible, but in some cases a test environment may not be appropriate even if feasible. The operational exercise requirement in CIP 009-5 should be clarified, especially if failover could risk service interruption. The mitigation of the threat of malicious code in CIP 007-5 is too vague and leaves too much to the auditor's interpretation. The CIP 006-5 requirement for two or more different physical access controls may not always be practical or necessary even when it is technically feasible. CIP 005-5 should consider data diodes, possibly exempting systems with only a data diode connection from "external connectivity" provisions. The words "when technically feasible" should be added to CIP 004-5, Table R5, Part 5.5 to reflect the possibility that a device might have a hard coded password that cannot be changed.

Individual

Tracy Richardson

Springfield Utility Board

In the Draft CIP-006-5 RSAW, "deficiencies" are mentioned in terms of creating "low risk" or "high risk" to the reliability of the bulk power system. However, the CIP-006-5 Standard, nor any other related documentation,

appears to mention or provide guidance on how to determine risk to the bulk power system. Risk determination is only discussed in the RSAW, which states that non-compliance is to be left up to “his/her (CEA’s) professional judgment”. An individual’s professional judgment does not promote any kind of consistent application of risk assessment.

Individual

Ed Nagy

LCEC

: (CIP-002-5 Requirement Attachment 1 – Do Not Support – R1 or Attachment 1 - 2.12) The bright-line criterion is too inclusive as it includes Control Centers of low/no impact Radial Transmission Operators (TOP) unnecessarily. The SDT has taken a position that in order to comply with FERC Order 706, Paragraph 280 that all TOP Control Centers MUST be identified as Critical Assets. In reality, FERC Order 706 states that “It is difficult to envision a scenario in which a TOP Control Center would not be identified as a Critical Asset.” The Commission did not say that all TOP Control Centers MUST be identified as Critical Assets! The Commission clearly states that “Responsible entities should also examine the impact that misuse of those control centers could have on the ELECTRICAL FACILITIES THEY CONTROL and what the COMBINED impact of those facilities could be on the reliability of the Bulk-Power System. Since the bright-line criterion is replacing the responsible entities methodology, it is critical that the bright-line criteria also consider the impact of the facilities CONTROLLED by a TOP Control Center and the COMBINED impact of those facilities. CIP-002-5 Attachment 1 - 2.12 includes all TOP Control Centers as Medium Impact to the BES without regard for the COMBINED impact of the facilities controlled by the Control Center. This results in the applicability of Cyber Security Controls to Control Centers that do not impact the Bulk Electric System (BES). In CIP-002-5 Attachment 1 Requirement 2.5 Transmission Facilities are identified as Medium Impact to the BES if their “Aggregate weighted value” exceeds 3000. The SDT explains that this value is derived from weighted values related to three connected 345kV lines and five connected 230kV lines at a transmission station or substation. Attachment 1 - 2-12 includes TOP Control Centers as Medium Impact to the BES when ALL OF THEIR BES Transmission Lines COMBINED, DO NOT meet the Medium Impact requirement in Attachment 1 - 2-5. Including these TOP Control Centers as Medium Impact to the BES is not necessary; conflicts with FERC Order 706 and the rational used within CIP-002-5 Attachment 1 – 2.5 To “Include BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion IF they are deemed HIGHLY LIKELY to have SIGNIFICANT IMPACT on the BES.”

In general, the Cyber Security Controls that are required for Medium and High Impact BES Cyber Systems are nearly identical. This results in a mismatch between the level of controls required and the impact to the BES. The impact of this is even more significant since entities that do not impact the BES are being included as Medium Impact based on the bright-line criteria.

Group

BC Hydro

Patricia Robertson

CIP-002-5 R1: BC Hydro requests clarification on the Applicability of Distribution Providers ie does 4.2.1 mean any DPs owning assets in this section must comply with the CIP standards? Are these the only DP assets that need to be considered for CIP compliance? CIP-002-5 R1: In a few of the bullet points within this section the wording “…is subject to one or more requirements in a NERC or Regional Reliability Standard” standard is used. Can the wording be changed to be more explicit as to naming the standards that the Registered Entity may be subject to (i.e. 4.1.2.2 and 4.1.2.3) CIP-002-5 R2: BC Hydro requests clarification on the term "associated data centers". Are these the "data centers" that service/support a control center? CIP-004-5 R3: BC Hydro has concerns with the personnel risk assessment program requirements, ie when performing ID verifications outside of the US and Canada it can be difficult and time-consuming (6 to 8 weeks) to conduct International ID verifications, assuming the information is available (which is not always the case), and suggests the following language be added to 3.1 (ID verification): “If it is not possible to perform a full ID verification (i.e. international) then the Registered Entity will document the reason the full seven year criminal history records check could not be performed.” CIP-004-5 R3: When referencing the previous version the standard states “Specified that identity confirmation is only required for each individual’s initial assessment.” BC Hydro is requesting clarification that this is correct as this is not the most secure method (i.e. people can always create an alias so the ongoing checks should also include an ID verification. CIP-004-5 R4: BC Hydro requests clarification for the word “verify” – i.e. how would the Registered Entity be expected to provide evidence of access control ie evidence of proper access control to a locked cabinet that contains sensitive information – would a policy suffice? CIP-004-5 R5: 5.1: BC Hydro requests clarification for the word “removal” – is this meant to mean deletion or would disabling the access suffice. CIP-004-5 R5: 5.4: This section appears to be redundant. BC Hydro requests clarification on what scenarios would fall into this category that are not covered within 5.1 to 5.3. CIP-004-5 R5: 5.5: “For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action”; such a requirement could negatively impact the reliability of the bulk electric system in cases where there is a high movement of staff between locations. In such cases the password may change so many times that it impacts people’s ability to access BES cyber systems (they forget the password due to the high change rate). CIP-007-5 R1: 1.2: “Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or

removable media." Introduction of physical port protection is "assumed" to refer to logical ports only. Can having strong physical access controls to BES Cyber System be a compensating control here? Will having the BES cyber systems in locked cabinets suffice? The requirement is not clear if the protection has to be on the individual devices. The measures indicate signage as a potential control however this would not satisfy the requirement the way the requirement is written. CIP-007-5 R4: "Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 days to identify undetected Cyber Security Incidents." BC Hydro requests clarification on the word "review". Would an automated SIEM technology solution, which monitors events in real-time, not satisfy this requirement? CIP-010-5 R1: BC Hydro assumes the test environment has to be a close representation to production but not an exact mirror and would like this confirmed. CIP-010-5 R2: "Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes." This requirement will be onerous and require significant effort without adding any significant security benefit. Would an effective change control process not satisfy compliance when paired with other controls that can mitigate the risk of unauthorized changes such as monitoring of unauthorized access via a SIEM technical solution?

BC Hydro voted Negative due to the issues provided for Question 1 and supports the rest of the standards/requirements.

Individual

Patricia Lynch

NRG Energy Inc.

CIP-002 BES System Categorization - No comments CIP-003 1.Background –and all standards where language for internal controls state that" each entity shall implement, in a manner that identifies, assesses and corrects deficiencies"- There is no clear mechanism identified that would explain how this will be interpreted and audited by the regional entity. 2. Requirement R2 should be revised to make it clear that it applies only to low impact BES cyber systems (it is inconvenient to have to refer back to the CIP-002 R2 and this is not consistent with the wording of R1). 3. Requirement 4- If a delegate can delegate authority to another person (as contemplated in the Guidelines and Technical Basis section), that should be made clear in the requirement itself. CIP-004 1.CIP-004-5 R2.1 contains elements which can comprise a training program. If role-based training is required (as indicated by R. 2), must all roles identified receive some training from each of the elements in R2.1? If all roles must receive some training for each of the elements in R. 2.1, what is the value of having role-based training? Customized training per roles- how many would be required? This would be difficult to identify, coordinate, implement and measure. Please provide detail as to role definition. Define if training is classified at high level description of user roles or defined by various tasks to determine training. CIP-005 No comments CIP-006 1. Requirement 1.7 should be revised from "within 15 minutes of the unauthorized physical access." to "within 15 minutes of detection." CIP-007 No comments CIP-008 1. Requirement 3.1.2- implies that the Cyber Security Incident Response plan must be updated based on any documented lessons learned. However, lessons learned may not impact any change in the plan but relate to execution of the plan and performance of the personnel in that execution. This should be reworded to include "as applicable". CIP-009 1. Although best practice, through implementation of activities as outlined in Requirement R1.5, this can result in significant impact to the BES as this can result in considerable delay to return to service following a actual recovery, particularly in a control center. CIP-010 No comments CIP-011 No comments DEFINITION: Control Center- as data centers are not a defined term, an entity should be able to choose what constitutes as an associated data center

Group

Florida Municipal Power Agency

Frank Gaffney

FMPA appreciates the hard and excellent work of the SDT to significantly improve the CIP standards and develop a prudent method to protect the Bulk Electric System from cyber attacks. Although we have several comments, only one comment is causing us to vote Negative for any of the standards. CIP-002-5, Attachment 1, Bullet 2.12: The SDT added thresholds for Control Centers for small GOPs and small BAs to define a boundary between "Medium" and "Low" Control Centers, but no equivalent threshold for small TOPs, which is inappropriate. Why would a small control center controlling 1499 MW of generation be "Low" whereas a small TOP's control center for two 138 kV substations with only four 138 kV Facilities be "Medium"? We suggest that a threshold be added for small TOPs to distinguish between Medium and Low. The threshold can be design similar in concept to bullet 2.5, but including >100 kV and <200 kV Facilities with a score of 350. In this way, all of the transmission Facilities under the control of the Control Center could be added up and compared to the weighted score 3000 metric of bullet 2.5 to determine if that Control Center is Medium or Low.

These are issues that FMPA believes ought to be fixed, but are not causing us to vote negatively. Zero-Defect solution doesn't get us all the way there: The helpful phrase: "shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented … policies" was added to many requirements to try and address the "zero-defect" problem. However, by choosing the active word "implement", the zero-defect problem is reintroduced. "Implement" means: "to fulfill, perform, carry out", which means that in order to prove that a policy was carried out, detailed evidence of the results of executing the policy is needed, reintroducing the zero-defect problem. FMPA recommends replacing the word "implement" with "institute" which means "to set into

operation" or "to bring into practice or use" for which the evidence would be less onerous (e.g., the policy itself and proof that it was instituted, such as procedures that support the policy) avoiding reintroduction of the zero-defect problem. CIP-002-5, R1: How is an auditor to verify identification of all BES Cyber Systems that are applicable to R1.1 and R1.2? FMPA waits with interest on what the RSAW will look like. CIP-003-5, R4: The SDT seems to intend to address the zero-defect issue; however, by not associating the documentation of delegation contained in the 3rd sentence to the process of the first sentence, the goal is not accomplished and a strict reading of the requirement still includes a zero-defect problem of needing to document delegation for every delegation and delegation change within 30 days because there is more than one requirement embedded in R4. CIP-006-5, R1: The standard does not answer the question "how big does an opening in the Physical Security Perimeter have to be before is it deemed an access point"? It seems the SDT wants to use the 96 square inches used by some defense agencies, if so, we recommend explicitly stating that in the standard. CIP-006-5, R1.9 and R2.3, CIP-007-5, R4.3, CIP-008-5, R2.3: These are data retention requirements and should not be requirements of the Standard, especially considering the Paragraph 81 effort which is seeking to retire requirements just like this. CIP-006-5, R2.1: The measure does not match the requirement. The requirement is for "continuous escorted access", the measure describes evidence at discrete points in time, not continuous. How is an entity to prove that a visitor was continuously escorted? Does this essentially mean video surveillance? Or written attestations of the person providing the escort?

Group

Duke Energy

Greg Rowland

Duke Energy supports the proposed 10 standards, the implementation plan, and the definitions.

CIP-002 Guidelines and Technical Basis; Requirement R1; Attachment 1; Overall Application; First Bullet: The last few sentences of this bullet make several references to the term "BES Asset". Duke Energy believes this is an artifact from previous drafts and should be replaced with a more current term. CIP-002 Guidelines and Technical Basis; Requirement R1; Attachment 1; Medium Impact Rating; Generation; Criterion 2.13: Duke Energy recommends the removal of the last sentence referencing 300 MW. Duke Energy believes this is an artifact from previous drafts. CIP-003; Requirement R2: Duke Energy recommends that the word "assets" be replaced with "Low Impact BES Cyber Systems" such that the policy will not conflict with other policies required at a site that also houses Medium or High Impact BES Cyber Systems. CIP-004; Requirement R1.1: Duke Energy recommends that "cyber security practices and physical security practices" be changed to "cyber security practices and/or physical security practices" to allow entities flexibility in crafting meaningful and unique awareness communications. CIP-004; Requirement 3.1: Duke Energy recommends that the Interpretation concerning the need to only perform an initial identity verification be incorporated into the requirement as opposed to the guidance document. Duke Energy recommends rewording the requirement to, "Process to confirm identity. This process needs only to be performed prior to initially granting access and does not require reconfirmation during the tenure of employment.". CIP-006; Requirement 1.7; Duke Energy would like to request clarification on why the wording in Requirement R1.7 differs from that in Requirement R1.5. Specifically, why does R1.5 specify alerting "within 15 minutes of detection" whereas R1.7 specifies alerting "within 15 minutes of the unauthorized physical access"? CIP-006; Guidelines and Technical Basis; Requirement R1; Methods to monitor physical access; First Bullet: Duke Energy recommends modification of the last sentence to read "These alarms must provide for notification within 15 minutes to personnel responsible for response" to align with the requirement. Immediate appears in the guidelines but not in the requirement itself. CIP-006; Guidelines and Technical Basis; Last Paragraph: Duke Energy recommends striking this statement concerning outage records. Outage records are not required to be maintained within the current set of requirements. CIP-007; Guidelines and Technical Basis; Requirement R4; R4.1: Duke Energy recommends clarification around the last two sentences. Currently, it refers to an entity which neglects to enable logging would be in violation. Per the Background section, a sole instance of failure is not grounds for a violation so long as it is adequately identified, assessed, and corrected. The statements in the Guidelines seem to be relics of a previous draft which conflict with the new approach. CIP-010; Requirement R3.3; Duke Energy recommends rewording the requirement to, "Prior to adding a new applicable Cyber Asset…" to clarify that this requirement only applies to Cyber Assets meeting the criteria in the Applicable Systems section and would not include a Cyber Asset that is temporarily connected for less than 30 days for the purposes of troubleshooting, eg. Definitions Document; BES Cyber System: Duke Energy requests clarification on the definition of BES Cyber System. Can a non-BES Cyber Asset be placed into the logical grouping of a BES Cyber System so long as the BES Cyber System contains at least one BES Cyber Asset? Currently, the definition would not support such an inclusion, but Duke Energy believes the intent is there such as to afford protections to such non-BES Cyber Assets as part of a larger logical grouping where appropriate. Definitions Document; CIP Exception Circumstance: Duke Energy requests clarification on the term "mutual assistance agreement". Definitions Document; Physical Access Control Systems: Duke Energy requests justification for the inclusion of the word "alert" as it did not appear in earlier drafts. Duke Energy recommends that because this was added late, it should simply be removed. Implementation Plan; Scenario of Unplanned Changes After the Effective Date; Duke Energy requests clarification of the term "Effective Date" and its usage in the title of this table. Is this the Effective Date of Version 5 or the Effective Date of a change or something else?

Individual

Anthony Jablonski

ReliabilityFirst
Even though ReliabilityFirst votes in the Affirmative for the Version 5 of the CIP Standards since we believe it is a much improved version and provides a “net gain” to bulk power system (BPS) reliability; the standards still focuses on defining the applicability of cyber security assets and controls using BPS reliability criteria. ReliabilityFirst offers the following comments for consideration: CIP-002-5, Section 5 Background, states “This standard provides “bright-line” criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities...” This may still be a fatal flaw in the methodology. Examples are: • BPS assets (facilities, elements, etc.) not categorized as high or medium impact default to low impact and do not require discrete identification. Under the low impact categorization, the associated BES Cyber Assets and BES Cyber Systems at these BPS Assets will be protected only in the areas of cyber security awareness, physical access control, and electronic access control and the entity will have obligations regarding incident response. These are not the full complement of CIP Standard and Requirement security controls and provide a very basic or rudimentary set of security controls that may not provide an adequate level of protection due to the “electronic interconnectedness” of these systems with BES Cyber Assets and BES Cyber Systems categorized as high or medium impact. Weak cyber security controls applied to the low impact BES Cyber Systems can have adverse security and reliability related impact on those BES Cyber Systems categorized as high or medium impact. Secondarily, as these low impact assets do not require discrete identification, the compliance monitoring of the associated BES Cyber System security controls will likely be only the verification of program level policies and not actual testing of implemented security controls. This provides very little assurance that these assets are properly protected. • CIP-002-5, Section 5 Background: Real-time Operations, states “To provide a better defined time horizon than “Real-time,” BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise.” A compromise of any BES Cyber Asset can have an immediate (far less than 15 minutes) impact on the affected BPS Asset and any interconnected BES Cyber Assets and Systems with the potential for far reaching impact. Again, in this instance we are defining cyber security asset applicability using reliability criteria. A 15 minute window for operations staff to assess and take automated or manual action makes sense from a reliability perspective. To say a Cyber Asset is only declared a BES Cyber Asset if it would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise does not consider how all instances of cyber compromise can be attempted and then realized. Again, due to BES Cyber System interconnectedness, a BES Cyber System may be compromised with no immediate impact, only that it has been compromised for later malware activation or for deeper reconnaissance into the control system network. A 15 minute window means nothing regarding identification of BES Cyber Systems and Assets that can have an adverse effect on BPS reliability. Ultimately, with BPS Asset reliability criteria defining the applicability of cyber security assets and therefore those that will be protected with appropriate security controls, the risk and impact of interconnected SCADA and ICS may never be fully assessed or taken into consideration. The focus for the CIP Standards should be placed on the identification of all BES Cyber Systems and associated BES Cyber Assets, their interconnectedness; and the reliability operating services they support such as Control, Monitoring, Situational Awareness, Inter-Entity Real-Time Coordination and Communication, etc. This model will provide for more “full featured” cyber security that supports reliability without any gaps. The NRC Cyber Security model detailed in 10 CFR 73.54 including Regulatory Guide 5.71 may provide a relative comparison by which to reassess and rewrite the NERC CIP Standards.
Individual
Jianmei Chai
Consumers Energy Company
CIP-002 rev 5 and Attachment 1 Section 3.4 of the Attachment 1 is inconsistent with the requirement in CIP-002-5 Section 4.1.2.4. The two sections speak of the same Black-Start/Restoration Plan cranking path(s), yet describe each differently, potentially leading to different outcomes. Additionally, it would seem that with the current wording, all cranking paths (as 4.1.2.4 says “Each”) identified in the Restoration Plan, which could be used as part of the initial restoration efforts, would need to comply. The requirement, in both Section 4.1.2.4 and Attachment 1, Section 3.4 should read specifically that only the initial “Primary Cranking Path” be included for compliance. Also, Paragraph 3.4 uses the phrase “… in the electrical path of ‘transmission’ lines used …”, in describing the restoration path. There needs to be clarification on whether this solely applies to Transmission (capital T) or any and all lines in the path. If the latter, Consumers Energy recommends striking the word “transmission” entirely. Again, the rewrite needs to be consistent with section 4.1.2.4. Additionally, the Functional Entities in section 4.2.1.3 and the Impact Rating Criteria in Attachment 1, section 3.6, for Distribution Providers to include facilities containing “A Protection System that applies to Transmission …” is a new (initially introduced in draft 2) unsubstantiated requirement for Low Impact assets. The requirement should be deleted, or if such assets are to be included, the “applies to Transmission” phrase needs to be better defined, and only those assets/systems that can have a significant impact, such as impacting one or more Interconnection IROLs, should be included. Consumers Energy suggests wording pertaining to the IROLs similar to that found in section 2.9. Section 4.2.2 indicates that all BES facilities be included. Consumers Energy recommends that the criteria specified in section 4.2.1 for Distribution Providers also apply to Generation Resources. By not including this specific criteria, the scope of assets included in CIP Version 5 significantly increases from CIP Version 4. This seems excessive, as Generation

Resources often fall off-line without any adverse impact on the BES. Therefore, it makes sense to only include Generation Resources that would be most likely to have an adverse impact on the BES, which would be those specified in 4.2.1. Attachment 1 (of CIP-002) Attachment 1, Section 2.1, states "Commissioned generation, by the each group of generating units at a single plant location...." The use of the word "by" in this sentence does not make sense and should be reworded. Attachment 1, Section 3.3, lists "Transmission Substations and Stations" and "Generation Resources" in the list of Low Impact Cyber Systems at Facilities requiring compliance. Without the ability to perform a risk-based assessment any longer (as in CIP versions 1-4) all such Facilities will have cyber assets regulated (and regulated the same, regardless of importance) unless an entity can show that the cyber systems at these facilities will not meet the rather vague (see additional comment below) definition of BES Cyber Asset, and thus not qualify at all as a BES Cyber Asset. The definition currently does not provide adequate help in identifying assets and therefore the result of section 3.3 will be, as a minimum, to include all Transmission Substations/Stations and BES Generation Resources in the low impact category, thus requiring compliance. As noted below, Consumers Energy believes that modification to the BES Cyber Asset definition will correct this deficiency. Lastly, Consumers Energy recommends a minor modification to section 3.6 for clarity, such that it read "... Protection and UFLS and UVLS systems, specified in the Applicability Section 4.2.1, above." CIP-003 rev 5 Requirement R2 requires entities to have some protection for any BES Cyber Asset/System, regardless of actual impact that the cyber asset may have on facilities determined to be "Low Impact". In spite of numerous comments to the contrary provided to the SDT in previous drafts, this aspect of rev 5 remains. This would infer that all such low impact cyber/programmable devices are of the same value or importance of function to BES reliability, but this is far from true. In the proposed standard, a configurable electronic panel meter (providing local, seldom-used indication) in a substation, would potentially rise to the same level of compliance (albeit "Low") as an RTU or protective relay in that same substation. In this regard, Consumers Energy recommend that the SDT consider developing bright-line criteria that could be used for defining BES Cyber Assets at different levels based on the asset's impact of MW levels, system disturbance potential, or other substantial BES events. Back in CIP-002, rev 5 - Attachment 1, Section 2, (and especially item 2.5) the SDT seems comfortable eliminating applicability for facilities of lower voltages or MW value. It would seem nonsensical to then include cyber assets at other facilities, if the impact on reliability due to a compromised cyber asset was equally as small or even minute. The Definitions document The Definition of a BES Cyber Asset continues to be vague, in spite of past comments to the SDT. In rev 5 draft 3, it states: BES Cyber Asset A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. The use of "adversely impact" and "reliable operation" in this definition is particularly vague. Instead, it has been previously recommended that the SDT use a more definitive definition regarding the impact/effect of a cyber event, or one providing 'bright-line' criteria, but the definition has remained essentially the same again in draft 3. At this time, Consumers Energy proposes the inclusion of the NERC Glossary term, "Adverse Reliability Impact" in place of the two phrases. The Adverse Reliability Impact definition is fairly specific, concise and states: Adverse Reliability Impact Current FERC-approved definition: The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection. Recently NERC BOT-approved definition: The impact of an event that results in Bulk Electric System instability or Cascading. Without the use of the Adverse Reliability Impact definition, the SDT unilaterally and significantly extends the potential scope of cyber assets being regulated, in both our HVD and LVD DCO, and Generation facilities. The Cyber Asset and BES Cyber System definitions do not consider if or how "programmable electronic devices" can be accessed or are connected. Consumers Energy recommends adding additional clarification similar to that in CIP Version 3, CIP-002 R3.1, "The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter."

In revision 5, draft 3, the SDT has revised the use of the Reliability Operating Service to no longer be a NERC defined term, but maintained the concept of the same. The continued use of the reliability operating service in the Application Guidelines, as a guide or aid in determining BES Cyber Systems should be discontinued. The concept is highly subjective and opens the door to numerous areas of increased scope in the standards applicability. As noted earlier by Consumers Energy, the SDT should instead refer to and use the very well-defined term, "Adverse Reliability Impact" for determining which cyber assets/systems may impact the BES.

Individual

Scott Berry

Indiana Municipal Power Agency

Control Center – IMPA does not support the definition of Control Center. The definition uses the words "monitor and control" and when it comes to defining what is included in those words the SDT has told the industry to reference the FAQ Document for Cyber Security Standards CIP-002 –CIP-009 (May 9, 2005). In this document, the answer to question 12 (page 5 of 24) states that "monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction." IMPA does not agree with including

“manually or by voice instruction” in this usage and then apply it to the definition of Control Center. The consequences of using these words will make many small entities have new Control Centers, and they will have BES Cyber Assets due to having a simple wired telephone or a wired fax machine that can have numbers programmed into it (the definition of a Cyber Asset covers programmable electronic devices). This could lead to many small entities owning TOP or GOP Control Centers because generally most of them do perform reliability tasks for transmission or generation at two or more locations. In addition, the loss of a telephone could lead to not starting or stopping a 20 mva generating unit (connected to the BES at 100kV or above) which an auditor could judge as having an adverse impact because it is a registered BES Facility. This scenario is unlikely due to entities having backup communications (another land line or cell phone communications) but when it comes to the evaluation of a telephone it states under BES Cyber Asset that “Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact." IMPA does not support the use of manual or voice instructions (especially voice instructions) when it comes to the terms “monitor and control” in the definition of Control Center and recommends updating these terms from a document written in 2005 in a new document to reflect the removal of them.
no comment
Group
Tampa Electric Company
Ron Donahey
Tampa Electric (TEC) wanted to thank the SDT for the hard work and energy that the SDT have put in during the development of version 5, despite the many challenges along the way. We support the intent and overall direction that the standards take. For CIP-002 R 1.3, TEC believes the intent is to provide protection at BES Facilities that do not meet the Attachment 1 Criteria 1.1 through 2.13. However, we believe that the CIP-002-5 R1.3 wording is technically flawed and conflicts with the definitions of BES Cyber Assets/Systems. By definition, to qualify as a BES Cyber Asset/System the asset must have a 15 minute impact on reliability of the BES. However a low impact facility cannot have such an impact to the BES per the attachment 1 criteria. Based upon this reasoning, we believe it is not possible to have a facility that meets the criteria of CIP003 R1.3.
Tampa Electric (TEC) wanted to thank the SDT for the hard work and energy that the SDT have put in during the development of version 5, despite the many challenges along the way. We support the intent and overall direction that the standards take. For CIP-002 R 1.3, TEC believes the intent is to provide protection at BES Facilities that do not meet the Attachment 1 Criteria 1.1 through 2.13. However, we believe that the CIP-002-5 R1.3 wording is technically flawed and conflicts with the definitions of BES Cyber Assets/Systems. By definition, to qualify as a BES Cyber Asset/System the asset must have a 15 minute impact on reliability of the BES. However a low impact facility cannot have such an impact to the BES per the attachment 1 criteria. Based upon this reasoning, we believe it is not possible to have a facility that meets the criteria of CIP003 R1.3.
Individual
Michael R. Lombardi
Northeast Utilities
Northeast Utilities (NU) supports all 10 of the proposed (draft 3) CIP V5 standards, the implementation plan, and the set of definitions.
In addition to our support, Northeast Utilities offers the following comments for your consideration: We assume Draft 3 is relatively stable, yet for CIP-004-5, Part 5.2, the revocation of an individual’s access “by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access” is administratively burdensome without a corresponding benefit to reliability. We suggest the “by the end of the next calendar day” be replaced with “within 30 days.” Since there is a low risk to physical or cyber security. CIP-006-5, Part 1.7, states: “Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the unauthorized physical access.” Please clarify that statement, especially the personnel to be notified. Is notification automated, manual, or is it our choice? Additionally, please clarify if cabinets inside a PSP require individual alarming. NU recognizes that compliance with CIP V5 Standards will be a multimillion dollar effort. NU encourages NERC to institute compliance changes that clearly improve physical and cyber security to justify the capital and O&M costs the industry will incur.
Individual
d mason
HHWP
For us, the addition of the following language to the implementation plan for unplanned changes resulting in a higher categorization only muddles the timeline for compliance: "...with additional time to comply for requirements in the same manner as those timelines specified in the section 'Initial Performance of Certain Periodic Requirements' above."
Group
Dairyland Power Cooperative

Tommy Drea
Group
PPL Corporation NERC Registered Affiliates
Brenda Lyn Truhe
The PPL Companies thank the Standards Drafting Team for their work on CIP Version 5. Please consider the following comment for CIP-004-5 Table R5 – Access Revocation. In Part 5.4 - Applicable Systems, should PACS also be listed here? We ask as some cyber assets in a PACS can also have individual user accounts. We have the same comment for Part 5.5. Additionally, CIP-007-5 Part 5.5 Requirements, the first paragraph uses the term “interactive user access”. This is not a defined term; however, it is similar to the CIP V5 Definitions defined term Interactive Remote Access. Should the term "interactive user access" be defined or clarified in the Guidelines and Technical Basis? CIP-003 states “An inventory, list or discrete identification of low impact BES cyber systems is not required.” CIP-005 Guidelines and Technical Basis states an ESP is required around networks even if standalone regardless of impact classification. Please confirm the requirements in CIP-005 do not imply a list of Low Impact assets is needed.
Individual
Benjamin Smith
Tampa Electric
Project 2008-06 Successive Ballot CIP-002-5 September 2012_in, please refer to comments of Ron Donahey of Tampa Electric
Individual
Don Schmit
Nebraska Public Power District
Individual
Kevin Koloini
American Municipal Power
Group
Bonneville Power Administration
Chris Higgins
BPA believes CIP-002-5 is unclear. Attachment 1 doesn’t specify where within-hour generation and interchange scheduling systems related to Balancing, Managing Constraints, and Inter-Entity Coordination fall within the high-medium-low impact framework. Impacts on IROL identification and BA, TOP, and GOP planning systems feeding real-time operations are also unclear. BPA reiterates previous comments and will seek clarity post-balloting. CIP-003-5 – R2 uses the term ‘asset’, this term is not defined by NERC and may be misinterpreted without definition. BPA believes CIP-003-5 R2 is referencing R1, part 1.3 of CIP-002-5, not R2, part 1.3 which doesn’t exist. Suggest rewording R2 to remove the term “asset” and correct the reference to CIP-002-5. CIP-005-5 – BPA understands the valid security reasons for the requirement for access control on outbound connections, and has concerns with impact this will have on our ability to operate as required. BPA requests more clarity regarding the types of devices that would qualify as intermediate devices, beyond the requirements that they must support encryption for any interactive sessions and multifactor-authentication for access to any interactive sessions. Definitions – Please reconsider previous comments for Cyber Security Incident, BES Cyber Asset, Critical Assets and define “programmable” in “Cyber Asset”.
Individual
Doug Hohlbaugh
FirstEnergy
FirstEnergy (FE) is conditionally approving and voting affirmative to the complete set of the CIP Version 5 standards. Our voting position is based on clarifying text that we believe must be added to the CIP-005-5 Guidelines and Technical Basis section for Requirement R1 (specifically parts 1.3 and part 1.5) to remove the operational barriers that may prevent Entities from implementing encryption among sites on a BES Cyber System network using either encrypted tunnels or tunnel-less encryption technologies. FE believes that NERC shares the opinion that the plain language of the standards should encourage the implementation of encryption technologies on critical networks. Consequently, FE proposes the following text (see ITEM 1) for the CIP-005-5 Guidelines and Technical Basis section for Requirement R1. At the discretion of the SDT, language may need to be added to CIP-005-5 R1.3 and R1.5 if that is required to ensure clarity in the formal Standards to support the audit process. ITEM 1: "Some Entities employ encryption as a strong measure for securing communications among discrete physical sites (e.g. data centers and control centers). Encryption (either via encrypted tunnels or group encrypted transport) effectively satisfies the establishment of 'discrete Electronic Security Perimeters' as referenced in Section 4.2.3.2 of each Applicability section. Provided the termination points of the encryption are protected within

Physical Security Perimeters, the requirements for CIP-005-5 R1.3 (inbound & outbound access permissions and deny-by-default) and CIP-005-5 R1.5 (inbound & outbound malicious traffic inspection) may be achieved at central firewall(s) protecting the BES Cyber System network to which the ESPs are connected. For traffic communicating within the encrypted network, the CIP-005-5 R1.3 and CIP-005-5 R1.5 requirements do not need to be duplicated at the encryption endpoints. This enables effective implementation of encryption, which might not otherwise be operationally feasible if traffic inspection were required inside of the protected network due to the latency and convergence delays that are introduced." ITEM 2: Additionally, FE understands that serially connected cyber assets would not be considered to be within an Electronic Security Perimeter (ESP) nor are they in scope for requirements applicable to BES Cyber Systems with External Routable Connectivity. Regarding the ESP, we come to this conclusion from reading of the standard drafting team's response to comments for Question B12 related to CIP-005-5 Requirement R1 which states "CIP-005-5, however, is focused on those two higher risk forms of connectivity and do not have mandatory requirements on serial, non dial-up forms of communication." Regarding the "… with External Routable Connectivity" applicability FE understands this to also excludes serially connected devices based on information listed in the Background section (Section 5) under the heading "Applicable Systems Columns in Tables". As an example, "Medium Impact BES Cyber Systems with External Routable Connectivity – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity." We conclude that serial are not in scope when this applicability is used based on the second sentence that states "This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity." While it's understood that serially connected devices are in scope for other areas of the CIP V5 standards, FE requests that the standard drafting team confirm or clarify FE's view related to the ESP and the "w/ ERC" applicable items. ITEM 3: FE notes that within each Background section (Section 5) under the heading "Applicable Systems Columns in Tables" that the defined applicability statement for "Medium Impact BES Cyber Systems with External Routable Connectivity" is consistently stated throughout the CIP V5 standards with the exception of CIP-004-5. In CIP-004-5 the statement is missing the second sentence that appears in the other standards where Medium Impact BES Cyber Systems with External Routable Connectivity is also referenced in the Background sections. ITEM 4: These comments are supported by the following FE Registered Ballot Body personnel which include Segment 1 – William J. Smith; Segment 3 – Stephan Kern; Segment 4 – Douglas Hohlbaugh; Segment 5 – Ken Dresner and Segment 6 - Kevin Querry.
FE appreciates the hard work of the drafting team and the effort given moving from Draft 2 to Draft 3 is evident. Most notably, changes made to address various "zero defects" issues and allowing entities to implement strong internal compliance programs that include corrective action programs is a significant step forward. We offer the following additional comments to further improve the CIP V5 standards. ITEM 1: CIP-002-5 Background Section – The sentence that states "In transition from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets" should be struck or reworded. A BES Cyber System can be vastly different due to the removal of connectivity exclusions (non-routable) that exist in CIP V4. ITEM 2: CIP-007-5 R3, part 3.1 – Consider adding "Per device capability," to the beginning of the requirement. Otherwise, if a deter posture is selected, potentially in conflict with other requirements (e.g. 4.1). ITEM 3: CIP-010-1, R1, part 1.1.4 – Consider limiting the applicability for Medium to only those with External Routable Connectivity for consistency with CIP-007-5 R1, Part 1.1 ITEM 4: Background Section (ALL) – The statement that bulleted lists are "or" and numbered are "and" should be deleted. The list should be clear by direct reading within the standard. ITEM5: CIP-004-5 R5, Part 5.5 – Consider indicating within 35 days for consistency with other monthly requirements (e.g. CIP-007-5 R2, part 2.3).
Individual
Tony Kroskey
Brazos Electric Power Cooperative
Individual
Daniel Duff
Liberty Electric Power LLC
CIP-004: Please refer to detailed comments from the last round of balloting. Smaller entities rely on remote vendor support,and the lack of a method for allowing such support will result in a less reliable bulk electric system. CIP-007: Including specific password requirements in a standard that will take years to modify insures that new and safer technologies cannot be implemented by the industry, and again negatively impacts the reliability of the BES. Definitions: Control Center should be redefined. See the comments of Indiana Municipal Power Agency.
Individual
Darryl Curtis
Oncor Electric Delivery Company
N/A
Oncor supports the shift in compliance to the internal controls approach and we look forward to NERC providing a programmatic/principles framework in a collaborative approach with the industry. In the absence of this framework, it is unknown how the concept of "identify, assess and correct" will evolve. As the framework is

developed including the "identify, assess and correct" concept, Oncor requests that continuous focus be placed on implementing principles including this concept and not requiring or specifying internal controls which would place additional compliance burden on entities. The internal controls principles/framework should enable entities to establish internal controls model utilizing deficiency correction approach but should not mandate the approach. Internal Controls Program needs to be defined by an Entity, it is not a “One Size Fits All”. The standards/RSAWs should reflect this understanding.
Individual
Robert W. Roddy
Dairyland Power Cooperative
Individual
Travis Metcalfe
Tacoma Power
Definitions: Control Center The relocation of the term “including their associated data center” reduces the clarity of Control Center and should be clarified to address two issues: 1. The word “associated” provides no guidance as to whether this is association by ownership, functionality or physical location. If the intent suggested on page 20 of the consideration of comments is to only cover data centers at the same physical site as the control center, the term should read “including their onsite associated data center.” If the intent suggested on page 30 of the consideration of comments is only to cover data centers owned by the same owner as the control center, the term should read “including their associated data center(s) owned by the registered entity.” Unfortunately both of these approaches could allow registered entities to avoid many CIP compliance requirements simply by outsourcing or physically relocating data centers. 2. Although the SDT suggests that many definitions of data center exist, they are not clear enough to separate out the typical equipment in substation control rooms & communication hubs versus the more complex equipment in a SCADA data center. For example, a transmission substation control will likely include every item listed in the wikipedia definition: “A data center or computer center (also datacenter) is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices.” BES Cyber System Information Tacoma Power supports removing the ambiguous phrase “pose a security threat.” Page 23 of the consideration of comments states “the SDT does feel that it is prudent to remove this phrase,” however it still appears in the latest revision. CIP-002 Section 4.2.2 -Applicability The capitalized term “Facilities” in “All BES Facilities” would to include only assets with electrical terminals and does not include items such as Control Centers, data centers, SPS/RAS or protection systems. As used elsewhere within the CIP standards, lower case “facilities” would apply more broadly. Appendix 1- section 3.2 “Low Impact Rating” Replace “Transmission substations and stations” with “Transmission substations and transmission switchyards” or with “Transmission stations.” It is currently unclear why both stations and substations are listed. It is also ambiguous whether transmission applies to both terms, or just the first. CIP-006-5 R1.7 Comment and Recommendation Comment – The PACS associated with High or Medium Impact BES Cyber Systems is not an applicable system to the CIP-008-5 Incident Reporting and Response Planning requirement, therefore will not have responsible personnel identified in the BES Cyber Security Incident Response Plan. Recommendation – Change requirement language to read as follows: 1. “Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to responsible personnel identified in the CIP-006-5 R1 Physical Security Plan within 15 minutes of the unauthorized physical access.” Or more simply: 2. “Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to responsible personnel within 15 minutes of the unauthorized physical access.”
Group
SPP and Members
Lesley Bingham
SPP does not find sufficient deficiencies in any of the standards, the implementation plan or the set of definitions to vote against them.
CIP-002-5 Requirement 1 How is an entity to comply with both the “consider each of the following assets” section of Requirement 1 and adhere to the criteria for review in Attachment 1? CIP-002-5 Attachment 1 provides much detail for assisting many of the Responsible Entities classify assets into a High, Medium or Low Impact to the Bulk Electric System. However, there is no such guidance for the Transmission Operator (TOP). In the current draft of Attachment 1, TOPs of all sizes are considered as either High of Medium Impact. Smaller TOPs do not have the same impact on the BES, but will incur similar costs to implement their CIP compliance programs. Was a cost-benefit analysis done on the impact of CIP compliance for NERC and the TOPs, focusing on the needs of smaller operators? CIP-005-5 Requirement 1.2 The definition of External Routable Connectivity does not anticipate a situation where serial protocol may be used over IP connectivity. This may happen to provide flexibility of routing design, but may not strictly comply with the External Routable Connectivity definition. As an example, communication between two devices may take advantage of the Ethernet ports on the devices, but run serial protocol between the devices. The devices aren’t using ip and the connections must be programmed internally to

use serial protocol. By explicitly stating, “routable protocol connection” in the definition and focusing an auditor’s attention on the connection, the auditor may see the Ethernet port being used and determine noncompliance. Recommend deleting the word “connection” at the end of the definition of External Routable Connectivity. Requirement 1.5 is still geared towards implementing an IDS/IPS. An IDS would not provide the additional protection for an Electronic Security Perimeter (ESP) if a firewall failed, which seems to be called for in the FERC Order. Also, an IDS or IPS would provide no protection against an insider threat. It’s also important to note that “malicious” activity cannot be determined strictly by watching for an activity. Traffic to an ESP which is malicious may in fact appear to be normal. The qualification of “malicious” vs “normal” requires knowing an actor’s intent, which cannot always be gleaned from log entries, traffic patterns or signatures. Requirement 2.1 We would request clarification that the Interactive Remote Access must not be initiated from a device which allows direct access. Suggest the language “Utilize an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not initially directly access an applicable Cyber Asset.” Requirement 2.2 We would request clarification on whether the “Intermediate Device” is expected to provide the encryption or if two devices are envisioned for compliance. Requirement 2.3 We would request clarification on whether the multi-factor authentication is required for the Intermediate Device, for access to the Electronic Access Point or to the individual Applicable Systems. Suggest the language “Require multi-factor authentication for initiating all Interactive Remote Access Sessions.” CIP-006-5 Requirement 1.2 The “5. Background” section of CIP-006-5 includes a definition/description of “Medium Impact BES Cyber Systems with External Routable Connectivity,” that notes an exclusion in the following sentence: “This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.” When this definition/description of cyber systems is used for the applicability in requirements such as CIP-006-5 R1.2, R1.4, and R1.5, it is used with the added inclusion of “and their associated…PCA.” Looking at the Version 5 definitions document, the definition of Protected Cyber Assets reads “One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter…” It appears that the inclusive “and associated PCAs” statements in the requirements negates the exclusion statement from the “Background,” and makes the intended applicability of such physical security requirements to specific cyber assets unclear for cyber assets without direct external connectivity which reside in the same ESP as cyber assets with direct external connectivity. Requirement 1.5 and 1.7 We would request a change in language that would clarify that the entire BES Cyber Incident Response Team is not required to respond to a Physical Security concern. Suggest the language “Issue an alarm or alert in response to detected unauthorized physical access through a physical access point into a Physical Security Perimeter/to a Physical Control System to appropriate personnel identified in the BES Cyber Security incident Response Plan within 15 minutes of the unauthorized access.” CIP-007-5 Requirement 4.4 Recommend changing “undetected” to “potential” Requirement 5.6 Recommend removing “where technically feasible” (If you can’t implement technical controls, you can implement procedural controls. The TFE language is not needed.) CIP-008-5 Requirement 1.1 Recommend adding “assess” between “identify” and “classify” Requirement 1.2 Recommend clarifying that only incidents clearly identified as “Reportable Cyber Security Incidents” must be reported to ES-ISAC . Suggest that timeframe specify “Initial notification…exceed one hour from identification as a Reportable Cyber Security Incident.” CIP-010-1 Requirement 1.4/1.5 Recommend clarifying when an active test is required. Language in these two requirements is very similar and can be confusing on whether both require an active test or if one requires a review of controls as opposed to testing a change. Requirement 1.5 Recommend the following: Document the results of the testing and, if a test environment was used, the baseline configuration differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments. Where baseline configuration differences are to be documented, the differences must include, at a minimum, the items described in CIP-010: R1.1.1, R1.1.2, R1.1.3, R1.1.4 and 1.1.5. General note: Group expressed concern that three different versions of the standard might be included in one audit. This will create a much more complex audit environment. Entities need one consistent set of standards and clear timeframes for audit periods to reduce the likelihood of multiple standards in one audit.

Group

Western Area Power Administration

Brandy A. Dunn

For CIP-003-5 to 009-5 and CIP-010-1 and 011-1, we agree with the move away from the “zero defects” stance used in Version 3 and 4 standards to the internal controls approach. However, this should have been preceded with an appropriate framework, ample industry involvement, and appropriate outreach and training. We are concerned that NERC is moving forward too quickly without a cohesive strategy by placing language in Standards prior to industry having a complete understanding of (and training on) NERC’s definition of “internal controls”. Also, the CIP-002-4 and Version-5 ”bright-line criteria” steps away from a risk based method to a prescriptive approach. This is an inverted philosophy from the approach Draft-3 used in the other CIP-V5 standards. Although Western appreciates the efforts and reasons behind this, we feel more work will be needed, or perhaps an entirely different approach to Cyber Security in the industry will need to be investigated.

Individual

David Francis

MISO

Comments on CIP Version 5 MISO supports the latest draft of CIP Version 5 as providing greater clarity to Registered Entities regarding their compliance obligations and wishes to commend the SDT for its attention and responsiveness to much of the industry's comments on previous drafts. MISO also supports an overall shift in the emphasis of compliance from perfection to the identification, assessment, and correction of deficiencies. In particular, MISO submits that such a shift in focus from strict liability to a regime in which finding and correcting deficiencies is encouraged and in which proactive compliance is rewarded is the only logical way to ensure the security of the Cyber Assets on which the reliable operation of the Bulk Electric System is founded. At the same time, MISO is concerned that the process for determining the sufficiency of a Responsible Entity's efforts to identify, assess, and correct deficiencies is ambiguous and may lead to arbitrary or inconsistent auditing under the regional Compliance Monitoring and Enforcement Programs ("CMEP"). For instance, what constitutes a deficiency may be an issue that is subject to disagreement and varying interpretation. Moreover, the question of whether all deficiencies must be treated equally or whether Entities may implement varying levels and types of responses remains unanswered. Similarly, what constitutes an appropriate corrective measure may also be susceptible to subjective interpretation. With respect to the obligation to identify deficiencies, without further guidance from NERC, it is highly likely that auditors will take inconsistent positions on whether a Responsible Entity's efforts to identify deficiencies were sufficiently robust. Further, without this guidance, an entity is likely to continue to be audited to a strict liability regime with 'consideration' given to its processes to "identify, assess, and correct". This would result in a substantial, additional burden on Registered Entities. Additionally, underlying many of these ambiguities is the question of whether the "identify, assess, and correct" paradigm ostensibly requires the use of internal controls and whether those controls are now subject to audit. Although the September 11, 2012 Webinar specifically states that Version 5 does "not require 'internal controls' or additional process[es]," MISO respectfully submits that the assurance of the SDT on this subject is no guarantee of the verisimilitude of this assertion. More importantly, the structure and substance of an audit of these requirements may well result in a scope that encompasses a Registered Entity's internal controls. Thus, MISO requests that NERC provide, in conjunction with its submission of Version 5 to FERC, public guidance both to the industry and the regional entities containing suggestions for the implementation of "identify, assess, and correct" programs as well as delineating the properly auditable aspects of such programs and the standards that will apply to those aspects in determining compliance. Unless Responsible Entities are able to anticipate – and therefore gear their compliance efforts towards – the proposed auditing of specific aspects of their internal "identify, assess, and correct" programs, these programs will simply extend the industry's current perception of the existing CIP paradigm to the next generation of CIP Reliability Standards, e.g., substantial, administrative burden with minor benefits to the reliability of the Bulk Electric System.
Individual
Rick Keetch
NRG Energy Power Marketing
1. Background –and all standards where language for internal controls state that" each entity shall implement, in a manner that identifies, assesses and corrects deficiencies"- There is no clear mechanism identified that would explain how this will be interpreted and audited by the regional entity. 2. Requirement R2 should be revised to make it clear that it applies only to low impact BES cyber systems (it is inconvenient to have to refer back to the CIP-002 R2 and this is not consistent with the wording of R1). 3. Requirement 4- If a delegate can delegate authority to another person (as contemplated in the Guidelines and Technical Basis section), that should be made clear in the requirement itself. 1. CIP-004-5 R2.1 contains elements which can comprise a training program. If role-based training is required (as indicated by R. 2), must all roles identified receive some training from each of the elements in R2.1? If all roles must receive some training for each of the elements in R. 2.1, what is the value of having role-based training? Customized training per roles- how many would be required? This would be difficult to identify, coordinate, implement and measure. Please provide detail as to role definition. Define if training is classified at high level description of user roles or defined by various tasks to determine training. Requirement 1.7 should be revised from "within 15 minutes of the unauthorized physical access." to "within 15 minutes of detection." CIP-008 VOTE YES 1. Requirement 3.1.2- implies that the Cyber Security Incident Response plan must be updated based on any documented lessons learned. However, lessons learned may not impact any change in the plan but relate to execution of the plan and performance of the personnel in that execution. This should be reworded to include "as applicable". CIP-009 VOTE NO 1. Although best practice, through implementation of activities as outlined in Requirement R1.5, this can result in significant impact to the BES as this can result in considerable delay to return to service following a actual recovery, particularly in a control center. DEFINITION: Control Center- as data centers are not a defined term, an entity should be able to choose what constitutes as an associated data center
Individual
Keith Comeaux
NRG Energy, Inc
Individual
Matthew Morais

ERCOT ISO
ERCOT is voting to approve CIP-002-5, but the SDT issued certain guidance statements in response to SRC comments that are potentially problematic in practice. Those matters are discussed below, and ERCOT requests that the SDT take appropriate action consistent with these comments to remedy the potential problems created by the relevant guidance statements. In response to SRC comments that requested clarification on criteria 2.3 and 2.6 with respect to what specifically triggers the relevant third party notifications under those criteria, the SDT noted that with respect to 2.3, the notification is pursuant to a contract – specifically, when the relevant functional entities identify a resource as a Reliability-Must-Run resource. This is potentially problematic. Accordingly, ERCOT requests clarification regarding the appropriateness of using "Reliability Must Run" (RMR) or similar concepts for identifying, "Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year." As an initial matter, RMR contracts are generally only relevant in ISO/RTO markets where they are needed to keep uneconomic units running for reliability purposes until alternative market solutions address the issue. Accordingly, it is questionable if this approach would even be available in vertically integrated regions. In addition, the designation of RMR resources is performed pursuant to specific tariff/protocol processes that are not based on NERC standards, but are rather based on the particular qualifications/conditions in the respective entities rules. As such, it is possible that they are outside of the purview of the NERC Reliability Standards, which are linked to specific reliability standards in Section 215 of the FPA – i.e. the basis for RMR contracts may not align with the basis for the NERC reliability standards. The SDT guidance does refer to the TPL standards and additional contracts generally, but this further confuses the point and creates a disconnect between the relevant processes that drive the notification under criterion 2.3 - RMR contracts are unrelated to the TPL standards or the opaque and undefined process superficially described by the SDT where the RRO coordinates certain actions. Also, because the RMR process is performed by ISOs/RTOs under their tariff rules and not the NERC Standards, they are not executing the agreements in a NERC functional role, which creates a disconnect between the third party NERC functions under criterion 2.3 and the entity executing the RMR with the resource. While it is possible that an ISO/RTO involved in RMR agreements is registered as one of the relevant functions, the function is not making that determination in its NERC functional role (i.e. PC or TP) pursuant to NERC authority. Given the potential problems created by linking the relevant notification to a reliability needs determination pursuant to an RMR process, the SDT should reconsider this guidance as it relates to RMR contracts, and focus on appropriate reliability needs/determinations under relevant NERC Standards, which align with NERC's authority and the reliability metrics that serve as the benchmark for NERC's authority generally and the specific NERC Standards. For example, units may be identified in planning studies performed pursuant to the NERC standards that are not relevant under regions' RMR processes, or vice-versa. Although the SDT discusses TPL-003, the scope of applicable standards under which third party actions trigger notifications pursuant to criterion 2.3 must be specifically defined. The general reference to TPL-003 does not accomplish this. Also, in regards to references to Category C3 contingencies under TPL-003, there is no requirement for the Planning Authority or Transmission Planner to provide or communicate the results of the studies to the asset owners. This would create a new obligation beyond their responsibilities under the NERC Standards. With respect to criterion 2.6, the SRC requested similar clarifications regarding the appropriate scope of standards that trigger the third party notification. The SDT noted that with respect to 2.6, that criterion includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, Establish and Communicate System Operating Limits, R5.1.1 and R5.1.3. The SDT went on to note that IROLs may be based on dynamic System phenomena such as instability or voltage collapse, and that derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response. ERCOT requests clarification as to whether FAC-014-2 is the only standard required for use in identifying, "Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." ERCOT appreciates the specific reference, but in order to provide certainty to all relevant entities, the scope of relevant standards must be specifically defined – the SDT should explicitly state that FAC-014-2 is the only relevant standard, or, alternatively, identify any other relevant standards. It should also be noted that FAC-014-2 does not require the Reliability Coordinator, Planning Coordinator, or Transmission Planner to communicate any of this information to the asset owners. This would create a new obligation beyond their responsibilities under the NERC Standards. CIP-003-5: Requirement R4 requires that an entity have a documented process for identifying and documenting delegations of authority unless there are no delegations. The documentation of the delegation should be sufficient without the need to create and maintain a documented process for identifying and documenting said delegations. This requirement is administrative in nature and is suitable for elimination pursuant to the SAR P81 process. Accordingly, the Standard Drafting Team should consider the need for this requirement in version 5. CIP-004-5: This requirement is administrative in nature and is suitable for elimination pursuant to the SAR P81 process. The risk to the BES would be minimal because a quarterly awareness bulletin was not sent. Accordingly, the Standard Drafting Team should consider the need for this requirement in version 5. Interactive Remote Access Definition: This definition is unworkable in practice. ERCOT is voting to approve the standard to move v-5 forward because it offers incremental improvements over v-4, however, the SDT should provide additional clarification on this interpretation, or revise it, to mitigate the unworkable result of its potential interpretation, which is described below. As written, this definition appears to require that entities declare each of

their internal networks as an ESP, including their corporate networks. Many entities monitor their corporate network in much the same manner as their ESPs. Requiring encryption within their corporate networks would introduce an unacceptable security risk by rendering their monitoring capabilities ineffective. ERCOT requests appropriate clarifications or that the definition be modified to specify that Interactive Remote Access and the associated technical controls be required when traffic is traversing an untrusted or public network only.
ERCOT believes that there are aspects of CIP v-5 that provide incremental benefits relative to v-4. ERCOT supports those aspects of v-5. However, the requirements in v-5 that implicate internal controls are not appropriate for NERC Standards. Accordingly, to support the beneficial aspects of v-5 moving forward, ERCOT is voting in favor of most v-5 standards, subject to the position that the requirements related to internal controls should be removed. Internal controls are not suitable for reliability standards. Entities' internal controls are beyond the scope of Section 215 of the Federal Power Act, and, therefore, beyond the scope of reliability standards. Furthermore, inclusion of internal controls in reliability standards is inconsistent with NERC's risk based initiative because they are not related to actual reliability impacts. In addition, imposition of mandatory controls in reliability standards is inappropriate because of the wide variety of organizational structures, which necessarily requires flexibility with respect to developing appropriate controls for each entity's specific circumstances. Even assuming there was any legitimate basis to include internal controls in reliability standards such requirements would be problematic in practice. The deficiency review processes in the proposed internal controls is ambiguous and susceptible to inefficient and ineffective CMEP results. What constitutes a deficiency will be an issue that is vulnerable to subjective disagreements. Even assuming there is agreement on that issue, what constitutes an appropriate remedy for a deficiency in terms of assessment and correction will similarly be susceptible to subjective disagreements. With respect to the obligation to evaluate the deficiency identification process itself, again, the potential for the introduction of subjective compliance review will be problematic in practice in terms of reviewing the merits of a decision to implement a modification or not, and, if a modification is implemented, whether the revision is adequate. This degree of subjectivity that will necessarily be required for compliance assessments of the relevant requirements is unacceptable. Accordingly, the internal control requirements would be problematic in terms of providing/gathering evidence to demonstrate an adequate level of compliance. In fact the relevant requirements are arguably similar to fill-in-the-blank type standards, which are ideal candidates for elimination pursuant to the SAR P81 effort, which FERC expressly rejected in Order 693 for this exact reason – they lacked adequate and important detail. Furthermore, there are multiple efforts by NERC and the industry related to the appropriate use of internal controls to more effectively administer the CMEP program. For example, the introduction of internal controls into the RSAW documents, the proposed inclusion of internal control requirements into COM-003, and, at issue here, the introduction of such requirements into CIPv5. Against this back drop, it may be best to reconsider the internal controls language in RSAWs and in Standards until such time that NERC and the industry have addressed the concept through the stakeholder process and determined the most effective/efficient means of utilizing internal controls in the relevant NERC programs. Although not appropriate for standards, internal controls can facilitate compliance. As such, the use of internal controls in the CMEP program is appropriate. Entities should receive CMEP benefits for utilizing internal controls. These benefits should be established in the context of CMEP policies/guidelines and/or Rules of Procedure, or, alternatively, considering incorporating such benefits/incentives in non-binding/non-exclusive measures. This use of internal controls is appropriate and should be considered by NERC in concert with industry. However, that approach is completely different than incorporating them in standards, which is inappropriate from both an authority and policy perspective. Consistent with the foregoing discussion, internal controls are inappropriate for reliability standards and v-5 should be revised to remove/revise any requirements that implicate internal controls, whether directly or indirectly. Alternative uses of internal controls in the CMEP program should continue to be reviewed by NERC in appropriate stakeholder forums.
Individual
Kathleen Goodman
ISO New England
Group
Transmission Access Policy Study Group
William J. Gallagher
CIP-002-5, Attachment 1, Section 2.12 now contains minimum thresholds for BA and GOP Control Centers to qualify as Medium Impact. There is no such threshold for TOP Control Centers, however, with the result that no TOP Control Center can be Low Impact. That is not a reasonable result; it is not the case that every TOP Control Center, no matter how small, is at least Medium Impact. TAPS supports the addition of a reasonable threshold to Section 2.12. FMPA's proposal is reasonable and objective: the threshold could be designed like Section 2.5, including >100 kV and <200 kV Facilities with a score of 350; all of the transmission Facilities under the control of the Control Center could be added up and compared to the weighted score 3000 metric of bullet 2.5 to determine if that Control Center is Medium or Low. Alternatively, the decision of whether a TOP Control Center should be considered Medium Impact could be made by the TP or PC, which have the information relevant to make such case-by-case determinations. The starting presumption could be that all non-High Impact TOP Control Centers are Low Impact, or that they are Medium Impact, or that TOP Control Centers that control Transmission Facilities over 200 kV are Medium Impact and those that do not are Low Impact. There are many ways to achieve a reasonable, supportable threshold; failing to include any threshold, however, is not reasonable or supportable. In addition,

TAPS believes that the Applicability section of CIP-002-5 is inconsistent between functional registrations: under Section 4.1.2.4, a DP that owns a Cranking Path is a Responsible Entity, and under Section 4.2.1.4, the standard is applicable to Cranking Paths owned by DPs, without limitation. Under Section 4.2.2, however, the only Elements for which TOs and TOPs must comply – including Cranking Paths - are BES Facilities. Since Cranking Paths are not necessarily BES Facilities under either the current BES definition or the proposed new BES definition, the applicability language in the standard would make non-BES Cranking Paths subject to the CIP standards, but only if owned by DPs. Non-BES Cranking Paths owned or operated by TOs or TOPs would not be subject to the standard. There is no technical justification for this difference. To achieve consistent treatment of DPs, TOs, and TOPs, as well as to take advantage of the work done to develop the proposed new BES definition and BES exception process, TAPS asks the SDT to consider changing the applicability language in Sections 4.1.2.4 and 4.2.1.4 from "Each Cranking Path and group of Elements meeting the initial switching..." to "Each Cranking Path and group of Elements that are part of the BES and that meet the initial switching...."
TAPS supports the SDT's goal of removing the "zero-defect" problem from the CIP standards. We are concerned, however, that use of "shall implement" reintroduces the problem by requiring zero-defect "implementation." We suggest replacing the word "implement" with "institute," so that the evidence required to demonstrate compliance would be, for example, proof of procedures supporting the policy instituted. TAPS suggests, as a general matter of good practice, that the SDT avoid including any requirements that would be likely to be deleted by the Paragraph 81 effort. Data retention requirements (CIP-006-5, R1.9 and R2.3; CIP-007-5, R4.3; and CIP-008-5, R2.3) fall into this category.
Group
Associated Electric Cooperative, Inc. - JRO00088
David Dockery, NERC Reliability Compliance Coordinator
AECI wishes to thank and compliment the SDT for their dedication, effort, and the improved quality of CIP Standards submitted within this third draft for Comment and Ballot, and the SDT's evidenced consideration of earlier comments. AECI is and has recommended to our membership that voting be affirmative for CIP-003-5 through CIP-011-1. Regrettably AECI is voting and recommending negative vote on CIP-002-5. We reference NRECA's comment of concern as well as their proposed wording for revision to CIP-002-5 Attachment 1 Criteria 2.12, and the related new criteria NRECA proposes within the Low Impact (L) section. If the SDT cannot adopt NRECA's proposal, we secondarily propose the SDT's providing an exclusion clause within the Criteria 2.12, for Adverse Impact Studies that determine a TOP to have no Adverse Impact to the BES, consistent with the base criteria within 2.3, yet worded to be exclusive rather than inclusive, and with assurances concerning the quality of such studies before the ERO. Such studies are of course not as simple as a Criteria 2.3 study, yet should be achievable for the class of TOP that AECI envisions exercising the exclusion. AECI is also aware of alternative wording being submitted by APPA, as well as other small entities. We bow to the SDT's expertise on weighing and selecting the most worthy proposal. Without something on the page, AECI does know and is concerned for TOPs that will be wrongfully placed into the Medium Impact Category. Even with this added consideration, CIP Version 5 will provide FERC and NERC with visibility into Low Impact Control Centers, and can then determine whether further governance is warranted. Finally, with added consideration for the smaller TOPs in place, AECI and its members can vote favorably on CIP-002-5 as well.
++CLARITY SUGGESTIONS, Referenced to Clean copies++ (1) For all Requirements including "in a manner that" language to address zero defect, please consider adding the following language to their corresponding Measures: "Where the entity is identifying, assessing, and correcting its own deficiencies, the entity is satisfactorily performing this requirement." (2) Implementation Plan, p 4, final paragraph, QUESTION: Are we to add the time allowances, corresponding with line-item events within the table that immediately follows, to the periodic times for corresponding line-item events? (3) Definitions, Interactive Remote Access, REPLACE: "access may be initiated" WITH: "access is likely initiated" RATIONALE: avoids auditors implying "may only be initiated" (4) Definitions, Protected Cyber Assets ("PCA"), REPLACE: "part" WITH: "a component", REPLACE: "within the same" WITH: "located within or composing a common", REPLACE: "same ESP" WITH: "same ESP (ie High Water Marking)" (5) General, Parts 4.1.2.3 and 4.2.1.3, REPLACE: "is subject to one or more requirements in a NERC or Regional Reliability Standard." WITH: "can affect the reliability of either Medium or High Impact Facilities." RATIONALE: DPs would benefit from additional screening clarity. (6) CIP-002-5 - Attachment 1, part 3 Low Impact Rating (L), Criteria 4.2, REPLACE: "stations" WITH: "Transmission stations" (7) General, "Applicable Systems" Columns in Tables:, bullet "Medium Impact BES Cyber Systems with External Routable Connectivity", COMMENT: "cannot be directly accessed" implies "can be indirectly accessed" so this sentence appears to stray beyond the original SDT intent. (8) CIP-004-5, R4.2 Measures COMMENT: Bottom sentence in R4 Rationale and corresponding Guidelines indicate no SDT expectation that a list of authorizations is necessary, only record of authorizations, but R4.2 becomes less clear because the phrase "list of individuals who have been authorized" appears in both Examples. Could a comparison between quarterly snapshots of provisioned individuals or groups, correlated against chronological record of user authorization changes, serve as an additional Example of the stated intent of this requirement having been met? (9) CIP-004-5, R4.3 Requirement COMMENT: Additional guidance for scope of "specific, associated privileges". Some are concerned auditors might see this as a directive for them to dig-down to individual file-access privileges, although R4 Guidelines appear to bind verification to BES Cyber System access. (10) CIP-004-5, R4.4 Requirement GUIDANCE: Wording of R4.4 appears to preclude Requirements 4.2 and 4.3, for verifying access to information storage locations for BES Cyber System information. Please clarify. ++QUALITY

SUGGESTIONS++ (1) Implementation Plan, p 3, part 6: MOVE: “CIP-006-5, Requirement R3, Part 3.1” to part 7 below, RATIONALE: 24mo periodicity. REMOVE “CIP-008-5, Requirement R3, Part 3.1” and “CIP-009-5, Requirement R3, Part 3.1”, RATIONALE: timing conflict with immediate predecessor on list, which triggers timers for these two items. (2) Implementation Plan, p 3, part 7, FYI: Conflicting 36 month periodicity but 24 month initial. (3) Implementation Plan, p 4, Previous Identity Verification, REPLACE: “R4, Part 4.1” WITH: “R3, Part 3.1” (4) General, p 6, Background, (final paragraph supporting 300 MW UVLS/UFLS), MOVE: to CIP-002-5 Guidelines and Technical Basis, REPLACE: with “see CIP-002 Guidelines and Technical Basis”

Individual

Richard Vine

California Independent System Operator

CIP-004-5 R7 - R7.2 For reassignments and transfers suggest changing the duration from one calendar day to 30 calendar days as is prescribed for terminations in Parts7.4 for the same rationale as was provided by the Drafting Team in 7.4. A transfer is not as high a risk as a termination.

Individual

Alan Johnson

NRG Energy, Inc.

CIP-003 (Cyber security policies, senior manager and delegation) 1. Background –and all standards where language for internal controls state that” each entity shall implement, in a manner that identifies, assesses and corrects deficiencies”- There is no clear mechanism identified that would explain how this will be interpreted and audited by the regional entity. 2. Requirement R2 should be revised to make it clear that it applies only to low impact BES cyber systems (it is inconvenient to have to refer back to the CIP-002 R2 and this is not consistent with the wording of R1). 3. Requirement 4- If a delegate can delegate authority to another person (as contemplated in the Guidelines and Technical Basis section), that should be made clear in the requirement itself. CIP-004 1. CIP-004-5 R2.1 contains elements which can comprise a training program. If role-based training is required (as indicated by R. 2), must all roles identified receive some training from each of the elements in R2.1? If all roles must receive some training for each of the elements in R. 2.1, what is the value of having role-based training? Customized training per roles- how many would be required? This would be difficult to identify, coordinate, implement and measure. Please provide detail as to role definition. Define if training is classified at high level description of user roles or defined by various tasks to determine training. CIP-006 VOTE YES 1. Requirement 1.7 should be revised from “within 15 minutes of the unauthorized physical access.” to “within 15 minutes of detection.” CIP-008 1. Requirement 3.1.2- implies that the Cyber Security Incident Response plan must be updated based on any documented lessons learned. However, lessons learned may not impact any change in the plan but relate to execution of the plan and performance of the personnel in that execution. This should be reworded to include “as applicable”. CIP-009 1. Although best practice, through implementation of activities as outlined in Requirement R1.5, this can result in significant impact to the BES as this can result in considerable delay to return to service following a actual recovery, particularly in a control center. DEFINITION: Control Center- as data centers are not a defined term, an entity should be able to choose what constitutes as an associated data center

Individual

Dale Dunckel

OCPD

Sections 4.1.2.1 and further 4.2.1.1 and Section 4.1.2.3 it appears in these section that a small entity that has a stand alone UFLS system with no communication is subject to a cyber security standard. Further a small entity that is part of a larger load shedding program should maintain their program, but the entity that is responsible should be the one with the cyber security based on the common control system.

Group

Hydro One

Sasa Maljukan

– To avoid possible confusion and misinterpretation we suggest changing “at least once every 15 calendar months” to “at least once in every 15 calendar months period.” – For clarification, suggest adding “mimic display” to the second paragraph of CIP-007 R5 Rationale, resulting in “Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, mimic displays etc.).” – CIP-008 R1 Part 1.2 requires reporting to the ES-ISAC which may not be acceptable to the Canadian entities. We’d like to suggest that the current wording is replaced with more general one. – We recommend changing CIP-008 R2 Part 2.1 from “at least once every calendar year, not to exceed 15 months” to “at least once in every 15 calendar months period.” – For clarity, recommend changing CIP-009 R1 Part 1.5 from “One or more processes to preserve data for determining the cause of a Cyber Security Incident that

triggers activation of the recovery plan(s), per device capability. Data preservation should not impede or restrict recovery" to "One or more processes, per device capability, to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), except where data preservation impedes or restricts recovery."
Individual
Rebecca Moore Darrah
MISO
MISO supports the latest draft of CIP Version 5 as providing greater clarity to Registered Entities regarding their compliance obligations and wishes to commend the SDT for its attention and responsiveness to much of the industry's comments on previous drafts. MISO also supports an overall shift in the emphasis of compliance from perfection to the identification, assessment, and correction of deficiencies. In particular, MISO submits that such a shift in focus from strict liability to a regime in which finding and correcting deficiencies is encouraged and in which proactive compliance is rewarded is the only logical way to ensure the security of the Cyber Assets on which the reliable operation of the Bulk Electric System is founded. At the same time, MISO is concerned that the process for determining the sufficiency of a Responsible Entity's efforts to identify, assess, and correct deficiencies is ambiguous and may lead to arbitrary or inconsistent auditing under the regional Compliance Monitoring and Enforcement Programs ("CMEP"). For instance, what constitutes a deficiency may be an issue that is subject to disagreement and varying interpretation. Moreover, the question of whether all deficiencies must be treated equally or whether Entities may implement varying levels and types of responses remains unanswered. Similarly, what constitutes an appropriate corrective measure may also be susceptible to subjective interpretation. With respect to the obligation to identify deficiencies, without further guidance from NERC, it is highly likely that auditors will take inconsistent positions on whether a Responsible Entity's efforts to identify deficiencies were sufficiently robust. Further, without this guidance, an entity is likely to continue to be audited to a strict liability regime with 'consideration' given to its processes to "identify, assess, and correct". This would result in a substantial, additional burden on Registered Entities. Additionally, underlying many of these ambiguities is the question of whether the "identify, assess, and correct" paradigm ostensibly requires the use of internal controls and whether those controls are now subject to audit. Although the September 11, 2012 Webinar specifically states that Version 5 does "not require 'internal controls' or additional process[es]," MISO respectfully submits that the assurance of the SDT on this subject is no guarantee of the verisimilitude of this assertion. More importantly, the structure and substance of an audit of these requirements may well result in a scope that encompasses a Registered Entity's internal controls. Thus, MISO requests that NERC provide, in conjunction with its submission of Version 5 to FERC, public guidance both to the industry and the regional entities containing suggestions for the implementation of "identify, assess, and correct" programs as well as delineating the properly auditable aspects of such programs and the standards that will apply to those aspects in determining compliance. Unless Responsible Entities are able to anticipate – and therefore gear their compliance efforts towards – the proposed auditing of specific aspects of their internal "identify, assess, and correct" programs, these programs will simply extend the industry's current perception of the existing CIP paradigm to the next generation of CIP Reliability Standards, e.g., substantial, administrative burden with minor benefits to the reliability of the Bulk Electric System.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments
Cyber Security Order 706 Version 5 CIP Standards

Comment Form
Combined Question 1 and Question 2 Summaries
October 26, 2012

The Project 2008-06 Drafting Team thanks all commenters who submitted comments on the Version 5 of the CIP Cyber Security Standards and its Implementation Plan for consideration by the SDT in finalizing Version 5 and related documents. The 10 standards were posted for a 30-day formal comment period from September 11, 2012 through October 10, 2012 and successive ballots through October 10, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 112 sets of comments, including comments from approximately 258 different people from approximately 153 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Table of Contents

Introduction 7

"Identifies, Assesses, and Corrects Deficiencies" Comments 8

Section 4 - Applicability 10

Draft Reliability Standard Audit Worksheet 13

"Annual" and Other Time Parameters 13

Authorized Access List and Specific Rights Reviews in Multiple Standards 14

Data Retention Requirements 15

CIP-002-5 16

Requirement R1 18

Requirement R2 20

Attachment 1 20

Criterion 1.2 21

Criterion 1.4 22

Criterion 2.1 22

Criterion 2.3 23

Criterion 2.4 24

Criterion 2.5 25

Criterion 2.6 27

Criterion 2.8 27

Criterion 2.9 27

Criterion 2.10 27

Criterion 2.11 28

Criterion 2.12 28
Criterion 2.13 31
Criterion 3.1 31
Criterion 3.4 31
CIP-003-5 32
CIP Senior Manager 32
Policy Requirements 32
Requirement R2 33
Requirement R4 33
CIP-004-5 35
General 35
Requirement R1 35
Requirement R2 36
Requirement R3 37
Requirement R4 38
Requirement R5 40
CIP-005-5 43
High Water Marking 43
Background Section 43
Consideration of Data Diodes 44
Requirement R1 44
Requirement R1 VSLs 48
Requirement R2 48
CIP-006-5 52

General 52
Background Section 52
Requirement R1 52
Requirement R2 55
Requirement R3 56
Guidelines and Technical Basis 56
CIP-007-5 57
General Comments 57
Effective Dates 57
Requirement R1 57
Requirement R2 58
Requirement R3 62
Requirement R4 64
Requirement R5 68
CIP-008-5 71
General 71
Requirement R1 71
Requirement R2 72
Requirement R3 73
CIP-009-5 75
Requirement R1 75
Requirement R2 76
Requirement R3 77
Guidelines and Technical Basis 78

CIP-010-1 79
Timeframes for Configuration Control Activities 79
Cross References to CIP-005-5 and CIP-007-5 on Impacted Controls 79
Requirement R1 79
Requirement R2 80
Requirement R3 80
CIP-011-1 82
Requirement R1 82
Requirement R2 82
Implementation Plan 83
Effective Date 83
Initial Performance of Certain Periodic Requirements 85
Previous Identity Verification 86
Planned or Unplanned Changes Resulting in a Higher Categorization 86
Applicability Reference Tables 87
Definitions 88
BES Cyber Asset 88
BES Cyber System 88
BES Cyber System Information Responses 88
CIP Exceptional Circumstance Responses 88
CIP Senior Manager Responses 88
Control Center 89
Cyber Asset 89
Cyber Security Incident 90

Electronic Access Control and Monitoring System 91
Intermediate Device (now “Intermediate System”) 91
Interactive Remote Access 92
Reportable Cyber Security Incident 93

Introduction

The Standard Drafting Team (SDT) thanks all commenters for their continued focus on providing constructive and useful feedback for improving and refining the standards. In response to draft 3 of the Version 5 CIP Cyber Security Standards, the SDT received input that was focused on several issues that assisted the SDT in refining the standards to the final set of standards now posted for recirculation ballot. The SDT carefully considered all comments in determining whether to make particular changes to the standards.

In response to comments provided to draft 3, the drafting team greatly appreciates those entities that focused their comments on the issues most critical to them, as it facilitated a qualitative representative assessment of the areas requiring the greatest review. The focus on those major concerns that were essential as a condition to find consensus was greatly appreciated.

Furthermore, the SDT wishes to thank the industry for their significant engagement and support in developing these standards. Industry participants and observers, whether formally or informally, and whether in person or through other means, provided important perspectives and subject matter expertise that facilitated the SDT's consideration of the complicated issues and technical matters reflected in these standards. This truly was a collaborative process with participation from virtually every facet of our diverse and committed industry. Security and reliability were reflected in each consideration, and the extensive and consistent industry participation throughout the process is reflected in high approvals in response to the successive ballot from draft 3 that ended October 10, 2012.

At this stage, the drafting team has reached a point where it has made a good faith effort at resolving applicable objections, and it has not made any substantive changes since posting draft 3. Therefore, the team is posting the standards, related definitions and implementation plan for a recirculation ballot. As in past drafts of the Version 5 CIP Cyber Security Standards, the SDT thoroughly considered proposed changes and evaluated them carefully by considering several important variables, such as, but not limited to, whether such changes were in the interest of cyber security and reliability, whether they would improve or reduce consensus, whether they had unintended consequences for other types of entities, and whether they were in support of the SDT's obligation to respond to regulatory directives, most notably from FERC Order No. 706. The SDT has done its best to be responsive to all inputs, recognizing that it is not possible to adopt every suggestion and also recognizing the considerable diversity of entities and assets to which the standards will apply.

In the accompanying comment form for draft 3, the drafting team asked the following two questions:

1. If, after reviewing the posted standards and General Summary of Consideration of Comments, you do not support one or more of the 10 standards, the implementation plan or set of definitions, please indicate the specific item you do not support (the standard and Requirement number, specific defined term, or implementation plan) and the specific reason you cannot support it here.
2. If you have a brief comment you would like to provide that has not already been provided among the previously submitted feedback in response to draft 1 and draft 2, please provide it here. Please limit your comment to 200 words or less.

In reviewing comments, the SDT determined that some common issues were presented by different entities in response to either Question 1 or Question 2, depending on how the particular entity organized its comments. As a whole, the SDT found that the responses were thoughtful, organized, and focused. In this summary, the SDT is responding to all comments from industry that were submitted in response to both Question 1 and Question 2 in one consolidated summary form rather than providing a separate summary for each of Question 1 and Question 2. Since most issues and comments were not isolated in response to one question or the other, this single summary provides the most efficient and thorough method with which to provide the SDT's response.

Commenters addressed a wide variety of topics in their comments, but the most commented upon subjects include comments on the Transmission Operator (TOP) Control Center Criterion in CIP-002-5's Attachment 1 and comments regarding the SDT's use of the "in a manner that identifies, assesses, and corrects deficiencies" language. The TOP topic is discussed in detail under the CIP-002-5 portion of this summary, and the "identifies, assesses, and corrects deficiencies" topic is addressed immediately below as part of this summary's general discussion. Other topics are discussed relative to their particular standard or definition, and the associated table of contents for this document lists most topics of discussion.

"Identifies, Assesses, and Corrects Deficiencies" Comments

As noted in the background sections of the standards, and in response to comments from draft 2, the SDT has incorporated within CIP Version 5 a recognition that certain Requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain Requirements. The intent is to change the basis of a violation in those Requirements so that they are not focused on *whether* there is a

deficiency, but on identifying, assessing, and correcting deficiencies. Note that, where used, the addition of language modifies "implement"; it does not itself require or specify internal controls, though it certainly enables their use for those entities that have adopted an internal controls or compliance management approach. For purposes of this summary, the "identifies, assesses, and corrects deficiencies" phrase is sometimes referenced as simply "IAC."

This topic was a source of several comments on draft 3, and the SDT appreciates the comments, feedback, and the spectrum of concern or support on this issue. The SDT believes that Version 5 is the right time to take a step in a direction that promotes security and reliability by incorporating a self-correcting aspect in certain Requirements. This is a new step, but it is informed, collectively, by implementation and audit experience from Versions 1 through 3 of the CIP Cyber Security Standards.

Many commenters support the SDT's addition of a self-correcting aspect and applaud the overall shift in the emphasis of compliance from perfection to the identification, assessment, and correction of deficiencies. The commenters support the shift from zero tolerance for deficiencies to encouraging finding and correcting deficiencies. The SDT considers such self-correction as an essential component to improved reliability and security, and it thanks commenters for their support. Though there were several specific suggestions or concerns, as noted below, the consensus position of the industry is one of support for the approach, as reflected in both comments and the overwhelming approval of the standards that use the approach.

While this is a new direction, the SDT believes there is tremendous benefit in eliminating the zero-defect language in the standards, and it is therefore worthwhile of inclusion in the CIP standards. However, the SDT acknowledges this is a developing concept and encourages the industry to continue to work alongside NERC in implementing the compliance monitoring strategy for the language.

Some commenters presented concern that there is no clear mechanism with how this approach will be audited or that there may be inconsistent audits across Regions. The SDT is well aware of this concern, and it is encouraged by ongoing coordination and support among both NERC and several regions. The SDT expects that NERC will continue to develop tools such as the Reliability Standard Audit Worksheets (RSAWs) in a manner that involves the industry and the members of the SDT. Importantly, the language to "identify, assess, and correct deficiencies" modifies "implement" where used, and it is meant simply to express that implementation of the Requirement is not in a "zero defect" manner.

Commenters also questioned whether this approach indeed does require internal controls. The SDT notes that the compliance initiatives that relate to internal controls are not the same as the approach in the standard. The SDT contemplates that the "identify, assess, and correct deficiencies" language is appropriate regardless of how compliance may be monitored, while noting that the standards approach is also supportive of the compliance approach where and if used. At its core, the SDT intends in using the language to signal an important transition to self-correction as part of the expected performance of a Requirement itself as opposed to a mere deficiency constituting the basis for violation.

Some commenters also proposed alternative, additional, or supporting language to augment the "identify, assess, and correct deficiencies" language in the Requirements or other supporting components of the standards, or proposed addition of the language to other requirements. The SDT has previously considered such alternative language and evaluated carefully where the language should be used, and, upon reexamining those proposals in response to comments, the SDT continues to support those concepts in the compliance monitoring approach and documents rather than in the standards themselves. Language noting that certain actions are not violations is too prescriptive for either the Requirements or the measures, and they do not comport with the style and form of the standards. With continuing input, coordination, and education, the SDT is confident that the Requirement language as presented is the appropriate mechanism to empower the industry to focus on correcting deficiencies as part of the expected performance of the Requirements while not requiring or prescribing a particular assessment of the how the entity accomplishes it.

Additionally, in response to perspectives expressed by commenters on the "identify, assess, and correct" deficiencies language, the SDT shares the view that NERC must ensure going forward that the compliance monitoring approach is consistent. The SDT believes that most of the industry is ready to transition to a new approach and that this reflects the consensus position. The SDT and the industry have an opportunity to incorporate significant improvements and lessons learned from implementation and audit of previous versions, and the SDT is encouraged by not only industry support, but also from NERC's direction in continuing to work with the industry in implementation of risk-based initiatives. The SDT will remain engaged after approval of the standards to work with NERC to provide input into the RSAW development process.

Section 4 - Applicability

There were many comments that "group of Elements" from the standards' applicability section, parts 4.1.2.4 and 4.2.1.4 should be deleted on the bases that it is redundant with Cranking Path and would create ambiguity, citing that these and initial switching Requirements are included in the Cranking Path. The SDT considered the language that is included in Requirement R1.5 of EOP-005-2, which says: "Identification of Cranking Paths and initial switching Requirements

between each Blackstart Resource and the unit(s) to be started." The addition of the term "group of Elements" is based on this Requirement that includes "and initial switching Requirements" in addition to the Cranking Path, and it is meant to include the group of Elements that is included in these initial switching Requirements.

One commenter requested clarification on the applicability of Section 4 with respect to Distribution Providers (DPs). The SDT notes that the clarification is included in the Guidelines and Technical Basis section of the standards relating to applicability. The guidance specifically says: "Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2." This means that DPs that own assets listed in 4.2 are subject to the standard. In addition, "For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above" are excluded from applicability of the CIP standards. That means that only systems and equipment listed in 4.2.1 are subject to the CIP Cyber Security standards.

Many commenters stated that the qualifications for applicable assets in section 4 for Cranking Paths unfairly includes non-BES facilities for DPs while excluding those from Transmission Owners (TOs) and TOPs, for which all BES Facilities are defined under section 4 as applicable. Alternate language was proposed to only include BES facilities in the scope for Cranking Paths. The SDT clarifies that those TOs that own BES Facilities as well as non-BES facilities that are qualified for DPs will also be registered as DPs. A review of the registry listing from September, 2012 showed that 232 of the 340 registered TOs (68%) are also registered as DPs. The SDT further points out that the inclusion of DPs in the applicability ensures that non-BES facilities, such as those that support the restoration of the BES, that are impactful to the reliability and operability of the BES are included.

One comment read that it appears that small entities that own stand-alone UFLS systems with no communication facilities would have applicable Requirements under these standards. It is the intent of the SDT to include all UFLS systems that meet the criteria defined in section 4. These criteria do not include any exclusion based on connectivity. The SDT points out that for DPs, only those UFLS systems that can automatically shed 300 MW or more under a common control system are qualified for applicability. The Requirements that are applicable based on connectivity are specified in CIP-003 through CIP-011. The commenter also stated that, "Further a small entity that is part of a larger load shedding program should maintain their program, but the entity that is responsible should be the one with the cyber security based on the common control system." The SDT clarifies that the owner of all qualified cyber systems is the entity responsible for compliance of these cyber systems: while the common control system that is capable of shedding 300 MW qualifies that UFLS, all cyber systems that impact the reliable operation of the UFLS system become in scope. The

responsibility for the compliance of each of these cyber systems to applicable Requirements belongs to the owner of that cyber system.

One commenter stated that the Functional Entities in section 4.2.1.3 and the Impact Rating Criteria in Attachment 1, section 3.6, for DPs to include facilities containing "A Protection System that applies to Transmission ..." is a new (initially introduced in draft 2) unsubstantiated Requirement for low impact assets. The SDT points out that among the tasks of the DP in the Functional Model is to "design and maintain protective relaying systems, under-frequency Load shedding systems, under-voltage Load shedding systems, and Special Protection Systems that interface with the transmission system." Further, the NERC Statement of Compliance Registry Criteria (Appendix 5B of the NERC Rules of Procedure) includes:

> "III.b.2 Distribution Provider is the responsible entity that owns, controls, or operates Facilities that are part of any of the following Protection Systems or programs designed, installed, and operated for the protection of the Bulk Power System:
>
> - a required UFLS program.
> - a required UVLS program.
> - a required Special Protection System.
> - a required transmission Protection System."

The same commenter suggested that the inclusion of all BES Facilities in section 4 is excessive. The SDT takes the position that cyber systems that impact the real-time operation of any BES Facility must be subject to some form of protection that is commensurate with its impact. The SDT points out that only those BES Cyber Systems that have a real-time impact to the BES are included by definition. This is also in consideration of comments in FERC Order No. 761.

Another commenter wrote that the use of the defined term "BES Facilities" in the applicability section would exclude such assets as Control Centers and Protection Systems. While these facilities are not BES Facilities per se, they are facilities essential to the reliable operation of the applicable BES Facilities and are included for applicability because of the function they are providing for reliable operation of BES Facilities.

One commenter stated that the clause "is subject to one or more Requirements in a NERC or Regional Reliability Standard" was unclear and proposed "can affect the reliability of either Medium or High Impact Facilities." The SDT believes that DPs have to comply with NERC Reliability Standards for some facilities they own and that the current clause

provides certainty as to what those facilities are since these DPs are required to comply with these standards. The SDT feels that the proposed language provides less certainty and is more subjective.

One commenter noted that exempting utility owned communications infrastructure (exemption of communications facilities between ESPs) creates a cyber security issue. The SDT believes that utility owned carrier services should be treated in exactly the same way a third party carrier is viewed in terms of trust, and that adequate protection measures should be taken to protect against an untrusted (from the BES Cyber System point of view) service provider.

Draft Reliability Standard Audit Worksheet

Some commenters provided input and feedback in their comments to the draft RSAW for CIP-006-5 that NERC Compliance Operations posted concurrently with draft 3 of the CIP Cyber Security Standards. The intent of the SDT in contributing to the development of a draft RSAW for CIP-006-5 was to begin the initiative of developing RSAWs in concurrence with standard development projects. The SDT provided input to the draft of the RSAW, and it is encouraged by the opportunity for the SDT and industry to continue to provide input as the RSAWs continue to be developed subsequent to the industry's approval of these standards. The SDT has forwarded these constructive inputs to NERC Compliance Operations for their continuing consideration.

"Annual" and Other Time Parameters

Some commenters pointed out that in a few instances, the SDT inadvertently continued to use the "at least once each calendar year (or similar)" language in conjunction with the convention to not exceed 15 calendar months. The SDT has reviewed the standards and eliminated those "calendar year" references where the SDT intended to use only the phrase "at least once every 15 calendar months."

A few commenters continued to suggest alternatives or expressed preference for retaining only the "annual" reference, which would result in continued reliance on CAN-0010. The SDT has not implemented that change because within Version 5 there is an opportunity and an obligation to unambiguously reference the periodic time parameter. The SDT also explained this in greater detail in response to draft 2 of the Version 5 CIP Cyber Security Standards on pages six and seven of summary consideration of comment form A.

One commenter expressed a desire to adopt a "once per month" convention instead of using, "At least once every 35 calendar days..." where that phrase is used. This is similar to the discussion on "annual," and for similar reasons, the SDT has not made the change. The SDT intends for these time periods to be repeatable on a basis that approximates

performance on the same day per month, or more frequently. The SDT believes it is reasonable to use 35 calendar days to account for those scenarios where a month may begin or end on a weekend, or for holidays.

Authorized Access List and Specific Rights Reviews in Multiple Standards

One commenter identified possible issues with a lack of understanding and inconsistent implementation for authorized access lists and specific rights review in Versions 1 through 3 of CIP-004 Requirement R4, CIP-003 Requirement R5, and CIP-007 Requirement R5. The commenter further stated that there was a concern that the quarterly and annual verification of CIP-004-5 Requirements Parts 4.2 and 4.3 are predicated on some generalizations and/or assumptions that are not complete and will not sufficiently resolve existing issues.

Similarly to the comment above, another commenter had issues with a lack of understanding and an inconsistent implementation for authorized access list and specifics rights review with the multiple standards as mentioned in the previous paragraph. The commenter was concerned that CIP-004-5 Requirement Parts 4.2 and 4.3 quarterly and annual verifications are predicated on some generalizations and/or assumptions that are not complete and will not sufficiently resolve the existing issues. Furthermore, the commenter stated that access authorizations and provisioning warrant further clarity in the recirculation ballot because they require significant resources, involve extensive complex data and are among the most currently violated Requirements. In response to the two aforementioned comment responses, the SDT has modified Requirement Parts 4.2 through 4.5 to state up front to which type of access each Requirement Part applies. CIP-007-5 Requirement Part 5.2 is a security hardening control applying to the enabling or disabling of generic accounts (From the Technical Guidelines section: A generic account is a group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type).

The key distinction between CIP-007-5 Requirement Part 5.2 and CIP-004-5 Requirement Part 4.3 it that generic accounts and associated privileges are not authorized nor is there the same concept of "need to know." CIP-004-5 Requirement Part 4.3 applies to user accounts only and would not necessarily indicate a full listing of user accounts and privileges on the system. However, one could envision a process by which an entity finds it more efficient to perform a full account listing and thereby produce evidence in compliance for both Requirement Parts. The SDT also point out that the identification of default or generic accounts occurs only once and does not require annual verification.

The SDT acknowledges the listing of individuals with authorized access to shared accounts (CIP-007-5 Requirement Part 5.3) has a connection to the authorization of CIP-004-5 Requirement R4 because entities must know the list of individuals

authorized to a shared account in order to fully perform the quarterly and annual assessments. However, entities may comply with the Requirement to authorize access to a BES Cyber System without specifying how they obtain such access. Overall, the SDT sees valid arguments for this Requirement Part residing in both CIP-004-5 and CIP-007-5. Because of the history of prior versions, the difference in applicability, and the significance in moving a Requirement Part to a different standard, the SDT choose to retain the Requirement in its original location.

Data Retention Requirements

There were several commenters that stated specifically and in general to exclude any data retention Requirements from the standard. In response, these few Requirements are not intended to specify a retention period as done in the Compliance section of standards, but to retain information for the purpose of incident response and analysis.

CIP-002-5

Draft 3 of CIP-002-5 obtained an affirmative ballot result of 74.9% with a quorum of 80.6% of the ballot pool at its successive ballot of October 2012. This result indicates a very significant improvement from the previous ballot and achieves a high level of stakeholder consensus.

One commenter noted an inconsistency in sub-Requirement numbering in the standard. This has been corrected and the part numbers have been changed in CIP-002-5 to remove the "R" from Requirement "R1.1", etc., to "1.1", etc.

There was a comment that stated the purpose of the standard is inconsistent with the approach, further noting that "the standard as written evaluates only the impact of a degradation to a group of Facilities instead of evaluating the degradation of a BES Cyber System." The SDT notes that the standard has taken the approach that the categorization of qualified BES Cyber Systems is based on the impact of the functions performed by the assets they are supporting. This is consistent with risk management approaches that evaluate risks based on the functional objective of the organization (in this case the reliable operation of the BES). The same entity proposed a multilevel evaluation of the impact of cyber systems based on functional impact as well as the individual impact of the cyber system within the functional impact. This multilevel approach was one that was proposed to stakeholders early in the development process: industry comments called for a simpler approach which resulted in the current one.

Another commenter stated that the CIP-002-4 and Version 5 "bright-line criteria" step away from a risk based method to a prescriptive approach. The commenter further wrote that it is an inverted philosophy from the approach draft 3 used in the other CIP Version 5 standards. The SDT notes that CIP-002-5 follows on the approach used in Version 4, which has been approved by the industry and by FERC, for using bright lines instead of an entity-defined risk-based methodology for evaluating the impact of assets, and the SDT is extending the concept with a multi-tiered approach to categorizing all BES Cyber Systems according to impact.

There was a comment that the standards use the term "Transmission stations or substations," and the commenter proposed some other terms such as "switchyards." The SDT points out that a brief clarifying paragraph is included in the Guidelines and Technical Basis explaining the use of these terms in the section on Transmission criteria: "*The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain*

autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist." The SDT also made minor editorial changes when using this term for more consistency.

There was a comment that the paragraph in the Background section that deals with the 300 MW UFLS threshold should be moved to the Guidelines and Technical Basis section. The SDT points out that section 4 is a common section that is in all the standards and believes that the explanation of the 300 MW threshold used in the common section 4 should be included in the common part of the Background section to carry it into all the CIP standards in this series.

One commenter provided general feedback on the approach taken for CIP-002-5. The commenter cited concerns on the Facilities-based approach to evaluating the impact of BES Cyber Systems. The SDT had extensive discussions in the last several years on the merits of both the systems-based and facilities-based approaches. The SDT points out to the commenter that entities are free to use any method to arrive at the identified and categorized BES Cyber Systems. Regarding the evaluation of the impact based on the function of the assets, a fundamental concept in risk management frameworks, including the National Institute of Standards and Technology (NIST) Risk Management Framework, is that the evaluation of the risk for systems must be related to the mission of the organization, in this case, the reliability of the BES. The entity also commented on the lower level of protection for low impact BES Cyber Systems. This is consistent with tailoring the level of protection according to the risk (in this case, the impact) and optimizing available protection resources for the systems that most need the protection according to their impact on the mission of the organization. The commenter also commented on the consideration of "interconnectedness". The SDT has taken the approach of considering connectivity in the development and application of Requirements.

There was a comment made that the section on BES reliability operating services in the Guidelines and Technical Basis section should be removed as it contains many subjective areas. The SDT has gone through several iterations of including these in the standards or as guidance and has resolved to providing guidance on functions for applicable functional entities based on the functional model. The section has been well-received with comments requesting the included enhancements in the past drafts.

A recommendation was made that the undefined term "adversely impact" should be replaced with "Adverse Reliability Impact" throughout the standard and definitions document to be consistent with the defined term in the NERC Glossary. The SDT disagrees, because where the SDT has used the term Adverse Reliability Impact, it has used it precisely for the meaning defined in the NERC Glossary. It is not appropriate to use the NERC Glossary term when it is not the intent of

the SDT to use the meaning of the defined term. The NERC Glossary term is very specific to a level of impact on the reliability of the BES. This is not always the appropriate level or meaning in all cases where the term "adversely impact" is used.

One commenter noted that the diagram at the end of the Guidelines and Technical Basis section is confusing. In response, the SDT notes the flowchart is an actual use case provided by an observer and may not be applicable in all environments. It is meant to provide one approach used by an entity.

Requirement R1

There were several commenters that noted there was inconsistency in the words used in Requirement R1 and Attachment 1, criterion 3.4 of section 3 (Low Impact), regarding restoration, with terms used in EOP-005-2 and with terms used elsewhere in the standard. The SDT has made changes to these sections to be consistent with the terms used in EOP-005-2: Blackstart Resources and Cranking Path and initial switching Requirements.

One commenter requested that additional reference to the specific standards be included where the term "...is subject to one or more Requirements in a NERC or Regional Reliability Standard" is used. The commenter furthermore stated that this term is not specifically used in Requirement R1 or the Requirement Parts. However, it is used in section 4 to qualify UVLS/UFLS, Special Protection Systems and Protection Systems owned by DPs that are subject to these CIP standards. In response, the SDT notes the intent is to include only those assets for DPs that are covered by a NERC Reliability Standard, which would be those, by implication, that are related to the reliable operation of the BES. References to other standards within a standard are not recommended practice in NERC standards drafting.

There was a comment that the last sentence in the opening paragraph for Requirement R1 in the Guidelines and Technical Basis section for Requirement R1 is confusing. The SDT has clarified and simplified the sentence.

One commenter stated that the use of the term "considers" in Requirement R1 leads to the same confusion as exists with the existing CIP-002-3 standard as some entities will argue that "consider" does not mandate a required subsequent action. The commenter proposes that the Requirement should be restated as "For each asset type enumerated below, each Responsible Entity shall: . . ." In using the term "considers", the SDT recognized that all entities do not own all the types of assets listed. The proposed language assumes that all entities own all of the types of assets listed. In providing this consideration, the SDT seeks to avoid situations where entities end up having null lists for each one of the type of asset that it does not own.

The same commenter stated that the assertion in Requirement Part 1.3 that the entity is not required to produce a list of low impact BES Cyber Systems renders this Requirement not auditable for accuracy or completeness; and that to demonstrate that all high and medium impact BES Cyber Systems have been properly categorized, the entity must be prepared to produce a list of all BES Cyber Systems that were evaluated, the remainder of which represent the low impact BES Cyber Systems. The commenter further stated that the entity must be prepared to demonstrate the minimal Requirements applicable to low impacting BES Cyber Systems have been properly implemented, also requiring a list of impacted systems. The SDT has considered the considerable increase in the scope of cyber systems included in this version and has taken the approach that those Requirements that apply to the anticipated large number of low impact field systems should be focused on program components that provide the corresponding level of protection, rather than a disproportionate effort in managing compliance for these systems.

One commenter suggested the removal of Requirement Part 1.3 and the low impact category in Attachment 1. The SDT has taken the approach that all BES Cyber Systems should be subject to some level of protection. The SDT has provided an approach to allow the specification of the commensurate level of protection for low impact cyber systems while providing a framework that would minimize entities' compliance burden for the large number of low impact cyber systems that it anticipates.

One commenter recommended that the six asset categories included as part of Requirement R1 be removed and the drafting team instead reference Attachment 1, if needed, to ensure consistency in language as well as prevent unnecessary duplication. The inclusion of the asset types in Requirement R1 is a direct result of comments from a large number of stakeholders on draft 2 to provide some reference to asset types required to be considered in Versions 1 through 3. The SDT has made modifications to improve overall consistency within the standard.

Another commenter noted that, in Requirement Part 1.3, the intent is to provide protection at BES Facilities that do not meet Attachment 1, criteria 1.1 through 2.13. The commenter added that the wording is technically flawed and conflicts with the definitions of BES Cyber Assets and BES Cyber Systems. The commenter continued to add that, by definition, to qualify as a BES Cyber Asset and System the asset must have a 15 minute impact on reliability of the BES and that a low impact facility cannot have such an impact to the BES. The SDT points out that while the definition of the BES Cyber System and BES Cyber Asset assumes impact on the function of the Facilities, systems and equipment (asset), an asset in the low impact does not assume that it has no impact on real-time operation of the BES. The 15 minute stipulation in the definition of BES Cyber Asset describes an impact on the function performed by the low impact asset for the BES.

One question arose which asked how an auditor is to verify identification of all BES Cyber Systems that are applicable to Requirements Parts 1.1 and 1.2. There are current Requirements to identify Critical Cyber Assets in Versions 1 through 4. The SDT expects that auditors will continue to use similar methodologies used to verify compliance to such Requirements.

One commenter stated that its interpretation of Requirement R1 meant that each qualified cyber asset must be marked. This is not the intent, and the SDT does not believe that the language in Requirement R1 is specifying any such marking for cyber assets at each asset. The clause "at each asset" is purposely included in close proximity to "BES Cyber Systems," which is the phrase that "at each asset" is intended to qualify, not the word "identify". Certainly, the expectation is that the identification of the BES Cyber System would include information in some fashion about which asset it is "at". The proposed language "Identify and list each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at the asset level," does not meet the intent of the Requirement, since it must be clear that the identification must have enough information to identify the BES Cyber System, including the information on what asset it is located at.

Requirement R2

Many commenters noted that alternative, clearer language for Requirement Part 2.1 would ensure that there is no implied Requirement for updates outside of the annual Requirement review. The SDT believes the 15 month review is sufficient for categorization of BES Cyber Systems, and it has modified the language to provide additional clarity.

Attachment 1

There was a proposal that the language should be modified to specify that the applicable functional obligations referenced within criteria 1.1 through 1.4, 2.11, and 2.12 apply to only those real time tasks identified in the Functional Model. The SDT points out that the applicability of the Requirements is to BES Cyber Systems, and that the definition of BES Cyber Assets (and by reference, BES Cyber Systems) only includes those that impact real-time operation. The functional model does not define the tasks of the functional entity in terms of real-time or non-real-time, but the term real-time is used rather to describe its relationship with other functional entities.

Many commenters reiterated their comment on the rationale for categorization as high impact those Control Centers that control at least one of the medium impact facilities. The SDT responds that the localized impact of a facility at a single location is different and less impactful than the impact of a Control Center that controls one such facility and other facilities in the wide area.

There was one comment that stated Attachment 1 does not specify where within-hour generation and interchange scheduling systems related to Balancing, Managing Constraints, and Inter-Entity Coordination fall within the high-medium-low impact framework. The SDT clarifies that these systems used to perform functions that are not impactful to real-time operation of the BES, as such would not be defined as BES Cyber Systems, unless these systems are also performing functions impactful to the real-time operation of the BES. They would be included in scope in the initial scoping of supporting the functional obligations of the relevant functional entity, but systems strictly performing these functions in the absence of other functions impactful to real-time operation would fall out of scope.

There was a comment that the first bullet under the overall heading of the Guidelines and Technical Basis section for Attachment 1 makes several references to the term "BES Asset." The SDT has corrected the inappropriate capitalization of BES asset and uses the term BES asset as referenced in Requirement R1 of CIP-002-5.

One commenter expressed concerns that restoration facilities were categorized as low impact facilities. This issue was raised in comments received in previous drafts and the SDT has discussed this at length, reaching out to other NERC technical committees. After consideration of the overall risks to the availability of adequate restoration resources, the SDT's resolution was to categorize restoration facilities as low impact, as explained under the Guidelines and Technical Basis section of CIP-002-5, on pages 30 and 31.

Many criteria in Attachment 1 relate to Interconnection Reliability Operating Limits (IROLs). One commenter wrote that this may be a problem in the WECC area where the RCs have not yet defined IROLs. Consultation with WECC indicated that WECC is in the process of defining IROLs and that IROLs will be defined well within the implementation timeline of these standards.

Another commenter stated that since the term "associated data centers" has been removed from Attachment 1 and that it should be removed from the Guidelines and Technical Basis section. The term has been moved to the definition of the Control Center and an additional clarification has been included where it is referenced in the Guidelines and Technical Basis section.

Criterion 1.2

One commenter noted that the 3000 MW minimum specified in criterion 1.2 is excessive and does not appropriately reflect the potential risk a network-connected Balancing Authority (BA) has not only upon its own service area but also

upon the rest of North American BA, Reliability Coordinator (RC), and TOP registered entities with which it is directly or indirectly connected via the ICCP communication networks. The SDT carefully considered discussions from stakeholders and reviewed data on the distribution of BAs that would be affected. The SDT concluded that the threshold would include the majority of BAs with significant impact.

Criterion 1.4

Many commenters noted that this criterion would require that a 1500 MW Generator Operator (GOP) Control Center take on a High impact rating, while the rest of the Facility is medium impact. The commenter added that even if the criterion is intended to apply to multiple locations, the aggregated generation should be 3000 MW or greater - consistent with the risk level assigned to a BA Control Center. The SDT points out that a control room for a single generating plant at a single location does not meet the definition of a Control Center. The criterion has not defined a specific numeric bright line for a generation Control Center. For example, a generation Control Center could control three 1200 MW generation Facilities, for a total of 3600 MW, at more than one location, and still be qualified for a medium impact generation Control Center if none of these meet criteria 2.1, 2.3, 2.6 or 2.9. It is true that if one of the generation Facilities the Control Center controls meets criterion 2.1 for 1500 MW, it would be categorized as a high impact asset.

Criterion 2.1

One commenter requested clarification on the relationship between a single plant location and a single Interconnection used in the defined term meaning. In making these qualifications, the SDT considered scenarios where sets of units within a single plant location may service multiple Interconnections, as pointed out by the commenter. In these cases, the SDT wanted to ensure that the impact considered is consistent with the bright line defined in this criterion, which was based on numbers reviewed for each Interconnection. The same entity inquired about “multiple generators with different interconnection facilities which connect to different parts of the same substation.” It is not clear whether the commenter is using the general term interconnection (meaning connection to the Transmission System) or in the meaning of the defined term.

One commenter felt that the use of the word “by” in the first sentence of this criterion does not make sense and should be reworded. The use of the word provides an entity with the capability of evaluating groups of units when a single plant location may be servicing multiple Interconnections and is logically partitioned into more than one generation output. There are further qualifications which may provide additional grouping criteria, such as common cyber systems.

One commenter suggested that the 15 minute stipulation should be extended to 30 minutes to be consistent with some criteria in reliability standards. Some standards have used 15 minutes, which the SDT has used as its criterion. The commenter seems to suggest that the 15 minutes is "tighter" than 30 minutes. Extending the interval to 30 minutes would in fact reign in more cyber systems rather than reduce the number of cyber systems (by extending the criterion for real-time, more cyber systems are likely to meet this criterion than 15 minutes).

One commenter requested clarification on the term "commissioned generation." The term is used to specify generation resources that have been commissioned for operation and is intended to exclude generation that has not been commissioned for operation (such as mothballed generation, generation shut down for maintenance, or new generation that has not been commissioned for operation yet).

Criterion 2.3

There were many comments that the term "planning horizon of one year or more" is unclear and could be misinterpreted. The SDT has added guidance on this to make it clear that the planning horizon of one year or more means that the plan covers a reliability planning span of one year or more and that it does not necessarily mean that the operating day is over one year. The intent is to exclude generation required to operate or keep on operating to temporarily avoid reliability impacts.

There were many comments on the guidance relating to the role of the Regional Entity (RE)/ Regional Reliability Organization (RRO) and noted that the RE/RRO is not required to perform coordination of the actions resulting from planning studies. The commenter also noted that the term RRO is no longer the appropriate term. The necessary changes have been made.

One commenter asked whether the term "generation Facility" in this criterion is designed to cover a single unit at a facility, or all units at a single plant or Interconnection, as described in section 2.1. The SDT intended to include in this criterion all generation Facilities required to meet the designation: these can be a single unit, a set of units or all the units in the plant.

One commenter noted that the Guideline and Technical Basis section omitted the TP as one of the possible entities that could designate the generation Facilities. The SDT notes this has been corrected.

A commenter asked whether the phrase, "such as due to a Category C3 contingency" was intended to provide guidance to what faults to run and whether the term "Adverse Reliability Impact" which is used in Attachment 1, meant to be the criteria for all types of contingencies. The phrase "such as due to a category C3 contingency" is intended to provide an example of the type of condition that could lead a Planning Coordinator (PC) or Transmission Planner to designate "must run" generation Facilities. The term "Adverse Reliability Impact" is used here to qualify the reason the PC or TP would designate such generation Facilities. In response, the SDT notes it is intended to distinguish from designations made for power market management reasons.

One entity commented that the guidance provided in this section in the Guidelines and Technical Basis section referenced "Reliability Must Runs (RMRs)" and discussed the differences between market RMRs and what this criterion intended. The SDT points out that this is the reason it has avoided using the term "reliability must run" in the Requirement itself. However, this term has been used interchangeably in both contexts for lack of a better term, and that the meaning of the term and the reason for having these units differ depending on the context. The SDT has included an extended discussion of the underlying reason for the criterion in the Guidelines and Technical Basis, focusing on the long term remediation for BES deficiencies to avoid Adverse Reliability Impact. The SDT also made additional changes to the guidance to clarify the role of the RE in coordination and contracts.

There was a comment that the criterion is based on studies from functional entities that do not have applicability under this standard and on notifications from these entities. The SDT notes that these activities are implemented today and that there are TPL standards that require these functional entities to perform these studies. The standard also requires these planning entities to provide an action plan for remediation of identified deficiencies.

Criterion 2.4

In this section, medium impact is assigned to Transmission Facilities operated at 500kV or higher. One commenter noted that exclusion is warranted for distribution stations that are situated at the receiving end of a radial 500kV line. The commenter further noted that specific instances exist of 500/69kV stations whose only purpose is to provide distribution service. The applicability, which is section 4, stipulates applicability to BES Facilities for entities other than DPs. If the facility meets the qualification for designation as a non-BES facility under the definition of the Bulk Electric System, then it is not in scope for application of these CIP standards.

Criterion 2.5

One commenter noted that the 200kV floor specified in criterion 2.5 does not adequately consider the risk to the BES imposed by large regional areas that are predominately sub-200kV. The commenter noted the BES is defined as 100kV and above and the criterion needs to consider all of the BES in some manner. The SDT has not excluded any BES Transmission Facility in its applicability, but believes that not all BES Transmission Facilities should be protected at the medium impact level. The categorization is one that is based on impact, and the SDT believes that the inclusion of ALL BES Transmission Facilities at a single impact category is unjustified and defeats the concept of tiered levels of protection based on impact.

One commenter stated that, as currently defined, the values in the table force a label of critical on non-critical Facilities as proven by intricate studies performed by transmission planning engineers. The commenter recommends the values be revised as follows: Voltage Value of a Line 200kV - 399kV - Weight Value per Line - 800; Voltage Value of a line 400kV to 499kV - Weight Value per Line - 1300. The SDT based the values in the table on values published in an engineering report, has reviewed comments from previous drafts, and believes that it has a technical basis, as described in the Guidelines and Technical Basis section, for using these values.

A commenter provided an extensive discussion of the concerns on the application of this criterion for Direct Current (DC) Facilities. The commenter argued that in the case of DC Facilities, the impact is better assessed in a wide area perspective rather than as a localized way as specified in this criterion. The commenter further commented that such studies could be conducted to provide an impact based on MW rather than the approach used in 2.5 in the case of DC Facilities. The SDT has not considered this approach for DC Facilities and any criterion that is based on a “study” (that is not currently required by any reliability standard) to determine the impact of these DC Facilities would be contrary to the bright line approach.

One commenter requested that diagrams be provided to illustrate the bullets in the Guidelines and Technical Basis. The SDT discussed providing diagrams to illustrate the bullets, but resolved that there are many configurations that can provide these illustrations and that these would raise additional questions for entities that would not be familiar with specific configurations. Entities should use their specific configuration to apply these concepts.

One commenter requested many clarifications. These are listed below with their responses:

1. Is/how is a DC line counted?
   A DC line is counted at the operating voltage for the purpose of application of criterion 2.5.

2. If you have a tie between two subs that has a transformer in series, does the line receive a weighting factor (seems to per guidance)? Do you use the higher or lower voltage? Is it the same for both ends of the line?
   If the transformer in at the site of a Transmission station or substation, it is considered as part of the Facilities of that station or substation and lines incoming and outgoing of the station or substation are considered in the application of this criterion. If the transformer is in a dedicated station, each of the stations (including the transformer station) will consider incoming and outgoing lines of the station or substation in the application of the criterion.

3. From the guidance document, it was clarified that radial facilities that only provide support for "single generation facilities" would not be included. What is the definition of a "single generation facility"? Uncertain situations might include two base load turbines aggregated on one line or wind farm collector subs which have multiple sites feeding into a single high voltage collector sub?
   These examples are all considered as a radial connection to a single generation facility.

4. From the guidance document, in the last bullet on page 27, it is not clear what the statement "In these cases" is referring to, whether the designation as a single facility or multiple facilities.
   The clause "In these cases" is qualified further by "of these transformers being within the "fence" of the substation or station": this is referring to what is considered a single facility.

5. From the guidance document, in the last bullet on page 28. How would classification of the number of substation connections be handled if two lines are parallel between the same two subs, but one has been tapped for local, non-networked load service?"
   Assuming that the tap is at the station or substation, these would be considered connections to one other substation, but both outgoing lines would be counted for the purpose of aggregate weighting. If the tap is not at the station or substation, there is not enough information to definitively make a determination without evaluating the specific facts and circumstances.

One commenter inquired during the comment period on whether the connections to other stations or substations that are considered are only those that are operating at voltage levels between 200kV and 499kV. The SDT reviewed previous drafts and clarified the criterion to ensure that the qualification of voltage levels of 200kV and higher for these connections is more explicitly stated rather than implied.

Criterion 2.6

One comment was on the obligation for the RC with respect to IROLs. RCs are required to provide to its TOPs in its RC footprint the SOLs under FAC-014-2, Requirement R5.1. In particular, it requires the RC to provide specific information related to IROLs in the sub-Requirements of 5.1. The particular agreements between RCs, TOs and TOPs to enable the proper management of IROLs in compliance with the NERC Reliability Standards are beyond the purview of the guidance. The SDT points out that the delegation of functional obligations must be considered in these Requirements.

Criterion 2.8

A commenter noted correctly that Transmission Facilities under 2.8 that do not affect Transmission, in aggregate, for generation that is less than 1500 MW do not qualify under this criterion, even if the generation facility (plant) contain cyber systems that qualify under 2.1., (provided they do not qualify under other criteria).

Another commenter noted that, in the case where the generation is not owned by the TO/TOP would be at the mercy of the Generation Owner's (GOs) application of the standard even if the TO's facilities would not otherwise be in scope. The commenter is correct in that the TOs Facilities providing the connection would be deemed to be a medium impact. This is consistent with the impact of these Transmission Facilities on the BES.

Criterion 2.9

One commenter requested clarification on what an automated switching system is. Automated switching systems refer to systems implemented in software that perform the same automated protection functions as Special Protection Systems or Remedial Action Schemes.

Criterion 2.10

One commenter stated that the guidance document specifies that the SDT "chose the term 'each' to represent that the criterion applied to a discrete System or Facility". The commenter's interpretation of this statement is that a regional UFLS program which sheds more than 300 MW and is comprised of multiple independent UFLS relays in at different substations would not be given a Medium Impact Rating at the NERC or RRO program level and that an individual relay would only be given a Medium Impact Rating if that relay shed more than 300 MW by itself. The commenter's interpretation is partially correct in that individual independent relays that are part of a UFLS system that sheds 300 MW or more in the program Requirements, but do not shed the required load by a common control system, (e.g., they individually trigger independently, even if they are configured to trigger based on the same sensed conditions) do not qualify. However, if the individual relays are all triggered automatically by a common control system that determines

that conditions warrant the action (such as a control panel that triggers a system of relays in a substation), then they are part of a load shedding system that can automatically shed more than 300 MW and therefore qualifies. The commenter's assertion that a single relay that sheds 300 MW or more does qualify is correct.

The same commenter noted the statement on ERCOT's LaaR demand/response program is not considered as qualifying under this criterion and requested more general guidance in the Guidelines and Technical Basis section for this criterion that talks to these types of programs. The SDT has included a more general statement in this section.

Criterion 2.11

There was a comment that the Guidelines and Technical Basis section on this criterion incorrectly referenced a 300 MW threshold. The SDT has made the necessary correction.

Criterion 2.12

Many comments related to the portion of criterion 2.12 of Attachment 1 that is applicable to TOP Control Centers. Commenters stated that criterion 2.12 of Attachment 1 included all TOP Control Centers, not already categorized in the high impact category, as medium impact and that many smaller TOP entities' Control Centers should be categorized as low impact in the same manner that criteria were defined for generation and balancing authority Control Centers. Many commenters proposed alternate proposals for a threshold that could provide such a criterion to be used as a candidate for categorization as low impact, such as voltage levels lower than 200 KV or using throughput indicators similar to those used in the case of transmission substations in criterion 2.5. Others provided proposals to restructure the thresholds for all three impact levels for TOP Control Centers. One commenter also proposed an exclusion clause in criterion 2.12 that would be based on engineering analysis that demonstrated minimal impact to the BES. In response, the SDT did not find any such study that would be required by an existing NERC Reliability Standard.

As part of a consolidated response to more than one entity that provided comments on draft 2's CIP-002-5, Attachment 1, criterion 2.11 (which maps to criterion 2.12 in draft 3 and draft 4), the drafting team carefully considered comments to include a threshold for TOP Control Centers, but, to reiterate previous considerations and response to the comments related to that criterion (on page 35 of consideration of comments form A), such a threshold is not supported in consideration of the functions provided by those Control Centers. The largest concentration of cyber traffic is to and from Control Centers, and loss, compromise, or misuse of cyber systems at control centers constitutes a high risk to reliability. Furthermore, criterion 2.12 applies to "Control Centers" used to perform the functional obligations of TOPs, so it is only applicable to the extent the Control Center meets the criteria of the proposed definition.

While there is clear guidance in the NERC Reliability Standards that the SDT could use to determine bright lines for generation in the wide area (such as contingency reserve Requirements), the SDT did not find any in the Transmission area to support thresholds for TOP Control Centers. The source for transmission substation bright lines, based on throughput in a Transmission station or substation according to voltage level, provided easily measureable thresholds because of their localized nature: for a given single location, the application of the threshold criteria can be easily determined. There was no bright line that the SDT could find applicable and justifiable in a wide area situation for TOP Control Centers that control many interconnected Transmission Facilities in many locations. The SDT could not find any technical guidance, either in NERC technical studies, or in existing NERC Reliability Standards Requirements, on how the loss of interconnected Transmission Facilities could be used as a basis for establishing thresholds for TOP Control Center impact. The TOPs span of control is not limited to just Transmission lines, but to a large number of diverse Transmission Facilities that relate to the reliable operation of the BES. This complexity, together with the interrelated impact from the large number of diverse Functional Entity types that impact TOP functional obligations, make it very difficult to define a justifiable threshold that can be rationalized considering all the scenarios that could impact real-time operation for a TOP Control Center.

As stated in the guidance for CIP-002-5, the reasoning and purpose for the 1500 MW threshold for generation is different:

> "By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected."
>
> The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used."

Furthermore, the SDT has an obligation to be responsive to FERC Order No. 706, which was issued after a notice of proposed rulemaking, and several points from that order were reiterated in subsequent FERC Order No. 761. The SDT has discussed this issue very significantly in several face-to-face SDT meetings. In addition to the technical reasons and differences explained above, the SDT anticipates that any threshold for TOP Control Centers will likely be met with a directive countering such threshold upon filing for approval of these standards.

The SDT based its approach in the development of this criterion in consideration of the following comments and Directive from FERC Order No. 706 approving CIP Cyber Security Standards Version 1 and FERC Order No. 761 approving CIP Cyber Security Standards Version 4.

In its Order No. 706, Para 280, FERC supports the reasoning for its subsequent Directive in paragraph 282 with the following comment:

> "...it is difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be identified as a critical asset..."

The SDT points out that Medium and High Impact under Version 5 translate closely to "Critical Asset" under previous versions. The Directive in FERC Order No. 706, Para 282 further states:

> "Therefore, consistent with the discussion above, the Commission directs the ERO, through the Reliability Standards development process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets."

As explained earlier, the SDT's consideration of misuse of TOP Control Centers and the role they provide, pursuant to this Directive, do not support an exclusionary threshold from medium impact in CIP-002-5, Attachment 1.

In its Order 761 approving NERC CIP Cyber Security Standards Version 4, FERC commented in paragraph 21 that:

> "...Version 4 will offer an increase in the overall protection for bulk electric system components that clearly require protection, including control centers"

In the same Order 761, Para 57, FERC further commented with the following:

> "However, we continue to expect comprehensive protection of all control centers and control systems as NERC works to comply with the Requirements of Order No. 706."

Again, in the case of Generation and BA Control Centers, the SDT used the 1500 MW threshold for consistency with the rationale used for generation bright lines. As stated, no such source can be used for wide-area transmission in the non-CIP reliability standards or other published source.

Therefore, the SDT opted to keep criterion 2.12 as it applies to TOP Control Centers (i) to ensure that all TOP Control Centers are adequately protected, in the absence of technically justifiable thresholds for lower impact TOP Control Centers, (ii) because of the critical nature of their real-time reliability functions for the interconnected Transmission systems they monitor and control, and (iii) in consideration of FERC comments and Directives expressed in Order No. 706 and reiterated in Order No. 761.

Criterion 2.13

One commenter believes that the 1500 MW minimum specified in criterion 2.13 is excessive and unreasonably excludes a significant number of BAs from meaningful participation in protecting the BES from cyber-attack and that establishing criteria effectively eliminates significant numbers of interconnected control centers fails to address the specific concerns outlined in both FERC Order No. 706 and FERC Order No. 761. The SDT considered the MW distribution of BAs and determined that the 1500 MW is consistent with generation thresholds established (and approved by FERC in Version 4) in other criteria and is appropriate in including a significant number of BAs at the medium impact category. The SDT points out low impact cyber systems are still subject to protection Requirements.

Criterion 3.1

There was a comment that criterion 3.1 should specifically state that only Generation and BA Control Centers are included. While combination of the criteria for Control Centers currently results in only Generation and BA Control Centers, this criterion is intended to catch all Control Centers that have not already met a previous criterion in section 1 and 2 (high and medium impact). The current language conveys this intent.

Criterion 3.4

One commenter stated that the use of the terms “critical” and “initial system restoration” in criterion 3.4 is problematic. The commenter noted that initial system restoration is not a defined term and registered entities have regularly argued that none of their resources are critical as they have many options from which to draw upon. The SDT has made modifications to the criterion that uses language consistent to EOP-005-2 and defined terms.

The commenter also noted that the Low Impact Rating criteria needs to include automatic Load shed systems that do not shed sufficient Load to meet criterion 2.10. All Load shedding systems that are part of the BES are included automatically as stated in the Applicability section (section 4). For DPs, Load shedding systems that meet the qualifications in section 4 are included and are all included as medium impact.

CIP-003-5

CIP Senior Manager

A commenter expressed concern on the designation of the CIP Senior Manager by a "high level official" and whether that official could be the same person as the CIP Senior Manager. The SDT notes that the language regarding "high level official" is but one example in the measure. An entity is free to determine the best way to designate a CIP Senior Manager for its unique circumstance. This could be by high level official, by committee, through authorization from a board of directors, or from any number of other options.

The SDT received a comment that there was a concern that by only requiring the identification of the CIP Senior Manager by name that the Requirement was not auditable in instances where multiple individuals have the same name at the same company. The SDT appreciates that this is a very real scenario. However, the SDT believes that this is specifically the style of auditing that it sees is incompatible with the objectives it is setting out to achieve. The SDT believes that real cyber security program leadership transcends the name on the document. Audits, instead of verifying a name on a page, should instead validate the Requirement objective that the individual identified as the CIP Senior Manager is in fact leading and managing the implementation and continuous adherence to the CIP standards.

One comment indicated that "The CIP Senior Manager relies on both the definition in the CIP Glossary and the "Responsible Entity" verbiage in every standard in section 4." The SDT does not agree. The definition of a CIP Senior Manager stands alone. However, the Requirement itself is for the Responsible Entity (the entity obligated to comply with the standard) to identify a CIP Senior Manager.

Policy Requirements

One commenter expressed concern that the SDT was too prescriptive in its language around electronic access controls in the low impact policy. The SDT does not believe this to be the case. On the contrary, the SDT has some concern that it may have left the policy up for too much interpretation. However, the SDT believed that the entity is in the best place to determine the appropriate access controls for its given situation, while still implementing an ESP of some form.

Numerous commenters expressed confusion over the applicability of the policy Requirements. The SDT considered many approaches to this issue and believes that the applicability of these requirements is clear as drafted. Requirement R1 applies to high and medium BES Cyber Systems and states as much explicitly in the Requirement. The intent of

Requirement R2 is to apply to those assets that contain low impact BES Cyber Systems and not to the BES Cyber Systems themselves. This effectively allows the entity to track implementation of the policy at a higher level of abstraction (per asset rather than per BES Cyber System), and the SDT believes this will substantially reduce the burden of evidence required by the low impact policy. The reference to CIP-002-5 is to further clarify the intended reference to asset rather than BES Cyber System. The language following the numbered list specifying that "an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required" is part of the Requirement language of Requirement R2 and should be interpreted as such. This language was explicitly included to give the industry the assurance that this Requirement would be audited (sampled) at the asset (substation, generation plant, etc.) level and not the individual Cyber Asset level. The SDT also believes that entities will be able to implement internal controls to ensure the implementation of the cyber security policy at its low impact assets. The SDT does not believe that there is any double jeopardy between Requirements R1 and R2.

One commenter suggested that the SDT modify the Requirement language for the cyber security policies to clarify that multiple policy documents could "collectively" address the topics in the Requirements. The SDT agrees and has updated the standard to reflect this change.

The SDT received comments that Requirements R1 and R2 require annual review of the policy, but never explicitly require the policy to receive updates as a result of that review. The SDT believes this is implicit in the Requirement, and updates would occur as part of an entity's ongoing compliance with the Requirement.

Requirement R2

One commenter questioned the necessity of Requirement Part 2.4 considering that entities are not required to monitor for incidents to their low impact BES Cyber Systems. The SDT appreciates this concern. This element was specifically included because the SDT strongly believes that incident response is a key component of a resilient system. Even though an entity may not be constantly monitoring for a Cyber Security Incident at its low impact BES Cyber Systems, the SDT expects that should an incident be discovered, a plan should be in place for rapid execution.

Requirement R4

The SDT received comments requesting that language be added into the Requirement clarifying that the delegation authority may itself be delegated. The SDT considered adding language to the standard to clarify this, however, the SDT believed that the Requirement was clear as is and that there was no language that prevented this delegation. The SDT included the discussion on this topic in the Guidelines and Technical Basis section specifically to clarify this issue.

One commenter pointed out that Requirement R4 as written requires that the delegations from the CIP Senior Manager be updated within 30 days of the initial delegation. The SDT agrees this is confusing and has struck this language from the Requirement.

The SDT received questions on why it included the IAC language on the Requirement to delegate authority from the CIP Senior Manager. The SDT specifically included the IAC language because it believes that in a very large organization, it is likely that changes in personnel without adequate update of delegation documentation could result in very minor deficiencies that have little or no impact on the reliability of the BES. These are precisely the types of administrative violations that the SDT is attempting to eliminate from the CIP standards. The SDT believes that, given this is all a single Requirement, the documentation required in the third sentence of Requirement R4 is part of the overall process specified in the first sentence of the Requirement; consequently, the IAC language applies to all parts of Requirement R4.

CIP-004-5

General

One commenter believes that the evidence retention for verifying access should be less than the audit cycle (which is three years for BAs, RCs and TOPs), especially if the SDT plans to keep the quarterly reviews to verify that access has been properly removed. Entities are required to demonstrate compliance with the Requirements for the entire audit period for all NERC Reliability Standards, regardless of evidence retention Requirements.

One commenter noted that within each Background section (section 5) under the heading "Applicable Systems Columns in Tables" is missing the second sentence that appears in the other standards where Medium Impact BES Cyber Systems with External Routable Connectivity is also referenced in the Background sections. The SDT confirms that it intended that phrase to be consistent wherever that applicability term was used, and the SDT has modified the background to clarify that intent.

There was a comment that within CIP-004-5, the definition of EACMS appeared inconsistent with the definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards", and that it could result in misidentification, misapplication or inconsistent application of standards. The SDT has modified the background section with respect to EACMS to provide clarification that these are examples only that support the definition.

Requirement R1

A few commenters requested that Requirement R1 include the IAC language. In response, since the Requirement may be performed at any time during the quarter, the addition of the IAC language would not be appropriate.

One commenter requested clarification on the types of materials to be provided for security awareness on a quarterly basis. The Requirement is to provide an ongoing reinforcement that cannot be provided by an annual training Requirement. The SDT has written the Requirement to allow for flexibility in implementation by the entity. The measure provides some examples of how the entity may meet this Requirement.

A few commenters considered Requirement R1 to be administrative in nature and suitable for elimination pursuant to the SAR Paragraph 81 project. While this Requirement is partly administrative, it does provide the benefit of the entity being able to timely address and make staff aware of emerging threats and vulnerabilities. This awareness can improve security for the entity.

One commenter requested that Requirement Part 1.1 be modified as, "cyber security practices and/or physical security practices." The SDT clarified that the Requirement part applies to cyber security, which may include awareness on associated physical security.

Requirement R2

One commenter recommended that the training content Requirement Part 2.1 be moved to the measures. The SDT considered the training topics listed to be worthy of being listed as a Requirement for a minimal core competency in security practices. Entities are encouraged to add more topics as relevant to their needs.

One commenter recommended that Requirement Part 2.2 be modified to address newly registered entities. In response, the compliance dates for newly registered entities are addressed in the supplementary implementation plan provided with the Version 5 standards.

One commenter considers it is a security risk to address some of the concepts listed in Requirement Parts 2.1.1 through 2.1.9 with every single person with a need for physical or cyber access to a cyber system, regardless of his or her role. The SDT believes that, as written, the Requirement is flexible to allow the entity to design and implement a security training program that fits their needs. The Requirement does not preclude an entity from using a single or multiple training courses with differing depth in the training provided.

Several commenters requested clarification on the necessary training for personnel based on individual roles, functions, or responsibilities, including changes to roles, functions, or responsibilities. The SDT believes that, as written, the Requirement is flexible to allow the entity to design and implement a security training program that fits their needs. The Requirement does not preclude an entity from using a single or multiple training courses with differing depth in the training provided. How the training program is implemented is at the discretion of the entity.

One commenter requested that CIP Exceptional Circumstances be removed from Requirement Part 2.2, as this applies to numerous parts and is stated at the policy level. The SDT believes that, as written, the Requirement provides necessary guidance related to the Requirement without introducing the need to rely on or link to other Requirements.

One commenter requested clarification on whether the training required by Requirement R2 extends to contractors and vendor support staff. The SDT notes that, as written, the Requirement is clear that training is to be provided to anyone having authorized electronic access and authorized unescorted physical access.

One commenter requested that Requirement Part 2.1.9 be removed. The SDT considers the training topic relevant to address the vulnerabilities of internetworked systems and to address the risks of systems that are integrated and reliant upon data from other sources to perform necessary tasks (interoperability).

Requirement R3

Several commenters noted concerns regarding Requirement R3 where employee history is not available, including the identity verification necessary to perform the criminal history check, and how to comply with these instances. The Requirement provides for this, "If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed."

One commenter requested that the timeline for personnel risk assessments pursuant to Requirement R3 be modified to 10 years to align with other governmental standards and practices. The SDT is not clear if the commenter means performed every 10 years or reviewing the prior 10 years for criminal history. The SDT has kept the timing Requirement of the existing standards as approved by FERC Order No. 706.

Many commenters requested clarification for Requirement R3 that ongoing identity verification is not required. The SDT has noted in guidance and the implementation plan that identity verification is required only initially. However, the Requirement is written to be flexible to allow the entity to design and implement their personnel risk assessment program in a manner that meets their needs to confirm identity. For some, this may include performing subsequent identity verification or it could include confirmation of previous verifications.

One commenter noted grammar concerns with the Requirement R3 table parts. The SDT believes that the overarching Requirement provides the necessary context and clarity for the table.

One commenter stated Requirement Part 3.3 unclear as to whether the evaluation process includes an expectation of clearly defined evaluation criteria for approval/disapproval of the access request. The SDT has modified the Requirement to make this clearer.

Two commenters considered Requirement Part 3.4 unclear as to whether the entity is to perform the evaluation or permits the contractor or service vendor to perform the evaluation using its own criteria with an assertion to the entity of compliance and acceptability. The SDT believes that, as written, the Requirement is flexible to allow the entity to design and implement a personnel risk assessment program that fits their needs. The entity is responsible for ensuring that the obligations of the Requirement are met by their contractors and service vendors.

One commenter requested that the table parts for Requirement R3 be modified to require that a personnel risk assessment must be complete before granting access. The overarching Requirement R3 states that a personnel risk assessment is required in order to obtain access.

One commenter requested that Requirement Parts 3.5 and 3.6 include a clause that it is subject to applicable law and collective bargaining unit agreements. This concern is addressed in the guidance provided for Requirement R3. As written, the Requirement is flexible to allow the entity to design and implement a personnel risk assessment program that fits its needs.

Several commenters requested clarification on whose identity must be verified. As written, the Requirement is clear that personnel risk assessment is to be performed for anyone having authorized electronic access and authorized unescorted physical access. This is further defined in Requirement Part 3.4.

One commenter recommended consolidation of Requirement Parts 3.3 and 3.4 into Requirement Part 3.2. As written, the Requirement defines each individual element to be performed and that these are each elements contained within the program specified by Requirement R3.

One commenter considered Requirement Part 3.3 redundant of Requirement Part 3.2. Requirement Part 3.2 is the performance of the criminal history records check. Requirement Part 3.3 is the evaluation of the records collected under Requirement Part 3.2.

Requirement R4

A few commenters noted concerns regarding the efficacy of Requirement Part 4.2. The SDT considers this Requirement as a key element for security. The intent of the Requirement is to review the accounts residing on the systems with the

records of what accounts are supposed to be on the systems. This helps to provide an assurance that accounts have not been added through malicious code and that provisioning processes are functioning properly.

One commenter recommended that Requirement Part 4.2 be removed and provide it as an example of an internal control that the Compliance Enforcement Authority (CEA) would expect to see. The SDT considers this Requirement as a key element for security. The intent of the Requirement is to review the accounts residing on the systems with the records of what accounts are supposed to be on the systems. This helps to provide an assurance that accounts have not been added through malicious code and that provisioning processes are functioning properly.

Several commenters requested clarity in Requirement Part 4.3 related to which accounts and types are subject to an annual review. Individual user accounts, user account groups or user roles are required to be reviewed on an annual basis. User account groups or user roles are to be reviewed where these are used to for role-based management of access permissions. While review of other account types (i.e.: default account) is a good security practice, it is not a Requirement under the CIP Version 5 standards.

One commenter requested clarification of Requirement R4 regarding the word “verify” and how an entity is expected to provide evidence of access control. The Requirements mandate that access is limited to only those requiring said access. It is the responsibility of the entity to determine how they can demonstrate this limitation through the use of technical or procedural controls. The SDT believes the Requirements are written to allow flexibility in implementation to allow the entity to develop a program that meets its needs. The use of access controls lists, key control processes, and log books should be considered as options.

There was a comment that the phrase “based on need, as determined by the Responsible Entity” within Requirement Part 4.1 does not add anything meaningful to the standard. The SDT added the language based on industry comment concerns to help clarify that the appropriateness is determined by the entity and not by the CEA.

One commenter stated that the concept of role-based privilege management has not been established adequately in the Requirement. The SDT believes that Requirement Part 4.1 is written with sufficient flexibility to allow the entity to implement access control processes that meet their needs. The Requirement does not preclude the use of role-based privilege management. Requirement Part 4.3 has been modified to address this concern.

One commenter requested clarity on the measures for Requirement Part 4.2. The measures are examples of how the Requirement may be met. They are not an all-inclusive list of possibilities. It would not be feasible to list all options available.

One commenter noted concerns regarding Requirement Part 4.3 related to the level of access permission review to be performed. The detailed access privileges are to be reviewed to determine if they are appropriate. This can include review of access to file systems. As noted in the guidance, "The privilege review at least once every 15 calendar months is more detailed…"

Several commenters requested clarification regarding the verification of access to information storage locations pursuant to Requirement Part 4.4. As noted in Requirement Part 4.1, there are three distinct types of access noted; (1) Electronic access, (2) Unescorted physical access into a Physical Security Perimeter (PSP), and (3) Access to designated storage locations, whether physical or electronic, for BES Cyber System Information. The intent of Requirement Part 4.4 is the review of access to BES Cyber System Information only.

One commenter requested clarification on the scope of physical access controls for BES Cyber System Information in Requirement Part 4.1.3. Physical access control for BES Cyber System Information only pertains to the protection of hard copies of said information. The hard copies of BES Cyber System Information are not required to be within a PSP, and therefore, CIP-006-5 may not apply.

Several commenters requested clarification on the phrase "within the last seven years." In order to obtain or retain access, a person must have had a personnel risk assessment "within the last seven years" of when access was provided and ongoing. The Requirement is written to be flexible to allow the entity to design and implement their personnel risk assessment program in a manner that meets its needs. For some, this may include performing personnel risk assessments more frequently.

Requirement R5

One commenter noted that Requirement Part 5.1 does not distinguish between termination for cause and termination without cause. The SDT removed the distinction between types of terminations to meet FERC Order No. 706, Paragraphs 460 and 461, requiring immediate revocation for any person no longer needing access regardless of termination reason.

There were an abundance of commenters that noted that the time frame listed Requirement Part 5.2 is difficult to comply with and is unnecessarily short when the employee is remaining with the company if the transfer or reassignment was in the normal course of business and not for disciplinary reasons. The Requirement allows for the entity to review the access for the individual and retain access as long as necessary for transition from the prior position. The timing was determined to be necessary to meet the to meet FERC Order No. 706, Paragraphs 460 and 461, requiring immediate revocation for any person no longer needing access which includes reassignment and transfer. Note that the timing is based on when the entity determines that the individual no longer needs access, which may not necessarily be the same date as the transfer or reassignment.

One commenter requested clarification for the word "removal" in Requirement Part 5.1. Removal refers to rendering the individual unable to use the access. This may be accomplished through deletion, disabling, revocation, or removal. The SDT wanted to provide flexibility in allowing any of these means to be used.

A few commenters requested clarification regarding Requirement Part 5.4 on what scenarios would fall into this category that are not covered within Requirement Parts 5.1 to 5.3. Requirement Part 5.1 is removing the person's ability for unescorted physical access and Interactive Remote Access. This can be accomplished by revoking just these elements (i.e.: RSA, VPN, Active Directory). Requirement Part 5.4 is to clean up the remaining accounts for the users, such as access to applications, databases, and other systems.

One commenter had concerns that Requirement Part 5.5 could negatively impact the reliability of the bulk electric system in cases where there is a high movement of staff between locations. In such cases the password may change so many times that it impacts people's ability to access BES Cyber Systems (they forget the password due to the high change rate). The SDT believes that due to the capabilities of these accounts, prompt changing of the password is appropriate to minimize the risk from separated employees and contractors.

One commenter requested that "termination action" be replaced with "termination" in Requirement Parts 5.1, 5.3, and 5.4. Please see the Guidelines and Technical Basis section of the standard for additional information regarding a termination action. This section addresses the concerns noted.

There was a request that the phrase "and time" be removed from Requirement Part 5.3, as it is unnecessary, given the reference to a calendar day rather than a twenty-four hour period. The SDT agrees with that clarification and has modified the Requirement to address this comment.

One commenter considers the time limits for revoking access upon terminations to be an extreme challenge. The SDT used the timeline for terminations to meet FERC Order No. 706, Paragraphs 460 and 461, requiring "immediate" revocation for any person no longer needing access, including all terminations, and the SDT believes the approach reflected in the standards is a reasonable means of accomplishing the directive.

One commenter requested consideration of Requirement Parts 5.4 and 5.5 to include Physical Access Control Systems (PACS) since some cyber assets in a PACS can also have individual user and shared accounts. The SDT considers all PACS devices to be subject to the same Requirements, regardless of impact categorization. While removal of access and changing of shared account passwords on all assets is a good security practice, it is not a Requirement under the CIP version 5 standards except where noted in Requirement Parts 5.4 and 5.5.

One commenter requested that Requirement Part 5.5 be changed to 35 days for consistency with other monthly Requirements. The time parameter in this requirement is different than the periodic performance time periods in requirement parts that use the 35 calendar days period. The SDT does not consider this action to be an ongoing monthly Requirement similar to those noted in CIP-007-5.

CIP-005-5

High Water Marking

There was a comment that per the Guidelines and Technical Basis section for CIP-005-5 Requirement R1, all of the Cyber Assets and Cyber Systems, even other BES Cyber Systems of lesser impact, within the Electronic Security Perimeter (ESP) will be elevated to the level of the highest impact BES Cyber System present in the ESP. The commenter recommended that this concept be included in section 5 background of every standard, not just in CIP-005-5 guidance. The SDT considered whether to include this in the background in each standard, but determined that it was most appropriate to make clarifying changes to the Guidelines and Technical Basis section in CIP-005-5.

Background Section

One commenter suggested that to ensure consistency between the standard and the list of "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" to update this section to reflect the same definition as used in this list. In response, these do not change or modify the definitions, but provide further background and guidance information.

There was a comment in the Guidelines and Technical Basis section that stated that an ESP is required around networks even if standalone regardless of impact classification. The commenter ask the SDT to confirm the Requirement in CIP-005-5 do not imply a list of Low Impact assets is needed. In response, the SDT has added the word 'applicable' before BES Cyber Systems in the guidelines to clarify this.

A question was raised regarding the scenario where a network switch may be divided into multiple ESPs and has one port outside the ESP that provides no routing between VLANs. Furthermore, the commenter questioned the following regarding Requirement R1.5: "does two distinct machines need to be utilized, one as a fire, and one as intrusion prevention or can it be done via one device and when the EAP is segmented into multiple network where one LAN is critical and one is non-critical; and does an IDS need to be on each network segment monitoring inbound/outbound traffic on the segment or just at the EAP monitoring inbound/outbound traffic." In response, the SDT is writing Requirements for the "what's" and leaving the "how's" to the entities to implement in ways that best protect their environments while still meeting the intent of the Requirement. These standards cannot and should not be exactly prescriptive in every possible technical situation. If that were the case, they would be constantly outdated or they would actually increase our risk by presenting a monoculture to adversaries where a vulnerability in one would be the same vulnerability in all. For the VLAN question, the SDT notes that an ESP (a logical border) is required around every network

to which a BES Cyber System is connected and any external connectivity to other networks must be controlled with an Electronic Access Point (EAP). The SDT has chosen to not prescribe precisely what protective functions must reside on what devices or what the standard network architecture must be for the reasons noted above. A method for detecting malicious communication must be present at each EAP for control centers (high and medium impact).

Consideration of Data Diodes

One commenter stated that CIP-005-5 should consider data diodes which possibly would exempt systems only with a data diode connection from "external connectivity" provisions. In response, the SDT notes that the definition of 'External Routable Connectivity' includes the term 'bi-directional' in order to handle data diode situations that physically enforce a uni-directional flow. Therefore systems behind a data diode do not have External Routable Connectivity.

Requirement R1

One commenter asked what the rationale was for standalone networks that have no external connectivity to other networks to must have a defined ESP. The intent is to define the 'Associated Protected Cyber Assets (PCAs)' and the high watermarking concept. In response, in previous versions of the CIP standards, Cyber Assets on the same network (within the same ESP) with a Critical Cyber Asset had to meet the CIP-007-5 Requirements. The definition of an ESP in Version 5 is required to carry this same concept forward, as well as to handle the new issue of what level of protection is required for these Cyber Assets now that we can have multiple impact levels within the same ESP. Therefore, if a BES Cyber System is connected to a routable protocol network, even an isolated network, the ESP (which is simply the 'logical border') must be defined as that also defines the 'Associated Protected Cyber Assets'. All of these Cyber Assets within that ESP then become 'Associated PCAs' of the highest impact level BES Cyber System in the ESP.

A commenter stated that the definition of Electronic Security Perimeter allows the Responsible Entity to serially connect certain Cyber Assets to a communications processor that, in turn, communicates to other Cyber Assets using a routable protocol, and in doing so declare that the Digital Protective Control Devices do not need to reside within the ESP and therefore are not subject to CIP standards. In response, the SDT notes that connectivity is no longer a filter that kicks Cyber Assets out of scope and makes them 'no longer subject to the CIP standards'. Cyber Assets are subject to the CIP standards based on their functionality and resultant potential impact to BES reliability. It is true that certain Requirements, such as CIP-005 Requirement R1, only apply if a BES Cyber System is connected to a routable protocol network, but that is because its main point is to secure what can enter or leave routable protocol networks on which BES Cyber Systems reside. CIP-005-5 is no longer a 'scoping standard' for what is or is not in scope of the CIP standards as a whole as it has been in the past. BES Cyber Systems are in scope of the CIP standards. CIP-005-5 Requirement R1

therefore is now back to a network security Requirement that requires controlling what can enter or leave a routable protocol network.

There was a comment that requested clarification text added to the Guidelines and Technical Basis section for Requirement R1, specifically Requirement Parts 1.3 and 1.5, to remove the operational barriers that may prevent entities from implementation encryption among sites on a BES Cyber System network using either encrypted tunnels or tunnel-less encryption technologies. The commenter provided possible language to be added to CIP-005-5 Requirement Parts 1.3 and 1.5:

> "Some Entities employ encryption as a strong measure for securing communications among discrete physical sites (e.g. data centers and control centers). Encryption (either via encrypted tunnels or group encrypted transport) effectively satisfies the establishment of 'discrete Electronic Security Perimeters' as referenced in Section 4.2.3.2 of each Applicability section. Provided the termination points of the encryption are protected within Physical Security Perimeters, the Requirements for CIP-005-5 R1.3 (inbound & outbound access permissions and deny-by-default) and CIP-005-5 R1.5 (inbound & outbound malicious traffic inspection) may be achieved at central firewall(s) protecting the BES Cyber System network to which the ESPs are connected. For traffic communicating within the encrypted network, the CIP-005-5 R1.3 and CIP-005-5 R1.5 Requirements do not need to be duplicated at the encryption endpoints. This enables effective implementation of encryption, which might not otherwise be operationally feasible if traffic inspection were required inside of the protected network due to the latency and convergence delays that are introduced."

In response, The SDT believes the Requirements as written do not preclude the use of encryption. However, encryption alone does not constitute an ESP or EAP. For example, if malware is introduced via portable media to a BES Cyber System and it tries to communicate outbound to a command and control server to get further instructions or provide remote access to the BES Cyber System, the fact that there is an encrypted tunnel up to the next higher level site does not provide an EAP where the communications are inspected to determine whether they should be allowed or not. If an entity wishes to state that a wide area network of sites are within one ESP, regardless of encryption, then all Cyber Assets (which includes, e.g., all communication or networking equipment) within that very large ESP become associated PCAs and must meet the Requirements of the highest level BES Cyber System in the ESP. The standards do not preclude doing this, but there are implications that Responsible Entities should take into account.

For Requirement Part 1.2, one commenter stated that the definition of External Routable Connectivity does not anticipate a situation where serial protocol may be used over IP connectivity. The commenter provided an example, where communication between two devices may take advantage of the Ethernet ports on the devices, but run serial

protocol between the devices. Furthermore, the commenter stated that by explicitly stating, "routable protocol connection" in the definition and focusing an auditor's attention on the connection, the auditor may see the Ethernet port being used and determine noncompliance. Lastly, the commenter recommended deleting the word "connection" at the end of the definition of External Routable Connectivity. In response, the SDT disagrees. The definition is based on the type of protocol, not the transport used. Ethernet is not a routable protocol; it is a transport medium with no concept of network level addressing. It should not be assumed that transport determines protocol as routable protocols can be carried on serial lines and non-routable protocols can be carried on Ethernet. It is not a matter of transport but the protocol.

There was one suggestion in Requirement Part 1.3 that the term "permissions" can be substituted with the term "controls" to align the term with the language in the measure. In the measure, the SDT uses "access control list" as an example, and the SDT has not made a change to the Requirement language, as the use of "permissions" stems from prior versions of the CIP Cyber Security Standards. The SDT believes that the term is well-understood in this context.

One commenter had a concern with the phrase "outbound access permission" in Requirement Part 1.3 which calls for requiring inbound and outbound access permission, including the reason for granting access and denying all other access by default. The commenter furthered stated that target threat vectors to the BES Cyber Systems would be inbound to those networks and those attempts inbound into the networks need to be monitored and controlled, and that while there is the possibility that could be malicious code internal to these networks communicating, that tracking all outbound communication from one trusted network to another trusted network would more than double the monitoring that is required. In addition, the commenter stated that the CIP standards have other controls to help monitor and detect the malicious code internal to the networks. In response, the SDT does not think that having an outbound rule in an EAP that allows communication from all hosts on one internal network to all hosts on another internal network is burdensome. The benefit received of being alerted to BES Cyber Systems trying to suddenly communicate with unknown networks or hosts we believe outweighs the burden of such rules. The SDT is not prescribing the level of granularity of these rules. The intent is just that EAPs function as EAPs and don't have rule sets that allow a BES Cyber System to talk to any device in existence. The Requirement is in essence "you shall not blindly trust all hosts inside the ESP to talk to any device on earth". It is up to the entity how granular they control what the hosts inside the ESP can talk to. Some may go extremely granular and specify exactly what host can talk to what host over what port; some, due to the frequency of change or other reasons, may limit it to anything on this network can talk to anything on these other internal networks. Both are compliant. But BES Cyber Systems should probably not be able to communicate directly with all home PC's on the cable company's consumer broadband network or to any machine in unfriendly nations.

One commenter stated that Requirement Part 1.5 needed to include an explicit Requirement for real-time monitoring and/or alerting upon detection of known or suspected malicious communication. The SDT notes that monitoring and alerting is addressed in CIP-007-5, which also includes Electronic Access Control or Monitoring Systems (EACMS) (CIP-007-5, Requirement R4).

With regards to Requirement R1.5, one commenter proposed the following language: "Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. ESP-to-ESP communications within a discrete BES Cyber System shall be excluded." As an example, the communication links between a primary transmission control center and its backup control center shall be excluded. The SDT disagrees. If malicious code is trying to replicate itself from a primary control center to the backup Control Center, then this Requirement should be in place. Having both the primary and backup Control Centers compromised defeats the purpose. If the primary system is compromised via malware or remote control Trojans to the point that its integrity is gone and the entity needs to fail over to the backup while the primary is rebuilt, the backup needs this protection from the malware on the primary system. If the malware walked into the primary system via portable media or other means, an Intrusion Detection System (IDS)/ Intrusion Protection System (IPS) type system may save the backup system from compromise as well.

Another comment regarding Requirement Part 1.5 states that the Requirement is still geared towards implementing an IDS/IPS and that an IDS would not provide the additional protection for an ESP if a firewall failed. Also, the commenter noted that an IDS or IPS would provide no protection against an insider threat. The commenter closed by stating that "malicious" activity cannot be determined strictly by watching for an activity and that traffic to an ESP which is malicious may in fact appear to be normal. The qualification of "malicious" vs. "normal" requires knowing an actor's intent, which cannot always be gleaned from log entries, traffic patterns or signatures. In response, the SDT has invested many hours in these very discussions and has arrived at the current Requirement. The Order makes it clear that the alternate control is also not simply another firewall. Having two firewalls in sequence would provide no value as the rule sets would be identical. The solution the SDT arrived at for an alternate control at an EAP was to detect malicious traffic (usually implemented in today's technology via IDS/IPS as noted, but not prescribed). This would allow that if the firewall was misconfigured (e.g. an admin puts in a temporary any/any/all rule for troubleshooting and forgets to remove it after testing) then at least there would be this alternate control looking for malicious traffic and providing some means of protection which the SDT believes is the intent of the Order. As to the issue with "malicious" implying knowledge of an

actor's intent, the SDT has responded to this in previous drafts by inserting the words "known or suspected" to clarify that it is only malicious traffic that is previously known or suspected to be malicious.

Relating to requiring IDS and IPS to have firewalls, one commenter stated that it may be onerous compared to the benefit received. In response, the SDT disagrees. The SDT has already scoped this Requirement to the highest impact BES Cyber Systems which should be subject to the more stringent Requirements. The SDT believes that the benefit received from detecting malicious communications into and out of control centers far outweighs the burden.

One commenter asked for SDT clarification related to the ESP, External Routable Connectivity, and whether serially connected Cyber Assets are within scope for Requirements applicable to BES Cyber Systems with External Routable Connectivity. The SDT confirms that all BES Cyber Assets are in scope of all the CIP Version 5 standards. However, for certain Requirements, the type of connectivity limits applicability. EAPs for example, are only required around routable protocol networks to control what can get into and out of these networks. There is no EAP for a serial connection if there is no routable protocol running over it. Note that it is protocol based, not transport based. Routable protocols can run over serial transports. The same holds true for ERC – it is routable protocol based.

Requirement R1 VSLs

There was a comment that the language in the VSL should match the same language and logic as in Requirement R2. An example was provided that, the Responsible Entity should have a low VSL for not having a sub-part in its documented process, medium for not implementing one of the applicable items, high for not implementing two applicable items and severe for not implementing three applicable items, and thus, would result in a more consistent application throughout the standard. The SDT notes that it modified the VSLs for Requirement R1 in response to comments from draft 2 because of the difficulties and impracticalities of determining the measurements for graduated VSLs for Requirement R1.

Requirement R2

There was a clarification request for Requirment Part 2.2 with regards to allowing that encryption may be terminated at a firewall that protects an Intermediate Device in additoin to the Intermediate Device itself. The SDT believes that the definition of Intermediate Device provides sufficient flexibility in implementation to allow for what the commenter had requested. Additional references regarding the Intermedate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested clarification of how CIP-007-5 Requirement Part 5.1 and CIP-005-5 Requirement Part 2.3 differ. CIP-007-5 Requirement Part 5.1 refers to all user authentication; whereas CIP-005-5 Requirement Part 2 only refers to remote access.

There was a request that "where technically feasible" be added to Requirement Parts 2.2 and 2.3. The language "where technically feasible" is included in the overarching Requirement R2 to recognize that this applies to all of the Requirement Parts contained in Requirement R2, not just Requirement Parts 2.2 and 2.3.

Several commenters stated that CIP-005-5 Requirement Part 2.1 be modified to address situations where the Intermediate Device can be locally accessed (a local administrator, for example) inside the PSP. The SDT believes that, as currently written, the Requirement provides the level of protection necessary in that the Intermediate Device cannot be within an ESP and thus provides the necessary protection of the Cyber Assets within the ESP. The remaining controls for the Intermediate Device(s) provide a defense-in-depth proteciton of those systems. Additional references regarding the Intermedate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter considered that CIP-005-5 Requirement Part 2.2 does not achieve the intention, which is to have traffic inspected by the IDS in an unencrypted state. The SDT notes that, as written, the Requirement and definition of Intermediate Device, collectively; provide sufficient flexibility in implementation to allow for what the commenter has noted. It is at the entity's discretion to design their Interactive Remote Access infrastructure and monitoring to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. Please see http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested clarification of CIP-005-5 Requirement Part 2.1 regarding the protections to be afforded to an "Intermediate Device". Per the definitions of Intermediate Device and Electronic Access Control or Monitoring Systems, these devices are subject to the protection of EACMS.

There was a request for clarification of CIP-005-5 Requirement Part 2.2 as to the reasonableness to include traffic between the "Intermediate Device " and device(s) within the ESP to be in scope of CIP, as it traverses an EAP. Many instances of Interactive Remote Access originate from systems that are not within a trusted network or across the

Internet. The encryption is required to terminate before going into the ESP through an EAP. It is at the entity's discretion to design their Interactive Remote Access infrastructure and monitoring to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested that CIP-005-5 Requirement Part 2.2 be modified as "Interactive Remote Access sessions must utilize encryption to an Intermediate Device." The SDT believes that, as written, the Requirement language achieves the same concept and result.

A recommendation was made that CIP-005-5 Requirement Part 2.3 is modified as "Interactive Remote Access sessions must utilize multifactor authentication to an Intermediate Device." The SDT considered authentication to be necessary for the session, not for each device. The user may not actually log into each Intermediate Device itself.

A request for clarification was made of CIP-005-5 Requirement Part 2.2 regarding whether the "Intermediate Device" is expected to provide the encryption or if two devices are envisioned for compliance. The SDT believes that, as written, Requirement and definition of Intermediate Device, collectively, provide sufficient flexibility in implementation to allow for what the commenters have noted. It is at the entity's discretion to design their Interactive Remote Access infrastructure to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested clarification of CIP-005-5 Requirement Part 2.3 on whether the multi-factor authentication is required for the Intermediate Device, for access to the EAP or to the individual Applicable Systems. The commenter suggested the language to read "Require multi-factor authentication for initiating all Interactive Remote Access Sessions." The SDT considered authentication to be necessary for the session, not for each device. The user may not actually log into each Intermediate Device itself.

One commenter requested clarification of CIP-005-5 Requirement Part 2.1 on whether VPN is an acceptable form of remote access. It is at the entity's discretion to design their Interactive Remote Access infrastructure to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There

are case examples showing differing implementations. Please see http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

CIP-006-5

General

There were comments that CIP-006-5 does not require an entity to define a Physical Security Perimeter (PSP) and wonders if entities must assume that it is required. In response, the SDT notes that access points to the PSP must be controlled, which by definition, requires the PSP. It is not necessary to have an additional Requirement stating the existence of a PSP.

Background Section

One commenter stated that the background section includes a definition/description of "Medium Impact BES Cyber Systems with External Routable Connectivity," that notes an exclusion in the following sentence: "This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity." When this definition/description of Cyber Systems is used for the applicability in Requirements such as CIP-006-5 Requirement Parts 1.2, 1.4, and 1.5, it is used with the added inclusion of "and their associated...PCA." It appears the inclusive "and associated PCAs" statements in the Requirements negate the exclusion statement from the "Background," and makes the intended applicability of such physical security Requirements to specific Cyber Assets unclear for Cyber Assets without direct external connectivity which reside in the same ESP as Cyber Assets with direct external connectivity. In response, the exclusion in the background section states that it only applies to those Cyber Assets which are part of the BES Cyber System and not PCAs.

Requirement R1

One commenter stated that the deficiency correction language should not be added to CIP-006-5 Requirement R1 because it is a binary Requirement to either have a plan or not. The SDT notes that while the possession of a plan is binary, the implementation is not. Entities must document a plan with all of the applicable table parts and implement the plan at applicable BES Cyber Systems.

One commenter noted that the term "BES Cyber Systems without External Routable Connectivity" should be just "BES Cyber Systems". The SDT notes that "without External Routable Connectivity" is used to distinguish lesser obligations than those applying to "BES Cyber Systems WITH External Routable Connectivity".

Several commenters stated that CIP-006-5 Requirement R1 does not answer the question of how big an opening needs to be before it is considered an access point. In response, the SDT does not agree this question needs to be answered in a

standard's Requirement. This is an implementation-specific question. An entity may choose 96 square inches as its general measure, but that should not be the Requirement. Specifying exactly the qualifications of an access point would go beyond just the 96 square inch Requirement and likely cause significantly more confusion than currently exists.

One commenter did not agree Requirement Part 1.3 is responsive to the directive in FERC Order No. 706, Paragraph 573 to provide layered and complementary security procedures. In response, the SDT notes that in paragraph 575, the Commission specifically states it was not the intent to create an inflexible rule of redundant access control. The proposed Requirement meets the objective of having multiple physical access control measures. The Cyber Asset independence of these measures is not material to meeting the directive.

More than one commenter argued that Requirement Part 1.3 presents technical challenges without any additional security benefit. They request NERC to provide compliance feedback to industry demonstrating that "one or more" physical access methods have proven ineffective. In response, the SDT is addressing the directive in FERC Order No. 706, Paragraph 572. The SDT believes the proposed wording provides the most security benefit to the industry while still meeting the FERC directive.

One commenter suggested that for Requirement Parts 1.5 and 1.7 to remove the 15 minute maximum timeframe limit for issuing an alert. In response, the SDT notes that for physical security breaches, the threat is automatically severe and immediate and the 15 minute timeframe is necessary to provide a minimum expectation for issuing an alert.

One commenter proposed the words "of the unauthorized access" should be added to the end of Requirement Parts 1.5 and 1.7, but this would be redundant since detection is already qualified singularly in the Requirement Part.

There was a request for clarification if monitoring is needed on PACS inside a PSP according to part 1.7. In reviewing the possibility of combining Requirement Parts 1.5 and 1.7, the SDT found that monitoring and alerting Requirements applying to PACs could be interpreted to mean those inside a PSP. To clarify, the SDT notes that entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

One commenter stated that in Requirement Parts 1.5 and 1.7, BES Cyber Security Incident Response Plan is not a defined term and should not be capitalized. The SDT agrees and has made this change. Furthermore, the commenter noted that unauthorized physical access should not automatically trigger the incident response plan because the physical security

team and incident response team are often separate groups, and a single instance of a detection of unauthorized physical access is not necessarily a Cyber Security Incident. The SDT notes that an attempt to compromise the PSP is by definition a Cyber Security Incident, and the organization of physical security and incident response teams should not preclude the Requirement to identify the Cyber Security Incident. The physical security team's response to unauthorized physical access could be part of the organization's incident response plan.

Several commenters stated that Requirement Part 1.7 should be modified to require response within 15 minutes of the detection rather than the actual incident, consistent with Requirement Part 1.5. The SDT agrees and has made the clarification.

One commenter proposed that Requirement Parts 1.5 and 1.7 be combined because they use similar wording, but the SDT believes entities benefit by emphasizing the applicability to PACS outside of the PSP.

There was a comment that stated that Requirement Parts 1.6 and 1.7 should include badge readers outside of the PSP and access cannot be controlled as specified. In response, these Requirement Parts are separated because they must be monitored differently than those Cyber Assets inside a PSP. The SDT also notes that badge readers, by themselves are not necessarily considered PACS if they do not control the controlling, logging or alerting of access.

One commenter noted that a responsible entity needs to monitor each PACS system for unauthorized physical access to a PACS. However, there is no Requirement that the PACS be contained within a PSP. Therefore, a question was raised as to how does one control physical access to the PACS? In response, the SDT notes that PACS must control access according to Requirement Part 1.1, which is not the same level as Requirement Parts 1.2 through 1.5, but some form of access control must still exist for the entity.

Several commenters noted that Requirement Part 1.7 requires coordination with the incident response team, but CIP-008-5 does not apply to PACS. In response, the incident response plan does not apply to individual Cyber Assets, but compromise of a PSP and associated PACS is by definition a Cyber Security Incident affecting a BES Cyber System.

One commenter requested clarification on whether the issuance of an alert according to Requirement Parts 1.5 and 1.7 is automated, manual, or by choice. The SDT clarifies this is by choice of the entity.

There was a suggestion that there is a discrepancy between the change description stating PACS does not need to be inside a PSP and Requirement Parts 1.5 and 1.7 stating obligations for monitoring and alerting for unauthorized access to PACS. In response, Requirement Parts 1.2 through 1.5 applies to the BES Cyber System. PACS have a less stringent obligation in Requirement Part 1.1 to have a plan for restricting unauthorized access, but this is not the same obligation as having a PSP. The SDT has clarified the change rationale for Requirement Part 1.1.

One commenter stated that Requirement Part 1.8 should add "initial" before entry to align with the visitor control program. In response, the situation allowed for in the visitor control program is to avoid an escort continually signing in a visitor needing to perform a maintenance activity. This is not the same concern for authorized personnel who typically badge in each time without the overhead of an escort.

One commenter stated that Requirement Part 1.9 should be moved to data retention. In response, the retention of these logs serves the reliability objective of having access logs to support incident identification and response.

Requirement R2

There was a comment that the CIP Exceptional Circumstances should be removed since it applies globally at a policy level. In response, the CIP Exceptional Circumstance provision is controlled at a policy level but does not apply globally to all Requirements in the standard. The standards specify which Requirements the exception may apply to as a response to the FERC Order No. 706 beginning with paragraph 372, which directs additional guidance on policy exceptions.

Several comments stated that the Requirement could allow a visitor to go a long span of time without signing out. In response, the SDT notes the scenario of brief exit/entry intervals provided in comments is the purpose for allowing this provision. Specifying what timeframe constitutes the necessity of an exit sign-out goes beyond the security benefit provided by this Requirement Part.

Several commenters noted that the measure in Requirement Part 2.1 does not match the Requirement because the evidence does not demonstrate continuous access but discrete points in time. In response, the Requirement to have a program that provides continuous escorted visitor access can be measured by the program document. Evidence of compliance with the procedure requires discrete sampling to provide assurance in the implementation of the program.

One comment was that Requirement Part 2.2 would require manual or automated logging of entry and exit from the physical security perimeter and the Requirement for egress has not been explicitly defined as a Requirement. In response, egress logging has been required since CIP-006-3.

There was a comment that Requirement Part 2.3 should be moved to data retention. In response, R2.3 was not included as an evidentiary requirement. The SDT notes that the retention of these logs serves the reliability objective of having access logs to support incident identification and response.

Requirement R3

One commenter stated that Requirement R3 should have the language allowing an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R3 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One comment was that the 24 month interval in Requirement Part 3.1 is excessive for a normally occupied control center. In response, a normally occupied control center would also receive a significant amount of testing in the operation of access control. The objective this Requirement primarily addresses field assets where access is not tested as frequently, and the timeframe is appropriate for these assets.

Guidelines and Technical Basis

Several commenters recommended modifying the section dealing with alarms to be from “immediately after” an incident to “within 15 minutes.” This better aligns with the Requirement and the SDT agrees.

CIP-007-5

General Comments

One commenter requested guidance on how to comply with CIP-007-5 Requirements on Medium BES Cyber Systems serially connected devices with regards to patching, anti-virus, etc. on a large number of programmable protective relays; and also why other measures implemented for substation assets, such as physical protection, are not adequate. In response, the SDT notes that BES Cyber Assets by definition can have an impact on BES reliability and therefore require basic cyber security protections offered by CIP-007-5 regardless of their connectivity. For patch management, the intent is that entities know about the security patches that are available for their BES Cyber Assets, what vulnerabilities they represent, and mitigate those vulnerabilities. If a security patch for a device is only exploitable over a routable protocol connection and the device is only attached serially with non-routable protocols, then that patch would be documented as not applicable. The anti-virus Requirements and guidance already mention that the entity is to document and implement how they protect against the introduction of malicious code to the BES Cyber System. For some of the devices in the example, the entity may document that there is no method to introduce malicious code.

Effective Dates

One commenter raised a concern that the effective date of the order providing applicable regulatory approval, and Requirement Part 5.2 shall become effective 12 months later, as to provide entities more time to identify and inventory all enabled default or other generic account types. In response, it is the intent of the SDT that the entity has the accounts inventoried on the effective date, not one year later. That is why there is a two to three year implementation period so that all these prerequisite activities have sufficient time to be completed so that the entity is fully compliant on the effective date. The Requirements that require periodic reviews may have their first performance take place after the effective date, but that is outlined in the implementation plan.

Requirement R1

One comment stated that a new term of “Control Center Environment” was introduced in this standard and it could potentially have a different meaning than “Control Center”. The commenter requested clarification, and in response, the SDT agrees and has changed the term to “Control Center.”

For CIP-007-5 Requirement Part 1.2, several questions were asked about the phrase, “Protect against the use of unnecessary physical input/output (I/O) ports used for network connectivity, console commands, or removable media.” Introduction of physical port protection is “assumed” to refer to logical ports only. First, a question was raised about

strong physical access controls to BES Cyber System be a compensating control here. Second, will having the BES cyber systems in locked cabinets suffice? The Requirement is not clear if the protection has to be on the individual devices. The measures indicate signage as a potential control however this would not satisfy the Requirement the way the Requirement is written. For CIP-007-5 Requirement Part 1.2, the commenter sought clarification regarding physical I/O ports that are externally accessible. For example, most servers have PCI slots, CPU slots, memory slots, etc, which are physical I/O ports. As the standard is currently written, it would seem organizations need to disable these ports. Additionally, the language "console commands" is too ambiguous. In response, the SDT notes that many of these issues are addressed in the included guidance. FERC has stated that the PSP does not meet the intent of their Order. The SDT agrees with the 'console commands' comment and has added additional guidance to address it.

For CIP-007-5 Requirement Part 1.1, several comments were made about the phrase, ""If a device has no provision for disabling or restricting logical ports on the device, then those ports that are open are deemed needed." The Requirement does not provide any provisions for limiting access to those ports or services that cannot be disabled. The Requirement's measures ask for host-based protective measures. For those devices that are not capable of providing localized protective measures, such as relays, there is a question as to how this Requirement would be met. Previously, when a port or service could not be disabled, a TFE would require mitigation of the potential vulnerability. Under CIP-007-5, if the entity leaves these ports and services open they are in compliance but there is a question of whether the vulnerability of the device still remains. In response, the SDT notes that the Requirement does provide provision for those ports and services that cannot be disabled which is the phrase in question. If a device has no provision for disabling or restricting the ports, they are deemed "needed" and the Requirement only requires "unneeded" ports to be disabled. The intent is to not require TFEs for devices where the device does not allow for the Requirement to be met. The Requirements in CIP-005-5 for limiting inbound and outbound communications at the ESP is a mitigating factor for devices like this that do not allow for their "unneeded" ports to be disabled.

Requirement R2

There was one comment that stated the rationale specified a 30 day time frame while the Requirement states 35 days. The commenter requested that the rationale section be revised for consistency with the Requirement language. In response, the SDT agrees and has changed the rationale to 35 days to agree with the Requirement.

One commenter suggested adding "with External Routable Connectivity" to the Medium Impact applicability for the patch management Requirements within Requirement Parts 2.1 through 2.4. As justification, the commenter stated that they understand the comments of the SDT; however, the commenter believes that a combination of no external routable

connectivity, frequency of access to medium impact facilities, and policies reduces the risks to those facilities from the insider that would introduce threats ("thumb drives, laptops, smart phones") into the environment to an acceptable level. While devices with no external connectivity may have some physical access risks associated with the use of thumb drives, laptops, etc., the fact that they are isolated from other BES devices must be considered when addressing appropriate protections. The lack of external connectivity reduces the risks to that isolated device; therefore, the risk to the BES is minimal. Additionally, physical security is adequate mitigation from the external threats as once physical security is breached; there are other immediate and evident concerns that do not involve BES Cyber Systems. Alternatively, a request was made that the timeframes for Requirement Parts 2.2 and 2.3 be revised to 90 days for Medium Impact BES Cyber Systems. In response, while routable protocol connectivity is a way that systems can be compromised, it is not the only way and in many examples today is not the primary way. Insider threats (intentional and unintentional, from both employees and non-employees, from both portable media and support laptops) are means in which systems are compromised today. Therefore the intent of this Requirement is to remain aware of the vulnerabilities in the BES Cyber Systems through the security patches that are released for them and analyze and mitigate those vulnerabilities. If a system has no connectivity and a security patch is released that can only be exploited via network connectivity, then that vulnerability is already mitigated and the patch is not applicable. As to the 90 day alternative, the SDT believes that a timely analysis and plan are necessary due to the nature of the environment we are in where 'Patch Tuesday' is immediately followed by 'Exploit Wednesday' as attackers quickly reverse engineer released security patches to create and release exploit code. The SDT has not put a maximum timeframe on implementation due to numerous reliability concerns, but the analysis and mitigation planning needs to occur in a timely fashion.

There was a comment that Requirement Part 2.1 requires the Responsible Entity to identify a source or sources that the entity will track for the release of cyber security patches. Furthermore, the commenter stated, *"the corresponding guidance suggests that the third-party SCADA system vendor is an appropriate source for patch availability notification. The ability of a Responsible Entity to wait until a SCADA system vendor "certifies" a patch before requiring the Responsible Entity to begin the assessment and follow-on patching process introduces unnecessary risk to the BES. There is a significant difference between assessing a patch for applicability and assessing a patch for installability. An applicable patch may be found to be incompatible with the third-party vendor's systems, would not be certified, and should not be installed. That does not mean the vulnerability being addressed by the patch should not be mitigated, rather it is incumbent upon the Responsible Entity to protect its systems in a timely manner. The Responsible Entity needs to select a patch availability source that is timely, including the original patch provider and well recognized general information providers like US-CERT, SANS @Risk, and nCircle. There is no harm in then waiting for the SCADA vendor to certify the patch before installing it, but the Responsible Entity is at least aware of the vulnerability, can assess the risk, and take*

appropriate interim action." In response, the SDT agrees with the concept; however, the SDT does not find it appropriate to prescribe in regulation certain 'timely' sources, including private firms, that must be used. Patch monitoring services can come and go. The SDT also believes that it should not use undefined terms such as 'timely' in a mandatory Requirement, nor should it define 'timely' as it refers to the seemingly unlimited number of patch sources that will exist with the significantly expanded scope of Version 5. The SDT believes that the reliability of the BES will be better served by mandating that all vulnerabilities in all applicable BES Cyber Systems be known and analyzed by all entities than by trying to micro-manage what must occur with each system, patch, and vendor through a one-size-fits-all process. As stated in the guidance, patching systems can cause more risk to BES reliability than having a non-patched system in a given situation and the Responsible Entity, not the SDT, is in the best place to weigh these risks and develop an appropriate plan.

For CIP-007-5 Requirement 2, part 2.1, a comment was made that the patch management process for substation or plant control systems could include security patches for Cyber Assets such as panel meters, relays, controllers, Programmable Logical Control (PLCs), and other electronic devices that are part of the BES Cyber System and do not have network connectivity. In response, the SDT agrees that any Cyber Asset that meets the definition of BES Cyber Asset is included in the CIP-007-5 patch management Requirement regardless of connectivity and that is the intent. While routable protocol connectivity is a way that systems can be compromised, it is not the only way and in many examples today is not the primary way. Insider threats (intentional and unintentional, from both employees and non-employees, from both portable media and support laptops) are means by which systems are compromised today. Therefore the intent of this Requirement is to remain aware of the vulnerabilities in the BES Cyber Systems through the security patches that are released for them and analyze and mitigate those vulnerabilities. If a system has no connectivity and a security patch is released that can only be exploited via network connectivity, then that vulnerability is already mitigated and the patch is not applicable.

One commenter requested a definition in Requirement Part 2.1 for the phrase "applicable asset," and also suggested that the phrase "Applicable Cyber Asset" should be called "Applicable System" to align with wording in the column "Applicable Systems". In response, the SDT notes that individual BES Cyber Assets have patches, not systems of Cyber Assets. A system is a logical grouping of one or more BES Cyber Assets. While the applicability is at the system level, the Requirement is to perform patch management on all of the applicable BES Cyber Assets within those applicable systems.

There was a comment made on the change from 30 days to 35 days within Requirement Part 2.2. The comment was that this change allows utilities to manage patches monthly while coinciding with vendor releases, all without running into

issues of the Requirement being less than a full month. However, the commenter stated that this should be extended to 40 days to accommodate time to review the vendor releases, and that the additional five days on top of the existing 35 days will ensure that those utilities with patch management programs are not penalized due to variations in patch release dates from month to month. In response, the intent is for a process that approximates "monthly" and the SDT has already added in at least a four period to account for holidays, weekends, and other factors. The SDT does not agree that it needs further extension. Timely analysis of security patches is the goal.

Within Requirement Parts 2.2 and 2.3, one commenter requested clarification of the use of term "mitigation plan" and how it would provide value. To clarify Requirement Part 2.2 the commenter suggested mentioning that the mitigation plan is intended as an internal document and not submitted to the RE. In response, the SDT agrees and that these plans are internal documents and not submitted to the RE. In previous drafts, these were called 'remediation plans' and the SDT received comments that this term was used for what was submitted to Regional Entities in response to violations of the standard, so the SDT changed the term to 'mitigation plan' to avoid that confusion. The SDT has added this clarification to the guidance.

There was a comment with regard to CIP-007-5 Requirement Part 2.3 that reads, "Available actions to entities should include: 1) Apply the patches 2) Develop dated implementation plan 3) Create/revise existing mitigation plan". In many cases, patches will be applied, but outside of a 35 day period to accommodate outage schedules for optimizing reliability and availability of systems. In many cases, when an applicable patch is provided by a vendor, there may be no additional mitigation implemented during the time from patch availability until installation. Requiring entities to "create a dated mitigation plan or revise an existing mitigation plan will result in a paperwork exercise and yield no reliability or security benefits for the affected cyber assets. Adding an option to "Develop dated implementation plan" without requiring a mitigation plan to be created/modified permits entities to apply resources to application of patches and optimizing reliability." In response, the SDT notes that the 'dated mitigation plan' could simply consist of the date the entity plans to implement the security patch if beyond the initial 35 day period; therefore it is not simply a paperwork exercise that provides no reliability benefit. The intent of the Requirement is to mitigate the applicable vulnerabilities either through the installation of the patch or by some other means. Implementation of the patch is mitigation and having a record of the entity's plan to implement the patch is not seen as unnecessary paperwork.

There was a comment that Requirement Part 2.3 requires the Responsible Entity to either install the patch within 35 calendar days or simply create or update a mitigation plan. Furthermore, the commenter stated "there are no boundaries of what is acceptable in a mitigation plan, no expectation of justifying the decision, and no Requirement for

the CIP Senior Manager approval, thus allowing an entity to completely avoid the Requirement to patch a critical system by creating an illogical plan with unreasonable milestone dates. The need to wait for a scheduled outage at a field asset is well understood. Allowing an entity to determine patches will only be installed when the control center server is replaced (typically every four years), as has been seen during a CIP audit, is unreasonable and poses significant risk to the reliability of the BES. This Requirement does not require compensating measures appropriate to the vulnerability to be put into place until the patch is installed, thus furthering the potential risk. In effect, the provisions of this Requirement have the potential of creating a paper exercise with little value, with an expectation that the CIP auditor simply accept the documented plan without comment. (3) Requirement Part 2.4 furthers the inaction of the Responsible Entity by requiring the entity to follow the potentially illogical plan that the entity designed to avoid having to patch in the first place. As long as an extension of the plan is not required, there is still no CIP Senior Manager or delegate approval required." In response, the SDT believes that the reliability of the BES will be better served by mandating that all vulnerabilities in all applicable BES Cyber Systems be known and analyzed by all entities than by trying to micro-manage what must occur with each system, patch, and vendor through a one-size-fits-all process. As stated in the guidance, patching systems can cause more risk to BES reliability than having a non-patched system in a given situation and the Responsible Entity, not the SDT, is in the best place to weigh these risks and develop an appropriate plan. The SDT has no way to write a mandatory Requirement for a "logical" plan.

One commenter believes that the language in Requirement Part 2.4 be aligned with the language in Requirement Part 2.3. The commenter suggests that either both or neither should specify the approval Requirement of the CIP Senior Manager of delegate. The commenter recommends that the language of "…timeframe specified in Requirement Part 2.3 is approved" be added. In response, the SDT notes the CIP Senior Manager approval was added to Requirement Part 2.4 specifically to handle situations where entities might repeatedly extend their documented timeframe with no management oversight. The intent was not to have management approval of every patch in normal day-to-day processes. Entities are free to do so, but it was not the SDT's intent to make that a mandatory Requirement. Management approval of every patch on every BES Cyber Asset would tend to become a "rubber stamp" with no meaning. The SDT's intent was to have approval of exceptions so that if someone were simply moving deadlines to avoid complying with the intent of the Requirement it would be subject to management oversight.

Requirement R3

There was a comment that within Requirement Part 3.1 to consider adding the phrase "per device capability" to the beginning of the Requirement, or otherwise, if a deter posture is selected, it may be potentially in conflict with other

Requirements. In response, the Requirement is written at the system level in order to handle the device-specific issues. The SDT believes the included guidance also provides suggestions on how to handle device abilities.

With regard to CIP-007-5 Requirement 3, parts 3.1, 3.2, and 3.3, there was a comment that these three Requirement Parts do not have any timeline for action. A question was raised if an auditor will audit when the activity occurred and audit only that a process is created and executed per the registered entities process or procedure. In response, the answer to the question is yes. Malware protection is an inexact art as we are protecting against an intelligent and always changing adversary. Malware of today is quite different than malware of just a few years ago. The intent is for entities to think about the malware problem, document what they are doing about it for each BES Cyber System, and then do it. Prescribing certain technologies/tools/timeframes is not helpful in this rapidly changing area and tends to bog the industry and the regulator down in paperwork (such as TFEs) when agility in this area is required in order to protect BES reliability.

Within Requirement Part 3.2, one commenter stated that the word 'identified' is ambiguous and inconsistent with other malicious code phrases, and the commenter suggested changing the language to 'detected'. The SDT agrees with this clarification and has made the suggested change as this is how the measures and guidance were written as well.

One comment was related to the applicability section of Requirement Part 3.2. A suggestion was provided to revise this section to apply to Medium Impact assets with external routable protocol to read: "Medium Impact BES Cyber Systems with external routable protocol and their associated". In response, the SDT's intent is for the basic security protections, including malware prevention, to be applied to all BES Cyber Systems not just those with External Routable Connectivity. BES Reliability can be threatened on isolated networks of BES Cyber Systems through the introduction of malware through portable media or laptops used for support.

One commenter requested clarification on Requirement Part 3.3 which requires the anti-malware updating process to address testing of the signature or pattern file. In support of this request, the commenter stated that a number of registered entities have taken the position in the past that they address this aspect of the existing CIP Version 3 Requirement by relying upon the vendor to test before release. In response, the Requirement is taken verbatim from previous industry and FERC approved versions of the CIP standards. If the entity is obtaining tested signature updates from their control system vendor for a turnkey product, then that is compliant. The SDT does not think more prescription as to where the testing must occur is needed.

There was one comment raised that use of the term 'deter' is ambiguous and the commenter suggested replacing this language in Requirement Part 3.2. The commenter suggested replacing the language to read: "Configure the measures implemented in Requirement Part 3.1 such that it blocks or prevents access to files with potentially harmful code." This recommendation was based on the assumption that the recommendation for removal of the term "deter" is accepted in Requirement Part 3.1. In response, the SDT has purposefully added the word 'deter' so that entities are not in immediate violation of the Requirement should zero day malicious code enter the environment. There are no 100% preventions, so the SDT has added this verb to allow for that. Antivirus software tools today do deter, but do not 100% prevent.

Requirement R4

One commenter requested clarification around the last two sentences of the guidance section. The commenter also stated that currently, an entity that neglects to enable logging would be in violation. Per the Background section, a sole instance of deficiency is not grounds for a violation so long as it is adequately identified, assessed, and corrected. The statements in the guidelines seem to be relics of a previous draft which conflict with the new approach. In response, the SDT agrees and has rewritten the guidance to properly align with the Requirement.

One comment read that CIP-007-5 Requirement R4 for security event monitoring does not state any Requirements as to when the security events, particularly in Requirement Parts 4.1 (log events) and 4.2 (event alerts) are to reviewed, escalated, and mitigated. A question followed that asked if there are any Requirements for immediate action from the IT security personnel for detected failed access attempts, failed login attempts, or specific event alerts. In response, no, there are no prescriptive timeframes for response to alerts. The Requirement is to generate an alert for security events. Alerting someone to a condition is one thing, responding to the condition is dependent upon numerous variables that cannot be prescribed.

A recommendation was made to revise this Requirement to include the sentence from the guidance section, "that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment." The SDT's intent was not for the Responsible Entity to determine in totality the events to be logged, but that it must log the listed events at a minimum (subject to device capability). The Responsible Entity is free to log events above and beyond these and is encouraged to do so. However, the Responsible Entity cannot ignore the listed events.

As currently written, CIP-007-5 Requirement Part 4.1 would necessitate the logging at every Cyber Asset that is capable when there is not a network at the BES Cyber System. A suggestion was made to rewrite this Requirement to read, "for BES Cyber Systems that have Cyber Assets connected to a network via a routable protocol, log events at the BES Cyber System Level…" In response, the SDT's intent is that if a Cyber Asset has a local log on the device, then it should be utilized. For example, a completely standalone and isolated substation relay should log security events internally if it is capable of such so that if it begins misoperating there is some log to go review on the device to see if/who/when someone has accessed it. The Requirement is not dependent on external connectivity.

In Requirement Part 4.3, one commenter suggested that this is a data retention Requirement and should not be a Requirement of the standard. In response, the SDT's intent is that this is not strictly 'data retention for the purposes of audit' Requirement, but an actual cyber security Requirement to have ready access to the past 90 days of logs for the applicable systems for quick determination of potential cyber causes of reliability-affecting events. Quickly determining whether a BES event could have had a cyber security cause is a reliability-focused Requirement and the primary way to do that is to have ready access to security event logs. Configuring a system to retain the past five minutes of security event logs is of little to no value. This is a separate issue from having evidence for audits that you maintained 90 days of logs throughout the audit period.

Within the Guidelines and Technical Basis section of CIP-007-5, Requirement R4, a question was asked if the following quotation references to NIST are the guiding principles and documentation for the development of the RSAWs and auditing of this Requirement, "Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring." In response, these guidelines are not auditable, only Requirement statements are auditable. These are provided solely for use at the discretion of Responsible Entities, several of whom have asked in previous drafts for further guidance.

One commenter requested clarification on the word "review" with regard to the statement within Requirement Part 4.4 of "Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 days to identify undetected Cyber Security Incidents." The commenter questioned if an automated SIEM technology solution, which monitors real-time, would satisfy the Requirement. In response, the SDT states that the intent, as per FERC Order No. 706, is to manually review the logged events in order to ensure that automated tools such as SIEM systems are tuned appropriately and are not missing security events.

One commenter stated that CIP-007-5, Requirement R4, part 4.1.2 calls out failed access attempts and failed login attempts and is unclear as to why the phrases "failed access attempts" and "failed login attempts" are separated. The

commenter requested clarification on the following two questions: Are "failed access attempts" referring to physical attempts, and are they referring to some other form of electronic access to undermine the login process? In response, the SDT notes that as outlined in the guidance, access attempts primarily occur at EAPs and involve 'access' across the ESP. Login attempts primarily occur at the BES Cyber Systems. The monitoring Requirement applies to both situations.

A comment was issued on Requirement Part 4.1.3 that this Requirement of malicious code prevention methods to log is already contained in Requirement Part 3.2. The commenter suggested removing this Requirement. In response, the SDT notes that logging and alerting when malicious code is detected is a separate Requirement from the actual response to the alert and the mitigation of the malicious code on the BES Cyber System. The SDT sees no duplication between these Requirements.

There was a comment that within CIP-007-5 Requirement Parts 4.2 through 4.4 the Requirements and sub Requirements have become less clear than previous CIP standards versions. The commenter stated it was unclear if Requirement Part 4.4 replaces the previous monitoring Requirements in their entirety or if it represents an additional manual sampling action that occurs outside of a primary monitoring process which may be automated. The commenter suggested to consider modifying the aforementioned Requirements to make it clear to registered entities which logging is required, how logs should be monitored, and what actions are required in the event of an interruption in logging. In response, the SDT notes that Requirement Part 4.4, as noted in the Rationale and Change Justification, is in response to FERC Order No. 706 and the Directive to require a manual review of logs to insure that automated tools are not missing events. Automated tools are only as good as their rule sets, which require periodic tuning.

One commenter noted that a clarification may be needed for Requirement Part 4.2 as to whether the alert needs to be generated real-time with automatic notification or if the alert can be generated by a long after-the-fact manual review of security event logs. In response, the SDT's intent is, in general, for a real-time alert, but the SDT did not specify that as a timeframe in the Requirement because, for example, an after-the-fact review or analysis of logs would not require a computer-generated alert.

One commenter stated that Requirement Part 4.2 is a questionable and subjective Requirement as it states that an entity needs to generate alerts for security events that the entity determines necessary. In response, the SDT has set a minimum threshold of alerts that must be generated if the system is capable of it. All other types of alerts vary widely by the type of system in question and should not be prescribed. The alerts that can be generated by a Windows or Unix

server in a data center are quite different than what can be generated by some legacy purpose-built device in a substation.

A request was made to clarify Requirement Part 4.3 as to whether original source logs must be retained or if post-log analysis summaries are sufficient. In response, the SDT states that the language in the Requirement and measure provides the necessary level of clarity.

There were several comments on Requirement Part 4.4 that need to be clarified that the review of a summarization or sampling of logs is not acceptable as the primary means of log analysis and alert generation. The purpose of the manual review is to achieve a level of comfort that the log analysis tool is properly configured and is not missing important security events. A random sample review of logs otherwise runs a significant risk of completely missing security events that pose potential risk to BES reliability. Similarly, another comment for CIP 007-5, R4.4 read, in the Requirements column of the table, the draft language indicates a need to review logs to, "identify undetected Cyber Security Incidents." A question was raised if this is intended to be "identify detected Cyber Security Incidents?" Also for CIP-007-5 Requirement Part 4.4, a recommendation was made to change "undetected" to "potential". In response to the aforementioned comments, the SDT notes the intent is to review logs to insure that any automated tools or processes are tuned so that they are catching all Cyber Security Incidents, therefore the SDT believes that the 'undetected' word is correct. If attempts to breach the security of a BES Cyber System are being missed because the automated tools are not tuned or maintained, then this Requirement's intent is to catch that.

One comment read that in Requirement Part 4.4, to be consistent with other Requirements, that the phrase "15 days" be changed to "15 calendar days." In response, the SDT agrees with this clarification and has made the change.

A recommendation was provided to change the language in Requirement Part 4.2 to read "Detected failed login attempts from part 4.1." In response, the SDTs intent is that alerts be generated when it is detected that event logging has failed.

One commenter raised an issue that in Requirement Part 4.4 the words "summarization" and "sampling" components are too broad. In support of this, the commenter encouraged specificity in all measures. Additionally, the term "undetected" is unclear and confusing. The commenter stated that clarification, such as "logged but not previously selected for alerting or alarming" could be helpful. In response, the SDT has chosen to not provide further prescription but to use the words from FERC Order No. 706 to allow entities to meet the intent without prescribing exactly how to summarize or sample

the logs. Sufficient summaries or samples are dependent on many variables and do not lend themselves to a one-size-fits-all approach.

A comment was made with regard to Requirement Part 4.4 that a manual log review is a labor intensive and outdated approach. The technical guidance should allow for use of network behavior analysis or other automated review processes for this Requirement. The commenter believes that this Requirement is ambiguous. The commenter further stated that the Requirement to review 'undetected' Cyber Security Incidents is essentially a Requirement to perform manual reviews. By requiring a manual review, the entities are encouraged to record the absolute minimum event types as to minimize the burden of the manual review. Further, the Requirement to perform manual reviews would incentivize entities to not invest in systems that can perform automated log analysis and event correlation. In response, the SDT has added this Requirement in response to a directive in a FERC Order. The intent is to ensure that such automated tools are continually tuned and are not missing events that should be caught and alerted on.

A request was made to clarify Requirement Part 4.4 that the review of a summarization or sampling of logs is not acceptable as the primary means of log analysis and alert generation. Furthermore, the commenter stated that the purpose of the manual review is to achieve a level of comfort that the log analysis tool is properly configured and is not missing important security events. A random sample review of logs otherwise runs a significant risk of completely missing security events that pose potential risk to BES reliability. With regards to the Requirement column of the table for Requirement Part 4.4, the draft language indicates a need to review logs to "identify undetected Cyber Security Incidents". Is this intended to "identify detected Cyber Security Incidents"? One last comment was a suggestion to change the word "undetected" to "potential". In response, the SDT states that the intent is to review logs to insure that any automated tools or processes are tuned so that they are catching all Cyber Security Incidents, therefore the SDT believes that the 'undetected' word is correct. If attempts to breach the security of a BES Cyber System are being missed because the automated tools are not tuned or maintained, then this Requirement's intent is to catch that.

Requirement R5

There was a comment that the TFE language in CIP-007-5 Requirement Part 5.6 is unnecessary since technical or procedural controls can be used and that the phrase "per Cyber Asset capability" be used instead. In response, since many Cyber Assets used today utilize shared accounts and have no capability for individual accounts, periodically changing passwords is necessary. The SDT is aware that some systems have passwords that cannot be changed, or that if changed will break the system's functionality. Therefore, the SDT allowed for TFE's since the entity may not be able to

change the password either technically or procedurally. The SDT chose not to use the 'per Cyber Asset capability' as this is an instance where documenting and implementing some alternative control is necessary.

Within the Rationale section of CIP-007-5 Requirement R5, there was a suggestion to add the phrase “mimic display” to the second paragraph which outlines what is not included in interactive user access. In response, the SDT disagrees because the definition agreed to by the SDT is very clear and by adding another example with a non-widely used term would not add further clarity.

One commenter asked how CIP-007-5 Requirement Part 5.1 and CIP-005-5 Requirement Part 2.3 differ. The commenter stated that both appear to require authentication of Interactive Remote Access sessions. In response, CIP-007-5 Requirement Part 5.1 refers to any user access, including local access while physically present at the device. CIP-005-5 Requirement Part 2.3 refers to remote access.

A commenter believes that including specific password Requirements within a standard is contrary to new and safer technologies by the industry. In response, the SDT notes that the password Requirements have been worded in such a way that they only apply if passwords are used for authentication. If other, stronger means of authentication are used (tokens, biometrics, etc.) then the password Requirements do not apply. The Requirements are only “for password only authentication”.

One commenter stated that the term “generic account types” used in Requirement Part 5.2 is not defined and has not been well understood by entities to date. In response, the SDT notes that the term is now “default or generic” and the guidance provides some further explanation. The SDT does not believe that there is a sufficient definition of “generic” that will add any value beyond its normal dictionary definition.

One commenter suggested that within Requirement Part 5.2, alternate wording be provided to specify “known” enabled default or other generic account types. In response, the SDT agrees and has made the recommended clarification. The SDT notes this concept was already included in Requirement Part 5.4 and has included it here in Requirement Part 5.2 as well.

One commenter stated that Requirement Part 5.4 needs to be clarified that it pertains to active user accounts. The comments stated that there is no value to changing a password for an inactive or disabled user account until such time as the account is enabled. The commenter requested that the Requirement should also be clarified to require the initial

password change prior to placing the BES Cyber Asset into service. In response, the SDT disagrees. A known, published password should be changed even if the account is disabled. If the account is accidentally re-enabled, the password would be widely known. The SDT agrees that it would be a good practice to not only change the default password but also disable the default accounts if feasible, but it is not a Requirement.

There was a comment with regard to Requirement Part 5.4 that the word 'known' is ambiguous. For clarity, the commenter suggested changing the phrase "known default passwords" to "knowable default passwords". In response, the SDT disagrees that changing "known" to "knowable" solves the issue. The Requirement applies to the Responsible Entity, therefore it is "known to the Responsible Entity". Some vendors include "back door" user accounts in devices that are known only to the vendor and not the Responsible Entities. The Requirement is for the Responsible Entity to document only those that they know of.

A commenter suggested that Requirement Part 5.5's limitation to "password only" authentication is too narrow in scope and needs to include any use of a password for interactive access, even if part of a multi-factor authentication. The commenter also stated that this would need to include user accounts that are capable of being used interactively even if the intended use is only programmatic (e.g., an FTP account). Another comment to Requirement Part 5.5 was that the first paragraph uses the phrase "interactive user access" and that this is not a defined term. However, it is similar to the CIP Version 5 definitions defined term. The commenter questions whether the phrase "interactive user access" should be defined or clarified in the Guidelines and Technical Basis section. The SDT has added language clarifying "interactive user access" from the rationale for Requirement R5 to the Guidelines and Technical Basis section for Requirement Part 5.5.

One commenter recommended that the phrase "…at least once every 15 calendar months" be replaced with "at least once each calendar year." In response, and as described earlier, the SDT disagrees as it has standardized throughout the CIP standards that the original use of the word 'annual' be replaced with 'once every 15 calendar months.'

With regard to Requirement Part 5.7, one commenter requested a clarification to establish an upper bound (or maximum number of attempts) to generate an alert or initiate an account lockout. In response, the SDT disagrees that a prescriptive number of attempts is warranted. The entities will be in a better position to determine how many attempts in what time interval are needed for the particular situation. There may be widely varying circumstances to take into account such as is the login used by a process that is vital and will locking it out or slowing the interval between tries affect reliability.

CIP-008-5

General

One commenter stated that both CIP-008-5 and CIP-009-5 have plan update Requirements and should be considered for removal. In response, the SDT does not agree these should be removed in this version because we address multiple Directives in FERC Order No. 706 related to the update of plan documents.

Requirement R1

One commenter suggested adding "assess" to the required processes in Requirement Part 1.1. The SDT does not agree there is a need to include "assess" in the Requirement Part.

One commenter recommended increasing the one hour reporting threshold in Requirement Part 1.2. In response, the SDT uses this timeframe to respond to a directive in FERC Order No. 706, Paragraphs 673 and 676. The one hour also refers to the preliminary reporting required from the point at which the entity has determined an incident is a Reportable Cyber Security Incident.

Several commenters suggested that the obligation to report to the ES-ISAC in Requirement Part 1.2 may not be acceptable for some Canadians, but the SDT is unaware of any ES-ISAC reporting restrictions for Canadians. However, the SDT has clarified that such reporting to ES-ISAC is only required, unless prohibited by law, to account for scenarios where federal or provincial laws may prohibit such action.

Several commenters stated that notification of the ES-ISAC occurs only after a Cyber Security Incident is determined to be reportable and the one hour timeframe should start at the determination of the incident as being Reportable. The SDT has modified the Requirement to clarify the one hour timeframe is from determination rather than identification.

One commenter requested clarification on the term "preliminary notice." In response, we quote from the Technical Guidelines section of CIP-008-5, "This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report."

There was a comment that the one hour timestamp in Requirement Part 1.2 would require a paperwork intensive burden on the entity that may qualify for removal according to Paragraph 81 of FERC's Order on the Find, Fix, and Track process.

In response, while additional documentation may be necessary to demonstrate compliance with the timeline, the objective this Requirement goes beyond an administrative function.

One commenter suggested changing the one hour reporting threshold of Requirement Part 1.2 to 24 hours to align with EOP-004-2. In response, the one hour threshold is directed as a change in FERC Order No. 706;the SDTs for both CIP Version 5 and EOP-004-2 agrees this obligation was best left in the context of CIP-008-5.

One commenter stated that the roles and responsibilities of the incident response plans specified in Requirement Part 1.3 should be left to the Responsible Entity. They expressed concern for an auditor determining certain roles were left out of the plan. In response, the Requirement Part does not specify which roles must be in the plan, but having roles and responsibilities is a necessary part of an effective incident response plan.

Requirement R2

One comment read that Requirement R2 should have the language allowing an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R2 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One commenter proposed Requirement Part 2.1 needs clarification on whether a plan with multiple scenarios needs to have each scenario tested. In response, the SDT does not agree this clarification is necessary. It could be a benefit to consider multiple scenarios, and imposing a Requirement to test each would be a disincentive. Regardless, it is best left to the entity to determine how to test its plan.

There was a suggestion that the testing periodicity in Requirement Part 2.1 is inconsistent from the period used across other standards. The SDT agrees and has made this modification.

One commenter proposed adding wording to confirm a single incident response plan is sufficient for all High and Medium Impact BES Cyber Systems. In response, the Requirement Part does not preclude having a single plan, and the rationale in Requirement R1 suggests doing so.

One commenter suggested that documentation of a Reportable Cyber Security Incident suffers a “catch-22” in that one of the steps is a determination of whether or not an incident is Reportable. In response, the documentation of a Reportable

Cyber Security Incident can be performed after-the-fact. This is not a Requirement to document each step contemporaneously with each action.

One commenter recommended removing the documentation of deviations in Requirement Part 2.2 since it is mostly captured in the lessons learned. In response, the lessons learned activity likely will use documentation captured from the Cyber Security Incident, but there is no obligation to document the use of the plan. The SDT chose to use documentation of deviations because this is a much less documentation-centric activity than documenting how the plan was used.

Several commenters stated that Requirement Part 2.3 should be moved to data retention. In response, the retention of this information serves the purpose of supporting follow-up incident analysis and correlation activates. There is otherwise no obligation to retain this information.

Requirement R3

There was a comment that Requirement R3 should have the language allowing an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R3 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One commenter stated that CIP-008-5 Requirement R3 should allow deficiency correction. In response, the SDT does not agree this Requirement meets the criteria to be considered as high frequency, zero tolerance obligations as are the other Requirements that allow for deficiency correction.

There was a comment that in Requirement Part 3.1.2, lessons learned do not always trigger a plan update and that a qualifier “as applicable” should be added. The SDT agrees and has added the clarification, “lessons learned associated with the plan.” Corresponding changes have also been made in CIP-009-5.

There was a proposal that the timeframe in Requirement Part 3.2 could be extended to 90 calendar days consistent with 3.1. The SDT notes that Requirement Part 3.1 also includes the lessons learned obligation so the cumulative time to update should be longer.

One commenter proposed removing Requirement Part 3.2 or specifying only the affected roles and responsibilities. In response, the SDT notes that notification of all individuals is necessary for communication during a Cyber Security Incident.

One commenter stated for Requirement Parts 3.1 and 3.2, the wording needs to be rearranged to read better - the phrase 'no later than 90 calendar days after' should be added at the start of the sentence and deleted from the end. The SDT agrees and has made this change.

CIP-009-5

Requirement R1

One commenter stated that the roles and responsibilities of the recovery plans specified in Requirement Part 1.2 should be left to the Responsible Entity. They express concern for an auditor determining certain roles were left out of the plan. In response, the Requirement Part does not specify which roles must be in the plan, but having roles and responsibilities is a necessary part of an effective recovery plan.

There was a comment that Requirement Part 1.2 discusses responders without any additional clarification of who fits into this category. In response, this language has been carried forward from previous versions and the SDT has not received any additional comments supporting modification. The SDT agrees additional guidance would be helpful and has added clarification in the Technical Guidelines section of CIP-009-5.

There was one comment that stated that there should be more consistency in the applicability column of the tables and requests clarity on what applies if a Medium Impact BES Cyber System does not have a connectivity qualifier. In response, the lack of a qualifier only means that all Medium Impact BES Cyber Systems are applicable.

One commenter requested clarity on the intended frequency of performing Requirement Part 1.4. In response, the frequency is determined by the Responsible Entity. Some cyber systems may require a daily backup while other cyber systems, for example, at a power plant, may only require backups after major changes to the system.

One commenter suggested removing “and to address backup failures” from Requirement Part 1.4 because it may lead the reader to the notion of having another pre-determined plan to account for unknown issues during the backup. In response, the SDT notes that addressing backup failures meets the objective of the Requirement and purpose for verifying the successful completion of backups. Without this obligation, an entity could simply perform validation testing without performing any corrective action on the backup process.

Several commenters proposed changing Requirement Part 1.5 to “One or more processes, per device capability, to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), except where data preservation impedes or restricts recovery.” However, the rephrasing has a subtle change in meaning. The per device capability exception applies to the preservation of data and not the procedure itself.

One commenter stated that Requirement Part 1.5 can lead to delay in recovery operations, particularly in a Control Center. In response, the SDT notes the provision of the Requirement that data preservation should not impede recovery.

One commenter requested clarification of Requirement Part 1.5. They state that it would seem the activity would delay recovery. In response, planning to preserve evidence could include additional individuals assisting in the recovery or retaining failed Cyber Asset equipment during recovery operation.

One commenter suggested adding a CIP Exceptional Circumstance qualifier to Requirement Part 1.5. In response, the SDT removed this qualifier based on industry comments because an event triggering recovery could most likely be a CIP Exceptional Circumstance, and thus nullify the Requirement. However, Requirement Part 1.5 achieves the same objective in having a qualifier to avoid the disruption of restoration activities. The commenter also expressed concern about the intent of Requirement Part 1.5 and suggests moving this to CIP-008-5. In response, the objective is to have this performed in any recovery operation and not just Cyber Security Incidents.

There was a comment for Requirement Part 1.5 suggesting that the Requirements could put the registered entity into a "catch-22" scenario where it could try to comply with the Requirement by saving logs, which might impede recovery. In response, the plan should address the issue where saving information impedes recovery as indicated in the Requirement Part.

One commenter stated that in Requirement Part 1.5, the device capability should be worded to clearly qualify the preservation of data. The SDT agrees and has made this change. They also suggested the measure be updated to include the device capability qualifier. However, the qualifier itself only applies to the Requirement and does not need to have inclusion in the measure.

Requirement R2

There was one comment that the words 'between tests of the plan' are not needed. The SDT agrees and has made this clarification.

One commenter requested clarification on how an entity tests a representative sample of information if, per Requirement Part 2.1, they performed a paper drill. In response, the SDT notes that the test in Requirement Part 2.2 is not necessarily the same test performed in Requirement Part 2.1.

One commenter proposed Requirement Parts 2.1 and 2.3 need clarification on whether a plan with multiple scenarios needs to have each scenario tested. In response, the SDT does not agree this clarification is necessary. It could be a benefit to consider multiple scenarios, and imposing a Requirement to test each would be disincentive. Regardless, it is best left to the entity to determine how best to test their plan.

There was a request for clarification on the difference between 2.1 and 2.3 and for additional guidance on what types of operational exercise the SDT considers meeting the Requirement. In response, the SDT refers to the Technical Guidelines section of CIP-009-5, which states "The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, '[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims).'"

One commenter suggested that Requirement Part 2.2 needs to provide additional clarification for a "representative sample" of information used to recover BES Cyber System functionality. In response, the SDT does not think it provides a benefit to further specify a representative sample of information in this Requirement. Otherwise, this Requirement becomes focused on the sample of information rather than the recovery of information. As specified in the rationale, "Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information."

A clarification request was made on Requirement Part 2.2 regarding a representative sample. The representative sample must be determined by the Responsible Entity. It could be a test of all the most recent backup tapes or it could be a single representative test for multiple instances of the same system.

Requirement R3

There was a comment that this Requirement should include language that would allow an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R3 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One commenter suggested that a lessons learned activity should not be required for every failure of equipment in the field. In response, failure of equipment in the field does not indicate a recovery operation in all cases.

There was a proposal that the timeframe in Requirement Part 3.2 be extended to 90 calendar days consistent with 3.1. The SDT notes that Requirement Part 3.1 also includes the lessons learned obligation so the cumulative time to update should be longer.

There were several comments on parts 3.1 and 3.2 that the wording needed to be rearranged to read better - the words 'No later than 90 calendar days after' should be added at the start of the sentence and deleted from the end. The SDT agrees and has made this clarification.

Guidelines and Technical Basis

One entity commented that the guidelines state that recovery plan information is BES Cyber System Information, which is not consistent with the definition of BES Cyber System Information. The SDT agrees and has modified the guidance to state that recovery plan information may be considered BES Cyber System Information.

CIP-010-1

Timeframes for Configuration Control Activities

The SDT received comments that the timeframes for configuration control activities are inconsistent. The SDT believes that the timeframes specified are consistent and are reflective of a reasonable configuration change control process.

Cross References to CIP-005-5 and CIP-007-5 on Impacted Controls

Comments expressed concern over the cross-reference to CIP-005-5 and CIP-007-5 as it related to the controls that could potentially be impacted by a change. The commenter recommended that the Requirement be broadened to include any control rather than simply those included in CIP-005-5 and CIP-007-5. The SDT appreciates the concern expressed in this comment and wrestled with this issue itself. After changes to this issue during multiple rounds of industry comment, the SDT believes that bounding the controls that need to be assessed is the most auditable approach.

The SDT received comments regarding a concern over double jeopardy between CIP-005-5, CIP-007-5, and CIP-010-1, specifically as it relates to the documentation of logical network accessible ports. The SDT does not believe this is a double jeopardy situation. CIP-005-5 and CIP-007-5 specify how ports are to be configured whereas CIP-010-1 specifies that they be documented.

Requirement R1

The SDT received numerous comments to add the “external routable connectivity” qualifier to the applicability section in Requirement R1. The SDT appreciates the concern regarding the amount of effort involved in maintaining baseline documentation for disconnected Cyber Assets. However, since these devices are disconnected, the point in time at which the device is interacted with is the only time that the configuration may actually be validated. Given this, the SDT believes it is worthwhile to formalize the configuration change management process for these systems such that an understanding of the current configuration of the device is assured at all times.

One commenter identified confusion as it relates to comma usage in CIP-010-1 Requirement Part 1.5.1. The SDT has clarified the Requirement and removed the incorrect comma.

One commenter asked for clarification that the items in the baseline are “current” and not historical. The SDT confirms that it expects that the baseline is a current representation of the configuration and that this should be kept up to date by Requirement Part 1.3.

One comment from industry asked for clarification as it relates to Requirement Part 1.4.2 and whether this verification that security controls are in place was to be performed on the production system itself. The SDT clarifies that this is the case. The intent of the Requirement is to ensure that the production system is properly protected following a change that affected its baseline configuration.

Several commenters asked for clarification on the use of TFEs in Requirement Part 1.5 (testing of changes) and whether the SDT actually meant CIP Exceptional Circumstances. The SDT envisioned that operational issues may prevent the ability to test a change prior to its implementation. The SDT believes that the TFE process provides the protection necessary to ensure that violations are not issued for a wide range of circumstances, including but not limited to those operational issues contemplated in the CIP Exceptional Circumstances definition.

Requirement R2

Comments expressed that the IAC language should be removed from CIP-010-5 Requirement Part 2.1 because this Requirement was itself an internal control. The SDT agrees that the Requirement represents a control; however it believes that, particularly given the required periodicity, that there could be deficiencies identified in the control itself and it therefore warranted the IAC language.

Requirement R3

One commenter recommended that the language in Requirement Part 3.3 be modified to add the word applicable ("Prior to adding a new applicable Cyber Asset...") in order to clarify that this Requirement did not apply to those systems that are temporarily connected for less than 30 days. The SDT agrees that this is consistent with the intent of the language and has modified the language accordingly.

The SDT received concerns regarding the performance of active vulnerability assessment prior to the deployment of new BES Cyber Assets. The SDT agrees that these assessments may be imperfect and that there may be some applications that will not properly function outside of a full production environment. However, the SDT continues to believe that since this is the only time when active scans may be safely performed on future production equipment that it is in the best interest of the BES for an active vulnerability assessment to be performed.

The SDT received comments preferring additional specificity as to what to validate during a vulnerability assessment. The SDT appreciates these concerns, but believes that a vulnerability assessment for an EMS system may look substantially

different from an assessment of a PLC. The SDT believes that the best approach is to allow the entity to define an appropriate assessment methodology for their environment, which may then be evaluated by an auditor.

The SDT received comments that questioned the technical feasibility of monitoring for changes to the baseline configuration. The SDT originally had intended for this monitoring to occur on a more frequent basis, potentially real-time monitoring. However, it was persuaded that there are some systems for which real-time monitoring would be infeasible. The SDT does believe that given the relatively high level items included in the baseline, that periodic monitoring every 35 days is a reasonable method to ensure that changes are not taking place outside of an entity's change control program.

Numerous commenters expressed concern about the Requirement to document the differences between the test and production environments. The SDT reminds the industry that this Requirement was the result of a FERC directive. Additionally, the SDT reminds the industry that it believes that for a relatively stable testing environment, that this documentation could be done once and utilized for multiple changes or testing cycles.

Commenters asked questions about the multiple timeframes for the vulnerability assessments for high impact BES Cyber Systems. The SDT confirms that these time frames are intended. Effectively, this requires an annual paper or active vulnerability assessment, but an active vulnerability assessment must be performed at least every three years. The SDT believes that the confusion raised by the question is due to the reader not considering the entire table as itself a single Requirement.

One commenter expressed confusion on the applicability of CIP-010-1 to access points. The SDT clarifies that since access points are the point at which access is controlled, they are included in the definition of EACMS and as such are applicable to CIP-010-1.

One commenter asked for clarification that the test environment did not have to be an exact mirror of the production environment. The SDT confirms that this was the intent of using the phrase "models the baseline configuration."

CIP-011-1

Requirement R1

Commenters requested that Requirement Parts 1.1 and 1.2 of CIP-011-1 Requirement R1 be clarified to indicate that a single method or procedure was sufficient. The SDT agrees that this is the intent and has clarified the standard as requested.

Commenters suggested that CIP-011-1 Requirement Part 1.2 should contain a measure that indicates "repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program." The SDT does not see how a repository is evidence of a procedure to protect and securely handle BES Cyber System Information. The SDT agrees that an information repository may be used effectively to meet this Requirement, but it is only a component of the evidence based upon a particular manner of implementation.

Requirement R2

One commenter requested that Requirement R2 of CIP-011-1 be moved to CIP-010-1 as it could be considered part of a change control process. The SDT believes that the objective of this Requirement is the protection of the information in a BES Cyber System and therefore believes it is appropriate to include in CIP-011-1.

Commenters identified a typographical error in the measure of Requirement Part 2.2. The SDT appreciates this correction and has updated the standard.

Implementation Plan

Effective Date

Several commenters had questions or concerns about the Version 3 to Version 4 to Version 5 transition within the standards' implementation plan. Some questioned whether extending Version 3 to the effective date of Version 5, and superseding Version 4, is still possible, while others asked for a deadline for accomplishing such a transition plan. The SDT appreciates these concerns, as they are issues of efficiency, planning, effort, and cost for all of the industry. However, the SDT also acknowledges that not all entities are situated exactly the same. As such, the SDT is hesitant to provide a "deadline" or other trigger for FERC action that would serve to foreclose the opportunity for the implementation language to be adopted in time to implement moving directly from Version 3 to Version 5. The SDT expects that the filing will address this issue in a manner such that certainty about the issue may come as soon as possible, and that the filing and other coordination between NERC and FERC is the appropriate venue for supporting the implementation plan after industry approval. In the meantime, it is reasonable to expect that some entities may need to make a risk-informed judgment to proceed with Version 4 implementation by a certain date if the proposal in the implementation plan is not approved expediently. Some entities may be able to wait longer than others into 2013 before making that determination. The SDT has communicated directly with NERC to underscore the importance of coordination of this effort, and the SDT believes that having an approved set of standards, definitions, and implementation plan before the end of 2012 continues to provide a reasonable timeline to consider the implementation plan proposal.

There was one comment that 36 months to comply with CIP-003-5 Requirement R2 is excessively long since it only requires documentation of a few policies. The SDT notes that CIP-003-5 Requirement R2 requires implementation, and not just documentation of policies. This expands to a significantly large number of the overall reported BES Cyber Systems, which warrants such a timeline.

One commenter suggested that it misleads entities to allow the provision suspending compliance with Version 4. The SDT does not agree this is misleading. The SDT has been careful to communicate the risk in awaiting this order to begin planning compliance with Version 4. Furthermore, the FERC approving this provision, even if it is closer to the Version 4 Effective Date, still spares entities and auditors alike untold expenses of a compliance monitoring program for Version 4.

A few commenters asked about audits in 2015 during the expected transition window to Version 5's effective date. That is outside the scope of the SDT, but the SDT has tried to account for a smooth transition within the implementation plan,

to include specifications for initial required performances of periodic events. In response to this question and the issue of transition from Version 3 to Version 5, the SDT understands that NERC is preparing information to assist in the smooth transition among CIP standards versions, and that such information will be coordinated upon certainty that Version 5 has been approved by the industry and is no longer subject to change.

One commenter stated that the effective date language should be qualified with a statement that sufficient time should be given for completion of CIP-002-5 R2 to comply with CIP-003 through CIP-011. The SDT believes this is already well understood and ongoing communication and training will provide entities further guidance to categorize BES Cyber Systems with sufficient time to comply with CIP-003 through CIP-011.

Several entities comment that NERC and the drafting team should request FERC to suspend compliance with Version 4 and allow entities to transition from Version 3 to Version 5 on the effective date. In response, the proposed effective date does bypass Version 4 and provides the FERC the opportunity to issue an order approving this provision. In effect, this is the industry and SDT communication to the FERC requesting the bypass of Version 4.

There was a comment that suggested extending Version 3 until Version 5 becomes effective could not be accomplished in Canada through an implementation plan. In response, the SDT notes that Canadian jurisdictions would be subject to the second provision for "those jurisdictions where no regulatory approval is required." The commenter is correct that the proposal in the Implementation Plan, if approved, would supersede any other Order to the contrary. In all cases of reliability standards, the Implementation Plan is subject to regulatory or other applicable federal approval.

A few commenters noted that CIP-003-5 is dependent upon CIP-004-5 through CIP-009-5, CIP-010-1, and CIP-011-1 passing. The SDT confirms the commenters' understanding and notes that the implementation plan conditions all standards passing before any of them become effective.

One commenter expressed concern that the implementation of CIP-004 through CIP-011 should be combined into those standards. The SDT points out that the implementation of security procedures in CIP-004 through CIP-011 is included in those Requirements that have actions associated with them. The entity should refer to the high level Requirement for the implementation language.

Initial Performance of Certain Periodic Requirements

Several commenters stated some confusion with the initial performance of periodic Requirements section or suggested that it is unnecessary and, if retained, should be in guidance. The SDT notes this section was incorporated from industry comments, and moving this section to guidance would be misleading because the additional time for compliance with periodic Requirements would not be enforceable in guidance.

There was a comment that no provision for CIP Exceptional Circumstances exists for some periodic Requirements and that an entity should be allowed to track instances of non-compliance in CIP Exceptional Circumstances rather than self-report. In response, the SDT has indicated where exceptions may occur to the standards in defined CIP Exceptional Circumstances. Most of the periodic Requirements should have enough lag time built in to avoid the need for self-reporting in emergency situations. Otherwise, it is not envisioned all compliance activities should cease in a CIP Exceptional Circumstance, but only the ones indicated in the Requirements.

One commenter proposed revisions to the following initial periodic Requirements, and the SDT responds in order:

- CIP-004-5 Requirement Parts 4.2 through 4.4 should be required on or before the effective date to preclude record-keeping errors. The SDT notes that record-keeping errors, while not the most efficient, are not violations of the standard.
- CIP-006-5 Requirement Part 3.2 should tie to the previous testing interval and allow 24 months for the newly in-scope Cyber Assets. In response, tying the interval to previously in-scope Critical Cyber Assets would cause more confusion than is necessary for this Requirement, and the SDT believes the 12 calendar months are appropriate timeframes for testing PACS.
- CIP-008-5 Requirement Part 3.1 and CIP-009-5 Requirement Part 3.1 should not be included in the initial performance of periodic requirements section since they are not periodic, but are performed in response to a test. The SDT agrees.
- CIP-010-1 Requirement Parts 3.1 and 3.2 should not be included because it would be similar to part 3.3 in adding a new Cyber Asset to the BES Cyber System. In response, the SDT retains the additional timeframe because strict compliance would suggest this periodic timeframe be performed immediately on the effective dates for all BES Cyber Systems in scope, which would be infeasible for most all entities.
- CIP-009-5 Requirement Part 2.3 is included in both groups 6 and 7. The SDT notes this is not the case.

- Group 8 of the periodic Requirements dealing with the continued effectiveness of previous personnel risk assessments is already incorporated in the Requirement language. In response, strict compliance with the Requirement would otherwise suggest immediate compliance with this Requirement on the effective date.

One commenter suggested that NERC imposing Requirements before the effective date goes beyond NERC's legal authority. In response, the implementation plan does not modify the effective date of any Requirement but makes clear when the initial performance must occur for certain Requirements. By stating a Requirement can be performed prior to the effective date does not impose a different effective date. Rather, this clarifies that on the effective date, the entity has complied with the Requirement by performance of a past activity.

There was an observation that CIP-006-5 Requirement Part 3.1 and the Requirements specified in section 7 have periodicities longer than the initial performance. This is correct and intended by the SDT because even though the periodicity is longer, the benefit achieved by the initial performance puts it closer to the effective date.

Previous Identity Verification

One commenter noted an incorrect reference to CIP-004-5 Requirement Part 4.1, and the SDT expresses their gratitude for uncovering this error.

Planned or Unplanned Changes Resulting in a Higher Categorization

Several commenters suggested that the distinction between planned and unplanned changes is not clear and the timeframe for planned changes should be extended to 18-24 months. In response, the SDT carries forward this language that has been in effect since Version 2. The 12 months is also carried forward as the time entities with existing CCAs have to implement CIP Requirements on new CCAs. The SDT does not consider this 12 month timeframe unreasonable and notes in the example given that updates to a generation facility would be considered a planned change and compliance would be part of the maintenance performed during the outage.

One commenter stated that the addition of time for initial performance of periodic Requirements muddles the timeline for compliance. In response, the implementation plan would not preclude an entity from complying earlier to benefit the entity with a consistent compliance schedule, but without this provision, the periodic Requirements would need to be performed prior to the 12 month period, and this is neither reasonable nor appropriate. This language was added since the last posting in response to multiple entities' request.

There was a comment that suggested the last scenario in unplanned changes be clarified as the first high or medium impact BES Cyber System overall rather than at a facility. The SDT has made this clarification by providing a clarifying parenthetical phrase to row five of the "Scenario of Unplanned Changes After the Effective Date" table that underscores the meaning of that row in relation to and in context with rows one through four.

There was a request for clarification on the use of Effective Date in the table heading "Scenario of Unplanned Changes After the Effective Date". In response, the SDT notes that this is the effective date specified in each standard for Version 5 of the CIP Cyber Security Standards.

Applicability Reference Tables

One commenter proposed revisions to the Requirement applicability, and the SDT responds in order:

- CIP-004-5 Requirements R4 and R5 should apply to Protected Cyber Assets. In response, we have addressed most of the risk by authorizing and revoking access associated with the BES Cyber System. We carry forward the precedent of applicability in this case from previous standards, and do not find a justification for adding them to the applicability of these Requirement Parts.
- CIP-005-5 Requirement R1 should apply to PACS as it does in the current standard.
- CIP-005-5 R1 should apply to PACS as it does in the current standard. In previous versions, CIP-005 R2 applied but not R1. The SDT received significant industry feedback that this applicability was confusing and resulted in multiple interpretations. The SDT addresses access control at the device level in CIP-007-5 and avoids the confusion around the disconnect between applicability in CIP-005-4 R1 and R2, and for this reason, CIP-005-5, Requirement R1 does not apply to PACS.

There was a comment that CIP-005-5 Requirement R2 should apply to EACMS. In response, the EACMS are referenced as part of the Requirement. The confusion of recursive Requirements is not worth the reliability and security benefit gained by their inclusion.

Definitions

BES Cyber Asset

One entity commented that the definition should reference "the items in Attachment 1" instead of "Facilities, systems, or equipment," because "Facilities, systems, or equipment" is subjective and lends itself to differing interpretations, and Attachment 1 provides greater clarity and guidance on the criteria to define BES Cyber Assets. The SDT points out that a definition is used in a standard and cannot reference a part of the standard. The term "Facilities, systems or equipment" has been used as part of the definition of Critical Assets for Versions 1, 2, 3 and 4.

BES Cyber System

One commenter wrote that the definition uses the word logically that may be mistakenly interpreted to mean networked instead of validly grouped. The SDT believes that the rest of the definition of the BES Cyber System in relation to the performance of reliability functions provides clarity to the meaning used here.

BES Cyber System Information Responses

The SDT received a concern regarding the phrase "not publicly available" in that if BES Cyber System Information was made public, it would then be outside the scope of the standard. The SDT appreciates this concern; however, it believes that the meaning is ultimately clear as to the intent.

CIP Exceptional Circumstance Responses

The SDT received a request to clarify the punctuation in the definition of CIP Exceptional Circumstances. The SDT has updated the punctuation as requested.

One commenter expressed concern about the ability to declare a CIP Exceptional Circumstance for hardware, software or equipment failure. The concern of the commenter was that this could open the door to bypassing Requirements for minor issues. The SDT did not envision this as a free for all and believes that the obligation to have policy around the declaration and response to CIP Exceptional Circumstances should minimize any abuse of this definition.

CIP Senior Manager Responses

One commenter requested that the SDT address the accepted interpretation request in RFI Project 2012-INT-06. While the SDT has an obligation to incorporate existing interpretations, the response to the interpretation that was highlighted has not been posted and therefore the SDT would risk contradicting a pending standards interpretation action.

Additionally, since that interpretation has not been approved by industry, there is no way for the SDT to determine whether it reflects a level of consensus of the industry. As such, the SDT believes that this would be too large of a change to incorporate at this point in the development process.

Control Center

Many entities requested clarification on the term “associated data centers” in the definition of Control Centers and asked whether these are the "data centers" that service/support a control center”. Comments were also made that “data center” is not a defined term. The SDT believes that the term “data center” is a commonly understood term of practice and that a specific glossary definition is not required. The intent of including “associated data centers” in the definition of Control Centers is to include only those systems that are associated with the Control Center Cyber Assets and directly support the functions of the functional entities defined. These will be the BES Cyber Systems that directly provide monitoring and control functions for the Control Center operators’ use in the performance of their real-time functions, and to ensure that this does not include certain types of field data aggregating or processing assets that are associated with field transmission or generation assets. Control Center data centers do not necessarily reside in the same facility where operators are hosted, but may extend the Control Center to include facilities hosting these cyber systems outside of the facility hosting the Control Center operators.

One entity requested clarification on the meaning of “location” in the definition. The NERC Guideline for Critical Asset identification has an extensive discussion of control rooms and Control Centers. In general, a location is delineated by a physical boundary that hosts a set of BES Facilities.

One entity suggested the addition of “CIP” to the term or some indication that this is only a definition used in the CIP context. The SDT is proposing the term to be included in the NERC Glossary. The convention is that when the term is used in its capitalized form (initial letter of each word), then it is used as the NERC Glossary defined meaning of the term. Otherwise, it is used in the undefined, generic meaning. This does not have any effect on other standards that do not use the term in its capitalized form. Other standards which wish to use the NERC Glossary term as defined (or wish to amend it through the development process) can use the capitalized form.

Cyber Asset

One entity commented that the inclusion of “hardware, software and data” in the definition of Cyber Asset was redundant and proposed a simplified definition of “Entity programmable electronic devices”. The SDT’s approach to existing definitions is to make only the modifications necessary for additional clarity or intent. This definition is based on

the previous definition of Cyber Asset. The SDT believes that removing the terms “hardware, software and data” would not provide additional clarity and that the addition of “Entity” in the qualification of “programmable” would inappropriately limit the general scope of the definition of cyber asset. The protection Requirements in the standards include those necessary to ensure that proper processes are included for protection from inappropriate modification or misuse of programs not directly modified by the entity.

Another entity commented that the proposed definition could be interpreted to require utilities to demonstrate consideration of - in addition to hardware - all software and data on each programmable electronic device, which would be impracticable and overly burdensome. The entity recommends changing the definition to “Programmable electronic device.” The SDT points out that the inclusion of these qualifications has been part of the definition of cyber assets since Versions 1, 2, 3 and 4 and that the modifications to the previous definition ensures that the definition includes the data when it is on these devices.

One entity commented that the inclusion in voice communication for a Control Center operator to implement operating actions in the execution of a Control Center functional obligation would include many smaller entities as Control Centers. The determination of whether a facility is considered a Control Center is dependent on whether it meets the definition, not on size or on how it performs its functional obligations. The manner in which it implements its functional obligations will determine what are qualified BES Cyber Assets. For example, in the environment that the commenter describes, there may be many BES Cyber Assets that provide monitoring and alarming information on which the operator will initiate a real-time operation for the BES. The impact of such monitoring and alarming systems on the real-time operation of the BES warrants the protection commensurate with its function.

Cyber Security Incident

One commenter suggested modifying the definition of Cyber Security Incident to eliminate attempts of compromise or disruption because such a definition is broad enough to include any erroneous traffic. The SDT disagrees. Attempts of compromise imply intent far beyond erroneous traffic and should be analyzed and recorded as part of the CIP-008-5 incident response plan.

There was a comment that the definition of Cyber Security Incident should also apply to PCAs, EACMS and PACS. In response, the definition has no applicability, and an incident occurring on PCAs, EACMS and PACS already meets the definition of having the potential to impact the BES Cyber System.

There was a comment suggesting that it is difficult to determine the intent of an attacker, and the commenter further suggested that "suspicious" is vague. In response, the SDT intends that such determination is best left to the entity. Without the qualifiers of suspicious and malicious, it could be interpreted that many nominal events would be considered Cyber Security Incidents.

Electronic Access Control and Monitoring System

One commenter stated that the definition of EACMS is inconsistent with the definition used in the background section of Version 5 CIP Standards. In response, the guidance provided in the background section is not a definition. It only provides example EACMS for the purpose of adding context for the reader.

Intermediate Device (now "Intermediate System")

A recommendation was made that the definition of Intermediate Device be modified to remove the phrase "or collection of Cyber Assets", as they consider this limiting the scope. The SDT used "A Cyber Asset or collection of Cyber Assets" to allow for flexibility so that an entity could use one or more devices to perform the noted functional Requirements. The scope of the definition and Requirements is limited to only Interactive Remote Access to BES Cyber Systems. Further, it was noted in prior comments that entities may not be able to implement a single device that provides encryption and multifactor authentication. As a result of comments, the definition has been modified to "Intermediate System" to better align with the asset and system concepts used throughout the Version 5 standards.

One commenter requested clarification on the definition of Intermediate Device. The SDT has worked the definition to allow for flexibility in the selection and implementation of technology to meet their needs. The definition does not prevent an entity from having an Intermediate Device within an ESP, just not the ESP containing the BES Cyber Systems being remotely accessed. The definition term (not the definition's meaning) has also been modified to "Intermediate System" to better align with the asset and system concepts used throughout the Version 5 standards. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested more clarity regarding the types of devices that would qualify as intermediate devices, beyond the Requirements that they must support encryption for any interactive sessions and multifactor-authentication for access to any interactive sessions. Additional references are available in the *Guidance for Secure Interactive Remote*

Access document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

Interactive Remote Access

One commenter suggested that, as written, the definition appears to require that entities declare each of their internal networks as an ESP, including their corporate networks. The commenter discussed that many entities monitor their corporate network in much the same manner as their ESPs, and that requiring encryption within their corporate networks would introduce an unacceptable security risk by rendering their monitoring capabilities ineffective. The commenter requested appropriate clarifications or that the definition be modified to specify that Interactive Remote Access and the associated technical controls be required when traffic is traversing an untrusted or public network only. In response, the SDT notes that it is not necessary to declare the encryption termination point as a part of the ESP. It is allowable to have the termination point reside outside of the ESP, such as a corporate firewall to allow for corporate boundary systems to monitor network traffic as described. In this scenario, the corporate firewall would be considered and protected as an EACMS but still not considered to define an ESP.

There was a recommendation to remove the second sentence of the Interactive Remote Access definition. The SDT added this language to address comments and concerns raised during this project and Project 2010-15: Expedited Revisions to CIP-005-3.

One comment suggested that the definition of Interactive Remote Access be modified to remove the sentence, "Remote access can be initiated from: ... contractors and consultants." The SDT added this language to address comments and concerns raised during this project and Project 2010-15: Expedited Revisions to CIP-005-3.

There was one request that the definition be modified as “access is likely initiated…” The SDT used “may be initiated” to allow for flexibility rather than using words such as “shall be initiated” or “will be initiated” which are far more restrictive and align to the concern noted.

There was a suggestion that the definition of Interactive Remote Access be modified to remove Requirement language within the definition. The SDT considers all parts of the definition to be clarification of what is and is not Interactive Remote Access. The Requirements are the technical controls to be implemented.

Reportable Cyber Security Incident

There was a comment suggesting that the definition of Reportable Cyber Security Incident is too broad and should specifically state that a malware infection of an in-scope Cyber Asset should be reported. In response, the SDT provides additional guidance in the context of CIP-008-5 that would generally ensure the proper reporting of a malware infection. However, a malware infection itself would cause additional uncertainty in the definition. Moreover, entities would be left to wonder if a contained malware infection was reportable or not. For these reasons, the SDT does not agree with the recommendation to further specify Reportable Cyber Security Incident.

One commenter said that this definition should be removed and addressed solely within the standard. In response, the SDT believes there is sufficient consensus for the definition and moving this term to a local definition in CIP-008-5 would be a significant change and potentially cause uncertainty in the enforceability of this definition.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.

Anticipated Actions	Anticipated Date
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-002-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required CIP-002-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-5

3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-5:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Background:

This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.

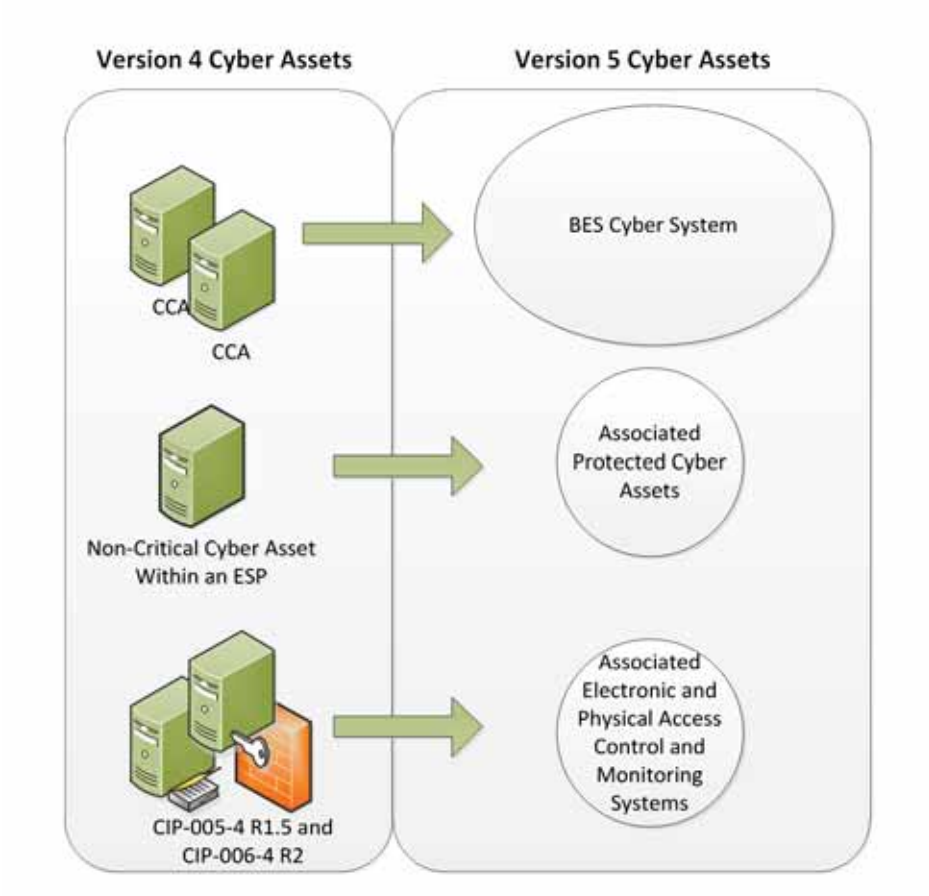

In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and

scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS") – Examples include: Electronic Access Points, Intermediate Devices, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")– Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA") – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

Rationale – R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** Special Protection Systems that support the reliable operation of the Bulk Electric System; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

Rationale – R2

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

R2. The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5 - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)

- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some

of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, BAs, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of BAs with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1. .

- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the

backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

  - 230 kV –> 700 MVA
  - 345 kV –> 1,300 MVA
  - 500 kV –> 2,000 MVA
  - 765 kV –> 3,000 MVA

  In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

  - For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities

would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.
- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as

specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.

- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric

System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to

restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.

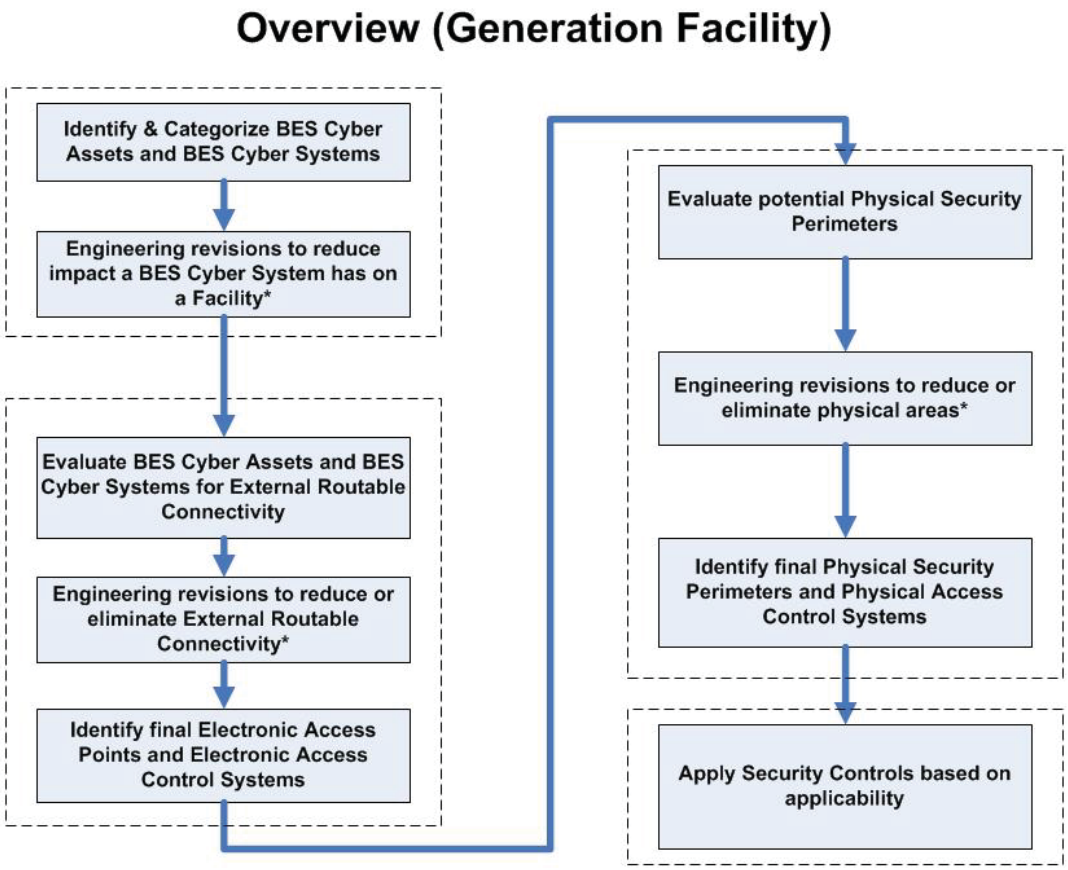

* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

~~**Note**: On September 21, 2012, this draft was revised to clarify references from "generator interface facility" to "generator interconnection Facility" in Attachment 1, criteria 2.4, 2.5, and 2.8. As noted on page 33 of the consideration of comments, form A, the SDT intended to use "generator interconnection Facility." It also corrects instances of incorrect functional model references from "Generation Operator" to "Generator Operator" and corrects the numbering format in Attachment 1, section 3.~~

~~No other changes were made to this standard or any of the other CIP V5 standards currently posted, except for a conforming change from "Generation Operator" to "Generator Operator" in the definitions document.~~

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. ~~4.~~ Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the ~~third~~ fourth posting of Version 5 of the CIP Cyber Security Standards for a ~~30~~10-day ~~formal comment period~~recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for ~~formal comment and parallel successive~~ recirculation ballot addresses the comments received from the ~~second~~ third posting and ballot.

Anticipated Actions	Anticipated Date
~~30-day Formal Comment Period with Parallel Successive Ballot~~	~~September 2012~~
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-002-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required CIP-002-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-5

3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-002-5:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Background:

This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.

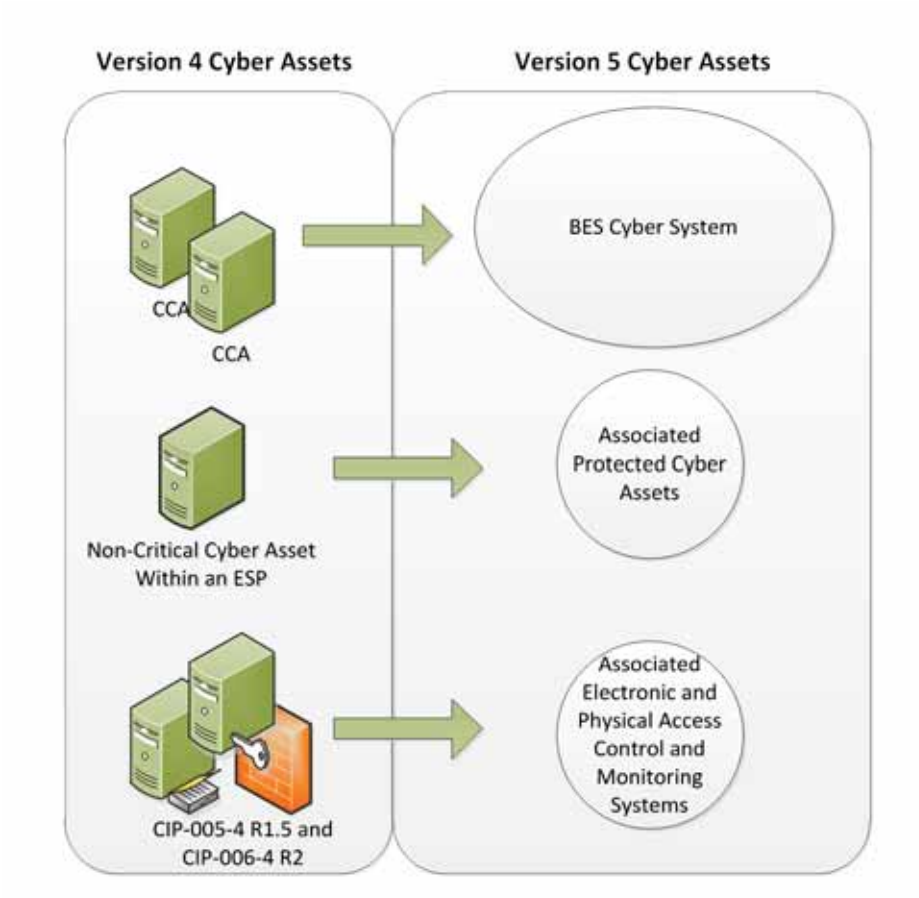

In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets-, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and

scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS") – Examples include: Electronic Access Points, Intermediate Devices, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")– Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA") – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

Rationale – R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts ~~R~~1.1 through ~~R~~1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

~~**1.**~~**i.** Control Centers and backup Control Centers;

~~**2.**~~**ii.** Transmission stations and substations~~ and stations~~;

~~**3.**~~**iii.** Generation resources;

~~**4.**~~**iv.** Systems and facilities critical to system restoration, including Blackstart Resources~~blackstart generators~~ and ~~substations in the electrical path of transmission lines used for initial system restoration~~Cranking Paths and initial switching requirements;

~~**5.**~~**v.** Special Protection Systems that support the reliable operation of the Bulk Electric System; and

~~**6.**~~**vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required). [11]

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts ~~R~~1.1 and ~~R~~1.2.

Rationale – R2

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

R2. The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

~~R~~2.1 Review ~~(and update as needed)~~ the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

~~R~~2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5 - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation ~~that~~ is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value~~s~~" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations~~ and stations~~.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources~~blackstart generators~~ and ~~substations in the electrical path of transmission lines used for initial system restoration~~Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)

- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of~~that~~ the BES assets supported by~~that~~ these BES Cyber Systems ~~support, on the reliable operation of the BES~~.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5, these groups of Facilities, systems, and equipment are sometimes designated as BES a~~A~~ssets. For example, an identified BES a~~A~~sset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some

of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, BAs, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of BAs with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. ~~which coordinates~~ A~~a~~ctions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are~~,~~ usually formalized in the form of an ~~formal~~ agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1. ~~The value of 300 MW is the same value used for UFLS and UVLS~~.

- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the

backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

  - 230 kV –> 700 MVA
  - 345 kV –> 1,300 MVA
  - 500 kV –> 2,000 MVA
  - 765 kV –> 3,000 MVA

  In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

  - For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities

would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.

- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

- The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as

specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.

- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric

System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to

restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.

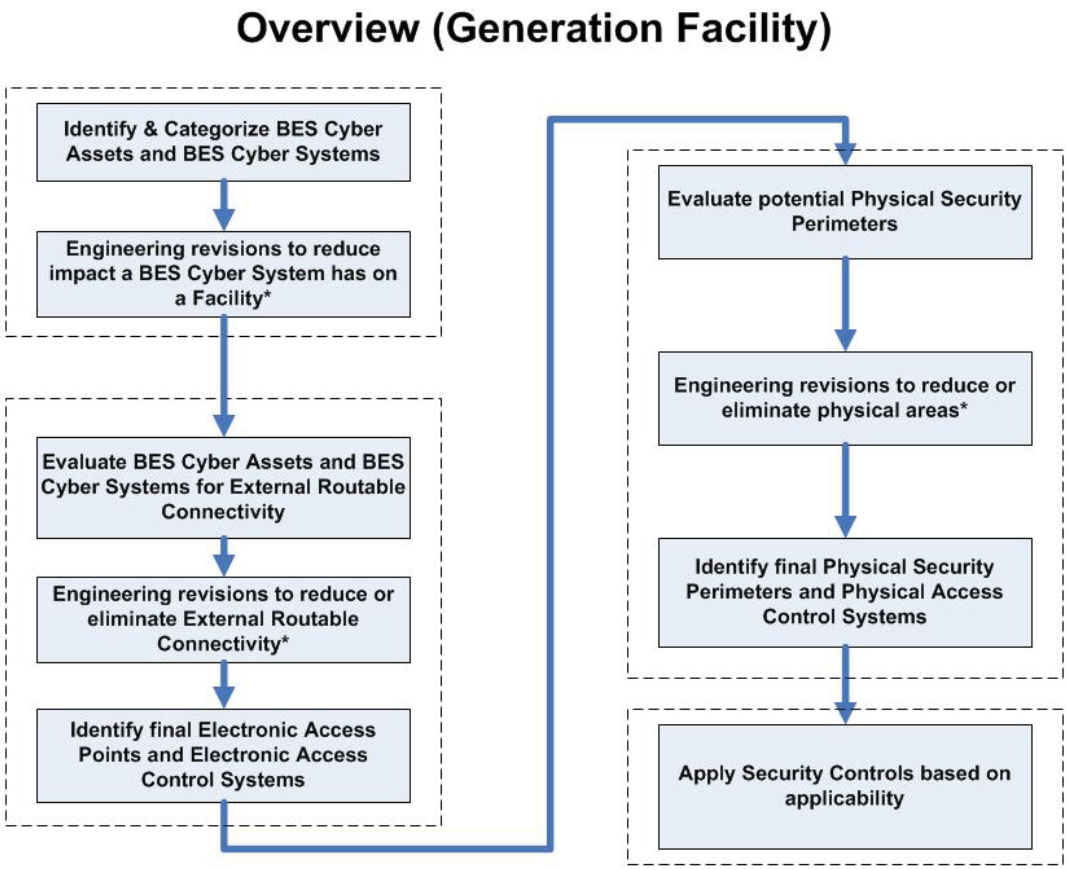

* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.

Anticipated Actions	Anticipated Date
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-003-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale – R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale – R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

Review and approval of the cyber security policy at least every 15 calendar months ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- **2.1** Cyber security awareness;
- **2.2** Physical security controls;
- **2.3** Electronic access controls for external routable protocol connections and Dial-up Connectivity; and
- **2.4** Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale – R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale – R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-5, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not

necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-5, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-5, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

~~**Note**: On September 14, 2012, NERC was alerted that the reference to CIP-002-5 in Requirement R2 of CIP-003-5 was incorrect.~~

~~This revised draft corrects the reference from "CIP-002-5, Requirement R2, Part R1.3" to "CIP-002-5, Requirement R1, Part R1.3." It is clear by the reference's context that it should be Requirement R1.~~

~~No other changes were made to this standard or any of the other CIP V5 standards currently posted.~~

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. ~~4.~~ Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the ~~third~~ fourth posting of Version 5 of the CIP Cyber Security Standards for a ~~30~~10-day ~~formal comment period~~recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for ~~formal comment and parallel successive~~ recirculation ballot addresses the comments received from the ~~second~~ third posting and ballot.

Anticipated Actions	Anticipated Date
~~30-day Formal Comment Period with Parallel Successive Ballot~~	~~September 2012~~
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-003-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale – R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale – R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

Review and approval of the cyber security policy at least every 15 calendar months ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics,- and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Cyber security awareness;

2.2 Physical security controls;

2.3 Electronic access controls for external routable protocol connections and Dial-up Connectivity; and

2.4 Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale – R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale – R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of ~~the initial delegation and~~ any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-5, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not

necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-5, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-5, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.

Anticipated Actions	Anticipated Date
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-004-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-004-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-5

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-5:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

Requirements and Measures

Rationale for R1: Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).
Reference to prior version: *CIP-004-4, R1*		**Change Rationale:** *Changed to remove the need to ensure or prove everyone with authorized* electronic or authorized unescorted physical *access "received" ongoing reinforcement – to state that security awareness has been reinforced.* *Moved example mechanisms to guidance.*	

Rationale for R2: To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:
   - The visitor control program
   - Electronic interconnectivity supporting the operation and control of BES Cyber Systems
   - Storage media as part of the handling of BES Cyber Systems information
2. Change references from Critical Cyber Assets to BES Cyber Systems.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
Reference to prior version: *CIP004-4, R2.2.1*		**Change Rationale:** *Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
Reference to prior version: *CIP004-4, R2.1*		**Change Rationale:** *Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.*	
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.
Reference to prior version: *CIP004-4, R2.3*		**Change Rationale:** *Updated to replace "annually" with "once every 15 calendar months."*	

Rationale for R3: To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Addressed interpretation request in guidance. Specified that process for identity confirmation is required. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.*	

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.*	

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
Reference to prior version: *NEW*		Change Rationale: *There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.*	
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.
Reference to prior version: *CIP-004-4, R3.3*		Change Rationale: *Separated into its own table item.*	

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.
Reference to prior version: *CIP-004-3, R3, R3.3*		**Change Rationale**: *Whether for initial access or maintaining access, establishes that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment.*	

Rationale for R4: To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.
Reference to prior version: *CIP 003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1*		**Change Rationale:** Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
Reference to prior version: *CIP 004-4, R4.1*		**Change Rationale:** *Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.*	

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.
Reference to prior version: *CIP 007-4, R5.1.3*		**Change Rationale:** *Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary.*	

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.
Reference to prior version: *CIP-003-4, R5.1.2*		**Change Rationale:** *Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.*	

Rationale for R5: The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate."

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R5 – Access Revocation*. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
Reference to prior version: *CIP 004-4, R4.2*		**Change Rationale:** *The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards* ***to require immediate revocation*** *for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*	

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
Reference to prior version: *CIP-004-4, R4.2*		**Change Rationale:** *FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.*	

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.
Reference to prior version: *NEW*		**Change Rationale:** *FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.*	

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
Reference to prior version: *NEW*		**Change Rationale:** *FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.*	

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.
Reference to prior version: *CIP-007-4, R5.2.3*		**Change Rationale:** *To provide clarification of expected actions in managing the passwords.*	

Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Regional Variances

None.

Interpretations

None.

Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1: The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

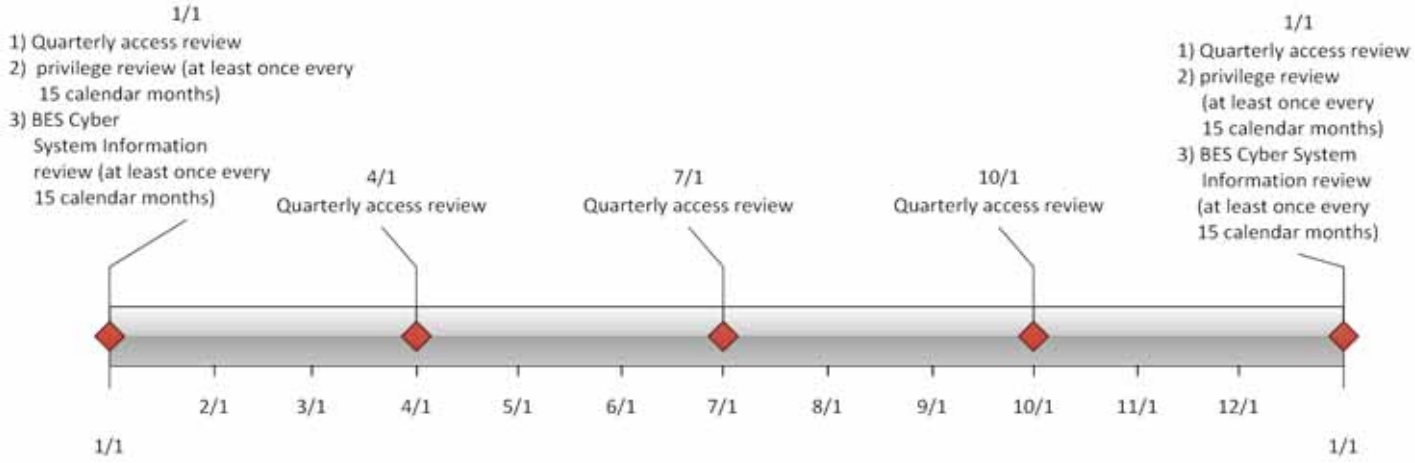

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the third fourth posting of Version 5 of the CIP Cyber Security Standards for a 3010-day formal comment periodrecirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive recirculation ballot addresses the comments received from the second third posting and ballot.

Anticipated Actions	Anticipated Date
30-day Formal Comment Period with Parallel Successive Ballot	September 2012
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-004-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-004-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-5

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-5:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

Requirements and Measures

Rationale for R1: Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices ~~and~~ (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).
Reference to prior version: *CIP-004-4, R1*		**Change Rationale:** *Changed to remove the need to ensure or prove everyone with authorized* electronic or authorized unescorted physical *access "received" ongoing reinforcement – to state that security awareness has been reinforced.* *Moved example mechanisms to guidance.*	

Rationale for R2: To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:
   - The visitor control program
   - Electronic interconnectivity supporting the operation and control of BES Cyber Systems
   - Storage media as part of the handling of BES Cyber Systems information
2. Change references from Critical Cyber Assets to BES Cyber Systems.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
Reference to prior version: *CIP004-4, R2.2.1*		**Change Rationale:** *Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.*	

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
Reference to prior version: *CIP004-4, R2.1*		**Change Rationale:** *Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.*	
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.
Reference to prior version: *CIP004-4, R2.3*		**Change Rationale:** *Updated to replace "annually" with "once every 15 calendar months."*	

Rationale for R3: To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Addressed interpretation request in guidance. Specified that process for identity confirmation is ~~only~~ required ~~for each individual's initial assessment~~. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.*	

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Specify that the seven year criminal history check covers all locations where the individual has resided for six months or more, including current residence regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.*	

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process ~~Process~~ to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
Reference to prior version: *NEW*		Change Rationale: *There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.*	
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.
Reference to prior version: *CIP-004-4, R3.3*		Change Rationale: *Separated into its own table item.*	

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.
Reference to prior version: *CIP-004-3, R3, R3.3*		**Change Rationale**: *Whether for initial access or maintaining access, establishes that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment.*	

Rationale for R4: To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.
Reference to prior version: *CIP 003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1*		**Change Rationale:** Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*	

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
Reference to prior version: *CIP 004-4, R4.1*		**Change Rationale:** *Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.*	

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.
Reference to prior version: *CIP 007-4, R5.1.3*		**Change Rationale:** *Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary.*	

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.
Reference to prior version: *CIP-003-4, R5.1.2*		**Change Rationale:** *Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.*	

Rationale for R5: The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate."

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R5 – Access Revocation*. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
Reference to prior version: *CIP 004-4, R4.2*		**Change Rationale:** *The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards* ***to require immediate revocation*** *for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*	

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
Reference to prior version: *CIP-004-4, R4.2*		**Change Rationale:** *FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.*	

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date ~~and time~~ of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.
Reference to prior version: *NEW*		**Change Rationale:** *FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.*	

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
Reference to prior version: *NEW*		**Change Rationale:** *FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.*	

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.
Reference to prior version: *CIP-007-4, R5.2.3*		**Change Rationale:** *To provide clarification of expected actions in managing the passwords.*	

Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Regional Variances

None.

Interpretations

None.

Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1: The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and ~~does not require reconfirmation~~ only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

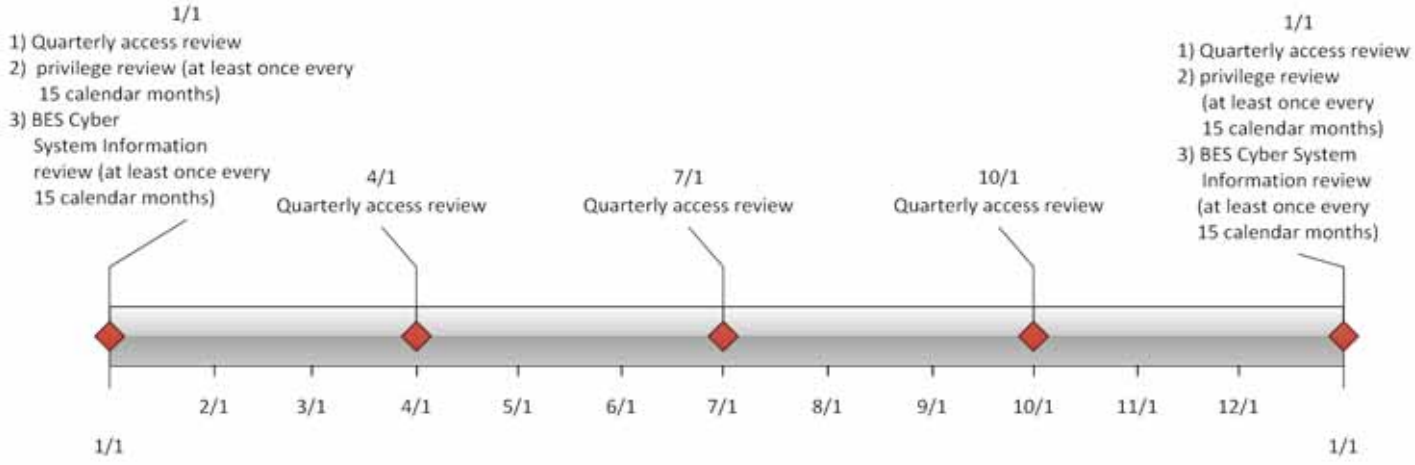

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.

Anticipated Actions	Anticipated Date
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-005-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-005-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-5

3. Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-005-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes.

These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity.

This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for R1: The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*	
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and BES Cyber System.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
Reference to prior version: *CIP-005-4, R2.1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.*	
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
Reference to prior version: *CIP-005-4, R2.3*		**Change Rationale:** *Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.*	

Rationale for R2: Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in *Guidance for Secure Interactive Remote Access* published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
Reference to prior version: *New*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.
Reference to prior version: *CIP-007-5, R3.1*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.*	

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
Reference to prior version: *CIP-007-5, R3.2*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run

between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. ~~4.~~ Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the ~~third~~ fourth posting of Version 5 of the CIP Cyber Security Standards for a ~~30~~10-day ~~formal comment period~~recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for ~~formal comment and parallel successive~~ recirculation ballot addresses the comments received from the ~~second~~ third posting and ballot.

Anticipated Actions	Anticipated Date
~~30-day Formal Comment Period with Parallel Successive Ballot~~	~~September 2012~~
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-005-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-005-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-5

3. Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-005-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it -believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes.

These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact -BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity.

This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for R1: The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*	
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and BES Cyber System.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
Reference to prior version: *CIP-005-4, R2.1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.*	
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
Reference to prior version: *CIP-005-4, R2.3*		**Change Rationale:** *Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.*	

Rationale for R2: Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in *Guidance for Secure Interactive Remote Access* published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The ~~Intermediate Device~~Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an ~~Intermediate Device~~Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the ~~Intermediate Device~~Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Utilize an Intermediate ~~Device~~ System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
Reference to prior version: *New*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate ~~Device~~System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.
Reference to prior version: *CIP-007-5, R3.1*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.*	

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
Reference to prior version: *CIP-007-5, R3.2*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The ~~standard does not require segmenting~~CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification.~~, and m~~Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber ~~s~~Systems within the ESP ~~will be elevated to~~must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The ~~standard~~ CIP Cyber Security Standards accomplish~~es this~~ the "high water mark" by ~~defining~~ associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run

between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.

Anticipated Actions	Anticipated Date
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-006-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-5

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-006-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale: Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. *Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.*

Summary of Changes: The entire content of CIP-006-5 is intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

Added details to address FERC Order No. 706, Paragraph 572, directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.
Reference to prior version: *CIP-006-4c, R2.1 for Physical Access Control Systems* *New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity*		**Change Description and Justification:** *Change Description and Justification: To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected at the same level as required in Parts 1.2 through 1.5.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
Reference to prior version: *CIP006-4c, R3 & R4*		**Change Description and Justification:** *This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
Reference to prior version: CIP006-4c, R3 & R4		**Change Description and Justification:** *The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.* *Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.* *FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).*	

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*	
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
Reference to prior version: CIP006-4c, R5		**Change Description and Justification:** *Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.
Reference to prior version: CIP006-4c, R5		**Change Description and Justification:** *Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.
Reference to prior version: CIP-006-4c, R6		**Change Description and Justification:** *CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.* *Examples of logging methods have been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change.*	

Rationale: To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.
Reference to prior version: *CIP-006-4c, R1.6.2*		**Change Description and Justification:** *Added the ability to not do this during CIP Exceptional Circumstances.*	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
Reference to prior version: *CIP-006-4c R1.6.1*		**Change Description and Justification:** *Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.*	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change*	

Rationale: To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.
Reference to prior version: *CIP-006-4c, R8.1 and R8.2*		**Change Description and Justification:** *Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the third fourth posting of Version 5 of the CIP Cyber Security Standards for a 3010-day formal comment periodrecirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive recirculation ballot addresses the comments received from the second third posting and ballot.

Anticipated Actions	Anticipated Date
30-day Formal Comment Period with Parallel Successive Ballot	September 2012
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-006-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-5

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-006-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale: Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. *Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.*

Summary of Changes: The entire content of CIP-006-5 is intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

Added details to address FERC Order No. 706, Paragraph 572, directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.
Reference to prior version: *CIP-006-4c, R2.1 for Physical Access Control Systems* *New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity*		**Change Description and Justification:** *Change Description and Justification: To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected ~~by a Physical Security Perimeter~~at the same level as required in Parts 1.2 through 1.5.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
Reference to prior version: *CIP006-4c, R3 & R4*		**Change Description and Justification:** *This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
Reference to prior version: CIP006-4c, R3 & R4		**Change Description and Justification:** *The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.* *Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.* *FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).*	

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident r~~R~~esponse p~~P~~lan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
Reference to prior version: *CIP006-4c, R5*		**Change Description and Justification:** *Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.*	
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
Reference to prior version: CIP006-4c, R5		**Change Description and Justification:** *Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident r~~R~~esponse p~~P~~lan within 15 minutes of the ~~unauthorized physical access~~detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.
Reference to prior version: CIP006-4c, R5		**Change Description and Justification:** *Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.
Reference to prior version: CIP-006-4c, R6		**Change Description and Justification:** *CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.* *Examples of logging methods have been moved to the Guidelines and Technical Basis section.*	

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change.*	

Rationale: To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.
Reference to prior version: *CIP-006-4c, R1.6.2*		**Change Description and Justification:** *Added the ability to not do this during CIP Exceptional Circumstances.*	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
Reference to prior version: *CIP-006-4c R1.6.1*		**Change Description and Justification:** *Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.*	

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.
Reference to prior version: CIP-006-4c, R7		**Change Description and Justification:** *No change*	

Rationale: To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.
Reference to prior version: *CIP-006-4c, R8.1 and R8.2*		**Change Description and Justification:** *Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.~~These alarms must provide for immediate notification to personnel responsible for response.~~
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

~~Outage records should address when the installed control, monitor, and logging systems or hardware at access points are broken or unavailable.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.

Anticipated Actions	Anticipated Date
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-007-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-007-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-5

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-007-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident

response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for R1: The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are needed. Physical I/O ports were added in response to a FERC order. The unneeded physical ports in Control Centers (which are the highest risk, most impactful areas) should be protected as well.

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.
Reference to prior version: *CIP-007-4, R2.1 and R2.2*		**Change Description and Justification:** *The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.*	

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
Reference to prior version: *NEW*		**Change Description and Justification:** *On March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.*	

Rationale for R2: Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" and there has been confusion as to what constitutes the availability date. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.
Reference to prior version: *CIP-007, R3*		**Change Rationale:** *The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches. Documenting the source is used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.
Reference to prior version: *CIP-007, R3.1*		**Change Rationale:** *Similar to the current wording but added "from the source or sources identified in 2.1" to clarify the 35-day time frame.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
Reference to prior version: *CIP-007, R3.2*		**Change Rationale:** *The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.*	
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.
Reference to prior version: *CIP-007, R3.2*		**Change Rationale:** *Similar to the current wording but added that the plan must be implemented within the timeframe specified in the plan, or in a revised plan as approved by the CIP Senior Manager or delegate.*	

Rationale for R3: Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.

Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"

In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
Reference to prior version: *CIP-007-4, R4; CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.*	

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
Reference to prior version: *CIP-007-4, R4* *CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes.*	

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.
Reference to prior version: *CIP-007-4, R4; CIP-007-4, R4.2*		**Change Rationale:** *Requirement essentially unchanged from previous versions; updated to refer to previous parts of the requirement table.*	

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Summary of Changes: Beginning in Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor."

The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the System. There are a few events explicitly listed that if a Cyber Asset or BES Cyber System can log, then it must log.

In addition, this requirement sets up parameters for the monitoring and reviewing of processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
Reference to prior version: *CIP-005-4, R3; CIP-007-4, R5, R5.1.2, R6.1, andR6.3*		**Change Description and Justification:** *This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.2*		**Change Description and Justification:** *This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate a response.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.4*		**Change Rationale:** *No substantive change.*	
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.5*		**Change Description and Justification:** *Beginning in Paragraph 525 and also 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for an approximately biweekly summary or sampling review of logs.*	

Rationale for R5: To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

Summary of Changes (From R5):

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT believes these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.
Reference to prior version: *CIP-007-4, R5*		**Change Rationale:** *The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.
Reference to prior version: *CIP-007-4, R5.2 and R5.2.1*		**Change Rationale:** *CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.
Reference to prior version: *CIP-007-4, R5.2.2*		**Change Rationale:** *No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
Reference to prior version: *CIP-007-4, R5.2.1*		**Change Rationale:** *The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.
Reference to prior version: *CIP-007-4, R5.3*		**Change Rationale:** *CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
Reference to prior version: *CIP-007-4, R5.3.3*		**Change Rationale:** **This was originally Requirement R5.5.3, but moved to add "external routable connectivity" to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.
Reference to prior version: *New Requirement*		**Change Rationale:** *Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only,

which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as

it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include:

(i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports.

The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. ~~4.~~ Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the ~~third~~ fourth posting of Version 5 of the CIP Cyber Security Standards for a ~~30~~10-day ~~formal comment period~~recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for ~~formal comment and parallel successive~~ recirculation ballot addresses the comments received from the ~~second~~ third posting and ballot.

Anticipated Actions	Anticipated Date
~~30-day Formal Comment Period with Parallel Successive Ballot~~	~~September 2012~~
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-007-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-007-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-5

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-007-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident

response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for R1: The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are needed. Physical I/O ports were added in response to a FERC order. The unneeded physical ports in Control Centers ~~environments~~ (which are the highest risk, most impactful areas) should be protected as well.

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.
Reference to prior version: *CIP-007-4, R2.1 and R2.2*		**Change Description and Justification:** *The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.*	

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
Reference to prior version: *NEW*		**Change Description and Justification:** *On March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.*	

Rationale for R2: Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" and there has been confusion as to what constitutes the availability date. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.
Reference to prior version: *CIP-007, R3*		**Change Rationale:** *The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches. Documenting the source is used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.
Reference to prior version: *CIP-007, R3.1*		**Change Rationale:** *Similar to the current wording but added "from the source or sources identified in 2.1" to clarify the ~~30~~35-day time frame.*	

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
Reference to prior version: *CIP-007, R3.2*		**Change Rationale:** *The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.*	
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.
Reference to prior version: *CIP-007, R3.2*		**Change Rationale:** *Similar to the current wording but added that the plan must be implemented within the timeframe specified in the plan, or in a revised plan as approved by the CIP Senior Manager or delegate.*	

Rationale for R3: Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.

Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"

In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
Reference to prior version: *CIP-007-4, R4; CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.*	

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of ~~identified~~ detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
Reference to prior version: *CIP-007-4, R4* *CIP-007-4, R4.1*		**Change Rationale:** *See the Summary of Changes.*	

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.
Reference to prior version: *CIP-007-4, R4; CIP-007-4, R4.2*		**Change Rationale:** *Requirement essentially unchanged from previous versions; updated to refer to previous parts of the requirement table.*	

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Summary of Changes: Beginning in Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor."

The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the System. There are a few events explicitly listed that if a Cyber Asset or BES Cyber System can log, then it must log.

In addition, this requirement sets up parameters for the monitoring and reviewing of processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
Reference to prior version: *CIP-005-4, R3; CIP-007-4, R5, R5.1.2, R6.1, andR6.3*		**Change Description and Justification:** *This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.2*		**Change Description and Justification:** *This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate a response.*	

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.4*		**Change Rationale:** *No substantive change.*	
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.
Reference to prior version: *CIP-005-4, R3.2; CIP-007-4, R6.5*		**Change Description and Justification:** *Beginning in Paragraph 525 and also 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for an approximately biweekly summary or sampling review of logs.*	

Rationale for R5: To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

Summary of Changes (From R5):

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT ~~feels~~ believes these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.
Reference to prior version: *CIP-007-4, R5*		**Change Rationale:** *The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.
Reference to prior version: *CIP-007-4, R5.2 and R5.2.1*		**Change Rationale:** *CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.
Reference to prior version: *CIP-007-4, R5.2.2*		**Change Rationale:** *No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
Reference to prior version: *CIP-007-4, R5.2.1*		**Change Rationale:** *The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.
Reference to prior version: *CIP-007-4, R5.3*		**Change Rationale:** *CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
Reference to prior version: *CIP-007-4, R5.3.3*		**Change Rationale:** **This was originally Requirement R5.5.3, but moved to add "external routable connectivity" to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.*	

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.
Reference to prior version: *New Requirement*		**Change Rationale:** *Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only,

which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as

it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include:

(i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device~~, but the entity disables or neglects to enable that logging, it is a violation~~ then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log

analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.

Anticipated Actions	Anticipated Date
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-008-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-008-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-5

3. Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-008-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes.

These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

B. Requirements and Measures

Rationale for R1: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions. These are described below each Requirement Part.

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).*	

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.*	
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Conforming change to reference new defined term Cyber Security Incidents.*	

Rationale for R2: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** *Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.*	

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain records related to Reportable Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.
Reference to prior version: *CIP-008, R2*		**Change Description and Justification:** *Removed references to the retention period because the Standard addresses data retention in the Compliance Section.*	

Rationale for R3: Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident.*

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *CIP-008, R1.5*		**Change Description and Justification:** *Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.*	

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *CIP-008, R1.4*		**Change Description and Justification:** *Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a Cyber Security Incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. Table top exercises (TTX) can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response

activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

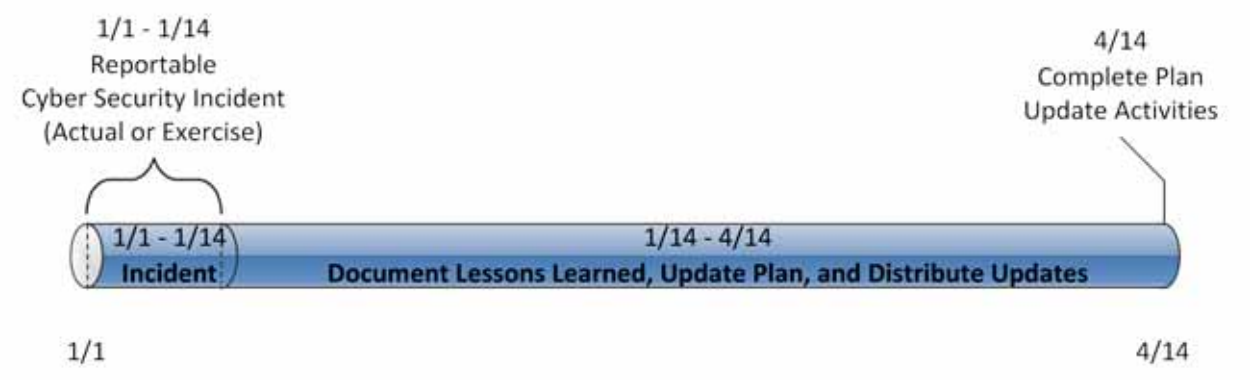

Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the incident and documenting the lessons learned as soon after the incident as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the incident response team.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

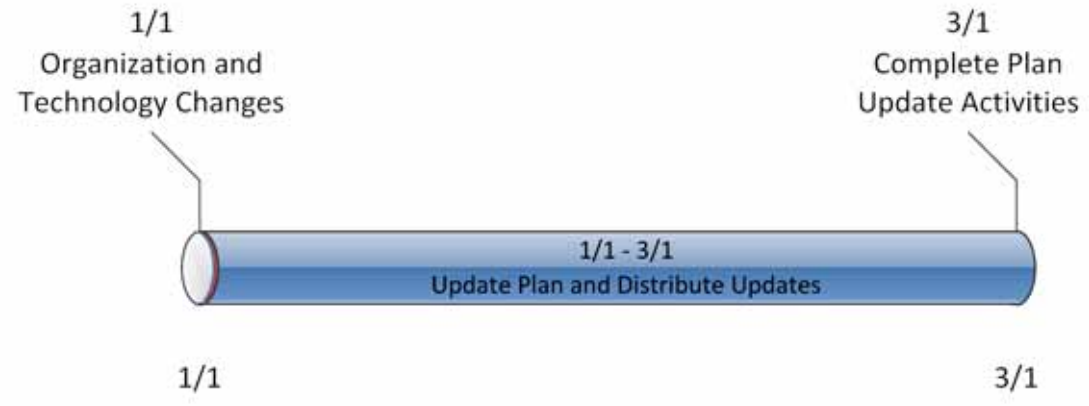

Figure 2: Timeline for Plan Changes in 3.2

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the third fourth posting of Version 5 of the CIP Cyber Security Standards for a 3010-day formal comment periodrecirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive recirculation ballot addresses the comments received from the second third posting and ballot.

Anticipated Actions	Anticipated Date
30-day Formal Comment Period with Parallel Successive Ballot	September 2012
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-008-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-008-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-5

3. Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-008-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it -believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes.

These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

B. Requirements and Measures

Rationale for R1: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions. These are described below each Requirement Part.

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from ~~identification~~ the determination of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).
Reference to prior version: *CIP-008, R1.1*		**Change Description and Justification:** *Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).*	

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.*	
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).
Reference to prior version: *CIP-008, R1.2*		**Change Description and Justification:** *Conforming change to reference new defined term Cyber Security Incidents.*	

Rationale for R2: The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test each Cyber Security Incident response plan(s) at least once every ~~calendar year, not to exceed~~ 15 calendar months ~~between executions of the plan(s)~~: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.
Reference to prior version: *CIP-008, R1.6*		**Change Description and Justification:** *Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.*	

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain records related to Reportable Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.
Reference to prior version: *CIP-008, R2*		**Change Description and Justification:** *Removed references to the retention period because the Standard addresses data retention in the Compliance Section.*	

Rationale for R3: Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident.*

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 90 calendar days a~~A~~fter completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response~~, and not to exceed 90 calendar days after completion~~: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *CIP-008, R1.5*		**Change Description and Justification:** *Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.*	

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 60 calendar days a~~A~~fter a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan~~, not to exceed 60 calendar days~~: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *CIP-008, R1.4*		**Change Description and Justification:** *Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a Cyber Security Incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. Table top exercises (TTX) can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response

activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

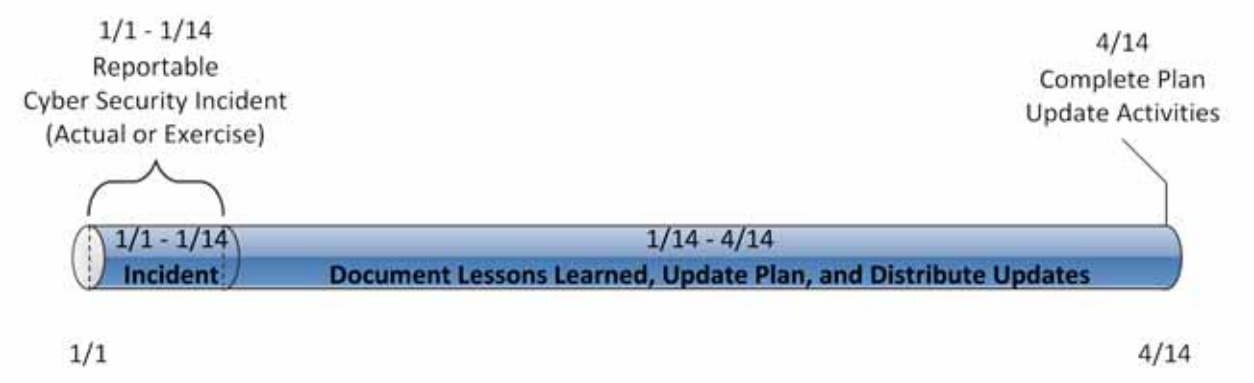

Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the incident and documenting the lessons learned as soon after the incident as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the incident response team.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

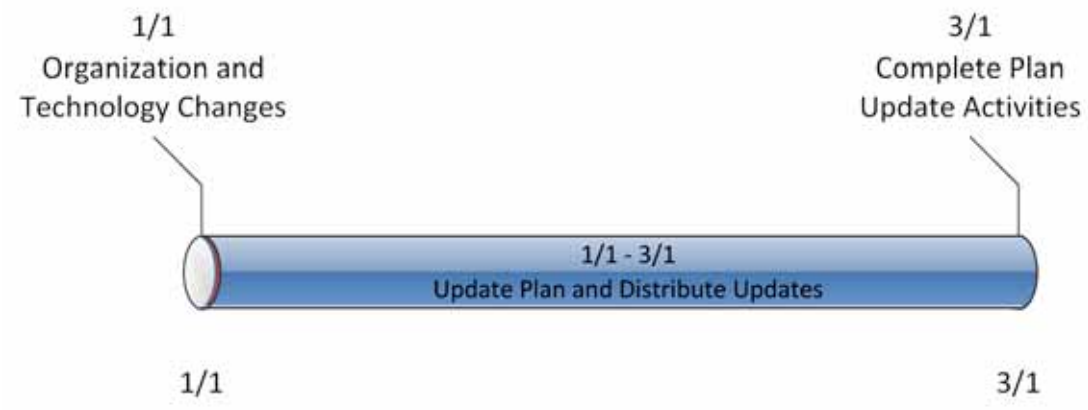

Figure 2: Timeline for Plan Changes in 3.2

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.

Anticipated Actions	Anticipated Date
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-009-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-5

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-009-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident

response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for R1: Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
Reference to prior version: *CIP-009, R1.1*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
Reference to prior version: *CIP-009, R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.
Reference to prior version: *CIP-009, R4*		**Change Description and Justification:** *Addresses FERC Order Paragraph 739 and 748. The modified wording was abstracted from Paragraph 744.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Addresses FERC Order Section 739 and 748.*	
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added requirement to address FERC Order No. 706, Paragraph 706.*	

Rationale for R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Minor wording change; essentially unchanged.*	

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
Reference to prior version: *CIP-009, R5*		**Change Description and Justification:** *Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.*	

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.*	

Rationale for R3: To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

Summary of Changes: Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *CIP-009, R1 and R3*		**Change Description and Justification:** *Added the timeframes for performing lessons learned and completing the plan updates. This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the specific changes that would require an update.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

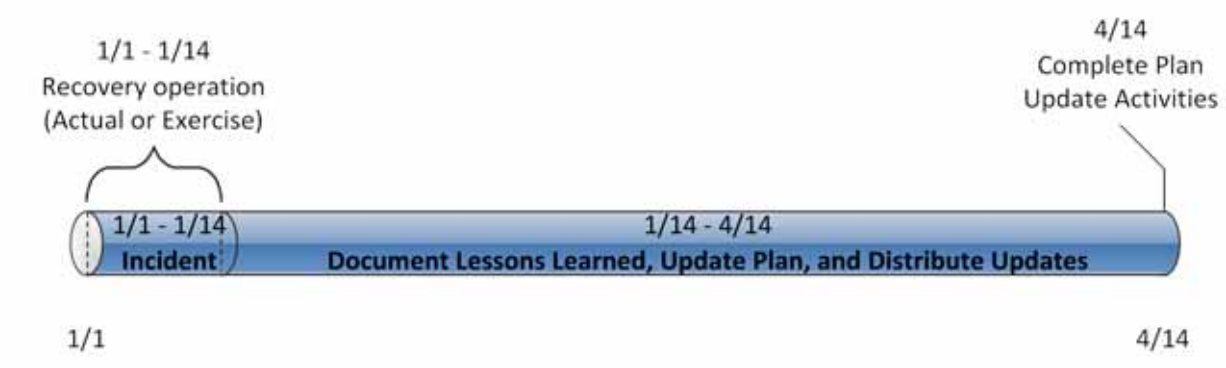

R1. **Figure 1: CIP-009-5 R3 Timeline**

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

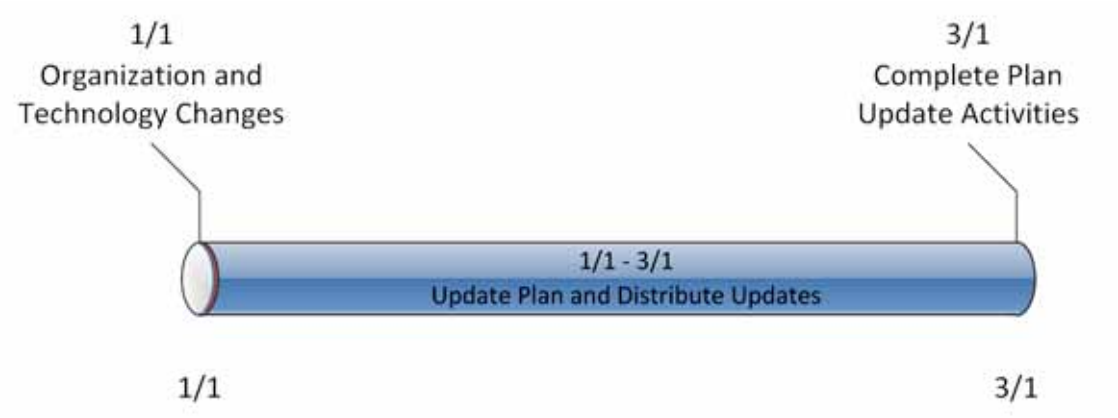

R2. **Figure 2: Timeline for Plan Changes in 3.2**

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the third fourth posting of Version 5 of the CIP Cyber Security Standards for a 3010-day formal comment periodrecirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive recirculation ballot addresses the comments received from the second third posting and ballot.

Anticipated Actions	Anticipated Date
30-day Formal Comment Period with Parallel Successive Ballot	September 2012
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-009-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-5

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-009-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident

response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

Rationale for R1: Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
Reference to prior version: *CIP-009, R1.1*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
Reference to prior version: *CIP-009, R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.
Reference to prior version: *CIP-009, R4*		**Change Description and Justification:** *Addresses FERC Order Paragraph 739 and 748. The modified wording was abstracted from Paragraph 744.*	

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Addresses FERC Order Section 739 and 748.*	
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s)~~, per device capability~~. Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added requirement to address FERC Order No. 706, Paragraph 706.*	

Rationale for R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months ~~between tests of the plan~~: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Minor wording change; essentially unchanged.*	

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
Reference to prior version: *CIP-009, R5*		**Change Description and Justification:** *Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.*	

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.
Reference to prior version: *CIP-009, R2*		**Change Description and Justification:** *Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.*	

Rationale for R3: To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

Summary of Changes: Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days a~~A~~fter completion of a recovery plan test or actual recovery~~, and not to exceed 90 calendar days~~: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *CIP-009, R1 and R3*		**Change Description and Justification:** *Added the timeframes for performing lessons learned and completing the plan updates.This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.*	

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days a~~A~~fter a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan~~, and not to exceed 60 calendar days~~: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the specific changes that would require an update.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

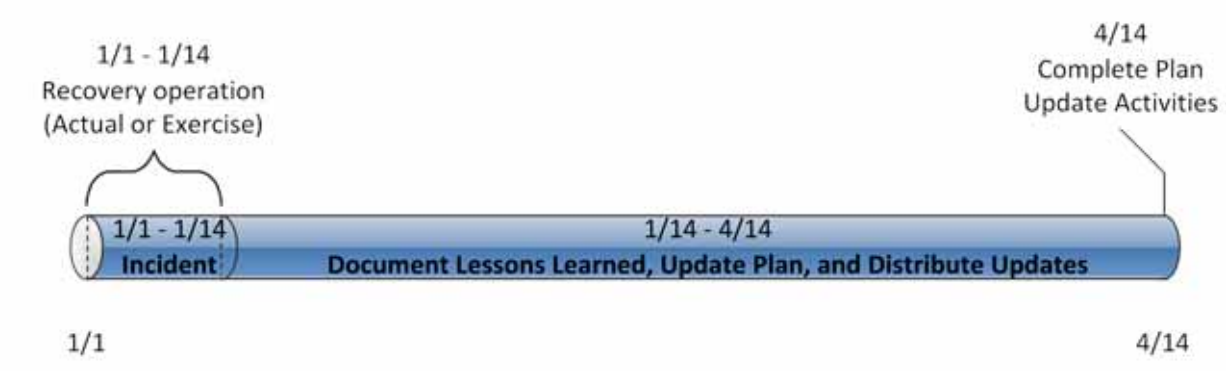

R1. **Figure 1: CIP-009-5 R3 Timeline**

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

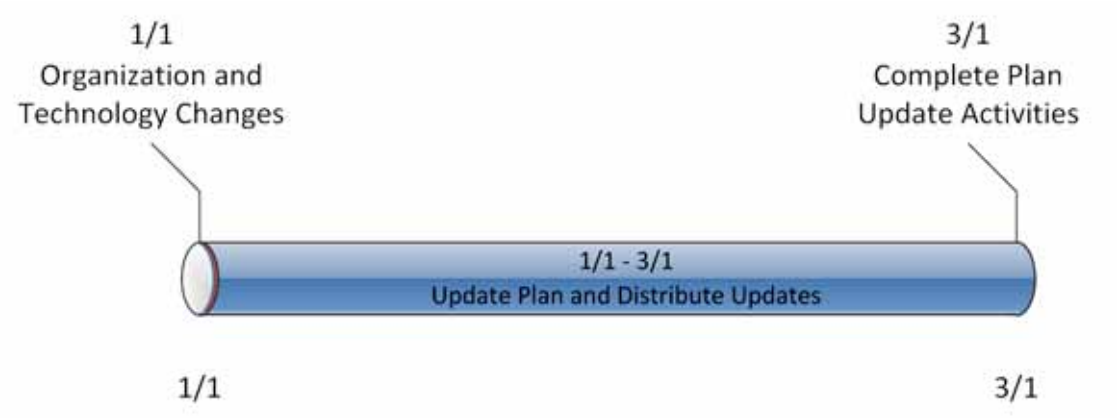

R2. **Figure 2: Timeline for Plan Changes in 3.2**

When notifying individuals of response plan changes, entities should keep in mind that recovery plans ~~are~~ may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.

Anticipated Actions	Anticipated Date
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-010-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-010-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-1

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-010-1:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-010-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the

documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)**– Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)**– Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System

B. Requirements and Measures

Rationale – R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.
Reference to prior version: *New Requirement*		**Change Rationale:** *The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.
Reference to prior version: *CIP-007-3, R9; CIP-003-3, R6*		**Change Rationale:** *The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3, Requirement R6.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
Reference to prior version: *CIP-007-3, R9; CIP-005-3, R5*		**Change Rationale:** *Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.* *This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.*	

Rationale – R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.
Reference to prior version: *New Requirement*		**Change Rationale:** *The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.* *This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397.* *Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.*	

Rationale – R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.
Reference to prior version: *CIP-005-4, R4; CIP-007-4, R8*		**Change Rationale:** *As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.* *As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.*	
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).
Reference to prior version: *CIP-005-3, R4.5; CIP-007-3, R8.4*		**Change Rationale:** *Added a requirement for an entity planned date of completion as per the directive in FERC Order No. 706, Paragraph 643.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If

additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-5. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-5 R2.1 requires entities to track, evaluate, and install security patches, CIP-010 R1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.

4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
4.5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the third fourth posting of Version 5 of the CIP Cyber Security Standards for a 3010-day formal comment periodrecirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive recirculation ballot addresses the comments received from the second third posting and ballot.

Anticipated Actions	Anticipated Date
30-day Formal Comment Period with Parallel Successive Ballot	September 2012
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-010-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-010-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-1

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-010-1:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-010-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the

documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)**– Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)**– Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System

B. Requirements and Measures

Rationale – R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.
Reference to prior version: *New Requirement*		**Change Rationale:** *The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.
Reference to prior version: *CIP-007-3, R9; CIP-003-3, R6*		**Change Rationale:** *The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3, Requirement R6.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
Reference to prior version: *CIP-007-3, R9; CIP-005-3, R5*		**Change Rationale:** *Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment~~,~~ or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-3, R1*		**Change Rationale:** *This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.* *This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.*	

Rationale – R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.
Reference to prior version: *New Requirement*		**Change Rationale:** *The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.* *This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397.* *Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.*	

Rationale – R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.
Reference to prior version: *CIP-005-4, R4; CIP-007-4, R8*		**Change Rationale:** *As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.* *As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.*	
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).
Reference to prior version: *CIP-005-3, R4.5; CIP-007-3, R8.4*		**Change Rationale:** *Added a requirement for an entity planned date of completion as per the directive in FERC Order No. 706, Paragraph 643.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If

additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-5. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-5 R2.1 requires entities to track, evaluate, and install security patches, CIP-010 R1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.

4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the fourth posting of Version 5 of the CIP Cyber Security Standards for a 10-day recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for recirculation ballot addresses the comments received from the third posting and ballot.

Anticipated Actions	Anticipated Date
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-011-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-011-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-1

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-011-1:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-011-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)**– Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System

Rationale – R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Summary of Changes: CIP 003-4 R4, R4.2, and R 4.3 have been moved to CIP 011 R1. CIP-003-4, Requirement R4.1 was moved to the definition of BES Cyber System Information.

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-1 Table R1 – Information Protection. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.
Reference to prior version: *CIP-003-3, R4; CIP-003-3, R4.2*		**Change Rationale:** *The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection (*e.g., confidential, public, internal use only, etc.*) This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.*	

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).
Reference to prior version: *CIP-003-3, R4;*		**Change Rationale:** *The SDT changed the language from "protect" information to "Procedures for protecting and securely handling" to clarify the protection that is required.*	

Rationale – R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.
Reference to prior version: *CIP-007-3, R7.2*		**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*	

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.
Reference to prior version: *CIP-007-3, R7.1*		**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.* *The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the

analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).
5. ~~4.~~ Third posting for 30-day formal comment period and concurrent ballot (September 2012).

Description of Current Draft

This is the ~~third~~ fourth posting of Version 5 of the CIP Cyber Security Standards for a ~~30~~10-day ~~formal comment period~~recirculation ballot. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ballot. A second posting of Version 5 was posted in April 2012 for a 40-day comment period and ballot. A third posting of Version 5 was posted in September 2012 for a 30-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for ~~formal comment and parallel successive~~ recirculation ballot addresses the comments received from the ~~second~~ third posting and ballot.

Anticipated Actions	Anticipated Date
~~30-day Formal Comment Period with Parallel Successive Ballot~~	~~September 2012~~
Recirculation ballot	November 2012
BOT adoption	December 2012

Effective Dates

1. **24 Months Minimum** – CIP-011-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-011-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
1	TBD	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-1

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-011-1:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Background:

Standard CIP-011-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)**– Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System

Rationale – R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Summary of Changes: CIP 003-4 R4, R4.2, and R 4.3 have been moved to CIP 011 R1. CIP-003-4, Requirement R4.1 was moved to the definition of BES Cyber System Information.

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-1 Table R1 – Information Protection. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.
Reference to prior version: *CIP-003-3, R4; CIP-003-3, R4.2*		**Change Rationale:** *The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection (*e.g., confidential, public, internal use only, etc.*) This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.*	

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).
Reference to prior version: *CIP-003-3, R4;*		**Change Rationale:** *The SDT changed the language from "protect" information to "Procedures for protecting and securely handling" to clarify the protection that is required.*	

Rationale – R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.
Reference to prior version: *CIP-007-3, R7.2*		**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.*	

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of ~~a~~ an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.
Reference to prior version: *CIP-007-3, R7.1*		**Change Rationale:** *Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.* *The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the

analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Implementation Plan for Version 5 CIP Cyber Security Standards

October 26, 2012

Prerequisite Approvals
All Version 5 CIP Cyber Security Standards and the proposed additions, modifications, and retirements of terms to the *Glossary of Terms* used in *NERC Reliability Standards* must be approved before these standards can become effective.

Applicable Standards
The following standards and definitions, collectively referred to as "Version 5 CIP Cyber Security Standards,"[1] are covered by this Implementation Plan:

CIP–002–5 — Cyber Security — BES Cyber System Categorization
CIP–003–5 — Cyber Security — Security Management Controls
CIP–004–5 — Cyber Security — Personnel and Training
CIP–005–5 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–5 — Cyber Security — Physical Security of BES Cyber Systems
CIP–007–5 — Cyber Security — Systems Security Management
CIP–008–5 — Cyber Security — Incident Reporting and Response Planning
CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems
CIP–010–1 — Cyber Security — Configuration Change Management and Vulnerability Assessments
CIP–011–1 — Cyber Security — Information Protection

"Definitions of Terms used in Version 5 CIP Cyber Security Standards" document, which includes proposed additions, modifications, and retirements of terms to the *Glossary of Terms used in NERC Reliability Standards*.

These standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

When these standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards become effective, all prior versions of these standards are retired.

[1] Although CIP-010-1 and CIP-011-1 are proposed as first versions, any reference to "Version 5 CIP Cyber Security Standards" includes CIP-010-1 and CIP-011-1, in addition to CIP-002-5 through CIP-009-5, because CIP-010-1 and CIP-011-1 were developed as part of the "Version 5 CIP Cyber Security Standards" development process.

Compliance with Standards

Once these standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards become effective, the responsible entities identified in the Applicability Section of the standard must comply with the requirements.

Proposed Effective Date for Version 5 CIP Cyber Security Standards

Responsible entities shall comply with all requirements in CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 as follows:

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[2]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5 R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Initial Performance of Certain Periodic Requirements

Specific Version 5 CIP Cyber Security Standards have periodic requirements that contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and responsible entities shall comply initially with those periodic requirements as follows:

1. On or before the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-002-5, Requirement R2
   - CIP-003-5, Requirement R1
2. On or before the Effective Date of CIP-003-5, Requirement R2 for the following requirement:
   - CIP-003-5, Requirement R2

[2] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

3. Within 14 calendar days after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-007-5, Requirement R4, Part 4.4
4. Within 35 calendar days after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-010-1, Requirement R2, Part 2.1
5. Within three calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5, Requirement R4, Part 4.2
6. Within 12 calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5, Requirement R2, Part 2.3
   - CIP-004-5, Requirement R4, Parts 4.3 and 4.4
   - CIP-006-5, Requirement R3, Part 3.1
   - CIP-008-5, Requirement R2, Part 2.1
   - CIP-009-5, Requirement R2, Parts 2.1, 2.2
   - CIP-010-1, Requirement R3, Parts 3.1
7. Within 24 calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-009-5, Requirement R2, Part 2.3
   - CIP-010-1, Requirement R3, Part 3.2
8. Within 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment for the following requirement:
   - CIP-004-5, Requirement R3, Part 3.5.

Previous Identity Verification

A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be reperformed under CIP-004-5, Requirement R3, Part 3.1.

Planned or Unplanned Changes Resulting in a Higher Categorization

Planned changes refer to any changes of the electric system or BES Cyber System as identified through the annual assessment under CIP-002-5, Requirement R2, which were planned and implemented by the responsible entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the Version 5 CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System, as identified through the annual assessment under CIP-002-5, Requirement R2, which were not planned by the responsible entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-5, Attachment 1, criteria.

For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies first medium impact or high impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 months

Applicability Reference Tables

The following tables are provided as a convenient reference to show which requirements in the Version 5 CIP Cyber Security Standards apply to specific Cyber Assets.

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-004-5 R2	Cyber Security Training Program	X	X	
CIP-004-5 R3	Personnel Risk Assessment Program	X	X	
CIP-004-5 R4	Access Management Program	X	X	
CIP-004-5 R5	Access Revocation	X	X	
CIP-005-5 R1 Part 1.2	Electronic Security Perimeter			X
CIP-005-5 R2	Remote Access Management			X
CIP-006-5 R1	Physical Security Plan	X	X	X
CIP-006-5 R2	Visitor Control Program	X		X
CIP-006-5 R3	Maintenance and Testing Program		X	

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-007-5 R1	Ports and Services	X	X	X
CIP-007-5 R2	Security Patch Management	X	X	X
CIP-007-5 R3	Malicious Code Prevention	X	X	X
CIP-007-5 R4	Security Event Monitoring	X	X	X
CIP-007-5 R5	System Access Control	X	X	X
CIP-010-1 R1	Configuration Change Management	X	X	X
CIP-010-1 R2	Configuration Monitoring	X	X	X
CIP-010-1 R3	Vulnerability Assessments	X	X	X
CIP-011-1 R1	Information Protection	X	X	
CIP-011-1 R2	BES Cyber Asset Reuse and Disposal	X	X	X

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 5 CIP Cyber Security Standards

~~September 17~~October 26, 2012

~~**Note**: On September 17, 2012, NERC was alerted that some references in the "Initial Performance of Certain Periodic Requirements" section were incorrectly synchronized to certain changes that occurred in the standards since draft 2.~~

~~This revised draft corrects the reference from "CIP-007-5, Requirement R4, Part 4.5" to "CIP-007-5, Requirement R4, Part R4.4," it removes the references to "CIP-007-5, Requirement R3, Part 3.3" and "CIP-011-1, Requirement R1, Part 1.3," and it removes the duplicate reference to CIP-009-5, Requirement R2, Part 2.3. It also corrects instances of typographical spelling errors of "identified" and "security."~~

~~No other changes were made to this implementation plan or any of the other CIP V5 standards currently posted.~~

Prerequisite Approvals

All Version 5 CIP Cyber Security Standards and the proposed additions, modifications, and retirements of terms to the *Glossary of Terms* used in *NERC Reliability Standards* must be approved before these standards can become effective.

Applicable Standards

The following standards and definitions, collectively referred to as "Version 5 CIP Cyber Security Standards,"[1] are covered by this Implementation Plan:

CIP–002–5 — Cyber Security — BES Cyber System Categorization
CIP–003–5 — Cyber Security — Security Management Controls
CIP–004–5 — Cyber Security — Personnel and Training
CIP–005–5 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–5 — Cyber Security — Physical Security of BES Cyber Systems
CIP–007–5 — Cyber Security — Systems Security Management
CIP–008–5 — Cyber Security — Incident Reporting and Response Planning
CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems
CIP–010–1 — Cyber Security — Configuration Change Management and Vulnerability Assessments
CIP–011–1 — Cyber Security — Information Protection

[1] Although CIP-010-1 and CIP-011-1 are proposed as first versions, any reference to "Version 5 CIP Cyber Security Standards" includes CIP-010-1 and CIP-011-1, in addition to CIP-002-5 through CIP-009-5, because CIP-010-1 and CIP-011-1 were developed as part of the "Version 5 CIP Cyber Security Standards" development process.

"Definitions of Terms used in Version 5 CIP Cyber Security Standards" document, which includes proposed additions, modifications, and retirements of terms to the *Glossary of Terms used in NERC Reliability Standards*.

These standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

When these standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards become effective, the responsible entities identified in the Applicability Section of the standard must comply with the requirements.

Proposed Effective Date for Version 5 CIP Cyber Security Standards

Responsible entities shall comply with all requirements in CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 as follows:

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[2]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5 R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Initial Performance of Certain Periodic Requirements

Specific Version 5 CIP Cyber Security Standards have periodic requirements that contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to,

[2] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

". . . at least once every 15 calendar months . . .", and responsible entities shall comply initially with those periodic requirements as follows:

1. On or before the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-002-5, Requirement R2
   - CIP-003-5, Requirement R1
2. On or before the Effective Date of CIP-003-5, Requirement R2 for the following requirement:
   - CIP-003-5, Requirement R2
3. Within 14 calendar days after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-007-5, Requirement R4, Part 4.4
4. Within 35 calendar days after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-010-1, Requirement R2, Part 2.1
5. Within three calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5, Requirement R4, Part 4.2
6. Within 12 calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5, Requirement R2, Part 2.3
   - CIP-004-5, Requirement R4, Parts 4.3 and 4.4
   - CIP-006-5, Requirement R3, Part 3.1
   - CIP-008-5, Requirement R2, Part 2.1
   - ~~CIP-008-5, Requirement R3, Part 3.1~~
   - CIP-009-5, Requirement R2, Parts 2.1, 2.2
   - ~~CIP-009-5, Requirement R3, Part 3.1~~
   - CIP-010-1~~5~~, Requirement R3, Parts 3.1
7. Within 24 calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-009-5, Requirement R2, Part 2.3
   - CIP-010-1, Requirement R3, Part 3.2

8. Within 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment for the following requirement:
   - CIP-004-5, Requirement R3, Part 3.5.

Previous Identity Verification

A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be reperformed under CIP-004-5, Requirement R3~~4~~, Part 3~~4~~.1.

Planned or Unplanned Changes Resulting in a Higher Categorization

Planned changes refer to any changes of the electric system or BES Cyber System as identified through the annual assessment under CIP-002-5, Requirement R2, which were planned and implemented by the responsible entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the Version 5 CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System, as identified through the annual assessment under CIP-002-5, Requirement R2, which were not planned by the responsible entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-5, Attachment 1, criteria.

For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same

manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies first medium impact or high impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 months

Applicability Reference Tables

The following tables are provided as a convenient reference to show which requirements in the Version 5 CIP Cyber Security Standards apply to specific Cyber Assets.

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-004-5 R2	Cyber Security Training Program	X	X	
CIP-004-5 R3	Personnel Risk Assessment Program	X	X	
CIP-004-5 R4	Access Management	X	X	

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
	Program			
CIP-004-5 R5	Access Revocation	X	X	
CIP-005-5 R1 Part 1.2	Electronic Security Perimeter			X
CIP-005-5 R2	Remote Access Management			X
CIP-006-5 R1	Physical Security Plan	X	X	X
CIP-006-5 R2	Visitor Control Program	X		X
CIP-006-5 R3	Maintenance and Testing Program		X	
CIP-007-5 R1	Ports and Services	X	X	X
CIP-007-5 R2	Security Patch Management	X	X	X
CIP-007-5 R3	Malicious Code Prevention	X	X	X
CIP-007-5 R4	Security Event Monitoring	X	X	X
CIP-007-5 R5	System Access Control	X	X	X
CIP-010-1 R1	Configuration Change Management	X	X	X
CIP-010-1 R2	Configuration Monitoring	X	X	X
CIP-010-1 R3	Vulnerability Assessments	X	X	X
CIP-011-1 R1	Information Protection	X	X	
CIP-011-1 R2	BES Cyber Asset Reuse and Disposal	X	X	X

Definitions of Terms Used in Version 5 CIP Cyber Security Standards

This section includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards and proposes terms for retirement. Terms already defined in the Glossary of Terms used in NERC Reliability Standards are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary. New defined terms are underscored. For existing glossary terms, new language is shown as underscored, while deleted language is shown as stricken. The list of terms proposed for retirement is at the end of the document.

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

BES Cyber System

One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

BES Cyber System Information

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

CIP Exceptional Circumstance

A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.

Control Center

One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

Cyber Assets

Programmable electronic devices, ~~and communication networks~~ including the hardware, software, and data in those devices.

Cyber Security Incident

~~Any~~ A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter ~~of a Critical Cyber Asset~~, or~~,~~
- Disrupts, or was an attempt to disrupt, the operation of a ~~Critical Cyber Asset~~ BES Cyber System.

Dial-up Connectivity

A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.

Electronic Access Control or Monitoring Systems ("EACMS")

Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Devices.

Electronic Access Point ("EAP")

A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Electronic Security Perimeter ("ESP")

The logical border surrounding a network to which ~~Critical Cyber Assets~~ BES Cyber Systems are connected using a routable protocol ~~and for which access is controlled~~.

External Routable Connectivity

The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.

Interactive Remote Access

User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Intermediate System

A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.

Physical Access Control Systems ("PACS")

Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Physical Security Perimeter ("PSP")

~~The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.~~

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Protected Cyber Assets ("PCA")

One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Reportable Cyber Security Incident

A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.

Terms to be retired from the *Glossary of Terms used in NERC Reliability Standards* **once the standards that use those terms are replaced:**

Critical Assets

Critical Cyber Assets

Definitions of Terms Used in Version 5 CIP Cyber Security Standards

This section includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards and proposes terms for retirement. Terms already defined in the Glossary of Terms used in NERC Reliability Standards are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary. New defined terms are underscored. For existing glossary terms, new language is shown as underscored, while deleted language is shown as stricken. The list of terms proposed for retirement is at the end of the document.

~~**Note**: On September 21, 2012, consistent with corrections to CIP-002-5, this draft was revised to correct the incorrect functional model reference in Control Center from "Generation Operator" to "Generator Operator"~~

~~No other changes were made to the definitions or any of the other CIP V5 standards currently posted except as specified in CIP-002-5.~~

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

BES Cyber System

One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

BES Cyber System Information

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and

Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

CIP Exceptional Circumstance

A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death~~,~~; a natural disaster~~,~~; civil unrest~~,~~; an imminent or existing hardware, software, or equipment failure~~,~~; a Cyber Security Incident requiring emergency assistance~~,~~; a response by emergency services~~,~~; the enactment of a mutual assistance agreement~~,~~; or an impediment of large scale workforce availability.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.

Control Center

One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

Cyber Assets

Programmable electronic devices, ~~and communication networks~~ including the hardware, software, and data in those devices.

Cyber Security Incident

~~Any~~ A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter~~ of a Critical Cyber Asset~~, or~~,~~
- Disrupts, or was an attempt to disrupt, the operation of a ~~Critical Cyber Asset~~ BES Cyber System.

Dial-up Connectivity

A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.

Electronic Access Control or Monitoring Systems ("EACMS")

Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Devices.

Electronic Access Point ("EAP")

A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Electronic Security Perimeter ("ESP")

The logical border surrounding a network to which ~~Critical Cyber Assets~~ BES Cyber Systems are connected using a routable protocol ~~and for which access is controlled~~.

External Routable Connectivity

The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.

Interactive Remote Access

User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Intermediate ~~Device~~ System

A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate ~~Device~~ System must not be located inside the Electronic Security Perimeter.

Physical Access Control Systems ("PACS")

Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Physical Security Perimeter ("PSP")

~~The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.~~

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Protected Cyber Assets ("PCA")

One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Reportable Cyber Security Incident

A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.

Terms to be retired from the *Glossary of Terms used in NERC Reliability Standards* **once the standards that use those terms are replaced:**

Critical Assets

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2008-06 - CSO Order 706

Unofficial Comment Form

Please **DO NOT** use this form for submitting comments. Please use the electronic form to submit comments on the VRFs and VSLs of the Standards. The electronic comment form must be completed by 8 p.m. ET, **November 5, 2012.**

If you have questions please contact Steven Noess at steven.noess@nerc.net or by telephone at 404-446-2560.

Project Page

Background Information

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

Version 5 of the NERC CIP Cyber Security Standards is intended to address all remaining standards related issues of FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed. Additional information about the project is available on the project page.

One of the ERO's priorities is to develop a robust set of critical infrastructure reliability standards that enable the industry to adapt to continuously changing threats and vulnerabilities by emphasizing security risk management.

The VRFs and VSLs for all of the standards have been consolidated into one document. Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the ERO Sanction Guidelines.

You do not have to answer all questions. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.

1. Do you agree with the VRFs and VSLs for CIP-002-5? If not, please provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

2. Do you agree with the VRFs and VSLs for CIP-003-5? If not, please provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

3. Do you agree with the VRFs and VSLs for CIP-004-5? If not, please provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

4. Do you agree with the VRFs and VSLs for CIP-005-5? If not, please provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

5. Do you agree with the VRFs and VSLs for CIP-006-5? If not, please provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

6. Do you agree with the VRFs and VSLs for CIP-007-5? If not, please provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

7. Do you agree with the VRFs and VSLs for CIP-008-5? If not, please provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

8. Do you agree with the VRFs and VSLs for CIP-009-5? If not, please provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

9. Do you agree with the VRFs and VSLs for CIP-010-1? If not, please provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

10. Do you agree with the VRFs and VSLs for CIP-011-1? If not, please provide specific suggestions for improvement.

    ☐ Yes

    ☐ No

    Comments:

11. If you have any other comments on these VRFs and VSLs that you haven't already mentioned above, please provide them here:

    Comments:

Project 2008-06 - Cyber Security Order No. 706 - V5

Consolidated VSLs from all standards

October 26, 2012

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	High	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES Cyber Systems have not been categorized	four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of	six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or	to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.	100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified;	medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible	or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber Systems have not been identified.	Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	
R2	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity did not complete its	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (R2.2)	approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (R2.2)	approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (R2.2)	required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			review in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1)	months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did	within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar	documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar months of the previous approval. (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				complete this approval in less than or equal to 17 calendar months of the previous approval. (R1)	months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	
R2	**Operations Planning**	**Lower**	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible	The Responsible Entity did not document or implement any cyber security policies for assets with a low impact rating that address the topics as required by R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2)	Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this	Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				the previous approval. (R2)	the previous approval. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, and	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days but did document this change in less than 40 calendar days of the change. (R4)	delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	has Identified deficiencies but did not assess or correct the deficiencies.(R4) OR The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, but did not identify, assess, or correct the deficiencies.(R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions	OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the	and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals	and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for	The Responsible Entity has a program for conducting Personnel	The Responsible Entity has a program for conducting Personnel	The Responsible Entity did not have all of the required elements as

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments	Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did not identify, assess, and	Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess,	described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including	correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)	and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)	or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors,	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess,	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess,	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted	and correct the deficiencies. (3.5)	and correct the deficiencies. (3.5)	for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter, and did not identify, assess and	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2)	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies.	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for	storage locations where BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)	BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						for four or more BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1)	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1)	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4)	OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or	OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or	access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR	more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances, and did not identify, assess, and correct			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the deficiencies. (5.5)			

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning and Same Day Operations**	**Medium**			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-5 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						outbound access permissions and deny all other access by default. (1.3) OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8) OR The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of	The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7) OR The Responsible Entity	The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies.	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity documented and implemented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			entry but did not identify, assess, or correct the deficiencies. (1.8) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)	has a process communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)	(1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5) OR The Responsible Entity has a process to	operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					monitor for unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.6) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)	deficiencies, but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						(1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						different controls, but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						correct the deficiencies. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter or to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						minutes to identified personnel(1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9)
R2	**Same-Day**	**Medium**	N/A	The Responsible Entity	The Responsible Entity	The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations			included a visitor control program that requires logging of each of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or	included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1) OR The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)	has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)		retain visitor logs for at least ninety days. (2.3)
R3	**Long Term Planning**	**Lower**	The Responsible Entity has documented and	The Responsible Entity has documented and	The Responsible Entity has documented and	The Responsible Entity has not documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						months. (3.1)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible,	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* and has identified deficiencies but did not assess or correct the deficiencies. (R1) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* but did not identify, assess, or correct the deficiencies. (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				unnecessary physical input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)	had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)	
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified and	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity did not implement or document one or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)	deficiencies. (2.1) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65	more process(es) that included the applicable items in *CIP-007-5 Table R2* but did not identify, assess, or correct the deficiencies. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the	released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the	calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources identified but did not identify, assess, or	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or	correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the	CIP Senior Manager or delegate and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4) OR The Responsible Entity documented a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or	deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or correct the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)		deficiencies. (2.4)
R3	**Same Day Operations**	**Medium**		The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and has identified deficiencies but did not assess or correct the deficiencies. (3.3) OR The Responsible Entity	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.2) OR The Responsible Entity	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R3* and has identified deficiencies but did not assess or correct the deficiencies. (R3) OR The Responsible Entity did not implement or document one or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)	has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and did not identify, assess, or correct the deficiencies. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and has identified deficiencies but did	more process(es) that included the applicable items in *CIP-007-5 Table R3* and did not identify, assess, or correct the deficiencies. (R3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.1) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					not assess or correct the deficiencies. (3.3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies. (3.3)	has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies. (3.1)
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4*

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged	an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged	by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and has identified deficiencies but did not assess or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system	and has identified deficiencies but did not assess or correct the deficiencies. (R4) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4* and did not identify, assess, or correct the deficiencies. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and has identified deficiencies but did not assess or correct	detect and log all of the required types of events described in 4.1.1 through 4.1.3 and has identified deficiencies but did not assess or correct the deficiencies. (4.1) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct the deficiencies. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and has	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and has	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and has identified deficiencies but did not assess or correct	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and has identified deficiencies but did not assess or correct the deficiencies. (R5) OR The Responsible Entity did not implement or document one or more process(es) that included the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not identify, assess, or correct the	identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and did not identify, assess, or correct the	the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System	applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and has identified deficiencies but did not assess or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies. (5.6)	deficiencies. (5.6)	Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and has identified deficiencies but did not assess or correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3)	process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and did not identify, assess, or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords and has identified deficiencies but did not assess or correct the deficiencies. (5.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only	OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within	procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					17 calendar months but less than or equal to 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal	deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					to 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and has identified deficiencies but did not assess or correct the deficiencies. (5.7) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Security Incident response plan, but did not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Cyber Security Incident occurs. (2.2)	
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities,	response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				or • Cyber Security Incident response groups or individuals, or • Technology changes.	or individuals, or • Technology changes.	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Planning Real-time Operations	Lower	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests,	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Part 2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1)	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or	OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				• Responders, or • Technology changes.	responsibilities, or • Responders, or Technology changes.	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline	identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to determine required	correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline	management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the verification documentation. (1.4.3)	security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the	configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s)	OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				existing baseline configuration but did not identify, assess, or correct the deficiencies in the determination of affected security controls. (1.4.1)	that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to verify that required	process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2) OR The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did	not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					not identify, assess, or correct the deficiencies in the required controls. (1.4.2) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process for testing changes in an	the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and identified deficiencies but did not assess or correct the	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficiencies. (1.5.2) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)	
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						calendar days. (2.1) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days and identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						to the baseline at least once every 35 calendar days but did not identify, assess, or correct the deficiencies. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems. (3.1)	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A		The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented a BES Cyber System Information protection program which	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					includes one or more procedures for protection and secure handling BES Cyber System Information but did not identify, assess, or correct the deficiencies. (1.2)	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

Project 2008-06 - Cyber Security Order No. 706 - V5

~~Working Draft (September 11, 2012) of~~ Consolidated VSLs from all standards October 26, 2012

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	High	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES Cyber Systems have	fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible	fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of	considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been	Entities with a total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been	100 or fewer high or medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR	not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identified.	identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber Systems have not been identified.	For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	not been identified.
R2	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (R2.2)	The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (R2.2)	The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (R2.2)	approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			review in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1)	months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did	within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar	documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar months of the previous approval. (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				complete this approval in less than or equal to 17 calendar months of the previous approval. (R1)	months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	
R2	**Operations Planning**	**Lower**	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible	The Responsible Entity did not document or implement any cyber security policies for assets with a low impact rating that address the topics as required by R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2)	Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this	Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager ~~or delegate~~ according to Requirement R2 within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager ~~or delegate~~ according to Requirement R2 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager ~~or delegate~~ according to Requirement R2 within 16 calendar months but did complete this approval in less than or equal to 17	review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager ~~or delegate~~ according to Requirement R2 within 17 calendar months but did complete this approval in less than or equal to 18	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar months of the previous approval. (R2)	calendar months of the previous approval. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	Senior Manager, and has Identified deficiencies but did not assess or correct the deficiencies.(R4) OR The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, but did not identify, assess, or correct the deficiencies.(R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and	OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices ~~and associated physical security practices~~ during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices ~~and associated physical security practices~~ during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices ~~and associated physical security practices~~ during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices ~~and associated physical security practices~~. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and	did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to	did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to	OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a	The Responsible Entity has a program for	The Responsible Entity has a program for	The Responsible Entity did not have all of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk	conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did	conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and	required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel	did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel	physical access for four or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and	Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and	Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and	checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized	did not identify, assess, and correct the deficiencies. (3.5)	did not identify, assess, and correct the deficiencies. (3.5)	for access authorization for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter, and did not	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2)	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identify, assess and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary, and did not identify, assess and correct	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for	access to the designated storage locations where BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies.	BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(4.4)			previous verification but for four or more BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies.	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies.	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the	(5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity	(5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity	unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies. (5.4) OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5)	has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances, and did not identify,			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			assess, and correct the deficiencies. (5.5)			

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning and Same Day Operations**	**Medium**			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-5 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						outbound access permissions and deny all other access by default. (1.3) OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has a process to log authorized physical entry ~~through~~ into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8) OR The Responsible Entity has a process to log authorized physical entry ~~through~~ into any Physical Security Perimeter with sufficient information to identify the	The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7) OR The Responsible Entity	The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies.	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity documented and implemented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual and date and time of entry but did not identify, assess, or correct the deficiencies. (1.8) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)	has a process communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)	(1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5) OR The Responsible Entity has a process to	operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					monitor for unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.6) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6) ~~OR~~ ~~The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified deficiencies~~	deficiencies, but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~but did not assess or correct the deficiencies. (1.9)~~ ~~OR~~ ~~The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct deficiencies. (1.9)~~	(1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						different controls, but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						correct the deficiencies. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter or to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						minutes to identified personnel(1.7) OR The Responsible Entity does not have a process to log authorized physical entry ~~through any~~into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Same-Day Operations**	**Medium**	N/A	The Responsible Entity included a visitor control program that requires logging of each of the initial entry and last exit dates and times of the visitor ~~on a daily basis~~, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact	The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1) OR The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				and but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)		control program to retain visitor logs for at least ninety days. (2.3)
R3	**Long Term**	**Lower**	The Responsible Entity	The Responsible Entity	The Responsible Entity	The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning		has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	has not documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						within 27 calendar months. (3.1)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible,	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* and has identified deficiencies but did not assess or correct the deficiencies. (R1) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* but did not identify, assess, or correct the deficiencies. (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				unnecessary physical input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)	had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)	
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity did not implement or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)	correct the deficiencies. (2.1) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to	OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the	document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* but did not identify, assess, or correct the deficiencies. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the	evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did	security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources	OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated	identified but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion and has identified deficiencies	obtain approval by the CIP Senior Manager or delegate and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated	but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the	documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	deficiencies. (2.3)	correct the deficiencies. (2.4)
R3	**Same Day Operations**	**Medium**		The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and has identified deficiencies but did not assess or correct the deficiencies. (3.3) OR	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of ~~identified~~ detected malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.2) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R3* and has identified deficiencies but did not assess or correct the deficiencies. (R3) OR The Responsible Entity did not implement or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of ~~identified~~ detected malicious code and did not identify, assess, or correct the deficiencies. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and has identified	document one or more process(es) that included the applicable items in *CIP-007-5 Table R3* and did not identify, assess, or correct the deficiencies. (R3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficiencies but did not assess or correct the deficiencies. (3.3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies. (3.1)
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or	Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or	events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and has identified deficiencies but did not assess or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems	*CIP-007-5 Table R4* and has identified deficiencies but did not assess or correct the deficiencies. (R4) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4* and did not identify, assess, or correct the deficiencies. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	(per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and has identified deficiencies but did	capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and has identified deficiencies but did not assess or correct the deficiencies. (4.1) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct the deficiencies. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					not assess or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					sampling of logged events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and has identified deficiencies but did not assess or correct	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and has identified deficiencies but did not assess or correct the deficiencies. (R5) OR The Responsible Entity did not implement or document one or more process(es) that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not identify, assess, or	change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and did not identify, assess, or	the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System	included the applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and has identified deficiencies but did not assess or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct the deficiencies. (5.6)	correct the deficiencies. (5.6)	Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and has identified deficiencies but did not assess or correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3)	or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and did not identify, assess, or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords and has identified deficiencies but did not assess or correct the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only	deficiencies. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within	technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and did not identify,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					17 calendar months but less than or equal to 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal	assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					to 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and has identified deficiencies but did not assess or correct the deficiencies. (5.7) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						alerts after a threshold of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Security Incident response plan, but did not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable	~~(2.1)~~ The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Cyber Security Incident occurs. (2.2)	
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities,	response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				or • Cyber Security Incident response groups or individuals, or • Technology changes.	or individuals, or • Technology changes.	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests,	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Part 2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1)	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or	OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				• Responders, or • Technology changes.	responsibilities, or • Responders, or Technology changes.	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline	identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to determine required	correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline	management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the verification documentation. (1.4.3)	security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the	configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s)	OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				existing baseline configuration but did not identify, assess, or correct the deficiencies in the determination of affected security controls. (1.4.1)	that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to verify that required	process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2) OR The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did	not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					not identify, assess, or correct the deficiencies in the required controls. (1.4.2) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process for testing changes in an	the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and identified deficiencies but did not assess or correct the	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficiencies. (1.5.2) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)	
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						calendar days. (2.1) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days and identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						to the baseline at least once every 35 calendar days but did not identify, assess, or correct the deficiencies. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems. (3.1)	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A		The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented a BES Cyber System Information protection program which	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					includes one or more procedures for protection and secure handling BES Cyber System Information but did not identify, assess, or correct the deficiencies. (1.2)	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal.~~disposal or reuse processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~Asset as specified in R 2.~~ (R2~~.1~~)

Project 2008-06 - Cyber Security Order 706 - Version 5

Mapping Document Showing Translation of CIP-002-4 to CIP-009-4 into CIP-002-5 to CIP-009-5, CIP-010-1, and CIP-011-1.

Standard: CIP-002-4 – Cyber Security—Critical Asset Identification		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-002-4 R1.	CIP-002-5 R1.1	Critical Asset Identification – Instead of identifying Critical Assets as in previous versions, the Responsible Entity must Identify Facilities, systems, or equipment that meet the criteria specified in CIP-002-5, Attachment 1.
CIP-002-4 R2.	CIP-002-5 R1.2, R1.3	Critical Cyber Asset Identification – Using the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 Impact Rating Criteria, the Responsible Entity must identify and categorize its BES Cyber Systems as high impact or medium impact. BES Cyber Systems not identified as high impact or medium impact default to low impact. New standard identifies BES Cyber Systems as a grouping of BES Cyber Assets because it allows entities to apply some requirements at a system rather than asset level.

Standard: CIP-002-4 – Cyber Security—Critical Asset Identification		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-002-4 R2.	DELETED	Routable protocol exemption – A complete exemption of Cyber Assets based on communication characteristics no longer applies. This is because the vulnerability some security requirements address is not mitigated by the lack of routable protocols (e.g., training, response, recovery, etc.) Where the lack of routable protocols itself meets the requirement objective, the exemption is applied at the requirement level.
CIP-002-4 R3.	CIP-002-5 R2, R2.1, R2.2	Annual Approval – R2.1 states that the review must be at least once every 15 calendar months. However, the CIP Sr. Manager now approves identifications required in CIP-002-5 R1 as noted above.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R1.	CIP-003-5 R1, 1.1 through 1.9	Cyber Security Policy – Includes high impact and medium impact BES Cyber Systems. A separate requirement applies to low impact BES Cyber Systems. Clarified that the cyber security policy needs to only reference the subject matter topics at a high level rather than each individual requirement in the CIP Cyber Security Standards.
CIP-003-4 R1.1.	CIP-003-5 R 1.9	Provision for emergency situations – Identified the specific exceptional circumstances in which emergency exceptions can be taken in response to the directive in FERC Order No. 706, Paragraph 443.
NEW	CIP-003-5 R2	Cyber Security Policy for BES Cyber Systems not identified as high or medium impact (low impact). Clarified programmatic controls that apply to low impact BES Cyber Systems and that discrete identification of such systems is not required. Added that the CIP Senior Manager approve the policies at least once every 15 calendar months.
CIP-003-4 R1.2.	DELETED	The Cyber Security Policy is readily available –This was in response to general confusion around the term “readily available.” Training requirements in CIP-004-5 provide for knowledge of policy.
CIP-003-4 R1.3.	CIP-003-5 R1	The review and approval by the CIP Senior Manager at least once every 15 calendar months language has been added to R1.
CIP-003-4 R2.	CIP-003-5 R3	Single senior manager – Created a definition of CIP Senior Manager to facilitate references across standards.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R2.1.	CIP-003-5 R3	The CIP Senior Manager shall be identified by name, title, and date of designation – The CIP Senior Manager only needs to be identified by name. The other details were considered unnecessary, administrative requirements.
CIP-003-4 R2.2.	CIP-003-5 R3	Changes to the CIP Senior Manager and any delegations must be documented within 30 calendar days of the change.
CIP-003-4 R2.3.	CIP-003-5 R4	Delegate authority – Made clear that where allowed by the standards, the CIP Senior Manager may delegate authority and such delegations must be documented. Added that the Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a process to delegate actions, unless no delegations are used.
CIP-003-4 R2.4.	DELETED	Authorize and document any exception – The FERC Order No. 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the standards.
CIP-003-4 R3.	DELETED	Exceptions – The FERC Order No. 706 made clear that you could not take exceptions to areas of your Cyber Security Policy that were also required as part of other NERC CIP requirements. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the standards.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R3.1.	DELETED	Exceptions - Requirement R3 is deleted.
CIP-003-4 R3.2.	DELETED	Exceptions - Requirement R3 is deleted.
CIP-003-4 R3.3.	DELETED	Exceptions - Requirement R3 is deleted.
CIP-003-4 R4.	CIP-011-1 R1, 1.1, 1.2	Information Protection - Removed language to "protect" information, and replaced with requirements for methods to identify BES Cyber System Information and procedures for handling BES Cyber System Information, including storage, transit, and use to clarify the protection that is required. Added language that the entity implements its information protection programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-003-4 R4.1.	Definition	Identification – Replaced this requirement with the defined term BES Cyber System Information.
CIP-003-4 R4.2.	CIP-011-5 R1.1	Classification – Removed the explicit requirement for classification, as there was no requirement to have multiple levels of protection. This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.
CIP-003-4 R4.3.	CIP-011-5 R1.3	Assessment – No significant changes.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R5.	CIP-004-5 R4.4	Authorize personnel for access to protected information – Clarified: "Program for managing access" included the authorization of access, as well as handling and access control procedures. Grouped requirements for electronic access, physical access, and access to BES Cyber System Information in CIP 004-5 R4. Added language that the entity implements its documented access management programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-003-4 R5.1.	CIP-004-5 R4.1	Authorizing personnel.
CIP-003-4 R5.1.1.	CIP-004-5 R4.1	Have a process to authorize, which could include identifying specific personnel to authorize access.
CIP-003-4 R5.1.2.	CIP-004-5 R4.3, R4.4	Verification.
CIP-003-4 R5.2.	CIP-004-5 R4.3, R4.4	Verify access privileges – Moved requirement to ensure consistency among access reviews. Clarified precise meaning in the term "annual". Clarified what was necessary in performing verification by stating the objective was to confirm access privileges are correct and the minimum necessary for performing assigned work functions.
CIP-003-4 R5.3.	CIP-004-5 R4.3, R4.4	Annual Review – No significant changes.

Standard: CIP-003-4 – Cyber Security—Security Management Controls		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-003-4 R6.	CIP-010-1 R1, R2	Change Control and Configuration Management – Moved configuration change management to a separate standard because of the additional requirements necessary for satisfying FERC directives, and the subject matter in CIP version 4 is spread across CIP-003-4 and CIP-007-4. The baseline requirement is incorporated from the *DHS Catalog for Control Systems Security*. The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed. Added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-4 R6. Added language that the entity implements its documented processes in a manner that identifies, assesses, and corrects deficiencies.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R1.	CIP-004-5 R1, 1.1	Security awareness program and quarterly reinforcement - Changed to remove the need to ensure everyone with authorized access receive this material, and moved example mechanisms to guidance.
CIP-004-4 R2.	CIP-004-5 R2	Training - Addition of identifying the training content. Adding content for the visitor control program and storage as part of the handling of BES Cyber Systems information. Also added the FERC Order No. 706, directed electronic interconnectivity supporting the operation and control of BES Cyber Systems. This requirement is also reorganized into the respective requirements for "program" and "implementation" of the training. Added language that the entity implements its documented programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-004-4 R2.1.	CIP-004-5 R2.2	Training prior to authorized access – No significant changes.
CIP-004-4 R2.2.	CIP-004-5 R2.1.1-2.1.9	Training subject matter – This requirement is reorganized into the respective requirements for "program" and "implementation" of the training.
CIP-004-4 R2.2.1.	CIP-004-5 R2.1	Proper use of CCAs – Changed to refer to BES Cyber Systems. Requirement now addresses cyber security issues, not the business or functional use of the BES Cyber System.
CIP-004-4 R2.2.2.	CIP-004-5 R2.1	Physical and electronic access controls training – No significant changes. Refers to BES Cyber Systems.
CIP-004-4 R2.2.3.	CIP-004-5 R2.1	Information handling training – Core training added for the handling of BES Cyber System Information, with the addition of storage media.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R2.2.4.	CIP-004-5 R2.1, R2.1.1-R2.1.9	Incident identification and notification, incident handling and CCA recovery training – Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for individuals having a role in the recovery to address FERC Order No. 706, Paragraph 413.
CIP-004-4 R2.3.	CIP-004-5 R2.3	Annual training – Replaced "Annually" with "at least once every 15 calendar months."
CIP-004-4 R3.	CIP-004-5 R3	Personnel Risk Assessment –. Added language that the entity implements its documented programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-004-4 R3.1.	CIP-004-5 R3.1, 3.2.1, 3.2.2	Identification and 7-year criminal check – Addressed interpretation request in guidance. Specified that identity verification is only required for each individual's initial assessment. Specified that the 7-year criminal history check covers all locations where the individual has resided, been employed, and/or attended school for 6 consecutive months or more, including current residence, regardless of duration. Added additional wording based on interpretation request. Provision is made for when a full 7-year check cannot be performed.
CIP-004-4 R3.2.	CIP-004-5 R3.5	Perform the PRA every 7 years– Removed the "for cause" part of the requirement.
CIP-004-4 R3.3.	CIP-004-5 R3.4	Addresses the contractor or vendor performed PRA.
NEW	CIP-004-5 R3.3	Process to evaluate criminal history records checks for authorizing access.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-004-4 R4.	CIP-004-5 R4.1, 4.3	Authorize access - CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need-to-know" basis, or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.
CIP-004-4 R4.1.	CIP-004-5 R4.2	Quarterly review of access – Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4 R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.
CIP-004-4 R4.2.	CIP-004-5 R5	Prevent further access - The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the standards to require immediate revocation for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination, instead of within 24 hours. For transfers, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53, Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.
NEW	CIP-004-5 R2.1	Added to help facilitate understanding what roles the entity has to support the role-based training program.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-004-5 R2.1.4	Visitor control program training – Personnel administering the visitor control program and/or providing escort should be part of the core training per FERC Order No. 706, Paragraph 432.
NEW	CIP-004-5 R3.3	PRA failure criteria – Requires process or criteria to evaluate personnel risk assessments to determine when to deny authorized access.
NEW	CIP-004-5 R5.2	Transfers – The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53, Version 3, to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.

Standard: CIP-004-4 – Cyber Security—Personnel & Training		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-004-5 R5.4	Completion of revocation – The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the standards to require immediate revocation for any person no longer needing access. In order to meet the immediate time frame, entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
NEW	CIP-004-5 R5.5	Completion of revocation (shared accounts) – To provide clarification of expected actions in managing the passwords

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R1.	CIP-005-5 R1.1	Electronic Security Perimeter identification – Changes include referencing the defined terms Electronic Access Point and BES Cyber System.
CIP-005-4a R1.1.	Definition	Access Points – This was moved to the definition of Electronic Access Points.
CIP-005-4a R1.2.	Guidance	Dial-up accessible CCA – This is a clarifying statement that was moved to Guidance.
CIP-005-4a R1.3.	Guidance	Communication links between ESPs – This is a clarifying statement that was moved to Guidance.
CIP-005-4a R1.4.	Applicability	Applicability for Non-Critical Cyber Asset – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.5.	Applicability	Access control and monitoring Cyber Assets – To remove any cross referencing, these Cyber Assets are now included in the Applicability column for each cyber security requirement.
CIP-005-4a R1.6.	Measures	Maintain Documentation – This is a measure for the requirement to have ESP documentation.
CIP-005-4a R2.	CIP-005-5 R1	Electronic Access Controls – No significant changes.
CIP-005-4a R2.1.	CIP-005-5 R1.2, 1.3	Deny access by default - Changes include referring to the defined term Electronic Access Point, and to focus on the entity knowing and having justification for what it allows through the EAP. R1.3 explicitly states the network admission control includes both inbound and outbound connections.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R2.2.	CIP-007-5 R1.1, 1.2	Enable specific ports/services – Consolidated port hardening requirements to CIP-007.
CIP-005-4a R2.3.	CIP-005-5 R1.4	Secure dial-up – Changed to refer to the defined term Electronic Access Point. Added clarification as to the goal of "secure," which is that the BES Cyber System should not be directly accessible with a phone number only.
CIP-005-4a R2.4.	CIP-005-5 R2,2.3	Strong access control – Added a new requirement for remote access in response to increased vulnerabilities in VPN technology. This requirement also clarified strong access control meant multi-factor (or more) authentication.
CIP-005-4a R2.5.	Measures	Example of evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.1.	CIP-004-5 R4	The processes for access request and authorization – Consolidated with other similar requirements to CIP-004-5 R4.
CIP-005-4a R2.5.2.	Measures	The authentication methods – Example of evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.3.	Measures	The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4. Example of evidence requirements are considered as part of the measure.
CIP-005-4a R2.5.4.	Measures	The controls used to secure dial-up accessible connections. Example of evidence requirements are considered as part of the measure.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R2.6.	DELETED	Appropriate Use Banner – The drafting team considered this requirement administrative. The objective of having an appropriate use banner is to prevent accidental use of the system and help allow prosecution of unauthorized individuals accessing the system. The drafting team did not consider either of these rising to the level of meeting a reliability objective.
CIP-005-4a R3.	CIP-007-5 R4, 4.1	Monitoring Electronic Access – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the standards.
CIP-005-4a R3.1.	CIP-007-5 R4, 4.1	Dial-up Accessible – Removed specific references to dial-up devices. Incorporated into logging/monitoring requirements. The drafting team did not feel further referencing this technology was necessary.
CIP-005-4a R3.2.	CIP-007-5, R4, 4.2	Alerts – Consolidated monitoring requirements to CIP-007-5 R4 to ensure consistent language across all monitoring requirements in the standards.
CIP-005-4a R4.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements.
CIP-005-4a R4.1.	Measures	A document identifying the vulnerability assessment process – Example of evidence requirements are considered as part of the measure.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R4.2.	CIP-010-1 R3.1, 3.2	A review to verify that only ports and services required for operations at these access points are enabled - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to Guidance.
CIP-005-4a R4.3.	CIP-010-1 R3.1, 3.2	The discovery of all access points to the Electronic Security Perimeter - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to Guidance.
CIP-005-4a R4.4.	CIP-010-1 R3.1, 3.2	A review of controls for default accounts, passwords, and network management community strings - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to Guidance.
CIP-005-4a R4.5.	CIP-010-1 R3.4	Mitigation plan - Consolidated vulnerability assessment requirements to CIP-010-1 R3 to ensure consistent language across all vulnerability assessment requirements. Added element to have an entity defined date of completion of the mitigation plan per FERC Order No. 706, Paragraph 643.

Standard: CIP-005-4a – Cyber Security—Electronic Security Perimeter(s)		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-005-4a R5.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.1.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.2.	DELETED	The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-005-4a R5.3.	CIP-007-5 R4.4	Retain relevant log information – Log retention requirements are consolidated to CIP-007-5 R4.
NEW	CIP-005-5 R1.5	Inspect and detect potential malicious communications – Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The order makes clear this is not simple redundancy of firewalls; thus the drafting team has decided to add the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs.
NEW	CIP-005-5 R2.1,2.2	Remote Access: intermediate device and encryption – This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R1.	CIP-006-5 R1	Physical Security Plan – Removed the requirement for senior management approval of the physical security plan because there is already approval of the physical security policy and delegation of the task in complying for this program. Additional approval is not considered necessary to meeting the reliability objective of physical security for the BES Cyber System.
CIP-006-4c R1.1.	CIP-006-5 R1.2, 1.3	Physical Security Perimeter – For high impact BES Cyber Systems clarified that two or more different physical access controls (this does not require two completely independent physical access control systems) must be used to collectively allow unescorted physical access into Physical Security Perimeters.
CIP-006-4c R1.2.	DELETED	No longer requires identification of all physical access points.
CIP-006-4c R1.3.	CIP-006-5 R1.4, 1.5	Monitor physical access – A documented plan is required as part of CIP-006-5 R1 that references the new alerting term in Table Row 1.5. Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.
CIP-006-4c R1.4.	CIP-004-5 R2.3	Appropriate use of access controls – The term “appropriate” used in prior versions is subject to a high degree of subjectivity. The training requirement specifies role-based training on physical access controls.
CIP-006-4c R1.5.	CIP-004-5 R4 and R5	Review of access authorization requests and revocation of access authorization requirements were consolidated to CIP-004-5.
CIP-006-4c R1.6.	CIP-006-5 R2	Visitor control program - A documented program is required as part of CIP-006-5 R2. Otherwise, no significant change.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R1.6.1.	CIP-006-5 R2.2	Log entry and exit of visitors - Addressed multi entry requirements and added the point of contact of who can be considered the sponsor for the person to enter the DPB. There is no need to document the escort or handoffs between escorts.
CIP-006-4c R1.6.2.	CIP-006-5 R2.1	Continuous escorted access of visitors – No significant change.
CIP-006-4c R1.7.	DELETED	Update of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R1.8.	DELETED	Annual review of the physical security plan - The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
CIP-006-4c R2.	Applicability	Protection of Physical Access Control Systems – Applicability to Physical Access Control and Monitoring Systems were moved to the Applicability section of each security requirement, and added this as a defined term in the glossary.
CIP-006-4c R2.1.	Applicability, CIP-006-5 R1.1	Physical Access Control Systems be protected from unauthorized physical access - Applicability to Physical Access Control Systems were moved to the Applicability section of each security requirement. For this particular requirement, see CIP-006-5, Item 1.1, which applies to Physical Access Control Systems.
CIP-006-4c R2.2.	CIP-006-5 R1.6, 1.7	Protection of Physical Access Control Systems - Applicability to Physical Access Control Systems were moved to the Applicability section of each security requirement throughout CP version 5.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R3.	Applicability	Protection of Electronic Access Control Systems - Applicability to what protections Electronic Access Control and Monitoring Systems need were moved to the Applicability section of each security requirement.
CIP-006-4c R4.	CIP-006-5 R1.2, 1.3	Physical Access Controls – R1.3 addresses FERC Order No. 706 Paragraph 572 related directives for physical security defense in depth by providing the examples in the guidance document of physical security defense in depth via multifactor authentication or layered Physical Security Perimeter(s).
CIP-006-4c R5.	CIP-006-5 R1.4, 1.5, 1.6, 1.7	Monitor physical access – Changed the term to alert for unauthorized access and clarified the actions taken for review of unauthorized physical access alerts. Examples of methods to implement have been moved to the Guidance section of this requirement.
CIP-006-4c R6.	CIP-006-5 R1.8,	Log physical access – CIP-006-4 R6 was specific to the logging of access at identified access points. This now more generally requires logging of physical access into the defined physical boundary. Examples of methods to implement have been moved to the Guidance section of this requirement.
CIP-006-4c R7.	CIP-006-5 R1.9 and CIP-008-5 Evidence Retention	Access log retention - Retain relevant incident related log information is addressed in CIP-008-5.
CIP-006-4c R8.	CIP-006-5 R3	Maintenance and Testing.

Standard: CIP-006-4c – Cyber Security—Physical Security of Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-006-4c R8.1.	CIP-006-5 R3.1	Physical access control system three-year testing and maintenance – Shortened periodicity of testing to 24 calendar months to address FERC Order No. 706, Paragraph 581 directives. Added testing of locally mounted security hardware devices.
CIP-006-4c R8.2.	REMOVED	Testing and maintenance records are considered the measurement of Item 3.1.
CIP-006-4c R8.3.	REMOVED	Removed. With the addition of the "identify, assess, and correct deficiencies" language in CIP-006-5, Requirement R1, this requirement part is no longer necessary.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R1.	CIP-010-1 R1.4	Assess security controls following changes - Provides clarity on when testing must occur, and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.
CIP-007-4 R1.1.	CIP-010-1 R1.5	Test procedures – This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.
CIP-007-4 R1.2.	CIP-010-1 R1.5	Testing reflects production environment - This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.
CIP-007-4 R1.3.	CIP-010-1 R1.4, 1.5	The Responsible Entity shall document test results. The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R2.	CIP-007-5 R1	Ports and Services – The requirement focuses on the entity knowing, and only allowing those ports that are necessary. The additional classification of "normal" or "emergency" added no value and has been removed. Added language that the entity implements its documented programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-007-4 R2.1.	CIP-007-5 R1.1	Enable only those ports and services required for normal and emergency operations –. The requirement focuses on the entity knowing and allowing those ports necessary. The additional classification of 'normal or emergency' added no value and has been removed.
CIP-007-4 R2.2.	CIP-007-5 R1.1, 1.2	Disable other ports/services –In March 18, 2010 FERC issued an order to approve NERC"s interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.
CIP-007-4 R2.3.	DELETED	Compensating measures – See description and justification for CIP-007-4 R2.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R3.	CIP-007-5 R2	Security Patch Management – The existing wording, or CIP-007-4 R3, R3.1 and R3.2 was separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "Document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades." There has been confusion as to what constitutes the availability. Due to issues that may occur regarding control system vendor license and service agreements flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets. Added language that the entity implements its documented programs in a manner that identifies, assesses, and corrects deficiencies.
CIP-007-4 R3.1.	CIP-007-5 R2.2	Assess patches – Similar to the current wording, but added reference to "identification of a source or sources that the Responsible Entity tracks" to establish where the release is from. The word in previous versions: "The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades," has led to varying opinions as to what constitutes "availability" of the patches or upgrades. The addition attempts to clarify where the release is from. There was a change made that reads "since the last evaluation at least once every 35 calendar days".

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R3.2.	CIP-007-5 R2.3, 2.4	Implement patches - This is the same concept as in the current CIP-007 R3.2 wording; however, a 35 calendar day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used. Splitting the implementation of security related patches, hot fixes, and/or updates into a separate item from compensating measures will provide granularity. Automated processes allow the implementation to be documented and confirmed electronically in a short time period. Manual processes may take an extended period of time to complete documentation of the installation. Priority should be given to the implementation rather than the documentation.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R4.	CIP-007-5 R3, 3.1, 3.2, 3.3	Malicious Software Prevention – In prior versions, this requirement has arguably been the single greatest generator of TFE's as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets of these standards expands to more field assets, this issue will only grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method, nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a Responsible Entity does this should be detailed in its Cyber Security Policy so that it can be audited for compliance…" In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level, and regardless of technology, along with the enhanced change management requirements, meets this directive.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R4.1.	CIP-007-5 R3.1	Malware prevention tools – See description and justification for CIP-007-4 R3.
CIP-007-4 R4.2.	CIP-007-5 R3.2, 3.3	Update malicious code detections – See description and justification for CIP-007-4 R3.
CIP-007-4 R5.	CIP-007-5 R5.1	Use at least one authentication method – The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase, "that minimize the risk of unauthorized access," was removed and more appropriately captured in the Rationale Statement.
CIP-007-4 R5.1.	CIP-004-5 R4.1,	Access authorization – CIP-003-4, CIP-004-4 CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need-to-know" basis, or with respect to work functions performed. These were consolidated in CIP-004-5 R4.1 to ensure consistency in the requirement language.
CIP-007-4 R5.1.1.	CIP-003-5 R5.2	Access authorization – CIP-003-5 R5.2 requires CIP Senior Manager or delegate approval for all requirements for authorization in the CIP Cyber Security Standards.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R5.1.2.	CIP-007-5 R4.1	Identify security events for after-the-fact investigation – This requirement is derived from NIST 800-53, Version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the phrase, "system events related to cyber security," from informal comments received. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP, as required in CIP-005-4 R3, and user access and activity logs, as required in CIP-007-5 R5, are also included here.
CIP-007-4 R5.1.3.	CIP-004-5 R4.3	Account privilege verification – Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary for performing assigned work functions. Stated that the account privilege verification be conducted at least once every 15 calendar months.
CIP-007-4 R5.2.	CIP-007-5 R5.2	Identify account types and determine acceptable use – CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure, at best.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R5.2.1.	CIP-007-5 R5.4	Change default vendor passwords – The requirement for the "removal, disabling, or renaming of such accounts where possible," has been removed and incorporated into Guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded, uniquely generated default password was manufactured with the BES Cyber System.
CIP-007-4 R5.2.2.	CIP-007-5 R5.3	Identify those individuals with access to shared accounts - No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.
CIP-007-4 R5.2.3.	CIP-007-5 R5.2, 5.3	Identify account types and determine acceptable use – No significant changes.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R5.3.	CIP-007-5 R5.5	Implement a password policy – CIP-007-4 R5.3 requires the use of passwords, and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials, while recognizing password parameters alone do not achieve this. The drafting team believes allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.
CIP-007-4 R5.3.1.	CIP-007-5 R5.5	Password length – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.2.	CIP-007-5 R5.5	Password complexity – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R5.3.3.	CIP-007-5 R5.5, 5.6	Password change frequency – See description and justification for CIP-007-4 R5.3.
CIP-007-4 R6.	CIP-007-5 R4	Security Status Monitoring – Consolidated requirements for monitoring electronic events into CIP-007-5 R4.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R6.1.	CIP-007-5 R4.1	Identify security events – This requirement is derived from NIST 800-53, Version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the phrase, "system events related to cyber security" from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. Access logs from the ESP, as required in CIP-005-4 R3, and user access and activity logs, as required in CIP-007-5 R5, are also included here.
CIP-007-4 R6.2.	CIP-007-5 R4.2	Identify security events for Real-time alerting – This requirement is derived from alerting requirements in CIP-005-4 R3.2 and CIP-007-4 R6.2, in addition to NIST 800-53, Version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate an immediate response.
CIP-007-4 R6.3.	CIP-007-5 R4.1	Identify security events for after-the-fact investigation – See description and justification for CIP-007-4 R6.1.
CIP-007-4 R6.4.	CIP-007-5 R4.4	Retain relevant log information – No significant changes.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R6.5.	CIP-007-5 R4.5	Review logs – Beginning in Paragraph 525, and also Paragraph 628 of the FERC Order No. 706, the commission directs a manual review of security event logs on a more periodic basis, and suggests a weekly review. The order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for a weekly summary or sampling review of logs.
CIP-007-4 R7.	CIP-011-1 R2.1	Disposal or Redeployment – Consistent with FERC Order No. 706, Paragraph 631, clarified that the goal was to prevent the unauthorized retrieval of information from the asset, removing the word “erase” as, depending on the media itself, erasure may not be sufficient to meet this goal. Moved requirement explicitly requiring records of destruction/redeployment to a measure of compliance. Added requirement for chain of custody if the device is taken outside the Physical Security Perimeter.
CIP-007-4 R7.1.	CIP-011-1 R2.2	Disposal - Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the asset, removing the word “erase” since, depending on the media itself, erasure may not be sufficient to meet this goal. Moved requirement explicitly requiring records of destruction/redeployment, to a measure of compliance. Added requirement for chain of custody if the device is taken outside the Physical Security Perimeter.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-007-4 R7.2.	CIP-011-1 R2.1	Redeployment – See description and justification for CIP-007-4 R7.
CIP-007-4 R7.3.	Measures	See description and justification for CIP-007-4 R7.
CIP-007-4 R8.	CIP-010-1 R3	Cyber Vulnerability Assessment – Consolidated requirements for vulnerability assessments from CIP-005-4 and CIP-007-4.
CIP-007-4 R8.1.	Measures	A document identifying the vulnerability assessment process – This is example evidence required for compliance.
CIP-007-4 R8.2.	CIP-010-1 R3.1, 3.2	Ports and services review – As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are included in Guidance.
CIP-007-4 R8.3.	CIP-010-1 R3.1, 3.2	A review of controls for default accounts – As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are included in Guidance.
CIP-007-4 R8.4.	CIP-010-1 R3.4	Mitigation plan – Added a requirement for an entity planned date of completion as per the FERC directive in Order No. 706, Paragraph 643.
CIP-007-4 R9.	DELETED	Documentation Review and Maintenance – The drafting team considered this requirement fully administrative and as part of the internal program to maintain compliance evidence.
NEW	CIP-007-5 R1.2	Restrict physical I/O ports – In March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g., TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

Standard: CIP-007-4 – Cyber Security—Systems Security Management		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-007-5 R2.1	Identify patch sources – Defining the source(s) that a Responsible Entity monitors for the release of security related patches, hot fixes, and/or updates will provide a starting point for assessing the effectiveness of the patch management process. Documenting the source is also used to determine when the assessment time frame clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.
NEW	CIP-007-5 R4.3	Generate Real-time alerts and respond to audit-processing failures – This requirement was derived from NIST 800-53, Version 3 AU-5, which addresses response to audit processing failures. Some interpretations of version 4 CIP Cyber Security Standards considered the failure of the security event monitoring and alerting system to be a violation. The purpose of this requirement is to have mitigation in place rather than penalizing audit processing failures.
NEW	CIP-007-5 R5.7	Limits or alerts on exceeding unsuccessful log in attempts threshold – Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-008-4 R1.	CIP-008-5 R1	Cyber Security Incident Response Plan – Separated requirement into multiple requirements in a comparable manner as CIP-009-4, where individual aspects of maintaining the plan are listed as separate requirements.
CIP-008-4 R1.1.	CIP-008-5 R1.1, 1.2	Identify reportable cyber security events – Defined the term Reportable Cyber Security Incident and further described the meaning in relation to CIP-008-5. "Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity. EOP-004-2 will address the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. In R1.2, language was added to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) and that notification, even if a preliminary notice, exceed one hour.
CIP-008-4 R1.2.	CIP-008-5 R1.3, R1.4	Roles and responsibilities of incident response teams –Replaced "incident response teams" with "incident response groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams. Conforming change to reference new defined term Cyber Security Incidents.
CIP-008-4 R1.3.	DELETED	Reporting cyber security incidents – Coordinated with EOP-004-2 drafting team to ensure EOP-004-2 becomes the single standard for reporting incidents, and ensure EOP-004-2 references the defined term Reportable Cyber Security Incidents.

Standard: CIP-008-4 – Cyber Security—Incident Reporting and Response Planning		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-008-4 R1.4.	CIP-008-5 R3.1.2, 3.4	Update incident response plan following review – Included additional specification on update of response plan. Addresses FERC Order No. 706, Paragraph 686 directive to modify on lessons learned. Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.
CIP-008-4 R1.5.	CIP-008-5 R3.1, R3.3	Review incident response plans annually – Specified what the annual review entails. Addresses FERC Order No. 706, Paragraph 686 to document test, or actual incidents and lessons learned.
CIP-008-4 R1.6.	CIP-008-5 R2.1, 2.2	Test incident response plans annually – Allows deviation from plan(s) during actual events or testing if deviations are recorded for review, and specifies activities required to maintain the plan. In R2.1, changed "Annually" to at least once every 15 calendars months.
CIP-008-4 R2.	CIP-008-5 R2.3	Cyber Security Incident Documentation –Removed references to the retention period because the standard addresses data retention in the Compliance section.
NEW	CIP-008-5 R3.1.1	Document any lessons learned - Addresses FERC Order No. 706, Paragraph 686 to document test or actual incidents and lessons learned.
NEW	CIP-008-5 R3.1,R3.3.1	Communicate incident response plan updates – Added specific timing requirement on communication of plan changes based on review of the DHS Controls and NIST 800-53 guideline.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
CIP-009-4 R1.	CIP-009-5 R1, R3.1, R3.3	Recovery Plan – Added requirement for documentation of any identified deficiencies or lessons learned. Added the requirement to additionally review plans after technology changes. Added requirement parts to document any lessons learned (3.3.1), update recovery plan based on documented lessons learned (3.3.2), and notify each person or group of any updates to the recovery plan (3.3.1).
CIP-009-4 R1.1.	CIP-009-5 R1.1	Conditions for activation of recovery plan – Minor wording changes, essentially unchanged.
CIP-009-4 R1.2.	CIP-009-5 R1.2	Roles and responsibilities of recovery plan responders – No significant changes.
CIP-009-4 R2.	CIP-009-5 R2, R2.1	Test recovery plan annually – Added language that the entity implements its documented programs in a manner that identifies, assesses, and corrects deficiencies. Changed “Annually” to at least once every 15 calendars months.
CIP-009-4 R3.	CIP-009-5 R3.2	Review results of recovery plan activities (tests, events) – Added the time frame for update.
CIP-009-4 R4.	CIP-009-5 R1.3	Backup processes – No significant changes.
CIP-009-4 R5.	CIP-009-5 R2.2	Test information used for recovery – Combined requirement from CIP-009-4 R5 and included requirement to test when initially stored. Addresses FERC Order No. 706, Directives 739 and 748 related to testing of backups. Changed “Annually” to at least once every 15 calendars months.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-009-5 R1.4	Testing of backup media – Addresses FERC Order No. 706, Paragraph 739 and 748 directives regarding the testing of backup media.
NEW	CIP-009-5 R1.5	Process to preserve data for analysis – Added requirement to address FERC Order No. 706, Paragraph 706, regarding the necessity to have procedures in place to retain Cyber Asset evidence as part of the recovery planning.
NEW	CIP-009-5 R2.3	Test each of the recovery plans for high impact BES Cyber Systems at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. Addresses FERC Order No. 706, Paragraph 725, to add the requirement that the recovery plan test be a full operational test once every 3 years.
NEW	CIP-009-5 R3.4	Communicate recovery plan updates – This change ensures that recovery personnel are aware of any changes to recovery plans.
Standard: New Requirements in CIP-010-1 and CIP-011-1		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-1 R1.1	Baseline configuration – Baseline requirement incorporated from the DHS Catalog for Control Systems Security (also NIST 800-53). The baseline requirement is also an attempt to clarify precisely when the change management process must be invoked and which elements of the configuration must be managed.

Standard: CIP-009-4 – Cyber Security—Recovery Plans for Critical Cyber Assets		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Description and Change Justification**
NEW	CIP-010-1 R2.1	The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes. This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397. DHS Catalog & addresses FERC Order No. 706, Paragraph 397. Thirty-five calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.
NEW	CIP-010-1 R3.2	Live Vulnerability Assessment for high impact BES Cyber Systems – Addresses FERC Order No. 706, Paragraph 541, 542, 544, and 547 directives regarding the performance of a live vulnerability assessment.
NEW	CIP-010-1 R3.3	Perform active VA on new BES Cyber Assets for high impact - Addresses FERC Order No. 706, Paragraph 541, 542, 544, and 547 directives regarding the performance of a vulnerability assessment prior to placing a new Cyber Asset into production.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-4

3. Purpose: NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its records of approvals as specified in Requirement R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 The Regional Entity shall serve as the Compliance Enforcement Authority with the following exceptions:

- For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.2. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change “Control Center” to “control center”	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-4

3. Purpose: Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-003-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-4 Requirement R2.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance	

		Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-4

3. Purpose: Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-004-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-004-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);

- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program. Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-4a

3. Purpose: Standard CIP-005-4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4a should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-005-4a, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-4a:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4a.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.1 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.1 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.2 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-4a from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Developed separately.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2	Approved by NERC Board of	Modifications to clarify the requirements and to bring the compliance elements into	Revised.

	Trustees 5/6/09	conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Changed CIP-005-2 to CIP-005-3. Changed all references to CIP Version "2" standards to CIP Version "3" standards. For Violation Severity Levels, changed, "To be developed later" to "Developed separately."	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010	Addition
4a	01/24/11	Adopted by the NERC Board of Trustees	Update to conform to changes to CIP-002-4 (Project 2008-06) Update version number from "3" to "4a"

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-4c

3. Purpose: Standard CIP-006-4 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-4c should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-006-4c, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-006-4c:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the

Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-4c for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	May 2, 2006	Adopted by NERC Board of Trustees	
1	January 18, 2008	FERC Order issued approving CIP-006-1	
	February 12, 2008	Interpretation of R1 and Additional Compliance Information Section 1.4.4 adopted by NERC Board of Trustees	Project 2007-27
2		Updated version number from -1 to -2 Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	Project 2008-06
2	May 6, 2009	Adopted by NERC Board of Trustees	
	August 5, 2009	Interpretation of R4 adopted by NERC Board of Trustees	Project 2008-15
2	September 30, 2009	FERC Order issued approving CIP-006-2	
3	November 18, 2009	Updated version number from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized. Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	Project 2009-21
3	December 16, 2009	Adopted by NERC Board of Trustees	
	February 16, 2010	Interpretation of R1 and R1.1 adopted by NERC Board of Trustees	Project 2009-13
3	March 31, 2010	FERC Order issued approving CIP-006-3	
2a/3a	July 15, 2010	FERC Order issued approving the Interpretation of R1 and R1.1. Updated version numbers from -2/-3 to -2a/-3a.	
4	January 24,	Adopted by NERC Board of Trustees	

	2011		
3c/4c	May 19, 2011	FERC Order issued approving two interpretations: 1) Interpretation of R1 and Additional Compliance Information Section 1.4.4; and 2) Interpretation of R4. Updated version number from -3/-4 to -3c/-4c.	

Appendix 1

Requirement Number and Text of Requirement
R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following: R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
Question
If a completely enclosed border cannot be created, what does the phrase, "to control physical access" require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption? Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?
Response
For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are "physical in nature." The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

Appendix 2

Interpretation of Requirement R1.1.

Request: *Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*

Interpretation:

Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border.

CIP-006-1 — Requirement 1.1 requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

CIP-006-1 — Additional Compliance Information 1.4.4 identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.

1.4. Additional Compliance Information

1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.

Appendix 3

The following interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R4 was developed by the standard drafting team assigned to Project 2008-14 (Cyber Security Violation Severity Levels) on October 23, 2008.

Request:

1. *For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*
2. *Does the term, "time of access" mean logging when the person entered the facility or does it mean logging the entry/exit time and "length" of time the person had access to the critical asset?*

Interpretation:

No, monitoring and logging of access are only required for ingress at this time. The term "time of access" refers to the time an authorized individual enters the physical security perimeter.

Requirement Number and Text of Requirement

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-4

3. Purpose: Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-007-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-4 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	

		Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-4

3. Purpose: Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-008-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-4 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated Version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-4

3. Purpose: Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-009-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-009-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

Project 2008-06 - Cyber Security Order No. 706 - V5

Working Draft (September 11, 2012) of Consideration of Issues and Directives

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 233 (Related paragraph: 25) Para 233 "The Commission continues to believe and is further persuaded by the comments that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. Moreover, we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk-Power System should be addressed in NERCs Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need	FERC Order No. 706	In its development of CIP Version 5, the Standards Drafting Team (SDT) considered many existing cyber security frameworks. Notably, the SDT included consideration of the NIST Risk Management Framework, NIST Publication 800-53, as well as the "DHS Catalog of Control Systems Security: Recommendations for Standards Developers" in the development of its requirements for cyber systems categorization and applicable requirements. Five key features of the NIST Risk Management Framework were incorporated into Version 5 of NERC CIP Standards: (1) ensuring that all BES Cyber Systems associated with the Bulk Power System, based on their function, receive some level of protection, (2) customizing protection to the mission of the cyber systems subject to protection, (3) a tiered approach to security controls which specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk Power System, (4) the concept of the BES Cyber System itself, and (5) Version 5 has incorporated the "Assess" and "Monitor" processes of the NIST Risk Management Framework in the development of the requirements and enabled these processes through additional language for identifying, assessing, and correcting deficiencies in controls.. Features 2 and 3 above are tightly coupled. In the NIST Risk Management Framework, there is a concept of tailoring and scoping which allows the organization to determine which controls are applicable to their specific environment. In the NERC compliance framework, all requirements are mandatory and enforceable, and, therefore, this concept does not translate directly. As such, the customization of protections by mission is based upon the environment that the BES Cyber System supports (control center, transmission facility, generation facility) and utilizes the tiered model and the requirement applicability to provide this customization to the individual environments that together support a

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
for new CIP Reliability Standards, or as part of an assessment of NERCs performance of its responsibilities as the ERO." Para 25 "The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework. "		combined mission of Bulk Power System reliability. The NIST Security Control Catalogue in 800-53, Revision 3 and the DHS Catalog of Controls Systems Security were also used as a reference in addressing many of the FERC directives in Order No. 706. Additionally, the SDT included members representing federal agencies and NIST, in particular, during the development of these CIP standards.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 and 249 Para 258 "Likewise, the ERO should consider Northern Californias suggestion that the ERO establish a formal feedback loop to assist the industry in developing policies and procedures." Para 249 "In contrast, FirstEnergy agrees that NERC should provide guidance to entities without a wide-area view, such as a generation owner or a partial generation owner, on how to approach a risk-based assessment. Likewise, Northern California suggests that NERC establish a process for informal, case-by-case consultations with responsible entities that need assistance in complying with CIP-002-1. In addition, as part of the re-examination of CIP-002-1, Northern California encourages the incorporation of a formalized feedback loop to assist the industry in developing policies and procedures."	FERC Order No. 706	CIP-002-5 classifies BES Cyber Systems through impact thresholds, and does not use risk-based assessments performed by individual entities. CIP-002-5, Attachment 1's bright line criteria were developed in consideration of a wide area view, and it obviates the need for a formal feedback loop or a need for a wide area view by smaller entities.
Para 258 and 252	FERC Order No. 706	Early during the development of CIP-002-5, the SDT discussed the concept of Design-Basis Threat (DBT). The SDT, in CIP-002-5, classifies BES Cyber Systems through impact

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 "As to Entergys suggestion that the ERO provide a DBT profile of potential adversaries, the ERO should consider this issue in the Reliability Standards development process." Para 252 "Entergy suggests, as an alternative approach to critical asset identification, that the ERO provide a Design-Basis Threat (DBT) a profile of the type, composition, and capabilities of an adversary that would assist the industry as a technical baseline against which to establish the proper designs, controls and processes. Entergy claims that a DBT approach would address many of the Commissions concerns regarding the risk-based methodology. For example, a DBT would focus the appropriate emphasis on the potential consequences from an outage of a critical asset. In addition, a DBT would address the Commissions concern that responsible entities will not have enough guidance in developing a risk-based methodology and not know how to identify a critical asset. Entergy contends that a DBT		thresholds, and does not use risk-based assessments performed by individual entities. The complexity and subjectivity involved in an entity's risk-based assessment, such as one based on DBT, would run counter to the CIP-002-5 objectives of categorization based on impact defined by bright-line criteria. CIP-002-5, Attachment 1's bright line criteria uses an impact-based approach as an alternative to DBT. This approach was approved by the Commission in its Order No. 761 approving Version 4 of the CIP Cyber Security Standards.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
approach would provide the industry with more certainty in implementing the CIP Reliability Standards."		
Para 272 (1 of 2) "Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, **the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset.** In doing so, the ERO should consider Juniper's comments. Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data."	FERC Order No. 706	This was completed by CIPC in the Version 3 CIP standards guidelines. The guidelines are entitled "Identifying Critical Assets" and "Identifying Critical Cyber Assets" and are available for download from www.nerc.com.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 272 (2 of 2) "Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset. In doing so, the ERO should consider Juniper's comments. **Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data."**	FERC Order No. 706	Guidance developed for CIP-002-5 addresses situational awareness and inter-utility data exchange.
Para 285 (related paragraph: 278) Para 285 "The Commission directs the ERO to consider the comment from ISA99 Team	FERC Order No. 706	The exclusion of Cyber Assets based on non-routable protocols has been removed from CIP-002-5, and added as an applicability filter for requirements where: (i) the use of non-routable protocols is a mitigating factor for the vulnerabilities a requirement addresses, or (ii) implementation of routable protocols, when not otherwise used, would be required to comply with the requirement (e.g. malware updates, security event monitoring, and alerting, etc.).

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
[ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience].” Para 278 “ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience. In contrast, Energy Producers notes that CIP-002-1 as proposed by NERC provides that a critical cyber asset must have either routable protocols or a dial-up connection. Energy Producers states that this is a useful, objective criterion which will assist in the unambiguous identification of such assets and therefore should be retained.”		

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 296 "With regard to METC-ITC's comment, the ERO should consider in its Reliability Standards development process the suggestion that the CIP Reliability Standards require oversight by a corporate officer (or the equivalent, since some entities do not have corporate officers) rather than by a "senior manager."	FERC Order No. 706	The requirement that the senior manager have "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" ensures that the senior manager is of the sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for Responsible Entities, from municipal, cooperative, federal agencies, investor-owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis. In Version 5, this is addressed in the definition of CIP Senior Manager. The SDT believes the filing for Version 2 also addressed this issue.
Para 321 " SPP and ReliabilityFirst suggest modifying CIP-002-1 to allow an entity to rely upon the assessment of another entity with interest in the matter. We believe that this is a worthwhile suggestion for the ERO to pursue and the ERO should consider this proposal in the Reliability Standards development process. We note that, even without such a provision, an entity such as a small generator operator is not foreclosed from consulting with a balancing authority or other appropriate entity with a wide-area view of the transmission system."	FERC Order No. 706	The SDT believes that this suggestion would be applicable in a model of an entity's own risk-based methodology, where certain small entities may not benefit from a wider area view. The change to "bright line" criteria for identifying BES Cyber Systems in CIP-002-5, along with refining the scope of certain requirements through applicability columns based on impact and connectivity characteristics, no longer requires entities to use a self-defined risk-based methodology, which addresses this concern.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 355 (also see paragraph 356) "The Commission believes that responsible entities would benefit from additional guidance regarding the topics and processes to address in the cyber security policy required pursuant to CIP-003-1. While commenters support the need for guidance, many are concerned about providing such guidance through a modification of the Reliability Standard. We are persuaded by these commenters. Accordingly, the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address. However, we will not dictate the form of such guidance. For example, the ERO could develop a guidance document or white paper that would be referenced in the Reliability Standard. On the other hand, if it is determined in the course of the Reliability Standards development process that specific guidance is important enough to be incorporated directly into a Requirement, this option is not foreclosed. The entities remain responsible, however, to comply with the cyber security policy pursuant to CIP-003-1."		The SDT has chosen to provide guidance to Responsible Entities through the introduction of topical areas in the requirement language that must be addressed in cyber security policies in CIP-003-5, requirements R1 and R2. Additionally, as directed, the SDT has provided guidance about these topical areas in the Guidelines and Technical Basis section of Reliability Standard CIP-003-5.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 376 "... the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards. In response to EEI, we believe that this clarification is needed because, for example, it is important that a responsible entity understand that exceptions that individually may be acceptable must not lead cumulatively to results that undermine compliance with the Requirements themselves."	FERC Order No. 706	The SDT removed the CIP-003-4 requirement to document exceptions to the Cyber Security Policy. • The SDT considers this a general management issue that is not within the scope of a compliance requirement. • The SDT found no reliability basis in this requirement. • Removal of this requirement provides clarity that the only exceptions to the requirements is through the defined Technical Feasibility Exception process, where specifically allowed.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 386 "The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly. In general, the Commission agrees with commenters and believes that access to protected information should cease as soon as possible but not later than 24 hours from the time of termination for cause."	FERC Order No. 706	To address this directive, in CIP-004-5, requirement R5, Responsible Entities must revoke access to the electronic and physical locations where it stores BES Cyber System Information. This could include records, closets, substation control houses, records management systems, file shares, or other physical and logical areas under the Responsible Entity's control. The SDT specified the revocation action to be completed "by the end of the next calendar day following the effective date and time of the termination action" to provide a more defined time threshold, following the SDT's discussion of the difficulty in defining an exact time in a termination process that typically includes multiple steps and organizations within an entity.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 397 and 398 "The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes. The Commission believes that these considerations are significant aspects of change control and configuration management that deserve express acknowledgement in the Reliability Standard. While we agree with Entergy that the NIST Security Risk Management Framework offers valuable guidance on how to deal with these matters, our concern here is that the potential problems alluded to be explicitly acknowledged. Our proposal does not speak to how these problems should be addressed. We do not believe that the changes will have burdensome consequences, but we also note that addressing any unnecessary burdens can be dealt with in the Reliability Standards development process."	FERC Order No. 706	Two new requirements in a new standard CIP-010-1 were added to address this change: CIP-010-1, requirement R1 (part 1.5), requires additional testing prior to a configuration change in a test environment; CIP-010-1, requirement R2 (part 2.1), requires monitoring of the configuration of the BES Cyber System. • The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System. • Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) prior to their implementation in the production environment to aid in identifying any accidental consequences, to required cyber security controls, of the change.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 412 "The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world."	FERC Order No. 706	The SDT addresses this through the defense in depth framework that has been designed through the full suite of revised CIP Standards. The standards address defense in depth through personnel management, systems management, and information management. The Standards are written in the perspective that the Responsible Entity is required to protect its cyber systems from internal and external threat. The requirements include both preventive and detective controls. The requirements mandate appropriate vetting of personnel to minimize the risk of internal threat. They then build upon this through secure system design for internal use and remote access. These controls are further enhanced by the requirement of robust monitoring and alerting activities. Specific requirements in the identification and protection of physical and electronic security perimeters assume a default posture of "deny-by-default" to reinforce the posture of mutual distrust.
Para 433 ". . . we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard."	FERC Order No. 706	The SDT addressed this by determining that identification of certain core training elements would be beneficial, and the identification of those core training elements that must be provided in the training program should be role based, as required in CIP-004-5, requirement R2.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 434 "The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets."	FERC Order No. 706	The SDT added this as a topic for role-specific training in CIP-004-5, requirement R2 (part 2.1). Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems.
Para 435 "Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves."	FERC Order No. 706	The SDT has considered the issue and has determined that no modifications are necessary. In practice, this training is often conducted as computer-based training (CBT), and the training is aimed at an entity's own policies. The SDT believes that assessments of the adequacy of the training during the compliance monitoring process implicitly evaluate the adequate training of the trainers or the efficacy of the training method.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 446 (1 of 2) (Review the referenced Comments) " APPA/LPPC seek **clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees.** SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees. The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."	FERC Order No. 706	The SDT clarifies the discretion in reviewing personnel risk assessments in CIP-004-5, requirement R3, by requiring the Responsible Entity to establish and document criteria for personnel risk assessments. The requirements in CIP-004-5 also provide additional detail about what type of records (whether criminal, work history, domicile, etc) a Responsible Entity must examine.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 446 (2 of 2) (Review the Referenced Comments) "APPA/LPPC seek clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees. **SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees.** The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."	FERC Order No. 706	In CIP-004-5, requirement R3, the SDT has specified that the seven-year criminal history records check must include current residence, regardless of duration, and include other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 460 "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."	FERC Order No. 706	In CIP-004-5, requirement R5, the SDT has addressed this directive by requiring initiation of the revocation of physical and interactive remote access, to be completed within 24 hours of termination, concurrent with the termination or disciplinary action (Part 5.1), or by the end of the calendar day in cases of transfers or reassignments (Part 5.2) for access that the Responsible Entity determines is no longer needed.. CIP-004-5, requirement R5 (part 5.4) augments the requirements in parts 5.1 and 5.2 that respond to the directive. In order to meet the immediate time frame, Entities will likely have initial revocation procedures to prevent physical and interactive remote access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. Part 5.4 requires the Responsible Entity to complete the revocation process within the time specified (30 days). Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
Para 464 "We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification."	FERC Order No. 706	The SDT notes that it addresses this issue in previous versions of the CIP standards. Version 2 added the requirement for a personnel risk assessment prior to being granted access, and Version 3 required implementation of a visitor control program. The changes made to the requirements in Version 5 maintain and improve upon these requirements. CIP-004-5, requirement R4 makes clear that individuals not properly authorized for unescorted physical access will not have such access. CIP-006-5 restricts access through implementation of a visitor management program.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 473 "The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entitys obligations regarding vendors with access to critical cyber assets."	FERC Order No. 706	CIP-002-5, requirement R1 makes clear that asset owners are responsible for complying with the standards.
Para 476 "We direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent with the Commissions determinations above."	FERC Order No. 706	Guidance in CIP-002-5 states that the owning Responsible Entity is responsible for complying with the CIP Cyber Security Standards. Furthermore, the guidelines and technical basis for CIP-002-5 states that where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 496 (Related: Para 503) Para 496 "The Commission adopts the CIP NOPRs proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter" Para 503 "The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures."	FERC Order No. 706	The drafting team addresses this in CIP-005-5, requirement R1 (part 1.5). Per FERC Order No. 706, Paragraphs 496 through 503, Electronic Security Perimeters (ESP) need two distinct security measures, such that the cyber assets do not lose all perimeter protection if one measure fails or is misconfigured, in a defense-in-depth approach. The Order makes clear that this is not simple redundancy of firewalls; thus, the drafting team added the security requirement of malicious traffic inspection (IDS/IPS) as a second security control for electronic access points for High Impact BES Cyber Systems.
Para 502 "The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process."	FERC Order No. 706	The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security requirement of malicious traffic inspection (IDS/IPS) as a second security control for electronic access points for High Impact BES Cyber Systems.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 504 (Related: Para 495) Para 504 "The ERO should consider in the Reliability Standards development process Northern Indiana's and Xcel's concerns regarding the phrase "single access point at the dial up device." Para 495 "Northern Indiana and Xcel ask the Commission to clarify or direct the ERO to clarify the phrase "single access point at the dial up device" in CIP-005-1, Requirement R1.2. Xcel asks whether this refers to the initiating device, the device at the point of termination, or both. Northern Indiana would not modify CIP-005-1, but urges that any modifications to Requirement R2 should allow continued reliance on legacy systems."	FERC Order No. 706	The SDT has deleted the troublesome language relating to "single access point at the dial up device," and the SDT has clarified that an Electronic Security Perimeter applies to routable connectivity. CIP-005-5 also separated the requirement for dial-up connectivity, specifying in CIP-005-5, R1.4, that a Responsible Entity must perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible, on its high and medium impact BES Cyber Systems with dial-up connectivity.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 511 "The Commission adopts the CIP NOPRs proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies."	FERC Order No. 706	CIP-005-5, requirement R2 has additional security requirements for remote access from the work started in the Urgent Action Revisions to CIP-005-3. One of these requirements is two-factor authentication and specific examples of two-factor authentication are provided in the guideline referenced in the rationale for this requirement.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 525 "The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily…" Para 628. "Requirement R6 of CIP-007-1 does not address the frequency with which log should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly…"	FERC Order No. 706	In CIP-007-5, requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of once every 15 days. CIP-007-5, requirement R4, combines CIP-005-4, requirement R5 and CIP-007-4, requirement R6, and addresses FERC Order No. 706's directives from a system-wide perspective. The primary feedback received on this requirement from comment periods was the vagueness of terms "security event" and "monitor." The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach to specify a minimum set of security event types to log and review, and allows the entity to define relevant security events in addition to the specified minimum. In addition, CIP-007-5, requirement R4, sets up parameters for the logging and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC Order No. 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 526 (1 of 2) ". . . the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments.	FERC Order No. 706	In CIP-007-5, requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of once every 15 days. (Also see response to paragraph 525).
Para 526 (2 of 2) "The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs."	FERC Order No. 706	CIP-007-5, requirement R4, sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. (Also see response to paragraph 525).
Para 528 "The Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs."	FERC Order No. 706	In CIP-007-5, requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of once every 15 days. In addition, CIP-007-5, requirement R4, sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC Order No. 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings. (Also see response to paragraph 525).

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 541 ". . . we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments."	FERC Order No. 706	In CIP-010-1, requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires paper assessments at least once every 15 months in the intervening years.
Para 542 ". . . the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems."	FERC Order No. 706	In CIP-010-1, requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires paper assessments at least once every 15 months in the intervening years.
Para 544 (1 of 2) "the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification."	FERC Order No. 706	The SDT addresses this paragraph in CIP-010-1, requirement R3. • The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new Cyber Asset undergo an active vulnerability assessment. • An exception is made for specified CIP Exceptional Circumstances. • Additionally, the new requirement in CIP-010-1, requirement R1 (part 1.5) requires testing of all changes for High Impact BES Cyber Systems that deviate from the baseline configuration in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) to ensure that required security controls are not adversely affected.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 544 (2 of 2) “. . . we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment”	FERC Order No. 706	The SDT has added a requirement in CIP-010-5, requirement R3 (part 3.3), to perform an active vulnerability assessment of a new Cyber Asset in High Impact BES Cyber Systems.
Para 547 ". . . we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"	FERC Order No. 706	In CIP-010-1, requirement R3, the SDT has added requirements for an “active vulnerability assessment” to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires paper assessments at least once every 15 months in the intervening years.
Para 572 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."	FERC Order No. 706	The SDT addressed this in CIP-006-5, requirement R1 (part 1.3) for High Impact BES Cyber Assets, by requiring Responsible Entities to “utilize two or more different physical access controls to collectively allow physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.”

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 581 "The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years."	FERC Order No. 706	The SDT addressed this in CIP-006-5, requirement R3 (part 3.1) by changing the frequency to a 24-month testing cycle; after deliberation and consideration, the SDT determined that a requirement of more frequent testing (e.g., 12 months), would pose unreasonable burden for Responsible Entities with a large number of physical security perimeters dispersed over large geographic areas.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 609, Sentence 5 "The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a representative system one that includes the essential equipment and adequately represents the functioning of the production system. **We therefore direct the ERO to develop requirements addressing what constitutes a representative system and to modify CIP-007-1 accordingly.** The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."	FERC Order No. 706	The SDT has introduced the concept of a “baseline configuration” around which the change control process is based. The SDT further utilizes this “baseline configuration” to provide clarity as to what is considered a representative system as it relates to performing active vulnerability assessments in CIP-010-1.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 609, Sentence 6 "The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a representative system one that includes the essential equipment and adequately represents the functioning of the production system. We therefore direct the ERO to develop requirements addressing what constitutes a representative system and to modify CIP-007-1 accordingly. **The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."**	FERC Order No. 706	The SDT has provided additional guidance on testing systems in the Guidelines and Technical Basis section of CIP-010-1. Furthermore, and in addition to guidance, the requirements of CIP-010-1 R1.5 and CIP-010-1 R3.2 identify a "representative system" as a system that exists in a test environment (or production environment where tests can be performed in a manner that minimizes adverse effects) that models the baseline configuration of the BES Cyber System in a production environment. This baseline configuration concept is developed by entities in CIP-010-1 R1.1 and further contains details on what constitutes a "representative system."

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 610 “. . . we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above.”	FERC Order No. 706	CIP-010-1, requirements R1 (part 1.5) requires Responsible Entities to account for any additional differences between the two systems, the SDT proposes using the words similar to those directly from FERC Order No. 706, paragraph 610: “Document the differences between the test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.”

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 611 "With respect to MidAmericans proposal that the differences between the testing and production environments only be reported when the production and test environments are established, the ERO should consider this matter in the Reliability Standards development process However, the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."	FERC Order No. 706	The SDT has added a requirement for the Responsible Entity to, "document…the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments." The SDT has included this requirement for each test performed in the representative environment. The SDT appreciates the concern brought up by MidAmerican and believes that entities should be free to use the same documentation multiple times to provide compliance with this requirement so as to minimize the documentation overhead, but also believes that it is important for entities to give consideration to the configuration of their representative system each time a test is performed in order to ensure the validity of the test results.
Paras 622 (Related: See Paras 614 and 619) "Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere."	FERC Order No. 706	The "acceptance of risk" language was removed in Version 2, and it has not been used in Version 5. Malicious software prevention exceptions have been placed under the TFE process since Version 2.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 622 (Related: See Paras 614 and 619) "The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above."	FERC Order No. 706	The drafting team addressed this in CIP-007-5, requirement R3. The drafting team is taking the approach of making this requirement a competency-based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive. When remote access is used to connect to a BES Cyber Asset, an intermediate device is required in CIP-005-5, requirement R2 (part 2.1) and guidance is further included for the cyber security policy in CIP-003-5, Requirement R2 to maintain up-to-date anti-malware software and patch levels before initiating interactive remote access.
Para 628 "The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1."	FERC Order No. 706	In CIP-007-5, requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of once every 15 days.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 633 "The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it."	FERC Order No. 706	The SDT addresses this directive in CIP-011-1, requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from the BES Cyber Asset. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal. Additional guidance was added to the standard as further clarification: Media sanitization is generally classified into four categories: disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes. This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 635 "the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."	FERC Order No. 706	The SDT addresses this directive in CIP-011-1, requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from the BES Cyber Asset. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal. Additional guidance was added to the standard as further clarification: Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes. This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 643 (1 of 2) **"The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments**, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."	FERC Order No. 706	In order to provide more direction on what "features, functionality, and vulnerabilities" should be addressed in a vulnerability assessment, the SDT included guidance in CIP-010-1 on active and paper vulnerability assessment. The SDT further referenced NIST SP800-115 to provide entities additional guidance on how to conduct a vulnerability assessment.
Para 643 (2 of 2) "The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, **and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."**	FERC Order No. 706	In CIP-010-1, requirement R3 (part 3.4), the SDT added a requirement for an entity planned date of completion to the remediation action plan following a vulnerability assessment.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 660 (Related, See Para 661) "The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. In developing the guidance, the ERO should consider the specific examples provided by commenters, described above. However, we direct the ERO to develop and provide guidance on the term reportable incident. The Commission is not opposed to the suggestion that the ERO create a reference document containing the reporting criteria and thresholds and requiring responsible entities to comply with the reference document in the revised Reliability Standard CIP-008-1, but will allow the ERO to determine the best method to accomplish the goal of better defining reportable incident."	FERC Order No. 706	In addition to defining the term Reportable Cyber Security Incident as one that compromises or disrupts the functional tasks of a Responsible Entity, CIP-008-5 also provides further guidance for determining a Reportable Cyber Security Incident in the "Guidelines and Technical Basis" section of the standard. The definition and guidance describe a reportable incident based on characteristics of impact to the BES, rather than enumerating threats and characteristics of malware.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 661 (Related, See Para 660) "the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."	FERC Order No. 706	CIP-008-5 addresses the four parts of this directive as follows: 1. Added: Reportable Cyber Security Incidents include, as a minimum, any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. In turn, a Cyber Security Incident includes a malicious act or suspicious event that compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter. 2. CIP-008-4, requirement R1 (part 1.2) contains provisions for reporting Cyber Security Incidents. 3. See 1, above. 4. Guidance and measurements have been developed to provide information that may be used to enhance an auditable and enforceable standard.
Para 673 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order No. 706	Cyber Security Incident Reporting and Response Planning: CIP-008-4, requirement R1 (part 1.3) contains provisions for reporting Cyber Security Incidents to the ES-ISAC within one hour of identification, even if it is a preliminary report.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 676 "The Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order No. 706	Cyber Security - Incident Reporting and Response Planning: CIP-008-4, requirement R1 (part 1.3) contains provisions for reporting Cyber Security Incidents to the ES-ISAC within one hour of identification, even if it is a preliminary report. . Cyber Security - Incident Reporting and Response Planning: CIP-008-4, requirement R1 (part 1.3) contains provisions for reporting Cyber Security Incidents to the ES-ISAC within one hour of identification, even if it is a preliminary report.
Para 686 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned."	FERC Order No. 706	In CIP-008-5, Requirement R3 and its parts, the SDT includes additional specification on the update of response plan and modifies the response plan requirements to incorporate lessons learned. Maintenance of documentation of paper drills, full operational drills, and responses to actual incidents is part of the documentation required to demonstrate compliance with the security controls in CIP-008-5 and is already subject to the evidence retention requirements associated with all NERC Reliability Standards.
Para 687 (also see Footnote in Order) "In light of the comments received, the Commission clarifies that, with respect to full operational testing under CIP-008-1,	FERC Order No. 706	CIP 008-5, Requirement R2, Part 2.1 is written to allow the testing requirement to be satisfied by responding to an actual Reportable Cyber Security Incident; or with a paper drill or table top exercise; or with a full operational exercise. The reporting of Cyber Security Incidents is addressed in the requirement R1 (part 1.2).

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
such testing need not require a responsible entity to remove any systems from service. The Commission understands that use of the term full operational exercise in this context can be confusing. We interpret the priority of the testing required by this provision to be that planned response actions are exercised in reference to a presumed or hypothetical incident contemplated by the cyber security response plan, and not necessarily that the presumed incident is performed on the live system. A responsible entity should assume a certain type of incident had occurred, and then ensure that its employees take what action would be required under the response plan, given the hypothetical incident. A responsible entity must ensure that it is properly identifying potential incidents as physical or cyber and contacting the appropriate government, law enforcement or industry authorities. CIP-008-1 should require a responsible entity to verify the list of entities that must be called pursuant to its cyber security incident response plan and that the contact numbers at those agencies are correct. The ERO should clarify this in the revised Reliability Standard and may use a term different than		The Guidelines and Technical Basis section of CIP-008-5 refer to operational exercises in the FEMA Homeland Security Exercise Evaluation Program as one of the following three types: drill, functional exercise, and full-scale exercise. It defines that "[a] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, emergency operation centers, etc.) and "boots on the ground" response (e.g., firefighters decontaminating mock victims)." The SDT believes the term operational exercise has become well understood and appropriate for both incident response and recovery exercises.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
full operational exercise."		
Para 694 "For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard"	FERC Order No. 706	The SDT added in CIP-009-5, Requirement R2, a requirement to implement the recovery plan.
Para 706 "The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard."	FERC Order No. 706	CIP-009-5, Requirement R1, Part 1.5 requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service. The SDT captured the objective of this control, but did not explicitly use the term "forensics" due to the legal interpretations associated with the term.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 710 (Related: Para 706) "Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report."	FERC Order No. 706	CIP-009-5, Requirement R1, Part 1.5 requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service.
Para 725 "The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years."	FERC Order No. 706	CIP-009-5, Requirement R2, Part 2.3 requires an operational exercise at least once every three calendar years.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 739 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."	FERC Order No. 706	In CIP-009-5, Requirement R1, Part 1.4 the SDT added requirements related to restoration processes based on review of the DHS Controls, and requires verification initially after backup to ensure that the process completed successfully. In CIP-009-5, Requirement R2, part 2.2, requires a Responsible Entity to ensure that the information is useable and is compatible with current system configurations for High Impact BES Cyber Systems or Medium Impact BES Cyber Systems at Control Centers.
Para 748 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."	FERC Order No. 706	In CIP-009-5, Requirement R1, Part 1.4 the SDT added requirements related to restoration processes based on review of the DHS Catalog of Control Systems Security: Recommendations for Standards Developers (a derivation of NIST SP800-53 for Control Systems), and requires verification initially after backup to ensure that the process completed successfully.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
	NERC Alert regarding remote access VPN vulnerabilities	Addressed in CIP-005-5 ▪ Creates basic requirements to protect critical systems from untrusted networks. ▪ Identifies protective measures that provide secure access to critical systems. ▪ Helps ensure secure practices by employees, contractors, and service vendors to minimize exploitation of vulnerabilities. ▪ Addresses questions regarding ability to audit or enforce the requirement through the design of clear measures. ▪ Significant guidance provided to address implementation options for organizations of differing sizes, capabilities, and complexity. Additional information is provided in “Guidance for Secure Interactive Remote Access” published by NERC in July 2011. Additionally, remote access is specifically required to be included in an entity’s cyber security policy. Guidance is included to assist the entity in determining what this topic in the cyber security policy should address.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 13 "The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."	Order Approving Interpretation of Reliability Standard CIP-007-2 in Docket No. RD10-3-000, March 18, 2010	CIP-007-5, Requirement R1, Part 1.2 requires Responsible Entities (for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers) to "protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media."

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments
Cyber Security Order 706 Version 5 CIP Standards

Comment Form
Combined Question 1 and Question 2 Summaries
October 26, 2012

The Project 2008-06 Drafting Team thanks all commenters who submitted comments on the Version 5 of the CIP Cyber Security Standards and its Implementation Plan for consideration by the SDT in finalizing Version 5 and related documents. The 10 standards were posted for a 30-day formal comment period from September 11, 2012 through October 10, 2012 and successive ballots through October 10, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 112 sets of comments, including comments from approximately 258 different people from approximately 153 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Table of Contents

Introduction 7

"Identifies, Assesses, and Corrects Deficiencies" Comments 8

Section 4 - Applicability 10

Draft Reliability Standard Audit Worksheet 13

"Annual" and Other Time Parameters 13

Authorized Access List and Specific Rights Reviews in Multiple Standards 14

Data Retention Requirements 15

CIP-002-5 16

Requirement R1 18

Requirement R2 20

Attachment 1 20

Criterion 1.2 21

Criterion 1.4 22

Criterion 2.1 22

Criterion 2.3 23

Criterion 2.4 24

Criterion 2.5 25

Criterion 2.6 27

Criterion 2.8 27

Criterion 2.9 27

Criterion 2.10 27

Criterion 2.11 28

Criterion 2.12 28
Criterion 2.13 31
Criterion 3.1 31
Criterion 3.4 31
CIP-003-5 32
CIP Senior Manager 32
Policy Requirements 32
Requirement R2 33
Requirement R4 33
CIP-004-5 35
General 35
Requirement R1 35
Requirement R2 36
Requirement R3 37
Requirement R4 38
Requirement R5 40
CIP-005-5 43
High Water Marking 43
Background Section 43
Consideration of Data Diodes 44
Requirement R1 44
Requirement R1 VSLs 48
Requirement R2 48
CIP-006-5 52

General 52
Background Section 52
Requirement R1 52
Requirement R2 55
Requirement R3 56
Guidelines and Technical Basis 56
CIP-007-5 57
General Comments 57
Effective Dates 57
Requirement R1 57
Requirement R2 58
Requirement R3 62
Requirement R4 64
Requirement R5 68
CIP-008-5 71
General 71
Requirement R1 71
Requirement R2 72
Requirement R3 73
CIP-009-5 75
Requirement R1 75
Requirement R2 76
Requirement R3 77
Guidelines and Technical Basis 78

CIP-010-1 79
Timeframes for Configuration Control Activities 79
Cross References to CIP-005-5 and CIP-007-5 on Impacted Controls 79
Requirement R1 79
Requirement R2 80
Requirement R3 80
CIP-011-1 82
Requirement R1 82
Requirement R2 82
Implementation Plan 83
Effective Date 83
Initial Performance of Certain Periodic Requirements 85
Previous Identity Verification 86
Planned or Unplanned Changes Resulting in a Higher Categorization 86
Applicability Reference Tables 87
Definitions 88
BES Cyber Asset 88
BES Cyber System 88
BES Cyber System Information Responses 88
CIP Exceptional Circumstance Responses 88
CIP Senior Manager Responses 88
Control Center 89
Cyber Asset 89
Cyber Security Incident 90

Electronic Access Control and Monitoring System 91
Intermediate Device (now “Intermediate System”) 91
Interactive Remote Access 92
Reportable Cyber Security Incident 93

Introduction

The Standard Drafting Team (SDT) thanks all commenters for their continued focus on providing constructive and useful feedback for improving and refining the standards. In response to draft 3 of the Version 5 CIP Cyber Security Standards, the SDT received input that was focused on several issues that assisted the SDT in refining the standards to the final set of standards now posted for recirculation ballot. The SDT carefully considered all comments in determining whether to make particular changes to the standards.

In response to comments provided to draft 3, the drafting team greatly appreciates those entities that focused their comments on the issues most critical to them, as it facilitated a qualitative representative assessment of the areas requiring the greatest review. The focus on those major concerns that were essential as a condition to find consensus was greatly appreciated.

Furthermore, the SDT wishes to thank the industry for their significant engagement and support in developing these standards. Industry participants and observers, whether formally or informally, and whether in person or through other means, provided important perspectives and subject matter expertise that facilitated the SDT's consideration of the complicated issues and technical matters reflected in these standards. This truly was a collaborative process with participation from virtually every facet of our diverse and committed industry. Security and reliability were reflected in each consideration, and the extensive and consistent industry participation throughout the process is reflected in high approvals in response to the successive ballot from draft 3 that ended October 10, 2012.

At this stage, the drafting team has reached a point where it has made a good faith effort at resolving applicable objections, and it has not made any substantive changes since posting draft 3. Therefore, the team is posting the standards, related definitions and implementation plan for a recirculation ballot. As in past drafts of the Version 5 CIP Cyber Security Standards, the SDT thoroughly considered proposed changes and evaluated them carefully by considering several important variables, such as, but not limited to, whether such changes were in the interest of cyber security and reliability, whether they would improve or reduce consensus, whether they had unintended consequences for other types of entities, and whether they were in support of the SDT's obligation to respond to regulatory directives, most notably from FERC Order No. 706. The SDT has done its best to be responsive to all inputs, recognizing that it is not possible to adopt every suggestion and also recognizing the considerable diversity of entities and assets to which the standards will apply.

In the accompanying comment form for draft 3, the drafting team asked the following two questions:

1. If, after reviewing the posted standards and General Summary of Consideration of Comments, you do not support one or more of the 10 standards, the implementation plan or set of definitions, please indicate the specific item you do not support (the standard and Requirement number, specific defined term, or implementation plan) and the specific reason you cannot support it here.
2. If you have a brief comment you would like to provide that has not already been provided among the previously submitted feedback in response to draft 1 and draft 2, please provide it here. Please limit your comment to 200 words or less.

In reviewing comments, the SDT determined that some common issues were presented by different entities in response to either Question 1 or Question 2, depending on how the particular entity organized its comments. As a whole, the SDT found that the responses were thoughtful, organized, and focused. In this summary, the SDT is responding to all comments from industry that were submitted in response to both Question 1 and Question 2 in one consolidated summary form rather than providing a separate summary for each of Question 1 and Question 2. Since most issues and comments were not isolated in response to one question or the other, this single summary provides the most efficient and thorough method with which to provide the SDT's response.

Commenters addressed a wide variety of topics in their comments, but the most commented upon subjects include comments on the Transmission Operator (TOP) Control Center Criterion in CIP-002-5's Attachment 1 and comments regarding the SDT's use of the "in a manner that identifies, assesses, and corrects deficiencies" language. The TOP topic is discussed in detail under the CIP-002-5 portion of this summary, and the "identifies, assesses, and corrects deficiencies" topic is addressed immediately below as part of this summary's general discussion. Other topics are discussed relative to their particular standard or definition, and the associated table of contents for this document lists most topics of discussion.

"Identifies, Assesses, and Corrects Deficiencies" Comments

As noted in the background sections of the standards, and in response to comments from draft 2, the SDT has incorporated within CIP Version 5 a recognition that certain Requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain Requirements. The intent is to change the basis of a violation in those Requirements so that they are not focused on *whether* there is a

deficiency, but on identifying, assessing, and correcting deficiencies. Note that, where used, the addition of language modifies "implement"; it does not itself require or specify internal controls, though it certainly enables their use for those entities that have adopted an internal controls or compliance management approach. For purposes of this summary, the "identifies, assesses, and corrects deficiencies" phrase is sometimes referenced as simply "IAC."

This topic was a source of several comments on draft 3, and the SDT appreciates the comments, feedback, and the spectrum of concern or support on this issue. The SDT believes that Version 5 is the right time to take a step in a direction that promotes security and reliability by incorporating a self-correcting aspect in certain Requirements. This is a new step, but it is informed, collectively, by implementation and audit experience from Versions 1 through 3 of the CIP Cyber Security Standards.

Many commenters support the SDT's addition of a self-correcting aspect and applaud the overall shift in the emphasis of compliance from perfection to the identification, assessment, and correction of deficiencies. The commenters support the shift from zero tolerance for deficiencies to encouraging finding and correcting deficiencies. The SDT considers such self-correction as an essential component to improved reliability and security, and it thanks commenters for their support. Though there were several specific suggestions or concerns, as noted below, the consensus position of the industry is one of support for the approach, as reflected in both comments and the overwhelming approval of the standards that use the approach.

While this is a new direction, the SDT believes there is tremendous benefit in eliminating the zero-defect language in the standards, and it is therefore worthwhile of inclusion in the CIP standards. However, the SDT acknowledges this is a developing concept and encourages the industry to continue to work alongside NERC in implementing the compliance monitoring strategy for the language.

Some commenters presented concern that there is no clear mechanism with how this approach will be audited or that there may be inconsistent audits across Regions. The SDT is well aware of this concern, and it is encouraged by ongoing coordination and support among both NERC and several regions. The SDT expects that NERC will continue to develop tools such as the Reliability Standard Audit Worksheets (RSAWs) in a manner that involves the industry and the members of the SDT. Importantly, the language to "identify, assess, and correct deficiencies" modifies "implement" where used, and it is meant simply to express that implementation of the Requirement is not in a "zero defect" manner.

Commenters also questioned whether this approach indeed does require internal controls. The SDT notes that the compliance initiatives that relate to internal controls are not the same as the approach in the standard. The SDT contemplates that the "identify, assess, and correct deficiencies" language is appropriate regardless of how compliance may be monitored, while noting that the standards approach is also supportive of the compliance approach where and if used. At its core, the SDT intends in using the language to signal an important transition to self-correction as part of the expected performance of a Requirement itself as opposed to a mere deficiency constituting the basis for violation.

Some commenters also proposed alternative, additional, or supporting language to augment the "identify, assess, and correct deficiencies" language in the Requirements or other supporting components of the standards, or proposed addition of the language to other requirements. The SDT has previously considered such alternative language and evaluated carefully where the language should be used, and, upon reexamining those proposals in response to comments, the SDT continues to support those concepts in the compliance monitoring approach and documents rather than in the standards themselves. Language noting that certain actions are not violations is too prescriptive for either the Requirements or the measures, and they do not comport with the style and form of the standards. With continuing input, coordination, and education, the SDT is confident that the Requirement language as presented is the appropriate mechanism to empower the industry to focus on correcting deficiencies as part of the expected performance of the Requirements while not requiring or prescribing a particular assessment of the how the entity accomplishes it.

Additionally, in response to perspectives expressed by commenters on the "identify, assess, and correct" deficiencies language, the SDT shares the view that NERC must ensure going forward that the compliance monitoring approach is consistent. The SDT believes that most of the industry is ready to transition to a new approach and that this reflects the consensus position. The SDT and the industry have an opportunity to incorporate significant improvements and lessons learned from implementation and audit of previous versions, and the SDT is encouraged by not only industry support, but also from NERC's direction in continuing to work with the industry in implementation of risk-based initiatives. The SDT will remain engaged after approval of the standards to work with NERC to provide input into the RSAW development process.

Section 4 - Applicability

There were many comments that "group of Elements" from the standards' applicability section, parts 4.1.2.4 and 4.2.1.4 should be deleted on the bases that it is redundant with Cranking Path and would create ambiguity, citing that these and initial switching Requirements are included in the Cranking Path. The SDT considered the language that is included in Requirement R1.5 of EOP-005-2, which says: "Identification of Cranking Paths and initial switching Requirements

between each Blackstart Resource and the unit(s) to be started." The addition of the term "group of Elements" is based on this Requirement that includes "and initial switching Requirements" in addition to the Cranking Path, and it is meant to include the group of Elements that is included in these initial switching Requirements.

One commenter requested clarification on the applicability of Section 4 with respect to Distribution Providers (DPs). The SDT notes that the clarification is included in the Guidelines and Technical Basis section of the standards relating to applicability. The guidance specifically says: "Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2." This means that DPs that own assets listed in 4.2 are subject to the standard. In addition, "For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above" are excluded from applicability of the CIP standards. That means that only systems and equipment listed in 4.2.1 are subject to the CIP Cyber Security standards.

Many commenters stated that the qualifications for applicable assets in section 4 for Cranking Paths unfairly includes non-BES facilities for DPs while excluding those from Transmission Owners (TOs) and TOPs, for which all BES Facilities are defined under section 4 as applicable. Alternate language was proposed to only include BES facilities in the scope for Cranking Paths. The SDT clarifies that those TOs that own BES Facilities as well as non-BES facilities that are qualified for DPs will also be registered as DPs. A review of the registry listing from September, 2012 showed that 232 of the 340 registered TOs (68%) are also registered as DPs. The SDT further points out that the inclusion of DPs in the applicability ensures that non-BES facilities, such as those that support the restoration of the BES, that are impactful to the reliability and operability of the BES are included.

One comment read that it appears that small entities that own stand-alone UFLS systems with no communication facilities would have applicable Requirements under these standards. It is the intent of the SDT to include all UFLS systems that meet the criteria defined in section 4. These criteria do not include any exclusion based on connectivity. The SDT points out that for DPs, only those UFLS systems that can automatically shed 300 MW or more under a common control system are qualified for applicability. The Requirements that are applicable based on connectivity are specified in CIP-003 through CIP-011. The commenter also stated that, "Further a small entity that is part of a larger load shedding program should maintain their program, but the entity that is responsible should be the one with the cyber security based on the common control system." The SDT clarifies that the owner of all qualified cyber systems is the entity responsible for compliance of these cyber systems: while the common control system that is capable of shedding 300 MW qualifies that UFLS, all cyber systems that impact the reliable operation of the UFLS system become in scope. The

responsibility for the compliance of each of these cyber systems to applicable Requirements belongs to the owner of that cyber system.

One commenter stated that the Functional Entities in section 4.2.1.3 and the Impact Rating Criteria in Attachment 1, section 3.6, for DPs to include facilities containing "A Protection System that applies to Transmission ..." is a new (initially introduced in draft 2) unsubstantiated Requirement for low impact assets. The SDT points out that among the tasks of the DP in the Functional Model is to "design and maintain protective relaying systems, under-frequency Load shedding systems, under-voltage Load shedding systems, and Special Protection Systems that interface with the transmission system." Further, the NERC Statement of Compliance Registry Criteria (Appendix 5B of the NERC Rules of Procedure) includes:

> "III.b.2 Distribution Provider is the responsible entity that owns, controls, or operates Facilities that are part of any of the following Protection Systems or programs designed, installed, and operated for the protection of the Bulk Power System:
>
> - a required UFLS program.
> - a required UVLS program.
> - a required Special Protection System.
> - a required transmission Protection System."

The same commenter suggested that the inclusion of all BES Facilities in section 4 is excessive. The SDT takes the position that cyber systems that impact the real-time operation of any BES Facility must be subject to some form of protection that is commensurate with its impact. The SDT points out that only those BES Cyber Systems that have a real-time impact to the BES are included by definition. This is also in consideration of comments in FERC Order No. 761.

Another commenter wrote that the use of the defined term "BES Facilities" in the applicability section would exclude such assets as Control Centers and Protection Systems. While these facilities are not BES Facilities per se, they are facilities essential to the reliable operation of the applicable BES Facilities and are included for applicability because of the function they are providing for reliable operation of BES Facilities.

One commenter stated that the clause "is subject to one or more Requirements in a NERC or Regional Reliability Standard" was unclear and proposed "can affect the reliability of either Medium or High Impact Facilities." The SDT believes that DPs have to comply with NERC Reliability Standards for some facilities they own and that the current clause

provides certainty as to what those facilities are since these DPs are required to comply with these standards. The SDT feels that the proposed language provides less certainty and is more subjective.

One commenter noted that exempting utility owned communications infrastructure (exemption of communications facilities between ESPs) creates a cyber security issue. The SDT believes that utility owned carrier services should be treated in exactly the same way a third party carrier is viewed in terms of trust, and that adequate protection measures should be taken to protect against an untrusted (from the BES Cyber System point of view) service provider.

Draft Reliability Standard Audit Worksheet

Some commenters provided input and feedback in their comments to the draft RSAW for CIP-006-5 that NERC Compliance Operations posted concurrently with draft 3 of the CIP Cyber Security Standards. The intent of the SDT in contributing to the development of a draft RSAW for CIP-006-5 was to begin the initiative of developing RSAWs in concurrence with standard development projects. The SDT provided input to the draft of the RSAW, and it is encouraged by the opportunity for the SDT and industry to continue to provide input as the RSAWs continue to be developed subsequent to the industry's approval of these standards. The SDT has forwarded these constructive inputs to NERC Compliance Operations for their continuing consideration.

"Annual" and Other Time Parameters

Some commenters pointed out that in a few instances, the SDT inadvertently continued to use the "at least once each calendar year (or similar)" language in conjunction with the convention to not exceed 15 calendar months. The SDT has reviewed the standards and eliminated those "calendar year" references where the SDT intended to use only the phrase "at least once every 15 calendar months."

A few commenters continued to suggest alternatives or expressed preference for retaining only the "annual" reference, which would result in continued reliance on CAN-0010. The SDT has not implemented that change because within Version 5 there is an opportunity and an obligation to unambiguously reference the periodic time parameter. The SDT also explained this in greater detail in response to draft 2 of the Version 5 CIP Cyber Security Standards on pages six and seven of summary consideration of comment form A.

One commenter expressed a desire to adopt a "once per month" convention instead of using, "At least once every 35 calendar days..." where that phrase is used. This is similar to the discussion on "annual," and for similar reasons, the SDT has not made the change. The SDT intends for these time periods to be repeatable on a basis that approximates

performance on the same day per month, or more frequently. The SDT believes it is reasonable to use 35 calendar days to account for those scenarios where a month may begin or end on a weekend, or for holidays.

Authorized Access List and Specific Rights Reviews in Multiple Standards

One commenter identified possible issues with a lack of understanding and inconsistent implementation for authorized access lists and specific rights review in Versions 1 through 3 of CIP-004 Requirement R4, CIP-003 Requirement R5, and CIP-007 Requirement R5. The commenter further stated that there was a concern that the quarterly and annual verification of CIP-004-5 Requirements Parts 4.2 and 4.3 are predicated on some generalizations and/or assumptions that are not complete and will not sufficiently resolve existing issues.

Similarly to the comment above, another commenter had issues with a lack of understanding and an inconsistent implementation for authorized access list and specifics rights review with the multiple standards as mentioned in the previous paragraph. The commenter was concerned that CIP-004-5 Requirement Parts 4.2 and 4.3 quarterly and annual verifications are predicated on some generalizations and/or assumptions that are not complete and will not sufficiently resolve the existing issues. Furthermore, the commenter stated that access authorizations and provisioning warrant further clarity in the recirculation ballot because they require significant resources, involve extensive complex data and are among the most currently violated Requirements. In response to the two aforementioned comment responses, the SDT has modified Requirement Parts 4.2 through 4.5 to state up front to which type of access each Requirement Part applies. CIP-007-5 Requirement Part 5.2 is a security hardening control applying to the enabling or disabling of generic accounts (From the Technical Guidelines section: A generic account is a group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type).

The key distinction between CIP-007-5 Requirement Part 5.2 and CIP-004-5 Requirement Part 4.3 it that generic accounts and associated privileges are not authorized nor is there the same concept of "need to know." CIP-004-5 Requirement Part 4.3 applies to user accounts only and would not necessarily indicate a full listing of user accounts and privileges on the system. However, one could envision a process by which an entity finds it more efficient to perform a full account listing and thereby produce evidence in compliance for both Requirement Parts. The SDT also point out that the identification of default or generic accounts occurs only once and does not require annual verification.

The SDT acknowledges the listing of individuals with authorized access to shared accounts (CIP-007-5 Requirement Part 5.3) has a connection to the authorization of CIP-004-5 Requirement R4 because entities must know the list of individuals

authorized to a shared account in order to fully perform the quarterly and annual assessments. However, entities may comply with the Requirement to authorize access to a BES Cyber System without specifying how they obtain such access. Overall, the SDT sees valid arguments for this Requirement Part residing in both CIP-004-5 and CIP-007-5. Because of the history of prior versions, the difference in applicability, and the significance in moving a Requirement Part to a different standard, the SDT choose to retain the Requirement in its original location.

Data Retention Requirements

There were several commenters that stated specifically and in general to exclude any data retention Requirements from the standard. In response, these few Requirements are not intended to specify a retention period as done in the Compliance section of standards, but to retain information for the purpose of incident response and analysis.

CIP-002-5

Draft 3 of CIP-002-5 obtained an affirmative ballot result of 74.9% with a quorum of 80.6% of the ballot pool at its successive ballot of October 2012. This result indicates a very significant improvement from the previous ballot and achieves a high level of stakeholder consensus.

One commenter noted an inconsistency in sub-Requirement numbering in the standard. This has been corrected and the part numbers have been changed in CIP-002-5 to remove the "R" from Requirement "R1.1", etc., to "1.1", etc.

There was a comment that stated the purpose of the standard is inconsistent with the approach, further noting that "the standard as written evaluates only the impact of a degradation to a group of Facilities instead of evaluating the degradation of a BES Cyber System." The SDT notes that the standard has taken the approach that the categorization of qualified BES Cyber Systems is based on the impact of the functions performed by the assets they are supporting. This is consistent with risk management approaches that evaluate risks based on the functional objective of the organization (in this case the reliable operation of the BES). The same entity proposed a multilevel evaluation of the impact of cyber systems based on functional impact as well as the individual impact of the cyber system within the functional impact. This multilevel approach was one that was proposed to stakeholders early in the development process: industry comments called for a simpler approach which resulted in the current one.

Another commenter stated that the CIP-002-4 and Version 5 "bright-line criteria" step away from a risk based method to a prescriptive approach. The commenter further wrote that it is an inverted philosophy from the approach draft 3 used in the other CIP Version 5 standards. The SDT notes that CIP-002-5 follows on the approach used in Version 4, which has been approved by the industry and by FERC, for using bright lines instead of an entity-defined risk-based methodology for evaluating the impact of assets, and the SDT is extending the concept with a multi-tiered approach to categorizing all BES Cyber Systems according to impact.

There was a comment that the standards use the term "Transmission stations or substations," and the commenter proposed some other terms such as "switchyards." The SDT points out that a brief clarifying paragraph is included in the Guidelines and Technical Basis explaining the use of these terms in the section on Transmission criteria: "*The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain*

autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist." The SDT also made minor editorial changes when using this term for more consistency.

There was a comment that the paragraph in the Background section that deals with the 300 MW UFLS threshold should be moved to the Guidelines and Technical Basis section. The SDT points out that section 4 is a common section that is in all the standards and believes that the explanation of the 300 MW threshold used in the common section 4 should be included in the common part of the Background section to carry it into all the CIP standards in this series.

One commenter provided general feedback on the approach taken for CIP-002-5. The commenter cited concerns on the Facilities-based approach to evaluating the impact of BES Cyber Systems. The SDT had extensive discussions in the last several years on the merits of both the systems-based and facilities-based approaches. The SDT points out to the commenter that entities are free to use any method to arrive at the identified and categorized BES Cyber Systems. Regarding the evaluation of the impact based on the function of the assets, a fundamental concept in risk management frameworks, including the National Institute of Standards and Technology (NIST) Risk Management Framework, is that the evaluation of the risk for systems must be related to the mission of the organization, in this case, the reliability of the BES. The entity also commented on the lower level of protection for low impact BES Cyber Systems. This is consistent with tailoring the level of protection according to the risk (in this case, the impact) and optimizing available protection resources for the systems that most need the protection according to their impact on the mission of the organization. The commenter also commented on the consideration of "interconnectedness". The SDT has taken the approach of considering connectivity in the development and application of Requirements.

There was a comment made that the section on BES reliability operating services in the Guidelines and Technical Basis section should be removed as it contains many subjective areas. The SDT has gone through several iterations of including these in the standards or as guidance and has resolved to providing guidance on functions for applicable functional entities based on the functional model. The section has been well-received with comments requesting the included enhancements in the past drafts.

A recommendation was made that the undefined term "adversely impact" should be replaced with "Adverse Reliability Impact" throughout the standard and definitions document to be consistent with the defined term in the NERC Glossary. The SDT disagrees, because where the SDT has used the term Adverse Reliability Impact, it has used it precisely for the meaning defined in the NERC Glossary. It is not appropriate to use the NERC Glossary term when it is not the intent of

the SDT to use the meaning of the defined term. The NERC Glossary term is very specific to a level of impact on the reliability of the BES. This is not always the appropriate level or meaning in all cases where the term "adversely impact" is used.

One commenter noted that the diagram at the end of the Guidelines and Technical Basis section is confusing. In response, the SDT notes the flowchart is an actual use case provided by an observer and may not be applicable in all environments. It is meant to provide one approach used by an entity.

Requirement R1

There were several commenters that noted there was inconsistency in the words used in Requirement R1 and Attachment 1, criterion 3.4 of section 3 (Low Impact), regarding restoration, with terms used in EOP-005-2 and with terms used elsewhere in the standard. The SDT has made changes to these sections to be consistent with the terms used in EOP-005-2: Blackstart Resources and Cranking Path and initial switching Requirements.

One commenter requested that additional reference to the specific standards be included where the term "...is subject to one or more Requirements in a NERC or Regional Reliability Standard" is used. The commenter furthermore stated that this term is not specifically used in Requirement R1 or the Requirement Parts. However, it is used in section 4 to qualify UVLS/UFLS, Special Protection Systems and Protection Systems owned by DPs that are subject to these CIP standards. In response, the SDT notes the intent is to include only those assets for DPs that are covered by a NERC Reliability Standard, which would be those, by implication, that are related to the reliable operation of the BES. References to other standards within a standard are not recommended practice in NERC standards drafting.

There was a comment that the last sentence in the opening paragraph for Requirement R1 in the Guidelines and Technical Basis section for Requirement R1 is confusing. The SDT has clarified and simplified the sentence.

One commenter stated that the use of the term "considers" in Requirement R1 leads to the same confusion as exists with the existing CIP-002-3 standard as some entities will argue that "consider" does not mandate a required subsequent action. The commenter proposes that the Requirement should be restated as "For each asset type enumerated below, each Responsible Entity shall: . . ." In using the term "considers", the SDT recognized that all entities do not own all the types of assets listed. The proposed language assumes that all entities own all of the types of assets listed. In providing this consideration, the SDT seeks to avoid situations where entities end up having null lists for each one of the type of asset that it does not own.

The same commenter stated that the assertion in Requirement Part 1.3 that the entity is not required to produce a list of low impact BES Cyber Systems renders this Requirement not auditable for accuracy or completeness; and that to demonstrate that all high and medium impact BES Cyber Systems have been properly categorized, the entity must be prepared to produce a list of all BES Cyber Systems that were evaluated, the remainder of which represent the low impact BES Cyber Systems. The commenter further stated that the entity must be prepared to demonstrate the minimal Requirements applicable to low impacting BES Cyber Systems have been properly implemented, also requiring a list of impacted systems. The SDT has considered the considerable increase in the scope of cyber systems included in this version and has taken the approach that those Requirements that apply to the anticipated large number of low impact field systems should be focused on program components that provide the corresponding level of protection, rather than a disproportionate effort in managing compliance for these systems.

One commenter suggested the removal of Requirement Part 1.3 and the low impact category in Attachment 1. The SDT has taken the approach that all BES Cyber Systems should be subject to some level of protection. The SDT has provided an approach to allow the specification of the commensurate level of protection for low impact cyber systems while providing a framework that would minimize entities' compliance burden for the large number of low impact cyber systems that it anticipates.

One commenter recommended that the six asset categories included as part of Requirement R1 be removed and the drafting team instead reference Attachment 1, if needed, to ensure consistency in language as well as prevent unnecessary duplication. The inclusion of the asset types in Requirement R1 is a direct result of comments from a large number of stakeholders on draft 2 to provide some reference to asset types required to be considered in Versions 1 through 3. The SDT has made modifications to improve overall consistency within the standard.

Another commenter noted that, in Requirement Part 1.3, the intent is to provide protection at BES Facilities that do not meet Attachment 1, criteria 1.1 through 2.13. The commenter added that the wording is technically flawed and conflicts with the definitions of BES Cyber Assets and BES Cyber Systems. The commenter continued to add that, by definition, to qualify as a BES Cyber Asset and System the asset must have a 15 minute impact on reliability of the BES and that a low impact facility cannot have such an impact to the BES. The SDT points out that while the definition of the BES Cyber System and BES Cyber Asset assumes impact on the function of the Facilities, systems and equipment (asset), an asset in the low impact does not assume that it has no impact on real-time operation of the BES. The 15 minute stipulation in the definition of BES Cyber Asset describes an impact on the function performed by the low impact asset for the BES.

One question arose which asked how an auditor is to verify identification of all BES Cyber Systems that are applicable to Requirements Parts 1.1 and 1.2. There are current Requirements to identify Critical Cyber Assets in Versions 1 through 4. The SDT expects that auditors will continue to use similar methodologies used to verify compliance to such Requirements.

One commenter stated that its interpretation of Requirement R1 meant that each qualified cyber asset must be marked. This is not the intent, and the SDT does not believe that the language in Requirement R1 is specifying any such marking for cyber assets at each asset. The clause "at each asset" is purposely included in close proximity to "BES Cyber Systems," which is the phrase that "at each asset" is intended to qualify, not the word "identify". Certainly, the expectation is that the identification of the BES Cyber System would include information in some fashion about which asset it is "at". The proposed language "Identify and list each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at the asset level," does not meet the intent of the Requirement, since it must be clear that the identification must have enough information to identify the BES Cyber System, including the information on what asset it is located at.

Requirement R2

Many commenters noted that alternative, clearer language for Requirement Part 2.1 would ensure that there is no implied Requirement for updates outside of the annual Requirement review. The SDT believes the 15 month review is sufficient for categorization of BES Cyber Systems, and it has modified the language to provide additional clarity.

Attachment 1

There was a proposal that the language should be modified to specify that the applicable functional obligations referenced within criteria 1.1 through 1.4, 2.11, and 2.12 apply to only those real time tasks identified in the Functional Model. The SDT points out that the applicability of the Requirements is to BES Cyber Systems, and that the definition of BES Cyber Assets (and by reference, BES Cyber Systems) only includes those that impact real-time operation. The functional model does not define the tasks of the functional entity in terms of real-time or non-real-time, but the term real-time is used rather to describe its relationship with other functional entities.

Many commenters reiterated their comment on the rationale for categorization as high impact those Control Centers that control at least one of the medium impact facilities. The SDT responds that the localized impact of a facility at a single location is different and less impactful than the impact of a Control Center that controls one such facility and other facilities in the wide area.

There was one comment that stated Attachment 1 does not specify where within-hour generation and interchange scheduling systems related to Balancing, Managing Constraints, and Inter-Entity Coordination fall within the high-medium-low impact framework. The SDT clarifies that these systems used to perform functions that are not impactful to real-time operation of the BES, as such would not be defined as BES Cyber Systems, unless these systems are also performing functions impactful to the real-time operation of the BES. They would be included in scope in the initial scoping of supporting the functional obligations of the relevant functional entity, but systems strictly performing these functions in the absence of other functions impactful to real-time operation would fall out of scope.

There was a comment that the first bullet under the overall heading of the Guidelines and Technical Basis section for Attachment 1 makes several references to the term "BES Asset." The SDT has corrected the inappropriate capitalization of BES asset and uses the term BES asset as referenced in Requirement R1 of CIP-002-5.

One commenter expressed concerns that restoration facilities were categorized as low impact facilities. This issue was raised in comments received in previous drafts and the SDT has discussed this at length, reaching out to other NERC technical committees. After consideration of the overall risks to the availability of adequate restoration resources, the SDT's resolution was to categorize restoration facilities as low impact, as explained under the Guidelines and Technical Basis section of CIP-002-5, on pages 30 and 31.

Many criteria in Attachment 1 relate to Interconnection Reliability Operating Limits (IROLs). One commenter wrote that this may be a problem in the WECC area where the RCs have not yet defined IROLs. Consultation with WECC indicated that WECC is in the process of defining IROLs and that IROLs will be defined well within the implementation timeline of these standards.

Another commenter stated that since the term "associated data centers" has been removed from Attachment 1 and that it should be removed from the Guidelines and Technical Basis section. The term has been moved to the definition of the Control Center and an additional clarification has been included where it is referenced in the Guidelines and Technical Basis section.

Criterion 1.2

One commenter noted that the 3000 MW minimum specified in criterion 1.2 is excessive and does not appropriately reflect the potential risk a network-connected Balancing Authority (BA) has not only upon its own service area but also

upon the rest of North American BA, Reliability Coordinator (RC), and TOP registered entities with which it is directly or indirectly connected via the ICCP communication networks. The SDT carefully considered discussions from stakeholders and reviewed data on the distribution of BAs that would be affected. The SDT concluded that the threshold would include the majority of BAs with significant impact.

Criterion 1.4

Many commenters noted that this criterion would require that a 1500 MW Generator Operator (GOP) Control Center take on a High impact rating, while the rest of the Facility is medium impact. The commenter added that even if the criterion is intended to apply to multiple locations, the aggregated generation should be 3000 MW or greater - consistent with the risk level assigned to a BA Control Center. The SDT points out that a control room for a single generating plant at a single location does not meet the definition of a Control Center. The criterion has not defined a specific numeric bright line for a generation Control Center. For example, a generation Control Center could control three 1200 MW generation Facilities, for a total of 3600 MW, at more than one location, and still be qualified for a medium impact generation Control Center if none of these meet criteria 2.1, 2.3, 2.6 or 2.9. It is true that if one of the generation Facilities the Control Center controls meets criterion 2.1 for 1500 MW, it would be categorized as a high impact asset.

Criterion 2.1

One commenter requested clarification on the relationship between a single plant location and a single Interconnection used in the defined term meaning. In making these qualifications, the SDT considered scenarios where sets of units within a single plant location may service multiple Interconnections, as pointed out by the commenter. In these cases, the SDT wanted to ensure that the impact considered is consistent with the bright line defined in this criterion, which was based on numbers reviewed for each Interconnection. The same entity inquired about “multiple generators with different interconnection facilities which connect to different parts of the same substation.” It is not clear whether the commenter is using the general term interconnection (meaning connection to the Transmission System) or in the meaning of the defined term.

One commenter felt that the use of the word “by” in the first sentence of this criterion does not make sense and should be reworded. The use of the word provides an entity with the capability of evaluating groups of units when a single plant location may be servicing multiple Interconnections and is logically partitioned into more than one generation output. There are further qualifications which may provide additional grouping criteria, such as common cyber systems.

One commenter suggested that the 15 minute stipulation should be extended to 30 minutes to be consistent with some criteria in reliability standards. Some standards have used 15 minutes, which the SDT has used as its criterion. The commenter seems to suggest that the 15 minutes is "tighter" than 30 minutes. Extending the interval to 30 minutes would in fact reign in more cyber systems rather than reduce the number of cyber systems (by extending the criterion for real-time, more cyber systems are likely to meet this criterion than 15 minutes).

One commenter requested clarification on the term "commissioned generation." The term is used to specify generation resources that have been commissioned for operation and is intended to exclude generation that has not been commissioned for operation (such as mothballed generation, generation shut down for maintenance, or new generation that has not been commissioned for operation yet).

Criterion 2.3

There were many comments that the term "planning horizon of one year or more" is unclear and could be misinterpreted. The SDT has added guidance on this to make it clear that the planning horizon of one year or more means that the plan covers a reliability planning span of one year or more and that it does not necessarily mean that the operating day is over one year. The intent is to exclude generation required to operate or keep on operating to temporarily avoid reliability impacts.

There were many comments on the guidance relating to the role of the Regional Entity (RE)/ Regional Reliability Organization (RRO) and noted that the RE/RRO is not required to perform coordination of the actions resulting from planning studies. The commenter also noted that the term RRO is no longer the appropriate term. The necessary changes have been made.

One commenter asked whether the term "generation Facility" in this criterion is designed to cover a single unit at a facility, or all units at a single plant or Interconnection, as described in section 2.1. The SDT intended to include in this criterion all generation Facilities required to meet the designation: these can be a single unit, a set of units or all the units in the plant.

One commenter noted that the Guideline and Technical Basis section omitted the TP as one of the possible entities that could designate the generation Facilities. The SDT notes this has been corrected.

A commenter asked whether the phrase, "such as due to a Category C3 contingency" was intended to provide guidance to what faults to run and whether the term "Adverse Reliability Impact" which is used in Attachment 1, meant to be the criteria for all types of contingencies. The phrase "such as due to a category C3 contingency" is intended to provide an example of the type of condition that could lead a Planning Coordinator (PC) or Transmission Planner to designate "must run" generation Facilities. The term "Adverse Reliability Impact" is used here to qualify the reason the PC or TP would designate such generation Facilities. In response, the SDT notes it is intended to distinguish from designations made for power market management reasons.

One entity commented that the guidance provided in this section in the Guidelines and Technical Basis section referenced "Reliability Must Runs (RMRs)" and discussed the differences between market RMRs and what this criterion intended. The SDT points out that this is the reason it has avoided using the term "reliability must run" in the Requirement itself. However, this term has been used interchangeably in both contexts for lack of a better term, and that the meaning of the term and the reason for having these units differ depending on the context. The SDT has included an extended discussion of the underlying reason for the criterion in the Guidelines and Technical Basis, focusing on the long term remediation for BES deficiencies to avoid Adverse Reliability Impact. The SDT also made additional changes to the guidance to clarify the role of the RE in coordination and contracts.

There was a comment that the criterion is based on studies from functional entities that do not have applicability under this standard and on notifications from these entities. The SDT notes that these activities are implemented today and that there are TPL standards that require these functional entities to perform these studies. The standard also requires these planning entities to provide an action plan for remediation of identified deficiencies.

Criterion 2.4

In this section, medium impact is assigned to Transmission Facilities operated at 500kV or higher. One commenter noted that exclusion is warranted for distribution stations that are situated at the receiving end of a radial 500kV line. The commenter further noted that specific instances exist of 500/69kV stations whose only purpose is to provide distribution service. The applicability, which is section 4, stipulates applicability to BES Facilities for entities other than DPs. If the facility meets the qualification for designation as a non-BES facility under the definition of the Bulk Electric System, then it is not in scope for application of these CIP standards.

Criterion 2.5

One commenter noted that the 200kV floor specified in criterion 2.5 does not adequately consider the risk to the BES imposed by large regional areas that are predominately sub-200kV. The commenter noted the BES is defined as 100kV and above and the criterion needs to consider all of the BES in some manner. The SDT has not excluded any BES Transmission Facility in its applicability, but believes that not all BES Transmission Facilities should be protected at the medium impact level. The categorization is one that is based on impact, and the SDT believes that the inclusion of ALL BES Transmission Facilities at a single impact category is unjustified and defeats the concept of tiered levels of protection based on impact.

One commenter stated that, as currently defined, the values in the table force a label of critical on non-critical Facilities as proven by intricate studies performed by transmission planning engineers. The commenter recommends the values be revised as follows: Voltage Value of a Line 200kV - 399kV - Weight Value per Line - 800; Voltage Value of a line 400kV to 499kV - Weight Value per Line - 1300. The SDT based the values in the table on values published in an engineering report, has reviewed comments from previous drafts, and believes that it has a technical basis, as described in the Guidelines and Technical Basis section, for using these values.

A commenter provided an extensive discussion of the concerns on the application of this criterion for Direct Current (DC) Facilities. The commenter argued that in the case of DC Facilities, the impact is better assessed in a wide area perspective rather than as a localized way as specified in this criterion. The commenter further commented that such studies could be conducted to provide an impact based on MW rather than the approach used in 2.5 in the case of DC Facilities. The SDT has not considered this approach for DC Facilities and any criterion that is based on a “study” (that is not currently required by any reliability standard) to determine the impact of these DC Facilities would be contrary to the bright line approach.

One commenter requested that diagrams be provided to illustrate the bullets in the Guidelines and Technical Basis. The SDT discussed providing diagrams to illustrate the bullets, but resolved that there are many configurations that can provide these illustrations and that these would raise additional questions for entities that would not be familiar with specific configurations. Entities should use their specific configuration to apply these concepts.

One commenter requested many clarifications. These are listed below with their responses:

1. Is/how is a DC line counted?
   A DC line is counted at the operating voltage for the purpose of application of criterion 2.5.

2. If you have a tie between two subs that has a transformer in series, does the line receive a weighting factor (seems to per guidance)? Do you use the higher or lower voltage? Is it the same for both ends of the line?
   If the transformer in at the site of a Transmission station or substation, it is considered as part of the Facilities of that station or substation and lines incoming and outgoing of the station or substation are considered in the application of this criterion. If the transformer is in a dedicated station, each of the stations (including the transformer station) will consider incoming and outgoing lines of the station or substation in the application of the criterion.

3. From the guidance document, it was clarified that radial facilities that only provide support for "single generation facilities" would not be included. What is the definition of a "single generation facility"? Uncertain situations might include two base load turbines aggregated on one line or wind farm collector subs which have multiple sites feeding into a single high voltage collector sub?
   These examples are all considered as a radial connection to a single generation facility.

4. From the guidance document, in the last bullet on page 27, it is not clear what the statement "In these cases" is referring to, whether the designation as a single facility or multiple facilities.
   The clause "In these cases" is qualified further by "of these transformers being within the "fence" of the substation or station": this is referring to what is considered a single facility.

5. From the guidance document, in the last bullet on page 28. How would classification of the number of substation connections be handled if two lines are parallel between the same two subs, but one has been tapped for local, non-networked load service?"
   Assuming that the tap is at the station or substation, these would be considered connections to one other substation, but both outgoing lines would be counted for the purpose of aggregate weighting. If the tap is not at the station or substation, there is not enough information to definitively make a determination without evaluating the specific facts and circumstances.

One commenter inquired during the comment period on whether the connections to other stations or substations that are considered are only those that are operating at voltage levels between 200kV and 499kV. The SDT reviewed previous drafts and clarified the criterion to ensure that the qualification of voltage levels of 200kV and higher for these connections is more explicitly stated rather than implied.

Criterion 2.6

One comment was on the obligation for the RC with respect to IROLs. RCs are required to provide to its TOPs in its RC footprint the SOLs under FAC-014-2, Requirement R5.1. In particular, it requires the RC to provide specific information related to IROLs in the sub-Requirements of 5.1. The particular agreements between RCs, TOs and TOPs to enable the proper management of IROLs in compliance with the NERC Reliability Standards are beyond the purview of the guidance. The SDT points out that the delegation of functional obligations must be considered in these Requirements.

Criterion 2.8

A commenter noted correctly that Transmission Facilities under 2.8 that do not affect Transmission, in aggregate, for generation that is less than 1500 MW do not qualify under this criterion, even if the generation facility (plant) contain cyber systems that qualify under 2.1., (provided they do not qualify under other criteria).

Another commenter noted that, in the case where the generation is not owned by the TO/TOP would be at the mercy of the Generation Owner's (GOs) application of the standard even if the TO's facilities would not otherwise be in scope. The commenter is correct in that the TOs Facilities providing the connection would be deemed to be a medium impact. This is consistent with the impact of these Transmission Facilities on the BES.

Criterion 2.9

One commenter requested clarification on what an automated switching system is. Automated switching systems refer to systems implemented in software that perform the same automated protection functions as Special Protection Systems or Remedial Action Schemes.

Criterion 2.10

One commenter stated that the guidance document specifies that the SDT "chose the term 'each' to represent that the criterion applied to a discrete System or Facility". The commenter's interpretation of this statement is that a regional UFLS program which sheds more than 300 MW and is comprised of multiple independent UFLS relays in at different substations would not be given a Medium Impact Rating at the NERC or RRO program level and that an individual relay would only be given a Medium Impact Rating if that relay shed more than 300 MW by itself. The commenter's interpretation is partially correct in that individual independent relays that are part of a UFLS system that sheds 300 MW or more in the program Requirements, but do not shed the required load by a common control system, (e.g., they individually trigger independently, even if they are configured to trigger based on the same sensed conditions) do not qualify. However, if the individual relays are all triggered automatically by a common control system that determines

that conditions warrant the action (such as a control panel that triggers a system of relays in a substation), then they are part of a load shedding system that can automatically shed more than 300 MW and therefore qualifies. The commenter's assertion that a single relay that sheds 300 MW or more does qualify is correct.

The same commenter noted the statement on ERCOT's LaaR demand/response program is not considered as qualifying under this criterion and requested more general guidance in the Guidelines and Technical Basis section for this criterion that talks to these types of programs. The SDT has included a more general statement in this section.

Criterion 2.11

There was a comment that the Guidelines and Technical Basis section on this criterion incorrectly referenced a 300 MW threshold. The SDT has made the necessary correction.

Criterion 2.12

Many comments related to the portion of criterion 2.12 of Attachment 1 that is applicable to TOP Control Centers. Commenters stated that criterion 2.12 of Attachment 1 included all TOP Control Centers, not already categorized in the high impact category, as medium impact and that many smaller TOP entities' Control Centers should be categorized as low impact in the same manner that criteria were defined for generation and balancing authority Control Centers. Many commenters proposed alternate proposals for a threshold that could provide such a criterion to be used as a candidate for categorization as low impact, such as voltage levels lower than 200 KV or using throughput indicators similar to those used in the case of transmission substations in criterion 2.5. Others provided proposals to restructure the thresholds for all three impact levels for TOP Control Centers. One commenter also proposed an exclusion clause in criterion 2.12 that would be based on engineering analysis that demonstrated minimal impact to the BES. In response, the SDT did not find any such study that would be required by an existing NERC Reliability Standard.

As part of a consolidated response to more than one entity that provided comments on draft 2's CIP-002-5, Attachment 1, criterion 2.11 (which maps to criterion 2.12 in draft 3 and draft 4), the drafting team carefully considered comments to include a threshold for TOP Control Centers, but, to reiterate previous considerations and response to the comments related to that criterion (on page 35 of consideration of comments form A), such a threshold is not supported in consideration of the functions provided by those Control Centers. The largest concentration of cyber traffic is to and from Control Centers, and loss, compromise, or misuse of cyber systems at control centers constitutes a high risk to reliability. Furthermore, criterion 2.12 applies to "Control Centers" used to perform the functional obligations of TOPs, so it is only applicable to the extent the Control Center meets the criteria of the proposed definition.

While there is clear guidance in the NERC Reliability Standards that the SDT could use to determine bright lines for generation in the wide area (such as contingency reserve Requirements), the SDT did not find any in the Transmission area to support thresholds for TOP Control Centers. The source for transmission substation bright lines, based on throughput in a Transmission station or substation according to voltage level, provided easily measureable thresholds because of their localized nature: for a given single location, the application of the threshold criteria can be easily determined. There was no bright line that the SDT could find applicable and justifiable in a wide area situation for TOP Control Centers that control many interconnected Transmission Facilities in many locations. The SDT could not find any technical guidance, either in NERC technical studies, or in existing NERC Reliability Standards Requirements, on how the loss of interconnected Transmission Facilities could be used as a basis for establishing thresholds for TOP Control Center impact. The TOPs span of control is not limited to just Transmission lines, but to a large number of diverse Transmission Facilities that relate to the reliable operation of the BES. This complexity, together with the interrelated impact from the large number of diverse Functional Entity types that impact TOP functional obligations, make it very difficult to define a justifiable threshold that can be rationalized considering all the scenarios that could impact real-time operation for a TOP Control Center.

As stated in the guidance for CIP-002-5, the reasoning and purpose for the 1500 MW threshold for generation is different:

> "By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected."
>
> The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used."

Furthermore, the SDT has an obligation to be responsive to FERC Order No. 706, which was issued after a notice of proposed rulemaking, and several points from that order were reiterated in subsequent FERC Order No. 761. The SDT has discussed this issue very significantly in several face-to-face SDT meetings. In addition to the technical reasons and differences explained above, the SDT anticipates that any threshold for TOP Control Centers will likely be met with a directive countering such threshold upon filing for approval of these standards.

The SDT based its approach in the development of this criterion in consideration of the following comments and Directive from FERC Order No. 706 approving CIP Cyber Security Standards Version 1 and FERC Order No. 761 approving CIP Cyber Security Standards Version 4.

In its Order No. 706, Para 280, FERC supports the reasoning for its subsequent Directive in paragraph 282 with the following comment:

> "...it is difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be identified as a critical asset..."

The SDT points out that Medium and High Impact under Version 5 translate closely to "Critical Asset" under previous versions. The Directive in FERC Order No. 706, Para 282 further states:

> "Therefore, consistent with the discussion above, the Commission directs the ERO, through the Reliability Standards development process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets."

As explained earlier, the SDT's consideration of misuse of TOP Control Centers and the role they provide, pursuant to this Directive, do not support an exclusionary threshold from medium impact in CIP-002-5, Attachment 1.

In its Order 761 approving NERC CIP Cyber Security Standards Version 4, FERC commented in paragraph 21 that:

> "...Version 4 will offer an increase in the overall protection for bulk electric system components that clearly require protection, including control centers"

In the same Order 761, Para 57, FERC further commented with the following:

> "However, we continue to expect comprehensive protection of all control centers and control systems as NERC works to comply with the Requirements of Order No. 706."

Again, in the case of Generation and BA Control Centers, the SDT used the 1500 MW threshold for consistency with the rationale used for generation bright lines. As stated, no such source can be used for wide-area transmission in the non-CIP reliability standards or other published source.

Therefore, the SDT opted to keep criterion 2.12 as it applies to TOP Control Centers (i) to ensure that all TOP Control Centers are adequately protected, in the absence of technically justifiable thresholds for lower impact TOP Control Centers, (ii) because of the critical nature of their real-time reliability functions for the interconnected Transmission systems they monitor and control, and (iii) in consideration of FERC comments and Directives expressed in Order No. 706 and reiterated in Order No. 761.

Criterion 2.13

One commenter believes that the 1500 MW minimum specified in criterion 2.13 is excessive and unreasonably excludes a significant number of BAs from meaningful participation in protecting the BES from cyber-attack and that establishing criteria effectively eliminates significant numbers of interconnected control centers fails to address the specific concerns outlined in both FERC Order No. 706 and FERC Order No. 761. The SDT considered the MW distribution of BAs and determined that the 1500 MW is consistent with generation thresholds established (and approved by FERC in Version 4) in other criteria and is appropriate in including a significant number of BAs at the medium impact category. The SDT points out low impact cyber systems are still subject to protection Requirements.

Criterion 3.1

There was a comment that criterion 3.1 should specifically state that only Generation and BA Control Centers are included. While combination of the criteria for Control Centers currently results in only Generation and BA Control Centers, this criterion is intended to catch all Control Centers that have not already met a previous criterion in section 1 and 2 (high and medium impact). The current language conveys this intent.

Criterion 3.4

One commenter stated that the use of the terms “critical” and “initial system restoration” in criterion 3.4 is problematic. The commenter noted that initial system restoration is not a defined term and registered entities have regularly argued that none of their resources are critical as they have many options from which to draw upon. The SDT has made modifications to the criterion that uses language consistent to EOP-005-2 and defined terms.

The commenter also noted that the Low Impact Rating criteria needs to include automatic Load shed systems that do not shed sufficient Load to meet criterion 2.10. All Load shedding systems that are part of the BES are included automatically as stated in the Applicability section (section 4). For DPs, Load shedding systems that meet the qualifications in section 4 are included and are all included as medium impact.

CIP-003-5

CIP Senior Manager

A commenter expressed concern on the designation of the CIP Senior Manager by a "high level official" and whether that official could be the same person as the CIP Senior Manager. The SDT notes that the language regarding "high level official" is but one example in the measure. An entity is free to determine the best way to designate a CIP Senior Manager for its unique circumstance. This could be by high level official, by committee, through authorization from a board of directors, or from any number of other options.

The SDT received a comment that there was a concern that by only requiring the identification of the CIP Senior Manager by name that the Requirement was not auditable in instances where multiple individuals have the same name at the same company. The SDT appreciates that this is a very real scenario. However, the SDT believes that this is specifically the style of auditing that it sees is incompatible with the objectives it is setting out to achieve. The SDT believes that real cyber security program leadership transcends the name on the document. Audits, instead of verifying a name on a page, should instead validate the Requirement objective that the individual identified as the CIP Senior Manager is in fact leading and managing the implementation and continuous adherence to the CIP standards.

One comment indicated that "The CIP Senior Manager relies on both the definition in the CIP Glossary and the "Responsible Entity" verbiage in every standard in section 4." The SDT does not agree. The definition of a CIP Senior Manager stands alone. However, the Requirement itself is for the Responsible Entity (the entity obligated to comply with the standard) to identify a CIP Senior Manager.

Policy Requirements

One commenter expressed concern that the SDT was too prescriptive in its language around electronic access controls in the low impact policy. The SDT does not believe this to be the case. On the contrary, the SDT has some concern that it may have left the policy up for too much interpretation. However, the SDT believed that the entity is in the best place to determine the appropriate access controls for its given situation, while still implementing an ESP of some form.

Numerous commenters expressed confusion over the applicability of the policy Requirements. The SDT considered many approaches to this issue and believes that the applicability of these requirements is clear as drafted. Requirement R1 applies to high and medium BES Cyber Systems and states as much explicitly in the Requirement. The intent of

Requirement R2 is to apply to those assets that contain low impact BES Cyber Systems and not to the BES Cyber Systems themselves. This effectively allows the entity to track implementation of the policy at a higher level of abstraction (per asset rather than per BES Cyber System), and the SDT believes this will substantially reduce the burden of evidence required by the low impact policy. The reference to CIP-002-5 is to further clarify the intended reference to asset rather than BES Cyber System. The language following the numbered list specifying that "an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required" is part of the Requirement language of Requirement R2 and should be interpreted as such. This language was explicitly included to give the industry the assurance that this Requirement would be audited (sampled) at the asset (substation, generation plant, etc.) level and not the individual Cyber Asset level. The SDT also believes that entities will be able to implement internal controls to ensure the implementation of the cyber security policy at its low impact assets. The SDT does not believe that there is any double jeopardy between Requirements R1 and R2.

One commenter suggested that the SDT modify the Requirement language for the cyber security policies to clarify that multiple policy documents could "collectively" address the topics in the Requirements. The SDT agrees and has updated the standard to reflect this change.

The SDT received comments that Requirements R1 and R2 require annual review of the policy, but never explicitly require the policy to receive updates as a result of that review. The SDT believes this is implicit in the Requirement, and updates would occur as part of an entity's ongoing compliance with the Requirement.

Requirement R2

One commenter questioned the necessity of Requirement Part 2.4 considering that entities are not required to monitor for incidents to their low impact BES Cyber Systems. The SDT appreciates this concern. This element was specifically included because the SDT strongly believes that incident response is a key component of a resilient system. Even though an entity may not be constantly monitoring for a Cyber Security Incident at its low impact BES Cyber Systems, the SDT expects that should an incident be discovered, a plan should be in place for rapid execution.

Requirement R4

The SDT received comments requesting that language be added into the Requirement clarifying that the delegation authority may itself be delegated. The SDT considered adding language to the standard to clarify this, however, the SDT believed that the Requirement was clear as is and that there was no language that prevented this delegation. The SDT included the discussion on this topic in the Guidelines and Technical Basis section specifically to clarify this issue.

One commenter pointed out that Requirement R4 as written requires that the delegations from the CIP Senior Manager be updated within 30 days of the initial delegation. The SDT agrees this is confusing and has struck this language from the Requirement.

The SDT received questions on why it included the IAC language on the Requirement to delegate authority from the CIP Senior Manager. The SDT specifically included the IAC language because it believes that in a very large organization, it is likely that changes in personnel without adequate update of delegation documentation could result in very minor deficiencies that have little or no impact on the reliability of the BES. These are precisely the types of administrative violations that the SDT is attempting to eliminate from the CIP standards. The SDT believes that, given this is all a single Requirement, the documentation required in the third sentence of Requirement R4 is part of the overall process specified in the first sentence of the Requirement; consequently, the IAC language applies to all parts of Requirement R4.

CIP-004-5

General

One commenter believes that the evidence retention for verifying access should be less than the audit cycle (which is three years for BAs, RCs and TOPs), especially if the SDT plans to keep the quarterly reviews to verify that access has been properly removed. Entities are required to demonstrate compliance with the Requirements for the entire audit period for all NERC Reliability Standards, regardless of evidence retention Requirements.

One commenter noted that within each Background section (section 5) under the heading "Applicable Systems Columns in Tables" is missing the second sentence that appears in the other standards where Medium Impact BES Cyber Systems with External Routable Connectivity is also referenced in the Background sections. The SDT confirms that it intended that phrase to be consistent wherever that applicability term was used, and the SDT has modified the background to clarify that intent.

There was a comment that within CIP-004-5, the definition of EACMS appeared inconsistent with the definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards", and that it could result in misidentification, misapplication or inconsistent application of standards. The SDT has modified the background section with respect to EACMS to provide clarification that these are examples only that support the definition.

Requirement R1

A few commenters requested that Requirement R1 include the IAC language. In response, since the Requirement may be performed at any time during the quarter, the addition of the IAC language would not be appropriate.

One commenter requested clarification on the types of materials to be provided for security awareness on a quarterly basis. The Requirement is to provide an ongoing reinforcement that cannot be provided by an annual training Requirement. The SDT has written the Requirement to allow for flexibility in implementation by the entity. The measure provides some examples of how the entity may meet this Requirement.

A few commenters considered Requirement R1 to be administrative in nature and suitable for elimination pursuant to the SAR Paragraph 81 project. While this Requirement is partly administrative, it does provide the benefit of the entity being able to timely address and make staff aware of emerging threats and vulnerabilities. This awareness can improve security for the entity.

One commenter requested that Requirement Part 1.1 be modified as, "cyber security practices and/or physical security practices." The SDT clarified that the Requirement part applies to cyber security, which may include awareness on associated physical security.

Requirement R2

One commenter recommended that the training content Requirement Part 2.1 be moved to the measures. The SDT considered the training topics listed to be worthy of being listed as a Requirement for a minimal core competency in security practices. Entities are encouraged to add more topics as relevant to their needs.

One commenter recommended that Requirement Part 2.2 be modified to address newly registered entities. In response, the compliance dates for newly registered entities are addressed in the supplementary implementation plan provided with the Version 5 standards.

One commenter considers it is a security risk to address some of the concepts listed in Requirement Parts 2.1.1 through 2.1.9 with every single person with a need for physical or cyber access to a cyber system, regardless of his or her role. The SDT believes that, as written, the Requirement is flexible to allow the entity to design and implement a security training program that fits their needs. The Requirement does not preclude an entity from using a single or multiple training courses with differing depth in the training provided.

Several commenters requested clarification on the necessary training for personnel based on individual roles, functions, or responsibilities, including changes to roles, functions, or responsibilities. The SDT believes that, as written, the Requirement is flexible to allow the entity to design and implement a security training program that fits their needs. The Requirement does not preclude an entity from using a single or multiple training courses with differing depth in the training provided. How the training program is implemented is at the discretion of the entity.

One commenter requested that CIP Exceptional Circumstances be removed from Requirement Part 2.2, as this applies to numerous parts and is stated at the policy level. The SDT believes that, as written, the Requirement provides necessary guidance related to the Requirement without introducing the need to rely on or link to other Requirements.

One commenter requested clarification on whether the training required by Requirement R2 extends to contractors and vendor support staff. The SDT notes that, as written, the Requirement is clear that training is to be provided to anyone having authorized electronic access and authorized unescorted physical access.

One commenter requested that Requirement Part 2.1.9 be removed. The SDT considers the training topic relevant to address the vulnerabilities of internetworked systems and to address the risks of systems that are integrated and reliant upon data from other sources to perform necessary tasks (interoperability).

Requirement R3

Several commenters noted concerns regarding Requirement R3 where employee history is not available, including the identity verification necessary to perform the criminal history check, and how to comply with these instances. The Requirement provides for this, "If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed."

One commenter requested that the timeline for personnel risk assessments pursuant to Requirement R3 be modified to 10 years to align with other governmental standards and practices. The SDT is not clear if the commenter means performed every 10 years or reviewing the prior 10 years for criminal history. The SDT has kept the timing Requirement of the existing standards as approved by FERC Order No. 706.

Many commenters requested clarification for Requirement R3 that ongoing identity verification is not required. The SDT has noted in guidance and the implementation plan that identity verification is required only initially. However, the Requirement is written to be flexible to allow the entity to design and implement their personnel risk assessment program in a manner that meets their needs to confirm identity. For some, this may include performing subsequent identity verification or it could include confirmation of previous verifications.

One commenter noted grammar concerns with the Requirement R3 table parts. The SDT believes that the overarching Requirement provides the necessary context and clarity for the table.

One commenter stated Requirement Part 3.3 unclear as to whether the evaluation process includes an expectation of clearly defined evaluation criteria for approval/disapproval of the access request. The SDT has modified the Requirement to make this clearer.

Two commenters considered Requirement Part 3.4 unclear as to whether the entity is to perform the evaluation or permits the contractor or service vendor to perform the evaluation using its own criteria with an assertion to the entity of compliance and acceptability. The SDT believes that, as written, the Requirement is flexible to allow the entity to design and implement a personnel risk assessment program that fits their needs. The entity is responsible for ensuring that the obligations of the Requirement are met by their contractors and service vendors.

One commenter requested that the table parts for Requirement R3 be modified to require that a personnel risk assessment must be complete before granting access. The overarching Requirement R3 states that a personnel risk assessment is required in order to obtain access.

One commenter requested that Requirement Parts 3.5 and 3.6 include a clause that it is subject to applicable law and collective bargaining unit agreements. This concern is addressed in the guidance provided for Requirement R3. As written, the Requirement is flexible to allow the entity to design and implement a personnel risk assessment program that fits its needs.

Several commenters requested clarification on whose identity must be verified. As written, the Requirement is clear that personnel risk assessment is to be performed for anyone having authorized electronic access and authorized unescorted physical access. This is further defined in Requirement Part 3.4.

One commenter recommended consolidation of Requirement Parts 3.3 and 3.4 into Requirement Part 3.2. As written, the Requirement defines each individual element to be performed and that these are each elements contained within the program specified by Requirement R3.

One commenter considered Requirement Part 3.3 redundant of Requirement Part 3.2. Requirement Part 3.2 is the performance of the criminal history records check. Requirement Part 3.3 is the evaluation of the records collected under Requirement Part 3.2.

Requirement R4

A few commenters noted concerns regarding the efficacy of Requirement Part 4.2. The SDT considers this Requirement as a key element for security. The intent of the Requirement is to review the accounts residing on the systems with the

records of what accounts are supposed to be on the systems. This helps to provide an assurance that accounts have not been added through malicious code and that provisioning processes are functioning properly.

One commenter recommended that Requirement Part 4.2 be removed and provide it as an example of an internal control that the Compliance Enforcement Authority (CEA) would expect to see. The SDT considers this Requirement as a key element for security. The intent of the Requirement is to review the accounts residing on the systems with the records of what accounts are supposed to be on the systems. This helps to provide an assurance that accounts have not been added through malicious code and that provisioning processes are functioning properly.

Several commenters requested clarity in Requirement Part 4.3 related to which accounts and types are subject to an annual review. Individual user accounts, user account groups or user roles are required to be reviewed on an annual basis. User account groups or user roles are to be reviewed where these are used to for role-based management of access permissions. While review of other account types (i.e.: default account) is a good security practice, it is not a Requirement under the CIP Version 5 standards.

One commenter requested clarification of Requirement R4 regarding the word “verify” and how an entity is expected to provide evidence of access control. The Requirements mandate that access is limited to only those requiring said access. It is the responsibility of the entity to determine how they can demonstrate this limitation through the use of technical or procedural controls. The SDT believes the Requirements are written to allow flexibility in implementation to allow the entity to develop a program that meets its needs. The use of access controls lists, key control processes, and log books should be considered as options.

There was a comment that the phrase “based on need, as determined by the Responsible Entity” within Requirement Part 4.1 does not add anything meaningful to the standard. The SDT added the language based on industry comment concerns to help clarify that the appropriateness is determined by the entity and not by the CEA.

One commenter stated that the concept of role-based privilege management has not been established adequately in the Requirement. The SDT believes that Requirement Part 4.1 is written with sufficient flexibility to allow the entity to implement access control processes that meet their needs. The Requirement does not preclude the use of role-based privilege management. Requirement Part 4.3 has been modified to address this concern.

One commenter requested clarity on the measures for Requirement Part 4.2. The measures are examples of how the Requirement may be met. They are not an all-inclusive list of possibilities. It would not be feasible to list all options available.

One commenter noted concerns regarding Requirement Part 4.3 related to the level of access permission review to be performed. The detailed access privileges are to be reviewed to determine if they are appropriate. This can include review of access to file systems. As noted in the guidance, "The privilege review at least once every 15 calendar months is more detailed…"

Several commenters requested clarification regarding the verification of access to information storage locations pursuant to Requirement Part 4.4. As noted in Requirement Part 4.1, there are three distinct types of access noted; (1) Electronic access, (2) Unescorted physical access into a Physical Security Perimeter (PSP), and (3) Access to designated storage locations, whether physical or electronic, for BES Cyber System Information. The intent of Requirement Part 4.4 is the review of access to BES Cyber System Information only.

One commenter requested clarification on the scope of physical access controls for BES Cyber System Information in Requirement Part 4.1.3. Physical access control for BES Cyber System Information only pertains to the protection of hard copies of said information. The hard copies of BES Cyber System Information are not required to be within a PSP, and therefore, CIP-006-5 may not apply.

Several commenters requested clarification on the phrase "within the last seven years." In order to obtain or retain access, a person must have had a personnel risk assessment "within the last seven years" of when access was provided and ongoing. The Requirement is written to be flexible to allow the entity to design and implement their personnel risk assessment program in a manner that meets its needs. For some, this may include performing personnel risk assessments more frequently.

Requirement R5

One commenter noted that Requirement Part 5.1 does not distinguish between termination for cause and termination without cause. The SDT removed the distinction between types of terminations to meet FERC Order No. 706, Paragraphs 460 and 461, requiring immediate revocation for any person no longer needing access regardless of termination reason.

There were an abundance of commenters that noted that the time frame listed Requirement Part 5.2 is difficult to comply with and is unnecessarily short when the employee is remaining with the company if the transfer or reassignment was in the normal course of business and not for disciplinary reasons. The Requirement allows for the entity to review the access for the individual and retain access as long as necessary for transition from the prior position. The timing was determined to be necessary to meet the to meet FERC Order No. 706, Paragraphs 460 and 461, requiring immediate revocation for any person no longer needing access which includes reassignment and transfer. Note that the timing is based on when the entity determines that the individual no longer needs access, which may not necessarily be the same date as the transfer or reassignment.

One commenter requested clarification for the word "removal" in Requirement Part 5.1. Removal refers to rendering the individual unable to use the access. This may be accomplished through deletion, disabling, revocation, or removal. The SDT wanted to provide flexibility in allowing any of these means to be used.

A few commenters requested clarification regarding Requirement Part 5.4 on what scenarios would fall into this category that are not covered within Requirement Parts 5.1 to 5.3. Requirement Part 5.1 is removing the person's ability for unescorted physical access and Interactive Remote Access. This can be accomplished by revoking just these elements (i.e.: RSA, VPN, Active Directory). Requirement Part 5.4 is to clean up the remaining accounts for the users, such as access to applications, databases, and other systems.

One commenter had concerns that Requirement Part 5.5 could negatively impact the reliability of the bulk electric system in cases where there is a high movement of staff between locations. In such cases the password may change so many times that it impacts people's ability to access BES Cyber Systems (they forget the password due to the high change rate). The SDT believes that due to the capabilities of these accounts, prompt changing of the password is appropriate to minimize the risk from separated employees and contractors.

One commenter requested that "termination action" be replaced with "termination" in Requirement Parts 5.1, 5.3, and 5.4. Please see the Guidelines and Technical Basis section of the standard for additional information regarding a termination action. This section addresses the concerns noted.

There was a request that the phrase "and time" be removed from Requirement Part 5.3, as it is unnecessary, given the reference to a calendar day rather than a twenty-four hour period. The SDT agrees with that clarification and has modified the Requirement to address this comment.

One commenter considers the time limits for revoking access upon terminations to be an extreme challenge. The SDT used the timeline for terminations to meet FERC Order No. 706, Paragraphs 460 and 461, requiring "immediate" revocation for any person no longer needing access, including all terminations, and the SDT believes the approach reflected in the standards is a reasonable means of accomplishing the directive.

One commenter requested consideration of Requirement Parts 5.4 and 5.5 to include Physical Access Control Systems (PACS) since some cyber assets in a PACS can also have individual user and shared accounts. The SDT considers all PACS devices to be subject to the same Requirements, regardless of impact categorization. While removal of access and changing of shared account passwords on all assets is a good security practice, it is not a Requirement under the CIP version 5 standards except where noted in Requirement Parts 5.4 and 5.5.

One commenter requested that Requirement Part 5.5 be changed to 35 days for consistency with other monthly Requirements. The time parameter in this requirement is different than the periodic performance time periods in requirement parts that use the 35 calendar days period. The SDT does not consider this action to be an ongoing monthly Requirement similar to those noted in CIP-007-5.

CIP-005-5

High Water Marking

There was a comment that per the Guidelines and Technical Basis section for CIP-005-5 Requirement R1, all of the Cyber Assets and Cyber Systems, even other BES Cyber Systems of lesser impact, within the Electronic Security Perimeter (ESP) will be elevated to the level of the highest impact BES Cyber System present in the ESP. The commenter recommended that this concept be included in section 5 background of every standard, not just in CIP-005-5 guidance. The SDT considered whether to include this in the background in each standard, but determined that it was most appropriate to make clarifying changes to the Guidelines and Technical Basis section in CIP-005-5.

Background Section

One commenter suggested that to ensure consistency between the standard and the list of "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" to update this section to reflect the same definition as used in this list. In response, these do not change or modify the definitions, but provide further background and guidance information.

There was a comment in the Guidelines and Technical Basis section that stated that an ESP is required around networks even if standalone regardless of impact classification. The commenter ask the SDT to confirm the Requirement in CIP-005-5 do not imply a list of Low Impact assets is needed. In response, the SDT has added the word 'applicable' before BES Cyber Systems in the guidelines to clarify this.

A question was raised regarding the scenario where a network switch may be divided into multiple ESPs and has one port outside the ESP that provides no routing between VLANs. Furthermore, the commenter questioned the following regarding Requirement R1.5: "does two distinct machines need to be utilized, one as a fire, and one as intrusion prevention or can it be done via one device and when the EAP is segmented into multiple network where one LAN is critical and one is non-critical; and does an IDS need to be on each network segment monitoring inbound/outbound traffic on the segment or just at the EAP monitoring inbound/outbound traffic." In response, the SDT is writing Requirements for the "what's" and leaving the "how's" to the entities to implement in ways that best protect their environments while still meeting the intent of the Requirement. These standards cannot and should not be exactly prescriptive in every possible technical situation. If that were the case, they would be constantly outdated or they would actually increase our risk by presenting a monoculture to adversaries where a vulnerability in one would be the same vulnerability in all. For the VLAN question, the SDT notes that an ESP (a logical border) is required around every network

to which a BES Cyber System is connected and any external connectivity to other networks must be controlled with an Electronic Access Point (EAP). The SDT has chosen to not prescribe precisely what protective functions must reside on what devices or what the standard network architecture must be for the reasons noted above. A method for detecting malicious communication must be present at each EAP for control centers (high and medium impact).

Consideration of Data Diodes

One commenter stated that CIP-005-5 should consider data diodes which possibly would exempt systems only with a data diode connection from "external connectivity" provisions. In response, the SDT notes that the definition of 'External Routable Connectivity' includes the term 'bi-directional' in order to handle data diode situations that physically enforce a uni-directional flow. Therefore systems behind a data diode do not have External Routable Connectivity.

Requirement R1

One commenter asked what the rationale was for standalone networks that have no external connectivity to other networks to must have a defined ESP. The intent is to define the 'Associated Protected Cyber Assets (PCAs)' and the high watermarking concept. In response, in previous versions of the CIP standards, Cyber Assets on the same network (within the same ESP) with a Critical Cyber Asset had to meet the CIP-007-5 Requirements. The definition of an ESP in Version 5 is required to carry this same concept forward, as well as to handle the new issue of what level of protection is required for these Cyber Assets now that we can have multiple impact levels within the same ESP. Therefore, if a BES Cyber System is connected to a routable protocol network, even an isolated network, the ESP (which is simply the 'logical border') must be defined as that also defines the 'Associated Protected Cyber Assets'. All of these Cyber Assets within that ESP then become 'Associated PCAs' of the highest impact level BES Cyber System in the ESP.

A commenter stated that the definition of Electronic Security Perimeter allows the Responsible Entity to serially connect certain Cyber Assets to a communications processor that, in turn, communicates to other Cyber Assets using a routable protocol, and in doing so declare that the Digital Protective Control Devices do not need to reside within the ESP and therefore are not subject to CIP standards. In response, the SDT notes that connectivity is no longer a filter that kicks Cyber Assets out of scope and makes them 'no longer subject to the CIP standards'. Cyber Assets are subject to the CIP standards based on their functionality and resultant potential impact to BES reliability. It is true that certain Requirements, such as CIP-005 Requirement R1, only apply if a BES Cyber System is connected to a routable protocol network, but that is because its main point is to secure what can enter or leave routable protocol networks on which BES Cyber Systems reside. CIP-005-5 is no longer a 'scoping standard' for what is or is not in scope of the CIP standards as a whole as it has been in the past. BES Cyber Systems are in scope of the CIP standards. CIP-005-5 Requirement R1

therefore is now back to a network security Requirement that requires controlling what can enter or leave a routable protocol network.

There was a comment that requested clarification text added to the Guidelines and Technical Basis section for Requirement R1, specifically Requirement Parts 1.3 and 1.5, to remove the operational barriers that may prevent entities from implementation encryption among sites on a BES Cyber System network using either encrypted tunnels or tunnel-less encryption technologies. The commenter provided possible language to be added to CIP-005-5 Requirement Parts 1.3 and 1.5:

> "Some Entities employ encryption as a strong measure for securing communications among discrete physical sites (e.g. data centers and control centers). Encryption (either via encrypted tunnels or group encrypted transport) effectively satisfies the establishment of 'discrete Electronic Security Perimeters' as referenced in Section 4.2.3.2 of each Applicability section. Provided the termination points of the encryption are protected within Physical Security Perimeters, the Requirements for CIP-005-5 R1.3 (inbound & outbound access permissions and deny-by-default) and CIP-005-5 R1.5 (inbound & outbound malicious traffic inspection) may be achieved at central firewall(s) protecting the BES Cyber System network to which the ESPs are connected. For traffic communicating within the encrypted network, the CIP-005-5 R1.3 and CIP-005-5 R1.5 Requirements do not need to be duplicated at the encryption endpoints. This enables effective implementation of encryption, which might not otherwise be operationally feasible if traffic inspection were required inside of the protected network due to the latency and convergence delays that are introduced."

In response, The SDT believes the Requirements as written do not preclude the use of encryption. However, encryption alone does not constitute an ESP or EAP. For example, if malware is introduced via portable media to a BES Cyber System and it tries to communicate outbound to a command and control server to get further instructions or provide remote access to the BES Cyber System, the fact that there is an encrypted tunnel up to the next higher level site does not provide an EAP where the communications are inspected to determine whether they should be allowed or not. If an entity wishes to state that a wide area network of sites are within one ESP, regardless of encryption, then all Cyber Assets (which includes, e.g., all communication or networking equipment) within that very large ESP become associated PCAs and must meet the Requirements of the highest level BES Cyber System in the ESP. The standards do not preclude doing this, but there are implications that Responsible Entities should take into account.

For Requirement Part 1.2, one commenter stated that the definition of External Routable Connectivity does not anticipate a situation where serial protocol may be used over IP connectivity. The commenter provided an example, where communication between two devices may take advantage of the Ethernet ports on the devices, but run serial

protocol between the devices. Furthermore, the commenter stated that by explicitly stating, "routable protocol connection" in the definition and focusing an auditor's attention on the connection, the auditor may see the Ethernet port being used and determine noncompliance. Lastly, the commenter recommended deleting the word "connection" at the end of the definition of External Routable Connectivity. In response, the SDT disagrees. The definition is based on the type of protocol, not the transport used. Ethernet is not a routable protocol; it is a transport medium with no concept of network level addressing. It should not be assumed that transport determines protocol as routable protocols can be carried on serial lines and non-routable protocols can be carried on Ethernet. It is not a matter of transport but the protocol.

There was one suggestion in Requirement Part 1.3 that the term "permissions" can be substituted with the term "controls" to align the term with the language in the measure. In the measure, the SDT uses "access control list" as an example, and the SDT has not made a change to the Requirement language, as the use of "permissions" stems from prior versions of the CIP Cyber Security Standards. The SDT believes that the term is well-understood in this context.

One commenter had a concern with the phrase "outbound access permission" in Requirement Part 1.3 which calls for requiring inbound and outbound access permission, including the reason for granting access and denying all other access by default. The commenter furthered stated that target threat vectors to the BES Cyber Systems would be inbound to those networks and those attempts inbound into the networks need to be monitored and controlled, and that while there is the possibility that could be malicious code internal to these networks communicating, that tracking all outbound communication from one trusted network to another trusted network would more than double the monitoring that is required. In addition, the commenter stated that the CIP standards have other controls to help monitor and detect the malicious code internal to the networks. In response, the SDT does not think that having an outbound rule in an EAP that allows communication from all hosts on one internal network to all hosts on another internal network is burdensome. The benefit received of being alerted to BES Cyber Systems trying to suddenly communicate with unknown networks or hosts we believe outweighs the burden of such rules. The SDT is not prescribing the level of granularity of these rules. The intent is just that EAPs function as EAPs and don't have rule sets that allow a BES Cyber System to talk to any device in existence. The Requirement is in essence "you shall not blindly trust all hosts inside the ESP to talk to any device on earth". It is up to the entity how granular they control what the hosts inside the ESP can talk to. Some may go extremely granular and specify exactly what host can talk to what host over what port; some, due to the frequency of change or other reasons, may limit it to anything on this network can talk to anything on these other internal networks. Both are compliant. But BES Cyber Systems should probably not be able to communicate directly with all home PC's on the cable company's consumer broadband network or to any machine in unfriendly nations.

One commenter stated that Requirement Part 1.5 needed to include an explicit Requirement for real-time monitoring and/or alerting upon detection of known or suspected malicious communication. The SDT notes that monitoring and alerting is addressed in CIP-007-5, which also includes Electronic Access Control or Monitoring Systems (EACMS) (CIP-007-5, Requirement R4).

With regards to Requirement R1.5, one commenter proposed the following language: "Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. ESP-to-ESP communications within a discrete BES Cyber System shall be excluded." As an example, the communication links between a primary transmission control center and its backup control center shall be excluded. The SDT disagrees. If malicious code is trying to replicate itself from a primary control center to the backup Control Center, then this Requirement should be in place. Having both the primary and backup Control Centers compromised defeats the purpose. If the primary system is compromised via malware or remote control Trojans to the point that its integrity is gone and the entity needs to fail over to the backup while the primary is rebuilt, the backup needs this protection from the malware on the primary system. If the malware walked into the primary system via portable media or other means, an Intrusion Detection System (IDS)/ Intrusion Protection System (IPS) type system may save the backup system from compromise as well.

Another comment regarding Requirement Part 1.5 states that the Requirement is still geared towards implementing an IDS/IPS and that an IDS would not provide the additional protection for an ESP if a firewall failed. Also, the commenter noted that an IDS or IPS would provide no protection against an insider threat. The commenter closed by stating that "malicious" activity cannot be determined strictly by watching for an activity and that traffic to an ESP which is malicious may in fact appear to be normal. The qualification of "malicious" vs. "normal" requires knowing an actor's intent, which cannot always be gleaned from log entries, traffic patterns or signatures. In response, the SDT has invested many hours in these very discussions and has arrived at the current Requirement. The Order makes it clear that the alternate control is also not simply another firewall. Having two firewalls in sequence would provide no value as the rule sets would be identical. The solution the SDT arrived at for an alternate control at an EAP was to detect malicious traffic (usually implemented in today's technology via IDS/IPS as noted, but not prescribed). This would allow that if the firewall was misconfigured (e.g. an admin puts in a temporary any/any/all rule for troubleshooting and forgets to remove it after testing) then at least there would be this alternate control looking for malicious traffic and providing some means of protection which the SDT believes is the intent of the Order. As to the issue with "malicious" implying knowledge of an

actor's intent, the SDT has responded to this in previous drafts by inserting the words "known or suspected" to clarify that it is only malicious traffic that is previously known or suspected to be malicious.

Relating to requiring IDS and IPS to have firewalls, one commenter stated that it may be onerous compared to the benefit received. In response, the SDT disagrees. The SDT has already scoped this Requirement to the highest impact BES Cyber Systems which should be subject to the more stringent Requirements. The SDT believes that the benefit received from detecting malicious communications into and out of control centers far outweighs the burden.

One commenter asked for SDT clarification related to the ESP, External Routable Connectivity, and whether serially connected Cyber Assets are within scope for Requirements applicable to BES Cyber Systems with External Routable Connectivity. The SDT confirms that all BES Cyber Assets are in scope of all the CIP Version 5 standards. However, for certain Requirements, the type of connectivity limits applicability. EAPs for example, are only required around routable protocol networks to control what can get into and out of these networks. There is no EAP for a serial connection if there is no routable protocol running over it. Note that it is protocol based, not transport based. Routable protocols can run over serial transports. The same holds true for ERC – it is routable protocol based.

Requirement R1 VSLs

There was a comment that the language in the VSL should match the same language and logic as in Requirement R2. An example was provided that, the Responsible Entity should have a low VSL for not having a sub-part in its documented process, medium for not implementing one of the applicable items, high for not implementing two applicable items and severe for not implementing three applicable items, and thus, would result in a more consistent application throughout the standard. The SDT notes that it modified the VSLs for Requirement R1 in response to comments from draft 2 because of the difficulties and impracticalities of determining the measurements for graduated VSLs for Requirement R1.

Requirement R2

There was a clarification request for Requirment Part 2.2 with regards to allowing that encryption may be terminated at a firewall that protects an Intermediate Device in additoin to the Intermediate Device itself. The SDT believes that the definition of Intermediate Device provides sufficient flexibility in implementation to allow for what the commenter had requested. Additional references regarding the Intermedate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested clarification of how CIP-007-5 Requirement Part 5.1 and CIP-005-5 Requirement Part 2.3 differ. CIP-007-5 Requirement Part 5.1 refers to all user authentication; whereas CIP-005-5 Requirement Part 2 only refers to remote access.

There was a request that "where technically feasible" be added to Requirement Parts 2.2 and 2.3. The language "where technically feasible" is included in the overarching Requirement R2 to recognize that this applies to all of the Requirement Parts contained in Requirement R2, not just Requirement Parts 2.2 and 2.3.

Several commenters stated that CIP-005-5 Requirement Part 2.1 be modified to address situations where the Intermediate Device can be locally accessed (a local administrator, for example) inside the PSP. The SDT believes that, as currently written, the Requirement provides the level of protection necessary in that the Intermediate Device cannot be within an ESP and thus provides the necessary protection of the Cyber Assets within the ESP. The remaining controls for the Intermediate Device(s) provide a defense-in-depth proteciton of those systems. Additional references regarding the Intermedate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter considered that CIP-005-5 Requirement Part 2.2 does not achieve the intention, which is to have traffic inspected by the IDS in an unencrypted state. The SDT notes that, as written, the Requirement and definition of Intermediate Device, collectively; provide sufficient flexibility in implementation to allow for what the commenter has noted. It is at the entity's discretion to design their Interactive Remote Access infrastructure and monitoring to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. Please see http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested clarification of CIP-005-5 Requirement Part 2.1 regarding the protections to be afforded to an "Intermediate Device". Per the definitions of Intermediate Device and Electronic Access Control or Monitoring Systems, these devices are subject to the protection of EACMS.

There was a request for clarification of CIP-005-5 Requirement Part 2.2 as to the reasonableness to include traffic between the "Intermediate Device " and device(s) within the ESP to be in scope of CIP, as it traverses an EAP. Many instances of Interactive Remote Access originate from systems that are not within a trusted network or across the

Internet. The encryption is required to terminate before going into the ESP through an EAP. It is at the entity's discretion to design their Interactive Remote Access infrastructure and monitoring to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested that CIP-005-5 Requirement Part 2.2 be modified as "Interactive Remote Access sessions must utilize encryption to an Intermediate Device." The SDT believes that, as written, the Requirement language achieves the same concept and result.

A recommendation was made that CIP-005-5 Requirement Part 2.3 is modified as "Interactive Remote Access sessions must utilize multifactor authentication to an Intermediate Device." The SDT considered authentication to be necessary for the session, not for each device. The user may not actually log into each Intermediate Device itself.

A request for clarification was made of CIP-005-5 Requirement Part 2.2 regarding whether the "Intermediate Device" is expected to provide the encryption or if two devices are envisioned for compliance. The SDT believes that, as written, Requirement and definition of Intermediate Device, collectively, provide sufficient flexibility in implementation to allow for what the commenters have noted. It is at the entity's discretion to design their Interactive Remote Access infrastructure to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested clarification of CIP-005-5 Requirement Part 2.3 on whether the multi-factor authentication is required for the Intermediate Device, for access to the EAP or to the individual Applicable Systems. The commenter suggested the language to read "Require multi-factor authentication for initiating all Interactive Remote Access Sessions." The SDT considered authentication to be necessary for the session, not for each device. The user may not actually log into each Intermediate Device itself.

One commenter requested clarification of CIP-005-5 Requirement Part 2.1 on whether VPN is an acceptable form of remote access. It is at the entity's discretion to design their Interactive Remote Access infrastructure to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There

are case examples showing differing implementations. Please see http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

CIP-006-5

General

There were comments that CIP-006-5 does not require an entity to define a Physical Security Perimeter (PSP) and wonders if entities must assume that it is required. In response, the SDT notes that access points to the PSP must be controlled, which by definition, requires the PSP. It is not necessary to have an additional Requirement stating the existence of a PSP.

Background Section

One commenter stated that the background section includes a definition/description of "Medium Impact BES Cyber Systems with External Routable Connectivity," that notes an exclusion in the following sentence: "This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity." When this definition/description of Cyber Systems is used for the applicability in Requirements such as CIP-006-5 Requirement Parts 1.2, 1.4, and 1.5, it is used with the added inclusion of "and their associated...PCA." It appears the inclusive "and associated PCAs" statements in the Requirements negate the exclusion statement from the "Background," and makes the intended applicability of such physical security Requirements to specific Cyber Assets unclear for Cyber Assets without direct external connectivity which reside in the same ESP as Cyber Assets with direct external connectivity. In response, the exclusion in the background section states that it only applies to those Cyber Assets which are part of the BES Cyber System and not PCAs.

Requirement R1

One commenter stated that the deficiency correction language should not be added to CIP-006-5 Requirement R1 because it is a binary Requirement to either have a plan or not. The SDT notes that while the possession of a plan is binary, the implementation is not. Entities must document a plan with all of the applicable table parts and implement the plan at applicable BES Cyber Systems.

One commenter noted that the term "BES Cyber Systems without External Routable Connectivity" should be just "BES Cyber Systems". The SDT notes that "without External Routable Connectivity" is used to distinguish lesser obligations than those applying to "BES Cyber Systems WITH External Routable Connectivity".

Several commenters stated that CIP-006-5 Requirement R1 does not answer the question of how big an opening needs to be before it is considered an access point. In response, the SDT does not agree this question needs to be answered in a

standard's Requirement. This is an implementation-specific question. An entity may choose 96 square inches as its general measure, but that should not be the Requirement. Specifying exactly the qualifications of an access point would go beyond just the 96 square inch Requirement and likely cause significantly more confusion than currently exists.

One commenter did not agree Requirement Part 1.3 is responsive to the directive in FERC Order No. 706, Paragraph 573 to provide layered and complementary security procedures. In response, the SDT notes that in paragraph 575, the Commission specifically states it was not the intent to create an inflexible rule of redundant access control. The proposed Requirement meets the objective of having multiple physical access control measures. The Cyber Asset independence of these measures is not material to meeting the directive.

More than one commenter argued that Requirement Part 1.3 presents technical challenges without any additional security benefit. They request NERC to provide compliance feedback to industry demonstrating that "one or more" physical access methods have proven ineffective. In response, the SDT is addressing the directive in FERC Order No. 706, Paragraph 572. The SDT believes the proposed wording provides the most security benefit to the industry while still meeting the FERC directive.

One commenter suggested that for Requirement Parts 1.5 and 1.7 to remove the 15 minute maximum timeframe limit for issuing an alert. In response, the SDT notes that for physical security breaches, the threat is automatically severe and immediate and the 15 minute timeframe is necessary to provide a minimum expectation for issuing an alert.

One commenter proposed the words "of the unauthorized access" should be added to the end of Requirement Parts 1.5 and 1.7, but this would be redundant since detection is already qualified singularly in the Requirement Part.

There was a request for clarification if monitoring is needed on PACS inside a PSP according to part 1.7. In reviewing the possibility of combining Requirement Parts 1.5 and 1.7, the SDT found that monitoring and alerting Requirements applying to PACs could be interpreted to mean those inside a PSP. To clarify, the SDT notes that entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

One commenter stated that in Requirement Parts 1.5 and 1.7, BES Cyber Security Incident Response Plan is not a defined term and should not be capitalized. The SDT agrees and has made this change. Furthermore, the commenter noted that unauthorized physical access should not automatically trigger the incident response plan because the physical security

team and incident response team are often separate groups, and a single instance of a detection of unauthorized physical access is not necessarily a Cyber Security Incident. The SDT notes that an attempt to compromise the PSP is by definition a Cyber Security Incident, and the organization of physical security and incident response teams should not preclude the Requirement to identify the Cyber Security Incident. The physical security team's response to unauthorized physical access could be part of the organization's incident response plan.

Several commenters stated that Requirement Part 1.7 should be modified to require response within 15 minutes of the detection rather than the actual incident, consistent with Requirement Part 1.5. The SDT agrees and has made the clarification.

One commenter proposed that Requirement Parts 1.5 and 1.7 be combined because they use similar wording, but the SDT believes entities benefit by emphasizing the applicability to PACS outside of the PSP.

There was a comment that stated that Requirement Parts 1.6 and 1.7 should include badge readers outside of the PSP and access cannot be controlled as specified. In response, these Requirement Parts are separated because they must be monitored differently than those Cyber Assets inside a PSP. The SDT also notes that badge readers, by themselves are not necessarily considered PACS if they do not control the controlling, logging or alerting of access.

One commenter noted that a responsible entity needs to monitor each PACS system for unauthorized physical access to a PACS. However, there is no Requirement that the PACS be contained within a PSP. Therefore, a question was raised as to how does one control physical access to the PACS? In response, the SDT notes that PACS must control access according to Requirement Part 1.1, which is not the same level as Requirement Parts 1.2 through 1.5, but some form of access control must still exist for the entity.

Several commenters noted that Requirement Part 1.7 requires coordination with the incident response team, but CIP-008-5 does not apply to PACS. In response, the incident response plan does not apply to individual Cyber Assets, but compromise of a PSP and associated PACS is by definition a Cyber Security Incident affecting a BES Cyber System.

One commenter requested clarification on whether the issuance of an alert according to Requirement Parts 1.5 and 1.7 is automated, manual, or by choice. The SDT clarifies this is by choice of the entity.

There was a suggestion that there is a discrepancy between the change description stating PACS does not need to be inside a PSP and Requirement Parts 1.5 and 1.7 stating obligations for monitoring and alerting for unauthorized access to PACS. In response, Requirement Parts 1.2 through 1.5 applies to the BES Cyber System. PACS have a less stringent obligation in Requirement Part 1.1 to have a plan for restricting unauthorized access, but this is not the same obligation as having a PSP. The SDT has clarified the change rationale for Requirement Part 1.1.

One commenter stated that Requirement Part 1.8 should add "initial" before entry to align with the visitor control program. In response, the situation allowed for in the visitor control program is to avoid an escort continually signing in a visitor needing to perform a maintenance activity. This is not the same concern for authorized personnel who typically badge in each time without the overhead of an escort.

One commenter stated that Requirement Part 1.9 should be moved to data retention. In response, the retention of these logs serves the reliability objective of having access logs to support incident identification and response.

Requirement R2

There was a comment that the CIP Exceptional Circumstances should be removed since it applies globally at a policy level. In response, the CIP Exceptional Circumstance provision is controlled at a policy level but does not apply globally to all Requirements in the standard. The standards specify which Requirements the exception may apply to as a response to the FERC Order No. 706 beginning with paragraph 372, which directs additional guidance on policy exceptions.

Several comments stated that the Requirement could allow a visitor to go a long span of time without signing out. In response, the SDT notes the scenario of brief exit/entry intervals provided in comments is the purpose for allowing this provision. Specifying what timeframe constitutes the necessity of an exit sign-out goes beyond the security benefit provided by this Requirement Part.

Several commenters noted that the measure in Requirement Part 2.1 does not match the Requirement because the evidence does not demonstrate continuous access but discrete points in time. In response, the Requirement to have a program that provides continuous escorted visitor access can be measured by the program document. Evidence of compliance with the procedure requires discrete sampling to provide assurance in the implementation of the program.

One comment was that Requirement Part 2.2 would require manual or automated logging of entry and exit from the physical security perimeter and the Requirement for egress has not been explicitly defined as a Requirement. In response, egress logging has been required since CIP-006-3.

There was a comment that Requirement Part 2.3 should be moved to data retention. In response, R2.3 was not included as an evidentiary requirement. The SDT notes that the retention of these logs serves the reliability objective of having access logs to support incident identification and response.

Requirement R3

One commenter stated that Requirement R3 should have the language allowing an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R3 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One comment was that the 24 month interval in Requirement Part 3.1 is excessive for a normally occupied control center. In response, a normally occupied control center would also receive a significant amount of testing in the operation of access control. The objective this Requirement primarily addresses field assets where access is not tested as frequently, and the timeframe is appropriate for these assets.

Guidelines and Technical Basis

Several commenters recommended modifying the section dealing with alarms to be from “immediately after” an incident to “within 15 minutes.” This better aligns with the Requirement and the SDT agrees.

CIP-007-5

General Comments

One commenter requested guidance on how to comply with CIP-007-5 Requirements on Medium BES Cyber Systems serially connected devices with regards to patching, anti-virus, etc. on a large number of programmable protective relays; and also why other measures implemented for substation assets, such as physical protection, are not adequate. In response, the SDT notes that BES Cyber Assets by definition can have an impact on BES reliability and therefore require basic cyber security protections offered by CIP-007-5 regardless of their connectivity. For patch management, the intent is that entities know about the security patches that are available for their BES Cyber Assets, what vulnerabilities they represent, and mitigate those vulnerabilities. If a security patch for a device is only exploitable over a routable protocol connection and the device is only attached serially with non-routable protocols, then that patch would be documented as not applicable. The anti-virus Requirements and guidance already mention that the entity is to document and implement how they protect against the introduction of malicious code to the BES Cyber System. For some of the devices in the example, the entity may document that there is no method to introduce malicious code.

Effective Dates

One commenter raised a concern that the effective date of the order providing applicable regulatory approval, and Requirement Part 5.2 shall become effective 12 months later, as to provide entities more time to identify and inventory all enabled default or other generic account types. In response, it is the intent of the SDT that the entity has the accounts inventoried on the effective date, not one year later. That is why there is a two to three year implementation period so that all these prerequisite activities have sufficient time to be completed so that the entity is fully compliant on the effective date. The Requirements that require periodic reviews may have their first performance take place after the effective date, but that is outlined in the implementation plan.

Requirement R1

One comment stated that a new term of “Control Center Environment” was introduced in this standard and it could potentially have a different meaning than “Control Center”. The commenter requested clarification, and in response, the SDT agrees and has changed the term to “Control Center.”

For CIP-007-5 Requirement Part 1.2, several questions were asked about the phrase, “Protect against the use of unnecessary physical input/output (I/O) ports used for network connectivity, console commands, or removable media.” Introduction of physical port protection is “assumed” to refer to logical ports only. First, a question was raised about

strong physical access controls to BES Cyber System be a compensating control here. Second, will having the BES cyber systems in locked cabinets suffice? The Requirement is not clear if the protection has to be on the individual devices. The measures indicate signage as a potential control however this would not satisfy the Requirement the way the Requirement is written. For CIP-007-5 Requirement Part 1.2, the commenter sought clarification regarding physical I/O ports that are externally accessible. For example, most servers have PCI slots, CPU slots, memory slots, etc, which are physical I/O ports. As the standard is currently written, it would seem organizations need to disable these ports. Additionally, the language "console commands" is too ambiguous. In response, the SDT notes that many of these issues are addressed in the included guidance. FERC has stated that the PSP does not meet the intent of their Order. The SDT agrees with the 'console commands' comment and has added additional guidance to address it.

For CIP-007-5 Requirement Part 1.1, several comments were made about the phrase, ""If a device has no provision for disabling or restricting logical ports on the device, then those ports that are open are deemed needed." The Requirement does not provide any provisions for limiting access to those ports or services that cannot be disabled. The Requirement's measures ask for host-based protective measures. For those devices that are not capable of providing localized protective measures, such as relays, there is a question as to how this Requirement would be met. Previously, when a port or service could not be disabled, a TFE would require mitigation of the potential vulnerability. Under CIP-007-5, if the entity leaves these ports and services open they are in compliance but there is a question of whether the vulnerability of the device still remains. In response, the SDT notes that the Requirement does provide provision for those ports and services that cannot be disabled which is the phrase in question. If a device has no provision for disabling or restricting the ports, they are deemed "needed" and the Requirement only requires "unneeded" ports to be disabled. The intent is to not require TFEs for devices where the device does not allow for the Requirement to be met. The Requirements in CIP-005-5 for limiting inbound and outbound communications at the ESP is a mitigating factor for devices like this that do not allow for their "unneeded" ports to be disabled.

Requirement R2

There was one comment that stated the rationale specified a 30 day time frame while the Requirement states 35 days. The commenter requested that the rationale section be revised for consistency with the Requirement language. In response, the SDT agrees and has changed the rationale to 35 days to agree with the Requirement.

One commenter suggested adding "with External Routable Connectivity" to the Medium Impact applicability for the patch management Requirements within Requirement Parts 2.1 through 2.4. As justification, the commenter stated that they understand the comments of the SDT; however, the commenter believes that a combination of no external routable

connectivity, frequency of access to medium impact facilities, and policies reduces the risks to those facilities from the insider that would introduce threats ("thumb drives, laptops, smart phones") into the environment to an acceptable level. While devices with no external connectivity may have some physical access risks associated with the use of thumb drives, laptops, etc., the fact that they are isolated from other BES devices must be considered when addressing appropriate protections. The lack of external connectivity reduces the risks to that isolated device; therefore, the risk to the BES is minimal. Additionally, physical security is adequate mitigation from the external threats as once physical security is breached; there are other immediate and evident concerns that do not involve BES Cyber Systems. Alternatively, a request was made that the timeframes for Requirement Parts 2.2 and 2.3 be revised to 90 days for Medium Impact BES Cyber Systems. In response, while routable protocol connectivity is a way that systems can be compromised, it is not the only way and in many examples today is not the primary way. Insider threats (intentional and unintentional, from both employees and non-employees, from both portable media and support laptops) are means in which systems are compromised today. Therefore the intent of this Requirement is to remain aware of the vulnerabilities in the BES Cyber Systems through the security patches that are released for them and analyze and mitigate those vulnerabilities. If a system has no connectivity and a security patch is released that can only be exploited via network connectivity, then that vulnerability is already mitigated and the patch is not applicable. As to the 90 day alternative, the SDT believes that a timely analysis and plan are necessary due to the nature of the environment we are in where 'Patch Tuesday' is immediately followed by 'Exploit Wednesday' as attackers quickly reverse engineer released security patches to create and release exploit code. The SDT has not put a maximum timeframe on implementation due to numerous reliability concerns, but the analysis and mitigation planning needs to occur in a timely fashion.

There was a comment that Requirement Part 2.1 requires the Responsible Entity to identify a source or sources that the entity will track for the release of cyber security patches. Furthermore, the commenter stated, *"the corresponding guidance suggests that the third-party SCADA system vendor is an appropriate source for patch availability notification. The ability of a Responsible Entity to wait until a SCADA system vendor "certifies" a patch before requiring the Responsible Entity to begin the assessment and follow-on patching process introduces unnecessary risk to the BES. There is a significant difference between assessing a patch for applicability and assessing a patch for installability. An applicable patch may be found to be incompatible with the third-party vendor's systems, would not be certified, and should not be installed. That does not mean the vulnerability being addressed by the patch should not be mitigated, rather it is incumbent upon the Responsible Entity to protect its systems in a timely manner. The Responsible Entity needs to select a patch availability source that is timely, including the original patch provider and well recognized general information providers like US-CERT, SANS @Risk, and nCircle. There is no harm in then waiting for the SCADA vendor to certify the patch before installing it, but the Responsible Entity is at least aware of the vulnerability, can assess the risk, and take*

appropriate interim action." In response, the SDT agrees with the concept; however, the SDT does not find it appropriate to prescribe in regulation certain 'timely' sources, including private firms, that must be used. Patch monitoring services can come and go. The SDT also believes that it should not use undefined terms such as 'timely' in a mandatory Requirement, nor should it define 'timely' as it refers to the seemingly unlimited number of patch sources that will exist with the significantly expanded scope of Version 5. The SDT believes that the reliability of the BES will be better served by mandating that all vulnerabilities in all applicable BES Cyber Systems be known and analyzed by all entities than by trying to micro-manage what must occur with each system, patch, and vendor through a one-size-fits-all process. As stated in the guidance, patching systems can cause more risk to BES reliability than having a non-patched system in a given situation and the Responsible Entity, not the SDT, is in the best place to weigh these risks and develop an appropriate plan.

For CIP-007-5 Requirement 2, part 2.1, a comment was made that the patch management process for substation or plant control systems could include security patches for Cyber Assets such as panel meters, relays, controllers, Programmable Logical Control (PLCs), and other electronic devices that are part of the BES Cyber System and do not have network connectivity. In response, the SDT agrees that any Cyber Asset that meets the definition of BES Cyber Asset is included in the CIP-007-5 patch management Requirement regardless of connectivity and that is the intent. While routable protocol connectivity is a way that systems can be compromised, it is not the only way and in many examples today is not the primary way. Insider threats (intentional and unintentional, from both employees and non-employees, from both portable media and support laptops) are means by which systems are compromised today. Therefore the intent of this Requirement is to remain aware of the vulnerabilities in the BES Cyber Systems through the security patches that are released for them and analyze and mitigate those vulnerabilities. If a system has no connectivity and a security patch is released that can only be exploited via network connectivity, then that vulnerability is already mitigated and the patch is not applicable.

One commenter requested a definition in Requirement Part 2.1 for the phrase "applicable asset," and also suggested that the phrase "Applicable Cyber Asset" should be called "Applicable System" to align with wording in the column "Applicable Systems". In response, the SDT notes that individual BES Cyber Assets have patches, not systems of Cyber Assets. A system is a logical grouping of one or more BES Cyber Assets. While the applicability is at the system level, the Requirement is to perform patch management on all of the applicable BES Cyber Assets within those applicable systems.

There was a comment made on the change from 30 days to 35 days within Requirement Part 2.2. The comment was that this change allows utilities to manage patches monthly while coinciding with vendor releases, all without running into

issues of the Requirement being less than a full month. However, the commenter stated that this should be extended to 40 days to accommodate time to review the vendor releases, and that the additional five days on top of the existing 35 days will ensure that those utilities with patch management programs are not penalized due to variations in patch release dates from month to month. In response, the intent is for a process that approximates "monthly" and the SDT has already added in at least a four period to account for holidays, weekends, and other factors. The SDT does not agree that it needs further extension. Timely analysis of security patches is the goal.

Within Requirement Parts 2.2 and 2.3, one commenter requested clarification of the use of term "mitigation plan" and how it would provide value. To clarify Requirement Part 2.2 the commenter suggested mentioning that the mitigation plan is intended as an internal document and not submitted to the RE. In response, the SDT agrees and that these plans are internal documents and not submitted to the RE. In previous drafts, these were called 'remediation plans' and the SDT received comments that this term was used for what was submitted to Regional Entities in response to violations of the standard, so the SDT changed the term to 'mitigation plan' to avoid that confusion. The SDT has added this clarification to the guidance.

There was a comment with regard to CIP-007-5 Requirement Part 2.3 that reads, "Available actions to entities should include: 1) Apply the patches 2) Develop dated implementation plan 3) Create/revise existing mitigation plan". In many cases, patches will be applied, but outside of a 35 day period to accommodate outage schedules for optimizing reliability and availability of systems. In many cases, when an applicable patch is provided by a vendor, there may be no additional mitigation implemented during the time from patch availability until installation. Requiring entities to "create a dated mitigation plan or revise an existing mitigation plan will result in a paperwork exercise and yield no reliability or security benefits for the affected cyber assets. Adding an option to "Develop dated implementation plan" without requiring a mitigation plan to be created/modified permits entities to apply resources to application of patches and optimizing reliability." In response, the SDT notes that the 'dated mitigation plan' could simply consist of the date the entity plans to implement the security patch if beyond the initial 35 day period; therefore it is not simply a paperwork exercise that provides no reliability benefit. The intent of the Requirement is to mitigate the applicable vulnerabilities either through the installation of the patch or by some other means. Implementation of the patch is mitigation and having a record of the entity's plan to implement the patch is not seen as unnecessary paperwork.

There was a comment that Requirement Part 2.3 requires the Responsible Entity to either install the patch within 35 calendar days or simply create or update a mitigation plan. Furthermore, the commenter stated "there are no boundaries of what is acceptable in a mitigation plan, no expectation of justifying the decision, and no Requirement for

the CIP Senior Manager approval, thus allowing an entity to completely avoid the Requirement to patch a critical system by creating an illogical plan with unreasonable milestone dates. The need to wait for a scheduled outage at a field asset is well understood. Allowing an entity to determine patches will only be installed when the control center server is replaced (typically every four years), as has been seen during a CIP audit, is unreasonable and poses significant risk to the reliability of the BES. This Requirement does not require compensating measures appropriate to the vulnerability to be put into place until the patch is installed, thus furthering the potential risk. In effect, the provisions of this Requirement have the potential of creating a paper exercise with little value, with an expectation that the CIP auditor simply accept the documented plan without comment. (3) Requirement Part 2.4 furthers the inaction of the Responsible Entity by requiring the entity to follow the potentially illogical plan that the entity designed to avoid having to patch in the first place. As long as an extension of the plan is not required, there is still no CIP Senior Manager or delegate approval required." In response, the SDT believes that the reliability of the BES will be better served by mandating that all vulnerabilities in all applicable BES Cyber Systems be known and analyzed by all entities than by trying to micro-manage what must occur with each system, patch, and vendor through a one-size-fits-all process. As stated in the guidance, patching systems can cause more risk to BES reliability than having a non-patched system in a given situation and the Responsible Entity, not the SDT, is in the best place to weigh these risks and develop an appropriate plan. The SDT has no way to write a mandatory Requirement for a "logical" plan.

One commenter believes that the language in Requirement Part 2.4 be aligned with the language in Requirement Part 2.3. The commenter suggests that either both or neither should specify the approval Requirement of the CIP Senior Manager of delegate. The commenter recommends that the language of "…timeframe specified in Requirement Part 2.3 is approved" be added. In response, the SDT notes the CIP Senior Manager approval was added to Requirement Part 2.4 specifically to handle situations where entities might repeatedly extend their documented timeframe with no management oversight. The intent was not to have management approval of every patch in normal day-to-day processes. Entities are free to do so, but it was not the SDT's intent to make that a mandatory Requirement. Management approval of every patch on every BES Cyber Asset would tend to become a "rubber stamp" with no meaning. The SDT's intent was to have approval of exceptions so that if someone were simply moving deadlines to avoid complying with the intent of the Requirement it would be subject to management oversight.

Requirement R3

There was a comment that within Requirement Part 3.1 to consider adding the phrase "per device capability" to the beginning of the Requirement, or otherwise, if a deter posture is selected, it may be potentially in conflict with other

Requirements. In response, the Requirement is written at the system level in order to handle the device-specific issues. The SDT believes the included guidance also provides suggestions on how to handle device abilities.

With regard to CIP-007-5 Requirement 3, parts 3.1, 3.2, and 3.3, there was a comment that these three Requirement Parts do not have any timeline for action. A question was raised if an auditor will audit when the activity occurred and audit only that a process is created and executed per the registered entities process or procedure. In response, the answer to the question is yes. Malware protection is an inexact art as we are protecting against an intelligent and always changing adversary. Malware of today is quite different than malware of just a few years ago. The intent is for entities to think about the malware problem, document what they are doing about it for each BES Cyber System, and then do it. Prescribing certain technologies/tools/timeframes is not helpful in this rapidly changing area and tends to bog the industry and the regulator down in paperwork (such as TFEs) when agility in this area is required in order to protect BES reliability.

Within Requirement Part 3.2, one commenter stated that the word 'identified' is ambiguous and inconsistent with other malicious code phrases, and the commenter suggested changing the language to 'detected'. The SDT agrees with this clarification and has made the suggested change as this is how the measures and guidance were written as well.

One comment was related to the applicability section of Requirement Part 3.2. A suggestion was provided to revise this section to apply to Medium Impact assets with external routable protocol to read: "Medium Impact BES Cyber Systems with external routable protocol and their associated". In response, the SDT's intent is for the basic security protections, including malware prevention, to be applied to all BES Cyber Systems not just those with External Routable Connectivity. BES Reliability can be threatened on isolated networks of BES Cyber Systems through the introduction of malware through portable media or laptops used for support.

One commenter requested clarification on Requirement Part 3.3 which requires the anti-malware updating process to address testing of the signature or pattern file. In support of this request, the commenter stated that a number of registered entities have taken the position in the past that they address this aspect of the existing CIP Version 3 Requirement by relying upon the vendor to test before release. In response, the Requirement is taken verbatim from previous industry and FERC approved versions of the CIP standards. If the entity is obtaining tested signature updates from their control system vendor for a turnkey product, then that is compliant. The SDT does not think more prescription as to where the testing must occur is needed.

There was one comment raised that use of the term 'deter' is ambiguous and the commenter suggested replacing this language in Requirement Part 3.2. The commenter suggested replacing the language to read: "Configure the measures implemented in Requirement Part 3.1 such that it blocks or prevents access to files with potentially harmful code." This recommendation was based on the assumption that the recommendation for removal of the term "deter" is accepted in Requirement Part 3.1. In response, the SDT has purposefully added the word 'deter' so that entities are not in immediate violation of the Requirement should zero day malicious code enter the environment. There are no 100% preventions, so the SDT has added this verb to allow for that. Antivirus software tools today do deter, but do not 100% prevent.

Requirement R4

One commenter requested clarification around the last two sentences of the guidance section. The commenter also stated that currently, an entity that neglects to enable logging would be in violation. Per the Background section, a sole instance of deficiency is not grounds for a violation so long as it is adequately identified, assessed, and corrected. The statements in the guidelines seem to be relics of a previous draft which conflict with the new approach. In response, the SDT agrees and has rewritten the guidance to properly align with the Requirement.

One comment read that CIP-007-5 Requirement R4 for security event monitoring does not state any Requirements as to when the security events, particularly in Requirement Parts 4.1 (log events) and 4.2 (event alerts) are to reviewed, escalated, and mitigated. A question followed that asked if there are any Requirements for immediate action from the IT security personnel for detected failed access attempts, failed login attempts, or specific event alerts. In response, no, there are no prescriptive timeframes for response to alerts. The Requirement is to generate an alert for security events. Alerting someone to a condition is one thing, responding to the condition is dependent upon numerous variables that cannot be prescribed.

A recommendation was made to revise this Requirement to include the sentence from the guidance section, "that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment." The SDT's intent was not for the Responsible Entity to determine in totality the events to be logged, but that it must log the listed events at a minimum (subject to device capability). The Responsible Entity is free to log events above and beyond these and is encouraged to do so. However, the Responsible Entity cannot ignore the listed events.

As currently written, CIP-007-5 Requirement Part 4.1 would necessitate the logging at every Cyber Asset that is capable when there is not a network at the BES Cyber System. A suggestion was made to rewrite this Requirement to read, "for BES Cyber Systems that have Cyber Assets connected to a network via a routable protocol, log events at the BES Cyber System Level…" In response, the SDT's intent is that if a Cyber Asset has a local log on the device, then it should be utilized. For example, a completely standalone and isolated substation relay should log security events internally if it is capable of such so that if it begins misoperating there is some log to go review on the device to see if/who/when someone has accessed it. The Requirement is not dependent on external connectivity.

In Requirement Part 4.3, one commenter suggested that this is a data retention Requirement and should not be a Requirement of the standard. In response, the SDT's intent is that this is not strictly 'data retention for the purposes of audit' Requirement, but an actual cyber security Requirement to have ready access to the past 90 days of logs for the applicable systems for quick determination of potential cyber causes of reliability-affecting events. Quickly determining whether a BES event could have had a cyber security cause is a reliability-focused Requirement and the primary way to do that is to have ready access to security event logs. Configuring a system to retain the past five minutes of security event logs is of little to no value. This is a separate issue from having evidence for audits that you maintained 90 days of logs throughout the audit period.

Within the Guidelines and Technical Basis section of CIP-007-5, Requirement R4, a question was asked if the following quotation references to NIST are the guiding principles and documentation for the development of the RSAWs and auditing of this Requirement, "Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring." In response, these guidelines are not auditable, only Requirement statements are auditable. These are provided solely for use at the discretion of Responsible Entities, several of whom have asked in previous drafts for further guidance.

One commenter requested clarification on the word "review" with regard to the statement within Requirement Part 4.4 of "Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 days to identify undetected Cyber Security Incidents." The commenter questioned if an automated SIEM technology solution, which monitors real-time, would satisfy the Requirement. In response, the SDT states that the intent, as per FERC Order No. 706, is to manually review the logged events in order to ensure that automated tools such as SIEM systems are tuned appropriately and are not missing security events.

One commenter stated that CIP-007-5, Requirement R4, part 4.1.2 calls out failed access attempts and failed login attempts and is unclear as to why the phrases "failed access attempts" and "failed login attempts" are separated. The

commenter requested clarification on the following two questions: Are "failed access attempts" referring to physical attempts, and are they referring to some other form of electronic access to undermine the login process? In response, the SDT notes that as outlined in the guidance, access attempts primarily occur at EAPs and involve 'access' across the ESP. Login attempts primarily occur at the BES Cyber Systems. The monitoring Requirement applies to both situations.

A comment was issued on Requirement Part 4.1.3 that this Requirement of malicious code prevention methods to log is already contained in Requirement Part 3.2. The commenter suggested removing this Requirement. In response, the SDT notes that logging and alerting when malicious code is detected is a separate Requirement from the actual response to the alert and the mitigation of the malicious code on the BES Cyber System. The SDT sees no duplication between these Requirements.

There was a comment that within CIP-007-5 Requirement Parts 4.2 through 4.4 the Requirements and sub Requirements have become less clear than previous CIP standards versions. The commenter stated it was unclear if Requirement Part 4.4 replaces the previous monitoring Requirements in their entirety or if it represents an additional manual sampling action that occurs outside of a primary monitoring process which may be automated. The commenter suggested to consider modifying the aforementioned Requirements to make it clear to registered entities which logging is required, how logs should be monitored, and what actions are required in the event of an interruption in logging. In response, the SDT notes that Requirement Part 4.4, as noted in the Rationale and Change Justification, is in response to FERC Order No. 706 and the Directive to require a manual review of logs to insure that automated tools are not missing events. Automated tools are only as good as their rule sets, which require periodic tuning.

One commenter noted that a clarification may be needed for Requirement Part 4.2 as to whether the alert needs to be generated real-time with automatic notification or if the alert can be generated by a long after-the-fact manual review of security event logs. In response, the SDT's intent is, in general, for a real-time alert, but the SDT did not specify that as a timeframe in the Requirement because, for example, an after-the-fact review or analysis of logs would not require a computer-generated alert.

One commenter stated that Requirement Part 4.2 is a questionable and subjective Requirement as it states that an entity needs to generate alerts for security events that the entity determines necessary. In response, the SDT has set a minimum threshold of alerts that must be generated if the system is capable of it. All other types of alerts vary widely by the type of system in question and should not be prescribed. The alerts that can be generated by a Windows or Unix

server in a data center are quite different than what can be generated by some legacy purpose-built device in a substation.

A request was made to clarify Requirement Part 4.3 as to whether original source logs must be retained or if post-log analysis summaries are sufficient. In response, the SDT states that the language in the Requirement and measure provides the necessary level of clarity.

There were several comments on Requirement Part 4.4 that need to be clarified that the review of a summarization or sampling of logs is not acceptable as the primary means of log analysis and alert generation. The purpose of the manual review is to achieve a level of comfort that the log analysis tool is properly configured and is not missing important security events. A random sample review of logs otherwise runs a significant risk of completely missing security events that pose potential risk to BES reliability. Similarly, another comment for CIP 007-5, R4.4 read, in the Requirements column of the table, the draft language indicates a need to review logs to, "identify undetected Cyber Security Incidents." A question was raised if this is intended to be "identify detected Cyber Security Incidents?" Also for CIP-007-5 Requirement Part 4.4, a recommendation was made to change "undetected" to "potential". In response to the aforementioned comments, the SDT notes the intent is to review logs to insure that any automated tools or processes are tuned so that they are catching all Cyber Security Incidents, therefore the SDT believes that the 'undetected' word is correct. If attempts to breach the security of a BES Cyber System are being missed because the automated tools are not tuned or maintained, then this Requirement's intent is to catch that.

One comment read that in Requirement Part 4.4, to be consistent with other Requirements, that the phrase "15 days" be changed to "15 calendar days." In response, the SDT agrees with this clarification and has made the change.

A recommendation was provided to change the language in Requirement Part 4.2 to read "Detected failed login attempts from part 4.1." In response, the SDTs intent is that alerts be generated when it is detected that event logging has failed.

One commenter raised an issue that in Requirement Part 4.4 the words "summarization" and "sampling" components are too broad. In support of this, the commenter encouraged specificity in all measures. Additionally, the term "undetected" is unclear and confusing. The commenter stated that clarification, such as "logged but not previously selected for alerting or alarming" could be helpful. In response, the SDT has chosen to not provide further prescription but to use the words from FERC Order No. 706 to allow entities to meet the intent without prescribing exactly how to summarize or sample

the logs. Sufficient summaries or samples are dependent on many variables and do not lend themselves to a one-size-fits-all approach.

A comment was made with regard to Requirement Part 4.4 that a manual log review is a labor intensive and outdated approach. The technical guidance should allow for use of network behavior analysis or other automated review processes for this Requirement. The commenter believes that this Requirement is ambiguous. The commenter further stated that the Requirement to review 'undetected' Cyber Security Incidents is essentially a Requirement to perform manual reviews. By requiring a manual review, the entities are encouraged to record the absolute minimum event types as to minimize the burden of the manual review. Further, the Requirement to perform manual reviews would incentivize entities to not invest in systems that can perform automated log analysis and event correlation. In response, the SDT has added this Requirement in response to a directive in a FERC Order. The intent is to ensure that such automated tools are continually tuned and are not missing events that should be caught and alerted on.

A request was made to clarify Requirement Part 4.4 that the review of a summarization or sampling of logs is not acceptable as the primary means of log analysis and alert generation. Furthermore, the commenter stated that the purpose of the manual review is to achieve a level of comfort that the log analysis tool is properly configured and is not missing important security events. A random sample review of logs otherwise runs a significant risk of completely missing security events that pose potential risk to BES reliability. With regards to the Requirement column of the table for Requirement Part 4.4, the draft language indicates a need to review logs to "identify undetected Cyber Security Incidents". Is this intended to "identify detected Cyber Security Incidents"? One last comment was a suggestion to change the word "undetected" to "potential". In response, the SDT states that the intent is to review logs to insure that any automated tools or processes are tuned so that they are catching all Cyber Security Incidents, therefore the SDT believes that the 'undetected' word is correct. If attempts to breach the security of a BES Cyber System are being missed because the automated tools are not tuned or maintained, then this Requirement's intent is to catch that.

Requirement R5

There was a comment that the TFE language in CIP-007-5 Requirement Part 5.6 is unnecessary since technical or procedural controls can be used and that the phrase "per Cyber Asset capability" be used instead. In response, since many Cyber Assets used today utilize shared accounts and have no capability for individual accounts, periodically changing passwords is necessary. The SDT is aware that some systems have passwords that cannot be changed, or that if changed will break the system's functionality. Therefore, the SDT allowed for TFE's since the entity may not be able to

change the password either technically or procedurally. The SDT chose not to use the 'per Cyber Asset capability' as this is an instance where documenting and implementing some alternative control is necessary.

Within the Rationale section of CIP-007-5 Requirement R5, there was a suggestion to add the phrase “mimic display” to the second paragraph which outlines what is not included in interactive user access. In response, the SDT disagrees because the definition agreed to by the SDT is very clear and by adding another example with a non-widely used term would not add further clarity.

One commenter asked how CIP-007-5 Requirement Part 5.1 and CIP-005-5 Requirement Part 2.3 differ. The commenter stated that both appear to require authentication of Interactive Remote Access sessions. In response, CIP-007-5 Requirement Part 5.1 refers to any user access, including local access while physically present at the device. CIP-005-5 Requirement Part 2.3 refers to remote access.

A commenter believes that including specific password Requirements within a standard is contrary to new and safer technologies by the industry. In response, the SDT notes that the password Requirements have been worded in such a way that they only apply if passwords are used for authentication. If other, stronger means of authentication are used (tokens, biometrics, etc.) then the password Requirements do not apply. The Requirements are only “for password only authentication”.

One commenter stated that the term “generic account types” used in Requirement Part 5.2 is not defined and has not been well understood by entities to date. In response, the SDT notes that the term is now “default or generic” and the guidance provides some further explanation. The SDT does not believe that there is a sufficient definition of “generic” that will add any value beyond its normal dictionary definition.

One commenter suggested that within Requirement Part 5.2, alternate wording be provided to specify “known” enabled default or other generic account types. In response, the SDT agrees and has made the recommended clarification. The SDT notes this concept was already included in Requirement Part 5.4 and has included it here in Requirement Part 5.2 as well.

One commenter stated that Requirement Part 5.4 needs to be clarified that it pertains to active user accounts. The comments stated that there is no value to changing a password for an inactive or disabled user account until such time as the account is enabled. The commenter requested that the Requirement should also be clarified to require the initial

password change prior to placing the BES Cyber Asset into service. In response, the SDT disagrees. A known, published password should be changed even if the account is disabled. If the account is accidentally re-enabled, the password would be widely known. The SDT agrees that it would be a good practice to not only change the default password but also disable the default accounts if feasible, but it is not a Requirement.

There was a comment with regard to Requirement Part 5.4 that the word 'known' is ambiguous. For clarity, the commenter suggested changing the phrase "known default passwords" to "knowable default passwords". In response, the SDT disagrees that changing "known" to "knowable" solves the issue. The Requirement applies to the Responsible Entity, therefore it is "known to the Responsible Entity". Some vendors include "back door" user accounts in devices that are known only to the vendor and not the Responsible Entities. The Requirement is for the Responsible Entity to document only those that they know of.

A commenter suggested that Requirement Part 5.5's limitation to "password only" authentication is too narrow in scope and needs to include any use of a password for interactive access, even if part of a multi-factor authentication. The commenter also stated that this would need to include user accounts that are capable of being used interactively even if the intended use is only programmatic (e.g., an FTP account). Another comment to Requirement Part 5.5 was that the first paragraph uses the phrase "interactive user access" and that this is not a defined term. However, it is similar to the CIP Version 5 definitions defined term. The commenter questions whether the phrase "interactive user access" should be defined or clarified in the Guidelines and Technical Basis section. The SDT has added language clarifying "interactive user access" from the rationale for Requirement R5 to the Guidelines and Technical Basis section for Requirement Part 5.5.

One commenter recommended that the phrase "…at least once every 15 calendar months" be replaced with "at least once each calendar year." In response, and as described earlier, the SDT disagrees as it has standardized throughout the CIP standards that the original use of the word 'annual' be replaced with 'once every 15 calendar months.'

With regard to Requirement Part 5.7, one commenter requested a clarification to establish an upper bound (or maximum number of attempts) to generate an alert or initiate an account lockout. In response, the SDT disagrees that a prescriptive number of attempts is warranted. The entities will be in a better position to determine how many attempts in what time interval are needed for the particular situation. There may be widely varying circumstances to take into account such as is the login used by a process that is vital and will locking it out or slowing the interval between tries affect reliability.

CIP-008-5

General

One commenter stated that both CIP-008-5 and CIP-009-5 have plan update Requirements and should be considered for removal. In response, the SDT does not agree these should be removed in this version because we address multiple Directives in FERC Order No. 706 related to the update of plan documents.

Requirement R1

One commenter suggested adding "assess" to the required processes in Requirement Part 1.1. The SDT does not agree there is a need to include "assess" in the Requirement Part.

One commenter recommended increasing the one hour reporting threshold in Requirement Part 1.2. In response, the SDT uses this timeframe to respond to a directive in FERC Order No. 706, Paragraphs 673 and 676. The one hour also refers to the preliminary reporting required from the point at which the entity has determined an incident is a Reportable Cyber Security Incident.

Several commenters suggested that the obligation to report to the ES-ISAC in Requirement Part 1.2 may not be acceptable for some Canadians, but the SDT is unaware of any ES-ISAC reporting restrictions for Canadians. However, the SDT has clarified that such reporting to ES-ISAC is only required, unless prohibited by law, to account for scenarios where federal or provincial laws may prohibit such action.

Several commenters stated that notification of the ES-ISAC occurs only after a Cyber Security Incident is determined to be reportable and the one hour timeframe should start at the determination of the incident as being Reportable. The SDT has modified the Requirement to clarify the one hour timeframe is from determination rather than identification.

One commenter requested clarification on the term "preliminary notice." In response, we quote from the Technical Guidelines section of CIP-008-5, "This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report."

There was a comment that the one hour timestamp in Requirement Part 1.2 would require a paperwork intensive burden on the entity that may qualify for removal according to Paragraph 81 of FERC's Order on the Find, Fix, and Track process.

In response, while additional documentation may be necessary to demonstrate compliance with the timeline, the objective this Requirement goes beyond an administrative function.

One commenter suggested changing the one hour reporting threshold of Requirement Part 1.2 to 24 hours to align with EOP-004-2. In response, the one hour threshold is directed as a change in FERC Order No. 706;the SDTs for both CIP Version 5 and EOP-004-2 agrees this obligation was best left in the context of CIP-008-5.

One commenter stated that the roles and responsibilities of the incident response plans specified in Requirement Part 1.3 should be left to the Responsible Entity. They expressed concern for an auditor determining certain roles were left out of the plan. In response, the Requirement Part does not specify which roles must be in the plan, but having roles and responsibilities is a necessary part of an effective incident response plan.

Requirement R2

One comment read that Requirement R2 should have the language allowing an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R2 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One commenter proposed Requirement Part 2.1 needs clarification on whether a plan with multiple scenarios needs to have each scenario tested. In response, the SDT does not agree this clarification is necessary. It could be a benefit to consider multiple scenarios, and imposing a Requirement to test each would be a disincentive. Regardless, it is best left to the entity to determine how to test its plan.

There was a suggestion that the testing periodicity in Requirement Part 2.1 is inconsistent from the period used across other standards. The SDT agrees and has made this modification.

One commenter proposed adding wording to confirm a single incident response plan is sufficient for all High and Medium Impact BES Cyber Systems. In response, the Requirement Part does not preclude having a single plan, and the rationale in Requirement R1 suggests doing so.

One commenter suggested that documentation of a Reportable Cyber Security Incident suffers a “catch-22” in that one of the steps is a determination of whether or not an incident is Reportable. In response, the documentation of a Reportable

Cyber Security Incident can be performed after-the-fact. This is not a Requirement to document each step contemporaneously with each action.

One commenter recommended removing the documentation of deviations in Requirement Part 2.2 since it is mostly captured in the lessons learned. In response, the lessons learned activity likely will use documentation captured from the Cyber Security Incident, but there is no obligation to document the use of the plan. The SDT chose to use documentation of deviations because this is a much less documentation-centric activity than documenting how the plan was used.

Several commenters stated that Requirement Part 2.3 should be moved to data retention. In response, the retention of this information serves the purpose of supporting follow-up incident analysis and correlation activates. There is otherwise no obligation to retain this information.

Requirement R3

There was a comment that Requirement R3 should have the language allowing an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R3 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One commenter stated that CIP-008-5 Requirement R3 should allow deficiency correction. In response, the SDT does not agree this Requirement meets the criteria to be considered as high frequency, zero tolerance obligations as are the other Requirements that allow for deficiency correction.

There was a comment that in Requirement Part 3.1.2, lessons learned do not always trigger a plan update and that a qualifier “as applicable” should be added. The SDT agrees and has added the clarification, “lessons learned associated with the plan.” Corresponding changes have also been made in CIP-009-5.

There was a proposal that the timeframe in Requirement Part 3.2 could be extended to 90 calendar days consistent with 3.1. The SDT notes that Requirement Part 3.1 also includes the lessons learned obligation so the cumulative time to update should be longer.

One commenter proposed removing Requirement Part 3.2 or specifying only the affected roles and responsibilities. In response, the SDT notes that notification of all individuals is necessary for communication during a Cyber Security Incident.

One commenter stated for Requirement Parts 3.1 and 3.2, the wording needs to be rearranged to read better - the phrase 'no later than 90 calendar days after' should be added at the start of the sentence and deleted from the end. The SDT agrees and has made this change.

CIP-009-5

Requirement R1

One commenter stated that the roles and responsibilities of the recovery plans specified in Requirement Part 1.2 should be left to the Responsible Entity. They express concern for an auditor determining certain roles were left out of the plan. In response, the Requirement Part does not specify which roles must be in the plan, but having roles and responsibilities is a necessary part of an effective recovery plan.

There was a comment that Requirement Part 1.2 discusses responders without any additional clarification of who fits into this category. In response, this language has been carried forward from previous versions and the SDT has not received any additional comments supporting modification. The SDT agrees additional guidance would be helpful and has added clarification in the Technical Guidelines section of CIP-009-5.

There was one comment that stated that there should be more consistency in the applicability column of the tables and requests clarity on what applies if a Medium Impact BES Cyber System does not have a connectivity qualifier. In response, the lack of a qualifier only means that all Medium Impact BES Cyber Systems are applicable.

One commenter requested clarity on the intended frequency of performing Requirement Part 1.4. In response, the frequency is determined by the Responsible Entity. Some cyber systems may require a daily backup while other cyber systems, for example, at a power plant, may only require backups after major changes to the system.

One commenter suggested removing “and to address backup failures” from Requirement Part 1.4 because it may lead the reader to the notion of having another pre-determined plan to account for unknown issues during the backup. In response, the SDT notes that addressing backup failures meets the objective of the Requirement and purpose for verifying the successful completion of backups. Without this obligation, an entity could simply perform validation testing without performing any corrective action on the backup process.

Several commenters proposed changing Requirement Part 1.5 to “One or more processes, per device capability, to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), except where data preservation impedes or restricts recovery.” However, the rephrasing has a subtle change in meaning. The per device capability exception applies to the preservation of data and not the procedure itself.

One commenter stated that Requirement Part 1.5 can lead to delay in recovery operations, particularly in a Control Center. In response, the SDT notes the provision of the Requirement that data preservation should not impede recovery.

One commenter requested clarification of Requirement Part 1.5. They state that it would seem the activity would delay recovery. In response, planning to preserve evidence could include additional individuals assisting in the recovery or retaining failed Cyber Asset equipment during recovery operation.

One commenter suggested adding a CIP Exceptional Circumstance qualifier to Requirement Part 1.5. In response, the SDT removed this qualifier based on industry comments because an event triggering recovery could most likely be a CIP Exceptional Circumstance, and thus nullify the Requirement. However, Requirement Part 1.5 achieves the same objective in having a qualifier to avoid the disruption of restoration activities. The commenter also expressed concern about the intent of Requirement Part 1.5 and suggests moving this to CIP-008-5. In response, the objective is to have this performed in any recovery operation and not just Cyber Security Incidents.

There was a comment for Requirement Part 1.5 suggesting that the Requirements could put the registered entity into a "catch-22" scenario where it could try to comply with the Requirement by saving logs, which might impede recovery. In response, the plan should address the issue where saving information impedes recovery as indicated in the Requirement Part.

One commenter stated that in Requirement Part 1.5, the device capability should be worded to clearly qualify the preservation of data. The SDT agrees and has made this change. They also suggested the measure be updated to include the device capability qualifier. However, the qualifier itself only applies to the Requirement and does not need to have inclusion in the measure.

Requirement R2

There was one comment that the words 'between tests of the plan' are not needed. The SDT agrees and has made this clarification.

One commenter requested clarification on how an entity tests a representative sample of information if, per Requirement Part 2.1, they performed a paper drill. In response, the SDT notes that the test in Requirement Part 2.2 is not necessarily the same test performed in Requirement Part 2.1.

One commenter proposed Requirement Parts 2.1 and 2.3 need clarification on whether a plan with multiple scenarios needs to have each scenario tested. In response, the SDT does not agree this clarification is necessary. It could be a benefit to consider multiple scenarios, and imposing a Requirement to test each would be disincentive. Regardless, it is best left to the entity to determine how best to test their plan.

There was a request for clarification on the difference between 2.1 and 2.3 and for additional guidance on what types of operational exercise the SDT considers meeting the Requirement. In response, the SDT refers to the Technical Guidelines section of CIP-009-5, which states "The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, '[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims).'"

One commenter suggested that Requirement Part 2.2 needs to provide additional clarification for a "representative sample" of information used to recover BES Cyber System functionality. In response, the SDT does not think it provides a benefit to further specify a representative sample of information in this Requirement. Otherwise, this Requirement becomes focused on the sample of information rather than the recovery of information. As specified in the rationale, "Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information."

A clarification request was made on Requirement Part 2.2 regarding a representative sample. The representative sample must be determined by the Responsible Entity. It could be a test of all the most recent backup tapes or it could be a single representative test for multiple instances of the same system.

Requirement R3

There was a comment that this Requirement should include language that would allow an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R3 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One commenter suggested that a lessons learned activity should not be required for every failure of equipment in the field. In response, failure of equipment in the field does not indicate a recovery operation in all cases.

There was a proposal that the timeframe in Requirement Part 3.2 be extended to 90 calendar days consistent with 3.1. The SDT notes that Requirement Part 3.1 also includes the lessons learned obligation so the cumulative time to update should be longer.

There were several comments on parts 3.1 and 3.2 that the wording needed to be rearranged to read better - the words 'No later than 90 calendar days after' should be added at the start of the sentence and deleted from the end. The SDT agrees and has made this clarification.

Guidelines and Technical Basis

One entity commented that the guidelines state that recovery plan information is BES Cyber System Information, which is not consistent with the definition of BES Cyber System Information. The SDT agrees and has modified the guidance to state that recovery plan information may be considered BES Cyber System Information.

CIP-010-1

Timeframes for Configuration Control Activities

The SDT received comments that the timeframes for configuration control activities are inconsistent. The SDT believes that the timeframes specified are consistent and are reflective of a reasonable configuration change control process.

Cross References to CIP-005-5 and CIP-007-5 on Impacted Controls

Comments expressed concern over the cross-reference to CIP-005-5 and CIP-007-5 as it related to the controls that could potentially be impacted by a change. The commenter recommended that the Requirement be broadened to include any control rather than simply those included in CIP-005-5 and CIP-007-5. The SDT appreciates the concern expressed in this comment and wrestled with this issue itself. After changes to this issue during multiple rounds of industry comment, the SDT believes that bounding the controls that need to be assessed is the most auditable approach.

The SDT received comments regarding a concern over double jeopardy between CIP-005-5, CIP-007-5, and CIP-010-1, specifically as it relates to the documentation of logical network accessible ports. The SDT does not believe this is a double jeopardy situation. CIP-005-5 and CIP-007-5 specify how ports are to be configured whereas CIP-010-1 specifies that they be documented.

Requirement R1

The SDT received numerous comments to add the “external routable connectivity” qualifier to the applicability section in Requirement R1. The SDT appreciates the concern regarding the amount of effort involved in maintaining baseline documentation for disconnected Cyber Assets. However, since these devices are disconnected, the point in time at which the device is interacted with is the only time that the configuration may actually be validated. Given this, the SDT believes it is worthwhile to formalize the configuration change management process for these systems such that an understanding of the current configuration of the device is assured at all times.

One commenter identified confusion as it relates to comma usage in CIP-010-1 Requirement Part 1.5.1. The SDT has clarified the Requirement and removed the incorrect comma.

One commenter asked for clarification that the items in the baseline are “current” and not historical. The SDT confirms that it expects that the baseline is a current representation of the configuration and that this should be kept up to date by Requirement Part 1.3.

One comment from industry asked for clarification as it relates to Requirement Part 1.4.2 and whether this verification that security controls are in place was to be performed on the production system itself. The SDT clarifies that this is the case. The intent of the Requirement is to ensure that the production system is properly protected following a change that affected its baseline configuration.

Several commenters asked for clarification on the use of TFEs in Requirement Part 1.5 (testing of changes) and whether the SDT actually meant CIP Exceptional Circumstances. The SDT envisioned that operational issues may prevent the ability to test a change prior to its implementation. The SDT believes that the TFE process provides the protection necessary to ensure that violations are not issued for a wide range of circumstances, including but not limited to those operational issues contemplated in the CIP Exceptional Circumstances definition.

Requirement R2

Comments expressed that the IAC language should be removed from CIP-010-5 Requirement Part 2.1 because this Requirement was itself an internal control. The SDT agrees that the Requirement represents a control; however it believes that, particularly given the required periodicity, that there could be deficiencies identified in the control itself and it therefore warranted the IAC language.

Requirement R3

One commenter recommended that the language in Requirement Part 3.3 be modified to add the word applicable ("Prior to adding a new applicable Cyber Asset...") in order to clarify that this Requirement did not apply to those systems that are temporarily connected for less than 30 days. The SDT agrees that this is consistent with the intent of the language and has modified the language accordingly.

The SDT received concerns regarding the performance of active vulnerability assessment prior to the deployment of new BES Cyber Assets. The SDT agrees that these assessments may be imperfect and that there may be some applications that will not properly function outside of a full production environment. However, the SDT continues to believe that since this is the only time when active scans may be safely performed on future production equipment that it is in the best interest of the BES for an active vulnerability assessment to be performed.

The SDT received comments preferring additional specificity as to what to validate during a vulnerability assessment. The SDT appreciates these concerns, but believes that a vulnerability assessment for an EMS system may look substantially

different from an assessment of a PLC. The SDT believes that the best approach is to allow the entity to define an appropriate assessment methodology for their environment, which may then be evaluated by an auditor.

The SDT received comments that questioned the technical feasibility of monitoring for changes to the baseline configuration. The SDT originally had intended for this monitoring to occur on a more frequent basis, potentially real-time monitoring. However, it was persuaded that there are some systems for which real-time monitoring would be infeasible. The SDT does believe that given the relatively high level items included in the baseline, that periodic monitoring every 35 days is a reasonable method to ensure that changes are not taking place outside of an entity's change control program.

Numerous commenters expressed concern about the Requirement to document the differences between the test and production environments. The SDT reminds the industry that this Requirement was the result of a FERC directive. Additionally, the SDT reminds the industry that it believes that for a relatively stable testing environment, that this documentation could be done once and utilized for multiple changes or testing cycles.

Commenters asked questions about the multiple timeframes for the vulnerability assessments for high impact BES Cyber Systems. The SDT confirms that these time frames are intended. Effectively, this requires an annual paper or active vulnerability assessment, but an active vulnerability assessment must be performed at least every three years. The SDT believes that the confusion raised by the question is due to the reader not considering the entire table as itself a single Requirement.

One commenter expressed confusion on the applicability of CIP-010-1 to access points. The SDT clarifies that since access points are the point at which access is controlled, they are included in the definition of EACMS and as such are applicable to CIP-010-1.

One commenter asked for clarification that the test environment did not have to be an exact mirror of the production environment. The SDT confirms that this was the intent of using the phrase "models the baseline configuration."

CIP-011-1

Requirement R1

Commenters requested that Requirement Parts 1.1 and 1.2 of CIP-011-1 Requirement R1 be clarified to indicate that a single method or procedure was sufficient. The SDT agrees that this is the intent and has clarified the standard as requested.

Commenters suggested that CIP-011-1 Requirement Part 1.2 should contain a measure that indicates "repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program." The SDT does not see how a repository is evidence of a procedure to protect and securely handle BES Cyber System Information. The SDT agrees that an information repository may be used effectively to meet this Requirement, but it is only a component of the evidence based upon a particular manner of implementation.

Requirement R2

One commenter requested that Requirement R2 of CIP-011-1 be moved to CIP-010-1 as it could be considered part of a change control process. The SDT believes that the objective of this Requirement is the protection of the information in a BES Cyber System and therefore believes it is appropriate to include in CIP-011-1.

Commenters identified a typographical error in the measure of Requirement Part 2.2. The SDT appreciates this correction and has updated the standard.

Implementation Plan

Effective Date

Several commenters had questions or concerns about the Version 3 to Version 4 to Version 5 transition within the standards' implementation plan. Some questioned whether extending Version 3 to the effective date of Version 5, and superseding Version 4, is still possible, while others asked for a deadline for accomplishing such a transition plan. The SDT appreciates these concerns, as they are issues of efficiency, planning, effort, and cost for all of the industry. However, the SDT also acknowledges that not all entities are situated exactly the same. As such, the SDT is hesitant to provide a "deadline" or other trigger for FERC action that would serve to foreclose the opportunity for the implementation language to be adopted in time to implement moving directly from Version 3 to Version 5. The SDT expects that the filing will address this issue in a manner such that certainty about the issue may come as soon as possible, and that the filing and other coordination between NERC and FERC is the appropriate venue for supporting the implementation plan after industry approval. In the meantime, it is reasonable to expect that some entities may need to make a risk-informed judgment to proceed with Version 4 implementation by a certain date if the proposal in the implementation plan is not approved expediently. Some entities may be able to wait longer than others into 2013 before making that determination. The SDT has communicated directly with NERC to underscore the importance of coordination of this effort, and the SDT believes that having an approved set of standards, definitions, and implementation plan before the end of 2012 continues to provide a reasonable timeline to consider the implementation plan proposal.

There was one comment that 36 months to comply with CIP-003-5 Requirement R2 is excessively long since it only requires documentation of a few policies. The SDT notes that CIP-003-5 Requirement R2 requires implementation, and not just documentation of policies. This expands to a significantly large number of the overall reported BES Cyber Systems, which warrants such a timeline.

One commenter suggested that it misleads entities to allow the provision suspending compliance with Version 4. The SDT does not agree this is misleading. The SDT has been careful to communicate the risk in awaiting this order to begin planning compliance with Version 4. Furthermore, the FERC approving this provision, even if it is closer to the Version 4 Effective Date, still spares entities and auditors alike untold expenses of a compliance monitoring program for Version 4.

A few commenters asked about audits in 2015 during the expected transition window to Version 5's effective date. That is outside the scope of the SDT, but the SDT has tried to account for a smooth transition within the implementation plan,

to include specifications for initial required performances of periodic events. In response to this question and the issue of transition from Version 3 to Version 5, the SDT understands that NERC is preparing information to assist in the smooth transition among CIP standards versions, and that such information will be coordinated upon certainty that Version 5 has been approved by the industry and is no longer subject to change.

One commenter stated that the effective date language should be qualified with a statement that sufficient time should be given for completion of CIP-002-5 R2 to comply with CIP-003 through CIP-011. The SDT believes this is already well understood and ongoing communication and training will provide entities further guidance to categorize BES Cyber Systems with sufficient time to comply with CIP-003 through CIP-011.

Several entities comment that NERC and the drafting team should request FERC to suspend compliance with Version 4 and allow entities to transition from Version 3 to Version 5 on the effective date. In response, the proposed effective date does bypass Version 4 and provides the FERC the opportunity to issue an order approving this provision. In effect, this is the industry and SDT communication to the FERC requesting the bypass of Version 4.

There was a comment that suggested extending Version 3 until Version 5 becomes effective could not be accomplished in Canada through an implementation plan. In response, the SDT notes that Canadian jurisdictions would be subject to the second provision for "those jurisdictions where no regulatory approval is required." The commenter is correct that the proposal in the Implementation Plan, if approved, would supersede any other Order to the contrary. In all cases of reliability standards, the Implementation Plan is subject to regulatory or other applicable federal approval.

A few commenters noted that CIP-003-5 is dependent upon CIP-004-5 through CIP-009-5, CIP-010-1, and CIP-011-1 passing. The SDT confirms the commenters' understanding and notes that the implementation plan conditions all standards passing before any of them become effective.

One commenter expressed concern that the implementation of CIP-004 through CIP-011 should be combined into those standards. The SDT points out that the implementation of security procedures in CIP-004 through CIP-011 is included in those Requirements that have actions associated with them. The entity should refer to the high level Requirement for the implementation language.

Initial Performance of Certain Periodic Requirements

Several commenters stated some confusion with the initial performance of periodic Requirements section or suggested that it is unnecessary and, if retained, should be in guidance. The SDT notes this section was incorporated from industry comments, and moving this section to guidance would be misleading because the additional time for compliance with periodic Requirements would not be enforceable in guidance.

There was a comment that no provision for CIP Exceptional Circumstances exists for some periodic Requirements and that an entity should be allowed to track instances of non-compliance in CIP Exceptional Circumstances rather than self-report. In response, the SDT has indicated where exceptions may occur to the standards in defined CIP Exceptional Circumstances. Most of the periodic Requirements should have enough lag time built in to avoid the need for self-reporting in emergency situations. Otherwise, it is not envisioned all compliance activities should cease in a CIP Exceptional Circumstance, but only the ones indicated in the Requirements.

One commenter proposed revisions to the following initial periodic Requirements, and the SDT responds in order:

- CIP-004-5 Requirement Parts 4.2 through 4.4 should be required on or before the effective date to preclude record-keeping errors. The SDT notes that record-keeping errors, while not the most efficient, are not violations of the standard.
- CIP-006-5 Requirement Part 3.2 should tie to the previous testing interval and allow 24 months for the newly in-scope Cyber Assets. In response, tying the interval to previously in-scope Critical Cyber Assets would cause more confusion than is necessary for this Requirement, and the SDT believes the 12 calendar months are appropriate timeframes for testing PACS.
- CIP-008-5 Requirement Part 3.1 and CIP-009-5 Requirement Part 3.1 should not be included in the initial performance of periodic requirements section since they are not periodic, but are performed in response to a test. The SDT agrees.
- CIP-010-1 Requirement Parts 3.1 and 3.2 should not be included because it would be similar to part 3.3 in adding a new Cyber Asset to the BES Cyber System. In response, the SDT retains the additional timeframe because strict compliance would suggest this periodic timeframe be performed immediately on the effective dates for all BES Cyber Systems in scope, which would be infeasible for most all entities.
- CIP-009-5 Requirement Part 2.3 is included in both groups 6 and 7. The SDT notes this is not the case.

- Group 8 of the periodic Requirements dealing with the continued effectiveness of previous personnel risk assessments is already incorporated in the Requirement language. In response, strict compliance with the Requirement would otherwise suggest immediate compliance with this Requirement on the effective date.

One commenter suggested that NERC imposing Requirements before the effective date goes beyond NERC's legal authority. In response, the implementation plan does not modify the effective date of any Requirement but makes clear when the initial performance must occur for certain Requirements. By stating a Requirement can be performed prior to the effective date does not impose a different effective date. Rather, this clarifies that on the effective date, the entity has complied with the Requirement by performance of a past activity.

There was an observation that CIP-006-5 Requirement Part 3.1 and the Requirements specified in section 7 have periodicities longer than the initial performance. This is correct and intended by the SDT because even though the periodicity is longer, the benefit achieved by the initial performance puts it closer to the effective date.

Previous Identity Verification

One commenter noted an incorrect reference to CIP-004-5 Requirement Part 4.1, and the SDT expresses their gratitude for uncovering this error.

Planned or Unplanned Changes Resulting in a Higher Categorization

Several commenters suggested that the distinction between planned and unplanned changes is not clear and the timeframe for planned changes should be extended to 18-24 months. In response, the SDT carries forward this language that has been in effect since Version 2. The 12 months is also carried forward as the time entities with existing CCAs have to implement CIP Requirements on new CCAs. The SDT does not consider this 12 month timeframe unreasonable and notes in the example given that updates to a generation facility would be considered a planned change and compliance would be part of the maintenance performed during the outage.

One commenter stated that the addition of time for initial performance of periodic Requirements muddles the timeline for compliance. In response, the implementation plan would not preclude an entity from complying earlier to benefit the entity with a consistent compliance schedule, but without this provision, the periodic Requirements would need to be performed prior to the 12 month period, and this is neither reasonable nor appropriate. This language was added since the last posting in response to multiple entities' request.

There was a comment that suggested the last scenario in unplanned changes be clarified as the first high or medium impact BES Cyber System overall rather than at a facility. The SDT has made this clarification by providing a clarifying parenthetical phrase to row five of the "Scenario of Unplanned Changes After the Effective Date" table that underscores the meaning of that row in relation to and in context with rows one through four.

There was a request for clarification on the use of Effective Date in the table heading "Scenario of Unplanned Changes After the Effective Date". In response, the SDT notes that this is the effective date specified in each standard for Version 5 of the CIP Cyber Security Standards.

Applicability Reference Tables

One commenter proposed revisions to the Requirement applicability, and the SDT responds in order:

- CIP-004-5 Requirements R4 and R5 should apply to Protected Cyber Assets. In response, we have addressed most of the risk by authorizing and revoking access associated with the BES Cyber System. We carry forward the precedent of applicability in this case from previous standards, and do not find a justification for adding them to the applicability of these Requirement Parts.
- CIP-005-5 Requirement R1 should apply to PACS as it does in the current standard.
- CIP-005-5 R1 should apply to PACS as it does in the current standard. In previous versions, CIP-005 R2 applied but not R1. The SDT received significant industry feedback that this applicability was confusing and resulted in multiple interpretations. The SDT addresses access control at the device level in CIP-007-5 and avoids the confusion around the disconnect between applicability in CIP-005-4 R1 and R2, and for this reason, CIP-005-5, Requirement R1 does not apply to PACS.

There was a comment that CIP-005-5 Requirement R2 should apply to EACMS. In response, the EACMS are referenced as part of the Requirement. The confusion of recursive Requirements is not worth the reliability and security benefit gained by their inclusion.

Definitions

BES Cyber Asset

One entity commented that the definition should reference "the items in Attachment 1" instead of "Facilities, systems, or equipment," because "Facilities, systems, or equipment" is subjective and lends itself to differing interpretations, and Attachment 1 provides greater clarity and guidance on the criteria to define BES Cyber Assets. The SDT points out that a definition is used in a standard and cannot reference a part of the standard. The term "Facilities, systems or equipment" has been used as part of the definition of Critical Assets for Versions 1, 2, 3 and 4.

BES Cyber System

One commenter wrote that the definition uses the word logically that may be mistakenly interpreted to mean networked instead of validly grouped. The SDT believes that the rest of the definition of the BES Cyber System in relation to the performance of reliability functions provides clarity to the meaning used here.

BES Cyber System Information Responses

The SDT received a concern regarding the phrase "not publicly available" in that if BES Cyber System Information was made public, it would then be outside the scope of the standard. The SDT appreciates this concern; however, it believes that the meaning is ultimately clear as to the intent.

CIP Exceptional Circumstance Responses

The SDT received a request to clarify the punctuation in the definition of CIP Exceptional Circumstances. The SDT has updated the punctuation as requested.

One commenter expressed concern about the ability to declare a CIP Exceptional Circumstance for hardware, software or equipment failure. The concern of the commenter was that this could open the door to bypassing Requirements for minor issues. The SDT did not envision this as a free for all and believes that the obligation to have policy around the declaration and response to CIP Exceptional Circumstances should minimize any abuse of this definition.

CIP Senior Manager Responses

One commenter requested that the SDT address the accepted interpretation request in RFI Project 2012-INT-06. While the SDT has an obligation to incorporate existing interpretations, the response to the interpretation that was highlighted has not been posted and therefore the SDT would risk contradicting a pending standards interpretation action.

Additionally, since that interpretation has not been approved by industry, there is no way for the SDT to determine whether it reflects a level of consensus of the industry. As such, the SDT believes that this would be too large of a change to incorporate at this point in the development process.

Control Center

Many entities requested clarification on the term “associated data centers” in the definition of Control Centers and asked whether these are the "data centers" that service/support a control center”. Comments were also made that “data center” is not a defined term. The SDT believes that the term “data center” is a commonly understood term of practice and that a specific glossary definition is not required. The intent of including “associated data centers” in the definition of Control Centers is to include only those systems that are associated with the Control Center Cyber Assets and directly support the functions of the functional entities defined. These will be the BES Cyber Systems that directly provide monitoring and control functions for the Control Center operators’ use in the performance of their real-time functions, and to ensure that this does not include certain types of field data aggregating or processing assets that are associated with field transmission or generation assets. Control Center data centers do not necessarily reside in the same facility where operators are hosted, but may extend the Control Center to include facilities hosting these cyber systems outside of the facility hosting the Control Center operators.

One entity requested clarification on the meaning of “location” in the definition. The NERC Guideline for Critical Asset identification has an extensive discussion of control rooms and Control Centers. In general, a location is delineated by a physical boundary that hosts a set of BES Facilities.

One entity suggested the addition of “CIP” to the term or some indication that this is only a definition used in the CIP context. The SDT is proposing the term to be included in the NERC Glossary. The convention is that when the term is used in its capitalized form (initial letter of each word), then it is used as the NERC Glossary defined meaning of the term. Otherwise, it is used in the undefined, generic meaning. This does not have any effect on other standards that do not use the term in its capitalized form. Other standards which wish to use the NERC Glossary term as defined (or wish to amend it through the development process) can use the capitalized form.

Cyber Asset

One entity commented that the inclusion of “hardware, software and data” in the definition of Cyber Asset was redundant and proposed a simplified definition of “Entity programmable electronic devices”. The SDT’s approach to existing definitions is to make only the modifications necessary for additional clarity or intent. This definition is based on

the previous definition of Cyber Asset. The SDT believes that removing the terms “hardware, software and data” would not provide additional clarity and that the addition of “Entity” in the qualification of “programmable” would inappropriately limit the general scope of the definition of cyber asset. The protection Requirements in the standards include those necessary to ensure that proper processes are included for protection from inappropriate modification or misuse of programs not directly modified by the entity.

Another entity commented that the proposed definition could be interpreted to require utilities to demonstrate consideration of - in addition to hardware - all software and data on each programmable electronic device, which would be impracticable and overly burdensome. The entity recommends changing the definition to “Programmable electronic device.” The SDT points out that the inclusion of these qualifications has been part of the definition of cyber assets since Versions 1, 2, 3 and 4 and that the modifications to the previous definition ensures that the definition includes the data when it is on these devices.

One entity commented that the inclusion in voice communication for a Control Center operator to implement operating actions in the execution of a Control Center functional obligation would include many smaller entities as Control Centers. The determination of whether a facility is considered a Control Center is dependent on whether it meets the definition, not on size or on how it performs its functional obligations. The manner in which it implements its functional obligations will determine what are qualified BES Cyber Assets. For example, in the environment that the commenter describes, there may be many BES Cyber Assets that provide monitoring and alarming information on which the operator will initiate a real-time operation for the BES. The impact of such monitoring and alarming systems on the real-time operation of the BES warrants the protection commensurate with its function.

Cyber Security Incident

One commenter suggested modifying the definition of Cyber Security Incident to eliminate attempts of compromise or disruption because such a definition is broad enough to include any erroneous traffic. The SDT disagrees. Attempts of compromise imply intent far beyond erroneous traffic and should be analyzed and recorded as part of the CIP-008-5 incident response plan.

There was a comment that the definition of Cyber Security Incident should also apply to PCAs, EACMS and PACS. In response, the definition has no applicability, and an incident occurring on PCAs, EACMS and PACS already meets the definition of having the potential to impact the BES Cyber System.

There was a comment suggesting that it is difficult to determine the intent of an attacker, and the commenter further suggested that "suspicious" is vague. In response, the SDT intends that such determination is best left to the entity. Without the qualifiers of suspicious and malicious, it could be interpreted that many nominal events would be considered Cyber Security Incidents.

Electronic Access Control and Monitoring System

One commenter stated that the definition of EACMS is inconsistent with the definition used in the background section of Version 5 CIP Standards. In response, the guidance provided in the background section is not a definition. It only provides example EACMS for the purpose of adding context for the reader.

Intermediate Device (now "Intermediate System")

A recommendation was made that the definition of Intermediate Device be modified to remove the phrase "or collection of Cyber Assets", as they consider this limiting the scope. The SDT used "A Cyber Asset or collection of Cyber Assets" to allow for flexibility so that an entity could use one or more devices to perform the noted functional Requirements. The scope of the definition and Requirements is limited to only Interactive Remote Access to BES Cyber Systems. Further, it was noted in prior comments that entities may not be able to implement a single device that provides encryption and multifactor authentication. As a result of comments, the definition has been modified to "Intermediate System" to better align with the asset and system concepts used throughout the Version 5 standards.

One commenter requested clarification on the definition of Intermediate Device. The SDT has worked the definition to allow for flexibility in the selection and implementation of technology to meet their needs. The definition does not prevent an entity from having an Intermediate Device within an ESP, just not the ESP containing the BES Cyber Systems being remotely accessed. The definition term (not the definition's meaning) has also been modified to "Intermediate System" to better align with the asset and system concepts used throughout the Version 5 standards. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested more clarity regarding the types of devices that would qualify as intermediate devices, beyond the Requirements that they must support encryption for any interactive sessions and multifactor-authentication for access to any interactive sessions. Additional references are available in the *Guidance for Secure Interactive Remote*

Access document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

Interactive Remote Access

One commenter suggested that, as written, the definition appears to require that entities declare each of their internal networks as an ESP, including their corporate networks. The commenter discussed that many entities monitor their corporate network in much the same manner as their ESPs, and that requiring encryption within their corporate networks would introduce an unacceptable security risk by rendering their monitoring capabilities ineffective. The commenter requested appropriate clarifications or that the definition be modified to specify that Interactive Remote Access and the associated technical controls be required when traffic is traversing an untrusted or public network only. In response, the SDT notes that it is not necessary to declare the encryption termination point as a part of the ESP. It is allowable to have the termination point reside outside of the ESP, such as a corporate firewall to allow for corporate boundary systems to monitor network traffic as described. In this scenario, the corporate firewall would be considered and protected as an EACMS but still not considered to define an ESP.

There was a recommendation to remove the second sentence of the Interactive Remote Access definition. The SDT added this language to address comments and concerns raised during this project and Project 2010-15: Expedited Revisions to CIP-005-3.

One comment suggested that the definition of Interactive Remote Access be modified to remove the sentence, "Remote access can be initiated from: ... contractors and consultants." The SDT added this language to address comments and concerns raised during this project and Project 2010-15: Expedited Revisions to CIP-005-3.

There was one request that the definition be modified as “access is likely initiated…” The SDT used “may be initiated” to allow for flexibility rather than using words such as “shall be initiated” or “will be initiated” which are far more restrictive and align to the concern noted.

There was a suggestion that the definition of Interactive Remote Access be modified to remove Requirement language within the definition. The SDT considers all parts of the definition to be clarification of what is and is not Interactive Remote Access. The Requirements are the technical controls to be implemented.

Reportable Cyber Security Incident

There was a comment suggesting that the definition of Reportable Cyber Security Incident is too broad and should specifically state that a malware infection of an in-scope Cyber Asset should be reported. In response, the SDT provides additional guidance in the context of CIP-008-5 that would generally ensure the proper reporting of a malware infection. However, a malware infection itself would cause additional uncertainty in the definition. Moreover, entities would be left to wonder if a contained malware infection was reportable or not. For these reasons, the SDT does not agree with the recommendation to further specify Reportable Cyber Security Incident.

One commenter said that this definition should be removed and addressed solely within the standard. In response, the SDT believes there is sufficient consensus for the definition and moving this term to a local definition in CIP-008-5 would be a significant change and potentially cause uncertainty in the enforceability of this definition.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Recirculation Ballots and Non-binding Poll Open Through 8 p.m. ET Monday, November 5, 2012

Now Available

Recirculation ballot windows for 10 CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1), a set of new and revised NERC Glossary definitions, implementation plan, and a non-binding poll for the associated VRFs and VSLs for all 10 standards, are open through 8 p.m. Eastern on **Monday, November 5, 2012**.

Clean and redline versions of each of the ten CIP Version 5 standards (which include CIP-002-5 through CIP-009-5 and CIP-010-1 and CIP-011-1), showing changes made since the successive ballot that ended on October 10, 2012, are posted.

The SDT made several minor changes for clarity, consistency, and grammar in each of the standards, none of which were substantive. There were also modifications and additions to clarify particular information in the background, rationales, and Guidelines and Technical Basis sections of certain standards, as well as the change of the name of one defined term (but not the definition itself) from "Intermediate Device" to "Intermediate System" to better align with the asset and system concepts used throughout the Version 5 standards. The following summarizes at a high level some of the changes to the requirements:

- **CIP-002-5**: Minor formatting changes in the requirements to clarify that the parts are parts, not sub-requirements (i.e., renumbered from "R1.1", etc., to "1.1", etc., to conform to other standard numbering. Change does not appear in "tracked changes" for redline purposes); clarification of the SDT's intent with respect to kV value connections in attachment 1, criterion 2.5; clarification of the listing of restoration assets for consistency in the requirements and low impact section of attachment 1; and other clarifications in the Guidelines and Technical Basis.

- **CIP-003-5**: Clarification that the one or more policies required by Requirements R1 and R2 must "collectively" include the items listed, and clarification that the "within 30 days" update logically only applies to changes.

- **CIP-004-5**: Clarification for consistency with other standards of the background description of "Medium Impact BES Cyber Systems with External Routable Connectivity." Also clarified in Requirement R1, part 1.1, that the reinforcement of cyber security practices that is required may

include associated physical security practices.

- **CIP-006-5**: Clarification in Requirement R1, part 1.7 that the alarm or alert that must be issued in response to detected unauthorized physical access must occur within 15 minutes of the detection, which is consistent with the subject of the requirement part.

- **CIP-007-5**: Clarification in Requirement R3, part 3.2 in response to uncertainty over what was meant by "identified malicious code" to "detected malicious code," and clarification of Requirement R5, part 5.2 to specify that it only applies to "known" account types, which is consistent with part 5.4.

- **CIP-008-5**: Clarification that reporting to ES-ISAC is required unless prohibited by law and a logical clarification that the report must occur upon determination that a Cyber Security Incident is reportable, as a reportable incident is not identified until it is determined that it is reportable. Also clarified for consistency the time references.

- **CIP-009-5**: Modified "per device capability" to "per Cyber Asset capability" to be consistent with use in other standards and clarified time references for consistency.

- **Implementation Plan**: Minor changes for clarification and consistency, including correction of part references and removal of two illogical references from the initial performance of periodic requirements section, as the performance of those parts are not periodic in nature, but are predicated upon the performance of a different requirement part. Additionally, the SDT provided a clarifying parenthetical phrase to row five of the "Scenario of Unplanned Changes After the Effective Date" table that underscores the meaning of that row in relation to and in context with rows one through four.

In addition, the following documents are posted to assist stakeholders in their review:

- Clean versions of the approved versions of CIP-002-4 through CIP-009-4 are posted because the extent of the changes to each of the standards makes a redline of the posted draft standards against the approved standards impractical.
- Consideration of Issues and Directives – The consideration of issues and directives provides the FERC issues and directives related to the CIP project and the associated consideration by the drafting team.
- Clean and redline versions of the consolidated VRFs and VSLs for all standards, showing changes made since the successive ballot that ended on October 10, 2012.

Instructions

In the recirculation ballot, votes are counted by exception. Only members of the ballot pool may cast a ballot; all ballot pool members may change their previously cast votes. A ballot pool member who failed to cast a ballot during the last ballot window may cast a ballot in the recirculation ballot window. If a ballot pool member does not participate in the recirculation ballot, that member's vote cast in the previous ballot will be carried over as that member's vote in the recirculation ballot.

The ballot pool for the standards has been cloned to create a ballot pool for a non-binding poll of the associated VRFs and VSLs for all 10 CIP standards. During the non-binding poll window, a comment period is open for comments on the VRFs and VSLs. Please use the electronic comment form to submit specific suggestions for the VRFs and VSLs. (There is no comment period associated with recirculation ballots, therefore, the comment form ask questions specific to the VRFs and VSLs.)

Members of the ballot pools associated with this project may log in and submit their votes for the standards and opinion for the non-binding poll of VRFs and VSLs by clicking here.

Next Steps

If approved, the standards will be presented to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009, with additional directives to be addressed within 90-days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the

CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related issues of FERC Order No. 706.

One of the ERO's priorities is to develop a robust set of critical infrastructure reliability standards that enable the industry to adapt to continuously changing threats and vulnerabilities by emphasizing security risk management. NERC staff and industry are working together to accomplish this goal in 2012.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Development Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2008-06 Cyber Security Order 706 Version 5 CIP

Recirculation Ballots and Non-binding Poll Open Through 8 p.m. ET Monday, November 5, 2012

Now Available

Recirculation ballot windows for 10 CIP standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1), a set of new and revised NERC Glossary definitions, implementation plan, and a non-binding poll for the associated VRFs and VSLs for all 10 standards, are open through 8 p.m. Eastern on **Monday, November 5, 2012**.

Clean and redline versions of each of the ten CIP Version 5 standards (which include CIP-002-5 through CIP-009-5 and CIP-010-1 and CIP-011-1), showing changes made since the successive ballot that ended on October 10, 2012, are posted.

The SDT made several minor changes for clarity, consistency, and grammar in each of the standards, none of which were substantive. There were also modifications and additions to clarify particular information in the background, rationales, and Guidelines and Technical Basis sections of certain standards, as well as the change of the name of one defined term (but not the definition itself) from "Intermediate Device" to "Intermediate System" to better align with the asset and system concepts used throughout the Version 5 standards. The following summarizes at a high level some of the changes to the requirements:

- **CIP-002-5**: Minor formatting changes in the requirements to clarify that the parts are parts, not sub-requirements (i.e., renumbered from "R1.1", etc., to "1.1", etc., to conform to other standard numbering. Change does not appear in "tracked changes" for redline purposes); clarification of the SDT's intent with respect to kV value connections in attachment 1, criterion 2.5; clarification of the listing of restoration assets for consistency in the requirements and low impact section of attachment 1; and other clarifications in the Guidelines and Technical Basis.

- **CIP-003-5**: Clarification that the one or more policies required by Requirements R1 and R2 must "collectively" include the items listed, and clarification that the "within 30 days" update logically only applies to changes.

- **CIP-004-5**: Clarification for consistency with other standards of the background description of "Medium Impact BES Cyber Systems with External Routable Connectivity." Also clarified in Requirement R1, part 1.1, that the reinforcement of cyber security practices that is required may

include associated physical security practices.

- **CIP-006-5**: Clarification in Requirement R1, part 1.7 that the alarm or alert that must be issued in response to detected unauthorized physical access must occur within 15 minutes of the detection, which is consistent with the subject of the requirement part.

- **CIP-007-5**: Clarification in Requirement R3, part 3.2 in response to uncertainty over what was meant by "identified malicious code" to "detected malicious code," and clarification of Requirement R5, part 5.2 to specify that it only applies to "known" account types, which is consistent with part 5.4.

- **CIP-008-5**: Clarification that reporting to ES-ISAC is required unless prohibited by law and a logical clarification that the report must occur upon determination that a Cyber Security Incident is reportable, as a reportable incident is not identified until it is determined that it is reportable. Also clarified for consistency the time references.

- **CIP-009-5**: Modified "per device capability" to "per Cyber Asset capability" to be consistent with use in other standards and clarified time references for consistency.

- **Implementation Plan**: Minor changes for clarification and consistency, including correction of part references and removal of two illogical references from the initial performance of periodic requirements section, as the performance of those parts are not periodic in nature, but are predicated upon the performance of a different requirement part. Additionally, the SDT provided a clarifying parenthetical phrase to row five of the "Scenario of Unplanned Changes After the Effective Date" table that underscores the meaning of that row in relation to and in context with rows one through four.

In addition, the following documents are posted to assist stakeholders in their review:

- Clean versions of the approved versions of CIP-002-4 through CIP-009-4 are posted because the extent of the changes to each of the standards makes a redline of the posted draft standards against the approved standards impractical.
- Consideration of Issues and Directives – The consideration of issues and directives provides the FERC issues and directives related to the CIP project and the associated consideration by the drafting team.
- Clean and redline versions of the consolidated VRFs and VSLs for all standards, showing changes made since the successive ballot that ended on October 10, 2012.

Instructions

In the recirculation ballot, votes are counted by exception. Only members of the ballot pool may cast a ballot; all ballot pool members may change their previously cast votes. A ballot pool member who failed to cast a ballot during the last ballot window may cast a ballot in the recirculation ballot window. If a ballot pool member does not participate in the recirculation ballot, that member's vote cast in the previous ballot will be carried over as that member's vote in the recirculation ballot.

The ballot pool for the standards has been cloned to create a ballot pool for a non-binding poll of the associated VRFs and VSLs for all 10 CIP standards. During the non-binding poll window, a comment period is open for comments on the VRFs and VSLs. Please use the electronic comment form to submit specific suggestions for the VRFs and VSLs. (There is no comment period associated with recirculation ballots, therefore, the comment form ask questions specific to the VRFs and VSLs.)

Members of the ballot pools associated with this project may log in and submit their votes for the standards and opinion for the non-binding poll of VRFs and VSLs by clicking here.

Next Steps

If approved, the standards will be presented to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Background

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standard Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order No. 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009, with additional directives to be addressed within 90-days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the

CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards related issues of FERC Order No. 706.

One of the ERO's priorities is to develop a robust set of critical infrastructure reliability standards that enable the industry to adapt to continuously changing threats and vulnerabilities by emphasizing security risk management. NERC staff and industry are working together to accomplish this goal in 2012.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Development Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Project 2008-06 Cyber Security Order 706 (CIP Version 5)

Recirculation Ballot Results

Now Available

Twelve recirculation ballot windows for the following 10 CIP standards, the associated implementation plan, and a set of new and revised NERC Glossary definitions, concluded on Monday, November 5, 2012.

The non-binding poll of the associated VRFs/VSLs for all 10 CIP standards has been extended by one additional day in order to achieve a quorum. Please take this opportunity to submit an opinion if you have not already done so. If you do not intend to cast a supportive or negative opinion, please cast an abstention to help us achieve a quorum.

Voting statistics for each ballot are listed below, and the Ballot Results webpage provides a link to the detailed results. Once a quorum is reached on the non-binding poll, a separate announcement will be sent with the results.

Ballot	Results
CIP-002-5 Cyber Security – BES Cyber System Identification	Quorum: 85.33% Approval: 78.59%
CIP-003-5 Cyber Security – Security Management Controls	Quorum: 85.33% Approval: 92.75%
CIP-004-5 Cyber Security – Personnel and Training	Quorum: 85.54% Approval: 89.73%
CIP-005-5 Cyber Security – Electronic Security Perimeter(s)	Quorum: 85.54% Approval: 93.73%
CIP-006-5 Cyber Security – Physical Security	Quorum: 85.54% Approval: 95.53%
CIP-007-5 Cyber Security – Systems Security Management	Quorum: 85.54% Approval: 91.79%
CIP-008-5 Cyber Security – Incident Reporting and Response Planning	Quorum: 85.54% Approval: 95.47%
CIP-009-5 Cyber Security – Recovery Plans for BES Cyber Assets and Systems	Quorum: 85.33% Approval: 94.60%
CIP-010-1 Cyber Security – Configuration Change Management	Quorum: 85.54% Approval: 88.99%

Ballot	Results
CIP-011-1 Cyber Security — Information Protection	Quorum: 85.54% Approval: 95.67%
CIP V5 Implementation Plan	Quorum: 83.47% Approval: 94.91%
CIP V5 Definitions	Quorum: 83.47% Approval: 93.23%

Next Steps
The standards will be presented to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Background
In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

Version 5 of the NERC CIP Cyber Security Standards is intended to address all remaining standards related issues of FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed. Additional information about the project is available on the project webpage.

Standards Development Process
The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, at wendy.muller@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Standards Admin Home
Registered Ballot Body
Ballot Events
Current Ballot Pools
Current Ballots
Previous Ballots
Vetting
Proxy Pool
NERC Home

Ballot Results

Ballot Name:	Project 2008-06 Recirculation Ballot CIP-002-5
Ballot Period:	10/26/2012 - 11/5/2012
Ballot Type:	Recirculation
Total # Votes:	413
Total Ballot Pool:	484
Quorum:	**85.33 % The Quorum has been reached**
Weighted Segment Vote:	78.59 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative		Negative		Abstain	No Vote
			# Votes	Fraction	# Votes	Fraction	# Votes	
1 - Segment 1.	125	1	73	0.709	30	0.291	9	13
2 - Segment 2.	10	0.9	8	0.8	1	0.1	1	0
3 - Segment 3.	120	1	77	0.762	24	0.238	5	14
4 - Segment 4.	38	1	19	0.613	12	0.387	3	4
5 - Segment 5.	103	1	59	0.776	17	0.224	8	19
6 - Segment 6.	60	1	34	0.756	11	0.244	4	11
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.5	5	0.5	0	0	2	3
9 - Segment 9.	9	0.3	3	0.3	0	0	1	5
10 - Segment 10.	9	0.7	6	0.6	1	0.1	0	2
Totals	**484**	**7.4**	**284**	**5.816**	**96**	**1.584**	**33**	**71**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Negative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Negative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Negative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	
1	Cleco Power LLC	Danny McDaniel	Abstain	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Negative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Negative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Abstain	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Negative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Negative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Negative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Negative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Negative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	
1	Northeast Utilities	David Boguslawski	Affirmative	

1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Negative	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Negative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Negative	
1	Transmission Agency of Northern California	Bryan Griess	Abstain	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Negative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	

3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Negative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Abstain	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Negative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Negative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Negative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Negative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	

3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Negative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	
3	Snohomish County PUD No. 1	Mark Oens	Negative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Abstain	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Negative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Negative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Negative	
4	Consumers Energy	David Frank Ronk	Negative	
4	Cowlitz County PUD	Rick Syring	Negative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Negative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	

4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Abstain	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Negative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Abstain	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Negative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Negative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Negative	
5	Cowlitz County PUD	Bob Essex	Negative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Negative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Abstain	
5	JEA	John J Babik	Affirmative	

5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Negative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Negative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Abstain	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Negative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	

6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Abstain	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	
6	Florida Municipal Power Pool	Thomas Washburn	Negative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Negative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Negative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Negative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		James A Maenner		
8		Roger C Zaklukiewicz	Affirmative	
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	

9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G. Dvorsky	Affirmative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2009 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Standards Admin Home
Registered Ballot Body
Ballot Events
Current Ballot Pools
Current Ballots
Previous Ballots
Vetting
Proxy Pool
NERC Home

Ballot Results

Ballot Name:	Project 2008-06 Recirculation Ballot CIP-003-5
Ballot Period:	10/26/2012 - 11/5/2012
Ballot Type:	Recirculation
Total # Votes:	413
Total Ballot Pool:	484
Quorum:	**85.33 % The Quorum has been reached**
Weighted Segment Vote:	92.75 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative		Negative		Abstain	No Vote
			# Votes	Fraction	# Votes	Fraction	# Votes	
1 - Segment 1.	125	1	97	0.924	8	0.076	7	13
2 - Segment 2.	10	0.9	9	0.9	0	0	1	0
3 - Segment 3.	120	1	93	0.912	9	0.088	4	14
4 - Segment 4.	38	1	28	0.875	4	0.125	2	4
5 - Segment 5.	103	1	71	0.91	7	0.09	6	19
6 - Segment 6.	60	1	43	0.935	3	0.065	3	11
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	6	0.6	0	0	1	3
9 - Segment 9.	9	0.3	3	0.3	0	0	1	5
10 - Segment 10.	9	0.7	6	0.6	1	0.1	0	2
Totals	**484**	**7.5**	**356**	**6.956**	**32**	**0.544**	**25**	**71**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	

1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	

3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Negative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	

3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Negative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Negative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Abstain	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Affirmative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Negative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	

4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Abstain	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Negative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Abstain	
5	JEA	John J Babik	Affirmative	

5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	

6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		Edward C Stein	Affirmative	
8		James A Maenner		
8		Roger C Zaklukiewicz	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	

9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G. Dvorsky	Affirmative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2009 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Standards Admin Home
Registered Ballot Body
Ballot Events
Current Ballot Pools
Current Ballots
Previous Ballots
Vetting
Proxy Pool
NERC Home

Ballot Results

Ballot Name:	Project 2008-06 Recirculation Ballot CIP-004-5
Ballot Period:	10/26/2012 - 11/5/2012
Ballot Type:	Recirculation
Total # Votes:	414
Total Ballot Pool:	484
Quorum:	**85.54 % The Quorum has been reached**
Weighted Segment Vote:	89.73 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative		Negative		Abstain	No Vote
			# Votes	Fraction	# Votes	Fraction	# Votes	
1 - Segment 1.	125	1	92	0.893	11	0.107	9	13
2 - Segment 2.	10	0.9	8	0.8	1	0.1	1	0
3 - Segment 3.	120	1	91	0.901	10	0.099	5	14
4 - Segment 4.	38	1	26	0.867	4	0.133	4	4
5 - Segment 5.	103	1	68	0.883	9	0.117	8	18
6 - Segment 6.	60	1	39	0.886	5	0.114	5	11
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	6	0.6	0	0	1	3
9 - Segment 9.	9	0.3	3	0.3	0	0	1	5
10 - Segment 10.	9	0.7	6	0.6	1	0.1	0	2
Totals	**484**	**7.5**	**339**	**6.73**	**41**	**0.77**	**34**	**70**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Negative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Abstain	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Abstain	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	

1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	

3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Abstain	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Negative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	

3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Negative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Abstain	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Affirmative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	

4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Negative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Abstain	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Abstain	
5	JEA	John J Babik	Affirmative	

5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Abstain	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	

6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Abstain	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner		
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	

9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G. Dvorsky	Affirmative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2009 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Standards Admin Home
Registered Ballot Body
Ballot Events
Current Ballot Pools
Current Ballots
Previous Ballots
Vetting
Proxy Pool
NERC Home

Ballot Results

Ballot Name:	Project 2008-06 Recirculation Ballot CIP-005-5
Ballot Period:	10/26/2012 - 11/5/2012
Ballot Type:	Recirculation
Total # Votes:	414
Total Ballot Pool:	484
Quorum:	**85.54 % The Quorum has been reached**
Weighted Segment Vote:	93.73 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative		Negative		Abstain	No Vote
			# Votes	Fraction	# Votes	Fraction	# Votes	
1 - Segment 1.	125	1	94	0.904	10	0.096	8	13
2 - Segment 2.	10	0.9	9	0.9	0	0	1	0
3 - Segment 3.	120	1	93	0.921	8	0.079	5	14
4 - Segment 4.	38	1	26	0.897	3	0.103	5	4
5 - Segment 5.	103	1	70	0.897	8	0.103	7	18
6 - Segment 6.	60	1	41	0.911	4	0.089	4	11
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	6	0.6	0	0	1	3
9 - Segment 9.	9	0.3	3	0.3	0	0	1	5
10 - Segment 10.	9	0.7	7	0.7	0	0	0	2
Totals	**484**	**7.5**	**349**	**7.03**	**33**	**0.47**	**32**	**70**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Negative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Abstain	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Abstain	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	

1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	

3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Abstain	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Abstain	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	

3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Negative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Abstain	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Affirmative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	

4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Abstain	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Abstain	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Abstain	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	

5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	

6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Abstain	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Abstain	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		James A Maenner		
8		Edward C Stein	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	

9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G. Dvorsky	Affirmative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2009 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Standards Admin Home
Registered Ballot Body
Ballot Events
Current Ballot Pools
Current Ballots
Previous Ballots
Vetting
Proxy Pool
NERC Home

Ballot Results

Ballot Name:	Project 2008-06 Recirculation Ballot CIP-006-5
Ballot Period:	10/26/2012 - 11/5/2012
Ballot Type:	Recirculation
Total # Votes:	414
Total Ballot Pool:	484
Quorum:	**85.54 % The Quorum has been reached**
Weighted Segment Vote:	95.53 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative		Negative		Abstain	No Vote
			# Votes	Fraction	# Votes	Fraction	# Votes	
1 - Segment 1.	125	1	97	0.933	7	0.067	8	13
2 - Segment 2.	10	0.9	9	0.9	0	0	1	0
3 - Segment 3.	120	1	96	0.941	6	0.059	4	14
4 - Segment 4.	38	1	27	0.9	3	0.1	4	4
5 - Segment 5.	103	1	72	0.935	5	0.065	8	18
6 - Segment 6.	60	1	43	0.956	2	0.044	4	11
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	6	0.6	0	0	1	3
9 - Segment 9.	9	0.3	3	0.3	0	0	1	5
10 - Segment 10.	9	0.7	7	0.7	0	0	0	2
Totals	**484**	**7.5**	**360**	**7.165**	**23**	**0.335**	**31**	**70**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Negative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Abstain	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Abstain	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	

1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	

3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Abstain	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	

3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Negative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Abstain	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Affirmative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	

4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Abstain	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	

5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Abstain	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	

6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Abstain	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		Edward C Stein	Affirmative	
8		James A Maenner		
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	

9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G. Dvorsky	Affirmative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2009 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Standards Admin Home
Registered Ballot Body
Ballot Events
Current Ballot Pools
Current Ballots
Previous Ballots
Vetting
Proxy Pool
NERC Home

Ballot Results

Ballot Name:	Project 2008-06 Recirculation Ballot CIP-007-5
Ballot Period:	10/26/2012 - 11/5/2012
Ballot Type:	Recirculation
Total # Votes:	414
Total Ballot Pool:	484
Quorum:	**85.54 % The Quorum has been reached**
Weighted Segment Vote:	91.79 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative		Negative		Abstain	No Vote
			# Votes	Fraction	# Votes	Fraction	# Votes	
1 - Segment 1.	125	1	94	0.922	8	0.078	10	13
2 - Segment 2.	10	0.9	8	0.8	1	0.1	1	0
3 - Segment 3.	120	1	93	0.921	8	0.079	5	14
4 - Segment 4.	38	1	27	0.9	3	0.1	4	4
5 - Segment 5.	103	1	70	0.909	7	0.091	8	18
6 - Segment 6.	60	1	41	0.932	3	0.068	5	11
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	6	0.6	0	0	1	3
9 - Segment 9.	9	0.3	3	0.3	0	0	1	5
10 - Segment 10.	9	0.7	6	0.6	1	0.1	0	2
Totals	**484**	**7.5**	**348**	**6.884**	**31**	**0.616**	**35**	**70**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Abstain	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Abstain	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Abstain	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	

1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	

3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Abstain	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	

3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Negative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Abstain	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Affirmative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	

4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Abstain	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Abstain	
5	JEA	John J Babik	Affirmative	

5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Abstain	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	

6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Abstain	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		Edward C Stein	Affirmative	
8		James A Maenner		
8		Roger C Zaklukiewicz	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	

9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G. Dvorsky	Affirmative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2009 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Standards Admin Home
Registered Ballot Body
Ballot Events
Current Ballot Pools
Current Ballots
Previous Ballots
Vetting
Proxy Pool
NERC Home

Ballot Results

Ballot Name:	Project 2008-06 Recirculation Ballot CIP-008-5
Ballot Period:	10/26/2012 - 11/5/2012
Ballot Type:	Recirculation
Total # Votes:	414
Total Ballot Pool:	484
Quorum:	**85.54 % The Quorum has been reached**
Weighted Segment Vote:	95.47 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative		Negative		Abstain	No Vote
			# Votes	Fraction	# Votes	Fraction	# Votes	
1 - Segment 1.	125	1	98	0.925	8	0.075	6	13
2 - Segment 2.	10	0.9	9	0.9	0	0	1	0
3 - Segment 3.	120	1	96	0.941	6	0.059	4	14
4 - Segment 4.	38	1	27	0.9	3	0.1	4	4
5 - Segment 5.	103	1	74	0.937	5	0.063	6	18
6 - Segment 6.	60	1	44	0.957	2	0.043	3	11
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	6	0.6	0	0	1	3
9 - Segment 9.	9	0.3	3	0.3	0	0	1	5
10 - Segment 10.	9	0.7	7	0.7	0	0	0	2
Totals	**484**	**7.5**	**364**	**7.16**	**24**	**0.34**	**26**	**70**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Abstain	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Negative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	

1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	

3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Abstain	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	

3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Negative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Abstain	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Affirmative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	

4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Abstain	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	

5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	

6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Abstain	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner		
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	

9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G. Dvorsky	Affirmative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2009 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Standards Admin Home
Registered Ballot Body
Ballot Events
Current Ballot Pools
Current Ballots
Previous Ballots
Vetting
Proxy Pool
NERC Home

Ballot Results

Ballot Name:	Project 2008-06 Recirculation Ballot CIP-009-5
Ballot Period:	10/26/2012 - 11/5/2012
Ballot Type:	Recirculation
Total # Votes:	413
Total Ballot Pool:	484
Quorum:	**85.33 % The Quorum has been reached**
Weighted Segment Vote:	94.60 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative		Negative		Abstain	No Vote
			# Votes	Fraction	# Votes	Fraction	# Votes	
1 - Segment 1.	125	1	98	0.942	6	0.058	8	13
2 - Segment 2.	10	0.9	9	0.9	0	0	1	0
3 - Segment 3.	120	1	95	0.931	7	0.069	4	14
4 - Segment 4.	38	1	26	0.867	4	0.133	4	4
5 - Segment 5.	103	1	72	0.923	6	0.077	7	18
6 - Segment 6.	60	1	41	0.932	3	0.068	4	12
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	6	0.6	0	0	1	3
9 - Segment 9.	9	0.3	3	0.3	0	0	1	5
10 - Segment 10.	9	0.7	7	0.7	0	0	0	2
Totals	**484**	**7.5**	**357**	**7.095**	**26**	**0.405**	**30**	**71**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Abstain	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Abstain	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	

1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	

3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Abstain	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Affirmative	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	

3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Negative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Abstain	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Affirmative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	

4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Negative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Abstain	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	

5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Abstain	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	

6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Abstain	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo		
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Negative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner		
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	

9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G. Dvorsky	Affirmative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2009 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Standards Admin Home
Registered Ballot Body
Ballot Events
Current Ballot Pools
Current Ballots
Previous Ballots
Vetting
Proxy Pool
NERC Home

Ballot Results

Ballot Name:	Project 2008-06 Recirculation Ballot CIP-010-1
Ballot Period:	10/26/2012 - 11/5/2012
Ballot Type:	Recirculation
Total # Votes:	414
Total Ballot Pool:	484
Quorum:	**85.54 % The Quorum has been reached**
Weighted Segment Vote:	88.99 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative		Negative		Abstain	No Vote
			# Votes	Fraction	# Votes	Fraction	# Votes	
1 - Segment 1.	125	1	90	0.882	12	0.118	10	13
2 - Segment 2.	10	0.9	8	0.8	1	0.1	1	0
3 - Segment 3.	120	1	90	0.891	11	0.109	5	14
4 - Segment 4.	38	1	26	0.867	4	0.133	4	4
5 - Segment 5.	103	1	67	0.87	10	0.13	8	18
6 - Segment 6.	60	1	38	0.864	6	0.136	5	11
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	6	0.6	0	0	1	3
9 - Segment 9.	9	0.3	3	0.3	0	0	1	5
10 - Segment 10.	9	0.7	6	0.6	1	0.1	0	2
Totals	**484**	**7.5**	**334**	**6.674**	**45**	**0.826**	**35**	**70**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Negative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Negative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Abstain	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Negative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Abstain	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	

1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Negative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Negative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	

3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Abstain	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Negative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	

3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Negative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Abstain	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Affirmative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	

4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Abstain	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Negative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Negative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Negative	
5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Abstain	
5	JEA	John J Babik	Affirmative	

5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Abstain	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Negative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Negative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	

6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Abstain	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Negative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		James A Maenner		
8		Roger C Zaklukiewicz	Affirmative	
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	

9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G. Dvorsky	Affirmative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2009 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Standards Admin Home
Registered Ballot Body
Ballot Events
Current Ballot Pools
Current Ballots
Previous Ballots
Vetting
Proxy Pool
NERC Home

Ballot Results	
Ballot Name:	Project 2008-06 Recirculation Ballot CIP-011-1
Ballot Period:	10/26/2012 - 11/5/2012
Ballot Type:	Recirculation
Total # Votes:	414
Total Ballot Pool:	484
Quorum:	**85.54 % The Quorum has been reached**
Weighted Segment Vote:	95.67 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	97	0.942	6	0.058	9	13
2 - Segment 2.	10	0.9	9	0.9	0	0	1	0
3 - Segment 3.	120	1	94	0.94	6	0.06	6	14
4 - Segment 4.	38	1	27	0.9	3	0.1	4	4
5 - Segment 5.	103	1	74	0.937	5	0.063	6	18
6 - Segment 6.	60	1	43	0.956	2	0.044	4	11
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	6	0.6	0	0	1	3
9 - Segment 9.	9	0.3	3	0.3	0	0	1	5
10 - Segment 10.	9	0.7	7	0.7	0	0	0	2
Totals	**484**	**7.5**	**360**	**7.175**	**22**	**0.325**	**32**	**70**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Affirmative	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Abstain	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Affirmative	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	

1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative	
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	

3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Negative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Abstain	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	

3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Abstain	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Negative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Abstain	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Negative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy	Affirmative	
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	

4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Abstain	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Affirmative	
5	JEA	John J Babik	Affirmative	

5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	

6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Abstain	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner		
8		Edward C Stein	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	

9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G. Dvorsky	Affirmative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Affirmative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2009 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Standards Admin Home
Registered Ballot Body
Ballot Events
Current Ballot Pools
Current Ballots
Previous Ballots
Vetting
Proxy Pool
NERC Home

Ballot Results

Ballot Name:	Project 2008-06 Recirculation Ballot Implementation Plan .
Ballot Period:	10/26/2012 - 11/5/2012
Ballot Type:	Recirculation
Total # Votes:	404
Total Ballot Pool:	484
Quorum:	**83.47 % The Quorum has been reached**
Weighted Segment Vote:	94.91 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	125	1	91	0.948	5	0.052	14	15
2 - Segment 2.	10	0.7	7	0.7	0	0	2	1
3 - Segment 3.	120	1	93	0.949	5	0.051	7	15
4 - Segment 4.	38	1	27	0.964	1	0.036	4	6
5 - Segment 5.	103	1	67	0.918	6	0.082	8	22
6 - Segment 6.	60	1	42	0.955	2	0.045	5	11
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	6	0.6	0	0	1	3
9 - Segment 9.	9	0.3	3	0.3	0	0	1	5
10 - Segment 10.	9	0.6	5	0.5	1	0.1	1	2
Totals	**484**	**7.2**	**341**	**6.834**	**20**	**0.366**	**43**	**80**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	

1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Abstain	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Abstain	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Abstain	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Abstain	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	

1	Northeast Utilities	David Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Abstain	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Affirmative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Affirmative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Abstain	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles Yeung		
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	

3	American Public Power Association	Nathan Mitchell	Affirmative	
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Abstain	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Affirmative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Negative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	

3	Mississippi Power	Jeff Franklin	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Abstain	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Negative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Abstain	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Abstain	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	

4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Abstain	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Abstain	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Negative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Abstain	

5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Affirmative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Negative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Abstain	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono		
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	David Thompson	Affirmative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		

6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Abstain	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Negative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Affirmative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		Edward C Stein	Affirmative	
8		James A Maenner		
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		

9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	
9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G. Dvorsky	Affirmative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2009 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

Standards Admin Home
Registered Ballot Body
Ballot Events
Current Ballot Pools
Current Ballots
Previous Ballots
Vetting
Proxy Pool
NERC Home

Ballot Results

Ballot Name:	Project 2008-06 Recirculation Ballot Definitions
Ballot Period:	10/26/2012 - 11/5/2012
Ballot Type:	Definitions
Total # Votes:	404
Total Ballot Pool:	484
Quorum:	**83.47 % The Quorum has been reached**
Weighted Segment Vote:	93.23 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative		Negative		Abstain	No Vote
			# Votes	Fraction	# Votes	Fraction	# Votes	
1 - Segment 1.	125	1	91	0.919	8	0.081	11	15
2 - Segment 2.	10	0.7	7	0.7	0	0	2	1
3 - Segment 3.	120	1	91	0.929	7	0.071	7	15
4 - Segment 4.	38	1	28	0.933	2	0.067	2	6
5 - Segment 5.	103	1	66	0.892	8	0.108	7	22
6 - Segment 6.	60	1	42	0.933	3	0.067	4	11
7 - Segment 7.	0	0	0	0	0	0	0	0
8 - Segment 8.	10	0.6	6	0.6	0	0	1	3
9 - Segment 9.	9	0.3	3	0.3	0	0	1	5
10 - Segment 10.	9	0.7	6	0.6	1	0.1	0	2
Totals	**484**	**7.3**	**340**	**6.806**	**29**	**0.494**	**35**	**80**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	

1	Baltimore Gas & Electric Company	Gregory S Miller		
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Abstain	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Abstain	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Abstain	
1	CPS Energy	Richard Castrejana	Affirmative	
1	Dairyland Power Coop.	Robert W. Roddy	Abstain	
1	Dayton Power & Light Co.	Hertzel Shamash		
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Michael S Crowley	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Entergy Services, Inc.	Edward J Davis	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	Gainesville Regional Utilities	Luther E. Fair		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative	
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Abstain	
1	Idaho Power Company	Ronald D Schellberg	Affirmative	
1	Imperial Irrigation District	Tino Zaragoza	Abstain	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	
1	Keys Energy Services	Stanley T Rzad	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt		
1	Muscatine Power & Water	Tim Reed		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Cole C Brodine	Affirmative	
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Affirmative	
1	New York Power Authority	Arnold J. Schuff		
1	New York State Electric & Gas Corp.	Raymond P Kinney		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David Boguslawski	Affirmative	

1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Affirmative	
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Affirmative	
1	Oncor Electric Delivery	Brenda Pulis	Affirmative	
1	Orange and Rockland Utilities, Inc.	Edward Bedder	Affirmative	
1	Orlando Utilities Commission	Brad Chase		
1	PacifiCorp	Ryan Millard	Affirmative	
1	PECO Energy	Ronald Schloendorn		
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain	
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Raj Rana	Rajendrasinh D Rana	Abstain	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.		
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Negative	
1	South California Edison Company	Steven Mavis	Affirmative	
1	South Mississippi Electric Power Association	Rodney A. Wilson	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Affirmative	
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative	
1	Southwestern Power Administration	Angela L Summer	Abstain	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry G Akens	Negative	
1	Trans Bay Cable LLC	Steven Powell	Negative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	Midwest ISO, Inc.	Marie Knox	Affirmative	
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool, Inc.	Charles Yeung		
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Richard J. Mandes	Affirmative	
3	Alameda Municipal Power	Douglas Draeger	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	

3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blachly-Lane Electric Co-op	Bud Tracy	Affirmative	
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham	Affirmative	
3	Central Electric Power Cooperative	Ralph J Schulte		
3	Central Lincoln PUD	Steve Alexanderson	Affirmative	
3	City of Alexandria	Michael Marcotte		
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	
3	City of Lodi, California	Elizabeth Kirkley	Affirmative	
3	City of McMinnville	John C Dietz		
3	City of Palo Alto	Eric R Scott	Affirmative	
3	City of Redding	Bill Hughes	Affirmative	
3	City Water, Light & Power of Springfield	Roger Powers	Affirmative	
3	Clearwater Power Co.	Dave Hagen	Affirmative	
3	Cleco Corporation	Michelle A Corley	Abstain	
3	Colorado Springs Utilities	Charles Morgan	Affirmative	
3	ComEd	Bruce Krawczyk		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Constellation Energy	CJ Ingersoll		
3	Consumers Energy	Richard Blumenstock	Negative	
3	Consumers Power Inc.	Roman Gillen	Affirmative	
3	Coos-Curry Electric Cooperative, Inc	Roger Meader	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Affirmative	
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F. Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Abstain	
3	Entergy	Joel T Plessinger	Affirmative	
3	Fall River Rural Electric Cooperative	Bryan Case	Affirmative	
3	FirstEnergy Energy Delivery	Stephan Kern	Affirmative	
3	Flathead Electric Cooperative	John M Goroski		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Georgia Power Company	Anthony L Wilson	Affirmative	
3	Georgia Systems Operations Corporation	William N. Phinney	Affirmative	
3	Grays Harbor PUD	Wesley W Gray		
3	Great River Energy	Brian Glover	Affirmative	
3	Gulf Power Company	Paul C Caldwell	Affirmative	
3	Hydro One Networks, Inc.	David Kiguel	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz	Abstain	
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Norman D Harryhill	Affirmative	
3	Lane Electric Cooperative, Inc.	Rick Crinklaw	Affirmative	
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative	
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Jeff Franklin	Affirmative	

3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	
3	Muscatine Power & Water	John S Bos	Negative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	Marilyn Brown		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	Northern Lights Inc.	Jon Shelby	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David Anderson	Affirmative	
3	Old Dominion Electric Coop.	Bill Watson		
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	PacifiCorp	Dan Zollner	Affirmative	
3	Piedmont EMC	Robin W Blanton		
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters		
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Benton County	Gloria Bender	Abstain	
3	Public Utility District No. 1 of Clallam County	David Proebstel		
3	Puget Sound Energy, Inc.	Erin Apperson	Affirmative	
3	Raft River Rural Electric Cooperative	Heber Carpenter	Affirmative	
3	Rutherford EMC	Thomas M Haire	Negative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Negative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	South Mississippi Electric Power Association	Gary Hutson	Affirmative	
3	Southern California Edison Co.	David B Coher		
3	Tacoma Public Utilities	Travis Metcalfe	Abstain	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Turlock Irrigation District	John Souza	Affirmative	
3	Umatilla Electric Cooperative	Steve Eldrige	Affirmative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power	Kevin Koloini	Abstain	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	Central Lincoln PUD	Shamus J Gamache	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle		
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Consumers Energy	David Frank Ronk	Affirmative	
4	Cowlitz County PUD	Rick Syring	Affirmative	
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Thomas Richards		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	

4	Imperial Irrigation District	Diana U Torres		
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Affirmative	
4	Northern California Power Agency	Tracy R Bibb		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Pacific Northwest Generating Cooperative	Aleka K Scott	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steven McElhaney	Affirmative	
4	Tacoma Public Utilities	Keith Morisette	Abstain	
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
4	WPPI Energy	Patrick Connors		
5	AEP Service Corp.	Brock Ondayko	Affirmative	
5	AES Corporation	Leo Bernier	Affirmative	
5	Amerenue	Sam Dwyer	Affirmative	
5	Arizona Public Service Co.	Edward Cambridge	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Affirmative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	BrightSource Energy, Inc.	Chifong Thomas	Abstain	
5	Caithness Long Island, LLC	Jason M Moore		
5	Chelan County Public Utility District #1	John Yale	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Brian Horton	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Cogentrix Energy, Inc.	Mike D Hirst		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad		
5	Consumers Energy Company	David C Greyerbiehl	Negative	
5	Cowlitz County PUD	Bob Essex	Affirmative	
5	CPS Energy	Robert Stevens		
5	Dairyland Power Coop.	Tommy Drea	Abstain	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Energy Services, Inc.	Tracey Stubbs		
5	Exelon Nuclear	Michael Korchynsky		
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Affirmative	
5	Green Country Energy	Greg Froehling		
5	Imperial Irrigation District	Marcela Y Caballero	Abstain	
5	JEA	John J Babik	Affirmative	

5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	
5	Madison Gas and Electric Co.	Steven Schultz	Affirmative	
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Negative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	New York Power Authority	Gerald Mannarino		
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern California Power Agency	Hari Modi		
5	Northern Indiana Public Service Co.	William O. Thompson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Affirmative	
5	Occidental Chemical	Michelle R DAntuono		
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Platte River Power Authority	Roland Thiel	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis		
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Puget Sound Energy, Inc.	Tom Flynn	Affirmative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative	
5	South Carolina Electric & Gas Co.	Edward Magic		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Southern California Edison Co.	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran		
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz		
5	U.S. Bureau of Reclamation	Martin Bauer		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	WPPI Energy	Steven Leovy	Affirmative	
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	
6	ACES Power Marketing	Jason L Marshall	Abstain	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Arkansas Electric Cooperative Corporation	Keith Sugg		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Black Hills Power	andrew heinle		
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	

6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Abstain	
6	Colorado Springs Utilities	Lisa C Rosintoski		
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell		
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager		
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah		
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Municipal Power Pool	Thomas Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P. Mitchell	Affirmative	
6	Imperial Irrigation District	Cathy Bretz	Abstain	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer		
6	Luminant Energy	Brad Jones	Affirmative	
6	Madison Gas and Electric Co.	Jeffrey Keebler	Affirmative	
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	New York Power Authority	William Palazzo	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach		
6	Progress Energy	John T Sturgeon		
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen		
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	Steven J Hulet	Affirmative	
6	Santee Cooper	Michael Brown	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	William T Moojen	Affirmative	
6	South California Edison Company	Lujuanna Medina	Affirmative	
6	South Mississippi Electric Power Association	Joel Rogers	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tenaska Power Services Co.	John D Varnell	Abstain	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	
6	Westar Energy	Grant L Wilkerson	Affirmative	
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Xcel Energy, Inc.	David F Lemmons	Affirmative	
8		Edward C Stein	Affirmative	
8		James A Maenner		
8		Roger C Zaklukiewicz	Affirmative	
8	APX	Michael Johnson	Affirmative	
8	INTELLIBIND	Kevin Conway		
8	JDRJC Associates	Jim Cyrulewski	Affirmative	
8	Network & Security Technologies	Nicholas Lauriat	Abstain	
8	Power Energy Group LLC	Peggy Abbadini		
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative	
9	California Energy Commission	William M Chamberlain		
9	Central Lincoln PUD	Bruce Lovelin		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Affirmative	

9	Maine Public Utilities Commission	Michael Simmons		
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative	
9	New York State Department of Public Service	Thomas G. Dvorsky	Affirmative	
9	Oregon Public Utility Commission	Jerome Murray	Abstain	
9	Public Utilities Commission of Ohio	Klaus Lambeck		
9	Utah Public Service Commission	Ric Campbell		
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B. Edge	Affirmative	
10	Southwest Power Pool RE	Emily Pennel	Negative	
10	Texas Reliability Entity, Inc.	Donald G Jones	Affirmative	
10	Western Electricity Coordinating Council	Steven L. Rueckert		

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2009 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Project 2008-06 Cyber Security Order 706 (CIP Version 5)

Non-Binding Poll Results

Now Available

A non-binding poll of the associated VRFs/VSLs for all 10 CIP standards concluded on Tuesday, November 13, 2012.

Voting statistics for the non-binding poll are listed below.

	Non-binding Poll
VRFs/VSLs	Quorum: 75.41% Supportive Opinions: 83.82%

Next Steps
The standards will be presented to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Background
In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

Version 5 of the NERC CIP Cyber Security Standards is intended to address all remaining standards related issues of FERC Order No. 706.

The SDT believes the NERC Version 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed. Additional information about the project is available on the project webpage.

Standards Development Process
The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Development Administrator, at monica.benson@nerc.net or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Non-binding Poll Results

Project 2008-06 Non-binding Poll for 10 Standards

Non-binding Poll Results	
Non-binding Poll Name:	Project 2008-06 Non-binding Poll VRFs and VSLs - 10 Standards
Poll Period:	10/26/2012 - 11/13/2012
Total # Opinions:	365
Total Ballot Pool:	484
Summary Results:	75.41% of those who registered to participate provided an opinion or an abstention; 83.82% of those who provided an opinion indicated support for the VRFs and VSLs.

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	Comments
1	Ameren Services	Kirit Shah	Affirmative	
1	American Electric Power	Paul B. Johnson		
1	American Transmission Company, LLC	Andrew Z Pusztai	Abstain	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Abstain	
1	ATCO Electric	Glen Sutton	Abstain	
1	Austin Energy	James Armke	Affirmative	
1	Avista Corp.	Scott J Kinney	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Abstain	
1	Baltimore Gas & Electric Company	Gregory S Miller	Abstain	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Beaches Energy Services	Joseph S Stonecipher		
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Negative	
1	Central Electric Power Cooperative	Michael B Bax	Abstain	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs		
1	City of Pasadena	Marco A Sustaita	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City Water, Light & Power of Springfield	Shaun Anders		

1	Clark Public Utilities	Jack Stamper	Affirmative		
1	Cleco Power LLC	Danny McDaniel	Negative		
1	Colorado Springs Utilities	Paul Morland	Affirmative		
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative		
1	Corporate Risk Solutions, Inc.	Joseph Doetzl	Affirmative		
1	CPS Energy	Richard Castrejana	Affirmative		
1	Dairyland Power Coop.	Robert W. Roddy	Abstain		
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative		
1	Deseret Power	James Tucker			
1	Dominion Virginia Power	Michael S Crowley	Abstain		
1	Duke Energy Carolina	Douglas E. Hils	Affirmative		
1	East Kentucky Power Coop.	George S. Carruba	Affirmative		
1	Edison Electric Institute	David Batz	Abstain		
1	Empire District Electric Co.	Ralph F Meyer	Affirmative		
1	Entergy Services, Inc.	Edward J Davis	Abstain		
1	FirstEnergy Corp.	William J Smith	Abstain		
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative		
1	Florida Power & Light Co.	Mike O'Neil	Affirmative		
1	Gainesville Regional Utilities	Luther E. Fair			
1	Georgia Transmission Corporation	Jason Snodgrass	Abstain		
1	Great River Energy	Gordon Pietsch	Abstain		
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon	Affirmative		
1	Hydro One Networks, Inc.	Ajay Garg	Affirmative		
1	Hydro-Quebec TransEnergie	Bernard Pelletier			
1	Idaho Power Company	Ronald D Schellberg			
1	Imperial Irrigation District	Tino Zaragoza			
1	Indianapolis Power & Light Co.	Michael Holtsclaw			
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain		
1	JEA	Ted Hobson	Negative		
1	KAMO Electric Cooperative	Walter Kenyon			
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative		
1	Keys Energy Services	Stanley T Rzad	Affirmative		
1	Lakeland Electric	Larry E Watt			
1	Lee County Electric Cooperative	John W Delucca	Affirmative		
1	Lincoln Electric System	Doug Bantam	Abstain		
1	Lower Colorado River Authority	Martyn Turner	Affirmative		
1	M & A Electric Power Cooperative	William Price	Abstain		
1	Manitoba Hydro	Joe D Petaski	Abstain		
1	MEAG Power	Danny Dees	Affirmative		
1	MidAmerican Energy Co.	Terry Harbour	Affirmative		
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative		
1	Minnkota Power Coop. Inc.	Richard Burt			
1	Muscatine Power & Water	Tim Reed			
1	N.W. Electric Power Cooperative,	Mark Ramsey	Abstain		

	Inc.				
1	National Grid	Saurabh Saksena			
1	Nebraska Public Power District	Cole C Brodine	Affirmative		
1	New Brunswick Power Transmission Corporation	Randy MacDonald	Abstain		
1	New York Power Authority	Arnold J. Schuff	Abstain		
1	New York State Electric & Gas Corp.	Raymond P Kinney	Abstain		
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative		
1	Northeast Missouri Electric Power Cooperative	Kevin White	Abstain		
1	Northeast Utilities	David Boguslawski			
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative		
1	NorthWestern Energy	John Canavan	Affirmative		
1	Ohio Valley Electric Corp.	Robert Mattey	Abstain		
1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Abstain		
1	Omaha Public Power District	Doug Peterchuck	Affirmative		
1	Oncor Electric Delivery	Brenda Pulis	Affirmative		
1	Orange and Rockland Utilities, Inc.	Edward Bedder			
1	Orlando Utilities Commission	Brad Chase	Affirmative		
1	PacifiCorp	Ryan Millard	Abstain		
1	PECO Energy	Ronald Schloendorn	Abstain		
1	Platte River Power Authority	John C. Collins	Abstain		
1	Portland General Electric Co.	John T Walker	Affirmative		
1	Potomac Electric Power Co.	David Thorne	Abstain		
1	PowerSouth Energy Cooperative	Larry D Avery	Affirmative		
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative		
1	Progress Energy Carolinas	Brett A. Koelsch	Abstain		
1	Public Service Company of New Mexico	Laurie Williams	Affirmative		
1	Public Service Electric and Gas Co.	Kenneth D. Brown			
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel	Abstain		
1	Public Utility District No. 2 of Grant County	Kyle M. Hussey			
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative		
1	Raj Rana	Rajendrasinh D Rana			
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative		
1	Sacramento Municipal Utility District	Tim Kelley	Abstain		
1	Salmon River Electric Cooperative	Kathryn J Spence	Affirmative		
1	Salt River Project	Robert Kondziolka	Abstain		
1	Santee Cooper	Terry L Blackwell	Negative		
1	SCE&G	Henry Delk, Jr.			
1	Seattle City Light	Pawel Krupa	Abstain		

1	Sho-Me Power Electric Cooperative	Denise Stevens			
1	Sierra Pacific Power Co.	Rich Salgo	Abstain		
1	Snohomish County PUD No. 1	Long T Duong	Negative		
1	South California Edison Company	Steven Mavis	Affirmative		
1	South Mississippi Electric Power Association	Rodney A. Wilson			
1	Southern Company Services, Inc.	Robert A. Schaffeld	Negative		
1	Southern Illinois Power Coop.	William Hutchison	Negative		
1	Southwest Transmission Cooperative, Inc.	James Jones	Negative		
1	Southwestern Power Administration	Angela L Summer	Abstain		
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative		
1	Tampa Electric Co.	Beth Young	Affirmative		
1	Tennessee Valley Authority	Larry G Akens	Abstain		
1	Trans Bay Cable LLC	Steven Powell	Affirmative		
1	Transmission Agency of Northern California	Bryan Griess	Abstain		
1	Tri-State G & T Association, Inc.	Tracy Sliman	Affirmative		
1	Tucson Electric Power Co.	John Tolo	Affirmative		
1	United Illuminating Co.	Jonathan Appelbaum	Abstain		
1	Vermont Electric Power Company, Inc.	Kim Moulton			
1	Westar Energy	Allen Klassen	Abstain		
1	Western Area Power Administration	Brandy A Dunn	Affirmative		
1	Wolverine Power Supply Coop., Inc.	Michelle Denike	Affirmative		
1	Xcel Energy, Inc.	Gregory L Pieper			
2	Alberta Electric System Operator	Mark B Thompson	Abstain		
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain		
2	California ISO	Rich Vine	Affirmative		
2	Electric Reliability Council of Texas, Inc.	Charles B Manning	Affirmative		
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative		
2	Midwest ISO, Inc.	Marie Knox	Affirmative		
2	New Brunswick System Operator	Alden Briggs	Abstain		
2	New York Independent System Operator	Gregory Campoli			
2	PJM Interconnection, L.L.C.	Tom Bowe			
2	Southwest Power Pool, Inc.	Charles H. Yeung	Affirmative		
3	AEP	Michael E Deloach	Abstain		
3	Alabama Power Company	Richard J. Mandes	Negative		
3	Alameda Municipal Power	Douglas Draeger	Affirmative		
3	Ameren Services	Mark Peters	Affirmative		
3	American Public Power	Nathan Mitchell	Affirmative		

	Association				
3	Anaheim Public Utilities Dept.	Kelly Nguyen			
3	APS	Steven Norris	Affirmative		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative		
3	Atlantic City Electric Company	NICOLE BUCKMAN	Abstain		
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain		
3	Blachly-Lane Electric Co-op	Bud Tracy			
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative		
3	Central Electric Cooperative, Inc. (Redmond, Oregon)	Dave Markham			
3	Central Electric Power Cooperative	Ralph J Schulte			
3	Central Lincoln PUD	Steve Alexanderson	Abstain		
3	City of Alexandria	Michael Marcotte			
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative		
3	City of Bartow, Florida	Matt Culverhouse			
3	City of Clewiston	Lynne Mila			
3	City of Farmington	Linda R Jacobson	Abstain		
3	City of Garland	Ronnie C Hoeinghaus			
3	City of Green Cove Springs	Gregg R Griffin	Affirmative		
3	City of Lodi, California	Elizabeth Kirkley	Affirmative		
3	City of McMinnville	John C Dietz			
3	City of Palo Alto	Eric R Scott			
3	City of Redding	Bill Hughes	Abstain		
3	City Water, Light & Power of Springfield	Roger Powers			
3	Clearwater Power Co.	Dave Hagen			
3	Cleco Corporation	Michelle A Corley	Negative		
3	Colorado Springs Utilities	Charles Morgan	Affirmative		
3	ComEd	Bruce Krawczyk	Abstain		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative		
3	Constellation Energy	CJ Ingersoll	Abstain		
3	Consumers Energy	Richard Blumenstock	Abstain		
3	Consumers Power Inc.	Roman Gillen			
3	Coos-Curry Electric Cooperative, Inc	Roger Meader			
3	Cowlitz County PUD	Russell A Noble	Negative		
3	CPS Energy	Jose Escamilla	Affirmative		
3	Dayton Power & Light Co.	Jeffrey Fuller	Affirmative		
3	Delmarva Power & Light Co.	Michael R. Mayer	Abstain		
3	Detroit Edison Company	Kent Kujala	Affirmative		
3	Dominion Resources Services	Michael F. Gildea			
3	Duke Energy Carolina	Henry Ernst-Jr			
3	Entergy	Joel T Plessinger	Abstain		
3	Fall River Rural Electric Cooperative	Bryan Case			
3	FirstEnergy Energy Delivery	Stephan Kern	Abstain		

3	Flathead Electric Cooperative	John M Goroski	Abstain		
3	Florida Municipal Power Agency	Joe McKinney			
3	Florida Power Corporation	Lee Schuster	Affirmative		
3	Georgia Power Company	Anthony L Wilson	Negative		
3	Georgia Systems Operations Corporation	William N. Phinney	Abstain		
3	Grays Harbor PUD	Wesley W Gray			
3	Great River Energy	Brian Glover	Affirmative		
3	Gulf Power Company	Paul C Caldwell	Negative		
3	Hydro One Networks, Inc.	David Kiguel	Affirmative		
3	Imperial Irrigation District	Jesus S. Alcaraz			
3	JEA	Garry Baker	Abstain		
3	KAMO Electric Cooperative	Theodore J Hilmes	Abstain		
3	Kansas City Power & Light Co.	Charles Locke	Affirmative		
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative		
3	Lakeland Electric	Norman D Harryhill			
3	Lane Electric Cooperative, Inc.	Rick Crinklaw			
3	Lincoln Electric System	Jason Fortik	Abstain		
3	Los Angeles Department of Water & Power	Daniel D Kurowski	Affirmative		
3	Louisville Gas and Electric Co.	Charles A. Freibert			
3	M & A Electric Power Cooperative	Stephen D Pogue	Abstain		
3	Madison Gas and Electric Co.	Darl Shimko	Abstain		
3	Manitoba Hydro	Greg C. Parent	Abstain		
3	Manitowoc Public Utilities	Thomas E Reed	Affirmative		
3	MidAmerican Energy Co.	Thomas C. Mielnik	Abstain		
3	Mississippi Power	Jeff Franklin	Negative		
3	Modesto Irrigation District	Jack W Savage	Affirmative		
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative		
3	Muscatine Power & Water	John S Bos	Negative		
3	Nebraska Public Power District	Tony Eddleman	Abstain		
3	New York Power Authority	Marilyn Brown	Abstain		
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative		
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann			
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative		
3	Northern Lights Inc.	Jon Shelby			
3	NRG Energy Power Marketing, Inc.	Rick Keetch			
3	NW Electric Power Cooperative, Inc.	David McDowell	Abstain		
3	Ocala Electric Utility	David Anderson	Affirmative		
3	Old Dominion Electric Coop.	Bill Watson			
3	Orange and Rockland Utilities, Inc.	David Burke			
3	Orlando Utilities Commission	Ballard K Mutters	Abstain		

3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative		
3	Pacific Gas and Electric Company	John H Hagen	Affirmative		
3	PacifiCorp	Dan Zollner	Abstain		
3	Piedmont EMC	Robin W Blanton			
3	Platte River Power Authority	Terry L Baker	Abstain		
3	PNM Resources	Michael Mertz	Affirmative		
3	Potomac Electric Power Co.	Robert Reuter	Abstain		
3	Progress Energy Carolinas	Sam Waters			
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain		
3	Public Utility District No. 1 of Benton County	Gloria Bender	Affirmative		
3	Public Utility District No. 1 of Clallam County	David Proebstel			
3	Puget Sound Energy, Inc.	Erin Apperson			
3	Raft River Rural Electric Cooperative	Heber Carpenter			
3	Rutherford EMC	Thomas M Haire	Abstain		
3	Sacramento Municipal Utility District	James Leigh-Kendall	Abstain		
3	Salt River Project	John T. Underhill	Abstain		
3	Santee Cooper	James M Poston	Negative		
3	Seattle City Light	Dana Wheelock	Abstain		
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative		
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Abstain		
3	Snohomish County PUD No. 1	Mark Oens	Negative		
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative		
3	South Mississippi Electric Power Association	Gary Hutson			
3	Southern California Edison Co.	David B Coher			
3	Tacoma Public Utilities	Travis Metcalfe	Abstain		
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative		
3	Tennessee Valley Authority	Ian S Grant			
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative		
3	Turlock Irrigation District	John Souza	Affirmative		
3	Umatilla Electric Cooperative	Steve Eldrige			
3	Westar Energy	Bo Jones	Affirmative		
3	Wisconsin Electric Power Marketing	James R Keller			
3	Wisconsin Public Service Corp.	Gregory J Le Grave	Affirmative		
3	Xcel Energy, Inc.	Michael Ibold	Abstain		
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative		
4	American Municipal Power	Kevin Koloini	Abstain		
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative		
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative		
4	Central Lincoln PUD	Shamus J Gamache	Abstain		

4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative		
4	City of Clewiston	Kevin McCarthy			
4	City of New Smyrna Beach Utilities Commission	Tim Beyrle			
4	City of Redding	Nicholas Zettel	Abstain		
4	City Utilities of Springfield, Missouri	John Allen	Affirmative		
4	Consumers Energy	David Frank Ronk	Abstain		
4	Cowlitz County PUD	Rick Syring	Negative		
4	Detroit Edison Company	Daniel Herring	Affirmative		
4	Flathead Electric Cooperative	Russ Schneider			
4	Florida Municipal Power Agency	Frank Gaffney			
4	Fort Pierce Utilities Authority	Thomas Richards	Abstain		
4	Georgia System Operations Corporation	Guy Andrews	Abstain		
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain		
4	Imperial Irrigation District	Diana U Torres			
4	Indiana Municipal Power Agency	Jack Alvey	Abstain		
4	LaGen	Richard Comeaux			
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain		
4	National Rural Electric Cooperative Association	Barry R. Lawson	Abstain		
4	North Carolina Eastern Municipal Power Agency	Cecil Rhodes	Abstain		
4	Northern California Power Agency	Tracy R Bibb			
4	Ohio Edison Company	Douglas Hohlbaugh	Abstain		
4	Oklahoma Municipal Power Authority	Ashley Stringer	Abstain		
4	Pacific Northwest Generating Cooperative	Aleka K Scott			
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Negative		
4	Sacramento Municipal Utility District	Mike Ramirez	Abstain		
4	Seattle City Light	Hao Li	Abstain		
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative		
4	South Mississippi Electric Power Association	Steven McElhaney			
4	Tacoma Public Utilities	Keith Morisette	Abstain		
4	West Oregon Electric Cooperative, Inc.	Marc M Farmer			
4	Wisconsin Energy Corp.	Anthony Jankowski	Abstain		
4	WPPI Energy	Patrick Connors			
5	AEP Service Corp.	Brock Ondayko	Abstain		
5	AES Corporation	Leo Bernier	Affirmative		
5	Amerenue	Sam Dwyer	Affirmative		
5	Arizona Public Service Co.	Edward Cambridge	Affirmative		

5	Associated Electric Cooperative, Inc.	Brad Haralson			
5	Avista Corp.	Edward F. Groce	Affirmative		
5	BC Hydro and Power Authority	Clement Ma	Abstain		
5	Black Hills Corp	George Tatar	Affirmative		
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Abstain		
5	Bonneville Power Administration	Francis J. Halpin	Affirmative		
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative		
5	BrightSource Energy, Inc.	Chifong Thomas			
5	Caithness Long Island, LLC	Jason M Moore			
5	Chelan County Public Utility District #1	John Yale	Abstain		
5	City and County of San Francisco	Daniel Mason			
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative		
5	City of Redding	Paul A. Cummings	Abstain		
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative		
5	City of Tallahassee	Brian Horton			
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative		
5	Cleco Power	Stephanie Huffman	Negative		
5	Cogentrix Energy, Inc.	Mike D Hirst	Affirmative		
5	Colorado Springs Utilities	Jennifer Eckels	Affirmative		
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative		
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Abstain		
5	Consumers Energy Company	David C Greyerbiehl	Abstain		
5	Cowlitz County PUD	Bob Essex	Negative		
5	CPS Energy	Robert Stevens	Affirmative		
5	Dairyland Power Coop.	Tommy Drea			
5	Detroit Edison Company	Christy Wicke	Affirmative		
5	Dominion Resources, Inc.	Mike Garton	Abstain		
5	Duke Energy	Dale Q Goodwine	Affirmative		
5	Dynegy Inc.	Dan Roethemeyer	Affirmative		
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain		
5	Edison Mission Marketing & Trading Inc.	Brenda J Frazer	Affirmative		
5	Electric Power Supply Association	John R Cashin	Abstain		
5	Energy Services, Inc.	Tracey Stubbs	Abstain		
5	Exelon Nuclear	Michael Korchynsky	Abstain		
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative		
5	FirstEnergy Solutions	Kenneth Dresner			
5	Florida Municipal Power Agency	David Schumann			
5	Great River Energy	Preston L Walsh			

5	Green Country Energy	Greg Froehling			
5	Imperial Irrigation District	Marcela Y Caballero			
5	JEA	John J Babik	Affirmative		
5	Kansas City Power & Light Co.	Brett Holland	Affirmative		
5	Kissimmee Utility Authority	Mike Blough	Abstain		
5	Lakeland Electric	James M Howard	Affirmative		
5	Liberty Electric Power LLC	Daniel Duff	Negative		
5	Lincoln Electric System	Dennis Florom	Abstain		
5	Los Angeles Department of Water & Power	Kenneth Silver	Abstain		
5	Lower Colorado River Authority	Tom Foreman			
5	Luminant Generation Company LLC	Mike Laney	Affirmative		
5	Madison Gas and Electric Co.	Steven Schultz	Abstain		
5	Manitoba Hydro	S N Fernando	Abstain		
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain		
5	MEAG Power	Steven Grego	Affirmative		
5	MidAmerican Energy Co.	Christopher Schneider	Abstain		
5	Muscatine Power & Water	Mike Avesing	Negative		
5	Nebraska Public Power District	Don Schmit	Affirmative		
5	New York Power Authority	Gerald Mannarino	Abstain		
5	NextEra Energy	Allen D Schriver	Affirmative		
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative		
5	Northern California Power Agency	Hari Modi			
5	Northern Indiana Public Service Co.	William O. Thompson	Affirmative		
5	NRG Energy, Inc.	Patricia A. Lynch			
5	Occidental Chemical	Michelle R DAntuono	Affirmative		
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative		
5	Orlando Utilities Commission	Richard K Kinas	Affirmative		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative		
5	PacifiCorp	Sandra L. Shaffer			
5	Platte River Power Authority	Roland Thiel	Abstain		
5	Portland General Electric Co.	Gary L Tingley	Affirmative		
5	PowerSouth Energy Cooperative	Tim Hattaway	Abstain		
5	PPL Generation LLC	Annette M Bannon	Affirmative		
5	Progress Energy Carolinas	Wayne Lewis			
5	PSEG Fossil LLC	Tim Kucey	Abstain		
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins	Affirmative		
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative		
5	Puget Sound Energy, Inc.	Tom Flynn			
5	Reedy Creek Energy Services	Bernie Budnik			
5	Sacramento Municipal Utility District	Bethany Hunter	Abstain		
5	Salt River Project	William Alkema			

5	Santee Cooper	Lewis P Pierce	Negative		
5	Seattle City Light	Michael J. Haynes	Abstain		
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative		
5	Snohomish County PUD No. 1	Sam Nietfeld	Negative		
5	South Carolina Electric & Gas Co.	Edward Magic			
5	South Mississippi Electric Power Association	Jerry W Johnson			
5	Southern California Edison Co.	Denise Yaffe	Affirmative		
5	Southern Company Generation	William D Shultz	Affirmative		
5	Tampa Electric Co.	RJames Rocha	Affirmative		
5	Tenaska, Inc.	Scott M. Helyer	Abstain		
5	Tennessee Valley Authority	David Thompson	Abstain		
5	Trans Canada Power	John Fish	Affirmative		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran			
5	Tri-State G & T Association, Inc.	Barry Ingold			
5	U.S. Army Corps of Engineers	Melissa Kurtz			
5	U.S. Bureau of Reclamation	Martin Bauer			
5	Westar Energy	Bryan Taggart			
5	Wisconsin Electric Power Co.	Linda Horn	Abstain		
5	WPPI Energy	Steven Leovy	Abstain		
5	Xcel Energy, Inc.	Liam Noailles	Abstain		
6	ACES Power Marketing	Jason L Marshall	Abstain		
6	AEP Marketing	Edward P. Cox	Abstain		
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative		
6	APS	Randy A. Young	Affirmative		
6	Arkansas Electric Cooperative Corporation	Keith Sugg	Affirmative		
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Abstain		
6	Black Hills Power	andrew heinle			
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative		
6	City of Austin dba Austin Energy	Lisa L Martin	Affirmative		
6	City of Redding	Marvin Briggs	Abstain		
6	Cleco Power LLC	Robert Hirchak	Negative		
6	Colorado Springs Utilities	Lisa C Rosintoski			
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative		
6	Constellation Energy Commodities Group	Brenda L Powell	Abstain		
6	Dominion Resources, Inc.	Louis S. Slade	Abstain		
6	Duke Energy Carolina	Walter Yeager			
6	Entergy Services, Inc.	Terri F Benoit	Abstain		
6	Exelon Power Team	Pulin Shah	Abstain		
6	FirstEnergy Solutions	Kevin Querry	Abstain		
6	Florida Municipal Power Agency	Richard L. Montgomery			
6	Florida Municipal Power Pool	Thomas Washburn	Abstain		
6	Florida Power & Light Co.	Silvia P. Mitchell	Abstain		

6	Imperial Irrigation District	Cathy Bretz	Abstain		
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative		
6	Lakeland Electric	Paul Shipps	Affirmative		
6	Lincoln Electric System	Eric Ruskamp	Abstain		
6	Los Angeles Department of Water & Power	Brad Packer	Abstain		
6	Luminant Energy	Brad Jones	Affirmative		
6	Madison Gas and Electric Co.	Jeffrey Keebler	Abstain		
6	Manitoba Hydro	Daniel Prowse	Abstain		
6	MidAmerican Energy Co.	Dennis Kimm	Abstain		
6	New York Power Authority	William Palazzo	Affirmative		
6	North Carolina Municipal Power Agency #1	Matthew Schull	Affirmative		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative		
6	NRG Energy, Inc.	Alan Johnson	Abstain		
6	Omaha Public Power District	David Ried	Affirmative		
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative		
6	PacifiCorp	Scott L Smith	Abstain		
6	Platte River Power Authority	Carol Ballantine	Abstain		
6	Portland General Electric Co.	John Jamieson			
6	PPL EnergyPlus LLC	Mark A Heimbach			
6	Progress Energy	John T Sturgeon			
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain		
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen			
6	Sacramento Municipal Utility District	Diane Enderby	Abstain		
6	Salt River Project	Steven J Hulet	Abstain		
6	Santee Cooper	Michael Brown	Negative		
6	Seattle City Light	Dennis Sismaet	Affirmative		
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative		
6	Snohomish County PUD No. 1	William T Moojen			
6	South California Edison Company	Lujuanna Medina	Affirmative		
6	South Mississippi Electric Power Association	Joel Rogers	Abstain		
6	Southern Company Generation and Energy Marketing	John J. Ciza	Negative		
6	Tacoma Public Utilities	Michael C Hill	Affirmative		
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative		
6	Tenaska Power Services Co.	John D Varnell	Affirmative		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain		
6	Westar Energy	Grant L Wilkerson			
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative		
6	Xcel Energy, Inc.	David F Lemmons	Abstain		

8		Roger C Zaklukiewicz	Affirmative		
8		Edward C Stein	Affirmative		
8		James A Maenner	Abstain		
8	APX	Michael Johnson	Affirmative		
8	INTELLIBIND	Kevin Conway	Negative		
8	JDRJC Associates	Jim Cyrulewski	Affirmative		
8	Network & Security Technologies	Nicholas Lauriat	Abstain		
8	Power Energy Group LLC	Peggy Abbadini			
8	Utility Services, Inc.	Brian Evans-Mongeon	Abstain		
8	Volkmann Consulting, Inc.	Terry Volkmann	Affirmative		
9	California Energy Commission	William M Chamberlain			
9	Central Lincoln PUD	Bruce Lovelin			
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson			
9	Maine Public Utilities Commission	Michael Simmons			
9	National Association of Regulatory Utility Commissioners	Diane J. Barney	Affirmative		
9	New York State Department of Public Service	Thomas G. Dvorsky	Affirmative		
9	Oregon Public Utility Commission	Jerome Murray	Abstain		
9	Public Utilities Commission of Ohio	Klaus Lambeck			
9	Utah Public Service Commission	Ric Campbell	Affirmative		
10	Florida Reliability Coordinating Council	Linda Campbell	Abstain		
10	Midwest Reliability Organization	James D Burley	Abstain		
10	New York State Reliability Council	Alan Adamson	Affirmative		
10	Northeast Power Coordinating Council	Guy V. Zito	Affirmative		
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative		
10	SERC Reliability Corporation	Carter B. Edge	Abstain		
10	Southwest Power Pool RE	Emily Pennel	Abstain		
10	Texas Reliability Entity, Inc.	Donald G Jones	Negative		
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain		

Exhibit G

Order No. 672 Criteria for Approving Proposed Reliability Standards

EXHIBIT G – Demonstration that the proposed Reliability Standard is just, reasonable, not unduly discriminatory or preferential and in the public interest

Order No. 672 Criteria

In order to approve a Reliability Standard proposed by the ERO, FERC must determine, after notice and opportunity for public hearing, that the standard is just, reasonable, not unduly discriminatory or preferential and in the public interest. In Order No. 672,[58] FERC identified a number of criteria it will use to analyze Reliability Standards proposed for approval to ensure they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. Consideration of how proposed CIP Version 5 meets the guidelines identified by FERC in Order No. 672 as necessary to concluding a Reliability Standard meets the statutory criteria follows:

1. Proposed Reliability Standards must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve that goal.[59]

The proposed CIP Version 5 provides a cyber security framework for the identification and protection of BES Cyber Systems to support the reliable operation of

---

[58] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

[59] Order No. 672 at P 321. The proposed Reliability Standard must address a reliability concern that falls within the requirements of section 215 of the FPA. That is, it must provide for the reliable operation of Bulk-Power System facilities. It may not extend beyond reliable operation of such facilities or apply to other facilities. Such facilities include all those necessary for operating an interconnected electric energy transmission network, or any portion of that network, including control systems. The proposed Reliability Standard may apply to any design of planned additions or modifications of such facilities that is necessary to provide for reliable operation. It may also apply to Cybersecurity protection.

Order No. 672 at P 324. The proposed Reliability Standard must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve this goal. Although any person may propose a topic for a Reliability Standard to the ERO, in the ERO's process, the specific proposed Reliability Standard should be developed initially by persons within the electric power industry and community with a high level of technical expertise and be based on sound technical and engineering criteria. It should be based on actual data and lessons learned from past operating incidents, where appropriate. The process for ERO approval of a proposed Reliability Standard should be fair and open to all interested persons.

the BES. These standards recognize the differing roles of each entity in the operation of the BES, the criticality and vulnerability of the assets needed to manage BES reliability, and the risks to which they are exposed. Business and operational demands for maintaining a reliable BES increasingly rely on BES Cyber Systems to support critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these BES Cyber Systems.

2. Proposed Reliability Standards must be applicable only to users, owners and operators of the Bulk Power System, and must be clear and unambiguous as to what is required and who is required to comply.[60]

The proposed CIP Version 5 is applicable to Reliability Coordinators, Balancing Authorities, Interchange Authorities, Transmission Owners, Transmission Operators, Generator Owners, Generator Operators, and Distribution Providers (collectively referred to as Responsible Entities). These entities are users, owners, or operators of the Bulk Power System.

The proposed CIP Version 5 standards achieve their stated goal of providing a cyber security framework for the identification and protection of BES Cyber Systems that support reliable operation of the BES. Specifically, proposed Reliability Standard CIP-002-5 requires the identification and documentation of BES Cyber Systems for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable

---

[60] Order No. 672 at P 322. The proposed Reliability Standard may impose a requirement on any user, owner, or operator of such facilities, but not on others.

Order No. 672 at P 325. The proposed Reliability Standard should be clear and unambiguous regarding what is required and who is required to comply. Users, owners, and operators of the Bulk-Power System must know what they are required to do to maintain reliability.

operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. These BES Cyber Systems are to be identified through the application of the criteria included in Attachment 1 of the proposed CIP-002-5 standard.

Requirement R1 requires a process for the consideration of certain assets for the identification of high impact and medium impact BES Cyber Systems, as specified under the impact criteria in Attachment 1, at each of those assets. It also requires identification of the assets that have Low Impact BES Cyber Systems. This will ensure that entities evaluate their entire portfolio of BES assets against the criteria in Attachment 1 to determine those assets that have BES Cyber Systems that support the reliable operation of the BES.

Requirement R2 mandates that lists required by Requirement R1 are reviewed by a CIP Senior Manager on a periodic basis. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

The rest of the proposed CIP Version 5 mandates the minimum protection that must be provided to those BES Cyber Systems identified in CIP-002-5.

Reliability Standard CIP-003-5 requires each Responsible Entity, for its high impact and medium impact BES Cyber Systems, to review and obtain CIP Senior Manager Approval at least once every 15 calendar months for documented cyber security policies that collectively address topics referenced in CIP-004 through CIP-011-1. In addition, each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3 (those assets that have low impact BES Cyber Systems), shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber

security policies that collectively address the following topics: cyber security awareness; physical security controls; electronic access controls for external routable protocol connections and Dial-up Connectivity; and incident response to a Cyber Security Incident.

Reliability Standard CIP-004-5 requires that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such access maintain awareness of the Responsible Entity's security practices.

Reliability Standard CIP-005-5 requires Responsible Entities to manage electronic access to BES Cyber Systems by specifying a controlled ESP in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. It also establishes requirements for management of secure remote access to Cyber Assets in order to provide adequate safeguards through robust identification, authentication, and encryption techniques.

Reliability Standard CIP-006-5 requires Responsible Entities to manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Reliability Standard CIP-007-5 requires Responsible Entities to manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Reliability Standard CIP-008-5 requires Responsible Entities to mitigate the risk to the reliable operation of the BES in the case of a Cyber Security Incident by specifying incident response requirements.

Reliability Standard CIP-009-5 requires Responsible Entities, in order to support recovery of reliability functions performed by BES Cyber Systems, to specify recovery plans in support of the continued stability, operability, and reliability of the BES.

Reliability Standard CIP-010-1 requires Responsible Entities, for the purpose of preventing and detecting unauthorized changes to BES Cyber Systems, to meet configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

Reliability Standard CIP-011-1 requires Responsible Entities, in order to prevent unauthorized access to BES Cyber System Information, to meet certain information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

The proposed CIP Version 5 standards have been developed by a standard drafting team with a broad base of BES and cyber security knowledge following the scope identified in the Standard Authorization Request that resulted in the initiation of NERC Project 2008-06 Cyber Security Order 706. The standard drafting team for this project adhered to NERC's regulatory-approved standards development process, which allows for industry comment and ballot of the proposed standards. Extensive industry comments on the proposed standards were received and evaluated through several

postings. Many of the comments have been incorporated into the final draft of the standards, resulting in thoroughly vetted, high quality standards.

3. A proposed Reliability Standard must include clear and understandable consequences and a range of penalties (monetary and/or non-monetary) for a violation.[61]

Each primary requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the ERO Sanction Guidelines. The table included in **Exhibit F** shows the VRFs and VSLs resulting in the indicated range of penalties for violations.

4. A proposed Reliability Standard must identify clear and objective criterion or measure for compliance, so that it can be enforced in a consistent and non-preferential manner.[62]

Each of the requirements in the proposed CIP Version 5 is clear in identifying the required performance and the responsible entity. The proposed CIP Version 5 identifies clear and objective criteria in the language of the requirements so that that the standards can be enforced in a consistent and non-preferential manner. The language in the requirements is unambiguous with respect to the applicable entity expectations. Each requirement has a single associated measure.

---

[61] Order No. 672 at P 326. The possible consequences, including range of possible penalties, for violating a proposed Reliability Standard should be clear and understandable by those who must comply.

[62] Order No. 672 at P 327. There should be a clear criterion or measure of whether an entity is in compliance with a proposed Reliability Standard. It should contain or be accompanied by an objective measure of compliance so that it can be enforced and so that enforcement can be applied in a consistent and non-preferential manner.

5. Proposed Reliability Standards should achieve a reliability goal effectively and efficiently — but do not necessarily have to reflect "best practices" without regard to implementation cost or historical regional infrastructure design.[63]

The proposed CIP Version 5 helps the industry achieve the stated goals of identifying BES Cyber Systems and their associated BES Cyber Assets to ensure BES reliability effectively and efficiently. While there may be an increase in implementation costs as the number of assets within scope of the CIP Version 5 standards increase under the methodology in proposed CIP-002-5, the NERC Board of Trustees and the industry approved the revised methodology because there is recognition that it is needed to help ensure Bulk Power System reliability. Accordingly, the costs associated with implementing the proposed CIP-002 through CIP-011 Reliability Standards are not determined to be excessive or unreasonably burdensome.

6. Proposed Reliability Standards cannot be "lowest common denominator," *i.e.*, cannot reflect a compromise that does not adequately protect Bulk-Power System reliability. Proposed Reliability Standards can consider costs to implement for smaller entities, but not at consequences of less than excellence in operating system reliability.[64]

---

[63] Order No. 672 at P 328. The proposed Reliability Standard does not necessarily have to reflect the optimal method, or "best practice," for achieving its reliability goal without regard to implementation cost or historical regional infrastructure design. It should however achieve its reliability goal effectively and efficiently.

[64] Order No. 672 at P 329. The proposed Reliability Standard must not simply reflect a compromise in the ERO's Reliability Standard development process based on the least effective North American practice — the so-called "lowest common denominator" — if such practice does not adequately protect Bulk-Power System reliability. Although FERC will give due weight to the technical expertise of the ERO, we will not hesitate to remand a proposed Reliability Standard if we are convinced it is not adequate to protect reliability.

Order No. 672 at P 330. A proposed Reliability Standard may take into account the size of the entity that must comply with the Reliability Standard and the cost to those entities of implementing the proposed Reliability Standard. However, the ERO should not propose a "lowest common denominator" Reliability Standard that would achieve less than excellence in operating system reliability solely to protect against reasonable expenses for supporting this vital national infrastructure. For example, a small owner or operator of the Bulk-Power System must bear the cost of complying with each Reliability Standard that applies to it.

The proposed CIP Version 5 does not aim at the "lowest common denominator." The proposed CIP-002-5 standard provides clear and uniform criteria for identifying BES Cyber Systems on the Bulk Electric System. The proposed CIP-003-5 to CIP-09-5, retain the same requirement language as the previous FERC approved standards, with confirming modifications, and have already been determined to meet this criterion. Proposed CIP-010-1 and CIP-011-1 are new standards that contain requirements previously defined across several CIP standards in Versions 1 through 4.

7. Proposed Reliability Standards must be designed to apply throughout North America to the maximum extent achievable with a single Reliability Standard while not favoring one geographic area or regional model. It should take into account regional variations in the organization and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.[65]

The requirements in the proposed CIP Version 5 apply throughout North America, with no exceptions. CIP Version 5 is a set of standards that will be universally applicable in the portions of the United States and Canada that recognize NERC as the ERO.

[64] Order No. 672 at P 331. A proposed Reliability Standard should be designed to apply throughout the interconnected North American Bulk-Power System, to the maximum extent this is achievable with a single Reliability Standard. The proposed Reliability Standard should not be based on a single geographic or regional model but should take into account geographic variations in grid characteristics, terrain, weather, and other such factors; it should also take into account regional variations in the organizational and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.

8. Proposed Reliability Standards should cause no undue negative effect on competition or restriction of the grid beyond any restriction necessary for reliability.[66]

The proposed CIP Version 5 enhances the operation and reliability of the grid and do not constrain competition or restrict transmission capability. The purpose of the proposed CIP Version 5 is to provide a cybersecurity framework for the identification and protection of BES Cyber Systems to support reliable operation of the Bulk Electric System.

Specifically, proposed Reliability Standard CIP-002-5 requires the identification and documentation of the BES Cyber Systems that support the reliable operation of the BES. The proposed CIP Version 5 does not have a business practice impact and thus will not result in a negative effect on competition.

9. The implementation time for the proposed Reliability Standard is reasonable.[67]

The Implementation Plan provided in **Exhibit B** specifies how Responsible Entities should transition during the timeframe from FERC acceptance of proposed CIP Version 5 until the Effective Date:

> 24 Months Minimum – The Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the

[66] Order No. 672 at P 332. As directed by section 215 of the FPA, FERC itself will give special attention to the effect of a proposed Reliability Standard on competition. The ERO should attempt to develop a proposed Reliability Standard that has no undue negative effect on competition. Among other possible considerations, a proposed Reliability Standard should not unreasonably restrict available transmission capability on the Bulk-Power System beyond any restriction necessary for reliability and should not limit use of the Bulk-Power System in an unduly preferential manner. It should not create an undue advantage for one competitor over another.

[67] Order No. 672 at P 333. In considering whether a proposed Reliability Standard is just and reasonable, FERC will consider also the timetable for implementation of the new requirements, including how the proposal balances any urgency in the need to implement it against the reasonableness of the time allowed for those who must comply to develop the necessary procedures, software, facilities, staffing or other relevant capability.

> later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.

Upon FERC approval, the proposed implementation plan will allow Responsible Entities to transition directly to CIP Version 5, by staying the effective date for CIP Version 4. In the interim, CIP Version 3 will remain in effect.

Based on precedent and lessons learned from past practice, NERC believes the length of time between FERC approval of the proposed CIP Version 4 standards and the effective date is reasonable. The proposed CIP Version 5 standards do not create any differentiation in requirements based on size. All entities, small and large, are expected to comply with these standards in the same manner.

In addition, NERC recognizes that it takes time to perform a thorough examination of all BES assets to determine whether they meet the criteria included in Attachment 1. Furthermore, new equipment may have to be installed, and new policies and procedures implemented, by Responsible Entities in order to meet the requirements of the CIP-003-5 through CIP-009-5 Reliability Standards.

Several commenters questioned the need for an additional year of implementation time for low impact BES Cyber Systems. In response, the standards drafting team determined that an additional year of implementation for low impact BES Cyber Systems is needed to allow Responsible Entities to formulate and implement effective security solutions for physical and electronic perimeter protection. Despite not requiring an

inventory of low impact BES Cyber Systems, entities must still implement these policy changes in applicable locations where no perimeter protection currently exists. As such, staggered implementation promotes prioritization of high and medium impact assets.

10. The Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[68]

NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure, the NERC *Reliability Standards Development Procedure*, and its replacement NERC *Standards Processes Manual*, which is incorporated into the Rules of Procedure as Appendix 3A. In its ERO Certification Order, FERC determined that NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards. The development process is open to any person or entity with a legitimate interest in the reliability of the Bulk Power System. NERC considers the comments of all stakeholders and a vote of stakeholders and the NERC Board of Trustees is required to approve a Reliability Standard for submission to FERC. The drafting team developed this standard by following NERC's regulatory-approved standards development process.

[68] Order No. 672 at P 334. Further, in considering whether a proposed Reliability Standard meets the legal standard of review, we will entertain comments about whether the ERO implemented its Commission-approved Reliability Standard development process for the development of the particular proposed Reliability Standard in a proper manner, especially whether the process was open and fair. However, we caution that we will not be sympathetic to arguments by interested parties that choose, for whatever reason, not to participate in the ERO's Reliability Standard development process if it is conducted in good faith in accordance with the procedures approved by FERC.

11. NERC must explain any balancing of vital public interests in the development of proposed Reliability Standards.[69]

NERC has identified no competing public interests regarding the request for approval of this proposed CIP Version 5. No comments were received that indicated the proposed standards conflicts with other vital public interests.

12. Proposed Reliability Standards must consider any other appropriate factors.[70]

No other factors for FERC's consideration were identified in the development of the proposed CIP Version 5.

13. Proposed Reliability Standard must not conflict with prior FERC Rules or Orders.[71]

The proposed CIP Version 5 standards do not conflict with any other prior FERC Rules or Orders. The proposed CIP Version 5 addresses several of the directives identified in FERC Order No. 706 that were not addressed in prior versions. The standard drafting team is continuing to develop CIP Version 5 standards that meet the rest of the directives identified in FERC Order No. 706.

---

[69] Order No. 672 at P 335. Finally, we understand that at times development of a proposed Reliability Standard may require that a particular reliability goal must be balanced against other vital public interests, such as environmental, social and other goals. We expect the ERO to explain any such balancing in its application for approval of a proposed Reliability Standard.

[70] Order No. 672 at P 323. In considering whether a proposed Reliability Standard is just and reasonable, we will consider the following general factors, as well as other factors that are appropriate for the particular Reliability Standard proposed.

[71] Order No. 672 at P 444. A potential conflict between a Reliability Standard under development and a Transmission Organization function, rule, order, tariff, rate schedule, or agreement accepted, approved, or ordered by the Commission should be identified and addressed during the ERO's Reliability Standard Development Process.

Exhibit H

Consideration of Issues and Directives

Project 2008-06 - Cyber Security Order No. 706 - V5

Consideration of Issues and Directives

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 233 (Related paragraph: 25) Para 233 "The Commission continues to believe and is further persuaded by the comments that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. Moreover, we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk-Power System should be addressed in NERCs Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need	FERC Order No. 706	In its development of CIP Version 5, the Standards Drafting Team (SDT) considered many existing cyber security frameworks. Notably, the SDT included consideration of the NIST Risk Management Framework, NIST Publication 800-53, as well as the "DHS Catalog of Control Systems Security: Recommendations for Standards Developers" in the development of its requirements for cyber systems categorization and applicable requirements. Five key features of the NIST Risk Management Framework were incorporated into Version 5 of NERC CIP Standards: (1) ensuring that all BES Cyber Systems associated with the Bulk Power System, based on their function, receive some level of protection, (2) customizing protection to the mission of the cyber systems subject to protection, (3) a tiered approach to security controls which specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk Power System, (4) the concept of the BES Cyber System itself, and (5) Version 5 has incorporated the "Assess" and "Monitor" processes of the NIST Risk Management Framework in the development of the requirements and enabled these processes through additional language for identifying, assessing, and correcting deficiencies in controls.. Features 2 and 3 above are tightly coupled. In the NIST Risk Management Framework, there is a concept of tailoring and scoping which allows the organization to determine which controls are applicable to their specific environment. In the NERC compliance framework, all requirements are mandatory and enforceable, and, therefore, this concept does not translate directly. As such, the customization of protections by mission is based upon the environment that the BES Cyber System supports (control center, transmission facility, generation facility) and utilizes the tiered model and the requirement applicability to provide this customization to the individual environments that together support a

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
for new CIP Reliability Standards, or as part of an assessment of NERCs performance of its responsibilities as the ERO." Para 25 "The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework. "		combined mission of Bulk Power System reliability. The NIST Security Control Catalogue in 800-53, Revision 3 and the DHS Catalog of Controls Systems Security were also used as a reference in addressing many of the FERC directives in Order No. 706. Additionally, the SDT included members representing federal agencies and NIST, in particular, during the development of these CIP standards.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 and 249 Para 258 "Likewise, the ERO should consider Northern Californias suggestion that the ERO establish a formal feedback loop to assist the industry in developing policies and procedures." Para 249 "In contrast, FirstEnergy agrees that NERC should provide guidance to entities without a wide-area view, such as a generation owner or a partial generation owner, on how to approach a risk-based assessment. Likewise, Northern California suggests that NERC establish a process for informal, case-by-case consultations with responsible entities that need assistance in complying with CIP-002-1. In addition, as part of the re-examination of CIP-002-1, Northern California encourages the incorporation of a formalized feedback loop to assist the industry in developing policies and procedures."	FERC Order No. 706	CIP-002-5 classifies BES Cyber Systems through impact thresholds, and does not use risk-based assessments performed by individual entities. CIP-002-5, Attachment 1's bright line criteria were developed in consideration of a wide area view, and it obviates the need for a formal feedback loop or a need for a wide area view by smaller entities.
Para 258 and 252	FERC Order No. 706	Early during the development of CIP-002-5, the SDT discussed the concept of Design-Basis Threat (DBT). The SDT, in CIP-002-5, classifies BES Cyber Systems through impact

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 "As to Entergys suggestion that the ERO provide a DBT profile of potential adversaries, the ERO should consider this issue in the Reliability Standards development process." Para 252 "Entergy suggests, as an alternative approach to critical asset identification, that the ERO provide a Design-Basis Threat (DBT) a profile of the type, composition, and capabilities of an adversary that would assist the industry as a technical baseline against which to establish the proper designs, controls and processes. Entergy claims that a DBT approach would address many of the Commissions concerns regarding the risk-based methodology. For example, a DBT would focus the appropriate emphasis on the potential consequences from an outage of a critical asset. In addition, a DBT would address the Commissions concern that responsible entities will not have enough guidance in developing a risk-based methodology and not know how to identify a critical asset. Entergy contends that a DBT		thresholds, and does not use risk-based assessments performed by individual entities. The complexity and subjectivity involved in an entity's risk-based assessment, such as one based on DBT, would run counter to the CIP-002-5 objectives of categorization based on impact defined by bright-line criteria. CIP-002-5, Attachment 1's bright line criteria uses an impact-based approach as an alternative to DBT. This approach was approved by the Commission in its Order No. 761 approving Version 4 of the CIP Cyber Security Standards.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
approach would provide the industry with more certainty in implementing the CIP Reliability Standards."		
Para 272 (1 of 2) "Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, **the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset.** In doing so, the ERO should consider Juniper's comments. Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data."	FERC Order No. 706	This was completed by CIPC in the Version 3 CIP standards guidelines. The guidelines are entitled "Identifying Critical Assets" and "Identifying Critical Cyber Assets" and are available for download from www.nerc.com.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 272 (2 of 2) "Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset. In doing so, the ERO should consider Juniper's comments. **Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data."**	FERC Order No. 706	Guidance developed for CIP-002-5 addresses situational awareness and inter-utility data exchange.
Para 285 (related paragraph: 278) Para 285 "The Commission directs the ERO to consider the comment from ISA99 Team	FERC Order No. 706	The exclusion of Cyber Assets based on non-routable protocols has been removed from CIP-002-5, and added as an applicability filter for requirements where: (i) the use of non-routable protocols is a mitigating factor for the vulnerabilities a requirement addresses, or (ii) implementation of routable protocols, when not otherwise used, would be required to comply with the requirement (e.g. malware updates, security event monitoring, and alerting, etc.).

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
[ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience].” Para 278 “ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience. In contrast, Energy Producers notes that CIP-002-1 as proposed by NERC provides that a critical cyber asset must have either routable protocols or a dial-up connection. Energy Producers states that this is a useful, objective criterion which will assist in the unambiguous identification of such assets and therefore should be retained.”		

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 296 "With regard to METC-ITC's comment, the ERO should consider in its Reliability Standards development process the suggestion that the CIP Reliability Standards require oversight by a corporate officer (or the equivalent, since some entities do not have corporate officers) rather than by a "senior manager."	FERC Order No. 706	The requirement that the senior manager have "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" ensures that the senior manager is of the sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for Responsible Entities, from municipal, cooperative, federal agencies, investor-owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis. In Version 5, this is addressed in the definition of CIP Senior Manager. The SDT believes the filing for Version 2 also addressed this issue.
Para 321 " SPP and ReliabilityFirst suggest modifying CIP-002-1 to allow an entity to rely upon the assessment of another entity with interest in the matter. We believe that this is a worthwhile suggestion for the ERO to pursue and the ERO should consider this proposal in the Reliability Standards development process. We note that, even without such a provision, an entity such as a small generator operator is not foreclosed from consulting with a balancing authority or other appropriate entity with a wide-area view of the transmission system."	FERC Order No. 706	The SDT believes that this suggestion would be applicable in a model of an entity's own risk-based methodology, where certain small entities may not benefit from a wider area view. The change to "bright line" criteria for identifying BES Cyber Systems in CIP-002-5, along with refining the scope of certain requirements through applicability columns based on impact and connectivity characteristics, no longer requires entities to use a self-defined risk-based methodology, which addresses this concern.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 355 (also see paragraph 356) "The Commission believes that responsible entities would benefit from additional guidance regarding the topics and processes to address in the cyber security policy required pursuant to CIP-003-1. While commenters support the need for guidance, many are concerned about providing such guidance through a modification of the Reliability Standard. We are persuaded by these commenters. Accordingly, the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address. However, we will not dictate the form of such guidance. For example, the ERO could develop a guidance document or white paper that would be referenced in the Reliability Standard. On the other hand, if it is determined in the course of the Reliability Standards development process that specific guidance is important enough to be incorporated directly into a Requirement, this option is not foreclosed. The entities remain responsible, however, to comply with the cyber security policy pursuant to CIP-003-1."		The SDT has chosen to provide guidance to Responsible Entities through the introduction of topical areas in the requirement language that must be addressed in cyber security policies in CIP-003-5, requirements R1 and R2. Additionally, as directed, the SDT has provided guidance about these topical areas in the Guidelines and Technical Basis section of Reliability Standard CIP-003-5.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 376 ". . . the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards. In response to EEI, we believe that this clarification is needed because, for example, it is important that a responsible entity understand that exceptions that individually may be acceptable must not lead cumulatively to results that undermine compliance with the Requirements themselves."	FERC Order No. 706	The SDT removed the CIP-003-4 requirement to document exceptions to the Cyber Security Policy. • The SDT considers this a general management issue that is not within the scope of a compliance requirement. • The SDT found no reliability basis in this requirement. • Removal of this requirement provides clarity that the only exceptions to the requirements is through the defined Technical Feasibility Exception process, where specifically allowed.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 386 "The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly. In general, the Commission agrees with commenters and believes that access to protected information should cease as soon as possible but not later than 24 hours from the time of termination for cause."	FERC Order No. 706	To address this directive, in CIP-004-5, requirement R5, Responsible Entities must revoke access to the electronic and physical locations where it stores BES Cyber System Information. This could include records, closets, substation control houses, records management systems, file shares, or other physical and logical areas under the Responsible Entity's control. The SDT specified the revocation action to be completed "by the end of the next calendar day following the effective date and time of the termination action" to provide a more defined time threshold, following the SDT's discussion of the difficulty in defining an exact time in a termination process that typically includes multiple steps and organizations within an entity.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 397 and 398 "The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes. The Commission believes that these considerations are significant aspects of change control and configuration management that deserve express acknowledgement in the Reliability Standard. While we agree with Entergy that the NIST Security Risk Management Framework offers valuable guidance on how to deal with these matters, our concern here is that the potential problems alluded to be explicitly acknowledged. Our proposal does not speak to how these problems should be addressed. We do not believe that the changes will have burdensome consequences, but we also note that addressing any unnecessary burdens can be dealt with in the Reliability Standards development process."	FERC Order No. 706	Two new requirements in a new standard CIP-010-1 were added to address this change: CIP-010-1, requirement R1 (part 1.5), requires additional testing prior to a configuration change in a test environment; CIP-010-1, requirement R2 (part 2.1), requires monitoring of the configuration of the BES Cyber System. • The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System. • Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) prior to their implementation in the production environment to aid in identifying any accidental consequences, to required cyber security controls, of the change.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 412 "The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world."	FERC Order No. 706	The SDT addresses this through the defense in depth framework that has been designed through the full suite of revised CIP Standards. The standards address defense in depth through personnel management, systems management, and information management. The Standards are written in the perspective that the Responsible Entity is required to protect its cyber systems from internal and external threat. The requirements include both preventive and detective controls. The requirements mandate appropriate vetting of personnel to minimize the risk of internal threat. They then build upon this through secure system design for internal use and remote access. These controls are further enhanced by the requirement of robust monitoring and alerting activities. Specific requirements in the identification and protection of physical and electronic security perimeters assume a default posture of "deny-by-default" to reinforce the posture of mutual distrust.
Para 433 ". . . we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard."	FERC Order No. 706	The SDT addressed this by determining that identification of certain core training elements would be beneficial, and the identification of those core training elements that must be provided in the training program should be role based, as required in CIP-004-5, requirement R2.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 434 "The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets."	FERC Order No. 706	The SDT added this as a topic for role-specific training in CIP-004-5, requirement R2 (part 2.1). Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems.
Para 435 "Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves."	FERC Order No. 706	The SDT has considered the issue and has determined that no modifications are necessary. In practice, this training is often conducted as computer-based training (CBT), and the training is aimed at an entity's own policies. The SDT believes that assessments of the adequacy of the training during the compliance monitoring process implicitly evaluate the adequate training of the trainers or the efficacy of the training method.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 446 (1 of 2) (Review the referenced Comments) " APPA/LPPC seek **clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees.** SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees. The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."	FERC Order No. 706	The SDT clarifies the discretion in reviewing personnel risk assessments in CIP-004-5, requirement R3, by requiring the Responsible Entity to establish and document criteria for personnel risk assessments. The requirements in CIP-004-5 also provide additional detail about what type of records (whether criminal, work history, domicile, etc) a Responsible Entity must examine.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 446 (2 of 2) (Review the Referenced Comments) "APPA/LPPC seek clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees. **SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees.** The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."	FERC Order No. 706	In CIP-004-5, requirement R3, the SDT has specified that the seven-year criminal history records check must include current residence, regardless of duration, and include other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 460 "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."	FERC Order No. 706	In CIP-004-5, requirement R5, the SDT has addressed this directive by requiring initiation of the revocation of physical and interactive remote access, to be completed within 24 hours of termination, concurrent with the termination or disciplinary action (Part 5.1), or by the end of the calendar day in cases of transfers or reassignments (Part 5.2) for access that the Responsible Entity determines is no longer needed.. CIP-004-5, requirement R5 (part 5.4) augments the requirements in parts 5.1 and 5.2 that respond to the directive. In order to meet the immediate time frame, Entities will likely have initial revocation procedures to prevent physical and interactive remote access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. Part 5.4 requires the Responsible Entity to complete the revocation process within the time specified (30 days). Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
Para 464 "We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification."	FERC Order No. 706	The SDT notes that it addresses this issue in previous versions of the CIP standards. Version 2 added the requirement for a personnel risk assessment prior to being granted access, and Version 3 required implementation of a visitor control program. The changes made to the requirements in Version 5 maintain and improve upon these requirements. CIP-004-5, requirement R4 makes clear that individuals not properly authorized for unescorted physical access will not have such access. CIP-006-5 restricts access through implementation of a visitor management program.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 473 "The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entitys obligations regarding vendors with access to critical cyber assets."	FERC Order No. 706	CIP-002-5, requirement R1 makes clear that asset owners are responsible for complying with the standards.
Para 476 "We direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent with the Commissions determinations above."	FERC Order No. 706	Guidance in CIP-002-5 states that the owning Responsible Entity is responsible for complying with the CIP Cyber Security Standards. Furthermore, the guidelines and technical basis for CIP-002-5 states that where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 496 (Related: Para 503) Para 496 "The Commission adopts the CIP NOPRs proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter" Para 503 "The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures."	FERC Order No. 706	The drafting team addresses this in CIP-005-5, requirement R1 (part 1.5). Per FERC Order No. 706, Paragraphs 496 through 503, Electronic Security Perimeters (ESP) need two distinct security measures, such that the cyber assets do not lose all perimeter protection if one measure fails or is misconfigured, in a defense-in-depth approach. The Order makes clear that this is not simple redundancy of firewalls; thus, the drafting team added the security requirement of malicious traffic inspection (IDS/IPS) as a second security control for electronic access points for High Impact BES Cyber Systems.
Para 502 "The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process."	FERC Order No. 706	The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security requirement of malicious traffic inspection (IDS/IPS) as a second security control for electronic access points for High Impact BES Cyber Systems.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 504 (Related: Para 495) Para 504 "The ERO should consider in the Reliability Standards development process Northern Indiana's and Xcel's concerns regarding the phrase "single access point at the dial up device." Para 495 "Northern Indiana and Xcel ask the Commission to clarify or direct the ERO to clarify the phrase "single access point at the dial up device" in CIP-005-1, Requirement R1.2. Xcel asks whether this refers to the initiating device, the device at the point of termination, or both. Northern Indiana would not modify CIP-005-1, but urges that any modifications to Requirement R2 should allow continued reliance on legacy systems."	FERC Order No. 706	The SDT has deleted the troublesome language relating to "single access point at the dial up device," and the SDT has clarified that an Electronic Security Perimeter applies to routable connectivity. CIP-005-5 also separated the requirement for dial-up connectivity, specifying in CIP-005-5, R1.4, that a Responsible Entity must perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible, on its high and medium impact BES Cyber Systems with dial-up connectivity.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 511 "The Commission adopts the CIP NOPRs proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies."	FERC Order No. 706	CIP-005-5, requirement R2 has additional security requirements for remote access from the work started in the Urgent Action Revisions to CIP-005-3. One of these requirements is two-factor authentication and specific examples of two-factor authentication are provided in the guideline referenced in the rationale for this requirement.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 525 "The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily…" Para 628. "Requirement R6 of CIP-007-1 does not address the frequency with which log should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly…"	FERC Order No. 706	In CIP-007-5, requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of once every 15 days. CIP-007-5, requirement R4, combines CIP-005-4, requirement R5 and CIP-007-4, requirement R6, and addresses FERC Order No. 706's directives from a system-wide perspective. The primary feedback received on this requirement from comment periods was the vagueness of terms "security event" and "monitor." The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach to specify a minimum set of security event types to log and review, and allows the entity to define relevant security events in addition to the specified minimum. In addition, CIP-007-5, requirement R4, sets up parameters for the logging and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC Order No. 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 526 (1 of 2) ". . . the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments.	FERC Order No. 706	In CIP-007-5, requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of once every 15 days. (Also see response to paragraph 525).
Para 526 (2 of 2) "The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs."	FERC Order No. 706	CIP-007-5, requirement R4, sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. (Also see response to paragraph 525).
Para 528 "The Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs."	FERC Order No. 706	In CIP-007-5, requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of once every 15 days. In addition, CIP-007-5, requirement R4, sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC Order No. 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings. (Also see response to paragraph 525).

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 541 ". . . we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments."	FERC Order No. 706	In CIP-010-1, requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires paper assessments at least once every 15 months in the intervening years.
Para 542 ". . . the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems."	FERC Order No. 706	In CIP-010-1, requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires paper assessments at least once every 15 months in the intervening years.
Para 544 (1 of 2) "the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification."	FERC Order No. 706	The SDT addresses this paragraph in CIP-010-1, requirement R3. • The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new Cyber Asset undergo an active vulnerability assessment. • An exception is made for specified CIP Exceptional Circumstances. • Additionally, the new requirement in CIP-010-1, requirement R1 (part 1.5) requires testing of all changes for High Impact BES Cyber Systems that deviate from the baseline configuration in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) to ensure that required security controls are not adversely affected.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 544 (2 of 2) “. . . we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment”	FERC Order No. 706	The SDT has added a requirement in CIP-010-5, requirement R3 (part 3.3), to perform an active vulnerability assessment of a new Cyber Asset in High Impact BES Cyber Systems.
Para 547 ". . . we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"	FERC Order No. 706	In CIP-010-1, requirement R3, the SDT has added requirements for an “active vulnerability assessment” to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires paper assessments at least once every 15 months in the intervening years.
Para 572 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."	FERC Order No. 706	The SDT addressed this in CIP-006-5, requirement R1 (part 1.3) for High Impact BES Cyber Assets, by requiring Responsible Entities to “utilize two or more different physical access controls to collectively allow physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.”

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 581 "The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years."	FERC Order No. 706	The SDT addressed this in CIP-006-5, requirement R3 (part 3.1) by changing the frequency to a 24-month testing cycle; after deliberation and consideration, the SDT determined that a requirement of more frequent testing (e.g., 12 months), would pose unreasonable burden for Responsible Entities with a large number of physical security perimeters dispersed over large geographic areas.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 609, Sentence 5 "The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a representative system one that includes the essential equipment and adequately represents the functioning of the production system. **We therefore direct the ERO to develop requirements addressing what constitutes a representative system and to modify CIP-007-1 accordingly.** The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."	FERC Order No. 706	The SDT has introduced the concept of a “baseline configuration” around which the change control process is based. The SDT further utilizes this “baseline configuration” to provide clarity as to what is considered a representative system as it relates to performing active vulnerability assessments in CIP-010-1.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 609, Sentence 6 "The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a representative system one that includes the essential equipment and adequately represents the functioning of the production system. We therefore direct the ERO to develop requirements addressing what constitutes a representative system and to modify CIP-007-1 accordingly. **The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."**	FERC Order No. 706	The SDT has provided additional guidance on testing systems in the Guidelines and Technical Basis section of CIP-010-1. Furthermore, and in addition to guidance, the requirements of CIP-010-1 R1.5 and CIP-010-1 R3.2 identify a “representative system” as a system that exists in a test environment (or production environment where tests can be performed in a manner that minimizes adverse effects) that models the baseline configuration of the BES Cyber System in a production environment. This baseline configuration concept is developed by entities in CIP-010-1 R1.1 and further contains details on what constitutes a “representative system.”

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 610 “. . . we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above.”	FERC Order No. 706	CIP-010-1, requirements R1 (part 1.5) requires Responsible Entities to account for any additional differences between the two systems, the SDT proposes using the words similar to those directly from FERC Order No. 706, paragraph 610: “Document the differences between the test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.”

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 611 "With respect to MidAmericans proposal that the differences between the testing and production environments only be reported when the production and test environments are established, the ERO should consider this matter in the Reliability Standards development process However, the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."	FERC Order No. 706	The SDT has added a requirement for the Responsible Entity to, "document…the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments." The SDT has included this requirement for each test performed in the representative environment. The SDT appreciates the concern brought up by MidAmerican and believes that entities should be free to use the same documentation multiple times to provide compliance with this requirement so as to minimize the documentation overhead, but also believes that it is important for entities to give consideration to the configuration of their representative system each time a test is performed in order to ensure the validity of the test results.
Paras 622 (Related: See Paras 614 and 619) "Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere."	FERC Order No. 706	The "acceptance of risk" language was removed in Version 2, and it has not been used in Version 5. Malicious software prevention exceptions have been placed under the TFE process since Version 2.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 622 (Related: See Paras 614 and 619) "The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above."	FERC Order No. 706	The drafting team addressed this in CIP-007-5, requirement R3. The drafting team is taking the approach of making this requirement a competency-based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive. When remote access is used to connect to a BES Cyber Asset, an intermediate device is required in CIP-005-5, requirement R2 (part 2.1) and guidance is further included for the cyber security policy in CIP-003-5, Requirement R2 to maintain up-to-date anti-malware software and patch levels before initiating interactive remote access.
Para 628 "The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1."	FERC Order No. 706	In CIP-007-5, requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of once every 15 days.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 633 "The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it."	FERC Order No. 706	The SDT addresses this directive in CIP-011-1, requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from the BES Cyber Asset. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal. Additional guidance was added to the standard as further clarification: Media sanitization is generally classified into four categories: disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes. This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 635 "the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."	FERC Order No. 706	The SDT addresses this directive in CIP-011-1, requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from the BES Cyber Asset. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal. Additional guidance was added to the standard as further clarification: Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes. This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 643 (1 of 2) **"The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments**, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."	FERC Order No. 706	In order to provide more direction on what "features, functionality, and vulnerabilities" should be addressed in a vulnerability assessment, the SDT included guidance in CIP-010-1 on active and paper vulnerability assessment. The SDT further referenced NIST SP800-115 to provide entities additional guidance on how to conduct a vulnerability assessment.
Para 643 (2 of 2) "The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, **and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."**	FERC Order No. 706	In CIP-010-1, requirement R3 (part 3.4), the SDT added a requirement for an entity planned date of completion to the remediation action plan following a vulnerability assessment.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 660 (Related, See Para 661) "The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. In developing the guidance, the ERO should consider the specific examples provided by commenters, described above. However, we direct the ERO to develop and provide guidance on the term reportable incident. The Commission is not opposed to the suggestion that the ERO create a reference document containing the reporting criteria and thresholds and requiring responsible entities to comply with the reference document in the revised Reliability Standard CIP-008-1, but will allow the ERO to determine the best method to accomplish the goal of better defining reportable incident."	FERC Order No. 706	In addition to defining the term Reportable Cyber Security Incident as one that compromises or disrupts the functional tasks of a Responsible Entity, CIP-008-5 also provides further guidance for determining a Reportable Cyber Security Incident in the "Guidelines and Technical Basis" section of the standard. The definition and guidance describe a reportable incident based on characteristics of impact to the BES, rather than enumerating threats and characteristics of malware.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 661 (Related, See Para 660) "the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."	FERC Order No. 706	CIP-008-5 addresses the four parts of this directive as follows: 1. Added: Reportable Cyber Security Incidents include, as a minimum, any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. In turn, a Cyber Security Incident includes a malicious act or suspicious event that compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter. 2. CIP-008-4, requirement R1 (part 1.2) contains provisions for reporting Cyber Security Incidents. 3. See 1, above. 4. Guidance and measurements have been developed to provide information that may be used to enhance an auditable and enforceable standard.
Para 673 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order No. 706	Cyber Security Incident Reporting and Response Planning: CIP-008-4, requirement R1 (part 1.3) contains provisions for reporting Cyber Security Incidents to the ES-ISAC within one hour of identification, even if it is a preliminary report.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 676 "The Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order No. 706	Cyber Security - Incident Reporting and Response Planning: CIP-008-4, requirement R1 (part 1.3) contains provisions for reporting Cyber Security Incidents to the ES-ISAC within one hour of identification, even if it is a preliminary report. . Cyber Security - Incident Reporting and Response Planning: CIP-008-4, requirement R1 (part 1.3) contains provisions for reporting Cyber Security Incidents to the ES-ISAC within one hour of identification, even if it is a preliminary report.
Para 686 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned."	FERC Order No. 706	In CIP-008-5, Requirement R3 and its parts, the SDT includes additional specification on the update of response plan and modifies the response plan requirements to incorporate lessons learned. Maintenance of documentation of paper drills, full operational drills, and responses to actual incidents is part of the documentation required to demonstrate compliance with the security controls in CIP-008-5 and is already subject to the evidence retention requirements associated with all NERC Reliability Standards.
Para 687 (also see Footnote in Order) "In light of the comments received, the Commission clarifies that, with respect to full operational testing under CIP-008-1,	FERC Order No. 706	CIP 008-5, Requirement R2, Part 2.1 is written to allow the testing requirement to be satisfied by responding to an actual Reportable Cyber Security Incident; or with a paper drill or table top exercise; or with a full operational exercise. The reporting of Cyber Security Incidents is addressed in the requirement R1 (part 1.2).

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
such testing need not require a responsible entity to remove any systems from service. The Commission understands that use of the term full operational exercise in this context can be confusing. We interpret the priority of the testing required by this provision to be that planned response actions are exercised in reference to a presumed or hypothetical incident contemplated by the cyber security response plan, and not necessarily that the presumed incident is performed on the live system. A responsible entity should assume a certain type of incident had occurred, and then ensure that its employees take what action would be required under the response plan, given the hypothetical incident. A responsible entity must ensure that it is properly identifying potential incidents as physical or cyber and contacting the appropriate government, law enforcement or industry authorities. CIP-008-1 should require a responsible entity to verify the list of entities that must be called pursuant to its cyber security incident response plan and that the contact numbers at those agencies are correct. The ERO should clarify this in the revised Reliability Standard and may use a term different than		The Guidelines and Technical Basis section of CIP-008-5 refer to operational exercises in the FEMA Homeland Security Exercise Evaluation Program as one of the following three types: drill, functional exercise, and full-scale exercise. It defines that “[a] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, emergency operation centers, etc.) and "boots on the ground" response (e.g., firefighters decontaminating mock victims).” The SDT believes the term operational exercise has become well understood and appropriate for both incident response and recovery exercises.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
full operational exercise.”		
Para 694 “For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard”	FERC Order No. 706	The SDT added in CIP-009-5, Requirement R2, a requirement to implement the recovery plan.
Para 706 "The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard."	FERC Order No. 706	CIP-009-5, Requirement R1, Part 1.5 requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service. The SDT captured the objective of this control, but did not explicitly use the term “forensics” due to the legal interpretations associated with the term.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 710 (Related: Para 706) "Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report."	FERC Order No. 706	CIP-009-5, Requirement R1, Part 1.5 requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service.
Para 725 "The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years."	FERC Order No. 706	CIP-009-5, Requirement R2, Part 2.3 requires an operational exercise at least once every three calendar years.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 739 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."	FERC Order No. 706	In CIP-009-5, Requirement R1, Part 1.4 the SDT added requirements related to restoration processes based on review of the DHS Controls, and requires verification initially after backup to ensure that the process completed successfully. In CIP-009-5, Requirement R2, part 2.2, requires a Responsible Entity to ensure that the information is useable and is compatible with current system configurations for High Impact BES Cyber Systems or Medium Impact BES Cyber Systems at Control Centers.
Para 748 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."	FERC Order No. 706	In CIP-009-5, Requirement R1, Part 1.4 the SDT added requirements related to restoration processes based on review of the DHS Catalog of Control Systems Security: Recommendations for Standards Developers (a derivation of NIST SP800-53 for Control Systems), and requires verification initially after backup to ensure that the process completed successfully.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
	NERC Alert regarding remote access VPN vulnerabilities	Addressed in CIP-005-5 ▪ Creates basic requirements to protect critical systems from untrusted networks. ▪ Identifies protective measures that provide secure access to critical systems. ▪ Helps ensure secure practices by employees, contractors, and service vendors to minimize exploitation of vulnerabilities. ▪ Addresses questions regarding ability to audit or enforce the requirement through the design of clear measures. ▪ Significant guidance provided to address implementation options for organizations of differing sizes, capabilities, and complexity. Additional information is provided in "Guidance for Secure Interactive Remote Access" published by NERC in July 2011. Additionally, remote access is specifically required to be included in an entity's cyber security policy. Guidance is included to assist the entity in determining what this topic in the cyber security policy should address.

Project 2008-06 Cyber Security Order No. 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 13 "The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."	Order Approving Interpretation of Reliability Standard CIP-007-2 in Docket No. RD10-3-000, March 18, 2010	CIP-007-5, Requirement R1, Part 1.2 requires Responsible Entities (for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers) to "protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media."